Citrix ADC 13.0

Machine translated content

Disclaimer

Die offizielle Version dieses Inhalts ist auf Englisch. Für den einfachen Einstieg wird Teil des Inhalts der Citrix Dokumentation maschinell übersetzt. Citrix hat keine Kontrolle über maschinell übersetzte Inhalte, die Fehler, Ungenauigkeiten oder eine ungeeignete Sprache enthalten können. Es wird keine Garantie, weder ausdrücklich noch stillschweigend, für die Genauigkeit, Zuverlässigkeit, Eignung oder Richtigkeit von Übersetzungen aus dem englischen Original in eine andere Sprache oder für die Konformität Ihres Citrix Produkts oder Ihres Diensts mit maschinell übersetzten Inhalten gegeben, und jegliche Garantie, die im Rahmen der anwendbaren Endbenutzer-Lizenzvereinbarung oder der Vertragsbedingungen oder einer anderen Vereinbarung mit Citrix gegeben wird, dass das Produkt oder den Dienst mit der Dokumentation übereinstimmt, gilt nicht in dem Umfang, in dem diese Dokumentation maschinell übersetzt wurde. Citrix kann nicht für Schäden oder Probleme verantwortlich gemacht werden, die durch die Verwendung maschinell übersetzter Inhalte entstehen können.

Contents

Citrix ADC-Versionshinweise

August 11, 2022

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

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

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

> **Hinweis**
>
> - Die [# XXXXXX] -Labels unter den Problembeschreibungen sind interne Tracking-IDs, die vom Citrix ADC-Team verwendet werden.
> - Diese Versionshinweise dokumentieren keine sicherheitsrelevanten Korrekturen. Eine Liste der sicherheitsbezogenen Fixes und Advisorys finden Sie im Citrix Security Bulletin.

Um das Dokument mit den Versionshinweisen für einen bestimmten Build anzuzeigen, klicken Sie auf den entsprechenden Link in der folgenden Tabelle. Wenn die Versionshinweise für einen Build aktualisiert werden, werden auch die Versionsnummer der Versionshinweise und das Veröffentlichungsdatum aktualisiert. Das Veröffentlichungsdatum der Versionshinweise entspricht möglicherweise nicht dem Build-GA-Datum.

Versionshinweise für Citrix ADC Release 13.0	Veröffentlichungshinweise Veröffentlichungsdatum	Version der Veröffentlichungshinweise
Build 87.9	03. August 2022	1.0
Build 86.17	17. Juni 2022	1.0
Build 85.19	25. Mai 2022	3.0
Build 84.11	31. Januar 2022	3.0
Build 83.29	15. November 2021	1.0
Build 82.45	19. Juli 2021	2.0
Build 79.64	28. April 2021	3.0
Build 76.31	06. April 2021	3.0
Build 71.44	19. Februar 2021	4.0

Versionshinweise für Citrix ADC Release 13.0	Veröffentlichungshinweise Veröffentlichungsdatum	Version der Veröffentlichungshinweise
Build 67.43	26. November 2020	2.0
Build 64.35	21. Januar 2021	4.0
Build 61.48	04. September 2020	3.0
Build 58.32	07. Juli 2020	1.0
Build 52.24	20. Juli 2020	4.0
Build 47.24	20. April 2020	2.0
Build 41.28	20. April 2020	3.0

Erste Schritte mit Citrix ADC

July 8, 2022

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

Citrix ADC verstehen

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

1. Daten-Switching
2. Firewall-Sicherheit
3. Optimierung
4. Politische Infrastruktur
5. Paketfluss
6. Beschränkung des Systems

Daten-Switching

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

Firewall-Sicherheit

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

Optimierung

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

Politische Infrastruktur

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

und die Prioritäten bestimmen die Reihenfolge, in der die Richtlinien bewertet werden.

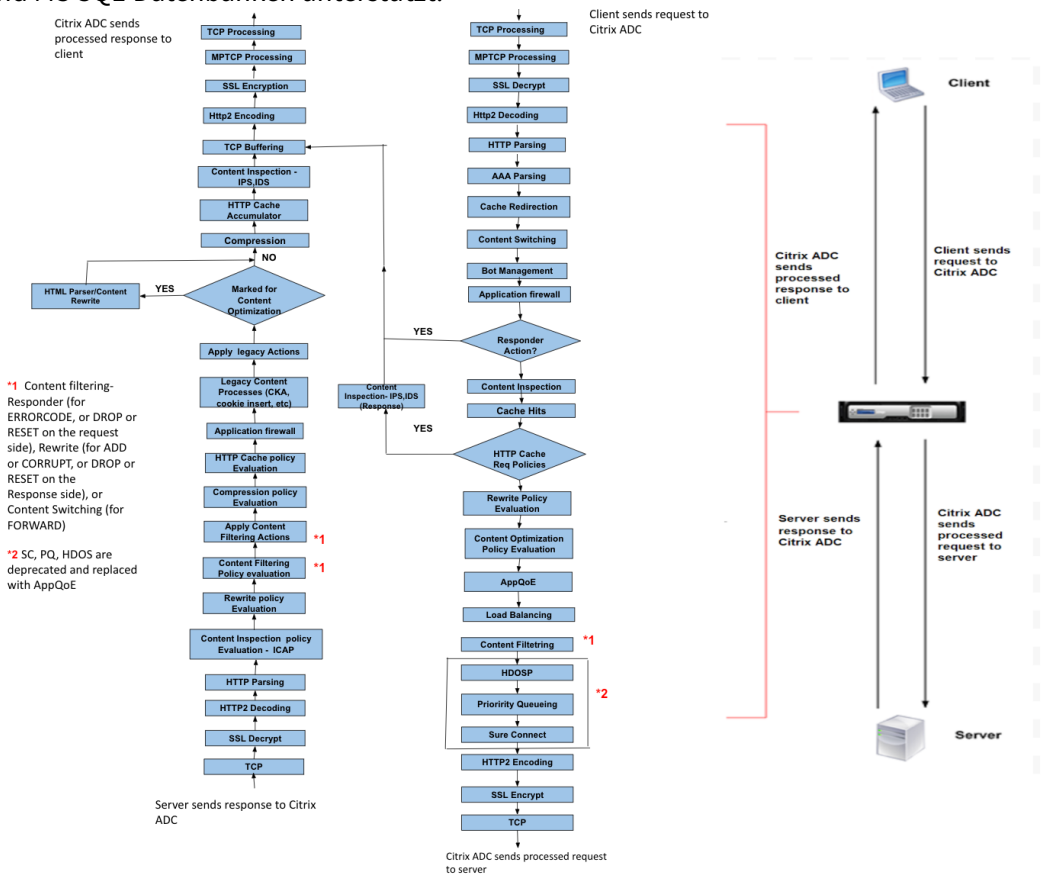
Wenn eine ADC-Appliance Datenverkehr empfängt, bestimmt die entsprechende Richtlinienliste, wie der Datenverkehr verarbeitet werden soll. Jede Richtlinie in der Liste enthält einen oder mehrere Ausdrücke, die zusammen die Kriterien definieren, die eine Verbindung erfüllen muss, um der Richtlinie zu entsprechen.

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

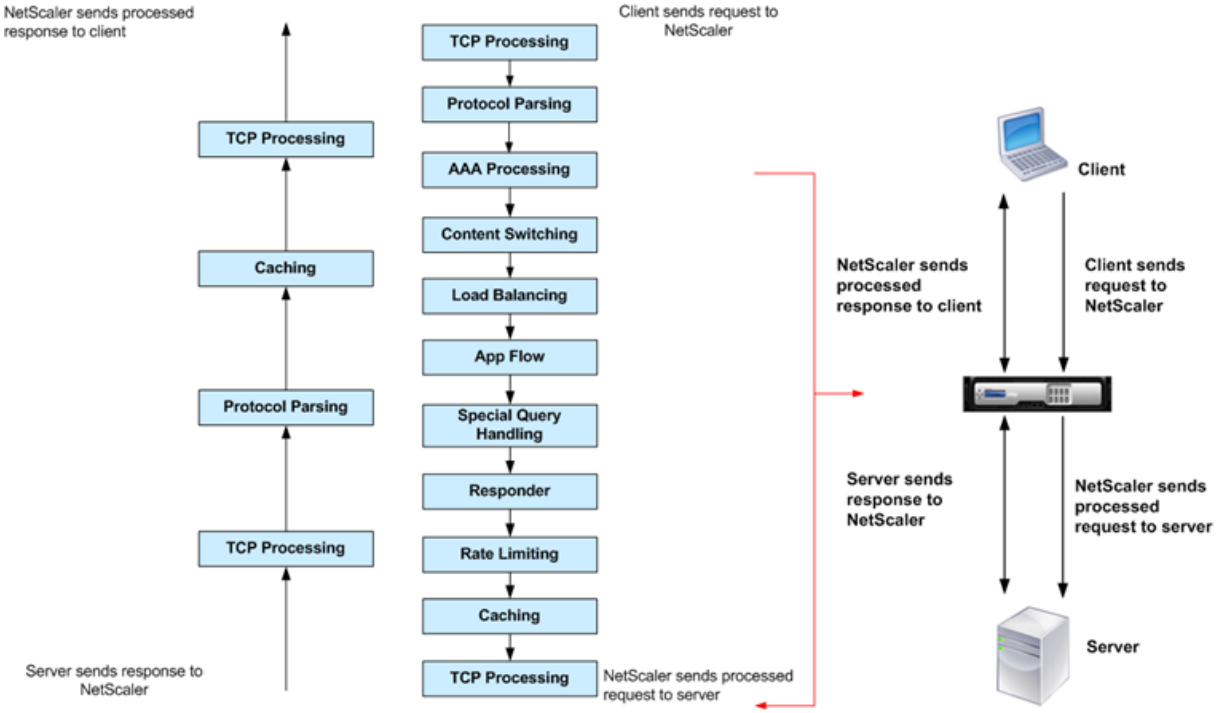
Paketfluss

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

Die folgende Abbildung zeigt den DataStream-Paketfluss in der Citrix ADC-Appliance. DataStream wird für MySQL- und MS SQL-Datenbanken unterstützt.



Die folgende Abbildung zeigt den DataStream-Paketfluss in der Citrix ADC-Appliance. DataStream wird für MySQL- und MS SQL-Datenbanken unterstützt. Informationen zur DataStream-Funktion finden Sie unter DataStream.



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

Beschränkung des Systems

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

Wo passt eine Citrix ADC Appliance in das Netzwerk?

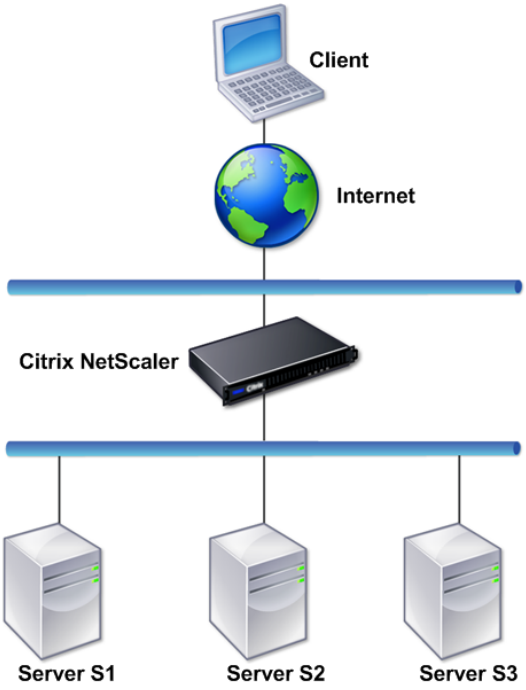
October 5, 2021

Eine Citrix ADC Appliance befindet sich zwischen den Clients und den Servern, sodass Clientanforderungen und Serverantworten durch sie geleitet werden. In einer typischen Installation stellen virtuelle Server, die auf der Appliance konfiguriert sind, Verbindungspunkte bereit, die Clients für den Zugriff auf die Anwendungen hinter der Appliance verwenden. In diesem Fall besitzt die Appliance öffentliche IP-Adressen, die ihren virtuellen Servern zugeordnet sind, während die realen Server in einem privaten Netzwerk isoliert sind. Es ist auch möglich, das Gerät in einem transparenten Modus als L2-Brücke oder L3-Router zu betreiben oder sogar Aspekte dieser und anderer Modi zu kombinieren.

Physische Bereitstellungsmodi

Eine Citrix ADC Appliance, die sich logisch zwischen Clients und Servern befindet, kann in einem der beiden physischen Modi bereitgestellt werden: Inline und One-Arm. Im Inline-Modus werden mehrere Netzwerkschnittstellen mit verschiedenen Ethernet-Segmenten verbunden und die Appliance wird zwischen den Clients und den Servern platziert. Die Appliance verfügt über eine separate Netzwerkschnittstelle zu jedem Client-Netzwerk und eine separate Netzwerkschnittstelle zu jedem Servernetzwerk. Die Appliance und die Server können in verschiedenen Subnetzen in dieser Konfiguration vorhanden sein. Es ist möglich, dass sich die Server in einem öffentlichen Netzwerk befinden und die Clients über die Appliance direkt auf die Server zugreifen, wobei die Appliance die L4-L7-Funktionen transparent anwendet. Üblicherweise werden virtuelle Server (später beschrieben) so konfiguriert, dass sie eine Abstraktion der realen Server bereitstellen. Die folgende Abbildung zeigt eine typische Inline-Bereitstellung.

Abbildung 1. Inline-Bereitstellung



Im Einarmmodus ist nur eine Netzwerkschnittstelle der Appliance an ein Ethernet-Segment angeschlossen. Die Appliance isoliert in diesem Fall nicht die Client- und Serverseiten des Netzwerks, sondern bietet Zugriff auf Anwendungen über konfigurierte virtuelle Server. Der Einarmmodus kann Netzwerkänderungen vereinfachen, die für die Citrix ADC Installation in einigen Umgebungen erforderlich sind.

Beispiele für Inline- (zweiarmige) und einarmige Bereitstellung finden Sie unter Grundlegendes zu allgemeinen Netzwerktopologien.

Citrix ADC als L2-Gerät

Eine Citrix ADC Appliance, die als L2-Gerät fungiert, soll im L2-Modus betrieben werden. Im L2-Modus leitet die ADC-Appliance Pakete zwischen Netzwerkschnittstellen weiter, wenn alle folgenden Bedingungen erfüllt sind:

- Die Pakete sind für die MAC-Adresse (Media Access Control) eines anderen Geräts bestimmt.
- Die Ziel-MAC-Adresse befindet sich auf einer anderen Netzwerkschnittstelle.
- Die Netzwerkschnittstelle ist Mitglied desselben virtuellen LANs (VLAN).

Standardmäßig sind alle Netzwerkschnittstellen Mitglieder eines vordefinierten VLAN, VLAN 1. ARP-Anforderungen und -Antworten (Address Resolution Protocol) werden an alle Netzwerkschnittstellen

weitergeleitet, die Mitglieder desselben VLAN sind. Um Überbrückungsschleifen zu vermeiden, muss der L2-Modus deaktiviert werden, wenn ein anderes L2-Gerät parallel zur Citrix ADC Appliance arbeitet.

Informationen zur Interaktion der L2- und L3-Modi finden Sie unter Paketweiterleitungsmodi.

Informationen zum Konfigurieren des L2-Modus finden Sie im Abschnitt “Aktivieren und Deaktivieren des Layer-2-Modus” in den Paketweiterleitungsmodi.

Citrix ADC als Paketweiterleitungsgerät

Eine Citrix ADC Appliance kann als Paketweiterleitungsgerät fungieren, und diese Betriebsart wird als L3-Modus bezeichnet. Wenn der L3-Modus aktiviert ist, leitet die Appliance alle empfangenen Unicastpakete weiter, die für eine IP-Adresse bestimmt sind, die nicht zur Appliance gehört, wenn eine Route zum Ziel vorhanden ist. Die Appliance kann auch Pakete zwischen VLANs weiterleiten.

In beiden Betriebsmodi, L2 und L3, löscht die Appliance im Allgemeinen Pakete, die sich in folgenden Bereichen befinden:

- Multicast-Rahmen
- Unbekannte Protokollrahmen für die MAC-Adresse einer Appliance (Nicht-IP und Nicht-ARP)
- Spanning Tree Protokoll (es sei denn, BridgeBPDUs ist ON)

Informationen zur Interaktion der L2- und L3-Modi finden Sie unter Paketweiterleitungsmodi.

Informationen zum Konfigurieren des L3-Modus finden Sie unter Paketweiterleitungsmodi.

Kommunikation einer Citrix ADC Appliance mit Clients und Servern

October 5, 2021

Eine Citrix ADC Appliance wird normalerweise vor einer Serverfarm bereitgestellt und fungiert als transparenter TCP-Proxy zwischen Clients und Servern, ohne dass eine clientseitige Konfiguration erforderlich ist. Diese grundlegende Betriebsart wird als Request-Switching-Technologie bezeichnet und ist der Kern der Citrix ADC Funktionalität. Anforderungsumschaltung ermöglicht es einer Appliance, die TCP-Verbindungen zu multiplex und zu entlasten, persistente Verbindungen zu pflegen und den Datenverkehr auf Anforderungsebene (Anwendungsschicht) zu verwalten. Dies ist möglich, da die Appliance die HTTP-Anforderung von der TCP-Verbindung trennen kann, für die die Anforderung gesendet wird.

Abhängig von der Konfiguration kann eine Appliance den Datenverkehr verarbeiten, bevor sie die Anforderung an einen Server weiterleitet. Wenn der Client beispielsweise versucht, auf eine sichere

Anwendung auf dem Server zuzugreifen, führt die Appliance möglicherweise die erforderliche SSL-Verarbeitung durch, bevor Datenverkehr an den Server gesendet wird.

Um den effizienten und sicheren Zugriff auf Serverressourcen zu erleichtern, verwendet eine Appliance eine Gruppe von IP-Adressen, die gemeinsam als Citrix ADC-eigene IP-Adressen bezeichnet werden. Um den Netzwerkverkehr zu verwalten, weisen Sie IP-Adressen von Citrix ADC zu virtuellen Entitäten zu, die zu den Bausteinen Ihrer Konfiguration werden. Zum Konfigurieren des Lastenausgleichs erstellen Sie beispielsweise virtuelle Server, um Clientanforderungen zu empfangen und sie an Dienste zu verteilen, bei denen es sich um Entitäten handelt, die die Anwendungen auf Ihren Servern darstellen.

Grundlegendes zu Citrix ADC-eigenen IP-Adressen

Um als Proxy zu fungieren, verwendet eine Citrix ADC Appliance eine Vielzahl von IP-Adressen. Die wichtigsten IP-Adressen von Citrix ADC sind:

- Citrix ADC IP-Adresse (NSIP)

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

- IP-Adresse (VIP) desvirtuellen Servers

  Eine VIP-Adresse ist die IP-Adresse, die einem virtuellen Server zugeordnet ist. Es ist die öffentliche IP-Adresse, mit der Clients eine Verbindung herstellen. Bei einer Appliance, die einen großen Datenverkehr verwaltet, können viele VIPs konfiguriert sein.

- Subnetz-IP-Adresse (SNIP)

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

- IP Set

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

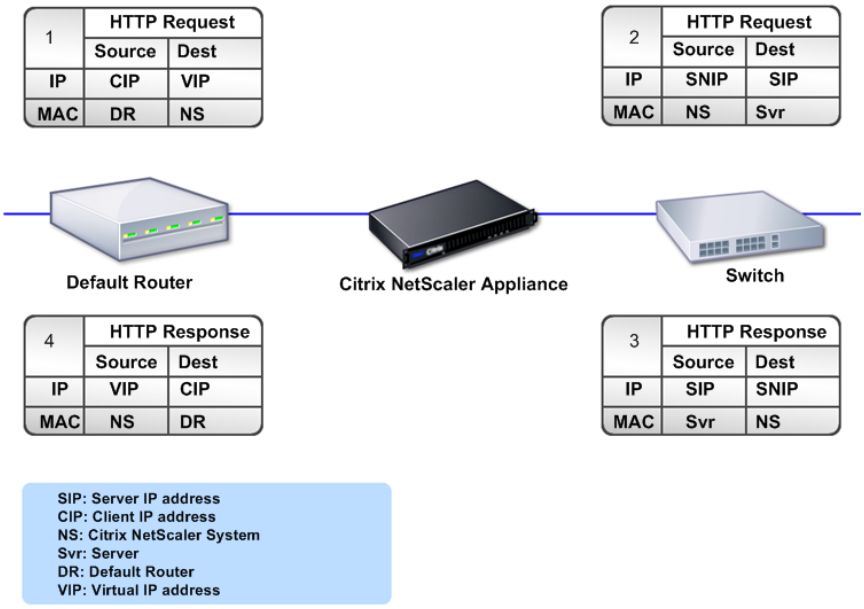
- Net-Profil

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

Verwalten von Verkehrsflüssen

Da eine Citrix ADC Appliance als TCP-Proxy fungiert, werden IP-Adressen übersetzt, bevor Pakete an einen Server gesendet werden. Wenn Sie einen virtuellen Server konfigurieren, stellen Clients eine Verbindung zu einer VIP-Adresse auf der Citrix ADC Appliance her, anstatt eine direkte Verbindung mit einem Server herzustellen. Wie von den Einstellungen auf dem virtuellen Server bestimmt, wählt die Appliance einen geeigneten Server aus und sendet die Anforderung des Clients an diesen Server. Standardmäßig verwendet die Appliance eine SNIP-Adresse, um Verbindungen mit dem Server herzustellen, wie in der folgenden Abbildung dargestellt.

Abbildung 1. Virtuelle Server-basierte Verbindungen



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

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

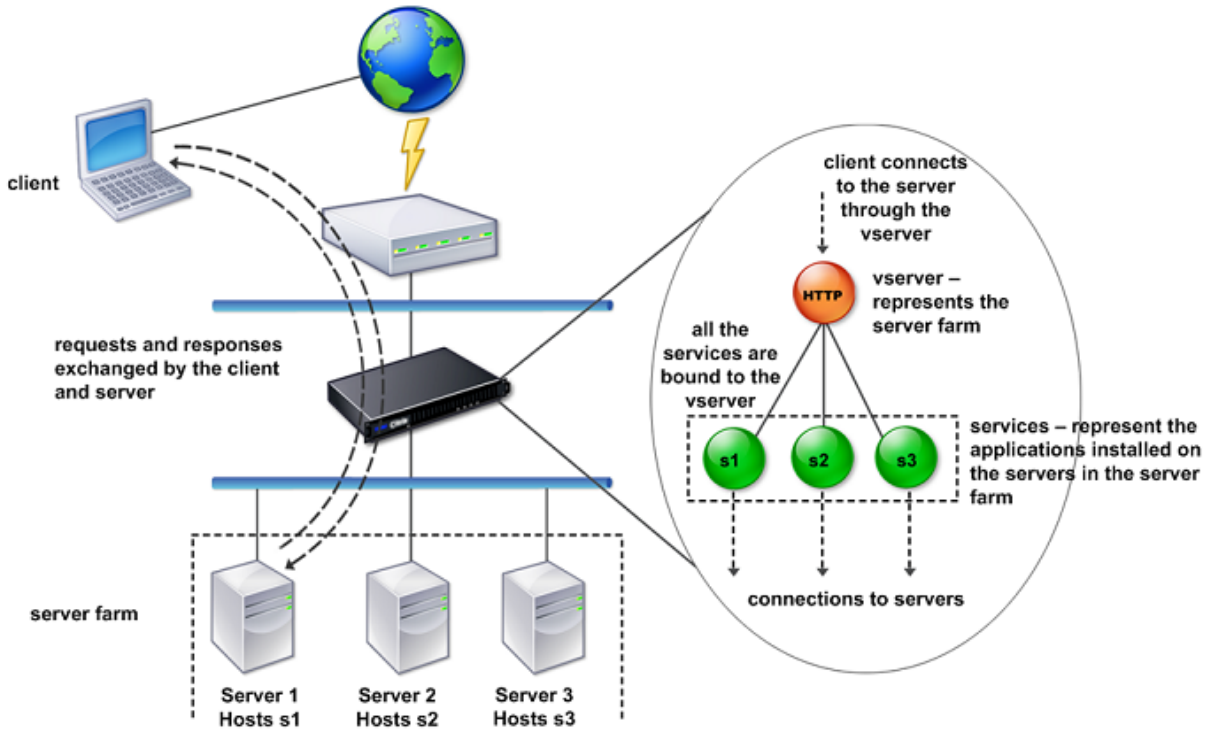
Verbindungen zu den Servern verwendet wird.

Bausteine für Verkehrsmanagement

Die Konfiguration einer Citrix ADC Appliance besteht in der Regel aus einer Reihe virtueller Entitäten, die als Bausteine für die Datenverkehrsverwaltung dienen. Der Bausteinansatz unterstützt die Trennung von Verkehrsflüssen. Virtuelle Entitäten sind Abstraktionen, die normalerweise IP-Adressen, Ports und Protokollhandler für die Verarbeitung von Datenverkehr darstellen. Clients greifen über diese virtuellen Entitäten auf Anwendungen und Ressourcen zu. Die am häufigsten verwendeten Entitäten sind virtuelle Server und Dienste. Virtuelle Server stellen Gruppen von Servern in einer Serverfarm oder einem Remotenetzwerk dar, und Dienste stellen bestimmte Anwendungen auf jedem Server dar.

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

Abbildung 2. Funktionsweise von Bausteinen für die Verkehrsverwaltung

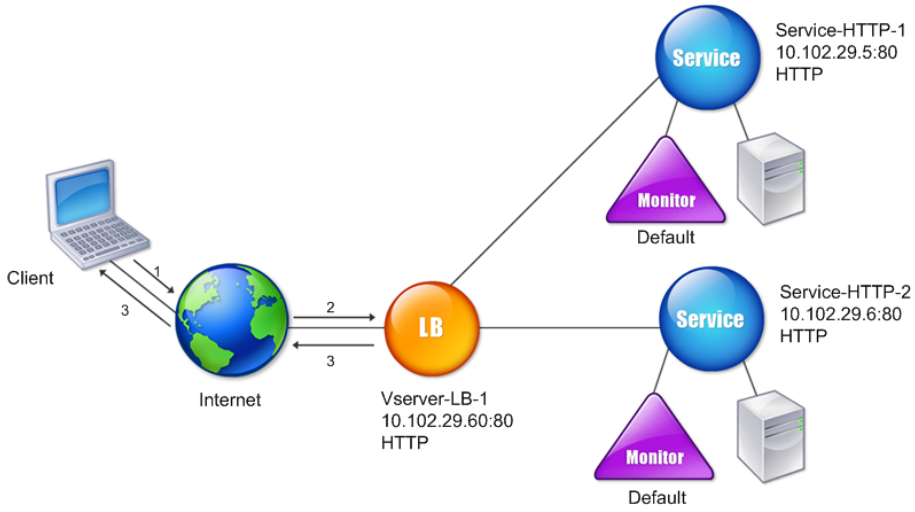


Einfache Lastausgleichskonfiguration

Im Beispiel in der folgenden Abbildung ist die Citrix ADC Appliance so konfiguriert, dass sie als Load Balancer fungiert. Für diese Konfiguration müssen Sie virtuelle Entitäten konfigurieren, die für den Lastenausgleich spezifisch sind, und diese in einer bestimmten Reihenfolge binden. Als Load Balancer verteilt eine Appliance Clientanforderungen auf mehrere Server und optimiert so die Ressourcennutzung.

Die grundlegenden Bausteine einer typischen Lastausgleichskonfiguration sind Dienste und virtuelle Lastausgleichsserver. Die Dienste stellen die Anwendungen auf den Servern dar. Die virtuellen Server abstrahieren die Server, indem sie eine einzige IP-Adresse angeben, mit der sich die Clients verbinden. Um sicherzustellen, dass Clientanforderungen an einen Server gesendet werden, müssen Sie jeden Dienst an einen virtuellen Server binden. Das heißt, Sie müssen Dienste für jeden Server erstellen und die Dienste an einen virtuellen Server binden. Clients verwenden die VIP-Adresse, um eine Verbindung mit einer Citrix ADC Appliance herzustellen. Wenn die Appliance Clientanforderungen empfängt, die an die VIP-Adresse gesendet werden, werden sie an einen Server gesendet, der durch den Lastausgleichsalgorithmus bestimmt wird. Der Lastenausgleich verwendet eine virtuelle Entität namens Monitor, um zu verfolgen, ob ein bestimmter konfigurierter Dienst (Server plus Anwendung) für den Empfang von Anforderungen verfügbar ist.

Abbildung 3. Lastenausgleich virtueller Server, Dienste und Monitore



Zusätzlich zum Konfigurieren des Lastausgleichsalgorithmus können Sie mehrere Parameter konfigurieren, die sich auf das Verhalten und die Leistung der Lastausgleichskonfiguration auswirken. Beispielsweise können Sie den virtuellen Server so konfigurieren, dass die Persistenz basierend auf der Quell-IP-Adresse beibehalten wird. Die Appliance leitet dann alle Anfragen von einer bestimmten IP-Adresse an denselben Server weiter.

Grundlegendes zu virtuellen Servern

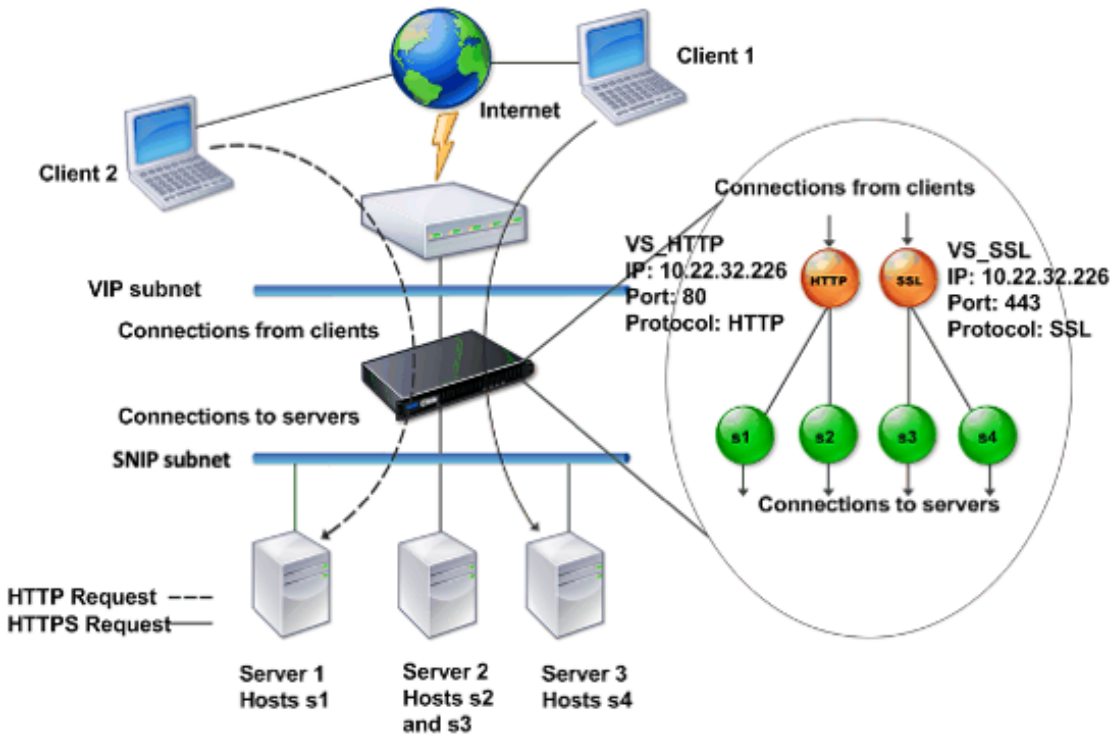
Ein virtueller Server ist eine Citrix ADC Entität, mit der externe Clients auf Anwendungen zugreifen können, die auf den Servern gehostet werden. Sie wird durch einen alphanumerischen Namen, eine virtuelle IP-Adresse (VIP), einen Port und ein Protokoll dargestellt. Der Name des virtuellen Servers ist nur von lokaler Bedeutung und soll die Identifizierung des virtuellen Servers erleichtern. Wenn ein Client versucht, auf Anwendungen auf einem Server zuzugreifen, sendet er eine Anforderung an den VIP anstelle der IP-Adresse des physischen Servers. Wenn die Appliance eine Anforderung an die VIP-Adresse erhält, beendet sie die Verbindung auf dem virtuellen Server und verwendet im Auftrag des Clients eine eigene Verbindung mit dem Server. Die Port- und Protokolleinstellungen des virtuellen Servers bestimmen die Anwendungen, die der virtuelle Server darstellt. Beispielsweise kann ein Webserver durch einen virtuellen Server und einen Dienst dargestellt werden, dessen Port und Protokoll auf 80 bzw. HTTP festgelegt sind. Mehrere virtuelle Server können dieselbe VIP-Adresse, aber unter-

schiedliche Protokolle und Ports verwenden.

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

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

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



Die obige Abbildung zeigt eine Konfiguration, die aus zwei virtuellen Servern mit einer gemeinsamen VIP-Adresse, aber unterschiedlichen Ports und Protokollen besteht. Jeder der virtuellen Server verfügt über zwei Dienste, die an ihn gebunden sind. Die Dienste s1 und s2 sind an VS_HTTP gebunden und stellen die HTTP-Anwendungen auf Server 1 und Server 2 dar. Die Dienste s3 und s4 sind an VS_SSL gebunden und stellen die SSL-Anwendungen auf Server 2 und Server 3 dar (Server 2 bi-

etet sowohl HTTP- als auch SSL-Anwendungen). Wenn die Appliance eine HTTP-Anforderung an die VIP-Adresse empfängt, verarbeitet sie die Anforderung gemäß den Einstellungen von VS_HTTP und sendet sie an Server 1 oder Server 2. Wenn die Appliance eine HTTPS-Anforderung an die VIP-Adresse empfängt, verarbeitet sie sie entsprechend den Einstellungen von VS_SSL und sendet sie entweder an Server 2 oder Server 3.

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

Virtuelle Server können in folgende Kategorien gruppiert werden:

- Virtueller Lastausgleichsserver

  Empfängt Anforderungen und leitet sie an einen entsprechenden Server weiter. Die Auswahl des entsprechenden Servers basiert auf der Konfiguration der verschiedenen Load Balancing-Methoden.

- Virtueller Server für die Cache-Umleitung

  Leitet Clientanforderungen für dynamischen Inhalt an Ursprungsserver und Anforderungen an statische Inhalte an Cacheserver um. Virtuelle Cache-Umleitungsserver funktionieren häufig in Verbindung mit virtuellen Servern mit Lastenausgleich.

- Virtueller Content Switching-Server

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

- Virtuelles privates Netzwerk (VPN) virtueller Server

  Entschlüsselt den getunnelten Datenverkehr und sendet ihn an Intranetanwendungen.

- Virtueller SSL-Server

  Empfangen und entschlüsselt SSL-Datenverkehr und leitet dann zu einem entsprechenden Server um. Die Auswahl des entsprechenden Servers ähnelt der Auswahl eines virtuellen Lastenausgleichsservers.

Verstehen von Dienstleistungen

Dienste stellen Anwendungen auf einem Server dar. Während Dienste normalerweise mit virtuellen Servern kombiniert werden, kann ein Dienst in Ermangelung eines virtuellen Servers weiterhin anwendungsspezifischen Datenverkehr verwalten. Sie können beispielsweise einen HTTP-Dienst auf einer Citrix ADC Appliance erstellen, um eine Webserveranwendung darzustellen. Wenn der Client versucht, auf eine Website zuzugreifen, die auf dem Webserver gehostet wird, fängt die Appliance die HTTP-Anforderungen ab und erstellt eine transparente Verbindung mit dem Webserver.

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

Ein Service ist auch ein Punkt zum Anwenden von Features. Betrachten Sie das Beispiel der SSL-Beschleunigung. Um dieses Feature verwenden zu können, müssen Sie einen SSL-Dienst erstellen und ein SSL-Zertifikat an den Dienst binden. Wenn die Appliance eine HTTPS-Anforderung empfängt, entschlüsselt sie den Datenverkehr und sendet ihn im Klartext an den Server. Nur ein begrenzter Satz von Funktionen kann im Nur-Service-Fall konfiguriert werden.

Dienste verwenden Entitäten, die als Monitore bezeichnet werden, um den Zustand von Anwendungen zu verfolgen. Jeder Dienst verfügt über einen Standardmonitor, der auf dem Diensttyp basiert und an ihn gebunden ist. Wie in den auf dem Monitor konfigurierten Einstellungen angegeben, sendet die Appliance in regelmäßigen Abständen Prüfpunkte an die Anwendung, um ihren Status zu bestimmen. Wenn die Prüfpunkte fehlschlagen, markiert die Appliance den Dienst als ausgefallen. In solchen Fällen reagiert die Appliance auf Clientanforderungen mit einer entsprechenden Fehlermeldung oder leitet die Anforderung gemäß den konfigurierten Lastenausgleichsrichtlinien erneut weiter.

Einführung in die Citrix ADC Produktlinie

October 5, 2021

Die Citrix ADC Produktlinie optimiert die Bereitstellung von Anwendungen über das Internet und private Netzwerke und kombiniert Sicherheit, Optimierung und Datenverkehrsmanagement auf Anwendungsebene zu einer einzigen, integrierten Appliance. Sie können eine Citrix ADC Appliance in Ihrem Serverraum installieren und alle Verbindungen an die verwalteten Server weiterleiten. Die von Ihnen aktivierten Citrix ADC Funktionen und die von Ihnen festgelegten Richtlinien werden dann auf eingehenden und ausgehenden Datenverkehr angewendet.

Eine Citrix ADC Appliance kann als Ergänzung zu vorhandenen Load Balancern, Servern, Caches und Firewalls in jedes Netzwerk integriert werden. Es erfordert keine zusätzliche Client- oder serverseitige

Software und kann mit den webbasierten GUI- und CLI-Konfigurationsdienstprogrammen von Citrix ADC konfiguriert werden.

Dieses Artikel enthält die folgenden Abschnitte:

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

Citrix ADC Hardwareplattformen

Citrix ADC Hardware ist auf einer Vielzahl von Plattformen verfügbar, die eine Reihe von Hardware-spezifikationen aufweisen:

Citrix ADC MPX-Hardwareplattform

Citrix ADC SDX Hardwareplattform

Citrix ADC Editionen

Das Citrix ADC Betriebssystem ist in drei Editionen verfügbar:

- Standard
- Erweitert
- Premium

Die Standard und Advanced Edition verfügen über eingeschränkte Funktionen. Funktionslizenzen sind für alle Editionen erforderlich.

Weitere Informationen zu Citrix ADC Software-Editionen finden Sie im Datenblatt Citrix ADC Editions.

Informationen zum Abrufen und Installieren von Lizenzen finden Sie unter Lizenzierung.

Unterstützte Versionen auf Citrix ADC Hardware

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

Citrix ADC MPX Hardware-Software-Kompatibilitätsmatrix

Citrix ADC SDX Hardware-Software-Kompatibilitätsmatrix

Unterstützte Browser

Um auf die Citrix ADC GUI zuzugreifen, muss Ihre Workstation über einen unterstützten Webbrowser verfügen.

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

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

Die folgenden Browserversionen für Citrix ADC 11.1 lauten:

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

Installieren der Hardware

October 5, 2021

Überprüfen Sie vor der Installation einer Citrix ADC Appliance die Checkliste vor der Installation.

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

Aufgabe

Beschreibung

1. Lesen Sie Sicherheit, Warnhinweise, Warnungen und andere Informationen

   Lesen Sie die Warn- und Gefahreninformationen, die Sie wissen müssen, bevor Sie das Produkt installieren.

2. Vorbereitung für die Installation

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

3. Installieren der Hardware

   Montieren Sie die Appliance im Rack, installieren Sie Transceiver (falls verfügbar), und schließen Sie die Appliance an das Netzwerk und eine Stromquelle an.

4. Konfigurieren Sie die Appliance.

   Konfigurieren Sie die Anfangseinstellungen der Citrix ADC Appliance mithilfe der grafischen Benutzeroberfläche oder der seriellen Konsole.

   Führen Sie die Schritte in den folgenden Dokumentationen aus, um diese Aufgaben auszuführen:

   - Citrix ADC MPX-Hardwaredokumentation
   - Citrix ADC SDX-Hardwaredokumentation

Zugriff auf eine Citrix ADC Appliance

October 5, 2021

Eine Citrix ADC Appliance verfügt sowohl über eine Befehlszeilenschnittstelle (CLI) als auch über eine GUI. Die GUI enthält ein Konfigurationsdienstprogramm für die Konfiguration der Appliance und ein statistisches Dienstprogramm namens Dashboard. Für den ersten Zugriff werden alle Appliances mit der standardmäßigen Citrix ADC IP-Adresse (NSIP) von 192.168.100.1 und der Standard-Subnetzmaske von 255.255.0.0 ausgeliefert. Sie können während der Erstkonfiguration einen neuen NSIP und eine zugeordnete Subnetzmaske zuweisen.

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

- Haben Sie einen NSIP ausgewählt, bei dem es sich um eine IP-Adresse handelt, die bereits einem anderen Gerät in Ihrem Netzwerk zugewiesen ist?
- Haben Sie denselben NSIP mehreren Citrix ADC Appliances zugewiesen?
- Das NSIP ist auf allen physischen Ports erreichbar. Bei den Ports eines Citrix ADC handelt es sich um Hostports, nicht um Switch-Ports.

In der folgenden Tabelle werden die verfügbaren Zugriffsmethoden zusammengefasst.

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

Befehlszeilenschnittstelle

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

Melden Sie sich über den Konsolenport an der Befehlszeilenschnittstelle an

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

Gehen Sie folgendermaßen vor, um sich über den Konsolenport an der CLI anzumelden:

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

Melden Sie sich mit SSH an der Befehlszeilenschnittstelle an

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

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

- PuTTY

  Open-Source-Software, die auf mehreren Plattformen unterstützt wird. Verfügbar unter:

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

- Vandyke Software SecureCRT

  Kommerzielle Software, die auf der Windows-Plattform unterstützt wird. Verfügbar unter:

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

Diese Programme werden vom Citrix ADC -Team getestet, das überprüft hat, dass sie ordnungsgemäß mit einer Citrix ADC Appliance funktionieren. Andere Programme könnten auch korrekt funktionieren, wurden jedoch nicht getestet.

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

Gehen Sie folgendermaßen vor, um sich mit einem SSH-Client bei einer Citrix ADC Appliance anzumelden:

1. Starten Sie auf Ihrer Workstation den SSH-Client.
2. Verwenden Sie für die Erstkonfiguration die Standard-IP-Adresse (NSIP), die 192.168.100.1 ist. Verwenden Sie für den nachfolgenden Zugriff das NSIP, das während der Erstkonfiguration zugewiesen wurde. Wählen Sie entweder SSH1 oder SSH2 als Protokoll aus.
3. Geben Sie unter Benutzername ein `nsroot`. Geben Sie unter Password ein `nsroot` und wenn dieses Kennwort nicht funktioniert, geben Sie die Seriennummer der Appliance ein. Der Seriennummern-Barcode ist auf der Rückseite der Appliance verfügbar. Zum Beispiel.

```
login as: nsroot

Using keyboard-interactive authentication.

Password:

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




Done

>

<!--NeedCopy-->
```


Citrix ADC Benutzeroberfläche

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

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

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

Die GUI enthält ein Konfigurationsdienstprogramm und ein statistisches Dienstprogramm namens Dashboard, auf das Sie über eine Workstation zugreifen, die mit einem Ethernet-Port der Appliance verbunden ist.

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

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

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

Die folgenden Browser werden unterstützt.

Betriebssystem: Windows 7

Browser: Internet Explorer (Version 9, 10 und 11), Mozilla Firefox (Version 3.6.25 und höher), Google Chrome (neueste).

Betriebssystem: Windows 64 Bit

Browser: Internet Explorer (Version 8, 9, 10 und 11), Google Chrome (neueste Version)

Betriebssystem:
MAC-Browser : Mozilla Firefox (Version 3.6.25 und höher), Safari (Version 5.1.3 und höher), Google Chrome (neueste Version)

Verwenden der Citrix ADC GUI

Nachdem Sie sich am Konfigurationsdienstprogramm angemeldet haben, können Sie die Appliance über eine grafische Oberfläche konfigurieren, die kontextbezogene Hilfe enthält.

Gehen Sie folgendermaßen vor, um sich an der GUI anzumelden:

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

   Hinweis: Wenn Sie zwei Citrix ADC Appliances in einem Hochverfügbarkeitssetup haben, greifen Sie nicht auf die GUI zu, indem Sie die IP-Adresse der sekundären Citrix ADC Appliance eingeben. Wenn Sie dies tun und die GUI zum Konfigurieren der sekundären Appliance verwenden, werden Ihre Konfigurationsänderungen nicht auf die primäre Citrix ADC Appliance angewendet.

2. Geben Sie im Textfeld Benutzername ein `nsroot`.
3. Geben Sie im Textfeld Kennwort das Administratorkennwort ein, das Sie dem `nsroot` Konto während der Erstkonfiguration zugewiesen haben, und klicken Sie auf **Anmelden**. Wenn dieses Kennwort nicht funktioniert, geben Sie die Seriennummer der Appliance ein. Der Seriennummern-Barcode ist auf der Rückseite der Appliance verfügbar.

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

Verwenden des Statistischen Dienstprogramms

Dashboard, das Statistikdienstprogramm, ist eine browserbasierte Anwendung, die Diagramme und Tabellen anzeigt, in denen Sie die Leistung einer Citrix ADC Appliance überwachen können.

Gehen Sie folgendermaßen vor, um sich beim Dashboard anzumelden:

1. Öffnen Sie Ihren Webbrowser und geben Sie den NSIP als HTTP-Adresse ein. Die Seite Citrix Anmeldung wird angezeigt.
2. Geben Sie im Textfeld Benutzername ein `nsroot`.
3. Geben Sie im Textfeld Kennwort das Administratorkennwort ein, das Sie dem `nsroot` Konto bei der Erstkonfiguration zugewiesen haben. Wenn dieses Kennwort nicht funktioniert, geben Sie die Seriennummer der Appliance ein. Der Seriennummern-Barcode ist auf der Rückseite der Appliance verfügbar.

Erstkonfiguration von ADC

October 5, 2021

Informationen zur Erstkonfiguration einer Citrix ADC MPX-Appliance finden Sie unter Erstkonfiguration einer Citrix MPX-Appliance.

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

NITRO API

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

Sichern der Citrix ADC-Bereitstellung

October 8, 2021

Um die Sicherheit über den Bereitstellungslebenszyklus der Citrix ADC Appliance aufrechtzuerhalten, empfiehlt Citrix, die folgenden Sicherheitsaspekte zu berücksichtigen:

- Physische Sicherheit
- Appliance-Sicherheit
- Netzwerksicherheit
- Verwaltung und Verwaltung

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

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

Konfigurieren der Hochverfügbarkeit

October 5, 2021

Sie können zwei Citrix ADC Appliances in einer Hochverfügbarkeitskonfiguration bereitstellen, wobei eine Einheit aktiv Verbindungen akzeptiert und Server verwaltet, während die sekundäre Einheit die

erste überwacht. Die Citrix ADC Appliance, die aktiv Verbindungen akzeptiert und die Server verwaltet, wird als primäre Einheit bezeichnet und die andere als sekundäre Einheit in einer Hochverfügbarkeitskonfiguration bezeichnet. Wenn in der primären Einheit ein Fehler auftritt, wird die sekundäre Einheit zur primären Einheit und beginnt aktiv, Verbindungen zu akzeptieren.

Jede Citrix ADC Appliance in einem Hochverfügbarkeitspaar überwacht die andere durch das Senden periodischer Nachrichten, sogenannte Heartbeat-Nachrichten oder Zustandsprüfungen, um den Zustand oder den Status des Peer-Knotens zu bestimmen. Wenn eine Zustandsprüfung für eine primäre Einheit fehlschlägt, versucht die sekundäre Einheit die Verbindung für einen bestimmten Zeitraum erneut. Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit. Wenn ein Wiederholungsversuch bis zum Ende des angegebenen Zeitraums nicht erfolgreich ist, übernimmt die sekundäre Einheit für die primäre Einheit in einem Prozess namens Failover. Die folgende Abbildung zeigt zwei Hochverfügbarkeitskonfigurationen, eine im Einarmmodus und die andere im Zweiarmmodus.

Abbildung 1. Hohe Verfügbarkeit im Einarmmodus

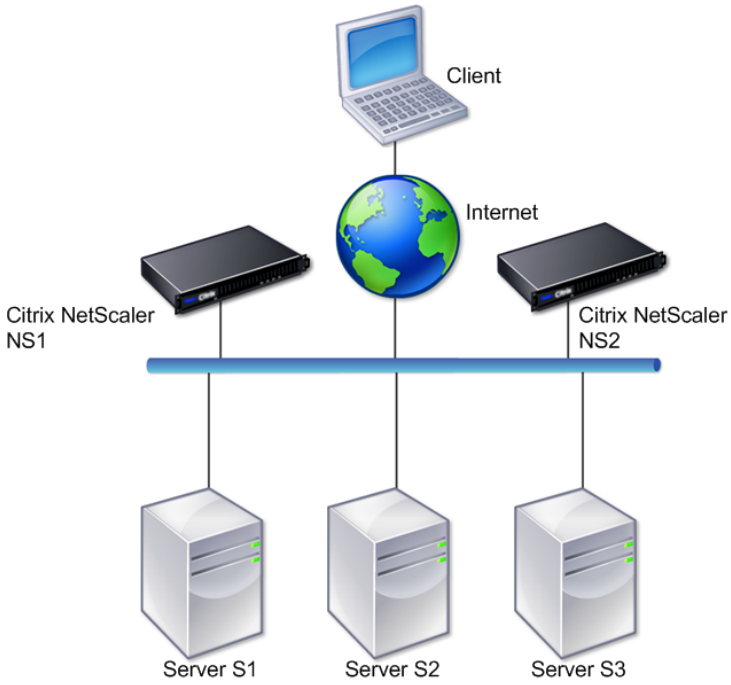
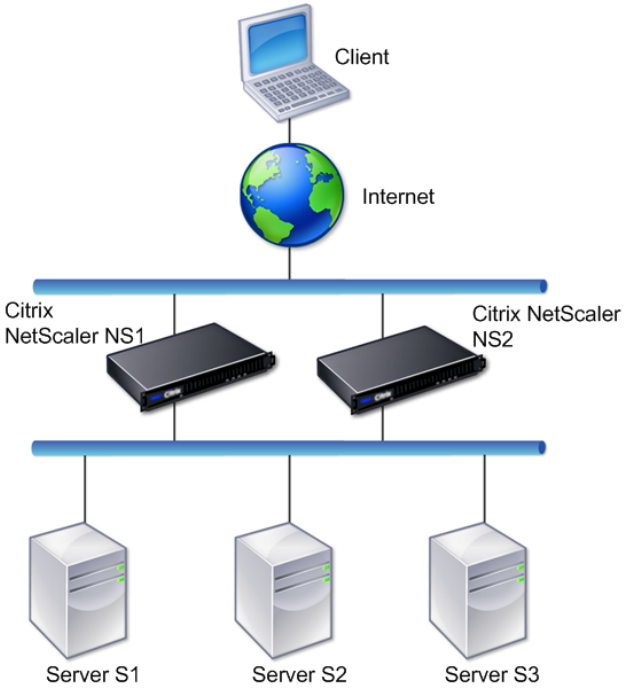


Abbildung 2. Hohe Verfügbarkeit im Zweiarm-Modus



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

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

Um eine Hochverfügbarkeitsumgebung einzurichten, konfigurieren Sie eine ADC-Appliance als primäre und eine andere als sekundäre. Führen Sie die folgenden Aufgaben für jede der ADC-Appliances aus:

- Fügen Sie einen Knoten hinzu.
- Deaktivieren Sie die Überwachung der Hochverfügbarkeit für nicht verwendete Schnittstellen.

Hinzufügen eines Knotens

Ein Knoten ist eine logische Darstellung einer Peer-Citrix ADC Appliance. Es identifiziert die Peer-Einheit nach ID und NSIP. Eine Appliance verwendet diese Parameter, um mit dem Peer zu kommunizieren und seinen Status zu verfolgen. Wenn Sie einen Knoten hinzufügen, tauschen die primären und sekundären Einheiten die Heartbeat-Nachrichten asynchron aus. Die Knoten-ID ist eine ganze Zahl, die nicht größer als 64 sein darf.

Über CLI

Gehen Sie folgendermaßen vor, um einen Knoten über die Befehlszeile hinzuzufügen:

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

- add HA node <id> <IPAddress>
- <id>HA-Knoten anzeigen

  Beispiel

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

Über GUI

Gehen Sie folgendermaßen vor, um einen Knoten über die GUI hinzuzufügen:

1. Navigieren Sie zu **System** > **Hochverfügbarkeit** .
2. Klicken Sie auf der Registerkarte **Knoten** auf **Hinzufügen** .
3. Geben Sie auf der Seite **HA-Knoten erstellen** im Textfeld **Remote-Knoten-IP-Adresse** die NSIP-Adresse (z. B. 10.102.29.170) des Remote-Knotens ein.
4. Stellen Sie sicher, dass das Kontrollkästchen **Remote-System für die Teilnahme an Hochverfügbarkeit-Setup konfigurieren** aktiviert ist. Geben Sie die Anmeldeinformationen des Remoteknotens in den Textfeldern unter **Anmeldeinformationen des Remote-Systems ein**.
5. Aktivieren Sie das Kontrollkästchen **HA-Monitor auf ausgeschalteten Schnittstellen/Kanälen deaktivieren,** um den HA-Monitor auf heruntergeschalteten Schnittstellen zu deaktivieren.

Stellen Sie sicher, dass der hinzugefügte Knoten in der Liste der Knoten auf der Registerkarte Knoten angezeigt wird.

Deaktivieren der Überwachung der Hochverfügbarkeit für nicht verwendete Schnittstellen

Der Hochverfügbarkeitsmonitor ist eine virtuelle Entität, die eine Schnittstelle überwacht. Sie müssen den Monitor für Schnittstellen deaktivieren, die nicht verbunden sind oder für den Datenverkehr verwendet werden. Wenn der Monitor auf einer Schnittstelle aktiviert ist, deren Status DOWN ist, wird der Status des Knotens NOT UP. In einer Hochverfügbarkeitskonfiguration kann ein primärer Knoten, der in den Status NOT UP eintritt, zu einem Hochverfügbarkeits-Failover führen. Eine Schnittstelle wird unter folgenden Bedingungen als DOWN gekennzeichnet:

- Die Schnittstelle ist nicht verbunden
- Die Schnittstelle funktioniert nicht ordnungsgemäß
- Das Kabel, das die Schnittstelle verbindet, funktioniert nicht ordnungsgemäß

Über CLI

Gehen Sie folgendermaßen vor, um den Hochverfügbarkeitsmonitor für eine nicht verwendete Schnittstelle über die Befehlszeile zu deaktivieren:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den Hochverfügbarkeitsmonitor für eine nicht verwendete Schnittstelle zu deaktivieren und zu überprüfen, ob sie deaktiviert ist:

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

  Beispiel

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

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


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

Über GUI

Gehen Sie folgendermaßen vor, um den Hochverfügbarkeitsmonitor für nicht verwendete Schnittstellen über die GUI zu deaktivieren:

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

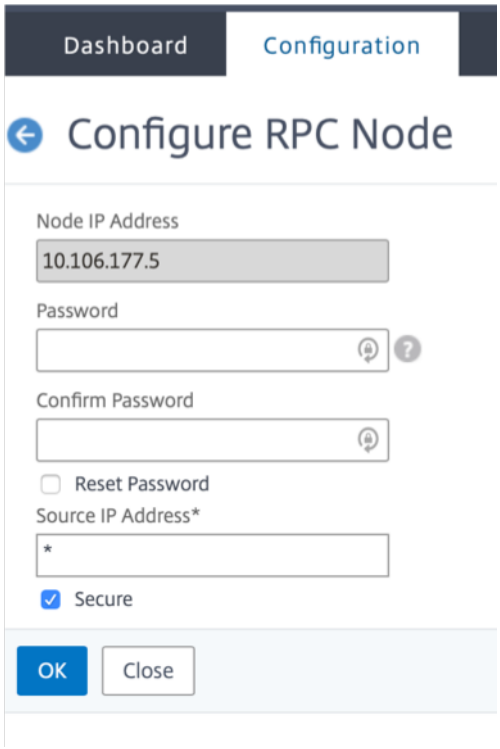
Ändern eines RPC-Knotenkennworts

October 5, 2021

Für die Kommunikation mit anderen Citrix ADC Appliances benötigt jede Appliance Kenntnisse über die anderen Appliances, einschließlich der Authentifizierung auf der Citrix ADC-Appliance. RPC-Knoten sind interne Systementitäten, die für die System-zu-System-Kommunikation von Konfigurations- und Sitzungsinformationen verwendet werden. Auf jeder Citrix ADC Appliance ist ein RPC-Knoten vorhanden und speichert Informationen wie die IP-Adressen der anderen Citrix ADC-Appliance und die für die Authentifizierung verwendeten Kennwörter. Die Citrix ADC Appliance, die die andere Citrix ADC Appliance kontaktiert, überprüft das Kennwort im RPC-Knoten.

So ändern Sie ein RPC-Knotenkennwort über die GUI

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



5. Wählen Sie **Sichern** aus, und klicken Sie dann auf **OK** .

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

So ändern Sie ein RPC-Knotenkennwort über die CLI

Geben Sie in der Befehlszeile die folgenden Befehle ein:

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

Beispiel:


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

<!--NeedCopy-->
```

Konfigurieren Sie zum ersten Mal eine FIPS-Appliance

December 3, 2021

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

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

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

Konfigurieren Sie sicheres HTTPS mithilfe der CLI

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

1. Initialisieren Sie das Hardwaresicherheitsmodul (HSM) auf der FIPS-Karte der Appliance. Informationen zum Initialisieren des HSM finden Sie unter Konfigurieren des HSM.
2. Wenn die Appliance Teil eines Hochverfügbarkeitssetups ist, aktivieren Sie die SIM. Informationen zum Aktivieren der SIM auf den primären und sekundären Appliances finden Sie unter Konfigurieren von FIPS-Appliances in einem Hochverfügbarkeits-Setup.
3. Importieren Sie den FIPS-Schlüssel in das HSM der FIPS-Karte der Appliance. Geben Sie an der Eingabeaufforderung Folgendes ein:

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

4. Fügen Sie ein Zertifikatsschlüsselpaar hinzu. Geben Sie an der Eingabeaufforderung Folgendes ein:

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

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

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

   ```
   bind ssl service nshttps-::11-443 -certkeyname server
   ```

Konfigurieren Sie sicheres HTTPS mithilfe der GUI

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

1. Initialisieren Sie das Hardwaresicherheitsmodul (HSM) auf der FIPS-Karte der Appliance. Informationen zum Initialisieren des HSM finden Sie unter Konfigurieren des HSM.
2. Wenn die Appliance Teil eines Hochverfügbarkeitssetups ist, aktivieren Sie das Secure Information System (SIM). Informationen zum Aktivieren der SIM auf den primären und sekundären Appliances finden Sie unter Konfigurieren von FIPS-Appliances in einem Hochverfügbarkeits-Setup.
3. Importieren Sie den FIPS-Schlüssel in das HSM der FIPS-Karte der Appliance. Weitere Informationen zum Importieren eines FIPS-Schlüssels finden Sie im Abschnitt Importieren eines vorhandenen FIPS-Schlüssels .
4. Navigieren Sie zu **Traffic Management > SSL > Zertifikate**.
5. Klicken Sie im Detailbereich auf Installieren.
6. Geben Sie im Dialogfeld Zertifikat installieren die Zertifikatsdetails ein.
7. Klicken Sie auf Erstellen und dann auf Schließen.
8. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
9. Klicken Sie im Detailbereich auf der Registerkarte Aktion auf Interne Dienste.

10. Wählen Sie `nshttps-127.0.0.1-443` aus der Liste aus, und klicken Sie dann auf Öffnen.
11. Wählen Sie auf der Registerkarte SSL-Einstellungen im Bereich Verfügbar das in Schritt 7 erstellte Zertifikat aus, klicken Sie auf Hinzufügen, und klicken Sie dann auf OK.
12. Wählen Sie `nshttps-::1l-443` aus der Liste aus, und klicken Sie dann auf Öffnen.
13. Wählen Sie auf der Registerkarte SSL-Einstellungen im Bereich Verfügbar das in Schritt 7 erstellte Zertifikat aus, klicken Sie auf Hinzufügen, und klicken Sie dann auf OK.
14. Klicken Sie auf OK.

Konfigurieren von sicherem RPC mithilfe der CLI

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

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

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

4. Fügen Sie ein Zertifikatsschlüsselpaar hinzu. Geben Sie an der Eingabeaufforderung Folgendes ein:

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

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

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

   ```
   bind ssl service nskrpcs-127.0.0.1-3009 -certkeyname server
   ```

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

6. Aktivieren Sie den sicheren RPC-Modus. Geben Sie an der Eingabeaufforderung Folgendes ein:

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

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

Konfigurieren Sie sicheren RPC über die GUI

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

1. Initialisieren Sie das Hardwaresicherheitsmodul (HSM) auf der FIPS-Karte der Appliance. Informationen zum Initialisieren des HSM finden Sie unter Konfigurieren des HSM.
2. Aktivieren Sie das sichere Informationssystem (SIM). Informationen zum Aktivieren der SIM auf den primären und sekundären Appliances finden Sie unter Konfigurieren Sie FIPS-Appliances in einem Hochverfügbarkeits-Setup.
3. Importieren Sie den FIPS-Schlüssel in das HSM der FIPS-Karte der Appliance. Weitere Informationen zum Importieren eines FIPS-Schlüssels finden Sie im Abschnitt Bestehenden FIPS-Schlüssel importieren .
4. Navigieren Sie zu **Traffic Management > SSL > Zertifikate**.
5. Klicken Sie im Detailbereich auf Installieren.
6. Geben Sie im Dialogfeld Zertifikat installieren die Zertifikatsdetails ein.
7. Klicken Sie auf Erstellen und dann auf Schließen.
8. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
9. Klicken Sie im Detailbereich auf der Registerkarte Aktion auf Interne Dienste.
10. Wählen Sie `nsrpcs-127.0.0.1-3008` aus der Liste aus, und klicken Sie dann auf Öffnen.
11. Wählen Sie auf der Registerkarte SSL-Einstellungen im Bereich Verfügbar das in Schritt 7 erstellte Zertifikat aus, klicken Sie auf Hinzufügen, und klicken Sie dann auf OK.
12. Wählen Sie `nskrpcs-127.0.0.1-3009` aus der Liste aus, und klicken Sie dann auf Öffnen.
13. Wählen Sie auf der Registerkarte SSL-Einstellungen im Bereich Verfügbar das in Schritt 7 erstellte Zertifikat aus, klicken Sie auf Hinzufügen, und klicken Sie dann auf OK.
14. Wählen Sie `nsrpcs-::11-3008` aus der Liste aus, und klicken Sie dann auf Öffnen.
15. Wählen Sie auf der Registerkarte SSL-Einstellungen im Bereich Verfügbar das in Schritt 7 erstellte Zertifikat aus, klicken Sie auf Hinzufügen, und klicken Sie dann auf OK.
16. Klicken Sie auf OK.
17. Navigieren Sie zu **System > Netzwerk > RPC**.
18. Wählen Sie im Detailbereich die IP-Adresse aus, und klicken Sie auf Öffnen.
19. Wählen Sie im Dialogfeld RPC-Knoten konfigurieren die Option Sicher aus.
20. Klicken Sie auf OK.

Gemeinsame Netzwerktopologien

October 5, 2021

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

sich um den gebräuchlichsten Bereitstellungstyp handelt.

Einrichten einer gemeinsamen Zweiarm-Topologie

In einer Zweiarm-Topologie ist eine Netzwerkschnittstelle mit dem Clientnetzwerk verbunden und eine andere Netzwerkschnittstelle mit dem Servernetzwerk verbunden, wodurch sichergestellt wird, dass der gesamte Datenverkehr durch die Appliance fließt. Diese Topologie erfordert möglicherweise eine erneute Verbindung der Hardware und kann auch zu einer vorübergehenden Ausfallzeit führen. Die grundlegenden Varianten der Zweiarm-Topologie sind mehrere Subnetze, in der Regel mit der Appliance in einem öffentlichen Subnetz und den Servern in einem privaten Subnetz und im transparenten Modus, sowohl mit der Appliance als auch mit den Servern im öffentlichen Netzwerk.

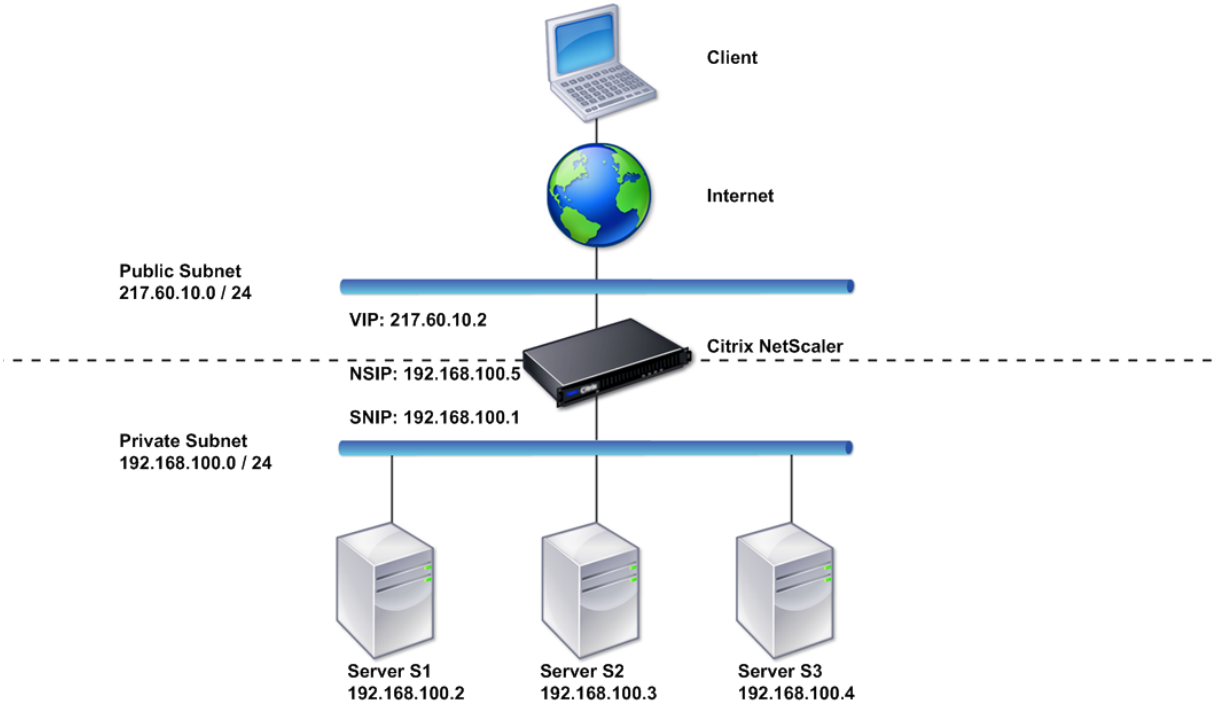
Einrichten einer einfachen Zweiarm-Topologie mit mehreren Subnetzen

Eine der am häufigsten verwendeten Topologien verfügt über die Citrix ADC Appliance zwischen den Clients und den Servern, wobei ein virtueller Server für die Verarbeitung der Clientanforderungen konfiguriert ist. Diese Konfiguration wird verwendet, wenn sich die Clients und Server in verschiedenen Subnetzen befinden. In den meisten Fällen befinden sich die Clients und Server in öffentlichen bzw. privaten Subnetzen.

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

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

Abbildung 1. Topologiediagramm für Zweiarm-Modus, mehrere Subnetze



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

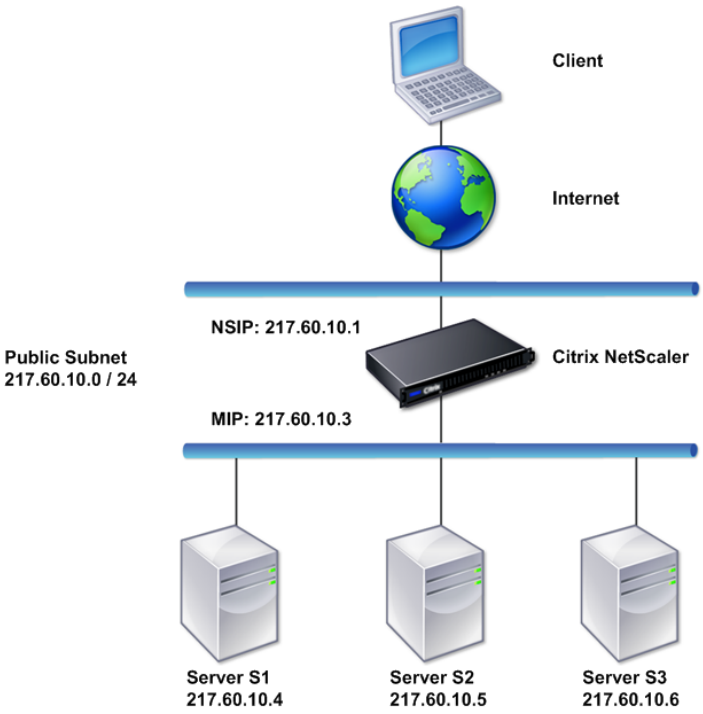
1. Konfigurieren Sie den NSIP und das Standardgateway, wie unter Konfigurieren der NetScaler IP-Adresse (NSIP)beschrieben.
2. Konfigurieren Sie den SNIP, wie unter Subnetz-IP-Adressen konfigurierenbeschrieben.
3. Aktivieren Sie die USNIP-Option, wie im Abschnitt So aktivieren oder deaktivieren Sie den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

Einrichten einer einfachen transparenten Zweiarm-Topologie

Verwenden Sie den transparenten Modus, wenn die Clients direkt auf die Server zugreifen müssen, ohne dass ein virtueller Server vorhanden ist. Die Server-IP-Adressen müssen öffentlich sein, da die Clients darauf zugreifen können müssen. In dem Beispiel in der folgenden Abbildung wird eine Citrix ADC Appliance zwischen dem Client und dem Server platziert, sodass der Datenverkehr durch die Ap-

pliance geleitet werden muss. Sie müssen den L2-Modus aktivieren, um die Pakete zu überbrücken. NSIP und MIP befinden sich im selben öffentlichen Subnetz, 217.60.10.0/24.

Abbildung 2. Topologiediagramm für zweiarmige, transparente Modus



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

1. Konfigurieren Sie den NSIP und das Standardgateway, wie unter Konfigurieren der NetScaler IP-Adresse (NSIP)beschrieben.
2. Aktivieren Sie den L2-Modus, wie im Layer-2-Modus aktivieren unddeaktivieren beschrieben.
3. Konfigurieren Sie das Standard-Gateway der verwalteten Server als MIP.
4. Verbinden Sie die Netzwerkschnittstellen mit den entsprechenden Ports am Switch.

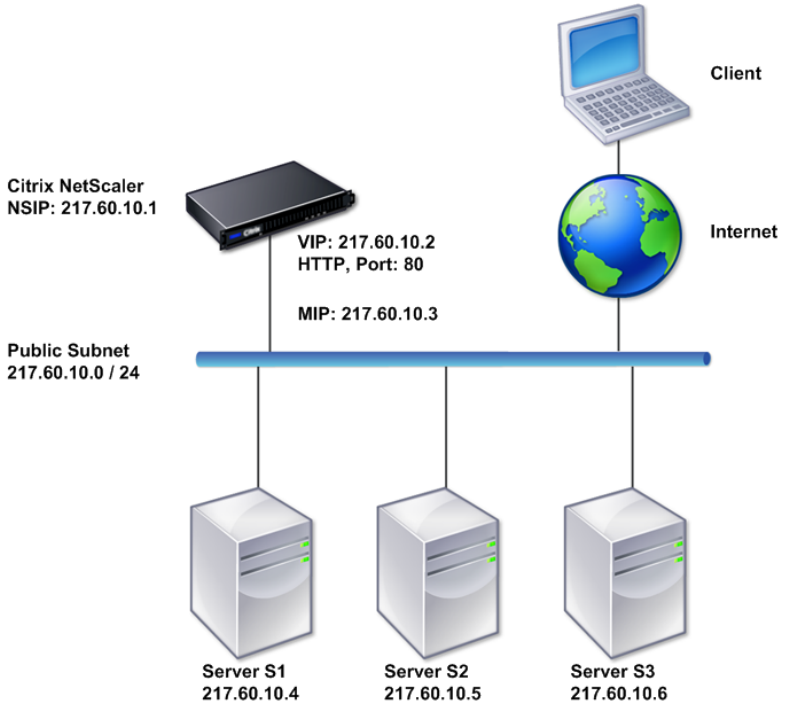
Ein-arm-Topologien einrichten

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

Einrichten einer einfachen Einarm-Topologie für einzelne Subnetze

Sie können eine Einarm-Topologie mit einem einzelnen Subnetz verwenden, wenn sich die Clients und Server im selben Subnetz befinden. Betrachten Sie beispielsweise eine Citrix ADC Appliance, die im Einarmmodus zur Verwaltung der Server S1, S2 und S3 bereitgestellt wird. Ein virtueller Server vom Typ HTTP wird auf einer ADC-Appliance konfiguriert, und HTTP-Dienste werden auf den Servern ausgeführt. Wie in der folgenden Abbildung gezeigt, befinden sich die Citrix ADC IP-Adresse (NSIP), die zugeordnete IP-Adresse (MIP) und die Server-IP-Adressen im selben öffentlichen Subnetz 217.60.10.0/24.

Abbildung 3. Topologiediagramm für Einarmmodus, Einzelsubnetz



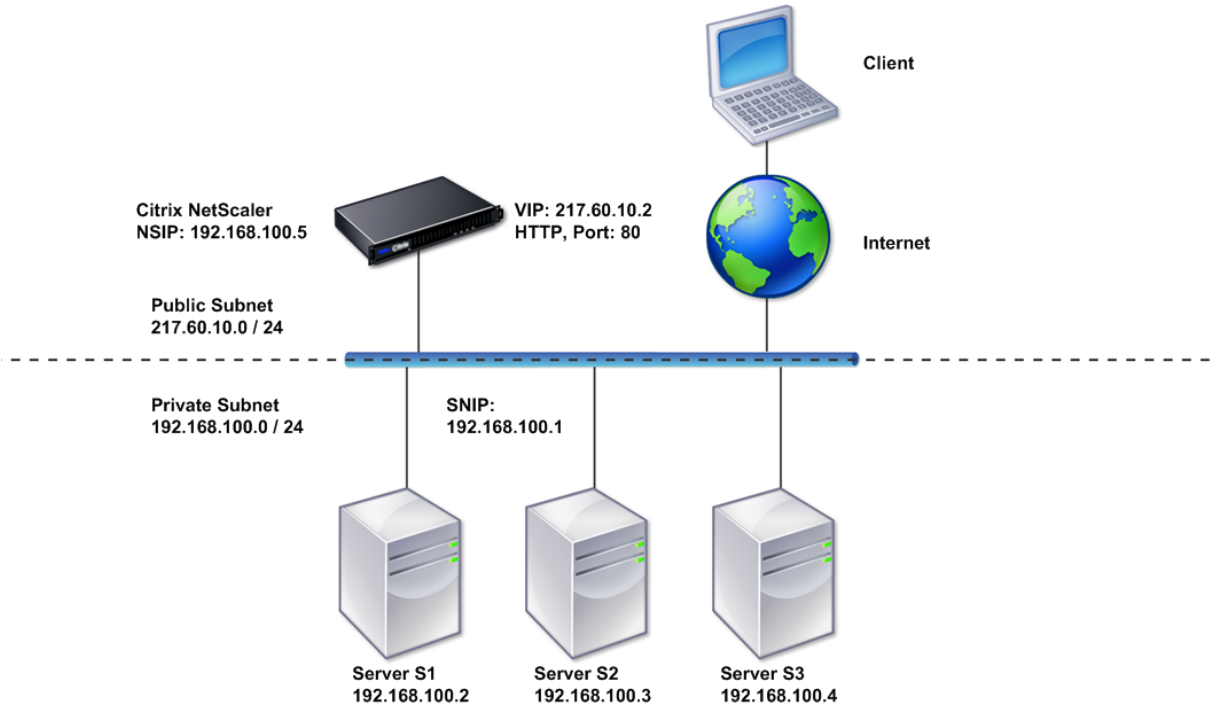
Gehen Sie folgendermaßen vor, um eine Citrix ADC Appliance im Einarmmodus mit einem einzelnen Subnetz bereitzustellen:

1. Konfigurieren Sie den NSIP und das Standardgateway wie unter Konfigurieren der Citrix ADC IP-Adresse (NSIP)beschrieben.
2. Konfigurieren Sie den virtuellen Server und die Dienste, wie im Abschnitt Erstellen eines virtuellen Servers und im Abschnitt Dienste konfigurieren beschrieben.
3. Verbinden Sie eine der Netzwerkschnittstellen mit dem Switch.

Einrichten einer einfachen Mehrfachsubnetz-Topologie mit mehreren Armen

Sie können eine Einarm-Topologie mit mehreren Subnetzen verwenden, wenn sich die Clients und Server in den verschiedenen Subnetzen befinden. Betrachten Sie beispielsweise eine Citrix ADC Appliance, die im Einarmmodus zur Verwaltung der Server S1, S2 und S3 bereitgestellt wird, wobei die Server mit Switch SW1 im Netzwerk verbunden sind. Ein virtueller Server vom Typ HTTP wird auf der Appliance konfiguriert, und HTTP-Dienste werden auf den Servern ausgeführt. Diese drei Server befinden sich im privaten Subnetz, daher ist eine Subnetz-IP-Adresse (SNIP) für die Kommunikation mit ihnen konfiguriert. Die Option Subnetz-IP-Adresse (USNIP) verwenden muss aktiviert sein, damit die Appliance die SNIP anstelle einer MIP verwendet. Wie in der folgenden Abbildung gezeigt, befindet sich die virtuelle IP-Adresse (VIP) im öffentlichen Subnetz 217.60.10.0/24; die NSIP-, SNIP- und die Server-IP-Adressen befinden sich im privaten Subnetz 192.168.100.0/24.

Abbildung 4. Topologiediagramm für Einarmmodus, mehrere Subnetze



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

1. Konfigurieren Sie den NSIP und das Standardgateway, wie unter Konfigurieren der NetScaler IP-Adresse (NSIP)beschrieben.
2. Konfigurieren Sie das SNIP und aktivieren Sie die USNIP-Option, wie unter Subnetz-IP-Adressen

konfigurierenbeschrieben.

3. Konfigurieren Sie den virtuellen Server und die Dienste, wie im Abschnitt Erstellen eines virtuellen Servers und im Abschnitt Dienste konfigurieren beschrieben.
4. Verbinden Sie eine der Netzwerkschnittstellen mit dem Switch.

Systemverwaltungseinstellungen

October 5, 2021

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

Systemeinstellungen

October 5, 2021

Die Konfiguration der Systemeinstellungen umfasst grundlegende Aufgaben wie das Konfigurieren von HTTP-Ports zur Aktivierung der Keep-Alive und der Serverabladung, das Festlegen der maximalen Anzahl von Verbindungen für jeden Server und das Festlegen der maximalen Anzahl von Anforderungen pro Verbindung. Sie können die Client-IP-Adresse in Situationen aktivieren, in denen eine Proxy-IP-Adresse nicht geeignet ist, und Sie können die HTTP-Cookie-Version ändern.

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

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

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

Parametertyp: HTTP-Port-Informationen

Gibt an: Die HTTP-Ports des Webservers, die von den verwalteten Servern verwendet werden. Wenn Sie die Ports angeben, führt die Appliance die Anforderungsumschaltung für jede Clientanforderung durch, die über einen Zielport verfügt, der mit einem angegebenen Port übereinstimmt.

> Hinweis: Wenn eine eingehende Clientanforderung nicht für einen Dienst oder einen virtuellen Server bestimmt ist, der speziell auf der Appliance konfiguriert ist, muss der Zielport in der Anforderung mit einem der global konfigurierten HTTP-Ports übereinstimmen. Dies ermöglicht es der Appliance, die Keep-Alive-Verbindung und die Serverentlastung durchzuführen.

Parameterart: Grenzwerte

Gibt an: Die maximale Anzahl von Verbindungen zu jedem verwalteten Server und die maximale Anzahl von Anforderungen, die über jede Verbindung gesendet werden. Wenn Sie z. B. Max Connections auf 500 festlegen und die Appliance drei Server verwaltet, können maximal 500 Verbindungen zu jedem der drei Server geöffnet werden. Standardmäßig kann die Appliance eine unbegrenzte Anzahl von Verbindungen zu einem der von ihr verwalteten Server erstellen. Um eine unbegrenzte Anzahl von Anforderungen pro Verbindung anzugeben, setzen Sie Max. Anforderungen auf 0.

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

Parametertyp: Client-IP-Einfügung

Gibt an: Einfügen der IP-Adresse des Clients in den HTTP-Request-Header aktivieren/deaktivieren. Sie können einen Namen für das Kopfzeilenfeld im angrenzenden Textfeld angeben. Wenn ein von einer Appliance verwalteter Webserver eine Subnetz-IP-Adresse erhält, identifiziert der Server diese als IP-Adresse des Clients. Einige Anwendungen benötigen die IP-Adresse des Clients für Protokollierungszwecke oder zur dynamischen Bestimmung des vom Webserver bereitzustellenden Inhalts.

Sie können das Einfügen der tatsächlichen Client-IP-Adresse in die HTTP-Header-Anforderung aktivieren, die vom Client an einen, einige oder alle Server gesendet wird, die von der Appliance verwaltet werden. Sie können dann auf die eingefügte Adresse durch eine geringfügige Änderung am Server zugreifen (über ein Apache-Modul, eine ISAPI-Schnittstelle oder eine NSAPI-Schnittstelle).

Parametertyp: Cookie-Version

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

Parameterart: Anforderungen/Antworten

Gibt an: Optionen für die Verarbeitung bestimmter Arten von Anforderungen und Aktivieren/Deaktivieren der Protokollierung von HTTP-Fehlerantworten.

Parametertyp: Einfügen von Serverkopfzeilen

Gibt an: Fügen Sie einen Server-Header in Citrix ADC-generierte HTTP-Antworten ein.

Gehen Sie folgendermaßen vor, um HTTP-Parameter über die GUI zu konfigurieren:

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

Gehen Sie folgendermaßen vor, um den FTP-Portbereich über die GUI festzulegen:

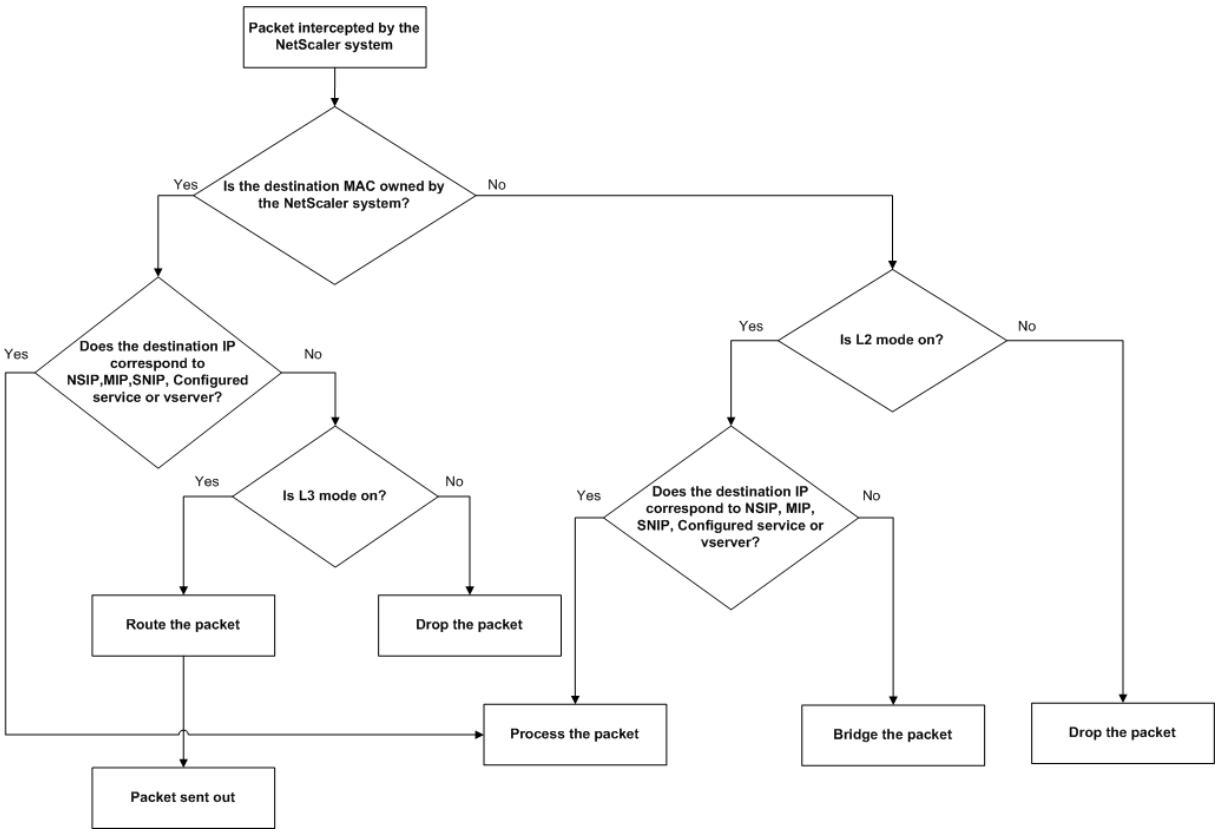
1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Globale Systemeinstellungen ändern**.
3. Geben Sie unter **FTP-Portbereich** in den Textfeldern **Startport** und **Endport** die niedrigste bzw.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

Paketweiterleitungsmodi

April 7, 2022

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

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



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

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

Layer-2-Modus aktivieren und deaktivieren

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

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

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

L2-Modus aktivieren.

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

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

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

Beispiele

```
1      > enable ns mode l2
2      Done
3      > show ns mode
4
5      Mode Acronym Status
6      ------- ------- ------
7      1) Fast Ramp FR ON
8      2) Layer 2 mode L2 ON
9      .
10     .
11     .
12     Done
13     >
14
15     > disable ns mode l2
16     Done
17     > show ns mode
18
19     Mode Acronym Status
20     ------- ------- ------
21     1) Fast Ramp FR ON
22     2) Layer 2 mode L2 OFF
23     .
24     .
25     .
26     Done
27     >
28 <!--NeedCopy-->
```

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

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

Layer-3-Modus aktivieren und deaktivieren

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

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

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

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

Beispiele

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

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



```
14      .
15      .
16      Done
17      >
18
19      > disable ns mode l3
20      Done
21      > show ns mode
22
23      Mode Acronym Status
24      ------- ------- ------
25      1) Fast Ramp FR ON
26      2) Layer 2 mode L2 OFF
27      .
28      .
29      .
30      9) Layer 3 mode (ip forwarding) L3 OFF
31      .
32      .
33      .
34      Done
35      >
36  <!--NeedCopy-->
```

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

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

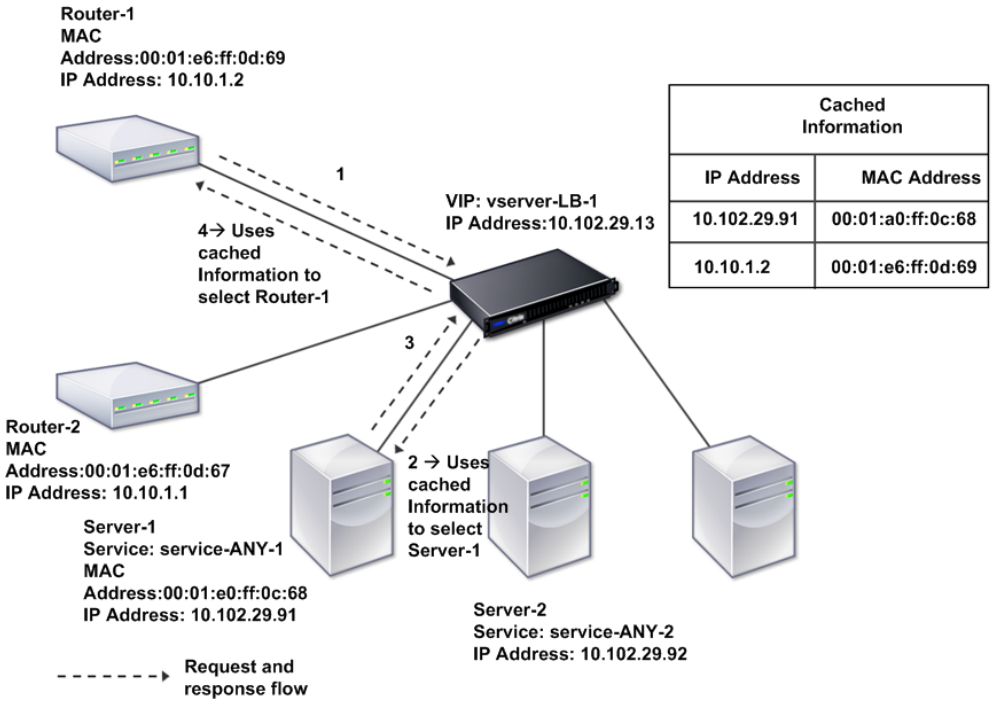
Mac-basierten Weiterleitungsmodus aktivieren und deaktivieren

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

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

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

Abbildung 2. Mac-basierter Weiterleitungsprozess



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

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

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

Bei einigen Bereitstellungen müssen die eingehenden und ausgehenden Pfade durch verschiedene Router fließen. In diesen Situationen bricht die MAC-basierte Weiterleitung das Topologiedesign. Für

einen Global Server Load Balancing (GSLB) -Site, bei dem die eingehenden und ausgehenden Pfade durch verschiedene Router fließen müssen, müssen Sie die MAC-basierte Weiterleitung deaktivieren und den Standardrouter der Appliance als ausgehenden Router verwenden.

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

Mac-basierte Weiterleitung mit der CLI aktivieren oder deaktivieren

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

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

  “‘ pre codeblock

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

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

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

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


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

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie im Detailbereich unter der Gruppe **Modi und Funktionen** auf **Modi konfigurieren**.
3. Um den MAC-basierten Weiterleitungsmodus zu aktivieren, aktivieren Sie im Dialogfeld **Modi konfigurieren** das Kontrollkästchen **MAC-basierte Weiterleitung**. Deaktivieren Sie das Kontrollkästchen, um den MAC-basierten Weiterleitungsmodus zu deaktivieren
4. Klicken Sie auf **OK**. Der **Aktivieren-/Deaktivierenmodus?** wird im Detailbereich angezeigt.
5. Klicken Sie auf **Ja**.

Netzwerkschnittstellen

October 5, 2021

Die Citrix ADC Schnittstellen sind in Slot-/Port-Notation nummeriert. Sie können nicht nur die Eigenschaften einzelner Schnittstellen ändern, sondern auch virtuelle LANs konfigurieren, um den Datenverkehr auf bestimmte Hostgruppen zu beschränken. Sie können Verbindungen auch zu Hochgeschwindigkeitskanälen zusammenfassen.

Virtuelle LANs

Die Citrix ADC Appliance unterstützt Port (Layer 2) und IEEE802.1Q-getaggte virtuelle LANs (VLANs). VLAN-Konfigurationen sind nützlich, wenn Sie den Verkehr auf bestimmte Gruppen von Stationen beschränken müssen. Sie können eine Netzwerkschnittstelle so konfigurieren, dass sie mehreren VLANs angehört, indem Sie IEEE 802.1q-Tagging verwenden.

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

Die Citrix ADC Appliance unterstützt die folgenden VLAN-Typen.

- Standard-VLAN

  Standardmäßig sind die Netzwerkschnittstellen einer Citrix ADC Appliance in einem einzigen, portbasierten VLAN als nicht getaggte Netzwerkschnittstellen enthalten. Dieses Standard-VLAN hat eine VID von 1 und ist dauerhaft vorhanden. Es kann nicht gelöscht werden und seine VID kann nicht geändert werden.

- Port-basierte VLANs

Eine Reihe von Netzwerkschnittstellen, die eine gemeinsame, exklusive Layer-2-Broadcastdomäne gemeinsam nutzen, definieren die Mitgliedschaft in einem portbasierten VLAN. Sie können mehrere portbasierte VLANs konfigurieren. Wenn Sie einem neuen VLAN als nicht markierte Member eine Schnittstelle hinzufügen, wird sie automatisch aus dem Standard-VLAN entfernt.

- Tagged VLAN

  Eine Netzwerkschnittstelle kann ein markierter oder nicht markierter Member eines VLAN sein. Jede Netzwerkschnittstelle ist ein nicht getaggtes Mitglied von nur einem VLAN (seinem nativen VLAN). Die nicht markierte Netzwerkschnittstelle leitet die Frames für das native VLAN als nicht markierte Frames weiter. Eine getaggte Netzwerkschnittstelle kann Teil von mehr als einem VLAN sein. Achten Sie beim Konfigurieren der Tagging darauf, dass beide Enden der Verbindung über die entsprechenden VLAN-Einstellungen verfügen. Mit dem Konfigurationsdienstprogramm können Sie ein getaggtes VLAN (nsvlan) definieren, das beliebige Ports als markierte Mitglieder des VLAN gebunden haben kann. Die Konfiguration dieses VLAN erfordert einen Neustart der ADC-Appliance und muss daher während der anfänglichen Netzwerkkonfiguration durchgeführt werden.

Aggregatkanäle verknüpfen

Die Link-Aggregation kombiniert eingehende Daten von mehreren Ports zu einer einzigen Hochgeschwindigkeits-Verbindung. Die Konfiguration des Link-Aggregatkanals erhöht die Kapazität und Verfügbarkeit des Kommunikationskanals zwischen einer Citrix ADC Appliance und anderen angeschlossenen Geräten. Ein aggregierter Link wird auch als Kanal bezeichnet.

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

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

Uhrsynchronisierung

April 7, 2022

Sie können Ihre Citrix ADC-Appliance so konfigurieren, dass ihre lokale Uhr mit einem Network Time Protocol (NTP) -Server synchronisiert wird. Dadurch wird sichergestellt, dass die Uhr dieselben Datums- und Uhrzeiteinstellungen hat wie die anderen Server in Ihrem Netzwerk. NTP verwendet den User Datagram Protocol (UDP) Port 123 als Transportschicht. Fügen Sie NTP-Server in der NTP-Konfigurationsdatei hinzu, damit die Appliance regelmäßig Updates von diesen Servern erhält.

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

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

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

   ```
   restrict localhost

   restrict 127.0.0.2
   ```

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

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

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

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


6. Starten Sie die Appliance neu, um die Uhrsynchronisierung

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

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

or

/bin/sh /etc/ntpd_ctl full_start
<!--NeedCopy-->
```

DNS-Konfiguration

July 8, 2022

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

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

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

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

Fügen Sie einen Namenserver mithilfe der CLI hinzu

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

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

  Beispiel

  “‘

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

  “‘

Fügen Sie einen Namenserver über die GUI hinzu

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

SNMP-Konfiguration

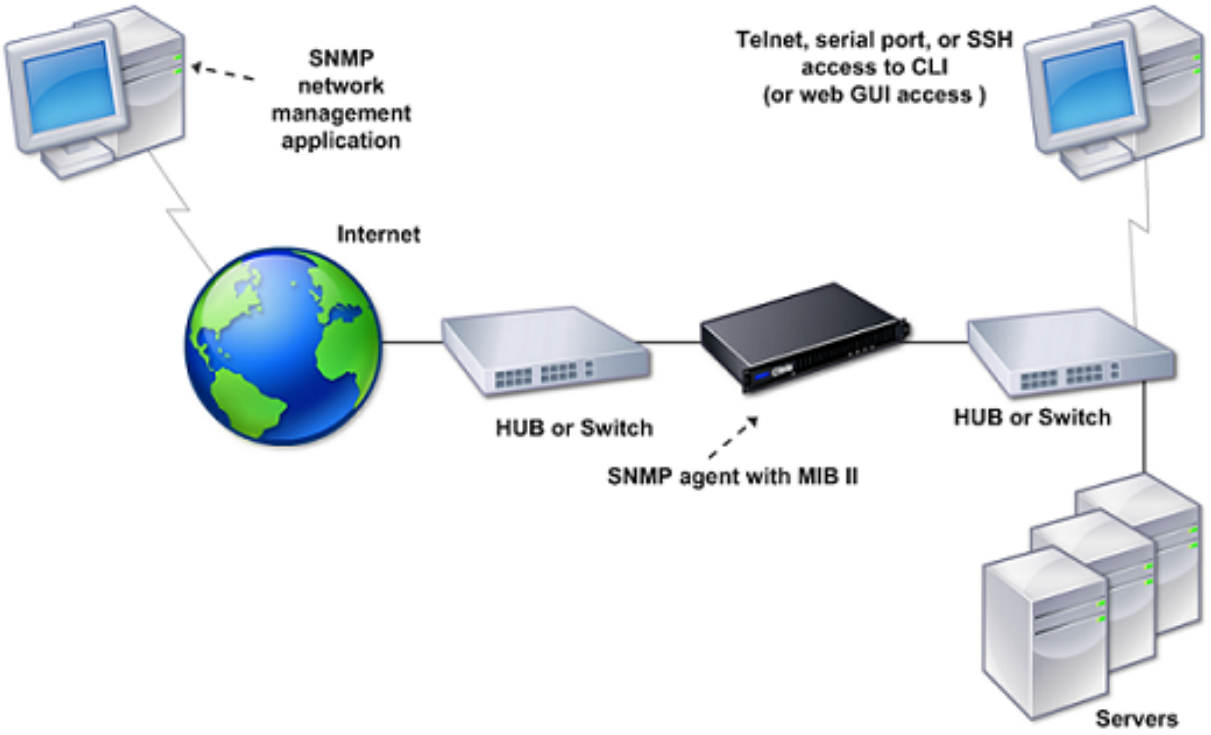
October 5, 2021

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

SNMP-Überwachung verwendet Traps-Nachrichten und Alarme. SNMP-Traps-Meldungen sind asynchrone Ereignisse, die der Agent generiert, um anormale Bedingungen zu signalisieren, die durch Alarme angezeigt werden. Wenn Sie beispielsweise informiert werden möchten, wenn die CPU-Auslastung über 90 Prozent liegt, können Sie einen Alarm für diese Bedingung einrichten. Die

folgende Abbildung zeigt ein Netzwerk mit einer Citrix ADC Appliance, für die SNMP aktiviert und konfiguriert ist.

Abbildung 1. SNMP auf der Citrix ADC Appliance



Der SNMP-Agent auf einer Citrix ADC Appliance unterstützt SNMP Version 1 (SNMPv1), SNMP Version 2 (SNMPv2) und SNMP Version 3 (SNMPv3). Da er im zweisprachigen Modus arbeitet, kann der Agent SNMPv2-Abfragen wie Get-Bulk und SNMPv1-Abfragen verarbeiten. Der SNMP-Agent sendet auch Traps, die mit SNMPv2 kompatibel sind und unterstützt SNMPv2-Datentypen, z. B. counter64 SNMPv1-Manager (Programme auf anderen Servern, die SNMP-Informationen von der ADC-Appliance anfordern) verwenden bei der Verarbeitung von SNMP-Abfragen die Datei NS-MIB-SMIV1.mib. SNMPv2-Manager verwenden die Datei NS-MIB-SMIV2.mib.

Die Citrix ADC Appliance unterstützt die folgenden unternehmensspezifischen MIBs:

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

Zum Konfigurieren von SNMP geben Sie an, welche Manager den SNMP-Agent abfragen, SNMP-Trap-Listener hinzufügen, die die SNMP-Trap-Nachrichten empfangen, und SNMP-Alarme konfigurieren können.

Hinzufügen von SNMP-Managern

Sie können eine Workstation konfigurieren, auf der eine Verwaltungsanwendung ausgeführt wird, die SNMP-Version 1, 2 oder 3 entspricht, um auf eine Appliance zuzugreifen. Eine solche Workstation wird SNMP-Manager genannt. Wenn Sie keinen SNMP-Manager auf der Appliance angeben, akzeptiert die Appliance SNMP-Abfragen von allen IP-Adressen im Netzwerk und antwortet darauf. Wenn Sie einen oder mehrere SNMP-Manager konfigurieren, akzeptiert die Appliance SNMP-Abfragen nur von diesen spezifischen IP-Adressen. Wenn Sie die IP-Adresse eines SNMP-Managers angeben, können Sie den Parameter netmask verwenden, um Zugriff von ganzen Subnetzen zu gewähren. Sie können maximal 100 SNMP-Manager oder Netzwerke hinzufügen. So fügen Sie einen SNMP-Manager über die CLI hinzu

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

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

Beispiel:

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

So fügen Sie über die GUI einen SNMP-Manager hinzu:

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

Hinzufügen von SNMP-Trap-Listener

Nachdem Sie die Alarme konfiguriert haben, müssen Sie den Trap-Listener angeben, an den die Appliance die Trap-Nachrichten sendet. Neben der Angabe von Parametern wie IP-Adresse und Zielport des Trap-Listener können Sie den Trap-Typ (entweder generisch oder spezifisch) und die SNMP-Version angeben.

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

So fügen Sie einen SNMP-Trap-Listener über die CLI hinzu

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

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

Beispiel:

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

So fügen Sie einen SNMP-Trap-Listener über die GUI hinzu

1. Erweitern Sie im Navigationsbereich System, erweitern Sie **SNMP**, und klicken Sie dann auf **Traps**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **SNMP-Trap-Ziel erstellen** im Textfeld **Ziel-IP-Adresse** die IP-Adresse ein (z. B. 10.102.29.3).
4. Klicken Sie auf **Create** und dann auf **Close**.
5. Stellen Sie sicher, dass die hinzugefügte SNMP-Trap im Abschnitt **Details** am unteren Rand des Bereichs angezeigt wird.

SNMP-Alarme konfigurieren

Sie konfigurieren Alarme so, dass die Appliance eine Trap-Nachricht generiert, wenn ein Ereignis eintritt, das einem der Alarme entspricht. Die Konfiguration eines Alarms besteht darin, den Alarm zu

aktivieren und den Schweregrad festzulegen, bei dem eine Falle generiert wird. Es gibt fünf Schweregrade: Kritisch, Major, Minor, Warnung und Information. Eine Trap wird nur gesendet, wenn der Schweregrad des Alarms mit dem für die Trap angegebenen Schweregrad übereinstimmt.

Einige Alarme sind standardmäßig aktiviert. Wenn Sie einen SNMP-Alarm deaktivieren, generiert die Appliance keine Trapmeldungen, wenn entsprechende Ereignisse auftreten. Wenn Sie beispielsweise den SNMP-Alarm für Anmeldefehler deaktivieren, generiert die Appliance keine Trap-Nachricht, wenn ein Anmeldefehler auftritt.

So aktivieren oder deaktivieren Sie einen Alarm über die CLI

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

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

  Beispiel

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

So stellen Sie den Schweregrad des Alarms über die CLI ein

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den Schweregrad des Alarms festzulegen und sicherzustellen, dass der Schweregrad korrekt eingestellt wurde:

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

Beispiel:

```
set snmp alarm LOGIN-FAILURE -severity Major
Done
show snmp alarm LOGIN-FAILURE
```



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

So konfigurieren Sie Alarme über die GUI

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

Konfiguration überprüfen

October 5, 2021

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

Konfigurations-Checkliste

- Der Build läuft:
- Es gibt keine Inkompatibilitätsprobleme. (Inkompatibilitätsprobleme werden in den Versionshinweisen des Builds dokumentiert.)
- Die Port-Einstellungen (Geschwindigkeit, Duplex, Flusssteuerung, Überwachung) sind identisch mit dem Port des Switches.
- Genügend SNIP-IP-Adressen wurden so konfiguriert, dass sie alle serverseitigen Verbindungen in Spitzenzeiten unterstützen.
  - Die Anzahl der konfigurierten SNIP-IP-Adressen ist: __

- Die erwartete Anzahl gleichzeitiger Serververbindungen ist:
  [] 62.000 [] 124.000 [] Andere____

Checkliste für die Topologiekonfiguration

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

Die eingegebenen Routen sind:

_____

- Wenn sich die Citrix ADC Appliance in einer öffentlich-privaten Topologie befindet, wurde die umgekehrte NAT konfiguriert.
- Die auf der ADC-Appliance konfigurierten Failover-Einstellungen (Hochverfügbarkeit) werden in einer Einarm- oder Zweiarm-Konfiguration aufgelöst. Alle nicht verwendeten Netzwerkschnittstellen wurden deaktiviert:

  _____

- Wenn sich die ADC-Appliance hinter einem externen Lastausgleichsdienst befindet, ist die Lastausgleichsrichtlinie auf dem externen Lastausgleichsdienst nicht die “geringste Verbindung”.

  Die auf dem externen Lastausgleichsdienst konfigurierte Lastausgleichsrichtlinie lautet:

  _____

- Wenn die ADC-Appliance vor einer Firewall platziert wird, wird das Sitzungszeitlimit auf der Firewall auf einen Wert größer als oder gleich 300 Sekunden festgelegt.

  Hinweis: Die TCP-Leerlaufverbindung auf einer Citrix ADC Appliance beträgt 360 Sekunden. Wenn das Timeout auf der Firewall ebenfalls auf 300 Sekunden oder länger eingestellt ist, kann die Appliance das TCP-Verbindungsmultiplexing effektiv durchführen, da Verbindungen nicht früher geschlossen werden.

  Der für das Sitzungszeitlimit konfigurierte Wert lautet: _____

Prüfliste für die Serverkonfiguration

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

  Der für das Keep-Alive-Timeout konfigurierte Wert lautet: _____

- Das Standard-Gateway wurde auf den richtigen Wert gesetzt. (Das Standard-Gateway sollte entweder eine Citrix ADC Appliance oder ein Upstream-Router sein.) Das Standard-Gateway ist:

  _____

- Die Serverporteinstellungen (Geschwindigkeit, Duplex, Flusssteuerung, Überwachung) sind identisch mit den Switch-Port-Einstellungen.

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

  Der Wert MaxConn (maximale Anzahl von Verbindungen), der festgelegt wurde, lautet:

  _____

- Wenn ein Netscape Enterprise Server verwendet wird, werden die maximalen Anforderungen pro Verbindungsparameter auf der Citrix ADC Appliance festgelegt. Die maximale Anforderung pro Verbindungswert, der festgelegt wurde, ist:

  _____

Checkliste zur Konfiguration von Softwarefunktionen

- Muss die Funktion Layer 2-Modus deaktiviert werden? (Deaktivieren Sie, wenn ein anderes Layer 2-Gerät parallel mit einer Citrix ADC Appliance arbeitet.)

  Grund für die Aktivierung oder Deaktivierung:

  _____

- Muss die MAC-basierte Weiterleitungsfunktion deaktiviert werden? (Wenn die vom Rückgabewert verwendete MAC-Adresse anders ist, sollte sie deaktiviert werden.)

  Grund für die Aktivierung oder Deaktivierung:

  _____

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

  Grund für die Aktivierung oder Deaktivierung:

  _____

- Müssen die Standardeinstellungen der Überspannungsschutzfunktion geändert werden?

  Grund für die Änderung oder Nichtänderung:

  _____

Zugriffs-Checkliste

- Die System-IPs können über das clientseitige Netzwerk angepingt werden.
- Die System-IPs können vom serverseitigen Netzwerk aus angepingt werden.

- Die verwalteten Server können über den Citrix ADC angepingt werden.
- Internet-Hosts können von den verwalteten Servern angepingt werden.
- Auf die verwalteten Server kann über den Browser zugegriffen werden.
- Auf das Internet kann über verwaltete Server über den Browser zugegriffen werden.
- Auf das System kann über SSH zugegriffen werden.
- Der Administratorzugriff auf alle verwalteten Server funktioniert.

> Hinweis: Wenn Sie das Ping-Dienstprogramm verwenden, stellen Sie sicher, dass für den Ping-Server ICMP ECHO aktiviert ist, oder Ihr Ping wird nicht erfolgreich ausgeführt.

Firewall-Checkliste

Die folgenden Firewall-Anforderungen wurden erfüllt:

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

Lastenausgleichsverkehr auf einer Citrix ADC Appliance

October 5, 2021

Die Lastenausgleichsfunktion verteilt Clientanforderungen auf mehrere Server, um die Ressourcenauslastung zu optimieren. In einem realen Szenario mit einer begrenzten Anzahl von Servern, die Dienste für eine große Anzahl von Clients bereitstellen, kann ein Server überlastet werden und die Leistung der Serverfarm beeinträchtigen. Eine Citrix ADC Appliance verwendet Lastausgleichskriterien, um Engpässe zu vermeiden, indem sie jede Clientanforderung an den Server weiterleitet, der für die Bearbeitung der Anforderung am besten geeignet ist.

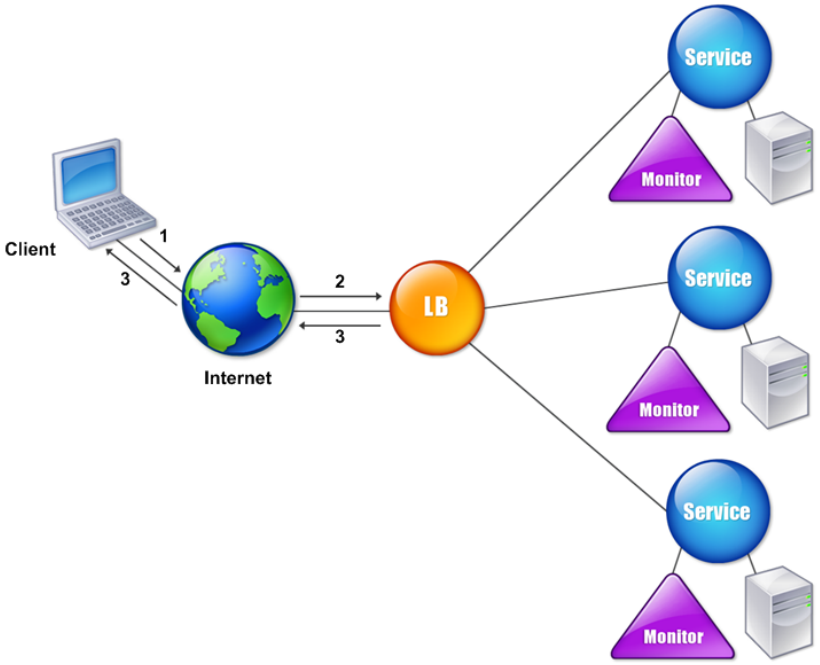
Zum Konfigurieren des Lastenausgleichs definieren Sie einen virtuellen Server, der mehreren Servern in einer Serverfarm als Proxy dient und die Last unter ihnen ausgleicht.

Wenn ein Client eine Verbindung zum Server initiiert, beendet ein virtueller Server die Clientverbindung und initiiert eine neue Verbindung mit dem ausgewählten Server oder verwendet eine vorhandene Verbindung mit dem Server, um den Lastenausgleich durchzuführen. Die Lastenausgleichsfunktion bietet Datenverkehrsverwaltung von Layer 4 (TCP und UDP) bis Layer 7 (FTP, HTTP und HTTPS).

Die Citrix ADC Appliance verwendet eine Reihe von Algorithmen, sogenannte Lastausgleichsmethoden, um zu bestimmen, wie die Last auf die Server verteilt wird. Die Standardmethode für den Lastenausgleich ist die Methode Kleinste Verbindungen.

Eine typische Lastausgleichsbereitstellung besteht aus den in der folgenden Abbildung beschriebenen Entitäten.

Abbildung 1. Lastenausgleich-Architektur



Die Entitäten funktionieren wie folgt:

- **Virtueller Server**. Eine Entität, die durch eine IP-Adresse, einen Port und ein Protokoll dargestellt wird. Die virtuelle Server-IP-Adresse (VIP) ist in der Regel eine öffentliche IP-Adresse. Der Client sendet Verbindungsanforderungen an diese IP-Adresse. Der virtuelle Server stellt eine Bank von Servern dar.
- **Dienst**. Eine logische Darstellung eines Servers oder einer Anwendung, die auf einem Server ausgeführt wird. Identifiziert die IP-Adresse des Servers, einen Port und ein Protokoll. Die Dienste sind an die virtuellen Server gebunden.
- **Server-Objekt** Eine Entität, die durch eine IP-Adresse dargestellt wird. Das Serverobjekt wird erstellt, wenn Sie einen Dienst erstellen. Die IP-Adresse des Dienstes wird als Name des Serverobjekts verwendet. Sie können auch ein Serverobjekt erstellen und dann Dienste erstellen, indem Sie das Serverobjekt verwenden.
- **Überwachen**. Eine Entität, die die Integrität der Dienste verfolgt. Die Appliance prüft die Server regelmäßig über den Monitor, der an jeden Dienst gebunden ist. Wenn ein Server nicht innerhalb eines angegebenen Antwortzeitlimits reagiert und die angegebene Anzahl von Prüfpunk-

ten fehlschlägt, wird der Dienst mit DOWN gekennzeichnet. Anschließend führt die Appliance den Lastausgleich unter den verbleibenden Diensten durch.

Lastausgleich

October 5, 2021

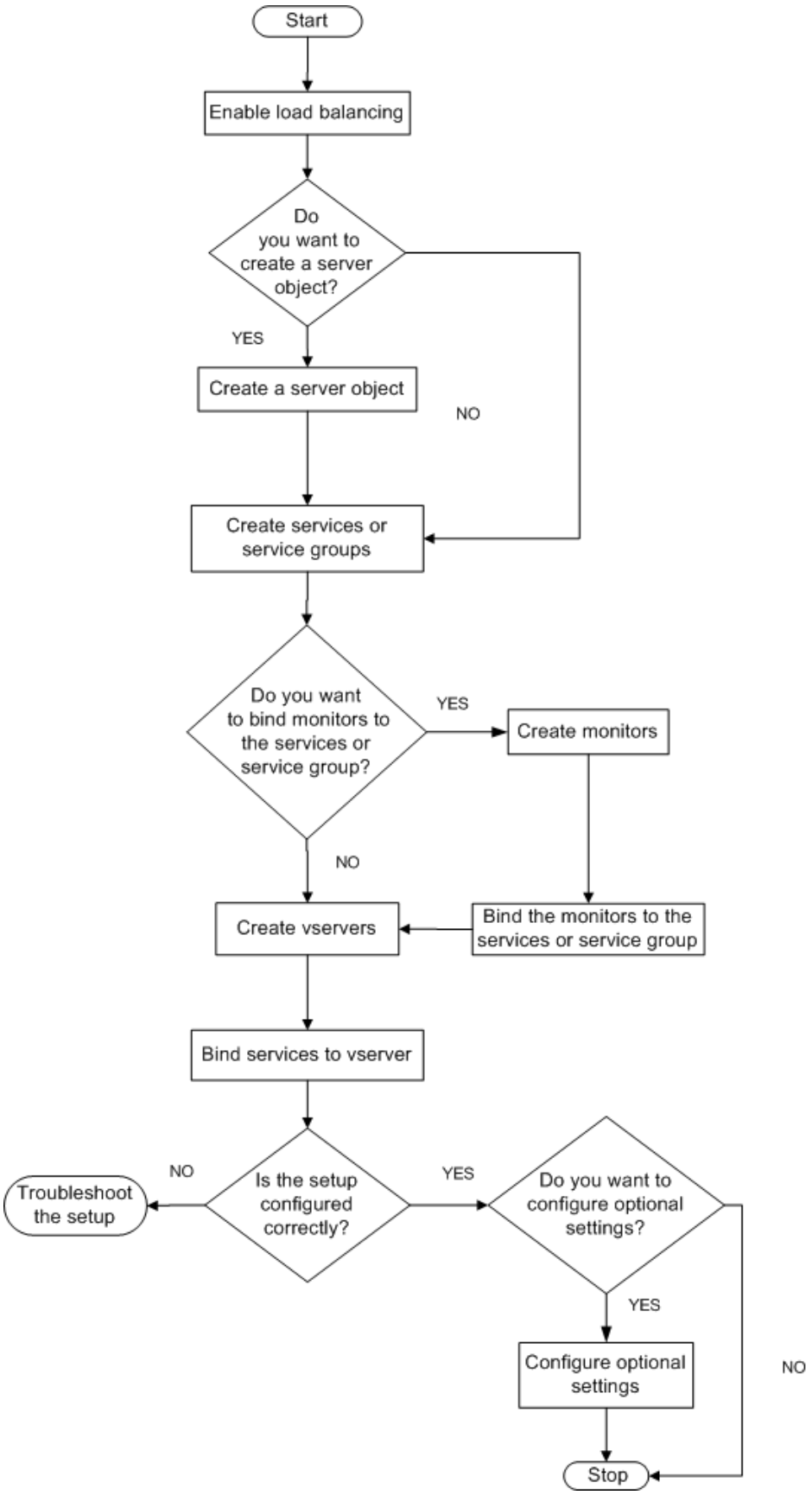
Um den Lastenausgleich zu konfigurieren, müssen Sie zuerst Dienste erstellen. Anschließend erstellen Sie virtuelle Server und binden die Dienste an die virtuellen Server. Standardmäßig bindet die Citrix ADC Appliance einen Monitor an jeden Dienst. Überprüfen Sie nach dem Binden der Dienste Ihre Konfiguration, indem Sie sicherstellen, dass alle Einstellungen korrekt sind.

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

Optional können Sie einem Service Gewichtungen zuweisen. Die Lastausgleichsmethode verwendet dann die zugewiesene Gewichtung, um einen Service auszuwählen. Für die ersten Schritte können Sie jedoch optionale Aufgaben auf die Konfiguration einiger grundlegender Persistenzeinstellungen, für Sitzungen, die eine Verbindung zu einem bestimmten Server beibehalten müssen, und einige grundlegende Konfigurationsschutzeinstellungen beschränken.

Das folgende Flussdiagramm veranschaulicht die Reihenfolge der Konfigurationsaufgaben.

Abbildung 1. Abfolge von Aufgaben zum Konfigurieren des Lastenausgleichs



Lastenausgleich aktivieren

Stellen Sie vor der Konfiguration des Lastenausgleichs sicher, dass die Lastenausgleichsfunktion aktiviert ist.

So aktivieren Sie den Lastenausgleich mit der CLI

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

- Funktion lb aktivieren
- Funktion anzeigen

  Beispiel

  “‘ pre codeblock

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

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

So aktivieren Sie den Lastausgleich mit der GUI

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

Konfigurieren von Diensten und einem virtuellen Server

Wenn Sie die Dienste identifiziert haben, für die Sie den Lastausgleich durchführen möchten, können Sie die anfängliche Lastausgleichskonfiguration implementieren, indem Sie die Dienstobjekte er-

stellen, einen virtuellen Lastausgleichsserver erstellen und die Dienstobjekte an den virtuellen Server binden.

So implementieren Sie die anfängliche Lastausgleichskonfiguration über die CLI

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

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

  Beispiel

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

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

So implementieren Sie die anfängliche Lastausgleichskonfiguration über die GUI

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

Persistenzeinstellungen

October 5, 2021

Sie müssen die Persistenz auf einem virtuellen Server konfigurieren, wenn Sie die Zustände der Verbindungen auf den Servern beibehalten möchten, die von diesem virtuellen Server dargestellt werden (z. B. Verbindungen, die im E-Commerce verwendet werden). Die Appliance verwendet dann die konfigurierte Lastausgleichsmethode für die erste Auswahl eines Servers, leitet jedoch alle nachfolgenden Anforderungen vom selben Client an denselben Server weiter.

Wenn die Persistenz konfiguriert ist, überschreibt sie die Lastausgleichsmethoden, sobald der Server ausgewählt wurde. Wenn die konfigurierte Persistenz für einen ausgefallenen Dienst gilt, verwendet die Appliance die Lastausgleichsmethoden, um einen neuen Dienst auszuwählen, und der neue Dienst wird für nachfolgende Anforderungen vom Client dauerhaft. Wenn sich der ausgewählte Dienst im Status Nicht verfügbar befindet, werden die ausstehenden Anforderungen weiterhin bedient, aber keine neuen Anforderungen oder Verbindungen akzeptiert. Nach Ablauf der Abschaltperiode werden die vorhandenen Verbindungen geschlossen. In der folgenden Tabelle sind die Persistenzarten aufgeführt, die Sie konfigurieren können.

Persistenz-Typ	Persistente Verbindungen
Quell-IP, SSL-Sitzungs-ID, Regel, DESTIP, SRCIPDESTIP	250K
CookieInsert, URL passiv, Benutzerdefinierte Server-ID	Speicherbegrenzung. Im Falle von CookieInsert, wenn Timeout nicht 0 ist, ist eine beliebige Anzahl von Verbindungen erlaubt, bis sie durch den Speicher begrenzt sind.

Tabelle 1. Einschränkungen bei der Anzahl gleichzeitiger persistenter Verbindungen

Wenn die konfigurierte Persistenz aufgrund fehlender Ressourcen auf einer Appliance nicht aufrechterhalten werden kann, werden die Lastausgleichsmethoden für die Serverauswahl verwendet. Die Persistenz wird je nach Persistenztyp für einen konfigurierten Zeitraum beibehalten. Einige Persistenztypen sind spezifisch für bestimmte virtuelle Server. Die folgende Tabelle zeigt die Beziehung.

Persistence TypeHeader 1	HTTP	HTTPS	TCP	UDP/IP	SSL_Bridge
Quell-IP	JA	JA	JA	JA	JA

Persistence TypeHeader 1	HTTP	HTTPS	TCP	UDP/IP	SSL_Bridge
CookieInsert	JA	JA	NEIN	NEIN	NEIN
SSL Session ID	NEIN	JA	NEIN	NEIN	JA
URL Passive	JA	JA	NEIN	NEIN	NEIN
Benutzerdefinie Server-ID	JA	JA	NEIN	NEIN	NEIN
Regel	JA	JA	NEIN	NEIN	NEIN
SRCIPDESTIP	Nicht zutreffend	Nicht zutreffend	JA	JA	Nicht zutreffend
DESTIP	Nicht zutreffend	Nicht zutreffend	JA	JA	Nicht zutreffend

Tabelle 2. Persistenztypen, die für jeden virtuellen Servertyp verfügbar sind

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

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

Konfigurieren der Persistenz basierend auf Cookies

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

Die Citrix ADC Appliance fügt das Cookie ein: <NSC_XXXX>=<ServiceIP> <ServicePort>

Wobei:

- <<NSC_XXXX> ist die virtuelle Server-ID, die vom Namen des virtuellen Servers abgeleitet wird.

- <<ServiceIP> ist der hexadezimale Wert der IP-Adresse des Dienstes.
- <<ServicePort> ist der hexadezimale Wert des Ports des Dienstes.

Der ADC verschlüsselt ServiceIP und ServicePort, wenn er ein Cookie einfügt, und entschlüsselt sie, wenn er ein Cookie erhält.

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

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

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

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

Hinweis: Die meisten derzeit installierten Client-Software (Microsoft Internet Explorer und Netscape-Browser) verstehen HTTP-Cookie Version 0; einige HTTP-Proxys verstehen jedoch HTTP-Cookie Version 1.

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

Ein Administrator kann die HTTP-Cookie-Version ändern.

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

Geben Sie an der Eingabeaufforderung;

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

Beispiel:


```
set ns param -cookieversion 1
<!--NeedCopy-->
```

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

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

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

So konfigurieren Sie die Persistenz basierend auf Cookies über die CLI

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

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

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

Beispiel:

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


So konfigurieren Sie die Persistenz basierend auf Cookies über die GUI

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

Konfigurieren der Persistenz basierend auf Server-IDs in URLs

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

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

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

Beispiel: Payload-Ausdruck

Der Ausdruck URLQUERY contains sid= konfiguriert das System so, dass die Server-ID aus der URL-Abfrage einer Clientanforderung nach dem passenden Token sid= extrahiert wird. Somit`http://www.citrix.com/index.asp?\\&sid;=c0a864100050` wird eine Anfrage mit der URL an den Server mit der IP-Adresse10.102.29.10 und Port 80.

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

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

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

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

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

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

Beispiel:

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

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

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie die Persistenz konfigurieren möchten (z. B. vServer-LB-1), und klicken Sie dann auf Öffnen.
3. Wählen Sie im Dialogfeld Virtuellen Server konfigurieren (Load Balancing) auf der Registerkarte Methode und Persistenz in der Liste Persistenz die Option URLPASSIVE aus.
4. Geben Sie im Textfeld Timeout (min) den Zeitüberschreitungswert ein (z. B. 2).
5. Geben Sie im Textfeld Regel einen gültigen Ausdruck ein. Alternativ klicken Sie neben dem Textfeld Regel auf Konfigurieren, und verwenden Sie das Dialogfeld Ausdruck erstellen, um einen Ausdruck zu erstellen.
6. Klicken Sie auf OK.

7. Stellen Sie sicher, dass der virtuelle Server, für den Sie die Persistenz konfiguriert haben, korrekt konfiguriert ist, indem Sie den virtuellen Server auswählen und den Abschnitt Details unten im Bereich anzeigen.

Konfigurieren von Features zum Schutz der Lastausgleichskonfiguration

October 5, 2021

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

URL-Umleitung konfigurieren

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

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

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

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

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

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

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


Beispiel:

```
    > set lb vserver vserver-LB-1 -redirectURL <http://www.newdomain.
       com/mysite/maintenance>
     Done
    > show lb vserver vserver-LB-1
        vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
        State: DOWN
        Last state change was at Wed Jun 17 08:56:34 2009 (+666 ms)
        .
        .
        .
        Redirect URL: <http://www.newdomain.com/mysite/maintenance>
        .
        .
        .
     Done
    >
<!--NeedCopy-->
```

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

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

Konfigurieren von virtuellen Backup-Servern

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

Sie können einen virtuellen Backupserver konfigurieren, wenn Sie einen virtuellen Server erstellen

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

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

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

So konfigurieren Sie einen virtuellen Backupserver über die CLI

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

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

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

Beispiel:

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



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

So richten Sie einen virtuellen Backupserver über die GUI ein

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie den virtuellen Backupserver konfigurieren möchten (z. B. vServer-LB-1), und klicken Sie dann auf Öffnen.
3. Wählen Sie im Dialogfeld Virtuellen Server konfigurieren (Load Balancing) auf der Registerkarte Erweitert in der Liste Virtueller Server sichern den virtuellen Backupserver aus (z. B. vServer-LB-2, und klicken Sie dann auf OK.
4. Stellen Sie sicher, dass der konfigurierte virtuelle Backupserver im Abschnitt Details am unteren Rand des Bereichs angezeigt wird.

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

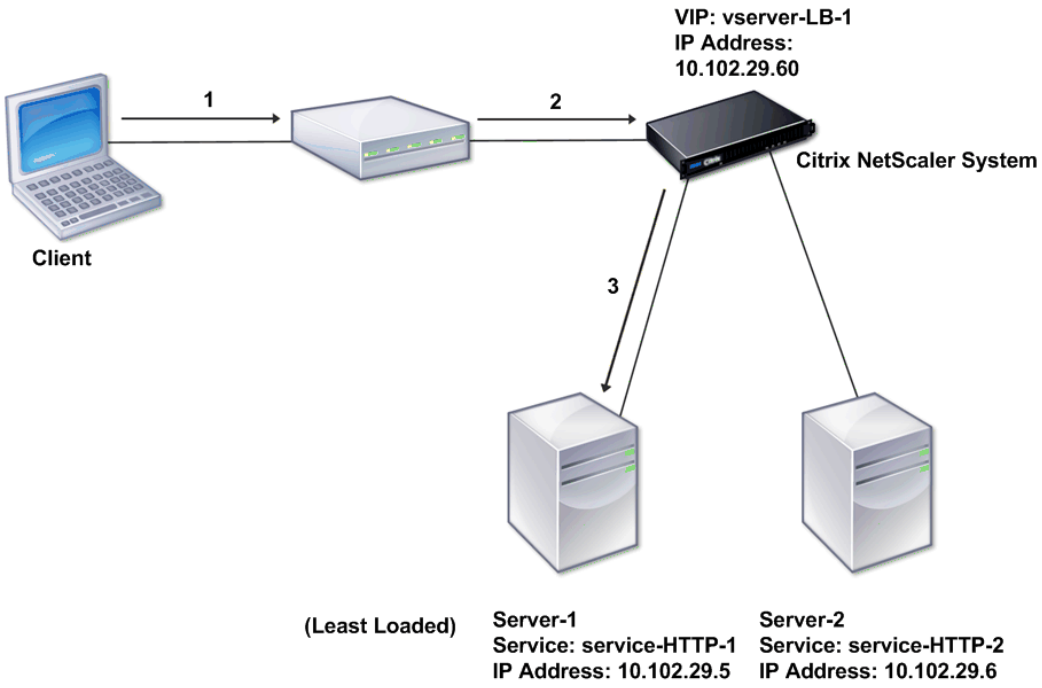
Ein typisches Lastausgleichszenario

October 5, 2021

In einem Lastausgleichs-Setup befinden sich die Citrix ADC Appliances logisch zwischen dem Client und der Serverfarm und verwalten den Datenverkehr zu den Servern.

Die folgende Abbildung zeigt die Topologie einer grundlegenden Lastausgleichskonfiguration.

Abbildung 1. Grundlegende Load Balancing-Topologie

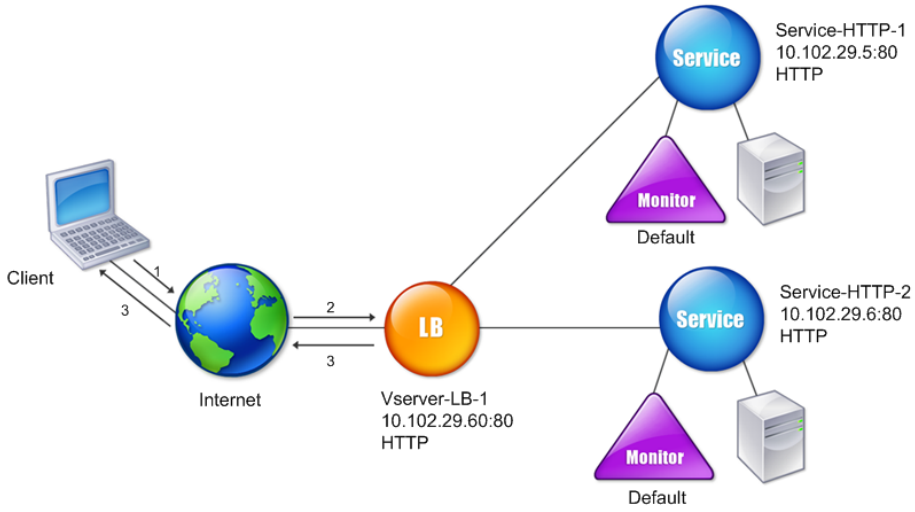


Der virtuelle Server wählt den Dienst aus und weist ihn zu, um Clientanforderungen zu erfüllen. Betrachten Sie das Szenario in der obigen Abbildung, in dem die Dienste Service-HTTP-1 und Service-HTTP-2 erstellt und an den virtuellen Server mit dem Namen virtueller Server-LB-1 gebunden werden. Virtual Server-LB-1 leitet die Clientanforderung entweder an Service-HTTP-1 oder Service-HTTP-2 weiter. Das System wählt den Dienst für jede Anforderung mithilfe der Load Balancing-Methode Lost Connections aus. In der folgenden Tabelle sind die Namen und Werte der grundlegenden Entitäten aufgeführt, die auf dem System konfiguriert werden müssen.

Tabelle 1. LB-Konfigurationsparameterwerte

Die folgende Abbildung zeigt die Lastausgleichsprobenwerte und die erforderlichen Parameter, die in der vorhergehenden Tabelle beschrieben werden.

Abbildung 2. Load Balancing Entity Modell



In den folgenden Tabellen sind die Befehle aufgeführt, die zum Konfigurieren dieser Lastausgleich-seinrichtung über die Befehlszeile verwendet werden.

Aufgabe	Befehl
So aktivieren Sie den Lastenausgleich	Funktion lb aktivieren
So erstellen Sie einen Dienst mit dem Namen Service-HTTP-1	add service service-HTTP-1 10.102.29.5 HTTP 80
So erstellen Sie einen Dienst mit dem Namen Service-HTTP-2	add service service-HTTP-2 10.102.29.6 HTTP 80
So erstellen Sie einen virtuellen Server mit dem Namen vServer-LB-1	add lb vserver vserver-LB-1 HTTP 10.102.29.60 80
So binden Sie einen Dienst mit dem Namen Service-HTTP-1 an einen virtuellen Server mit dem Namen vServer-LB-1	bind lb vserver vserver-LB-1 service-HTTP-1

Aufgabe	Befehl
So binden Sie einen Dienst mit dem Namen Service-HTTP-2 an einen virtuellen Server mit dem Namen vServer-LB-1	bind lb vserver vserver-LB-1 service-HTTP-2

Tabelle 2. Aufgaben zur Erstkonfiguration

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

Aufgabe	Befehl
So zeigen Sie die Eigenschaften eines virtuellen Servers mit dem Namen vServer-LB-1 an	show lb vserver vserver-LB-1
So zeigen Sie die Statistiken eines virtuellen Servers mit dem Namen vServer-LB-1 an	stat lb vserver vserver-LB-1
So zeigen Sie die Eigenschaften eines Dienstes mit dem Namen Service-HTTP-1 an	show service service-HTTP-1
So zeigen Sie die Statistiken eines Dienstes mit dem Namen Service-HTTP-1 an	stat service service-HTTP-1
So zeigen Sie die Bindungen eines Dienstes mit dem Namen Service-HTTP-1 an	show service bindings service-HTTP-1

Tabelle 3. Überprüfungsaufgaben

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

Aufgabe	Befehl
So konfigurieren Sie einen virtuellen Server für die Umleitung der Clientanforderung an eine URL auf einem virtuellen Server namens vServer-LB-1	set lb vserver vserver-LB-1 -redirectURL http://www.newdomain.com/mysite/maintenance
So legen Sie einen virtuellen Backupserver auf einem virtuellen Server namens vServer-LB-1 fest	set lb vserver vserver-LB-1 -backupVserver vserver-LB-2

Tabelle 4. Anpassungsaufgaben

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

Anwendungsfall: So erzwingen Sie Secure- und HttpOnly-Cookie-Optionen für Websites, die die Citrix ADC Appliance verwenden

October 5, 2021

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

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

  > HINWEIS:
  >
  > Sie können die Option HttpOnly nicht verwenden, wenn eine Webanwendung Zugriff auf Cookie-Inhalte benötigt, indem Sie ein clientseitiges Skript wie JavaScript oder ein clientseitiges Java-Applet verwenden. Sie können die in diesem Dokument erwähnte Methode

> verwenden, um nur die servergenerierten Cookies und nicht die von der Citrix ADC Appliance generierten Cookies neu zu schreiben. Zum Beispiel AppFirewall, Persistenz, VPN-Sitzungscookies und so weiter.

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

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

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

1. Erstellen Sie eine Rewrite-Aktion.

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

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

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

2. Erstellen Sie eine Richtlinie zum Umschreiben, um die Aktion auszulösen.

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

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

   ```
   bind lb vserver mySSLVServer -policyName rw_force_secure_cookie -
       priority 100 -gotoPriorityExpression NEXT -type RESPONSE
   ```



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

Beispiele:

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

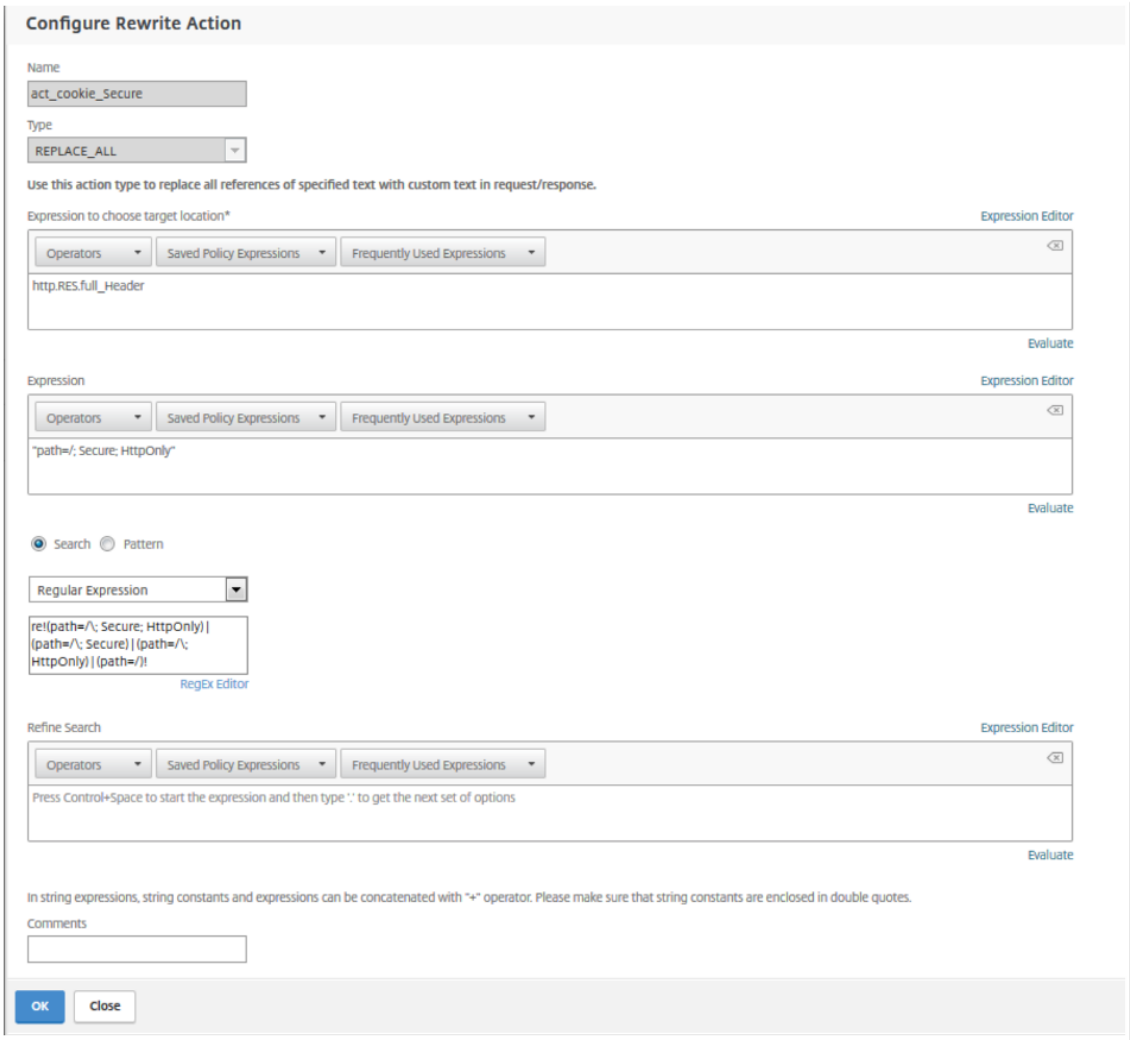
```
1 Set-Cookie: CtxsAuthId=C5614491; path=/Citrix/ProdWeb
2 <!--NeedCopy-->
```

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

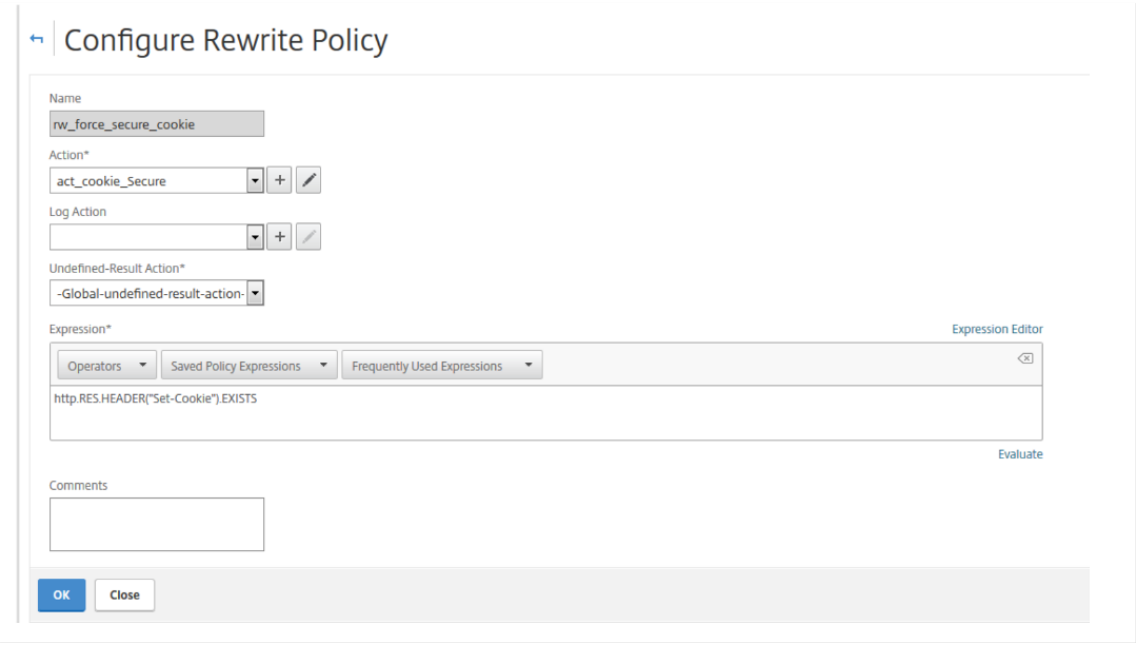
```
1 Set-Cookie: CtxsAuthId=C5614491; Secure; HttpOnly; path=/Citrix/ProdWeb
     /
2 <!--NeedCopy-->
```

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

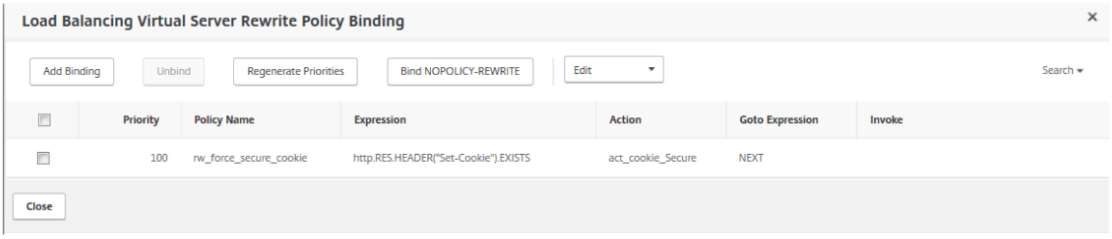
1. Navigieren Sie zu **AppExpert > Umschreiben > Aktionen**und klicken Sie auf **Hinzufügen**, um eine neue Neuschreibaktion hinzuzufügen.



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



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



Beschleunigen des Lastausgleichsverkehrs durch Verwendung von Komprimierung

October 5, 2021

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

Die Citrix ADC Komprimierung ist eine richtlinienbasierte Funktion. Eine Richtlinie filtert Anforderun-

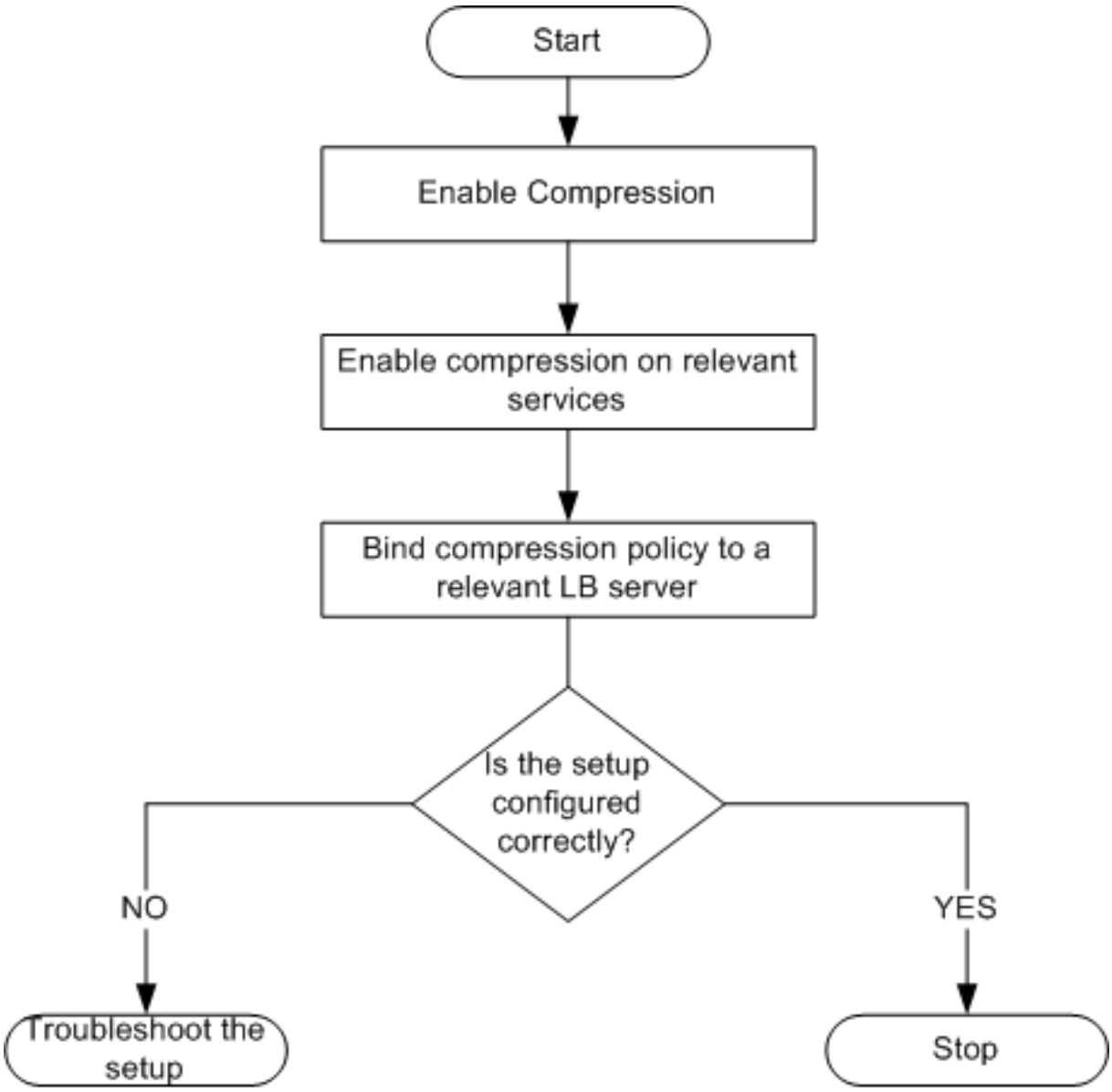
gen und Antworten, um Antworten zu identifizieren, die komprimiert werden sollen, und gibt die Art der Komprimierung an, die auf jede Antwort angewendet werden soll. Die Appliance bietet mehrere integrierte Richtlinien zum Komprimieren gängiger MIME-Typen wie text/html, text/plain, text/xml, text/css, text/rtf, application/msword, application/vnd.ms-excel und application/vnd.ms-powerpoint. Sie können auch benutzerdefinierte Richtlinien erstellen. Die Appliance komprimiert keine komprimierten MIME-Typen wie Anwendung/Oktetstream, Binär-, Byte- und komprimierte Bildformate wie GIF und JPEG.

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

Komprimierungskonfigurations-Tasksequenz

Das folgende Flussdiagramm zeigt die Reihenfolge der Aufgaben zum Konfigurieren der grundlegenden Komprimierung in einer Lastausgleichseinrichtung.

Abbildung 1. Abfolge von Aufgaben zum Konfigurieren der Komprimierung



> Hinweis: Die Schritte in der obigen Abbildung gehen davon aus, dass der Lastausgleich bereits konfiguriert wurde.

Komprimierung aktivieren

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

So aktivieren Sie die Komprimierung über die CLI

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

- enable ns feature CMP
- show ns feature

```
> enable ns feature CMP


Done

> show ns feature


        Feature                         Acronym             Status

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

1)      Web Logging                     WL                  ON

2)      Surge Protection                SP                  OFF

.

7) Compression Control CMP ON

8)      Priority Queuing                PQ                  OFF

.

Done

```



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

So aktivieren Sie die Komprimierung über die GUI

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

Konfigurieren von Diensten zum Komprimieren von Daten

Zusätzlich zur globalen Aktivierung der Komprimierung müssen Sie sie für jeden Dienst aktivieren, der komprimierte Dateien bereitstellt.

So aktivieren Sie die Komprimierung für einen Dienst mit der CLI

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

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

```
> show service SVC_HTTP1


SVC_HTTP1 (10.102.29.18:80) - HTTP


State: UP


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


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


Server Name: 10.102.29.18


```



```
Server ID : 0   Monitor Threshold : 0

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

Use Source IP: NO

Client Keepalive(CKA): NO

Access Down Service: NO

TCP Buffering(TCPB): NO

HTTP Compression(CMP): YES

Idle timeout: Client: 180 sec   Server: 360 sec

Client IP: DISABLED

Cacheable: NO

SC: OFF

SP: OFF

Down state flush: ENABLED

1)      Monitor Name: tcp-default

State: DOWN     Weight: 1

Probes: 1095    Failed [Total: 1095 Current: 1095]
```



```
64
65
66 Last response: Failure - TCP syn sent, reset received.
67
68
69 Response Time: N/A
70
71
72 Done
73
74 <!--NeedCopy-->
```

So aktivieren Sie die Komprimierung für einen Dienst mit der GUI

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

Binden einer Komprimierungsrichtlinie an einen virtuellen Server

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

So binden oder lösen Sie die Bindung einer Komprimierungsrichtlinie an einen virtuellen Server mithilfe der Befehlszeile

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

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

Beispiel:

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

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

BoundServiceGroups:
1)GroupName:Service-Group-1

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

1)Policy:ns_cmp_msappPriority:0

Done

<!--NeedCopy-->
```

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

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, an den Sie eine Komprimierungsrichtlinie binden oder aufheben möchten (z. B. vServer-LB-1), und klicken Sie dann auf Öffnen.

3. Klicken Sie im Dialogfeld Virtuellen Server konfigurieren (Lastenausgleich) auf der Registerkarte Richtlinien auf Komprimierung.
4. Führen Sie einen der folgenden Schritte aus:
   - Um eine Komprimierungsrichtlinie zu binden, klicken Sie auf Richtlinie einfügen, und wählen Sie dann die Richtlinie aus, die Sie an den virtuellen Server binden möchten.
   - Um die Bindung einer Komprimierungsrichtlinie aufzuheben, klicken Sie auf den Namen der Richtlinie, die Sie vom virtuellen Server aufheben möchten, und klicken Sie dann auf Richtlinie aufheben.
5. Klicken Sie auf OK.

Sichere Lastenausgleichung durch Verwendung von SSL

October 5, 2021

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

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

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

SSL-Konfigurations-Tasksequenz

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

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

Das folgende Flussdiagramm zeigt die Reihenfolge der Aufgaben zum Konfigurieren einer grundlegenden SSL-Offload-Setup.

Abbildung 1. Abfolge von Tasks zum Konfigurieren von SSL-Offload

SSL-Offload aktivieren

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

Aktivieren von SSL über die CLI

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

```
1 -  enable ns feature SSL
2 -  show ns feature
3 <!--NeedCopy-->
```

Beispiel:

```
1  > enable ns feature ssl
2
3  Done
4
5
6  > show ns feature
7
8
9  Feature Acronym Status
10
11
12 ------- ------- ------
13
14
15 1) Web Logging WL ON
16
17
18 2) SurgeProtection SP OFF
19
20
21 3) Load Balancing LB ON . . .
22
23
24  9) SSL Offloading SSL ON
25
26
```



```
10) Global Server Load Balancing GSLB ON . .


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

Aktivieren von SSL über die GUI

Führen Sie die folgenden Schritte aus:

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

HTTP-Dienste erstellen

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

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

Hinzufügen eines HTTP-Dienstes über die CLI

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

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

Beispiel:

```
> add service SVC_HTTP1 10.102.29.18 HTTP 80


 Done
```



```
5
6
7  > show service SVC_HTTP1
8
9
10         SVC_HTTP1 (10.102.29.18:80) - HTTP
11
12
13         State: UP
14
15
16         Last state change was at Wed Jul 15 06:13:05 2009
17
18
19         Time since last state change: 0 days, 00:00:15.350
20
21
22         Server Name: 10.102.29.18
23
24
25         Server ID : 0   Monitor Threshold : 0
26
27
28         Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
29
30
31         Use Source IP: NO
32
33
34         Client Keepalive(CKA): NO
35
36
37         Access Down Service: NO
38
39
40         TCP Buffering(TCPB): NO
41
42
43         HTTP Compression(CMP): YES
44
45
46         Idle timeout: Client: 180 sec   Server: 360 sec
47
48
49         Client IP: DISABLED
```



```
50
51
52          Cacheable: NO
53
54
55          SC: OFF
56
57
58          SP: OFF
59
60
61          Down state flush: ENABLED
62
63
64
65
66
67  1)      Monitor Name: tcp-default
68
69
70                  State: UP       Weight: 1
71
72
73                  Probes: 4       Failed [Total: 0 Current: 0]
74
75
76                  Last response: Success - TCP syn+ack received.
77
78
79                  Response Time: N/A
80
81
82   Done
83  <!--NeedCopy-->
```

Hinzufügen eines HTTP-Dienstes mit der GUI

Führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Traffic Management > SSL Offload > Services**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Dienst erstellen** den Namen des Dienstes, die IP-Adresse und den Port ein (z. B. SVC_HTTP1, 10.102.29.18 und 80).
4. Wählen Sie in der Liste **Protokoll** den Typ des Dienstes aus (z. B. HTTP).

5. Klicken Sie auf **Erstellen**und dann auf **Schließen**. Der konfigurierte HTTP-Dienst wird auf der Seite Dienste angezeigt.
6. Überprüfen Sie, ob die von Ihnen konfigurierten Parameter korrekt konfiguriert sind, indem Sie den Dienst auswählen und den Abschnitt Details am unteren Rand des Bereichs anzeigen.

Hinzufügen eines SSL-basierten virtuellen Servers

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

Hinzufügen eines SSL-basierten virtuellen Servers mit der CLI

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

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

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

Beispiel:

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


  > show lb vserver vserver-SSL-1


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


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


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



```
15
16
17    Effective State: DOWN Client Idle Timeout: 180 sec
18
19
20    Down state flush: ENABLED
21
22
23    Disable Primary Vserver On Down : DISABLED
24
25
26    No. of Bound Services : 0 (Total) 0 (Active)
27
28
29    Configured Method: LEASTCONNECTION Mode: IP
30
31
32    Persistence: NONE
33
34
35    Vserver IP and Port insertion: OFF
36
37
38    Push: DISABLED Push VServer: Push Multi Clients: NO Push Label Rule:
          Done
39  <!--NeedCopy-->
```

Hinzufügen eines SSL-basierten virtuellen Servers über die GUI

Führen Sie die folgenden Schritte aus:

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

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

Binden von Diensten an den virtuellen SSL-Server

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

Die Datenübertragung zwischen der Appliance und den Servern kann verschlüsselt oder in Klartext erfolgen. Wenn die Datenübertragung zwischen der Appliance und den Servern verschlüsselt ist, ist die gesamte Transaktion von Ende zu Ende sicher. Weitere Informationen zum Konfigurieren des Systems für End-to-End-Sicherheit finden Sie unter SSL-Offload and Acceleration.

Binden eines Dienstes an einen virtuellen Server mit der CLI

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

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

Beispiel:

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



  Done


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


  ADDRESS State: DOWN[Certkey not bound]


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

```



```
17
18    Time since last state change: 0 days, 00:31:53.70
19
20
21    Effective State: DOWN Client Idle
22
23
24    Timeout: 180 sec
25
26
27    Down state flush: ENABLED Disable Primary Vserver On Down :
28
29
30    DISABLED No. of Bound Services : 1 (Total) 0 (Active)
31
32
33    Configured Method: LEASTCONNECTION Mode: IP Persistence: NONE Vserver
          IP and
34
35
36    Port insertion: OFF Push: DISABLED Push VServer: Push Multi Clients:
         NO Push Label Rule:
37
38
39
40
41
42    1) SVC_HTTP1 (10.102.29.18: 80) - HTTP
43
44
45    State: DOWN Weight: 1
46
47
48    Done
49  <!--NeedCopy-->
```

Binden eines Dienstes an einen virtuellen Server mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL Offload > Virtuelle Server**.
2. Wählen Sie im Detailbereich einen virtuellen Server aus, und klicken Sie dann auf **Öffnen**.
3. Aktivieren Sie auf der Registerkarte **Dienste** in der Spalte **Aktiv** die Kontrollkästchen neben den Diensten, die Sie an den ausgewählten virtuellen Server binden möchten.
4. Klicken Sie auf **OK**.

5. Stellen Sie sicher, dass der Leistungsindikator Anzahl gebundener Dienste im Abschnitt Details am unteren Rand des Bereichs um die Anzahl der Dienste erhöht wird, die Sie an den virtuellen Server gebunden haben.

Hinzufügen eines Zertifikatschlüsselpaars

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

ECDSA-Zertifikate mit nur den folgenden Kurven werden unterstützt:

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

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

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

Hinzufügen eines Zertifikatsschlüsselpaars über die CLI

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

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

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

Beispiel:


```
> add ssl certKey CertKey-SSL-1 -cert ns-root.cert -key ns-root.key

 Done


> show sslcertkey CertKey-SSL-1


   Name: CertKey-SSL-1 Status: Valid,


   Days to expiration:4811 Version: 3


   Serial Number: 00 Signature Algorithm: md5WithRSAEncryption Issuer:
      C=US,ST=California,L=San


   Jose,O=Citrix ANG,OU=NS Internal,CN=de fault


   Validity Not Before: Oct 6 06:52:07 2006 GMT Not After : Aug 17
      21:26:47 2022 GMT


   Subject: C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS Internal,
      CN=d efault Public Key


   Algorithm: rsaEncryption Public Key


   size: 1024


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

Hinzufügen eines Zertifikatsschlüsselpaars über die GUI

Führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Traffic Management > SSL > Zertifikate**.

2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld Zertifikat installieren** im Textfeld Certificate-Key Pair Name einen Namen für das Zertifikatschlüsselpaar ein, das Sie hinzufügen möchten, z. B. Certkey-SSL-1.
4. Klicken Sie unter **Details** in Zertifikatdateiname auf **Durchsuchen (Appliance)**, um das Zertifikat zu finden. Sowohl das Zertifikat als auch der Schlüssel werden im Ordner /nsconfig/ssl/ der Appliance gespeichert. Um ein Zertifikat auf dem lokalen System zu verwenden, wählen Sie Lokal aus.
5. Wählen Sie das Zertifikat aus, das Sie verwenden möchten, und klicken Sie dann auf **Auswählen**.
6. Klicken Sie unter Dateiname des privaten Schlüssels auf **Durchsuchen (Appliance)**, um die Datei mit dem privaten Schlüssel zu suchen. Um einen privaten Schlüssel auf dem lokalen System zu verwenden, wählen Sie Lokal aus.
7. Wählen Sie den Schlüssel aus, den Sie verwenden möchten, und klicken Sie auf **Auswählen**. Um den im Zertifikatschlüsselpaar verwendeten Schlüssel zu verschlüsseln, geben Sie das Kennwort für die Verschlüsselung in das Textfeld Kennwort ein.
8. Klicken Sie auf **Installieren**.
9. Doppelklicken Sie auf das Zertifikatschlüsselpaar, und überprüfen Sie im Fenster Zertifikatdetails, ob die Parameter korrekt konfiguriert und gespeichert wurden.

Binden eines SSL-Zertifikatsschlüsselpaars an den virtuellen Server

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

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

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

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

Beispiel:


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

Done

> show ssl vserver Vserver-SSL-1



     Advanced SSL configuration for VServer Vserver-SSL-1:

     DH: DISABLED

     Ephemeral RSA: ENABLED Refresh Count: 0

     Session Reuse: ENABLED Timeout: 120 seconds

     Cipher Redirect: ENABLED

     SSLv2 Redirect: ENABLED

     ClearText Port: 0

     Client Auth: DISABLED

     SSL Redirect: DISABLED

     Non FIPS Ciphers: DISABLED

     SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED

```



```
44
45
46
47
48 1) CertKey Name: CertKey-SSL-1 Server Certificate
49
50
51 1) Cipher Name: DEFAULT
52
53
54    Description: Predefined Cipher Alias
55
56
57 Done
58 <!--NeedCopy-->
```

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

Führen Sie die folgenden Schritte aus:

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

Konfigurieren der Unterstützung für Outlook-Webzugriff

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

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

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

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

- Erstellen Sie eine SSL-Richtlinie.
- Binden Sie die Richtlinie an den virtuellen SSL-Server.

Erstellen einer SSL-Aktion zum Aktivieren der OWA-Unterstützung

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

Erstellen einer SSL-Aktion zum Aktivieren der OWA-Unterstützung über die CLI

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

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

Beispiel:

```
1     > add ssl action Action-SSL-OWA -OWASupport enabled
2
3
4
5
6     Done
7
8
9     > show SSL action Action-SSL-OWA
10
11
12    Name: Action-SSL-OWA
13
14
15    Data Insertion Action: OWA
16
17
18    Support: ENABLED
19
20
21    Done
```



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

Erstellen einer SSL-Aktion zum Aktivieren der OWA-Unterstützung mit der GUI

Führen Sie die folgenden Schritte aus:

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

Erstellen von SSL-Richtlinien

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

Erstellen einer SSL-Richtlinie mit der CLI

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

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

Beispiel:

```
1 > add ssl policy Policy-SSL-1 -rule ns_true -reqaction Action-SSL-OWA
2
3 Done
4
5 > show ssl policy Policy-SSL-1
6
7 Name: Policy-SSL-1 Rule: ns_true
8
9 Action: Action-SSL-OWA Hits: 0
10
```



```
Policy is bound to following entities

1) PRIORITY : 0

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

Erstellen einer SSL-Richtlinie über die GUI

Führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Traffic Management > SSL > Richtlinien**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld Create SSL Policy** im Textfeld Name den Namen der SSL-Richtlinie ein (z. B. Policy-SSL-1).
4. Wählen Sie unter “Aktion **anfordern** “ die konfigurierte SSL-Aktion aus, die Sie dieser Richtlinie zuordnen möchten (z. B. Action-SSL-OWA). Der allgemeine Ausdruck ns_true wendet die Richtlinie auf alle erfolgreichen SSL-Handshake-Datenverkehr an. Um bestimmte Antworten zu filtern, können Sie jedoch Richtlinien mit einer höheren Detailgenauigkeit erstellen. Weitere Informationen zum Konfigurieren granularer Richtlinienausdrücke finden Sie unter SSL-Aktionen und Richtlinien.
5. Wählen Sie in **Benannte Ausdrücke**den integrierten allgemeinen Ausdruck ns_true aus und klicken Sie auf **Ausdruck hinzufügen**. Der Ausdruck ns_true wird jetzt im Textfeld Ausdruck angezeigt.
6. Klicken Sie auf **Erstellen**und dann auf **Schließen**.
7. Überprüfen Sie, ob die Richtlinie korrekt konfiguriert ist, indem Sie die Richtlinie auswählen und den Abschnitt Details unten im Bereich.

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

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

Binden einer SSL-Richtlinie an einen virtuellen SSL-Server über die CLI

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


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

Beispiel:

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

 Done

> show ssl vserver Vserver-SSL-1

Advanced SSL configuration for VServer Vserver-SSL-1:

DH: DISABLED

Ephemeral RSA: ENABLED

Refresh Count: 0

Session Reuse: ENABLED

Timeout: 120 seconds

Cipher Redirect: ENABLED

SSLv2 Redirect: ENABLED

ClearText Port: 0

Client Auth: DISABLED

SSL Redirect: DISABLED

Non FIPS Ciphers: DISABLED

SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED

1) CertKey Name: CertKey-SSL-1 Server Certificate

1) Policy Name: Policy-SSL-1 Priority: 0

1) Cipher Name: DEFAULT Description: Predefined Cipher Alias
```



```
38
39 Done
40 <!--NeedCopy-->
```

Binden einer SSL-Richtlinie an einen virtuellen SSL-Server über die GUI

Führen Sie die folgenden Schritte aus:

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

Funktionen auf einen Blick

October 5, 2021

Citrix ADC Funktionen können unabhängig oder in Kombination konfiguriert werden, um spezifische Anforderungen zu erfüllen. Obwohl einige Features in mehr als einer Kategorie passen, können die zahlreichen Citrix ADC Funktionen im Allgemeinen als Anwendungswechsel und Verkehrsverwaltungsfunktionen, Anwendungsbeschleunigungsfunktionen sowie Anwendungssicherheits- und Firewallfunktionen sowie Anwendungssichtbarkeitsfunktion kategorisiert werden.

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

Anwendungsumschaltung und Traffic-Management-Funktionen

October 5, 2021

Im Folgenden finden Sie die Funktionen der Anwendungsumschaltung und des Verkehrsmanagements.

SSL-Offload

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

Weitere Informationen finden Sie unter SSL-Offload und Beschleunigung.

Zugriffssteuerungslisten

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

Weitere Informationen finden Sie unter Zugriffssteuerungsliste.

Lastausgleich

Entscheidungen zum Lastenausgleich basieren auf einer Vielzahl von Algorithmen, einschließlich Round Robin, geringste Verbindungen, gewichtete geringste Bandbreite, gewichtete kleinste Pakete, minimale Reaktionszeit und Hashing basierend auf URL, Domänenquell-IP oder Ziel-IP. Sowohl das TCP als auch das UDP-Protokoll werden unterstützt, sodass die Citrix ADC Appliance den gesamten Datenverkehr ausgleichen kann, der diese Protokolle als zugrunde liegenden Träger verwendet (z. B. HTTP, HTTPS, UDP, DNS, NNTP und allgemeiner Firewall-Datenverkehr). Darüber hinaus kann die ADC-Appliance die Sitzungsbeständigkeit basierend auf Quell-IP-, Cookie-, Server-, Gruppen- oder SSL-Sitzung aufrechterhalten. Es ermöglicht Benutzern, benutzerdefinierte Extended Content Verification (ECV) auf Server, Caches, Firewalls und andere Infrastrukturgeräte anzuwenden, um sicherzustellen, dass diese Systeme ordnungsgemäß funktionieren und den Benutzern den richtigen Inhalt bereitstellen. Es kann auch Integritätsprüfungen mit Ping-, TCP- oder HTTP-URL durchführen, und der Benutzer kann Monitore basierend auf Perl-Skripten erstellen.
Um eine umfassende WAN-Optimierung zu ermöglichen, können die CloudBridge-Appliances, die in Rechenzentren bereitgestellt werden, über Citrix ADC Appliances Lastausbalanciert werden. Die Bandbreite und Anzahl gleichzeitiger Sitzungen lassen sich erheblich verbessern.

Weitere Informationen finden Sie unter Load Balancing.

Traffic-Domänen

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

Weitere Informationen finden Sie unter Traffic-Domains.

Netzwerkadressübersetzung

Network Address Translation (NAT) beinhaltet die Änderung der Quell- und/oder Ziel-IP-Adressen und/oder der TCP/UDP-Portnummern von IP-Paketen, die die Citrix ADC Appliance passieren. Wenn Sie NAT auf der Appliance aktivieren, erhöht sich die Sicherheit Ihres privaten Netzwerks und schützt es vor einem öffentlichen Netzwerk wie dem Internet, indem Sie die Quell-IP-Adressen Ihres Netzwerks ändern, wenn Daten über die Citrix ADC Appliance weitergeleitet werden.

Die Citrix ADC Appliance unterstützt die folgenden Arten der Netzwerkadressübersetzung:

INAT: In Inbound NAT (INAT) überwacht eine IP-Adresse (normalerweise öffentlich), die auf der Citrix ADC Appliance konfiguriert ist, Verbindungsanforderungen im Namen eines Servers. Bei einem Anforderungspaket, das von der Appliance an einer öffentlichen IP-Adresse empfangen wird, ersetzt der ADC die Ziel-IP-Adresse durch die private IP-Adresse des Servers. Mit anderen Worten, die Appliance fungiert als Proxy zwischen Clients und dem Server. Die INAT-Konfiguration umfasst INAT-Regeln, die eine 1:1 -Beziehung zwischen der IP-Adresse auf der Citrix ADC Appliance und der IP-Adresse des Servers definieren.

RNAT: In der Reverse Network Address Translation (RNAT) ersetzt die Citrix ADC Appliance bei einer von einem Server initiierten Sitzung die Quell-IP-Adresse in den vom Server generierten Paketen durch eine IP-Adresse (Typ SNIP), die auf der Appliance konfiguriert ist. Die Appliance verhindert dadurch, dass die IP-Adresse des Servers in einem der vom Server generierten Pakete angezeigt wird. Eine RNAT Konfiguration beinhaltet eine RNAT Regel, die eine Bedingung angibt. Die Appliance führt RNAT für die Pakete aus, die der Bedingung entsprechen.

Stateless NAT46 Translation: Stateless NAT46 ermöglicht die Kommunikation zwischen IPv4- und IPv6-Netzwerken über IPv4- zu IPv6-Paketübersetzung und umgekehrt, ohne dass Sitzungsinforma-

tionen auf der Citrix ADC Appliance verwaltet werden. Eine statuslose NAT46-Konfiguration umfasst eine IPv4-IPv6-INAT-Regel und ein NAT46-IPv6-Präfix.

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

Weitere Informationen finden Sie unter Konfigurieren der Netzwerkadressübersetzung.

Multipath-TCP-Unterstützung

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

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

Content Switching

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

Weitere Informationen finden Sie unter Content Switching.

Globaler Serverlastenausgleich (GSLB)

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

Weitere Informationen finden Sie unter Globaler Server-Lastenausgleich.

Dynamisches Routing

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

Weitere Informationen finden Sie unter Konfigurieren dynamischer Routen.

Link-Lastenausgleich

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

Weitere Informationen finden Sie unter Link Load Balancing.

TCP-Optimierung

Sie können TCP-Profile verwenden, um den TCP-Datenverkehr zu optimieren. TCP-Profile definieren, wie virtuelle NetScaler Server TCP-Datenverkehr verarbeiten. Administratoren können die integrierten TCP-Profile verwenden oder benutzerdefinierte Profile konfigurieren. Nachdem Sie ein TCP-Profil definiert haben, können Sie es an einen einzelnen virtuellen Server oder an mehrere virtuelle Server binden.

Einige der wichtigsten Optimierungsfunktionen, die von TCP-Profilen aktiviert werden können, sind:

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

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

CloudBridge-Connector

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

Weitere Informationen finden Sie unter CloudBridge.

DataStream

Die NetScaler DataStream Funktion bietet einen intelligenten Mechanismus für die Anforderungsumschaltung auf der Datenbankebene, indem Anforderungen auf der Grundlage der gesendeten SQL-Abfrage verteilt werden.

Bei der Bereitstellung vor Datenbankservern sorgt ein NetScaler für eine optimale Verteilung des Datenverkehrs von den Anwendungsservern und Webservern. Administratoren können Datenverkehr gemäß Informationen in der SQL-Abfrage und auf Basis von Datenbanknamen, Benutzernamen, Zeichensätzen und Paketgröße segmentieren.

Sie können den Lastenausgleich so konfigurieren, dass Anforderungen gemäß Lastausgleichsalgorithmen gewechselt werden, oder Sie können die Switching-Kriterien ausarbeiten, indem Sie Content Switching so konfigurieren, dass eine Entscheidung getroffen wird, die auf SQL-Abfrageparametern wie Benutzername, Datenbanknamen und Befehlsparameter basiert. Sie können Monitore weiter konfigurieren, um die Zustände von Datenbankservern zu verfolgen.

Die erweiterte Richtlinieninfrastruktur auf der Citrix ADC Appliance enthält Ausdrücke, mit denen Sie die Anforderungen auswerten und verarbeiten können. Die erweiterten Ausdrücke bewerten den Datenverkehr, der mit MySQL Datenbankservern verbunden ist. Sie können anforderungsbasierte Ausdrücke (Ausdrücke, die mit MYSQL.CLIENT und MYSQL.REQ beginnen) in erweiterten Richtlinien

verwenden, um Anforderungswechselentscheidungen am Content Switching den virtuellen Server-Bindpunkt und antwortbasierte Ausdrücke (Ausdrücke, die mit MYSQL.RES beginnen) zu treffen, um Serverantworten an Benutzer auszuwerten. konfigurierte Integritätsüberwachungen.

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

Weitere Informationen finden Sie unter DataStream.

Funktionen für Anwendungsbeschleunigung

October 5, 2021

- AppCompress

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

- Cacheumleitung

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

  Weitere Informationen finden Sie unter Cache-Umleitung.

- AppCache

  Optimiert die Bereitstellung von Webinhalten und Anwendungsdaten, indem ein schnelles In-Memory-HTTP/1.1- und HTTP/1.0-kompatibles Web-Caching für statische und dynamische Inhalte bereitgestellt wird. Dieser integrierte Cache speichert die Ergebnisse eingehender Anwendungsanforderungen, selbst wenn eine eingehende Anforderung gesichert oder die Daten komprimiert werden. Anschließend werden die Daten wiederverwendet, um nachfolgende Anforderungen für die gleichen Informationen zu erfüllen. Durch die direkte Bereitstellung von Daten aus dem integrierten Cache kann die Appliance die Regenerierungszeiten von Seiten reduzieren, da keine statischen und dynamischen Inhaltsanforderungen an den Server übertragen werden müssen.

  Weitere Informationen finden Sie unter Integriertes Caching.

- TCP-Pufferung

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

Anwendungssicherheit und Firewall-Funktionen

September 28, 2022

Nachfolgend sind die Sicherheits- und Firewall-Funktionen aufgeführt.

Inhaltsfilterung

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

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

Weitere Informationen finden Sie unter Inhaltsfilterung.

Responder

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

Weitere Informationen finden Sie unter Responder.

Rewrite

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

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

Weitere Informationen finden Sie unter Rewrite.

Prioritätsqueuing

Priorisiert Benutzeranfragen, um sicherzustellen, dass der wichtigste Datenverkehr bei einem Anstieg des Anforderungsvolumens zuerst bedient wird. Sie können die Priorität basierend auf Anforderungs-URLs, Cookies oder einer Vielzahl anderer Faktoren festlegen. Die Appliance platziert Anforderungen in einer dreistufigen Warteschlange basierend auf ihrer konfigurierten Priorität, sodass geschäftskritische Transaktionen auch bei Überspannungen oder Standortangriffen reibungslos ablaufen können.

Weitere Informationen finden Sie unter Priority Queuing.

Überlastungsschutz

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

Weitere Informationen finden Sie unter Überlastungsschutz.

Citrix Gateway

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

Weitere Informationen finden Sie unter Citrix Gateway.

Anwendungs-Firewall

Schützt Anwendungen vor Missbrauch durch Hacker und Malware, wie Cross-Site-Scripting-Angriffe, Pufferüberlauf-Angriffe, SQL-Injection-Angriffe und kraftvolles Surfen, indem der Datenverkehr zwischen jedem geschützten Webserver und Benutzern gefiltert wird, die eine Verbindung zu einer beliebigen Website auf diesem Webserver herstellen. Die Anwendungsfirewall untersucht den gesamten

Datenverkehr auf Hinweise auf Angriffe auf Webserversicherheit oder Missbrauch von Webserverressourcen und ergreift geeignete Maßnahmen, um den Erfolg dieser Angriffe zu verhindern.

Weitere Informationen finden Sie unter Anwendungs-Firewall.

Sichtbarkeitsfunktion für Anwendungen

October 5, 2021

- Citrix Application Delivery Management

  Citrix Application Delivery Management (ADM) ist ein Hochleistungssammler, der End-to-End-User Experience Transparenz über den Web- und HDX-Datenverkehr (ICA) bietet. Es sammelt HTTP- und ICA-AppFlow-Datensätze, die von Citrix ADC Appliances generiert wurden, und füllt analytische Berichte über Layer 3- bis Layer-7-Statistiken aus. Citrix ADM bietet eingehende Analysen für die letzten fünf Minuten an Echtzeitdaten und für historische Daten, die für die letzte Stunde, einen Tag, eine Woche und einen Monat gesammelt wurden.

  HDX (ICA) Analytisches Dashboard ermöglicht es Ihnen, einen Drilldown von HDX-Benutzern, Anwendungen, Desktops und sogar von Informationen auf Gatewayebene durchzuführen. Entsprechend bietet HTTP-Analysen eine Vogelperspektive von Webanwendungen, auf die zugegriffen wird, Client-IP-Adressen und Server-IP-Adressen und anderen Dashboards. Der Administrator kann einen Drilldown durchführen und die Problempunkte in jedem dieser Dashboards identifizieren, je nach Anwendungsfall.

- Verbesserte Anwendungstransparenz mit AppFlow

  Die Citrix ADC Appliance ist ein zentraler Kontrollpunkt für den gesamten Anwendungsverkehr im Rechenzentrum. Es sammelt Informationen auf Fluss- und Benutzersitzungsebene, die für die Überwachung der Anwendungsleistung, Analyse und Business Intelligence-Anwendungen nützlich sind. AppFlow überträgt diese Informationen mithilfe des IPFIX-Formats (Internet Protocol Flow Information Export), bei dem es sich um einen offenen IETF-Standard (Internet Engineering Task Force) handelt, der in RFC 5101 definiert ist. IPFIX (die standardisierte Version von NetFlow von Cisco) wird häufig zur Überwachung von Netzwerkflussinformationen verwendet. AppFlow definiert neue Informationselemente, um Informationen auf Anwendungsebene darzustellen.

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

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

Sie können AppFlow für einen virtuellen Server aktivieren, um die zu überwachenden Flows durch Stichproben und Filtern des Anwendungsdatenverkehrs zu begrenzen. AppFlow kann auch Statistiken für den virtuellen Server bereitstellen.

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

Weitere Informationen finden Sie unter AppFlow.

- Stream-Analysen

  Die Leistung Ihrer Website oder Anwendung hängt davon ab, wie gut Sie die Bereitstellung der am häufigsten angeforderten Inhalte optimieren. Techniken wie Caching und Komprimierung tragen dazu bei, die Bereitstellung von Services für Kunden zu beschleunigen, aber Sie müssen in der Lage sein, die am häufigsten angeforderten Ressourcen zu identifizieren und diese dann zwischenspeichern oder komprimieren. Sie können die am häufigsten verwendeten Ressourcen identifizieren, indem Sie Echtzeitstatistiken über Website-oder Anwendungsdatenverkehr aggregieren. Statistiken wie häufig auf eine Ressource im Verhältnis zu anderen Ressourcen zugegriffen wird und wie viel Bandbreite von diesen Ressourcen verbraucht wird, helfen Ihnen zu bestimmen, ob diese Ressourcen zwischengespeichert oder komprimiert werden müssen, um die Serverleistung und die Netzwerkauslastung zu verbessern. Statistiken wie Antwortzeiten und die Anzahl gleichzeitiger Verbindungen mit der Anwendung helfen Ihnen, festzustellen, ob Sie serverseitige Ressourcen verbessern müssen.

  Wenn sich die Website oder Anwendung nicht häufig ändert, können Sie Produkte verwenden, die statistische Daten sammeln, und dann die Statistiken manuell analysieren und die Bereitstellung von Inhalten optimieren. Wenn Sie jedoch keine manuellen Optimierungen durchführen möchten oder Ihre Website oder Anwendung dynamisch ist, benötigen Sie eine Infrastruktur, die nicht nur statistische Daten sammeln kann, sondern auch die Bereitstellung von Ressourcen basierend auf den Statistiken automatisch optimieren kann. Auf der Citrix ADC Appliance wird diese Funktionalität durch die Funktion Stream Analytics bereitgestellt. Die Funktion arbeitet auf einer einzelnen Citrix ADC Appliance und sammelt Laufzeitstatistiken basierend auf den von Ihnen definierten Kriterien. Bei Verwendung mit Citrix ADC Richtlinien bietet das Feature auch die Infrastruktur, die Sie für die automatische Optimierung des Datenverkehrs in Echtzeit benötigen.

  Weitere Informationen finden Sie unter Aktionsanalysen.

Citrix ADC Lösungen

October 5, 2021

Citrix ADC Lösungen vereinfachen die Einrichtung häufig bereitgestellter Konfigurationen. Überprüfen Sie diesen Raum von Zeit zu Zeit, um zusätzliche Lösungen zu erhalten.

Dieser Abschnitt enthält die folgenden Lösungen.

- Einrichten von Citrix ADC für Citrix Virtual Apps and Desktops
- Voreinstellung für globale Server Load Balancing (GSLB)
- Anycast-Unterstützung in Citrix ADC
- Bereistellen einer digitale Werbeplattform auf AWS mit Citrix ADC
- Verbesserung der Clickstream-Analytik in AWS mit Citrix ADC
- Citrix ADC in einer privaten Cloud verwaltet von Microsoft Windows Azure Pack und Cisco ACI

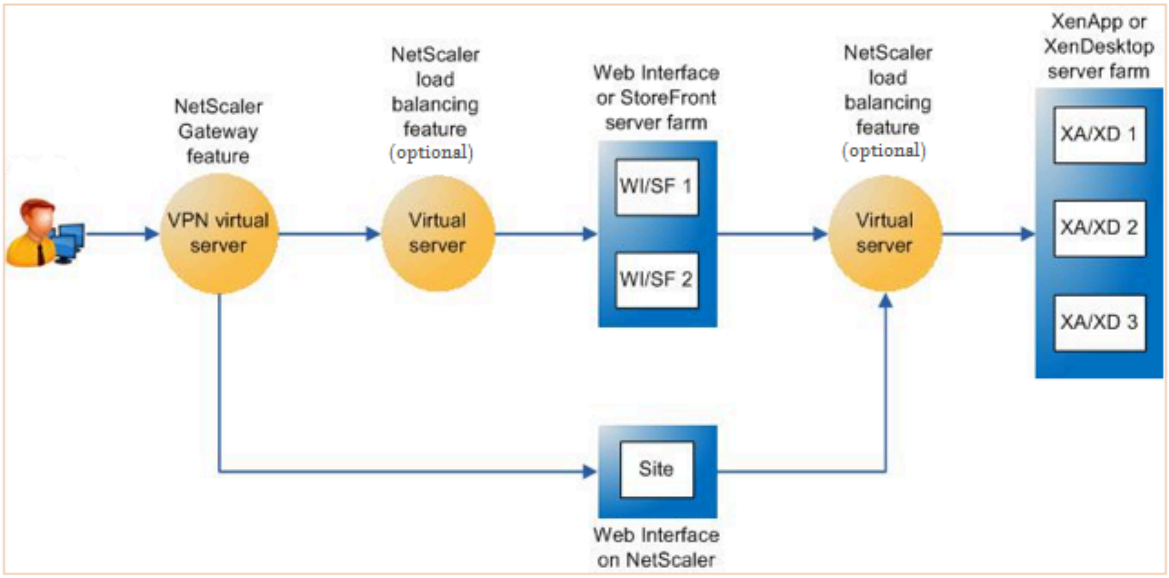
Einrichten von Citrix ADC für Citrix Virtual Apps and Desktops

October 5, 2021

Eine Citrix ADC Appliance kann Lastausgleich und sicheren Remote-Zugriff auf Ihre Citrix Virtual Apps and Desktops-Anwendungen ermöglichen. Sie können die Citrix ADC Load Balancing-Funktion verwenden, um den Datenverkehr auf den Citrix Virtual Apps and Desktops Server zu verteilen. Sie können die Citrix Gateway Funktion verwenden, um sicheren Remote-Zugriff auf die Server zu ermöglichen.

Citrix ADC kann außerdem den Datenverkehr beschleunigen und optimieren und Sichtbarkeitsfunktionen bieten, die für Citrix Virtual Apps and Desktops-Bereitstellungen nützlich sind.

Abbildung 1. Citrix ADC Appliance in Citrix Virtual Apps and Desktops Setup



Die vorangehende Abbildung zeigt die an dieser Bereitstellung beteiligten Komponenten:

- **NetScaler Gateway.** Stellt die URL für den Benutzerzugriff bereit und bietet Sicherheit durch Authentifizierung der Benutzer.
- **Citrix ADC Lastenausgleichsserver.** Der Lastausgleich des Datenverkehrs für das Webinterface oder StoreFront -Server. Sie können auch einen virtuellen Lastausgleichsserver vor den Citrix Virtual Apps und Desktop-Servern bereitstellen, um Schlüsselkomponenten wie XML-Broker und DDC-Server (Desktop Delivery Controller) auszugleichen.
- **Webinterface oder StoreFront oder Webinterface auf Citrix ADC.** Stellt die Schnittstelle bereit, über die Sie auf die Anwendungen zugreifen können.

  Hinweis: Webinterface auf Citrix ADC (WIonNS) ist eine Anpassung des Webinterface-Produkts, das auf der Citrix ADC-Appliance gehostet wird.
- **Citrix Virtual Apps and Desktops.** Stellt die Anwendungen bereit, auf die Ihre Benutzer zugreifen möchten.

So richten Sie Citrix ADC für Citrix Virtual Apps and Desktops über die Citrix ADC GUI ein

Voraussetzungen

- Citrix Virtual Apps und Desktop-Server sind konfiguriert und verfügbar.
- Webinterface, StoreFront oder Webinterface auf Citrix ADC -Servern sind konfiguriert und verfügbar.

- Sie verfügen über Kenntnisse in Citrix Gateway, Citrix ADC, Citrix Virtual Apps and Desktops sowie StoreFront/Webinterface/Webinterface unter Citrix ADC.
- Stellen Sie sicher, dass Sie einen virtuellen Server und einen Dienst konfiguriert und den Dienst an den virtuellen Server gebunden haben. Weitere Informationen:
  - Lastenausgleich für XenDesktop
  - Lastenausgleich XenApp

Vorgehensweise:

1. Melden Sie sich bei der Citrix ADC Appliance an, und klicken Sie auf der Registerkarte **Konfiguration** auf **XenApp und XenDesktop**.
2. Klicken Sie im **Detailbereich** auf **Erste Schritte**. Wenn das Setup auf dem Citrix ADC vorhanden ist, klicken Sie auf den Link **Bearbeiten**, der jedem Abschnitt entspricht, den Sie ändern möchten.
3. Wählen Sie das Produkt (StoreFront, Webinterface oder Webinterface auf Citrix ADC) aus, das in Ihrer Bereitstellung die Schnittstelle für den Zugriff auf die Citrix Virtual Apps and Desktops-Anwendungen bereitstellt.
4. Richten Sie den sicheren Remote-Zugriff ein.
   a) Geben Sie im Abschnitt **NetScaler Gateway -Einstellungen** die Details für den virtuellen VPN-Server an und klicken Sie auf **Weiter**.
   b) Wählen Sie im Abschnitt **Serverzertifikat** ein vorhandenes Zertifikat aus oder installieren Sie ein neues Zertifikat und klicken Sie auf **Weiter**.
   c) Konfigurieren Sie im Abschnitt **Authentifizierung** den zu verwendenden primären Authentifizierungsmechanismus, geben Sie die Serverdetails an, oder verwenden Sie einen vorhandenen Server, und klicken Sie auf **Weiter**.
   d) Geben Sie im Abschnitt **StoreFront** die Details des Servers an, der die Schnittstelle für den Zugriff auf die Anwendungen bereitstellt, und klicken Sie auf **Weiter**.
   e) Sie können einen der folgenden Schritte als StoreFront -Server verwenden.
      i. Virtueller LB-Server, der auf mehrere SF-Server verweist.
      ii. Webinterface oder StoreFront-Server können direkt von der Citrix ADC Appliance aus erreicht werden.
      iii. Webinterface auf Citrix ADC.
5. Klicken Sie auf **Fertig**, um die Konfiguration abzuschließen.

Voreinstellung für globale Server Load Balancing (GSLB)

October 5, 2021

Die SSLB-betriebene Zonenpräferenz ist eine Funktion, die Citrix Virtual Apps and Desktops, StoreFront und Citrix ADC integriert, um Clients Zugriff auf das optimierteste Rechenzentrum basierend auf dem Clientstandort zu ermöglichen.

In einer verteilten Bereitstellung von Citrix Virtual Apps and Desktops wählt StoreFront möglicherweise kein optimales Rechenzentrum aus, wenn mehrere äquivalente Ressourcen von mehreren Rechenzentren verfügbar sind. In solchen Fällen wählt StoreFront nach dem Zufallsprinzip ein Rechenzentrum aus. Es kann die Anfrage an jeden der Citrix Virtual Apps and Desktops s-Server in jedem Rechenzentrum senden, unabhängig von der Nähe zum Client, der die Anfrage stellt.

Die Client-IP-Adresse wird untersucht, wenn eine HTTP-Anfrage bei der Citrix Gateway -Appliance eingeht. Die tatsächliche Client-IP-Adresse wird verwendet, um die Liste der Vorlieben für Rechenzentren zu erstellen, die an StoreFront weitergeleitet wird. Wenn die Citrix ADC Appliance so konfiguriert ist, dass der Zoneneinstellungsheader eingefügt wird, kann StoreFront 3.5 oder höher die von der Appliance bereitgestellten Informationen verwenden, um die Liste der Delivery Controller neu anzuordnen und eine Verbindung mit einem optimalen Delivery Controller in derselben Zone wie der Client herzustellen. StoreFront wählt den optimalen virtuellen Gateway-VPN-Server für die ausgewählte Rechenzentrumszone aus, fügt diese Informationen der ICA-Datei mit den entsprechenden IP-Adressen hinzu und sendet sie an den Client. StoreFront versucht dann, Anwendungen zu starten, die auf den Delivery Controllern des bevorzugten Rechenzentrums gehostet werden, bevor versucht wird, gleichwertige Controller in anderen Rechenzentren zu kontaktieren.

Weitere Informationen zum Konfigurieren dieser Lösung finden Sie hier.

Für eine Videoübersicht über GSLB-basierte Zonenpräferenzlösung klicken Sie aufhttps://www.youtube.com/watch?v=Y8DELum0Xp0.

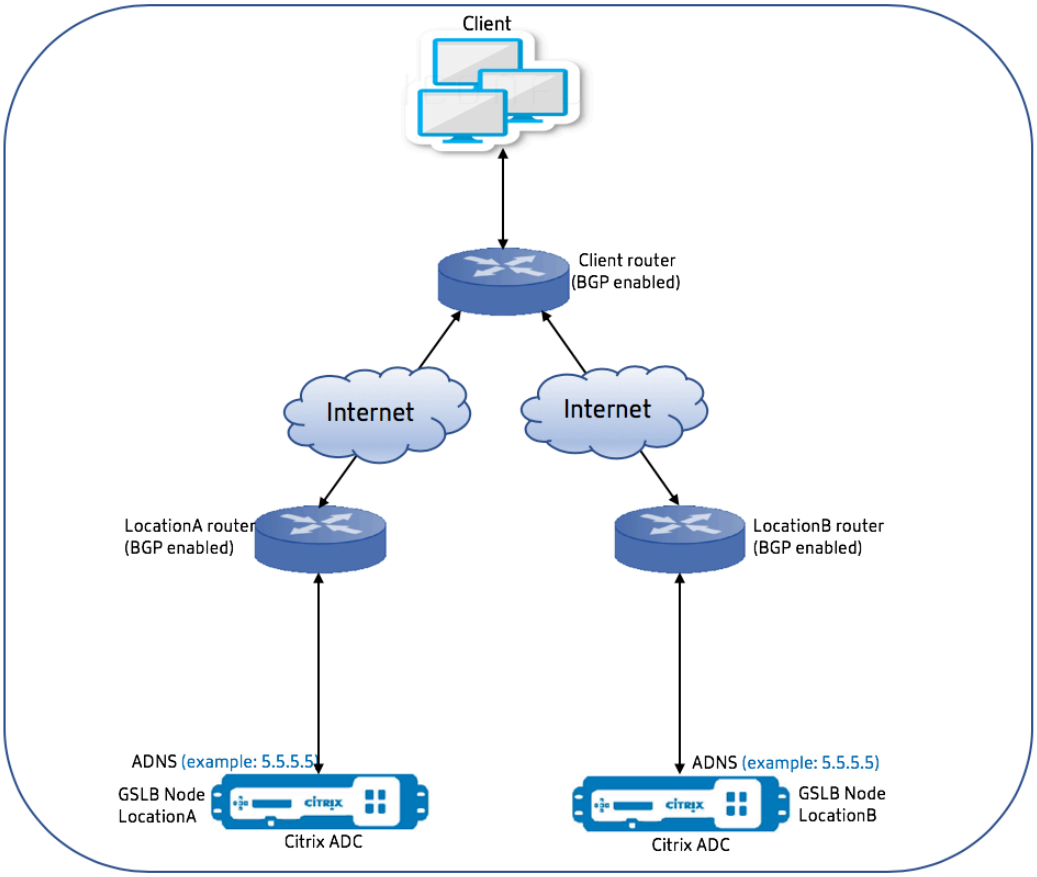
Anycast-Unterstützung in Citrix ADC

October 5, 2021

Anycast ist eine Art von Netzwerk, in dem eine Gruppe von Servern eine IP-Adresse teilt. Die Clientanforderung wird basierend auf ihren Routingtabellen an den topografisch nächstgelegenen Server weitergeleitet. Dieses Routing reduziert Latenzprobleme, sorgt für hohe Verfügbarkeit und minimiert Ausfallzeiten.

Citrix ADC unterstützt Anycast-Netzwerk mit Global Server Load Balancing (GSLB) und DNS-Funktionen.

Das folgende Diagramm veranschaulicht ein Topologiediagramm von Anycast in Citrix ADC.



Anycast GSLB

Die Citrix ADC GSLB-Funktion bietet Lastausgleich an global verteilten Standorten zusammen mit Disaster Recovery und gewährleistet eine kontinuierliche Verfügbarkeit von Anwendungen.

Bei einem Ausfall bietet GSLB eine sofortige Notfallwiederherstellung, indem Datenverkehr zum nächstgelegenen oder leistungsstärksten Rechenzentrum weitergeleitet wird. Die GSLB kann jedoch Folgendes nicht kontrollieren:

- Wie wird der DNS-Verkehr an GSLB-Knoten an verschiedenen geografischen Standorten weitergeleitet?
- Wie viel Latenz hinzugefügt wird, während DNS-Abfragen an GSLB-Knoten weitergeleitet werden.

In einem typischen GSLB-Setup verfügt jedes Rechenzentrum über einen GSLB-Knoten, der mit dem standortspezifischen Autoritative Domain Name Server (ADNS) konfiguriert ist, um DNS-Abfragen zu empfangen. Der ADNS jedes Standorts wird als Nameserver im DNS-Resolver konfiguriert. Wenn die Anzahl der GSLB-Knoten zunimmt, erhöht sich auch die Anzahl der Nameserver-Datensätze. In

solchen Fällen muss LDNS bei einem Ausfall eines Rechenzentrums die Auflösung mit einem anderen Nameserver wiederholen. Diese Wiederholung erhöht die Latenz in der DNS-Auflösung.
Jedes Mal, wenn ein GSLB-Knoten hinzugefügt wird, müssen die Nameserver-Datensätze aktualisiert werden .

Um diese Nachteile zu überwinden, können Sie Anycast ADNS verwenden. In Anycast ADNS wird eine einzelne ADNS-IP-Adresse für alle GSLB-Knoten verwendet und der DNS-Datenverkehr wird über dynamisches Routing an GSLB-Knoten weitergeleitet.

Wenn eine GSLB-Site beispielsweise DOWN ist, wird die Routingtabelle aktualisiert und die Route zu dieser Site wird entfernt. Daher werden die DNS-Abfragen nicht an die Websites gesendet, die DOWN sind. Infolgedessen gibt es keine Wiederholungen.

Wenn ein neuer GSLB-Knoten hinzugefügt wird, wird dem neuen Knoten dieselbe ADNS-IP-Adresse zugewiesen. Das dynamische Routing aktualisiert automatisch die Routingtabellen mit Routen zu neuen Standorten basierend auf den Routingalgorithmen. Daher müssen Sie die DNS-Namensserver-Einträge nicht aktualisieren. Der Rollout neuer GSLB-Standorte wird mit Anycast einfacher und schneller gestaltet.

So konfigurieren Sie eine ADNS-IP-Adresse in einem Anycast-Modus

Aktivieren Sie das Host-Routing auf der ADNS-IP in einer Citrix ADC Appliance und legen Sie die entsprechende Route Health Injection (RHI) -Ebene fest. Meistens gäbe es keine virtuellen Server auf der ADNS IP und daher muss RHI Level als NONE ausgewählt werden. Durch Aktivieren der Hostroute auf der ADNS-IP wird sie zu einer Kernelroute. Sie können dann das dynamische Routing Ihrer Wahl aktivieren und das Routingprotokoll so konfigurieren, dass die Kernel-Routen neu verteilt werden.

ADNS-IP-Konfiguration - Beispiel

Geben Sie an der Eingabeaufforderung;

```
add service adns_public 5.5.5.5 ADNS 53

set ip 5.5.5.5 -hostRoute ENABLED -vserverRHILevel ALL_VSERVERS
<!--NeedCopy-->
```

BGP-Konfiguration im GSLB-Standort - Beispiel

```
Site1#sh run
```



```
!
hostname Site1
!
log syslog
log record-priority
!
ns route-install bgp
!
interface lo0
 ip address 127.0.0.1/8
 ipv6 address fe80::1/64
 ipv6 address ::1/128
!
interface vlan0
 ip address 10.102.148.94/25
 ipv6 address fe80::e84c:f4ff:fe74:4588/64
!
interface vlan2
 ip address 172.18.30.15/24
!
router bgp 5
 redistribute kernel -----> redistributing the kernel routes
 neighbor 172.18.30.30 remote-as 4
 neighbor 172.18.30.30 advertisement-interval 1
 neighbor 172.18.30.30 timers 4 16
!
End

Site1#
<!--NeedCopy-->
```

GSLB-Standort-Routingtabelle - Beispiel

```
Site1#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, I - Intranet
       * - candidate default

K       5.5.5.5/32 via 0.0.0.0 ---------------------------------------->
```



```
      Kernel Route for ADNS
C       10.102.148.0/25 is directly connected, vlan0
C       127.0.0.0/8 is directly connected, lo0
B       172.18.10.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
B       172.18.20.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
C       172.18.30.0/24 is directly connected, vlan2
B       192.168.3.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
B       192.168.5.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h
B       192.168.10.0/24 [20/0] via 172.18.30.30, vlan2, 01w5d22h

Gateway of last resort is not set
Site1#
<!--NeedCopy-->
```

Anycast DNS

Sie können Anycast DNS für virtuelle DNS-Proxyserver auf Citrix ADC verwenden. Wenn mehrere DNS-Namensserver konfiguriert sind, reagiert der DNS-Resolver basierend auf Round-Robin-Methode. Wenn der Resolver beispielsweise keine Antwort vom ersten Server erhält, wechselt er nach Ablauf des konfigurierten Timeout-Werts zum zweiten Server. Der Wechsel vom ersten Server zum zweiten Server erhöht die Latenz in der DNS-Auflösung. Wenn die DNS-Resolver mit Anycast konfiguriert sind, kann diese Latenz eliminiert werden.

DNS-Konfiguration - Beispiel

Geben Sie an der Eingabeaufforderung;

```
add lb vserver dns DNS 5.5.5.50 53

set ip 5.5.5.50 -hostRoute ENABLED -vserverRHILevel ALL_VSERVERS
<!--NeedCopy-->
```

Bereistellen einer digitale Werbeplattform auf AWS mit Citrix ADC

October 5, 2021

Mit dem sich entwickelnden Charakter digitaler Plattformen steht eine Vielzahl von Werbeanwendungen zur Verfügung. Zum Beispiel soziale Medien, Direct Mail, Videos, Banner, Pops, Interstitials, Rich Media und so weiter. Werbetreibende setzen schnell Videonwerbenetzwerke auf und machen fast

40% des Werbeverkehrs aus. Angesichts der stärkeren Nutzung von Mobiltelefonen durch moderne Benutzer hat das Schalten von Videoanzeigen auf der mobilen Plattform jedoch einen erheblichen Anstieg verzeichnet.

Die digitalen Werbeplattformen stehen vor mehreren Herausforderungen. Einige der Herausforderungen sind:

- Sicherheitsbedrohungen
- Hohe Betriebskosten
- Eine große Auswahl an Geräten steht zur Verfügung, um Datenverkehr über das Internet zu senden. Die verschiedenen Protokolle für Echtzeitkommunikation stellen folgende Herausforderungen dar:
  - WebRTC
  - Adaptives Streaming
  - UDP für Video, wobei WebRTC UDP über HTTP verwendet

Um mit dem komplexen Verhalten von Werbeplattformen umzugehen, bietet die Citrix ADC Lösung mit ihrer gesamten Suite von Funktionen und Funktionen, die gut in AWS integriert sind, einen sofortigen, sicheren und zuverlässigen Zugriff auf digitalen Werbeinventar, überall und jederzeit. Citrix ADC spielt eine entscheidende Rolle bei der Bereitstellung der SaaS und Web-Apps für digitale Plattformen.

Integration der digitalen Werbeplattform mit Citrix ADC

Übersicht über die digitale Werbeplattform

Die digitale Werbeplattform besteht aus den folgenden Schlüsselkomponenten:

- Werbe-Austausch
- Ad-Netzwerk
- Demand-Side-Plattform (DSP)
- Versorgungsseite Plattform (SSP)
- Echtzeit-Gebotssysteme (RTB)

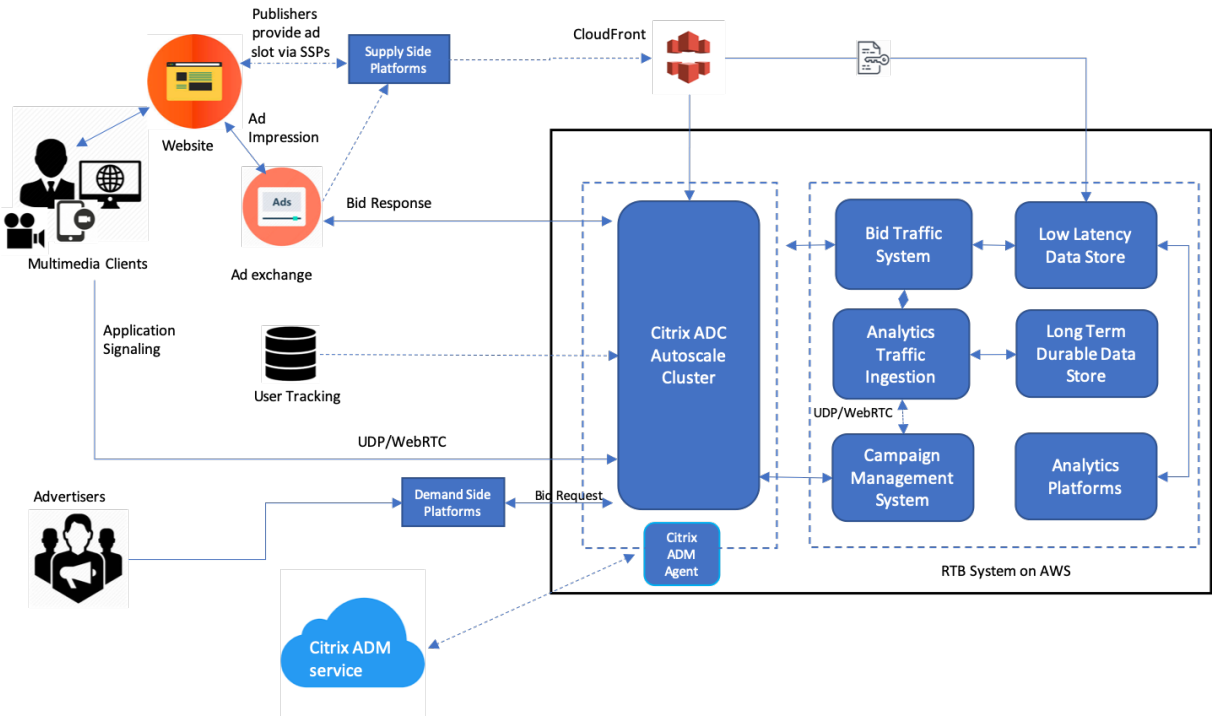
Ein Überblick über den in einem Werbesystem verfolgten Prozess ist wie folgt.

- Die erste Transaktion findet statt, wenn der Benutzer die Website besucht.
- Dies löst eine Angebots-/Werbeanfrage (einschließlich demografischer Informationen des Nutzers) aus, die an den Anzeigenserver oder Publisher gesendet wird, der sich an einen Anzeigenaustausch wendet.
- Die Werbeverlage senden die Werbeanfrage über SSPs an einen Werbebörse.
- Die Anzeigenbörse übermittelt diese Anfrage und die zugehörigen Daten an DSP, die mitteilen, dass eine Anfrage für Impressionen oder Werbung verfügbar ist. Daher können mehrere Werbetreibende automatisch Gebote in Echtzeit abgeben, um ihre Werbung zu schalten.

- In der Zwischenzeit müssen die Werbetreibenden ihre Kampagnen in DSP einrichten. Verwenden Sie die Informationen über den Benutzer von Data Management Platform (DMP), um zu beurteilen, wie viel er bereit ist, für die Bereitstellung einer Werbung an den Benutzer zu zahlen.
- DSPs reichen diese Echtzeit-Gebote für jeden Werbeeindruck ab, da sie der Werbebörse bereitgestellt werden.
- Welcher Bieter auch immer innerhalb eines Zeitraums, der von der Werbebörse oder den SSPs festgelegt wird, erhält von den Publishern einen Werbeplatz, um ihre Werbung zu schalten. Andernfalls verlieren sie die Möglichkeit, die richtige Werbung für ihre Hauptdemografie zu erhalten.

Wie digitale Werbeplattform in Citrix ADC integriert ist

Das folgende Diagramm zeigt, wie die verschiedenen Komponenten der Werbeplattform mit Citrix ADC und Citrix Application Delivery Management (ADM) kommunizieren, um Online-Werbung zu schalten.



Wie Citrix ADC beiträgt

Bei der Veröffentlichung von Werbung hilft die Citrix ADC Lösung bei der Handhabung und Verarbeitung des inkonsistenten Zustroms von Gebotsverkehr. Es dient als Einstiegspunkt für den gesamten Datenverkehr, um die Skalierbarkeit und Verfügbarkeit in den Availability Zones sicherzustellen. Um der Elastizität des Werbeverkehrs gerecht zu werden, wird er in einer Autoscaling-Gruppe vor Webanwendungen und Datenbankservern eingesetzt.

Die Werbeplattform auf AWS mit Citrix ADC Lösung ermöglicht es Ihnen, die Echtzeit-Performance, hohe Skalierbarkeit und hohe Verfügbarkeit auf der ganzen Welt zu erhalten. Sie können Rich Media-, Video-, Mobil- und Nativwerbung in Echtzeit kaufen und verkaufen. Es reduziert die Gesamtbetriebskosten und die Latenz, die mit dem Betrieb einer Werbeplattform verbunden sind. Es ist der Proxy mit der besten Leistung, mit den umfangreichen Funktionen, die Back-End-Server während des Autoscale-Verbindungs-Multiplexings ordnungsgemäß zu entfernen und sicherzustellen, dass der Endbenutzerverkehr niemals beeinträchtigt wird. Citrix ADC unterstützt den Lastenausgleich der Protokolle HTTP, UDP, WebRTC und RTSP, die in den Werbeplattformen verwendet werden.

Citrix ADC fügt sich mit den folgenden Schlüsselattributen kohärent in die AWS-Umgebung ein:

- Content Switching — Wechseln Sie basierend auf dem Hostnamen zur richtigen Plattform.
- Sicherheitsschutz — Verwenden Sie die Funktionalität der Webanwendungsfirewall (WAF), die Ratenbegrenzung (über Client-IP) und den Schutz vor DDoS-Angriffen.
- Autoscaling von Front-End- und Back-End-Datenverkehr.
- End-to-End-Transparenz und Anomalieerkennung für ADC-Appliances unter Verwendung von ADM.
- Niedrige Latenz

Wie Citrix ADM beiträgt

Citrix ADC nutzt Citrix ADM, um die folgenden Herausforderungen zu meistern, mit denen die digitalen Werbeplattformen konfrontiert sind:

- Identifizieren Sie die Trendabweichungen von der erwarteten
- Analyse der Anwendungsleistung in Echtzeit
- Kapazitäts-Überwachung

Vorteile der Integration von Werbeplattformen mit Citrix ADC und ADM

Die Citrix ADC Lösung bietet einem Anbieter digitaler Werbeplattformen die folgenden Funktionen und Vorteile.

Niedrige Kosten

- In den AWS Autoscaling Service integriert, kann die Citrix ADC VPX-Instanz Ihre Front-End- und Back-End-Ressourcen automatisch nach oben oder unten skalieren. Dies bietet eine Zero-Touch-Konfiguration, die auf die Elastizität von Werbeplattformen ausgerichtet ist.
- Konsolidierung der Bereitstellung aller Arten von Verkehr von einem einzigen Punkt aus.

Weitere Informationen zur Autoscaling von AWS finden Sie unter Hinzufügen von Back-End-AWS Autoscaling-Service.

Hohe Verfügbarkeit

- Wenn eine Availability Zone nicht mehr verfügbar ist, wendet Citrix ADC seine Fehlertoleranzfähigkeit an, um die Server in einer anderen Availability Zone ohne Verkehrsunterbrechung automatisch zu erkennen.
- Außerdem werden Server ordnungsgemäß beendet, wodurch der Verlust von Clientverbindungen vermieden wird.

Weitere Informationen finden Sie unter Funktionsweise von Hochverfügbarkeit in AWS.

Analyse der Anwendungsleistung

Die intelligente Analyse von Citrix ADM und die Analyse der Anwendungsleistung gewährleistet:

- Gewinnen Sie Einblick in die Probleme (Anomalien der Serverantwort, 5XX-Fehler usw.), die die Endbenutzererfahrung plagen.
- Informieren Sie den Administrator, sofort Korrekturmaßnahmen zu ergreifen.

Weitere Informationen finden Sie unter Leistungsindikatoren für Anwendungsanalysen.

Reichhaltige Firewall-Sicherheit

Die häufigsten Sicherheitslücken treten in Webanwendungen eher in Netzwerken auf. Es ist wichtig, Ihre Webanwendungen vor unbefugtem Zugriff wie Bots, Datendiebstählen und Angriffen auf die Anwendungsschicht zu schützen.

Citrix ADC bietet umfassende und integrierte Layer 4 bis Layer 7-Sicherheit, die Folgendes umfasst:

- Web App Firewall (WAF) zum Schutz Ihrer Webanwendungen, zur Identifizierung und Minderung bösartiger Bots mit regelmäßig aktualisierten Bot-Signaturen und verhaltensbasierter Erkennung.
- Ratenbegrenzung, um zu verhindern, dass eine Werbeplattform überfordert wird.

Weitere Informationen finden Sie unter Citrix Web App Firewall.

Wählen Sie den richtigen AWS-Instanztyp für die Werbeplattform

Wählen Sie den richtigen AWS-Instanztyp für ADC in Abhängigkeit von den folgenden zwei Faktoren:

- Anzahl der Nutzer, die gleichzeitig auf die Werbeplattform zugreifen.
- Die durchschnittliche Anzahl der Benutzer auf der Plattform.

Der Citrix ADC kann in verschiedenen EC2-Instanzen bereitgestellt werden, darunter c5, c5n, m5 usw. Verwenden Sie für Werbeplattformen die folgenden AWS-Instanztypen:

- c5 oder c5n eignet sich für die Abwicklung von starkem SSL-Verkehr.
- c5.large kann bis zu 1000 SSL TPS verarbeiten.

Weitere Informationen finden Sie unter VPX-AWS-Unterstützungsmatrix.

Verbesserung der Clickstream-Analyse in AWS mit Citrix ADC

December 3, 2021

Kunden greifen zunehmend über verschiedene Anwendungen wie mobile Apps, SaaS-Apps usw. auf die Unternehmensprodukte zu. Daher können Anwendungen zu einer Landmine von Kundenerlebnisdaten werden. Um das Kundenverhalten online zu verfolgen, bilden kundenorientierte Unternehmen datengesteuerte Profile für jeden ihrer Kunden, die diese Kundenverhaltensdaten verwenden.

Ein Clickstream ist eine Sequenz oder ein Stream von Ereignissen, die Benutzeraktionen (Klicks) auf einer Website oder einer mobilen Anwendung darstellen. Der Umfang von Clickstream reicht jedoch über Klicks hinaus. Es umfasst Produktsuchen, Impressionen, Käufe und solche Ereignisse, die für das Unternehmen von Relevanz sein könnten. Das bloße Sammeln und Speichern der Kundenerlebnisdaten ist nicht von großem Wert. Es ist notwendig, die hochkomplexen Daten zur richtigen Zeit nahtlos an die richtigen Anbieter zu verteilen. Unternehmen können Wert aus den Daten ableiten und schnell bewusste Entscheidungen treffen, um ihre Strategien zu verbessern. Daher nutzen Unternehmen zunehmend Clickstream Analytics, um Einblicke in die Customer Experience Journey der Apps zu erhalten.

Dieses Dokument vermittelt Ihnen ein gutes Verständnis darüber, warum Clickstream-Daten von größter Bedeutung sind, wie sie gesammelt, gespeichert, verteilt und in aussagekräftige und umsetzbare Analysen umgewandelt werden.

Citrix ADC lässt sich in Citrix ADM integrieren und bietet AWS-Services wie Amazon Kinesis Data Firehose einen Mehrwert, um Unternehmen mit der besten Analyselösung auszustatten, die sich um Clickstreams der Benutzer dreht.

Diese Citrix ADC-Lösung hilft Ihnen, komplexe Geschäftsprobleme effizient und äußerst einfach zu lösen. Citrix ADC und AWS Kinesis helfen dabei, die Probleme mit dem schlecht gestalteten Workflow zu erfassen. Citrix ADM hilft dabei, Probleme im Zusammenhang mit der Web-App und der Netzwerkleistung zu erfassen, indem relevante Filter angewendet werden. Die Verbindung von Citrix ADC mit Citrix ADM und AWS Kinesis hilft Ihnen, den enormen Zustrom von Clickstream-Daten in jeder Phase zu verwalten und zu analysieren. Diese Lösung ist hochverfügbar, skalierbar, robust und stellt sicher, dass die Lieferung kontinuierlich und sicher ist. So können Sie umsetzbare Erkenntnisse ableiten.

Warum entscheiden sich Unternehmen für Clickstream-Analytics?

Unternehmen entscheiden sich für Clickstream in erster Linie, um zu verstehen, wie Benutzer mit der Anwendung interagieren, und um Einblicke in die Verbesserung der Ziele der Anwendung zu erhalten.

Clickstream Analytics ist ein Anwendungsfall zum Abrufen von Informationen, der das Verhalten, die Navigationsgewohnheiten Ihres Benutzers usw. verfolgt. Clickstream-Analytics gibt Ihnen Informationen zu:

- Auf welchen Link klicken Ihre Kunden öfter und zu welchem Zeitpunkt.
- Wo war der Besucher, bevor er meine Website erreichte?
- Wie viel Zeit hat der Besucher auf jeder Seite verbracht?
- Wann und wo hat der Besucher im Webbrowser auf die Schaltfläche “Zurück” geklickt?
- Welche Artikel hat der Besucher zu seinem Warenkorb hinzugefügt (oder daraus entfernt)?
- Von welcher Seite hat der Besucher meine Website verlassen?

Analysedienst zur Verwaltung von Clickstream-Daten mit Amazon Kinesis

Sie können Amazon Kinesis verwenden, um Clickstream Analytics durchzuführen. Amazon Kinesis ermöglicht Clickstream-Analysen mit den folgenden Services:

- Amazon Kinesis Data Firehose
- Amazon Kinesis Data Analytics
- Amazon Kinesis-Datenströme

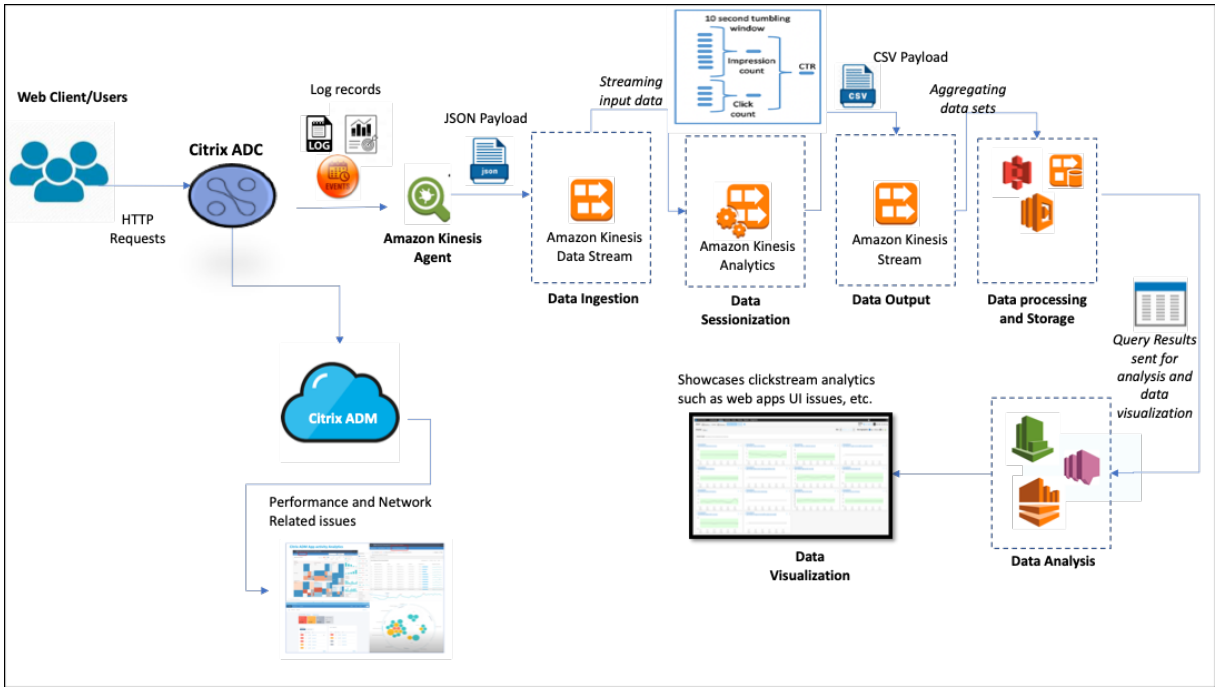
Mit Amazon Kinesis können Sie Ihre riesigen Datensätze in jedem Maßstab sammeln und analysieren. AWS Kinesis kann Daten aus verschiedenen Quellen verarbeiten, wie zum Beispiel:

- Mobile und Webanwendungen (z. B. Gaming, E-Commerce)
- IoT-Geräte
- Anwendungen für soziale Netzwerke
- Dienstleistungen des Finanzhandels
- Geospatiale Dienste

Wie Citrix ADC Clickstream-Analysen ermöglicht

Die Citrix ADC-Lösung zusammenstellt und liefert sicher Informationen über die Aktivitäten der Benutzer, wie besuchte Websites, die verbrauchte Bandbreite und den Navigationsfluss. Unternehmen analysieren diesen hohen Durchsatz und die kontinuierlichen Clickstream-Daten, um die Wirksamkeit der folgenden Punkte zu bestätigen:

- Site-Layout
- Marketingkampagnen
- Neue Anwendungsfunktionen



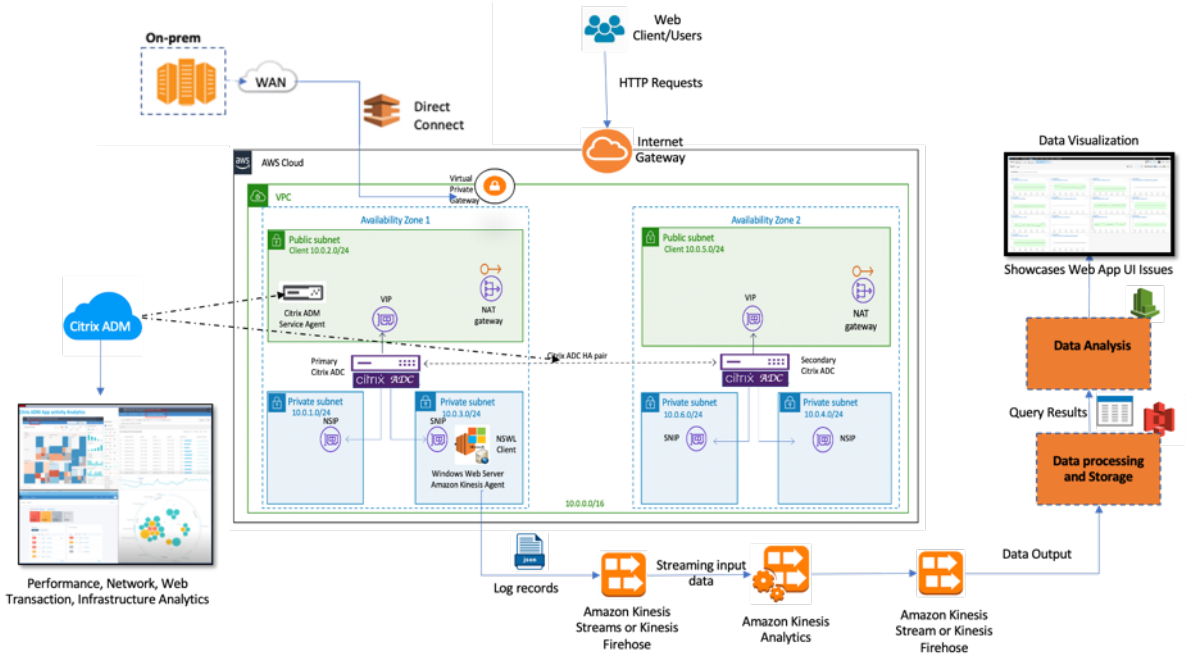
Da Citrix ADC in der Lage ist, einen robusten Netzwerkschutz für Unternehmensumgebungen bereitzustellen, werden die Serverkosten durch das Auslagern rechenintensiver Aufgaben und das Ausführen von Sitzungen mit diesen Daten reduziert. Dadurch können Unternehmen Ereignisse in Echtzeit mit hoher Verfügbarkeit, Sicherheit und geringer Latenz immer identifizieren.

Informationen zur Konfiguration finden Sie unter Konfigurieren der Citrix ADC-Lösung für Clickstream Analytics.

Wie Citrix ADC und Citrix ADM die AWS-Umgebung ergänzen

Das folgende Diagramm veranschaulicht den End-to-End-Benutzerworkflow zur Durchführung von Clickstream-Analysen in der AWS-Infrastruktur. Dieses Diagramm hilft Ihnen, die folgenden Prozesse zu verstehen:

- Wie der Benutzer mit Citrix ADC interagiert
- Wie Citrix ADC Benutzeraktionen erfasst und Clickstream-Daten generiert
- Wie die Clickstream-Daten an AWS-Services geliefert werden (Amazon Kinesis)
- Wie Amazon Kinesis die Datenprotokolle verarbeitet und speichert, um aussagekräftige Clickstream Analytics zu erstellen



Der Citrix ADC lässt sich nahtlos in die AWS-Umgebung und Citrix ADM integrieren, wodurch Unternehmen mit variablem Volumen und unterschiedlicher Natur der Clickstream-Daten kompatibel sind. Es bietet Dienste zum einfachen Laden und Analysieren von Streaming-Wissen. Sie können auch benutzerdefinierte Streaming-Wissensanwendungen für spezielle Wünsche erstellen.

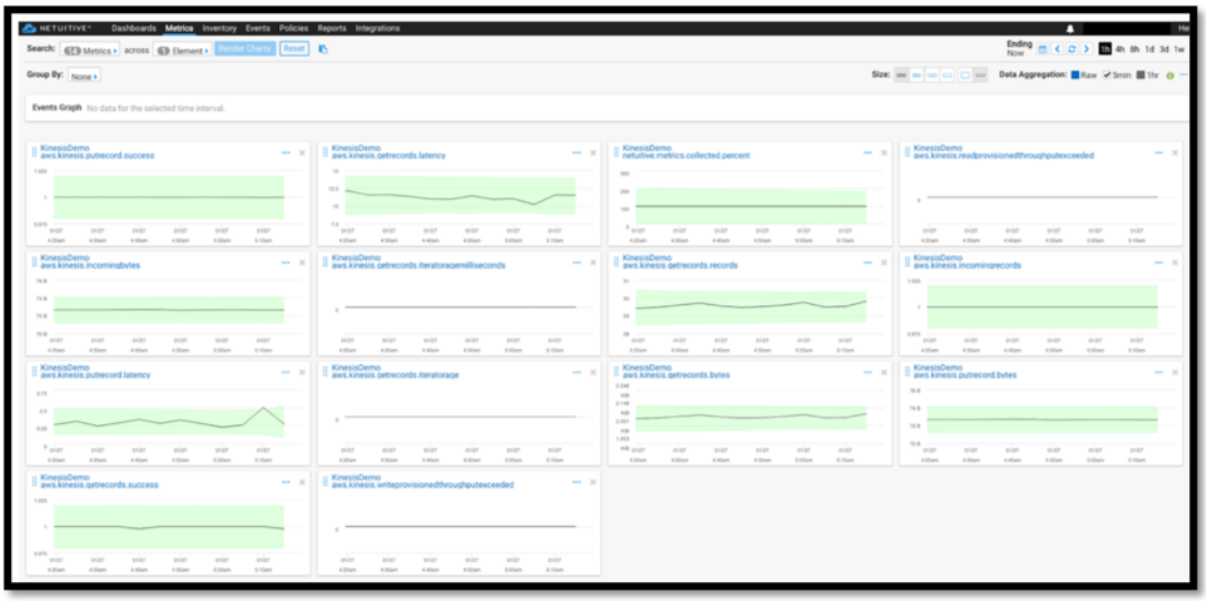
Amazon Kinesis

Die AWS-Umgebung verfügt über verschiedene Dienste, die Analysen zu den Benutzerereignissen, Protokollen und Metriken durchführen, die von Citrix ADC erfasst wurden. Die Daten können Website-Clickstreams, Finanztransaktionen, Social-Media-Feeds, IT-Protokolle und Ereignisse zur Standortverfolgung sein.

- Amazon Kinesis Data Streams führen Analysen in Szenarien durch, die skalierbares und dauerhaftes Echtzeit-Datenstreaming beinhalten, das kontinuierlich GB an Daten pro Sekunde aus mehreren Quellen erfassen kann.
- Amazon Kinesis Data Analytics kann für Szenarien mit geringerer Latenz zwischen der Sitzungsgenerierung verwendet werden, da das Aggregieren verschiedener Datensätze weniger Zeit benötigt.
- Amazon Kinesis Agent für Microsoft Windows sammelt, analysiert, filtert und streamt Eingabedaten in Kinesis-Datenströme.
- Sobald die Daten in der Cloud verfügbar sind, können Sie die genaue Datenpipeline implementieren, um die gewünschten Ergebnisse zu erhalten. Sie können diese Informationen beispielsweise in Amazon Quick Sight verwenden, einem Visualisierungstool, das zum Erstellen von Dashboards verwendet wird.

Das AWS Kinesis-Dashboard bietet folgende Angebote:

- Zeigt Probleme mit der Benutzeroberfläche von Web-Apps
- Visualisierungen von Metriken zur Webnutzung, wie Ereignisse pro Stunde, Besucherzahl und Referenzen in nahezu Echtzeit.
- Sitzungsweise Analyse



Citrix ADM Analytics

Durch die Verwendung von Citrix ADM mit Citrix ADC erhalten Sie einen Blick auf alle Geschäftsumgebungen mit einer einzigen Glasscheibe. Die erfassten Protokolle von Citrix ADC werden in Citrix ADM eingespeist, das Ihre einzelnen Anwendungen als eine einzige Entität behandelt. Sie können wertvolle Erkenntnisse gewinnen und Probleme mit den folgenden ADM-Funktionen effektiv beheben:

- Intelligente Analytik
- Web-Transaktionsanalyse
- Erkennung von Anomalien
- Leistungs- und Netzwerkprobleme

Das folgende ADM-Service-Dashboard hilft Ihnen dabei, wertvolle Erkenntnisse zu gewinnen, um die Probleme effektiv zu beheben.

Wie Citrix ADM mit Clickstream-Analytics korreliert

Clickstream-Analysedaten können mit ADM-Analysen korreliert werden, um die Anwendungsleistung zu beschreiben, vorherzusagen und zu verbessern.

Weitere Informationen zu Citrix ADM finden Sie unter Citrix ADM%20is%20A%20Centralised%20Management%20S
&text=you%20CAN%20USE%20Adm%20TO, von%20A%20Single%2C%20Unified%20Console.)

Zum Beispiel bemerkt eine Organisation, die ihre Protokolle analysiert, dass die meisten Benutzer ihre Websites verlassen. Um jedoch die Ursache für dieses Benutzerverhalten zu finden, müssen sie herausfinden, welcher Teil ihrer Anwendung schlecht funktioniert. Mit Clickstream-Analysedaten und ADM-Analysen können Sie die folgenden Erkenntnisse ableiten, um den Grund für das Verlassen einer Website durch Benutzer zu analysieren:

- Wird der Benutzer aufgrund von Latenzzeiten, 5xx-Fehlern abgebrochen?
- Gibt es SSL-Handshake-Fehler?
- Gibt es einen Teil der Anwendung, der Leistungs- oder Netzwerkprobleme aufweist?
- Gibt es einen 404-Fehler oder die Ladezeit der Seite dauert ewig, um zu antworten, und so weiter.
- Stehen Kunden vor Anomalien der Serverantwort?

Der Citrix ADM Service bietet Web Insights, mit denen IT-Administratoren die Lösung von Problemen mit den folgenden Funktionen beschleunigen können:

- Bietet integrierte und Echtzeitüberwachung aller Webanwendungen, die vom Citrix ADC bedient werden.
- Verschaffen Sie sich einen ganzheitlichen Überblick über die Anwendungsleistung zu Zeit, Latenz und das Verhalten des üblichen Benutzers durch Observability-Tools (z. B. globales Service-Graph).
- Führen Sie intelligente Analysen durch, um Anomalien der Serverantwort zu verstehen.
- SSL-Erkenntnisse tragen zur Behebung von 5xx- und 4xx-Fehlern bei.
- So führen Sie Aufzeichnungen aller Websitzungen, die Folgendes beinhalten:
  - Detaillierte Protokolle jeder Web-Transaktion
  - Suchfunktion, um relevante Logs zu finden
  - Möglichkeit, einen ADC-zu-Endbenutzer im Vergleich zu isolieren ADC-zu-Server-Problem

Arten von Daten, die von ADC für Clickstream-Analytics exportiert werden

Citrix ADC erfasst die verschiedenen Quellen, die verschiedene Datenformen generieren, die wie folgt lauten:

- Webserver-Protokolle

  Die Webserver-Protokollierungsfunktion sendet Protokolle von HTTP- und HTTPS-Anfragen zum Speichern und Abrufen an ein Clientsystem. Diese Protokolle enthalten eine große Menge an Daten, die schwer zu verstehen und daraus sinnvoll sind. Analytische Tools helfen dabei, sie zu verstehen und daraus einen Mehrwert zu schaffen. Weitere Informationen zur Konfiguration finden Sie im **Abschnitt Konfiguration der Webprotokollierung** in diesem Dokument.

- Syslogs

  Die primäre Verwendung von Syslogs ist für das Systemmanagement. Die proaktive Syslog-Überwachung zahlt sich aus, da die Ausfallzeiten von Servern und anderen Geräten in Ihrer Infrastruktur erheblich reduziert werden. Syslog identifiziert kritische Netzwerkprobleme und meldet sie proaktiv.

- Zugriff auf Protokolle

  Die Zugriffsprotokolle speichern Informationen über Ereignisse, die auf Ihrem Webserver aufgetreten sind. Wenn beispielsweise jemand Ihre Website besucht, wird ein Protokoll aufgezeichnet und gespeichert, um dem Webserver-Administrator Informationen wie die IP-Adresse des Besuchers, welche Seiten er angeschaut hat, Statuscodes und verwendeten Browser zur Verfügung zu stellen. Der Zugriff auf Protokolle kann überwältigend sein, wenn es an angemessenen Kenntnissen mangelt, um sie zu verstehen.
  Sie können Ihr System so programmieren, dass es integriert ist mit:

  - Citrix ADC für nahtlose Lieferung
  - Kinesis für umsetzbare Erkenntnisse, die für Unternehmen nützlich sind

- Überwachungsprotokolle

  Mit der Funktion “Audit-Protokollierung” können Sie die Citrix ADC-Status und Statusinformationen protokollieren, die von verschiedenen Modulen im Kernel und in den Daemons auf Benutzerebene gesammelt wurden.

- Fehler-Logs

  Die Fehlerprotokolldatei ist eine Hilfe für Administratoren, um weitere Informationen zu einem bestimmten Fehler bereitzustellen, der auf dem Webserver aufgetreten ist.

Konfigurieren der Citrix ADC-Lösung für Clickstream Analytics

Die Webserver-Protokollierungsfunktion ermöglicht es Ihnen, Protokolle von HTTP- und HTTPS-Anfragen zur Speicherung und Abruf an ein Clientsystem zu senden.

Um den Citrix ADC für die Webserver-Protokollierung zu konfigurieren, müssen Sie:

- Web-Logging-Funktion aktivieren
- Konfigurieren Sie die Größe des Puffers, um die Protokolleinträge vorübergehend zu speichern, da der Webprotokollserver auf dem Citrix ADC ausgeführt wird.

So konfigurieren Sie die Webserver-Protokollierung mit der CLI:

1. Aktivieren Sie die Webserver-Protokollierungsfunktion.

```
enable ns feature WL
<!--NeedCopy-->
```

2. [Optional] Ändern/Konfigurieren Sie die Puffergröße zum Speichern der protokollierten Informationen.

```
set ns weblogparam -bufferSizeMB 60
<!--NeedCopy-->
```

3. Installieren Sie den Citrix ADC Web Logging (NSWL) Client. Weitere Informationen finden Sie unter Installieren des Citrix ADC Web Logging (NSWL) -Clients

4. Installieren Sie den NSWL-Client unter Windows, indem Sie die folgenden Vorgänge auf dem System ausführen, auf das Sie das Paket heruntergeladen haben.

a) Extrahieren und kopieren Sie die< release number > Datei nswl_win–.zip< build number > aus dem Paket auf ein Windows-System, auf dem Sie den NSWL-Client installieren möchten.

b) Entpacken Sie die Datei auf dem Windows-System in einem Verzeichnis (genannt < NSWL-HOME>). Bin, Samples und andere Verzeichnisse werden extrahiert.

c) Führen Sie an der Eingabeaufforderung den folgenden Befehl aus dem < NSWL-HOME > Verzeichnis\ bin aus:

```
nswl -install -f < path of the log.conf file >\log.conf
<!--NeedCopy-->
```

> **Hinweis:**
>
> Um den NSWL-Client zu deinstallieren, führen Sie an der Eingabeaufforderung den folgenden Befehl aus dem < NSWL-HOME > Verzeichnis\ bin aus:

```
nswl -remove
<!--NeedCopy-->
```

5. Konfigurieren Sie nach der Installation des NSWL-Clients den NSWL-Client mit der ausführbaren NSWL-Datei. Diese Konfigurationen werden in der NSWL-Client-Konfigurationsdatei (log.conf) gespeichert.

   Führen Sie die folgenden Befehle aus dem Verzeichnis aus, in dem sich die ausführbare NSWL-Datei befindet:

```
\ns\bin
<!--NeedCopy-->
```

6. Fügen Sie in der NSWL-Clientkonfigurationsdatei (log.conf) die Citrix ADC-IP-Adresse (NSIP) hinzu, von der der NSWL-Client Protokolle sammelt, indem Sie in der Eingabeaufforderung des Clientsystems Folgendes ausführen:

```
nswl -addns -f < Path to the configuration(log.conf) file >\log.
   conf
<!--NeedCopy-->
```


7. Geben Sie den NSIP (IP-Adresse), den Benutzernamen als `nsroot` und das Kennwort der Citrix ADC-Appliance als “Instanz-ID/Ihr eingestelltes Kennwort” ein, damit:

   - NSWL-Client stellt eine Verbindung zum ADC her, nachdem Sie die NetScaler-IP-Adresse (NSIP) zur NSWL-Konfigurationsdatei hinzugefügt haben
   - ADC puffert die HTTP- und HTTPS-Anforderungsprotokolleinträge, bevor er sie an den Client sendet.
   - Der Client kann die Einträge filtern (indem er die log.conf-Datei ändert), bevor er sie speichert.

> Hinweis:
>
> Ändern Sie das Standardkennwort für Citrix ADC und fahren Sie dann mit der Konfiguration fort. Geben Sie den folgenden Befehl ein, um das Kennwort zu ändern:

```
set system user nsroot -password <your password>
<!--NeedCopy-->
```

Konfigurieren des Amazon Kinesis-Agenten

Führen Sie die folgenden Schritte in der AWS-Webkonsole aus, um den Amazon Kinesis-Agent zu konfigurieren:

1. Erstellen Sie eine Konfigurationsdatei (appsettings.json) und stellen Sie sie bereit. Konfigurationsdateien definieren Gruppen von Quellen, Senken und Pipes, die Quellen mit Senken verbinden, zusammen mit optionalen Transformationen.

   Das folgende Beispiel ist eine vollständige `appsettings.json` Konfigurationsdatei, die den Kinesis Agent so konfiguriert, dass Windows-Anwendungsprotokollereignisse an Kinesis Data Firehose streamen.

```
{

"Sources": [
    {

        "Id": "NSWLog",
        "SourceType": "DirectorySource",
        "Directory": "C:\Users\Administrator\Downloads\nswl_win
           -13.0-52.24\bin",
        "FileNameFilter": "*.log"
        "RecordParser": "TimeStamp",
```



```
11          "TimestampFormat": "yyyy-MM-dddd HH:mm:ss.ffff", //
               Optional parameter required only by the timestamp
               record parser
12          "TimeZoneKind": "UTC", //Local or UTC
13          "SkipLines": 0 //Skip a number of lines at the beginning
               of each file
14       }
15
16      ],
17  "Sinks": [
18      {
19
20          "Id": "ApplicationLogKinesisFirehoseSink",
21          "SinkType": "KinesisFirehose",
22          "StreamName": "Delivery-ik-logs",
23          "AccessKey": "Your Access Key",
24          "SecretKey": "YourSecretKey",
25          "Region": "ap-south-1"
26       }
27
28      ],
29  "Pipes": [
30      {
31
32      "Id": "ApplicationLogSourceToApplicationLogKinesisFirehoseSink
           ",
33      "SourceRef": "ApplicationLogSource",
34      "SinkRef": "ApplicationLogKinesisFirehoseSink"
35       }
36
37      ],
38  "Telemetrics":
39      {
40
41      "off": "true"
42       }
43
44   }
45
46  <!--NeedCopy-->
```

2. Richten Sie einen Kinesis Agent für Datenquellen ein, um Daten zu sammeln und diese kontinuierlich an Amazon Kinesis Firehose/Kinesis Data Analytics zu senden. Weitere Informationen finden Sie unter Erste Schritte mit Amazon Kinesis Agent für Microsoft Windows.

3. Erstellen Sie mit Amazon Kinesis Firehoseeinen End-to-End-Daten-Delivery-Stream. Der Lieferdatenstrom überträgt Ihre Daten vom Agenten an das Ziel. Das Ziel umfasst Amazon Kinesis Analytics, Amazon Redshift, Amazon Elasticsearch-Service und Amazon S3. Wählen Sie für die Quelle **Direct PUT oder andere Quellen** aus, um einen Kinesis Data Firehose-Bereitstellungsstream zu erstellen.
4. Verarbeiten Sie die eingehenden Protokolldaten mithilfe von SQL-Abfragen in Amazon Kinesis Analytics.
5. Laden Sie verarbeitete Daten von Kinesis Analytics in Amazon Elasticsearch Service, um die Daten zu indizieren.
6. Analysieren und visualisieren Sie die verarbeiteten Daten mit Visualisierungstools wie Kibana und AWS QuickInsight Services.

Referenzen

- Anzeigen und Exportieren von Syslog-Nachrichten
- Citrix Networking für Hybrid Multi Cloud
- Schreiben in AWK Kinesis Data Streams mit Kinesis Agent

Citrix ADC in einer privaten Cloud verwaltet von Microsoft Windows Azure Pack und Cisco ACI

October 5, 2021

Sie können eine Citrix ADC Appliance zum Lastenausgleich in einer privaten Cloud verwenden, die über Microsoft Windows Azure Pack verwaltet wird. Das Netzwerk für die Private Cloud wird mithilfe von Cisco ACI und Citrix ADC automatisiert.

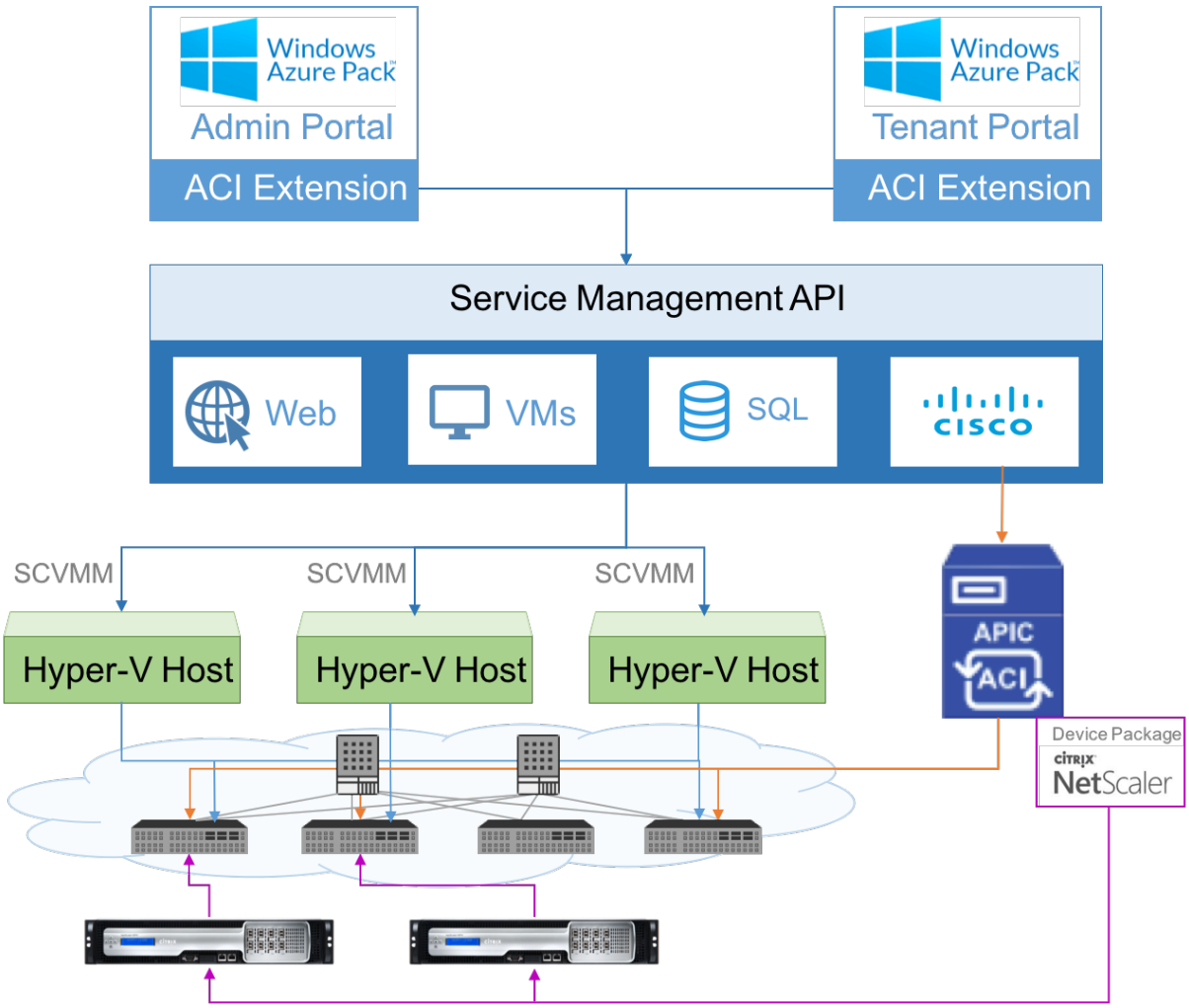
Diese Lösung umfasst viele Integrationspunkte wie Windows Azure Pack (WAP) zu Cisco APIC, Cisco APIC zu System Center Virtual Machine Manager (SCVMM) und Cisco APIC zu Citrix ADC. Als Mandant in der Private Cloud können Sie NAT aktivieren, Netzwerkdienste bereitstellen und einen Load Balancer hinzufügen.

WAP unterstützt Mandanten- und Administratorportale, auf denen ein Administrator administrative Aufgaben wie ACI-Registrierung, VIP-Bereich, Citrix ADC Gerätezuordnung mit der Cloud der virtuellen Maschine und der Erstellung von Mandantenbenutzerkonten ausführen kann. Mandanten können sich beim WAP-Mandantenportal anmelden und Netzwerk-, Bridge-Domänen und Virtual Routing and Forwarding (VRFs) konfigurieren und die Citrix ADC -Lastausgleichs- und RNAT-Funktionen nutzen.

Wichtig

- In dieser Lösung bietet die Citrix ADC Appliance nur einen einfachen Lastausgleich.
- Mandanten können mehrere VIP-Adressen mit unterschiedlichen Ports für dasselbe Netzwerk bereitstellen, müssen jedoch sicherstellen, dass die Kombination zwischen IP und Port eindeutig ist.
- Das Citrix ADC Gerätepaket unterstützt nur die Einzelkontextbereitstellung. Jeder Mandant erhält eine dedizierte Citrix ADC Instanz.
- WAP unterstützt Citrix ADC MPX-Appliances und virtuelle Citrix ADC VPX Appliances, einschließlich Citrix ADC VPX-Instanzen, die auf der Citrix ADC SDX-Plattform bereitgestellt werden.

Die folgende Abbildung gibt einen Überblick über die Lösung:



Voraussetzungen

Stellen Sie sicher, dass:

- Sie verfügen über konzeptionelle Kenntnisse über Cisco ACI Komponenten und Citrix ADCs.
  - Weitere Informationen zu Cisco ACI und seinen Komponenten finden Sie in der Produktdokumentation unter: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.
  - Weitere Informationen zu Citrix ADCs finden Sie in der Citrix ADC Produktdokumentation unterhttp://docs.citrix.com/.
- Alle erforderlichen Komponenten von Cisco ACI, einschließlich Cisco APIC im Rechenzentrum, werden eingerichtet und konfiguriert. Weitere Informationen zu Cisco ACI und seinen Komponenten finden Sie in der Produktdokumentation unter: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.
- Sie wissen, wie Sie Cisco ACI mit Microsoft Windows Azure Pack integrieren. Siehe Produktdokumentation unter: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/virtualization/b_ACI_Virtualization_Guide_2_2_1.html.
- Sie verfügen über konzeptionelle Kenntnisse über Microsoft Windows Azure Pack. Siehe Produktdokumentation unter: https://www.microsoft.com/en-in/cloud-platform/windows-azure-pack.
- Sie haben die Citrix ADC -Software Version 11.1 oder höher installiert.
- Sie konfigurieren Citrix ADCs in Cisco ACI, so dass sie mit Cisco APIC verwaltet werden können.
- Stellen Sie in Cisco APIC sicher, dass:
  - Die Managementkonnektivität von Cisco APIC mit Citrix ADC wird hergestellt.
  - Sie laden das Citrix ADC Gerätepaket Version *11.1—52.3* hoch und registrieren das Citrix ADC Gerät mithilfe von Cisco APIC in Cisco ACI.
  - Konfigurieren Sie die Citrix ADC Appliance in Cisco APIC Common Tenant und stellen Sie sicher, dass keine Fehler in Cisco APIC vorhanden sind.
  - Sie haben alle APIC-spezifischen Konfigurationen wie VLAN-Pool, L3OutservicesDom, L3Extout, Ressourcenpool konfiguriert. Weitere Informationen finden Sie in der *Cisco-Dokumentation*.

Erstellen eines Citrix ADC Load Balancer in einem Plan im Service Management Portal (Admin Portal)

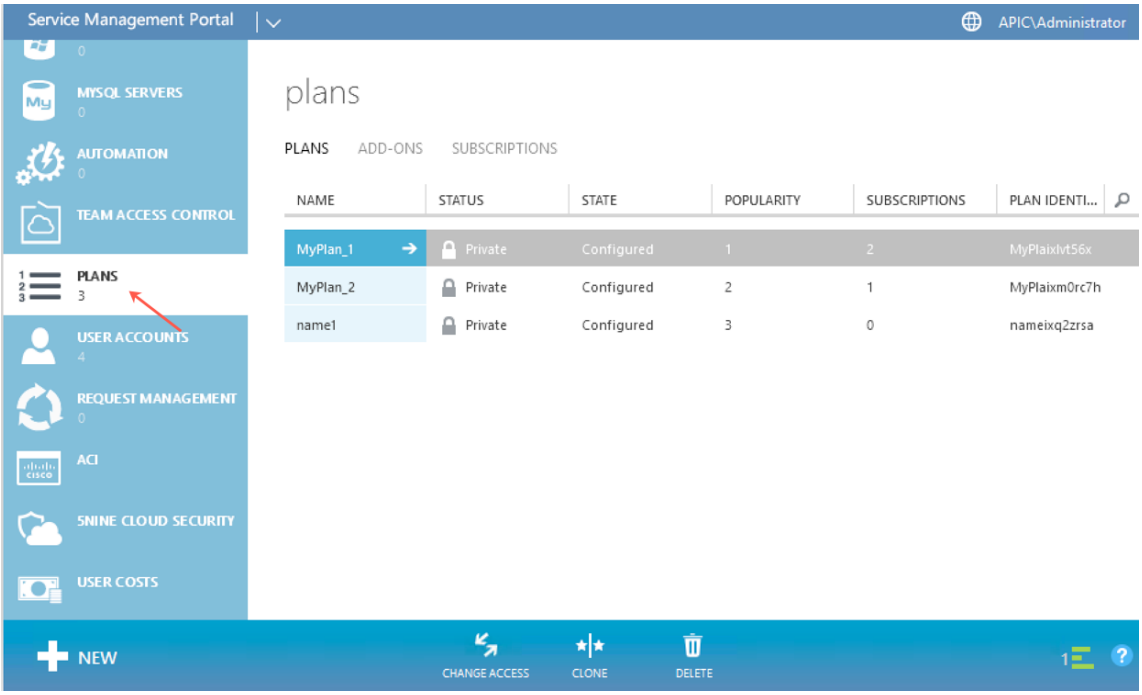
October 5, 2021

Das Service Management Portal in WAP ermöglicht es einem Administrator, Cisco APIC bei WAP zu registrieren und auch einen Hosting-Plan zu erstellen. Im Rahmen des Plans können Sie den VIP-Bereich angeben, den Citrix ADC Load Balancer mit dem Plan verknüpfen und Mandantenbenutzerkonten er-

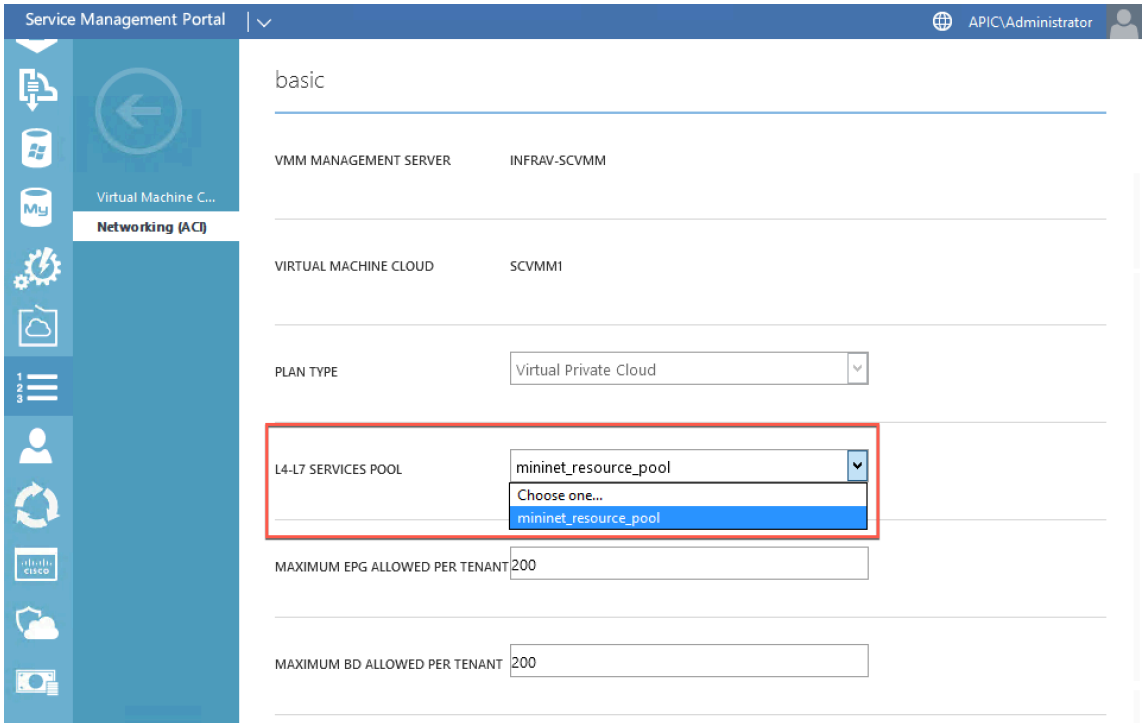
stellen.

So erstellen Sie einen Citrix ADC Load Balancer in einem Plan im Admin-Portal:

1. Melden Sie sich beim Service Management Portal (Admin Portal) an.
2. Wählen Sie im Navigationsbereich die Option **PLANS** aus.



3. Wählen Sie im Plänebereich den Plan aus, den Sie einen Load Balancer hinzufügen möchten.
4. Wählen Sie im Bereich des ausgewählten Plans die Option **Netzwerk (ACI)** aus.
5. Wählen Sie im Bereich **Netzwerk (ACI)** in der Dropdownliste **L4-L7 SERVICE POOL** den L4-L7-Ressourcenpool aus, den Sie in Cisco APIC erstellt hatten.



6. Erstellen Sie ein Mandantenbenutzerkonto, und ordnen Sie den Benutzer mit dem von Ihnen erstellten Plan zu.

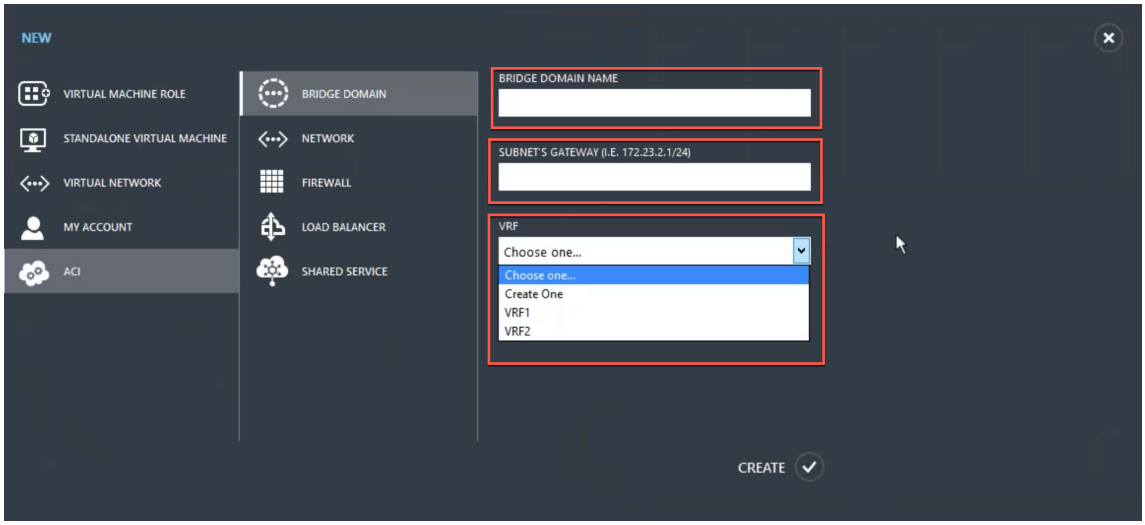
Konfigurieren eines Citrix ADC Load Balancer mit dem Service Management Portal (Mandantenportal)

October 5, 2021

In WAP kann der Mandant, sobald der Mandant die Bridge Domain (BD), VRF und ein Netzwerk erstellt hat, einen Citrix ADC Load Balancer über das Service Management Portal (Mandant Portal) konfigurieren.

So konfigurieren Sie Citrix ADC Load Balancer im Service Management Portal (Mandantenportal)

1. Melden Sie sich beim Service Management Portal (Mandantenportal) an.
2. Erstellen Sie eine Bridge-Domäne und einen VRF wie folgt:
   a. Wählen Sie im Navigationsbereich **ACI** aus.
   b. Klicken Sie auf **NEW**.
   c. Wählen Sie im Bereich **NEW** die Option **BRIDGE DOMAIN** .



d. Geben Sie im Feld **BRIDGE DOMAIN** den Bridge-Domänennamen ein (z. B. BD01).

e. (Optional) Geben Sie im Feld **SUBNET'S GATEWAY** das Gateway des Subnetzes ein (z. B. 192.168.1.1/24).

f. Wählen Sie im Feld **VRF** einen VRF aus, der bereits Teil des Abonnements ist, oder wählen Sie **Erstellen**, um einen VRF zu erstellen.

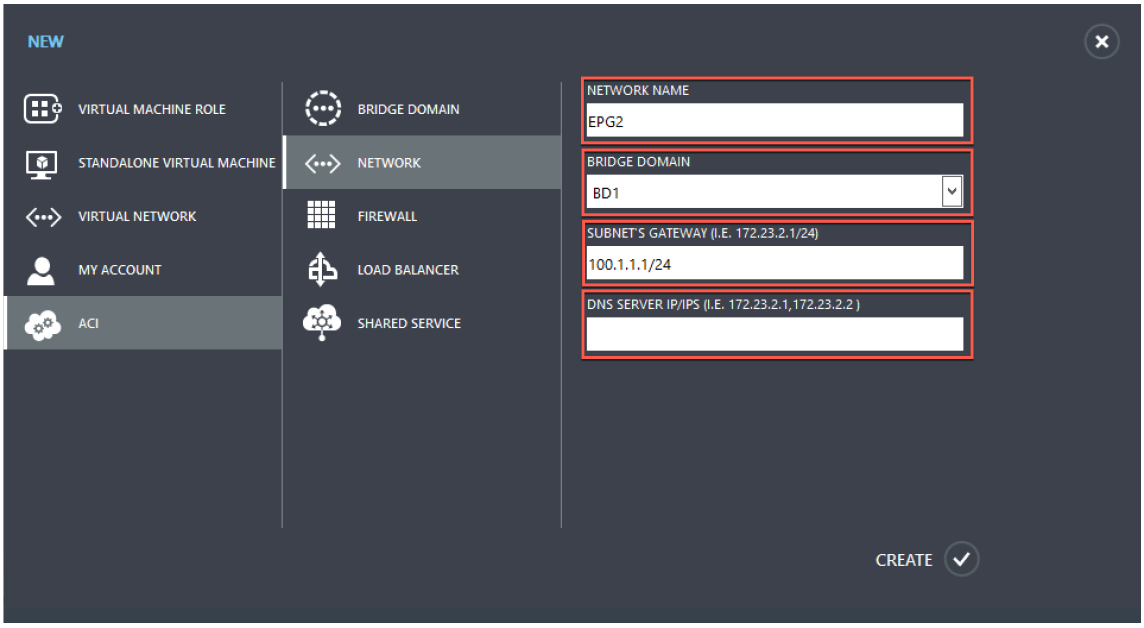
g. Klicken Sie auf **CREATE**.

3. Erstellen Sie ein Netzwerk, und ordnen Sie es der erstellten Bridge-Domäne zu. Führen Sie folgende Schritte aus:

   a. Wählen Sie im Navigationsbereich **ACI** aus.

   b. Klicken Sie auf **NEW**.

   c. Wählen Sie im Bereich **NEW** die Option **NETWORK** aus.



d. Geben Sie im Feld **NETWORK NAME** den Netzwerknamen ein (z. B. S01).

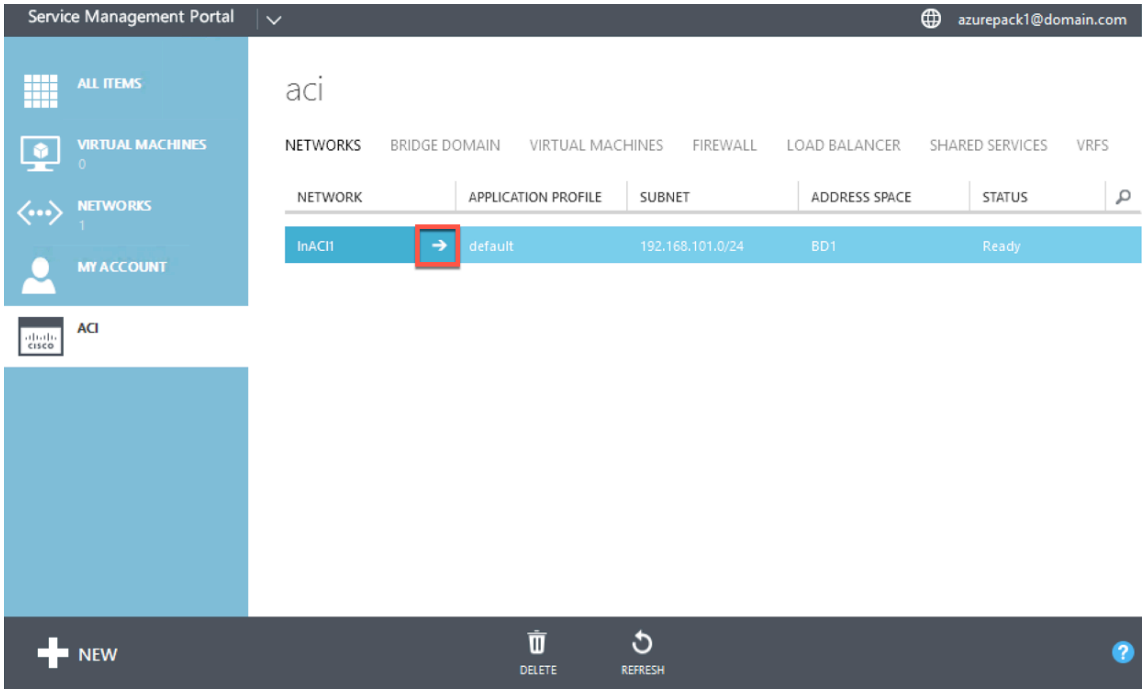
e. Wählen Sie in der Dropdownliste **BRIDGE DOMAIN** die Bridgedomäne aus, die Sie erstellt haben. (z. B. BD01).

f. Geben Sie im Feld **Gateway** Feld des Subnetzes die Gateway-Adresse des Subnetzes ein (z. B. 172.23.2.1/24).

g. (Optional) Geben Sie im Feld **DNS SERVER IP/IPS** die DNS-Serverdetails ein.

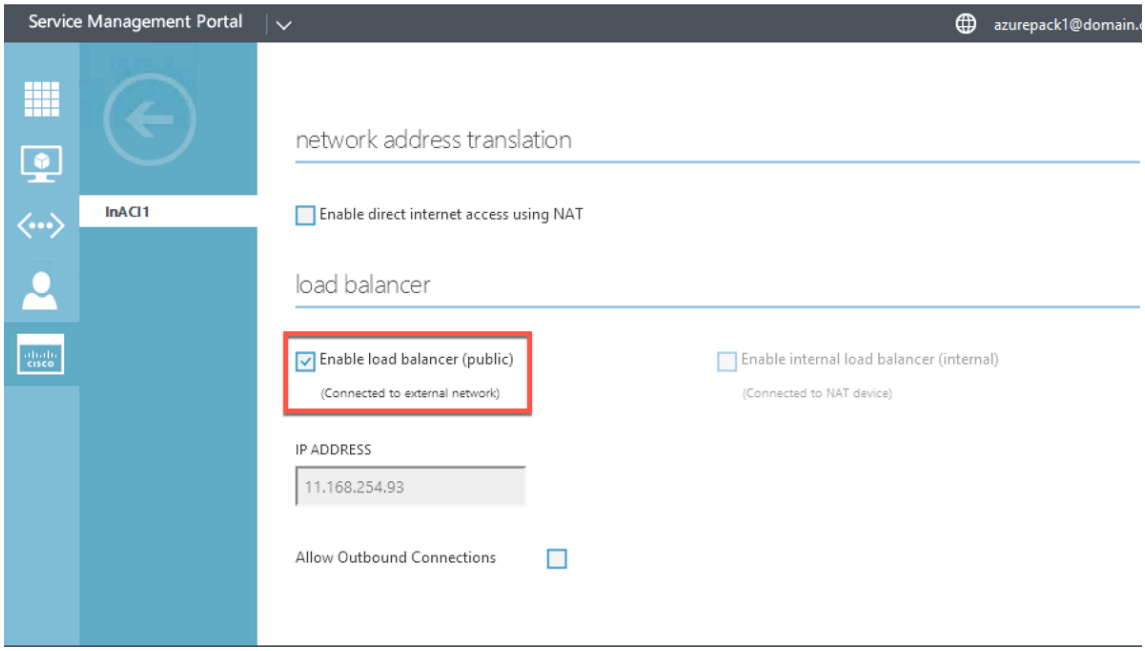
h. Klicken Sie auf **CREATE**.

4. Wählen Sie im **ACI-Bereich** die Option **NETWORKS** aus.

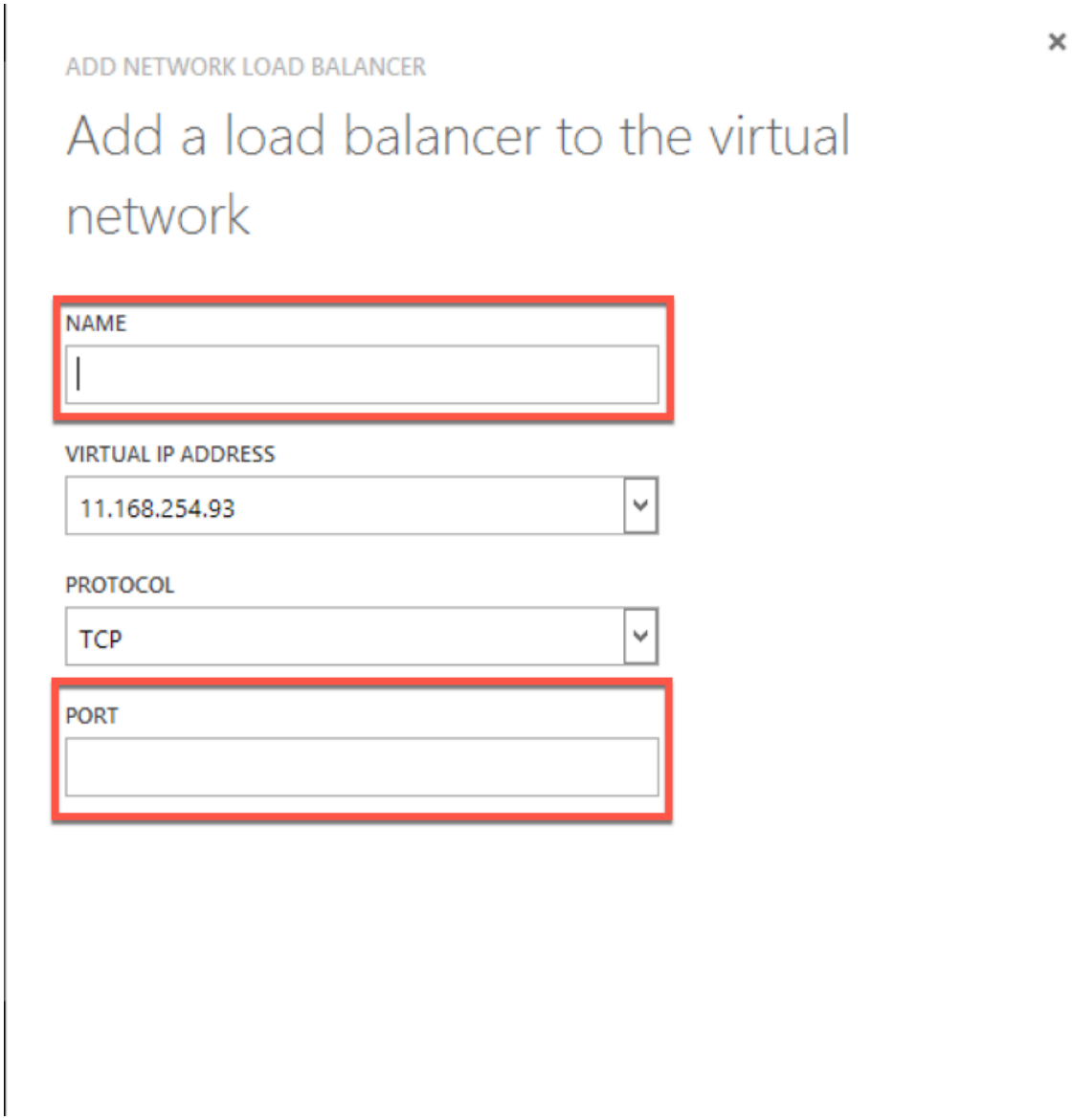


5. Doppelklicken Sie auf das Netzwerk, das Sie erstellt haben. Wählen Sie dann im Netzwerkbereich **Load Balancer aktivieren (öffentlich)**. Im Feld **IP-Adresse** wird automatisch ein VIP aus dem VIP-Bereich zugewiesen, den der Administrator im Admin-Portal konfiguriert hat. Weitere Informationen finden Sie unter Erstellen eines Citrix ADC Load Balancer in einem Plan im Service Management Portal (Admin-Portal).

6. Doppelklicken Sie auf das Netzwerk, das Sie erstellt haben. Wählen Sie dann im Netzwerkbereich **Load Balancer aktivieren (öffentlich)**. Im Feld **IP-Adresse** wird automatisch ein VIP aus dem VIP-Bereich zugewiesen, den der Administrator im Admin-Portal konfiguriert hat. Weitere Informationen finden Sie unter Erstellen eines Citrix ADC Load Balancer in einem Plan im Service Management Portal (Admin-Portal).



7. Wählen Sie im Netzwerkbereich die Registerkarte **Lastausgleichsdienste** aus, und klicken Sie auf **Hinzufügen**.



8. Gehen Sie im Bereich **ADD NETWORK LOAD BALANCER** folgendermaßen vor:

   a. Geben Sie im Feld **NAME** den Namen für den Load Balancer ein.

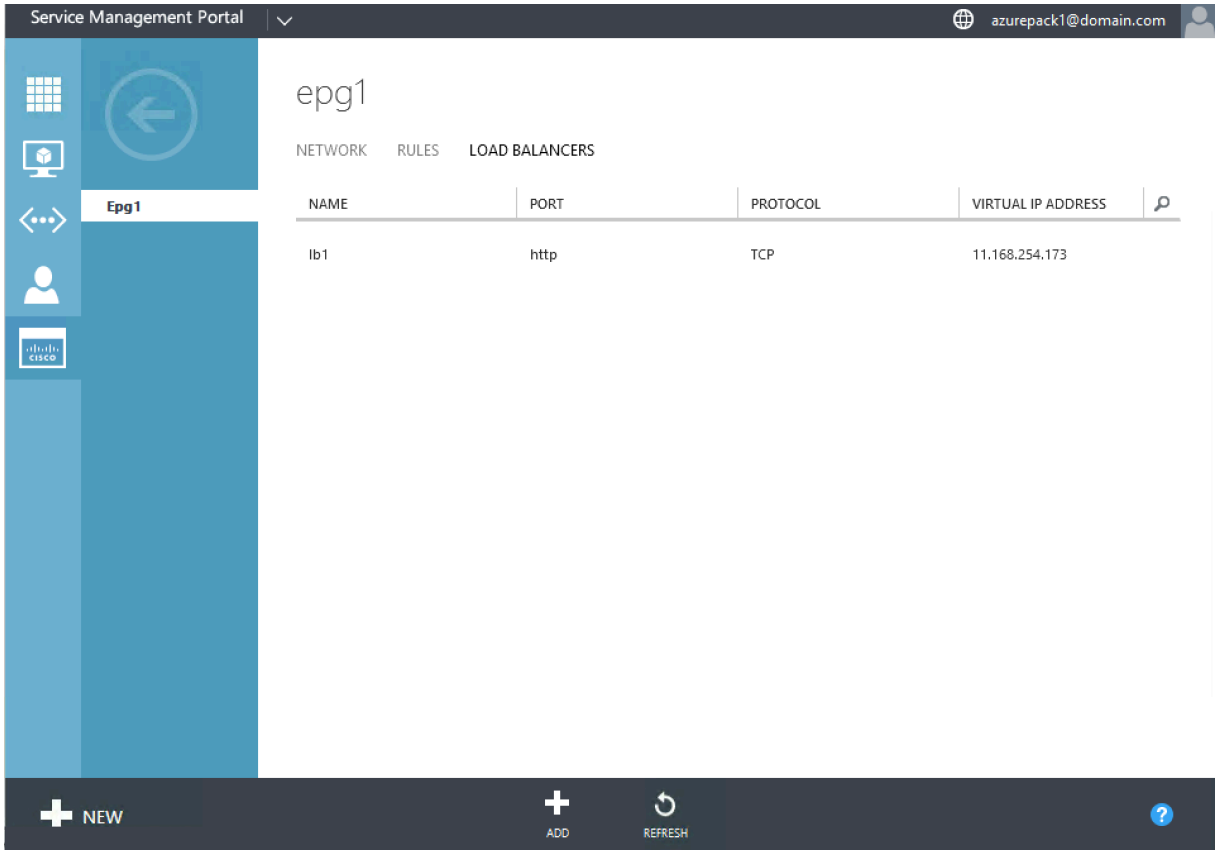
   b. Weisen Sie dem Load Balancer optional im Feld **VIRTUAL IP ADDRESS** eine VIP-Adresse aus dem VIP-Bereich zu, den Sie zuvor definiert haben.

   c. Wählen Sie optional im Feld **PROTOCOL** die Option **TCP** aus.

   d. Geben Sie im Feld **PORT** die Portnummer ein.

9. Klicken Sie auf **CREATE**.

   Der Citrix ADC Load Balancer wird auf der Registerkarte **LOAD BALANCERS** angezeigt, und der Citrix ADC Load Balancer ist Datenpfad bereit.



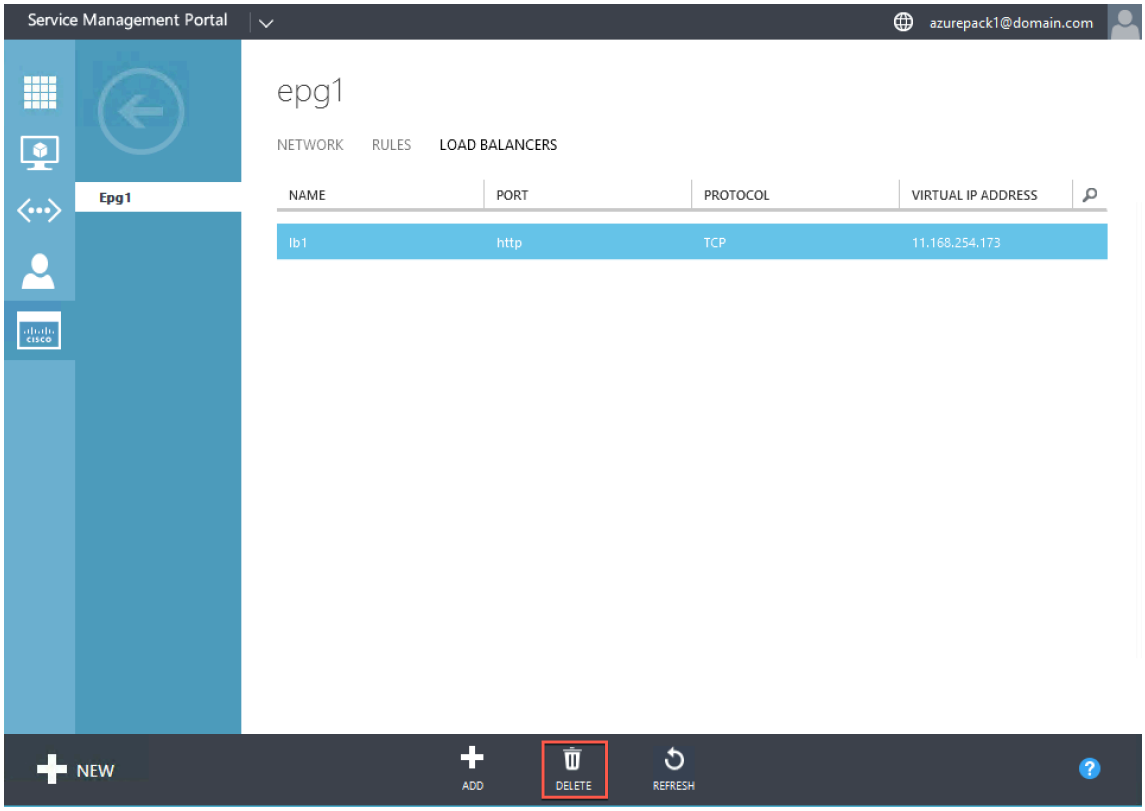
Löschen eines Citrix ADC Load Balancer aus dem Netzwerk

October 5, 2021

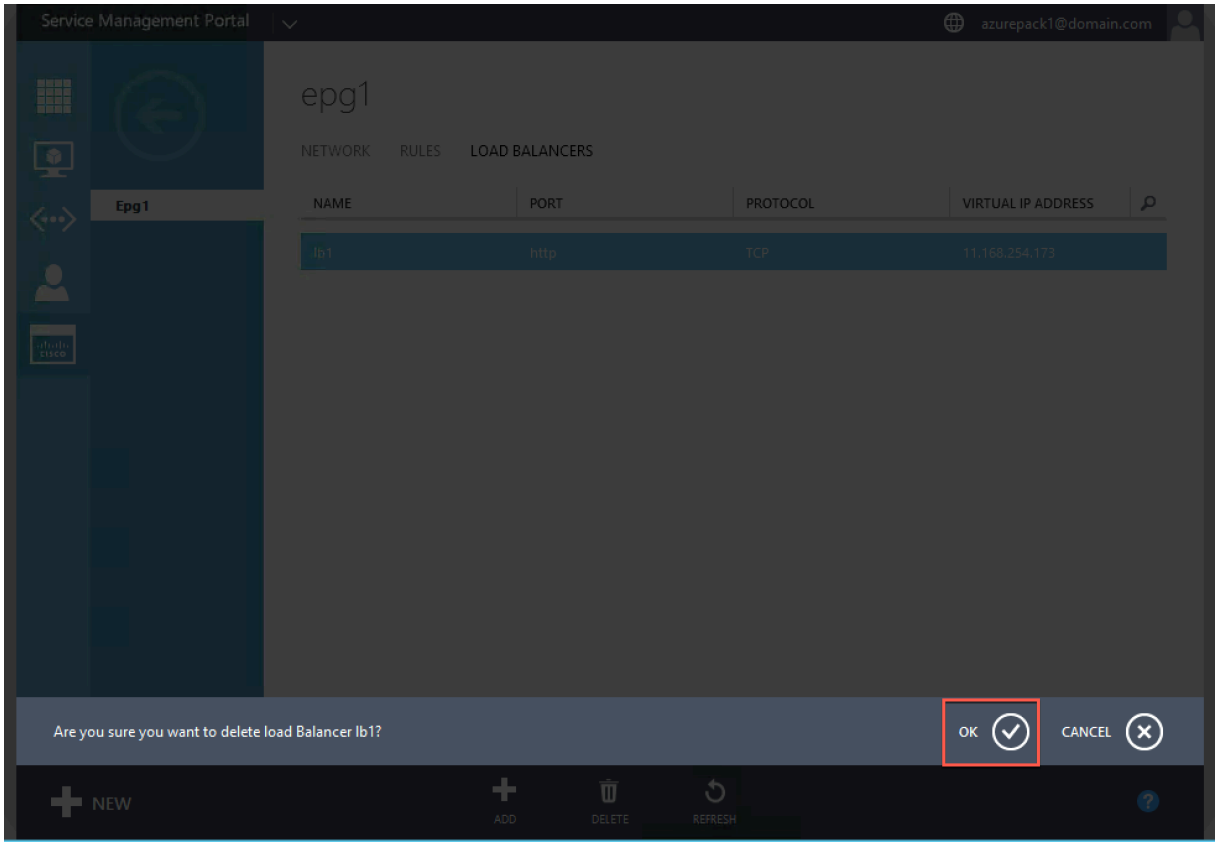
Mit dem Service Management Portal (Mandant Portal) können Sie den von Ihnen erstellten Citrix ADC Load Balancer aus dem Netzwerk löschen.

So löschen Sie einen Citrix ADC Load Balancer aus dem Netzwerk:

1. Melden Sie sich beim Service Management Portal (Mandantenportal) an.
2. Wählen Sie im Navigationsbereich **ACI** aus.
3. Klicken Sie im **ACI-Bereich** auf der Registerkarte **NETWORKS** auf das Netzwerk, das Sie erstellt haben.
4. Wählen Sie im Bereich des ausgewählten Netzwerks den Citrix ADC Load Balancer aus, und klicken Sie auf **DELETE**.



5. Klicken Sie auf **OK**, um den Citrix ADC Load Balancer zu löschen.



Native Cloud-Lösung von Citrix für Microservices auf Basis von Kubernetes

October 5, 2021

Während Unternehmen schneller Innovationen entwickeln und näher an Kunden herankommen, entwickeln sie ihren internen Prozess neu und brechen Grenzen innerhalb ihrer Organisation auf. Sie entfernen Silos, um die richtigen Fertigkeiten im selben Team zusammenzuziehen. Eines der Ziele ist die Erstellung und Bereitstellung von Softwareanwendungen mit Geschwindigkeit, Agilität und Effizienz. In diesem Zusammenhang werden moderne Anwendungsarchitekturen, die auf Microservices basieren, von einer wachsenden Zahl von Unternehmen übernommen.
Mithilfe einer Microservices-Architektur können Sie Anwendungen als Gruppen von lose gekoppelten Diensten erstellen, die unabhängig voneinander bereitgestellt, aktualisiert und skaliert werden können.

Cloud-native ist ein Ansatz, der bei der Erstellung und Bereitstellung von Anwendungen mit den folgenden Schlüsselattributen auf der Microservices-Architektur beruht:

- Bereitstellen von Anwendungen als lose gekoppelte Microservices oder Container
- Umfasst einen sehr hohen Automatisierungsgrad
- Implementiert agile DevOps-Prozesse und kontinuierliche Bereitstellungs-Workflows
- Zentriert rund um APIs für Interaktion und Zusammenarbeit

Wie hilft Kubernetes in der Cloud native Journey?

Um das gewünschte Maß an Agilität und Stabilität zu bieten, benötigen Cloud-native Anwendungen ein hohes Maß an Infrastrukturautomatisierung, -sicherheit, -netzwerk und -überwachung. Sie benötigen ein Container-Orchestrierungssystem, das Container in großem Maßstab effizient verwalten kann. Kubernetes hat sich als die beliebteste Plattform für die Bereitstellung und Orchestrierung von Containern entwickelt. Kubernetes abstrahiert die komplexe Aufgabe der Ausführung, Bereitstellung und Verwaltung von Containern von Entwicklern und Operatoren und plant automatisch Container zwischen einem Cluster von Knoten. Kubernetes und das Cloud-Native Computing Foundation (CNCF) -Ökosystem unterstützen Sie beim Aufbau einer Plattform für cloudbasierte Lösungen.

Einige der wichtigsten Vorteile der Verwendung von Kubernetes:

- Vereinfachte Anwendungsbereitstellung, sei es lokale, hybride oder öffentliche Cloud-Infrastruktur
- Beschleunigte Anwendungsentwicklung und -bereitstellung
- Erhöht die Agilität, Flexibilität und Skalierbarkeit von Anwendungen

Was ist die native Cloud-Lösung von Citrix?

Um die Vorteile der Verwendung von Kubernetes in der Produktion zu maximieren, müssen Sie Kubernetes in verschiedene Tools, herstellerbezogene und Open-Source-Komponenten integrieren. Die Sicherstellung der Zuverlässigkeit und Sicherheit ihrer Cloud-nativen Anwendung in der Produktion ist eine Herausforderung für viele Unternehmen.
Als Anbieter branchenführender Citrix ADCs bietet Citrix eine Cloud-native Citrix Lösung, um die Herausforderungen in einer Produktionsumgebung von Kubernetes zu bewältigen.

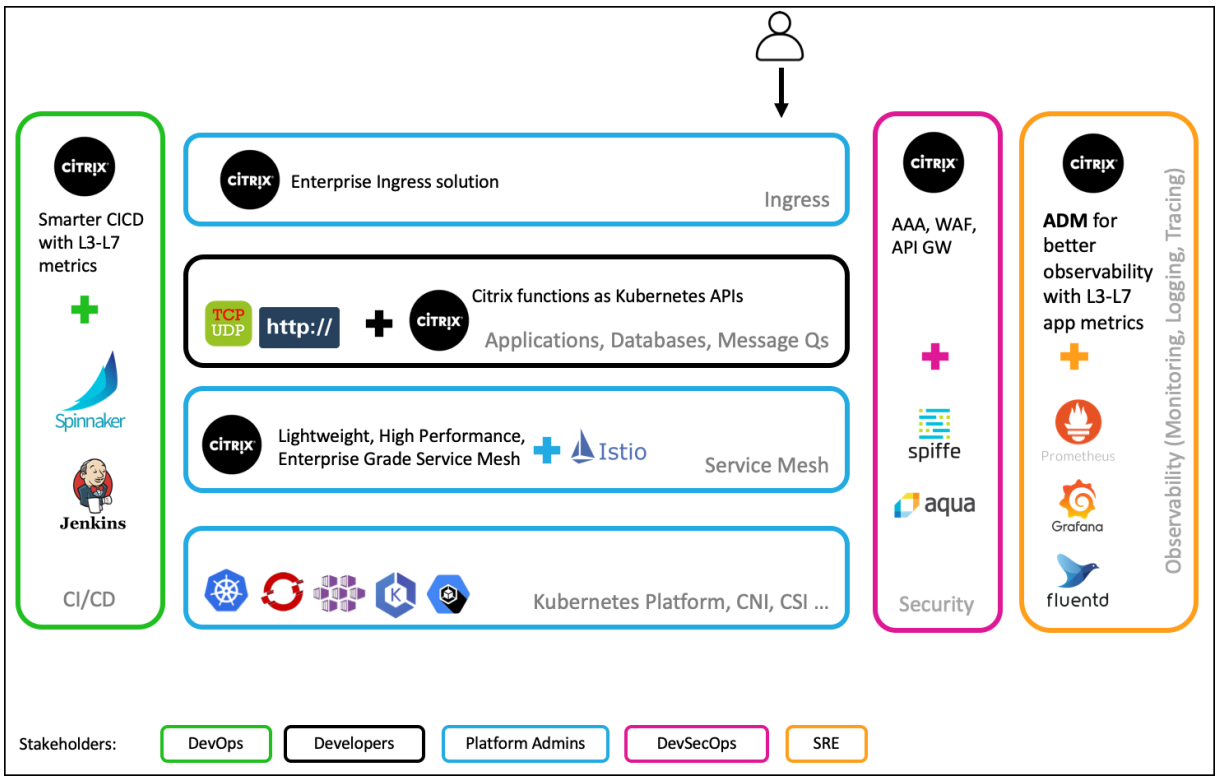
Die native Cloud-Lösung von Citrix nutzt die erweiterte Datenverkehrsverwaltung, Beobachtbarkeit und umfassende Sicherheitsfunktionen von Citrix ADCs, um Zuverlässigkeit und Sicherheit in Unternehmen zu gewährleisten. Sie bietet vollständige Transparenz für den Anwendungsdatenverkehr in Ihrer Kubernetes-Umgebung, liefert sofortiges Feedback und hilft Ihnen, aussagekräftige Einblicke in die Anwendungsleistung zu gewinnen.

In der folgenden Tabelle sind die wichtigsten Anforderungen verschiedener Stakeholder bei der Implementierung einer Ingress-Lösung aufgeführt.

Stakeholder	Job-Funktion	Benötigt
Plattform-	Sicherstellen der Verfügbarkeit von Kubernetes-Clustern	Einfachere Möglichkeiten zur Verwaltung von Anwendungen, die in mehreren Clustern, Betriebs- und Plattformlebenszyklusmanagement bereitgestellt werden
DevOps	Beschleunigen Sie die Bereitstellung von Anwendungen für die Produktion	Integration mit CI/CD-Pipeline, Unterstützung für Bereitstellungstechniken wie Canary und Blue-Green für eine schnellere Bereitstellung
Die Entwickler	Entwicklung und Test von Microservices	Möglichkeiten, Traffic in den Kubernetes-Cluster zu bringen, Tracing und Debugging, Ratenbegrenzung für Anwendungen und Authentifizierung für Anwendungen

Stakeholder	Job-Funktion	Benötigt
SREs	Sicherstellen der Verfügbarkeit von Anwendungen zur Einhaltung von Service Level Agreements	Erweiterte Telemetrie für Anwendungen und Infrastruktur
SecOPs	Gewährleistung der Einhaltung	Sicherer Ingress-Datenverkehr, API-Schutz, Service-Mesh für sichere Kommunikation zwischen Microservices im Kubernetes-Cluster

Das folgende Diagramm erläutert die native Citrix Cloud-Lösung und wie sie die verschiedenen Herausforderungen bewältigt, mit denen Stakeholder auf ihrer Cloud-Native-Journey konfrontiert sind.



Die native Lösung von Citrix Cloud bietet die folgenden wichtigen Vorteile:

- Bietet eine fortschrittliche Kubernetes Ingress Lösung, die den Anforderungen von Entwicklern, SREs, DevOps und Netzwerk- oder Cluster-Administratoren gerecht wird.
- Eliminiert die Notwendigkeit, ältere Anwendungen basierend auf TCP- oder UDP-Datenverkehr neu zu schreiben, während sie in eine Kubernetes-Umgebung verschoben werden.

- Schützt Anwendungen mit Citrix ADC Richtlinien, die als Kubernetes-APIs bereitgestellt werden.
- Hilft bei der Bereitstellung leistungsstarker Microservices für Nord-Süd-Verkehr und Ost-West-Verkehr.
- Bietet eine All-in-One-Ansicht aller Microservices mit Citrix ADM Servicegraphen.
- Ermöglicht eine schnellere Fehlerbehebung von Microservices bei verschiedenen Arten von Datenverkehr, einschließlich TCP, UDP, HTTP, HTTPS und SSL.
- Schützt APIs.
- Automatisiert die CI/CD-Pipeline für Canary-Bereitstellungen.
- Bietet eingängige Integrationen mit Open-Source-Tools aus CNCF.

Weitere Informationen zu verschiedenen Komponenten der Citrix Cloud-nativen Lösung finden Sie unter den folgenden Links:

- Kubernetes Ingress Lösung
- Service-Mesh
- Lösungen für Beobachtbarkeit
- API-Gateway für Kubernetes

Kubernetes Ingress Lösung

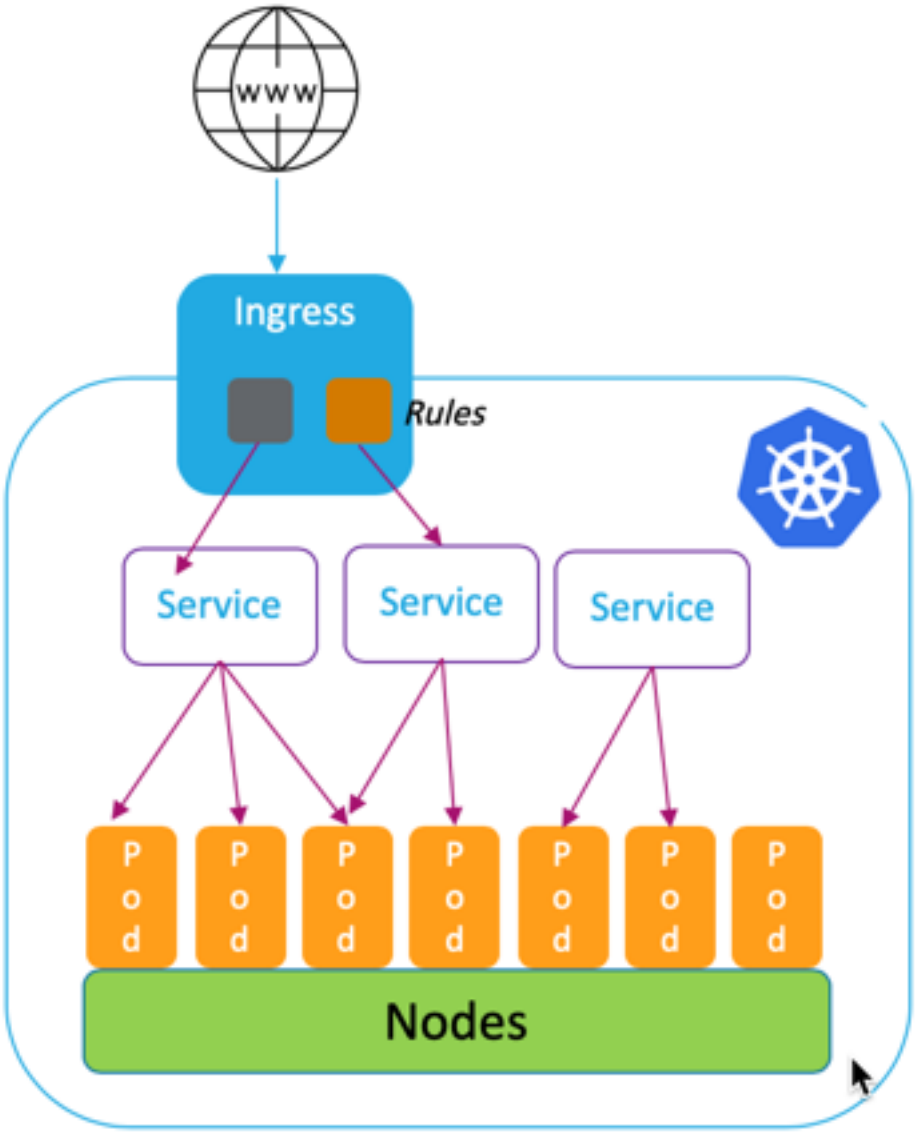
October 5, 2021

Dieses Thema bietet einen Überblick über die von Citrix bereitgestellte Kubernetes Ingress Lösung und erläutert die Vorteile.

Was ist Kubernetes Ingress?

Wenn Sie eine Anwendung in einem Kubernetes-Cluster ausführen, müssen Sie externen Benutzern eine Möglichkeit bieten, von außerhalb des Kubernetes-Clusters auf die Anwendungen zuzugreifen. Kubernetes stellt ein Objekt namens Ingress bereit, das die effektivste Möglichkeit bietet, mehrere Dienste mit einer stabilen IP-Adresse verfügbar zu machen. Ein Kubernetes-Eingangsobjekt ist immer mit einem oder mehreren Diensten verknüpft und fungiert als Einstiegspunkt für externe Benutzer, um auf Dienste zuzugreifen, die innerhalb des Clusters ausgeführt werden.

Das folgende Diagramm erklärt, wie Kubernetes Ingress funktioniert.



Die Kubernetes Ingress-Implementierung besteht aus den folgenden Komponenten:

- **Ingress-Ressource**. Mit einer Ingress-Ressource können Sie Regeln für den Zugriff auf Anwendungen außerhalb des Clusters definieren.
- **Ingress-Controller**. Ein Ingress-Controller ist eine Anwendung, die innerhalb des Clusters bereitgestellt wird, die Regeln interpretiert, die im Ingress definiert sind. Ingress-Controller wandelt die Ingress-Regeln in Konfigurationsanweisungen für eine in den Cluster integrierte Load Balancing-Anwendung um. Der Load Balancer kann eine Softwareanwendung sein, die innerhalb Ihres Kubernetes-Clusters ausgeführt wird, oder eine Hardware-Appliance, die außerhalb des Clusters ausgeführt wird.

- **Ingress-Gerät**. Ein Ingress-Gerät ist eine Lastausgleichsanwendung wie Citrix ADC CPX, VPX oder MPX, die den Lastausgleich gemäß den Konfigurationsanweisungen des Ingress-Controller durchführt.

Was ist die Kubernetes Ingress-Lösung von Citrix?

In dieser Lösung stellt Citrix eine Implementierung des Kubernetes Ingress Controller zur Verwaltung und Weiterleitung des Datenverkehrs in Ihren Kubernetes-Cluster mithilfe von Citrix ADCs (Citrix ADC CPX, VPX oder MPX) bereit. Der Citrix Ingress Controller integriert Citrix ADCs in Ihre Kubernetes-Umgebung und konfiguriert Citrix ADC CPX, VPX oder MPX gemäß den Ingress-Regeln.

Standardlösungen von Kubernetes Ingress bieten Load Balancing nur auf Layer 7 (HTTP- oder HTTPS-Datenverkehr). Manchmal müssen Sie viele Legacy-Anwendungen verfügbar machen, die auf TCP oder UDP oder Anwendungen angewiesen sind und eine Möglichkeit benötigen, diese Anwendungen auszugleichen. Die Citrix Kubernetes Ingress-Lösung bietet TCP-, TCP-SSL-und UDP-Datenverkehr neben dem standardmäßigen HTTP- oder HTTPS-Ingress Unterstützung. Außerdem funktioniert es nahtlos über mehrere Clouds oder lokale Rechenzentren hinweg.

Citrix ADC bietet Richtlinien für die Verkehrsverwaltung der Enterprise-Klasse wie Rewrite und Responder-Richtlinien für den effizienten Lastenausgleich auf Layer 7. Kubernetes Ingress fehlt jedoch solche Richtlinien für das Verkehrsmanagement der Unternehmensklasse. Mit der Kubernetes Ingress-Lösung von Citrix können Sie Rewrite- und Responderrichtlinien für Anwendungsverkehr in einer Kubernetes-Umgebung mithilfe von CRDs von Citrix anwenden.

Die Kubernetes Ingress Lösung von Citrix unterstützt auch die automatisierte Kanary-Bereitstellung für Ihre CI/CD-Anwendungspipeline. In dieser Lösung ist Citrix ADC in die Spinnaker-Plattform integriert und dient als Quelle für die Bereitstellung präziser Metriken für die Analyse der kanarischen Bereitstellung mit Kayenta. Nach der Analyse der Metriken generiert Kayenta einen Aggregatwert für den Kanarienvogel und beschließt, die kanarische Version zu bewerben oder zu scheitern. Sie können auch die Verteilung des Datenverkehrs auf die Canary-Version mithilfe der Citrix ADC Richtlinieninfrastruktur regeln.

In der folgenden Tabelle werden die Vorteile der Ingress-Lösung von Citrix über Kubernetes Ingress zusammengefasst.

Funktionen	Kubernetes Eindringen	Ingress-Lösung von Citrix
HTTP- und HTTPS-Unterstützung	Ja	Ja
URL-Routing	Ja	Ja
TLS	Ja	Ja
Lastausgleich	Ja	Ja

Funktionen	Kubernetes Eindringen	Ingress-Lösung von Citrix
TCP, TCP-SSL	Nein	Ja
UDP	Nein	Ja
HTTP/2	Ja	Ja
Automatisierte Kanarienbereitstellung mit CI/CD-Tools	Nein	Ja
Unterstützung für die Anwendung von Citrix ADC Rewrite- und Responderrichtlinien	Nein	Ja
Authentifizierung (Open Authorization (OAuth), gegenseitige TLS (MTLs))	Nein	Ja
Unterstützung für die Anwendung von Citrix Rate-Limiting-Richtlinien	Nein	Ja

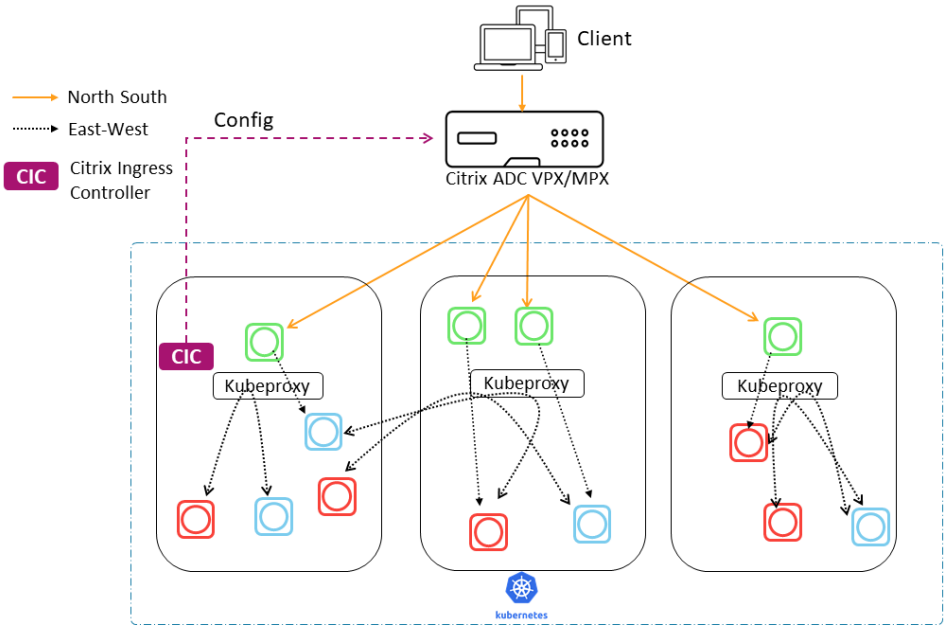
Bereitstellungsoptionen für Kubernetes Ingress Lösung

Die Kubernetes Ingress Lösung von Citrix bietet Ihnen eine flexible Architektur, je nachdem, wie Sie Ihre Citrix ADC- und Kubernetes-Umgebung verwalten möchten.

Einheitliches Ingress (einstufig)

In einer einheitlichen Ingress-Architektur (einstufig) wird ein Citrix MPX- oder VPX-Gerät, das außerhalb des Kubernetes-Clusters bereitgestellt wird, mithilfe des Citrix ingress controller in die Kubernetes-Umgebung integriert. Der Citrix ingress controller wird als Pod im Kubernetes-Cluster bereitgestellt und automatisiert die Konfiguration von Citrix ADCs basierend auf Änderungen an den Microservices oder den Ingress-Ressourcen. Das Citrix ADC Gerät führt Funktionen wie Lastenausgleich, TLS-Beendigung und HTTP- oder TCP-Protokolloptimierungen für eingehenden Datenverkehr aus und leitet den Datenverkehr dann an den richtigen Microservice innerhalb eines Kubernetes-Clusters weiter. Diese Architektur eignet sich am besten in Szenarien, in denen das gleiche Team die Kubernetes-Plattform und andere Netzwerkinfrastrukturen wie Application Delivery Controller (ADCs) verwaltet.

Das folgende Diagramm zeigt eine Bereitstellung mit der einheitlichen Ingress-Architektur.



Eine einheitliche Ingress-Lösung bietet die folgenden wesentlichen Vorteile:

- Bietet eine Möglichkeit, die Funktionen Ihrer vorhandenen Citrix ADC Infrastruktur auf die Kubernetes-Umgebung zu erweitern
- Ermöglicht Ihnen das Anwenden von Datenverkehrsmanagementrichtlinien für eingehenden Datenverkehr
- Bietet eine vereinfachte Architektur, die für netzwerkfähige DevOps-Teams geeignet ist
- Unterstützt Mandantenfähigkeit

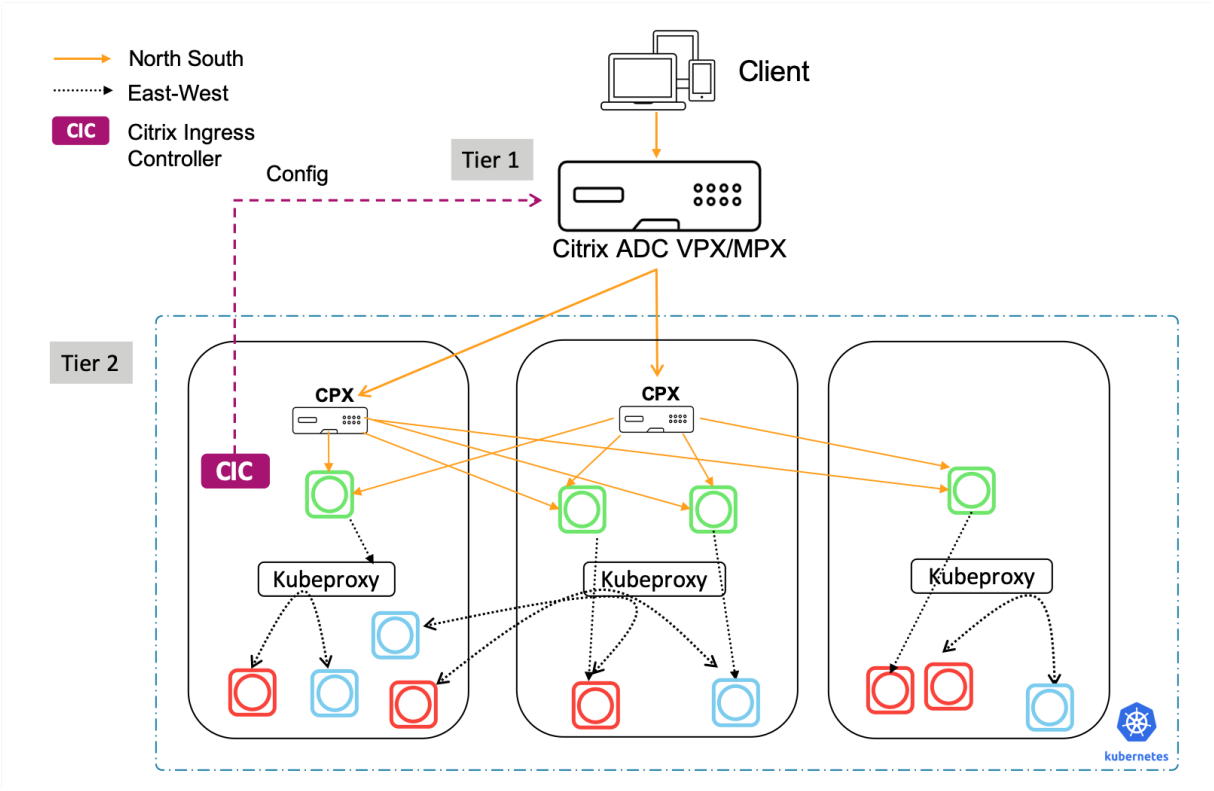
Zweistufiges Eindringen

In einer Dual-Tier-Architektur fungiert Citrix ADC (MPX oder VPX), die außerhalb des Kubernetes-Clusters bereitgestellt werden, auf Ebene 1 und Lastenausgleich zwischen Nord-Süd-Datenverkehr und Citrix ADC-CPXs, die innerhalb des Clusters ausgeführt werden. Citrix ADC CPX fungiert auf Stufe 2 und führt Load Balancing für Microservices innerhalb des Kubernetes-Clusters durch.

In Szenarien, in denen separate Teams die Kubernetes-Plattform und die Netzwerkinfrastruktur verwalten, ist die Dual-Tier-Architektur am besten geeignet.

Netzwerkteams verwenden Citrix ADC Tier 1 für Anwendungsfälle wie GSLB, TLS-Beendigung auf der Hardwareplattform und TCP-Lastenausgleich. Kubernetes-Plattform-Teams können Tier 2 Citrix ADC (CPX) für Layer 7 (HTTP/HTTPS) Lastausgleich, gegenseitiges TLS sowie Beobachtbarkeit oder Überwachung von Microservices verwenden. Der Citrix ADC (CPX) der Stufe 2 kann eine andere Software-Release-Version als der Citrix ADC der Stufe 1 haben, um neu verfügbare Funktionen zu erfüllen.

Das folgende Diagramm zeigt eine Bereitstellung mit Dual-Tier-Architektur.



Ein Dual-Tier-Ingress bietet die folgenden wesentlichen Vorteile:

- Gewährleistet hohe Geschwindigkeit der Anwendungsentwicklung für Entwickler oder Plattform-Teams
- Ermöglicht die Anwendung von entwicklergesteuerten Verkehrsmanagementrichtlinien für Microservices innerhalb des Kubernetes-Clusters
- Ermöglicht Cloud-Skalierung und Mandantenfähigkeit

Weitere Informationen finden Sie in der Dokumentation zu Citrix ingress controller.

Erste Schritte

Um mit der Kubernetes Ingress Lösung von Citrix zu beginnen, können Sie die folgenden Beispiele ausprobieren:

- Lastenausgleich Ingress-Datenverkehr mit Citrix ADC CPX in Minikube
- Lastenausgleich Nord-Süd-Ingress-Datenverkehr mit Citrix ADC CPX-Proxy
- Lastenausgleich Ost-West-Microservice-Datenverkehr mit Citrix ADC CPX-Proxy
- Tiefer Tauchgang über Kubernetes Features mit Citrix ADC CPX

Service-Mesh

October 5, 2021

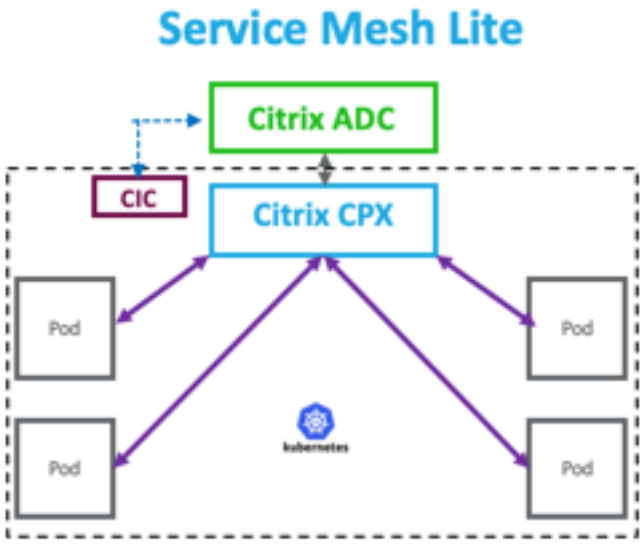
Ein Service-Mesh ist eine Infrastrukturschicht für die Verarbeitung von Service-to-Service-Kommunikation für cloudnative Anwendungen, die APIs verwenden. Es bietet eine Möglichkeit, Ihre Microservices zu verbinden, zu sichern und zu überwachen. Citrix bietet zwei Lösungen, um Ihre Service-Mesh-Anforderungen zu erfüllen:

- Service Mesh lite
- Service-Mesh (Citrix ADC Integration mit Istio)

Service Mesh lite

Eine vollwertige Service-Mesh-Implementierung ist komplex und erfordert eine steile Lernkurve. Wenn Sie nach einer vereinfachten Implementierung eines Servicemesh mit ähnlichen Vorteilen suchen, bietet Citrix eine Lösung namens Service Mesh Lite mit geringerer Komplexität. In dieser Lösung wird ein Citrix ADC CPX als zentralisierter Lastausgleichsdienst im Kubernetes-Cluster ausgeführt und der Lastenausgleich zwischen den Mikrodiensten erfolgt. Citrix ADC CPX erzwingt Richtlinien für eingehenden und intercontainerübergreifenden Datenverkehr.

Das folgende Diagramm zeigt eine Service-Mesh-Lite-Architektur.



Weitere Informationen finden Sie in der Service Mesh Lite-Dokumentation.

Service-Mesh (Citrix ADC Integration mit Istio)

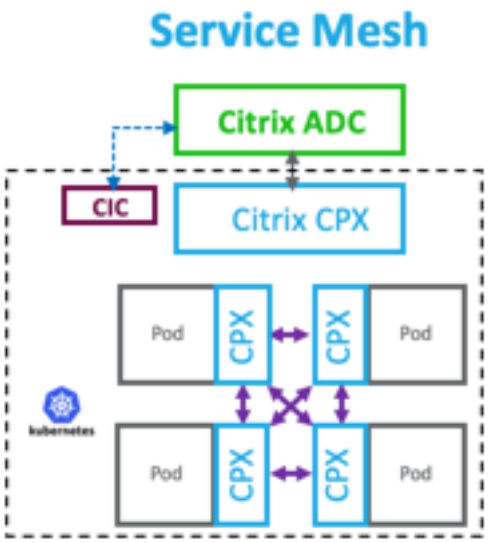
Citrix bietet eine Service-Mesh-Lösung durch die Integration von Citrix ADC in Istio. Istio, ein Open Source und plattformunabhängiges Service-Mesh, ist eine der beliebtesten Service-Mesh-Implementierungen. Durch die Integration von Citrix ADC in Istio können Sie die Citrix ADC-Funktionen nutzen, um den Datenverkehr für Anwendungen im Service-Mesh zu sichern und zu optimieren.

Citrix ADC kann auf folgende Weise in Istio integriert werden:

- Citrix ADC MPX, VPX oder CPX als Istio Ingress Gateway an das Service-Mesh, um Datenverkehr für den Kubernetes-Cluster verfügbar zu machen.
- Citrix ADC CPX als Beiwagen Proxy mit Anwendungscontainern im Service-Mesh zur Steuerung der Kommunikation zwischen Anwendungen.

Sie können entweder die Integration unabhängig verwenden, oder Sie können beide Möglichkeiten kombinieren, um eine einheitliche Datenebenenlösung zu haben.

Das folgende Diagramm zeigt eine Service-Mesh-Architektur.



Service Mesh ist ideal für hochsichere Anwendungen und bietet auch folgende Vorteile.

- Bietet feinkörniges (modularisiertes) Verkehrsmanagement pro Container
- Sorgt für eine umfassendere Beobachtbarkeit, Analyse und Sicherheit (Mutual TLS) aufgrund der Sidecar Implementierung
- Ermöglicht die automatisierte Kanary-Bereitstellung für jeden Container mit integriertem Citrix ADC CPX

- Unterstützt Cloud-Portabilität
- Ermöglicht das Auslagern einiger der von Anwendungen ausgeführten Funktionen auf den Beiwagen
- Bietet geringere Seitenwagen Latenz
- Bietet Integrationen mit Open-Source-Tools
- Bietet Skalierbarkeit

Weitere Informationen finden Sie in der Dokumentation zu Citrix ADC Integration mit Istio.

Lösungen für Beobachtbarkeit

October 5, 2021

In einer Microservices-basierten Architektur ist die Transparenz der Service-zu-Service-Kommunikation von entscheidender Bedeutung, um eine effiziente und robuste Architektur aufzubauen. Herkömmliche Methoden zur Protokollierung und Überwachung sind nicht in der Lage, die Herausforderungen einer Microservices-Architektur zu bewältigen. Die Observability-Lösungen von Citrix bieten Ihnen die Möglichkeit zu sehen, was passiert, wenn Ihre Dienste miteinander interagieren und aussagekräftige Einblicke in Ihr System erhalten.

Citrix bietet die folgenden Lösungen, um die Anforderungen an die Beobachtbarkeit Ihrer Microservices-Architektur zu erfüllen:

- Citrix ADM Service Graph und Analytics
- Citrix ADC Observability Exporteur

Citrix ADM Service Graph und Analytics

Citrix Application Delivery Management (ADM) ist eine zentralisierte Verwaltungslösung, die unternehmensweite Transparenz und Automatisierung für Verwaltungsaufträge bietet, die über mehrere Instanzen hinweg ausgeführt werden müssen.

In einer Microservice-Architektur stellt die Fehlerbehebung eine Herausforderung dar, da sich eine einzelne Endbenutzeranforderung über mehrere Microservices erstrecken kann.

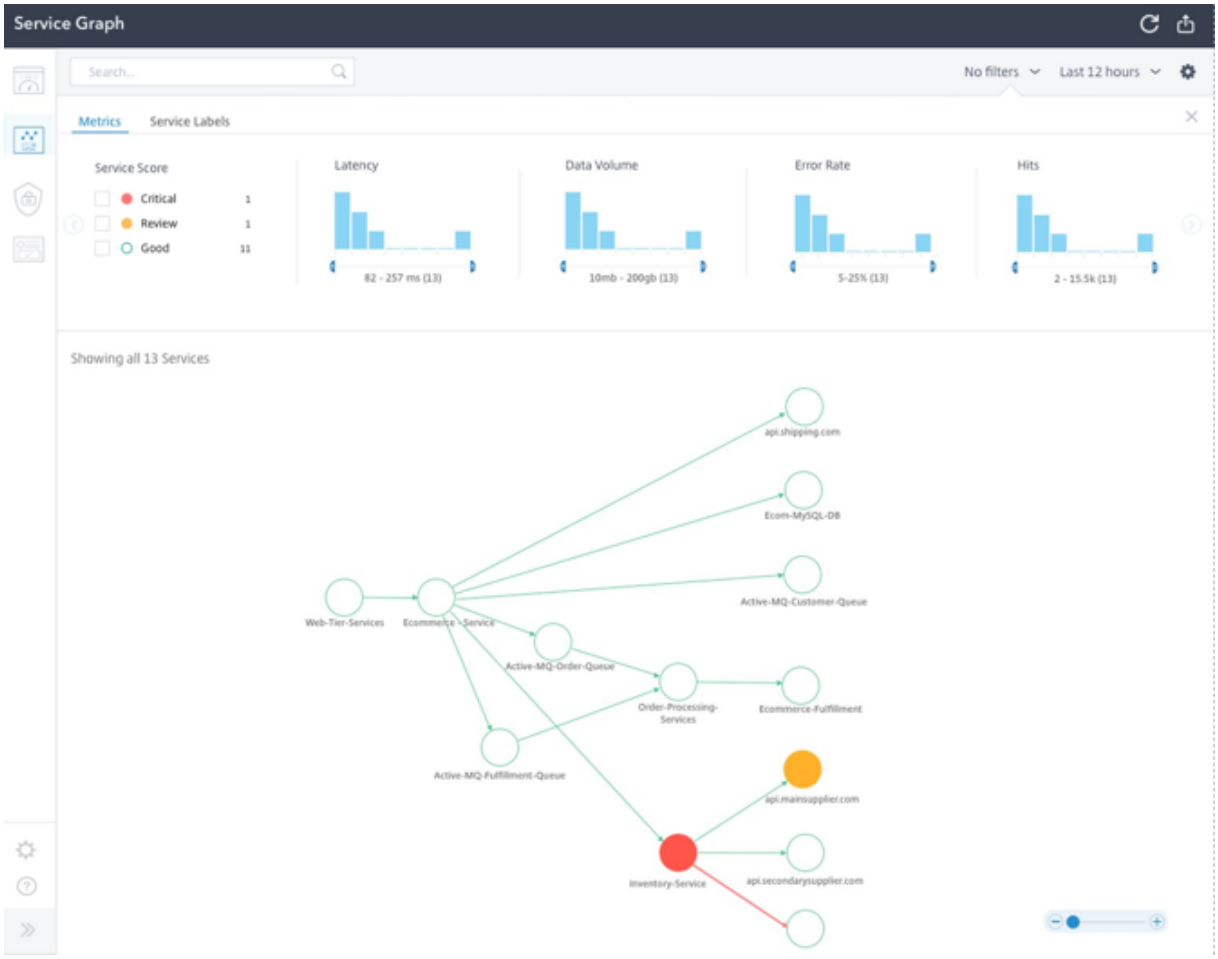
Das Service-Graph und die Analyse von Citrix ADM bieten Einblick in Interaktionen zwischen Microservices und helfen, Probleme basierend auf verschiedenen Metriken wie Latenz- und HTTP-Fehlern zu identifizieren und zu beheben.

Citrix ADM bietet auch erweiterte Analysen basierend auf Metriken und Transaktionsprotokollen, die von Citrix ADC erfasst wurden.

Citrix ADM Lösung bietet folgende Vorteile:

- Bietet einen einzigen Fensterbereich für Anwendungen in Containern, lokal oder in der Cloud
- Bietet bessere Beobachtbarkeit und schnellere Fehlerbehebung für Microservices
- Unterstützt die Bereitstellung von Canary

Das folgende Diagramm zeigt ein Beispieldienstdiagramm für eine Anwendung, die mehrere Microservices enthält.



Weitere Informationen zum Einrichten von Citrix ADM Service Graph und Analytics finden Sie im Service-Diagramm und in der Analytics-Dokumentation .

Citrix ADC Observability Exporteur

Citrix ADC Observability Exporter ist ein Container, der Metriken und Transaktionen von Citrix ADCs sammelt und sie in geeignete Formate (wie JSON, AVRO) für unterstützte Endpunkte umwandelt. Sie können die vom Citrix ADC Observability Exporter gesammelten Daten auf den gewünschten Endpunkt exportieren. Durch die Analyse der Daten erhalten Sie wertvolle Erkenntnisse auf Microservice-Ebene für Anwendungen, die von Citrix ADCs weitergeleitet werden.

Unterstützung für verteilte Ablaufverfolgung

Verteilte Tracer ermöglichen es Ihnen, den Datenfluss zwischen Ihren Microservices zu visualisieren und helfen, Engpässe in Ihrer Microservices-Architektur zu identifizieren. OpenRacing ist eine Spezifikation und ein Standardsatz von APIs zum Entwerfen und Implementieren von verteiltem Tracing.

Der Citrix Observability Exporter implementiert Distributed Tracing für Citrix ADC und unterstützt derzeit Zipkin als verteilter Tracer.

Sie können die Trace-Analyse verbessern, indem Sie Elasticsearch und Kibana mit Zipkin verwenden. Elasticsearch ermöglicht eine langfristige Aufbewahrung der Trace-Daten. Mit Kibana erhalten Sie viel tieferen Einblick in die Daten, indem Sie ein Tool zum Erkunden und Visualisieren von Protokollnachrichten bereitstellen.

Unterstützung für Transaktionssammlung und Streaming-Unterstützung

Der Citrix ADC Observability Exporter unterstützt das Sammeln von Transaktionen und das Streamen an Endpunkte. Derzeit unterstützt Citrix ADC Observability Exporter Elasticsearch und Kafka als Transaktionsendpunkte.

Weitere Informationen finden Sie in der Dokumentation zum Citrix ADC Observability Exporter.

Aktivieren von Analysen mithilfe von Anmerkungen in der YAML-Datei des Citrix ingress controller

Sie können Analysen mithilfe des Analyseprofils aktivieren, das in Ingress oder Service vom Typ LoadBalancer-Konfiguration als intelligente Annotation definiert ist. Sie können die spezifischen Parameter definieren, die Sie überwachen müssen, indem Sie sie in der Ingress- oder Dienstkonfiguration der Anwendung angeben. Weitere Informationen zum Aktivieren von Analysen mit Anmerkungen finden Sie unter Analytics mit Anmerkungen.

API-Gateway für Kubernetes

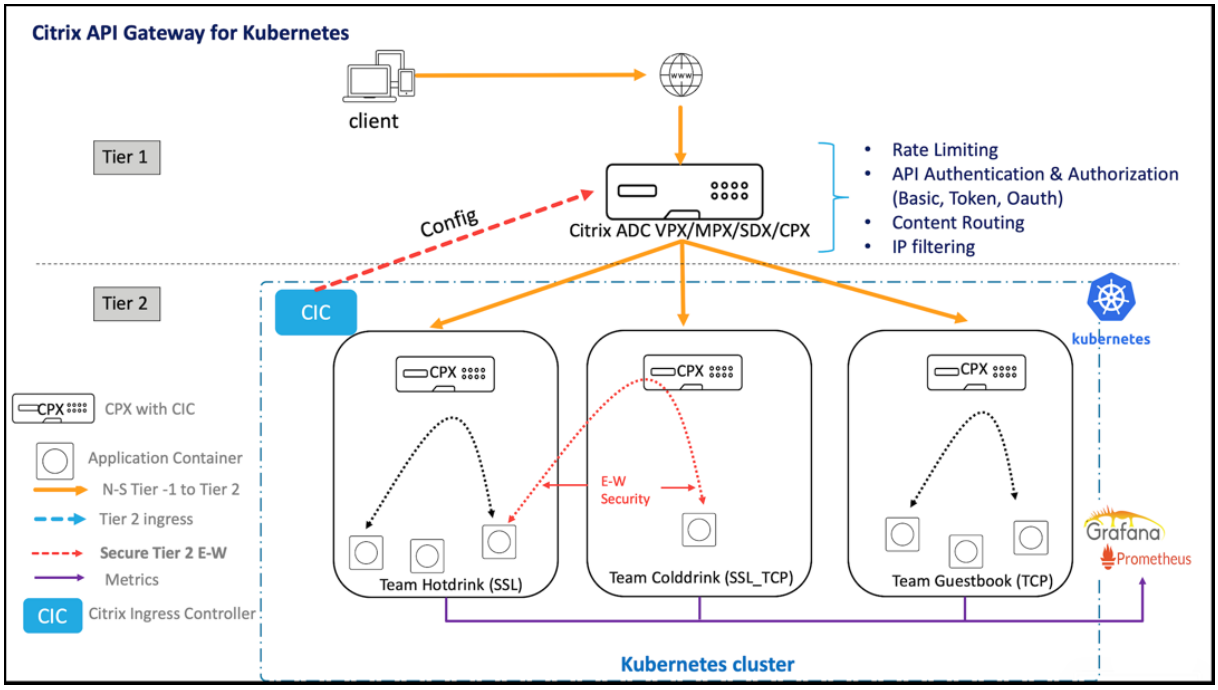
October 5, 2021

Ein API-Gateway fungiert als einziger Einstiegspunkt für Ihre APIs und gewährleistet einen sicheren und zuverlässigen Zugriff auf mehrere APIs und Microservices in Ihrem System.

Citrix stellt ein API-Gateway der Enterprise-Klasse für den Nord-Süd-API-Datenverkehr in den Kubernetes-Cluster bereit. Das
API-Gateway kann mit Kubernetes über den Citrix Ingress Controller und den Citrix ADC (Citrix ADC

MPX, VPX oder CPX) integriert werden, der als Ingress Gateway für lokale oder Cloud-Bereitstellungen bereitgestellt wird.

Das folgende Diagramm zeigt eine zweistufige Topologie für das API-Gateway.



Mit dem von Citrix angebotenen API-Gateway können Sie die folgenden Funktionen ausführen:

- Erzwingen von Authentifizierungsrichtlinien
- Tarifbeschränkung des Zugangs zu Diensten
- Erweitertes Content-Routing
- Flexible und umfassende Transformation von HTTP-Transaktionen unter Verwendung der Rewrite- und Responder-Richtlinien
- Durchsetzung von Firewall-Richtlinien für Webanwendungen

Wie funktioniert das API-Gateway?

Das API-Gateway basiert auf dem Citrix Ingress-Gateway und verwendet Kubernetes-API-Erweiterungen wie benutzerdefinierte Ressourcendefinitionen (CRDs). Mithilfe von CRDs können Sie das Citrix ADC und das API-Gateway automatisch in derselben Instanz konfigurieren.

Citrix stellt die folgenden CRDs für das API-Gateway bereit:

- Authentifizierungs-CRD
- Grenzwert CRD
- Content-Routing CRD
- Rewrite und Responder CRD
- WAF CRD

Wesentliche Vorteile der Verwendung des API-Gateway

Im Folgenden werden die wichtigsten Vorteile des von Citrix angebotenen API-Gateway aufgeführt:

- Verwendet das erweiterte Verkehrsmanagement und die umfassenden Sicherheitsfunktionen von Citrix ADC.
- Optimiert Ihre Bereitstellungen, indem mehrere Netzwerkfunktionen in einer einzigen Komponente des Citrix Ingress-Gateway konsolidiert werden.
- Reduziert die betriebliche Komplexität und Kosten für die Bereitstellung mehrerer Komponenten.
- Sorgt für eine bessere Leistung für den Anwendungsdatenverkehr, indem mehrere Hops der TCP- oder TLS-Entschlüsselung reduziert werden, während separate Komponenten verwendet werden.
- Vereinfacht die Bereitstellung und Integration in Ihre Kubernetes-Umgebungen, entweder durch direkte Verwendung von YAMLs oder Helmcharts.

Bereitstellen des API-Gateway

Weitere Informationen zum Konfigurieren der API-Gateway Features mithilfe von CRDs finden Sie in der Dokumentation des Citrix Ingress Controller:

- Authentifizierung
- Ratenbegrenzung
- Erweitertes Content-Routing
- Richtlinien für Rewrite und Responder
- Richtlinien für die Firewall von Webanwendungen

Verwenden Sie Citrix ADM zur Fehlerbehebung bei nativen Citrix Cloud-Netzwerken

February 24, 2022

Übersicht

Dieses Dokument enthält Informationen darüber, wie Sie Citrix ADM verwenden können, um Kubernetes-Microservice-Anwendungen bereitzustellen und zu überwachen. Sie beschäftigen sich auch mit der Verwendung der CLI, der Dienstdiagramme und der Ablaufverfolgung, damit die Plattform- und SRE-Teams Probleme beheben können.

Überblick über Anwendungsleistung und Latenz

TLS-Verschlüsselung

TLS ist ein Verschlüsselungsprotokoll zur Sicherung der Internetkommunikation. Ein TLS-Handshake ist der Prozess, der eine Kommunikationssitzung startet, die TLS-Verschlüsselung verwendet. Während eines TLS-Handshakes tauschen die beiden kommunizierenden Seiten Nachrichten aus, um sich gegenseitig zu bestätigen, sich gegenseitig zu verifizieren, die von ihnen verwendeten Verschlüsselungsalgorithmen festzulegen und Sitzungsschlüssel zu vereinbaren. TLS-Handshakes sind ein grundlegender Bestandteil der Funktionsweise von HTTPS.

TLS im Vergleich zu SSL-Handshakes

SSL (Secure Sockets Layer) war das ursprüngliche Verschlüsselungsprotokoll, das für HTTP entwickelt wurde. TLS (Transport Layer Security) hat SSL vor einiger Zeit ersetzt. SSL-Handshakes werden jetzt TLS-Handshakes genannt, obwohl der Name “SSL” immer noch weit verbreitet ist.

Wann findet ein TLS-Handshake statt?

Ein TLS-Handshake findet immer dann statt, wenn ein Benutzer über HTTPS zu einer Website navigiert und der Browser zuerst den Original-Server der Website abfragt. Ein TLS-Handshake findet auch dann statt, wenn andere Kommunikationen HTTPS verwenden, einschließlich API-Aufrufe und DNS-über-HTTPS-Abfragen.

TLS-Handshakes treten auf, nachdem eine TCP-Verbindung über einen TCP-Handshake geöffnet wurde.

Was passiert während eines TLS-Handshakes?

- Während eines TLS-Handshakes führen der Client und der Server zusammen Folgendes aus:
  - Geben Sie an, welche Version von TLS (TLS 1.0, 1.2, 1.3 usw.) sie verwenden.
  - Entscheiden Sie, welche Verschlüsselungssammlungen (siehe folgenden Abschnitt) sie verwenden.
  - Authentifizieren Sie die Identität des Servers über den öffentlichen Schlüssel des Servers und die digitale Signatur der SSL-Zertifizierungsstelle.
  - Generieren Sie Sitzungsschlüssel, um die symmetrische Verschlüsselung zu verwenden, nachdem der Handshake abgeschlossen ist.

Was sind die Schritte eines TLS-Handshakes?

- TLS-Handshakes sind eine Reihe von Datagrammen oder Nachrichten, die von einem Client und einem Server ausgetauscht werden. Ein TLS-Handshake umfasst mehrere Schritte, da der Client und der Server die Informationen austauschen, die für den Abschluss des Handshakes und die Ermöglichung weiterer Konversationen erforderlich sind.

Die genauen Schritte innerhalb eines TLS-Handshakes variieren je nach Art des verwendeten Schlüsselaustauschalgorithmus und den von beiden Seiten unterstützten Verschlüsselungssammlungen. Der

RSA-Schlüsselaustauschalgorithmus wird am häufigsten verwendet. Es geht wie folgt:

1. `client hello`-Meldung: Der Client initiiert den Handshake, indem er eine "Hallo" -Nachricht an den Server sendet. Die Meldung enthält, welche TLS-Version der Client unterstützt, welche Verschlüsselungssammlungen unterstützt werden und eine Reihe von zufälligen Bytes, die als "client random" bezeichnet werden.
2. `server hello`-Meldung: Als Antwort auf die Hello-Nachricht des Clients sendet der Server eine Nachricht mit dem SSL-Zertifikat des Servers, der vom Server ausgewählten Verschlüsselungssammlung und dem "zufälligen Server", einer weiteren zufälligen Bytefolge, die vom Server generiert wird.
3. Authentifizierung: Der Client überprüft das SSL-Zertifikat des Servers bei der Zertifizierungsstelle, die es ausgestellt hat. Dies bestätigt, dass der Server der ist, für den er sich ausgibt, und dass der Client mit dem tatsächlichen Eigentümer der Domäne interagiert.
4. Das Premaster-Secret: Der Client sendet eine weitere zufällige Bytefolge, das "premaster secret". Das Premaster-Secret ist mit dem öffentlichen Schlüssel verschlüsselt und kann nur mit dem privaten Schlüssel vom Server entschlüsselt werden. (Der Client erhält den öffentlichen Schlüssel aus dem SSL-Zertifikat des Servers.)
5. Verwendeter privater Schlüssel: Der Server entschlüsselt das Premaster-Secret.
6. Sitzungsschlüssel erstellt: Sowohl der Client als auch der Server generieren Sitzungsschlüssel aus dem zufälligen Client, dem zufälligen Server und dem Premaster-Secret. Sie sollten zu den gleichen Ergebnissen kommen.
7. Der Client ist bereit: Der Client sendet eine "fertige" Nachricht, die mit einem Sitzungsschlüssel verschlüsselt ist.
8. Server ist bereit: Der Server sendet eine "fertige" Nachricht, die mit einem Sitzungsschlüssel verschlüsselt ist.
9. Sichere symmetrische Verschlüsselung erreicht: Der Handshake ist abgeschlossen und die Kommunikation wird unter Verwendung der Sitzungsschlüssel fortgesetzt.

Alle TLS-Handshakes verwenden eine asymmetrische Verschlüsselung (den öffentlichen und privaten Schlüssel), aber nicht alle verwenden den privaten Schlüssel beim Generieren von Sitzungsschlüsseln. Ein kurzlebiger Diffie-Hellman-Handschlag läuft beispielsweise wie folgt ab:

1. Client-Hallo: Der Client sendet eine Client-Hello-Nachricht mit der Protokollversion, dem zufälligen Client und einer Liste von Verschlüsselungssammlungen.

2. Server-Hallo: Der Server antwortet mit seinem SSL-Zertifikat, seiner ausgewählten Verschlüsselungssammlung und dem Server zufällig. Im Gegensatz zu dem im vorherigen Abschnitt beschriebenen RSA-Handshake enthält der Server in dieser Nachricht auch Folgendes (Schritt 3).

3. Digitale Signatur des Servers: Der Server verwendet seinen privaten Schlüssel, um den Client zufällig, den Server zufällig und seinen DH-Parameter* zu verschlüsseln. Diese verschlüsselten Daten fungieren als digitale Signatur des Servers und stellen fest, dass der Server über den

privaten Schlüssel verfügt, der mit dem öffentlichen Schlüssel aus dem SSL-Zertifikat übereinstimmt.

4. Digitale Signatur bestätigt: Der Client entschlüsselt die digitale Signatur des Servers mit dem öffentlichen Schlüssel und überprüft, ob der Server den privaten Schlüssel kontrolliert und wer er vorgibt zu sein. Client-DH-Parameter: Der Client sendet seinen DH-Parameter an den Server.
5. Client und Server berechnen das Premaster-Secret: Anstatt dass der Client das Premaster-Secret generiert und an den Server sendet, wie bei einem RSA-Handshake, verwenden der Client und der Server die ausgetauschten DH-Parameter, um ein passendes Premaster-Secret separat zu berechnen.
6. Sitzungsschlüssel erstellt: Jetzt berechnen der Client und der Server Sitzungsschlüssel aus dem Premaster-Secret, dem Client zufällig und dem Server zufällig, genau wie bei einem RSA-Handshake.
    - **Der Kunde ist bereit** Wie ein RSA-Handshake
    - Server ist bereit
    - Sichere symmetrische Verschlüsselung erreicht

    *DH-Parameter: DH steht für Diffie-Hellman. Der Diffie-Hellman-Algorithmus verwendet Exponentialberechnungen, um zum selben Premaster-Secret zu gelangen. Der Server und der Client stellen jeweils einen Parameter für die Berechnung bereit, und wenn sie kombiniert werden, führen sie zu einer anderen Berechnung auf jeder Seite, wobei die Ergebnisse gleich sind.

Weitere Informationen zum Kontrast zwischen kurzlebigen Diffie-Hellman-Handshakes und anderen Arten von Handshakes und wie sie eine Vorwärtsgeheimnis erreichen, finden Sie in dieser TLS-Protokolldokumentation.

Was ist eine Verschlüsselungssammlung?

- Eine Verschlüsselungssuite ist eine Reihe von Verschlüsselungsalgorithmen, die beim Aufbau einer sicheren Kommunikationsverbindung verwendet werden. (Ein Verschlüsselungsalgorithmus ist eine Reihe mathematischer Operationen, die an Daten ausgeführt werden, um die Daten zufällig erscheinen zu lassen.) Es gibt verschiedene Verschlüsselungssammlungen, die weit verbreitet sind, und ein wesentlicher Bestandteil des TLS-Handshakes ist die Vereinbarung, welche Verschlüsselungssammlung für diesen Handshake verwendet wird.

Für die ersten Schritte siehe Referenz: TLS-Protokolldokumentation.

Citrix Application Delivery Management-SSL-Dashboard

Citrix Application Delivery Management (ADM) optimiert jetzt jeden Aspekt der Zertifikatsverwaltung für Sie. Über eine einzige Konsole können Sie automatisierte Richtlinien einrichten, um den richtigen Aussteller, die richtige Schlüsselstärke und korrekte Algorithmen sicherzustellen, während Sie nicht

verwendete oder bald ablaufende Zertifikate im Auge behalten. Um das SSL-Dashboard von Citrix ADM und seine Funktionen zu verwenden, müssen Sie wissen, was ein SSL-Zertifikat ist und wie Sie Citrix ADM verwenden können, um Ihre SSL-Zertifikate zu verfolgen.

Ein SSL-Zertifikat (Secure Socket Layer), das Teil einer SSL-Transaktion ist, ist ein digitales Eingabeformular (X509), das ein Unternehmen (Domain) oder eine Person identifiziert. Das Zertifikat verfügt über eine Public-Key-Komponente, die für jeden Client sichtbar ist, der eine sichere Transaktion mit dem Server initiieren möchte. Der entsprechende private Schlüssel, der sich sicher auf der Citrix Application Delivery Controller (ADC) -Appliance befindet, wird verwendet, um die Verschlüsselung und Entschlüsselung des asymmetrischen Schlüssels (oder des öffentlichen Schlüssels) abzuschließen.

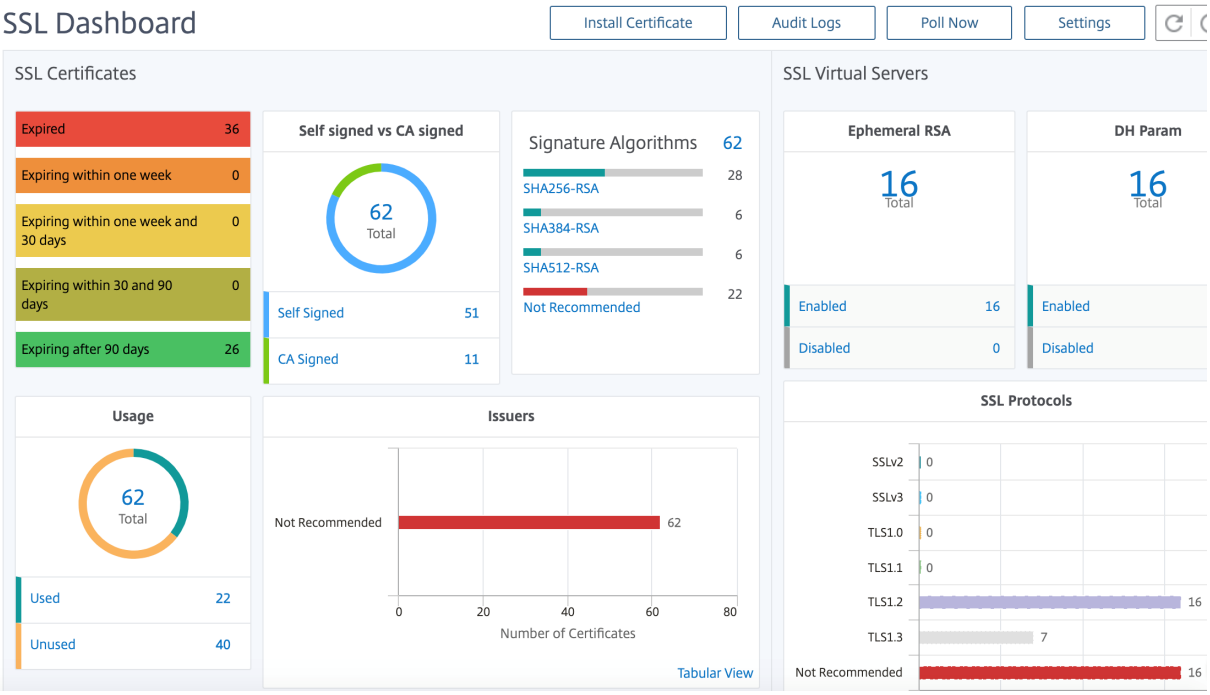
Sie können ein SSL-Zertifikat und einen Schlüssel auf eine der folgenden Arten beziehen:

- Von einer autorisierten Zertifizierungsstelle (CA)
- Durch Generieren eines neuen SSL-Zertifikats und eines neuen Schlüssels auf der Citrix ADC-Appliance

Citrix ADM bietet eine zentrale Ansicht der in allen verwalteten Citrix ADC-Instanzen installierten SSL-Zertifikate. Im SSL-Dashboard können Sie Diagramme anzeigen, mit denen Sie Zertifikatsaussteller, wichtige Stärken, Signaturalgorithmen, abgelaufene oder nicht verwendete Zertifikate usw. nachverfolgen können. Sie können auch die Verteilung der SSL-Protokolle sehen, die auf Ihren virtuellen Servern ausgeführt werden, und die Schlüssel, die auf ihnen aktiviert sind.

Sie können auch Benachrichtigungen einrichten, um Sie darüber zu informieren, wann Zertifikate ablaufen werden, und Informationen darüber enthalten, welche Citrix ADC-Instanzen diese Zertifikate verwenden.

Sie können die Zertifikate einer Citrix ADC Instanz mit einem Zertifizierungsstellenzertifikat verknüpfen. Stellen Sie jedoch sicher, dass die Zertifikate, die Sie mit demselben CA-Zertifikat verknüpfen, dieselbe Quelle und denselben Aussteller haben. Nachdem Sie die Zertifikate mit einem CA-Zertifikat verknüpft haben, können Sie die Verknüpfung aufheben.



Um loszulegen, lesen Sie die SSL-Dashboard-Dokumentation.

Integrationen von Drittanbietern

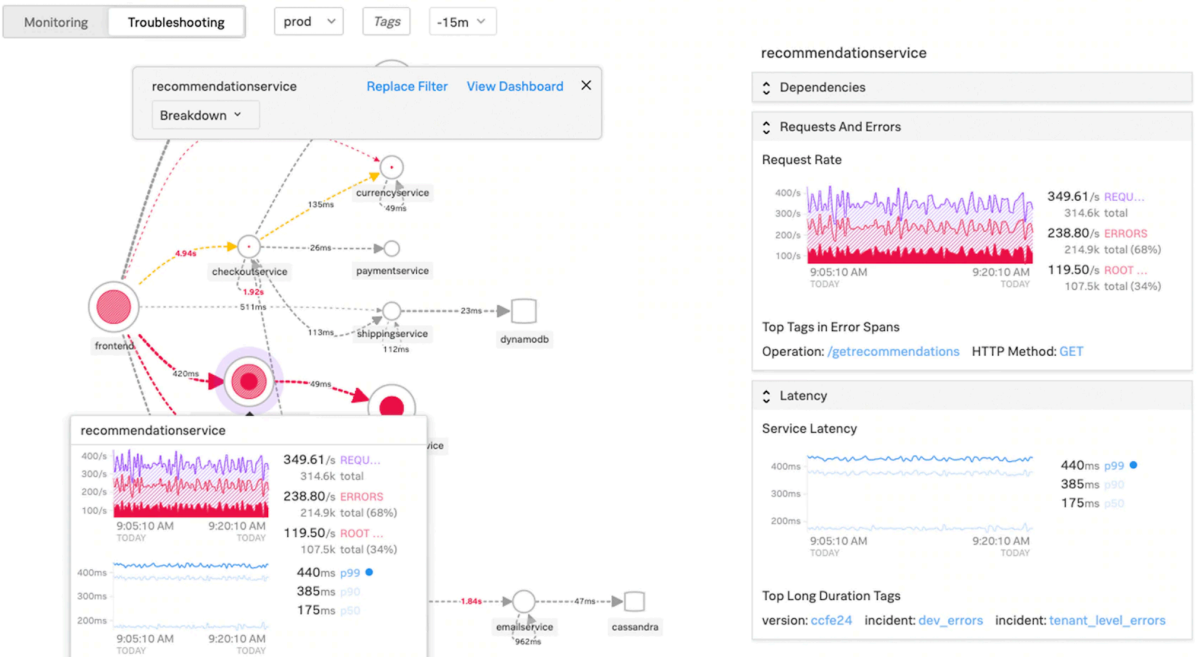
Die Anwendungslatenz wird in Millisekunden gemessen und kann je nach verwendeter Metrik eines von zwei Dingen anzeigen. Die gebräuchlichere Methode zur Messung der Latenz wird als “Round-Trip-Zeit” (oder RTT) bezeichnet. RTT berechnet die Zeit, die ein Datenpaket benötigt, um im Netzwerk von einem Punkt zum anderen zu gelangen und eine Antwort an die Quelle zurückzusenden. Die andere Messung wird als “Time to First Byte” (oder TTFB) bezeichnet und zeichnet die Zeit auf, die vom Zeitpunkt, an dem ein Paket einen Punkt im Netzwerk verlässt, bis zu dem Moment, zu dem es an seinem Ziel ankommt, benötigt wird. RTT wird häufiger zur Messung der Latenz verwendet, da es von einem einzigen Punkt im Netzwerk aus ausgeführt werden kann und keine Datenerfassungssoftware auf dem Zielpunkt installiert werden muss (wie dies bei TTFB der Fall ist).

Durch die Überwachung der Bandbreitennutzung und -leistung Ihrer Anwendung in Echtzeit erleichtert der ADM-Dienst die Identifizierung von Problemen und die vorbeugende Behandlung potenzieller Probleme, bevor sie sich manifestieren und Benutzer in Ihrem Netzwerk betreffen. Diese Flow-basierte Lösung verfolgt die Nutzung nach Schnittstelle, Anwendung und Konversation und liefert Ihnen detaillierte Informationen zu Aktivitäten in Ihrem Netzwerk.

Verwenden von Splunk-Tools

Infrastruktur und Anwendungsleistung sind voneinander abhängig. Um das vollständige Bild zu sehen, bietet SignalFX eine nahtlose Korrelation zwischen der Cloud-Infrastruktur und den darauf

laufenden Microservices. Wenn Ihre Anwendung aufgrund von Speicherverlust, einem verrauschten Nachbarcontainer oder einem anderen infrastrukturbezogenen Problem auftritt, informiert SignalFX Sie darüber. Um das Bild zu vervollständigen, ermöglicht der kontextbezogene Zugriff auf Splunk-Protokolle und -Ereignisse eine tiefere Fehlerbehebung und Ursachenanalyse.



Weitere Informationen zu SignalFX Microservices APM und zur Fehlerbehebung mit Splunk finden Sie unter Splunk für DevOps-Informationen .

MongoDB-Unterstützung

MongoDB speichert Daten in flexiblen, JSON-ähnlichen Dokumenten. Bedeutungsfelder können von Dokument zu Dokument variieren und die Datenstruktur kann im Laufe der Zeit geändert werden.

Das Dokumentmodell wird den Objekten in Ihrem Anwendungscode zugeordnet, sodass Sie problemlos mit Daten arbeiten können.

On-Demand-Abfragen, Indizierung und Echtzeitaggregation bieten leistungsstarke Möglichkeiten, auf Ihre Daten zuzugreifen und sie zu analysieren.

MongoDB ist im Kern eine verteilte Datenbank, sodass Hochverfügbarkeit, horizontale Skalierung und geografische Verteilung integriert und einfach zu bedienen sind.

MongoDB wurde entwickelt, um die Anforderungen moderner Apps mit einer technologischen Grundlage zu erfüllen, die Ihnen Folgendes ermöglicht:

- Das Dokumentdatenmodell — das Ihnen die beste Art bietet, mit Daten zu arbeiten.
- Ein Design verteilter Systeme, mit dem Sie Daten intelligent dort ablegen können, wo Sie sie haben möchten.

- Ein einheitliches Erlebnis, das Ihnen die Freiheit gibt, überall zu arbeiten, sodass Sie Ihre Arbeit zukunftssicher machen und die Anbieterbindung vermeiden können.

Mit diesen Funktionen können Sie eine Intelligent Operational Data Platform aufbauen, die von MongoDB unterstützt wird. Weitere Informationen finden Sie in der MongoDB-Dokumentation.

Lastenausgleich für eingehenden Datenverkehr zu TCP- oder UDP-basierten Anwendungen

In einer Kubernetes-Umgebung ist ein Ingress ein Objekt, das den Zugriff auf die Kubernetes-Dienste von außerhalb des Kubernetes-Clusters ermöglicht. Bei Standard-Kubernetes Ingress-Ressourcen wird davon ausgegangen, dass der gesamte Datenverkehr HTTP-basiert ist und keine nicht-HTTP-basierten Protokolle wie TCP, TCP-SSL und UDP unterstützt. Daher können kritische Anwendungen, die auf L7-Protokollen wie DNS, FTP, LDAP basieren, nicht mit Standard-Kubernetes Ingress verfügbar gemacht werden.

Die Kubernetes-Standardlösung besteht darin, einen Dienst vom Typ LoadBalancer zu erstellen. Weitere Informationen finden Sie unter Service Type LoadBalancer in Citrix ADC .

Die zweite Option besteht darin, das Eingangsobjekt mit Anmerkungen zu versehen. Mit dem Citrix ingress controller können Sie TCP- oder UDP-basierten Ingress-Datenverkehr ausgleichen. Es enthält die folgenden Anmerkungen, die Sie in Ihrer Kubernetes Ingress-Ressourcendefinition verwenden können, um den TCP- oder UDP-basierten Ingress-Datenverkehr zu belasten:

- ingress.citrix.com/insecure-service-type: Die Annotation ermöglicht den L4-Lastausgleich mit TCP, UDP oder ANY als Protokoll für Citrix ADC.
- ingress.citrix.com/insecure-port: Die Annotation konfiguriert den TCP-Port. Die Anmerkung ist hilfreich, wenn Micro-Service-Zugriff an einem nicht standardmäßigen Port erforderlich ist. Standardmäßig ist Port 80 konfiguriert.

Weitere Informationen finden Sie unter Load Balancing von eingehendem Datenverkehr zu TCP- oder UDP-basierten Anwendungen.

Überwachen und verbessern Sie die Leistung Ihrer TCP- oder UDP-basierten Anwendungen

Anwendungsentwickler können den Zustand von TCP- oder UDP-basierten Anwendungen über umfangreiche Monitore (wie TCP-ECV, UDP-ECV) in Citrix ADC genau überwachen. Die ECV-Monitore (Extended Content Validation) helfen bei der Überprüfung, ob die Anwendung erwarteten Inhalt zurückgibt oder nicht.

Die Anwendungsleistung kann auch verbessert werden, indem Persistenzmethoden wie Quell-IP verwendet werden. Sie können diese Citrix ADC-Funktionen über Smart Annotations in Kubernetes verwenden. Das Folgende ist ein Beispiel:


```
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
    name: mongodb
    annotations:
        ingress.citrix.com/insecure-port:  “80”
        ingress.citrix.com/frontend-ip:  “192.168.1.1”
        ingress.citrix.com/csvserver:  ‘{
  “l2conn” :” on”  }
 ’
        ingress.citrix.com/lbvserver:  ‘{
  “mongodb-svc” :{
  “lbmethod” :” SRCIPDESTIPHASH”  }
  }
 ’
        ingress.citrix.com/monitor:  ‘{
  “mongodbsvc” :{
  “type” :” tcp-ecv”  }
  }
 ’
Spec:
    rules:
    - host: mongodb.beverages.com
      http:
        paths:
        - path: /
          backend:
            serviceName: mongodb-svc
            servicePort: 80
<!--NeedCopy-->
```

Citrix Application Delivery Management (ADM) -Dienst

Der Citrix ADM-Dienst bietet die folgenden Vorteile:

- **Agilität** — Einfach zu bedienen, zu aktualisieren und zu verwenden. Das Servicemodell des Citrix ADM Service ist über die Cloud verfügbar, sodass die bereitgestellten Funktionen einfach zu bedienen, zu aktualisieren und zu verwenden sind. Die Häufigkeit von Updates in Kombination mit der automatischen Update-Funktion verbessert die Citrix ADC Bereitstellung schnell.
- **Schnellere Wertschöpfung** — Schnellere Erreichung der Geschäftsziele. Im Gegensatz zur herkömmlichen on-premises Bereitstellung können Sie Ihren Citrix ADM-Dienst mit wenigen Klicks verwenden. Sie sparen nicht nur Installations- und Konfigurationszeit, sondern

verschwenden auch Zeit und Ressourcen für potenzielle Fehler.

- **Verwaltung mehrerer Standorte** — Single Pane of Glass für Instanzen in Rechenzentren mit mehreren Standorten. Mit dem Citrix ADM-Dienst können Sie Citrix ADCs verwalten und überwachen, die sich in verschiedenen Bereitstellungstypen befinden. Sie haben One-Stop-Management für Citrix ADCs, die on-premises und in der Cloud bereitgestellt werden.
- **Betriebseffizienz** — Optimierte und automatisierte Methode zur Erzielung höherer Betriebsproduktivität. Mit dem Citrix ADM Service werden Ihre Betriebskosten reduziert, indem Sie Zeit, Geld und Ressourcen bei der Wartung und Aktualisierung der herkömmlichen Hardwarebereitstellungen sparen.

Service-Diagramm für Kubernetes-Anwendungen

Mit dem Service-Diagramm für die Cloud-native Anwendungsfunktion in Citrix ADM können Sie:

- Sicherstellung der Gesamtleistung der Anwendung durch End-to-End-Anwendung
- Identifizieren Sie Engpässe, die durch die gegenseitige Abhängigkeit verschiedener Komponenten Ihrer Anwendungen entstehen
- Sammeln Sie Einblicke in die Abhängigkeiten der verschiedenen Komponenten Ihrer Anwendungen
- Überwachen Sie Dienste innerhalb des Kubernetes-Clusters
- Überwachen Sie, welcher Dienst Probleme hat
- Prüfen Sie die Faktoren, die zu Leistungsproblemen beitragen
- Detaillierte Sichtbarkeit der HTTP-Transaktionen des Dienstes anzeigen
- Analysieren der HTTP-, TCP- und SSL-Metriken

Durch die Visualisierung dieser Metriken in Citrix ADM können Sie die Ursache von Problemen analysieren und die erforderlichen Fehlerbehebungsaktionen schneller durchführen. Service Graph zeigt Ihre Anwendungen in verschiedenen Komponentendiensten an. Diese Dienste, die innerhalb des Kubernetes-Clusters ausgeführt werden, können mit verschiedenen Komponenten innerhalb und außerhalb der Anwendung kommunizieren.

Informationen zu den ersten Schritten finden Sie unter Service Graph einrichten.

Service-Diagramm für dreistufige Webanwendungen

Mit der Service Graph-Funktion aus dem Anwendungs-Dashboard können Sie Folgendes anzeigen:

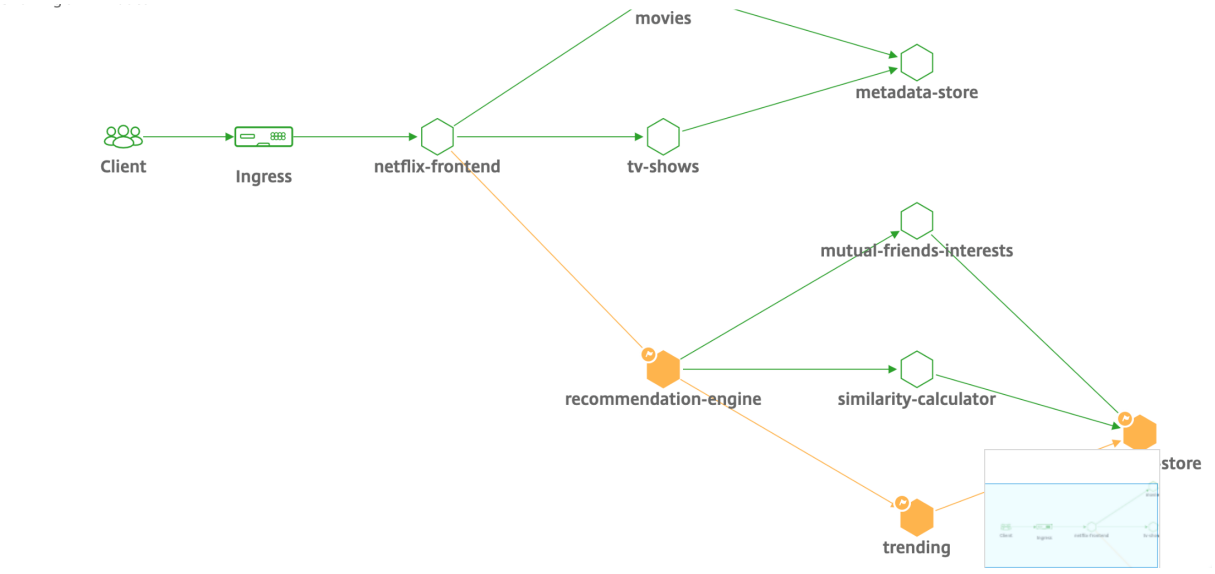
- Details zur Konfiguration der Anwendung (mit dem virtueller Content Switching-Server und dem virtuellen Load Balancing-Server)
  - Für GSLB-Anwendungen können Sie Rechenzentrum, ADC-Instanz, virtuelle CS- und LB-Server anzeigen
- Ende-zu-Ende-Transaktionen vom Kunden zum Service

- Der Ort, von dem aus der Client auf die Anwendung zugreift
- Der Name des Rechenzentrums, in dem die Clientanforderungen verarbeitet werden, und die zugehörigen Citrix ADC-Metriken des Rechenzentrums (nur für GSLB-Anwendungen)
- Metrikdetails für Client, Service und virtuelle Server
- Wenn die Fehler vom Kunden oder vom Dienst stammen
- Der Dienststatus wie " **Kritisch**", " **Überprüfung**" und " **Gut**". Citrix ADM zeigt den Dienststatus basierend auf der Reaktionszeit des Dienstes und der Fehleranzahl an.
  - **Kritisch (rot)** — Zeigt an, wenn die durchschnittliche Reaktionszeit des Service > 200 ms UND Fehlerzähler > 0
  - **Überprüfung (orange)** — Zeigt an, wenn die durchschnittliche Reaktionszeit des Service > 200 ms ODER Fehlerzähler > 0
  - **Gut (grün)** — Zeigt keinen Fehler an und durchschnittliche Reaktionszeit < 200 ms
- Der Kundenstatus wie " **Kritisch**", " **Überprüfung**" und " **Gut**". Citrix ADM zeigt den Clientstatus basierend auf der Latenz des Clientnetzwerks und der Fehleranzahl an.
  - **Kritisch (rot)**— Zeigt an, wenn die durchschnittliche Netzwerklatenz des Clients > 200 ms UND Fehleranzahl > 0
  - **Überprüfung (orange)** — Zeigt an, wenn die durchschnittliche Clientnetzwerklatenz > 200 ms ODER Fehlerzähler > 0
  - **Gut (grün)** — Zeigt keinen Fehler an und durchschnittliche Latenz des Client-Netzwerks < 200 ms
- Der Status des virtuellen Servers wie " **Kritisch**", " **Überprüfung**" und " **Gut**". Citrix ADM zeigt den Status des virtuellen Servers basierend auf dem App-Score an.
  - **Kritisch (rot)** — Zeigt an, wenn der App-Wert < 40 ist
  - **Überprüfung (orange)** — Zeigt an, wenn der App-Score zwischen 40 und 75 liegt
  - **Gut (grün)** — Zeigt an, wenn der App-Score > 75 ist

Zu beachtenswerte Punkte:

- Im Service-Diagramm werden nur Load Balancing, Content Switching und virtuelle GSLB-Server angezeigt.
- Wenn kein virtueller Server an eine benutzerdefinierte Anwendung gebunden ist, sind die Details im Service-Diagramm für die Anwendung nicht sichtbar.
- Sie können Metriken für Clients und Services im Service-Diagramm nur anzeigen, wenn aktive Transaktionen zwischen virtuellen Servern und Webanwendung stattfinden.
- Wenn keine aktiven Transaktionen zwischen virtuellen Servern und der Webanwendung verfügbar sind, können Sie Details im Service-Diagramm nur basierend auf den Konfigurationsdaten wie Load Balancing, Content Switching, virtuelle GSLB-Server und Dienste anzeigen.
- Es kann 10 Minuten dauern, bis Aktualisierungen in der Anwendungskonfiguration im Service-Diagramm angezeigt werden.

Weitere Informationen finden Sie unter Service-Diagramm für Anwendungen.



Informationen zum Einstieg finden Sie in der Service Graph-Dokumentation.

Fehlerbehebung für Citrix ADC-Teams

Lassen Sie uns einige der häufigsten Attribute für die Fehlerbehebung bei der Citrix ADC-Plattform besprechen und wie diese Techniken zur Fehlerbehebung auf die Tier-1-Bereitstellungen für Microservices-Topologien angewendet werden.

Der Citrix ADC verfügt über eine Befehlszeilenschnittstelle (CLI), die Befehle in Echtzeit anzeigt und zum Bestimmen von Laufzeitkonfigurationen, Statik und Richtlinienkonfiguration nützlich ist. Dies wird über den Befehl **“SHOW”** erleichtert.

SHOW - ADC-CLI-Operationen ausführen:

```
>Show running config (-summary -fullValues)

 Ability to search (grep command)
> “sh running config | -i grep vserver”

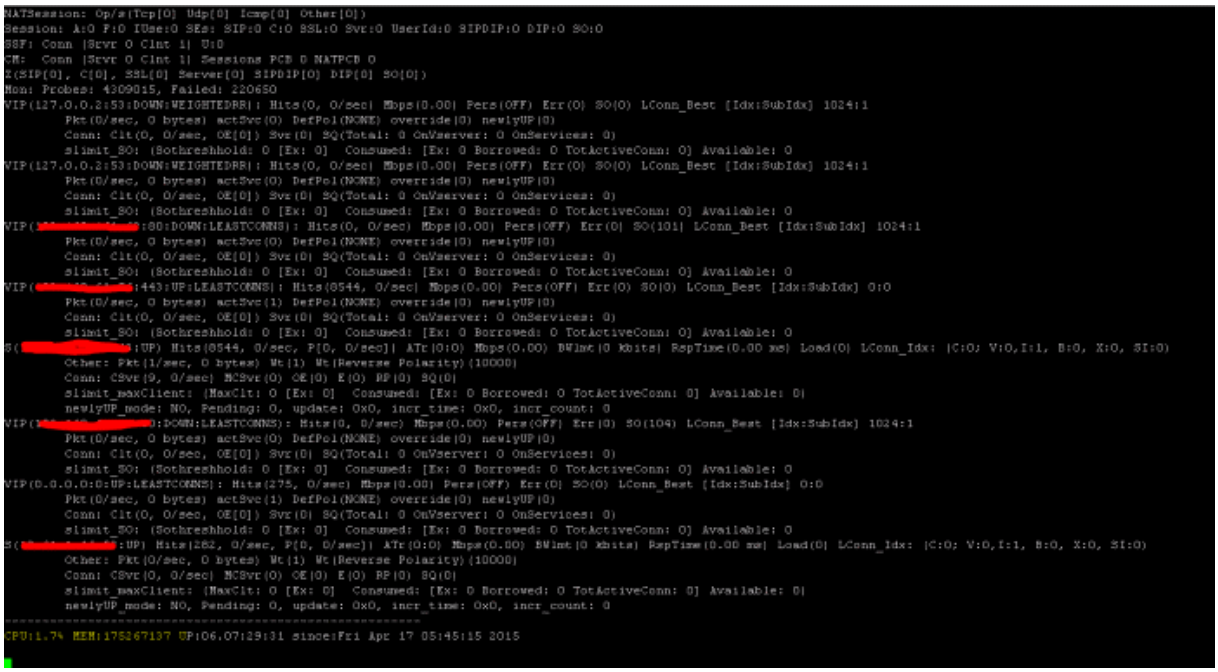
Check the version.
>Show license
   “sh license”
<!--NeedCopy-->
```

SSL Statistiken anzeigen

```
>Sh ssl
```



```
2           System
3           Frontend
4           Backend
5           Encryption
6  <!--NeedCopy-->
```



Der Citrix ADC verfügt über einen Befehl zum Aufzählen von Statistiken für alle Objekte basierend auf einem Zählerintervall von sieben (7) Sekunden. Dies wird über den Befehl **“STAT”** erleichtert.

Hochgranulare L3-L7-Telemetrie von Citrix ADC

- Systemebene: CPU- und Speicherauslastung von ADC.
- HTTP-Protokoll: #Requests /Responses, GET/POST Split, HTTP-Fehler für N-S und E-W (nur für Service Mesh Lite, Sidecar bald).
- SSL: #Sessions und #Handshakes nur für N-S- und E-W-Verkehr für Service Mesh Lite.
- IP-Protokoll: #Packets empfangen/gesendet, #Bytes empfangen/gesendet, #Truncated -Pakete und #IP Adresssuche.
- Citrix ADC AAA: #Active -Sitzungen
- Schnittstelle: #Total Multicast-Pakete, #Total übertragene Bytes und #Jumbo -Pakete empfangen/gesendet.
- Virtueller Lastenausgleichsserver und virtueller Content Switching-Server: #Packets, #Hits und #Bytes empfangen/gesendet.

STAT - ADC-CLI-Operationen ausführen:


```
>Statistics
 “stat ssl”
<!--NeedCopy-->
```

```
> stat ns

System overview

Up since        Thu Apr 16 19:45:15 2015
Packet CPU usage (%)                1.60
Management CPU usage (%)            0.80
Memory usage (MB)                    165
InUse Memory (%)                   17.03
Last Transition time Th...015
System state                          UP
Master state                     Primary
# SSL cards UP                         0
# SSL cards present                    0

System Disks                   Used (%) Available
/flash Used (%)                       17      1168
/var Used (%)                         13     11246

Throughput Statistics                    Rate (/s)               Total
Megabits received                               2               288237
Megabits transmitted                            3               345685

TCP Connections                  Client   Server
All client connections              158      272
Established client connections      158      145

HTTP                                     Rate (/s)               Total
Total requests                                  0               191529
Total responses                                 0               263011
Request bytes received                       7007           1178810535
Response bytes received                    164477          12348432171

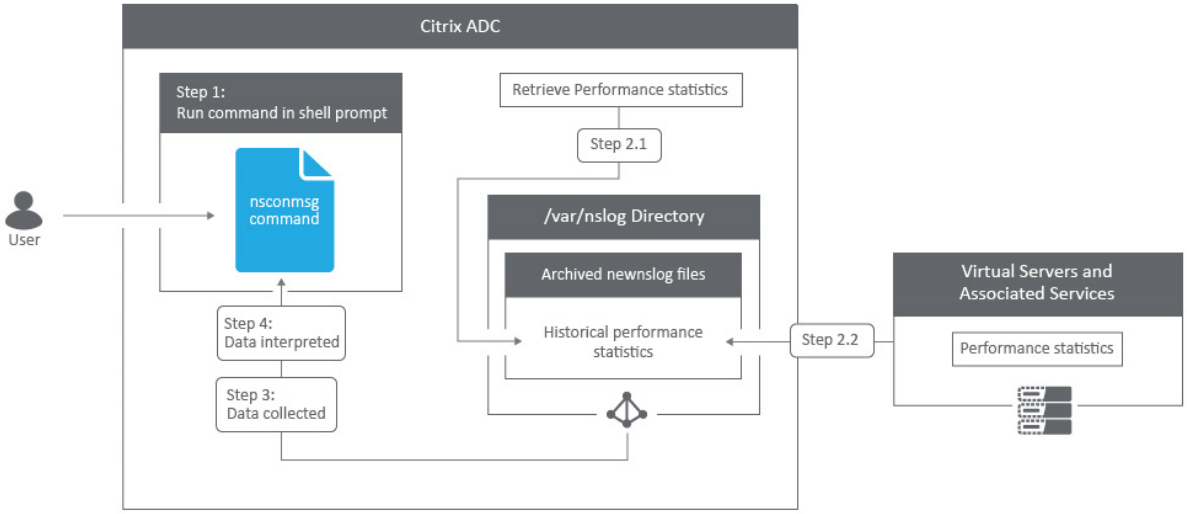
SSL                                      Rate (/s)               Total
```

Der Citrix ADC verfügt über eine Protokollarchivstruktur, die das Durchsuchen von Statistiken und Leistungsindikatoren bei der Behandlung bestimmter Fehler über den Befehl **“NSCONMSG”** ermöglicht.

NSCONMSG - Haupt-Protokolldatei (NS-Datenformat)

```
    Cd /var/nslog

     “Mac Moves”
    nsconmsg -d current -g nic_err
<!--NeedCopy-->
```

Nstcpdump

Sie können `nstcpdump` für die Fehlerbehebung auf niedriger Ebene verwenden. `nstcpdump` sammelt weniger detaillierte Informationen als `nstrace`. Öffnen Sie die ADC-CLI und geben Sie ein `shell`. Sie können Filter mit verwenden `nstcpdump`, aber keine für ADC-Ressourcen spezifischen Filter verwenden. Die Dump-Ausgabe kann direkt im CLI-Bildschirm angezeigt werden.

CTRL + C — Drücken Sie diese Tasten gleichzeitig, um eine zu stoppen `nstcpdump`.

`nstcpdump.sh dst host x.x.x.x` — Zeigt den an den Zielhost gesendeten Datenverkehr an.

`nstcpdump.sh -n src host x.x.x.x` — Zeigt den Datenverkehr vom angegebenen Host an und wandelt keine IP-Adressen in Namen um (-n).

`nstcpdump.sh host x.x.x.x` — Zeigt den Datenverkehr zu und von der angegebenen Host-IP an.

![Beispiel`nstcpdump`](/en-us/citrix-adc/media/nstcpdump.png)

NSTRACE - Paket-Trace-Datei

NSTRACE ist ein Paket-Debugging-Tool auf niedriger Ebene zur Fehlerbehebung bei Netzwerken. Es ermöglicht Ihnen, Capture-Dateien zu speichern, die Sie mit den Analysewerkzeugen weiter analysieren können. Zwei gängige Tools sind Network Analyzer und Wireshark.

![Ausgabe von `nstrace`](/en-us/citrix-adc/media/nstrace.png)

```
> start nstrace -size 0
 Done
> stop nstrace
 Done
```

Sobald die NSTRACE-Capture-Datei in /var/nstrace auf dem ADC erstellt wurde, können Sie die Capture-Datei zur Paketerfassung und Netzwerkanalyse in Wireshark importieren.

SYSCTL - Ausführliche ADC-Informationen: Beschreibung, Modell, Plattform, CPUs usw

```
    sysctl -a grep hw.physmem

    hw.physmem: 862306304
    netscaler.hw_physmem_mb: 822
<!--NeedCopy-->
```

aaad.debug - Open Pipe für Debug-Informationen zur Authentifizierung

```
process_radius Got RADIUS event
process_radius Received BAD_ACCESS_REJECT for: <username>
process_radius Sending reject.
send_reject_with_code Rejecting with error code 4001.
```

Weitere Informationen zur Behebung von Authentifizierungsproblemen über ADC oder ADC Gateway mit dem Modul aaad.debug finden Sie im aaad.debug-Supportartikel.

Es besteht auch die Möglichkeit, Leistungsstatistiken und Ereignisprotokolle direkt für den ADC abzurufen. Weitere Informationen dazu finden Sie im ADC-Supportdokument.

Fehlerbehebung für SRE und Plattformteams

Kubernetes-Verkehrsströme

Norden/Süden:

- Nord/Süd-Verkehr ist der Datenverkehr, der vom Benutzer über den Ingress in den Cluster fließt.

Ost/West:

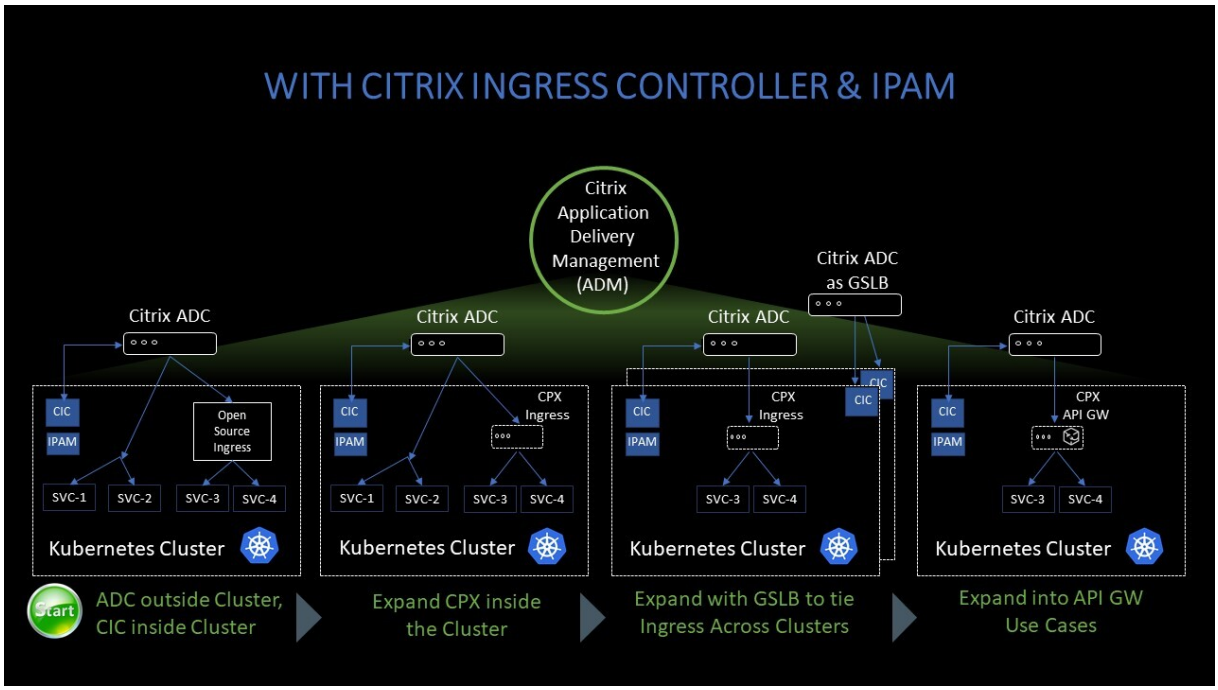
- Der Ost/West-Verkehr ist der Verkehr, der um den Kubernetes-Cluster fließt: Service-to-Service oder Service-zu-Datenspeicher.

Wie Citrix ADC CPX-Last den Ost-West-Verkehrsfluss in einer Kubernetes-Umgebung ausgleicht

Nachdem Sie den Kubernetes-Cluster bereitgestellt haben, müssen Sie den Cluster in ADM integrieren, indem Sie die Details der Kubernetes-Umgebung in ADM angeben. ADM überwacht die Änderungen der Kubernetes-Ressourcen wie Dienste, Endpunkte und Ingress-Regeln.

Wenn Sie eine ADC CPX-Instanz im Kubernetes-Cluster bereitstellen, registriert sie sich automatisch bei ADM. Im Rahmen des Registrierungsprozesses erfährt ADM mehr über die IP-Adresse der CPX-Instanz und den Port, über den es die Instanz erreichen kann, um sie mithilfe von NITRO REST-APIs zu konfigurieren.

Die folgende Abbildung zeigt, wie die ADC CPX-Last den Ost-West-Verkehrsfluss in einem Kubernetes-Cluster ausgleicht.



In diesem Beispiel wird

Knoten 1 und Knoten 2 der Kubernetes-Cluster enthalten Instanzen eines Front-End-Dienstes und eines Back-End-Dienstes. Wenn die ADC CPX-Instanzen in Knoten 1 und Knoten 2 bereitgestellt werden, werden die ADC CPX-Instanzen automatisch bei ADM registriert. Sie müssen den Kubernetes-Cluster manuell in ADM integrieren, indem Sie die Kubernetes-Clusterdetails in ADM konfigurieren.

Wenn ein Client den Front-End-Dienst anfordert, gleicht die eingehende Ressourcenlast die Anforderung zwischen den Instanzen des Front-End-Dienstes auf den beiden Knoten aus. Wenn eine Instanz des Front-End-Dienstes Informationen von den Back-End-Diensten im Cluster benötigt, leitet sie die Anforderungen an die ADC CPX-Instanz in ihrem Knoten weiter. Diese ADC CPX-Instanz gleicht die Anforderungen zwischen den Back-End-Diensten im Cluster aus und sorgt für einen Ost-West-Verkehrsfluss.

ADM Service Graph für Anwendungen

Mit der Service Graph-Funktion in Citrix ADM können Sie alle Dienste in einer grafischen Darstellung überwachen. Diese Funktion bietet auch eine detaillierte Analyse und nützliche Metriken. Sie können Service-Diagramme anzeigen für:

- Für alle Citrix ADC-Instanzen konfigurierte Anwendungen
- Kubernetes-Anwendungen
- 3-stufige Webanwendungen

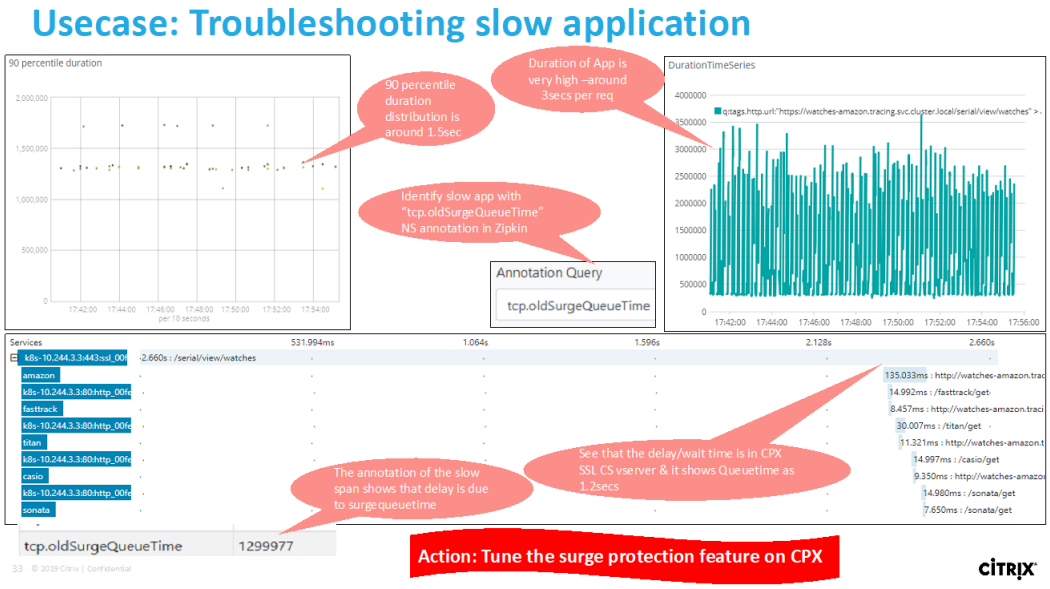
Um loszulegen, sehen Sie sich die Details im Service Graphan.

Zähler für Microservice-Anwendungen anzeigen

Das Service-Diagramm zeigt auch alle Microservice-Anwendungen an, die zu den Kubernetes-Clustern gehören. Der Mauszeiger auf einem Service, um die Metrik-Details anzuzeigen.

Sie können Folgendes anzeigen:

- Der Dienstname
- Das vom Dienst verwendete Protokoll wie SSL, HTTP, TCP, SSL über HTTP
- **Treffer** — Die Gesamtzahl der vom Dienst erhaltenen Treffer
- **Reaktionszeit des Service** — Die durchschnittliche Reaktionszeit, die vom Service in Anspruch genommen wurde.
  (Reaktionszeit = Client-RTT+ letztes Byte anfordern - erstes Byte anfordern)
- **Errors** — Die Gesamtzahl der Fehler wie 4xx, 5xx usw.
- **Datenvolumen** — Das Gesamtvolumen der vom Dienst verarbeiteten Daten
- **Namespace** — Der Namensraum des Service
- **Clustername** — Der Clustername, in dem der Dienst gehostet wird
- **SSL-Serverfehler** — Die gesamten SSL-Fehler vom Dienst



Diese spezifischen Leistungsindikatoren und Transaktionsprotokolle können mithilfe einer Reihe unterstützter Endpunkte über den Citrix Observability Exporter (COE) extrahiert werden. Weitere Informationen zu COE finden Sie in den folgenden Abschnitten.

Exporteur für Citrix ADC-Statistiken

Dies ist ein einfacher Server, der Citrix ADC-Statistiken kratzt und sie über HTTP nach Prometheus exportiert. Prometheus kann dann als Datenquelle zu Grafana hinzugefügt werden, um die Citrix ADC-Statistiken grafisch anzuzeigen.

Um die Statistiken und Zähler von Citrix ADC-Instanzen zu überwachen, `citrix-adc-metric-exporter` kann als Container oder Skript ausgeführt werden. Das Exportprogramm sammelt Citrix ADC-Statistiken wie die Gesamtzahl der Treffer auf einen virtuellen Server, die HTTP-Anforderungsrate, die SSL-Verschlüsselungs-Entschlüsselungsrate usw. von den Citrix ADC-Instanzen und hält sie so lange, bis der Prometheus-Server die Statistiken abruft und sie mit einem Zeitstempel speichert. Grafana kann dann auf den Prometheus-Server verwiesen werden, um die Statistiken abzurufen, sie zu zeichnen, Alarme einzustellen, Heatmaps zu erstellen, Tabellen zu generieren usw. nach Bedarf, um die Citrix ADC-Statistiken zu analysieren.

Einzelheiten zum Einrichten des Exportprogramms für die Arbeit in einer Umgebung, wie in der Abbildung dargestellt, finden Sie in den folgenden Abschnitten. Ein Hinweis, auf welchen Citrix ADC-Entitäten/Metriken der Exporteur standardmäßig kratzt und wie er geändert werden kann, wird ebenfalls erläutert.

Weitere Informationen zu Exporter for Citrix ADC finden Sie im Metrics Exporter GitHub.

ADM-Dienst verteilte Ablaufverfolgung

Im Service-Diagramm können Sie die Ansicht für die verteilte Ablaufverfolgung verwenden, um:

- Analysieren Sie die gesamte Leistung des Dienstes.
- Visualisieren Sie den Kommunikationsfluss zwischen dem ausgewählten Dienst und seinen voneinander abhängigen Diensten.
- Identifizieren Sie, welcher Dienst auf Fehler hinweist, und beheben Sie den fehlerhaften Dienst
- Zeigen Sie Transaktionsdetails zwischen dem ausgewählten Dienst und jedem voneinander abhängigen Dienst an.

Voraussetzungen für die verteilte ADM-Ablaufverfolgung

Um die Trace-Informationen für den Dienst anzuzeigen, müssen Sie:

- Stellen Sie sicher, dass eine Anwendung die folgenden Trace-Header verwaltet, während sie Ost-West-Verkehr sendet:

- x-request-id
- x-b3-traceid
- x-b3-spanid
- x-b3-parentspanid
- x-b3-sampled
- x-b3-flags
- x-ot-span-context

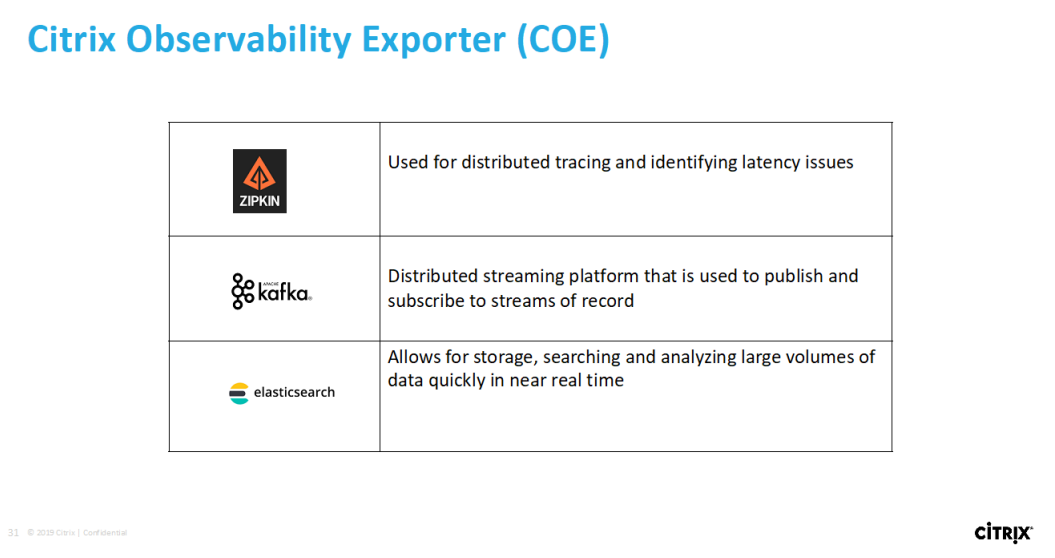
  - Aktualisieren Sie die CPX-YAML-Datei mit NS_DISTRIBUTED_TRACING und den Wert auf YES. Informationen zu den ersten Schritten finden Sie unter Verteilte Ablaufverfolgung.

Parsen des Citrix ADC Observability Exporter (COE)

Citrix Observability Exporter ist ein Container, der Metriken und Transaktionen von Citrix ADCs sammelt und sie für unterstützte Endpunkte in geeignete Formate (wie JSON, AVRO) umwandelt. Sie können die vom Citrix Observability Exporter gesammelten Daten zum gewünschten Endpunkt exportieren. Durch die Analyse der an den Endpunkt exportierten Daten erhalten Sie wertvolle Erkenntnisse auf Microservices-Ebene für Anwendungen, die von Citrix ADCs bereitgestellt werden.

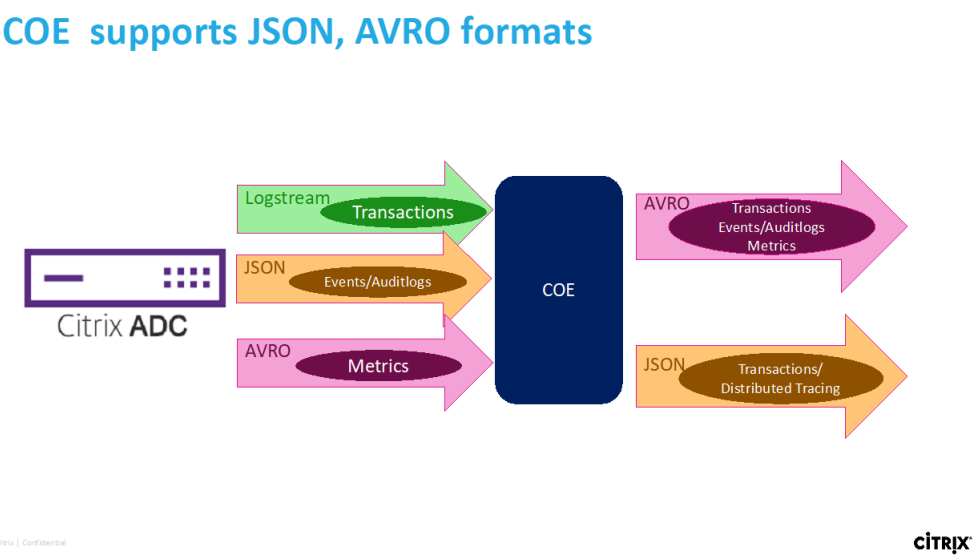
Weitere Informationen zu COE finden Sie im COE GitHub.

COE mit Elasticsearch als Transaktionsendpunkt



Wenn Elasticsearch als Transaktionsendpunkt angegeben ist, wandelt Citrix Observability Exporter die Daten in das JSON-Format um. Auf dem Elasticsearch-Server erstellt Citrix Observability Exporter

stündlich Elasticsearch-Indizes für jeden ADC. Diese Indizes basieren auf Daten, Stunde, UUID des ADC und dem Typ der HTTP-Daten (http_event oder http_error). Anschließend lädt der Citrix Observability Exporter die Daten im JSON-Format unter Elastic-Suchindizes für jeden ADC hoch. Alle regulären Transaktionen werden in den http_event-Index aufgenommen und alle Anomalien werden in den http_error-Index aufgenommen.



Unterstützung für verteilte Ablaufverfolgung mit Zipkin

In einer Microservice-Architektur kann sich eine einzelne Endbenutzeranfrage über mehrere Microservices erstrecken, was die Verfolgung einer Transaktion und das Beheben von Fehlerquellen schwierig macht. In solchen Fällen können herkömmliche Methoden der Leistungsüberwachung nicht genau bestimmen, wo Fehler auftreten und was der Grund für eine schlechte Leistung ist. Sie müssen Datenpunkte erfassen, die für jeden Microservice spezifisch sind, der eine Anfrage bearbeitet, und diese analysieren, um aussagekräftige Erkenntnisse zu erhalten.

Das verteilte Tracing begegnet dieser Herausforderung, indem es eine Möglichkeit bietet, eine Transaktion durchgängig zu verfolgen und zu verstehen, wie sie über mehrere Microservices hinweg gehandhabt wird.

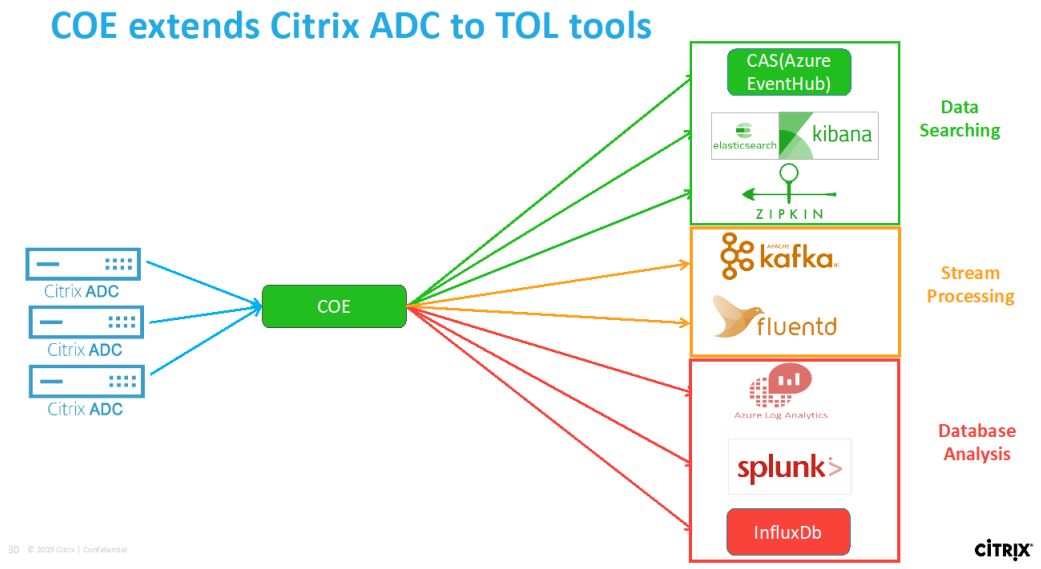
OpenTracing ist eine Spezifikation und ein Standardsatz von APIs zum Entwerfen und Implementieren von verteiltem Tracing. Verteilte Tracer ermöglichen es Ihnen, den Datenfluss zwischen Ihren Microservices zu visualisieren und helfen, Engpässe in Ihrer Microservices-Architektur zu identifizieren.

Citrix ADC Observability Exporter implementiert die verteilte Ablaufverfolgung für Citrix ADC und unterstützt derzeit Zipkin als verteilten Tracer.

Derzeit können Sie die Leistung auf Anwendungsebene mit Citrix ADC überwachen. Mit Citrix Observability Exporter mit Citrix ADC können Sie Protokollierungsdaten für Microservices jeder Anwendung

abrufen, die von Ihrem Citrix ADC CPX, MPX oder VPX bereitgestellt werden.

Um loszulegen, lesen Sie den GitHub Observability Exporter.

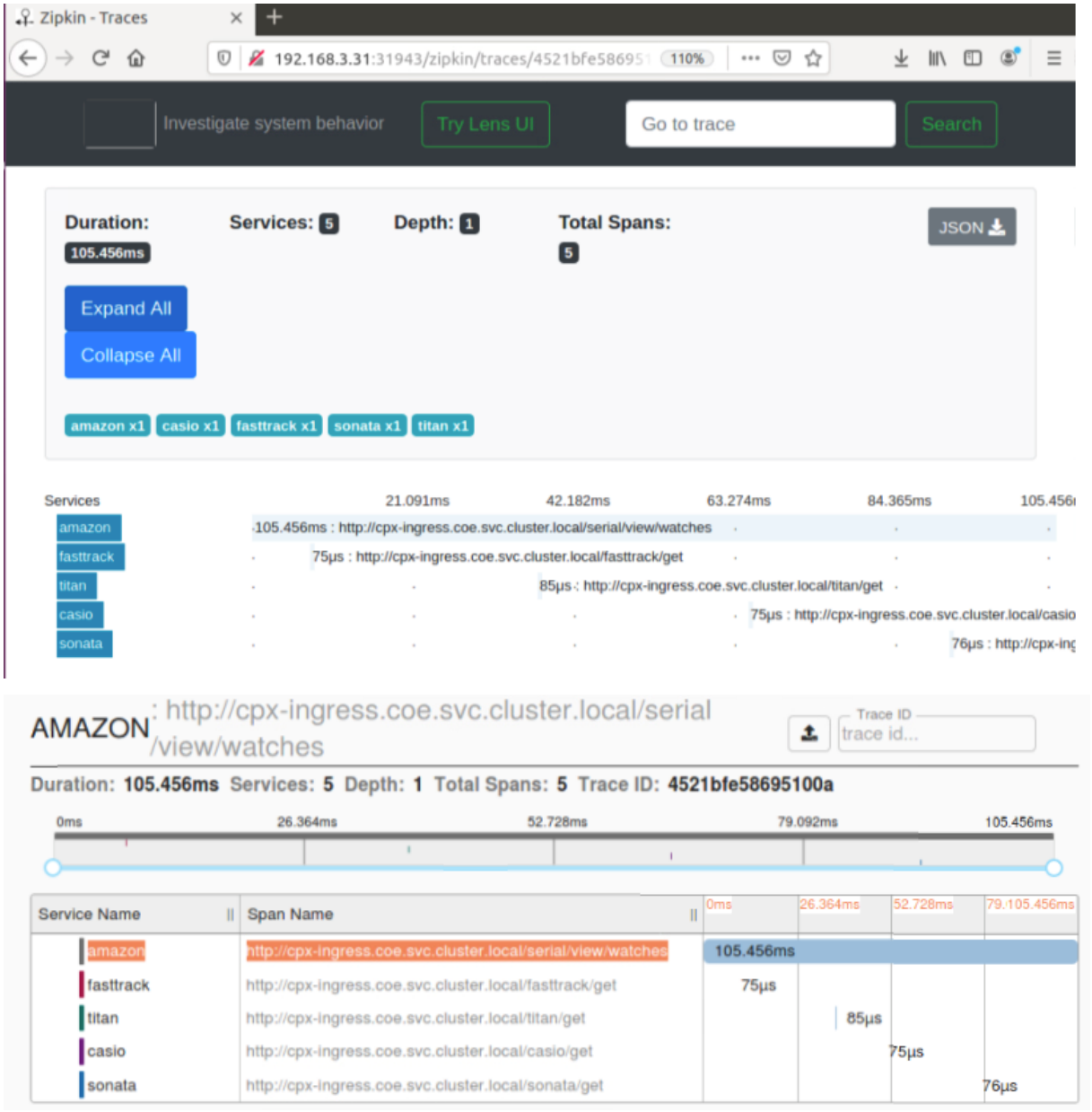


Zipkin für das Debugging von Anwendungen

Zipkin ist ein verteiltes Open Source-Verfolgungssystem, das auf Dappers Papier von Googlebasiert. Dapper ist Googles System für die systemverteilte Rückverfolgung in der Produktion. Google erklärt dies in seinem Artikel: “Wir haben Dapper entwickelt, um den Entwicklern von Google mehr Informationen über das Verhalten komplexer verteilter Systeme zu liefern”. Die Beobachtung des Systems aus verschiedenen Blickwinkeln ist bei der Fehlersuche von entscheidender Bedeutung, insbesondere wenn ein System komplex und verteilt ist.

Die folgenden Zipkin-Verfolgungsdaten identifizieren insgesamt 5 Bereiche und 5 Dienste im Zusammenhang mit der Watches-Beispielanwendung. Die Trace-Daten zeigen die spezifischen Span-Daten über die 5 Microservices hinweg.

Um loszulegen, siehe Zipkin.



Beispiel für einen Zipkin-Zeitraum, der die Anwendungslatenz für die erste Anforderung zum Laden

Services: amazon

Date Time	Relative Time	Annotation	Address
7/15/2020, 2:14:24 PM		Server Start	10.10.235.179:1719 (amazon)
7/15/2020, 2:14:24 PM	105.456ms	Server Finish	10.10.235.179:1719 (amazon)

Key	Value
component	py_zipkin
http.host	amazon:1719
http.method	GET
http.path	/serial/view/watches
http.url	http://cpx-ingress.coe.svc.cluster.local/serial/view/watches
Local Component	amazon
peer.address	10.10.235.190

Kibana zum Anzeigen von Daten

Kibana ist eine offene Benutzeroberfläche, mit der Sie Ihre Elasticsearch-Daten visualisieren und im Elastic Stack navigieren können. Erledigen Sie alles, von der Verfolgung der Abfrageladung bis hin zum Verständnis des Ablaufs von Anfragen

Egal, ob Sie Analyst oder Administrator sind, Kibana macht Ihre Daten umsetzbar, indem es die folgenden drei Schlüsselfunktionen bereitstellt:

- **Eine Open Source Analyse- und Visualisierungsplattform.** Erkunden Sie mit Kibana Ihre Elasticsearch-Daten und erstellen Sie anschließend wunderschöne Visualisierungen und Dashboards.
- **Eine Benutzeroberfläche für die Verwaltung des Elastic Stack.** Verwalten Sie Ihre Sicherheitseinstellungen, weisen Sie Benutzerrollen zu, erstellen Sie Snapshots, rollen Sie Ihre Daten

zusammen und vieles mehr — alles bequem über eine Kibana-Benutzeroberfläche.

- **Ein zentraler Knotenpunkt für die Lösungen von Elastic.** Von der Protokollanalyse über die Dokumentenerkennung bis hin zum SIEM ist Kibana das Portal für den Zugriff auf diese und andere Funktionen.

Kibana wurde entwickelt, um Elasticsearch als Datenquelle zu verwenden. Stellen Sie sich Elasticsearch als die Engine vor, die die Daten speichert und verarbeitet, wobei Kibana an der Spitze sitzt.

Auf der Homepage bietet Kibana die folgenden Optionen zum Hinzufügen von Daten:

- Importieren Sie Daten mit dem Dateidaten-Visualizer.
- Richten Sie mithilfe unserer integrierten Tutorials einen Datenfluss zu Elasticsearch ein. Wenn es für deine Daten kein Tutorial gibt, gehe zur Beats Übersicht, um mehr über andere Datenversender in der Beats-Familie zu erfahren.
- Fügen Sie einen Beispieldatensatz hinzu und testen Sie Kibana, ohne selbst Daten zu laden.
- Indizieren Sie Ihre Daten mit REST-APIs oder Clientbibliothekenin Elasticsearch.

Kibana verwendet ein Indexmuster, um anzugeben, welche Elasticsearch-Indizes untersucht werden sollen. Wenn Sie eine Datei hochladen, ein integriertes Tutorial ausführen oder Beispieldaten hinzufügen, erhalten Sie ein kostenloses Indexmuster und können mit der Erkundung beginnen. Wenn Sie Ihre eigenen Daten laden, können Sie in Stack Managementein Indexmuster erstellen.

Schritt 1: Index-Pattern für Logstash konfigurieren

Schritt 2: Wählen Sie den Index aus und generieren Sie den zu füllenden Datenverkehr.

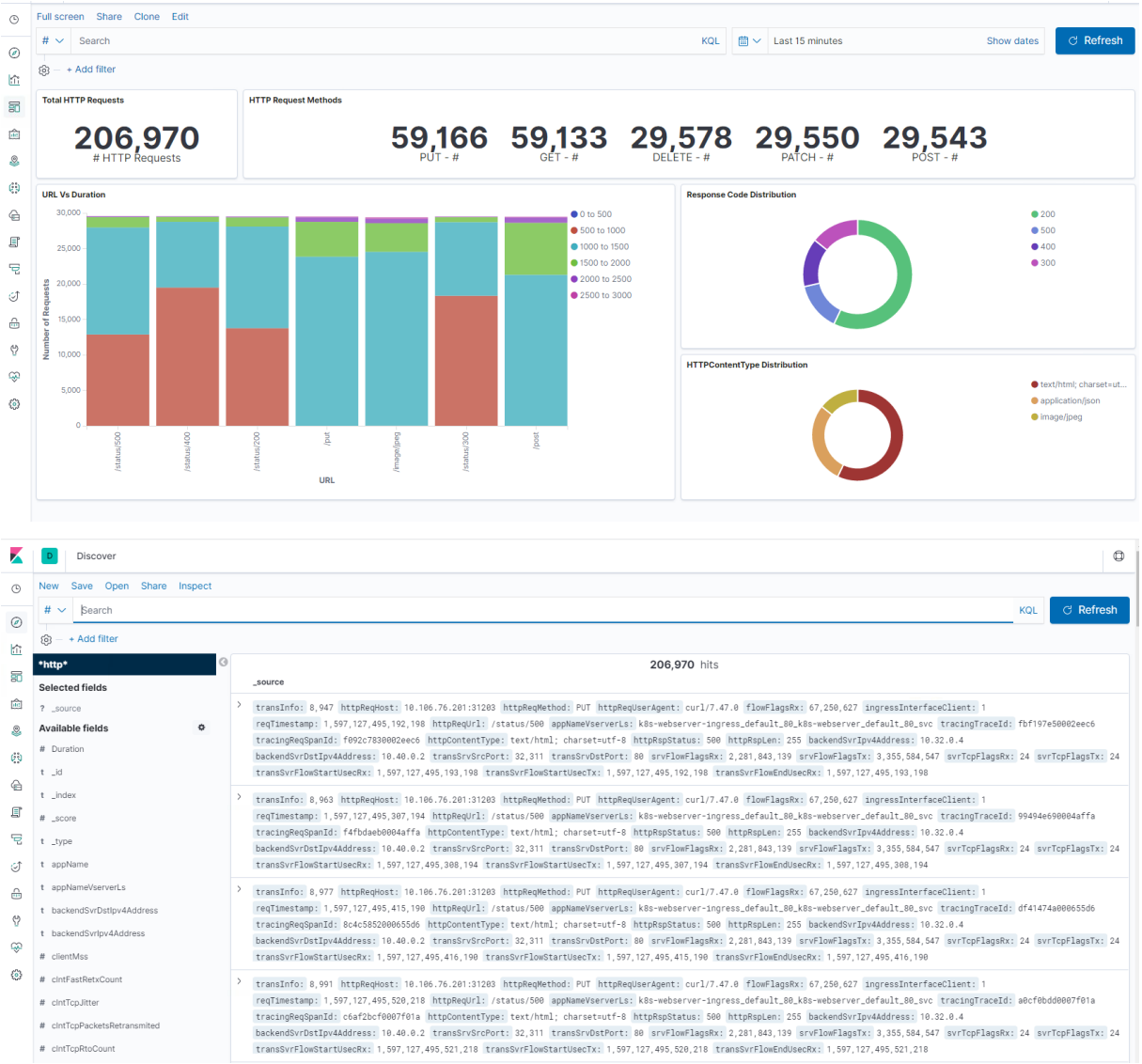
Schritt 3: Generieren Sie eine Anwendung aus den unstrukturierten Daten aus Protokoll-Feeds.

Schritt 4: Kibana formatiert die Logstash-Eingabe, um Berichte und Dashboards zu erstellen.

- Zeit-Bereich
- Tabellarische Ansicht
- Trefferzahlen basierend auf der Anwendung.
  - Zeit-IP, Agent, Maschine.OS, Antwortcode (200), URL
  - Filtern nach Werten

Schritt 5: Visualisieren Sie die Daten in einem Aggregationsbericht.

- Ergebnisaggregation in einem Diagrammbericht (Torte, Grafik usw.)



Bereitstellen einer Citrix ADC VPX- Instanz

October 5, 2021

> **Hinweis:**
>
> Citrix ADM Service Connect ist standardmäßig aktiviert, nachdem Sie Citrix ADC oder Citrix Gateway installiert oder aktualisiert haben, um 13.0 Build 61.xx und höher freizugeben. Weitere Informationen finden Sie unter Data Governance und Citrix ADM Service verbinden.

Das Citrix ADC VPX Produkt ist eine virtuelle Appliance, die auf einer Vielzahl von Virtualisierungs- und Cloud-Plattformen gehostet werden kann:

- Citrix Hypervisor
- VMware ESX
- Microsoft Hyper-V
- Linux KVM
- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

Weitere Informationen finden Sie im Datenblatt zu Citrix ADC VPX.

Weitere Informationen zum Provisionieren einer Citrix ADC VPX-Instanz auf einer SDX-Appliance finden Sie unter Provisioning von Citrix ADC-Instanzen.

Citrix Application Delivery Management für Citrix ADC VPX

Die Citrix Application Delivery Management-Software ist eine zentralisierte Verwaltungslösung, die den Betrieb vereinfacht, indem Administratoren unternehmensweite Sichtbarkeit bietet und Verwaltungsaufträge automatisiert, die über mehrere Instanzen hinweg ausgeführt werden müssen.

Sie können Citrix ADC VPX-Instanzen zusätzlich zu anderen Citrix Anwendungsnetzwerkprodukten wie Citrix Gateway, Citrix ADC SDX, Citrix ADC CPX und Citrix SD-WAN verwalten und überwachen. Mit der Application Delivery Management-Software können Sie die gesamte globale Anwendungsbereitstellungsinfrastruktur über eine einzige einheitliche Konsole verwalten, überwachen und beheben.

Weitere Informationen finden Sie in der Dokumentation zu Citrix Application Delivery Management.

Support-Matrix und Nutzungsrichtlinien

October 4, 2022

In diesem Dokument werden die verschiedenen Hypervisoren und Funktionen aufgeführt, die auf einer Citrix ADC VPX-Instanz unterstützt werden. Das Dokument beschreibt auch ihre Nutzungsrichtlinien und bekannte Einschränkungen.

Tabelle 1. VPX-Instanz auf Citrix Hypervisor

Citrix Hypervisor Version	SysID	VPX Modelle
8.2 unterstützt ab 13.0 64.x, 8.0, 7.6, 7.1	450000	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G

Tabelle 2. VPX-Instanz auf dem VMware ESXi-Hypervisor

ESXi-Version	ESXi-Veröffentlichungsdatum im Format MM/DD/YYYY	ESXi-Build-Nummer	Citrix ADC VPX Version	SysID	VPX Modelle
ESXi 7.0-Update 3f	07/12/2022	20036589	Ab 13.0-86.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 7.0-Update 3d	03/29/2022	19482537	Ab 13.0-86.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

ESXi-Version	ESXi-Veröffentlichungsdatum im Format MM/DD/YYYY	ESXi-Build-Nummer	Citrix ADC VPX Version	SysID	VPX Modelle
ESXi 7.0 3c aktualisieren	01/27/2022	19193900	ab 13.0-85.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 7.0 aktualisiert 2d	09/14/2021	18538813	ab 13,0-83.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 7.0 Update 2a	12/17/2020	17867351	Ab 13.0-82.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

ESXi-Version	ESXi-Veröffentlichungsdatum im Format MM/DD/YYYY	ESXi-Build-Nummer	Citrix ADC VPX Version	SysID	VPX Modelle
ESXi 7.0 aktualisieren 1d	12/17/2020	17551050	Ab 13.0-82.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 7.0 Update 1c	12/17/2020	17325551	Ab 13.0-82.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 7.0 update 1b	10/06/2020	16850804	Ab 13.0-76.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

ESXi-Version	ESXi-Veröffentlichungsdatum im Format MM/DD/YYYY	ESXi-Build-Nummer	Citrix ADC VPX Version	SysID	VPX Modelle
ESXi 7.0b	06/23/2020	16324942	Ab 13.0-71.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 7.0 GA	04/02/2020	15843807	Ab 13.0-71.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.7 P04	11/19/2020	17167734	Ab 13.0-67.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

ESXi-Version	ESXi-Veröffentlichungsdatum im Format MM/DD/YYYY	ESXi-Build-Nummer	Citrix ADC VPX Version	SysID	VPX Modelle
ESXi 6.7 P03	08/20/2020	16713306	Ab 13.0-67.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.7 P02	04/28/2020	16075168	Ab 13.0-67.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.7 P01	12/05/2019	15160138	Ab 13.0-67.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

ESXi-Version	ESXi-Veröffentlichungsdatum im Format MM/DD/YYYY	ESXi-Build-Nummer	Citrix ADC VPX Version	SysID	VPX Modelle
ESXi 6.7 Update 3	08/20/2019	14320388	Ab 13.0-58.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.7 U2	04/11/2019	13006603	Ab 13.0-47.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.5 GA	11/15/2016	4564106	Ab 13.0-47.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

ESXi-Version	ESXi-Veröffentlichungsdatum im Format MM/DD/YYYY	ESXi-Build-Nummer	Citrix ADC VPX Version	SysID	VPX Modelle
ESXi 6.5 U1g	3/20/2018	7967591	Ab 13.0 47.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.0 Update 3	2/24/2017	5050593	Ab 12.0-51.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G
ESXi 6.0 Express Patch 11	10/5/2017	6765062	Ab 12.0-56.x	450010	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10G, VPX 15G, VPX 25G, VPX 40G, VPX 100G

Tabelle 3. VPX auf Microsoft Hyper-V

Hyper-V-Version	SysID	VPX Modelle
2012, 2012 R2, 2016, 2019	450020	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000

Tabelle 4. VPX-Instanz auf generischem KVM

Generische KVM-Version	SysID	VPX Modelle
RHEL 7.4, RHEL 7.5 (ab Citrix ADC Version 12.1 50.x), RHEL 7.6, RHEL 8.2, Ubuntu 16.04, Ubuntu 18.04, RHV 4.2	450070	VPX 10, VPX 25, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX 8000, VPX 10 G, VPX 15 G. VPX 25G, VPX 40G, VPX 100G

Zu beachtende Punkte:

Berücksichtigen Sie bei der Verwendung von KVM-Hypervisoren die folgenden Punkte.

- Die VPX-Instanz ist für Hypervisor Releaseversionen in Tabelle 1—4 und nicht für Patch-Releases innerhalb einer Version qualifiziert. Es wird jedoch erwartet, dass die VPX-Instanz nahtlos mit Patch-Versionen einer unterstützten Version funktioniert. Wenn dies nicht der Fall ist, öffnen Sie einen Supportfall für die Fehlerbehebung und das Debuggen.
- Verwenden Sie die Befehle `ip link`, um RHEL 8.2-Netzwerkbrücken zu konfigurieren.
- Bevor Sie RHEL 7.6 verwenden, führen Sie die folgenden Schritte auf dem KVM-Host aus:
  1. Bearbeiten Sie /etc/default/grub und hängen Sie `"kvm_intel.preemption_timer=0"` an die Variable `GRUB_CMDLINE_LINUX` an.
  2. Generieren Sie grub.cfg mit dem Befehl `"## grub2-mkconfig -o /boot/grub2/grub.cfg"` neu.
  3. Starten Sie den Hostcomputer neu.
- Bevor Sie Ubuntu 18.04 verwenden, führen Sie die folgenden Schritte auf dem KVM-Host aus:
  1. Bearbeiten Sie /etc/default/grub und hängen Sie `"kvm_intel.preemption_timer=0"` an die Variable `GRUB_CMDLINE_LINUX` an.
  2. Generieren Sie grub.cfg mit dem Befehl `"## grub-mkconfig -o /boot/grub/grub.cfg "` neu.
  3. Starten Sie den Hostcomputer neu.

Tabelle 5. VPX-Instanz auf AWS

AWS-Version	SysID	VPX Modelle
Nicht zutreffend	450040	VPX 10, VPX 200, VPX 1000, VPX 3000, VPX 5000, VPX BYOL, VPX 8000, VPX 10G, VPX 15G und VPX 25G sind nur mit BYOL mit EC2-Instanztypen (C5, M5 und C5n) verfügbar

> Hinweis:
> Das VPX 25G-Angebot bietet nicht den gewünschten 25G-Durchsatz in AWS, kann jedoch eine höhere SSL-Transaktionsrate im Vergleich zum VPX 15G-Angebot bieten.

Tabelle 6. VPX-Instanz auf Azure

Azure-Version	SysID	VPX Modelle
Nicht zutreffend	450020	VPX 10, VPX 200, VPX 1000, VPX 3000, VPX BYOL

Tabelle 7. VPX-Feature-Matrix

	VPX on XenServer		VPX on VMware ESX				VPX on Microsoft Hyper-V	VPX on generic KVM			VPX on AWS	VPX on Azure	VPX on GCP
Features	**PV**	**SR-IOV**	**PV**	**SR-IOV**	**Emulated**	**PCI Passthrough**	**PV**	**PV**	**SR-IOV**	**PCI Passthrough**			
Multi-PE Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Clustering Support	Yes	Yes[1]	Yes	Yes[1]	Yes	Yes	Yes	Yes	Yes[1]	Yes	No	No	No
VLAN Tagging	Yes	Yes	Yes	Yes	Yes	Yes	Yes (only on 2012R2)	Yes	Yes	Yes	No	No	No
Detecting Link Events	No[2]	Yes[3]	No[2]	Yes[3]	No[2]	Yes[3]	No[2]	No[2]	Yes[3]	Yes[3]	No[2]	No[2]	No[2]
Interface Parameter Configuration	No	No	No	No	No	Yes	No	No	No	Yes	No	No	No
Static LA	Yes[2]	Yes[3]	Yes[2]	No	Yes[2]	Yes[3]	Yes[2]	Yes[2]	Yes[3]	Yes[3]	No	No	No
LACP	No	Yes[3]	Yes[2]	No	Yes[2]	Yes[3]	No	Yes[2]	Yes[3]	Yes[3]	No	No	No
Static CLAG	No	No	No	No	No	No	No	No	No	No	No	No	No
LACP CLAG	No	No	Yes[2]	No	Yes[2]	Yes[3]	No	Yes[2]	Yes[3]	Yes[3]	No	No	No
Hot-plug	No	No	No	No	No	No	No	No	No	No	Yes	No	No

Die in der vorstehenden Tabelle verwendeten hochgestellten Zahlen (1, 2, 3) beziehen sich auf die folgenden Punkte mit entsprechender Nummerierung:

1. Clustering-Unterstützung ist auf SRIOV für clientseitige und serverseitige Schnittstellen und nicht für die Rückwandplatine verfügbar.

2. Interface DOWN Ereignisse werden in Citrix ADC VPX-Instanzen nicht aufgezeichnet.
3. Für statische LA wird möglicherweise weiterhin Datenverkehr auf der Schnittstelle gesendet, deren physischer Status DOWN ist.
4. Für LACP kennt das Peer-Gerät das Interface DOWN-Ereignis basierend auf dem LACP-Timeout-Mechanismus.
    - Kurzes Timeout: 3 Sekunden
    - Langes Timeout: 90 Sekunden
5. Teilen Sie für LACP keine Schnittstellen zwischen VMs.
6. Bei dynamischem Routing hängt die Konvergenzzeit vom Routingprotokoll ab, da Linkereignisse nicht erkannt werden.
7. Die überwachte statische Route-Funktionalität schlägt fehl, wenn Sie keine Monitore an statische Routen binden, da der Routenstatus vom VLAN-Status abhängt. Der VLAN-Status hängt vom Verbindungsstatus ab.
8. Eine teilweise Fehlererkennung erfolgt bei hoher Verfügbarkeit nicht, wenn ein Verbindungsfehler vorliegt. Eine Hohe-Verfügbarkeit-Split-Brain-Bedingung kann auftreten, wenn ein Verbindungsfehler vorliegt.
    - Wenn ein Linkereignis (Deaktivieren/Aktivieren, Zurücksetzen) von einer VPX-Instanz generiert wird, ändert sich der physische Status des Links nicht. Bei statischer LA wird jeder vom Peer initiierte Datenverkehr auf der Instanz gelöscht.
    - Damit die VLAN-Tagging-Funktion funktioniert, gehen Sie folgendermaßen vor:

    Legen Sie auf VMware ESX die VLAN-ID der Portgruppe auf dem vSwitch des VMware ESX-Servers auf 1-4095 fest. Weitere Informationen zum Festlegen einer VLAN-ID auf dem vSwitch des VMware ESX-Servers finden Sie unter VMware ESX Server 3 802.1Q VLAN Solutions.

Tabelle 8. Unterstützte Browser

Betriebssystem	Browser und Versionen
Windows 7	Internet Explorer-8, 9, 10 und 11; Mozilla Firefox 3.6.25 und höher; Google Chrome-15 und höher
Windows 64-Bit	Internet Explorer — 8, 9; Google Chrome — 15 und höher
MAC	Mozilla Firefox - 12 und höher; Safari - 5.1.3; Google Chrome - 15 und höher

Richtlinien für die Verwendung

Folgen Sie diesen Nutzungsrichtlinien:

Weitere Informationen zu **VMware ESXi CPU-Überlegungen** im Dokument Performance Best Practices for VMware vSphere 6.5. Hier ist ein Auszug:

- Es wird nicht empfohlen, dass virtuelle Maschinen mit hohem CPU/Speicherbedarf auf einem Host/Cluster sind, der überbelegt ist.
- In den meisten Umgebungen ermöglicht ESXi eine erhebliche CPU-Überbelegung, ohne die Leistung der virtuellen Maschine zu beeinträchtigen. Auf einem Host können Sie mehr vCPUs ausführen als die Gesamtzahl der physischen Prozessorkerne in diesem Host.
- Wenn ein ESXi-Host CPU-gesättigt wird, d.h. die virtuellen Maschinen und andere Lasten auf dem Host alle CPU-Ressourcen verlangen, die der Host hat, funktionieren latenzsensitive Workloads möglicherweise nicht gut. In diesem Fall möchten Sie möglicherweise die CPU-Last reduzieren, indem Sie beispielsweise einige virtuelle Maschinen ausschalten oder auf einen anderen Host migrieren oder DRS erlauben, sie automatisch zu migrieren.
- Citrix empfiehlt die neueste Hardwarekompatibilitätsversion, um die neuesten Funktionen des ESXi-Hypervisors für die virtuelle Maschine nutzen zu können. Weitere Informationen zur Hardware- und ESXi-Versionskompatibilität finden Sie in der VMware-Dokumentation.
- Der Citrix ADC VPX ist eine latenzempfindliche, leistungsstarke virtuelle Appliance. Um die erwartete Leistung zu erzielen, benötigt die Appliance eine vCPU-Reservierung, Speicherreservierung und vCPU-Pinning auf dem Host. Außerdem muss Hyper-Threading auf dem Host deaktiviert werden. Wenn der Host diese Anforderungen nicht erfüllt, treten Probleme wie Hochverfügbarkeitsfailover, CPU-Anstieg innerhalb der VPX-Instanz, Trägheit beim Zugriff auf die VPX CLI, Absturz des Pitboss-Daemons, Paketausfälle und ein niedriger Durchsatz auf.

Ein Hypervisor gilt als übermäßig bereitgestellt, wenn eine der folgenden beiden Bedingungen erfüllt ist:

- Die Gesamtzahl der auf dem Host bereitgestellten virtuellen Kerne (vCPU) ist größer als die Gesamtzahl der physischen Kerne (pCPUs).
- Die Gesamtzahl der bereitgestellten VMs verbrauchen mehr vCPUs als die Gesamtzahl der pCPUs.

  Wenn eine Instanz übermäßig bereitgestellt wird, garantiert der Hypervisor möglicherweise nicht die für die Instanz reservierten Ressourcen (wie CPU, Speicher und andere) aufgrund von Hypervisor-Planungs-Overheads, Fehlern oder Einschränkungen mit dem Hypervisor. Dieses Verhalten kann zu einem Mangel an CPU-Ressource für Citrix ADC führen und zu den im ersten Punkt unter den **Nutzungsrichtlinien** genannten Problemen führen. Als Administratoren wird empfohlen, die Mandanten auf dem Host zu reduzieren, sodass die Gesamtanzahl der auf dem Host bereitgestellten vCPUs kleiner oder gleich der Gesamtzahl der pCPUs ist.

Beispiel

Wenn für ESX-Hypervisor der Parameter `%RDY%` einer VPX-vCPU in der Befehlsausgabe von `esxtop` größer als 0 ist, wird für den ESX-Host Zeitplanungsoverhead angegeben, was zu Latenzproblemen für die VPX-Instanz führen kann.

Reduzieren Sie in einer solchen Situation die Mandanten auf dem Host, sodass `%RDY%` immer auf 0 zurückkehrt. Wenden Sie sich alternativ an den Hypervisor-Anbieter, um den Grund für die Nichteinhalten der durchgeführten Ressourcenreservierung zu prüfen.

- Hot Adding wird nur für PV- und SRIOV-Schnittstellen mit Citrix ADC auf AWS unterstützt. VPX-Instanzen mit ENA-Schnittstellen unterstützen kein Hot-Plug, und das Verhalten der Instanzen kann unvorhersehbar sein, wenn Hot-Plugging versucht wird.
- Das heiße Entfernen entweder über die AWS-Webkonsole oder die AWS CLI-Schnittstelle wird mit PV-, SRIOV- und ENA-Schnittstellen für Citrix ADC nicht unterstützt. Das Verhalten der Instanzen kann unvorhersehbar sein, wenn versucht wird, Hot-Removal durchzuführen.

Befehle zur Steuerung der CPU-Auslastung der Paket-Engine

Sie können zwei Befehle (`set ns vpxparam` und `show ns vpxparam`) verwenden, um das CPU-Auslastungsverhalten von VPX-Instanzen in Hypervisor- und Cloud-Umgebungen zu steuern:

- `set ns vpxparam [-cpuyield (YES | NO | DEFAULT)] [-masterclockcpu1 (YES | NO)]`

  Erlauben Sie jeder VM, CPU-Ressourcen zu verwenden, die einer anderen VM zugewiesen wurden, aber nicht verwendet werden.

  Parameter für `Set ns vpxparam`:

  -cpuyield: Freigabe von zugewiesenen, aber nicht genutzten CPU-Ressourcen.

  - **YES**: Erlauben Sie, dass zugewiesene, aber ungenutzte CPU-Ressourcen von einer anderen VM verwendet werden.
  - **NO**: Reservieren Sie alle CPU-Ressourcen für die VM, der sie zugewiesen wurden. Diese Option zeigt einen höheren Prozentsatz in Hypervisor- und Cloud-Umgebungen für die VPX-CPU-Auslastung.
  - **DEFAULT**: Nein.

  > **Hinweis**
  >
  > Auf allen Citrix ADC VPX-Plattformen beträgt die vCPU-Auslastung auf dem Hostsystem 100 Prozent. Geben Sie den Befehl `set ns vpxparam -cpuyield YES` ein, um diese Verwendung zu überschreiben.

Wenn Sie die Clusterknoten auf “yield” setzen möchten, müssen Sie die folgenden zusätzlichen Konfigurationen für CCO durchführen:

- Wenn ein Cluster gebildet wird, erhalten alle Knoten “yield=DEFAULT”.
- Wenn ein Cluster unter Verwendung der Knoten gebildet wird, die bereits auf “yield=Yes” eingestellt sind, werden die Knoten mit “yield=DEFAULT” zum Cluster hinzugefügt.

> Hinweis:
>
> Wenn Sie die Clusterknoten auf “Yield=yes” setzen möchten, können Sie erst nach der Bildung des Clusters konfigurieren, aber nicht bevor der Cluster gebildet wurde.

-masterclockcpu1: Sie können die Haupttaktquelle von CPU0 (Management-CPU) auf CPU1 verschieben. Dieser Parameter hat die folgenden Optionen:

- **YES**: Erlauben Sie der VM, die Haupttaktquelle von CPU0 auf CPU1 zu verschieben.
- **NO**: VM verwendet CPU0 für die Haupttaktquelle. Standardmäßig ist CPU0 die Haupttaktquelle.

- `show ns vpxparam`

  Zeigt die aktuellen `vpxparam`-Einstellungen an.

Andere Referenzen

- Für Citrix Ready-Produkte besuchen Sie Citrix Ready Marketplace.
- Informationen zum Citrix Ready-Produktsupport finden Sie auf der FAQ-Seite.
- Informationen zu VMware ESX-Hardwareversionen finden Sie unter Upgrade von VMware Tools.

Optimize Citrix ADC VPX performance on VMware ESX, Linux KVM, and Citrix Hypervisors

December 7, 2021

The Citrix ADC VPX performance greatly varies depending on the hypervisor, allocated system resources, and the host configurations. To achieve the desired performance, first follow the recommendations in the VPX data sheet, and then further optimize it using the best practices provided in this document.

Citrix ADC VPX instance on VMware ESX hypervisors

This section contains details of configurable options and settings, and other suggestions that help you achieve optimal performance of Citrix ADC VPX instance on VMware ESX hypervisors.

- Recommended configuration on ESX hosts
- Citrix ADC VPX with E1000 network interfaces
- Citrix ADC VPX with VMXNET3 network interfaces
- Citrix ADC VPX with SR-IOV and PCI passthrough network interfaces

Recommended configuration on ESX hosts

To achieve high performance for VPX with E1000, VMXNET3, SR-IOV, and PCI passthrough network interfaces, follow these recommendations:

- The total number of virtual CPUs (vCPUs) provisioned on the ESX host must be less than or equal to the total number of physical CPUs (pCPUs) on the ESX host.
- Non-uniform Memory Access (NUMA) affinity and CPU affinity must be set for the ESX host to achieve good results.

  – To find the NUMA affinity of a Vmnic, log in to the host locally or remotely, and type:

```
#vsish -e get /net/pNics/vmnic7/properties | grep NUMA
Device NUMA Node: 0
<!--NeedCopy-->
```

  – To set NUMA and vCPU affinity for a VM, see VMware documentation.

Citrix ADC VPX with E1000 network interfaces

Perform the following settings on the VMware ESX host:

- On the VMware ESX host, create two vNICs from one pNIC vSwitch. Multiple vNICs create multiple Rx threads in the ESX host. This increases the Rx throughput of the pNIC interface.
- Enable VLANs on the vSwitch port group level for each vNIC that you have created.
- To increase vNIC transmit (Tx) throughput, use a separate Tx thread in the ESX host per vNIC. Use the following ESX command:

  – For ESX version 5.5:


```
esxcli system settings advanced set  -o /Net/NetTxWorldlet  -
    i
<!--NeedCopy-->
```

- For ESX version 6.0 onwards:

```
esxcli system settings advanced set -o /Net/NetVMTxType  -i 1
<!--NeedCopy-->
```

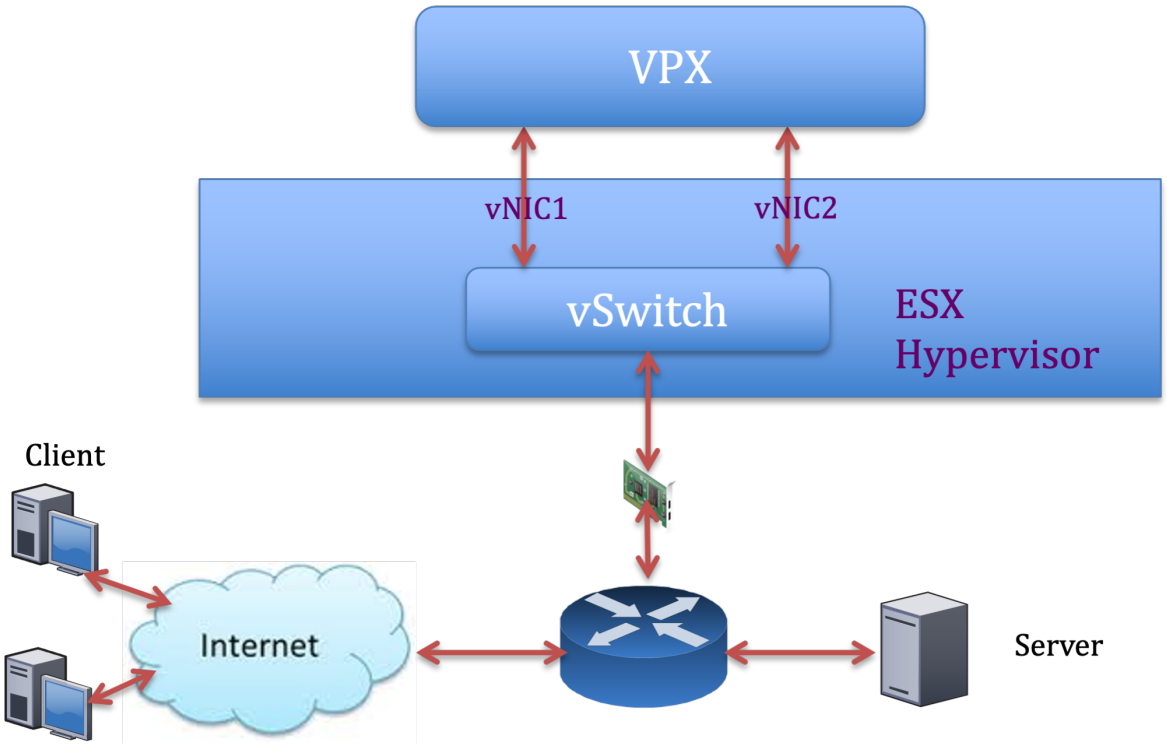
- To further increase the vNIC Tx throughput, use a separate Tx completion thread and Rx threads per device (NIC) queue. Use the following ESX command:

```
esxcli system settings advanced set -o /Net/
   NetNetqRxQueueFeatPairEnable -i 0
<!--NeedCopy-->
```

> Note:
>
> Make sure that you reboot the VMware ESX host to apply the updated settings.

Two vNICs per pNIC deployment

The following is a sample topology and configuration commands for the **Two vNICs per pNIC** model of deployment that delivers better network performance.



Citrix ADC VPX sample configuration:

To achieve the deployment shown in the preceding sample topology, perform the following configuration on the Citrix ADC VPX instance:

- On the client side, bind the SNIP (1.1.1.2) to network interface 1/1 and enable the VLAN tag mode.

```
1  bind vlan 2 -ifnum 1/1  - tagged
2  bind vlan 2 -IPAddress 1.1.1.2 255.255.255.0
3  <!--NeedCopy-->
```

- On the server side, bind the SNIP (2.2.2.2) to network interface 1/1 and enable the VLAN tag mode.

```
1  bind vlan 3 -ifnum 1/2  - tagged
2  bind vlan 3 -IPAddress 2.2.2.2 255.255.255.0
3  <!--NeedCopy-->
```

- Add an HTTP virtual server (1.1.1.100) and bind it to a service (2.2.2.100).


```
add lb vserver v1 HTTP 1.1.1.100 80 -persistenceType NONE -
   Listenpolicy None -cltTimeout 180
add service s1 2.2.2.100 HTTP 80 -gslb NONE -maxClient 0 -maxReq
   0 -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout
   180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
bind lb vserver v1 s1
<!--NeedCopy-->
```

> Note:
>
> Make sure that you include the following two entries in the route table:
>
> - 1.1.1.0/24 subnet with gateway pointing to SNIP 1.1.1.2
> - 2.2.2.0/24 subnet with gateway pointing to SNIP 2.2.2.2

Citrix ADC VPX with VMXNET3 network interfaces

To achieve high performance for VPX with VMXNET3 network interfaces, do the following settings on the VMware ESX host:

- Create two vNICs from one pNIC vSwitch. Multiple vNICs create multiple Rx threads in the ESX host. This increases the Rx throughput of the pNIC interface.
- Enable VLANs on the vSwitch port group level for each vNIC that you have created.
- To increase vNIC transmit (Tx) throughput, use a separate Tx thread in the ESX host per vNIC. Use the following ESX commands:
  - For ESX version 5.5:

```
esxcli system settings advanced set  -o /Net/NetTxWorldlet  -i
<!--NeedCopy-->
```

  - For ESX version 6.0 onwards:

```
 esxcli system settings advanced set -o /Net/NetVMTxType  -i 1
 <!--NeedCopy-->
```

On the VMware ESX host, perform the following configuration:

- On the VMware ESX host, create two vNICs from 1 pNIC vSwitch. Multiple vNICs create multiple Tx and Rx threads in the ESX host. This increases the Tx and Rx throughput of the pNIC interface.
- Enable VLANs on the vSwitch port group level for each vNIC that you have created.
- To increase Tx throughput of a vNIC, use a separate Tx completion thread and Rx threads per device (NIC) queue. Use the following command:


```
esxcli system settings advanced set -o /Net/
   NetNetqRxQueueFeatPairEnable -i 0
<!--NeedCopy-->
```

- Configure a VM to use one transmit thread per vNIC, by adding the following setting to the VM's configuration:

```
ethernetX.ctxPerDev = "1"
<!--NeedCopy-->
```

For more information, see Best Practices for Performance Tuning of Telco and NFV Workloads in vSphere

> Note:
>
> Make sure that you reboot the VMware ESX host to apply the updated settings.

You can configure VMXNET3 as a **Two vNICs per pNIC** deployment. For more information, see Two vNICs per pNIC deployment.

Citrix ADC VPX with SR-IOV and PCI passthrough network interfaces

To achieve high performance for VPX with SR-IOV and PCI passthrough network interfaces, see Recommended configuration on ESX hosts.

Citrix ADC VPX instance on Linux-KVM platform

This section contains details of configurable options and settings, and other suggestions that help you achieve optimal performance of Citrix ADC VPX instance on Linux-KVM platform.

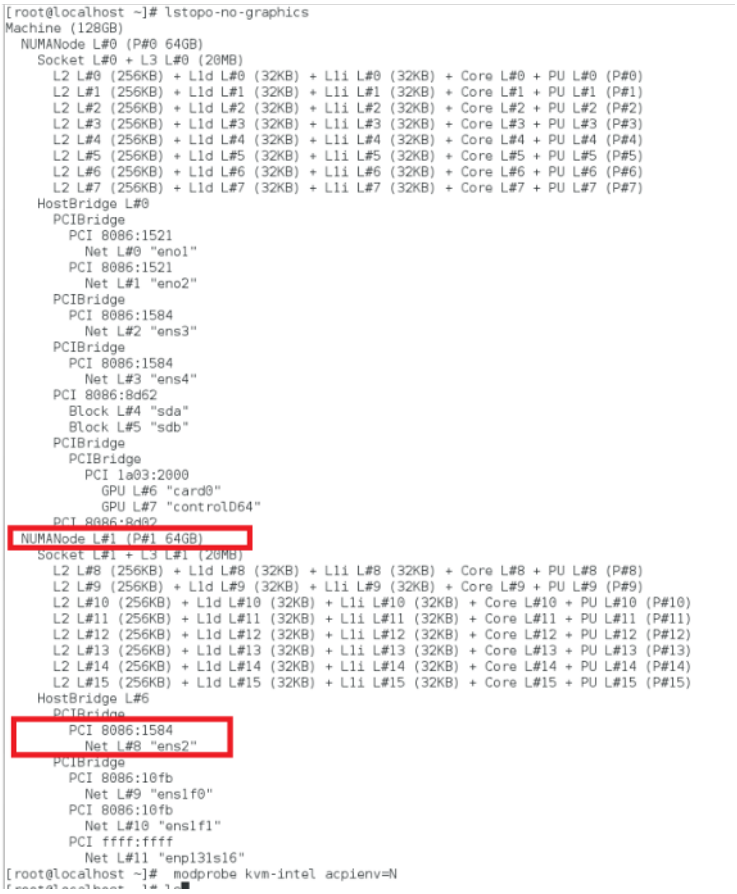
- Performance settings for KVM
- Citrix ADC VPX with PV network interfaces
- Citrix ADC VPX with SR-IOV and Fortville PCIe passthrough network interfaces

Performance settings for KVM

Perform the following settings on the KVM host:

Find the NUMA domain of the NIC using the `lstopo` command:

Make sure that memory for the VPX and the CPU is pinned to the same location.
In the following output, the 10G NIC "ens2" is tied to NUMA domain #1.



Allocate the VPX memory from the NUMA domain.

The `numactl` command indicates the NUMA domain from which the memory is allocated. In the following output, around 10 GB RAM is allocated from NUMA node #0.

```
[root@localhost ~]# numactl --hardware
available: 2 nodes (0-1)
node 0 cpus: 0 1 2 3 4 5 6 7
node 0 size: 65429 MB
node 0 free: 55854 MB
node 1 cpus: 8 9 10 11 12 13 14 15
node 1 size: 65536 MB
node 1 free: 52388 MB
node distances:
node   0   1
  0:  10  21
  1:  21  10
[root@localhost ~]#
```

To change the NUMA node mapping, follow these steps.

1. Edit the .xml of the VPX on the host.


```
/etc/libvirt/qemu/<VPX_name>.xml
<!--NeedCopy-->
```

2. Add the following tag:

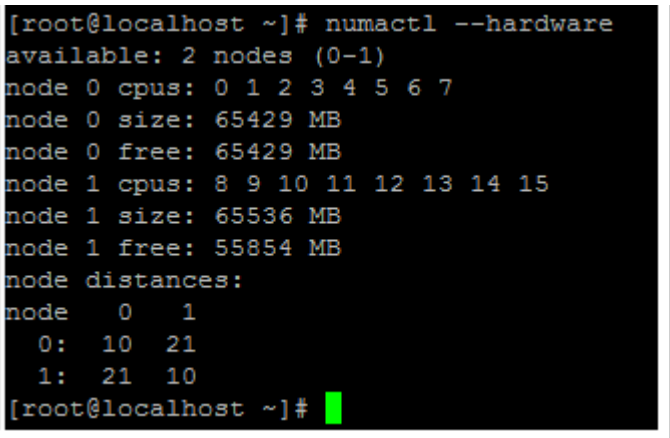
```
<numatune>
<memory mode="strict" nodeset="1"/>    This is the NUMA domain
   name
</numatune>
<!--NeedCopy-->
```

3. Shut down the VPX.
4. Run the following command:

```
virsh define /etc/libvirt/qemu/<VPX_name>.xml
<!--NeedCopy-->
```

   This command updates the configuration information for the VM with the NUMA node mappings.

5. Power on the VPX. Then check the `numactl -hardware` command output on the host to see the updated memory allocations for the VPX.



Pin vCPUs of VPX to physical cores.

- To view the vCPU to pCPU mappings of a VPX, type the following command

```
virsh vcpupin <VPX name>
<!--NeedCopy-->
```



```
root@localhost qemu]#  virsh vcpupin NS-VPX-DVR
CPU: CPU Affinity
----------------------------------
  0: 8
  1: 9
  2: 10
  3: 11
```

The vCPUs 0–4 are mapped to physical cores 8–11.

- To view the current pCPU usage, type the following command:

```
mpstat -P ALL 5
<!--NeedCopy-->
```

```
[root@localhost qemu]# mpstat -P ALL 5
Linux 3.10.0-123.el7.x86_64 (localhost.localdomain)     05/17/2016      _x86_64_        (16 CPU)

02:26:20 PM  CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest  %gnice   %idle
02:26:25 PM  all    0.24    0.00    1.67    0.00    0.00    0.00    0.00   17.32    0.00   80.78
02:26:25 PM    0    0.20    0.00    1.00    0.00    0.00    0.00    0.00    0.00    0.00   98.80
02:26:25 PM    1    0.20    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    2    0.20    0.00    0.40    0.00    0.00    0.00    0.00    0.00    0.00   99.40
02:26:25 PM    3    0.00    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.80
02:26:25 PM    4    0.20    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    5    0.60    0.00    0.20    0.00    0.00    0.00    0.00    0.00    0.00   99.20
02:26:25 PM    6    0.40    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00   99.60
02:26:25 PM    7    1.62    0.00    1.42    0.00    0.00    0.00    0.00    0.00    0.00   96.96
02:26:25 PM    8    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM    9    0.00    0.00    7.60    0.00    0.00    0.00    0.00   92.40    0.00    0.00
02:26:25 PM   10    0.20    0.00    7.00    0.00    0.00    0.00    0.00   92.80    0.00    0.00
02:26:25 PM   11    0.00    0.00    8.60    0.00    0.00    0.00    0.00   91.40    0.00    0.00
02:26:25 PM   12    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   13    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   14    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
02:26:25 PM   15    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00    0.00  100.00
```

In this output, 8 is management CPU, and 9–11 are packet engines.

- To change the vCPU to pCPU pinning, there are two options.
  - Change it at runtime after the VPX boots up using the following command:

```
virsh vcpupin <VPX name> <vCPU id>  <pCPU number>
virsh vcpupin NetScaler-VPX-XML 0 8
virsh vcpupin NetScaler-VPX-XML 1 9
virsh vcpupin NetScaler-VPX-XML 2 10
virsh vcpupin NetScaler-VPX-XML 3 11
<!--NeedCopy-->
```

  - To make static changes to the VPX, edit the `.xml` file as before with the following tags:
    1. Edit the .xml file of the VPX on the host


```
/etc/libvirt/qemu/<VPX_name>.xml
<!--NeedCopy-->
```

2. Add the following tag:

```
<vcpu placement='static' cpuset='8-11'>4</vcpu>
    <cputune>
        <vcpupin vcpu='0' cpuset='8'/>
        <vcpupin vcpu='1' cpuset='9'/>
        <vcpupin vcpu='2' cpuset='10'/>
        <vcpupin vcpu='3' cpuset='11'/>
    </cputune>
<!--NeedCopy-->
```

3. Shut down the VPX.
4. Update the configuration information for the VM with the NUMA node mappings using the following command:

```
virsh define /etc/libvirt/qemu/ <VPX_name>.xml
<!--NeedCopy-->
```

5. Power on the VPX. Then check the `virsh vcpupin <VPX name>` command output on the host to see the updated CPU pinning.

Eliminate host interrupt overhead.

- Detect VM_EXITS using the `kvm_stat` command.

  At the hypervisor level, host interrupts are mapped to the same pCPUs on which the vCPUs of the VPX are pinned. This might cause vCPUs on the VPX to get kicked out periodically.

  To find the VM exits done by VMs running the host, use the `kvm_stat` command.

```
[root@localhost ~]# kvm_stat -1  | grep EXTERNAL
kvm_exit(EXTERNAL_INTERRUPT)  1728349 27738
[root@localhost ~]#
<!--NeedCopy-->
```

  A higher value in the order of 1+M indicates an issue.

If a single VM is present, the expected value is 30–100 K. Anything more than that can indicate that there are one or more host interrupt vectors mapped to the same pCPU.

- Detect host interrupts and migrate host interrupts.

  When you run the `concatenate` command for the "/proc/interrupts" file, it displays all the host interrupt mappings. If one or more active IRQs map to the same pCPU, its corresponding counter increments.

  Move any interrupts that overlap with your Citrix ADC VPX's pCPUs to unused pCPUs:

```
echo 0000000f > /proc/irq/55/smp_affinity
0000000f - - > it is a bitmap, LSBs indicates that IRQ 55 can
   only be scheduled on pCPUs 0 - 3
<!--NeedCopy-->
```

- Disable IRQ balance.

  Disable IRQ balance daemon, so that no rescheduling happens on the fly.

```
service irqbalance stop
service irqbalance show - To check the status
service irqbalance start - Enable if needed
<!--NeedCopy-->
```

  Make sure you run the `kvm_stat` command to ensure that there are not many counters.

Citrix ADC VPX with PV network interfaces

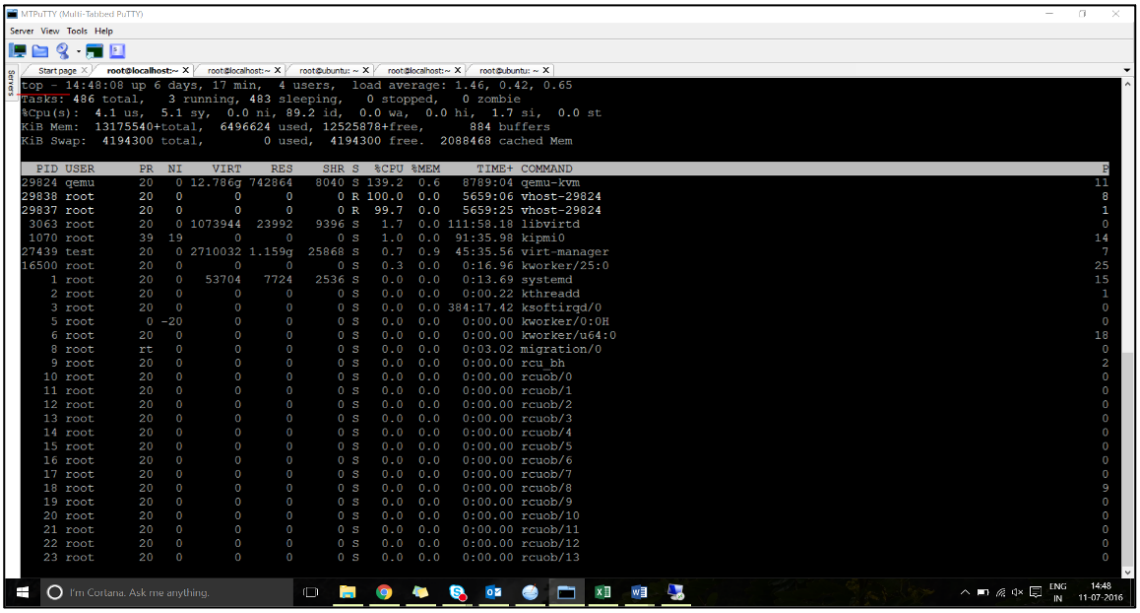
You can configure para-virtualization (PV), SR-IOV, and PCIe passthrough network interfaces as a **Two vNICs per pNIC** deployment. For more information, see Two vNICs per pNIC deployment.

For optimal performance of PV (virtio) interfaces, follow these steps:

- Identify the NUMA domain to which the PCIe slot/NIC is tied to.
- The Memory and vCPU for the VPX must be pinned to the same NUMA domain.
- Vhost thread must be bound to the CPUs in the same NUMA domain.

Bind the virtual host threads to the corresponding CPUs:

1. Once the traffic is started, run the `top` command on the host.



2. Identify the virtual host process (named as `vhost-<pid-of-qemu>`) affinity.
3. Bind the vHost processes to the physical cores in the NUMA domain identified earlier using the following command:

```
taskset -pc <core-id> <process-id>
<!--NeedCopy-->
```

Example:

```
taskset -pc 12 29838
<!--NeedCopy-->
```

4. The processor cores corresponding to the NUMA domain can be identified with the following command:

```
[root@localhost ~]# virsh capabilities | grep cpu
<cpu>
    </cpu>
        <cpus num='8'>
            <cpu id='0' socket_id='0' core_id='0' siblings='0'/>
            <cpu id='1' socket_id='0' core_id='1' siblings='1'/>
            <cpu id='2' socket_id='0' core_id='2' siblings='2'/>
            <cpu id='3' socket_id='0' core_id='3' siblings='3'/>
```



```
9               <cpu id='4' socket_id='0' core_id='4' siblings='4'/>
10              <cpu id='5' socket_id='0' core_id='5' siblings='5'/>
11              <cpu id='6' socket_id='0' core_id='6' siblings='6'/>
12              <cpu id='7' socket_id='0' core_id='7' siblings='7'/>
13          </cpus>
14
15          <cpus num='8'>
16          <cpu id='8' socket_id='1' core_id='0' siblings='8'/>
17          <cpu id='9' socket_id='1' core_id='1' siblings='9'/>
18          <cpu id='10' socket_id='1' core_id='2' siblings='10'/>
19          <cpu id='11' socket_id='1' core_id='3' siblings='11'/>
20          <cpu id='12' socket_id='1' core_id='4' siblings='12'/>
21          <cpu id='13' socket_id='1' core_id='5' siblings='13'/>
22          <cpu id='14' socket_id='1' core_id='6' siblings='14'/>
23          <cpu id='15' socket_id='1' core_id='7' siblings='15'/>
24          </cpus>
25
26      <cpuselection/>
27      <cpuselection/>
28
29  <!--NeedCopy-->
```

Bind the QEMU process to the corresponding physical core:

1. Identify the physical cores on which the QEMU process is running. For more information, see the preceding output.
2. Bind the QEMU process to the same physical cores to which you bind the vCPUs, using the following command:

```
1  taskset  -pc 8-11 29824
2  <!--NeedCopy-->
```

Citrix ADC VPX with SR-IOV and Fortville PCIe passthrough network interfaces

For optimal performance of the SR-IOV and Fortville PCIe passthrough network interfaces, follow these steps:

- Identify the NUMA domain to which the PCIe slot/NIC is tied to.
- The Memory and vCPU for the VPX must be pinned to the same NUMA domain.

Sample VPX XML file for vCPU and memory pinning for Linux KVM:


```
    <domain type='kvm'>
        <name>NetScaler-VPX</name>
        <uuid>138f7782-1cd3-484b-8b6d-7604f35b14f4</uuid>
        <memory unit='KiB'>8097152</memory>
        <currentMemory unit='KiB'>8097152</currentMemory>
        <vcpu placement='static'>4</vcpu>

    <cputune>
        <vcpupin vcpu='0' cpuset='8'/>
        <vcpupin vcpu='1' cpuset='9'/>
        <vcpupin vcpu='2' cpuset='10'/>
        <vcpupin vcpu='3' cpuset='11'/>
    </cputune>

    <numatune>
    <memory mode='strict' nodeset='1'/>
    </numatune>

    </domain>
<!--NeedCopy-->
```

Citrix ADC VPX instance on Citrix Hypervisors

This section contains details of configurable options and settings, and other suggestions that help you achieve optimal performance of Citrix ADC VPX instance on Citrix Hypervisors.

- Performance settings for Citrix Hypervisors
- Citrix ADC VPX with SR-IOV network interfaces
- Citrix ADC VPX with para-virtualized interfaces

Performance settings for Citrix Hypervisors

Find the NUMA domain of the NIC using the “xl” command:

```
xl info -n
<!--NeedCopy-->
```

Pin vCPUs of VPX to physical cores.

```
xl vcpu-pin <Netsclaer VM Name>  <vCPU id>  <physical CPU id>
```



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

Check binding of vCPUs.

```
xl vcpu-list
<!--NeedCopy-->
```

Allocate more than 8 vCPUs to Citrix ADC VMs.

For configuring more than 8 vCPUs, run the following commands from the Citrix Hypervisor console:

```
xe vm-param-set uuid=your_vms_uuid VCPUs-max=16
xe vm-param-set uuid=your_vms_uuid VCPUs-at-startup=16
<!--NeedCopy-->
```

Citrix ADC VPX with SR-IOV network interfaces

For optimal performance of the SR-IOV network interfaces, follow these steps:

- Identify the NUMA domain to which the PCIe slot or NIC is tied to.
- Pin the Memory and vCPU for the VPX to the same NUMA domain.
- Bind the Domain-0 vCPU to the remaining CPU.

Citrix ADC VPX with para-virtualized interfaces

For optimal performance, two vNICs per pNIC and one vNIC per pNIC configurations are advised, as in other PV environments.

To achieve optimal performance of para-virtualized (netfront) interfaces, follow these steps:

- Identify the NUMA domain to which the PCIe slot or NIC is tied to.
- Pin the memory and vCPU for the VPX to the same NUMA domain.
- Bind the Domain-0 vCPU to the remaining CPU of the same NUMA domain.
- Pin host Rx/Tx threads of vNIC to Domain-0 vCPUs.

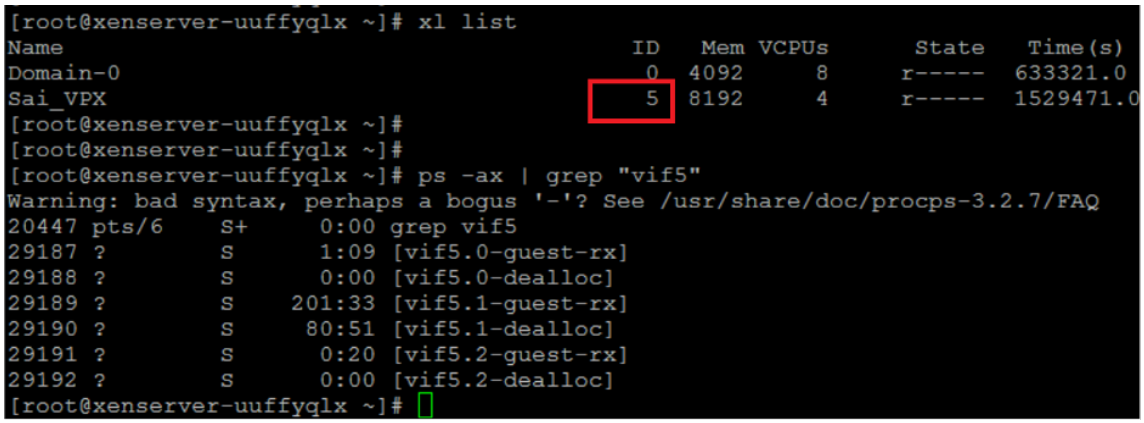
Pin host threads to Domain-0 vCPUs:

1. Find Xen-ID of the VPX by using the `xl list` command on the Citrix Hypervisor host shell.
2. Identify host threads by using the following command:


```
ps -ax | grep vif <Xen-ID>
<!--NeedCopy-->
```

In the following example, these values indicate:

- **vif5.0** - The threads for first interface allocated to VPX in XenCenter (management interface).
- **vif5.1** - The threads for second interface assigned to VPX and so on.



3. Pin the threads to Domain-0 vCPUs using the following command:

```
taskset  - pc <core-id> <process-id>
<!--NeedCopy-->
```

Example:

```
taskset -pc 1 29189
<!--NeedCopy-->
```

Wenden Sie Citrix ADC VPX-Konfigurationen beim ersten Start der Citrix ADC Appliance in der Cloud an

October 5, 2021

Sie können die Citrix ADC VPX-Konfigurationen beim ersten Start der Citrix ADC Appliance in einer Cloud-Umgebung anwenden. Diese Phase wird in diesem Dokument als **Preboot-Phase** behandelt. Daher wird in bestimmten Fällen wie der ADC-gepoolten Lizenzierung eine bestimmte VPX-Instanz in

viel geringerer Zeit aufgebracht. Diese Funktion ist in Microsoft Azure, Google Cloud-Plattform und AWS-Clouds verfügbar.

Was sind Benutzerdaten

Wenn Sie eine VPX-Instanz in einer Cloud-Umgebung bereitstellen, haben Sie die Möglichkeit, Benutzerdaten an die Instanz zu übergeben. Mit den Benutzerdaten können Sie allgemeine automatisierte Konfigurationsaufgaben ausführen, das Startverhalten von Instanzen anpassen und Skripts ausführen, nachdem die Instanz gestartet wurde. Beim ersten Start führt die Citrix ADC VPX-Instanz die folgenden Aufgaben aus:

- Liest die Benutzerdaten.
- Interpretiert die in Benutzerdaten bereitgestellte Konfiguration.
- Wendet die neu hinzugefügte Konfiguration beim Booten an.

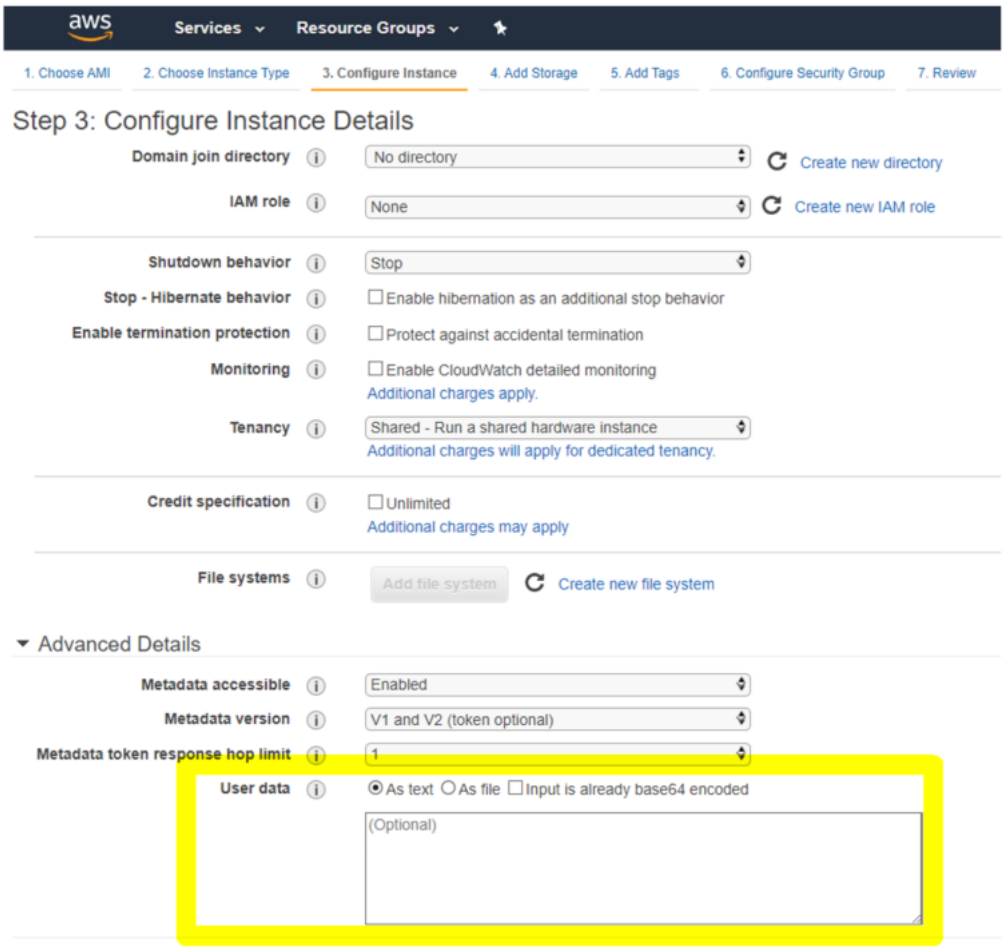
So stellen Sie Preboot-Benutzerdaten in Cloud-Instanz zur Verfügung

Sie können der Cloud-Instanz Preboot-Benutzerdaten im XML-Format zur Verfügung stellen. Verschiedene Clouds haben unterschiedliche Schnittstellen zur Bereitstellung von Benutzerdaten.

Bereitstellung von Preboot-Benutzerdaten über die AWS-Konsole

Wenn Sie eine Citrix ADC VPX-Instanz über die AWS-Konsole bereitstellen, navigieren **Sie zu Instanzdetails konfigurieren > Erweiterte Details**und geben Sie die Preboot-Benutzerdatenkonfiguration im Feld **Benutzerdaten** an.

Ausführliche Anweisungen zu jedem der Schritte finden Sie unter Bereitstellen einer Citrix ADC VPX-Instanz in AWS mithilfe der AWS-Webkonsole.
Weitere Informationen finden Sie in der AWS-Dokumentation zum Starten einer Instanz.



Bereitstellung von Preboot-Benutzerdaten mit AWS CLI

Geben Sie den folgenden Befehl in die AWS CLI ein:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --count 1 \
    --subnet-id subnet-08fc749671b2d077c \
    --key-name MyKeyPair \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --user-data file://my_script.txt
<!--NeedCopy-->
```

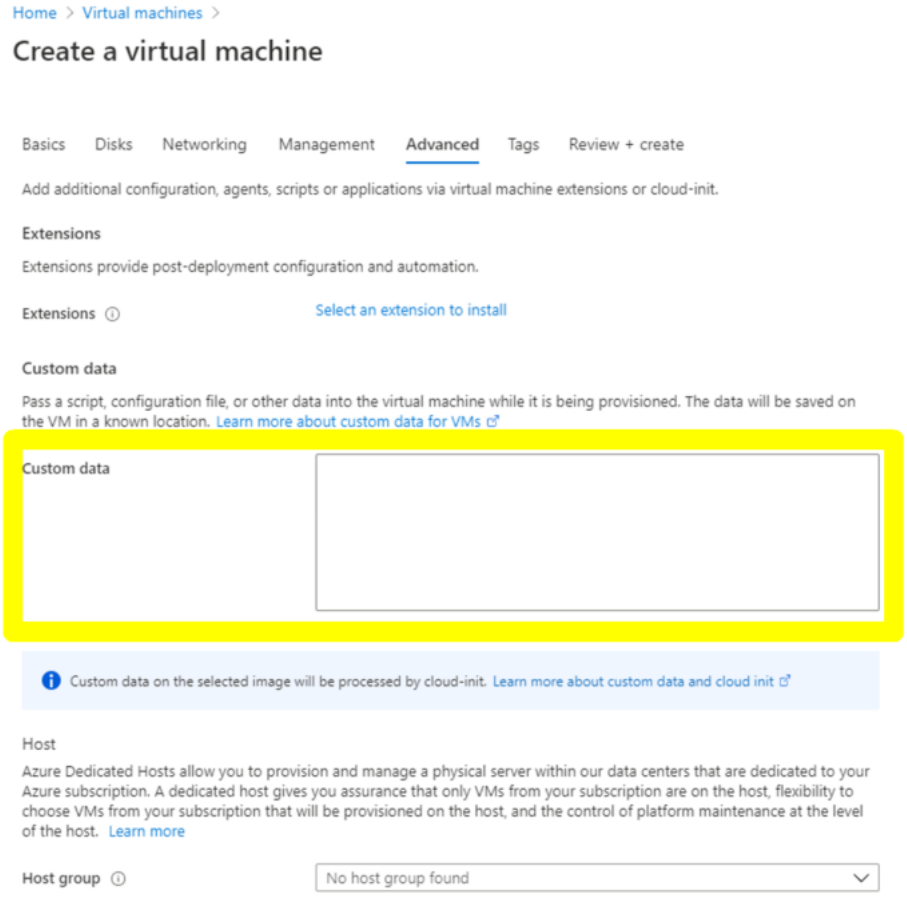
Weitere Informationen finden Sie in der AWS-Dokumentation zu Running Instances.

Weitere Informationen finden Sie in der AWS-Dokumentation zur Verwendung von Instanz-

Benutzerdaten

Stellen Sie Preboot-Benutzerdaten mit der Azure-Konsole bereit

Wenn Sie eine Citrix ADC VPX-Instanz mit der Azure-Konsole bereitstellen, navigieren **Sie zu Virtuelle Maschine erstellen > Erweitert** . Geben Sie im Feld **Benutzerdefinierte Daten** eine Preboot-Benutzerdatenkonfiguration an.



Bereitstellen von Preboot-Benutzerdaten mit der Azure CLI

Geben Sie den folgenden Befehl in die Azure CLI ein:

```
az vm create \
  --resource-group myResourceGroup \
  --name MyVm \
  --image debian \
  --custom-data MyCloudInitScript.txt \
<!--NeedCopy-->
```


Beispiel:

```
az vm create --resource-group MyResourceGroup -name MyVm --image debian
    --custom-data MyCloudInitScript.txt
<!--NeedCopy-->
```

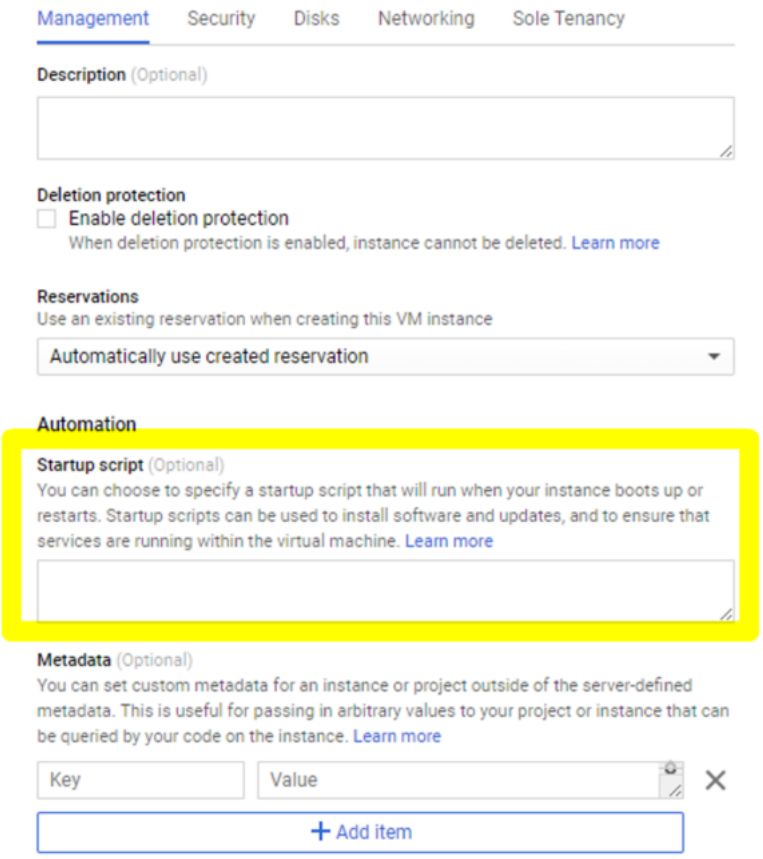
Sie können Ihre benutzerdefinierten Daten oder Preboot-Konfiguration als Datei an den Parameter "—custom-data" übergeben. In diesem Beispiel lautet der Dateiname **MyCloudInitScript.txt**.

Weitere Informationen finden Sie in der Azure CLI-Dokumentation.

Stellen Sie Preboot-Benutzerdaten mit der GCP-Konsole bereit

Wenn Sie eine Citrix ADC VPX-Instanz mit der GCP-Konsole bereitstellen, füllen Sie die Eigenschaften der Instanz aus. Erweitern Sie **Management, Sicherheit, Datenträger, Netzwerke, Einzelmandanten**. Navigieren Sie zur Registerkarte **Verwaltung**. Geben Sie im Abschnitt **Automatisierung** die Konfiguration der Preboot-Benutzerdaten im Feld **Startskript** ein.

Ausführliche Informationen zum Erstellen der VPX-Instanz mit GCP finden Sie unter Bereitstellen einer Citrix ADC VPX-Instanz auf der Google Cloud Platform.



Stellen Sie Preboot-Benutzerdaten mit der gcloud CLI bereit

Geben Sie den folgenden Befehl in die GCP CLI ein:

```
1 gcloud compute instances create INSTANCE_NAMES --metadata-from-file=
     startup-script=LOCAL_FILE_PATH
2 <!--NeedCopy-->
```

metadata-from-file - Liest den Wert oder die Benutzerdaten aus einer Datei, die im <LOCAL_FILE_PATH>.

Weitere Informationen finden Sie in der gcloud CLI-Dokumentation

Preboot-Benutzerdatenformat

Die Preboot-Benutzerdaten müssen der Cloud-Instanz im XML-Format zur Verfügung gestellt werden. Die Citrix ADC Preboot-Benutzerdaten, die Sie während des Bootens über die Cloud-Infrastruktur bereitstellen, können die folgenden vier Abschnitte umfassen:

- Citrix ADC-Konfiguration wird mit dem <NS-CONFIG> Tag dargestellt.
- Benutzerdefiniertes Bootstrapping des Citrix ADC, der mit dem <NS-BOOTSTRAP> Tag dargestellt wird.
- Speichern von Benutzerskripten in Citrix ADC, dargestellt mit dem <NS-SCRIPTS> Tag.
- Gepoolte Lizenzierungskonfiguration, die mit dem <NS-LICENSE-CONFIG> Tag dargestellt wird.

Sie können die vorangegangenen vier Abschnitte in beliebiger Reihenfolge innerhalb der ADC-Preboot-Konfiguration angeben.
Stellen Sie sicher, dass Sie die in den folgenden Abschnitten gezeigten Formatierung genau befolgen, während Sie die Preboot-Benutzerdaten bereitstellen.

> Hinweis:
>
> Die gesamte Preboot-Benutzerdatenkonfiguration muss in das <NS-PRE-BOOT-CONFIG> Tag eingeschlossen sein, wie in den folgenden Beispielen gezeigt.

Beispiel 1:

```
<NS-PRE-BOOT-CONFIG>
     <NS-CONFIG>          </NS-CONFIG>
     <NS-BOOTSTRAP>       </NS-BOOTSTRAP>
     <NS-SCRIPTS>         </NS-SCRIPTS>
     <NS-LICENSE-CONFIG>  </NS-LICENSE-CONFIG>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Beispiel 2:

```
<NS-PRE-BOOT-CONFIG>
    <NS-LICENSE-CONFIG> </NS-LICENSE-CONFIG>
    <NS-SCRIPTS>        </NS-SCRIPTS>
    <NS-BOOTSTRAP>      </NS-BOOTSTRAP>
    <NS-CONFIG>         </NS-CONFIG>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Verwenden Sie das <NS-CONFIG> Tag, um die spezifischen Citrix ADC VPX-Konfigurationen bereitzustellen, die im Preboot-Stadium auf die VPX-Instanz angewendet werden müssen. Diese Konfiguration wird in einer neuen “ns.conf” -Datei gespeichert. Wenn der ADC zum ersten Mal hochgefahren wird, werden die in der Datei “ns.conf” gespeicherten Konfigurationen auf die VPX-Instanz angewendet.

> HINWEIS:
>
> Der <NS-CONFIG> Abschnitt muss über gültige ADC CLI-Befehle verfügen. Die CLIs werden nicht auf die syntaktischen Fehler oder das Format überprüft.

Citrix ADC-Konfigurationen

Verwenden Sie das <NS-CONFIG> Tag, um die spezifischen Citrix ADC VPX-Konfigurationen bereitzustellen, die im Preboot-Stadium auf die VPX-Instanz angewendet werden müssen. Diese Konfiguration wird in einer neuen "ns.conf" -Datei gespeichert. Wenn der ADC zum ersten Mal hochgefahren wird, werden die in der Datei "ns.conf" gespeicherten Konfigurationen auf die VPX-Instanz angewendet.

> HINWEIS:
>
> Der <NS-CONFIG> Abschnitt muss über gültige ADC CLI-Befehle verfügen. Die CLIs werden nicht auf die syntaktischen Fehler oder das Format überprüft.

Beispiel:

Im folgenden Beispiel enthält der <NS-CONFIG> Abschnitt die Details der Konfigurationen. Ein VLAN mit der ID '5' ist konfiguriert und an den SNIP gebunden (5.0.0.1). Ein virtueller Lastenausgleichsserver (4.0.0.101) ist ebenfalls konfiguriert.

```
<NS-PRE-BOOT-CONFIG>

    <NS-CONFIG>
        add vlan 5
        add ns ip  5.0.0.1  255.255.255.0

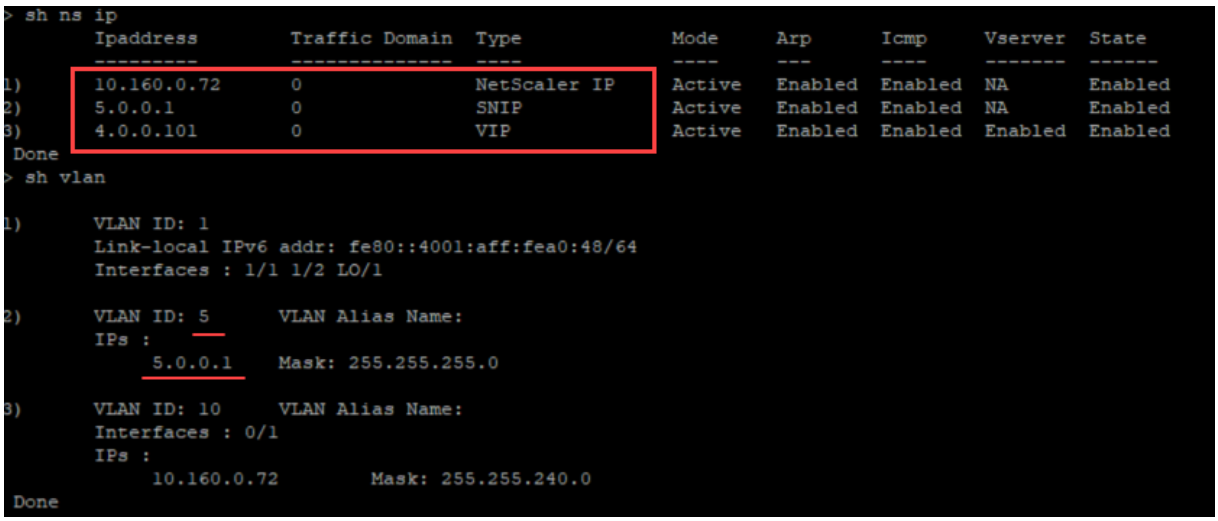
        bind vlan 5 -IPAddress  5.0.0.1  255.255.255.0
        enable ns feature WL SP LB RESPONDER
        add server 5.0.0.201  5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0 -cip
D SABLED -usip
NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
        add lb vserver preboot_v4_101 HTTP  4.0.0.101  80 -persistenceType NONE -cltTimeout 180
    </NS-CONFIG>

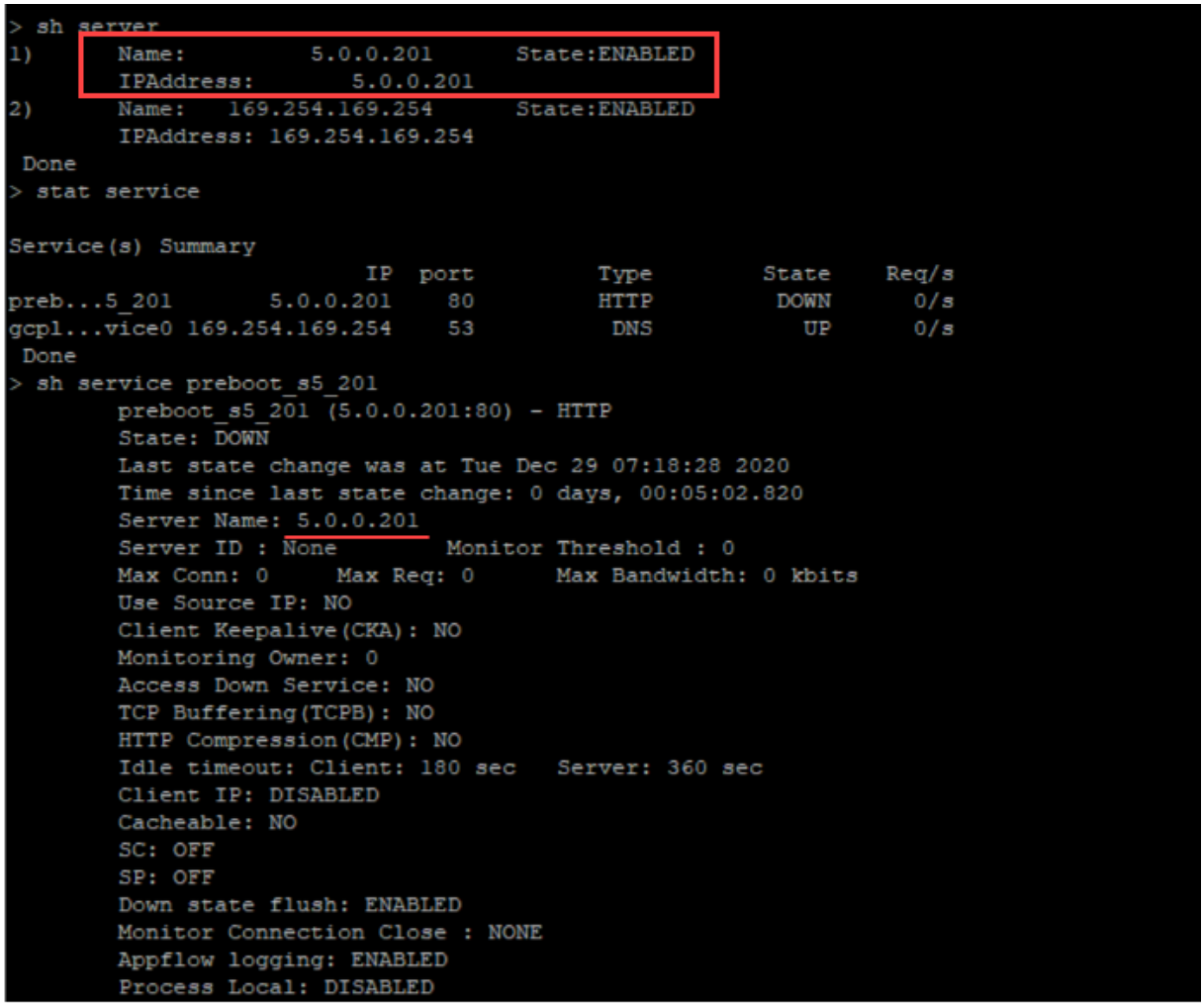
</NS-PRE-BOOT-CONFIG>
```

Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:


```
<NS-PRE-BOOT-CONFIG>
     <NS-CONFIG>
         add vlan 5
         add ns ip 5.0.0.1 255.255.255.0
         bind vlan 5 -IPAddress 5.0.0.1 255.255.255.0
         enable ns feature WL SP LB RESPONDER
         add server 5.0.0.201 5.0.0.201
         add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip
 NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -
    TCPB NO -CMP NO
         add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180
     </NS-CONFIG>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Die Citrix ADC VPX-Instanz enthält die im <NS-CONFIG> Abschnitt angewendete Konfiguration, wie in den folgenden Abbildungen gezeigt.





Benutzer-Skripts

Verwenden Sie das <NS-SCRIPTS> Tag, um jedes Skript bereitzustellen, das in der Citrix ADC VPX-Instanz gespeichert und ausgeführt werden muss.

Sie können viele Skripts in das <NS-SCRIPTS> Tag aufnehmen. Jedes Skript muss in das <SCRIPT> Tag aufgenommen sein.
Jeder <SCRIPT> Abschnitt entspricht einem Skript und enthält alle Details des Skripts unter Verwendung der folgenden Sub-Tags.

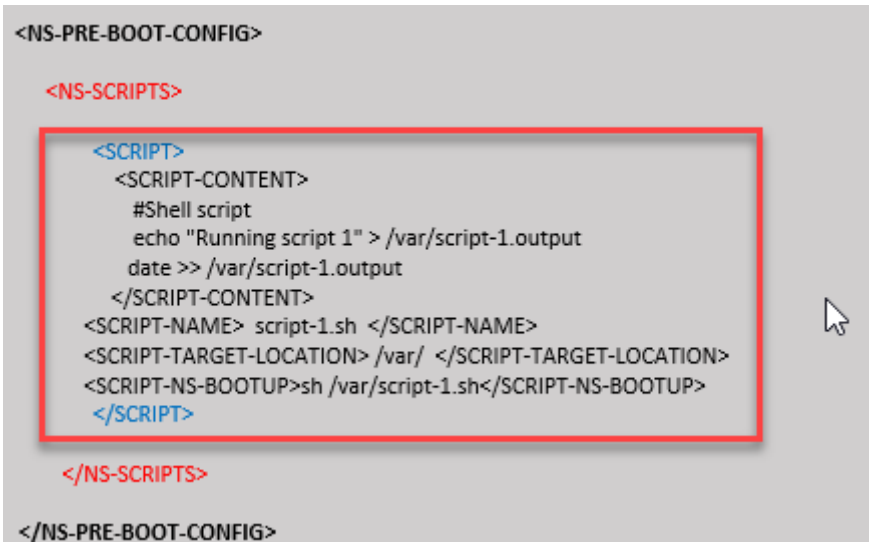
- **<SCRIPT-NAME>:** Gibt den Namen der Skriptdatei an, die gespeichert werden muss.
- **<SCRIPT-CONTENT>:** Gibt den Inhalt der Datei an, die gespeichert werden muss.
- **<SCRIPT-TARGET-LOCATION>:** Gibt den angegebenen Zielspeicherort an, an dem diese Datei gespeichert werden muss. Wenn der Zielspeicherort nicht angegeben wird, wird die Datei oder das Skript standardmäßig im Verzeichnis "/nsconfig" gespeichert.
- **<SCRIPT-NS-BOOTUP>:** Geben Sie die Befehle an, die Sie zum Ausführen des Skripts verwen-

den.

- Wenn Sie den <SCRIPT-NS-BOOTUP> Abschnitt verwenden, werden die im Abschnitt bereitgestellten Befehle in "/nsconfig/nsafter.sh" gespeichert, und die Befehle werden ausgeführt, nachdem die Paket-Engine im Rahmen der Ausführung "nsafter.sh" hochgefahren ist.
- Wenn Sie den <SCRIPT-NS-BOOTUP> Abschnitt nicht verwenden, wird die Skriptdatei an dem von Ihnen angegebenen Zielspeicherort gespeichert.

Beispiel 1:

In diesem Beispiel enthält das <NS-SCRIPTS> Tag Details zu nur einem Skript: script-1.sh. Das Skript "script-1.sh" wird im Verzeichnis "/var" gespeichert. Das Skript wird mit dem angegebenen Inhalt gefüllt und nach dem Hochfahren der Paket-Engine mit dem Befehl "sh /var/script-1.sh" ausgeführt.



Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:

```
<NS-PRE-BOOT-CONFIG>
    <NS-SCRIPTS>
    <SCRIPT>
            <SCRIPT-CONTENT>
                #Shell script
                echo ”Running script 1” > /var/script-1.output
                date >> /var/script-1.output
            </SCRIPT-CONTENT>

                <SCRIPT-NAME> script-1.sh </SCRIPT-NAME>
                <SCRIPT-TARGET-LOCATION> /var/ </SCRIPT-TARGET-LOCATION
                    >
                <SCRIPT-NS-BOOTUP>sh /var/script-1.sh</SCRIPT-NS-BOOTUP
```



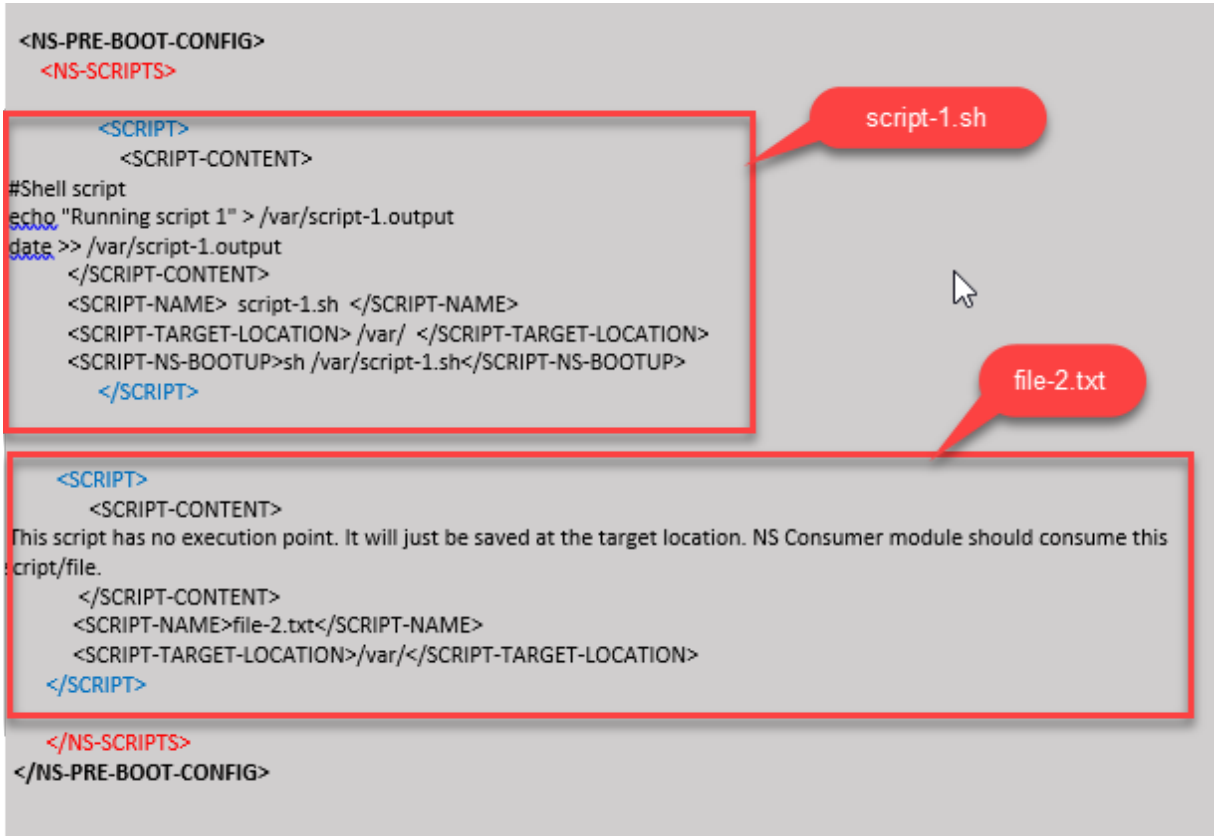
```
                        >
13          </SCRIPT>
14      </NS-SCRIPTS>
15  </NS-PRE-BOOT-CONFIG>
16  <!--NeedCopy-->
```

Im folgenden Snapshot können Sie überprüfen, ob das Skript “script-1.sh” im Verzeichnis “/var/” gespeichert ist. Das Skript “Script-1.sh” wird ausgeführt und die Ausgabedatei wird entsprechend erstellt.

Beispiel 2:

Im folgenden Beispiel enthält das <NS-SCRIPTS> Tag Details zu zwei Skripten.

- Das erste Skript wird als “script-1.sh” im Verzeichnis “/var” gespeichert. Das Skript wird mit dem angegebenen Inhalt gefüllt und nach dem Hochfahren der Paket-Engine mit dem Befehl “sh /var/script-1.sh” ausgeführt.
- Das zweite Skript wird als “file-2.txt” im Verzeichnis “/var” gespeichert. Diese Datei wird mit dem angegebenen Inhalt gefüllt. Es wird jedoch nicht ausgeführt, da der Bootup-Ausführungsbefehl nicht bereitgestellt <SCRIPT-NS-BOOTUP> wird.



Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:

```
<NS-PRE-BOOT-CONFIG>
    <NS-SCRIPTS>
        <SCRIPT>
            <SCRIPT-CONTENT>
               #Shell script
               echo ”Running script 1” > /var/script-1.output
               date >> /var/script-1.output
            </SCRIPT-CONTENT>

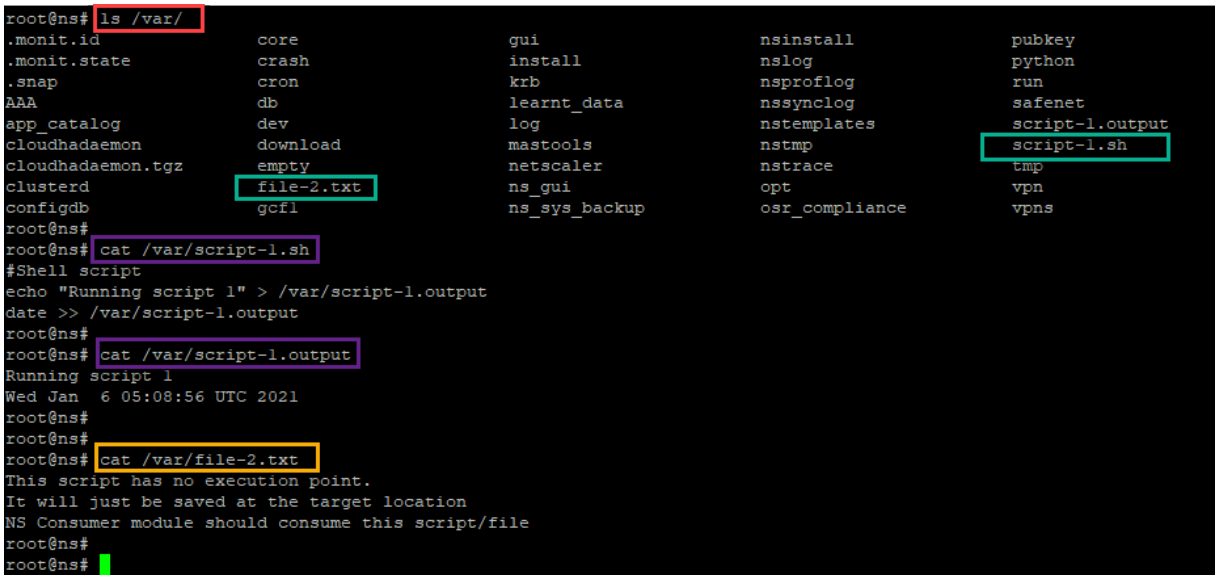
            <SCRIPT-NAME>  script-1.sh  </SCRIPT-NAME>
            <SCRIPT-TARGET-LOCATION> /var/  </SCRIPT-TARGET-LOCATION>
            <SCRIPT-NS-BOOTUP>sh /var/script-1.sh</SCRIPT-NS-BOOTUP>
            </SCRIPT>

        <SCRIPT>
            <SCRIPT-CONTENT>
                This script has no execution point.
                It will just be saved at the target location
                NS Consumer module should consume this script/file
```



```
            </SCRIPT-CONTENT>
            <SCRIPT-NAME>file-2.txt</SCRIPT-NAME>
            <SCRIPT-TARGET-LOCATION>/var/</SCRIPT-TARGET-LOCATION>
        </SCRIPT>
    </NS-SCRIPTS>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Im folgenden Snapshot können Sie überprüfen, ob script-1.sh und file-2.txt im Verzeichnis "/var/" erstellt wurden. Die Script-1.sh wird ausgeführt und die Ausgabedatei wird entsprechend erstellt.



Lizenzierung

Verwenden Sie das <NS-LICENSE-CONFIG> Tag, um die gepoolte Citrix ADC-Lizenzierung anzuwenden, während Sie die VPX-Instanz hochfahren. Verwenden Sie das <LICENSE-COMMANDS> Tag im <NS-LICENSE-CONFIG> Abschnitt, um die gepoolten Lizenzbefehle bereitzustellen. Diese Befehle müssen syntaktisch gültig sein.

Sie können die gepoolten Lizenzierungsdetails wie Lizenztyp, Kapazität und Lizenzserver im <LICENSE-COMMANDS> Abschnitt mit den standardmäßigen gepoolten Lizenzbefehlen angeben. Weitere Informationen finden Sie unter Konfigurieren der Lizenzierung der gepoolten Kapazität von Citrix ADC.

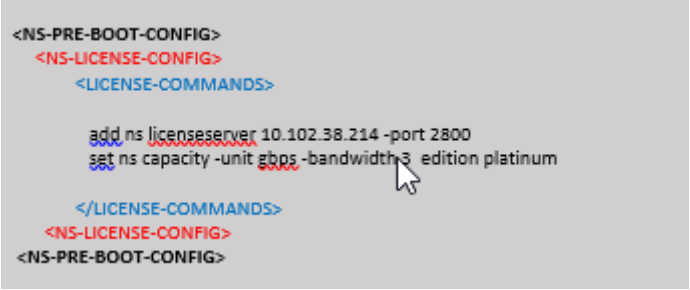
Nach dem <NS-LICENSE-CONFIG>Anwenden des wird der VPX beim Booten mit der angeforderten Edition geliefert, und VPX versucht, die konfigurierten Lizenzen vom Lizenzserver auszuchecken.

- Wenn das Auschecken der Lizenz erfolgreich ist, wird die konfigurierte Bandbreite auf VPX angewendet.

- Wenn das Auschecken der Lizenz fehlschlägt, wird die Lizenz nicht innerhalb von 10 bis 12 Minuten vom Lizenzserver abgerufen. Infolgedessen wird das System neu gestartet und wechselt in einen nicht lizenzierten Zustand.

Beispiel:

Im folgenden Beispiel wird der VPX nach dem <NS-LICENSE-CONFIG>Anwenden des beim Booten die Premium Edition bereitgestellt, und VPX versucht, die konfigurierten Lizenzen vom Lizenzserver auszuchecken (10.102.38.214).



Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:

```
<NS-PRE-BOOT-CONFIG>
   <NS-LICENSE-CONFIG>
        <LICENSE-COMMANDS>
            add ns licenseserver 10.102.38.214 -port 2800
            set ns capacity -unit gbps -bandwidth 3  edition platinum
        </LICENSE-COMMANDS>
    </NS-LICENSE-CONFIG>
</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Wie in der folgenden Abbildung gezeigt, können Sie den Befehl “Lizenzserver anzeigen” ausführen und überprüfen, ob der Lizenzserver (10.102.38.214) dem VPX hinzugefügt wird.

Bootstrapping

Verwenden Sie das <NS-BOOTSTRAP> Tag, um die benutzerdefinierten Bootstrapping-Informationen bereitzustellen. Sie können die <NEW-BOOTSTRAP-SEQUENCE> Tags <SKIP-DEFAULT-BOOTSTRAP > und innerhalb des <NS-BOOTSTRAP> Abschnitts verwenden. In diesem Abschnitt wird Citrix ADC

Appliance darüber informiert, ob der Standard-Bootstrap vermieden werden soll oder nicht. Wenn das Standard-Bootstrapping vermieden wird, bietet Ihnen dieser Abschnitt die Möglichkeit, eine neue Bootstrapping-Sequenz bereitzustellen.

Standardmäßige Bootstrap-Konfiguration

Die Standard-Bootstrap-Konfiguration in der Citrix ADC Appliance folgt diesen Schnittstellenzuweisungen:

- **Eth0** - Verwaltungsschnittstelle mit einer bestimmten NSIP-Adresse.
- **Eth1** - Clientorientierte Schnittstelle mit einer bestimmten VIP-Adresse.
- **Eth2** - Server-Schnittstelle mit einer bestimmten SNIP-Adresse.

Anpassen der Bootstrap-Konfiguration

Sie können die standardmäßige Bootstrap-Sequenz überspringen und eine neue Bootstrap-Sequenz für die Citrix ADC VPX-Instanz bereitstellen. Verwenden Sie das <NS-BOOTSTRAP> Tag, um die benutzerdefinierten Bootstrapping-Informationen bereitzustellen. Sie können beispielsweise das Standard-Bootstrapping ändern, bei dem die Verwaltungsschnittstelle (NSIP), die clientseitige Schnittstelle (VIP) und die Serverschnittstelle (SNIP) immer in einer bestimmten Reihenfolge bereitgestellt werden.

Die folgende Tabelle zeigt das Bootstrapping-Verhalten mit den verschiedenen zulässigen Werten <SKIP-DEFAULT-BOOTSTRAP> und <NEW-BOOTSTRAP-SEQUENCE> Tags an.

SKIP-DEFAULT-BOOTSTRAP	NEW-BOOTSTRAP-SEQUENCE	Bootstrap-Verhalten
JA	JA	Das standardmäßige Bootstrapping-Verhalten wird übersprungen, und eine neue benutzerdefinierte Bootstrap-Sequenz im <NS-BOOTSTRAP> Abschnitt wird ausgeführt.
JA	NEIN	Das standardmäßige Bootstrapping-Verhalten wird übersprungen, die im <NS-CONFIG> Abschnitt bereitgestellten Bootstrap-Befehle werden ausgeführt.

Sie können die Bootstrap-Konfiguration mit den folgenden drei Methoden anpassen:

- Geben Sie nur die Schnittstellendetails
- Geben Sie die Schnittstellendetails zusammen mit IP-Adressen und Subnetzmaske an
- Geben Sie Bootstrap-bezogene Befehle im <NS-CONFIG> Abschnitt

Methode 1: Benutzerdefinierter Bootstrap durch Angabe nur der Schnittstellendetails

Sie geben die verwaltungs-, clientorientierten und serverorientierten Schnittstellen an, nicht jedoch deren IP-Adressen und Subnetzmasken. Die IP-Adressen und Subnetzmasken werden durch Abfragen der Cloud-Infrastruktur ausgefüllt.

Benutzerdefiniertes Bootstrap-Beispiel für AWS

Sie geben die benutzerdefinierte Bootstrap-Sequenz an, wie im folgenden Beispiel gezeigt. Weitere Informationen finden Sie unter So stellen Sie Preboot-Benutzerdaten in Cloud-Instanzbereit. Eth1-Schnittstelle wird als Verwaltungsschnittstelle (NSIP), Eth0-Schnittstelle als Client-Schnittstelle (VIP) und Eth2-Schnittstelle als Serverschnittstelle (SNIP) zugewiesen. Der <NS-BOOTSTRAP> Abschnitt enthält nur die Schnittstellendetails und nicht die Details von IP-Adressen und Subnetzmasken.

```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

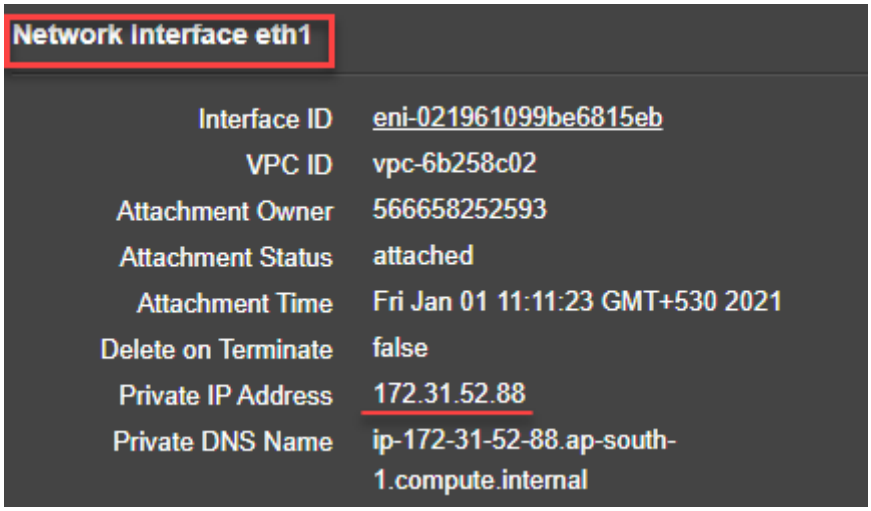
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

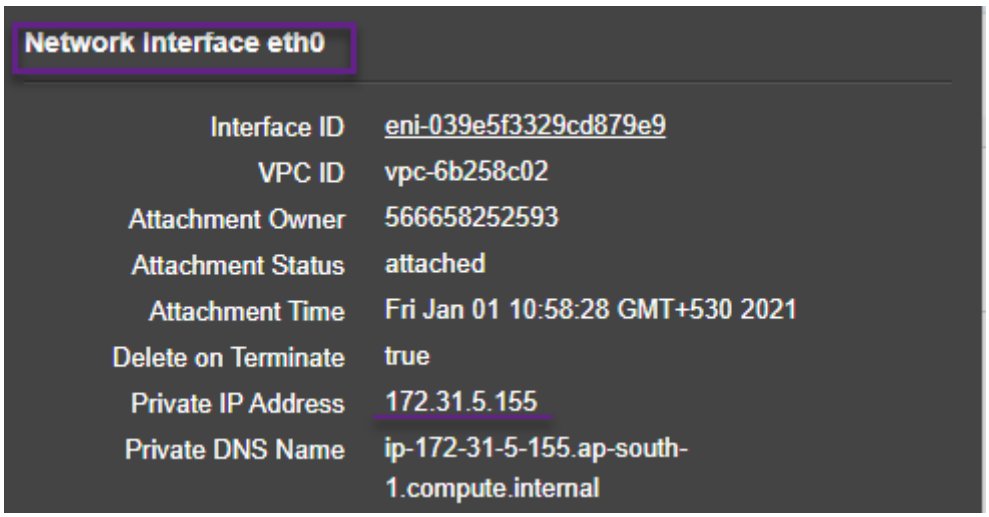
        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

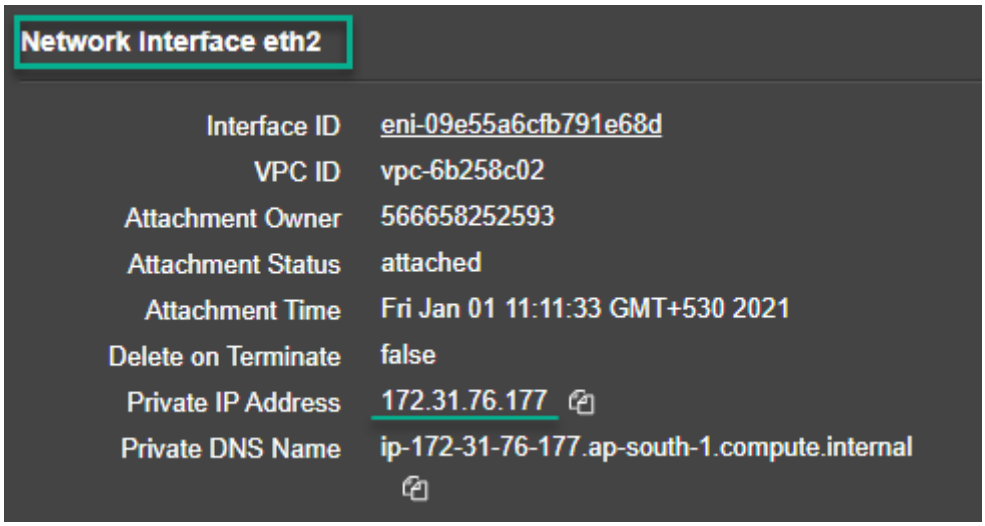
    </NS-BOOT STRAP>
</NS-PRE-BOOT-CONFIG>
```

Nachdem die VM-Instanz erstellt wurde, können Sie im AWS-Portal die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

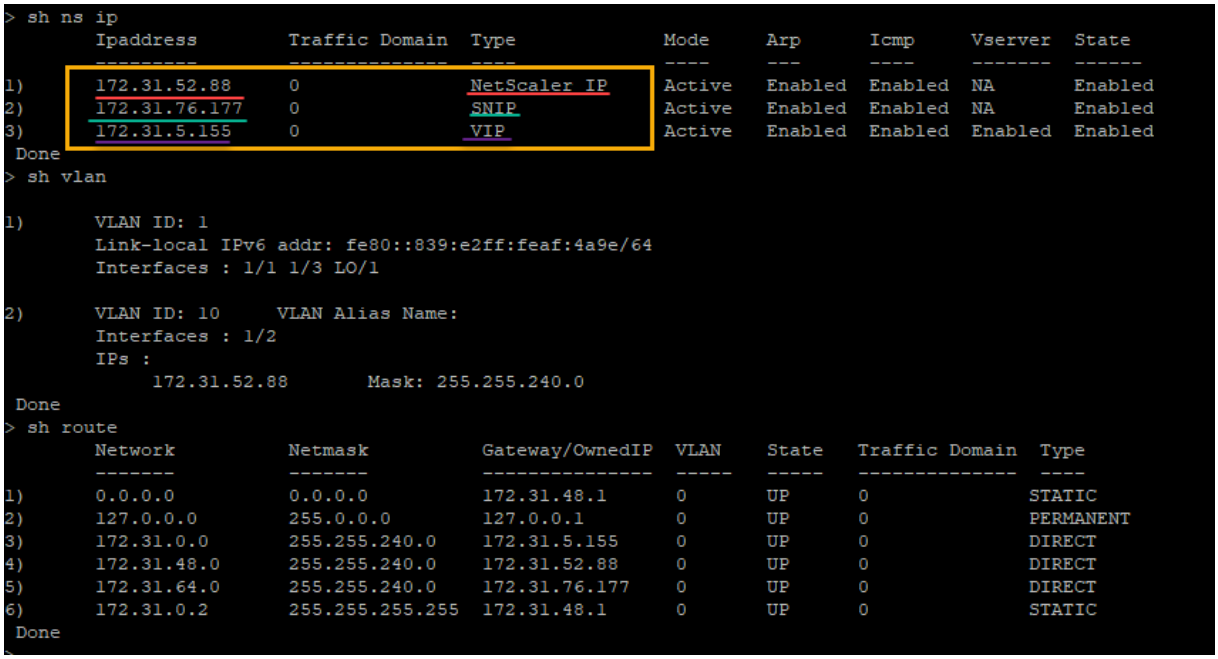
1. Navigieren Sie zum **AWS Portal > EC2-Instanzen**und wählen Sie die Instanz aus, die Sie erstellt haben, indem Sie die benutzerdefinierten Bootstrap-Informationen angeben.
2. Auf der Registerkarte **Beschreibung** können Sie die Eigenschaften jeder Netzwerkschnittstelle überprüfen, wie in den folgenden Abbildungen gezeigt.







Sie können den `show nsip` Befehl in **ADC CLI**ausführen und die Netzwerkschnittstellen überprüfen, die beim ersten Start der ADC-Appliance auf die ADC VPX-Instanz angewendet wurden.



```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.31.52.88     0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.31.76.177    0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      172.31.5.155     0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
        Interfaces : 1/1 1/3 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.31.52.88       Mask: 255.255.240.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.31.48.1      0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.31.0.0       255.255.240.0    172.31.5.155     0       UP      0               DIRECT
4)      172.31.48.0      255.255.240.0    172.31.52.88     0       UP      0               DIRECT
5)      172.31.64.0      255.255.240.0    172.31.76.177    0       UP      0               DIRECT
6)      172.31.0.2       255.255.255.255  172.31.48.1      0       UP      0               STATIC
 Done
```

Benutzerdefiniertes Bootstrap-Beispiel für Azure

Sie geben die benutzerdefinierte Bootstrap-Sequenz an, wie im folgenden Beispiel gezeigt. Weitere Informationen finden Sie unter So stellen Sie Preboot-Benutzerdaten in Cloud-Instanzbereit. Die Eth2-Schnittstelle wird als Verwaltungsschnittstelle (NSIP), Eth1-Schnittstelle als Client-Schnittstelle (VIP) und Eth0-Schnittstelle als Serverschnittstelle (SNIP) zugewiesen. Der <NS-BOOTSTRAP> Abschnitt enthält nur die Schnittstellendetails und nicht die Details von IP-Adressen und Subnetzmasken.


```
<NS-PRE-BOOT-CONFIG>

    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

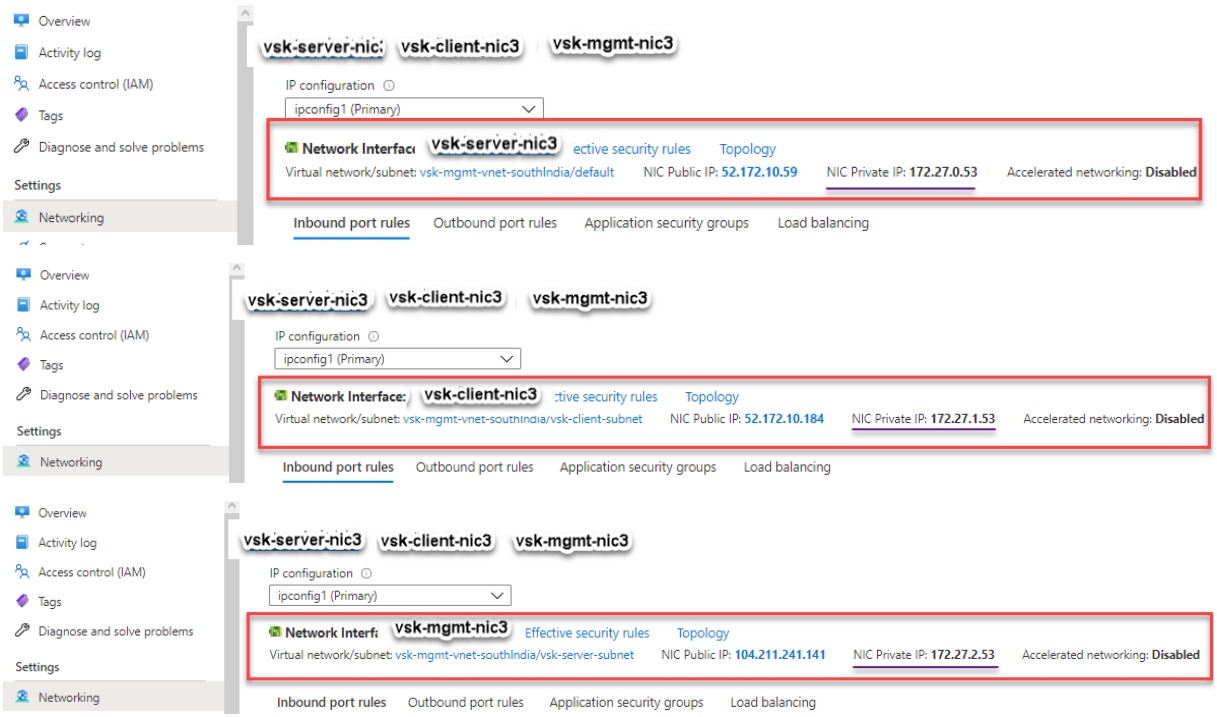
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOTSTRAP>

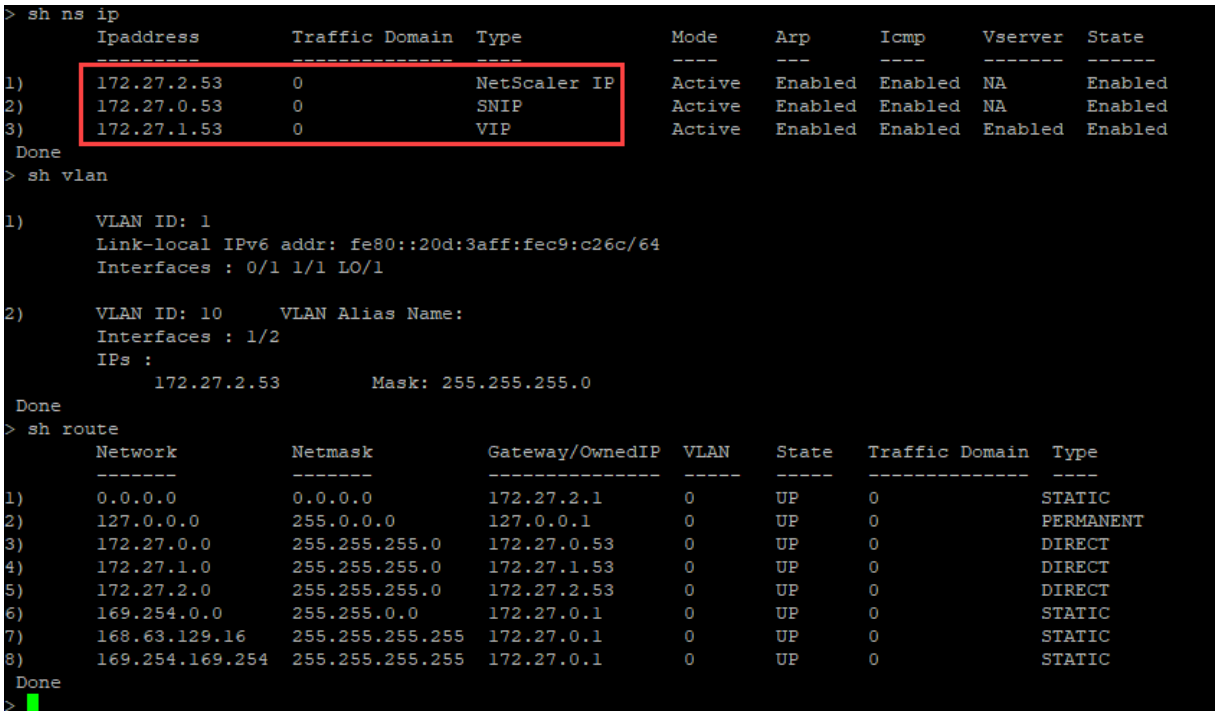
</NS-PRE-BOOT-CONFIG>
```

Sie können sehen, dass die Citrix ADC VPX-Instanz mit drei Netzwerkschnittstellen erstellt wurde. Navigieren Sie zum **Azure-Portal > VM-Instanz > Netzwerk**, und überprüfen Sie die Netzwerkeigenschaften der drei Netzwerkkarten wie in den folgenden Abbildungen gezeigt.



Sie können den Befehl “show nsip” in der ADC CLI ausführen und überprüfen, ob die im <NS-

BOOTSTRAP> Abschnitt angegebene neue Bootstrap-Sequenz angewendet wird. Sie können den Befehl “Route anzeigen” ausführen, um die Subnetzmaske zu überprüfen.



Benutzerdefinierte Bootstrap-Beispiele für GCP

Sie geben die benutzerdefinierte Bootstrap-Sequenz an, wie im folgenden Beispiel gezeigt. Weitere Informationen finden Sie unter So stellen Sie Preboot-Benutzerdaten in Cloud-Instanzbereit. Eth1-Schnittstelle wird als Verwaltungsschnittstelle (NSIP), Eth0-Schnittstelle als Client-Schnittstelle (VIP) und Eth2-Schnittstelle als Serverschnittstelle (SNIP) zugewiesen. Der <NS-BOOTSTRAP> Abschnitt enthält nur die Schnittstellendetails und nicht die Details von IP-Adressen und Subnetzmasken.


```
<NS-PRE-BOOT-CONFIG>
    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
        </MGMT-INTERFACE-CONFIG>

        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
        </CLIENT-INTERFACE-CONFIG>

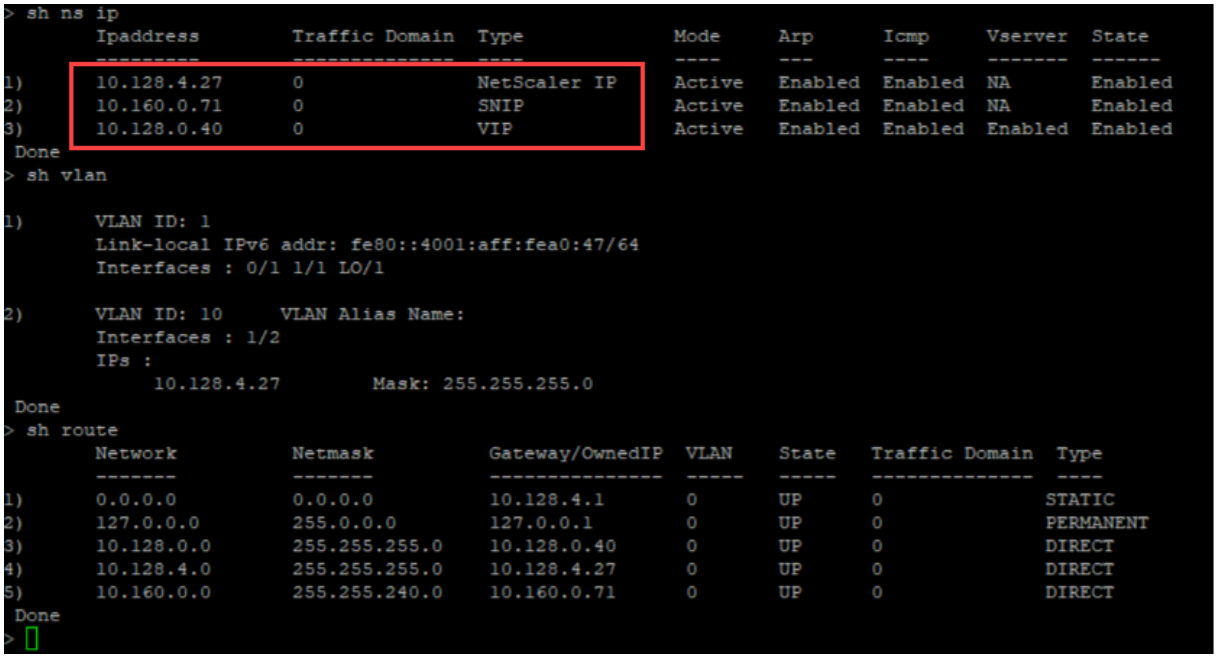
        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOT STRAP>
</NS-PRE-BOOT-CONFIG>
```

Nachdem die VM-Instanz im GCP-Portal erstellt wurde, können Sie die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

1. Wählen Sie die Instanz aus, die Sie erstellt haben, indem Sie die benutzerdefinierten Bootstrap-Informationen angeben.
2. Navigieren Sie zu den Eigenschaften der Netzwerkschnittstelle und überprüfen Sie die NIC-Details wie folgt:

Sie können den `show nsip` Befehl in **ADC CLI**ausführen und die Netzwerkschnittstellen überprüfen, die beim ersten Start der ADC-Appliance auf die ADC VPX-Instanz angewendet wurden.



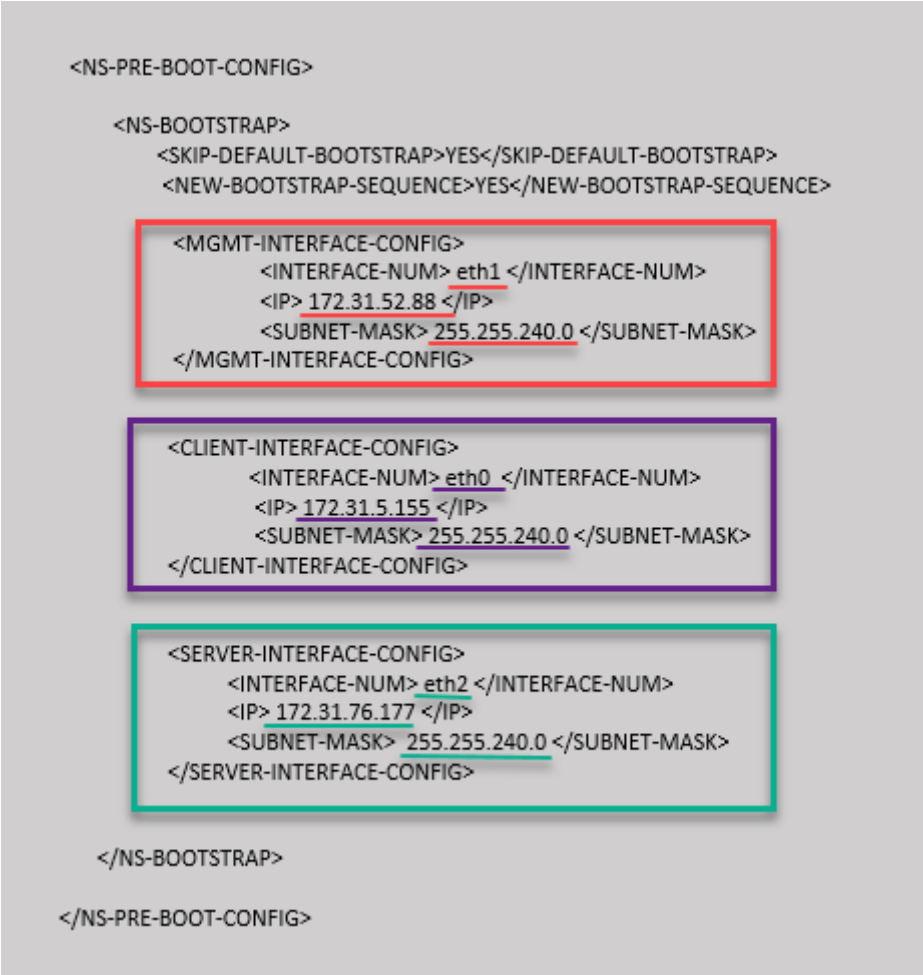
Methode 2: Benutzerdefiniertes Bootstrap durch Angabe der Schnittstellen, IP-Adressen und Subnetzmasken

Sie geben die verwaltungs-, clientorientierten und serverorientierten Schnittstellen zusammen mit ihren IP-Adressen und der Subnetzmaske an.

Benutzerdefinierte Bootstrap-Beispiele für AWS

Im folgenden Beispiel überspringen Sie den Standard-Bootstrap und führen eine neue Bootstrap-Sequenz für die Citrix ADC Appliance aus. Für die neue Bootstrap-Sequenz geben Sie folgende Details an:

- **Verwaltungsschnittstelle:** Interface - Eth1, NSIP - 172.31.52.88 und Subnetzmaske - 255.255.240.0
- **Clientorientierte Schnittstelle:** Schnittstelle - Eth0, VIP - 172.31.5.155 und Subnetzmaske - 255.255.240.0.
- **Server-zugewandte Schnittstelle:** Schnittstelle - Eth2, SNIP - 172.31.76.177 und Subnetzmaske - 255.255.240.0.



Sie können den `show nsip` Befehl in der ADC CLI ausführen und überprüfen, ob die im `<NS-BOOTSTRAP>` Abschnitt angegebene neue Bootstrap-Sequenz angewendet wird. Sie können den Befehl “Route anzeigen” ausführen, um die Subnetzmaske zu überprüfen.


```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.31.52.88     0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.31.76.177    0               SNIP             Passive  Enabled  Enabled  NA       Enabled
3)      172.31.5.155     0               VIP              Passive  Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
        Interfaces : 1/1 1/3 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.31.52.88       Mask: 255.255.240.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.31.48.1      0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.31.0.0       255.255.240.0    172.31.5.155     0       UP      0               DIRECT
4)      172.31.48.0      255.255.240.0    172.31.52.88     0       UP      0               DIRECT
5)      172.31.64.0      255.255.240.0    172.31.76.177    0       UP      0               DIRECT
6)      172.31.0.2       255.255.255.255  172.31.48.1      0       UP      0               STATIC
 Done
>
```

Benutzerdefiniertes Bootstrap-Beispiel für Azure

Im folgenden Beispiel wird eine neue Bootstrap-Sequenz für ADC erwähnt und der Standard-Bootstrap wird übersprungen. Sie geben die Schnittstellendetails zusammen mit den IP-Adressen und Subnetzmasken wie folgt an:

- Verwaltungsschnittstelle (eth2), NSIP (172.27.2.53) und Subnetzmaske (255.255.255.0)
- Clientorientierte Schnittstelle (eth1), VIP (172.27.1.53) und Subnetzmaske (255.255.255.0)
- Server-zugewandte Schnittstelle (eth0), SNIP (172.27.0.53) und Subnetzmaske (255.255.255.0)


```
<NS-PRE-BOOT-CONFIG>

    <NS-BOOTSTRAP>
        <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
        <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth2 </INTERFACE-NUM>
            <IP> 172.27.2.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>

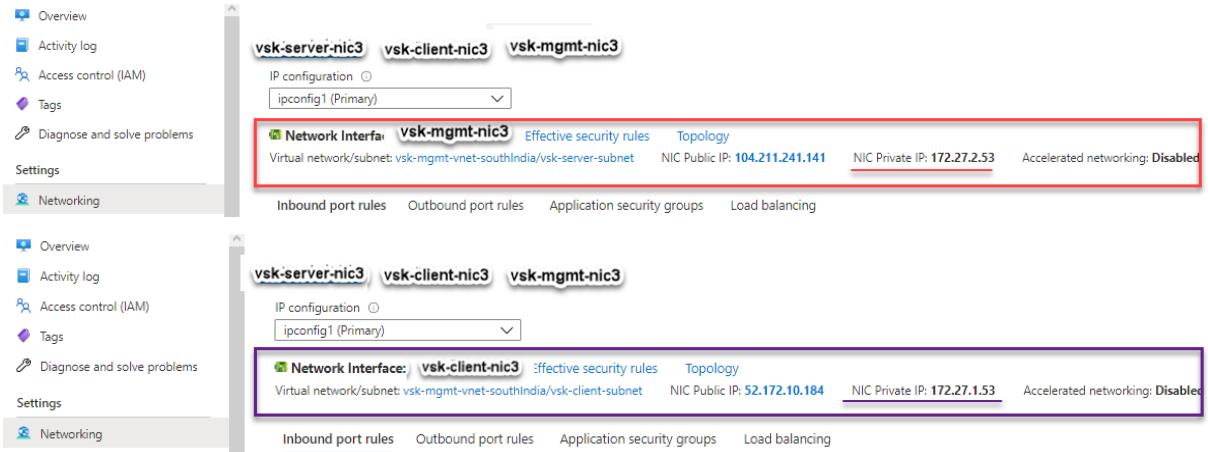
        <CLIENT-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth1 </INTERFACE-NUM>
            <IP> 172.27.1.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
            </CLIENT-INTERFACE-CONFIG>

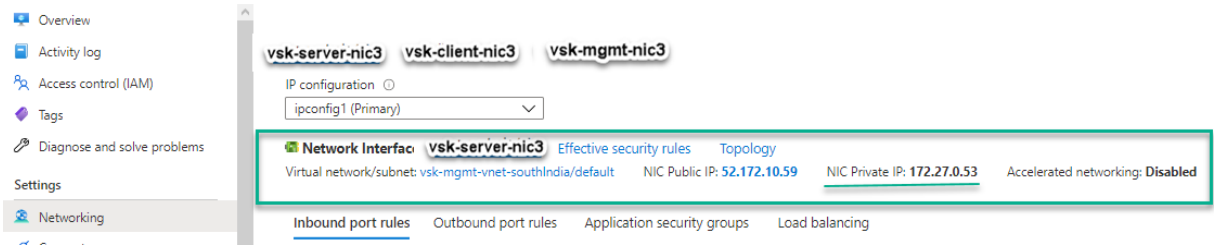
        <SERVER-INTERFACE-CONFIG>
            <INTERFACE-NUM> eth0 </INTERFACE-NUM>
            <IP> 172.27.0.53 </IP>
            <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </SERVER-INTERFACE-CONFIG>

    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
```

Sie können sehen, dass die Citrix ADC VPX-Instanz mit drei Netzwerkschnittstellen erstellt wurde. Navigieren Sie zum **Azure-Portal > VM-Instanz > Netzwerk**, und überprüfen Sie die Netzwerkeigenschaften der drei Netzwerkkarten wie in den folgenden Abbildungen gezeigt.





Sie können den `show nsip` Befehl in der ADC CLI ausführen und überprüfen, ob die im <NS-BOOTSTRAP> Abschnitt angegebene neue Bootstrap-Sequenz angewendet wird. Sie können den Befehl "Route anzeigen" ausführen, um die Subnetzmaske zu überprüfen.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.27.2.53      0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.27.0.53      0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      172.27.1.53      0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::20d:3aff:fec9:c26c/64
        Interfaces : 0/1 1/1 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.27.2.53        Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.27.2.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.27.0.0       255.255.255.0    172.27.0.53      0       UP      0               DIRECT
4)      172.27.1.0       255.255.255.0    172.27.1.53      0       UP      0               DIRECT
5)      172.27.2.0       255.255.255.0    172.27.2.53      0       UP      0               DIRECT
6)      169.254.0.0      255.255.0.0      172.27.0.1       0       UP      0               STATIC
7)      168.63.129.16    255.255.255.255  172.27.0.1       0       UP      0               STATIC
8)      169.254.169.254  255.255.255.255  172.27.0.1       0       UP      0               STATIC
 Done
```

Benutzerdefiniertes Bootstrap-Beispiel für GCP

Im folgenden Beispiel wird eine neue Bootstrap-Sequenz für ADC erwähnt und der Standard-Bootstrap wird übersprungen. Sie geben die Schnittstellendetails zusammen mit den IP-Adressen und Subnetzmasken wie folgt an:

- Verwaltungsschnittstelle (eth2), NSIP (10.128.4.31) und Subnetzmaske (255.255.255.0)
- Clientorientierte Schnittstelle (eth1), VIP (10.128.0.43) und Subnetzmaske (255.255.255.0)
- Server-zugewandte Schnittstelle (eth0), SNIP (10.160.0.75) und Subnetzmaske (255.255.255.0)


```
<NS-PRE-BOOT-CONFIG>
   <NS-BOOTSTRAP>
         <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
         <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>
          <MGMT-INTERFACE-CONFIG>
               <INTERFACE-NUM> eth2 </INTERFACE-NUM>
               <IP> 10.128.4.31 </IP>
               <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
           </MGMT-INTERFACE-CONFIG>
          <CLIENT-INTERFACE-CONFIG>
               <INTERFACE-NUM> eth1 </INTERFACE-NUM>
               <IP> 10.128.0.43 </IP>
               <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
          </CLIENT-INTERFACE-CONFIG>
          <SERVER-INTERFACE-CONFIG>
               <INTERFACE-NUM> eth0 </INTERFACE-NUM>
               <IP> 10.160.0.75 </IP>
               <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
          </SERVER-INTERFACE-CONFIG>
   </NS-BOOTSTRAP>
</NS-PRE-BOOT-CONFIG>
```

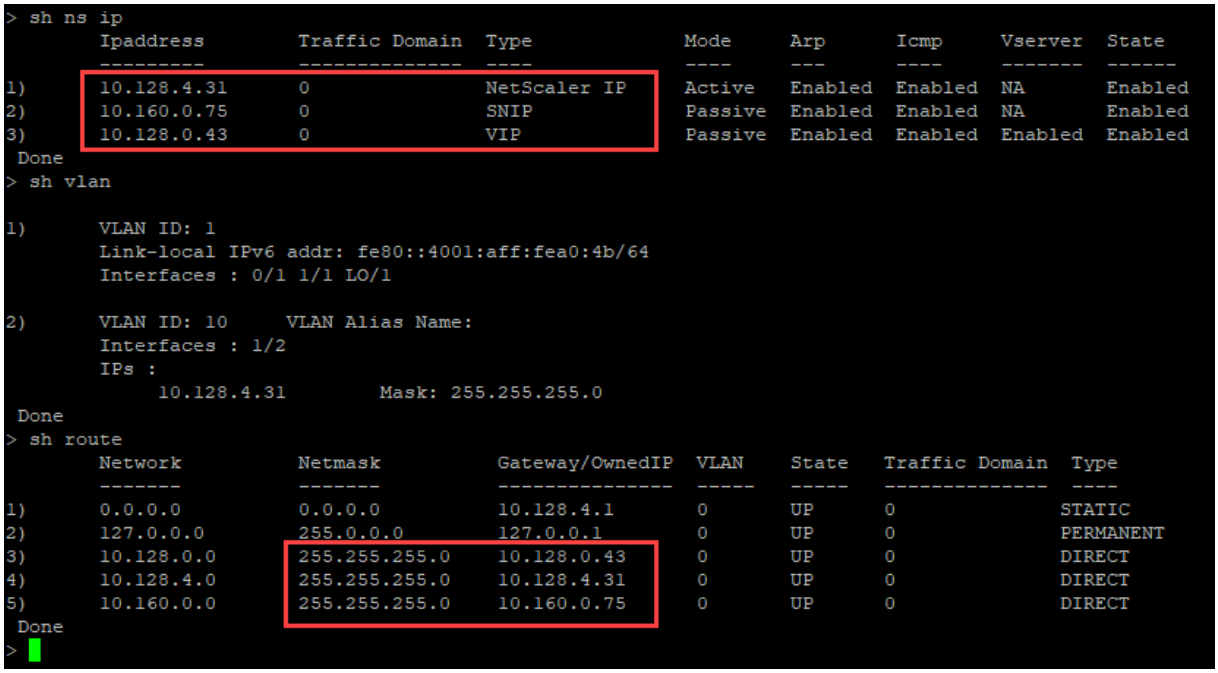
Nachdem die VM-Instanz im GCP-Portal mit dem benutzerdefinierten Bootstrap erstellt wurde, können Sie die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

1. Wählen Sie die Instanz aus, die Sie erstellt haben, indem Sie die benutzerdefinierten Bootstrap-Informationen angeben.
2. Navigieren Sie zu den Eigenschaften der Netzwerkschnittstelle und überprüfen Sie die Netzwerkdetails wie folgt.

Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	default	default	vsk-defnw-st-ip1 (10.160.0.75)	–	34.93.216.90 (ephemeral)	Premium	Off	View details
nic1	vsk-vpc-network-1	asia-south1-subnet-1	vsk-vpc-nw1-st-ip1 (10.128.0.43)	–	35.244.40.113 (ephemeral)	Premium		View details
nic2	vsk-vpc-network-2	asia-south1-subnet-5	vsk-nw2-st-ip-1 (10.128.4.31)	–	34.93.202.214 (ephemeral)	Premium		View details

Sie können den `show nsip` Befehl in der ADC CLI ausführen und überprüfen, ob die im <NS-BOOTSTRAP> Abschnitt angegebene neue Bootstrap-Sequenz angewendet wird. Sie können den Befehl “Route anzeigen” ausführen, um die Subnetzmaske zu überprüfen.



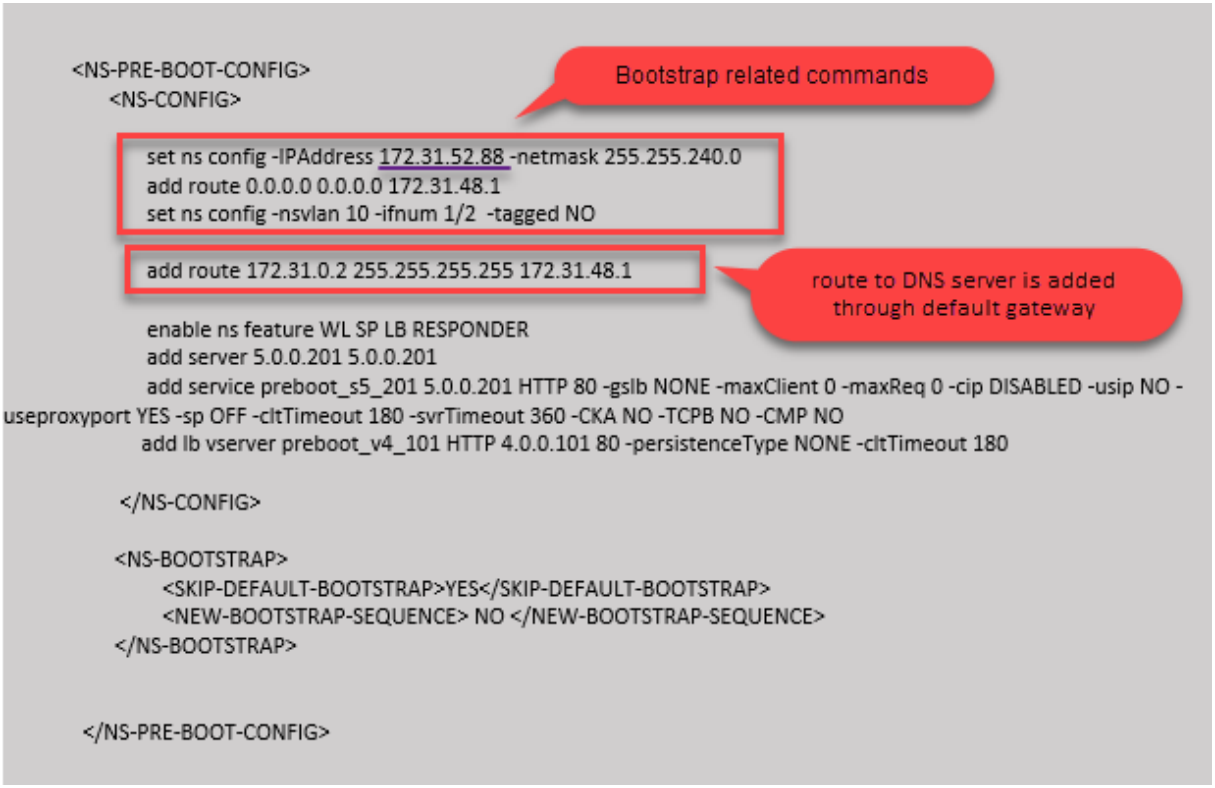
Methode 3: Benutzerdefiniertes Bootstrap durch Bereitstellung von Bootstrap-bezogenen Befehlen im <NS-CONFIG> Abschnitt

Sie können die Bootstrap-bezogenen Befehle im <NS-CONFIG> Abschnitt angeben. In dem <NS-BOOTSTRAP> Abschnitt müssen Sie das <NEW-BOOTSTRAP-SEQUENCE> als “Nein” angeben, um die Bootstrapping-Befehle im <NS-CONFIG> Abschnitt auszuführen. Sie müssen auch die Befehle angeben, um NSIP, Standardroute und NSVLAN zuzuweisen. Geben Sie außerdem die Befehle ein, die für die von Ihnen verwendete Cloud relevant sind.

Stellen Sie vor der Bereitstellung eines benutzerdefinierten Bootstrap sicher, dass Ihre Cloud-Infrastruktur eine bestimmte Schnittstellenkonfiguration unterstützt.

Benutzerdefiniertes Bootstrap-Beispiel für AWS

In diesem Beispiel werden Bootstrap-bezogene Befehle im <NS-CONFIG> Abschnitt bereitgestellt. Der <NS-BOOTSTRAP> Abschnitt gibt an, dass das Standard-Bootstrapping übersprungen wird und die im <NS-CONFIG> Abschnitt enthaltenen benutzerdefinierten Bootstrap-Informationen ausgeführt werden. Sie müssen auch die Befehle zum Erstellen von NSIP, zum Hinzufügen einer Standardroute und zum Hinzufügen von NSVLAN angeben.



Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:

```
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>

        set ns config -IPAddress 172.31.52.88 -netmask 255.255.240.0
        add route 0.0.0.0 0.0.0.0 172.31.48.1
        set ns config -nsvlan 10 -ifnum 1/2  -tagged NO
        add route 172.31.0.2 255.255.255.255 172.31.48.1

        enable ns feature WL SP LB RESPONDER
        add server 5.0.0.201 5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip NO - useproxyport
            YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO
             -CMP NO
        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180

    </NS-CONFIG>

    <NS-BOOTSTRAP>
```

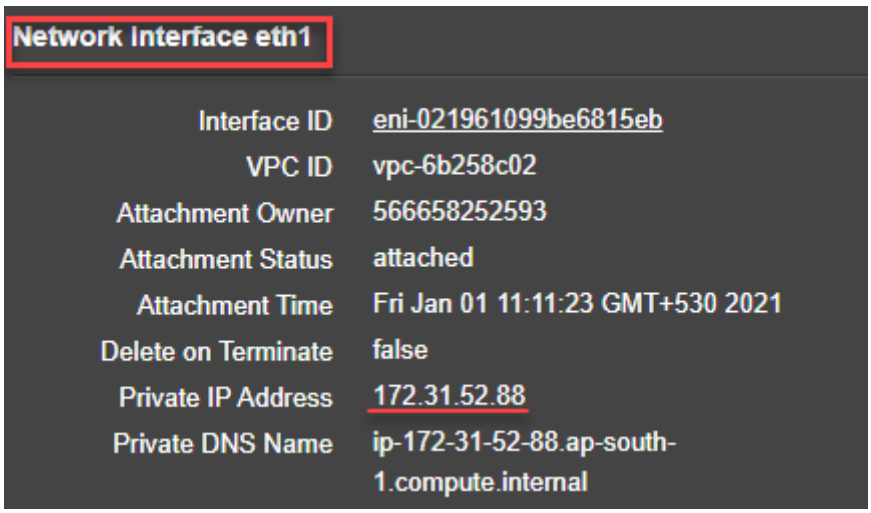


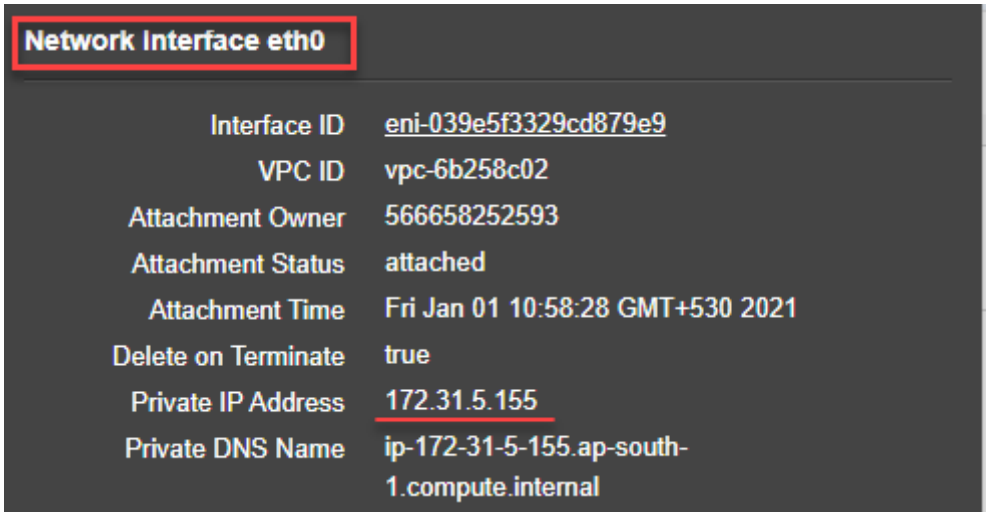
```
      <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
      <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
     </NS-BOOTSTRAP>

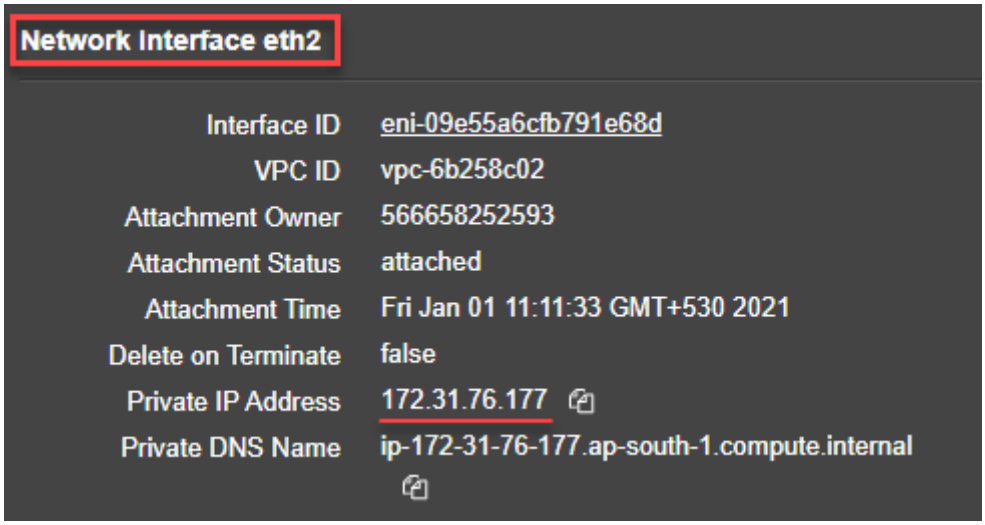

</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Nachdem die VM-Instanz erstellt wurde, können Sie im AWS-Portal die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

1. Navigieren Sie zum **AWS Portal > EC2-Instanzen**und wählen Sie die Instanz aus, die Sie erstellt haben, indem Sie die benutzerdefinierten Bootstrap-Informationen angeben.
2. Auf der Registerkarte **Beschreibung** können Sie die Eigenschaften jeder Netzwerkschnittstelle überprüfen, wie in den folgenden Abbildungen gezeigt.







Sie können den `show nsip` Befehl in **ADC CLI**ausführen und die Netzwerkschnittstellen überprüfen, die beim ersten Start der ADC-Appliance auf die ADC VPX-Instanz angewendet wurden.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.31.52.88     0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::839:e2ff:feaf:4a9e/64
        Interfaces : 1/1 1/3 LO/1

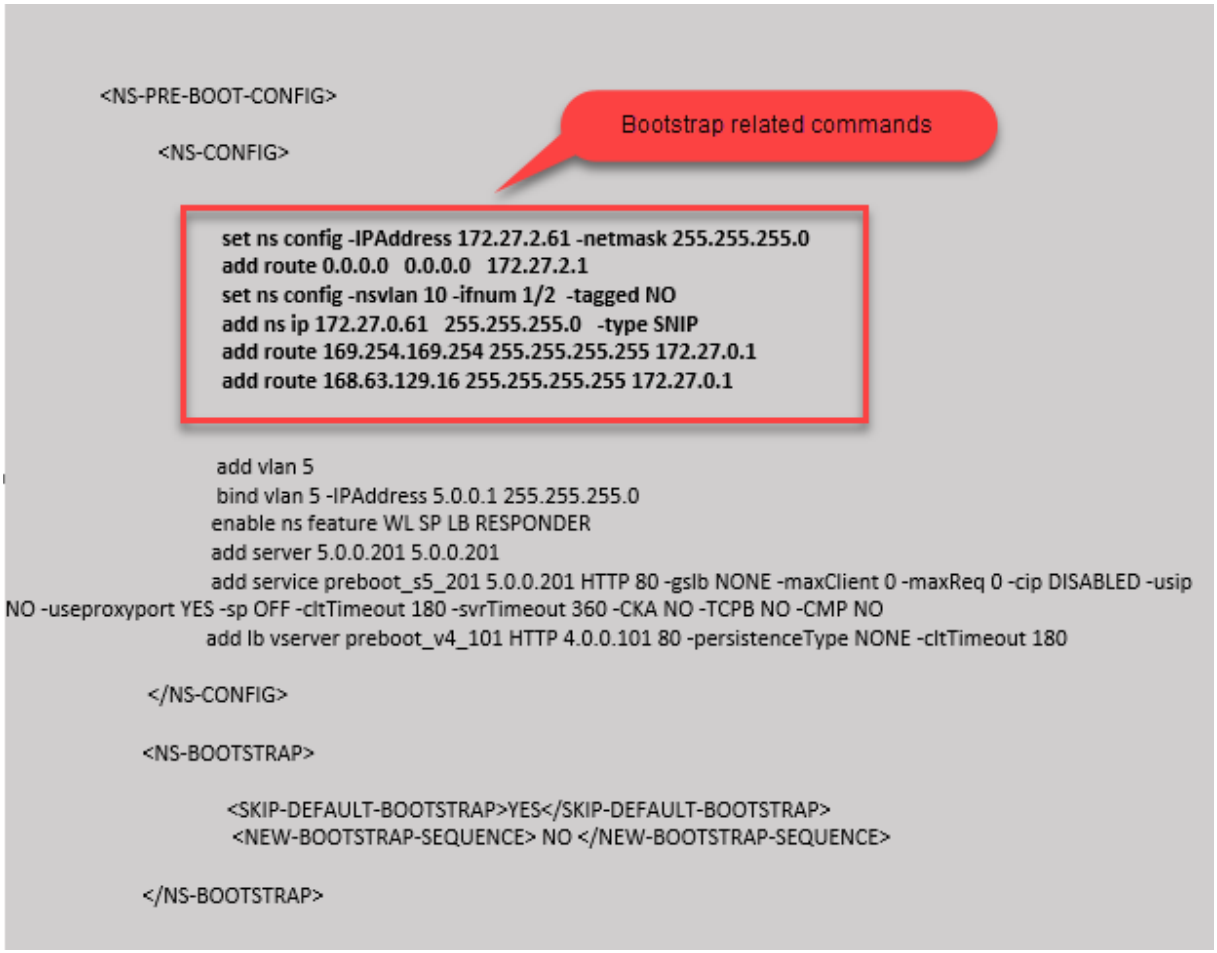
2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.31.52.88       Mask: 255.255.240.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.31.48.1      0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.31.48.0      255.255.240.0    172.31.52.88     0       UP      0               DIRECT
4)      172.31.0.2       255.255.255.255  172.31.48.1      0       UP      0               STATIC
 Done
>
```

Benutzerdefiniertes Bootstrap-Beispiel für Azure

In diesem Beispiel werden Bootstrap-bezogene Befehle im <NS-CONFIG> Abschnitt bereitgestellt. Der <NS-BOOTSTRAP> Abschnitt gibt an, dass das Standard-Bootstrapping übersprungen wird und die im <NS-CONFIG> Abschnitt enthaltenen benutzerdefinierten Bootstrap-Informationen ausgeführt werden.

> Hinweis:
>
> Für Azure Cloud sind Instance Metadata Server (IMDS) und DNS-Server nur über die primäre

> Schnittstelle (Eth0) zugänglich. Wenn die Eth0-Schnittstelle nicht als Verwaltungsschnittstelle (NSIP) verwendet wird, muss die Eth0-Schnittstelle daher zumindest als SNIP für IMDS- oder DNS-Zugriff auf die Arbeit konfiguriert werden. Die Route zum IMDS-Endpunkt (169.254.169.254) und zum DNS-Endpunkt (168.63.129.16) über das Gateway von Eth0 muss ebenfalls hinzugefügt werden.




```
<NS-PRE-BOOT-CONFIG>

   <NS-CONFIG>

        set ns config -IPAddress 172.27.2.61 -netmask 255.255.255.0
        add route 0.0.0.0   0.0.0.0   172.27.2.1
        set ns config -nsvlan 10 -ifnum 1/2  -tagged NO
        add ns ip 172.27.0.61   255.255.255.0   -type SNIP
        add route 169.254.169.254 255.255.255.255 172.27.0.1
        add route 168.63.129.16 255.255.255.255 172.27.0.1

```



```
        add vlan 5
        bind vlan 5 -IPAddress 5.0.0.1 255.255.255.0
        enable ns feature WL SP LB RESPONDER
        add server 5.0.0.201 5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport
            YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO
             -CMP NO
        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180

    </NS-CONFIG>

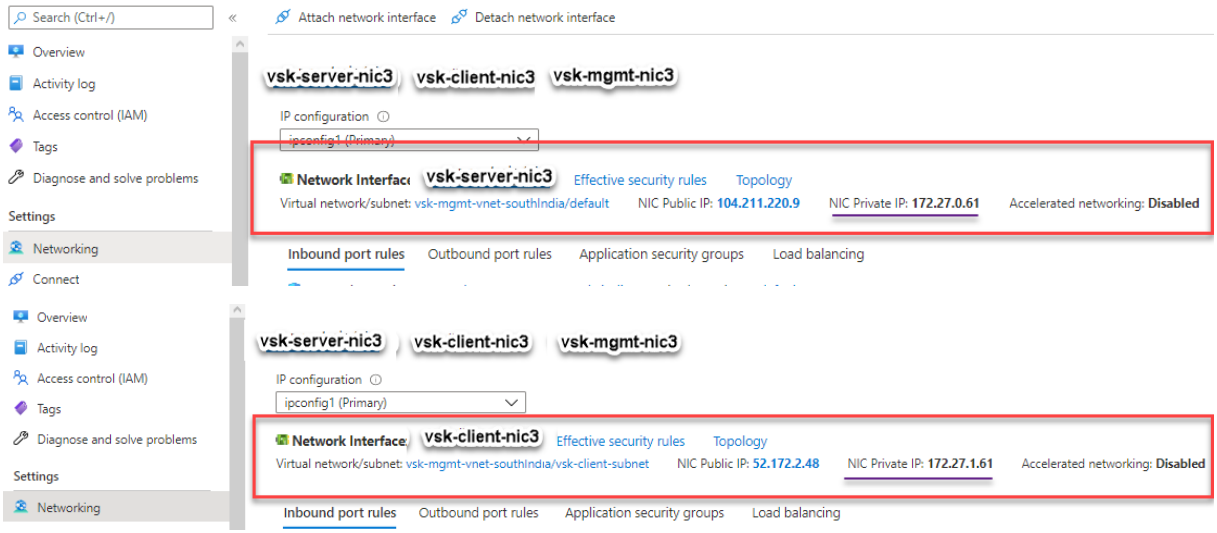
    <NS-BOOTSTRAP>

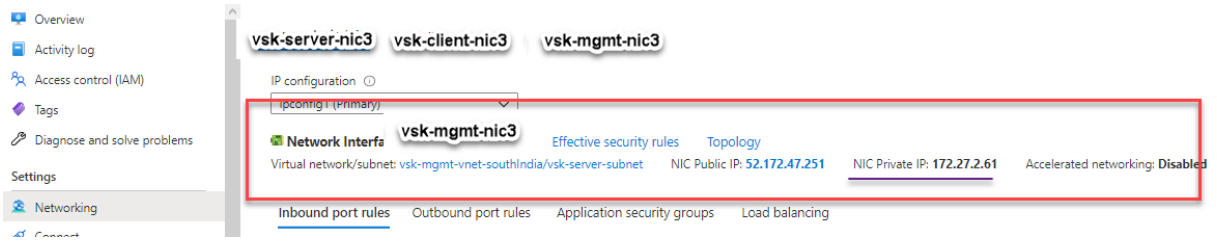
    <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
    <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>

    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

Sie können sehen, dass die Citrix ADC VPX-Instanz mit drei Netzwerkschnittstellen erstellt wird. Navigieren Sie zum **Azure-Portal > VM-Instanz > Netzwerk**, und überprüfen Sie die Netzwerkeigenschaften der drei Netzwerkkarten wie in den folgenden Abbildungen gezeigt.





Sie können den `show nsip` Befehl in der ADC CLI ausführen und überprüfen, ob die im <NS-BOOTSTRAP> Abschnitt angegebene neue Bootstrap-Sequenz angewendet wird. Sie können den Befehl “Route anzeigen” ausführen, um die Subnetzmaske zu überprüfen.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      172.27.2.61      0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      172.27.0.61      0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

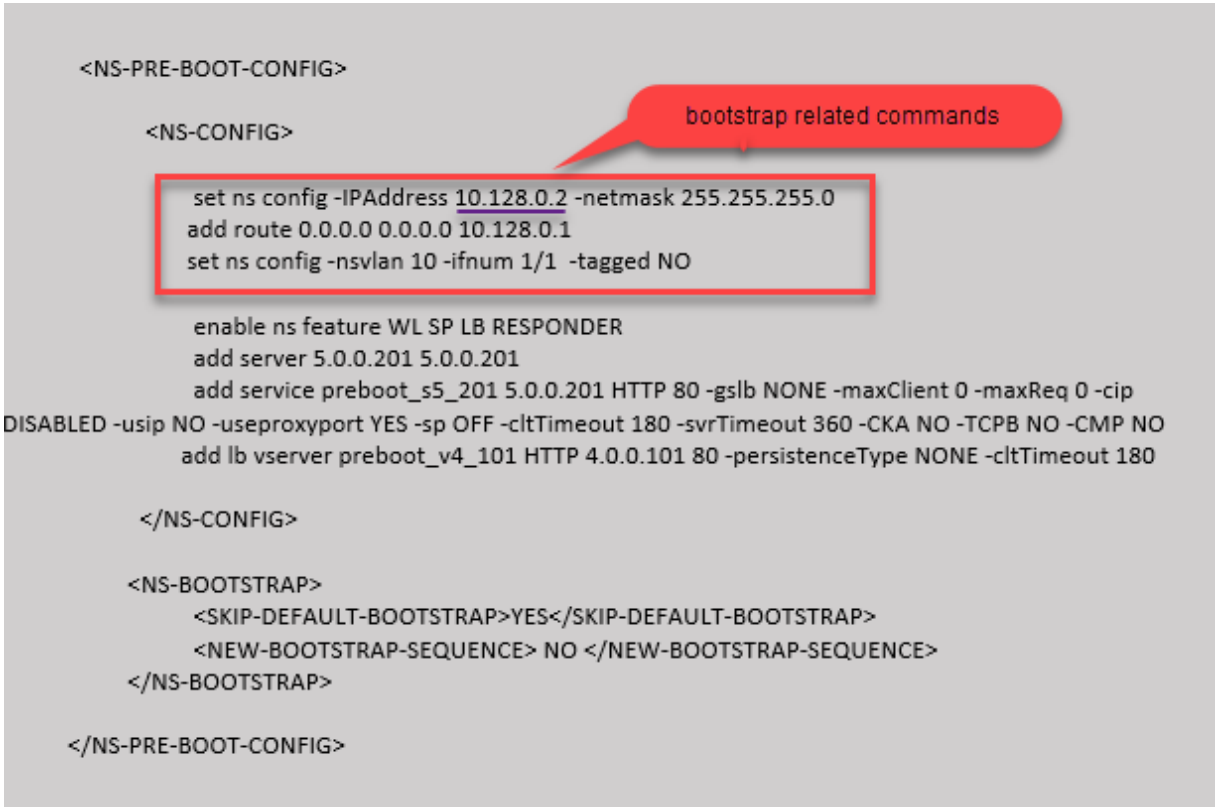
1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::20d:3aff:fec9:9076/64
        Interfaces : 0/1 1/1 LO/1

2)      VLAN ID: 5      VLAN Alias Name:

3)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/2
        IPs :
             172.27.2.61        Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          172.27.2.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      172.27.0.0       255.255.255.0    172.27.0.61      0       UP      0               DIRECT
4)      172.27.2.0       255.255.255.0    172.27.2.61      0       UP      0               DIRECT
5)      169.254.0.0      255.255.0.0      172.27.0.1       0       UP      0               STATIC
6)      168.63.129.16    255.255.255.255  172.27.0.1       0       UP      0               STATIC
7)      169.254.169.254  255.255.255.255  172.27.0.1       0       UP      0               STATIC
 Done
```

Benutzerdefiniertes Bootstrap-Beispiel für GCP

In diesem Beispiel werden Bootstrap-bezogene Befehle im <NS-CONFIG> Abschnitt bereitgestellt. Der <NS-BOOTSTRAP> Abschnitt gibt an, dass das Standard-Bootstrapping übersprungen wird und die im <NS-CONFIG> Abschnitt enthaltenen benutzerdefinierten Bootstrap-Informationen angewendet werden.



Sie können die im vorherigen Screenshot gezeigte Konfiguration von hier aus kopieren:

```
<NS-PRE-BOOT-CONFIG>

    <NS-CONFIG>

        set ns config -IPAddress 10.128.0.2 -netmask 255.255.255.0
        add route 0.0.0.0 0.0.0.0 10.128.0.1
        set ns config -nsvlan 10 -ifnum 1/1  -tagged NO

        enable ns feature WL SP LB RESPONDER
        add server 5.0.0.201 5.0.0.201
        add service preboot_s5_201 5.0.0.201 HTTP 80 -gslb NONE -
            maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport
            YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO
             -CMP NO
        add lb vserver preboot_v4_101 HTTP 4.0.0.101 80 -
            persistenceType NONE -cltTimeout 180

    </NS-CONFIG>

    <NS-BOOTSTRAP>
```



```
17          <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
18          <NEW-BOOTSTRAP-SEQUENCE> NO </NEW-BOOTSTRAP-SEQUENCE>
19       </NS-BOOTSTRAP>
20
21  </NS-PRE-BOOT-CONFIG>
22  <!--NeedCopy-->
```

Nachdem die VM-Instanz im GCP-Portal mit dem benutzerdefinierten Bootstrap erstellt wurde, können Sie die Eigenschaften der Netzwerkschnittstelle wie folgt überprüfen:

1. Wählen Sie die Instanz aus, die Sie erstellt haben, indem Sie die benutzerdefinierten Bootstrap-Informationen angeben.
2. Navigieren Sie zu den Eigenschaften der Netzwerkschnittstelle und überprüfen Sie die Netzwerkdetails wie in der Abbildung gezeigt.

Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP
nic0	default	default	10.160.0.74	–	34.93.9.79 (ephemeral)
nic1	vsk-vpc-network-1	asia-south1-subnet-1	asia-south1-subnet1-10-128-0-2 (10.128.0.2)	–	34.93.245.110 (ephemeral)
nic2	vsk-vpc-network-2	asia-south1-subnet-5	10.128.4.30	–	34.93.146.248 (ephemeral)

Sie können den `show nsip` Befehl in **ADC CLI**ausführen und sicherstellen, dass die im vorherigen <NS-CONFIG> Abschnitt bereitgestellten Konfigurationen beim ersten Start der ADC-Appliance angewendet werden.

```
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      10.128.0.2       0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      4.0.0.101        0               VIP              Active   Enabled  Enabled  Enabled  Enabled
 Done
> sh vlan

1)      VLAN ID: 1
        Link-local IPv6 addr: fe80::4001:aff:fea0:4a/64
        Interfaces : 0/1 1/2 LO/1

2)      VLAN ID: 10     VLAN Alias Name:
        Interfaces : 1/1
        IPs :
             10.128.0.2         Mask: 255.255.255.0
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State   Traffic Domain  Type
        -------          -------          ---------------  -----   -----   --------------  ----
1)      0.0.0.0          0.0.0.0          10.128.0.1       0       UP      0               STATIC
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP      0               PERMANENT
3)      10.128.0.0       255.255.255.0    10.128.0.2       0       UP      0               DIRECT
 Done
```

Auswirkungen des Anhängen und Trennen von NICs in AWS und Azure

AWS und Azure bieten die Möglichkeit, eine Netzwerkschnittstelle an eine Instanz anzuhängen und eine Netzwerkschnittstelle von einer Instanz zu trennen. Das Anhängen oder Trennen von Schnittstellen kann die Positionen der Schnittstelle verändern. Citrix empfiehlt daher, dass Sie keine

Schnittstellen von der ADC VPX-Instanz trennen. Wenn Sie eine Schnittstelle trennen oder anhängen, wenn benutzerdefiniertes Bootstrapping konfiguriert ist, weist die Citrix ADC VPX-Instanz die primäre IP der neu verfügbaren Schnittstelle in der Position der Verwaltungsschnittstelle als NSIP zu. Wenn nach dem, das Sie getrennt haben, keine weiteren Schnittstellen verfügbar sind, wird die erste Schnittstelle zur Verwaltungsschnittstelle für die ADC VPX-Instanz gemacht.
Zum Beispiel wird eine Citrix ADC VPX-Instanz mit 3 Schnittstellen aufgebracht: Eth0 (SNIP), Eth1 (NSIP) und Eth2 (VIP). Wenn Sie die Eth1-Schnittstelle von der Instanz trennen, bei der es sich um eine Verwaltungsschnittstelle handelt, konfiguriert ADC die nächste verfügbare Schnittstelle (Eth2) als Verwaltungsschnittstelle. Dadurch wird auf die ADC VPX-Instanz immer noch über die primäre IP der Eth2-Schnittstelle zugegriffen. Wenn Eth2 ebenfalls nicht verfügbar ist, wird die verbleibende Schnittstelle (Eth0) zur Verwaltungsschnittstelle gemacht. Daher besteht der Zugriff auf ADC VPX-Instanz weiterhin.
Betrachten wir eine andere Zuordnung von Schnittstellen wie folgt: Eth0 (SNIP), Eth1 (VIP) und Eth2 (NSIP). Wenn Sie Eth2 (NSIP) trennen, da nach Eth2 keine neue Schnittstelle verfügbar ist, wird die erste Schnittstelle (Eth0) zur Verwaltungsschnittstelle gemacht.

Installieren einer Citrix ADC VPX Instanz auf einem Bare-Metal-Server

October 5, 2021

Ein Bare-Metal ist ein vollständig dedizierter physischer Server, der physische Isolation bietet und vollständig in die Cloud-Umgebung integriert ist. Es wird auch als Single-Tenant-Server bezeichnet. Mit einem Mandantenverhältnis können Sie den lauten Nachbareffekt vermeiden. Mit Bare-Metal werden Sie nicht Zeuge des lauten Nachbareffekts, da Sie der einzige Benutzer sind.

Ein Bare-Metal-Server, der mit einem Hypervisor installiert wird, bietet Ihnen eine Management-Suite zum Erstellen virtueller Maschinen auf dem Server. Der Hypervisor führt keine Anwendungen nativ aus. Ziel ist es, Ihre Workloads in separate virtuelle Maschinen zu virtualisieren, um die Flexibilität und Zuverlässigkeit der Virtualisierung zu erreichen.

Voraussetzungen für die Installation der Citrix ADC VPX Instanz auf Bare-Metal-Servern

Ein Bare-Metal-Server muss von einem Cloud-Anbieter bezogen werden, der alle Systemanforderungen für den jeweiligen Hypervisor erfüllt.

Installieren Sie die Citrix ADC VPX Instanz auf Bare-Metal-Servern

Um Citrix ADC VPX Instanzen auf einem Bare-Metal-Server zu installieren, müssen Sie zuerst einen Bare-Metal-Server mit ausreichenden Systemressourcen von einem Cloud-Anbieter beziehen. Auf

diesem Bare-Metal-Server muss jeder der unterstützten Hypervisoren wie Linux KVM, VMware ESX, Citrix Hypervisor oder Microsoft Hyper-V installiert und konfiguriert werden, bevor die ADC VPX-Instanz bereitgestellt wird.

Weitere Informationen zur Liste der verschiedenen Hypervisoren und Funktionen, die von einer Citrix ADC VPX-Instanz unterstützt werden, finden Sie unter Unterstützungsmatrix und Nutzungsrichtlinien.

Weitere Informationen zur Installation von Citrix ADC VPX Instanzen auf verschiedenen Hypervisoren finden Sie in der entsprechenden Dokumentation.

- **Citrix Hypervisor:** Siehe Installieren einer Citrix ADC VPX-Instanz auf Citrix Hypervisor.
- **VMware ESX:** Siehe Installieren einer Citrix ADC VPX-Instanz unter VMware ESX.
- **Microsoft Hyper-V:** Siehe Installieren einer Citrix ADC VPX-Instanz auf Microsoft Hyper-V-Server.
- **Linux KVM-Plattform:** Siehe Installieren einer Citrix ADC VPX-Instanz auf der Linux-KVM-Plattform.

Installieren einer Citrix ADC VPX-Instanz auf Citrix Hypervisor

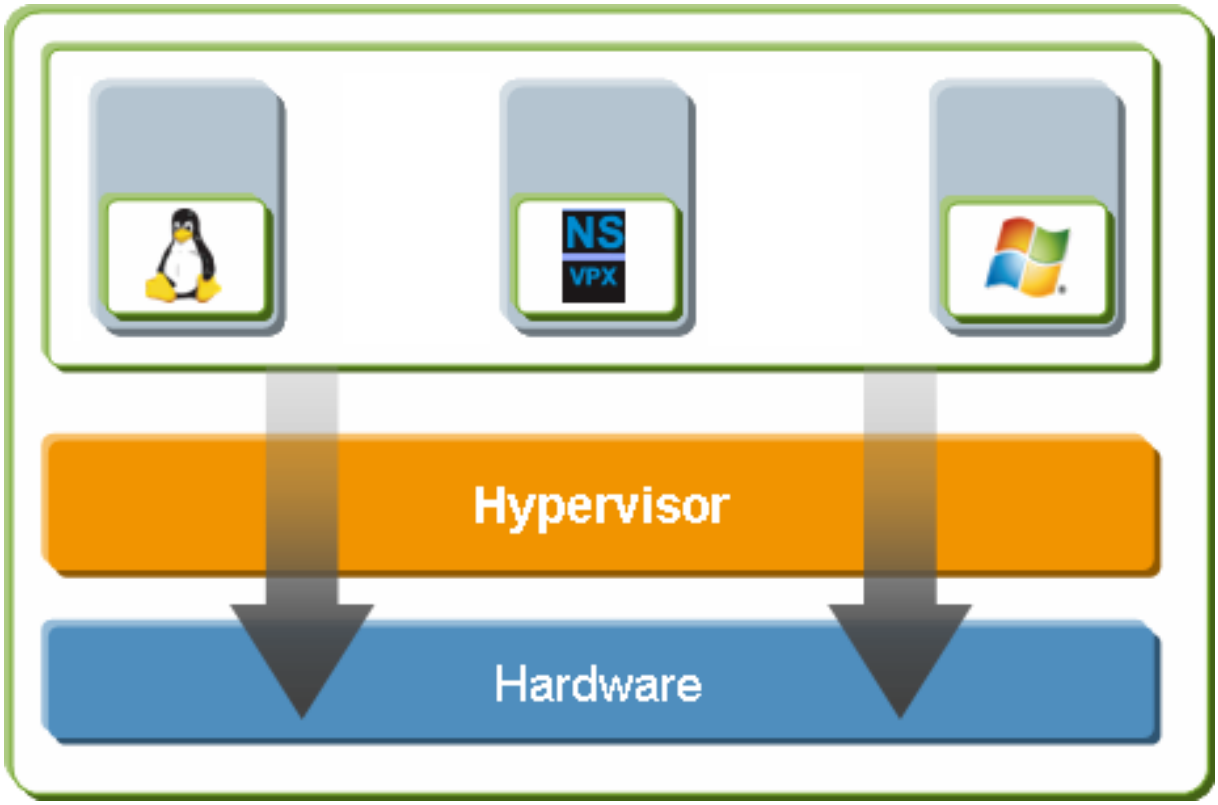
October 5, 2021

Um VPX-Instanzen auf dem Citrix Hypervisor zu installieren, müssen Sie zuerst den Hypervisor auf einem Computer mit ausreichenden Systemressourcen installieren. Um die Citrix ADC VPX-Instanzinstallation durchzuführen, verwenden Sie Citrix XenCenter, das auf einem Remotecomputer installiert sein muss, der über das Netzwerk eine Verbindung zum Hypervisor-Host herstellen kann.

Weitere Informationen zu Hypervisor finden Sie in der Dokumentation zu Citrix Hypervisor.

Die folgende Abbildung zeigt die Bare-Metal-Lösungsarchitektur der Citrix ADC VPX-Instanz auf Hypervisor.

Abbildung. Eine Citrix ADC VPX-Instanz auf Citrix Hypervisor



Voraussetzungen für die Installation einer Citrix ADC VPX-Instanz auf Hypervisor

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, gehen Sie folgendermaßen vor:

- Installieren Sie Hypervisor Version 6.0 oder höher auf Hardware, die die Mindestanforderungen erfüllt.
- Installieren Sie XenCenter auf einer Verwaltungs-Workstation, die die Mindestsystemanforderungen erfüllt.
- Beziehen Sie Lizenzdateien für virtuelle Appliances. Weitere Informationen zu Lizenzen für virtuelle Geräte finden Sie im *Citrix ADC VPX -Lizenzhandbuch* unter http://support.citrix.com/article/ctx122426.

Hardwareanforderungen für Hypervisor

In der folgenden Tabelle werden die Mindestanforderungen an die Hardware für eine Hypervisor-Plattform beschrieben, auf der eine Citrix ADC VPX-Instanz ausgeführt wird.

Tabelle 1. Mindestsystemanforderungen für Hypervisor, auf dem eine nCore VPX-Instanz ausgeführt wird

Komponente	Voraussetzung
CPU	2 oder mehr 64-Bit-x86-CPUs mit aktivierter Virtualisierungsunterstützung (Intel-VT). AMD Prozessor wird nicht unterstützt. Um die Citrix ADC VPX-Instanz auszuführen, muss die Hardwareunterstützung für die Virtualisierung auf dem Hypervisor-Host aktiviert sein. Stellen Sie sicher, dass die BIOS-Option für die Virtualisierungsunterstützung nicht deaktiviert ist. Weitere Informationen finden Sie in der BIOS-Dokumentation.
RAM	3 GB
Speicherplatz	Lokal angeschlossener Speicher (PATA, SATA, SCSI) mit 40 GB Speicherplatz. Hinweis: Die Hypervisor-Installation erstellt eine 4-GB-Partition für die Hypervisor-Host-Steuerdomäne. Der verbleibende Speicherplatz ist für die Citrix ADC VPX-Instanz und andere virtuelle Maschinen verfügbar.
NIC	Eine 1-Gbit/s-Netzwerkkarte; empfohlen: zwei 1-Gbit/s-Netzwerkkarten

Weitere Informationen zur Installation von Hypervisor finden Sie in der Hypervisor-Dokumentation unterhttp://support.citrix.com/product/xens/.

In der folgenden Tabelle sind die virtuellen Computerressourcen aufgeführt, die Hypervisor für jede virtuelle nCore VPX-Appliance bereitstellen muss.

Tabelle 2. Minimale virtuelle Computing-Ressourcen, die zum Ausführen einer NCore VPX-Instanz erforderlich sind

Komponente	Voraussetzung
Speicher	2 GB
Virtuelle CPU (vCPU)	2
Virtuelle Netzwerkschnittstellen	2

> Hinweis: Für die Verwendung der
> Citrix ADC VPX Instanz in der Produktion empfiehlt Citrix, dass die CPU-Priorität (in den Eigenschaften der virtuellen Maschine) auf die höchste Stufe gesetzt wird, um das Planungsverhalten und die Netzwerklatenz zu verbessern.

XenCenter -Systemanforderungen

XenCenter ist eine Windows-Clientanwendung. Es kann nicht auf demselben Computer wie der Hypervisor-Host ausgeführt werden. Weitere Informationen zu minimalen Systemanforderungen und der Installation von XenCenter finden Sie in den folgenden Hypervisor-Dokumenten:

- Systemanforderungen
- Installieren

Installieren von Citrix ADC VPX-Instanzen auf Hypervisor mithilfe von XenCenter

Nachdem Sie Hypervisor und XenCenter installiert und konfiguriert haben, können Sie mit XenCenter virtuelle Appliances auf Hypervisor installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt vom Arbeitsspeicher ab, der auf der Hardware verfügbar ist, auf der Hypervisor ausgeführt wird.

Nachdem Sie XenCenter zur Installation der ersten Citrix ADC VPX Instanz (XVA-Image) auf Hypervisor verwendet haben, können Sie mit dem Command Center die Citrix ADC VPX-Instanz bereitstellen. Weitere Informationen finden Sie in der Command Center-Dokumentation .

Gehen Sie folgendermaßen vor, um Citrix ADC VPX-Instanzen auf Hypervisor mithilfe von XenCenter zu installieren:

1. Starten Sie XenCenter auf Ihrer Workstation.
2. Klicken Sie im Menü Server auf Hinzufügen.
3. Geben Sie im Dialogfeld Neuen Server hinzufügen im Textfeld Hostname die IP-Adresse oder den DNS-Namen des Hypervisor ein, mit dem Sie eine Verbindung herstellen möchten.
4. Geben Sie in die Textfelder Benutzername und Kennwort die Administratoranmeldeinformationen ein, und klicken Sie dann auf Verbinden. Der Hypervisor-Name wird im Navigationsbereich mit einem grünen Kreis angezeigt, der angibt, dass der Hypervisor verbunden ist.
5. Klicken Sie im Navigationsbereich auf den Namen des Hypervisor, auf dem Sie die Citrix ADC VPX-Instanz installieren möchten.
6. Klicken Sie im Menü VM auf Importieren.
7. Navigieren Sie im Dialogfeld Importieren im Dateinamen importieren zu dem Speicherort, an dem Sie die XVA-Imagedatei der Citrix ADC VPX-Instanz gespeichert haben. Stellen Sie sicher, dass die Option Exportierte VM ausgewählt ist, und klicken Sie dann auf Weiter.

8. Wählen Sie den Hypervisor aus, auf dem Sie die virtuelle Appliance installieren möchten, und klicken Sie dann auf Weiter.
9. Wählen Sie das lokale Speicher-Repository aus, in dem die virtuelle Appliance gespeichert werden soll, und klicken Sie dann auf Importieren, um den Importvorgang zu starten.
10. Sie können die virtuellen Netzwerkschnittstellen nach Bedarf hinzufügen, ändern oder löschen. Wenn Sie fertig sind, klicken Sie auf Weiter.
11. Klicken Sie auf Fertig stellen, um den Importvorgang abzuschließen.

    Hinweis: Um den Status des Importprozesses anzuzeigen, klicken Sie auf die Registerkarte **Protokoll** .
12. Wenn Sie eine andere virtuelle Appliance installieren möchten, wiederholen Sie die Schritte 5 bis 11.

> **Hinweis:**
>
> Wenn Sie nach der Erstkonfiguration der VPX-Instanz die Appliance auf die neueste Softwareversion aktualisieren möchten, lesen Sie Upgraden oder Downgrade der Systemsoftware.

Konfigurieren von VPX-Instanzen für die Verwendung von SR-IOV-Netzwerkschnittstellen (Single Root I/O Virtualization, Single Root I/O Virtualization)

October 5, 2021

Nachdem Sie eine Citrix ADC VPX-Instanz auf XenServer installiert und konfiguriert haben, können Sie die virtuelle Appliance so konfigurieren, dass SR-IOV-Netzwerkschnittstellen verwendet werden.

Einschränkungen

XenServer unterstützt die folgenden Funktionen auf SRIOV-Schnittstellen nicht:

- L2-Modus Umschaltung
- Clustering
- Adminpartitionierung [Freigegebener VLAN-Modus]
- Hochverfügbarkeit [Aktiv - Aktiver Modus]
- Jumbo-Rahmen
- IPv6-Protokoll in Clusterumgebung

Voraussetzungen

Stellen Sie auf dem XenServer Host Folgendes sicher:

- Fügen Sie die Intel 82599 NIC (NIC) zum Host hinzu.
- Blockieren Sie den `ixgbevf` Treiber auf, indem Sie der Datei **/etc/modprobe.d/blacklist.conf** den folgenden Eintrag hinzufügen:

  blacklist ixgbevf
- Aktivieren Sie SR-IOV Virtual Functions (VfS), indem Sie den folgenden Eintrag zur Datei **/etc/-modprobe.d/ixgbe** hinzufügen:

  options ixgbe max_vfs=*<number_of_VFs>*

  Dabei <*number_VFs*> ist die Anzahl der SR-IOV-VFs, die Sie erstellen möchten.
- Stellen Sie sicher, dass SR-IOV im BIOS aktiviert ist.

IXGBE Treiberversion 3.22.3 wird empfohlen.

Zuweisen von SR-IOV-VFs zur VPX-Instanz mithilfe des XenServer Hosts

Gehen Sie folgendermaßen vor, um SR-IOV-Netzwerkschnittstellen der Citrix ADC VPX-Instanz zuzuweisen:

1. Verwenden Sie auf dem XenServer Host den folgenden Befehl, um die SR-IOV-VFs der Citrix ADC VPX-Instanz zuzuweisen:

   xe host-call-plugin plugin=iovirt host-uuid=<*Xen host UUID*> **fn=assign_free_vf args:uuid**=<*Netscalar VM UUID*> **args:ethdev**=<*interface name*> **args:mac=***<Mac addr>*

   Wobei:

   - <*Xen host UUID*> ist die UUID des XenServer Hosts.
   - <*NetScaler VM UUID*> ist die UUID der Citrix ADC VPX-Instanz.
   - <*interface name*> ist die Schnittstelle für die SR-IOV-VFs.
   - <*MAC address* > ist die MAC-Adresse des SR-IOV VF.

   > **Hinweis:**
   >
   > Geben Sie die MAC-Adresse an, die Sie im Parameter args:mac= verwenden möchten. Wenn nicht angegeben, generiert das `iovirt` Skript zufällig eine MAC-Adresse und weist sie zu. Wenn Sie die SR-IOV-VFs im Link-Aggregationsmodus verwenden möchten, stellen Sie sicher, dass Sie die MAC-Adresse als 00:00:00:00:00:00 angeben.
2. Starten Sie die Citrix ADC VPX-Instanz.

Aufheben der Zuweisung von SR-IOV-VFs zur VPX-Instanz mithilfe des XenServer Hosts

Wenn Sie ein falsches SR-IOV-VFs zugewiesen haben oder wenn Sie ein zugewiesenes SR-IOV-VFs ändern möchten, müssen Sie die Zuweisung der SR-IOV-VFs aufheben und der Citrix ADC VPX-Instanz neu zuweisen.

Gehen Sie folgendermaßen vor, um die Zuweisung der SR-IOV-Netzwerkschnittstelle aufzuheben, die einer Citrix ADC VPX-Instanz zugewiesen ist:

1. Verwenden Sie auf dem XenServer Host den folgenden Befehl, um die SR-IOV-VFs der Citrix ADC VPX-Instanz zuzuweisen und die Citrix ADC VPX-Instanz neu zu starten:

   xe host-call-plugin plugin=iovirt **host-uuid**=<*Xen_host_UUID*> **fn**=unassign_all **args:uuid**=<*Netscalar_VM_U*

   Wobei:

   - <*Xen_host_UUID*> ist die UUID des XenServer Hosts.
   - <*Netscalar_VM_UUID*> ist die UUID der Citrix ADC VPX-Instanz.

2. Starten Sie die Citrix ADC VPX-Instanz.

Konfigurieren von VLAN auf der SR-IOV-Schnittstelle

> **Wichtig**
>
> Stellen Sie beim Zuweisen der SR-IOV-VFs zur Citrix ADC VPX-Instanz sicher, dass Sie die MAC-Adresse 00:00:00:00:00:00 für die VFs angeben.

Um die virtuellen SR-IOV-Funktionen im Link-Aggregationsmodus zu verwenden, müssen Sie die Spoofprüfung für virtuelle Funktionen deaktivieren, die Sie erstellt haben. Verwenden Sie auf dem XenServer Host den folgenden Befehl, um die Spoofprüfung zu deaktivieren:

ip link set <*interface_name*> **vf** <*VF_id*> **spoofchk** off

Wobei:

- <interface_name>ist der Schnittstellenname.
- <VF_id>ist die virtuelle Funktions-ID.

Nachdem Sie die Spoofprüfung für alle erstellten virtuellen Funktionen deaktiviert haben, starten Sie die Citrix ADC VPX-Instanz neu, und konfigurieren Sie die Linkaggregation. Anweisungen finden Sie unter Konfigurieren der Link-Aggregation.

Konfigurieren von VLAN auf der SR-IOV-Schnittstelle

Sie können VLAN für die virtuellen SR-IOV-Funktionen konfigurieren, Anweisungen finden Sie unter Konfigurieren eines VLANs.

> **Wichtig**
>
> Stellen Sie sicher, dass der XenServer Host keine VLAN-Einstellungen für die VF-Schnittstelle enthält.

Installieren einer Citrix ADC VPX-Instanz auf VMware ESX

April 7, 2022

Stellen Sie vor der Installation von Citrix ADC VPX-Instanzen auf VMware ESX sicher, dass VMware ESX Server auf einem Computer mit ausreichenden Systemressourcen installiert ist. Um eine Citrix ADC VPX-Instanz auf VMware ESXi zu installieren, verwenden Sie den VMware vSphere-Client. Der Client oder das Tool muss auf einem Remote-Computer installiert sein, der über das Netzwerk eine Verbindung zu VMware ESX herstellen kann.

Dieser Abschnitt enthält die folgenden Themen:

- Voraussetzungen
- Installieren einer Citrix ADC VPX-Instanz auf VMware ESX

> **Wichtig**
>
> Sie können keine standardmäßigen VMware Tools installieren oder die VMware Tools-Version aktualisieren, die auf einer Citrix ADC VPX-Instanz verfügbar ist. VMware Tools für eine Citrix ADC VPX-Instanz werden im Rahmen der Citrix ADC-Softwareversion bereitgestellt.

Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, gehen Sie folgendermaßen vor:

- Installieren Sie VMware ESX auf Hardware, die die Mindestanforderungen erfüllt.
- Installieren Sie VMware Client auf einer Management-Workstation, die die Mindestsystemanforderungen erfüllt.
- Laden Sie die Setupdateien der Citrix ADC VPX Appliance herunter.
- Beschriften Sie die physischen Netzwerkports von VMware ESX.
- Beziehen Sie die VPX-Lizenzdateien. Weitere Informationen zu Citrix ADC VPX-Instanzlizenzen finden Sie unter Lizenzierungsübersicht.

VMware ESX-Hardwareanforderungen

In der folgenden Tabelle werden die Mindestsystemanforderungen für VMware ESX-Server beschrieben, auf denen die virtuelle Citrix ADC VPX NCore Appliance ausgeführt wird.

Tabelle 1. Mindestsystemanforderungen für einen VMware ESX-Server, auf dem eine Citrix ADC VPX-Instanz ausgeführt wird

Komponente	Voraussetzung
-	2 oder mehr 64-Bit-x86-CPUs mit aktivierter Virtualisierungsunterstützung (Intel-VT). Um die Citrix ADC VPX-Instanz ausführen zu können, muss die Hardwareunterstützung für die Virtualisierung auf dem VMware ESX-Host aktiviert sein. Stellen Sie sicher, dass die BIOS-Option für die Virtualisierungsunterstützung nicht deaktiviert ist. Weitere Informationen finden Sie in Ihrer BIOS-Dokumentation.
RAM	3 GB
Speicherplatz	40 GB freier Speicherplatz
Netzwerk	Eine 1-Gbit/s-NIC (NIC); Zwei 1-Gbit/s-NICs empfohlen

Hinweise zur Installation von VMware ESX finden Sie unterhttp://www.vmware.com/.

In der folgenden Tabelle sind die virtuellen Computerressourcen aufgeführt, die der VMware ESX-Server für jede virtuelle VPX NCore Appliance bereitstellen muss.

Tabelle 2. Minimale virtuelle Datenverarbeitungsressourcen für die Ausführung einer Citrix ADC VPX-Instanz

Komponente	Voraussetzung
Speicher	4 GB
Virtuelle CPU (vCPU)	2
Virtuelle Netzwerkschnittstellen	1. In ESX können Sie maximal 10 virtuelle Netzwerkschnittstellen installieren, wenn die VPX-Hardware auf Version 7 oder höher aktualisiert wird.
Speicherplatz	20 GB

> Hinweis
>
> Dies gilt zusätzlich zu den Datenträgeranforderungen für den Hypervisor.

Für die Produktionsnutzung der virtuellen VPX-Appliance muss die vollständige Speicherzuweisung reserviert werden. CPU-Zyklen (in MHz), die mindestens der Geschwindigkeit eines CPU-Kerns des ESX entsprechen, müssen reserviert werden.

Systemanforderungen für VMware vSphere-Clients

VMware vSphere ist eine Clientanwendung, die auf Windows- und Linux-Betriebssystemen ausgeführt werden kann. Es kann nicht auf demselben Computer wie der VMware ESX-Server ausgeführt werden. In der folgenden Tabelle werden die Mindestsystemanforderungen beschrieben.

Tabelle 3. Mindestsystemanforderungen für die Installation des VMware vSphere-Clients

Komponente	Voraussetzung
Betriebssystem	Für detaillierte Anforderungen von VMware, suchen Sie nach der PDF-Datei “vSphere Compatibility Matrixes” unter http://kb.vmware.com/.
CPU	750 MHz; 1 Gigahertz (GHz) oder schneller empfohlen
RAM	1 GB; 2 GB empfohlen
NIC (NIC)	Netzwerkkarte mit 100 Mbit/s oder schneller

Systemanforderungen für OVF Tool 1.0

OVF Tool ist eine Client-Anwendung, die auf Windows- und Linux-Systemen ausgeführt werden kann. Es kann nicht auf demselben Computer wie der VMware ESX-Server ausgeführt werden. In der folgenden Tabelle werden die Mindestsystemanforderungen beschrieben.

Tabelle 4. Mindestsystemanforderungen für die Installation von OVF-Werkzeugen

Komponente	Voraussetzung
Betriebssystem	Für detaillierte Anforderungen von VMware suchen Sie unter nach der PDF-Datei “OVF Tool User Guide” http://kb.vmware.com/.

Komponente	Voraussetzung
CPU	Mindestens 750 MHz, 1 GHz oder schneller empfohlen
RAM	1 GB Minimum, 2 GB empfohlen
NIC (NIC)	Netzwerkkarte mit 100 Mbit/s oder schneller

Weitere Informationen zur Installation von OVF finden Sie unter der PDF-Datei “OVF Tool User Guide” http://kb.vmware.com/.

Herunterladen der Setup-Dateien für Citrix ADC VPX

Das Citrix ADC VPX-Instanz-Setup-Paket für VMware ESX folgt dem Formatstandard Open Virtual Machine (OVF). Sie können die Dateien von der Citrix Website herunterladen. Sie benötigen ein Citrix Konto, um sich anzumelden. Wenn Sie kein Citrix-Konto haben, rufen Sie die Startseite unter http://www.citrix.comauf, klicken Sie auf den **Link Neue Benutzer**und befolgen Sie die Anweisungen zum Erstellen eines neuen Citrix-Kontos.

Navigieren Sie nach der Anmeldung auf der Citrix Homepage zum folgenden Pfad:

Citrix.com > **Downloads > Citrix ADC > Virtuelle Appliances**.

Kopieren Sie die folgenden Dateien auf eine Arbeitsstation im selben Netzwerk wie der ESX-Server. Kopieren Sie alle drei Dateien in denselben Ordner.

- NSVPX-ESX-<release number>-<build number>-disk1.vmdk (for example, NSVPX-ESX-13.0-71.44_nc_64-disk1.vmdk)
- NSVPX-ESX-<release number>-<build number>.ovf (for example, NSVPX-ESX-13.0-71.44_nc_64.ovf)
- NSVPX-ESX-<release number>-<build number>.mf (for example, NSVPX-ESX-13.0-71.44_nc_64.mf)

Beschriften der physischen Netzwerkports von VMware ESX

Beschriften Sie vor der Installation einer virtuellen VPX-Appliance alle Schnittstellen, die Sie virtuellen Appliances zuweisen möchten, in einem eindeutigen Format, z. B. NS_NIC_1_1, NS_NIC_1_2 usw. In großen Bereitstellungen hilft die Beschriftung in einem eindeutigen Format bei der schnellen Identifizierung der Schnittstellen, die der virtuellen VPX-Appliance zugeordnet sind, unter anderen Schnittstellen, die von anderen virtuellen Maschinen wie Windows und Linux verwendet werden. Eine solche Kennzeichnung ist besonders wichtig, wenn verschiedene Arten von virtuellen Maschinen Schnittstellen teilen.

Gehen Sie folgendermaßen vor, um die physischen Netzwerkports von VMware ESX Server zu beschriften:

1. Melden Sie sich mithilfe des vSphere-Clients beim VMware ESX-Server an.
2. Wählen Sie auf dem vSphere-Client die Registerkarte Konfiguration aus, und klicken Sie dann auf Netzwerk.
3. Klicken Sie in der oberen rechten Ecke auf “Netzwerk hinzufügen”.
4. Wählen Sie im Assistenten zum Hinzufügen von Netzwerken für **VerbindungstypVirtuelle Maschine**aus, und klicken Sie dann auf Weiter.
5. Scrollen Sie durch die Liste der physischen vSwitch-Adapter und wählen Sie den physischen Port aus, der der Schnittstelle 1/1 auf den virtuellen Appliances zugeordnet wird.
6. Geben Sie die Bezeichnung der Schnittstelle ein, z. B. **NS_NIC_1_1**, als Namen des vSwitch, der der Schnittstelle 1/1 der virtuellen Appliances zugeordnet ist.
7. Klicken Sie auf Weiter, um die Erstellung von vSwitch abzuschließen. Wiederholen Sie den Vorgang, beginnend mit Schritt 2, um zusätzliche Schnittstellen hinzuzufügen, die von Ihren virtuellen Appliances verwendet werden sollen. Beschriften Sie die Schnittstellen nacheinander im richtigen Format (z. B. NS_NIC_1_2).

Installieren einer Citrix ADC VPX-Instanz auf VMware ESX

Nachdem Sie VMware ESX installiert und konfiguriert haben, können Sie den VMware vSphere-Client verwenden, um virtuelle Appliances auf dem VMware ESX-Server zu installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der Menge an Speicher ab, die auf der Hardware verfügbar ist, auf der VMware ESX ausgeführt wird.

Gehen Sie folgendermaßen vor, um Citrix ADC VPX-Instanzen auf VMware ESX mithilfe von VMware vSphere Client zu installieren:

1. Starten Sie den VMware vSphere Client auf Ihrer Workstation.
2. Geben Sie im Textfeld **IP-Adresse/Name** die IP-Adresse des VMware ESX-Servers ein, mit dem Sie eine Verbindung herstellen möchten.
3. Geben Sie in die Textfelder **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein, und klicken Sie dann auf Anmelden.
4. Klicken Sie im Menü **Datei** auf **OVF-Vorlage bereitstellen**.
5. Navigieren Sie im Dialogfeld **OVF-Vorlage bereitstellen** unter **Deploy from file** zu dem Speicherort, an dem Sie die Citrix ADC VPX-Instanz-Setupdateien gespeichert haben, wählen Sie die OVF-Datei aus, und klicken Sie auf **Weiter**.
6. Ordnen Sie die in der OVF-Vorlage für virtuelle Appliance angezeigten Netzwerke den Netzwerken zu, die Sie auf dem ESX-Host konfiguriert haben. Klicken Sie auf **Weiter**, um mit der Installation einer virtuellen Appliance auf VMware ESX zu beginnen. Wenn die Installation abgeschlossen ist, informiert Sie ein Popup-Fenster über die erfolgreiche Installation.
7. Sie können nun die Citrix ADC VPX-Instanz starten. Wählen Sie im Navigationsbereich die Citrix ADC VPX-Instanz aus, die Sie installiert haben, und wählen Sie im Kontextmenü die Option **Einschalten**aus.

8. Konfigurieren Sie nach dem Booten der VM über die Konsole die Citrix ADC IP-, Netmask- und Gateway-Adressen. Wenn Sie die Konfiguration abgeschlossen haben, wählen Sie in der Konsole die Option **Speichern und beenden** .
9. Wenn Sie eine weitere virtuelle Appliance installieren möchten, wiederholen Sie Schritt 6.

> **Hinweis**
>
> Standardmäßig verwendet die Citrix ADC VPX-Instanz E1000 Netzwerkschnittstellen.
>
> Nach der Installation können Sie den vSphere Client oder vSphere Web Client verwenden, um virtuelle Appliances auf VMware ESX zu verwalten.
>
> Damit die VLAN-Tagging-Funktion funktioniert, legen Sie auf VMware ESX die VLAN-ID der Portgruppe auf All (4095) auf dem vSwitch des VMware ESX-Servers fest. Weitere Informationen zum Festlegen einer VLAN-ID auf dem vSwitch des VMware ESX-Servers finden Sie unter http://www.vmware.com/pdf/esx3_vlan_wp.pdf.

Migrieren Sie eine Citrix ADC VPX-Instanz mithilfe von VMware VMotion

Sie können eine Citrix ADC VPX-Instanz mithilfe von VMware vSphere vMotion migrieren.

Folgen Sie diesen Nutzungsrichtlinien:

- VMware unterstützt die VMotion-Funktion auf virtuellen Maschinen, die mit PCI-Passthrough- und SR-IOV-Schnittstellen konfiguriert sind, nicht.
- Unterstützte Schnittstellen sind E1000 und VMXNET3. Um vMotion auf Ihrer VPX-Instanz zu verwenden, stellen Sie sicher, dass die Instanz mit einer unterstützten Schnittstelle konfiguriert ist.
- Weitere Informationen zur Migration einer Instanz mithilfe von VMware VMotion finden Sie in der VMware-Dokumentation.

Konfigurieren einer Citrix ADC VPX-Instanz für die Verwendung der VMXNET3-Netzwerkschnittstelle

October 5, 2021

Nachdem Sie die Citrix ADC VPX-Instanz auf VMware ESX installiert und konfiguriert haben, können Sie den VMware vSphere-Webclient verwenden, um die virtuelle Appliance für die Verwendung von VMXNET3-Netzwerkschnittstellen zu konfigurieren.

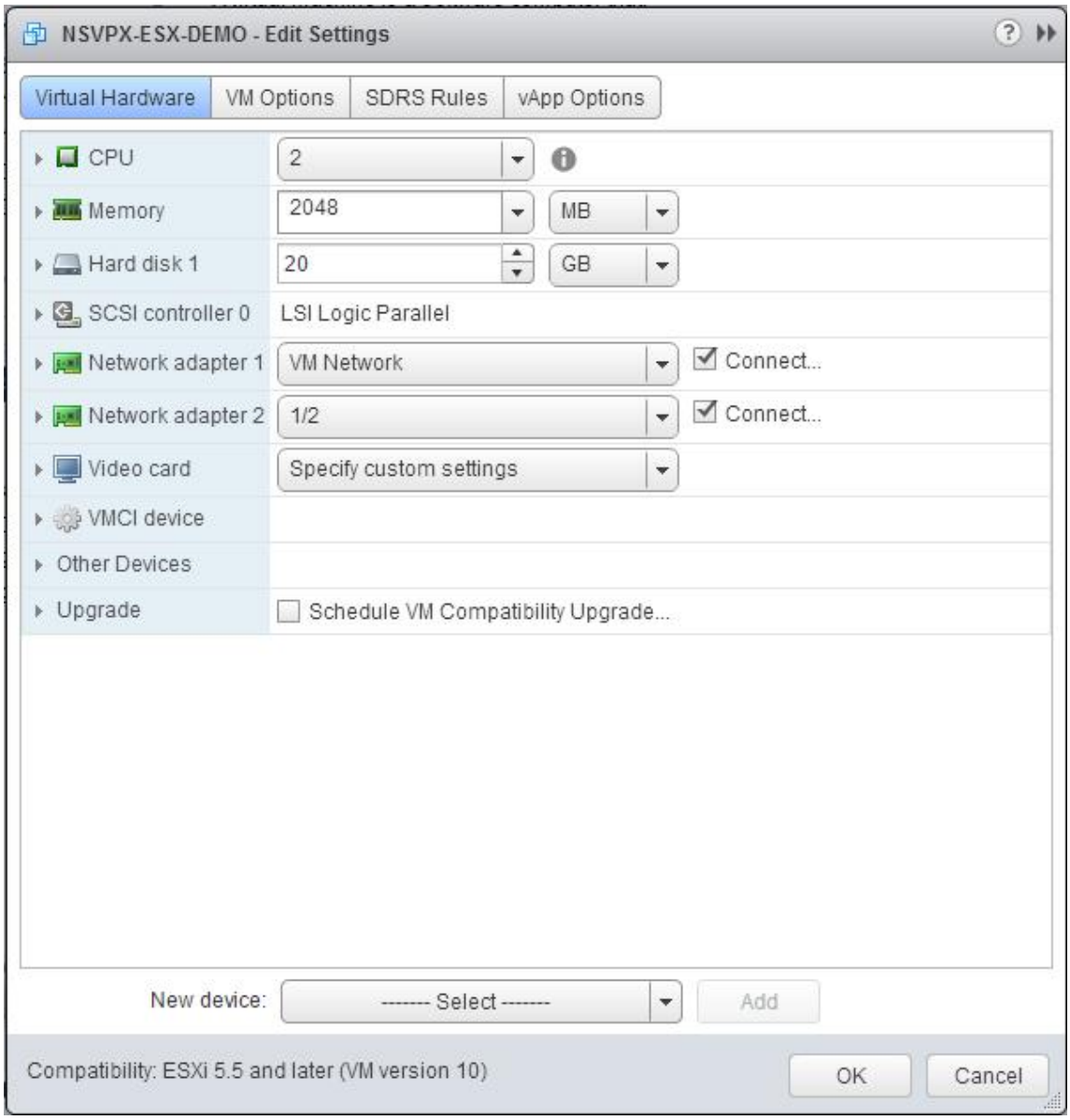
So konfigurieren Sie Citrix ADC VPX-Instanzen für die Verwendung von VMXNET3-Netzwerkschnittstellen mithilfe des VMware vSphere Web Client:

1. Wählen Sie im vSphere Web Client Hosts und Clusteraus.
2. Aktualisieren Sie die Kompatibilitätseinstellung der Citrix ADC VPX-Instanz wie folgt auf ESX:

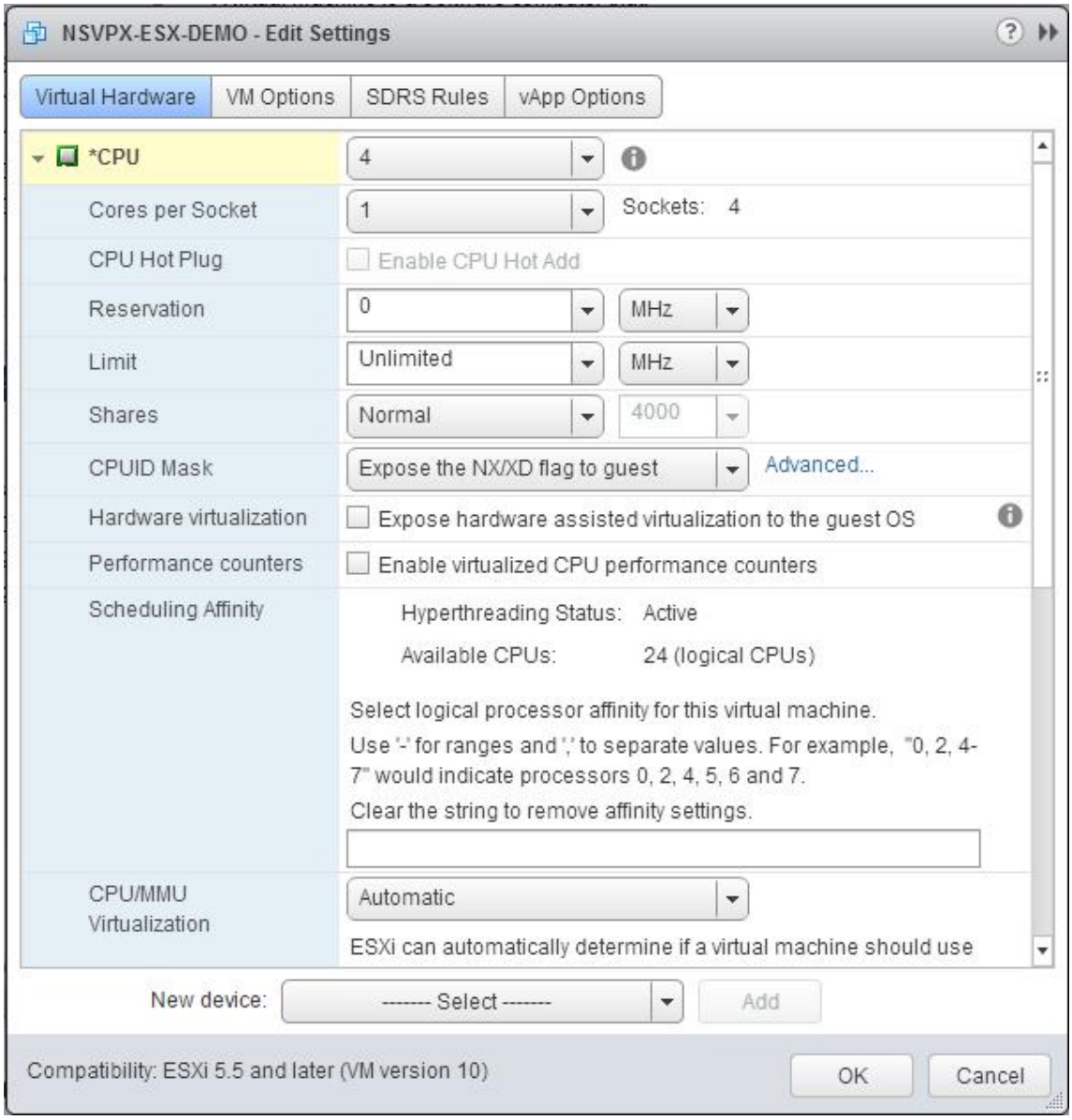
   a. Schalten Sie die Citrix ADC VPX-Instanz aus.

   b. Klicken Sie mit der rechten Maustaste auf die Citrix ADC VPX Instanz, und wählen Sie Kompatibilität > VM-Kompatibilität aktualisieren.

   c. Wählen Sie im Dialogfeld VM-Kompatibilität konfigurieren die Option ESXi 5.5 und höher aus der Dropdownliste Kompatibel mit aus, und klicken Sie auf OK.
3. Klicken Sie mit der rechten Maustaste auf die Citrix ADC VPX Instanz, und klicken Sie auf Einstellungen bearbeiten.



4. Klicken Sie im Dialogfeld <virtual_appliance> - Einstellungen bearbeiten auf den Abschnitt CPU.



5. Aktualisieren Sie im Abschnitt CPU Folgendes:

   - CPU-Anzahl
   - Anzahl der Sockets
   - Reservierungen
   - Limit
   - Freigaben

   Legen Sie die Werte wie folgt fest:

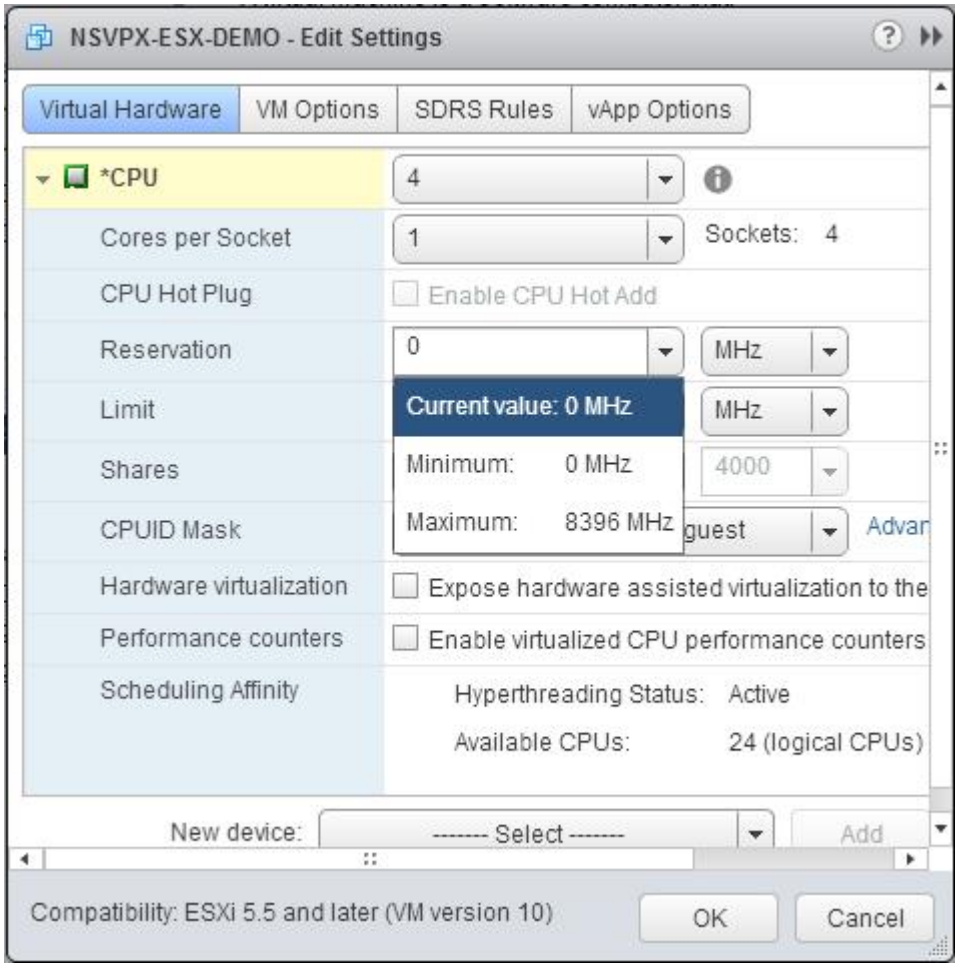
   a. Wählen Sie in der Dropdownliste CPU die Anzahl der CPUs aus, die der virtuellen Appliance zugewiesen werden sollen.

   b. Wählen Sie in der Dropdownliste Kerne pro Sockel die Anzahl der Sockets aus.

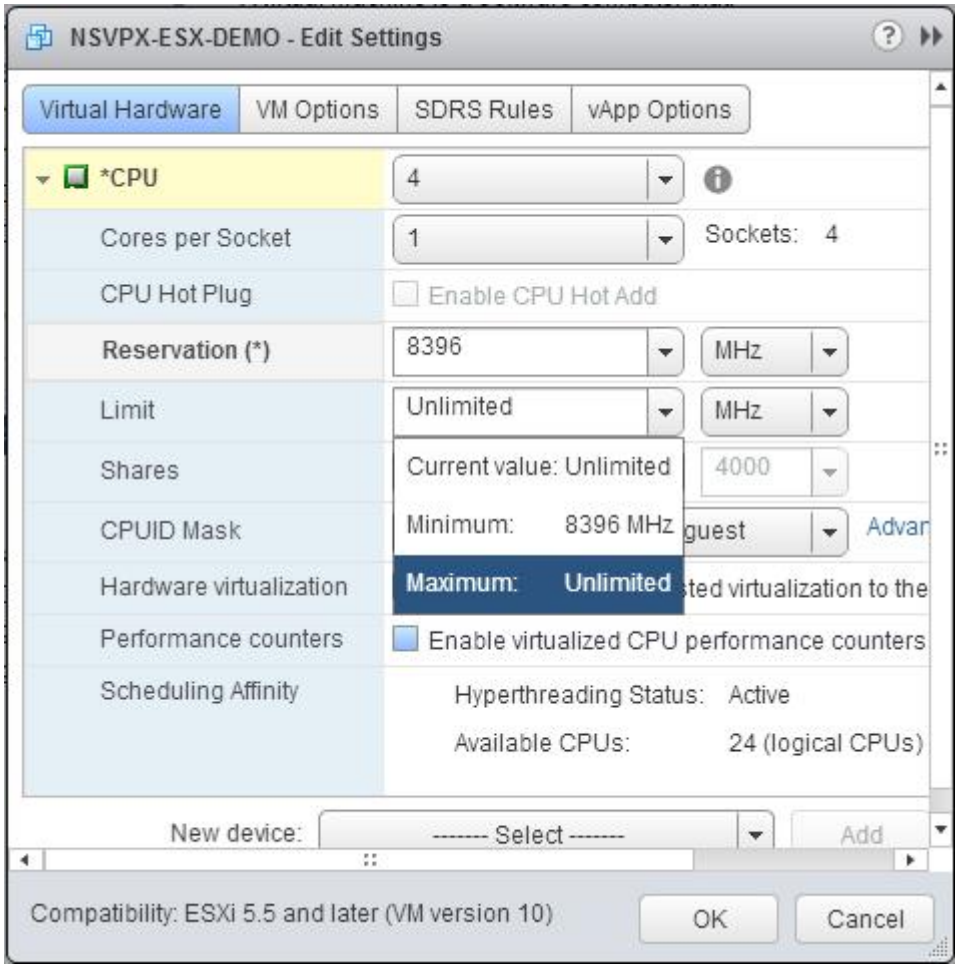
c. (Optional) Aktivieren oder deaktivieren Sie im Feld CPU-Hotplug das Kontrollkästchen CPU-Hotadd aktivieren.

Hinweis: Citrix empfiehlt, den Standard zu akzeptieren (deaktiviert).

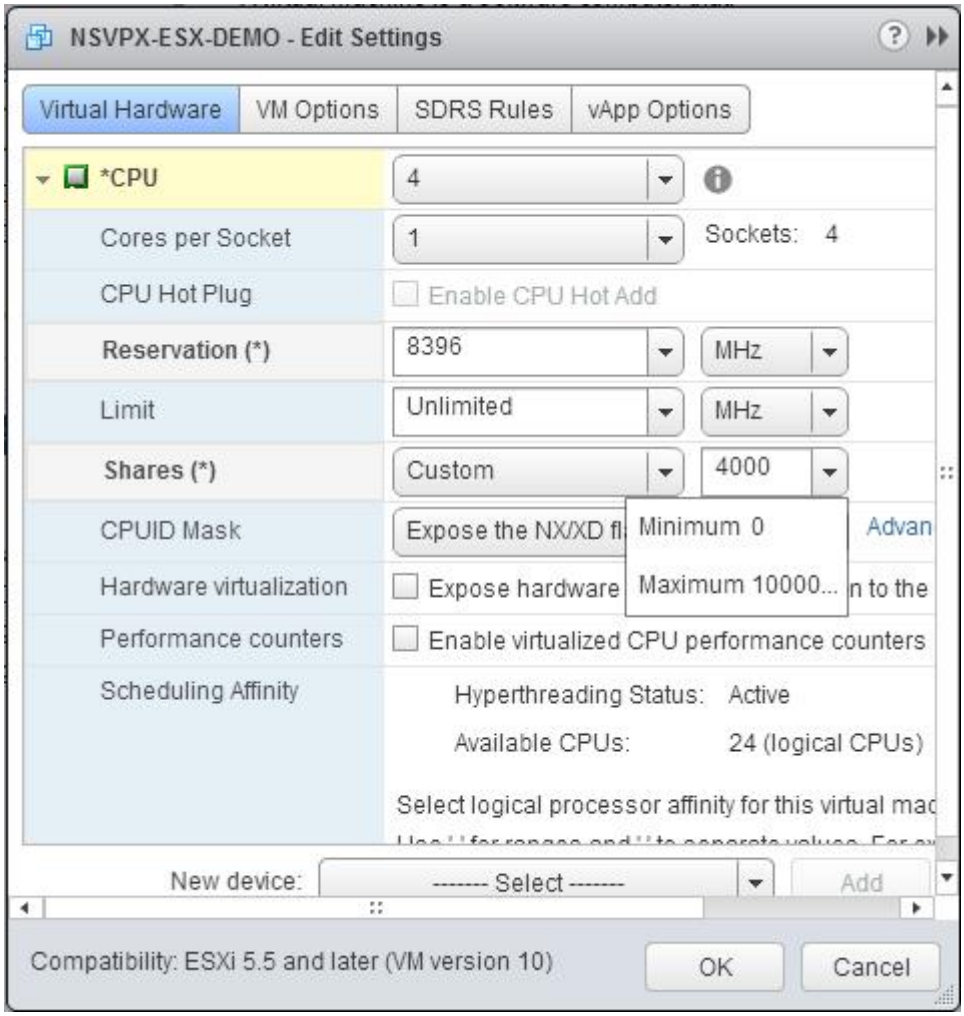
d. Wählen Sie in der Dropdownliste Reservierung die Zahl aus, die als Maximalwert angezeigt wird.



e. Wählen Sie in der Dropdownliste Limit die Zahl aus, die als Maximalwert angezeigt wird.



f. Wählen Sie in den Dropdownlisten Freigaben die Option Benutzerdefiniert und die Zahl, die als Maximalwert angezeigt wird.



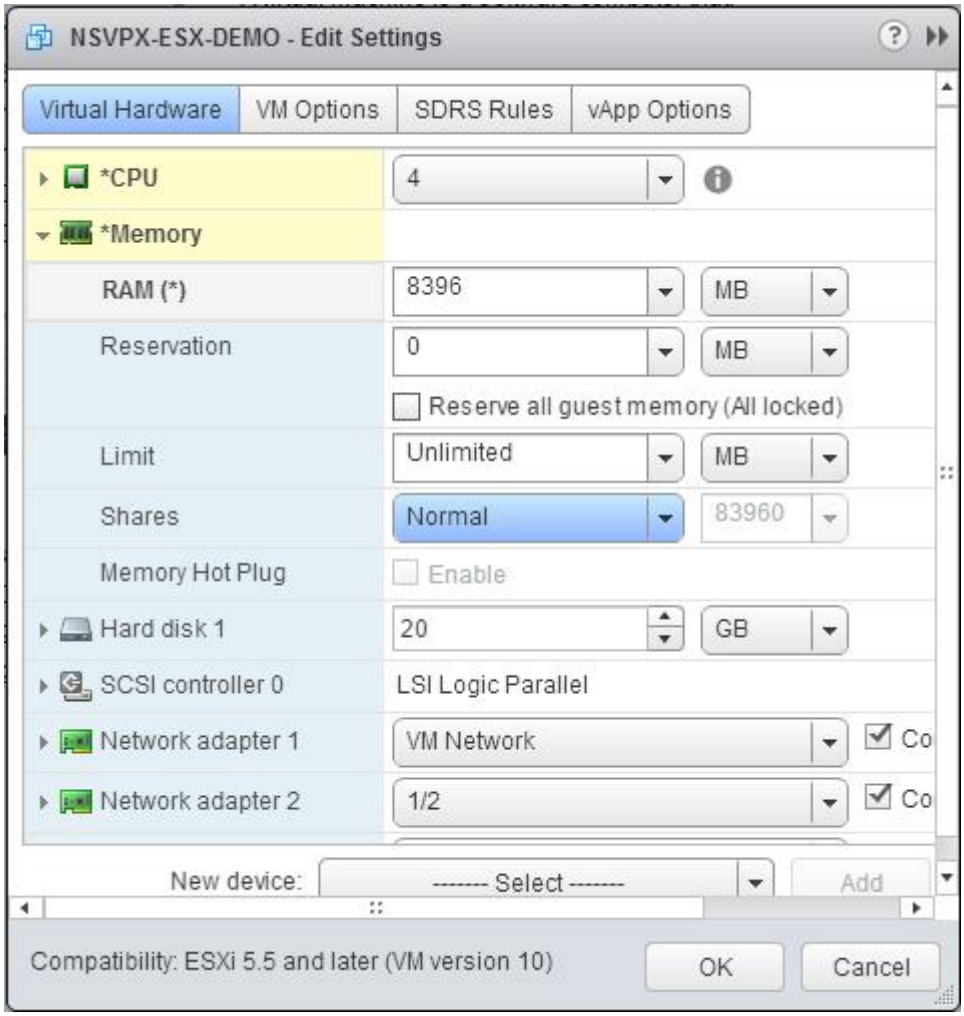
6. Aktualisieren Sie im Abschnitt Speicher Folgendes:

   - Größe des RAM
   - Reservierungen
   - Limit
   - Freigaben

   Legen Sie die Werte wie folgt fest:

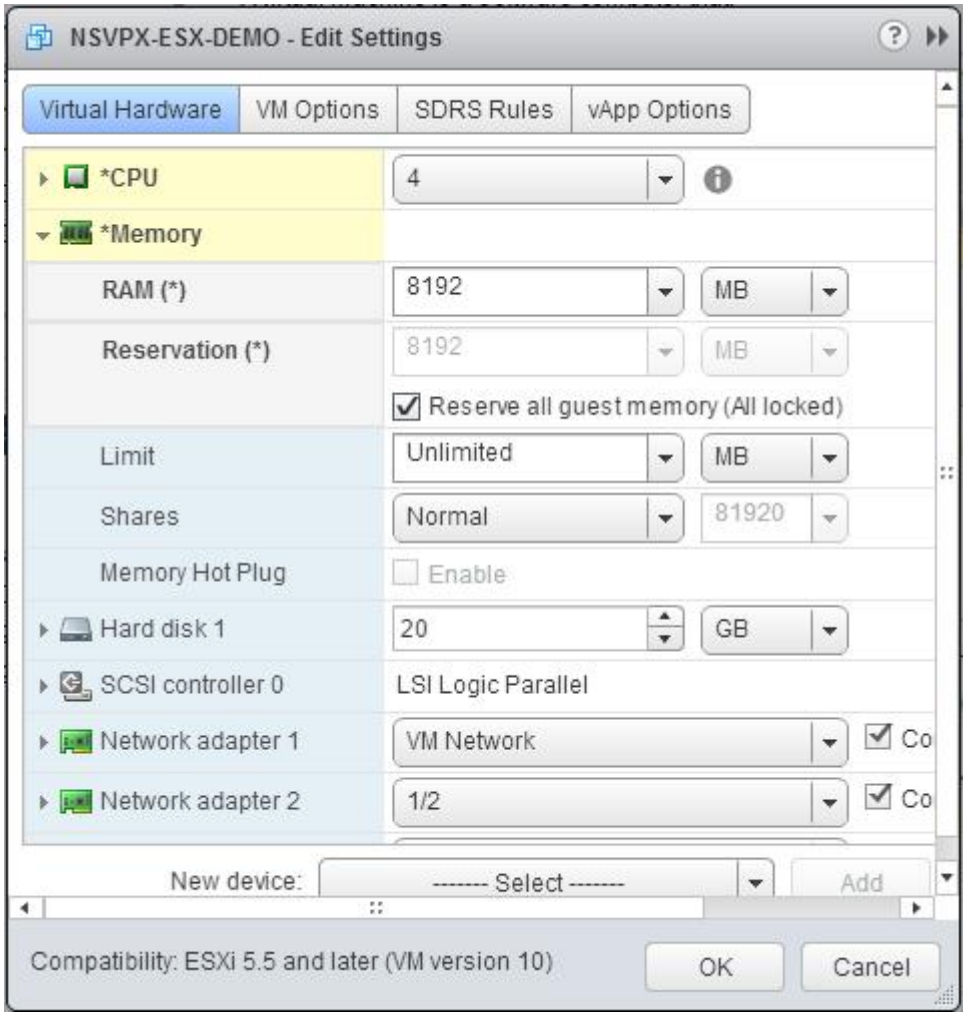
   a. Wählen Sie in der Dropdownliste RAM die Größe des RAM aus. Es muss die Anzahl der vCPUs x 2 GB sein. Wenn die Anzahl der vCPUs beispielsweise 4 beträgt, muss der Arbeitsspeicher 4 x 2 GB = 8 GB betragen.

   Hinweis: Stellen Sie bei einer Advanced- oder Premium-Edition der Citrix ADC VPX Appliance sicher, dass Sie jeder vCPU 4 GB RAM zuweisen. Wenn beispielsweise die Anzahl der vCPU 4 ist, dann RAM = 4 x 4 GB = 16 GB.

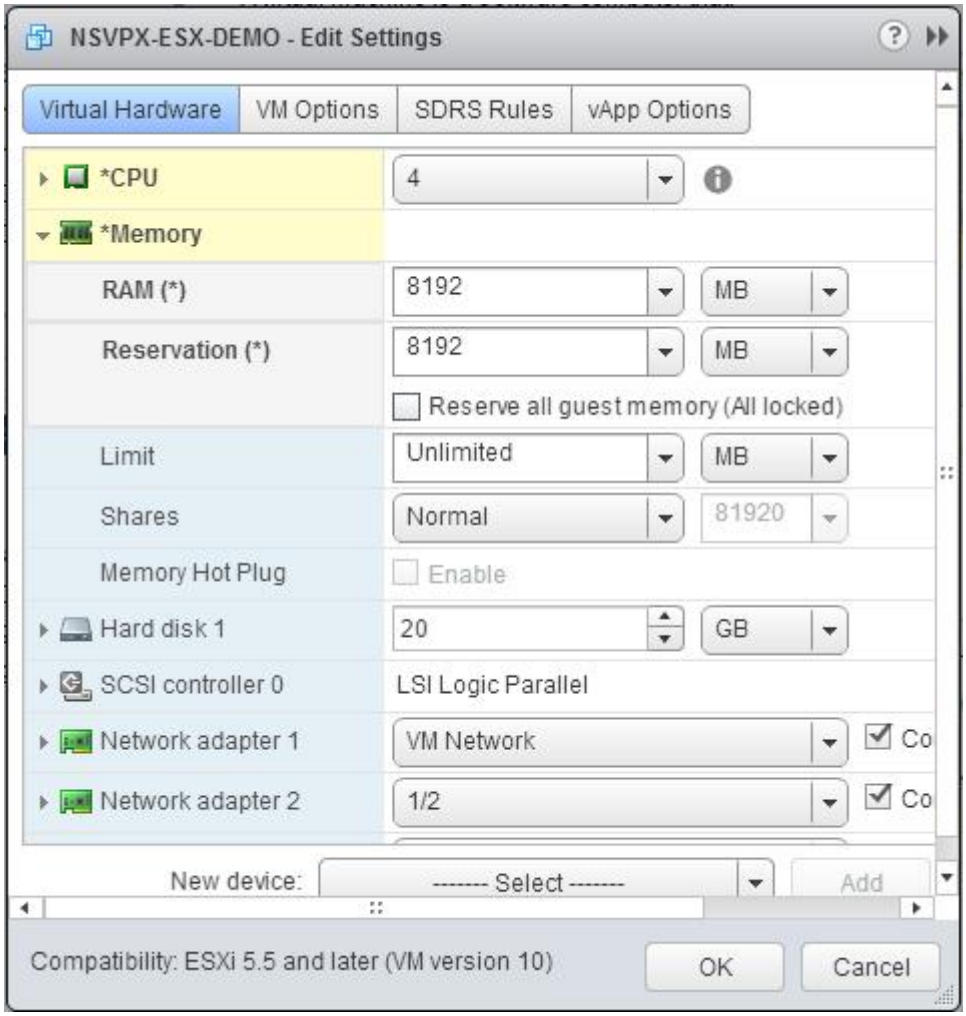


b. Geben Sie in der Dropdownliste Reservierung den Wert für die Speicherreservierung ein, und aktivieren Sie das Kontrollkästchen Alle Gastspeicher reservieren (Alle gesperrt) . Die Speicherreservierung muss die Anzahl der vCPUs x 2 GB sein. Wenn die Anzahl der vCPUs beispielsweise 4 beträgt, muss die Speicherreservierung 4 x 2 GB = 8 GB betragen.

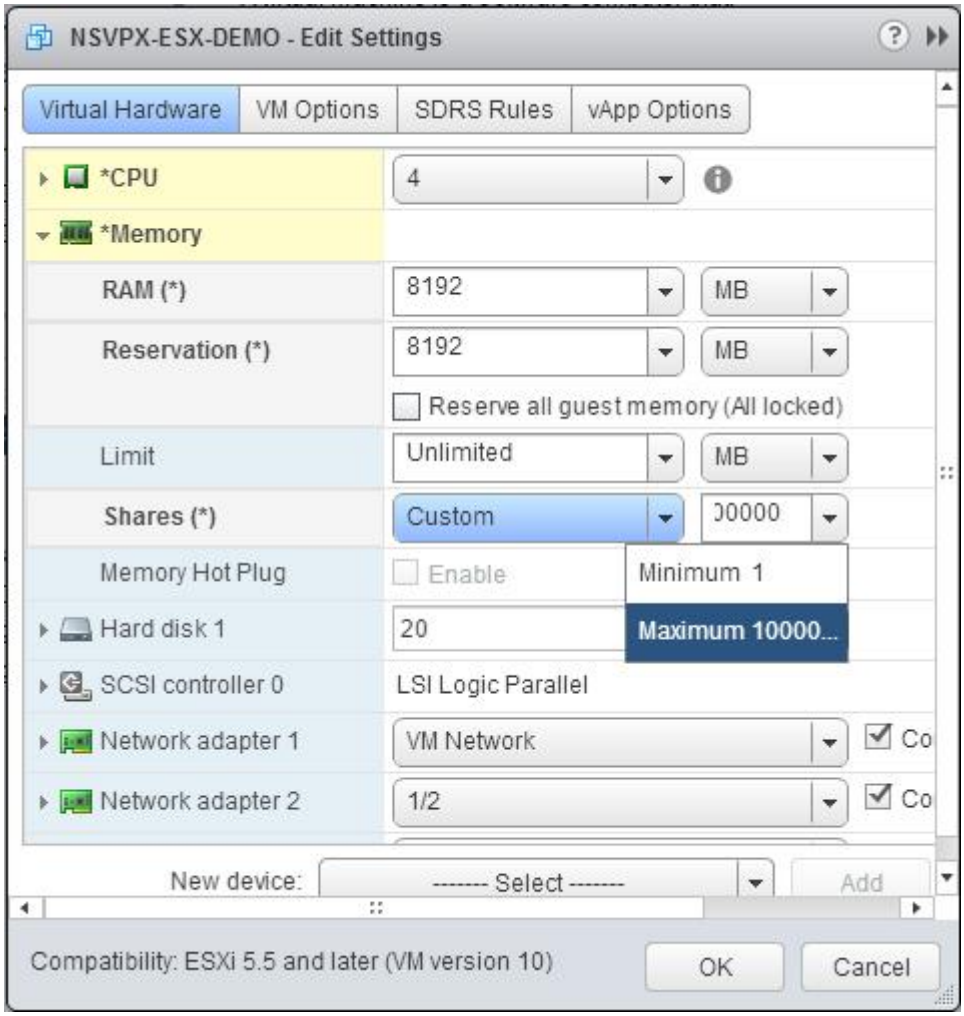
Hinweis: Stellen Sie bei einer Advanced- oder Premium-Edition der Citrix ADC VPX Appliance sicher, dass Sie jeder vCPU 4 GB RAM zuweisen. Wenn beispielsweise die Anzahl der vCPU 4 ist, dann RAM = 4 x 4 GB = 16 GB.



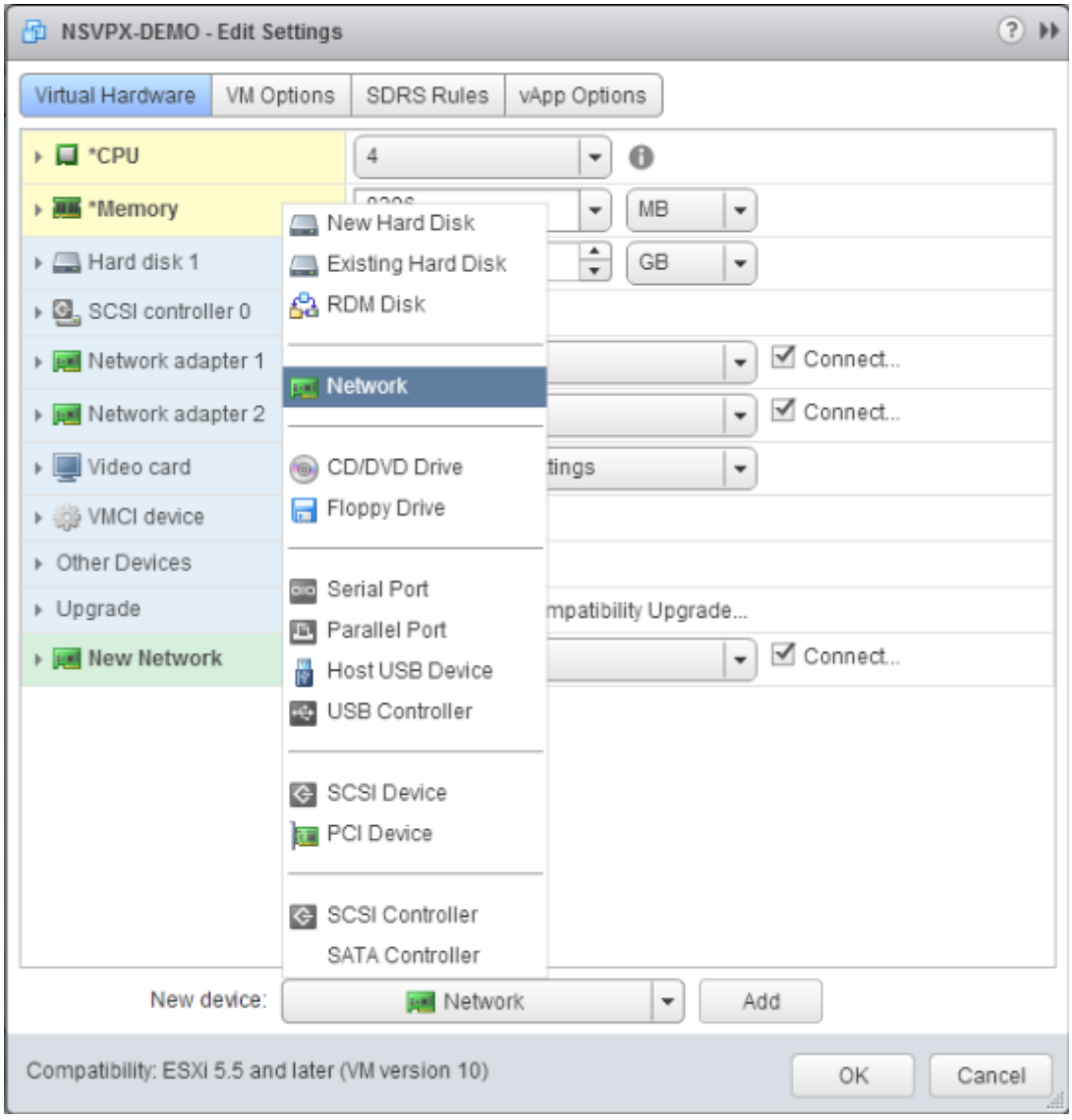
c. Wählen Sie in der Dropdownliste Limit die Zahl aus, die als Maximalwert angezeigt wird.



d. Wählen Sie in den Dropdownlisten Freigaben die Option Benutzerdefiniert und die Zahl, die als Maximalwert angezeigt wird.



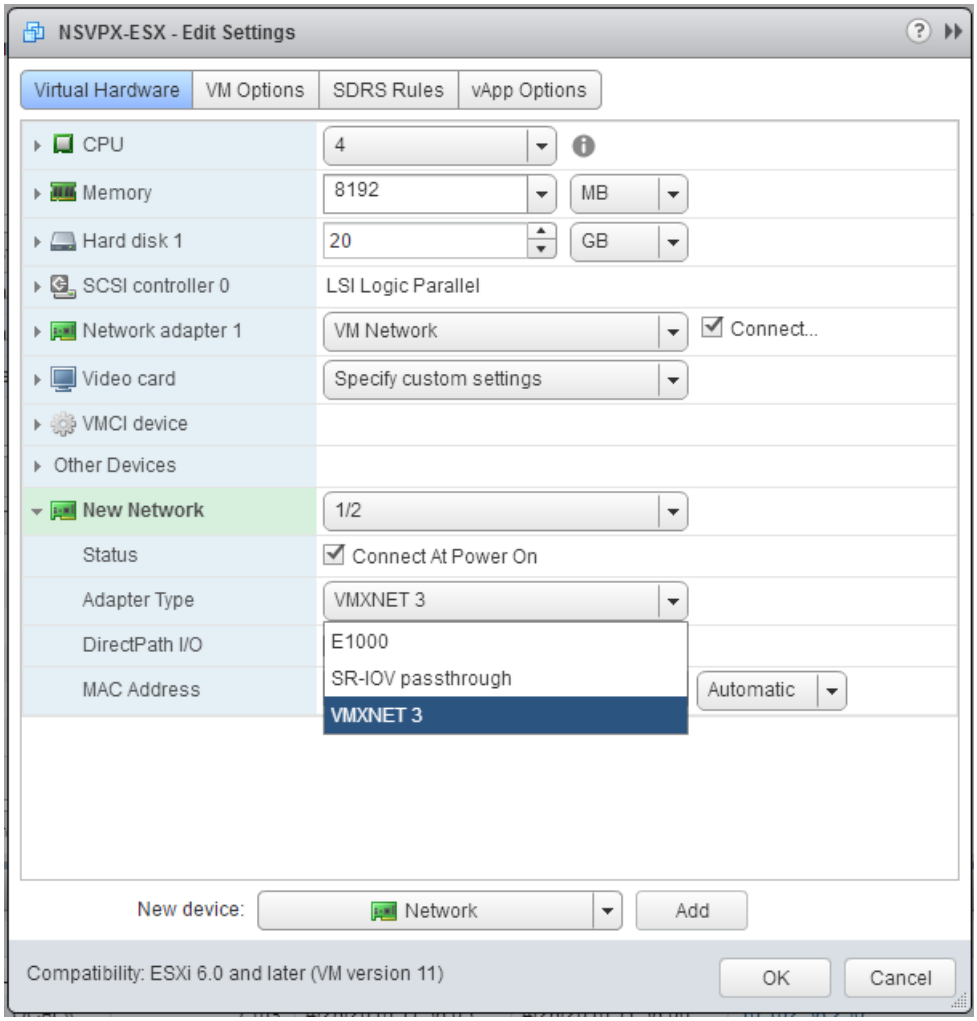
7. Fügen Sie eine VMXNET3-Netzwerkschnittstelle hinzu. Wählen Sie in der Dropdownliste Neues Gerät die Option Netzwerk aus und klicken Sie auf Hinzufügen.



8. Wählen Sie im Abschnitt Neues Netzwerk aus der Dropdownliste die Netzwerkschnittstelle aus, und führen Sie die folgenden Schritte aus:

   a. Wählen Sie in der Dropdownliste Adaptertyp die Option VMXNET3 aus.

> **Wichtig**
>
> Die standardmäßige E1000-Netzwerkschnittstelle und VMXNET3 können nicht koexistieren. Stellen Sie sicher, dass Sie die E1000-Netzwerkschnittstelle entfernen und VMXNET3 (0/1) als Verwaltungsschnittstelle verwenden.



9. Klicken Sie auf OK.
10. Schalten Sie die Citrix ADC VPX-Instanz ein.
11. Sobald die Citrix ADC VPX-Instanz eingeschaltet ist, können Sie die Konfiguration mithilfe des folgenden Befehls überprüfen:

    ```
    show interface summary
    ```

Die Ausgabe muss alle von Ihnen konfigurierten Schnittstellen anzeigen:

```
1 > show interface summary
2 ---------------------------------------------------------------------------

3       Interface  MTU        MAC                Suffix
4 ---------------------------------------------------------------------------
```



```
1     0/1        1500       00:0c:29:89:1d:0e    NetScaler Vir...rface,
      VMXNET3
2     1/1        9000       00:0c:29:89:1d:18    NetScaler Vir...rface,
      VMXNET3
3     1/2        9000       00:0c:29:89:1d:22    NetScaler Vir...rface,
      VMXNET3
4     LO/1       9000       00:0c:29:89:1d:0e    Netscaler Loopback
    interface
```

> **Hinweis:**
>
> Nachdem Sie eine VMXNET3-Schnittstelle hinzugefügt und die Citrix ADC VPX Appliance neu gestartet haben, ändert der VMware ESX-Hypervisor möglicherweise die Reihenfolge, in der die NIC der VPX-Appliance angezeigt wird. Daher bleibt der Netzwerkadapter 1 möglicherweise nicht immer 0/1, was zu einem Verlust der Verwaltungskonnektivität mit der VPX-Appliance führt. Um dieses Problem zu vermeiden, ändern Sie das virtuelle Netzwerk des Netzwerkadapters entsprechend.
>
> Dies ist eine Einschränkung des VMware ESX Hypervisors.

Konfigurieren einer Citrix ADC VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnittstelle

October 5, 2021

Nachdem Sie die Citrix ADC VPX-Instanz auf VMware ESX installiert und konfiguriert haben, können Sie den VMware vSphere Webclient verwenden, um die virtuelle Appliance für die Verwendung von Single-Root-I/O-V-Virtualisierungs-Netzwerkschnittstellen (SR-IOV) zu konfigurieren.

Einschränkungen

Für Citrix ADC VPX, die mit SR-IOV-Netzwerkschnittstelle konfiguriert ist, gelten folgende Einschränkungen:

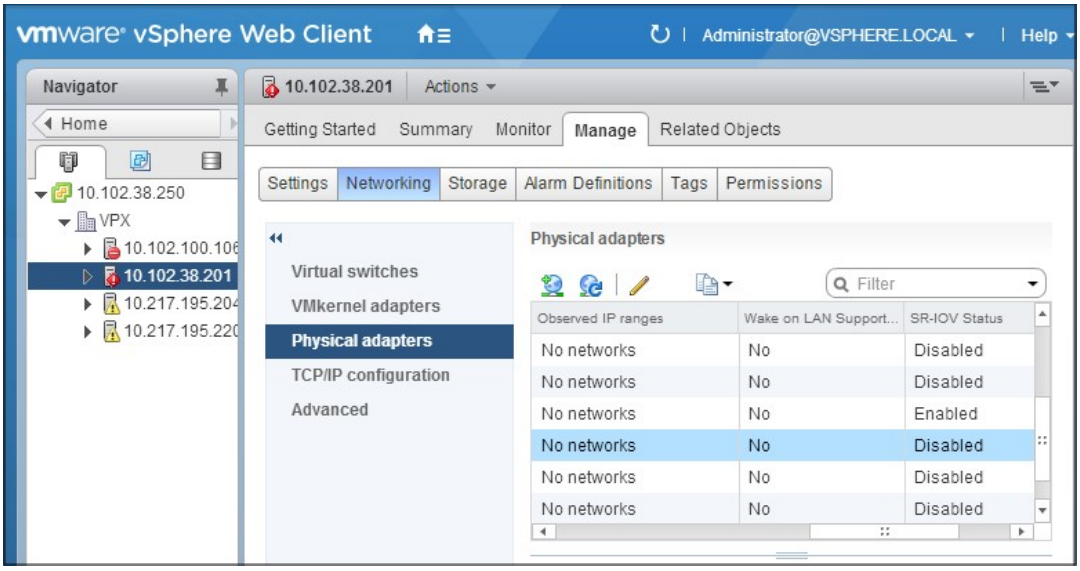
- Die folgenden Funktionen werden auf SR-IOV-Schnittstellen, die die Intel 82599 10G-NIC auf ESX VPX verwenden, nicht unterstützt:
  - L2-Modus Umschaltung
  - Statische Link-Aggregation und LACP
  - Clustering
  - Adminpartitionierung [Freigegebener VLAN-Modus]
  - Hochverfügbarkeit [Aktiv - Aktiver Modus]

  - Jumbo-Rahmen
  - IPv6
- Die folgenden Funktionen werden auf der SR-IOV-Schnittstelle mit einer Intel 82599 10G-NIC auf KVM VPX nicht unterstützt:
  - Statische Link-Aggregation und LACP
  - L2-Modus Umschaltung
  - Clustering
  - Adminpartitionierung [Freigegebener VLAN-Modus]
  - Hochverfügbarkeit [Aktiv — Aktiver Modus]
  - Jumbo-Rahmen
  - IPv6
  - Die VLAN-Konfiguration auf Hypervisor für SR-IOV VF-Schnittstelle über `ip link` Befehl wird nicht unterstützt

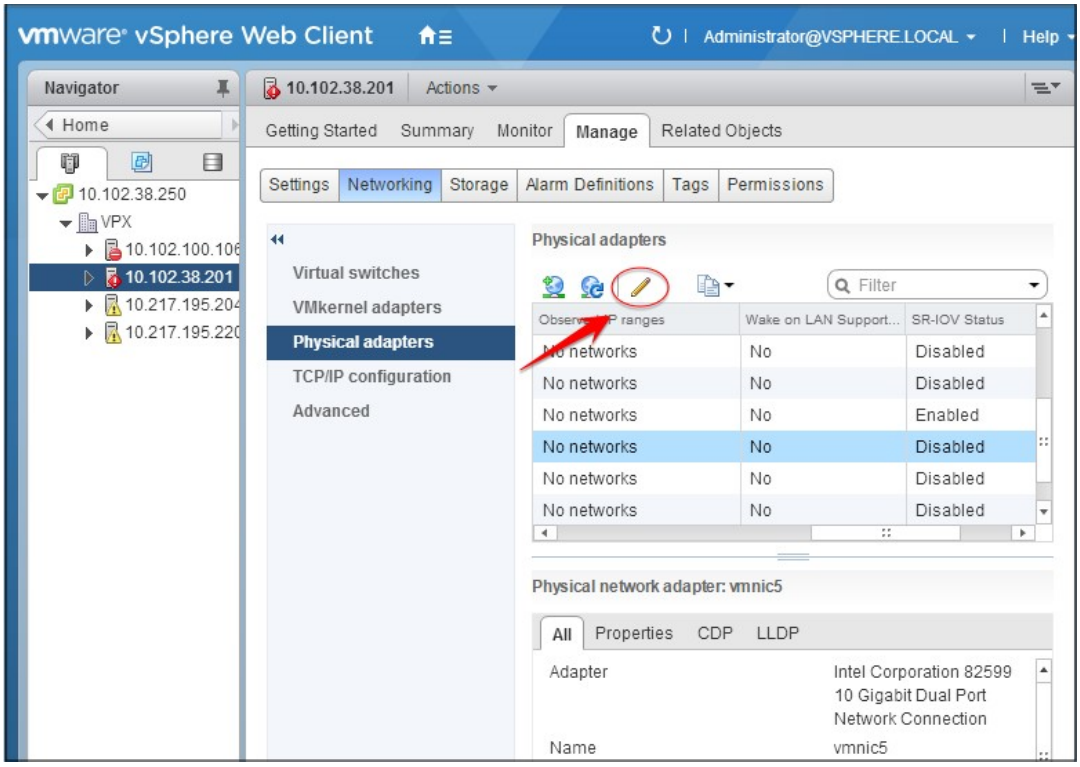
Voraussetzung

Stellen Sie sicher, dass Sie:

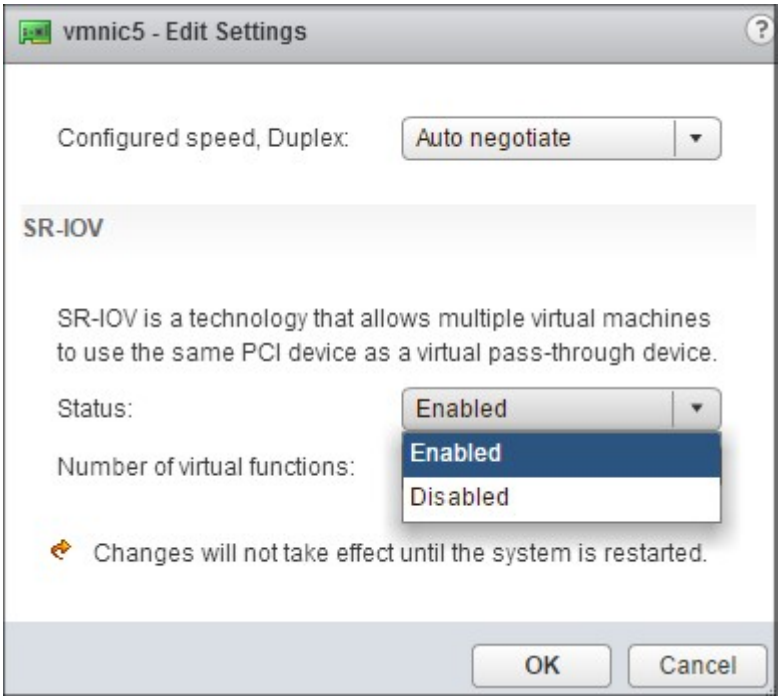
- Fügen Sie die Intel 82599 NIC (NIC) zum ESX-Host hinzu. IXGBE Treiberversion 3.7.13.7.14iov wird empfohlen.
- Aktivieren Sie SR-IOV auf dem physischen Hostadapter wie folgt:
  1. Navigieren Sie im vSphere Web Client zum Host.
  2. Wählen Sie auf der Registerkarte **Verwalten > Netzwerk** die Option **Physische Adapter** aus. Das Feld SR-IOV Status zeigt an, ob ein physischer Adapter SR-IOV unterstützt.



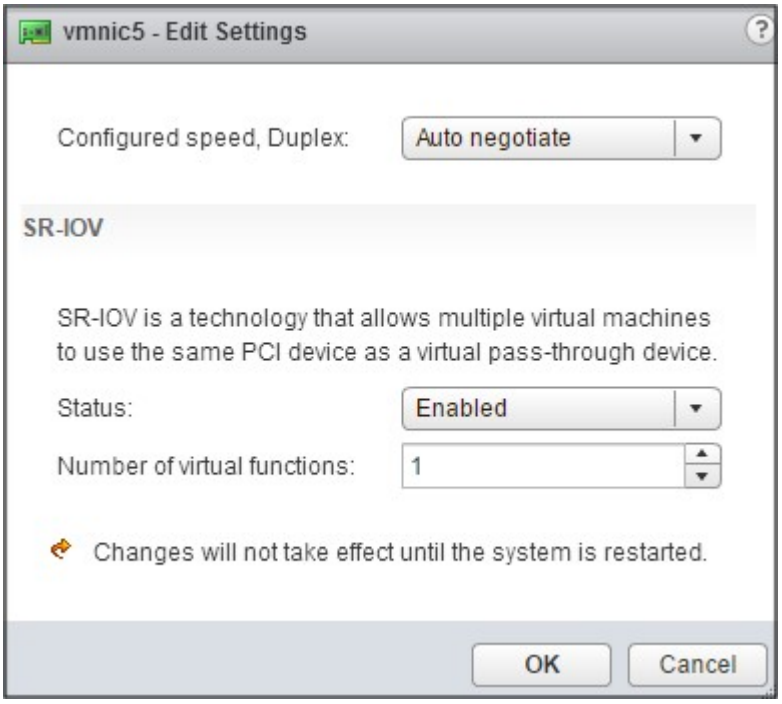
  3. Wählen Sie den physischen Adapter aus, und klicken Sie dann auf das Stiftsymbol, um das Dialogfeld **Einstellungen bearbeiten** zu öffnen.



4. Wählen Sie unter SR-IOV in der Dropdownliste **Status** die Option **Aktiviert** aus.



5. Geben Sie im Feld **Anzahl der virtuellen Funktionen** die Anzahl der virtuellen Funktionen ein, die Sie für den Adapter konfigurieren möchten.



6. Klicken Sie auf **OK**.
7. Starten Sie den Host neu.

- Erstellen Sie einen Distributed Virtual Switch (DVS) und `Portgroups`. Anweisungen finden Sie in der VMware Dokumentation.

  > **Hinweis:**
  >
  > Citrix hat die SR-IOV-Konfiguration `Portgroups` nur auf DVS qualifiziert.

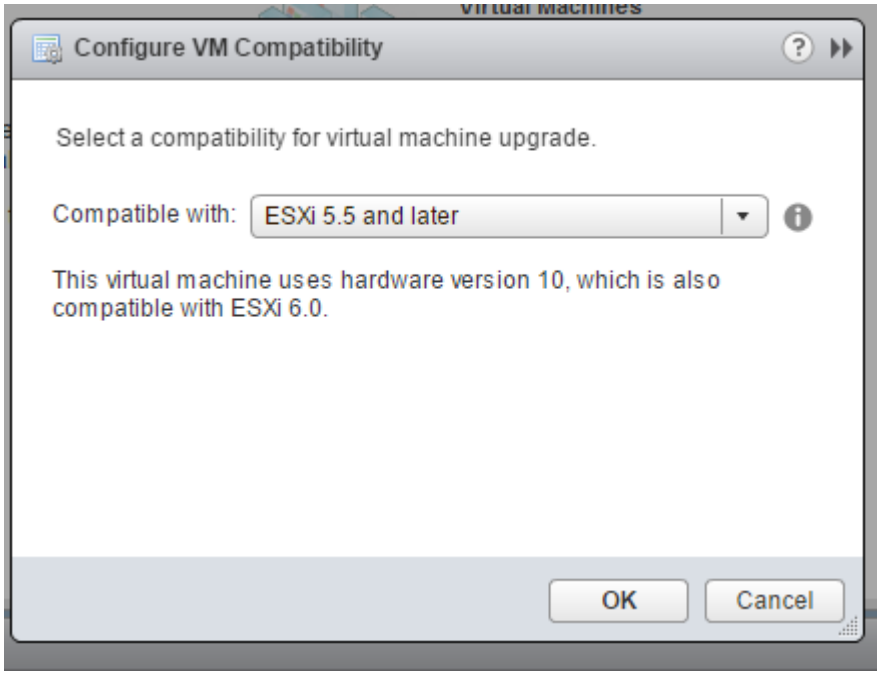
So konfigurieren Sie Citrix ADC VPX-Instanzen für die Verwendung der SR-IOV-Netzwerkschnittstelle mithilfe von VMware vSphere Web Client:

1. Wählen Sie im vSphere Web Client **Hosts und Cluster**aus.
2. Aktualisieren Sie die Kompatibilitätseinstellung der Citrix ADC VPX-Instanz wie folgt auf ESX 5.5 oder höher:

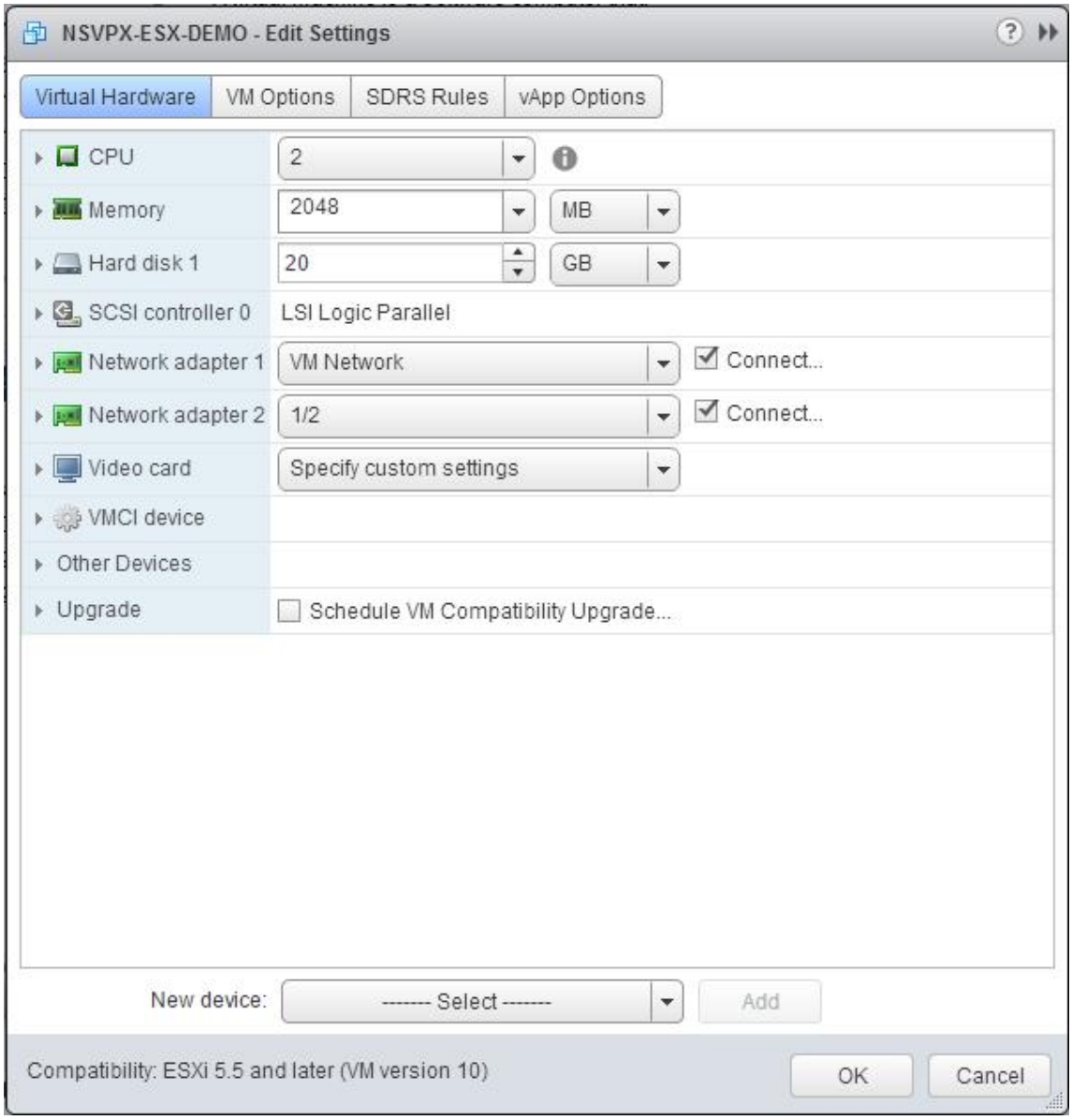
   a. Schalten Sie die Citrix ADC VPX-Instanz aus.

   b. Klicken Sie mit der rechten Maustaste auf die Citrix ADC VPX Instanz, und wählen Sie **Kompatibilität > VM-Kompatibilität aktualisieren**.

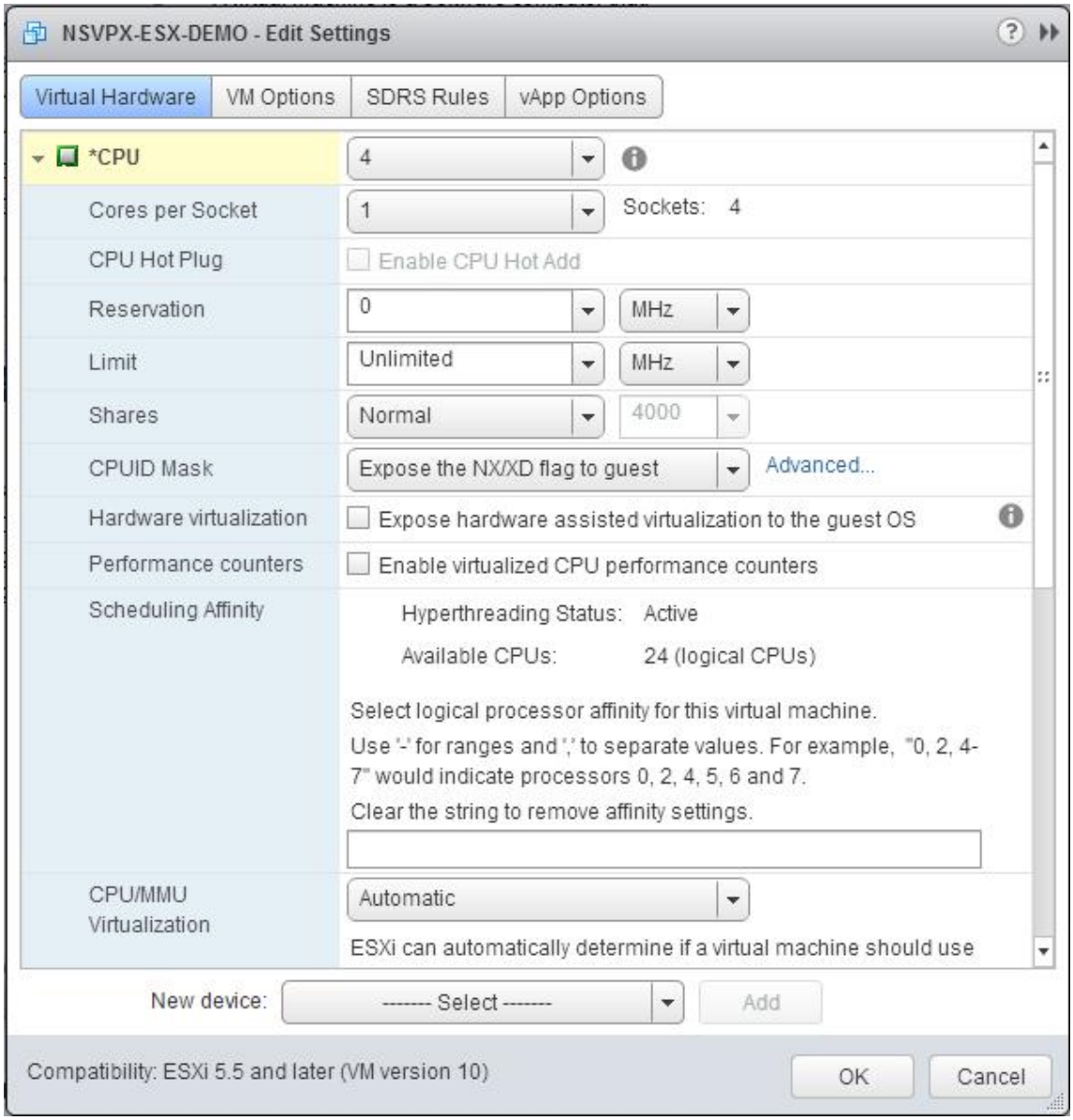
   c. Wählen Sie im Dialogfeld **VM-Kompatibilität konfigurieren** die Option **ESXi 5.5 und höher** aus der Dropdownliste **Kompatibel mit** aus, und klicken Sie auf **OK**.



3. Klicken Sie mit der rechten Maustaste auf die Citrix ADC VPX Instanz, und klicken Sie auf **Einstellungen bearbeiten**.



4. Klicken Sie im Dialogfeld **<virtual_appliance> - Einstellungen bearbeiten** auf den Abschnitt **CPU**.



5. Aktualisieren Sie im Abschnitt **CPU** die folgenden Einstellungen:

   - CPU-Anzahl
   - Anzahl der Sockets
   - Reservierungen
   - Limit
   - Freigaben

   Legen Sie die Werte wie folgt fest:

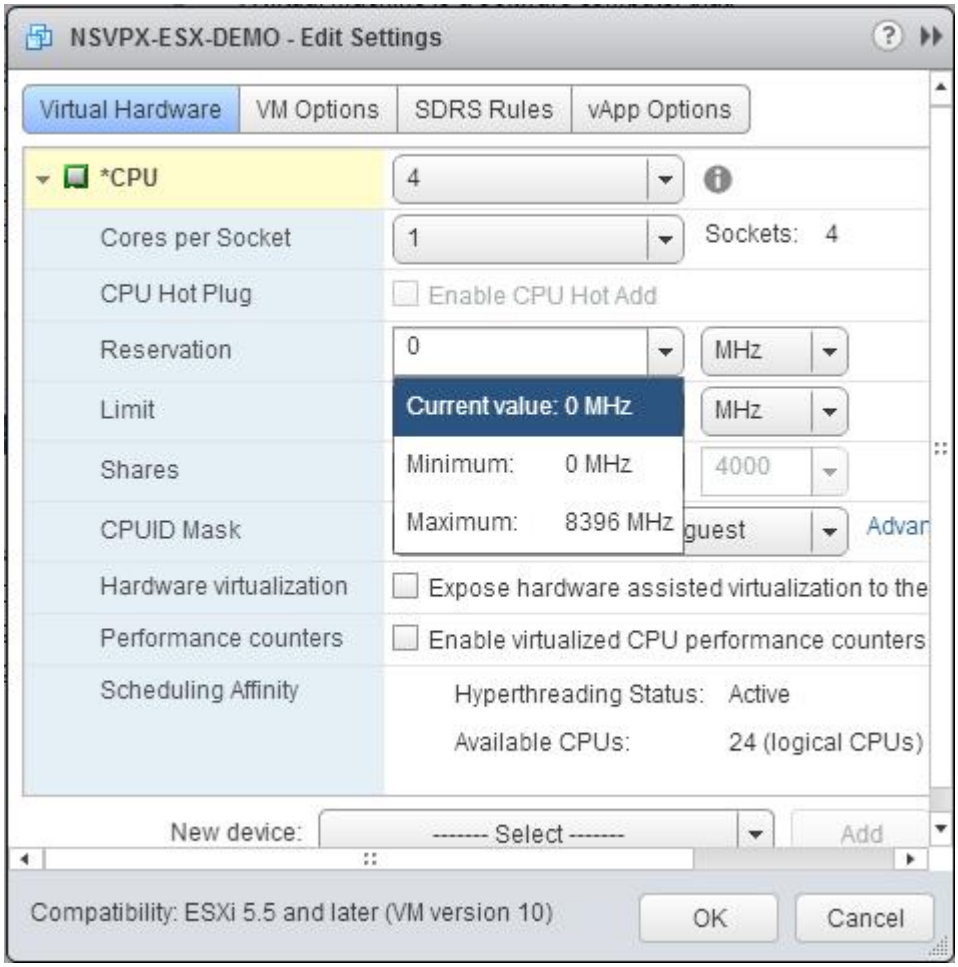
   a. Wählen Sie in der Dropdownliste **CPU** die Anzahl der CPUs aus, die der virtuellen Appliance zugewiesen werden sollen.

   b. Wählen Sie in der Dropdownliste **Kerne pro Sockel** die Anzahl der Sockets aus.

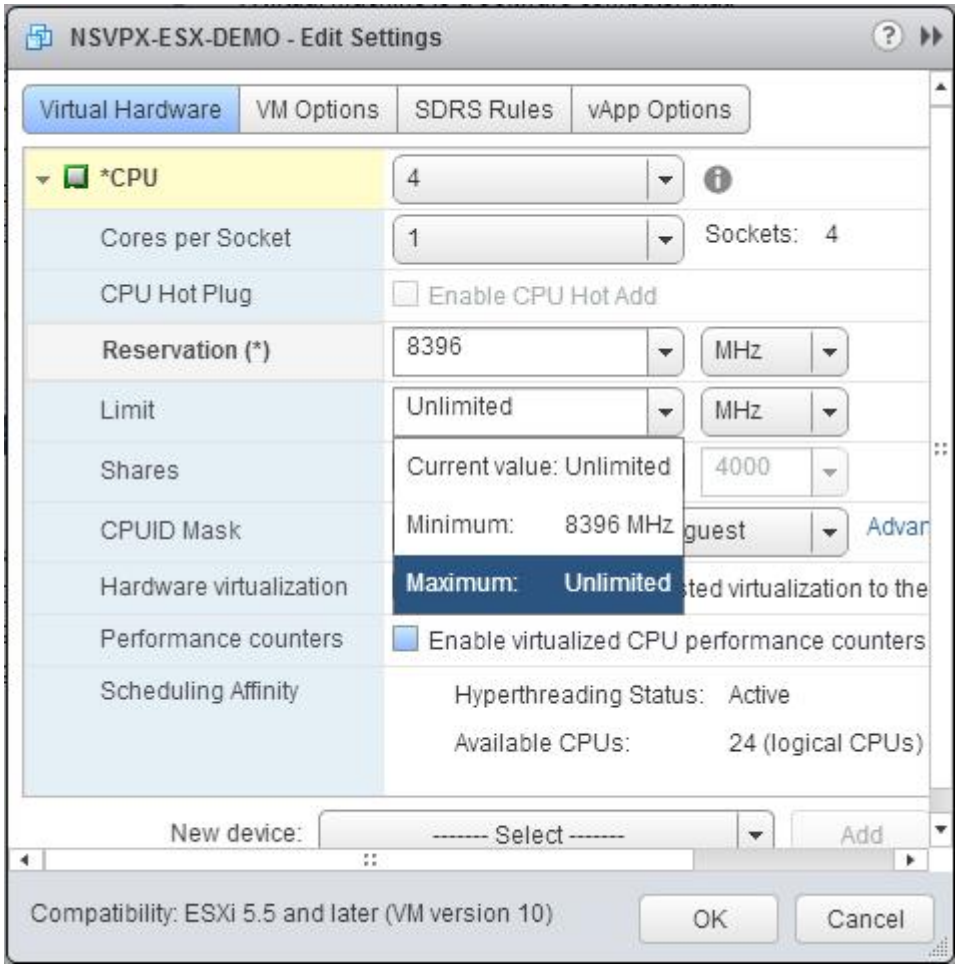
c. (Optional) Aktivieren oder deaktivieren Sie im Feld **CPU Hot Plug** das Kontrollkästchen **CPU Hot Add aktivieren** .

Hinweis: Citrix empfiehlt, den Standard zu akzeptieren (deaktiviert).

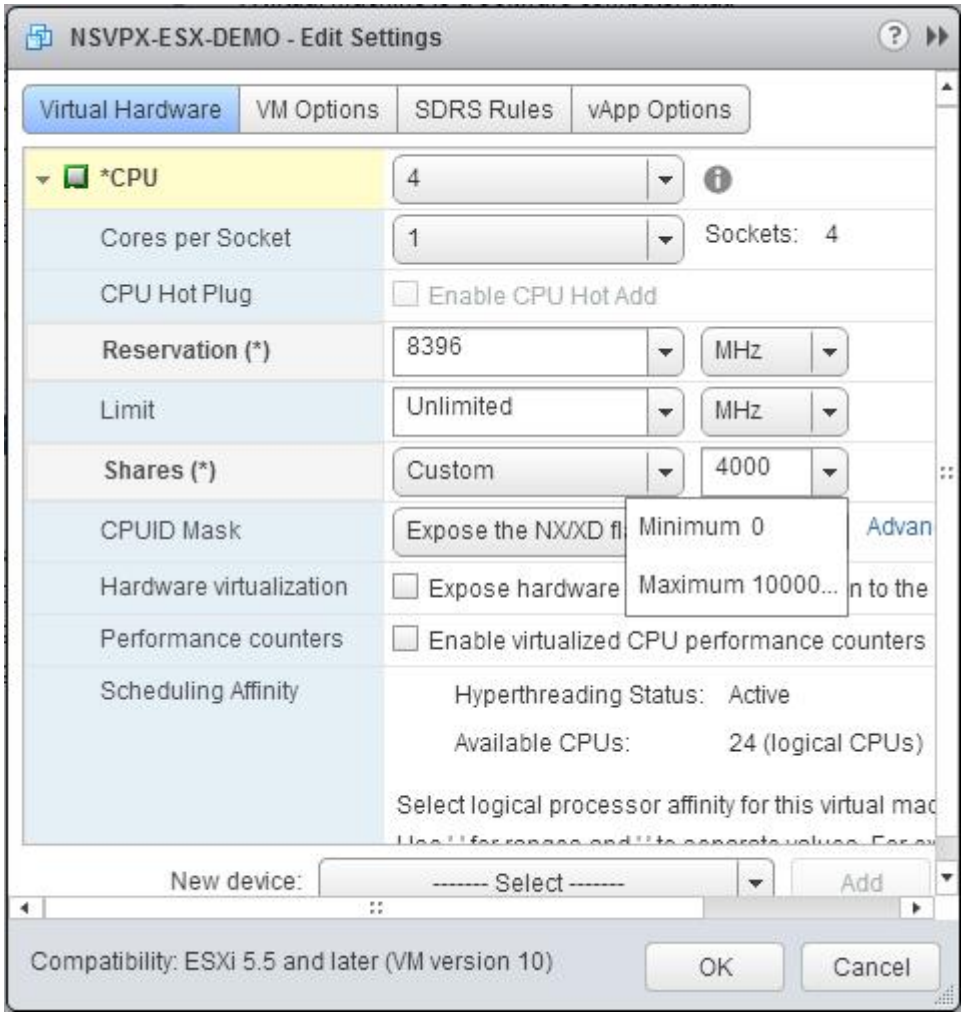
d. Wählen Sie in der Dropdownliste **Reservierung** die Zahl aus, die als Maximalwert angezeigt wird.



e. Wählen Sie in der Dropdownliste **Limit** die Zahl aus, die als Maximalwert angezeigt wird.



f. Wählen Sie in den Dropdownlisten **Freigaben** die Option **Benutzerdefiniert** und die Zahl, die als Maximalwert angezeigt wird.



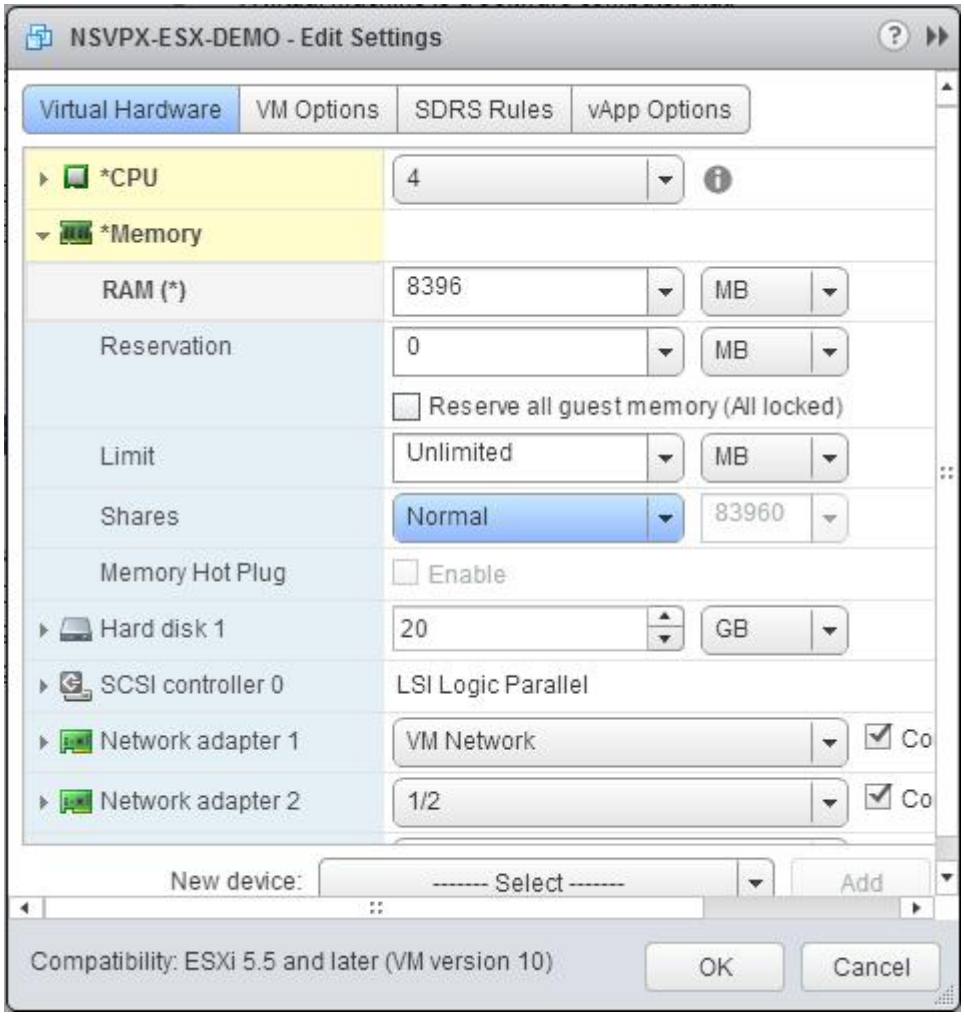
6. Aktualisieren Sie im Abschnitt **Speicher** die folgenden Einstellungen:

   - Größe des RAM
   - Reservierungen
   - Limit
   - Freigaben

   Legen Sie die Werte wie folgt fest:

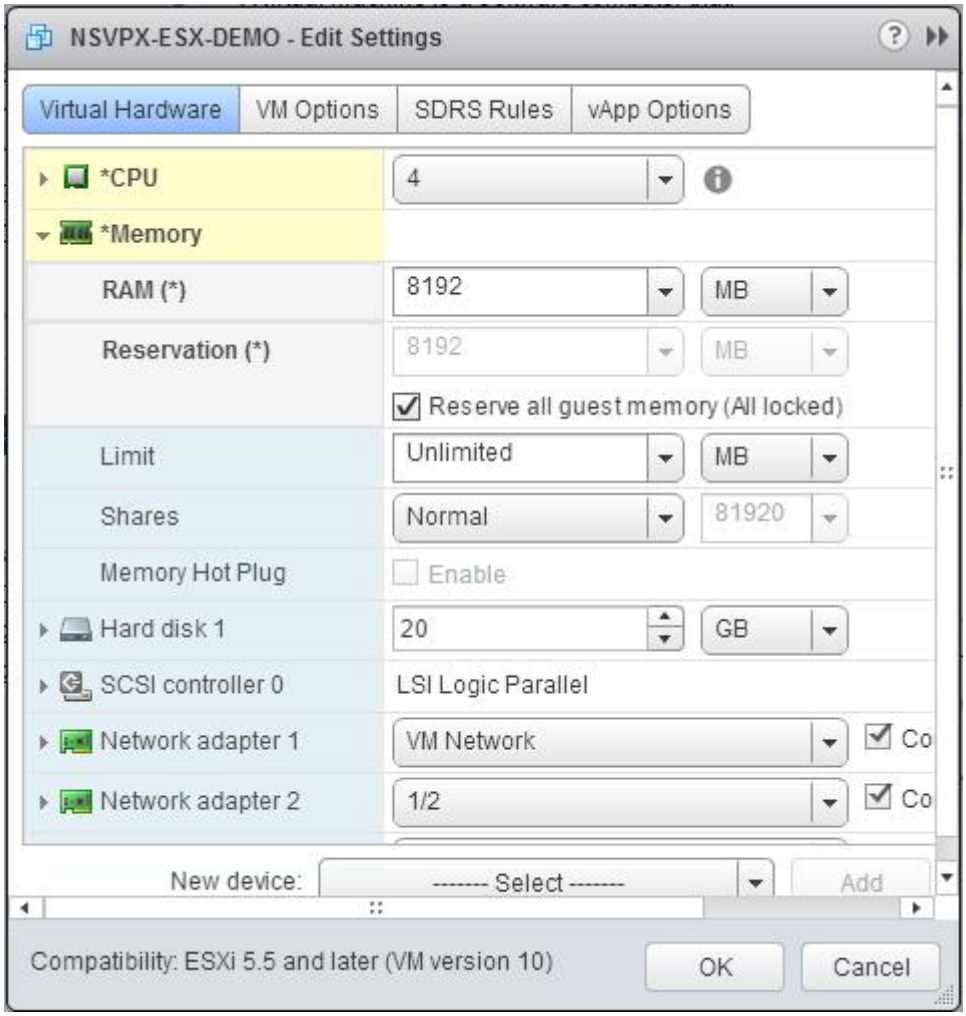
   a. Wählen Sie in der Dropdownliste **RAM** die Größe des RAM aus. Es muss die Anzahl der vCPUs x 2 GB sein. Wenn beispielsweise die Anzahl der vCPU 4 ist, dann RAM = 4 x 2 GB = 8 GB.

   Hinweis: Stellen Sie für die Advanced- oder Premium-Edition der Citrix ADC VPX Appliance sicher, dass Sie jeder vCPU 4 GB RAM zuweisen. Wenn beispielsweise die Anzahl der vCPU 4 ist, dann RAM = 4 x 4 GB = 16 GB.

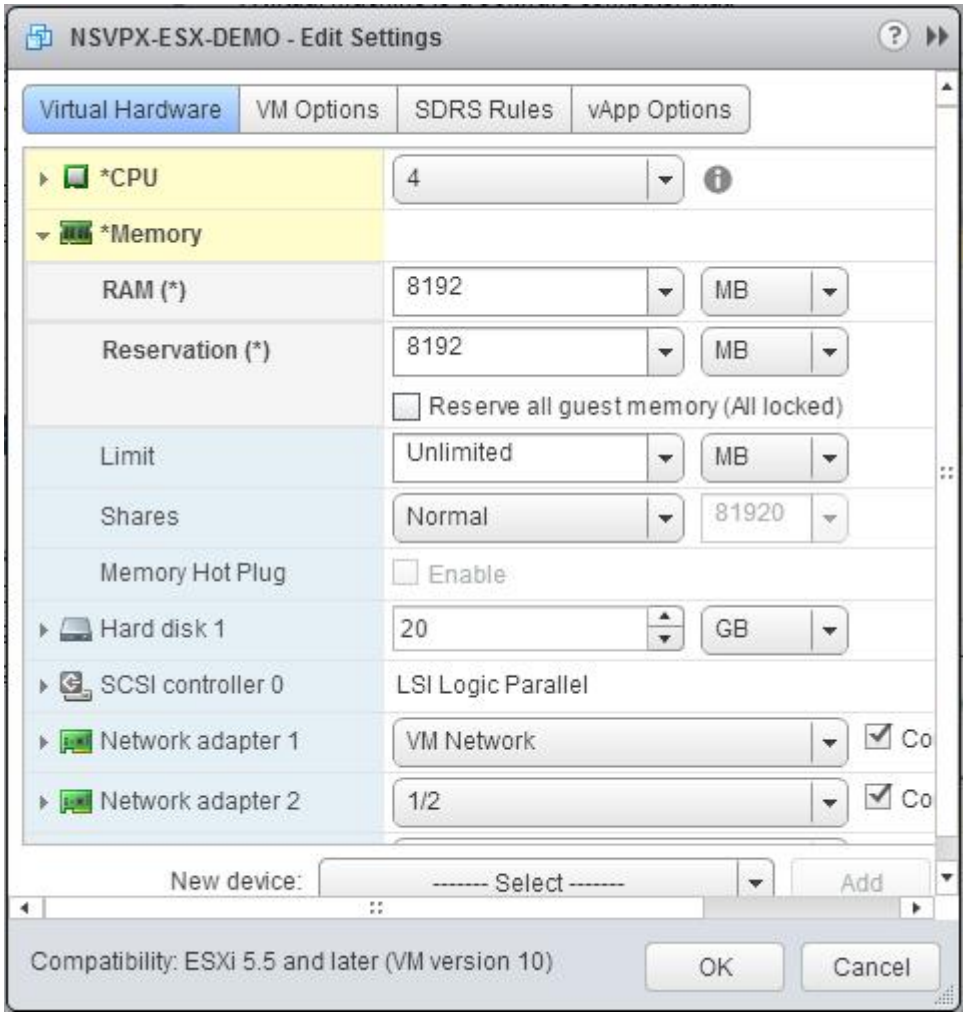


b. Geben Sie in der Dropdownliste **Reservierung** den Wert für die Speicherreservierung ein, und aktivieren Sie das Kontrollkästchen **Alle Gastspeicher reservieren (Alle gesperrt)** . Die Speicherreservierung muss die Anzahl der vCPUs x 2 GB sein. Wenn die Anzahl der vCPUs beispielsweise 4 beträgt, muss die Speicherreservierung 4 x 2 GB = 8 GB betragen.

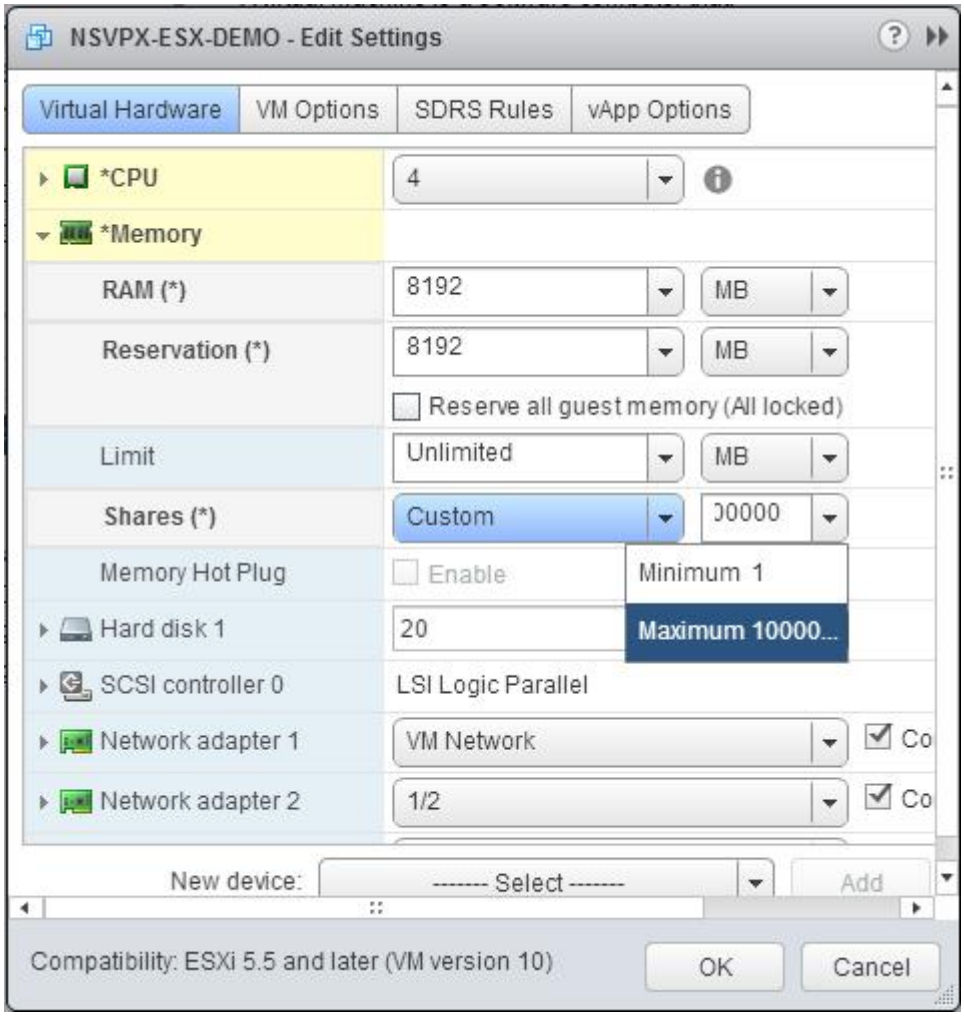
Hinweis: Stellen Sie für die Advanced- oder Premium-Edition der Citrix ADC VPX Appliance sicher, dass Sie jeder vCPU 4 GB RAM zuweisen. Wenn beispielsweise die Anzahl der vCPU 4 ist, dann RAM = 4 x 4 GB = 16 GB.



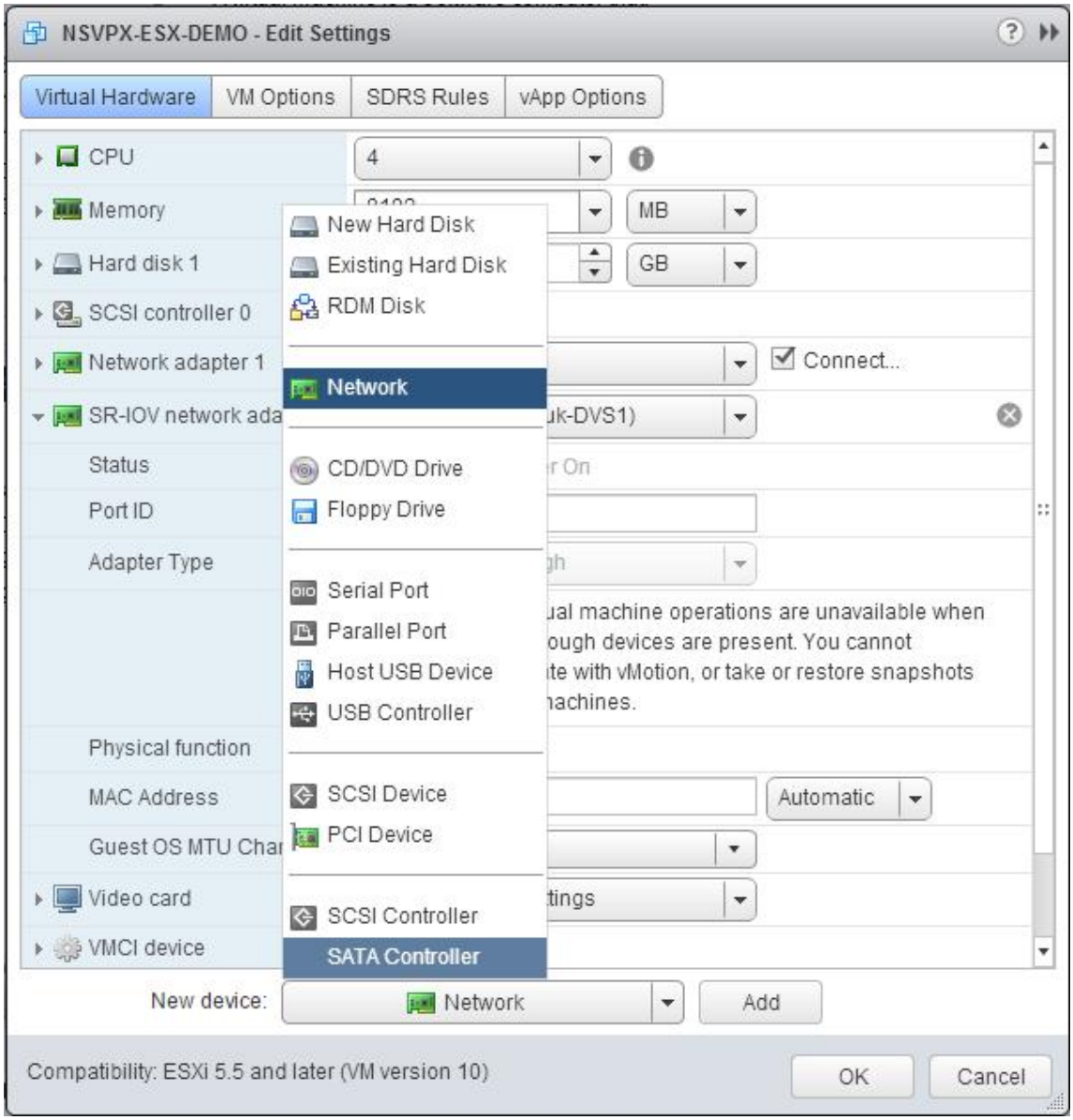
c. Wählen Sie in der Dropdownliste **Limit** die Zahl aus, die als Maximalwert angezeigt wird.



d. Wählen Sie in den Dropdownlisten **Freigaben** die Option **Benutzerdefiniert** aus, und wählen Sie die Zahl aus, die als Maximalwert angezeigt wird.

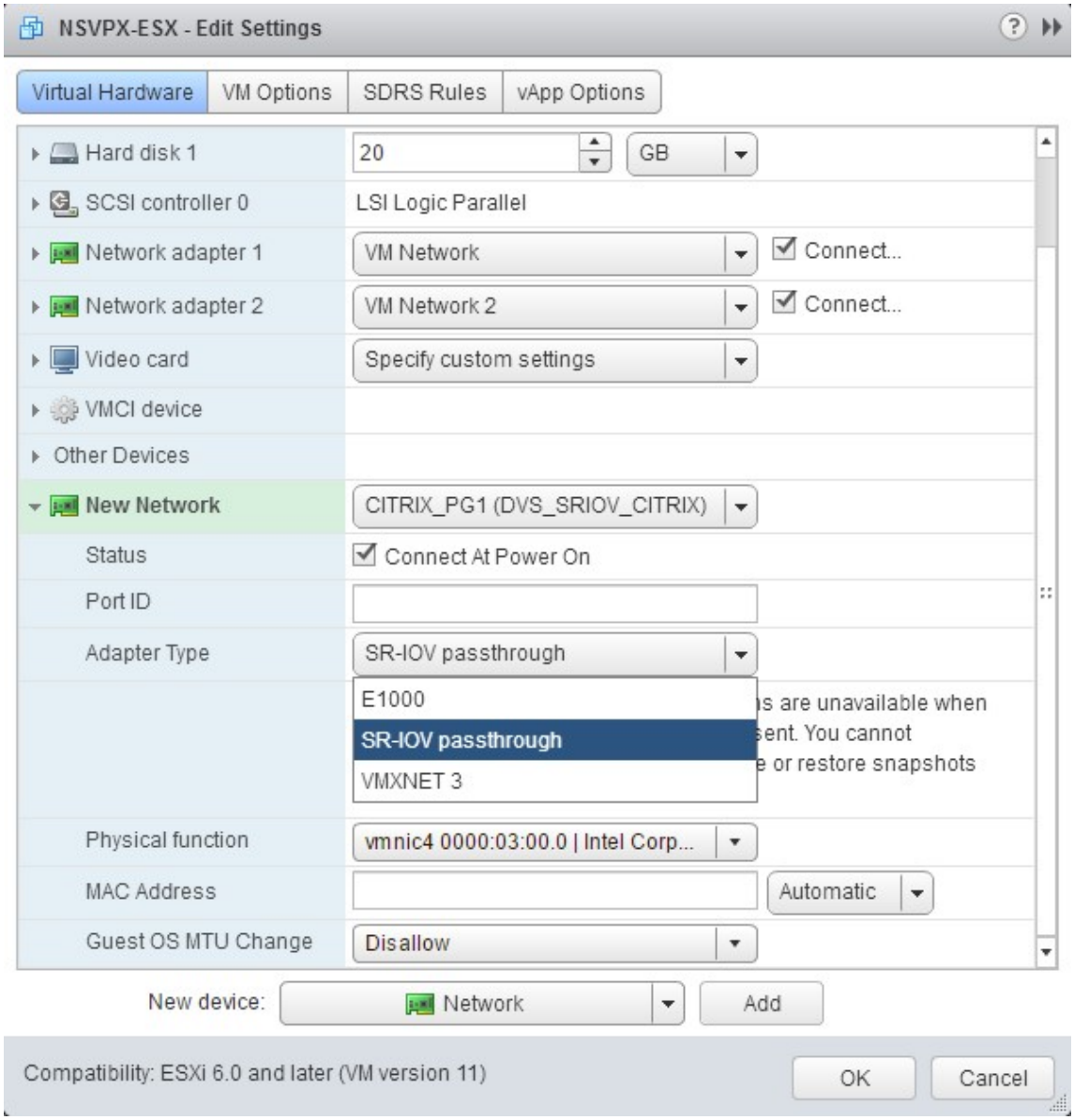


7. Fügen Sie eine SR-IOV-Netzwerkschnittstelle hinzu. Wählen Sie in der Dropdownliste **Neues Gerät** die Option **Netzwerk** aus und klicken Sie auf **Hinzufügen**.

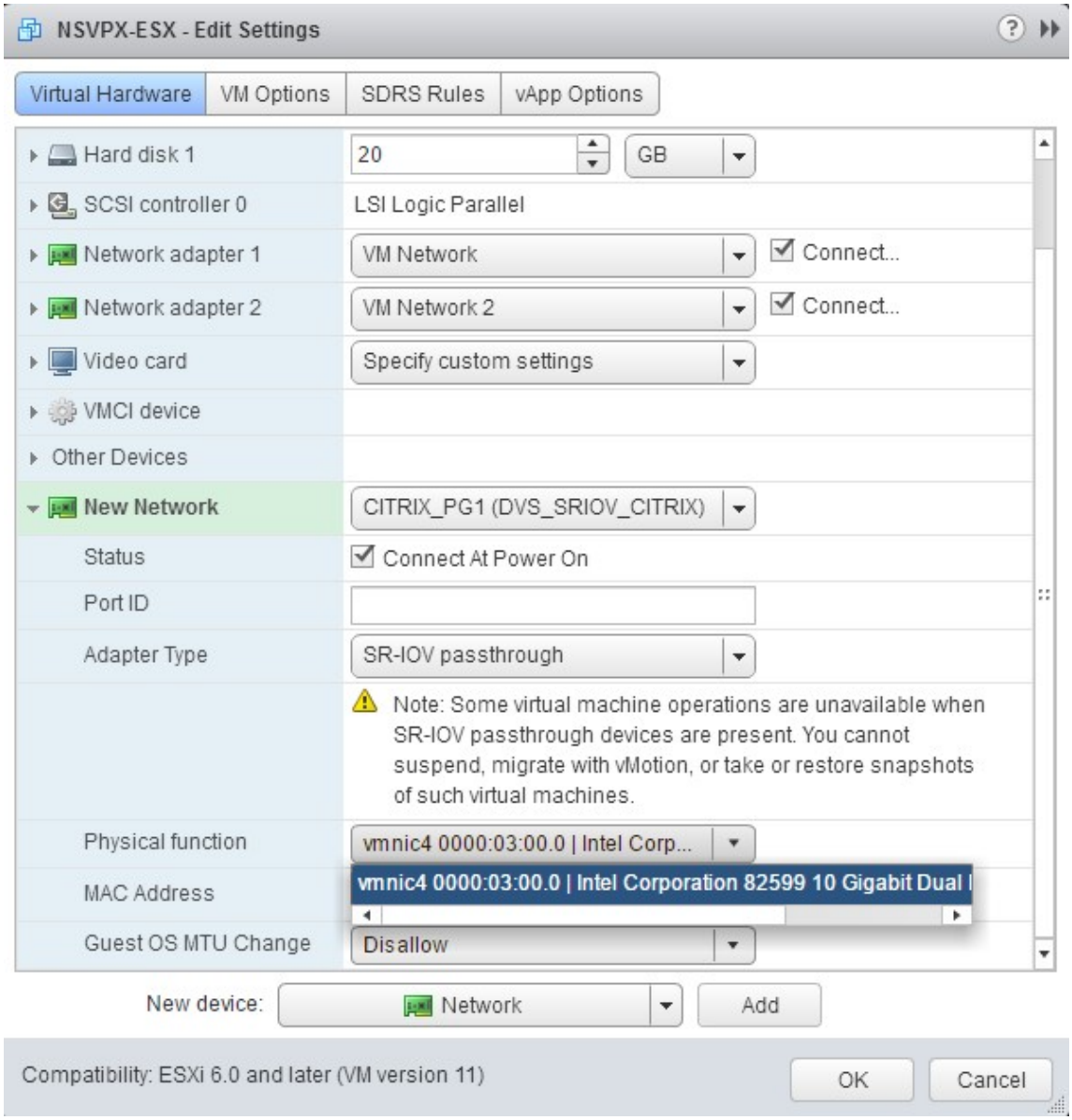


8. Im Abschnitt **Neues Netzwerk**. Wählen Sie in der Dropdownliste `Portgroup` das von Ihnen erstellte aus, und gehen Sie wie folgt vor:

   a. Wählen Sie in der Dropdownliste **Adaptertyp** die Option **SR-IOV-Passthrough** aus.

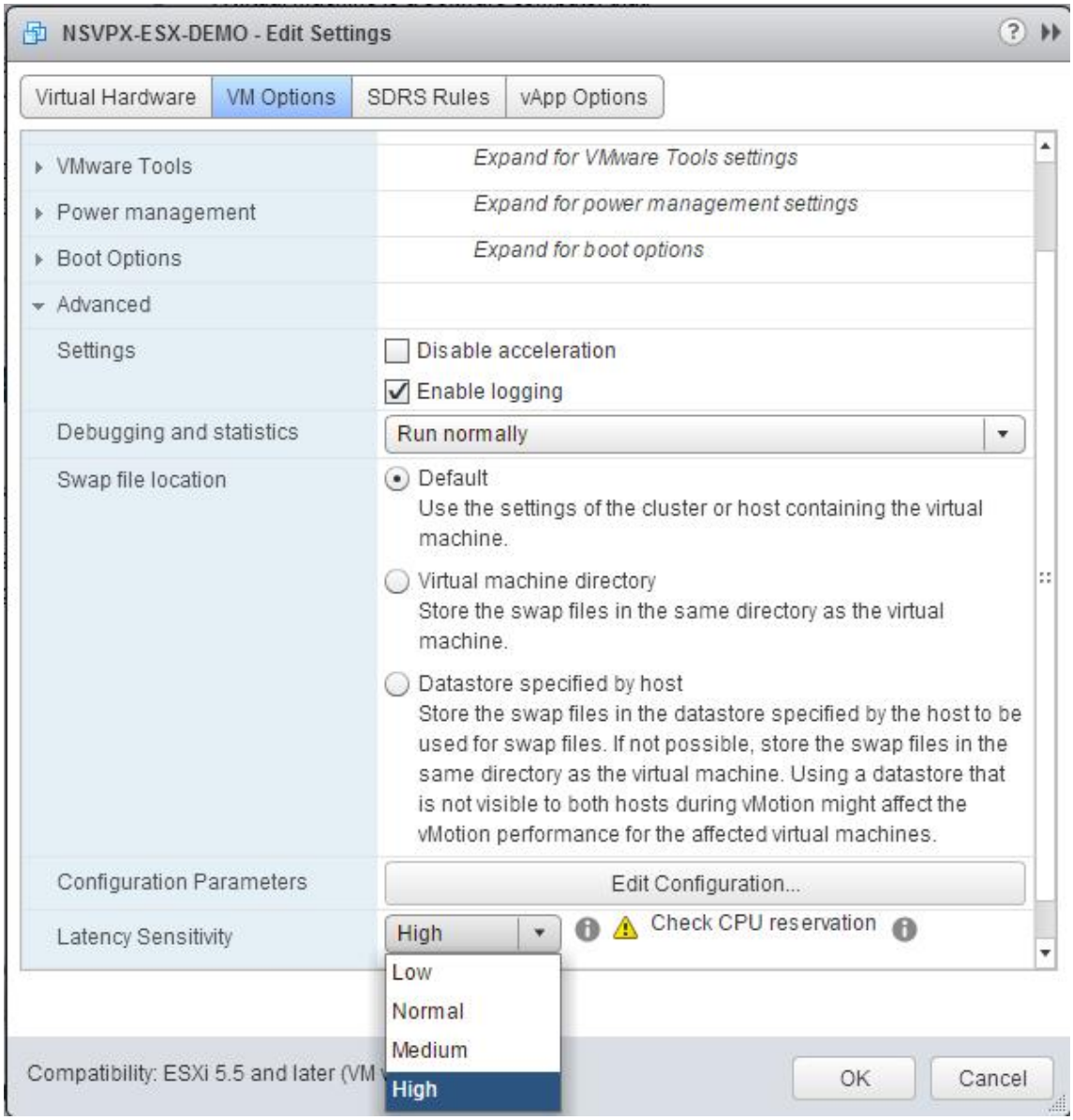


b. Wählen Sie in der Dropdownliste **Physische Funktion** den physischen Adapter aus, der dem zugeordnet ist `Portgroup`.



c. Wählen Sie in der Dropdownliste **Gastbetriebssystem-MTU-Änderung** die Option **Verbieten** aus.

9. Klicken Sie im <virtual_appliance> Dialogfeld **- Einstellungen bearbeiten** auf die Registerkarte **VM-Optionen**.
10. Wählen Sie auf der Registerkarte **VM-Optionen** den Abschnitt **Erweitert** aus. Wählen Sie in der Dropdownliste **Latenzempfindlichkeit** die Option **Hoch** aus.



11. Klicken Sie auf **OK**.
12. Schalten Sie die Citrix ADC VPX-Instanz ein.
13. Sobald die Citrix ADC VPX-Instanz eingeschaltet ist, können Sie die Konfiguration mithilfe des folgenden Befehls überprüfen:

    ```
    show interface summary
    ```

Die Ausgabe muss alle von Ihnen konfigurierten Schnittstellen anzeigen:

```
1 > show interface summary
2 ---------------------------------------------------------------------------
```



```
3        Interface  MTU        MAC                Suffix
4 ----------------------------------------------------------------------------

5  1     0/1        1500       00:0c:29:1b:81:0b  NetScaler Virtual
       Interface
6  2     10/1       1500       00:50:56:9f:0c:6f  Intel 82599 10G VF
       Interface
7  3     10/2       1500       00:50:56:9f:5c:1e  Intel 82599 10G VF
       Interface
8  4     10/3       1500       00:50:56:9f:02:1b  Intel 82599 10G VF
       Interface
9  5     10/4       1500       00:50:56:9f:5a:1d  Intel 82599 10G VF
       Interface
10 6     10/5       1500       00:50:56:9f:4e:0b  Intel 82599 10G VF
       Interface
11 7     LO/1       1500       00:0c:29:1b:81:0b  Netscaler Loopback
       interface
12  Done
13 > show inter 10/1
14 1)      Interface 10/1 (Intel 82599 10G VF Interface) #1
15         flags=0xe460 <ENABLED, UP, UP, HAMON, 802.1q>
16         MTU=1500, native vlan=55, MAC=00:50:56:9f:0c:6f, uptime 0
               h21m53s
17         Actual: media FIBER, speed 10000, duplex FULL, fctl NONE,
               throughput 10000
18         LLDP Mode: NONE,                LR Priority: 1024
19
20         RX: Pkts(838020742) Bytes(860888485431) Errs(0) Drops(2527)
               Stalls(0)
21         TX: Pkts(838149954) Bytes(860895860507) Errs(0) Drops(0) Stalls
               (0)
22         NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
23         Bandwidth thresholds are not set.
24  Done
```

Migrieren der Citrix ADC VPX von E1000 zu SR-IOV- oder VMXNET3-Netzwerkschnittstellen

October 5, 2021

24. Mai 2018

Sie können Ihre beendenden Citrix ADC VPX-Instanzen, die E1000 Netzwerkschnittstellen verwenden, so konfigurieren, dass SR-IOV- oder VMXNET3-Netzwerkschnittstellen verwendet werden.

Informationen zum Konfigurieren einer vorhandenen Citrix ADC VPX-Instanz für die Verwendung von SR-IOV-Netzwerkschnittstellen finden Sie unter Konfigurieren einer Citrix ADC VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnittstelle.

Informationen zum Konfigurieren einer vorhandenen Citrix ADC VPX-Instanz für die Verwendung von VMXNET3-Netzwerkschnittstellen finden Sie unter Konfigurieren einer Citrix ADC VPX-Instanz für die Verwendung der VMXNET3-Netzwerkschnittstelle.

Konfigurieren einer Citrix ADC VPX-Instanz für die Verwendung der PCI-Passthrough-Netzwerkschnittstelle

October 5, 2021

Übersicht

Nachdem Sie eine Citrix ADC VPX-Instanz auf VMware ESX Server installiert und konfiguriert haben, können Sie den vSphere Web Client verwenden, um die virtuelle Appliance für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen zu konfigurieren.

Die PCI-Passthrough-Funktion ermöglicht einem virtuellen Gastcomputer den direkten Zugriff auf physische PCI- und PCIe-Geräte, die mit einem Host verbunden sind.

Voraussetzungen

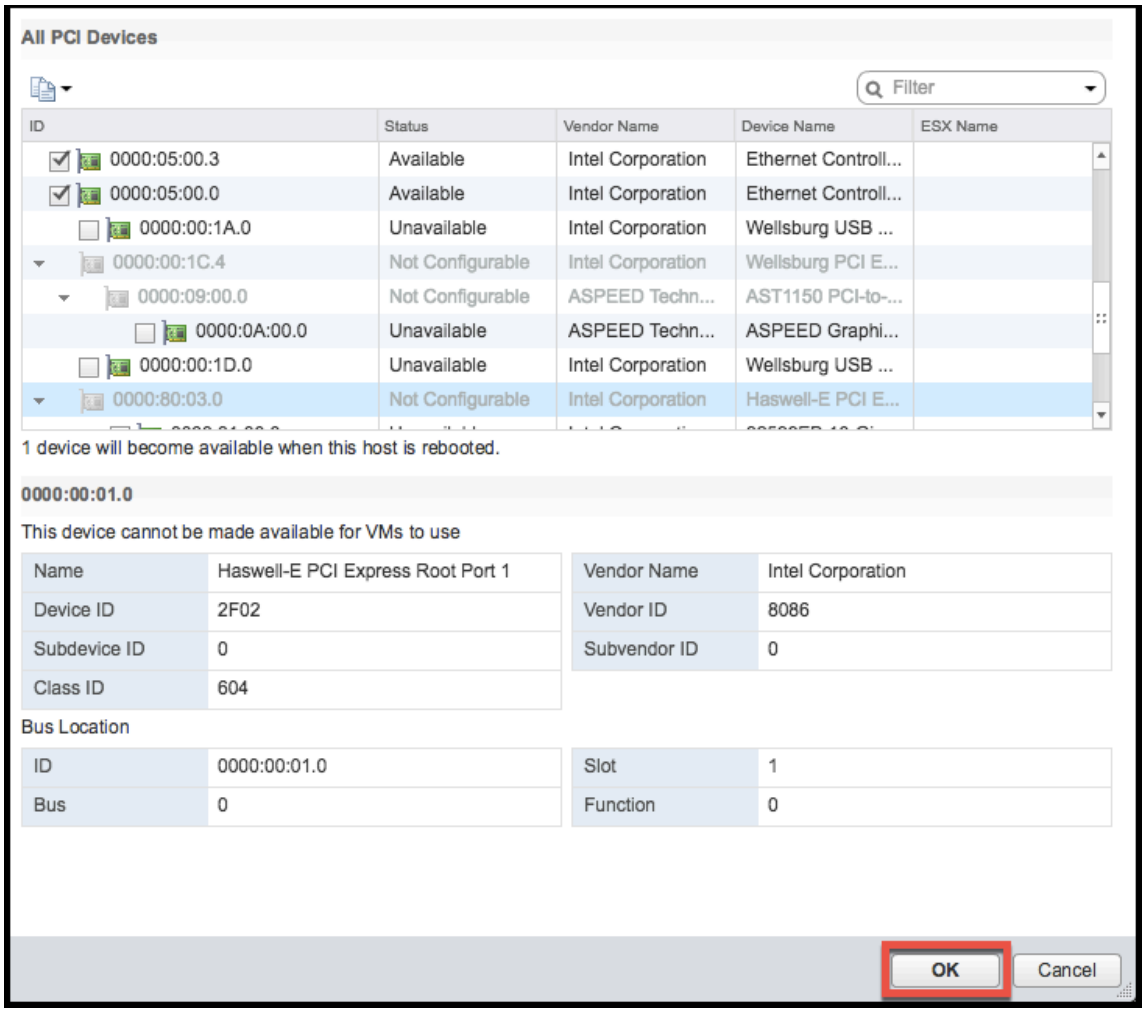
- Die Firmware-Version der Intel XL710 NIC auf dem Host ist 5.04.
- Ein PCI-Passthrough-Gerät, das mit dem Host verbunden und konfiguriert ist
- Unterstützte Netzwerkkarten:
  - Intel X710 10G NIC
  - Intel XL710 Dual Port 40G NIC
  - Intel XL710 Netzwerkkarte mit einem Anschluss, 40 G

Konfigurieren von Passthrough-Geräten auf einem Host

Bevor Sie ein Passthrough-PCI-Gerät auf einer virtuellen Maschine konfigurieren, müssen Sie es auf dem Host-Computer konfigurieren. Gehen Sie folgendermaßen vor, um Passthrough-Geräte auf einem Host zu konfigurieren.

1. Wählen Sie den Host im Navigator-Bedienfeld des vSphere Web Client aus.

2. Klicken Sie auf **Verwalten** > **Einstellungen** > **PCI-Geräte** . Alle verfügbaren Passthrough-Geräte werden angezeigt.
3. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie konfigurieren möchten, und klicken Sie auf **Bearbeiten**.
4. Das Fenster **PCI-Geräteverfügbarkeit bearbeiten** wird angezeigt.
5. Wählen Sie die Geräte aus, die für den Passthrough verwendet werden sollen, und klicken Sie auf **OK**.



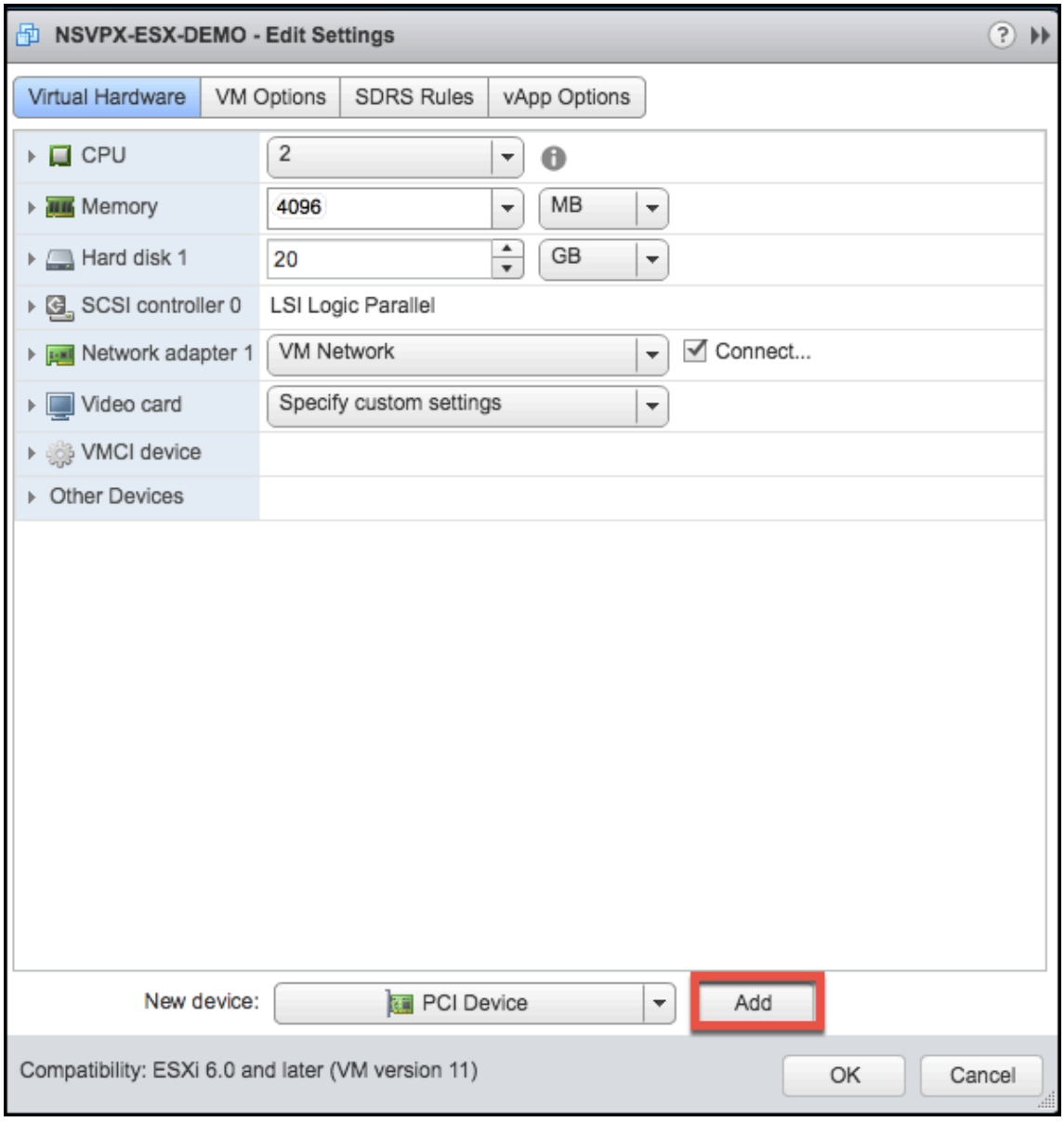
6. Starten Sie den Hostcomputer neu.

Konfigurieren von Passthrough-Geräten auf einer Citrix ADC VPX-Instanz

Gehen Sie folgendermaßen vor, um ein Passthrough-PCI-Gerät auf einer Citrix ADC VPX-Instanz zu konfigurieren.

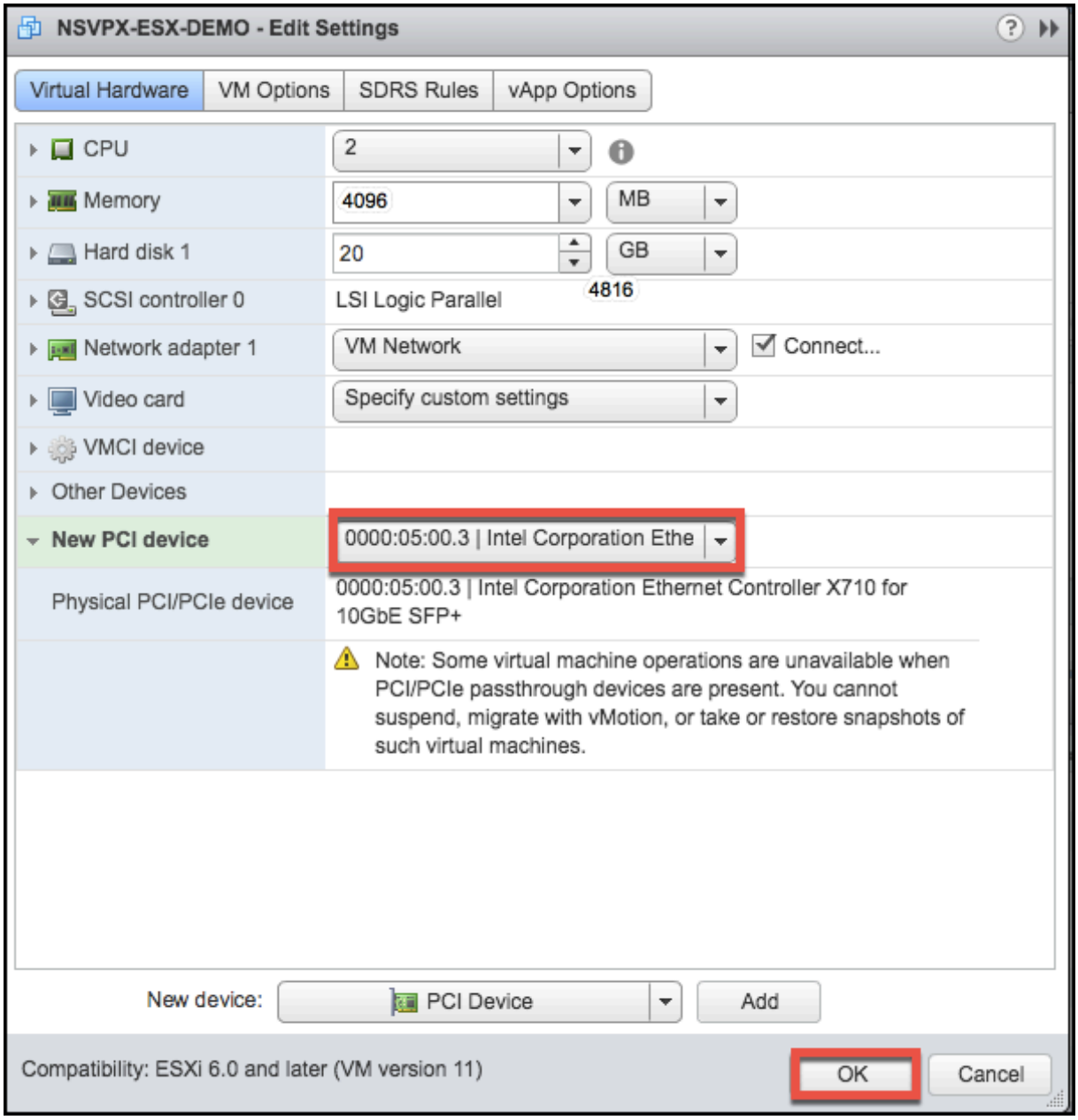
1. Schalten Sie die virtuelle Maschine aus.

2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Einstellungen bearbeiten**.
3. Wählen Sie auf der Registerkarte **Virtuelle Hardware** im Dropdownmenü **Neues Gerät** die Option **PCI-Gerät** aus, und klicken Sie auf **Hinzufügen**.



4. Erweitern Sie **Neues PCI-Gerät**, und wählen Sie das Passthrough-Gerät aus, das mit der virtuellen Maschine verbunden werden soll, aus der Dropdownliste aus, und klicken Sie auf **OK**.

> **Hinweis:**
>
> VMXNET3-Netzwerkschnittstelle und PCI-Passthrough-Netzwerkschnittstelle können nicht koexistieren.



1. Schalten Sie den virtuellen Gastcomputer ein.

Sie haben die Schritte zum Konfigurieren von Citrix ADC VPX für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen abgeschlossen.

Apply Citrix ADC VPX configurations at the first boot of the Citrix ADC appliance on VMware ESX hypervisor

December 7, 2021

You can apply the Citrix ADC VPX configurations during the first boot of the Citrix ADC appliance on the VMware ESX hypervisor. Therefore in certain cases, a specific setup or VPX instance is brought up in much lesser time.

For more information on Preboot user data and its format, see Apply Citrix ADC VPX configurations at the first boot of the Citrix ADC appliance in cloud.

> Note:
>
> To bootstrap using preboot user data in ESX, default gateway config must be passed in <NS-CONFIG> section. For more information on the content of the <NS-CONFIG> tag, see Sample-<NS-CONFIG>-section.

Sample <NS-CONFIG> section:

```
<NS-PRE-BOOT-CONFIG>

    <NS-CONFIG>
        add route 0.0.0.0 0.0.0.0  10.102.38.1
    </NS-CONFIG>

    <NS-BOOTSTRAP>
            <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
            <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
                <INTERFACE-NUM> eth0 </INTERFACE-NUM>
                <IP> 10.102.38.216 </IP>
                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>

</NS-PRE-BOOT-CONFIG>
<!--NeedCopy-->
```

How to provide preboot user data on ESX hypervisor

You can provide preboot user data on ESX hypervisor in the following two ways:

- Using CD/DVD ISO
- Using OVF Property

Provide user data using CD/DVD ISO

You can use VMware vSphere client to inject user data into the VM as an ISO image using the CD/DVD drive.

Follow these steps to provide user data using CD/DVD ISO:

1. Create a file with file name `userdata` that contains the preboot user data content. For more information on the content of the <NS-CONFIG> tag, see Sample <NS-CONFIG> section.

   > Note: File name must be strictly used as `userdata`.

2. Store the `userdata` file in a folder, and build an ISO image using the folder.

   You can build an ISO image with `userdata` file by the following two methods:

   - Using any image processing tool such as PowerISO.
   - Using `mkisofs` command in Linux.

   The following sample configuration shows how to generate an ISO image using the `mkisofs` command in Linux.

```
root@ubuntu:~/sai/14jul2021# ls -l total 4
drwxr-xr-x 2 root root 4096 Jul 14 12:32 esx_preboot_userdata
root@ubuntu:~/sai/14jul2021#
root@ubuntu:~/sai/14jul2021# ls -l esx_preboot_userdata/total 4
-rw-r--r-- 1 root root 3016 Jul 14 12:32 userdata
root@ubuntu:~/sai/14jul2021# mkisofs -o esx_preboot_userdata.iso
    ./esx_preboot_userdata
I: -input-charset not specified, using utf-8 (detected in locale
    settings)
Total translation table size: 0
Total rockridge attributes bytes: 0
Total directory bytes: 112
Path table size(bytes): 10
Max brk space used 0
176 extents written (0 MB)
root@ubuntu:~/sai/14jul2021# ls -lh
total 356K
drwxr-xr-x 2 root root 4.0K Jul 14 12:32 esx_preboot_userdata
-rw-r--r-- 1 root root 352K Jul 14 12:34 esx_preboot_userdata.iso

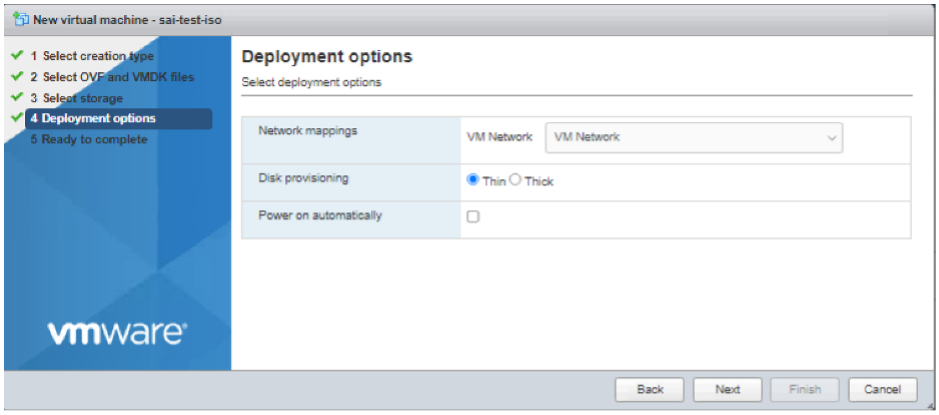
root@ubuntu:~/sai# ls preboot_userdata_155_193 userdata
root@ubuntu:~/sai# mkisofs -o preboot_userdata_155_193.iso ./
    preboot_userdata_155_193
I: -input-charset not specified, using utf-8 (detected in locale
    settings)
```



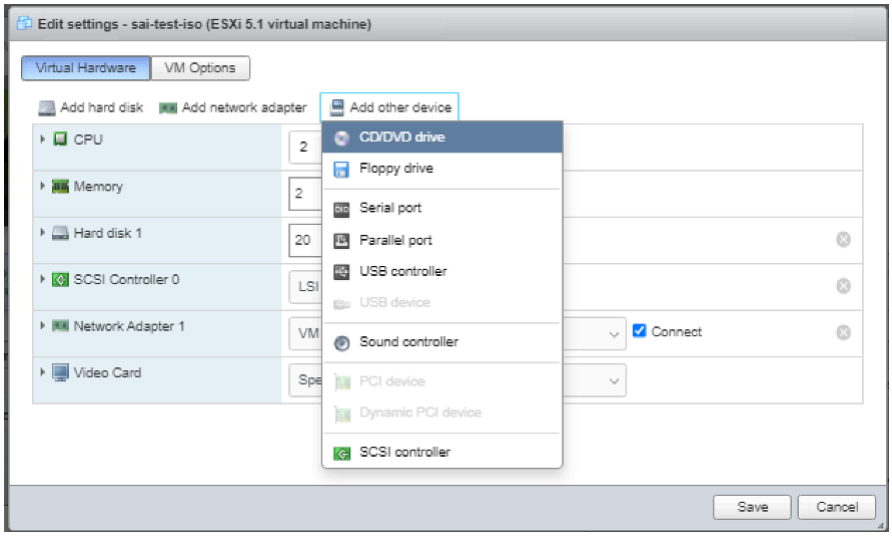
```
Total translation table size: 0
Total rockridge attributes bytes: 0
Total directory bytes: 112
Path table size(bytes): 10
Max brk space used 0
176 extents written (0 MB)

<!--NeedCopy-->
```

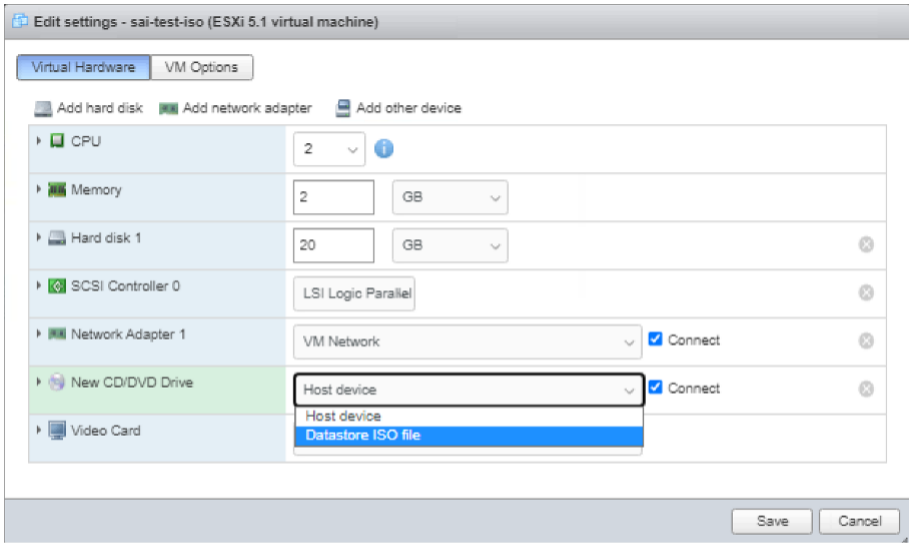
3. Provision the Citrix ADC VPX instance using standard deployment process to create the VM. But do not power on the VM automatically.



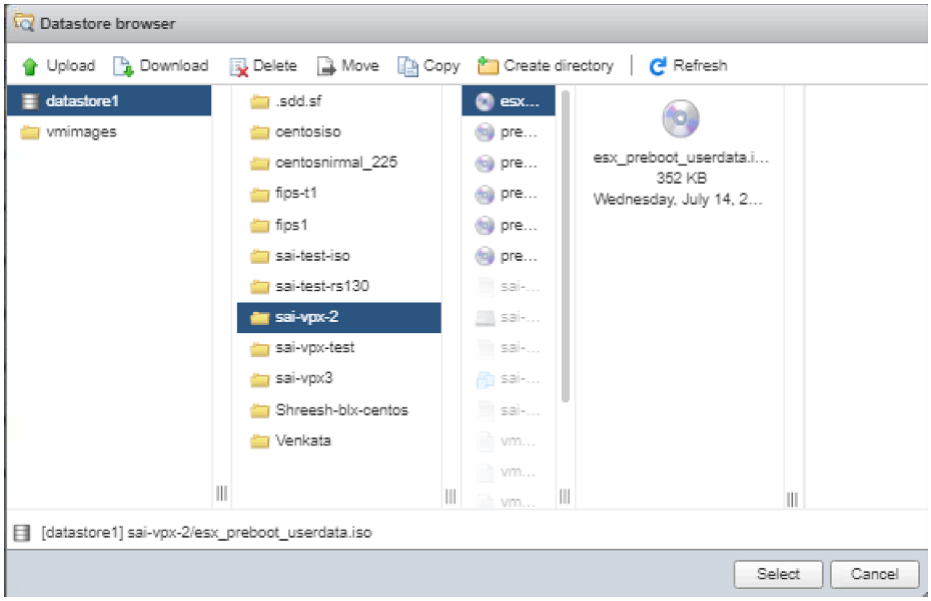
4. After the VM is successfully created, attach the ISO file as CD/DVD drive to the VM.



5. Navigate to **New CD/DVD Drive** and choose **Datastore ISO file** from the drop-down menu.



6. Select a Datastore in the vSphere Client.



7. Power on the VM.

Provide user data using OVF property

Follow these steps to provide user data using OVF property.

1. Create a file with user data content.


```
root@ubuntu:~/sai/14jul2021# cat esx_userdata.xml
<NS-PRE-BOOT-CONFIG>
    <NS-CONFIG>
        add route 0.0.0.0 0.0.0.0 10.102.38.1
    </NS-CONFIG>

    <NS-BOOTSTRAP>
            <SKIP-DEFAULT-BOOTSTRAP>YES</SKIP-DEFAULT-BOOTSTRAP>
            <NEW-BOOTSTRAP-SEQUENCE>YES</NEW-BOOTSTRAP-SEQUENCE>

        <MGMT-INTERFACE-CONFIG>
                <INTERFACE-NUM> eth0 </INTERFACE-NUM>
                <IP>    10.102.38.219 </IP>
                <SUBNET-MASK> 255.255.255.0 </SUBNET-MASK>
        </MGMT-INTERFACE-CONFIG>
    </NS-BOOTSTRAP>
</NS-PRE-BOOT-CONFIG>
```

2. Encode the user data content with Base64 encoding. You can perform the Base64 encoding using the following two methods:

   - In Linux, use the following command:

   ```
   base64 <userdata-filename>  >   <outuput-file>
   <!--NeedCopy-->
   ```

   Example:

   ```
   base64 esx_userdata.xml  > esx_userdata_b64
   <!--NeedCopy-->
   ```

   ```
   root@ubuntu:~/sai/14jul2021# base64 esx_userdata.xml > esx_userdata_b64
   root@ubuntu:~/sai/14jul2021#
   root@ubuntu:~/sai/14jul2021# cat esx_userdata_b64
   PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+CglhZGQgcm91dGUgMC4wLjAuMCAw
   LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkFQPgog
   ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1CT09U
   U1RSQVA+CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1RT
   VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICAgICAg
   ICAgICAgIDxJTlRFUkZBQ0UtTlVNPiBldGgwIDwvSU5URVJGQUNFLU5VTT4KICAgICAgICAgICAg
   ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk5FVC1N
   QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
   RS1DT05GSUc+CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg==
   ```

   - Use online tools to encode user data content, for example, Base64 Encode and Decode.

3. Include a **Product** section in the OVF template of a Citrix ADC VPX instance on ESX hypervisor.

   Sample Product section:


```
<ProductSection>

  <Info>Information about the installed software</Info>
  <Product>NSVPX-VSK Template</Product>
  <Vendor>Citrix</Vendor>
  <VendorUrl>www.citrix.com</VendorUrl>
  <Category> Preboot Userdata </Category>

  <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
     userConfigurable="true" ovf:value="">

    <Label>Userdata</Label>
    <Description> Userdata for ESX VPX </Description>
  </Property>

</ProductSection>
<!--NeedCopy-->
```

4. Provide the base64 encoded user data as the `ovf:value` for `guestinfo.userdata` property in the Product section.

```
<ProductSection>

  <Info>Information about the installed software</Info>
  <Product>NSVPX-VSK Template</Product>
  <Vendor>Citrix</Vendor>
  <VendorUrl>www.citrix.com</VendorUrl>
  <Category> Preboot Userdata </Category>
  <Property ovf:key="guestinfo.userdata" ovf:type="string" ovf:
     userConfigurable="true"
    ovf:value="PE5TLVBSRS1CT09ULUNPTkZJRz4KICAgIDxOUy1DT05GSUc+
       CglhZGQgcm91dGUgMC4wLjAuMCAw
    LjAuMC4wIDEwLjEwMi4zOC4xCiAgICA8L05TLUNPTkZJRz4KCiAgICA8TlMtQk9PVFNUUkFQ

    ICAgICAgICAgICA8U0tJUC1ERUZBVUxULUJPT1RTVFJBUD5ZRVM8L1NLSVAtREVGQVVMVC1C

    U1RSQVA+
       CiAgICAgICAgICAgIDxORVctQk9PVFNUUkFQLVNFUVVFTkNFPllFUzwvTkVXLUJPT1RT

    VFJBUC1TRVFVRU5DRT4KCiAgICAgICAgPE1HTVQtSU5URVJGQUNFLUNPTkZJRz4KICAgICAg

    ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
```

```
15      ICAgIDxJUD4gICAgMTAuMTAyLjM4LjIxOSA8L0lQPgogICAgICAgICAgICAgICAgPFNVQk5F
16      QVNLPiAyNTUuMjU1LjI1NS4wIDwvU1VCTkVULU1BU0s+
           CiAgICAgICAgPC9NR01ULUlOVEVSRkFD
17      RS1DT05GSUc+
           CiAgICA8L05TLUJPT1RTVFJBUD4KPC9OUy1QUkUtQk9PVC1DT05GSUc+Cg
           ==”>
18
19      <Label>Userdata</Label>
20      <Description> Userdata for ESX VPX </Description>
21    </Property>
22
23  </ProductSection>
24  <!--NeedCopy-->
```

5. Use the modified OVF template with Product section for the VM deployment.

```
Please change the default NSROOT password.
Enter new password:
Please re-enter your password:
 Done
> sh ns ver
        NetScaler NS13.0: Build 83.9005.nc, Date: Jul 13 2021, 02:56:05   (64-bit)
 Done
> sh ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  S
tate
        ---------        --------------  ----             ----     ---      ----     -------  -
-----
1)      10.102.38.219    0               NetScaler IP     Active   Enabled  Enabled  NA       E
nabled
 Done
> sh route
        Network          Netmask          Gateway/OwnedIP  VLAN    State    Traffic Domain  Type
        -------          -------          ---------------  -----   -----    --------------  ----
1)      0.0.0.0          0.0.0.0          10.102.38.1      0       UP       0               STATI
C
2)      127.0.0.0        255.0.0.0        127.0.0.1        0       UP       0               PERMA
NENT
3)      10.102.38.0      255.255.255.0    10.102.38.219    0       UP       0               DIREC
T
 Done
```

Installieren einer Citrix ADC VPX Instanz in VMware Cloud auf AWS

October 5, 2021

Mit VMware Cloud (VMC) auf AWS können Sie Cloud-Softwaredefinierte Rechenzentren (SDDC) in AWS mit der gewünschten Anzahl von ESX-Hosts erstellen. VMC auf AWS unterstützt Citrix ADC VPX Bereitstellungen. VMC stellt eine Benutzeroberfläche bereit, die gleiche wie bei vCenter vor Ort ist. Es funktioniert identisch mit den ESX-basierten Citrix ADC VPX Bereitstellungen.

Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, gehen Sie folgendermaßen vor:

- Ein VMware SDDC muss mindestens mit einem Host vorhanden sein.
- Laden Sie die Setup-Dateien der Citrix ADC VPX Appliance herunter.
- Erstellen Sie entsprechende Netzwerksegmente auf VMware SDDC, mit denen sich die virtuellen Maschinen verbinden.
- VPX-Lizenzdateien abrufen. Weitere Informationen zu Citrix ADC VPX-Instanzlizenzen finden Sie im *Citrix ADC VPX Licensing Guide* unter http://support.citrix.com/article/ctx131110.

VMware Cloud-Hardwareanforderungen

In der folgenden Tabelle sind die virtuellen Computerressourcen aufgeführt, die das VMware SDDC für jede virtuelle VPX NCore-Appliance bereitstellen muss.

Tabelle 1. Minimale virtuelle Datenverarbeitungsressourcen für die Ausführung einer Citrix ADC VPX-Instanz

Komponente	Voraussetzung
Speicher	2 GB
Virtuelle CPU (vCPU)	2
Virtuelle Netzwerkschnittstellen	In VMware SDDC können Sie maximal 10 virtuelle Netzwerkschnittstellen installieren, wenn die VPX-Hardware auf Version 7 oder höher aktualisiert wird.
Speicherplatz	20 GB

> Hinweis:
>
> Dies gilt zusätzlich zu den Datenträgeranforderungen für den Hypervisor.

Für die Produktion der virtuellen VPX-Appliance muss die vollständige Speicherzuweisung reserviert werden.

Systemanforderungen für OVF Tool 1.0

OVF Tool ist eine Client-Anwendung, die auf Windows- und Linux-Systemen ausgeführt werden kann. In der folgenden Tabelle werden die Mindestsystemanforderungen beschrieben.

Tabelle 2. Mindestsystemanforderungen für die Installation von OVF-Werkzeugen

Komponente	Voraussetzung
Betriebssystem	Ausführliche Anforderungen von VMware finden Sie unter der PDF-Datei “OVF Tool User Guide”http://kb.vmware.com/.
CPU	mindestens 750 MHz, 1 GHz oder schneller empfohlen
RAM	1 GB Minimum, 2 GB empfohlen
NIC	Netzwerkkarte mit 100 Mbit/s oder schneller

Informationen zur Installation von OVF finden Sie unter der PDF-Datei “OVF Tool User Guide”http://kb.vmware.com/.

Herunterladen der Setup-Dateien für Citrix ADC VPX

Das Setuppaket für Citrix ADC VPX für VMware ESX folgt dem Format Open Virtual Machine (OVF). Sie können die Dateien von der Citrix Website herunterladen. Sie benötigen ein Citrix Konto, um sich anzumelden. Wenn Sie kein Citrix-Konto haben, rufen Sie die Startseite unter http://www.citrix.comauf. Klicken Sie auf den **Link Neue Benutzer**, und folgen Sie den Anweisungen, um ein neues Citrix Konto zu erstellen.

Navigieren Sie nach der Anmeldung auf der Citrix Homepage zum folgenden Pfad:

Citrix.com > **Downloads > Citrix ADC > Virtuelle Appliances**.

Kopieren Sie die folgenden Dateien auf eine Arbeitsstation im selben Netzwerk wie der ESX-Server. Kopieren Sie alle drei Dateien in denselben Ordner.

- NSVPX-ESX- <release number>- <build number>-disk1.vmdk (zum Beispiel NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX- <release number>- <build number>.ovf (zum Beispiel NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX- <release number>- <build number>.mf (zum Beispiel NSVPX-ESX-13.0-79.64.mf)

Installieren einer Citrix ADC VPX Instanz in VMware Cloud

Nachdem Sie VMware SDDC installiert und konfiguriert haben, können Sie mit dem SDDC virtuelle Appliances in der VMware Cloud installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der Menge des auf dem SDDC verfügbaren Speichers ab.

Gehen Sie folgendermaßen vor, um Citrix ADC VPX Instanzen in VMware Cloud zu installieren:

1. Öffnen Sie VMware SDDC auf Ihrer Workstation.

2. Geben Sie in die Textfelder **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein, und klicken Sie dann auf Anmelden.
3. Klicken Sie im Menü **Datei** auf **OVF-Vorlage bereitstellen**.
4. Navigieren Sie im Dialogfeld **OVF-Vorlage bereitstellen** unter **Datei bereitstellen** zu dem Speicherort, an dem Sie die Setupdateien der Citrix ADC VPX-Instanz gespeichert haben, wählen Sie die OVF-Datei aus, und klicken Sie auf **Weiter**.

   > **Hinweis:** Standardmäßig verwendet die Citrix ADC VPX Instanz E1000 Netzwerkschnittstellen. Um ADC mit der VMXNET3-Schnittstelle bereitzustellen, ändern Sie die OVF so, dass die VMXNET3-Schnittstelle anstelle von E1000 verwendet wird.

5. Ordnen Sie die in der OVF-Vorlage der virtuellen Appliance angezeigten Netzwerke den Netzwerken zu, die Sie auf dem VMware SDDC konfiguriert haben. Klicken Sie auf **Weiter**, um mit der Installation einer virtuellen Appliance auf VMware SDDC zu beginnen.
6. Sie können nun die Citrix ADC VPX-Instanz starten. Wählen Sie im Navigationsbereich die installierte Citrix ADC VPX-Instanz aus, und wählen Sie im Kontextmenü die Option **Einschalten**aus. Klicken Sie auf die Registerkarte **Konsole**, um einen Konsolenport zu emulieren.
7. Wenn Sie eine andere virtuelle Appliance installieren möchten, wiederholen Sie dies in Schritt 6.
8. Geben Sie die Verwaltungs-IP-Adresse aus demselben Segment an, das als Verwaltungsnetzwerk ausgewählt wurde. Das gleiche Subnetz wird für das Gateway verwendet.
9. VMware SDDC erfordert, dass NAT- und Firewall-Regeln explizit für alle privaten IP-Adressen erstellt werden, die zu Netzwerksegmenten gehören.

Installieren einer Citrix ADC VPX-Instanz auf Microsoft Hyper-V-Server

October 5, 2021

Um Citrix ADC VPX-Instanzen unter Microsoft Windows Server zu installieren, müssen Sie zunächst Windows Server mit aktivierter Hyper-V-Rolle auf einem Computer mit ausreichenden Systemressourcen installieren. Beim Installieren der Hyper-V-Rolle müssen Sie die Netzwerkkarten auf dem Server angeben, den Hyper-V zum Erstellen von virtuellen Netzwerken verwenden soll. Sie können einige NICs für den Host reservieren. Verwenden Sie Hyper-V Manager, um die Citrix ADC VPX-Instanzinstallation durchzuführen.

Die Citrix ADC VPX-Instanz für Hyper-V wird im VHD-Format (Virtual Hard Disk) bereitgestellt. Es enthält die Standardkonfiguration für Elemente wie CPU, Netzwerkschnittstellen sowie Festplattengröße und -format. Nach der Installation der Citrix ADC VPX-Instanz können Sie die Netzwerkadapter

auf der virtuellen Appliance konfigurieren, virtuelle Netzwerkkarten hinzufügen und dann die Citrix ADC IP-Adresse, die Subnetzmaske und das Gateway zuweisen und die grundlegende Konfiguration der virtuellen Appliance abschließen.

Wenn Sie nach der Erstkonfiguration der VPX-Instanz die Appliance auf die neueste Softwareversion aktualisieren möchten, siehe Upgrade einer eigenständigen Citrix ADC VPX Appliance

> **Hinweis:**
>
> Intermediate System-to-Intermediate System (ISIS) -Protokoll wird auf der virtuellen Citrix ADC VPX Appliance, die auf der HyperV-2012-Plattform gehostet wird, nicht unterstützt.

Voraussetzungen für die Installation der Citrix ADC VPX-Instanz auf Microsoft-Servern

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, gehen Sie folgendermaßen vor:

- Aktivieren Sie die Hyper-V-Rolle auf Windows-Servern. Weitere Informationen finden Sie unter http://technet.microsoft.com/en-us/library/ee344837(WS.10).aspx.
- Laden Sie die Setup-Dateien der virtuellen Appliance herunter.
- Beschaffen Sie sich Lizenzdateien der Citrix ADC VPX Instanz. Weitere Informationen zu Citrix ADC VPX-Instanzlizenzen finden Sie im *Citrix ADC VPX Licensing Guide* unter http://support.citrix.com/article/ctx131110.

Microsoft-Server-Hardwareanforderungen

In der folgenden Tabelle werden die Mindestsystemanforderungen für Microsoft-Server beschrieben.

Tabelle 1. Mindestsystemanforderungen für Microsoft-Server

Komponente	Voraussetzung
CPU	64-Bit-Prozessor mit 1,4 GHz
RAM	8 GB
Speicherplatz	32 GB oder höher

In der folgenden Tabelle sind die virtuellen Computerressourcen für jede Citrix ADC VPX-Instanz aufgeführt.

Tabelle 2. Minimale virtuelle Datenverarbeitungsressourcen für die Ausführung einer Citrix ADC VPX-Instanz

Komponente	Voraussetzung
RAM	4 GB
Virtuelle CPU	2
Speicherplatz	20 GB
Virtuelle Netzwerkschnittstellen	1

Laden Sie die Setup-Dateien für Citrix ADC VPX herunter

Die Citrix ADC VPX Instanz für Hyper-V wird im Format Virtual Hard Disk (VHD) bereitgestellt. Sie können die Dateien von der Citrix Website herunterladen. Sie benötigen ein Citrix Konto, um sich anzumelden. Wenn Sie kein Citrix-Konto haben, rufen Sie die Startseite unter http://www.citrix.comauf, klicken Sie auf **Anmelden > Mein Konto > Citrix Account erstellen**und befolgen Sie die Anweisungen zum Erstellen eines Citrix-Kontos.

Gehen Sie folgendermaßen vor, um die Setup-Dateien der Citrix ADC VPX Instanz herunterzuladen:

1. Navigieren Sie in einem Webbrowser zu http://www.citrix.com/.
2. Melden Sie sich mit Ihrem Benutzernamen und Kennwort an.
3. Klicken Sie auf **Downloads**.
4. **Wählen Sie im Dropdownmenü Produkt** auswählen die Option **Citrix ADC (NetScaler ADC)**aus.
5. Klicken **Sie unter Citrix ADC Release X.X > Virtual Appliances**auf **Citrix ADC VPX Release X.X**.
6. Laden Sie die komprimierte Datei auf Ihren Server herunter.

Installieren der Citrix ADC VPX-Instanz auf Microsoft-Servern

Nachdem Sie die Hyper-V-Rolle auf Microsoft Server aktiviert und die Dateien der virtuellen Appliance extrahiert haben, können Sie den Hyper-V-Manager verwenden, um die Citrix ADC VPX-Instanz zu installieren. Nachdem Sie die virtuelle Maschine importiert haben, müssen Sie die virtuellen Netzwerkkarten konfigurieren, indem Sie sie den von Hyper-V erstellten virtuellen Netzwerken zuordnen.

Sie können maximal acht virtuelle Netzwerkkarten konfigurieren. Selbst wenn die physische Netzwerkkarte DOWN ist, geht die virtuelle Appliance davon aus, dass die virtuelle Netzwerkkarte UP ist, da sie weiterhin mit den anderen virtuellen Appliances auf demselben Host (Server) kommunizieren kann.

> **Hinweis:**
>
> Sie können keine Einstellungen ändern, während die virtuelle Appliance ausgeführt wird. Fahren Sie die virtuelle Appliance herunter, und nehmen Sie dann Änderungen vor.

So installieren Sie die Citrix ADC VPX-Instanz auf Microsoft Server mithilfe des Hyper-V-Managers:

1. Klicken Sie zum Starten von Hyper-V-Manager auf **Start**, zeigen Sie auf **Verwaltung**, und klicken Sie dann auf **Hyper-V-Manager**.
2. Wählen Sie im Navigationsbereich unter **Hyper-V Verwalten**r den Server aus, auf dem Sie die Citrix ADC VPX-Instanz installieren möchten.
3. Klicken Sie im Menü **Aktion** auf **Virtuelle Maschine importieren**e.
4. Geben Sie im Dialogfeld **Virtuelle Maschine importieren** unter **Speicherort** den Pfad des Ordners an, der die Softwaredateien der Citrix ADC VPX enthält, und wählen Sie dann **Virtuelle Maschine kopieren (neue eindeutige ID erstellen)** . Dieser Ordner ist der übergeordnete Ordner, der die Ordner Snapshots, virtuelle Festplatten und virtuelle Maschinen enthält.
5. Hinweis: Wenn Sie eine komprimierte Datei erhalten haben, stellen Sie sicher, dass Sie die Dateien in einen Ordner extrahieren, bevor Sie den Pfad zum Ordner angeben.
6. Klicken Sie auf **Importieren**.
7. Stellen Sie sicher, dass die importierte virtuelle Appliance unter **Virtuelle Maschinen**aufgeführt ist.
8. Wiederholen Sie die Schritte **2** bis **6**, um eine andere virtuelle Appliance zu installieren.

> **Wichtig**
>
> Stellen Sie sicher, dass Sie die Dateien in einen anderen Ordner in Schritt **4**extrahieren.

Automatische Bereitstellung einer Citrix ADC VPX-Instanz auf Hyper-V

Die automatische Bereitstellung der Citrix ADC VPX-Instanz ist optional. Wenn die automatische Bereitstellung nicht erfolgt, bietet die virtuelle Appliance eine Option zum Konfigurieren der IP-Adresse usw.

Gehen Sie folgendermaßen vor, um die Citrix ADC VPX-Instanz auf Hyper-V automatisch bereitzustellen.

1. Erstellen Sie ein ISO9660-kompatibles ISO-Image unter Verwendung der XML-Datei, wie im Beispiel dargestellt. Stellen Sie sicher, dass der Name der XML-Datei **Benutzerdaten**ist.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>

```



```
<Environment xmlns:oe=`"http://schemas.dmtf.org/ovf/environment/1`"

xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`"

oe:id=""

xmlns=`"http://schemas.dmtf.org/ovf/environment/1`">

<PlatformSection>

<Kind>HYPER-V</Kind>

<Version>2013.1</Version>

<Vendor>CISCO</Vendor>

<Locale>en</Locale>

</PlatformSection>

<PropertySection>

<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0" />

<Property oe:key="com.citrix.netscaler.platform" oe:value="NS1000V"/>

<Property oe:key="com.citrix.netscaler.orch_env" oe:value="cisco-orch-env"/>

<Property oe:key="com.citrix.netscaler.mgmt.ip" oe:value="10.102.100.122"/>

<Property oe:key="com.citrix.netscaler.mgmt.netmask" oe:value="255.255.255.128"/>

<Property oe:key="com.citrix.netscaler.mgmt.gateway" oe:value="10.102.100.67"/></PropertySection>

</Environment>
<!--NeedCopy-->
```

2. Kopieren Sie das ISO-Image auf den Hyper-V-Server.

3. Wählen Sie die virtuelle Appliance aus, die Sie importiert haben, und wählen Sie dann im Menü **Aktion** die Option **Einstellungen** aus. Sie können auch die virtuelle Appliance auswählen und dann mit der rechten Maustaste klicken und **Einstellungen**auswählen. Das Fenster **Einstellungen** für die ausgewählte virtuelle Appliance wird angezeigt.
4. Klicken Sie im Fenster **Einstellungen** unter dem Hardware-Abschnitt auf **IDE Controller**.
5. Wählen Sie im rechten Fensterbereich **DVD-Laufwerk** aus, und klicken Sie auf **Hinzufügen**. Das DVD-Laufwerk wird im linken Fensterbereich unter dem **IDE-Controller** Abschnitt hinzugefügt.
6. Wählen Sie das **DVD-Laufwerk** aus, das in Schritt 5 hinzugefügt wurde. Wählen Sie im rechten Fensterbereich das **Optionsfeld Bilddatei** aus, klicken Sie auf **Durchsuchen**, und wählen Sie das ISO-Image aus, das Sie auf dem Hyper-V-Server kopiert haben, in Schritt 2.
7. Klicken Sie auf **Apply**.

> **Hinweis:**
>
> Die virtuelle Appliance-Instanz wird in der Standard-IP-Adresse angezeigt, wenn:
>
> - Das DVD-Laufwerk ist angehängt und die ISO-Datei wird nicht bereitgestellt.
> - Die ISO-Datei enthält die Benutzerdatendatei nicht.
> - Der Dateiname oder das Format der Benutzerdaten ist nicht korrekt.

Gehen Sie folgendermaßen vor, um virtuelle Netzwerkkarten auf der Citrix ADC VPX-Instanz zu konfigurieren:

1. Wählen Sie die virtuelle Appliance aus, die Sie importiert haben, und wählen Sie dann im Menü **Aktion** die Option **Einstellungen** aus.
2. Klicken Sie im Dialogfeld **Einstellungen für <virtual appliance name>** im linken Bereich auf **Hardware hinzufügen**.
3. Wählen Sie im rechten Fensterbereich aus der Liste der Geräte die Option **Netzwerkadapter** aus.
4. Klicken Sie auf **Hinzufügen**.
5. Stellen Sie sicher, dass **Netzwerkadapter (nicht verbunden)** im linken Bereich angezeigt wird.
6. Wählen Sie den Netzwerkadapter im linken Bereich aus.
7. Wählen Sie im rechten Fensterbereich im Menü **Netzwerk** das virtuelle Netzwerk aus, mit dem der Adapter verbunden werden soll.
8. Wiederholen Sie die Schritte **6** und **7**, um das virtuelle Netzwerk für andere Netzwerkadapter auszuwählen.
9. Klicken Sie auf **Übernehmen**, und klicken Sie dann auf **OK**.

So konfigurieren Sie die Citrix ADC VPX-Instanz:

1. Klicken Sie mit der rechten Maustaste auf die virtuelle Appliance, die Sie zuvor installiert haben, und wählen Sie dann **Start**aus.
2. Öffnen Sie die Konsole, indem Sie auf die virtuelle Appliance doppelklicken.

3. Geben Sie die Citrix ADC IP-Adresse, die Subnetzmaske und das Gateway für Ihre virtuelle Appliance ein.

Sie haben die grundlegende Konfiguration Ihrer virtuellen Appliance abgeschlossen. Geben Sie die IP-Adresse in einem Webbrowser ein, um auf die virtuelle Appliance zuzugreifen.

> **Hinweis:**
>
> Sie können auch die Vorlage für virtuelle Maschinen (VM) verwenden, um die Citrix ADC VPX-Instanz mithilfe von SCVMM bereitzustellen.
>
> Wenn Sie die Microsoft Hyper-V NIC-Teaming-Lösung mit NetScaler VPX-Instanzen verwenden, finden Sie im Artikel CTX224494 weitere Informationen.

Installieren einer Citrix ADC VPX-Instanz auf der Linux-KVM-Plattform

October 5, 2021

Um einen Citrix ADC VPX für die Linux-KVM-Plattform einzurichten, können Sie die grafische Virtual Machine Manager (Virtual Manager) -Anwendung verwenden. Wenn Sie die Linux-KVM-Befehlszeile bevorzugen, können Sie das `virsh` Programm verwenden.

Das Host-Linux-Betriebssystem muss mit Virtualisierungstools wie KVM Module und QEMU auf geeigneter Hardware installiert werden. Die Anzahl der virtuellen Maschinen (VMs), die auf dem Hypervisor bereitgestellt werden können, hängt von der Anwendungsanforderung und der ausgewählten Hardware ab.

Nachdem Sie eine Citrix ADC VPX-Instanz bereitgestellt haben, können Sie weitere Schnittstellen hinzufügen.

Einschränkungen und Nutzungsrichtlinien

Allgemeine Empfehlungen

Um unvorhersehbares Verhalten zu vermeiden, wenden Sie die folgenden Empfehlungen an:

- Ändern Sie nicht die MTU der VNet-Schnittstelle, die mit der VPX-VM verknüpft ist. Fahren Sie die VPX-VM herunter, bevor Sie Konfigurationsparameter wie Schnittstellenmodi oder CPU ändern.
- Erzwingen Sie das Herunterfahren der VPX-VM nicht. Das heißt, verwenden Sie nicht den Befehl **Erzwingen aus** .
- Alle Konfigurationen, die auf dem Host Linux durchgeführt werden, sind möglicherweise dauerhaft, abhängig von Ihren Linux-Distributionseinstellungen. Sie können diese Konfigurationen dauerhaft festlegen, um ein konsistentes Verhalten bei Neustarts des Host-Linux-Betriebssystems sicherzustellen.

- Das Citrix ADC-Paket muss für jede bereitgestellte Citrix ADC VPX-Instanz eindeutig sein.

Einschränkungen

- Live-Migration einer VPX-Instanz, die auf KVM ausgeführt wird, wird nicht unterstützt.

Voraussetzungen für die Installation einer Citrix ADC VPX-Instanz auf der Linux-KVM-Plattform

October 5, 2021

Überprüfen Sie die Mindestsystemanforderungen für einen Linux-KVM-Server, der auf einer Citrix ADC VPX-Instanz ausgeführt wird.

CPU-Anforderung:

- 64-Bit-x86-Prozessoren mit der Hardwarevirtualisierungsfunktion, die in Intel VT-X-Prozessoren enthalten ist.

Um zu testen, ob Ihre CPU den Linux-Host unterstützt, geben Sie den folgenden Befehl an der Linux-Shell-Eingabeaufforderung

```
\*.egrep '^flags.\*(vmx|svm)' /proc/cpuinfo*
<!--NeedCopy-->
```

Wenn die **BIOS-Einstellungen** für die vorhergehende Erweiterung deaktiviert sind, müssen Sie sie im BIOS aktivieren.

- Stellen Sie mindestens 2 CPU-Kerne für Host Linux bereit.
- Es gibt keine spezifische Empfehlung für die Prozessorgeschwindigkeit, aber höher die Geschwindigkeit, desto besser die Leistung der VM-Anwendung.

Speicherbedarf (RAM):

Mindestens 4 GB für den Host-Linux-Kernel. Fügen Sie mehr Arbeitsspeicher hinzu, wie es von den VMs benötigt wird.

Festplattenanforderung:

Berechnen Sie den Speicherplatz für Host-Linux-Kernel und VM-Anforderungen. Eine einzelne Citrix ADC VPX VM benötigt 20 GB Speicherplatz.

Softwareanforderungen

Der verwendete Host-Kernel muss ein 64-Bit-Linux-Kernel, Version 2.6.20 oder höher, mit allen Virtualisierungstools sein. Citrix empfiehlt neuere Kernel wie 3.6.11-4 und höher.

Viele Linux-Distributionen wie Red Hat, CentOS und Fedora haben Kernelversionen und zugehörige Virtualisierungstools getestet.

Hardwareanforderungen für Gast-VM

Citrix ADC VPX unterstützt IDE- und VirtIO-Festplattentypen. Der Festplattentyp wurde in der XML-Datei konfiguriert, die Teil des Citrix ADC Pakets ist.

Netzwerkanforderungen

Citrix ADC VPX unterstützt para-virtualisierte, SR-IOV- und PCI-Passthrough-Netzwerkschnittstellen von VirtIO.

Weitere Informationen zu den unterstützten Netzwerkschnittstellen finden Sie unter:

- Bereitstellen der Citrix ADC VPX-Instanz mithilfe des Virtual Machine Manager
- Konfigurieren einer Citrix ADC VPX-Instanz für die Verwendung von SR-IOV-Netzwerkschnittstellen
- Konfigurieren einer Citrix ADC VPX-Instanz für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen

Quellschnittstelle und Modi

Der Quellgerätetyp kann entweder Bridge oder MacVTap sein. In MacVTap sind vier Modi möglich - VEPA, Bridge, Private und Pass-Through. Überprüfen Sie die Arten von Schnittstellen, die Sie verwenden können, und die unterstützten Datenverkehrstypen wie folgt:

Brücke:

- Linux-Brücke.
- `Ebtables` und `iptables` Einstellungen auf Host Linux filtern möglicherweise den Datenverkehr auf der Bridge, wenn Sie nicht die richtige Einstellung auswählen oder `IPtable` Dienste deaktivieren.

MacVTap (VEPA-Modus):

- Bessere Leistung als eine Brücke.
- Schnittstellen von demselben niedrigeren Gerät können auf den virtuellen Rechnern gemeinsam genutzt werden.
- Inter-VM-Kommunikation mit derselben

- niedrigeres Gerät ist nur möglich, wenn der Upstream- oder Downstream-Switch den VEPA-Modus unterstützt.

MacVTap (privater Modus):

- Bessere Leistung als eine Brücke.
- Schnittstellen von demselben niedrigeren Gerät können auf den virtuellen Rechnern gemeinsam genutzt werden.
- Inter-VM-Kommunikation mit demselben niedrigeren Gerät ist nicht möglich.

MacVTap (Bridge-Modus):

- Besser im Vergleich zu Bridge.
- Schnittstellen von demselben niedrigeren Gerät können für die VMs gemeinsam genutzt werden.
- Die Kommunikation zwischen VM mit demselben niedrigeren Gerät ist möglich, wenn die untere Geräteverbindung UP ist.

MacVTap (Pass-Through-Modus):

- Besser im Vergleich zu Bridge.
- Schnittstellen von demselben niedrigeren Gerät können nicht für die VMs freigegeben werden.
- Nur eine VM kann das untere Gerät verwenden.

> Hinweis: Um die beste Leistung durch die VPX-Instanz zu erzielen, stellen Sie sicher, dass die `lro` Funktionen `gro` und auf den Quellschnittstellen ausgeschaltet sind.

Eigenschaften von Quellschnittstellen

Stellen Sie sicher, dass Sie die Funktionen generic-Receive-offload (`gro`) und Large-Receive-Offload (`lro`) der Quellschnittstellen ausschalten. Um die `lro` Funktionen `gro` und auszuschalten, führen Sie die folgenden Befehle an der Linux-Shell des Hosts aus.

```
ethtool -K eth6 gro off
ethool -K eth6 lro off
```

Beispiel:

```
1     [root@localhost ~]# ethtool -K eth6
2
3                   Offload parameters for eth6:
4
5                                       rx-checksumming: on
6
7                                       tx-checksumming: on
```



```
8
9                       scatter-gather: on
10
11                      tcp-segmentation-offload: on
12
13                      udp-fragmentation-offload: off
14
15                      generic-segmentation-offload: on
16
17                      generic-receive-offload: off
18
19                      large-receive-offload: off
20
21                      rx-vlan-offload: on
22
23                      tx-vlan-offload: on
24
25                      ntuple-filters: off
26
27                      receive-hashing: on
28
29      [root@localhost ~]#
30  <!--NeedCopy-->
```

Beispiel:

Wenn die Linux-Brücke des Hosts wie im folgenden Beispiel als Quellgerät verwendet wird, müssen die `lro` Funktionen an den VNet-Schnittstellen ausgeschaltet werden, bei denen es sich um die virtuellen Schnittstellen handelt, die den Host mit den Gast-VMs verbinden.

```
1       [root@localhost ~]# brctl show eth6_br
2
3       bridge name     bridge  id              STP enabled interfaces
4
5       eth6_br         8000.00e0ed1861ae          no         eth6
6
7                                                             vnet0
8
9                                                             vnet2
10
11      [root@localhost ~]#
12  <!--NeedCopy-->
```

Im vorhergehenden Beispiel werden die beiden virtuellen Schnittstellen von eth6_br abgeleitet und

werden als vnet0 und vnet2 dargestellt. Führen Sie die folgenden Befehle aus, um auszuschalten `gro` und `lro` Funktionen für diese Schnittstellen.

```
    ethtool -K vnet0 gro off
            ethtool -K vnet2 gro off
            ethtool -K vnet0 lro off
                    ethtool -K vnet2 lro off
<!--NeedCopy-->
```

Promiscuous-Modus

Der Promiscuous-Modus muss aktiviert sein, damit die folgenden Funktionen funktionieren:

- L2-Modus
- Verarbeitung von Multicastdatenverkehr
- Broadcast
- IPV6-Datenverkehr
- virtual MAC
- Dynamisches Routing

Verwenden Sie den folgenden Befehl, um den Promiscuous-Modus zu aktivieren.

```
[root@localhost ~]# ifconfig eth6 promisc
[root@localhost ~]# ifconfig eth6
eth6       Link encap:Ethernet  HWaddr 78:2b:cb:51:54:a3
           inet6 addr: fe80::7a2b:cbff:fe51:54a3/64 Scope:Link
           UP BROADCAST RUNNING PROMISC MULTICAST  MTU:9000  Metric:1
           RX packets:142961 errors:0 dropped:0 overruns:0 frame:0
           TX packets:2895843 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:14330008 (14.3 MB)  TX bytes:1019416071 (1.0 GB)

[root@localhost ~]#
<!--NeedCopy-->
```

Modul erforderlich

Um eine bessere Netzwerkleistung zu erzielen, stellen Sie sicher, dass das Modul vhost_net im Linux-Host vorhanden ist. Um die Existenz des vhost_net-Moduls zu überprüfen, führen Sie den folgenden Befehl auf dem Linux-Host aus:


```
lsmod | grep ”vhost_net”
<!--NeedCopy-->
```

Wenn vhost_net noch nicht ausgeführt wird, geben Sie den folgenden Befehl ein, um es auszuführen:

```
modprobe vhost_net
<!--NeedCopy-->
```

Bereitstellen der Citrix ADC VPX Instanz mithilfe von OpenStack

October 5, 2021

Sie können eine Citrix ADC VPX-Instanz in einer OpenStack-Umgebung bereitstellen, indem Sie entweder den **Nova-Boot-Befehl** (OpenStack CLI) oder Horizon (OpenStack-Dashboard) verwenden.

Das Provisioning einer VPX-Instanz umfasst optional die Verwendung von Daten aus dem Konfigurationslaufwerk. Das Konfigurationslaufwerk ist ein spezielles Konfigurationslaufwerk, das beim Booten als CD-ROM-Gerät an die Instanz anhängt. Dieses Konfigurationslaufwerk kann verwendet werden, um Netzwerkkonfiguration wie Verwaltungs-IP-Adresse, Netzwerkmaske, Standard-Gateway zu übergeben und Kundenskripte zu injizieren.

In einer Citrix ADC Appliance ist der Standardauthentifizierungsmechanismus kennwortbasiert. Jetzt wird der SSH-Schlüsselpaar-Authentifizierungsmechanismus für Citrix ADC VPX-Instanzen in der OpenStack-Umgebung unterstützt.

Das Schlüsselpaar (öffentlicher Schlüssel und privater Schlüssel) wird generiert, bevor der Public Key Cryptographie-Mechanismus verwendet wird. Sie können verschiedene Mechanismen wie Horizon, Puttygen.exe für Windows und `ssh-keygen` für die Linux-Umgebung verwenden, um das Schlüsselpaar zu generieren. Weitere Informationen zum Generieren von Schlüsselpaaren finden Sie in der Online-Dokumentation der jeweiligen Mechanismen.

Sobald ein Schlüsselpaar verfügbar ist, kopieren Sie den privaten Schlüssel an einen sicheren Ort, auf den autorisierte Personen Zugriff haben. In OpenStack kann Public Key mit dem Boot-Befehl Horizon oder Nova auf einer VPX-Instanz bereitgestellt werden. Wenn eine VPX-Instanz mithilfe von OpenStack bereitgestellt wird, erkennt sie zuerst, dass die Instanz in einer OpenStack-Umgebung gestartet wird, indem sie eine bestimmte BIOS-Zeichenfolge liest. Diese Zeichenfolge ist OpenStack Foundation und für Red Hat Linux-Distributionen wird sie in /etc/nova/release gespeichert. Dies ist ein Standardmechanismus, der in allen OpenStack-Implementierungen verfügbar ist, die auf der KVM-Hypervisor-Plattform basieren. Das Laufwerk muss ein bestimmtes OpenStack-Label haben.

Wenn das Konfigurationslaufwerk erkannt wird, versucht die Instanz, die Netzwerkkonfiguration, die benutzerdefinierten Skripts und das SSH-Schlüsselpaar zu lesen, falls vorhanden.

Benutzer-Datendatei

Die Citrix ADC VPX-Instanz verwendet eine benutzerdefinierte OVF-Datei, auch Benutzerdatendatei genannt, um Netzwerkkonfiguration, benutzerdefinierte Skripts zu injizieren. Diese Datei wird als Teil des Konfigurationslaufwerks bereitgestellt. Hier ist ein Beispiel für eine benutzerdefinierte OVF-Datei.

```
```
<?xml version=”1.0” encoding=”UTF-8” standalone=”no”?>
<Environment xmlns:oe=”http://schemas.dmtf.org/ovf/environment/1”
xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance”
oe:id=””
xmlns=”http://schemas.dmtf.org/ovf/environment/1”
xmlns:cs=”http://schemas.citrix.com/openstack”>
<PlatformSection>
<Kind></Kind>
<Version>2016.1</Version>
<Vendor>VPX</Vendor>
<Locale>en</Locale>
</PlatformSection>
<PropertySection>
<Property oe:key=”com.citrix.netscaler.ovf.version” oe:value=”1.0”/>
<Property oe:key=”com.citrix.netscaler.platform” oe:value=”NSVPX”/>
<Property oe:key=”com.citrix.netscaler.orch_env” oe:value=”openstack-
   orch-env”/>
<Property oe:key=”com.citrix.netscaler.mgmt.ip” oe:value=”10.1.2.22”/>
<Property oe:key=”com.citrix.netscaler.mgmt.netmask” oe:value=”
   255.255.255.0”/>
<Property oe:key=”com.citrix.netscaler.mgmt.gateway” oe:value=”10.1.2.1
   ”/>
</PropertySection>
 <cs:ScriptSection>
   <cs:Version>1.0</cs:Version>
     <ScriptSettingSection xmlns=”http://schemas.citrix.com/openstack”
        xmlns:i=”http://www.w3.org/2001/XMLSchema-instance”>
         <Scripts>
           <Script>
                 <Type>shell</Type>
                 <Parameter>X Y</Parameter>
                <Parameter>Z</Parameter>
                <BootScript>before</BootScript>
```

 
```

```
                    <Text>
                          #!/bin/bash
                          echo ”Hi, how are you” $1 $2 >> /var/sample.txt
                    </Text>
              </Script>
              <Script>
                    <Type>python</Type>
                    <BootScript>after</BootScript>
                     <Text>
                          #!/bin/python
  print(”Hello”);
                     </Text>
              </Script>
    <Script>
                    <Type>perl</Type>
                    <BootScript>before</BootScript>
                     <Text>
                          !/usr/bin/perl
  my $name = ”VPX”;
  print ”Hello, World $name !\n” ;
                     </Text>
              </Script>
              <Script>
                   <Type>nscli</Type>
                   <BootScript>after</BootScript>
                   <Text>
                    add vlan 33
  bind vlan 33 -ifnum 1/2
                   </Text>
              </Script>
           </Scripts>
      </ScriptSettingSection>
  </cs:ScriptSection>
</Environment>
<!--NeedCopy--> ```
```

In der OVF-Datei vor ”PropertySection” wird für die NetScaler-Netzwerkkonfiguration verwendet, während sie zum Einschließen aller Skripts verwendet <cs:ScriptSection> wird. <Scripts></Scripts> Tags werden verwendet, um alle Skripts zusammen zu bündeln. Jedes Skript ist zwischen <Script> </Script> Tags definiert. Jedes Skript-Tag hat folgende Felder/Tags:

a) <Type>: Gibt den Wert für den Skripttyp an. Mögliche Werte: Shell/Perl/Python/NSLCI (für NetScaler CLI-Skripts)

b) <Parameter>: Stellt Parameter für das Skript bereit. Jedes Skript kann mehrere <Parameter> Tags

haben.

c) <BootScript>: Gibt den Skriptausführungspunkt an. Mögliche Werte für dieses Tag: vorher/nachher. “before” gibt an, dass das Skript ausgeführt wird, bevor PE auftaucht. “after” gibt an, dass das Skript ausgeführt wird, nachdem PE angezeigt wird.

d) <Text>: Fügt den Inhalt eines Skripts ein.

> **Hinweis:**
>
> Derzeit kümmert sich die VPX-Instanz nicht um die Bereinigung von Skripten. Als Administrator müssen Sie die Gültigkeit des Skripts überprüfen.
>
> Nicht alle Abschnitte müssen vorhanden sein. Verwenden Sie eine leere “PropertySection”, um nur Skripts zu definieren, die beim ersten Start oder einer leeren Ausführung ausgeführt werden sollen, um nur die Netzwerkkonfiguration zu definieren.
>
> Nachdem die erforderlichen Abschnitte der OVF-Datei (Benutzerdatendatei) ausgefüllt wurden, verwenden Sie diese Datei, um die VPX-Instanz bereitzustellen.

Netzwerkkonfiguration

Im Rahmen der Netzwerkkonfiguration lautet die VPX-Instanz:

- Verwaltungs-IP-Adresse
- Netzwerkmaske
- Standard-Gateway

Nachdem die Parameter erfolgreich gelesen wurden, werden sie in der NetScaler Konfiguration aufgefüllt, damit die Instanz remote verwaltet werden kann. Wenn die Parameter nicht erfolgreich gelesen werden oder das Konfigurationslaufwerk nicht verfügbar ist, wechselt die Instanz zum Standardverhalten:

- Die Instanz versucht, die IP-Adressinformationen von DHCP abzurufen.
- Wenn DHCP ausfällt oder Times-Out ausfällt, wird die Instanz mit der Standardnetzwerkkonfiguration (192.168.100.1/16) erstellt.

Kundenskript

Die VPX-Instanz erlaubt es, während der ersten Bereitstellung ein benutzerdefiniertes Skript auszuführen. Die Appliance unterstützt Skripts vom Typ Shell, Perl, Python und Citrix ADC CLI-Befehle.

SSH-Schlüsselpaar-Authentifizierung

Die VPX-Instanz kopiert den öffentlichen Schlüssel, der im Konfigurationslaufwerk als Teil der Instanzmeta-Daten verfügbar ist, in die Datei authorized_keys. Dadurch kann der Benutzer mit dem privaten Schlüssel auf die Instanz zugreifen.

> **Hinweis:**
>
> Wenn ein SSH-Schlüssel angegeben wird, funktionieren die Standardanmeldeinformationen (nsroot/nsroot) nicht mehr. Wenn ein kennwortbasierter Zugriff erforderlich ist, melden Sie sich mit dem entsprechenden privaten SSH-Schlüssel an und legen Sie manuell ein Kennwort fest.

Voraussetzungen

Bevor Sie eine VPX-Instanz in der OpenStack-Umgebung bereitstellen, extrahieren Sie die Datei `.qcow2` aus der TGZ-Datei und bauen Sie

Ein OpenStack-Bild aus dem qcow2-Image. Führen Sie die folgenden Schritte aus:

1. Extrahieren Sie die `.qcow2` Datei aus der `.tqz` Datei, indem Sie den folgenden Befehl eingeben

```
tar xvzf <TAR file>
tar xvzf <NSVPX-KVM-12.0-26.2_nc.tgz>
NSVPX-KVM.xml
NSVPX-KVM-12.0-26.2_nc.qcow2
```

2. Erstellen Sie ein OpenStack-Image mit der in Schritt 1 extrahierten `.qcoz2` Datei, indem Sie den folgenden Befehl eingeben.

```
openstack image create --container-format bare --property
   hw_disk_bus=ide --disk-format qcow2 --file <path to qcow2 file>
    --public <name of the OpenStack image>

glance image-create --name=”NS-VPX-12-0-26-2” --property
   hw_disk_bus=ide --ispublic=
true --container-format=bare --disk-format=qcow2< NSVPX-KVM
   -12.0-26.2_nc.qcow2
```

Abbildung 1: Die folgende Abbildung enthält eine Beispielausgabe für den Befehl glance image-create.


```
+------------------+------------------------------------------------------+
| Field            | Value                                                |
+------------------+------------------------------------------------------+
| checksum         | 154ade3fc7dca7d1706b1d03d7d97552                     |
| container_format | bare                                                 |
| created_at       | 2017-03-13T08:52:31Z                                 |
| disk_format      | qcow2                                                |
| file             | /v2/images/322c1e0f-cce8-4b7b-b53e-bd8152c388ed/file |
| id               | 322c1e0f-cce8-4b7b-b53e-bd8152c388ed                 |
| min_disk         | 0                                                    |
| min_ram          | 0                                                    |
| name             | VPX-KVM-12.0-26.2                                    |
| owner            | 58d17d81df5d4406afbb4fdab3a58d79                     |
| properties       | hw_disk_bus='ide'                                    |
| protected        | False                                                |
| schema           | /v2/schemas/image                                    |
| size             | 784338944                                            |
| status           | active                                               |
| updated_at       | 2017-03-13T08:52:43Z                                 |
| virtual_size     | None                                                 |
| visibility       | public                                               |
+------------------+------------------------------------------------------+
```

Provisioning einer VPX-Instanz

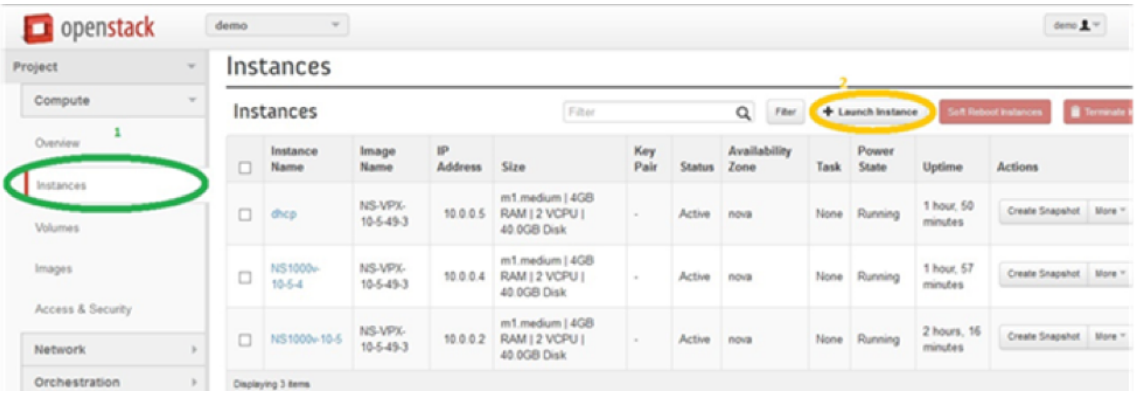
Sie können eine VPX-Instanz auf zwei Arten bereitstellen, indem Sie eine der folgenden Optionen verwenden:

- Horizon (OpenStack-Dashboard)
- Nova-Startbefehl (OpenStack CLI)

Bereitstellen einer VPX-Instanz mit dem OpenStack-Dashboard

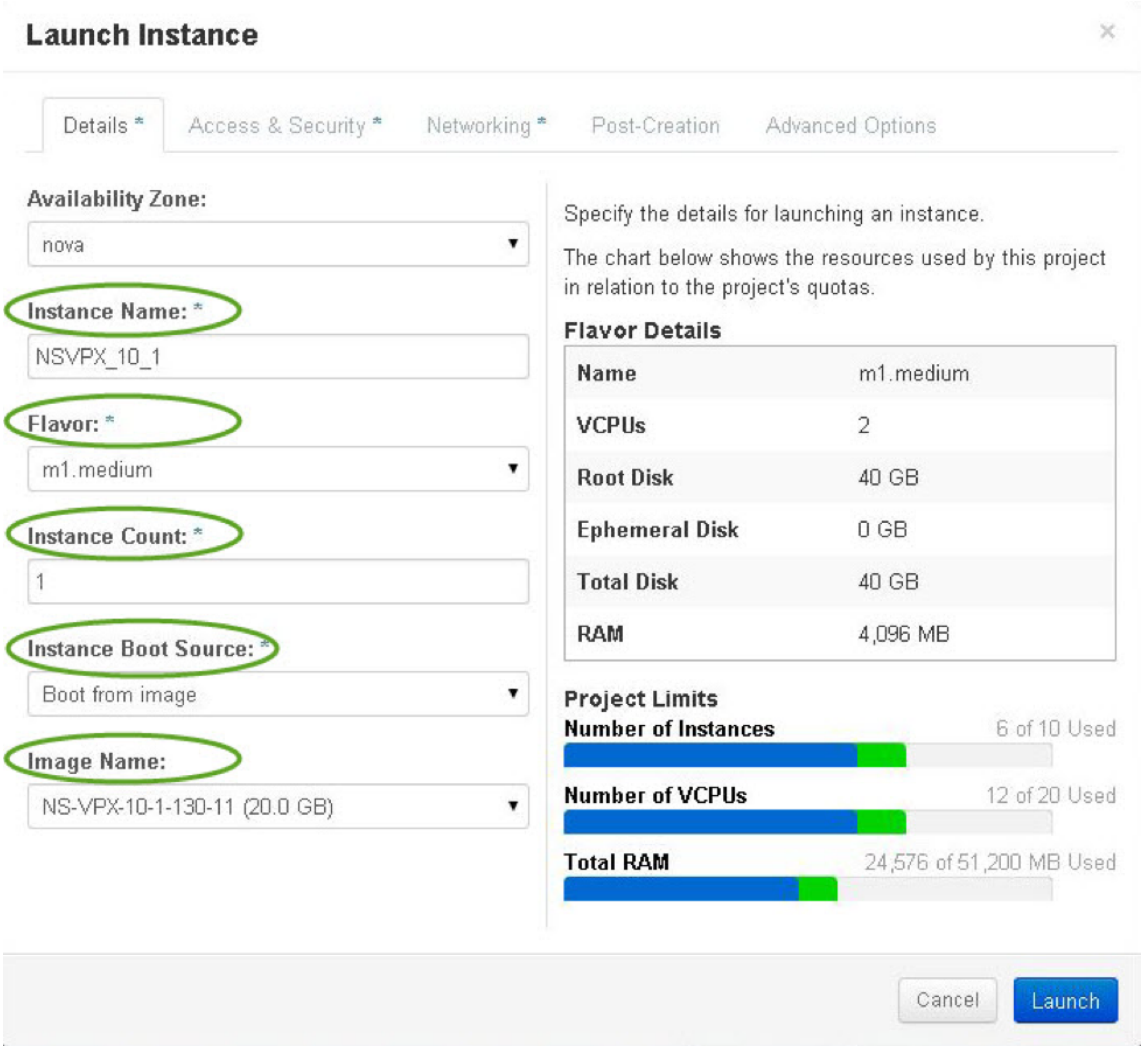
Gehen Sie folgendermaßen vor, um die VPX-Instanz mithilfe von Horizon bereitzustellen:

1. Melden Sie sich beim OpenStack-Dashboard an.
2. Wählen Sie im Projektfenster auf der linken Seite des Dashboards die Option **Instanzen**aus.
3. Klicken Sie im Instanzen Bedienfeld auf **Instanz starten**, um den Instanzentart-Assistenten zu öffnen.



4. Geben Sie im Assistenten zum Starten von Instanz die folgenden Details ein:

   a) Instanzname
   b) Instanz-Flavor
   c) Instanzanzahl
   d) Instanz-Boot-Quelle
   e) Imagename



5. Stellen Sie ein neues Schlüsselpaar oder ein vorhandenes Schlüsselpaar über Horizon bereit, indem Sie die folgenden Schritte ausführen:

   a) Wenn Sie kein vorhandenes Schlüsselpaar haben, erstellen Sie den Schlüssel mithilfe vorhandener Mechanismen. Wenn Sie einen vorhandenen Schlüssel haben, überspringen Sie diesen Schritt.

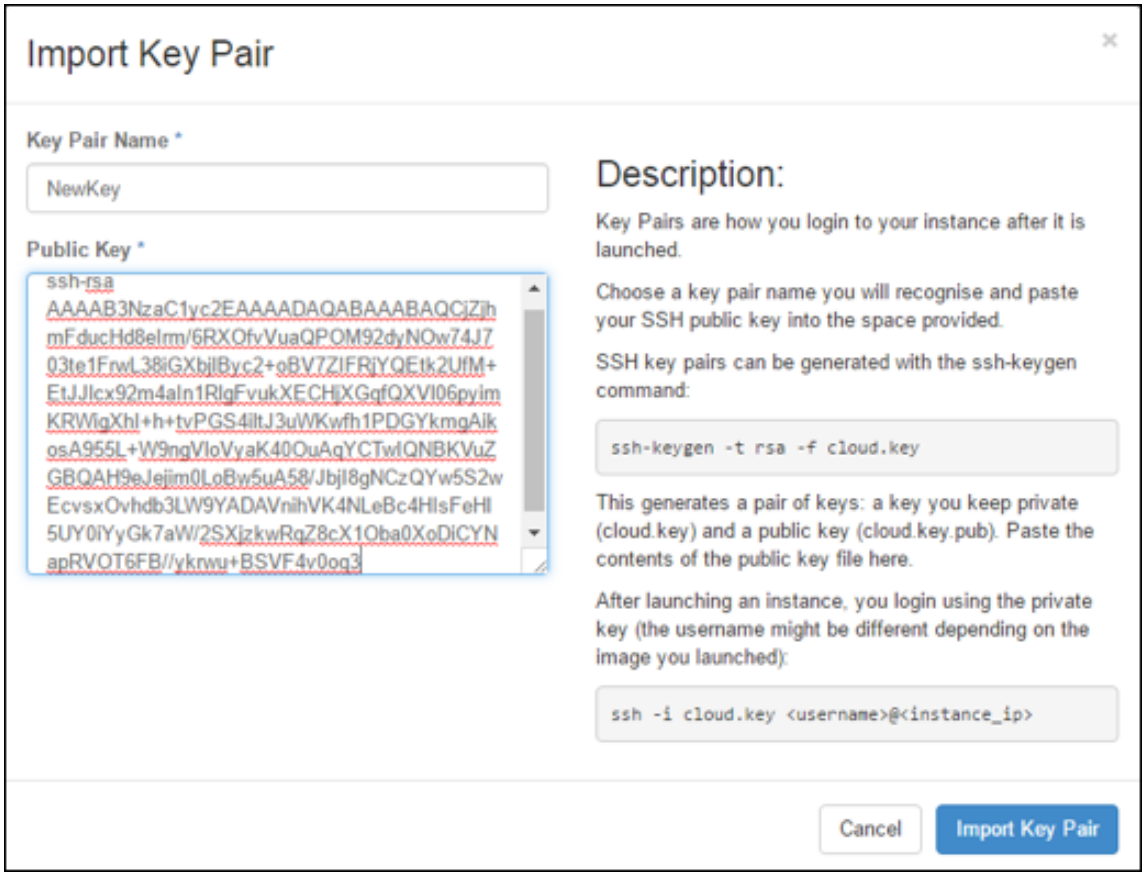
   b) Kopieren Sie den Inhalt des öffentlichen Schlüssels.

   c) Gehen Sie zu **Horizon > Instanzen > Neue Instanzen erstellen**.

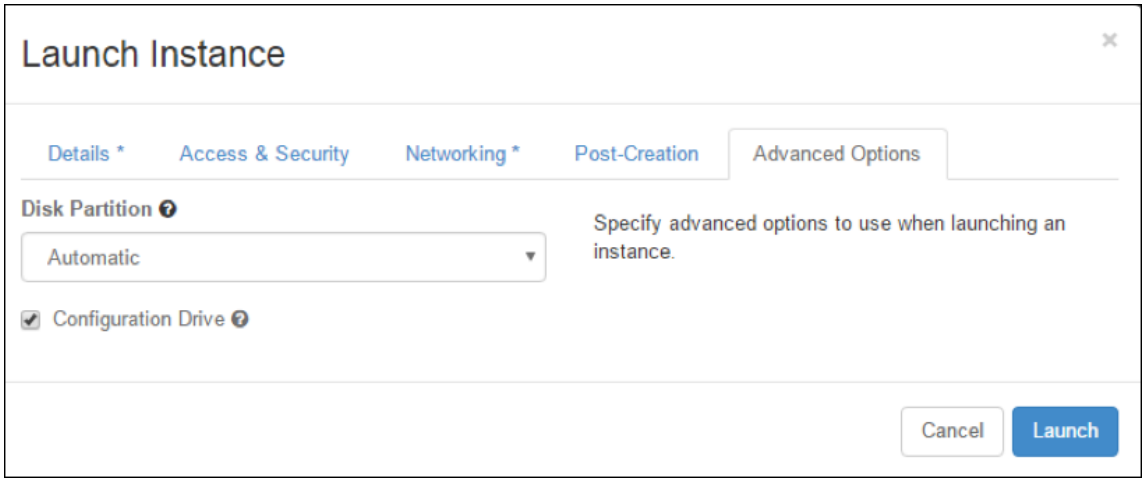
d) Klicken Sie auf **Zugriff und Sicherheit**.

e) Klicken Sie auf das + Zeichen neben dem Dropdownmenü **Schlüsselpaar** und geben Sie Werte für die angezeigten Parameter an.

f) Fügen Sie den Inhalt des öffentlichen Schlüssels in das Feld *Öffentlicher Schlüssel* ein, geben Sie dem Schlüssel einen Namen und klicken Sie auf **Schlüsselpaar importieren**.



6. Klicken Sie im Assistenten auf die Registerkarte **Post-Creation**. Fügen Sie im Anpassungsskript den Inhalt der Benutzerdatendatei hinzu. Die Benutzerdatendatei enthält die IP-Adresse, Netmask- und Gateway-Details sowie Kundenskripte der VPX-Instanz.
7. Nachdem ein Schlüsselpaar ausgewählt oder importiert wurde, aktivieren Sie die Option config-drive und klicken Sie auf **Starten**.



Provisioning der VPX-Instanz mi OpenStack CLI

Folgen Sie diesen Schritten zum Provisioning einer VPX-Instanz mit OpenStack CLI.

1. Um ein Image aus qcow2 zu erstellen, geben Sie den folgenden Befehl ein:

   ```
   openstack image create --container-format bare --property hw_disk_bus=
   ide --diskformat qcow2 --file NSVPX-OpenStack.qcow2 --public VPX-ToT-
   Image
   ```

2. Um ein Image zum Erstellen einer Instanz auszuwählen, geben Sie den folgenden Befehl ein:

   ```
   openstack image list | more
   ```

3. Um eine Instanz eines bestimmten Flavor zu erstellen, geben Sie den folgenden Befehl ein, um eine Flavor-ID/Name von aus einer Liste auszuwählen:

   ```
   openstack flavor list
   ```

4. Um eine Netzwerkkarte an ein bestimmtes Netzwerk anzuhängen, geben Sie den folgenden Befehl ein, um eine Netzwerk-ID aus einer Netzwerkliste auszuwählen:

   ```
   openstack network list
   ```

5. Um eine Instanz zu erstellen, geben Sie den folgenden Befehl ein:

   ```
   1 openstack server create --flavor FLAVOR_ID --image IMAGE_ID --key-
       name KEY_NAME
   2 --user-data USER_DATA_FILE_PATH --config-drive True --nic net-id=
       net-uuid
   3 INSTANCE_NAME
   4 openstack server create --image VPX-ToT-Image --flavor m1.medium
       --user-data
   ```



```
5 ovf.xml --config-drive True --nic net-id=2734911b-ee2b-48d0-a1b6-3
     efd44b761b9
6 VPX-ToT
```

Abbildung 2: Die folgende Abbildung zeigt eine Beispielausgabe.

```
+--------------------------------------+--------------------------------------------------------------------------+
| Field                                | Value                                                                    |
+--------------------------------------+--------------------------------------------------------------------------+
| OS-DCF:diskConfig                    | MANUAL                                                                   |
| OS-EXT-AZ:availability_zone          |                                                                          |
| OS-EXT-SRV-ATTR:host                 | None                                                                     |
| OS-EXT-SRV-ATTR:hypervisor_hostname  | None                                                                     |
| OS-EXT-SRV-ATTR:instance_name        | instance-000001c2                                                        |
| OS-EXT-STS:power_state               | 0                                                                        |
| OS-EXT-STS:task_state                | scheduling                                                               |
| OS-EXT-STS:vm_state                  | building                                                                 |
| OS-SRV-USG:launched_at               | None                                                                     |
| OS-SRV-USG:terminated_at             | None                                                                     |
| accessIPv4                           |                                                                          |
| accessIPv6                           |                                                                          |
| addresses                            |                                                                          |
| adminPass                            | pFVvMtq7N8Z6                                                             |
| config_drive                         | True                                                                     |
| created                              | 2017-03-13T10:32:59Z                                                     |
| flavor                               | m1.medium (3)                                                            |
| hostId                               |                                                                          |
| id                                   | a1fe991e-3604-43a0-9dd6-59fa0f3749df                                     |
| image                                | VPX-ToT-Image (f0c2f9d1-08f2-4b2e-9943-2ee6bc2edbc7)                     |
| key_name                             | None                                                                     |
| name                                 |VPX-ToT                                                                   |
| os-extended-volumes:volumes_attached | []                                                                       |
| progress                             | 0                                                                        |
| project_id                           | 58d17d81df5d4406afbb4fdab3a58d79                                         |
| properties                           |                                                                          |
| security_groups                      | [{u'name': u'default'}]                                                  |
| status                               | BUILD                                                                    |
| updated                              | 2017-03-13T10:33:00Z                                                     |
| user_id                              | a6347b33916b4eb1b1f76360a9c8f935                                         |
+--------------------------------------+--------------------------------------------------------------------------+
```

Bereitstellen der Citrix ADC VPX-Instanz mithilfe des Virtual Machine Manager

October 5, 2021

Der Virtual Machine Manager ist ein Desktop-Tool zur Verwaltung von VM-Gästen. Es ermöglicht Ihnen, neue VM-Gäste und verschiedene Arten von Speicher zu erstellen und virtuelle Netzwerke zu verwalten. Sie können über den integrierten VNC-Viewer auf die grafische Konsole der VM-Gäste zugreifen und Performance-Statistiken entweder lokal oder remote anzeigen.

Nach der Installation Ihrer bevorzugten Linux-Distribution mit aktivierter KVM-Virtualisierung können Sie mit der Provisioning virtueller Maschinen fortfahren.

Wenn Sie mit Virtual Machine Manager eine Citrix ADC VPX-Instanz bereitstellen, stehen Ihnen zwei Optionen zur Verfügung:

- Geben Sie die IP-Adresse, das Gateway und die Netzmaske manuell ein
- IP-Adresse, Gateway und Netzmaske automatisch zuweisen (Auto-Provisioning)

Sie können zwei Arten von Images verwenden, um eine Citrix ADC VPX-Instanz bereitzustellen:

- RAW
- QCOW2

Sie können ein Citrix ADC VPX RAW-Image in ein QCOW2-Image konvertieren und die Citrix ADC VPX-Instanz bereitstellen. Um das RAW-Image in ein QCOW2-Image zu konvertieren, geben Sie den folgenden Befehl ein:

```
qemu-img convert -O qcow2 original-image.raw image-converted.qcow
```

Beispiel:

```
qemu-img convert -O qcow2 NSVPX-KVM-11.1-12.5_nc.raw NSVPX-KVM-11.1-12.5_nc
.qcow
```

Eine typische Citrix ADC VPX Bereitstellung auf KVM umfasst die folgenden Schritte:

- Überprüfen der Voraussetzungen für das automatische Provisioning einer Citrix ADC VPX-Instanz
- Provisioning der Citrix ADC VPX-Instanz mit einem RAW-Image
- Provisioning der Citrix ADC VPX-Instanz mit einem QCOW2-Image
- Hinzufügen zusätzlicher Schnittstellen zu einer VPX-Instanz mithilfe von Virtual Machine Manager

Prüfen der Voraussetzungen für die automatische Bereitstellung einer Citrix ADC VPX-Instanz

Die automatische Bereitstellung ist eine optionale Funktion und beinhaltet die Verwendung von Daten vom CD-ROM-Laufwerk. Wenn diese Funktion aktiviert ist, müssen Sie die Verwaltungs-IP-Adresse, die Netzwerkmaske und das Standard-Gateway der Citrix ADC VPX-Instanz während der Erstinstallation nicht eingeben.

Sie müssen die folgenden Aufgaben ausführen, bevor Sie eine VPX-Instanz automatisch bereitstellen können:

1. Erstellen Sie eine benutzerdefinierte XML-Datei oder Benutzerdatendatei (Open Virtualization Format) (OVF).
2. Konvertieren Sie die OVF-Datei in ein ISO-Image mit einer Online-Anwendung (z. B. PowerISO).
3. Hängen Sie das ISO-Image auf dem KVM-Host mit beliebigen Secure Copy (SCP) -basierten Tools ein.

Beispiel für OVF-XML-Datei:

Hier ist ein Beispiel für den Inhalt einer OVF-XML-Datei, die Sie als Beispiel verwenden können, um Ihre Datei zu erstellen.


```
<?xml version=”1.0” encoding=”UTF-8” standalone=”no”?>

<Environment xmlns:oe=”`http://schemas.dmtf.org/ovf/environment/1”`

xmlns:xsi=”`http://www.w3.org/2001/XMLSchema-instance”`

oe:id=””

xmlns=”`http://schemas.dmtf.org/ovf/environment/1”`

xmlns:cs=”`http://schemas.citrix.com/openstack”>`

<PlatformSection>

<Kind></Kind>

<Version>2016.1</Version>

<Vendor>VPX</Vendor>

<Locale>en</Locale>

</PlatformSection>

<PropertySection>

<Property oe:key=”com.citrix.netscaler.ovf.version” oe:value=”1.0”/>

<Property oe:key=”com.citrix.netscaler.platform” oe:value=”NSVPX”/>

<Property oe:key=”com.citrix.netscaler.orch_env” oe:value=”KVM”/>

<Property oe:key=”com.citrix.netscaler.mgmt.ip” oe:value=”10.1.2.22”/>

<Property oe:key=”com.citrix.netscaler.mgmt.netmask” oe:value=”
   255.255.255.0”/>

<Property oe:key=”com.citrix.netscaler.mgmt.gateway” oe:value=”10.1.2.1
   ”/>

</PropertySection>

</Environment>
<!--NeedCopy-->
```


In der vorangehenden OVF-XML-Datei wird “PropertySection” für die NetScaler-Netzwerkkonfiguration verwendet. Wenn Sie die Datei erstellen, geben Sie Werte für die Parameter an, die am Ende des Beispiels hervorgehoben werden:

- Verwaltungs-IP-Adresse
- Netzmaske
- Gateway

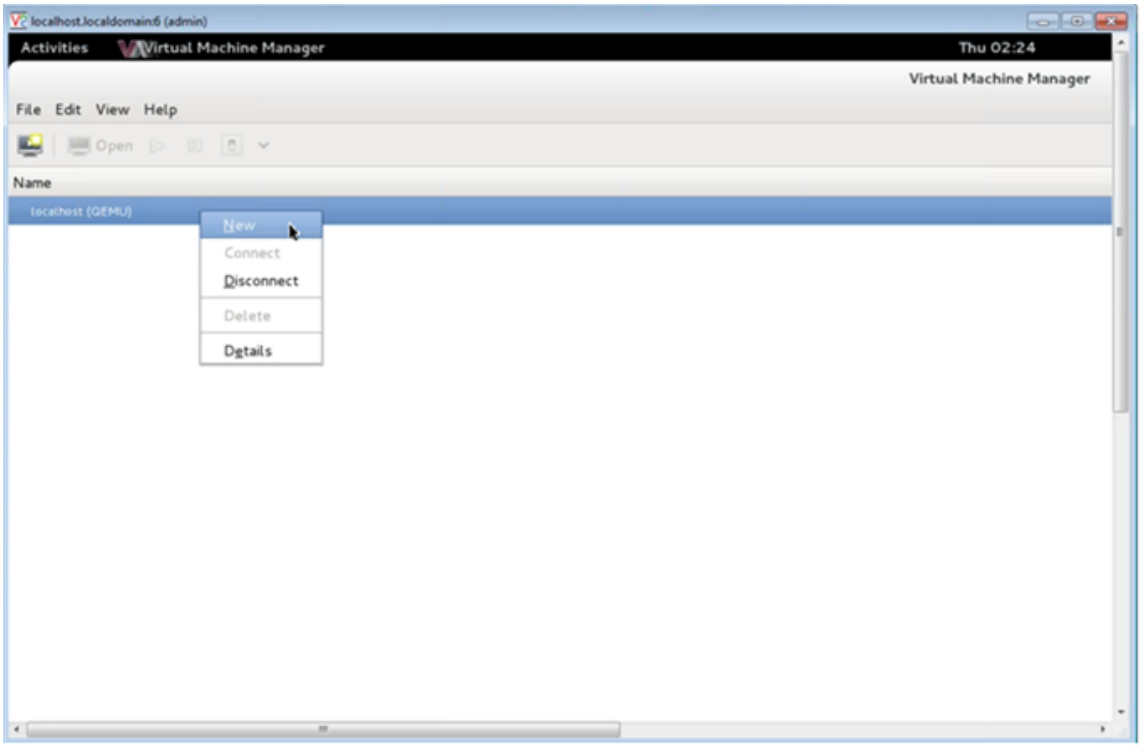
> **Wichtig**
>
> Wenn die OVF-Datei nicht ordnungsgemäß XML-formatiert ist, wird der VPX-Instanz die Standard-Netzwerkkonfiguration zugewiesen, nicht die in der Datei angegebenen Werte.

Bereitstellen der Citrix ADC VPX Instanz mithilfe eines RAW-Images

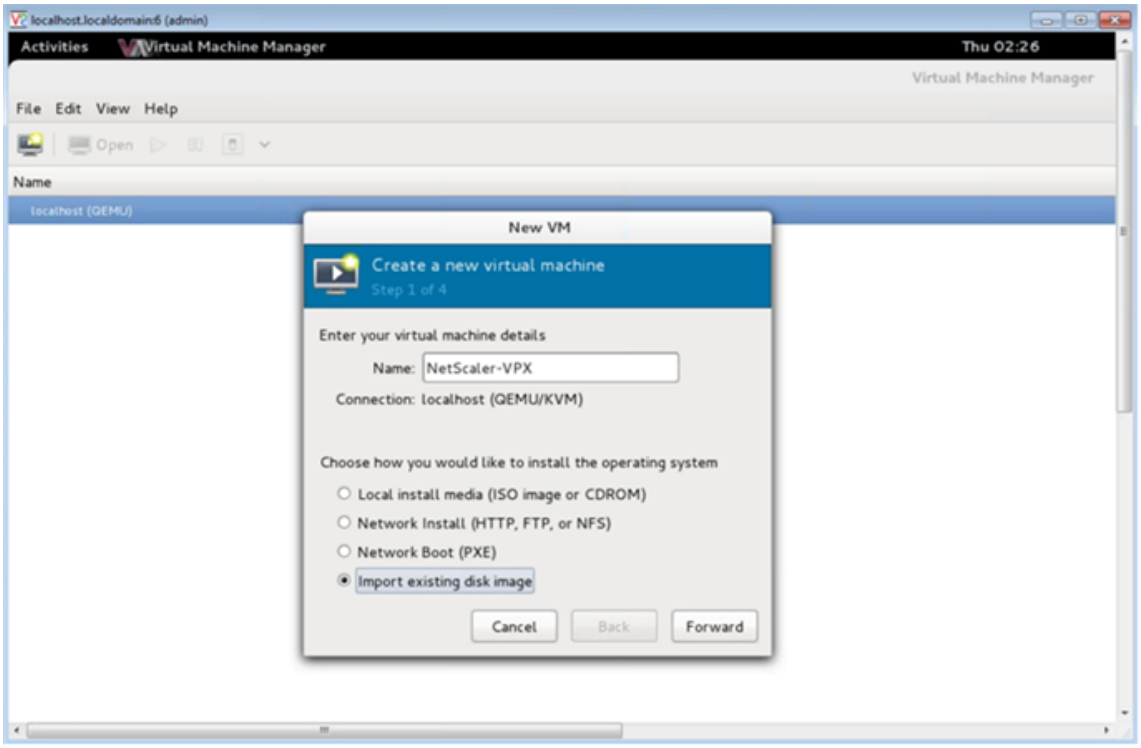
Mit dem Virtual Machine Manager können Sie eine Citrix ADC VPX-Instanz mit einem RAW-Image bereitstellen.

Gehen Sie folgendermaßen vor, um eine Citrix ADC VPX-Instanz mithilfe des Virtual Machine Manager bereitzustellen:

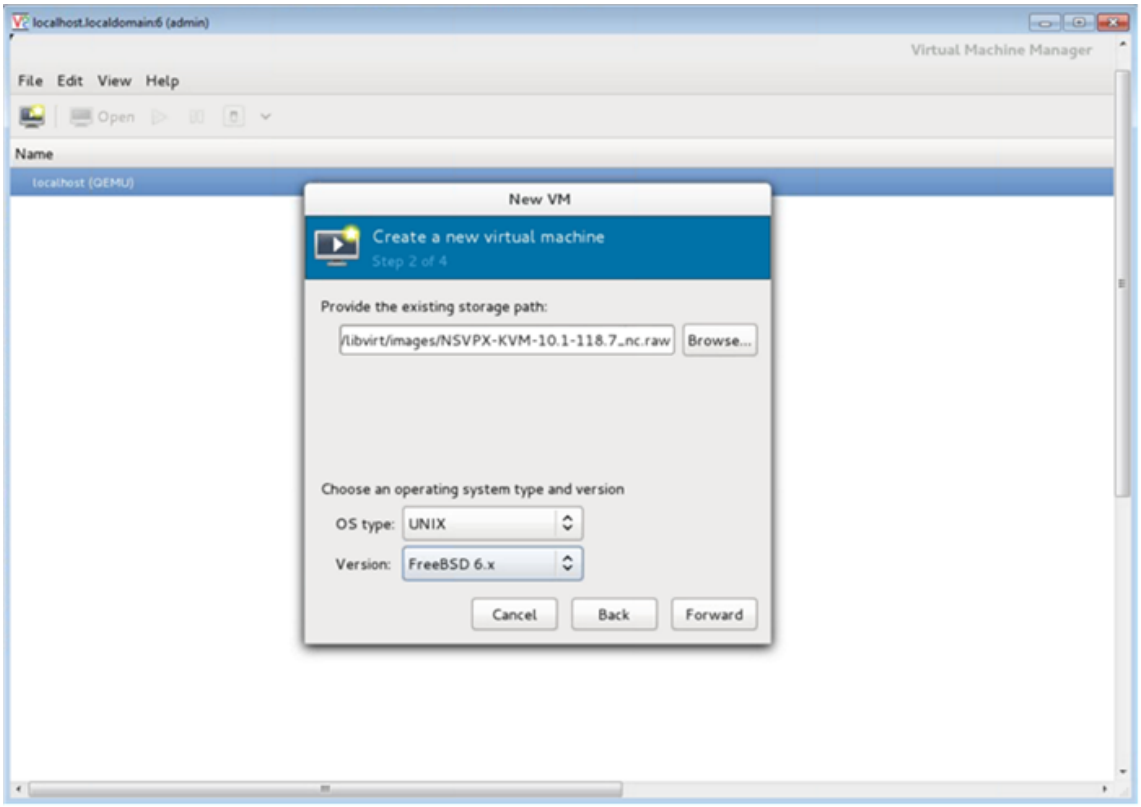
1. Öffnen Sie den Virtual Machine Manager (**Anwendung** > **Systemprogramme** > **Virtual Machine Manager**), und geben Sie die Anmeldeinformationen im Fenster **Authentifizieren** ein.
2. Klicken Sie auf das  oder klicken Sie mit der rechten Maustaste auf **localhost (QEMU)**, um eine neue Citrix ADC VPX-Instanz zu erstellen.



3. Geben Sie im Textfeld **Name** einen Namen für die neue VM ein (z. B. NetScaler-VPX).
4. Wählen Sie im Fenster **Neue VM** unter Auswählen, wie Sie das Betriebssystem installieren möchten die Option **Vorhandenes Datenträgerimage importieren** aus, und klicken Sie dann auf **Weiterleiten**.

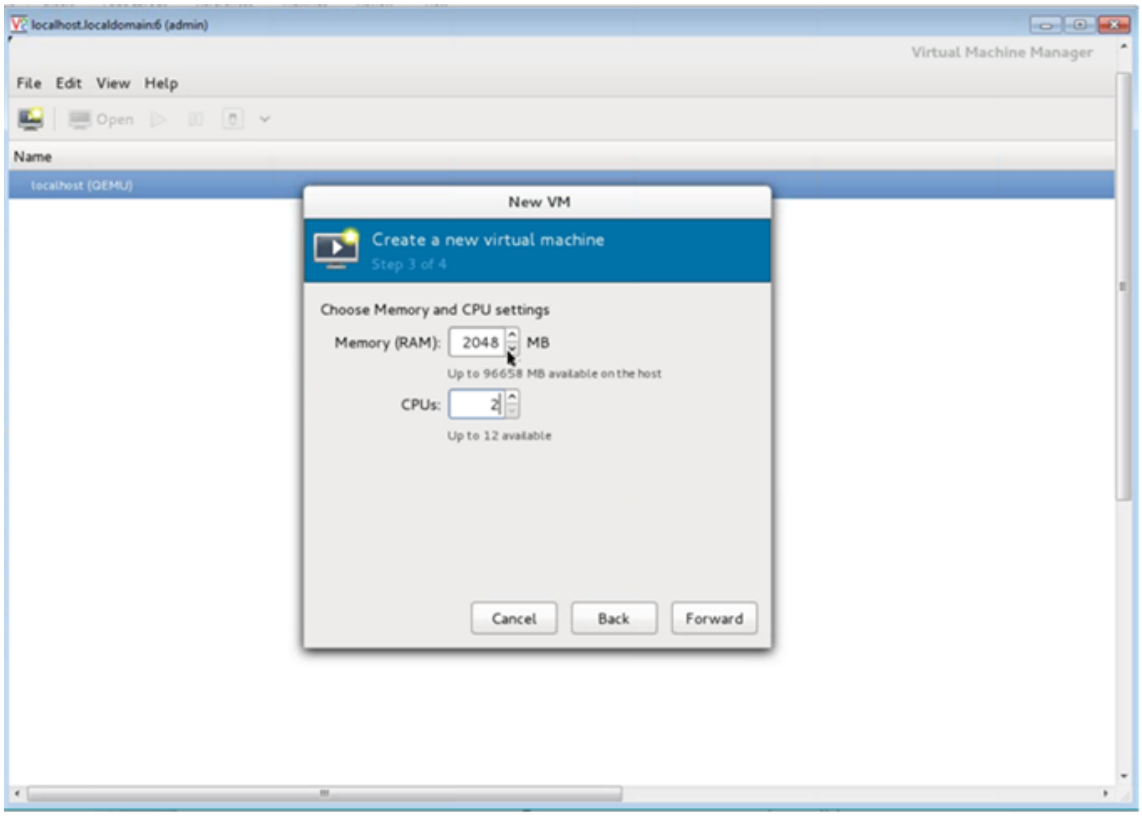


5. Navigieren Sie im Feld **Vorhandenen Speicherpfad bereitstellen** im Pfad zum Image. Wählen Sie den Betriebssystemtyp als UNIX und Version als FreeBSD 6.x. Klicken Sie dann auf **Weiterleiten**.

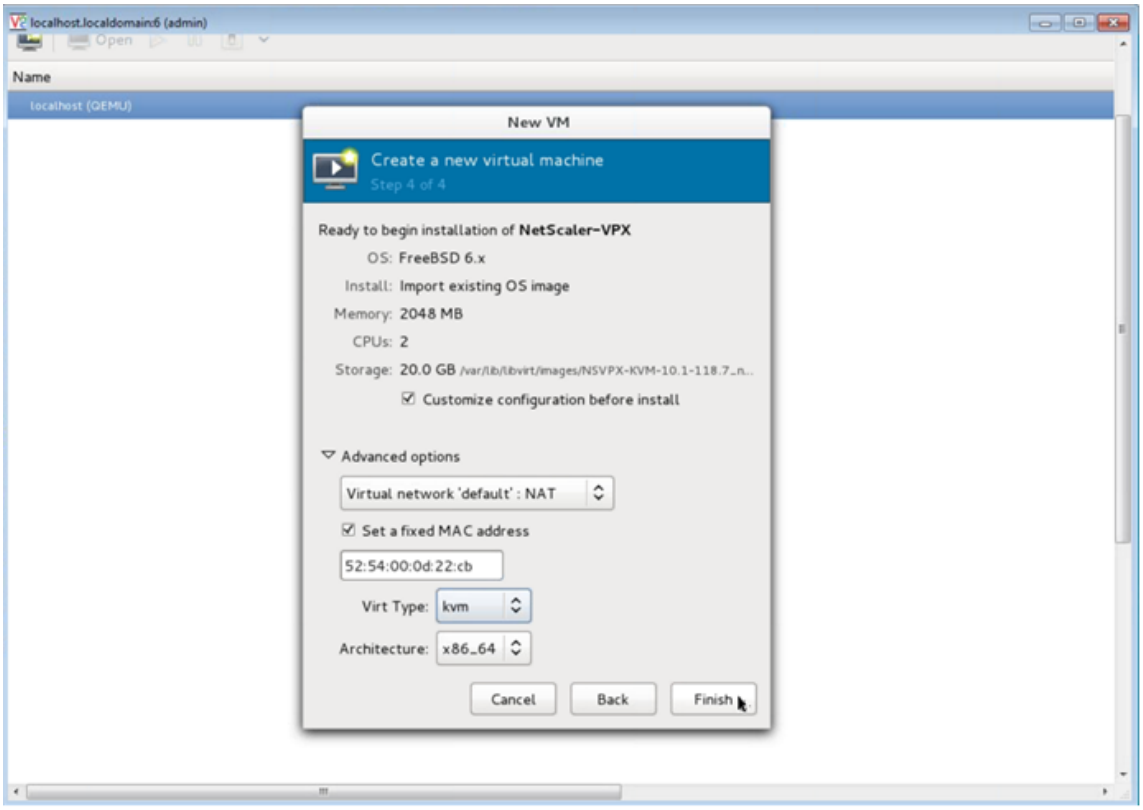


6. **Wählen Sie unter Speicher- und CPU-Einstellungen** auswählen die folgenden Einstellungen aus, und klicken Sie dann auf **Weiterleiten** :

   - Arbeitsspeicher (RAM) — 2048 MB
   - CPU— 2

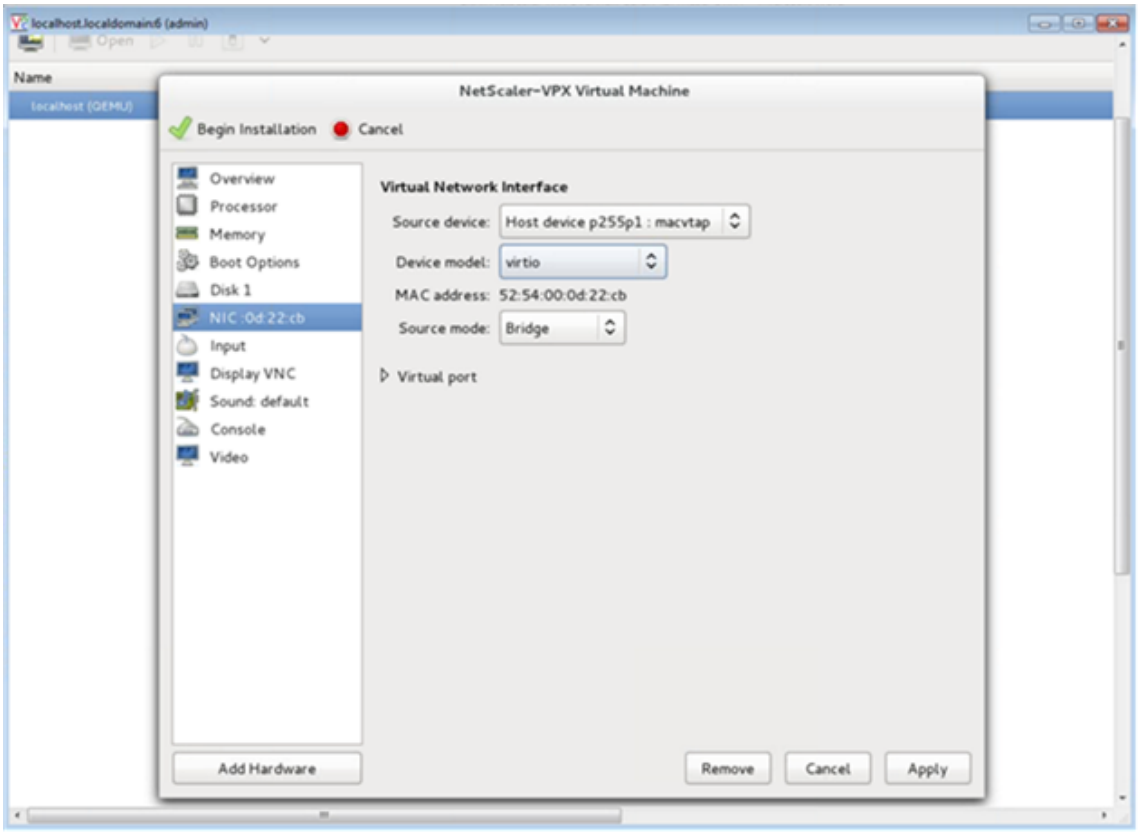


7. Aktivieren Sie das Kontrollkästchen **Konfiguration vor der Installation anpassen** . Optional können Sie unter **Erweiterte Optionen** die MAC-Adresse anpassen. Stellen Sie sicher, dass der ausgewählte **Virt-Typ** KVM ist und die ausgewählte Architektur x86_64 ist. Klicken Sie auf **Fertig stellen**.



8. Wählen Sie eine Netzwerkkarte aus, und stellen Sie die folgende Konfiguration bereit:

   - Quellgerät- `ethX macvtap` oder Bridge
   - Geräte-Modell— `virtio`
   - Quellmodus— Brücke



9. Klicken Sie auf **Apply**.
10. Wenn Sie die VPX-Instanz automatisch bereitstellen möchten, finden Sie im Abschnitt **Aktivieren des automatischen Provisioning durch Anschließen eines CD-ROM-Laufwerks** in diesem Dokument. Klicken Sie andernfalls auf **Installation beginnen**. Nachdem Sie den Citrix ADC VPX auf KVM bereitgestellt haben, können Sie weitere Schnittstellen hinzufügen.

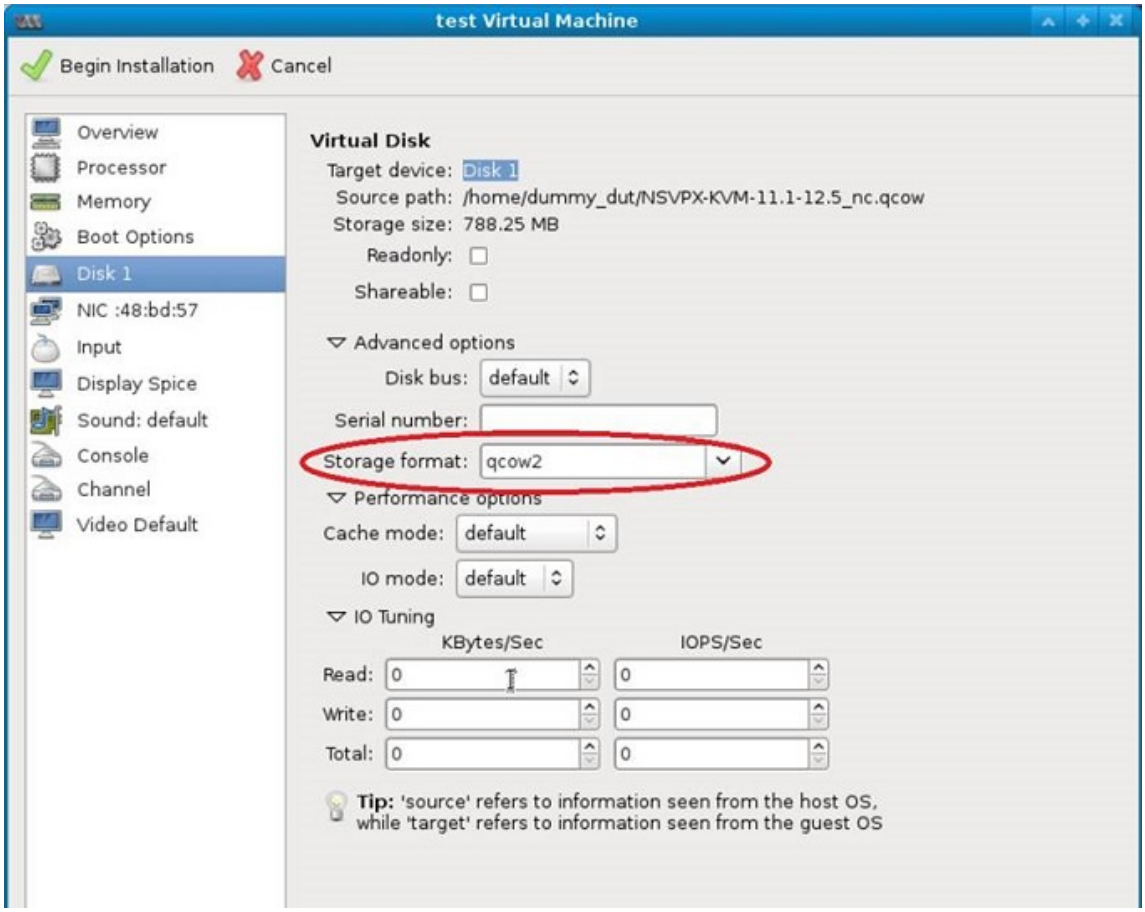
Bereitstellen der Citrix ADC VPX Instanz mithilfe eines QCOW2-Images

Mit Virtual Machine Manager können Sie die Citrix ADC VPX-Instanz mit einem QCOW2-Image bereitstellen.

Gehen Sie folgendermaßen vor, um eine Citrix ADC VPX-Instanz mit einem QCOW2-Image bereitzustellen:

1. Folgen Sie **Schritt 1** bis **Schritt 8** unter Bereitstellen der Citrix ADC VPX-Instanz mithilfe eines RAW-Images.

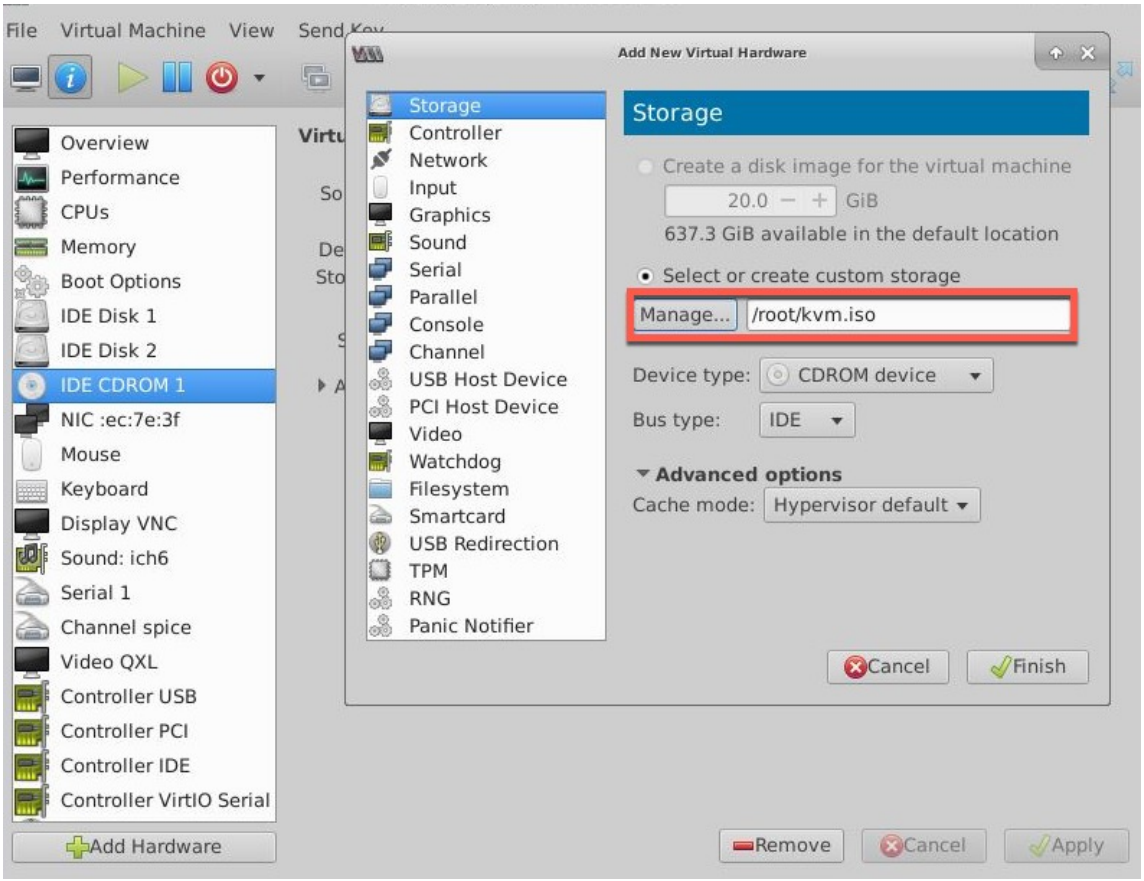
   Hinweis: Stellen Sie sicher, dass Sie **qcow2**image in **Schritt 5**auswählen.
2. Wählen Sie **Datenträger 1** aus, und klicken Sie auf **Erweiterte Optionen** .
3. Wählen Sie **qcow2** aus der Dropdownliste Speicherformat aus.



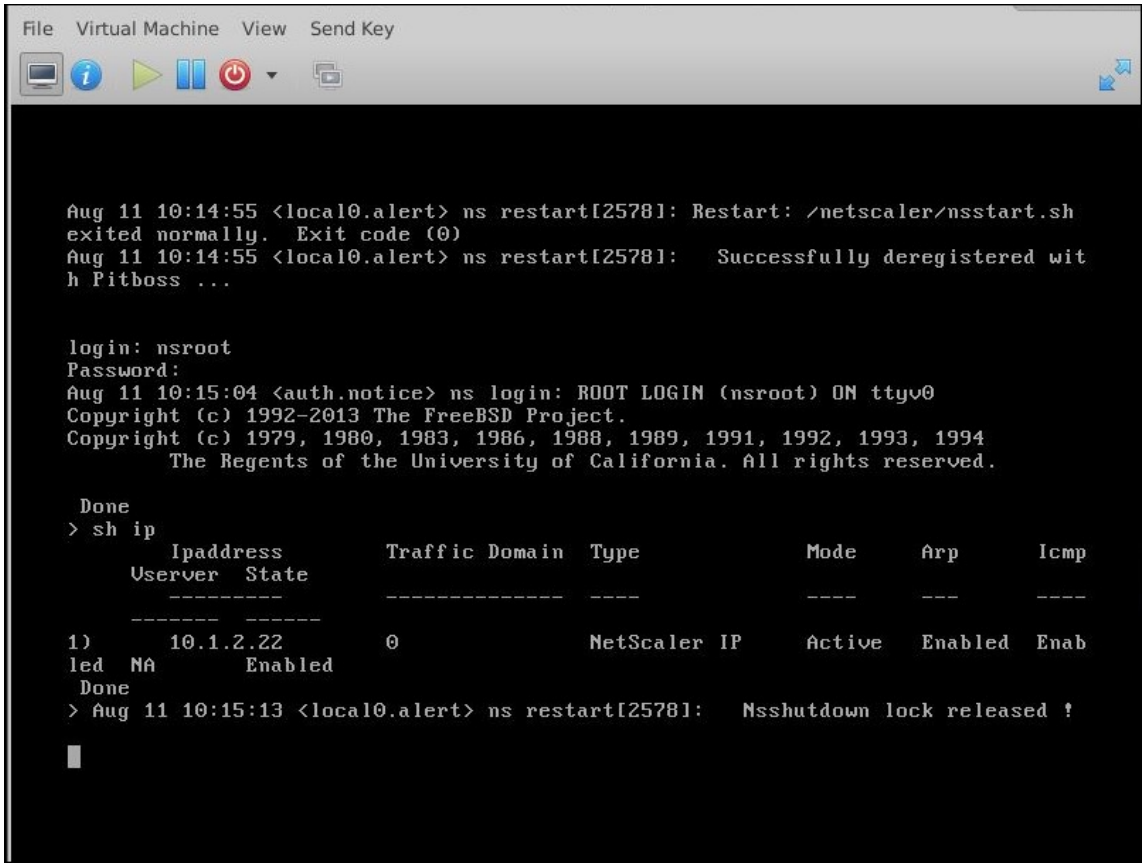
4. Klicken Sie auf **Übernehmen**, und klicken Sie dann auf **Installation beginnen**. Nachdem Sie den Citrix ADC VPX auf KVM bereitgestellt haben, können Sie weitere Schnittstellen hinzufügen.

Aktivieren der automatischen Bereitstellung durch Anfügen eines CD-ROM-Laufwerks

1. Klicken Sie auf **Hardware hinzufügen > Speicher > Gerätetyp > CD-ROM-Gerät**.
2. Klicken Sie auf **Verwalten**, wählen Sie die richtige ISO-Datei aus, die Sie im Abschnitt “Voraussetzungen für die automatische Bereitstellung einer Citrix ADC VPX-Instanz” bereitgestellt haben, und klicken Sie auf **Fertig stellen**. Eine neue CDROM unter Ressourcen auf Ihrer Citrix ADC VPX-Instanz wird erstellt.



3. Schalten Sie die VPX-Instanz ein und stellt automatisch die in der OVF-Datei bereitgestellte Netzwerkkonfiguration bereit, wie in der Beispielbildaufnahme gezeigt.



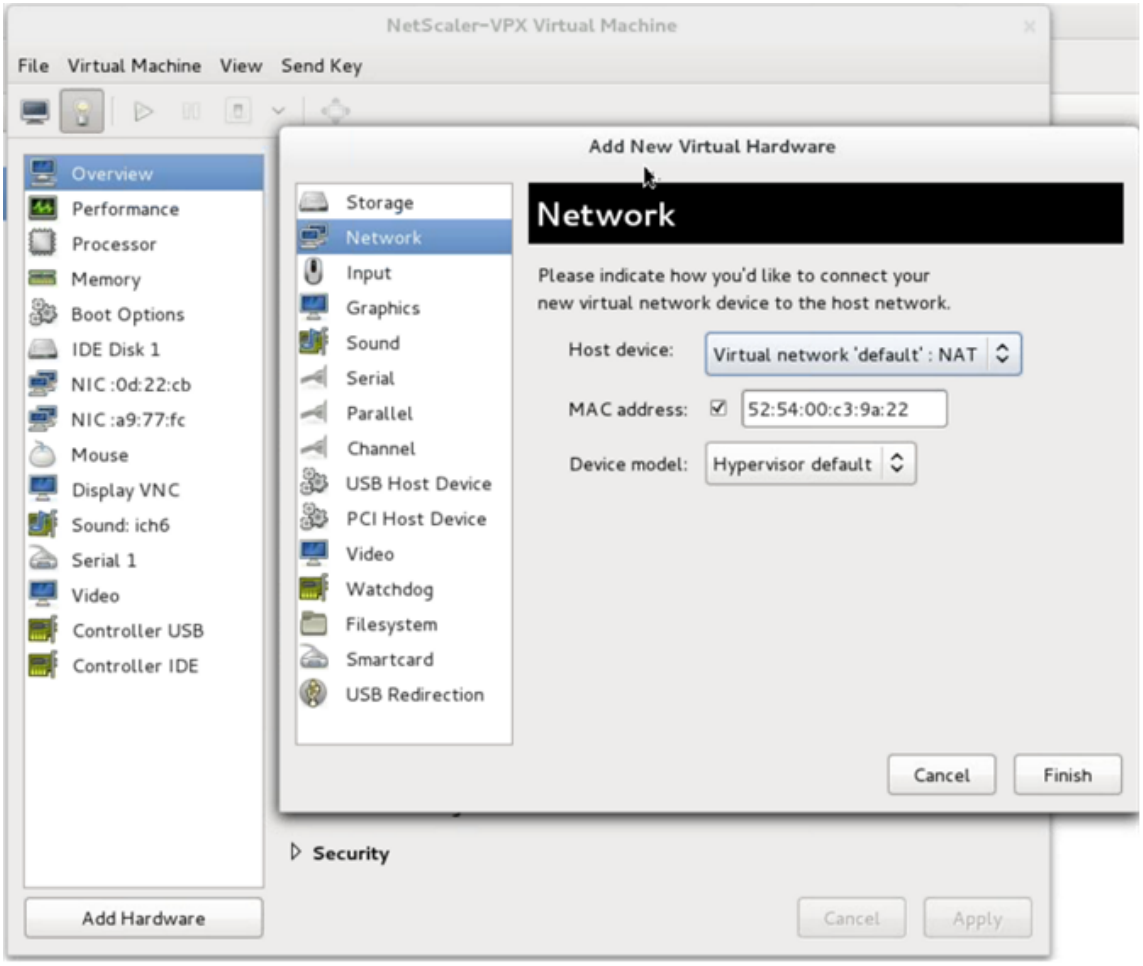
4. Wenn die automatische Bereitstellung fehlschlägt, wird die Instanz die Standard-IP-Adresse (192.168.100.1) angezeigt. In diesem Fall müssen Sie die Erstkonfiguration manuell abschließen. Weitere Informationen finden Sie unter Konfigurieren des ADC zum ersten Mal.

Fügen Sie der Citrix ADC VPX-Instanz weitere Schnittstellen hinzu, indem Sie den Virtual Machine Manager verwenden

Nachdem Sie die NetScaler VPX-Instanz auf KVM bereitgestellt haben, können Sie zusätzliche Schnittstellen hinzufügen.

Gehen Sie folgendermaßen vor, um weitere Schnittstellen hinzuzufügen.

1. Fahren Sie die NetScaler VPX-Instanz herunter, die auf der KVM ausgeführt wird.
2. Klicken Sie mit der rechten Maustaste auf die VPX-Instanz und wählen Sie **Öffnen** aus dem Popup-Menü.
3. Klicken Sie auf das  in der Kopfzeile, um die Details der virtuellen Hardware anzuzeigen.
4. Klicken Sie auf **Hardware hinzufügen**. Wählen **Sie im Fenster Neue virtuelle Hardware hinzufügen**im Navigationsmenü die Option **Netzwerk**aus.



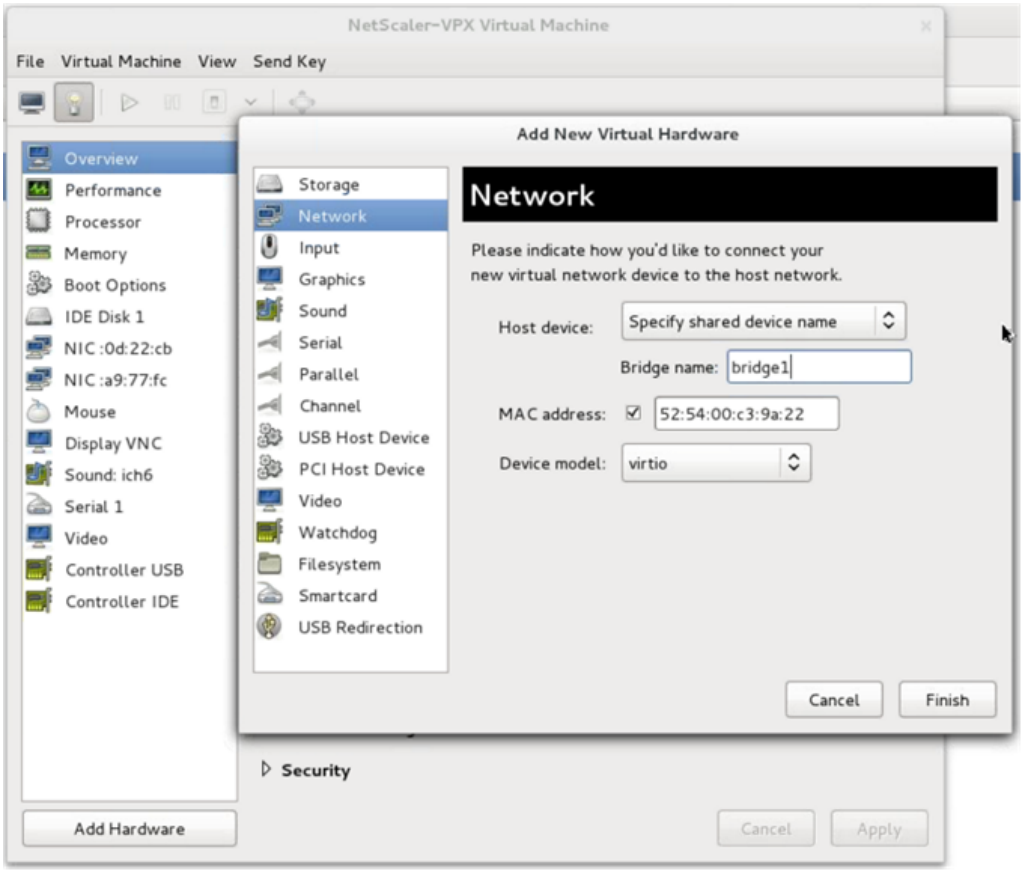
5. Wählen Sie im Feld **Hostgerät** den physischen Schnittstellentyp aus. Der Hostgerätetyp kann entweder Bridge oder MacVTap sein. Im Falle von MacVTap sind VEPA, Bridge, Private und Pass-Through vier Modi möglich.

    a) Für Brücke

        i. Hostgeräte— Wählen Sie die Option Shared Device Name angeben.

        ii. Geben Sie den Bridge-Namen an, der im KVM-Host konfiguriert ist.

            Hinweis: Stellen Sie sicher, dass Sie eine Linux-Bridge im KVM-Host konfiguriert haben, die physische Schnittstelle an die Bridge gebunden haben und die Bridge in den UP-Zustand versetzen.



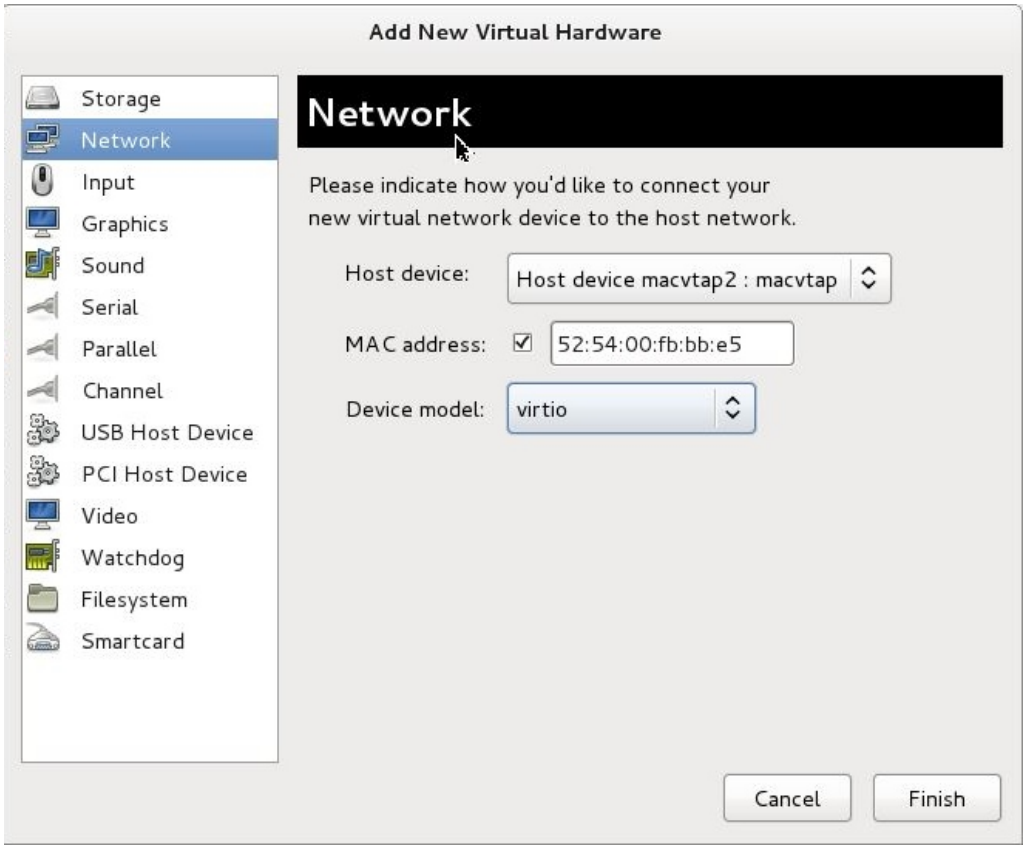
iii. Gerätemodell—`virtio`.

iv. Klicken Sie auf Fertig stellen.

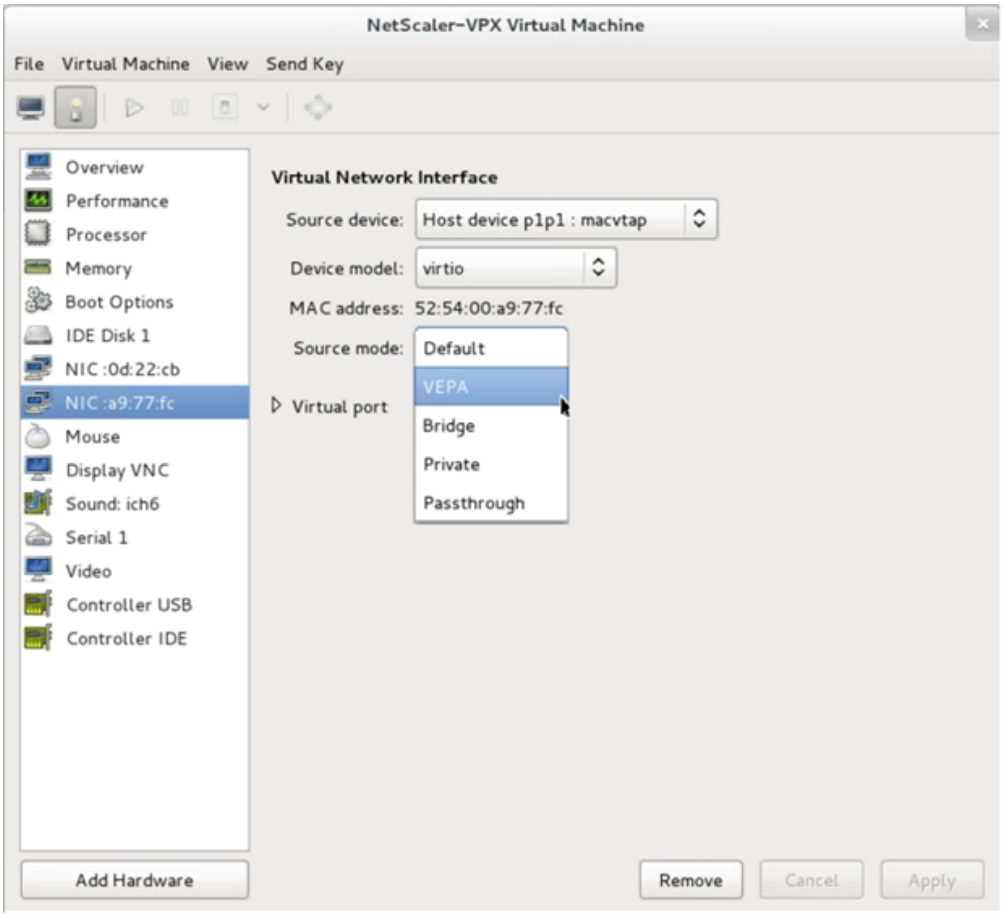
b) Für MacVtap

i. Hostgerät — Wählen Sie die physische Schnittstelle aus dem Menü aus.

ii. Gerätemodell—`virtio`.



iii. Klicken Sie auf Fertig stellen. Sie können die neu hinzugefügte Netzwerkkarte im Navigationsbereich anzeigen.



iv. Wählen Sie die neu hinzugefügte Netzwerkkarte aus, und wählen Sie den Quellmodus für diese Netzwerkkarte. Die verfügbaren Modi sind VEPA, Bridge, Private und Passthrough. Weitere Informationen zu Schnittstelle und Modi finden Sie unter Quellschnittstelle und Modi.

v. Klicken Sie auf Apply.

6. Wenn Sie die VPX-Instanz automatisch bereitstellen möchten, lesen Sie den Abschnitt “Hinzufügen eines Konfigurationslaufwerks zum Aktivieren des automatischen Provisioning” in diesem Dokument. Schalten Sie andernfalls die VPX-Instanz ein, um die Erstkonfiguration manuell abzuschließen.

> **Wichtig**
>
> Schnittstellenparameterkonfigurationen wie Geschwindigkeit, Duplex und Autonegotiation werden nicht unterstützt.

Konfigurieren einer Citrix ADC VPX-Instanz für die Verwendung von SR-IOV-Netzwerkschnittstellen

October 5, 2021

Sie können eine Citrix ADC VPX Instanz, die auf der Linux-KVM-Plattform ausgeführt wird, mithilfe der Single-Root-I/O-Virtualisierung (SR-IOV) mit den folgenden NICs konfigurieren:

- Intel 82599 10G
- Intel X710 10G
- Intel XL710 40G
- Intel X722 10G

In diesem Abschnitt werden folgende Schritte beschrieben:

- Konfigurieren einer Citrix ADC VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnittstelle
- Statische LA/LACP auf der SR-IOV-Schnittstelle konfigurieren
- Konfigurieren von VLAN auf der SR-IOV-Schnittstelle

Einschränkungen

Beachten Sie die Einschränkungen bei der Verwendung von Intel 82599, X710, XL710 und X722 NICs. Die folgenden Funktionen werden nicht unterstützt.

Einschränkungen für Intel 82599 NIC:

- L2-Modus Umschaltung
- Admin-Partitionierung (freigegebener VLAN-Modus).
- Hohe Verfügbarkeit (Aktiv-Aktiv-Modus).
- Jumbo-Rahmen.
- IPv6: Sie können nur bis zu 30 eindeutige IPv6-Adressen in einer VPX-Instanz konfigurieren, wenn Sie mindestens eine SR-IOV-Schnittstelle haben.
- Die VLAN-Konfiguration auf Hypervisor für SRIOV VF-Schnittstelle über `ip link` Befehl wird nicht unterstützt.
- Schnittstellenparameterkonfigurationen wie Geschwindigkeit, Duplex und Autonegotiationen werden nicht unterstützt.

Einschränkungen für Intel X710 10G, Intel XL710 40G und Intel X722 10G NICs:

- L2-Modus Umschaltung
- Admin-Partitionierung (freigegebener VLAN-Modus).
- In einem Cluster werden Jumbo-Frames nicht unterstützt, wenn die XL710-NIC als Datenschnittstelle verwendet wird.

- Die Schnittstellenliste wird neu sortiert, wenn Schnittstellen getrennt und wieder verbunden werden.
- Schnittstellenparameterkonfigurationen wie Geschwindigkeit, Duplex und Autonegotiationen werden nicht unterstützt.
- Schnittstellenname ist 40/X für Intel X710 10G, Intel XL710 40G und Intel X722 10G NICs
- Bis zu 16 Intel XL710/X710/X722 SRIOV- oder PCI-Passthrough-Schnittstellen können auf einer VPX-Instanz unterstützt werden.

> **Hinweis:** Für Intel X710 10G, Intel XL710 40G und Intel X722 10G NICs zur Unterstützung von IPv6 müssen Sie den Vertrauensmodus auf den Virtual Functions (VFs) aktivieren, indem Sie den folgenden Befehl auf dem KVM-Host eingeben:
>
> ```
> ## ip link set <PNIC> <VF> trust on
> ```
>
> Beispiel:
>
> ```
> ## ip link set ens785f1 vf 0 trust on
> ```

Voraussetzungen

Bevor Sie eine Citrix ADC VPX-Instanz für die Verwendung von SR-IOV-Netzwerkschnittstellen konfigurieren, führen Sie die folgenden erforderlichen Aufgaben aus. Weitere Informationen zum Abschließen der entsprechenden Aufgaben finden Sie in der Spalte NIC.

Aufgabe	Intel 82599 NIC	Intel X710, XL710 und X722 NICs
1. Fügen Sie die Netzwerkkarte dem KVM-Host hinzu.	-	-
2. Laden Sie den neuesten Intel-Treiber herunter und installieren Sie ihn.	IXGBE Treiber	I40E-Treiber
3. Listet den Treiber auf dem KVM-Host auf.	Fügen Sie den folgenden Eintrag in der Datei /etc/modprobe.d/blacklist.conf hinzu: `blacklist ixgbevf`. Verwenden Sie den IXGBE Treiber Version 4.3.15 (empfohlen).	Fügen Sie den folgenden Eintrag in der Datei /etc/modprobe.d/blacklist.conf hinzu: `blacklist i40evf`. Verwenden Sie den i40e-Treiber Version 2.0.26 (empfohlen).

Aufgabe	Intel 82599 NIC	Intel X710, XL710 und X722 NICs
4. Aktivieren Sie SR-IOV Virtual Functions (VFs) auf dem KVM-Host. In beiden Befehlen in den nächsten beiden Spalten: `number_of_VFs` = die Anzahl der virtuellen VFs, die Sie erstellen möchten. `device_name` = der Name der Schnittstelle.	Wenn Sie eine frühere Version von Kernel 3.8 verwenden, fügen Sie der Datei /etc/modprobe.d/ixgbe den folgenden Eintrag hinzu und starten Sie den KVM-Host neu: `options ixgbe max_vfs =<number_of_VFs>` Wenn Sie Kernel 3.8 Version oder höher verwenden, erstellen Sie VFs mit dem folgenden Befehl: `echo < number_of_VFs> > /sys/class/net/<device_name >/device/sriov_numvfs`. Siehe Beispiel in Abbildung 1.	Wenn Sie eine frühere Version von Kernel 3.8 verwenden, fügen Sie der Datei /etc/modprobe.d/i40e.conf den folgenden Eintrag hinzu, und starten Sie den KVM-Host neu: `options i40e max_vfs=< number_of_VFs>`. Wenn Sie Kernel 3.8 Version oder höher verwenden, erstellen Sie VFs mit dem folgenden Befehl: `echo<number_of_VFs> > /sys/class/net/< device_name>/device/ sriov_numvfs`. Siehe Beispiel in Abbildung 2.
5. Machen Sie die VFs persistent, indem Sie die Befehle, die Sie zum Erstellen von VFs verwendet haben, zur Datei rc.local hinzufügen.	Siehe Beispiel in Abbildung 3.	Siehe Beispiel in Abbildung 3.

> **Wichtig**
>
> Stellen Sie beim Erstellen der SR-IOV-VFs sicher, dass Sie den VFs keine MAC-Adressen zuweisen.

Abbildung 1: Aktivieren Sie SR-IOV-VFs auf dem KVM-Host für Intel 82599 10G-NIC.

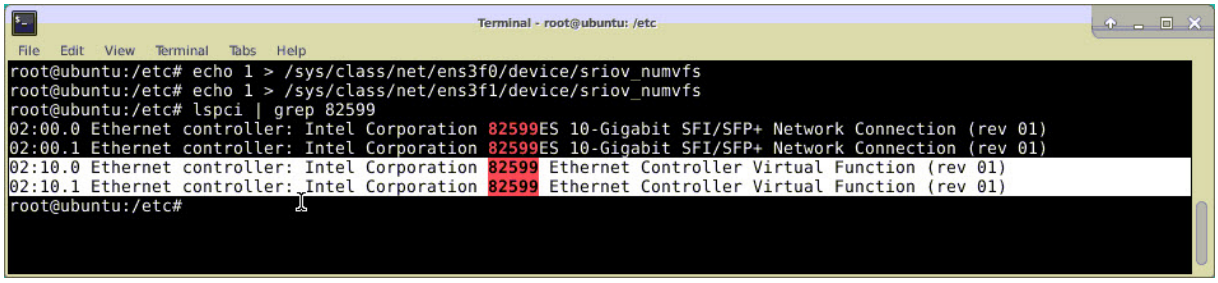


Abbildung 2: Aktivieren Sie SR-IOV-VFs auf dem KVM-Host für Intel X710 10G und XL710 40G NICs.

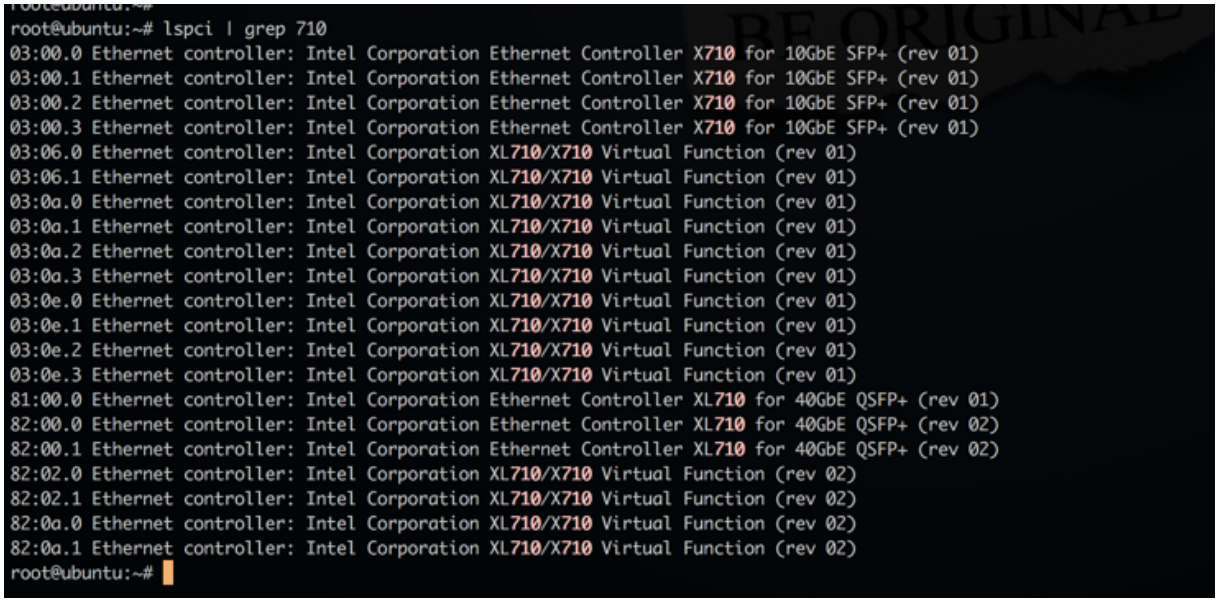


Abbildung 3: Aktivieren Sie SR-IOV-VFs auf dem KVM-Host für Intel X722 10G-NIC.

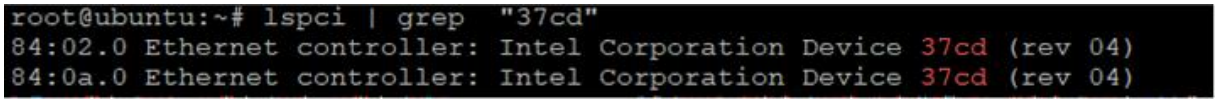
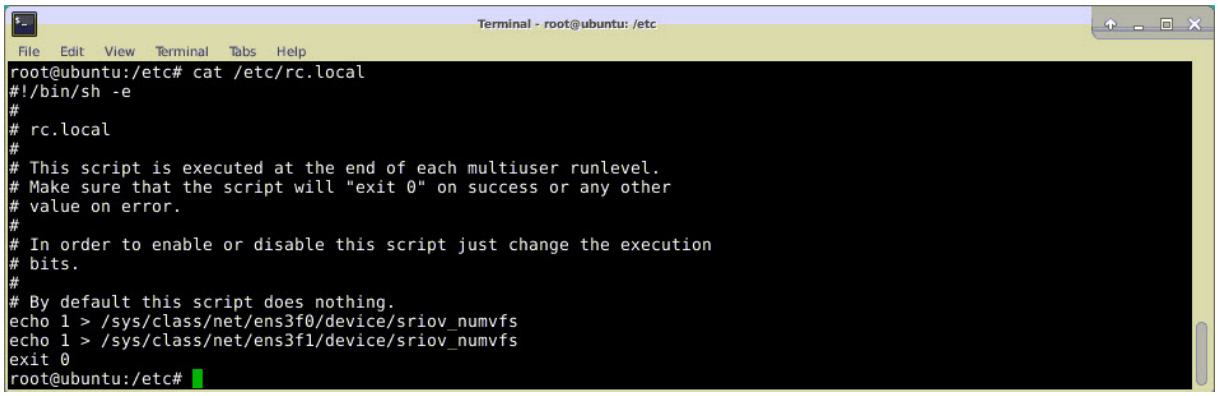


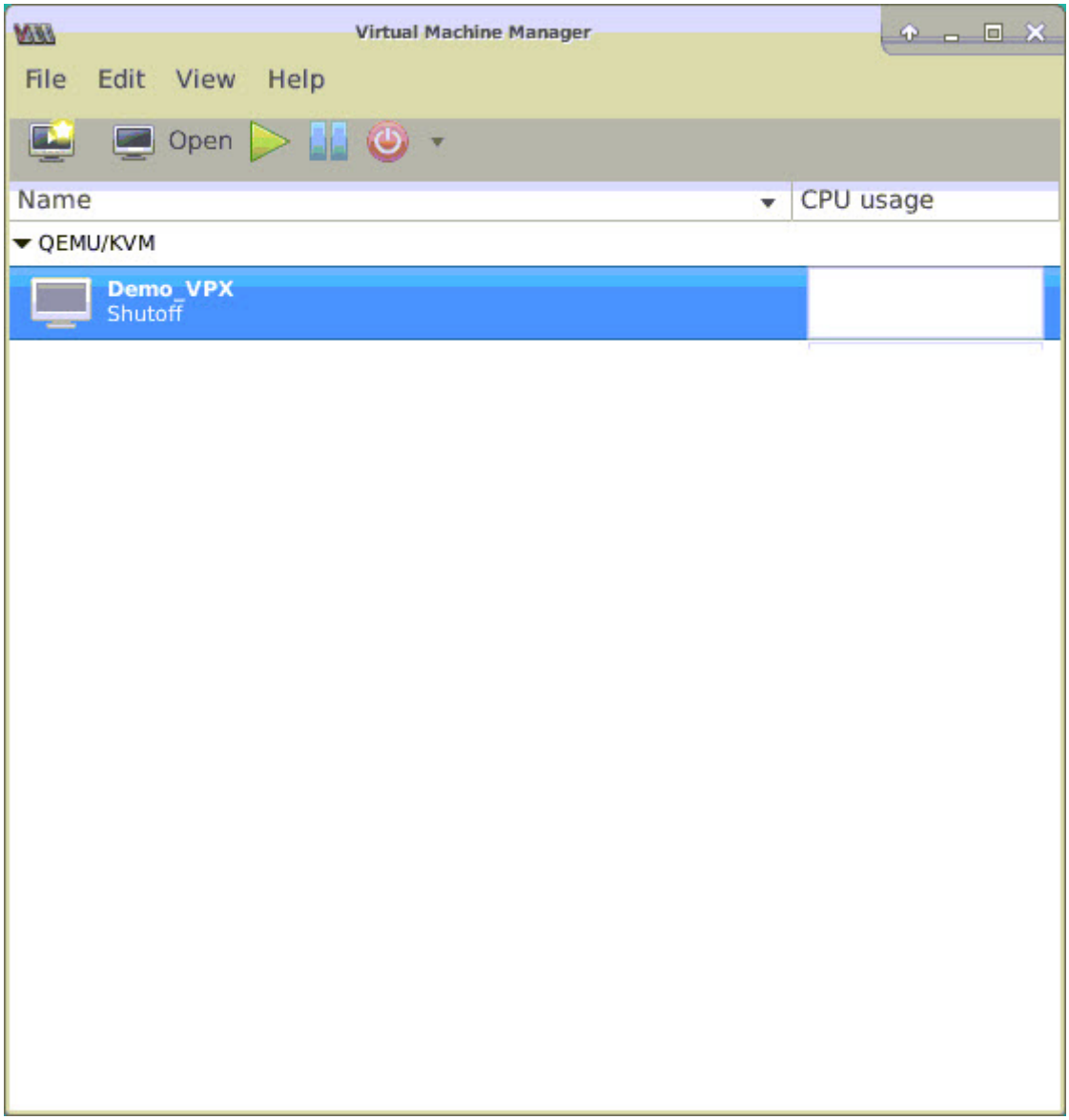
Abbildung 4: Machen Sie die VFs persistent.



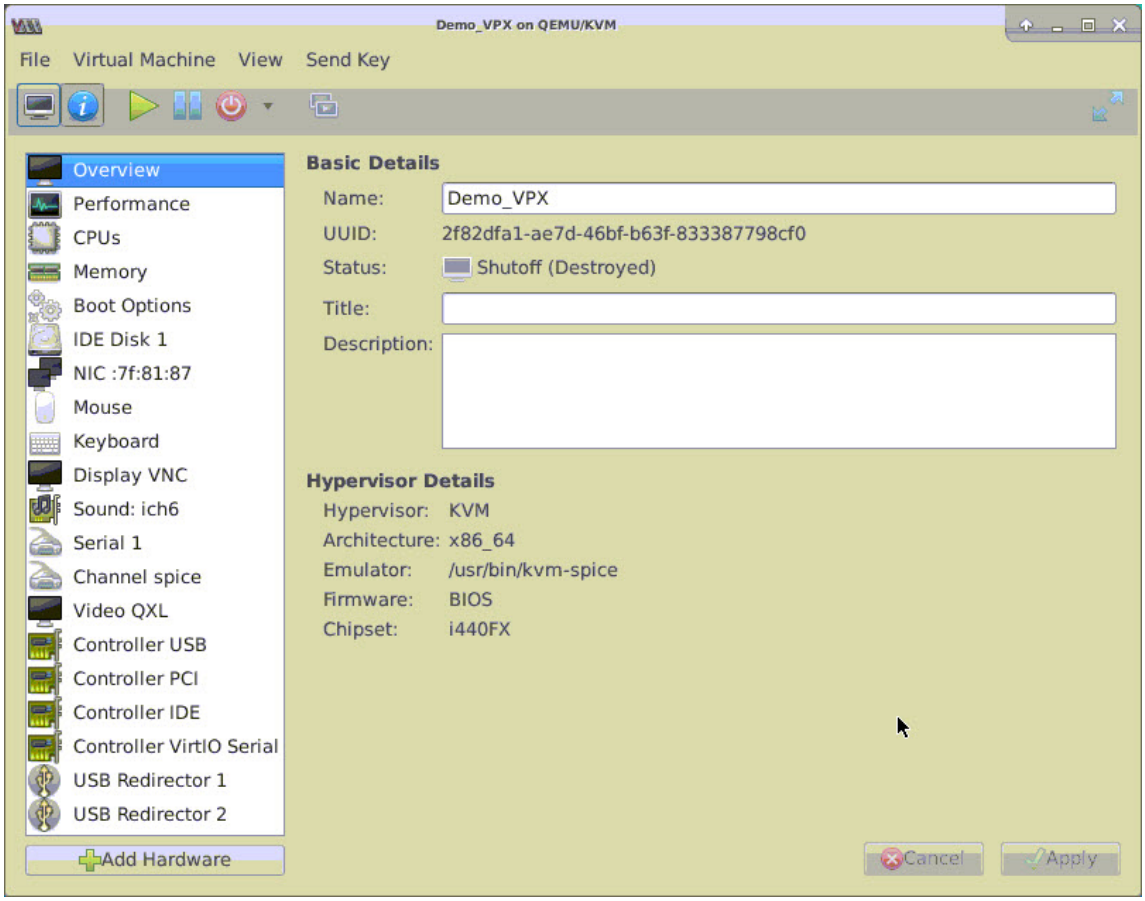
Konfigurieren einer Citrix ADC VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnittstelle

Führen Sie die folgenden Schritte aus, um die Citrix ADC VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnittstelle mit Virtual Machine Manager zu konfigurieren:

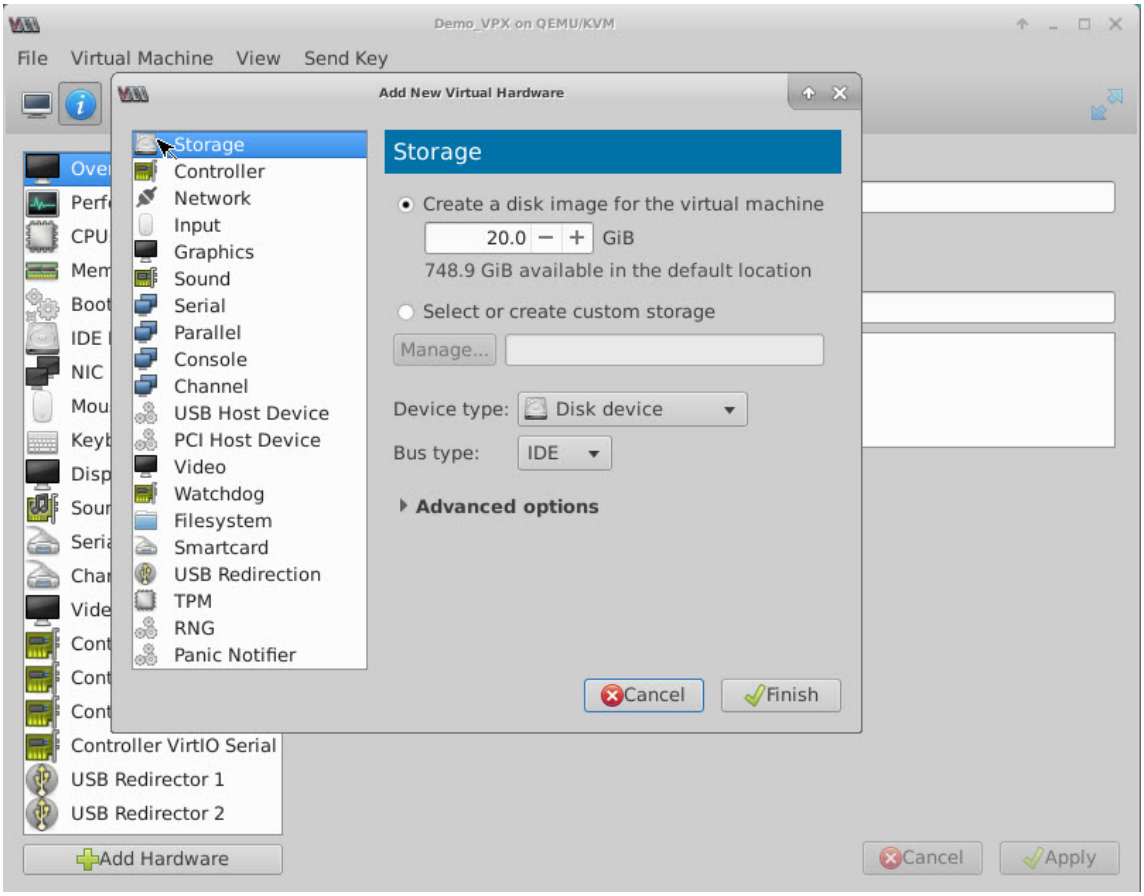
1. Schalten Sie die Citrix ADC VPX-Instanz aus.
2. Wählen Sie die Citrix ADC VPX-Instanz und dann Öffnen aus.



3. <virtual machine on KVM>Wählen Sie im Fenster das **I-Symbol** aus.



4. Wählen Sie **Hardware hinzufügen**aus.



5. Führen **Sie im Dialogfeld Neue virtuelle Hardware hinzufügen** die folgenden Schritte aus:

   a) Wählen Sie PCI-Hostgerätaus.
   b) Wählen Sie im Abschnitt Host-Device die von Ihnen erstellte VF aus, und klicken Sie auf Fertig stellen.

Abbildung 4: VF für Intel 82599 10G NIC

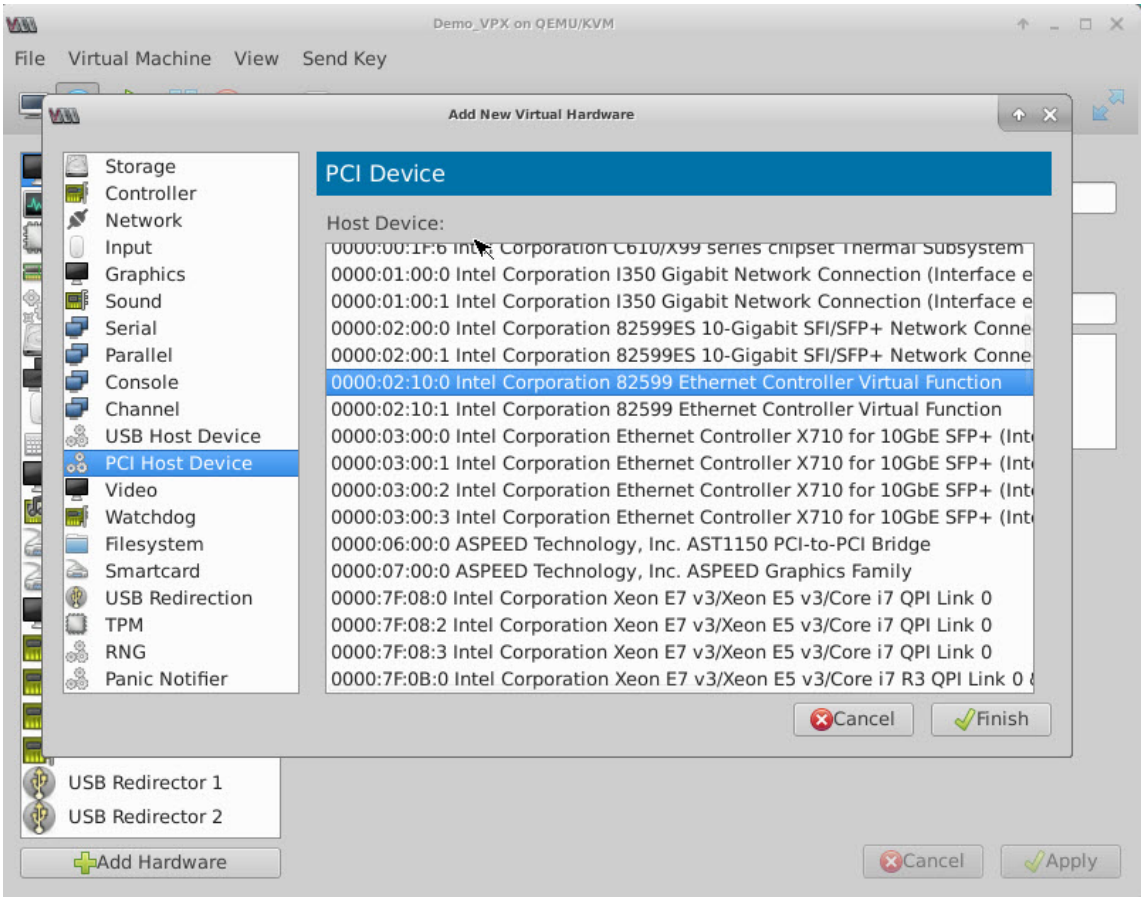


Abbildung 5: VF für Intel XL710 40G NIC

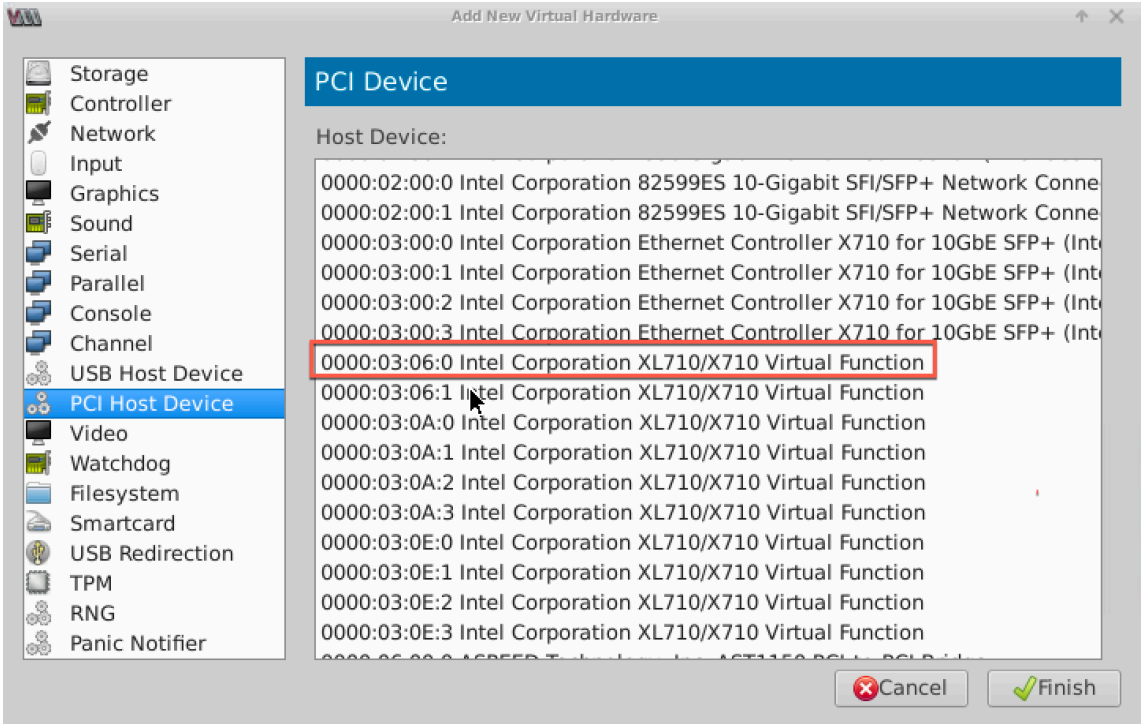
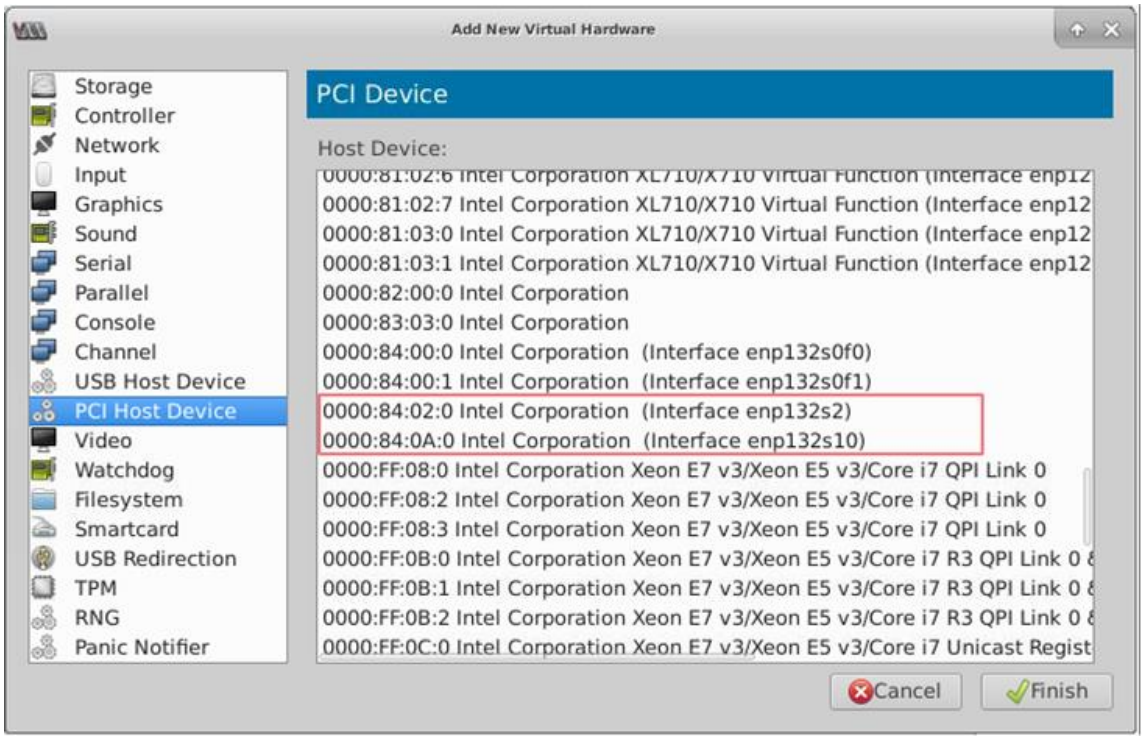


Abbildung 6: VF für Intel X722 10G NIC



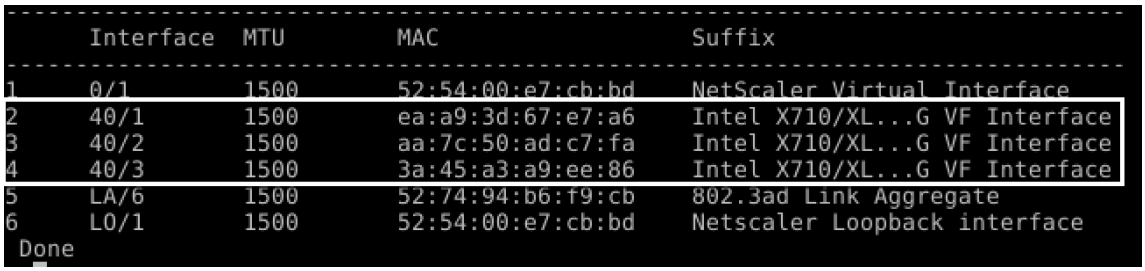
6. Wiederholen Sie Schritt 4 und 5, um die von Ihnen erstellten VFs hinzuzufügen.
7. Schalten Sie die Citrix ADC VPX-Instanz ein.
8. Nachdem die Citrix ADC VPX-Instanz eingeschaltet wurde, verwenden Sie den folgenden Befehl, um die Konfiguration zu überprüfen:

```
show interface summary
<!--NeedCopy-->
```

Die Ausgabe zeigt alle von Ihnen konfigurierten Schnittstellen an.

Abbildung 6: Zusammenfassung der Ausgabe für Intel 82599 NIC.

Abbildung 7. Zusammenfassung der Ausgabe für Intel X710 und XL710 NICs.



Statische LA/LACP auf der SR-IOV-Schnittstelle konfigurieren

> **Wichtig**
>
> Achten Sie beim Erstellen der SR-IOV-VFs darauf, dass Sie den VFs keine MAC-Adressen zuweisen.

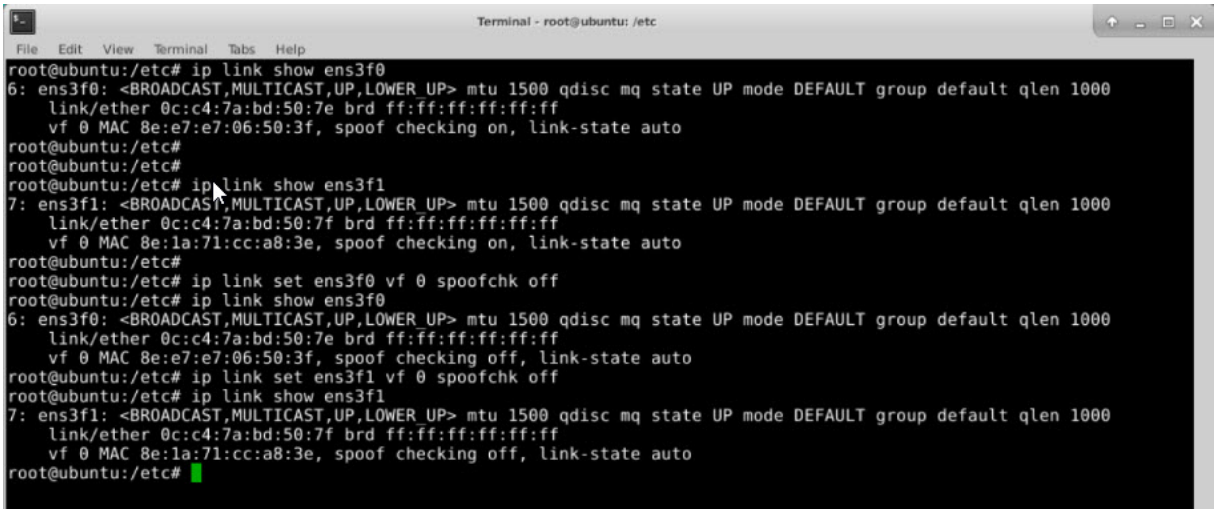
Um die SR-IOV-VFs im Linkaggregationsmodus zu verwenden, deaktivieren Sie die Spoofprüfung für VFs, die Sie erstellt haben. Verwenden Sie auf dem KVM-Host den folgenden Befehl, um die Spoofprüfung zu deaktivieren:

```
*ip link set \<interface\\_name\> vf \<VF\\_id\> spoofchk off*
```

Wobei:

- Schnittstellenname — ist der Schnittstellenname.
- vf_id — ist die virtuelle Funktions-ID.

Beispiel:



Nachdem Sie die Spoofprüfung für alle VFs deaktiviert haben, die Sie erstellt haben. Starten Sie die Citrix ADC VPX-Instanz neu, und konfigurieren Sie die Linkaggregation. Ausführliche Anweisungen finden Sie unter Konfigurieren der Link-Aggregation.

Konfigurieren von VLAN auf der SR-IOV-Schnittstelle

Sie können VLAN auf SR-IOV-VFs konfigurieren. Ausführliche Anweisungen finden Sie unter Konfigurieren eines VLANs.

> **Wichtig**
>
> Stellen Sie sicher, dass der KVM-Host keine VLAN-Einstellungen für die VF-Schnittstelle enthält.

Konfigurieren einer Citrix ADC VPX-Instanz für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen

October 5, 2021

Nachdem Sie eine Citrix ADC VPX-Instanz auf der Linux-KVM-Plattform installiert und konfiguriert haben, können Sie den Virtual Machine Manager verwenden, um die virtuelle Appliance für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen zu konfigurieren.

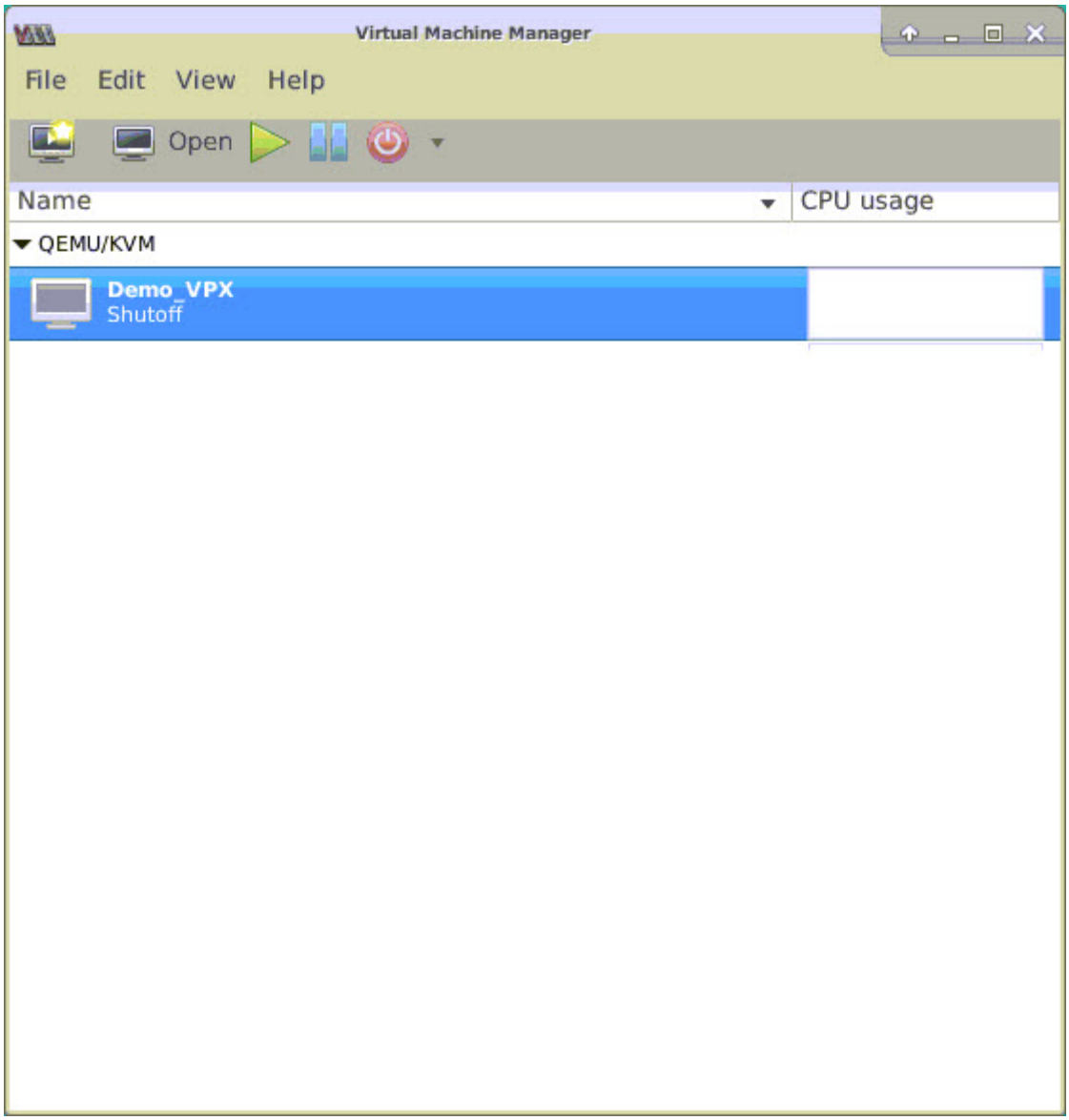
Voraussetzungen

- Die Firmware-Version der Intel XL710-NIC (NIC) auf dem KVM-Host ist 5.04.
- Der KVM-Host unterstützt Eingabe-Output-Speicherverwaltungseinheit (IOMMU) und Intel VT-d und ist im BIOS des KVM-Hosts aktiviert. Fügen Sie auf dem KVM-Host den folgenden Eintrag zur Datei **/boot/grub2/grub.cfg** hinzu, um IOMMU zu aktivieren:**intel_iommu=1**

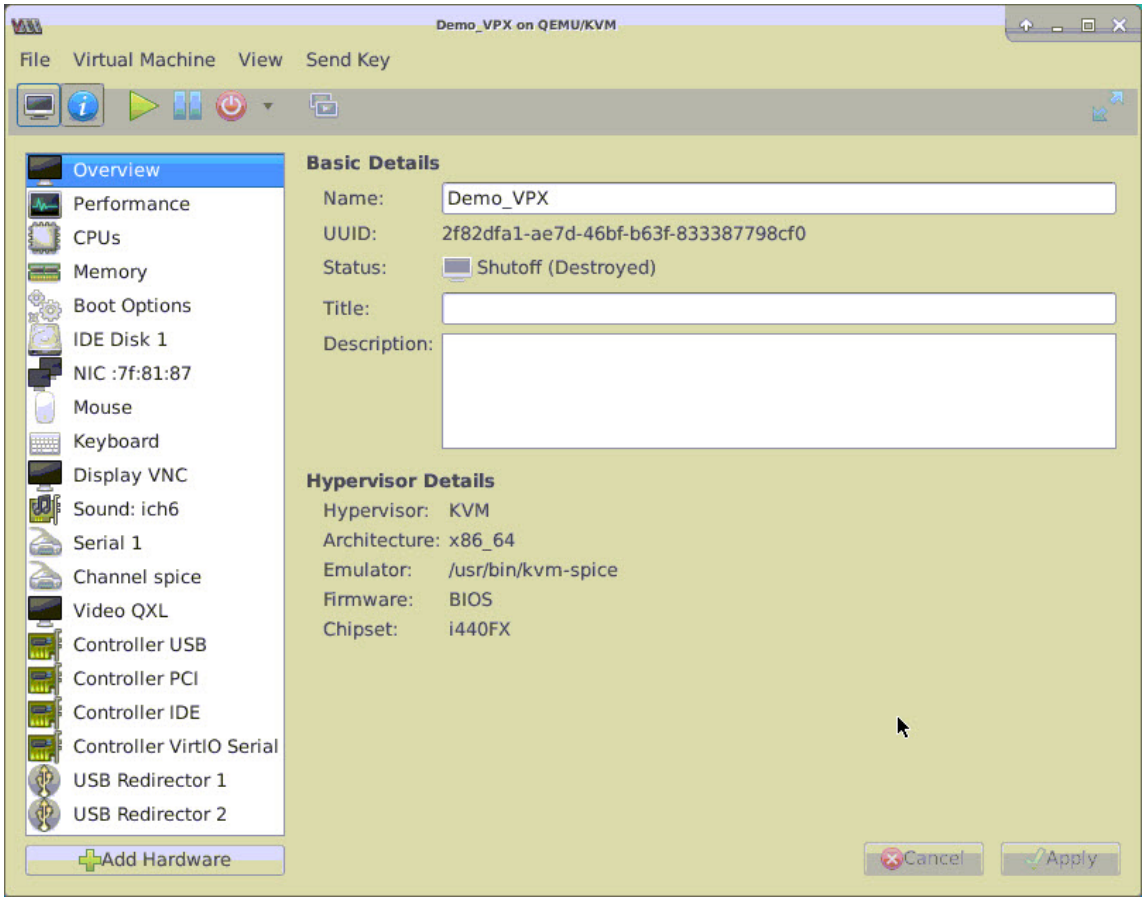
- Führen Sie den folgenden Befehl aus und starten Sie den KVM-Host neu: **Grub2-mkConfig —o /boot/grub2/grub.cfg**

So konfigurieren Sie Citrix ADC VPX-Instanzen für die Verwendung von PCI-Passthrough-Netzwerkschnittstellen mithilfe des Virtual Machine Manager:

1. Schalten Sie die Citrix ADC VPX-Instanz aus.
2. Wählen Sie die Citrix ADC VPX-Instanz aus, und klicken Sie auf **Öffnen**.



3. Klicken Sie im Fenster **virtual_machine im KVM** -Fenster auf das **I-Symbol** .

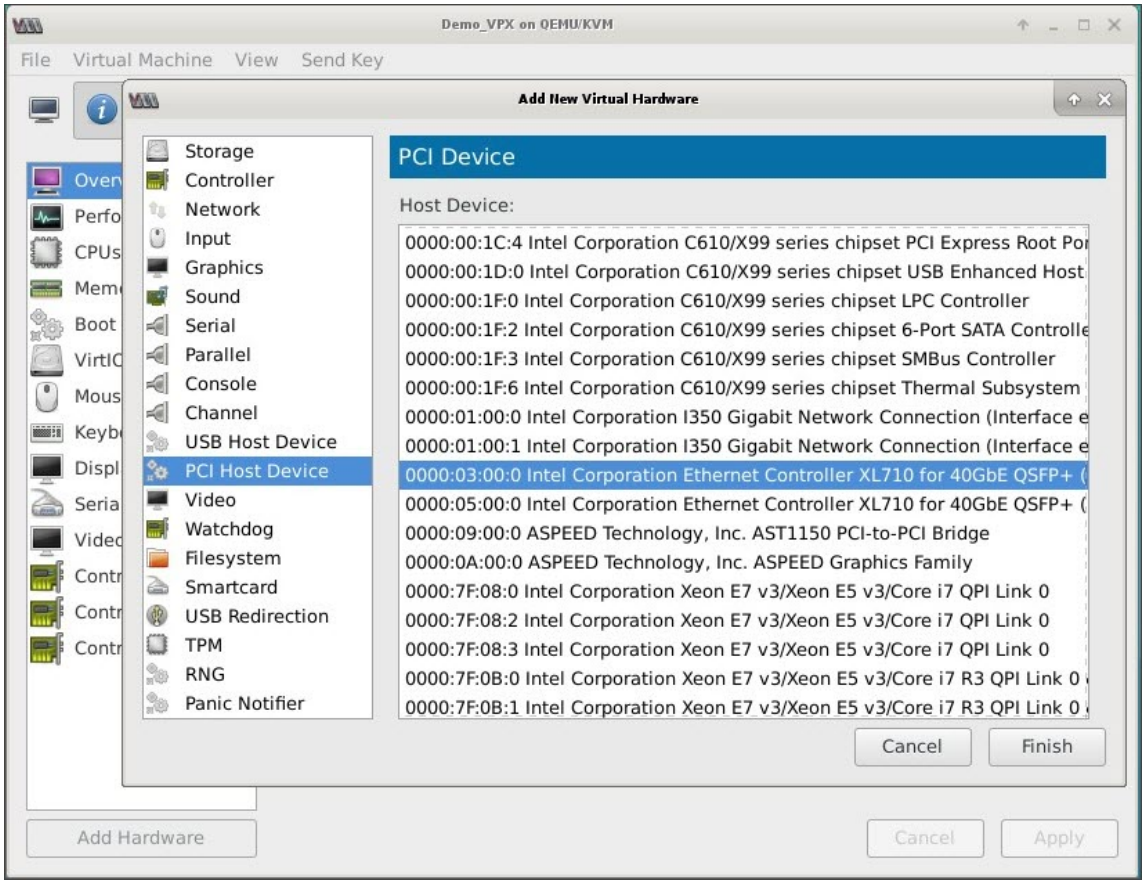


4. Klicken Sie auf **Hardware hinzufügen**.
5. Führen **Sie im Dialogfeld Neue virtuelle Hardware hinzufügen** die folgenden Schritte aus:

   a. Wählen Sie **PCI-Hostgerät**aus.

   b. Wählen Sie im Abschnitt **Hostgerät** die physische Intel XL710 Funktion aus.

   c. Klicken Sie auf **Fertig stellen**.

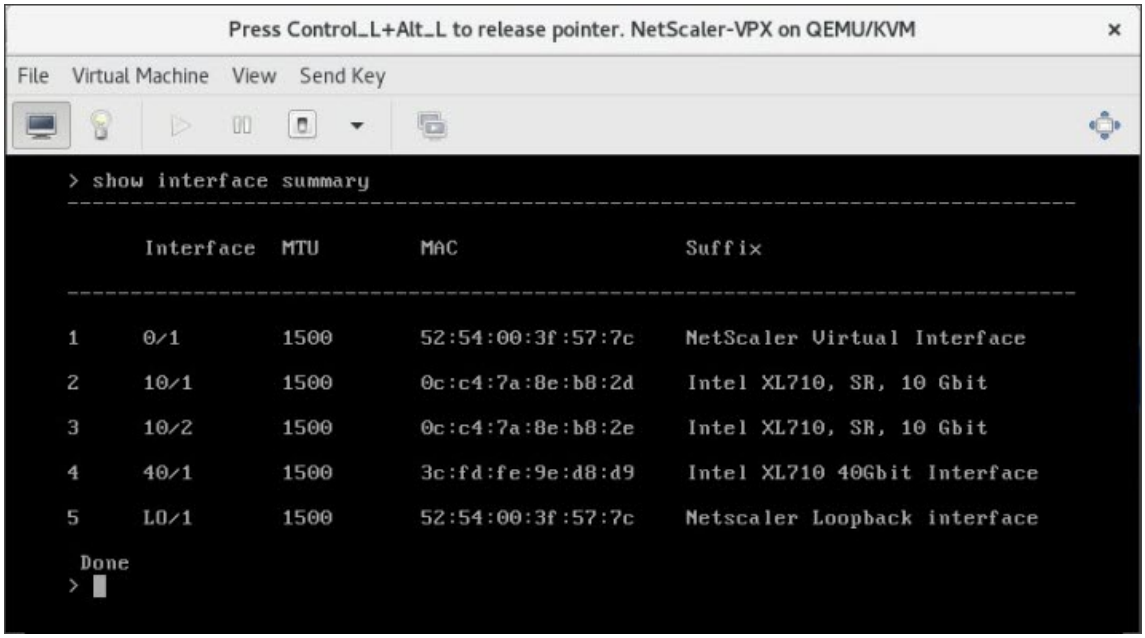


6. Wiederholen Sie die Schritte **4** und **5**, um zusätzliche physische Funktionen des Intel XL710 hinzuzufügen.
7. Schalten Sie die Citrix ADC VPX-Instanz ein.
8. Sobald die Citrix ADC VPX-Instanz eingeschaltet ist, können Sie die Konfiguration mithilfe des folgenden Befehls überprüfen:

```
COMMAND

> show interface summary
```

Die Ausgabe muss alle von Ihnen konfigurierten Schnittstellen anzeigen:



Stellen Sie die Citrix ADC VPX-Instanz mithilfe des virsh Programms bereit

October 5, 2021

Das `virsh` Programm ist ein Befehlszeilentool zur Verwaltung von VM-Gästen. Seine Funktionalität ähnelt der von Virtual Machine Manager. Es ermöglicht Ihnen, den Status eines VM-Gastes (Start, Stopp, Pause usw.) zu ändern, neue Gäste und Geräte einzurichten und vorhandene Konfigurationen zu bearbeiten. Das `virsh` Programm ist auch nützlich für das Skripten von VM-Gastverwaltungsvorgängen.

Gehen Sie folgendermaßen vor, um Citrix ADC VPX mithilfe des `virsh` Programms bereitzustellen:

1. Verwenden Sie den Befehl tar, um das Citrix ADC VPX-Paket aufzuheben. Das Paket NSVPX-KVM-*_nc.tgz enthält die folgenden Komponenten:
   - Die Domänen-XML-Datei mit VPX-Attributen [NSVPX-KVM-*_nc.xml]
   - Prüfen Sie die Summe des NS-VM-Datenträgerimages [CheckSum.txt]
   - NS-VM-Datenträgerabbildimage [NSVPX-KVM-*_nc.raw]

   Beispiel:

```
tar -xvzf NSVPX-KVM-10.1-117_nc.tgz
NSVPX-KVM-10.1-117_nc.xml
NSVPX-KVM-10.1-117_nc.raw
```



```
4 checksum.txt
5 <!--NeedCopy-->
```

2. Kopieren Sie die XML-Datei NSVPX-KVM-*_nc.xml in eine Datei mit dem Namen <DomainName>-NSVPX-KVM-*_nc.xml. Der <DomainName> ist auch der Name der virtuellen Maschine. Beispiel:

```
1 cp NSVPX-KVM-10.1-117_nc.xml NetScaler-VPX-NSVPX-KVM-10.1-117_nc.
     xml
2 <!--NeedCopy-->
```

3. Bearbeiten Sie die Datei <DomainName> -nsvpx-kvm-*_nc.xml, um die folgenden Parameter anzugeben:

   - name— Geben Sie den Namen an.
   - Mac - Geben Sie die MAC-Adresse an.
     Hinweis: Der Domänenname und die MAC-Adresse müssen eindeutig sein.
   - Quelldatei - Geben Sie den absoluten Quellpfad für das Datenträgerimage an. Der Dateipfad muss absolut sein. Sie können den Pfad der RAW-Imagedatei oder einer QCOW2-Imagedatei angeben.

     Wenn Sie eine RAW-Image-Datei angeben möchten, geben Sie den Pfad der Datenträgerimagequelle an, wie im folgenden Beispiel gezeigt:

     Beispiel:

```
1   <name>NetScaler-VPX</name>
2   <mac address='52:54:00:29:74:b3'/>
3   <source file='/root/NSVPX-KVM-10.1-117_nc.raw'/>
4   <!--NeedCopy-->
```

     Geben Sie den absoluten QCOW2-Datenträgerimagequellpfad an, und definieren Sie den Treibertyp als **qcow2**, wie im folgenden Beispiel gezeigt:

     Beispiel:

```
1   <name>NetScaler-VPX</name>
2   <mac address='52:54:00:29:74:b3'/>
3   <driver name ='qemu' type='qcow2'/>
4   <source file='/root/NSVPX-KVM-10.1-117_nc.qcow'/>*
5   <!--NeedCopy-->
```


4. Bearbeiten Sie die Datei <DomainName> -nsvpx-kvm-*_nc.xml, um die Netzwerkdetails zu konfigurieren:

   - source dev— Geben Sie die Schnittstelle an.
   - mode — Geben Sie den Modus an. Die Standardschnittstelle ist **Macvtap Bridge**.

   Beispiel: Modus: MacVTap Bridge Setzen Sie Zielschnittstelle als `ethx` und Modus als Bridge-Modelltyp als `virtio`

```
  <interface type='direct'>
      <mac address='52:54:00:29:74:b3'/>
      <source dev='eth0' mode='bridge'/>
      <target dev='macvtap0'/>
      <model type='virtio'/>
      <alias name='net0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
         function='0x0'/>
    </interface>
<!--NeedCopy-->
```

   Hier ist eth0 die physische Schnittstelle, die an die VM angeschlossen ist.

5. Definieren Sie die VM-Attribute in der <DomainName>Datei -nsVPX-KVM-*_nc.xml mit dem folgenden Befehl: `virsh` define <DomainName>-NsVPX-KVM-*_nc.xml Beispiel:

```
virsh define NS-VPX-NSVPX-KVM-10.1-117_nc.xml
<!--NeedCopy-->
```

6. Starten Sie die VM, indem Sie den folgenden Befehl eingeben: `virsh` start [<DomainName>|<DomainUUID>] Beispiel:

```
virsh start NetScaler-VPX
<!--NeedCopy-->
```

7. Verbinden Sie die Gast-VM über die `virsh` Konsolenkonsole [<DomainName><DomainUUID>| |<DomainID>] Beispiel:

```
virsh console NetScaler-VPX
<!--NeedCopy-->
```


Fügen Sie Citrix ADC VPX-Instanz mithilfe `virsh` des Programms weitere Schnittstellen hinzu

Nachdem Sie Citrix ADC VPX auf KVM bereitgestellt haben, können Sie zusätzliche Schnittstellen hinzufügen.

Gehen Sie folgendermaßen vor, um weitere Schnittstellen hinzuzufügen:

1. Fahren Sie die Citrix ADC VPX-Instanz herunter, die auf der KVM ausgeführt wird.
2. Bearbeiten Sie die Datei <DomainName>-nsVPX-KVM-*_nc.xml mit dem Befehl: `virsh` edit [<DomainName>|<DomainUUID>]
3. <DomainName>Fügen Sie in der Datei -nsvpx-kvm-*_nc.xml die folgenden Parameter an:

   a) **Für MacVtap**

   - Schnittstellentyp — Geben Sie den Schnittstellentyp als ‘direct’ an.
   - MAC-Adresse— Geben Sie die MAC-Adresse an und stellen Sie sicher, dass die MAC-Adresse über die Schnittstellen eindeutig ist.
   - source dev— Geben Sie den Schnittstellennamen an.
   - mode - Geben Sie den Modus an. Die unterstützten Modi sind Bridge, VEPA, Private und Pass-Through
   - Modelltyp— Geben Sie den Modelltyp an als `virtio`

   Beispiel:

   Modus: MacVTap Pass-Through

   Setzen Sie die Zielschnittstelle als
   `ethx`, Modus als
   Bridge und Modelltyp als
   `virtio`

```
<interface type='direct'>
      <mac address='52:54:00:29:74:b3'/>
      <source dev='eth1' mode='passthrough'/>
      <model type='virtio'/>
 </interface>
<!--NeedCopy-->
```

   Hier eth1 ist die physische Schnittstelle, die an die VM angeschlossen ist.

   b) **Für Bridge-Modus**

   Hinweis: Stellen Sie sicher, dass Sie eine Linux-Bridge im KVM-Host konfiguriert haben, die physische Schnittstelle an die Bridge gebunden haben und die Bridge in den UP-Zustand versetzen.

- Schnittstellentyp — Geben Sie den Schnittstellentyp als ‘Bridge’ an.
- MAC-Adresse— Geben Sie die MAC-Adresse an und stellen Sie sicher, dass die MAC-Adresse über die Schnittstellen eindeutig ist.
- Quellbrücke — Geben Sie den Bridge-Namen an.
- Modelltyp— Geben Sie den Modelltyp an als `virtio`

Beispiel: Bridge-Modus

```
<interface type='bridge'>
      <mac address='52:54:00:2d:43:a4'/>
      <source bridge='br0'/>
      <model type='virtio'/>
 </interface>
<!--NeedCopy-->
```

Verwalten der Citrix ADC VPX Gast-VMs

October 5, 2021

Sie können den Virtual Machine Manager und das `virsh` Programm verwenden, um Verwaltungsaufgaben wie das Starten oder Stoppen eines VM-Gastes, das Einrichten neuer Gäste und Geräte, das Bearbeiten vorhandener Konfigurationen und die Verbindung mit der grafischen Konsole über Virtual Network Computing (VNC) auszuführen.

Verwalten der VPX-Gast-VMs mithilfe von Virtual Machine Manager

- Liste der VM-Gäste

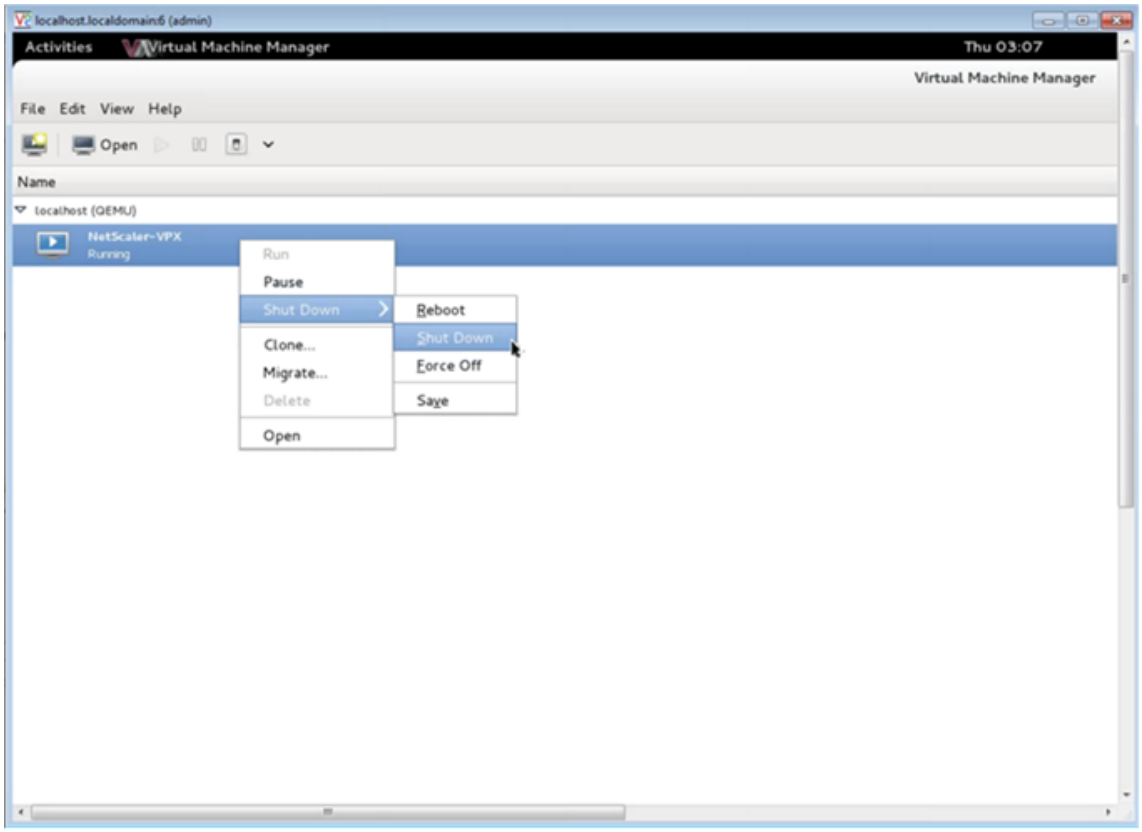
  Im Hauptfenster des Virtual Machine Manager wird eine Liste aller VM-Gäste für jeden VM-Hostserver angezeigt, mit dem er verbunden ist. Jeder VM-Gasteintrag enthält den Namen der virtuellen Maschine zusammen mit seinem Status (Ausführen, Pausiert oder Shutoff), der wie im Symbol angezeigt wird.

- Öffnen einer grafischen Konsole

  Wenn Sie eine grafische Konsole für einen VM-Gast öffnen, können Sie mit dem Computer wie mit einem physischen Host über eine VNC-Verbindung interagieren. Um die grafische Konsole im Virtual Machine Manager zu öffnen, klicken Sie mit der rechten Maustaste auf den Eintrag VM-Gast, und wählen Sie im Popupmenü die Option Öffnen aus.

- Starten und Herunterfahren eines Gastes

Sie können einen VM-Gast aus dem Virtual Machine Manager starten oder stoppen. Um den Status der VM zu ändern, klicken Sie mit der rechten Maustaste auf den Eintrag VM-Gast, und wählen Sie Ausführen oder eine der Optionen zum Herunterfahren aus dem Popupmenü aus.



- Neustart eines Gastes

  Sie können einen VM-Gast über den Virtual Machine Manager neu starten. Um die VM neu zu starten, klicken Sie mit der rechten Maustaste auf den Eintrag VM-Gast, und wählen Sie dann im Popupmenü die Option Herunterfahren > Neustart aus.

- Löschen eines Gastes

  Beim Löschen eines VM-Gastes wird standardmäßig die XML-Konfiguration entfernt. Sie können auch die Speicherdateien eines Gastes löschen. Dadurch wird der Gast komplett gelöscht.

  1. Klicken Sie im Virtual Machine Manager mit der rechten Maustaste auf den Eintrag VM-Gast.
  2. Wählen Sie Löschen aus dem Einblendmenü. Ein Bestätigungsfenster wird geöffnet.
     Hinweis: Die Option Löschen ist nur aktiviert, wenn der VM-Gast heruntergefahren wird.
  3. Klicken Sie auf Löschen.
  4. Um den Gast vollständig zu löschen, löschen Sie die zugehörige RAW-Datei, indem Sie das Kontrollkästchen Zugehörige Speicherdateien löschen aktivieren.

Verwalten Sie die Citrix ADC VPX-Gast-VMs mit dem `virsh` Programm

- Listen Sie die VM-Gäste und ihre aktuellen Status auf.

  So zeigen `virsh` Sie Informationen über die Gäste an

  ```
  virsh list --all
  ```

  Die Befehlsausgabe zeigt alle Domänen mit ihrem Status an. Beispielausgabe:

  ```
  Id Name                 State
  ----------------------------------
    0 Domain-0            running
    1 Domain-1            paused
    2 Domain-2            inactive
    3 Domain-3            crashed
  <!--NeedCopy-->
  ```

- Öffne eine `virsh` Konsole.

  Verbinden der Gast-VM über die Konsole

  ```
  virsh console [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Beispiel:

  ```
  virsh console NetScaler-VPX
  ```

- Starten und schließen Sie einen Gast.

  Gäste können mit dem Domainnamen oder Domain-UUID gestartet werden.

  ```
  virsh start [<DomainName> | <DomainUUID>]
  ```

  Beispiel:

  ```
  virsh start NetScaler-VPX
  ```

  So schließen Sie einen Gast:

  ```
  virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Beispiel:

  ```
  virsh shutdown NetScaler-VPX
  ```

- Neustart eines Gastes

  ```
  virsh reboot [<DomainID> | <DomainName> | <DomainUUID>]
  ```

  Beispiel:

  ```
  virsh reboot NetScaler-VPX
  ```


Löschen eines Gastes

Um eine Gast-VM zu löschen, müssen Sie den Gast herunterfahren und den Befehl <DomainName>-NSVPX-KVM-*_NC.xml aufheben, bevor Sie den Befehl delete ausführen.

```
virsh shutdown [<DomainID> | <DomainName> | <DomainUUID>]
virsh undefine [<DomainName> | <DomainUUID>]
<!--NeedCopy-->
```

Beispiel:

```
virsh shutdown NetScaler-VPX
virsh undefine NetScaler-VPX
<!--NeedCopy-->
```

> Hinweis: Der Befehl delete entfernt keine Datenträgerimage-Datei, die manuell entfernt werden muss.

Bereitstellen der Citrix ADC VPX-Instanz mit SR-IOV unter OpenStack

October 5, 2021

Sie können Hochleistungs-Citrix ADC VPX-Instanzen mit Single-Root-E/A-Virtualisierungs-Technologie (SR-IOV) auf OpenStack bereitstellen.

Sie können eine Citrix ADC VPX-Instanz, die SR-IOV-Technologie verwendet, auf OpenStack in drei Schritten bereitstellen:

- Aktivieren Sie SR-IOV Virtual Functions (VFs) auf dem Host.
- Konfigurieren und stellen Sie die VFs OpenStack zur Verfügung.
- Stellen Sie Citrix ADC VPX auf OpenStack bereit.

Voraussetzungen

Stellen Sie sicher, dass Sie:

- Fügen Sie die Intel 82599 NIC (NIC) zum Host hinzu.
- Laden Sie den neuesten IXGBE Treiber von Intel herunter und installieren Sie ihn.
- Blockieren Sie den IXGBEVF-Treiber auf dem Host auf. Fügen Sie den folgenden Eintrag in die Datei /etc/modprobe.d/blacklist.conf hinzu: Sperrliste `ixgbevf`

> **Hinweis:**
>
> Die `ixgbe` Treiberversion muss mindestens 5.0.4 sein.

Aktivieren von SR-IOV-VFs auf dem Host

Führen Sie einen der folgenden Schritte aus, um SR-IOV-VFs zu aktivieren:

- <number_of_VFs>Wenn Sie eine Kernel-Version vor 3.8 verwenden, fügen Sie den folgenden Eintrag in die Datei /etc/modprobe.d/ixgbe hinzu und starten Sie den Host neu: options ixgbe max_vfs=
- Wenn Sie Kernel 3.8 oder höher verwenden, erstellen Sie VFs mit dem folgenden Befehl:

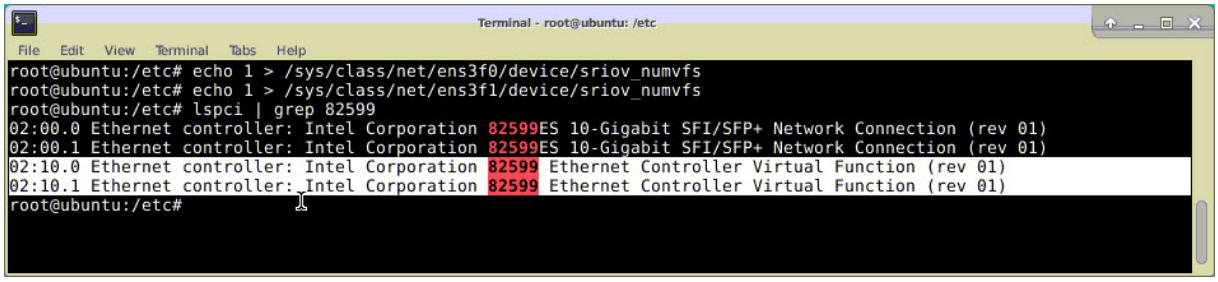
```
1     echo <number_of_VFs> > /sys/class/net/<device_name>/device/
         sriov_numvfs
2  <!--NeedCopy-->
```

Wobei:

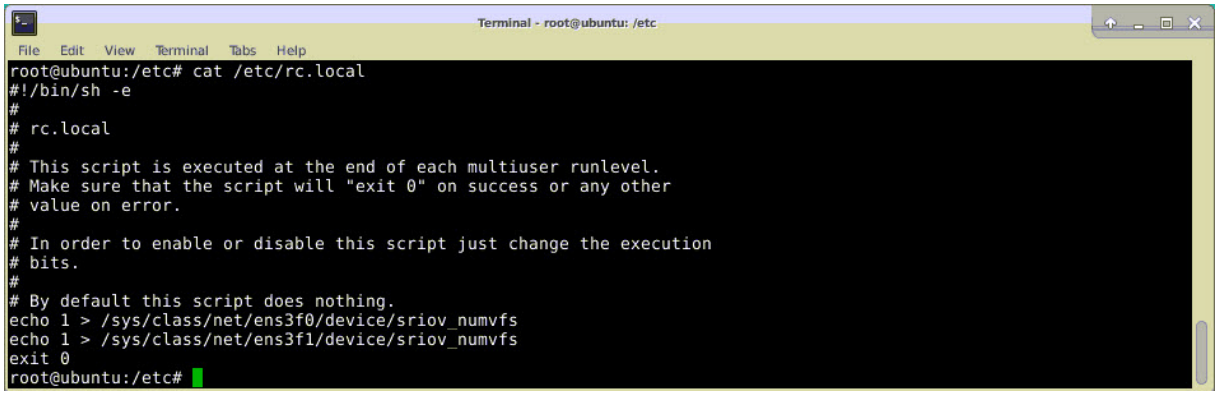
- Number_of_VFS ist die Anzahl der virtuellen Funktionen, die Sie erstellen möchten.
- device_name ist der Schnittstellenname.

> **Wichtig**
>
> Stellen Sie beim Erstellen der SR-IOV-VFs sicher, dass Sie den VFs keine MAC-Adressen zuweisen.

Hier ist ein Beispiel für vier VFs, die erstellt werden.



Machen Sie die VFs persistent, fügen Sie die Befehle, die Sie zum Erstellen von VFs verwendet haben, zur Datei **rc.local** hinzu. Hier ist ein Beispiel, das den Inhalt der rc.local-Datei zeigt.



Weitere Informationen finden Sie in diesem Intel SR-IOV-Konfigurationshandbuch.

Konfigurieren und stellen Sie die VFs für OpenStack zur Verfügung

Folgen Sie den Schritten unter dem Link, um SR-IOV auf OpenStack zu konfigurieren: https://wiki.openstack.org/wiki/SR-IOV-Passthrough-For-Networking.

Bereitstellen der Citrix ADC VPX Instanz auf OpenStack

Sie können eine Citrix ADC VPX-Instanz in einer OpenStack-Umgebung bereitstellen, indem Sie die OpenStack-CLI verwenden.

Das Provisioning einer VPX-Instanz umfasst optional die Verwendung von Daten aus dem Konfigurationslaufwerk. Das Konfigurationslaufwerk ist ein spezielles Konfigurationslaufwerk, das beim Booten an die Instanz anhängt. Dieses Konfigurationslaufwerk kann verwendet werden, um Netzwerkkonfigurationsinformationen wie Management-IP-Adresse, Netzwerkmaske und Standardgateway usw. an die Instanz zu übergeben, bevor Sie die Netzwerkeinstellungen für die Instanz konfigurieren.

Wenn OpenStack eine VPX-Instanz zur Verfügung stellt, erkennt sie zuerst, dass die Instanz in einer OpenStack-Umgebung gestartet wird, indem sie eine bestimmte BIOS-Zeichenfolge (OpenStack Foundation) liest, die OpenStack angibt. Bei Red Hat Linux-Distributionen wird die Zeichenfolge in /etc/nova/release gespeichert. Dies ist ein Standardmechanismus, der in allen OpenStack-Implementierungen verfügbar ist, die auf der KVM-Hypervisor-Plattform basieren. Das Laufwerk muss ein bestimmtes OpenStack-Label haben. Wenn das Konfigurationslaufwerk erkannt wird, versucht die Instanz, die folgenden Informationen aus dem im nova Boot-Befehl angegebenen Dateinamen zu lesen. In den folgenden Verfahren heißt die Datei userdata.txt.

- Verwaltungs-IP-Adresse
- Netzwerkmaske
- Standard-Gateway

Sobald die Parameter erfolgreich gelesen wurden, werden sie im NetScaler Stack aufgefüllt. Dies hilft bei der Remote-Verwaltung der Instanz. Wenn die Parameter nicht erfolgreich gelesen werden oder das Konfigurationslaufwerk nicht verfügbar ist, wechselt die Instanz zum Standardverhalten:

- Die Instanz versucht, die IP-Adressinformationen von DHCP abzurufen.
- Wenn DHCP fehlschlägt oder Timeout ausfällt, wird die Instanz mit der Standardnetzwerkkonfiguration (192.168.100.1/16) angezeigt.

Bereitstellen der Citrix ADC VPX-Instanz auf OpenStack über CLI

Sie können eine VPX-Instanz in einer OpenStack-Umgebung mithilfe der OpenStack-CLI bereitstellen. Im Folgenden finden Sie eine Zusammenfassung der Schritte zum Bereitstellen einer Citrix ADC VPX-Instanz auf OpenStack:

1. Extrahieren der `.qcow2` Datei aus der TGZ-Datei
2. Erstellen eines OpenStack-Images aus dem qcow2-Image
3. Provisioning einer VPX-Instanz

Führen Sie die folgenden Schritte aus, um eine VPX-Instanz in einer OpenStack-Umgebung bereitzustellen.

1. Extrahiere das. `qcow2` Datei aus der `.tqz` Datei, indem Sie den Befehl eingeben:

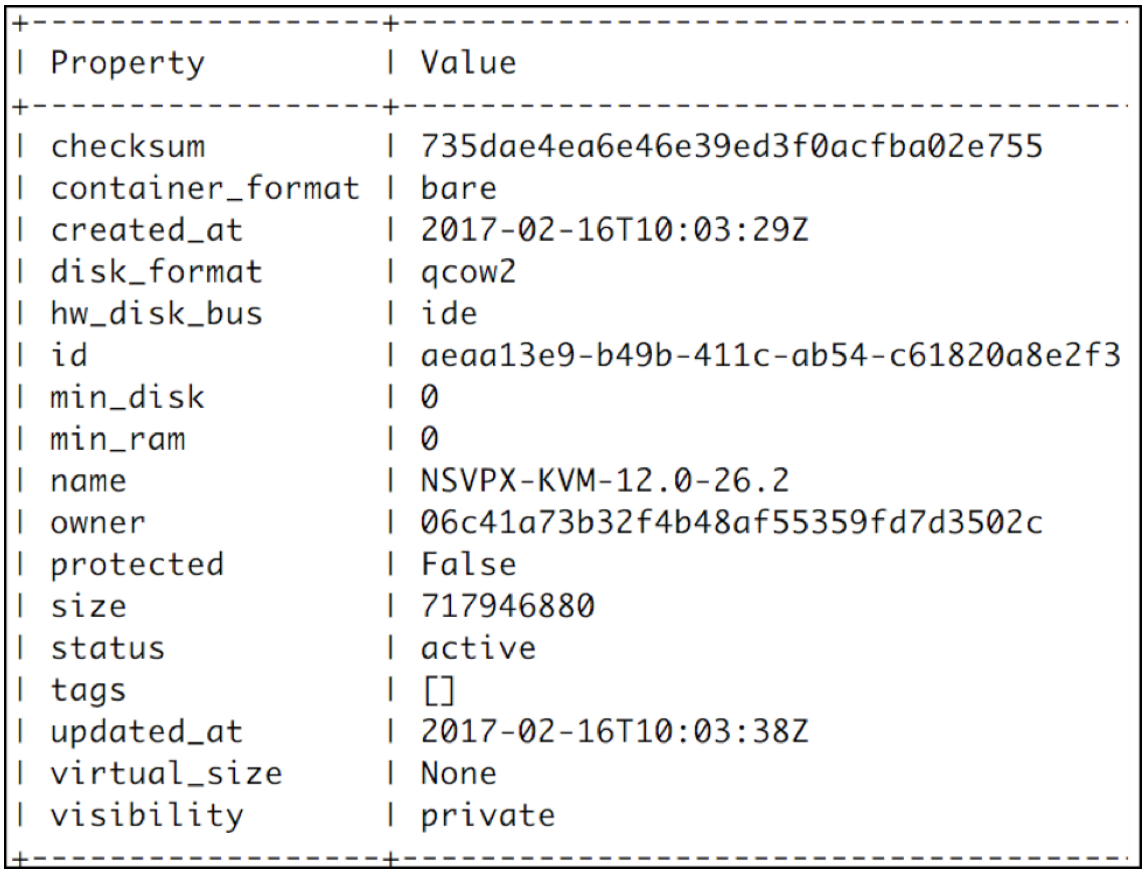
```
tar xvzf <TAR file>
tar xvzf NSVPX-KVM-12.0-26.2_nc.tgz
NSVPX-KVM.xml
NSVPX-KVM-12.0-26.2_nc.qcow2
<!--NeedCopy-->
```

2. Erstellen Sie ein OpenStack-Image mit der in Schritt 1 extrahierten `.qcoz2` Datei, indem Sie den folgenden Befehl eingeben:

```
glance image-create --name="<name of the OpenStack image>" --
    property hw_disk_bus=ide --is-public=true --container-format=
    bare --disk-format=qcow2< <name of the qcow2 file>

glance image-create --name="NS-VPX-12-0-26-2" --property
    hw_disk_bus=ide --is-public= true --container-format=bare --
    disk-format=qcow2< NSVPX-KVM-12.0-26.2_nc.qcow2
<!--NeedCopy-->
```


Die folgende Abbildung enthält eine Beispielausgabe für den Befehl glance image-create.



Property	Value
checksum	735dae4ea6e46e39ed3f0acfba02e755
container_format	bare
created_at	2017-02-16T10:03:29Z
disk_format	qcow2
hw_disk_bus	ide
id	aeaa13e9-b49b-411c-ab54-c61820a8e2f3
min_disk	0
min_ram	0
name	NSVPX-KVM-12.0-26.2
owner	06c41a73b32f4b48af55359fd7d3502c
protected	False
size	717946880
status	active
tags	[]
updated_at	2017-02-16T10:03:38Z
virtual_size	None
visibility	private

3. Nachdem ein OpenStack-Image erstellt wurde, stellen Sie die Citrix ADC VPX-Instanz bereit.

```
nova boot --image NSVPX-KVM-12.0-26.2 --config-drive=true --
   userdata
./userdata.txt --flavor m1. medium --nic net-id=3b258725-eaae-
455e-a5de-371d6d1f349f --nic port-id=218ba819-9f55-4991-adb6-
02086a6bdee2 NSVPX-10
<!--NeedCopy-->
```

Im vorherigen Befehl ist userdata.txt die Datei, die Details wie IP-Adresse, Netzmaske und Standardgateway für die VPX-Instanz enthält. Die Benutzerdatendatei ist eine vom Benutzer anpassbare Datei. NSVPX-KVM-12.0-26.2 ist der Name der virtuellen Appliance, die Sie bereitstellen möchten. —NIC port-id=218ba819-9f55-4991-adb6-02086a6bdee2 ist der OpenStack ss.

Die folgende Abbildung zeigt eine Beispielausgabe des nova Boot-Befehls.

Property	Value
OS-DCF:diskConfig	MANUAL
OS-EXT-AZ:availability_zone	
OS-EXT-SRV-ATTR:host	-
OS-EXT-SRV-ATTR:hypervisor_hostname	-
OS-EXT-SRV-ATTR:instance_name	instance-0000003c
OS-EXT-STS:power_state	0
OS-EXT-STS:task_state	scheduling
OS-EXT-STS:vm_state	building
OS-SRV-USG:launched_at	-
OS-SRV-USG:terminated_at	-
accessIPv4	
accessIPv6	
adminPass	43EjPdM5shLz
config_drive	True
created	2017-02-20T11:53:37Z
flavor	m1.medium (3)
hostId	
id	6b9f6968-aab9-463c-b619-d58c73db3187
image	NSVPX-KVM-12.0-26.2 (a5478b8a-8435-48d1-b4a0-1494e2c8f8b1)
key_name	-
metadata	{}
name	NSVPX-10
os-extended-volumes:volumes_attached	[]
progress	0
security_groups	default
status	BUILD
tenant_id	06c41a73b32f4b48af55359fd7d3502c
updated	2017-02-20T11:53:38Z
user_id	418524f7101b4f0389ecbb36da9916b5

Die folgende Abbildung zeigt ein Beispiel der Datei userdata.txt. Die Werte innerhalb der<PropertySection></PropertySection> Tags sind die Werte, die vom Benutzer konfigurierbar sind und die Informationen wie IP-Adresse, Netzmaske und Standardgateway enthalten.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<Environment xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
oe:id=""
xmlns="http://schemas.dmtf.org/ovf/environment/1">
<PlatformSection>
<Kind>NOVA</Kind>
<Version>2013.1</Version>
<Vendor>Openstack</Vendor>
<Locale>en</Locale>
</PlatformSection>
<PropertySection>
<Property oe:key="com.citrix.netscaler.ovf.version" oe:value="1.0"
   />
<Property oe:key="com.citrix.netscaler.platform" oe:value="vpx"/>
citrix.com 4
<Property oe:key="com.citrix.netscaler.orch_env"
oe:value="openstack-orch-env"/>
```



```
<Property oe:key="com.citrix.netscaler.mgmt.ip"
oe:value="10.1.0.100"/>
<Property oe:key="com.citrix.netscaler.mgmt.netmask"
oe:value="255.255.0.0"/>
<Property oe:key="com.citrix.netscaler.mgmt.gateway"
oe:value="10.1.0.1"/>
</PropertySection>
</Environment>
<!--NeedCopy-->
```

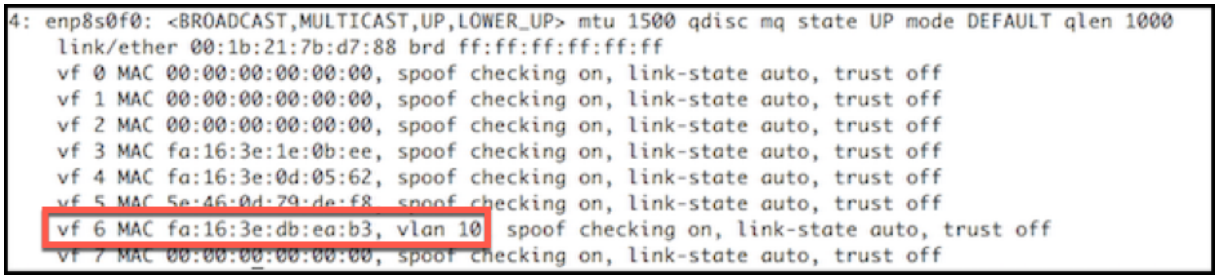
Zusätzliche unterstützte Konfigurationen: Erstellen und Löschen von VLANs auf SR-IOV-VFs vom Host

Geben Sie den folgenden Befehl ein, um ein VLAN auf dem SR-IOV VF zu erstellen:

```
ip link show enp8s0f0 vf 6 vlan 10
```

Im vorherigen Befehl "enp8s0f0" ist der Name der physikalischen Funktion.

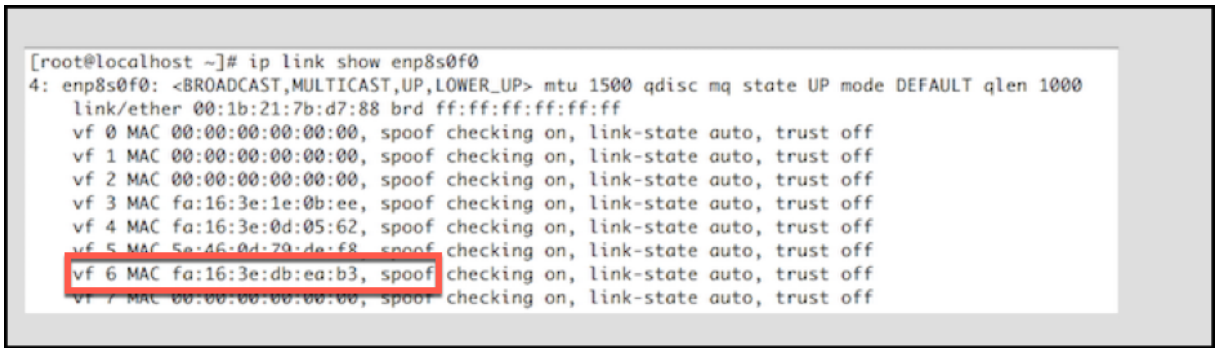
Beispiel: VLAN 10, erstellt auf vf 6



Geben Sie den folgenden Befehl ein, um ein VLAN auf dem SR-IOV VF zu löschen:

```
ip link show enp8s0f0 vf 6 vlan 0
```

Beispiel: VLAN 10, aus vf 6 entfernt



Mit diesen Schritten wird das Verfahren zum Bereitstellen einer Citrix ADC VPX-Instanz, die die SRIOV-Technologie verwendet, auf OpenStack abgeschlossen.

Konfigurieren einer Citrix ADC VPX-Instanz auf KVM für die Verwendung von OVS-DPDK-basierten Hostschnittstellen

October 5, 2021

Sie können eine Citrix ADC VPX-Instanz konfigurieren, die auf KVM (Fedora und RHOS) ausgeführt wird, um Open vSwitch (OVS) mit Data Plane Development Kit (DPDK) für eine bessere Netzwerkleistung zu verwenden. In diesem Dokument wird beschrieben, wie die Citrix ADC VPX-Instanz so konfiguriert wird, dass sie an den `vhost-user` Ports arbeitet, die von OVS-DPDK auf dem KVM-Host bereitgestellt werden.

OVS ist ein Multilayer-Virtual Switch, der unter der Open-Source-Apache 2.0-Lizenz lizenziert DPDK ist eine Reihe von Bibliotheken und Treibern für die schnelle Paketverarbeitung.

Die folgenden Versionen von Fedora, RHOS, OVS und DPDK sind für die Konfiguration einer Citrix ADC VPX-Instanz qualifiziert:

Fedora	RHOS
Fedora 25	RHOS 7,4
OVS 2.7.0	OVS 2.6.1
DPDK 16.11.12	DPDK 16.11.12

Voraussetzungen

Stellen Sie vor der Installation von DPDK sicher, dass der Host über 1 GB große Seiten verfügt.

Weitere Informationen finden Sie in dieser Dokumentation zu den DPDK-Systemanforderungen. Es folgt eine Zusammenfassung der Schritte, die erforderlich sind, um eine Citrix ADC VPX-Instanz auf KVM für die Verwendung von OVS DPDK-basierten Host-Interfaces zu konfigurieren:

- Installieren Sie DPDK.
- Erstellen und Installieren von OVS.
- Erstellen Sie eine OVS-Brücke.
- Schließen Sie eine physikalische Schnittstelle an die OVS-Brücke an.
- Hängen Sie `vhost-user` Ports an den OVS-Datenpfad an.
- Stellen Sie einen KVM-VPX mit OVS-DPDK-basierten `vhost-user` Ports bereit.

DPDK installieren

Um DPDK zu installieren, folgen Sie den Anweisungen in diesem Open vSwitch mit DPDK-Dokument .

Erstellen und Installieren von OVS

Laden Sie OVS von der OVS-Downloadseite herunter. Erstellen und installieren Sie als Nächstes OVS mit einem DPDK-Datapath. Folgen Sie den Anweisungen im Dokument Installieren von Open vSwitch .

Ausführlichere Informationen finden Sie im DPDK Getting Started Guide für Linux.

Erstellen einer OVS-Brücke

Geben Sie je nach Bedarf den Befehl Fedora oder RHOS ein, um eine OVS-Brücke zu erstellen:

Fedora-Befehl:

```
1 > $OVS_DIR/utilities/ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0
     datapath_type=netdev
2 <!--NeedCopy-->
```

RHOS-Befehl:

```
1 ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0 datapath_type=netdev
2 <!--NeedCopy-->
```

Schließen Sie die physikalische Schnittstelle an die OVS-Brücke an

Binden Sie die Ports an DPDK und fügen Sie sie dann an die OVS-Brücke an, indem Sie die folgenden Fedora- oder RHOS-Befehle eingeben:

Fedora-Befehl:

```
1 > $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface
     dpdk0 type=dpdk  options:dpdk-devargs=0000:03:00.0
2
3 > $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 dpdk1 -- set Interface
     dpdk1 type=dpdk  options:dpdk-devargs=0000:03:00.1
4 <!--NeedCopy-->
```

RHOS-Befehl:


```
ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface dpdk0 type=dpdk
    options:dpdk-devargs=0000:03:00.0


ovs-vsctl add-port ovs-br0 dpdk1 -- set Interface dpdk1 type=dpdk
    options:dpdk-devargs=0000:03:00.1
<!--NeedCopy-->
```

Die als Teil der Optionen `dpdk-devargs` gezeigte gibt den PCI-BDF der jeweiligen physikalischen NIC an.

Anhängen von `vhost-user` Ports an den OVS-Datenpfad

Geben Sie die folgenden Fedora- oder RHOS-Befehle ein, um `vhost-user` Ports an den OVS-Datenpfad anzuhängen:

Fedora-Befehl:

```
> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user1 -- set
    Interface vhost-user1 type=dpdkvhostuser -- set Interface vhost-
    user1  mtu_request=9000

> $OVS_DIR/utilities/ovs-vsctl add-port ovs-br0 vhost-user2 -- set
    Interface vhost-user2 type=dpdkvhostuser -- set Interface vhost-
    user2  mtu_request=9000

chmod g+w  /usr/local/var/run/openvswitch/vhost*
<!--NeedCopy-->
```

RHOS-Befehl:

```
ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1
    type=dpdkvhostuser -- set Interface vhost-user1  mtu_request=9000

ovs-vsctl add-port ovs-br0 vhost-user2 -- set Interface vhost-user2
    type=dpdkvhostuser -- set Interface vhost-user2  mtu_request=9000

chmod g+w /var/run/openvswitch/vhost*
<!--NeedCopy-->
```


Stellen Sie einen KVM-VPX mit OVS-DPDK-basierten `vhost-user` Ports bereit

Sie können eine VPX-Instanz auf Fedora KVM mit OVS-DPDK-basierten `vhost-user` Ports nur von der CLI aus bereitstellen, indem Sie die folgenden QEMU-Befehle verwenden:
Fedora Befehl:

```
qemu-system-x86_64 -name KVM-VPX -cpu host -enable-kvm -m 4096M \

-object memory-backend-file,id=mem,size=4096M,mem-path=/dev/hugepages,
   share=on -numa node,memdev=mem \

-mem-prealloc -smp sockets=1,cores=2 -drive file=<absolute-path-to-disc
   -image-file>,if=none,id=drive-ide0-0-0,format=<disc-image-format> \

-device ide-drive,bus=ide.0,unit=0,drive=drive-ide0-0-0,id=ide0-0-0,
   bootindex=1 \

-netdev type=tap,id=hostnet0,script=no,downscript=no,vhost=on \

-device virtio-net-pci,netdev=hostnet0,id=net0,mac=52:54:00:3c:d1:ae,
   bus=pci.0,addr=0x3 \

-chardev socket,id=char0,path=</usr/local/var/run/openvswitch/vhost-
   user1> \

-netdev type=vhost-user,id=mynet1,chardev=char0,vhostforce -device
   virtio-net-pci,mac=00:00:00:00:00:01,netdev=mynet1,mrg_rxbuf=on \

-chardev socket,id=char1,path=</usr/local/var/run/openvswitch/vhost-
   user2> \

-netdev type=vhost-user,id=mynet2,chardev=char1,vhostforce -device
   virtio-net

pci,mac=00:00:00:00:00:02,netdev=mynet2,mrg_rxbuf=on \

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

Verwenden Sie für RHOS die folgende XML-Beispieldatei, um die Citrix ADC VPX-Instanz mithilfe von bereitzustellen `virsh`.


```
<domain type='kvm'>

  <name>dpdk-vpx1</name>

  <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>

  <memory unit='KiB'>16777216</memory>

  <currentMemory unit='KiB'>16777216</currentMemory>

  <memoryBacking>

    <hugepages>

      <page size='1048576' unit='KiB'/>

    </hugepages>

  </memoryBacking>

  <vcpu placement='static'>6</vcpu>

  <cputune>

    <shares>4096</shares>

    <vcpupin vcpu='0' cpuset='0'/>

    <vcpupin vcpu='1' cpuset='2'/>

    <vcpupin vcpu='2' cpuset='4'/>

    <vcpupin vcpu='3' cpuset='6'/>

    <emulatorpin cpuset='0,2,4,6'/>

  </cputune>

  <numatune>

    <memory mode='strict' nodeset='0'/>

  </numatune>

  <resource>
```



```
46
47      <partition>/machine</partition>
48
49    </resource>
50
51    <os>
52
53      <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
54
55      <boot dev='hd'/>
56
57    </os>
58
59    <features>
60
61      <acpi/>
62
63      <apic/>
64
65    </features>
66
67    <cpu mode='custom' match='minimum' check='full'>
68
69      <model fallback='allow'>Haswell-noTSX</model>
70
71      <vendor>Intel</vendor>
72
73      <topology sockets='1' cores='6' threads='1'/>
74
75      <feature policy='require' name='ss'/>
76
77      <feature policy='require' name='pcid'/>
78
79      <feature policy='require' name='hypervisor'/>
80
81      <feature policy='require' name='arat'/>
82
83  <domain type='kvm'>
84
85    <name>dpdk-vpx1</name>
86
87    <uuid>aedb844b-f6bc-48e6-a4c6-36577f2d68d6</uuid>
88
89    <memory unit='KiB'>16777216</memory>
90
```



```
<currentMemory unit='KiB'>16777216</currentMemory>

<memoryBacking>

  <hugepages>

    <page size='1048576' unit='KiB'/>

  </hugepages>

</memoryBacking>

<vcpu placement='static'>6</vcpu>

<cputune>

  <shares>4096</shares>

  <vcpupin vcpu='0' cpuset='0'/>

  <vcpupin vcpu='1' cpuset='2'/>

  <vcpupin vcpu='2' cpuset='4'/>

  <vcpupin vcpu='3' cpuset='6'/>

  <emulatorpin cpuset='0,2,4,6'/>

</cputune>

<numatune>

  <memory mode='strict' nodeset='0'/>

</numatune>

<resource>

  <partition>/machine</partition>

</resource>

<os>

  <type arch='x86_64' machine='pc-i440fx-rhel7.0.0'>hvm</type>
```



```
136
137     <boot dev='hd'/>
138
139   </os>
140
141   <features>
142
143     <acpi/>
144
145     <apic/>
146
147   </features>
148
149   <cpu mode='custom' match='minimum' check='full'>
150
151     <model fallback='allow'>Haswell-noTSX</model>
152
153     <vendor>Intel</vendor>
154
155     <topology sockets='1' cores='6' threads='1'/>
156
157     <feature policy='require' name='ss'/>
158
159     <feature policy='require' name='pcid'/>
160
161     <feature policy='require' name='hypervisor'/>
162
163     <feature policy='require' name='arat'/>
164
165     <feature policy='require' name='tsc_adjust'/>
166
167     <feature policy='require' name='xsaveopt'/>
168
169     <feature policy='require' name='pdpe1gb'/>
170
171     <numa>
172
173       <cell id='0' cpus='0-5' memory='16777216' unit='KiB' memAccess='
            shared'/>
174
175     </numa>
176
177   </cpu>
178
179   <clock offset='utc'/>
```



```
180
181   <on_poweroff>destroy</on_poweroff>
182
183   <on_reboot>restart</on_reboot>
184
185   <on_crash>destroy</on_crash>
186
187   <devices>
188
189     <emulator>/usr/libexec/qemu-kvm</emulator>
190
191     <disk type='file' device='disk'>
192
193       <driver name='qemu' type='qcow2' cache='none'/>
194
195       <source file='/home/NSVPX-KVM-12.0-52.18_nc.qcow2'/>
196
197       <target dev='vda' bus='virtio'/>
198
199       <address type='pci' domain='0x0000' bus='0x00' slot='0x07'
              function='0x0'/>
200
201     </disk>
202
203     <controller type='ide' index='0'>
204
205       <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
              function='0x1'/>
206
207     </controller>
208
209     <controller type='usb' index='0' model='piix3-uhci'>
210
211       <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
              function='0x2'/>
212
213     </controller>
214
215     <controller type='pci' index='0' model='pci-root'/>
216
217     <interface type='direct'>
218
219       <mac address='52:54:00:bb:ac:05'/>
220
221       <source dev='enp129s0f0' mode='bridge'/>
```



```
222
223         <model type='virtio'/>
224
225         <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
               function='0x0'/>
226
227       </interface>
228
229       <interface type='vhostuser'>
230
231         <mac address='52:54:00:55:55:56'/>
232
233         <source type='unix' path='/var/run/openvswitch/vhost-user1' mode=
               'client'/>
234
235         <model type='virtio'/>
236
237         <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
               function='0x0'/>
238
239       </interface>
240
241       <interface type='vhostuser'>
242
243         <mac address='52:54:00:2a:32:64'/>
244
245         <source type='unix' path='/var/run/openvswitch/vhost-user2' mode=
               'client'/>
246
247         <model type='virtio'/>
248
249         <address type='pci' domain='0x0000' bus='0x00' slot='0x05'
               function='0x0'/>
250
251       </interface>
252
253       <interface type='vhostuser'>
254
255         <mac address='52:54:00:2a:32:74'/>
256
257         <source type='unix' path='/var/run/openvswitch/vhost-user3' mode=
               'client'/>
258
259         <model type='virtio'/>
260
```



```
261         <address type='pci' domain='0x0000' bus='0x00' slot='0x06'
               function='0x0'/>
262
263       </interface>
264
265       <interface type='vhostuser'>
266
267         <mac address='52:54:00:2a:32:84'/>
268
269         <source type='unix' path='/var/run/openvswitch/vhost-user4' mode=
               'client'/>
270
271        <model type='virtio'/>
272
273         <address type='pci' domain='0x0000' bus='0x00' slot='0x09'
               function='0x0'/>
274
275       </interface>
276
277       <serial type='pty'>
278
279         <target port='0'/>
280
281       </serial>
282
283       <console type='pty'>
284
285         <target type='serial' port='0'/>
286
287       </console>
288
289       <input type='mouse' bus='ps2'/>
290
291       <input type='keyboard' bus='ps2'/>
292
293       <graphics type='vnc' port='-1' autoport='yes'>
294
295         <listen type='address'/>
296
297       </graphics>
298
299       <video>
300
301         <model type='cirrus' vram='16384' heads='1' primary='yes'/>
302
```



```
303         <address type='pci' domain='0x0000' bus='0x00' slot='0x02'
               function='0x0'/>
304
305       </video>
306
307       <memballoon model='virtio'>
308
309         <address type='pci' domain='0x0000' bus='0x00' slot='0x08'
               function='0x0'/>
310
311       </memballoon>
312
313     </devices>
314
315 </domain
316 <!--NeedCopy-->
```

Punkte zu beachten

In der XML-Datei muss die hugepage Größe 1 GB betragen, wie in der Beispieldatei gezeigt.

```
1 <memoryBacking>
2
3     <hugepages>
4
5       <page size='1048576' unit='KiB'/>
6
7     </hugepages>
8 <!--NeedCopy-->
```

In der Beispieldatei ist vhost-user1 auch der vhost Benutzerport, der an ovs-br0 gebunden ist.

```
1 <interface type='vhostuser'>
2
3       <mac address='52:54:00:55:55:56'/>
4
5       <source type='unix' path='/var/run/openvswitch/vhost-user1' mode=
           'client'/>
6
7       <model type='virtio'/>
8
```



```
9         <address type='pci' domain='0x0000' bus='0x00' slot='0x04'
              function='0x0'/>
10
11      </interface>
12  <!--NeedCopy-->
```

Um die Citrix ADC VPX-Instanz aufzurufen, verwenden Sie den `virsh` Befehl.

Citrix ADC VPX auf AWS

June 1, 2022

Sie können eine Citrix ADC VPX-Instanz auf Amazon Web Services (AWS) starten. Die Citrix ADC VPX-Appliance ist als Amazon Machine Image (AMI) im AWS Marketplace verfügbar. Mit einer Citrix ADC VPX-Instanz auf AWS können Sie AWS-Cloud-Computing-Funktionen nutzen und Citrix ADC Load Balancing- und Traffic-Management-Funktionen für ihre Geschäftsanforderungen verwenden. Die VPX-Instanz unterstützt alle Funktionen der Datenverkehrsverwaltung einer physischen Citrix ADC Appliance und kann als eigenständige Instanzen oder in HA-Paaren bereitgestellt werden. Weitere Informationen zu VPX-Funktionen finden Sie im VPX-Datenblatt.

Erste Schritte

Bevor Sie mit Ihrer VPX-Bereitstellung beginnen, müssen Sie mit den folgenden Informationen vertraut sein:

- AWS-Terminologie
- AWS-VPX-Unterstützungsmatrix
- Einschränkungen und Nutzungsrichtlinien
- Voraussetzungen
- So funktioniert eine Citrix ADC VPX-Instanz auf AWS

Bereitstellen einer Citrix ADC VPX-Instanz auf AWS

In AWS werden die folgenden Bereitstellungstypen für VPX-Instanzen unterstützt:

- Eigenständig
- Hochverfügbarkeit (aktiv-Passiv)
  - Hochverfügbarkeit innerhalb derselben Zone
  - Hochverfügbarkeit über verschiedene Zonen hinweg mit Elastic IP
  - Hochverfügbarkeit über verschiedene Zonen hinweg mit Private IP
- Aktiv-Aktiv GSLB

- Autoscaling (Active-Active) mit ADM

Hybrid-Bereitstellungen

- Bereitstellen von Citrix ADC in AWS Outpost
- Bereitstellen von Citrix ADC in VMC in AWS

Lizenzierung

Für eine Citrix ADC VPX-Instanz auf AWS ist eine Lizenz erforderlich. Die folgenden Lizenzoptionen sind für Citrix ADC VPX-Instanzen verfügbar, die auf AWS ausgeführt werden:

- Kostenlos (unbegrenzt)
- Stündlich
- jährlich
- BYOL
- Kostenlose Testversion (alle Citrix ADC VPX-AWS-Abonnementangebote für 21 Tage kostenlos im AWS Marketplace.)

Automatisierung

- Citrix ADM: Intelligente Bereitstellung
- AWS-Schnellstarts: Citrix ADC VPX für Webanwendungen auf AWS
- GitHub CFTs: Citrix ADC Vorlagen und Skripts für die AWS-Bereitstellung
- GitHub Ansible: Citrix ADC Vorlagen und Skripts für die AWS-Bereitstellung
- GitHub Terraform: Citrix ADC Vorlagen und Skripts für die AWS-Bereitstellung
- AWS-Pattern-Bibliothek (PL): Citrix ADC VPX

Blogs

- Wie Citrix ADC auf AWS Kunden hilft, Anwendungen sicher bereitzustellen
- Anwendungsbereitstellung in Hybrid Cloud mit Citrix ADC und AWS
- Citrix ist ein AWS-Netzwerkkompetenzpartner
- Citrix ADC: Immer bereit für Public Clouds
- Einfache Skalierung oder Skalierung in öffentlichen Clouds mit Citrix ADC
- Citrix erweitert die Auswahl an ADC-Bereitstellungen mit AWS Outposts

- Verwenden von Citrix ADC mit Amazon VPC-Ingress-Routing
- Citrix bietet Auswahl, Leistung und vereinfachte Bereitstellung in AWS
- Die Sicherheit der Citrix Web App Firewall — jetzt auf dem AWS Marketplace
- Wie Aria Systems die Citrix Web App Firewall auf AWS verwendet

Videos

- Vereinfachung der Public Cloud Citrix ADC-Bereitstellungen durch ADM
- Provisioning und Konfiguration von Citrix ADC VPX in AWS mit sofort einsatzbereiten Terraform-Skripten
- Bereitstellen von Citrix ADC HA in AWS mithilfe der CloudFormation-Vorlage
- Bereitstellen von Citrix ADC HA über Availability Zones hinweg mit AWS QuickStart
- So stellen Sie Citrix ADC in AWS bereit
- Citrix ADC Autoscale mit ADM
- Citrix ADC unterstützt automatische Backend-Serverskalierung in AWS oder AWS Autoscaling-Gruppe

Fallstudien von Kunden

- Technologielösung — Xenit AB
- Ein besserer Weg, um mit Citrix und AWS Cloud Geschäfte zu machen — Aria
- Entdecken Sie den Vorteil von Citrix ADC und AWS
- Regen zu vermieten - Kundenbericht

Lösungen

- Bereitstellung einer digitalen Werbeplattform auf AWS mit Citrix ADC
- Verbesserung der Clickstream-Analyse in AWS mit Citrix ADC

Support

- Öffnen eines Support-Falls
- Informationen zum Angebot von Citrix ADC-Abonnements finden Sie unter Problembehandlung bei einer VPX-Instanz in AWS. Um einen Support-Fall zu erstellen, suchen Sie Ihre AWS-Kontonummer und Ihren Support-PIN-Code und rufen Sie den Citrix Support an.

- Stellen Sie für Citrix ADC Customer Licensed Offering oder BYOL sicher, dass Sie über den gültigen Support- und Wartungsvertrag verfügen. Wenn Sie keine Vereinbarung haben, wenden Sie sich an Ihren Citrix Vertreter.

Zusätzliche Referenzen

- AWS-Webinar auf Abruf — Citrix ADC auf AWS
- Bereitstellungshandbücher für Citrix ADC VPX auf AWS
- Erstellen eines VPX Amazon Machine Image (AMI) in SC2S/geheimer Region
- Citrix ADC auf AWS
- Citrix ADC und AWS validiertes Referenzdesign
- Citrix ADC VPX — Datenblatt
- Citrix ADC im AWS Marketplace
- Citrix ADC ist Teil der AWS-Netzwerkpartnerlösungen (Load Balancer)
- Citrix ADC für VMware Cloud auf AWS
- AWS FAQs

AWS-Terminologie

October 5, 2021

In diesem Abschnitt wird die Liste der häufig verwendeten AWS-Begriffe und -Ausdrücke beschrieben. Weitere Informationen finden Sie unter AWS Glossar.

Begriff	Definition
Amazon Machine Image (AMI)	Ein Maschinenimage, das die Informationen bereitstellt, die zum Starten einer Instanz erforderlich sind, bei der es sich um einen virtuellen Server in der Cloud handelt.
Elastic Block Store	Bietet persistente Blockspeicher-Volumes für die Verwendung mit Amazon EC2-Instanzen in der AWS-Cloud.
Simple Storage Service (S3)	Speicher für das Internet. Es wurde entwickelt, um Web-Scale-Computing für Entwickler einfacher zu machen.

Begriff	Definition
Elastic Compute Cloud (EC2)	Ein Webdienst, der sichere, skalierbare Rechenkapazität in der Cloud bereitstellt. Es wurde entwickelt, um Web-basierte Cloud Computing für Entwickler einfacher zu machen.
Elastischer Lastenausgleich (ELB)	Verteilt eingehenden Anwendungsdatenverkehr auf mehrere EC2-Instanzen in mehreren Availability Zones. Dies erhöht die Fehlertoleranz Ihrer Anwendungen.
Elastische Netzwerkschnittstelle (ENI)	Eine virtuelle Netzwerkschnittstelle, die Sie an eine Instanz in einer Virtual Private Cloud (VPC) anfügen können.
Elastic IP (EIP) Adresse	Eine statische, öffentliche IPv4-Adresse, die Sie in Amazon EC2 oder Amazon VPC zugewiesen und dann einer Instanz zugeordnet haben. Elastic IP-Adressen sind Ihrem Konto zugeordnet, nicht einer bestimmten Instanz. Sie sind elastisch, weil Sie sie leicht zuordnen, befestigen, lösen und befreien können, wenn sich Ihre Bedürfnisse ändern.
Instanztyp	Amazon EC2 bietet eine große Auswahl an Instanztypen, die für verschiedene Anwendungsfälle optimiert sind. Instanztypen umfassen unterschiedliche Kombinationen von CPU-, Arbeitsspeicher-, Speicher- und Netzwerkkapazität und bieten Ihnen die Flexibilität, den geeigneten Ressourcenmix für Ihre Anwendungen auszuwählen.

Begriff	Definition
Identity and Access Management (IAM)	Eine AWS-Identität mit Berechtigungsrichtlinien, die bestimmen, was die Identität in AWS tun kann und nicht. Sie können eine IAM-Rolle verwenden, um Anwendungen, die auf einer EC2-Instanz ausgeführt werden, den sicheren Zugriff auf Ihre AWS-Ressourcen zu ermöglichen. Die IAM-Rolle ist erforderlich, um VPX-Instanzen in einem Hochverfügbarkeits-Setup bereitzustellen.
Internet-Gateway	Verbindet ein Netzwerk mit dem Internet. Sie können Datenverkehr für IP-Adressen außerhalb Ihrer VPC an das Internet-Gateway weiterleiten.
Schlüsselpaar	Eine Reihe von Sicherheitsanmeldeinformationen, die Sie zum elektronischen Nachweis Ihrer Identität verwenden. Ein Schlüsselpaar besteht aus einem privaten Schlüssel und einem öffentlichen Schlüssel.
Routentabellen	Eine Reihe von Routingregeln, die den Datenverkehr steuert, der ein Subnetz verlässt, das der Routingtabelle zugeordnet ist. Sie können einer einzelnen Routingtabelle mehrere Subnetze zuordnen, aber ein Subnetz kann jeweils nur einer Routingtabelle zugeordnet werden.
Sicherheitsgruppen	Eine benannte Gruppe zulässiger eingehender Netzwerkverbindungen für eine Instanz.
Subnetze	Ein Segment des IP-Adressbereichs einer VPC, an die EC2-Instanzen angeschlossen werden können. Sie können Subnetze erstellen, um Instanzen entsprechend den Sicherheits- und betrieblichen Anforderungen zu gruppieren.

Begriff	Definition
Virtuelle Private Cloud (VPC)	Ein Webservice zum Provisioning eines logisch isolierten Abschnitts der AWS-Cloud, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können.
Auto Scaling	Ein Webservice zum automatischen Starten oder Beenden von Amazon EC2-Instanzen basierend auf benutzerdefinierten Richtlinien, Zeitplänen und Zustandsprüfungen.
CloudFormation	Ein Service zum Schreiben oder Ändern von Vorlagen, die zugehörige AWS-Ressourcen zusammen als Einheit erstellen und löschen.

VPX-AWS-Unterstützungsmatrix

December 3, 2021

In den folgenden Tabellen sind das unterstützte VPX-Modell und die AWS-Regionen, Instanztypen und Dienste aufgeführt.

Tabelle 1: Unterstützte VPX-Modelle auf AWS

Unterstütztes VPX-Modell
Citrix ADC VPX Standard/Erweiterte/Premium Edition — 200 Mbit/s
Citrix ADC VPX Standard/Erweiterte/Premium Edition — 1000 Mbit/s
Citrix ADC VPX Standard/Erweiterte/Premium Edition — 3 Gbit/s
Citrix ADC VPX Standard/Erweitert/Premium Edition — 5 Gbit/s
Citrix ADC VPX Standard/Erweitert/Premium — 10 Mbit/s
Citrix ADC VPX Express — 20 Mbit/s
Citrix ADC VPX — vom Kunden lizenziert
Citrix ADC (ehemals NetScaler) VPX FIPS — vom Kunden lizenziert

Tabelle: 2 Unterstützte AWS-Regionen

Unterstützte AWS Regionen
US-Westregion (Oregon)
US-Westregion (Nordkalifornien)
Ost-Region (Ohio)
Region Amerikanischer Osten (Nord-Virginia)
Region Asien-Pazifik (Mumbai)
Region Asien-Pazifik (Seoul)
Region Kanada (Zentral)
Region Asien-Pazifik (Singapur)
Region Asien-Pazifik (Sydney)
Asien-Pazifik (Tokio)
Region Asien-Pazifik (Hongkong)
Region Kanada (Zentral)
Region China (Peking)
Region China (Ningxia)
Region EU (Frankfurt)
Region EU (Irland)
EU (London)
EU (Paris)
Region EU (Mailand)
Region Südamerika (São Paulo)
AWS-Region GovCloud (US-Ost)
AWS-Region GovCloud (US-West)
AWS-Region “Top Secret” (C2S)
Region Mittlerer Osten (Bahrain)
Afrika (Kapstadt)
C2S

Tabelle 3: Unterstützte AWS-Instanztypen

Unterstützte AWS-Instanztypen
t2.medium, t2.large, t2.x large, t2.2x large
m3.large, m3.x large, m3.2x large
c4.large, c4.large, c4.2x large, c4.4x large, c4.8x large
m4.large, m4.large, m4.2x large, m4.4x large, m4.10x large
m5.large, m5.x large, m5.2x large, m5.4x large, m5.12x large, m5.24x large
c5.large, c5.x large, c5.2x large, c5.4x large, c5.9x large, c5.18x large, c5.24x large
C5n.large, C5n.x large, C5n.2x large, C5n.4x large, C5n.9x large, C5n.18x large
D2.x large, D2.2x large, D2.4x large, D2.8x large
m5a.large, m5a.xlarge, m5a.2xlarge, m5a.8xlarge, m5a.12xlarge, m5a.16xlarge, m5a.24xlarge
t3a.medium, t3a.large, t3a.xlarge, t3a.2xlarge

Tabelle 4: Unterstützte AWS-Services

Unterstützte AWS Services
EC2: Startet ADC-Instanzen.
Lambda: Ruft Citrix ADC VPX NITRO-APIs während der Bereitstellung von Citrix ADC VPX-Instanzen über CFT auf.
VPC- und VPC-Ingress-Routing: VPC erstellt isolierte Netzwerke, in denen ADC gestartet werden kann. Das VPC Ingress Routing wird in der Firewall Load Balancing-Lösung verwendet.
Route53: Verteilt den Datenverkehr auf alle ADC VPX-Knoten der Citrix ADC Autoscale-Lösung.
ELB: Verteilt den Datenverkehr auf alle ADC VPX-Knoten in der Citrix ADC Autoscale-Lösung.
Cloudwatch: Überwacht Leistung und Systemparameter für die Citrix ADC VPX Instanz.
AWS Autoscaling: Wird für die automatische Skalierung von Backend-Servern verwendet.
Cloud-Bildung: CloudFormation-Vorlagen werden verwendet, um Citrix ADC VPX-Instanzen bereitzustellen.
Simple Queue Service (SQS): Überwacht Skalierungs- und Herunterskalierungsereignisse beim Back-End-Autoscaling.
Simple Notification Service (SNS): Überwacht Skalierungs- und Herunterskalierungsereignisse beim Back-End-Autoscaling.
Identitäts- und Zugriffsmanagement (IAM): Bietet Zugriff auf AWS-Services und -Ressourcen.

Unterstützte AWS Services
AWS-Außenposten: Bereitstellung von Citrix ADC VPX-Instanzen in AWS Outposts.

Citrix empfiehlt die folgenden AWS-Instanztypen:

- M5- und C5n-Serien für Marketplace-Editionen oder bandbreitenbasierte Poollizenzierung.
- C5n-Serie für vCPU-basierte Pool-Lizenzierung.

VPX-Angebot auf dem AWS-Marktplatz	AWS-Instanzempfehlung
VPX 10, VPX Express 20, VPX 200	M5.xLarge
VPX 1000, VPX 3 G, VPX 5 G	M5.2xLarge

Citrix empfiehlt die folgenden AWS-Instanztypen basierend auf dem Durchsatz.

VPX mit gepoolter Lizenzierung (Bandbreitenlizenzen)	AWS-Instanzempfehlung
VPX 8G	C5n.4xLarge
VPX 10G, VPX 15G, VPX 25G	C5n.9xLarge

> Hinweis:
>
> Das VPX 25G-Angebot bietet nicht den gewünschten 25G-Durchsatz in AWS, kann jedoch zu einer höheren SSL-Transaktionsrate führen.

Gehen Sie wie folgt vor, um einen Durchsatz von mehr als 5G zu erreichen:

- Wählen Sie **Citrix ADC VPX — Customer Licensed (BYOL)-Angebot** im AWS Marketplace.
- Wählen Sie **Pooled Licensing (Bandbreitenlizenzen)** in der Citrix ADC GUI oder CLI aus.

Um Ihre Instanz basierend auf verschiedenen Metriken wie Paketen pro Sekunde und SSL-Transaktionsrate zu ermitteln, wenden Sie sich an Ihren Citrix Kontakt, um Unterstützung zu erhalten. Wenden Sie sich an den Citrix Support, um Informationen zur vCPU-basierten Poollizenzierung und Größenbestimmung zu erhalten.

Einschränkungen und Nutzungsrichtlinien

October 5, 2021

Bei der Bereitstellung einer Citrix ADC VPX-Instanz in AWS gelten die folgenden Einschränkungen und Verwendungsrichtlinien:

- Bevor Sie beginnen, lesen Sie den Abschnitt AWS-Terminologie unter Bereitstellen einer Citrix ADC VPX-Instanz auf AWS.
- Das Clustering-Feature wird für VPX nicht unterstützt.
- Damit das Hochverfügbarkeitssetup effektiv funktioniert, verknüpfen Sie ein dediziertes NAT-Gerät der Verwaltungsschnittstelle oder verknüpfen Sie EIP mit NSIP. Weitere Informationen zu NAT finden Sie in der AWS-Dokumentation unter NAT-Instances.
- Datenverkehr und Verwaltungsverkehr müssen durch ENIs getrennt werden, die zu verschiedenen Subnetzen gehören.
- Nur die NSIP-Adresse darf auf der Management-ENI vorhanden sein.
- Wenn eine NAT-Instanz zur Sicherheit verwendet wird, anstatt dem NSIP einen EIP zuzuweisen, sind entsprechende Änderungen beim Routing auf VPC-Ebene erforderlich. Anweisungen zum Vornehmen von Routingänderungen auf VPC-Ebene finden Sie in der AWS-Dokumentation unter Szenario 2: VPC mit öffentlichen und privaten Subnetzen.
- Eine VPX-Instanz kann von einem EC2-Instanztyp in einen anderen verschoben werden (z. B. von m3.large zu m3.xlarge).
- Für Speicheroptionen für VPX in AWS empfiehlt Citrix EBS, da es dauerhaft ist und die Daten auch verfügbar sind, nachdem sie von der Instanz getrennt wurden.
- Das dynamische Hinzufügen von ENIs zu VPX wird nicht unterstützt. Starten Sie die VPX-Instanz neu, um das Update anzuwenden. Citrix empfiehlt, die eigenständige Instanz oder die HA-Instanz zu beenden, das neue ENI anzuhängen und die Instanz dann neu zu starten.
- Sie können einem ENI mehrere IP-Adressen zuweisen. Die maximale Anzahl von IP-Adressen pro ENI wird durch den EC2-Instanztyp bestimmt, siehe Abschnitt “IP-Adressen pro Netzwerkschnittstelle pro Instanztyp” in Elastic Network Interfaces. Sie müssen die IP-Adressen in AWS zuweisen, bevor Sie sie ENIs zuweisen. Weitere Informationen finden Sie unter Elastic Network Interfaces.
- Citrix empfiehlt, die Interface-Befehle zum Aktivieren und Deaktivieren von Citrix ADC VPX Schnittstellen zu vermeiden.
- Die Citrix ADC Befehle `set ha node \<NODE\_ID\> -haStatus STAYPRIMARY` und `set ha node \<NODE\_ID\> -haStatus STAYSECONDARY` sind standardmäßig deaktiviert.
- IPv6 wird für VPX nicht unterstützt.
- Aufgrund von AWS-Einschränkungen werden diese Funktionen nicht unterstützt:
  - Gratuitous ARP(GARP)

  - L2-Modus
  - Tagged VLAN
  - Dynamisches Routing
  - virtual MAC

- Damit RNAT funktioniert, stellen Sie sicher, dass die **Quelle/Destination Check** deaktiviert ist. Weitere Informationen finden Sie unter "Ändern der Quelle/Zielüberprüfung" in Elastic Network Interfaces.

- In einer Citrix ADC VPX Bereitstellung auf AWS in einigen AWS-Regionen kann die AWS-Infrastruktur möglicherweise keine AWS-API-Aufrufe auflösen. Dies geschieht, wenn die API-Aufrufe über eine Nichtverwaltungsschnittstelle auf der Citrix ADC VPX-Instanz ausgegeben werden.
  Beschränken Sie zur Problemumgehung die API-Aufrufe nur auf die Verwaltungsschnittstelle. Erstellen Sie dazu ein NSVLAN auf der VPX-Instanz und binden Sie die Verwaltungsschnittstelle mit dem entsprechenden Befehl an das NSVLAN.
  Beispiel:
  ```
  set ns config -nsvlan <vlan id> -ifnum 1/1 -tagged NO
  save config
  ```
  Starten Sie die VPX-Instanz an der Eingabeaufforderung neu. Weitere Informationen zum Konfigurieren `nsvlan`finden Sie unter Konfigurieren von NSVLAN.

- In der AWS-Konsole kann die vCPU-Auslastung, die für eine VPX-Instanz auf der Registerkarte **Überwachung** angezeigt wird, hoch sein (bis zu 100 Prozent), selbst wenn die tatsächliche Auslastung wesentlich geringer ist. Um die tatsächliche vCPU-Auslastung **anzuzeigen, navigieren Sie zu Alle CloudWatch-Metriken**anzeigen. Weitere Informationen finden Sie unter Überwachen Sie Ihre Instanzen mit Amazon CloudWatch.

Voraussetzungen

January 25, 2022

Bevor Sie versuchen, eine VPX-Instanz in AWS zu erstellen, stellen Sie sicher, dass Sie über Folgendes verfügen:

- **Ein AWS-Konto**: zum Starten eines Citrix ADC VPX AMI in einer AWS Virtual Private Cloud (VPC). Unter www.aws.amazon.com können Sie kostenlos ein AWS-Konto erstellen.

- **Ein AWS Identity and Access Management (IAM) -Benutzerkonto**: zum sicheren Steuern des Zugriffs auf AWS-Services und -Ressourcen für Ihre Benutzer. Weitere Informationen zum Erstellen eines IAM-Benutzerkontos finden Sie unter Erstellen von IAM-Benutzern (Konsole). Eine

IAM-Rolle ist sowohl für eigenständige als auch für Hochverfügbarkeitsbereitstellungen obligatorisch.

Die mit Ihrem AWS-Konto verknüpfte IAM-Rolle muss für verschiedene Szenarien über die folgenden IAM-Berechtigungen verfügen.

HA-Paar in derselben AWS-Zone:

```
”ec2:DescribeInstances”,
”ec2:AssignPrivateIpAddresses”,
”iam:SimulatePrincipalPolicy”,
”iam:GetRole”
<!--NeedCopy-->
```

HA-Paar mit elastischen IP-Adressen über verschiedene AWS-Zonen hinweg:

```
”ec2:DescribeInstances”,
”ec2:DescribeAddresses”,
”ec2:AssociateAddress”,
”ec2:DisassociateAddress”,
”iam:SimulatePrincipalPolicy”,
”iam:GetRole”
<!--NeedCopy-->
```

HA-Paar mit privaten IP-Adressen über verschiedene AWS-Zonen hinweg:

```
”ec2:DescribeInstances”,
”ec2:DescribeRouteTables”,
”ec2:DeleteRoute”,
”ec2:CreateRoute”,
”ec2:ModifyNetworkInterfaceAttribute”,
”iam:SimulatePrincipalPolicy”,
”iam:GetRole”
<!--NeedCopy-->
```

HA-Paar mit privaten IP-Adressen und elastischen IP-Adressen über verschiedene AWS-Zonen hinweg:

```
”ec2:DescribeInstances”,
”ec2:DescribeAddresses”,
```



```
3   "ec2:AssociateAddress",
4   "ec2:DisassociateAddress",
5   "ec2:DescribeRouteTables",
6   "ec2:DeleteRoute",
7   "ec2:CreateRoute",
8   "ec2:ModifyNetworkInterfaceAttribute",
9   "iam:SimulatePrincipalPolicy",
10  "iam:GetRole"
11  <!--NeedCopy-->
```

Autoscaling des AWS-Backends:

```
1   "ec2:DescribeInstances",
2   "autoscaling:*",
3   "sns:CreateTopic",
4   "sns:DeleteTopic",
5   "sns:ListTopics",
6   "sns:Subscribe",
7   "sqs:CreateQueue",
8   "sqs:ListQueues",
9   "sqs:DeleteMessage",
10  "sqs:GetQueueAttributes",
11  "sqs:SetQueueAttributes",
12  "iam:SimulatePrincipalPolicy",
13  "iam:GetRole",
14  <!--NeedCopy-->
```

> Hinweis:
>
> - Wenn Sie eine Kombination der vorhergehenden Funktionen verwenden, verwenden Sie die Kombination von IAM-Berechtigungen für jede der Funktionen.
> - Wenn Sie die Citrix CloudFormation-Vorlage verwenden, wird die IAM-Rolle automatisch erstellt. Die Vorlage erlaubt es nicht, eine bereits erstellte IAM-Rolle auszuwählen.
> - Wenn Sie sich über die GUI bei der VPX-Instanz anmelden, wird eine Aufforderung zur Konfiguration der erforderlichen Berechtigungen für die IAM-Rolle angezeigt. Ignorieren Sie die Aufforderung, wenn Sie die Berechtigungen bereits konfiguriert haben.

- **AWS CLI**: So verwenden Sie alle Funktionen, die von der AWS Management Console aus Ihrem Terminalprogramm bereitgestellt werden. Weitere Informationen finden Sie im AWS CLI-Benutzerhandbuch. Sie benötigen auch die AWS CLI, um den Netzwerkschnittstellentyp in SR-IOV zu ändern.

- **Elastic Network Adapter (ENA)**: Für den treiberfähigen ENA-Instanz-Typ, z. B. M5-, C5-Instanzen, muss die Firmware-Version 13.0 und höher sein.

Funktionsweise einer Citrix ADC VPX-Instanz in AWS

October 5, 2021

Die Citrix ADC VPX-Instanz ist als AMI im AWS-Marketplace verfügbar und kann als EC2-Instanz innerhalb einer AWS VPC gestartet werden. Die Citrix ADC VPX AMI-Instanz benötigt mindestens 2 virtuelle CPUs und 2 GB Arbeitsspeicher. Eine EC2-Instanz, die in einer AWS VPC gestartet wird, kann auch die für die VPX-Konfiguration erforderlichen Schnittstellen, mehrere IP-Adressen pro Schnittstelle sowie öffentliche und private IP-Adressen bereitstellen. Jede VPX-Instanz benötigt mindestens drei IP-Subnetze:

- Ein Management-Subnetz
- Ein Client-Subnetz (VIP)
- Ein Backend-Subnetz (SNIP, MIP usw.)

Citrix empfiehlt drei Netzwerkschnittstellen für eine Standard-VPX-Instanz in der AWS-Installation.

AWS stellt derzeit Multi-IP-Funktionen nur für Instanzen zur Verfügung, die in einer AWS VPC ausgeführt werden. Eine VPX-Instanz in einer VPC kann zum Lastausgleich von Servern verwendet werden, die in EC2-Instanzen ausgeführt werden. Mit einer Amazon VPC können Sie eine virtuelle Netzwerkumgebung erstellen und steuern, einschließlich Ihres eigenen IP-Adressbereichs, Subnetze, Routentabellen und Netzwerk-Gateways.

Hinweis: Standardmäßig können Sie für jedes AWS-Konto bis zu 5 VPC-Instanzen pro AWS-Region erstellen. Sie können höhere VPC-Grenzwerte anfordern, indem Sie das Antragsformular von Amazon absendenhttp://aws.amazon.com/contact-us/vpc-request.

Abbildung 1. Eine Beispielbereitstellung von Citrix ADC VPX-Instanz in der AWS-Architektur

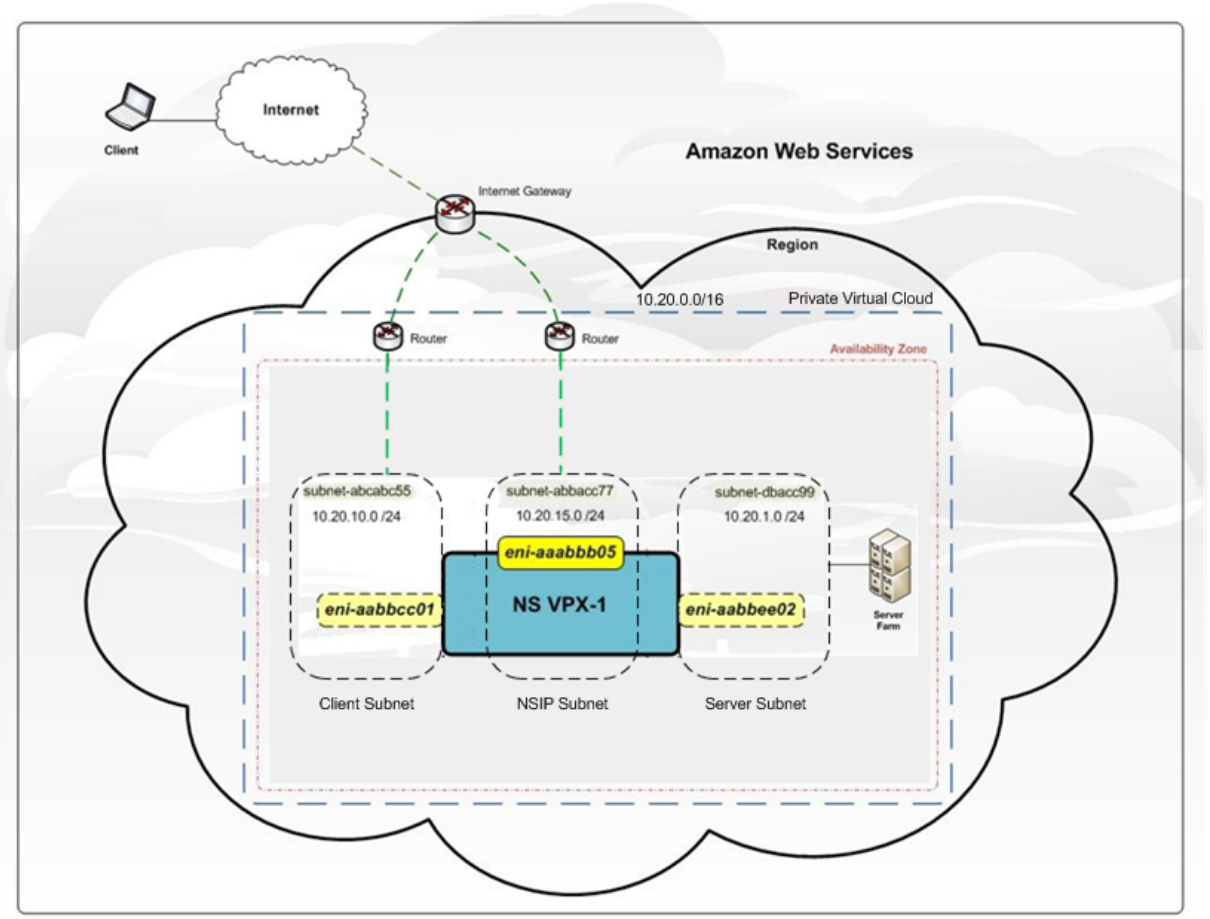


Abbildung 1 zeigt eine einfache Topologie einer AWS VPC mit einer Citrix ADC VPX Bereitstellung. Die AWS VPC verfügt über:

1. Ein einzelnes Internet-Gateway zum Weiterleiten des Datenverkehrs in und aus der VPC.
2. Netzwerkverbindung zwischen dem Internet-Gateway und dem Internet.
3. Drei Subnetze, jeweils eines für Management, Client und Server.
4. Netzwerkverbindung zwischen dem Internet-Gateway und den beiden Subnetzen (Verwaltung und Client).
5. Eine eigenständige Citrix ADC VPX-Instanz, die in der VPC bereitgestellt wird. Die VPX-Instanz verfügt über drei ENIs, eine mit jedem Subnetz verbunden.

Bereitstellen einer eigenständigen Citrix ADC VPX-Instanz in AWS

October 5, 2021

Sie können eine eigenständige Citrix ADC VPX-Instanz in AWS mithilfe der folgenden Optionen bereitstellen:

- AWS-Webkonsole
- Citrix erstellte CloudFormation-Vorlage
- AWS CLI

In diesem Thema wird das Verfahren zum Bereitstellen einer Citrix ADC VPX-Instanz in AWS beschrieben.

Lesen Sie vor dem Start der Bereitstellung die folgenden Themen:

- Voraussetzungen
- Einschränkungs- und Nutzungsrichtlinien

Bereitstellen einer Citrix ADC VPX-Instanz in AWS mithilfe der AWS-Webkonsole

Sie können eine Citrix ADC VPX-Instanz auf AWS über die AWS-Webkonsole bereitstellen. Der Bereitstellungsprozess umfasst die folgenden Schritte:

1. Erstellen eines Schlüsselpaars
2. Erstellen einer virtuellen privaten Cloud (VPC)
3. Weitere Subnetze hinzufügen
4. Erstellen von Sicherheitsgruppen und Sicherheitsregeln
5. Routentabellen hinzufügen
6. Erstellen eines Internet-Gateway
7. Erstellen einer Citrix ADC VPX-Instanz
8. Erstellen und Anfügen weiterer Netzwerkschnittstellen
9. Elastische IP-Adressen an die Management-NIC anhängen
10. Herstellen einer Verbindung mit der VPX-Instanz

Schritt 1: Erstellen Sie ein Schlüsselpaar.

Amazon EC2 verwendet ein Schlüsselpaar zum Verschlüsseln und Entschlüsseln von Anmeldeinformationen. Um sich bei der Instanz anzumelden, müssen Sie ein Schlüsselpaar erstellen, den Namen des Schlüsselpaars beim Starten der Instanz angeben und den privaten Schlüssel angeben, wenn Sie eine Verbindung mit der Instanz herstellen.

Wenn Sie eine Instanz mit dem AWS Launch Instance Wizard überprüfen und starten, werden Sie aufgefordert, ein vorhandenes Schlüsselpaar zu verwenden oder ein neues Schlüsselpaar zu erstellen. Weitere Informationen zum Erstellen eines Schlüsselpaars finden Sie unter Amazon EC2-Schlüsselpaare.

Schritt 2: Erstellen einer VPC.

Eine Citrix ADC VPC-Instanz wird in einer AWS VPC bereitgestellt. Mit einer VPC können Sie das virtuelle Netzwerk definieren, das Ihrem AWS-Konto gewidmet ist. Weitere Informationen zu AWS VPC finden Sie unter Erste Schritte mit Amazon VPC.

Beachten Sie beim Erstellen einer VPC für Ihre Citrix ADC VPX-Instanz die folgenden Punkte:

- Verwenden Sie die Option VPC with a Single Public Subnet, um eine AWS-VPC in einer AWS-Availability Zone zu erstellen.
- Citrix empfiehlt, mindestens **drei Subnetze**der folgenden Typen zu erstellen:
  - Ein Subnetz für den Verwaltungsdatenverkehr. Sie platzieren die Management-IP (NSIP) in diesem Subnetz. Standardmäßig wird die elastische Netzwerkschnittstelle (ENI) eth0 für die Verwaltung IP verwendet.
  - Ein oder mehrere Subnetze für den Clientzugriffsverkehr (User-to-Citrix ADC VPX), über die Clients eine Verbindung zu einer oder mehreren virtuellen IP (VIP) -Adressen herstellen, die den virtuellen Servern des Citrix ADC Load Balancing zugewiesen sind.
  - Ein oder mehrere Subnetze für den Serverzugriffsverkehr (VPX-zu-Server), über den Ihre Server eine Verbindung zu VPX-eigenen Subnetz-IP (SNIP) -Adressen herstellen. Weitere Informationen zum Citrix ADC Lastenausgleich und zu virtuellen Servern, virtuellen IP-Adressen (VIPs) und Subnetz-IP-Adressen (SNIPs) finden Sie unter:
  - Alle Subnetze müssen sich in derselben Availability Zone befinden.

Schritt 3: Fügen Sie Subnetzehinzu.

Wenn Sie den VPC-Assistenten verwendet haben, wurde nur ein Subnetz erstellt. Je nach Anforderung möchten Sie möglicherweise weitere Subnetze erstellen. Weitere Informationen zum Erstellen weiterer Subnetze finden Sie unter Hinzufügen eines Subnetzes zu Ihrer VPC.

Schritt 4: Erstellen von Sicherheitsgruppen und Sicherheitsregeln.

Um eingehenden und ausgehenden Datenverkehr zu steuern, erstellen Sie Sicherheitsgruppen und fügen Sie den Gruppen Regeln hinzu. Weitere Informationen zum Erstellen von Gruppen und zum Hinzufügen von Regeln finden Sie unter Sicherheitsgruppen für Ihre VPC.

Für Citrix ADC VPX -Instanzen stellt der EC2-Assistent Standardsicherheitsgruppen bereit, die von AWS Marketplace generiert werden und auf empfohlenen Einstellungen von Citrix basieren. Sie können jedoch weitere Sicherheitsgruppen basierend auf Ihren Anforderungen erstellen.

> **Hinweis:**
>
> Port 22, 80, 443, der auf der Sicherheitsgruppe für SSH-, HTTP- und HTTPS-Zugriff geöffnet werden soll.

Schritt 5: Routentabellen hinzufügen.

Die Routing-Tabelle enthält eine Reihe von Regeln, die als Routen bezeichnet werden, um zu bestimmen, wohin der Netzwerkverkehr gerichtet wird. Jedes Subnetz in Ihrer VPC muss einer Routentabelle zugeordnet sein. Weitere Informationen zum Erstellen einer Routentabelle finden Sie unter Routentabellen.

Schritt 6: Erstellen Sie ein Internet-Gateway.

Ein Internet-Gateway dient zwei Zwecken: ein Ziel in Ihren VPC-Routentabellen für den internetroutbaren Datenverkehr bereitzustellen und NAT (Network Address Translation, Network Address

Translation, Network Address Translation, NAT) für Instanzen durchzuführen, denen öffentliche IPv4-Adressen zugewiesen wurden.

Erstellen Sie ein Internet-Gateway für den Internetverkehr. Weitere Informationen zum Erstellen eines Internet-Gateways finden Sie im Abschnitt Anhängen eines Internet-Gateways.

Schritt 7: Erstellen Sie eine Citrix ADC VPX-Instanz mithilfe des AWS EC2-Dienstes.

Führen Sie die folgenden Schritte aus, um eine Citrix ADC VPX-Instanz mithilfe des AWS EC2-Service zu erstellen.

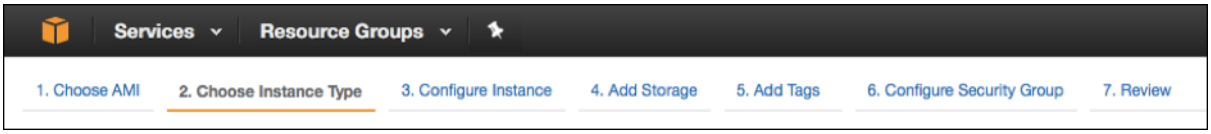
1. Gehen Sie im AWS-Dashboard zu **Compute > EC2 > Launch Instance > AWS Marketplace**.

   Bevor Sie auf **Instanz starten**klicken, stellen Sie sicher, dass Ihre Region korrekt ist, indem Sie die Hinweis überprüfen, die unter **Instanz starten**angezeigt wird.

2. Suchen Sie in der Suchleiste AWS Marketplace mit dem Schlüsselwort Citrix ADC VPX.
3. Wählen Sie die Version aus, die Sie bereitstellen möchten, und klicken Sie dann auf **Auswählen**. Für die Citrix ADC VPX-Version haben Sie folgende Optionen:
   - Eine lizenzierte Version
   - Citrix ADC VPX Express-Appliance (Dies ist eine kostenlose virtuelle Appliance, die über Citrix ADC 12.0 56.20 verfügbar ist.)
   - Bringen Sie Ihr eigenes Gerät

Der Assistent zum Starten von Instanz wird gestartet. Folgen Sie dem Assistenten, um eine Instanz zu erstellen. Der Assistent fordert Sie auf:

- Instanztyp auswählen
- Instanz konfigurieren
- Speicher hinzufügen
- Tags hinzufügen
- Sicherheitsgruppe konfigurieren
- Überprüfen



Schritt 8: Erstellen und Anfügen weiterer Netzwerkschnittstellen.

Erstellen Sie zwei weitere Netzwerkschnittstellen für VIP und SNIP. Weitere Informationen zum Erstellen weiterer Netzwerkschnittstellen finden Sie im Abschnitt Erstellen einer Netzwerkschnittstelle .

Nachdem Sie die Netzwerkschnittstellen erstellt haben, müssen Sie sie an die VPX-Instanz anhängen. Fahren Sie vor dem Anfügen der Schnittstelle die VPX-Instanz herunter, schließen Sie die Schnittstelle an und schalten Sie die Instanz ein. Weitere Informationen zum Anhängen von Netzwerkschnittstellen finden Sie im Abschnitt Anhängen einer Netzwerkschnittstelle beim Starten einer Instanz .

Schritt 9: Zuweisen und Zuordnen von elastischen IPs.

Wenn Sie einer EC2-Instanz eine öffentliche IP-Adresse zuweisen, bleibt sie nur zugewiesen, bis die Instanz gestoppt wird. Danach wird die Adresse wieder in den Pool freigegeben. Wenn Sie die Instanz neu starten, wird eine neue öffentliche IP-Adresse zugewiesen.

Im Gegensatz dazu bleibt eine elastische IP-Adresse (EIP) zugewiesen, bis die Adresse von einer Instanz getrennt wird.

Weisen Sie eine elastische IP für die Management-NIC zu und ordnen Sie sie zu. Weitere Informationen zum Zuweisen und Zuordnen elastischer IP-Adressen finden Sie in den folgenden Themen:

- Zuweisen einer elastischen IP-Adresse
- Eine Elastic IP-Adresse mit einer laufenden Instanz verknüpfen

Mit diesen Schritten wird das Verfahren zum Erstellen einer Citrix ADC VPX-Instanz in AWS abgeschlossen. Es kann einige Minuten dauern, bis die Instanz fertig ist. Überprüfen Sie, ob Ihre Instanz ihre Statusüberprüfungen bestanden hat. Sie können diese Informationen in der Spalte **Statusüberprüfungen** auf der Seite Instanzen anzeigen.

Schritt 10: Verbinden Sie sich mit der VPX-Instanz.

Nachdem Sie die VPX-Instanz erstellt haben, verbinden Sie die Instanz mit der GUI und eines SSH-Clients.

- Grafische Benutzeroberfläche (GUI)

Im Folgenden finden Sie die standardmäßigen Administratoranmeldeinformationen für den Zugriff auf eine Citrix ADC VPX-Instanz.

Benutzername: `nsroot`

Kennwort: Das Standardkennwort für das ns-Root-Konto ist auf die AWS Instanz -ID der Citrix ADC VPX-Instanz festgelegt. Bei Ihrer ersten Anmeldung werden Sie aus Sicherheitsgründen aufgefordert, das Kennwort zu ändern. Nachdem Sie das Kennwort geändert haben, müssen Sie die Konfiguration speichern. Wenn die Konfiguration nicht gespeichert wird und die Instanz neu gestartet wird, müssen Sie sich mit dem Standardkennwort anmelden. Ändern Sie das Kennwort an der Eingabeaufforderung erneut.

- SSH-Client

Wählen Sie in der AWS Management Console die Citrix ADC VPX-Instanz aus, und klicken Sie auf **Verbinden**. Folgen Sie den Anweisungen auf der Seite Mit **Ihrer Instanz verbinden**.

Weitere Informationen zum Bereitstellen einer eigenständigen Citrix ADC VPX-Instanz in AWS mithilfe der AWS-Webkonsole finden Sie unter:

- Szenario: eigenständige Instanz
- Konfigurieren einer Citrix NetScaler VPX-Instanz in AWS mithilfe der Citrix CloudFormation-Vorlage

Konfigurieren einer Citrix ADC VPX-Instanz mithilfe der Citrix CloudFormation-Vorlage

Sie können die von Citrix bereitgestellte CloudFormation-Vorlage verwenden, um den Start der VPX-Instanz zu automatisieren. Die Vorlage bietet Funktionen zum Starten einer einzelnen Citrix ADC VPX-Instanz oder zum Erstellen einer Hochverfügbarkeitsumgebung mit einem Paar von Citrix ADC VPX-Instanzen.

Sie können die Vorlage über AWS Marketplace oder GitHub starten.

Die CloudFormation-Vorlage erfordert eine vorhandene VPC-Umgebung und startet eine VPX-Instanz mit drei elastischen Netzwerkschnittstellen (ENIs). Bevor Sie die CloudFormation-Vorlage starten, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen:

- Eine virtuelle private AWS-Cloud (VPC)
- Drei Subnetze innerhalb der VPC: eines für die Verwaltung, eines für den Clientdatenverkehr und eines für Back-End-Server
- Ein EC2-Schlüsselpaar zum Aktivieren des SSH-Zugriffs auf die Instanz
- Eine Sicherheitsgruppe mit offenen UDP 3003, TCP 3009—3010, HTTP, SSH-Ports

Weitere Informationen zum Vervollständigen der Voraussetzungen finden Sie im Abschnitt Bereitstellen einer Citrix ADC VPX-Instanz auf AWS mit der AWS Web Console oder in der AWS-Dokumentation.

In diesem Video erfahren Sie, wie Sie eine eigenständige Citrix ADC VPX-Instanz mithilfe der im AWS Marketplace verfügbaren Citrix CloudFormation-Vorlage konfigurieren und starten können.

Darüber hinaus konfigurieren und starten Sie eine eigenständige Citrix ADC VPX Express-Instanz mithilfe der in GitHub verfügbaren Citrix CloudFormation-Vorlage:

https://github.com/citrix/citrix-adc-aws-cloudformation/tree/master/templates/standalone/

Eine IAM-Rolle ist für eine eigenständige Bereitstellung nicht obligatorisch. Citrix empfiehlt jedoch, für zukünftige Anforderungen eine IAM-Rolle mit den erforderlichen Berechtigungen zu erstellen und an die Instanz anzuhängen. Die IAM-Rolle stellt sicher, dass die eigenständige Instanz bei Bedarf problemlos mit SR-IOV in einen Hochverfügbarkeitsknoten konvertiert wird.

Weitere Informationen zu den erforderlichen Berechtigungen finden Sie unter Konfigurieren von Citrix ADC VPX-Instanzen für die Verwendung der SR-IOV-Netzwerkschnittstelle.

> Hinweis
> Wenn Sie eine Citrix ADC VPX-Instanz unter AWS mithilfe der AWS-Webkonsole bereitstellen, ist der CloudWatch-Dienst standardmäßig aktiviert. Wenn Sie eine Citrix ADC VPX-Instanz mithilfe der Citrix CloudFormation-Vorlage bereitstellen, ist die Standardoption Ja. Wenn Sie den CloudWatch-Dienst deaktivieren möchten, wählen Sie Nein. Weitere Informationen finden Sie unter Überwachen Ihrer Instanzen mit Amazon CloudWatch

Konfigurieren einer Citrix ADC VPX-Instanz mithilfe der AWS CLI

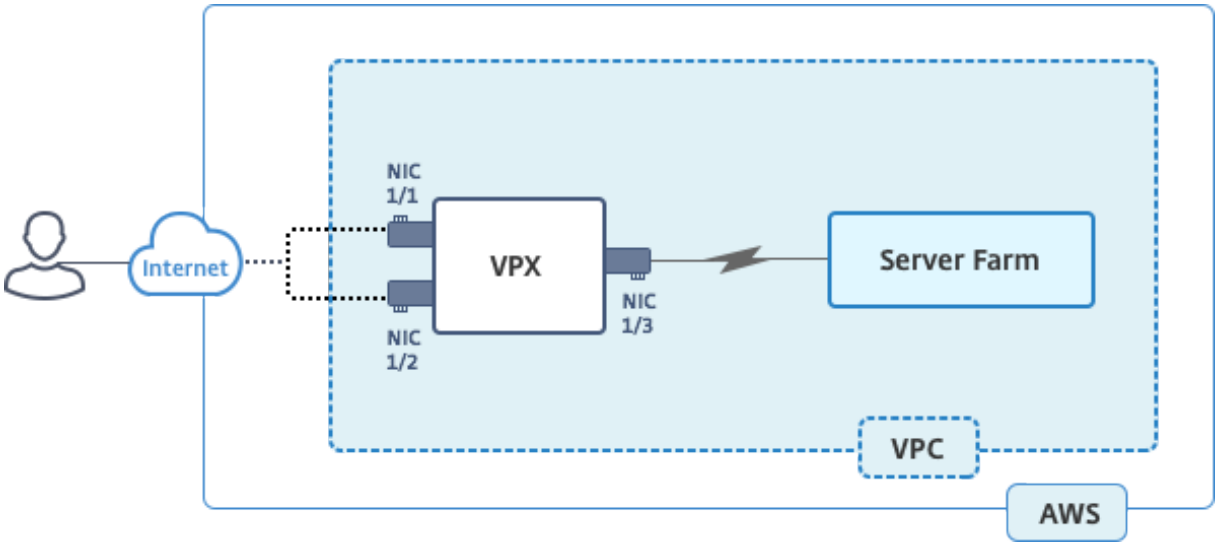
Sie können die AWS CLI zum Starten von Instanzen verwenden. Weitere Informationen finden Sie in der Dokumentation zur AWS-Befehlszeilenschnittstelle.

Szenario: eigenständige Instanz

October 5, 2021

In diesem Szenario wird veranschaulicht, wie eine eigenständige Citrix ADC VPX EC2-Instanz in AWS mithilfe der AWS-GUI bereitgestellt wird. Erstellen Sie eine eigenständige VPX-Instanz mit drei Netzwerkkarten. Die Instanz, die als virtueller Lastausgleichsserver konfiguriert ist, kommuniziert mit Backend-Servern (der Serverfarm). Richten Sie für diese Konfiguration die erforderlichen Kommunikationswege zwischen der Instanz und den Back-End-Servern sowie zwischen der Instanz und den externen Hosts im öffentlichen Internet ein.

Weitere Informationen zum Verfahren zum Bereitstellen einer VPX-Instanz finden Sie unter Bereitstellen einer eigenständigen Citrix ADC VPX-Instanz auf AWS.



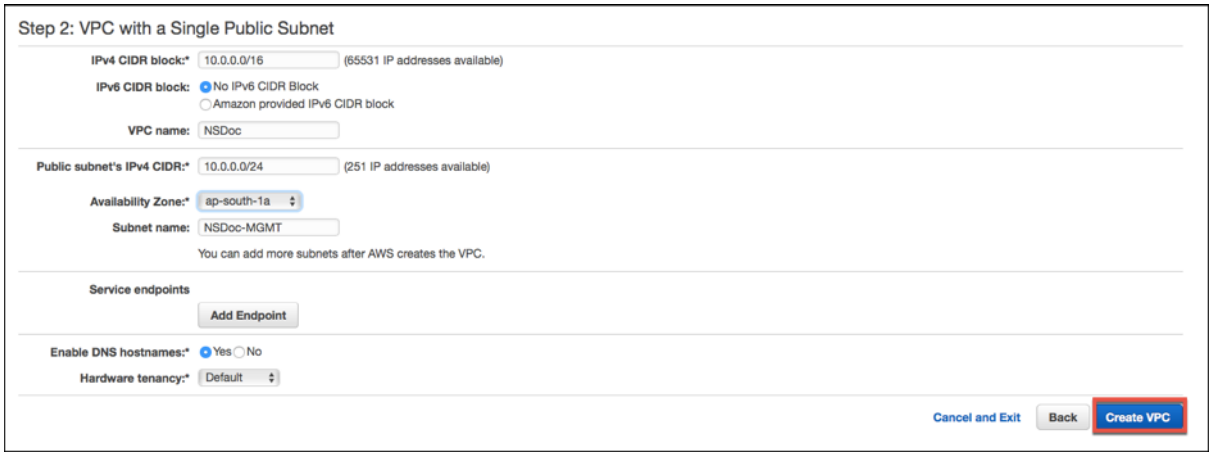
Erstellen Sie drei Netzwerkkarten. Jede Netzwerkkarte kann mit einem Paar von IP-Adressen (öffentlich und privat) konfiguriert werden. Die NICs dienen den folgenden Zwecken.

NIC	Zweck	Verbunden mit
eth0	Bedienen des Management-Datenverkehrs (NSIP)	Eine öffentliche IP-Adresse und eine private IP-Adresse
eth1	Dient zum clientseitigen Datenverkehr (VIP)	Eine öffentliche IP-Adresse und eine private IP-Adresse
eth2	Kommuniziert mit Back-End-Servern (SNIP)	Eine öffentliche IP-Adresse (Private IP-Adresse ist nicht zwingend erforderlich)

Schritt 1: Erstellen einer VPC.

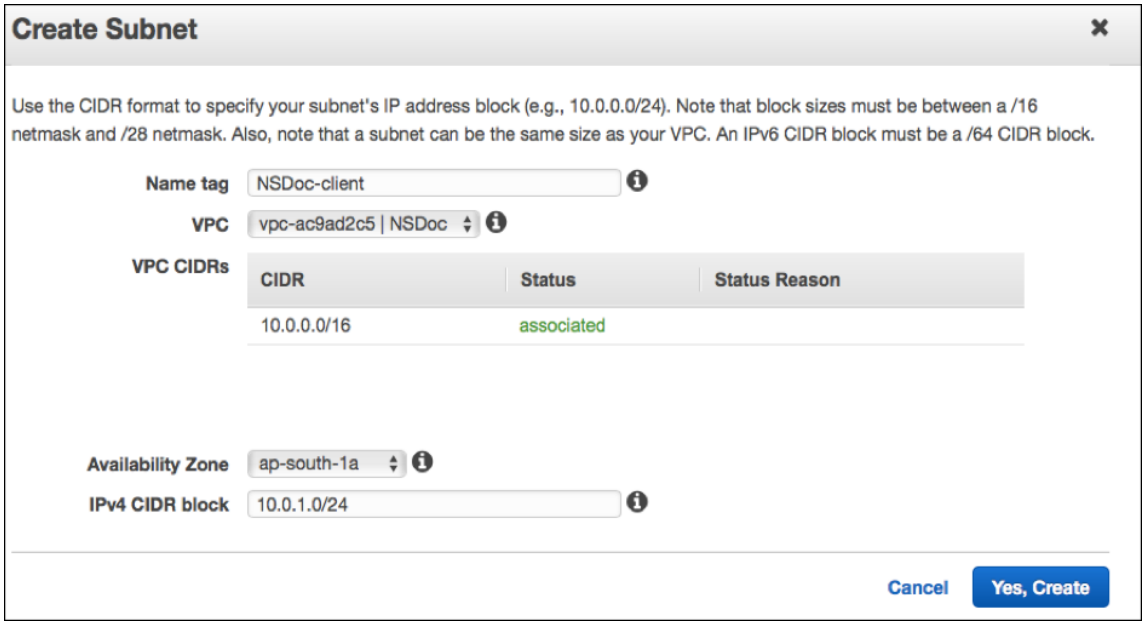
1. Melden Sie sich bei der AWS-Webkonsole an, und navigieren Sie zu **Netzwerk- und Inhaltsbereitstellung** > **VPC**. Klicken Sie auf **VPC-Assistenten starten**.
2. Wählen Sie **VPC mit einem einzelnen öffentlichen Subnetz** aus, und klicken Sie auf **Auswählen**.
3. Legen Sie für dieses Szenario den IP-CIDR-Block auf 10.0.0.0/16 fest.
4. Geben Sie einen Namen für die VPC an.
5. Stellen Sie das öffentliche Subnetz auf 10.0.0.0/24. (Dies ist das Verwaltungsnetzwerk).
6. Wählen Sie eine Verfügbarkeitszone aus.
7. Geben Sie einen Namen für das Subnetz an.

8. Klicken Sie auf **VPC**erstellen.

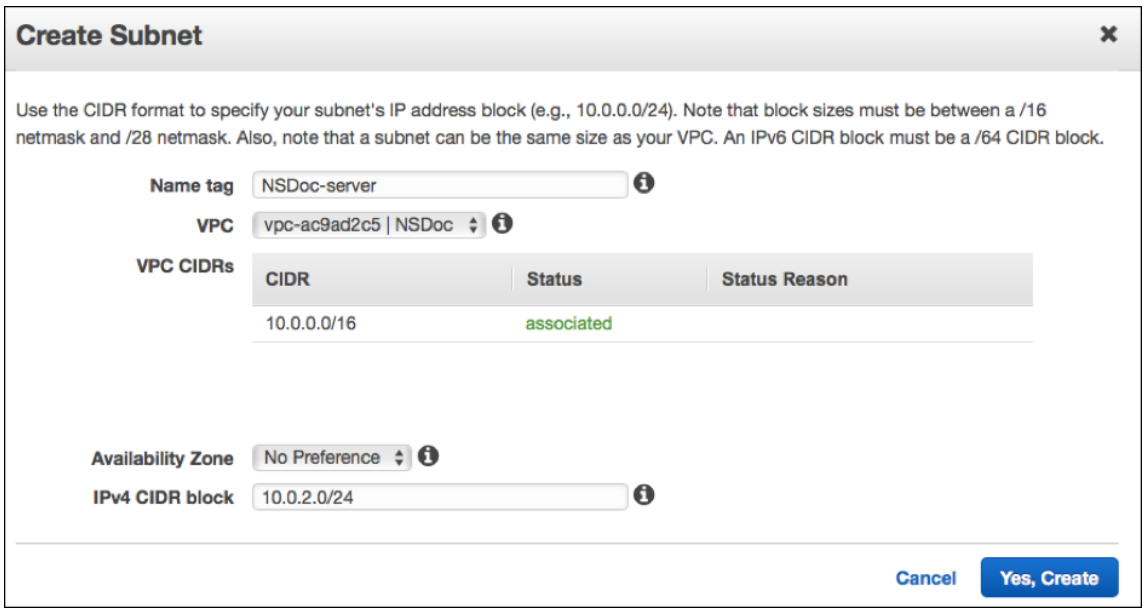


Schritt 2: Erstellen Sie zusätzliche Subnetze.

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets, Subnet erstellen, nachdem Sie die folgenden Details eingegeben haben.
   - Namensschild: Geben Sie einen Namen für Ihr Subnetz an.
   - VPC: Wählen Sie die VPC aus, für die Sie das Subnetz erstellen.
   - Availability Zone: Wählen Sie die Availability Zone, in der Sie die VPC in Schritt 1 erstellt haben.
   - IPv4-CIDR-Block: Geben Sie einen IPv4-CIDR-Block für Ihr Subnetz an. Wählen Sie für dieses Szenario 10.0.1.0/24.

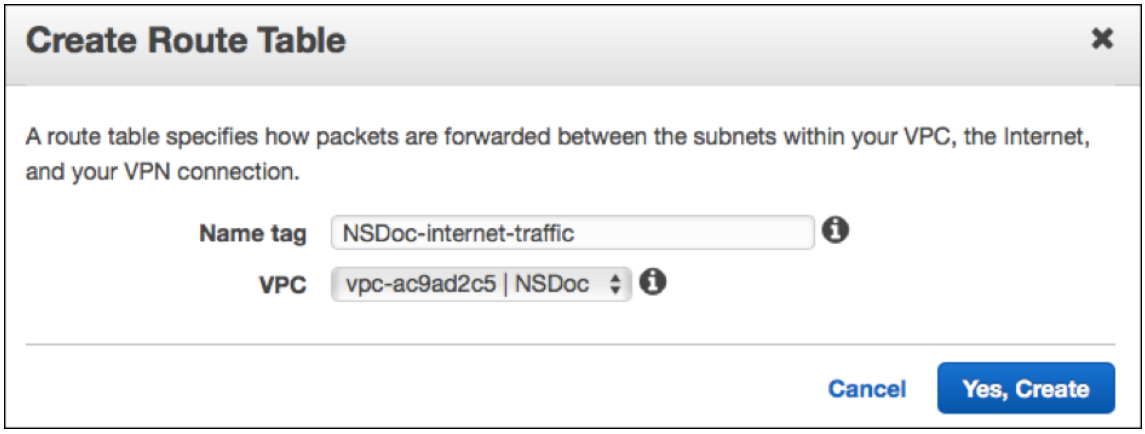


3. Wiederholen Sie die Schritte, um ein weiteres Subnetz für Back-End-Server zu erstellen.



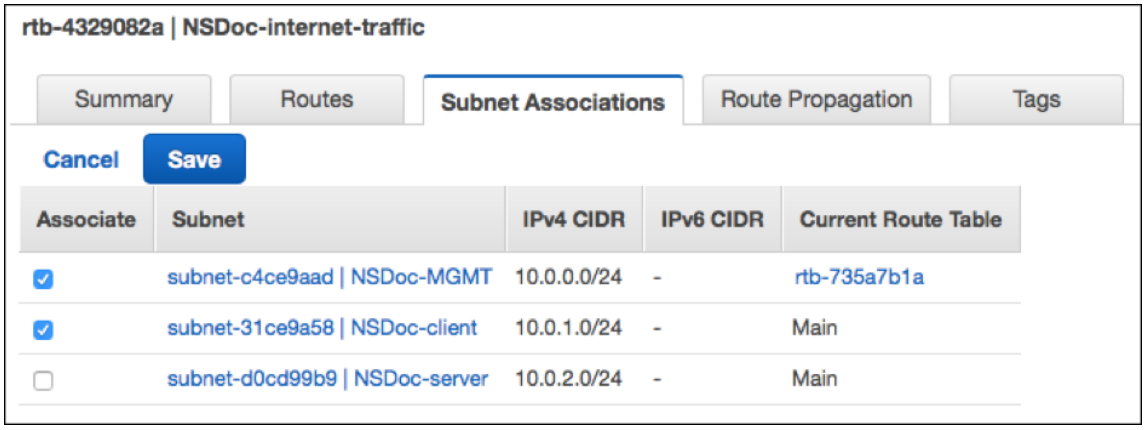
Schritt 3: Erstellen Sie eine Routentabelle.

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich **Routentabellen** > **Routentabelle erstellen**.
3. Fügen Sie im Fenster Routentabelle erstellen einen Namen hinzu, und wählen Sie die VPC aus, die Sie in Schritt 1 erstellt haben.
4. Klicken Sie auf **Yes, Create**.



   Die Routing-Tabelle wird allen Subnetzen zugewiesen, die Sie für diese VPC erstellt haben, so dass das Routing von Datenverkehr von einer Instanz in einem Subnetz eine Instanz in einem anderen Subnetz erreichen kann.

5. Klicken Sie auf Subnetzzuordnungen, und klicken Sie dann auf Bearbeiten.
6. Klicken Sie auf das Verwaltungs- und Client-Subnetz, und klicken Sie auf Speichern. Dadurch wird eine Routentabelle nur für den Internetverkehr erstellt.



7. Klicken Sie auf **Routen > Bearbeiten > Weitere Route hinzufügen**.
8. Fügen Sie im Feld Ziel 0.0.0.0/0 hinzu, und klicken Sie auf das Feld Ziel, um igw- <xxxx> das Internet Gateway auszuwählen, das der VPC-Assistent automatisch erstellt hat.
9. Klicken Sie auf Speichern.

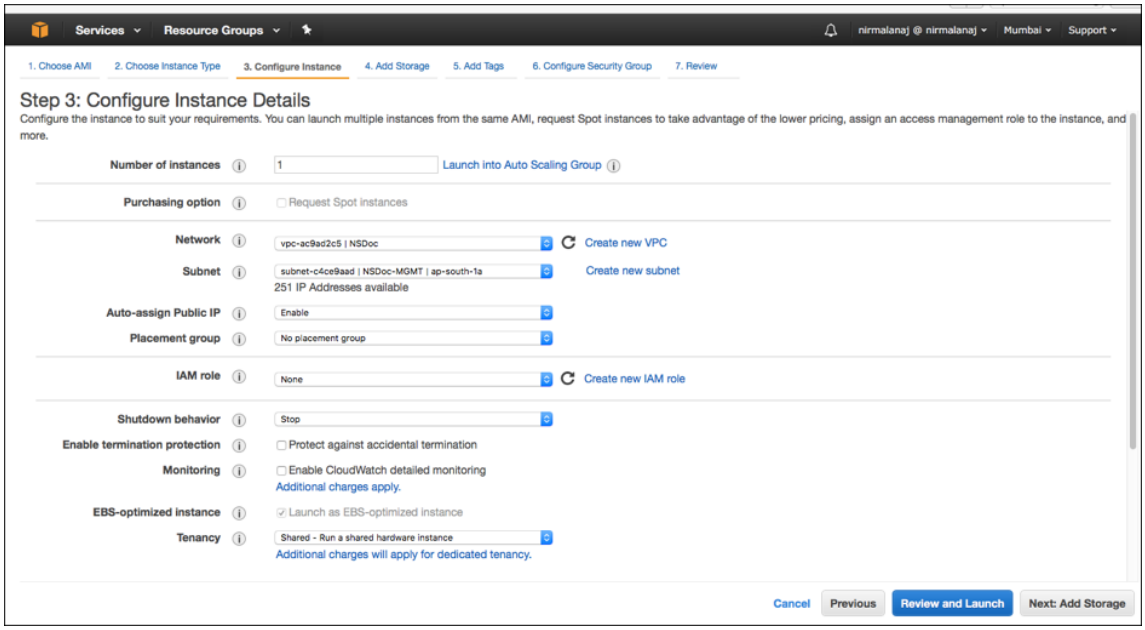
10. Führen Sie die Schritte aus, um eine Routentabelle für serverseitigen Datenverkehr zu erstellen.

Schritt 4: Erstellen einer Citrix ADC VPX-Instanz.

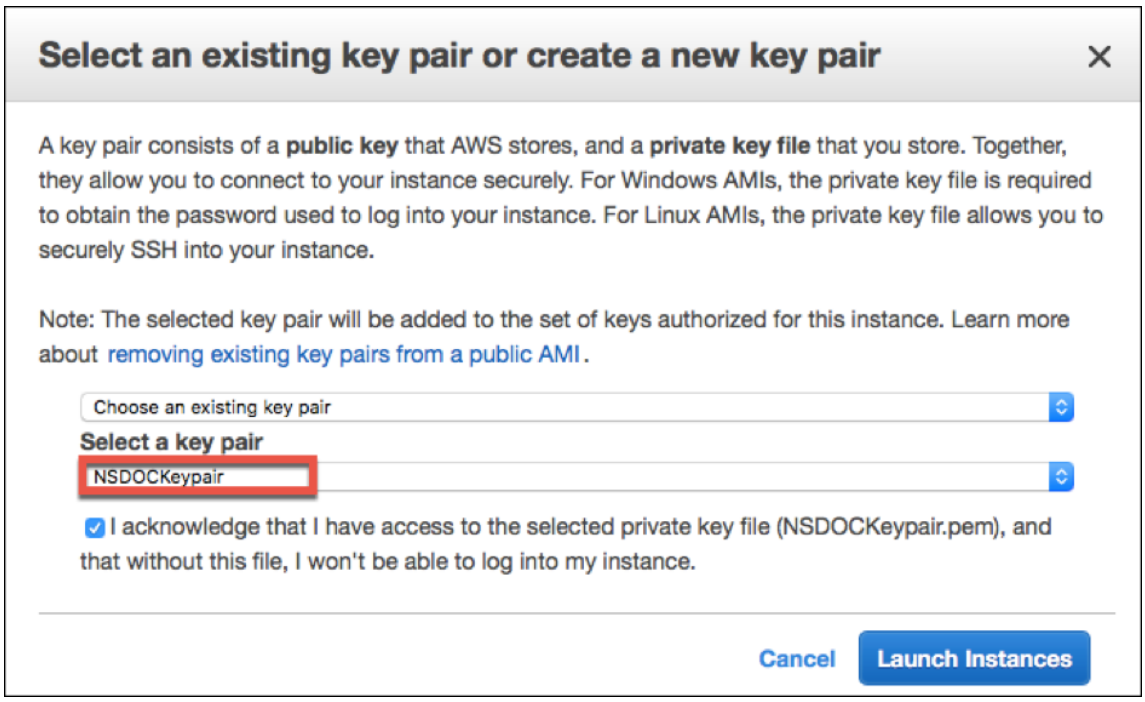
1. Melden Sie sich an der AWS Management Console an, und klicken Sie unter **Compute** auf **EC2** .
2. Klicken Sie auf AWS Marketplace. Geben Sie in der Suchleiste AWS Marketplace Citrix ADC VPX ein, und drücken Sie die Eingabetaste. Die verfügbaren Citrix ADC VPX Editionen werden angezeigt.
3. Klicken **Sie auf Auswählen**, um die gewünschte Citrix ADC VPX Edition auszuwählen. Der EC2-Instanz-Assistent wird gestartet.
4. Wählen Sie auf der Seite **Instanztyp auswählen** die Option **m4. Xlarge** (empfohlen) und klicken Sie auf **Weiter: Instanzdetails konfigurieren**.

5. Wählen Sie auf der Seite Instanzdetails konfigurieren Folgendes aus, und klicken Sie dann auf Weiter: Speicher hinzufügen.

    - Anzahl der Instanzen: 1
    - Netzwerk: die VPC, die in Schritt 1 erstellt wurde
    - Subnetz: das Management-Subnetz
    - Öffentliche IP automatisch zuweisen: Aktivieren



6. Wählen Sie auf der Seite Speicher hinzufügen die Standardoption aus, und klicken Sie auf Weiter: Tags hinzufügen.
7. Fügen Sie auf der Seite Tags hinzufügen einen Namen für die Instanz hinzu, und klicken Sie auf Weiter: Sicherheitsgruppe konfigurieren.
8. Wählen Sie auf der Seite Configure Security Group die Standardoption (die von AWS Marketplace generiert wird und auf den empfohlenen Einstellungen von Citrix Systems basiert) und klicken Sie dann auf **Review and Launch > Launch**.
9. Sie werden aufgefordert, ein vorhandenes Schlüsselpaar auszuwählen oder ein neues Schlüsselpaar zu erstellen. Wählen Sie in der Dropdownliste Schlüsselpaar auswählen das Schlüsselpaar aus, das Sie als Voraussetzung erstellt haben (siehe Abschnitt Voraussetzung).
10. Aktivieren Sie das Kontrollkästchen, um das Schlüsselpaar zu bestätigen, und klicken Sie auf Instanzen starten.



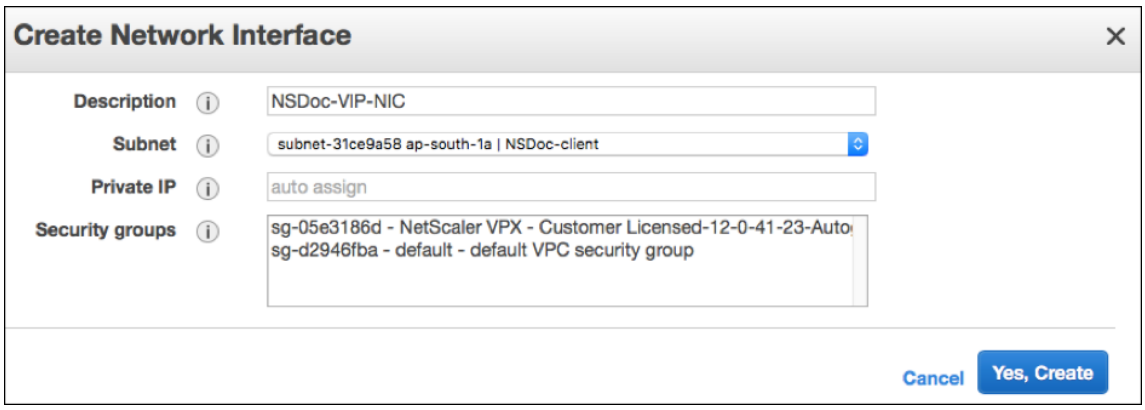
Der Assistent zum Starten von Instanz zeigt den Startstatus an, und die Instanz wird in der Liste der Instanzen angezeigt, wenn sie vollständig gestartet wurde.

Klicken Sie in der Prüfinstanz in der AWS-Konsole auf EC2 > Laufende Instanzen. Wählen Sie die Instanz aus, und fügen Sie einen Namen hinzu. Stellen Sie sicher, dass der Instanzentatus ausgeführt wird und die Statusüberprüfungen abgeschlossen sind.

Schritt 5: Erstellen und Anfügen weiterer Netzwerkschnittstellen.

Wenn Sie die VPC erstellt haben, ist nur eine Netzwerkschnittstelle zugeordnet. Fügen Sie nun zwei weitere Netzwerkschnittstellen zur VPC hinzu, für VIP und SNIP.

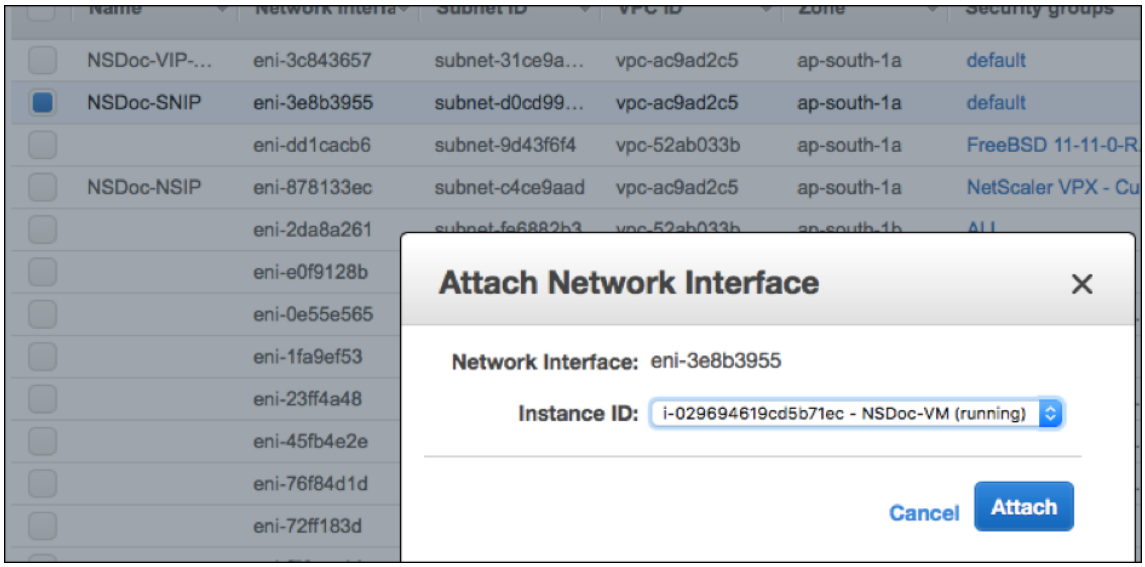
1. Öffnen Sie die Amazon EC2 Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfacesaus.
3. Wählen Sie Netzwerkschnittstelle erstellen.
4. Geben Sie unter Beschreibung einen beschreibenden Namen ein.
5. Wählen Sie unter Subnet das Subnetz aus, das Sie zuvor für den VIP erstellt haben.
6. Lassen Sie für Private IP die Standardoption bei.
7. Wählen Sie für Sicherheitsgruppen die Gruppe aus.
8. Klicken Sie auf **Yes, Create**.



9. Nachdem die Netzwerkschnittstelle erstellt wurde, fügen Sie der Schnittstelle einen Namen hinzu.
10. Wiederholen Sie die Schritte, um eine Netzwerkschnittstelle für serverseitigen Datenverkehr zu erstellen.

Schließen Sie die Netzwerkschnittstellenan:

1. Wählen Sie im Navigationsbereich Network Interfacesaus.
2. Wählen Sie die Netzwerkschnittstelle aus und wählen Sie Anhängen.
3. Wählen Sie im Dialogfeld Netzwerkschnittstelle anhängen die Instanz aus, und wählen Sie Anhängen.



Schritt 6: Bringen Sie eine elastische IP an das NSIP an.

1. Wechseln Sie in der AWS-Verwaltungskonsole zu **NETWORK & SECURITY > Elastic IPs**.
2. Überprüfen Sie, ob verfügbare kostenlose EIP beigefügt werden kann. Wenn keine, klicken Sie auf **Neue Adresse zuweisen**.

3. Wählen Sie die neu zugewiesene IP-Adresse aus und wählen Sie **Aktionen > Adresse zuordnen**.
4. Klicken Sie auf das Optionsfeld **Netzwerkschnittstelle**.
5. Wählen Sie in der Dropdownliste Netzwerkschnittstelle die Verwaltungs-NIC aus.
6. Wählen Sie im Dropdownmenü **Private IP** die von AWS generierte IP-Adresse aus.
7. Aktivieren Sie das Kontrollkästchen **Neuzuordnen**.
8. Klicken Sie auf **Zuordnen**.

Zugriff auf die VPX-Instanz:

Nachdem Sie eine eigenständige Citrix ADC VPX Instanz mit drei Netzwerkkarten konfiguriert haben, melden Sie sich bei der VPX-Instanz an, um die Citrix ADC-seitige Konfiguration abzuschließen. Verwendung der folgenden Optionen:

- GUI: Geben Sie die öffentliche IP der Management-NIC im Browser ein. Melden Sie sich an, indem Sie `nsroot` als Benutzernamen und die Instanz-ID (i-0c1ffe1d987817522) als Kennwort verwenden.

> Hinweis
>
> Bei Ihrer ersten Anmeldung werden Sie aus Sicherheitsgründen aufgefordert, das Kennwort zu ändern. Nachdem Sie das Kennwort geändert haben, müssen Sie die Konfiguration speichern. Wenn die Konfiguration nicht gespeichert wird und die Instanz neu gestartet wird, müssen Sie sich mit dem Standardkennwort anmelden. Ändern Sie das Kennwort erneut an der Eingabeaufforderung und speichern Sie die Konfiguration.

- SSH: Öffnen Sie einen SSH-Client und geben Sie ein:

```
ssh -i \<location of your private key\> ns root@\<public DNS of the instance
\>
```

Um den öffentlichen DNS zu finden, klicken Sie auf die Instanz und dann auf **Verbinden**.

Weitere Informationen:

- Informationen zum Konfigurieren der IP-Adressen im Besitz von Citrix ADC (NSIP, VIP und SNIP) finden Sie unter Konfigurieren von IP-Adressen im Besitz von Citrix ADC.
- Sie haben eine BYOL-Version der Citrix ADC VPX Appliance konfiguriert. Weitere Informationen finden Sie im VPX-Lizenzierungshandbuch unterhttp://support.citrix.com/article/CTX122426

Download einer Citrix ADC VPX-Lizenz

October 5, 2021

Nach dem Start der Citrix ADC VPX-kundenlizenzierten Instanz vom AWS-Marktplatz ist eine Lizenz erforderlich. Weitere Informationen zur VPX-Lizenzierung finden Sie unter Übersicht über die Lizenzierung.

Sie müssen:

1. Verwenden Sie das Lizenzierungsportal innerhalb der Citrix Website, um eine gültige Lizenz zu generieren.
2. Laden Sie die Lizenz auf die Instanz hoch.

Wenn es sich um eine **kostenpflichtige** Marketplace-Instanz handelt, müssen Sie keine Lizenz installieren. Der richtige Funktionsumfang und die richtige Leistung werden automatisch aktiviert.

Wenn Sie eine Citrix ADC VPX-Instanz mit einer Modellnummer über VPX 5000 verwenden, ist der Netzwerkdurchsatz möglicherweise nicht der gleiche wie in der Lizenz der Instanz angegeben. Andere Funktionen wie SSL-Durchsatz und SSL-Transaktionen pro Sekunde können jedoch verbessert werden.

Im `c4.8xlarge` Instanztyp wird eine 5-Gbit/s-Netzwerkbandbreite beobachtet.

So migrieren Sie das AWS-Abonnement auf BYOL

In diesem Abschnitt wird das Verfahren zur Migration vom AWS-Abonnement auf Bring your own License (BYOL) beschrieben, und umgekehrt.

Führen Sie die folgenden Schritte aus, um ein AWS-Abonnement auf BYOL zu migrieren:

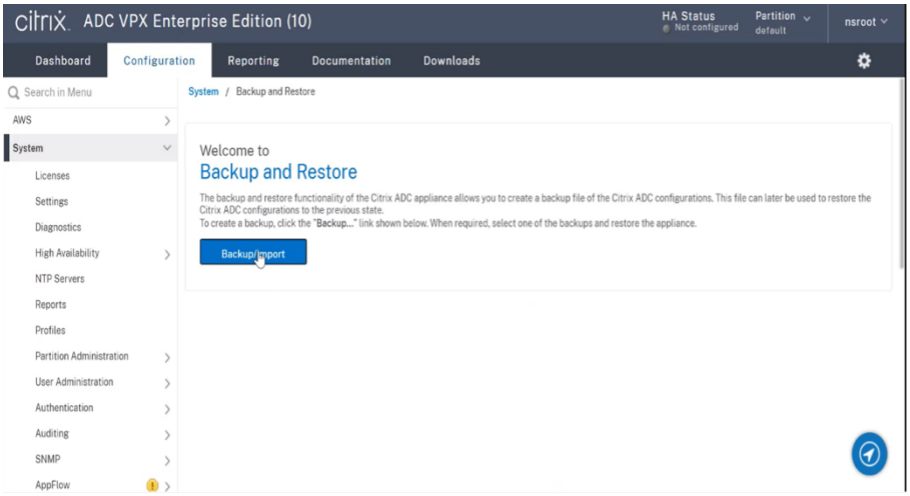
> Hinweis:
>
> Der **Schritt 2** und der **Schritt 3** werden auf der Citrix ADC VPX-Instanz ausgeführt, und alle anderen Schritte werden im AWS-Portal ausgeführt.

1. Erstellen Sie eine BYOL EC2-Instanz mit Citrix ADC VPX - Kundenlizenziert in derselben Availability Zone wie die alte EC2-Instanz, die dieselbe Sicherheitsgruppe, IAM-Rolle und das gleiche Subnetz hat. Die neue EC2-Instanz muss nur eine ENI-Schnittstelle haben.

2. Gehen Sie folgendermaßen vor, um die Daten auf der alten EC2-Instanz mit der Citrix ADC GUI zu sichern.

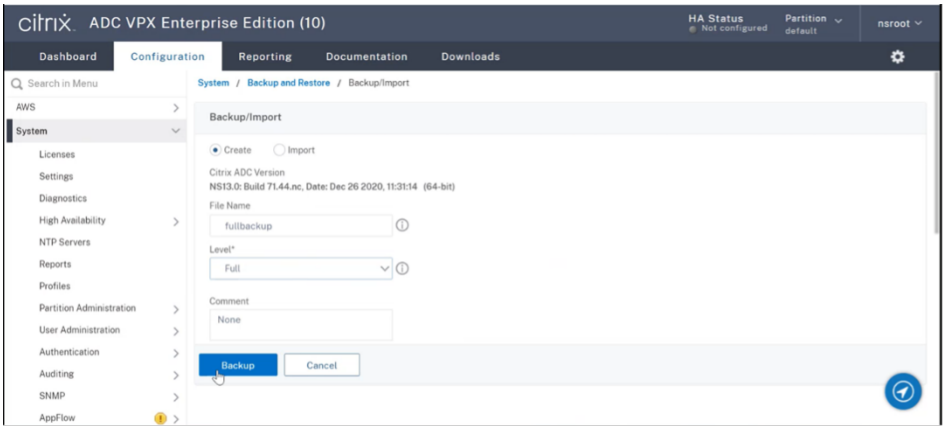
   a) Navigieren Sie zu **System > Sichern und Wiederherstellen**.

   b) Klicken Sie auf der **Begrüßungsseite** auf **Backup/Importieren**, um den Vorgang zu starten.

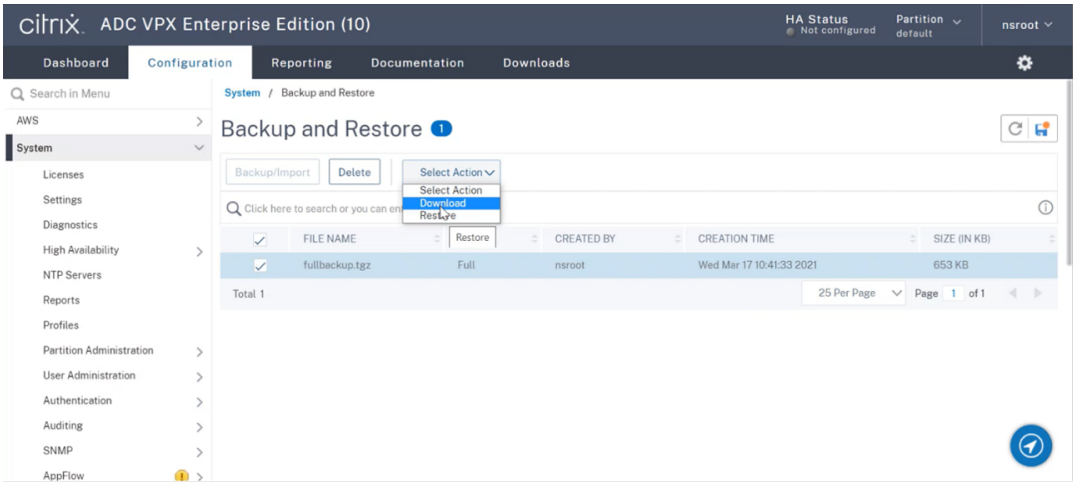


   c) Geben Sie auf der Seite **“Backup/Import** “ die folgenden Details ein:

   - **Name** — Name der Sicherungsdatei.
   - **Level** — Wählen Sie die Backup-Level als **Full**aus.
   - **Kommentar** — Geben Sie eine kurze Beschreibung des Backup an.



   d) Klicken Sie auf **Backup**. Sobald die Backup abgeschlossen ist, können Sie die Datei auswählen und auf Ihren lokalen Computer herunterladen.

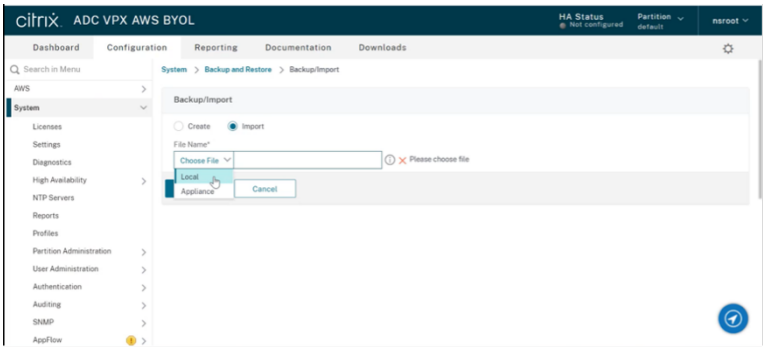


3. Gehen Sie folgendermaßen vor, um die Daten auf der neuen EC2-Instanz mit der Citrix ADC GUI wiederherzustellen:

   a) Navigieren Sie zu **System > Sichern und Wiederherstellen**.

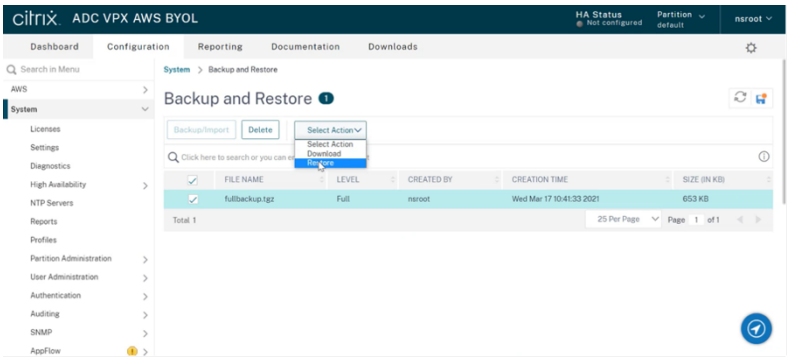
   b) Klicken Sie auf **Backup/Import**, um den Vorgang zu starten.

   c) Wählen Sie die Option **Importieren** aus und laden Sie die Sicherungsdatei hoch.

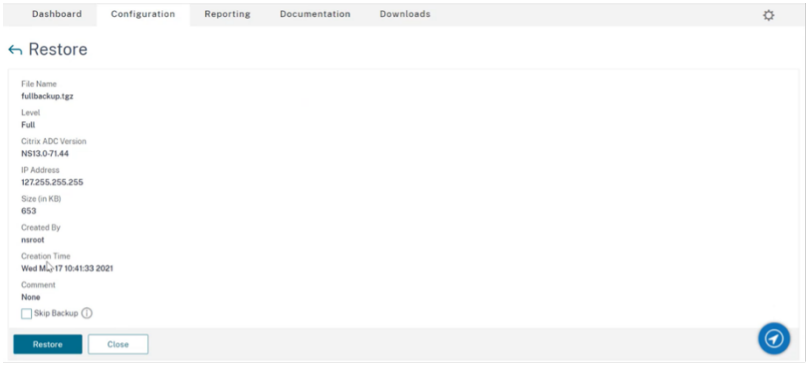


   d) Wählen Sie die Datei aus.

   e) **Wählen Sie im Dropdownmenü Aktion** auswählen die Option **Wiederherstellen**aus.



   f) Überprüfen Sie auf der Seite **Wiederherstellen** die Dateidetails und klicken Sie auf **Wiederherstellen**.



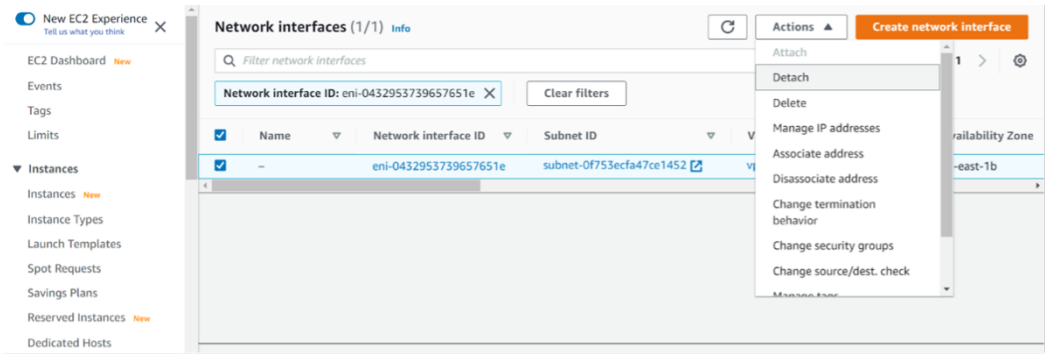
g) Starten Sie nach der Wiederherstellung die EC2-Instanz neu.

4. Verschieben Sie alle Schnittstellen (mit Ausnahme der Verwaltungsschnittstelle, an die die NSIP-Adresse gebunden ist) von der alten EC2-Instanz zur neuen EC2-Instanz. Gehen Sie folgendermaßen vor, um eine Netzwerkschnittstelle von einer EC2-Instanz in eine andere zu verschieben:

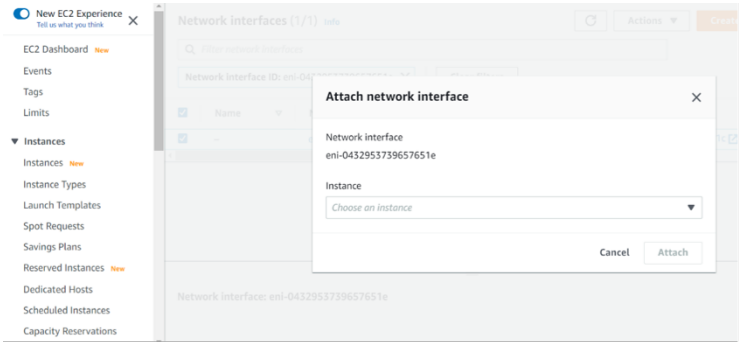
   a) Stoppen Sie im **AWS-Portal**sowohl die alte als auch die neue EC2-Instanz.

   b) Navigieren Sie zu **Netzwerkschnittstellen**und wählen Sie die Netzwerkschnittstelle aus, die an die alte EC2-Instanz angeschlossen ist.

   c) Trennen Sie die EC2-Instanz, indem Sie auf **Aktionen > Trennen**klicken.



   d) Schließen Sie die Netzwerkschnittstelle an die neue EC2-Instanz an, indem Sie auf **Aktionen > Anhängen**klicken. Geben Sie den Namen der EC2-Instanz ein, an den die Netzwerkschnittstelle angeschlossen werden muss.



e) Führen Sie den **Schritt 1** bis **Schritt 4** für alle anderen angehängten Schnittstellen aus. Vergewissern Sie sich, dass Sie die Reihenfolge befolgen und die Reihenfolge der Schnittstelle beibehalten. Das heißt, trennen Sie zuerst Schnittstelle 2 und schließen Sie es an, trennen Sie dann Schnittstelle 3 und schließen Sie es an und so weiter.

5. Sie können die Verwaltungsschnittstelle nicht von einer alten EC2-Instanz trennen. Verschieben Sie also alle sekundären IP-Adressen (falls vorhanden) auf der Verwaltungsschnittstelle (primäre Netzwerkschnittstelle) der alten EC2-Instanz auf die neue EC2-Instanz. Gehen Sie folgendermaßen vor, um eine IP-Adresse von einer Schnittstelle in eine andere zu verschieben:

   a) Stellen Sie im **AWS-Portal**sicher, dass sich sowohl die alten als auch die neue EC2-Instanzen im Status " **Stop** " befinden.

   b) Navigieren Sie zu **Netzwerkschnittstellen**und wählen Sie die Verwaltungsnetzwerkschnittstelle aus, die an die alte EC2-Instanz angeschlossen ist.

   c) Klicken Sie auf **Aktionen > IP-Adresse verwalten**und notieren Sie sich alle sekundären IP-Adressen (falls vorhanden).

   d) Navigieren Sie zur Verwaltungsnetzwerkschnittstelle oder zur primären Schnittstelle der neuen EC2-Instanz.

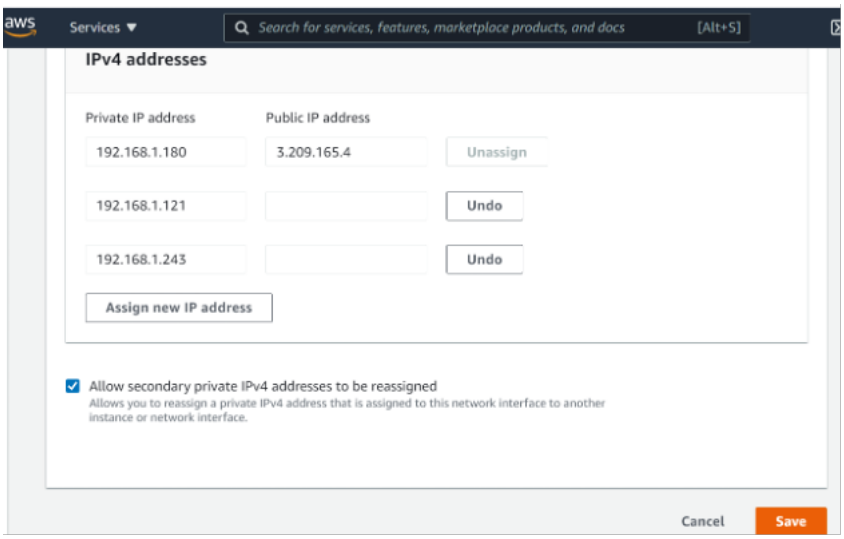
   e) Klicken Sie auf **Aktionen > IP-Adressen verwalten**.

   f) Klicken Sie unter **IPv4-Adressen**auf **Neue IP-Adresse zuweisen**.

   g) Geben Sie die IP-Adressen ein, die im **Schritt 3**vermerkt sind.

   h) Aktivieren **Sie das Kontrollkästchen Neuzuweisung sekundärer privater IP-Adressen** zulassen.

   i) Klicken Sie auf **Speichern**.



6. Starten Sie die neue EC2-Instanz und überprüfen Sie die Konfiguration. Nachdem die gesamte Konfiguration verschoben wurde, können Sie die alte EC2-Instanz gemäß Ihren Anforderungen löschen oder behalten.
7. Wenn eine EIP-Adresse an die NSIP-Adresse der alten EC2-Instanz angehängt ist, verschieben Sie die alte Instanz-NSIP-Adresse an die NSIP-Adresse der neuen Instanz.
8. Wenn Sie zur alten Instanz zurückkehren möchten, führen Sie die gleichen Schritte in entgegengesetzter Weise zwischen der alten und der neuen Instanz aus.
9. Nachdem Sie von der Abonnementinstanz zur BYOL-Instanz umgezogen sind, ist eine Lizenz erforderlich. Gehen Sie folgendermaßen vor, um eine Lizenz zu installieren:
    - Verwenden Sie das Lizenzportal auf der Citrix Website, um eine gültige Lizenz zu generieren.
    - Laden Sie die Lizenz auf die Instanz hoch. Weitere Informationen finden Sie unter VPX ADC - Installieren einer neuen Lizenz.

> Hinweis:
>
> Wenn Sie die BYOL-Instanz auf eine Abonnementinstanz (kostenpflichtige Marketplace-Instanz) verschieben, müssen Sie die Lizenz nicht installieren. Der richtige Funktionsumfang und die richtige Leistung werden automatisch aktiviert.

Einschränkungen

Die Verwaltungsschnittstelle kann nicht auf die neue EC2-Instanz verschoben werden. Citrix empfiehlt daher, die Verwaltungsschnittstelle manuell zu konfigurieren. Weitere Informationen finden Sie unter **Schritt 5** des vorherigen Verfahrens. Eine neue EC2-Instanz wird mit dem genauen Replikat der alten EC2-Instanz erstellt, aber nur die NSIP-Adresse hat eine neue IP-Adresse.

Lastausgleichsserver in verschiedenen Availability Zones

October 5, 2021

Eine VPX-Instanz kann zum Lastenausgleich von Servern verwendet werden, die in derselben Availability Zone ausgeführt werden, oder in:

- Eine andere Availability Zone (AZ) in derselben AWS VPC
- Eine andere AWS-Region
- AWS EC2 in einer VPC

Um es einer VPX-Instanz zu ermöglichen, dass Server, die außerhalb der AWS VPC ausgeführt werden, in der sich die

VPX-Instanz befindet, ausgeführt werden, konfigurieren Sie die Instanz so, dass sie EIPs zum Weiterleiten des Datenverkehrs über das Internet-Gateway verwendet:

1. Konfigurieren Sie ein SNIP auf der Citrix ADC VPX-Instanz mithilfe der Citrix ADC CLI oder der GUI.
2. Aktivieren Sie das Routing von Datenverkehr aus der AZ, indem Sie ein öffentliches Subnetz für den serverseitigen Datenverkehr erstellen.
3. Fügen Sie der Routingtabelle mithilfe der AWS GUI-Konsole eine Internet-Gateway -Route hinzu.
4. Ordnen Sie die Routingtabelle, die Sie aktualisiert haben, dem serverseitigen Subnetz zu.
5. Ordnen Sie eine EIP der serverseitigen privaten IP-Adresse zu, die einer Citrix ADC SNIP-Adresse zugeordnet ist.

Funktionsweise der Hochverfügbarkeit in AWS

October 5, 2021

Sie können zwei Citrix ADC VPX -Instanzen in AWS als aktives und passives High Availability (HA) -Paar konfigurieren. Wenn Sie eine Instanz als primären Knoten und die andere als sekundären Knoten konfigurieren, akzeptiert der primäre Knoten Verbindungen und verwaltet Server. Der sekundäre Knoten überwacht den primären. Wenn der primäre Knoten aus irgendeinem Grund keine Verbindungen akzeptieren kann, übernimmt der sekundäre Knoten die Übernahme.

In AWS werden die folgenden Bereitstellungstypen für VPX-Instanzen unterstützt:

- Hohe Verfügbarkeit innerhalb derselben Zone
- Hohe Verfügbarkeit über verschiedene Zonen hinweg

> **Hinweis:**
>
> Stellen Sie sicher, dass beide Citrix ADC VPX Instanzen mit IAM-Rollen verknüpft und dem NSIP mit der Elastic IP (EIP) -Adresse zugewiesen sind. Sie müssen kein EIP für NSIP zuweisen, wenn der NSIP über die NAT-Instanz ins Internet gelangen kann.

Hohe Verfügbarkeit innerhalb derselben Zonen

In einer Hochverfügbarkeitsbereitstellung innerhalb derselben Zonen müssen beide VPX-Instanzen ähnliche Netzwerkkonfigurationen haben.

Folgen Sie diesen beiden Regeln:

Regel 1. Jede NIC auf einer VPX-Instanz muss sich im selben Subnetz wie die entsprechende NIC in der anderen VPX befinden. Beide Instanzen müssen Folgendes haben:

- Verwaltungsschnittstelle im selben Subnetz (als Management-Subnetz bezeichnet)

- Clientschnittstelle im selben Subnetz (als Client-Subnetz bezeichnet)
- Serverschnittstelle im selben Subnetz (als Server-Subnetz bezeichnet)

Regel 2. Die Reihenfolge der Mgmt-NIC, der Client-NIC und der Server-NIC auf beiden Instanzen muss identisch sein.
Beispielsweise wird das folgende Szenario nicht unterstützt.

VPX-Instanz 1

NIC 0:
Verwaltungs-NIC 1:
Client-NIC 2: Server

VPX-Instanz 2

NIC 0: Verwaltung

NIC 1: Server

NIC 2: Client

In diesem Szenario befindet sich NIC 1 von Instanz 1 im Clientsubnetz, während NIC 1 von Instanz 2 im Serversubnetz ist. Damit HA funktioniert, muss sich NIC 1 der beiden Instanzen entweder im Client-Subnetz oder im Serversubnetz befinden.

Ab 13.0 41.xx kann eine hohe Verfügbarkeit erreicht werden, indem sekundäre private IP-Adressen migriert werden, die an die Netzwerkkarten (Client- und serverseitige Netzwerkkarten) des primären HA-Knotens nach dem Failover angeschlossen sind. In dieser Bereitstellung gilt:

- Beide VPX-Instanzen haben die gleiche Anzahl von Netzwerkkarten und Subnetzzuordnung gemäß der NIC-Aufzählung.
- Jede VPX-NIC hat eine zusätzliche private IP-Adresse, mit Ausnahme der ersten NIC - die der Verwaltungs-IP-Adresse entspricht. Die zusätzliche private IP-Adresse wird als primäre private IP-Adresse in der AWS-Webkonsole angezeigt. In unserem Dokument verweisen wir auf diese zusätzliche IP-Adresse als Dummy-IP-Adresse).
- Die Dummy-IP-Adressen dürfen auf der Citrix ADC Instanz nicht als VIP und SNIP konfiguriert werden.
- Andere sekundäre private IP-Adressen müssen bei Bedarf erstellt und als VIP und SNIP konfiguriert werden.
- Bei Failover sucht der neue Primärknoten nach konfigurierten SNIPs und VIPs und verschiebt sie von NICs, die an den vorherigen primären Knoten angeschlossen sind, auf die entsprechenden Netzwerkkarten auf dem neuen Primärbereich.
- Citrix ADC Instanzen erfordern IAM-Berechtigungen, damit HA funktioniert. Fügen Sie der IAM-Richtlinie, die jeder Instanz hinzugefügt wurde, die folgenden IAM-Berechtigungen hinzu.


```
”iam:GetRole”
”ec2:DescribeInstances”
”ec2:DescribeNetworkInterfaces”
”ec2:AssignPrivateIpAddresses”
```

> Hinweis:`unassignPrivateIpAddress` ist nicht erforderlich.

Diese Methode ist schneller als die Legacy-Methode. Bei der älteren Methode hängt HA von der Migration elastischer AWS-Netzwerkschnittstellen des primären Knotens zum sekundären Knoten ab.

Für eine Legacy-Methode sind die folgenden Richtlinien erforderlich:

```
”iam:GetRole”
”ec2:DescribeInstances”
”ec2:DescribeAddresses”
”ec2:AssociateAddress”
”ec2:DisassociateAddress”
```

Weitere Informationen finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares in AWS.

Hohe Verfügbarkeit über verschiedene Zonen hinweg

Sie können zwei Citrix ADC VPX -Instanzen in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS Availability Zones als aktives und passives High Availability Pair im Independent Network Configuration (INC) -Modus konfigurieren. Beim Failover migriert die EIP (Elastic IP) des VIP der primären Instanz auf die sekundäre, die als neue primäre Instanz übernommen wird. Im Failover-Prozess wird die AWS-API:

- Überprüft die virtuellen Server, die `IPSets` an sie angeschlossen sind.
- Sucht die IP-Adresse mit einer zugeordneten öffentlichen IP-Adresse aus den beiden IP-Adressen, die der virtuelle Server überwacht. Eine, die direkt an den virtuellen Server angeschlossen ist, und eine, die über den IP-Satz verbunden ist.
- Verknüpfen Sie die öffentliche IP (EIP) mit der privaten IP, die zum neuen primären VIP gehört.

Für HA über verschiedene Zonen hinweg sind folgende Richtlinien erforderlich:

```
”iam:GetRole”
”ec2:DescribeInstances”
”ec2:DescribeAddresses”
”ec2:AssociateAddress”
”ec2:DisassociateAddress”
```

Weitere Informationen finden Sie unter Hochverfügbarkeit in AWS Availability Zones.

Bevor Sie mit der Bereitstellung beginnen

Bevor Sie eine HA-Bereitstellung in AWS starten, lesen Sie das folgende Dokument:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien
- Bereitstellen einer Citrix ADC VPX-Instanz auf AWS
- Hohe Verfügbarkeit

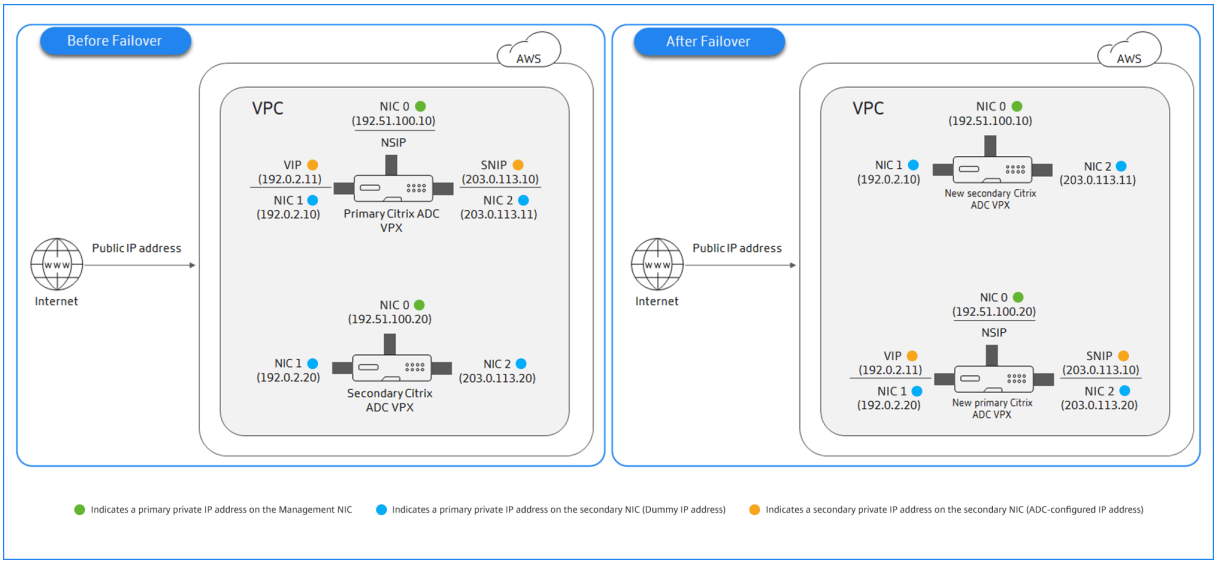
Stellen Sie ein VPX-HA-Paar in derselben AWS-Verfügbarkeitszone bereit

January 25, 2022

Sie können zwei Citrix ADC VPX-Instanzen auf AWS als Hochverfügbarkeitspaar (HA) in derselben AWS-Zone konfigurieren, in der sich beide VPX-Instanzen im selben Subnetz befinden. HA wird erreicht, indem sekundäre private IP-Adressen, die an die NICs (client- und serverseitige NICs) des primären HA-Knotens angeschlossen sind, nach einem Failover zum sekundären HA-Knoten migriert. Alle Elastic IP-Adressen, die mit den sekundären privaten IP-Adressen verknüpft sind, werden ebenfalls migriert.

Die folgende Abbildung zeigt ein HA-Failoverszenario durch Migration sekundärer privater IP-Adressen.

Abbildung 1. Ein Citrix ADC VPX HA-Paar auf AWS mit privater IP-Migration



Bevor Sie mit Ihrem Dokument beginnen, lesen Sie die folgenden Dokumente:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien
- Bereitstellen einer Citrix ADC VPX-Instanz auf AWS

- Hohe Verfügbarkeit

So stellen Sie ein VPX-HA-Paar in derselben Zone bereit

Hier ist eine Zusammenfassung der Schritte zum Bereitstellen eines VPX-HA-Paars in derselben Zone:

1. Erstellen Sie zwei VPX-Instanzen auf AWS mit jeweils drei Netzwerkkarten
2. Weisen Sie VIP und SNIP des primären Knotens eine sekundäre private AWS IP-Adresse zu
3. Konfigurieren von VIP und SNIP auf dem primären Knoten mit sekundären privaten IP-Adressen von AWS
4. Konfigurieren der HA auf beiden Knoten

Schritt 1. Erstellen Sie zwei VPX-Instanzen (primäre und sekundäre Knoten) mit derselben VPC mit jeweils drei NICs (Ethernet 0, Ethernet 1, Ethernet 2)

Befolgen Sie die Schritte unter Bereitstellen einer Citrix ADC VPX-Instanz auf AWS mithilfe der AWS-Webkonsole.

Schritt 2. Weisen Sie auf dem primären Knoten sekundäre private IP-Adressen für Ethernet 1 (Client-IP oder VIP) und Ethernet 2 (Backend-Server-IP oder SNIP) zu

Die AWS-Konsole weist den konfigurierten NICs automatisch primäre private IP-Adressen zu. Weisen Sie VIP und SNIP mehr private IP-Adressen zu, die als sekundäre private IP-Adressen bekannt sind.

Gehen Sie folgendermaßen vor, um einer Netzwerkschnittstelle eine sekundäre private IPv4-Adresse zuzuweisen:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Netzwerkschnittstellen aus, und wählen Sie dann die an die Instanz angeschlossene Netzwerkschnittstelle aus.
3. Wählen Sie Aktionen, IP-Adressen verwalten.
4. Wählen Sie unter IPv4-Adressen die Option Neue IP zuweisen.
5. Geben Sie eine bestimmte IPv4-Adresse ein, die innerhalb des Subnetzbereichs der Instanz liegt, oder lassen Sie das Feld leer, damit Amazon eine IP-Adresse für Sie auswählen kann.
6. (Optional) Wählen Sie Neuzuweisung zulassen, damit die sekundäre private IP-Adresse neu zugewiesen werden kann, wenn sie bereits einer anderen Netzwerkschnittstelle zugewiesen ist.
7. Wählen Sie Ja, Aktualisieren.

Unter der Instanzbeschreibung werden die zugewiesenen sekundären privaten IP-Adressen angezeigt.

Schritt 3. Konfigurieren von VIP und SNIP auf dem primären Knoten mit sekundären privaten IP-Adressen

Greifen Sie mit SSH auf den primären Knoten zu. Öffnen Sie einen SSH-Client und geben Sie ein:

```
ssh -i <location of your private key> nsroot@<public DNS of the
   instance>
<!--NeedCopy-->
```

Konfigurieren Sie als Nächstes VIP und SNIP.

Geben Sie für VIP Folgendes ein:

```
add ns ip <IPAddress> <netmask> -type <type>
<!--NeedCopy-->
```

Geben Sie für SNIP Folgendes ein:

```
add ns ip <IPAddress> <netmask> -type SNIP
<!--NeedCopy-->
```

Tippen Sie `save config` zum Speichern ein.

Um die konfigurierten IP-Adressen anzuzeigen, geben Sie den folgenden Befehl ein:

```
show ns ip
<!--NeedCopy-->
```

Weitere Informationen finden Sie in den folgenden Themen:

- Konfigurieren und Verwalten virtueller IP-Adressen (VIP)
- Configuring the NSIP address

Schritt 4: Konfigurieren von HA auf beiden Instanzen

Öffnen Sie auf dem primären Knoten einen Shell-Client und geben Sie den folgenden Befehl ein:

```
add ha node <id> <private IP address of the management NIC of the
   secondary node>
```



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

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein:

```
add ha node <id> < private IP address of the management NIC of the
    primary node >
<!--NeedCopy-->
```

Geben Sie `save config` ein, um die Konfiguration zu speichern.

Um die konfigurierten HA-Knoten anzuzeigen, geben Sie ein `show ha node`.

Nach dem Failover werden die sekundären privaten IP-Adressen, die auf dem vorherigen primären Knoten als VIP und SNIP konfiguriert sind, auf den neuen primären Knoten migriert.

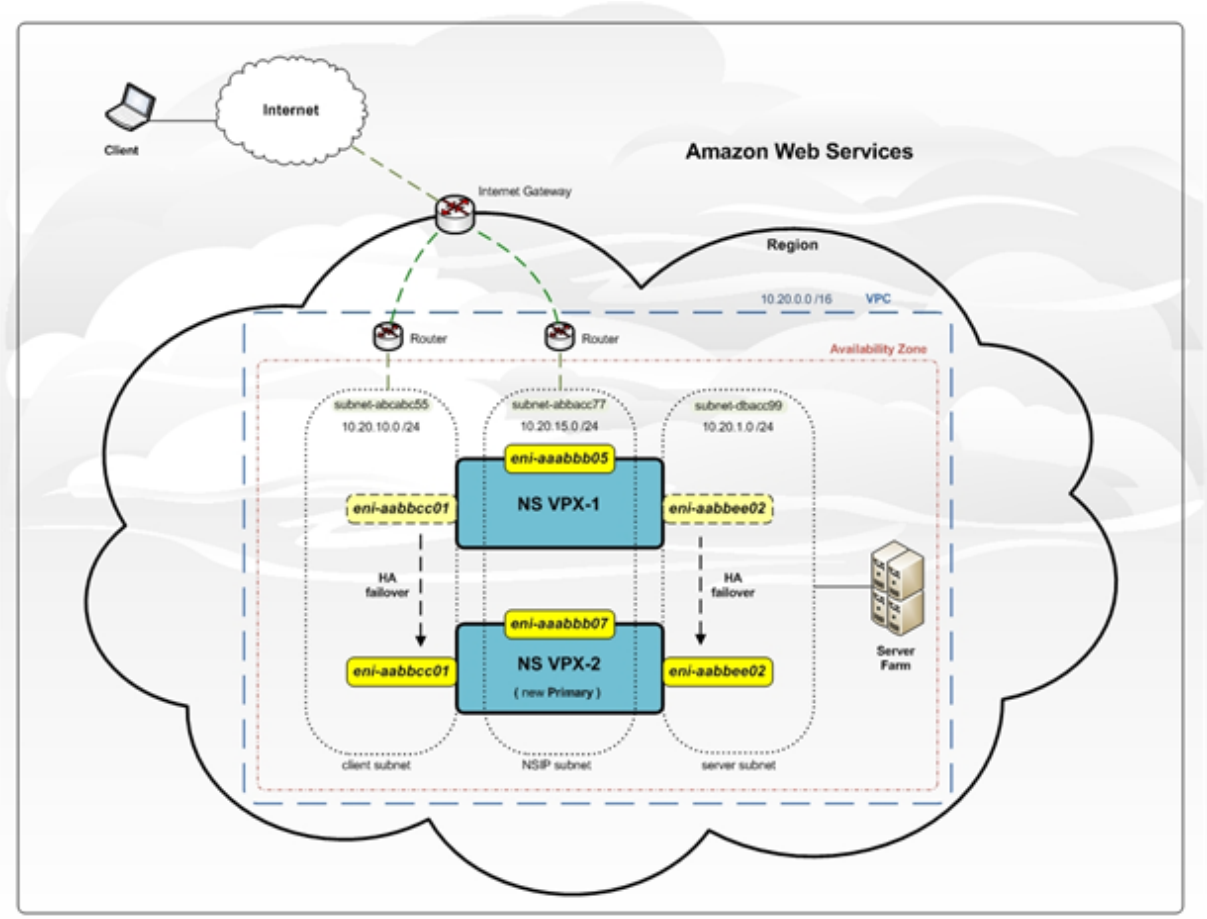
Um ein Failover auf einem Knoten zu erzwingen, geben Sie `force HA`Failover ein.

Legacy-Methode für die Bereitstellung eines VPX-HA-Paars

Vor der Veröffentlichung von 13.0 41.x wurde die HA innerhalb derselben Zone durch die AWS Elastic Network Interface (ENI) -Migration erreicht. Diese Methode ist jedoch langsam veraltet.

Die folgende Abbildung zeigt ein Beispiel für die HA-Bereitstellungsarchitektur für Citrix ADC VPX-Instanzen auf AWS.

Abbildung 1. Ein Citrix ADC VPX HA-Paar in AWS mit ENI-Migration



Sie können zwei VPX-Instanzen in AWS als HA-Paar bereitstellen, indem Sie eine der folgenden Optionen verwenden:

- Erstellen Sie die Instanzen mit IAM-Rolle manuell mithilfe der AWS Management Console und konfigurieren Sie anschließend HA darauf.
- Oder automatisieren Sie die Hochverfügbarkeitsbereitstellung mithilfe der Citrix CloudFormation-Vorlage.

Die CloudFormation-Vorlage reduziert die Anzahl der Schritte zum Erstellen eines HA-Paars erheblich und erstellt automatisch eine IAM-Rolle. In diesem Abschnitt wird beschrieben, wie ein Citrix ADC VPX HA-Paar (aktiv-passiv) mithilfe der Citrix CloudFormation-Vorlage bereitgestellt wird.

Beachten Sie die folgenden Punkte, wenn Sie zwei Citrix ADC VPX-Instanzen als HA-Paar bereitstellen.

Zu beachtendes Punkte

- HA in AWS erfordert, dass der primäre Knoten über mindestens zwei ENIs verfügt (eine für die Verwaltung und die andere für den Datenverkehr), und der sekundäre Knoten muss über eine Management-ENI verfügen. Erstellen Sie aus Sicherheitsgründen jedoch drei ENIs auf

dem primären Knoten, da Sie mit diesem Setup das private und öffentliche Netzwerk trennen können (empfohlen).
- Der sekundäre Knoten hat immer eine ENI-Schnittstelle (für die Verwaltung) und der primäre Knoten kann bis zu vier ENIs haben.
- Die NSIP-Adressen für jede VPX-Instanz in einem Hochverfügbarkeitspaar müssen auf der Standard-ENI der Instanz konfiguriert werden.
- Amazon erlaubt keine Broadcast-/Multicast-Pakete in AWS. Infolgedessen werden in einem HA-Setup ENIs auf Datenebene von der primären zur sekundären VPX-Instanz migriert, wenn die primäre VPX-Instanz ausfällt.
- Da die standardmäßige (Verwaltungs-) ENI nicht auf eine andere VPX-Instanz verschoben werden kann, verwenden Sie nicht die Standard-ENI für Client- und Serververkehr (Datenebenenverkehr).
- Die Meldung AWSCONFIG IOCTL NSAPI_HOTPLUG_INTF Erfolgsausgabe 0 in der /var/log/ns.log zeigt an, dass die beiden Daten-ENIs erfolgreich an die sekundäre Instanz (die neue primäre) angehängt wurden.
- Ein Failover kann aufgrund des AWS Detach/Attach ENI Mechanismus bis zu 20 Sekunden dauern.
- Nach einem Failover wird die ausgefallene Instanz immer neu gestartet.
- Die Heartbeat-Pakete werden nur über die Verwaltungsschnittstelle empfangen.
- Die Konfigurationsdatei der primären und sekundären VPX-Instanz wird synchronisiert, einschließlich des `nsroot` Kennworts. Das`nsroot` Kennwort des sekundären Knotens wird nach der HA-Konfigurationssynchronisierung auf das des primären Knotens festgelegt.
- Um Zugriff auf die AWS-API-Server zu haben, muss der VPX-Instanz entweder eine öffentliche IP-Adresse zugewiesen sein oder das Routing muss auf VPC-Subnetzebene korrekt eingerichtet sein, was auf das Internet-Gateway der VPC verweist.
- Nameservers/DNS-Server werden auf VPC-Ebene mit DHCP-Optionen konfiguriert.
- Die Citrix CloudFormation-Vorlage erstellt kein HA-Setup zwischen verschiedenen Availability Zones.
- Die Citrix CloudFormation-Vorlage erstellt keinen INC-Modus.
- Die AWS-Debug-Meldungen sind in der Protokolldatei /var/log/ns.log auf der VPX-Instanz verfügbar.

Stellen Sie mithilfe der Citrix CloudFormation-Vorlage ein Hochverfügbarkeitspaar bereit

Bevor Sie die CloudFormation-Vorlage starten, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen:

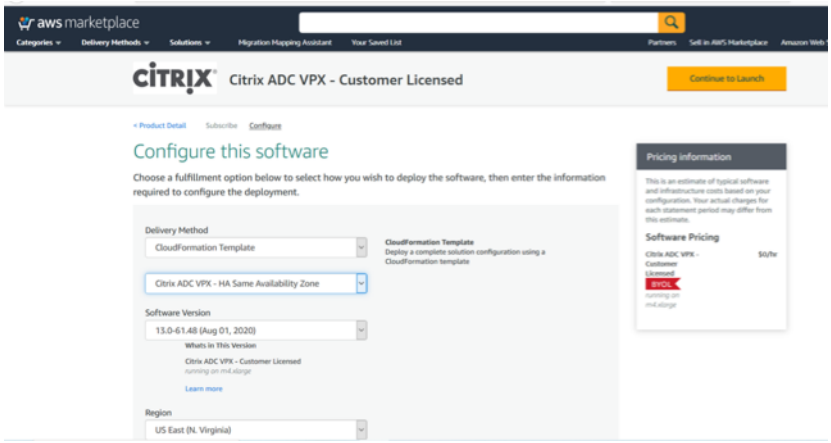
- EINE VPC
- Drei Subnetze innerhalb der VPC

- Eine Sicherheitsgruppe mit UDP 3003, TCP 3009—3010, HTTP, SSH-Ports geöffnet
- Ein Schlüsselpaar
- Erstellen Sie ein Internet-Gateway
- Bearbeiten von Routinetabellen für Client- und Verwaltungsnetzwerke, um auf das Gateway

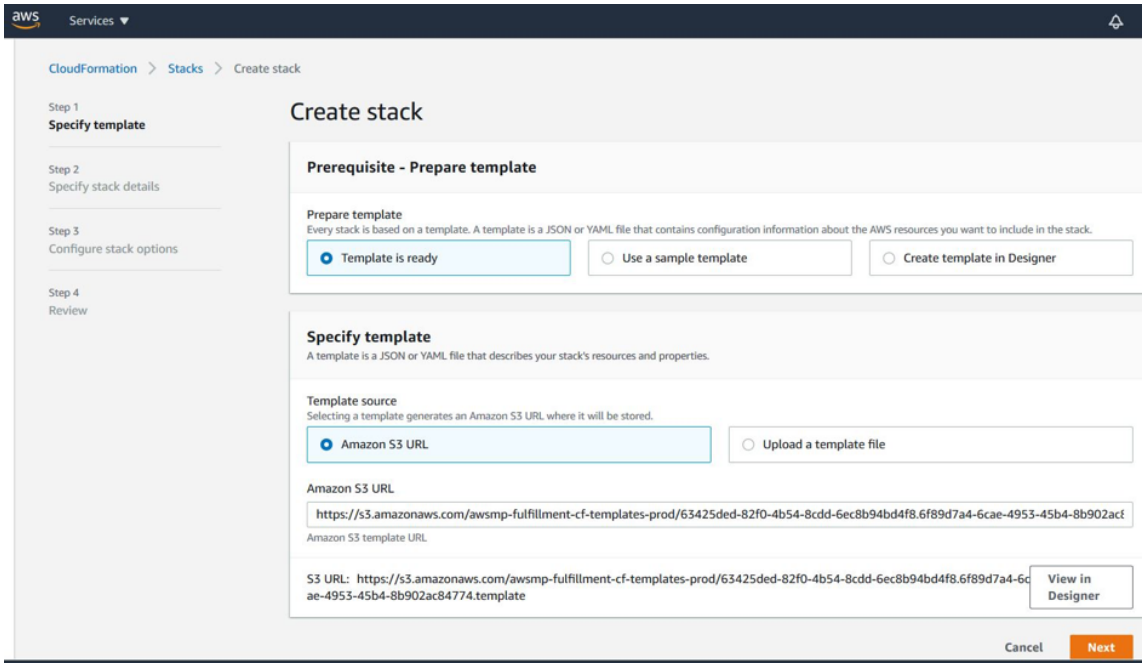
> **Hinweis**
>
> Die Citrix CloudFormation-Vorlage erstellt automatisch eine IAM-Rolle. Bestehende IAM-Rollen werden nicht in der Vorlage angezeigt.

So starten Sie die Citrix CloudFormation-Vorlage:

1. Melden Sie sich mit Ihren AWS-Anmeldeinformationen am AWS-Marketplace an .
2. Geben Sie im Suchfeld **Citrix ADC VPX** ein, um nach dem Citrix ADC AMI zu suchen, und klicken Sie auf **Los**.
3. Klicken Sie auf der Suchergebnisseite auf das gewünschte Citrix ADC VPX Angebot.
4. Klicken Sie auf die Registerkarte **Preise**, um zu **Preisinformationen** zu gelangen.
5. Wählen Sie die Region und die **Fulfillment-Option** als **Citrix ADC VPX — Kundenlizenziert**aus.
6. Klicken Sie auf **Weiter, um zu abonnieren**.
7. Überprüfen Sie die Details auf der Seite **Abonnieren** und klicken Sie **auf Configuration fortsetzen**.
8. Wählen Sie **Bereitstellungsmethode** als **CloudFormation-Vorlage** aus.
9. Wählen Sie die erforderliche CloudFormation-Vorlage aus.
10. Wählen Sie **Softwareversion** und **Region** aus und klicken Sie auf **Weiter zu Launch**.



11. Wählen Sie unter **Aktion auswählen** die Option **CloudFormation starten** aus, und klicken Sie auf **Starten**. Die Seite **Stapel erstellen** wird angezeigt.
12. Klicken Sie auf **Weiter**.

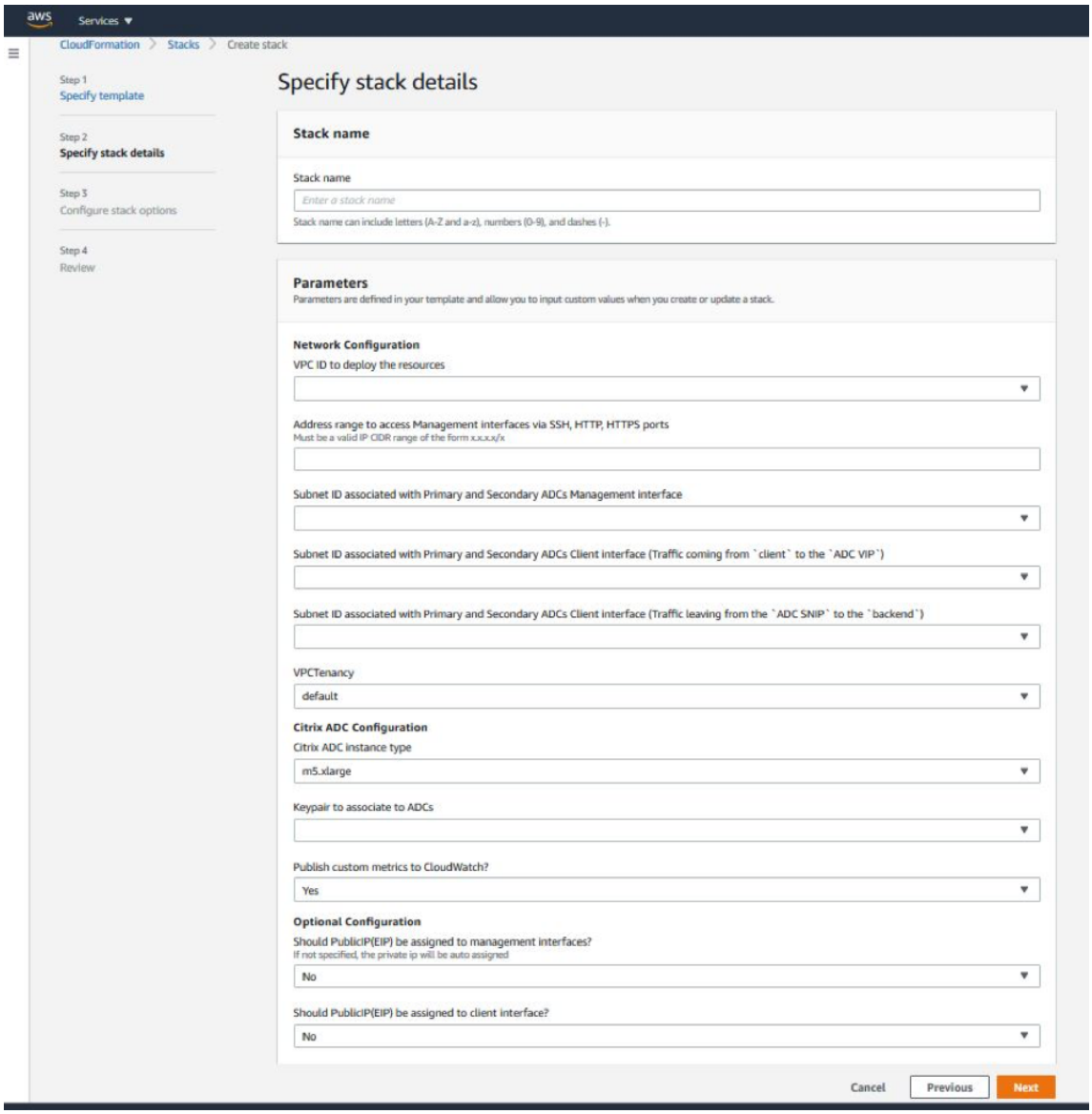


13. Die Seite **Stapeldetails angeben** wird angezeigt. Geben Sie die folgenden Details ein.

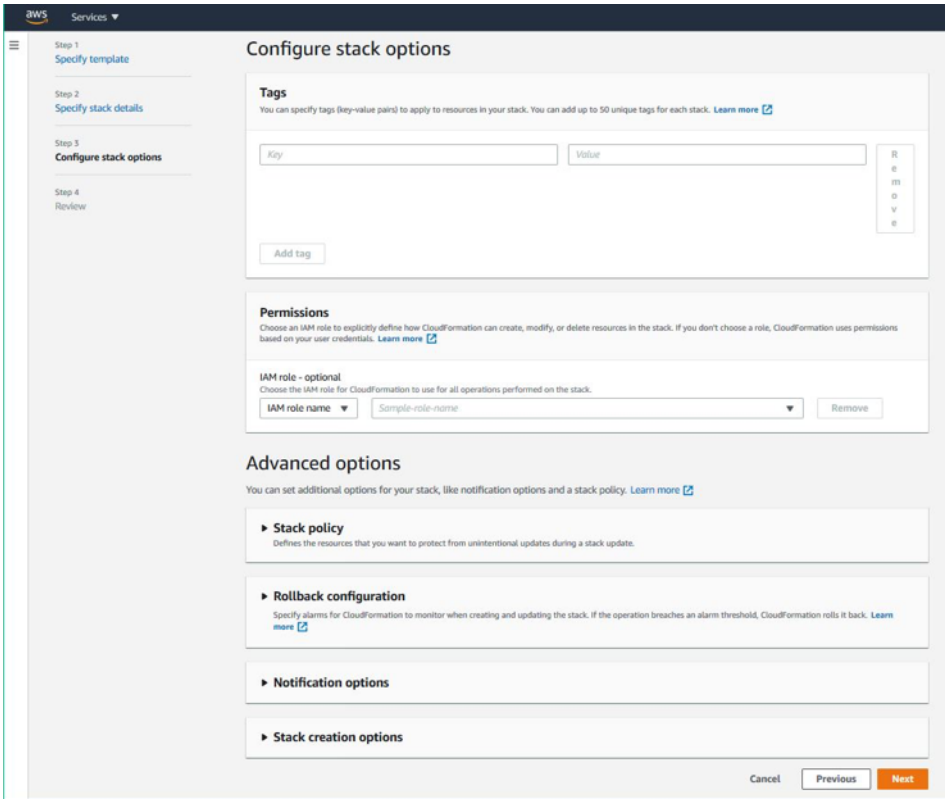
    - Geben Sie einen **Stack-Namen**ein. Der Name muss innerhalb von 25 Zeichen sein.
    - Führen Sie unter **Netzwerkkonfiguration**die folgenden Schritte aus:
        - Wählen Sie **Verwaltungsteilnetz**, **Client-Subnetz** und **Server-Subnetz** aus. Stellen Sie sicher, dass Sie die richtigen Teilnetze auswählen, die Sie in der VPC erstellt haben, die Sie unter VPC-ID ausgewählt haben.
        - Fügen Sie **primäre Verwaltungs-IP**, **sekundäre Verwaltungs-IP, Client-IPund Server-** Die IP-Adressen müssen zu denselben Subnetzen der jeweiligen Teilnetze gehören. Alternativ können Sie die Vorlage die IP-Adressen automatisch zuweisen lassen.
        - Wählen Sie **Standard** für **vpcTenancy**aus.
    - Führen Sie unter **Citrix ADC Configuration**die folgenden Schritte aus:
        - Wählen Sie **m5.xlarge** als **Instanztyp**aus.
        - Wählen Sie im Menü für Schlüsselpaar das **Schlüsselpaar**aus, das Sie bereits erstellt haben.
        - Standardmäßig sind die **Benutzerdefinierte Metriken in CloudWatch veröffentlichen?** Option ist auf **Ja**eingestellt. Wenn Sie diese Option deaktivieren möchten, wählen Sie **Nein**aus.

          Weitere Informationen zu CloudWatch-Metriken finden Sie unter Überwachen Ihrer Instanzen mit Amazon CloudWatch.
    - Führen Sie unter **Optionale Konfiguration**die folgenden Schritte aus:
        - Standardmäßig **sollte PublicIp (EIP) Management-Interfaces zugewiesen werden?** Option ist auf **Nein**eingestellt.

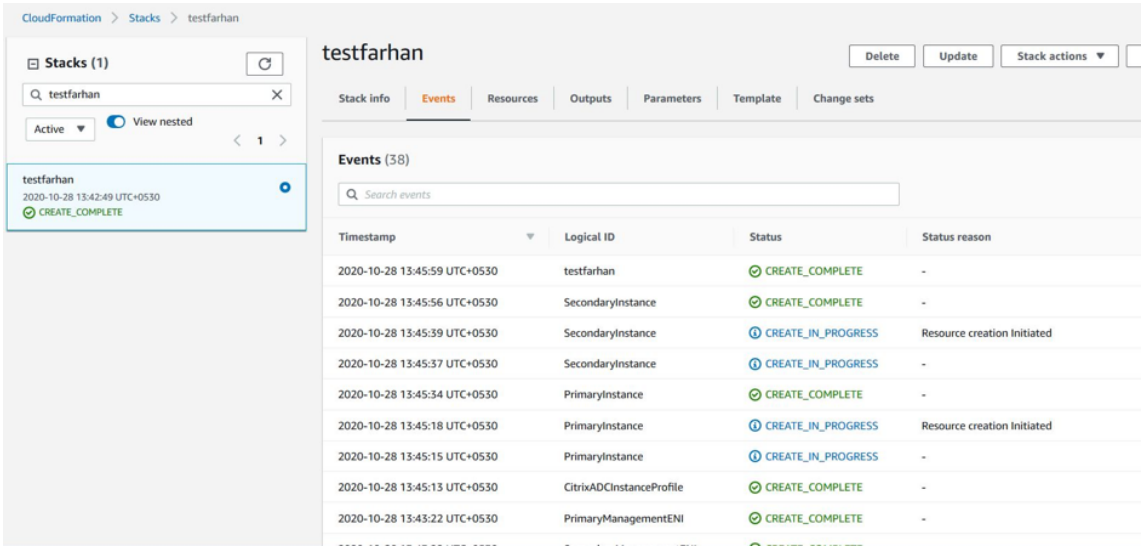
- Standardmäßig **sollte PublicIp (EIP) der Clientschnittstelle zugewiesen werden?** Option ist auf **Nein**eingestellt.



14. Klicken Sie auf **Weiter**.
15. Die Seite **Stack-Optionen konfigurieren** wird angezeigt. Dies ist eine optionale Seite.



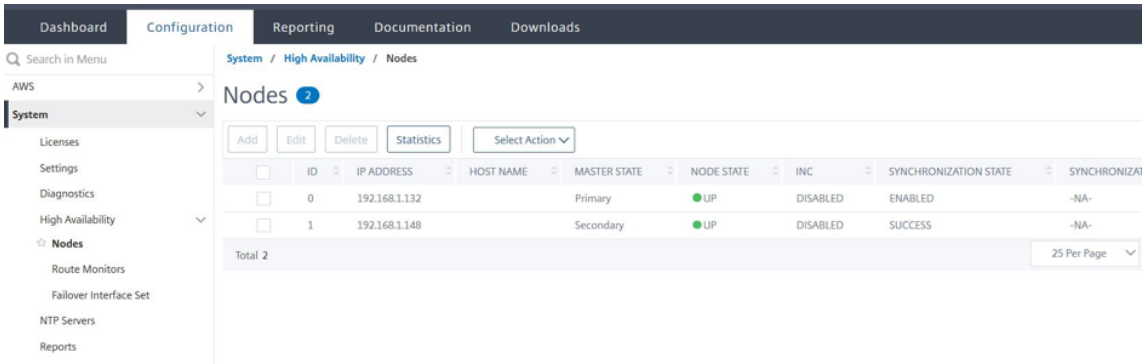
16. Klicken Sie auf **Weiter**.
17. Die Seite **Optionen** wird angezeigt. (Dies ist eine optionale Seite.). Klicken Sie auf **Weiter**.
18. Die Seite **Überprüfen** wird angezeigt. Nehmen Sie sich einen Moment Zeit, um die Einstellungen zu überprüfen und gegebenenfalls Änderungen vorzunehmen.
19. Wählen Sie die Option **Ich bestätige, dass AWS CloudFormation IAM-Ressourcen erstellt**. , und klicken Sie dann auf **Stapel erstellen**.
20. Der Status **CREATE-IN-PROGRESS** wird angezeigt. Warten Sie bis der Status **CREATE-COMPLETE**ist. Wenn sich der Status nicht in **COMPLETE**ändert, überprüfen Sie die Registerkarte **Ereignisse** auf den Grund des Fehlers und erstellen Sie die Instanz mit den richtigen Konfigurationen neu.



21. Navigieren Sie nach dem Erstellen einer IAM-Ressource zu **EC2 Management Console > Instanzen**. Sie finden zwei VPX-Instanzen, die mit IAM-Rolle erstellt wurden. Die primären und sekundären Knoten werden jeweils mit drei privaten IP-Adressen und drei Netzwerkschnittstellen erstellt.

22. Melden Sie sich am primären Knoten mit dem Benutzernamen`nsroot` und der Instanz-ID als Kennwort an. Navigieren Sie in der GUI zu **System > Hochverfügbarkeit > Knoten**. Der Citrix ADC VPX ist bereits von der CloudFormation-Vorlage als HA-Paar konfiguriert.

23. Das Citrix ADC VPX HA-Paar wird angezeigt.



Überwachen Sie Ihre Instanzen mit Amazon CloudWatch

Sie können den Amazon CloudWatch-Dienst verwenden, um eine Reihe von Citrix ADC VPX-Metriken wie CPU- und Speicherauslastung und Durchsatz zu überwachen. CloudWatch überwacht Ressourcen und Anwendungen, die auf AWS ausgeführt werden, in Echtzeit. Sie können über die AWS Management Console auf das Amazon CloudWatch-Dashboard zugreifen. Weitere Informationen finden Sie unter Amazon CloudWatch.

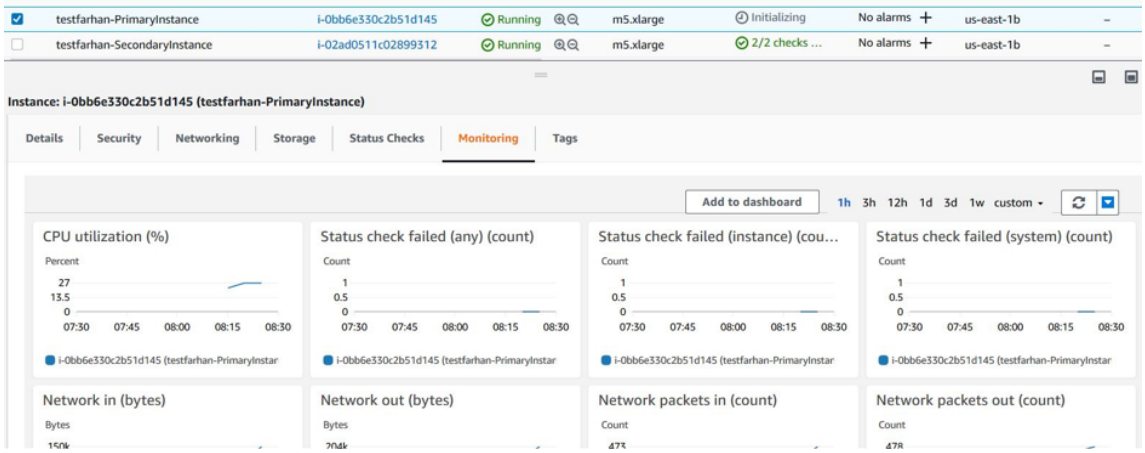
Zu beachtendes Punkte

- Wenn Sie eine Citrix ADC VPX-Instanz auf AWS mithilfe der AWS-Webkonsole bereitstellen, ist der CloudWatch-Dienst standardmäßig aktiviert.
- Wenn Sie eine Citrix ADC VPX-Instanz mithilfe der Citrix CloudFormation-Vorlage bereitstellen, lautet die Standardoption “Ja”. Wenn Sie den CloudWatch-Dienst deaktivieren möchten, wählen Sie “Nein”.
- Metriken sind für CPU (Verwaltung und Paket-CPU-Auslastung), Arbeitsspeicher und Durchsatz (eingehend und ausgehend) verfügbar.

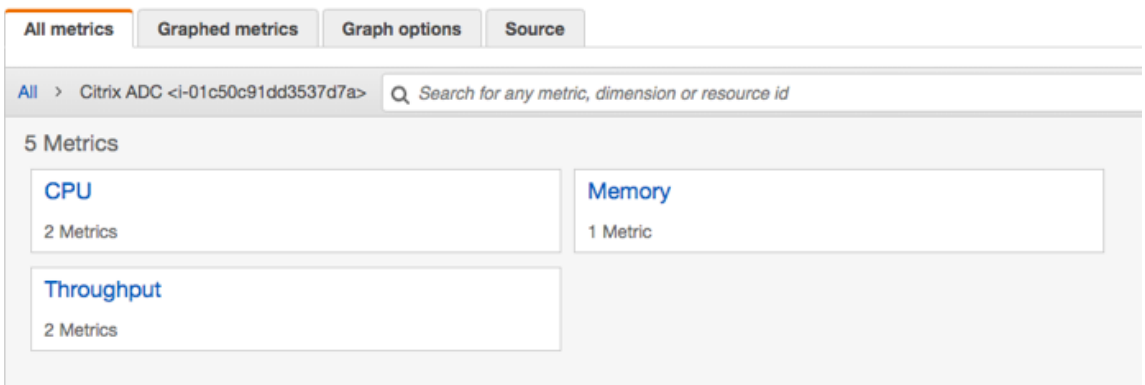
So zeigen Sie CloudWatch-Metriken an

Gehen Sie folgendermaßen vor, um CloudWatch-Metriken für Ihre Instanz anzuzeigen:

1. Melden Sie sich bei **AWS Management Console > EC2 > Instanzen** an.
2. Wählen Sie die Instanz aus.
3. Klicken Sie auf **Überwachung**.
4. Klicken Sie auf **Alle CloudWatch-Metriken anzeigen**.

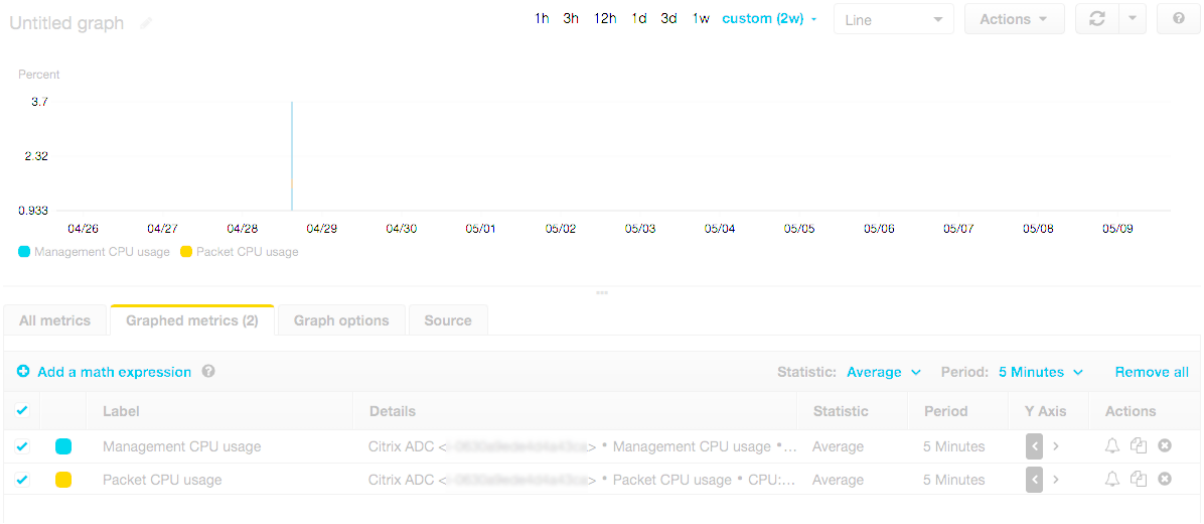


5. Klicken Sie unter Alle Metriken auf Ihre Instanz-ID.



6. Klicken Sie auf die Metriken, die Sie anzeigen möchten, und legen Sie die Dauer fest (nach Minuten, Stunden, Tagen, Wochen, Monaten).
7. Klicken Sie auf **Graphierte Metriken**, um die Nutzungsstatistiken anzuzeigen. Verwenden Sie die **Grafikoptionen**, um Ihr Diagramm anzupassen.

Abbildung. Graphische Metriken für die CPU-



Konfigurieren von SR-IOV auf einem Hochverfügbarkeits-Setup

Unterstützung für SR-IOV-Schnittstellen in einem Hochverfügbarkeitssetup ist ab Citrix ADC Version 12.0 57.19 verfügbar. Weitere Informationen zur Konfiguration von SR-IOV finden Sie unter Konfigurieren von Citrix ADC VPX-Instanzen für die Verwendung der SR-IOV-Netzwerkschnittstelle.

Zugehörige Ressourcen

So funktioniert Hochverfügbarkeit auf AWS

Hochverfügbarkeit über verschiedene AWS-Verfügbarkeitszonen

January 25, 2022

Sie können zwei Citrix ADC VPX-Instanzen in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen als aktiv-passives Paar mit hoher Verfügbarkeit im Modus Independent Network Configuration (INC) konfigurieren. Wenn der primäre Knoten aus irgendeinem Grund keine Verbindungen akzeptieren kann, übernimmt der sekundäre Knoten die Übernahme.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit. Weitere Informationen zu INC finden Sie unter Konfigurieren von Hochverfügbarkeitsknoten in verschiedenen Subnetzen.

Zu beachtendes Punkte

- Lesen Sie die folgenden Dokumente, bevor Sie mit der Bereitstellung beginnen:
  - AWS-Terminologie
  - Voraussetzungen
  - Einschränkungen und Nutzungsrichtlinien
- Das VPX-Hochverfügbarkeitspaar kann sich entweder in derselben Availability Zone in einem anderen Subnetz oder in zwei verschiedenen AWS-Verfügbarkeitszonen befinden.
- Citrix empfiehlt, dass Sie verschiedene Subnetze für die Verwaltung (NSIP), den Clientverkehr (VIP) und den Back-End-Server (SNIP) verwenden.
- Hochverfügbarkeit muss im Modus Independent Network Configuration (INC) festgelegt werden, damit ein Failover funktioniert.
- Für die beiden Instanzen muss Port 3003 für UDP-Verkehr geöffnet sein, da dieser für Heartbeats verwendet wird.
- Die Management-Subnetze beider Knoten müssen über interne NAT Zugriff auf das Internet oder auf den AWS-API-Server haben, damit die restlichen APIs funktionsfähig sind.
- Die IAM-Rolle muss über eine E2-Berechtigung für die öffentliche IP- oder Elastic IP (EIP) -Migration und EC2-Routentabellen-Berechtigungen für die private IP-Migration verfügen.

Sie können Hochverfügbarkeit in AWS Availability Zones auf folgende Weise bereitstellen:

- Verwenden von elastischen IP-Adressen
- Verwenden privater IP-Adressen

Bereitstellen eines VPX Hochverfügbarkeitspaars mit elastischen IP-Adressen in verschiedenen AWS-Zonen

January 28, 2022

Sie können zwei Citrix ADC VPX-Instanzen in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen mit elastischen IP-Adressen im INC-Modus konfigurieren.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit. Weitere Informationen zu INC finden Sie unter Konfigurieren von Hochverfügbarkeitsknoten in verschiedenen Subnetzen.

So funktioniert HA mit EIP-Adressen in verschiedenen AWS-Zonen

Bei einem Failover migriert das EIP des VIP der primären Instanz zur sekundären Instanz, die als neue primäre Instanz übernimmt. Im Failover-Prozess führt die AWS-API:

1. Überprüft die virtuellen Server, die `IPSets` an sie angeschlossen sind.
2. Sucht die IP-Adresse mit einer zugeordneten öffentlichen IP-Adresse aus den beiden IP-Adressen, die der virtuelle Server überwacht. Eine, die direkt an den virtuellen Server angeschlossen ist, und eine, die über den IP-Satz angeschlossen ist.
3. Ordnet die öffentliche IP (EIP) der privaten IP zu, die zum neuen primären VIP gehört.

> **Hinweis**
>
> Um Ihr Netzwerk vor Angriffen wie Denial-of-Service (DoS) zu schützen, können Sie bei der Verwendung eines EIP Sicherheitsgruppen in AWS erstellen, um den IP-Zugriff einzuschränken. Zur Hochverfügbarkeit können Sie gemäß Ihren Bereitstellungen von EIP zu einer privaten IP-Verlagungslösung wechseln.

So stellen Sie ein VPX-Paar mit hoher Verfügbarkeit und elastischen IP-Adressen in verschiedenen AWS-Zonen bereit

Im Folgenden finden Sie eine Zusammenfassung der Schritte zum Bereitstellen eines VPX-Paares in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen.

1. Erstellen Sie eine virtuelle Private Cloud von Amazon.
2. Stellen Sie zwei VPX-Instanzen in zwei verschiedenen Availability Zones oder in derselben Zone, aber in verschiedenen Subnetzen bereit.
3. Konfigurieren der Hochverfügbarkeit
   a) Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.
   b) Fügen Sie in beiden Instanzen einen IP-Satz hinzu.
   c) Binden Sie die in beiden Instanzen festgelegte IP an den VIP.
   d) Fügen Sie einen virtuellen Server in der primären Instanz hinzu.

Verwenden Sie für die Schritte 1 und 2 die AWS-Konsole. Verwenden Sie für Schritte 3 die Citrix ADC VPX GUI oder die CLI.

Schritt 1. Erstellen Sie eine Amazon Virtual Private Cloud (VPC).

Schritt 2. Stellen Sie zwei VPX-Instanzen in zwei verschiedenen Availability Zones oder in derselben Zone, aber in verschiedenen Subnetzen bereit. Schließen Sie eine EIP an die VIP des primären VPX an.

Weitere Informationen zum Erstellen einer VPC und zum Bereitstellen einer VPX-Instanz auf AWS finden Sie unter Bereitstellen einer eigenständigen Citrix ADC VPX Instanz auf AWS und Scenario: Standalone-Instanz

Schritt 3. Konfigurieren Sie Hochverfügbarkeit. Sie können die Citrix ADC VPX CLI oder die GUI verwenden, um Hochverfügbarkeit einzurichten.

Konfigurieren Sie Hochverfügbarkeit über die CLI

1. Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.

   Auf dem primären Knoten:

   ```
   add ha node 1 <sec_ip> -inc ENABLED
   ```

   Auf dem sekundären Knoten:

   ```
   add ha node 1 <prim_ip> -inc ENABLED
   ```

   <sec_ip> bezieht sich auf die private IP-Adresse der Verwaltungs-NIC des sekundären Knotens

   <prim_ip> bezieht sich auf die private IP-Adresse der Verwaltungs-NIC des primären Knotens

2. Fügen Sie das IP-Set in beiden Instanzen hinzu.

   Geben Sie in beiden Instanzen den folgenden Befehl ein.

   ```
   add ipset <ipsetname>
   ```

3. Binden Sie den IP-Satz an den VIP-Satz auf beiden Instanzen.

   Geben Sie in beiden Instanzen den folgenden Befehl ein:

   ```
   add ns ip <secondary vip> <subnet> -type VIP
   ```

   ```
   bind ipset <ipsetname> <secondary VIP>
   ```

   > **Hinweis**
   >
   > Sie können den IP-Satz an den primären VIP oder an den sekundären VIP binden. Wenn Sie den IP-Satz jedoch an den primären VIP binden, verwenden Sie den sekundären VIP, um ihn dem virtuellen Server hinzuzufügen, und umgekehrt.

4. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu.

   Geben Sie den folgenden Befehl ein:

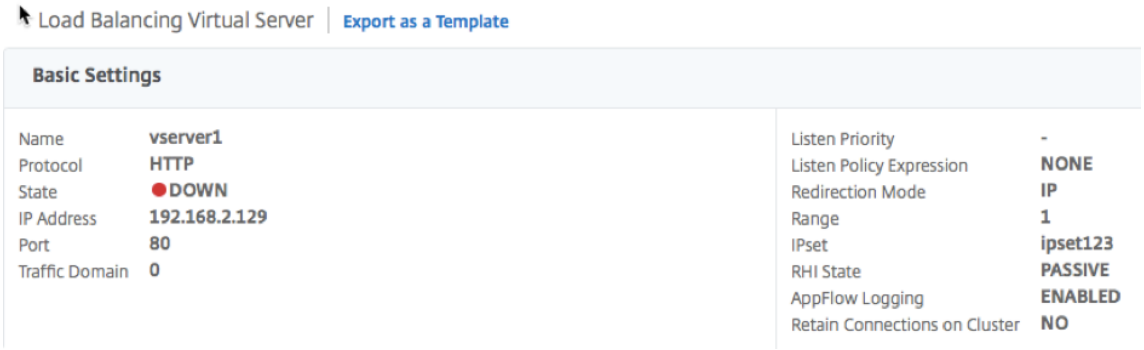
   ```
   add <server_type> vserver <vserver_name> <protocol> <primary_vip> <port
   > -ipset \<ipset_name>
   ```

Konfigurieren der Hochverfügbarkeit mit der GUI

1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein
2. Melden Sie sich mit dem Benutzernamen nsroot und der Instanz-ID als Kennwort am primären Knoten an.

3. Wechseln Sie in der GUI zu **Konfiguration** > **System** > **Hochverfügbarkeit**. Klicken Sie auf **Hinzufügen**.
4. Fügen Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des sekundären Knotens hinzu.
5. Wählen Sie **den Modus NIC (Unabhängige Netzwerkkonfiguration) auf Selbstknoten einschalten** .
6. Fügen Sie unter **Remote System Login Credential**den Benutzernamen und das Kennwort für den sekundären Knoten hinzu und klicken Sie auf **Erstellen**.
7. Wiederholen Sie die Schritte im sekundären Knoten.
8. Fügen Sie den IP-Satz hinzu und binden Sie den IP-Satz an den VIP-Satz beider Instanzen
9. Navigieren Sie in der GUI zu **System** > **Netzwerk** > **IPs** > **Hinzufügen**.
10. Fügen Sie die erforderlichen Werte für IP-Adresse, Netzwerkmaske, IP-Typ (virtuelle IP) hinzu und klicken Sie auf **Erstellen**.
11. Navigieren Sie zu **System** > **Netzwerk** > **IP-Sets** > **Hinzufügen**. Fügen Sie einen IP-Set-Namen hinzu und klicken Sie auf **Einfügen**.
12. Wählen Sie auf der Seite IPv4s die virtuelle IP aus und klicken Sie auf **Einfügen**. Klicken Sie auf **Erstellen**, um den IP-Satz zu erstellen.
13. Fügen Sie einen virtuellen Server in der primären Instanz hinzu

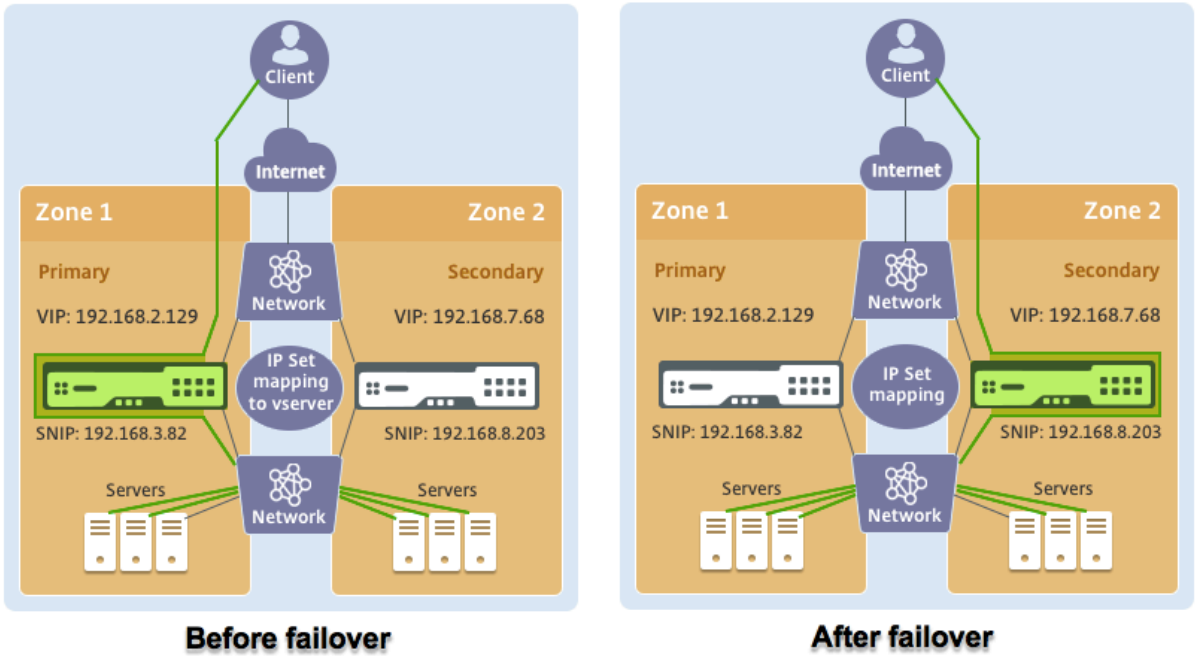
    Gehen Sie in der GUI zu **Konfiguration** > **Traffic Management** > **Virtuelle Server** > **Hinzufügen**.



Szenario

In diesem Szenario wird eine einzelne VPC erstellt. In dieser VPC werden zwei VPX-Instanzen in zwei Availability Zones erstellt. Jede Instanz hat drei Subnetze - eines für die Verwaltung, eines für den Client und eines für den Backend-Server. Ein EIP ist an den VIP des primären Knotens angeschlossen.

Diagramm: Dieses Diagramm veranschaulicht das Citrix ADC VPX Hochverfügbarkeits-Setup im INC-Modus in AWS



Verwenden Sie für dieses Szenario CLI, um Hochverfügbarkeit zu konfigurieren.

1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.

   Geben Sie die folgenden Befehle auf dem primären und sekundären Knoten ein.

   Auf Primär:

   ```
   add ha node 1 192.168.6.82 -inc enabled
   ```

   Hier bezieht sich 192.168.6.82 auf die private IP-Adresse der Management-NIC des sekundären Knotens.

   Auf Sekundarstufe:

   ```
   add ha node 1 192.168.1.108 -inc enabled
   ```

   Hier bezieht sich 192.168.1.108 auf die private IP-Adresse der Management-NIC des primären Knotens.

2. Fügen Sie einen IP-Satz hinzu und binden Sie den IP-Satz auf beiden Instanzen an den VIP

   Auf Primär:

   ```
   add ipset ipset123
   ```

   ```
   add ns ip 192.168.7.68 255.255.255.0 -type VIP
   ```

   ```
   bindipset ipset123 192.168.7.68
   ```

   Auf Sekundarstufe:

   ```
   add ipset ipset123
   ```



```
add ns ip 192.168.7.68 255.255.255.0 -type VIP

bind ipset ipset123 192.168.7.68
```

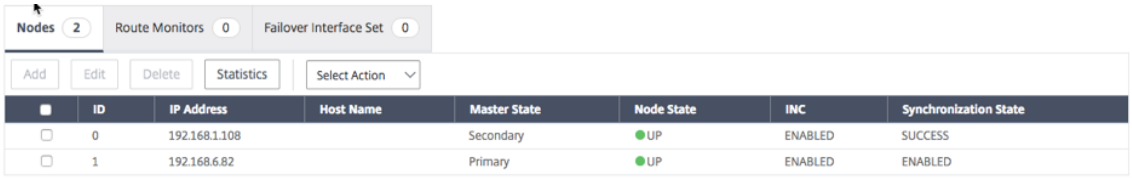
3. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu.

   Der folgende Befehl:

   ```
   add lbvserver vserver1 http 192.168.2.129 80 -ipset ipset123
   ```

4. Speichern Sie die Konfiguration.

5. Nach einem erzwungenen Failover wird der sekundäre zum neuen primären.



Bereitstellen eines VPX Hochverfügbarkeitspaars mit privaten IP-Adressen in verschiedenen AWS-Zonen

February 24, 2022

Sie können zwei Citrix ADC VPX-Instanzen in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen mit privaten IP-Adressen im INC-Modus konfigurieren. Diese Lösung kann einfach in das vorhandene Multizonen-VPX-Hochverfügbarkeitspaar mit elastischen IP-Adressenintegriert werden. Daher können Sie beide Lösungen zusammen verwenden.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit. Weitere Informationen zu INC finden Sie unter Konfigurieren von Hochverfügbarkeitsknoten in verschiedenen Subnetzen.

> Hinweis:
>
> Diese Bereitstellung wird ab Citrix ADC Release 13.0 Build 67.39 unterstützt. Diese Bereitstellung ist mit AWS Transit Gateway und VPC-Peering kompatibel.

Voraussetzungen

Stellen Sie sicher, dass die mit Ihrem AWS-Konto verknüpfte IAM-Rolle über die folgenden IAM-Berechtigungen verfügt:

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeAddresses",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeRouteTables",
                "ec2:DeleteRoute",
                "ec2:CreateRoute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "iam:SimulatePrincipalPolicy",
                "iam:GetRole"
            ],
            "Resource": "*",
            "Effect": "Allow"
         }

    ]
 }


<!--NeedCopy-->
```

So stellen Sie ein VPX-Hochverfügbarkeitspaar mit privaten IP-Adressen in verschiedenen AWS-Zonen bereit

Im Folgenden finden Sie eine Zusammenfassung der Schritte zum Bereitstellen eines VPX-Paares in zwei verschiedenen Subnetzen oder zwei verschiedenen AWS-Verfügbarkeitszonen unter Verwendung privater IP-Adressen.

1. Erstellen Sie eine virtuelle Private Cloud von Amazon.
2. Stellen Sie zwei VPX-Instanzen in zwei verschiedenen Availability Zones bereit.

3. Konfigurieren der Hochverfügbarkeit
   a) Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.
   b) Fügen Sie die entsprechenden Routentabellen in der VPC hinzu, die auf die Clientschnittstelle verweist.
   c) Fügen Sie einen virtuellen Server in der primären Instanz hinzu.

Verwenden Sie für die Schritte 1 und 2 die AWS-Konsole. Verwenden Sie für Schritt 3 die Citrix ADC VPX GUI oder die CLI.

Schritt 1. Erstellen Sie eine Amazon Virtual Private Cloud (VPC).

Schritt 2. Stellen Sie zwei VPX-Instanzen in zwei verschiedenen Availability Zones mit der gleichen Anzahl von ENI (Network Interface) bereit.

Weitere Informationen zum Erstellen einer VPC und zum Bereitstellen einer VPX-Instanz auf AWS finden Sie unter Bereitstellen einer eigenständigen Citrix ADC VPX Instanz auf AWS und Scenario: Standalone-Instanz

Schritt 3. Konfigurieren Sie die ADC-VIP-Adressen, indem Sie ein Subnetz auswählen, das sich nicht mit den Amazon VPC-Subnetzen überschneidet. Wenn Ihre VPC 192.168.0.0/16 ist, können Sie zur Konfiguration von ADC-VIP-Adressen ein beliebiges Subnetz aus diesen IP-Adressbereichen auswählen:

- 0.0.0.0 - 192.167.0.0
- 192.169.0.0 - 254.255.255.0

In diesem Beispiel wurde das ausgewählte 10.10.10.0/24-Subnetz und VIPs in diesem Subnetz erstellt. Sie können ein beliebiges Subnetz außer dem VPC-Subnetz (192.168.0.0/16) wählen.

Schritt 4. Fügen Sie aus der VPC-Routingtabelle eine Route hinzu, die auf die Clientschnittstelle (VIP) des primären Knotens verweist.

Geben Sie in der AWS CLI den folgenden Befehl ein:

```
1 aws ec2 create-route --route-table-id rtb-2272532 --destination-cidr-
     block 10.10.10.0/24 --gateway-id <eni-client-primary>
2 <!--NeedCopy-->
```

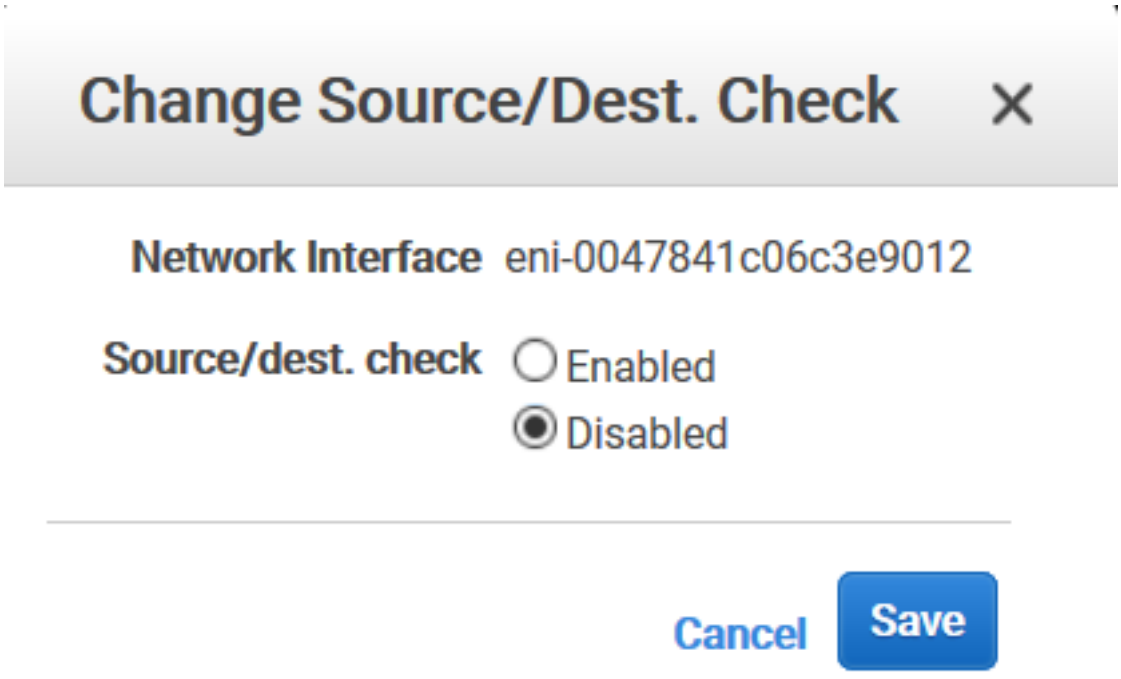
Führen Sie in der AWS-GUI die folgenden Schritte aus, um eine Route hinzuzufügen:

1. Öffnen Sie die Amazon EC2-Konsole.
2. Wählen Sie im Navigationsbereich **Route Tables**und wählen Sie die Routing-Tabelle aus.
3. Wählen Sie **Aktionen**und klicken Sie auf **Routen bearbeiten**.
4. Um eine Route hinzuzufügen, wählen Sie **Route hinzufügen**. Geben Sie für **Destination**den Ziel-CIDR-Block, eine einzelne IP-Adresse oder die ID einer Präfixliste ein. Wählen Sie für Gateway-ID das ENI einer Client-Schnittstelle des primären Knotens aus.

> Hinweis
>
> Sie müssen **Source/Dest-Check** auf dem Client-ENI der primären Instanz deaktivieren.

Um die Quell-/Zielüberprüfung für eine Netzwerkschnittstelle mithilfe der Konsole zu deaktivieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Amazon EC2-Konsole.
2. Wählen Sie im Navigationsbereich **Network Interfaces**aus.
3. Wählen Sie die Netzwerkschnittstelle einer primären Clientschnittstelle aus, wählen Sie **Aktionen**aus und klicken Sie auf Quelle/Dest **ändern. Überprüfe**.
4. Wählen Sie im Dialogfeld **Deaktiviert**und klicken Sie auf **Speichern**.



Schritt 5. Konfigurieren Sie Hochverfügbarkeit. Sie können die Citrix ADC VPX CLI oder die GUI verwenden, um Hochverfügbarkeit einzurichten.

Konfigurieren Sie Hochverfügbarkeit über die CLI

1. Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.

   Auf dem primären Knoten:

   ```
   add ha node 1 <sec_ip> -inc ENABLED
   <!--NeedCopy-->
   ```

   Auf dem sekundären Knoten:

   ```
   add ha node 1 <prim_ip> -inc ENABLED
   <!--NeedCopy-->
   ```

   <sec_ip>bezieht sich auf die private IP-Adresse der Management-NIC des sekundären Knotens.

   <prim_ip>bezieht sich auf die private IP-Adresse der Management-NIC des primären Knotens.

2. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu. Sie müssen es aus dem ausgewählten Subnetz hinzufügen, z. B. 10.10.10.0/24.

   Geben Sie den folgenden Befehl ein:

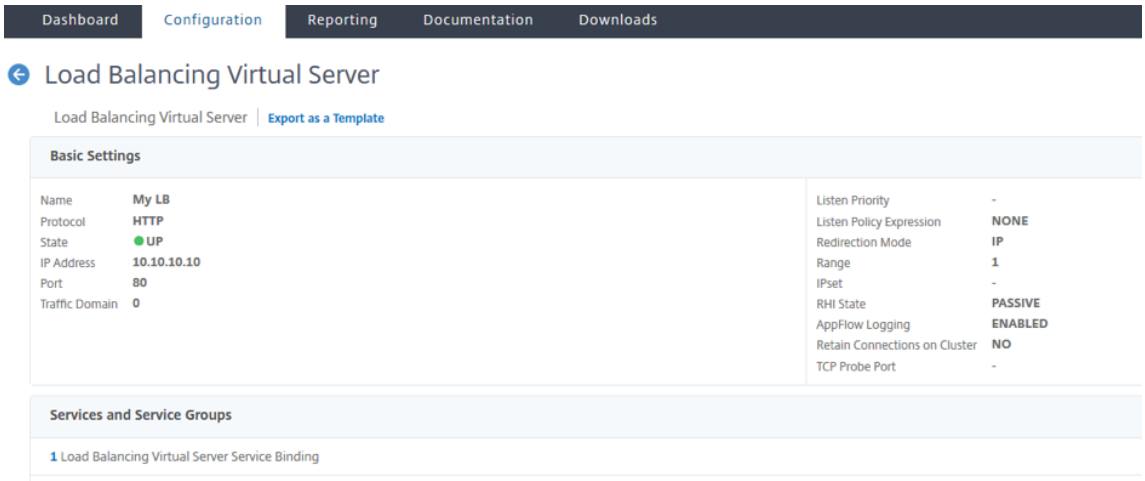
   ```
   add \<server\_type\> vserver \<vserver\_name\> \<protocol\> \<
      primary\_vip\> \<port\>
   <!--NeedCopy-->
   ```

Konfigurieren der Hochverfügbarkeit mit der GUI

1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein
2. Melden Sie sich mit dem Benutzernamen `nsroot` und der Instanz-ID als Kennwort am primären Knoten an.
3. Navigieren Sie zu **Konfiguration** > **System** > **Hochverfügbarkeit**und klicken Sie auf **Hinzufügen**.
4. Fügen Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des sekundären Knotens hinzu.

5. Wählen Sie **den Modus NIC (Unabhängige Netzwerkkonfiguration) auf Selbstknoten einschalten** .
6. Fügen Sie unter **Remote System Login Credential**den Benutzernamen und das Kennwort für den sekundären Knoten hinzu und klicken Sie auf **Erstellen**.
7. Wiederholen Sie die Schritte im sekundären Knoten.
8. Fügen Sie einen virtuellen Server in der primären Instanz hinzu

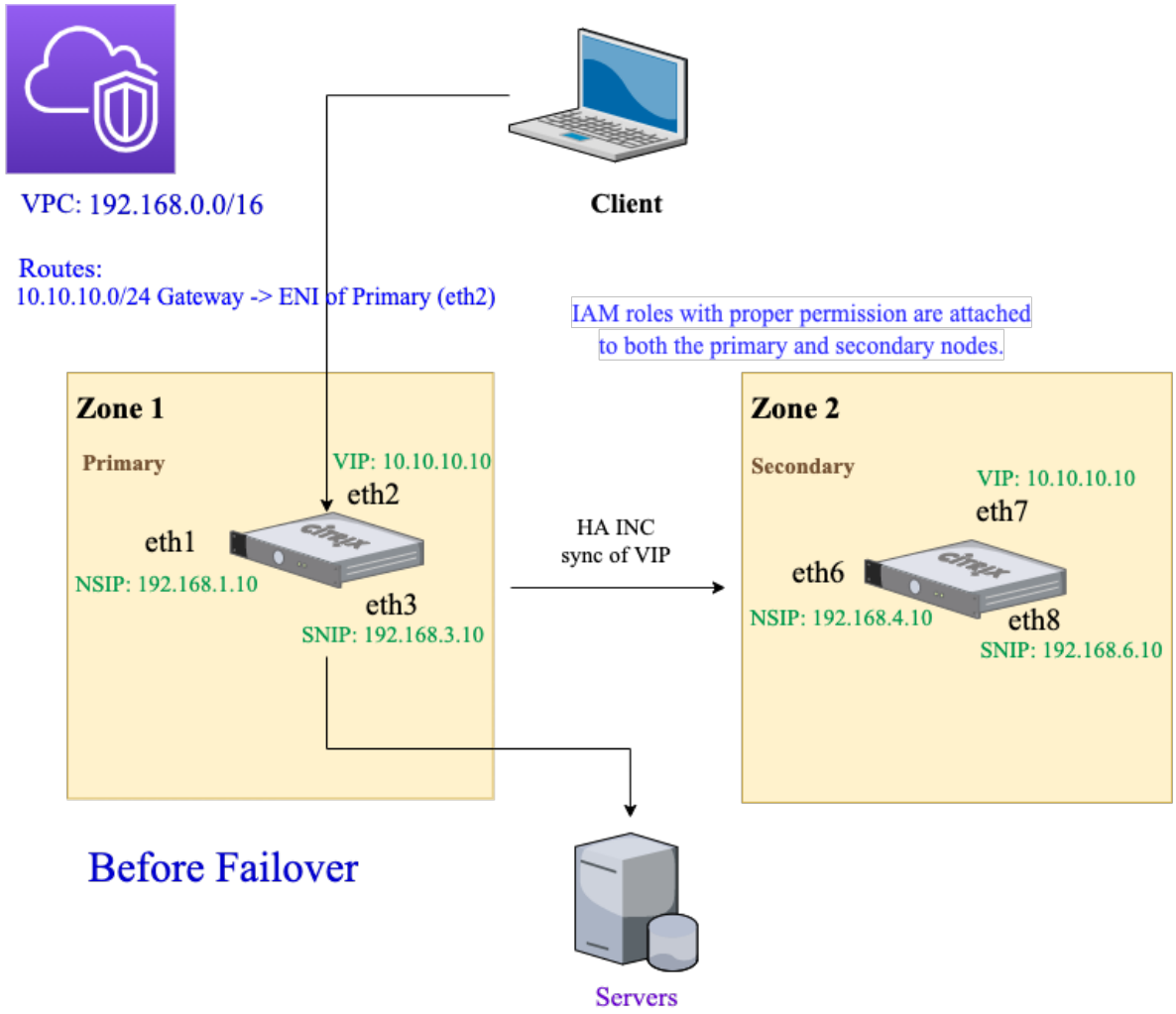
   Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Virtuelle Server** > **Hinzufügen**.

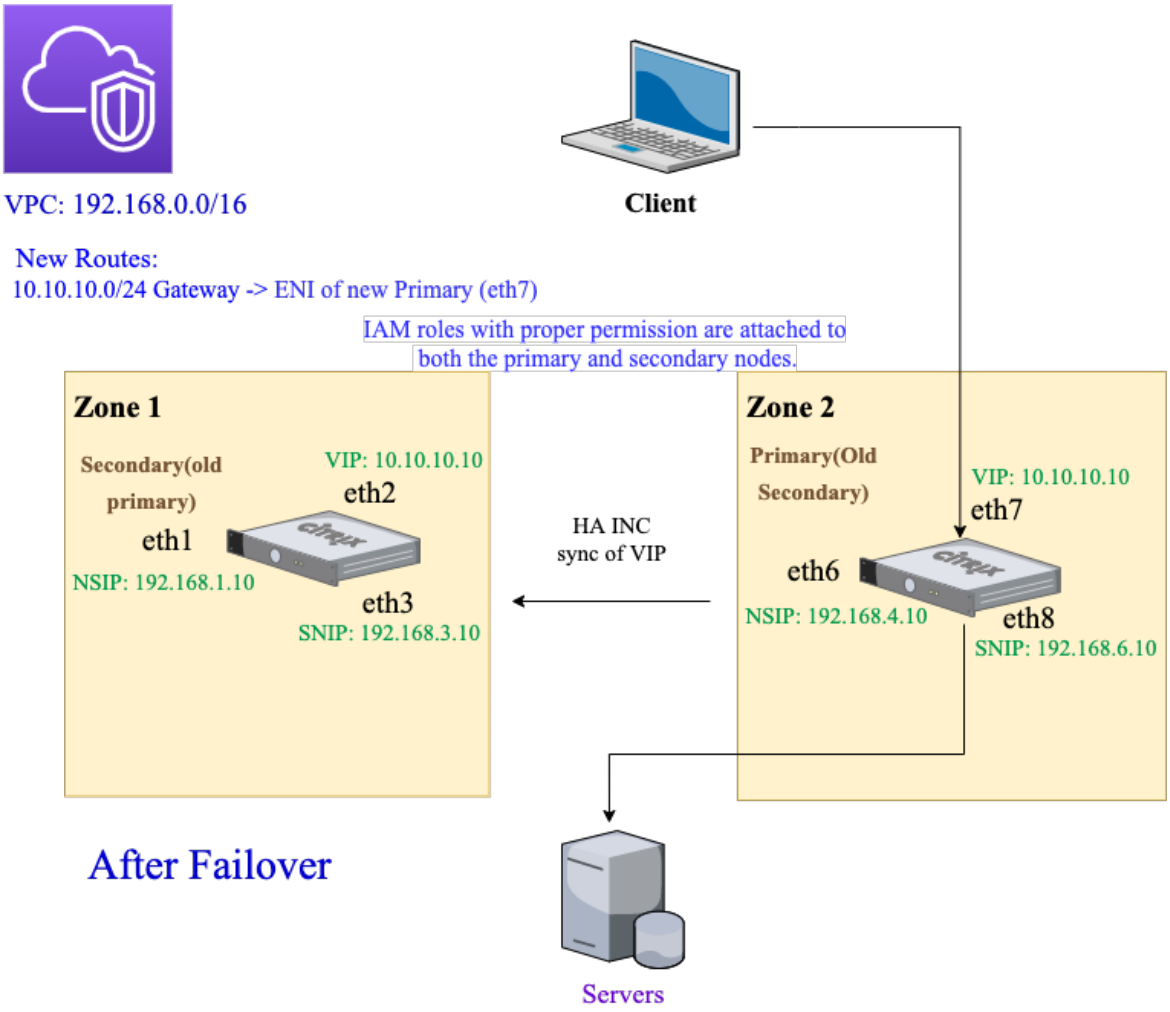


Szenario

In diesem Szenario wird eine einzelne VPC erstellt. In dieser VPC werden zwei VPX-Instanzen in zwei Availability Zones erstellt. Jede Instanz hat drei Subnetze - eines für die Verwaltung, eines für den Client und eines für den Backend-Server.

Die folgenden Diagramme veranschaulichen das Citrix ADC VPX Hochverfügbarkeitssetup im INC-Modus auf AWS. Das benutzerdefinierte Subnetz 10.10.10.10, das nicht Teil der VPC ist, wird als VIP verwendet. Daher kann das Subnetz 10.10.10.10 über Availability Zones hinweg verwendet werden.





Verwenden Sie für dieses Szenario CLI, um Hochverfügbarkeit zu konfigurieren.

1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.

   Geben Sie die folgenden Befehle auf dem primären und sekundären Knoten ein.

   Auf dem primären Knoten:

```
1 add ha node 1 192.168.4.10 -inc enabled
2 <!--NeedCopy-->
```

   Hier bezieht sich 192.168.4.10 auf die private IP-Adresse der Management-NIC des sekundären Knotens.

   Auf dem sekundären Knoten:

```
1 add ha node 1 192.168.1.10 -inc enabled
```



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

Hier bezieht sich 192.168.1.10 auf die private IP-Adresse der Management-NIC des primären Knotens.

2. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu.

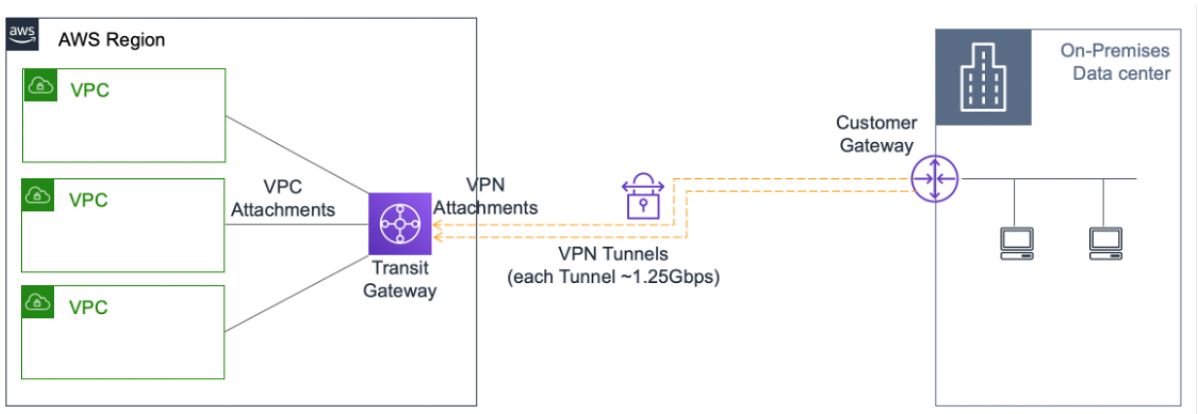
   Geben Sie den folgenden Befehl ein:

```
add lbvserver vserver1 http 10.10.10.10 80
<!--NeedCopy-->
```

3. Speichern Sie die Konfiguration.
4. Nach einem erzwungenen Failover:
   - Die sekundäre Instanz wird zur neuen primären Instanz.
   - Die VPC-Route, die auf die primäre ENI zeigt, migriert zum sekundären Client-ENI.
   - Der Clientverkehr wird auf die neue primäre Instanz fortgesetzt.

AWS Transit Gateway-Konfiguration für eine private HA-IP-Lösung

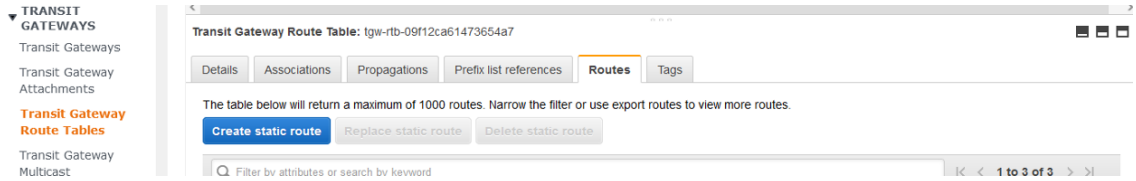
Sie benötigen AWS Transit Gateway, um das private VIP-Subnetz innerhalb des internen Netzwerks über AWS-VPCs, Regionen und lokale Netzwerke hinweg routbar zu machen. Die VPC muss eine Verbindung zu AWS Transit Gateway herstellen. Eine statische Route für das VIP-Subnetz oder den IP-Pool in der AWS Transit Gateway-Routingtabelle wird erstellt und auf die VPC gerichtet.



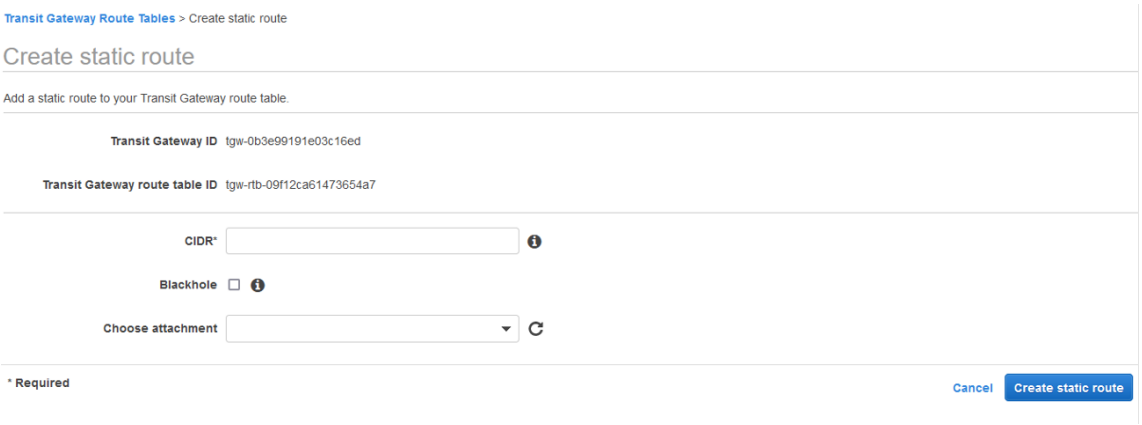
Gehen Sie folgendermaßen vor, um AWS Transit Gateway zu konfigurieren:

1. Öffnen Sie die Amazon VPC-Konsole.
2. Wählen Sie im Navigationsbereich **Transit Gateway Route Table** aus.

3. Wählen Sie die Registerkarte **Routen** und klicken Sie auf **Statische Route erstellen**.



4. Erstellen Sie eine statische Route, bei der CIDR auf Ihr privates VIPS-Subnetz und Befestigungspunkte an die VPC mit ADC VPX verweist.



5. Klicken Sie auf **Statische Route erstellen**und wählen Sie dann **Schließen**.

Bereitstellen einer Citrix ADC VPX Instanz in AWS Outposts

October 5, 2021

AWS Outposts ist ein Pool von AWS-Rechen- und Speicherkapazitäten, die an Ihrem Standort bereitgestellt werden. Outposts bietet AWS-Infrastruktur und -Services an Ihrem lokalen Standort. AWS betreibt, überwacht und verwaltet diese Kapazität als Teil einer AWS-Region. Sie können dieselben Citrix ADC VPX Instanzen, AWS-APIs, Tools und Infrastrukturen sowohl lokal als auch in der AWS-Cloud für ein konsistentes Hybriderlebnis verwenden.

Sie können Subnetze in Ihren Außenposten erstellen und diese angeben, wenn Sie AWS-Ressourcen wie EC2-Instanzen, EBS-Volumes, ECS-Cluster und RDS-Instanzen erstellen. Instanzen in den Außenposten-Subnetzen kommunizieren mit anderen Instanzen in der AWS-Region über private IP-Adressen, alle innerhalb derselben Amazon Virtual Private Cloud (VPC).

Weitere Informationen finden Sie im Benutzerhandbuch für AWS Outposts.

Funktionsweise von AWS Outposts

AWS Outposts wurde entwickelt, um mit einer konstanten und konsistenten Verbindung zwischen Ihren Außenstellen und einer AWS-Region zu arbeiten. Um diese Verbindung zur Region und zu den lokalen Arbeitslasten in Ihrer lokalen Umgebung herzustellen, müssen Sie Ihren Außenposten mit Ihrem lokalen Netzwerk verbinden. Ihr lokales Netzwerk muss WAN-Zugriff auf die Region und das Internet ermöglichen. Das Internet muss auch LAN- oder WAN-Zugriff auf das lokale Netzwerk bereitstellen, in dem sich Ihre lokalen Workloads oder Anwendungen befinden.

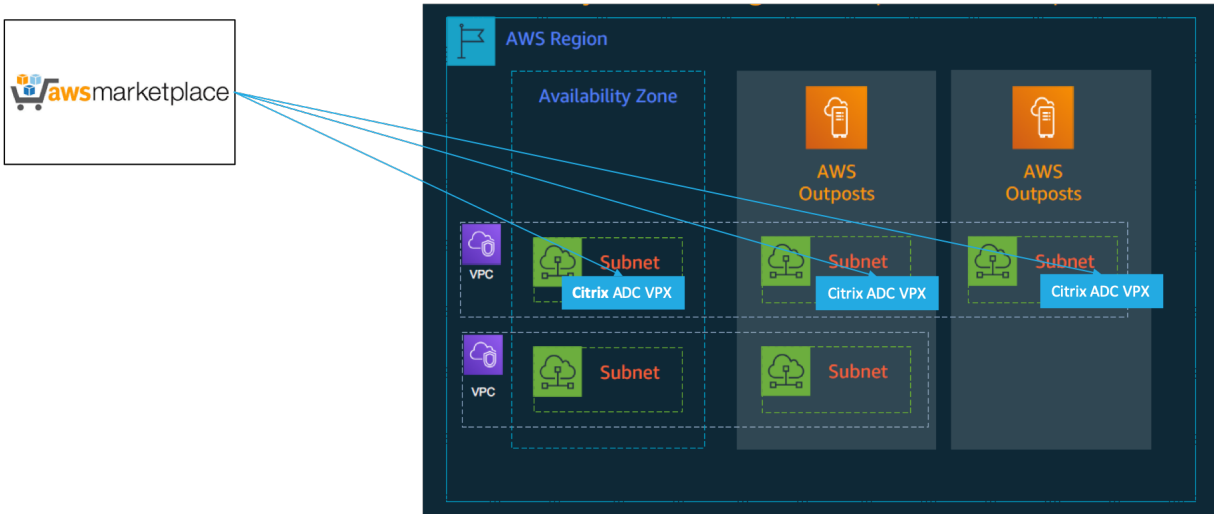
Voraussetzung

- Sie müssen einen AWS Outposts an Ihrem Standort installieren.
- Die Rechen- und Speicherkapazität von AWS Outposts muss zur Verwendung verfügbar sein.

Weitere Informationen zum Aufgeben einer Bestellung für AWS Outposts finden Sie in der folgenden AWS-Dokumentation:
https://aws.amazon.com/blogs/aws/aws-outposts-now-available-order-your-racks-today/

Bereitstellen einer Citrix ADC VPX Instanz in AWS Outposts mithilfe der AWS-Webkonsole

Die folgende Abbildung zeigt eine einfache Bereitstellung von Citrix ADC VPX Instanzen auf den Outposts. Das im AWS Marketplace vorhandene Citrix ADC AMI wird auch in den Außenposten bereitgestellt.



Melden Sie sich bei der AWS-Webkonsole an, und führen Sie die folgenden Schritte aus, um ADC VPX EC2-Instanzen auf Ihren AWS Outposts bereitzustellen.

1. Erstellen Sie ein Schlüsselpaar.
2. Erstellen Sie eine Virtual Private Cloud (VPC).

3. Fügen Sie weitere Subnetze hinzu.
4. Erstellen Sie Sicherheitsgruppen und Sicherheitsregeln.
5. Hinzufügen von Routentabellen.
6. Erstellen Sie ein Internet-Gateway.
7. Erstellen Sie eine ADC VPX-Instanz mithilfe des AWS EC2-Service.
   Navigieren Sie im AWS-Dashboard zu **Compute > EC2 > Launch Instanz > AWS Marketplace**.
8. Erstellen und fügen Sie weitere Netzwerkschnittstellen hinzu.
9. Verbinden Sie elastische IPs mit der Management-NIC.
10. Stellen Sie eine Verbindung mit der VPX-Instanz her.

Ausführliche Anweisungen zu jedem der Schritte finden Sie unter Bereitstellen einer Citrix ADC VPX-Instanz in AWS mithilfe der AWS-Webkonsole.

Informationen zur Hochverfügbarkeit innerhalb derselben Availability Zone-Bereitstellung finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares auf AWS.

Hinzufügen des Back-End-AWS-Autoscaling-Dienstes

October 5, 2021

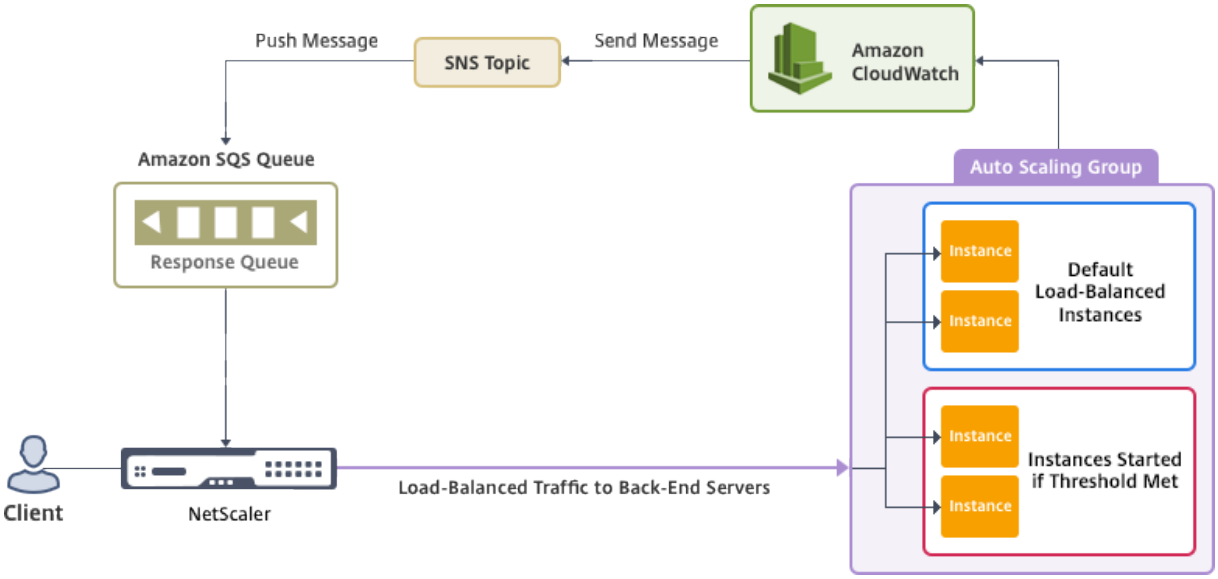
Effizientes Hosting von Anwendungen in einer Cloud erfordert eine einfache und kostengünstige Verwaltung der Ressourcen je nach Anwendungsbedarf. Um die steigende Nachfrage zu erfüllen, müssen Sie Netzwerkressourcen nach oben skalieren. Unabhängig davon, ob der Bedarf nachlässt, müssen Sie sich skalieren, um unnötige Kosten für ungenutzte Ressourcen zu vermeiden. Um die Kosten für die Ausführung der Anwendung zu minimieren, indem nur so viele Instanzen bereitgestellt werden, wie es zu einem bestimmten Zeitpunkt erforderlich ist, müssen Sie den Datenverkehr, den Arbeitsspeicher und die CPU-Auslastung usw. ständig überwachen. Die manuelle Überwachung des Datenverkehrs ist jedoch umständlich. Damit die Anwendungsumgebung dynamisch nach oben oder unten skaliert werden kann, müssen Sie die Prozesse der Überwachung des Datenverkehrs und der Skalierung von Ressourcen bei Bedarf automatisieren.

Die Citrix ADC VPX-Instanz ist in den AWS Auto Scaling-Service integriert und bietet folgende Vorteile:

- **Lastausgleich und -verwaltung**: Automatisch konfiguriert Server so, dass sie je nach Bedarf hoch- und herunterskaliert werden. Die VPX-Instanz erkennt automatisch Autoscale-Gruppen im Back-End-Subnetz und ermöglicht es einem Benutzer, die Autoscale-Gruppen auszuwählen, um die Last auszugleichen. All dies geschieht durch automatische Konfiguration der virtuellen und Subnetz-IP-Adressen auf der VPX-Instanz.
- **Hohe Verfügbarkeit**: Erkennt Autoscale-Gruppen, die sich über mehrere Availability Zones und Server mit Lastenausgleich erstrecken.
- **Bessere Netzwerkverfügbarkeit**: Die VPX-Instanz unterstützt:

  - Back-End-Server auf verschiedenen VPCs mit VPC-Peering
  - Back-End-Server in denselben Platzierungsgruppen
  - Back-End-Server in verschiedenen Availability Zones
- **Ordnungsgemäße Verbindungsbeendigung**: Entfernt Autoscale-Server ordnungsgemäß und vermeidet den Verlust von Clientverbindungen, wenn Scale-Down-Aktivität auftritt, mit der Funktion “Graceful Timeout”.

Diagramm: AWS Autoscaling Service mit einer Citrix ADC VPX Instanz



In diesem Diagramm wird veranschaulicht, wie der AWS AutoScaling-Dienst mit einer Citrix ADC VPX Instanz (Load Balancing virtueller Server) kompatibel ist. Weitere Informationen finden Sie in den folgenden AWS-Themen.

- Automatische Skalierung von Gruppen
- CloudWatch
- Einfacher Benachrichtigungsdienst (SNS)
- Einfacher Warteschlangendienst (Amazon SQS)

Voraussetzungen

Bevor Sie Autoscaling mit der Citrix ADC VPX-Instanz verwenden, müssen Sie die folgenden Aufgaben ausführen.

1. Lesen Sie die folgenden Themen:
   - Voraussetzungen
   - Einschränkungs- und Nutzungsrichtlinien
2. Erstellen Sie eine Citrix ADC VPX-Instanz auf AWS entsprechend Ihren Anforderungen.

- Weitere Informationen zum Erstellen einer eigenständigen Citrix ADC VPX Instanz finden Sie unter Bereitstellen einer eigenständigen Citrix ADC VPX-Instanz auf AWS und Scenario: Standalone-Instanz
- Weitere Informationen zur Bereitstellung von VPX-Instanzen im HA-Modus finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares auf AWS.

> **Hinweis**
>
> Citrix empfiehlt die CloudFormation-Vorlage zum Erstellen von Citrix ADC VPX -Instanzen in AWS.
>
> Citrix empfiehlt, drei Schnittstellen zu erstellen: eine für die Verwaltung (NSIP), eine für den clientseitigen LB Virtual Server (VIP) und eine für Subnetz-IP (NSIP).

3. Erstellen Sie eine AWS Autoscale-Gruppe. Wenn Sie keine vorhandene AutoScaling-Konfiguration haben, müssen Sie Folgendes tun:

   a) Erstellen einer Startkonfiguration

   b) Erstellen einer Autoskalierungsgruppe

   c) Überprüfen der Autoscaling Gruppe

   Weitere Informationen finden Sie unter http://docs.aws.amazon.com/autoscaling/latest/userguide/GettingStartedTutorial.html.

4. In der Gruppe AWS Autoscale müssen Sie mindestens eine Scale-Down-Richtlinie angeben. Die Citrix ADC VPX Instanz unterstützt nur die Step-Skalierungsrichtlinie. Die Richtlinie “Einfache Skalierung” und die Richtlinie “Zielverfolgung” werden für die Gruppe “Autoskalierung” nicht unterstützt.

Hinzufügen des AWS-Autoscaling-Dienstes zu einer Citrix ADC VPX-Instanz

Sie können den Autoscaling-Dienst einer VPX-Instanz mit einem einzigen Klick mit der GUI hinzufügen. Führen Sie die folgenden Schritte aus, um der VPX-Instanz den Autoscaling-Dienst hinzuzufügen:

1. Melden Sie sich bei der VPX-Instanz an, indem Sie Ihre Anmeldeinformationen für verwenden`nsroot`.
2. Wenn Sie sich zum ersten Mal bei der Citrix ADC VPX-Instanz anmelden, wird die standardmäßige Cloud-Profilseite angezeigt. Wählen Sie die AWS AutoScaling-Gruppe aus dem Dropdownmenü aus und klicken Sie auf **Erstellen**, um ein Cloud-Profil zu erstellen. Klicken Sie auf **Überspringen**, wenn Sie das Cloud-Profil später erstellen möchten.

   Punkte, die beim Erstellen eines Cloud-Profils berücksichtigtwerden müssen: Standardmäßig erstellt und fügt die CloudFormation-Vorlage die folgende IAM-Rolle an.


```
{

    ”Version”: ”2012-10-17”,

    ”Statement”: [

     {


            ”Action”: [

                ”ec2:DescribeInstances”,

                ”ec2:DescribeNetworkInterfaces”,

                ”ec2:DetachNetworkInterface”,

                ”ec2:AttachNetworkInterface”,

                ”ec2:StartInstances”,

                ”ec2:StopInstances”,

                ”ec2:RebootInstances”,

                ”autoscaling:*”,

                ”sns:*”,

                ”sqs:*”

             “iam: SimulatePrincipalPolicy”

             “iam: GetRole”

            ],

            ”Resource”: ”*”,

            ”Effect”: ”Allow”

        }

```

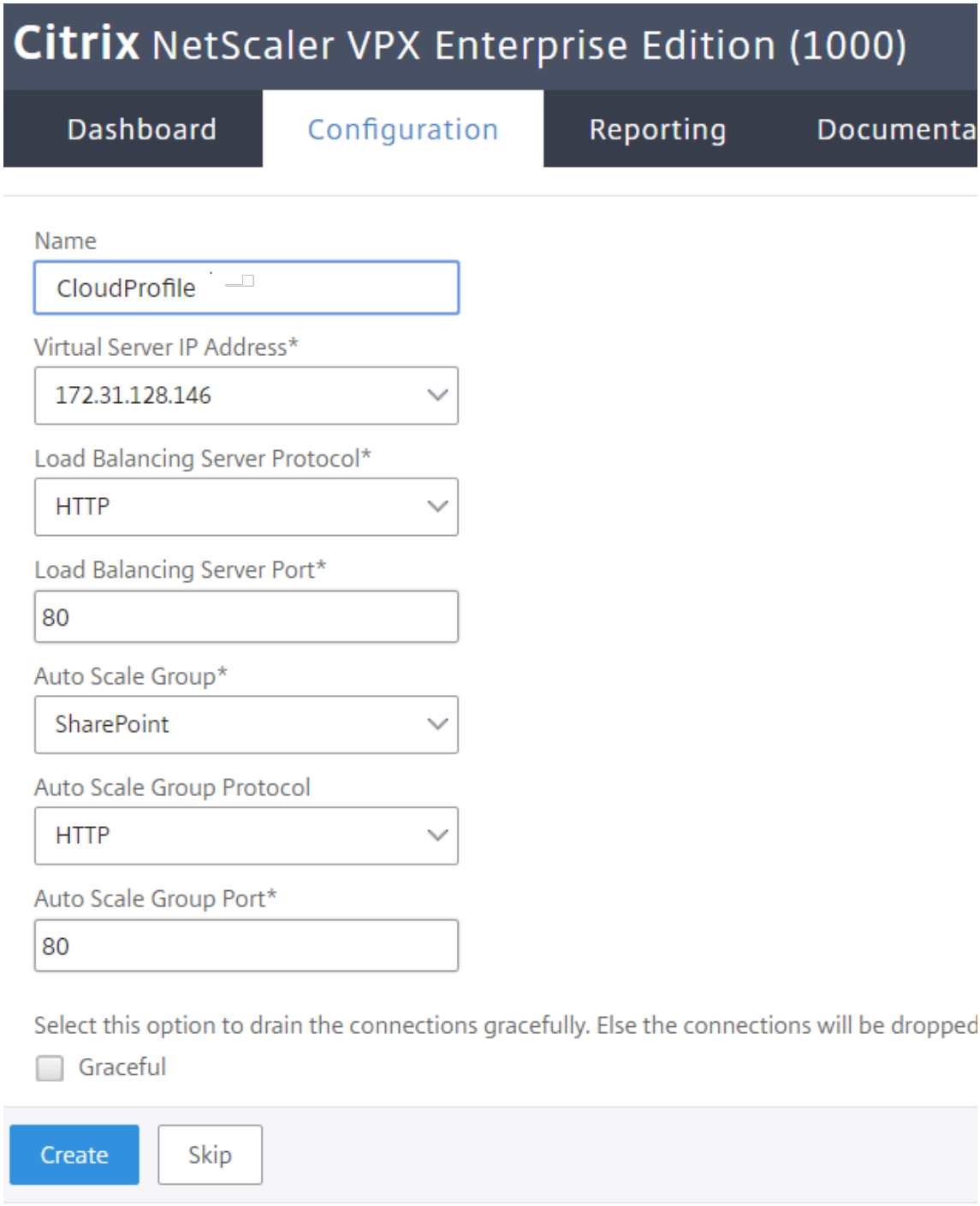


```
45
46       ]
47
48   }
49
50 <!--NeedCopy-->
```

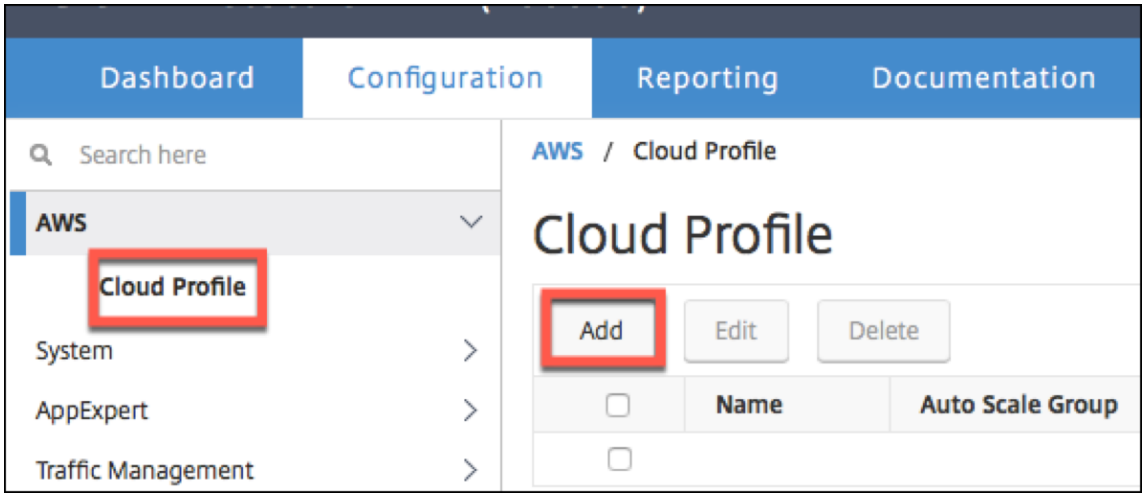
Stellen Sie sicher, dass die IAM-Rolle einer Instanz über die entsprechenden Berechtigungen verfügt.

- Die IP-Adresse des virtuellen Servers wird automatisch von der für die VPX-Instanz verfügbaren freien IP-Adresse abgeleitet. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/MultipleIP.html#ManageMultipleIP
- Die Autoscale-Gruppe wird aus der Autoscale-Gruppe, die in Ihrem AWS-Konto konfiguriert ist, vorausgefüllt. http://docs.aws.amazon.com/autoscaling/latest/userguide/AutoScalingGroup.html.
- Achten Sie bei der Auswahl des Protokolls und des Ports der Autoscaling Group darauf, dass die Server diese Protokolle und Ports überwachen und den richtigen Monitor in der Dienstgruppe binden. Standardmäßig wird der TCP-Monitor verwendet.
- Bei SSL-Protokolltyp Autoscaling ist nach dem Erstellen des Cloud-Profils der Lastausgleich der virtuelle Server oder die Dienstgruppe aufgrund eines fehlenden Zertifikats ausgefallen. Sie können das Zertifikat manuell an den virtuellen Server oder die Dienstgruppe binden.
- Wählen Sie die Option “Graceful Timeout” aus, um Autoscale-Server ordnungsgemäß zu entfernen. Wenn diese Option nicht ausgewählt ist, wird der Server die Autoscale-Gruppe unmittelbar nach Ausfall der Last entfernt, was zu Dienstunterbrechungen für die vorhandenen verbundenen Clients führen kann. Wenn Sie “Graceful” auswählen und ein Timeout geben, bedeutet dies im Falle einer Skalierung nach unten. Die VPX-Instanz entfernt den Server nicht sofort, sondern markiert einen der Server für die ordnungsgemäße Löschung. Während dieses Zeitraums lässt die Instanz keine neuen Verbindungen zu diesem Server zu. Bestehende Verbindung wird bereitgestellt, bis das Timeout eintritt, und nach einem Timeout entfernt die VPX-Instanz den Server.

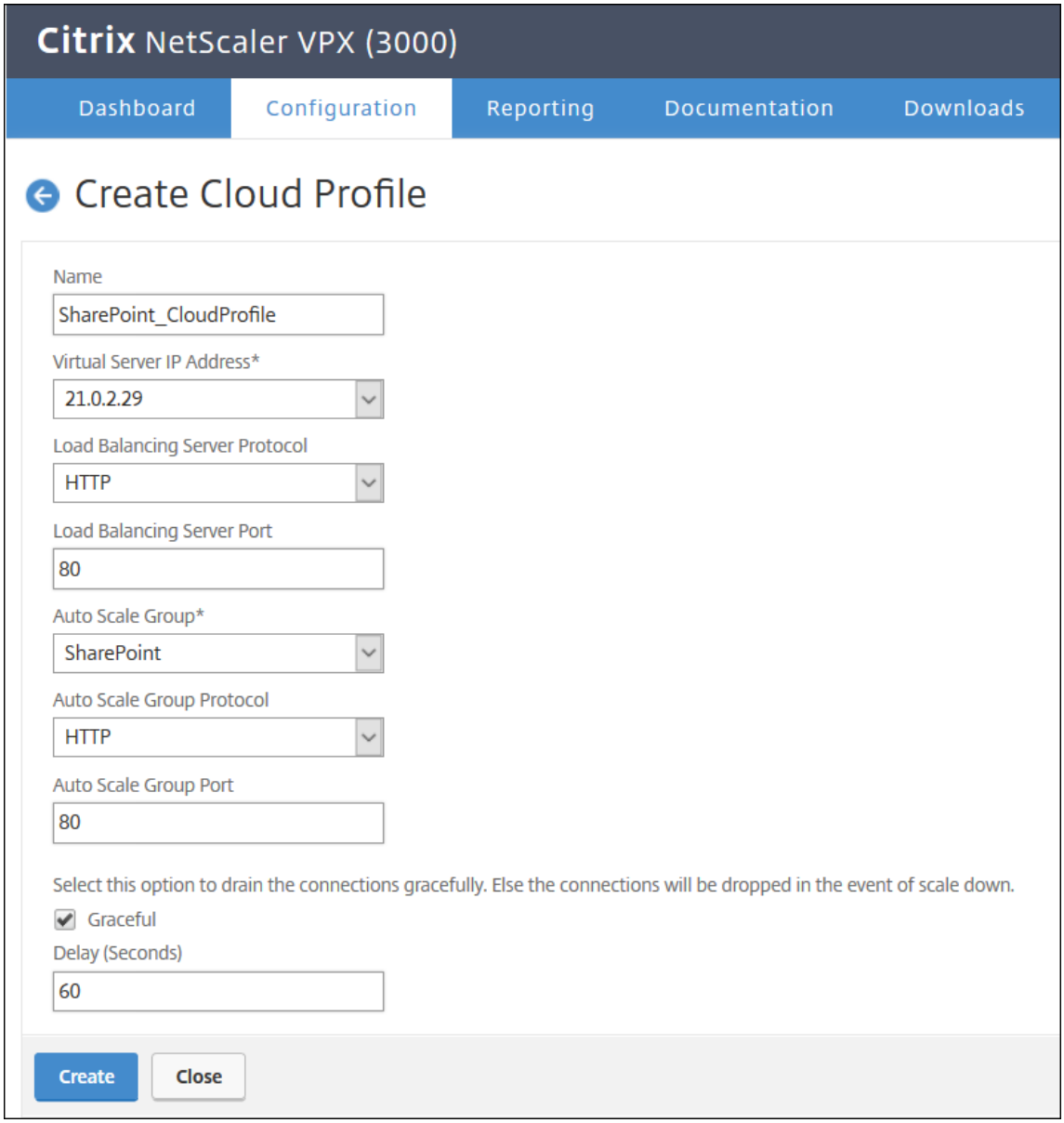
Abbildung: Seite Standard-Cloud-Profil



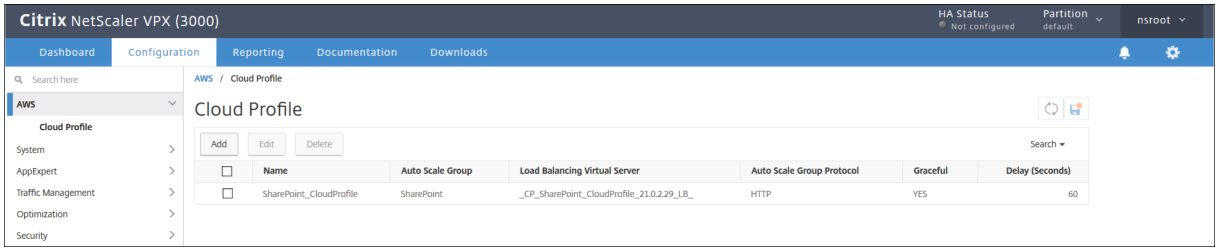
3. Wenn Sie nach der ersten Anmeldung ein Cloud-Profil erstellen möchten, gehen Sie auf der GUI zu **System > AWS > Cloud-Profil** und klicken Sie auf **Hinzufügen**.



Die Seite **Cloud-Profil erstellen** wird angezeigt.



Cloud Profile erstellt einen virtuellen Citrix ADC Load Balancing Server und eine Dienstgruppe mit Mitgliedern als Server der Autoscaling-Gruppe. Ihre Back-End-Server müssen über das auf der VPX-Instanz konfigurierte SNIP erreichbar sein.



> **Hinweis:**
>
> Um AutoScale-bezogene Informationen in der AWS-Konsole anzuzeigen, gehen Sie zu **EC2** > **Dashboard** > **Auto Scaling** > **Auto Scaling Group** .

Konfigurieren einer Citrix ADC VPX-Instanz für die Verwendung der SR-IOV-Netzwerkschnittstelle

October 5, 2021

> **Hinweis:**
>
> Unterstützung für SR-IOV-Schnittstellen in einem Hochverfügbarkeitssetup ist ab Citrix ADC Version 12.0 57.19 verfügbar.

Nachdem Sie eine Citrix ADC VPX-Instanz in AWS erstellt haben, können Sie die virtuelle Appliance mithilfe der AWS CLI für die Verwendung von SR-IOV-Netzwerkschnittstellen konfigurieren.

In allen Citrix ADC VPX-Modellen, außer Citrix ADC VPX AWS Marketplace Editions von 3G und 5G, ist SR-IOV in der Standardkonfiguration einer Netzwerkschnittstelle nicht aktiviert.

Bevor Sie mit der Konfiguration beginnen, lesen Sie die folgenden Themen:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien

Dieser Abschnitt enthält die folgenden Themen:

- Ändern des Schnittstellentyps in SR-IOV
- Konfigurieren von SR-IOV auf einem Hochverfügbarkeitssetup

Ändern Sie den Schnittstellentyp in SR-IOV

Sie können den Befehl show interface summary ausführen, um die Standardkonfiguration einer Netzwerkschnittstelle zu überprüfen.

Beispiel 1: Die folgende CLI-Bildschirmaufnahme zeigt die Konfiguration einer Netzwerkschnittstelle, bei der SR-IOV standardmäßig in Citrix ADC VPX AWS Marketplace Editions von 3G und 5G aktiviert ist.

```
> show interface summary
-------------------------------------------------------------------------
     Interface  MTU       MAC                Suffix
-------------------------------------------------------------------------
1      1/1      1500      0a:1e:2e:17:a2:37  Intel 82599 10G VF Interface
2      LO/1     1500      0a:1e:2e:17:a2:37  Netscaler Loopback interface
 Done
```


Beispiel 2: Die folgende CLI-Bildschirmaufnahme zeigt die Standardkonfiguration einer Netzwerkschnittstelle, bei der SR-IOV nicht aktiviert ist.

```
 Done
> sh int s
-------------------------------------------------------------------------------
      Interface  MTU        MAC                Suffix
-------------------------------------------------------------------------------
1     1/1        1500       12:fc:04:c5:d0:12  NetScaler Virtual Interface
2     LO/1       1500       12:fc:04:c5:d0:12  Netscaler Loopback interface
 Done
>
```

Weitere Informationen zum Ändern des Schnittstellentyps in SR-IOV finden Sie unterhttp://docs.aws.amazon.com/AWSEC2/latest/UserGuide/sriov-networking.html

So ändern Sie den Schnittstellentyp in SR-IOV

1. Fahren Sie die Citrix ADC VPX-Instanz herunter, die auf AWS ausgeführt wird.
2. Um SR-IOV auf der Netzwerkschnittstelle zu aktivieren, geben Sie den folgenden Befehl in der AWS CLI ein.

   ```
   $ aws ec2 modify-instance-attribute --instance-id \<instance\\_id\> --sriov-net-support simple
   ```

3. Um zu überprüfen, ob SR-IOV aktiviert wurde, geben Sie den folgenden Befehl in der AWS CLI ein.

   ```
   $ aws ec2 describe-instance-attribute --instance-id \<instance\\_id\> --attribute sriovNetSupport
   ```

   Beispiel 3: Der Netzwerkschnittstellentyp wurde unter Verwendung der AWS CLI in SR-IOV geändert.

   ```
   aws ec2 modify-instance-attribute --instance-id i-008c1230aaf303bee --sriov-net-support simple
   aws ec2 describe-instance-attribute --instance-id  i-008c1230aaf303bee  --attribute sriovNetSupport
   {
       "InstanceId": "i-008c1230aaf303bee",
       "SriovNetSupport": {
           "Value": "simple"
       }
   }
   ```

   Wenn SR-IOV nicht aktiviert ist, ist der Wert für SRIOVNetSupport nicht vorhanden.

   Beispiel 4: Im folgenden Beispiel ist die SR-IOV-Unterstützung nicht aktiviert.


```
{
    "InstanceId": "i-0c3e84cfa65b04cc8",
    "SriovNetSupport": {}
}
```

4. Schalten Sie die VPX-Instanz ein. Um den geänderten Status der Netzwerkschnittstelle anzuzeigen, geben Sie “Interface-Zusammenfassung anzeigen” in die CLI ein.

   Beispiel 5: Die folgende Bildschirmaufnahme zeigt die Netzwerkschnittstellen mit aktiviertem SR-IOV. Die Schnittstellen 10/1, 10/2, 10/3 sind SR-IOV aktiviert.

```
> show interface summary
-------------------------------------------------------------------------------
      Interface  MTU       MAC                Suffix
-------------------------------------------------------------------------------
1     10/1       1500      0a:1e:2e:17:a2:37  Intel 82599 10G VF Interface
2     10/2       1500      0a:df:17:0a:fe:83  Intel 82599 10G VF Interface
3     10/3       1500      0a:de:5d:31:bf:c3  Intel 82599 10G VF Interface
4     LO/1       1500      0a:1e:2e:17:a2:37  Netscaler Loopback interface
 Done
```

Mit diesen Schritten wird das Verfahren zum Konfigurieren von VPX-Instanzen für die Verwendung von SR-IOV-Netzwerkschnittstellen abgeschlossen.

Konfigurieren von SR-IOV für ein Hochverfügbarkeitssetup

Hochverfügbarkeit wird mit SR-IOV-Schnittstellen ab Citrix ADC Version 12.0 Build 57.19 unterstützt.

Wenn das Hochverfügbarkeitssetup manuell oder mithilfe der Citrix CloudFormation-Vorlage für Citrix ADC ab Version 12.0 56.20 bereitgestellt wurde, muss die IAM-Rolle, die dem Hochverfügbarkeitssetup zugeordnet ist, über die folgenden Berechtigungen verfügen:

- ec2:DescribeInstanzen
- ec2:DescribeNetworkInterfaces
- ec2:DetachNetworkInterface
- ec2:AttachNetworkInterface
- ec2:StartInstanzen
- ec2:StopInstanzen
- ec2:RebootInstanzen
- autoscaling:*
- sns:*
- sqs:*
- iam:SimulatePrincipalPolicy
- iam:GetRole

Standardmäßig fügt die Citrix CloudFormation-Vorlage für Citrix ADC Version 12.0 57.19 automatisch die erforderlichen Berechtigungen zur IAM-Rolle hinzu.

> **Hinweis:**
>
> Ein Hochverfügbarkeits-Setup mit SR-IOV-Schnittstellen benötigt etwa 100 Sekunden Ausfallzeiten.

Verwandte Ressourcen:

Weitere Informationen zu IAM-Rollen finden Sie in der AWS-Dokumentation.

Konfigurieren einer Citrix ADC VPX-Instanz für die Verwendung von Enhanced Networking mit AWS ENA

October 5, 2021

Nachdem Sie eine Citrix ADC VPX-Instanz in AWS erstellt haben, können Sie die virtuelle Appliance mithilfe von [AWS CLI für die Verwendung von Enhanced Networking with AWS Elastic Network Adapter (ENA)](https://aws.amazon.com/about-aws/whats-new/2016/06/introducing-elastic-network-adapter-ena-the-next-generation-network-interface-for-ec2-instances/)konfigurieren.

In Verbindung mit AWS ENA bietet das erweiterte Netzwerk eine höhere Bandbreite, eine höhere Paketper-Sekunden-Leistung (PPS) und konstant niedrigere Instanz-Latenzen.

Bevor Sie mit der Konfiguration beginnen, lesen Sie die folgenden Themen:

- Voraussetzungen
- Einschränkungen und Nutzungsrichtlinien

Die folgenden HA-Konfigurationen werden für ENA-fähige Instanzen unterstützt:

- Private IP-Adressen können innerhalb derselben Availability Zone verschoben werden.
- Elastische IP-Adressen können über Availability Zones verschoben werden.

Upgrade einer Citrix ADC VPX-Instanz in AWS

October 5, 2021

Sie können den EC2-Instanztyp, den Durchsatz, die Software-Edition und die Systemsoftware eines auf AWS ausgeführten Citrix ADC VPX aktualisieren. Für bestimmte Arten von Upgrades empfiehlt Citrix die Verwendung der High Availability Configuration Methode, um Ausfallzeiten zu minimieren.

> Hinweis:
>
> - Citrix ADC-Softwareversion 10.1.e-124.1308.e oder höher für ein Citrix ADC VPX AMI (einschließlich Dienstprogrammlizenz und Kundenlizenz) unterstützt die Instanzfamilien M1 und M2 nicht.
> - Aufgrund von Änderungen in der VPX-Instanzunterstützung wird ein Downgrade von 10.1.e-124 oder einer höheren Version auf 10.1.123.x oder eine frühere Version nicht unterstützt.
> - Die meisten Upgrades erfordern nicht den Start eines neuen AMI, und das Upgrade kann auf der aktuellen Citrix ADC AMI-Instanz durchgeführt werden. Wenn Sie ein Upgrade auf eine neue Citrix ADC AMI-Instanz durchführen möchten, verwenden Sie die Konfigurationsmethode für hohe Verfügbarkeit.

Ändern des EC2-Instanztyps einer Citrix ADC VPX-Instanz in AWS

Wenn Ihre Citrix ADC VPX-Instanzen Version 10.1.e-124.1308.e oder höher ausgeführt werden, können Sie den EC2-Instanztyp in der AWS-Konsole wie folgt ändern:

1. Stoppen Sie die VPX-Instanz.
2. Ändern Sie den EC2-Instanztyp über die AWS-Konsole.
3. Starten Sie die Instanz.

Sie können das obige Verfahren auch verwenden, um den EC2-Instanztyp für eine Version vor 10.1.e-124.1308.e zu ändern, es sei denn, Sie möchten den Instanztyp in M3 ändern. In diesem Fall müssen Sie zuerst das standardmäßige Citrix ADC-Upgradeverfahren befolgen, um die Citrix ADC-Software auf 10.1.e-124 oder eine spätere Version zu aktualisieren, und dann die obigen Schritte ausführen.

Aktualisieren des Durchsatzes oder der Software-Edition einer Citrix ADC VPX-Instanz auf AWS

Um die Software-Edition (z. B. um von Standard auf Premium Edition zu aktualisieren) oder den Durchsatz (z. B. um von 200 Mbit/s auf 1000 Mbit/s zu aktualisieren), hängt die Methode von der Lizenz der Instanz ab.

Verwendung einer Kundenlizenz (Bring-Your-Own-Lizenz)

Wenn Sie eine Kundenlizenz verwenden, können Sie die neue Lizenz von der Citrix Website erwerben und herunterladen und dann die Lizenz auf der VPX-Instanz installieren. Weitere Informationen zum Herunterladen und Installieren einer Lizenz von der Citrix Website finden Sie im VPX-Lizenzhandbuch.

Verwendung einer Versorgungslizenz (Dienstprogrammlizenz mit Stundengebühr)

AWS unterstützt keine direkten Upgrades für kostenpflichtige Instanzen. Um die Software-Edition oder den Durchsatz einer gebührenbasierten Citrix ADC VPX-Instanz zu aktualisieren, starten Sie ein neues AMI mit der gewünschten Lizenz und Kapazität und migrieren Sie die ältere Instanzkonfiguration auf die neue Instanz. Dies kann erreicht werden, indem eine Citrix ADC-Hochverfügbarkeitskonfiguration verwendet wird, wie unter Upgrade auf eine neue Citrix ADC AMI-Instanz unter Verwendung eines Citrix ADC-Unterabschnitts für hohe Verfügbarkeit auf dieser Seite beschrieben.

Aktualisieren der Systemsoftware einer Citrix ADC VPX-Instanz auf AWS

Wenn Sie eine VPX-Instanz mit 10.1.e-124.1308.e oder einer späteren Version aktualisieren müssen, befolgen Sie das standardmäßige Citrix ADC-Upgradeverfahren beim Upgrade und Downgrade einer Citrix ADC Appliance.

Wenn Sie eine VPX-Instanz mit einer älteren Version als 10.1.e-124.1308.e auf 10.1.e-124.1308.e oder höher aktualisieren müssen, aktualisieren Sie zuerst die Systemsoftware, und ändern Sie dann den Instanztyp wie folgt auf M3:

1. Stoppen Sie die VPX-Instanz.
2. Ändern Sie den EC2-Instanztyp über die AWS-Konsole.
3. Starten Sie die Instanz.

Upgrade auf eine neue Citrix ADC AMI-Instanz mithilfe einer Citrix ADC-Hochverfügbarkeitskonfiguration

Führen Sie die folgenden Aufgaben aus, um die Hochverfügbarkeitsmethode für das Upgrade auf eine neue Citrix ADC AMI-Instanz zu verwenden:

- Erstellen Sie eine neue Instanz mit dem gewünschten EC2-Instanztyp, der Software-Edition, dem Durchsatz oder der Software-Version vom AWS-Marktplatz.
- Konfigurieren Sie die hohe Verfügbarkeit zwischen der alten Instanz (die aktualisiert werden soll) und der neuen Instanz. Nachdem die hohe Verfügbarkeit zwischen der alten und der neuen Instanz konfiguriert wurde, wird die Konfiguration der alten Instanz mit der neuen Instanz synchronisiert.
- Erzwingen Sie ein HA-Failover von der alten Instanz auf die neue Instanz. Infolgedessen wird die neue Instanz primär und beginnt mit dem Empfang von Datenverkehr.
- Beenden Sie, und konfigurieren Sie die alte Instanz neu oder entfernen Sie sie aus AWS.

Zu berücksichtigende Voraussetzungen und Punkte

- Stellen Sie sicher, dass Sie verstehen, wie hohe Verfügbarkeit zwischen zwei Citrix ADC VPX -Instanzen in AWS funktioniert. Weitere Informationen zur Hochverfügbarkeitskonfiguration zwischen zwei Citrix ADC VPX-Instanzen in AWS finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares auf AWS.
- Sie müssen die neue Instanz in derselben Availability Zone wie die alte Instanz erstellen, wobei genau dieselbe Sicherheitsgruppe und dasselbe Subnetz vorhanden sind.
- Die Einrichtung für hohe Verfügbarkeit erfordert Zugriffs- und geheime Schlüssel, die mit dem AWS Identity and Access Management (IAM) -Konto des Benutzers für beide Instanzen verknüpft sind. Wenn beim Erstellen von VPX-Instanzen die richtigen Schlüsselinformationen nicht verwendet werden, schlägt das HA-Setup fehl. Weitere Informationen zum Erstellen eines IAM-Kontos für eine VPX-Instanz finden Sie unter Voraussetzungen.
  - Sie müssen die EC2-Konsole verwenden, um die neue Instanz zu erstellen. Sie können den AWS-1-Click-Start nicht verwenden, da er die Zugriffs- und geheimen Schlüssel nicht als Eingabe akzeptiert.
  - Die neue Instanz muss nur eine ENI-Schnittstelle haben.

Gehen Sie folgendermaßen vor, um eine Citrix ADC VPX-Instanz mithilfe einer Hochverfügbarkeitskonfiguration zu aktualisieren:

1. Konfigurieren Sie die hohe Verfügbarkeit zwischen der alten und der neuen Instanz. Um die Hochverfügbarkeit zwischen zwei Citrix ADC VPX-Instanzen zu konfigurieren, geben Sie an der Eingabeaufforderung jeder Instanz Folgendes ein:

   - `add ha node <nodeID> <IPaddress of the node to be added>`
   - `save config`

   Beispiel:

   Geben Sie an der Eingabeaufforderung der alten Instanz Folgendes ein:

   ```
   1 add ha node 30 192.0.2.30
   2 Done
   3 <!--NeedCopy-->
   ```

   Geben Sie an der Eingabeaufforderung der neuen Instanz Folgendes ein:

   ```
   1 add ha node 10 192.0.2.10
   2 Done
   3 <!--NeedCopy-->
   ```

   Beachten Sie Folgendes:

- Im HA-Setup ist die alte Instanz der primäre Knoten und die neue Instanz der sekundäre Knoten.
- Die NSIP-IP-Adresse wird nicht von der alten Instanz in die neue Instanz kopiert. Daher hat Ihre neue Instanz nach dem Upgrade eine andere Verwaltungs-IP-Adresse als die vorherige.
- Das `nsroot` Kontokennwort der neuen Instanz wird nach der HA-Synchronisierung auf das der alten Instanz festgelegt.

Weitere Informationen zur Hochverfügbarkeitskonfiguration zwischen zwei Citrix ADC VPX-Instanzen in AWS finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares auf AWS.

2. Erzwingen Sie ein HA-Failover. Um ein Failover in einer Hochverfügbarkeitskonfiguration zu erzwingen, geben Sie an der Eingabeaufforderung einer der Instanzen Folgendes ein:

```
1 force HA failover
2 <!--NeedCopy-->
```

Als Ergebnis des Erzwingen eines Failovers werden die ENIs der alten Instanz auf die neue Instanz migriert und der Datenverkehr fließt durch die neue Instanz (den neuen primären Knoten). Die alte Instanz (der neue sekundäre Knoten) wird neu gestartet.

Wenn die folgende Warnmeldung angezeigt wird, geben Sie N ein, um den Vorgang abzubrechen:

```
1 [WARNING]:Force Failover may cause configuration loss, peer health
      not optimum. Reason(s):
2 HA version mismatch
3 HA heartbeats not seen on some interfaces
4 Please confirm whether you want force-failover (Y/N)?
5 <!--NeedCopy-->
```

Die Warnmeldung wird angezeigt, da die Systemsoftware der beiden VPX-Instanzen nicht HA-kompatibel ist. Daher kann die Konfiguration der alten Instanz während eines erzwungenen Failovers nicht automatisch mit der neuen Instanz synchronisiert werden.

Es folgt die Problemumgehung für dieses Problem:

a) Geben Sie an der Citrix ADC -Shell Eingabeaufforderung der alten Instanz den folgenden Befehl ein, um eine Sicherung der Konfigurationsdatei (ns.conf) zu erstellen:

```
copy /nsconfig/ns.conf to /nsconfig/ns.conf.bkp
```

b) Entfernen Sie die folgende Zeile aus der Sicherungskonfigurationsdatei (ns.conf.bkp):

- `set ns config -IPAddress <IP> -netmask <MASK>`

Zum Beispiel `set ns config -IPAddress 192.0.2.10 -netmask 255.255.255.0`

c) Kopieren Sie die Backup-Konfigurationsdatei der alten Instanz (ns.conf.bkp) in das Verzeichnis /nsconfig der neuen Instanz.

d) Geben Sie an der Citrix ADC -Shell Eingabeaufforderung der neuen Instanz den folgenden Befehl ein, um die Konfigurationsdatei der alten Instanz (ns.conf.bkp) auf die neue Instanz zu laden:

- `batch -f /nsconfig/ns.conf.bkp`

e) Speichern Sie die Konfiguration auf der neuen Instanz.

- `save conifg`

f) Geben Sie an der Eingabeaufforderung eines der Knoten den folgenden Befehl ein, um ein Failover zu erzwingen, und geben Sie dann Y für die Warnmeldung ein, um den Failover-Vorgang zu bestätigen:

- `force ha failover`

Beispiel:

```
1         > force ha failover
2
3 WARNING]:Force Failover may cause configuration loss, peer health
     not optimum.
4         Reason(s):
5         HA version mismatch
6         HA heartbeats not seen on some interfaces
7         Please confirm whether you want force-failover (Y/N)? Y
8 <!--NeedCopy-->
```

3. Entfernen Sie die HA-Konfiguration, sodass sich die beiden Instanzen nicht mehr in einer HA-Konfiguration befinden. Entfernen Sie zuerst die HA-Konfiguration vom sekundären Knoten, und entfernen Sie dann die HA-Konfiguration vom primären Knoten.

   Um eine HA-Konfiguration zwischen zwei Citrix ADC VPX-Instanzen zu entfernen, geben Sie an der Eingabeaufforderung jeder Instanz Folgendes ein:

```
1     > remove ha node <nodeID>
2     >  save config
3 <!--NeedCopy-->
```


Weitere Informationen zur Hochverfügbarkeitskonfiguration zwischen zwei VPX-Instanzen in AWS finden Sie unter Bereitstellen eines Hochverfügbarkeitspaares auf AWS.

Beispiel:

Geben Sie an der Eingabeaufforderung der alten Instanz (neuer sekundärer Knoten) Folgendes ein:

```
1          > remove ha node 30
2            Done
3          > save config
4            Done
5  <!--NeedCopy-->
```

Geben Sie an der Eingabeaufforderung der neuen Instanz (neuer Primärknoten) Folgendes ein:

```
1          > remove ha node 10
2            Done
3          > save config
4            Done
5  <!--NeedCopy-->
```

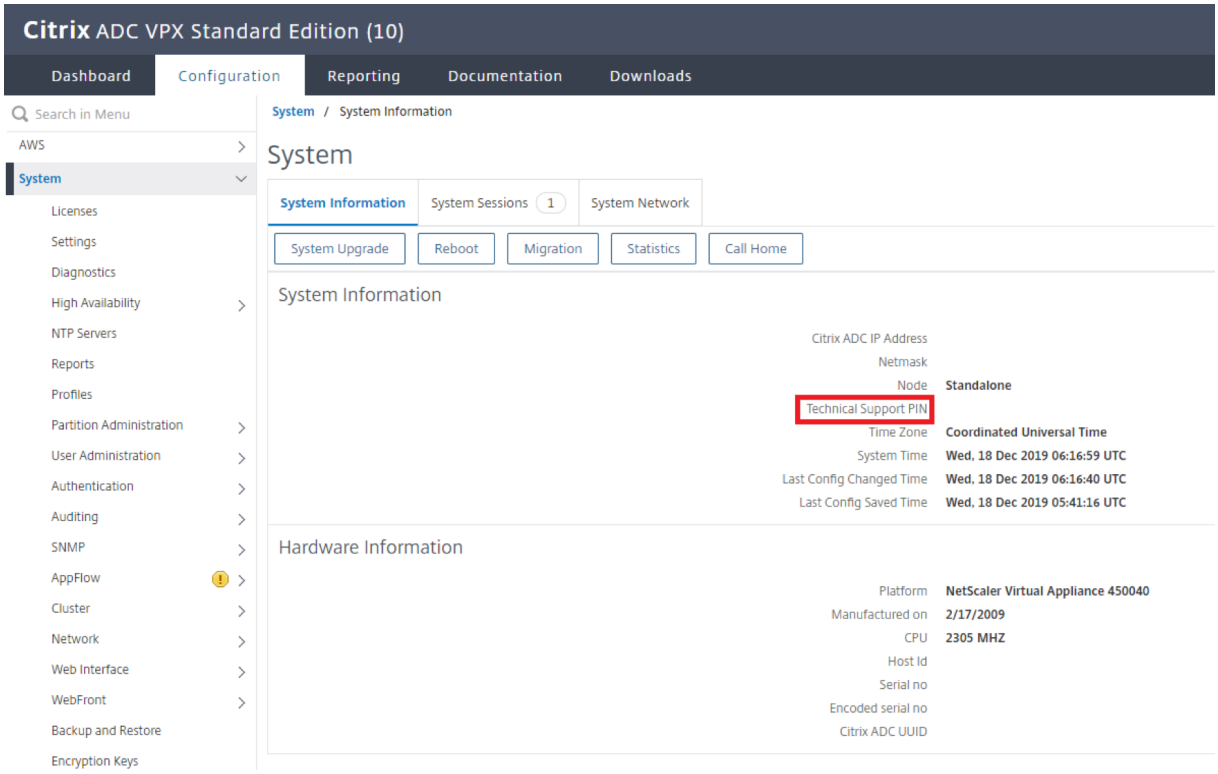
Problembehandlung bei einer VPX-Instanz in AWS

October 5, 2021

Amazon bietet keinen Konsolenzugriff auf eine Citrix ADC VPX-Instanz. Zur Fehlerbehebung müssen Sie die AWS GUI verwenden, um das Aktivitätsprotokoll anzuzeigen. Sie können nur debuggen, wenn das Netzwerk verbunden ist. Um das Systemprotokoll einer Instanz anzuzeigen, klicken Sie mit der rechten Maustaste auf die Instanz und wählen Sie Systemprotokoll

Citrix bietet Unterstützung für AWS Marketplace-lizenzierte Citrix ADC VPX-Instanzen (Dienstprogrammlizenz mit Stundengebühr) auf AWS. Um einen Support-Fall zu erstellen, suchen Sie Ihre AWS-Kontonummer und Ihren Support-PIN-Code und rufen Sie den Citrix Support an. Sie werden auch nach Ihrem Namen und Ihrer E-Mail-Adresse gefragt. Um die Support-PIN zu finden, melden Sie sich bei der VPX-GUI an und navigieren Sie zur Seite System.

Hier ist ein Beispiel für eine Systemseite, die die Support-PIN zeigt.



Häufig gestellte Fragen zu AWS

February 24, 2022

- **Unterstützt eine Citrix ADC VPX Instanz die verschlüsselten Volumes in AWS?**

  Verschlüsselung und Entschlüsselung erfolgen auf Hypervisor Ebene und funktioniert daher nahtlos mit jeder Instanz. Weitere Informationen zu den verschlüsselten Volumes finden Sie im folgenden AWS-Dokument:

  https://docs.aws.amazon.com/kms/latest/developerguide/services-ebs.html

- **Was ist der beste Weg, um die Citrix ADC VPX Instanz in AWS bereitzustellen?**

  Sie können eine Citrix ADC VPX Instanz in AWS auf eine der folgenden Arten bereitstellen:

  - AWS CloudFormation-Vorlage (CFT) in der AWS-Marketplace-Site
  - Citrix ADM
  - AWS Schnellstarts
  - Citrix AWS CFTs in GitHub
  - Citrix Terraform-Skripts in GitHub
  - Citrix Ansible Playbooks in GitHub
  - AWS EC2-Start-Workflow

Sie können eine der aufgelisteten Optionen basierend auf dem von Ihnen verwendeten Automatisierungswerkzeug auswählen.

Weitere Informationen zu den Optionen finden Sie unter Citrix ADC VPX on AWS.

- **Wie aktualisiere ich die Citrix ADC VPX Instanz in AWS?**

  Um die Citrix ADC VPX-Instanz in AWS zu aktualisieren, können Sie die Systemsoftware aktualisieren oder auf ein neues Citrix ADC VPX Amazon Machine Image (AMI) aktualisieren, indem Sie das Verfahren unter Upgrade einer Citrix ADC VPX-Instanz auf AWSbefolgen.

  Die empfohlene Möglichkeit, eine Citrix ADC VPX-Instanz zu aktualisieren, besteht darin, den ADM-Dienst zu verwenden, indem Sie das Verfahren unter Verwenden von Jobs zum Upgrade von Citrix ADC-Instanzenbefolgen.

- **Wie hoch ist die HA-Failover-Zeit für Citrix ADC VPX in AWS?**

  - Das HA-Failover von Citrix ADC VPX innerhalb der AWS Availability Zone dauert etwa 3 Sekunden.
  - Das HA-Failover von Citrix ADC VPX in AWS-Verfügbarkeitszonen dauert etwa 5 Sekunden.

- **Welchen Support erhalten Kunden des Citrix ADC VPX Marketplace-Abonnements, die die PIN für den technischen Support bereitstellen?**

  Standardmäßig wird der Dienst “Für Software auswählen” Kunden zur Verfügung gestellt, die die PIN für den technischen Support bereitstellen.

- **Müssen wir bei Hochverfügbarkeit in verschiedenen Zonen mithilfe der Elastic IP-Bereitstellung mehrere IPSets für jede Anwendung erstellen?**

  Ja. Wenn es mehrere Anwendungen mit mehreren VIPs gibt, die mehreren EIPs zugeordnet sind, sind mehrere IPSets erforderlich. Daher werden während des HA-Failovers alle primären VIP-Zuordnungen von EIPs in sekundäre (neue primäre) VIPs geändert.

- **Warum ist der INC-Modus bei hoher Verfügbarkeit für verschiedene Zonenbereitstellungen aktiviert?**

  HA-Paare in allen Availability Zones befinden sich in verschiedenen Netzwerken. Für die HA-Synchronisation darf die Netzwerkkonfiguration nicht synchronisiert werden. Dies wird erreicht, indem der INC-Modus für ein HA-Paar aktiviert wird.

- **Kann der HA-Knoten in einer Availability Zone mit Back-End-Servern in einer anderen Availability Zone kommunizieren, vorausgesetzt, diese Verfügbarkeitszonen befinden sich in derselben VPC?**

  Ja, Subnetze in verschiedenen Availability Zones derselben VPC sind erreichbar, indem eine zusätzliche Route hinzugefügt wird, die über SNIP auf das Backend-Server-Subnetz verweist. Wenn das SNIP-Subnetz von ADC in AZ1 beispielsweise 192.168.3.0/24 ist und das

Backend-Server-Subnetz in AZ2 192.168.6.0/24 ist, muss eine Route in der Citrix ADC Appliance hinzugefügt werden, die in AZ1 als 192.168.6.0 255.255.255.0 192.168.3.1 vorhanden ist.

- **Kann Hochverfügbarkeit über verschiedene Zonen mit Elastic IP und High Availability in verschiedenen Zonen über private IP-Bereitstellungen hinweg zusammenarbeiten?**

  Ja, beide Konfigurationen können auf dasselbe HA-Paar angewendet werden.

- **Wie weiß ein sekundärer Knoten im HA-Paar bei Hochverfügbarkeit in verschiedenen Zonen mit privaten IP-Bereitstellung, wenn mehrere Subnetze mit mehreren Routentabellen in einer VPC vorhanden sind, von der Routing-Tabelle Bescheid, die während des HA-Failovers überprüft werden soll?**

  Der sekundäre Knoten kennt die primären NICs und sucht in allen Routing-Tabellen in einer VPC.

- **Wie groß ist die Partition `/var`, wenn das Standardimage für VPX in AWS verwendet wird? Wie erhöht man den Speicherplatz?**

  Die Größe des Rootdatenträgers ist auf 20 GB begrenzt, um das Datenträgerimage klein zu halten.

  Wenn Sie den Verzeichnisspeicher für `/var/core/` oder `/var/crash/` vergrößern möchten, hängen Sie einen zusätzlichen Datenträger an. Um die Größe von `/var` zu erhöhen, müssen Sie derzeit einen zusätzlichen Datenträger anhängen und einen symbolischen Link zu `/var` erstellen, nachdem Sie den kritischen Inhalt auf den neuen Datenträger kopiert haben.

- **Wie viele Paket-Engines werden aktiviert und vCPUs zugewiesen?**

  Die Paket-Engines (PEs) sind durch die Anzahl der lizenzierten vCPUs begrenzt. Die Citrix ADC Daemons sind nicht an eine bestimmte vCPU angeheftet und werden möglicherweise auf einem der vCPUs ohne PE ausgeführt. Laut AWS ist der C5.9XLarge eine 36VCPU-Instanz mit 72 GB Speicher. Bei der gepoolten Lizenzierung wird die Citrix ADC VPX-Instanz mit der maximalen Anzahl von PEs bereitgestellt. In diesem Fall laufen 19 PEs auf Kernen 1 bis 19. ADC-Managementprozesse laufen jedoch von CPUs 20 bis 31 aus.

- **Wie entscheide ich die richtige AWS-Instanz für ADC?**

  1. Verstehen Sie Ihren Anwendungsfall und Ihre Anforderungen wie Durchsatz, PPS, SSL-Anforderungen und durchschnittliche Paketgröße.
  2. Wählen Sie das richtige ADC-Angebot und die richtige Lizenzierung für ADC, die Ihren Anforderungen entspricht, wie VPX-Bandbreitenangebote oder vCPU-basierte Lizenzierung.
  3. Entscheiden Sie sich basierend auf dem gewählten Angebot für die AWS-Instanz.

  Beispiel:

  Eine 5-Gbit/s-Lizenz ermöglicht 5 Datenpaket-Engines. Daher ist die vCPU-Anforderung 6 (5+1 für die Verwaltung). 6 vCPU-Instanz ist jedoch nicht verfügbar. Eine 8 vCPU ist also gut genug,

um diesen Durchsatz zu erreichen, vorausgesetzt, Sie wählen ein Netzwerk, das 5 Gbit/s Bandbreite unterstützt. Zum Beispiel müssen Sie m5.2xlarge für eine 5-Gbit/s-Bandbreitenlizenz wählen, um die maximale PE-Zuweisung für eine 5-Gbit/s-Lizenz zu ermöglichen. Wenn Sie jedoch eine vCPU-Lizenz verwenden, die nicht durch den Durchsatz begrenzt ist, erhalten Sie möglicherweise einen Durchsatz von 5 Gbit/s mithilfe der m5.xlarge-Instanz selbst.

Instance Size	vCPU	Memory (GiB)	Instance Storage (GiB)	Network Bandwidth (Gbps)	EBS Bandwidth (Mbps)
m5.large	2	8	EBS-Only	Up to 10	Up to 4,750
m5.xlarge	4	16	EBS-Only	Up to 10	Up to 4,750
m5.2xlarge	8	32	EBS-Only	Up to 10	Up to 4,750
m5.4xlarge	16	64	EBS-Only	Up to 10	4,750

- **Ist die Bereitstellung von drei NICs-drei Subnetzen für ADC in AWS obligatorisch**?

  `Three NICs-three subnets` ist die empfohlene Bereitstellung, bei der jede für Management-, Client- und Server-Netzwerk verwendet wird. Diese Bereitstellung bietet eine bessere Verkehrsisolation und VPX-Leistung. Zwei NICS-zwei Subnetze und ein NIC-One-Subnetz sind die anderen verfügbaren Optionen. Citrix empfiehlt nicht, dass mehrere Netzwerkkarten ein Subnetz in AWS teilen, z. B. zwei NICs - eine Subnetzbereitstellung. Weil dies zu Netzwerkproblemen wie asymmetrischem Routing führen kann. Weitere Informationen finden Sie unter Best Practices zum Konfigurieren von Netzwerkschnittstellen in AWS.

Bereitstellen einer Citrix ADC VPX-Instanz auf Microsoft Azure

January 25, 2022

Wenn Sie eine Citrix ADC VPX-Instanz in Microsoft Azure Resource Manager (ARM) bereitstellen, können Sie beide der folgenden Feature-Sets verwenden, um Ihre Geschäftsanforderungen zu erfüllen:

- Azure Cloud Computing-Funktionen
- Funktionen für Citrix ADC Load Balancing und Traffic Management

Sie können Citrix ADC VPX-Instanzen auf ARM entweder als eigenständige Instanzen oder als Hochverfügbarkeitspaare im aktiven Standby-Modus bereitstellen.

Sie können eine Citrix ADC VPX-Instanz auf Microsoft Azure auf zwei Arten bereitstellen:

- Über Azure Marketplace. Citrix ADC VPX ist eine virtuelle Appliance, die als Image in Microsoft Azure Marketplace zur Verfügung steht.
- Verwenden der JSON-Vorlage Citrix ADC Azure Resource Manager (ARM), die auf GitHub verfügbar ist. Weitere Informationen finden Sie im GitHub-Repository für Citrix NetScaler Lösungsvor-

lagen.

Der Microsoft Azure-Stack ist eine integrierte Plattform für Hardware und Software, die die Public Cloud-Dienste von Microsoft Azure in einem lokalen Rechenzentrum bereitstellt, damit Unternehmen Hybrid-Clouds erstellen können. Sie können jetzt die Citrix ADC VPX-Instanzen auf dem Microsoft Azure-Stack bereitstellen.

Voraussetzung

Sie benötigen einige Voraussetzungskenntnisse, bevor Sie eine Citrix VPX-Instanz auf Azure bereitstellen.

- Vertrautheit mit Azure-Terminologie und Netzwerkdetails. Weitere Informationen finden Sie unter Azure-Terminologie.
- Kenntnisse einer Citrix ADC-Appliance. Ausführliche Informationen zur Citrix ADC-Appliance finden Sie unter Citrix ADC
- Kenntnisse über Citrix ADC Netzwerke. Weitere Informationen finden Sie im Thema Netzwerk .

Funktionsweise einer Citrix ADC VPX-Instanz in Azure

In einer on-premises Bereitstellung benötigt eine Citrix ADC VPX-Instanz mindestens drei IP-Adressen:

- Verwaltungs-IP-Adresse, NSIP-Adresse genannt
- Subnetz-IP (SNIP) -Adresse für die Kommunikation mit der Serverfarm
- Virtual Server IP (VIP) Adresse für die Annahme von Clientanforderungen

Weitere Informationen finden Sie unter Netzwerkarchitektur für Citrix ADC VPX-Instanzen auf Microsoft Azure.

> **Hinweis**
>
> Virtuelle VPX Appliances können auf jedem Instanztyp bereitgestellt werden, der über zwei oder mehr Intel VT-X-Kerne und mehr als 2 GB Speicher verfügt. Weitere Informationen zu den Systemanforderungen finden Sie unter Datenblatt zu Citrix ADC VPX. Derzeit unterstützt die Citrix ADC VPX-Instanz nur die Intel-Prozessoren.

In einer Azure-Bereitstellung können Sie eine Citrix ADC VPX-Instanz in Azure auf drei Arten bereitstellen:

- Multi-NC-Multi-IP-Architektur
- Multi-IP-Architektur einer einzelnen NIC
- Einzelne Netzwerk-Einzel-IP

Je nach Bedarf können Sie jeden dieser unterstützten Architekturtypen verwenden.

Multi-NC-Multi-IP-Architektur

Bei diesem Bereitstellungstyp können Sie mehrere Netzwerkschnittstellen (NICs) an eine VPX-Instanz anschließen. Jede NIC kann eine oder mehrere IP-Konfigurationen haben - statische oder dynamische öffentliche und private IP-Adressen, die ihr zugewiesen sind.

Weitere Informationen finden Sie in den folgenden Anwendungsfällen:

- Konfigurieren eines Hochverfügbarkeitssetups mit mehreren IP-Adressen und NICs
- Konfigurieren eines Hochverfügbarkeits-Setups mit mehreren IP-Adressen und NICs mithilfe von PowerShell-Befehlen

> Hinweis
>
> Um MAC-Verschiebungen und Stummschaltung der Benutzeroberfläche in Azure-Umgebungen zu vermeiden, empfiehlt Citrix, ein VLAN pro Datenschnittstelle (ohne Tag) der ADC VPX-Instanz zu erstellen und die primäre IP der NIC in Azure zu binden. Weitere Informationen finden Sie im Artikel CTX224626 .

Multi-IP-Architektur einer einzelnen NIC

Bei diesem Bereitstellungstyp ist eine Netzwerkschnittstellen (NIC) mit mehreren IP-Konfigurationen verknüpft - statische oder dynamische öffentliche und private IP-Adressen, die ihr zugewiesen sind. Weitere Informationen finden Sie in den folgenden Anwendungsfällen:

- Konfigurieren mehrerer IP-Adressen für eine eigenständige Citrix ADC VPX-Instanz
- Konfigurieren Sie mehrere IP-Adressen für eine eigenständige Citrix ADC VPX-Instanz mithilfe von PowerShell-Befehlen

Einzelne Netzwerk-Einzel-IP

Bei diesem Bereitstellungstyp ist eine Netzwerkschnittstellen (NIC) mit einer einzigen IP-Adresse verknüpft, die zur Ausführung der Funktionen von NSIP, SNIP und VIP verwendet wird.

Weitere Informationen finden Sie im folgenden Anwendungsfall:

- Konfigurieren einer eigenständigen Citrix ADC VPX-Instanz

> **Hinweis**
>
> Der einzelne IP-Modus ist nur in Azure-Bereitstellungen verfügbar. Dieser Modus ist für eine Citrix ADC VPX-Instanz in Ihren Räumlichkeiten, in AWS oder in einer anderen Art von Bereitstellung nicht verfügbar.

Citrix ADC VPX-Lizenzierung

Eine Citrix ADC VPX-Instanz auf Azure benötigt eine Lizenz. Die folgenden Lizenzierungsoptionen sind für Citrix ADC VPX-Instanzen verfügbar, die auf Azure ausgeführt werden.

- **Abonnementbasierte Lizenzierung**: Citrix ADC VPX Appliances sind als kostenpflichtige Instanzen auf Azure Marketplace verfügbar. Die abonnementbasierte Lizenzierung ist eine Pay-as-you-go-Option. Benutzer werden stündlich berechnet. Die folgenden VPX-Modelle und Lizenztypen sind auf Azure Marketplace verfügbar.

VPX-Modell	Lizenztyp	Die empfohlene Instanz
VPX10	Standard, Fortgeschritten, Premium	Standard_D2s_v4
VPX200	Standard, Fortgeschritten, Premium	Standard_D2s_v4
VPX1000*	Standard, Fortgeschritten, Premium	Standard_D4s_v4
VPX3000*	Standard, Fortgeschritten, Premium	Standard_D4s_v4

> *: Für Modelle mit VPX 1000 und VPX 3000 müssen Sie Accelerated Networking auf Citrix ADC VPX-Instanzen aktivieren, um die gewünschte Leistung zu erzielen. Weitere Informationen zum Konfigurieren des beschleunigten Netzwerks finden Sie unter Konfigurieren einer Citrix ADC VPX-Instanz für die Verwendung des beschleunigten Azure-Netzwerks.

Citrix bietet technischen Support für abonnementbasierte Lizenzinstanzen. Informationen zum Einreichen eines Supportfalls finden Sie unter Unterstützung für Citrix ADC auf Azure — Abonnementlizenz mit Stundenpreis.

- **Bringen Sie Ihre eigene Lizenz (BYOL**) mit: Wenn Sie Ihre eigene Lizenz (BYOL) mitbringen, lesen Sie den VPX Licensing Guide unter http://support.citrix.com/article/CTX122426. Sie müssen:
  - Verwenden Sie das Lizenzportal auf der Citrix Website, um eine gültige Lizenz zu generieren.
  - Laden Sie die Lizenz auf die Instanz hoch.

VPX-Modell	Lizenztyp	Die empfohlene Instanz
VPX10	Standard, Fortgeschritten, Premium	Standard_D2s_v4

VPX-Modell	Lizenztyp	Die empfohlene Instanz
VPX200	Standard, Fortgeschritten, Premium	Standard_D2s_v4
VPX1000*	Standard, Fortgeschritten, Premium	Standard_D4s_v4
VPX3000*	Standard, Fortgeschritten, Premium	Standard_D4s_v4
VPX5000*	Standard, Fortgeschritten, Premium	Standard_D8s_v4
VPX8000*	Standard, Fortgeschritten, Premium	Standard_D8s_v4
VPX10000*	Standard, Fortgeschritten, Premium	Standard_D16s_v4

> *: Von VPX 1000- bis VPX 10000-Modellen müssen Sie Accelerated Networking auf Citrix ADC VPX-Instanzen aktivieren, um die gewünschte Leistung zu erzielen. Weitere Informationen zum Konfigurieren des beschleunigten Netzwerks finden Sie unter Konfigurieren einer Citrix ADC VPX-Instanz für die Verwendung des beschleunigten Azure-Netzwerks.

- **Citrix ADC VPX Check-In/Auschecken Lizenzierung**: Weitere Informationen finden Sie unter Citrix ADC VPX Check-In/Auschecken Lizenzierung.

> **Hinweis**
>
> In einer Azure-Stack-Umgebung ist **BYOL** die einzig verfügbare Lizenzierungsoption.

Ab NetScaler Version 12.0 56.20 erfordert VPX Express für lokale und Cloud-Bereitstellungen keine Lizenzdatei. Weitere Informationen zu Citrix ADC VPX Express finden Sie im Abschnitt “Citrix ADC VPX Express-Lizenz” in der Übersicht über die Citrix ADC Lizenzierung.

> **Hinweis**
>
> Unabhängig von der abonnementbasierten Stundenlizenz, die von Azure Marketplace gekauft wurde, wird in seltenen Fällen die Citrix ADC VPX Instanz, die in Azure bereitgestellt wird, möglicherweise mit einer standardmäßigen Citrix ADC-Lizenz geliefert. Dies geschieht aufgrund von Problemen mit dem Azure Instance Metadata Service (IMDS).
>
> Führen Sie einen Warmstart durch, bevor Sie eine Konfigurationsänderung an der Citrix ADC VPX-Instanz vornehmen, um die richtige Citrix ADC VPX-Lizenz zu aktivieren.

Einschränkungen

Das Ausführen der Citrix ADC VPX Load Balancing-Lösung unter ARM birgt die folgenden Einschränkungen:

- Die Azure-Architektur unterstützt die folgenden NetScaler-Funktionen nicht:
  - IPv6
  - Unentgeltliches ARP (GARP)
  - L2-Modus
  - Getagged VLAN
  - Dynamisches Routing
  - virtueller MAC
  - USIP
  - Jumbo Frames
  - Clustering

  > Hinweis
  >
  > Mit der Autoscale-Funktion für Citrix Application Delivery Management (ADM) (Cloud-Bereitstellung) unterstützen die ADC-Instanzen das Clustering auf allen Lizenzen. Weitere Informationen finden Sie unter Autoscaling von Citrix ADC VPX in Microsoft Azure mit Citrix ADM.

- Wenn Sie erwarten, dass Sie die virtuelle Citrix ADC VPX-Maschine jederzeit herunterfahren und vorübergehend freigeben müssen, weisen Sie beim Erstellen der virtuellen Maschine eine statische interne IP-Adresse zu. Wenn Sie keine statische interne IP-Adresse zuweisen, weist Azure der virtuellen Maschine bei jedem Neustart möglicherweise eine andere IP-Adresse zu, und auf die virtuelle Maschine kann nicht zugegriffen werden.
- In einer Azure-Bereitstellung werden nur die folgenden Citrix ADC VPX-Modelle unterstützt: VPX 10, VPX 200, VPX 1000 und VPX 3000. Weitere Informationen finden Sie im Citrix ADC VPX Datenblatt.

  Wenn Sie eine Citrix ADC VPX-Instanz mit einer Modellnummer über VPX 3000 verwenden, ist der Netzwerkdurchsatz möglicherweise nicht der gleiche wie in der Lizenz der Instanz angegeben. Andere Funktionen wie SSL-Durchsatz und SSL-Transaktionen pro Sekunde könnten sich jedoch verbessern.
- Die Bereitstellungs-ID, die von Azure während der Provisioning virtueller Maschinen generiert wird, ist für den Benutzer in ARM nicht sichtbar. Sie können die Bereitstellungs-ID nicht verwenden, um Citrix ADC VPX Appliance auf ARM bereitzustellen.
- Die Citrix ADC VPX-Instanz unterstützt 20 MB/s Durchsatz und Standardedition-Funktionen, wenn sie initialisiert wird.

- Die Citrix ADC VPX-Instanzen auf Azure mit aktiviertem beschleunigtem Netzwerk bieten eine bessere Leistung. Azure-beschleunigtes Netzwerk wird ab Version 13.0 Build 76.x auf Citrix ADC VPX-Instanzen unterstützt. Um beschleunigte Netzwerke auf ADC VPX zu ermöglichen, empfiehlt Citrix, einen Azure-Instanztyp zu verwenden, der beschleunigte Netzwerke unterstützt.
- Für eine XenApp - und XenDesktop Bereitstellung kann ein virtueller VPN-Server auf einer VPX-Instanz in den folgenden Modi konfiguriert werden:
  - Basismodus, in dem der Parameter des virtuellen `ICAOnly` VPN-Servers auf ON eingestellt ist. Der Basismodus funktioniert vollständig auf einer nicht lizenzierten Citrix ADC VPX-Instanz.
  - SmartAccess-Modus, in dem der Parameter des virtuellen `ICAOnly` VPN-Servers auf OFF eingestellt ist. Der SmartAccess Modus funktioniert nur für fünf Citrix ADC AAA-Sitzungsbenutzer auf einer nicht lizenzierten Citrix ADC VPX Instanz.

> **Hinweis**
>
> Um das SmartControl-Feature zu konfigurieren, müssen Sie eine Premium-Lizenz auf die Citrix ADC VPX Instanz anwenden.

Azure-Terminologie

October 5, 2021

Einige der Azure-Begriffe, die in der Citrix ADC VPX Azure-Dokumentation verwendet werden, sind unten aufgeführt.

1. Azure Load Balancer — Azure Load Balancer ist eine Ressource, die eingehenden Datenverkehr auf Computer in einem Netzwerk verteilt. Der Datenverkehr wird auf virtuelle Maschinen verteilt, die in einem Lastausgleichssatz definiert sind. Ein Load Balancer kann extern oder mit dem Internet verbunden sein oder intern sein.
2. Azure Resource Manager (ARM) — ARM ist das neue Verwaltungsframework für Dienste in Azure. Azure Load Balancer wird mit ARM-basierten APIs und Tools verwaltet.
3. Back-End-Adresspool — Dies sind IP-Adressen, die mit der NIC (NIC) der virtuellen Maschine verknüpft sind, auf die die Last verteilt wird.
4. BLOB - Binary Large Object — Jedes binäre Objekt wie eine Datei oder ein Image, das im Azure-Speicher gespeichert werden kann.
5. Front-End-IP-Konfiguration — Ein Azure Load Balancer kann eine oder mehrere Front-End-IP-Adressen enthalten, die auch als virtuelle IPs (VIPs) bezeichnet werden. Diese IP-Adressen dienen als Eindringen für den Datenverkehr.

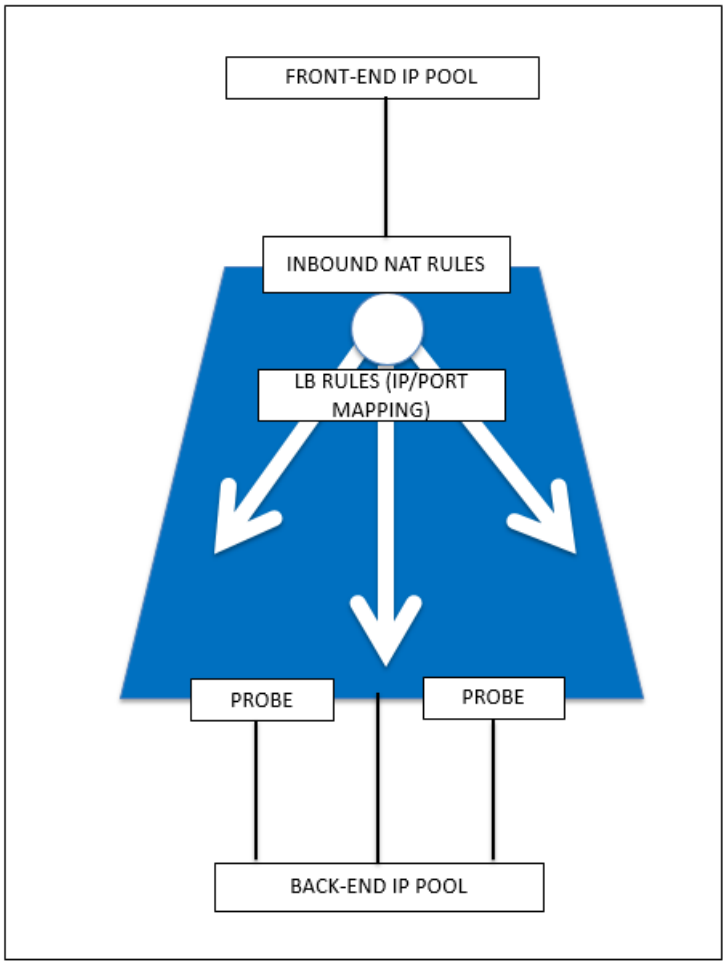
6. Öffentliche IP (ILPIP) auf Instanz-Ebene — Eine ILPIP ist eine öffentliche IP-Adresse, die Sie Ihrer virtuellen Maschine oder Rolleninstanz direkt zuweisen können und nicht dem Clouddienst, in dem sich die virtuelle Maschine oder Rolleninstanz befindet. Dies tritt nicht an die Stelle der VIP (virtuelle IP), die Ihrem Cloud-Dienst zugewiesen ist. Vielmehr handelt es sich um eine zusätzliche IP-Adresse, die Sie verwenden können, um eine direkte Verbindung mit Ihrer virtuellen Maschine oder Rolleninstanz herzustellen.

   Hinweis: In der Vergangenheit wurde ein ILPIP als PIP bezeichnet, was für öffentliches IP steht.

7. Eingehende NAT-Regeln — Dies enthält Regeln, die einen öffentlichen Port auf dem Load Balancer einem Port für eine bestimmte virtuelle Maschine im Back-End-Adresspool zuordnen.

8. IP-config - Es kann als ein IP-Adresspaar (öffentliche IP und private IP) definiert werden, das mit einer einzelnen NIC verknüpft ist. In einer IP-Konfiguration kann die öffentliche IP-Adresse NULL sein. Jeder NIC kann mehrere IP-Konfig zugeordnet sein, was bis zu 255 betragen kann.

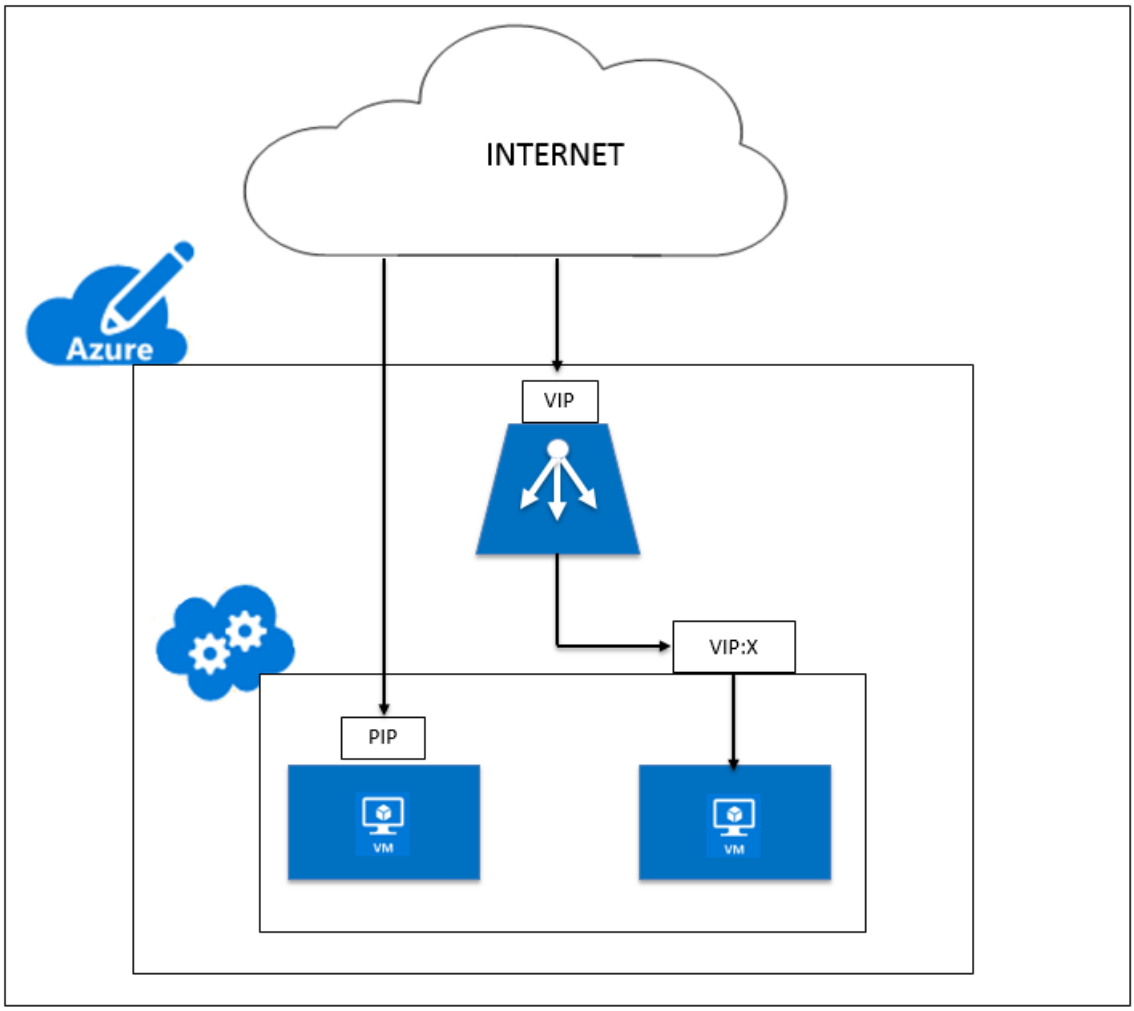
9. Lastenausgleichsregeln — Eine Regeleigenschaft, die eine gegebene Front-End-IP- und Port-Kombination einer Reihe von Back-End-IP-Adressen und einer Portkombination zuordnet. Mit einer einzelnen Definition einer Load Balancer-Ressource können Sie mehrere Load Balancing-Regeln definieren, wobei jede Regel eine Kombination aus Front-End-IP und Port sowie Back-End-IP und Port widerspiegelt, die virtuellen Maschinen zugeordnet sind.



10. Netzwerksicherheitsgruppe — Enthält eine Liste von Zugriffssteuerungslisten (ACL) -Regeln, die den Netzwerkverkehr für Ihre Instanzen der virtuellen Maschine in einem virtuellen Netzwerk zulassen oder verweigern. NSGs können entweder Subnetzen oder einzelnen Instanzen virtueller Maschinen innerhalb dieses Subnetzes zugeordnet werden. Wenn eine Netzwerksicherheitsgruppe mit einem Subnetz verknüpft ist, gelten die ACL-Regeln für alle Instanzen der virtuellen Maschine in diesem Subnetz. Darüber hinaus kann der Datenverkehr zu einer einzelnen virtuellen Maschine weiter eingeschränkt werden, indem eine Netzwerksicherheitsgruppe direkt mit dieser virtuellen Maschine verknüpft wird.

11. Private IP-Adressen — Wird für die Kommunikation innerhalb eines virtuellen Azure-Netzwerks und Ihres lokalen Netzwerks verwendet, wenn Sie ein VPN-Gateway verwenden, um Ihr Netzwerk auf Azure zu erweitern. Private IP-Adressen ermöglichen es Azure-Ressourcen, mit anderen Ressourcen in einem virtuellen Netzwerk oder einem lokalen Netzwerk über ein VPN-Gateway oder eine ExpressRoute-Schaltung zu kommunizieren, ohne eine vom Internet erreichbare IP-Adresse zu verwenden. Im Azure Resource Manager Bereitstellungsmodell ist eine private IP-Adresse den folgenden Arten von Azure-Ressourcen zugeordnet: virtuelle Maschinen, interne Lastausgleichsdienste (ILBs) und Anwendungsgateways.

12. Prüfpunkte — Dies enthält Integritätstprobes, die zur Überprüfung der Verfügbarkeit von Instanzen virtueller Maschinen im Back-End-Adresspool verwendet werden. Wenn eine bestimmte virtuelle Maschine für einige Zeit nicht auf Health Probes reagiert, wird sie aus dem Datenverkehr genommen. Mithilfe von Prüfpunkten können Sie den Zustand virtueller Instanzen verfolgen. Wenn ein Integritätstest fehlschlägt, wird die virtuelle Instanz automatisch aus der Rotation genommen.
13. Öffentliche IP-Adressen (PIP) — PIP wird für die Kommunikation mit dem Internet verwendet, einschließlich öffentlicher Azure-Dienste und ist mit virtuellen Maschinen, mit Internetzugang verbundenen Lastausgleichsdiensten, VPN-Gateways und Anwendungsgateways verknüpft.
14. Region - Ein Gebiet innerhalb einer Geographie, das keine nationalen Grenzen überschreitet und ein oder mehrere Rechenzentren enthält. Preise, regionale Dienstleistungen und Angebotsarten werden auf regionaler Ebene angezeigt. Eine Region wird in der Regel mit einer anderen Region gepaart, die bis zu mehreren hundert Meilen entfernt sein kann, um ein regionales Paar zu bilden. Regionale Paare können als Mechanismus für Disaster Recovery und Hochverfügbarkeitsszenarien verwendet werden. Auch allgemein als Standort bezeichnet.
15. Ressourcengruppe - Ein Container im Ressourcen-Manager enthält zugehörige Ressourcen für eine Anwendung. Die Ressourcengruppe kann alle Ressourcen für eine Anwendung oder nur die Ressourcen enthalten, die logisch zusammengefasst sind.
16. Speicherkonto — Mit einem Azure-Speicherkonto können Sie auf den Azure-BLOB, die Warteschlange, die Tabelle und die Dateidienste in Azure Storage zugreifen. Ihr Speicherkonto stellt den eindeutigen Namespace für Ihre Azure-Speicherdatenobjekte bereit.
17. Virtuelle Maschine — Die Software-Implementierung eines physischen Computers, auf dem ein Betriebssystem ausgeführt wird. Mehrere virtuelle Maschinen können gleichzeitig auf derselben Hardware ausgeführt werden. In Azure sind virtuelle Maschinen in einer Vielzahl von Größen verfügbar.
18. Virtuelles Netzwerk - Ein virtuelles Azure-Netzwerk ist eine Darstellung Ihres eigenen Netzwerks in der Cloud. Es handelt sich um eine logische Isolierung der Azure-Cloud, die Ihrem Abonnement gewidmet ist. Sie können die IP-Adressblöcke, DNS-Einstellungen, Sicherheitsrichtlinien und Routingtabellen in diesem Netzwerk vollständig steuern. Sie können Ihr VNet auch weiter in Subnetze segmentieren und virtuelle Azure IaaS-Maschinen und Clouddienste (PaaS-Rolleninstanzen) starten. Darüber hinaus können Sie das virtuelle Netzwerk mit Ihrem lokalen Netzwerk verbinden, indem Sie eine der in Azure verfügbaren Konnektivitätsoptionen verwenden. Im Wesentlichen können Sie Ihr Netzwerk auf Azure erweitern, mit vollständiger Kontrolle über IP-Adressblöcke mit dem Vorteil, dass Azure Enterprise Scale bietet.



Netzwerkarchitektur für Citrix ADC VPX-Instanzen in Microsoft Azure

October 5, 2021

In Azure Resource Manager (ARM) befindet sich eine virtuelle Citrix ADC VPX Maschine (VM) in einem virtuellen Netzwerk. Eine einzelne Netzwerkschnittstelle kann in einem bestimmten Subnetz des virtuellen Netzwerks erstellt werden und kann an die VPX-Instanz angehängt werden. Sie können den Netzwerkverkehr von und zu einer VPX-Instanz in einem virtuellen Azure-Netzwerk mit einer Netzwerksicherheitsgruppe filtern. Eine Netzwerksicherheitsgruppe enthält Sicherheitsregeln, die eingehenden Netzwerkverkehr zu oder ausgehenden Netzwerkverkehr von einer VPX-Instanz zulassen oder ablehnen. Weitere Informationen finden Sie unter Sicherheitsgruppen.

Die Netzwerksicherheitsgruppe filtert die Anforderungen an die Citrix ADC VPX-Instanz, und die VPX-Instanz sendet sie an die Server. Die Antwort von einem Server folgt dem gleichen Pfad in

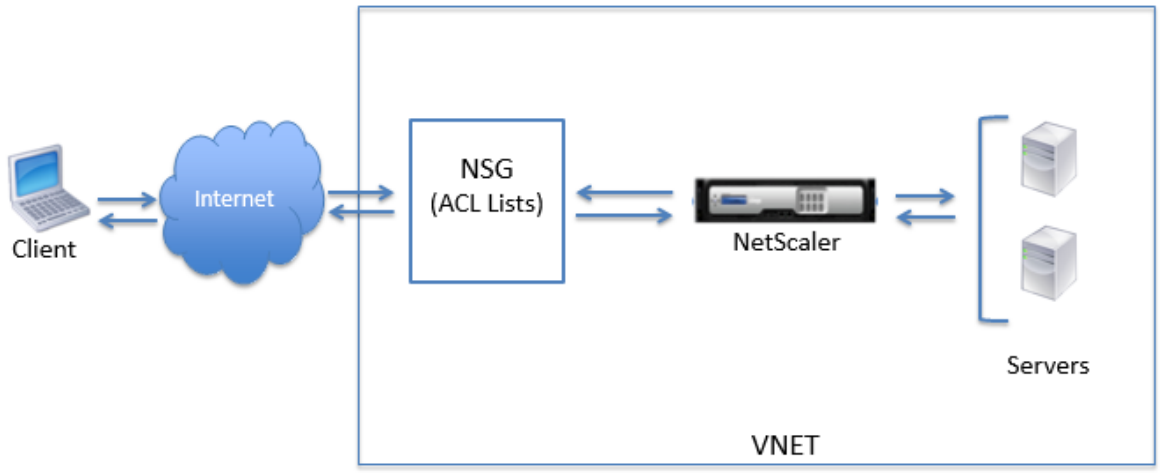
umgekehrter Richtung. Die Netzwerksicherheitsgruppe kann so konfiguriert werden, dass eine einzelne VPX-VM gefiltert wird oder mit Subnetzen und virtuellen Netzwerken Datenverkehr bei der Bereitstellung mehrerer VPX-Instanzen filtert werden kann.

Die NIC enthält Netzwerkkonfigurationsdetails wie das virtuelle Netzwerk, Subnetze, interne IP-Adresse und öffentliche IP-Adresse.

Bei ARM sollten Sie die folgenden IP-Adressen kennen, die für den Zugriff auf die VMs verwendet werden, die mit einer einzelnen Netzwerkkarte und einer einzelnen IP-Adresse bereitgestellt werden:

- Öffentliche IP-Adresse (PIP) ist die IP-Adresse, die direkt auf der virtuellen Netzwerkkarte der NetScaler VM konfiguriert wurde. Auf diese Weise können Sie direkt über das externe Netzwerk auf eine VM zugreifen.
- Die Citrix ADC IP (auch NSIP genannt) Adresse ist die interne IP-Adresse, die auf der VM konfiguriert ist. Es ist nicht routingfähig.
- Die virtuelle IP-Adresse (VIP) wird mithilfe des NSIP und einer Portnummer konfiguriert. Clients greifen über die PIP-Adresse auf NetScaler-Dienste zu, und wenn die Anforderung die Netzwerkkarte der NetScaler VPX-VM oder des Azure-Load Balancers erreicht, wird der VIP in interne IP (NSIP) und interne Portnummer übersetzt.
- Interne IP-Adresse ist die private interne IP-Adresse der VM aus dem Adress-Space-Pool des virtuellen Netzwerks. Diese IP-Adresse kann nicht vom externen Netzwerk aus erreicht werden. Diese IP-Adresse ist standardmäßig dynamisch, es sei denn, Sie setzen sie auf statisch. Der Datenverkehr aus dem Internet wird gemäß den Regeln, die in der Netzwerksicherheitsgruppe erstellt wurden, an diese Adresse weitergeleitet. Die Netzwerksicherheitsgruppe lässt sich in die Netzwerkkarte integrieren, um selektiv den richtigen Datenverkehr an den richtigen Port der NIC zu senden, was von den auf der VM konfigurierten Diensten abhängt.

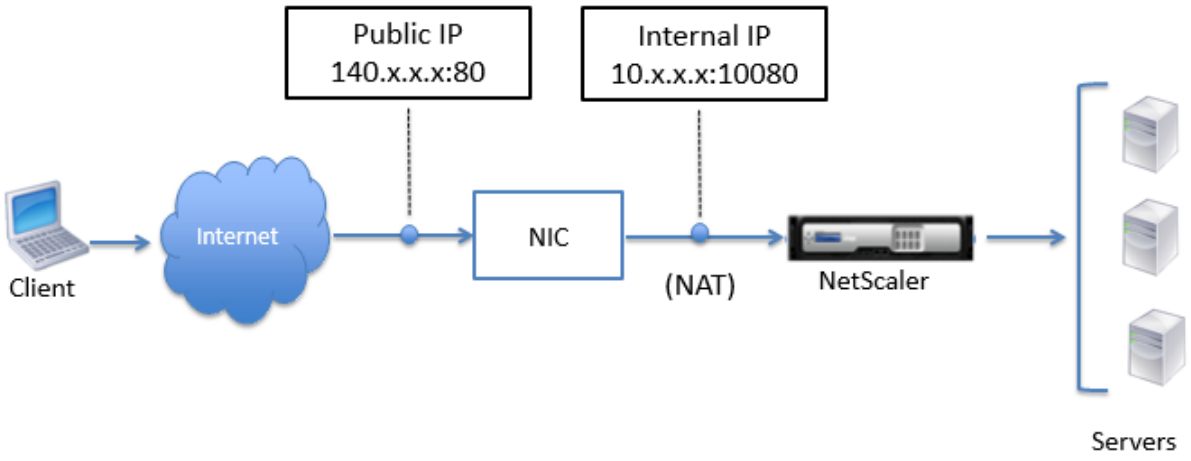
Die folgende Abbildung zeigt, wie der Datenverkehr von einem Client zu einem Server über eine in ARM bereitgestellte NetScaler VPX-Instanz fließt.



Verkehrsfluss durch Netzwerkadressübersetzung

Sie können auch eine öffentliche IP-Adresse (PIP) für Ihre Citrix ADC VPX-Instanz (Instanzebene) anfordern. Wenn Sie diese direkte PIP auf VM-Ebene verwenden, müssen Sie keine eingehenden und ausgehenden Regeln definieren, um den Netzwerkverkehr abzufangen. Die eingehende Anforderung aus dem Internet wird direkt auf der VM empfangen. Azure führt Network Address Translation (NAT) durch und leitet den Datenverkehr an die interne IP-Adresse der VPX-Instanz weiter.

Die folgende Abbildung zeigt, wie Azure Netzwerkadressübersetzung zur Zuordnung der internen NetScaler IP-Adresse durchführt.



In diesem Beispiel lautet die der Netzwerksicherheitsgruppe zugewiesene öffentliche IP 140.x.x.x und die interne IP-Adresse 10.x.x.x. Wenn die eingehenden und ausgehenden Regeln definiert sind, wird der öffentliche HTTP-Port 80 als Port definiert, auf dem die Clientanforderungen empfangen werden, und ein entsprechender privater Port, 10080, wird als Port definiert, auf dem die Citrix ADC VPX-Instanz wartet. Die Clientanforderung wird unter der öffentlichen IP-Adresse (140.x.x.x) empfangen. Azure führt die Netzwerkadressübersetzung durch, um das PIP der internen IP-Adresse 10.x.x.x an Port 10080 zuordnen, und leitet die Clientanforderung weiter.

> **Hinweis:**
>
> Citrix ADC VPX VMs in hoher Verfügbarkeit werden von externen oder internen Lastausgleichsdiensten gesteuert, deren eingehende Regeln definiert sind, um den Lastausgleichsverkehr zu steuern. Der externe Datenverkehr wird zuerst von diesen Lastausgleichsdiensten abgefangen, und der Datenverkehr wird entsprechend den konfigurierten Lastausgleichsregeln umgeleitet, bei denen Back-End-Pools, NAT-Regeln und Integritätstprobes auf den Lastausgleichsdiensten definiert sind.

Richtlinien zur Port-Nutzung

Sie können weitere eingehende und ausgehende Regeln n Netzwerksicherheitsgruppen konfigurieren, während Sie die Citrix ADC VPX-Instanz erstellen oder nachdem die virtuelle Maschine bereitgestellt wurde. Jede eingehende und ausgehende Regel ist einem öffentlichen und einem privaten Port zugeordnet.

Beachten Sie vor der Konfiguration der Regeln für Netzwerksicherheitsgruppen die folgenden Richtlinien bezüglich der Portnummern, die Sie verwenden können:

1. Die Citrix ADC VPX-Instanz reserviert die folgenden Ports. Sie können diese nicht als private Ports definieren, wenn Sie die öffentliche IP-Adresse für Anfragen aus dem Internet verwenden.

   Ports 21, 22, 80, 443, 8080, 67, 161, 179, 500, 520, 3003, 3008, 3009, 3010, 3011, 4001, 5061, 9000, 7000.

   Wenn Sie jedoch möchten, dass Internetdienste wie der VIP einen Standardport verwenden (z. B. Port 443), müssen Sie mithilfe der Netzwerksicherheitsgruppe eine Portzuordnung erstellen. Der Standardport wird dann einem anderen Port zugeordnet, der auf dem NetScaler für diesen VIP-Dienst konfiguriert ist.

   Beispielsweise kann ein VIP-Dienst auf Port 8443 der VPX-Instanz ausgeführt werden, wird aber dem öffentlichen Port 443 zugeordnet. Wenn der Benutzer also über die Public IP auf Port 443 zugreift, wird die Anforderung an den privaten Port 8443 weitergeleitet.
2. Öffentliche IP-Adresse unterstützt keine Protokolle, in denen die Portzuordnung dynamisch geöffnet wird, z. B. passives FTP oder ALG.
3. Hochverfügbarkeit funktioniert nicht für Datenverkehr, der eine öffentliche IP-Adresse (PIP) verwendet, die einer VPX-Instanz zugeordnet ist, anstelle eines auf dem Azure-Load Balancer konfigurierten PIP.

> **Hinweis:**
>
> In Azure Resource Manager ist eine Citrix ADC VPX-Instanz zwei IP-Adressen zugeordnet - eine öffentliche IP-Adresse (PIP) und eine interne IP-Adresse. Während der externe Datenverkehr mit dem PIP verbunden ist, ist die interne IP-Adresse oder der NSIP nicht routingfähig. Um VIP in VPX zu konfigurieren, verwenden Sie die interne IP-Adresse und einen der freien Ports. Verwenden Sie nicht die PIP, um VIP zu konfigurieren.

Konfigurieren einer eigenständigen Citrix ADC VPX-Instanz

October 5, 2021

Sie können eine einzelne Citrix ADC VPX-Instanz im ARM-Portal (Azure Resource Manager) im eigenständigen Modus bereitstellen, indem Sie die virtuelle Maschine erstellen und andere Ressourcen konfigurieren.

Voraussetzungen

Stellen Sie sicher, dass Sie Folgendes haben:

- Ein Microsoft Azure-Benutzerkonto
- Zugriff auf Microsoft Azure Resource Manager
- Microsoft Azure-SDK
- Microsoft Azure PowerShell

Melden Sie sich auf der Seite Microsoft Azure-Portal beim Azure Resource Manager-Portal an, indem Sie Ihren Benutzernamen und Ihr Kennwort angeben.

> **Hinweis:**
>
> Wenn Sie im ARM-Portal auf eine Option in einem Bereich klicken, wird rechts ein neuer Bereich geöffnet. Navigieren Sie von einem Bereich zum anderen, um Ihr Gerät zu konfigurieren.

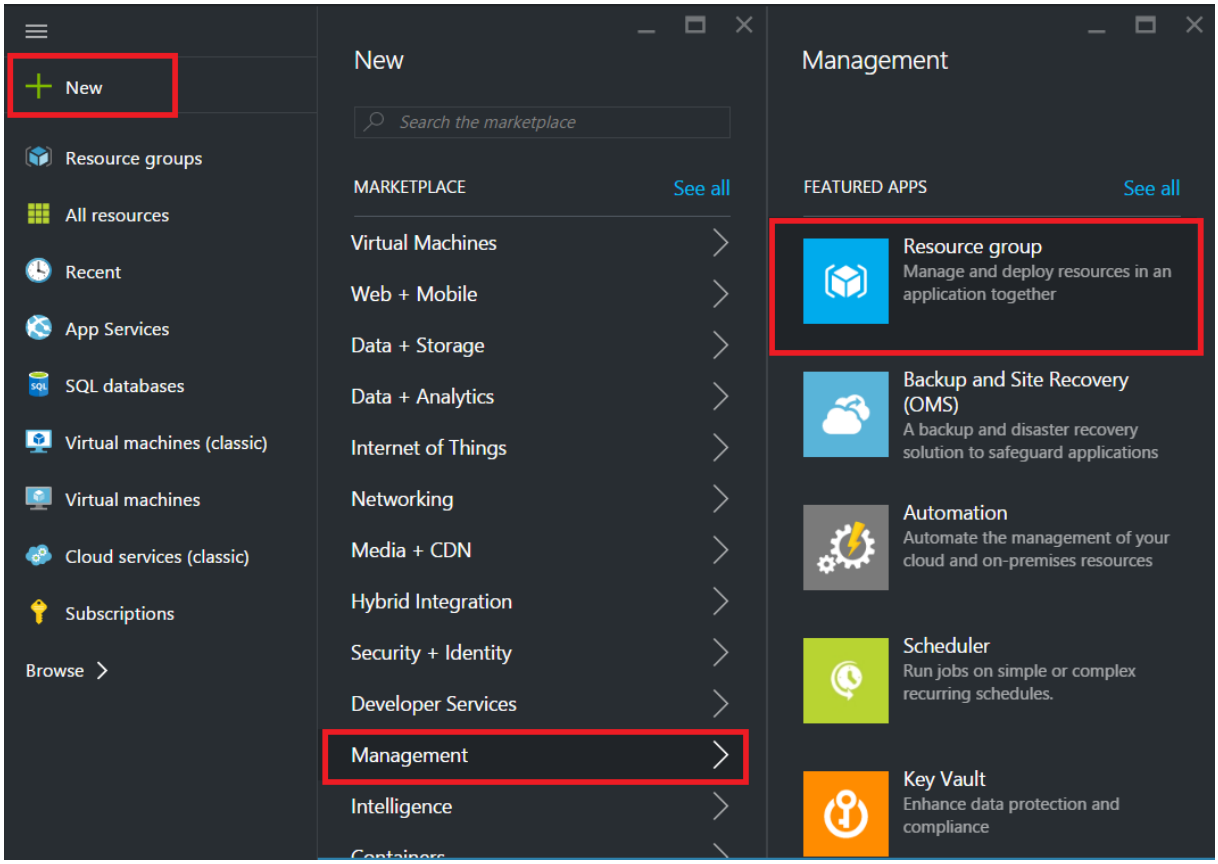
Zusammenfassung der Konfigurationsschritte

1. Konfigurieren einer Ressourcengruppe
2. Konfigurieren einer Netzwerksicherheitsgruppe
3. Konfigurieren des virtuellen Netzwerks und seiner Subnetze
4. Konfigurieren eines Speicherkontos
5. Konfigurieren eines Verfügbarkeitssatzes
6. Konfigurieren Sie eine Citrix ADC VPX-Instanz.

Konfigurieren einer Ressourcengruppe

Erstellen Sie eine neue Ressourcengruppe, die ein Container für alle Ressourcen ist. Verwenden Sie die Ressourcengruppe, um Ihre Ressourcen als Gruppe bereitzustellen, zu verwalten und zu überwachen.

1. Klicken Sie auf **Neu** > **Verwaltung** > **Ressourcengruppe** .
2. Geben Sie im Bereich **Ressourcengruppe** die folgenden Details ein:
    - Ressourcengruppenname
    - Speicherort der Ressourcengruppe
3. Klicken Sie auf **Erstellen**.

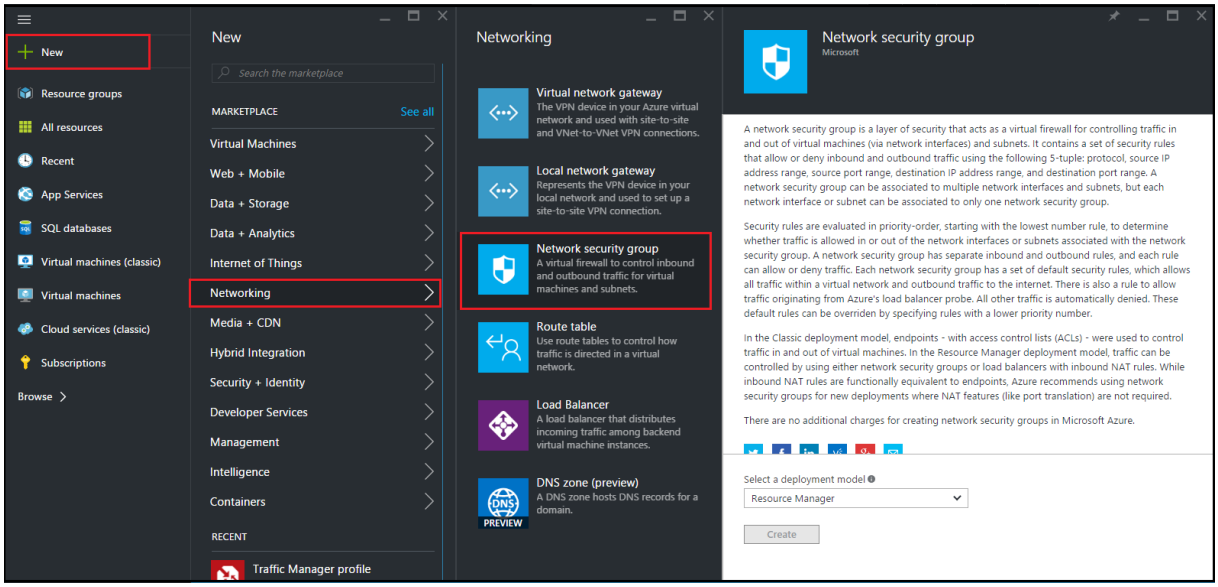


Konfigurieren einer Netzwerksicherheitsgruppe

Erstellen Sie eine Netzwerksicherheitsgruppe, um eingehende und ausgehende Regeln zuzuweisen, um den eingehenden und ausgehenden Datenverkehr innerhalb des virtuellen Netzwerks zu steuern. Mit der Netzwerksicherheitsgruppe können Sie Sicherheitsregeln für eine einzelne virtuelle Maschine definieren und Sicherheitsregeln für ein virtuelles Netzwerksubnetz definieren.

1. Klicken Sie auf **Neu** > **Netzwerk** > **Netzwerksicherheitsgruppe**.
2. Geben Sie im Bereich **Netzwerksicherheitsgruppe erstellen** die folgenden Details ein, und klicken Sie dann auf **Erstellen**.
    - Name - Geben Sie einen Namen für die Sicherheitsgruppe ein
    - Ressourcengruppe: Wählen Sie die Ressourcengruppe aus der Dropdownliste aus.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie den richtigen Speicherort ausgewählt haben. Die Liste der Ressourcen, die in der Dropdownliste angezeigt werden, unterscheidet sich für verschiedene Speicherorte.

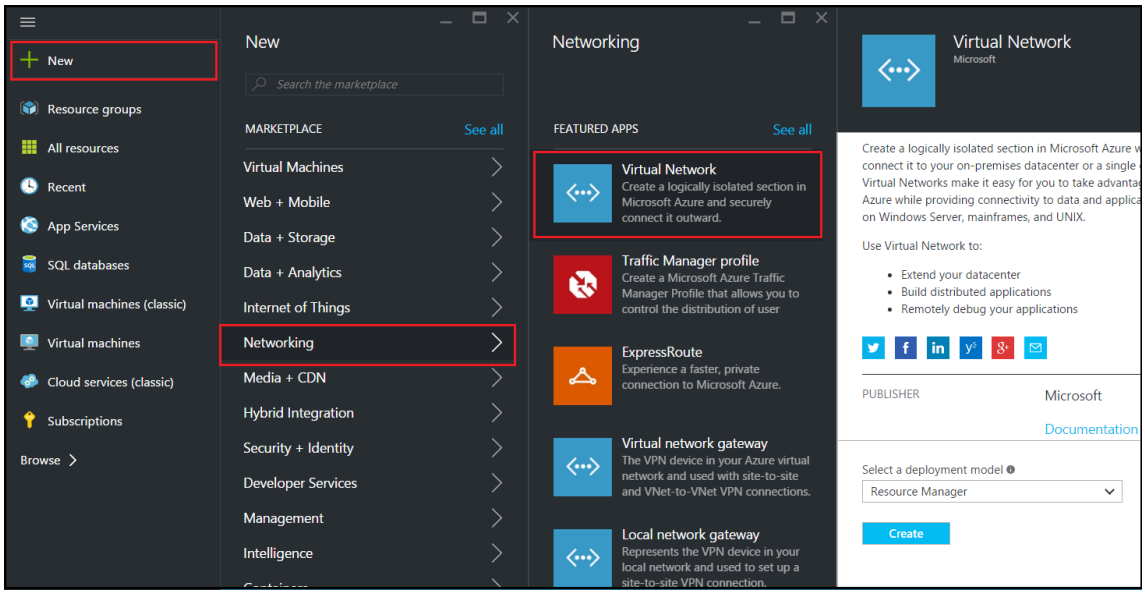


Konfigurieren eines virtuellen Netzwerks und der Subnetze

Virtuelle Netzwerke in ARM bieten eine Schicht von Sicherheit und Isolation für Ihre Dienste. VMs und Dienste, die Teil desselben virtuellen Netzwerks sind, können auf einander zugreifen.

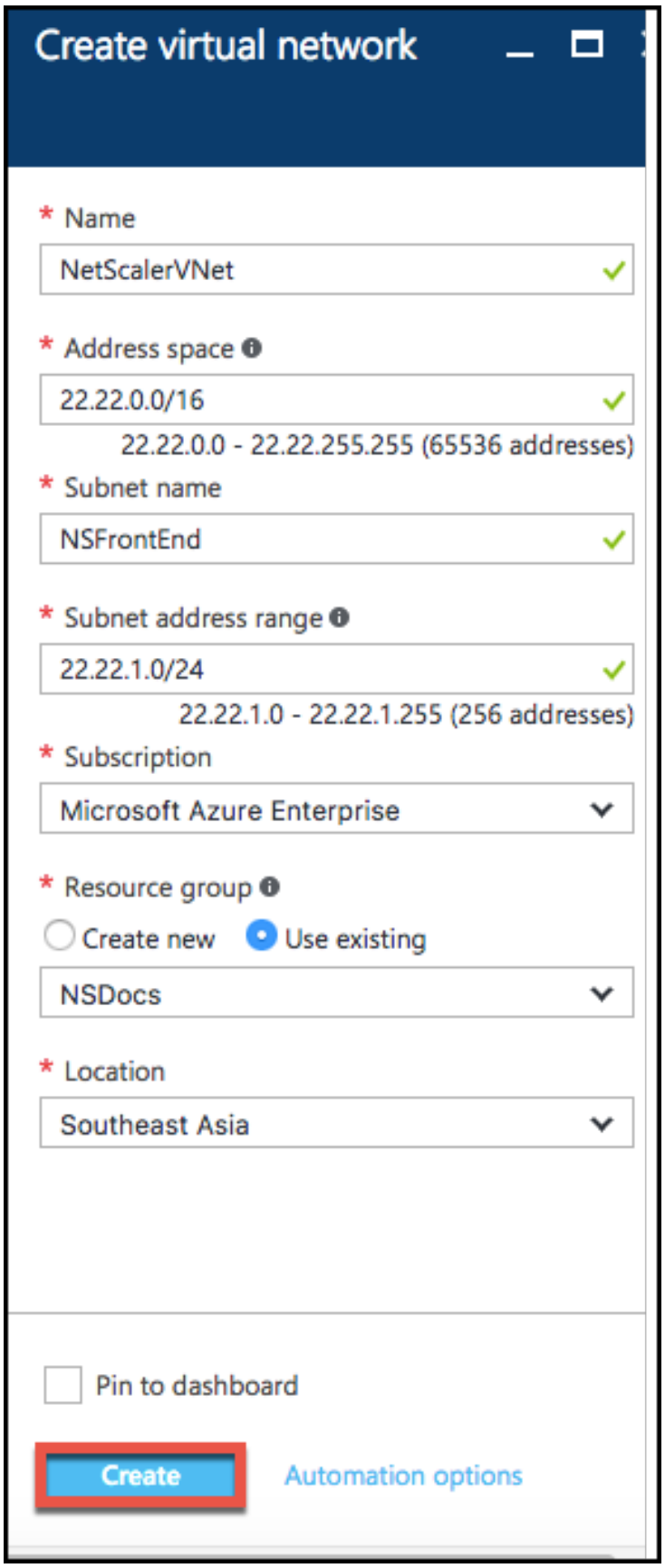
Für diese Schritte, um ein virtuelles Netzwerk und Subnetze zu erstellen.

1. Klicken Sie auf **Neu** > **Netzwerk** > **Virtuelles Netzwerk**.
2. Stellen Sie im Bereich **Virtuelles Netzwerk** sicher, dass der Bereitstellungsmodus **Ressourcen-manager** ist, und klicken Sie auf **Erstellen**.



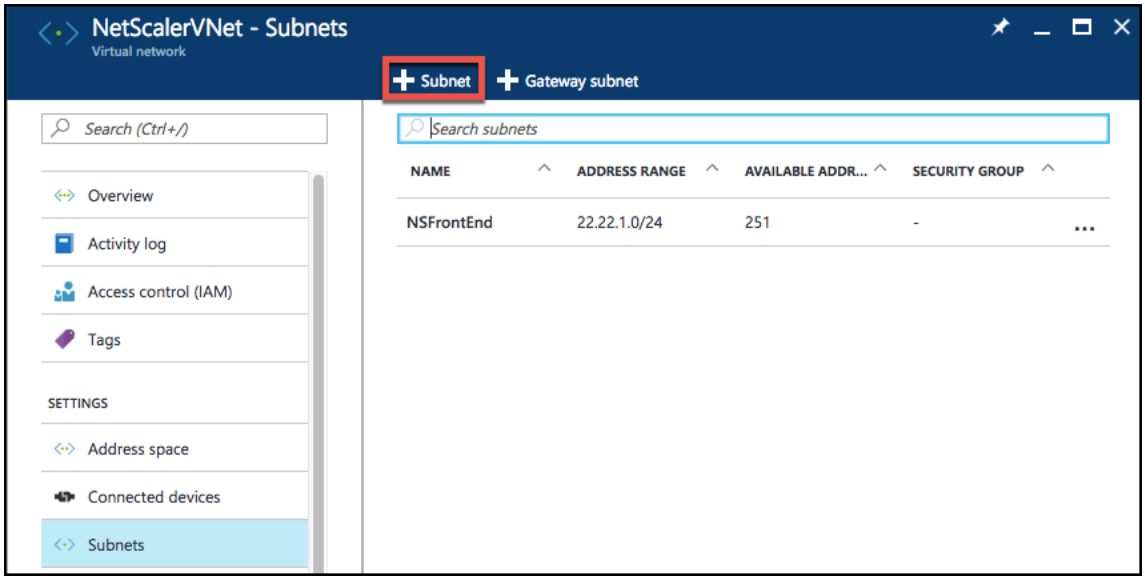
3. Geben Sie im Bereich **Virtuelles Netzwerk erstellen** die folgenden Werte ein, und klicken Sie dann auf **Erstellen**.

- Name des virtuellen Netzwerks
- Adressraum - Geben Sie den reservierten IP-Adressblock für das virtuelle Netzwerk ein
- Subnetz: Geben Sie den Namen des ersten Subnetzes ein (Sie erstellen das zweite Subnetz später in diesem Schritt)
- Subnetzadressbereich - Geben Sie den reservierten IP-Adressblock des Subnetzes ein
- Ressourcengruppe: Wählen Sie die zuvor erstellte Ressourcengruppe aus der Dropdownliste aus

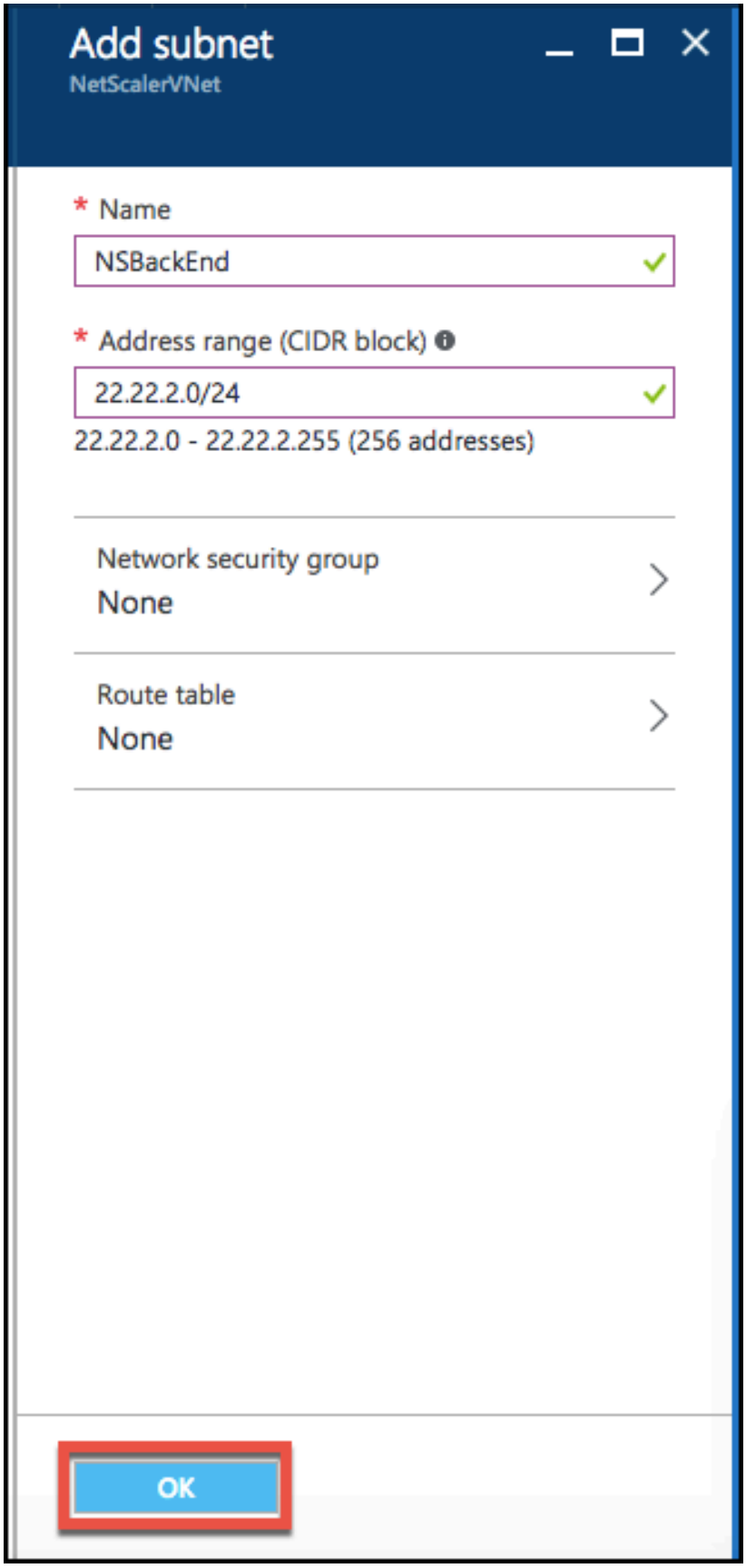


Konfigurieren des zweiten Subnetzes

1. Wählen Sie im Bereich **Alle Ressourcen** das neu erstellte virtuelle Netzwerk aus, und klicken Sie im Bereich **Einstellungen** auf **Subnetze**.



2. Klicken Sie auf **+ Subnetz**, und erstellen Sie das zweite Subnetz, indem Sie die folgenden Details eingeben.
   - Name des zweiten Subnetzes
   - Adressbereich - Geben Sie den reservierten IP-Adressblock des zweiten Subnetzes ein
   - Netzwerksicherheitsgruppe - wählen Sie die Netzwerksicherheitsgruppe aus der Drop-downliste
3. Klicken Sie auf **Erstellen**.

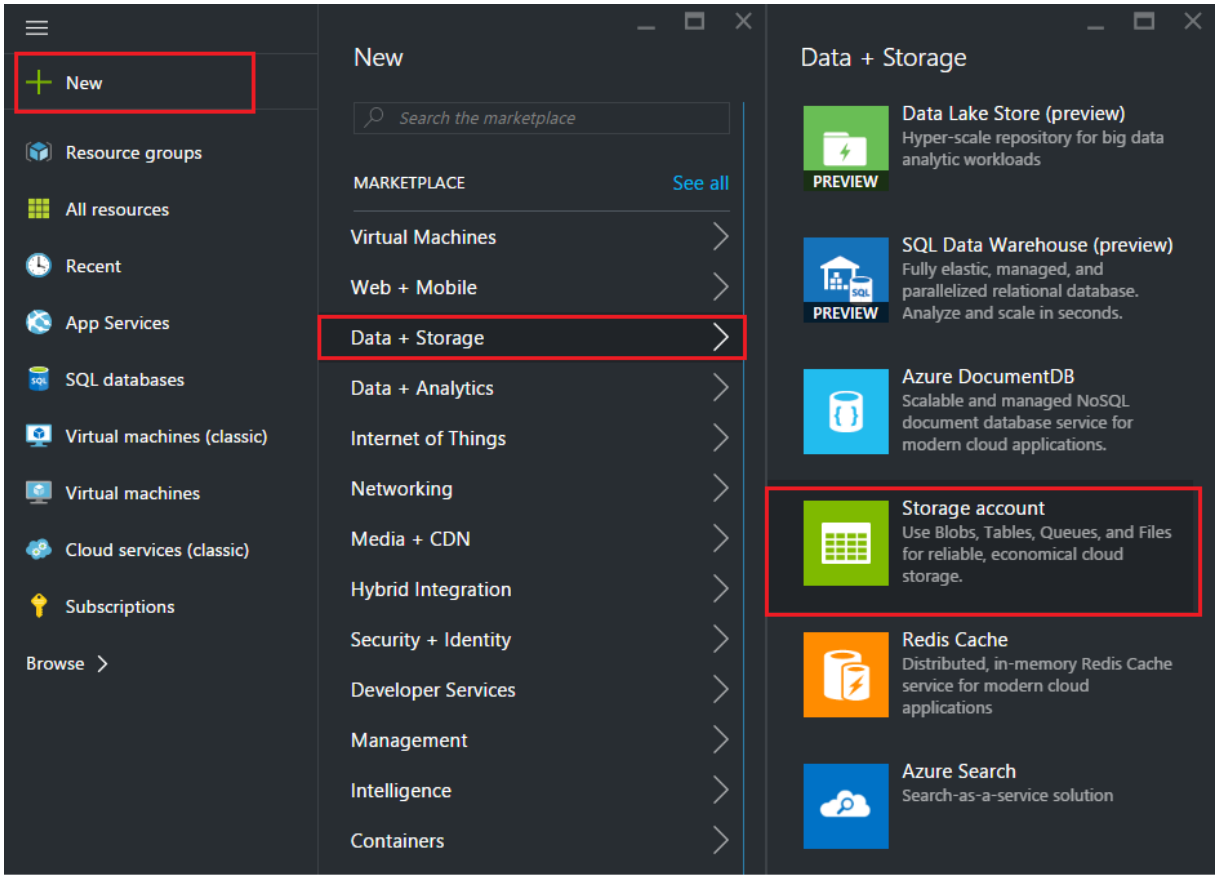


Konfigurieren eines Speicherkontos

Der ARM IaaS-Infrastrukturspeicher umfasst alle Dienste, in denen Daten in Form von Blobs, Tabellen, Warteschlangen und Dateien gespeichert werden können. Sie können auch Anwendungen mit diesen Formen von Speicherdaten in ARM erstellen.

Erstellen Sie ein Speicherkonto, um alle Ihre Daten zu speichern.

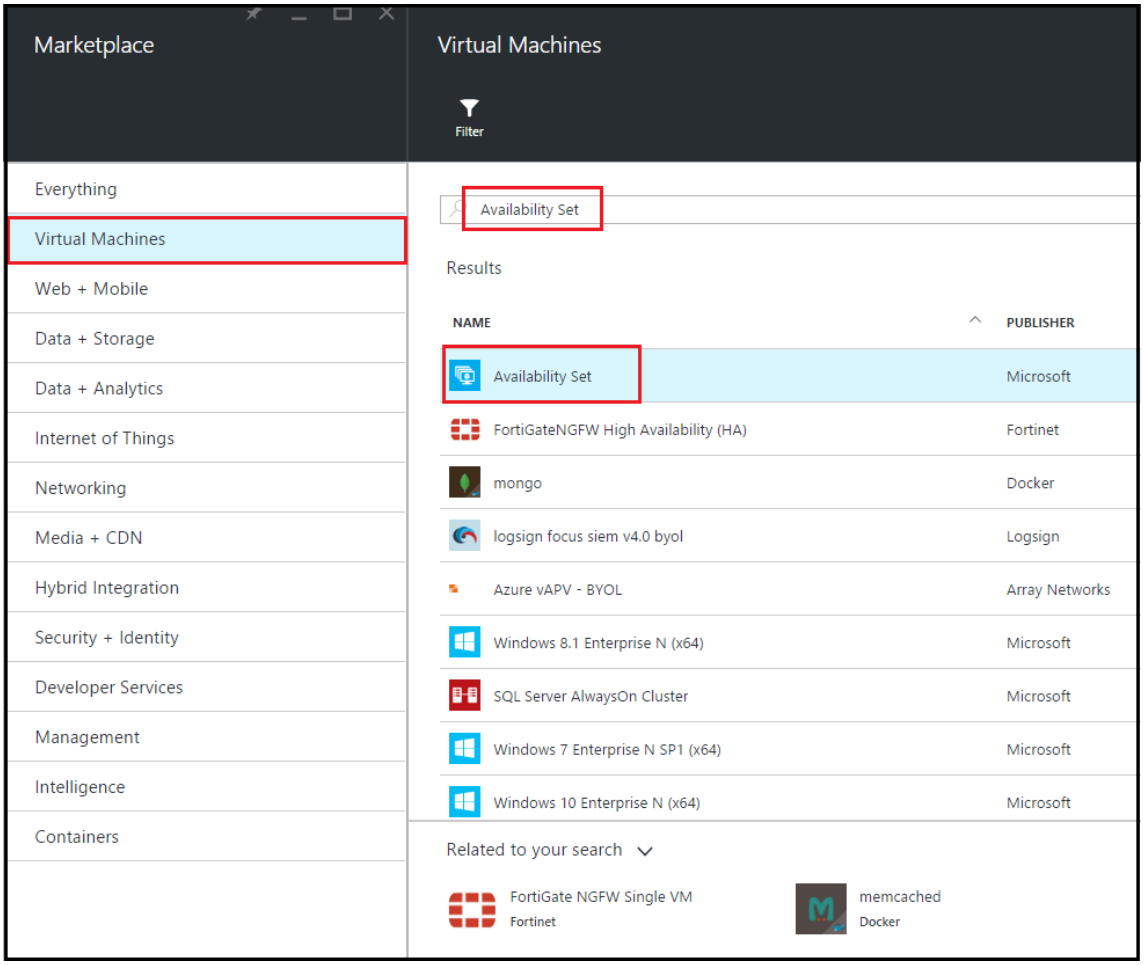
1. Klicken Sie auf **+Neu** > **Daten + Speicher** > **Speicherkonto**.
2. Geben Sie im Bereich **Speicherkonto erstellen** die folgenden Details ein:
    - Name des Kontos
    - Bereitstellungsmodus: Stellen Sie sicher, dass Sie **Ressourcen-Manager**auswählen
    - Kontoart - wählen Sie **Allzweck** aus der Dropdownliste
    - Replikation: Wählen Sie **Lokal redundanten Speicher** aus der Dropdownliste
    - Ressourcengruppe: Wählen Sie die neu erstellte Ressourcengruppe aus der Dropdownliste aus.
3. Klicken Sie auf **Erstellen**.



Konfigurieren eines Verfügbarkeitssatzes

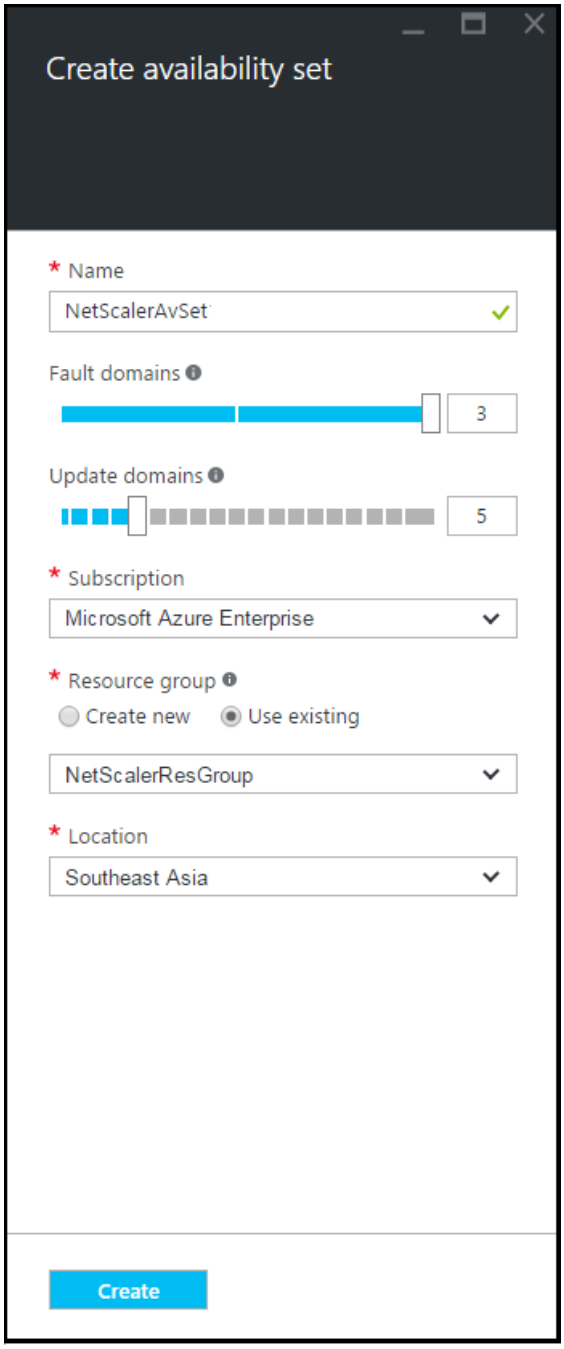
Ein Verfügbarkeitssatz garantiert, dass bei geplanten oder ungeplanten Wartungsarbeiten mindestens eine VM betriebsbereit gehalten wird. Zwei oder mehr virtuelle Rechner mit demselben "Verfügbarkeitssatz" werden auf verschiedenen Fehlerdomänen platziert, um redundante Dienste zu erreichen.

1. Klicken Sie auf **+Neu**.
2. Klicken Sie im Bereich MARKETPLACE auf **Alle anzeigen**, und klicken Sie auf **Virtuelle Maschinen**.
3. Suchen Sie nach Verfügbarkeitssatz, und wählen Sie dann **Verfügbarkeitssatzentität** aus der angezeigten Liste aus.



4. Klicken Sie auf **Erstellen,** und geben **Sie im Bereich Verfügbarkeitssatz** erstellen die folgenden Details ein:
   - Name des Satzes
   - Ressourcengruppe: Wählen Sie die neu erstellte Ressourcengruppe aus der Dropdownliste aus.

5. Klicken Sie auf **Erstellen**.



Konfigurieren einer Citrix ADC VPX-Instanz

Erstellen Sie eine Instanz von Citrix ADC VPX im virtuellen Netzwerk. Rufen Sie das Citrix ADC VPX Image vom Azure Marketplace ab, und erstellen Sie dann mithilfe des Azure Resource Manager Portals eine Citrix ADC VPX Instanz.

Bevor Sie mit dem Erstellen der Citrix ADC VPX Instanz beginnen, stellen Sie sicher, dass Sie ein

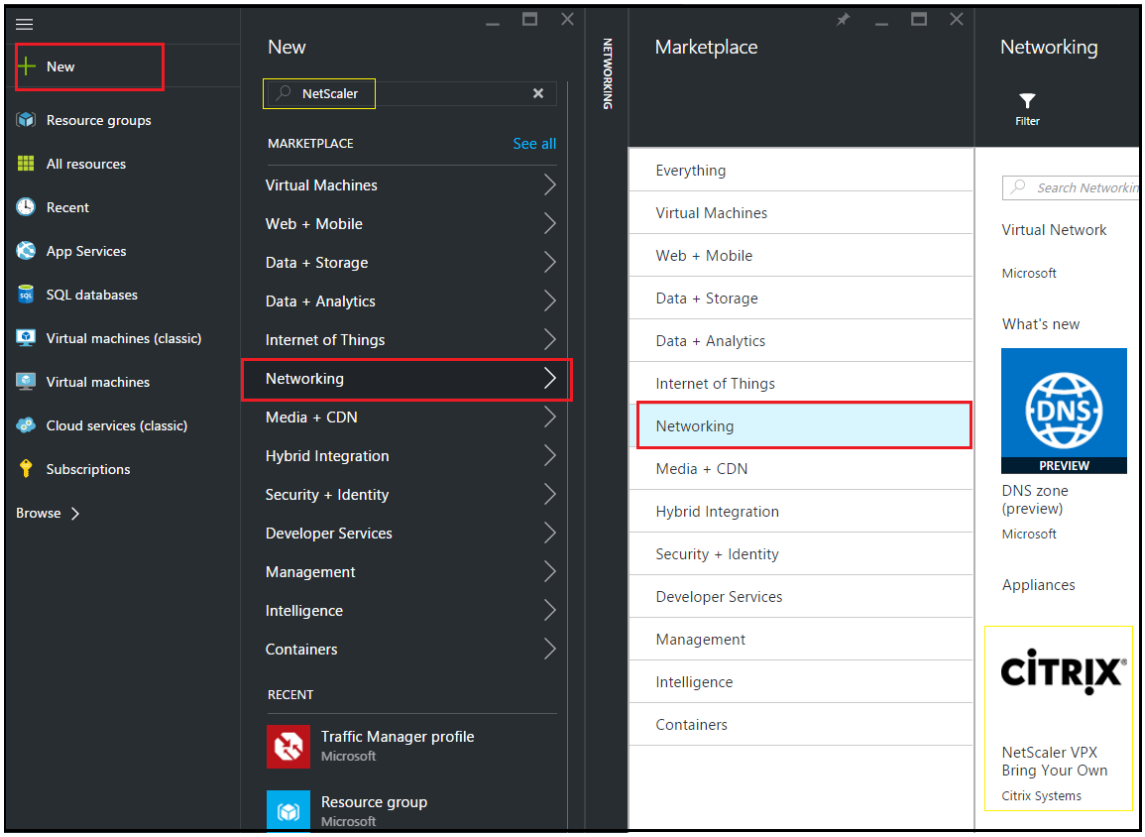
virtuelles Netzwerk mit den erforderlichen Subnetzen erstellt haben, in denen sich die Instanz befindet. Sie können während des VM-Provisionings virtuelle Netzwerke erstellen, jedoch ohne die Flexibilität, verschiedene Subnetze einzurichten. Hinweise zum Erstellen virtueller Netzwerke finden Sie unter http://azure.microsoft.com/en-us/documentation/articles/create-virtual-network/.

Konfigurieren Sie optional DNS-Server- und VPN-Konnektivität, mit der eine virtuelle Maschine auf Internetressourcen zugreifen kann.

> **Hinweis:**
>
> Citrix empfiehlt, vor der Bereitstellung der Citrix ADC VPX VM Ressourcengruppe, Netzwerksicherheitsgruppe, virtuelles Netzwerk und andere Entitäten zu erstellen, damit die Netzwerkinformationen während der Provisioning verfügbar sind.

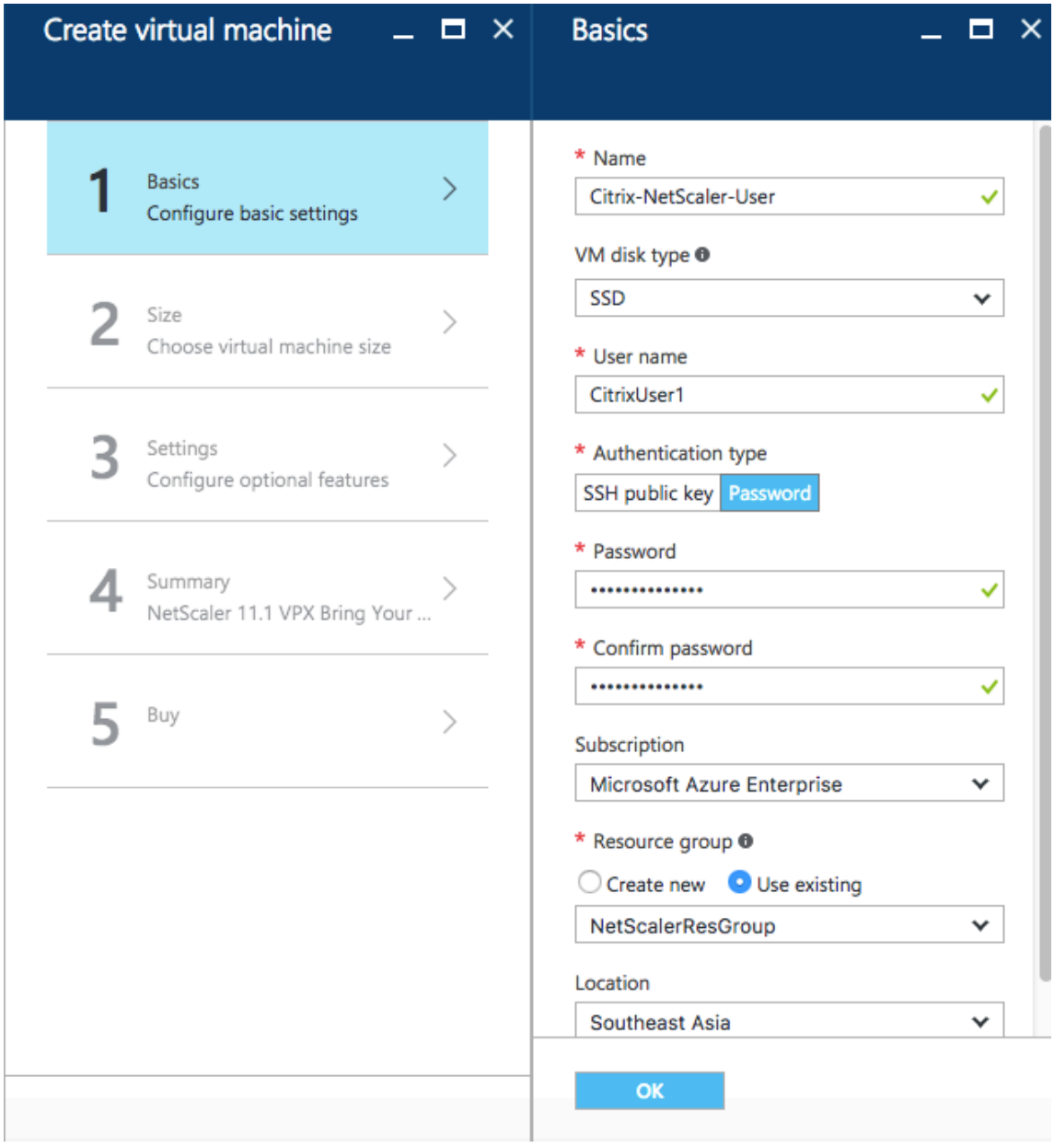
1. Klicken Sie auf **+Neu** > **Netzwerk**.
2. Klicken Sie auf **Alle anzeigen** und klicken Sie im Netzwerkbereich auf **Citrix ADC 13.0**.
3. Wählen Sie **Citrix ADC 13.0 VPX Bring Your Own License** aus der Liste der Softwarepläne.

   Als schnelle Möglichkeit, eine Entität im ARM-Portal zu finden, können Sie auch den Namen der Entität in das Suchfeld Azure Marketplace eingeben und drücken <Enter>. Geben Sie NetScaler in das Suchfeld ein, um die Citrix NetScaler Images zu suchen.



> **Hinweis:**
>
> Stellen Sie sicher, dass Sie das neueste Image auswählen. Ihr Citrix NetScaler Image hat möglicherweise die Release-Nummer im Namen.

4. Wählen Sie auf der Seite **Citrix ADC VPX Bring Your Own License** aus der Dropdownliste die Option **Resource Manager** aus, und klicken Sie auf **Create**.



5. Geben Sie im Bereich **Virtuelle Maschine erstellen** in jedem Abschnitt die erforderlichen Werte an, um eine virtuelle Maschine zu erstellen. Klicken Sie in jedem Abschnitt auf **OK**, um die Konfiguration zu speichern.

Grundlegende:

- Name - Geben Sie einen Namen für die Citrix ADC VPX-Instanz an
- VM-Datenträgertyp - Wählen Sie SSD (Standardwert) oder HDD aus dem Dropdownmenü
- Benutzername und Kennwort: Geben Sie einen Benutzernamen und ein Kennwort an, um auf die Ressourcen in der von Ihnen erstellten Ressourcengruppe zuzugreifen.
- Authentifizierungstyp - Wählen Sie SSH-Öffentlicher Schlüssel oder Kennwort
- Ressourcengruppe: Wählen Sie die Ressourcengruppe aus der Dropdownliste aus.

Sie können hier eine Ressourcengruppe erstellen, Citrix empfiehlt jedoch, eine Ressourcengruppe aus Ressourcengruppen im Azure Resource Manager zu erstellen und dann die Gruppe aus der Dropdownliste auszuwählen.

> **Hinweis:**
>
> Geben Sie in einer Azure-Stackumgebung zusätzlich zu den grundlegenden Parametern die folgenden Parameter an:
>
> - Azure-Stack-Domäne
> - Azure-Stack-Mandant (optional)
> - Azure-Client (optional)
> - Azure-Clientgeheimnis (optional)

Größe:

Je nach VM-Datenträgertyp, SDD oder HDD, die Sie in den Grundeinstellungen ausgewählt haben, werden die Datenträgergrößen angezeigt.

- Wählen Sie eine Datenträgergröße entsprechend Ihrer Anforderung aus und klicken Sie auf **Auswählen**.

Einstellungen:

- Wählen Sie den Standarddatenträgertyp (Standard)
- Speicherkonto - Wählen Sie das Speicherkonto aus
- Virtuelles Netzwerk - Wählen Sie das virtuelle Netzwerk
- Subnet - Legen Sie die Subnetzadresse fest
- Öffentliche IP-Adresse - Wählen Sie den Typ der IP-Adressenzuweisung
- Netzwerksicherheitsgruppe - Wählen Sie die Sicherheitsgruppe aus, die Sie erstellt haben. Stellen Sie sicher, dass eingehende und ausgehende Regeln in der Sicherheitsgruppe konfiguriert sind.
- Verfügbarkeitsset - Wählen Sie den Verfügbarkeitssatz aus dem Dropdownmenü aus.

Zusammenfassung:

Die Konfigurationseinstellungen werden validiert, und auf der Seite Zusammenfassung wird das Ergebnis der Validierung angezeigt. Wenn die Validierung fehlschlägt, wird auf der Seite Zusammenfassung der Grund des Fehlers angezeigt. Gehen Sie zurück zum jeweiligen Abschnitt und nehmen Sie ggf. Änderungen vor. Wenn die Validierung besteht, klicken Sie auf **OK**.

Kaufen:

Überprüfen Sie die Angebotsdetails und die rechtlichen Bedingungen auf der Seite Kauf und klicken Sie auf **Kaufen**.

Erstellen Sie für Hochverfügbarkeitsbereitstellungen zwei unabhängige Instanzen von Citrix ADC VPX in demselben Verfügbarkeitssatz und in derselben Ressourcengruppe, um sie in der aktiven Standby-Konfiguration bereitzustellen.

Konfigurieren mehrerer IP-Adressen für eine eigenständige Citrix ADC VPX-Instanz

October 5, 2021

In diesem Abschnitt wird erläutert, wie Sie eine eigenständige Citrix ADC VPX-Instanz mit mehreren IP-Adressen im Azure Resource Manager (ARM) konfigurieren. Der VPX-Instanz kann eine oder mehrere Netzwerkkarten angeschlossen sein, und jeder Netzwerkkarte kann eine oder mehrere statische oder dynamische öffentliche und private IP-Adressen zugewiesen sein. Sie können mehrere IP-Adressen als NSIP, VIP, SNIP usw. zuweisen.

Weitere Informationen finden Sie in der Azure-Dokumentation Zuweisen mehrerer IP-Adressen zu virtuellen Maschinen über das Azure-Portal.

Informationen zur Verwendung von PowerShell-Befehlen finden Sie unter Konfigurieren mehrerer IP-Adressen für eine Citrix ADC VPX-Instanz im Standalone-Modus mithilfe von PowerShell-Befehlen.

Anwendungsfall

In diesem Anwendungsfall wird eine eigenständige Citrix ADC VPX Appliance mit einer einzelnen Netzwerkkarte konfiguriert, die mit einem virtuellen Netzwerk (VNET) verbunden ist. Die Netzwerkkarte ist mit drei IP-Konfigurationen (ipconfig) verknüpft, wobei jeder Server einen anderen Zweck hat - wie in der Tabelle dargestellt.

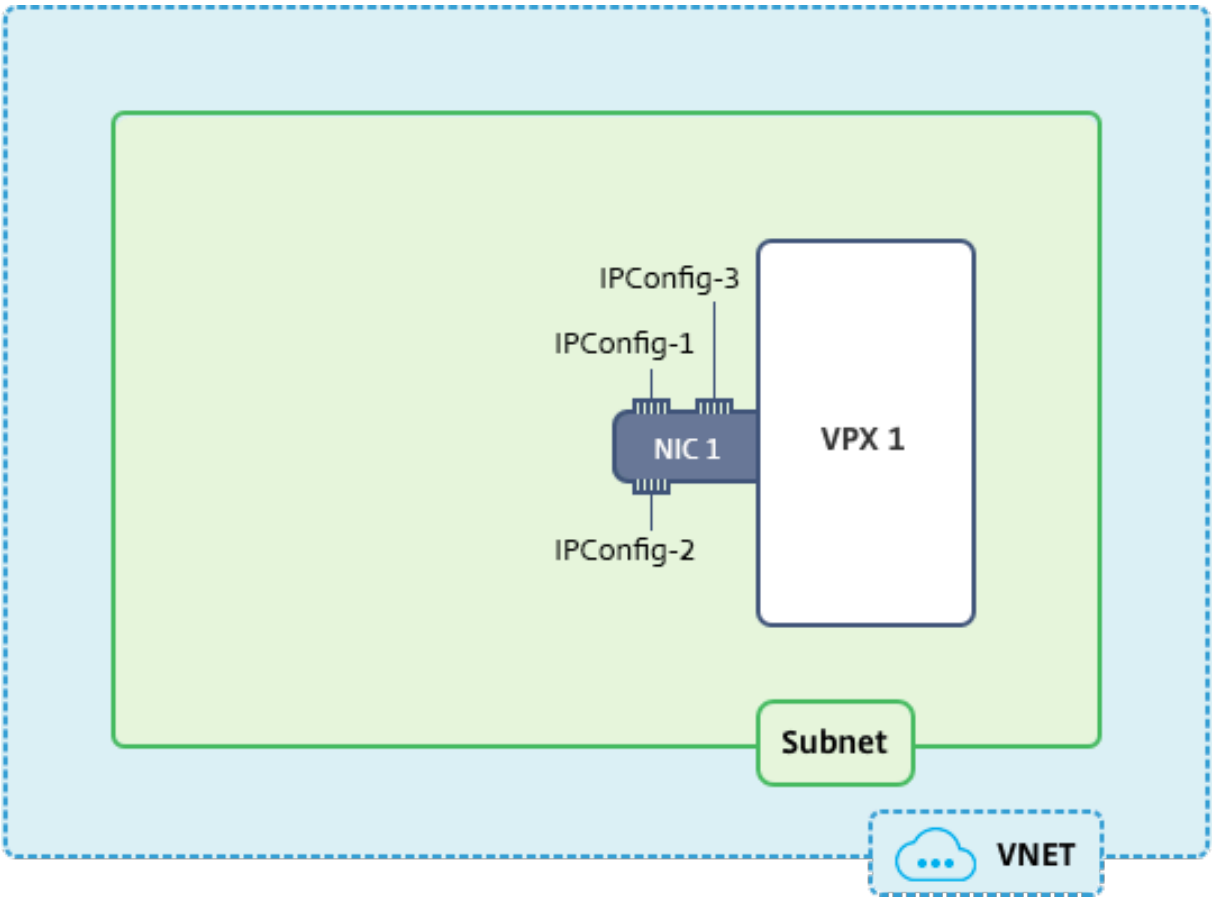
IP-Konfiguration	Verbunden mit	Zweck
ipconfig1	Statische öffentliche IP-Adresse; statische private IP-Adresse	Dient zum Verwalten von Datenverkehr
ipconfig2	Statische öffentliche IP-Adresse; statische private Adresse	Dient dem clientseitigen Datenverkehr

IP-Konfiguration	Verbunden mit	Zweck
ipconfig3	Statische private IP-Adresse	Kommuniziert mit Back-End-Servern

> **Hinweis:**
>
> `IPConfig-3` ist mit keiner öffentlichen IP-Adresse verknüpft.

Diagramm: Topologie

Hier ist die visuelle Darstellung des Anwendungsfalls.



> **Hinweis:**
>
> In einer Multi-Nic, Multi-IP Azure Citrix ADC VPX-Bereitstellung wird die private IP, die mit der primären (ersten) `IPConfig` der primären (ersten) Netzwerkkarte verknüpft ist, automatisch als Verwaltungs-NSIP der Appliance hinzugefügt. Die verbleibenden privaten IP-Adressen, die mit verknüpft sind, `IPConfigs` müssen in der VPX-Instanz als VIP oder SNIP mithilfe des `add ns ip` Befehls entsprechend Ihrer Anforderung hinzugefügt werden.

Voraussetzungen

Bevor Sie beginnen, erstellen Sie eine VPX-Instanz, indem Sie die unter diesem Link angegebenen Schritte ausführen:

Konfigurieren einer eigenständigen Citrix ADC VPX-Instanz

Für diesen Anwendungsfall wird die NSDoc0330VM VPX-Instanz erstellt.

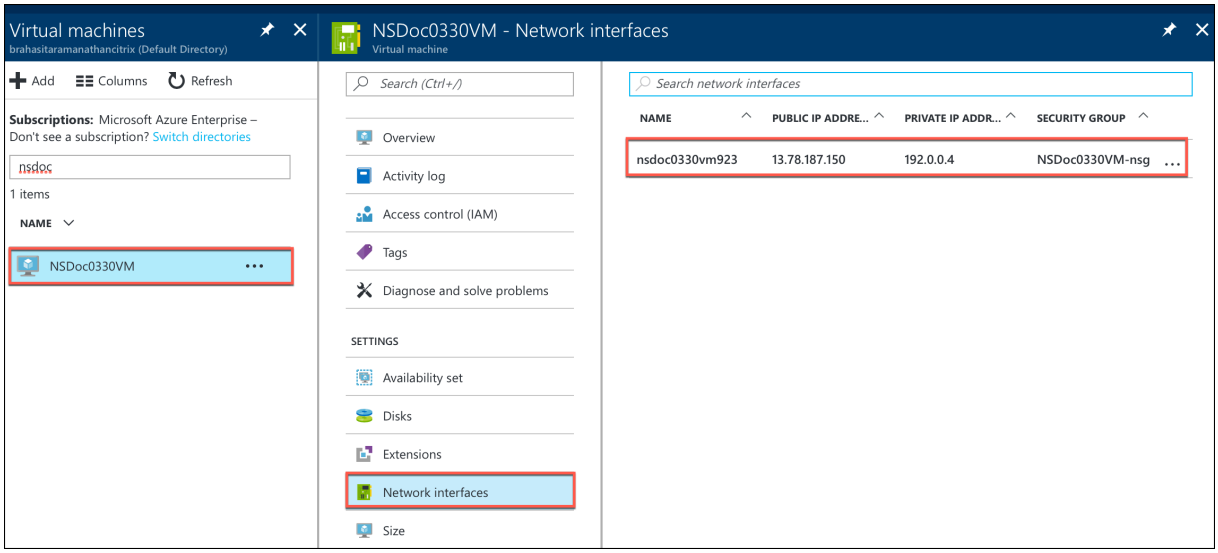
Verfahren zum Konfigurieren mehrerer IP-Adressen für eine Citrix ADC VPX-Instanz im Standalone-Modus.

Konfigurieren mehrerer IP-Adressen für eine Citrix ADC VPX Appliance im Standalone-Modus:

1. Hinzufügen von IP-Adressen zur VM
2. Konfigurieren von Citrix ADC eigenen IP-Adressen

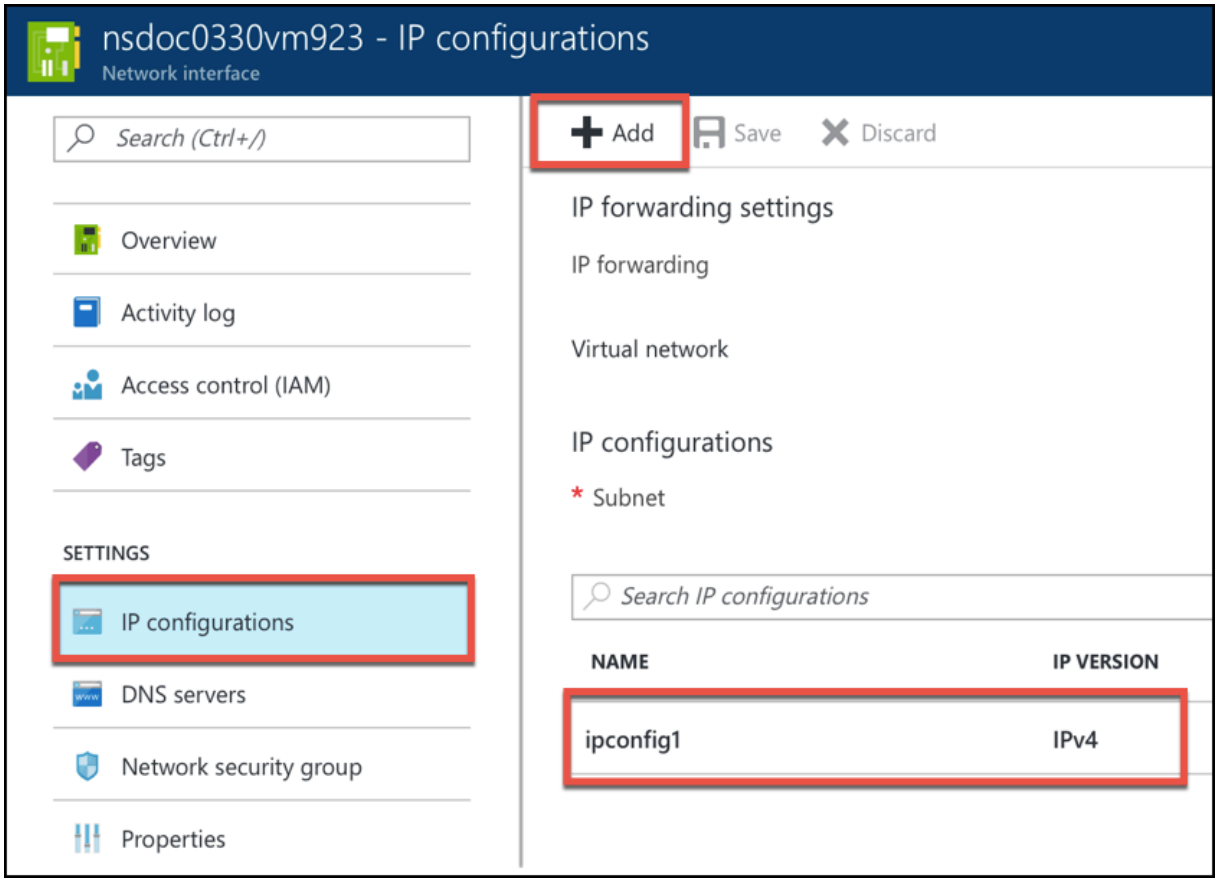
Schritt 1: Hinzufügen von IP-Adressen zur VM

1. Klicken Sie im Portal auf **Weitere Dienste > geben Sie virtuelle Maschinen** in das Filterfeld ein, und klicken Sie dann auf **Virtuelle Maschinen** .
2. Klicken Sie im Blade **Virtuelle Maschinen** auf die VM, der IP-Adressen hinzugefügt werden sollen. Klicken Sie auf **Netzwerkschnittstellen** im Blade der virtuellen Maschine, das angezeigt wird, und wählen Sie dann die Netzwerkschnittstelle aus.



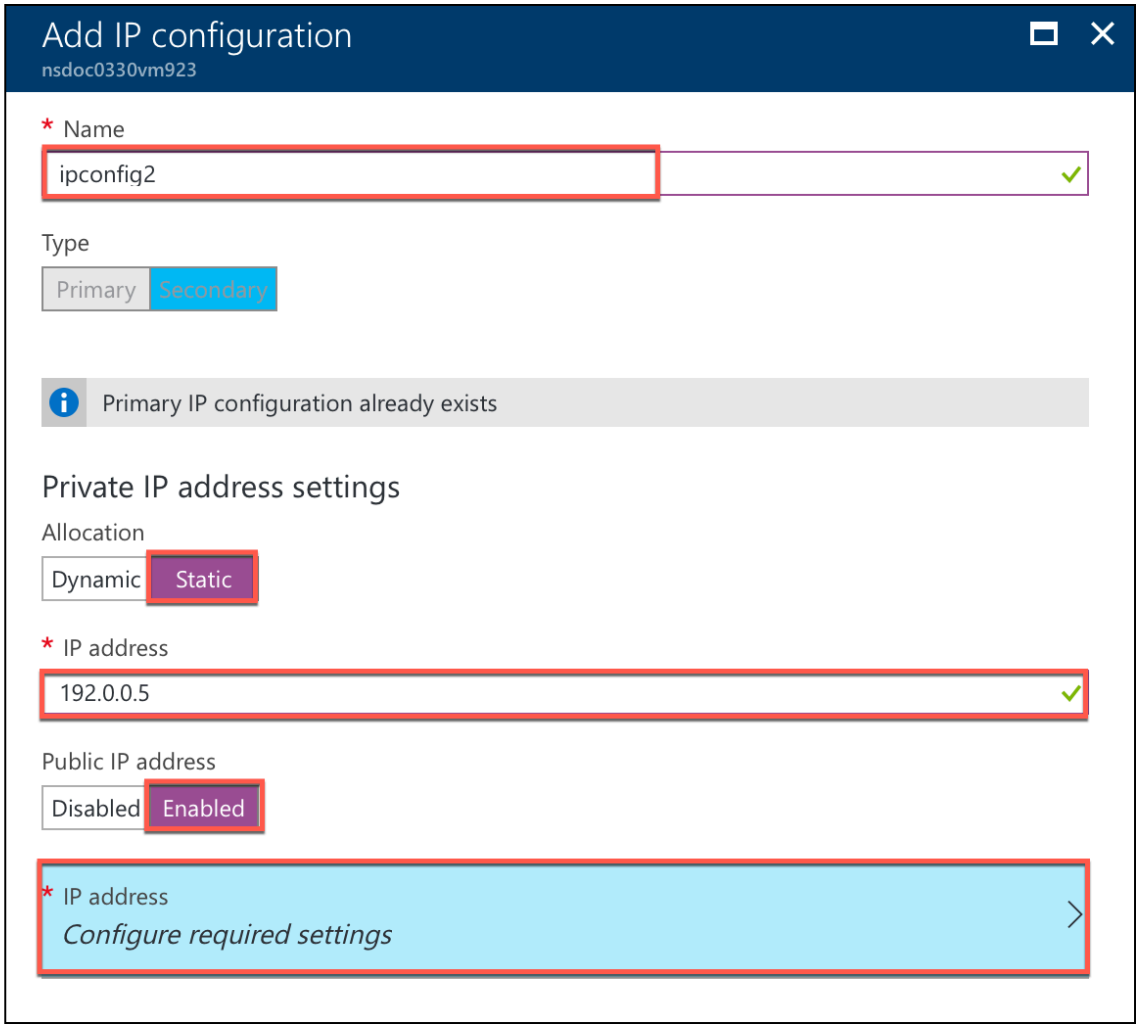
Klicken Sie im Blade, das für die ausgewählte NIC angezeigt wird, auf **IP-Konfigurationen**. Die vorhandene IP-Konfiguration, die beim Erstellen der VM, **ipconfig1**, zugewiesen wurde, wird angezeigt. Stellen Sie für diesen Anwendungsfall sicher, dass die IP-Adressen, die mit ipconfig1 verknüpft sind, statisch sind. Als nächstes erstellen Sie zwei weitere IP-Konfigurationen: ipconfig2 (VIP) und ipconfig3 (SNIP).

Um mehr zu erstellen `ipconfigs`, erstellen **Sie Hinzufügen**.



Geben **Sie im Fenster IP-Konfiguration hinzufügen** einen **Namen** ein, geben Sie die Zuweisungsmethode als **Statisch** an, geben Sie eine IP-Adresse ein (192.0.0.5 für diesen Anwendungsfall) und aktivieren Sie die **öffentliche IP-Adresse** .

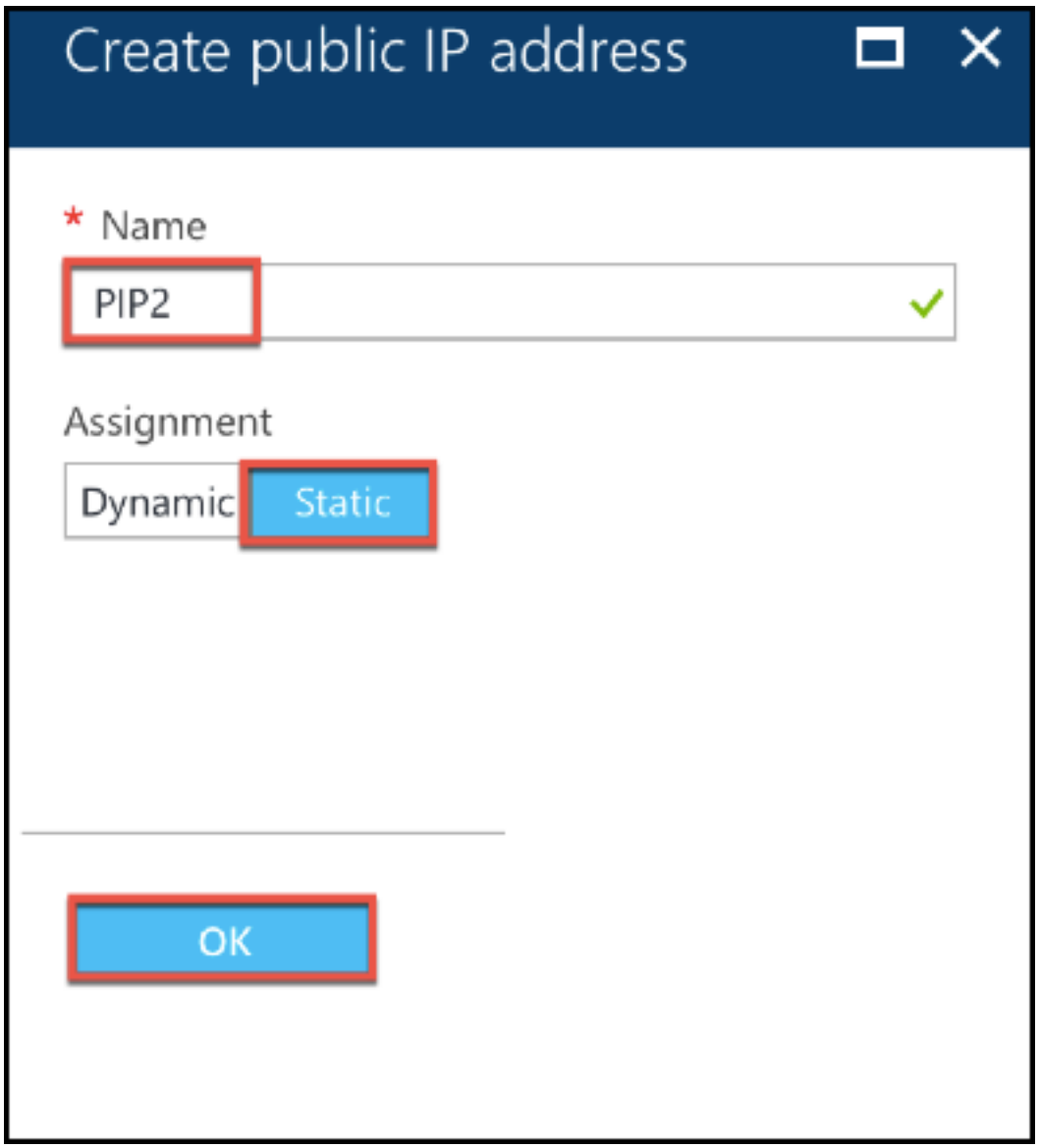
> **Hinweis:**
>
> Bevor Sie eine statische private IP-Adresse hinzufügen, überprüfen Sie die Verfügbarkeit der IP-Adresse und stellen Sie sicher, dass die IP-Adresse zu demselben Subnetz gehört, an das die Netzwerkkarte angeschlossen ist.



Klicken Sie als Nächstes auf **Erforderliche Einstellungen konfigurieren**, um eine statische öffentliche IP-Adresse für ipconfig2 zu erstellen.

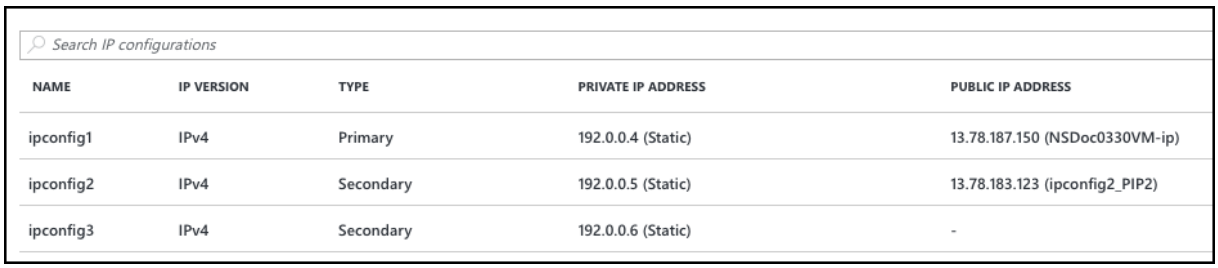
Standardmäßig sind öffentliche IPs dynamisch. Um sicherzustellen, dass die VM immer dieselbe öffentliche IP-Adresse verwendet, erstellen Sie eine statische öffentliche IP.

Fügen Sie im Blade Öffentliche IP-Adresse erstellen einen Namen hinzu, klicken Sie unter Zuweisung auf **Statisch**. Klicken Sie dann auf **OK**.



> **Hinweis:**
>
> Selbst wenn Sie die Zuweisungsmethode auf statisch festlegen, können Sie nicht die tatsächliche IP-Adresse angeben, die der öffentlichen IP-Ressource zugewiesen ist. Stattdessen wird sie aus einem Pool verfügbarer IP-Adressen am Azure-Standort zugewiesen, in dem die Ressource erstellt wird.

Führen Sie die Schritte aus, um eine weitere IP-Konfiguration für ipconfig3 hinzuzufügen. Öffentliche IP ist nicht obligatorisch.



Schritt 2: Konfigurieren von Citrix ADC-eigenen IP-Adressen

Konfigurieren Sie die Citrix ADC-eigenen IP-Adressen mit der GUI oder des Befehls`add ns ip`. Weitere Informationen finden Sie unter Konfigurieren von IP-Adressen im Besitz von Citrix ADC.

Konfigurieren eines Hochverfügbarkeitssetups mit mehreren IP-Adressen und Netzwerkkarten

October 5, 2021

In einer Microsoft Azure-Bereitstellung wird eine Hochverfügbarkeitskonfiguration von zwei Citrix ADC VPX-Instanzen mit Azure Load Balancer (ALB) erreicht. Dies wird durch die Konfiguration einer Integritätsprobe auf ALB erreicht, die jede VPX-Instanz überwacht, indem alle 5 Sekunden eine Integritätsprobe an primäre und sekundäre Instanzen gesendet wird.

In diesem Setup reagiert nur der primäre Knoten auf Integritätssonden und der sekundäre nicht. Sobald der Primärserver die Antwort an den Integritätstest sendet, beginnt die ALB den Datenverkehr an die Instanz zu senden. Wenn die primäre Instanz zwei aufeinander folgende Integritätstests nicht besteht, leitet ALB keinen Datenverkehr an diese Instanz um. Beim Failover reagiert die neue primäre Instanz auf Integritätstests und der ALB leitet den Datenverkehr an ihn weiter. Die standardmäßige VPX-Hochverfügbarkeits-Failover-Zeit beträgt drei Sekunden. Die gesamte Failover-Zeit, die für den Wechsel des Datenverkehrs dauern kann, kann maximal 13 Sekunden betragen.

Sie können ein Paar von Citrix ADC VPX -Instanzen mit mehreren Netzwerkkarten in einem aktiv-passiven Hochverfügbarkeitssetup in Azure bereitstellen. Jede NIC kann mehrere IP-Adressen enthalten.

Für eine Hochverfügbarkeitsbereitstellung mit mehreren NIC stehen folgende Optionen zur Verfügung:

- Hohe Verfügbarkeit mit Azure-Verfügbarkeitssatz
- Hochverfügbarkeit mit Azure Availability Zones

Weitere Informationen zu Azure Availability Set und Availability Zones finden Sie in der Azure-Dokumentation Verwalten der Verfügbarkeit virtueller Linux-Maschinen.

Hochverfügbarkeit mit Verfügbarkeitssatz

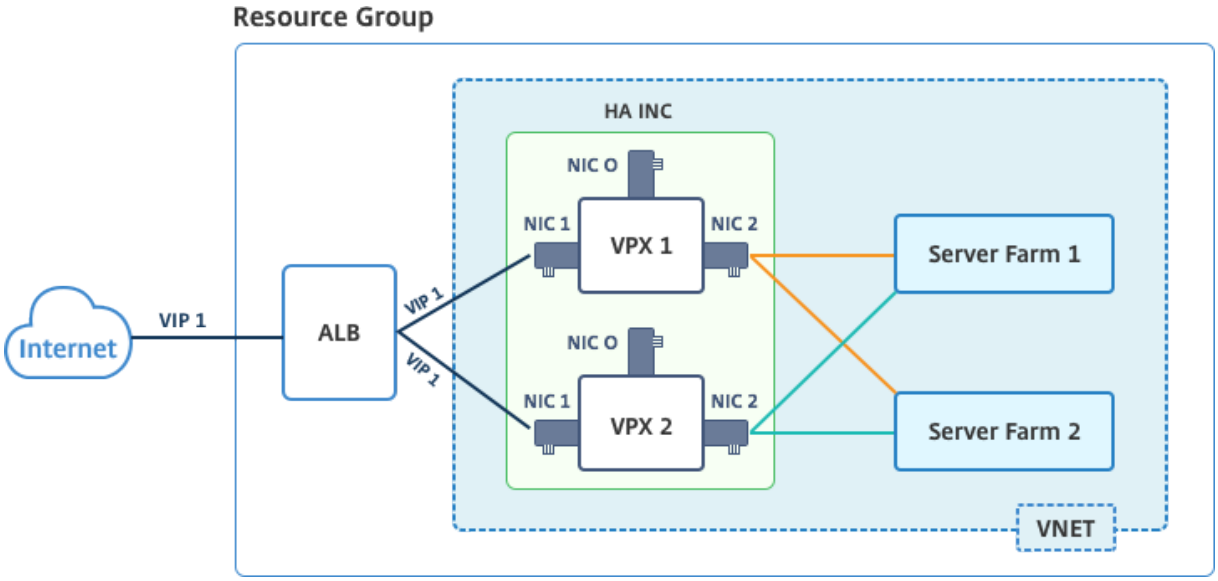
Ein Hochverfügbarkeits-Setup, das ein Verfügbarkeitsset verwendet, muss die folgenden Anforderungen erfüllen:

- Eine HA Independent Network Configuration (INC) Konfiguration
- Der Azure Load Balancer (ALB) im DSR-Modus (Direct Server Return)

Der gesamte Datenverkehr geht durch den primären Knoten. Der sekundäre Knoten bleibt im Standbymodus, bis der primäre Knoten ausfällt.

> **Hinweis:**
>
> Damit eine Citrix VPX Hochverfügbarkeitsbereitstellung in der Azure Cloud funktioniert, benötigen Sie eine Floating Public IP (PIP), die zwischen den beiden VPX-Knoten verschoben werden kann. Der Azure Load Balancer (ALB) stellt dieses schwebende PIP bereit, das im Falle eines Failovers automatisch auf den zweiten Knoten verschoben wird.

Diagramm: Beispiel für eine Hochverfügbarkeitsbereitstellungsarchitektur mit Azure Availability Set



In einer aktiv-passiven Bereitstellung werden die öffentlichen IP-Adressen (PIP) von ALB Frontend als VIP-Adressen in jedem VPX-Knoten hinzugefügt. In der HA-INC-Konfiguration sind die VIP-Adressen unverankert und SNIP-Adressen sind Instanzenpezifisch.

Sie können ein VPX-Paar im aktiven und passiven Hochverfügbarkeitsmodus auf zwei Arten bereitstellen, indem Sie Folgendes verwenden:

- **Citrix ADC VPX Standard Hochverfügbarkeitsvorlage**: Verwenden Sie diese Option, um ein HA-Paar mit der Standardoption von drei Subnetzen und sechs Netzwerkkarten zu konfigurieren.
- **Windows PowerShell Befehle**: Verwenden Sie diese Option, um ein HA-Paar entsprechend Ihren Subnetz- und NIC-Anforderungen zu konfigurieren.

In diesem Thema wird beschrieben, wie ein VPX-Paar im aktiv-passiven HA-Setup mithilfe der Citrix Vorlage bereitgestellt wird. Informationen zur Verwendung von PowerShell-Befehlen finden Sie unter Konfigurieren eines HA-Setups mit mehreren IP-Adressen und NICs mithilfe von PowerShell-Befehlen.

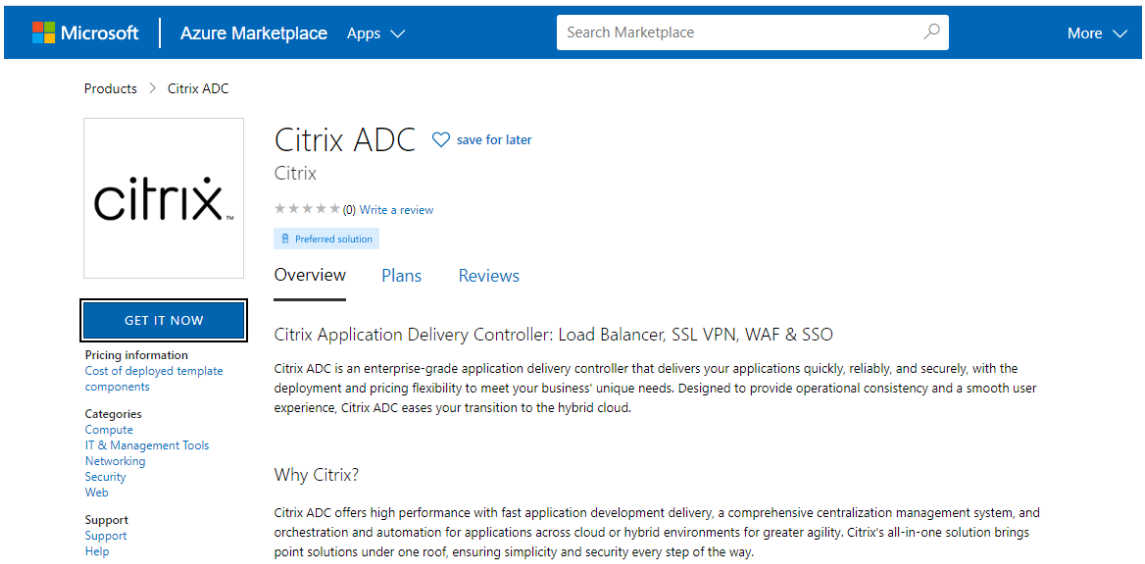
Konfigurieren von HA-INC-Knoten mithilfe der Citrix Hochverfügbarkeitsvorlage

Mithilfe der Standardvorlage können Sie ein Paar VPX-Instanzen im HA-INC-Modus schnell und effizient bereitstellen. Die Vorlage erstellt zwei Knoten mit drei Subnetzen und sechs Netzwerkkarten. Die Subnetze sind für Verwaltungs-, Client- und serverseitigen Datenverkehr, und jedes Subnetz verfügt über zwei Netzwerkkarten für beide VPX-Instanzen.

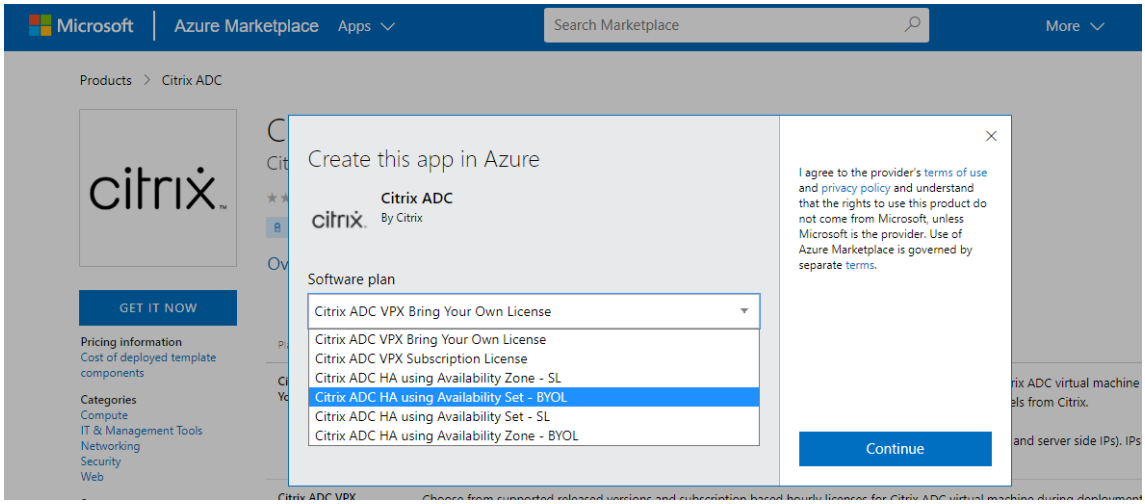
Sie können die Citrix ADC HA Pair Vorlage im Azure Marketplaceabrufen.

Führen Sie die folgenden Schritte aus, um die Vorlage zu starten und ein VPX-Paar mit hoher Verfügbarkeit bereitzustellen, indem Sie Azure-Verfügbarkeitssätze verwenden.

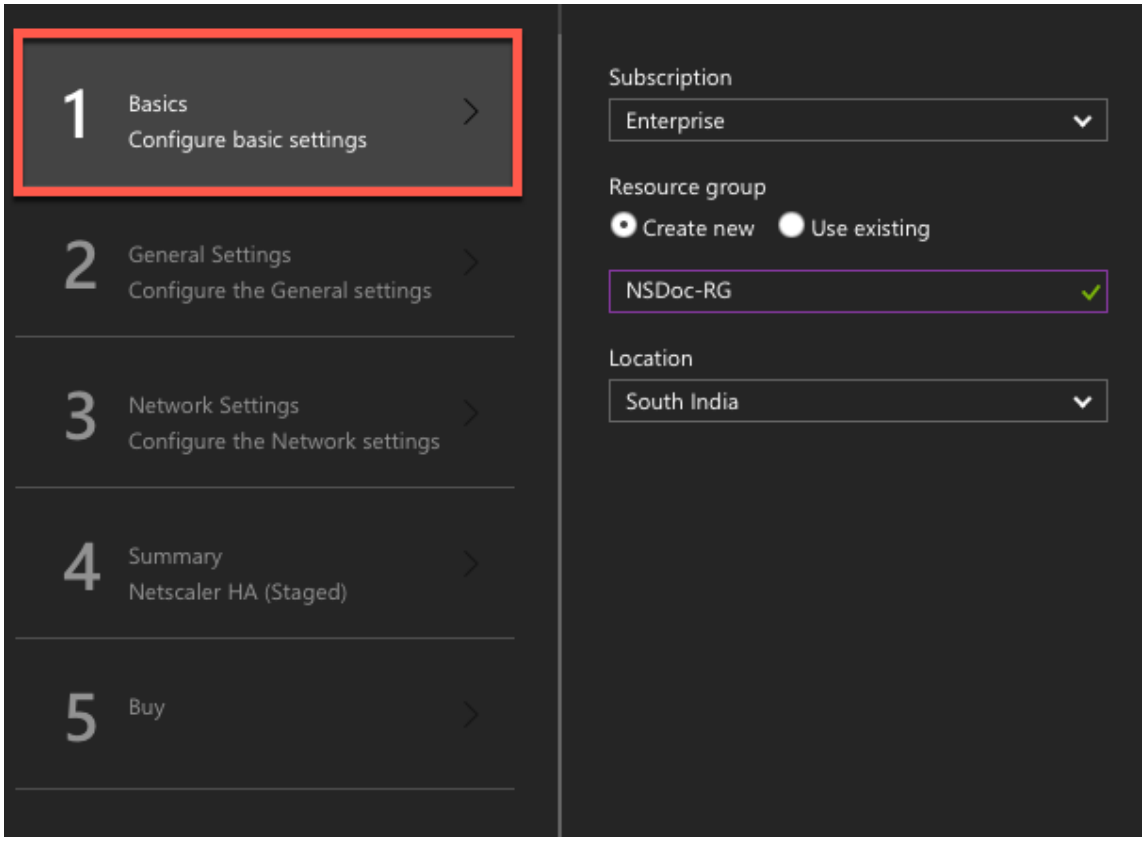
1. Suchen Sie in Azure Marketplace nach **Citrix ADC**.



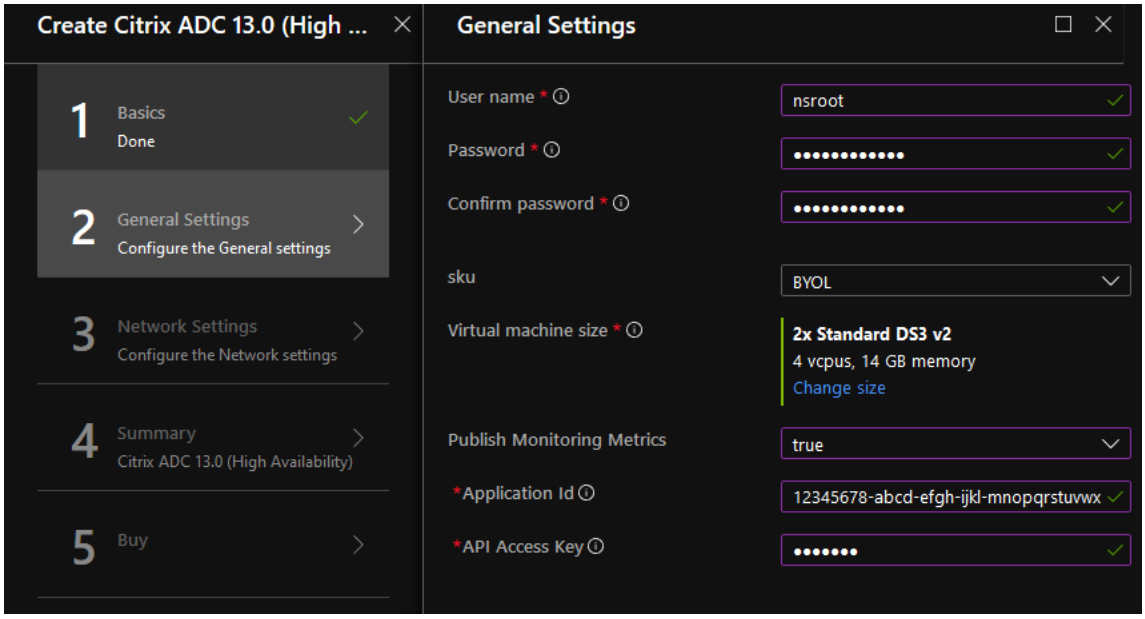
2. Klicken Sie auf **JETZT HOLEN**.
3. Wählen Sie die erforderliche HA-Bereitstellung zusammen mit der Lizenz aus und klicken Sie auf **Weiter**.



4. Die Seite **Grundlagen** wird angezeigt. Erstellen Sie eine Ressourcengruppe, und wählen Sie **OK**.

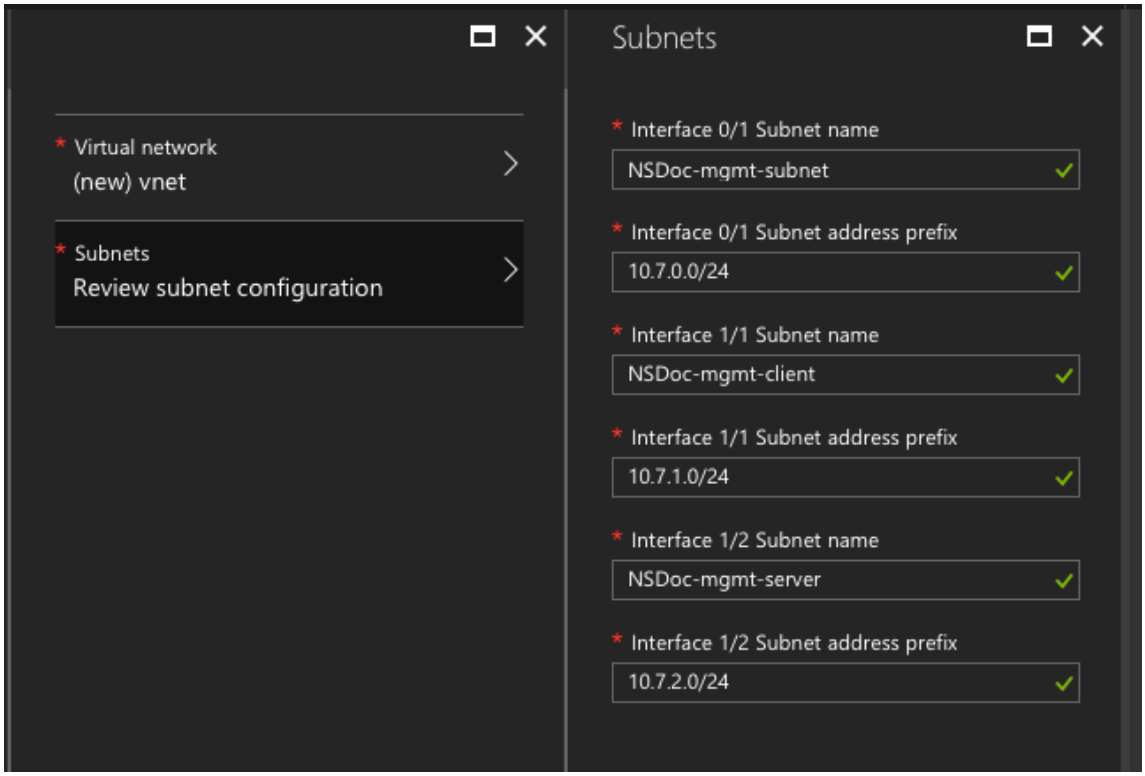


5. Die Seite **Allgemeine Einstellungen** wird angezeigt. Geben Sie die Details ein, und wählen Sie **OK**aus.



> Hinweis:
>
> Standardmäßig ist die Option " **Monitoring-Metriken veröffentlichen** " auf **"false"**festgelegt. Wenn Sie diese Option aktivieren möchten, wählen Sie " **true"**.
> Erstellen Sie eine Azure Active Directory (ADD) -Anwendung und Dienstprinzipal, die auf Ressourcen zugreifen können. Weisen Sie der neu erstellten AAD-Anwendung die Rolle der Mitwirkenden zu. Weitere Informationen finden Sie unter Verwenden des Portals zum Erstellen einer Azure Active Directory-Anwendung und eines Dienstprinzipals, die auf Ressourcen zugreifen können.

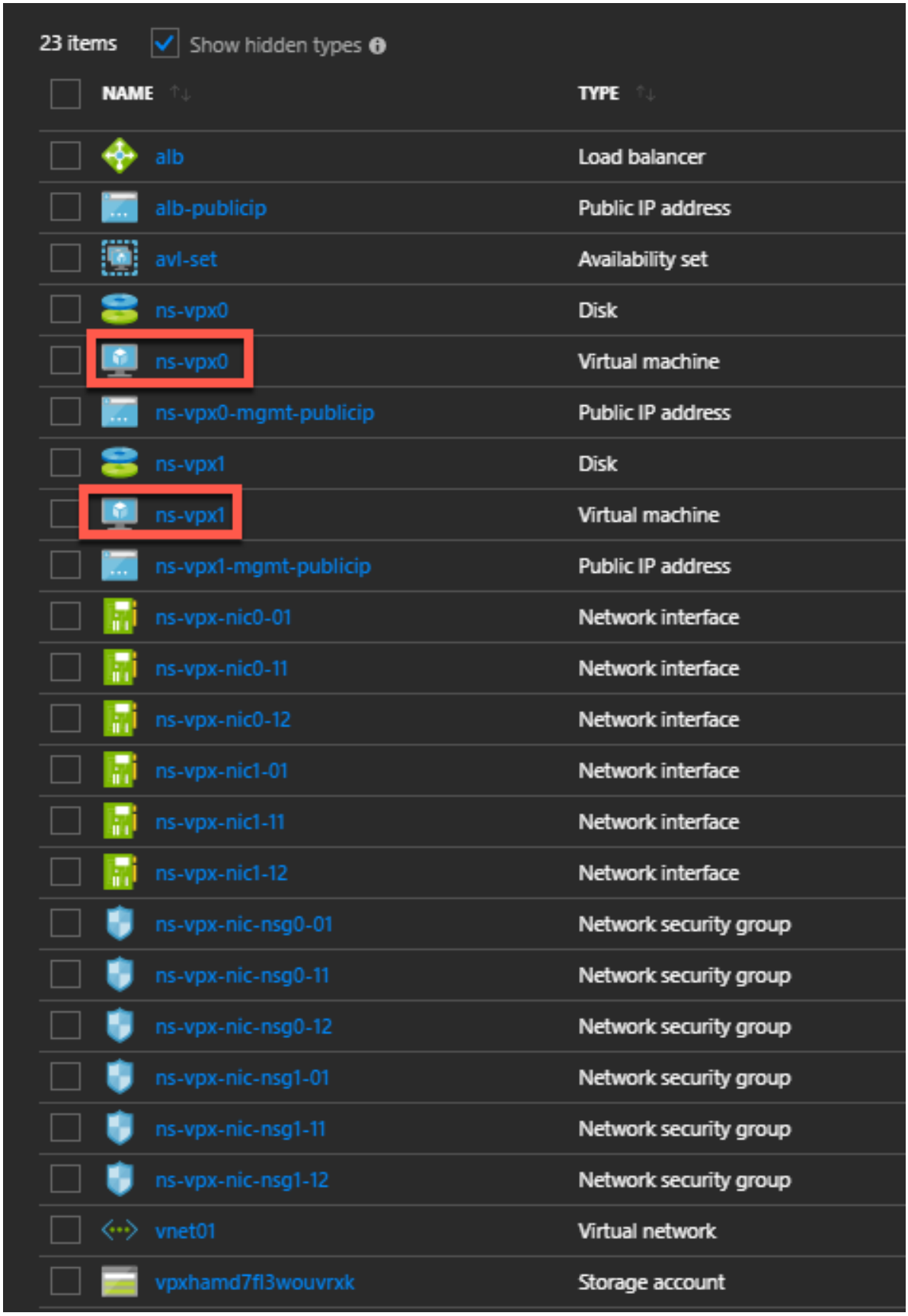
6. Die Seite **"Netzwerkeinstellungen** " wird angezeigt. Überprüfen Sie die VNet- und Subnetz-Konfigurationen, bearbeiten Sie die erforderlichen Einstellungen und wählen Sie **OK**aus.



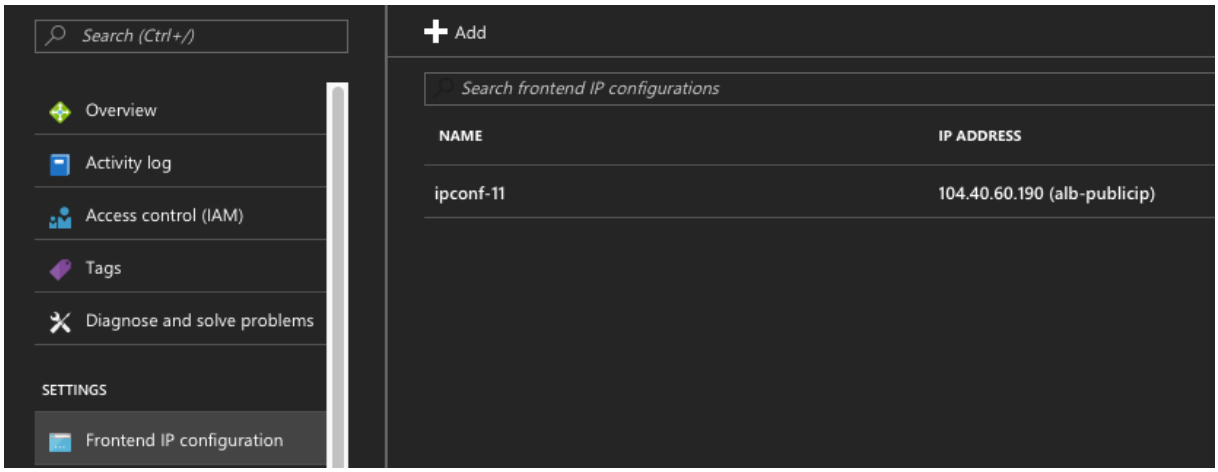
7. Die Seite **Zusammenfassung** wird angezeigt. Überprüfen Sie die Konfiguration und bearbeiten Sie entsprechend. Wählen Sie zur Bestätigung **OK** aus.
8. Die Seite **Kaufen** wird angezeigt. Wählen Sie **Kaufen**, um die Bereitstellung abzuschließen.

Es kann einen Moment dauern, bis die Azure-Ressourcengruppe mit den erforderlichen Konfigurationen erstellt wird. Wählen Sie nach Abschluss die **Ressourcengruppe** im Azure-Portal aus, um die Konfigurationsdetails wie LB-Regeln, Back-End-Pools und Integritäts-Sonden anzuzeigen. Das Hochverfügbarkeitspaar wird als ns-vpx0 und ns-vpx1 angezeigt.

Wenn weitere Änderungen für das HA-Setup erforderlich sind, z. B. das Erstellen weiterer Sicherheitsregeln und Ports, können Sie dies über das Azure-Portal vornehmen.



Als Nächstes müssen Sie den virtuellen Lastenausgleichsserver mit der **öffentlichen IP-Adresse (PIP) des ALB mit der Frontend-IP-Adresse (PIP)**auf dem primären Knoten konfigurieren. Um das ALB PIP zu finden, wählen Sie ALB > **Frontend IP-Konfiguration**.



Im Abschnitt **Ressourcen** finden Sie weitere Informationen zur Konfiguration des virtuellen Lastenausgleichsservers.

Ressourcen:

Die folgenden Links enthalten zusätzliche Informationen zur HA-Bereitstellung und zur Konfiguration virtueller Server:

- Konfigurieren von Hochverfügbarkeitsknoten in verschiedenen Subnetzen
- Einrichten des grundlegenden Lastenausgleichs

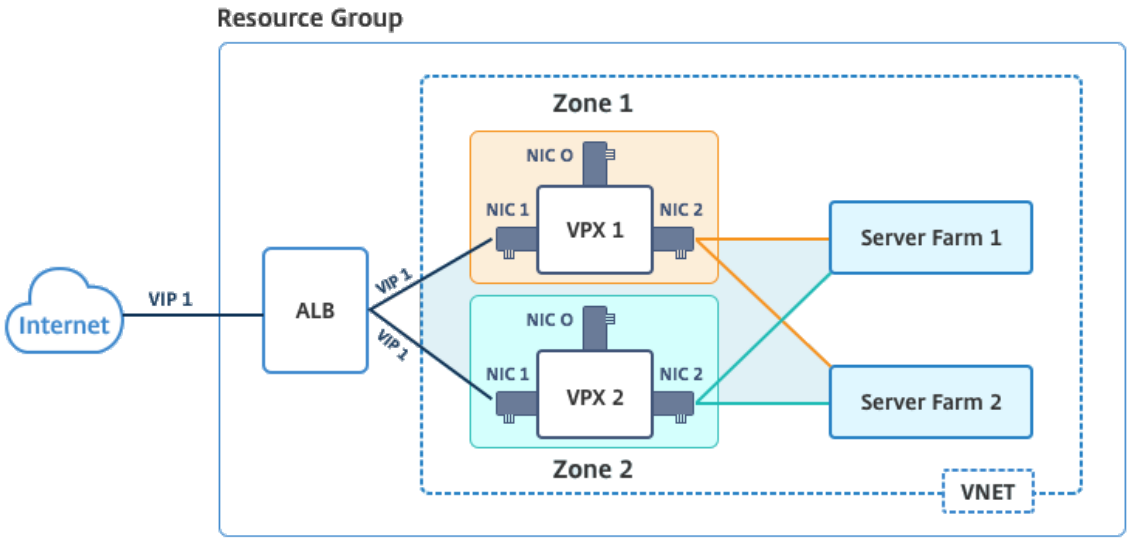
Verwandte Ressourcen:

- Konfigurieren eines Hochverfügbarkeitssetups mit mehreren IP-Adressen und Netzwerkkarten über PowerShell-Befehle
- Konfigurieren von GSLB in der aktiven Standby-HA-Bereitstellung in Azure

Hochverfügbarkeit durch Availability Zones

Azure Availability Zones sind fehlerisolierte Standorte in einer Azure-Region, die redundante Stromversorgung, Kühlung und Netzwerke bieten und die Ausfallsicherheit erhöhen. Nur bestimmte Azure-Regionen unterstützen Availability Zones. Weitere Informationen finden Sie in der Azure-Dokumentation [Was sind Availability Zones in Azure.

Diagramm: Beispiel für eine Hochverfügbarkeitsbereitstellungsarchitektur mit Azure Availability Zones



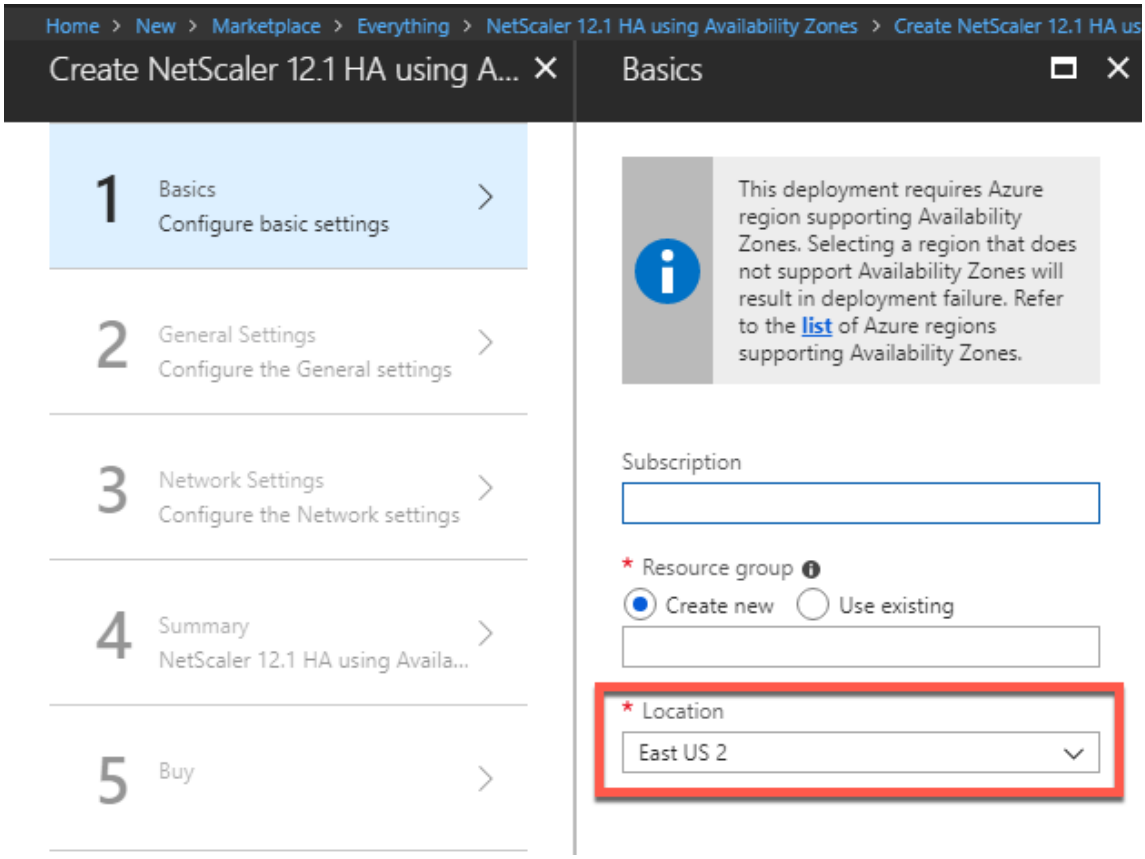
Sie können ein VPX-Paar im Hochverfügbarkeitsmodus bereitstellen, indem Sie die in Azure Marketplace verfügbare Vorlage NetScaler 13.0 HA using Availability Zones verwenden.

Führen Sie die folgenden Schritte aus, um die Vorlage zu starten und ein hochverfügbarkeitsfähiges VPX-Paar mithilfe von Azure Availability Zones bereitzustellen.

1. Wählen Sie in Azure Marketplace die Citrix Lösungsvorlage aus, und starten Sie sie.

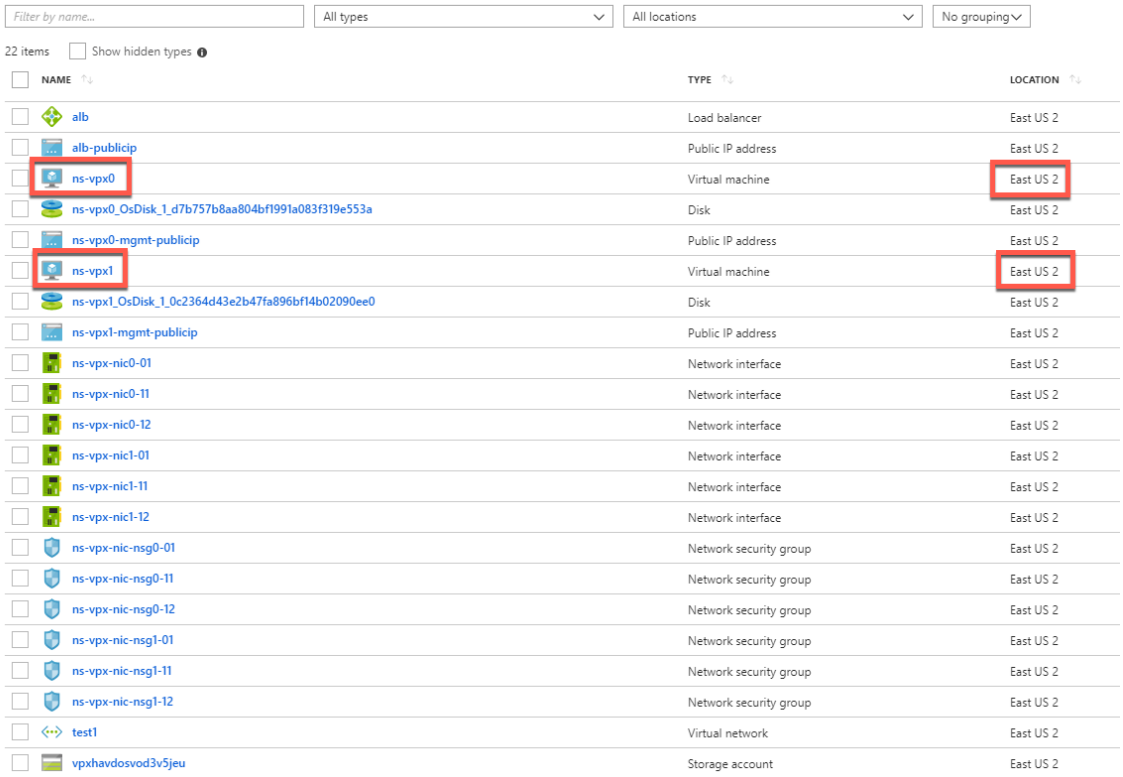
2. Stellen Sie sicher, dass der Bereitstellungstyp Resource Manager ist, und wählen Sie **Erstellen**aus.
3. Die Seite **Grundlagen** wird angezeigt. Geben Sie die Details ein und klicken Sie auf **OK**.

> Hinweis: Stellen Sie sicher, dass Sie eine Azure-Region auswählen, die Availability Zones unterstützt. Weitere Informationen zu Regionen, die Availability Zones unterstützen, finden Sie in der Azure-Dokumentation Was sind Availability Zones in Azure?



4. Die Seite **Allgemeine Einstellungen** wird angezeigt. Geben Sie die Details ein, und wählen Sie **OK**aus.
5. Die Seite **Netzwerkeinstellung** wird angezeigt. Überprüfen Sie die VNet- und Subnetz-Konfigurationen, bearbeiten Sie die erforderlichen Einstellungen und wählen Sie **OK**aus.
6. Die Seite **Zusammenfassung** wird angezeigt. Überprüfen Sie die Konfiguration und bearbeiten Sie entsprechend. Wählen Sie zur Bestätigung **OK** aus.
7. Die Seite **Kaufen** wird angezeigt. Wählen Sie **Kaufen**, um die Bereitstellung abzuschließen.

   Es kann einen Moment dauern, bis die Azure-Ressourcengruppe mit den erforderlichen Konfigurationen erstellt wird. Wählen Sie nach Abschluss die **Ressourcengruppe** aus, um die Konfigurationsdetails wie LB-Regeln, Back-End-Pools, Integritätstprobes usw. im Azure-Portal anzuzeigen. Das Hochverfügbarkeitspaar wird als ns-vpx0 und ns-vpx1 angezeigt. Sie können den Speicherort auch unter der Spalte **Standort** anzeigen.



Wenn weitere Änderungen für das HA-Setup erforderlich sind, z. B. das Erstellen weiterer Sicherheitsregeln und Ports, können Sie dies über das Azure-Portal vornehmen.

Überwachen Sie Ihre Instanz mit Metriken in Azure Monitor

Sie können Metriken auf der Azure Monitor-Datenplattform verwenden, um eine Reihe von Citrix ADC VPX-Ressourcen wie CPU, Speicherauslastung und Durchsatz zu überwachen. Der Metrikdienst überwacht Citrix ADC VPX Ressourcen, die auf Azure ausgeführt werden, in Echtzeit. Sie können den **Metrics Explorer** verwenden, um auf die gesammelten Daten zuzugreifen. Weitere Informationen finden Sie unter Übersicht über Azure Monitor-Metriken.

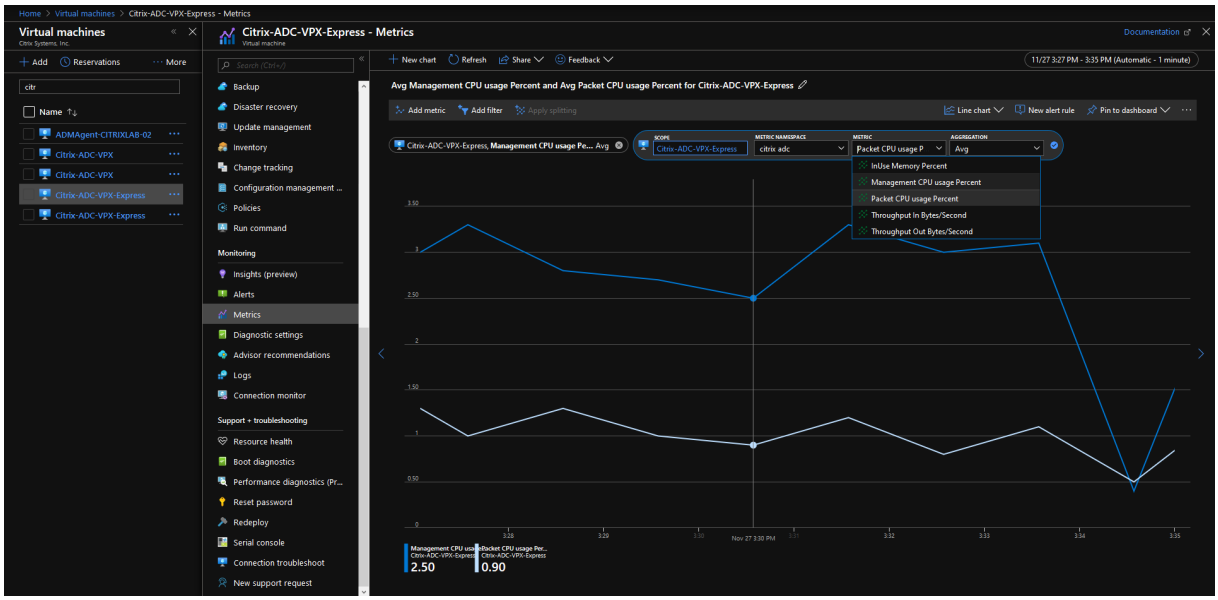
Punkte zu beachten

- Wenn Sie eine Citrix ADC VPX Instanz in Azure mithilfe des Azure Marketplace-Angebots bereitstellen, ist der Metrikdienst standardmäßig deaktiviert.
- Der Metrikdienst wird in Azure CLI nicht unterstützt.
- Metriken stehen für CPU (Management und Packet CPU-Auslastung), Arbeitsspeicher und Durchsatz (ein- und ausgehend) zur Verfügung.

So zeigen Sie Metriken im Azure-Monitor an

Gehen Sie folgendermaßen vor, um Metriken im Azure-Monitor für Ihre Instanz anzuzeigen:

1. Melden Sie sich bei **Azure Portal > Virtuelle Maschinen**an.
2. Wählen Sie die virtuelle Maschine aus, die der primäre Knoten ist.
3. Klicken Sie im Bereich **Überwachung** auf **Metriken**.
4. Klicken Sie im Dropdownmenü **Metric Namespace** auf **Citrix ADC**.
5. Klicken Sie unter **Alle Metriken** in **Metriken** Dropdownmenü auf die Metriken, die Sie anzeigen möchten.
6. Klicken Sie auf **Metrik hinzufügen**, um eine weitere Metrik im selben Diagramm anzuzeigen. Verwenden Sie die Diagrammoptionen, um Ihr Diagramm anzupassen.



Konfigurieren eines Hochverfügbarkeitssetups mit mehreren IP-Adressen und Netzwerkkarten über PowerShell-Befehle

October 5, 2021

Sie können ein Paar von Citrix ADC VPX -Instanzen mit mehreren Netzwerkkarten in einem aktiv-passiven Hochverfügbarkeitssetup in Azure bereitstellen. Jede NIC kann mehrere IP-Adressen enthalten.

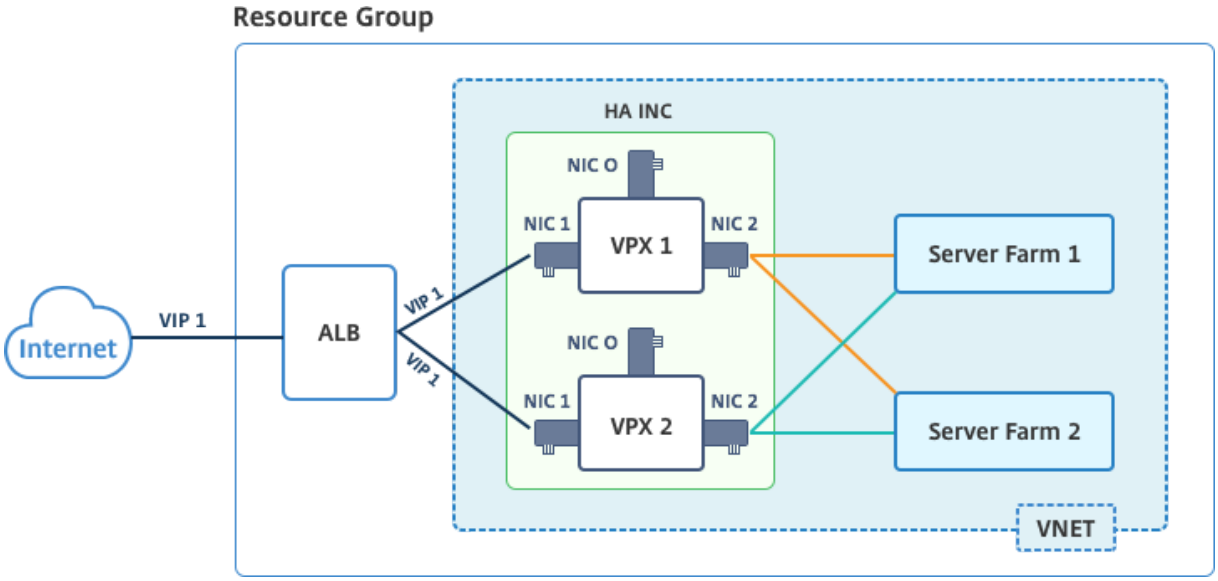
Für eine aktiv-passive Bereitstellung sind folgende Voraussetzungen erforderlich:

- Eine HA Independent Network Configuration (INC) Konfiguration
- Der Azure Load Balancer (ALB) im DSR-Modus (Direct Server Return)

Der gesamte Datenverkehr geht durch den primären Knoten. Der sekundäre Knoten bleibt im Standbymodus, bis der primäre Knoten ausfällt.

> **Hinweis:**
>
> Damit eine Citrix ADC VPX Hochverfügbarkeitsbereitstellung in einer Azure-Cloud funktioniert, benötigen Sie eine Floating Public IP (PIP), die zwischen den beiden Hochverfügbarkeitsknoten verschoben werden kann. Der Azure Load Balancer (ALB) stellt dieses schwebende PIP bereit, das im Falle eines Failovers automatisch auf den zweiten Knoten verschoben wird.

Diagramm: Beispiel einer aktiv-passiven Bereitstellungsarchitektur



In einer aktiven und passiven Bereitstellung werden die ALB Floating Public IP (PIP) Adressen als VIP-Adressen in jedem VPX-Knoten hinzugefügt. In der HA-INC-Konfiguration sind die VIP-Adressen unverankert und SNIP-Adressen sind Instanzenpezifisch.

ALB überwacht jede VPX-Instanz, indem es alle 5 Sekunden den Integritäts-Sonde sendet, und leitet den Datenverkehr nur an diese Instanz um, die die Reaktion der Integritätssonden in regelmäßigen Intervallen sendet. In einem HA-Setup reagiert der primäre Knoten auf Gesundheitssonden und sekundäre nicht. Wenn die primären Instanzen zwei aufeinanderfolgende Gesundheitssonden verpassen, leitet ALB den Datenverkehr nicht zu dieser Instanz um. Beim Failover reagiert die neue primäre Instanz auf Integritätstests und der ALB leitet den Datenverkehr an ihn weiter. Die standardmäßige VPX-Hochverfügbarkeits-Failover-Zeit beträgt drei Sekunden. Die gesamte Failoverzeit, die für die Umschaltung des Datenverkehrs benötigt wird, kann maximal 13 Sekunden betragen.

Sie können ein VPX-Paar im aktiv-passiven HA-Setup auf zwei Arten bereitstellen, indem Sie Folgendes verwenden:

- **Citrix ADC VPX Standard Hochverfügbarkeitsvorlage**: Verwenden Sie diese Option, um ein HA-Paar mit der Standardoption von drei Subnetzen und sechs Netzwerkkarten zu konfigurieren.

- **Windows PowerShell Befehle**: Verwenden Sie diese Option, um ein HA-Paar entsprechend Ihren Subnetz- und NIC-Anforderungen zu konfigurieren.

In diesem Thema wird beschrieben, wie ein VPX-Paar in aktiv-passiven HA-Setup mithilfe von PowerShell Befehlen bereitgestellt wird. Informationen zur Verwendung der Citrix ADC VPX Standard HA-Vorlage finden Sie unter Konfigurieren eines HA-Setups mit mehreren IP-Adressen und NICs.

Konfigurieren Sie HA-INC-Knoten mit PowerShell-Befehlen

Szenario: HA-INC PowerShell Bereitstellung

In diesem Szenario stellen Sie ein Citrix ADC VPX Paar mithilfe der in der Tabelle angegebenen Topologie bereit. Jede VPX-Instanz enthält drei Netzwerkkarten, wobei jede Netzwerkkarte in einem anderen Subnetz bereitgestellt wird. Jeder NIC wird eine IP-Konfiguration zugewiesen.

ALB	VPX1	VPX2
ALB ist mit öffentlicher IP 3 (pip3) verbunden	Management IP ist mit IPConfig1 konfiguriert, die eine öffentliche IP (pip1) und eine private IP (12.5.2.24) enthält; nic1; Mgmtsubnet=12.5.2.0/24	Management IP ist mit IPConfig5 konfiguriert, die eine öffentliche IP (pip3) und eine private IP (12.5.2.26) enthält; nic4; Mgmtsubnet=12.5.2.0/24
LB-Regeln und Port konfiguriert sind HTTP (80), SSL (443), Health Probe (9000)	Clientseitige IP ist mit IPConfig3 konfiguriert, die eine private IP (12.5.1.27); nic2; frontendSubet=12.5.1.0/24 enthält	Clientseitige IP ist mit IPConfig7 konfiguriert, die eine private IP (12.5.1.28) enthält; nic5; frontendSubet=12.5.1.0/24
-	Serverseitige IP ist mit IPConfig4 konfiguriert, die eine private IP (12.5.3.24); nic3; BackendSubnet=12.5.3.0/24 enthält	Serverseitige IP ist mit IPConfig8 konfiguriert, die eine private IP (12.5.3.28) enthält; nic6; BackendSubnet=12.5.3.0/24
-	Regeln und Ports für NSG sind SSH (22), HTTP (80), HTTPS (443)	-

Parametereinstellungen

Die folgenden Parametereinstellungen werden in diesem Szenario verwendet.

$locName= “South east Asia”

$rgName = “MulitIP-MultiNIC-RG”

$nicName1= “VM1-NIC1”

$nicName2 = “VM1-NIC2”

$nicName3= “VM1-NIC3”

$nicName4 = “VM2-NIC1”

$nicName5= “VM2-NIC2”

$nicName6 = “VM2-NIC3”

$vNetName = “Azure-MultiIP-ALB-vnet”

$vNetAddressRange= “12.5.0.0/16”

$frontEndSubnetName= “frontEndSubnet”

$frontEndSubnetRange= “12.5.1.0/24”

$mgmtSubnetName= “mgmtSubnet”

$mgmtSubnetRange= “12.5.2.0/24”

$backEndSubnetName = “backEndSubnet”

$backEndSubnetRange = “12.5.3.0/24”

$prmStorageAccountName = “multiipmultinicbstorage”

$avSetName = “multiple-avSet”

$vmSize= “Standard_DS4_V2”

$Publisher = “Citrix”

$offer = “netscalervpx-120”

$sku = “netscalerbyol”

$version=”latest”

$pubIPName1=”VPX1MGMT”

$pubIPName2=”VPX2MGMT”

$pubIPName3=”ALBPIP”

$domName1=”vpx1dns”

$domName2=”vpx2dns”

$domName3=”vpxalbdns”

$vmNamePrefix=”VPXMultiIPALB”

$osDiskSuffix1=”osmultiipalbdiskdb1”

$osDiskSuffix2=”osmultiipalbdiskdb2”

$lbName= “MultiIPALB”

$frontEndConfigName1= “FrontEndIP”

$backendPoolName1= “BackendPoolHttp”

$lbRuleName1= “LBRuleHttp”

$healthProbeName= “HealthProbe”

$nsgName=”NSG-MultiIP-ALB”

$rule1Name=”Inbound-HTTP”

$rule2Name=”Inbound-HTTPS”

$rule3Name=”Inbound-SSH”

Führen Sie die folgenden Schritte mithilfe von PowerShell Befehlen aus, um die Bereitstellung abzuschließen:

1. Erstellen einer Ressourcengruppe, eines Speicherkontos und eines Verfügbarkeitssatzes
2. Erstellen einer Netzwerksicherheitsgruppe und Hinzufügen von Regeln
3. Erstellen eines virtuellen Netzwerks und drei Subnetze
4. Öffentliche IP-Adressen erstellen
5. Erstellen von IP-Konfigurationen für VPX1
6. Erstellen von IP-Konfigurationen für VPX2
7. Erstellen von Netzwerkkarten für VPX1
8. Erstellen von Netzwerkkarten für VPX2
9. VPX1 erstellen
10. VPX2 erstellen
11. ALB erstellen

Erstellen Sie eine Ressourcengruppe, ein Speicherkonto und ein Verfügbarkeitsset.

```
New-AzureRmResourceGroup -Name $rgName -Location $locName

```



```
$prmStorageAccount=New-AzureRMStorageAccount -Name
    $prmStorageAccountName -ResourceGroupName $rgName -Type Standard_LRS
     -Location $locName


$avSet=New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
    $rgName -Location $locName
```

Erstellen Sie eine Netzwerksicherheitsgruppe und fügen Sie Regeln hinzu.

```
$rule1 = New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name -
    Description "Allow HTTP" -Access Allow -Protocol Tcp -Direction
    Inbound -Priority 101


-SourceAddressPrefix Internet -SourcePortRange * -
    DestinationAddressPrefix * -DestinationPortRange 80


$rule2 = New-AzureRmNetworkSecurityRuleConfig -Name $rule2Name -
    Description "Allow HTTPS" -Access Allow -Protocol Tcp -Direction
    Inbound -Priority 110


-SourceAddressPrefix Internet -SourcePortRange * -
    DestinationAddressPrefix * -DestinationPortRange 443


$rule3 = New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name -
    Description "Allow SSH" -Access Allow -Protocol Tcp -Direction
    Inbound -Priority 120


-SourceAddressPrefix Internet -SourcePortRange * -
    DestinationAddressPrefix * -DestinationPortRange 22


$nsg = New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName -
    Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,$rule3
```

Erstellen Sie ein virtuelles Netzwerk und drei Subnetze.


```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    $frontEndSubnetName -AddressPrefix $frontEndSubnetRange (this
    parameter value should be as per your requirement)


$mgmtSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name $mgmtSubnetName
     -AddressPrefix $mgmtSubnetRange


$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    $backEndSubnetName -AddressPrefix $backEndSubnetRange


$vnet =New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
    $rgName -Location $locName -AddressPrefix $vNetAddressRange -Subnet
    $frontendSubnet,$backendSubnet, $mgmtSubnet


$subnetName =”frontEndSubnet”


$subnet1=$vnet.Subnets|?{
 $_.Name -eq $subnetName }


$subnetName=”backEndSubnet”


$subnet2=$vnet.Subnets|?{
 $_.Name -eq $subnetName }


$subnetName=”mgmtSubnet”


$subnet3=$vnet.Subnets|?{
 $_.Name -eq $subnetName }
```

Erstellen Sie öffentliche IP-Adressen.

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
```



```
    $rgName -DomainNameLabel $domName1 -Location $locName -
    AllocationMethod Dynamic
2
3 $pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
    $rgName -DomainNameLabel $domName2 -Location $locName -
    AllocationMethod Dynamic
4
5 $pip3=New-AzureRmPublicIpAddress -Name $pubIPName3 -ResourceGroupName
    $rgName -DomainNameLabel $domName3 -Location $locName -
    AllocationMethod Dynamic
```

Erstellen Sie IP-Konfigurationen für VPX1.

```
1  $IpConfigName1 = ”IPConfig1”
2
3
4  $IPAddress = ”12.5.2.24”
5
6
7  $IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
     Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress $pip1
     -Primary
8
9
10 $IPConfigName3=”IPConfig-3”
11
12
13 $IPAddress=”12.5.1.27”
14
15
16 $IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
     Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary
17
18
19 $IPConfigName4 = ”IPConfig-4”
20
21
22 $IPAddress = ”12.5.3.24”
23
24
25 $IPConfig4 = New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4 -
     Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```


Erstellen Sie IP-Konfigurationen für VPX2.

```
$IpConfigName5 = ”IPConfig5”


$IPAddress=”12.5.2.26”


$IPConfig5=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName5 -
    Subnet $subnet3 -PrivateIpAddress $IPAddress -PublicIpAddress $pip2
    -Primary


$IPConfigName7=”IPConfig-7”


$IPAddress=”12.5.1.28”


$IPConfig7=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName7 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress -Primary


$IPConfigName8=”IPConfig-8”


$IPAddress=”12.5.3.28”


$IPConfig8=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName8 -
    Subnet $subnet2 -PrivateIpAddress $IPAddress -Primary
```

Erstellen Sie Netzwerkkarten für VPX1.

```
$nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig1 -
    NetworkSecurityGroupId $nsg.Id


$nic2=New-AzureRmNetworkInterface -Name $nicName2 -ResourceGroupName
    $rgName -Location $locName -IpConfiguration $IpConfig3 -
    NetworkSecurityGroupId $nsg.Id
```



```
5
6
7 $nic3=New-AzureRmNetworkInterface -Name $nicName3 -ResourceGroupName
      $rgName -Location $locName -IpConfiguration $IpConfig4 -
      NetworkSecurityGroupId $nsg.Id
```

Erstellen Sie Netzwerkkarten für VPX2.

```
1 $nic4=New-AzureRmNetworkInterface -Name $nicName4 -ResourceGroupName
      $rgName -Location $locName -IpConfiguration $IpConfig5 -
      NetworkSecurityGroupId $nsg.Id
2
3
4 $nic5=New-AzureRmNetworkInterface -Name $nicName5 -ResourceGroupName
      $rgName -Location $locName -IpConfiguration $IpConfig7 -
      NetworkSecurityGroupId $nsg.Id
5
6
7 $nic6=New-AzureRmNetworkInterface -Name $nicName6 -ResourceGroupName
      $rgName -Location $locName -IpConfiguration $IpConfig8 -
      NetworkSecurityGroupId $nsg.Id
```

Erstellen Sie VPX1.

Dieser Schritt umfasst die folgenden Teilschritte:

- VM-Konfigurationsobjekt erstellen
- Festlegen der Anmeldeinformationen, des Betriebssystems und des Images
- Netzwerkkarten hinzufügen
- Festlegen des Betriebssystemdatenträgers und Erstellen eines virtuellen Rechners

```
1  $suffixNumber = 1
2
3  $vmName=$vmNamePrefix + $suffixNumber
4
5  $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
       AvailabilitySetId $avSet.Id
6
7  $cred=Get-Credential -Message "Type the name and password for VPX
       login."
8
```



```
$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -ComputerName $vmName -Credential $cred

$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName $publisher -Offer $offer -Skus $sku -Version $version

$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id -Primary

$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2.Id

$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3.Id

$osDiskName=$vmName + "-" + $osDiskSuffix1

$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds/" + $osDiskName + ".vhd"

$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri $osVhdUri -CreateOption fromImage

Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -Name $sku

New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location $locName
```

Erstellen Sie VPX2.

```
```
$suffixNumber=2

$vmName=$vmNamePrefix + $suffixNumber

$vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId $avSet.Id

$cred=Get-Credential -Message "Type the name and password for VPX login
```

 
```

```
    .”
12
13
14 $vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
    ComputerName $vmName -Credential $cred
15
16
17 $vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
    $publisher -Offer $offer -Skus $sku -Version $version
18
19
20 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic4.Id -
    Primary
21
22
23 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic5.Id
24
25
26 $vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic6.Id
27
28
29 $osDiskName=$vmName + ”-” + $osDiskSuffix2
30
31
32 $osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + ”vhds/”
     + $osDiskName + ”.vhd”
33
34
35 $vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
    $osVhdUri -CreateOption fromImage
36
37
38 Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -
    Name $sku
39
40
41 New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
    $locName
42 <!--NeedCopy--> ```
```

Geben Sie die folgenden Befehle ein, um private und öffentliche IP-Adressen anzuzeigen, die den Netzwerkkarten zugewiesen sind:


```
```
$nic1.IPConfig

$nic2.IPConfig

$nic3.IPConfig

$nic4.IPConfig

$nic5.IPConfig

$nic6.IPConfig
<!--NeedCopy--> ```
```

**Erstellen Sie Azure-Lastenausgleich (ALB)**.

Dieser Schritt umfasst die folgenden Teilschritte:

- Frontend-IP-Konfiguration erstellen
- Integritätstest erstellen
- Back-End-Adresspool erstellen
- Erstellen von Lastenausgleichsregeln (HTTP und SSL)
- Erstellen Sie ALB mit Front-End-IP-Konfiguration, Back-End-Adresspool und LB-Regel
- Verknüpfen Sie IP-Konfiguration mit Back-End-Pools

```
$frontEndIP1=New-AzureRmLoadBalancerFrontendIpConfig -Name $frontEndConfigName1
 -PublicIpAddress $pip3

$healthProbe=New-AzureRmLoadBalancerProbeConfig -Name $healthProbeName
-Protocol Tcp -Port 9000 -IntervalInSeconds 5 -ProbeCount 2

$beAddressPool1=New-AzureRmLoadBalancerBackendAddressPoolConfig -Name
$backendPoolName1

$lbRule1=New-AzureRmLoadBalancerRuleConfig -Name $lbRuleName1 -FrontendIpConfigur
 $frontEndIP1 -BackendAddressPool $beAddressPool1 -Probe $healthProbe -
Protocol Tcp -FrontendPort 80 -BackendPort 80 -EnableFloatingIP
```


```

```
$lb=New-AzureRmLoadBalancer -ResourceGroupName $rgName -Name $lbName -
Location $locName -FrontendIpConfiguration $frontEndIP1 -LoadBalancingRule
 $lbRule1 -BackendAddressPool $beAddressPool1 -Probe $healthProbe

$nic2.IpConfigurations[0].LoadBalancerBackendAddressPools.Add($lb.
BackendAddressPools[0])

$nic5.IpConfigurations[0].LoadBalancerBackendAddressPools.Add($lb.
BackendAddressPools[0])

$lb=$lb |Set-AzureRmLoadBalancer

$nic2=$nic2 | Set-AzureRmNetworkInterface

$nic5=$nic5 | Set-AzureRmNetworkInterface
```

Nachdem Sie das Citrix ADC VPX-Paar erfolgreich bereitgestellt haben, melden Sie sich bei jeder VPX-Instanz an, um HA-INC- sowie SNIP- und VIP-Adressen zu konfigurieren.

1. Geben Sie den folgenden Befehl ein, um HA-Knoten hinzuzufügen.

   ```
   add ha node 1 PeerNodeNSIP -inc Enabled
   ```

2. Fügen Sie private IP-Adressen von clientseitigen Netzwerkkarten als SNIPs für VPX1 (NIC2) und VPX2 (NIC5) hinzu

   ```
   add nsip privateIPofNIC2 255.255.255.0 -type SNIP
   add nsip privateIPofNIC5 255.255.255.0 -type SNIP
   ```

3. Fügen Sie einen virtuellen Lastenausgleichsserver auf dem primären Knoten mit Front-End-IP-Adresse (öffentliche IP) von ALB hinzu.

   ```
   add lb virtual server v1 HTTP FrontEndIPofALB 80
   ```

Verwandte Ressourcen:

Konfigurieren von GSLB in der aktiven Standby-HA-Bereitstellung in Azure

Konfigurieren einer Citrix ADC VPX-Instanz für beschleunigte Azure-Netzwerke

December 7, 2021

Die beschleunigte Vernetzung ermöglicht die Netzwerkkarte der virtuellen Funktion (VF) mit Single Root I/O Virtualisierung (SR-IOV) auf eine virtuelle Maschine, was die Netzwerkleistung verbessert. Sie können diese Funktion bei starken Workloads verwenden, die Daten mit höherem Durchsatz mit zuverlässigem Streaming und geringerer CPU-Auslastung senden oder empfangen müssen.

Wenn eine NIC mit beschleunigter Vernetzung aktiviert ist, bündelt Azure die vorhandene paravirtualisierte (PV) -Schnittstelle der NIC mit einer SR-IOV VF-Schnittstelle. Die Unterstützung der SR-IOV VF-Schnittstelle ermöglicht und verbessert den Durchsatz der Citrix ADC VPX-Instanz.

Die beschleunigte Vernetzung bietet folgende Vorteile:

- Niedrigere Latenz
- Höhere Paketleistung pro Sekunde (pps)
- Verbesserter Durchsatz
- Reduzierter Jitter
- Verminderte CPU-Auslastung

> Hinweis:
>
> Azure-beschleunigtes Netzwerk wird ab Version 13.0 Build 76.29 auf Citrix ADC VPX-Instanzen unterstützt.

Voraussetzungen

- Stellen Sie sicher, dass Ihre VM-Größe den Anforderungen für beschleunigtes Azure-Netzwerk entspricht.
- Stoppen Sie VMs (einzeln oder in einem Verfügbarkeitssatz), bevor Sie beschleunigte Netzwerke auf einer Netzwerkkarte aktivieren.

Einschränkungen

Beschleunigtes Netzwerk kann nur für einige Instanztypen aktiviert werden. Weitere Informationen finden Sie unter Unterstützte Instanztypen.

NICs, die für beschleunigte Netzwerke unterstützt werden

Azure bietet Mellanox ConnectX3- und ConnectX4-NICs im SR-IOV-Modus für beschleunigtes Networking.

Wenn beschleunigtes Netzwerk auf einer Citrix ADC VPX-Schnittstelle aktiviert ist, bündelt Azure entweder ConnectX3- oder ConnectX4-Schnittstelle mit der vorhandenen PV-Schnittstelle einer Citrix ADC VPX Appliance.

Weitere Informationen zum Aktivieren beschleunigter Netzwerke vor dem Anschließen einer Schnittstelle an eine VM finden Sie unter Erstellen einer Netzwerkschnittstelle mit beschleunigtem Netzwerk.

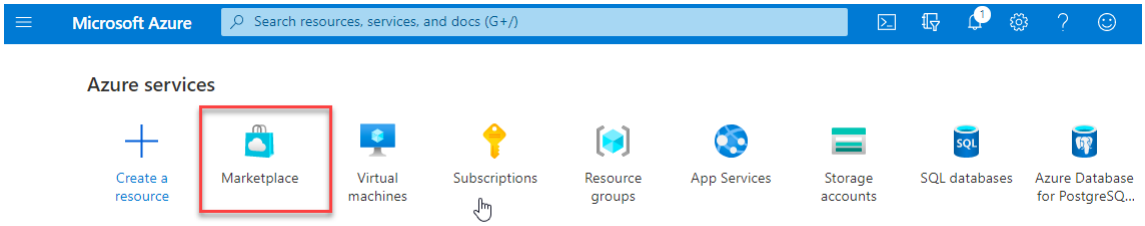
Weitere Informationen zum Aktivieren beschleunigter Netzwerke auf einer vorhandenen Schnittstelle auf einer VM finden Sie unter Aktivieren vorhandener Schnittstellen auf einer VM.

So aktivieren Sie beschleunigtes Netzwerk auf der Citrix ADC VPX-Instanz mit der Azure-Konsole

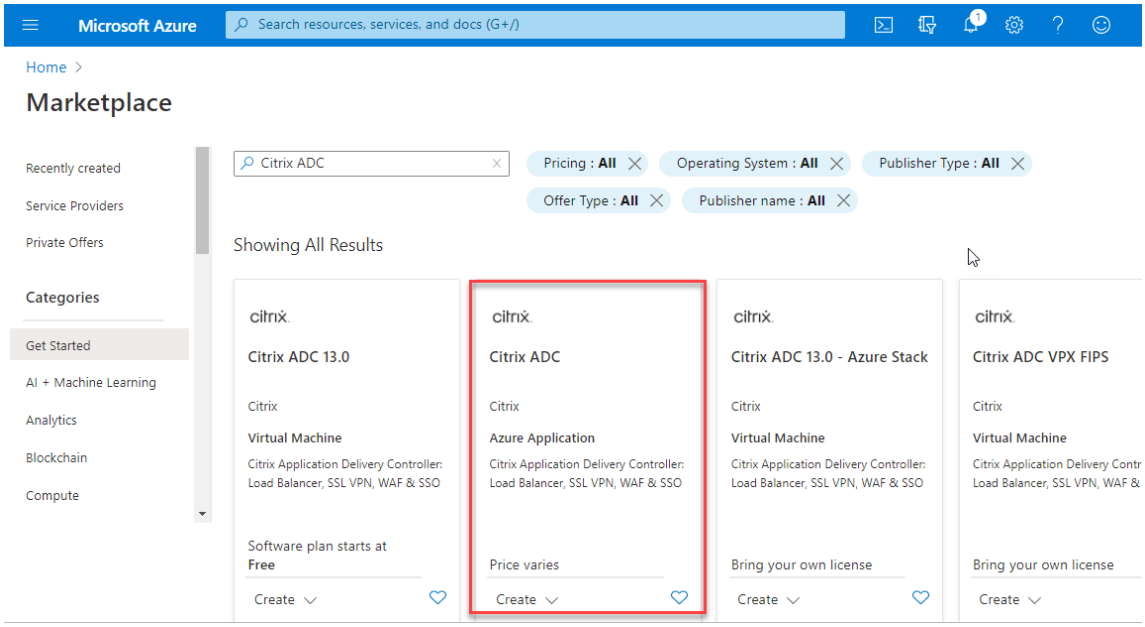
Sie können die beschleunigte Vernetzung auf einer bestimmten Schnittstelle über die Azure-Konsole oder die Azure PowerShell aktivieren.

Führen Sie die folgenden Schritte aus, um beschleunigtes Netzwerk mithilfe von Azure-Verfügbarkeitssätzen oder Availability Zones zu aktivieren.

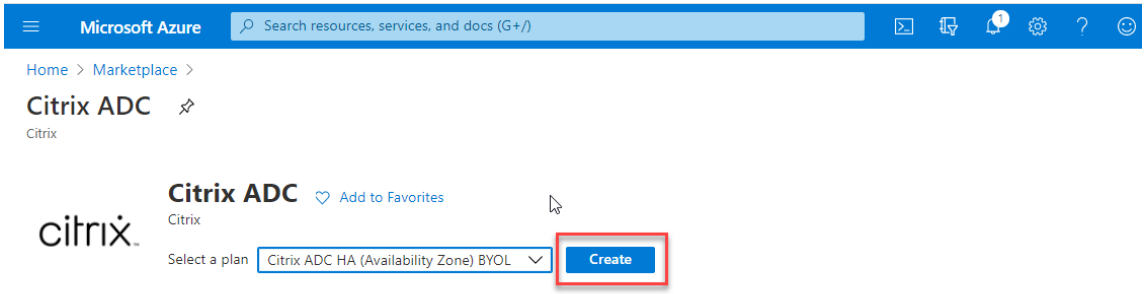
1. Melden Sie sich beim Azure-Portalan und navigieren Sie zu **Azure Marketplace**.



2. Suchen Sie im **Azure Marketplace**nach **Citrix ADC**.

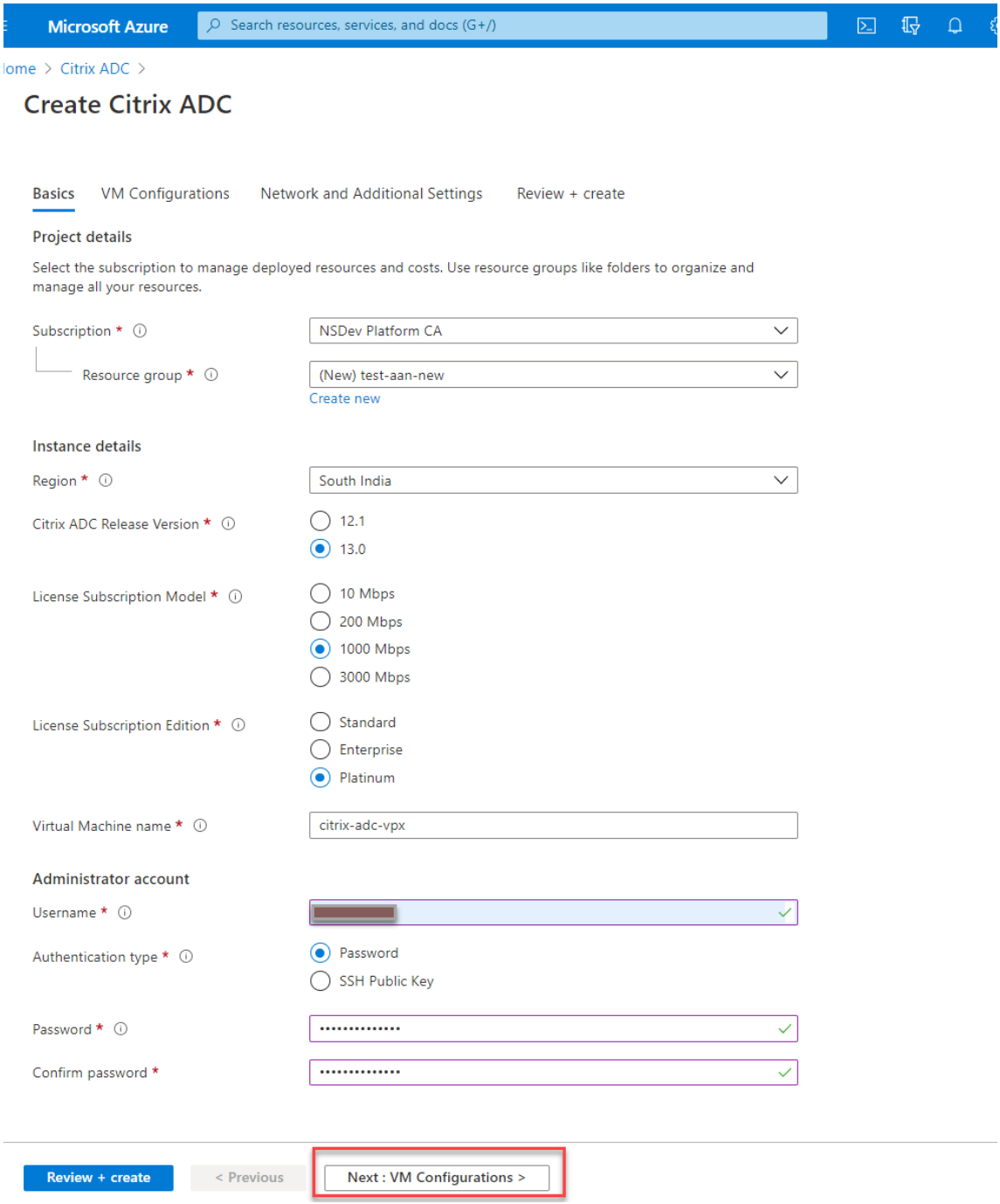


3. Wählen Sie einen Citrix ADC-Plan ohne FIPS zusammen mit der Lizenz aus und klicken Sie auf **Erstellen**.



Die Seite **Citrix ADC erstellen** wird angezeigt.

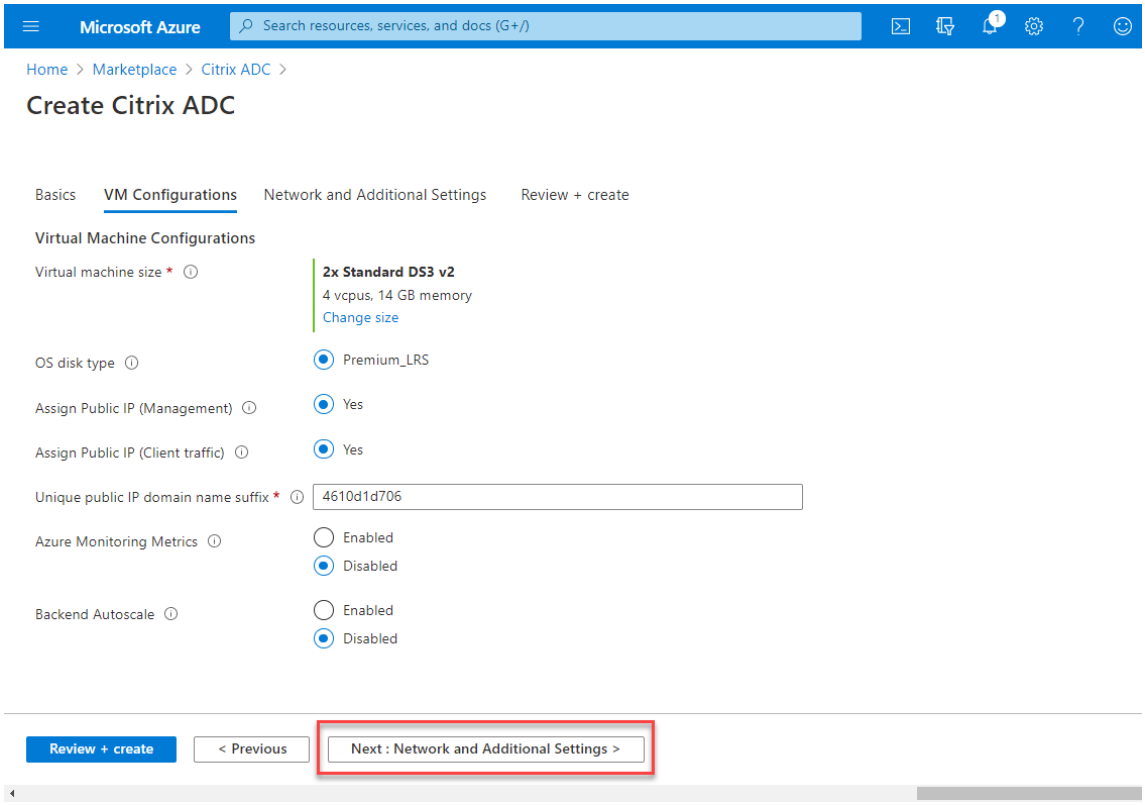
4. Erstellen Sie auf der Registerkarte **Grundlagen** eine Ressourcengruppe. Geben Sie auf der Registerkarte **Parameter** Details für die Felder Region, Admin-Benutzername, Admin-Kennwort, Lizenztyp (VM SKU) und andere ein.



5. Klicken Sie auf **Weiter: VM-Konfigurationen**.

   Führen Sie auf der Seite **VM-Konfigurationen** die folgenden Schritte aus:

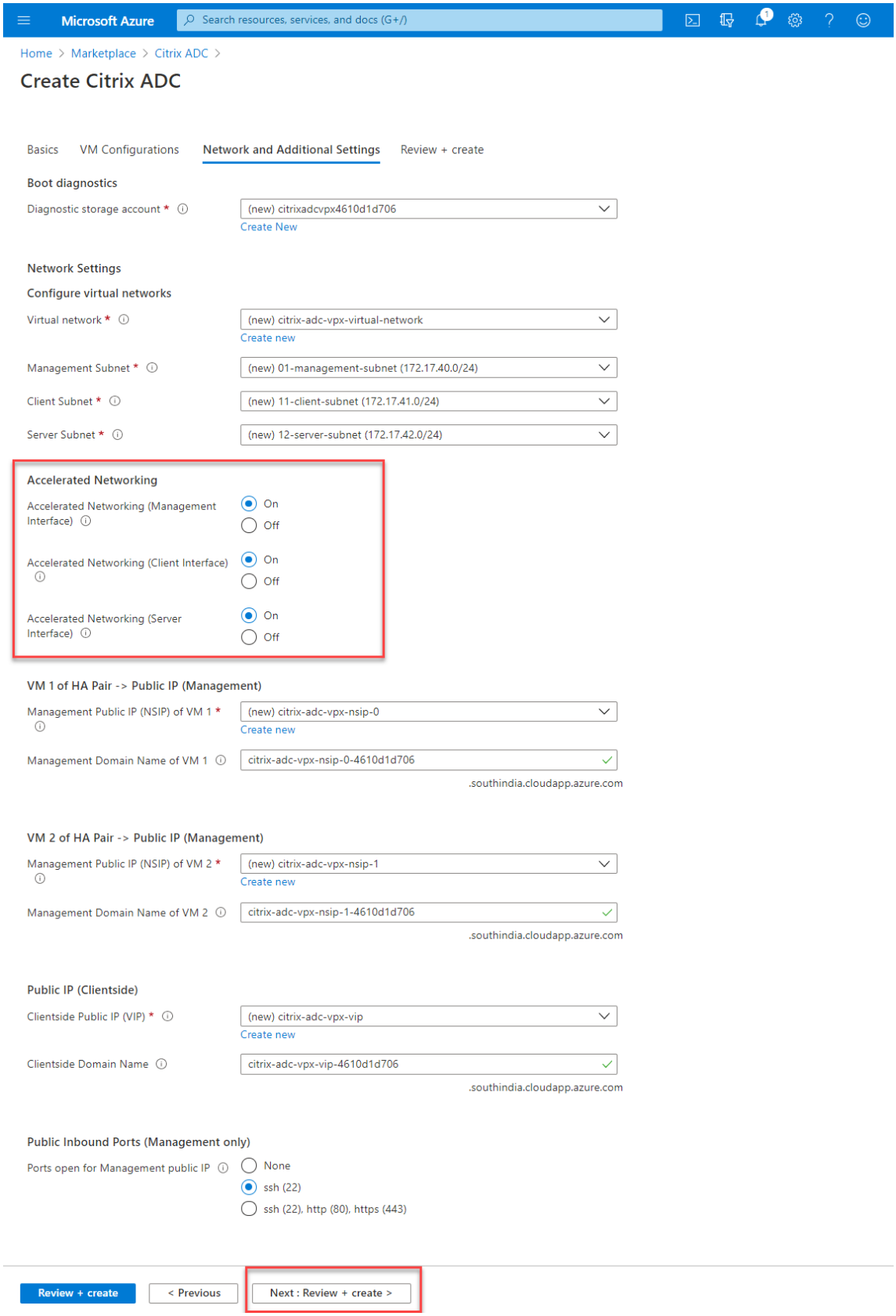
   a) Konfigurieren Sie das Suffix für öffentliche IP-Domäne
   b) Aktivieren oder deaktivieren Sie **Azure Monitoring-Metriken**.
   c) Aktivieren oder deaktivieren Sie **Backend Autoscale**.



6. Klicken Sie auf **Weiter: Netzwerk und Zusätzliche Einstellungen**.

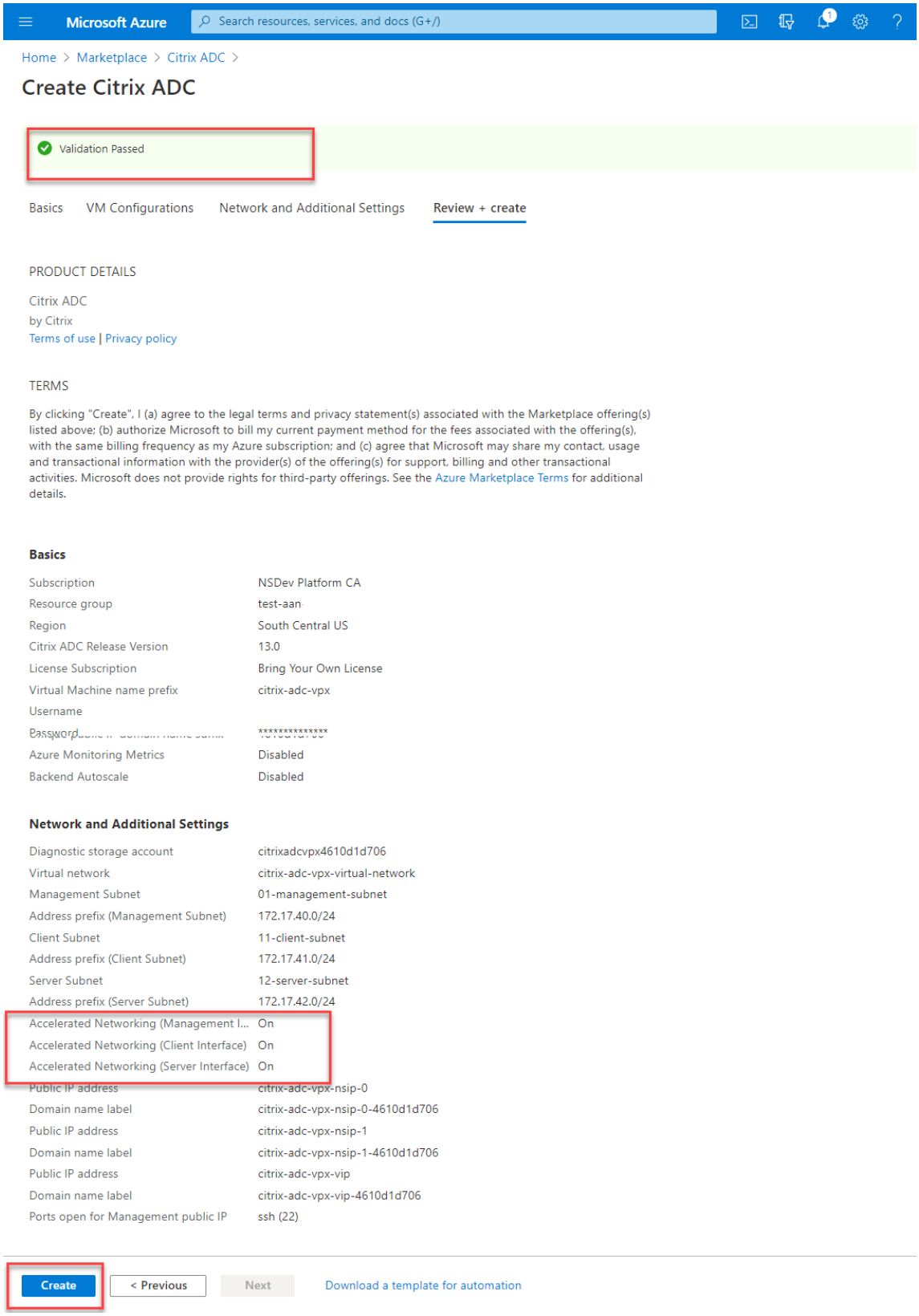
   Erstellen Sie auf der Seite **Netzwerk und zusätzliche Einstellungen** ein Boot-Diagnosekonto und konfigurieren Sie die Netzwerkeinstellungen.

   Im Abschnitt **Accelerated Networking** haben Sie die Möglichkeit, das beschleunigte Netzwerk separat für die Verwaltungsschnittstelle, die Client-Schnittstelle und die Serverschnittstelle zu aktivieren oder zu deaktivieren.



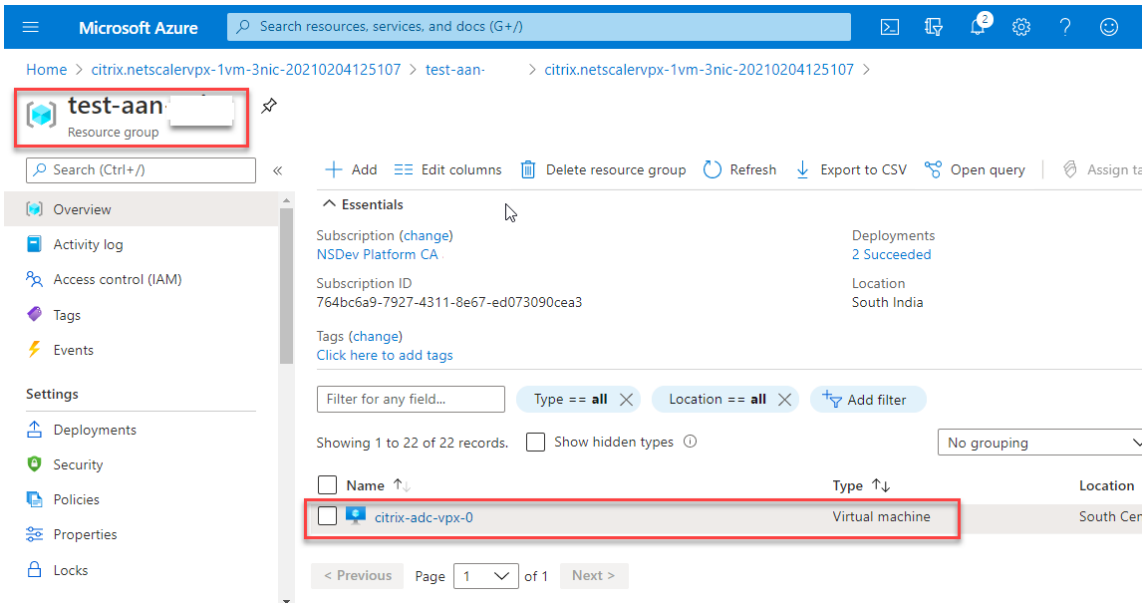
7. Klicken Sie auf **Weiter: Überprüfen + erstellen**.

   Überprüfen Sie nach erfolgreicher Validierung die Grundeinstellungen, VM-Konfigurationen, das Netzwerk und zusätzliche Einstellungen und klicken Sie auf **Erstellen**. Es kann einige Zeit dauern, bis die Azure-Ressourcengruppe mit den erforderlichen Konfigurationen erstellt wurde.

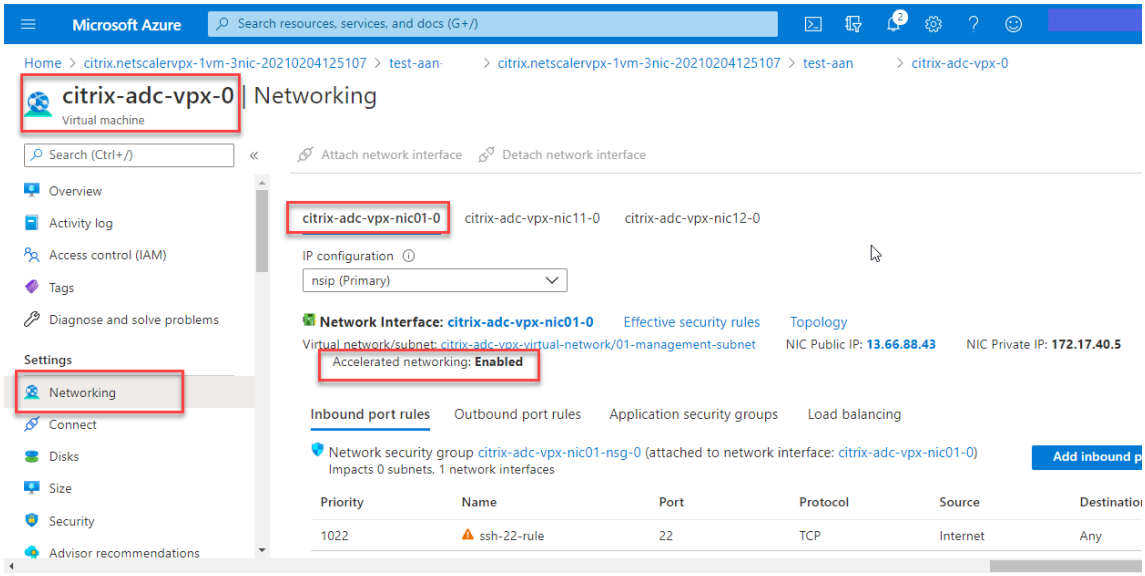


8. Wählen Sie nach Abschluss der Bereitstellung die **Ressourcengruppe** aus, um die Konfigura-

tionsdetails anzuzeigen.



9. Um die Konfigurationen für beschleunigte Netzwerke zu überprüfen, wählen Sie **Virtuelle Maschine > Netzwerk** aus. Der Status “Beschleunigtes Netzwerk” wird für jede Netzwerkkarte als **Aktiviert** oder **Deaktiviert** angezeigt.



Aktivieren Sie beschleunigte Netzwerke mit Azure PowerShell

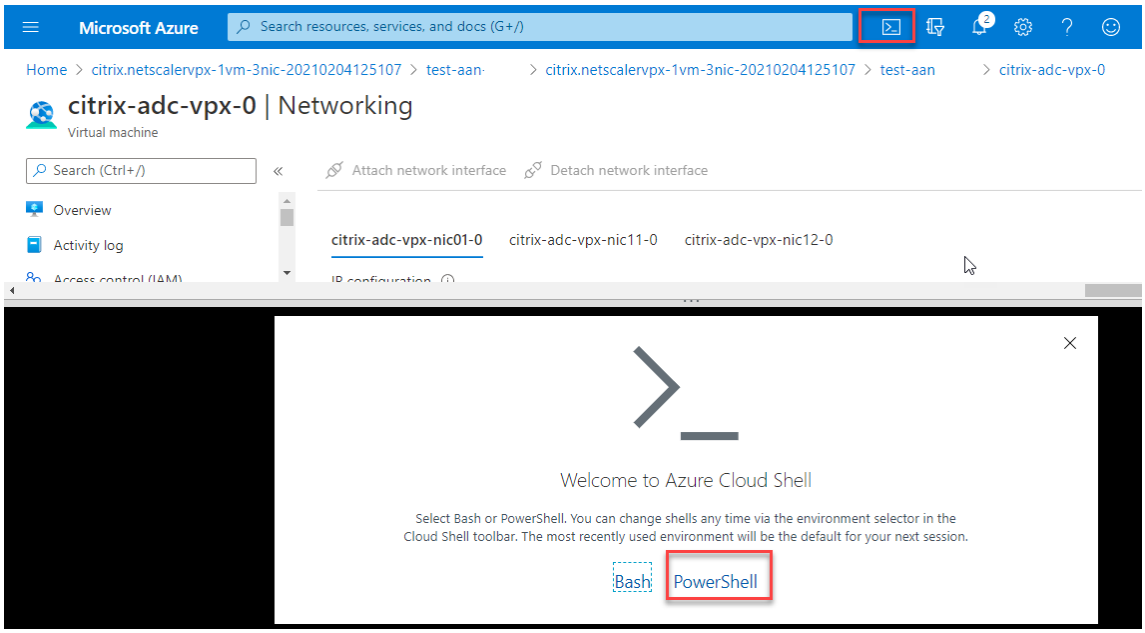
Wenn Sie nach der VM-Erstellung beschleunigtes Netzwerk aktivieren müssen, können Sie dies mit Azure PowerShell tun.

> Hinweis:
>
> Stellen Sie sicher, dass Sie die VM beenden, bevor Sie Accelerated Networking mit Azure PowerShell aktivieren.

Führen Sie die folgenden Schritte aus, um beschleunigtes Netzwerk mithilfe von Azure PowerShell zu aktivieren.

1. Navigieren Sie zum **Azure-Portal**und klicken Sie auf das **PowerShell-Symbol** in der rechten oberen Ecke.

   > Hinweis:
   >
   > Wenn Sie sich im Bash-Modus befinden, wechseln Sie in den PowerShell-Modus.



2. Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

```
az network nic update --name <nic-name> --accelerated-networking [true | false] --resource-group <resourcegroup-name>
<!--NeedCopy-->
```

Der beschleunigte Netzwerkparameter akzeptiert einen der folgenden Werte:

- **True:** Aktiviert beschleunigtes Netzwerk auf der angegebenen NIC.
- **False:** Deaktiviert das beschleunigte Netzwerk auf der angegebenen Netzwerkkarte.

So aktivieren Sie beschleunigtes Netzwerk auf einer bestimmten NIC:

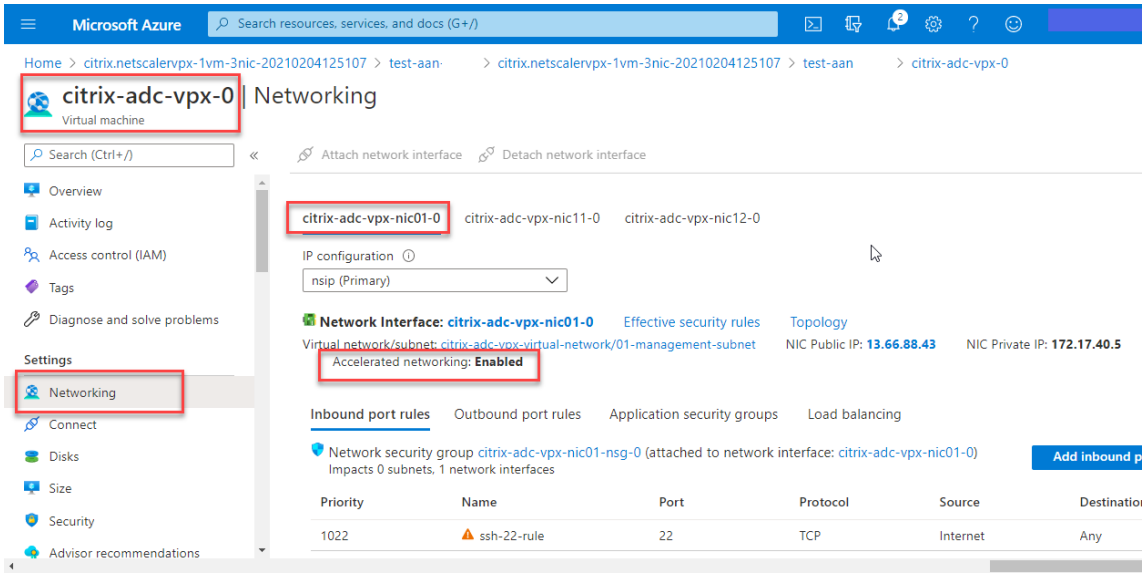

```
az network nic update --name citrix-adc-vpx-nic01-0 --accelerated-networking true --resource-group rsgp1-aan
<!--NeedCopy-->
```

So deaktivieren Sie das beschleunigte Netzwerk auf einer bestimmten NIC:

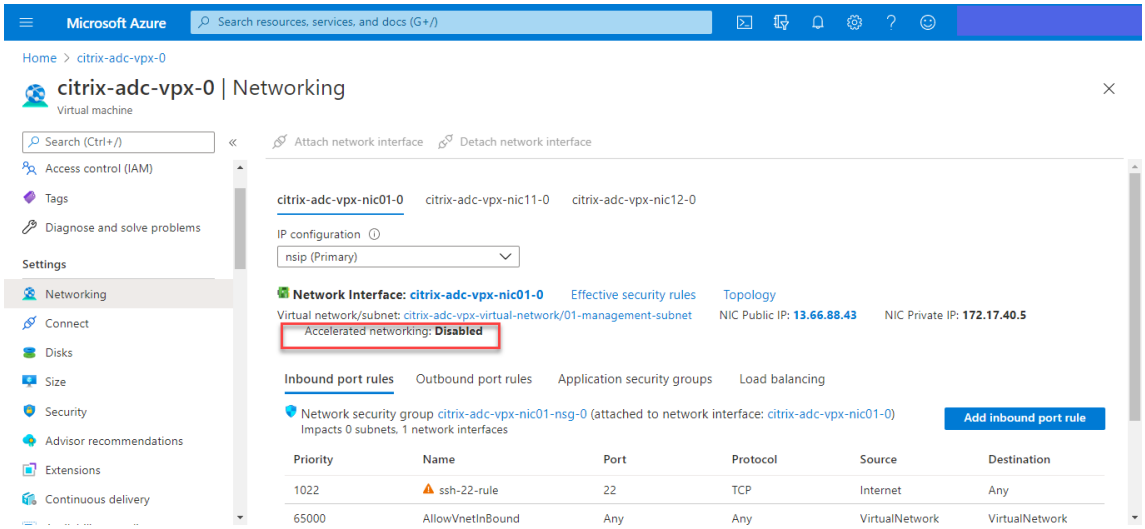
```
az network nic update --name citrix-adc-vpx-nic01-0 --accelerated-networking false --resource-group rsgp1-aan
<!--NeedCopy-->
```

3. Um den Status “Beschleunigtes Netzwerk” nach Abschluss der Bereitstellung zu überprüfen, navigieren Sie zu **VM > Netzwerk**.

   Im folgenden Beispiel sehen Sie, dass Accelerated Networking **aktiviert**ist.



   Im folgenden Beispiel sehen Sie, dass Accelerated Networking **deaktiviert**ist.



So überprüfen Sie beschleunigte Netzwerke auf einer Schnittstelle mithilfe der FreeBSD Shell von Citrix ADC

Sie können sich bei der FreeBSD-Shell von Citrix ADC anmelden und die folgenden Befehle ausführen, um den Status der beschleunigten Netzwerke zu überprüfen.

Beispiel für ConnectX3 NIC:

Das folgende Beispiel zeigt die Befehlsausgabe “ifconfig” der Mellanox ConnectX3-NIC. Der “50/n” zeigt die VF-Schnittstellen der Mellanox ConnectX3-NICs an. 0/1 und 1/1 geben die PV-Schnittstellen der Citrix ADC VPX-Instanz an. Sie können beobachten, dass sowohl die PV-Schnittstelle (1/1) als auch die CX3-VF-Schnittstelle (50/1) dieselben MAC-Adressen haben (00:22:48:1 c: 99:3 e). Dies deutet darauf hin, dass die beiden Schnittstellen gebündelt sind.


```
root@nvr-us-cx3# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=3<RXCSUM,TXCSUM>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
0/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:0d:3a:98:71:be
        inet 172.16.27.11 netmask 0xffffff00 broadcast 172.16.27.255
        inet6 fe80::20d:3aff:fe98:71be%0/1 prefixlen 64 autoconf scopeid 0x2
        nd6 options=3<PERFORMNUD,ACCEPT_RTADV>
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
1/1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=80019<RXCSUM,VLAN_MTU,VLAN_HWTAGGING,LINKSTATE>
        ether 00:22:48:1c:99:3e
        media: Ethernet autoselect (10Gbase-T <full-duplex>)
        status: active
50/1: flags=8842<BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500

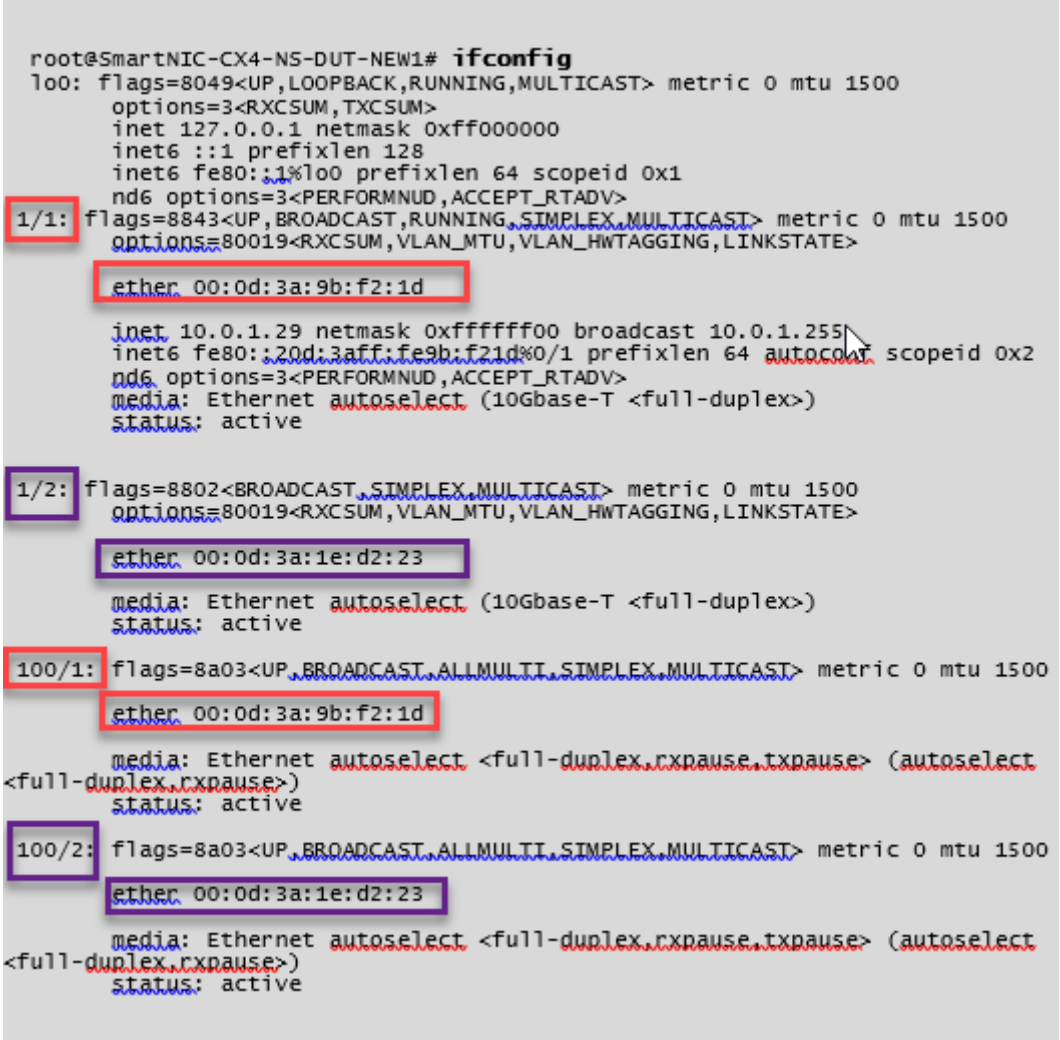
options=900b8<VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HWCSUM,VLAN_HWFILTER,LINKSTATE>
        ether 00:22:48:1c:99:3e
        media: Ethernet autoselect (<unknown subtype>)
        status: active
```

Beispiel für ConnectX4 NIC:

Das folgende Beispiel zeigt die Befehlsausgabe “ifconfig” der Mellanox ConnectX4-NIC. Der “100/n” zeigt die VF-Schnittstellen der Mellanox ConnectX4-NICs an. 0/1, 1/1 und 1/2 zeigt die PV-Schnittstellen der Citrix ADC VPX-Instanz an.

Sie können beobachten, dass sowohl die PV-Schnittstelle (1/1) als auch die CX4-VF-Schnittstelle (100/1) dieselben MAC-Adressen haben (00:0 d:3a:9b:f 2:1 d). Dies deutet darauf hin, dass die beiden Schnittstellen gebündelt sind. In ähnlicher Weise haben die PV-Schnittstelle (1/2) und die CX4

VF-Schnittstelle (100/2) dieselben MAC-Adressen (00:0 d:3a:1e:d 2:23).



So überprüfen Sie die beschleunigte Vernetzung auf einer Schnittstelle mit ADC CLI

Beispiel für ConnectX3 NIC:

Die folgende show interface befehlsausgabe zeigt an, dass die PV-Schnittstelle 1/1 mit der virtuellen Funktion 50/1 gebündelt ist, bei der es sich um eine SR-IOV VF-NIC handelt. Die MAC-Adressen von 1/1- und 50/1-NICs sind identisch. Nachdem die beschleunigte Vernetzung aktiviert wurde, werden die Daten der 1/1-Schnittstelle über den Datenpfad der 50/1-Schnittstelle gesendet, bei der es sich um eine ConnectX3-Schnittstelle handelt. Sie können sehen, dass der “show interface” -Ausgang der PV-Schnittstelle (1/1) auf den VF (50/1) zeigt. In ähnlicher Weise zeigt der “show interface” -Ausgang der VF-Schnittstelle (50/1) auf die PV-Schnittstelle (1/1).


```
> show interface 1/1

        Interface 1/1 (NetScaler Virtual Interface, SmartNIC, VF 50/1 Datapath 50/1) #1
        flags=0xe060 <ENABLED, UP, UP, HEARTBEAT, 802.1q>
        MTU=1500, native vlan=1, MAC=00:22:48:1c:99:3e, uptime 0h00m07s
        LLDP Mode: NONE,                LR Priority: 1024

        RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.

Done

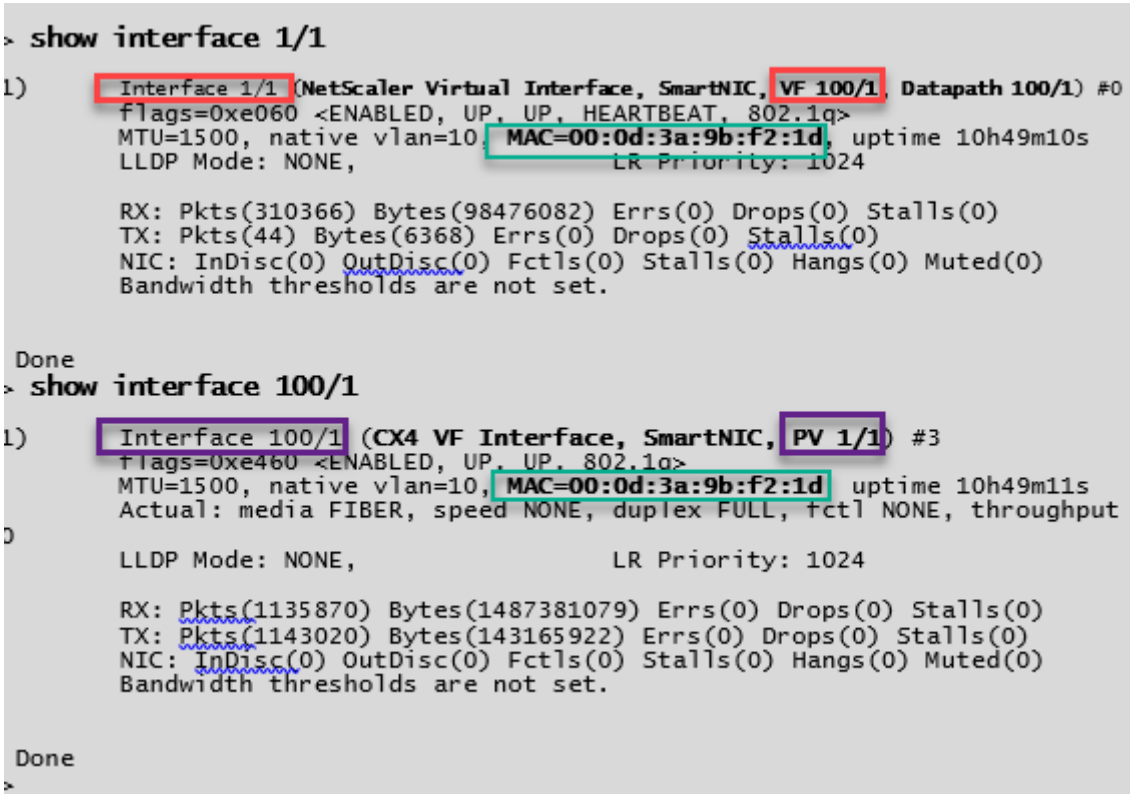
> show interface 50/1

      Interface 50/1 (CX3 VF Interface, SmartNIC, PV 1/1) #2
        flags=0xe460 <ENABLED, UP, UP, 802.1q>
        MTU=1500, native vlan=1, MAC=00:22:48:1c:99:3e, uptime 0h00m08s
        Actual: media NONE, speed 50000, duplex FULL, fctl NONE, throughput 50000
        LLDP Mode: NONE,                LR Priority: 1024

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

Beispiel für ConnectX4 NIC:

Die folgende show interface befehlsausgabe zeigt an, dass die PV-Schnittstelle 1/1 mit der virtuellen Funktion 100/1 gebündelt ist, bei der es sich um eine SR-IOV VF-NIC handelt. Die MAC-Adressen von 1/1- und 100/1-NICs sind identisch. Nachdem die beschleunigte Vernetzung aktiviert wurde, werden die Daten der 1/1-Schnittstelle über den Datenpfad der 100/1-Schnittstelle gesendet, bei der es sich um eine ConnectX4-Schnittstelle handelt. Sie können sehen, dass der “show interface” -Ausgang der PV-Schnittstelle (1/1) auf den VF (100/1) zeigt. In ähnlicher Weise zeigt der “show interface” -Ausgang der VF-Schnittstelle (100/1) auf die PV-Schnittstelle (1/1).



Zu beachtende Punkte in Citrix ADC

- Die PV-Schnittstelle gilt als primäre oder Hauptschnittstelle für alle notwendigen Operationen. Konfigurationen müssen nur an PV-Schnittstellen durchgeführt werden.
- Alle “set” -Operationen auf einer VF-Schnittstelle sind mit Ausnahme der folgenden blockiert:
  - Schnittstelle aktivieren
  - Interface deaktivieren
  - Schnittstelle zurücksetzen
  - klare Statistiken

  > Hinweis:
  >
  > Citrix empfiehlt, dass Sie keine Vorgänge auf der VF-Schnittstelle ausführen.
- Sie können die Bindung der PV-Schnittstelle mit der VF-Schnittstelle mit dem `show interface` Befehl überprüfen.

Konfigurieren Sie ein VLAN für eine PV-Schnittstelle

Wenn eine PV-Schnittstelle an ein VLAN gebunden ist, ist die zugehörige beschleunigte VF-Schnittstelle auch an dasselbe VLAN wie die PV-Schnittstelle gebunden. In diesem Beispiel ist die

PV-Schnittstelle (1/1) an VLAN (20) gebunden. Die VF-Schnittstelle (100/1), die mit der PV-Schnittstelle (1/1) gebündelt ist, ist ebenfalls an VLAN 20 gebunden.

Beispiel:

1. Erstellen Sie ein VLAN.

```
add vlan 20
<!--NeedCopy-->
```

2. Binden Sie ein VLAN an die PV-Schnittstelle.

```
bind vlan 20  -ifnum 1/1

show vlan

1)  VLAN ID: 1
    Link-local IPv6 addr: fe80::20d:3aff:fe9b:f21d/64
    Interfaces : LO/1

2)  VLAN ID: 10     VLAN Alias Name:
    Interfaces : 0/1 100/1
    IPs : 10.0.1.29  Mask: 255.255.255.0

3)  VLAN ID: 20     VLAN Alias Name:
    Interfaces :  1/1 100/2

<!--NeedCopy-->
```

> Hinweis:
>
> Der VLAN-Bindungsvorgang ist auf einer beschleunigten VF-Schnittstelle nicht zulässig.

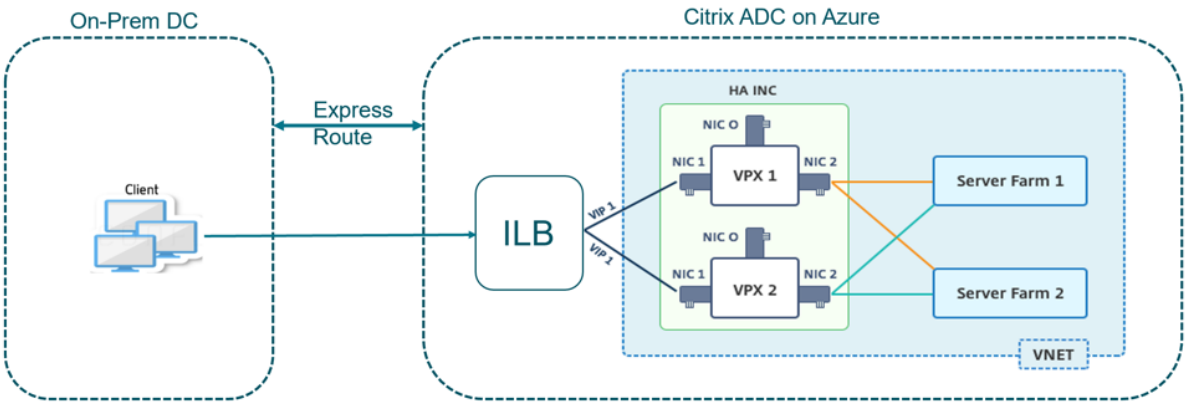
```
bind vlan 1 -ifnum 100/1
ERROR: Operation not permitted
<!--NeedCopy-->
```


Konfigurieren von HA-INC-Knoten über die Citrix Hochverfügbarkeitsvorlage mit Azure ILB

January 25, 2022

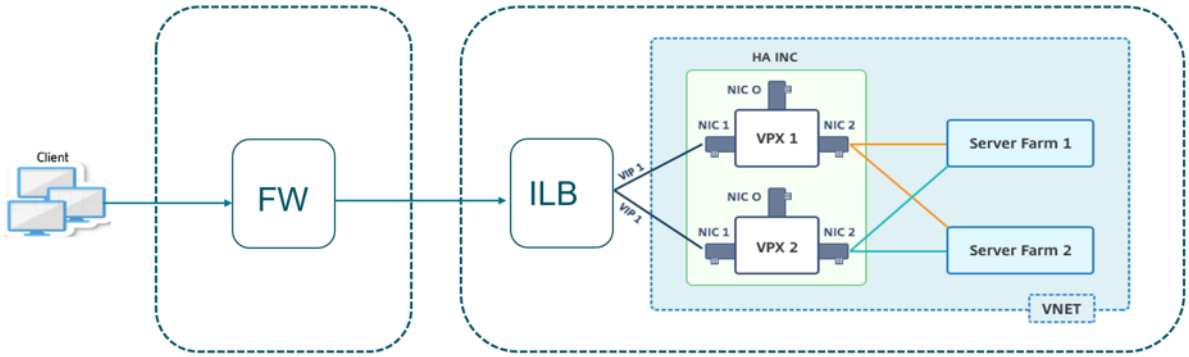
Sie können schnell und effizient ein Paar VPX-Instanzen im HA-INC-Modus bereitstellen, indem Sie die Standardvorlage für Intranetanwendungen verwenden. Der Azure Internal Load Balancer (ILB) verwendet eine interne oder private IP-Adresse für das Frontend, wie in Abbildung 1 dargestellt. Die Vorlage erstellt zwei Knoten mit drei Subnetzen und sechs NICs. Die Subnetze dienen der Verwaltung, des Clients und des serverseitigen Datenverkehrs, wobei jedes Subnetz zu einer anderen Netzwerkkarte auf jedem Gerät gehört.

Abbildung 1: Citrix ADC HA-Paar für Clients in einem internen Netzwerk



Sie können diese Bereitstellung auch verwenden, wenn sich das Citrix ADC HA-Paar hinter einer Firewall befindet, wie in Abbildung 2 dargestellt. Die öffentliche IP-Adresse gehört zur Firewall und ist mit NAT der Front-End-IP-Adresse der ILB verbunden.

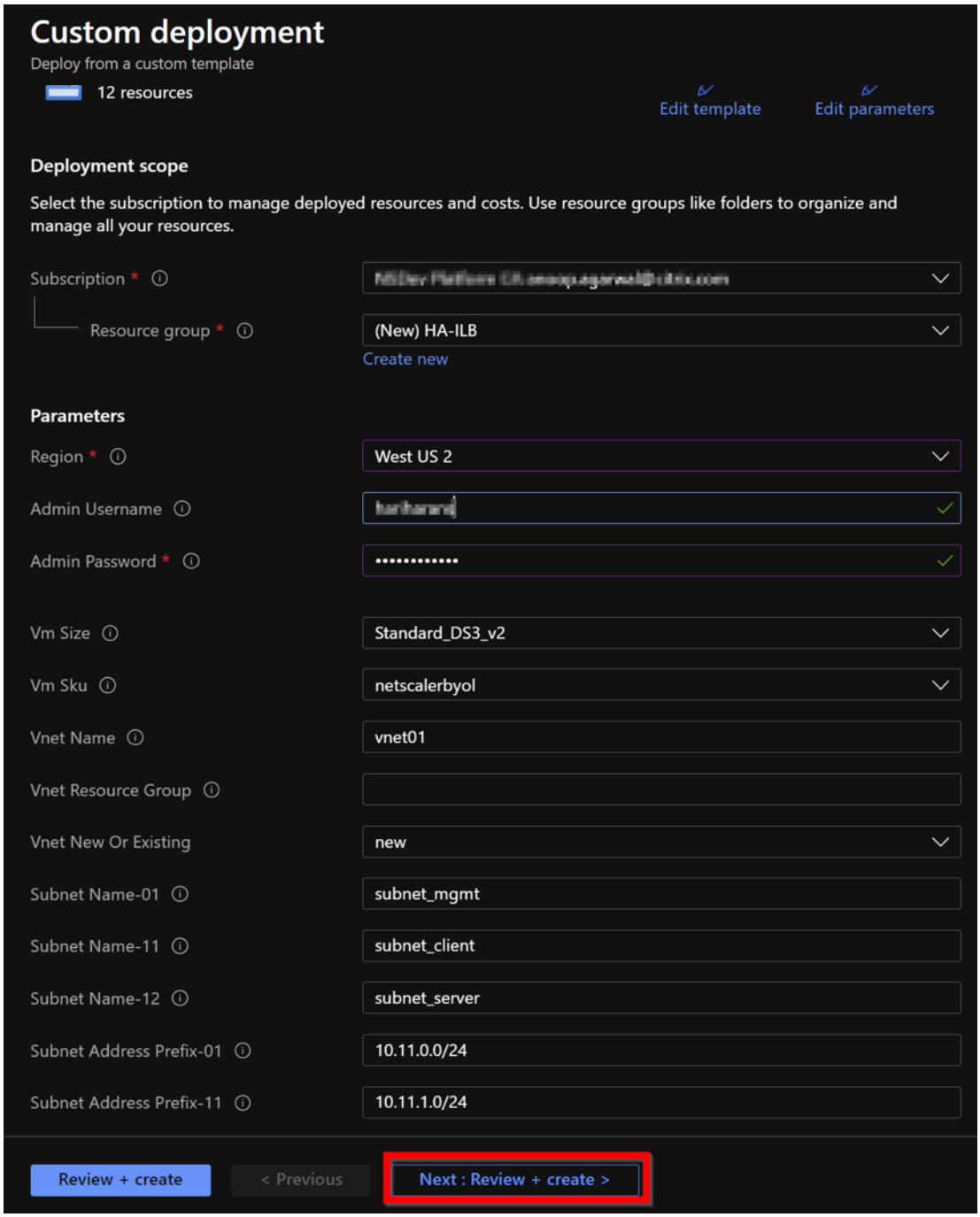
Abbildung 2: Citrix ADC HA-Paar mit Firewall mit öffentlicher IP-Adresse



Sie können die Citrix ADC HA-Paar-Vorlage für Intranetanwendungen im Azure-Portalabrufen.

Führen Sie die folgenden Schritte aus, um die Vorlage zu starten und ein Hochverfügbarkeits-VPX-Paar mithilfe von Azure Availability Sets bereitzustellen.

1. Navigieren Sie im Azure-Portal zur Seite **Benutzerdefinierte Bereitstellung** .
2. Die Seite **Grundlagen** wird angezeigt. Erstellen Sie eine Ressourcengruppe. Geben Sie auf der Registerkarte **Parameter** Details für die Region, den Admin-Benutzernamen, das Admin-Kennwort, den Lizenztyp (`VM sku`) und andere Felder ein.

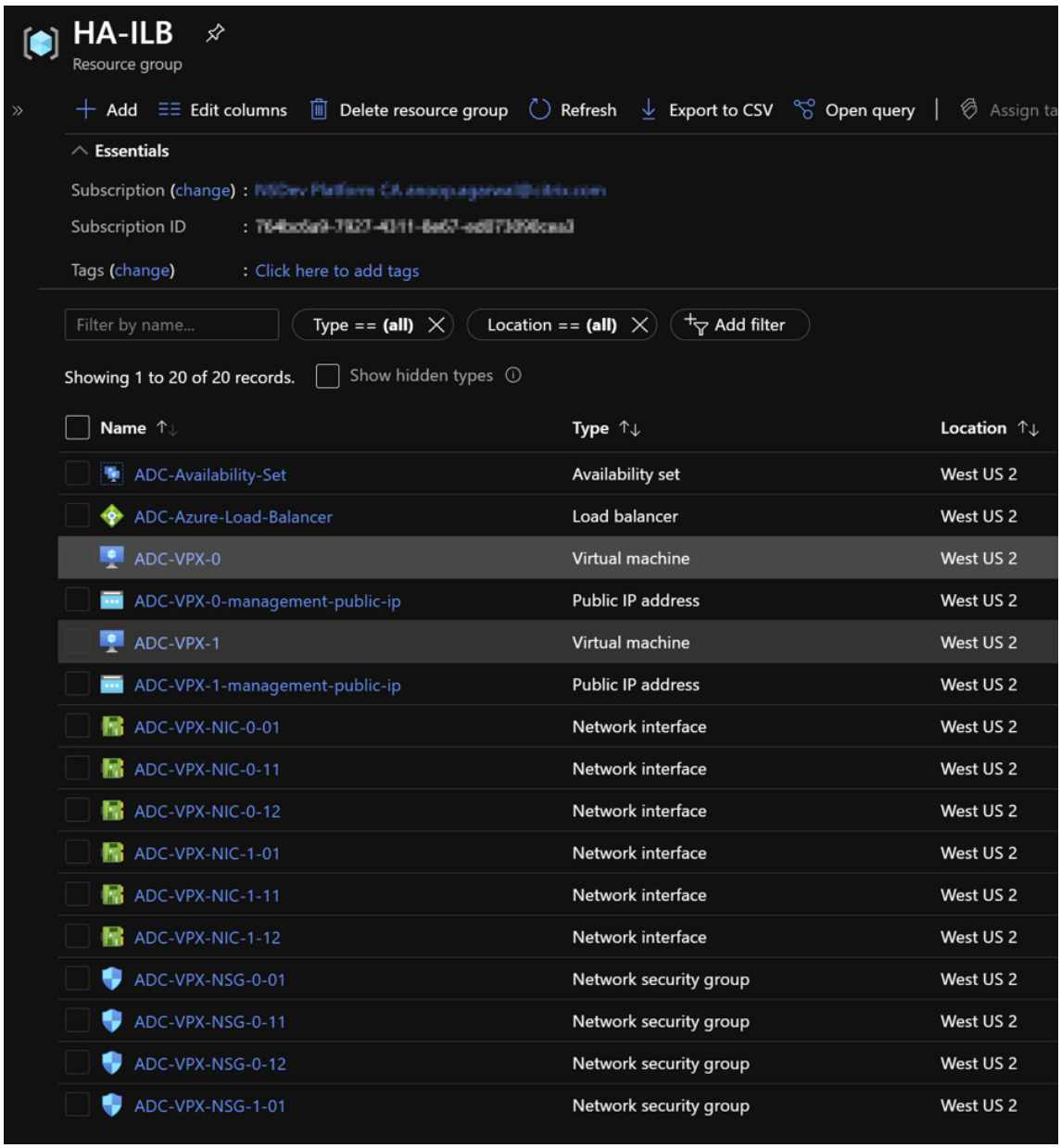


3. Klicken Sie auf **Weiter: Überprüfen + erstellen**.

Es kann einen Moment dauern, bis die Azure Resource Group mit den erforderlichen Konfigurationen erstellt wurde. Wählen Sie nach Abschluss die Ressourcengruppe im Azure-Portal aus, um die Konfigurationsdetails wie LB-Regeln, Back-End-Pools und Integritäts-Sonden anzuzeigen. Das Hochverfügbarkeitspaar erscheint als ADC-VPX-0 und ADC-VPX-1.

Wenn weitere Änderungen für das HA-Setup erforderlich sind, z. B. das Erstellen weiterer Sicherheitsregeln und Ports, können Sie dies über das Azure-Portal vornehmen.

Sobald die erforderliche Konfiguration abgeschlossen ist, werden die folgenden Ressourcen erstellt.

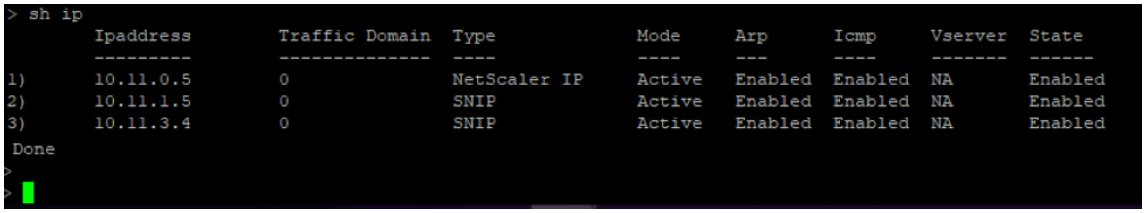


4. Sie müssen sich bei **ADC-VPX-0** und **ADC-VPX-1-Knoten** anmelden, um die folgende Konfiguration zu überprüfen:

- NSIP-Adressen für beide Knoten müssen sich im Management-Subnetz befinden.
- Auf den primären (ADC-VPX-0) und sekundären (ADC-VPX-1) Knoten müssen Sie zwei SNIP-Adressen sehen. Ein SNIP (Client-Subnetz) wird für die Reaktion auf ILB-Prüfpunkte verwendet und das andere SNIP (Serversubnetz) wird für die Back-End-Server-Kommunikation verwendet.

> Hinweis
>
> Im HA-INC-Modus unterscheiden sich die SNIP-Adresse der ADC-VPX-0- und ADC-VPX-1-VMs im selben Subnetz, im Gegensatz zu der klassischen lokalen ADC HA-Bereitstellung, bei der beide gleich sind.
> Um Bereitstellungen zu unterstützen, wenn sich das VPX-Paar SNIP in verschiedenen Subnetzen befindet oder wenn sich der VIP nicht im selben Subnetz wie ein SNIP befindet, müssen Sie entweder Mac-Based Forwarding (MBF) aktivieren oder jedem VPX-Knoten eine statische Host-Route für jeden VIP hinzufügen.

Auf dem primären Knoten (ADC-VPX-0)




```
> sh ha node
1)      Node ID:      0
        IP:       10.11.0.5 (ADC-VPX-0)
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:0:20:26 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.11.0.4
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

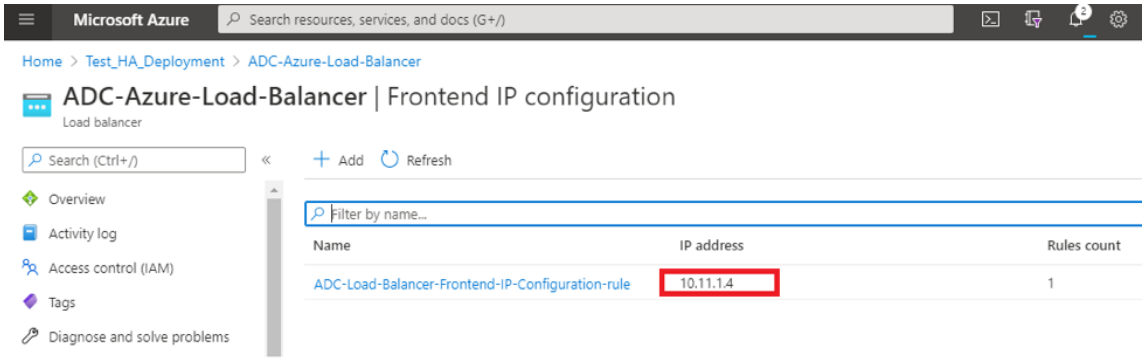
Auf dem sekundären Knoten (ADC-VPX-1)

```
> sh ip
       Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
       ---------        --------------  ----            ----     ---      ----     -------  ------
1)     10.11.0.4        0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)     10.11.1.6        0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)     10.11.3.5        0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
>
>
```

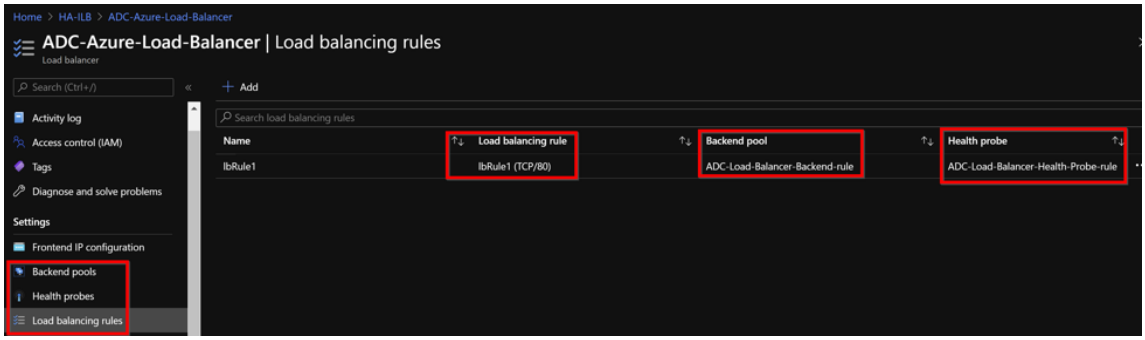


```
> sh ha node
1)      Node ID:      0
        IP:       10.11.0.4 (ADC-VPX-1)
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:0:24:18 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.11.0.5
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

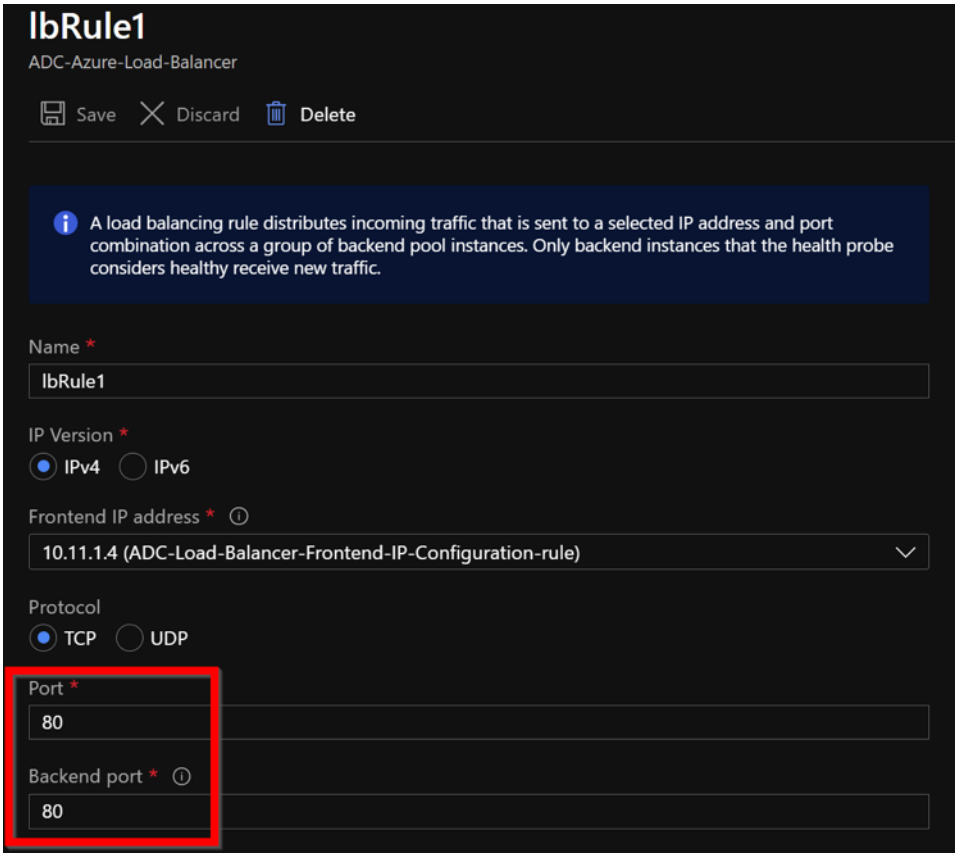
5. Nachdem die primären und sekundären Knoten aktiv sind und der Synchronisierungsstatus **ERFOLGREICH**ist, müssen Sie den virtuellen Lastausgleichsserver oder den virtuellen Gateway-Server auf dem Primärknoten (ADC-VPX-0) mit der privaten Floating IP (FIP) -Adresse des ADC Azure Load Balancers konfigurieren. Weitere Informationen finden Sie im Abschnitt Beispielkonfiguration .
6. Um die private IP-Adresse des ADC Azure Load Balancers zu finden, navigieren Sie zum **Azure-Portal > ADC Azure Load Balancer > Frontend IP-Konfiguration**.



7. Auf der **Azure Load Balancer-Konfigurationsseite** hilft die ARM-Vorlagenbereitstellung beim Erstellen der LB-Regel, Back-End-Pools und Gesundheitsproben.

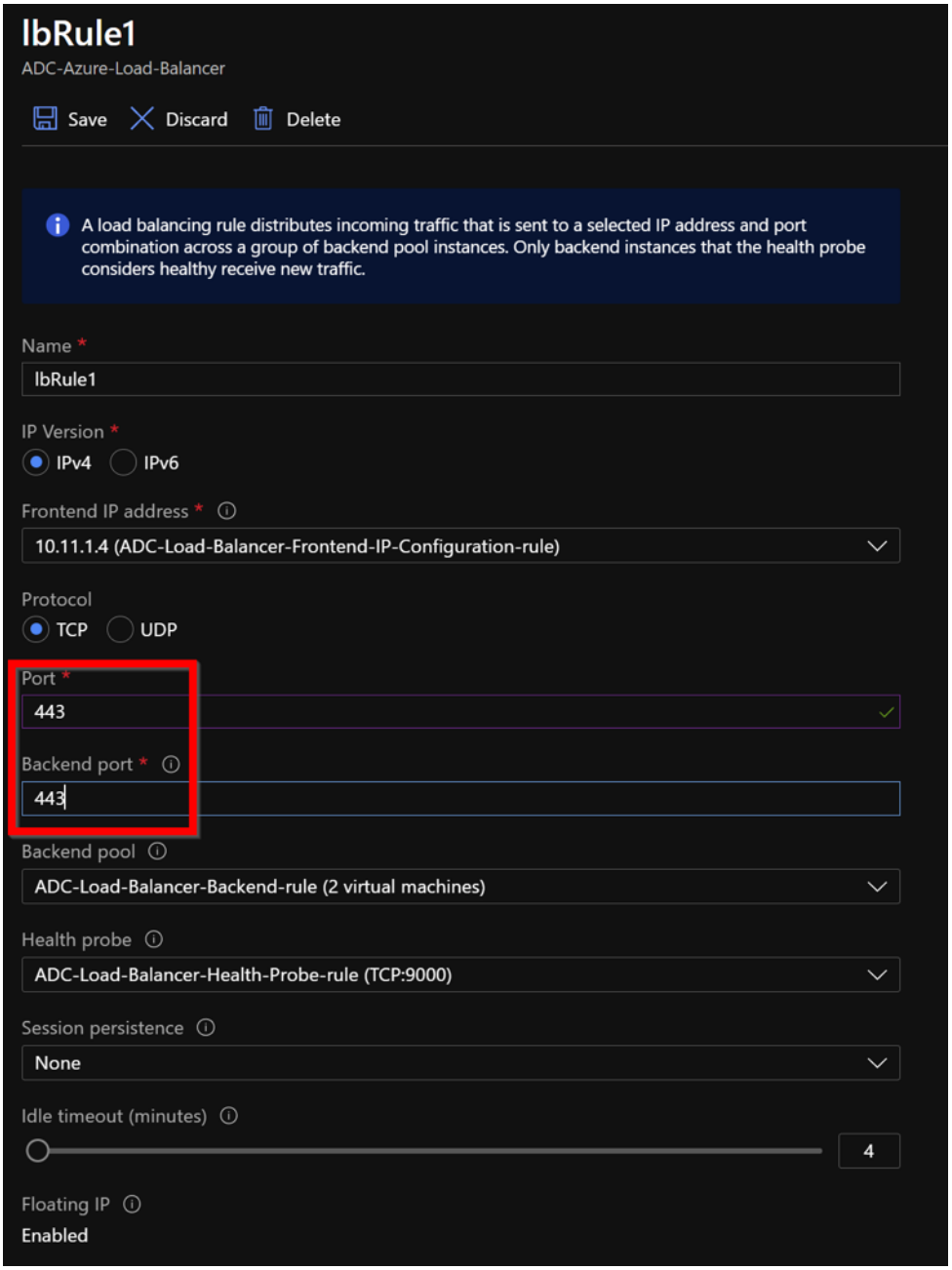


   - Die LB-Regel (LBrule1) verwendet standardmäßig Port 80.



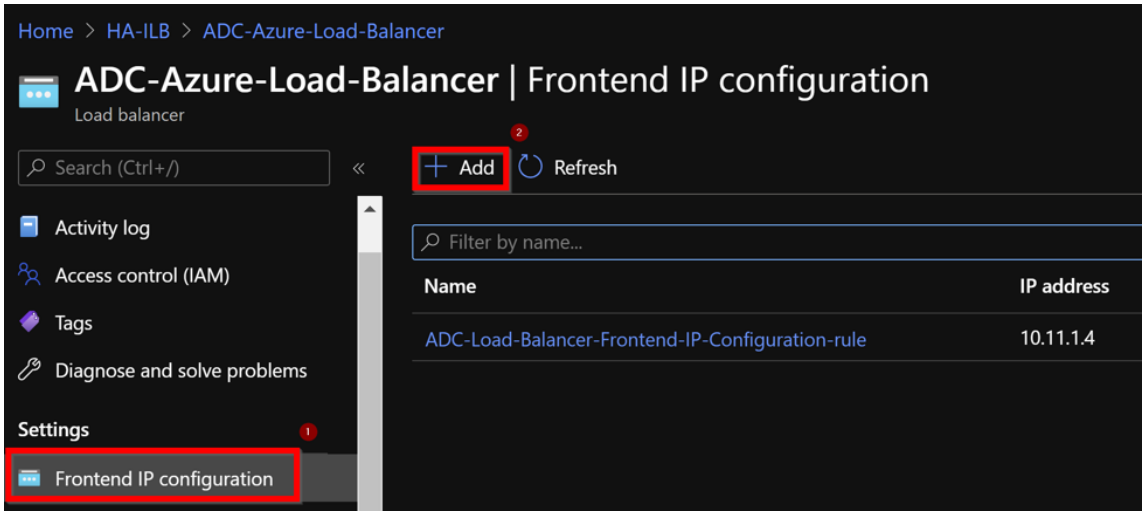
- Bearbeiten Sie die Regel, um Port 443 zu verwenden, und speichern Sie die Änderungen.

> Hinweis
>
> Für eine verbesserte Sicherheit empfiehlt Citrix, den SSL-Port 443 für den virtuellen LB-Server oder den virtuellen Gateway-Server zu verwenden.

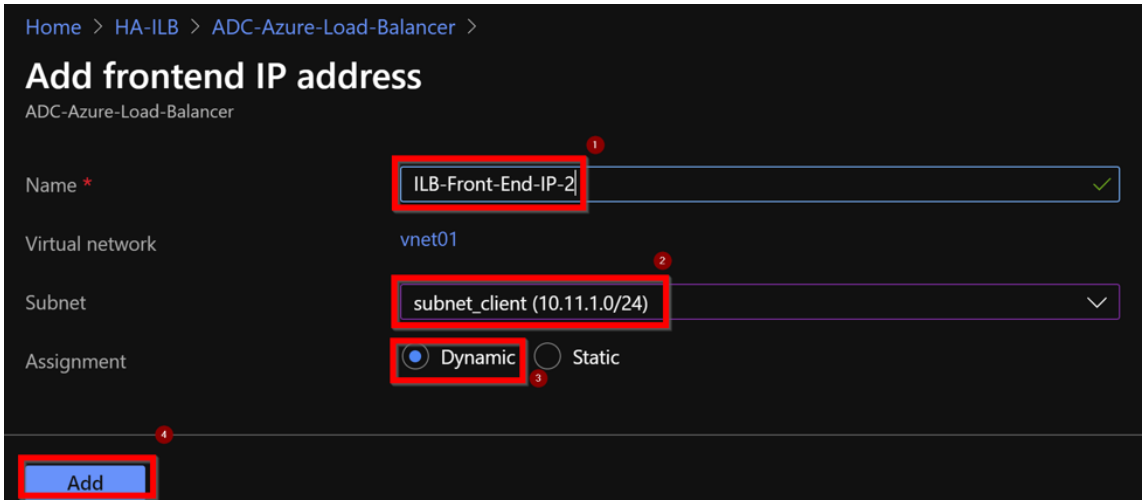


Gehen Sie wie folgt vor, um weitere VIP-Adressen zum ADC hinzuzufügen:

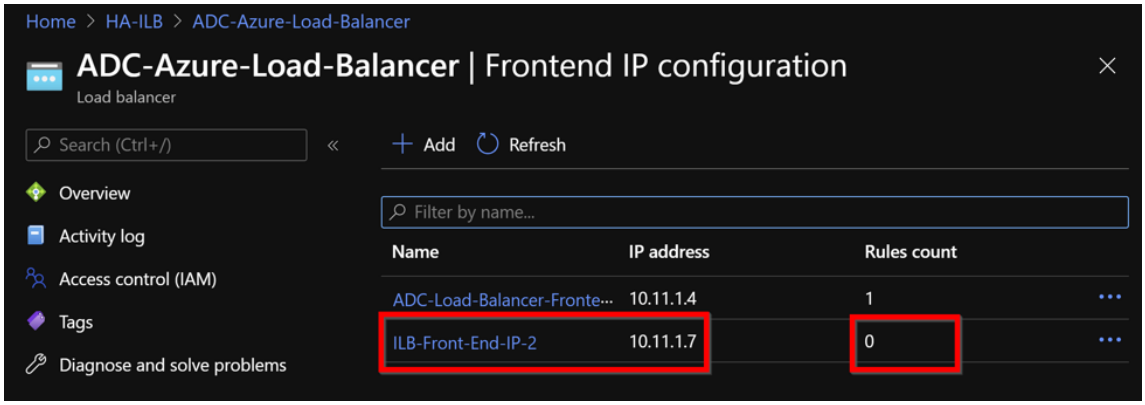
1. Navigieren Sie zu **Azure Load Balancer > Frontend-IP-Konfiguration**, und klicken Sie auf **Hinzufügen**, um eine neue interne Load Balancer-IP-Adresse zu erstellen.



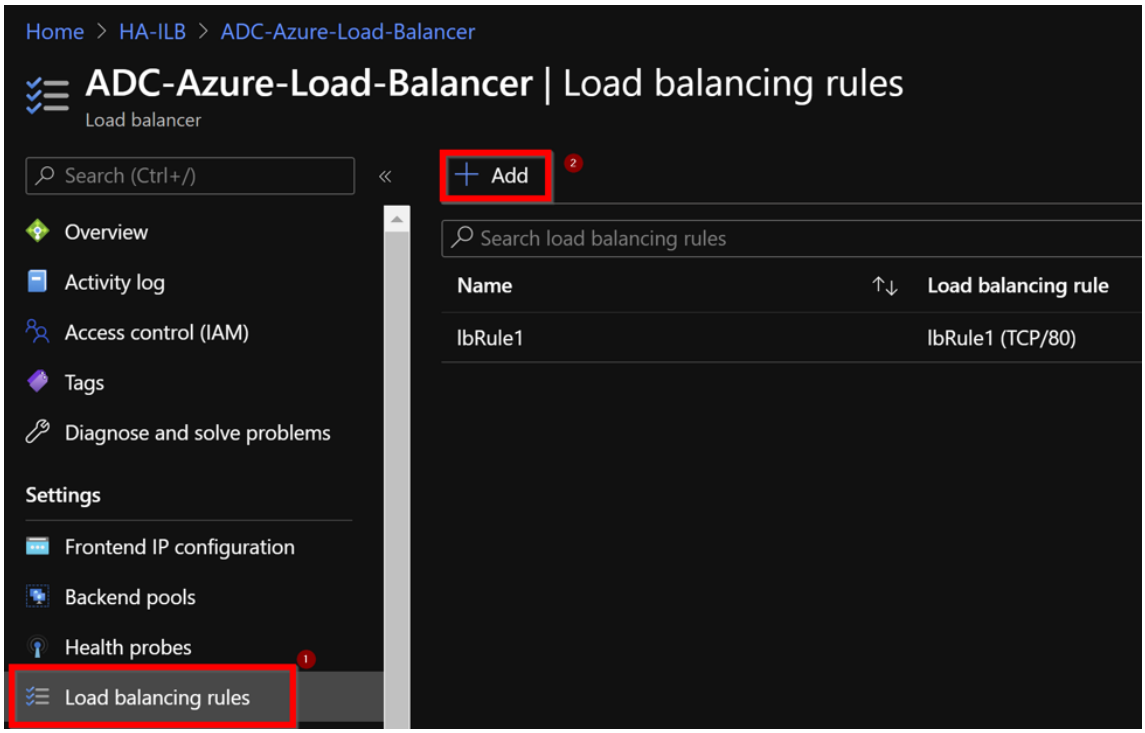
2. Geben Sie auf der Seite **Frontend-IP-Adresse hinzufügen** einen Namen ein, wählen Sie das Client-Subnetz aus, weisen Sie entweder dynamische oder statische IP-Adresse zu und klicken Sie auf **Hinzufügen**.



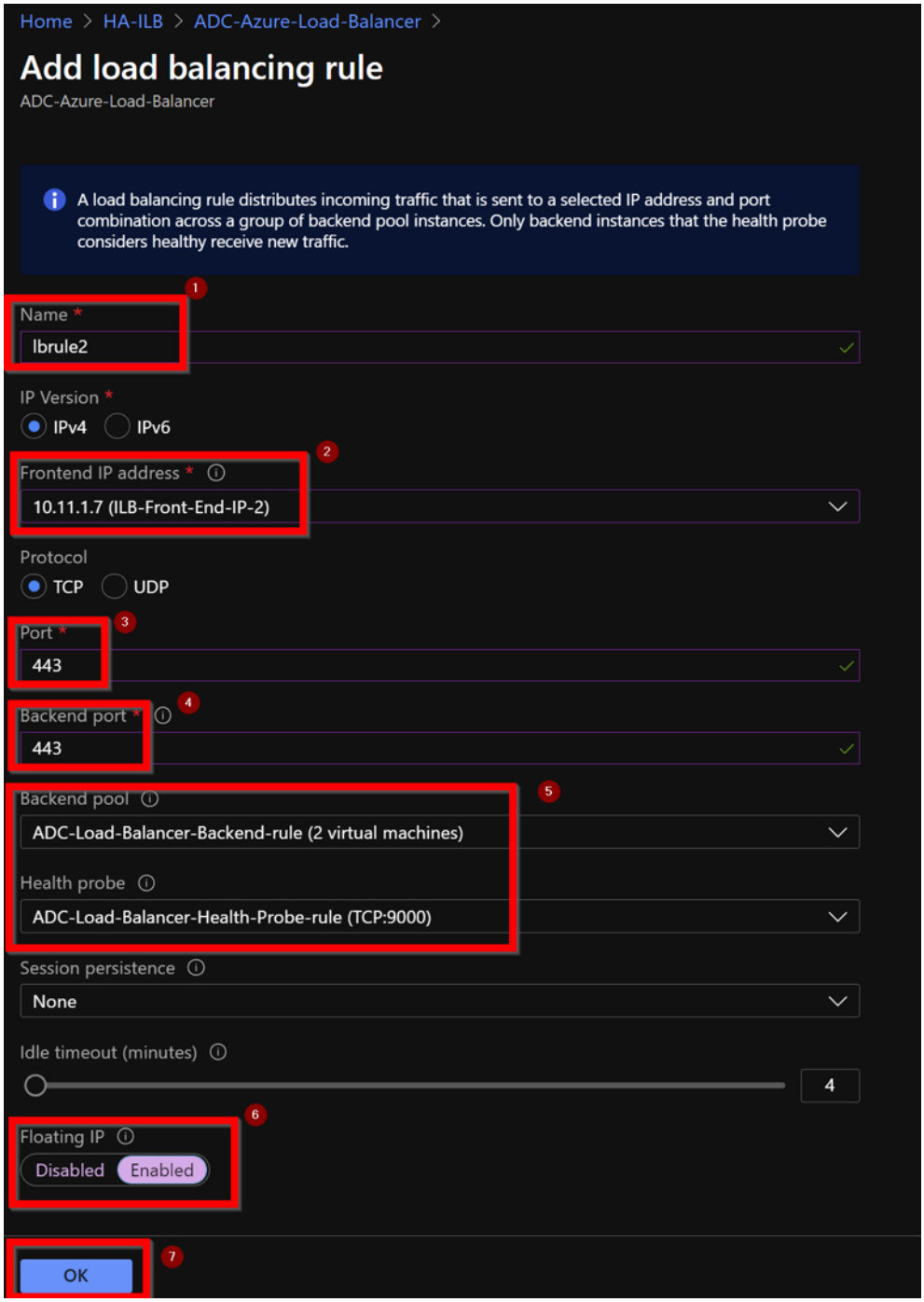
3. Die Front-End-IP-Adresse wird erstellt, aber eine LB-Regel ist nicht zugeordnet. Erstellen Sie eine neue Lastausgleichsregel, und verknüpfen Sie sie mit der Front-End-IP-Adresse.



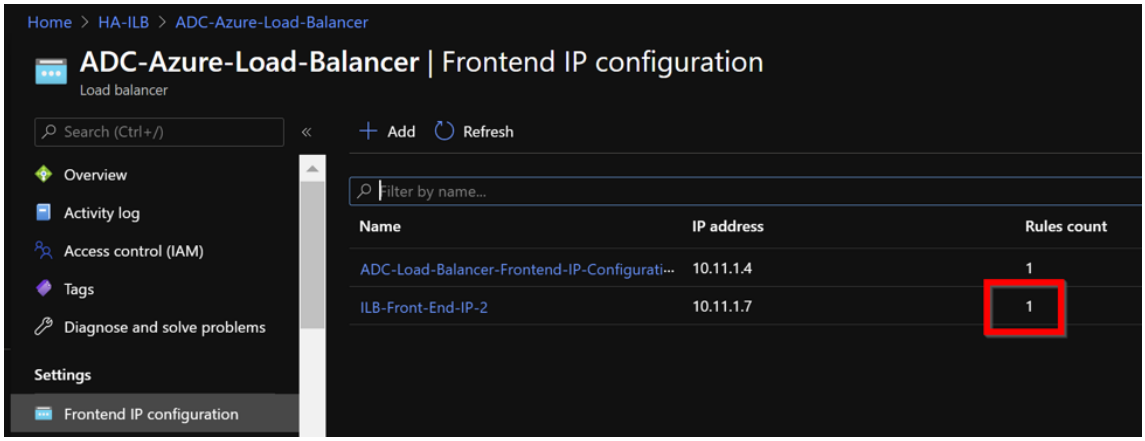
4. Wählen Sie auf der Seite **Azure Load Balancer** die Option **Load Balancing-Regeln**aus, und klicken Sie dann auf **Hinzufügen**.



5. Erstellen Sie eine neue LB-Regel, indem Sie die neue Front-End-IP-Adresse und den Port auswählen. Das**Floating-IP-Feld** muss auf **Enabled**gesetzt sein.



6. Jetzt zeigt die **Frontend-IP-Konfiguration** die angewendete LB-Regel an.



Beispiel-Konfiguration

Führen Sie zum Konfigurieren eines virtuellen Gateway-VPN-Servers und eines virtuellen Lastausgleichsservers die folgenden Befehle auf dem primären Knoten aus (ADC-VPX-0). Die Konfiguration synchronisiert sich automatisch mit dem sekundären Knoten (ADC-VPX-1).

Gateway Beispielkonfiguration

```
enable feature aaa LB SSL SSLVPN
enable ns mode MBF
add vpn vserver vpn_ssl SSL 10.11.1.4 443
add ssl certKey ckp -cert wild-cgwsanity.cer -key wild-cgwsanity.key
bind ssl vserver vpn_ssl -certkeyName ckp
<!--NeedCopy-->
```

Beispielkonfiguration für den Lastausgleich

```
enable feature LB SSL
enable ns mode MBF
add lb vserver lb_vs1 SSL 10.11.1.7 443
bind ssl vserver lb_vs1 -certkeyName ckp
<!--NeedCopy-->
```

Sie können jetzt mit dem vollqualifizierten Domänennamen (FQDN), der mit der internen IP-Adresse von ILB verknüpft ist, auf den Lastausgleich- oder virtuellen VPN-Server zugreifen.

Weitere Informationen zum Konfigurieren des virtuellen Lastausgleichsservers finden Sie im Abschnitt **Ressourcen** .

Ressourcen:

Die folgenden Links bieten zusätzliche Informationen zur HA-Bereitstellung und Konfiguration virtueller Server:

- Konfigurieren von Knoten mit hoher Verfügbarkeit in verschiedenen Subnetzen
- Richten Sie den grundlegenden Lastenausgleich ein

Verwandte Ressourcen:

- Konfigurieren eines Hochverfügbarkeits-Setups mit mehreren IP-Adressen und NICs mithilfe von PowerShell-Befehlen
- Konfigurieren von GSLB in der aktiven Standby-HA-Bereitstellung in Azure

Konfigurieren von HA-INC-Knoten mit der Citrix Hochverfügbarkeitsvorlage für internetorientierte Anwendungen

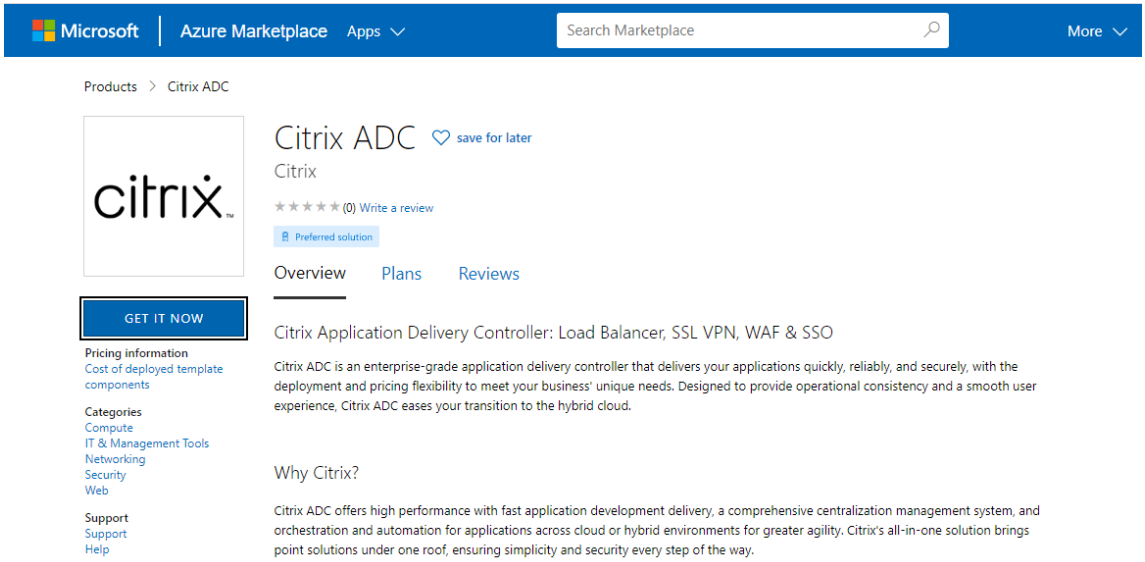
December 3, 2021

Sie können schnell und effizient ein Paar VPX-Instanzen im HA-INC-Modus bereitstellen, indem Sie die Standardvorlage für Internetanwendungen verwenden. Der Azure Load Balancer (ALB) verwendet eine öffentliche IP-Adresse für das Frontend. Die Vorlage erstellt zwei Knoten mit drei Subnetzen und sechs Netzwerkkarten. Die Subnetze sind für Verwaltungs-, Client- und serverseitigen Datenverkehr vorgesehen. Jedes Subnetz hat zwei Netzwerkkarten für beide VPX-Instanzen.

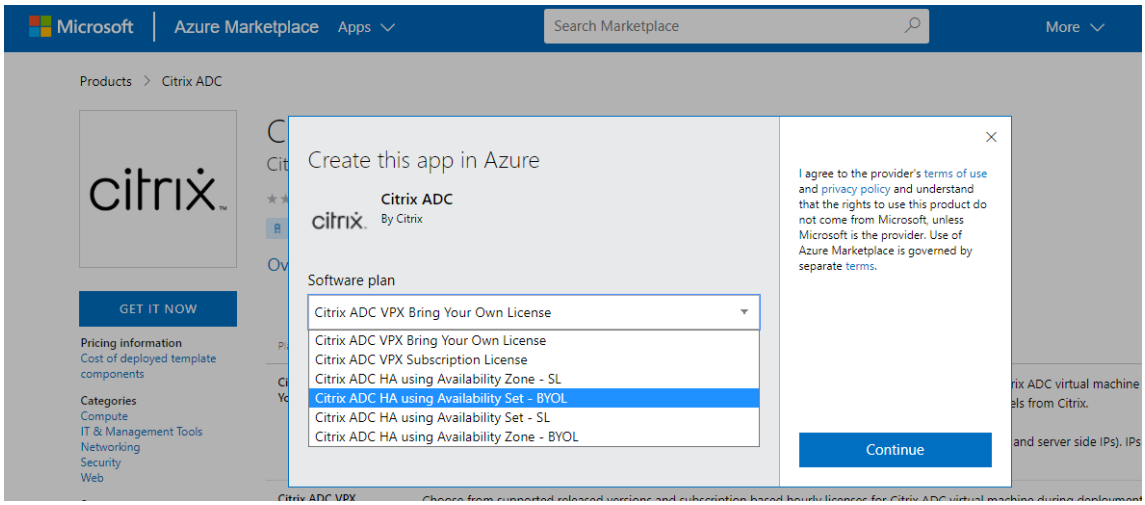
Sie können die Citrix ADC HA-Paar-Vorlage für internetorientierte Anwendungen im Azure Marketplaceabrufen.

Führen Sie die folgenden Schritte aus, um die Vorlage zu starten und ein Hochverfügbarkeits-VPX-Paar mithilfe von Azure Availability Sets oder Availability Zone bereitzustellen.

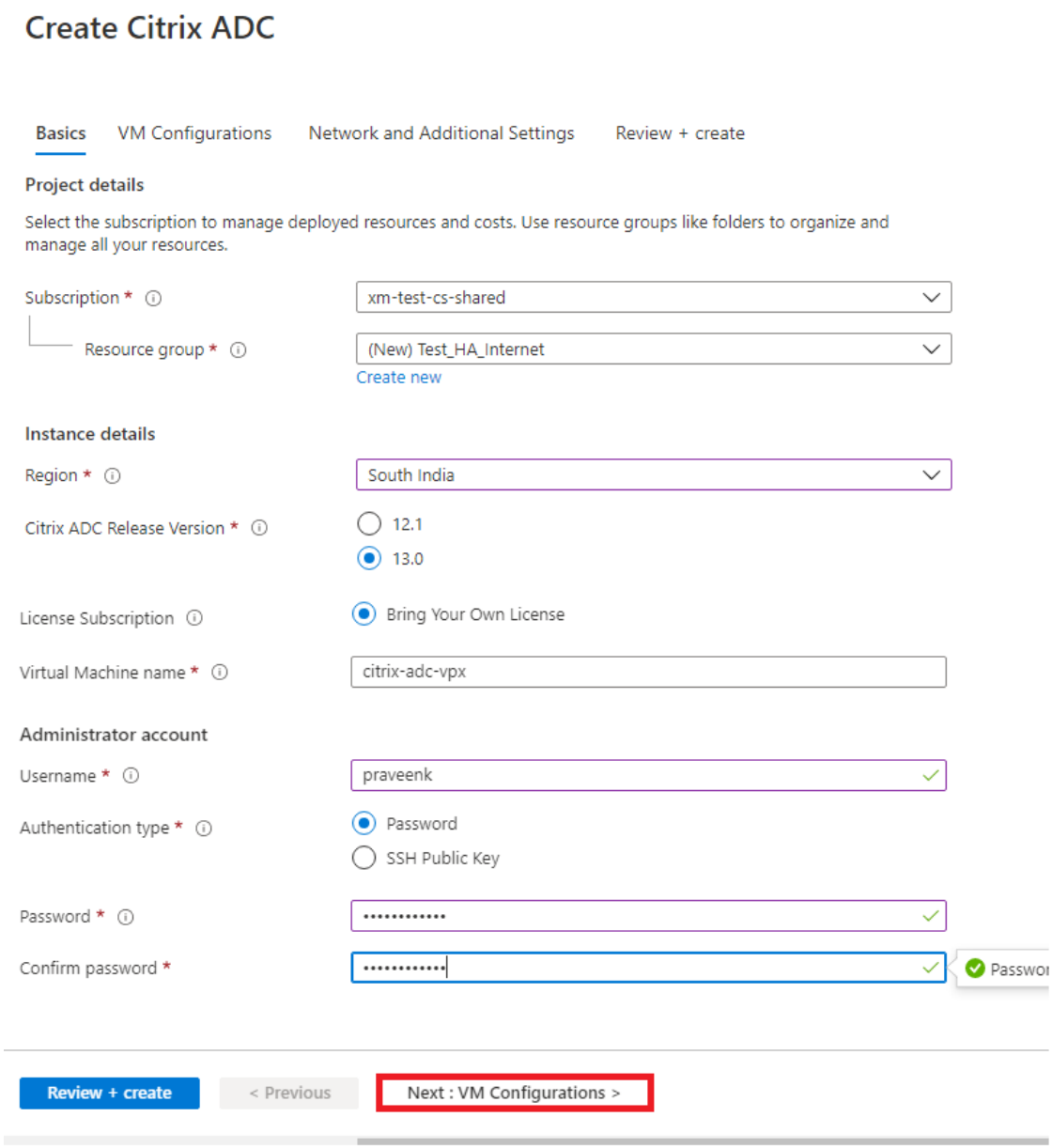
1. Suchen Sie im Azure Marketplace nach **Citrix ADC**.
2. Klicken Sie auf **JETZT HOLEN**.



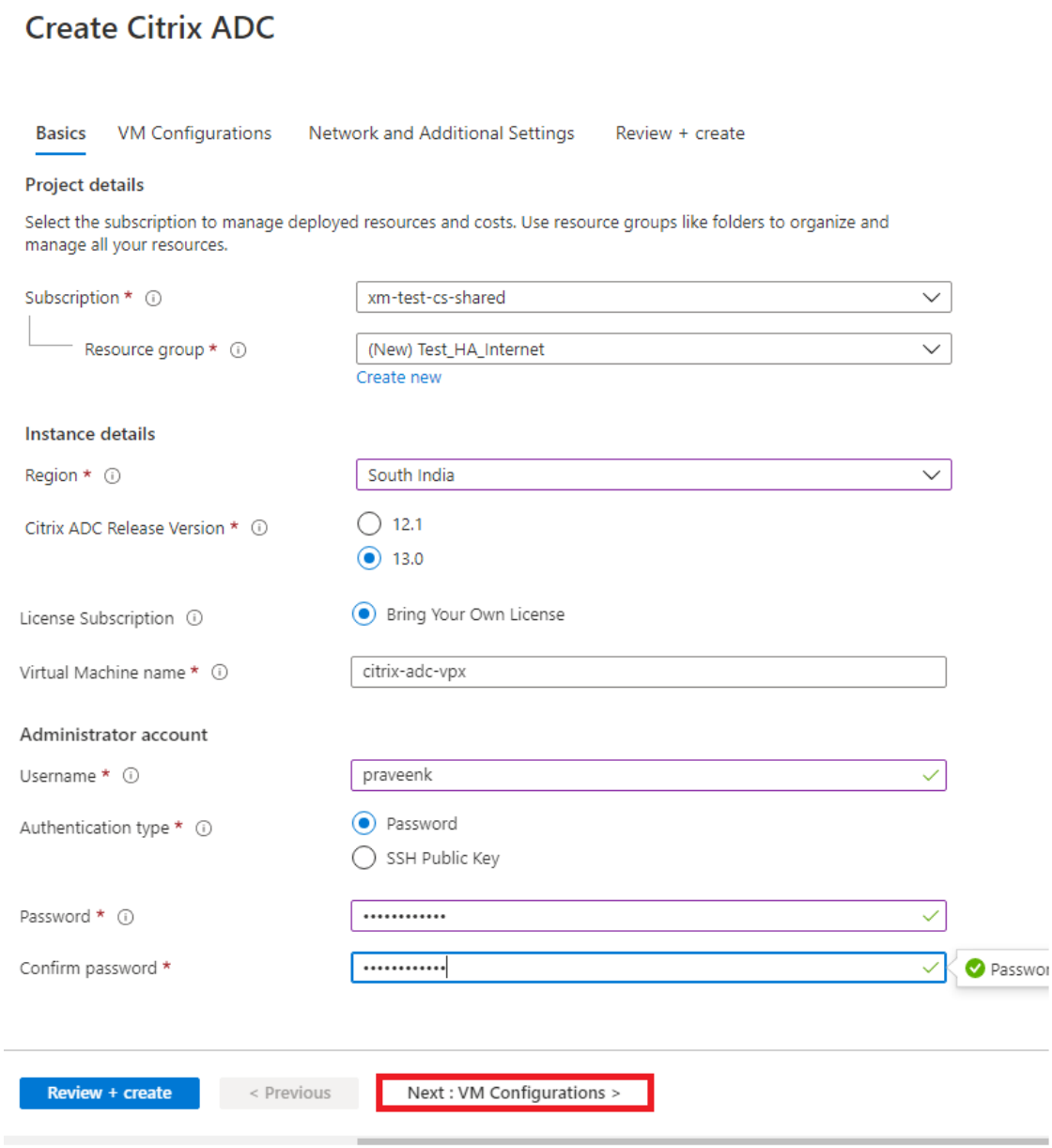
3. Wählen Sie die erforderliche HA-Bereitstellung zusammen mit der Lizenz aus und klicken Sie auf **Weiter**.



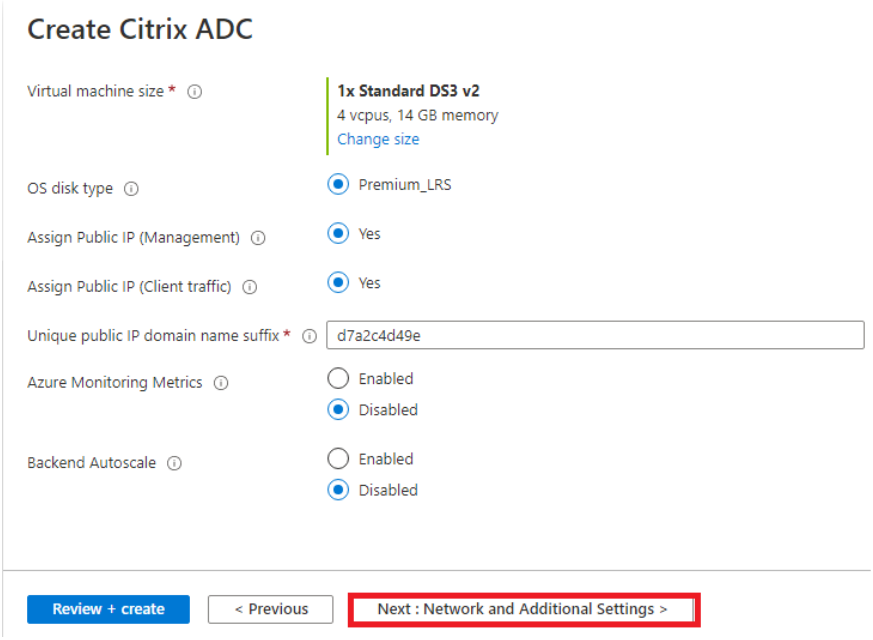
4. Die Seite **Grundlagen** wird angezeigt. Erstellen Sie eine Ressourcengruppe. Geben Sie auf der Registerkarte **Parameter** Details für die Felder Region, Admin-Benutzername, Admin-Kennwort, Lizenztyp (VM SKU) und andere ein.



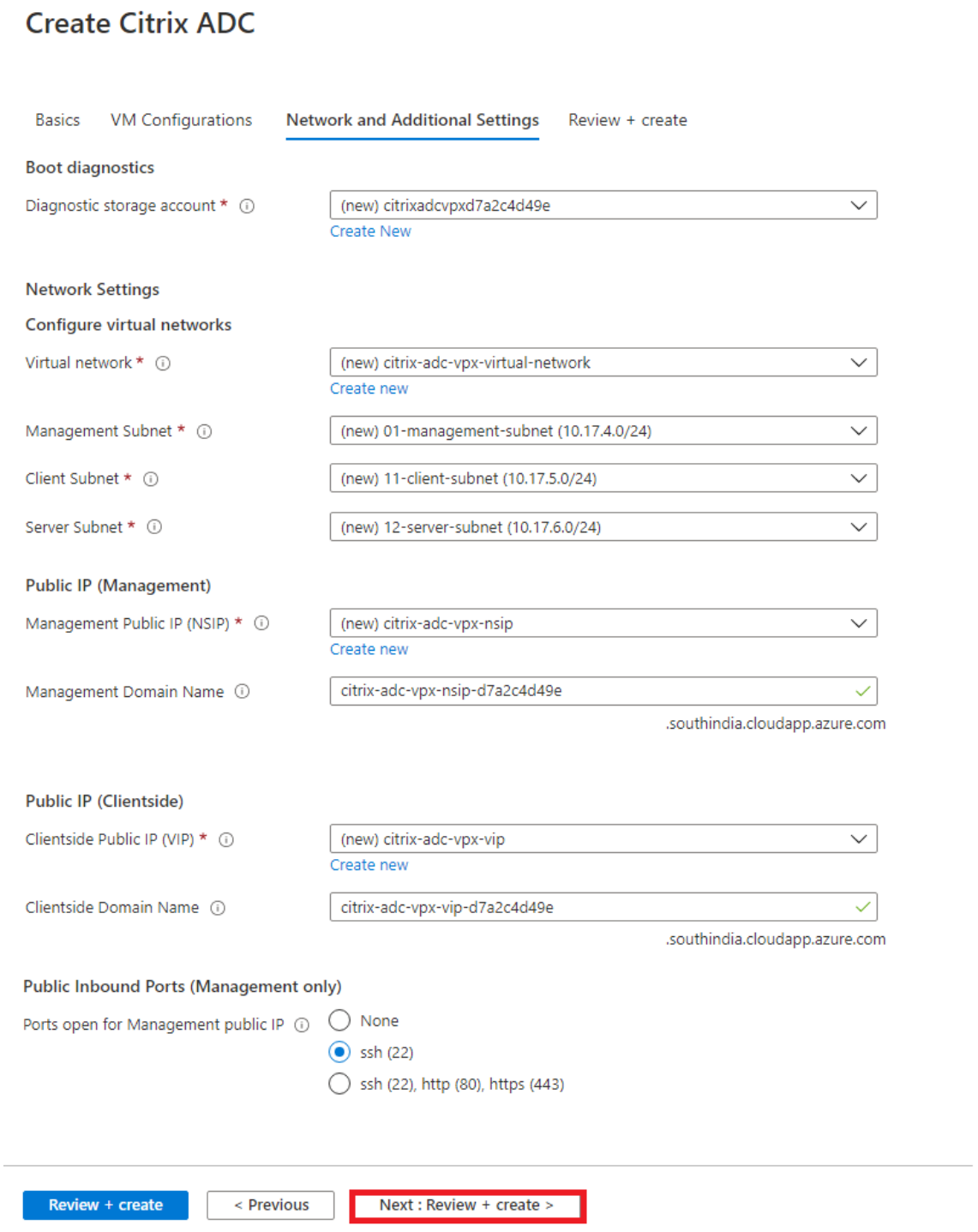
5. Klicken Sie auf **Weiter: VM-Konfigurationen**.



6. Führen Sie auf der Seite **VM-Konfigurationen** die folgenden Schritte aus:
   - Suffix für öffentliche IP-Domain konfigurieren
   - Aktivieren oder Deaktivieren von **Azure Monitoring-Metriken**
   - Aktivieren oder Deaktivieren von **Backend Autoscale**
7. Klicken Sie auf **Weiter: Netzwerk- und Zusatzeinstellungen**



8. Erstellen Sie auf der Seite **Netzwerk- und Zusatzeinstellungen** ein Boot Diagnostics-Konto und konfigurieren Sie die Netzwerkeinstellungen.

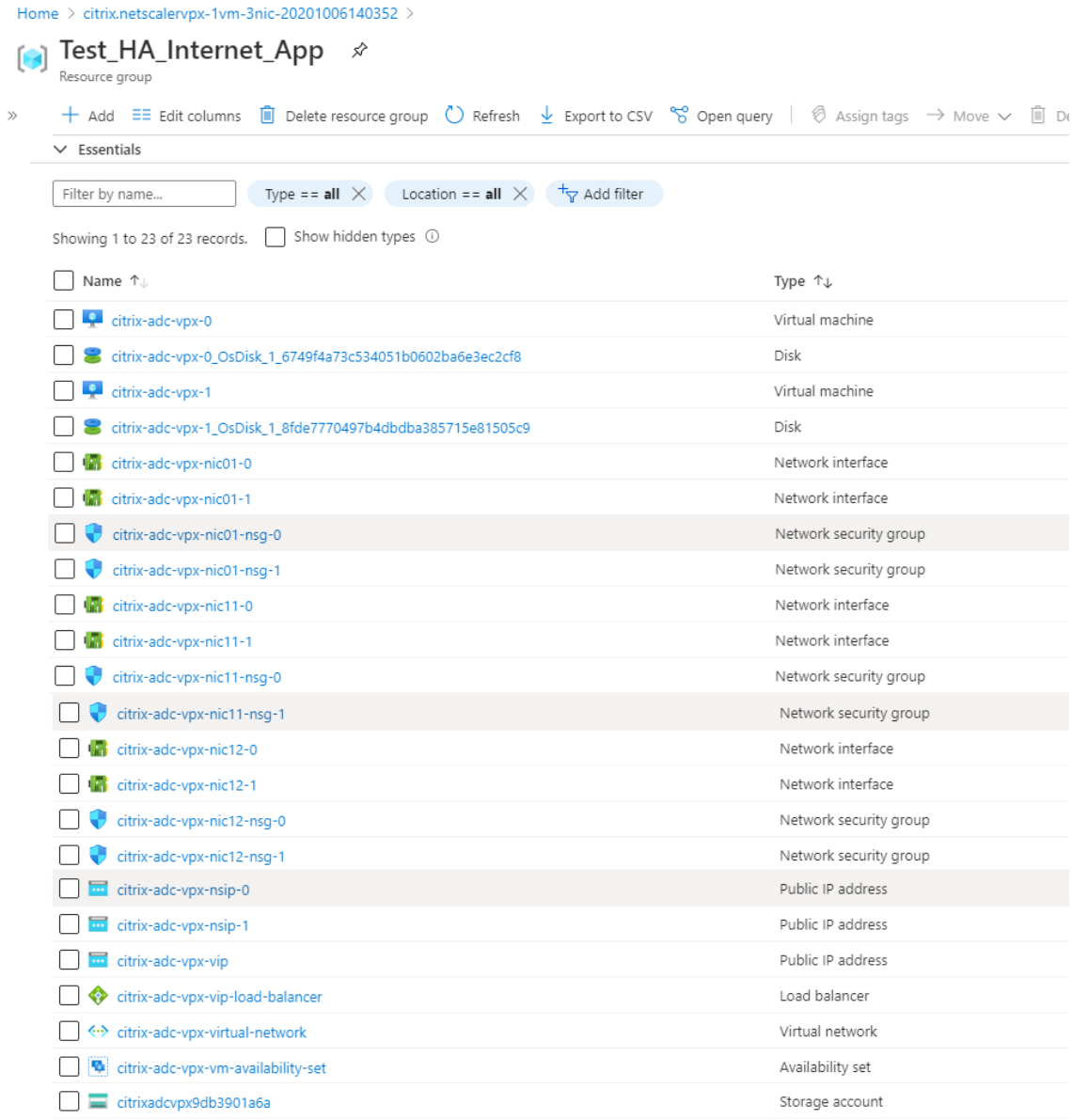


9. Klicken Sie auf **Weiter: Überprüfen + erstellen**.
10. Überprüfen Sie die Grundeinstellungen, die VM-Konfiguration, das Netzwerk und die zusätzlichen Einstellungen und klicken Sie auf **Erstellen**.

Es kann einen Moment dauern, bis die Azure-Ressourcengruppe mit den erforderlichen Konfigurationen erstellt wird. Wählen Sie nach Abschluss die Ressourcengruppe im Azure-Portal aus, um die Konfigurationsdetails wie LB-Regeln, Back-End-Pools und Health Probes anzuzeigen. Das Hochverfügbarkeitspaar erscheint als **Citrix-adc-vpx-0** und **citrix-adc-vpx-1**.

Wenn weitere Änderungen für das HA-Setup erforderlich sind, z. B. das Erstellen weiterer Sicherheitsregeln und Ports, können Sie dies über das Azure-Portal vornehmen.

Sobald die erforderliche Konfiguration abgeschlossen ist, werden die folgenden Ressourcen erstellt.



11. Sie müssen sich bei **Citrix-adc-vpx-0-** und **citrix-adc-vpx-1-Knoten** anmelden, um die folgende Konfiguration zu überprüfen:

- NSIP-Adressen für beide Knoten müssen sich im Management-Subnetz befinden.
- Auf den primären (Citrix-adc-vpx-0) und sekundären (citrix-adc-vpx-1) Knoten müssen Sie zwei SNIP-Adressen sehen. Ein SNIP (Client-Subnetz) wird verwendet, um auf die ALB-Prüfpunkte zu reagieren, und das andere SNIP (Serversubnetz) wird für die Back-End-Serverkommunikation verwendet.

> Hinweis:
>
> Im HA-INC-Modus unterscheiden sich die SNIP-Adressen der VMs citrix-adc-vpx-0 und citrix-adc-vpx-1-VMs im Gegensatz zur klassischen lokalen ADC-Hochverfügbarkeitsbereitstellung, bei der beide identisch sind.

Auf dem primären Knoten (citrix-adc-vpx-0)

```
> sh ip
        Ipaddress        Traffic Domain  Type            Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----            ----     ---      ----     -------  ------
1)      10.18.0.4        0               NetScaler IP    Active   Enabled  Enabled  NA       Enabled
2)      10.18.1.5        0               SNIP            Active   Enabled  Enabled  NA       Enabled
3)      10.18.2.4        0               SNIP            Active   Enabled  Enabled  NA       Enabled
 Done
```

```
> sh ha node
1)      Node ID:      0
        IP:       10.18.0.4 (ns-vpx0)
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:3:34:21 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.18.0.5
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
```

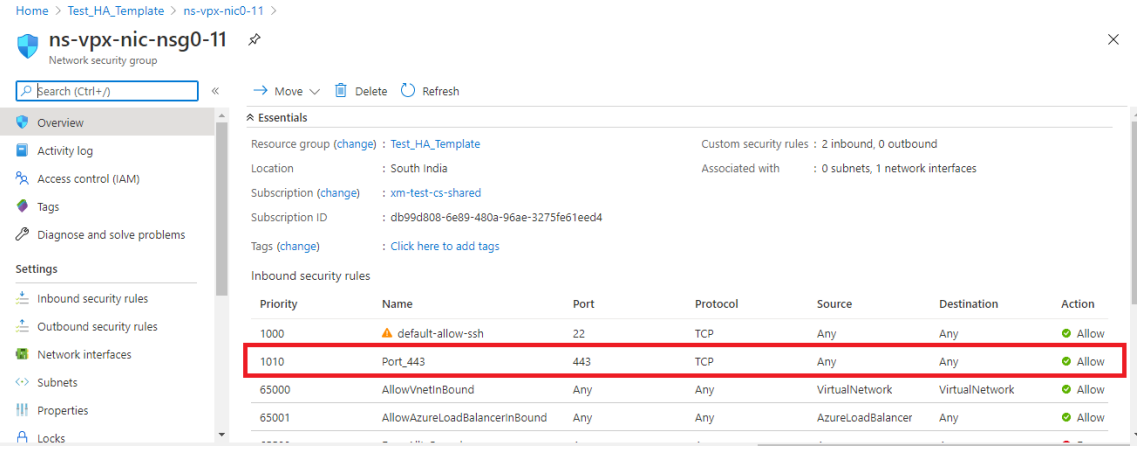
Auf dem sekundären Knoten (citrix-adc-vpx-1)

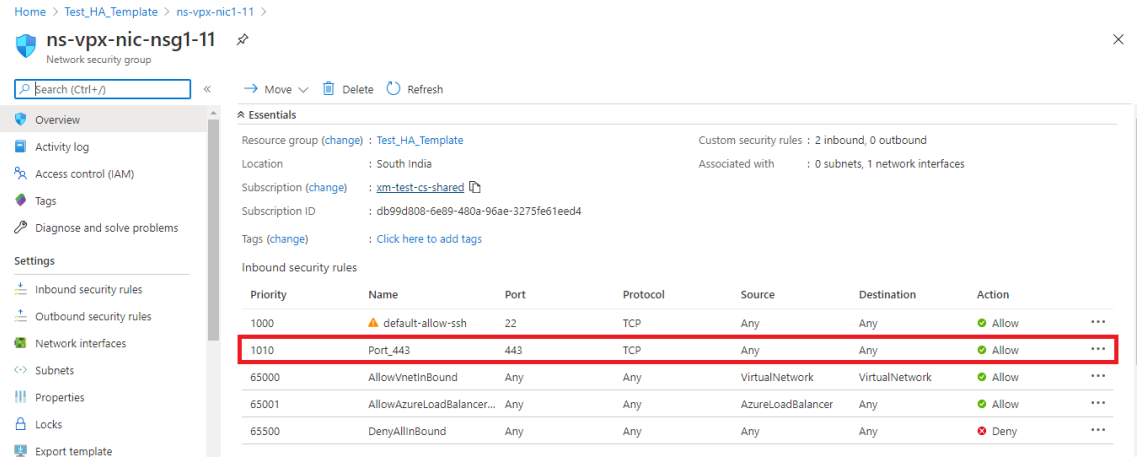

```
> show ip
        Ipaddress        Traffic Domain  Type             Mode     Arp      Icmp     Vserver  State
        ---------        --------------  ----             ----     ---      ----     -------  ------
1)      10.18.0.5        0               NetScaler IP     Active   Enabled  Enabled  NA       Enabled
2)      10.18.1.4        0               SNIP             Active   Enabled  Enabled  NA       Enabled
3)      10.18.2.5        0               SNIP             Active   Enabled  Enabled  NA       Enabled
 Done
>
```

```
> sh ha node
1)      Node ID:      0
        IP:       10.18.0.5 (ns-vpx1)
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 0:3:23:51 (days:hrs:min:sec)
2)      Node ID:      1
        IP:       10.18.0.4
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1 1/1 1/2
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : 1/1 1/2
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
>
```

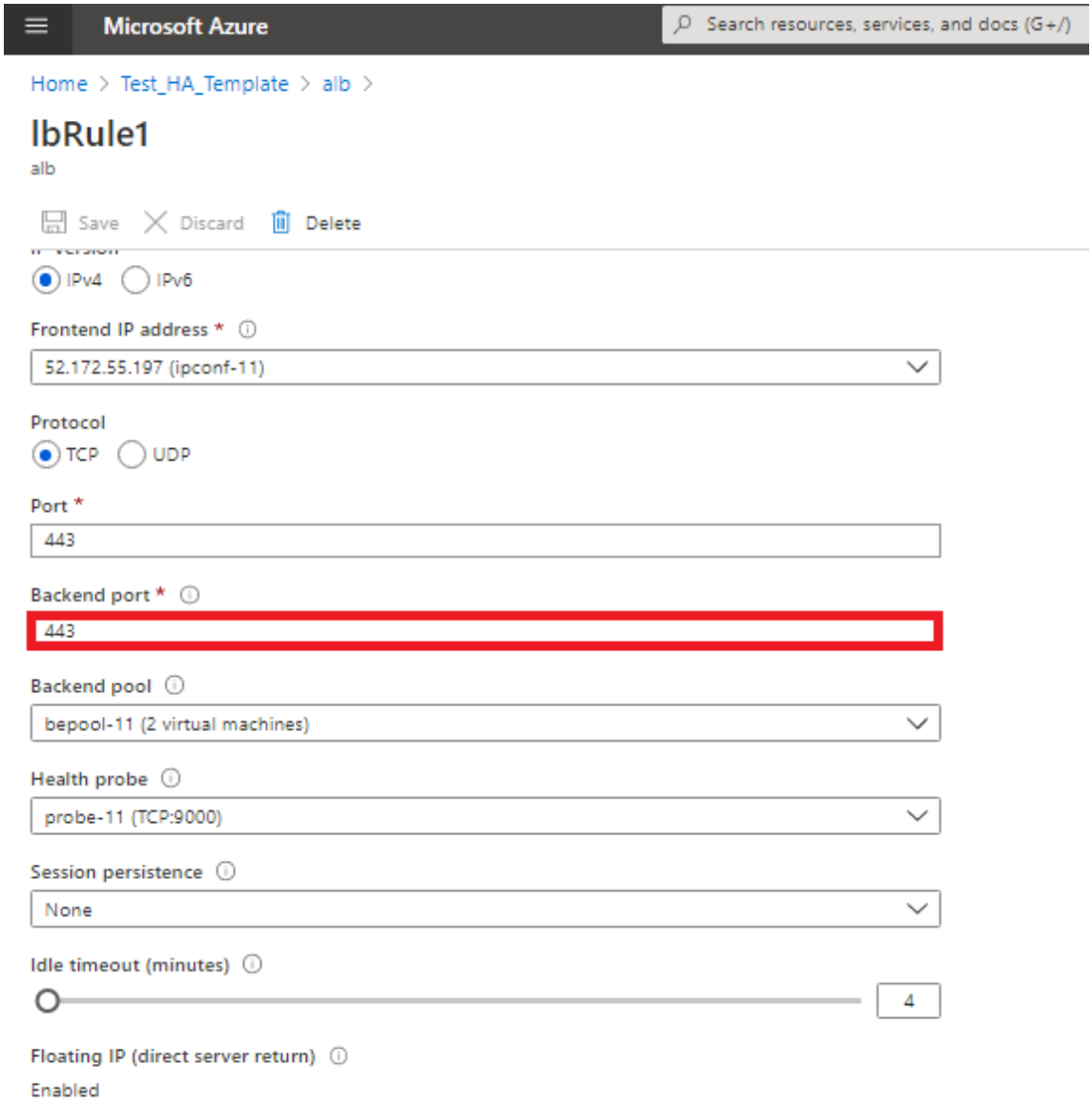
12. Nachdem der primäre und sekundäre Knoten UP sind und der Synchronisierungsstatus **ERFOLG**ist, müssen Sie den virtuellen Lastausgleichsserver oder den virtuellen Gateway-Server auf dem primären Knoten (citrix-adc-vpx-0) mit der öffentlichen IP-Adresse des virtuellen ALB-Servers konfigurieren. Weitere Informationen finden Sie im Abschnitt Beispielkonfiguration .
13. Um die öffentliche IP-Adresse des virtuellen ALB-Servers zu finden, navigieren Sie zum **Azure-Portal > Azure Load Balancer > Frontend IP-Konfiguration**.

14. Fügen Sie die eingehende Sicherheitsregel für den virtuellen Serverport 443 in der Netzwerksicherheitsgruppe beider Client-Schnittstellen hinzu.

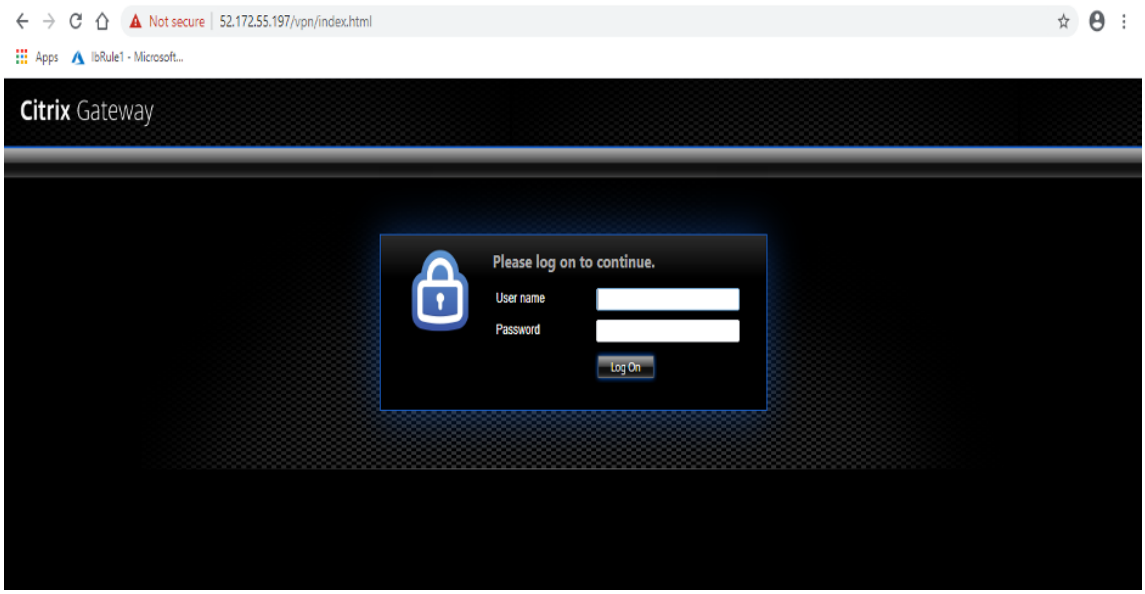




15. Konfigurieren Sie den ALB-Port, auf den Sie zugreifen möchten, und erstellen Sie eine eingehende Sicherheitsregel für den angegebenen Port. Der Backend-Port ist Ihr virtueller Serverport für den Lastenausgleich oder der virtuelle VPN-Server-Port.



16. Jetzt können Sie mit dem FQDN, der mit der öffentlichen IP-Adresse ALB verknüpft ist, auf den virtuellen Lastausgleichsserver oder den virtuellen VPN-Server zugreifen.



Beispielkonfiguration

Um einen virtuellen Gateway-VPN-Server und einen virtuellen Lastausgleichsserver zu konfigurieren, führen Sie die folgenden Befehle auf dem primären Knoten (ADC-VPX-0) aus. Die Konfiguration wird automatisch mit dem sekundären Knoten (ADC-VPX-1) synchronisiert.

Gateway-Beispiel

```
enable feature aaa LB SSL SSLVPN
add ip 52.172.55.197 255.255.255.0 -type VIP
add vpn vserver vpn_ssl SSL 52.172.55.197 443
add ssl certKey ckp -cert cgwsanity.cer -key cgwsanity.key
bind ssl vserver vpn_ssl -certkeyName ckp
<!--NeedCopy-->
```

Beispielkonfiguration für Lastenausgleich

```
enable feature LB SSL
enable ns mode MBF
add lb vserver lb_vs1 SSL 52.172.55.197 443
bind ssl vserver lb_vs1 -certkeyName ckp
<!--NeedCopy-->
```

Sie können jetzt mit dem vollqualifizierten Domänennamen (FQDN), der mit der internen IP-Adresse des ILB verknüpft ist, auf den Lastenausgleich oder virtuellen VPN-Server zugreifen.

Im Abschnitt **Ressourcen** finden Sie weitere Informationen zur Konfiguration des virtuellen Lastausgleichsservers.

Ressourcen:

Die folgenden Links enthalten zusätzliche Informationen zur HA-Bereitstellung und zur Konfiguration virtueller Server:

- Erstellen virtueller Server
- Einrichten des grundlegenden Lastenausgleichs

Konfigurieren Sie ein Hochverfügbarkeits-Setup mit externen und internen Load Balancern von Azure gleichzeitig

October 5, 2021

Das Hochverfügbarkeitspaar auf Azure unterstützt sowohl externe als auch interne Load Balancer gleichzeitig.

Sie haben die folgenden zwei Möglichkeiten, ein Hochverfügbarkeitspaar mit externen und internen Load Balancern von Azure zu konfigurieren:

- Verwenden von zwei virtuellen LB-Servern auf der Citrix ADC Appliance.
- Verwenden eines virtuellen LB-Servers und eines IP-Sets. Der einzelne virtuelle LB-Server dient Datenverkehr zu mehreren IPs, die durch das IPSet definiert sind.

Führen Sie die folgenden Schritte aus, um ein Hochverfügbarkeitspaar in Azure zu konfigurieren, wobei sowohl externe als auch interne Load Balancer gleichzeitig verwendet werden:

Verwenden Sie für die Schritte 1 und 2 das Azure-Portal. Verwenden Sie für die Schritte 3 und 4 die Citrix ADC VPX GUI oder die CLI.

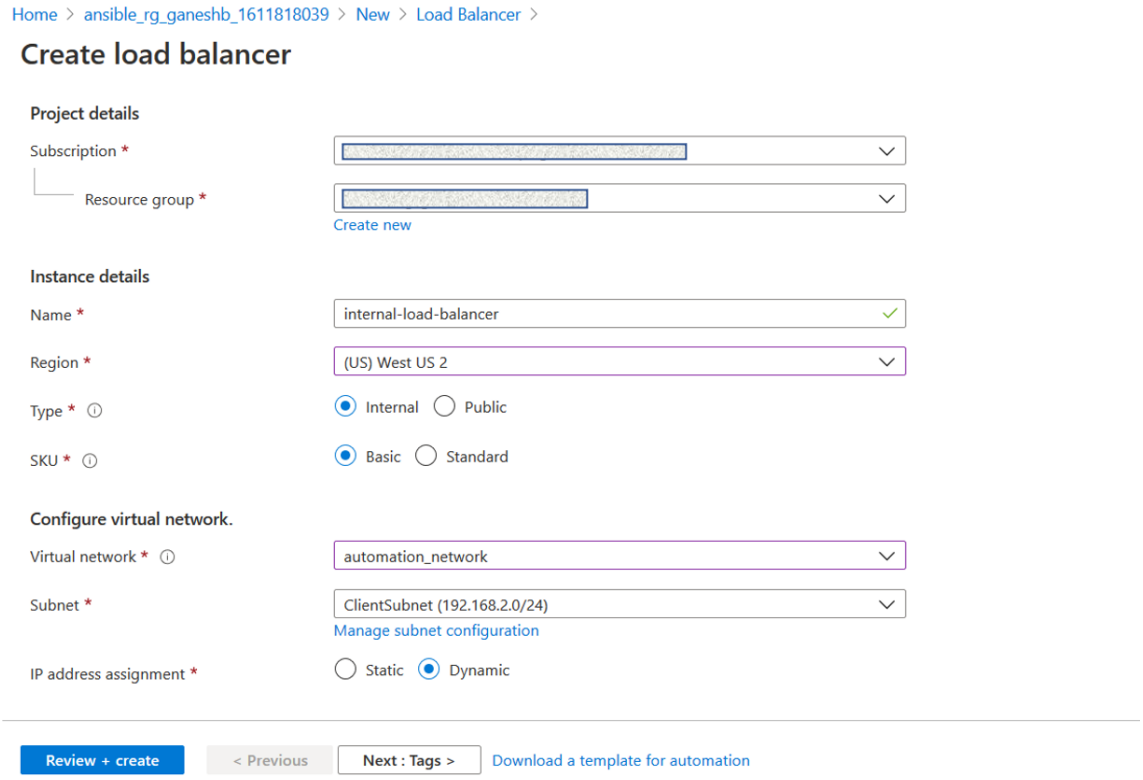
Schritt 1. Konfigurieren Sie einen Azure-Load Balancer, entweder einen externen Load Balancer oder einen internen Load Balancer.

Weitere Informationen zum Konfigurieren von Hochverfügbarkeits-Setups mit externen Azure Load Balancern finden Sie unter Konfigurieren eines Hochverfügbarkeits-Setups mit mehreren IP-Adressen und NIC.

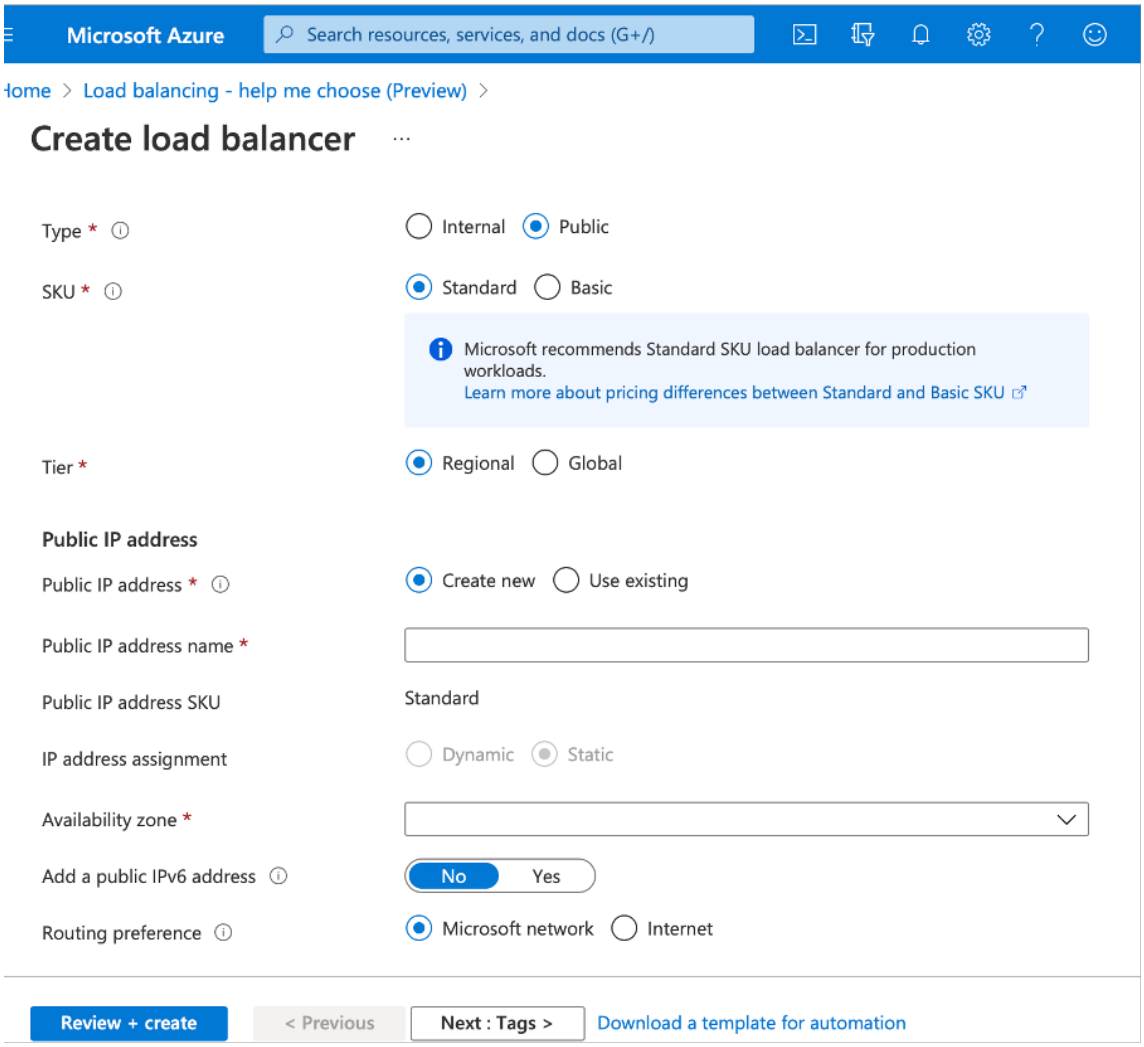
Weitere Informationen zum Konfigurieren von Hochverfügbarkeits-Setups mit internen Azure-Load Balancern finden Sie unter Konfigurieren von HA-INC-Knoten mithilfe der Citrix Hochverfügbarkeitsvorlage mit Azure ILB.

Schritt 2. Erstellen Sie einen zusätzlichen Load Balancer (ILB) in Ihrer Ressourcengruppe. Wenn Sie in Schritt 1 einen externen Load Balancer erstellt haben, erstellen Sie jetzt einen internen Load Balancer und umgekehrt.

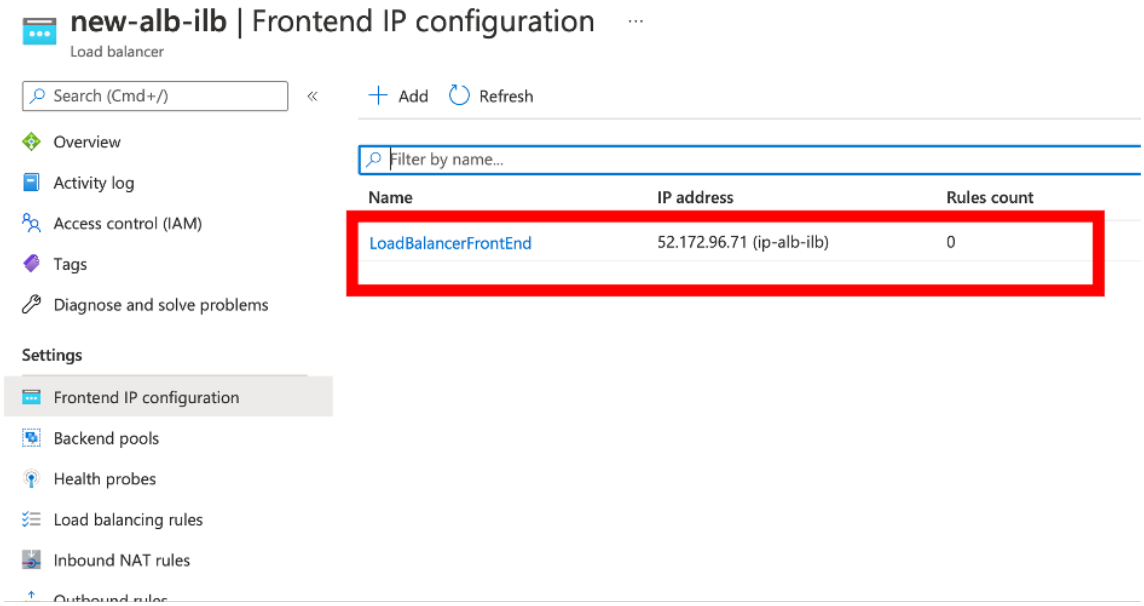
- Um einen internen Load Balancer zu erstellen, wählen Sie den Load Balancer-Typ als **Intern**aus. Für das Feld **Subnet** müssen Sie Ihr Citrix ADC Client-Subnetz auswählen. Sie können eine statische IP-Adresse in diesem Subnetz angeben, vorausgesetzt, es gibt keine Konflikte. Wählen Sie andernfalls die dynamische IP-Adresse aus.



- Um einen externen Load Balancer zu erstellen, wählen Sie den Load Balancer-Typ als **Public** und erstellen Sie hier die öffentliche IP-Adresse.



1. Nachdem Sie den Azure Load Balancer erstellt haben, navigieren Sie zur **Frontend-IP-Konfiguration** und notieren Sie sich die hier angezeigte IP-Adresse. Sie müssen diese IP-Adresse verwenden, während Sie den virtuellen ADC Load Balancing Server wie in Schritt 3 erstellen.



2. Auf der **Azure Load Balancer-Konfigurationsseite** hilft die Bereitstellung von ARM-Vorlagen beim Erstellen der LB-Regel, Back-End-Pools und Integritäts-Sonden.
3. Fügen Sie die Client-NICs mit hoher Verfügbarkeit zum Backend-Pool für die ILB hinzu.
4. Erstellen Sie eine Gesundheitssonde (TCP, 9000-Port)
5. Erstellen Sie zwei Load Balancing-Regeln:
    - Eine LB-Regel für HTTP-Datenverkehr (Webapp-Anwendungsfall) auf Port 80. Die Regel muss auch den Backend-Port 80 verwenden. Wählen Sie den erstellten Backend-Pool und die Integritätsprobe aus. Floating IP muss aktiviert sein.
    - Eine weitere LB-Regel für HTTPS- oder CVAD-Datenverkehr auf Port 443. Der Prozess ist der gleiche wie der HTTP-Datenverkehr.

Schritt 3. Erstellen Sie auf dem primären Knoten der Citrix ADC Appliance einen virtuellen Lastausgleichsserver für ILB.

1. Fügen Sie einen virtuellen Lastenausgleichsserver hinzu.

```
add lb vserver <name> <serviceType> [<ILB Frontend IP address>] [<
   port>]
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver vserver_name HTTP 52.172.96.71 80
```



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

> Hinweis:
>
> Verwenden Sie die Frontend-IP-Adresse des Load Balancers, die mit dem zusätzlichen Load Balancer verknüpft ist, den Sie in Schritt 2 erstellen.

2. Binden Sie einen Dienst an einen virtuellen Lastenausgleichsserver.

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

Beispiel:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Weitere Informationen finden Sie unter Einrichten des grundlegenden Lastenausgleichs

Schritt 4: Alternativ zu Schritt 3 können Sie mit IPSets einen virtuellen Lastausgleichsserver für ILB erstellen.

1. Fügen Sie eine IP-Adresse vom Typ Virtual Server IP (VIP) hinzu.

```
add nsip <ILB Frontend IP address> -type <type>
<!--NeedCopy-->
```

Beispiel:

```
add nsip 52.172.96.71 -type vip
<!--NeedCopy-->
```

2. Fügen Sie ein IPSet sowohl auf primären als auch auf sekundären Knoten hinzu.

```
add ipset <name>
<!--NeedCopy-->
```

Beispiel:


```
add ipset ipset1
<!--NeedCopy-->
```

3. Binden Sie IP-Adressen an den IP-Satz.

```
bind ipset <name> <ILB Frontend IP address>
<!--NeedCopy-->
```

Beispiel:

```
bind ipset ipset1 52.172.96.71
<!--NeedCopy-->
```

4. Stellen Sie den vorhandenen virtuellen LB-Server so ein, dass er das IPSet verwendet.

```
set lb vserver <vserver name> -ipset <ipset name>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver vserver_name -ipset ipset1
<!--NeedCopy-->
```

Weitere Informationen finden Sie unter Konfigurieren eines virtuellen Multi-IP-Servers.

Installieren Sie eine Citrix ADC VPX-Instanz auf Azure VMware Solution

July 15, 2022

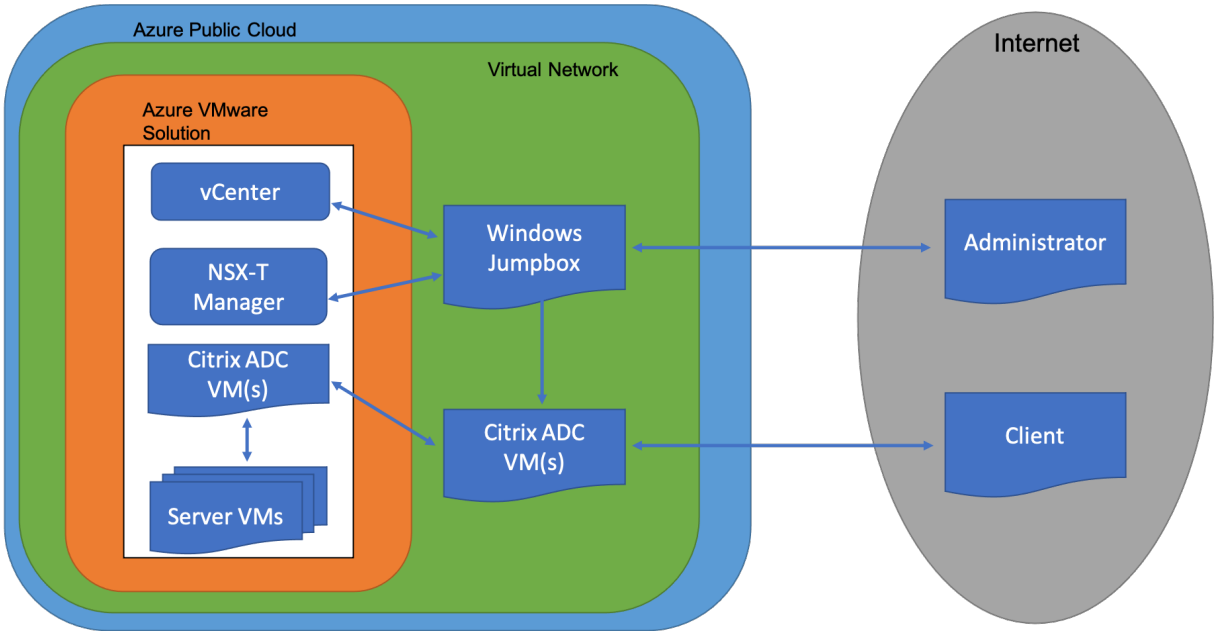
Azure VMware Solution (AVS) bietet Ihnen private Clouds, die vSphere-Cluster enthalten, die aus einer dedizierten Bare-Metal-Azure-Infrastruktur basieren. Die minimale Erstbereitstellung beträgt drei Hosts, aber zusätzliche Hosts können einzeln hinzugefügt werden, bis zu maximal 16 Hosts pro Cluster. Alle bereitgestellten Private Clouds verfügen über vCenter Server, vSAN, vSphere und NSX-T.

Mit der VMware Cloud (VMC) auf Azure können Sie Cloud-softwaredefinierte Rechenzentren (SDDC) auf Azure mit der Anzahl der gewünschten ESX-Hosts erstellen. Der VMC auf Azure unterstützt Citrix

ADC VPX-Bereitstellungen. VMC stellt eine Benutzeroberfläche bereit, die gleiche wie bei vCenter vor Ort ist. Es funktioniert ähnlich wie die ESX-basierten Citrix ADC VPX-Bereitstellungen.

Das folgende Diagramm zeigt die Azure VMware-Lösung in der Azure Public Cloud, auf die ein Administrator oder ein Client über das Internet zugreifen kann. Ein Administrator kann Workload- oder Server-VMs mit der Azure VMware-Lösung erstellen, verwalten und konfigurieren. Der Administrator kann von einer Windows Jumpbox aus auf das webbasierte vCenter und den NSX-T Manager des AVS zugreifen. Sie können die Citrix ADC VPX-Instanzen (eigenständige oder Hochverfügbarkeitspaar) und Server-VMs in Azure VMware Solution mit vCenter erstellen und das entsprechende Netzwerk mit NSX-T Manager verwalten. Die Citrix ADC VPX-Instanz auf AVS funktioniert ähnlich dem lokalen VMware-Host-Cluster. AVS wird von einer Windows Jumpbox aus verwaltet, die im selben virtuellen Netzwerk erstellt wird.

Ein Client kann nur auf den AVS-Dienst zugreifen, indem er sich mit dem VIP von ADC verbindet. Eine andere Citrix ADC VPX-Instanz außerhalb von Azure VMware Solution, aber im selben virtuellen Azure-Netzwerk, hilft dabei, den VIP der Citrix ADC VPX-Instanz in Azure VMware Solution als Dienst hinzuzufügen. Je nach Anforderung können Sie die Citrix ADC VPX-Instanz so konfigurieren, dass sie Dienste über das Internet bereitstellt.



Voraussetzungen

Bevor Sie mit der Installation einer virtuellen Appliance beginnen, gehen Sie folgendermaßen vor:

- Weitere Informationen zur Azure VMware-Lösung und ihren Voraussetzungen finden Sie in der Dokumentation zu Azure VMware Solution.
- Weitere Informationen zur Bereitstellung der Azure VMware-Lösung finden Sie unter Bereitstellen einer Azure VMware Solution Private Cloud.

- Weitere Informationen zum Erstellen einer Windows Jump Box-VM für den Zugriff und die Verwaltung der Azure VMware-Lösung finden Sie unter Zugriff auf eine private Cloud der Azure VMware Solution
- Laden Sie in der Windows Jump Box VM die Setupdateien der Citrix ADC VPX Appliance herunter.
- Erstellen Sie geeignete NSX-T-Netzwerksegmente auf VMware SDDC, mit denen sich die virtuellen Maschinen verbinden. Weitere Informationen finden Sie unter Hinzufügen eines Netzwerksegments in Azure VMware Solution
- VPX-Lizenzdateien abrufen.
- Virtuelle Maschinen (VMs), die in die Azure VMware Solution Private Cloud erstellt oder migriert wurden, müssen an ein Netzwerksegment angeschlossen sein.

VMware Cloud-Hardwareanforderungen

In der folgenden Tabelle sind die virtuellen Computerressourcen aufgeführt, die das VMware SDDC für jede virtuelle VPX NCore-Appliance bereitstellen muss.

Tabelle 1. Minimale virtuelle Datenverarbeitungsressourcen für die Ausführung einer Citrix ADC VPX-Instanz

Komponente	Voraussetzung
Speicher	2 GB
Virtuelle CPU (vCPU)	2
Virtuelle Netzwerkschnittstellen	In VMware SDDC können Sie maximal 10 virtuelle Netzwerkschnittstellen installieren, wenn die VPX-Hardware auf Version 7 oder höher aktualisiert wird.
Speicherplatz	20 GB

> Hinweis:
>
> Dies gilt zusätzlich zu den Datenträgeranforderungen für den Hypervisor.

Für die Produktion der virtuellen VPX-Appliance muss die vollständige Speicherzuweisung reserviert werden.

Systemanforderungen für OVF Tool 1.0

OVF Tool ist eine Client-Anwendung, die auf Windows- und Linux-Systemen ausgeführt werden kann. In der folgenden Tabelle werden die Systemvoraussetzungen für die Installation des OVF-Tools beschrieben.

Tabelle 2. Systemvoraussetzungen für die Installation von OVF-Werkzeugen

Komponente	Voraussetzung
Betriebssystem	Ausführliche Anforderungen von VMware finden Sie unter der PDF-Datei “OVF Tool User Guide”http://kb.vmware.com/.
CPU	mindestens 750 MHz, 1 GHz oder schneller empfohlen
RAM	1 GB Minimum, 2 GB empfohlen
NIC	Netzwerkkarte mit 100 Mbit/s oder schneller

Informationen zur Installation von OVF finden Sie unter der PDF-Datei “OVF Tool User Guide”http://kb.vmware.com/.

Herunterladen der Setup-Dateien für Citrix ADC VPX

Das Setuppaket für Citrix ADC VPX für VMware ESX folgt dem Format Open Virtual Machine (OVF). Sie können die Dateien von der Citrix Website herunterladen. Sie benötigen ein Citrix Konto, um sich anzumelden. Wenn Sie kein Citrix-Konto haben, rufen Sie die Startseite unter http://www.citrix.comauf. Klicken Sie auf den **Link Neue Benutzer**, und folgen Sie den Anweisungen, um ein neues Citrix Konto zu erstellen.

Navigieren Sie nach der Anmeldung auf der Citrix Homepage zum folgenden Pfad:

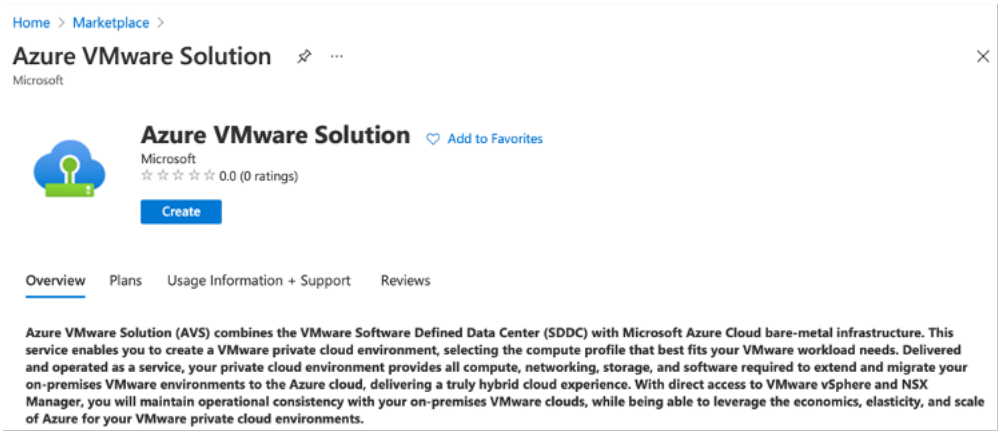
Citrix.com > **Downloads > Citrix ADC > Virtuelle Appliances**.

Kopieren Sie die folgenden Dateien auf eine Arbeitsstation im selben Netzwerk wie der ESX-Server. Kopieren Sie alle drei Dateien in denselben Ordner.

- NSVPX-ESX- <release number>- <build number>-disk1.vmdk (zum Beispiel NSVPX-ESX-13.0-79.64-disk1.vmdk)
- NSVPX-ESX- <release number>- <build number>.ovf (zum Beispiel NSVPX-ESX-13.0-79.64.ovf)
- NSVPX-ESX- <release number>- <build number>.mf (zum Beispiel NSVPX-ESX-13.0-79.64.mf)

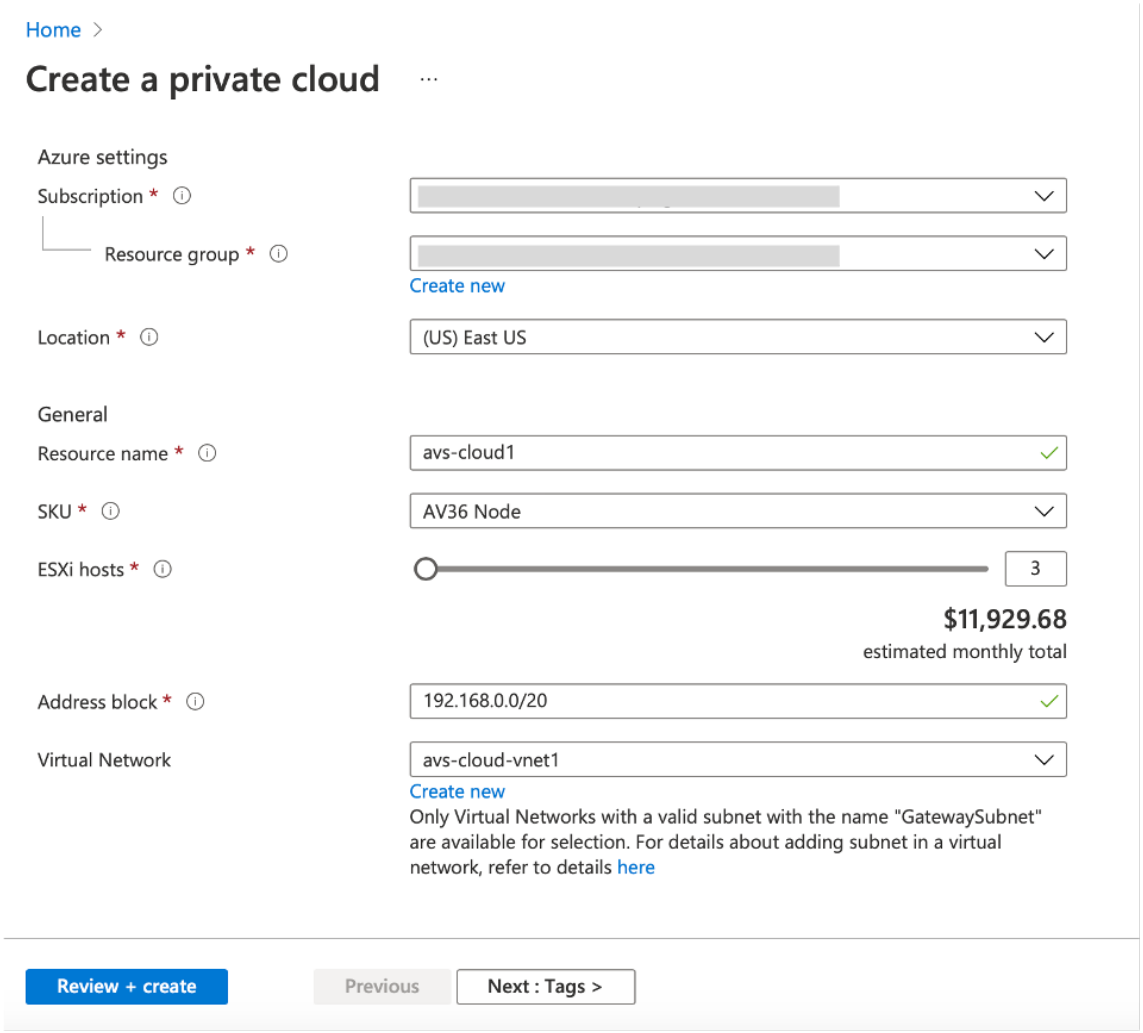
Bereitstellen von Azure VMware-Lösung

1. Melden Sie sich bei Ihrem Microsoft Azure-Portalan und navigieren Sie zu **Azure Marketplace**.
2. Suchen Sie im **Azure Marketplace**nach **Azure VMware Solution** und klicken Sie auf **Erstellen**.

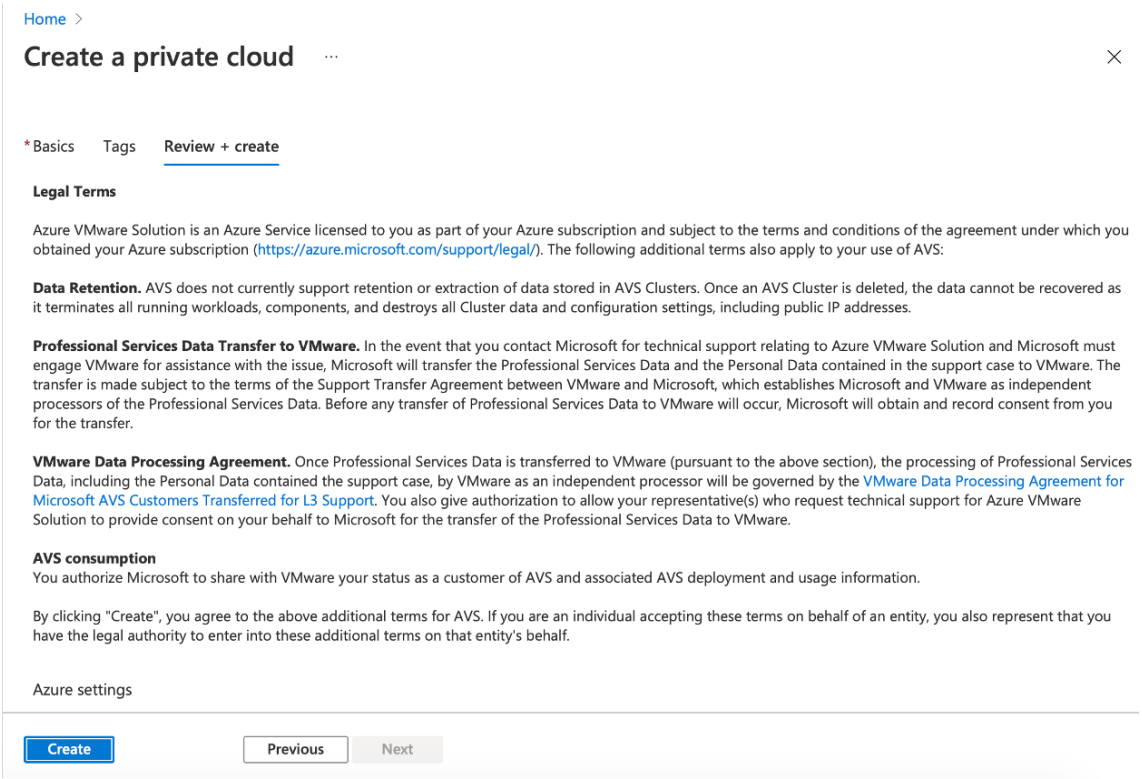


3. Geben **Sie auf der Seite Private Cloud erstellen** die folgenden Details ein:

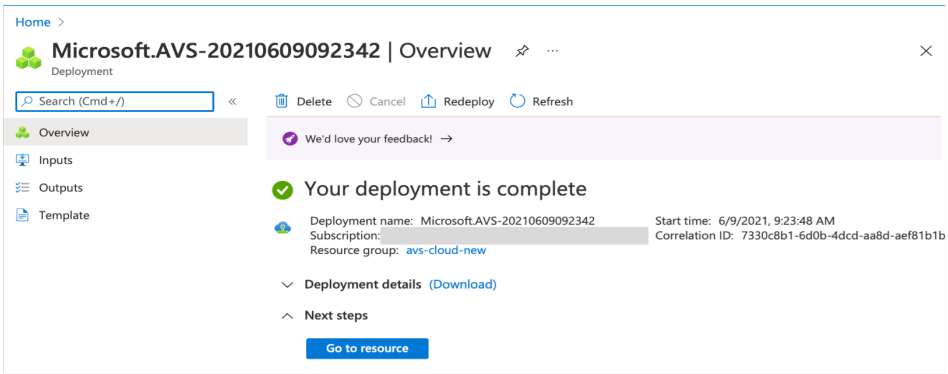
    - Wählen Sie mindestens 3 ESXi-Hosts aus, um den Standardcluster Ihrer Private Cloud zu erstellen.
    - Verwenden Sie für das Feld **Adressblock /22** Adressraum.
    - Stellen Sie für das **virtuelle Netzwerk**sicher, dass sich der CIDR-Bereich nicht mit einem Ihrer on-premises oder anderen Azure-Subnetze (virtuelle Netzwerke) oder mit dem Gateway-Subnetz überschneidet.
    - Das Gateway-Subnetz wird verwendet, um die Verbindung mit Private Cloud weiterzuleiten.



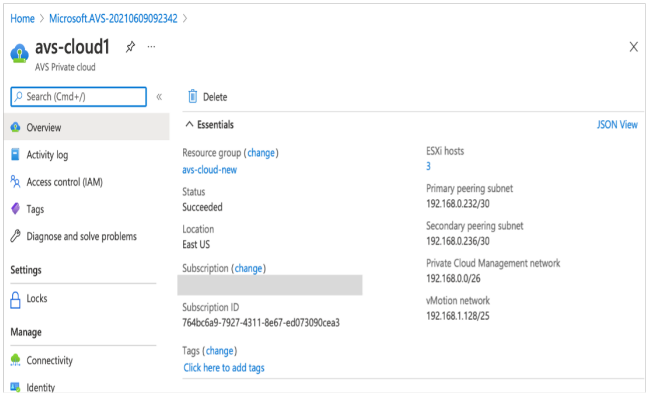
4. Klicken Sie auf **Review + Erstellen**.
5. Überprüfen Sie die Einstellungen. Wenn Sie Einstellungen ändern müssen, klicken Sie auf **Zurück**.



6. Klicken Sie auf **Erstellen**. Der Provisioning-Prozess der Private Cloud beginnt. Es kann bis zu zwei Stunden dauern, bis die Private Cloud bereitgestellt wird.



7. Klicken Sie auf **Gehe zu Ressource**, um die erstellte Private Cloud zu überprüfen.



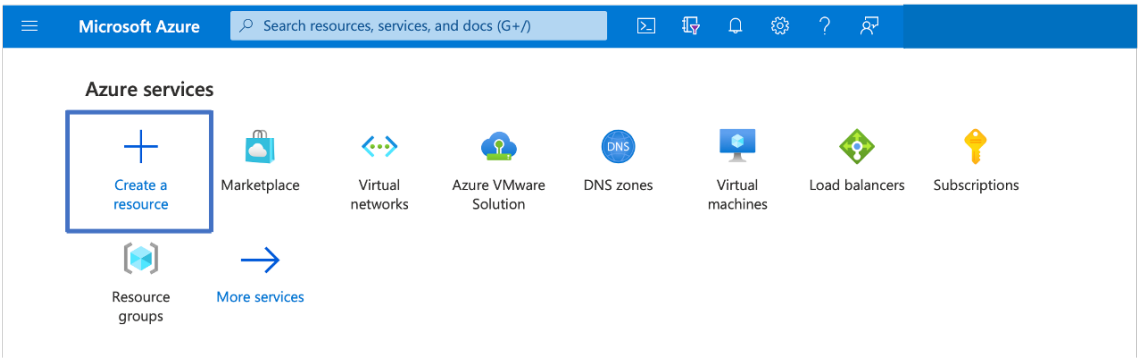
> Hinweis:
>
> Um auf diese Ressource zugreifen zu können, benötigen Sie eine VM in Windows, die als Sprungbox fungiert.

Verbinden Sie sich mit einer virtuellen Azure-Maschine unter Windows

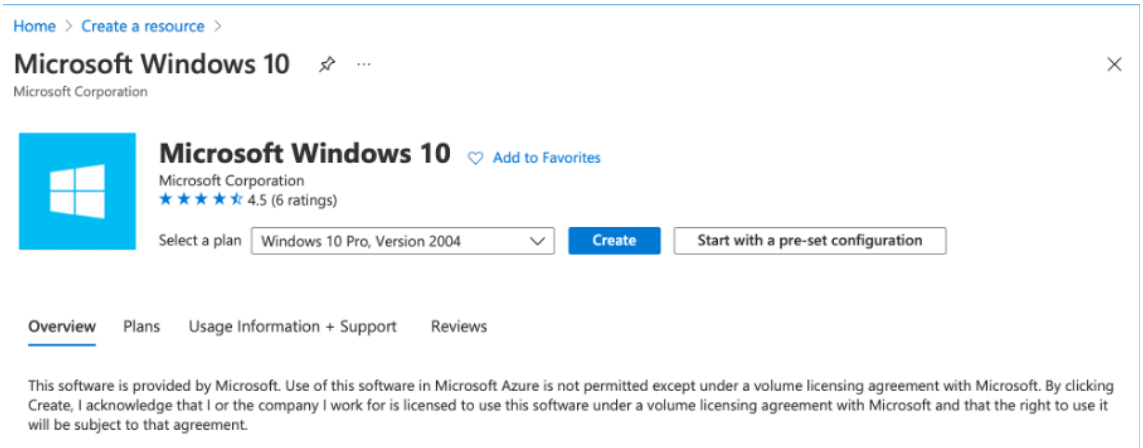
Dieses Verfahren zeigt Ihnen, wie Sie das Azure-Portal verwenden, um eine virtuelle Maschine (VM) in Azure bereitzustellen, auf der Windows Server 2019 ausgeführt wird. Um Ihre VM in Aktion zu sehen, rdp dann auf die VM und installieren den IIS-Webserver.

Um auf die von Ihnen erstellte Private Cloud zugreifen zu können, müssen Sie eine Windows Jump-Box innerhalb desselben virtuellen Netzwerks erstellen.

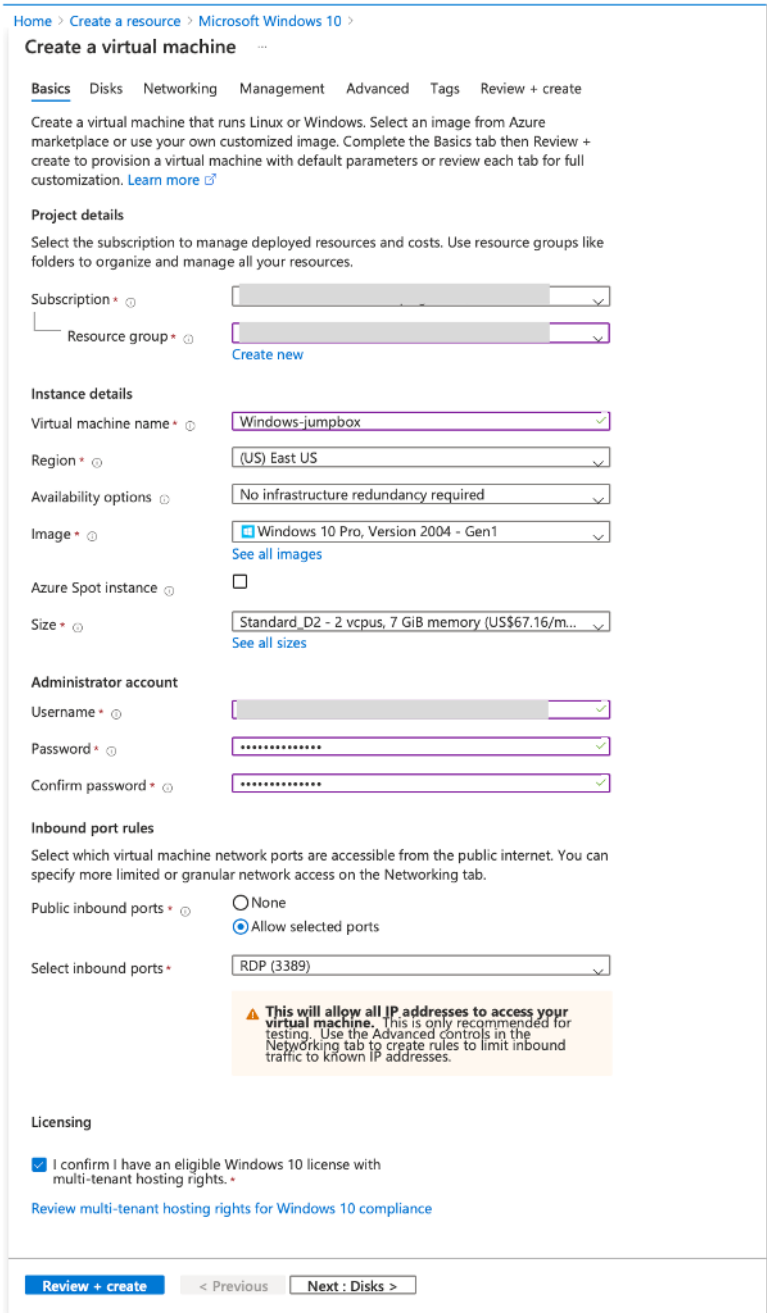
1. Wechseln Sie zum **Azure-Portal**und klicken Sie auf **Ressource erstellen**.



2. Suchen Sie nach **Microsoft Windows 10**und klicken Sie auf **Erstellen**.



3. Erstellen Sie eine virtuelle Maschine (VM), auf der Windows Server 2019 ausgeführt wird. Die Seite " **Virtuelle Maschine erstellen** " wird angezeigt. Geben Sie alle Details auf der Registerkarte **Grundlagen** ein und aktivieren Sie das Kontrollkästchen **Lizenzierung** . Belassen Sie die verbleibenden Standardeinstellungen und wählen Sie dann unten auf der Seite die Schaltfläche **Review + erstellen** .



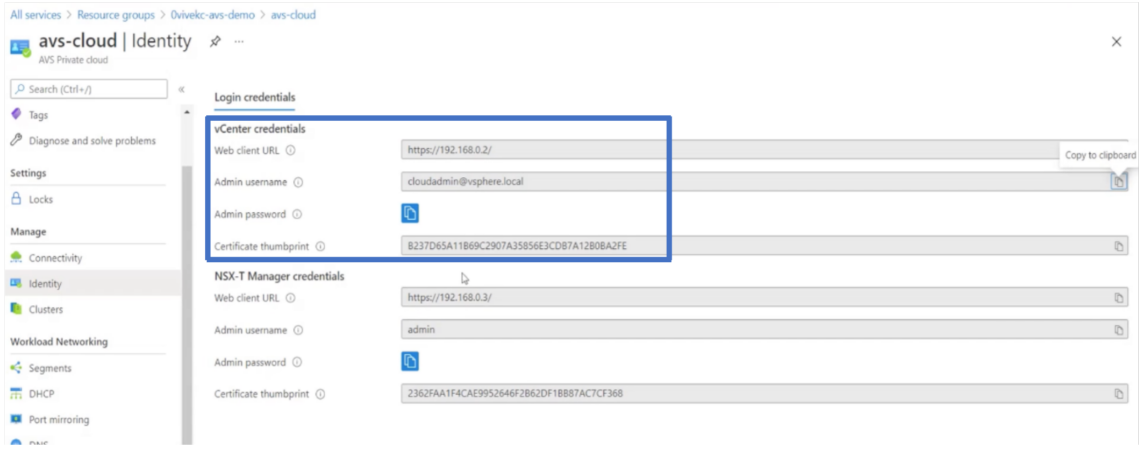
4. Nachdem die Validierung ausgeführt wurde, klicken Sie unten auf der Seite auf die Schaltfläche **Erstellen** .
5. Wählen Sie nach Abschluss der Bereitstellung **Gehe zu Ressource**aus.
6. Wechseln Sie zu der von Ihnen erstellten Windows-VM. Verwenden Sie die öffentliche IP-Adresse der Windows-VM und stellen Sie eine Verbindung mit RDP her.

   Verwenden Sie die Schaltfläche **Verbinden** im Azure-Portal, um eine Remotedesktop-Sitzung (RDP) von einem Windows-Desktop aus zu starten. Zuerst stellen Sie eine Verbindung mit der virtuellen Maschine her und melden sich dann an.

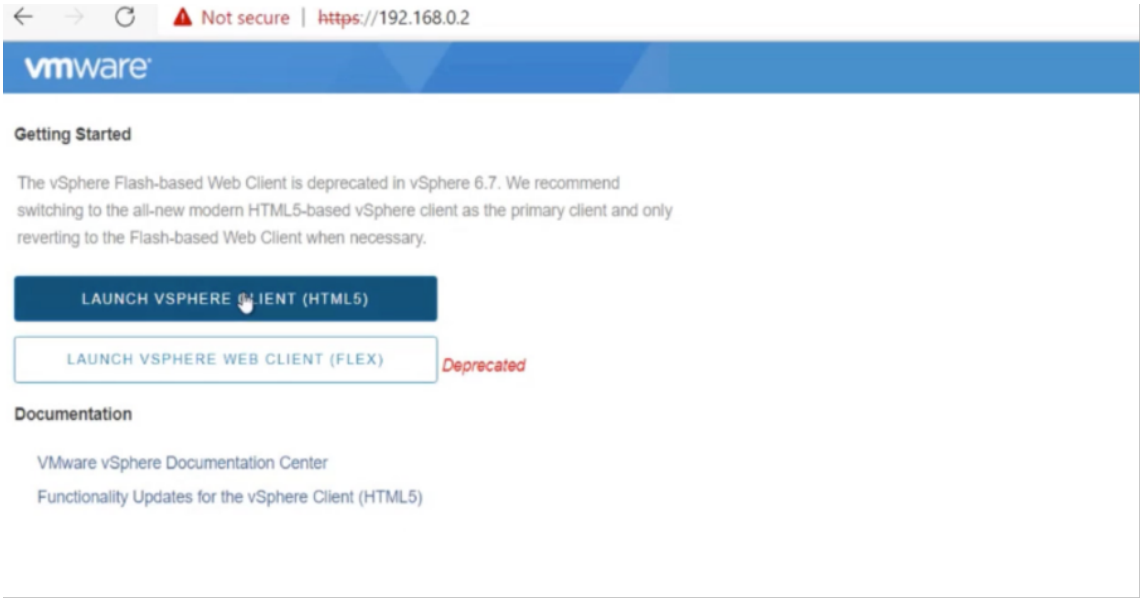
Um eine Verbindung mit einer Windows-VM von einem Mac aus herzustellen, müssen Sie einen RDP-Client für Mac wie Microsoft Remote Desktop installieren. Weitere Informationen finden Sie unter Herstellen und Melden Sie sich bei einer virtuellen Azure-Maschine unter Windowsan.

Greifen Sie auf Ihr Private Cloud vCenter Portal zu

1. Wählen Sie in Ihrer Azure VMware Solution Private Cloud unter **Verwalten**die Option **Identität**aus. Notieren Sie sich die vCenter-Anmeldeinformationen.

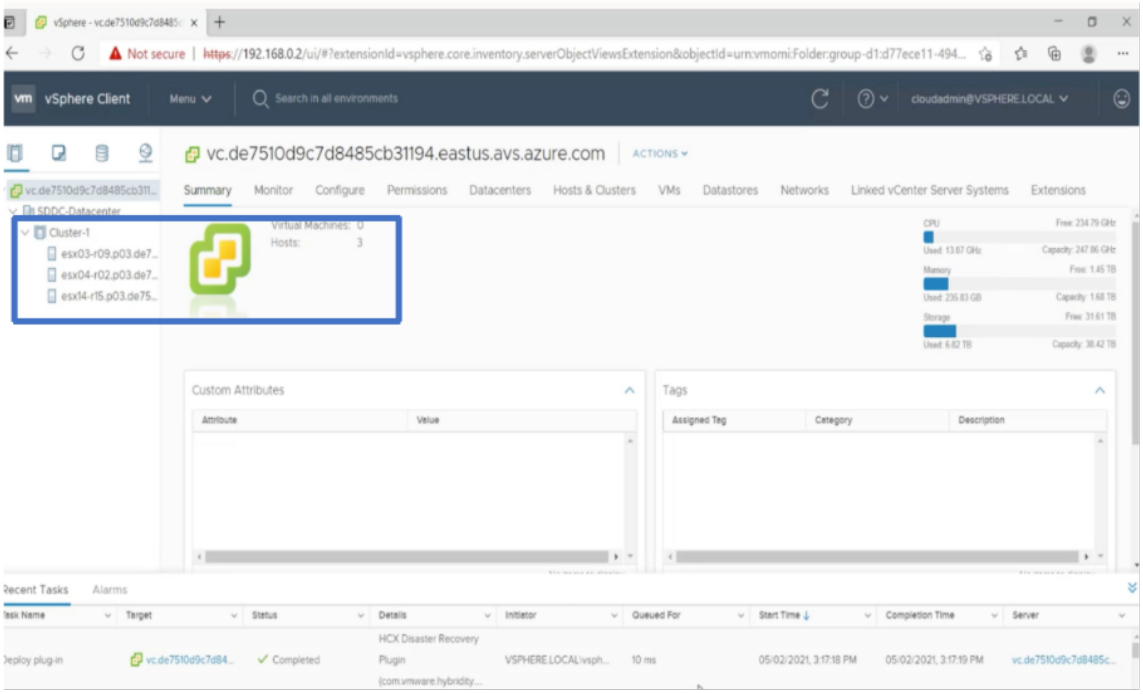


2. Starten Sie den vSphere-Client, indem Sie die vCenter-Webclient-URL eingeben.



3. Melden Sie sich mit den vCenter-Anmeldeinformationen Ihrer Azure VMware Solution Private Cloud bei VMware vSphere an.

4. Im vSphere-Client können Sie die ESXi-Hosts überprüfen, die Sie im Azure-Portal erstellt haben.



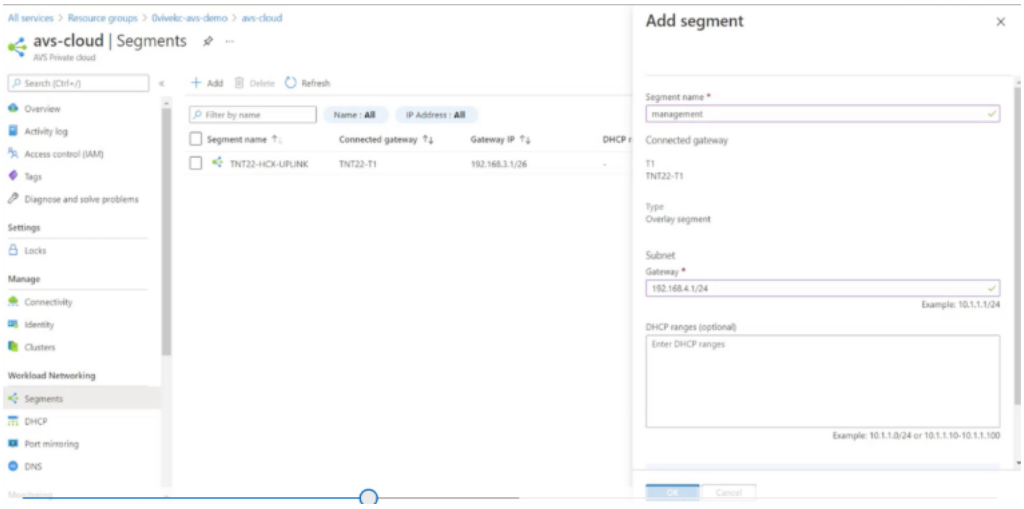
Weitere Informationen finden Sie unter Zugriff auf Ihr Private Cloud vCenter-Portal.

Erstellen Sie ein NSX-T-Segment im Azure-Portal

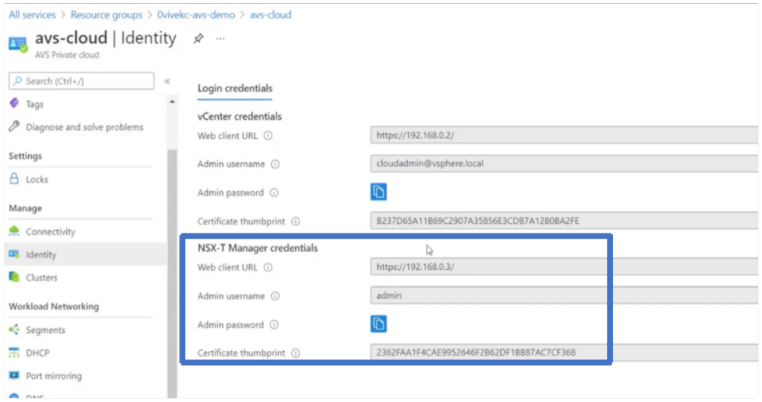
Sie können ein NSX-T-Segment über die Azure VMware Solution Console im Azure-Portal erstellen und konfigurieren. Diese Segmente sind mit dem Standard-Tier-1-Gateway verbunden, und die Workloads in diesen Segmenten erhalten Ost-West- und Nord-Süd-Konnektivität. Sobald Sie das Segment er-

stellt haben, wird es in NSX-T Manager und vCenter angezeigt.

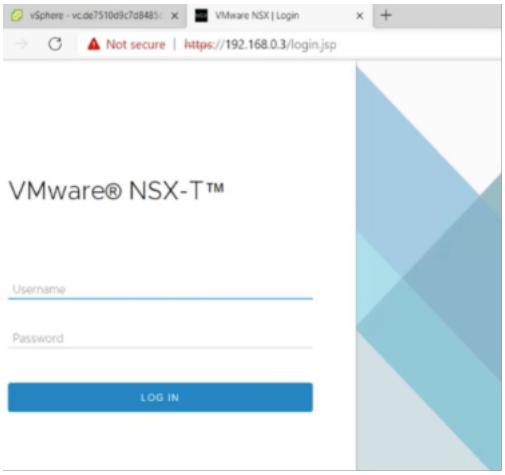
1. Wählen Sie in Ihrer Azure VMware Solution Private Cloud unter **Workload-Netzwerk Segmente > Hinzufügen**aus. Geben Sie die Details für das neue logische Segment ein und wählen Sie**OK**aus. Sie können drei separate Segmente für Client-, Management- und Server-Schnittstellen erstellen.



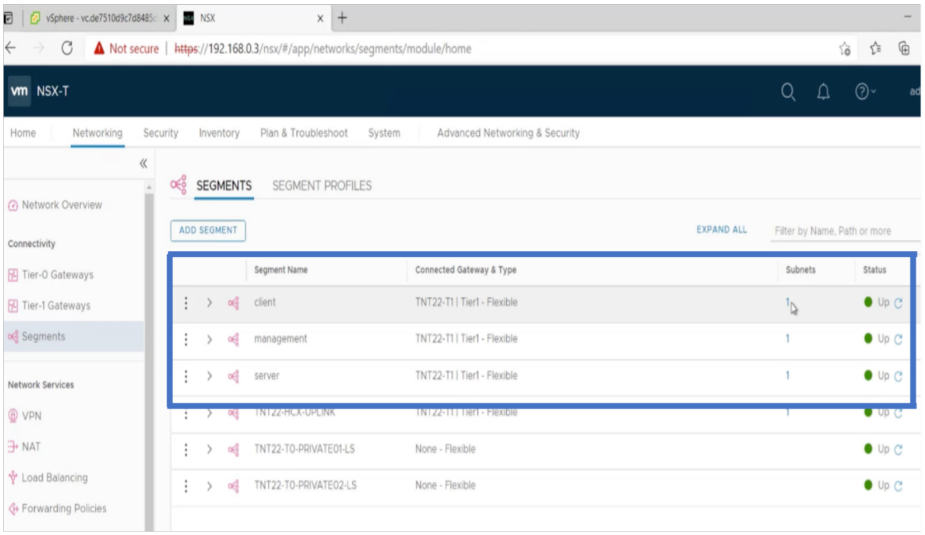
2. Wählen Sie in Ihrer Azure VMware Solution Private Cloud unter **Verwalten**die Option **Identität**aus. Notieren Sie sich die Anmeldeinformationen von NSX-T Manager.



3. Starten Sie den VMware NSX-T Manager, indem Sie die URL des NSX-T-Webclients eingeben.



4. Im NSX-T-Manager unter **Netzwerk > Segmente**sehen Sie alle Segmente, die Sie erstellt haben. Sie können die Subnetze auch überprüfen.



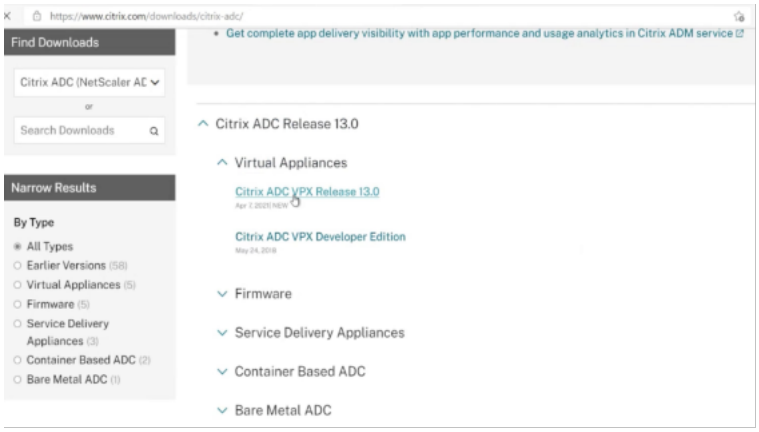
Weitere Informationen finden Sie unter Erstellen eines NSX-T-Segments im Azure-Portal.

Installieren einer Citrix ADC VPX Instanz in VMware Cloud

Nachdem Sie VMware Software-Defined Data Center (SDDC) installiert und konfiguriert haben, können Sie das SDDC verwenden, um virtuelle Appliances in der VMware-Cloud zu installieren. Die Anzahl der virtuellen Appliances, die Sie installieren können, hängt von der Menge des auf dem SDDC verfügbaren Speichers ab.

Um Citrix ADC VPX-Instanzen in der VMware Cloud zu installieren, führen Sie die folgenden Schritte in Windows Jumpbox VM aus:

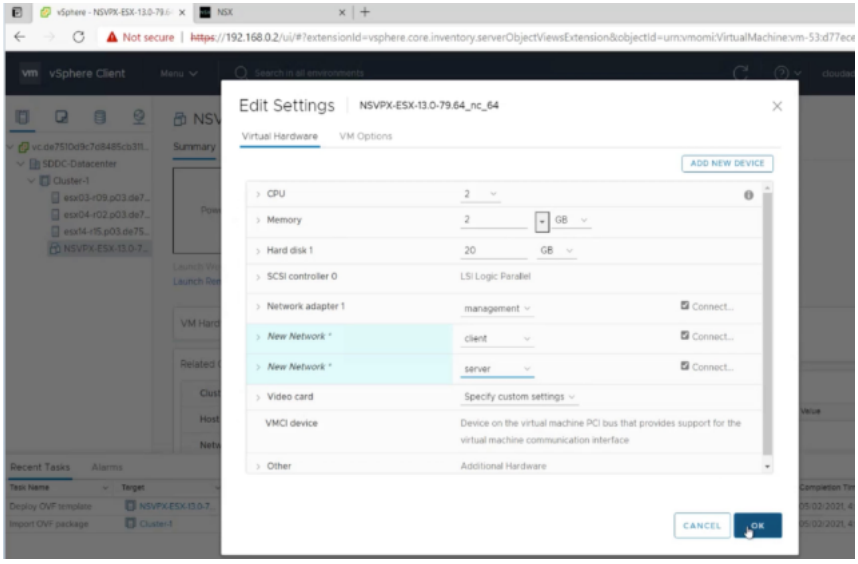
1. Laden Sie die Setupdateien der Citrix ADC VPX-Instanz für den ESXi-Host von der Citrix Downloads-Website herunter.



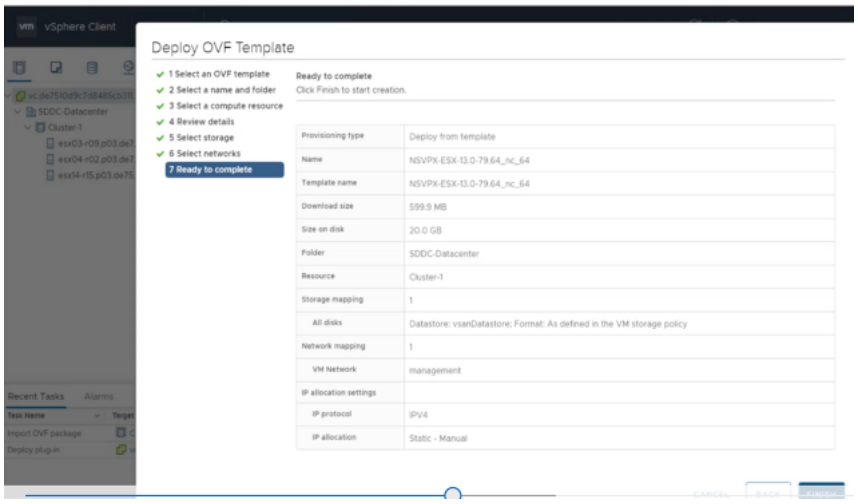
2. Öffnen Sie VMware SDDC in der Windows Jumpbox.
3. Geben Sie in die Felder **Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein, und klicken Sie dann auf **Anmelden**.
4. Klicken Sie im Menü **Datei** auf **OVF-Vorlage bereitstellen**.
5. Navigieren Sie im Dialogfeld **OVF-Vorlage bereitstellen im Feld Aus Datei bereitstellen**zu dem Speicherort, an dem Sie die Setupdateien der Citrix ADC VPX-Instanz gespeichert haben, wählen Sie die OVF-Datei aus, und klicken Sie auf**Weiter**.

   > HINWEIS:
   >
   > Standardmäßig verwendet die Citrix ADC VPX-Instanz E1000 Netzwerkschnittstellen. Um ADC mit der VMXNET3-Schnittstelle bereitzustellen, ändern Sie die OVF so, dass die VMXNET3-Schnittstelle anstelle von E1000 verwendet wird. Die Verfügbarkeit der VMXNET3-Schnittstelle ist durch die Azure-Infrastruktur begrenzt und ist möglicherweise in Azure VMware Solution nicht verfügbar.

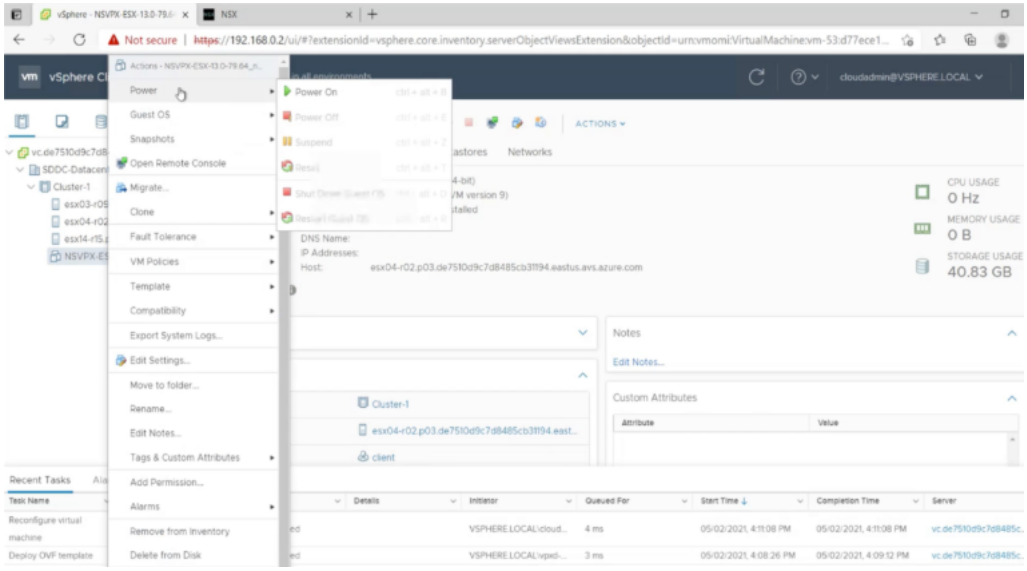
6. Ordnen Sie die in der OVF-Vorlage der virtuellen Appliance angezeigten Netzwerke den Netzwerken zu, die Sie auf dem VMware SDDC konfiguriert haben. Klicken Sie auf **OK**.



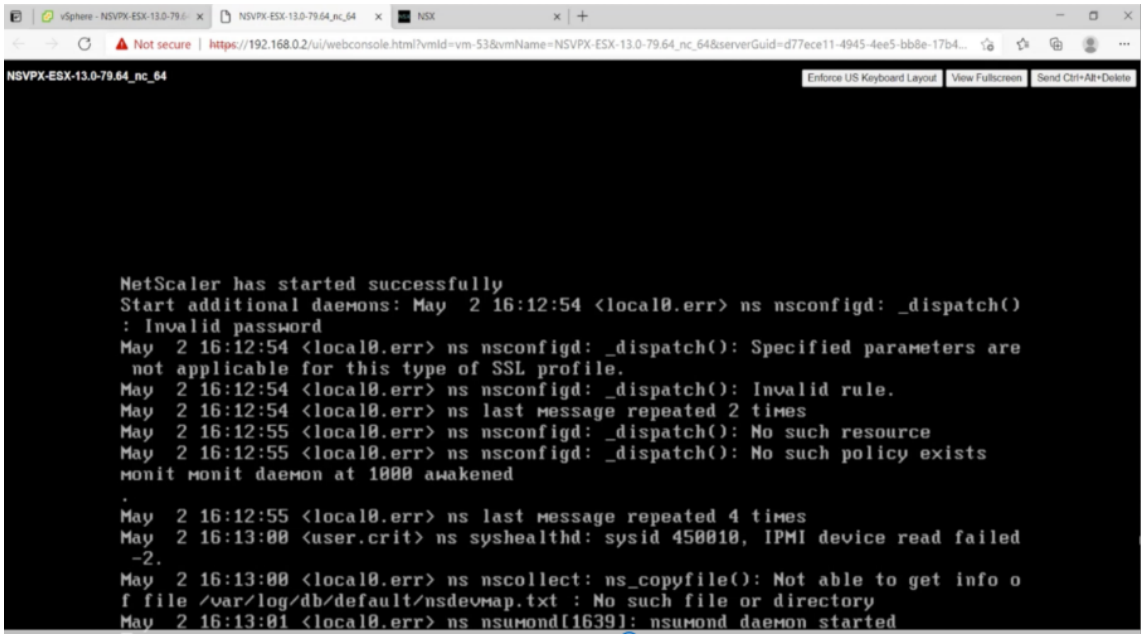
7. Klicken Sie auf **Fertig stellen**, um mit der Installation einer virtuellen Appliance auf VMware SDDC zu beginnen.



8. Sie können nun die Citrix ADC VPX-Instanz starten. Wählen Sie im Navigationsbereich die installierte Citrix ADC VPX-Instanz aus, und wählen Sie im Kontextmenü die Option **Einschalten**aus. Klicken Sie auf die Registerkarte **Konsole**, um einen Konsolenport zu emulieren.



9. Sie sind jetzt vom vSphere-Client aus mit der Citrix ADC VM verbunden.



10. Um mit den SSH-Schlüsseln auf die Citrix ADC Appliance zuzugreifen, geben Sie den folgenden Befehl in die CLI ein:

```
1 ssh nsroot@<management IP address>
2 <!--NeedCopy-->
```

Beispiel:


```
ssh nsroot@192.168.4.5
<!--NeedCopy-->
```

11. Sie können die ADC-Konfiguration mit dem `show ns ip` Befehl überprüfen.

    ! [Verifizieren mit `show nsip` Befehl] (/en-us/citrix-adc/media/avs-show-nsip.png)

Fügen Sie Azure Autoscale-Einstellungen hinzu

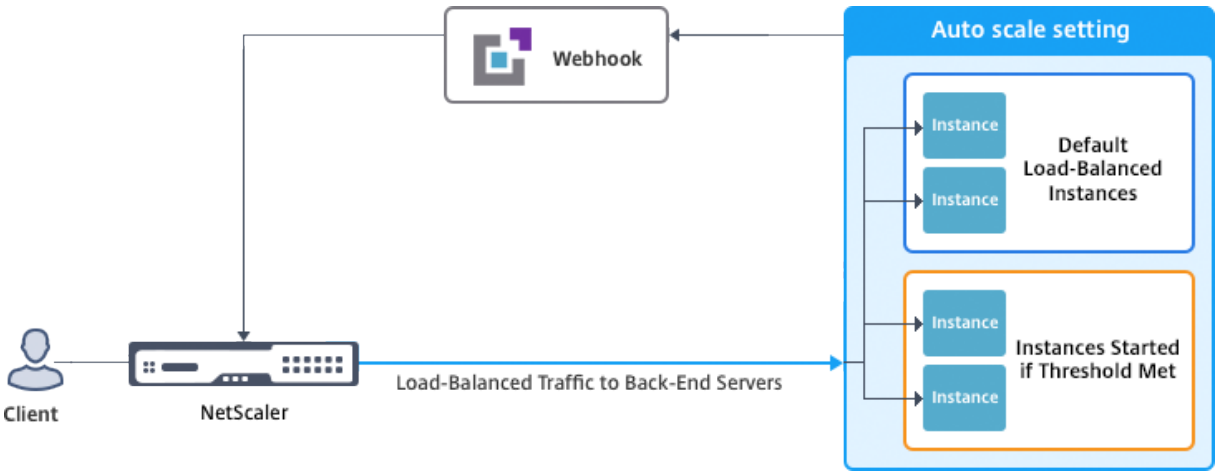
October 5, 2021

Effizientes Hosting von Anwendungen in einer Cloud erfordert eine einfache und kostengünstige Verwaltung der Ressourcen je nach Anwendungsbedarf. Um die steigende Nachfrage zu erfüllen, müssen Sie Netzwerkressourcen nach oben skalieren. Unabhängig davon, ob der Bedarf nachlässt, müssen Sie herunterskalieren, um unnötige Kosten für Leerlaufressourcen zu vermeiden. Um die Kosten für die Ausführung der Anwendung zu minimieren, müssen Sie den Datenverkehr, den Arbeitsspeicher und die CPU-Nutzung ständig überwachen und so weiter. Die manuelle Überwachung des Datenverkehrs ist jedoch umständlich. Damit die Anwendungsumgebung dynamisch nach oben oder unten skaliert werden kann, müssen Sie die Prozesse der Überwachung des Datenverkehrs und der Skalierung von Ressourcen bei Bedarf automatisieren.

Sie können Autoscale mit Azure VM Scale Sets (VMSS) für die eigenständige VPX Multi-IP-Bereitstellung und Hochverfügbarkeitsbereitstellung auf Azure verwenden.

Die Citrix ADC VPX-Instanz ist in die Skalierungssätze für virtuelle Maschinen (VMSS) und die Autoscale-Funktion von Azure integriert und bietet folgende Vorteile:

- Lastausgleich und -verwaltung: Automatisch konfiguriert Server so, dass sie je nach Bedarf hoch- und herunterskaliert werden. Die VPX-Instanz erkennt automatisch die VMSS Autoscale-Einstellung im Backend-Subnetz in derselben Ressourcengruppe wie die VPX-Instanz und ermöglicht dem Benutzer, die VMSS Autoscale-Einstellung auszuwählen, um die Last auszugleichen. All dies geschieht durch die automatische Konfiguration virtueller Citrix ADC Adressen und Subnetz-IP-Adressen auf der VPX-Instanz.
- Hochverfügbarkeit: Erkennt Autoscale-Gruppen in derselben Ressourcengruppe und Lastausgleichsserver.
- Bessere Netzwerkverfügbarkeit: Die VPX-Instanz unterstützt Back-End-Server in verschiedenen virtuellen Netzwerken (VNETs).



Weitere Informationen finden Sie im folgenden Azure-Thema

- Dokumentation zu Skalierungssätzen für virtuelle Maschinen
- Überblick über Autoscale in virtuellen Maschinen, Cloud-Diensten und Web-Apps von Microsoft Azure

Voraussetzungen

1. Lesen Sie die Azure-bezogenen Nutzungsrichtlinien. Weitere Informationen finden Sie unter Bereitstellen einer Citrix ADC VPX-Instanz auf Microsoft Azure.
2. Erstellen Sie je nach Anforderung eine oder mehrere Citrix ADC VPX -Instanzen mit drei Netzwerkschnittstellen in Azure (eigenständige oder hochverfügbare Bereitstellung).
3. Öffnen Sie den TCP 9001-Port in der Netzwerksicherheitsgruppe der 0/1-Schnittstelle der VPX-Instanz. Die VPX-Instanz verwendet diesen Port, um die Scale-Out- und Scale-In-Benachrichtigung zu empfangen.
4. Erstellen Sie einen Azure Virtual Machine Scale Set (VMSS) in derselben Ressourcengruppe. Wenn Sie über keine vorhandene VMSS-Konfiguration verfügen, führen Sie die folgenden Aufgaben aus:

   a) Erstellen eines VMSS

   b) Autoscale auf VMSS aktivieren

   c) Erstellen Sie eine Scale-In- und Scale-Out-Richtlinie in der VMSS-Autoscale-Einstellung

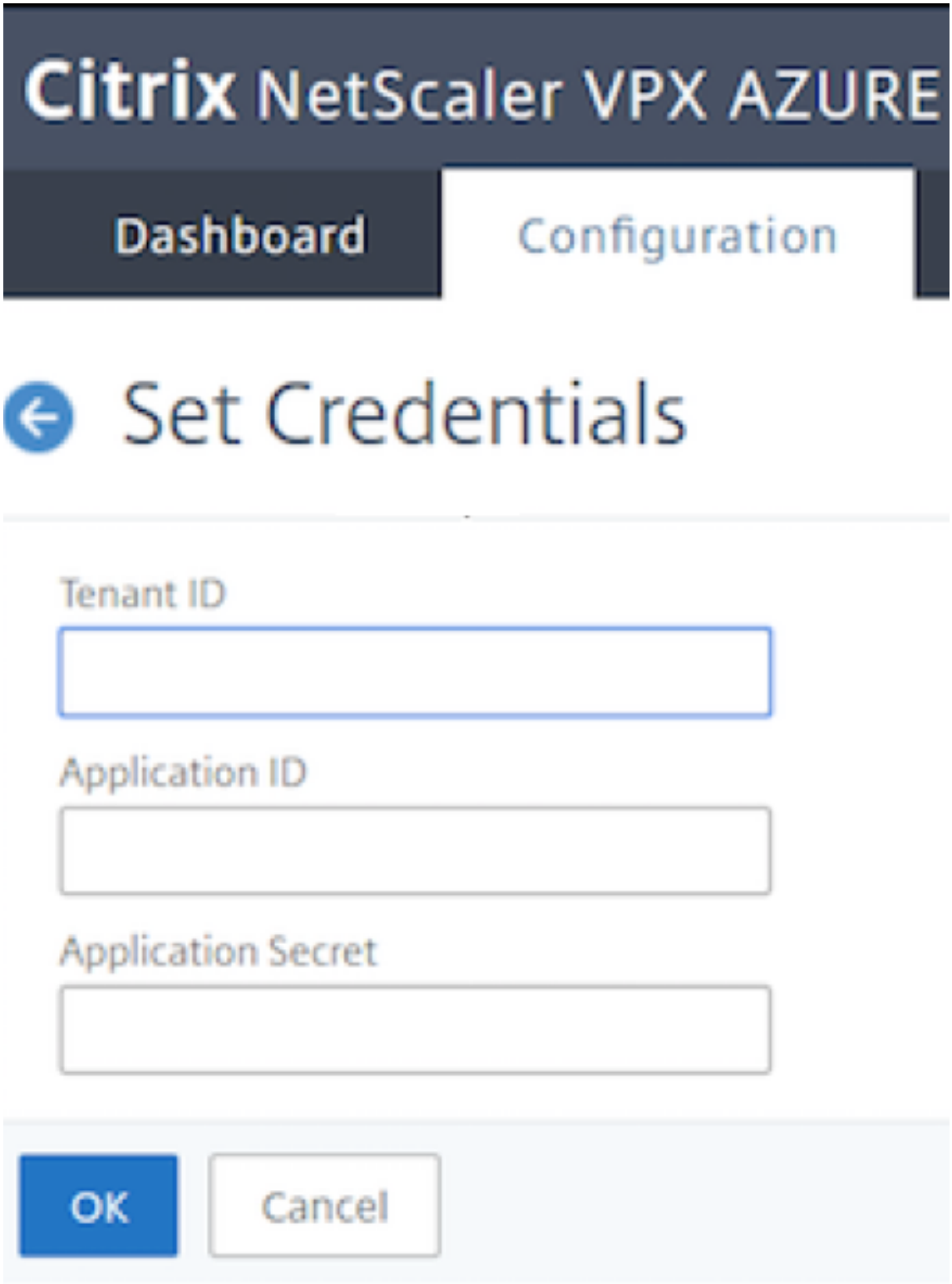
   Weitere Informationen finden Sie unter Überblick über Autoscale with Azure Skalierungssätze für virtuelle Maschinen.
5. Erstellen Sie eine Azure Active Directory (ADD) -Anwendung und Dienstprinzipal, die auf Ressourcen zugreifen können. Weisen Sie der neu erstellten AAD-Anwendung die Rolle der Mitwirkenden zu. Weitere Informationen finden Sie unter Verwenden des Portals zum Erstellen

einer Azure Active Directory-Anwendung und eines Dienstprinzipals, die auf Ressourcen zugreifen können.

Hinzufügen von VMSS zu einer Citrix ADC VPX-Instanz

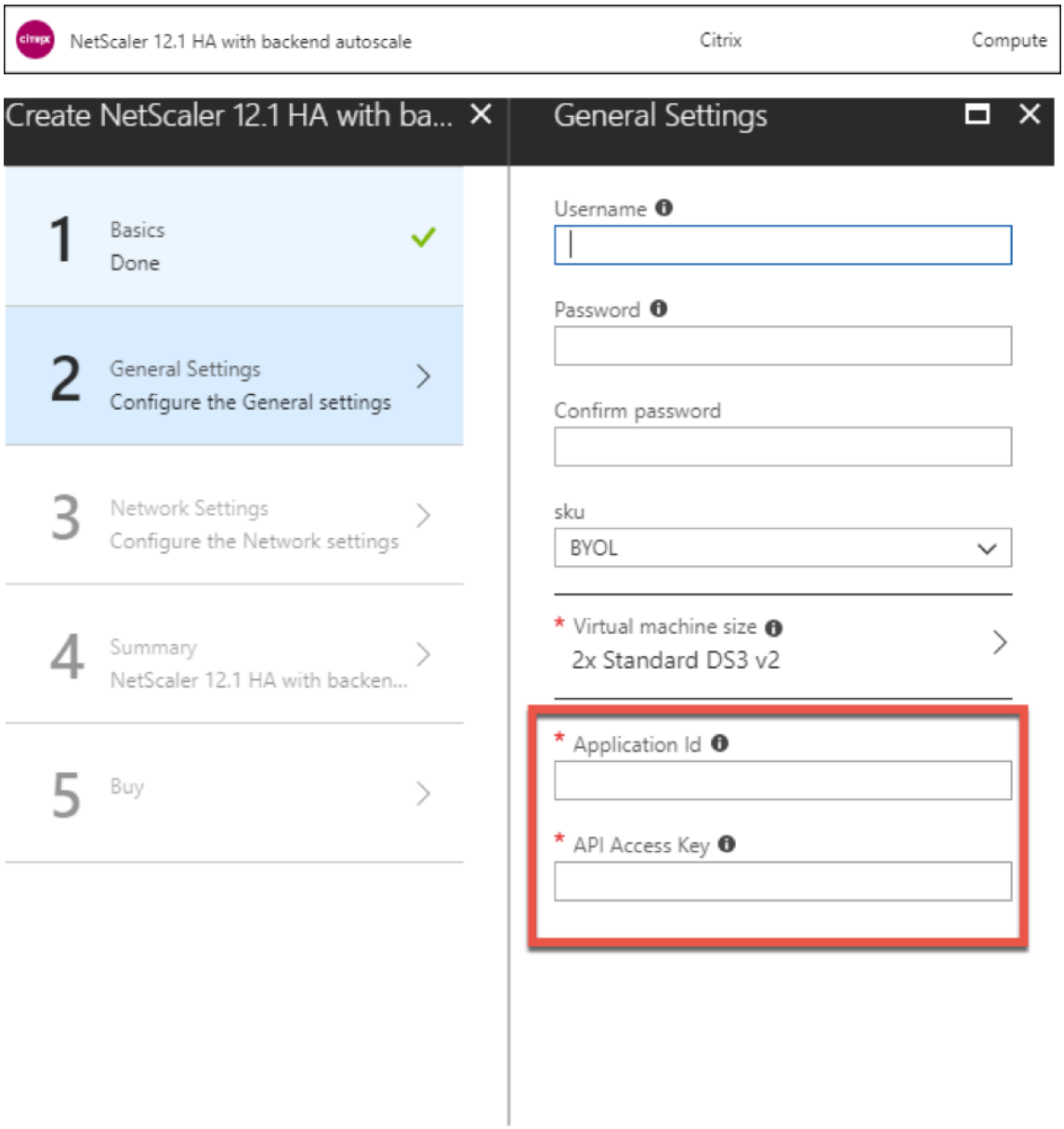
Sie können die Autoscale-Einstellung mit einem einzigen Klick zu einer VPX-Instanz hinzufügen, indem Sie die GUI verwenden. Führen Sie diese Schritte aus, um der VPX-Instanz die Autoscale-Einstellung hinzuzufügen:

1. Melden Sie sich bei der VPX-Instanz an.
2. Wenn Sie sich zum ersten Mal bei der Citrix ADC VPX-Instanz anmelden, wird die Seite Anmeldeinformationen festlegen angezeigt. Fügen Sie die erforderlichen Azure-Anmeldeinformationen hinzu, damit die Autoscale-Funktion funktioniert.



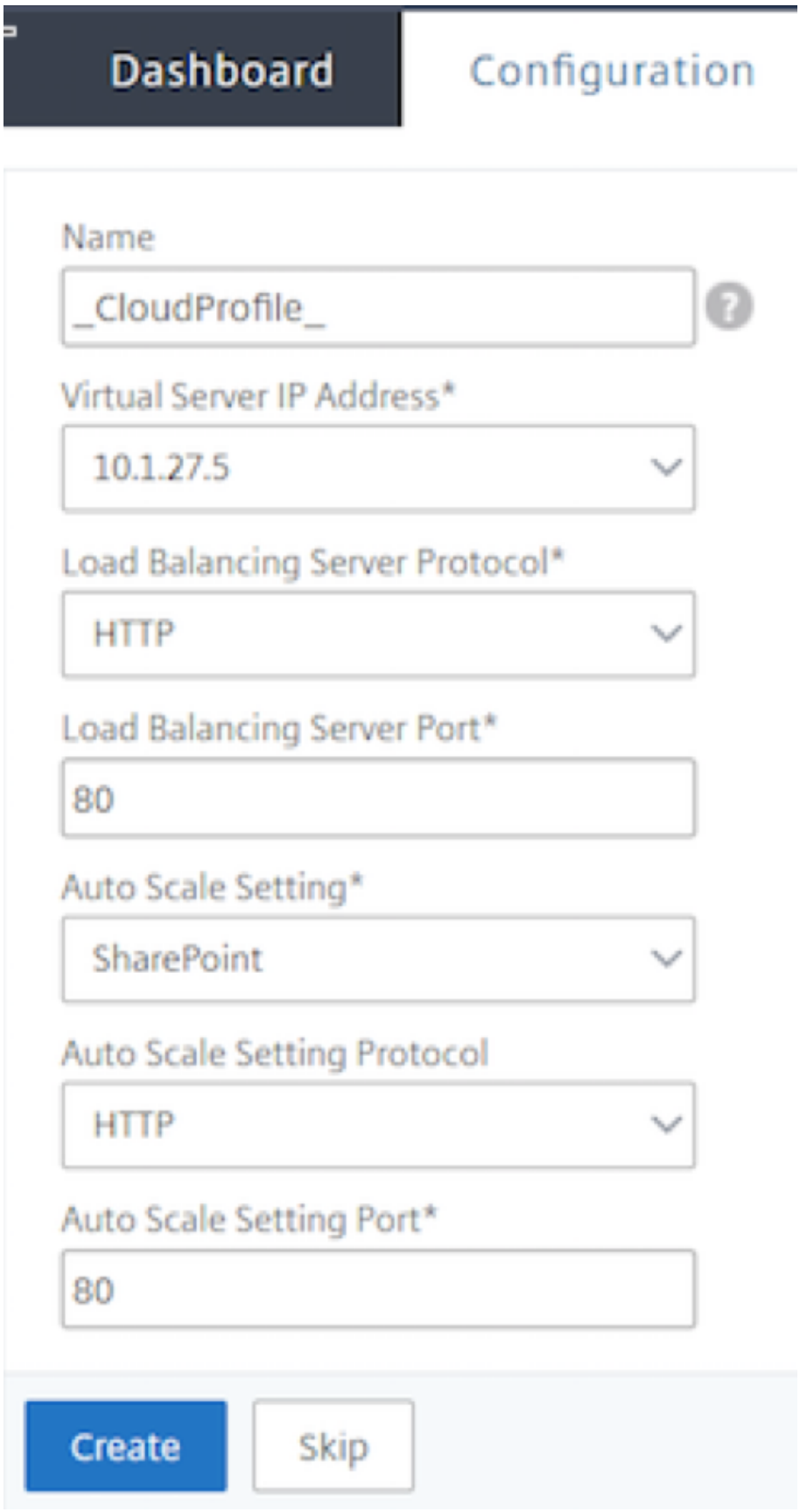
Die Seite “Anmeldeinformationen festlegen” wird nur angezeigt, wenn die Anwendungs-ID und der API-Zugriffsschlüssel nicht festgelegt sind oder die richtigen Anwendungs-ID und API-Zugriffsschlüssel (wie Application Secret) im Azure-Portal nicht festgelegt sind.

Wenn Sie das Angebot “NetScaler 12.1 HA mit Back-End-Autoscale” vom Azure Marketplace bereitstellen, fordert das Azure-Portal zur Eingabe der Hauptanmeldeinformationen des Azure-Dienstes (Anwendungs-ID und API-Zugriffsschlüssel) auf.



Informationen zum Erstellen einer Anwendungs-ID finden Sie unter Anwendung hinzufügen und Erstellen eines Zugriffsschlüssels oder eines Anwendungsgeheimnisses finden Sie unter Konfigurieren einer Clientanwendung für den Zugriff auf Web-APIs.

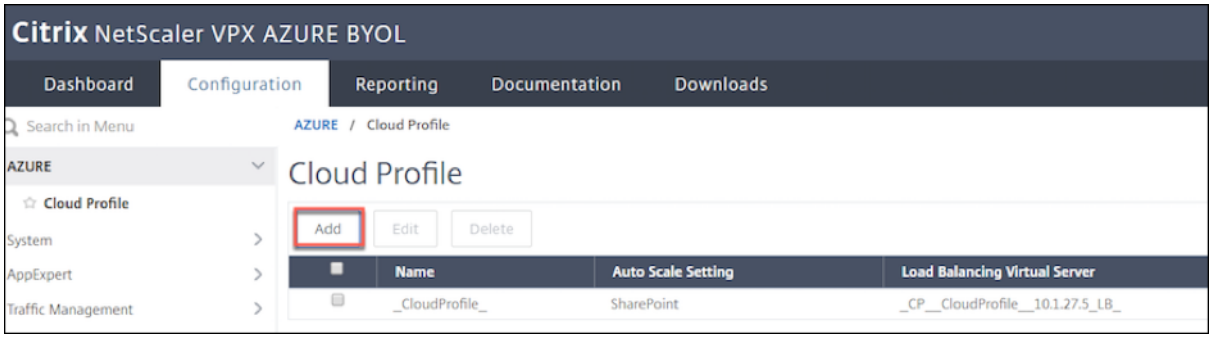
3. Geben Sie auf der Standard-Cloud-Profilseite die Details ein, wie im folgenden Beispiel gezeigt, und klicken Sie auf Erstellen.



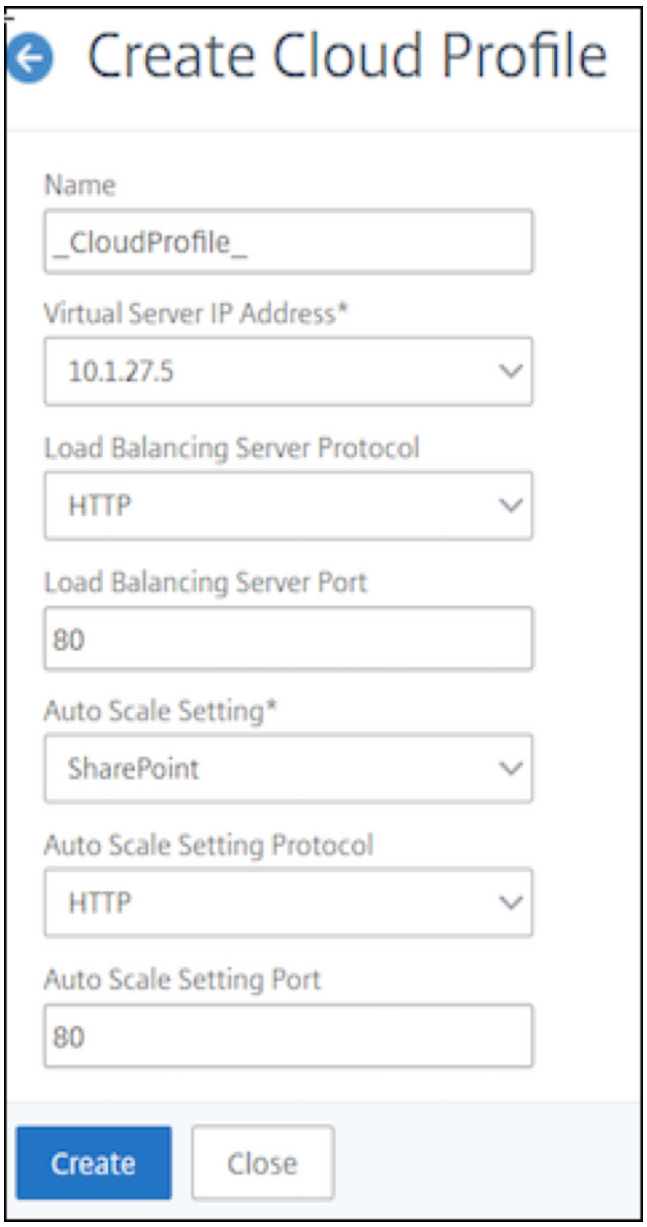
Punkte, die beim Erstellen eines Cloud-Profils berücksichtigt werden müssen

- Die IP-Adresse des virtuellen Servers wird automatisch von der freien IP-Adresse ausgefüllt, die für die VPX-Instanz verfügbar ist. Weitere Informationen finden Sie unter Zuweisen mehrerer IP-Adressen zu virtuellen Maschinen über das Azure-Portal.
- Die Autoscale-Einstellung wird in der Einstellung VMSS Autoscale vorausgefüllt, die in der aktuellen Ressourcengruppe Ihres Azure-Kontos konfiguriert ist. Weitere Informationen finden Sie unter Überblick über Autoscale with Azure Skalierungssätze für virtuelle Maschinen.
- Achten Sie bei der Auswahl des Protokolls und des Ports der Auto Scaling Group darauf, dass die Server diese Protokolle und Ports überwachen und den richtigen Monitor in der Dienstgruppe binden. Standardmäßig wird der TCP-Monitor verwendet.
- Für SSL-Protokolltyp Autos Scaling ist nach dem Erstellen des Cloud-Profils der Lastausgleich der virtuelle Server oder die Dienstgruppe aufgrund eines fehlenden Zertifikats ausgefallen. Sie können das Zertifikat manuell an den virtuellen Server oder die Dienstgruppe binden.

Wenn Sie nach der ersten Anmeldung ein Cloud-Profil erstellen möchten, gehen Sie in der GUI zu System > Azure > Cloud-Profil und klicken Sie auf Hinzufügen.



Die Seite Cloud-Profil erstellen wird angezeigt.



Cloud Profile erstellt einen virtuellen Citrix ADC Load Balancing (LB) Server (virtueller Server) und eine Dienstgruppe mit Mitgliedern (Servern) als Server der Auto Scaling-Gruppe. Ihre Back-End-Server müssen über das auf der VPX-Instanz konfigurierte SNIP erreichbar sein.

Um Autoscale-bezogene Informationen im Azure-Portal anzuzeigen, gehen Sie zu Alle Dienste > Skalierungssatz für virtuelle Computer > Skalierung auswählen.

Azure-Tags für Citrix ADC VPX Bereitstellung

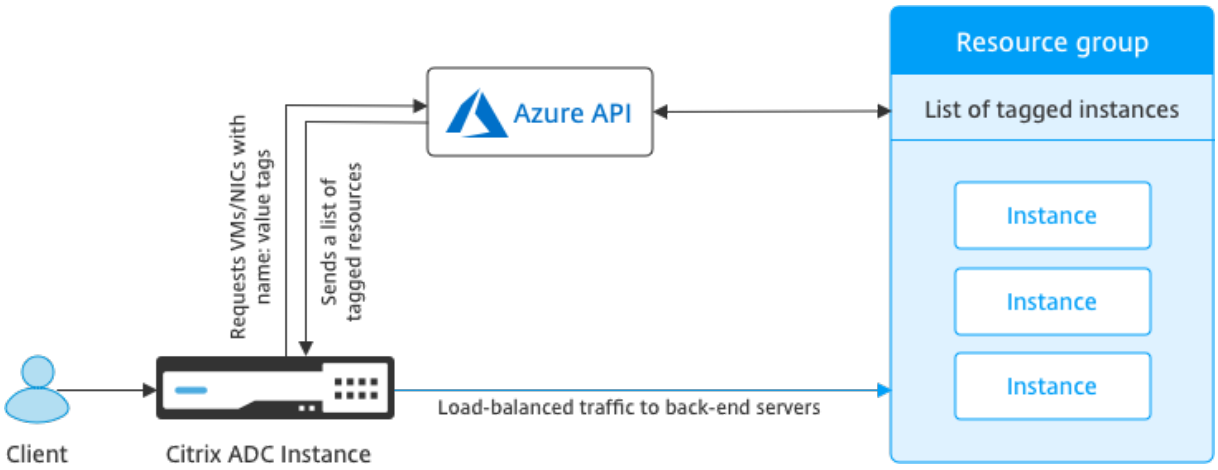
October 5, 2021

Im Azure-Cloud-Portal können Sie Ressourcen mit einem Namen: Wertepaar (wie Abt: Finance) kennzeichnen, um Ressourcen zwischen Ressourcengruppen und innerhalb des Portals über Abonnements hinweg zu kategorisieren und anzuzeigen. Tagging ist hilfreich, wenn Sie Ressourcen für die Abrechnung, Verwaltung oder Automatisierung organisieren müssen.

Funktionsweise des Azure-Tags für die VPX-Bereitstellung

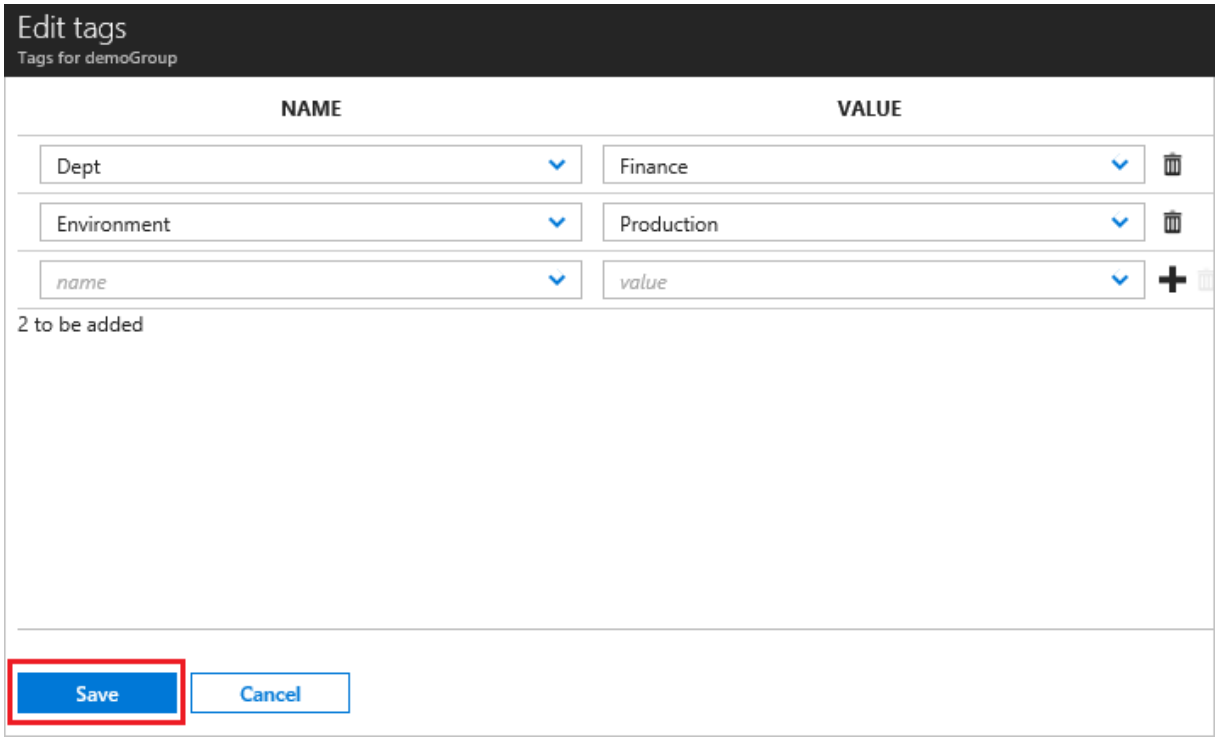
Für eigenständige Citrix ADC VPX-Instanzen und Hochverfügbarkeitsinstanzen, die in Azure Cloud bereitgestellt werden, können Sie jetzt Lastausgleichsdienstgruppen erstellen, die einem Azure-Tag zugeordnet sind. Die VPX-Instanz überwacht ständig virtuelle Azure-Computer (Back-End-Server) und Netzwerkschnittstellen (NICs) oder beides mit dem entsprechenden Tag und aktualisiert die Servicegruppe entsprechend.

Die VPX-Instanz erstellt die Dienstgruppe, die die Back-End-Server mit Tags ausgleicht. Die Instanz fragt die Azure-API nach allen Ressourcen ab, die mit einem bestimmten Tag-Namen und Tag-Wert gekennzeichnet sind. Abhängig vom zugewiesenen Abfragezeitraum (standardmäßig 60 Sekunden) fragt die VPX-Instanz regelmäßig die Azure-API ab und ruft die verfügbaren Ressourcen mit dem Tag-Namen und den Tag-Werten ab, die in der VPX-GUI zugewiesen sind. Wenn eine VM oder Netzwerkkarte mit dem entsprechenden Tag hinzugefügt oder gelöscht wird, erkennt der ADC die entsprechende Änderung und fügt die VM oder NIC IP-Adresse automatisch aus der Dienstgruppe hinzu oder löscht sie automatisch.



Voraussetzungen

Bevor Sie Citrix ADC Load Balancing-Dienstgruppen erstellen, fügen Sie den Servern in Azure ein Tag hinzu. Sie können das Tag entweder der virtuellen Maschine oder der Netzwerkkarte zuweisen.



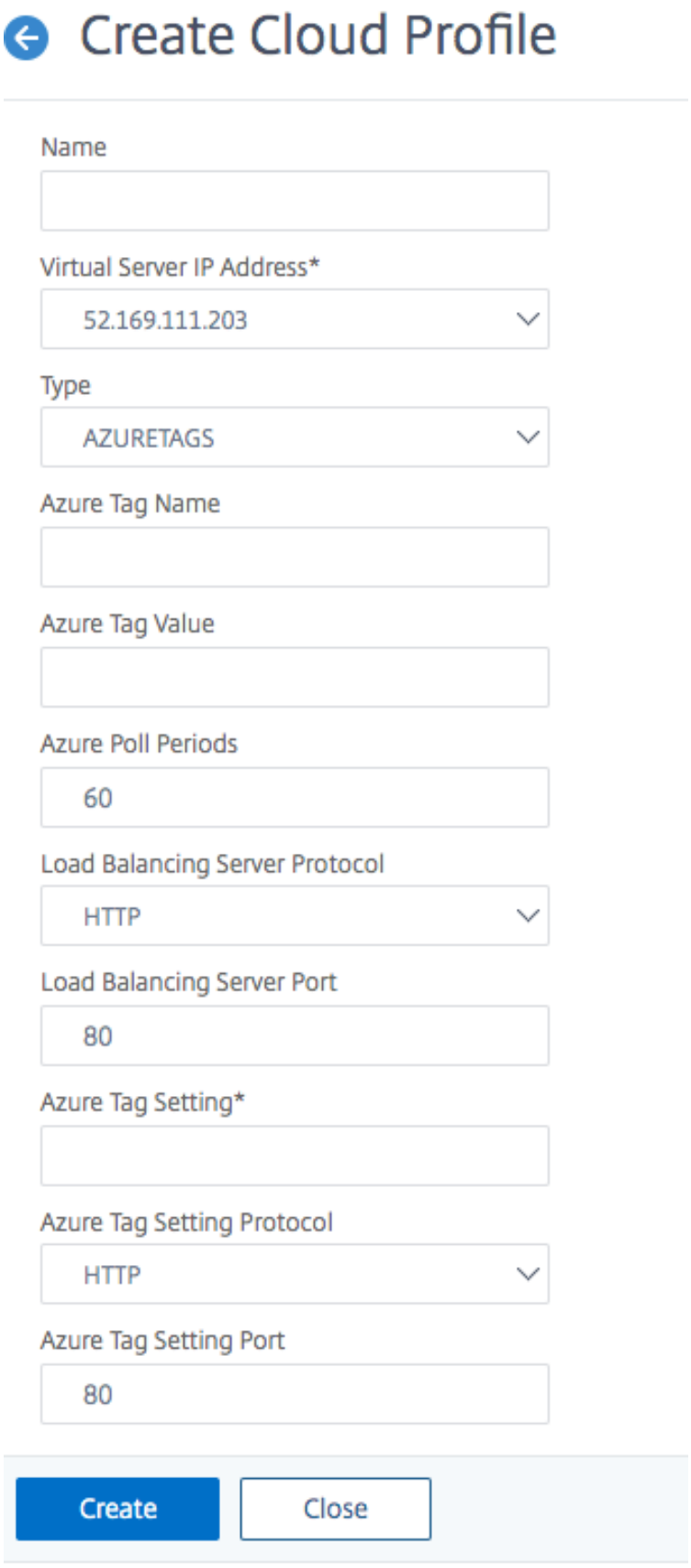
Weitere Informationen zum Hinzufügen von Azure-Tags finden Sie unter Microsoft-Dokument Verwenden Sie Tags zum Organisieren Ihrer Azure-Ressourcen.

> Hinweis
> ADC-CLI-Befehle zum Hinzufügen von Azure-Tag-Einstellungen unterstützen Tagnamen und Tag-Werte, die nur mit Ziffern oder Alphabeten und nicht mit anderen Tastaturzeichen beginnen.

Hinzufügen von Azure-Tag-Einstellungen mithilfe der VPX-GUI

Sie können das Azure-Tag-Cloud-Profil zu einer VPX-Instanz hinzufügen, indem Sie die VPX-GUI verwenden, damit die Instanz den Lastausgleich der Back-End-Server mit dem angegebenen Tag verwenden kann. Führen Sie die folgenden Schritte aus:

1. Gehen Sie auf der VPX-Benutzeroberfläche zu **Konfiguration > Azure > Cloud-Profil**.
2. Klicken Sie auf Hinzufügen, um ein Cloud-Profil zu erstellen. Das Cloud-Profilfenster wird geöffnet.



1. Geben Sie Werte für die folgenden Felder ein:
   - Name: Fügen Sie einen Namen für Ihr Profil hinzu
   - IP-Adresse des virtuellen Servers: Die IP-Adresse des virtuellen Servers wird automatisch von der freien IP-Adresse ausgefüllt, die für die VPX-Instanz verfügbar ist. Weitere Informationen finden Sie unter Zuweisen mehrerer IP-Adressen zu virtuellen Maschinen über das Azure-Portal.
   - Typ: Wählen Sie im Menü AZURETAGS.
   - Azure-Tag-Name: Geben Sie den Namen ein, den Sie den VMs oder NICs im Azure-Portal zugewiesen haben.
   - Azure-Tag-Wert: Geben Sie den Wert ein, den Sie den VMs oder Netzwerkkarten im Azure-Portal zugewiesen haben.
   - Azure-Abfrageperioden: Standardmäßig beträgt der Abfragezeitraum 60 Sekunden. Dies ist der Mindestwert. Sie können es nach Ihren Anforderungen ändern.
   - Load Balancing Server-Protokoll: Wählen Sie das Protokoll aus, das Ihr Load Balancer überwacht.
   - Load Balancing Server Port: Wählen Sie den Port aus, auf den Ihr Load Balancer wartet.
   - Azure-Tag-Einstellung: Der Name der Dienstgruppe, die für dieses Cloud-Profil erstellt wird.
   - Azure-Tag-Einstellprotokoll: Wählen Sie das Protokoll aus, das Ihre Back-End-Server überwachen.
   - Port für die Azure-Tag-Einstellung: Wählen Sie den Port aus, auf den Ihre Back-End-Server warten.
2. Klicken Sie auf **Erstellen**.

Für die getaggten VMs oder Netzwerkkarten werden ein virtueller Lastenausgleichsserver und eine Servicegruppe erstellt. Um den virtuellen Load Balancer anzuzeigen, navigieren Sie über die VPX GUI zu **Verkehrsverwaltung > Lastenausgleich > Virtuelle Server**.

Hinzufügen von Azure-Tag-Einstellungen mithilfe von VPX CLI

Geben Sie den folgenden Befehl in Citrix ADC CLI ein, um ein Cloud-Profil für Azure-Tags zu erstellen.

```
1 add cloud profile `<profile name>` -type azuretags -vServerName `<
    vserver name>` -serviceType HTTP -IPAddress `<vserver IP address>` -
    port 80 -serviceGroupName `<service group name>` -
    boundServiceGroupSvcType HTTP -vsvrbindsvcport 80 -azureTagName `<
    Azure tag specified on Azure portal>` -azureTagValue `<Azure value
    specified on the Azure portal>` -azurePollPeriod 60
2
3 <!--NeedCopy-->
```


> Wichtig
> Sie müssen alle Konfigurationen speichern. Andernfalls gehen die Konfigurationen nach dem Neustart der Instanz verloren. Geben Sie `save config` ein.

Beispiel 1: Hier ist ein Beispielbefehl für ein Cloud-Profil für HTTP-Datenverkehr aller Azure VMs/NICs, die mit dem Paar myTagName/myTagValue gekennzeichnet sind:

```
add cloud profile MyTagCloudProfile -type azuretags -vServerName
    MyTagVServer -serviceType HTTP -IPAddress 40.115.116.57 -port 80 -
    serviceGroupName MyTagsServiceGroup -boundServiceGroupSvcType HTTP -
    vsvrbindsvcport 80 -azureTagName myTagName -azureTagValue myTagValue
     -azurePollPeriod 60
Done
<!--NeedCopy-->
```

Geben Sie ein, um das Cloud-Profil anzuzeigen`show cloudprofile`.

Beispiel 2: Der folgende CLI-Befehl druckt Informationen über das neu hinzugefügte Cloud-Profil in Beispiel 1.

```
show cloudprofile
1)    Name:  MyTagCloudProfile Type:  azuretags         VServerName:
    MyTagVServer ServiceType:  HTTP       IPAddress:  52.178.209.133
    Port:  80               ServiceGroupName:  MyTagsServiceGroup
    BoundServiceGroupSvcType:  HTTP
       Vsvrbindsvcport:  80     AzureTagName:  myTagName AzureTagValue:
           myTagValue AzurePollPeriod:  60     GraceFul:  NO
          Delay:  60
<!--NeedCopy-->
```

Um ein Cloud-Profil zu entfernen, geben Sie rm Cloud-Profil ein `<cloud profile name>`

Beispiel 3: Mit dem folgenden Befehl wird das in Beispiel 1 erstellte Cloud-Profil entfernt.

```
> rm cloudprofile MyTagCloudProfile
  Done
<!--NeedCopy-->
```


Problembehandlung

Problem: In sehr seltenen Fällen kann der CLI-Befehl “rm cloud profile” die Dienstgruppe und Server, die mit dem gelöschten Cloud-Profil verknüpft sind, möglicherweise nicht entfernen. Dies geschieht, wenn der Befehl Sekunden vor Ablauf des Abfragezeitraums des gelöschten Cloud-Profils ausgegeben wird.

Lösung: Löschen Sie die verbleibenden Dienstgruppen manuell, indem Sie für jede der verbleibenden Dienstgruppen den folgenden CLI-Befehl eingeben:

```
#> rm servicegroup <serviceGroupName>

<!--NeedCopy-->
```

Entfernen Sie auch jeden der verbleibenden Server, indem Sie den folgenden CLI-Befehl für jeden der verbleibenden Server eingeben:

```
#> rm server <name>
<!--NeedCopy-->
```

Problem: Wenn Sie einer VPX-Instanz über die Befehlszeilenschnittstelle eine Azure-Tag-Einstellung hinzufügen, wird der rain_tags-Prozess nach einem Warmneustart weiterhin auf einem HA-Paar-Node ausgeführt.

Lösung: Beenden Sie den Prozess auf dem sekundären Knoten nach einem warmen Neustart manuell. Von der CLI des sekundären HA-Knotens beenden Sie die Shell-Eingabeaufforderung

```
#> shell

<!--NeedCopy-->
```

Verwenden Sie den folgenden Befehl, um den rain_tags-Prozess zu beenden:

```
# PID=`ps -aux | grep rain_tags | awk '{
 print $2 }
 '`; kill -9 $PID

<!--NeedCopy-->
```


Problem: Back-End-Server sind möglicherweise nicht erreichbar und werden von der VPX-Instanz als DOWN gemeldet, obwohl sie gesund sind.
Lösung: Stellen Sie sicher, dass die VPX-Instanz die getaggte IP-Adresse erreichen kann, die dem Back-End-Server entspricht. Bei einer getaggten NIC handelt es sich hierbei um die NIC-IP-Adresse. Bei einer getaggten VM handelt es sich dabei um die primäre IP-Adresse der VM. Wenn sich die VM/NIC in einem anderen Azure VNet befindet, stellen Sie sicher, dass VNet-Peering aktiviert ist.

Konfigurieren von GSLB auf Citrix ADC VPX-Instanzen

October 5, 2021

Citrix ADC Appliances, die für den Global Server Load Balancing (GSLB) konfiguriert sind, bieten Disaster Recovery und kontinuierliche Verfügbarkeit von Anwendungen, indem sie vor Fehlerpunkten in einem WAN schützen. GSLB kann die Last über Rechenzentren hinweg ausgleichen, indem sie Kundenanfragen an das nächstgelegene oder leistungsstärkste Rechenzentrum oder an überlebende Rechenzentren bei einem Ausfall weiterleitet.

In diesem Abschnitt wird beschrieben, wie Sie GSLB auf VPX-Instanzen auf zwei Standorten in einer Microsoft Azure-Umgebung mithilfe von Windows PowerShell Befehlen aktivieren.

> **Hinweis:**
>
> Weitere Informationen zu GSLB finden Sie unter Globaler Server-Lastenausgleich.

Sie können GSLB für eine Citrix ADC VPX-Instanz in Azure in zwei Schritten konfigurieren:

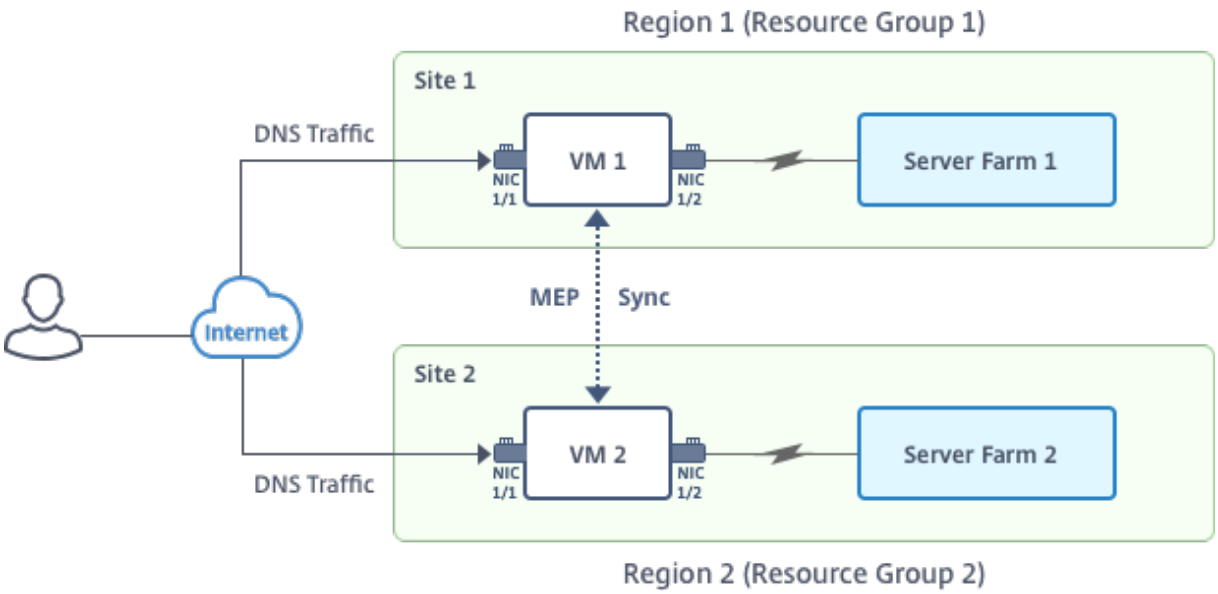
1. Erstellen Sie auf jeder Site eine VPX-Instanz mit mehreren Netzwerkkarten und mehreren IP-Adressen.
2. Aktivieren Sie GSLB für die VPX-Instanzen.

> **Hinweis:**
>
> Weitere Informationen zum Konfigurieren mehrerer Netzwerkkarten und IP-Adressen finden Sie unter: Konfigurieren mehrerer IP-Adressen für eine Citrix ADC VPX-Instanz im Standalone-Modus mithilfe von PowerShell-Befehlen

Szenario

Dieses Szenario umfasst zwei Standorte - Standort 1 und Standort 2. Jeder Standort verfügt über eine VM (VM1 und VM2), die mit mehreren Netzwerkkarten, mehreren IP-Adressen und GSLB konfiguriert ist.

Abbildung. GSLB-Setup implementiert an zwei Standorten - Standort 1 und Standort 2.



In diesem Szenario hat jede VM drei Netzwerkkarten - NIC 0/1, 1/1 und 1/2. Jede Netzwerkkarte kann mehrere private und öffentliche IP-Adressen haben. Die Netzwerkkarten werden für die folgenden Zwecke konfiguriert.

- NIC 0/1: Verwaltung des Datenverkehrs
- NIC 1/1: für den clientseitigen Datenverkehr
- NIC 1/2: Kommunikation mit Back-End-Servern

Informationen zu den IP-Adressen, die in diesem Szenario auf jeder Netzwerkkarte konfiguriert sind, finden Sie im Abschnitt Details zur IP-Konfiguration .

Parameter

Im Folgenden finden Sie Beispielparametereinstellungen für dieses Szenario in diesem Dokument. Sie können verschiedene Einstellungen verwenden, wenn Sie möchten.

```
$location="West Central US"

$vnetName="NSVPX-vnet"

$RGName="multiIP-RG"

$prmStorageAccountName="multiipstorageaccnt"

$avSetName="MultiIP-avset"

$vmSize="Standard_DS3_V2"
```



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

Hinweis: Die Mindestanforderung für eine VPX-Instanz ist 2 vCPUs und 2 GB RAM.

```
$publisher="citrix"

$offer="netscalervpx111"

$sku="netscalerbyol"

$version="latest"

$vmNamePrefix="MultiIPVPX"

$nicNamePrefix="MultiipVPX"

$osDiskSuffix="osdiskdb"

$numberOfVMs=1

$ipAddressPrefix="10.0.0."

$ipAddressPrefix1="10.0.1."

$ipAddressPrefix2="10.0.2."

$pubIPName1="MultiIP-pip1"

$pubIPName2="MultiIP-pip2"

$IpConfigName1="IPConfig1"

$IPConfigName2="IPConfig-2"

$IPConfigName3="IPConfig-3"

$IPConfigName4="IPConfig-4"

$frontendSubnetName="default"

$backendSubnetName1="subnet_1"

$backendSubnetName2="subnet_2"
```



```
40
41 $suffixNumber=10
42 <!--NeedCopy-->
```

Erstellen einer virtuellen Maschine

Führen Sie die Schritte 1 bis 10 aus, um VM1 mit mehreren Netzwerkkarten und mehreren IP-Adressen zu erstellen, indem Sie PowerShell-Befehle verwenden:

1. Ressourcengruppe erstellen
2. Erstellen eines Speicherkontos
3. Verfügbarkeitsset erstellen
4. Virtuelles Netzwerk erstellen
5. Öffentliche IP-Adresse erstellen
6. NICs erstellen
7. VM-Konfigurationsobjekt erstellen
8. Abrufen von Anmeldeinformationen und Festlegen von Betriebssystemeigenschaften für die VM
9. Netzwerkkarten hinzufügen
10. Festlegen des Betriebssystemdatenträgers und Erstellen eines virtuellen Rechners

Nachdem Sie alle Schritte und Befehle zum Erstellen von VM1 abgeschlossen haben, wiederholen Sie diese Schritte, um VM2 mit spezifischen Parametern zu erstellen.

Ressourcengruppe erstellen

```
1 New-AzureRMResourceGroup -Name $RGName -Location $location
2 <!--NeedCopy-->
```

Erstellen eines Speicherkontos

```
1 $prmStorageAccount=New-AzureRMStorageAccount -Name
     $prmStorageAccountName -ResourceGroupName $RGName -Type Standard_LRS
      -Location $location
2 <!--NeedCopy-->
```


Verfügbarkeitsset erstellen

```
$avSet=New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
    $RGName -Location $location
<!--NeedCopy-->
```

Virtuelles Netzwerk erstellen

1. Fügen Sie Subnetze hinzu.

```
$subnet1=New-AzureRmVirtualNetworkSubnetConfig -Name
    $frontendSubnetName -AddressPrefix ”10.0.0.0/24”
$subnet2=New-AzureRmVirtualNetworkSubnetConfig -Name
    $backendSubnetName1 -AddressPrefix ”10.0.1.0/24”
$subnet3=New-AzureRmVirtualNetworkSubnetConfig -Name
    $backendSubnetName2 -AddressPrefix ”10.0.2.0/24”
<!--NeedCopy-->
```

2. Virtuelles Netzwerkobjekt hinzufügen.

```
$vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
     $RGName -Location $location -AddressPrefix 10.0.0.0/16 -Subnet
     $subnet1, $subnet2, $subnet3
<!--NeedCopy-->
```

3. Subnetze abrufen.

```
$frontendSubnet=$vnet.Subnets|?{
 $\_.Name -eq $frontendSubnetName }

$backendSubnet1=$vnet.Subnets|?{
 $\_.Name -eq $backendSubnetName1 }

$backendSubnet2=$vnet.Subnets|?{
 $_.Name -eq $backendSubnetName2 }

<!--NeedCopy-->
```


Öffentliche IP-Adresse erstellen

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
    $RGName -Location $location -AllocationMethod Dynamic
$pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
    $RGName -Location $location -AllocationMethod Dynamic
<!--NeedCopy-->
```

NICs erstellen

NIC 0/1 erstellen

```
$nic1Name=$nicNamePrefix + $suffixNumber + "-Mgmnt"
$ipAddress1=$ipAddressPrefix + $suffixNumber
$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    SubnetId $frontendSubnet.Id -PublicIpAddress $pip1 -PrivateIpAddress
     $ipAddress1 -Primary
$nic1=New-AzureRMNetworkInterface -Name $nic1Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig1
<!--NeedCopy-->
```

NIC 1/1 erstellen

```
$nic2Name $nicNamePrefix + $suffixNumber + "-frontend"
$ipAddress2=$ipAddressPrefix1 + ($suffixNumber)
$ipAddress3=$ipAddressPrefix1 + ($suffixNumber + 1)
$IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -
    PublicIpAddress $pip2 -SubnetId $backendSubnet1.Id  -
    PrivateIpAddress $ipAddress2  -Primary
$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    SubnetId $backendSubnet1.Id  -PrivateIpAddress $ipAddress3
nic2=New-AzureRMNetworkInterface -Name $nic2Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig2, $IpConfig3
<!--NeedCopy-->
```

NIC 1/2 erstellen

```
$nic3Name=$nicNamePrefix + $suffixNumber + "-backend"
$ipAddress4=$ipAddressPrefix2 + ($suffixNumber)
```



```
$IPConfig4=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName4 -
    SubnetId $backendSubnet2.Id -PrivateIpAddress $ipAddress4 -Primary
$nic3=New-AzureRMNetworkInterface -Name $nic3Name -ResourceGroupName
    $RGName -Location $location -IpConfiguration $IpConfig4
<!--NeedCopy-->
```

VM-Konfigurationsobjekt erstellen

```
$vmName=$vmNamePrefix
$vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -
    AvailabilitySetId $avSet.Id
<!--NeedCopy-->
```

Abrufen von Anmeldeinformationen und Festlegen von Betriebssystemeigenschaften

```
$cred=Get-Credential -Message "Type the name and password for VPX login
    ."
$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -
    ComputerName $vmName -Credential $cred
$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName
    $publisher -Offer $offer -Skus $sku -Version $version
<!--NeedCopy-->
```

Netzwerkkarten hinzufügen

```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id -
    Primary
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic2.Id
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic3.Id
<!--NeedCopy-->
```

Festlegen des Betriebssystemdatenträgers und Erstellen eines virtuellen Rechners

```
$osDiskName=$vmName + "-" + $osDiskSuffix
$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString() + "vhds/"
     +$osDiskName + ".vhd"
$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
    $osVhdUri -CreateOption fromImage
```



```
4 Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -
    Name $sku
5 New-AzureRMVM -VM $vmConfig -ResourceGroupName $RGName -Location
    $location
6 <!--NeedCopy-->
```

> **Hinweis:**
>
> Wiederholen Sie die Schritte 1 bis 10, die unter “Erstellen von VMs mit PowerShell-Befehlen erstellen” aufgeführt sind, um VM2 mit Parametern zu erstellen, die für VM2 spezifisch sind.

IP-Konfigurationsdetails

Die folgenden IP-Adressen werden verwendet.

Tabelle 1. In VM1 verwendete IP-Adressen

NIC	Private IP	Öffentliche IP (PIP)	Beschreibung
0/1	10.0.0.10	PIP1	Konfiguriert als NSIP (Management-IP)
1/1	10.0.1.10	PIP2	Konfiguriert als SNIP/GSLB Site IP
-	10.0.1.11	-	Konfiguriert als LB-Server-IP. Öffentliche IP ist nicht obligatorisch
1/2	10.0.2.10	-	Konfiguriert als SNIP für das Senden von Monitorprobes an Dienste; öffentliche IP ist nicht obligatorisch

Tabelle 2. In VM2 verwendete IP-Adressen

NIC	Interne IP	Öffentliche IP (PIP)	Beschreibung
0/1	20.0.0.10	PIP4	Konfiguriert als NSIP (Management-IP)
1/1	20.0.1.10	PIP5	Konfiguriert als SNIP/GSLB Site IP

NIC	Interne IP	Öffentliche IP (PIP)	Beschreibung
-	20.0.1.11	-	Konfiguriert als LB-Server-IP. Öffentliche IP ist nicht obligatorisch
1/2	20.0.2.10	-	Konfiguriert als SNIP für das Senden von Monitorprobes an Dienste; öffentliche IP ist nicht obligatorisch

Hier finden Sie Beispielkonfigurationen für dieses Szenario, die die IP-Adressen und anfänglichen LB-Konfigurationen zeigen, die über die Citrix ADC VPX CLI für VM1 und VM2 erstellt wurden.

Hier ist eine Beispielkonfiguration auf VM1.

```
add ns ip 10.0.1.10 255.255.255.0 -mgmtAccess ENABLED
Add nsip 10.0.2.10 255.255.255.0
add service svc1 10.0.1.10 ADNS 53
add lb vserver v1 HTTP 10.0.1.11 80
add service s1 10.0.2.120 http 80
Add service s2 10.0.2.121 http 80
Bind lb vs v1 s[1-2]
<!--NeedCopy-->
```

Hier ist eine Beispielkonfiguration auf VM2.

```
add ns ip 20.0.1.10 255.255.255.0  -mgmtAccess ENABLED
Add nsip 20.0.2.10 255.255.255.0
add service svc1 20.0.1.10 ADNS 53
add lb vserver v1 HTTP 20.0.1.11 80
Add service s1 20.0.2.90 http 80
Add service s2 20.0.2.91 http 80
Bind lb vs v1 s[1-2]
<!--NeedCopy-->
```


Konfigurieren von GSLB-Sites und anderen Einstellungen

Führen Sie die im folgenden Thema beschriebenen Aufgaben aus, um die beiden GSLB-Sites und andere erforderliche Einstellungen zu konfigurieren:

Globaler Serverlastausgleich

Weitere Informationen finden Sie in diesem Support-Artikel:https://support.citrix.com/article/CTX110348

Hier ist ein Beispiel für eine GSLB-Konfiguration auf VM1 und VM2.

```
enable ns feature LB GSLB
add gslb site site1 10.0.1.10 -publicIP PIP2
add gslb site site2 20.0.1.10 -publicIP PIP5
add gslb service site1_gslb_http_svc1 10.0.1.11 HTTP 80 -publicIP PIP3
    -publicPort 80 -siteName site1
add gslb service site2_gslb_http_svc1 20.0.1.11 HTTP 80 -publicIP PIP6
    -publicPort 80 -siteName site2
add gslb vserver gslb_http_vip1 HTTP
bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1
bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1
bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
<!--NeedCopy-->
```

Sie haben GSLB auf Citrix ADC VPX-Instanzen konfiguriert, die in Azure ausgeführt werden.

Weitere Informationen zum Konfigurieren von GSLB auf Citrix ADC VPX-Instanzen finden Sie im folgenden Bild, um das Video zum Konfigurieren von Citrix ADC GSLB in Microsoft Azure anzuzeigen.

Konfigurieren Sie GSLB in einem aktiven Standby-Hochverfügbarkeits-Setup

June 21, 2022

Sie können den globalen Serverlastenausgleich (GSLB) bei der HA-Bereitstellung im aktiven Standby in Azure in drei Schritten konfigurieren:

1. Erstellen Sie ein VPX HA-Paar auf jeder GSLB-Site. Weitere Informationen zum Erstellen eines HA-Paares finden Sie unter Konfigurieren eines Hochverfügbarkeits-Setups mit mehreren IP-Adressen und NICs .
2. Konfigurieren Sie den Azure Load Balancer (ALB) mit der Front-End-IP-Adresse und -Regeln, um GSLB- und DNS-Datenverkehr zuzulassen.

   Dieser Schritt beinhaltet die folgenden Teilschritte. Das Szenario in diesem Abschnitt enthält die PowerShell-Befehle, die zum Ausführen dieser Teilschritte verwendet werden.

   a. Erstellen Sie ein Front-End-`IPconfig` für die GSLB-Site.

   b. Erstellen Sie einen Back-End-Adresspool mit der IP-Adresse der NIC 1/1 der Knoten in HA.

   c. Erstellen Sie Lastenausgleichsregeln für Folgendes:

   ```
   TCP/3009 - gslb communication
   TCP/3008 - gslb communication
   UDP/53 - DNS communication
   ```

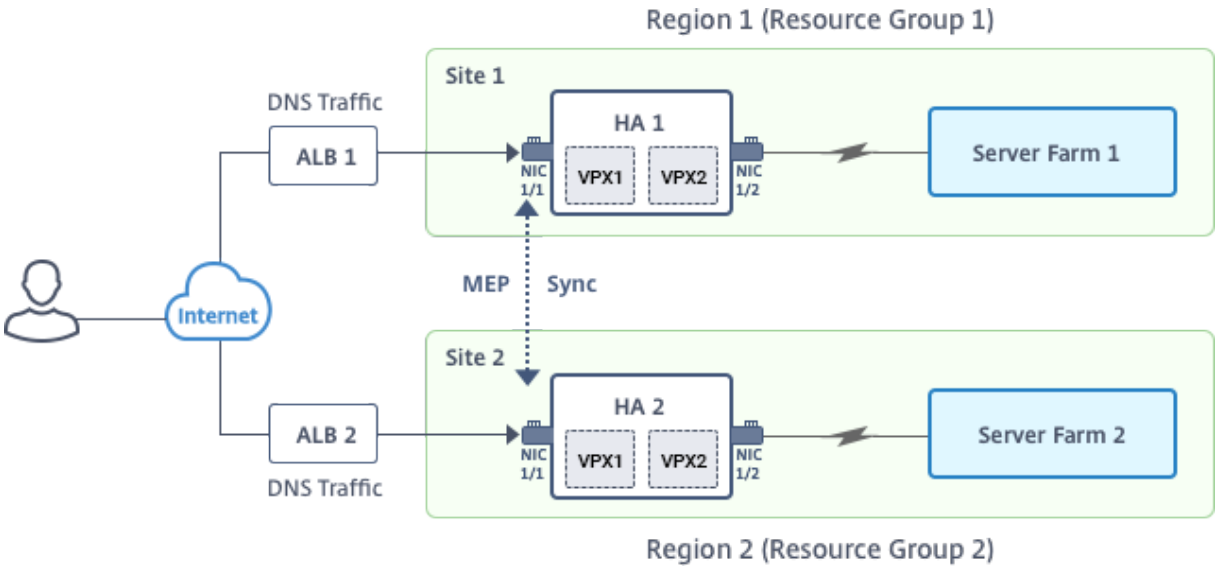
   d. Ordnen Sie den Back-End-Adresspool mit den in Schritt c erstellten LB-Regeln zu.

   e. Aktualisieren Sie die Netzwerksicherheitsgruppe von NIC 1/1 der Knoten in beiden HA-Paaren, um den Datenverkehr für TCP 3008-, TCP 3009- und UDP 53-Ports zuzulassen.
3. Aktivieren Sie GSLB auf jedem HA-Paar.

Szenario

Dieses Szenario umfasst zwei Standorte — Standort 1 und Standort 2. Jeder Standort verfügt über ein HA-Paar (HA1 und HA2), das mit mehreren Netzwerkkarten, mehreren IP-Adressen und GSLB konfiguriert ist.

Abbildung: GLSB auf Active-Standy HA-Bereitstellung in Azure



In diesem Szenario hat jede VM drei Netzwerkkarten - NIC 0/1, 1/1 und 1/2. Die Netzwerkkarten sind für die folgenden Zwecke konfiguriert.

NIC 0/1: zur Bedienung des Management-Datenverkehrs

NIC 1/1: zur Bedienung des clientseitigen Datenverkehrs

NIC 1/2: Kommunikation mit Back-End-Servern

Parameter-Einstellungen

Im Folgenden finden Sie Beispielparametereinstellungen für den ALB. Sie können verschiedene Einstellungen verwenden, wenn Sie möchten.

```
$locName="South east Asia"

$rgName="MulitIP-MultiNIC-RG"

$pubIPName4="PIPFORGSLB1"

$domName4="vpxgslbdns"

$lbName="MultiIPALB"

$frontEndConfigName2="FrontEndIP2"

$backendPoolName1="BackendPoolHttp"

$lbRuleName2="LBRuleGSLB1"
```



```
16
17 $lbRuleName3=”LBRuleGSLB2”
18
19 $lbRuleName4=”LBRuleDNS”
20
21 $healthProbeName=”HealthProbe”
```

Konfiguration von ALB mit der Front-End-IP-Adresse und Regeln, um GSLB- und DNS-Verkehr zuzulassen

Schritt 1. **Erstellen einer öffentlichen IP für GSLB-Site-IP**

```
1 $pip4=New-AzureRmPublicIpAddress -Name $pubIPName4 -ResourceGroupName
     $rgName -DomainNameLabel $domName4 -Location $locName -
     AllocationMethod Dynamic
2
3
4 Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName $rgName | Add-
     AzureRmLoadBalancerFrontendIpConfig -Name $frontEndConfigName2 -
     PublicIpAddress $pip4 | Set-AzureRmLoadBalancer
```

Schritt 2. **Erstellen Sie LB-Regeln und aktualisieren Sie die vorhandene ALB**.

```
1 $alb = get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName $rgName
2
3
4 $frontendipconfig2=Get-AzureRmLoadBalancerFrontendIpConfig -
     LoadBalancer $alb -Name $frontEndConfigName2
5
6
7 $backendPool=Get-AzureRmLoadBalancerBackendAddressPoolConfig -
     LoadBalancer $alb -Name $backendPoolName1
8
9
10 $healthprobe=Get-AzureRmLoadBalancerProbeConfig -LoadBalancer $alb -
     Name $healthProbeName
11
12
13 $alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName2 -
     BackendAddressPool $backendPool -FrontendIPConfiguration
     $frontendipconfig2 -Protocol ”Tcp” -FrontendPort 3009 -BackendPort
```



```
    3009 -Probe $healthprobe -EnableFloatingIP  | Set-
    AzureRmLoadBalancer
14
15
16 $alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName3 -
    BackendAddressPool $backendPool -FrontendIPConfiguration
    $frontendipconfig2 -Protocol "Tcp" -FrontendPort 3008 -BackendPort
    3008 -Probe $healthprobe -EnableFloatingIP  | Set-
    AzureRmLoadBalancer
17
18
19 $alb | Add-AzureRmLoadBalancerRuleConfig -Name $lbRuleName4 -
    BackendAddressPool $backendPool -FrontendIPConfiguration
    $frontendipconfig2 -Protocol "Udp" -FrontendPort 53 -BackendPort 53
    -Probe $healthprobe -EnableFloatingIP  | Set-AzureRmLoadBalancer
```

Aktivieren von GSLB für jedes Hochverfügbarkeitspaar

Jetzt haben Sie zwei Front-End-IP-Adressen für jedes ALB: ALB 1 und ALB 2. Eine IP-Adresse ist für den virtuellen LB-Server und die andere für die GSLB-Site-IP.

HA 1 hat die folgenden Front-End-IP-Adressen:

- FrontEndIPofALB1 (für virtuellen LB-Server)
- PIPFORGSLB1 (GSLB IP)

HA 2 hat die folgenden Front-End-IP-Adressen:

- FrontEndIPofALB2 (für virtuellen LB-Server)
- PIPFORGSLB2 (GSLB IP)

Die folgenden Befehle werden für dieses Szenario verwendet.

```
1  enable ns feature LB GSLB
2
3  add service dnssvc PIPFORGSLB1 ADNS 53
4
5  add gslb site site1 PIPFORGSLB1 -publicIP PIPFORGSLB1
6
7  add gslb site site2 PIPFORGSLB2 -publicIP PIPFORGSLB2
8
9  add gslb service site1_gslb_http_svc1 FrontEndIPofALB1 HTTP 80 -
    publicIP FrontEndIPofALB1 -publicPort 80 -siteName site1
10
```



```
add gslb service site2_gslb_http_svc1 FrontEndIPofALB2 HTTP 80 -
   publicIP FrontEndIPofALB2 -publicPort 80 -siteName site2

add gslb vserver gslb_http_vip1 HTTP

bind gslb vserver gslb_http_vip1 -serviceName site2_gslb_http_svc1

bind gslb vserver gslb_http_vip1 -serviceName site1_gslb_http_svc1

bind gslb vserver gslb_http_vip1 -domainName www.gslbindia.com -TTL 5
```

Verwandte Ressourcen:

Konfigurieren von GSLB auf Citrix ADC VPX-Instanzen

Globaler Serverlastausgleich

Konfigurieren der Intranet-IP für Adresspools für eine Citrix Gateway-App

October 5, 2021

In einigen Situationen benötigen Benutzer, die eine Verbindung mit dem Citrix Gateway -Plug-In herstellen, eine eindeutige IP-Adresse für eine Citrix ADC Gateway-Appliance. Wenn Sie Adresspools (auch als IP-Pooling bezeichnet) für eine Gruppe aktivieren, kann die Citrix Gateway Appliance jedem Benutzer einen eindeutigen IP-Adressenalias zuweisen. Sie konfigurieren Adresspools mithilfe von Intranet-IP (IIP) -Adressen.

Sie können Adresspools auf einer in Azure bereitgestellten Citrix Gateway -Appliance konfigurieren, indem Sie diese zweistufige Vorgehensweise ausführen:

- Registrieren der privaten IP-Adressen, die im Adresspool verwendet werden, in Azure
- Konfigurieren von Adresspools in der Citrix Gateway Appliance

Registrieren einer privaten IP-Adresse im Azure-Portal

In Azure können Sie eine Citrix ADC VPX-Instanz mit mehreren IP-Adressen bereitstellen. Sie können einer VPX-Instanz auf zwei Arten IP-Adressen hinzufügen:

a. Beim Provisioning einer VPX-Instanz

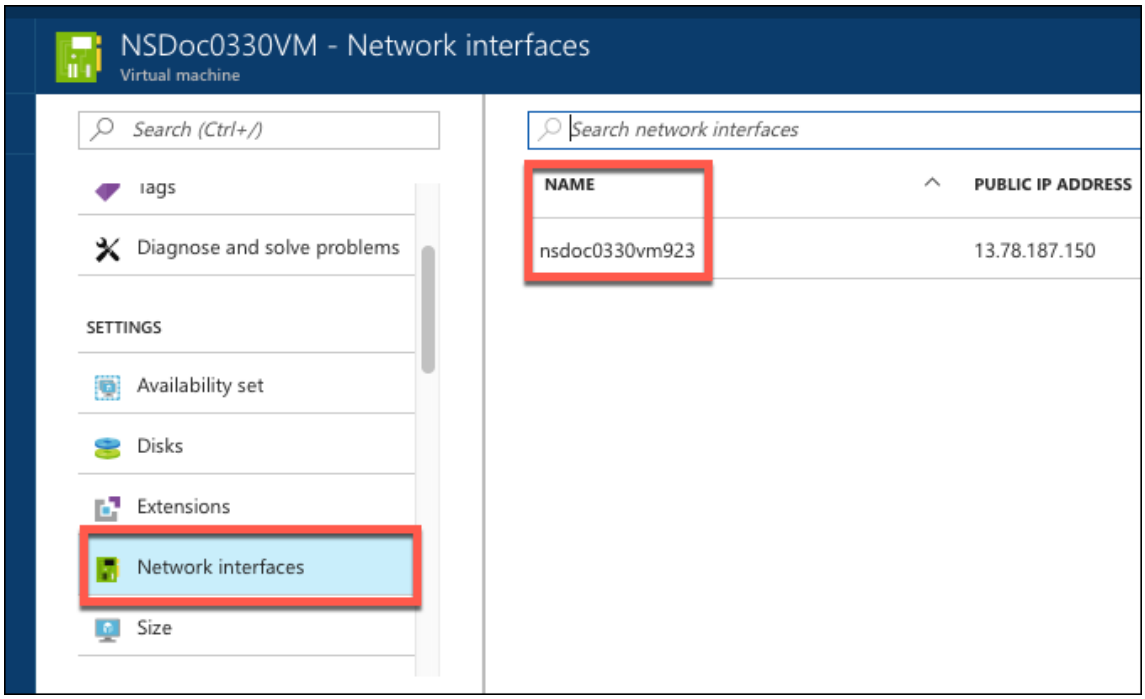
Weitere Informationen zum Hinzufügen mehrerer IP-Adressen während der Bereitstellung einer VPX-Instanz finden Sie unter Konfigurieren mehrerer IP-Adressen für eine eigenständige Citrix ADC-Instanz.

Informationen zum Hinzufügen von IP-Adressen mithilfe von PowerShell-Befehlen während der Bereitstellung einer VPX-Instanz finden Sie unter Konfigurieren mehrerer IP-Adressen für eine Citrix ADC VPX-Instanz im Standalone-Modus mithilfe von PowerShell-Befehlen.

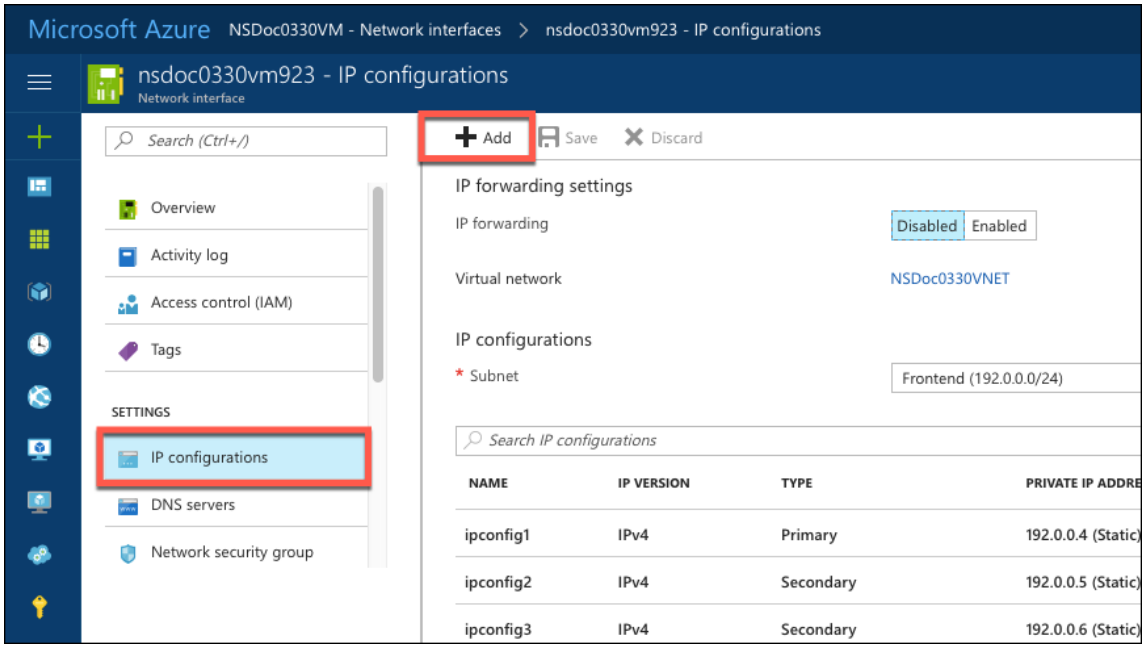
b. Nach der Provisioning einer VPX-Instanz

Nachdem Sie eine VPX-Instanz bereitgestellt haben, führen Sie die folgenden Schritte aus, um eine private IP-Adresse im Azure-Portal zu registrieren, die Sie als Adresspool in der Citrix Gateway Appliance konfigurieren.

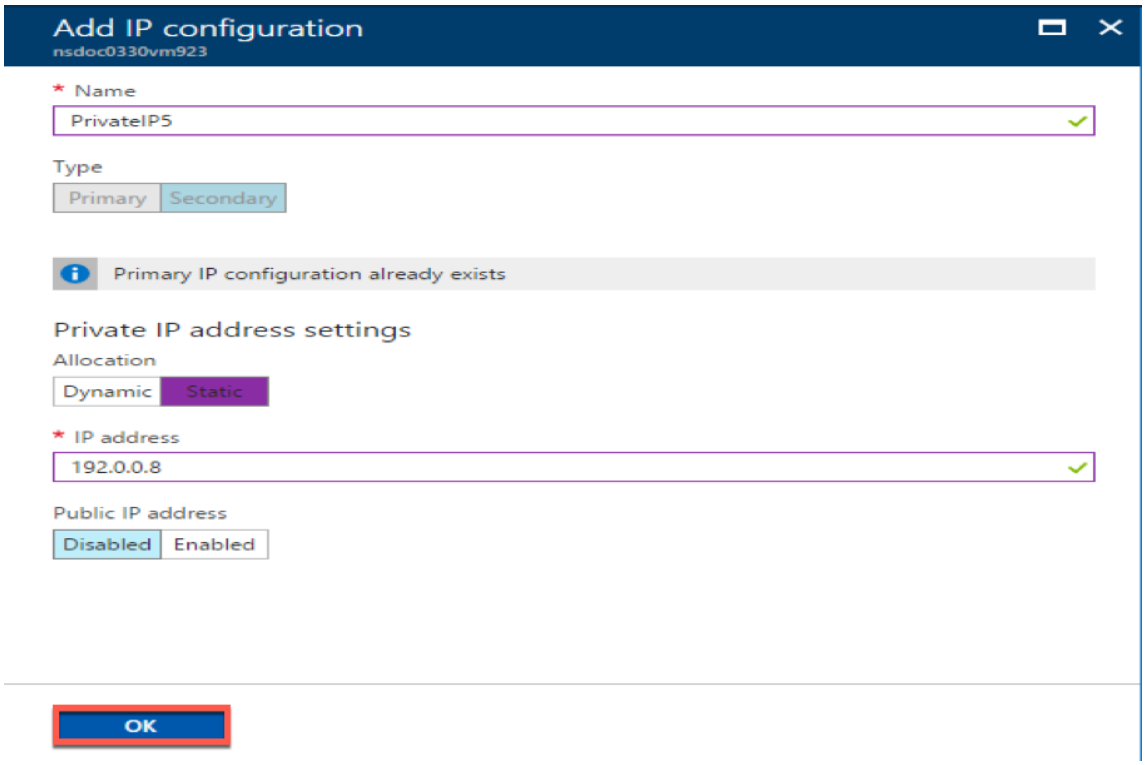
1. Wechseln Sie im Azure Resource Manager (ARM) zur bereits erstellten Citrix ADC VPX-Instanz > **Netzwerkschnittstellen**. Wählen Sie die Netzwerkschnittstelle, die an ein Subnetz gebunden ist, zu dem das IIP gehört, das Sie registrieren möchten.



2. Klicken Sie auf **IP-Konfigurationen**, und klicken Sie dann auf **Hinzufügen**.



3. Geben Sie die erforderlichen Details ein, wie im folgenden Beispiel gezeigt, und klicken Sie auf **OK**.



Konfigurieren von Adresspools in der Citrix Gateway Appliance

Weitere Informationen zum Konfigurieren von Adresspools auf dem Citrix Gateway finden Sie unter Konfigurieren von Adresspools.

Einschränkung: Sie können eine Reihe von IIP-Adressen nicht an Benutzer binden. Jede IIP-Adresse, die in einem Adresspool verwendet wird, muss registriert sein.

Konfigurieren Sie mehrere IP-Adressen für eine eigenständige Citrix ADC VPX-Instanz mithilfe von PowerShell-Befehlen

October 5, 2021

In einer Azure-Umgebung kann eine virtuelle Citrix ADC VPX Appliance mit mehreren Netzwerkkarten bereitgestellt werden. Jede Netzwerkkarte kann mehrere IP-Adressen haben. In diesem Abschnitt wird beschrieben, wie Sie eine Citrix ADC VPX-Instanz mit einer einzelnen Netzwerkkarte und mehreren IP-Adressen mithilfe von PowerShell-Befehlen bereitstellen. Sie können dasselbe Skript für die Multi-NIC- und Multi-IP-Bereitstellung verwenden.

> **Hinweis:**
>
> In diesem Dokument bezieht sich IP-Config auf ein Paar von IP-Adressen, öffentliche IP und private IP, die mit einer einzelnen Netzwerkkarte verknüpft sind. Weitere Informationen finden Sie im Abschnitt Azure-Terminologie .

Anwendungsfall

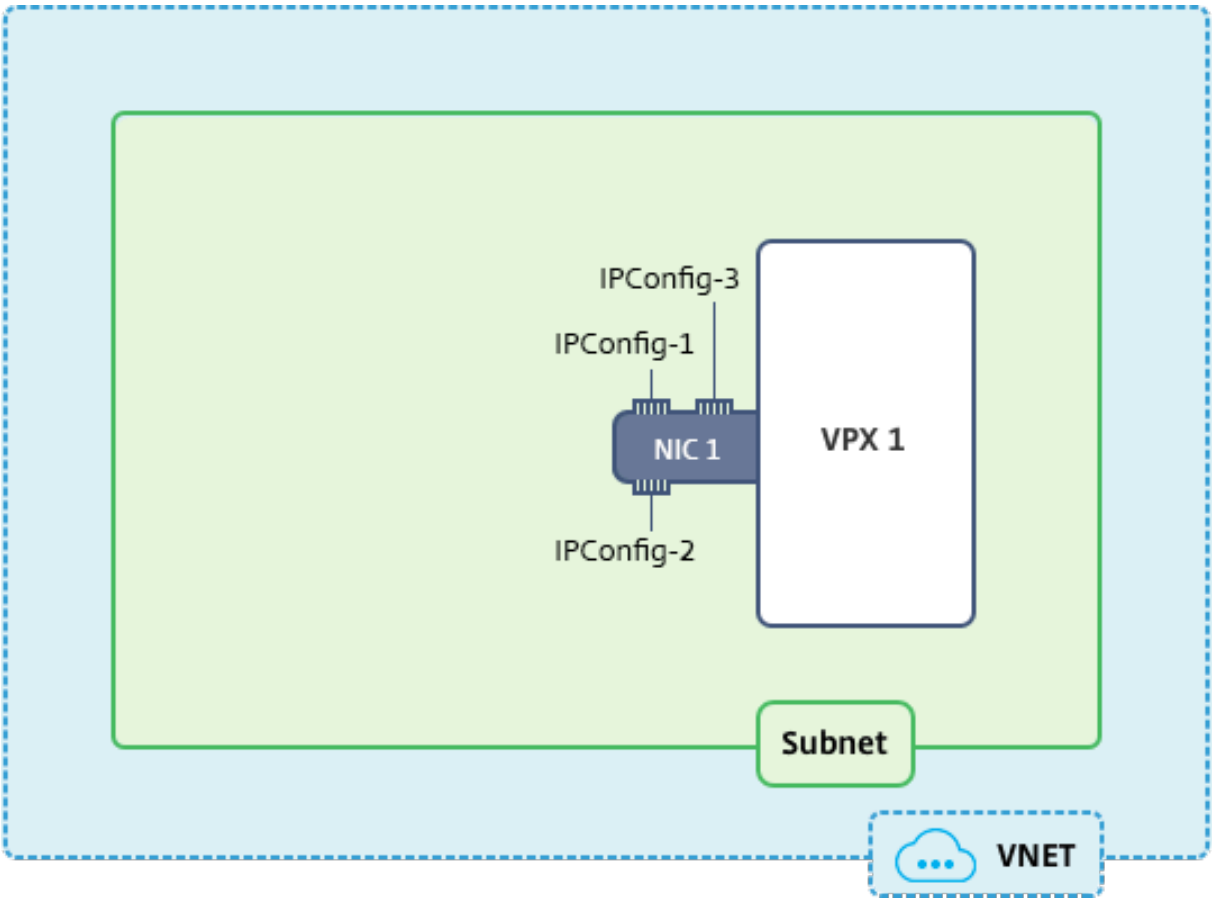
In diesem Anwendungsfall ist eine einzelne Netzwerkkarte mit einem virtuellen Netzwerk (VNET) verbunden. Die Netzwerkkarte ist drei IP-Konfigurationen zugeordnet, wie in der folgenden Tabelle dargestellt.

IP-Konfiguration	Verbunden mit
IPConfig-1	Statische öffentliche IP-Adresse; statische private IP-Adresse
IPConfig-2	Statische öffentliche IP-Adresse; statische Privatadresse
IPConfig-3	Statische private IP-Adresse

> **Hinweis:**
>
> ipConfig-3 ist mit keiner öffentlichen IP-Adresse verknüpft.

Diagramm: Topologie

Hier ist die visuelle Darstellung des Anwendungsfalls.



> **Hinweis:**
>
> In einer Multi-Nic, Multi-IP Azure Citrix ADC VPX-Bereitstellung wird die private IP-Adresse, die mit der primären (ersten) `IPConfig` der primären (ersten) Netzwerkkarte verknüpft ist, automatisch als Verwaltungs-NSIP-Adresse der Appliance hinzugefügt. Die verbleibenden privaten IP-Adressen, die mit verknüpft sind, `IPConfigs` müssen in der VPX-Instanz als VIPs oder SNIPs mit dem `add ns ip` Befehl hinzugefügt werden, wie von Ihren Anforderungen festgelegt.

Im Folgenden finden Sie die Schritte, die zum Konfigurieren mehrerer IP-Adressen für eine virtuelle Citrix ADC VPX Appliance im Standalone-Modus erforderlich sind:

1. Ressourcengruppe erstellen
2. Speicherkonto erstellen
3. Verfügbarkeitsset erstellen
4. Netzwerkdienstgruppe erstellen

5. Virtuelles Netzwerk erstellen
6. Öffentliche IP-Adresse erstellen
7. IP-Konfiguration zuweisen
8. Netzwerkkarte erstellen
9. Erstellen Sie Citrix ADC VPX-Instanz
10. NIC-Konfigurationen überprüfen
11. VPX-seitige Konfigurationen überprüfen

Skript

Parameter

Im Folgenden finden Sie Beispielparametereinstellungen für den Anwendungsfall in diesem Dokument. Sie können verschiedene Einstellungen verwenden, wenn Sie möchten.

$locName=”westcentralus”

$rgName=”Azure-MultiIP”

$nicName1=”VM1-NIC1”

$vNetName=”Azure-MultiIP-vnet”

$vNetAddressRange=”11.6.0.0/16”

$frontEndSubnetName=”frontEndSubnet”

$frontEndSubnetRange=”11.6.1.0/24”

$prmStorageAccountName=”multiipstorage”

$avSetName=”multiip-avSet”

$vmSize=”Standard_DS4_v2” (Dieser Parameter erstellt eine VM mit bis zu vier NICs.)

Hinweis: Die Mindestanforderung für eine VPX-Instanz ist 2 vCPUs und 2 GB RAM.

$Publisher = “Citrix”

$offer=”netscalervpx110-6531” (Sie können andere Angebote verwenden.)

$sku=”netscalerbyol” (Je nach Ihrem Angebot kann die SKU unterschiedlich sein.)

$version=”latest”

$pubIPName1=”PIP1”

$pubIPName2=”PIP2”

$domName1=”multiipvpx1”

$domName2=”multiipvpx2”

$vmNamePrefix=”VPXMultiIP”

$osDiskSuffix=”osmultiipalbdiskdb1”

Informationen zur Netzwerksicherheitsgruppe (NSG):

$nsgName=”NSG-MultiIP”

$rule1Name=”Inbound-HTTP”

$rule2Name=”Inbound-HTTPS”

$rule3Name=”Inbound-SSH”

$IpConfigName1=”IPConfig1”

$IPConfigName2=”IPConfig-2”

$IPConfigName3=”IPConfig-3”

1. Ressourcengruppe erstellen

```
New-AzureRmResourceGroup -Name $rgName -Location $locName
```

2. Speicherkonto erstellen

```
$prmStorageAccount = New-AzureRMStorageAccount -Name $prmStorageAccountName
 -ResourceGroupName $rgName -Type Standard_LRS -Location $locName
```

3. Verfügbarkeitsset erstellen

```
$avSet = New-AzureRMAvailabilitySet -Name $avSetName -ResourceGroupName
$rgName -Location $locName
```

4. Netzwerksicherheitsgruppe erstellen

1. Fügen Sie Regeln hinzu. Sie müssen der Netzwerksicherheitsgruppe eine Regel für jeden Port hinzufügen, der Datenverkehr bedient.

   ```
   $rule1=New-AzureRmNetworkSecurityRuleConfig -Name $rule1Name -Description
    ”Allow HTTP”-Access Allow -Protocol Tcp -Direction Inbound -Priority
   101 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
    * -DestinationPortRange 80
   $rule2=New-AzureRmNetworkSecurityRuleConfig -Name $rule2Name -Description
    ”Allow HTTPS”-Access Allow -Protocol Tcp -Direction Inbound -Priority
   110 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
    * -DestinationPortRange 443
   ```



```
$rule3=New-AzureRmNetworkSecurityRuleConfig -Name $rule3Name -Description
 "Allow SSH"-Access Allow -Protocol Tcp -Direction Inbound -Priority
120 -SourceAddressPrefix Internet -SourcePortRange * -DestinationAddressPrefix
 * -DestinationPortRange 22
```

2. Erstellen Sie ein Netzwerksicherheitsgruppenobjekt.

```
$nsg=New-AzureRmNetworkSecurityGroup -ResourceGroupName $rgName -
Location $locName -Name $nsgName -SecurityRules $rule1,$rule2,$rule3
```

5. Virtuelles Netzwerk erstellen

1. Fügen Sie Subnetze hinzu.

```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name $frontEndSubnetName
 -AddressPrefix $frontEndSubnetRange
```

2. Fügen Sie ein virtuelles Netzwerkobjekt hinzu.

```
$vnet=New-AzureRmVirtualNetwork -Name $vNetName -ResourceGroupName
$rgName -Location $locName -AddressPrefix $vNetAddressRange -Subnet
$frontendSubnet
```

3. Rufen Sie Subnetze ab.

```
$subnetName="frontEndSubnet"
$subnet1=$vnet.Subnets|?{ $_.Name -eq $subnetName }
```

6. Öffentliche IP-Adresse erstellen

```
$pip1=New-AzureRmPublicIpAddress -Name $pubIPName1 -ResourceGroupName
$rgName -DomainNameLabel $domName1 -Location $locName -AllocationMethod
Static
$pip2=New-AzureRmPublicIpAddress -Name $pubIPName2 -ResourceGroupName
$rgName -DomainNameLabel $domName2 -Location $locName -AllocationMethod
Static
```

> **Hinweis:**
>
> Prüfen Sie vor der Verwendung die Verfügbarkeit von Domainnamen.
>
> Die Zuordnungsmethode für IP-Adressen kann dynamisch oder statisch sein.

7. IP-Konfiguration zuweisen

Berücksichtigen Sie in diesem Anwendungsfall die folgenden Punkte, bevor Sie IP-Adressen zuweisen:

- ipConfig-1 gehört zum Subnetz1 von VPX1.
- ipConfig-2 gehört zum Subnetz 1 von VPX1.
- ipConfig-3 gehört zum Subnetz 1 von VPX1.

> **Hinweis:**
>
> Wenn Sie einer NIC mehrere IP-Konfigurationen zuweisen, muss eine Konfiguration als primäre zugewiesen werden.

```
$IPAddress1=”11.6.1.27”
$IPConfig1=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName1 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress1 -PublicIpAddress $pip1
     -Primary
$IPAddress2=”11.6.1.28”
$IPConfig2=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName2 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress2 -PublicIpAddress $pip2
$IPAddress3=”11.6.1.29”
$IPConfig3=New-AzureRmNetworkInterfaceIpConfig -Name $IPConfigName3 -
    Subnet $subnet1 -PrivateIpAddress $IPAddress3 -Primary
```

Verwenden Sie eine gültige IP-Adresse, die Ihren Subnetzanforderungen entspricht, und überprüfen Sie deren Verfügbarkeit.

8. Netzwerkkarte erstellen

```
$nic1=New-AzureRmNetworkInterface -Name $nicName1 -ResourceGroupName
$rgName -Location $locName -IpConfiguration $IpConfig1,$IpConfig2,$IPConfig3
 -NetworkSecurityGroupId $nsg.Id
```

9. Erstellen Sie Citrix ADC VPX-Instanz

1. Initialisieren Sie Variablen.

   ```
   $suffixNumber = 1
   $vmName = $vmNamePrefix + $suffixNumber
   ```

2. Erstellen Sie ein VM-Konfigurationsobjekt.

   ```
   $vmConfig=New-AzureRMVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId
    $avSet.Id
   ```

3. Legen Sie Anmeldeinformationen, Betriebssystem und Image fest.

   ```
   $cred=Get-Credential -Message ”Type the name and password for VPX login
   .”
   ```



```
$vmConfig=Set-AzureRMVMOperatingSystem -VM $vmConfig -Linux -ComputerName
 $vmName -Credential $cred
$vmConfig=Set-AzureRMVMSourceImage -VM $vmConfig -PublisherName $publisher
 -Offer $offer -Skus $sku -Version $version
```

4. Fügen Sie NIC hinzu.

```
$vmConfig=Add-AzureRMVMNetworkInterface -VM $vmConfig -Id $nic1.Id -
Primary
```

> **Hinweis:**
>
> In einer VPX-Bereitstellung mit mehreren Nic muss eine NIC primär sein. Daher muss "-Primary" angehängt werden, während diese NIC zur VPX-Instanz hinzugefügt wird.

5. Geben Sie den Betriebssystemdatenträger an und erstellen Sie VM.

```
$osDiskName=$vmName + "-"+ $osDiskSuffix1
$osVhdUri=$prmStorageAccount.PrimaryEndpoints.Blob.ToString()+ "vhds/"+
 $osDiskName + ".vhd"
$vmConfig=Set-AzureRMVMOSDisk -VM $vmConfig -Name $osDiskName -VhdUri
$osVhdUri -CreateOption fromImage
Set-AzureRmVMPlan -VM $vmConfig -Publisher $publisher -Product $offer -
Name $sku
New-AzureRMVM -VM $vmConfig -ResourceGroupName $rgName -Location
$locName
```

10. NIC-Konfigurationen überprüfen

Nachdem die VPX-Instanz gestartet wurde, können Sie die IP-Adressen, die `IPConfigs` der VPX-NIC zugewiesen sind, mit dem folgenden Befehl überprüfen.

```
$nic.IPConfig
```

11. VPX-seitige Konfigurationen überprüfen

Wenn die Citrix ADC VPX-Instanz gestartet wird, wird eine private IP-Adresse, die mit `IPconfig` der primären Netzwerkkarte verknüpft ist, als NSIP-Adresse hinzugefügt. Die verbleibenden privaten IP-Adressen müssen gemäß Ihren Anforderungen als VIP- oder SNIP-Adressen hinzugefügt werden. Verwenden Sie den folgenden Befehl.

```
add nsip <Private IPAddress><netmask> -type VIP/SNIP
```

Sie haben jetzt mehrere IP-Adressen für eine Citrix ADC VPX-Instanz im Standalone-Modus konfiguriert.

Zusätzliche PowerShell -Skripts für die Azure-Bereitstellung

October 8, 2021

Dieser Abschnitt enthält die PowerShell Cmdlets, mit denen Sie die folgenden Konfigurationen in Azure PowerShell ausführen können:

- Bereitstellen einer eigenständigen Citrix ADC VPX-Instanz
- Bereitstellen eines Citrix ADC VPX -Paars in einer Hochverfügbarkeit-Setup mit einem externen Azure-Load Balancer
- Bereitstellen eines Citrix ADC VPX Paares in einem Hochverfügbarkeitssetup mit dem internen Azure-Load Balancer

Weitere Informationen zu Konfigurationen, die Sie mithilfe von PowerShell Befehlen ausführen können, finden Sie in den folgenden Themen:

- Konfigurieren eines Hochverfügbarkeitssetups mit mehreren IP-Adressen und Netzwerkkarten über PowerShell-Befehle
- Konfigurieren von GSLB auf Citrix ADC VPX-Instanzen
- Konfigurieren von GSLB auf einem NetScaler Active-Standby Hochverfügbarkeitssetup
- Konfigurieren mehrerer IP-Adressen für eine Citrix ADC VPX-Instanz im Standalone-Modus über PowerShell-Befehle
- Konfigurieren mehrerer Azure-VIPs für eine eigenständige VPX-Instanz

Bereitstellen einer eigenständigen Citrix ADC VPX-Instanz

1. **Erstellen einer Ressourcengruppe**

   Die Ressourcengruppe kann alle Ressourcen für die Lösung oder nur die Ressourcen enthalten, die Sie als Gruppe verwalten möchten. Der hier angegebene Speicherort ist der Standardspeicherort für Ressourcen in dieser Ressourcengruppe. Stellen Sie sicher, dass alle Befehle zum Erstellen eines Load Balancer dieselbe Ressourcengruppe verwenden.

   ```
   $rgName=”<resource group name>”
   $locName=”<location name, such as West US>
   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

   Zum Beispiel:

   ```
   $rgName = ”ARM-VPX”
   $locName = ”West US”
   New-AzureRmResourceGroup -Name $rgName -Location $locName
   <!--NeedCopy-->
   ```


2. **Speicherkonto erstellen**

   Wählen Sie einen eindeutigen Namen für Ihr Speicherkonto, der nur Kleinbuchstaben und Zahlen enthält.

   ```
   $saName="<storage account name>"
   $saType="<storage account type>", geben Sie eines an: Standard_LRS, Standard_GRS
   , Standard_RAGRS oder Premium_LRS
   New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -
   Type $saType -Location $locName
   ```

   Zum Beispiel:

   ```
   1 $saName="vpxstorage"
   2 $saType="Standard_LRS"
   3 New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
         -Type $saType -Location $locName
   4 <!--NeedCopy-->
   ```

3. **Erstellen eines Verfügbarkeitssatzes**

   Verfügbarkeitssatz hilft, Ihre virtuellen Maschinen während Ausfallzeiten verfügbar zu halten, z. B. während der Wartung. Ein Load Balancer, der mit einem Verfügbarkeitssatz konfiguriert ist, stellt sicher, dass Ihre Anwendung immer verfügbar ist.

   ```
   $avName="<availability set name>"

   New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -
   Location $locName
   ```

4. **Erstellen eines virtuellen Netzwerks**

   Fügen Sie ein neues virtuelles Netzwerk mit mindestens einem Subnetz hinzu, wenn das Subnetz vorher nicht erstellt wurde.

   ```
   $FrontendAddressPrefix="10.0.1.0/24"
   $BackendAddressPrefix="10.0.2.0/24"
   $vnetAddressPrefix="10.0.0.0/16"
   $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name frontendSubnet
    -AddressPrefix $FrontendAddressPrefix
   $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name backendSubnet
    -AddressPrefix $BackendAddressPrefix
   New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName $rgName -
   Location $locName -AddressPrefix $vnetAddressPrefix -Subnet $frontendSubnet
   ,$backendSubnet
   ```


Zum Beispiel:

```
$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    frontendSubnet -AddressPrefix $FrontendAddressPrefix

$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    backendSubnet -AddressPrefix $BackendAddressPrefix

New-AzureRmVirtualNetwork -Name TestNet -ResourceGroupName $rgName
     -Location $locName -AddressPrefix $vnetAddressPrefix -Subnet
    $frontendSubnet,$backendSubnet
<!--NeedCopy-->
```

5. **Erstellen einer Netzwerkkarte**

   Erstellen Sie eine Netzwerkkarte, und ordnen Sie die Netzwerkkarte der Citrix ADC VPX-Instanz zu. Das in der obigen Prozedur erstellte Front-End-Subnetz wird bei 0 indiziert und das Back-End-Subnetz wird bei 1 indiziert. Erstellen Sie nun NIC auf eine der drei folgenden Arten:

   a) *NIC mit öffentlicher IP-Adresse*

   ```
   $nicName="<name of the NIC of the VM>"

   $pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
   $rgName -Location $locName -AllocationMethod Dynamic

   $nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
   $rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -
   PublicIpAddressId $pip.Id
   ```

   b) *NIC mit öffentlicher IP und DNS Label*

   ```
   $nicName="<name of the NIC of the VM>"

   $domName="<domain name label>"

   $pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
   $rgName -DomainNameLabel $domName -Location $locName -AllocationMethod
   Dynamic
   ```

   Bevor Sie $domName zuweisen, überprüfen Sie, ob es verfügbar ist oder nicht, indem Sie den Befehl verwenden:

   ```
   Test-AzureRmDnsAvailability -DomainQualifiedName $domName -Location
   $locName
   ```



```
$nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
$rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -
PublicIpAddressId $pip.Id
```

Zum Beispiel:

```
$nicName="frontendNIC"

$domName="vpxazure"

$pip = New-AzureRmPublicIpAddress -Name $nicName -
    ResourceGroupName $rgName -DomainNameLabel $domName -Location
    $locName -AllocationMethod Dynamic

$nic = New-AzureRmNetworkInterface -Name $nicName -
    ResourceGroupName $rgName -Location $locName -SubnetId $vnet.
    Subnets[0].Id -PublicIpAddressId $pip.Id
<!--NeedCopy-->
```

c) *NIC mit dynamischer öffentlicher Adresse und statischer privater IP-Adresse*

Stellen Sie sicher, dass die private (statische) IP-Adresse, die Sie der VM hinzufügen, den gleichen Bereich haben muss wie die des angegebenen Subnetzes.

```
$nicName="<name of the NIC of the VM>"

$staticIP="<available static IP address on the subnet>"

$pip = New-AzureRmPublicIpAddress -Name $nicName -ResourceGroupName
$rgName -Location $locName -AllocationMethod Dynamic

$nic = New-AzureRmNetworkInterface -Name $nicName -ResourceGroupName
$rgName -Location $locName -SubnetId $vnet.Subnets[$subnetIndex].Id -
PublicIpAddressId $pip.Id -PrivateIpAddress $staticIP
```

6. **Erstellen eines virtuellen Objekts**

```
$vmName="<VM name>"

$vmSize="<VM size string>"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
$rgName

$vm=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -AvailabilitySetId
 $avset.Id
```


7. **Abrufen des Citrix ADC VPX Images**

   ```
   $pubName="<Image publisher name>"
   ```

   ```
   $offerName="<Image offer name>"
   ```

   ```
   $skuName="<Image SKU name>"
   ```

   ```
   $cred=Get-Credential -Message "Type the name and password of the local administrator account."
   ```

   Geben Sie Ihre Anmeldeinformationen an, die für die Anmeldung bei VPX verwendet werden

   ```
   $vm=Set-AzureRmVMOperatingSystem -VM $vm -Linux -ComputerName $vmName -Credential $cred -Verbose
   ```

   ```
   $vm=Set-AzureRmVMSourceImage -VM $vm -PublisherName $pubName -Offer $offerName -Skus $skuName -Version "latest"
   ```

   ```
   $vm=Add-AzureRmVMNetworkInterface -VM $vm -Id $nic.Id
   ```

   Zum Beispiel:

   ```
   $pubName="citrix"
   ```

   Mit dem folgenden Befehl werden alle Angebote von Citrix angezeigt:

   ```
   1 Get-AzureRMVMImageOffer -Location $locName -Publisher $pubName |
       Select Offer
   2
   3 $offerName="netscalervpx110-6531"
   4 <!--NeedCopy-->
   ```

   Der folgende Befehl wird verwendet, um die vom Herausgeber angebotene SKU für einen bestimmten Angebotsnamen zu kennen:

   ```
   Get-AzureRMVMImageSku -Location $locName -Publisher $pubName -Offer $offerName | Select Skus
   ```

8. **Erstellen einer virtuellen Maschine**

   ```
   $diskName="<name identifier for the disk in Azure storage, such as OSDisk>"
   ```

   Zum Beispiel:

   ```
   1 $diskName="dynamic"
   2
   ```



```
3 $pubName="citrix"
4
5 $offerName="netscalervpx110-6531"
6
7 $skuName="netscalerbyol"
8
9 $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
    Name $saName
10
11 $osDiskUri=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds/"
    + $diskName  + ".vhd"
12
13 $vm=Set-AzureRmVMOSDisk -VM $vm -Name $diskName -VhdUri $osDiskUri
     -CreateOption fromImage
14 <!--NeedCopy-->
```

Wenn Sie VM aus Images erstellen, die auf Marketplace-Site vorhanden sind, verwenden Sie den folgenden Befehl, um den VM-Plan anzugeben:

```
Set-AzureRmVMPlan -VM $vm -Publisher $pubName -Product $offerName -Name
 $skuName
```

```
New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM $vm
```

Bereitstellen eines Citrix ADC VPX -Paars in einer Hochverfügbarkeit-Setup mit einem externen Azure-Load Balancer

Melden Sie sich mit Ihren Azure-Benutzeranmeldeinformationen bei AzureRmAccount an.

1. **Erstellen einer Ressourcengruppe**

   Der hier angegebene Speicherort ist der Standardspeicherort für Ressourcen in dieser Ressourcengruppe. Stellen Sie sicher, dass alle Befehle, die zum Erstellen eines Load Balancer verwendet werden, dieselbe Ressourcengruppe verwenden.

   ```
   $rgName="<resource group name>"
   ```

   ```
   $locName="<location name, such as West US>"
   ```

   ```
   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

   Zum Beispiel:

```
1 $rgName = "ARM-LB-NS"
2
3 $locName = "West US"
```



```
4
5 New-AzureRmResourceGroup -Name $rgName -Location $locName
6 <!--NeedCopy-->
```

2. **Speicherkonto erstellen**

   Wählen Sie einen eindeutigen Namen für Ihr Speicherkonto, der nur Kleinbuchstaben und Zahlen enthält.

   `$saName="<storage account name>"`

   `$saType="<storage account type>"`, geben Sie eines an: `Standard_LRS`, `Standard_GRS`, `Standard_RAGRS` oder `Premium_LRS`

   `New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -Type $saType -Location $locName`

   Zum Beispiel:

```
1 $saName="vpxstorage"
2
3 $saType="Standard_LRS"
4
5 New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
      -Type $saType -Location $locName
6 <!--NeedCopy-->
```

3. **Erstellen eines Verfügbarkeitssatzes**

   Ein Load Balancer, der mit einem Verfügbarkeitssatz konfiguriert ist, stellt sicher, dass Ihre Anwendung immer verfügbar ist.

   `$avName="<availability set name>"`

   `New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -Location $locName`

4. **Erstellen eines virtuellen Netzwerks**

   Fügen Sie ein neues virtuelles Netzwerk mit mindestens einem Subnetz hinzu, wenn das Subnetz vorher nicht erstellt wurde.

```
1 $vnetName = "LBVnet"
2
3 $FrontendAddressPrefix="10.0.1.0/24"
4
```



```
5 $BackendAddressPrefix=”10.0.2.0/24”
6
7 $vnetAddressPrefix=”10.0.0.0/16”
8
9 $frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    frontendSubnet -AddressPrefix $FrontendAddressPrefix
10
11 $backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    backendSubnet -AddressPrefix $BackendAddressPrefix
12
13 $vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
     $rgName -Location $locName -AddressPrefix $vnetAddressPrefix -
    Subnet $frontendSubnet,$backendSubnet
14 <!--NeedCopy-->
```

Hinweis: Wählen Sie den AddressPrefix-Parameterwert gemäß Ihrer Anforderung.

Weisen Sie dem virtuellen Netzwerk, das Sie zuvor in diesem Schritt erstellt haben, Front-End- und Back-End-Subnetz zu.

Wenn das Front-End-Subnetz das erste Element von Array VNet ist, muss subnetId $vNet.Subnets [0] .Id sein.

Wenn das Front-End-Subnetz das zweite Element im Array ist, muss die subnetID $vNet.Subnets [1] .Id und so weiter sein.

5. **Konfigurieren der Front-End-IP-Adresse und Erstellen eines Back-End-Adress-Pools**

   Konfigurieren Sie eine Front-End-IP-Adresse für den eingehenden Load Balancer Netzwerkverkehr und erstellen Sie einen Back-End-Adresspool, um den Lastausgleichsverkehr zu empfangen.

```
1 $pubName=”PublicIp1”
2
3 $publicIP1 = New-AzureRmPublicIpAddress -Name $pubName -
    ResourceGroupName $rgName -Location $locName -AllocationMethod
    Static -DomainNameLabel nsvpx
4 <!--NeedCopy-->
```

Hinweis: Überprüfen Sie, ob der Wert für DomainNameLabel verfügbar ist.

```
1 $FIPName = ”ELBFIP”
2
```



```
3 $frontendIP1 = New-AzureRmLoadBalancerFrontendIpConfig -Name
    $FIPName -PublicIpAddress $publicIP1
4
5 $BEPool = "LB-backend-Pool"
6
7 $beaddresspool1= New-AzureRmLoadBalancerBackendAddressPoolConfig -
    Name $BEPool
8 <!--NeedCopy-->
```

6. **Erstellen eines Gesundheitstasters**

   Erstellen Sie einen TCP-Integritätstest mit Port 9000 und Intervall 5 Sekunden.

```
1 $healthProbe = New-AzureRmLoadBalancerProbeConfig -Name
    HealthProbe -Protocol Tcp -Port 9000 -IntervalInSeconds 5 -
    ProbeCount 2
2 <!--NeedCopy-->
```

7. **Erstellen einer Lastausgleichsregel**

   Erstellen Sie eine LB-Regel für jeden Dienst, für den Sie Lastenausgleich arbeiten.

   Zum Beispiel:

   Sie können das folgende Beispiel verwenden, um den HTTP-Dienst Lastenausgleich zu verwenden.

```
1 $lbrule1 = New-AzureRmLoadBalancerRuleConfig -Name "HTTP-LB" -
    FrontendIpConfiguration $frontendIP1 -BackendAddressPool
    $beAddressPool1 -Probe $healthProbe -Protocol Tcp -FrontendPort
     80 -BackendPort 80
2 <!--NeedCopy-->
```

8. **Erstellen eingehender NAT-Regeln**

   Erstellen Sie NAT-Regeln für Dienste, für die Sie keinen Lastausgleich haben.

   Zum Beispiel beim Erstellen eines SSH-Zugriffs auf eine Citrix ADC VPX Instanz.

   Hinweis: Protocol-FrontendPort-BackendPort-Triplet darf für zwei NAT-Regeln nicht identisch sein.


```
$inboundNATRule1= New-AzureRmLoadBalancerInboundNatRuleConfig -
    Name SSH1     -FrontendIpConfiguration $frontendIP1 -Protocol
    TCP -FrontendPort 22 -BackendPort 22

$inboundNATRule2= New-AzureRmLoadBalancerInboundNatRuleConfig -
    Name SSH2 -FrontendIpConfiguration $frontendIP1 -Protocol TCP -
    FrontendPort 10022 -BackendPort 22
<!--NeedCopy-->
```

9. **Erstellen einer Load Balancer-Entität**

   Erstellen Sie den Load Balancer und fügen Sie alle Objekte (NAT-Regeln, Load Balancer-Regeln, Probe-Konfigurationen) zusammen.

```
$lbName="ELB"

$NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgName -Name
    $lbName -Location $locName -InboundNatRule $inboundNATRule1,
    $inboundNATRule2 -FrontendIpConfiguration $frontendIP1 -
    LoadBalancingRule $lbrule1 -BackendAddressPool $beAddressPool1
    -Probe $healthProbe
<!--NeedCopy-->
```

10. **Erstellen einer Netzwerkkarte**

    Erstellen Sie zwei Netzwerkkarten und verknüpfen Sie jede Netzwerkkarte mit jeder VPX-Instanz

    a) NIC1 mit VPX1

    Zum Beispiel:

```
$nicName="NIC1"

$lbName="ELB"

$bePoolIndex=0

* Rule indexes starts from 0.

$natRuleIndex=0

$subnetIndex=0

* Frontend subnet index
```



```
14
15 $lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
       $rgName
16
17 $nic1=New-AzureRmNetworkInterface -Name $nicName -
       ResourceGroupName $rgName -Location $locName -Subnet $vnet.
       Subnets[$subnetIndex] -LoadBalancerBackendAddressPool $lb.
       BackendAddressPools[$bePoolIndex] -LoadBalancerInboundNatRule
       $lb.InboundNatRules[$natRuleIndex]
18 <!--NeedCopy-->
```

b) NIC2 mit VPX2

Zum Beispiel:

```
1  $nicName="NIC2"
2
3  $lbName="ELB"
4
5  $bePoolIndex=0
6
7  $natRuleIndex=1
8
9  * Second Inbound NAT (SSH) rule we need to use
10
11 `$subnetIndex=0
12
13 * Frontend subnet index
14
15 $lb=Get-AzureRmLoadBalancer -Name $lbName -ResourceGroupName
       $rgName
16
17 $nic2=New-AzureRmNetworkInterface -Name $nicName -
       ResourceGroupName $rgName -Location $locName -Subnet $vnet.
       Subnets[$subnetIndex] -LoadBalancerBackendAddressPool $lb.
       BackendAddressPools[$bePoolIndex] -LoadBalancerInboundNatRule
       $lb.InboundNatRules[$natRuleIndex]
18 <!--NeedCopy-->
```

11. **Erstellen von Citrix ADC VPX-Instanzen**

    Erstellen Sie zwei Citrix ADC VPX-Instanzen als Teil derselben Ressourcengruppe und derselben Verfügbarkeitsgruppe, und fügen Sie sie an den externen Load Balancer an.

    a) Citrix ADC VPX-Instanz 1

Zum Beispiel:

```
$vmName="VPX1"

$vmSize="Standard_A3"

$pubName="citrix"

$offerName="netscalervpx110-6531"

$skuName="netscalerbyol"

$avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
    $rgName

$vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
   AvailabilitySetId $avset.Id

$cred=Get-Credential -Message "Type Credentials which will be used
    to login to VPX instance"

$vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
   $vmName -Credential $cred -Verbose

$vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
   Offer $offerName -Skus $skuName -Version "latest"

$vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $nic1.Id

$diskName="dynamic"

$storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
   Name $saName

$osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds1/
   " + $diskName  + ".vhd"

$vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
   $osDiskUri1 -CreateOption fromImage

Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product $offerName
    -Name $skuName

```



```
33 New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
       $vm1
34 <!--NeedCopy-->
```

b) Citrix ADC VPX-Instanz 2

Zum Beispiel:

```
1  $vmName=”VPX2”
2
3  $vmSize=”Standard_A3”
4
5  $avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
       $rgName
6
7  $vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
       AvailabilitySetId $avset.Id
8
9  $cred=Get-Credential -Message ” Type Credentials which will be
       used to login to VPX instance ”
10
11 $vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
       $vmName -Credential $cred -Verbose
12
13 $vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
       Offer $offerName -Skus $skuName -Version ”latest”
14
15 $vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $nic2.Id
16
17 $diskName=”dynamic”
18
19 $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
       Name $saName
20
21 $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + ”vhds2/
       ” + $diskName  + ”.vhd”
22
23 $vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
       $osDiskUri1 -CreateOption fromImage
24
25 Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product $offerName
       -Name $skuName
26
27 New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
```



```
    $vm2
<!--NeedCopy-->
```

12. **Konfigurieren der virtuellen Maschinen**

    Wenn beide Citrix ADC VPX-Instanzen gestartet werden, stellen Sie mithilfe des SSH-Protokolls eine Verbindung zu beiden Citrix ADC VPX-Instanzen her, um die virtuellen Maschinen zu konfigurieren.

    a) Aktiv-Aktiv: Führen Sie denselben Satz von Konfigurationsbefehlen in der Befehlszeile beider Citrix ADC VPX-Instanzen aus.

    b) Aktiv-Passiv: Führen Sie diesen Befehl in der Befehlszeile der beiden Citrix ADC VPX-Instanzen aus.

    ```
    add ha node ##nodeID <nsip of other Citrix ADC VPX>
    ```

    Führen Sie im Aktiv-Passiv-Modus Konfigurationsbefehle nur auf dem primären Knoten aus.

Bereitstellen eines Citrix ADC VPX Paares in einem Hochverfügbarkeitssetup mit dem internen Azure-Load Balancer

Melden Sie sich mit Ihren Azure-Benutzeranmeldeinformationen bei AzureRmAccount an.

1. **Erstellen einer Ressourcengruppe**

   Der hier angegebene Speicherort ist der Standardspeicherort für Ressourcen in dieser Ressourcengruppe. Stellen Sie sicher, dass alle Befehle zum Erstellen eines Load Balancer dieselbe Ressourcengruppe verwenden.

   ```
   $rgName=”\<resource group name\>”

   $locName=”\<location name, such as West US\>”

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   ```

   Zum Beispiel:

   ```
   $rgName = ”ARM-LB-NS”

   $locName = ”West US”

   New-AzureRmResourceGroup -Name $rgName -Location $locName
   <!--NeedCopy-->
   ```

2. **Speicherkonto erstellen**

Wählen Sie einen eindeutigen Namen für Ihr Speicherkonto, der nur Kleinbuchstaben und Zahlen enthält.

`$saName=”<storage account name>”`

`$saType=”<storage account type>”`, geben Sie eines an: `Standard_LRS`, `Standard_GRS`, `Standard_RAGRS` oder `Premium_LRS`

```
New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName -Type $saType -Location $locName
```

Zum Beispiel:

```
$saName=”vpxstorage”

$saType=”Standard_LRS”

New-AzureRmStorageAccount -Name $saName -ResourceGroupName $rgName
    -Type $saType -Location $locName
<!--NeedCopy-->
```

3. **Erstellen eines Verfügbarkeitssatzes**

   Ein Load Balancer, der mit einem Verfügbarkeitssatz konfiguriert ist, stellt sicher, dass Ihre Anwendung immer verfügbar ist.

   `$avName=”<availability set name>”`

   ```
   New-AzureRmAvailabilitySet -Name $avName -ResourceGroupName $rgName -Location $locName
   ```

4. **Erstellen eines virtuellen Netzwerks**

   Fügen Sie ein neues virtuelles Netzwerk mit mindestens einem Subnetz hinzu, wenn das Subnetz vorher nicht erstellt wurde.

```
$vnetName = ”LBVnet”

$vnetAddressPrefix=”10.0.0.0/16”

$FrontendAddressPrefix=”10.0.1.0/24”

$BackendAddressPrefix=”10.0.2.0/24”

```



```
$vnet=New-AzureRmVirtualNetwork -Name $vnetName -ResourceGroupName
    $rgName -Location $locName -AddressPrefix $vnetAddressPrefix -
    Subnet $frontendSubnet,$backendSubnet`

$frontendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    frontendSubnet -AddressPrefix $FrontendAddressPrefix

$backendSubnet=New-AzureRmVirtualNetworkSubnetConfig -Name
    backendSubnet -AddressPrefix $BackendAddressPrefix
<!--NeedCopy-->
```

Hinweis: Wählen Sie den AddressPrefix-Parameterwert gemäß Ihrer Anforderung.

Weisen Sie dem virtuellen Netzwerk, das Sie zuvor in diesem Schritt erstellt haben, Front-End- und Back-End-Subnetz zu.

Wenn das Front-End-Subnetz das erste Element von Array VNet ist, muss subnetId $vNet.Subnets [0] .Id sein.

Wenn das Front-End-Subnetz das zweite Element im Array ist, muss die subnetID $vNet.Subnets [1] .Id und so weiter sein.

5. **Erstellen eines Backend-Adresspool**

```
$beaddresspool= New-AzureRmLoadBalancerBackendAddressPoolConfig -Name "
LB-backend"
```

6. **Erstellen von NAT-Regeln**

Erstellen Sie NAT-Regeln für Dienste, für die Sie keinen Lastausgleich haben.

```
$inboundNATRule1= New-AzureRmLoadBalancerInboundNatRuleConfig -
    Name "Inboundnatrule1" -FrontendIpConfiguration $frontendIP -
    Protocol TCP -FrontendPort 3441 -BackendPort 3389

$inboundNATRule2= New-AzureRmLoadBalancerInboundNatRuleConfig -
    Name "RDP2" -FrontendIpConfiguration $frontendIP -Protocol TCP
    -FrontendPort 3442 -BackendPort 3389
<!--NeedCopy-->
```

Verwenden Sie Front-End-und Back-End-Ports nach Ihren Anforderungen.

7. **Erstellen eines Gesundheitstasters**

Erstellen Sie einen TCP-Integritätstest mit Port 9000 und Intervall 5 Sekunden.


```
$healthProbe = New-AzureRmLoadBalancerProbeConfig -Name ”
    HealthProbe”  ” -Protocol tcp -Port 9000 -IntervalInSeconds 5 -
    ProbeCount 2
<!--NeedCopy-->
```

8. **Erstellen einer Lastausgleichsregel**

   Erstellen Sie eine LB-Regel für jeden Dienst, für den Sie Lastenausgleich arbeiten.

   Beispiel:

   Sie können das folgende Beispiel verwenden, um den HTTP-Dienst Lastenausgleich zu verwenden.

```
$lbrule = New-AzureRmLoadBalancerRuleConfig -Name ”lbrule1” -
    FrontendIpConfiguration $frontendIP -BackendAddressPool
    $beAddressPool -Probe $healthProbe -Protocol Tcp -FrontendPort
    80 -BackendPort 80
<!--NeedCopy-->
```

   Verwenden Sie Front-End-und Back-End-Ports nach Ihren Anforderungen.

9. **Erstellen einer Load Balancer-Entität**

   Erstellen Sie den Load Balancer und fügen Sie alle Objekte (NAT-Regeln, Load Balancer-Regeln, Probe-Konfigurationen) zusammen.

```
$NRPLB = New-AzureRmLoadBalancer -ResourceGroupName $rgname -Name
    ”InternalLB” -Location $locName -FrontendIpConfiguration
    $frontendIP -InboundNatRule $inboundNATRule1,$inboundNatRule2 -
    LoadBalancingRule $lbrule -BackendAddressPool $beAddressPool -
    Probe $healthProbe
<!--NeedCopy-->
```

10. **Erstellen einer Netzwerkkarte**

    Erstellen Sie zwei Netzwerkkarten und ordnen Sie jede Netzwerkkarte jeder Citrix ADC VPX-Instanz zu

```
$backendnic1= New-AzureRmNetworkInterface -ResourceGroupName
    $rgName -Name lb-nic1-be -Location $locName -PrivateIpAddress
    10.0.2.6 -Subnet $backendSubnet -LoadBalancerBackendAddressPool
```



```
        $nrplb.BackendAddressPools[0] -LoadBalancerInboundNatRule
       $nrplb.InboundNatRules[0]
2  <!--NeedCopy-->
```

Diese Netzwerkkarte ist für Citrix ADC VPX 1. Die Private IP muss sich im selben Subnetz befinden wie die des hinzugefügten Subnetzes.

```
1  $backendnic2= New-AzureRmNetworkInterface -ResourceGroupName
       $rgName -Name lb-nic2-be -Location $locName -PrivateIpAddress
       10.0.2.7 -Subnet $backendSubnet -LoadBalancerBackendAddressPool
        $nrplb.BackendAddressPools[0] -LoadBalancerInboundNatRule
       $nrplb.InboundNatRules[1].
2  <!--NeedCopy-->
```

Diese NIC ist für Citrix ADC VPX 2. Der Parameter `Private IPAddress` kann jede private IP gemäß Ihrer Anforderung haben.

11. **Erstellen von Citrix ADC VPX-Instanzen**

    Erstellen Sie zwei VPX-Instanzen, die Teil derselben Ressourcengruppe und derselben Verfügbarkeitsgruppe sind, und fügen Sie sie dem internen Lastausgleichsdienst hinzu.

    a) Citrix ADC VPX-Instanz 1

    Zum Beispiel:

```
1  $vmName=”VPX1”
2
3  $vmSize=”Standard_A3”
4
5  $avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
       $rgName
6
7  $vm1=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
       AvailabilitySetId $avset.Id
8
9  $cred=Get-Credential -Message ”Type Credentials which will be used
       to login to VPX instance”
10
11 $vm1=Set-AzureRmVMOperatingSystem -VM $vm1 -Linux -ComputerName
       $vmName -Credential $cred -Verbose
12
13 $vm1=Set-AzureRmVMSourceImage -VM $vm1 -PublisherName $pubName -
       Offer $offerName -Skus $skuName -Version ”latest”
```



```
14
15 $vm1=Add-AzureRmVMNetworkInterface -VM $vm1 -Id $backendnic1.Id
16
17 $diskName="dynamic"
18
19 $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
       Name $saName
20
21 $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds1/
       " + $diskName  + ".vhd"
22
23 $vm1=Set-AzureRmVMOSDisk -VM $vm1 -Name $diskName -VhdUri
       $osDiskUri1 -CreateOption fromImage
24
25 Set-AzureRmVMPlan -VM $vm1 -Publisher $pubName -Product $offerName
        -Name $skuName
26
27 New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
       $vm1
28 <!--NeedCopy-->
```

b) Citrix ADC VPX-Instanz 2

Zum Beispiel:

```
1 $vmName="VPX2"
2
3 $vmSize="Standard_A3"
4
5 $avSet=Get-AzureRmAvailabilitySet -Name $avName -ResourceGroupName
       $rgName
6
7 $vm2=New-AzureRmVMConfig -VMName $vmName -VMSize $vmSize -
       AvailabilitySetId $avset.Id
8
9 $cred=Get-Credential -Message " Type Credentials which will be
       used to login to VPX instance "
10
11 $vm2=Set-AzureRmVMOperatingSystem -VM $vm2 -Linux -ComputerName
       $vmName -Credential $cred -Verbose
12
13 $vm2=Set-AzureRmVMSourceImage -VM $vm2 -PublisherName $pubName -
       Offer $offerName -Skus $skuName -Version "latest"
14
```



```
15 $vm2=Add-AzureRmVMNetworkInterface -VM $vm2 -Id $backendnic2.Id
16
17 $diskName="dynamic"
18
19 $storageAcc=Get-AzureRmStorageAccount -ResourceGroupName $rgName -
       Name $saName
20
21 $osDiskUri1=$storageAcc.PrimaryEndpoints.Blob.ToString() + "vhds2/
       " + $diskName  + ".vhd"
22
23 $vm2=Set-AzureRmVMOSDisk -VM $vm2 -Name $diskName -VhdUri
       $osDiskUri1 -CreateOption fromImage
24
25 Set-AzureRmVMPlan -VM $vm2 -Publisher $pubName -Product $offerName
        -Name $skuName
26
27 New-AzureRmVM -ResourceGroupName $rgName -Location $locName -VM
       $vm2
28 <!--NeedCopy-->
```

12. **Konfigurieren der virtuellen Maschinen**

    Wenn beide Citrix ADC VPX-Instanzen gestartet werden, stellen Sie mithilfe des SSH-Protokolls eine Verbindung zu beiden Citrix ADC VPX-Instanzen her, um die virtuellen Maschinen zu konfigurieren.

    a) Aktiv-Aktiv: Führen Sie denselben Satz von Konfigurationsbefehlen in der Befehlszeile beider Citrix ADC VPX-Instanzen aus.

    b) Aktiv-Passiv: Führen Sie diesen Befehl in der Befehlszeile der beiden Citrix ADC VPX-Instanzen aus.

    ```
    add ha node ##nodeID <nsip of other Citrix ADC VPX>
    ```

    Führen Sie im Aktiv-Passiv-Modus Konfigurationsbefehle nur auf dem primären Knoten aus.

Häufig gestellte Fragen zu Azure

October 5, 2021

- **unterscheidet sich das Upgradeverfahren der Citrix ADC VPX Instanz, die über Azure Marketplace installiert wurde, von der lokalen Upgradeprozedur?**

  Nein. Sie können Ihre Citrix ADC VPX-Instanz in der Microsoft Azure-Cloud auf Citrix ADC VPX Version 11.1 oder höher aktualisieren, indem Sie die standardmäßigen Citrix ADC VPX-

Upgradeverfahren verwenden. Sie können ein Upgrade entweder mit GUI- oder CLI-Prozeduren durchführen. Verwenden Sie für neue Installationen das Citrix ADC VPX Image für die Microsoft Azure-Cloud.

Um die Citrix ADC VPX-Upgrade-Builds herunterzuladen, gehen Sie zu **Citrix Downloads** > **Citrix ADC Firmware**.

- **Wie korrigiert man MAC-Bewegungen und Interface-Stummutes, die auf Citrix ADC VPX-Instanzen auf Azure gehostet werden?**

  In der Azure Multi-NIC-Umgebung zeigen alle Datenschnittstellen standardmäßig MAC-Bewegungen und Schnittstellenstummschaltung an. Um MAC-Verschiebungen und Stummschaltung der Benutzeroberfläche in Azure-Umgebungen zu vermeiden, empfiehlt Citrix, ein VLAN pro Datenschnittstelle (ohne Tag) der ADC VPX-Instanz zu erstellen und die primäre IP der Netzwerkkarte in Azure zu binden.

  Weitere Informationen finden Sie im Artikel CTX224626 .

Bereitstellen einer Citrix ADC VPX Instanz auf der Google Cloud Platform

January 25, 2022

Sie können eine Citrix ADC VPX-Instanz auf der Google Cloud Platform (GCP) bereitstellen. Mit einer VPX-Instanz in GCP können Sie die Vorteile der GCP-Cloud-Computing-Funktionen nutzen und Citrix Load Balancing und Traffic-Management-Funktionen für Ihre geschäftlichen Anforderungen nutzen. Sie können VPX-Instanzen in GCP als eigenständige Instanzen bereitstellen. Sowohl einzelne NIC- als auch Multi-NIC-Konfigurationen werden unterstützt.

Unterstützte Features

Alle Premium-, Advanced- und Standardfunktionen werden auf der GCP basierend auf dem verwendeten Lizenz-/Versionstyp unterstützt.

Einschränkung

- IPv6 wird nicht unterstützt.

Hardwareanforderungen

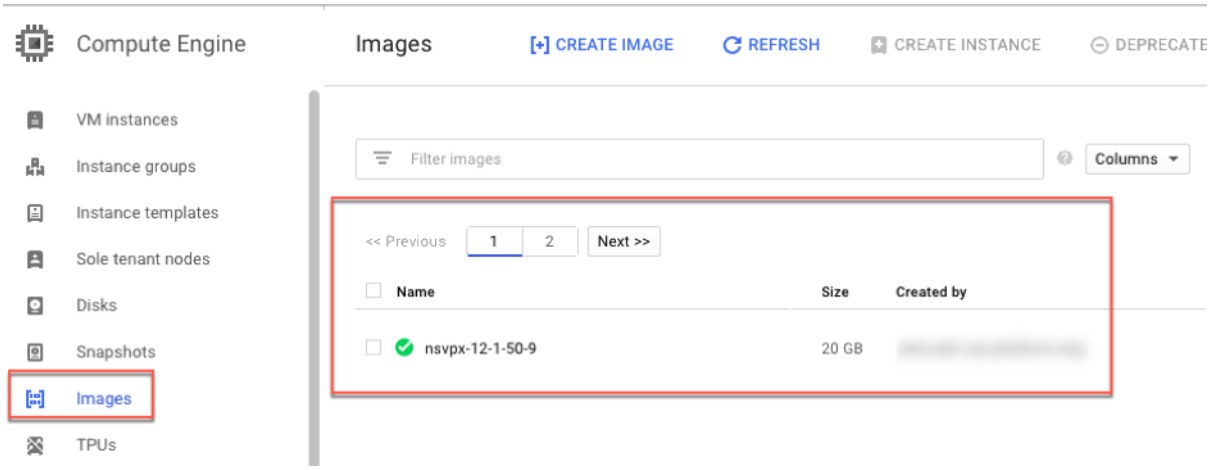
Die VPX-Instanz in GCP muss mindestens 2 vCPUs und 4 GB RAM haben.

Voraussetzungen

1. Installieren Sie das Dienstprogramm “gcloud” auf Ihrem Gerät. Das Dienstprogramm finden Sie unter diesem Link: https://cloud.google.com/sdk/install
2. Laden Sie das NSVPX-GCP-Image von der Citrix Download-Site herunter.
3. Laden Sie die Datei (z. B. NSVPX-GCP-12.1-50.9_NC_64.tar.gz) in einen Speicher-Bucket bei Google hoch, indem Sie die unter angegebenen Schritte ausführen https://cloud.google.com/storage/docs/uploading-objects.
4. Führen Sie den folgenden Befehl im gcloud-Dienstprogramm aus, um ein Image zu erstellen.

```
gcloud compute images create <IMAGE_NAME> --source-uri=gs://<
    STORAGE_BUCKET_NAME>/<FILE_NAME>.tar.gz --guest-os-features=
    MULTI_IP_SUBNET
<!--NeedCopy-->
```

Es kann einen Moment dauern, bis das Image erstellt wurde. Nachdem das Image erstellt wurde, wird es unter **Compute** > **Compute Engine** in der GCP-Konsole angezeigt.



Zu beachtendes Punkte

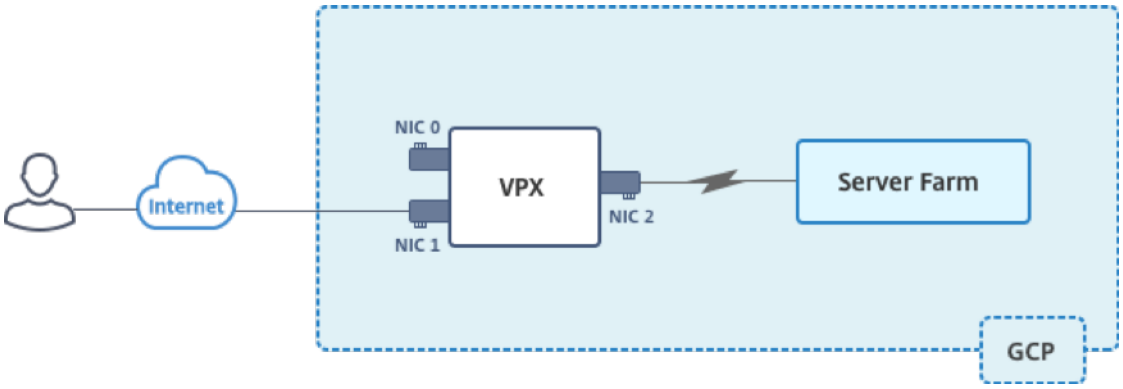
Berücksichtigen Sie die folgenden GCP-spezifischen Punkte, bevor Sie mit der Bereitstellung beginnen.

- Nach dem Erstellen der Instanz können Sie keine Netzwerkschnittstellen hinzufügen oder entfernen.
- Erstellen Sie für eine Multi-NIC-Bereitstellung separate VPC-Netzwerke für jede Netzwerkkarte. Eine Netzwerkkarte kann nur mit einem Netzwerk verknüpft werden.
- Für eine Single-NIC-Instanz erstellt die GCP-Konsole standardmäßig ein Netzwerk.

- Für eine Instanz mit mehr als zwei Netzwerkschnittstellen sind mindestens 4 vCPUs erforderlich.
- Wenn IP-Weiterleitung erforderlich ist, müssen Sie die IP-Weiterleitung aktivieren, während Sie die Instanz erstellen und die Netzwerkkarte konfigurieren.

Szenario: Bereitstellen einer eigenständigen VPX-Instanz mit mehreren NICs und mehreren IPs

Dieses Szenario veranschaulicht, wie eine eigenständige Citrix VPX-Instanz in GCP bereitgestellt wird. In diesem Szenario erstellen Sie eine eigenständige VPX-Instanz mit mehreren NICs. Die Instanz kommuniziert mit Back-End-Servern (der Serverfarm).



Erstellen Sie drei NICs, um den folgenden Zwecken zu dienen.

NIC	Zweck	Verbunden mit VPC-Netzwerk
NIC 0	Dient Verwaltungsdatenverkehr (Citrix ADC IP)	Management-Netzwerk
NIC 1	Dient clientseitigem Datenverkehr (VIP)	Kunden-Netzwerk
NIC 2	Kommuniziert mit Back-End-Servern (SNIP)	Back-End-Server-Netzwerk

Richten Sie außerdem die erforderlichen Kommunikationswege zwischen der Instanz und den Back-End-Servern sowie zwischen der Instanz und den externen Hosts im öffentlichen Internet ein.

Zusammenfassung der Bereitstellungsschritte

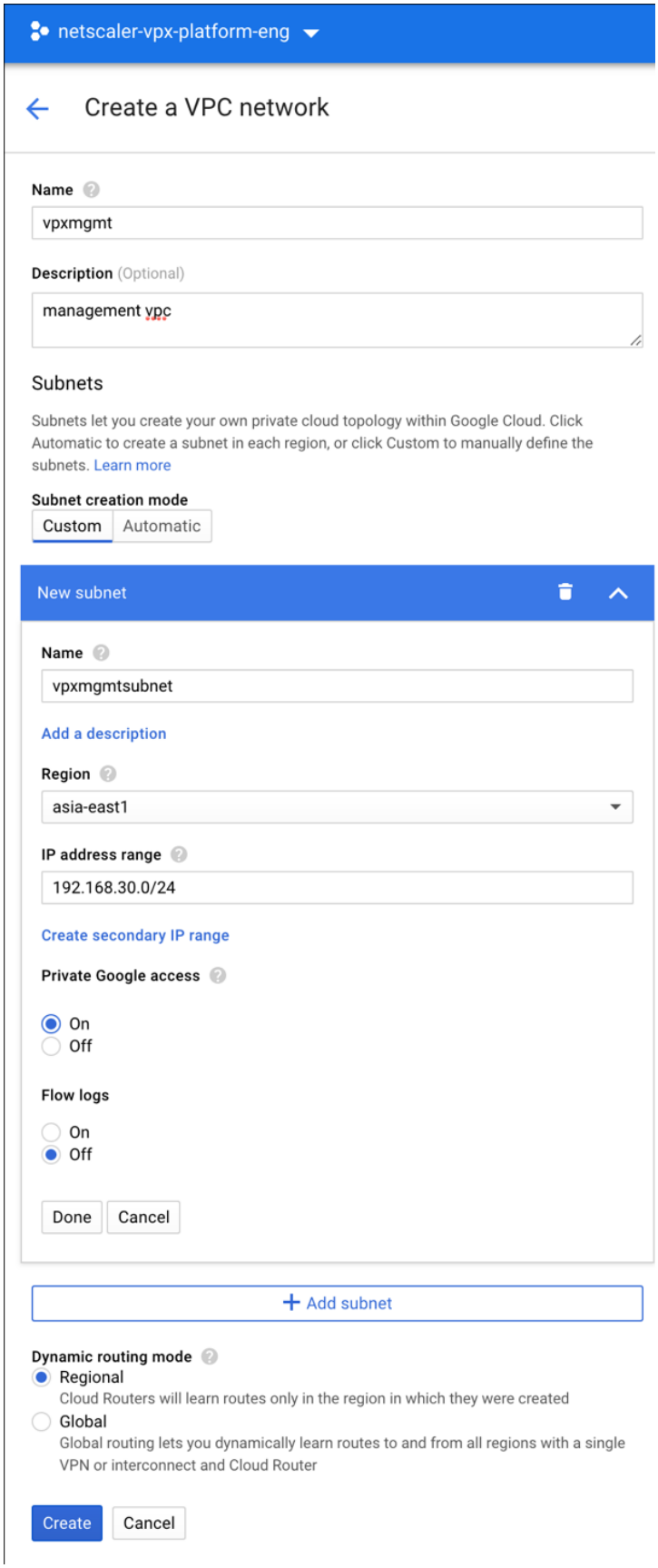
1. Erstellen Sie drei VPC-Netzwerke für drei verschiedene NICs.
2. Erstellen Sie Firewall-Regeln für die Ports 22, 80 und 443

3. Erstellen einer Instanz mit drei NICs

Hinweis: Erstellen Sie eine Instanz in derselben Region, in der Sie die VPC-Netzwerke erstellt haben.

Schritt 1. Erstellen Sie VPC-Netzwerke.

Erstellen Sie drei VPC-Netzwerke, die mit Verwaltungs-NIC, Client-NIC und Server-NIC verknüpft sind. Um ein VPC-Netzwerk zu erstellen, melden Sie sich bei **Google-Konsole > Netzwerk > VPC-Netzwerk > VPC-Netzwerk erstellen**an. Füllen Sie die erforderlichen Felder aus, wie in der Bildschirmaufnahme gezeigt, und klicken Sie auf **Erstellen**.

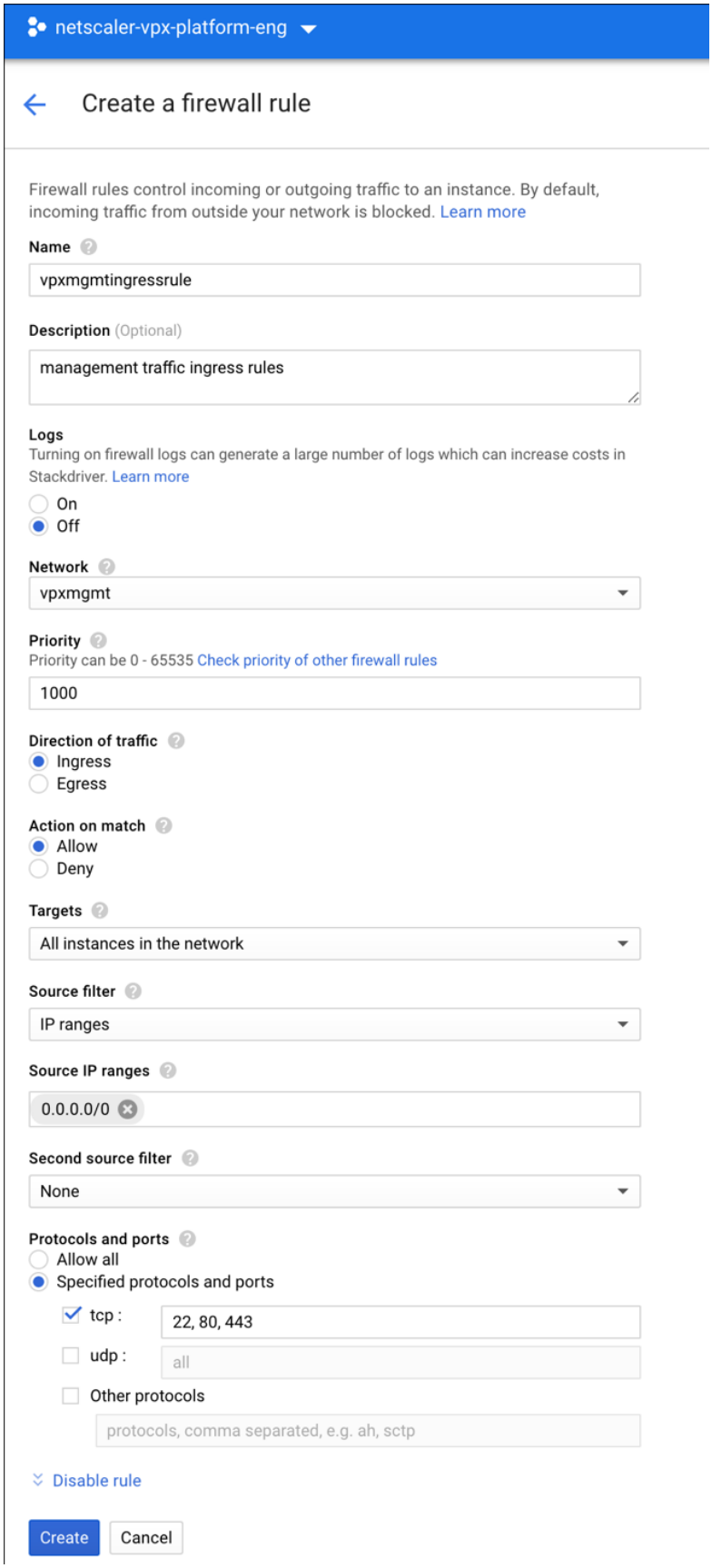


Erstellen Sie in ähnlicher Weise VPC-Netzwerke für client- und serverseitige Netzwerkkarten.

Hinweis: Alle drei VPC-Netzwerke müssen sich in derselben Region befinden, die in diesem Szenario Asien-Ost1 ist.

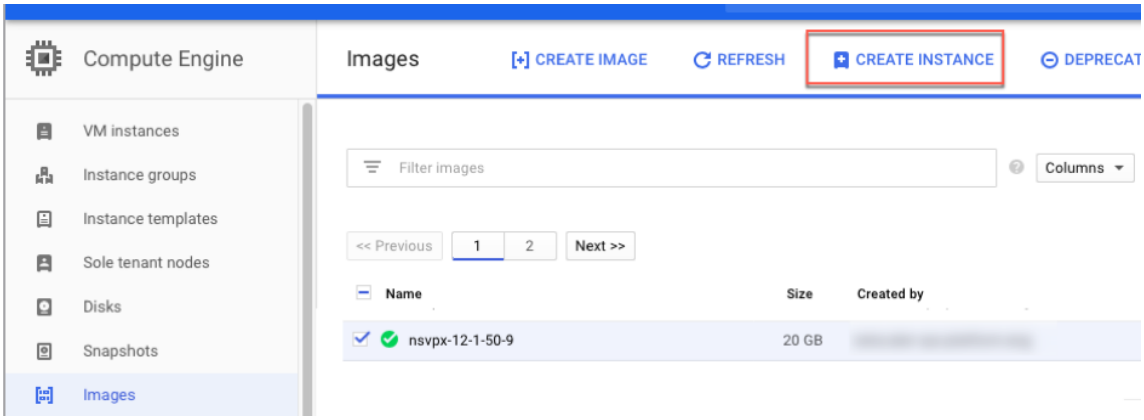
Schritt 2. Erstellen Sie Firewall-Regeln für die Ports 22, 80 und 443.

Erstellen Sie Regeln für SSH (Port 22), HTTP (Port 80) und HTTPS (Port 443) für jedes VPC-Netzwerk. Weitere Informationen zu Firewall-Regeln finden Sie unter Übersicht über Firewall-Regeln.



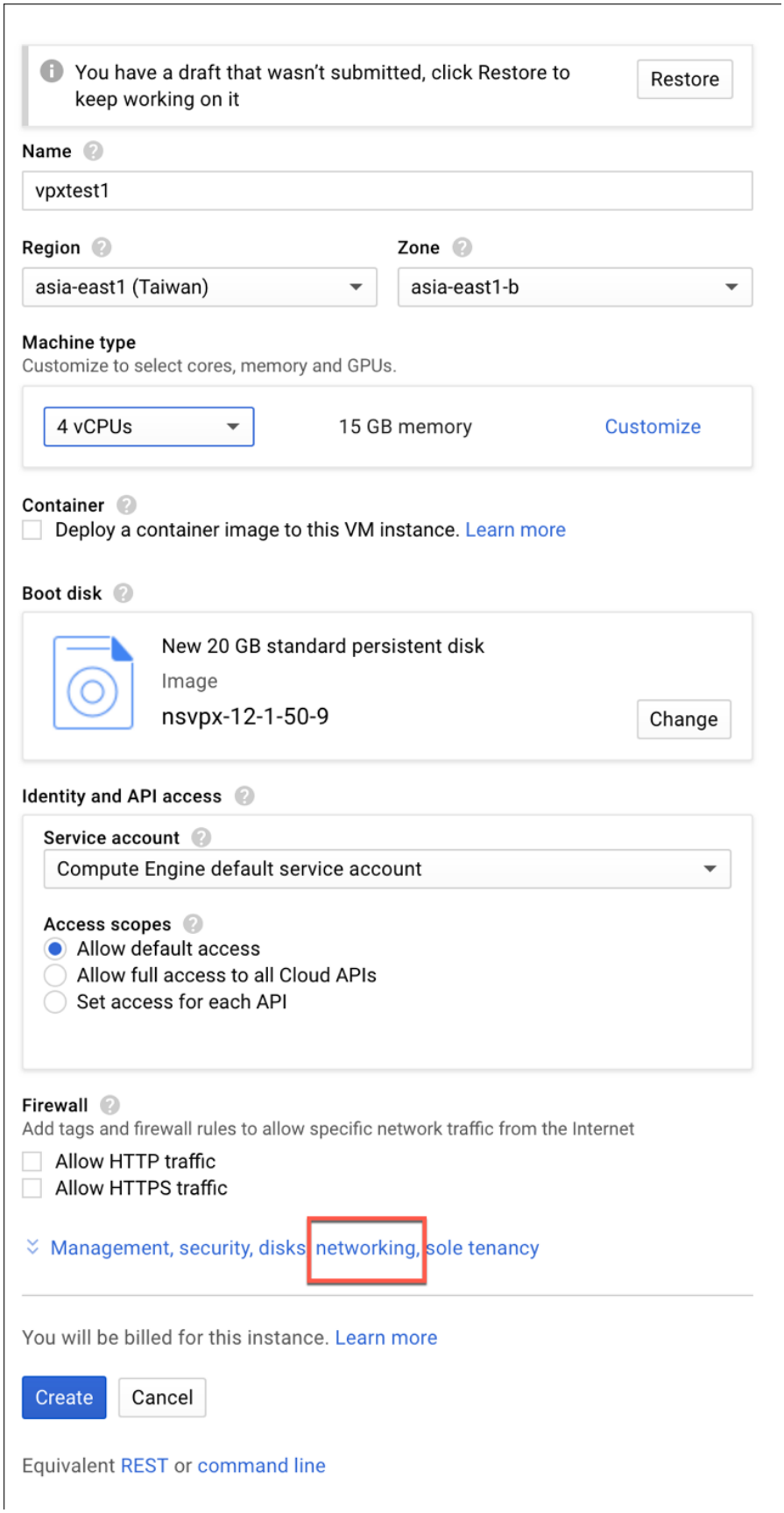
Schritt 3. Erstellen Sie die VPX-Instanz.

1. Melden Sie sich bei der GCP-Konsole an.
2. Bewegen Sie unter **Compute**den Mauszeiger über Compute Engine und wählen Sie **Images** aus.
3. Wählen Sie das Image aus und klicken Sie auf **Instanz erstellen**.

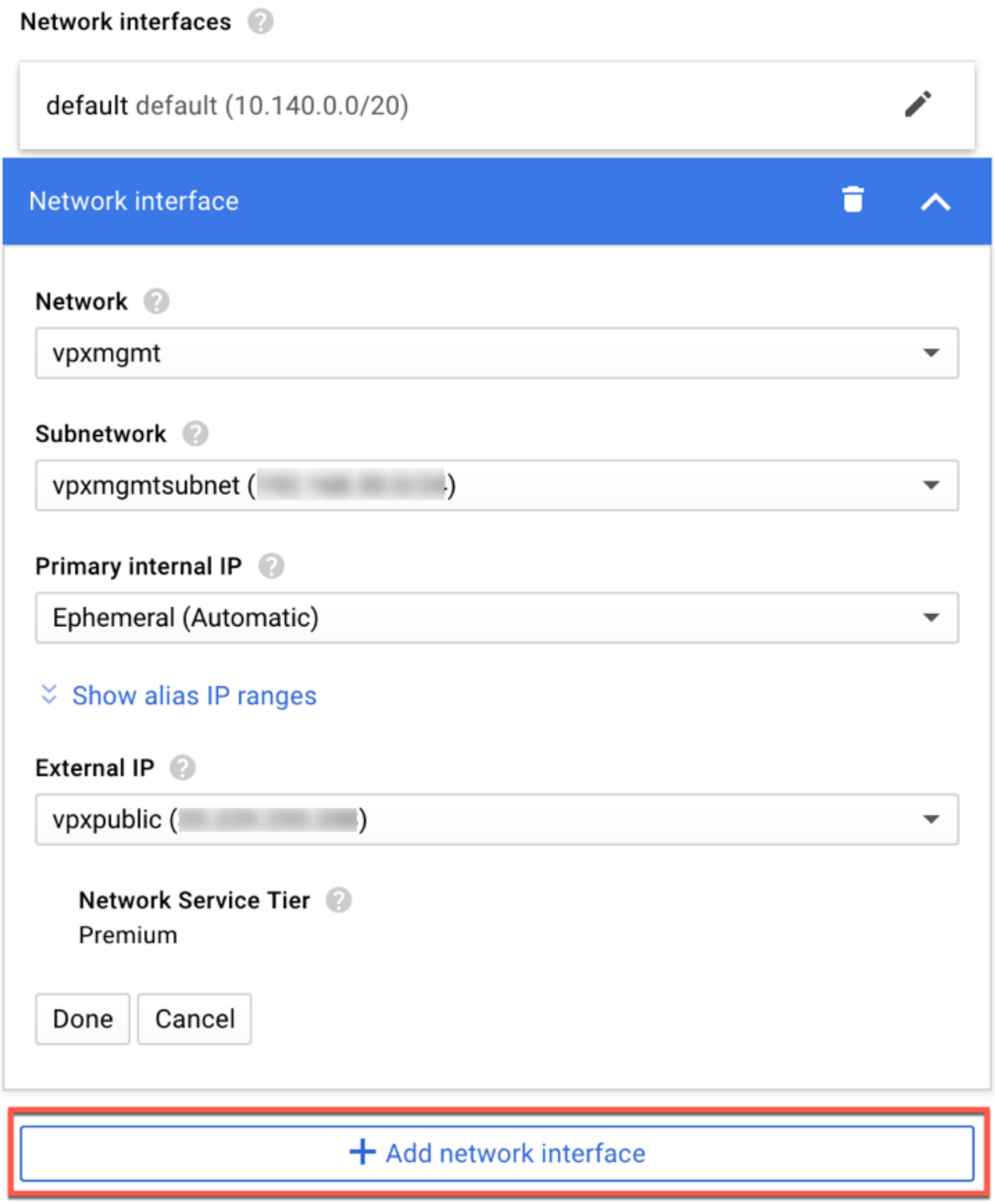


4. Wählen Sie eine Instanz mit 4 vCPUs aus, um mehrere Netzwerkkarten zu unterstützen.
5. Klicken Sie auf die Netzwerkoption unter Verwaltung, Sicherheit, Datenträger, Netzwerk, Einzelmandanten, um die zusätzlichen NICs hinzuzufügen.

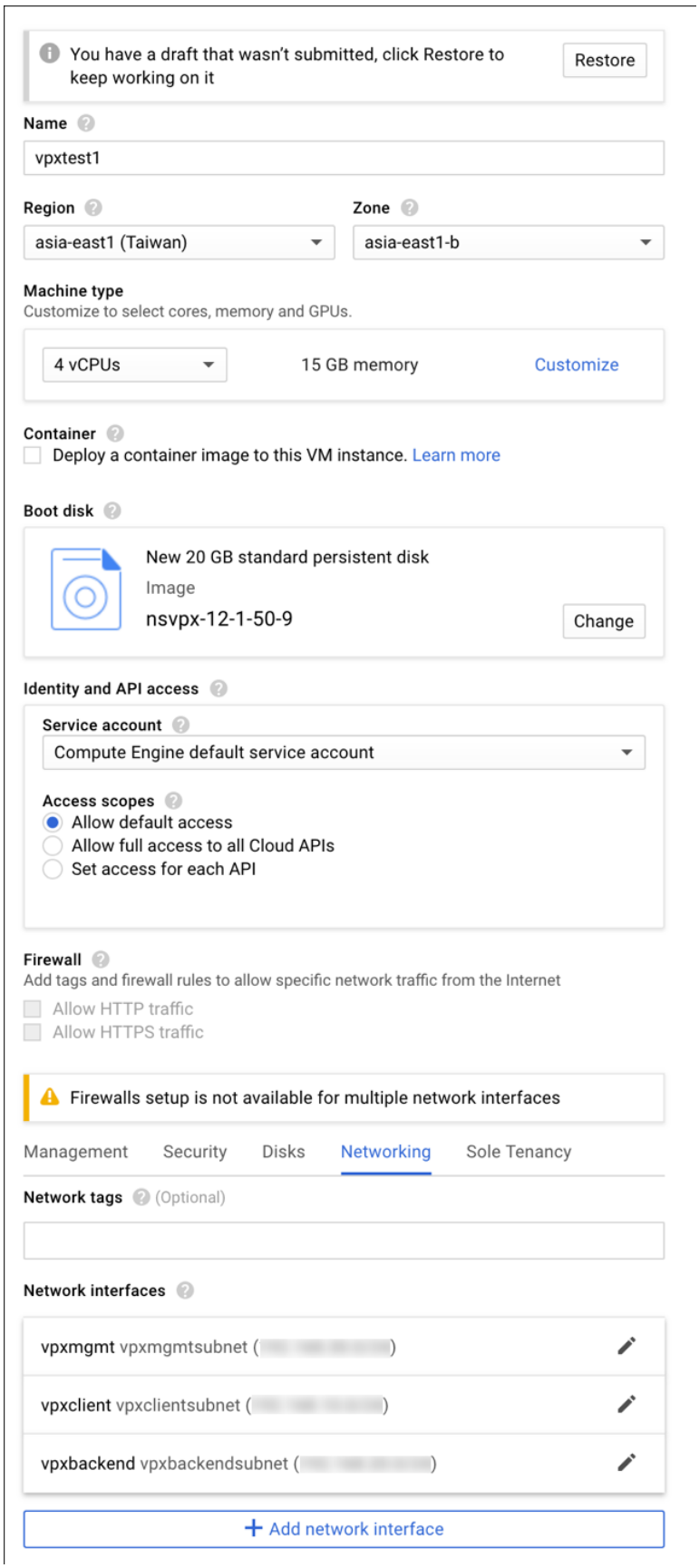
   Hinweis: Container-Image wird für VPX-Instanzen auf GCP nicht unterstützt.



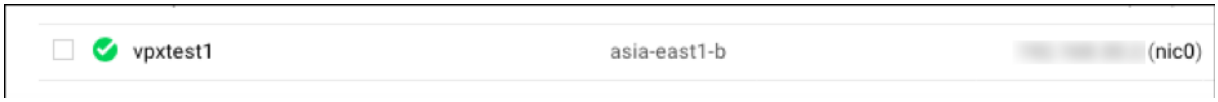
6. Klicken Sie unter **Netzwerkschnittstellen**auf das Bearbeitungssymbol, um die Standard-Netzwerkkarte zu bearbeiten. Diese NIC ist die Verwaltungs-NIC.
7. Wählen Sie im Fenster **Netzwerkschnittstellen** unter **Netzwerk**das VPC-Netzwerk aus, das Sie für die Verwaltungs-NIC erstellt haben.
8. Erstellen Sie für die Verwaltungs-NIC eine statische externe IP-Adresse. Klicken Sie unter der Liste Externe IP auf **IP-Adresse erstellen**.
9. Fügen Sie im Fenster **Neue statische IP-Adresse reservieren einen** Namen und eine Beschreibung hinzu und klicken Sie auf **Reservieren**.
10. Klicken Sie auf **Netzwerkschnittstelle hinzufügen**, um Netzwerkkarten für einen Client- und serverseitigen Datenverkehr zu erstellen.



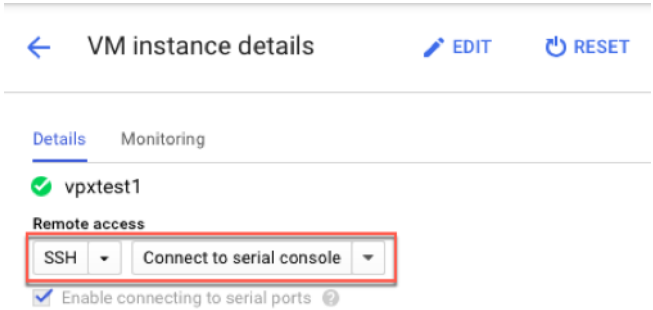
Nachdem Sie alle NICs erstellt haben, klicken Sie auf **Erstellen**, um die VPX-Instanz zu erstellen.



Die Instanz wird unter **VM-Instanzen**angezeigt.

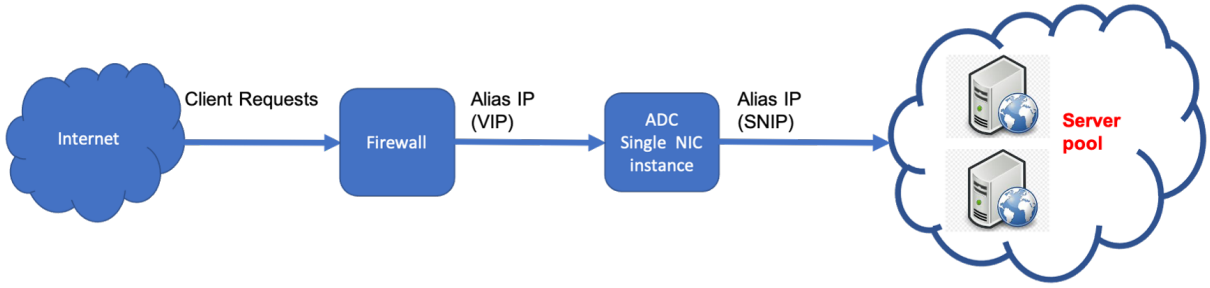


Verwenden Sie die GCP SSH oder die serielle Konsole, um die VPX-Instanz zu konfigurieren und zu verwalten.



Szenario: Bereitstellen einer eigenständigen VPX-Instanz mit einer einzigen NIC

Dieses Szenario veranschaulicht, wie eine eigenständige Citrix VPX-Instanz mit einer einzigen NIC in GCP bereitgestellt wird. Die Alias-IP-Adressen werden verwendet, um diese Bereitstellung zu erreichen.



Erstellen Sie eine einzelne NIC (NIC0) für folgende Zwecke:

- Behandeln Sie den Verwaltungsdatenverkehr (Citrix ADC IP) im Verwaltungsnetzwerk.
- Behandeln Sie clientseitigen Datenverkehr (VIP) im Clientnetzwerk.
- Kommunizieren Sie mit Back-End-Servern (SNIP) im Back-End-Server-Netzwerk.

Richten Sie die erforderlichen Kommunikationswege zwischen den folgenden ein:

- Instanz und die Back-End-Server.
- Instanz und die externen Hosts im öffentlichen Internet.

Zusammenfassung der Bereitstellungsschritte

1. Erstellen Sie ein VPC-Netzwerk für NIC0.

2. Erstellen Sie Firewall-Regeln für die Ports 22, 80 und 443.
3. Erstellen Sie eine Instanz mit einer einzigen NIC.
4. Fügen Sie Alias-IP-Adressen zu VPX hinzu.
5. Fügen Sie VIP und SNIP auf VPX hinzu.
6. Fügen Sie einen virtuellen Lastenausgleichsserver hinzu.
7. Fügen Sie der Instanz einen Dienst oder eine Servicegruppe hinzu.
8. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastenausgleichsserver der Instanz.

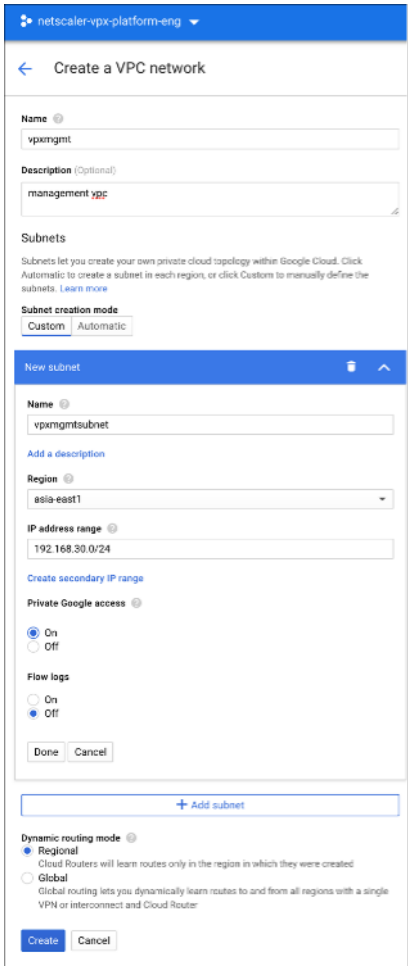
> **Hinweis**:
>
> Erstellen Sie eine Instanz in derselben Region, in der Sie die VPC-Netzwerke erstellt haben.

Schritt 1. Erstellen Sie ein VPC-Netzwerk.

Erstellen Sie ein VPC-Netzwerk, das Sie mit NIC0 verknüpfen möchten.

Gehen Sie folgendermaßen vor, um ein VPC-Netzwerk zu erstellen:

1. Melden Sie sich bei **GCP Console an > Netzwerk > VPC-Netzwerk > VPC-Netzwerk erstellen**
2. Füllen Sie die erforderlichen Felder aus, und klicken Sie auf **Erstellen**.



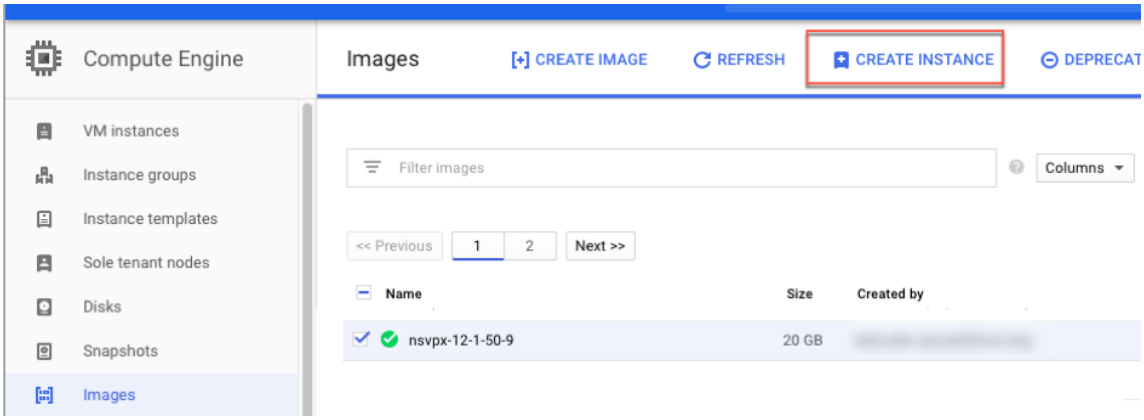
Schritt 2. Erstellen Sie Firewall-Regeln für die Ports 22, 80 und 443.

Erstellen Sie Regeln für SSH (Port 22), HTTP (Port 80) und HTTPS (Port 443) für das VPC-Netzwerk. Weitere Informationen zu Firewall-Regeln finden Sie unter Übersicht über Firewall-Regeln.

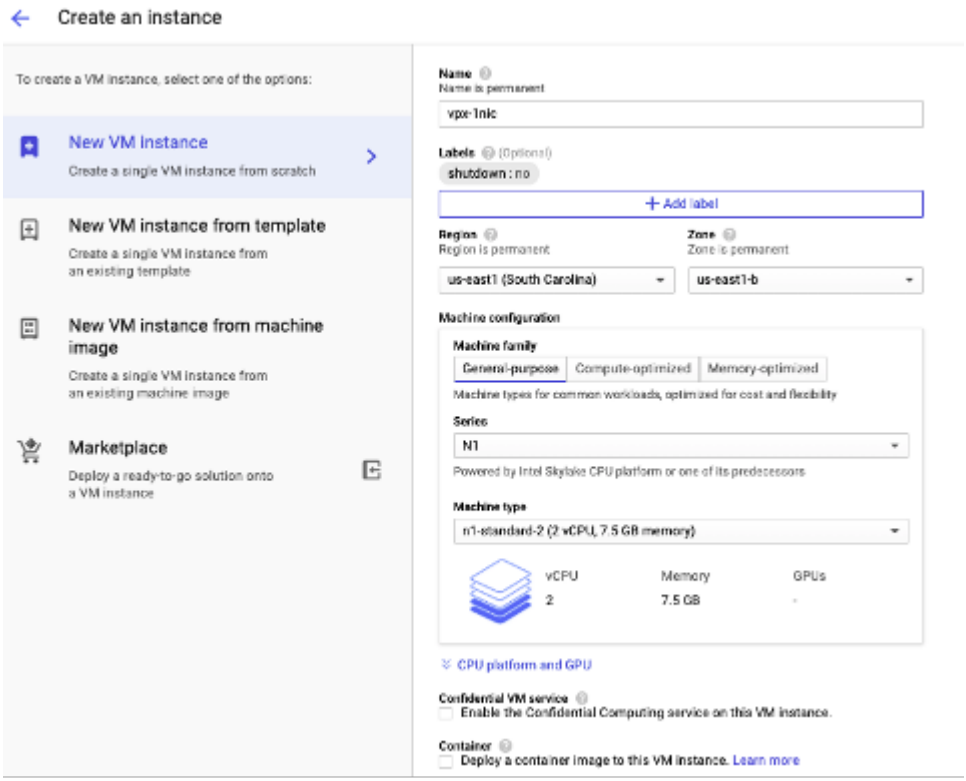
Schritt 3. Erstellen Sie eine Instanz mit einer einzelnen NIC.

Gehen Sie folgendermaßen vor, um eine Instanz mit einer einzelnen NIC zu erstellen:

1. Melden Sie sich an der **GCP-Konsole**an.
2. Bewegen **Sie unter Compute**den Mauszeiger über **Compute Engine**, und wählen Sie **Images**aus.
3. Wählen Sie das Image aus und klicken Sie auf **Instanz erstellen**.



4. Wählen Sie einen Instanztyp mit zwei vCPUs aus (Mindestanforderung für ADC).



5. Klicken Sie im Fenster **Verwaltung, Sicherheit, Datenträger, Netzwerk** auf die Registerkarte **Netzwerk**.
6. Klicken Sie unter **Netzwerkschnittstellen** auf das Symbol **Bearbeiten**, um die Standard-Netzwerkkarte zu bearbeiten.
7. Wählen Sie im Fenster **Netzwerkschnittstellen** unter **Netzwerk** das VPC-Netzwerk aus, das Sie erstellt haben.
8. Sie können eine statische externe IP-Adresse erstellen. Klicken Sie unter den **Externen IP-Adressen** auf **IP-Adresse erstellen**.

9. Fügen Sie im Fenster **Statische Adresse reservieren** einen Namen und eine Beschreibung hinzu und klicken Sie auf **Reservieren**.
10. Klicken Sie auf **Erstellen**, um die VPX-Instanz zu erstellen.
    Die neue Instanz wird unter VM-Instanzen angezeigt.

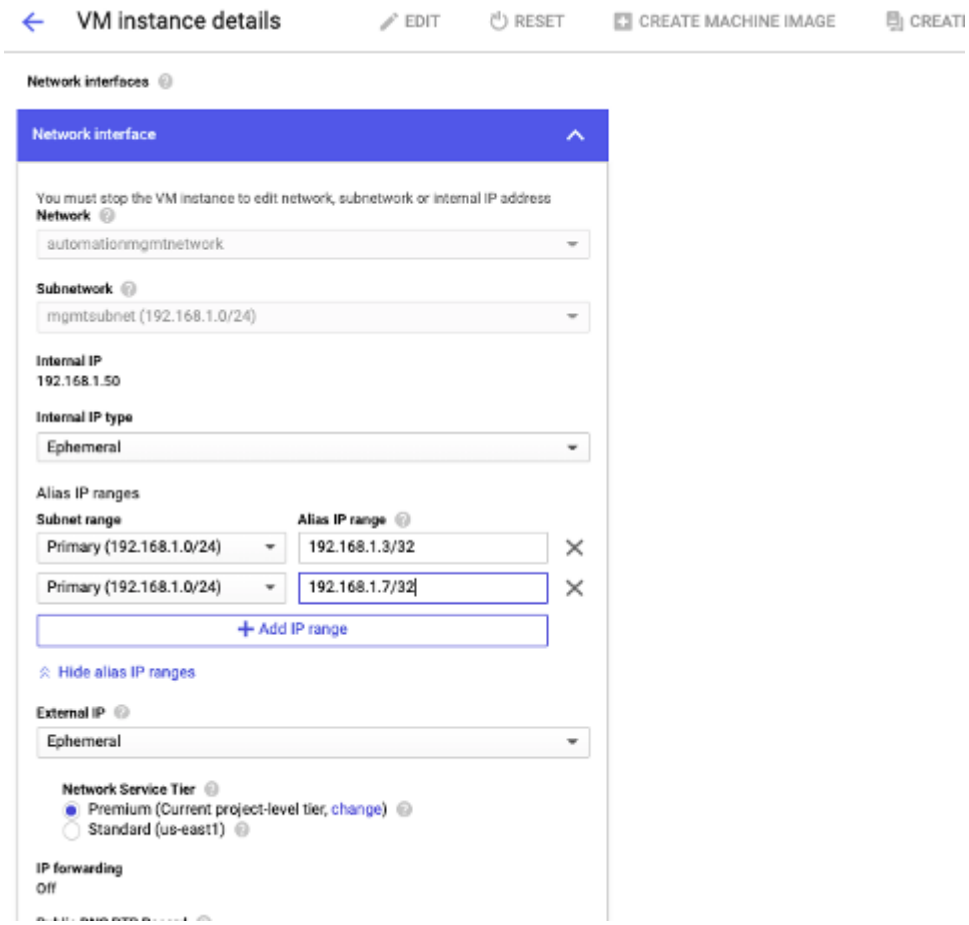
Schritt 4. Fügen Sie der VPX-Instanz Alias-IP-Adressen hinzu.

Weisen Sie der VPX-Instanz zwei Alias-IP-Adressen zu, die als VIP- und SNIP-Adressen verwendet werden sollen.

> **Hinweis:**
>
> Verwenden Sie nicht die primäre interne IP-Adresse der VPX-Instanz, um den VIP oder SNIP zu konfigurieren.

Gehen Sie folgendermaßen vor, um eine Alias-IP-Adresse zu erstellen:

1. Navigieren Sie zur VM-Instanz und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie im Fenster der **Netzwerkschnittstelle** die NIC0-Schnittstelle.
3. Geben Sie im Feld **Alias-IP-Bereich** die Alias-IP-Adressen ein.



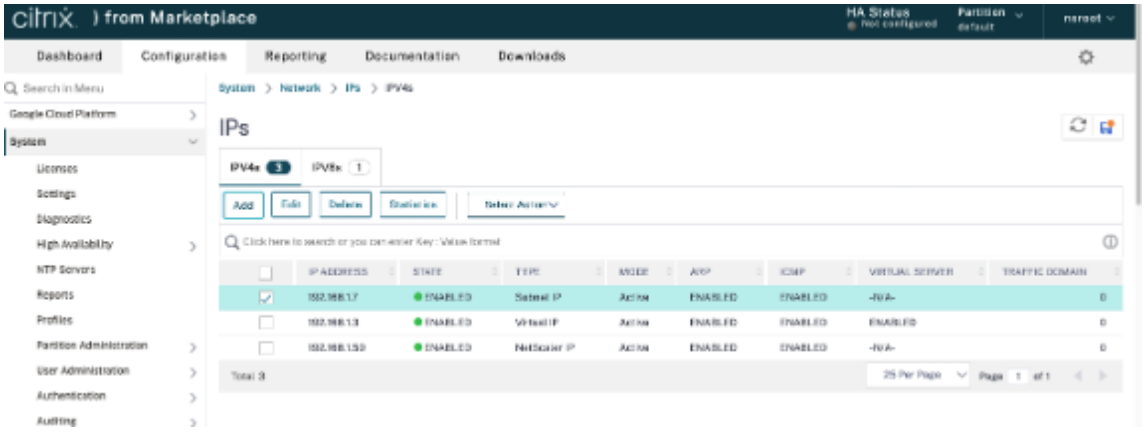
4. Klicken Sie auf **Fertig**und dann auf **Speichern**.

5. Überprüfen Sie die Alias-IP-Adressen auf der **Detailseite der VM-Instanz** .

Schritt 5. Fügen Sie VIP und SNIP in der VPX-Instanz hinzu.

Fügen Sie in der VPX-Instanz die IP-Adresse des Client-Alias und die IP-Adresse des Serveralias hinzu.

1. Navigieren Sie in der Citrix ADC GUI zu **System > Netzwerk > IPs > IPv4s**und klicken Sie auf **Hinzufügen**.

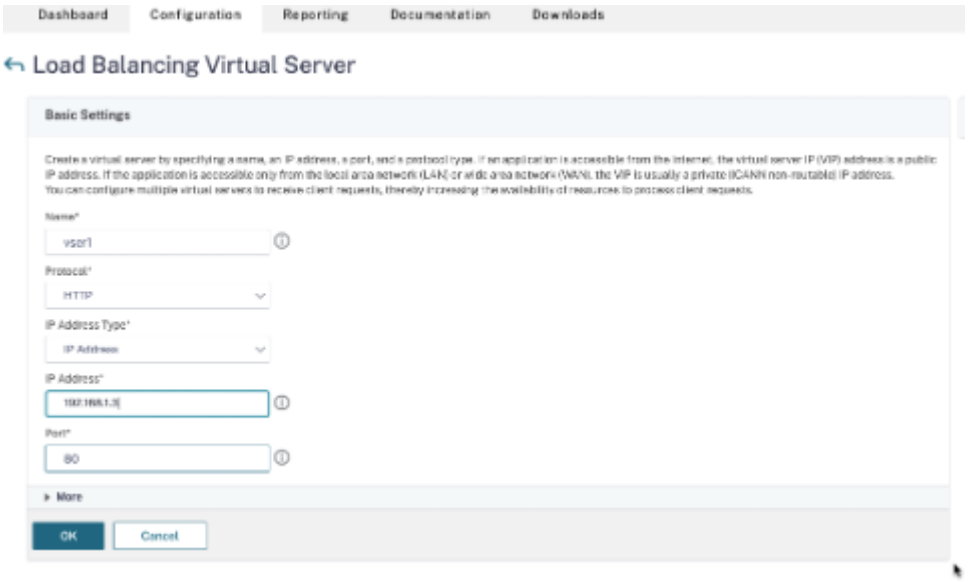


2. So erstellen Sie eine Client-Alias-IP-Adresse (VIP):
   - Geben Sie die Client-Alias-IP-Adresse und Netzmaske ein, die für das VPC-Subnetz in der VM-Instanz konfiguriert sind.
   - Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
   - Klicken Sie auf **Erstellen**.
3. So erstellen Sie eine IP-Adresse (SNIP) des Server-Alias:
   - Geben Sie die IP-Adresse und Netzmaske des Server-Alias ein, die für das VPC-Subnetz in der VM-Instanz konfiguriert sind.

- Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
- Klicken Sie auf **Erstellen**.

Schritt 6. Fügen Sie einen virtuellen Lastenausgleichsserver hinzu.

1. Navigieren Sie in der Citrix ADC GUI zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (Clientalias-IP) und Port hinzu.
3. Klicken Sie auf **OK**, um den virtuellen Lastenausgleichsserver zu erstellen.



Schritt 7. Fügen Sie der VPX-Instanz einen Dienst oder eine Dienstgruppe hinzu.

1. Navigieren Sie in der Citrix ADC GUI zu **Konfiguration > Traffic Management > Load Balancing > Services**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Dienstname, IP-Adresse, Protokoll und Port hinzu, und klicken Sie auf **OK**.

Schritt 8. Binden Sie die Service/Dienstgruppe an den virtuellen Load Balancing Server in der Instanz.

1. Navigieren Sie in der GUI zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den in **Schritt 6**konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Fenster **Service- und Dienstgruppen** auf **Keine Load Balancing Virtual Server-Dienstbindung**.
4. Wählen Sie den in **Schritt 7**konfigurierten Dienst aus und klicken Sie auf **Binden**.

Hinweise zu beachten, nachdem Sie die VPX-Instanz auf GCP bereitgestellt haben

- Melden Sie sich beim VPX mit Benutzernamen `nsroot` und Instanz-ID als Kennwort an. Ändern Sie an der Eingabeaufforderung das Kennwort und speichern Sie die Konfiguration.
- Um ein Paket für den technischen Support zu sammeln, führen Sie den Befehl `shell /netscaler/showtech_cloud.pl` anstelle des üblichen aus `show techsupport`.
- Löschen Sie nach dem Löschen einer Citrix ADC VM von der GCP-Konsole auch die zugehörige interne Zielinstanz von Citrix ADC. Gehen Sie dazu zur gcloud CLI und geben Sie den folgenden Befehl ein:

```
1  gcloud compute -q  target-instances delete <instance-name>-
      adcinternal --zone <zone>
2  <!--NeedCopy-->
```

> Hinweis: `<instance-name>-adcinternal` ist der Name der Zielinstanz, die gelöscht werden muss.

Citrix ADC VPX-Lizenzierung

Eine Citrix ADC VPX-Instanz auf GCP benötigt eine Lizenz. Die folgenden Lizenzierungsoptionen sind für Citrix ADC VPX-Instanzen verfügbar, die auf GCP ausgeführt werden.

- **Abonnementbasierte Lizenzierung**: Citrix ADC VPX Appliances sind als kostenpflichtige Instanzen auf dem GCP-Marktplatz verfügbar. Abonnementbasierte Lizenzierung ist eine Pay-as-you-go-Option. Benutzer werden stündlich berechnet. Die folgenden VPX-Modelle und Lizenz-Editionen sind auf dem GCP-Marktplatz verfügbar.

  |VPX-Modell|Lizenz-Editionen|
  |—|—|
  |VPX10| Standard, Fortgeschritten, Premium|
  | |

- **Bringen Sie Ihre eigene Lizenz (BYOL)**mit: Wenn Sie Ihre eigene Lizenz (BYOL) mitbringen, lesen Sie den VPX Licensing Guide unter http://support.citrix.com/article/CTX122426. Sie müssen:
  - Verwenden Sie das Lizenzportal auf der Citrix Website, um eine gültige Lizenz zu generieren.
  - Laden Sie die Lizenz auf die Instanz hoch.
- **Citrix ADC VPX Check-In/Auschecken Lizenzierung**: Weitere Informationen finden Sie unter Citrix ADC VPX Check-In/Auschecken Lizenzierung.

VPX Express für lokale und Cloud-Bereitstellungen erfordert keine Lizenzdatei. Weitere Informationen zu Citrix ADC VPX Express finden Sie im Abschnitt "Citrix ADC VPX Express-Lizenz" in der Übersicht über die Citrix ADC Lizenzierung.

GDM-Vorlagen zur Bereitstellung einer Citrix ADC VPX-Instanz

Sie können eine Citrix ADC VPX Google Deployment Manager (GDM) -Vorlage verwenden, um eine VPX-Instanz auf GCP bereitzustellen. Weitere Informationen finden Sie unter Citrix ADC GDM Templates.

Citrix ADC Marketplace-Images

Sie können die Images in GDM-Vorlagen verwenden, um die Citrix ADC-Appliance aufzurufen.

In der folgenden Tabelle sind die Images aufgeführt, die auf dem GCP Marketplace verfügbar sind.

Release	Imagename	Imageort
13.0	citrix-adc-vpx-10-enterprise-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-10-enterprise-13-0-83-29
13.0	citrix-adc-vpx-10-platinum-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-10-platinum-13-0-83-29
13.0	citrix-adc-vpx-10-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-10-standard-13-0-83-29
13.0	citrix-adc-vpx-200-enterprise-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-200-enterprise-13-0-83-29
13.0	citrix-adc-vpx-200-platinum-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-200-platinum-13-0-83-29

Release	Imagename	Imageort
13.0	citrix-adc-vpx-200-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-200-standard-13-0-83-29
13.0	citrix-adc-vpx-1000-advanced-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-advanced-13-0-83-29
13.0	citrix-adc-vpx-1000-premium-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-premium-13-0-83-29
13.0	citrix-adc-vpx-1000-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-1000-standard-13-0-83-29
13.0	citrix-adc-vpx-3000-enterprise-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-enterprise-13-0-83-29
13.0	citrix-adc-vpx-3000-platinum-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-platinum-13-0-83-29
13.0	citrix-adc-vpx-3000-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-3000-standard-13-0-83-29
13.0	citrix-adc-vpx-5000-enterprise-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-enterprise-13-0-83-29
13.0	citrix-adc-vpx-5000-platinum-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-platinum-13-0-83-29

Release	Imagename	Imageort
13.0	citrix-adc-vpx-5000-standard-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-5000-standard-13-0-83-29
13.0	citrix-adc-vpx-byol-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-byol-13-0-83-29
13.0	citrix-adc-vpx-express-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-express-13-0-83-29
13.0	citrix-adc-vpx-waf-1000-13-0-83-29	projects/citrix-master-project/global/images/citrix-adc-vpx-waf-1000-13-0-83-29

Ressourcen

- Erstellen von Instanzen mit mehreren Netzwerkschnittstellen
- Erstellen und Starten einer VM-Instanz

Verwandte Informationen

- Stellen Sie ein VPX-Paar mit hoher Verfügbarkeit auf der Google Cloud Platform bereit

Bereitstellen eines VPX-Hochverfügbarkeitspaars auf der Google Cloud Platform

October 5, 2021

Sie können zwei Citrix ADC VPX Instanzen auf Google Cloud Platform (GCP) als Aktiv-Passiv-Paar für hohe Verfügbarkeit (HA) konfigurieren. Wenn Sie eine Instanz als primären Knoten und die andere als sekundären Knoten konfigurieren, akzeptiert der primäre Knoten Verbindungen und verwaltet Server. Der sekundäre Knoten überwacht den primären. Wenn der primäre Knoten aus irgendeinem Grund keine Verbindungen akzeptieren kann, übernimmt der sekundäre Knoten.

Weitere Informationen zu HA finden Sie unter Hochverfügbarkeit.

Die Knoten müssen sich in derselben Region befinden; sie können sich jedoch entweder in derselben Zone oder in verschiedenen Zonen befinden. Weitere Informationen finden Sie unter Regionen und Zonen.

Jede VPX-Instanz benötigt mindestens drei IP-Subnetze (Google VPC-Netzwerke):

- Ein Management-Subnetz
- Ein Client-Subnetz (VIP)
- Ein Backend-Subnetz (SNIP, MIP usw.)

Citrix empfiehlt drei Netzwerkschnittstellen für eine Standard-VPX-Instanz.

Sie können ein VPX-Hochverfügbarkeitspaar mit den folgenden Methoden bereitstellen:

- Verwendung externer statischer IP-Adresse
- Private IP-Adresse verwenden

GDM-Vorlagen zum Bereitstellen eines VPX-Hochverfügbarkeitspaars auf GCP

Sie können eine Citrix ADC Google Deployment Manager (GDM) -Vorlage verwenden, um ein VPX-Hochverfügbarkeitspaar auf GCP bereitzustellen. Weitere Informationen finden Sie unter Citrix ADC GDM Templates.

Unterstützung von Weiterleitungsregeln für VPX Hochverfügbarkeitspaar auf GCP

Sie können ein VPX Hochverfügbarkeitspaar auf dem GCP mithilfe von Weiterleitungsregeln bereitstellen.

Weitere Informationen zu Weiterleitungsregeln finden Sie unter Übersicht über Weiterleitungsregeln.

Voraussetzungen

- Die Weiterleitungsregeln müssen sich in derselben Region wie die VPX-Instanzen befinden.
- Zielinstanzen müssen sich in derselben Zone wie die VPX-Instanz befinden.
- Die Anzahl der Zielinstanzen für primäre und sekundäre Knoten muss übereinstimmen.

Beispiel:

Sie haben ein hochverfügbarkeitsstarkes Paar in der `us-east1` Region mit primärem VPX in `us-east1-b` Zone und sekundärem VPX in `us-east1-c` Zone. Eine Weiterleitungsregel wird für den primären VPX mit der Zielinstanz in `us-east1-b` Zone konfiguriert. Konfigurieren Sie eine Zielinstanz für die sekundäre VPX in `us-east1-c` Zone, um die Weiterleitungsregel bei Failover zu aktualisieren.

Einschränkungen

In der Hochverfügbarkeitsbereitstellung von VPX werden nur Weiterleitungsregeln unterstützt, die mit Zielinstanzen am Backend konfiguriert sind.

Stellen Sie ein VPX Hochverfügbarkeitspaar mit externer statischer IP-Adresse auf der Google Cloud Platform bereit

December 7, 2021

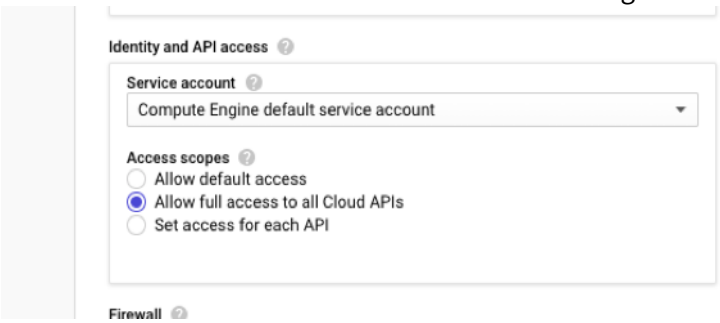
Sie können ein VPX-Paar mit hoher Verfügbarkeit auf GCP mit einer externen statischen IP-Adresse bereitstellen. Die Client-IP-Adresse des primären Knotens muss an eine externe statische IP-Adresse gebunden sein. Beim Failover wird die externe statische IP-Adresse auf den sekundären Knoten verschoben, damit der Datenverkehr fortgesetzt werden kann.

Eine statische externe IP-Adresse ist eine externe IP-Adresse, die für Ihr Projekt reserviert ist, bis Sie es freigeben möchten. Wenn Sie eine IP-Adresse für den Zugriff auf einen Dienst verwenden, können Sie diese IP-Adresse so reservieren, dass nur Ihr Projekt sie verwenden kann. Weitere Informationen finden Sie unter Reservieren einer statischen externen IP-Adresse.

Weitere Informationen zu HA finden Sie unter Hochverfügbarkeit.

Vorbereitung

- Lesen Sie die Beschränkung, Hardwareanforderungen und Hinweise, die unter Bereitstellen einer Citrix ADC VPX-Instanz auf Google Cloud Platformerwähnt werden. Diese Informationen gelten auch für HA-Bereitstellungen.
- Aktivieren Sie die **Cloud Resource Manager-API** für Ihr GCP-Projekt.
- Erlauben Sie beim Erstellen der Instanzen vollen Zugriff auf alle Cloud-APIs.



- Stellen Sie sicher, dass die mit Ihrem GCP-Dienstkonto verknüpfte IAM-Rolle die folgenden IAM-Berechtigungen besitzt:


```
REQUIRED_INSTANCE_IAM_PERMS = [

”compute.addresses.use”,
 “compute.forwardingRules.list” ,
 “compute.forwardingRules.setTarget” ,
 “compute.instances.setMetadata”
”compute.instances.addAccessConfig”,
”compute.instances.deleteAccessConfig”,
”compute.instances.get”,
”Compute.instances.list”,
”compute.networks.useExternalIp”,
”compute.subnetworks.useExternalIp”,
 “compute.targetInstances.list” ,
 “compute.targetInstances.use” ,
”compute.zones.list”,
]
<!--NeedCopy-->
```

- Wenn Sie Alias-IP-Adressen auf einer anderen Schnittstelle als der Verwaltungsschnittstelle konfiguriert haben, stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden zusätzlichen IAM-Berechtigungen verfügt:

```
”compute.instances.updateNetworkInterface”
<!--NeedCopy-->
```

- Wenn Sie GCP-Weiterleitungsregeln für den primären Knoten konfiguriert haben, lesen Sie die Einschränkungen und Anforderungen, die unter Unterstützung von Weiterleitungsregeln für VPX Hochverfügbarkeitspaar auf GCP aufgeführt sind, um sie beim Failover auf neue primäre Daten zu aktualisieren.

So stellen Sie ein VPX HA-Paar auf der Google Cloud Platform bereit

Hier ist eine Zusammenfassung der HA-Bereitstellungsschritte:

1. Erstellen Sie VPC-Netzwerke in derselben Region. Zum Beispiel Asien-Ost.
2. Erstellen Sie zwei VPX-Instanzen (primäre und sekundäre Knoten) in derselben Region. Sie können sich in derselben Zone oder verschiedenen Zonen befinden. Zum Beispiel Asia east-1a und Asia east-Ib.
3. Konfigurieren Sie HA-Einstellungen auf beiden Instanzen über die Citrix ADC GUI- oder ADC-CLI-Befehle.

Schritt 1. Erstellen von VPC-Netzwerken

Erstellen Sie VPC-Netzwerke basierend auf Ihren Anforderungen. Citrix empfiehlt Ihnen, drei VPC-Netzwerke für die Verknüpfung mit Verwaltungs-NIC, Client-NIC und Server-NIC zu erstellen.

Führen Sie die folgenden Schritte aus, um ein VPC-Netzwerk zu erstellen:

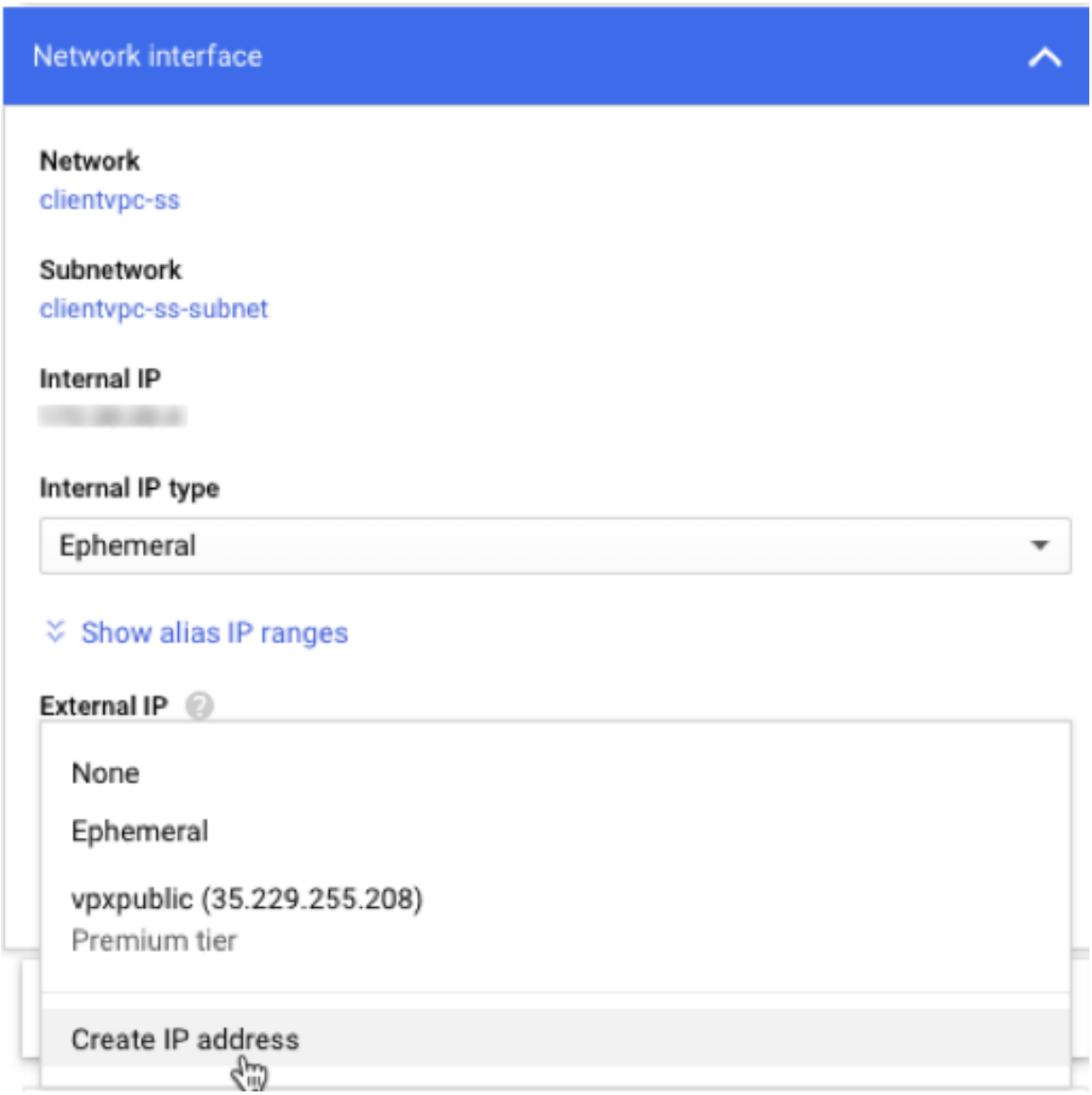
1. Melden Sie sich auf der **Google-Konsole an > Netzwerk > VPC-Netzwerk erstellen**.
2. Füllen Sie die erforderlichen Felder aus, und klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie im Abschnitt **Erstellen von VPC-Netzwerken** unter Bereitstellen einer Citrix ADC VPX-Instanz auf Google Cloud Platform.

Schritt 2. Erstellen Sie zwei VPX-Instanzen

Erstellen Sie zwei VPX-Instanzen, indem Sie die in Szenario angegebenen Schritte ausführen: Stellen Sie eine eigenständige VPX-Instanz mit mehreren NIC, Multi-IPbereit.

> **Wichtig**
>
> Weisen Sie der Client-IP-Adresse (VIP) des primären Knotens eine statische externe IP-Adresse zu. Sie können eine vorhandene reservierte IP-Adresse verwenden oder eine neue erstellen. Um eine statische externe IP-Adresse zu erstellen, navigieren Sie zu **Netzwerkschnittstelle > Externe IP**und klicken Sie auf **IP-Adresse erstellen**.



Wenn nach dem Failover der alte primäre neue sekundäre wird, wird die statische externe IP-Adresse von der alten primären IP-Adresse verschoben und an den neuen primären Server angeschlossen. Weitere Informationen finden Sie im Google Cloud-Dokument Reservieren einer statischen externen IP-Adresse.

Nachdem Sie die VPX-Instanzen konfiguriert haben, können Sie die VIP- und SNIP-Adressen konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von IP-Adressen im Besitz von Citrix ADC.

Schritt 3. Konfigurieren der Hochverfügbarkeit

Nachdem Sie die Instanzen auf der Google Cloud Platform erstellt haben, können Sie HA mithilfe der Citrix ADC GUI für CLI konfigurieren.

Konfigurieren von HA mit der GUI

Schritt 1. Richten Sie Hochverfügbarkeit im INC-Modus auf beiden Instanzen ein.

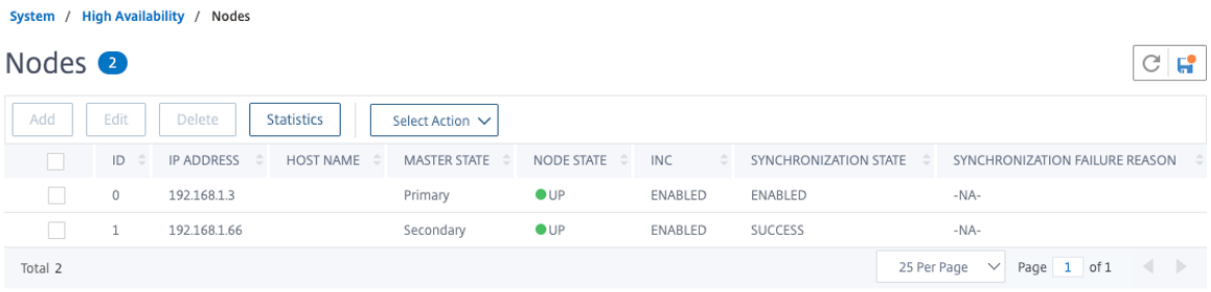
Führen Sie auf dem **primären Knoten**die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens von der GCP Console als Kennwort an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des sekundären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.

Führen Sie auf dem **sekundären Knoten**die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens von der GCP Console als Kennwort an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des primären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.

Bevor Sie fortfahren, stellen Sie sicher, dass der Synchronisationsstatus des sekundären Knotens auf der Seite **Knoten** als **SUCCESS** angezeigt wird.

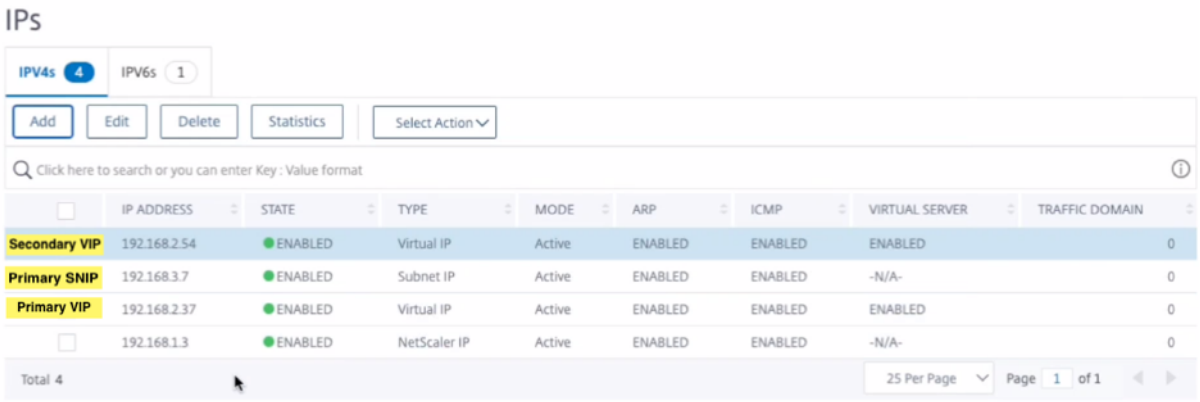


> **Hinweis:**
>
> Jetzt hat der sekundäre Knoten die gleichen Anmeldeinformationen wie der primäre Knoten.

Schritt 2. Fügen Sie auf beiden Knoten virtuelle IP-Adresse und Subnet-IP-Adresse hinzu.

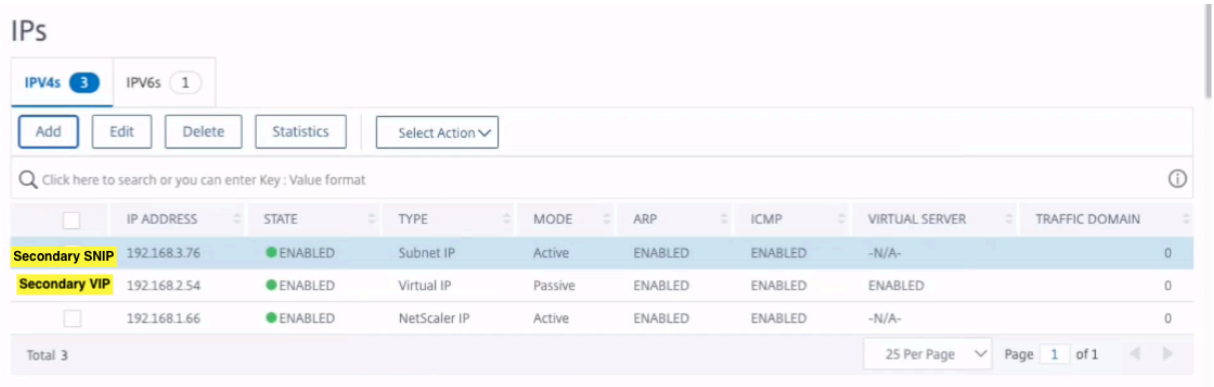
Führen Sie auf dem **primären Knoten**die folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie eine primäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der clientorientierten Schnittstelle der primären Instanz und Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert ist.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.
3. Fügen Sie eine primäre SNIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der serverorientierten Schnittstelle der Primärinstanz und Netzmaske ein, die für das Serversubnetz in der primären Instanz konfiguriert ist.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.
4. Fügen Sie eine sekundäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der clientorientierten Schnittstelle der sekundären Instanz und Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert ist.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.



Führen Sie auf dem **sekundären Knoten**die folgenden Schritte aus:

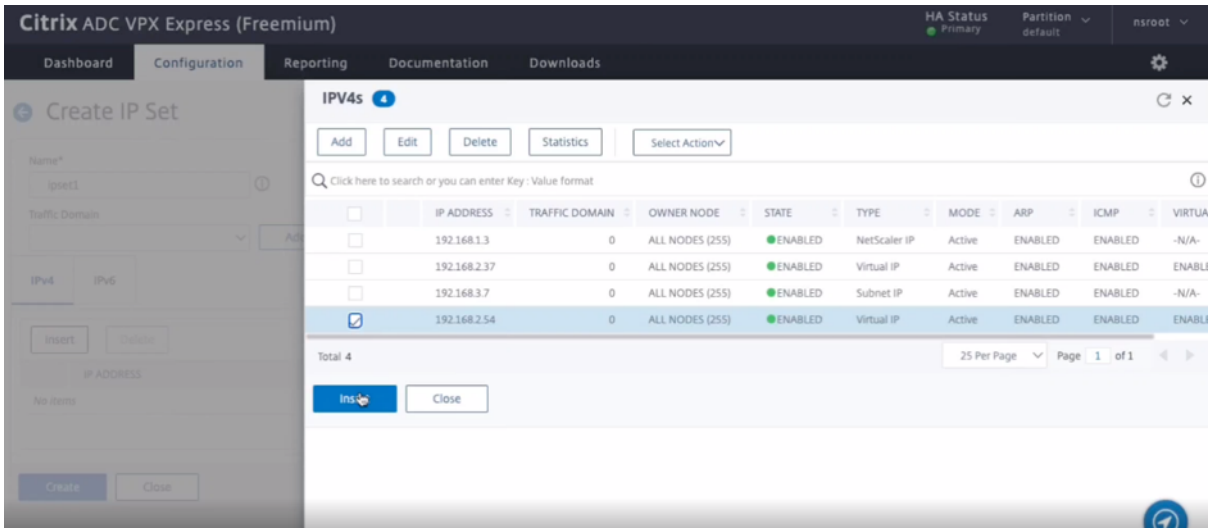
1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. Fügen Sie eine sekundäre VIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der clientorientierten Schnittstelle der sekundären Instanz und Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert ist.
   b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
3. Fügen Sie eine sekundäre SNIP-Adresse hinzu, indem Sie die folgenden Schritte ausführen:
   a) Geben Sie die interne IP-Adresse der serverorientierten Schnittstelle der sekundären Instanz und Netzmaske ein, die für das Serversubnetz in der sekundären Instanz konfiguriert ist.
   b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
   c) Klicken Sie auf **Erstellen**.



Schritt 3. Fügen Sie IP-Set hinzu und binden Sie die IP, die an den sekundären VIP auf beiden Instanzen festgelegt ist.

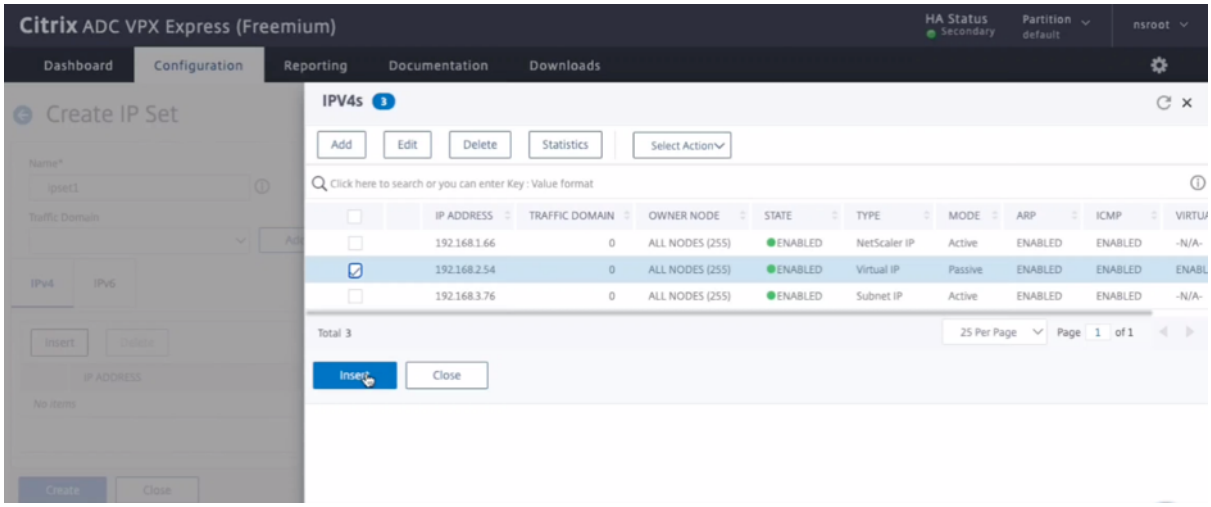
Führen Sie auf dem **primären Knoten**die folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IP-Sets > Hinzufügen**.
2. Fügen Sie einen IP-Set-Namen hinzu und klicken Sie auf **Einfügen**.
3. Wählen Sie auf der **IPv4s-Seite** die virtuelle IP (sekundäres VIP) aus und klicken Sie auf **Einfügen**.
4. Klicken Sie auf **Erstellen**, um den IP-Satz zu erstellen.



Führen Sie auf dem **sekundären Knoten**die folgenden Schritte aus:

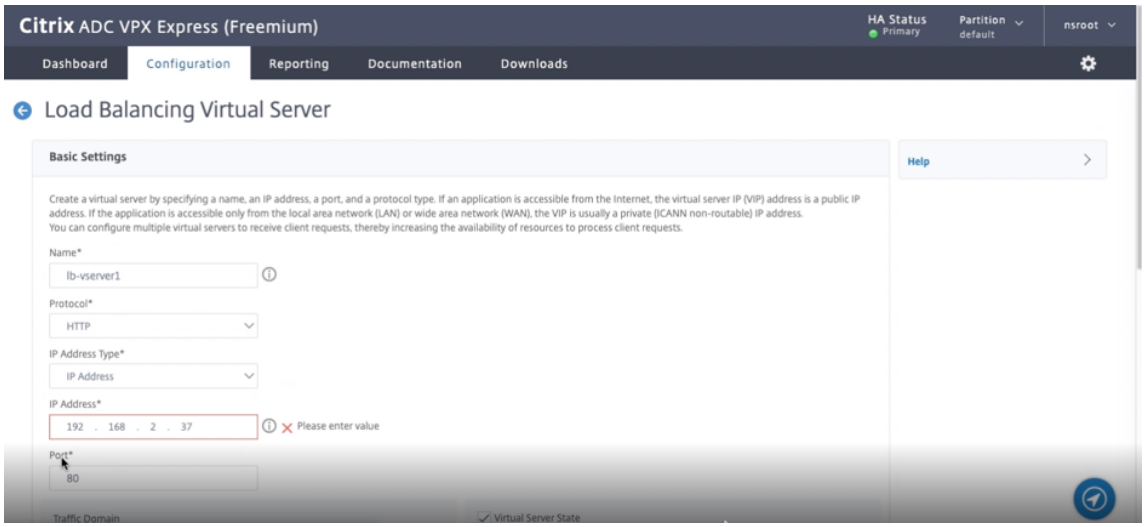
1. Navigieren Sie zu **System > Netzwerk > IP-Sets > Hinzufügen**.
2. Fügen Sie einen IP-Set-Namen hinzu und klicken Sie auf **Einfügen**.
3. Wählen Sie auf der **IPv4s-Seite** die virtuelle IP (sekundäres VIP) aus und klicken Sie auf **Einfügen**.
4. Klicken Sie auf **Erstellen**, um den IP-Satz zu erstellen.



> **Hinweis:**
>
> Der Name des IP-Sets muss auf beiden Instanzen identisch sein.

Schritt 4. Fügen Sie der primären Instanz einen virtuellen Lastausgleichsserver hinzu.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastenausgleich > Virtuelle Server > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (primäres VIP) und Port hinzu.



3. Klicken Sie auf **Mehr**. Navigieren Sie zu **IP-Bereichs-IP-Set-Einstellungen , wählen Sie im Dropdownmenü IPSet**aus und geben Sie das in**Schritt 3**erstellte IPSet ein.
4. Klicken Sie auf **OK**, um den virtuellen Lastenausgleichsserver zu erstellen.

Schritt 5. Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Services >**

Hinzufügen.

2. Fügen Sie die erforderlichen Werte für Servicename, IP-Adresse, Protokoll und Port hinzu und klicken Sie auf **OK**.

Schritt 6 Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf dem primären Knoten.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den in **Schritt 4**konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Registerkarte **Service- und Dienstgruppen** auf **Keine Load Balancing Virtual Server-Dienstbindung**.
4. Wählen Sie den in **Schritt 5**konfigurierten Dienst aus und klicken Sie auf " **Binden**".

Speichern Sie die Konfiguration. Nach einem erzwungenen Failover wird der sekundäre zum neuen primären. Die externe statische IP des alten primären VIP wechselt zum neuen sekundären VIP.

Konfigurieren der Hochverfügbarkeit mit CLI

Schritt 1. Richten Sie Hochverfügbarkeit im INC-Modus in beiden Instanzen ein.

Geben Sie auf dem primären Knoten den folgenden Befehl ein.

```
add ha node 1 <sec_ip> -inc ENABLED
<!--NeedCopy-->
```

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein.

```
add ha node 1 <prim_ip> -inc ENABLED
<!--NeedCopy-->
```

`sec_ip` bezieht sich auf die interne IP-Adresse der Verwaltungs-NIC des sekundären Knotens.

`prim_ip` bezieht sich auf die interne IP-Adresse der Verwaltungs-NIC des primären Knotens.

Schritt 2. Fügen Sie auf beiden Knoten virtuelle und Subnet-IPs hinzu.

Geben Sie auf dem primären Knoten den folgenden Befehl ein.

```
add ns ip <primary_vip> <subnet> -type VIP

add ns ip <secondary_vip> <subnet> -type VIP
```



```
4
5 add ns ip <primary_snip> <subnet> -type SNIP
6 <!--NeedCopy-->
```

primary_vip bezieht sich auf die interne IP-Adresse der clientorientierten Schnittstelle der primären Instanz.

secondary_vip bezieht sich auf die interne IP-Adresse der clientorientierten Schnittstelle der sekundären Instanz.

primary_snip bezieht sich auf die interne IP-Adresse der serverorientierten Schnittstelle der Primärinstanz.

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein.

```
1 add ns ip <secondary_vip> <subnet> -type VIP
2
3 add ns ip <secondary_snip> <subnet> -type SNIP
4 <!--NeedCopy-->
```

secondary_vip bezieht sich auf die interne IP-Adresse der clientorientierten Schnittstelle der sekundären Instanz.

secondary_snip bezieht sich auf die interne IP-Adresse der serverorientierten Schnittstelle der sekundären Instanz.

Schritt 3. Fügen Sie IP-Set hinzu und binden Sie IP, die auf beiden Instanzen an sekundären VIP eingestellt ist.

Geben Sie auf dem primären Knoten den folgenden Befehl ein:

```
1 add ipset <ipsetname>
2 bind ipset <ipsetname> <secondary VIP>
3 <!--NeedCopy-->
```

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein:

```
1 add ipset <ipsetname>
2 bind ipset <ipsetname> <secondary VIP>
3 <!--NeedCopy-->
```


> **Hinweis:**
>
> Der Name des IP-Sets muss auf beiden Instanzen identisch sein.

Schritt 4. Fügen Sie einen virtuellen Server auf der primären Instanz hinzu.

Geben Sie den folgenden Befehl ein:

```
add <server_type> vserver <vserver_name> <protocol> <primary_vip> <port
   > -ipset <ipset_name>
<!--NeedCopy-->
```

Schritt 5. Fügen Sie der primären Instanz einen Dienst oder eine Servicegruppe hinzu.

Geben Sie den folgenden Befehl ein:

```
add service <service_name> <service_ip_address> <protocol> <port>
<!--NeedCopy-->
```

Schritt 6 Binden Sie die Service/Dienstgruppe an den virtuellen Lastenausgleichsserver auf der primären Instanz.

Geben Sie den folgenden Befehl ein:

```
bind <server_type> vserver <vserver_name> <service_name>
<!--NeedCopy-->
```

> *Hinweis*:
>
> Geben Sie den Befehl `save config` ein, um die Konfiguration zu speichern. Andernfalls gehen die Konfigurationen verloren, nachdem Sie die Instanzen neu starten.

Schritt 7. Überprüfen Sie die Konfiguration.

Stellen Sie sicher, dass die an die primäre Client-NIC angehängte externe IP-Adresse bei einem Failover zur sekundären IP-Adresse wechselt.

1. Stellen Sie eine cURL-Anfrage an die externe IP-Adresse und stellen Sie sicher, dass sie erreichbar ist.
2. Führen Sie auf der primären Instanz Failover durch:

   Navigieren Sie in der GUI zu **Konfiguration > System > Hochverfügbarkeit > Aktion > Failover erzwingen**.

Geben Sie in der CLI den folgenden Befehl ein:

```
force ha failover -f
<!--NeedCopy-->
```

Navigieren Sie auf der GCP-Konsole zur sekundären Instanz. Die externe IP-Adresse muss nach dem Failover auf die sekundäre Client-NIC verschoben worden sein.

3. Stellen Sie eine cURL-Anforderung an die externe IP aus und stellen Sie sicher, dass sie wieder erreichbar ist.

Stellen Sie ein VPX-Hochverfügbarkeitspaar mit privater IP-Adresse auf der Google Cloud Platform bereit

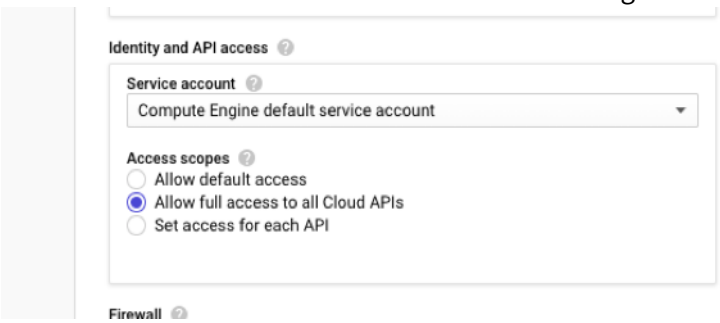
March 8, 2022

Sie können ein VPX-Hochverfügbarkeitspaar auf GCP mithilfe einer privaten IP-Adresse bereitstellen. Die Client-IP (VIP) muss als Alias-IP-Adresse auf dem primären Knoten konfiguriert sein. Beim Failover wird die Client-IP-Adresse auf den sekundären Knoten verschoben, damit der Datenverkehr wieder aufgenommen werden kann.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit.

Vorbereitung

- Lesen Sie die Beschränkung, Hardwareanforderungen und Hinweise, die unter Bereitstellen einer Citrix ADC VPX-Instanz auf Google Cloud Platformerwähnt werden. Diese Informationen gelten auch für Bereitstellungen mit hoher Verfügbarkeit.
- Aktivieren Sie die **Cloud Resource Manager-API** für Ihr GCP-Projekt.
- Erlauben Sie beim Erstellen der Instanzen vollen Zugriff auf alle Cloud-APIs.



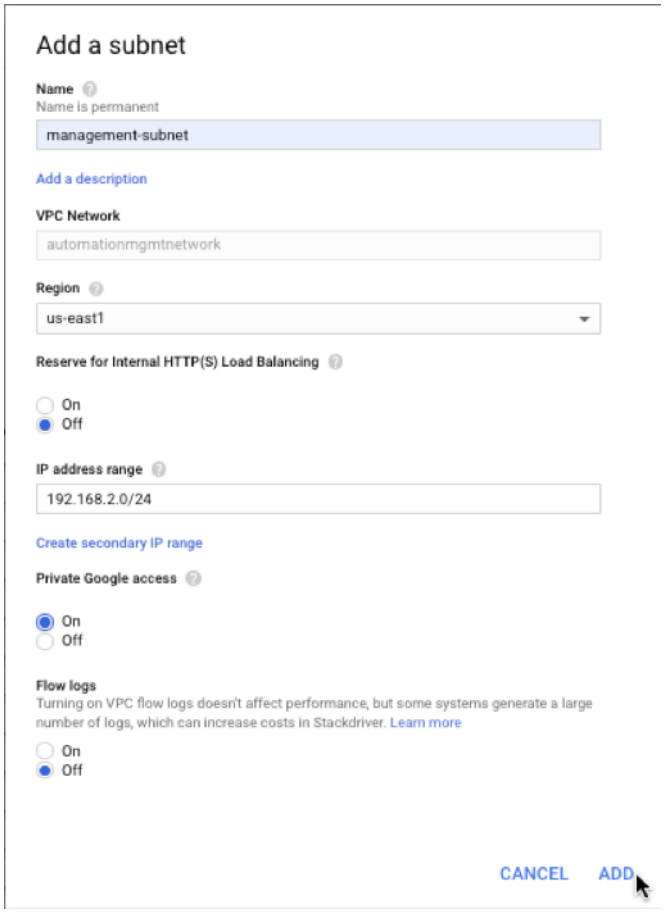
- Stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

```
REQUIRED_INSTANCE_IAM_PERMS = [
 “compute.forwardingRules.list” ,
 “compute.forwardingRules.setTarget” ,
 “compute.instances.setMetadata” ,
”compute.instances.get”,
”compute.instances.list”,
”compute.instances.updateNetworkInterface”,
 “compute.targetInstances.list” ,
 “compute.targetInstances.use” ,
”compute.zones.list”,
]
<!--NeedCopy-->
```

- Wenn Sie externe IP-Adressen auf einer anderen Schnittstelle als der Verwaltungsschnittstelle konfiguriert haben, stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden zusätzlichen IAM-Berechtigungen verfügt:

```
REQUIRED_INSTANCE_IAM_PERMS = [
”compute.addresses.use”
”compute.instances.addAccessConfig”,
”compute.instances.deleteAccessConfig”,
”compute.networks.useExternalIp”,
”compute.subnetworks.useExternalIp”,
]
<!--NeedCopy-->
```

- Wenn Ihre VMs keinen Internetzugang haben, müssen Sie **Private Google Access** im Verwaltungssubnetz aktivieren.



- Wenn Sie GCP-Weiterleitungsregeln für den primären Knoten konfiguriert haben, lesen Sie die Einschränkungen und Anforderungen, die unter Unterstützung von Weiterleitungsregeln für VPX Hochverfügbarkeitspaar auf GCP aufgeführt sind, um sie beim Failover auf neue primäre Daten zu aktualisieren.

So stellen Sie ein VPX Hochverfügbarkeitspaar auf der Google Cloud Platform bereit

Hier ist eine Zusammenfassung der Bereitstellungsschritte für hohe Verfügbarkeit:

1. Erstellen Sie VPC-Netzwerke in derselben Region. Zum Beispiel Asien-Ost.
2. Erstellen Sie zwei VPX-Instanzen (primäre und sekundäre Knoten) in derselben Region. Sie können sich in derselben Zone oder in verschiedenen Zonen befinden. Zum Beispiel Asia east-1a und Asia east-Ib.
3. Konfigurieren Sie Hochverfügbarkeitseinstellungen für beide Instanzen mit den Befehlen Citrix ADC-GUI oder ADC CLI-Befehle.

Schritt 1. Erstellen von VPC-Netzwerken

Erstellen Sie VPC-Netzwerke basierend auf Ihren Anforderungen. Citrix empfiehlt Ihnen, drei VPC-Netzwerke für die Verknüpfung mit Verwaltungs-NIC, Client-NIC und Server-NIC zu erstellen.

Führen Sie die folgenden Schritte aus, um ein VPC-Netzwerk zu erstellen:

1. Melden Sie sich auf der **Google-Konsole an > Netzwerk > VPC-Netzwerk > VPC-Netzwerk erstellen**.
2. Füllen Sie die erforderlichen Felder aus, und klicken Sie auf **Erstellen**.

Weitere Informationen finden Sie im Abschnitt **Erstellen von VPC-Netzwerken** unter Bereitstellen einer Citrix ADC VPX-Instanz auf Google Cloud Platform.

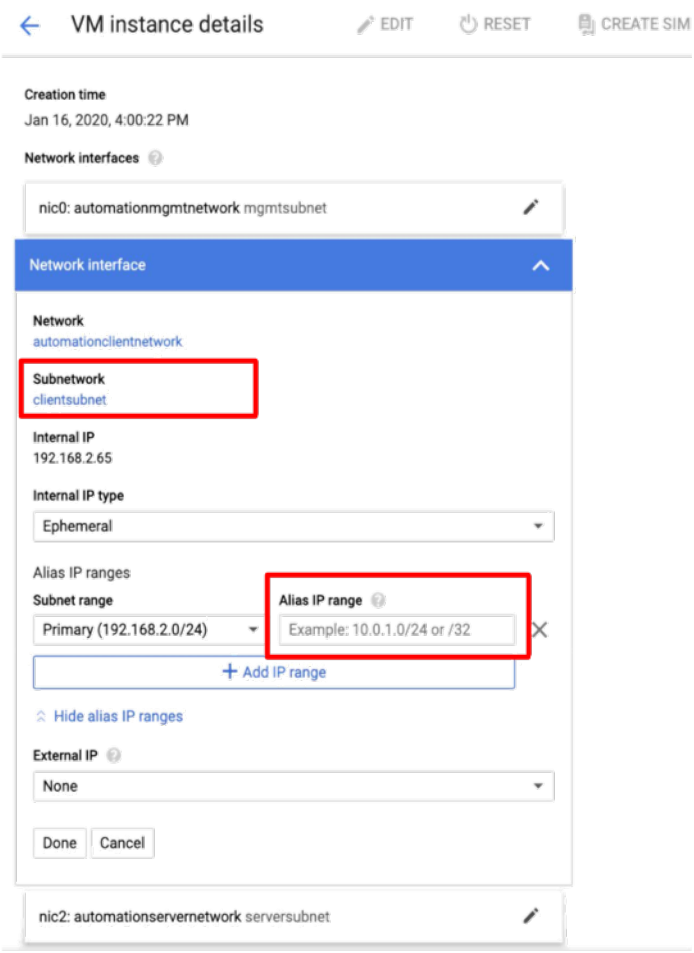
Schritt 2. Erstellen Sie zwei VPX-Instanzen

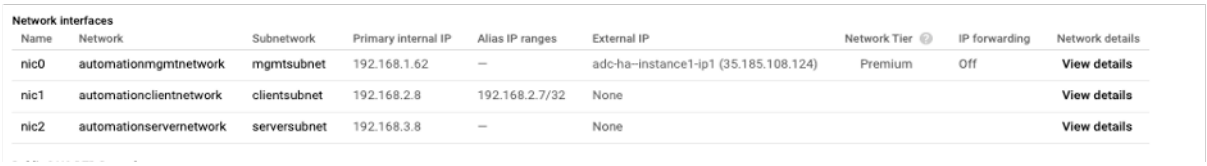
Erstellen Sie zwei VPX-Instanzen, indem Sie die in Szenario angegebenen Schritte ausführen: Stellen Sie eine eigenständige VPX-Instanz mit mehreren NIC, Multi-IPbereit.

> **Wichtig:**
>
> Weisen Sie dem primären Knoten eine Client-Alias-IP-Adresse zu. Verwenden Sie nicht die interne IP-Adresse der VPX-Instanz, um den VIP zu konfigurieren.

Führen Sie die folgenden Schritte aus, um eine Client-Alias-IP-Adresse zu erstellen:

1. Navigieren Sie zur VM-Instanz und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie im Fenster **Netzwerkschnittstelle** die Clientschnittstelle.
3. Geben Sie im Feld **Alias-IP-Bereich** die IP-Adresse des Client-Alias ein.





Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	automationmgmtnetwork	mgmtsubnet	192.168.1.62	–	adc-ha--instance1-ip1 (35.185.108.124)	Premium	Off	View details
nic1	automationclientnetwork	clientsubnet	192.168.2.8	192.168.2.7/32	None			View details
nic2	automationservernetwork	serversubnet	192.168.3.8	–	None			View details

Nach dem Failover, wenn der alte Primär zur neuen Sekundärgruppe wird, wechseln die Alias-IP-Adressen von der alten primären und sind an den neuen Primärbereich angehängt.

Nachdem Sie die VPX-Instanzen konfiguriert haben, können Sie die Virtual (VIP) und Subnet IP (SNIP) -Adressen konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von IP-Adressen im Besitz von Citrix ADC.

Schritt 3. Konfigurieren der Hochverfügbarkeit

Nachdem Sie die Instanzen auf der Google Cloud Platform erstellt haben, können Sie die Hochverfügbarkeit über die Citrix ADC-GUI oder CLI konfigurieren.

Konfigurieren der Hochverfügbarkeit mit der GUI

Schritt 1. Richten Sie die Hochverfügbarkeit im Modus INC Enabled auf beiden Knoten ein.

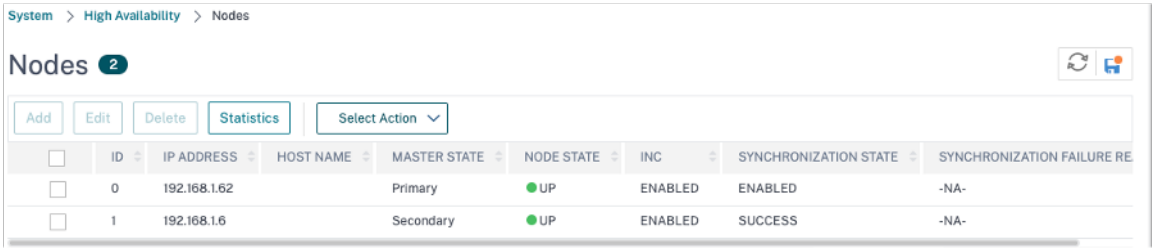
Führen Sie auf dem **primären Knoten**die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens von der GCP Console als Kennwort an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des sekundären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.

Führen Sie auf dem **sekundären Knoten**die folgenden Schritte aus:

1. Melden Sie sich bei der Instanz mit dem Benutzernamen `nsroot` und der Instanz-ID des Knotens von der GCP Console als Kennwort an.
2. Navigieren Sie zu **Konfiguration > System > Hohe Verfügbarkeit > Knoten**, und klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **IP-Adresse des Remote-Knotens** die private IP-Adresse der Verwaltungs-NIC des primären Knotens ein.
4. Aktivieren Sie das Kontrollkästchen **Inc-Modus (Independent Network Configuration) auf Selbstknoten** aktivieren.
5. Klicken Sie auf **Erstellen**.

Bevor Sie fortfahren, stellen Sie sicher, dass der Synchronisationsstatus des sekundären Knotens auf der Seite **Knoten** als **SUCCESS** angezeigt wird.



> **Hinweis**
>
> Jetzt hat der sekundäre Knoten die gleichen Anmeldeinformationen wie der primäre Knoten.

Schritt 2 Fügen Sie auf beiden Knoten virtuelle IP-Adresse und Subnet-IP-Adresse hinzu.

Führen Sie auf dem primären Knotendie folgenden Schritte aus:

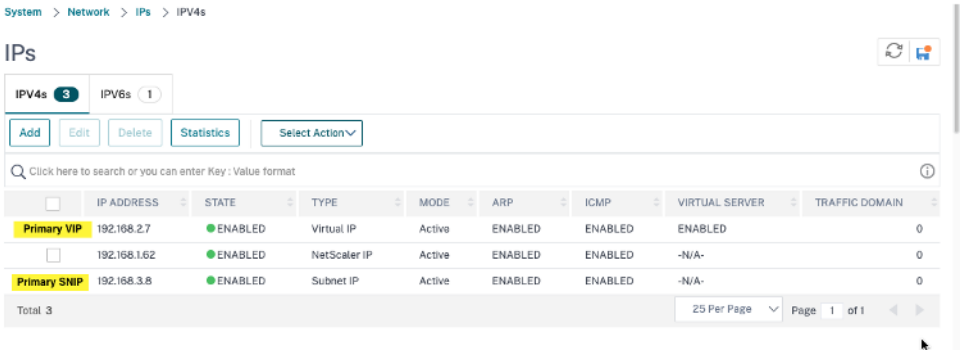
1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.

2. So erstellen Sie eine Client-Alias-IP-Adresse (VIP):

    a) Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert sind.
    b) Wählen Sie im Feld **IP-Typ** die Option **Virtuelle IP** aus dem Dropdownmenü aus.
    c) Klicken Sie auf **Erstellen**.

3. So erstellen Sie eine Server-IP-Adresse (SNIP):

    a) Geben Sie die interne IP-Adresse der serverorientierten Schnittstelle der Primärinstanz und Netzmaske ein, die für das Serversubnetz konfiguriert ist.
    b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
    c) Klicken Sie auf **Erstellen**.



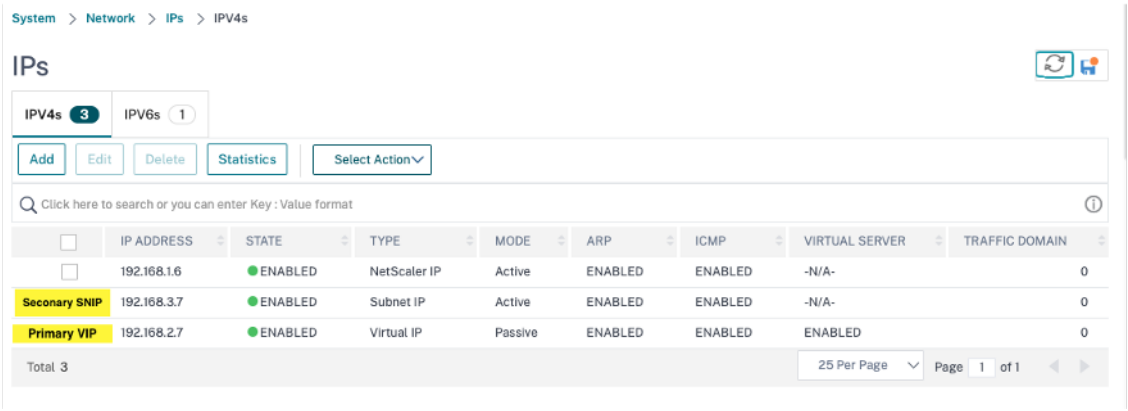
Führen Sie auf dem sekundären Knotendie folgenden Schritte aus:

1. Navigieren Sie zu **System > Netzwerk > IPs > IPv4s**, und klicken Sie auf **Hinzufügen**.
2. So erstellen Sie eine Client-Alias-IP-Adresse (VIP):

    a) Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der primären VM-Instanz konfiguriert sind.
    b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
    c) Klicken Sie auf **Erstellen**.

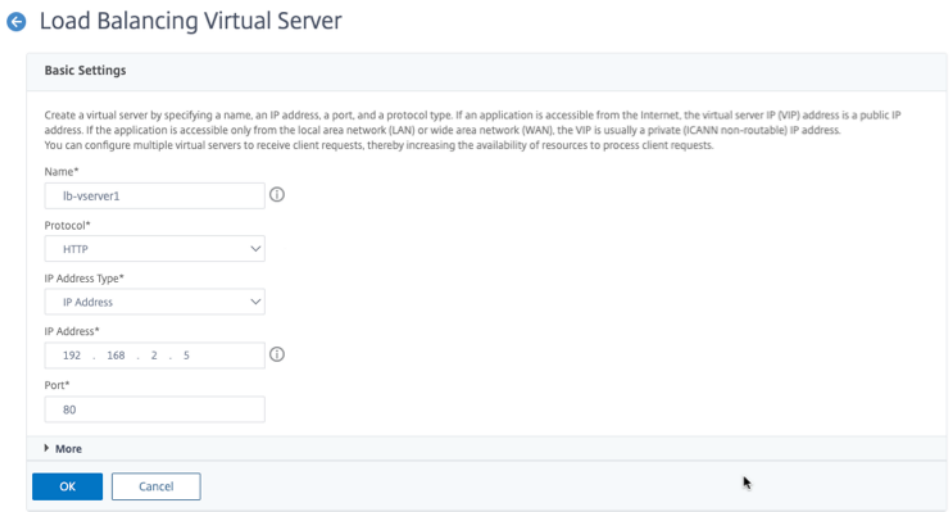
3. So erstellen Sie eine Server-IP-Adresse (SNIP):

    a) Geben Sie die interne IP-Adresse der serverorientierten Schnittstelle der sekundären Instanz und Netzmaske ein, die für das Serversubnetz konfiguriert ist.
    b) Wählen Sie im Feld **IP-Typ** die Option **Subnetz-IP** aus dem Dropdownmenü aus.
    c) Klicken Sie auf **Erstellen**.



Schritt 3. Fügen Sie einen virtuellen Lastausgleichsserver auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastenausgleich > Virtuelle Server > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (primäre Clientalias-IP-Adresse) und Port hinzu, und klicken Sie auf **OK**.



Schritt 4. Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Services > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Servicename, IP-Adresse, Protokoll und Port hinzu und klicken Sie auf **OK**.

Schritt 5. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf dem primären Knoten.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den in **Schritt 3**konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.

3. Klicken Sie auf der Registerkarte **Service- und Dienstgruppen** auf **Keine Load Balancing Virtual Server-Dienstbindung**.
4. Wählen Sie den in **Schritt 4**konfigurierten Dienst aus und klicken Sie auf “ **Binden**”.

Schritt 5. Speichern Sie die Konfiguration.

Nach einem erzwungenen Failover wird der sekundäre zum neuen primären. Die Client-Alias-IP (VIP) und die Server-Alias-IP (SNIP) von der alten primären wechselt zur neuen primären.

Konfigurieren Sie Hochverfügbarkeit über die CLI

Schritt 1. Richten Sie in beiden Instanzen die Hochverfügbarkeit im **INC-aktivierten** Modus mithilfe der Citrix ADC CLI ein.

Geben Sie auf dem primären Knoten den folgenden Befehl ein.

```
add ha node 1 <sec_ip> -inc ENABLED
<!--NeedCopy-->
```

Geben Sie auf dem sekundären Knoten den folgenden Befehl ein.

```
add ha node 1 <prim_ip> -inc ENABLED
<!--NeedCopy-->
```

Der `sec_ip` bezieht sich auf die interne IP-Adresse der Verwaltungs-NIC des sekundären Knotens.

Der `prim_ip` bezieht sich auf die interne IP-Adresse der Verwaltungs-NIC des primären Knotens.

Schritt 2 Fügen Sie VIP und SNIP auf beiden Knoten hinzu.

Geben Sie die folgenden Befehle auf den primären Knoten ein:

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP

<!--NeedCopy-->
```

> **Hinweis:**
>
> Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der VM-Instanz konfiguriert sind.


```
add ns ip <primary_snip> <subnet> -type SNIP
<!--NeedCopy-->
```

Der `primary_snip` bezieht sich auf die interne IP-Adresse der serverorientierten Schnittstelle der Primärinstanz.

Geben Sie die folgenden Befehle auf dem sekundären Knoten ein:

```
add ns ip <primary_client_alias_ip> <subnet> -type VIP
<!--NeedCopy-->
```

> Hinweis
>
> Geben Sie die Alias-IP-Adresse und die Netzmaske ein, die für das Client-Subnetz in der primären VM-Instanz konfiguriert sind.

```
add ns ip <secondary_snip> <subnet> -type SNIP
<!--NeedCopy-->
```

Der `secondary_snip` bezieht sich auf die interne IP-Adresse der serverorientierten Schnittstelle der sekundären Instanz.

> **Hinweis:**
>
> Geben Sie die IP-Adresse und Netzmaske ein, die für das Serversubnetz in der VM-Instanz konfiguriert sind.

Schritt 3. Fügen Sie einen virtuellen Server auf dem primären Knoten hinzu.

Geben Sie den folgenden Befehl ein:

```
add <server_type> vserver <vserver_name> <protocol> <
   primary_client_alias_ip> <port>
<!--NeedCopy-->
```

Schritt 4. Fügen Sie einen Dienst oder eine Dienstgruppe auf dem primären Knoten hinzu.

Geben Sie den folgenden Befehl ein:

```
add service <service_name> <service_ip_address> <protocol> <port>
<!--NeedCopy-->
```


Schritt 5. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastausgleichsserver auf dem primären Knoten.

Geben Sie den folgenden Befehl ein:

```
bind <server_type> vserver <vserver_name> <service_name>
<!--NeedCopy-->
```

> **Hinweis:**
>
> Um Ihre Konfiguration zu speichern, geben Sie den Befehl ein `save config`. Andernfalls gehen die Konfigurationen verloren, nachdem Sie die Instanzen neu starten.

Back-End-GCP-Autoskalierungsdienst hinzufügen

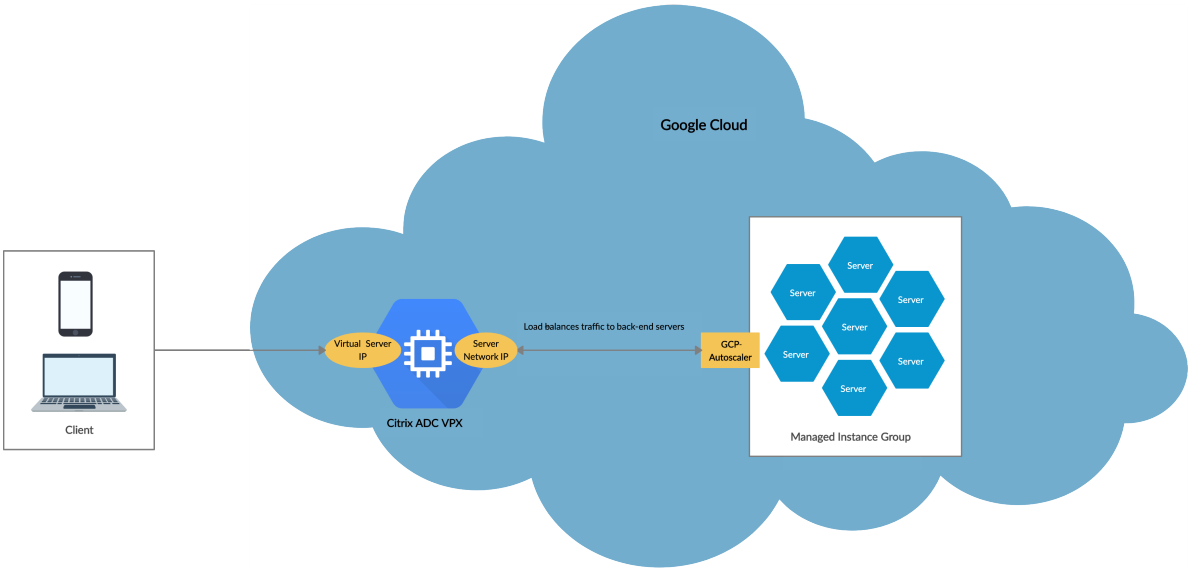
October 5, 2021

Effizientes Hosting von Anwendungen in einer Cloud erfordert eine einfache und kostengünstige Verwaltung der Ressourcen, je nach Anwendungsbedarf. Um der steigenden Nachfrage gerecht zu werden, müssen Sie die Netzwerkressourcen nach oben skalieren. Wenn der Bedarf nachlässt, müssen Sie nach unten skalieren, um unnötige Kosten für nicht ausgelastete Ressourcen zu vermeiden. Um die Kosten für die Ausführung der Anwendung zu minimieren, müssen Sie den Datenverkehr, den Arbeitsspeicher und die CPU-Nutzung ständig überwachen und so weiter. Die manuelle Überwachung des Datenverkehrs ist jedoch umständlich. Damit die Anwendungsumgebung dynamisch nach oben oder unten skaliert werden kann, müssen Sie die Prozesse der Überwachung des Datenverkehrs und der Skalierung von Ressourcen bei Bedarf automatisieren.

Die Citrix ADC VPX Instanz ist in den GCP-Autoskalierungsdienst integriert und bietet folgende Vorteile:

- **Lastausgleich und -verwaltung**: Automatisch konfiguriert Server so, dass sie je nach Bedarf hoch- und herunterskaliert werden. Die VPX-Instanz erkennt automatisch verwaltete Instanzgruppen im Backend-Subnetz und ermöglicht es Ihnen, die verwalteten Instanzgruppen auszuwählen, um die Last auszugleichen. Die virtuellen und Subnetz-IP-Adressen werden automatisch auf der VPX-Instanz konfiguriert.
- **Hohe Verfügbarkeit**: Erkennt verwaltete Instanzgruppen, die sich über mehrere Zonen und Lastausgleichsserver erstrecken.
- **Bessere Netzwerkverfügbarkeit**: Die VPX-Instanz unterstützt:
  - Back-End-Server in denselben Platzierungsgruppen
  - Back-End-Server in verschiedenen Zonen

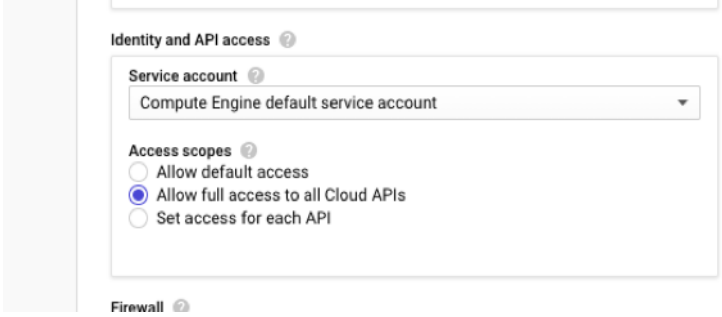
Dieses Diagramm veranschaulicht, wie der GCP-Autoskalierungsdienst in einer Citrix ADC VPX Instanz als virtueller Lastenausgleichsserver funktioniert.



Voraussetzungen

Bevor Sie Autoscaling mit der Citrix ADC VPX-Instanz verwenden, müssen Sie die folgenden Aufgaben ausführen.

- Erstellen Sie eine Citrix ADC VPX Instanz auf GCP entsprechend Ihren Anforderungen.
  - Weitere Informationen zum Erstellen einer Citrix ADC VPX-Instanz finden Sie unter Bereitstellen einer Citrix ADC VPX-Instanz auf der Google Cloud Platform.
  - Weitere Informationen zur Bereitstellung von VPX-Instanzen im HA-Modus finden Sie unter Bereitstellen eines VPX-Hochverfügbarkeitspaares auf der Google Cloud Platform.
- Aktivieren Sie die **Cloud Resource Manager-API** für Ihr GCP-Projekt.
- Erlauben Sie beim Erstellen der Instanzen vollen Zugriff auf alle Cloud-APIs.



- Stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:


```
REQUIRED_INSTANCE_IAM_PERMS = [

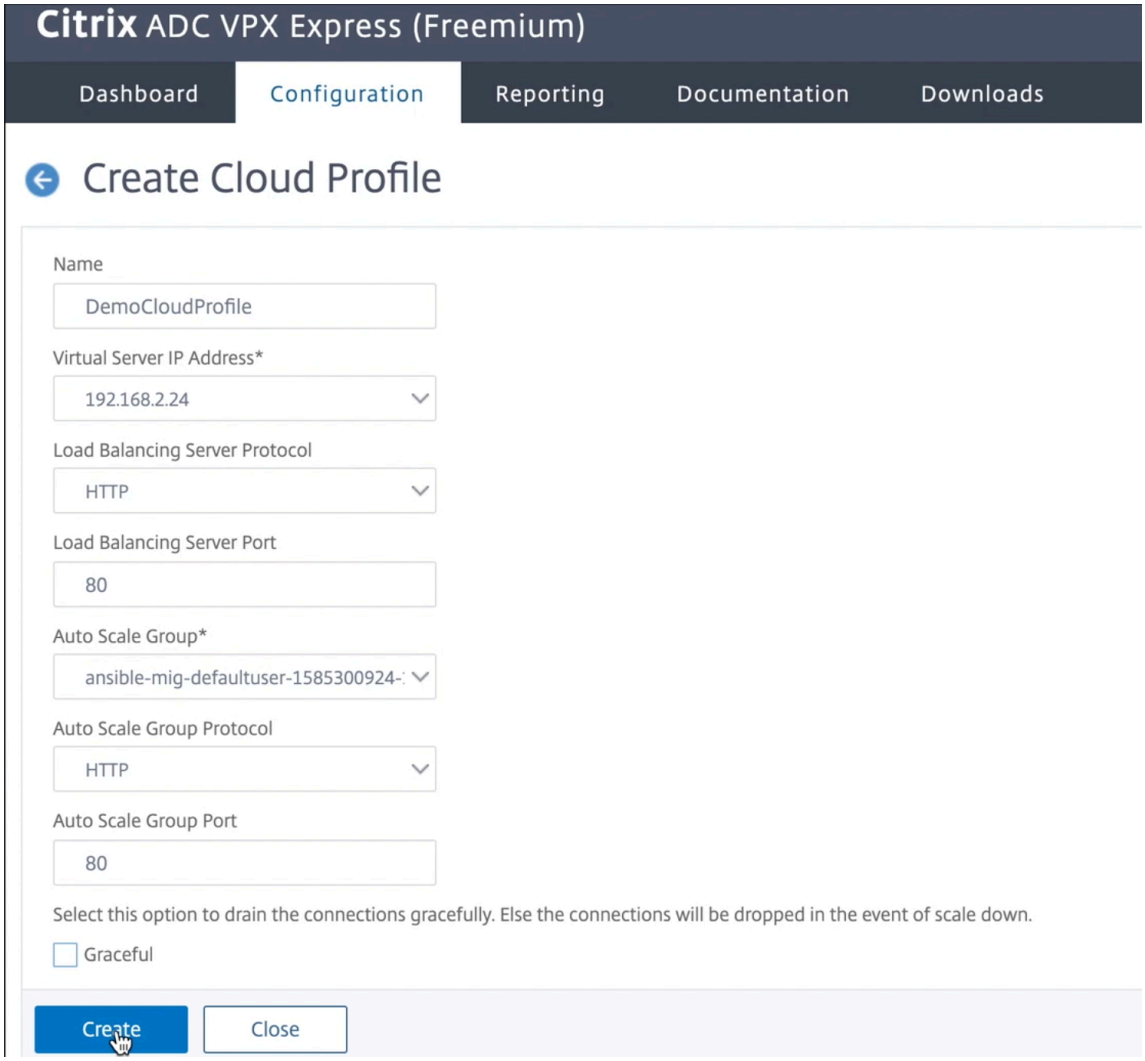
"compute.instances.get",
"compute.zones.list",
"compute.instanceGroupManagers.list",
"compute.instanceGroupManagers.get"
]
<!--NeedCopy-->
```

- Um die automatische Skalierung einzurichten, stellen Sie sicher, dass Folgendes konfiguriert ist:
  - Instanz-Vorlage
  - Gruppe “Verwaltete Instanz”
  - Richtlinie für die automatische Skalierung

Hinzufügen des GCP-Autoskalierungsdiensts zu einer Citrix ADC VPX Instanz

Sie können den Autoscaling-Dienst einer VPX-Instanz mit einem einzigen Klick mit der GUI hinzufügen. Führen Sie die folgenden Schritte aus, um der VPX-Instanz den Autoscaling-Dienst hinzuzufügen:

1. Melden Sie sich bei der VPX-Instanz an, indem Sie Ihre Anmeldeinformationen für verwendennsroot.
2. Wenn Sie sich zum ersten Mal bei der Citrix ADC VPX-Instanz anmelden, wird die standardmäßige Cloud-Profilseite angezeigt. Wählen Sie die GCP-verwaltete Instanzgruppe aus dem Dropdownmenü aus, und klicken Sie auf **Erstellen**, um ein Cloud-Profil zu erstellen.

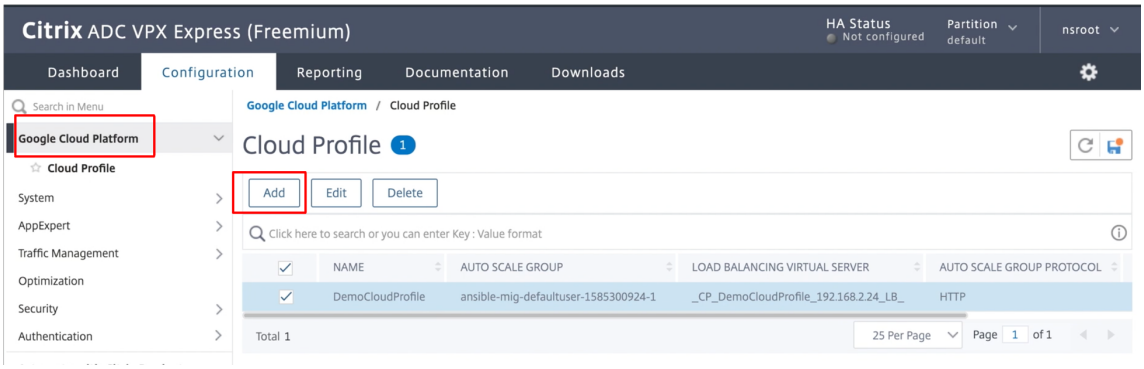


- Das Feld **IP-Adresse des virtuellen Servers** wird automatisch von allen IP-Adressen ausgefüllt, die den Instanzen zugeordnet sind.
- Die **Autoscale Group** wird aus der verwalteten Instanzgruppe vorausgefüllt, die für Ihr GCP-Konto konfiguriert ist.
- Stellen Sie bei der Auswahl von **Autoscale Group Protocol** und **Autoscale Group Port**sicher, dass die Server das konfigurierte Protokoll und die konfigurierten Ports überwachen. Binden Sie den richtigen Monitor in der Dienstgruppe. Standardmäßig wird der TCP-Monitor verwendet.
- Deaktivieren Sie das Kontrollkästchen **Ordnungsgemäß**, da es nicht unterstützt wird.

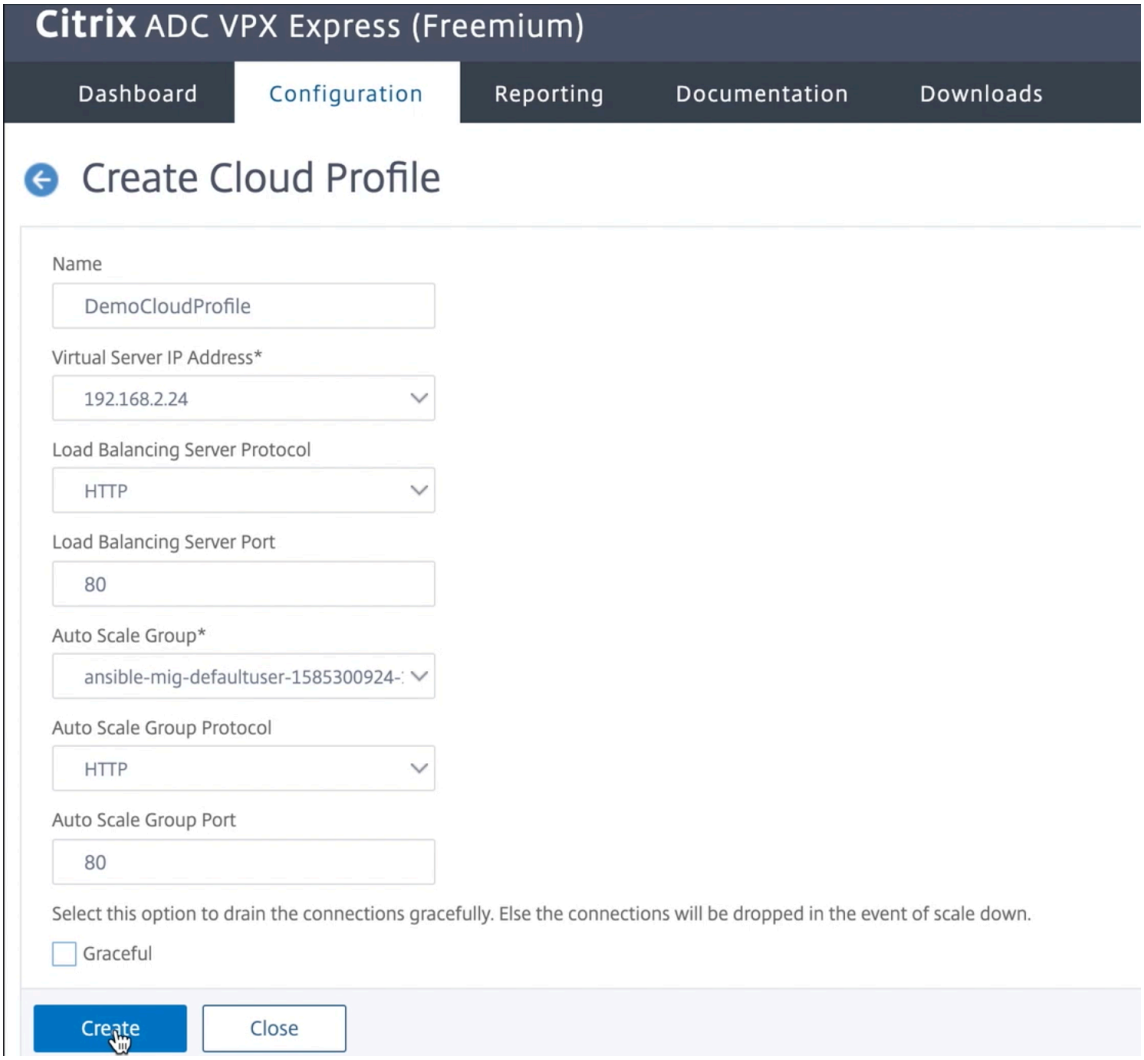
> Hinweis:
>
> Beim SSL-Protokolltyp Autoskalierung ist nach dem Erstellen des Cloud-Profils der virtuelle Lastenausgleich Server oder die Dienstgruppe aufgrund eines fehlenden Zertifikats heruntergefahren. Sie können das Zertifikat manuell an den virtuellen Server oder

> die Dienstgruppe binden.

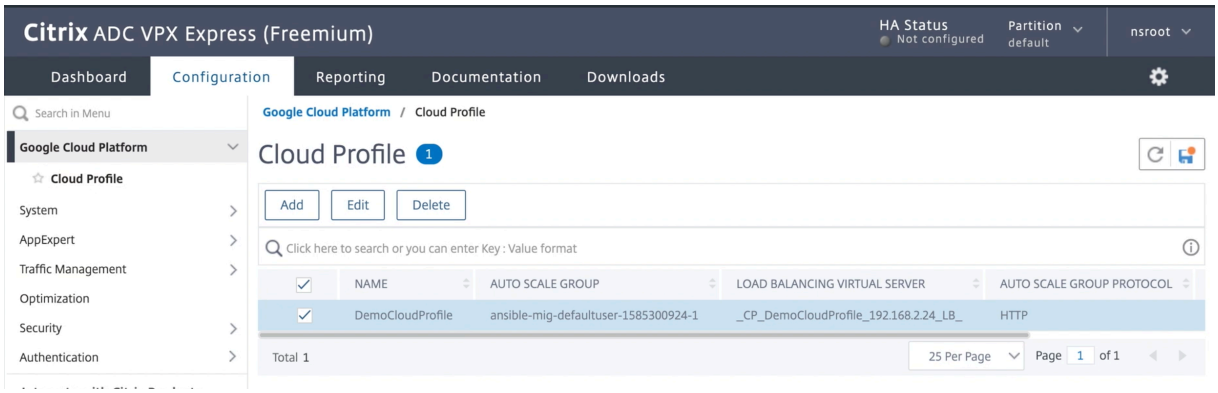
3. Nach der ersten Anmeldung, wenn Sie ein Cloud-Profil erstellen möchten, gehen Sie auf der Benutzeroberfläche zu **System > Google Cloud Platform > Cloud-Profil** und klicken Sie auf **Hinzufügen**.



Die Seite **Cloud-Profil erstellen** wird angezeigt.



Cloud Profile erstellt einen virtuellen Citrix ADC Lastenausgleich und eine Dienstgruppe mit Mitgliedern als Server der verwalteten Instanzgruppe. Ihre Back-End-Server müssen über das auf der VPX-Instanz konfigurierte SNIP erreichbar sein.



Unterstützung für VIP-Skalierung für Citrix ADC VPX-Instanz auf GCP

October 5, 2021

Eine Citrix ADC-Appliance befindet sich zwischen den Clients und den Servern, sodass Clientanfragen und Serverantworten sie durchlaufen. In einer typischen Installation stellen virtuelle Server, die auf der Appliance konfiguriert sind, Verbindungspunkte bereit, mit denen Clients auf die Anwendungen hinter der Appliance zugreifen. Die Anzahl der öffentlichen virtuellen IP-Adressen (VIP), die für eine Bereitstellung benötigt werden, variiert von Fall zu Fall.

Die GCP-Architektur schränkt jede Schnittstelle der Instanz ein, die mit einer anderen VPC verbunden werden soll. Eine VPC auf GCP ist eine Sammlung von Subnetzen, und jedes Subnetz kann sich über Zonen einer Region erstrecken. Darüber hinaus legt GCP die folgende Einschränkung vor:

- Es gibt eine 1:1 -Zuordnung der Anzahl öffentlicher IP-Adressen zur Anzahl der NICs. Einer NIC kann nur eine öffentliche IP-Adresse zugewiesen werden.
- An einem Instanztyp mit höherer Kapazität können maximal 8 NICs angeschlossen werden.

Zum Beispiel kann eine n1-Standard-2-Instanz nur 2 NICs haben, und die öffentlichen VIPs, die hinzugefügt werden können, sind auf 2 beschränkt. Weitere Informationen finden Sie unter VPC-Ressourcenkontingente.

Um höhere Maßstäbe öffentlicher virtueller IP-Adressen auf einer Citrix ADC VPX-Instanz zu erreichen, können Sie die VIP-Adressen als Teil der Metadaten der Instanz konfigurieren. Die ADC VPX-Instanz verwendet intern die vom GCP bereitgestellten Weiterleitungsregeln, um eine VIP-Skalierung zu erreichen. Die ADC VPX-Instanz bietet auch hohe Verfügbarkeit für die konfigurierten VIPs.
Nachdem Sie VIP-Adressen als Teil der Metadaten konfiguriert haben, können Sie einen virtuellen LB-Server mit derselben IP konfigurieren, die zum Erstellen der Weiterleitungsregeln verwendet wird.

Daher können wir Weiterleitungsregeln verwenden, um die Einschränkungen zu minimieren, die wir bei der Verwendung öffentlicher VIP-Adressen auf einer ADC VPX-Instanz auf GCP haben.

Weitere Informationen zu Weiterleitungsregeln finden Sie unter Übersicht über Weiterleitungsregeln.

Weitere Informationen zu HA finden Sie unter Hochverfügbarkeit.

Beachtenswerte Punkte

- Google berechnet einige zusätzliche Kosten für jede virtuelle IP-Weiterleitungsregel. Die tatsächlichen Kosten hängen von der Anzahl der erstellten Einträge ab. Die damit verbundenen Kosten entnehmen Sie den Google-Preisdokumenten.
- Die Weiterleitungsregeln gelten nur für öffentliche VIPs. Sie können Alias-IP-Adressen verwenden, wenn die Bereitstellung private IP-Adressen als VIPs benötigt.
- Sie können Weiterleitungsregeln nur für die Protokolle erstellen, die den virtuellen LB-Server benötigen. VIPs können im laufenden Betrieb erstellt, aktualisiert oder gelöscht werden. Sie können auch einen neuen virtuellen Lastausgleichsserver mit derselben VIP-Adresse, jedoch mit einem anderen Protokoll hinzufügen.

Vorbereitung

- Die Citrix ADC VPX-Instanz muss auf GCP bereitgestellt werden.
- Die externe IP-Adresse muss reserviert werden. Weitere Informationen finden Sie unter Reservieren einer statischen externen IP-Adresse.
- Stellen Sie sicher, dass Ihr GCP-Dienstkonto über die folgenden IAM-Berechtigungen verfügt:

```
REQUIRED_IAM_PERMS = [
”compute.addresses.list”,
”compute.addresses.get”,
”compute.addresses.use”,
”compute.forwardingRules.create”,
”compute.forwardingRules.delete”,
”compute.forwardingRules.get”,
”compute.forwardingRules.list”,
”compute.instances.use”,
”compute.subnetworks.use”,
”compute.targetInstances.create”
”compute.targetInstances.get”
”compute.targetInstances.use”,
]

```



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

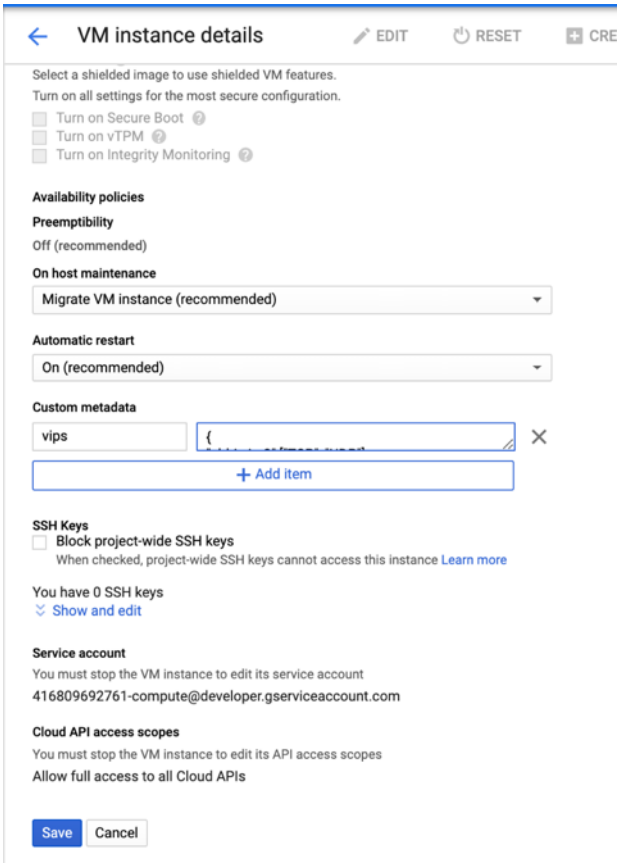
Konfigurieren externer IP-Adressen für die VIP-Skalierung auf der Citrix ADC VPX-Instanz

1. Navigieren Sie in der Google Cloud Console zur Seite **VM-Instanzen** .
2. Erstellen Sie eine neue VM-Instanz oder verwenden Sie eine vorhandene Instanz.
3. Klicken Sie auf den Instanznamen. Klicken Sie auf der **Detailseite der VM-Instanz** auf **Bearbeiten**.
4. Aktualisieren Sie die **benutzerdefinierten Metadaten**, indem Sie Folgendes eingeben:
   - Schlüssel = vips
   - Value = Geben Sie einen Wert im folgenden JSON-Format an:

     {
     “Name der externen reservierten IP”: [Liste der Protokolle],
     }

   GCP unterstützt die folgenden Protokolle:

   - AH
   - ESP
   - ICMP
   - SCT
   - TCP
   - UDP



Weitere Informationen finden Sie unter Benutzerdefinierte Metadaten.

Beispiel für benutzerdefinierte Metadaten:

{
“external-ip1-name”:[“TCP”, “UDP”],
“external-ip2-name”:[“ICMP”, “AH”]
}

In diesem Beispiel erstellt die ADC VPX-Instanz intern eine Weiterleitungsregel für jedes IP, Protokollpaar. Die Metadateneinträge werden den Weiterleitungsregeln zugeordnet. Dieses Beispiel hilft Ihnen zu verstehen, wie viele Weiterleitungsregeln für einen Metadateneintrag erstellt werden.

Vier Weiterleitungsregeln werden wie folgt erstellt:

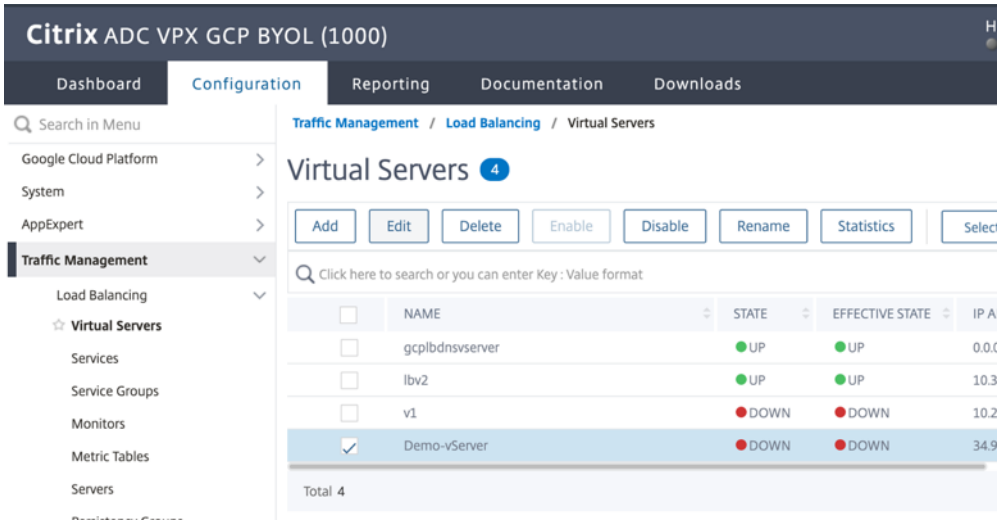
a) external-ip1-Name und TCP
b) external-ip1-Name und UDP
c) external-ip2-name und ICMP
d) external-ip2-name und AH

5. Klicken Sie auf **Speichern**.

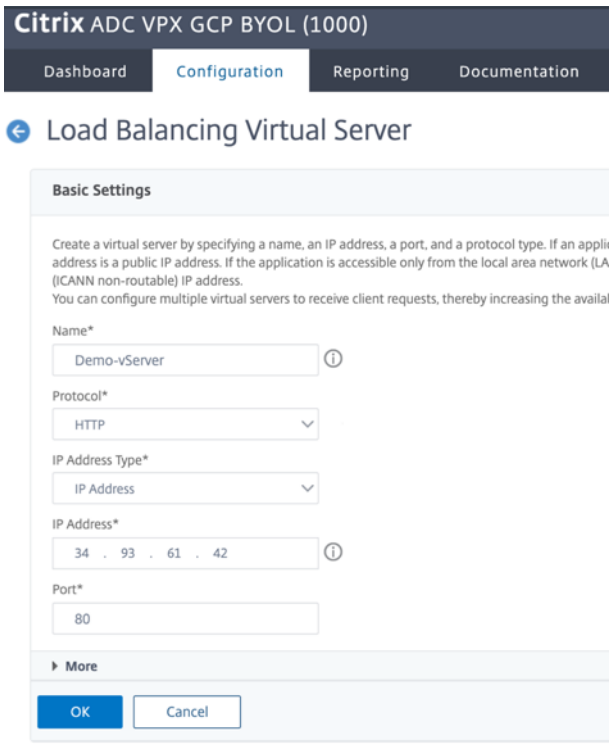
Einrichten eines virtuellen Lastausgleichsservers mit externer IP-Adresse auf einer Citrix ADC VPX-Instanz

Schritt 1. Fügen Sie einen virtuellen Lastenausgleichsserver hinzu.

1. Navigieren Sie zu **Konfiguration > Datenverkehrsverwaltung > Lastenausgleich > Virtuelle Server > Hinzufügen**.

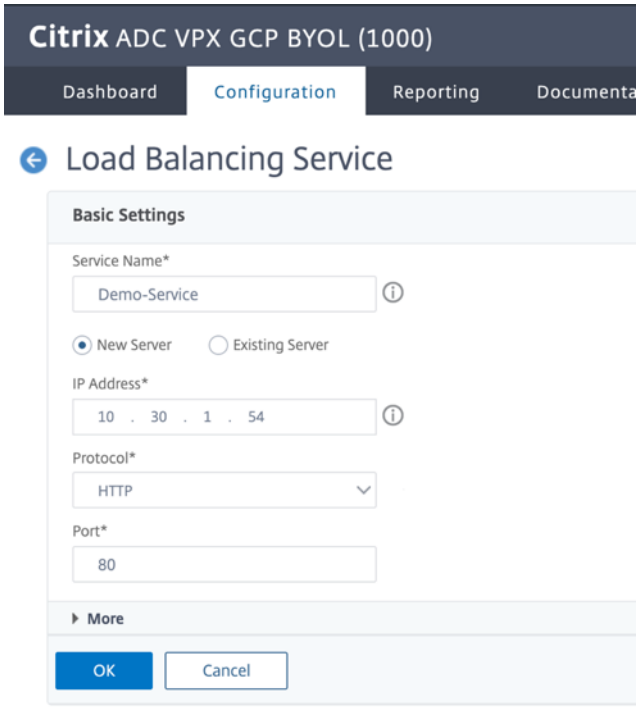


2. Fügen Sie die erforderlichen Werte für Name, Protokoll, IP-Adresstyp (IP-Adresse), IP-Adresse (Externe IP-Adresse der Weiterleitungsregel, die als VIP auf ADC hinzugefügt wird) und Port hinzu, und klicken Sie auf **OK**.



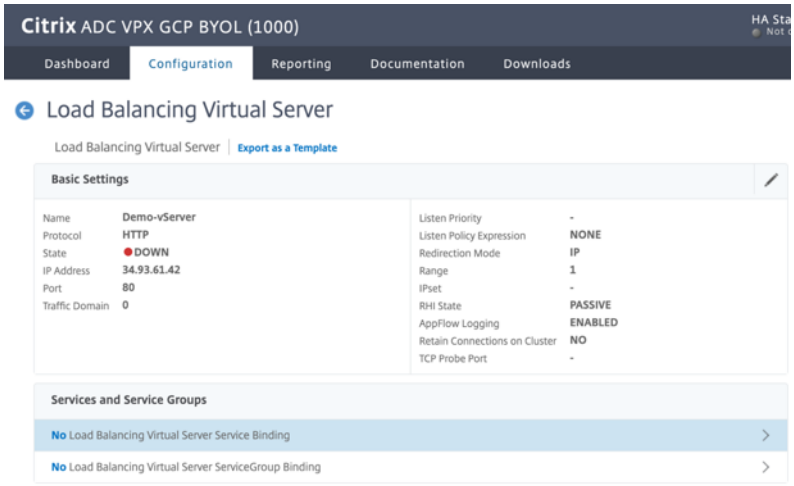
Schritt 2. Fügen Sie einen Dienst oder eine Dienstgruppe hinzu.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Services > Hinzufügen**.
2. Fügen Sie die erforderlichen Werte für Servicename, IP-Adresse, Protokoll und Port hinzu und klicken Sie auf **OK**.

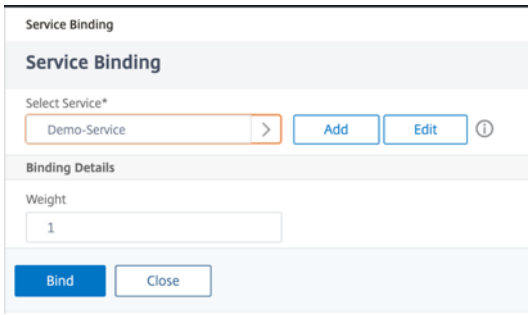


Schritt 3. Binden Sie den Dienst oder die Dienstgruppe an den virtuellen Lastenausgleichsserver.

1. Navigieren Sie zu **Konfiguration > Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie den in **Schritt 1**konfigurierten virtuellen Lastausgleichsserver aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Service- und Dienstgruppen** auf **Keine Load Balancing Virtual Server-Dienstbindung**.



4. Wählen Sie den in **Schritt 3**konfigurierten Dienst aus und klicken Sie auf " **Binden**".



5. Speichern Sie die Konfiguration.

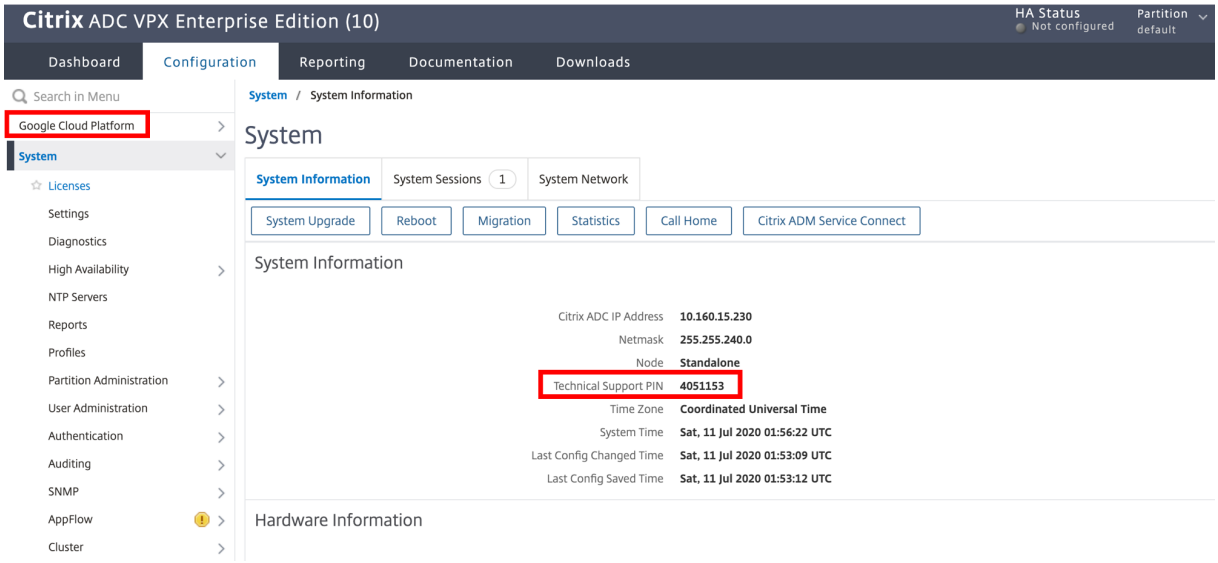
Problembehandlung bei einer VPX-Instanz auf GCP

October 5, 2021

Die Google Cloud Platform (GCP) bietet Konsolenzugriff auf eine Citrix ADC VPX Instanz. Sie können nur debuggen, wenn das Netzwerk verbunden ist. Um das Systemprotokoll einer Instanz anzuzeigen, greifen Sie auf die Konsole zu und überprüfen Sie die **Systemprotokolldateien**.

Citrix unterstützt gebührenbasierte Citrix ADC VPX Instanzen (Dienstprogrammlizenz mit Stundengebühr) auf GCP. Suchen Sie nach der GCP-Kontonummer und dem Support-PIN-Code und rufen Sie den Citrix Support an, um einen Supportfall einzulegen. Sie werden gebeten, Ihren Namen und Ihre E-Mail-Adresse anzugeben. Um die Support-PIN zu finden, melden Sie sich bei der VPX-GUI an und navigieren Sie zur Seite **System**.

Hier ist ein Beispiel für eine Systemseite, die die Support-PIN zeigt.



Jumbo-Frames auf Citrix ADC VPX-Instanzen

October 5, 2021

Citrix ADC VPX Appliances unterstützen den Empfang und die Übertragung von Jumbo-Frames mit bis zu 9216 Byte IP-Daten. Jumbo-Frames können große Dateien effizienter übertragen, als es mit der Standard-IP-MTU-Größe von 1500 Bytes möglich ist.

Eine Citrix ADC Appliance kann Jumbo-Frames in den folgenden Bereitstellungsszenarien verwenden:

- Jumbo an Jumbo. Die Appliance empfängt Daten als Jumbo-Frames und sendet sie als Jumbo-Frames.
- Nicht Jumbo an Jumbo. Die Appliance empfängt Daten als reguläre Frames und sendet sie als Jumbo-Frames.
- Jumbo an Nicht-Jumbo. Die Appliance empfängt Daten als Jumbo-Frames und sendet sie als reguläre Frames.

Weitere Informationen finden Sie unterKonfigurieren der Unterstützung von Jumbo Frames auf einer Citrix ADC Appliance.

Unterstützung für Jumbo Frames ist auf Citrix ADC VPX -Appliances verfügbar, die auf den folgenden Virtualisierungsplattformen ausgeführt werden:

- VMware ESX
- Linux-KVM-Plattform
- Citrix XenServer
- Amazon Web Services (AWS)

Jumbo-Frames auf VPX-Appliances funktionieren ähnlich wie Jumbo Frames auf MPX-Appliances. Weitere Informationen zu Jumbo-Frames und seinen Anwendungsfällen finden Sie unter Konfigurieren von Jumbo-Frames auf MPX-Appliances. Die Anwendungsfälle von Jumbo-Frames auf MPX-Appliances gelten auch für VPX-Appliances.

Konfigurieren von Jumbo-Frames für eine VPX-Instanz, die auf VMware ESX ausgeführt wird

Führen Sie die folgenden Aufgaben aus, um Jumbo-Frames auf einer Citrix ADC VPX-Appliance zu konfigurieren, die auf dem VMware ESX-Server ausgeführt wird:

1. Stellen Sie die MTU der Schnittstelle oder des Kanals der VPX-Appliance auf einen Wert im Bereich von 1501-9000 ein. Verwenden Sie die CLI oder GUI, um die MTU-Größe festzulegen. Die Citrix ADC VPX Appliances, die auf VMware ESX ausgeführt werden, unterstützen das Empfangen und Übertragen von Jumbo-Frames mit nur 9000 Byte IP-Daten.
2. Legen Sie die gleiche MTU-Größe auf den entsprechenden physischen Schnittstellen des VMware ESX-Servers mithilfe der Verwaltungsanwendungen fest. Weitere Informationen zum Festlegen der MTU-Größe auf den physischen Schnittstellen von VMware ESX finden Sie unter http://vmware.com/.

Konfigurieren von Jumbo-Frames für eine VPX-Instanz, die auf dem Linux-KVM-Server ausgeführt wird

Führen Sie die folgenden Aufgaben aus, um Jumbo-Frames auf einer Citrix ADC VPX Appliance zu konfigurieren, die auf einem Linux-KVM-Server ausgeführt wird:

1. Stellen Sie die MTU der Schnittstelle oder des Kanals der VPX-Appliance auf einen Wert im Bereich von 1501-9216 ein. Verwenden Sie die Citrix ADC VPX CLI oder GUI, um die MTU-Größe festzulegen.
2. Legen Sie die gleiche MTU-Größe auf den entsprechenden physischen Schnittstellen eines Linux-KVM-Servers mithilfe seiner Verwaltungsanwendungen fest. Weitere Hinweise zum Festlegen der MTU-Größe auf den physischen Schnittstellen von Linux-KVM finden Sie unterhttp://www.linux-kvm.org/.

Konfigurieren von Jumbo-Frames für eine VPX-Instanz, die auf Citrix XenServer ausgeführt wird

Führen Sie die folgenden Aufgaben aus, um Jumbo-Frames auf einer Citrix ADC VPX Appliance zu konfigurieren, die auf Citrix XenServer ausgeführt wird:

1. Stellen Sie mithilfe von XenCenter eine Verbindung zum XenServer her.

2. Fahren Sie alle VPX-Instanzen herunter, die die Netzwerke verwenden, für die die MTU geändert werden muss.
3. Wählen Sie auf der Registerkarte **Netzwerk** das Netzwerk - Netzwerk 0/1/2.
4. Wählen Sie **Eigenschaften** und bearbeiten Sie MTU.

Nachdem Sie die Jumbo-Frames auf dem XenServer konfiguriert haben, können Sie die Jumbo-Frames auf der ADC-Appliance konfigurieren. Weitere Informationen finden Sie unterKonfigurieren der Unterstützung von Jumbo Frames auf einer Citrix ADC Appliance.

Konfigurieren von Jumbo-Frames für eine VPX-Instanz, die in AWS ausgeführt wird

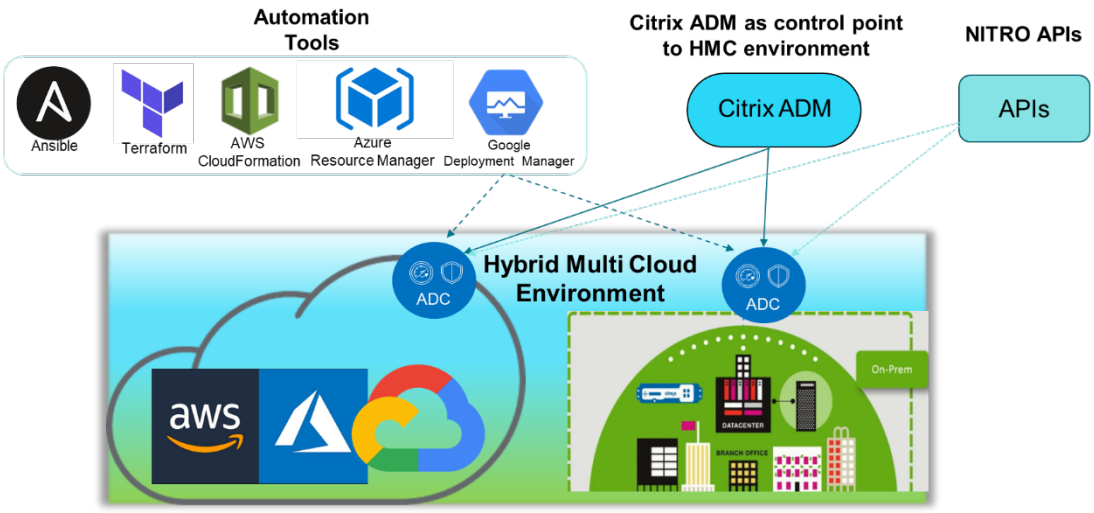
Konfiguration auf Hostebene ist für VPX unter Azure nicht erforderlich. Um Jumbo Frames auf VPX zu konfigurieren, befolgen Sie die Schritte unter Konfigurieren von Jumbo Frames Support auf einer Citrix ADC Appliance.

Automatisieren der Bereitstellung und Konfiguration von Citrix ADC

October 5, 2021

Citrix ADC bietet mehrere Tools zur Automatisierung Ihrer ADC-Bereitstellungen und -Konfigurationen. Dieses Dokument enthält eine kurze Zusammenfassung verschiedener Automatisierungswerkzeuge und Verweise auf verschiedene Automatisierungsressourcen, mit denen Sie ADC-Konfigurationen verwalten können.

Die folgende Abbildung gibt einen Überblick über die Automatisierung von Citrix ADC in einer hybriden Multi-Cloud (HMC) -Umgebung.



Automatisieren Sie Citrix ADC mit Citrix ADM

Citrix ADM fungiert als Automatisierungssteuerungsverweisen auf Ihre verteilte ADC-Infrastruktur. Der Citrix ADM bietet umfassende Automatisierungsfunktionen von der Bereitstellung von ADC-Appliances bis hin zum Upgrade. Im Folgenden sind die wichtigsten Automatisierungsfunktionen von ADM aufgeführt:

- Provisioning von Citrix ADC VPX-Instanzen in AWS
- Provisioning von Citrix ADC VPX-Instanzen in Azure
- StyleBooks
- Konfigurationsaufträge
- Konfigurations-Audit
- ADC-Upgrades
- SSL Zertifikatsverwaltung
- Integrationen - GitHub, ServiceNow, Integrationen von Ereignisbenachrichtigungen

Citrix ADM Blogs und Videos zur Automatisierung

- Anwendungsmigrationen mit StyleBooks
- Integrieren Sie ADC-Konfigurationen mit CI/CD mithilfe von ADM StyleBooks
- Vereinfachung der Public Cloud Citrix ADC Bereitstellungen durch ADM
- 10 Arten, wie der Citrix ADM -Service einfachere Citrix ADC Upgrades unterstützt

Citrix ADM bietet auch APIs für seine verschiedenen Funktionen, die Citrix ADM und Citrix ADC als Teil der gesamten IT-Automatisierung integrieren. Weitere Informationen finden Sie unter Citrix ADM Service-APIs.

Automatisieren Sie Citrix ADC mit Terraform

Terraform ist ein Tool, das Infrastruktur als Code-Ansatz für die Bereitstellung und Verwaltung von Cloud, Infrastruktur oder Service betrachtet. Citrix ADC Terraform-Ressourcen stehen in GitHub zur Verwendung zur Verfügung. Informationen zur detaillierten Dokumentation und Verwendung finden Sie in GitHub.

- Citrix ADC Terraform-Module zur Konfiguration von ADC für verschiedene Anwendungsfälle wie Load Balancing und GSLB
- Terraform Cloud-Skripts zur Bereitstellung von ADC in AWS
- Terraform-Cloud-Skripts zur Bereitstellung von ADC in Azure

Videos zu Terraform für ADC-Automatisierung

- Automatisieren Sie Ihre Citrix ADC-Bereitstellungen mit Terraform

- Bereitstellung und Konfiguration von ADC in HA-Einrichtung in AWS mit Terraform

Automatisieren Sie Citrix ADC mit Ansible

Ansible ist ein Open-Source-Tool für Softwarebereitstellung, Konfigurationsmanagement und Anwendungsbereitstellung, das die Infrastruktur als Code ermöglicht. Citrix ADC Ansible Module und Beispiel-Playbooks können in GitHub zur Verwendung gefunden werden. Informationen zur detaillierten Dokumentation und Verwendung finden Sie in GitHub.

- Ansible-Module zur Konfiguration von ADC
- Automatisieren Sie ADC mit Ansible-Whitepaper
- Ansible-Module für ADM

Citrix ist ein zertifizierter Ansible Automation Partner. Benutzer mit einem Red Hat Ansible Automation Platform-Abonnement können von Red Hat Automation Hubaus auf Citrix ADC Collections zugreifen.

Automatisierungsblogs von Terraform und Ansible

- Terraform und Ansible Automation für App-Bereitstellung und Sicherheit

Public Cloud-Vorlagen für ADC-Bereitstellungen

Public Cloud-Vorlagen vereinfachen die Bereitstellung Ihrer Bereitstellungen in Public Clouds. Für verschiedene Umgebungen stehen verschiedene Citrix ADC-Vorlagen zur Verfügung. Einzelheiten zur Verwendung finden Sie in den jeweiligen GitHub-Repositorys.

AWS-CFTs:

- CFTs zur Bereitstellung von Citrix ADC VPX auf AWS

Vorlagen für Azure Resource Manager (ARM):

- ARM-Vorlagen zur Bereitstellung von Citrix ADC VPX auf Azure

Vorlagen für Google Cloud-Bereitstellungsmanager (GDM):

- GDM-Vorlagen zur Bereitstellung von Citrix ADC VPX bei Google

Videos auf Vorlagen

- Bereitstellen von Citrix ADC HA in AWS mit CloudFormation Template
- Bereitstellen von Citrix ADC HA über Availability Zones mit AWS QuickStart
- Citrix ADC HA-Bereitstellung in GCP unter Verwendung von GDM-Templates

AWS Schnellstarts

- Citrix WAF Schnellstart
- AWS Quick Start für Citrix ADC VPX für Webanwendungen auf AWS

NITRO-APIs

Mit dem Citrix ADC NITRO-Protokoll können Sie die Citrix ADC Appliance mithilfe von Representational State Transfer (REST) programmgesteuert konfigurieren und überwachen. Daher können NITRO-Anwendungen in jeder Programmiersprache entwickelt werden. Für Anwendungen, die in Java oder .NET oder Python entwickelt werden müssen, werden NITRO-APIs über relevante Bibliotheken bereitgestellt, die als separate Software Development Kits (SDKs) verpackt sind.

- NITRO-API-Dokumentation
- Citrix ADC API Referenz
- Beispiel für ADC-Anwendungsfallkonfiguration mit NITRO API

FAQ

April 7, 2022

Der folgende Abschnitt hilft Ihnen bei der Kategorisierung der FAQs basierend auf Citrix Application Delivery Controller (ADC) VPX.

- Feature und Funktionalität
- Verschlüsselung
- Preisgestaltung und Verpackung
- Citrix ADC VPX Express
- Hypervisor
- Kapazitätsplanung oder -größe
- Systemanforderungen
- Weitere technische FAQs

Feature und Funktionalität

Was ist Citrix ADC VPX?

Citrix ADC VPX ist eine virtuelle ADC-Appliance, die auf einem Hypervisor gehostet werden kann, der auf Industriestandard-Servern installiert ist.

Enthalten Citrix ADC VPX alle Funktionen zur Optimierung von Webanwendungen als ADC-Appliances?

Ja. Citrix ADC VPX umfasst alle Lastenausgleich, Datenverkehrsverwaltung, Anwendungsbeschleunigung, Anwendungssicherheit (einschließlich Citrix ADC Gateway und Citrix Application Firewall) und Offload-Funktionen. Einen vollständigen Überblick über die Funktion und Funktionalität von Citrix ADC finden Sie unter Anwendungsbereitstellung auf Ihre Weise.

Gibt es Einschränkungen bei der Citrix Application Firewall bei der Verwendung auf Citrix ADC VPX?

Citrix Application Firewall auf Citrix ADC VPX bietet denselben Sicherheitsschutz wie auf Citrix ADC-Appliances. Die Leistung oder der Durchsatz der Citrix Application Firewall variiert je nach Plattform.

Gibt es Unterschiede zwischen Citrix ADC Gateway auf Citrix ADC VPX und Citrix ADC Gateway auf Citrix ADC-Appliances?

Funktional sind sie identisch. Citrix ADC Gateway auf Citrix ADC VPX unterstützt alle Citrix ADC Gateway-Funktionen, die in Citrix ADC Softwareversion 9.1 verfügbar sind. Da Citrix ADC-Appliances jedoch dedizierte SSL-Beschleunigungshardware bieten, bietet sie eine größere SSL-VPN-Skalierbarkeit als eine Citrix ADC VPX-Instanz.

Abgesehen von dem offensichtlichen Unterschied, auf einem Hypervisor laufen zu können, wie unterscheidet sich Citrix ADC VPX von physischen Citrix ADC-Appliances?

Es gibt zwei Hauptbereiche, in denen Kunden Verhaltensunterschiede feststellen. Das erste ist, dass Citrix ADC VPX nicht die gleiche Leistung bieten kann wie viele Citrix ADC-Appliances. Das zweite ist, dass Citrix ADC-Appliances zwar über eine eigene L2-Netzwerkfunktionalität verfügen, Citrix ADC VPX jedoch für seine L2-Netzwerkdienste auf den Hypervisor angewiesen ist. Im Allgemeinen schränkt dies nicht ein, wie der Citrix ADC VPX bereitgestellt werden kann. Es kann bestimmte L2-Funktionen geben, die auf einer physischen Citrix ADC-Appliance konfiguriert sind und auf dem zugrunde liegenden Hypervisor konfiguriert werden müssen.

Wie spielt Citrix ADC VPX eine Rolle auf dem Markt für Anwendungsbereitstellung?

Citrix ADC VPX ändert das Spiel auf dem Markt für Anwendungsbereitstellung auf folgende Weise:

- Indem eine Citrix ADC-Appliance noch erschwinglicher wird, ermöglicht Citrix ADC VPX jeder IT-Organisation, eine Citrix ADC-Appliance bereitzustellen. Dies ist nicht nur für ihre geschäftskritischsten Webanwendungen gedacht, sondern für alle ihre Webanwendungen.

- Citrix ADC VPX ermöglicht es Kunden, Netzwerk und Virtualisierung in ihren Rechenzentren weiter zu konvergieren. Citrix ADC VPX kann nicht nur zur Optimierung von Webanwendungen verwendet werden, die auf virtualisierten Servern gehostet werden. Darüber hinaus kann die Bereitstellung von Webanwendungen selbst zu einem virtualisierten Service werden, der einfach und schnell überall bereitgestellt werden kann. IT-Organisationen verwenden die Standard-Rechenzentrumsprozesse für Aufgaben wie Bereitstellung, Automatisierung und Rückladung für die Infrastruktur zur Bereitstellung von Webanwendungen.
- Citrix ADC VPX eröffnet neue Bereitstellungsarchitekturen, die nicht praktisch sind, wenn nur physische Appliances verwendet werden. Citrix ADC VPX und Citrix ADC MPX Appliances können als Basis verwendet werden, die auf die individuellen Bedürfnisse der jeweiligen Anwendung zugeschnitten sind, um prozessorintensive Aktionen wie Komprimierung und Anwendungsfirewall zu verarbeiten. Am Rechenzentrumsrand übernehmen Citrix ADC MPX-Appliances netzwerkweite Aufgaben mit hohem Volumen wie die anfängliche Datenverkehrsverteilung, SSL-Verschlüsselung oder Entschlüsselung, Denial-of-Service-Angriffsprävention (DoS) und den globalen Lastenausgleich. Die Kopplung von leistungsstarken Citrix ADC MPX-Appliances mit der einfach bereitzustellenden virtuellen Citrix ADC VPX Appliance bringt beispiellose Flexibilität und Anpassungsfunktionen für moderne, große Rechenzentrumsumgebungen und reduziert gleichzeitig die Gesamtkosten für Rechenzentren.

Wie passt Citrix ADC VPX in unsere Citrix Delivery Center-Strategie?

Mit der Verfügbarkeit von Citrix ADC VPX ist das gesamte Citrix Delivery Center-Angebot als virtualisiertes Angebot verfügbar. Das gesamte Citrix Delivery Center profitiert von den leistungsstarken Verwaltungs-, Bereitstellungs-, Überwachungs- und Berichtsfunktionen, die in Citrix XenCenter verfügbar sind. Dies kann schnell in fast jeder Umgebung eingesetzt und von überall aus zentral verwaltet werden. Mit einer integrierten, virtualisierten Anwendungsbereitstellungsinfrastruktur können Unternehmen Desktops, Client-Server-Anwendungen und Webanwendungen bereitstellen.

Verschlüsselung

Unterstützt Citrix ADC VPX SSL-Offload?

Ja. Citrix ADC VPX führt jedoch die gesamte SSL-Verarbeitung in Software durch, sodass Citrix ADC VPX nicht die gleiche SSL-Leistung wie Citrix ADC-Appliances bietet. Citrix ADC VPX kann bis zu 750 neue SSL-Transaktionen pro Sekunde unterstützen.

Beschleunigen SSL-Karten von Drittanbietern, die auf dem Server installiert sind, auf dem Citrix ADC VPX gehostet wird, die SSL-Verschlüsselung oder -Entschlüsselung?

Nein. Die Unterstützung von SSL-Karten von Drittanbietern kann den Citrix ADC VPX nicht bestimmten Hardwareimplementierungen zuordnen. Dies verringert die Fähigkeit eines Unternehmens, Citrix ADC VPX flexibel überall im Rechenzentrum zu hosten. Citrix ADC MPX-Appliances müssen verwendet werden, wenn mehr SSL-Durchsatz erforderlich ist, als Citrix ADC VPX bietet.

Unterstützt Citrix ADC VPX dieselben Verschlüsselungsverschlüsselungen wie physische Citrix ADC-Appliances?

VPX unterstützt alle Verschlüsselungsverschlüsselungen als physische Citrix ADC-Appliances, mit Ausnahme der ECDSA.

Was ist der SSL-Transaktionsdurchsatz von Citrix ADC VPX?

Informationen zum Durchsatz von SSL-Transaktionen finden Sie im Citrix ADC VPX Datenblatt .

Preisgestaltung und Verpackung

Wie ist Citrix ADC VPX verpackt?

Die Auswahl von Citrix ADC VPX ähnelt der Auswahl von Citrix ADC-Appliances. Zunächst wählt der Kunde die Citrix ADC Edition basierend auf seinen Funktionsanforderungen aus. Anschließend wählt der Kunde die spezifische Citrix ADC VPX -Bandbreitenstufe basierend auf den Durchsatzanforderungen aus. Citrix ADC VPX ist in Standard-, Advanced- und Premium-Editionen verfügbar. Citrix ADC VPX bietet von 10 Mbit/s (VPX 10) bis 100 Gbit/s (VPX 100G). Weitere Details finden Sie im Citrix ADC VPX Datenblatt.

Ist der Preis für Citrix ADC VPX für alle Hypervisoren gleich?

Ja.

Werden dieselben Citrix ADC-SKUs für VPX auf allen Hypervisoren verwendet?

Ja.

Kann eine Citrix ADC VPX-Lizenz von einem Hypervisor auf einen anderen verschoben werden (z. B. von VMware auf Hyper-V)?

Ja. Citrix ADC VPX-Lizenzen sind unabhängig vom zugrunde liegenden Hypervisor. Wenn Sie sich entscheiden, die virtuelle Citrix ADC VPX-Maschine von einem Hypervisor auf einen anderen zu ver-

schieben, müssen Sie keine neue Lizenz erwerben. Möglicherweise müssen Sie jedoch die vorhandene Citrix ADC VPX-Lizenz neu hosten.

Können Citrix ADC VPX-Instanzen aktualisiert werden?

Ja. Sowohl die Durchsatzbeschränkungen als auch die Citrix ADC Family Edition können aktualisiert werden. Upgrade-SKUs für beide Upgrade-Typen sind verfügbar.

Wie viele Lizenzen benötige ich, wenn ich Citrix ADC VPX in einem Hochverfügbarkeitspaar bereitstellen möchte?

Wie bei physischen Citrix ADC-Appliances erfordert eine Citrix ADC-Hochverfügbarkeitskonfiguration zwei aktive Instanzen. Daher muss der Kunde zwei Lizenzen erwerben.

Citrix ADC VPX Express und 90-Tage-Gebührentestversion

Enthalten Citrix ADC VPX Express alle Citrix ADC-Standardfunktionen? Umfasst es Citrix ADC Gateway und Load Balancing für Citrix Virtual Apps (ehemals XenApp), Webinterface und XML-Broker?

Ja. Citrix ADC VPX Express enthält die volle Citrix ADC Standardfunktionalität. Ab Citrix ADC Version 12.0—56.20 änderte Citrix das VPX Express-Verhalten.

Enthalten Citrix ADC VPX Express alle Citrix ADC-Standardfunktionen? Umfasst es Citrix ADC Gateway und Lastausgleich für Citrix Virtual Apps Webinterface und XML-Broker?

Ab Citrix ADC Version 12.0—56.20 bietet VPX Express das Featureset Citrix ADC Standard Edition mit Ausnahme der Gateway-Funktionalität. Vor der Version 12.0—56.20 enthält VPX alle Funktionen der Standardausgabe.

Benötigt Citrix ADC VPX Express eine Lizenz?

Mit der neuen Citrix ADC VPX Express-Version (12.0—56.20 und neuer) ist VPX Express kostenlos und benötigt keine Lizenzdateien für die Installation und wird unverbindlich geliefert. Wenn Sie bereits über eine VPX Express-Lizenz verfügen, bleibt das vorherige VPX Express-Verhalten erhalten. Wenn die VPX *Express-Lizenzdatei* entfernt und die Version 12.0—56.20 verwendet wird, wird das neue VPX-Express-Verhalten wirksam.

Lauf die Citrix ADC VPX Express-Lizenz ab?

Mit dem neuen VPX Express nein. Es gibt keine Lizenz und kein Ablaufdatum. Wenn Sie bereits eine VPX Express-Lizenz besitzen, läuft die Lizenz ein Jahr nach dem Download ab.

Enthalten Citrix ADC VPX Express die fünf kostenlosen Citrix ADC Gateway Concurrent-Lizenzen?

Ja, wenn Sie eine VPX-Express-Lizenz besitzen.

Gibt es ein Limit, wie viele Citrix ADC VPX Expresses ein Kunde herunterladen kann?

Fünf.

Unterstützt Citrix ADC VPX Express dieselben Verschlüsselungsverschlüsselungen wie Citrix ADC MPX-Appliances?

Für die allgemeine Verfügbarkeit sind dieselben starken Verschlüsselungsverschlüsselungen, die auf Citrix ADC-Appliances unterstützt werden, für Citrix ADC VPX und Citrix ADC VPX Express verfügbar. Es unterliegt denselben Import- oder Exportvorschriften.

Kann ich technische Supportfälle für Citrix ADC VPX Express einreichen?

Nein. Eine Citrix ADC VPX-Lizenz für den Einzelhandel wie VPX-10, VPX-200, VPX-1000, VPX-3000 ist erforderlich, um technische Supportfälle einzureichen. Citrix ADC VPX Express-Benutzer können jedoch sowohl das Citrix ADC VPX Knowledge Center verwenden als auch über die Z-Diskussionsforen Hilfe von der Community anfordern.

Kann Citrix ADC VPX Express auf eine Einzelhandelsversion aktualisiert werden?

Ja. Erwerben Sie einfach die Citrix ADC VPX-Lizenz für den Einzelhandel, die Sie benötigen, und wenden Sie dann die entsprechende Lizenz auf die Citrix ADC VPX Express-Instanz an.

Hypervisor

Welche VMware-Versionen unterstützt Citrix ADC VPX?

Citrix ADC VPX unterstützt VMware ESX und ESXi für Versionen 3.5 oder höher. Weitere Informationen finden Sie unter Supportmatrix und Nutzungsrichtlinien

Wie viele virtuelle Netzwerkschnittstellen können Sie für VMware einem VPX zuweisen?

Sie können einem Citrix ADC VPX bis zu 10 virtuelle Netzwerkschnittstellen zuweisen.

Wie können wir von vSphere auf die Citrix ADC VPX-Befehlszeile zugreifen?

Der VMware vSphere-Client bietet über eine Konsolenregisterkarte integrierten Zugriff auf die Citrix ADC VPX-Befehlszeile. Sie können auch jeden SSH- oder Telnet-Client verwenden, um auf die Befehlszeile zuzugreifen. Sie können die NSIP-Adresse des Citrix ADC VPX im SSH- oder Telnet-Client verwenden.

Wie können Sie auf die Citrix ADC VPX GUI zugreifen?

Um auf die Citrix ADC VPX GUI zuzugreifen, geben Sie die NSIP des Citrix ADC VPX, beispielsweise `http://NSIP address`, in das Adressfeld eines beliebigen Browsers ein.

Können zwei Citrix ADC VPX-Instanzen, die auf demselben VMware ESX installiert sind, in einem Hochverfügbarkeits-Setup konfiguriert werden?

Ja, aber es wird nicht empfohlen. Ein Hardwarefehler würde sich auf beide Citrix ADC VPX-Instanzen auswirken.

Können zwei Citrix ADC VPX-Instanzen, die auf zwei verschiedenen VMware ESX-Systemen ausgeführt werden, in einem Hochverfügbarkeits-Setup konfiguriert werden?

Ja. Es wird in einem Hochverfügbarkeits-Setup empfohlen.

Werden für die VMware interface-bezogene Ereignisse auf Citrix ADC VPX unterstützt?

Nein. Interface-bezogene Ereignisse werden nicht unterstützt.

Werden für die VMware getaggte VLANs auf Citrix ADC VPX unterstützt?

Ja. Citrix ADC-markierte VLANs werden ab Version 11.0 und höher von Citrix ADC VPX unterstützt. Weitere Informationen finden Sie in der Citrix-Dokumentation.

Werden Link-Aggregation und LACP für VMware auf Citrix ADC VPX unterstützt?

Nein. Link Aggregation und LACP werden für Citrix ADC VPX nicht unterstützt. Die Link-Aggregation muss auf VMware-Ebene konfiguriert werden.

Wie greifen wir auf die Citrix ADC VPX-Dokumentation zu?

Die Dokumentation ist über die Citrix ADC VPX GUI verfügbar. Nachdem Sie sich angemeldet haben, wählen Sie die Registerkarte **Dokumentation** .

Kapazitätsplanung oder -größe

Welche Leistung kann ich mit Citrix ADC VPX erwarten?

Citrix ADC VPX bietet eine gute Leistung. Ein bestimmtes Leistungsniveau, das mit Citrix ADC VPX erreicht werden kann, finden Sie im Citrix ADC VPX Datenblatt .

Wie können wir die maximale Leistung einer Citrix ADC Instanz schätzen, da die CPU-Leistung des Servers variiert?

Die Verwendung einer schnelleren CPU kann zu einer höheren Leistung führen (bis zu dem von der Lizenz zulässigen Maximum), während die Verwendung einer langsameren CPU die Leistung sicherlich einschränken kann.

Sind Citrix ADC VPX Bandbreiten- oder Durchsatzbeschränkungen für eingehenden Datenverkehr oder sowohl eingehenden als auch ausgehenden Datenverkehr?

Citrix ADC VPX-Bandbreitenbeschränkungen werden nur für den Datenverkehr durchgesetzt, der an den Citrix ADC eingeht, unabhängig davon, ob der Anforderungsverkehr oder der Antwortverkehr erfolgt. Dies zeigt an, dass ein Citrix ADC VPX-1000 (zum Beispiel) sowohl 1 Gbit/s eingehenden Datenverkehr als auch 1 Gbit/s ausgehenden Datenverkehr gleichzeitig verarbeiten kann. Eingehender und ausgehender Datenverkehr ist nicht identisch mit Anforderungs- und Antwortdatenverkehr. Für den Citrix ADC ist sowohl der Datenverkehr, der von Endpunkten (Anforderungsverkehr) kommt, als auch Datenverkehr von Ursprungsservern (Antwortverkehr) “eingehend” (d. h. in den Citrix ADC).

Können mehrere Instanzen von Citrix ADC VPX auf demselben Server ausgeführt werden?

Ja. Stellen Sie jedoch sicher, dass der physische Server über genügend CPU- und E/A-Kapazität verfügt, um die gesamte auf dem Host ausgeführte Arbeitslast zu unterstützen, da sonst die Leistung von Citrix ADC VPX beeinträchtigt werden kann.

Wenn mehr als eine Instanz von Citrix ADC VPX auf einem physischen Server ausgeführt wird, was ist die Mindestanforderungen für die Hardware pro Citrix ADC VPX-Instanz?

Jeder Citrix ADC VPX Instanz muss 2 GB physischen RAM, 20 GB Speicherplatz und 2 vCPUs zugewiesen werden.

Kann ich Citrix ADC VPX und andere Anwendungen auf demselben Server hosten?

Ja. Beispielsweise können Citrix ADC VPX, Citrix Virtual Apps Webinterface und Citrix Virtual Apps XML Broker alle virtualisiert werden und auf demselben Server ausgeführt werden. Stellen Sie für eine optimale Leistung sicher, dass der physische Host über genügend CPU- und E/A-Kapazität verfügt, um alle laufenden Workloads zu unterstützen.

Wird das Hinzufügen von CPU-Kernen zu einer einzelnen Citrix ADC VPX-Instanz die Leistung dieser Instanz erhöhen?

Abhängig von der Lizenz kann eine Citrix ADC VPX Instanz heute bis zu 4 vCPU verwenden. Das Hinzufügen einer zusätzlichen CPU zu einer Citrix ADC VPX-Instanz, die mehr CPUs verwenden kann, erhöht die Leistung.

Warum sieht Citrix ADC VPX so aus, als würde er mehr als 90% der CPU verbraucht, obwohl er im Leerlauf ist?

Es ist normales Verhalten und Citrix ADC-Appliances zeigen das gleiche Verhalten. Um die tatsächliche Ausdehnung der Citrix ADC VPX CPU-Auslastung anzuzeigen, verwenden Sie den Befehl stat CPU in der Citrix ADC CLI oder zeigen Sie die Citrix ADC VPX CPU-Auslastung von der Citrix ADC GUI an. Die Citrix ADC Paketverarbeitungs-Engine ist immer “auf der Suche nach Arbeit”, auch wenn keine Arbeit zu tun ist. Daher tut es alles, um die Kontrolle über die CPU zu übernehmen und sie nicht freizugeben. Auf einem Server, der mit Citrix ADC VPX und sonst nichts installiert ist, ergibt sich (aus der Sicht des Hypervisors), dass Citrix ADC VPX die gesamte CPU verbraucht. Ein Blick auf die CPU-Auslastung von “innerhalb von Citrix ADC” (über die Befehlszeilenschnittstelle oder der GUI) liefert ein Bild der verwendeten Citrix ADC VPX CPU-Kapazität.

Systemanforderungen

Was ist die Mindestanforderung für Citrix ADC VPX?

Die Systemanforderungen finden Sie unter Citrix ADC VPX Datenblatt .

Citrix ADC VPX erfordert:

- Prozessoranforderungen: Dual-Core-Server mit Intel Xeon.
- Speicher verfügbar: 4 GB RAM und 20 GB Festplatte. Für kritische Bereitstellungen empfiehlt Citrix keine 2 GB RAM für VPX, da das System in einer Umgebung mit sehr geringem Arbeitsspeicher arbeitet. Dies kann zu Skalierungs-, Leistungs- oder Stabilitätsproblemen führen.
- Hypervisor: Citrix Hypervisor 5.6 oder höher; VMware ESX/ESXi 3.5 oder höher, Windows Server 2008 R2 mit Hyper-V.
- Konnektivität: mindestens 100 Mbit/s. 1 Gbit/s empfohlen.

- Eine Netzwerkkarte, die mit dem Hypervisor kompatibel ist.

> **Hinweis**
>
> AMD-Prozessoren werden nicht unterstützt.

Was ist Intel VT-x?

Diese Funktionen, die manchmal als “Hardware-Assist” oder “Virtualisierungsassistent” bezeichnet werden, erfassen sensible oder privilegierte CPU-Anweisungen, die vom Gastbetriebssystem an den Hypervisor ausgeführt werden. Dies vereinfacht das Hosten von Gastbetriebssystemen (BSD für einen Citrix ADC VPX) auf dem Hypervisor.

Wie üblich sind VT-x?

Praktisch können alle Server, die innerhalb der letzten zwei Jahre ausgeliefert wurden, VT-x unterstützen. Viele Server werden mit deaktivierter Virtualisierungsunterstützung im BIOS ausgeliefert. Bevor Sie davon ausgehen, dass Sie Citrix ADC VPX nicht ausführen können, prüfen Sie, ob Sie diese Einstellung auf dem Server ändern müssen.

Gibt es eine Hardwarekompatibilitätsliste (HCL) für Citrix ADC VPX?

Solange der Server Intel VT-x unterstützt, muss Citrix ADC VPX auf jedem Server laufen, der mit dem zugrunde liegenden Hypervisor kompatibel ist. Eine umfassende Liste der unterstützten Plattformen finden Sie in der Hypervisor-HCL.

Auf welcher Version von Citrix ADC OS basiert Citrix ADC VPX?

Citrix ADC VPX basiert auf Citrix ADC 9.1 oder höheren Versionen.

Da Citrix ADC VPX auf BSD läuft, kann es nativ auf einem Server mit installiertem BSD Unix ausgeführt werden?

Nein. Citrix ADC VPX erfordert die Ausführung des Hypervisors. Detaillierte Hypervisor-Unterstützungen finden Sie im Datenblatt von Citrix ADC VPX.

Weitere technische FAQs

Funktioniert die Link-Aggregation auf einem physischen Server mit mehreren Netzwerkkarten?

LACP wird nicht unterstützt. Für den Citrix Hypervisor wird die statische Link-Aggregation unterstützt und hat Grenzen von vier Kanälen und sieben virtuellen Schnittstellen. Für VMware wird die statis-

che Link-Aggregation in Citrix ADC VPX nicht unterstützt, kann aber auf VMware-Ebene konfiguriert werden.

Wird MAC-basierte Weiterleitung (MBF) auf VPX unterstützt? Gibt es Änderungen gegenüber der Implementierung der Citrix ADC-Appliance?

MBF wird unterstützt und verhält sich genauso wie bei der Citrix ADC-Appliance. Der Hypervisor schaltet grundsätzlich alle von Citrix ADC VPX empfangenen Pakete nach außen und umgekehrt.

Wie wird der Citrix ADC VPX-Upgrade-Prozess durchgeführt?

Upgrades werden genauso ausgeführt wie für Citrix ADC-Appliances: Laden Sie eine Kerneldatei herunter und verwenden Sie install ns oder das Upgrade-Dienstprogramm in der Benutzeroberfläche.

Wie groß ist die Partition `/var` bei Verwendung des Standardimage für VPX? Wie erhöht man den Speicherplatz?

Die Größe des Rootdatenträgers ist auf 20 GB begrenzt, um das Datenträgerimage klein zu halten.

Wenn Sie den Verzeichnisspeicher für `/var/core/` oder `/var/crash/` vergrößern möchten, hängen Sie einen zusätzlichen Datenträger an. Um die Größe von `/var` zu erhöhen, müssen Sie derzeit einen zusätzlichen Datenträger anhängen und einen symbolischen Link zu `/var` erstellen, nachdem Sie den kritischen Inhalt auf den neuen Datenträger kopiert haben.

Was können wir erwarten, dass die NetScaler VPX Build-Nummerierung und die Interoperabilität mit anderen Builds berücksichtigt werden?

Citrix ADC VPX hat eine ähnliche Build-Nummerierung wie die 9.1. Cl (klassisch) und 9.1. Nc (NCore) Release, zum Beispiel 9.1_97.3.vpx, 9.1_97.3.nc und 9.1_97.3.cl.

Kann der Citrix ADC VPX Teil eines Hochverfügbarkeitssetups mit einer Citrix ADC-Appliance sein?

Keine unterstützte Konfiguration.

Befinden sich alle in Citrix ADC VPX sichtbaren Schnittstellen in direktem Zusammenhang mit der Anzahl der Schnittstellen auf dem Hypervisor?

Nein. Sie können bis zu sieben Schnittstellen (10 für VMware) über das Citrix ADC VPX Konfigurationsprogramm mit nur einer physischen Netzwerkkarte auf dem Hypervisor hinzufügen.

Kann Citrix Hypervisor XenMotion oder VMware VMotion oder Hyper-V Live-Migration verwendet werden, um aktive Instanzen von Citrix ADC VPX zu verschieben?

Citrix ADC VPX unterstützt keine XenMotion- oder Hyper-V-Live-Migration. vMotion wird ab Citrix ADC 12.1 Release unterstützt. Weitere Informationen finden Sie unter Versionshinweise.

Lizenzierungsübersicht

October 5, 2021

Citrix bietet eine breite Palette von Produkteditionen und Lizenzmodellen für MPX- und VPX-Appliances an, um die Anforderungen Ihres Unternehmens zu erfüllen.

Für den ordnungsgemäßen Betrieb einer Citrix ADC-Appliance muss sie über eine der Lizenzen der Citrix ADC Produktreihe verfügen. Die ADC-Produktlinie umfasst drei Familienausgaben:

- Standard Edition
- Advanced Edition
- Premium Edition

Weitere Informationen finden Sie im Citrix ADC-Datenblatt.

Nachdem Sie die Citrix ADC Edition ausgewählt haben, können Sie eines der MPX- und VPX-Lizenzangebote auswählen. Basierend auf den Kriterien wie Perpetual und Abonnement (Jahres- und Stundenabonnement), vCPU und Bandbreite, on-premises und Cloud und so weiter.

Citrix ADC VPX-Lizenzen

Im Folgenden sind VPX-spezifische Lizenzen.

Citrix ADC VPX Express-Lizenz

Ab Citrix ADC Release 12.0 56.20 benötigt VPX Express für on-premises und Cloud-Bereitstellungen keine Lizenzdatei und verfügt über die folgenden Funktionen:

- 20 Mbit/s Bandbreite
- Alle ADC-Standardlizenzfunktionen mit Ausnahme von Citrix Gateway und L4- und L7-Schutzmaßnahmen
- Maximal 250 SSL-Sitzungen
- 20 Mbit/s SSL-Durchsatz

Sie können die VPX Express License auf die folgenden zwei Optionen aktualisieren:

1. Eine eigenständige Citrix ADC VPX-Lizenz

2. Citrix ADC Pooled Capacity Lizenz für VPX-Instanzen. Weitere Informationen finden Sie unter Citrix ADC Pooled Capacity.

> **Wichtig**
>
> Clustering ist in der Standard Edition für die VPX Public Cloud und in der VPX Express-Lizenz verfügbar.

Citrix ADC VPX gepoolte Kapazitätslizenz

Sie können Citrix Application Delivery Management (ADM) verwenden, um ein Lizenzierungsframework zu erstellen, das einen gemeinsamen Bandbreiten- und Instanzpool umfasst. Vollständige Informationen finden Sie unter Gepoolte Kapazität von Citrix ADC.

Zugehörige Ressourcen

Citrix Lizenzierungssystem

So weisen Sie Citrix ADC VPX-Lizenzen zu

VPX-Lizenzierung in Cloud

Die VPX-Bereitstellung wird von Public Cloud-Anbietern wie Azure, AWS und Google unterstützt. Weitere Informationen finden Sie in den folgenden Dokumenten:

- VPX-Azure-Lizenz
- VPX-AWS-Lizenz
- VPX-GCP-Lizenz

Zuweisen und Anwenden einer Lizenz

October 5, 2021

In der Citrix MPX- und VPX-ADC-GUI können Sie Ihre Hardwareseriennummer (HSN) oder Ihren Lizenzzugriffscode verwenden, um Ihre Lizenzen zuzuweisen. Wenn auf Ihrem lokalen Computer bereits eine Lizenz vorhanden ist, können Sie sie auch auf die Appliance hochladen.

Für alle anderen Funktionen, z. B. die Rückgabe oder Neuzuweisung Ihrer Lizenz, müssen Sie das Lizenzportal verwenden. Optional können Sie weiterhin das Lizenzportal für die Lizenzzuweisung verwenden. Weitere Informationen finden Sie unter Verwenden von Verwalten von Lizenzen in My Account auf citrix.com.

Leitfaden zur Citrix Lizenzierung

Der Citrix Lizenzierungsleitfaden enthält auch Informationen zur Installation von Lizenzen in einer Citrix ADC Appliance und zur Installation von Lizenzen in anderen Citrix Produkten. Weitere Informationen finden Sie im Citrix Licensing Guide.

Voraussetzungen

> **Hinweis:**
>
> Erwerben Sie separate Lizenzen für jede Appliance in einem Hochverfügbarkeitspaar. Stellen Sie sicher, dass auf beiden Appliances dieselben Lizenzen installiert sind. Wenn Sie beispielsweise eine Premium-Lizenz für eine Appliance erwerben, müssen Sie eine andere Premium-Lizenz für die andere Appliance erwerben.

So verwenden Sie die Hardwareseriennummer oder den Lizenzzugriffscode, um Ihre Lizenzen zuzuweisen:

- Sie müssen über die Appliance auf öffentliche Domänen zugreifen können. Beispielsweise sollte die Appliance auf www.citrix.com zugreifen können. Die Lizenzzuweisungssoftware greift intern auf das Citrix Lizenzportal für Ihre Lizenz zu. So greifen Sie auf eine gemeinfreie Domäne zu:
  - Verwenden Sie einen Proxyserver oder richten Sie einen DNS-Server ein.
  - Konfigurieren Sie eine Citrix ADC IP-Adresse (NSIP) oder eine Subnetz-IP-Adresse (SNIP) auf der Citrix ADC Appliance.
- Ihre Lizenz muss mit Ihrer Hardware verknüpft sein, oder Sie benötigen einen gültigen Lizenzzugriffscode. Citrix sendet Ihren Lizenzzugriffscode per E-Mail, wenn Sie eine Lizenz erwerben.

Zuweisen einer Lizenz mit der GUI

Wenn Ihre Lizenz bereits mit Ihrer Hardware verknüpft ist, kann bei der Lizenzzuweisung die Seriennummer der Hardware verwendet werden. Andernfalls müssen Sie den Lizenzzugriffscode eingeben.

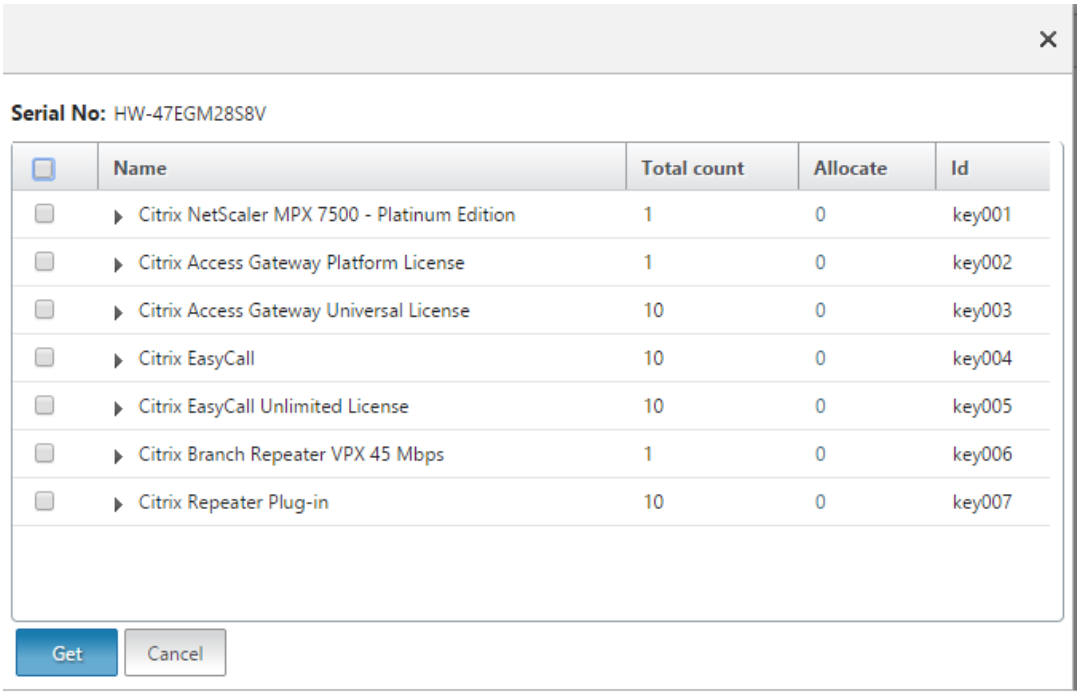
Sie können Lizenzen nach Bedarf für Ihre Bereitstellung teilweise zuweisen. Wenn Ihre Lizenzdatei beispielsweise 10 Lizenzen enthält, Ihre aktuelle Anforderung jedoch nur sechs Lizenzen umfasst, können Sie jetzt sechs Lizenzen zuweisen und später weitere Lizenzen zuweisen. Sie können nicht mehr als die Gesamtzahl der Lizenzen in Ihrer Lizenzdatei zuweisen.

So weisen Sie Ihre Lizenz zu

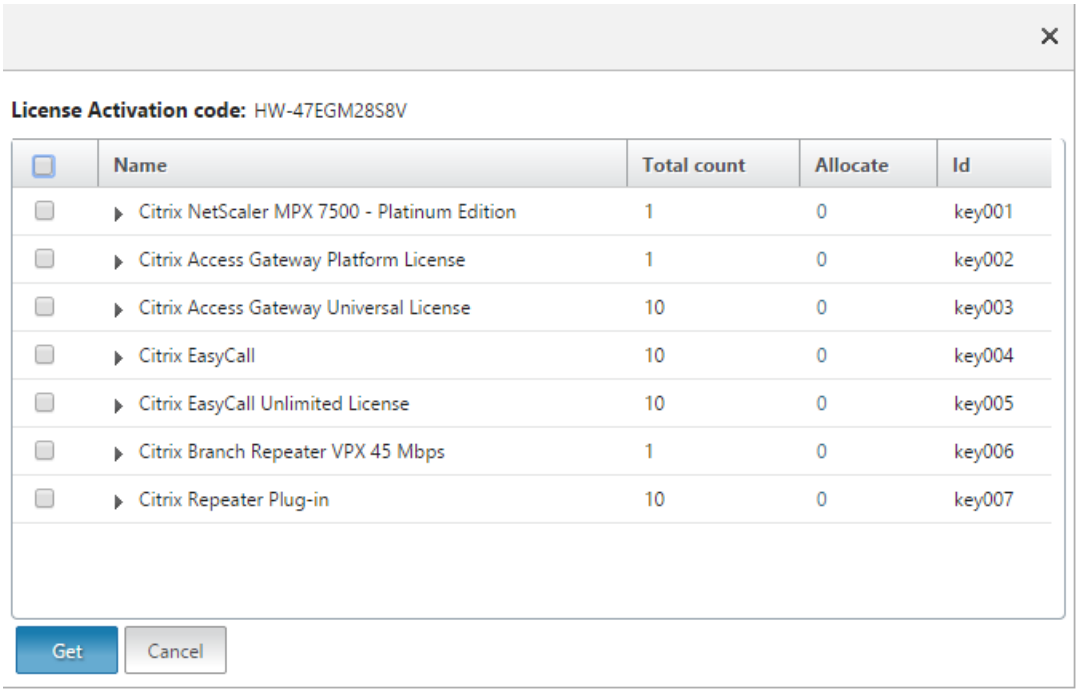
1. Geben Sie in einem Webbrowser die IP-Adresse der Citrix ADC-Appliance ein (z. B. `http://192.168.100.1`).
2. Geben Sie im Feld User Name und Password die Administratoranmeldeinformationen ein.

3. Navigieren Sie auf der Registerkarte **Configuration** zu **System > Licenses**.
4. Klicken Sie im Detailbereich auf **Lizenzen verwalten**, klicken Sie auf **Neue Lizenz hinzufügen**, und wählen Sie dann eine der folgenden Optionen aus:
   - **Seriennummer verwenden**: Die Software ruft intern die Seriennummer Ihrer Appliance ab und verwendet diese Nummer, um Ihre Lizenzen anzuzeigen.
   - **Lizenzzugriffscode verwenden**: Citrix sendet den Lizenzzugriffscode für die erworbene Lizenz per E-Mail. Geben Sie den Lizenzzugriffscode in das Textfeld ein.

     Wenn Sie keine Internetverbindung auf der Citrix ADC-Appliance konfigurieren möchten, können Sie einen Proxyserver verwenden. Aktivieren Sie das Kontrollkästchen **Connect through Proxy Server** und geben Sie die IP-Adresse und den Port des Proxyservers an.
5. Klicken Sie auf **Get Licenses**. Abhängig von der ausgewählten Option wird eines der folgenden Dialogfelder angezeigt.
   - Das folgende Dialogfeld wird angezeigt, wenn Sie Hardwareseriennummer ausgewählt haben.

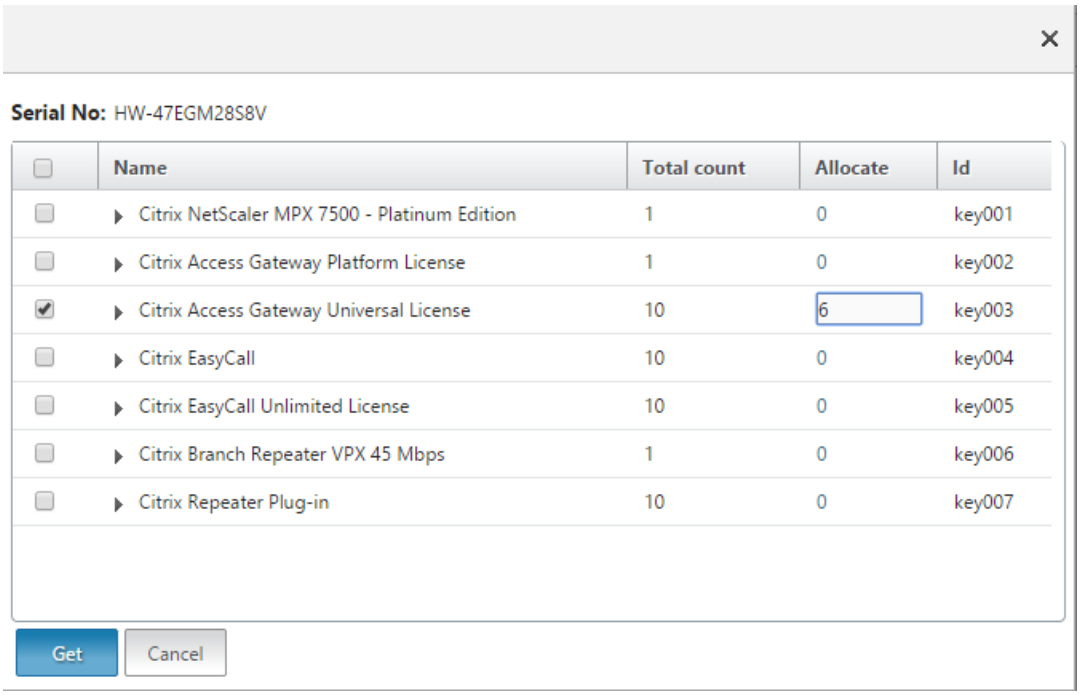


   - Das folgende Dialogfeld wird angezeigt, wenn Sie den Lizenzzugriffscode ausgewählt haben.



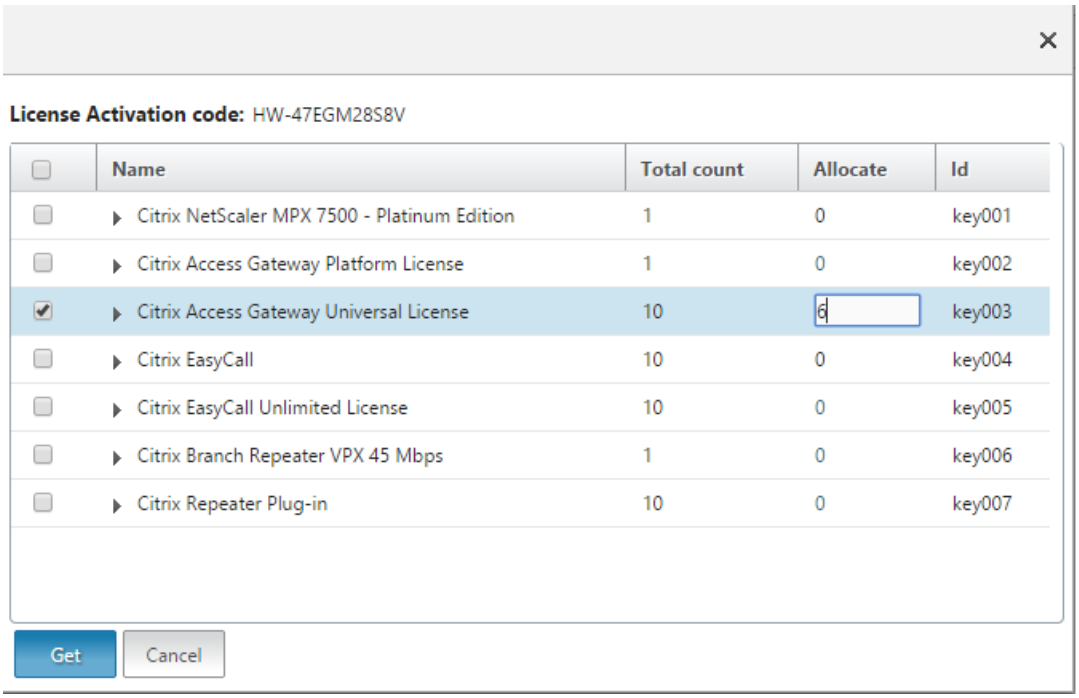
6. Wählen Sie die Lizenzdatei aus, mithilfe derer Sie Lizenzen zuteilen möchten.
7. Geben Sie in der Spalte **Zuweisen** die Anzahl der zu zuweisenden Lizenzen ein. Klicken Sie dann auf **Abrufen**.

   - Wenn Sie **Hardwareseriennummer** ausgewählt haben, geben Sie die Anzahl der Lizenzen ein, wie im folgenden Screenshot gezeigt.

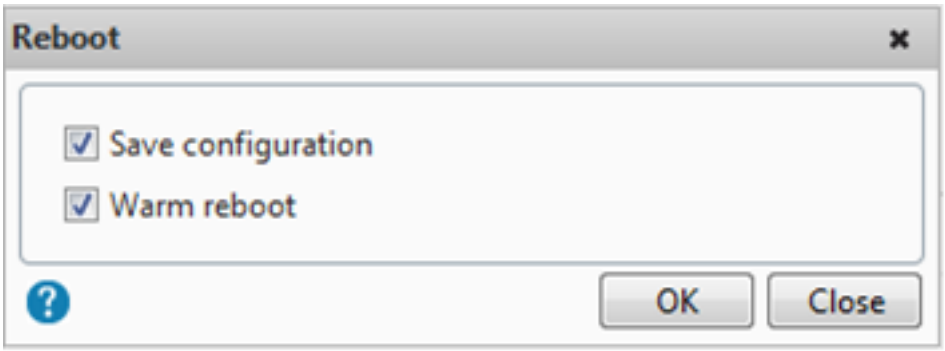


   - Wenn Sie **den Lizenzzugriffscode**ausgewählt haben, geben Sie die Anzahl der Lizenzen

ein, wie im folgenden Screenshot gezeigt.



8. Klicken Sie auf “Restart”, damit die Lizenz in Kraft tritt.
9. Klicken Sie im Dialogfeld Neustart auf **OK**, um mit den Änderungen fortzufahren, oder klicken Sie auf **Schließen**, um die Änderungen abzubrechen.



Installieren einer Lizenz

Wenn Sie die Lizenzdatei über den Zugriff auf das Lizenzierungsportal auf den lokalen Computer heruntergeladen haben, müssen Sie die Lizenz auf die Appliance hochladen.

So installieren Sie eine Lizenzdatei mit der GUI

1. Geben Sie in einem Webbrowser die IP-Adresse der Citrix ADC-Appliance ein (z. B. `http://192.168.100.1`).

2. Geben Sie im Feld User Name und Password die Administratoranmeldeinformationen ein.
3. Navigieren Sie auf der Registerkarte **Konfiguration** zu Systemlizenzen.
4. Klicken Sie im Detailbereich auf **Manage Licenses**.
5. Klicken Sie auf **Add New License** und wählen Sie dann **Upload license files from a local computer**.
6. Klicken Sie auf **Durchsuchen**. Navigieren Sie zum Speicherort der Lizenzdateien, wählen Sie die Lizenzdatei aus und klicken Sie auf **Open**.
7. Klicken Sie auf "Restart", um die Lizenz anzuwenden.
8. Klicken Sie im Dialogfeld Neustart auf **OK**, um mit den Änderungen fortzufahren, oder klicken Sie auf **Schließen**, um die Änderungen abzubrechen.

So installieren Sie die Lizenzen mit der CLI

1. Öffnen Sie eine **SSH-Verbindung** mit der ADC-Appliance mithilfe eines SSH-Clients, z. B. PuTTY.
2. Melden Sie sich mit den Administratoranmeldeinformationen bei der ADC-Appliance an.
3. Wechseln Sie zur Shell-Eingabeaufforderung, erstellen Sie ein`nsconfig` Lizenzunterverzeichnis im Verzeichnis, falls es nicht vorhanden ist, und kopieren Sie eine oder mehrere neue Lizenzdateien in dieses Verzeichnis.

   Beispiel

```
login: nsroot
Password: nsroot
Last login: Mon Aug  4 03:37:27 2008 from 10.102.29.9
Done
> shell
Last login: Mon Aug  4 03:51:42 from 10.103.25.64
root@ns# mkdir /nsconfig/license
root@ns# cd /nsconfig/license
<!--NeedCopy-->
```

   Kopieren Sie eine oder mehrere neue Lizenzdateien in dieses Verzeichnis.

   Hinweis: Die Citrix ADC Appliance fordert keine Neustartoption auf, wenn Sie die Lizenzen über die Befehlszeilenschnittstelle installieren. Führen Sie den Befehl reboot -w aus, um das System warm neu zu starten, oder führen Sie den Befehl restart aus, um das System normal neu zu starten.

Lizenzierte Funktionen überprüfen

Bevor Sie ein Feature verwenden, stellen Sie sicher, dass Ihre Lizenz das Feature unterstützt.

So überprüfen Sie die lizenzierten Funktionen mit der CLI

1. Öffnen Sie eine **SSH-Verbindung** mit der ADC-Appliance mithilfe eines SSH-Clients, z. B. PuTTY.
2. Melden Sie sich mit den Administratoranmeldeinformationen bei der ADC-Appliance an.
3. Geben Sie an der Eingabeaufforderung den Befehl sh ns license ein, um die von der Lizenz unterstützten Funktionen anzuzeigen.

   Beispiel

```
sh ns license
        License status:
                            Web Logging: YES
                        Surge Protection: YES
                          .......

                          HTML Injection: YES
 Done
<!--NeedCopy-->
```

So überprüfen Sie die lizenzierten Funktionen mit der GUI

1. Geben Sie in einem Webbrowser die IP-Adresse der ADC-Appliance ein, `http://192.168.100.1` z. B.
2. Geben Sie im Feld User Name und Password die Administratoranmeldeinformationen ein.
3. Geben Sie den Benutzernamen und das Kennwort ein, und klicken Sie auf **Anmelden**.
4. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Lizenzen**. Neben den lizenzierten Funktionen wird ein grünes Häkchen angezeigt.

Aktivieren oder Deaktivieren einer Funktion

Wenn Sie die Citrix ADC Appliance zum ersten Mal verwenden, müssen Sie ein Feature aktivieren, bevor Sie die Funktionalität nutzen können. Wenn Sie ein Feature vor der Aktivierung konfigurieren, wird eine Warnmeldung angezeigt. Die Konfiguration wird gespeichert, sie gilt jedoch erst, nachdem das Feature aktiviert wurde.

So aktivieren Sie ein Feature mit der CLI

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

- <FeatureName>Funktion aktivieren

- Funktion anzeigen

  Beispiel

```
enable feature lb cs
done
 >show feature

        Feature                        Acronym
           Status
        -------                        -------
           ------
 1)     Web Logging                    WL                    OFF
 2)     Surge Protection               SP                    ON
 3)     Load Balancing                 LB                    ON
 4)     Content Switching              CS                    ON
 5)     Cache Redirection              CR                    ON
 .
 .
 .
 24)    NetScaler Push                 push                  OFF
 Done
<!--NeedCopy-->
```

  Das Beispiel zeigt, wie Load Balancing (lb) und Content Switching (cs) aktiviert werden.

  Wenn der Lizenzschlüssel für ein bestimmtes Feature nicht verfügbar ist, wird für dieses Feature die folgende Fehlermeldung angezeigt:

  ERROR: feature(s) not licensed

  Hinweis: Um ein optionales Feature zu aktivieren, müssen Sie über eine funktionsspezifische Lizenz verfügen. Sie haben beispielsweise die Citrix NetScaler Advanced Edition-Lizenz erworben und installiert. Um die integrierte Cache-Funktion zu aktivieren, müssen Sie jedoch die AppCache Lizenz erwerben und installieren.

So deaktivieren Sie ein Feature mit der CLI

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

- <FeatureName>Funktion deaktivieren
- Funktion anzeigen

  Beispiel

Das folgende Beispiel zeigt, wie Sie den Lastausgleich (LB) deaktivieren.

```
> disable feature lb
 Done
> show feature

        Feature                         Acronym
           Status
        -------                         -------
           ------
 1)     Web Logging                     WL                      OFF
 2)     Surge Protection                SP                      ON
 3)     Load Balancing                  LB                      OFF
 4)     Content Switching               CS                      ON
 .
 .
 .
 24)    NetScaler Push                  push                    OFF
 Done
>
<!--NeedCopy-->
```

Informationen zum Ablauf der Lizenz überprüfen

Sie können die Informationen zum Ablauf der Citrix ADC -Lizenzen über GUI oder CLI überprüfen.

So überprüfen Sie Citrix ADC Lizenzablaufinformationen über die GUI:

Gehen Sie zu **Konfiguration > System > Lizenzen**.

Eine GUI-Warnung wird angezeigt, wenn das Ablaufdatum der ADC-Lizenz weniger als 30 Tage beträgt.

So überprüfen Sie die Lizenzablaufinformationen über CLI:

Geben Sie den Befehl “show ns license” ein.

```
> sh license
    License status:

    Web Logging: YES
    Surge Protection: YES

    Web Logging: YES
    Surge Protection: YES

    ...

Days to expiry: 204

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

Nach Ablauf der Lizenz generiert die Citrix ADC Appliance einen SNMP-Alarm “NS_LICENSE_EXPIRY” und ein Ablaufereignis wird an der Konsole protokolliert.

Nach Ablauf der Lizenz wird die Citrix ADC Appliance automatisch neu gestartet, um die Lizenz zu

widerrufen. Wenn die Citrix ADC Appliance Citrix Service Provider (CSP) -Lizenzen verwendet, wird die Appliance nicht automatisch neu gestartet, um die Lizenz zu widerrufen. Wenn der Benutzer die Appliance jedoch neu startet, wird sie als nicht lizenziert neu gestartet.

Upgrade einer Lizenz

Sie können eine Citrix ADC Appliance von einer Familienedition auf eine andere und von einem Kapazitätsbereich auf eine andere aktualisieren, indem Sie eine Lizenz mit höherer Kapazität erwerben.

Upgrades sind von zwei Arten:

- Editions-Upgrades: Standard auf Advanced, Standard zu Premium und Advanced to Premium. Edition-Upgrades müssen innerhalb derselben Bandbreite liegen.
- Kapazitätsupgrades: Sie können sowohl für vCPU als auch für Bandbreite von niedrigerer auf höherer Kapazität upgraden. Kapazitätsupgrades können nur für dieselbe Edition (Standard, Advanced oder Premium) durchgeführt werden.

Wenn Sie sowohl die Kapazität als auch die Edition aktualisieren möchten, starten Sie zuerst die Kapazität, starten Sie die Appliance neu, und aktualisieren Sie dann die Edition.

Beispiel: Um eine VPX 10 Mbit/s Standard Edition-Lizenz auf die VPX 200 Mbit/s Premium Edition zu aktualisieren, muss das Upgrade in zwei Schritten erfolgen.

- VPX Upgrade von 10 Mbps Standard Edition auf 200 Mbps Standard Edition.
- VPX Upgrade von 200 Mbps Standard Edition auf 200 Mbps Premium Edition.

> Hinweis:
>
> Sie können Citrix Application Delivery Management (ADM) verwenden, um ein Lizenzierungsframework zu erstellen, das einen gemeinsamen Bandbreiten- und Instanzpool umfasst. Vollständige Informationen finden Sie unter Gepoolte Kapazität von Citrix ADC.

Zugehörige Ressourcen

- Citrix Lizenzierungssystem
- Zuweisen von Citrix ADC VPX -Lizenzen

Daten-Governance

January 28, 2022

Was ist Citrix ADM Service Connect?

Citrix Application Delivery Management (ADM) Service Connect ist eine Funktion, die das nahtlose Onboarding von Citrix ADC MPX-, SDX- und VPX-Instanzen sowie Citrix Gateway-Appliances in den Citrix ADM Service ermöglicht. Mit dieser Funktion können die Citrix ADC-Instanz oder die Citrix Gateway-Appliance automatisch eine sichere Verbindung mit dem Citrix ADM Service herstellen und System-, Nutzungs- und Telemetriedaten an sie senden. Auf der Grundlage dieser Daten erhalten Sie Einblicke und Empfehlungen für Ihre Citrix ADC-Infrastruktur für den Citrix ADM Service.

Verwenden Sie die Verbindungsfunktion des Citrix ADM Service ADM Servicees und Onboarding Ihrer Citrix ADC-Instanzen oder Citrix Gateway-Appliances in den Citrix ADM Service. Sie können auch alle Ihre Citrix ADC und Citrix Gateway -Assets verwalten, ob lokal oder in der Cloud. Außerdem profitieren Sie vom Zugriff auf eine Vielzahl von Sichtbarkeitsfunktionen, die bei der schnellen Identifizierung von Leistungsproblemen, hoher Ressourcennutzung, kritischen Fehlern usw. helfen. Der Citrix ADM -Service bietet eine Vielzahl von Funktionen für Ihre Citrix ADC Instanzen und -Anwendungen. Weitere Informationen zum Citrix ADM Service finden Sie unter Citrix Application Delivery Management Service

> **Wichtig**
>
> - Die Citrix Gateway -Appliance unterstützt auch die Funktion “Citrix ADM Service Connect”. Zur besseren Vereinfachung wird die Citrix Gateway-Appliance in den aufeinanderfolgenden Abschnitten nicht explizit aufgerufen.

Was ist der Citrix ADM Dienst?

Der Citrix ADM Service ist eine Cloud-basierte Lösung, mit der Sie Ihre Citrix ADC-Instanzen verwalten, überwachen, orchestrieren, automatisieren und Fehler beheben können. Es bietet Ihnen auch analytische Einblicke und kuratierte, auf maschinellem Lernen basierende Empfehlungen zu Citrix ADC Instanzen sowie zu Anwendungsstatus, Leistung und Sicherheit. Weitere Informationen finden Sie unter Überblick über den Citrix ADM Service

Wie ist der Citrix ADM Service Connect aktiviert?

Citrix ADM Service Connect ist standardmäßig aktiviert, nachdem Sie Citrix ADC oder Gateway auf Version 13.0 Build 61.xx und höher installiert oder aktualisiert haben.

Welche Daten werden mit Citrix ADM Service Connect erfasst?

Die folgenden Details werden mit Citrix ADM Service Connect erfasst:

- **Citrix ADC Einzelheiten**
  - Seriennummer

  - Codierte Seriennummer
  - Host-ID
  - UUID
  - Verwaltungs-IP-Adresse
  - Hostname
  - Version
  - Buildtyp
  - Build
  - Lizenztyp
  - Hypervisor
  - Bereitstellungstyp (Standalone/HA)
  - Plattformtyp
  - Beschreibung der Plattform
  - System-ID
  - Modi aktiviert auf ADC
  - Auf ADC aktivierte Funktionen

- **Informationen zur Lizenz**
  - Auf Citrix ADC lizenzierte Funktionen
  - Nummer der Lizenz

- **Wichtige Nutzungsmetriken**
  - Datum und Uhrzeit des Systems
  - CPU-Nutzung in Prozent
  - Prozentsatz der Verwaltungs-C
  - Durchsatz
  - SSL neue Sessions
  - Durchsatz der SSL-Verschlüsselung
  - Durchsatz bei SSL-Entschlüsselung
  - Systembetriebszeit

- **Konfiguration**
  - ns.conf

> **Hinweis**
>
> Bevor der Citrix ADM Service Connect die `ns.conf` Datei von der Citrix ADC Appliance an den Citrix ADM Service sendet, anonymisiert er die verschlüsselten oder gehashten Kennwörter. Der Citrix ADM Service Connect sucht nach “-verschlüsselten” oder “-Passcrypt” -Parametern und ersetzt den zugehörigen verschlüsselten oder gehashten Wert durch ‘XXXX’. Der Citrix ADM Service Connect kodiert und komprimiert die `ns.conf` Datei dann

> und sendet sie an den Endpunkt des Citrix ADM-Service.

- **Details zum kritischen Fehler**
  - Festplattenausfälle
  - Ausfälle der SSL-Karte
  - Ausfälle der Stromversorgungseinheit (PSU)
  - Ausfall des Flashlaufwerks
  - Warmer Neustart
  - Anhaltende Speichernutzung über 90% oder ein Speicherleck
  - Anhaltende Zinsgrenze sinkt
- **Einzelheiten zur Diagnostik**

  > Hinweis:
  >
  > Das ADM-Diagnosetool verwendet die folgenden Diagnosedetails. Weitere Informationen finden Sie im Thema Diagnosetool in Citrix ADM.

  - ADC-CLI-Status
  - ADC-DNS-Status
  - Netzwerkverbindungsstatus zum ADM-Endpunkt “adm.cloud.com”
  - Netzwerkverbindungsstatus zum ADM-Endpunkt “agent.adm.cloud.com”
  - Netzwerkverbindungsstatus zum ADM-Vertrauensdienst “trust.citrixnetworkapi.net”
  - Netzwerkverbindungsstatus zur ADM-Download-Site “download.citrixnetworkapi.net”

Wie werden die Daten verwendet?

Durch die Erfassung der Daten kann Citrix Ihnen zeitnahe und detaillierte Einblicke in Ihre Citrix ADC-Installationen geben, darunter die folgenden:

- **Die wichtigsten Kennzahlen**. Details zu wichtigen Metriken zu CPU, Arbeitsspeicher, Durchsatz, SSL-Durchsatz und heben anomales Verhalten auf Citrix ADC-Instanzen hervor.
- **Kritische Fehler**. Alle kritischen Fehler, die möglicherweise in Ihren Citrix ADC-Instanzen aufgetreten sind.
- **Beratung zur Bereitstellung**. Identifizieren Sie Citrix ADC Instanzen, die im Standalone-Modus bereitgestellt werden, aber einen hohen Durchsatz haben und anfällig für einen einzelnen Fehlerpunkt sind.
- **Diagnose-Tool**. Wenn Sie eine ADC-Instanz in Citrix ADM integrieren, treten möglicherweise einige Probleme auf, die das erfolgreiche Onboarding der ADC-Instanz verhindern. Um die Probleme zu beheben, können Sie das Diagnosetool entweder manuell verwenden oder die Diagnoseinformationen in der ADM-GUI einsehen. Weitere Informationen finden Sie unter Diagnosetool.

Wie lange werden die gesammelten Daten aufbewahrt?

Alle gesammelten Daten werden nicht länger als 13 Monate aufbewahrt.

Wenn Sie sich dazu entschließen, die Nutzung des Dienstes zu beenden, indem Sie die Citrix ADM Service Connect-Funktion vom Citrix ADC deaktivieren, werden alle zuvor gesammelten Daten nach einem Zeitraum von 30 Tagen gelöscht.

Wo werden die Daten gespeichert und wie sicher sind sie?

Alle vom Citrix ADM Service Connect gesammelten Daten werden in einer der drei Regionen gespeichert — USA, Europäische Union und Australien und Neuseeland (ANZ). Weitere Informationen finden Sie unter Geografische Überlegungen.

Die Daten werden sicher mit strenger Tenant-Isolation auf der Datenbankschicht gespeichert.

Wie deaktiviere ich Citrix ADM Service Connect?

Wenn Sie die Datenerfassung über den Citrix ADM Service Connect deaktivieren möchten, finden Sie unter So aktivieren und deaktivieren Sie den Citrix ADM Service Connect.

Einführung in Citrix ADM Service Connect für Citrix ADC Appliances

February 24, 2022

Der Citrix ADM Service ist eine Cloud-basierte Lösung, mit der Sie Ihre Citrix ADC-Instanzen verwalten, überwachen, orchestrieren, automatisieren und Fehler beheben können. Es bietet auch analytische Erkenntnisse und kuratierte auf maschinellem Lernen basierende Empfehlungen für den Zustand, die Leistung und die Sicherheit Ihrer Anwendungen. Weitere Informationen finden Sie unter Citrix Application Delivery Management Service.

Citrix Application Delivery Management Service Connect ist eine Funktion, die das nahtlose Onboarding von Citrix ADC Instanzen in den Citrix ADM Dienst ermöglicht. Diese Funktion hilft Citrix ADC Instanzen und dem Citrix ADM Service, als ganzheitliche Lösung zu fungieren, die Kunden mehrfache Vorteile bietet.

Mit der Citrix ADM Service Connect-Funktion kann die Citrix ADC Instanz automatisch eine Verbindung mit dem Citrix ADM Dienst herstellen und System-, Nutzungs- und Telemetriedaten an sie senden. Basierend auf diesen Daten gibt Ihnen der Citrix ADM Service einige Einblicke und Empfehlungen zu Ihrer Citrix ADC- und Gateway-Infrastruktur wie folgt:

- Einblicke in Sicherheitsberatung, die Ihre gefährdeten ADC-Appliances hervorheben.

- Aktualisieren Sie die beratenden Erkenntnisse, in denen ADC-Geräte hervorgehoben werden, die das Ende der Wartung und das Ende der Lebensdauer erreicht haben oder gerade erreicht haben.
- Schnelle Identifizierung von Leistungsproblemen, hoher Ressourcennutzung und kritischen Fehlern.

Um die Leistungsfähigkeit des Citrix ADM Dienstes zu nutzen, können Sie Ihre Citrix ADC Instanzen für den Citrix ADM Dienst einbinden. Der Onboarding-Prozess nutzt ADM Service Connect und macht das Erlebnis für Sie reibungslos und schneller.

> **Wichtige Hinweise**
>
> - Citrix ADM Service Connect ist jetzt auf Citrix ADC MPX-, SDX- und VPX-Instanzen und Citrix Gateway -Appliances verfügbar.
> - Die Initiative im Citrix ADM Service, die diese Funktion für Citrix ADM Service Connect verwendet, ist das auf ADM Service Connect basierendes Low-Touch-Onboarding. Weitere Informationen finden Sie unter Berührungsarmes Onboarding von Citrix ADC-Instanzen mit Citrix ADM Service Connect.
> - Wenn ADM Service Connect auf einer ADC-Instanz aktiviert ist, werden bestimmte Diagnosedetails automatisch an den ADM Service gesendet.

Weitere Informationen finden Sie unter Data Governance.

> **Wichtig**
>
> Citrix ADM Service Connect erfasst die Prüfdaten nicht und kann nicht beim Einsteigen der ADC Appliance in den ADM Service helfen, wenn die folgenden Bedingungen erfüllt sind:
>
> - `NSinternal` das Benutzerkonto ist deaktiviert.
> - Der öffentliche SSH-Schlüssel ist nicht eingerichtet.
>
> Um das vorhergehende Szenario zu überwinden, empfiehlt Citrix, eine der folgenden Aktionen zu befolgen:
>
> - Aktivieren Sie das `internaluser` Benutzerkonto mithilfe des `set ns param -internaluserlogin ENABLED`.
> - Konfigurieren Sie die öffentliche Schlüsselauthentifizierung. Weitere Informationen finden Sie unter Zugriff auf eine Citrix ADC Appliance mit SSH-Schlüsseln und ohne Kennwort.

Wie verbindet der Citrix ADM Service die Unterstützung mit dem Citrix ADM Service?

Hier ist ein hochrangiger Workflow, wie Citrix ADM Service Connect in Citrix ADC mit Citrix ADM Service interagiert.

1. Citrix ADM Service Connects auf der Citrix ADC Appliance stellt mithilfe einer regelmäßigen Sondenanforderung automatisch eine Verbindung mit dem Citrix ADM Service her.
2. Diese Anforderung enthält System-, Nutzungs- und Telemetriedaten, mit denen der Citrix ADM Service Ihnen einige Einblicke und Empfehlungen zu Ihrer Citrix ADC-Infrastruktur gibt. Wie; schnelle Identifizierung von Leistungsproblemen, hohem Ressourcenverbrauch und kritischen Fehlern.
3. Sie können die Erkenntnisse und Empfehlungen anzeigen und beschließen, Ihre ADC-Instanzen in den Citrix ADM Service einzubinden, um mit der Verwaltung Ihrer Citrix ADC-Instanzen zu beginnen.
4. Wenn Sie sich für das Onboarding entscheiden, hilft Citrix ADM Service Connect dabei, das Onboarding nahtlos abzuschließen.

Auf welchen Versionen von Citrix ADC wird Citrix ADM Service Connect unterstützt?

Citrix ADM Service Connect wird auf allen Citrix ADC-Plattformen und allen Appliance-Modellen (MPX, VPX und SDX) unterstützt. Ab Citrix ADC Release 13.0 Build 61.xx ist Citrix ADM Service Connect standardmäßig für Citrix ADC Appliances aktiviert.

Wie aktiviere ich Citrix ADM Service Connect?

Wenn Sie ein bestehender Citrix ADC-Kunde sind und ein Upgrade auf Citrix ADC Release 13.0 Build 61.xx durchführen, ist Citrix ADM Service Connect im Rahmen des Upgrade-Vorgangs standardmäßig aktiviert.

Wenn Sie ein neuer Citrix ADC-Kunde sind und Citrix ADC Release 13.0 Build 61.xx installieren, ist Citrix ADM Service Connect standardmäßig als Teil des Installationsvorgangs aktiviert.

> **Hinweis**
>
> Im Gegensatz zu den neuen Citrix ADC Appliances finden vorhandene Citrix ADC Appliances die Route über den Citrix Insight Service (CIS) oder Call Home.

Wie aktiviere und deaktiviere ich Citrix ADM Service Connect?

Sie können Citrix ADM Service Connect über CLI-, GUI- oder NITRO-API-Methoden aktivieren und deaktivieren.

CLI verwenden

Um den Citrix ADM Service zu aktivieren, stellen Sie eine Verbindung mithilfe der CLI her.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set adm parameter -admserviceconnect ENABLED
```

So deaktivieren Sie Citrix ADM Service Connect mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set adm parameter -admserviceconnect DISABLED
```

> **Wichtig**
>
> Wenn sich Ihr Citrix ADC in Release 13.0 Build 61.xx befindet, lautet der Parametername zum Aktivieren oder Deaktivieren des Citrix ADC Service Connect “Autoconnect. “ Verwenden Sie zum Beispiel den `set adm parameter - autoconnect ENABLED` Befehl, um Service Connect zu aktivieren.

Verwenden der GUI

Citrix ADM Service Connect über die Citrix ADC-GUI deaktivieren

1. Geben Sie in einem Webbrowser die IP-Adresse der Citrix ADC-Appliance ein (z. B. http://192.0.2.10).
2. Geben Sie **unter Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie zu **System > Einstellungen > ADM-Parameter konfigurieren**.
4. Deaktivieren Sie auf der Seite **ADM-Parameter konfigurieren** das Dialogfeld **Citrix ADM Service Connect aktivieren**, und klicken Sie auf **OK**.

Verwenden der NITRO-API

Sie können Citrix ADM Service Connect mit dem Befehl **NITRO** deaktivieren.

- In Citrix ADC Release 13.0 Build 61.xx können Sie Citrix ADM Service Connect mit dem folgenden Befehl aktivieren oder deaktivieren:
  - `curl -X PUT -H ”Content-Type:application/json”http://192.0.2.10/nitro/v1/config/admparameter> -d '{ ”admparameter”:{ ”autoconnect”:”enabled” } } ' -u nsroot:Test@1`
- Ab Citrix ADC Release 13.0 Build 64.xx wird der Parametername “autoconnect” in umbenannt `admserviceconnect`. Sie können Citrix ADM Service Connect mit dem folgenden Befehl deaktivieren:


```
- curl -X PUT -H "Content-Type:application/json" http://192.0.2.10/
  nitro/v1/config/admparameter -d '{ "admparameter":{ "admserviceconnect
  ":"disabled" } } ' -u nsroot:Test@1
```

Diagnose-Tool

Wenn Sie eine ADC-Instanz in Citrix ADM integrieren, treten möglicherweise einige Probleme auf, die das erfolgreiche Onboarding der ADC-Instanz verhindern. Um die Probleme zu beheben, können Sie das Diagnosetool entweder manuell verwenden oder die Diagnoseinformationen in der ADM-GUI einsehen.

- Weitere Informationen zu den Details, die mit ADM Service Connect erfasst wurden, finden Sie unter Datenverwaltung.
- Weitere Informationen zum Diagnose-Tool finden Sie unter Diagnosetool.

Integriertes Agentenverhalten von Citrix ADM

Ab Citrix ADC Release 13.0 Build 61.xx und höher kommuniziert der in Citrix ADC-Instanzen verfügbare Citrix ADM-Agent mit dem ADM Service. Es kommuniziert ohne die Notwendigkeit einer manuellen Initialisierung auf der jeweiligen ADC-Instanz. Nachdem die Kommunikation mit dem ADM Service hergestellt wurde, bleibt der integrierte Agent immergrün, indem er sich regelmäßig automatisch auf die neueste Softwareversion aktualisiert.

Zuvor mussten Sie den integrierten Agenten auf den ADC-Instanzen mit `mastools` Befehlen initialisieren, um die Kommunikation mit dem ADM Service herzustellen und regelmäßige automatische Upgrades zu erstellen.
Weitere Informationen finden Sie unter Konfigurieren des integrierten ADC-Agenten für die Verwaltung von Instanzen.

Referenzen

Weitere Informationen zu Citrix ADM Service Connect finden Sie in den folgenden Themen:

- Data Governance: Data Governance.
- Citrix ADM Service: Citrix Application Delivery Management Service.

Upgrade und Downgrade einer Citrix ADC Appliance

October 5, 2021

> **Hinweis:**
>
> Citrix ADM Service Connect ist standardmäßig aktiviert, nachdem Sie Citrix ADC oder Citrix Gateway installiert oder aktualisiert haben, um 13.0 Build 61.xx und höher freizugeben. Weitere Informationen finden Sie unter Data Governance und Citrix ADM Service verbinden.

Citrix ADC 13.0 bietet neue und aktualisierte Funktionen mit erhöhter Funktionalität. Eine umfassende Liste der Erweiterungen finden Sie in den Versionshinweisen zur Versionsankündigung. Lesen Sie die Versionshinweise, bevor Sie Ihre Software aktualisieren.

Dieser Abschnitt enthält Informationen zum **Aktualisieren und Herunterstufen einer Citrix ADC Appliance** (MPX und VPX) Firmware **mithilfe der Citrix ADC GUI oder CLI**.

Sie können **Citrix ADM auch verwenden, um eine Citrix ADC Appliance zu aktualisieren**. Weitere Informationen:

- 10 Arten, wie der Citrix ADM -Service einfachere Citrix ADC Upgrades unterstützt
- Verwenden Sie den Citrix ADM Dienst, um Citrix ADC Instanzen zu aktualisieren
- Verwenden Sie Citrix ADM -Software, um Citrix ADC Instanzen zu aktualisieren

Informationen zum **Upgrade einer Citrix ADC SDX-Appliance**finden Sie unterUpgrade eines einzelnen Pakets.

Voraussetzungen

December 3, 2021

Bevor Sie mit dem Upgrade- oder Downgrade-Prozess beginnen, überprüfen Sie Folgendes:

- Zeit für das Upgrade von Citrix ADC-Appliances. Befolgen Sie das Verfahren zur Änderungskontrolle Ihrer Organisation. Weisen Sie doppelt so viel Zeit zu, um die Upgrades durchzuführen. Weisen Sie genügend Zeit zu, um jede der Citrix ADC-Appliance zu aktualisieren.
- Bewerten Sie die Support-Vereinbarung Ihres Unternehmens. Seriennummer der Dokumenteneinheit, Supportvereinbarung und Kontaktdetails für den Support vom Technischen Support von Citrix oder dem autorisierten Citrix Partner.
- Das Lizenzierungs-Framework und die Arten von Lizenzen. Ein Software-Edition-Upgrade erfordert möglicherweise neue Lizenzen, wie zum Beispiel:
  - ein Upgrade von der Standard Edition auf die Advanced Edition oder
  - die Standardausgabe zur Premium Edition oder
  - die Advanced Edition zur Premium Edition.

Vorhandene Citrix ADC -Lizenzen funktionieren weiterhin, wenn Sie auf Version 13.0 aktualisieren. Weitere Informationen finden Sie unter Lizenzierung

- Suchen Sie nach neuen und veralteten Befehlen, Parametern und SNMP-OIDs.
- Suchen Sie nach Citrix ADC MPX Hardware- und Softwarekompatibilitätsmatrix.
- Wenn die Anmeldeseite Citrix ADC Gateway angepasst ist, stellen Sie sicher, dass das Benutzeroberflächendesign auf Standard festgelegt ist.
- Wenn Sie ein Upgrade von LOM durchführen, lesen Sie die Seite LOM-Firmware-Upgrade.
- Laden Sie die Citrix ADC Firmware von den Citrix ADC Downloads herunter. Die detaillierten Schritte zum Herunterladen der Citrix ADC-Firmware finden Sie im Downloaden eines Citrix ADC-Versionspakets.
- Sichern Sie die Dateien. Führen Sie eine Sicherung der Konfigurationsdatei, der Anpassungsdatei, der Zertifikate, der Überwachungsskripte, der Lizenzdateien usw. entweder manuell durch oder lesen Sie die folgende Dokumentation zur Sicherung mit Citrix ADC CLI oder GUI - Backup und Wiederherstellung.
  - Weitere allgemeine benutzerdefinierte Dateien für das Backup finden Sie in der folgenden Liste.
    * `/nsconfig/monitors/*.pl`
    * `/nsconfig/htmlinjection/*`
    * `/nsconfig/rc.netscaler`
  - Sichern Sie den Anpassungsordner. Dies ist normalerweise unter `/var/customizations`. Ein Beispiel für die Anpassung ist eine Anmeldeseite mit einem Logo. Nachdem Sie den Anpassungsordner kopiert haben, müssen Sie ihn von der Citrix ADC-Appliance löschen, bevor Sie die Appliance aktualisieren. Ein Upgrade mit der Anpassung kann einige Probleme verursachen.

  > **Wichtig:**
  > Citrix empfiehlt dringend, die oben genannten Backup-Verfahren zu überprüfen. Haben Sie einen Aktionsplan für den Fall, dass das Update auf der Citrix ADC-Appliance nicht abgeschlossen wird.

- Stellen Sie sicher, dass im Verzeichnis /var und /flash ausreichend Platz für die Citrix ADC-Appliance vorhanden ist, bevor Sie ein Upgrade durchführen. Der /var benötigt 5 GB freien Speicherplatz (1 GB für das Upgrade-Paket + 4 GB für den Upgrade-Prozess)
  Der /flash benötigt genügend Speicherplatz, um über den neuen Kernel zu kopieren, der sich zwischen 140 MB und 160 MB unterscheidet, um sicherzustellen, dass mindestens 250 MB freier Speicherplatz verfügbar ist.
  Weitere Informationen zum Löschen des Speicherplatzes in /var finden Sie unter So geben Sie Speicherplatz im Verzeichnis /var frei, um Probleme mit einer Citrix ADC-Appliance zu

protokollieren.
Weitere Informationen zum Löschen des Speicherplatzes in /flash finden Sie unter https://support.citrix.com/article/CTX133587.

- Überprüfen Sie die Integrität der Citrix ADC-Appliance. Wenn Sie über eine Citrix ADC-Hardware-Appliance verfügen, empfiehlt Citrix dringend, mit `fsck`eine Datenträgerprüfung durchzuführen und die Integrität der Citrix ADC-Festplatte zu überprüfen. Im Falle eines Fehlers setzen Sie das Festplattenlaufwerk zurück und wiederholen Sie den Befehl Disk check. Wenn die Fehlermeldung erneut angezeigt wird, wenden Sie sich an den Citrix Support, um das Problem weiter zu untersuchen.
  - Überprüfen Sie die Datenträgerintegrität der Festplatte mit dem Befehl fsck. Weitere Informationen finden Sie unter CTX122845.
  - Überprüfen Sie die Integrität der Citrix ADC-Appliance mithilfe der Diagnosepaketdateien und laden Sie die Protokolle zur Analyse in Citrix Insight Service hoch. Weitere Informationen finden Sie unter So sammeln Sie ein Paket für den technischen Support.
- Überprüfen Sie die Citrix ADC VPX Support-Matrix und die Nutzungsrichtlinien.
- Prüfen Sie den FAQ-Bereich .
- Es ist eine bewährte Methode, ein Upgrade auf eine Hauptversion zu einem Zeitpunkt durchzuführen. Aktualisieren Sie nicht direkt auf die neueste Version.

  Wenn sich die Citrix ADC-Appliance beispielsweise in Release 12.0 befindet und Sie ein Upgrade auf Version 13.0 durchführen möchten, müssen Sie die Appliance zuerst auf Version 12.1 und dann auf Version 13.0 aktualisieren.
- Überprüfen Sie die Upgrade-Verfahren mit einer Testumgebung.

Weitere Informationen zu den Voraussetzungen für das Upgrade oder Downgrade der Citrix ADC-Appliance finden Sie in diesen Supportartikeln:

- CTX220371: Muss Artikel vor und nach dem Upgrade von Citrix ADC lesen

Überlegungen zum Upgrade - SNMP-Konfiguration

October 5, 2021

Der Timeout-Parameter für einen SNMP-Alarm ist eine interne Option, die keinen Einfluss auf die Alarmkonfiguration hat.

Der Timeout-Parameter kann in den SNMP-Alarmkonfigurationen in der laufenden Konfiguration (sh läuft) und der gespeicherten Konfiguration (ns.conf) angezeigt werden, selbst wenn Sie keine Änderungen an diesen SNMP-Alarmkonfigurationen vorgenommen haben.

Beim Upgrade auf einen Release-Build mit dem Fix für das Problem der Timeout-Einstellung werden die SNMP-Konfigurationen fälschlicherweise auf die Standardwerte zurückgesetzt.

Die folgenden SNMP-Alarme (falls konfiguriert) sind während eines Upgrades betroffen:

- APPFW-BUFFER-OVERFLOW
- APPFW-COOKIE
- APPFW-CSRF-TAG
- APPFW-DENY-URL
- APPFW-FIELD-CONSISTENCY
- APPFW-FIELD-FORMAT
- APPFW-POLICY-HIT
- APPFW-REFERER-HEADER
- APPFW-SAFE-COMMERCE
- APPFW-SAFE-OBJECT
- APPFW-SQL
- APPFW-START-URL
- APPFW-VIOLATIONS-TYPE
- APPFW-XML-ATTACHMENT
- APPFW-XML-DOS
- APPFW-XML-SCHEMA-COMPILE
- APPFW-XML-SOAP-FAULT
- APPFW-XML-SQL
- APPFW-XML-VALIDATION
- APPFW-XML-WSI
- APPFW-XML-XSS
- APPFW-XSS
- CLUSTER-BACKPLANE-HB-MISSING
- CLUSTER-NODE-HEALTH
- CLUSTER-NODE-QUORUM
- CLUSTER-VERSION-MISMATCH
- COMPACT-FLASH-ERRORS
- CONFIG-CHANGE
- CONFIG-SAVE
- HA-BAD-SECONDARY-STATE
- HA-NO-HEARTBEATS
- HA-SYNC-FAILURE
- HA-VERSION-MISMATCH
- HARD-DISK-DRIVE-ERRORS
- HA-STATE-CHANGE
- HA-STICKY-PRIMARY

- PORT-ALLOC-FAILED
- SYNFLOOD

Diese SNMP-Alarmkonfigurationen sind betroffen, wenn Sie den Citrix ADC auf die folgenden Release-Builds aktualisieren:

- Release 11.1 Build 61.2 oder höher
- Release 12.0 Build 61.0 oder höher
- Release 12.1 Build 30.1 oder höher
- Release 13.0 Build 51.4 oder höher

Beispiel

Betrachten wir ein Beispiel für den CLUSTER-NODE-HEALTH SNMP-Alarm.

```
1 CLUSTER-NODE-HEALTH SNMP alarm is set up by using the Citrix ADC
     command line:
2
3 > set snmp alarm CLUSTER-NODE-HEALTH -time 111 -state DISABLED -
     severity Major
4
5 > save config
6 <!--NeedCopy-->
```

Diese SNMP-Alarmkonfiguration wird in der gespeicherten Konfigurationsdatei (`ns.conf`) wie folgt angezeigt:

```
1 set snmp alarm CLUSTER-NODE-HEALTH -time 111 -state DISABLED -severity
     Major -timeout 86400
2
3 <!--NeedCopy-->
```

Während eines Upgrades auf einen der oben genannten Release-Builds wird der folgende Fehler in der Datei ns.log angezeigt:

```
1 May 23 09:14:46 <local0.err> ns nsconfigd: __init_config_filter(): (
     null) line 0: No such argument [-timeout]>> set snmp alarm CLUSTER-
     NODE-HEALTH -time 111 -state DISABLED -severity Major -timeout
     86400.
2 <!--NeedCopy-->
```


Nach dem Upgrade werden die SNMP-Alarmkonfigurationen auf die Standardwerte zurückgesetzt.

Workaround

Verwenden Sie einen der folgenden Workarounds:

- Entfernen Sie vor dem Upgrade die Timeout-Einstellung aus den SNMP-Konfigurationen in der gespeicherten Konfigurationsdatei (ns.conf).
- Konfigurieren Sie nach dem Upgrade die SNMP-Alarme ohne den Timeout-Parameter neu.

Download eines Citrix ADC-Releasepakets

October 5, 2021

Führen Sie die folgenden Schritte aus, um ein Citrix ADC Releasepaket herunterzuladen:

1. Öffnen Sie die Seite Citrix ADC Downloads in einem Webbrowser.
2. Erweitern Sie auf der Seite Citrix ADC Downloads die **Citrix ADC Version**, auf die Sie aktualisieren möchten.
3. Erweitern Sie eine der entsprechenden Kategorien und klicken Sie auf den Build-Link für Citrix ADC. Um beispielsweise eine Version der Citrix ADC Firmware herunterzuladen, erweitern Sie die **Firmware**und klicken Sie auf den Citrix ADC-Build, den Sie herunterladen möchten.
4. Erweitern Sie auf der ausgewählten Citrix ADC Buildseite den Abschnitt **Build** und klicken Sie auf **Datei herunterladen**, um das Citrix ADC Build-Paket herunterzuladen.

> **Hinweis:**
> Die Prüfsumme wird bereitgestellt, um sicherzustellen, dass Sie das heruntergeladene Baupaket mit dem tatsächlichen Paket abgleichen, das auf der Website gehostet wird. Die Prüfsumme ist ein wichtiger Check, um sicherzustellen, dass Sie die richtigen Bits haben.

Upgrade einer eigenständigen Citrix ADC Appliance

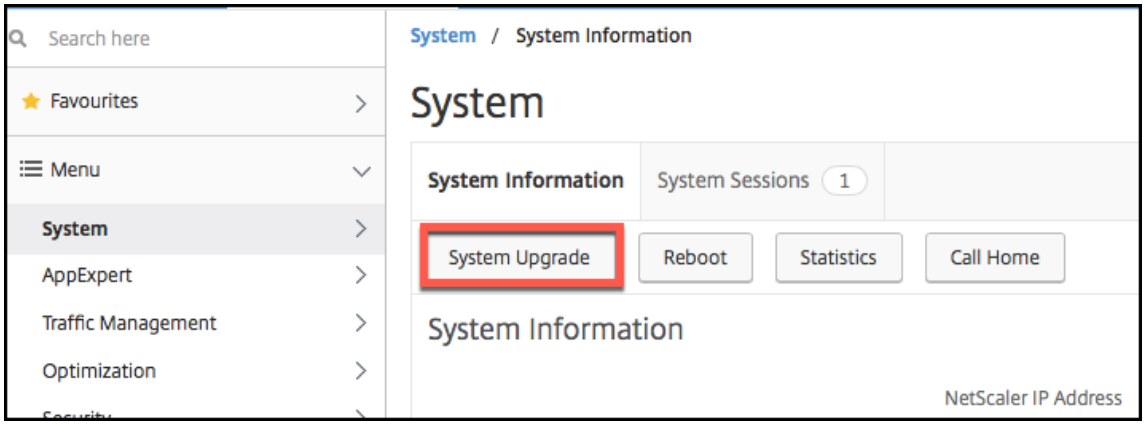
October 5, 2021

Bevor Sie die Systemsoftware aktualisieren, lesen Sie den Abschnitt Bevor Sie beginnen, und erfüllen Sie die Voraussetzungen wie das Sichern der erforderlichen Dateien und das Herunterladen der Citrix ADC-Firmware.

Upgrade einer eigenständigen Citrix ADC Appliance über die GUI

Führen Sie die folgenden Schritte aus, um ein eigenständiges Citrix ADC auf Version 13.0 mit der GUI zu aktualisieren.

1. Geben Sie in einem Webbrowser die IP-Adresse des Citrix ADC ein, z. B. `http://10.102.29.50` .
2. Geben Sie unter Benutzername und Kennwort die Administratoranmeldeinformationen ein (nsroot/nsroot), und klicken Sie dann auf **Anmelden**.
3. Klicken Sie auf der grafischen Benutzeroberfläche auf **Systemupgrade**.



4. Wählen Sie im Menü **Datei** auswählen die entsprechende Option: **Lokal** oder **Appliance**. Wenn Sie die Appliance-Option verwenden möchten, muss die Firmware zuerst in den Citrix ADC hochgeladen werden. Sie können eine beliebige Dateiübertragungsmethode wie WinSCP verwenden, um die Citrix ADC Firmware auf die Appliance hochzuladen.
5. Wählen Sie die richtige Datei aus und klicken Sie auf **Aktualisieren**.
6. Folgen Sie den Anweisungen, um die Software zu aktualisieren.
7. Wenn Sie dazu aufgefordert werden, wählen Sie **Neustart** aus.

Schließen Sie nach dem Upgrade alle Browser-Instanzen und löschen Sie den Cache Ihres Computers, bevor Sie auf die Appliance zugreifen.

Upgrade einer eigenständigen Citrix ADC Appliance mit der CLI

Führen Sie die folgenden Schritte aus, um ein eigenständiges Citrix ADC auf Version 13.0 mit der CLI zu aktualisieren:

Im folgenden Verfahren <release> und <releasenumber> stellen Sie die Release-Version dar, auf die Sie upgraden, und <targetbuildnumber> stellt die Build-Nummer dar, auf die Sie upgraden. Das Verfahren enthält optionale Schritte, um zu vermeiden, dass Aktualisierungen, die während des Upgrades in das Verzeichnis /etc übertragen werden, verloren gehen.

1. Verwenden Sie einen SSH-Client, z. B. PuTTY, um eine SSH-Verbindung zur Appliance zu öffnen.
2. Melden Sie sich mit den Administratoranmeldeinformationen bei der Appliance an. Speichern Sie die laufende Konfiguration. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   save config
   ```

3. Wechseln Sie zur Shell-Eingabeaufforderung, indem Sie den folgenden Befehl ausführen:

   ```
   shell
   ```

4. Erstellen Sie eine Kopie der Datei ns.conf. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

   - `cd /nsconfig`
   - `cp ns.conf ns.conf.NS<currentreleasenumber><currentbuildnumber>`

   Sie sollten die Konfigurationsdatei auf einem anderen Computer sichern.

5. (Optional) Wenn Sie einige der folgenden Dateien im Verzeichnis /etc geändert und nach /nsconfig kopiert haben, um die Persistenz zu erhalten, gehen möglicherweise alle Aktualisierungen verloren, die während des Upgrades in das Verzeichnis /etc übertragen werden:

   - ttys
   - resolv.conf
   - sshd_config
   - host.conf
   - newsyslog.conf
   - host.conf
   - httpd.conf
   - rc.conf
   - syslog.conf
   - crontab
   - monitrc

   Um zu vermeiden, dass diese Updates verloren gehen, erstellen Sie ein `/var/nsconfig_backup` Verzeichnis und verschieben Sie die angepassten Dateien in dieses Verzeichnis. Das heißt, verschieben Sie alle Dateien, die Sie im Verzeichnis /etc geändert und nach /nsconfig kopiert haben, indem Sie den folgenden Befehl ausführen:

   ```
   cp /nsconfig/<filename> /var/nsconfig_backup
   ```

   Beispiel:

   ```
   cp /nsconfig/syslog.conf /var/nsconfig_backup
   ```

6. Erstellen Sie einen Speicherort für das Installationspaket. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

- `cd /var/nsinstall`
- `cd <releasenumber>`

  > **Hinweis:**
  >
  > Wenn das gewünschte Versionsnummernverzeichnis nicht vorhanden ist, erstellen Sie mit dem folgenden Befehl ein Verzeichnis:
  >
  > `mkdir <releasenumber>`
  >
  > **Beispiel:**
  >
  > `mkdir 13.0`

- `mkdir build_<targetbuildnumber>`
- `cd build_<targetbuildnumber>`

7. Kopieren Sie die bereits heruntergeladene Citrix ADC-Firmware in das Build-Verzeichnis, das Sie im obigen Schritt erstellt haben, indem Sie eine beliebige Dateiübertragungsmethode wie WinSCP verwenden. Weitere Informationen zum Herunterladen der Citrix ADC-Firmware finden Sie im Abschnitt Bevor Sie beginnen .
8. Extrahieren Sie den Inhalt des Installationspakets. Beispiel:

   ```
   tar -xvzf build-13.0-37.2_nc_64.tgz
   ```

9. Führen Sie das Installationsskript aus, um die neue Version der Systemsoftware zu installieren.

   ```
   ./installns
   ```

10. Starten Sie den Citrix ADC neu, wenn Sie dazu aufgefordert werden.
11. (Optional) Wenn Sie eine Kopie der Datei ns.conf im Abschnitt Bevor Sie beginnen erstellt haben, gehen Sie wie folgt vor:

    a) Vergleichen Sie die Dateien in `/var/nsconfig_backup/etc` und nehmen Sie entsprechende Änderungen in vor `/etc`.
    b) Um die Persistenz aufrechtzuerhalten, verschieben Sie die aktualisierten Dateien `/etc` nach `/nsconfig`.
    c) Starten Sie die Appliance neu, um die Änderungen wirksam zu werden.

Im Folgenden finden Sie ein Beispiel für das Citrix ADC Firmware-Upgrade.

```
1 login: nsroot
2
3 Password: nsroot
4
5 Last login: Mon Apr 17 15:05:05 2018 from 10.252.243.134
```



```
Done

> save config

> shell

Last login: Mon Apr 17 15:05:05 2018 from 10.252.243.134

root@NSnnn# cd /var/nsinstall

root@NSnnn# cd 13.0

root@NSnnn# mkdir build_43.1

root@NSnnn# cd build_43.1

root@NSnnn# ftp <FTP server IP address>

ftp> mget build-13.0-41.1_nc.tgz

ftp> bye

root@NSnnn# tar xzvf build-13.0-41.1_nc.tgz

root@NSnnn# ./installns

installns version (13.0-41.1) kernel (ns-13.0-41.1_nc.gz)

...

Copying ns-13.0-41.1_nc.gz to /flash/ns-13.0-41.1_nc.gz ...

...

Installation has completed.

Reboot NOW? [Y/N] Y
```

Upgrade einer eigenständigen Citrix ADC Appliance mit der NITRO-API

Informationen zur Verwendung der NITRO-API zum Upgrade oder Downgrade eines Citrix ADC finden Sie unter Automatisieren von Citrix ADC Upgrade und Downgrade mit einer einzigen API.

Überprüfen des Entitätsstatus auf der Citrix ADC Appliance nach dem Upgrade

Überprüfen Sie nach dem Upgrade der Citrix ADC Appliance den Status der folgenden Entitäten:

- Virtuelle Server befinden sich im Status UP
- Die Monitore sind im UP-Zustand
- GSLB-Sites synchronisieren sich ohne Probleme
- Alle Zertifikate sind auf dem Gerät vorhanden
- Alle Lizenzen sind auf der Appliance vorhanden

Überprüfen und installieren Sie das Citrix ADC 13.0 Softwareupdate

Aktualisieren Sie die Citrix ADC -Software, wenn ein Update verfügbar ist, um die Leistung zu verbessern. Ein Citrix ADC Update kann Funktionsverbesserungen, Leistungsbehebungen oder Verbesserungen enthalten. Vergewissern Sie sich, dass Sie die Versionshinweise lesen, um zu sehen, welche Korrekturen und Verbesserungen im Update verfügbar sind. Gehen Sie folgendermaßen vor, um ein Softwareupdate zu überprüfen und zu installieren.

1. Klicken Sie auf der Citrix ADC Homepage im Menü **nsroot** oben rechts auf **Update suchen**.
2. Überprüfen Sie auf der Seite **Neueste Systemsoftwareupdates verfügbar** das verfügbare Softwareupdate, das Sie installieren können.
3. Klicken Sie auf **Herunterladen**, um das Installationspaket von der Citrix Download-Website herunterzuladen .
4. Nachdem Sie das Softwarepaket heruntergeladen haben, installieren Sie das Update entweder über CLI- oder GUI-Prozedur.

> **Hinweis:**
>
> Auf den Link **Nach Update suchen** kann nur zugegriffen werden, wenn Sie sich über das HTTP-Protokoll und nicht über das HTTPS-Protokoll bei der GUI anmelden.

Zugehörige Ressourcen

Die folgenden Ressourcen enthalten verwandte Informationen zum Upgrade oder Herabstufung einer Citrix ADC Appliance:

- Video-Tutorial - So aktualisieren Sie Ihren Citrix ADC mit CLI

Downgrade einer eigenständigen Citrix ADC Appliance

October 5, 2021

Sie können ein Downgrade auf eine frühere Version auf einem eigenständigen Citrix ADC über die CLI oder GUI durchführen.

> **Hinweis:**
>
> Bei der Herabstufung kann es zu Konfigurationsverlusten kommen. Vergleichen Sie die Konfigurationen vor und nach dem Downgrade, und geben Sie dann alle fehlenden Einträge manuell erneut ein.

Downgrade einer Citrix ADC Appliance über die CLI

Befolgen Sie die unten angegebenen Schritte, um eine eigenständige Citrix ADC Appliance, auf der Release 13.0 ausgeführt wird, auf eine frühere Version herabzustufen.

In diesem Verfahren stellen Sie die Release-Version <releasenumber> dar, <release> auf die Sie heruntergestuft werden, und <targetbuildnumber> stellt die Build-Nummer dar, auf die Sie heruntergestuft werden.

1. Öffnen Sie eine SSH-Verbindung zum Citrix ADC mithilfe eines SSH-Clients, z. B. PuTTY.
2. Melden Sie sich mit den Administratoranmeldeinformationen am Citrix ADC an. Speichern Sie die laufende Konfiguration. Geben Sie an der Eingabeaufforderung Folgendes ein:

   save config
3. Erstellen Sie eine Kopie der Datei ns.conf. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

   a) `cd /nsconfig`
   b) `cp ns.conf ns.conf.NS<currentbuildnumber>`

   Sie sollten eine Kopie der Konfigurationsdatei auf einem anderen Computer sichern.
4. Kopieren Sie die <releasenumber> Konfigurationsdatei (Ns.conf.ns <releasenumber>) nach ns.conf. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
cp ns.conf.NS<releasenumber> ns.conf
<!--NeedCopy-->
```

> **Hinweis:**
>
> ns.conf.NS<releasenumber> ist die Backup-Konfigurationsdatei, die automatisch erstellt wird, wenn die Systemsoftware von der Release-Version <releasenumber> auf die aktuelle Release-Version aktualisiert wird.
>
> Beim Herabstufen kann es zu einem gewissen Konfigurationsverlust kommen. Nachdem

> die Appliance neu gestartet wurde, vergleichen Sie die in Schritt 3 gespeicherte Konfiguration mit der laufenden Konfiguration und nehmen alle Anpassungen für Features und Entitäten vor, die vor dem Downgrade konfiguriert wurden. Speichern Sie die laufende Konfiguration, nachdem Sie die Änderungen vorgenommen haben.
>
> **Wichtig:**
>
> Wenn Routing aktiviert ist, führen Sie Schritt 5 aus. Andernfalls fahren Sie mit Schritt 6 fort.

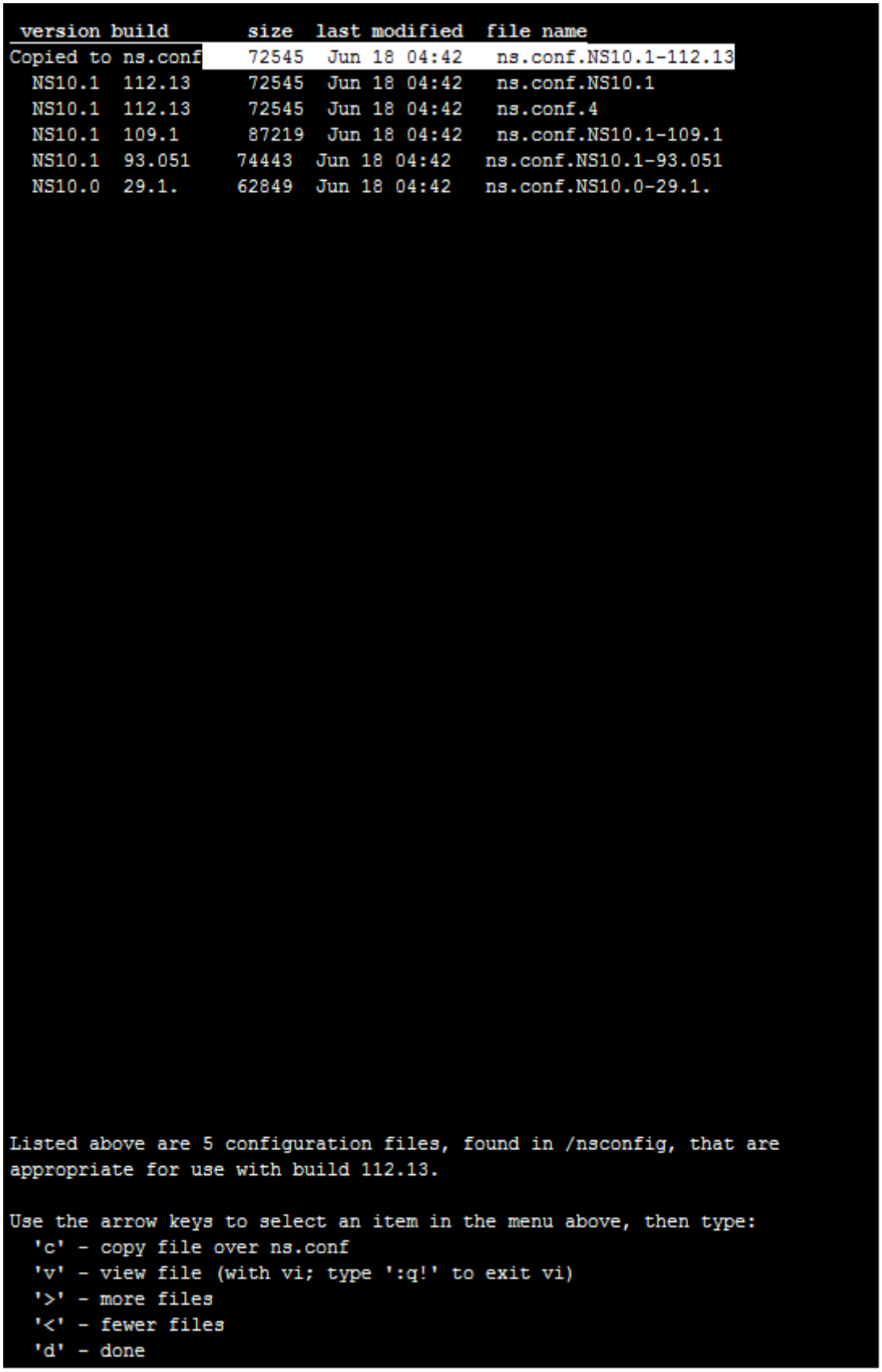
5. Wenn Routing aktiviert ist, enthält die Datei Zebos.conf die Konfiguration. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
cd /nsconfig
cp ZebOS.conf ZebOS.conf.NS
cp ZebOS.conf.NS<targetreleasenumber> ZebOS.conf
<!--NeedCopy-->
```

6. Wechseln Sie in ein Verzeichnis oder erstellen Sie es `/var/nsinstall/<releasenumber>nsinstall`, falls es nicht existiert.
7. Wechseln Sie in ein Verzeichnis oder erstellen Sie es `build_<targetbuildnumber>`, falls es nicht existiert.
8. Downloaden oder kopieren Sie das Installationspaket (`build-<release>-<targetbuildnumber>.tgz`) in dieses Verzeichnis und extrahieren Sie den Inhalt des Installationspakets.
9. Führen Sie das Skript `installns` aus, um die neue Version der Systemsoftware zu installieren. Das Script aktualisiert das `/etc` Verzeichnis.

   Wenn die Konfigurationsdatei für den Build, auf den Sie heruntergestuft werden, auf der Appliance vorhanden ist, werden Sie aufgefordert, diese Konfiguration zu laden:

   Abbildung 1. Downgrade Menü, falls Konfigurationsdatei vorhanden ist



Wenn der freie Speicherplatz auf dem Flash-Laufwerk nicht ausreicht, um den neuen Build zu installieren, bricht Citrix ADC die Installation ab. Bereinigen Sie das Flash-Laufwerk manuell und starten Sie die Installation neu.

Beispiel:

```
login: nsroot

Password: nsroot

Last login: Mon Apr 24 02:06:52 2017 from 10.102.29.9

Done

> save config

> shell

root@NSnnn# cp ns.conf.NS10.5 ns.conf

root@NSnnn# cd /var/nsinstall

root@NSnnn# mkdir 10.5nsinstall

root@NSnnn# cd 10.5nsinstall

root@NSnnn# mkdir build_57

root@NSnnn# cd build_57

root@NSnnn# ftp 10.102.1.1

ftp> mget build-10.5-57_nc.tgz

ftp> bye

root@NSnnn# tar -xzvf build-10.1-125_nc.tgz

root@NSnnn# ./installns

installns version (10.5-57) kernel (ns-10.5-57.gz)

...

```



```
...

...

Copying ns-10.5-57.gz to /flash/ns-10.5-57_nc.gz ...

Changing /flash/boot/loader.conf for ns-10.5-57 ...


Installation has completed.


Reboot NOW? [Y/N] Y
<!--NeedCopy-->
```

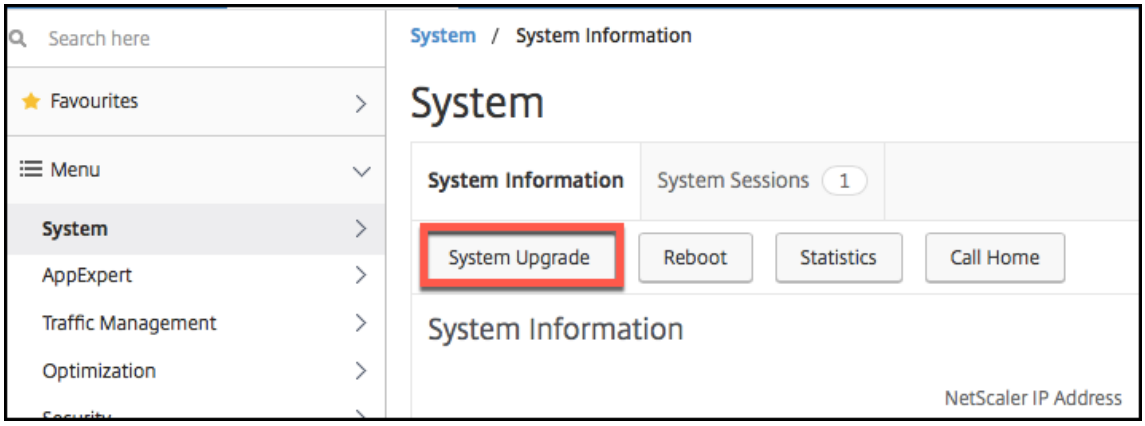
Downgraden einer Citrix ADC Appliance über die GUI

Sie können den Upgrade-Assistenten der GUI verwenden, um eine Citrix ADC Appliance, auf die Release 13.0 ausgeführt wird, auf eine frühere Version herabzustufen.

> **Hinweise:**
>
> Sie können eine Citrix ADC Appliance, auf der Release 13.0 ausgeführt wird, über die GUI nicht direkt auf Version 10.5 oder früher herunterstufen. Citrix empfiehlt, die CLI zum Herunterstufen zu verwenden.
>
> Weitere Informationen zum Citrix ADC Release-Lebenszyklus finden Sie auf der Produktmatrix-Website .
>
> Es ist eine bewährte Methode, auf jeweils eine Hauptversion herabzusetzen.
>
> Wenn sich die Citrix ADC Appliance beispielsweise auf Release 13.0 befindet und Sie auf Release 12.0 herunterstufen möchten, müssen Sie die Appliance zuerst auf Version 12.1 und dann auf Version 12.0 herunterstufen.

Befolgen Sie die unten angegebenen Schritte, um eine Citrix ADC Appliance, auf der Release 13.0 ausgeführt wird, über die GUI auf eine frühere Version herabzustufen.

1. Geben Sie in einem Webbrowser die IP-Adresse des Citrix ADC ein, z. B. `http://10.102.29.50` .
2. Geben Sie unter Benutzername und Kennwort die Administratoranmeldeinformationen ein und klicken Sie dann **auf Anmelden**.
3. Klicken Sie auf der grafischen Benutzeroberfläche auf **Systemupgrade**.



4. Wählen Sie im Menü **Datei** auswählen die entsprechende Option: **Lokal** oder **Appliance**. Wenn Sie die Appliance-Option verwenden möchten, muss die Firmware zuerst auf den Citrix ADC hochgeladen werden. Sie können eine beliebige Dateiübertragungsmethode wie WinSCP verwenden, um die Citrix ADC Firmware auf die Appliance hochzuladen.
5. Wählen Sie die richtige Datei aus und klicken Sie auf **Aktualisieren**.
6. Folgen Sie den Anweisungen, um die Software herabzusetzen.
7. Wenn Sie dazu aufgefordert werden, wählen Sie **Neustart** aus.

Schließen Sie nach dem Downgrade alle Browserinstanzen und leeren Sie den Cache Ihres Computers, bevor Sie auf die Appliance zugreifen.

Zugehörige Ressourcen

Die folgenden Ressourcen enthalten verwandte Informationen zum Upgrade oder Herabstufung einer Citrix ADC Appliance:

- Video-Tutorial - So aktualisieren Sie Ihren Citrix ADC mit CLI

Upgrade eines Hochverfügbarkeitspaars

October 5, 2021

Eine der Anforderungen von Citrix ADC Appliances in einem Hochverfügbarkeitssetup besteht darin, dieselbe Citrix ADC-Softwareversion auf beiden Appliances des Setups zu installieren. Wenn die Software auf einer Appliance aktualisiert wird, stellen Sie daher sicher, dass die Software auf beiden Appliances aktualisiert wird.

Sie können dasselbe Verfahren ausführen, um eine eigenständige Appliance oder jede Appliance in einem Hochverfügbarkeitspaar zu aktualisieren, obwohl zusätzliche Überlegungen für das Upgrade eines Hochverfügbarkeitspaars gelten.

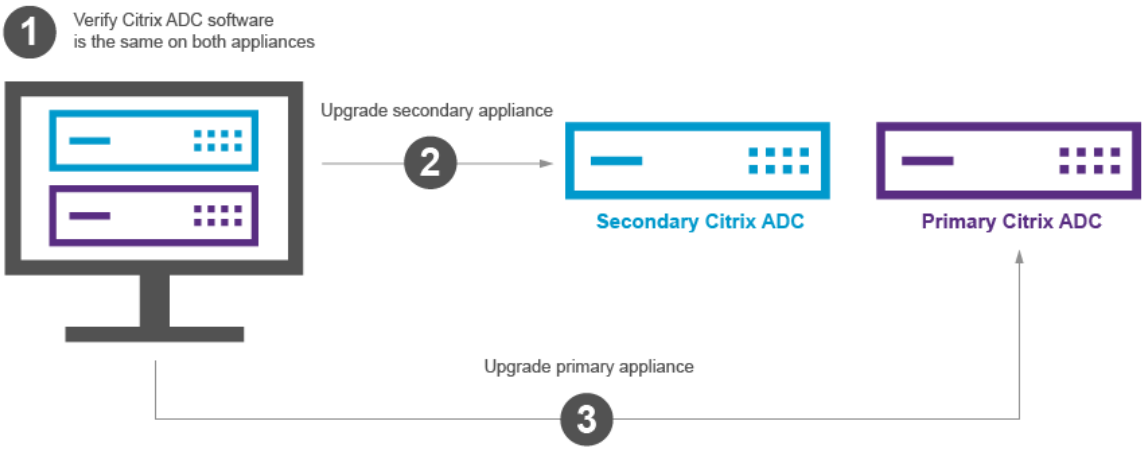
Bevor Sie ein Citrix ADC-Firmware-Upgrade für ein HA-Paar starten, lesen Sie die Voraussetzungen, die im Abschnitt Bevor Sie beginnen . Außerdem müssen Sie ein paar HA-spezifische Punkte berücksichtigen.

Punkte zu beachten

- Aktualisieren Sie zuerst den sekundären Knoten und dann den primären Knoten. Durch das Upgrade der Software auf der sekundären Appliance vor der primären Appliance wird sichergestellt, dass der Upgradevorgang problemlos abgeschlossen ist.
- Wenn auf beiden Knoten in einem Hochverfügbarkeitssetup verschiedene Citrix ADC -Softwareversionen ausgeführt werden, sind die folgenden Funktionen deaktiviert:
  - Synchronisierung der HA-Konfiguration
  - HA-Befehlspropagierung
  - HA-Synchronisierung von Status-Services-Informationen
  - Verbindungsspiegelung (Verbindungsfailover) von Sitzungen
  - HA-Synchronisierung von Informationen zu Persistenzsitzungen
- Die oben genannten Funktionalitäten sind deaktiviert, wenn beide Knoten in einem High Availability (HA) Setup verschiedene Builds derselben Version ausführen, aber beide Builds unterschiedliche interne HA-Versionen haben. Die oben genannten Funktionalitäten funktionieren gut, wenn beide Knoten in einem Hochverfügbarkeitssetup (HA) verschiedene Builds derselben Version ausführen, aber beide Builds die gleichen internen HA-Versionen haben.

  Überprüfen Sie im Abschnitt Hinweise zu den Versionshinweisen, ob sich die interne HA-Version im Citrix ADC Build geändert hat.
- Die Synchronisierung der Dateien im Modus Alle des Befehls HA-Dateien synchronisieren funktioniert erfolgreich, wenn auf den beiden Knoten in einer HA-Konfiguration unterschiedliche Citrix ADC -Softwareversionen ausgeführt werden oder auf den beiden Knoten unterschiedliche Builds derselben Version ausgeführt werden. Weitere Informationen finden Sie unter Synchronisieren von Konfigurationsdateien im Hochverfügbarkeits-Setup.

Abbildung. Upgrade eines Hochverfügbarkeitspaars



Sie können ein Upgrade mit der Citrix ADC CLI oder GUI durchführen.

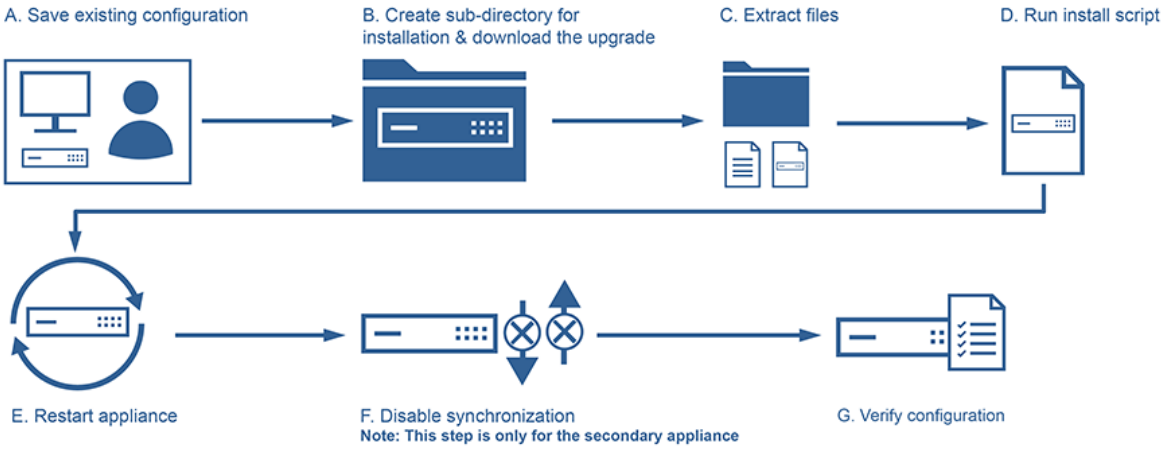
Upgrade eines Hochverfügbarkeitspaars mit der CLI

Der Upgrade-Prozess umfasst die folgenden Schritte:

1. Upgrade der Software auf der sekundären Appliance
2. Upgrade der Software auf der primären Appliance
3. Sekundäre Appliance synchronisieren

Upgrade der Software auf der sekundären Appliance

Die folgende Abbildung zeigt das Verfahren zum Aktualisieren von Software auf der sekundären Appliance:



1. Melden Sie sich mit einem SSH-Dienstprogramm wie PuTTY an der sekundären NetScaler-Appliance an, und geben Sie die NetScaler-IP (NSIP) an. Verwenden Sie die nsroot-Anmeldeinformationen, um sich bei der Appliance anzumelden.

2. Geben Sie in der Befehlszeilenschnittstelle der Appliance den folgenden Befehl ein, um die vorhandene Konfiguration zu speichern: save config
3. Wechseln Sie zur Shell-Eingabeaufforderung.

```
login as: username
Using keyboard-interactive authentication.
Password:
Last login: Wed Jun 24 14:59:16 2015 from 10.252.252.65
Done
> shell
Copyright (c) 1992-20

<!--NeedCopy-->
```

4. Führen Sie den folgenden Befehl aus, um in das Standardinstallationsverzeichnis zu wechseln: # cd /var/nsinstall
5. Führen Sie den folgenden Befehl aus, um ein temporäres Unterverzeichnis des Verzeichnisses nsinstall zu erstellen: **# mkdir x_xnsinstall**

   > Hinweis: Der Text x_x wird verwendet, um die NetScaler Version für zukünftige Konfigurationen zu benennen. Zum Beispiel, das Verzeichnis für die Installationsdateien von NetScaler 9.3 uns 9_3nsinstall genannt. Verwenden Sie keinen Punkt (.) im Ordnernamen. Dies kann zu fehlgeschlagenen Upgrades führen.

6. Wechseln Sie in das Verzeichnis **x_xnsinstall** .
7. Laden Sie das erforderliche Installationspaket und das Dokumentationspaket, z. B. ns-x.0-xx.x-doc.tgz, in das in Schritt 4 erstellte temporäre Verzeichnis herunter.

   > **Hinweis:**
   >
   > Einige Builds haben kein Dokumentationspaket, da es nicht installiert werden muss.
   >
   > Klicken Sie auf der GUI auf die Registerkarte **Dokumentation**, um auf die Dokumentation zuzugreifen.

8. Bevor Sie das Installationsskript ausführen, müssen die Dateien extrahiert und auf der Appliance abgelegt werden. Verwenden Sie den folgenden Befehl, um das von der Citrix Website heruntergeladene Paket zu entpacken: **tar -zxvf ns-x.0-xx.x-doc.tgz**. Im Folgenden finden Sie eine kurze Erläuterung der verwendeten Parameter.

   x: Dateien extrahieren

   v: Drucken Sie die Dateinamen, wie sie einzeln extrahiert werden

z: Die Datei wurde mit gzip komprimiert

f: Verwenden Sie das folgende tar-Archiv für die Operation

9. Führen Sie den folgenden Befehl aus, um die heruntergeladene Software zu installieren: #. /installns

   > Hinweis: Wenn die Appliance nicht über genügend Speicherplatz verfügt, um die neuen Kerneldateien zu installieren, führt der Installationsvorgang eine automatische Bereinigung des Flash-Laufwerks durch.

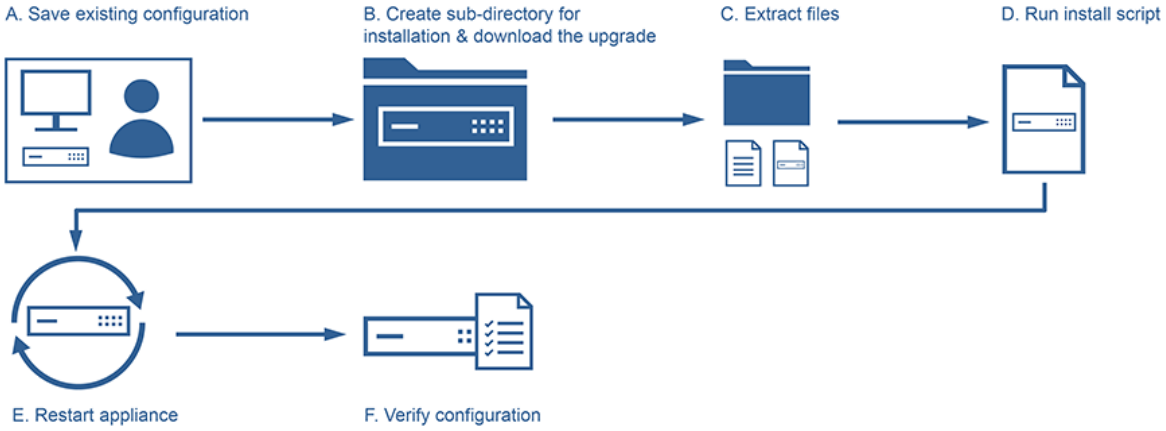
10. Nach Abschluss der Installation wird der Vorgang aufgefordert, die Appliance neu zu starten. Drücken Sie y, um die Appliance neu zu starten.
11. Melden Sie sich mit den nsroot-Anmeldeinformationen an der Befehlszeilenschnittstelle der Appliance an.
12. Führen Sie den folgenden Befehl aus, um den Status der NetScaler Appliance anzuzeigen: **show ha node** Die Ausgabe des vorherigen Befehls sollte angeben, dass es sich bei der Appliance um einen sekundären Knoten handelt und die Synchronisierung deaktiviert ist.
13. Führen Sie den folgenden Befehl aus, um ein Failover und eine Übernahme als primäre Appliance auszuführen: **Failover erzwingen**

Hier ist eine Beispielkonfiguration im neuen primären Knoten.

```
login: nsroot
Password: nsroot
Last login: Monday Apr  17 08:37:26 2017 from 10.102.29.9
Done
show ha node
        2 nodes:
1)      Node ID:      0
        IP:        10.0.4.2
        Node State: UP
        Master State: Primary
        ...
        Sync State: AUTO DISABLED
        Propagation: AUTO DISABLED
        ...
Done
<!--NeedCopy-->
```


Upgrade der Software auf der primären Appliance

Die folgende Abbildung zeigt das Verfahren zum Aktualisieren von Software auf der primären Appliance:



> Hinweis: Nach Abschluss des Verfahrens Software auf der sekundären Appliance aktualisieren ist die ursprüngliche primäre Appliance nun eine sekundäre Appliance.

1. Melden Sie sich mit einem SSH-Dienstprogramm wie PuTTY an der sekundären NetScaler-Appliance an. Verwenden Sie die nsroot-Anmeldeinformationen, um sich bei der Appliance anzumelden. Führen Sie die gleichen Schritte aus, wie im obigen Abschnitt erwähnt, um den Installationsvorgang abzuschließen. Wir müssen die gleichen Schritte ausführen, wie in Schritt 2 bis Schritt 9 im vorherigen Abschnitt erwähnt (Upgrade-Software der sekundären Appliance)
2. Nach Abschluss der Installation wird der Vorgang aufgefordert, die Appliance neu zu starten. Drücken Sie y, um die Appliance neu zu starten.
3. Melden Sie sich mit den nsroot-Anmeldeinformationen an der Befehlszeilenschnittstelle der Appliance an.
4. Führen Sie den folgenden Befehl aus, um den Status der NetScaler Appliance **anzuzeigen: show ha node**. Die Ausgabe des vorhergehenden Befehls sollte darauf hinweisen, dass die Appliance ein sekundärer Knoten ist und der Status des Knotenstatus als UP markiert ist.
5. Führen Sie den folgenden Befehl aus, um ein erzwungenes Failover durchzuführen, um sicherzustellen, dass es sich bei der Appliance um eine primäre Appliance handelt: **Failover erzwingen**
6. Stellen Sie sicher, dass die Appliance eine primäre Appliance ist.

   Hier ist ein Beispiel für die Konfiguration des neuen primären Knotens und des neuen sekundären Knotens.


```
show ha node
    Node ID:      0
    IP:   10.0.4.11
    Node State: UP
    Master State: Primary
    ...
    ...
    INC State: DISABLED
    Sync State: ENABLED
    Propagation: ENABLED
    Enabled Interfaces : 1/1
    Disabled Interfaces : None
    HA MON ON Interfaces : 1/1
    ...
    ...
    Local node information
    Critical Interfaces: 1/1
Done

Show ha node
    Node ID:      0
    IP:   10.0.4.2
    Node State: UP
    Master State: Secondary
    ..
    ..
    INC State: DISABLED
    Sync State: SUCCESS
    Propagation: ENABLED
    Enabled Interfaces : 1/1
    Disabled Interfaces : None
    HA MON ON Interfaces : 1/1
    . .
    . .
    Local node information:
    Critical Interfaces: 1/1
Done
<!--NeedCopy-->
```

Aktualisieren eines Hochverfügbarkeitspaars über die GUI

Führen Sie die folgenden Schritte aus, um ein Citrix ADC Paar in einem Hochverfügbarkeitssetup über die ADC-GUI zu aktualisieren: Betrachten Sie ein Beispiel für ein Hochverfügbarkeitssetup von Citrix

ADC Appliances CITRIX-ADC-A (primär) und CITRIX-ADC-B (sekundär).

1. **Aktualisieren Sie den sekundären Knoten**. Melden Sie sich mit Administratoranmeldeinformationen bei der GUI des sekundären Knotens an und führen Sie das Upgrade wie unter Upgrade einer eigenständigen Citrix ADC Appliance über die grafische Benutzeroberfläche beschrieben durch.

2. **Failover erzwingen**. Führen Sie ein Force-Failover auf dem sekundären Knoten über die grafische Benutzeroberfläche aus, wie unter Erzwingen eines Knotens zum Ausfall erzwingenbeschrieben.

   Nach dem Failover-Vorgang übernimmt der sekundäre Knoten den primären Knoten und der primäre Knoten wird zum neuen sekundären Knoten. Nach dem Failover-Vorgang in der Beispiel-HA-Setup:

   - CITRIX-ADC-B wird zum neuen primären
   - CITRIX-ADC-A wird die neue sekundäre

3. **Aktualisieren Sie den ursprünglichen primären Knoten (neuer sekundärer Knoten)**. Melden Sie sich bei der neuen GUI des sekundären Knotens (CITRIX-ADC-A) an und führen Sie das Upgrade wie unter Upgrade einer eigenständigen Citrix ADC Appliance über die grafische Benutzeroberfläche beschrieben durch.

4. **Failover erzwingen**. Führen Sie ein Force-Failover auf dem neuen sekundären Knoten (CITRIX-ADC-A) über die grafische Benutzeroberfläche durch, wie unter Einen Knoten zum Failover zwingenbeschrieben beschrieben.

   Nach diesem zweiten Failover-Vorgang kehrt der Status beider Knoten in denselben Zustand zurück wie vor dem Starten des HA-Upgradevorgangs. Nach dem Failover-Vorgang in der Beispiel-HA-Setup:

   - CITRIX-ADC-A wird primär
   - CITRIX-ADC-B wird sekundär

5. **Überprüfen Sie den Upgradevorgang**. Melden Sie sich an der GUI beider Knoten an. Navigieren Sie zu **System > Hohe Verfügbarkeit**, überprüfen Sie auf der Detailseite den HA-Status beider Knoten. Überprüfen Sie außerdem die aktualisierten Versionsdetails, die im oberen Bereich der GUI angezeigt werden.

Zugehörige Ressourcen

Die folgenden Ressourcen enthalten verwandte Informationen zum Upgrade eines Citrix ADC Hochverfügbarkeits-Setups:

- Video-Tutorial - So aktualisieren Sie Ihr Citrix ADC HA-Paar mit der GUI

Support für Softwareupgrades für hohe Verfügbarkeit für das Ausführen eines Upgrades ohne Ausfallzeiten

October 5, 2021

Während eines regulären Upgrades in einem Hochverfügbarkeitssetup führen beide Knoten irgendwann verschiedene Software-Builds aus. Diese beiden Builds können dieselben oder unterschiedliche interne Hochverfügbarkeitsversionsnummern haben.

Wenn beide Builds unterschiedliche Versionsnummern für hohe Verfügbarkeit aufweisen, wird das Verbindungs-Failover (auch wenn es aktiviert ist) für vorhandene Datenverbindungen nicht unterstützt. Mit anderen Worten, alle vorhandenen Datenverbindungen gehen verloren, was zu Ausfallzeiten führt.

Um dieses Problem zu beheben, kann in Service Software Upgrade (ISSU) für Hochverfügbarkeitssetups verwendet werden. ISSU führt eine Migrationsfunktionalität ein, die den Schritt Force-Failover im Upgrade-Prozess ersetzt. Die Migrationsfunktionalität übernimmt die Berücksichtigung der vorhandenen Verbindungen und umfasst den erzwungenen Failover-Vorgang.

Nach dem Migrationsvorgang empfängt der neue primäre Knoten immer Datenverkehr (Anforderung und Antwort) im Zusammenhang mit den vorhandenen Verbindungen, steuert sie aber zum alten primären Knoten. Der alte primäre Knoten verarbeitet den Datenverkehr und sendet ihn dann direkt an das Ziel.

Funktionsweise der erweiterten ISSU

Der reguläre Upgrade-Prozess in einem Hochverfügbarkeitssetup besteht aus folgenden aufeinanderfolgenden Schritten:

1. **Aktualisieren Sie den sekundären Knoten**. Dieser Schritt umfasst das Software-Upgrade des sekundären Knotens und den Neustart des Knotens.
2. **Failover erzwingen**. Wenn Sie das Force-Failover ausführen, werden der aktualisierte sekundäre Knoten auf den primären Knoten und der primäre Knoten auf den sekundären Knoten.
3. **Aktualisieren Sie den neuen sekundären Knoten**. Dieser Schritt umfasst das Software-Upgrade des neuen sekundären Knotens und den Neustart des Knotens.

Während des Zeitrahmens zwischen Schritt 1 und Schritt 3 führen beide Knoten verschiedene Software-Builds aus. Diese beiden Builds können dieselben oder unterschiedliche interne Hochverfügbarkeitsversionen haben.

Wenn beide Builds unterschiedliche Versionsnummern für hohe Verfügbarkeit aufweisen, wird das Verbindungs-Failover (auch wenn es aktiviert ist) für vorhandene Datenverbindungen nicht

unterstützt. Mit anderen Worten, alle vorhandenen Datenverbindungen gehen verloren, was zu Ausfallzeiten führt.

Der ISSU-Upgrade-Prozess in einem Hochverfügbarkeitssetup besteht aus den folgenden Schritten:

1. **Aktualisieren Sie den sekundären Knoten**. Dieser Schritt umfasst das Software-Upgrade des sekundären Knotens und den Neustart des Knotens.
2. **ISSU-Migrationsvorgang**. Der Schritt umfasst den Force-Failover-Vorgang und kümmert sich um die vorhandenen Verbindungen. Nachdem Sie den Migrationsvorgang durchgeführt haben, empfängt der neue primäre Knoten immer Datenverkehr (Anforderung und Antwort) im Zusammenhang mit den vorhandenen Verbindungen, leitet sie aber über das konfigurierte SYNC-VLAN im GRE-Tunnel zum alten primären Knoten. Der alte primäre Knoten verarbeitet den Datenverkehr und sendet ihn dann direkt an das Ziel. Der ISSU-Migrationsvorgang wird abgeschlossen, wenn alle vorhandenen Verbindungen geschlossen sind.
3. **Aktualisieren Sie den neuen sekundären Knoten**. Dieser Schritt umfasst das Software-Upgrade des neuen sekundären Knotens und den Neustart des Knotens.

Voraussetzungen

Bevor Sie mit der Ausführung des ISSU-Prozesses in einer Hochverfügbarkeitseinrichtung beginnen, gehen Sie durch die folgenden Voraussetzungen und Einschränkungen:

- Stellen Sie sicher, dass das SYNC-VLAN auf beiden Knoten des Hochverfügbarkeitssetups konfiguriert ist. Weitere Informationen finden Sie unter Beschränken des Synchronisationsdatenverkehrs für hohe Verfügbarkeit auf ein VLAN.
- ISSU wird in der Microsoft Azure-Cloud nicht unterstützt, da Microsoft Azure GRE-Tunneling nicht unterstützt.
- Hochverfügbarkeitspropagierung und Synchronisierung der Konfiguration funktionieren während der ISSU nicht.
- ISSU wird für IPv6-Hochverfügbarkeitssetup nicht unterstützt.
- ISSU wird für folgende Sitzungen nicht unterstützt:
  - Jumbo-Rahmen
  - IPv6-Sitzungen
  - Großes NAT (LSN)

Konfigurationsschritte

ISSU enthält eine Migrationsfunktion, die den Force-Failover-Vorgang im regulären Upgrade-Prozess eines Hochverfügbarkeitssetups ersetzt. Die Migrationsfunktionalität übernimmt die Berücksichtigung der vorhandenen Verbindungen und umfasst den erzwungenen Failover-Vorgang.

Während des ISSU-Prozesses eines Hochverfügbarkeitssetups führen Sie den Migrationsvorgang unmittelbar nach dem Upgrade des sekundären Knotens aus. Sie können den Migrationsvorgang von einem der beiden Knoten aus ausführen.

CLI-Prozedur

So führen Sie den Hochverfügbarkeitsmigrationsvorgang mit der CLI aus:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
start ns migration
<!--NeedCopy-->
```

GUI-Prozedur

So führen Sie den Hochverfügbarkeitsmigrationsvorgang mit der GUI aus:

Navigieren Sie zu **System**, klicken Sie auf Registerkarte **Systeminformationen**, klicken Sie auf **Registerkarte Migration**, und klicken Sie dann auf **Migration starten**.

ISSU-Statistiken

Sie können die ISSU-Statistiken zur Überwachung des aktuellen ISSU-Prozesses in einem Hochverfügbarkeitssetup anzeigen. Die ISSU-Statistiken zeigen die folgenden Informationen an:

- Aktueller Stand des ISSU-Migrationsoperationen
- Startzeit der ISSU-Migrationsoperation
- Endzeit der ISSU-Migrationsoperation
- Startzeit des Rollback-Vorgangs der ISSU

Sie können die ISSU-Statistiken für einen der HA-Knoten mit CLI oder GUI anzeigen.

CLI-Prozedur

So zeigen Sie die ISSU-Statistiken über die CLI an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show ns migration
<!--NeedCopy-->
```


GUI-Prozedur

So zeigen Sie die ISSU-Statistiken mit der GUI an:

Navigieren Sie zu **System**, klicken Sie auf die Registerkarte **Systeminformationen**, klicken Sie auf die **Registerkarte Migration**und dann auf **Migration anzeigen**.

Rollback des ISSU-Prozesses

Hochverfügbarkeitssetups (HA) unterstützen jetzt das Rollback des In-Service Software Upgrade-Prozesses (ISSU). Das ISSU-Rollback-Feature ist hilfreich, wenn Sie feststellen, dass das HA-Setup während des ISSU-Migrationsvorgangs nicht stabil ist oder nicht wie erwartet auf einem optimalen Niveau funktioniert.

Das ISSU-Rollback ist anwendbar, wenn der ISSU-Migrationsvorgang läuft. Das ISSU-Rollback funktioniert nicht, wenn ISSU-Migrationsvorgang bereits abgeschlossen ist. Mit anderen Worten, Sie müssen den ISSU-Rollback-Vorgang ausführen, wenn ISSU-Migrationsvorgang ausgeführt wird.

Das ISSU-Rollback funktioniert unterschiedlich basierend auf dem Status des ISSU-Migrationsvorgangs, wenn der ISSU-Rollback-Vorgang ausgelöst wird:

- **Während des ISSU-Migrationsvorgangs ist noch kein erzwungenes Failover aufgetreten**. Das ISSU-Rollback stoppt den ISSU-Migrationsvorgang und entfernt alle internen Daten im Zusammenhang mit der ISSU-Migration, die in beiden Knoten gespeichert sind. Der aktuelle primäre Knoten bleibt als primärer Knoten und verarbeitet weiterhin den Datenverkehr im Zusammenhang mit bestehenden und neuen Verbindungen.
- **Während des ISSU-Migrationsvorgangs wurde ein Failover erzwungen**. Wenn das Hochverfügbarkeits-Failover während des ISSU-Migrationsvorgangs stattgefunden hat, verarbeitet der neue primäre Knoten (z. B. N1) Datenverkehr im Zusammenhang mit den neuen Verbindungen. Der alte primäre Knoten (neuer sekundärer Knoten, sagt er ist N2) verarbeitet Datenverkehr im Zusammenhang mit den alten Verbindungen (bestehende Verbindungen vor dem ISSU-Migrationsvorgang).

  Das ISSU-Rollback stoppt den ISSU-Migrationsvorgang und löst ein erzwungenes Failover aus. Der neue primäre Knoten (N2) beginnt nun mit der Verarbeitung des Datenverkehrs im Zusammenhang mit den neuen Verbindungen. Der neue primäre Knoten (N2) verarbeitet weiterhin Datenverkehr im Zusammenhang mit alten Verbindungen (bestehende Verbindungen, die vor dem ISSU-Migrationsvorgang eingerichtet wurden). Mit anderen Worten, die bestehenden Verbindungen, die vor der ISSU-Migration eingerichtet wurden, gehen nicht verloren.

  Der neue sekundäre Knoten (N1) entfernt alle vorhandenen Verbindungen (neue Verbindungen, die während des ISSU-Migrationsvorgangs erstellt wurden) und verarbeitet keinen Datenverkehr. Mit anderen Worten, alle bestehenden Verbindungen, die nach dem Erzwungen-Failover des ISSU-Migrationsvorgangs hergestellt wurden, gehen für immer verloren.

Konfigurationsschritte

Sie können Citrix ADC CLI oder GUI verwenden, um den ISSU-Rollbackvorgang auszuführen.

CLI-Prozedur

So führen Sie den ISSU-Rollbackvorgang mit der CLI aus:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stop ns migration
<!--NeedCopy-->
```

GUI-Prozedur

So führen Sie den ISSU-Rollback-Vorgang mit der GUI durch:

Navigieren Sie zu **System**, klicken Sie auf Registerkarte **Systeminformationen**, klicken Sie auf **Registerkarte Migration**, und klicken Sie dann auf **Migration beenden**.

SNMP-Traps für In-Service Software-Upgrade-Prozess

Der In-Service Software Upgrade (ISSU) -Prozess für ein Hochverfügbarkeitssetup unterstützt die folgenden SNMP-Trap-Nachrichten zu Beginn und Ende des ISSU-Migrationsvorgangs.

SNMP-Trap	Beschreibung
migrationStarted	Dieser SNMP-Trap wird generiert und an die konfigurierten SNMP-Trap-Listener gesendet, wenn der ISSU-Migrationsvorgang gestartet wird.
migrationComplete	Dieser SNMP-Trap wird generiert und an die konfigurierten SNMP-Trap-Listener gesendet, wenn der ISSU-Migrationsvorgang abgeschlossen ist.

Der primäre Knoten (vor Beginn des ISSU-Prozesses) generiert immer diese beiden SNMP-Traps und sendet sie an die konfigurierten SNMP-Trap-Listener.

Es sind keine SNMP-Alarme mit den ISSU-SNMP-Traps verknüpft. Mit anderen Worten, diese Fallen werden unabhängig vom SNMP-Alarm generiert. Sie müssen nur die Trap SNMP Listener konfiguri-

eren.

Weitere Informationen zum Konfigurieren von SNMP-Trap-Listener finden Sie unter SNMP-Traps auf Citrix ADC.

Downgrade eines Hochverfügbarkeitspaars

October 5, 2021

Sie können auf eine beliebige Version eines Hochverfügbarkeitspaars herabstufen, indem Sie die Befehlszeilenschnittstelle verwenden. Die GUI unterstützt den Downgrade-Prozess nicht.

Um die Systemsoftware auf einem Citrix ADC Paar in einem Hochverfügbarkeitspaar herunterzustufen, müssen Sie die Software zuerst auf dem sekundären Knoten und dann auf dem primären Knoten herunterstufen. Anweisungen zum separaten Downgrade jedes Knotens finden Sie unter Downgrade einer eigenständigen Citrix ADC Appliance.

> **Wichtig**
>
> Bei der Herabstufung kann es zu Konfigurationsverlusten kommen. Sie sollten die Konfigurationen vor und nach dem Downgrade vergleichen und dann fehlende Einträge manuell erneut eingeben.

Behebung von Problemen im Zusammenhang mit den Installations-, Upgrade- und Downgrade-Prozessen

February 24, 2022

Wenn die Appliance nach Abschluss der Installation, des Upgrades oder des Downgrade-Prozesses nicht wie erwartet funktioniert, müssen Sie zunächst nach den häufigsten Ursachen des Problems suchen.

Ressourcen für die Fehlerbehebung

Verwenden Sie die folgenden Ressourcen, um ein Problem im Zusammenhang mit der Installation, Aktualisierung oder Herabstufung eines Citrix ADC zu beheben:

- Die Konfigurationsdateien der Appliance. Im Falle eines Hochverfügbarkeitspaars die Konfigurationsdateien beider Appliances.
- Die folgenden Dateien der Appliance(s):

  - Die relevanten newnslog-Dateien.
  - Die Datei ns.log.
  - Die Meldungsdatei.
- Ein Netzwerktopologie-Diagramm.

Probleme und Lösungen

Im Folgenden finden Sie die häufigsten Installations-, Upgrade- und Downgrade-Probleme sowie Tipps zur Lösung dieser Probleme:

1. **Problem**

   Das Upgrade einer Citrix ADC MPX Appliance schlägt aufgrund von Hardware- und Softwareintolerierbarkeit fehl.

   Lösung

   Sehen Sie sich die Citrix ADC MPX Hardware-Software-Kompatibilitätsmatrix an und prüfen Sie, ob das Software-Release auf der Citrix ADC MPX-Hardware unterstützt wird.

2. **Problem**

   Das Upgrade einer Citrix ADC VPX Appliance schlägt aufgrund von Citrix ADC VPX Appliance und Hypervisor-Inkompatibilität fehl.

   Lösung

   Sehen Sie sich die Citrix ADC VPX Appliance und die Hypervisor-Kompatibilitätsmatrix an, und prüfen Sie, ob das Citrix ADC VPX Appliance-Modell auf dem Hypervisor unterstützt wird.

3. **Problem**

   Das Upgrade einer Citrix ADC Appliance schlägt aufgrund von Hardwarefehlern fehl.

   Lösung

   Überprüfen Sie die Integrität der Citrix ADC Appliance. Wenn Sie über eine Citrix ADC Hardware-Appliance verfügen, empfiehlt Citrix, eine Festplattenprüfung durchzuführen und die Integrität der Citrix ADC -Festplatte zu überprüfen. `fsck`

   Weitere Informationen finden Sie unter Überprüfen der Dateisystemintegrität einer Citrix ADC Appliance.

4. **Problem**

   Upgrade einer Citrix ADC Appliance über die GUI Stalls.

   Lösung

   Aktualisieren Sie den Browser, um zu prüfen, ob das Upgrade fortschreitet oder nicht.

5. **Problem**

   Das Upgrade einer Citrix ADC Appliance schlägt aufgrund von geringem Platzangebot im /var-Verzeichnis fehl

   Lösung

   Geben Sie Speicherplatz im /var-Verzeichnis frei. Weitere Informationen finden Sie unter So geben Sie Speicherplatz im /var-Verzeichnis frei.

6. **Problem**

   Auf das Citrix ADC ist nach dem Software-Downgrade nicht zugegriffen

   Ursache

   Wenn während des Software-Downgrade-Prozesses die Konfigurationsdatei des vorhandenen Release und Builds nicht mit der Konfigurationsdatei der früheren Version und des Builds übereinstimmt, kann die Appliance die Konfiguration nicht laden, und die Standard-IP-Adresse wird der Appliance zugewiesen.

   Lösung

   - Stellen Sie sicher, dass auf die Appliance über die Konsole zugegriffen werden kann.
   - Überprüfen Sie die NSIP-Adresse und die Routen auf der Appliance.
     - Wenn sich die IP-Adresse auf die Standard-IP-Adresse 192.168.100.1 geändert hat, ändern Sie die IP-Adresse nach Bedarf.
     - Stellen Sie sicher, dass auf die Appliance zugegriffen werden kann.

7. **Problem**

   Wenn ich während eines Upgrades den Befehl zum Synchronisieren ausführe, wird die folgende Meldung angezeigt:

   Der Befehl ist auf dem sekundären Knoten fehlgeschlagen, aber auf dem primären Knoten erfolgreich.

   Lösung

   Führen Sie keine abhängigen Befehle aus (set /unset /bind /unbind), wenn die High Availability (HA) synchronisiert wird.

8. **Problem**

   Während eines Upgradevorgangs wird der Datenverkehr nicht durch den neuen primären Knoten geleitet, wenn Sie den Befehl erzwingen Failover ausführen.

   Lösung

   - Überprüfen Sie auf Probleme mit der Netzwerktopologie und den Switch-Konfigurationen.

- Führen Sie den Befehl set L2Param -garpreply ENABLED aus, um die GARP-Antwort zu aktivieren.
- Versuchen Sie, virtuellen MAC zu verwenden, wenn nicht bereits verwendet.
- Führen Sie den Befehl sendarp —a vom primären Knoten aus.

9. **Problem**

   Nach dem Upgrade oder Downgrade einer Citrix ADC Appliance schlägt die Verbindung mit der Appliance über SSH fehl.

   Lösung

   Führen Sie die folgenden Vorgänge in der Citrix ADC Appliance durch:

   - Entfernen Sie alte oder unsichere Hostschlüssel unter `/nsconfig/ssh/ssh_host_*`.
   - Überprüfen Sie die benutzerdefinierte SSHD-Konfiguration unter `/nsconfig/sshd_config` und prüfen Sie, ob sie noch relevant und kompatibel ist. Benennen Sie die benutzerdefinierte SSHD-Konfiguration um oder entfernen Sie sie entsprechend.
   - Kalter Neustart der Citrix ADC Appliance

10. **Problem**

    In einem HA-Paar werden die Geräte nach dem Ausführen des Befehls Force HA-Failover weiterhin neu gestartet. Das sekundäre Gerät wird nach einem Upgrade nicht angezeigt.

    Lösung

    Überprüfen Sie, ob das Verzeichnis /var voll ist. Wenn ja, entfernen Sie die alten Installationsdateien. Führen Sie den Befehl df —h aus, um den verfügbaren Speicherplatz anzuzeigen.

11. **Problem**

    Nach dem Upgrade eines HA-Paares wird einer der Knoten als Status UNKNOWN aufgeführt.

    Lösung

    - Überprüfen Sie, ob beide Knoten denselben Build ausführen. Wenn die Builds nicht identisch sind und HA-Knoten unterschiedliche Versionen haben, werden einige der Felder als UNKNOWN angezeigt, wenn Sie den Befehl show ha node ausführen.
    - Überprüfen Sie, ob die sekundäre Appliance erreichbar ist.

12. **Problem**

    Nach dem Upgrade des Citrix ADC zeigt die Schnittstelle, dass die meisten der virtuellen Server und Dienste für den Lastausgleich DOWN sind.

    Lösung

    Stellen Sie sicher, dass die SNIP-Adresse auf der sekundären Appliance aktiv ist. Geben Sie außerdem den Befehl show service ein, um zu sehen, ob der Dienst ausgeführt wird.

13. **Problem**

    Nach dem Ausführen eines Upgrades befinden sich alle virtuellen Server auf der sekundären Appliance.

    Lösung

    Aktivieren Sie den HA-Status und die HA-Synchronisierung, indem Sie die folgenden Befehle ausführen:

    - set node hastate enable
    - set node hasync enable

    Das Deaktivieren von HA wird nicht empfohlen.

14. **Problem**

    Nach einem Downgrade startet Citrix ADC nicht ordnungsgemäß.

    Lösung

    Überprüfen Sie, ob die richtige Lizenz installiert wurde.

15. **Problem**

    Bei einem HA-Paar werden einige Funktionen nicht synchronisiert, nachdem ein Upgrade durchgeführt wurde.

    Lösung

    Führen Sie den Befehl sync ha file misc aus, um die Konfigurationsdateien vom primären Knoten zum sekundären Knoten zu synchronisieren.

16. **Problem**

    Beim Neustart wird die folgende Fehlermeldung angezeigt:

    Ein oder mehrere Befehle in ns.conf sind fehlgeschlagen. Was soll ich tun?

    Lösung

    Stellen Sie sicher, dass kein Befehl in der Datei ns.conf die 255 Byte Grenze überschreitet. In Befehlen, die Richtlinien erstellen, die für die 255-Byte-Grenze zu lang sind, können Sie Mustersätze verwenden, um die Richtlinien zu verkürzen.

    Beispiel:

```
1 add cs policy p11 -rule 'HTTP.REQ.URL.ENDSWITH_ANY("
     ctx_file_extensions")'
2 Done
3 <!--NeedCopy-->
```


ctx_file_extensions ist ein Standard-Patset, das eine große Anzahl von Erweiterungen abdeckt. Zusätzlich zu den Standardmustersätzen können Sie benutzerdefinierte Mustersätze erstellen. Fügen Sie ein Patset hinzu, indem Sie den folgenden Befehl ausführen:

```
1 add patset <name>
2 <!--NeedCopy-->
```

Hinweis: Patsets werden nur ab Version 9.3 unterstützt.

17. **Problem**

    Beim Upgrade einer Citrix ADC VPX Appliance wird mir gesagt, dass ich Speicherplatz in /var freigeben soll. Welche Dateien kann ich entfernen?

    Lösung

    Entfernen Sie die alten Installationsdateien aus dem Verzeichnis /var/tmp/. Entfernen Sie auch unerwünschte Dateien aus /flash.

18. **Problem**

    Es besteht keine Verbindung zur grafischen Benutzeroberfläche (GUI), wenn Sie den Befehl HA-Failover erzwingen auf der sekundären Appliance ausführen.

    Lösung

    Melden Sie sich über die Befehlszeilenschnittstelle an der sekundären Appliance an und aktivieren Sie den Zugriff auf GUI, indem Sie den <IP> Befehl set ns ip -gui enabled ausführen.

19. **Problem**

    Nach dem Ausführen eines Upgrades und wenn ich auf einen Link auf der GUI klicke, der ein Java-Applet (Upgrade-Assistent oder Lizenz-Assistent) laden muss, wird die folgende Fehlermeldung angezeigt: **GUI-Version stimmt nicht mit der Kernel-Version überein. Bitte schließen Sie diese Instanz, löschen Sie den Java-Plug-in-Cache und öffnen Sie sie neu**.

    Lösung

    - Melden Sie sich mit der GUI am Citrix ADC an.
    - Navigieren Sie zu Citrix ADC Gateway > Globale Einstellungen.
    - Klicken Sie unter Einstellungen auf Globale Einstellungen ändern.
    - Wählen Sie im Detailbereich unter Client Experience die Option Standard aus der Liste des Benutzeroberflächendesigns aus.
    - Klicken Sie auf OK.

20. **Problem**

Wenn das Upgrade einer Citrix ADC Appliance aus irgendeinem Grund fehlgeschlagen ist, wie kann die Appliance mithilfe der gesicherten Dateien wiederhergestellt werden?

Lösung

Wenn das Upgrade nicht erfolgreich ist, stellen Sie die Appliance mithilfe der gesicherten Dateien auf die vorherige Version der Citrix ADC Appliance wieder her. Weitere Informationen finden Sie unter Sichern und Wiederherstellen einer Citrix ADC Appliance.

Weitere Informationen zum Backup und Wiederherstellen eines Citrix ADC Cluster-Setups finden Sie unter Sichern und Wiederherstellen eines Cluster-Setups.

21. **Problem**

    Wenn nach einem fehlgeschlagenen Upgrade einer Citrix ADC Appliance Lizenzen fehlen, wie kann das Problem behoben werden?

    Lösung

    Wenn eine Lizenz fehlt oder Sie die Lizenzen neu zuweisen möchten, lesen Sie das folgende Thema Übersicht über die Lizenzierung.

> **Hinweis:**
>
> Diese Schritte zur Fehlerbehebung gelten auch für Probleme mit Konfigurationsverlust beim Herabstufen der Software über mehrere Versionen hinweg.
>
> Weitere Probleme finden Sie in den Versionshinweisen, Knowledge Center-Artikeln und häufig gestellten Fragen.

FAQ

October 5, 2021

Antworten auf die Fragen, die Sie möglicherweise zum Upgrade der Citrix ADC-Firmware haben, finden Sie unter Häufig gestellte Fragen zum Installieren, Aktualisieren und Downgraden .

Neue und veraltete Befehle, Parameter und SNMP-OIDs

October 5, 2021

In diesem Abschnitt werden die neuen und veralteten Befehle, Parameter und SNMP-OIDs aufgelistet.

Neue Befehle

In der folgenden Tabelle sind die neuen Befehle in Version 13.0 aufgeführt.

Befehlsgruppe	Befehl
Authentifizierung, Autorisierung und Auditing	add aaa ssoprofile; rm aaa ssoprofile; show aaa ssoprofile; set aaa ssoprofile; add authentication citrixAuthAction; rm authentication citrixAuthAction; set authentication citrixAuthAction; unset authentication citrixAuthAction; show authentication citrixAuthAction; lock aaa user; set aaa otpparameter; show aaa otpparameter; add authentication emailAction; rm authentication emailAction; set authentication emailAction; show authentication emailAction; add authentication noAuthAction; rm authentication noAuthAction; set authentication noAuthAction; show authentication noAuthAction; add authentication captchaAction; rm authentication captchaAction; set authentication captchaAction; show authentication captchaAction; add authentication adfsProxyProfile; rm authentication adfsProxyProfile; set authentication adfsProxyProfile; show authentication adfsProxyProfile
AppFlow	bind appflow action; unbind appflow action
Anwendungs-Firewall	stat rnat6 and stat MapBmr

Befehlsgruppe	Befehl
Inhaltsprüfung	add contentInspection profile; rm contentInspection profile; set contentInspection profile; show contentInspection profile; add contentInspection callout; rm contentInspection callout; set contentInspection callout; show contentInspection callout; count contentInspection callout; set contentInspection parameter; unset contentInspection parameter; show contentInspection parameter
LSN	add lsn appsattributes; rm lsn appsattributes; set lsn appsattributes; show lsn appsattributes
Network	add rnat; rename rnat; bind rnat; unbind rnat; rm rnat
SSL	add ssl caCertGroup; bind ssl caCertGroup; rm ssl caCertGroup; unbind ssl caCertGroup; show ssl caCertGroup
System	enable system autorestorefeature ; rm system restorepoint; show system restorepoint; migrate ns; show ns timezone; disable system autorestorefeature; create system restorepoint
URL-Filterung	add urlfiltering Categorization; clear urlfiltering Categorization; show urlfiltering Categorization
VPN	add vpn urlPolicy; rm vpn urlPolicy; set vpn urlPolicy; show vpn urlPolicy; stat vpn urlPolicy; rename vpn urlPolicy; add vpn urlAction; rm vpn urlAction; set vpn urlAction; show vpn urlAction; rename vpn urlAction

Neue Parameter

Befehlsgruppe: Authentifizierung, Autorisierung und Auditing

Befehl:

- set aaa parameter [-maxKBQuestions]
- unset aaa parameter [-maxKBQuestions]
- show aaa parameter [-maxKBQuestions]

Befehlsgruppe: Admin Partition

Befehl:

- add ns ip6 [-advertiseOnDefaultPartition]
- set ns ip6 [-advertiseOnDefaultPartition]
- show ns ip6[-advertiseOnDefaultPartition]
- add ns ip [-advertiseOnDefaultPartition]
- set ns ip [-advertiseOnDefaultPartition]
- show ns ip[-advertiseOnDefaultPartition]

Befehlsgruppe: AppFlow

Befehl:

- bind appflow action [-analyticsProfile]
- unbind appflow action [-analyticsProfile]
- show appflow action [-analyticsProfile]
- set appflow param [-gxSessionReporting] [-usageRecordInterval] [-metrics] [-events [-auditlogs] [-observationPointId] [-distributedTracing] [-distTracingSamplingRate] [-tcpAttackCounterInterval]
- show appflow param [-observationPointId] [-subscriberIdObfuscationAlgo] [-gxSessionReporting] [-usageRecordInterval] [-metrics] [-events] [-auditlogs [-distributedTracing] [-distTracingSamplingRate] [-tcpAttackCounterInterval]

Befehlsgruppe: Anwendungsfirewall

Befehl:

- add appfw profile [-postBodyLimitSignature]
- add appfw profile [-rfcprofile]
- set appfw profile [-postBodyLimitSignature] [-rfcprofile]
- show appfw profile [-postBodyLimitSignature] [-rfcprofile]
- set appfw settings [-malformedReqAction]
- show appfw settings [-malformedReqAction]
- import appfw signatures [-preservedefactions]

Befehlsgruppe: Prüfung

Befehl:

- add audit syslogAction [-ContentInspectionLog]
- set audit syslogAction [-ContentInspectionLog]

- unset audit syslogAction [-ContentInspectionLog]
- show audit syslogAction [-ContentInspectionLog]
- add audit nslogAction [-ContentInspectionLog]
- set audit nslogAction [-ContentInspectionLog]
- unset audit nslogAction [-ContentInspectionLog]
- show audit nslogAction [-ContentInspectionLog]
- set audit syslogParams [-ContentInspectionLog]
- unset audit syslogParams [-ContentInspectionLog]
- show audit syslogParams [-ContentInspectionLog]
- set audit nslogParams [-ContentInspectionLog]
- unset audit nslogParams [-ContentInspectionLog]
- show audit nslogParams [-ContentInspectionLog]

Befehlsgruppe: Authentifizierung

Befehl:

- add authentication ldapAction [-KBAttribute] [-alternateEmailAttr]
- set authentication ldapAction [-KBAttribute] [-alternateEmailAttr]
- show authentication ldapAction [-KBAttribute] [-alternateEmailAttr]
- add authentication tacacsAction [-Attributes]
- set authentication tacacsAction [-Attributes]
- show authentication tacacsAction [-Attributes]
- add authentication samlAction [-Attributes] [-storeSAMLResponse]
- set authentication samlAction [-Attributes] [-storeSAMLResponse]
- show authentication samlAction [-Attributes] [-storeSAMLResponse]
- add authentication vserver [-certkeyNames]
- set authentication vserver [-certkeyNames]
- show authentication vserver [-certkeyNames]- show authentication loginSchema [-feature]- - add authentication OAuthIDPProfile [-configservice] [-signatureAlg] [-Attributes][-sendPassword]
- set authentication OAuthIDPProfile [-configservice] [-signatureAlg] [-Attributes] [-sendPassword]
- show authentication OAuthIDPProfile [-configservice] [-signatureAlg] [-Attributes] [-sendPassword]
- add authentication pushService [-CertEndpoint] [-signingKeyName] [-signingKey] [-clientID] [-clientSecret] [-CustomerID] [-refreshInterval] [-trustService]
- set authentication pushService [-CertEndpoint] [-signingKeyName] [-signingKey] [-clientID] [-clientSecret] [-CustomerID] [-refreshInterval] [-trustService]
- show authentication pushService [-clientID] [-clientSecret] [-CustomerID] [-CertEndpoint] [-refreshInterval] [-pushServiceStatus] [-trustService] [-pushCloudServerStatus] [-signingKeyName] [-signingKey]
- show authentication adfsProxyProfile [-adfsTrustStatus]

Befehlsgruppe: Basic

Befehl:

- add server [-queryType]
- show server [-queryType] [-serviceGroupEntName2] [-svcitmPriority] [-svcitmActSvcs] [-svcitmBoundSvcs] [-weight]
- add service [-contentInspectionProfileName]
- set service[-contentInspectionProfileName]
- unset service [-contentInspectionProfileName]- show service [-contentInspectionProfileName]- bind serviceGroup [-nameServer] [-dbsTTL]
- show serviceGroup [-numOfCurConnections] [-numOfLastConnections] [-nameServer] [-dbsTTL] [-svcitmActSvcs] [-svcitmPriority] [-svcitmBoundSvcs]

Befehlsgruppe: Cache-Umleitung

Befehl:

- add cr vserver [-UseOriginIpPortForCache]
- set cr vserver [-UseOriginIpPortForCache]
- show cr vserver [-UseOriginIpPortForCache]

Befehlsgruppe: Clustering

Befehl:

- show cluster instance [-heterogeneousFlag]

Befehlsgruppe: Content Switching

Befehl:

- add cs vserver [-persistenceType] [-persistMask] [-v6persistmasklen] [-timeout] [-cookieName] [-persistenceBackup] [-backupPersistenceTimeout]
- set cs vserver [-persistenceType] [-persistMask] [-v6persistmasklen] [-timeout] [-cookieName] [-persistenceBackup] [-backupPersistenceTimeout]
- show cs vserver [-persistenceType] [-persistMask] [-v6persistmasklen] [-timeout] [-cookieName] [-persistenceBackup] [-backupPersistenceTimeout]

Befehlsgruppe: DNS

Befehl:

- set dns nameServer [-type]
- rm dns nameServer [-type]
- enable dns nameServer [-type]
- disable dns nameServer [-type]
- show dns action64
- set dns parameter [-maxUDPPacketSize]
- show dns parameter [-maxUDPPacketSize]

Befehlsgruppe: GSLB

Befehl:

- show gslb service [-gslbsvcHealth] [-glsbsvcHealthdescr]
- show gslb parameter [-builtin]

Befehlsgruppe: Hochverfügbarkeit

Befehl:

- show HA node [-haSyncFailureReason]

Befehlsgruppe: ICA

Befehl:

- set ica parameter [-HDXInsightNonNSAP]
- show ica parameter [-HDXInsightNonNSAP]

Befehlsgruppe: Load Balancing

Befehl:

- add lb vserver [-adfsProxyProfile]
- set lb vserver [-adfsProxyProfile]
- unset lb vserver [-adfsProxyProfile]
- show lb vserver [-adfsProxyProfile]
- set lb parameter [-dbsTTL]
- show lb parameter [-dbsTTL]

Befehlsgruppe: LSN

Befehl:

- add lsn logprofile [-analyticsProfile] [-logSessDeletion]
- set lsn logprofile [-analyticsProfile] [-logSessDeletion]
- show lsn logprofile [-analyticsProfile] [-logSessDeletion]
- bind lsn appsprofile [-appsattributesname]
- unbind lsn appsprofile [-appsattributesname]
- show lsn appsprofile [-appsattributesname]

Befehlsgruppe: Netzwerk

Befehl:

- add route [-vlan]
- rm route [-vlan]
- add netProfile [-proxyProtocol] [-proxyProtocoltxversion]
- set netProfile [-proxyProtocol] [-proxyProtocoltxversion]
- NetProfile anzeigen [-proxyProtocol] [-proxyProtocoltxversion]

- set rnat [-name]
- unset rnat [-name]
- add rnat [-name]
- rename rnat [-name] [-newName]
- bind rnat [-name] [-natIP]
- unbind rnat [-name] [-natIP]
- rm rnat [-name]
- show rnat [-name] [-stateflag]

Befehlsgruppe: Richtlinie

Befehl:

- show policy expression
- show policy patset
- show policy urlset [-imported]
- import policy urlset [-subdomainExactMatch]

Befehlsgruppe: RDP

Befehl:

- add rdp clientprofile [-randomizeRDPFilename] [-rdpLinkAttribute]
- set rdp clientprofile [-randomizeRDPFilename] [-rdpLinkAttribute]
- show rdp clientprofile [-randomizeRDPFilename] [-rdpLinkAttribute]
- add rdp serverprofile [-rdpRedirection]
- set rdp serverprofile [-rdpRedirection]
- show rdp serverprofile [-rdpRedirection]

Befehlsgruppe: SSL

Befehl:

- create ssl ecdsaKey [-pkcs8]
- ssl certKey [-deletefromdevice]
- clear ssl certKey [-ocspstaplingCache]
- add ssl action [-caCertGrpName]
- show ssl action [-clientCertVerification] [-caCertGrpName]
- show ssl ocspResponder [-port]
- create ssl rsakey [-pkcs8]
- set ssl parameter [-ndcppComplianceCertCheck]
- show ssl parameter [-ndcppComplianceCertCheck]
- set ssl vserver [-preload] [-preload]
- show ssl dtlsProfile
- add ssl profile [-preload]

- set ssl profile [-preload]
- show ssl profile [-preload]

Befehlsgruppe: System

Befehl:

- create system backup [-useLocalTimezone] [-includekernel]
- show system backup [-useLocalTimezone]
- add ns tcpProfile [-taillossprobe]
- set ns tcpProfile [-taillossprobe]
- show ns tcpProfile [-taillossprobe]
- add ns icapProfile [-insertHTTPRequest]
- set ns icapProfile [-insertHTTPRequest]
- show ns icapProfile [-insertHTTPRequest]
- add ns httpProfile [-markTraceReqInval]
- set ns httpProfile [-markTraceReqInval]
- unset ns httpProfile [-markTraceReqInval]
- show ns httpProfile[- markTraceReqInval]
- save ns config all
- set ns param [-mgmthttpport] [-mgmthttpsport] [-proxyProtocol]
- show ns param [-mgmthttpport] [-mgmthttpsport] [-proxyProtocol]
- set ns httpParam [-ignoreConnectCodingScheme]
- show ns httpParam [-ignoreConnectCodingScheme]
- add ns icapProfile [-logAction]
- set ns icapProfile [-logAction]
- show ns icapProfile [-logAction]

Befehlsgruppe: Abonnent

Befehl:

- set subscriber gxInterface [-healthCheck] [-healthCheckTTL] [-cerRequestTimeout] [-negativeTTLLimitedSuccess] [-purgeSDBonGxFailure] [-gxReportingAvp1] [-gxReportingAvp1VendorId] [-gxReportingAvp1Type] [-gxReportingAvp2] [-gxReportingAvp2VendorId] [-gxReportingAvp2Type] [-gxReportingAvp3] [-gxReportingAvp3VendorId] [-gxReportingAvp3Type] [-gxReportingAvp4] [-gxReportingAvp4VendorId] [-gxReportingAvp4Type] [-gxReportingAvp5] [-gxReportingAvp5VendorId] [-gxReportingAvp5Type]
- show subscriber gxInterface [-healthCheck] [-healthCheckTTL] [-cerRequestTimeout] [-negativeTTLLimitedSuccess] [-purgeSDBonGxFailure] [-gxReportingAvp1] [-gxReportingAvp1VendorId] [-gxReportingAvp1Type] [-gxReportingAvp2] [-gxReportingAvp2VendorId] [-gxReportingAvp2Type] [-gxReportingAvp3] [-gxReportingAvp3VendorId] [-gxReportingAvp3Type] [-gxReportingAvp4] [-gxReportingAvp4VendorId] [-gxReportingAvp4Type] [-gxReportingAvp5] [-gxReportingAvp5VendorId] [-gxReportingAvp5Type]

Befehlsgruppe: Verkehrsmanagement

Befehl:

- show tm sessionPolicy
- show tm sessionAction
- show tm global
- show tm sessionParameter [-tmsessionpolicyBindtype] [-tmsessionpolicyCount]

Befehlsgruppe: URL-Filterung

Befehl:

- set urlfiltering parameter [-CloudHost] [-SeedDBPath]
- show urlfiltering parameter [-CloudHost] [-SeedDBPath]

Befehlsgruppe: VPN

Befehl:

- show vpn sessionPolicy
- add vpn sessionAction [-fqdnSpoofedIP]
- set vpn sessionAction [-fqdnSpoofedIP]
- show vpn sessionAction [-feature] [-fqdnSpoofedIP]
- show vpn clientlessAccessPolicy
- bind vpn global [-userDataEncryptionKey]
- unbind vpn global [-userDataEncryptionKey]
- show vpn global [-userDataEncryptionKey]
- set vpn parameter [-fqdnSpoofedIP] [-netmask]
- unset vpn parameter [-fqdnSpoofedIP]
- show vpn parameter [-fqdnSpoofedIP]

Veraltete Parameter

Befehlsgruppe: AppFlow

Befehl:

- add appflow action [-MetricsLog]
- show appflow action [-MetricsLog]

Befehlsgruppe: LSN

Befehl:

- add lsn transportprofile [-stuntimeout]
- set lsn transportprofile [-stuntimeout]

- show lsn transportprofile [-stuntimeout]

Befehlsgruppe: Netzwerk

Befehl:

- clear rnat

Lösungen für Telekommunikationsdienstleister

October 5, 2021

Informations- und Kommunikationstechnologie (ICT) geht es darum, den Internetnutzer näher an die Apps und Daten zu bringen. Dank der neuesten Rechenzentrumstechnologien können Benutzer, Apps und Daten überall lokalisiert werden. Ein Benutzer kann über das Büro oder von zu Hause aus oder von einem Standort wie einem Flughafen aus auf Apps und Daten zugreifen. Die Apps und Daten können sich entweder auf dem Firmengelände, in einer öffentlichen oder privaten Cloud oder auf einem Hybrid-Host befinden. Das Ergebnis war nur eine höhere Produktivität, aber auch eine geringere Betriebs- und Wartungskosten.

Service bietet die Kerninfrastruktur, die für die Übertragung der Apps und Daten des Benutzers über das Netzwerk erforderlich ist. Da die Kerninfrastruktur Millionen von Abonnenten und eine Vielzahl von Apps und Daten bedient, sind die Anforderungen an Skalierung und Protokollunterstützung sehr hoch. Die Kerninfrastruktur übernimmt zwei Hauptverkehrstypen: Datenebene und Steuerebene. Jede dieser Flugzeuge hat seine eigene Maßstabs- und Protokollunterstützungsanforderungen.

Die Datenebene ist der Teil der Kerninfrastruktur, die Benutzeranwendungen und Daten von End-to-End, d. h. zwischen Endbenutzergeräten und dem Anwendungsserver, transportiert. Die Anzahl der Benutzer, die auf Apps und Daten zugreifen, liegt in den Tausenden von Millionen, daher sind die Anforderungen an den Durchsatz und die IP-Adressierung sehr hoch. Jeder Benutzer im Netzwerk muss eindeutig identifizierbar sein. Nur dann kann der Dienstanbieter den Datenverkehr steuern, die Netzwerkauslastung überwachen, benutzerspezifische Dienste bereitstellen und Informationen korrekt protokollieren. Viele der heutigen Clientgeräte und Anwendungsserver unterstützen IPv6 nativ. Die Kerninfrastruktur muss nicht nur eine Mischung aus IPv4- und IPv6-Clients und Servern unterstützen, sondern auch Technologien für die Kommunikation zwischen IPv4 und IPv6 bereitstellen. Schließlich wird ein Dienstleister an der Qualität der Dienstleistung (direkt im Zusammenhang mit der Endbenutzererfahrung) und der Verfügbarkeit von Diensten ohne Unterbrechungen gemessen. Die Datenebene sollte robust genug sein, um gleichzeitig Qualität und Verfügbarkeit zu gewährleisten.

Die Control-Plane-Infrastruktur verwaltet den Benutzerverkehr und verwaltet die Geschäfts- und Netzwerkbetriebsdienste. Die wichtigsten der vielen Protokolle, die in dieser Ebene ausgeführt werden,

sind Durchmesser, Radius und SMPP. Durchmesser ist ein Basisprotokoll, über das mehrere andere funktionsspezifische Protokolle entwickelt wurden. Beispiel:

- GX-Schnittstelle zwischen der Policy and Charging Enforcement Function (PCEF) und der Policy and Charging Rules Function (PCRF)
- Gy-Schnittstelle zwischen dem Online Charging System (OCS) und dem Cisco Packet Data Network Gateway (PGW) /Policy and Charging Enforcement Function (PCEF)

Das Volumen des Verkehrs der Steuerebene steht in direktem Verhältnis zur Benutzeraktivität. Für die Verwaltung des Datenverkehrs der Steuerungsebene verwenden Dienstanbieter verschiedene ADC-Funktionen, wie Lastausgleich und Content Switching. Sie benötigen feinkörnige Kontrolle des Datenverkehrs auf Steuerebene, was dem Datenverkehr in der Komplexität entspricht.

Dienstleister müssen anspruchsvolle Service-Level-Agreements (SLAs) einhalten und von den Regulierungsbehörden sorgfältig auf Compliance geprüft werden. Die Einhaltung der Anforderungen bei der Verwaltung des Datenverkehrs und der Steuerung des Flugzeugverkehrs erfordert, dass ein Dienstleister seine Infrastruktur flink, im Budget, leicht aufrüstbar und flexibel hält. Als die leistungsstärksten und fortschrittlichsten ADCs auf dem Markt sind Citrix ADC Produkte eine natürliche Lösung für die Service-Provider-Umgebung.

Großes NAT

October 5, 2021

> **Hinweis:**
>
> Diese Funktion ist mit einer Lizenz für Citrix ADC Advanced oder Premium Edition verfügbar.

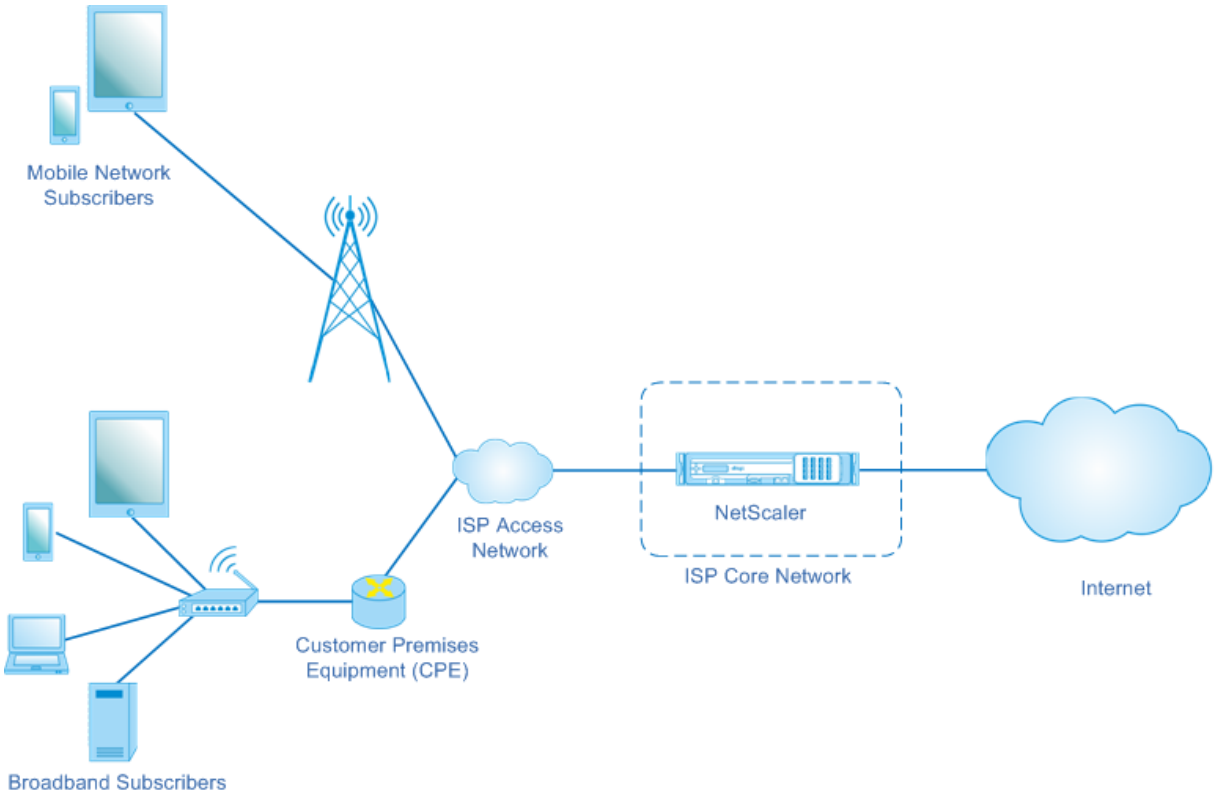
Das phänomenale Wachstum des Internets hat zu einem Mangel an öffentlichen IPv4-Adressen geführt. Large Scale NAT (LSN/CGNAT) bietet eine Lösung für dieses Problem und maximiert die Nutzung der verfügbaren öffentlichen IPv4-Adressen, indem einige öffentliche IPv4-Adressen unter einem großen Pool von Internetnutzern geteilt werden.

LSN übersetzt private IPv4-Adressen in öffentliche IPv4-Adressen. Es enthält Netzwerkadressen und Portübersetzungsmethoden, um viele private IP-Adressen in weniger öffentlichen IPv4-Adressen zu aggregieren. LSN wurde entwickelt, um NAT im großen Maßstab zu handhaben. Die Citrix ADC LSN-Funktion ist sehr nützlich für Internet Service Provider (ISPs) und Carrier, die Millionen von Übersetzungen zur Unterstützung einer großen Anzahl von Benutzern (Abonnenten) und bei sehr hohem Durchsatz bereitstellen.

LSN-Architektur

Die LSN-Architektur eines ISP, der Citrix Produkte verwendet, besteht aus Abonnenten (Internetbenutzer) in privaten Adressräumen, die über eine Citrix ADC Appliance auf das Internet zugreifen, die im Kernnetzwerk des ISP bereitgestellt wird. Abonnenten sind über das Zugangsnetzwerk des ISP mit dem ISP verbunden. In der Regel sind Abonnenten für die kommerzielle Nutzung des Internets direkt mit dem Zugangsnetzwerk des ISP verbunden. Die Bereitstellung dieser Abonnenten erfordert nur eine NAT-Ebene (NAT44).

Nicht-kommerzielle Abonnenten befinden sich jedoch in der Regel hinter Kunden-Premises Equipment (CPE), wie Router und Modems, die auch NAT implementiert. Diese beiden NAT-Ebenen erstellen das NAT444-Modell. Die Bereitstellung einer Citrix ADC Appliance im Kernnetzwerk eines ISP für die LSN-Funktionalität ist für die Abonnenten transparent und erfordert keine Konfigurationsänderungen an Abonnenten oder CPEs.



Large Scale NAT

Die Citrix ADC Appliance empfängt alle Abonnentenpakete, die für das Internet bestimmt sind. Die Appliance ist mit einem Pool vordefinierter NAT-IP-Adressen für LSN konfiguriert. Die Citrix ADC Appliance verwendet ihre LSN-Funktion, um die Quell-IP-Adresse (privat) und den Port des Pakets in die NAT-IP-Adresse (öffentlich) und den NAT-Port zu übersetzen und das Paket dann an das Ziel im Internet zu senden. Die Appliance verwaltet eine Aufzeichnung aller aktiven Sitzungen, die die LSN-Funktion verwenden. Diese Sitzungen werden LSN-Sitzungen genannt. Die Citrix ADC Appliance verwaltet auch die Zuordnungen zwischen Teilnehmer-IP-Adresse und -Port sowie NAT-IP-Adresse und

-Port für jede Sitzung. Diese Zuordnungen werden LSN-Zuordnungen genannt. Aus LSN-Sitzungen und LSN-Zuordnungen erkennt die Citrix ADC Appliance ein Antwortpaket (vom Internet empfangen), das zu einer bestimmten Sitzung gehört. Die Appliance übersetzt die Ziel-IP-Adresse und den Port des Antwortpakets von der NAT-IP-Adresse:Port in die Teilnehmer-IP-Adresse:Port und sendet das übersetzte Paket an den Abonnenten.

Von Citrix ADC Appliance unterstützte LSN-Funktionen

Im Folgenden werden einige der von Citrix ADC Appliance unterstützten LSN-Funktionen beschrieben:

NAT-Ressourcenzuordnung

Die Citrix ADC Appliance weist Abonnenten NAT-IP-Adressen und -Ports aus ihrem vordefinierten NAT-Ressourcenpool zu, um ihre Pakete für die Übertragung an externe Hosts (Internet) zu übersetzen. Die Citrix ADC Appliance unterstützt die folgenden Typen von NAT-IP-Adresse und Port-Zuweisung für Abonnenten:

- **Deterministisch.** Die Citrix ADC Appliance weist jedem Abonnenten eine NAT-IP-Adresse und einen Block von Ports zu. Die Appliance weist diesen Abonnenten nacheinander NAT-Ressourcen zu. Der erste Block von Ports auf der beginnenden NAT-IP-Adresse wird der IP-Adresse des beginnenden Teilnehmers zugewiesen. Der nächste Bereich von Ports wird dem nächsten Abonnenten zugewiesen usw., bis die NAT-Adresse nicht über genügend Ports für den nächsten Abonnenten verfügt. Zu diesem Zeitpunkt wird der erste Portblock auf der nächsten NAT-Adresse dem Abonnenten zugewiesen usw.

  Die Citrix ADC Appliance protokolliert die zugewiesene NAT-IP-Adresse und den Portblock für einen Abonnenten. Bei einer Verbindung kann ein Teilnehmer nur anhand seiner zugeordneten NAT-IP-Adresse und des Portblocks identifiziert werden. Aus diesem Grund protokolliert die Citrix ADC Appliance keine erstellten oder gelöschten LSN-Sitzungen. Wenn der gesamte Port Block verwendet wird, löscht die Citrix ADC Appliance jede neue Verbindung vom Abonnenten.

- **Dynamisch.** Die Citrix ADC Appliance weist eine zufällige NAT-IP-Adresse und einen Port aus dem LSN-NAT-Pool für die Verbindung eines Teilnehmers zu. Wenn die Portblockzuweisung in der Konfiguration aktiviert ist, weist die Appliance eine zufällige NAT-IP-Adresse und einen Block von Ports für einen Teilnehmer zu, wenn eine Verbindung zum ersten Mal initiiert wird. Die Citrix ADC Appliance weist dann diese NAT-IP-Adresse und einen der Ports aus dem zugewiesenen Block jeder nachfolgenden Verbindung dieses Abonnenten zu. Wenn der gesamte Block von Ports verwendet wird, weist die Appliance dem Abonnenten einen neuen zufälligen Portblock zu, wenn eine neue Verbindung initiiert wird. Einer der Ports im neuen Portblock wird für die neue Verbindung zugewiesen.

IP-Pooling

Die folgenden NAT-Ressourcenzuweisungsoptionen sind für nachfolgende Sitzungen eines Abonnenten verfügbar, dem eine zufällige NAT-IP-Adresse und Port für eine vorhandene Sitzung zugewiesen wurde.

- **Paarweise.** Die Citrix ADC Appliance weist dieselbe NAT-IP-Adresse für alle Sitzungen zu, die demselben Abonnenten zugeordnet sind. Wenn keine weiteren Ports für diese Adresse verfügbar sind, löscht die Appliance neue Verbindungen vom Abonnenten. Diese Option ist für das ordnungsgemäße Funktionieren bestimmter Anwendungen erforderlich, bei denen mehrere Sitzungen mit derselben Quell-IP-Adresse erstellt werden müssen (z. B. in Peer-to-Peer-Anwendungen, die RTP- oder RTCP-Protokoll verwenden.
- **Zufällig.** Die Citrix ADC Appliance weist zufällige NAT-IP-Adressen aus dem Pool für verschiedene Sitzungen zu, die demselben Teilnehmer zugeordnet sind.

Wiederverwenden von LSN-Zuordnungen

Die Citrix ADC Appliance kann eine vorhandene LSN-Zuordnung für neue Verbindungen wiederverwenden, die von derselben Teilnehmer-IP-Adresse und demselben Port stammen. Das Citrix ADC LSN-Feature unterstützt die folgenden Arten der Wiederverwendung von LSN-Zuordnungen:

1. **Endpunktunabhängig.** Die Citrix ADC Appliance verwendet die LSN-Zuordnung für nachfolgende Pakete, die von derselben Teilnehmer-IP-Adresse und demselben Port (x:x) an jede externe IP-Adresse und Port gesendet werden. Diese Art der Wiederverwendung von LSN-Karten ist nützlich für das ordnungsgemäße Funktionieren von VOIP- und Peer-to-Peer-Anwendungen.
2. **Adressenabhängig.** Die Citrix ADC Appliance verwendet die LSN-Zuordnung für nachfolgende Pakete, die von derselben Teilnehmer-IP-Adresse und demselben Port (x:x) an dieselbe externe IP-Adresse (Y) gesendet werden, unabhängig vom externen Port.
3. **Adressenport abhängig.** Die Citrix ADC Appliance verwendet die LSN-Zuordnung für nachfolgende Pakete, die von derselben internen IP-Adresse und demselben Port (x:x) an dieselbe externe IP-Adresse und denselben Port (Y:Y) gesendet werden, während die Zuordnung noch aktiv ist.

LSN-Filter

Die Citrix ADC Appliance kann Pakete von externen Hosts basierend auf den aktiven LSN-Sitzungen und LSN-Zuordnungen filtern. Betrachten Sie ein Beispiel für eine LSN-Zuordnung, die die Zuordnung von Teilnehmer-IP:Port (X:x), NAT IP:Port (N:n) und externem Host IP:Port (Y:y) umfasst. Das Citrix ADC LSN-Feature unterstützt die folgenden Filtertypen:

1. **Endpunktunabhängig.** Die Citrix ADC Appliance filtert nur die Pakete aus, die nicht für NAT IP bestimmt sind: Port (n:n), die die Teilnehmer-IP: Port (x:x) darstellt, unabhängig von der IP-

Adresse des externen Hosts und der Portquelle (z:z). Die Citrix ADC Appliance leitet alle Pakete, die für X:x bestimmt sind, weiter. Mit anderen Worten, das Senden von Paketen vom Abonnenten an eine externe IP-Adresse reicht aus, um Pakete von jedem externen Host an den Abonnenten zuzulassen. Diese Art der Filterung ist nützlich für das ordnungsgemäße Funktionieren von VOIP- und Peer-to-Peer-Anwendungen.

2. **Adressenabhängig.** Die Citrix ADC Appliance filtert Pakete aus, die nicht für NAT IP bestimmt sind: Port (n:n), die die Teilnehmer-IP: Port (x:x) darstellt. Darüber hinaus filtert die Appliance Pakete aus der externen Host-IP-Adresse und dem Port (Y:y) heraus, die für n:n bestimmt sind, wenn der Abonnent zuvor keine Pakete an y:anyPort (externer Port unabhängig) gesendet hat. Mit anderen Worten, das Empfangen von Paketen von einem bestimmten externen Host erfordert, dass der Abonnent zuerst Pakete an die IP-Adresse dieses bestimmten externen Hosts sendet.
3. **Adressenport abhängig.** Die Citrix ADC Appliance filtert Pakete aus, die nicht für NAT IP bestimmt sind: Port (n:n), die die Teilnehmer-IP: Port (x:x) darstellt. Darüber hinaus filtert die Appliance Pakete aus der externen Host-IP-Adresse und dem Port (Y:y) heraus, die für n:n bestimmt sind, wenn der Abonnent zuvor keine Pakete an y:y gesendet hat. Mit anderen Worten, das Empfangen von Paketen von einem bestimmten externen Host erfordert, dass der Abonnent zuerst Pakete an diese spezifische externe IP-Adresse und Port sendet.

Quoten

Die Citrix ADC Appliance kann die Anzahl der NAT-Ports und -Sitzungen für jeden Abonnenten beschränken, um eine faire Verteilung der Ressourcen auf die Abonnenten zu gewährleisten. Die Citrix ADC Appliance kann auch die Anzahl der Sitzungen für eine Teilnehmergruppe einschränken, um eine faire Verteilung der Ressourcen auf verschiedene Teilnehmergruppen zu gewährleisten.

- **Portkontingent.** Die Citrix ADC Appliance kann die LSN-NAT-Ports begrenzen, die von jedem Abonnenten für ein bestimmtes Protokoll gleichzeitig verwendet werden sollen. Beispielsweise können Sie jeden Abonnenten auf maximal 500 TCP-NAT-Ports beschränken. Wenn die LSN-NAT-Zuordnungen für einen Abonnenten das Limit erreichen, weist die Citrix ADC Appliance diesem Abonnenten keine zusätzlichen NAT-Ports des angegebenen Protokolls zu.
- **Abonnentensitzung Limit.** Die Anzahl der gleichzeitigen Sitzung für einen Abonnenten kann mehr als das Portkontingent sein. Die Citrix ADC Appliance kann die LSN-Sitzungen begrenzen, die für jeden Abonnenten für ein bestimmtes Protokoll zulässig sind. Wenn die Anzahl der LSN-Sitzungen das Limit für einen Abonnenten erreicht, erlaubt die Citrix ADC Appliance dem Abonnenten nicht, zusätzliche Sitzungen des angegebenen Protokolls zu öffnen.
- **Gruppensitzungslimit.** Die Citrix ADC Appliance kann die Gesamtanzahl der LSN-Sitzungen einschränken, die für eine Teilnehmergruppe für ein bestimmtes Protokoll zulässig sind. Wenn die Gesamtanzahl der LSN-Sitzungen die Grenze für eine Gruppe für ein bestimmtes Protokoll erreicht, erlaubt die Citrix ADC Appliance keinem Abonnenten der Gruppe, zusätzliche Sitzungen

des angegebenen Protokolls zu öffnen. Beispielsweise beschränken Sie eine Gruppe auf maximal 10000 UDP-Sitzungen. Wenn die Gesamtzahl der UDP-Sitzungen für diese Gruppe 10000 erreicht, erlaubt die Citrix ADC Appliance keinem Abonnenten der Gruppe das Öffnen zusätzlicher UDP-Sitzungen.

Anwendungs-Layer-Gateways

Bei einigen Protokollen der Anwendungsschicht werden auch die IP-Adressen und Protokollportnummern in der Nutzlast des Pakets kommuniziert. Application Layer Gateway für ein Protokoll analysiert die Nutzlast des Pakets und führt notwendige Änderungen durch, um sicherzustellen, dass das Protokoll weiterhin über LSN funktioniert.

Die Citrix ADC Appliance unterstützt ALG für die folgenden Protokolle:

- FTP
- ICMP
- TFTP
- PPTP
- SIP
- RTSP

Haarnadel-Unterstützung

Die Citrix ADC Appliance unterstützt die Kommunikation zwischen Abonnenten oder internen Hosts unter Verwendung von NAT-IP-Adressen. Diese Art der Kommunikation zwischen zwei Abonnenten, die NAT IP-Adressen verwenden, wird als Hairpin Flow bezeichnet. Der Haarnadelfluss ist standardmäßig aktiviert und kann nicht deaktiviert werden.

Vor der Konfiguration von LSN zu berücksichtigende Punkte

October 5, 2021

Berücksichtigen Sie die folgenden Punkte, bevor Sie LSN auf einer Citrix ADC Appliance konfigurieren:

- Stellen Sie sicher, dass Sie die verschiedenen Komponenten von Large Scale NAT kennen, die in RFCs 6888, 5382, 5508 und 4787 beschrieben sind.
- Endpoint Independent Mapping (EIM) und Endpoint Independent Filterung (EIF) sind standardmäßig deaktiviert. Diese Optionen müssen für die ordnungsgemäße Funktion von VoIP- und Peer-to-Peer-Anwendungen (P2P) aktiviert sein.
- **Logging LSN**: Im Folgenden sind die Überlegungspunkte für die Protokollierung von LSN-Informationen:

  - Citrix empfiehlt, die LSN-Informationen auf externen Protokollservern anstatt auf der Citrix ADC Appliance zu protokollieren. Die Protokollierung auf externen Servern erleichtert die optimale Leistung, wenn die Appliance eine große Anzahl von LSN-Protokolleinträgen erstellt (in der Größenordnung von Millionen).
  - Citrix empfiehlt die Verwendung von SYSLOG über TCP oder NSLOG. Standardmäßig verwendet SYSLOG UDP und NSLOG verwendet nur TCP, um Protokollinformationen an die Protokollserver zu übertragen. TCP ist zuverlässiger als UDP für die Übertragung kompletter Daten.
  - Die folgenden Einschränkungen gelten für SYSLOG über TCP:
    * Die Syslog über TCP-Lösung bietet keine Authentifizierung, Integritätsprüfung und Datenschutz.
    * Die Citrix ADC Appliance stützt sich auf das TCP-Protokoll, um die SYSLOG-Nachrichtenübermittlung an externe Protokollserver zu bestätigen.
- **Hochverfügbarkeit**: Im Folgenden werden die Überlegungen für die hohe Verfügbarkeit von Citrix ADC Appliances für LSN aufgeführt:
  - Citrix empfiehlt die Konfiguration der LSN-Funktion in einer Hochverfügbarkeitsbereitstellung von zwei Citrix ADC Appliances für den unterbrechungsfreien und nahtlosen Betrieb aller LSN-Sitzungen.
  - In einer Hochverfügbarkeitsbereitstellung empfiehlt Citrix:
    * Festlegen des SYNC VLAN-Parameters für die Widmung eines VLAN für die gesamte HA-bezogene Kommunikation.
    * Synchronisieren des symmetrischen RSS-Schlüssels des primären Knotens mit dem sekundären Knoten für die statusbehaftete Synchronisierung einer großen Anzahl von LSN-Zuordnungen und -Sitzungen.
    * Binden des Subnetzes der LSN-IP-Adressen an ein VLAN, um Überschwemmungen von GARP-Broadcasts auf allen VLANs nach einem Failover zu vermeiden.
  - Bei einer Hochverfügbarkeitsbereitstellung von Citrix ADC Appliances werden ALG-bezogene Sitzungen nicht auf die sekundäre Appliance gespiegelt.
- **Application Layer Gateways (ALGs)**: Im Folgenden werden die Überlegungspunkte für ALGs auf einer Citrix ADC Appliance aufgeführt:
  - Folgende werden für SIP ALG nicht unterstützt:
    * Multicast-IP-Adressen
    * Verschlüsseltes SDP
    * SIP-Nachrichten über TLS
    * FQDN-Übersetzung in SIP-Nachrichten
    * Authentifizierung von SIP-Nachrichten
    * Verkehrsdomänen, Adminpartitionen und Citrix ADC-Cluster.
    * SIP-Nachrichten mit mehrteiligen Körpern.
  - Folgende werden für RTSP ALG nicht unterstützt:

        * Multicast-RTSP-Sitzungen
        * RTSP-Sitzung über UDP
        * Citrix ADC Datenverkehrsdomänen, Adminpartitionen und Citrix ADC-Cluster
    - Die Citrix ADC Appliance unterstützt ALG für das IPsec-Protokoll nicht.
- Wenn Sie die LSN-Funktion deaktivieren, wenn einige LSN-Sitzungen auf der Citrix ADC Appliance vorhanden sind, bestehen diese Sitzungen für die Dauer des konfigurierten Zeitüberschreitungsintervalls.
- LSN hat Vorrang vor RNAT. Wenn ein Paket von einem angegebenen LSN-Abonnenten auch mit einer RNAT Regel übereinstimmt, wird das Paket gemäß der LSN-Konfiguration übersetzt.
- Die Weiterleitung von Paketen, die sich nur auf die LSN-Sitzungen beziehen, basiert auf der Routingtabelle der Citrix ADC Appliance.
- Anders als bei Subnetz-IP-Adressen basiert die Auswahl einer LSN-NAT-IP-Adresse für die Verbindung eines Teilnehmers nicht auf dem Routingeintrag für die Ziel-IP-Adresse.
- Bei eingehenden Paketen haben statische LSN-Zuordnungen Vorrang vor dynamischen LSN-Zuordnungen.
- Bei ausgehenden Paketen haben LSN-Anwendungsprofile Vorrang vor statischer Zuordnung.
- Wenn eine große Anzahl von LSN-Sitzungen (> 1 Million) auf der Citrix ADC Appliance vorhanden ist, empfiehlt Citrix, anstelle von allen ausgewählten LSN-Sitzungen anzuzeigen. Verwenden Sie in der Befehlszeilenschnittstelle oder im Konfigurationsdienstprogramm die Auswahlparameter zum Anzeigen des LSN-Sitzungsvorgangs.
- Um den aktiven Arbeitsspeicher zu reduzieren, der der LSN-Funktion zugewiesen ist, müssen Sie die Citrix ADC Appliance nach dem Ändern der Einstellung für den konfigurierten Arbeitsspeicher neu starten. Ohne einen warmen Neustart können Sie nur die Menge des aktiven Speichers erhöhen.

Konfigurationsschritte für LSN

October 5, 2021

Die Konfiguration von LSN auf einer Citrix ADC Appliance umfasst die folgenden Aufgaben:

1. **Legen Sie die globalen LSN-Parameter fest.** Globale Parameter umfassen die Menge an Citrix ADC-Arbeitsspeicher, der für die LSN-Funktion reserviert ist, und die Synchronisierung von LSN-Sitzungen in einem Hochverfügbarkeitssetup.
2. **Erstellen Sie eine LSN-Client-Entität und binden Sie Abonnenten daran.** Eine LSN-Client-Entität ist eine Gruppe von Abonnenten, für deren Datenverkehr die Citrix ADC Appliance LSN ausführen soll. Die Client-Entität enthält IPv4-Adressen und erweiterte ACL-Regeln zur Identifizierung von Abonnenten. Ein LSN-Client kann nur an eine LSN-Gruppe gebunden werden. Die Befehlszeilenschnittstelle verfügt über zwei Befehle zum Erstellen einer LSN-Client-Entität und

zum Binden eines Abonnenten an die LSN-Client-Entität. Das Konfigurationsdienstprogramm kombiniert diese beiden Vorgänge auf einem einzigen Bildschirm.

3. **Erstellen Sie einen LSN-Pool und binden Sie NAT-IP-Adressen an ihn.** Ein LSN-Pool definiert einen Pool von NAT-IP-Adressen, der von der Citrix ADC Appliance zum Ausführen von LSN verwendet wird. Dem Pool werden Parameter zugewiesen, z. B. Portblockzuweisung und NAT-Typ (deterministisch oder dynamisch). Ein an eine LSN-Gruppe gebundener LSN-Pool gilt für alle Abonnenten einer LSN-Client-Entität, die an dieselbe Gruppe gebunden ist. Nur LSN-Pools und LSN-Gruppen mit denselben NAT-Typeinstellungen können miteinander verbunden werden. Mehrere LSN-Pools können an eine LSN-Gruppe gebunden werden. Für Dynamic NAT kann ein LSN-Pool an mehrere LSN-Gruppen gebunden werden. Für deterministische NAT können Pools, die an eine LSN-Gruppe gebunden sind, nicht an andere LSN-Gruppen gebunden werden. Die Befehlszeilenschnittstelle verfügt über zwei Befehle zum Erstellen eines LSN-Pools und zum Binden von NAT-IP-Adressen an den LSN-Pool. Das Konfigurationsdienstprogramm kombiniert diese beiden Vorgänge auf einem einzigen Bildschirm.
4. **(Optional) Erstellen Sie ein LSN-Transportprofil für ein bestimmtes Protokoll.** Ein LSN-Transportprofil definiert verschiedene Timeouts und Limits, z. B. maximale LSN-Sitzungen und maximale Port-Auslastung, die ein Teilnehmer für ein bestimmtes Protokoll haben kann. Sie binden ein LSN-Transportprofil für jedes Protokoll (TCP, UDP und ICMP) an eine LSN-Gruppe. Ein Profil kann an mehrere LSN-Gruppen gebunden werden. Ein an eine LSN-Gruppe gebundenes Profil gilt für alle Abonnenten eines LSN-Clients, der an dieselbe Gruppe gebunden ist. Standardmäßig ist ein LSN-Transportprofil mit Standardeinstellungen für TCP-, UDP- und ICMP-Protokolle während der Erstellung an eine LSN-Gruppe gebunden. Dieses Profil wird als Standardtransportprofil bezeichnet. Ein LSN-Transportprofil, das Sie an eine LSN-Gruppe binden, überschreibt das standardmäßige LSN-Transportprofil für dieses Protokoll.
5. **(Optional) Erstellen Sie ein LSN-Anwendungsprofil für ein bestimmtes Protokoll und binden Sie eine Reihe von Zielports daran.** Ein LSN-Anwendungsprofil definiert die LSN-Zuordnungs- und LSN-Filtersteuerelemente einer Gruppe für ein bestimmtes Protokoll und für eine Gruppe von Zielports. Für eine Gruppe von Zielports binden Sie ein LSN-Profil für jedes Protokoll (TCP, UDP und ICMP) an eine LSN-Gruppe. Ein Profil kann an mehrere LSN-Gruppen gebunden werden. Ein LSN-Anwendungsprofil, das an eine LSN-Gruppe gebunden ist, gilt für alle Abonnenten eines LSN-Clients, der an dieselbe Gruppe gebunden ist. Standardmäßig ist ein LSN-Anwendungsprofil mit Standardeinstellungen für TCP-, UDP- und ICMP-Protokolle für alle Zielports während der Erstellung an eine LSN-Gruppe gebunden. Dieses Profil wird als Standardanwendungsprofil bezeichnet. Wenn Sie ein LSN-Anwendungsprofil mit einem bestimmten Satz von Zielports an eine LSN-Gruppe binden, überschreibt das gebundene Profil das standardmäßige LSN-Anwendungsprofil für dieses Protokoll an dieser Gruppe von Zielports. Die Befehlszeilenschnittstelle verfügt über zwei Befehle zum Erstellen eines LSN-Anwendungsprofils und zum Binden eines Satzes von Zielports an das LSN-Anwendungsprofil. Das Konfigurationsdienstprogramm kombiniert diese beiden Vorgänge auf einem einzigen

Bildschirm.

6. **Erstellen Sie eine LSN-Gruppe und binden Sie LSN-Pools, (optional) LSN-Transportprofile und (optional) LSN-Anwendungsprofile an die LSN-Gruppe.** Eine LSN-Gruppe ist eine Entität, die aus einem LSN-Client, LSN-Pool, LSN-Transportprofilen und LSN-Anwendungsprofilen besteht. B. Port-Blockgröße und Protokollierung von LSN-Sitzungen. Die Parametereinstellungen gelten für alle Abonnenten eines LSN-Clients, der an die LSN-Gruppe gebunden ist. Nur LSN-Pools und LSN-Gruppen mit denselben NAT-Typeinstellungen können miteinander verbunden werden. Mehrere LSN-Pools können an eine LSN-Gruppe gebunden werden. Für Dynamic NAT kann ein LSN-Pool an mehrere LSN-Gruppen gebunden werden. Für deterministische NAT können Pools, die an eine LSN-Gruppe gebunden sind, nicht an andere LSN-Gruppen gebunden werden. Nur eine LSN-Client-Entität kann an eine LSN-Gruppe gebunden werden, und eine LSN-Client-Entität, die an eine LSN-Gruppe gebunden ist, kann nicht an andere LSN-Gruppen gebunden werden. Die Befehlszeilenschnittstelle verfügt über zwei Befehle zum Erstellen einer LSN-Gruppe und zum Binden von LSN-Pools, LSN-Transportprofilen, LSN-Anwendungsprofilen an die LSN-Gruppe. Das Konfigurationsdienstprogramm kombiniert diese beiden Vorgänge in einem einzigen Bildschirm.

In der folgenden Tabelle sind die maximale Anzahl verschiedener LSN-Entitäten und Bindungen aufgeführt, die auf einer Citrix ADC Appliance erstellt werden können. Diese Grenzwerte unterliegen auch dem Speicher, der auf der Citrix ADC Appliance verfügbar ist.

LSN-Entitäten und Bindungen	Limit
LSN-Clients	1024
LSN-Pools	128
LSN-Gruppen	1024
Abonnentennetzwerke, die an einen LSN-Client gebunden werden können	64
Erweiterte ACLs, die an einen LSN-Client gebunden werden können	1024
NAT-IP-Adressen in einem Pool	4096
LSN-Pools, die an eine LSN-Gruppe gebunden werden können	8
LSN-Gruppen, die denselben LSN-Pool verwenden können	16
LSN-Transportprofile, die an eine LSN-Gruppe gebunden werden können	3 (jeweils eine für TCP, UDP und ICMP Protokolle)

LSN-Entitäten und Bindungen	Limit
LSN-Gruppen, die dasselbe LSN-Transportprofil verwenden können	8
LSN-Anwendungsprofile, die an eine LSN-Gruppe gebunden werden können	64
LSN-Gruppen, die dasselbe LSN-Anwendungsprofil verwenden können	8
Portbereiche, die an ein LSN-Anwendungsprofil gebunden werden können	8

Konfiguration über die Befehlszeilenschnittstelle

So erstellen Sie einen LSN-Client mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn client <clientname>

show lsn client
<!--NeedCopy-->
```

So binden Sie eine Netzwerkadresse oder eine ACL-Regel über die Befehlszeilenschnittstelle an einen LSN-Client

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn client <clientname> ((-network <ip_addr> [-netmask <netmask>]
    [-td<positive_integer>]) | -aclname <string>)

show lsn client
<!--NeedCopy-->
```

So erstellen Sie einen LSN-Pool mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add lsn pool <poolname> [-nattype ( DYNAMIC | DETERMINISTIC )] [-
    portblockallocation ( ENABLED | DISABLED )] [-portrealloctimeout <
    secs>] [-maxPortReallocTmq <positive_integer>]

show lsn pool
<!--NeedCopy-->
```

So binden Sie einen IP-Adressbereich mit der Befehlszeilenschnittstelle an einen LSN-Pool

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn pool <poolname> <lsnip>

show lsn pool
<!--NeedCopy-->
```

Hinweis: Um LSN-IP-Adressen aus einem LSN-Pool zu entfernen, verwenden Sie den Befehl unbind lsn pool.

So erstellen Sie ein LSN-Transportprofil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn transportprofile <transportprofilename> <transportprotocol> [-
    sessiontimeout <secs>] [-finrsttimeout <secs>] [-portquota <
    positive_integer>] [-sessionquota <positive_integer>] [-
    portpreserveparity ( ENABLED | DISABLED )] [-portpreserverange (
    ENABLED | DISABLED )] [-syncheck ( ENABLED | DISABLED )]

show lsn transportprofile
<!--NeedCopy-->
```

So erstellen Sie ein LSN-Anwendungsprofil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add lsn appsprofile <appsprofilename> <transportprotocol> [-ippooling (
    PAIRED | RANDOM )] [-mapping <mapping>] [-filtering <filtering>][-
    tcpproxy ( ENABLED | DISABLED )] [-td <positive_integer>]

show lsn appsprofile
<!--NeedCopy-->
```

So binden Sie einen Anwendungsprotokollportbereich mit der Befehlszeilenschnittstelle an ein LSN-Anwendungsprofil

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn appsprofile <appsprofilename> <lsnport>

show lsn appsprofile
<!--NeedCopy-->
```

So erstellen Sie eine LSN-Gruppe mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn group <groupname> -clientname <string> [-nattype ( DYNAMIC |
    DETERMINISTIC )] [-portblocksize <positive_integer>] [-logging (
    ENABLED | DISABLED )] [-sessionLogging ( ENABLED | DISABLED )][-
    sessionSync (ENABLED | DISABLED )] [-snmptraplimit <positive_integer
    >] [-ftp ( ENABLED | DISABLED )]

show lsn group
<!--NeedCopy-->
```

So binden Sie LSN-Profile und LSN-Pools mit der Befehlszeilenschnittstelle an eine LSN-Gruppe

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn group <groupname> (-poolname <string> | -transportprofilename
    <string> | -appsprofilename <string>)

```



```
show lsn group
<!--NeedCopy-->
```

Konfiguration mit dem Konfigurationsdienstprogramm

So konfigurieren Sie einen LSN-Client und binden eine IPv4-Netzwerkadresse oder eine ACL-Regel mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **System** > **Large Scale NAT** > **Clients**, fügen Sie einen Client hinzu, und binden Sie dann eine IPv4-Netzwerkadresse oder eine ACL-Regel an den Client.

So konfigurieren Sie einen LSN-Pool und binden NAT-IP-Adressen mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **System > Large Scale NAT** > **Pools**, fügen Sie einen Pool hinzu und binden Sie dann eine NAT-IP-Adresse oder einen Bereich von NAT-IP-Adressen an den Pool.

So konfigurieren Sie ein LSN-Transportprofil mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **System > Large scale NAT > Profile**.
2. Klicken Sie im Detailbereich auf Registerkarte **Transport**, und fügen Sie dann ein Transportprofil hinzu.

So konfigurieren Sie ein LSN-Anwendungsprofil mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **System > Large scale NAT > Profile**.
2. Klicken Sie im Detailbereich auf Registerkarte **Anwendung**, und fügen Sie dann ein Anwendungsprofil hinzu.

So konfigurieren Sie eine LSN-Gruppe und binden einen LSN-Client, Pools, Transportprofile und Anwendungsprofile mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **System > Large Scale NAT > Groups**, fügen Sie eine Gruppe hinzu, und binden Sie dann einen LSN-Client, Pools, Transportprofile und Anwendungsprofile an die Gruppe.

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- add lsn client
  - clientname

    Name für die LSN-Client-Entität. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem der LSN-Client erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält,

setzen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. lsn client1" oder lsn client1").

Dies ist ein obligatorisches Argument. Maximale Länge: 127

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- bind lsn client
  - clientname

    Name für die LSN-Client-Entität. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem der LSN-Client erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. lsn client1" oder lsn client1").

    Dies ist ein obligatorisches Argument. Maximale Länge: 127
  - Netzwerk

    IPv4-Adressen der LSN-Abonnenten oder Teilnehmernetzwerke, auf deren Datenverkehr die Citrix ADC Appliance Large Scale NAT ausführen soll.
  - Netzmaske

    Subnetzmaske für die im Parameter Network angegebene IPv4-Adresse.

    Standardwert: 255.255.255.255
  - td

    ID der Verkehrsdomäne, zu der dieser Teilnehmer oder das Teilnehmernetzwerk gehört (wie durch den Netzwerkparameter angegeben).

    Wenn Sie keine ID angeben, wird der Abonnent oder das Teilnehmernetzwerk Teil der Standardverkehrsdomäne.

    Standardwert: 0

    Mindestwert: 0

    maximaler Wert: 4094
  - aclname

    Name (n) aller konfigurierten erweiterten ACL (s), deren Aktion Allow lautet. Die in der erweiterten ACL-Regel angegebene Bedingung identifiziert den Datenverkehr von einem

LSN-Abonnenten, für den die Citrix ADC Appliance große NAT ausführen soll. Maximale Länge: 127

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- add lsn pool
  - poolname

    Name für den LSN-Pool. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem der LSN-Pool erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. lsn pool1" oder lsn pool1").

    Dies ist ein obligatorisches Argument. Maximale Länge: 127

  - nattype

    Art der NAT-IP-Adresse und Portzuweisung (aus den LSN-Pools, die an eine LSN-Gruppe gebunden sind) für Abonnenten (der LSN-Client-Entität, die an die LSN-Gruppe gebunden ist):

    Die verfügbaren Optionen funktionieren wie folgt:

    * **Deterministic** — Weisen Sie jedem Abonnenten (des LSN-Clients, der an die LSN-Gruppe gebunden ist) eine NAT-IP-Adresse und einen Port zu. Die Citrix ADC Appliance weist diesen Abonnenten nacheinander NAT-Ressourcen zu. Die Citrix ADC Appliance weist der Anfangsadresse des Abonnenten den ersten Ports (Blockgröße, die durch den Parameter für die Portblockgröße der LSN-Gruppe bestimmt wird) der ersten NAT-IP-Adresse zu. Der nächste Bereich von Ports wird dem nächsten Abonnenten zugewiesen usw., bis die NAT-Adresse nicht über genügend Ports für den nächsten Abonnenten verfügt. In diesem Fall wird der erste Portblock auf der nächsten NAT-Adresse für den Abonnenten verwendet usw. Da jeder Abonnent nun eine deterministische NAT-IP-Adresse und einen Block von Ports erhält, kann ein Abonnent ohne Protokollierung identifiziert werden. Bei einer Verbindung kann ein Teilnehmer nur anhand der NAT-IP-Adresse und -Port sowie der Ziel-IP-Adresse und -Port identifiziert werden.

    * **Dynamisch**—Weisen Sie eine zufällige NAT-IP-Adresse und einen Port aus dem LSN-NAT-Pool für eine Teilnehmerverbindung zu. Wenn die Portblockzuweisung aktiviert ist (im LSN-Pool) und eine Portblockgröße angegeben ist (in der LSN-Gruppe), weist die Citrix ADC Appliance eine zufällige NAT-IP-Adresse und einen Port-Block für einen

Abonnenten zu, wenn eine Verbindung zum ersten Mal initiiert wird. Die Appliance weist diese NAT-IP-Adresse und einen Port (aus dem zugewiesenen Block von Ports) für verschiedene Verbindungen von diesem Teilnehmer zu. Wenn alle Ports (für verschiedene Abonnentenverbindungen) vom zugewiesenen Portblock der Abonnenten zugewiesen sind, weist die Appliance dem Abonnenten einen neuen zufälligen Portblock zu. Nur LSN-Pools und LSN-Gruppen mit denselben NAT-Typeinstellungen können miteinander verbunden werden. Mehrere LSN-Pools können an eine LSN-Gruppe gebunden werden.

Mögliche Werte: DYNAMIC, DETERMINISTIC

Standardwert: DYNAMIC

- portblockallocation

  Weisen Sie jedem Abonnenten einen zufälligen NAT-Portblock aus dem verfügbaren NAT-Port-Pool einer NAT-IP-Adresse zu, wenn die NAT-Zuweisung als Dynamische NAT-Adresse festgelegt ist. Für jede Verbindung, die von einem Abonnenten initiiert wird, weist die Citrix ADC Appliance einen NAT-Port von den Abonnenten, die NAT-Port zugewiesen haben, um die LSN-Sitzung zu erstellen.

  Sie müssen die Portblockgröße in der gebundenen LSN-Gruppe festlegen. Wenn für einen Abonnenten alle Ports vom zugewiesenen Portblock des Abonnenten zugewiesen sind, weist die Citrix ADC Appliance dem Abonnenten einen neuen zufälligen Portblock zu.

  Für Deterministic NAT ist dieser Parameter standardmäßig aktiviert und kann nicht deaktiviert werden.

  Mögliche Werte: ENABLED, DISABLED

  Standardwert: DISABLED

- portrealloctimeout

  Die Wartezeit in Sekunden zwischen dem Freigeben der LSN-NAT-Ports (wenn eine LSN-Zuordnung entfernt wird) und der Neuzuweisung für eine neue LSN-Sitzung. Dieser Parameter ist notwendig, um Kollisionen zwischen alten und neuen Zuordnungen und Sitzungen zu vermeiden. Es stellt sicher, dass alle etablierten Sitzungen unterbrochen werden, anstatt an einen anderen Abonnenten umgeleitet zu werden. Dies gilt nicht für Ports, in:

  * Deterministische NAT
  * Adressenabhängige Filterung und Adressen-Port-abhängige Filterung
  * Dynamisches NAT mit Port-Block-Zuweisung

  In diesen Fällen werden Ports sofort neu zugestellt.

  Standardwert: 0

  Maximalwert: 600

- maxPortReallocTmq

  Maximale Anzahl von Ports, für die das Timeout für die Port-Neuzuweisung für jede NAT-IP-Adresse gilt. Mit anderen Worten, die maximale Queue-Größe für freigegebene Port-Warteschlangen, für die das Neuzuteilungs-Timeout für jede NAT-IP-Adresse gilt.

  Wenn die Warteschlangengröße voll ist, wird der nächste Port freigegeben sofort für eine neue LSN-Sitzung neu zugewiesen.

  Standardwert: 65536

  Maximalwert: 65536

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- bind lsn pool
  - poolname

    Name für den LSN-Pool. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem der LSN-Pool erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. lsn pool1" oder lsn pool1").

    Dies ist ein obligatorisches Argument. Maximale Länge: 127

  - lsnip

    IPv4-Adresse oder ein Bereich von IPv4-Adressen, die als NAT-IP-Adresse (n) für LSN verwendet werden sollen.

    Nachdem der Pool erstellt wurde, werden diese IPv4-Adressen der Citrix ADC Appliance als IP-Adresse des Typs LSN hinzugefügt. Eine LSN-IP-Adresse, die einem LSN-Pool zugeordnet ist, kann nicht mit anderen LSN-Pools freigegeben werden. Für diesen Parameter angegebene IP-Adressen dürfen auf der Citrix ADC Appliance nicht bereits als IP-Adressen im Besitz von Citrix ADC vorhanden sein. Trennen Sie den Bereich in der Befehlszeilenschnittstelle durch einen Bindestrich. Beispiel: 10.102.29.30-10.102.29.189. Sie können später einige oder alle LSN-IP-Adressen aus dem Pool entfernen und dem LSN-Pool IP-Adressen hinzufügen.

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- füge lsn transportprofile hinzu

- transportprofilename

  Name für das LSN-Transportprofil. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem das LSN-Transportprofil erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “lsn transport profile1” oder ‘lsn transport profile1’).

  Dies ist ein obligatorisches Argument. Maximale Länge: 127

- transportprotocol

  Protokoll, für das die LSN-Transportprofilparameter festgelegt werden sollen.

  Dies ist ein obligatorisches Argument.

  Mögliche Werte: TCP, UDP, ICMP

- sessiontimeout

  Zeitüberschreitung (in Sekunden) für eine leidende LSN-Sitzung. Wenn eine LSN-Sitzung für einen Zeitraum im Leerlauf ist, der diesen Wert überschreitet, entfernt die Citrix ADC Appliance die Sitzung.

  Dieses Timeout gilt nicht für eine TCP-LSN-Sitzung, wenn eine FIN- oder RST-Nachricht von einem der Endpunkte empfangen wird.

  Standardwert: 120

  Mindestwert: 60

- finrsttimeout

  Zeitüberschreitung in Sekunden für eine TCP-LSN-Sitzung, nachdem eine FIN- oder RST-Nachricht von einem der Endpunkte empfangen wurde.

  Wenn eine TCP-LSN-Sitzung im Leerlauf ist (nachdem die Citrix ADC Appliance eine FIN- oder RST-Nachricht empfängt) für einen Zeitraum, der diesen Wert überschreitet, entfernt die Citrix ADC-Appliance die Sitzung.

  Da die LSN-Funktion der Citrix ADC Appliance keine Statusinformationen über TCP-LSN-Sitzungen enthält, werden in diesem Timeout die Übertragung von FIN oder RST sowie ACK-Nachrichten vom anderen Endpunkt unterstützt, sodass beide Endpunkte die Verbindung ordnungsgemäß schließen können.

  Standardwert: 30

- portquota

Maximale Anzahl der LSN-NAT-Ports, die jeweils von jedem Abonnenten für das angegebene Protokoll verwendet werden. Beispielsweise kann jeder Abonnent auf maximal 500 TCP-NAT-Ports beschränkt werden. Wenn die LSN-NAT-Zuordnungen für einen Abonnenten das Limit erreichen, weist die Citrix ADC Appliance diesem Abonnenten keine zusätzlichen NAT-Ports zu.

Standardwert: 0

Mindestwert: 0

Maximalwert: 65535

- sessionquota

  Maximale Anzahl gleichzeitiger LSN-Sitzungen, die für jeden Abonnenten für das angegebene Protokoll zulässig sind. Wenn die Anzahl der LSN-Sitzungen das Limit für einen Abonnenten erreicht, erlaubt die Citrix ADC Appliance dem Abonnenten nicht, zusätzliche Sitzungen zu öffnen.

  Standardwert: 0

  Mindestwert: 0

  Maximalwert: 65535

- portpreserveparity

  Aktivieren Sie die Port-Parität zwischen einem Teilnehmeranschluss und dem zugeordneten LSN-NAT-Port. Wenn ein Teilnehmer beispielsweise eine Verbindung von einem ungeraden nummerierten Port initiiert, weist die Citrix ADC Appliance für diese Verbindung einen ungeraden nummerierten LSN-NAT-Port zu. Sie müssen diesen Parameter für das ordnungsgemäße Funktionieren von Protokollen festlegen, bei denen der Quellport gerade oder ungerade nummeriert sein muss, z. B. in Peer-to-Peer-Anwendungen, die RTP- oder RTCP-Protokoll verwenden.

  Mögliche Werte: ENABLED, DISABLED

  Standardwert: DISABLED

- portpreserverange

  Wenn ein Teilnehmer eine Verbindung von einem bekannten Port (0-1023) initiiert, weisen Sie für diese Verbindung einen NAT-Port aus dem bekannten Portbereich (0-1023) zu. Wenn ein Teilnehmer beispielsweise eine Verbindung von Port 80 initiiert, kann die Citrix ADC Appliance Port 100 als NAT-Port für diese Verbindung zuweisen.

  Dieser Parameter gilt für dynamische NAT ohne Portblockzuweisung. Sie gilt auch für deterministische NAT, wenn der zugewiesene Bereich der Ports bekannte Ports umfasst.

Wenn alle bekannten Ports aller verfügbaren NAT-IP-Adressen in verschiedenen Teilnehmerverbindungen (LSN-Sitzungen) verwendet werden und ein Teilnehmer eine Verbindung von einem bekannten Port initiiert, wird diese Verbindung von der Citrix ADC Appliance gelöscht.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

- syncheck

  Löschen Sie alle Nicht-SYN-Pakete für Verbindungen, für die keine LSN-NAT-Sitzung auf der Citrix ADC Appliance vorhanden ist.

  Wenn Sie diesen Parameter deaktivieren, akzeptiert die Citrix ADC Appliance alle Nicht-SYN-Pakete und erstellt einen neuen LSN-Sitzungseintrag für diese Verbindung.

  Im Folgenden finden Sie einige Gründe für die Citrix ADC Appliance, solche Pakete zu empfangen:

  * LSN-Sitzung für eine Verbindung existierte, aber die Citrix ADC Appliance entfernte diese Sitzung, da die LSN-Sitzung für eine Zeit im Leerlauf war, die das konfigurierte Sitzungszeitlimit überschritten hat.
  * Solche Pakete können Teil eines DoS-Angriffs sein.

  Mögliche Werte: ENABLED, DISABLED

  Standardwert: ENABLED

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- add lsn appsprofile
  - appsprofilename

    Name für das LSN-Anwendungsprofil. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem das LSN-Anwendungsprofil erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “lsn application profile1” oder ‘lsn application profile1’).

    Dies ist ein obligatorisches Argument. Maximale Länge: 127

  - transportprotocol

    Name des Protokolls, für das die Parameter dieses LSN-Anwendungsprofils gelten.

Dies ist ein obligatorisches Argument.

Mögliche Werte: TCP, UDP, ICMP

- ippooling

  NAT-IP-Adresszuweisungsoptionen für Sitzungen, die mit demselben Abonnenten verknüpft sind.

  Die verfügbaren Optionen funktionieren wie folgt:

  * **Paired**— Die Citrix ADC Appliance weist für alle Sitzungen dieselbe NAT-IP-Adresse zu, die mit demselben Abonnenten verknüpft sind. Wenn alle Ports einer NAT-IP-Adresse in LSN-Sitzungen (für gleiche oder mehrere Abonnenten) verwendet werden, löscht die Citrix ADC Appliance jede neue Verbindung vom Abonnenten.
  * **Random**— Die Citrix ADC Appliance weist zufällige NAT-IP-Adressen aus dem Pool für verschiedene Sitzungen zu, die demselben Teilnehmer zugeordnet sind.

  Dieser Parameter ist nur für die dynamische NAT-Zuweisung anwendbar.

  Mögliche Werte: PAIRED, RANDOM

  Standardwert: RANDOM

- mapping

  Typ der LSN-Zuordnung, die auf nachfolgende Pakete angewendet werden soll, die von derselben Teilnehmer-IP-Adresse und demselben Port stammen.

  Betrachten Sie ein Beispiel für eine LSN-Zuordnung, die die Zuordnung des Teilnehmers IP:Port (X: X), NAT IP:Port (N: N) und externer Host IP:Port (Y:Y) enthält.

  Die verfügbaren Optionen funktionieren wie folgt:

  * **ENDPOINT-INDEPENDENT**—Verwenden Sie die LSN-Zuordnung für nachfolgende Pakete, die von derselben Teilnehmer-IP-Adresse und demselben Port (x:x) an jede externe IP-Adresse und Port gesendet werden.
  * **ADDRESS-DEPENDENT**—Verwenden Sie die LSN-Zuordnung für nachfolgende Pakete, die von derselben Teilnehmer-IP-Adresse und demselben Port (x:x) an dieselbe externe IP-Adresse (Y) gesendet werden, unabhängig vom externen Port.
  * **ADDRESS-PORT-DEPENDENT**—Verwenden Sie die LSN-Zuordnung für nachfolgende Pakete, die von derselben internen IP-Adresse und demselben Port (x:x) an dieselbe externe IP-Adresse und denselben Port (Y:y) gesendet werden, während die Zuordnung noch aktiv ist.

  Mögliche Werte: ENDPOINT-INDEPENDENT, ADDRESS-DEPENDENT, ADDRESS-PORT-DEPENDENT

  Standardwert: ADDRESS-PORT-DEPENDENT

- filtering

  Filtertyp, der auf Pakete angewendet werden soll, die von externen Hosts stammen.

  Betrachten Sie ein Beispiel für eine LSN-Zuordnung, die die Zuordnung von Teilnehmer-IP:Port (X:x), NAT IP:Port (N:n) und externem Host IP:Port (Y:y) umfasst.

  Die verfügbaren Optionen funktionieren wie folgt:

  * **ENDPOINT INDEPENDENT**—Filtert nur Pakete aus, die nicht für die IP-Adresse des Teilnehmers und den Port X:x bestimmt sind, unabhängig von der IP-Adresse des externen Hosts und der Portquelle (z:z). Die Citrix ADC Appliance leitet alle Pakete, die für X:x bestimmt sind, weiter. Mit anderen Worten, das Senden von Paketen vom Abonnenten an eine externe IP-Adresse reicht aus, um Pakete von externen Hosts an den Abonnenten zuzulassen.
  * **ADDRESS DEPENDENT** - Filtert Pakete aus, die nicht für die IP-Adresse des Teilnehmers und Port X:x bestimmt sind. Darüber hinaus filtert die Appliance Pakete von Y:y aus, die für den Abonnenten bestimmt sind (x:x), wenn der Client zuvor keine Pakete an y:anyPort gesendet hat (externer Port unabhängig). Mit anderen Worten, das Empfangen von Paketen von einem bestimmten externen Host erfordert, dass der Abonnent zuerst Pakete an die IP-Adresse dieses bestimmten externen Hosts sendet.
  * **ADDRESS PORT DEPENDENT** (Standardeinstellung) — Filtert Pakete aus, die nicht für die IP-Adresse und den Port des Teilnehmers bestimmt sind (x:x). Darüber hinaus filtert die Citrix ADC Appliance Pakete von Y:y aus, die für den Abonnenten bestimmt sind (x:x), wenn der Abonnent zuvor keine Pakete an y:y gesendet hat. Mit anderen Worten, das Empfangen von Paketen von einem bestimmten externen Host erfordert, dass der Abonnent zuerst Pakete an diese externe IP-Adresse und Port sendet.

  Mögliche Werte: ENDPOINT-INDEPENDENT, ADDRESS-DEPENDENT, ADDRESS-PORT-DEPENDENT

  Standardwert: ADDRESS-PORT-DEPENDENT

- tcpproxy

  Aktivieren Sie den TCP-Proxy, mit dem die Citrix ADC Appliance den TCP-Datenverkehr mithilfe von Layer-4-Features optimieren kann.

  Mögliche Werte: ENABLED, DISABLED

  Standardwert: DISABLED

- td

  ID der Datenverkehrsdomäne, über die die Citrix ADC Appliance den ausgehenden Datenverkehr nach Durchführung von LSN sendet.

Wenn Sie keine ID angeben, sendet die Appliance den ausgehenden Datenverkehr über die Standardverkehrsdomäne mit der ID 0.

Standardwert: 65535

Maximalwert: 65535

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- bindet lsn appsprofile
  - appsprofilename

    Name für das LSN-Anwendungsprofil. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem das LSN-Anwendungsprofil erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “lsn application profile1” oder ‘lsn application profile1’).

    Dies ist ein obligatorisches Argument. Maximale Länge: 127

  - lsnport

    Portnummern oder Portnummern, die mit dem Zielport des eingehenden Pakets von einem Abonnenten übereinstimmen. Wenn der Zielport übereinstimmt, wird das LSN-Anwendungsprofil für die LSN-Sitzung angewendet. Trennen Sie einen Bereich von Ports durch einen Bindestrich. Zum Beispiel 40-90.

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- add lsn group
  - groupname

    Name für die LSN-Gruppe. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem die LSN-Gruppe erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “lsn group1” oder ‘lsn group1’).

    Dies ist ein obligatorisches Argument. Maximale Länge: 127

- clientname

  Name der LSN-Client-Entität, die der LSN-Gruppe zugeordnet werden soll. Sie können nur eine LSN-Client-Entität einer LSN-Gruppe zuordnen. Sie können diese Zuordnung nicht entfernen oder durch eine andere LSN-Client-Entität ersetzen, nachdem die LSN-Gruppe erstellt wurde.

  Dies ist ein obligatorisches Argument. Maximale Länge: 127

- nattype

  Art der NAT-IP-Adresse und Port-Zuweisung (aus den gebundenen LSN-Pools) für Teilnehmer:

  Die verfügbaren Optionen funktionieren wie folgt:

  * **Deterministic** — Weisen Sie jedem Abonnenten (des LSN-Clients, der an die LSN-Gruppe gebunden ist) eine NAT-IP-Adresse und einen Port zu. Die Citrix ADC Appliance weist diesen Abonnenten nacheinander NAT-Ressourcen zu. Die Citrix ADC Appliance weist der Anfangsadresse des Abonnenten den ersten Ports (Blockgröße, die durch den Parameter für die Portblockgröße der LSN-Gruppe bestimmt wird) der ersten NAT-IP-Adresse zu. Der nächste Bereich von Ports wird dem nächsten Abonnenten zugewiesen usw., bis die NAT-Adresse nicht über genügend Ports für den nächsten Abonnenten verfügt. In diesem Fall wird der erste Portblock auf der nächsten NAT-Adresse für den Abonnenten verwendet usw. Da jeder Abonnent nun eine deterministische NAT-IP-Adresse und einen Block von Ports erhält, kann ein Abonnent ohne Protokollierung identifiziert werden. Bei einer Verbindung kann ein Teilnehmer nur anhand der NAT-IP-Adresse und -Port sowie der Ziel-IP-Adresse und -Port identifiziert werden.
  * **Dynamisch**—Weisen Sie eine zufällige NAT-IP-Adresse und einen Port aus dem LSN-NAT-Pool für die Verbindung eines Teilnehmers zu. Wenn die Portblockzuweisung aktiviert ist (im LSN-Pool) und eine Portblockgröße angegeben ist (in der LSN-Gruppe), weist die Citrix ADC Appliance eine zufällige NAT-IP-Adresse und einen Port-Block für einen Abonnenten zu, wenn eine Verbindung zum ersten Mal initiiert wird. Die Appliance weist diese NAT-IP-Adresse und einen Port (aus dem zugewiesenen Block von Ports) für verschiedene Verbindungen von diesem Teilnehmer zu. Wenn alle Ports (für verschiedene Abonnentenverbindungen) vom zugewiesenen Portblock der Abonnenten zugewiesen sind, weist die Appliance dem Abonnenten einen neuen zufälligen Portblock zu.

  Mögliche Werte: DYNAMIC, DETERMINISTIC

  Standardwert: DYNAMIC

- portblocksize

Größe des NAT Portblocks, der für jeden Teilnehmer zugewiesen werden soll.

Um diesen Parameter für Dynamic NAT festzulegen, müssen Sie den Portblockzuweisungsparameter im gebundenen LSN-Pool aktivieren. Bei Deterministic NAT ist der Portblockzuweisungsparameter immer aktiviert und kann nicht deaktiviert werden.

In Dynamic NAT weist die Citrix ADC Appliance jedem Abonnenten einen zufälligen NAT-Portblock aus dem verfügbaren NAT-Port-Pool einer NAT-IP-Adresse zu. Wenn für einen Abonnenten alle Ports vom zugewiesenen Portblock des Abonnenten zugewiesen sind, weist die Appliance dem Abonnenten einen neuen zufälligen Portblock zu.

– logging

Protokollzuordnungseinträge und Sitzungen, die für diese LSN-Gruppe erstellt oder gelöscht wurden. Die Citrix ADC Appliance protokolliert LSN-Sitzungen für diese LSN-Gruppe nur, wenn Protokollierungs- und Sitzungsprotokollierungsparameter aktiviert sind.

Die Appliance verwendet ihr vorhandenes Syslog- und Überwachungsprotokoll-Framework, um LSN-Informationen zu protokollieren. Sie müssen die LSN-Protokollierung auf globaler Ebene aktivieren, indem Sie den LSN-Parameter in den zugehörigen NSLOG-Aktionsobjekten und SYLOG-Aktionsobjekten aktivieren. Wenn der Parameter Logging aktiviert ist, generiert die Citrix ADC Appliance Protokollmeldungen im Zusammenhang mit LSN-Zuordnungen und LSN-Sitzungen dieser LSN-Gruppe. Die Appliance sendet diese Protokollmeldungen dann an Server, die mit der NSLOG-Aktion und den SYSLOG-Aktions-Entitäten verknüpft sind.

Eine Protokollmeldung für einen LSN-Zuordnungseintrag besteht aus folgenden Informationen:

* NSIP-Adresse der Citrix ADC Appliance
* Zeitstempel
* Eintragstyp (MAPPING oder SESSION)
* Gibt an, ob der LSN-Zuordnungseintrag erstellt oder gelöscht wird
* IP-Adresse, Port und Traffic-Domänen-ID des Abonnenten
* NAT IP-Adresse und Port
* Protokollname
* Ziel-IP-Adresse, -Port und -Domänen-ID sind möglicherweise vorhanden, abhängig von den folgenden Bedingungen:
  · Ziel-IP-Adresse und -Port werden nicht für die endpoint-unabhängige Zuordnung protokolliert
  · Nur Ziel-IP-Adresse (und nicht Port) wird für die adressabhängige Zuordnung protokolliert

· Ziel-IP-Adresse und -Port werden für die Adress-Port-abhängige Zuordnung protokolliert

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

– sessionLogging

Protokollieren von Sitzungen, die für die LSN-Gruppe erstellt oder gelöscht wurden. Die Citrix ADC Appliance protokolliert LSN-Sitzungen für diese LSN-Gruppe nur, wenn Protokollierungs- und Sitzungsprotokollierungsparameter aktiviert sind.

Eine Protokollmeldung für eine LSN-Sitzung besteht aus folgenden Informationen:

* NSIP-Adresse der Citrix ADC Appliance
* Zeitstempel
* Eintragstyp (MAPPING oder SESSION)
* Gibt an, ob die LSN-Sitzung erstellt oder entfernt wird
* IP-Adresse, Port und Traffic-Domänen-ID des Abonnenten
* NAT IP-Adresse und Port
* Protokollname
* Ziel-IP-Adresse, -Port und -Domänen-ID des Datenverkehrs

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

– sessionSync

Synchronisieren Sie in einer Hochverfügbarkeitsbereitstellung Informationen aller LSN-Sitzungen in Bezug auf diese LSN-Gruppe mit dem sekundären Knoten. Nach einem Failover werden etablierte TCP-Verbindungen und UDP-Paketflüsse aktiv gehalten und auf dem sekundären Knoten (neuer primärer Knoten) fortgesetzt.

Damit diese Einstellung funktioniert, müssen Sie den globalen Sitzungssynchronisierungsparameter aktivieren.

Mögliche Werte: ENABLED, DISABLED

Standardwert: ENABLED

– snmptraplimit

Maximale Anzahl von SNMP-Trap-Nachrichten, die für die LSN-Gruppe in einer Minute generiert werden können.

Standardwert: 100

Mindestwert: 0

Maximalwert: 10000

- ftp

  Aktivieren Sie das Application Layer Gateway (ALG) für das FTP-Protokoll. Bei einigen Protokollen der Anwendungsschicht werden die IP-Adressen und Protokollportnummern normalerweise in der Paketnutzlast kommuniziert. Wenn sie als ALG fungiert, ändert die Appliance die Paketnutzlast, um sicherzustellen, dass das Protokoll weiterhin über LSN funktioniert.

  Hinweis: Die Citrix ADC Appliance enthält auch ALG für ICMP- und TFTP-Protokolle. ALG für das ICMP-Protokoll ist standardmäßig aktiviert, und es gibt keine Möglichkeit, es zu deaktivieren. ALG für das TFTP-Protokoll ist standardmäßig deaktiviert. ALG wird automatisch für eine LSN-Gruppe aktiviert, wenn Sie ein UDP-LSN-Anwendungsprofil mit endpunktunabhängiger Zuordnung, endpunktunabhängiger Filterung und Zielport als 69 (bekannter Port für TFTP) an die LSN-Gruppe binden.

  Mögliche Werte: ENABLED, DISABLED

  Standardwert: ENABLED

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- bind lsn group
  - groupname

    Name für die LSN-Gruppe. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem die LSN-Gruppe erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “lsn group1” oder ‘lsn group1’).

    Dies ist ein obligatorisches Argument. Maximale Länge: 127

  - poolname

    Name des LSN-Pools, der an die angegebene LSN-Gruppe gebunden werden soll. Nur LSN-Pools und LSN-Gruppen mit denselben NAT-Typeinstellungen können miteinander verbunden werden. Mehrere LSN-Pools können an eine LSN-Gruppe gebunden werden.

    Für deterministische NAT können Pools, die an eine LSN-Gruppe gebunden sind, nicht an andere LSN-Gruppen gebunden werden. Für Dynamic NAT können Pools, die an eine LSN-Gruppe gebunden sind, an mehrere LSN-Gruppen gebunden werden. Maximale Länge: 127

- transportprofilename

  Name des LSN-Transportprofils, das an die angegebene LSN-Gruppe gebunden werden soll. Binden Sie ein Profil für jedes Protokoll, für das Sie Einstellungen festlegen möchten.

  Standardmäßig ist ein LSN-Transportprofil mit Standardeinstellungen für TCP-, UDP- und ICMP-Protokolle während der Erstellung an eine LSN-Gruppe gebunden. Dieses Profil wird als Standardtransport bezeichnet.

  Ein LSN-Transportprofil, das Sie an eine LSN-Gruppe binden, überschreibt das standardmäßige LSN-Transportprofil für dieses Protokoll. Maximale Länge: 127

- appsprofilename

  Name des LSN-Anwendungsprofils, das an die angegebene LSN-Gruppe gebunden werden soll. Binden Sie für jede Gruppe von Zielports ein Profil für jedes Protokoll, für das Sie Einstellungen festlegen möchten.

  Standardmäßig ist ein LSN-Anwendungsprofil mit Standardeinstellungen für TCP-, UDP- und ICMP-Protokolle für alle Zielports während der Erstellung an eine LSN-Gruppe gebunden. Dieses Profil wird als Standardanwendungsprofil bezeichnet.

  Wenn Sie ein LSN-Anwendungsprofil mit einem bestimmten Satz von Zielports an eine LSN-Gruppe binden, überschreibt das gebundene Profil das standardmäßige LSN-Anwendungsprofil für dieses Protokoll an dieser Gruppe von Zielports. Maximale Länge: 127

Beispiel-LSN-Konfigurationen

October 5, 2021

Im Folgenden finden Sie Beispiele für die Konfiguration von LSN über die Befehlszeilenschnittstelle.

Erstellen Sie eine einfache LSN-Konfiguration mit einem einzelnen Teilnehmernetzwerk, einer einzelnen LSN-NAT-IP-Adresse und Standardeinstellungen:

```
1 add lsn client LSN-CLIENT-1
2
3 Done
4
5 bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0
6
7 Done
8
```



```
add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.3

Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1

Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1

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

Erstellen Sie eine LSN-Konfiguration mit einer erweiterten ACL zur Identifizierung von LSN-Abonnenten:

```
add ns acl LSN-ACL-2 ALLOW -srcIP 192.0.2.10-192.0.2.20

Done

apply acls

Done

add lsn client LSN-CLIENT-2

Done

bind lsn client LSN-CLIENT-2  - aclname LSN-ACL-2

Done

add lsn pool LSN-POOL-2

Done

bind lsn pool LSN-POOL-2 203.0.113.5-203.0.113.10

Done
```



```
24
25 add lsn group LSN-GROUP-2 -clientname LSN-CLIENT-2
26
27 Done
28
29 bind lsn group LSN-GROUP-2 -poolname LSN-POOL-2
30
31 Done
32 <!--NeedCopy-->
```

Erstellen Sie eine LSN-Konfiguration mit endpunktunabhängiger Zuordnung für HTTP-Protokoll (Port 80) und adressenport-abhängige Zuordnung für das SSH-Protokoll (Port 22). Beschränken Sie außerdem jeden Abonnenten auf maximal 1000 NAT-Ports für das TCP-Protokoll und 100 NAT-Ports für das UDP-Protokoll. Beschränken Sie jeden Abonnenten auf maximal 2000 gleichzeitige Sitzungen für das TCP-Protokoll. Beschränken Sie die Gruppe auf maximal 30000 gleichzeitige Sitzungen für das TCP-Protokoll:

```
1  add lsn client LSN-CLIENT-3
2
3  Done
4
5  bind lsn client LSN-CLIENT-3 -network 192.0.3.0 -netmask 255.255.255.0
6
7  Done
8
9  add lsn pool LSN-POOL-3
10
11 Done
12
13 bind lsn pool LSN-POOL-3 203.0.113.11
14
15 Done
16
17 add lsn group LSN-GROUP-3 -clientname LSN-CLIENT-3
18
19 Done
20
21 bind lsn group LSN-GROUP-3 -poolname LSN-POOL-3
22
23 Done
24
25 add lsn appsprofile LSN-APPS-HTTPPROFILE-3 TCP -mapping ENDPOINT-
       INDEPENDENT
```



```
26
27 Done
28
29 bind lsn appsprofile LSN-APPS-HTTPPROFILE-3 80
30
31 Done
32
33 bind lsn group LSN-GROUP-3 -applicationprofilename LSN-APPS-HTTPPROFILE
       -3
34
35 Done
36
37 add lsn appsprofile LSN-APPS-SSHPROFILE-3 TCP -mapping ADDRESS-PORT-
       DEPENDENT
38
39 Done
40
41 bind lsn appsprofile LSN-APPS-SSHPROFILE-3 22
42
43 Done
44
45 bind lsn group LSN-GROUP-3 -applicationprofilename LSN-APPS-SSHPROFILE
       -3
46
47 Done
48
49 add lsn transportprofile LSN-TRANS-PROFILE-TCP-3 TCP -portquota 1000 -
       sessionquota 2000 -groupSessionLimit 30000
50
51 Done
52
53 bind lsn group LSN-GROUP-3 -transportprofilename LSN-TRANS-PROFILE-TCP
       -3
54
55 Done
56
57 add lsn transportprofile LSN-TRANS-PROFILE-UDP-3 UDP -portquota 100
58
59 Done
60
61 bind lsn group LSN-GROUP-3 -transportprofilename LSN-TRANS-PROFILE-UDP
       -3
62
63 Done
64 <!--NeedCopy-->
```


Erstellen Sie eine LSN-Konfiguration für einen großen Satz von Abonnenten:

```
add lsn client LSN-CLIENT-4

Done

bind lsn client LSN-CLIENT-4 -network 192.0.4.0 -netmask 255.255.255.0

Done

bind lsn client LSN-CLIENT-4 -network 192.0.5.0 -netmask 255.255.255.0

Done

bind lsn client LSN-CLIENT-4 -network 192.0.6.0 -netmask 255.255.255.0

Done

bind lsn client LSN-CLIENT-4 -network 192.0.7.0 -netmask 255.255.255.0

Done

bind lsn client LSN-CLIENT-4 -network 192.0.8.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-4

Done

bind lsn pool LSN-POOL-4 203.0.113.30-203.0.113.40

Done

bind lsn pool LSN-POOL-4 203.0.113.45-203.0.113.50

Done

bind lsn pool LSN-POOL-4 203.0.113.55-203.0.113.60

Done

```



```
41 add lsn group LSN-GROUP-4 -clientname LSN-CLIENT-4
42
43 Done
44
45 bind lsn group LSN-GROUP-4 -poolname LSN-POOL-4
46
47 Done
48
49 add lsn appsprofile LSN-APPS-WELLKNOWNPROFILE-4 TCP -mapping ENDPOINT-
      INDEPENDENT
50
51 Done
52
53 bind lsn appsprofile LSN-APPS-WELLKNOWN-PORTS-PROFILE-4 1- 1023
54
55 Done
56
57 bind lsn group LSN-GROUP-4 -applicationprofilename LSN-APPS-WELLKNOWN-
      PORTS-PROFILE-4
58
59 Done
60 <!--NeedCopy-->
```

Erstellen Sie eine LSN-Konfiguration mit Freigabe von NAT-Ressourcen für mehrere LSN-Gruppen. In diesem Beispiel wird LSN-Pool LSN-POOL-5 für die LSN-Gruppen LSN-GROUP-5 und LSN-GROUP-6 freigegeben:

```
1  add lsn client LSN-CLIENT-5
2
3  Done
4
5  bind lsn client LSN-CLIENT-5 -network 192.0.15.0 -netmask 255.255.255.0
6
7  Done
8
9  add lsn pool LSN-POOL-5
10
11 Done
12
13 bind lsn pool LSN-POOL-5 203.0.113.12-203.0.113.14
14
15 Done
16
```



```
add lsn group LSN-GROUP-5 -clientname LSN-CLIENT-5

Done

bind lsn group LSN-GROUP-5 -poolname LSN-POOL-5

Done

add lsn client LSN-CLIENT-6

Done

bind lsn client LSN-CLIENT-6 -network 192.0.16.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-6

Done

bind lsn pool LSN-POOL-6 203.0.113.15-203.0.113.18

Done

add lsn group LSN-GROUP-6 -clientname LSN-CLIENT-6

Done

bind lsn group LSN-GROUP-6 -poolname LSN-POOL-6

Done

bind lsn group LSN-GROUP-6 -poolname LSN-POOL-5

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

Erstellen Sie eine LSN-Konfiguration mit deterministischer NAT-Ressourcenzuweisung:

```
add lsn client LSN-CLIENT-7

Done

```



```
bind lsn client LSN-CLIENT-7 -network 192.0.17.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-7 -nattype DETERMINISTIC

Done

bind lsn pool LSN-POOL-7 203.0.113.19-203.0.113.23

Done

add lsn group LSN-GROUP-7 -clientname LSN-CLIENT-7 -nattype
   DETERMINISTIC -portblocksize 1024

Done

bind lsn group LSN-GROUP-7 -poolname LSN-POOL-7

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

Erstellen Sie eine LSN-Konfiguration mit mehreren Teilnehmernetzen, die dieselbe Netzwerkadresse haben, aber jedes Netzwerk, das zu einer anderen Verkehrsdomäne gehört. Beschränken Sie außerdem den ausgehenden Datenverkehr im Zusammenhang mit dem HTTP-Protokoll (Port 80) und senden Sie ihn über eine bestimmte Datenverkehrsdomäne (td 5):

```
add lsn client LSN-CLIENT-8

Done

bind lsn client LSN-CLIENT-8 -network 192.0.18.0 -netmask 255.255.255.0
    -td 1

Done

bind lsn client LSN-CLIENT-8 -network 192.0.18.0 -netmask 255.255.255.0
    -td 2

Done

bind lsn client LSN-CLIENT-8 -network 192.0.18.0 -netmask 255.255.255.0
    -td 3
```



```
14
15 Done
16
17 add lsn pool LSN-POOL-8
18
19 Done
20
21 bind lsn pool LSN-POOL-8 203.0.113.80-203.0.113.86
22
23 Done
24
25 add lsn group LSN-GROUP-8 -clientname LSN-CLIENT-8
26
27 Done
28
29 bind lsn group LSN-GROUP-8 -poolname LSN-POOL-8
30
31 Done
32
33 add lsn appsprofile LSN-APPS-HTTP-PROFILE-8 TCP -td 5
34
35 Done
36
37 bind lsn appsprofile LSN-APPS-HTTP-PROFILE-8 80
38
39 Done
40
41 bind lsn group LSN-GROUP-8 -applicationprofilename LSN-APPS-HTTP-
      PROFILE-8
42
43 Done
44 <!--NeedCopy-->
```

Erstellen Sie eine LSN-Konfiguration, die den ausgehenden Datenverkehr eines bestimmten Protokolls (TCP) einschränkt und über eine bestimmte Datenverkehrsdomäne (td 5) sendet. Mit der endpunktunabhängigen Filterung empfangen Sie eingehenden Datenverkehr im Zusammenhang mit diesem Protokoll (TCP) in einer beliebigen Datenverkehrsdomäne:

```
1 add lsn client LSN-CLIENT-9
2
3 Done
4
5 bind lsn client LSN-CLIENT-9 -network 192.0.9.0 -netmask 255.255.255.0
```



```
    -td 1

Done

add lsn pool LSN-POOL-9

Done

bind lsn pool LSN-POOL-9 203.0.113.90

Done

add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9

Done

bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9

Done

add lsn appsprofile LSN-APPS-PROFILE-9 TCP -filtering ENDPOINT-
    INDEPENDENT -td 5

Done

bind lsn group LSN-GROUP-9 -approfile LSN-APPS-PROFILE-9

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

Erstellen Sie eine LSN-Konfiguration, die den ausgehenden HTTP-Datenverkehr (Port 80) einschränkt und über eine bestimmte Datenverkehrsdomäne (td 10) sendet. Bei adressabhängiger Filterung empfangen Sie eingehenden Datenverkehr im Zusammenhang mit diesem Protokoll (HTTP) in der angegebenen Datenverkehrsdomäne (td 10):

```
add lsn client LSN-CLIENT-10

Done

bind lsn client LSN-CLIENT-10 -network 192.0.10.0 -netmask
    255.255.255.0 -td 1

Done
```



```
8
9  add lsn pool LSN-POOL-10
10
11 Done
12
13 bind lsn pool LSN-POOL-10 203.0.113.100
14
15 Done
16
17 add lsn group LSN-GROUP-10 -clientname LSN-CLIENT-10
18
19 Done
20
21 bind lsn group LSN-GROUP-10 -poolname LSN-POOL-10
22
23 Done
24
25 add lsn appsprofile LSN-APPS-PROFILE-10 TCP -mapping ENDPOINT -
      INDEPENDENT -filtering ADDRESS-DEPENDENT -td 10
26
27 Done
28
29 bind lsn appsprofile LSN-APPS-PROFILE-10 80
30
31 Done
32
33 bind lsn group LSN-GROUP-10 -approfile LSN-APPS-PROFILE-10
34
35 Done
36 <!--NeedCopy-->
```

Statische LSN-Zuordnungen konfigurieren

October 5, 2021

Die Citrix ADC Appliance unterstützt die manuelle Erstellung einer 1:1 LSN-Zuordnung zwischen einer Teilnehmer-IP-Adresse:Port und einer NAT-IP-Adresse:Port. Statische LSN-Zuordnungen sind nützlich, wenn Sie sicherstellen möchten, dass die Verbindungen, die zu einer NAT-IP initiiert wurden: Port der Teilnehmer-IP-Adresse zuordnet: Port. Zum Beispiel Webserver, die sich im internen Netzwerk befinden.

So erstellen Sie eine statische LSN-Zuordnung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn static <name> <transportprotocol> <subscrIP> <subscrPort> [-td
    <positive_integer>] [<natIP> [<natPort>]] [-destIP <ip_addr> [-dsttd
     <positive_integer>]]
-  show lsn static
<!--NeedCopy-->
```

So erstellen Sie eine statische LSN-Zuordnung mit dem Konfigurationsdienstprogramm

Navigieren Sie zu System > Large Scale NAT > Statisch, und fügen Sie eine neue statische Zuordnung hinzu.

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

add lsn static name

Name des statischen LSN-Zuordnungseintrags. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem die LSN-Gruppe erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. lsn static1” oder lsn static1”). Dies ist ein obligatorisches Argument. Maximale Länge: 127

transportprotocol

Protokoll für den LSN-Zuordnungseintrag. Dies ist ein obligatorisches Argument. Mögliche Werte: TCP, UDP, ICMP

subscrIP

IPv4-Adresse eines LSN-Teilnehmers für den LSN-Zuordnungseintrag. Dies ist ein obligatorisches Argument.

subscrPort

Port des LSN-Teilnehmers für den LSN-Zuordnungseintrag. Dies ist ein obligatorisches Argument. Maximalwert: 65535

td

ID der Traffic-Domain, zu der der Abonnent gehört. Wenn Sie keine ID angeben, wird davon ausgegangen, dass der Abonnent Teil der Standardverkehrsdomäne ist. Standardwert: 0, Minimalwert: 0, Maximalwert: 4094

natIP

IPv4-Adresse, die bereits auf der Citrix ADC Appliance als Typ LSN vorhanden ist und als NAT-IP-Adresse für diesen Zuordnungseintrag verwendet wird.

natPort

NAT-Port für diesen LSN-Zuordnungseintrag.

destIP

Ziel-IP-Adresse für den LSN-Zuordnungseintrag.

dsttd

ID der Datenverkehrsdomäne, über die die Ziel-IP-Adresse für diesen LSN-Zuordnungseintrag von der Citrix ADC Appliance erreichbar ist. Wenn Sie keine ID angeben, wird angenommen, dass die Ziel-IP-Adresse über die Standardverkehrsdomäne mit der ID 0 erreichbar ist. Standardwert: 0, Minimalwert: 0, Maximalwert: 4094

Platzhalter-Port statische Zuordnungen

Ein statischer Zuordnungseintrag ist in der Regel eine Eins-zu-Eins-LSN-Zuordnung zwischen einer Teilnehmer-IP-Adresse:Port und einer NAT-IP-Adresse:Port. Ein eins-zu-eins-statischer LSN-Zuordnungseintrag stellt nur einen Port des Teilnehmers für das Internet bereit.

In einigen Situationen kann es erforderlich sein, alle Ports (64 KB) eines Teilnehmers für das Internet freizugeben (z. B. ein Server, der in einem internen Netzwerk gehostet wird und an jedem Port einen anderen Dienst ausführt). Um diese internen Dienste über das Internet zugänglich zu machen, müssen Sie alle Ports des Servers im Internet verfügbar machen.

Eine Möglichkeit, diese Anforderung zu erfüllen, besteht darin, 64K Eins-zu-Eins-Zuordnungseinträge, einen Zuordnungseintrag für jeden Port hinzuzufügen. Das Erstellen von 64K Einträgen ist sehr umständlich und eine große Aufgabe. Außerdem kann diese große Anzahl von Konfigurationseinträgen zu Leistungsproblemen in der Citrix ADC Appliance führen.

Eine weitere einfache Methode ist die Verwendung von Platzhalterports in einem statischen Zuordnungseintrag. Sie müssen nur einen statischen Zuordnungseintrag mit NAT-Port und Subscriber-Port-Parametern auf das Platzhalterzeichen (*) und den Protokollparameter auf ALL erstellen, um alle Ports eines Teilnehmers im Internet verfügbar zu machen. Bei eingehenden oder ausgehenden Verbindungen eines Abonnenten, die einem statischen Platzhalterzuordnungseintrag entsprechen, ändert sich der Port des Abonnenten nach dem NAT-Vorgang nicht.

Wenn eine vom Abonnenten initiierte Verbindung zum Internet mit einem Eintrag für statische Platzhalterzuordnung übereinstimmt, weist die Citrix ADC Appliance einen NAT-Port zu, der dieselbe Nummer hat wie der Abonnentenport, von dem aus die Verbindung hergestellt wird. Ähnlich wird ein Internet-Host mit dem Port eines Abonnenten verbunden, indem er eine Verbindung zum NAT-Port herstellt, der dieselbe Nummer wie der Port des Abonnenten hat.

Konfigurieren der Citrix ADC Appliance für den Zugriff auf alle Ports eines IPv4-Abonnenten

Um die Citrix ADC Appliance so zu konfigurieren, dass Zugriff auf alle Ports eines IPv4-Teilnehmers gewährt wird, erstellen Sie eine statische Platzhalterzuordnung mit den folgenden obligatorischen Parametereinstellungen:

- Protocol=ALL
- Subscriber port = *
- NAT port = *

In einer statischen Platzhalterzuordnung ist im Gegensatz zu einer statischen Eins-zu-Eins-zu-Eins-Zuordnung das Festlegen des NAT-IP-Parameters erforderlich. Außerdem kann die NAT-IP-Adresse, die einer statischen Platzhalterzuordnung zugewiesen ist, nicht für andere Abonnenten verwendet werden.

So erstellen Sie eine statische Platzhalterzuordnung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lsn static <name> ALL <subscrIP> *  <natIP> * [-td <
     positive_integer>] [-destIP <ip_addr> [-dsttd <positive_integer>]]
2
3 show lsn static
4 <!--NeedCopy-->
```


Beispielkonfiguration

In der folgenden Beispielkonfiguration einer statischen Platzhalterzuordnung werden alle Ports eines Teilnehmers mit der IP-Adresse 192.0.2.10 über NAT IP 203.0.11.33 zugänglich gemacht.

Beispielkonfiguration:

```
1 add lsn static NAT44-WILDCARD-STATIC-1 ALL  192.0.2.10 * 203.0.113.33 *
2
3 Done
4 <!--NeedCopy-->
```

Anwendungs-Layer-Gateways konfigurieren

October 5, 2021

Bei einigen Protokollen der Anwendungsschicht werden auch die IP-Adressen und Protokollportnummern in der Nutzlast des Pakets kommuniziert. Application Layer Gateway für ein Protokoll analysiert die Nutzlast des Pakets und führt notwendige Änderungen durch, um sicherzustellen, dass das Protokoll weiterhin über LSN funktioniert.

Die Citrix ADC Appliance unterstützt ALG für die folgenden Protokolle:

- FTP
- ICMP
- TFTP
- PPTP
- SIP
- RTSP

Application Layer Gateway für FTP-, ICMP- und TFTP-Protokolle

October 5, 2021

Sie können ALG für das FTP-Protokoll für eine LSN-Konfiguration aktivieren oder deaktivieren, indem Sie die FTP-Option der LSN-Gruppe der LSN-Konfiguration aktivieren oder deaktivieren.

ALG für das ICMP-Protokoll ist standardmäßig aktiviert, und es gibt keine Möglichkeit, es zu deaktivieren.

ALG für das TFTP-Protokoll ist standardmäßig deaktiviert. TFTP ALG wird automatisch für eine LSN-Konfiguration aktiviert, wenn Sie ein UDP LSN-Anwendungsprofil mit endpunktunabhängiger Zuordnung, endpunktunabhängiger Filterung und Zielport als 69 (bekannter Port für TFTP) an die LSN-Gruppe binden.

Beispiel-LSN-Konfiguration für FTP ALG:
In der folgenden Beispiel-LSN-Konfiguration ist FTP ALG für Abonnenten mit IP-Adresse im Bereich 192.0.2.30-192.0.2.100 aktiviert.

```
add ns acl LSN-ACL-1 ALLOW -srcIP 192.0.2.30-192.0.2.100

Done

apply acls

Done

add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1  -aclname LSN-ACL

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.10

Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1  -FTP ENABLED

Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1

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

Beispiel-LSN-Konfiguration für TFTP ALG:

In der folgenden LSN-Beispielkonfiguration sind endpunktunabhängige Zuordnung und endpunktunabhängige Filterung für das TFTP-Protokoll (UDP-Port 69) aktiviert. Die Citrix ADC Appliance aktiviert automatisch TFTP ALG für diese LSN-Konfiguration.

```
1  add lsn client LSN-CLIENT-2
2
3  Done
4
5  bind lsn client LSN-CLIENT-2 -network 198.51.100.0 -netmask
       255.255.255.0
6
7  Done
8
9  add lsn pool LSN-POOL-2
10
11 Done
12
13 bind lsn pool LSN-POOL-2 203.0.113.10-203.0.113.11
14
15 Done
16
17 add lsn group LSN-GROUP-2 -clientname LSN-CLIENT-2
18
19 Done
20
21 bind lsn group LSN-GROUP-2 -poolname pool1 LSN-POOL-2
22
23 Done
24
25 add lsn appsprofile LSNAPPSPROFILE-TFTP-2 UDP -mapping ENDPOINT-
       INDEPENDENT  - filtering  ENDPOINT-INDEPENDENT
26
27 Done
28
29 bind lsn appsprofile LSNAPPSPROFILE-TFTP-2 69
30
31 Done
32
33 bind lsn group LSN-GROUP-1 -applicationprofilename LSNAPPSPROFILE-TFTP
       -2
34
35 Done
36 <!--NeedCopy-->
```


Application Layer Gateway für PPTP-Protokoll

October 5, 2021

Die Citrix ADC Appliance unterstützt Application Layer Gateways (ALGs) für das Point-to-Point Tunneling-Protokoll (PPTP).

PPTP ist ein Netzwerkprotokoll, das eine sichere Übertragung von Daten von einem Remote-Client auf einen Unternehmensserver ermöglicht, indem ein Tunnel über TCP/IP-basierte Datennetzwerke erstellt wird. PPTP kapselt PPP-Pakete in IP-Pakete für die Übertragung über das Internet. PPTP richtet einen Tunnel für jedes kommunizierende PPTP-Netzwerkserverpaar (PNS) -PPTP Access Concentrator (PAC) ein. Nach dem Einrichten des Tunnels wird die erweiterte generische Routing Encapsulation (GRE) zum Austausch von PPP-Paketen verwendet. Eine Anruf-ID im GRE-Header gibt die Sitzung an, zu der ein bestimmtes PPP-Paket gehört.

Die Citrix ADC Appliance erkennt PPTP-Pakete, die am standardmäßigen TCP-Port 1723 ankommen. Die Appliance analysiert PPTP-Steuerungspakete, übersetzt die Anruf-ID und weist eine NAT-IP-Adresse zu. Für die bidirektionale Datenkommunikation zwischen Client und Server erstellt die Citrix ADC Appliance einen LSN-Sitzungseintrag basierend auf der Serveraufruf-ID und eine LSN-Sitzung basierend auf der Clientanruf-ID. Die Appliance analysiert dann die GRE-Datenpakete und übersetzt Anruf-IDs auf der Grundlage der beiden LSN-Sitzungseinträge.

Für PPTP-Protokoll enthält die Citrix ADC Appliance auch Timeout-Einstellung für alle unerlaubten PPTP-LSN-Sitzungen. Wenn eine PPTP-LSN-Sitzung für einen Zeitraum im Leerlauf ist, der die Zeitüberschreitungseinstellung überschreitet, entfernt die Citrix ADC Appliance die Sitzung.

Einschränkungen:

Im Folgenden sind die Einschränkungen von PPTP ALG auf einer Citrix ADC Appliance aufgeführt:

- PPTP ALG wird für den Haarnadel-LSN-Fluss nicht unterstützt.
- PPTP ALG wird nicht unterstützt, um mit RNAT Konfiguration zu arbeiten.
- PPTP ALG wird in Citrix ADC Clustern nicht unterstützt.

Konfigurieren von PPTP ALG

Die Konfiguration von PPTP ALG auf der Citrix ADC Appliance umfasst folgende Aufgaben:

- Erstellen Sie eine LSN-Konfiguration und aktivieren Sie PPTP ALG darauf. In einer LSN-Konfiguration enthält die LSN-Gruppe die PPTP-ALG-Einstellung. Anweisungen zum Erstellen einer LSN-Konfiguration finden Sie unter Konfigurationsschritte für LSN.
- (Optional) Legen Sie das globale Timeout für unzulässige PPTP-LSN-Sitzungen fest.

So aktivieren Sie PPTP-ALG für eine LSN-Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn group <groupname> -clientname <string> [-pptp ( ENABLED |
    DISABLED )]

show lsn group
<!--NeedCopy-->
```

So legen Sie das globale Timeout für unbenutzte PPTP-LSN-Sitzungen mit der CLI fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set appAlgParam -pptpGreIdleTimeout <positive_integer>

show appAlgParam
<!--NeedCopy-->
```

Beispiel:

In der folgenden LSN-Beispielkonfiguration ist PPTP ALG für Abonnenten im 192.0.2.0/24-Netzwerk aktiviert.

Auch leere PPTP LSN-Sitzungszeitüberschreitung ist auf 200 Sekunden festgelegt.

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.3

Done
```



```
16
17 add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1  -pptp ENABLED
18
19 Done
20
21 bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
22
23 Done
24
25 set appAlgParam -pptpGreIdleTimeout 200
26
27 Done
28 <!--NeedCopy-->
```

Application Layer Gateway für SIP-Protokoll

October 5, 2021

Die Verwendung von Large Scale NAT (LSN) mit Session Initiation Protocol (SIP) ist kompliziert, da SIP-Nachrichten IP-Adressen sowohl in den SIP-Headern als auch im SIP-Body enthalten. Wenn LSN mit SIP verwendet wird, enthalten die SIP-Header Informationen über den Anrufer und den Empfänger, und das Gerät übersetzt diese Informationen, um sie vor dem externen Netzwerk zu verstecken. Der SIP-Body enthält die SDP-Informationen (Session Description Protocol), die IP-Adressen und Portnummern für die Übertragung der Medien enthalten.

SIP ALG hält folgende RFCs ein:

- RFC 3261
- RFC 3581
- RFC 4566
- RFC 4475

> **Hinweis:**
>
> SIP ALG wird in einer eigenständigen Citrix ADC Appliance, in einem Citrix ADC-Hochverfügbarkeitssetup sowie in einem Citrix ADC-Cluster-Setup unterstützt.

Funktionsweise von SIP ALG

Die Art und Weise, wie die Übersetzung von IP-Adressen durchgeführt wird, hängt vom Typ und der Richtung der Nachricht ab. Eine Nachricht kann eine der folgenden sein:

- Eingehende Anfrage

- Ausgehende Antwort
- Ausgehende Anfrage
- Eingangsantwort

Bei einer ausgehenden Nachricht werden die private IP-Adresse und die Portnummer des SIP-Clients durch die öffentliche IP-Adresse und die Portnummer des Citrix ADC ersetzt, die während der *LSN-Konfiguration angegebene IP-Adresse und Portnummer des LSN-Pools*genannt wird. Bei einer eingehenden Nachricht werden die IP-Adresse des LSN-Pools und die Portnummer durch die private Adresse des Clients ersetzt. Wenn die Nachricht öffentliche IP-Adressen enthält, behält sie die Citrix ADC SIP ALG bei. Außerdem wird ein Lochloch auf der erstellt:

- LSN-Pool-IP-Adresse und -Port im Auftrag des privaten Clients, so dass die Nachrichten, die zu dieser IP-Adresse und dem Port aus dem öffentlichen Netzwerk gelangen, als SIP-Nachrichten behandelt werden.
- Öffentliche IP-Adresse und Port im Auftrag der öffentlichen Clients, so dass die Nachrichten, die zu dieser IP-Adresse und Port aus dem privaten Netzwerk gelangen, als SIP-Nachrichten behandelt werden.

Wenn eine SIP-Nachricht über das Netzwerk gesendet wird, sammelt das SIP Application Layer Gateway (ALG) Informationen aus der Nachricht und übersetzt die IP-Adressen in den folgenden Kopfzeilen in LSN-Pool-IP-Adressen:

- Via
- Kontakt
- Route
- Datensatzroute

In der folgenden SIP-Beispielanforderungsnachricht ersetzt LSN die IP-Adressen in den Headerfeldern, um sie vor dem externen Netzwerk auszublenden.

```
1 INVITE adam@10.102.185.156 SIP/2.0 Via: SIP/2.0/UDP 192.170.1.161:62914
     From: eve@10.120.210.3 To: adam@10.102.185.156 Call-ID: a12abcde@10
    .120.210.3 Contact: adam@10.102.185.156 Route: <sip:netscreen@10
    .150.20.3:5060> Record-Route: <sip:netscreen@10.150.20.3:5060>
2 <!--NeedCopy-->
```

Wenn eine Nachricht mit SDP-Informationen eintrifft, sammelt die SIP-ALG Informationen aus der Nachricht und übersetzt die IP-Adressen in den folgenden Feldern in LSN-Pool-IP-Adressen und Portnummern:

- c= (Verbindungsinformationen)

  Dieses Feld kann auf Sitzungs- oder Medienebene angezeigt werden. Es erscheint im folgenden Format:

c=<network-type><address-type><connection-address>

Wenn es sich bei der Ziel-IP-Adresse um eine Unicast-IP-Adresse handelt, erstellt die SIP-ALG unter Verwendung der IP-Adresse und der Portnummern, die im Feld m= angegeben sind.

- m= (Medienankündigung)

  Dieses Feld wird auf Medienebene angezeigt und enthält die Beschreibung des Mediums. Es erscheint im folgenden Format:

  m=<media><port><transport><fmt list>

- a=(information about the media field)

  Dieses Feld kann auf Sitzungs- oder Medienebene im folgenden Format angezeigt werden:

  a=<attribute>

  a=<attribute>:<value>

Der folgende Auszug aus einem Beispiel-SDP-Abschnitt zeigt die Felder, die für die Ressourcenzuordnung übersetzt werden.

o=user 2344234 55234434 IN IP4 10.150.20.3

c=IN IP4 10.150.20.3

m=audio 43249 RTP/AVP 0

Die folgende Tabelle zeigt, wie SIP-Nutzlast übersetzt wird.

Eingehende Anfrage (von öffentlich zu privat)	In:	Ohne
	Von:	Ohne
	Anruf-ID:	Ohne
	Über:	Ohne
	Anforderungs-URI:	Ersetzen Sie die IP-Adresse des LSN-Pools durch eine private IP-Adresse
	Kontakt:	Ohne
	Datensatzroute	Ohne
	Reiseroute:	Ohne
Ausgehende Antwort (von privat zu öffentlich)	In:	Ohne

	Von:	Ohne
	Anruf-ID:	Ohne
	Über:	Ohne
	Anforderungs-URI:	Ersetzen Sie die private IP-Adresse durch die IP-Adresse des LSN-Pools
	Kontakt:	Ersetzen Sie die private IP-Adresse durch die IP-Adresse des LSN-Pools
	Datensatzroute	Ohne
	Reiseroute:	Ohne
Ausgehende Anfrage (von privat zu öffentlich)	In:	Ohne
	Von:	Ohne
	Anruf-ID:	Ohne
	Über:	Ersetzen Sie die private IP-Adresse durch die IP-Adresse des LSN-Pools
	Anforderungs-URI:	Ohne
	Kontakt:	Ersetzen Sie die private IP-Adresse durch die IP-Adresse des LSN-Pools
	Datensatzroute	Ohne
	Reiseroute:	Ohne
Eingangsantwort (von öffentlich zu privat)	In:	Ohne
	Von:	Ohne
	Anruf-ID:	Ohne
	Über:	Ersetzen Sie die IP-Adresse des LSN-Pools durch eine private IP-Adresse
	Anforderungs-URI:	Ohne

	Kontakt:	Öffentliche IP-Adresse behalten, falls vorhanden
	Datensatzroute	Ohne
	Reiseroute:	Ohne

Einschränkungen der SIP ALG

Eine SIP-ALG hat folgende Einschränkungen:

- Es wird nur SDP-Nutzlast unterstützt.
- Folgende Komponenten werden nicht unterstützt:
  - Multicast-IP-Adressen
  - Verschlüsseltes SDP
  - SIP TLS
  - FQDN-Übersetzung
  - SIP-Layer-Authentifizierung
  - TD/Partitionierung
  - Mehrteiliger Körper
  - SIP-Nachrichten über IPv6-Netzwerk
  - Linie faltbar

Getestete SIP-Clients und Proxyserver

Folgende SIP-Clients und Proxyserver wurden mit SIP ALG getestet:

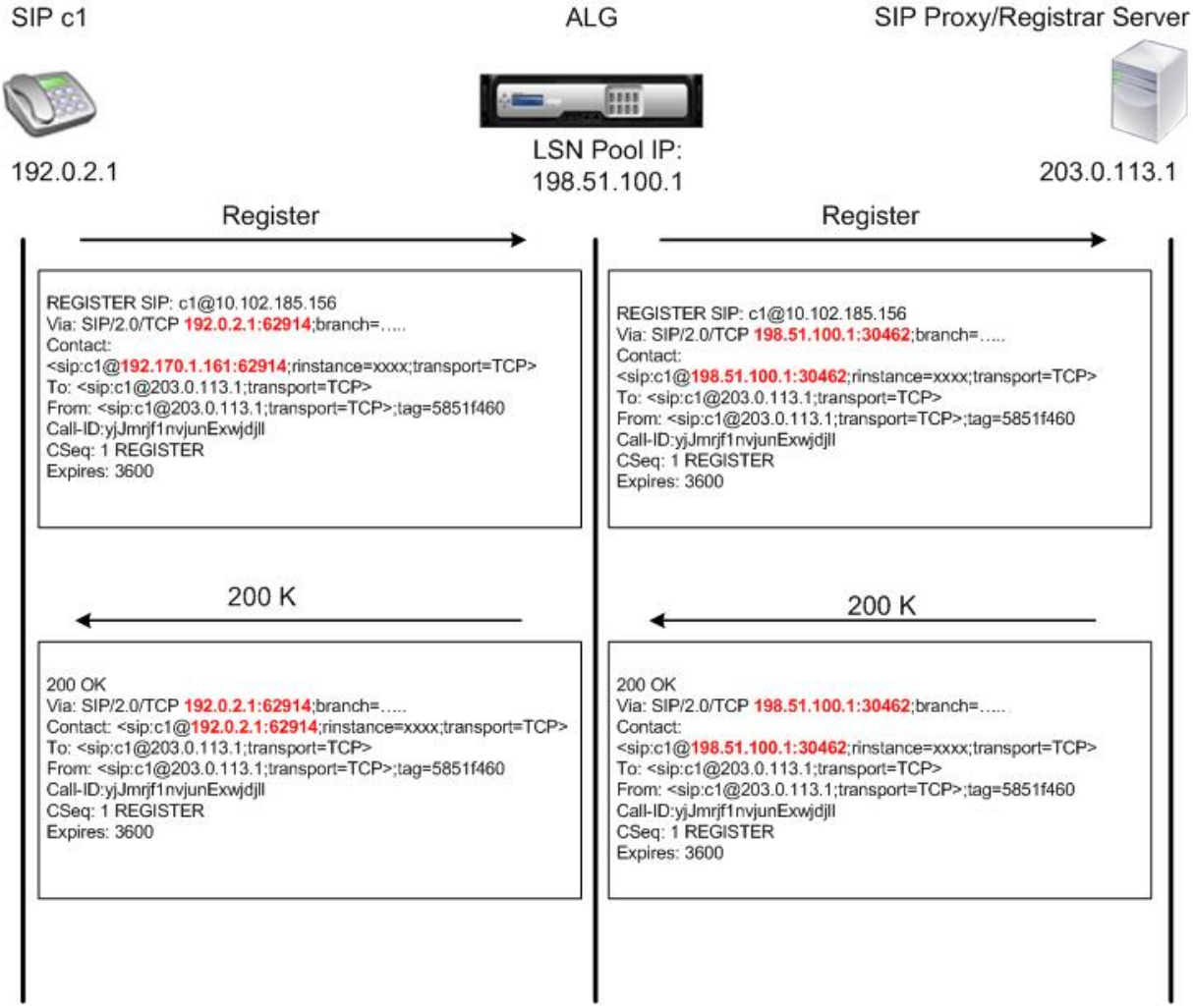
- **SIP-Kunden:** X-Lite, Zoiper, Ekiga. Avaya
- **Proxyserver:** openSIPS

LSN SIP-Szenario: SIP-Proxy außerhalb des privaten Netzwerks (Öffentliches Netzwerk)

SIP-Client-Registrierung

Bei einem typischen SIP-Aufruf muss sich der SIP-Client beim SIP-Registrar registrieren, indem er eine REGISTER-Anfrage zusammenstellt und an den SIP-Registrar sendet. Die SIP-ALG der Citrix ADC Appliance fängt die Anforderung ab, ersetzt die IP-Adresse und Portnummer in der Anforderung durch die IP-Adresse des LSN-Pools und die Portnummer in der LSN-Konfiguration und leitet die Anforderung an den SIP-Registrar weiter. Die SIP ALG öffnet dann ein Pinhole in der Citrix ADC Konfiguration, um eine

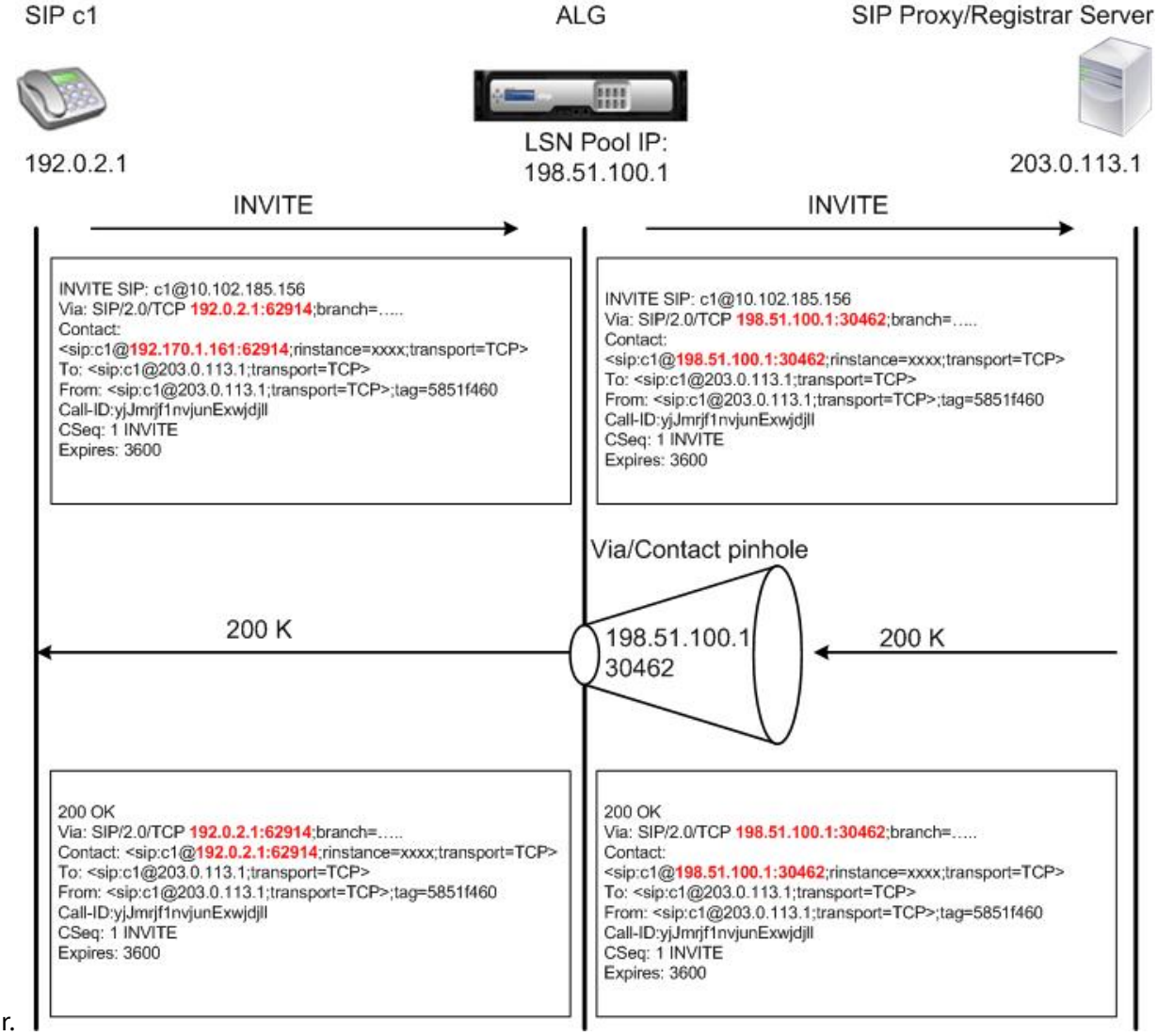
weitere SIP-Kommunikation zwischen dem SIP-Client und dem SIP-Registrar zu ermöglichen. Der SIP-Registrar sendet eine 200 OK-Antwort an den SIP-Client über die IP-Adresse und die Portnummer des LSN-Pools. Die Citrix ADC Appliance erfasst diese Antwort in der Pinhole, und die SIP-ALG ersetzt den SIP-Header, wodurch die ursprünglichen SIP-Felder Kontakt, Via, Route und Datensatzroute wieder in die Nachricht eingefügt werden. Die SIP ALG leitet die Nachricht dann an den SIP-Client weiter. Die folgende Abbildung zeigt, wie SIP ALG LSN in einem SIP-Anrufregistrierungsablauf verwendet.



Ausgehende Anrufe

Ein SIP-Aufruf wird mit einer SIP-INVITE-Nachricht initiiert, die vom internen an das externe Netzwerk gesendet wird. Die SIP-ALG führt NAT für die IP-Adressen und Portnummern in den SIP-Header-Feldern Via, Kontakt, Route und Record-Route durch und ersetzt sie durch die IP-Adresse des LSN-Pools und die Portnummer. LSN speichert diese Zuordnungen für nachfolgende SIP-Nachrichten im SIP-Aufruf. Die SIP ALG öffnet dann separate Pinholes in der Citrix ADC Konfiguration, um SIP und Medien über die Citrix ADC-Appliance an den dynamisch zugewiesenen Ports zu ermöglichen, die in den SDP- und SIP-Headern angegeben sind. Wenn

eine 200-OK-Nachricht beim Citrix ADC eintrifft, wird sie von einer der erstellten Pinholes erfasst. Die SIP-ALG ersetzt den SIP-Header und stellt die ursprünglichen SIP-Felder Kontakt, Via, Route und Datensatzroute wieder her und leitet die Nachricht dann an den internen SIP-Client weiter.

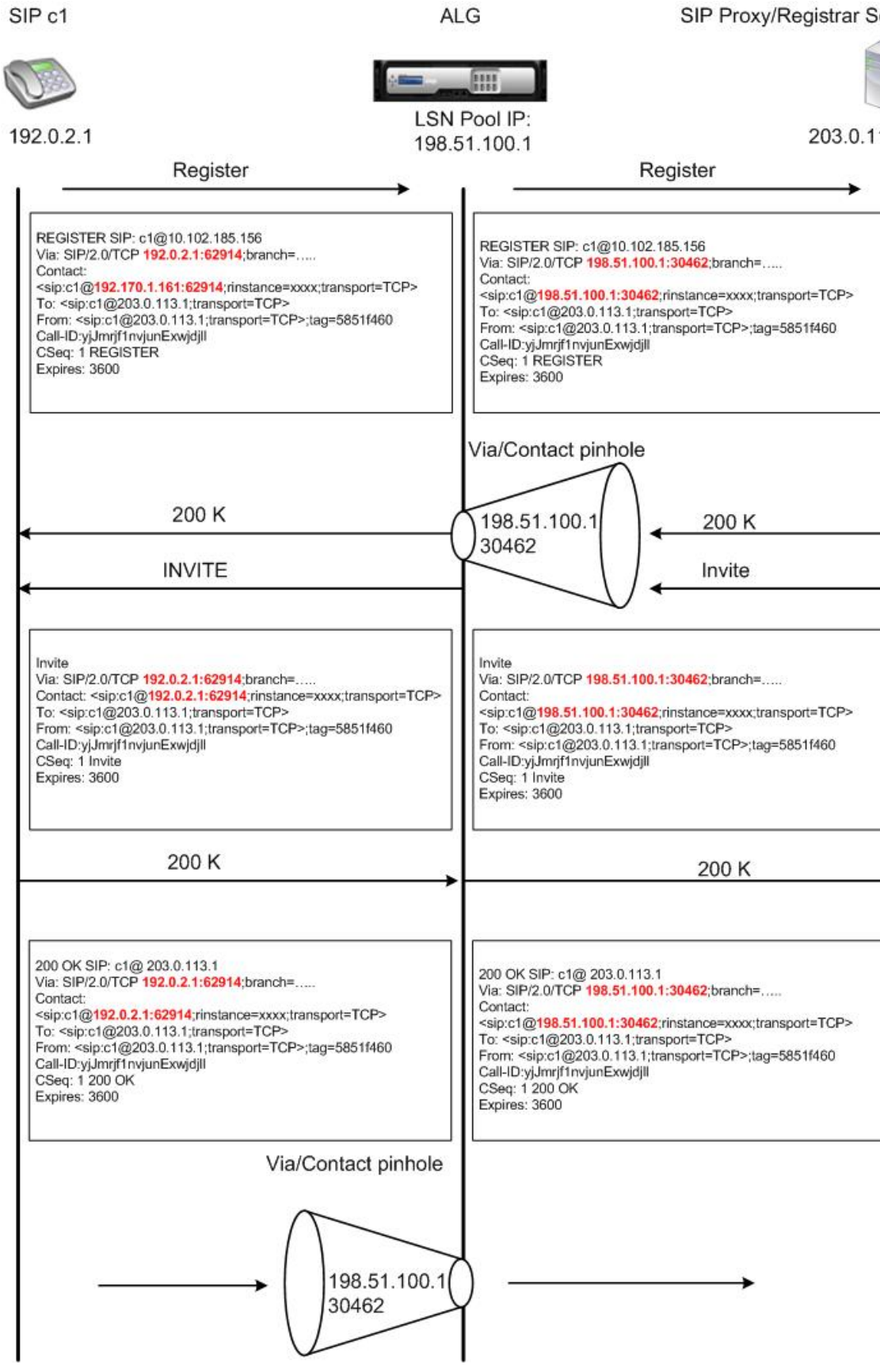


Eingehende Anrufe

Ein eingehender SIP-Anruf wird mit einer SIP-INVITE-Nachricht vom externen Client an das interne Netzwerk initiiert. Der SIP-Registrar leitet die INVITE-Nachricht an den SIP-Client im internen Netzwerk weiter und verwendet dabei das Lochloch, das erstellt wurde, als der interne SIP-Client beim SIP-Registrar registriert wurde.

Die SIP-ALG führt NAT für die LSN-IP-Adressen und Portnummern in den SIP-Header-Feldern Via, Kontakt, Route und Record-Route aus, übersetzt sie in die IP-Adresse und Portnummer des internen SIP-Clients und leitet die Anforderung an den SIP-Client weiter. Wenn die vom internen SIP-Client gesendete 200-OK-Antwortnachricht bei der Citrix ADC Appliance eintrifft, führt die SIP-ALG NAT für

die IP-Adressen und Portnummern in den SIP-Headerfeldern Via, Kontakt, Route und Record-Route aus und überträgt sie in die IP-Adresse und Portnummer des LSN-Pools und leitet die Antwort weiter.
-Nachricht an den SIP-Registrar und öffnet dann ein Lochloch in ausgehender Richtung für die weitere



SIP-Kommunikation.

Anrufbeendigung

Die BYE-Nachricht beendet einen Anruf. Wenn das Gerät eine BYE-Nachricht empfängt, übersetzt es die Header-Felder in der Nachricht genauso wie für jede andere Nachricht. Da jedoch eine BYE Nachricht vom Empfänger mit einem 200 OK quittiert werden muss, verzögert die ALG den Anrufabbau um 15 Sekunden, um Zeit für die Übertragung des 200 OK zu ermöglichen.

Anruf zwischen Clients im selben Netzwerk

Wenn sowohl Client A als auch Client B im selben Netzwerk einen Anruf initiieren, werden die SIP-Nachrichten über den SIP-Proxy im externen Netzwerk weitergeleitet. Die SIP ALG verarbeitet die INVITE von Client A als normaler ausgehender Anruf. Da sich Client B im selben Netzwerk befindet, sendet der SIP-Proxy das INIVITE zurück an die Citrix ADC Appliance. Das SIP ALG prüft die INIVITE-Nachricht, stellt fest, dass sie die NAT-IP-Adresse von Client A enthält, und ersetzt diese durch die private IP-Adresse des Clients A, bevor die Nachricht an Client B gesendet wird. Sobald der Anruf zwischen den Clients hergestellt ist, ist der Citrix ADC nicht an der Medienübertragung beteiligt. zwischen den Clients.

Weitere LSN SIP-Szenarien: SIP-Proxy im privaten Netzwerk

Wenn Sie den SIP-Proxyserver im privaten Netzwerk hosten möchten, empfiehlt Citrix, eine der folgenden Aktionen durchzuführen:

- Konfigurieren Sie eine statische LSN-Zuordnung für den privaten SIP-Proxy. Weitere Informationen finden Sie unter Konfigurieren von statischen LSN-Maps. Stellen Sie sicher, dass der NAT-Port mit dem Port identisch ist, der im SIP-ALG-Profil konfiguriert ist.
- Konfigurieren Sie den SIP-Proxyserver in einer demilitarisierten Zone (DMZ).

Abbildung 1. SIP-Anrufregistrierung

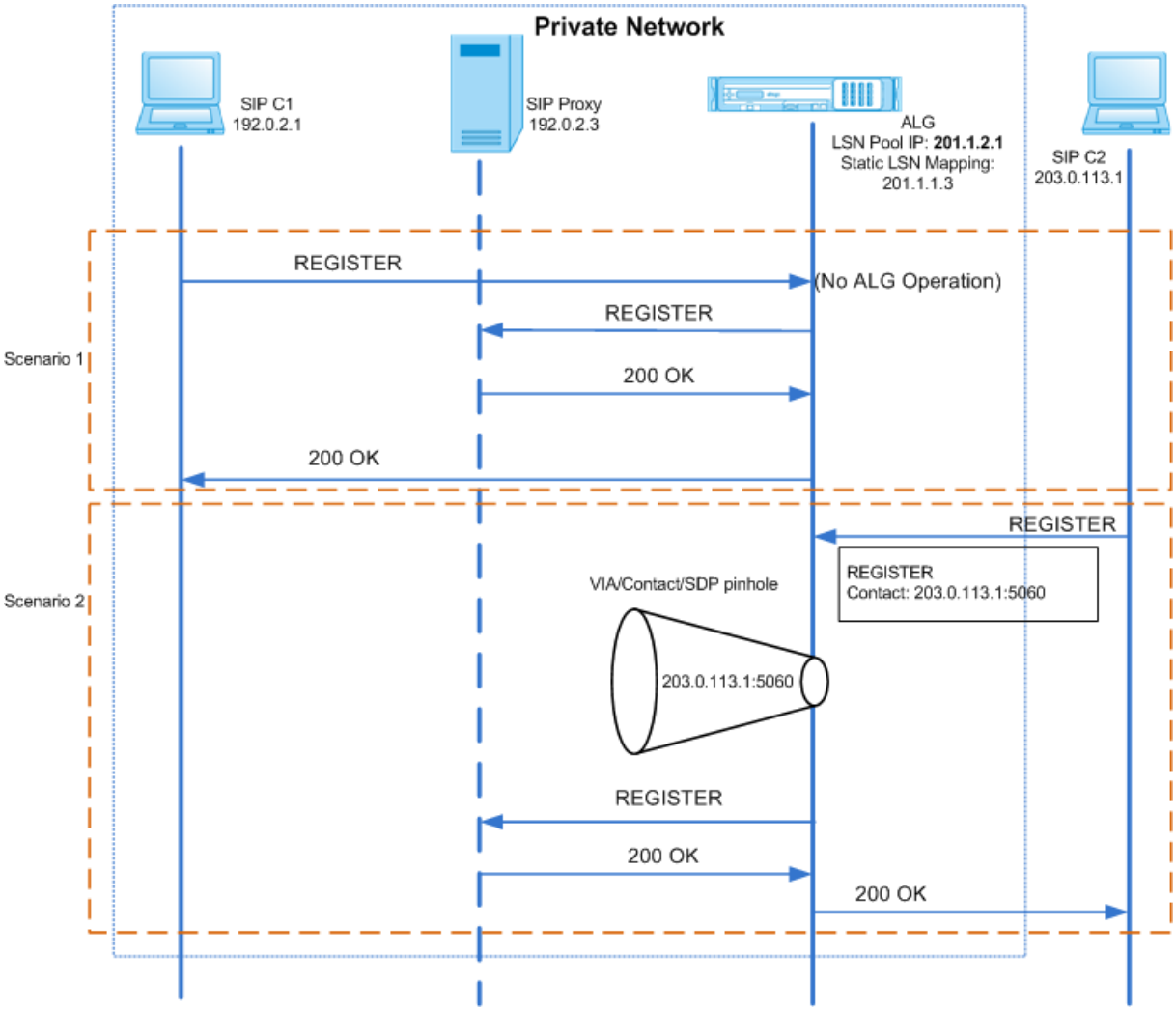
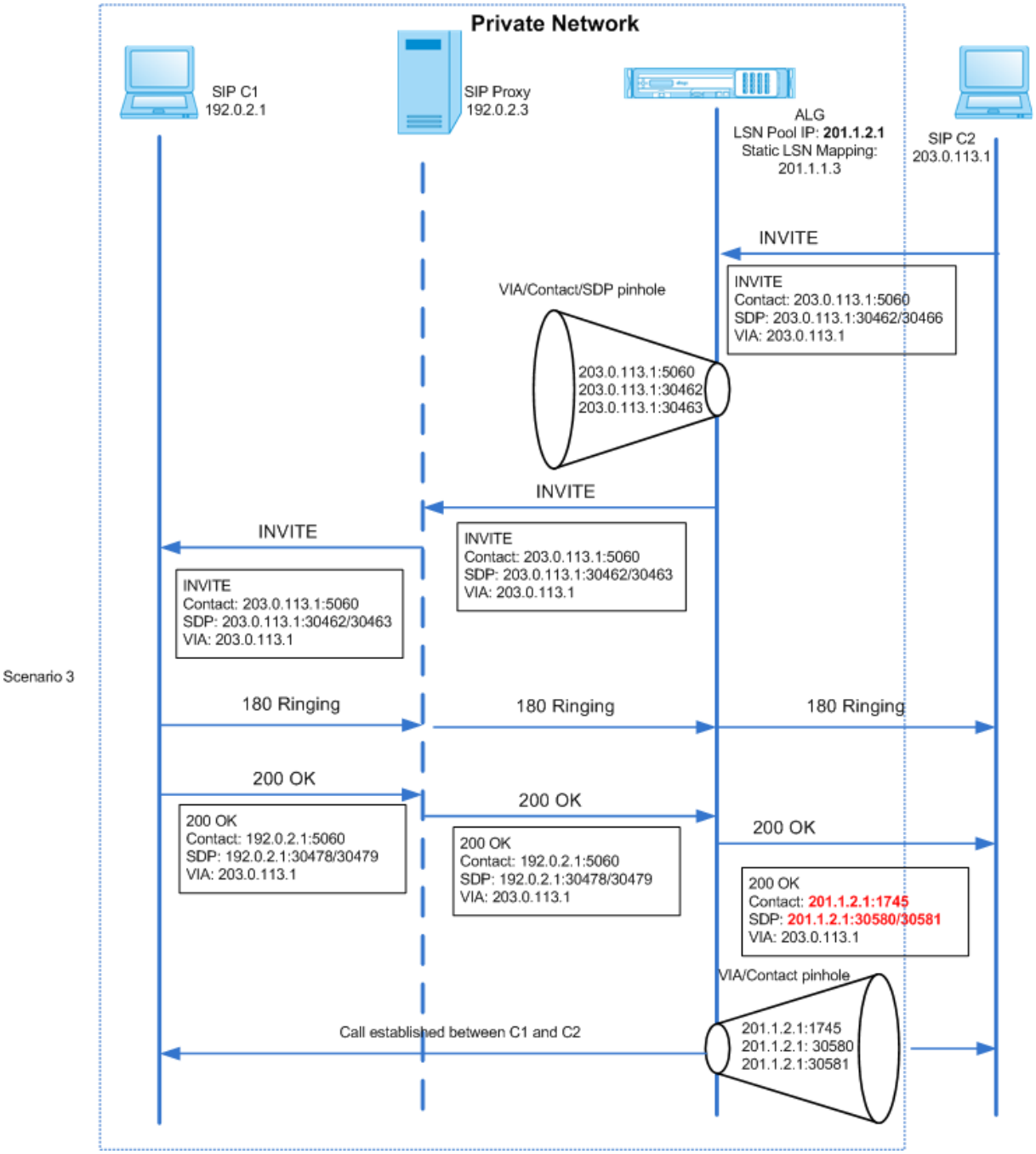


Abbildung 2. SIP-Eingehender Anruf



Die Abbildungen 1 und 2 zeigen die folgenden Szenarien:

- Szenario 1: Der SIP-Client im privaten Netzwerk registriert sich beim SIP-Proxyserver im selben Netzwerk. ALG-Vorgänge werden nicht ausgeführt, da sich der SIP-Client und der SIP-Proxyserver im selben Netzwerk befinden.
- Szenario 2: Der SIP-Client im öffentlichen Netzwerk registriert sich beim SIP-Proxyserver im privaten Netzwerk. Die REGISTER-Meldung vom öffentlichen SIP-Client wird mit der auf der Appliance konfigurierten statischen LSN-Zuordnung an die Citrix ADC Appliance gesendet, und die

Appliance erstellt ein Lochloch für weitere SIP-Vorgänge.

- Szenario 3 — SIP-Eingehender Anruf. Ein eingehender SIP-Anruf wird mit einer SIP-INVITE-Nachricht vom externen zum internen Netzwerk initiiert. Die Citrix ADC Appliance empfängt die INVITE-Nachricht vom SIP-Client C2, der sich im externen Netzwerk befindet, über die statischen LSN-Zuordnungen, die auf der Citrix ADC Appliance konfiguriert sind.
  Die Appliance erstellt ein Lochloch und leitet die INVITE-Nachricht an den SIP-Proxy weiter. Der SIP-Proxy leitet dann die INVITE-Nachricht an den SIP-Client C1 im internen Netzwerk weiter. Der SIP-Client C1 sendet dann 180 und 200 OK-Nachrichten an den SIP-Proxy, der die Nachricht wiederum über die Citrix ADC Appliance an den SIP-Client C2 weiterleitet.
  Wenn die vom internen SIP-Client C1 gesendete 200 OK-Antwortnachricht im Citrix ADC eintrifft, führt die SIP-ALG NAT für die IP-Adressen und Portnummern in den SIP-Headerfeldern Via, Kontakt, Route und Datensatzroute sowie in den SDP-Feldern aus und ersetzt sie durch die IP-Adresse des LSN-Pools und Portnummer . Die SIP ALG leitet dann die Antwortmeldung an SIP-Client C2 weiter und öffnet ein Lochloch in ausgehender Richtung für weitere SIP-Kommunikation.

Unterstützung für Überwachungsprotokolle

Sie können ALG-Informationen als Teil der LSN-Protokollierung protokollieren, indem Sie ALG in der LSN-Überwachungsprotokollierungskonfiguration aktivieren. Weitere Informationen zur LSN-Protokollierung finden Sie unter LSN protokollieren und überwachen. Eine Protokollmeldung für einen ALG-Eintrag im LSN-Protokoll besteht aus folgenden Informationen:

- Zeitstempel
- Typ der SIP-Nachricht (z. B. SIP-Anfrage)
- Quell-IP-Adresse und Port des SIP-Clients
- Ziel-IP-Adresse und Port des SIP-Proxy
- NAT IP-Adresse und Port
- SIP-Methode
- Sequenznummer
- Ob der SIP-Client registriert ist oder nicht
- Benutzername und Domäne des Anrufers
- Benutzername und Domäne des Receivers

Beispiel-Audit-Protokoll:

Anfrage:

```
1 07/19/2013:09:49:19 GMT Informational 0-PPE-0 : default ALG
     ALG_SIP_INFO_PACKET_EVENT 169 0 : Infomsg: "SIP request" - Group: g2
      - Call_ID: NTY0YjYwMTJmYjNhNDU5ZjlhMmQxOTM5ZTE3Zjc3NjM. - Transport
```



```
    : TCP - Source_IP: 192.169.1.165 - Source_port: 57952 -
    Destination_IP: 10.102.185.156 - Destination_port: 5060 - Natted_IP:
     10.102.185.191 - Natted_port: 10313 - Method: REGISTER -
    Sequence_Number: 3060 - Register: YES - Content_Type: -
    Caller_user_name: 156_pvt_1 - Callee_user_name: 156_pvt_1 -
    Caller_domain_name: - Callee_domain_name: -
<!--NeedCopy-->
```

Antwort:

```
07/19/2013:09:49:19 GMT Informational 0-PPE-0 : default ALG
    ALG_SIP_INFO_PACKET_EVENT 170 0 : Infomsg: "SIP response" - Group:
    g2 - Call_ID: NTY0YjYwMTJmYjNhNDU5ZjlhMmQxOTM5ZTE3Zjc3NjM. -
    Transport: TCP - Response_code 200 - Source_IP: 10.102.185.156 -
    Source_port: 5060 - Destination_IP: 192.169.1.165 - Destination_port
    : 57952 - Natted_IP: 10.102.185.191 - Natted_port: 10313 -
    Sequence_Number: 3060 - Content_Type: - Caller_user_name: 156_pvt_1
    - Callee_user_name: 156_pvt_1 - Caller_domain_name: -
    Callee_domain_name: -
<!--NeedCopy-->
```

Konfigurieren von SIP ALG

Sie müssen die SIP ALG als Teil der LSN-Konfiguration konfigurieren. Anweisungen zum Konfigurieren von LSN finden Sie unter Konfigurationsschritte für LSN. Stellen Sie beim Konfigurieren von LSN sicher, dass Sie:

- Legen Sie beim Hinzufügen des LSN-Anwendungsprofils die folgenden Parameter fest:
  - IP-Pooling = PAIRED
  - Adress- und Portzuordnung = ENDPOINT-INDEPENDENT
  - Filterung = ENDPOINT-INDEPENDENT

Wichtig: Damit die SIP ALG funktioniert, ist eine vollständige Konus-NAT-Konfiguration erforderlich.

Beispiel:

```
add lsn appsprofile app_tcp TCP -ippooling PAIRED -mapping ENDPOINT-
    INDEPENDENT -filtering ENDPOINT-INDEPENDENT
<!--NeedCopy-->
```

- Erstellen Sie ein SIP-ALG-Profil und stellen Sie sicher, dass Sie entweder den Quellportbereich oder den Zielportbereich definieren.

Beispiel:

```
add lsn sipalgprofile sipalgprofile_tcp -sipsrcportrange 1-65535 -
    sipdstportrange 5060 -openViaPinhole ENABLED -openRecordRoutePinhole
     ENABLED  - sipTransportProtocol TCP
<!--NeedCopy-->
```

- Legen Sie SIP ALG = ENABLED fest, während Sie die LSN-Gruppe erstellen.

Beispiel:

```
add lsn group g1 -clientname c1 -sipalg ENABLED
<!--NeedCopy-->
```

- Binden Sie das SIP-ALG-Profil an die LSN-Gruppe.

Beispiel SIP-ALG-Konfiguration:

Die folgende Beispielkonfiguration zeigt, wie Sie eine einfache LSN-Konfiguration mit einem einzelnen Teilnehmernetzwerk, einer einzelnen LSN-NAT-IP-Adresse, einer SIP-ALG-spezifischen Einstellung erstellen und SIP-ALG konfigurieren:

```
add lsn pool p1

Done

bind lsn pool p1 10.102.185.190

Done

add lsn client c1

Done

bind lsn client c1 -network 192.170.1.0 -netmask 255.255.255.0

Done

add lsn appsprofile app_tcp TCP -ippooling PAIRED -mapping ENDPOINT-
    INDEPENDENT -filtering ENDPOINT-INDEPENDENT

Done
```



```
20
21 add lsn appsprofile app_udp UDP -ippooling PAIRED -mapping ENDPOINT-
      INDEPENDENT -filtering ENDPOINT-INDEPENDENT
22
23 Done
24
25 bind lsn appsprofile app_tcp 1-65535
26
27 Done
28
29 bind lsn appsprofile app_udp 1-65535
30
31 Done
32
33 add lsn sipalgprofile sipalgprofile_tcp -sipdstportrange 5060 -
      openViaPinhole ENABLED -openRecordRoutePinhole ENABLED  -
      sipTransportProtocol TCP
34
35 Done
36
37 add lsn sipalgprofile sipalgprofile_udp -sipdstportrange 5060 -
      openViaPinhole ENABLED -openRecordRoutePinhole ENABLED -
      sipTransportProtocol UDP
38
39 Done
40
41 add lsn group g1 -clientname c1 -sipalg ENABLED
42
43 Done
44
45 bind lsn group g1 -poolname p1
46
47 Done
48
49 bind lsn group g1 -appsprofilename app_tcp
50
51 Done
52
53 bind lsn group g1 -appsprofilename app_udp
54
55 Done
56
57 bind lsn group g1 -sipalgprofilename sipalgprofile_tcp
58
59 Done
```



```
60
61 bind lsn group g1 -sipalgprofilename sipalgprofile_udp
62
63 Done
64 <!--NeedCopy-->
```

Application Layer Gateway für RTSP-Protokoll

October 5, 2021

Real Time Streaming Protocol (RTSP) ist ein Protokoll auf Anwendungsebene für die Übertragung von Echtzeit-Mediendaten. RTSP wird zum Einrichten und Steuern von Mediensitzungen zwischen Endpunkten verwendet und ist ein Kontrollkanalprotokoll zwischen dem Media-Client und dem Medienserver. Die typische Kommunikation ist zwischen einem Client und einem Streaming-Medienserver.

Das Streamen von Medien aus einem privaten Netzwerk in ein öffentliches Netzwerk erfordert die Übersetzung von IP-Adressen und Portnummern über das Netzwerk. Die Citrix ADC Funktionalität umfasst ein Application Layer Gateway (ALG) für RTSP, das mit Large Scale NAT (LSN) verwendet werden kann, um den Medienstrom zu analysieren und alle erforderlichen Änderungen vorzunehmen, um sicherzustellen, dass das Protokoll weiterhin über das Netzwerk funktioniert.

Die IP-Adressenübersetzung hängt vom Typ und der Richtung der Nachricht sowie vom Typ der Medien ab, die von der Client-Server-Bereitstellung unterstützt werden. Nachrichten werden wie folgt übersetzt:

- Ausgehende Anforderung: Private IP-Adresse an Citrix ADC eigene öffentliche IP-Adresse, die als LSN-Pool-IP-Adresse bezeichnet wird.
- Eingehende Antwort: Die IP-Adresse des LSN-Pools an die private IP-Adresse.
- Eingangsanforderung: Keine Übersetzung.
- Ausgehende Antwort: Private IP-Adresse an die IP-Adresse des LSN-Pools.

> **Hinweis:**
>
> RTSP ALG wird in einer eigenständigen Citrix ADC Appliance, in einem Citrix ADC-Hochverfügbarkeitssetup sowie in einem Citrix ADC-Cluster-Setup unterstützt.

Einschränkungen der RTSP ALG

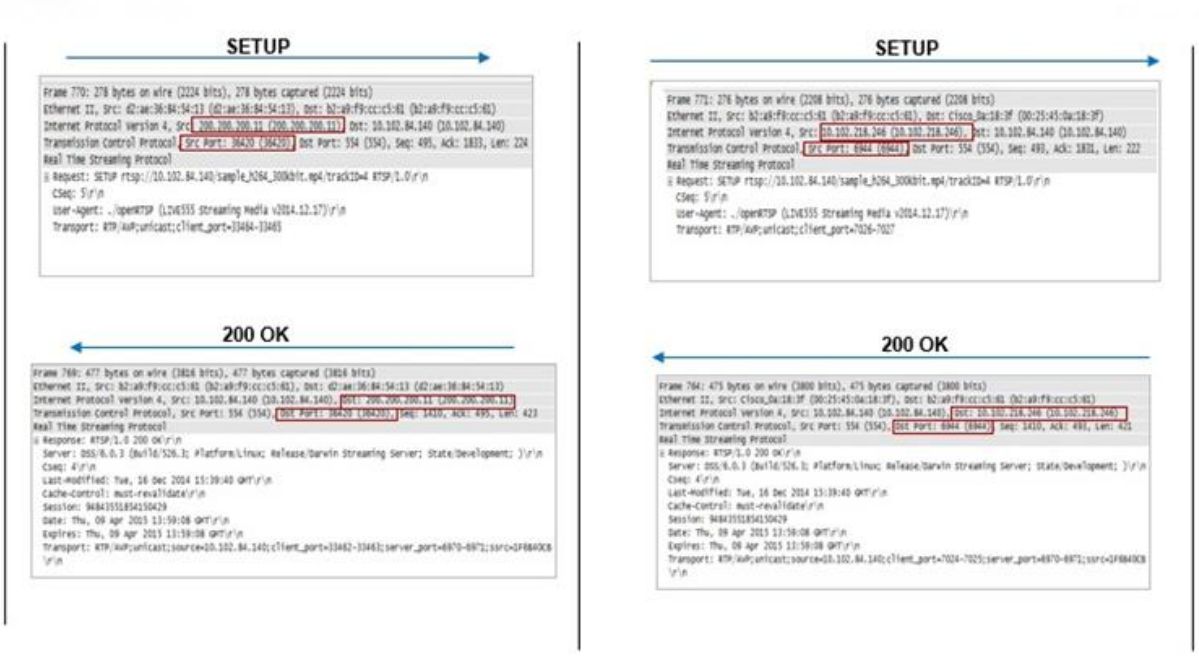
Die RTSP ALG unterstützt nicht Folgendes:

- Multicast-RTSP-Sitzungen

- RTSP-Sitzung über UDP
- TD/Admin-Partitionierung
- RSTP-Authentifizierung
- HTTP-Tunneling

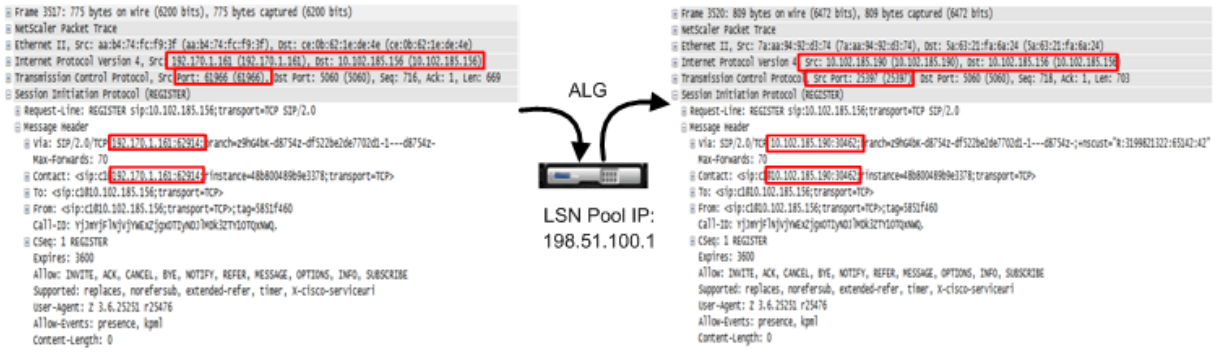
RTSP und LSN Szenario

Die folgende Abbildung zeigt einen RTSP SETUP-Anforderungsfluss. In der Regel gibt eine SETUP-Anforderung an, wie ein einzelner Medienstrom transportiert werden muss. Die Anforderung enthält die Medienstrom-URL und einen Transportbezeichner. Dieser Bezeichner enthält in der Regel einen lokalen Port für den Empfang von RTP-Daten (Audio oder Video) und einen anderen für den Empfang von RTCP-Daten (Meta-Informationen). Die Serverantwort bestätigt in der Regel die ausgewählten Parameter und füllt die fehlenden Teile aus, z. B. die ausgewählten Ports des Servers. Jeder Medienstrom muss mithilfe des Befehls SETUP konfiguriert werden, bevor eine Aggregatwiedergabeanforderung gesendet werden kann.

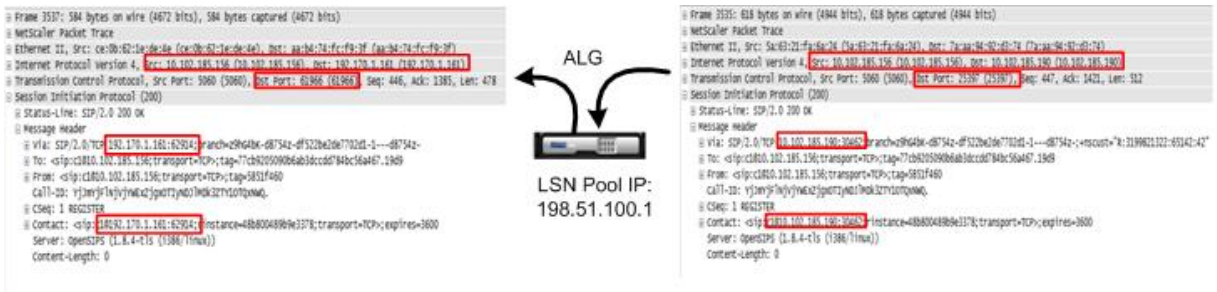


In einer typischen RTSP-Kommunikation sendet der Media-Client im öffentlichen Netzwerk eine SETUP-Anforderung an den Medienserver im privaten Netzwerk. RSTP ALG fängt die Anforderung ab und ersetzt im Medienstrom die öffentliche IP-Adresse und Portnummer durch die IP-Adresse des

LSN-Pools und die LSN-Portnummer. Die folgende Abbildung zeigt die Übersetzung, die von einer Citrix ADC Appliance im Medienstrom für eine ausgehende Anforderung durchgeführt wurde:



Der Medienserver im privaten Netzwerk verwendet die IP-Adresse des LSN-Pools und die LSN-Portnummer, um eine 200-OK-Antwort an den Medien-Client im öffentlichen Netzwerk zu senden. Die Citrix ADC RTSP ALG fängt die Antwort ab und ersetzt die IP-Adresse des LSN-Pools und die LSN-Portnummer durch die öffentliche IP-Adresse und Portnummer des Medienclients. Die folgende Abbildung zeigt die Übersetzung, die von einer Citrix ADC Appliance im Medienstrom für eine eingehende Antwort durchgeführt wurde:



Konfigurieren von RTSP ALG

Konfigurieren Sie RTSP ALG als Teil der LSN-Konfiguration. Anweisungen zum Konfigurieren von LSN finden Sie unter Konfigurationsschritte für LSN. Stellen Sie beim Konfigurieren von LSN sicher, dass Sie:

- Legen Sie den **NAT-Typ** als DETERMINSTIC oder DYNAMIC fest, während Sie den LSN-Pool hinzufügen.
- Legen Sie beim Hinzufügen des LSN-Anwendungsprofils die folgenden Parameter fest:
  - IP-Pooling = PAIRED
  - Adress- und Portzuordnung = ENDPOINT-INDEPENDENT
  - Filterung = ENDPOINT-INDEPENDENT
- Erstellen Sie ein RTSP-ALG-Profil und binden Sie das RTSP-ALG-Profil an die LSN-Gruppe

Beispiel-RTSP-ALG-Konfiguration:

Die folgende Beispielkonfiguration zeigt, wie eine einfache LSN-Konfiguration mit einem einzelnen Teilnehmernetzwerk, einer einzelnen LSN-NAT-IP-Adresse und RTSP-ALG-Einstellungen erstellt wird:

```
enable ns feature WL SP LB CS LSN

Done

add lsn pool pool1 -nattype DETERMINISTIC

Done

bind lsn pool pool1 10.102.218.246

Done

add lsn client client1

Done

bind lsn client client1 -network 200.200.200.11 -netmask 255.255.255.0

Done

add lsn appsprofile app1 TCP -ippooling PAIRED -mapping ENDPOINT-
    INDEPENDENT -filtering ENDPOINT-INDEPENDENT

Done

add lsn appsprofile app2 UDP -ippooling PAIRED -mapping ENDPOINT-
    INDEPENDENT -filtering ENDPOINT-INDEPENDENT

Done

bind lsn appsprofile app1 1-65535

Done

bind lsn appsprofile app2 1-65535

Done

add lsn rtspalgprofile rtspalgprofiledefault -rtspIdleTimeout 1000 -
    rtspportrange 554
```



```
38
39 Done
40
41 add lsn group group1 -clientname client1 -nattype DETERMINISTIC -
      portblocksize 512 -rtspalg ENABLED
42
43 Done
44
45 bind lsn group group1 -poolname pool1
46
47 Done
48
49 bind lsn group group1 -appsprofilename app1
50
51 Done
52
53 bind lsn group group1 -appsprofilename app2
54
55 Done
56
57 bind lsn group group1 -rtspalgprofilename rtspalgprofiledefault
58
59 Done
60 <!--NeedCopy-->
```

Application Layer Gateway für IPsec-Protokoll

October 5, 2021

Wenn die Kommunikation zwischen zwei Netzwerkgeräten (z. B. Client und Server) das IPsec-Protokoll verwendet, verwendet der IKE-Datenverkehr (der über UDP liegt) Portfelder, aber Encapsulating Security Payload (ESP) Datenverkehr nicht. Wenn ein NAT-Gerät auf dem Pfad zwei oder mehr Clients an demselben Ziel dieselbe NAT-IP-Adresse (aber unterschiedliche Ports) zuweist, kann das NAT-Gerät den Return ESP-Datenverkehr nicht unterscheiden und ordnungsgemäß weiterleiten. Daher schlägt IPsec-ESP-Datenverkehr auf dem NAT-Gerät fehl.

NAT-Traversal (NAT-T) -fähige IPsec-Endpunkte erkennen das Vorhandensein eines zwischengeschalteten NAT-Geräts während der IKE-Phase 1 und wechseln zum UDP-Port 4500 für alle nachfolgenden IKE- und ESP-Datenverkehr (Verkapselung von ESP in UDP). Ohne NAT-T-Unterstützung auf den Peer-IPsec-Endpunkten wird IPsec-geschützter ESP-Datenverkehr ohne UDP-Kapselung übertragen. Daher schlägt IPsec-ESP-Datenverkehr auf dem NAT-Gerät fehl.

Die Citrix ADC Appliance unterstützt IPsec ALG-Funktionalität (Application Layer Gateway) für große NAT-Konfigurationen. Die IPsec-ALG verarbeitet IPsec-ESP-Datenverkehr und verwaltet Sitzungsinformationen, so dass der Datenverkehr nicht fehlschlägt, wenn die IPsec-Endpunkte NAT-T (UDP-Kapselung des ESP-Datenverkehrs) nicht unterstützen.

Funktionsweise von IPsec ALG

Eine IPsec-ALG überwacht den IKE-Datenverkehr zwischen einem Client und dem Server und ermöglicht nur einen IKE-Phase-2-Nachrichtenaustausch zwischen dem Client und dem Server zu einem bestimmten Zeitpunkt.

Sobald die bidirektionalen ESP-Pakete für einen bestimmten Flow empfangen werden, erstellt die IPsec-ALG eine NAT-Sitzung für diesen bestimmten Flow, sodass nachfolgender ESP-Datenverkehr reibungslos fließen kann. Der ESP-Datenverkehr wird durch Sicherheitsparameterindizes (SPIs) identifiziert, die für einen Fluss und für jede Richtung eindeutig sind. Eine IPsec-ALG verwendet ESP-SPIs anstelle von Quell- und Zielports für die Ausführung großer NAT.

Wenn ein Tor keinen Verkehr erhält, ist ein Zeitabfall. Nach dem Timeout der beiden Tore ist ein weiterer IKE-Phase-2-Austausch zulässig.

IPsec-ALG-Timeouts

IPsec ALG auf einer Citrix ADC Appliance verfügt über drei Timeoutparameter:

- **ESP-Gate-Zeitüberschreitung**. Maximale Zeit, die die Citrix ADC Appliance ein IPsec-ALG-Gate für einen bestimmten Client auf einer bestimmten NAT-IP-Adresse für einen bestimmten Server blockiert, wenn kein bidirektionaler ESP-Datenverkehr zwischen dem Client und dem Server ausgetauscht wird.
- **IKE-Sitzungszeitüberschreitung**. Maximale Zeit, die die Citrix ADC Appliance die IKE-Sitzungsinformationen aufbewahrt, bevor sie entfernt wird, wenn für diese Sitzung kein IKE-Datenverkehr vorhanden ist.
- **ESP-Sitzungszeitüberschreitung**. Maximale Zeit, die Citrix ADC Appliance die ESP-Sitzungsinformationen aufbewahrt, bevor sie entfernt wird, wenn für diese Sitzung kein ESP-Datenverkehr vorhanden ist.

Vor der Konfiguration von IPsec ALG zu berücksichtigende Punkte

Bevor Sie mit der Konfiguration von IPsec ALG beginnen, sollten Sie die folgenden Punkte beachten:

- Sie müssen die verschiedenen Komponenten des IPsec-Protokolls verstehen.
- IPsec ALG wird für DS-Lite und Large Scale NAT64 Konfigurationen nicht unterstützt.
- IPsec ALG wird für den Haarnadel-LSN-Fluss nicht unterstützt.

- IPsec ALG funktioniert nicht mit RNAT Konfigurationen.
- IPsec ALG wird in Citrix ADC Clustern nicht unterstützt.

Konfigurationsschritte

Die Konfiguration von IPsec ALG für großformatige NAT44 auf einer Citrix ADC Appliance umfasst folgende Aufgaben:

- **Erstellen Sie ein LSN-Anwendungsprofil und binden Sie es an die LSN-Konfiguration.** Legen Sie beim Konfigurieren eines Anwendungsprofils die folgenden Parameter fest:
  - Protokoll = UDP
  - IP-Pooling = PAIRED
  - Port=500

Binden Sie das Anwendungsprofil an die LSN-Gruppe einer LSN-Konfiguration. Anweisungen zum Erstellen einer LSN-Konfiguration finden Sie unter Konfigurationsschritte für LSN.

- **Erstellen Sie ein IPsec-ALG-Profil**. Ein IPsec-Profil enthält verschiedene IPsec-Timeouts, wie z. B. IKE-Sitzungszeitüberschreitung, ESP-Sitzungszeitüberschreitung und ESP-Gate-Zeitüberschreitung. Sie binden ein IPsec-ALG-Profil an eine LSN-Gruppe. Ein IPsec-ALG-Profil weist die folgenden Standardeinstellungen auf:
  - IKE-Sitzungszeitüberschreitung = 60 Minuten
  - ESP-Sitzungszeitüberschreitung = 60 Minuten
  - ESP-Gate-Zeitüberschreitung = 30 Sekunden
- **Binden Sie das IPsec-ALG-Profil an die LSN-Konfiguration**. IPsec ALG ist für eine LSN-Konfiguration aktiviert, wenn Sie ein IPsec-ALG-Profil an die LSN-Konfiguration binden. Binden Sie das IPsec-ALG-Profil an die LSN-Konfiguration, indem Sie den IPsec-ALG-Profilparameter auf den Namen des erstellten Profils in der LSN-Gruppe festlegen. Ein IPsec-ALG-Profil kann an mehrere LSN-Gruppen gebunden werden, aber eine LSN-Gruppe kann nur ein IPsec-ALG-Profil haben.

So erstellen Sie ein LSN-Anwendungsprofil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lsn appsprofile <appsprofilename> UDP -ippooling PAIRED
2
3 show lsn appsprofile
4 <!--NeedCopy-->
```


So binden Sie den Zielport mit der Befehlszeilenschnittstelle an das LSN-Anwendungsprofil

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn appsprofile <appsprofilename> <lsnport>

show lsn appsprofile
<!--NeedCopy-->
```

So binden Sie ein LSN-Anwendungsprofil mit der Befehlszeilenschnittstelle an eine LSN-Gruppe

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn group <groupname> -appsprofilename <string>

show lsn group
<!--NeedCopy-->
```

So erstellen Sie ein IPsec-ALG-Profil mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ipsecalg profile <name> [-ikeSessionTimeout <positive_integer>] [-
    espSessionTimeout <positive_integer>] [-espGateTimeout <
    positive_integer>] [-connfailover ( ENABLED | DISABLED)

show ipsecalg profile <name>
<!--NeedCopy-->
```

So binden Sie ein IPsec-ALG-Profil an eine LSN-Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn group <groupname> -poolname <string> - ipsecAlgProfile <string
    >

show lsn group <name>
```



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

So erstellen Sie ein LSN-Anwendungsprofil und binden es mit der GUI an eine LSN-Konfiguration

Navigieren Sie zu **System** > **Large Scale NAT** > **Profile**, klicken Sie auf die Registerkarte **Anwendung**, fügen Sie ein LSN-Anwendungsprofil hinzu und binden Sie es an eine LSN-Gruppe.

So erstellen Sie ein IPsec-ALG-Profil mit der GUI**

Navigieren Sie zu **System** > **Large Scale NAT** > **Profile**, klicken Sie auf **IPSEC ALG** Registerkarte, und fügen Sie dann ein IPsec-ALG-Profil hinzu.

So binden Sie ein IPsec-ALG-Profil mit der GUIan eine LSN-Konfiguration**

1. Navigieren Sie zu **System** > **Large Scale NAT** > **LSN Group**, öffnen Sie die LSN-Gruppe.
2. Klicken Sie **unter Erweiterte Einstellungen**auf **+ IPSEC-ALG-Profil**, um das erstellte IPsec-ALG-Profil an die LSN-Gruppe zu binden.

Beispielkonfiguration

In der folgenden großformatigen NAT44-Beispielkonfiguration ist IPsec ALG für Abonnenten im 192.0.2.0/24-Netzwerk aktiviert. IPsec-ALG-Profil IPSECALGPROFILE-1 mit verschiedenen IPsec-Zeitüberschreitungseinstellungen wird erstellt und ist an LSN-Gruppe LSN-Gruppe -1 gebunden.

Beispielkonfiguration:

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.3-203.0.113.9

```



```
Done

add lsn appsprofile LSN-APPSPROFILE-1 UDP -ippooling PAIRED

Done

bind lsn appsprofile LSN-APPSPROFILE-1 500

Done

add ipsecalg profile  IPSECALGPROFILE-1 -ikeSessionTimeout 45  -
   espSessionTimeout 40  - espGateTimeout 20 -connfailover ENABLED

Done

bind lsn group LSN-GROUP-1 -appsprofilename LSN-APPSPROFILE-1

Done

bind lsn group LSN-GROUP-1 -poolname LSN-POOL-1

Done

bind lsn group LSN-GROUP-1 - ipsecAlgProfile IPSECALGPROFILE-1

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

Protokollierung und Überwachung LSN

October 5, 2021

Sie können LSN-Informationen protokollieren, um Probleme zu diagnostizieren, zu beheben und gesetzliche Anforderungen zu erfüllen. Sie können die Leistung des LSN-Features überwachen, indem Sie LSN-Statistikindikatoren verwenden und aktuelle LSN-Sitzungen anzeigen.

LSN protokollieren

Die Protokollierung von LSN-Informationen ist eine der wichtigen Funktionen, die die ISPs benötigen, um die gesetzlichen Anforderungen zu erfüllen und die Quelle des Datenverkehrs zu einem bestimmten Zeitpunkt zu identifizieren.

Eine Citrix ADC Appliance protokolliert LSN-Zuordnungseinträge und die LSN-Sitzungen, die für jede LSN-Gruppe erstellt oder gelöscht wurden. Sie können die Protokollierung von LSN-Informationen für eine LSN-Gruppe mithilfe der Protokollierungs- und Sitzungsprotokollierungsparameter der LSN-Gruppe steuern. Dies sind Parameter auf Gruppenebene und sind standardmäßig deaktiviert. Die Citrix ADC Appliance protokolliert LSN-Sitzungen für eine LSN-Gruppe nur, wenn Protokollierungs- und Sitzungsprotokollierungsparameter aktiviert sind.

In der folgenden Tabelle wird das Protokollierungsverhalten für eine LSN-Gruppe für verschiedene Einstellungen von Protokollierungs- und Sitzungsprotokollierungsparametern angezeigt.

Protokollierung	Sitzungsprotokollierung	Protokollierungsverhalten
Aktiviert	Aktiviert	Protokolliert LSN-Zuordnungseinträge sowie LSN-Sitzungen.
Aktiviert	Deaktiviert	Protokolliert LSN-Zuordnungseinträge, aber keine LSN-Sitzungen.
Deaktiviert	Aktiviert	Protokolliert weder Zuordnungseinträge noch LSN-Sitzungen.

Eine Protokollmeldung für einen LSN-Zuordnungseintrag besteht aus folgenden Informationen:

- Citrix ADC eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt.
- Zeitstempel
- Eintragstyp (MAPPING)
- Ob der LSN-Zuordnungseintrag erstellt oder gelöscht wurde
- IP-Adresse, Port und Traffic-Domänen-ID des Abonnenten
- NAT IP-Adresse und Port
- Protokollname
- Ziel-IP-Adresse, -Port und -Domänen-ID sind möglicherweise vorhanden, abhängig von den folgenden Bedingungen:
  - Ziel-IP-Adresse und -Port werden für die endpoint-unabhängige Zuordnung nicht protokolliert.
  - Für die Adressenabhängige Zuordnung wird nur die Ziel-IP-Adresse protokolliert. Der Port wird nicht protokolliert.
  - Ziel-IP-Adresse und -Port werden für die Adress-Port-abhängige Zuordnung protokolliert.

Eine Protokollmeldung für eine LSN-Sitzung besteht aus folgenden Informationen:

- Citrix ADC eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt.
- Zeitstempel
- Eintragstyp (SESSION)
- Gibt an, ob die LSN-Sitzung erstellt oder entfernt wird
- IP-Adresse, Port und Traffic-Domänen-ID des Abonnenten
- NAT IP-Adresse und Port
- Protokollname
- Ziel-IP-Adresse, -Port und -Domänen-ID des Datenverkehrs

Die Appliance verwendet ihr vorhandenes Syslog- und Überwachungsprotokoll-Framework, um LSN-Informationen zu protokollieren. Sie müssen die LSN-Protokollierung auf globaler Ebene aktivieren, indem Sie den LSN-Parameter in den zugehörigen NSLOG-Aktionsobjekten und SYLOG-Aktionsobjekten aktivieren. Wenn der Parameter Logging aktiviert ist, generiert die Citrix ADC Appliance Protokollmeldungen im Zusammenhang mit LSN-Zuordnungen und LSN-Sitzungen dieser LSN-Gruppe. Die Appliance sendet diese Protokollmeldungen dann an Server, die mit der NSLOG-Aktion und den SYSLOG-Aktionsobjekten verknüpft sind.

Für die Protokollierung von LSN-Informationen empfiehlt Citrix:

- Protokollieren der LSN-Informationen auf externen Protokollservern statt auf der Citrix ADC Appliance. Die Protokollierung auf externen Servern erleichtert die optimale Leistung, wenn die Appliance große Mengen an LSN-Protokolleinträgen (in der Größenordnung von Millionen) erstellt.
- Verwenden von SYSLOG über TCP oder NSLOG. Standardmäßig verwendet SYSLOG UDP und NSLOG verwendet nur TCP, um Protokollinformationen an die Protokollserver zu übertragen. TCP ist zuverlässiger als UDP für die Übertragung kompletter Daten.

  Hinweis:

  - Die auf der Citrix ADC Appliance generierten SYSLOG werden dynamisch an die externen Protokollserver gesendet.
  - Wenn Sie SYSLOG über TCP verwenden, wenn die TCP-Verbindung ausgefallen ist oder der SYSLOG-Server ausgelastet ist, speichern die Citrix ADC Appliances die Protokolle im Puffer und senden die Daten, sobald die Verbindung aktiv ist.

Weitere Informationen zum Konfigurieren der Protokollierung finden Sie unter Audit-Protokollierung.

Die Konfiguration der LSN-Protokollierung umfasst die folgenden Aufgaben:

- **Konfigurieren der Citrix ADC Appliance für die Protokollierung.** Bei dieser Aufgabe werden verschiedene Entitäten und Parameter der Citrix ADC Appliance erstellt und festgelegt:
  - **Erstellen Sie eine SYSLOG- oder NSLOG-Überwachungskonfiguration**. Das Erstellen einer Überwachungsprotokollierungskonfiguration umfasst die folgenden Aufgaben:

    * Erstellen Sie eine NSLOG- oder SYSLOG-Überwachungsaktion, und aktivieren Sie den LSN-Parameter. Überwachungsaktionen geben die IP-Adressen von Protokollservern an.
    * Erstellen Sie eine SYSLOG- oder NSLOG-Überwachungsrichtlinie, und binden Sie die Überwachungsaktion an die Überwachungsrichtlinie. Überwachungsaktionen geben die IP-Adressen von Protokollservern an. Optional können Sie die Transportmethode für Protokollmeldungen festlegen, die an die externen Protokollserver gesendet werden. Standardmäßig UDP ausgewählt ist, können Sie die Transportmethode als TCP für einen zuverlässigen Transportmechanismus festlegen. Binden Sie die Überwachungsrichtlinie an das System global.
    * Erstellen Sie eine SYSLOG- oder NSLOG-Überwachungsrichtlinie, und binden Sie die Überwachungsaktion an die Überwachungsrichtlinie.
    * Binden Sie die Überwachungsrichtlinie an das System global.
      Hinweis: Aktivieren Sie für eine vorhandene Überwachungsprotokollierungskonfiguration einfach den LSN-Parameter für die Protokollierung von LSN-Informationen auf dem Server, der durch die Überwachungsaktion angegeben wurde.
  - **Aktivieren Sie Protokollierungs- und Sitzungsprotokollierungsparameter.** Aktivieren Sie Protokollierungs- und Sitzungsprotokollierungsparameter entweder beim Hinzufügen von LSN-Gruppen oder nach dem Erstellen der Gruppen. Die Citrix ADC Appliance generiert Protokollmeldungen zu diesen LSN-Gruppen und sendet sie an den Server der Überwachungsaktionen, für die der LSN-Parameter aktiviert ist.
- **Protokollserver konfigurieren.** Diese Aufgabe beinhaltet die Installation von SYSLOG- oder NSLOG-Paketen auf den gewünschten Servern. Diese Aufgabe beinhaltet auch die Angabe der NSIP-Adresse der Citrix ADC Appliance in der Konfigurationsdatei von SYSLOG oder NSLOG. Durch die Angabe der NSIP-Adresse kann der Server die Protokollinformationen identifizieren, die von der Citrix ADC Appliance zum Speichern in einer Protokolldatei gesendet werden.

Weitere Informationen zum Konfigurieren der Protokollierung finden Sie unter Audit-Protokollierung.

SYSLOG-Konfiguration über die Befehlszeilenschnittstelle

So erstellen Sie eine SYSLOG-Serveraktion für die LSN-Protokollierung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel
      <logLevel>... [-transport (TCP)] [-lsn ( ENABLED | DISABLED )]
2 <!--NeedCopy-->
```


So erstellen Sie eine SYSLOG-Serverrichtlinie für die LSN-Protokollierung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add audit syslogPolicy <name> <rule> <action>
<!--NeedCopy-->
```

So binden Sie eine SYSLOG-Serverrichtlinie an das System Global für die LSN-Protokollierung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind system global [<policyName> [-priority <positive_integer>]]
<!--NeedCopy-->
```

SYSLOG-Konfiguration mit dem Konfigurationsdienstprogramm

So konfigurieren Sie eine SYSLOG-Serveraktion für die LSN-Protokollierung mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Systeme** > **Überwachung** > **Syslog**, und fügen Sie auf der Registerkarte Server einen neuen Überwachungsserver hinzu, oder bearbeiten Sie einen vorhandenen Server.
2. Um die LSN-Protokollierung zu aktivieren, wählen Sie die Option **Large Scale NAT-Protokollierung** aus.
3. (Optional) Um SYSLOG über TCP zu aktivieren, wählen Sie die Option **TCP-Protokollierung** .

So konfigurieren Sie eine SYSLOG-Serverrichtlinie für die LSN-Protokollierung mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Systeme** > **Überwachung** > **Syslog**, und fügen Sie auf der Registerkarte **Richtlinien** eine neue Richtlinie hinzu oder bearbeiten Sie eine vorhandene Richtlinie.

So binden Sie eine SYSLOG-Serverrichtlinie an das System Global für die LSN-Protokollierung mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Systeme** > **Überwachung** > **Syslog** .
2. Klicken Sie auf der Registerkarte **Richtlinien** in der Liste **Aktion** auf **Globale Bindungen**, um die globalen Überwachungsrichtlinien zu binden.

NSLOG-Konfiguration über die Befehlszeilenschnittstelle

So erstellen Sie eine NSLOG-Serveraktion für die LSN-Protokollierung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add audit nslogAction <name> <serverIP> [-serverPort <port>] -logLevel
     <logLevel> ... [-lsn ( ENABLED | DISABLED )]
2 <!--NeedCopy-->
```

So erstellen Sie eine NSLOG-Serverrichtlinie für die LSN-Protokollierung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add audit nslogPolicy <name> <rule> <action>
2 <!--NeedCopy-->
```

So binden Sie eine NSLOG-Serverrichtlinie an das System Global für die LSN-Protokollierung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind system global [<policyName>]
2 <!--NeedCopy-->
```

NSLOG-Konfiguration mit dem Konfigurationsdienstprogramm

So konfigurieren Sie eine NSLOG-Serveraktion für die LSN-Protokollierung mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Systeme** > **Überwachung** > **Nslog**, und fügen Sie auf der Registerkarte **Server** einen neuen Überwachungsserver hinzu, oder bearbeiten Sie einen vorhandenen Server.
2. Um die LSN-Protokollierung zu aktivieren, wählen Sie die Option **Large Scale NAT-Protokollierung** aus.

So konfigurieren Sie eine NSLOG-Serverrichtlinie für die LSN-Protokollierung mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Systeme** > **Überwachung** > **Nslog**, und fügen Sie auf der Registerkarte **Richtlinien** eine neue Richtlinie hinzu oder bearbeiten Sie eine vorhandene Richtlinie.

So binden Sie eine NSLOG-Serverrichtlinie an das System Global für die LSN-Protokollierung mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Systeme** > **Auditing** > **Nslog** .
2. Klicken Sie auf der Registerkarte **Richtlinien** in der Liste **Aktion** auf **Globale Bindungen**, um die globalen Überwachungsrichtlinien zu binden.

Beispiel

Die folgende Konfiguration gibt zwei SYSLOG- und zwei NSLOG-Server zum Speichern von Protokolleinträgen einschließlich LSN-Protokollen an. Die LSN-Protokollierung ist für die LSN-Gruppen LSN-GROUP-2 und LSN-GROUP-3 konfiguriert.

Die Citrix ADC Appliance generiert Protokollmeldungen im Zusammenhang mit LSN-Zuordnungen und LSN-Sitzungen dieser LSN-Gruppen und sendet sie an die angegebenen Protokollserver.

```
add audit syslogAction SYS-ACTION-1 198.51.101.10 -logLevel ALL -lsn
    ENABLED
Done
add audit syslogPolicy SYSLOG-POLICY-1 ns_true SYS-ACTION-1
Done
bind system global SYSLOG-POLICY-1
Done

add audit syslogAction SYS-ACTION-2 198.51.101.20 -logLevel ALL -lsn
    ENABLED
Done
add audit syslogPolicy SYSLOG-POLICY-2 ns_true SYS-ACTION-2
Done
bind system global SYSLOG-POLICY-2
Done

add audit nslogAction NSLOG-ACTION-1 198.51.101.30 -logLevel ALL -lsn
    ENABLED
Done
add audit nslogPolicy NSLOG-POLICY-1 ns_true NSLOG-ACTION-1
Done
```



```
19 bind system global NSLOG-POLICY-1
20 Done
21 add audit nslogAction NSLOG-ACTION-2 198.51.101.40 -logLevel ALL -lsn
      ENABLED
22 Done
23 add audit nslogPolicy NSLOG-POLICY-2 ns_true NSLOG-ACTION-2
24 Done
25 bind system global NSLOG-POLICY-2
26 Done
27
28 add lsn group LSN-GROUP-3 -clientname LSN-CLIENT-2  - logging ENABLED  -
      sessionLogging ENABLED
29 Done
30 set lsn group LSN-GROUP-2   - logging ENABLED  - sessionLogging ENABLED
31 Done
32 <!--NeedCopy-->
```

Die folgende Konfiguration gibt die SYSLOG-Konfiguration für das Senden von Protokollmeldungen an
den externen SYSLOG-Server 192.0.2.10 unter Verwendung von TCP an.

```
1 add audit syslogAction SYS-ACTION-1 192.0.2.10 -logLevel ALL -transport
     TCP
2 Done
3
4 add audit syslogPolicy SYSLOG-POLICY-1 ns_true SYS-ACTION-1
5 Done
6
7 bind system global SYSLOG-POLICY-1
8 Done
9 <!--NeedCopy-->
```

In der folgenden Tabelle werden Beispieleinträge für LSN-Protokolle jedes Typs angezeigt, der auf den konfigurierten Protokollservern gespeichert ist. Diese LSN-Protokolleinträge werden von einer Citrix ADC Appliance generiert, deren NSIP-Adresse 10.102.37.115 lautet.

LSN-Protokolleintragstyp	Beispielprotokolleintrag
Erstellung von LSN-Sitzungen	Local4.Informational 10.102.37.115 08/05/2014:09:59:48 GMT 0-PPE-0 : LSN LSN_SESSION 2581750 : SESSION CREATED Client IP:Port:TD 192.0.2.10: 15136:0, NatIP:NatPort 203.0.113.6: 6234, Destination IP:Port:TD 198.51.100.9: 80:0, Protocol: TCP
Löschung der LSN-Sitzung	Local4.Informational 10.102.37.115 08/05/2014:10:05:12 GMT 0-PPE-0 : LSN LSN_SESSION 3871790 : SESSION DELETED Client IP:Port:TD 192.0.2.11: 15130:0, NatIP:NatPort 203.0.113.6: 7887, Destination IP:Port:TD 198.51.101.2:80:0, Protocol: TCP
Erstellung von LSN-Zuordnungen	Local4.Informational 10.102.37.115 08/05/2014:09:59:47 GMT 0-PPE-0 : LSN LSN_MAPPING 2581580 : EIM CREATED Client IP:Port 192.0.2.15: 14567, NatIP:NatPort 203.0.113.5: 8214, Protocol: TCP
Löschung der LSN-Zuordnung	Local4.Informational 10.102.37.115 08/05/2014:10:05:12 GMT 0-PPE-0 : LSN LSN_MAPPING 3871700 : EIM DELETED Client IP:Port 192.0.3.15: 14565, NatIP:NatPort 203.0.113.11: 8217, Protocol: TCP

Minimale Protokollierung

Deterministische LSN-Konfigurationen und dynamische LSN-Konfigurationen mit Portblock reduzieren das LSN-Protokollvolumen erheblich. Für diese beiden Konfigurationstypen weist die Citrix ADC Appliance einem Abonnenten eine NAT-IP-Adresse und einen Block von Ports zu. Die Citrix ADC Appliance generiert zum Zeitpunkt der Zuweisung an einen Abonnenten eine Protokollnachricht für einen Portblock. Die Citrix ADC Appliance generiert auch eine Protokollmeldung, wenn eine NAT-IP-Adresse und ein Portblock freigegeben werden. Bei einer Verbindung kann ein Teilnehmer nur anhand seiner zugeordneten NAT-IP-Adresse und des Portblocks identifiziert werden. Aus diesem Grund protokolliert die Citrix ADC Appliance keine erstellten oder gelöschten LSN-Sitzungen. Außerdem protokolliert die Appliance weder einen Zuordnungseintrag, der für eine Sitzung erstellt wurde, noch wenn der Zuordnungseintrag entfernt wird.

Die minimale Protokollierungsfunktion für deterministische LSN-Konfigurationen und dynamische

LSN-Konfigurationen mit Portblock ist standardmäßig aktiviert und es gibt keine Möglichkeit, sie zu deaktivieren. Mit anderen Worten: Die Citrix ADC Appliance führt automatisch minimale Protokollierung für deterministische LSN-Konfigurationen und dynamische LSN-Konfigurationen mit Portblock durch. Es ist keine Option zum Deaktivieren dieser Funktion verfügbar. Die Appliance sendet die Protokollmeldungen an alle konfigurierten Protokollserver.

Eine Protokollmeldung für jeden Portblock besteht aus folgenden Informationen:

- NSIP-Adresse der Citrix ADC Appliance
- Zeitstempel
- Eintragstyp als DETERMINISTIC oder PORTBLOCK
- Gibt an, ob ein Portblock zugewiesen ist oder freigegeben wird
- IP-Adresse des Teilnehmers und zugewiesene NAT-IP-Adresse und Portblock
- Protokollname

Minimale Protokollierung für deterministische LSN-Konfiguration

Betrachten Sie ein Beispiel für eine einfache deterministische LSN-Konfiguration für vier Abonnenten mit der IP-Adresse 192.0.17.1, 192.0.17.2, 192.0.17.3 und 192.0.17.4.

In dieser LSN-Konfiguration ist die Portblockgröße auf 32768 und LSN NAT IP-Adresspool hat IP-Adressen im Bereich 203.0.113.19-203.0.113.23.

```
1  add lsn client LSN-CLIENT-7
2  Done
3  bind lsn client LSN-CLIENT-7 -network 192.0.17.0 -netmask
       255.255.255.253
4  Done
5  add lsn pool LSN-POOL-7 -nattype DETERMINISTIC
6  Done
7  bind lsn pool LSN-POOL-7 203.0.113.19-203.0.113.23
8  Done
9  add lsn group LSN-GROUP-7 -clientname LSN-CLIENT-7 -nattype
       DETERMINISTIC -portblocksize 32768
10 Done
11 bind lsn group LSN-GROUP-7 -poolname LSN-POOL-7
12 Done
13 <!--NeedCopy-->
```

Die Citrix ADC Appliance weist sequenziell aus dem LSN NAT-IP-Pool und auf der Grundlage der festgelegten Portblockgröße eine LSN NAT-IP-Adresse und einen Block von Ports zu jedem Abonnenten. Der erste Block von Ports (1024-33791) an der beginnenden NAT-IP-Adresse (203.0.113.19) wird der IP-Adresse des beginnenden Teilnehmers (192.0.17.1) zugewiesen. Der nächste Bereich von Ports wird

dem nächsten Abonnenten zugewiesen usw., bis die NAT-Adresse nicht über genügend Ports für den nächsten Abonnenten verfügt. Zu diesem Zeitpunkt wird der erste Portblock auf der nächsten NAT-IP-Adresse dem Abonnenten zugewiesen usw. Die Appliance protokolliert die NAT-IP-Adresse und den für jeden Abonnenten zugewiesenen Port.

Die Citrix ADC Appliance protokolliert keine für diese Abonnenten erstellten oder gelöschten LSN-Sitzungen. Die Appliance generiert die folgenden Protokollmeldungen für die LSN-Konfiguration.

```
1) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201453 0 :  Dtrstc ALLOC Client 12.0.0.241,
   NatInfo 50.0.0.2:59904 to 60415
2) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201454 0 :  Dtrstc ALLOC Client 12.0.0.242,
   NatInfo 50.0.0.2:60416 to 60927
3) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201455 0 :  Dtrstc ALLOC Client 12.0.0.243,
   NatInfo 50.0.0.2:60928 to 61439
4) 03/23/2015:00:30:56 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201455 0 :  Dtrstc ALLOC Client 12.0.0.243,
   NatInfo 50.0.0.2:60928 to 61439
<!--NeedCopy-->
```

Wenn Sie die LSN-Konfiguration entfernen, werden die zugewiesene NAT-IP-Adresse und der Port Block von jedem Abonnenten freigegeben. Die Appliance protokolliert die NAT-IP-Adresse und den Block von Ports, die von jedem Abonnenten freigegeben werden. Die Appliance generiert die folgenden Protokollmeldungen für jeden Abonnenten, wenn Sie die LSN-Konfiguration entfernen.

```
1) 03/23/2015:00:33:57 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201706 0 :  Dtrstc FREE Client 12.0.0.238,
   NatInfo 50.0.0.2:58368 to 58879
2) 03/23/2015:00:33:57 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201707 0 :  Dtrstc FREE Client 12.0.0.239,
   NatInfo 50.0.0.2:58880 to 59391
3) 03/23/2015:00:33:57 GMT  Informational 0-PPE-0 : default LSN
   LSN_DETERMINISTIC 79201708 0 :  Dtrstc FREE Client 12.0.0.240,
   NatInfo 50.0.0.2:59392 to 59903
<!--NeedCopy-->
```


Minimale Protokollierung für dynamische LSN-Konfiguration mit Portblock

Betrachten Sie ein Beispiel für eine einfache dynamische LSN-Konfiguration mit Portblock für jeden Teilnehmer im Netzwerk 192.0.2.0/24. In dieser LSN-Konfiguration ist die Portblockgröße auf 1024 festgelegt und der LSN NAT IP-Adresspool hat IP-Adressen im Bereich 203.0.113.3-203.0.113.4.

```
set lsn parameter -memLimit 4000
Done
add lsn client LSN-CLIENT-1
Done
bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0
Done
add lsn pool LSN-POOL-1
Done
bind lsn pool LSN-POOL-1 203.0.113.3-203.0.113.4
Done
add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1 -portblocksize 1024
Done
bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
Done
<!--NeedCopy-->
```

Die Citrix ADC Appliance weist einem Teilnehmer eine zufällige NAT-IP-Adresse und einen Block von Ports aus dem LSN NAT-IP-Pool und auf der Grundlage der festgelegten Portblockgröße zu, wenn er eine Sitzung zum ersten Mal initiiert. Citrix ADC protokolliert die NAT-IP-Adresse und den Block der Ports, die diesem Abonnenten zugewiesen sind. Die Appliance protokolliert keine LSN-Sitzung, die für diesen Abonnenten erstellt oder gelöscht wurde. Wenn alle Ports (für die Sitzungen verschiedener Teilnehmer) vom zugewiesenen Portblock des Teilnehmers zugewiesen sind, weist die Appliance dem Abonnenten eine neue zufällige NAT-IP-Adresse und einen Port-Block für zusätzliche Sitzungen zu. Der Citrix ADC protokolliert alle NAT-IP-Adresse und -Anschlussblöcke, die einem Abonnenten zugewiesen sind.

Die Appliance generiert die folgende Protokollmeldung, wenn der Teilnehmer mit der IP-Adresse 192.0.2.1 eine Sitzung initiiert. Die Protokollmeldung zeigt an, dass die Appliance dem Abonnenten die NAT-IP-Adresse 203.0.113.3 und den Portblock 1024-2047 zugewiesen hat.

```
03/23/2015:00:07:12 GMT  Informational 0-PPE-3 : default LSN
   LSN_PORTBLOCK 106725793 0 :  Portblock ALLOC Client 12.0.2.72,
   NatInfo 203.0.113.3:1024 to 2047, Proto:TCP
<!--NeedCopy-->
```


Sobald keine weiteren Sitzungen mehr vorhanden sind, die die zugewiesene NAT-IP-Adresse und einen der Ports im zugewiesenen Portblock verwenden, werden die zugewiesene NAT-IP-Adresse und der Port Block vom Abonnenten freigegeben. Citrix ADC protokolliert, dass die NAT-IP-Adresse und der Block von Ports vom Abonnenten freigegeben werden. Die Appliance generiert die folgenden Protokollmeldungen für den Abonnenten mit der IP-Adresse 192.0.2.1, wenn keine weiteren Sitzungen mehr übrig sind, die die zugewiesene NAT-IP-Adresse (203.0.113.3) und einen Port aus dem zugewiesenen Portblock (1024-2047) verwenden. Die Protokollmeldung zeigt, dass die NAT-IP-Adresse und der Portblock vom Abonnenten freigegeben werden.

```
1 03/23/2015:00:11:09 GMT Informational 0-PPE-3 : default LSN
     LSN_PORTBLOCK 106814342 0 :  Portblock FREE Client 12.0.3.122,
     NatInfo 203.0.113.3: 1024 to 2047, Proto:TC
2 <!--NeedCopy-->
```

Lastenausgleich SYSLOG-Server

Die Citrix ADC Appliance sendet ihre SYSLOG-Ereignisse und -Nachrichten an alle konfigurierten externen Protokollserver. Dies führt zur Speicherung redundanter Nachrichten und erschwert Systemadministratoren die Überwachung. Um dieses Problem zu beheben, bietet die Citrix ADC Appliance Lastausgleichsalgorithmen, die die SYSLOG-Nachrichten zwischen den externen Protokollservern für eine bessere Wartung und Leistung ausgleichen können. Die unterstützten Load Balancing-Algorithmen umfassen RoundRobin, LeastBandWidth, CustomLoad, LeastConnection, LeastPackets und AuditLogHash.

Lastenausgleich von SYSLOG-Servern über die Befehlszeilenschnittstelle

Fügen Sie einen Dienst hinzu, und geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGUDP an.

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

Fügen Sie einen virtuellen Lastausgleichsserver hinzu, geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGTCP an und Lastausgleichsmethode als AUDITLOGHASH an.

```
1 add lb vserver <name> <serviceType (SYSLOGTCP | SYSLOGUDP)> [-lbMethod
     <AUDITLOGHASH>]
2 <!--NeedCopy-->
```


Bing des Dienstes an den virtuellen Lastausgleichsserver.

```
Bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Fügen Sie eine SYSLOG-Aktion hinzu, und geben Sie den Namen des Lastausgleichsservers an, der SYSLOGTCP oder SYSLOGUDP als Diensttyp enthält.

```
add syslogaction <name> <serverIP> [-lbVserverName <string>] [-logLevel
    <logLevel>]
<!--NeedCopy-->
```

Fügen Sie eine SYSLOG-Richtlinie hinzu, indem Sie die Regel und die Aktion angeben.

```
add syslogpolicy <name> <rule> <action>
<!--NeedCopy-->
```

Binden Sie die SYSLOG-Richtlinie an das System global, damit die Richtlinie wirksam wird.

```
bind system global <policyName>
<!--NeedCopy-->
```

Lastenausgleich von SYSLOG-Servern mit dem Konfigurationsdienstprogramm

1. Fügen Sie einen Dienst hinzu, und geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGUDP an.

   Navigieren Sie zu Traffic Management > Services, klicken Sie auf Hinzufügen und wählen Sie SYLOGTCP oder SYSLOGUDP als Protokoll aus.

2. Fügen Sie einen virtuellen Lastausgleichsserver hinzu, geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGTCP an und Lastausgleichsmethode als AUDITLOGHASH an.

   Navigieren Sie zu Traffic Management > Virtuelle Server, klicken Sie auf Hinzufügen und wählen Sie SYLOGTCP oder SYSLOGUDP als Protokoll aus.

3. Bing des Dienstes an den virtuellen Lastausgleichsserver an den Dienst.

   Bing des Dienstes an den virtuellen Lastausgleichsserver.

   Navigieren Sie zu Traffic Management > Virtuelle Server, wählen Sie einen virtuellen Server aus und wählen Sie dann in der Load Balancing-Methode die AUDITLOGHASH aus.

4. Fügen Sie eine SYSLOG-Aktion hinzu, und geben Sie den Namen des Lastausgleichsservers an, der SYSLOGTCP oder SYSLOGUDP als Diensttyp enthält.

   Navigieren Sie zu System > Überwachung, klicken Sie auf Server und fügen Sie einen Server hinzu, indem Sie LB Vserver Option inServers auswählen.

5. Fügen Sie eine SYSLOG-Richtlinie hinzu, indem Sie die Regel und die Aktion angeben.

   Navigieren Sie zu System > Syslog, klicken Sie auf Richtlinien und fügen Sie eine SYSLOG-Richtlinie hinzu.

6. Binden Sie die SYSLOG-Richtlinie an das System global, damit die Richtlinie wirksam wird.

   Navigieren Sie zu System > Syslog, wählen Sie eine SYSLOG-Richtlinie aus und klicken Sie auf Aktion, und klicken Sie dann auf Globale Bindungen und binden Sie die Richtlinie an system global.

Beispiel:

Die folgende Konfiguration legt den Lastausgleich von SYSLOG-Nachrichten unter den externen Protokollservern fest, wobei die AUDITLOGHASH als Lastausgleichsmethode verwendet wird. Die Citrix ADC Appliance generiert SYSLOG-Ereignisse und Meldungen, die zwischen den Diensten, service1, service2 und Service 3 geladen werden.

```
add service service1 192.0.2.10 SYSLOGUDP 514
Done

add service service2 192.0.2.11 SYSLOGUDP 514
Done

add service service3 192.0.2.11 SYSLOGUDP 514
Done

add lb vserver lbvserver1 SYSLOGUDP -lbMethod AUDITLOGHASH
Done

bind lb vserver lbvserver1 service1
Done

bind lb vserver lbvserver1 service2
Done

bind lb vserver lbvserver1 service3
Done

add syslogaction sysaction1 -lbVserverName lbvserver1 -logLevel All
```



```
Done

add syslogpolicy syspol1 ns_true sysaction1
Done

bind system global syspol1
Done
<!--NeedCopy-->
```

Protokollieren von HTTP-Header-Informationen

Die Citrix ADC-Appliance kann nun Anforderungsheader-Informationen einer HTTP-Verbindung protokollieren, die die LSN-Funktionalität des Citrix ADC verwendet. Die folgenden Header-Informationen eines HTTP-Anforderungspakets können protokolliert werden:

- URL, für die die HTTP-Anforderung bestimmt ist.
- HTTP-Methode, die in der HTTP-Anforderung angegeben ist.
- HTTP-Version, die in der HTTP-Anforderung verwendet wird.
- IP-Adresse des Teilnehmers, der die HTTP-Anforderung gesendet hat.

Die HTTP-Header-Protokolle können von ISPs verwendet werden, um die Trends im Zusammenhang mit dem HTTP-Protokoll unter einem Satz ein Abonnenten sehen. Beispielsweise kann ein ISP diese Funktion verwenden, um die beliebtesten Websites unter einer Gruppe von Abonnenten zu ermitteln.

Ein HTTP-Header-Protokollprofil ist eine Sammlung von HTTP-Header-Attributen (z. B. URL und HTTP-Methode), die für die Protokollierung aktiviert oder deaktiviert werden können. Das HTTP-Header-Protokollprofil wird dann an eine LSN-Gruppe gebunden. Die Citrix ADC Appliance protokolliert dann HTTP-Header-Attribute, die im gebundenen HTTP-Header-Protokollprofil für die Protokollierung aktiviert sind, für alle HTTP-Anforderungen in Bezug auf die LSN-Gruppe. Die Appliance sendet dann die Protokollmeldungen an die konfigurierten Protokollserver.

Ein HTTP-Header-Protokollprofil kann an mehrere LSN-Gruppen gebunden werden, aber eine LSN-Gruppe kann nur ein HTTP-Header-Protokollprofil haben.

So erstellen Sie ein HTTP-Header-Protokollprofil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn httphdrlogprofile <httphdrlogprofilename> [-logURL ( ENABLED |
    DISABLED )] [-logMethod ( ENABLED | DISABLED )] [-logVersion (
    ENABLED | DISABLED )] [-logHost ( ENABLED | DISABLED )]

```



```
show lsn httphdrlogprofile
<!--NeedCopy-->
```

So binden Sie ein HTTP-Header-Protokollprofil mit der Befehlszeilenschnittstelle an eine LSN-Gruppe

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn group <groupname> -httphdrlogprofilename <string>

show lsn group <groupname>
<!--NeedCopy-->
```

Beispiel

Im folgenden Beispiel einer LSN-Konfiguration ist HTTP-Header-Protokollprofil HTTP-Header-Log-1 an LSN-Gruppe LSN-GROUP-1 gebunden. Das Protokollprofil hat alle HTTP-Attribute (URL, HTTP-Methode, HTTP-Version und HOST-IP-Adresse) für die Protokollierung aktiviert, so dass alle diese Attribute für alle HTTP-Anforderungen von Abonnenten (im Netzwerk 192.0.2.0/24) in Bezug auf die LSN-Gruppe protokolliert werden.

```
add lsn httphdrlogprofile HTTP-HEADER-LOG-1
Done

set lsn parameter -memLimit 4000
Done

add lsn client LSN-CLIENT-1
Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0
Done

add lsn pool LSN-POOL-1
Done

bind lsn pool LSN-POOL-1 203.0.113.3-203.0.113.4
Done

```



```
add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1 -portblocksize 1024
Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1
Done

bind lsn group  LSN-GROUP-1  -httphdrlogprofilename HTTP-HEADER-LOG-1
Done
<!--NeedCopy-->
```

Citrix ADC generiert die folgende HTTP-Header-Protokollmeldung, wenn einer der zum LSN-Konfigurationsbeispiel gehörenden Abonnenten eine HTTP-Anforderung sendet.

Die Protokollnachricht sagt uns, dass ein Client mit der IP-Adresse 192.0.2.33 eine HTTP-Anforderung an URL example.com mit der HTTP-Methode GET und HTTP-Version 1.1 sendet.

```
03/19/2015:16:24:04 GMT  Informational 0-PPE-1 : default LSN Message 59
     0 :  "LSN Client IP:TD 10.102.37.118:0 URL: example.com Host:
    192.0.2.33 Version: HTTP1.1 Method: GET"
<!--NeedCopy-->
```

Protokollieren von MSISDN-Informationen

Eine Mobile Station Integrated Subscriber Directory Number (MSISDN) ist eine Telefonnummer, die einen Teilnehmer in mehreren Mobilfunknetzen eindeutig identifiziert. Der MSISDN ist mit einem Ländercode und einem nationalen Bestimmungscode verknüpft, der den Betreiber des Teilnehmers identifiziert.

Sie können eine Citrix ADC Appliance so konfigurieren, dass sie MSISDNs in LSN-Protokolleinträgen für Abonnenten in Mobilfunknetzen einschließt. Das Vorhandensein von MSISDNs in den LSN-Protokollen hilft dem Administrator bei einer schnelleren und präzisen Rückverfolgung eines mobilen Teilnehmers, der gegen eine Richtlinie oder ein Gesetz verstoßen hat oder dessen Informationen von gesetzlichen Abfangstellen verlangt werden.

Die folgenden LSN-Beispielprotokolleinträge enthalten MSISDN-Informationen für eine Verbindung von einem mobilen Abonnenten in einer LSN-Konfiguration. Die Protokolleinträge zeigen, dass ein mobiler Abonnent, dessen MSISDN E 164:5556543210 ist, mit Ziel IP verbunden wurde: Port 23.0.0.1:80 über die NAT IP: Port 203.0.113.3:45195.

Protokolleintragstyp	Beispielprotokolleintrag
Erstellung von LSN-Sitzungen	Oct 14 15:37:30 10.102.37.77 10/14/2015:10:08:14 GMT 0-PPE-6 : default LSN LSN_SESSION 25012 0 : SESSION CREATED E164:5556543210 Client IP:Port:TD 192.0.2.50:4649:0, NatIP:NatPort 203.0.113.3:45195, Destination IP:Port:TD 23.0.0.1:0:0, Protocol: TCP
Erstellung von LSN-Zuordnungen	Oct 14 15:37:30 10.102.37.77 10/14/2015:10:08:14 GMT 0-PPE-6 : default LSN LSN_ADDR_MAPPING 25013 0 : ADM CREATED E164:5556543210 Client IP:Port:TD 192.0.2.50:4649:0, NatIP:NatPort 203.0.113.3:45195, Destination IP:Port:TD 23.0.0.1:0:0, Protocol: TCP
Löschung der LSN-Sitzung	Oct 14 15:40:30 10.102.37.77 10/14/2015:10:11:14 GMT 0-PPE-6 : default LSN LSN_SESSION 25012 0 : SESSION CREATED E164:5556543210 Client IP:Port:TD 192.0.2.50:4649:0, NatIP:NatPort 203.0.113.3:45195, Destination IP:Port:TD 23.0.0.1:0:0, Protocol: TCP
LSN-Zuordnung	Oct 14 15:40:30 10.102.37.77 10/14/2015:10:11:14 GMT 0-PPE-6 : default LSN LSN_ADDR_MAPPING 25013 0 : ADM CREATED E164:5556543210 Client IP:Port:TD 192.0.2.50:4649:0, NatIP:NatPort 203.0.113.3:45195, Destination IP:Port:TD 23.0.0.1:0:0, Protocol: TCP

Führen Sie die folgenden Aufgaben zum Einschließen von MSISDN-Informationen in LSN-Protokollen durch

- **Erstellen Sie ein LSN-Protokollprofil**. Ein LSN-Protokollprofil enthält den Protokollabonnentenidentifikationsparameter, der angibt, ob die MSISDN-Informationen in die LSN-Protokolle einer LSN-Konfiguration aufgenommen werden sollen. Aktivieren Sie beim Erstellen des LSN-Protokollprofils den Parameter für Protokollabonnenten.
- **Binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration**. Binden Sie das erstellte LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie

den Parameter Protokollprofilname auf den erstellten LSN-Protokollprofilnamen festlegen. Anweisungen zum Konfigurieren von Large Scale NAT finden Sie unter Konfigurationsschritte für LSN.

So erstellen Sie ein LSN-Protokollprofil mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn logprofile <logprofilename -logSubscriberID ( ENABLED |
   DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

So binden Sie ein LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Beispielkonfiguration:

In diesem Beispiel der LSN-Konfiguration ist für das LSN-Protokollprofil der Protokollabonnentenidentifikationsparameter aktiviert. Das Profil ist an die LSN-Gruppe LSN-GROUP-9 gebunden. MSISDN-Informationen sind in der LSN-Sitzung und LSN-Mapping-Protokolle für Verbindungen von mobilen Abonnenten enthalten (im Netzwerk 192.0.2.0/24).

```
add lsn logprofile  LOG-PROFILE-MSISDN-9   -logSubscriberID ENABLED

Done
add lsn client LSN-CLIENT-9

Done
bind lsn client LSN-CLIENT-9 -network 192.0.2.0 -netmask 255.255.255.0

Done
```



```
add lsn pool LSN-POOL-9

Done
bind lsn pool LSN-POOL-9 203.0.113.3-203.0.113.4

Done
add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9

Done
bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9

Done
bind lsn group  LSN-GROUP-9  -logprofilename LOG-PROFILE-MSISDN-9

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

Aktuelle LSN-Sitzungen anzeigen

Sie können die aktuellen LSN-Sitzungen zum Erkennen unerwünschter oder ineffizienter LSN-Sitzungen auf der Citrix ADC Appliance anzeigen. Sie können alle oder einige LSN-Sitzungen anhand von Selektionsparametern anzeigen.

Hinweis: Wenn mehr als eine Million LSN-Sitzungen auf der Citrix ADC Appliance vorhanden sind, empfiehlt Citrix die Anzeige ausgewählter LSN-Sitzungen statt aller mithilfe der Auswahlparameter.

Konfiguration über die Befehlszeilenschnittstelle

So zeigen Sie alle LSN-Sitzungen mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show lsn session
<!--NeedCopy-->
```

So zeigen Sie selektive LSN-Sitzungen mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
show lsn session [-clientname <string>] [-network <ip_addr> [-netmask <
    netmask>] [-td <positive_integer>]] [-natIP <ip_addr> [-natPort <
    port>]]
<!--NeedCopy-->
```

Beispiel

So zeigen Sie alle LSN-Sitzungen an, die auf einem Citrix ADC vorhanden sind

```
> show lsn session
        SubscrIP            SubscrPort      SubscrTD              DstIP                    DstPort DstTD     NatIP NatPort Proto   Dir
1.      192.0.2.10          15136           0             198.51.100.9          80          0       203.0.113.6     6234          TCP     OUT
2.      192.0.2.11          15130           0             198.51.101.2          80          0       203.0.113.6     7887          TCP     OUT
3.      192.0.2.12          16136           0             198.51.100.3          80          0       203.0.113.6     9807          TCP     OUT
4.      192.0.2.13          18148           0             198.51.101.6          80          0       203.0.113.6     4657          TCP     OUT
5.      192.0.2.14          13560           0             198.51.101.7          80          0       203.0.113.7     9341          TCP     OUT
6.      192.0.2.15          14567           0             198.51.100.8          80          0       203.0.113.5     8214          TCP     OUT
7.      192.0.2.15          16890           0             198.51.101.1          80          0       203.0.113.5     8214          TCP     OUT
8.      192.0.2.16          12345           0             198.51.102.9          80          0       203.0.113.5     1678          TCP     OUT
9.      192.0.2.19          19876           0             198.51.103.8          80          0       203.0.113.5     1567          TCP     OUT
10.     192.0.2.20          10989           0             198.51.104.19         80          0       203.0.113.11    1343          TCP     OUT
11.     192.0.3.13          18149           0             198.51.101.61         80          0       203.0.113.11    4653          TCP     OUT
12.     192.0.3.14          13510           0             198.51.101.74         80          0       203.0.113.11    9344          TCP     OUT
13.     192.0.3.15          14565           0             198.51.100.82         80          0       203.0.113.11    8217          TCP     OUT
14.     192.0.3.15          16899           0             198.51.101.12         80          0       203.0.113.11    8219          TCP     OUT
15.     192.0.3.16          12343           0             198.51.102.99         80          0       203.0.113.11    1673          TCP     OUT

Done
```

So zeigen Sie alle LSN-Sitzungen an, die sich auf eine LSN-Client-Entität LSN-CLIENT-2 beziehen

```
> show lsn session -clientname LSN-CLIENT-2
        SubscrIP            SubscrPort      SubscrTD              DstIP                    DstPort DstTD     NatIP NatPort Proto   Dir
1.      192.0.2.10          15136           0             198.51.100.9          80          0       203.0.113.6     6ß234         TCP     OUT
2.      192.0.2.11          15130           0             198.51.101.2          80          0       203.0.113.6     7887          TCP     OUT
3.      192.0.2.12          16136           0             198.51.100.3          80          0       203.0.113.6     9807          TCP     OUT
4.      192.0.2.13          18148           0             198.51.101.6          80          0       203.0.113.6     4657          TCP     OUT
5.      192.0.2.14          13560           0             198.51.101.7          80          0       203.0.113.7     9341          TCP     OUT
6.      192.0.2.15          14567           0             198.51.100.8          80          0       203.0.113.5     8214          TCP     OUT
7.      192.0.2.15          16890           0             198.51.101.1          80          0       203.0.113.5     8214          TCP     OUT
8.      192.0.2.16          12345           0             198.51.102.9          80          0       203.0.113.5     1678          TCP     OUT
9.      192.0.2.19          19876           0             198.51.103.8          80          0       203.0.113.5     1567          TCP     OUT
10.     192.0.2.20          10989           0             198.51.104.19         80          0       203.0.113.11    1343          TCP     OUT

Done
```

So zeigen Sie alle LSN-Sitzungen an, die 203.0.113.5 als NAT-IP-Adresse verwendet

```
> show lsn session –natIP 203.0.113.5
SubscrIP            SubscrPort      SubscrTD        DstIP                   DstPort DstTD     NatIP NatPort Proto   Dir
1.      192.0.2.15          14567           0             198.51.100.8          80          0       203.0.113.5     8214          TCP     OUT
2.      192.0.2.15          16890           0             198.51.101.1          80          0       203.0.113.5     8214          TCP     OUT
3.      192.0.2.16          12345           0             198.51.102.9          80          0       203.0.113.5     1678          TCP     OUT
4.      192.0.2.19          19876           0             198.51.103.8          80          0       203.0.113.5     1567          TCP     OUT
Done
```

Konfiguration mit dem Konfigurationsdienstprogramm

So zeigen Sie alle oder ausgewählte LSN-Sitzungen mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu System > Large Scale NAT > Sessions, und klicken Sie auf die Registerkarte NAT44.
2. Klicken Sie auf Suchen, um LSN-Sitzungen basierend auf Auswahlparametern anzuzeigen.

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- lsn-Sitzunganzeigen
  - clientname

    Name der LSN-Client-Entität. Maximale Länge: 127
  - Netzwerk

    IP-Adresse oder Netzwerkadresse des Teilnehmers.
  - Netzmaske

    Subnetzmaske für die IP-Adresse, die durch den Netzwerkparameter angegeben wird.

    Standardwert: 255.255.255.255
  - td

    Verkehrsdomänen-ID der LSN-Client-Entität.

    Standardwert: 0

    Mindestwert: 0

    maximaler Wert: 4094
  - natIP

    Zugeordnete NAT-IP-Adresse, die in LSN-Sitzungen verwendet wird.

LSN-Statistiken anzeigen

Sie können Statistiken zum LSN-Feature anzeigen, um die Leistung des LSN-Features auszuwerten oder Probleme zu beheben. Sie können eine Zusammenfassung der Statistiken des LSN-Features oder einer bestimmten LSN-Gruppe anzeigen. Die statistischen Leistungsindikatoren spiegeln Ereignisse seit dem letzten Neustart der Citrix ADC Appliance wider. Alle diese Leistungsindikatoren werden auf 0 zurückgesetzt, wenn die Citrix ADC Appliance neu gestartet wird.

So zeigen Sie alle LSN-Statistiken mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 stat lsn
2 <!--NeedCopy-->
```


So zeigen Sie Statistiken für eine angegebene LSN-Gruppe mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat lsn group [<groupname>]
<!--NeedCopy-->
```

Beispiel

```
> stat lsn

Large Scale NAT statistics
                                                    Rate(/s)
                                                       Total
LSN TCP Received Packets                              0
    40
LSN TCP Received Bytes                                0
    3026
LSN TCP Transmitted Packets                           0
    40
LSN TCP Transmitted Bytes                             0
    3026
LSN TCP Dropped Packets                               0
                          0
LSN TCP Current Sessions                              0
                          0
LSN UDP Received Packets                              0
                          0
LSN UDP Received Bytes                                0
                          0
LSN UDP Transmitted Packets                           0
                          0
LSN UDP Transmitted Bytes                             0
                          0
LSN UDP Dropped Packets                               0
                          0
LSN UDP Current Sessions                              0
                          0
LSN ICMP Received Packets                             0
    982
```



```
LSN ICMP Received Bytes                                 0
    96236
LSN ICMP Transmitted Packets                            0
                        0
LSN ICMP Transmitted Bytes                              0
                        0
LSN ICMP Dropped Packets                                0
    982
LSN ICMP Current Sessions                               0
                        0
LSN Subscribers                                         0
                        1

Done

> stat lsn group LSN-GROUP-1

LSN Group Statistics
                                                  Rate (/s)
                                                     Total
TCP Translated Pkts                                     0
    40
TCP Translated Bytes                                    0
    3026
TCP Dropped Pkts                                        0
                        0
TCP Current Sessions                                    0
                        0
UDP Translated Pkts                                     0
                        0
UDP Translated Bytes                                    0
                        0
UDP Dropped Pkts                                        0
                        0
UDP Current Sessions                                    0
                        0
ICMP Translated Pkts                                    0
                        0
ICMP Translated Bytes                                   0
                        0
ICMP Dropped Pkts                                       0
                        0
ICMP Current Sessions                                   0
                        0
Current Subscribers                                     0
```



```
                        1
44
45 Done
46 <!--NeedCopy-->
```

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- stat lsn-Gruppe
  - groupname

    Name der LSN-Gruppe. Maximale Länge: 127
  - Detail

    Gibt eine detaillierte Ausgabe an (einschließlich weiterer Statistiken). Die Ausgabe kann ziemlich voluminös sein. Ohne dieses Argument zeigt die Ausgabe nur eine Zusammenfassung an.
  - FullValues

    Gibt an, dass Zahlen und Zeichenfolgen in ihrer vollständigen Form angezeigt werden sollen. Ohne diese Option werden lange Zeichenfolgen gekürzt und große Zahlen abgekürzt.
  - ntimes

    Die Anzahl der Male, in Intervallen von sieben Sekunden, sollte die Statistik angezeigt werden.

    Standardwert: 1
  - logFile

    Der Name der Protokolldatei, die als Eingabe verwendet werden soll.
  - clearstats

    Löschen Sie die Statistiken/-Zähler

    Mögliche Werte: basic, full

Kompakte Protokollierung

Die Protokollierung von LSN-Informationen ist eine der wichtigen Funktionen, die von ISPs benötigt werden, um gesetzliche Anforderungen zu erfüllen und jederzeit die Quelle des Datenverkehrs zu identifizieren. Dies führt schließlich zu einer riesigen Menge an Protokolldaten, die die ISPs erfordern, große Investitionen für die Wartung der Protokollierungsinfrastruktur zu tätigen.

Kompakte Protokollierung ist eine Technik, um die Protokollgröße zu reduzieren, indem eine Notationsänderung mit kurzen Codes für Ereignis- und Protokollnamen verwendet wird. Beispielsweise C für Client, SC für erstellte Sitzung und T für TCP. Kompakte Protokollierung führt zu einer durchschnittlichen Verringerung der Protokollgröße um 40 Prozent.

Die folgenden Beispiele von NAT44-Zuordnungsprotokolleinträgen zeigen den Vorteil einer kompakten Protokollierung.

Default logging format	02/02/2016:01:1 GMT Informational 0-PPE-2 : default LSN LSN_ADDRPOR 85 0 : A&PDM CREATED Clien- tIP:Port:TD1.1.1. Destina- tionIP:Port:TD2 Protocol: TCP				
Compact logging format	02/02/2016:01:14:57 GMT Info 0-PE2:default LSN 87 0:A&PDMC	1.1.1.1:6500:0	N- 8.8.8.9:51066	D-2.2.2.2:80:0	T

Konfigurationsschritte

Führen Sie die folgenden Aufgaben für die Protokollierung von LSN-Informationen im kompakten Format aus:

- **Erstellen Sie ein LSN-Logprofil.** Ein LSN-Protokollprofil enthält den Parameter Log Compact, der angibt, ob Informationen im kompakten Format für eine LSN-Konfiguration protokolliert werden sollen.
- **Binden Sie das LSN-Logprofil an eine LSN-Gruppe einer LSN-Konfiguration.** Binden Sie das erstellte LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie den Parameter Log Profile Name auf den erstellten LSN-Protokollprofilnamen festlegen. Alle Sitzungen und Zuordnungen für diese LSN-Gruppe werden im kompakten Format protokolliert.

So erstellen Sie ein LSN-Protokollprofil mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn logprofile <logprofilename> -logCompact (ENABLED|DISABLED)

show lsn logprofile
<!--NeedCopy-->
```

So binden Sie ein LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn group <groupname> -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Beispielkonfiguration:

```
add lsn logprofile  LOG-PROFILE-COMPACT-9 -logCompact ENABLED

Done
add lsn client LSN-CLIENT-9
Done
bind lsn client LSN-CLIENT-9 -network 192.0.2.0 -netmask 255.255.255.0
Done
add lsn pool LSN-POOL-9
Done
bind lsn pool LSN-POOL-9 203.0.113.3-203.0.113.4
Done
add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9
Done
bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9
Done
bind lsn group  LSN-GROUP-9  - logProfileName LOG-PROFILE-COMPACT-9
Done
<!--NeedCopy-->
```


IPFIX-Protokollierung

Die Citrix ADC Appliance unterstützt das Senden von Informationen zu LSN-Ereignissen im IPFIX-Format (Internet Protocol Flow Information Export) an die konfigurierte Gruppe von IPFIX-Kollektoren. Die Appliance verwendet die vorhandene AppFlow Funktion, um LSN-Ereignisse im IPFIX-Format an die IPFIX-Kollektoren zu senden.

IPFIX-basierte Protokollierung ist für die folgenden großformatigen NAT44-bezogenen Ereignisse verfügbar:

- Erstellen oder Löschen einer LSN-Sitzung.
- Erstellen oder Löschen eines LSN-Zuordnungseintrags.
- Zuweisung oder Aufteilung von Portblöcken im Rahmen der deterministischen NAT.
- Zuweisung oder Aufteilung von Portblöcken im Kontext dynamischer NAT.
- Wann immer das Teilnehmersitzungskontingent überschritten wird.

Zu berücksichtigende Punkte, bevor Sie IPFIX-Protokollierung konfigurieren

Bevor Sie mit der Konfiguration von IPsec ALG beginnen, sollten Sie die folgenden Punkte beachten:

- Sie müssen die AppFlow Funktion und die IPFIX-Kollektoren auf der Citrix ADC Appliance konfigurieren. Anweisungen finden Sie unter Konfigurieren der AppFlow Funktion.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben für die Protokollierung von LSN-Informationen im IPFIX-Format aus:

- **Aktivieren Sie die LSN-Protokollierung in der AppFlow Konfiguration**. Aktivieren Sie den LSN-Protokollierungsparameter als Teil der AppFlow Konfiguration.
- **Erstellen Sie ein LSN-Protokollprofil**. Ein LSN-Protokollprofil enthält den IPFIX-Parameter, mit dem die Protokollinformationen im IPFIX-Format aktiviert oder deaktiviert werden.
- **Binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration**. Binden Sie das LSN-Protokollprofil an eine oder mehrere LSN-Gruppen. Ereignisse im Zusammenhang mit der gebundenen LSN-Gruppe werden im IPFIX-Format protokolliert.

So aktivieren Sie die LSN-Protokollierung in der AppFlow Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set appflow param -lsnLogging ( ENABLED | DISABLED )

```



```
show appflow param
<!--NeedCopy-->
```

So erstellen Sie ein LSN-Protokollprofil mit der CLI an der Eingabeaufforderung

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lsn logprofile <logProfileName>  -logipfix ( ENABLED | DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

So binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

So erstellen Sie ein LSN-Protokollprofil mit der GUI

Navigieren Sie zu **System** > **Large Scale NAT** > **Profile**, klicken Sie auf Register **Protokoll**, und fügen Sie dann ein Protokollprofil hinzu.

So binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration mit der GUI

1. Navigieren Sie zu **System** > **Large Scale NAT** > **LSN Group,** öffnen Sie die **LSN-Gruppe**.
2. Klicken Sie **unter Erweiterte Einstellungen** auf **+ Protokollprofil**, um das erstellte Protokollprofil an die LSN-Gruppe zu binden.

TCP SYN Leerlauf-Timeout

October 5, 2021

SYN-Leerlauf-Timeout ist das Timeout zum Herstellen von TCP-Verbindungen, die LSN auf der Citrix ADC Appliance verwenden. Wenn innerhalb des konfigurierten Zeitlimits keine TCP-Sitzung eingerichtet wird, entfernt der Citrix ADC die Sitzung. SYN Leerlauf-Timeout ist nützlich, um Schutz vor SYN-Flutangriffen zu bieten. In einer LSN-Konfiguration enthält die LSN-Gruppenentität die SYN-Leerlaufzeiteinstellung.

Beispiel:

In der folgenden LSN-Beispielkonfiguration wird SYN-Leerlaufzeitüberschreitung für TCP-Verbindungen auf 30 Sekunden festgelegt, die mit Teilnehmern aus dem 192.0.2.0/24-Netzwerk verbunden sind.

```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 203.0.113.3

Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1  - synidletimeout 30

Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1

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

Überschreiben der LSN-Konfiguration mit Lastenausgleichskonfiguration

October 5, 2021

Eine LSN-Konfiguration hat standardmäßig Vorrang vor jeder Lastausgleichskonfiguration. Um die LSN-Konfiguration (Large Scale Networking) mit der Load Balancing-Konfiguration für den Datenverkehr zu überschreiben, der beide Konfigurationen entspricht, erstellen Sie ein Net Profile mit aktiviertem Override LSN-Parameter und binden dieses Profil an den virtuellen Server der Load Balancing-Konfiguration. USNIP- oder USIP-Einstellungen der Lastausgleichskonfiguration werden auf den Datenverkehr angewendet, anstatt die LSN-IP-Adresse der LSN-Konfiguration anzuwenden.

Diese Option ist in einer LSN-Bereitstellung nützlich, die Citrix ADC Appliances und Value Added Services wie Firewall und Optimierungsgeräte umfasst. Bei diesem Bereitstellungstyp ist der eintreffende Datenverkehr auf der Citrix ADC Appliance erforderlich, um diese Mehrwertdienste durchlaufen zu können, bevor eine LSN-Konfiguration auf der Appliance auf den Datenverkehr angewendet wird. Damit die Citrix ADC Appliance den eingehenden Datenverkehr an einen Value Added Service senden kann, wird eine Lastausgleichskonfiguration erstellt, und die Überschreibung von LSN ist auf der Appliance aktiviert. Die Lastausgleichskonfiguration umfasst Value Added Services, die als Load Balancing Services dargestellt werden und an einen virtuellen Server vom Typ ANY gebunden sind. Der virtuelle Server ist mit Listenrichtlinien konfiguriert, um den Datenverkehr zu identifizieren, der an den Value Added Service gesendet werden soll.

So aktivieren Sie das Überschreiben von lsn in einem Netzprofil mit der CLI

Um das Überschreiben von lsn beim Hinzufügen eines Netzprofils zu aktivieren, geben Sie an der Eingabeaufforderung

```
add netProfile <name> -overrideLsn ( ENABLED | DISABLED )

show netprofile <name>
<!--NeedCopy-->
```

Um das Überschreiben von lsn beim Hinzufügen eines Netzprofils zu aktivieren, geben Sie an der Eingabeaufforderung

```
set netProfile <name> -overrideLsn ( ENABLED | DISABLED )

show netprofile <name>
<!--NeedCopy-->
```

So aktivieren Sie das Überschreiben von lsn in einem Netzprofil mit der GUI

1. Navigieren Sie zu **System** > **Netzwerk** > **Net Profile**.
2. Legen Sie den Parameter **Override LSN** fest, während Sie Netzprofile hinzufügen oder ändern.

In der folgenden Beispielkonfiguration hat Netprofil NETPROFILE-OVERRIDELSN-1 die Option Override LSN aktiviert und ist an den Lastenausgleich des virtuellen Servers LBVS-1 gebunden.

Beispielkonfiguration:

```
add netprofile NETPROFILE-OVERRIDELSN-1 -overrideLsn ENABLED

Done

set lb vserver LBVS-1 -netprofile NETPROFILE-OVERRIDELSN-1

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

LSN-Sitzungen löschen

October 5, 2021

Sie können unerwünschte oder ineffiziente LSN-Sitzungen von der Citrix ADC Appliance entfernen. Die Appliance gibt sofort Ressourcen (wie NAT-IP-Adresse, Port und Speicher) frei, die für diese Sitzungen zugewiesen wurden, sodass die Ressourcen für neue Sitzungen verfügbar sind. Die Appliance löscht auch alle nachfolgenden Pakete, die sich auf diese entfernten Sitzungen beziehen. Sie können alle oder ausgewählte LSN-Sitzungen von der Citrix ADC Appliance entfernen.

So löschen Sie alle LSN-Sitzungen mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
flush lsn session

show lsn session
<!--NeedCopy-->
```

So löschen Sie selektive LSN-Sitzungen mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
flush lsn session [-clientname <string>] [-network <ip_addr> [-netmask
    <netmask>] [-td <positive_integer>]] [-natIP <ip_addr> [-natPort <
    port>]]

show lsn session
<!--NeedCopy-->
```

Beispiel

Löschen aller auf einem Citrix ADC vorhandenen LSN-Sitzungen

```
flush lsn session

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

Alle LSN-Sitzungen im Zusammenhang mit LSN-Client-Entität LSN-CLIENT-1 löschen

```
flush lsn session -clientname LSN-CLIENT-1

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

Löschen Sie alle LSN-Sitzungen im Zusammenhang mit einem Teilnehmernetzwerk (192.0.2.0) der LSN-Client-Entität LSN-CLIENT-2, die zur Verkehrsdomäne 100 gehören

```
flush lsn session -clientname LSN-CLIENT-2 -network 192.0.2.0 -
    netmask 255.255.255.0 -td 100

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

So löschen Sie alle LSN-Sitzungen mit dem Konfigurationsdienstprogramm

Navigieren Sie zu System > Large Scale NAT > Sessions, und klicken Sie auf Sessions leeren.

Parameterbeschreibungen (von Befehlen, die in der CLI-Prozedur aufgeführt sind)

- lege lsn-Sitzung
  - clientname

    Name der LSN-Client-Entität. Maximale Länge: 127
  - Netzwerk

    IP-Adresse oder Netzwerkadresse des Teilnehmers.
  - Netzmaske

    Subnetzmaske für die IP-Adresse, die durch den Netzwerkparameter angegeben wird.

    Standardwert: 255.255.255.255
  - td

    Verkehrsdomänen-ID der LSN-Client-Entität.

    Standardwert: 0

    Mindestwert: 0

    maximaler Wert: 4094
  - natIP

    Zugeordnete NAT-IP-Adresse, die in LSN-Sitzungen verwendet wird.
  - natPort

    Zugeordneter NAT-Port, der in den LSN-Sitzungen verwendet wird.

Lastenausgleich SYSLOG-Server

October 5, 2021

Die Citrix ADC Appliance sendet ihre SYSLOG-Ereignisse und -Nachrichten an alle konfigurierten externen Protokollserver. Dies führt zur Speicherung redundanter Nachrichten und erschwert Systemadministratoren die Überwachung. Um dieses Problem zu beheben, bietet die Citrix ADC Appliance Lastausgleichsalgorithmen, die die SYSLOG-Nachrichten zwischen den externen Protokollservern für eine bessere Wartung und Leistung ausgleichen können. Die unterstützten Load Balancing-Algorithmen umfassen RoundRobin, LeastBandWidth, CustomLoad, LeastConnection, LeastPackets und AuditLogHash.

Lastenausgleich von SYSLOG-Servern über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

Fügen Sie einen Dienst hinzu, und geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGUDP an.

```
add service <name>(<IP> | <serverName>) <serviceType (SYSLOGTCP |
    SYSLOGUDP)> <port>
<!--NeedCopy-->
```

Fügen Sie einen virtuellen Lastausgleichsserver hinzu, geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGTCP an und Lastausgleichsmethode als AUDITLOGHASH an.

```
add lb vserver <name> <serviceType (SYSLOGTCP | SYSLOGUDP)> [-lbMethod
    <AUDITLOGHASH>]
<!--NeedCopy-->
```

Binden Sie den Dienst an den virtuellen Lastausgleichsserver.

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

1. Fügen Sie eine SYSLOG-Aktion hinzu, und geben Sie den Namen des Lastausgleichsservers an, der SYSLOGTCP oder SYSLOGUDP als Diensttyp enthält.

```
add syslogaction <name> <serverIP> [-lbVserverName <string>] [-logLevel
     <logLevel>]
<!--NeedCopy-->
```

Fügen Sie eine SYSLOG-Richtlinie hinzu, indem Sie die Regel und die Aktion angeben.

```
add syslogpolicy <name> <rule> <action>
<!--NeedCopy-->
```

Binden Sie die SYSLOG-Richtlinie an das System global, damit die Richtlinie wirksam wird.

```
bind system global <policyName>
<!--NeedCopy-->
```


Lastenausgleich von SYSLOG-Servern mit dem Konfigurationsdienstprogramm

1. Fügen Sie einen Dienst hinzu, und geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGUDP an.

   Navigieren Sie zu Traffic Management > Services, klicken Sie auf Hinzufügen und wählen Sie SYLOGTCP oder SYSLOGUDP als Protokoll aus.

2. Fügen Sie einen virtuellen Lastausgleichsserver hinzu, geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGTCP an und Lastausgleichsmethode als AUDITLOGHASH an.

   Navigieren Sie zu Traffic Management > Virtuelle Server, klicken Sie auf Hinzufügen und wählen Sie SYLOGTCP oder SYSLOGUDP als Protokoll aus.

3. Bing des Dienstes an den virtuellen Lastausgleichsserver an den Dienst.

   Bing des Dienstes an den virtuellen Lastausgleichsserver.

   Navigieren Sie zu Traffic Management > Virtuelle Server, wählen Sie einen virtuellen Server aus und wählen Sie dann in der Load Balancing-Methode die AUDITLOGHASH aus.

4. Fügen Sie eine SYSLOG-Aktion hinzu, und geben Sie den Namen des Lastausgleichsservers an, der SYSLOGTCP oder SYSLOGUDP als Diensttyp enthält.

   Navigieren Sie zu System > Überwachung, klicken Sie auf Server und fügen Sie einen Server hinzu, indem Sie LB Vserver Option inServers auswählen.

5. Fügen Sie eine SYSLOG-Richtlinie hinzu, indem Sie die Regel und die Aktion angeben.

   Navigieren Sie zu System > Syslog, klicken Sie auf Richtlinien und fügen Sie eine SYSLOG-Richtlinie hinzu.

6. Binden Sie die SYSLOG-Richtlinie an das System global, damit die Richtlinie wirksam wird.

   Navigieren Sie zu System > Syslog, wählen Sie eine SYSLOG-Richtlinie aus und klicken Sie auf Aktion, und klicken Sie dann auf Globale Bindungen und binden Sie die Richtlinie an system global.

Beispiel:

Die folgende Konfiguration legt den Lastausgleich von SYSLOG-Nachrichten unter den externen Protokollservern fest, wobei die AUDITLOGHASH als Lastausgleichsmethode verwendet wird. Die Citrix ADC Appliance generiert SYSLOG-Ereignisse und Meldungen, die zwischen den Diensten, service1, service2 und Service 3 geladen werden.

```
1 add service service1 192.0.2.10 SYSLOGUDP 514
2
3 add service service2 192.0.2.11 SYSLOGUDP 514
4
5 add service service3 192.0.2.11 SYSLOGUDP 514
```



```
6
7  add lb vserver lbvserver1 SYSLOGUDP -lbMethod AUDITLOGHASH
8
9  bind lb vserver lbvserver1 service1
10
11 bind lb vserver lbvserver1 service2
12
13 bind lb vserver lbvserver1 service3
14
15 add syslogaction sysaction1 -lbVserverName lbvserver1 -logLevel All
16
17 add syslogpolicy syspol1 ns_true sysaction1
18
19 bind system global syspol1
20 <!--NeedCopy-->
```

Einschränkungen:

Die Citrix ADC Appliance unterstützt keinen externen Lastenausgleich des virtuellen Servers, der die SYSLOG-Nachrichten zwischen den Protokollservern ausgleicht.

Port Control-Protokoll

October 5, 2021

Citrix ADC Appliances unterstützen jetzt Port Control Protocol (PCP) für Large Scale NAT (LSN). Viele Abonnentenanwendungen eines ISP müssen über das Internet zugänglich sein (z. B. IOT-Geräte (Internet of Things), z. B. eine IP-Kamera, die die Überwachung über das Internet ermöglicht). Eine Möglichkeit, diese Anforderung zu erfüllen, besteht darin, statische Large Scale NAT-Karten (LSN) zu erstellen. Aber für eine sehr große Anzahl von Abonnenten ist das Erstellen statischer LSN NAT-Karten keine machbare Lösung.

Port Control Protocol (PCP) ermöglicht es einem Abonnenten, spezifische LSN NAT-Zuordnungen für sich selbst und/oder für andere Geräte von Drittanbietern anzufordern. Das große NAT-Gerät erstellt eine LSN-Karte und sendet sie an den Abonnenten. Der Abonnent sendet die entfernten Geräte über das Internet die NAT-IP-Adresse:NAT-Port, an der sie eine Verbindung zum Abonnenten herstellen können.

In der Regel senden Anwendungen häufig Keepalive-Nachrichten an das große NAT-Gerät, damit ihre LSN-Zuordnungen keine Timeout aufweisen. PCP hilft, die Häufigkeit solcher Keep-Alive-Nachrichten zu reduzieren, indem die Anwendungen die Timeout-Einstellungen der LSN-Zuordnungen erlernen können. Dies trägt dazu bei, den Bandbreitenverbrauch im Zugangsnetzwerk des ISP und den Batterieverbrauch auf mobilen Geräten zu reduzieren.

PCP ist ein Client-Server-Modell und läuft über das UDP-Transportprotokoll. Eine Citrix ADC Appliance implementiert die PCP-Serverkomponente und ist mit RFC 6887 kompatibel.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben für die Konfiguration von PCP aus:

- (Optional) Erstellen Sie ein PCP-Profil. Ein PCP-Profil enthält Einstellungen für PCP-bezogene Parameter (z. B. zum Abhören von Zuordnungen und Peer-PCP-Anforderungen). Ein PCP-Profil kann an einen PCP-Server gebunden werden. Ein PCP-Profil, das an einen PCP-Server gebunden ist, wendet alle seine Einstellungen auf den PCP-Server an. Ein PCP-Profil kann an mehrere PCP-Server gebunden werden. Standardmäßig ist ein PCP-Profil mit Standardparametereinstellungen an alle PCP-Server gebunden. Ein PCP-Profil, das Sie an einen PCP-Server binden, überschreibt die standardmäßigen PCP-Profileinstellungen für diesen Server. Ein Standard-PCP-Profil weist die folgenden Parametereinstellungen auf:
  - Zuordnung: Aktiviert
  - Peer: Aktiviert
  - Minimale Kartenlebensdauer: 120 Sekunden
  - Maximale Lebensdauer: 86400 Sekunden
  - Ankündigungsanzahl: 10
  - Dritte: Deaktiviert
- Erstellen Sie einen PCP-Server und binden Sie ein PCP-Profil an ihn. Erstellen Sie einen PCP-Server auf der Citrix ADC Appliance, um PCP-bezogene Anforderungen und Nachrichten von den Abonnenten zu überwachen. Eine Subnetz-IP (SNIP) -Adresse muss einem PCP-Server zugewiesen werden, um darauf zuzugreifen. Standardmäßig überwacht ein PCP-Server Port 5351.
- Binden Sie den PCP-Server an eine LSN-Gruppe einer LSN-Konfiguration. Binden Sie den erstellten PCP-Server an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie den PCP-Server-Parameter so einstellen, dass der erstellte PCP-Server angegeben wird. Der erstellte PCP-Server kann nur von den Abonnenten dieser LSN-Gruppe zugegriffen werden.

> **Hinweis:**
>
> Ein PCP-Server für eine große NAT-Konfiguration erfüllt keine Anforderungen von Abonnenten, die aus ACL-Regeln identifiziert werden.

So erstellen Sie ein PCP-Profil mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add pcp profile <name> [-mapping ( ENABLED | DISABLED )] [-peer (
    ENABLED | DISABLED )] [-minMapLife <secs>]  [-maxMapLife <secs>] [-
    announceMultiCount <positive_integer>][-thirdParty ( ENABLED |
    DISABLED )]

show pcp profile <name>
<!--NeedCopy-->
```

So erstellen Sie einen PCP-Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add pcp server <name> <IPAddress> [-port <portNum|*>] [-pcpProfile <
    string>]

show pcp server <name>
<!--NeedCopy-->
```

Beispielkonfiguration für NAT44

In der folgenden Beispielkonfiguration ist PCP-Server PCP-SERVER-9 mit Standard-PCP-Einstellungen an LSN-Gruppe LSN-GROUP-9 gebunden. PCP-SERVER-9 bedient PCP-Anfragen von Teilnehmern im Netzwerk 192.0.2.0/24.

Beispielkonfiguration:

```
add pcp server PCP-SERVER-9 192.0.3.9

Done

add lsn client LSN-CLIENT-9

Done

bind lsn client LSN-CLIENT-9 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-9

```



```
Done

bind lsn pool LSN-POOL-9 203.0.113.3-203.0.113.4

Done

add lsn group LSN-GROUP-9 -clientname LSN-CLIENT-9

Done

bind lsn group LSN-GROUP-9 -poolname LSN-POOL-9

Done

bind lsn group  LSN-GROUP-9  -pcpServer PCP-SERVER-9

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

LSN44 in einem Cluster-Setup

October 5, 2021

Große NAT44-Konfigurationen werden bei einem Citrix ADC Cluster-Setup unterstützt.

Ein Citrix ADC-Cluster ist eine Gruppe von Citrix ADC Appliances, die als ein einzelnes System konfiguriert und verwaltet werden. Ein Citrix ADC Cluster bietet Skalierbarkeit und Verfügbarkeit. Jede Citrix ADC Appliance in einem Cluster-Setup fungiert als unabhängige LSN-Entität und wird als ein einzelnes System verwaltet.

Die LSN-Konfiguration in einem Cluster-Setup ist identisch mit einer eigenständigen Appliance, außer dass ein bestimmter Pool von LSN-IP-Adressen jeweils nur einem Knoten zugeordnet ist. Mit anderen Worten, eine LSN-IP-Pool-Entität wird in einem bestimmten Knoten als Spotted-Entity konfiguriert. Alle Knoten eines Cluster-Setups können über eine bestimmte LSN-IP-Pool-Entität verfügen. Um sicherzustellen, dass die Pakete, die sich auf eine LSN-Sitzung beziehen, auf demselben Clusterknoten empfangen werden, der den NAT-Vorgang ausgeführt hat, wird die Policy-basierte Backplane-Steuerung (PBS) konfiguriert. PBS steuert die empfangenen verwandten Pakete einer LSN-Sitzung auf denselben Clusterknoten.

Beispielkonfiguration:


```
add lsn client LSN-CLIENT-1

Done

bind lsn client LSN-CLIENT-1 -network 192.0.2.0 -netmask 255.255.255.0

Done

add lsn pool LSN-POOL-1

Done

bind lsn pool LSN-POOL-1 -ownerNode 1 203.0.113.3

Done

bind lsn pool LSN-POOL-1 -ownerNode 2 203.0.113.3

Done

add lsn group LSN-GROUP-1 -clientname LSN-CLIENT-1

Done

bind lsn group LSN-GROUP-1 -poolname pool1 LSN-POOL-1

Done

add ns acl b1 ALLOW -srcIP = 192.0.2.0-192.0.2.255 -type DFD -dfdhash
   SIP


Done

apply ns acls -type DFD

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


Dual-Stack Lite

October 5, 2021

Aufgrund des Mangels an IPv4-Adressen und der Vorteile von IPv6 gegenüber IPv4 haben viele ISPs den Übergang zur IPv6-Infrastruktur begonnen. Während des Übergangs müssen ISPs jedoch weiterhin IPv4 zusammen mit IPv6 unterstützen, da der Großteil des öffentlichen Internets immer noch nur IPv4 verwendet und viele Abonnenten IPv6 nicht unterstützen.

Dual Stack Lite (DS-Lite) ist eine IPv6-Übergangslösung für ISPs mit IPv6-Infrastruktur, um ihre IPv4-Abonnenten mit dem Internet zu verbinden. DS-Lite verwendet IPv4-in-IPv6-Tunneling, um das IPv4-Paket eines Teilnehmers über einen Tunnel im IPv6-Zugangsnetzwerk an den ISP zu senden. Das IPv6-Paket wird entkapselt, um das IPv4-Paket des Teilnehmers wiederherzustellen, und wird dann nach NAT-Adresse und Port-Übersetzung und anderer LSN-bezogener Verarbeitung an das Internet gesendet. Die Antwortpakete durchlaufen denselben Pfad zum Abonnenten.

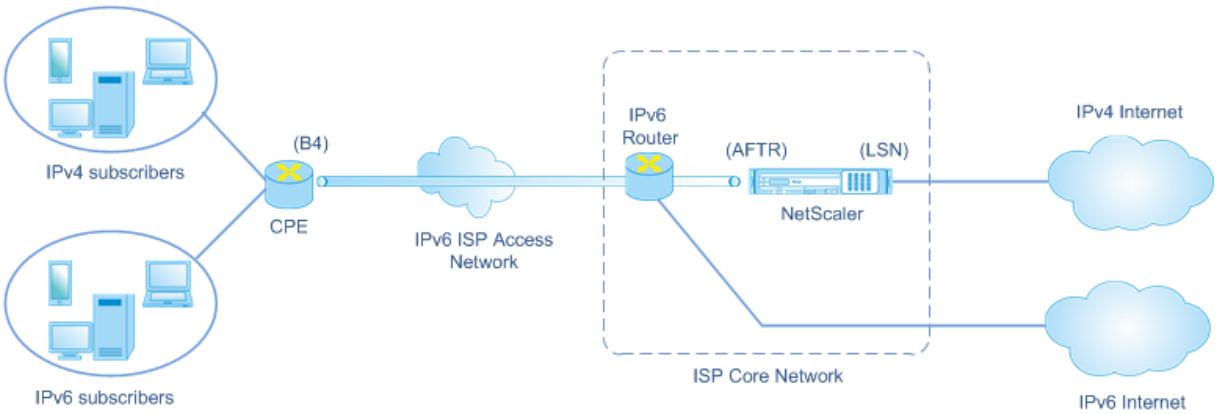
Die Citrix ADC Appliance implementiert die AFTR-Komponente einer DS-Lite-Bereitstellung und ist kompatibel mit RFC 6333.

Architektur

Die Dual-Stack Lite-Architektur für einen ISP besteht aus folgenden Komponenten:

- **Basis-Bridging Breitband (B4).** Basic Bridging Breitband (B4) ist ein Gerät oder eine Komponente, die sich in den Räumlichkeiten des Teilnehmers befindet. Typischerweise ist B4 eine Komponente in den CPE-Geräten in den Teilnehmergebäuden. IPv4-Abonnenten sind über das CPE-Gerät, das die B4-Komponente enthält, mit dem nur IPv6-ISP-Zugangsnetzwerk verbunden. Die Hauptfunktion des B4 besteht darin, einen IPv6-Tunnel zwischen B4 und einem Address Family Transition Router (AFTR) zu initiieren, um IPv4-Abfrage- oder Antwortpakete über den Tunnel zu senden oder zu empfangen. B4 enthält eine IPv6-Adresse, die als B4-Tunnelendpunktadresse bezeichnet wird. B4 verwendet diese Adresse, um IPv6-Pakete an AFTR zu senden und Pakete von AFTR zu empfangen.
- **Address Family Transition Router (AFTR).** AFTR ist ein Gerät oder eine Komponente, die sich im Kernnetz des ISP befindet. AFTR beendet den IPv6-Tunnel vom B4-Gerät. Mit anderen Worten, der IPv6-Tunnel wird zwischen B4 in der Teilnehmerprämisse und AFTR im ISP-Kernnetz gebildet. AFTR entkapselt IPv6-Pakete, die von B4 empfangen wurden, um die ursprünglichen IPv4-Pakete der Abonnenten wiederherzustellen. AFTR sendet die IPv4-Pakete an das LSN-Gerät oder die Komponente. LSN leitet die IPv4-Pakete an ihr Ziel weiter, nachdem die NAT-Adress- und Port-Übersetzung (NAT 44) und andere LSN-bezogene Verarbeitung durchgeführt wurde. AFTR enthält eine IPv6-Adresse, die als AFTR-Tunnelendpunktadresse bezeichnet wird. AFTR verwendet diese Adresse, um IPv6-Pakete an B4 zu senden und IPv6-Pakete von B4 zu empfangen. Die Citrix ADC Appliance implementiert die AFTR-Komponente.

- **Softwire.** Der zwischen B4 und AFTR erzeugte IPv6-Tunnel wird als Softwire bezeichnet.



Die DS-Lite-Architektur eines ISP, der eine Citrix ADC Appliance verwendet, besteht aus Abonnenten in privaten Adressräumen, die über eine Citrix ADC-Appliance auf das Internet zugreifen, die im Kernnetzwerk des ISP bereitgestellt wird. IPv4-Abonnenten sind mit einem CPE-Gerät verbunden, das die DS-Lite B4-Funktionalität enthält. Das CPE-Gerät ist über das reine IPv6-Zugriffsnetzwerk des ISP mit dem Kernnetzwerk des ISP verbunden. Die Citrix ADC Appliance enthält die DS-Lite AFTR- und LSN-Funktionalität.

IPv4-Abonnenten, die mit dem CPE-Gerät verbunden sind, werden private IPv4-Adressen entweder manuell oder über DHCP-Server zugewiesen, der auf dem CPE-Gerät ausgeführt wird. Auf dem CPE-Gerät wird die AFTR-Tunnelendpunktadresse manuell oder über DHCPv6 angegeben. Die Konfiguration von CPE-Geräten ist herstellerspezifisch und daher außerhalb des Anwendungsbereichs dieser Dokumentation.

Nach Erhalt eines Anforderungspakets, das von einem IPv4-Abonnenten stammt und an einen Speicherort im Internet bestimmt ist, kapselt die B4-Komponente des CPE-Geräts das IPv4-Paket in ein IPv6-Paket und sendet es an die Citrix ADC Appliance im Kernnetzwerk des ISP. Die AFTR-Funktionalität der Citrix ADC Appliance entkapselt das IPv6-Paket, um das ursprüngliche IPv4-Paket des Teilnehmers wiederherzustellen. Die LSN-Funktionalität der Citrix ADC Appliance übersetzt die Quell-IP-Adresse und den Port des IPv4-Pakets in eine NAT-IP-Adresse und einen NAT-Port, der aus dem konfigurierten NAT-Pool ausgewählt wurde, und sendet das Paket dann an sein Ziel im Internet.

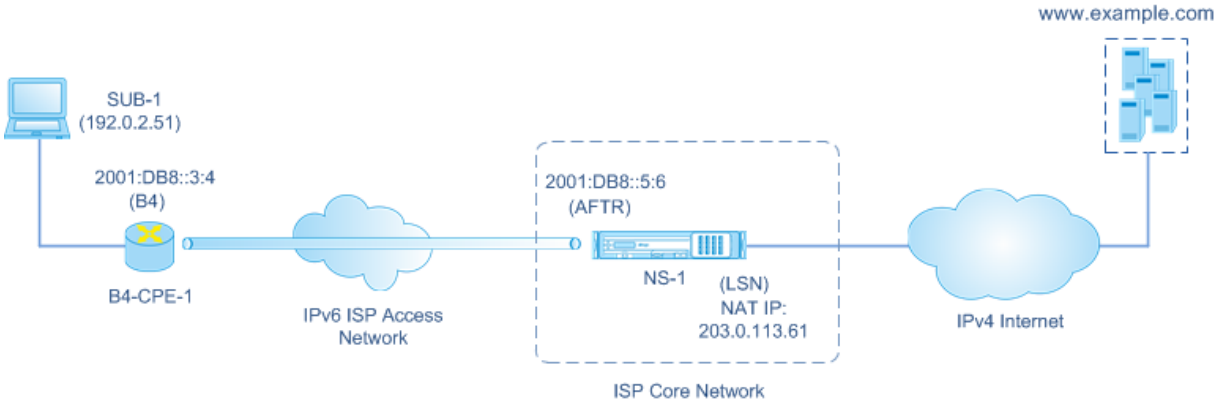
Die Appliance verwaltet eine Aufzeichnung aller aktiven Sitzungen, die die Funktionen AFTR und LSN verwenden. Diese Sitzungen werden als DS-Lite-Sitzungen bezeichnet. Die Citrix ADC Appliance verwaltet auch die Zuordnungen zwischen B4-IPv6-Adresse, Abonnentenadresse und -port sowie NAT-IPv4-Adresse und -Port für jede DS-Lite-Sitzung. Diese Zuordnungen werden als DS-Lite LSN-Zuordnungen bezeichnet. Aus DS-Lite-Sitzungseinträgen und DS-Lite-LSN-Zuordnungseinträgen erkennt die Citrix ADC Appliance ein Antwortpaket (das aus dem Internet empfangen wird) als zu einer bestimmten DS-Lite-Sitzung gehört.

Wenn die Citrix ADC Appliance ein Antwortpaket empfängt, das zu einer bestimmten DS-Lite-Sitzung gehört, übersetzt die LSN-Funktionalität der Appliance die Ziel-IP-Adresse und den Port

des Antwortpakets von NAT-IP-Adresse und -Port in die Abonnentenadresse und -port, die AFTR-Funktionalität kapselt die resultierende Paket in einem IPv6-Paket und sendet es an das CPE-Gerät. Die B4-Funktionalität des CPE-Geräts entkapselt das IPv6-Paket, um das IPv4-Antwortpaket wiederherzustellen, und sendet dann das IPv4-Paket an den Abonnenten.

Beispiel

Betrachten Sie ein Beispiel für eine DS-Lite-Bereitstellung, bestehend aus Citrix ADC NS-1 im Kernnetzwerk eines ISP, CPE-Gerät B4-CPE-1 in einer Teilnehmerprämisse und einem einzelnen IPv4-Abonnenten SUB-1. B4-CPE-1 unterstützt die B4-Funktionalität der DS-Lite-Funktion.



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt.

Entität	Name	Details
IPv4-Adresse des Teilnehmers SUB-1		192.0.2.51
IPv6-Adresse des Softwire-Endpunkts auf dem B4-Gerät (B4-CPE-1)		2001:DB8::3:4
IPv6-Adresse des Softwire-Endpunkts auf dem AFTR-Gerät (NS-1)		2001:DB8::5:6

Einstellungen auf der Citrix ADC Appliance NS-1:

Entität	Name	Details
LSN-Client	LSN-DSLITE-CLIENT-1	Network6 (Identifizieren des Datenverkehrs von B4-Geräten) = 2001:DB8::3:0/100
LSN-Pool	LSN-DSLITE-POOL-1	LSN IPs (NAT IP) = 203.0.113.61 - 203.0.113.70
IPv6-Profil	LSN-DSLITE-PROFILE-1	Typ = DS-LITE; IPv6-Adresse (AFTR IPv6-Adresse) = Eine der Citrix ADC eigenen IPv6-Adresse vom Typ SNIP6 = 2001:DB8::5:6
LSN-Gruppe	LSN-DSLITE-GROUP-1	LSN client = LSN-DSLITE-CLIENT-1; LSN pool = LSN-DSLITE-POOL-1;IPv6 profile = LSN-DSLITE-PROFILE-1

Es folgt der Verkehrsfluss in diesem Beispiel:

1. IPv4-Abonnent SUB-1 sendet eine Anfrage an (`http://www.example.com/`). Das IPv4-Paket hat:
   - Quell-IP-Adresse = 192.0.2.51
   - Quellport = 2552
   - Ziel-IP-Adresse = 198.51.100.250
   - Zielport = 80
2. Nach Erhalt des IPv4-Anforderungspakets kapselt B4-CPE-1 es in die Nutzlast eines IPv6-Pakets und sendet dann das IPv6-Paket an NS-1. Das IPv6-Paket hat:
   - Quell-IP-Adresse = 2001:DB8::3:4
   - Ziel-IP-Adresse = 2001:DB8::5:6
3. Wenn NS-1 das IPv6-Paket empfängt, entkapselt das AFTR-Modul das Paket, indem die IPv6-Header entfernt werden. Das resultierende Paket ist das ursprüngliche IPv4-Anforderungspaket von SUB-1.
4. Das LSN-Modul von NS-1 übersetzt die Quell-IP-Adresse und den Port des Pakets in eine NAT-IP-Adresse und einen NAT-Port, der aus dem konfigurierten NAT-Pool ausgewählt wurde. Das

übersetzte IPv4-Paket hat:

- Quell-IP-Adresse = 203.0.113.61
- Quellport = 3002
- Ziel-IP-Adresse = 198.51.100.250
- Zielport = 80

5. Das LSN-Modul erstellt auch eine LSN-Zuordnung und einen Sitzungseintrag für diese DS Lite-Sitzung. Die Zuordnung enthält die folgenden Informationen:
   - Quell-IP-Adresse des IPv6-Pakets (IPv6-Adresse von B4-CPE-1) = 2001:DB8::3:4
   - Quell-IP-Adresse des IPv4-Pakets (IPv4-Adresse von SUB-1) = 192.0.2.51
   - Quellport des IPv4-Pakets = 2552
   - NAT IP-Adresse = 203.0.113.61
   - NAT-Anschluss = 3002
6. NS-1 sendet das resultierende IPv4-Paket an sein Ziel im Internet.
7. Der Server für www.example.com verarbeitet das Anforderungspaket und sendet ein Antwortpaket. Das IPv4-Antwortpaket hat:
   - Quell-IP-Adresse = 198.51.100.250
   - Quellport = 80
   - Ziel-IP-Adresse = 203.0.113.61
   - Zielport = 3002
8. Nach Erhalt des IPv4-Pakets untersucht NS-1 die LSN-Zuordnungs- und Sitzungseinträge und stellt fest, dass das IPv4-Antwortpaket zu einer DS Lite-Sitzung gehört. Das LSN-Modul von NS-1 übersetzt die Ziel-IP-Adresse und den Port. Das IPv4-Paket hat jetzt:
   - Quell-IP-Adresse = 198.51.100.250
   - Quellport = 80
   - Ziel-IP-Adresse = 192.0.2.51
   - Zielport = 2552
9. Das AFTR-Modul von NS-1 kapselt das IPv4-Paket in ein IPv6-Paket und sendet dann das IPv6-Paket an B4-CPE-1. Das IPv6-Paket hat:
   - Quell-IP-Adresse = 2001:DB8:: 5:6
   - Ziel-IP-Adresse = 2001:DB8:: 3:4
10. Nach Erhalt des Pakets entkapselt B4-CPE-1 das IPv6-Paket, indem die IPv6-Header entfernt werden, und sendet dann das resultierende IPv4-Paket an CL-1.

Punkte, die vor der Konfiguration von DS-Lite zu beachten sind

October 5, 2021

Berücksichtigen Sie die folgenden Punkte, bevor Sie DS-Lite auf einer Citrix ADC Appliance konfigurieren:

1. Sie müssen die verschiedenen Komponenten von DS-Lite verstehen, die in RFC 6333 beschrieben sind.
2. Eine DS-Lite-Konfiguration auf einer Citrix ADC Appliance verwendet die LSN-Befehlssätze. In einer DS-Lite-Konfiguration gibt die LSN-Client-Entität die IPv6-Adresse oder IPv6-Netzwerkadresse oder ACL6-Regeln für die Identifizierung des Datenverkehrs vom B4-Gerät an. Eine DS-Lite-Konfiguration enthält auch ein IPv6-Profil, das die IPv6-Adressen-AFTR-Komponente auf einer Citrix ADC Appliance angibt. Weitere Informationen zur Citrix ADC LSN-Funktion finden Sie unter Large Scale NAT.
3. Bei einer DS-Lite-Konfiguration unterstützt die Citrix ADC Appliance LSN für IPv4-Pakete, die nur zu einem der folgenden Protokolle gehören. Die Citrix ADC Appliance löscht IPv4-Pakete, die zu anderen Protokollen gehören:
   - TCP
   - UDP
   - ICMP
4. Die Citrix ADC Appliance unterstützt die folgenden ALGs DS-Lite:
   - ICMP
   - FTP
   - TFTP
   - Sitzungsinitiationsprotokoll (SIP)
   - Echtzeit-Streaming-Protokoll (RTSP)

Konfigurieren von DS-Lite

October 5, 2021

Eine DS-Lite-Konfiguration auf einer Citrix ADC Appliance verwendet die LSN-Befehlssätze. In einer DS-Lite-Konfiguration gibt die LSN-Client-Entität die IPv6-Adresse oder IPv6-Netzwerkadresse oder ACL6-Regeln für die Identifizierung des Datenverkehrs vom B4-Gerät an. Weitere Informationen zur Citrix ADC LSN-Funktion finden Sie unter Large Scale NAT. Eine DS-Lite-Konfiguration enthält auch ein IPv6-Profil, das die IPv6-Adresse (vom Typ SNIP6) der DS-Lite-AFTR-Komponente auf einer Citrix ADC Appliance angibt.

Die Konfiguration von DS-Lite auf einer Citrix ADC Appliance umfasst die folgenden Aufgaben:

- **Stellen Sie die globalen LSN-Parameter**ein. Globale Parameter umfassen die Menge an Citrix ADC-Arbeitsspeicher, der für die LSN-Funktion reserviert ist, und die Synchronisierung von LSN-Sitzungen in einem Hochverfügbarkeitssetup.
- **Erstellen Sie eine LSN-Client-Entität zur Identifizierung des Datenverkehrs von B4-CPE-Geräten**. Die LSN-Client-Entität bezieht sich auf eine Reihe von DS-Lite B4-Geräten. Die Client-Entität enthält IPv6-Adressen oder IPv6-Netzwerkadresse oder ACL6-Regeln zur Identifizierung des Datenverkehrs von diesen B4-Geräten. Ein LSN-Client kann nur an eine LSN-Gruppe gebunden werden. Die Befehlszeilenschnittstelle verfügt über zwei Befehle zum Erstellen einer LSN-Client-Entität und zum Binden eines Abonnenten an die LSN-Client-Entität. Das Konfigurationsdienstprogramm kombiniert diese beiden Vorgänge auf einem einzigen Bildschirm.
- **Erstellen Sie einen LSN-Pool und binden Sie NAT-IP-Adressen daran**. Ein LSN-Pool definiert einen Pool von NAT-IP-Adressen, der von der Citrix ADC Appliance zum Ausführen von LSN verwendet wird. Die Befehlszeilenschnittstelle verfügt über zwei Befehle zum Erstellen eines LSN-Pools und zum Binden von NAT-IP-Adressen an den LSN-Pool. Das Konfigurationsdienstprogramm kombiniert diese beiden Vorgänge auf einem einzigen Bildschirm.
- **Erstellen Sie ein LSN IP6-Profil.** Ein LSN-IP6-Profil definiert die IPv6-Adresse der DS-Lite-AFTR-Komponente auf der Citrix ADC Appliance. Die IPv6-Adresse muss eine der Citrix ADC eigenen IPv6-Adresse vom Typ SNIP6 sein.
- **(Optional) Erstellen Sie ein LSN-Transportprofil für ein bestimmtes Protokoll**. Ein LSN-Transportprofil definiert verschiedene Timeouts und Limits, z. B. maximale LSN-Sitzungen und maximale Port-Auslastung, die ein Teilnehmer für ein bestimmtes Protokoll haben kann. Sie binden ein LSN-Transportprofil für jedes Protokoll (TCP, UDP und ICMP) an eine LSN-Gruppe. Ein Profil kann an mehrere LSN-Gruppen gebunden werden. Ein an eine LSN-Gruppe gebundenes Profil gilt für alle Abonnenten eines LSN-Clients, der an dieselbe Gruppe gebunden ist. Standardmäßig ist ein LSN-Transportprofil mit Standardeinstellungen für TCP-, UDP- und ICMP-Protokolle während der Erstellung an eine LSN-Gruppe gebunden. Dieses Profil wird als Standardtransportprofil bezeichnet. Ein LSN-Transportprofil, das Sie an eine LSN-Gruppe binden, überschreibt das standardmäßige LSN-Transportprofil für dieses Protokoll.
- **(Optional) Erstellen Sie ein LSN-Anwendungsprofil für ein bestimmtes Protokoll und binden Sie eine Reihe von Zielports daran**. Ein LSN-Anwendungsprofil definiert die LSN-Zuordnungs- und LSN-Filtersteuerelemente einer Gruppe für ein bestimmtes Protokoll und für eine Gruppe von Zielports. Für eine Gruppe von Zielports binden Sie ein LSN-Profil für jedes Protokoll (TCP, UDP und ICMP) an eine LSN-Gruppe. Ein Profil kann an mehrere LSN-Gruppen gebunden werden. Ein LSN-Anwendungsprofil, das an eine LSN-Gruppe gebunden ist, gilt für alle Abonnenten eines LSN-Clients, der an dieselbe Gruppe gebunden ist. Standardmäßig ist ein LSN-Anwendungsprofil mit Standardeinstellungen für TCP-, UDP- und ICMP-Protokolle für alle Zielports während der Erstellung an eine LSN-Gruppe gebunden. Dieses Profil wird

als Standardanwendungsprofil bezeichnet. Wenn Sie ein LSN-Anwendungsprofil mit einem bestimmten Satz von Zielports an eine LSN-Gruppe binden, überschreibt das gebundene Profil das standardmäßige LSN-Anwendungsprofil für dieses Protokoll an dieser Gruppe von Zielports. Die Befehlszeilenschnittstelle verfügt über zwei Befehle zum Erstellen eines LSN-Anwendungsprofils und zum Binden eines Satzes von Zielports an das LSN-Anwendungsprofil. Das Konfigurationsdienstprogramm kombiniert diese beiden Vorgänge auf einem einzigen Bildschirm.

- **Erstellen Sie eine LSN-Gruppe und binden Sie LSN-Pools, LSN-IPv6-Profil, (optional) LSN-Transportprofile und (optional) LSN-Anwendungsprofile an die LSN-Gruppe**. Eine LSN-Gruppe ist eine Entität, die aus einem LSN-Client, einem LSN-IPv6-Profil, LSN-Pool, LSN-Transportprofilen und LSN-Anwendungsprofilen besteht. B. Port-Blockgröße und Protokollierung von LSN-Sitzungen. Die Parametereinstellungen gelten für alle Abonnenten eines LSN-Clients, der an die LSN-Gruppe gebunden ist. Nur ein LSN-IPv6-Profil kann an eine LSN-Gruppe gebunden werden, und ein LSN-IPv6-Profil, das an eine LSN-Gruppe gebunden ist, kann nicht an andere LSN-Gruppen gebunden werden. Nur LSN-Pools und LSN-Gruppen mit denselben NAT-Typeinstellungen können miteinander verbunden werden. Mehrere LSN-Pools können an eine LSN-Gruppe gebunden werden. Nur eine LSN-Client-Entität kann an eine LSN-Gruppe gebunden werden, und eine LSN-Client-Entität, die an eine LSN-Gruppe gebunden ist, kann nicht an andere LSN-Gruppen gebunden werden. Die Befehlszeilenschnittstelle verfügt über zwei Befehle zum Erstellen einer LSN-Gruppe und zum Binden von LSN-Pools, LSN-Transportprofilen und LSN-Anwendungsprofilen an die LSN-Gruppe. Das Konfigurationsdienstprogramm kombiniert diese beiden Vorgänge in einem einzigen Bildschirm.

Konfiguration über die Befehlszeile

So erstellen Sie einen LSN-Client mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn client <clientname>

show lsn client
<!--NeedCopy-->
```

So binden Sie ein IPv6-Netzwerk oder eine ACL6-Regel über die Befehlszeilenschnittstelle an einen LSN-Client:

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
bind lsn client <clientname> (-network6 <ipv6_addr|*>| -acl6name <
    string>)

show lsn client
<!--NeedCopy-->
```

So erstellen Sie einen LSN-Pool mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn pool <poolname> [-nattype ( DYNAMIC )] [-portblockallocation (
    ENABLED | DISABLED )] [-portrealloctimeout <secs>] [-
    maxPortReallocTmq <positive_integer>]

show lsn pool
<!--NeedCopy-->
```

So binden Sie einen IP-Adressbereich mit der Befehlszeilenschnittstelle an einen LSN-Pool:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn pool <poolname> <lsnip>

show lsn pool
<!--NeedCopy-->
```

Hinweis: Verwenden Sie zum Entfernen von LSN-IP-Adressen aus einem LSN-Pool den Befehl unbind lsn pool.

So konfigurieren Sie ein LSN-IPv6-Profil mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn ip6profile <name>  -type DS-Lite  -network6 < ipv6_addr|*s >

show lsn ip6profile
<!--NeedCopy-->
```

So erstellen Sie ein LSN-Transportprofil mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add lsn transportprofile <transportprofilename> <transportprotocol> [-
    sessiontimeout <secs>] [-finrsttimeout <secs>] [-portquota <
    positive_integer>] [-sessionquota <positive_integer>] [-
    portpreserveparity ( ENABLED | DISABLED )] [-portpreserverange (
    ENABLED | DISABLED )] [-syncheck ( ENABLED | DISABLED )]

show lsn transportprofile
<!--NeedCopy-->
```

So erstellen Sie ein LSN-Anwendungsprofil mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn appsprofile <appsprofilename> <transportprotocol> [-ippooling (
    PAIRED | RANDOM )] [-mapping <mapping>] [-filtering <filtering>][-
    tcpproxy ( ENABLED | DISABLED )] [-td <positive_integer>]

show lsn appsprofile
<!--NeedCopy-->
```

So binden Sie einen Anwendungsprotokollportbereich mit der Befehlszeilenschnittstelle an ein LSN-Anwendungsprofil:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn appsprofile <appsprofilename> <lsnport>

show lsn appsprofile
<!--NeedCopy-->
```

So erstellen Sie eine LSN-Gruppe mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn group <groupname> -clientname <string> [-nattype ( DYNAMIC )]
    [-portblocksize <positive_integer>] [-logging (ENABLED | DISABLED )]
     [-sessionLogging ( ENABLED | DISABLED )][-sessionSync ( ENABLED |
    DISABLED )] [-snmptraplimit<positive_integer>] [-ftp ( ENABLED |
    DISABLED )] [-pptp ( ENABLED |DISABLED )] [-sipalg ( ENABLED |
    DISABLED )] [-rtspalg ( ENABLED |DISABLED )] [-ip6profile <string>]

```



```
3 show lsn group
4 <!--NeedCopy-->
```

So binden Sie LSN-Protokollprofile und LSN-Pools mit der Befehlszeilenschnittstelle an eine LSN-Gruppe:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind lsn group <groupname> (-poolname <string> | -transportprofilename
     <string> | -httphdrlogprofilename <string> | -appsprofilename <
     string> | -sipalgprofilename <string> | rtspalgprofilename <string>)
2
3 show lsn group
4 <!--NeedCopy-->
```

Konfiguration mit dem Konfigurationsdienstprogramm

So konfigurieren Sie einen LSN-Client und binden eine IPv6-Netzwerkadresse oder eine ACL6-Regel mit dem Konfigurationsdienstprogramm:

Navigieren Sie zu **System** > **Large Scale NAT** > **Clients**, fügen Sie einen Client hinzu, und binden Sie dann eine IPv6-Netzwerkadresse oder eine ACL6-Regel an den Client.

So konfigurieren Sie einen LSN-Pool und binden NAT-IP-Adressen mit dem Konfigurationsdienstprogramm:

Navigieren Sie zu **System** > **Large Scale NAT** > **Pools**, fügen Sie einen Pool hinzu und binden Sie dann eine NAT-IP-Adresse oder einen Bereich von NAT-IP-Adressen an den Pool.

So konfigurieren Sie ein LSN-IPv6-Profil mit dem Konfigurationsdienstprogramm:

Navigieren Sie zu **System** > **Large Scale NAT** > **Profile**, klicken Sie auf die Registerkarte **IPv6**, und weisen Sie eine IPv6-Adresse für DS-Lite AFTR zu.

So konfigurieren Sie ein LSN-Transportprofil mit dem Konfigurationsdienstprogramm:

1. Navigieren Sie zu **System** > **Large Scale NAT** > **Profile**.
2. Klicken Sie im Detailbereich auf **Transport**, und fügen Sie dann ein Transportprofil hinzu.

So konfigurieren Sie ein LSN-Anwendungsprofil mit dem Konfigurationsdienstprogramm:

1. Navigieren Sie zu **System** > **Large Scale NAT** > **Profile**.
2. Klicken Sie im Detailbereich auf **Anwendung**, und fügen Sie dann ein Anwendungsprofil hinzu.

So konfigurieren Sie eine LSN-Gruppe und binden einen LSN-Client, ein LSN-IPv6-Profil, Pools, Transportprofile und Anwendungsprofile mit dem Konfigurationsdienstprogramm:

Navigieren Sie zu **System** > **Large Scale NAT** > **Groups**, fügen Sie eine Gruppe hinzu und binden Sie dann einen LSN-Client, ein LSN-IPv6-Profil, Pools, Transportprofile und Anwendungsprofile an die Gruppe.

```
> add lsn client LSN-DSLITE-CLIENT-1
Done
> bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/100
Done
> add lsn pool LSN-DSLITE-POOL-1
Done
> bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70
Done
> add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
   DB8::5:6
Done
> add lsn group LSN-DSLITE-GROUP-1 -clientname LSN-DSLITE-CLIENT-1 -
   portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-1
Done
> add lsn group LSN-DSLITE-GROUP-1 -poolname LSN-DSLITE-POOL-1
Done
```

Protokollierung und Überwachung DS-Lite

Sie können DS-Lite-Informationen protokollieren, um Probleme zu diagnostizieren oder zu beheben und gesetzliche Anforderungen zu erfüllen. Die Citrix ADC Appliance unterstützt alle LSN-Protokollierungsfunktionen für die Protokollierung von DS-Lite-Informationen. Verwenden Sie zum Konfigurieren der DS-Lite-Protokollierung die unter Logging and Monitoring LSN beschriebenen Verfahren zum Konfigurieren der LSN-Protokollierung.

Eine Protokollmeldung für einen DS-Lite LSN-Zuordnungseintrag besteht aus folgenden Informationen:

- Citrix ADC eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel
- Eintragstyp (MAPPING)
- Ob der DS-Lite LSN-Zuordnungseintrag erstellt oder gelöscht wurde
- IPv6-Adresse von B4
- IP-Adresse, Port und Traffic-Domänen-ID des Abonnenten
- NAT IP-Adresse und Port
- Protokollname

- Ziel-IP-Adresse, -Port und -Domänen-ID sind möglicherweise vorhanden, abhängig von den folgenden Bedingungen:
  - Ziel-IP-Adresse und -Port werden für die endpoint-unabhängige Zuordnung nicht protokolliert.
  - Für die Adressenabhängige Zuordnung wird nur die Ziel-IP-Adresse protokolliert. Der Port wird nicht protokolliert.
  - Ziel-IP-Adresse und -Port werden für die Adress-Port-abhängige Zuordnung protokolliert.

Eine Protokollmeldung für eine DS-Lite-Sitzung besteht aus folgenden Informationen:

- Citrix ADC eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel
- Eintragstyp (SESSION)
- Ob die DS-Lite-Sitzung erstellt oder entfernt wird
- IPv6-Adresse von B4
- IP-Adresse, Port und Traffic-Domänen-ID des Abonnenten
- NAT IP-Adresse und Port
- Protokollname
- Ziel-IP-Adresse, -Port und -Domänen-ID des Datenverkehrs

Die folgende Tabelle zeigt Beispieleinträge für DS-Lite-Protokolle jedes Typs, der auf den konfigurierten Protokollservern gespeichert ist. Diese Protokolleinträge werden von einer Citrix ADC Appliance generiert, deren NSIP-Adresse 10.102.37.115 lautet. Sie können DS-Lite-Informationen protokollieren, um Probleme zu diagnostizieren oder zu beheben und gesetzliche Anforderungen zu erfüllen. Die Citrix ADC Appliance unterstützt alle LSN-Protokollierungsfunktionen für die Protokollierung von DS-Lite-Informationen. Verwenden Sie zum Konfigurieren der DS-Lite-Protokollierung die unter Logging and Monitoring LSN beschriebenen Verfahren zum Konfigurieren der LSN-Protokollierung.

Eine Protokollmeldung für einen DS-Lite LSN-Zuordnungseintrag besteht aus folgenden Informationen:

- Citrix ADC eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel
- Eintragstyp (MAPPING)
- Ob der DS-Lite LSN-Zuordnungseintrag erstellt oder gelöscht wurde
- IPv6-Adresse von B4
- IP-Adresse, Port und Traffic-Domänen-ID des Abonnenten
- NAT IP-Adresse und Port
- Protokollname
- Ziel-IP-Adresse, -Port und -Domänen-ID sind möglicherweise vorhanden, abhängig von den folgenden Bedingungen:

- Ziel-IP-Adresse und -Port werden für die endpoint-unabhängige Zuordnung nicht protokolliert.
- Für die Adressenabhängige Zuordnung wird nur die Ziel-IP-Adresse protokolliert. Der Port wird nicht protokolliert.
- Ziel-IP-Adresse und -Port werden für die Adress-Port-abhängige Zuordnung protokolliert.

Eine Protokollmeldung für eine DS-Lite-Sitzung besteht aus folgenden Informationen:

- Citrix ADC eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel
- Eintragstyp (SESSION)
- Ob die DS-Lite-Sitzung erstellt oder entfernt wird
- IPv6-Adresse von B4
- IP-Adresse, Port und Traffic-Domänen-ID des Abonnenten
- NAT IP-Adresse und Port
- Protokollname
- Ziel-IP-Adresse, -Port und -Domänen-ID des Datenverkehrs

Die folgende Tabelle zeigt Beispieleinträge für DS-Lite-Protokolle jedes Typs, der auf den konfigurierten Protokollservern gespeichert ist. Diese Protokolleinträge werden von einer Citrix ADC Appliance generiert, deren NSIP-Adresse 10.102.37.115 lautet.

LSN-Protokolleintragstyp	Beispielprotokolleintrag
DS-Lite-Sitzungserstellung	Local4.Informational 10.102.37.115 08/14/2015:13:35:38 GMT 0-PPE-1 : default LSN LSN_SESSION 37647607 0 : SESSION CREATED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 203.0.113.61:3002, Destination IP:Port:TD 198.51.100.250:80:0, Protocol:TCP
DS-Lite-Sitzungslöschung	Local4.Informational 10.102.37.115 08/14/2015:13:38:22 GMT 0-PPE-1 : default LSN LSN_SESSION 37647617 0 : SESSION DELETED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 203.0.113.61:3002, Destination IP:Port:TD 198.51.100.250:80:0, Protocol: TCP

DS-Lite LSN-Mapping-Erstellung	Local4.Informational 10.102.37.115 08/14/2015:13:35:39 GMT 0-PPE-1 : default LSN LSN_EIM_MAPPING 37647610 0 : EIM CREATED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 198.51.100.250:80, Protocol: TCP
DS-Lite LSN-Zuordnung Löschen	Local4.Informational 10.102.37.115 08/14/2015:13:38:25 GMT 0-PPE-1 : default LSN LSN_EIM_MAPPING 37647618 0 : EIM DELETED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 198.51.100.250:80, Protocol: TCP

Aktuelle DS-Lite-Sitzungen anzeigen

Sie können die aktuellen DS-Lite-Sitzungen anzeigen, um unerwünschte oder ineffiziente Sitzungen auf der Citrix ADC Appliance zu erkennen. Sie können alle oder einige DS-Lite-Sitzungen auf der Grundlage von Auswahlparametern anzeigen.

Konfiguration über die Befehlszeilenschnittstelle

So zeigen Sie alle DS-Lite-Sitzungen mit der Befehlszeilenschnittstelle an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show lsn session -nattype DS-Lite
<!--NeedCopy-->
```

So zeigen Sie ausgewählte DS-Lite-Sitzungen mit der Befehlszeilenschnittstelle an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show lsn session -nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```


Beispiel:

Die folgende Beispielausnahme zeigt alle DS-Lite-Sitzungen an, die auf einer Citrix ADC Appliance vorhanden sind:

```
show lsn session  - nattype DS-Lite
  B4-Address SubscrIP SubscrPort SubscrTD DstIP DstPort DstTD NatIP
     NatPort Proto Dir

1.  2001:DB8::3:4 192.0.2.51 2552 0 198.51.100.250 80 0 203.0.113.61
    3002 TCP OUT

2.  2001:DB8::3:4 192.0.2.51 3551 0 198.51.100.300 80 0 203.0.113.61
    52862 TCP OUT

3.  2001:DB8::3:4 192.0.2.100 4556 0 198.51.100.250 0 0 203.0.113.61
    48116 ICMP OUT

4.  2001: DB8::190 192.0.2.150 3881 0 198.51.100.199 80 0 203.0.113.69
    48305 TCP OUT

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

Konfiguration mit dem Konfigurationsdienstprogramm

So zeigen Sie alle oder ausgewählte DS-Lite-Sitzungen mit dem Konfigurationsdienstprogramm an

1. **Navigieren Sie zu System** > **Large Scale NAT** > **Sessions**und klicken Sie auf die Registerkarte **DS-Lite** .
2. Klicken Sie auf **Suchen**, um DS-Lite-Sitzungen anhand von Auswahlparametern anzuzeigen.

DS-Lite-Sitzungen löschen

Sie können unerwünschte oder ineffiziente DS-Lite-Sitzungen von der Citrix ADC Appliance entfernen. Die Appliance gibt sofort die für diese Sitzungen zugewiesenen Ressourcen (z. B. NAT-IP-Adresse, Port und Speicher) frei, sodass die Ressourcen für neue Sitzungen verfügbar sind. Die Appliance löscht auch alle nachfolgenden Pakete, die sich auf diese entfernten Sitzungen beziehen. Sie können alle oder ausgewählte DS-Lite-Sitzungen von der Citrix ADC Appliance entfernen.

So löschen Sie alle DS-Lite-Sitzungen mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
flush lsn session -nattype DS-Lite
show lsn session -nattype DS-Lite
```

So löschen Sie ausgewählte DS-Lite-Sitzungen mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
flush lsn session  - nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]

show lsn session  - nattype DS-Lite
<!--NeedCopy-->
```

So löschen Sie alle oder ausgewählte DS-Lite-Sitzungen mit dem Konfigurationsdienstprogramm:

1. Navigieren Sie zu **System** > **Large Scale NAT** > **Sessions**und klicken Sie auf die Registerkarte **DS-Lite**.
2. Klicken Sie auf **Sitzungen leeren**.

Konfigurieren statischer DS-Lite-Karten

October 5, 2021

Die Citrix ADC Appliance unterstützt die manuelle Erstellung von DS-Lite-LSN-Zuordnungen, die die Zuordnung zwischen den folgenden Informationen enthalten:

- IP-Adresse und Port des Teilnehmers sowie IPv6-Adresse des B4-Geräts oder -Komponente
- NAT IP-Adresse und Port

Statische DS-Lite-LSN-Zuordnungen sind nützlich, wenn Sie sicherstellen möchten, dass die initiierten Verbindungen zu einer NAT-IP-Adresse und Port der Teilnehmer-IP-Adresse und -Port über das angegebene B4-Gerät zugeordnet werden (z. B. Webserver im internen Netzwerk).

Hinweis: Diese Funktion wird in Version 11.0 Build 64.x und höher unterstützt.

So erstellen Sie eine statische DS-Lite-LSN-Zuordnung mit der Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add lsn static <name> <transportprotocol> <subscrIP> <subscrPort> [-td
    <positive_integer>] [-network6 <B4_ADDR>] [<natIP> [<natPort>]] [-
    destIP<ip_addr> [-dsttd <positive_integer>]]

show lsn static
<!--NeedCopy-->
```

Parameterbeschreibungen

add lsn static

- Name

Name des statischen LSN-Zuordnungseintrags. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem die LSN-Gruppe erstellt wurde. Die folgende Anforderung gilt nur für die CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “ds-lite lsn static1” oder ‘ds-lite lsn static1’). Dies ist ein obligatorisches Argument. Maximale Länge: 127

- transportprotocol

Protokoll für den DS-Lite LSN-Zuordnungseintrag.

- subscrIP

IPv4-Adresse eines Teilnehmers für den DS-Lite LSN-Zuordnungseintrag.

- subscrPort

Port des Teilnehmers für den DS-Lite LSN-Mapping-Eintrag.

- Network6

IPv6-Adresse des B4-Geräts oder der Komponente.

- td

ID der Verkehrsdomäne, zu der das B4-Gerät gehört. Die IPv6-Adresse des B4-Geräts wird im Parameter network6 angegeben. Wenn Sie keine ID angeben, wird davon ausgegangen, dass das B4-Gerät Teil der Standardverkehrsdomäne ist.

- natIP

IPv4-Adresse, die bereits auf der Citrix ADC Appliance als Typ LSN vorhanden ist und als NAT-IP-Adresse für diesen Zuordnungseintrag verwendet wird.

- natPort

NAT-Port für diesen DS-Lite LSN-Zuordnungseintrag.

- destIP

Ziel-IP-Adresse für den DS-Lite LSN-Zuordnungseintrag.

- dsttd

ID der Datenverkehrsdomäne, über die die Ziel-IP-Adresse für diesen DS-Lite-LSN-Zuordnungseintrag von der Citrix ADC Appliance erreichbar ist. Wenn Sie keine ID angeben, wird angenommen, dass die Ziel-IP-Adresse über die Standardverkehrsdomäne mit der ID 0 erreichbar ist.

So erstellen Sie eine statische DS-Lite-LSN-Zuordnung mit dem Konfigurationsdienstprogramm

Navigieren Sie zu System > Large Scale NAT > Statisch, und fügen Sie eine neue statische DS-Lite-LSN-Zuordnung hinzu.

Konfigurieren der deterministischen NAT-Zuweisung für DS-Lite

October 5, 2021

Deterministische NAT-Zuweisung für DS-Lite-LSN-Bereitstellungen ist eine Art NAT-Ressourcenzuweisung, bei der die Citrix ADC Appliance vorab aus dem LSN-NAT-IP-Pool und auf der Grundlage der angegebenen Portblockgröße eine LSN-NAT-IP-Adresse und einen Block von Ports für jeden Abonnenten (Abonnent hinter B4-Gerät) zuweist.

Hinweis: Diese Funktion wird in Version 11.0 Build 64.x und höher unterstützt.

Die Appliance weist diesen Abonnenten nacheinander NAT-Ressourcen zu. Der erste Block von Ports auf der beginnenden NAT-IP-Adresse wird der IP-Adresse des beginnenden Teilnehmers zugewiesen. Der nächste Bereich von Ports wird dem nächsten Abonnenten zugewiesen usw., bis die NAT-Adresse nicht über genügend Ports für den nächsten Abonnenten verfügt. Zu diesem Zeitpunkt wird der erste Portblock auf der nächsten NAT-Adresse dem Abonnenten zugewiesen usw.

Die Citrix ADC Appliance protokolliert die zugewiesene NAT-IP-Adresse und den Portblock für einen Abonnenten. Für eine Verbindung kann ein Teilnehmer nur durch seine zugeordnete NAT-IP-Adresse und Portblock identifiziert werden. Aus diesem Grund protokolliert die Citrix ADC Appliance nicht das Erstellen oder Löschen einer LSN-Sitzung.

Ein DS-Lite-Abonnent kann nur einen deterministischen Portblock haben. Wenn der gesamte Port Block verwendet wird, löscht die Citrix ADC Appliance jede neue Verbindung vom Abonnenten.

Beispiel: Deterministisches DS-Lite

In diesem Beispiel umfasst eine deterministische DS-Lite-Konfiguration vier Abonnenten mit IP-Adressen 192.0.17.5, 192.0.17.6, 192.0.17.7 und 192.0.17.8. Diese IPv4-Abonnenten befinden sich hinter einem B4-Gerät mit der IPv6-Adresse 2001:DB8:: 3:4. In dieser Konfiguration ist die Portblockgröße auf 20480 festgelegt und der LSN NAT IP-Adresspool hat IP-Adressen im Bereich 203.0.113.41-203.0.113.42.

Die Citrix ADC Appliance weist sequenziell aus dem LSN NAT IP-Pool und auf der Grundlage der festgelegten Portblockgröße eine LSN NAT-IP-Adresse und einen Block von Ports zu jedem Abonnenten. Der erste Block von Ports (1024-21503) an der beginnenden NAT-IP-Adresse (203.0.113.41) wird der IP-Adresse des beginnenden Teilnehmers (192.0.17.5) zugewiesen. Der nächste Bereich von Ports wird dem nächsten Abonnenten zugewiesen usw., bis die NAT-Adresse nicht über genügend Ports für den nächsten Abonnenten verfügt. Zu diesem Zeitpunkt wird der erste Portblock auf der nächsten NAT-IP-Adresse dem Abonnenten zugewiesen usw. Der Citrix ADC protokolliert die NAT-IP-Adresse und den für jeden Abonnenten zugewiesenen Ports.

Die Citrix ADC Appliance protokolliert keine für diese Abonnenten erstellten oder gelöschten LSN-Sitzungen.

In der folgenden Tabelle sind die NAT-IP-Adresse und die Ports aufgeführt, die jedem Abonnenten in diesem Beispiel zugewiesen werden:

IP-Adresse des Teilnehmers	Zugewiesene NAT-IP-Adresse	Zugeteilter Block von Ports	IPv6-Adresse von B4
192.0.17.5	203.0.113.41	1024 - 21503	2001:DB8::3:4
192.0.17.6	203.0.113.41	21504 - 41983	2001:DB8::3:4
192.0.17.7	203.0.113.41	41984 - 62463	2001:DB8::3:4
192.0.17.8	203.0.113.42	1024 - 21503	2001:DB8::3:4

Konfigurationsschritte

Sie müssen deterministische NAT als Teil der DS-Lite-Konfiguration konfigurieren. Anweisungen zum Konfigurieren von DS-Lite finden Sie unter Konfigurieren von DS-Lite.

Stellen Sie bei der Konfiguration von DS-Lite sicher, dass Sie:

- Legen Sie den Parameter NAT-Typ auf Deterministisch fest, wenn Sie den LSN-Pool und die LSN-Gruppe hinzufügen.
- Legen Sie beim Hinzufügen der LSN-Gruppe den gewünschten Portblockgrößenparameter fest,

es sei denn, Sie können den Standardwert akzeptieren.

Punkte, die vor der Konfiguration von Deterministic DS-Lite zu beachten sind

Berücksichtigen Sie folgende Punkte, bevor Sie deterministisches DS-Lite konfigurieren:

- Die vollständige IP-Adresse jedes Teilnehmers muss in einem separaten Befehl add lsn client angegeben werden, indem die Parameter Network und Netmask festgelegt werden. (Setzen Sie Netzmaske auf 255.255.255.255.) Außerdem muss die IPv4-Adresse des im Parameter Network6 angegebenen B4-Geräts vollständig sein (/128-Präfix). Mit anderen Worten, Netzwerk- und Netzwerk6-Parameter akzeptieren keine anderen Adressen als /32-Bit-Maske bzw. /128-Präfix.
- Die Citrix ADC Appliance löscht Verbindungen von Abonnenten, die nicht in einer deterministischen DS-Lite-Konfiguration angegeben sind, sich aber hinter B4-Geräten befinden, die in einer deterministischen DS-Lite-Konfiguration angegeben sind.
- Die Citrix ADC Appliance erkennt Abonnenten mit derselben IPv4-Adresse wie verschiedene Abonnenten, wenn sie sich hinter verschiedenen B4-Geräten befinden. Eine Kombination aus Subscriber IPv4-Adresse und B4-Gerät definiert einen eindeutigen Abonnenten in der LSN-Client-Entität einer DS-Lite-Konfiguration.

Beispiel für deterministische DS-Lite-Konfiguration:

Die folgende Konfiguration verwendet die im Abschnitt Beispiel: Deterministic DS-Lite aufgeführten Einstellungen.

```
1  add lsn client LSN-DSLITE-CLIENT-10
2
3  Done
4  bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.5 -netmask
       255.255.255.255 -network6 2001:DB8::3:4/128
5
6  Done
7  bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.6 -netmask
       255.255.255.255 -network6 2001:DB8::3:4/128
8
9  Done
10 bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.7 -netmask
       255.255.255.255 -network6 2001:DB8::3:4/128
11
12 Done
13 bind lsn client LSN-DSLITE-CLIENT-10 -network 192.0.17.8 -netmask
       255.255.255.255 -network6 2001:DB8::3:4/128
14
```



```
15 Done
16 add lsn pool LSN-DSLITE-POOL-10 -nattype DETERMINISTIC
17
18 Done
19 bind lsn pool LSN-DSLITE-POOL-10  203.0.113.41-203.0.113.42
20
21 Done
22 add lsn ip6profile LSN-DSLITE-PROFILE-10 -type DS-Lite -network6 2001:
      DB8::5:6
23
24 Done
25 add lsn group LSN-DSLITE-GROUP-10 -clientname LSN-DSLITE-CLIENT-10 -
      nattype DETERMINISTIC -portblocksize 20480 -ip6profile LSN-DSLITE-
      PROFILE-10
26
27 Done
28 bind lsn group LSN-DSLITE-GROUP-10 -poolname LSN-DSLITE-POOL-10
29
30 Done
31 <!--NeedCopy-->
```

Konfigurieren von Application Layer Gateways für DS-Lite

October 5, 2021

Bei einigen Protokollen der Anwendungsschicht werden auch die IP-Adressen und Protokollportnummern in der Nutzlast des Pakets kommuniziert. Application Layer Gateway (AGL) für ein Protokoll analysiert die Paketnutzlast und führt notwendige Änderungen durch, um sicherzustellen, dass das Protokoll weiterhin über DS-Lite funktioniert.

Die Citrix ADC Appliance unterstützt ALG für die folgenden Protokolle für DS-Lite:

- FTP
- ICMP
- TFTP
- SIP
- RTSP

Application Layer Gateway für FTP-, ICMP- und TFTP-Protokolle

October 5, 2021

Sie können ALG für das FTP-Protokoll für eine DS-Lite-Konfiguration aktivieren oder deaktivieren, indem Sie die Option FTP ALG der LSN-Gruppe der Konfiguration aktivieren oder deaktivieren.

ALG für das ICMP-Protokoll ist standardmäßig aktiviert, und es gibt keine Möglichkeit, es zu deaktivieren.

ALG für das TFTP-Protokoll ist standardmäßig deaktiviert. TFTP ALG wird automatisch für eine DS-Lite-Konfiguration aktiviert, wenn Sie ein UDP LSN-Anwendungsprofil mit endpunktunabhängiger Zuordnung, endpunktunabhängiger Filterung und Zielport als 69 (bekannter Port für TFTP) an die LSN-Gruppe binden.

Application Layer Gateway für SIP-Protokoll

October 5, 2021

Die Verwendung von DS-Lite mit Session Initiation Protocol (SIP) ist kompliziert, da SIP-Nachrichten sowohl in den SIP-Headern als auch im SIP-Body IP-Adressen enthalten. Wenn LSN mit SIP verwendet wird, enthalten die SIP-Header Informationen über den Anrufer und den Empfänger, und das Gerät übersetzt diese Informationen, um sie vor dem externen Netzwerk zu verstecken. Der SIP-Body enthält die SDP-Informationen (Session Description Protocol), die IP-Adressen und Portnummern für die Übertragung der Medien enthalten. SIP ALG für DS-Lite ist kompatibel mit RFC 3261, RFC 3581, RFC 4566 und RFC 4475.

> **Hinweis:**
>
> SIP ALG wird in einer eigenständigen Citrix ADC Appliance, in einem Citrix ADC-Hochverfügbarkeitssetup sowie in einem Citrix ADC-Cluster-Setup unterstützt.

Einschränkungen der SIP ALG

SIP ALG für DS-Lite hat folgende Einschränkungen:

- Es wird nur SDP-Nutzlast unterstützt.
- Folgende Komponenten werden nicht unterstützt:
  - Multicast-IP-Adressen
  - Verschlüsseltes SDP
  - SIP TLS
  - FQDN-Übersetzung

- SIP-Layer-Authentifizierung
- Admin-Partitionen
- Mehrteiliger Körper
- Linie faltbar

Konfigurieren von SIP ALG

Sie müssen die SIP ALG als Teil der LSN-Konfiguration konfigurieren. Anweisungen zum Konfigurieren von LSN finden Sie unter Konfigurieren von DS-Lite. Stellen Sie beim Konfigurieren von LSN sicher, dass Sie:

- Legen Sie beim Hinzufügen eines LSN-Anwendungsprofils die folgenden Parameter fest:
  - IP-Pooling = PAIRED
  - Adress- und Portzuordnung = ENDPOINT-INDEPENDENT
  - Filterung = ENDPOINT-INDEPENDENT
- Erstellen Sie ein SIP-ALG-Profil und stellen Sie sicher, dass Sie entweder den Quellportbereich oder den Zielportbereich definieren. Binden Sie das SIP-ALG-Profil an die LSN-Gruppe
- SIP ALG in der LSN-Gruppe aktivieren

So aktivieren Sie SIP ALG für eine LSN-Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn group <groupname> -clientname <string>[-sipalg ( ENABLED |
    DISABLED )]

show lsn group<groupname>
<!--NeedCopy-->
```

So aktivieren Sie SIP ALG für eine LSN-Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn sipalgprofile<sipalgprofilename>[-dataSessionIdleTimeout<
    positive_integer>][-sipSessionTimeout<positive_integer>][-
    registrationTimeout<positive_integer>][-sipsrcportrange<port[-port
    ]>][-sipdstportrange<port[-port]>][-openRegisterPinhole ( ENABLED |
    DISABLED )][-openContactPinhole ( ENABLED | DISABLED )][-
```



```
    openViaPinhole ( ENABLED | DISABLED )][-openRecordRoutePinhole (
    ENABLED | DISABLED )]-sipTransportProtocol ( TCP | UDP )[-
    openRoutePinhole ( ENABLED | DISABLED )][-rport ( ENABLED | DISABLED
     )]
2
3 show lsn sipalgprofile<sipalgprofilename>
4 <!--NeedCopy-->
```

Beispielkonfiguration

Die folgende DS-Lite-Beispielkonfiguration, SIP ALG ist für TCP-Datenverkehr von B4-Geräten im Netzwerk 2001:DB8::3:0/96 aktiviert.

```
1  add lsn client LSN-DSLITE-CLIENT-1
2  Done
3  bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/96
4  Done
5  add lsn pool LSN-DSLITE-POOL-1
6  Done
7  bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70
8  Done
9  add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
     DB8::5:6
10 Done
11 add lsn appsprofile LSN-DSLITE-APPS-PROFILE-1 TCP -ippooling PAIRED -
     mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
12 Done
13 add lsn sipalgprofile SIPALGPROFILE-1  -sipdstportrange 5060 -
     sipTransportProtocol TCP
14 Done
15 add lsn group LSN-DSLITE-GROUP-1 -clientname LSN-DSLITE-CLIENT-1 -
     portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-1 -sipalg ENABLED
16 Done
17 bind lsn group LSN-DSLITE-GROUP-1 -poolname LSN-DSLITE-POOL-1
18 Done
19 bind lsn group LSN-DSLITE-GROUP-1 -appsprofilename LSN-DSLITE-APPS-
     PROFILE-1
20 Done
21 bind lsn group LSN-DSLITE-GROUP-1 -sipalgprofilename SIPALGPROFILE-1
22 Done
23 <!--NeedCopy-->
```


Application Layer Gateway für RTSP-Protokoll

October 5, 2021

Real Time Streaming Protocol (RTSP) ist ein Protokoll auf Anwendungsebene für die Übertragung von Echtzeit-Mediendaten. RTSP wird zum Einrichten und Steuern von Mediensitzungen zwischen Endpunkten verwendet und ist ein Kontrollkanalprotokoll zwischen dem Media-Client und dem Medienserver. Die typische Kommunikation ist zwischen einem Client und einem Streaming-Medienserver.

Das Streamen von Medien aus einem privaten Netzwerk in ein öffentliches Netzwerk erfordert die Übersetzung von IP-Adressen und Portnummern über das Netzwerk. Die Citrix ADC Funktionalität umfasst ein Application Layer Gateway (ALG) für RTSP, das mit Large Scale NAT (LSN) verwendet werden kann, um den Medienstrom zu analysieren und alle erforderlichen Änderungen vorzunehmen, um sicherzustellen, dass das Protokoll weiterhin über das Netzwerk funktioniert.

Die IP-Adressenübersetzung hängt vom Typ und der Richtung der Nachricht sowie vom Typ der Medien ab, die von der Client-Server-Bereitstellung unterstützt werden. Nachrichten werden wie folgt übersetzt:

- Ausgehende Anforderung: Private IP-Adresse an die öffentliche IP-Adresse des Citrix ADC namens LSN-IP-Adresse.
- Eingehende Antwort: LSN-IP-Adresse an private IP-Adresse.
- Eingangsanforderung: Keine Übersetzung.
- Ausgehende Antwort: Private IP-Adresse an die IP-Adresse des LSN-Pools.

> **Hinweis:**
>
> RTSP ALG wird in einer eigenständigen Citrix ADC Appliance, in einem Citrix ADC-Hochverfügbarkeitssetup sowie in einem Citrix ADC-Cluster-Setup unterstützt.

Einschränkungen der RTSP ALG

Die RTSP ALG unterstützt nicht Folgendes:

- Multicast-RTSP-Sitzungen
- RTSP-Sitzung über UDP
- Admin-Partitionen
- RTSP-Authentifizierung
- HTTP-Tunneling

Konfigurieren von RTSP ALG

Konfigurieren Sie RTSP ALG als Teil der LSN-Konfiguration. Anweisungen zum Konfigurieren von LSN finden Sie unter Konfigurieren von DS-Lite. Stellen Sie beim Konfigurieren von LSN sicher, dass Sie:

- Legen Sie beim Hinzufügen eines LSN-Anwendungsprofils die folgenden Parameter fest:
  - IP-Pooling = PAIRED
  - Adress- und Portzuordnung = ENDPOINT-INDEPENDENT
  - Filterung = ENDPOINT-INDEPENDENT
- RTSP ALG in der LSN-Gruppe aktivieren
- Erstellen Sie ein RTSP-ALG-Profil und binden Sie das RTSP-ALG-Profil an die LSN-Gruppe

So aktivieren Sie RTSP ALG für eine LSN-Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lsn group <groupname> -clientname <string> [-rtspalg ( ENABLED |
     DISABLED )]
2
3 show lsn group <groupname>
4 <!--NeedCopy-->
```

So aktivieren Sie RTSP ALG für eine LSN-Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lsn rtspalgprofile <rtspalgprofilename> [-rtspIdleTimeout <
     positive_integer>] -rtspportrange <port[-port]> [-
     rtspTransportProtocol (TCP|UDP)]
2
3 show lsn rtspalgprofile <rtspalgprofilename>
4 <!--NeedCopy-->
```

Beispiel-RTSP-ALG-Konfiguration

Die folgende DS-Lite-Beispielkonfiguration, RTSP ALG ist für TCP-Datenverkehr von B4-Geräten im Netzwerk 2001:DB8::4:0/96 aktiviert.

Beispiel-RTSP-ALG-Konfiguration:


```
add lsn client LSN-DSLITE-CLIENT-5
Done
bind lsn client LSN-DSLITE-CLIENT-5 -network6 2001:DB8::4:0/96
Done
add lsn pool LSN-DSLITE-POOL-5
Done
bind lsn pool LSN-DSLITE-POOL-5 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-DSLITE-PROFILE-5 -type DS-Lite -network6 2001:
   DB8::5:6
Done
add lsn appsprofile LSN-DSLITE-APPS-PROFILE-5 TCP -ippooling PAIRED -
   mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
Done
add lsn rtspalgprofile RTSPALGPROFILE-5 -rtspIdleTimeout 1000 -
   rtspportrange 554
Done
add lsn group LSN-DSLITE-GROUP-5 -clientname LSN-DSLITE-CLIENT-5 -
   portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-5 -rtspalg ENABLED
Done
bind lsn group LSN-DSLITE-GROUP-5 -poolname LSN-DSLITE-POOL-5
Done
bind lsn group LSN-DSLITE-GROUP-5 -appsprofilename LSN-DSLITE-APPS-
   PROFILE-5
Done
bind lsn group LSN-DSLITE-GROUP-5 -rtspalgprofilename RTSPALGPROFILE-5
Done
<!--NeedCopy-->
```

Protokollierung und Überwachung DS-Lite

October 5, 2021

Sie können DS-Lite-Informationen protokollieren, um Probleme zu diagnostizieren oder zu beheben und gesetzliche Anforderungen zu erfüllen. Die Citrix ADC Appliance unterstützt alle LSN-Protokollierungsfunktionen für die Protokollierung von DS-Lite-Informationen. Verwenden Sie zum Konfigurieren der DS-Lite-Protokollierung die unter Logging and Monitoring LSN beschriebenen Verfahren zum Konfigurieren der LSN-Protokollierung.

Eine Protokollmeldung für einen DS-Lite LSN-Zuordnungseintrag besteht aus folgenden Informationen:

- Citrix ADC eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel
- Eintragstyp (MAPPING)
- Ob der DS-Lite LSN-Zuordnungseintrag erstellt oder gelöscht wurde
- IPv6-Adresse von B4
- IP-Adresse, Port und Traffic-Domänen-ID des Abonnenten
- NAT IP-Adresse und Port
- Protokollname
- Ziel-IP-Adresse, -Port und -Domänen-ID sind möglicherweise vorhanden, abhängig von den folgenden Bedingungen:
  - Ziel-IP-Adresse und -Port werden für die endpoint-unabhängige Zuordnung nicht protokolliert.
  - Für die Adressenabhängige Zuordnung wird nur die Ziel-IP-Adresse protokolliert. Der Port wird nicht protokolliert.
  - Ziel-IP-Adresse und -Port werden für die Adress-Port-abhängige Zuordnung protokolliert.

Eine Protokollmeldung für eine DS-Lite-Sitzung besteht aus folgenden Informationen:

- Citrix ADC eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel
- Eintragstyp (SESSION)
- Ob die DS-Lite-Sitzung erstellt oder entfernt wird
- IPv6-Adresse von B4
- IP-Adresse, Port und Traffic-Domänen-ID des Abonnenten
- NAT IP-Adresse und Port
- Protokollname
- Ziel-IP-Adresse, -Port und -Domänen-ID des Datenverkehrs

Die folgende Tabelle zeigt Beispieleinträge für DS-Lite-Protokolle jedes Typs, der auf den konfigurierten Protokollservern gespeichert ist. Diese Protokolleinträge werden von einer Citrix ADC Appliance generiert, deren NSIP-Adresse 10.102.37.115 lautet. Sie können DS-Lite-Informationen protokollieren, um Probleme zu diagnostizieren oder zu beheben und gesetzliche Anforderungen zu erfüllen. Die Citrix ADC Appliance unterstützt alle LSN-Protokollierungsfunktionen für die Protokollierung von DS-Lite-Informationen. Verwenden Sie zum Konfigurieren der DS-Lite-Protokollierung die unter Logging and Monitoring LSN beschriebenen Verfahren zum Konfigurieren der LSN-Protokollierung.

Eine Protokollmeldung für einen DS-Lite LSN-Zuordnungseintrag besteht aus folgenden Informationen:

- Citrix ADC eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt

- Zeitstempel
- Eintragstyp (MAPPING)
- Ob der DS-Lite LSN-Zuordnungseintrag erstellt oder gelöscht wurde
- IPv6-Adresse von B4
- IP-Adresse, Port und Traffic-Domänen-ID des Abonnenten
- NAT IP-Adresse und Port
- Protokollname
- Ziel-IP-Adresse, -Port und -Domänen-ID sind möglicherweise vorhanden, abhängig von den folgenden Bedingungen:
  - Ziel-IP-Adresse und -Port werden für die endpoint-unabhängige Zuordnung nicht protokolliert.
  - Für die Adressenabhängige Zuordnung wird nur die Ziel-IP-Adresse protokolliert. Der Port wird nicht protokolliert.
  - Ziel-IP-Adresse und -Port werden für die Adress-Port-abhängige Zuordnung protokolliert.

Eine Protokollmeldung für eine DS-Lite-Sitzung besteht aus folgenden Informationen:

- Citrix ADC eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel
- Eintragstyp (SESSION)
- Ob die DS-Lite-Sitzung erstellt oder entfernt wird
- IPv6-Adresse von B4
- IP-Adresse, Port und Traffic-Domänen-ID des Abonnenten
- NAT IP-Adresse und Port
- Protokollname
- Ziel-IP-Adresse, -Port und -Domänen-ID des Datenverkehrs

Die folgende Tabelle zeigt Beispieleinträge für DS-Lite-Protokolle jedes Typs, der auf den konfigurierten Protokollservern gespeichert ist. Diese Protokolleinträge werden von einer Citrix ADC Appliance generiert, deren NSIP-Adresse 10.102.37.115 lautet.

LSN-Protokolleintragstyp	Beispielprotokolleintrag
DS-Lite-Sitzungserstellung	Local4.Informational 10.102.37.115 08/14/2015:13:35:38 GMT 0-PPE-1 : default LSN LSN_SESSION 37647607 0 : SESSION CREATED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 203.0.113.61:3002, Destination IP:Port:TD 198.51.100.250:80:0, Protocol:TCP

DS-Lite-Sitzungslöschung	Local4.Informational 10.102.37.115 08/14/2015:13:38:22 GMT 0-PPE-1 : default LSN LSN_SESSION 37647617 0 : SESSION DELETED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 203.0.113.61:3002, Destination IP:Port:TD 198.51.100.250:80:0, Protocol: TCP
DS-Lite LSN-Mapping-Erstellung	Local4.Informational 10.102.37.115 08/14/2015:13:35:39 GMT 0-PPE-1 : default LSN LSN_EIM_MAPPING 37647610 0 : EIM CREATED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 198.51.100.250:80, Protocol: TCP
DS-Lite LSN-Zuordnung Löschen	Local4.Informational 10.102.37.115 08/14/2015:13:38:25 GMT 0-PPE-1 : default LSN LSN_EIM_MAPPING 37647618 0 : EIM DELETED 2001:DB8::3:4 Client IP:Port:TD 192.0.2.51:2552:0, NatIP:NatPort 198.51.100.250:80, Protocol: TCP

Aktuelle DS-Lite-Sitzungen anzeigen

Sie können die aktuellen DS-Lite-Sitzungen anzeigen, um unerwünschte oder ineffiziente Sitzungen auf der Citrix ADC Appliance zu erkennen. Sie können alle oder einige DS-Lite-Sitzungen auf der Grundlage von Auswahlparametern anzeigen.

So zeigen Sie alle DS-Lite-Sitzungen mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 show lsn session -nattype DS-Lite
2 <!--NeedCopy-->
```

So zeigen Sie ausgewählte DS-Lite-Sitzungen mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
show lsn session  - nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```

Die folgende Beispielausnahme zeigt alle DS-Lite-Sitzungen an, die auf einer Citrix ADC Appliance vorhanden sind:

> lsn-Sitzung anzeigen —nattype DS-lite

```
  B4-Address SubscrIP SubscrPort SubscrTD DstIP DstPort DstTD NatIP
     NatPort Proto Dir

1. 2001:DB8::3:4 192.0.2.51 2552 0 198.51.100.250 80 0 203.0.113.61
    3002 TCP OUT

2. 2001:DB8::3:4 192.0.2.51 3551 0 198.51.100.300 80 0 203.0.113.61
    52862 TCP OUT

3. 2001:DB8::3:4 192.0.2.100 4556 0 198.51.100.250 0 0 203.0.113.61
    48116 ICMP OUT

4. 2001: DB8::190 192.0.2.150 3881 0 198.51.100.199 80 0 203.0.113.69
    48305 TCP OUT
Done
<!--NeedCopy-->
```

Konfiguration mit dem Konfigurationsdienstprogramm

So zeigen Sie alle oder ausgewählte DS-Lite-Sitzungen mit dem Konfigurationsdienstprogramm an

1. **Navigieren Sie zu System** > **Large Scale NAT** > **Sessions**und klicken Sie auf die Registerkarte **DS-Lite** .
2. Klicken Sie auf **Suchen**, um DS-Lite-Sitzungen anhand von Auswahlparametern anzuzeigen.

DS-Lite-Sitzungen löschen

Sie können unerwünschte oder ineffiziente DS-Lite-Sitzungen von der Citrix ADC Appliance entfernen. Die Appliance gibt sofort die für diese Sitzungen zugewiesenen Ressourcen (z. B. NAT-IP-Adresse, Port und Speicher) frei, sodass die Ressourcen für neue Sitzungen verfügbar sind. Die Appliance löscht

auch alle nachfolgenden Pakete, die sich auf diese entfernten Sitzungen beziehen. Sie können alle oder ausgewählte DS-Lite-Sitzungen von der Citrix ADC Appliance entfernen.

So löschen Sie alle DS-Lite-Sitzungen mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
flush lsn session -nattype DS-Lite

show lsn session -nattype DS-Lite
<!--NeedCopy-->
```

So löschen Sie ausgewählte DS-Lite-Sitzungen mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
flush lsn session -nattype DS-Lite [-clientname <string>] [-network <
    ip_addr> [-netmask <netmask>] [-td <positive_integer>]] [-natIP <
    ip_addr> [-natPort <port>]]

show lsn session -nattype DS-Lite
<!--NeedCopy-->
```

So löschen Sie alle oder ausgewählte DS-Lite-Sitzungen mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **System** > **Large Scale NAT** > **Sessions**und klicken Sie auf die Registerkarte **DS-Lite**.
2. Klicken Sie auf **Sitzungen leeren**.

Protokollieren von HTTP-Header-Informationen

Die Citrix ADC Appliance kann Anforderungsheader-Informationen einer HTTP-Verbindung protokollieren, die die DS-Lite-Funktionalität verwendet. Die folgenden Header-Informationen eines HTTP-Anforderungspakets können protokolliert werden:

- URL, für die die HTTP-Anforderung bestimmt ist
- HTTP-Methode, die in der HTTP-Anforderung angegeben ist
- HTTP-Version, die in der HTTP-Anforderung verwendet wird

- IPv4-Adresse des Abonnenten, der die HTTP-Anforderung gesendet hat

Die HTTP-Header-Protokolle können von ISPs verwendet werden, um die Trends im Zusammenhang mit dem HTTP-Protokoll unter einer Gruppe von Abonnenten zu sehen. Beispielsweise kann ein ISP diese Funktion verwenden, um die beliebteste Website unter einer Reihe von Abonnenten herauszufinden.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben aus, um die Citrix ADC Appliance zum Protokollieren von HTTP-Header-Informationen zu konfigurieren:

- **Erstellen Sie ein HTTP-Header-Log-Profil**. Ein HTTP-Header-Protokollprofil ist eine Sammlung von HTTP-Header-Attributen (z. B. URL und HTTP-Methode), die für die Protokollierung aktiviert oder deaktiviert werden können.
- **Binden Sie den HTTP-Header an eine LSN-Gruppe einer DS-Lite-LSN-Konfiguration**. Binden Sie das HTTP-Header-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie den HTTP-Header-Logprofilnamenparameter auf den Namen des erstellten HTTP-Header-Protokollprofils festlegen. Die Citrix ADC Appliance protokolliert dann HTTP-Header-Informationen aller HTTP-Anforderungen in Bezug auf die LSN-Gruppe. Ein HTTP-Header-Protokollprofil kann an mehrere LSN-Gruppen gebunden werden, aber eine LSN-Gruppe kann nur ein HTTP-Header-Protokollprofil haben.

So erstellen Sie ein HTTP-Header-Protokollprofil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lsn httphdrlogprofile <httphdrlogprofilename> [-logURL ( ENABLED |
     DISABLED )] [-logMethod ( ENABLED | DISABLED )] [-logVersion (
     ENABLED | DISABLED )] [-logHost ( ENABLED | DISABLED )]
2
3 show lsn httphdrlogprofile
4 <!--NeedCopy-->
```

So binden Sie ein HTTP-Header-Protokollprofil mit der Befehlszeilenschnittstelle an eine LSN-Gruppe

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
bind lsn group <groupname> -httphdrlogprofilename <string>

show lsn group <groupname>
<!--NeedCopy-->
```

Beispielkonfiguration

In der folgenden DS-Lite-LSN-Konfiguration ist HTTP-Header-Protokollprofil HTTP-Header-Log-1 an LSN-Gruppe LSN-DSLITE-GROUP-1 gebunden. Im Protokollprofil sind alle HTTP-Attribute (URL, HTTP-Methode, HTTP-Version und HOST-IP-Adresse) für die Protokollierung aktiviert, sodass alle diese Attribute für alle HTTP-Anforderungen von B4-Geräten protokolliert werden (im Netzwerk 2001:DB 8:5001: :/96).

Beispielkonfiguration:

```
add lsn httphdrlogprofile HTTP-HEADER-LOG-1

Done

add lsn client LSN-DSLITE-CLIENT-1

Done

bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/100

Done

add lsn pool LSN-DSLITE-POOL-1

Done

bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70

Done

add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
   DB8::5:6

Done

add lsn group LSN-DSLITE-GROUP-1 -clientname LSN-DSLITE-CLIENT-1 -
   portblocksize 1024 -ip6profile LSN-DSLITE-PROFILE-1
```



```
26
27 Done
28
29 bind lsn group LSN-DSLITE-GROUP-1 -poolname LSN-DSLITE-POOL-1
30
31 Done
32
33 bind lsn group LSN-DSLITE-GROUP-1 -httphdrlogprofilename HTTP-HEADER-
       LOG-1
34
35 Done
36 <!--NeedCopy-->
```

IPFIX-Protokollierung

Die Citrix ADC Appliance unterstützt das Senden von Informationen zu LSN-Ereignissen im IPFIX-Format (Internet Protocol Flow Information Export) an die konfigurierte Gruppe von IPFIX-Kollektoren. Die Appliance verwendet die vorhandene AppFlow Funktion, um LSN-Ereignisse im IPFIX-Format an die IPFIX-Kollektoren zu senden.

IPFIX-basierte Protokollierung ist für die folgenden DS_lite-bezogenen Ereignisse verfügbar:

- Erstellen oder Löschen einer LSN-Sitzung.
- Erstellen oder Löschen eines LSN-Zuordnungseintrags.
- Zuweisung oder Aufteilung von Portblöcken im Rahmen der deterministischen NAT.
- Zuweisung oder Aufteilung von Portblöcken im Kontext dynamischer NAT.
- Wann immer das Teilnehmersitzungskontingent überschritten wird.

Zu berücksichtigende Punkte, bevor Sie IPFIX-Protokollierung konfigurieren

Bevor Sie mit der Konfiguration von IPsec ALG beginnen, sollten Sie die folgenden Punkte beachten:

- Sie müssen die AppFlow Funktion und die IPFIX-Kollektoren auf der Citrix ADC Appliance konfigurieren. Anweisungen finden Sie unter Konfigurieren der AppFlow-Funktion.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben für die Protokollierung von LSN-Informationen im IPFIX-Format aus:

- **Aktivieren Sie die LSN-Protokollierung in der AppFlow Konfiguration**. Aktivieren Sie den LSN-Protokollierungsparameter als Teil der AppFlow Konfiguration.

- **Erstellen Sie ein LSN-Protokollprofil**. Ein LSN-Protokollprofil enthält den IPFIX-Parameter, mit dem die Protokollinformationen im IPFIX-Format aktiviert oder deaktiviert werden.
- **Binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration**. Binden Sie das LSN-Protokollprofil an eine oder mehrere LSN-Gruppen. Ereignisse im Zusammenhang mit der gebundenen LSN-Gruppe werden im IPFIX-Format protokolliert.

So aktivieren Sie die LSN-Protokollierung in der AppFlow Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set appflow param -lsnLogging (ENABLED |DISABLED )

show appflow param
<!--NeedCopy-->
```

Um ein LSN-Protokollprofil mit der CLI an der Eingabeaufforderung zu erstellen, geben Sie

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lsn logprofile <logProfileName>  -logipfix ( ENABLED | DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

So binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

So erstellen Sie ein LSN-Protokollprofil mit der GUI

Navigieren Sie zu **System** > **Large Scale NAT** > **Profile**, klicken Sie auf Register **Protokoll**, und fügen Sie dann ein Protokollprofil hinzu.

So binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration mit der GUI

1. Navigieren Sie zu **System** > **Large Scale NAT** > **LSN Group,** öffnen Sie die **LSN-Gruppe**.
2. Klicken Sie **unter Erweiterte Einstellungen** auf **+ Protokollprofil**, um das erstellte Protokollprofil an die LSN-Gruppe zu binden.

Port Control Protocol für DS-Lite

October 5, 2021

Citrix ADC Appliances unterstützen jetzt Port Control Protocol (PCP) für Large Scale NAT (LSN). Viele Abonnentenanwendungen eines ISP müssen über das Internet zugänglich sein (z. B. IOT-Geräte (Internet of Things), z. B. eine IP-Kamera, die die Überwachung über das Internet ermöglicht). Eine Möglichkeit, diese Anforderung zu erfüllen, besteht darin, statische Large Scale NAT-Karten (LSN) zu erstellen. Aber für eine sehr große Anzahl von Abonnenten ist das Erstellen statischer LSN NAT-Karten keine machbare Lösung.

Port Control Protocol (PCP) ermöglicht es einem Abonnenten, spezifische LSN NAT-Zuordnungen für sich selbst und/oder für andere Geräte von Drittanbietern anzufordern. Das große NAT-Gerät erstellt eine LSN-Karte und sendet sie an den Abonnenten. Der Abonnent sendet die entfernten Geräte über das Internet die NAT-IP-Adresse:NAT-Port, an der sie eine Verbindung zum Abonnenten herstellen können.

In der Regel senden Anwendungen häufig Keepalive-Nachrichten an das große NAT-Gerät, damit ihre LSN-Zuordnungen keine Timeout aufweisen. PCP hilft, die Häufigkeit solcher Keep-Alive-Nachrichten zu reduzieren, indem die Anwendungen die Timeout-Einstellungen der LSN-Zuordnungen erlernen können. Dies trägt dazu bei, den Bandbreitenverbrauch im Zugangsnetzwerk des ISP und den Batterieverbrauch auf mobilen Geräten zu reduzieren.

PCP ist ein Client-Server-Modell und läuft über das UDP-Transportprotokoll. Eine Citrix ADC Appliance implementiert die PCP-Serverkomponente und ist mit RFC 6887 kompatibel.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben für die Konfiguration von PCP aus:

- (Optional) Erstellen Sie ein PCP-Profil. Ein PCP-Profil enthält Einstellungen für PCP-bezogene Parameter (z. B. zum Abhören von Zuordnungen und Peer-PCP-Anforderungen). Ein PCP-Profil kann an einen PCP-Server gebunden werden. Ein PCP-Profil, das an einen PCP-Server gebunden ist, wendet alle seine Einstellungen auf den PCP-Server an. Ein PCP-Profil kann an

mehrere PCP-Server gebunden werden. Standardmäßig ist ein PCP-Profil mit Standardparametereinstellungen an alle PCP-Server gebunden. Ein PCP-Profil, das Sie an einen PCP-Server binden, überschreibt die standardmäßigen PCP-Profileinstellungen für diesen Server. Ein Standard-PCP-Profil weist die folgenden Parametereinstellungen auf:

- Zuordnung: Aktiviert
- Peer: Aktiviert
- Minimale Kartenlebensdauer: 120 Sekunden
- Maximale Lebensdauer: 86400 Sekunden
- Ankündigungsanzahl: 10
- Dritte: Deaktiviert

- Erstellen Sie einen PCP-Server und binden Sie ein PCP-Profil an ihn. Erstellen Sie einen PCP-Server auf der Citrix ADC Appliance, um PCP-bezogene Anforderungen und Nachrichten von den Abonnenten zu überwachen. Eine Subnetz-IP (SNIP) -Adresse muss einem PCP-Server zugewiesen werden, um darauf zuzugreifen. Standardmäßig überwacht ein PCP-Server Port 5351.
- Binden Sie den PCP-Server an eine LSN-Gruppe einer LSN-Konfiguration. Binden Sie den erstellten PCP-Server an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie den PCP-Server-Parameter so einstellen, dass der erstellte PCP-Server angegeben wird. Der erstellte PCP-Server kann nur von den Abonnenten dieser LSN-Gruppe zugegriffen werden.
  Hinweis: Ein PCP-Server für eine große NAT-Konfiguration erfüllt keine Anfragen von Abonnenten, die anhand von ACL-Regeln identifiziert wurden.

So erstellen Sie ein PCP-Profil mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add pcp profile <name> [-mapping ( ENABLED | DISABLED )] [-peer (
     ENABLED | DISABLED )] [-minMapLife <secs>]  [-maxMapLife <secs>] [-
     announceMultiCount <positive_integer>][-thirdParty ( ENABLED |
     DISABLED )]
2
3 show pcp profile <name>
4 <!--NeedCopy-->
```

So erstellen Sie einen PCP-Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add pcp server <name> <IPAddress> [-port <portNum|*>] [-pcpProfile <
    string>]

show pcp server <name>
<!--NeedCopy-->
```

Beispielkonfiguration für DS-LITE

In der folgenden Beispielkonfiguration ist PCP-Server PCP-SERVER-1 mit PCP-Einstellungen von PCP-DSLITE-PROFILE-1 an die LSN-Gruppe LSN-DSLITE-GROUP-1 gebunden. PCP-SERVER-9 dient PCP-Anfragen von IPv4-Abonnenten hinter B4-Geräten aus dem Netzwerk 2001:DB8::3:0/100.

Beispielkonfiguration:

```
add pcp profile PCP-DSLITE-PROFILE-1 -minMapLife 300
Done
add pcp server PCP-DSLITE-SERVER-1 192.0.3.10  -pcpProfile PCP-DSLITE-
    PROFILE-1
Done
add lsn client LSN-DSLITE-CLIENT-1
Done
bind lsn client LSN-DSLITE-CLIENT-1 -network6 2001:DB8::3:0/100
Done
add lsn pool LSN-DSLITE-POOL-1
Done
bind lsn pool LSN-DSLITE-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-DSLITE-PROFILE-1 -type DS-Lite -network6 2001:
    DB8::5:6
Done
add lsn group LSN-DSLITE-PROFILE-1 -clientname LSN-NAT64-CLIENT-1  -
    ip6profile LSN-NAT64-PROFILE-1
Done
bind lsn group LSN-DSLITE-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
bind lsn group LSN-DSLITE-GROUP-1 -poolname  PCP-NAT64-SERVER-1
Done
<!--NeedCopy-->
```


Großes NAT64

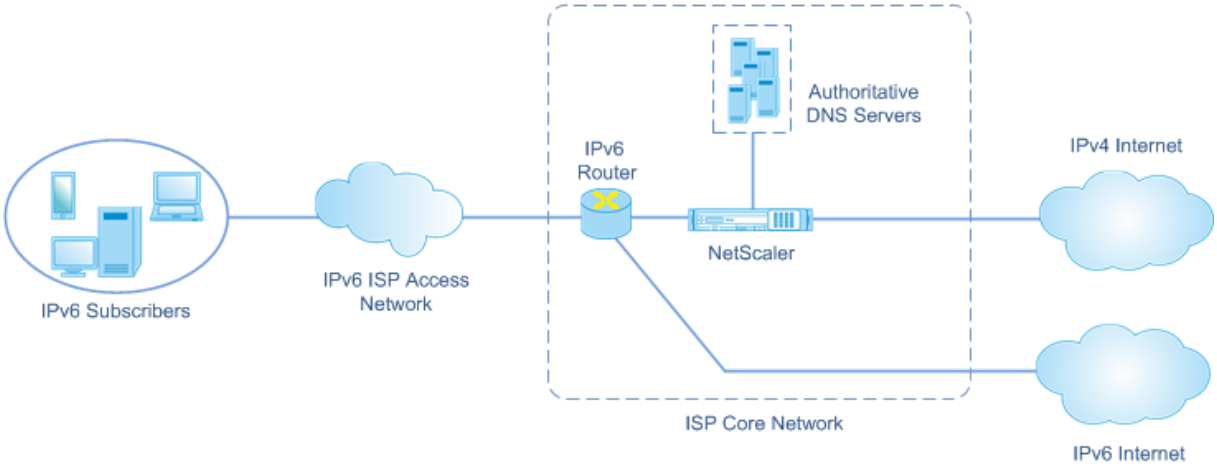
October 5, 2021

Aufgrund der bevorstehenden Erschöpfung von IPv4-Adressen haben ISPs den Übergang zur IPv6-Infrastruktur begonnen. Während des Übergangs müssen ISPs jedoch weiterhin IPv4 zusammen mit IPv6 unterstützen, da der Großteil des öffentlichen Internets immer noch IPv4 verwendet. Der große NAT64 ist eine IPv6-Übergangslösung für ISPs mit IPv6-Infrastruktur, um ihre nur IPv6-Abonnenten mit dem IPv4-Internet zu verbinden. DNS64 ist eine Lösung, um die Erkennung von nur IPv4-Domänen durch nur IPv6-Clients zu ermöglichen. DNS64 wird mit großem NAT64 verwendet, um eine nahtlose Kommunikation zwischen nur IPv6-Clients und nur IPv4-Servern zu ermöglichen.

Eine Citrix ADC Appliance implementiert große NAT64 und DNS64 und ist kompatibel mit RFCs 6145, 6146, 6147, 6052, 3022, 2373, 2765 und 2464.

Architektur

Die NAT64-Architektur eines ISP, der eine Citrix ADC Appliance verwendet, besteht aus IPv6-Abonnenten, die über eine Citrix ADC-Appliance auf das IPv4-Internet zugreifen, die im Kernnetzwerk des ISP bereitgestellt wird. IPv6-Abonnenten sind über das reine IPv6-Zugriffsnetzwerk des ISP mit dem Kernnetzwerk des ISP verbunden.



Die groß angelegte NAT64-Funktionalität einer Citrix ADC Appliance ermöglicht die Kommunikation zwischen IPv6-Clients und IPv4-Servern über IPv6-zu-IPv4-Paketübersetzung und umgekehrt, während die Sitzungsinformationen auf der Citrix ADC-Appliance.Citrix ADC DNS64-Funktionalität stellt nur IPv4-Domänen zu IPv6- Abonnenten, indem DNS-AAAA-Einträge für reine IPv4-Domänen synthetisiert und an die Abonnenten gesendet werden.

NAT64 im großen Maßstab hat zwei Hauptkomponenten: NAT64-Präfix und NAT IPv4-Pool. DNS64 hat eine Hauptkomponente, DNS64-Präfix, die denselben Wert wie das NAT64-Präfix hat.

Nach Erhalt einer AAAA-Anforderung von einem Nur-IPv6-Abonnenten für einen Domänennamen, der auf einem Nur-IPv4-Webserver im Internet gehostet wird, synthetisiert die Citrix ADC DNS64-Funktionalität einen AAAA-Eintrag für den Domänennamen und sendet ihn an den Abonnenten. Der AAAA-Eintrag wird synthetisiert, indem das DNS64-Präfix (das auf das NAT64-Präfix gesetzt ist) und die tatsächliche IPv4-Adresse des Domänennamens verkettet wird.

Der Abonnent verfügt nun über eine IPv6-Zieladresse, die dem gewünschten Domänennamen entspricht. Der Abonnent sendet die Anfrage an die synthetisierte IPv6-Adresse. Nach Erhalt der IPv6-Anforderung übersetzt die große Citrix ADC NAT64-Funktionalität das IPv6-Anforderungspaket in ein IPv4-Anforderungspaket. NAT64 im großen Maßstab setzt die Zieladresse der IPv4-Anforderung auf die IPv4-Adresse, die aus der Zieladresse der IPv6-Anforderung extrahiert wird, indem das NAT64-Präfix von der IPv6-Adresse entfernt wird. Der Zielport wird von der IPv6-Anforderung beibehalten. Large Scale NAT64 setzt auch die Quell-IP-Adresse:Quellport des IPv4-Pakets auf die NAT-IP-Adresse:NAT-Port, der aus dem konfigurierten NAT-Pool ausgewählt wurde.

Die Appliance verwaltet eine Aufzeichnung aller aktiven Sitzungen, die die große NAT64-Funktionalität verwenden. Diese Sitzungen werden als große NAT64-Sitzungen bezeichnet. Die Appliance verwaltet auch die Zuordnungen zwischen Teilnehmer-IPv6-Adresse und -Port sowie NAT-IPv4-Adresse und -Port für jede große NAT64-Sitzung. Diese Mappings werden als große NAT64-Mappings bezeichnet. Von großen NAT64-Sitzungseinträgen und großen NAT64-Zuordnungseinträgen erkennt die Citrix ADC Appliance ein Antwortpaket (aus dem Internet empfangen) als zu einer bestimmten NAT64-Sitzung gehört.

Wenn die Appliance ein IPv4-Antwortpaket empfängt, das zu einer bestimmten NAT64-Sitzung gehört, verwendet sie die in der NAT64-Sitzung gespeicherten Informationen, um das IPv4-Paket in ein IPv6-Paket zu übersetzen, und sendet dann das IPv6-Antwortpaket an den Abonnenten.

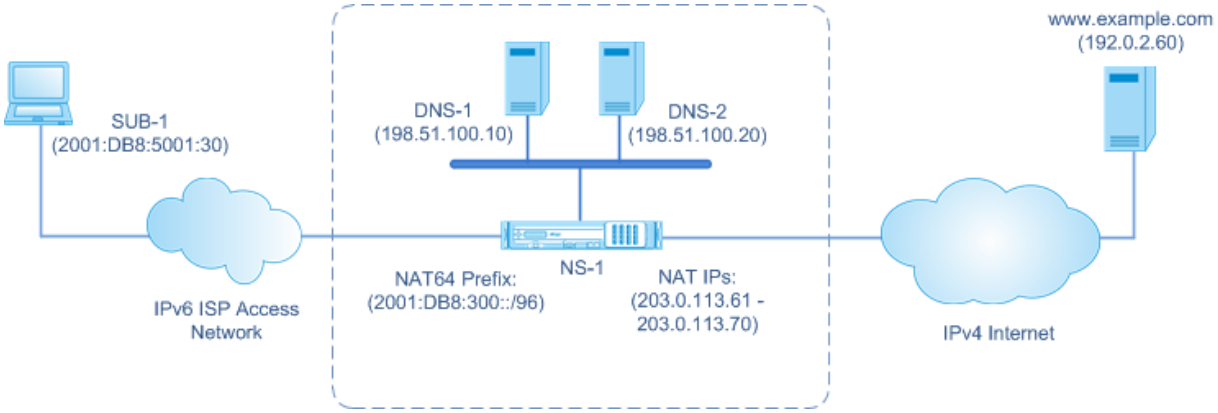
Beispiel: Verkehrsfluss der NAT64- und DNS64-Bereitstellung

Betrachten Sie ein Beispiel für eine umfangreiche NAT64- und DNS64-Bereitstellung, bestehend aus Citrix ADC Appliance NS-1 und zwei lokalen DNS-Servern, DNS-1 und DNS-2, im Kernnetzwerk eines ISP und IPv6-Abonnenten SUB-1. SUB-1 ist über das IPv6-Zugangsnetzwerk des ISP mit NS-1 verbunden. NS-1 umfasst umfangreiche NAT64- und DNS64-Konfigurationen für die Kommunikation zwischen IPv6-Teilnehmern SUB-1 und IPv4-Hosts (intern und extern).

Große NAT64-Konfiguration umfasst ein NAT64-Präfix (2001:DB 8:300: :/96) und NAT IPv4-Pool für die Übersetzung von IPv6-Anforderungen in IPv4-Anforderungen und IPv4-Antworten auf IPv6-Antworten.

Die DNS64-Konfiguration umfasst einen virtuellen DNS-Lastausgleichsserver LBVS-DNS64-1 (2001:DB 8:9999: :99) und ein DNS64-Präfix (2001:DB 8:300: :/96). LBVS-DNS64-1 stellt lokalen DNS-Server DNS-1 und DNS-2 für die Abonnenten des ISP dar. Das DNS64-Präfix, das den gleichen Wert wie das NAT64-Präfix hat, wird für die Synthese von DNS-AAAA-Einträgen aus DNS-A-Einträgen verwendet, die von

DNS-Servern DNS-1 und DNS-2 empfangen werden. NS-1 antwortet mit einem synthetisierten AAAA-Eintrag an SUB-1 für eine DNS-Anforderung zum Auflösen eines IPv4-Hosts.



DNS64-Datenverkehr

Der Datenverkehr fließt zwischen dem IPv6-Abonnenten SUB-1 und der Site`www.example.com`, die sich auf einem nur IPv4-Webserver im Internet befindet, wie folgt:

1. IPv6-Abonnent SUB-1 sendet eine DNS-AAAA-Anforderung für`www.example.com` an den angegebenen DNS-Server (2001:DB 8:9999: :99).
2. DNS-Lastenausgleichsserver LBVS-DNS64-1 (2001:DB 8:9999: :99) auf der Citrix ADC Appliance NS1 empfängt die AAAA-Anforderung. Der Lastausgleichsalgorithmus von LBVS-DNS64-1 wählt DNS-Server DNS-1 aus und leitet die AAAA-Anforderung an ihn weiter.
3. DNS-1 gibt einen leeren Datensatz oder eine Fehlermeldung zurück, da kein AAAA-Eintrag verfügbar ist`www.example.com`.
4. Da die DNS64-Option auf LBVS-DNS64-1 aktiviert ist und die AAAA-Anforderung von CL1 der in DNS64-Policy-1 angegebenen Bedingung entspricht, sendet NS1 eine DNS-A-Anforderung für die IPv4-Adresse von an DNS-1`www.example.com`.
5. DNS-1 reagiert mit dem A-Rekord von 192.0.2.60 für`www.example.com`.
6. DNS64-Modul auf NS1 synthetisiert einen AAAA-Datensatz für,`www.example.com` indem das DNS64-Präfix (2001:DB 8:300: :/96), das mit LBVS-DNS64-1 verknüpft ist, und die IPv4-Adresse (192.0.2.60) für`www.example.com` = 2001:DB 8:300: :192.0.2.60
7. NS1 sendet den synthetisierten AAAA-Datensatz an den IPv6-Client CL1. NS1 speichert auch den A-Datensatz in seinen Speicher. NS1 verwendet den zwischengespeicherten A-Datensatz, um AAAA-Datensätze für nachfolgende AAAA-Anforderungen zu synthetisieren.

NAT64-Datenverkehr

1. IPv6-Abonnent SUB-1 sendet eine Anfrage an 2001:DB 8:5001:30`www.example.com`. Das IPv6-Paket hat:

- Quell-IP-Adresse = 2001:DB 8:5001:30
- Quellport = 2552
- Ziel-IP-Adresse = 2001:DB 8:300::192.0.2.60
- Zielport = 80

2. IPv6-Abonnent SUB-1 sendet eine Anfrage an 2001:DB 8:5001:30www.example.com. Das IPv6-Paket hat:

   - Quell-IP-Adresse = 2001:DB 8:5001:30
   - Quellport = 2552
   - Ziel-IP-Adresse = 2001:DB 8:300::192.0.2.60
   - Zielport = 80

3. Wenn NS-1 das IPv6-Paket empfängt, erstellt das große NAT64-Modul ein übersetztes IPv4-Anforderungspaket mit:

   - Quell-IP-Adresse = Eine der IPv4-Adressen, die im konfigurierten NAT-Pool verfügbar sind (203.0.113.61)
   - Quellport = Einer der Ports, die mit der zugewiesenen NAT IPv4-Adresse verfügbar sind (3002)
   - Ziel-IP-Adresse = IPv4-Adresse, die aus der Zieladresse der IPv6-Anforderung extrahiert wurde, indem das NAT64-Präfix (2001:DB 8:300: :/96) aus der IPv6-Adresse (192.0.2.60) entfernt wurde.
   - Zielport = Zielport der IPv6-Anforderung (80)

4. Das große NAT64-Modul erstellt auch Zuordnungs- und Sitzungseinträge für diesen großen NAT64-Fluss. Die Sitzungs- und Zuordnungseinträge enthalten die folgenden Informationen:

   - Quell-IP-Adresse des IPv6-Pakets = 2001:DB 8:5001:30
   - Quellport des IPv6-Pakets = 2552
   - NAT IP-Adresse = 203.0.113.61
   - NAT-Anschluss = 3002
   - NS-1 sendet das resultierende IPv4-Paket an sein Ziel im Internet.

5. Nach Erhalt des Anforderungspaketswww.example.com verarbeitet der Server für das Paket und sendet ein Antwortpaket an NS-1. Das IPv4-Antwortpaket hat:

   - Quell-IP-Adresse = 192.0.2.60
   - Quellport = 80
   - Ziel-IP-Adresse = 203.0.113.61
   - Zielport = 3002

6. Nach Erhalt des IPv4-Antwortpakets untersucht NS-1 die großen NAT64-Zuordnungs- und Sitzungseinträge und stellt fest, dass das IPv4-Antwortpaket zu einer großen NAT64-Sitzung gehört. Das große NAT64-Modul erstellt ein übersetztes IPv6-Antwortpaket:

- Quell-IP-Adresse = 2001:DB 8:300: :192.0.2.60
- Quellport = 80
- Ziel-IP-Adresse = 2001:DB 8:5001:30
- Zielport = 2552

7. NS-1 sendet die übersetzte IPv6-Antwort an den Client SUB-1.

Große NAT64-Funktionen, die auf Citrix ADC Appliances unterstützt werden

Der große NAT64 auf einer Citrix ADC Appliance unterstützt den standardmäßigen LSN-Funktionsumfang. Weitere Informationen zu diesen LSN-Funktionen finden Sie unter LSN Architecture.

Im Folgenden finden Sie einige der großen NAT64-Funktionen, die von Citrix ADC Appliances unterstützt werden:

- ALGs. Unterstützung von Application Layer Gateway (ALG) für SIP-, RTSP-, FTP-, ICMP- und TFTP-Protokolle.
- Deterministisch/Fixed NAT. Unterstützung für die Vorzuweisung von Port-Blöcken an Abonnenten, um die Protokollierung zu minimieren.
- Zuordnung. Unterstützung von Endpoint-Independent Mapping (EIM), Address-dependent Mapping (ADM) und Address-Port Dependent Mapping (APDM).
- Filterung. Unterstützung von Endpoint-Independent Filtern (EIF), Address-Dependent Filtern (ADF) und Address-Port-Dependent Filtern (APDF).
- Quoten. Konfigurierbare Beschränkungen für die Anzahl der Ports, Sitzungen pro Teilnehmer und Sitzungen pro LSN-Gruppe.
- Statische Zuordnung. Unterstützung für die manuelle Definition eines großen NAT64-Mappings.
- Hairpin Flow Unterstützung für die Kommunikation zwischen Teilnehmern oder internen Hosts unter Verwendung von NAT-IP-Adressen.
- 464XLAT-Verbindungen. Unterstützung für die Kommunikation zwischen nur IPv4-Anwendungen auf IPv6-Teilnehmerhosts und IPv4-Hosts im Internet über IPv6-Netzwerk.
- Variable Länge NAT64 und DNS64 Präfixe. Die Citrix ADC Appliance unterstützt die Definition von NAT64- und DNS64-Präfixen mit Längen 32, 40, 48, 56, 64 und 96.
- Mehrere NAT64- und DNS64-Präfix. Die Citrix ADC Appliance unterstützt mehrere NAT64- und DNS64-Präfixe.
- LSN-Clients. Unterstützung für die Angabe oder Identifizierung von Abonnenten für große NAT64 mithilfe von IPv6-Präfixen und erweiterten ACL6-Regeln.
- Protokollierung Unterstützung für die Protokollierung von NAT64-Sitzungen für die Strafverfolgung. Darüber hinaus werden die folgenden für die Protokollierung unterstützt.
  - **Zuverlässige SYSLOG**. Unterstützung für das Senden von SYSLOG-Nachrichten über TCP an externe Protokollserver für einen zuverlässigeren Transportmechanismus.
  - **Lastenausgleich von Protokollservern**. Unterstützung für den Lastenausgleich externer Protokollserver zur Verhinderung der Speicherung redundanter Protokollmeldungen.

- **Minimale Protokollierung**. Deterministische LSN-Konfigurationen oder dynamische LSN-Konfigurationen mit Portblock reduzieren das große NAT64-Protokollvolumen erheblich.
- **Protokollieren von MSISDN-Informationen**. Unterstützung für die Einbeziehung der MSISDN-Informationen von Abonnenten in große NAT64-Protokolle, um Abonnentenaktivitäten über das Internet zu identifizieren und zu verfolgen.

Zu berücksichtigende Punkte für die Konfiguration von NAT64 Large Scale

October 5, 2021

Bevor Sie mit der Konfiguration von NAT64 und DNS64 beginnen, sollten Sie folgende Punkte beachten:

1. Vergewissern Sie sich, dass Sie die verschiedenen Komponenten von großen NAT64 verstehen, die in RFCs beschrieben werden.
2. Die Citrix ADC Appliance unterstützt nur die folgenden ALGs für große NAT64:
   - FTP
   - TFTP
   - ICMP
   - SIP
   - RTSP
3. Bei einem Hochverfügbarkeitssetup von zwei Citrix ADC Appliances wird die große NAT64-Sitzungssynchronisierung (Verbindungsspiegelung) nicht unterstützt.

Konfigurieren von DNS64

October 5, 2021

Das Erstellen der erforderlichen Entitäten für die statusbehaftete NAT64-Konfiguration auf der Citrix ADC Appliance umfasst die folgenden Verfahren:

- Fügen Sie DNS-Dienste hinzu. DNS-Dienste sind logische Darstellungen von DNS-Servern, für die die Citrix ADC Appliance als DNS-Proxyserver fungiert. Weitere Informationen zum Festlegen optionaler Parameter eines Dienstes finden Sie unter Load Balancing.
- Fügen Sie DNS64-Aktion und DNS64-Richtlinie hinzu, und binden Sie dann die DNS64-Aktion an die DNS64-Richtlinie. Eine DNS64-Richtlinie legt Bedingungen fest, die mit dem Datenverkehr für die DNS64-Verarbeitung gemäß den Einstellungen in der zugeordneten DNS64-Aktion

abgeglichen werden sollen. Die DNS64-Aktion gibt das obligatorische DNS64-Präfix sowie die optionalen Einstellungen für die Regel und die zugeschalteten Regeln an.

- Erstellen Sie einen virtuellen DNS-Lastausgleichsserver und binden Sie die DNS-Dienste und die DNS64-Richtlinie daran. Der virtuelle DNS-Lastenausgleichsserver fungiert als DNS-Proxyserver für DNS-Server, die durch die gebundenen DNS-Dienste dargestellt werden. Datenverkehr, der auf dem virtuellen Server eintrifft, wird mit der gebundenen DNS64-Richtlinie für die DNS64-Verarbeitung abgeglichen. Weitere Informationen zum Festlegen optionaler Parameter eines virtuellen Lastausgleichsservers finden Sie unter Load Balancing.

> **Hinweis:**
>
> Die Befehlszeilenschnittstelle verfügt über separate Befehle für diese beiden Aufgaben, aber die GUI kombiniert sie in einem einzigen Dialogfeld.

- Aktivieren Sie das Zwischenspeichern von DNS-Datensätzen. Aktivieren Sie den globalen Parameter für die Citrix ADC Appliance, um DNS-Einträge zwischenzuspeichern, die über DNS-Proxyvorgänge abgerufen werden. Weitere Informationen zum Aktivieren des Zwischenspeichers von DNS-Datensätzen finden Sie unter Aktivieren des Zwischenspeichers von DNS-Datensätzen.

So erstellen Sie einen Dienst vom Typ DNS mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add service <name> <IP> <serviceType> <port> …
2 <!--NeedCopy-->
```

So erstellen Sie eine DNS64-Aktion mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add dns action64 <actionName> -Prefix <ipv6_addr|*> [-mappedRule <
     expression>] [-excludeRule <expression>]
2 <!--NeedCopy-->
```

So erstellen Sie eine DNS64-Richtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add dns policy64 <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

So erstellen Sie einen virtuellen DNS-Load Balancing Server mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> DNS <IPAddress> <port> -dns64 (ENABLED | DISABLED
    ) [-bypassAAAA ( YES | NO)] ...
<!--NeedCopy-->
```

So binden Sie die DNS-Dienste und die DNS64-Richtlinie mit der Befehlszeilenschnittstelle an den virtuellen DNS-Lastausgleichsserver

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name> <serviceName> ...

bind lb vserver <name> -policyName <string> -priority <positive_integer
    > ...
<!--NeedCopy-->
```

Beispielkonfiguration:

```
add service SVC-DNS-1 203.0.113.50 DNS 53
Done
add service SVC-DNS-2 203.0.113.60 DNS 53
Done
add dns Action64 DNS64-Action-1 -Prefix 2001:DB8:300::/96
Done
add dns Policy64 DNS64-Policy-1 -rule "CLIENT.IPv6.SRC.IN_SUBNET(2001:
    DB8:5001::/64)" -action DNS64-Action-1
Done
add lb vserver LBVS-DNS64-1 DNS 2001:DB8:9999::99 53 -dns64 ENABLED
Done
bind lb vserver LBVS-DNS64-1 SVC-DNS-1
Done
```



```
13 bind lb vserver LBVS-DNS64-1 SVC-DNS-2
14 Done
15 bind lb vserver LBVS-DNS64-1 -policyname DNS64-Policy-1 -priority 2
16 Done
17 <!--NeedCopy-->
```

Konfigurieren von Large Scaler NAT64

October 5, 2021

Eine umfangreiche NAT64-Konfiguration auf einer Citrix ADC Appliance verwendet die LSN-Befehlssätze. In einer großen NAT64-Konfiguration gibt die LSN-Client-Entität die IPv6-Adresse oder IPv6-Netzwerkadresse oder ACL6-Regeln für die Identifizierung von IPv6-Abonnenten an. Eine NAT64-Konfiguration enthält auch ein IPv6-Profil, das ein NAT64-Präfix angibt.

Die Konfiguration von NAT64 auf einer Citrix ADC Appliance umfasst die folgenden Aufgaben:

- Legen Sie die globalen LSN-Parameter fest. Globale Parameter umfassen die Menge an Citrix ADC-Arbeitsspeicher, der für die LSN-Funktion reserviert ist, und die Synchronisierung von LSN-Sitzungen in einem Hochverfügbarkeitssetup.
- Erstellen Sie eine LSN-Client-Entität zum Identifizieren des Datenverkehrs von IPv6-Abonnenten. Die LSN-Client-Entität bezieht sich auf eine Gruppe von IPv6-Abonnenten. Die Client-Entität enthält IPv6-Adressen oder IPv6-Netzwerkpräfixe oder ACL6-Regeln, um den Datenverkehr von diesen Abonnenten zu identifizieren. Ein LSN-Client kann nur an eine LSN-Gruppe gebunden werden. Die Befehlszeilenschnittstelle verfügt über zwei Befehle zum Erstellen einer LSN-Client-Entität und zum Binden eines Abonnenten an die LSN-Client-Entität. Die GUI kombiniert diese beiden Operationen auf einem einzigen Bildschirm.
- Erstellen Sie einen LSN-Pool und binden Sie NAT-IP-Adressen an ihn. Ein LSN-Pool definiert einen Pool von NAT-IP-Adressen, der von der Citrix ADC Appliance zum Ausführen von NAT64-großformatigen NAT64 verwendet wird. Die Befehlszeilenschnittstelle verfügt über zwei Befehle zum Erstellen eines LSN-Pools und zum Binden von NAT-IP-Adressen an den LSN-Pool. Die GUI kombiniert diese beiden Operationen auf einem einzigen Bildschirm.
- Erstellen Sie ein LSN IP6-Profil. Ein LSN IP6-Profil definiert das NAT64-Präfix für eine große NAT64-Konfiguration.
- (Optional) Erstellen Sie ein LSN-Transportprofil für ein bestimmtes Protokoll. Ein LSN-Transportprofil definiert verschiedene Timeouts und Limits, z. B. maximale große NAT64-Sitzungen und maximale Port-Auslastung, die ein Teilnehmer für ein bestimmtes Protokoll haben kann. Sie binden ein LSN-Transportprofil für jedes Protokoll (TCP, UDP und ICMP) an eine LSN-Gruppe. Ein Profil kann an mehrere LSN-Gruppen gebunden werden. Ein an eine LSN-Gruppe gebundenes Profil gilt für alle Abonnenten eines LSN-Clients, der an dieselbe

Gruppe gebunden ist. Standardmäßig ist ein LSN-Transportprofil mit Standardeinstellungen für TCP-, UDP- und ICMP-Protokolle während der Erstellung an eine LSN-Gruppe gebunden. Dieses Profil wird als Standardtransportprofil bezeichnet. Ein LSN-Transportprofil, das Sie an eine LSN-Gruppe binden, überschreibt das standardmäßige LSN-Transportprofil für dieses Protokoll.

- (Optional) Erstellen Sie ein LSN-Anwendungsprofil für ein bestimmtes Protokoll und binden Sie eine Reihe von Zielports daran. Ein LSN-Anwendungsprofil definiert die LSN-Zuordnungs- und LSN-Filtersteuerelemente einer Gruppe für ein bestimmtes Protokoll und für eine Gruppe von Zielports. Für eine Gruppe von Zielports binden Sie ein LSN-Profil für jedes Protokoll (TCP, UDP und ICMP) an eine LSN-Gruppe. Ein Profil kann an mehrere LSN-Gruppen gebunden werden. Ein LSN-Anwendungsprofil, das an eine LSN-Gruppe gebunden ist, gilt für alle Abonnenten eines LSN-Clients, der an dieselbe Gruppe gebunden ist. Standardmäßig ist ein LSN-Anwendungsprofil mit Standardeinstellungen für TCP-, UDP- und ICMP-Protokolle für alle Zielports während der Erstellung an eine LSN-Gruppe gebunden. Dieses Profil wird als Standardanwendungsprofil bezeichnet. Wenn Sie ein LSN-Anwendungsprofil mit einem bestimmten Satz von Zielports an eine LSN-Gruppe binden, überschreibt das gebundene Profil das standardmäßige LSN-Anwendungsprofil für dieses Protokoll an dieser Gruppe von Zielports. Die Befehlszeilenschnittstelle verfügt über zwei Befehle zum Erstellen eines LSN-Anwendungsprofils und zum Binden eines Satzes von Zielports an das LSN-Anwendungsprofil. Die GUI kombiniert diese beiden Operationen auf einem einzigen Bildschirm.
- Erstellen Sie eine LSN-Gruppe und binden Sie LSN-Pools, LSN-IPv6-Profil, (optional) LSN-Transportprofile und (optional) LSN-Anwendungsprofile an die LSN-Gruppe. Eine LSN-Gruppe ist eine Entität, die aus einem LSN-Client, einem LSN-IPv6-Profil, LSN-Pool, LSN-Transportprofilen und LSN-Anwendungsprofilen besteht. B. Port-Blockgröße und Protokollierung von LSN-Sitzungen. Die Parametereinstellungen gelten für alle Abonnenten eines LSN-Clients, der an die LSN-Gruppe gebunden ist. Nur ein LSN-IPv6-Profil kann an eine LSN-Gruppe gebunden werden, und ein LSN-IPv6-Profil, das an eine LSN-Gruppe gebunden ist, kann nicht an andere LSN-Gruppen gebunden werden. Nur LSN-Pools und LSN-Gruppen mit denselben NAT-Typeinstellungen können miteinander verbunden werden. Mehrere LSN-Pools können an eine LSN-Gruppe gebunden werden. Nur eine LSN-Client-Entität kann an eine LSN-Gruppe gebunden werden, und eine LSN-Client-Entität, die an eine LSN-Gruppe gebunden ist, kann nicht an andere LSN-Gruppen gebunden werden. Die Befehlszeilenschnittstelle verfügt über zwei Befehle zum Erstellen einer LSN-Gruppe und zum Binden von LSN-Pools, LSN-Transportprofilen und LSN-Anwendungsprofilen an die LSN-Gruppe. Die GUI kombiniert diese beiden Operationen in einem einzigen Bildschirm.

Konfiguration über die Befehlszeile

Sie können verschiedene Konfigurationen über die Befehlszeilenschnittstelle erstellen. Befolgen Sie die unten angegebenen Schritte.

So erstellen Sie einen LSN-Client mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn client <clientname

show lsn client
<!--NeedCopy-->
```

So binden Sie ein IPv6-Netzwerk oder eine ACL6-Regel über die Befehlszeilenschnittstelle an einen LSN-Client

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn client <clientname> (-network6 <ipv6_addr|*>| -acl6name <
   string>)

show lsn client
<!--NeedCopy-->
```

So erstellen Sie einen LAN-Pool mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn pool <poolname>

show lsn pool <poolname>
<!--NeedCopy-->
```

So binden Sie NAT-IP-Adressen mit der Befehlszeilenschnittstelle an einen LSN-Pool

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn pool <poolname> <lsnip>

show lsn pool
<!--NeedCopy-->
```


> **Hinweis:**
>
> Verwenden Sie zum Entfernen von NAT-IP-Adressen (LSN-IP-Adressen) aus einem LSN-Pool den Befehl unbind lsn pool.

So konfigurieren Sie ein LSN-IPv6-Profil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn ip6profile <name>  - type NAT64 -natprefix <ipv6_addr|*>

show lsn ip6profile
<!--NeedCopy-->
```

So erstellen Sie ein LSN-Transportprofil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn transportprofile <transportprofilename> <transportprotocol> [-
    sessiontimeout <secs>] [-finrsttimeout <secs>] [-portquota <
    positive_integer>] [-sessionquota <positive_integer>] [-
    portpreserveparity ( ENABLED | DISABLED )] [-portpreserverange (
    ENABLED | DISABLED )] [-syncheck ( ENABLED | DISABLED )]

show lsn transportprofile
<!--NeedCopy-->
```

So erstellen Sie ein LSN-Anwendungsprofil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn appsprofile <appsprofilename> <transportprotocol> [-ippooling (
    PAIRED | RANDOM )] [-mapping <mapping>] [-filtering <filtering>][-
    tcpproxy ( ENABLED | DISABLED )]

show lsn appsprofile
<!--NeedCopy-->
```


So binden Sie einen Anwendungsprotokollportbereich mit der Befehlszeilenschnittstelle an ein LSN-Anwendungsprofil

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn appsprofile <appsprofilename> <lsnport>

show lsn appsprofile
<!--NeedCopy-->
```

So erstellen Sie eine LSN-Gruppe mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn group <groupname> -clientname <string> [-nattype ( DYNAMIC |
    DETERMINISTIC )] [-portblocksize <positive_integer>] [-logging(
    ENABLED | DISABLED )] [-sessionLogging ( ENABLED | DISABLED )][-
    sessionSync ( ENABLED | DISABLED )] [-snmptraplimit<positive_integer
    >] [-ftp ( ENABLED | DISABLED )] [-sipalg ( ENABLED | DISABLED )] [-
    rtspalg ( ENABLED |DISABLED )] [-ip6profile <string>]

show lsn group
<!--NeedCopy-->
```

So binden Sie LSN-Protokollprofile und LSN-Pools mit der Befehlszeilenschnittstelle an eine LSN-Gruppe

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn group <groupname> (-poolname <string> | -transportprofilename
    <string> | -httphdrlogprofilename <string> | -appsprofilename <
    string> | -sipalgprofilename <string> | rtspalgprofilename <string>)

show lsn group
<!--NeedCopy-->
```

Beispiel für große NAT64-Konfigurationen

Hier sind einige Beispielkonfigurationen von großformatigen NAT64:

Einfache großformatige NAT64-Konfiguration mit Standardeinstellungen:

```
add lsn client LSN-NAT64-CLIENT-1

bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96

add lsn pool LSN-NAT64-POOL-1

bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70

add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
    :300::/96

add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
    ip6profile LSN-NAT64-PROFILE-1

bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1

<!--NeedCopy-->
```

Einfache großformatige NAT64-Konfiguration mit einer erweiterten ACL6-Regel zur Identifizierung von Abonnenten:

```
add ns acl6 LSN-NAT64-ACL-2 ALLOW  - srcIPv6 = 2001:DB8:5002::20 - 2001:
    DB8:5002::200

apply acl6s

add lsn client LSN-NAT64-CLIENT-2

bind lsn client LSN-NAT64-CLIENT-2  - acl6name LSN-NAT64-ACL-2

add lsn pool LSN-NAT64-POOL-2

bind lsn pool LSN-NAT64-POOL-2 203.0.113.5-203.0.113.10

add lsn ip6profile LSN-NAT64-PROFILE-2 -type NAT64 -natprefix 2001:DB8
    :302::/96

add lsn group LSN-NAT64-GROUP-2 -clientname LSN-NAT64-CLIENT-2 -
    ip6profile LSN-NAT64-PROFILE-2

```



```
17 bind lsn group LSN-NAT64-GROUP-2 -poolname LSN-NAT64-POOL-2
18
19 <!--NeedCopy-->
```

Große NAT64-Konfiguration mit deterministischer NAT-Ressourcenzuweisung:

```
1  add lsn client LSN-NAT64-CLIENT-7
2
3  bind lsn client LSN-NAT64-CLIENT-7 -network6 2001:DB8:1002::7/128
4
5  add lsn pool LSN-NAT64-POOL-7 -nattype DETERMINISTIC
6
7  bind lsn pool LSN-NAT64-POOL-7 203.0.113.24-203.0.113.27
8
9  add lsn ip6profile LSN-NAT64-PROFILE-7 -type NAT64 -natprefix 2001:DB8
       :307::/96
10
11 add lsn group LSN-NAT64-GROUP-7 -clientname LSN-NAT64-CLIENT-7 -
       ip6profile LSN-NAT64-PROFILE-7 -nattype DETERMINISTIC -portblocksize
        256
12
13 bind lsn group LSN-NAT64-GROUP-7 -poolname LSN-POOL-7
14
15 <!--NeedCopy-->
```

Konfigurieren von Application Layer Gateways für Large Scale NAT64

October 5, 2021

Bei einigen Protokollen der Anwendungsschicht werden auch die IP-Adressen und Protokollportnummern in der Paketnutzlast kommuniziert. Application Layer Gateway für ein Protokoll analysiert die Nutzlast des Pakets und führt notwendige Änderungen durch, um sicherzustellen, dass das Protokoll weiterhin über große NAT64 funktioniert.

Die Citrix ADC Appliance unterstützt ALG für die folgenden Protokolle für große NAT64:

- FTP
- ICMP
- TFTP
- SIP
- RTSP

Application Layer Gateway für FTP-, ICMP- und TFTP-Protokolle

October 5, 2021

Sie können ALG für das FTP-Protokoll für eine große NAT64-Konfiguration aktivieren oder deaktivieren, indem Sie die Option FTP ALG der LSN-Gruppe der Konfiguration aktivieren oder deaktivieren.

ALG für das ICMP-Protokoll ist standardmäßig aktiviert, und es gibt keine Möglichkeit, es zu deaktivieren.

ALG für das TFTP-Protokoll ist standardmäßig deaktiviert. TFTP ALG wird automatisch für eine groß angelegte NAT64-Konfiguration aktiviert, wenn Sie ein UDP LSN-Anwendungsprofil mit endpunktunabhängiger Zuordnung, endpunktunabhängiger Filterung und Zielport als 69 (bekannter Port für TFTP) an die LSN-Gruppe binden.

Application Layer Gateway für SIP-Protokoll

October 5, 2021

Die Verwendung von Large Scale NAT64 mit Session Initiation Protocol (SIP) ist kompliziert, da SIP-Nachrichten IP-Adressen in den SIP-Headern sowie im SIP-Body enthalten. Wenn LSN mit SIP verwendet wird, enthalten die SIP-Header Informationen über den Anrufer und den Empfänger, und das Gerät übersetzt diese Informationen, um sie vor dem externen Netzwerk zu verstecken. Der SIP-Body enthält die SDP-Informationen (Session Description Protocol), die IP-Adressen und Portnummern für die Übertragung der Medien enthalten. SIP ALG für große NAT64 ist kompatibel mit RFC 3261, RFC 3581, RFC 4566 und RFC 4475.

> **Hinweis:**
>
> SIP ALG wird in einer eigenständigen Citrix ADC Appliance, in einem Citrix ADC-Hochverfügbarkeitssetup sowie in einem Citrix ADC-Cluster-Setup unterstützt.

Einschränkungen der SIP ALG

SIP ALG für große NAT64 hat folgende Einschränkungen:

- Es wird nur SDP-Nutzlast unterstützt.
- Folgende Komponenten werden nicht unterstützt:
  - Multicast-IP-Adressen
  - Verschlüsseltes SDP
  - SIP TLS

- FQDN-Übersetzung
- SIP-Layer-Authentifizierung
- Traffic-Domänen
- Admin-Partitionen
- Mehrteiliger Körper
- Linie faltbar

Konfigurieren von SIP ALG

Sie müssen die SIP ALG als Teil der LSN-Konfiguration konfigurieren. Anweisungen zur Konfiguration von LSN finden Sie unter Konfiguration Large Scale NAT64. Stellen Sie beim Konfigurieren von LSN sicher, dass Sie:

- Legen Sie beim Hinzufügen eines LSN-Anwendungsprofils die folgenden Parameter fest:
  - IP-Pooling = PAIRED
  - Adress- und Portzuordnung = ENDPOINT-INDEPENDENT
  - Filterung = ENDPOINT-INDEPENDENT
- Erstellen Sie ein SIP-ALG-Profil und stellen Sie sicher, dass Sie entweder den Quellportbereich oder den Zielportbereich definieren. Binden Sie das SIP-ALG-Profil an die LSN-Gruppe.
- Aktivieren Sie SIP ALG in der LSN-Gruppe.

So aktivieren Sie SIP ALG für eine LSN-Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lsn group <groupname> -clientname <string> [-sipalg ( ENABLED |
     DISABLED )]
2
3 show lsn group <groupname>
4 <!--NeedCopy-->
```

So aktivieren Sie SIP ALG für eine LSN-Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lsn sipalgprofile <sipalgprofilename>[-dataSessionIdleTimeout <
     positive_integer>][-sipSessionTimeout <positive_integer>] [-
     registrationTimeout <positive_integer>] [-sipsrcportrange <port[-
     port]>] [-sipdstportrange <port[-port]>] [-openRegisterPinhole (
```



```
    ENABLED | DISABLED )] [-openContactPinhole ( ENABLED | DISABLED )]
    [-openViaPinhole ( ENABLED | DISABLED )] [-openRecordRoutePinhole (
    ENABLED | DISABLED )]-sipTransportProtocol ( TCP | UDP ) [-
    openRoutePinhole ( ENABLED | DISABLED )] [-rport ( ENABLED |
    DISABLED )]

show lsn sipalgprofile <sipalgprofilename
<!--NeedCopy-->
```

Beispielkonfiguration

Die folgende große NAT64-Beispielkonfiguration, SIP ALG, ist für TCP-Datenverkehr von Teilnehmergeräten im Netzwerk 2001 aktiviert: DB 8:1003: :/96.

```
add lsn client LSN-NAT64-CLIENT-9

Done
bind lsn client LSN-NAT64-CLIENT-9 -network6 2001:DB8:1002::/96

Done
add lsn pool LSN-NAT64-POOL-9

Done
bind lsn pool LSN-NAT64-POOL-9 203.0.113.90

Done
add lsn ip6profile LSN-NAT64-PROFILE-9 -type NAT64 -natprefix 2001:DB8
    :309::/96

Done
add lsn appsprofile LSN-NAT64-APPS-PROFILE-9 TCP -ippooling PAIRED -
    mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT

Done
add lsn sipalgprofile SIPALGPROFILE-9  -sipdstportrange 5060  -
    sipTransportProtocol TCP

Done
add lsn group LSN-NAT64-GROUP-9 -clientnameLSN-NAT64-CLIENT-9 -
    ip6profile LSN-NAT64-PROFILE-7 -sipalg ENABLED

Done
```



```
25 bind lsn group LSN-NAT64-GROUP-9 -poolnameLSN-NAT64-POOL-9
26 Done
27 bind lsn group LSN-NAT64-GROUP-9 -appsprofilename LSN-NAT64-APPS-
      PROFILE-9
28 Done
29 bind lsn group LSN-NAT64-GROUP-9 -sipalgprofilename SIPALGPROFILE-9
30 Done
31 <!--NeedCopy-->
```

Application Layer Gateway für RTSP-Protokoll

October 5, 2021

Real Time Streaming Protocol (RTSP) ist ein Protokoll auf Anwendungsebene für die Übertragung von Echtzeit-Mediendaten. RTSP wird zum Einrichten und Steuern von Mediensitzungen zwischen Endpunkten verwendet und ist ein Kontrollkanalprotokoll zwischen dem Media-Client und dem Medienserver. Die typische Kommunikation ist zwischen einem Client und einem Streaming-Medienserver.

Das Streamen von Medien aus einem privaten Netzwerk in ein öffentliches Netzwerk erfordert die Übersetzung von IP-Adressen und Portnummern über das Netzwerk. Die Citrix ADC Funktionalität umfasst ein Application Layer Gateway (ALG) für RTSP, das mit Large Scale NAT (LSN) verwendet werden kann, um den Medienstrom zu analysieren und alle erforderlichen Änderungen vorzunehmen, um sicherzustellen, dass das Protokoll weiterhin über das Netzwerk funktioniert.

Die IP-Adressenübersetzung hängt vom Typ und der Richtung der Nachricht sowie vom Typ der Medien ab, die von der Client-Server-Bereitstellung unterstützt werden. Nachrichten werden wie folgt übersetzt:

- Ausgehende Anforderung: Private IP-Adresse an die öffentliche IP-Adresse des Citrix ADC namens LSN-IP-Adresse.
- Eingehende Antwort: LSN-IP-Adresse an private IP-Adresse.
- Eingangsanforderung: Keine Übersetzung.
- Ausgehende Antwort: Private IP-Adresse an die IP-Adresse des LSN-Pools.

> **Hinweis:**
>
> RTSP ALG wird in einer eigenständigen Citrix ADC Appliance, in einem Citrix ADC-Hochverfügbarkeitssetup sowie in einem Citrix ADC-Cluster-Setup unterstützt.

Einschränkungen der RTSP ALG

Die RTSP ALG unterstützt nicht Folgendes:

- Multicast-RTSP-Sitzungen
- RTSP-Sitzung über UDP
- Admin-Partitionen
- RTSP-Authentifizierung
- HTTP-Tunneling

Konfigurieren von RTSP ALG

Konfigurieren Sie RTSP ALG als Teil der LSN-Konfiguration. Anweisungen zum Konfigurieren von LSN finden Sie unter Konfigurieren von Large Scale NAT64. Stellen Sie während der Konfiguration sicher, dass Sie:

- Legen Sie beim Hinzufügen eines LSN-Anwendungsprofils die folgenden Parameter fest:
  - IP-Pooling = PAIRED
  - Adress- und Portzuordnung = ENDPOINT-INDEPENDENT
  - Filterung = ENDPOINT-INDEPENDENT
- RTSP ALG in der LSN-Gruppe aktivieren
- Erstellen Sie ein RTSP-ALG-Profil und binden Sie das RTSP-ALG-Profil an die LSN-Gruppe

So aktivieren Sie RTSP ALG für eine LSN-Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn group <groupname> -clientname <string> [-rtspalg ( ENABLED |
    DISABLED )]

show lsn group <groupname>
<!--NeedCopy-->
```

So aktivieren Sie RTSP ALG für eine LSN-Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn rtspalgprofile <rtspalgprofilename> [-rtspIdleTimeout <
    positive_integer>] -rtspportrange <port[-port]> [-
    rtspTransportProtocol (TCP|UDP)]
```



```
2
3 show lsn rtspalgprofile <rtspalgprofilename>
4 <!--NeedCopy-->
```

Beispiel-RTSP-ALG-Konfiguration

Die folgende große NAT64-Beispielkonfiguration, RTSP ALG, ist für TCP-Datenverkehr von Teilnehmergeräten im Netzwerk 2001:DB 8:1002: :/96 aktiviert.

```
1 add lsn client LSN-NAT64-CLIENT-9
2 Done
3 bind lsn client LSN-NAT64-CLIENT-9 -network6 2001:DB8:1002::/96
4 Done
5 add lsn pool LSN-NAT64-POOL-9
6 Done
7 bind lsn pool LSN-NAT64-POOL-9 203.0.113.90
8 Done
9 add lsn ip6profile LSN-NAT64-PROFILE-9 -type NAT64 -natprefix 2001:DB8
    :309::/96
10 Done
11 add lsn appsprofile LSN-NAT64-APPS-PROFILE-9 TCP -ippooling PAIRED -
    mapping ENDPOINT-INDEPENDENT -filtering ENDPOINT-INDEPENDENT
12 Done
13 add lsn rtspalgprofile RTSPALGPROFILE-9 -rtspIdleTimeout 1000 -
    rtspportrange 554
14 Done
15 add lsn group LSN-NAT64-GROUP-9 -clientname LSN-NAT64-CLIENT-9 -
    ip6profile LSN-NAT64-PROFILE-7 -rtspalg ENABLED
16 Done
17 bind lsn group LSN-NAT64-GROUP-9 -poolname LSN-NAT64-POOL-9
18 Done
19 bind lsn group LSN-NAT64-GROUP-9 -appsprofilename LSN-NAT64-APPS-
    PROFILE-9
20 Done
21 bind lsn group LSN-NAT64-GROUP-9  -rtspalgprofilename RTSPALGPROFILE-9
22 Done
23 <!--NeedCopy-->
```


Konfigurieren statischer großformatige NAT64-Karten

October 5, 2021

Die Citrix ADC Appliance unterstützt die manuelle Erstellung von NAT64-Zuordnungen, die die Zuordnung zwischen den folgenden Informationen enthalten:

- IP-Adresse und Port des Teilnehmers
- NAT IP-Adresse und Port

Statische Large Scale NAT64-Zuordnungen sind nützlich, wenn Sie sicherstellen möchten, dass die IPv4-Verbindungen, die mit einer NAT-IP-Adresse initiiert wurden: Port sind IPv6-übersetzt und der IP-Adresse des Teilnehmers zugeordnet: Port (z. B. Webserver, die sich im internen Netzwerk befinden).

So erstellen Sie eine Large Scale NAT64-Zuordnung mit der Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn static <name> <transportprotocol> <subscrIP> <subscrPort>  [<
    natIP> [<natPort>]] [-destIP <ip_addr> [-dsttd <positive_integer>]]

show lsn static
<!--NeedCopy-->
```

Platzhalterport Statische NAT64-Karten im großen Maßstab

Ein statischer NAT64-Zuordnungseintrag im großen Maßstab ist normalerweise eine Eins-zu-Eins-Zuordnung zwischen einer Teilnehmer-IPv6-Adresse:Port und einer NAT-IPv4-Adresse:Port. Ein eins-zu-eins-statischer NAT64-Mapping-Eintrag stellt nur einen Port der Teilnehmer-IP-Adresse im Internet zur Verfügung.

Einige Situationen erfordern möglicherweise, dass alle Ports (64K - begrenzt auf die maximale Anzahl von Ports einer NAT IPv4-Adresse) einer Teilnehmer-IP-Adresse im Internet verfügbar gemacht werden (z. B. ein Server, der in einem internen Netzwerk gehostet wird und auf jedem Port einen anderen Dienst ausführt). Um diese internen Dienste über das Internet zugänglich zu machen, müssen Sie alle Ports des Servers im Internet verfügbar machen.

Eine Möglichkeit, diese Anforderung zu erfüllen, besteht darin, 64 Tausend Eins-zu-Eins-zu-Eins-Zuordnungseinträge für jeden Port hinzuzufügen. Das Erstellen dieser Einträge ist sehr umständlich und eine große Aufgabe. Außerdem kann diese große Anzahl von Konfigurationseinträgen zu Leistungsproblemen in der Citrix ADC Appliance führen.

Eine einfachere Methode ist die Verwendung von Platzhalterports in einem statischen Zuordnungseintrag. Sie müssen nur einen statischen Zuordnungseintrag mit NAT-Port und Subscriber-Port-Parametern auf das Platzhalterzeichen (*) und den Protokollparameter auf ALL erstellen, um alle Ports einer Teilnehmer-IP-Adresse für alle Protokolle im Internet verfügbar zu machen.

Bei eingehenden oder ausgehenden Verbindungen eines Abonnenten, die einem statischen Platzhalterzuordnungseintrag entsprechen, ändert sich der Port des Abonnenten nach dem NAT-Vorgang nicht. Wenn eine vom Abonnenten initiierte Verbindung zum Internet mit einem Eintrag für statische Platzhalterzuordnung übereinstimmt, weist die Citrix ADC Appliance einen NAT-Port zu, der dieselbe Nummer hat wie der Abonnentenport, von dem aus die Verbindung hergestellt wird. Ähnlich wird ein Internet-Host mit dem Port eines Abonnenten verbunden, indem er eine Verbindung zum NAT-Port herstellt, der dieselbe Nummer wie der Port des Abonnenten hat.

Erstellen Sie eine statische Platzhalterzuordnung mit den folgenden obligatorischen Parametereinstellungen, um die Citrix ADC Appliance so zu konfigurieren, dass Zugriff auf alle Ports einer Subscriber-IPv6-Adresse gewährt wird:

- Protocol=ALL
- Subscriber port = *
- NAT port = *

In einer statischen Platzhalterzuordnung ist im Gegensatz zu einer statischen Eins-zu-Eins-zu-Eins-Zuordnung das Festlegen des NAT-IP-Parameters erforderlich. Außerdem kann die NAT-IP-Adresse, die einer statischen Platzhalterzuordnung zugewiesen ist, nicht für andere Abonnenten verwendet werden.

So erstellen Sie eine statische Platzhalterzuordnung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn static <name> ALL <subscrIP> *  <natIP> * [-td <
   positive_integer>] [-destIP <ip_addr>

show lsn static
<!--NeedCopy-->
```

In der folgenden Beispielkonfiguration einer statischen Platzhalterzuordnung werden alle Ports eines Teilnehmers mit IP-Adresse 2001:DB 8:5001: :3 über NAT IP 203.0.11.33 zugänglich gemacht.

```
add lsn static NAT64-WILDCARD-STATIC-1 ALL 2001:DB8:5001::3 *
   203.0.113.33 *
Done
<!--NeedCopy-->
```


Protokollierung und Überwachung großer NAT64

October 5, 2021

Sie können umfangreiche NAT64-Informationen protokollieren, um Probleme zu diagnostizieren und zu beheben und gesetzliche Anforderungen zu erfüllen. Sie können die Leistung der großen NAT64-Bereitstellung überwachen, indem Sie statistische Leistungsindikatoren verwenden und die zugehörigen aktuellen Sitzungen anzeigen.

Protokollierung großer Maßstab NAT64

Die Protokollierung großer NAT64-Informationen ist erforderlich, damit ISPs die gesetzlichen Anforderungen erfüllen und die Quelle des Datenverkehrs jederzeit identifizieren können.

Eine Protokollmeldung für einen großen NAT64-Mapping-Eintrag besteht aus folgenden Informationen:

- Citrix ADC eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt.
- Zeitstempel
- Eintragstyp (MAPPING).
- Ob der Zuordnungseintrag erstellt oder gelöscht wurde.
- IP-Adresse, Port und Traffic-Domänen-ID des Abonnenten.
- NAT-IP-Adresse und -Port.
- Protokollname.
- Ziel-IP-Adresse, -Port und -Domänen-ID sind möglicherweise vorhanden, abhängig von den folgenden Bedingungen:
  - Ziel-IP-Adresse und -Port werden für die endpunktunabhängige Zuordnung nicht protokolliert.
  - Für die adressabhängige Zuordnung wird nur die Ziel-IP-Adresse protokolliert. Der Port wird nicht protokolliert.
  - Ziel-IP-Adresse und -Port werden für die adressen-port-abhängige Zuordnung protokolliert.

Eine Protokollmeldung für eine große NAT64-Sitzung besteht aus folgenden Informationen:

- Citrix ADC eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel
- Eintragstyp (SESSION)
- Gibt an, ob die Sitzung erstellt oder entfernt wird
- IP-Adresse, Port und Traffic-Domänen-ID des Abonnenten

- NAT IP-Adresse und Port
- Protokollname
- Ziel-IP-Adresse, -Port und -Domänen-ID des Datenverkehrs

In der folgenden Tabelle werden Beispieleinträge für große NAT64-Protokolle jedes Typs aufgeführt, der auf den konfigurierten Protokollservern gespeichert ist. Die Protokolleinträge zeigen, dass ein Abonnent, dessen IPv6-Adresse 2001:db 8:5001::9 mit Ziel IP verbunden war: Port 23.0.0.1:80 über NAT IP:port 203.0.113.63:45195 am 7. April 2016 von 14:07:57 GMT bis 14:10:59 GMT.

Protokolleintragstyp	Beispielprotokolleintrag
Sitzungserstellung	04/07/2016:14:07:57 GMT Informational 0-PPE-10 : default LSN LSN_SESSION 5532 0 : SESSION CREATED Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP
Mapping-Erstellung	04/07/2016:14:07:57 GMT Informational 0-PPE-10 : default LSN LSN_ADDR_MAPPING 5533 0 : ADM CREATED Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:TD 23.0.0.1:80, Protocol: TCP
Sitzungslöschung	04/07/2016:14:10:59 GMT 0-PPE-10 : default LSN LSN_SESSION 25012 0 : SESSION DELETED Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP
Zuordnungslöschung	04/07/2016:14:10:59 GMT 0-PPE-10 : default LSN LSN_ADDR_MAPPING 25013 0 : ADM DELETED Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP

Konfigurationsschritte

Sie können die Protokollierung großer NAT64-Informationen für eine große NAT64-Konfiguration konfigurieren, indem Sie die Protokollierungs- und Sitzungsprotokollierungsparameter der LSN-Gruppen

festlegen. Dies sind Parameter auf Gruppenebene und sind standardmäßig deaktiviert. Die Citrix ADC Appliance protokolliert große NAT64-Sitzungen für eine LSN-Gruppe nur, wenn Protokollierungs- und Sitzungsprotokollierungsparameter aktiviert sind.

In der folgenden Tabelle wird das Protokollierungsverhalten für eine LSN-Gruppe für verschiedene Einstellungen von Protokollierungs- und Sitzungsprotokollierungsparametern angezeigt.

Protokollierung	Sitzungsprotokollierung	Protokollierungsverhalten
Aktiviert	Aktiviert	Protokolliert LSN-Zuordnungseinträge sowie LSN-Sitzungen
Aktiviert	Deaktiviert	Protokolliert LSN-Zuordnungseinträge, aber keine LSN-Sitzungen
Deaktiviert	Aktiviert	Protokolliert weder Zuordnungseinträge noch LSN-Sitzungen

So protokollieren Sie umfangreiche NAT64-Informationen mit der CLI

Um die Protokollierungs- und Sitzungsprotokollierungsparameter beim Hinzufügen einer LSN-Gruppe festzulegen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn group <groupname> -clientname <string> [-logging (ENABLED|
    DISABLED)] [-sessionLogging (ENABLED|DISABLED)]

show lsn group
<!--NeedCopy-->
```

Um die Protokollierungs- und Sitzungsprotokollierungsparameter für eine vorhandene LSN-Gruppe festzulegen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lsn group <groupname> [-logging (ENABLED|DISABLED)] [-
    sessionLogging (ENABLED|DISABLED)]

show lsn group
<!--NeedCopy-->
```


Beispielkonfiguration

In diesem Beispiel der großformatigen NAT64-Konfiguration sind Protokollierungs- und Sitzungsprotokollierungsparamter für LSN-Gruppe LSN-NAT64-GROUP-1 aktiviert.

Die Citrix ADC Appliance protokolliert umfangreiche NAT64-Sitzungs- und Zuordnungsinformationen für Verbindungen von Abonnenten (im Netzwerk 2001:DB 8:5001: :/96).

Beispielkonfiguration:

```
1  add lsn client LSN-NAT64-CLIENT-1 Done
2  Done
3  bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
4  Done
5  add lsn pool LSN-NAT64-POOL-1
6  Done
7  bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
8  Done
9  add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
       :300::/96
10 Done
11 add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
       ip6profile LSN-NAT64-PROFILE-1  -logging ENABLED -sessionLogging
       ENABLED
12 Done
13 bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
14 Done
15 <!--NeedCopy-->
```

Protokollieren von MSISDN-Informationen für Large Scale NAT64

Eine Mobile Station Integrated Subscriber Directory Number (MSISDN) ist eine Telefonnummer, die einen Teilnehmer in mehreren Mobilfunknetzen eindeutig identifiziert. Der MSISDN ist mit einem Ländercode und einem nationalen Bestimmungscode verknüpft, der den Betreiber des Teilnehmers identifiziert.

Sie können eine Citrix ADC Appliance so konfigurieren, dass sie MSISDNs in großen NAT64-LSN-Protokolleinträgen für Abonnenten in Mobilfunknetzen einschließt. Das Vorhandensein von MSISDNs in den LSN-Protokollen erleichtert eine schnellere und genaue Rückverfolgung eines mobilen Teilnehmers, der gegen eine Richtlinie oder ein Gesetz verstoßen hat oder dessen Informationen von gesetzlichen Abfangbehörden verlangt werden.

Die folgenden LSN-Beispielprotokolleinträge enthalten MSISDN-Informationen für eine Verbindung von einem mobilen Abonnenten in einer LSN-Konfiguration. Die Protokolleinträge zeigen, dass ein

mobiler Abonnent, dessen MSISDN E164:5556543210 ist und IPv6-Adresse 2001:db8:5001::9 mit Ziel IP verbunden war: Port 23.0.0.1:80 über die NAT IP: Port 203.0.113.63:45195am 7. April 2016 von 14:07:57 GMT bis 14:10:59 GMT.

Protokolleintragstyp	Beispielprotokolleintrag
Sitzungserstellung	04/07/2016:14:07:57 GMT Informational 0-PPE-10 : default LSN LSN_SESSION 5532 0 : SESSION CREATED **E164:5556543210** Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP
Mapping-Erstellung	04/07/2016:14:07:57 GMT Informational 0-PPE-10 : default LSN LSN_ADDR_MAPPING 5533 0 : ADM CREATED **E164:5556543210** Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:TD 23.0.0.1:80, Protocol: TCP
Sitzungslöschung	04/07/2016:14:10:59 GMT 0-PPE-10 : default LSN LSN_SESSION 25012 0 : SESSION DELETED **E164:5556543210** Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP
Zuordnungslöschung	04/07/2016:14:10:59 GMT 0-PPE-10 : default LSN LSN_ADDR_MAPPING 25013 0 : ADM DELETED **E164:5556543210** Client IP-Port:TD **2001:db8:5001::9-34937:0**, NatIP:NatPort 203.0.113.63:45195, Destination IP:Port:TD 23.0.0.1:0:80, Protocol: TCP

Konfigurationsschritte

Führen Sie die folgenden Aufgaben aus, um MSISDN-Informationen in LSN-Protokolle einzuschließen:

- **Erstellen Sie ein LSN-Protokollprofil**. Ein LSN-Protokollprofil enthält den Protokollabonnentenidentifikationsparameter, der angibt, ob die MSISDN-Informationen in die LSN-Protokolle einer LSN-Konfiguration aufgenommen werden sollen.
- Binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration.Binden Sie das erstellte LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie den Pa-

rameter Protokollprofilname auf den erstellten LSN-Protokollprofilnamen festlegen. MSISDN-Informationen sind in allen LSN-Protokollen enthalten, die mit mobilen Abonnenten dieser LSN-Gruppe zusammenhängen.

So erstellen Sie ein LSN-Protokollprofil mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn logprofile <logprofilename> -logSubscriberID ( ENABLED |
   DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

So binden Sie ein LSN-Protokollprofil an eine LSN-Gruppe einer NAT64-LSN-Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Beispielkonfiguration

In diesem Beispiel der NAT64-LSN-Konfiguration hat das LSN-Protokollprofil LOG-PROFILE-MSISDN-1 den Protokollabonnentenidentifikationsparameter aktiviert. LOG-PROFILE-MSISDN-1 ist an die LSN-Gruppe LSN-NAT64-GROUP-1 gebunden. MSISDN-Informationen sind in den LSN-Sitzungs- und LSN-Mapping-Protokollen für Verbindungen von mobilen Abonnenten enthalten (im Netzwerk 2001:DB 8:5001::/96).

```
add lsn logprofile  LOG-PROFILE-MSISDN-1  -logSubscriberID ENABLED
Done
add lsn client LSN-NAT64-CLIENT-1
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
```



```
7  add lsn pool LSN-NAT64-POOL-1
8  Done
9  bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
10 Done
11 add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
      :300::/96
12 Done
13 add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
      ip6profile LSN-NAT64-PROFILE-1
14 Done
15 bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
16 Done
17 bind lsn group LSN-NAT64-GROUP-1 -logprofilename  LOG-PROFILE-MSISDN-1
18 Done
19 <!--NeedCopy-->
```

Kompakte Protokollierung für große NAT

Die Protokollierung von LSN-Informationen ist eine der wichtigen Funktionen, die von ISPs benötigt werden, um gesetzliche Anforderungen zu erfüllen und jederzeit die Quelle des Datenverkehrs zu identifizieren. Dies führt schließlich zu einer riesigen Menge an Protokolldaten, die die ISPs erfordern, große Investitionen für die Wartung der Protokollierungsinfrastruktur zu tätigen.

Kompakte Protokollierung ist eine Technik, um die Protokollgröße zu reduzieren, indem eine Notationsänderung mit kurzen Codes für Ereignis- und Protokollnamen verwendet wird. Beispielsweise C für Client, SC für erstellte Sitzung und T für TCP. Kompakte Protokollierung führt zu einer durchschnittlichen Verringerung der Protokollgröße um 40 Prozent.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben für die Protokollierung von LSN-Informationen im kompakten Format aus:

1. Erstellen Sie ein LSN-Protokollprofil. Ein LSN-Protokollprofil enthält den Parameter Log Compact, der angibt, ob Informationen im kompakten Format für eine LSN-Konfiguration protokolliert werden sollen.
2. Binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration. Binden Sie das erstellte LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie den Parameter Log Profile Name auf den erstellten LSN-Protokollprofilnamen festlegen. Alle Sitzungen und Zuordnungen für diese LSN-Gruppe werden im kompakten Format protokolliert.

So erstellen Sie ein LSN-Protokollprofil mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lsn logprofile <logprofilename> -logCompact (ENABLED|DISABLED)

show lsn logprofile
<!--NeedCopy-->
```

So binden Sie ein LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn group <groupname> -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

Beispielkonfiguration für NAT64:

```
add lsn logprofile  LOG-PROFILE-COMPACT-1 -logCompact ENABLED
Done
add lsn client LSN-NAT64-CLIENT-1
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
    :300::/96
Done
add lsn group LSN-NAT64-PROFILE-1 -clientname LSN-NAT64-CLIENT-1  -
    ip6profile LSN-NAT64-PROFILE-1
Done
bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
bind lsn group LSN-NAT64-GROUP-1  - logProfileName LOG-PROFILE-COMPACT-1
Done
<!--NeedCopy-->
```


Protokollieren von HTTP-Header-Informationen

Die Citrix ADC-Appliance kann Anforderungsheader-Informationen einer HTTP-Verbindung protokollieren, die die großformatige NAT64-Funktionalität von Citrix ADC verwendet. Die folgenden Header-Informationen eines HTTP-Anforderungspakets können protokolliert werden:

- URL, für die die HTTP-Anforderung bestimmt ist
- HTTP-Methode, die in der HTTP-Anforderung angegeben ist
- HTTP-Version, die in der HTTP-Anforderung verwendet wird
- IPv6-Adresse des Abonnenten, der die HTTP-Anforderung gesendet hat

Die HTTP-Header-Protokolle können von ISPs verwendet werden, um die Trends im Zusammenhang mit dem HTTP-Protokoll unter einer Gruppe von Abonnenten zu sehen. Beispielsweise kann ein ISP diese Funktion verwenden, um die beliebteste Website unter einer Reihe von Abonnenten herauszufinden.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben aus, um die Citrix ADC Appliance zum Protokollieren von HTTP-Header-Informationen zu konfigurieren:

- Erstellen Sie ein HTTP-Header-Log-Profil. Ein HTTP-Header-Protokollprofil ist eine Sammlung von HTTP-Header-Attributen (z. B. URL und HTTP-Methode), die für die Protokollierung aktiviert oder deaktiviert werden können.
- Binden Sie den HTTP-Header an eine LSN-Gruppe einer großen NAT64-Konfiguration. Binden Sie das HTTP-Header-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie den HTTP-Header-Logprofilnamenparameter auf den Namen des erstellten HTTP-Header-Protokollprofils festlegen. Die Citrix ADC Appliance protokolliert dann HTTP-Header-Informationen aller HTTP-Anforderungen in Bezug auf die LSN-Gruppe. Ein HTTP-Header-Protokollprofil kann an mehrere LSN-Gruppen gebunden werden, aber eine LSN-Gruppe kann nur ein HTTP-Header-Protokollprofil haben.

So erstellen Sie ein HTTP-Header-Protokollprofil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lsn httphdrlogprofile <httphdrlogprofilename> [-logURL ( ENABLED |
     DISABLED )] [-logMethod ( ENABLED | DISABLED )] [-logVersion (
     ENABLED | DISABLED )] [-logHost ( ENABLED | DISABLED )]
2
3 show lsn httphdrlogprofile
4 <!--NeedCopy-->
```


So binden Sie ein HTTP-Header-Protokollprofil mit der Befehlszeilenschnittstelle an eine LSN-Gruppe

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lsn group <groupname> -httphdrlogprofilename <string>

show lsn group <groupname>
<!--NeedCopy-->
```

Beispielkonfiguration

```
add lsn httphdrlogprofile HTTP-HEADER-LOG-1
Done
add lsn client LSN-NAT64-CLIENT-1 Done
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
   :300::/96
Done
add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
   ip6profile LSN-NAT64-PROFILE-1
Done
bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
Done
bind lsn group LSN-NAT64-GROUP-1 -httphdrlogprofilename HTTP-HEADER-LOG
   -1
Done
<!--NeedCopy-->
```

Aktuelle großformatige NAT64-Sitzungen anzeigen

Sie können die aktuellen großformatigen NAT64-Sitzungen anzeigen, um unerwünschte oder ineffiziente Sitzungen auf der Citrix ADC Appliance zu erkennen. Sie können alle oder einige große NAT64-Sitzungen anhand von Selektionsparametern anzeigen.

> **Hinweis:**
>
> Wenn mehr als eine Million groß angelegte NAT64-Sitzungen auf der Citrix ADC Appliance vorhanden sind, empfiehlt Citrix, die Auswahlparameter zur Anzeige ausgewählter großformatiger NAT64-Sitzungen zu verwenden, anstatt sie alle anzuzeigen.

So zeigen Sie alle großformatigen NAT64-Sitzungen mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show lsn session  -nattype NAT64
<!--NeedCopy-->
```

So zeigen Sie selektive großformatige NAT64-Sitzungen mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show lsn session  -nattype NAT64 [-network6 <ipv6_addr|*>] [-clientname
    <string>] [-natIP <ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```

Anzeige der NAT64-Statistiken im großen Maßstab

Sie können Statistiken im Zusammenhang mit dem großen NAT64-Modul anzeigen und deren Leistung bewerten oder Probleme beheben. Sie können eine Zusammenfassung der Statistiken aller großen NAT64-Konfigurationen oder einer bestimmten großen NAT64-Konfiguration anzeigen. Die statistischen Leistungsindikatoren spiegeln Ereignisse seit dem letzten Neustart der Citrix ADC Appliance wider. Alle diese Leistungsindikatoren werden auf 0 zurückgesetzt, wenn die Citrix ADC Appliance neu gestartet wird.

So zeigen Sie die Gesamtstatistiken der großen NAT64 mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat lsn nat64
<!--NeedCopy-->
```


So zeigen Sie Statistiken für eine bestimmte große NAT64-Konfiguration mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat lsn group <groupname>
<!--NeedCopy-->
```

Löschen großer NAT64-Sitzungen

Sie können unerwünschte oder ineffiziente große NAT64-Sitzungen von der Citrix ADC Appliance entfernen. Die Appliance gibt sofort Ressourcen (wie NAT-IP-Adresse, Port und Speicher) frei, die für diese Sitzungen zugewiesen wurden, sodass die Ressourcen für neue Sitzungen verfügbar sind. Die Appliance löscht auch alle nachfolgenden Pakete, die sich auf diese entfernten Sitzungen beziehen. Sie können alle oder ausgewählte große NAT64-Sitzungen aus der Citrix ADC Appliance entfernen.

So löschen Sie alle großformatigen NAT64-Sitzungen mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
flush lsn session -nattype NAT64

show lsn session -nattype NAT64
<!--NeedCopy-->
```

So löschen Sie selektive großformatige NAT64-Sitzungen mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
flush lsn session -nattype NAT64 [-network6 <ipv6_addr|*>] [-
   clientname <string>] [-natIP <ip_addr> [-natPort <port>]]

show lsn session -nattype NAT64 [-network6 <ipv6_addr|*>] [-clientname
    <string>] [-natIP <ip_addr> [-natPort <port>]]
<!--NeedCopy-->
```

Beispielkonfiguration:

Löschen aller großen NAT64-Sitzungen, die auf einer Citrix ADC Appliance vorhanden sind

```
flush lsn session  -nattype NAT64
Done
<!--NeedCopy-->
```

Löschen aller großen NAT64-Sitzungen im Zusammenhang mit der Client-Entität LSN-NAT64-CLIENT-1

```
flush lsn session -nattype NAT64 -clientname LSN-NAT64-CLIENT-1
Done
<!--NeedCopy-->
```

Löschen aller großen NAT64-Sitzungen im Zusammenhang mit einem Teilnehmernetzwerk (2001:DB8:5001: :/96) der LSN-Client-Entität LSN-NAT64-CLIENT-2

```
flush lsn session -nattype NAT64 -network6 2001:DB8:5001::/96 -
   clientname LSN-NAT64-CLIENT-2
Done
<!--NeedCopy-->
```

IPFIX-Protokollierung

Die Citrix ADC Appliance unterstützt das Senden von Informationen zu LSN-Ereignissen im IPFIX-Format (Internet Protocol Flow Information Export) an die konfigurierte Gruppe von IPFIX-Kollektoren. Die Appliance verwendet die vorhandene AppFlow Funktion, um LSN-Ereignisse im IPFIX-Format an die IPFIX-Kollektoren zu senden.

IPFIX-basierte Protokollierung ist für die folgenden NAT64-bezogenen Ereignisse verfügbar:

- Erstellen oder Löschen einer LSN-Sitzung.
- Erstellen oder Löschen eines LSN-Zuordnungseintrags.
- Zuweisung oder Aufteilung von Portblöcken im Rahmen der deterministischen NAT.
- Zuweisung oder Aufteilung von Portblöcken im Kontext dynamischer NAT.
- Wann immer das Teilnehmersitzungskontingent überschritten wird.

Zu berücksichtigende Punkte, bevor Sie IPFIX-Protokollierung konfigurieren

Bevor Sie mit der Konfiguration von IPsec ALG beginnen, sollten Sie die folgenden Punkte beachten:

- Sie müssen die AppFlow Funktion und die IPFIX-Kollektoren auf der Citrix ADC Appliance konfigurieren. Anweisungen finden Sie unter Konfigurieren der AppFlow-Funktion.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben für die Protokollierung von LSN-Informationen im IPFIX-Format aus:

- **Aktivieren Sie die LSN-Protokollierung in der AppFlow Konfiguration**. Aktivieren Sie den LSN-Protokollierungsparameter als Teil der AppFlow Konfiguration.
- **Erstellen Sie ein LSN-Protokollprofil**. Ein LSN-Protokollprofil enthält den IPFIX-Parameter, mit dem die Protokollinformationen im IPFIX-Format aktiviert oder deaktiviert werden.
- **Binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration**. Binden Sie das LSN-Protokollprofil an eine oder mehrere LSN-Gruppen. Ereignisse im Zusammenhang mit der gebundenen LSN-Gruppe werden im IPFIX-Format protokolliert.

So aktivieren Sie die LSN-Protokollierung in der AppFlow Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set appflow param -lsnLogging ( ENABLED | DISABLED )

show appflow param
<!--NeedCopy-->
```

Um ein LSN-Protokollprofil mit der CLI an der Eingabeaufforderung zu erstellen, geben Sie

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lsn logprofile <logProfileName>  -logipfix ( ENABLED | DISABLED )

show lsn logprofile
<!--NeedCopy-->
```

So binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
bind lsn group <groupname>  -logProfileName <lsnlogprofilename>

show lsn group
<!--NeedCopy-->
```

So erstellen Sie ein LSN-Protokollprofil mit der GUI

Navigieren Sie zu **System** > **Large Scale NAT** > **Profile**, klicken Sie auf Register **Protokoll**, und fügen Sie dann ein Protokollprofil hinzu.

So binden Sie das LSN-Protokollprofil an eine LSN-Gruppe einer LSN-Konfiguration mit der GUI

1. Navigieren Sie zu **System** > **Large Scale NAT** > **LSN Group,** öffnen Sie die **LSN-Gruppe**.
2. Klicken Sie **unter Erweiterte Einstellungen** auf **+ Protokollprofil**, um das erstellte Protokollprofil an die LSN-Gruppe zu binden.

Port Control Protocol für Large Scale NAT64

October 5, 2021

Citrix ADC Appliances unterstützen jetzt Port Control Protocol (PCP) für Large Scale NAT (LSN). Viele Abonnentenanwendungen eines ISP müssen über das Internet zugänglich sein (z. B. IOT-Geräte (Internet of Things), z. B. eine IP-Kamera, die die Überwachung über das Internet ermöglicht). Eine Möglichkeit, diese Anforderung zu erfüllen, besteht darin, statische Large Scale NAT-Karten (LSN) zu erstellen. Aber für eine sehr große Anzahl von Abonnenten ist das Erstellen statischer LSN NAT-Karten keine machbare Lösung.

Port Control Protocol (PCP) ermöglicht es einem Abonnenten, spezifische LSN NAT-Zuordnungen für sich selbst und/oder für andere Geräte von Drittanbietern anzufordern. Das große NAT-Gerät erstellt eine LSN-Karte und sendet sie an den Abonnenten. Der Abonnent sendet die entfernten Geräte über das Internet die NAT-IP-Adresse:NAT-Port, an der sie eine Verbindung zum Abonnenten herstellen können.

In der Regel senden Anwendungen häufig Keepalive-Nachrichten an das große NAT-Gerät, damit ihre LSN-Zuordnungen keine Timeout aufweisen. PCP hilft, die Häufigkeit solcher Keep-Alive-Nachrichten zu reduzieren, indem die Anwendungen die Timeout-Einstellungen der LSN-Zuordnungen erlernen können. Dies trägt dazu bei, den Bandbreitenverbrauch im Zugangsnetzwerk des ISP und den Batterieverbrauch auf mobilen Geräten zu reduzieren.

PCP ist ein Client-Server-Modell und läuft über das UDP-Transportprotokoll. Eine Citrix ADC Appliance implementiert die PCP-Serverkomponente und ist mit RFC 6887 kompatibel.

Konfigurationsschritte

Führen Sie die folgenden Aufgaben für die Konfiguration von PCP aus:

- **(Optional) Erstellen Sie ein PCP-Profil**. Ein PCP-Profil enthält Einstellungen für PCP-bezogene Parameter (z. B. zum Abhören von Zuordnungen und Peer-PCP-Anforderungen). Ein PCP-Profil kann an einen PCP-Server gebunden werden. Ein PCP-Profil, das an einen PCP-Server gebunden ist, wendet alle seine Einstellungen auf den PCP-Server an. Ein PCP-Profil kann an mehrere PCP-Server gebunden werden. Standardmäßig ist ein PCP-Profil mit Standardparametereinstellungen an alle PCP-Server gebunden. Ein PCP-Profil, das Sie an einen PCP-Server binden, überschreibt die standardmäßigen PCP-Profileinstellungen für diesen Server. Ein Standard-PCP-Profil weist die folgenden Parametereinstellungen auf:
  - Zuordnung: Aktiviert
  - Peer: Aktiviert
  - Minimale Kartenlebensdauer: 120 Sekunden
  - Maximale Lebensdauer: 86400 Sekunden
  - Ankündigungsanzahl: 10
  - Dritte: Deaktiviert
- **Erstellen Sie einen PCP-Server und binden Sie ein PCP-Profil an ihn**. Erstellen Sie einen PCP-Server auf der Citrix ADC Appliance, um PCP-bezogene Anforderungen und Nachrichten von den Abonnenten zu überwachen. Eine Subnetz-IP-Adresse (SNIP) oder (SNIP6) muss einem PCP-Server zugewiesen werden, um darauf zuzugreifen. Standardmäßig überwacht ein PCP-Server Port 5351.
- **Binden Sie den PCP-Server an eine LSN-Gruppe einer LSN-Konfiguration**. Binden Sie den erstellten PCP-Server an eine LSN-Gruppe einer LSN-Konfiguration, indem Sie den PCP-Server-Parameter so einstellen, dass der erstellte PCP-Server angegeben wird. Der erstellte PCP-Server kann nur von den Abonnenten dieser LSN-Gruppe zugegriffen werden.

> **Hinweis:**
>
> Ein PCP-Server für eine große NAT-Konfiguration erfüllt keine Anforderungen von Abonnenten, die aus ACL-Regeln identifiziert werden.

So erstellen Sie ein PCP-Profil mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add pcp profile <name> [-mapping ( ENABLED | DISABLED )] [-peer (
    ENABLED | DISABLED )] [-minMapLife <secs>]  [-maxMapLife <secs>] [-
    announceMultiCount <positive_integer>][-thirdParty ( ENABLED |
    DISABLED )]

show pcp profile <name>
<!--NeedCopy-->
```

So erstellen Sie einen PCP-Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add pcp server <name> <IPAddress> [-port <portNum|*>] [-pcpProfile <
    string>]

show pcp server <name>
<!--NeedCopy-->
```

Beispielkonfiguration für NAT64

In der folgenden Beispielkonfiguration ist PCP-Server PCP-SERVER-1 mit PCP-Einstellungen von PCP-PROFILE-1 an die LSN-Gruppe LSN-NAT64-GROUP-1 gebunden. PCP-SERVER-1 bedient PCP-Anfragen von IPv6-Abonnenten im Netzwerk 2001:DB 8:5001: :/96.

Beispielkonfiguration:

```
add pcp profile PCP-PROFILE-1 -minMapLife 400
Done
add pcp server PCP-SERVER-1 2001:DB8:6001::90  -pcpProfile PCP-PROFILE
    -1
Done
add lsn client LSN-NAT64-CLIENT-1
Done
bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
Done
add lsn pool LSN-NAT64-POOL-1
Done
bind lsn pool LSN-NAT64-POOL-1 203.0.113.61 - 203.0.113.70
Done
add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
    :300::/96
```



```
14 Done
15 add lsn group LSN-NAT64-PROFILE-1 -clientname LSN-NAT64-CLIENT-1  -
      ip6profile LSN-NAT64-PROFILE-1
16 Done
17 bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
18 Done
19 bind lsn group LSN-NAT64-GROUP-1  - pcpServer PCP-NAT64-SERVER-1
20 Done
21 <!--NeedCopy-->
```

LSN64 in einem Cluster-Setup

October 5, 2021

Große NAT64-Konfigurationen werden bei einem Citrix ADC Cluster-Setup unterstützt.

Ein Citrix ADC-Cluster ist eine Gruppe von Citrix ADC Appliances, die als ein einzelnes System konfiguriert und verwaltet werden. Ein Citrix ADC Cluster bietet Skalierbarkeit und Verfügbarkeit. Jede Citrix ADC Appliance in einem Cluster-Setup fungiert als unabhängige LSN-Entität und wird als ein einzelnes System verwaltet.

Die LSN-Konfiguration in einem Cluster-Setup ist identisch mit einer eigenständigen Appliance, mit Ausnahme eines bestimmten Pools von LSN-IP-Adressen sind jeweils nur einem Knoten zugeordnet. Mit anderen Worten, eine LSN-IP-Pool-Entität wird in einem bestimmten Knoten als Spotted-Entity konfiguriert. Alle Knoten eines Cluster-Setups können über eine bestimmte LSN-IP-Pool-Entität verfügen. Um sicherzustellen, dass die Pakete, die sich auf eine LSN-Sitzung beziehen, auf demselben Clusterknoten empfangen werden, der den NAT-Vorgang ausgeführt hat, wird die Policy-basierte Backplane-Steuerung (PBS) konfiguriert. PBS steuert die empfangenen verwandten Pakete einer LSN-Sitzung auf denselben Clusterknoten.

Beispielkonfiguration:

```
1 add lsn client LSN-NAT64-CLIENT-1
2
3 Done
4
5 bind lsn client LSN-NAT64-CLIENT-1 -network6 2001:DB8:5001::/96
6
7 Done
8
9 add lsn pool LSN-NAT64-POOL-1
```



```
10
11 Done
12
13 bind lsn pool LSN-NAT64-POOL-1 -ownerNode 1  203.0.113.61 -
      203.0.113.70
14
15 Done
16
17 bind lsn pool LSN-NAT64-POOL-1 -ownerNode 2  203.0.113.101 -
      203.0.113.110
18
19 Done
20
21 add lsn ip6profile LSN-NAT64-PROFILE-1 -type NAT64 -natprefix 2001:DB8
      :300::/96
22
23 Done
24
25 add lsn group LSN-NAT64-GROUP-1 -clientname LSN-NAT64-CLIENT-1  -
      ip6profile LSN-NAT64-PROFILE-1
26
27 Done
28
29 bind lsn group LSN-NAT64-GROUP-1 -poolname LSN-NAT64-POOL-1
30
31 Done
32
33 add ns acl6 NAT64-DFD ALLOW -srcIPv6 = 2001:DB8:5001:: -type DFD -
      dfdhash SIP -dfdprefix 64
34
35 Done
36
37 apply ns acls6 -type DFD
38
39 Done
40 <!--NeedCopy-->
```

Zuordnen von Adresse und Port mittels Übersetzung

October 5, 2021

Mapping Address and Port using Translation (MAP-T) ist eine IPv6-Übergangslösung für ISPs mit IPv6-

Infrastruktur, um ihre IPv4-Abonnenten mit dem IPv4-Internet _.MAP-T zu verbinden, basiert auf zustandslosen IPv4- und IPv6-Adressumsetzungstechnologien. MAP-T ist ein Mechanismus, der doppelte Übersetzung (IPv4 nach IPv6 und umgekehrt) auf Kunden-Edge-Geräten (CE) und Grenzroutern (im ISP-Kernnetz) durchführt.

In einer MAP-T-Bereitstellung implementiert das CE-Gerät eine Kombination aus statusbehafteten NAPT44-Übersetzung und statusloser NAT46-Übersetzung. Das CE-Gerät erhält NAT-IP und den Port-Block, der für die Übersetzung über DHCPv6 oder eine andere Methode verwendet werden soll.

Wenn ein IPv4-Paket von einem Teilnehmergerät am CE-Gerät ankommt, führt das CE-Gerät NAPT44 aus und speichert die NAPT44-Bindungsinformationen. Nach der NAT44-Übersetzung wird das Paket der NAT46-Übersetzung unterzogen und dann an das BR-Gerät weitergeleitet, das sich im Kernnetz des ISP befindet. Das BR-Gerät empfängt die IPv6-Pakete vom CE-Gerät, extrahiert und validiert die NAT-IP und den Portblock, die in den IPv6-Header eingebettet sind, und leitet das IPv4-Paket an das IPv4-Internet weiter. Wenn der BR das IPv4-Paket aus dem Internet empfängt, übersetzt er das IPv4-Paket in ein IPv6-Paket und sendet das IPv6-Paket an das CE-Gerät.

MAP-T ist auf einem BR-Gerät zustandslos, so dass das BR-Gerät nicht benötigt, um NAT auf dem Datenverkehr auszuführen. Stattdessen wird die NAT-Funktionalität an die CE-Geräte delegiert. Diese Delegierung und statuslose Funktionalität in BR-Geräten ermöglicht es der BR-Bereitstellung, proportional zum Verkehrsaufkommen zu skalieren.

Die Citrix ADC Appliance implementiert die BR-Funktionalität einer MAP-T-Lösung, wie in RFC 7599 beschrieben.

Konfigurieren von MAP-T

Die Konfiguration von MAP-T auf einer Citrix ADC Appliance umfasst die folgenden Aufgaben:

- Hinzufügen einer Standardzuordnungsregel
- Hinzufügen einer grundlegenden Zuordnungsregel
- Binden Sie einen IPv4-NAT-Adressbereich von CE-Geräten an eine grundlegende Zuordnungsregel
- Hinzufügen einer Zuordnungsdomäne und Binden einer grundlegenden Zuordnungsregel und einer Standardzuordnungsregel an die Domäne

So fügen Sie eine Standardzuordnungsregel mit der CLI hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add MapDmr <name> -BRIpv6Prefix ( <ipv6_addr> | <*> )
```



```
show MapDmr <name>
<!--NeedCopy-->
```

So fügen Sie eine grundlegende Zuordnungsregel mit der CLI hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add MapBmr <name> -RuleIpv6Prefix <ipv6_addr> | <*>  [-psidoffset <
    positive_integer>] [-EAbitLength <positive_integer>]  [-psidlength <
    positive_integer>]

show MapBmr <name>
<!--NeedCopy-->
```

So binden Sie IPv4-NAT-Adressbereich von CE-Geräten mit der CLI an eine grundlegende Zuordnungsregel

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind MapBmr <name> (-network <ip_addr>  [-netmask <netmask>])

show MapBmr <name>
<!--NeedCopy-->
```

So fügen Sie eine Zuordnungsdomäne mit der CLI hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add MapDomain <name> -MapDmrName <string>

show MapDomain <name>
<!--NeedCopy-->
```

So binden Sie eine grundlegende Zuordnungsregel mit der CLI an eine Zuordnungsdomäne

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
bind MapDomain <name> -MapBmrName <string>

show MapDomain <name>
<!--NeedCopy-->
```

Beispielkonfiguration

```
add mapdmr DMR-1 -BRIpv6Prefix 2002:db8::/64

Done

add mapbmr BMR-1 -ruleIpv6Prefix 2002:db8:89ab::/48 -eAbitLength 16 -
    psidlength 8 -psidoffset 6

Done

bind mapbmr BMR-1 -network 192.0.1.0 -netmask 255.255.255.0

Done

add MapDomain MAP-DOMAIN-1 -mapdmrname DMR-1

Done

bind MapDomain MAP-DOMAIN-1 -mapbmrname BMR-1
Done
<!--NeedCopy-->
```

Telco-Teilnehmerverwaltung

December 7, 2021

Die Zahl der Abonnenten in einem Telekommunikationsnetz nimmt zu einem beispiellosen Tempo zu, und die Verwaltung dieser Abonnenten wird zu einer Herausforderung für Dienstleister. Neuere, schnellere und intelligentere Geräte stellen hohe Anforderungen an das Netzwerk und die Teilnehmerverwaltungssysteme. Es ist nicht mehr möglich, jedem Abonnenten den gleichen Servicestandard zu bieten, und die Notwendigkeit einer Datenverarbeitung auf Teilnehmerbasis ist unerlässlich.

Die Citrix ADC Appliance bietet den Profilabonnenten auf der Grundlage ihrer Informationen, die in der Policy and Charging Rules Function (PCRF) gespeichert sind. Wenn ein mobiler Teilnehmer eine Verbindung zum Internet herstellt, ordnet das Paketgateway dem Abonnenten eine IP-Adresse zu und leitet das Datenpaket an die Appliance weiter. Die Appliance empfängt die Teilnehmerinformationen dynamisch, oder Sie können statische Abonnenten konfigurieren. Diese Informationen ermöglichen es der Appliance, ihre umfassenden Traffic-Management-Funktionen wie Content Switching, integriertes Caching, Rewrite und Responder auf Teilnehmerbasis anzuwenden, um den Datenverkehr zu verwalten.

Bevor Sie die Citrix ADC Appliance zum Verwalten von Abonnenten konfigurieren, müssen Sie dem Modul, in dem Abonnentensitzungen gespeichert sind, Speicher zuweisen. Für dynamische Abonnenten müssen Sie eine Schnittstelle konfigurieren, über die die Appliance Sitzungsinformationen erhält. Statischen Abonnenten müssen IDs zugewiesen werden, und Sie können sie Richtlinien zuordnen.

Sie können auch Folgendes tun:

- Durchsetzung und Verwaltung der Abonnentenrichtlinien.
- Konfigurieren Sie die Appliance, um einen Abonnenten eindeutig zu identifizieren, indem Sie nur das IPv6-Präfix anstelle der vollständigen IPv6-Adresse verwenden.
- Verwenden Sie Richtlinien, um TCP-Datenverkehr sowohl für dynamische als auch für statische Abonnenten zu optimieren. Diese Richtlinien verknüpfen unterschiedliche TCP-Profile mit unterschiedlichen Benutzertypen.
- Verwalten von Leerlaufsitzungen auf einer Citrix ADC Appliance.
- Aktivieren Sie die Protokollierung auf einem Protokollserver.
- Entfernen Sie LSN-Sitzungen für gelöschte Teilnehmersitzungen.

Zuweisen von Speicher für das Teilnehmersitzungsspeichermodul

Jeder Teilnehmersitzungseintrag verbraucht 1 KB Arbeitsspeicher. Die Speicherung von 500.000 Teilnehmersitzungen zu einem beliebigen Zeitpunkt erfordert 500 MB Arbeitsspeicher. Dieser Wert muss der minimalen Speicheranforderungen hinzugefügt werden, die als Teil der Ausgabe des Befehls show extendedmemoryparam angezeigt wird. Im folgenden Beispiel ist die Ausgabe für eine Citrix ADC VPX Instanz mit 3 Paket-Engines und 8 GB Arbeitsspeicher.

Um 500.000 Teilnehmersitzungen auf dieser Appliance zu speichern, muss der konfigurierte Arbeitsspeicher 2058+500 MB betragen (500.000 x 1 KB = 500 MB).

> **Hinweis:**
>
> Der konfigurierte Speicher muss ein Vielfaches von 2 MB aufweisen und darf die maximale Speicherauslastung nicht überschreiten. Die Appliance muss neu gestartet werden, damit die Änderungen wirksam werden.

Beispiel

```
show extendedmemoryparam
        Extended Memory Global Configuration. This memory is utilized by
            LSN and Subscriber Session Store Modules:
         Active Memory Usage: 0 MBytes
         Configured Memory Limit: 0 MBytes
         Minimum Memory Required: 2058 MBytes
         Maximum Memory Usage Limit: 2606 MBytes
     Done
     set extendedmemoryparam -memLimit 2558
     Done
     show extendedmemoryparam
             Extended Memory Global Configuration. This memory is
                utilized by LSN and Subscriber Session Store Modules:

             Active Memory Usage: 2558 MBytes
             Configured Memory Limit: 2558 MBytes
             Minimum Memory Required: 2058 MBytes
             Maximum Memory Usage Limit: 2606 MBytes
     Done
<!--NeedCopy-->
```

Konfigurieren einer Schnittstelle für dynamische Abonnenten

Die Citrix ADC Appliance empfängt die Teilnehmerinformationen dynamisch über einen der folgenden Schnittstellentypen:

- GX-Schnittstelle
- RADIUS-Schnittstelle
- RADIUS- und GX-Schnittstelle

> **Hinweis:**
>
> - Ab NetScaler Version 12.0 Build 57.19 wird die Gx-Schnittstelle für eine Clusterbereitstellung unterstützt. Weitere Informationen finden Sie unter Gx-Schnittstelle in einer Cluster-Topologie.
> - In einem HA-Setup werden die Teilnehmersitzungen kontinuierlich auf dem sekundären Knoten synchronisiert. Im Falle eines Failovers stehen die Teilnehmerinformationen auf dem sekundären Knoten weiterhin zur Verfügung.

GX-Schnittstelle

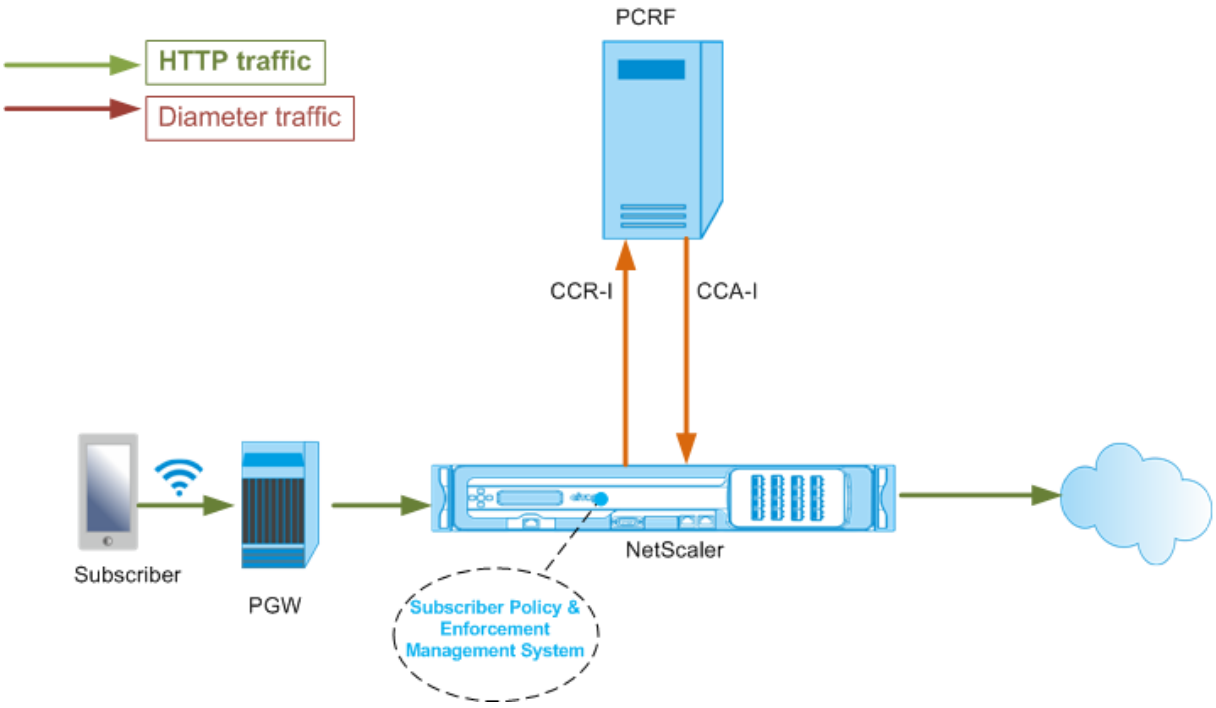
Eine GX-Schnittstelle (gemäß 3GPP 29.212) ist eine Standardschnittstelle, die auf dem Durchmesserprotokoll basiert, die den Austausch von Richtlinienkontroll- und Gebührenregeln zwischen einer PCRF und einer PCEF-Entität (Policy and Charging Enforcement Function, Policy and Charging Enforcement Function, PCEF) in einem Telco-Netzwerk ermöglicht.

Wenn eine IP-CAN-Sitzung eingerichtet wird, leitet das Paket-Gateway die Teilnehmer-ID, z. B. den MSISDN, und die Framed-IP-Adressinformationen über den Abonnenten an den PCRF als Durchmesser-Nachricht weiter. Wenn das Datenpaket vom Paketgateway (PGW) an die Appliance ankommt, verwendet die Appliance die Teilnehmer-IP-Adresse, um die PCRF abzufragen, um die Teilnehmerinformationen abzurufen. Dies wird auch als sekundäre PCEF-Funktionalität bezeichnet.

Die von der Appliance über die GX-Schnittstelle empfangenen Policy and Charging Control (PCC) -Regeln werden während der Teilnehmersitzung auf der Appliance gespeichert, d. h., bis der PCRF eine Re-Auth-Request (RAR-Nachricht) mit einem Session-Release-Cause-AVP sendet oder die Teilnehmersitzung von der CLI oder der -Konfigurationsdienstprogramm. Wenn Updates für einen vorhandenen Abonnenten vorhanden sind, sendet der PCRF die Aktualisierungen in einer RAR-Nachricht. Eine Abonnentensitzung wird initiiert, wenn sich ein Abonnent am Netzwerk anmeldet, und beendet, wenn sich der Abonnent abmeldet.

> **Hinweis**: Wenn der PCRF-Server ausgefallen ist, erstellt die Citrix ADC Appliance negative Sitzungen für die ausstehenden oder eingehenden GX-Abonnentenanforderungen. Wenn der PCRF-Server erneut erstellt wird, verhindert die Citrix ADC Appliance einen Sturm von Anforderungen, indem sie darauf wartet, dass die negativen Sitzungen abgelaufen sind, bevor die spezifischen Teilnehmeranforderungen ausgeführt werden.

Die folgende Abbildung zeigt den Datenfluss auf hoher Ebene. Es geht davon aus, dass der Datenebenenverkehr HTTP ist. Die Appliance sendet eine Credit Control Request (CCR) über eine Gx-Schnittstelle an den PCRF-Server und empfängt in der Credit Control Antwort (CCA) die PCC-Regeln und optional andere Informationen, wie z. B. den RAT (Radio Access Technology) Typ, die für den jeweiligen Teilnehmer gelten. PCC-Regeln enthalten einen oder mehrere Richtliniennamen (Regel) und andere Parameter. Die Appliance verwendet diese Informationen, um die auf der Appliance gespeicherten vordefinierten Regeln abzurufen und den Datenfluss zu lenken. Außerdem werden diese Informationen während der Teilnehmersitzung im Abonnentenrichtlinien- und Erzwingungsverwaltungssystem gespeichert. Nachdem eine Abonnentensitzung beendet wurde, verwirft die Appliance alle Informationen über den Abonnenten.



Das folgende Beispiel zeigt die Befehle zum Konfigurieren einer GX-Schnittstelle. Die Befehle sind fett.

Führen Sie die folgenden Aufgaben aus, um eine GX-Schnittstelle einzurichten

Fügen Sie für jede Gx-Schnittstelle einen DIAMETER-Dienst hinzu. Beispiel:

```
1 add service pcrf-svc1 203.0.113.1 DIAMETER 3868
2
3 add service pcrf-svc2 203.0.113.2 DIAMETER 3868
4 <!--NeedCopy-->
```

Fügen Sie einen nicht adressierbaren DIAMETER Load Balancing virtuellen Server hinzu, und binden Sie die in Schritt 1 erstellten Dienste an diesen virtuellen Server. Geben Sie für mehr als einen Dienst einen persistenceType und persistAVPno an, damit bestimmte Sitzungen vom gleichen PCRF-Server verarbeitet werden. Beispiel:

```
1 add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
     persistAVPno 263
2
3 bind lb vserver vdiam pcrf-svc1
4
5 bind lb vserver vdiam pcrf-svc2
```



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

Konfigurieren Sie Citrix ADC-Diameter-Identität und -Realm. Identität und Realm werden als Origin-Host- und Origin-Realm-AVPs in Durchmessermeldungen verwendet, die vom Gx-Client gesendet werden. Beispiel:

```
set ns diameter -identity netscaler.com -realm com
<!--NeedCopy-->
```

Konfigurieren Sie die GX-Schnittstelle, um den in Schritt 2 erstellten virtuellen Server als virtuellen PCRF-Server zu verwenden. Geben Sie den PCRF-Bereich an, der als Ziel-Realm-AVP in Durchmessermeldungen verwendet werden soll, die vom Gx-Client gesendet werden. Beispiel:

```
set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf.com
<!--NeedCopy-->
```

Legen Sie den Abonnentenschnittstellentyp auf GXOnly fest. Beispiel:

```
set subscriber param -interfaceType GxOnly
<!--NeedCopy-->
```

Geben Sie Folgendes ein, um die Konfiguration und den Status der GX-Schnittstelle anzuzeigen:

```
show subscriber gxinterface
<!--NeedCopy-->
```

Beispiel

```
show subscriber gxinterface
    Gx Interface parameters:
        PCRF Vserver: vdiam (DOWN)
        Gx Client Identity...:  netscaler1.com
        Gx Client Realm ..........:  com
        PCRF Realm: epc.mnc030.mcc234.3gppnetwork.org
        Hold Packets On Subscriber Absence: YES
        CCR Request Timeout: 4 Seconds
```



```
9          CCR Request Retry Attempts: 1
10         Gx HealthCheck enabled: NO
11         Gx HealthCheck TTL : 30 Seconds
12         CER Request Timeout: 10 Seconds
13         RevalidationTimeout: 30 Seconds
14         NegativeTTL: 60 Seconds
15         NegativeTTL Limited Success: NO
16         Purge SDB on Gx Failure: YES
17         ServicePath AVP code: 262099    ServicePath AVP VendorID: 3845
18         PCRF Connection State: PCRF is not ready
19     Done
20
21 <!--NeedCopy-->
```

ARGUMENTS

vServer

Name des virtuellen Lastausgleichs- oder Content Switching-Server, zu dem die GX-Verbindungen hergestellt werden. Der Diensttyp des virtuellen Servers muss DIAMETER oder SSL_DIAMETER sein. Dieser Parameter schließt sich mit dem Service-Parameter gegenseitig aus. Daher können Sie nicht sowohl den Dienst als auch den virtuellen Server in der GX-Schnittstelle festlegen.

Service

Name des DIAMETER oder SSL_DIAMETER Dienstes, der PCRF entspricht, zu dem die Gx-Verbindung hergestellt wird. Dieser Parameter schließt sich mit dem vserver-Parameter gegenseitig aus. Daher können Sie nicht sowohl den Dienst als auch den virtuellen Server in der GX-Schnittstelle festlegen.

pcrfRealm

Der Bereich von PCRF, an den die Nachricht weitergeleitet werden soll. Dies ist der Bereich, der in Destination-Realm AVP vom Citrix ADC Gx-Client (als Diameter Knoten) verwendet wird.

holdOnSubscriberAbsence

Setzen Sie auf Ja, um Pakete zu speichern, bis die Teilnehmersitzungsinformationen vom PCRF-Server abgerufen werden. Wenn dieser Wert auf Nein gesetzt ist, wird das Standardabonnentenprofil angewendet, bis die Teilnehmersitzungsinformationen vom PCRF-Server abgerufen werden. Wenn kein Standardabonnentenprofil konfiguriert ist, wird ein UNDEF für Ausdrücke ausgelöst, die Abonnentenattribute verwenden.

requestTimeout

Zeit in Sekunden, innerhalb der die Gx CCR-Anforderung abgeschlossen werden muss. Wenn die Anforderung nicht innerhalb dieses Zeitraums abgeschlossen wird, wird die Anforderung für die Anzahl der im Parameter RequestRetryAttempts angegebenen Zeiten erneut übertragen. Wenn die Anforderung auch nach der erneuten Übertragung nicht abgeschlossen ist, wird das Standardabonnentenprofil auf diesen Abonnenten angewendet. Wenn kein Standardabonnentenprofil konfiguriert ist, wird ein UNDEF für Ausdrücke ausgelöst, die Abonnentenattribute verwenden. Null deaktiviert das Timeout. Standardwert: 10

requestRetryAttempts

Geben Sie an, wie oft eine Anforderung erneut übertragen werden muss, wenn die Anforderung nicht innerhalb des im Parameter RequestTimeout angegebenen Werts abgeschlossen wird. Standardwert: 3.

healthCheck

Setzen Sie auf Ja, um die Inline-Integritätsprüfung des Gx-Peers zu aktivieren. Wenn diese Option aktiviert ist, sendet Citrix ADC DWR-Pakete an den PCRF-Server. Wenn die Gx-Sitzung im Leerlauf ist, läuft der HealthCheck Timer ab und DWR-Pakete werden initiiert, um zu überprüfen, ob der PCRF-Server aktiv ist. Standardwert: Nein.
Hinweis: Dieser Parameter wird in Citrix ADC 12.1 Build 51.xx und höher unterstützt.

healthCheckTTL

Zeit in Sekunden für Watchdog Überwachung definiert. Nach Ablauf der TTL-Zeit für die Zustandsprüfung wird DWR gesendet, um den Status des PCRF-Servers zu überprüfen. Jede CCR-, CCA-, RAR- oder RAA-Nachricht setzt den Timer zurück.
Mindestwert: 6 Sekunden. Standardwert: 30 Sekunden.
Hinweis: Dieser Parameter wird in Citrix ADC 12.1 Build 51.xx und höher unterstützt.

cerRequestTimeout

Zeit in Sekunden für die Weiterübertragung des Capabilities Exchange Request definiert. Citrix ADC initiiert eine neue CER-Meldung, wenn innerhalb dieser konfigurierten Zeit kein CEA vom PCRF empfangen wird.
Wenn keine Antwort vom PCRF-Server empfangen wird, versucht die Appliance, die CER-Nachricht fünfmal zu senden. Wenn auch nach 5 CER-Nachrichten keine Antwort auftritt, schließt die Appliance die TCP-Verbindung und meldet einen Fehler. Wenn der Zeitüberschreitungswert auf 0 festgelegt ist, ist die Integritätsprüfung der Anwendung deaktiviert.

Mindestwert: 0 Sekunden. Standardwert: 0 Sekunden.
Hinweis: Dieser Parameter wird in Citrix ADC 12.1 Build 51.xx und höher unterstützt.

revalidationTimeout

Zeit, in Sekunden, nach der die Gx CCR-U-Anforderung nach einer PCRF-Aktivität in einer Sitzung gesendet wird. Jede RAR- oder CCA-Nachricht setzt den Timer zurück. Null-Wert deaktiviert das Leerlauf-Timeout.

negativeTTL

Zeit in Sekunden, nach der die Gx CCR-I-Anforderung für Sitzungen erneut gesendet wird, die nicht von PCRF aufgelöst wurden, weil der Server heruntergefahren ist oder keine Antwort vorliegt oder eine fehlgeschlagene Antwort empfangen wird. Anstatt den PCRF-Server ständig abzufragen, hält eine Negativ-TTL die Appliance an einer ungelösten Sitzung fest. Bei negativen Sitzungen erbt die Appliance die Attribute vom Standardabonnentenprofil, sofern eines konfiguriert ist, und von der RADIUS-Kontoführungsmeldung, sofern eines empfangen wird. Nullwert deaktiviert die negativen Sitzungen. Die Appliance installiert keine negativen Sitzungen, selbst wenn eine Teilnehmersitzung nicht abgerufen werden konnte. Standardwert: 600

negativeTTLLimitedSuccess

Setzen Sie auf Ja, um eine negative Sitzung für den Teilerfolgs-Antwortcode zu erstellen (2002). Wenn dieser Wert auf Nein gesetzt ist, wird eine reguläre Sitzung erstellt. Standardwert: Nein.

Dieser Parameter wird in Citrix ADC 12.1 Build 49.xx und höher unterstützt.

purgeSDBonGxFailure

Setzen Sie auf Ja, um die Teilnehmerdatenbank zu leeren, wenn die GX-Schnittstelle fehlschlägt. Der GX-Schnittstellenfehler umfasst sowohl DWR-Überwachung (falls aktiviert) als auch Netzwerk-HealthCheck (falls aktiviert). Wenn diese Option auf Ja festgelegt ist, werden alle Teilnehmersitzungen gelöscht.
Standardwert: Nein.
Hinweis: Dieser Parameter wird in Citrix ADC 12.1 Build 51.xx und höher unterstützt.

servicePathAVP

Der AVP-Code, in dem PCRF den für einen Abonnenten geltenden Dienstpfad sendet.

servicePathVendorid

Die Lieferanten-ID des AVP, in dem PCRF den für einen Abonnenten geltenden Dienstpfad sendet.

So konfigurieren Sie die GX-Schnittstelle mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Abonnent** > **Parameter**.
2. Klicken Sie auf **Abonnentenparameter konfigurieren**.
3. Wählen Sie unter Interface-Typ **GxOnly**aus.
4. Geben Sie die Werte für alle erforderlichen Parameter an.
5. Klicken Sie auf **OK**.

Erkennung von Transportfehlern über etablierte Gx-Verbindungen

Hinweis: Diese Funktion wird in Citrix ADC 12.1 Build 51.xx und höher unterstützt.

Eine Citrix ADC Appliance kann so konfiguriert werden, dass Transportfehler über etablierte Gx-Verbindungen mithilfe von DWR-Meldungen (Device Watchdog Request) und DWA (Device Watchdog answer) erkannt werden.

Nachdem eine Gx-Sitzung eingerichtet wurde, wird ein vordefinierter Timer ausgelöst, um festzustellen, ob eine Sitzung im Leerlauf ist. Eine DWR-Nachricht wird gesendet, nachdem der Leerlaufzeittimer abgelaufen ist. Der Leerlaufzeittimer wird jedes Mal zurückgesetzt, wenn die Citrix ADC Appliance eine Nachricht über eine etablierte Gx-Sitzung empfängt. Die Verfügbarkeit des Peers wird basierend auf der DWA-Nachricht bestätigt, nachdem eine DWR-Nachricht gesendet wurde.

- Wenn der DWA empfangen wird, wird die Verfügbarkeit eines Peers bestätigt und der Watchdog-Timer wird zurückgesetzt.
- Wenn der DWA nicht empfangen wird und der Watchdog-Zeitgeber zweimal hintereinander abläuft, wird die Sitzung als heruntergefahren und Peer nicht verfügbar angesehen. Die Appliance schließt die Sitzung und versucht, eine neue Sitzung mit dem Gx-Peer einzurichten.

Wenn der Watchdog-Zeitgeber zweimal ohne Antwort abläuft, betrachtet die Citrix ADC Appliance die GX-Verbindung als fehlerhaft und löst einen Verbindungsabschluss aus. Sobald die Verbindung geschlossen ist, wird keine andere Watchdog-Anfrage an den Gx-Peer gesendet. Citrix ADC Appliance verwendet die nächste verfügbare Gx-Sitzung für alle PCRF-Anforderungen.

So erkennen Sie Transportfehler über etablierte Gx-Verbindungen mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set subscriber gxInterface [-vServer <string>] [-service <string>] [-
    healthCheck ( YES | NO )] [-healthCheckTTL<positive_integer>][-
    cerRequestTimeout <positive_integer>] [-purgeSDBonGxFailure ( YES |
    NO )]
<!--NeedCopy-->
```

Beispiel:

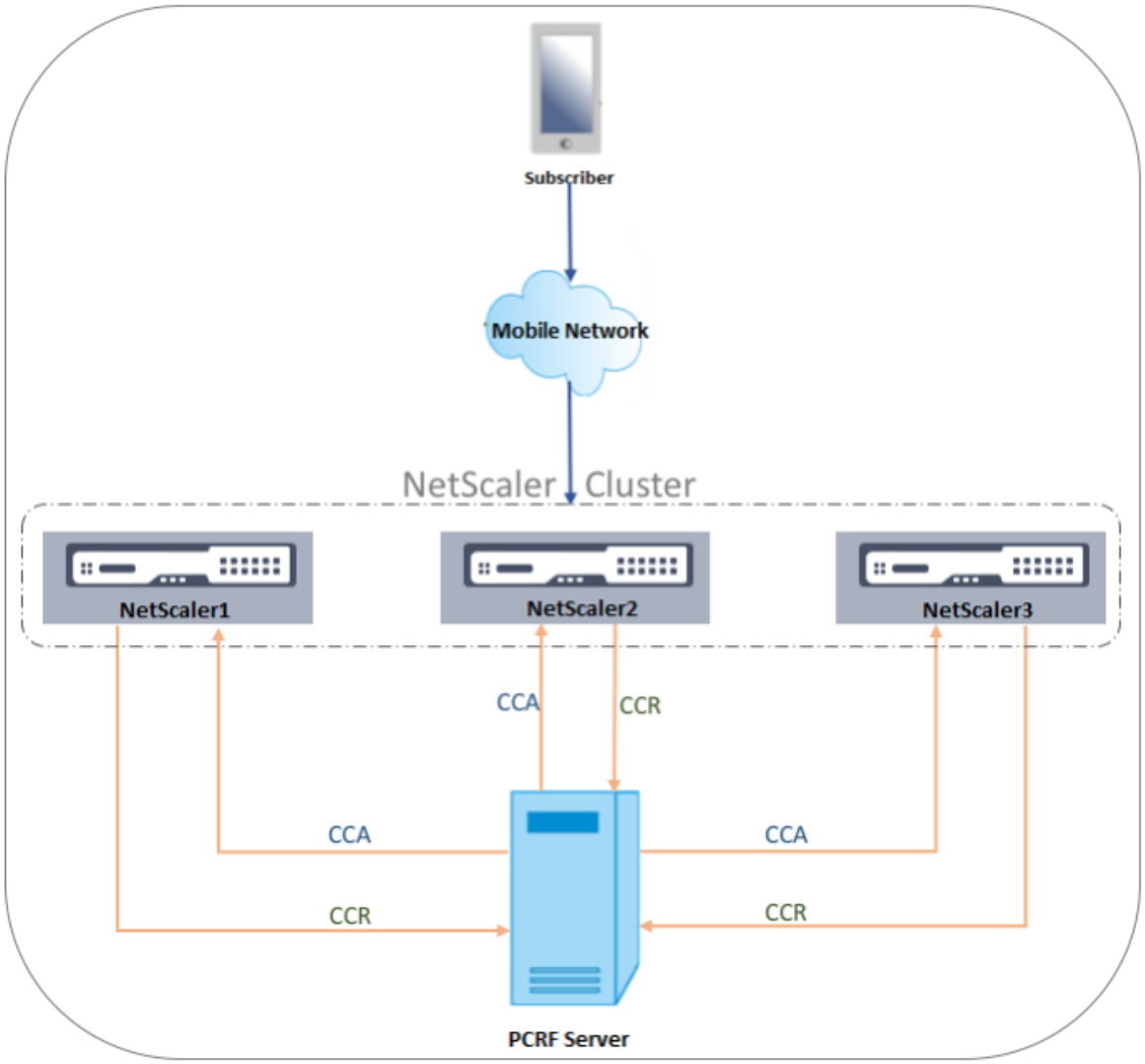
```
set subscriber gxInterface set subscriber gxInterface -vServer vdiam -
    healthCheck YES -healthCheckTTL 31 -cerRequestTimeout 15
    purgeSDBonGxFailure  YES
<!--NeedCopy-->
```

So erkennen Sie Transportfehler über etablierte Gx-Verbindungen mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Abonnent** > **Parameter**.
2. Klicken Sie auf **Abonnentenparameter konfigurieren**.
3. Wählen Sie unter **Interfacetyp GxOnly**aus.
4. Geben Sie die Werte für alle erforderlichen Parameter an.
5. Wählen Sie **Integritätsprüfung** und geben Sie Werte für **Integritätsprüfung TTL** und **CER Request Timeout** an.
6. Klicken Sie auf **OK**.

GX-Schnittstelle in einer Cluster-Topologie

Die Citrix ADC Appliance unterstützt die Gx-Schnittstelle in einer Cluster-Topologie.



Die Citrix ADC Knoten im Cluster kommunizieren über die Gx-Schnittstelle mit einem externen PCRF-Server. Wenn ein Knoten Clientdatenverkehr empfängt, führt die Appliance Folgendes aus:

- Sendet eine CCR-I-Anforderung an den PCRF-Server, um Teilnehmerinformationen abzurufen.
- Der PCRF-Server antwortet mit einem CCR-A.
- Der Citrix ADC Knoten speichert dann die empfangenen Abonnenteninformationen in seinem Abonnentenspeicher und wendet die Regeln auf den Clientdatenverkehr an.

Jeder Knoten verwaltet einen unabhängigen Abonnentenspeicher, und Abonnentensitzungen werden nicht mit anderen Knoten synchronisiert.

Gemäß dem Diameter Base Protocol RFC 6733 muss jeder Peer mit einer eindeutigen Diameter-Identität konfiguriert werden, um mit anderen Peers über das Diameter-Protokoll zu kommunizieren. Daher wird in einer Clusterbereitstellung die Konfiguration der Diameter-Identität entdeckt. Die Diameter-Parameter (Identität, Realm, Server Close Propagation) für jeden Knoten können individuell über die GUI oder die CLI konfiguriert werden.

Wenn ein Knoten zu einem Cluster hinzugefügt wird, nimmt er die Standard-Diameter-Parameter an (identity=netscaler.com, realm=com, serverClosePropogation=NO). Nachdem die Knoten hinzugefügt wurden, müssen die Diameter-Parameter für jeden Knoten konfiguriert werden.

So konfigurieren Sie die Diameter-Parameter mit der GUI

1. Navigieren Sie zu **System** > **Einstellungen**.
2. Klicken Sie im Detailbereich auf **Diameter-Parameter ändern**.
3. Wählen Sie auf der Seite Diameter-Parameter den Citrix ADC Knoten aus, für den Sie die Diameter-Parameter konfigurieren möchten, und klicken Sie dann auf **Konfigurieren**.
4. Konfigurieren Sie auf der Seite "Diameter-Parameter konfigurieren" den Durchmesser Identität, den Diameter-Bereich und den Server Close Propagation für den ausgewählten Knoten.
5. Klicken Sie auf **OK**.

So konfigurieren Sie die Diameter-Parameter mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns diameter [-identity <string>] [-ownerNode <positive_integer>]
<!--NeedCopy-->
```

ARGUMENTS

Identität

Diameter Identity wird verwendet, um einen Diameter Knoten eindeutig zu identifizieren. Bevor Sie die Durchmesserkonfiguration einrichten, muss der Citrix ADC Appliance (als Diameter Knoten) eine eindeutige Durchmesseridentität zugewiesen werden.

Legen Sie beispielsweise ns diameter -identity netscaler.com -ownerNode 1 fest. Also, wenn Citrix ADC-System Identität in Durchmessermeldungen verwenden muss, verwendet es 'netscaler.com' als Origin-Host AVP, wie in RFC3588 definiert.

Maximale Länge: 255

OwnerNode

OwnerNode stellt die ID des Clusterknotens dar, für den die Durchmesser-ID festgelegt ist. OwnerNode kann nur über CLIP konfiguriert werden.

Mindestwert: 0

Maximalwert: 31

Beispiel:

set ns diameter -identity netscaler1.com -ownerNode 1

Hinweis:

Die Option OwnerNode wird auch dem Befehl show ns diameter hinzugefügt.

Beispiel:

```
show diameter -ownerNode <0-31>
<!--NeedCopy-->
```

Wenn der Befehl show ns diameter ausgeführt wird, zeigt er die Diameter-Parameter für einen bestimmten Knoten an.

So konfigurieren Sie eine GX-Schnittstelle für die Clusterbereitstellung

Führen Sie die folgenden Aufgaben aus, um eine GX-Schnittstelle einzurichten:

Fügen Sie für jede Gx-Schnittstelle einen DIAMETER-Dienst hinzu.

Beispiel:

```
add service pcrf-svc1 203.0.113.1 DIAMETER 3868
add service pcrf-svc2 203.0.113.2 DIAMETER 3868
<!--NeedCopy-->
```

Fügen Sie einen virtuellen DIAMETER-Load Balancing Server hinzu, und binden Sie die in Schritt 1 erstellten Dienste an diesen virtuellen Server.

Beispiel:

```
add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
    persistAVPno 263

bind lb vserver vdiam pcrf-svc1

bind lb vserver vdiam pcrf-svc2
<!--NeedCopy-->
```


Konfigurieren Sie Citrix ADC Durchmesseridentität und Realm auf allen Clusterknoten. Identität und Realm werden als Origin-Host- und Origin-Realm-AVPs in Durchmessermeldungen verwendet, die vom Gx-Client gesendet werden.

Beispiel:

```
set ns diameter -identity node0.netscaler.com -realm netscaler.com -
    ownerNode 0

set ns diameter -identity node1.netscaler.com -realm netscaler.com -
    ownerNode 1
<!--NeedCopy-->
```

Konfigurieren Sie die GX-Schnittstelle, um den in Schritt 2 erstellten virtuellen Server als virtuellen PCRF-Server zu verwenden, und legen Sie auch den PCRF-Realm fest.

Beispiel:

```
set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf.com

Set the subscriber interface type to GxOnly.
<!--NeedCopy-->
```

Beispiel:

```
set subscriber param -interfaceType GxOnly
<!--NeedCopy-->
```

Geben Sie Folgendes ein, um die Konfiguration und den Status der GX-Schnittstelle anzuzeigen:

```
show subscriber gxinterface
<!--NeedCopy-->
```

RADIUS-Schnittstelle

Bei einer RADIUS-Schnittstelle leitet das Paketgateway die Teilnehmerinformationen in einer RADIUS-Accounting Start-Nachricht über die RADIUS-Schnittstelle an die Appliance weiter, wenn eine IP-CAN-Sitzung eingerichtet wird. Ein Dienst vom Typ RadiusListener verarbeitet RADIUS-Buchhaltungsnachrichten. Fügen Sie einen gemeinsamen Schlüssel für den RADIUS-Client hinzu.

Wenn ein freigegebener Schlüssel nicht konfiguriert ist, wird die RADIUS-Nachricht im Hintergrund gelöscht. Das folgende Beispiel zeigt die Befehle zum Konfigurieren einer RADIUS-Schnittstelle. Die Befehle sind fett.

So richten Sie eine RADIUS-Schnittstelle ein:

Erstellen Sie einen RADIUS-Listener-Dienst an der SNIP-Adresse, an der die RADIUS-Nachrichten empfangen werden. Beispiel:

```
1 add service srad1 192.0.0.206 RADIUSLISTENER 1813
2 <!--NeedCopy-->
```

Konfigurieren Sie die RADIUS-Schnittstelle des Abonnenten für die Verwendung dieses Dienstes. Beispiel:

```
1 set subscriber radiusInterface -listeningService srad1
2 <!--NeedCopy-->
```

Legen Sie den Abonnentenschnittstellentyp auf RadiusOnly fest. Beispiel:

```
1 set subscriber param -interfaceType RadiusOnly
2 <!--NeedCopy-->
```

Fügen Sie einen RADIUS-Client hinzu, der ein Subnetz und einen gemeinsamen Schlüssel angibt. Beispiel:

```
1 add radius client 192.0.2.0/24 -radkey client123
2 <!--NeedCopy-->
```

Ein Subnetz von 0.0.0.0/0 bedeutet, dass es der Standardgeheimnis für alle Clients ist. Geben Sie Folgendes ein, um die Konfiguration und den Status der RADIUS-Schnittstelle anzuzeigen:

```
1 show subscriber radiusInterface
2 <!--NeedCopy-->
```

RADIUS-Schnittstellenparameter:

Radius-Listener-Dienst: srad1 (UP)

Fertig

Beispiel:

```
add service pcrf-svc1 203.0.113.1 DIAMETER 3868

add service pcrf-svc2 203.0.113.2 DIAMETER 3868
<!--NeedCopy-->
```

ARGUMENTS

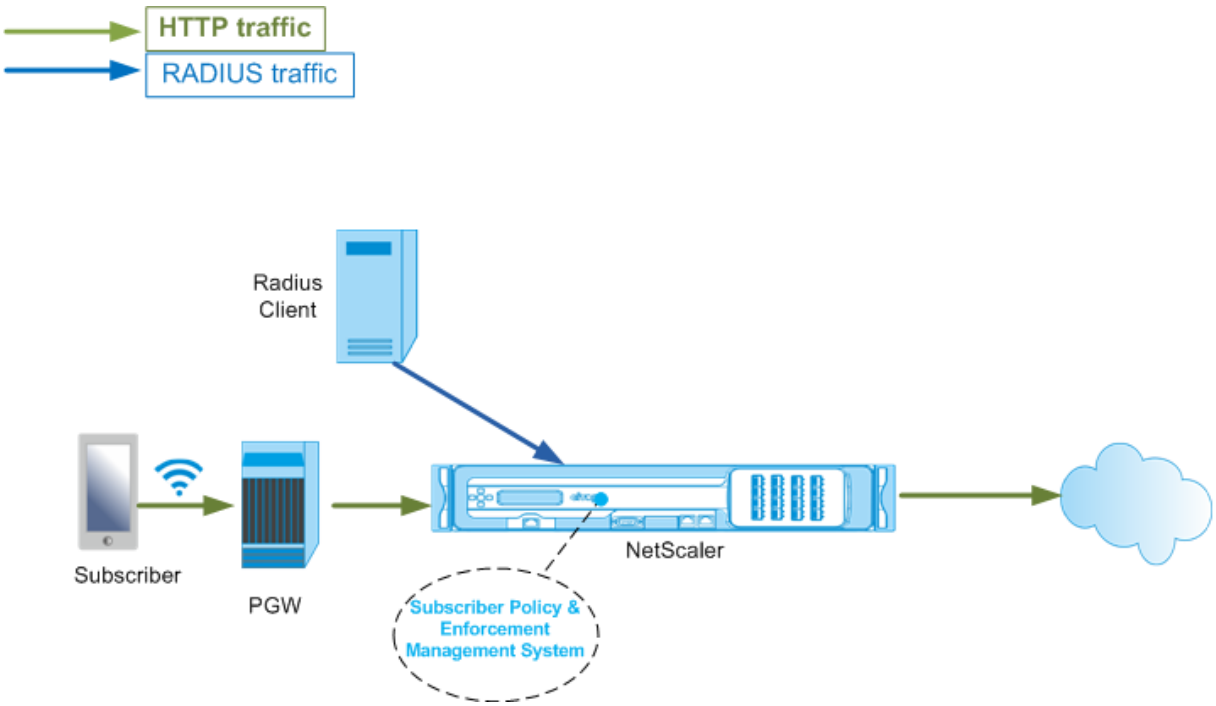
ListeningService

Name des RADIUS-Listening-Dienstes, der die RADIUS-Kontoführungsanforderungen verarbeitet.

SVRState

Der Status des RADIUS-Listening-Dienstes.

Die folgende Abbildung zeigt den Datenfluss auf hoher Ebene.



So konfigurieren Sie die RadiusOnly-Schnittstelle mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Abonnent** > **Parameter**.

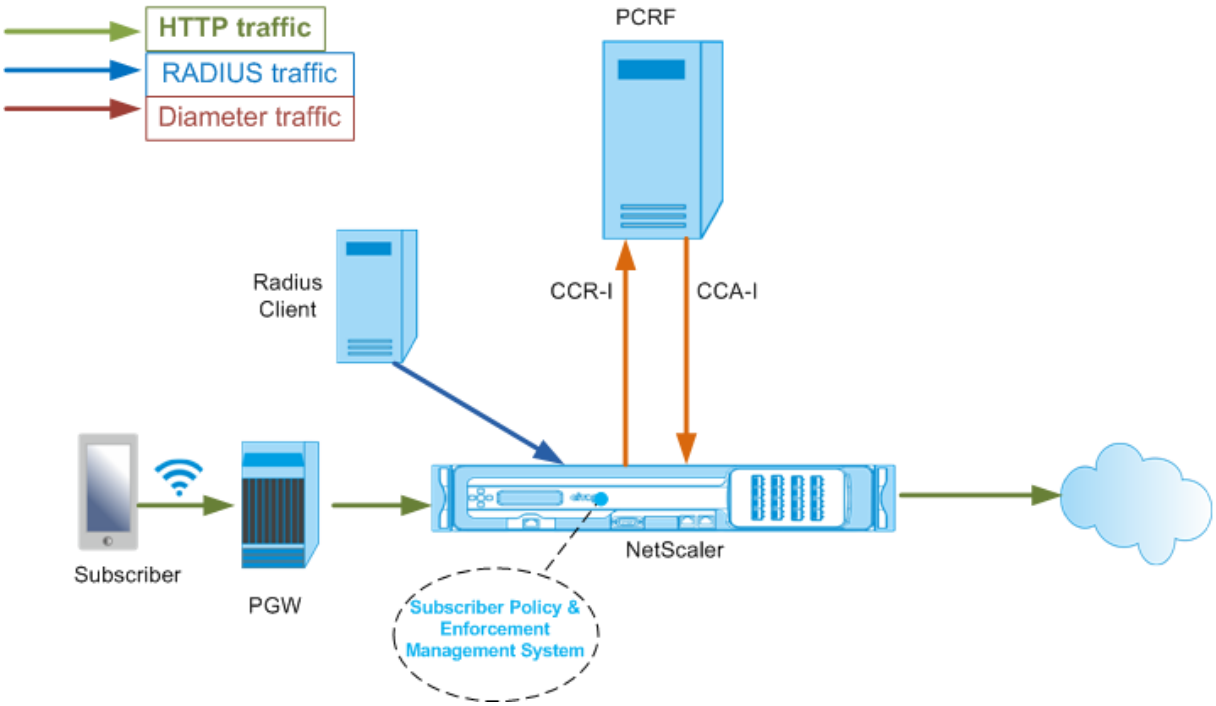
2. Klicken Sie auf **Abonnentenparameter konfigurieren**.
3. Wählen Sie unter Schnittstellentyp die Option **RadiusOnly**aus.
4. Geben Sie die Werte für alle erforderlichen Parameter an.
5. Klicken Sie auf **OK**.

RADIUS- und GX-Schnittstelle

Bei einer RADIUS- und GX-Schnittstelle leitet das Paketgateway bei der Einrichtung einer IP-CAN-Sitzung die Teilnehmer-ID wie MSISDN und Framed-IP-Adressinformationen über den Abonnenten der Appliance über die RADIUS-Schnittstelle weiter. Die Appliance verwendet diese Teilnehmer-ID, um die PCRF auf der Gx-Schnittstelle abzufragen, um die Teilnehmerinformationen abzurufen. Dies wird als primäre PCEF-Funktionalität bezeichnet. Das folgende Beispiel zeigt die Befehle zum Konfigurieren einer RADIUS- und GX-Schnittstelle.

```
1 set subscriber param -interfaceType RadiusandGx
2 add service pcrf-svc 203.0.113.1 DIAMETER 3868
3 add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
     persistAVPno 263
4 bind lb vserver vdiam pcrf-svc
5 set subscriber gxInterface -vServer vdiam -pcrfRealm testrealm1.net -
     holdOnSubscriberAbsence YES -revalidationTimeout 60 -negativeTTL 120
6 add service srad1 192.0.0.206 RADIUSLISTENER 1813    set subscriber
     radiusInterface -listeningService srad1
7 <!--NeedCopy-->
```

Die folgende Abbildung zeigt den Datenfluss auf hoher Ebene.



So konfigurieren Sie die RadiusAndGX-Schnittstelle mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Abonnent** > **Parameter**.
2. Klicken Sie auf **Abonnentenparameter konfigurieren**.
3. Wählen Sie unter Schnittstellentyp die Option **RadiusAndGX** aus.
4. Geben Sie die Werte für alle erforderlichen Parameter an.
5. Klicken Sie auf **OK**.

Statische Abonnenten konfigurieren

Sie können die Abonnenten manuell auf der Citrix ADC Appliance mit der Befehlszeile oder des Konfigurationsdienstprogramms konfigurieren. Sie erstellen statische Abonnenten, indem Sie eine eindeutige Abonnenten-ID zuweisen und optional jedem Abonnenten eine Richtlinie zuweisen. Die folgenden Beispiele zeigen die Befehle zum Konfigurieren eines statischen Teilnehmers.

In den folgenden Beispielen gibt **SubscriptionIdValue** die internationale Telefonnummer an, und **SubscriptionIdType** (in diesem Beispiel E164) gibt das allgemeine Format für internationale Telefonnummern an.

```
1    add subscriber profile 203.0.113.6 -subscriberRules policy1 policy2
         -subscriptionIdType E164 -subscriptionIdvalue 98767543211
```



```
2     add subscriber profile 2002::a66:e8d3/64 -subscriberRules policy1
         policy3 -subscriptionIdtype E164 -subscriptionIdvalue
         98767543212
3     add subscriber profile 203.0.24.2 10 -subscriberRules policy2
         policy3 -subscriptionIdtype E164 -subscriptionIdvalue
         98767543213
4  <!--NeedCopy-->
```

Um die konfigurierten Abonnentenprofile anzuzeigen, geben Sie Folgendes ein:

> Abonnentenprofil anzeigen

```
1     > show subscriber profile
2
3     1)  Subscriber IP: 203.0.24.2 VLAN:10
4         Profile Attributes:
5                 Active Rules: policy2, policy3
6                 Subscriber Id Type: E164
7                 Subscriber Id Value: 98767543213
8     2)  Subscriber IP: 2002::/64
9         Profile Attributes:
10                Active Rules: policy1, policy3
11                Subscriber Id Type: E164
12                Subscriber Id Value: 98767543212
13    3)  Subscriber IP: 203.0.113.6
14        Profile Attributes:
15                Active Rules: policy1, policy2
16                Subscriber Id Type: E164
17                Subscriber Id Value: 98767543211
18
19     Done
20 <!--NeedCopy-->
```

Standardabonnentenprofil

Ein Standardabonnentenprofil wird verwendet, wenn die AbonnentenIP-Adresse nicht im Abonnentensitzungsspeicher auf der Appliance gefunden wird. Im folgenden Beispiel wird ein Standardabonnentenprofil mit der Abonnentenregelrichtlinien1 hinzugefügt.

```
1     > add subscriber profile * -subscriberRules policy1
2  <!--NeedCopy-->
```


Abonnentensitzungen anzeigen und löschen

Verwenden Sie den folgenden Befehl, um alle statischen und dynamischen Teilnehmersitzungen anzuzeigen.

> show subscriber sessions

```
    > show subscriber sessions
    1)  Subscriber IP: 2002::/64
        Session Attributes:
                Active Rules: policy1, policy3
                Subscriber Id Type: E164
                Subscriber Id Value: 98767543212
    2)  Subscriber IP: *
        Session Attributes:
                Active Rules: policy1
    3)  Subscriber IP: 203.0.24.2 VLAN:10
        Session Attributes:
                Active Rules: policy2, policy3
                Subscriber Id Type: E164
                Subscriber Id Value: 98767543213
    4)  Subscriber IP: 203.0.113.6
        Session Attributes:
                Active Rules: policy1, policy2
                Subscriber Id Type: E164
                Subscriber Id Value: 98767543211
    5)  Subscriber IP: 192.168.0.11
        Session Attributes:
                Idle TTL remaining: 361 Seconds
                Active Rules: policy1
                Subscriber Id Type: E164
                Subscriber Id Value: 1234567811
                Service Path: policy1
                AVP(44): 34 44 32 42 42 38 41 43  2D 30 30 30 30 30 30
                   31 31
                AVP(257): 00 01 C0 A8 0A 02
                PCRF-Host: host.pcrf.com
                AVP(280): 74 65 73 74 2E 63 6F 6D

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

Verwenden Sie den folgenden Befehl, um eine einzelne Sitzung oder den gesamten Sitzungsspeicher zu löschen. Wenn Sie keine IP-Adresse angeben, wird der vollständige Abonnenten-Sitzungsspeicher

gelöscht.

```
clear subscriber sessions <ip>
<!--NeedCopy-->
```

Durchsetzung von Abonnentenrichtlinien und -verwaltungssystem

Die Citrix ADC Appliance verwendet die IP-Adresse des Abonnenten als Schlüssel für das Durchsetzungs- und Verwaltungssystem der Abonnentenrichtlinien.

Sie können Abonnentenausdrücke hinzufügen, um die Abonnenteninformationen zu lesen, die im Erzwingungs- und Verwaltungssystem für Abonnentenrichtlinien verfügbar sind. Diese Ausdrücke können mit Richtlinienregeln und -aktionen verwendet werden, die für Citrix ADC Features konfiguriert sind, z. B. integriertes Caching, Rewrite, Responder und Content Switching.

Die folgenden Befehle sind ein Beispiel für das Hinzufügen einer abonnentenbasierten Responderaktion und -richtlinie. Die Richtlinie wird auf true ausgewertet, wenn der Abonnentenregelwert pol1 lautet.

```
    add responder action error_msg respondwith '"HTTP/1.1 403 OKrnrn" +
        " You are  not authorized to access Internet"'
    add responder policy no_internet_access "SUBSCRIBER.RULE_ACTIVE("
       pol1")" error_msg
<!--NeedCopy-->
```

Das folgende Beispiel zeigt die Befehle zum Hinzufügen einer abonnentenbasierten Umschreibaktion und -richtlinie. Die Aktion fügt einen HTTP-Header X-nokia-msisdn ein, indem der Wert von AVP (45) in der Teilnehmersitzung verwendet wird.

```
    > add rewrite action AddHDR-act insert_http_header X-Nokia-MSISDN "
       SUBSCRIBER.AVP(45).VALUE"
    > add rewrite policy AddHDR-pol "HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.
       URL).EQUALS_ANY("patset-test")" AddHDR-act
<!--NeedCopy-->
```

Im folgenden Beispiel werden zwei Richtlinien auf der Appliance konfiguriert. Wenn die Appliance die Abonnenteninformationen überprüft und die Abonnentenregel cache_enable lautet, führt sie Zwischenspeicherung durch. Wenn die Abonnentenregel cache_disable lautet, führt die Appliance kein Zwischenspeichern durch.


```
1      > add cache policy nocachepol -rule "SUBSCRIBER.RULE_ACTIVE("
          cache_disable")" - action NOCACHE
2      > add cache policy cachepol -rule "SUBSCRIBER.RULE_ACTIVE("
          cache_enable")" - action CACHE -storeInGroup cg1
3  <!--NeedCopy-->
```

Eine vollständige Liste der Ausdrücke, die mit SUBSCRIBER beginnen, finden Sie im Richtlinienkonfigurationshandbuch.

> **Wichtige**
>
> Citrix ADC-Softwareversion 12.1 unterstützt die IPANDVLAN-Schlüsselsuchmethode, wenn die Abonnentenschnittstelle auf GXOnly festgelegt ist. Weitere Informationen finden Sie unter Nachschlagmethode für IP-Adresse und VLAN-ID-Schlüssel.

IPv6-Präfix-basierte Teilnehmersitzungen

Ein Telco-Benutzer wird durch das IPv6-Präfix und nicht durch die vollständige IPv6-Adresse identifiziert. Die Citrix ADC Appliance verwendet nun das Präfix anstelle der vollständigen IPv6-Adresse (/128), um einen Abonnenten in der Datenbank (Abonnentenspeicher) zu identifizieren. Für die Kommunikation mit dem PCRF-Server (z. B. in einer CCR-I-Nachricht) verwendet die Appliance nun das Framed-IPv6-Präfix AVP anstelle der vollständigen IPv6-Adresse. Die Standardlänge des Präfix ist /64, Sie können die Appliance jedoch so konfigurieren, dass sie einen anderen Wert verwendet.

So konfigurieren Sie das IPv6-Präfix mit der Befehlszeile

```
set subscriber param [-ipv6PrefixLookupList <positive_integer> ...]
```

Der erste Beispielbefehl unten setzt ein einzelnes Präfix und der zweite Beispielbefehl setzt mehrere Präfixe.

```
1      set subscriber param -ipv6PrefixLookupList 64
2      set subscriber param -ipv6PrefixLookupList 64 72 96
3  <!--NeedCopy-->
```

So konfigurieren Sie das IPv6-Präfix mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **Abonnent** > **Parameter**.
2. Klicken Sie im Detailbereich unter **Einstellungen** auf **Subscriber Parameter konfigurieren**, und geben Sie in der **IPv6-Präfix Lookupliste**ein oder mehrere Präfixe an.

IP-Adresse und VLAN-ID-Schlüssel-Suchmethode

Die Citrix ADC Appliance verwendet die IP-Adresse des Abonnenten als Schlüsselsuchmethode für das Durchsetzungs- und Verwaltungssystem der Abonnentenrichtlinien. Diese Methode ist nicht wirksam, wenn sich die IP-Adressen überlappen. In solchen Fällen können Sie die VLAN-ID als zusätzlichen Subscriber Lookup-Typ verwenden. Die IPANDVLAN-Schlüsselsuchmethode wird nur unterstützt, wenn die Teilnehmerschnittstelle auf GXOnly festgelegt ist. Wenn IPANDVLAN als Suchmethode konfiguriert ist, führt die Citrix ADC Appliance Folgendes aus:

- Schließt die ursprüngliche VLAN-ID in die GX-Abfrage für IPv4-Abonnenten ein.
- Enthält den Gx VLAN AVP in allen Gx-Antworten. Wenn jedoch eine VLAN-ID nicht übereinstimmt, ignoriert die Appliance die Antworten.

Wenn die Appliance beispielsweise ein CCR-I mit GXSessionid-a:IPv4-b:vlan-c sendet und die Antwort GXSessionid-a:IPv4-b:vlan-d enthält, wird die Antwort gelöscht, und ein Standardabonnenteneintrag wird erstellt.

> **Hinweis:**
>
> - Schnittstellentyp RadiusAndGX und RadiusOnly können nicht zusammen mit dem Schlüsseltyp IPANDVLAN konfiguriert werden.
> - Wenn der Datenverkehr von einer IPv6-Adresse stammt, verwendet die Citrix ADC Appliance die IP-Lookup-Methode.

So konfigurieren Sie IP oder IPANDVLAN als Schlüsselsuchmethode mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set subscriber param [-keytype ( IP | IPANDVLAN )] [-interfaceType <
   interfaceType>]
<!--NeedCopy-->
```

Beispiel:

```
set subscriber param -keytype IPANDVLAN -interfaceType GxOnly

set subscriber param -keytype IP -interfaceType GxOnly
<!--NeedCopy-->
```

> **Hinweis:**
>
> Ändern des Schlüsseltype-Parameters von IP in IPANDVLAN und umgekehrt löscht alle Teil-

> nehmerdaten.

VLAN-Parameter

Der VLAN-Parameter wird auch für die folgenden Befehle hinzugefügt.

```
add subscriber profile <ip>@ [-vlan]

set subscriber profile <ip>@ [-vlan] [-subscriptionIdType  <
   subscriptionIdType>]

show subscriber profile [<ip>@] [-vlan]

rm subscriber profile <ip>@ [-vlan <positive_integer>]
<!--NeedCopy-->
```

Argumente

IP

Stellt die IP-Adresse des Teilnehmers dar. Dies ist ein obligatorisches Argument und kann nicht geändert werden, nachdem das Abonnentenprofil hinzugefügt wurde.

Vlan

Stellt die VLAN-Nummer dar, auf der sich der Abonnent befindet. Die VLAN-Nummer kann nicht geändert werden, nachdem das Teilnehmerprofil hinzugefügt wurde.

Mindestwert: 1

Maximalwert: 4096

```
add subscriber profile 192.0.2.23 10

set subscriber profile 192.0.2.23 10 -subscriptionIdtype E164

show subscriber profile 192.0.2.23 10

rm subscriber profile 192.0.2.23 10

<!--NeedCopy-->
```


So konfigurieren Sie IP oder IPANDVLAN als Schlüsselsuchmethode über die GUI

1. Navigieren Sie zu **Traffic Management** > **Abonnent** > **Parameter.**
2. Klicken Sie auf **Abonnentenparameter konfigurieren.**
3. Wählen Sie unter **Schlüsseltyp** die Option **IP** oder **IPANDVLAN** entsprechend Ihren Anforderungen aus.
4. Schließen Sie die Konfiguration ab, und klicken Sie auf **OK**.

Leerlaufsitzungsverwaltung von Teilnehmersitzungen in einem Telco-Netzwerk

Die Abonnentensitzung auf einer Citrix ADC Appliance basiert auf Ereignissen der Steuerungsebene, wie z. B. einer RADIUS-Accounting Stop Nachricht, einer Durchmesser-RAR-Meldung (Session Release) oder einem Befehl Abonnentensitzung löschen. In einigen Bereitstellungen erreichen die Nachrichten von einem RADIUS-Client oder einem PCRF-Server möglicherweise nicht die Appliance. Außerdem können die Nachrichten bei starkem Datenverkehr verloren gehen. Eine lange Zeit im Leerlauf befindlichen Teilnehmersitzung verbraucht weiterhin Arbeitsspeicher und IP-Ressourcen auf der Citrix ADC Appliance. Die Leerlaufsitzungsverwaltungsfunktion stellt konfigurierbare Zeitgeber zur Identifizierung von Leerlaufsitzungen bereit und bereinigt diese Sitzungen basierend auf der angegebenen Aktion.

Eine Sitzung gilt als Leerlauf, wenn kein Datenverkehr von diesem Teilnehmer auf der Datenebene oder der Steuerebene empfangen wird. Sie können eine Aktualisierung angeben, beenden (PCRF informieren und dann die Sitzung löschen) oder löschen (ohne PCRF zu informieren) Aktion. Die Aktion wird erst ausgeführt, nachdem die Sitzung für die im Leerlaufzeitparameter angegebene Zeit inaktiv ist.

So konfigurieren Sie das Zeitlimit für Leerlaufsitzungen und die zugehörige Aktion mit der Befehlszeile

```
set subscriber param [-idleTTL <positive_integer>] [-idleAction <
   idleAction>]
<!--NeedCopy-->
```

Beispiele:

```
set subscriber param -idleTTL 3600 -idleAction ccrTerminate

set subscriber param -idleTTL 3600 -idleAction ccrUpdate

set subscriber param -idleTTL 3600 -idleAction delete
<!--NeedCopy-->
```


Um das Timeout für Leerlaufsitzungen zu deaktivieren, setzen Sie das Leerlaufzeitlimit auf Null.

set subscriber param –idleTTL 0

So konfigurieren Sie das Zeitlimit für Leerlaufsitzungen und die zugehörige Aktion mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **Abonnent** > **Parameter**.
2. Klicken Sie im Detailbereich unter **Einstellungen** auf **Subscriber Parameters konfigurieren**, und geben Sie eine **Leerlaufzeit** und **Leerlaufaktion** an.

Protokollierung von Abonnentensitzungsereignissen

Wenn Sie die Abonnentenprotokollierung aktivieren, können Sie die für einen Abonnenten spezifischen RADIUS- und Gx-Steuerebenenmeldungen verfolgen und die historischen Daten verwenden, um Teilnehmeraktivitäten zu analysieren. Einige der wichtigsten Attribute sind MSISDN und Zeitstempel. Folgende Attribute werden ebenfalls protokolliert:

- Sitzungsereignis (Installieren, Aktualisieren, Löschen, Fehler)
- GX-Meldungstyp (CCR-I, CCR-U, CCR-T, RAR)
- Radius-Meldungstyp (Start, Stop)
- Teilnehmer-IP
- SubscriberID-Typ (MSISDN(E164), IMSI)
- SubscriberID-Wert

Mithilfe dieser Protokolle können Sie Benutzer nach IP-Adresse und, falls verfügbar, MSISDN verfolgen.

Sie können die Protokollierung der Abonnentensitzungen auf einem lokalen oder entfernten Syslog- oder Nslog-Server aktivieren. Das folgende Beispiel zeigt, wie Sie die Abonnentenprotokollierung auf einem Remote-Syslog-Server aktivieren.

```
1     > add syslogAction sysact1 192.0.2.0 -loglevel EMERGENCY ALERT
         CRITICAL ERROR WARNING NOTICE INFORMATIONAL -subscriberlog
         enabled
2  <!--NeedCopy-->
```

Aus diesen Protokollen können Sie Informationen zu allen Aktivitäten im Zusammenhang mit einem Benutzer erhalten, z. B. zu dem Zeitpunkt, zu dem eine Sitzung aktualisiert, gelöscht oder erstellt (installiert) wurde. Darüber hinaus werden Fehlermeldungen protokolliert.

Beispiele:

1. Die folgenden Protokolleinträge sind Beispiele für die Erstellung von RadiusAndGX-Sitzungen, die Sitzungsaktualisierung und das Löschen von Sitzungen.

   > 09/30/2015:16:29:18 GMT Informational 0-PPE-0 : default SUBSCRIBER SESSION_EVENT 147 0 : Session Install, GX MsgType: CCR-I, RADIUS MsgType: Start, IP: 100.10.1.1, ID: E164 - 30000000001
   >
   > 09/30/2015:16:30:18 GMT Informational 0-PPE-0 : default SUBSCRIBER SESSION_EVENT 148 0 : Session Update, GX MsgType: CCR-U, IP: 100.10.1.1, ID: E164 - 30000000001
   >
   > 09/30/2015:17:27:56 GMT Informational 0-PPE-0 : default SUBSCRIBER SESSION_EVENT 185 0 : Session Delete, GX MsgType: CCR-T, RADIUS MsgType: Stop, IP: 100.10.1.1, ID: E164 - 30000000001

2. Die folgenden Protokolleinträge sind Beispiele für Fehlermeldungen, z. B. wenn ein Abonnent auf dem PCRF-Server nicht gefunden wird und wenn die Appliance keine Verbindung mit dem PCRF-Server herstellen kann.

   > 09/30/2015:16:44:15 GMT Error 0-PPE-0 : default SUBSCRIBER SESSION_FAILURE 169 0 : Failure Reason: PCRF failure response, GX MsgType: CCR-I, IP: 100.10.1.1
   >
   > Sep 30 13:03:01 09/30/2015:16:49:08 GMT 0-PPE-0 : default SUBSCRIBER SESSION_FAILURE 176 0 : Failure Reason: Unable to connect to PCRF, GX MsgType: CCR-I, RADIUS MsgType: Start, IP: 100.10.1.1, ID: E164 - 30000000001#000#000#000#000#000#000#000#000#000#000#000#000#

Abonnentenbewusste LSN-Sitzungsbeendigung

Wenn in früheren Versionen eine Abonnentensitzung gelöscht wird, wenn eine RADIUS-Buchhaltungs-STOP oder eine PCRF-RAR-Nachricht empfangen wird, oder als Ergebnis eines anderen Ereignisses, wie TTL-Ablauf oder Leerung, werden die entsprechenden LSN-Sitzungen des Abonnenten erst nach dem konfigurierten LSN-Zeitüberschreitungszeitraum entfernt. LSN-Sitzungen, die bis zum Ablauf dieser Zeitüberschreitung geöffnet bleiben, verbrauchen weiterhin Ressourcen auf der Appliance.

Ab Release 11.1 wird ein neuer Parameter (subscrSessionRemoval) hinzugefügt. Wenn dieser Parameter aktiviert ist und die Abonnenteninformationen aus der Abonnentendatenbank gelöscht werden, werden LSN-Sitzungen, die diesem Abonnenten entsprechen, ebenfalls entfernt. Wenn dieser Parameter deaktiviert ist, wird die Zeitüberschreitung für die Teilnehmersitzungen gemäß den LSN-Zeitüberschreitungseinstellungen festgelegt.

So konfigurieren Sie die abonnentenunterstützende LSN-Sitzungsbeendigung mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set lsn parameter -subscrSessionRemoval (          DISABLED )
ENABLED
```

```
1      > set lsn parameter -subscrSessionRemoval ENABLED
2      Done
3      > sh lsn parameter
4                  LSN Global Configuration:
5
6                  Active Memory Usage: 0 MBytes
7                  Configured Memory Limit: 0 MBytes
8                  Maximum Memory Usage Limit: 912 MBytes
9                  Session synchronization: ENABLED
10                 Subscriber aware session removal: ENABLED
11 <!--NeedCopy-->
```

So konfigurieren Sie die abonnentenunterstützende LSN-Sitzungsbeendigung mit der GUI

1. Navigieren Sie zu **System** > **Large Scale NAT**.
2. Klicken Sie unter **Erste Schritte**auf **LSN-Parameter festlegen**.
3. Legen Sie den **Parameter Abonnentenunterstützung fest**.

Problembehandlung

Wenn Ihre Bereitstellung nicht wie erwartet funktioniert, verwenden Sie die folgenden Befehle zur Fehlerbehebung:

- show subscriber gxinterface Die Ausgabe
  dieses Befehls kann folgende Fehlermeldungen enthalten (hier mit vorgeschlagenen Antworten):
  - Gx Interface Not Configured-Verwenden Sie set subscriber param Befehl, um den richtigen Schnittstellentyp zu konfigurieren.
  - PCRF nicht konfiguriert-Konfigurieren eines Diameter vServer oder Service auf GxInterface-Verwenden Sie den Befehl set subscriber gx interface, um dieser Schnittstelle einen virtuellen Diameter Server oder Dienst zuzuweisen.
  - PCRF ist nicht bereit, den entsprechenden vserver/service für weitere Details zu überprüfen. Verwenden Sie den Befehl show LB vserver oder show service, um den Status des Dienstes zu überprüfen.

  - Citrix ADC wartet auf CEA von PCRF-fähigkeitsaushandlungen zwischen PCRF und Citrix ADC möglicherweise fehlschlägt. Dies könnte ein intermittierender Zustand sein. Wenn es weiterhin besteht, überprüfen Sie die DIAMETER-Einstellungen auf Ihrem PCRF-Server.
  - Speicher ist nicht zum Speichern von Teilnehmersitzungen konfiguriert. Bitte verwenden Sie 'set extendedmemoryparam -memlimit <>'-Verwenden Sie den Befehl set extendedmemoryparam, um erweiterten Speicher zu konfigurieren.
- show subscriber radiusinterface
  Wenn "Nicht konfiguriert" die Ausgabe dieses Befehls ist, verwenden Sie den Befehl set subscriber radiusinterface, um einen RadiusListener Dienst anzugeben.

Wenn die Abonnentenprotokollierung aktiviert ist, können Sie detailliertere Informationen aus den Protokolldateien abrufen.

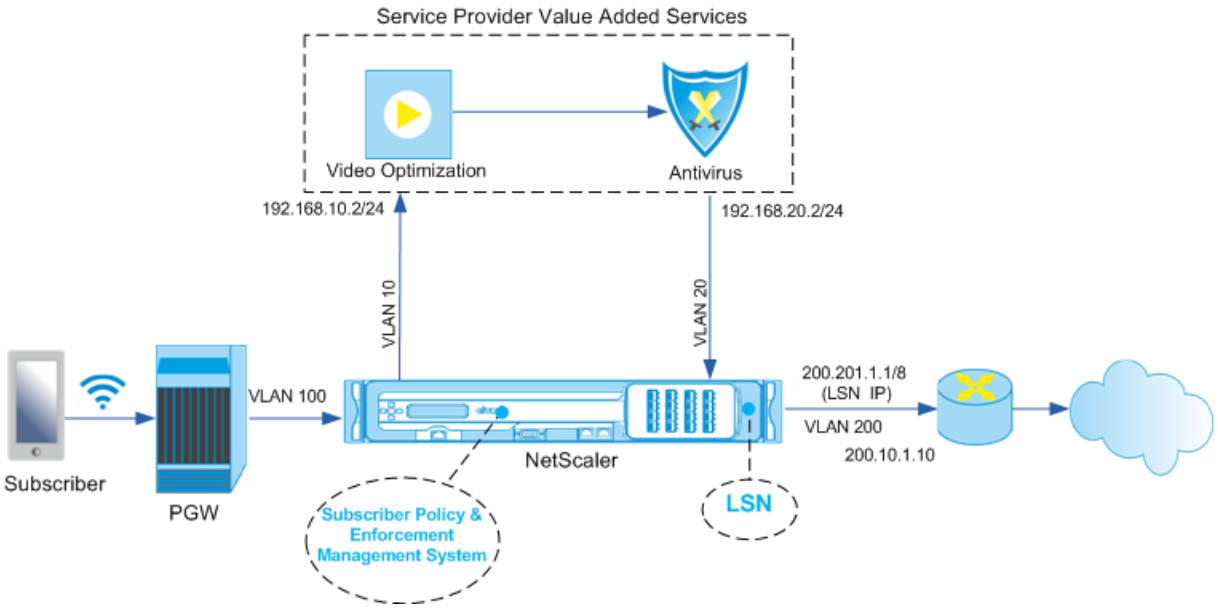
Abonnentenbewusste Verkehrssteuerung

October 5, 2021

Die Verkehrssteuerung leitet den Teilnehmerverkehr von einem Punkt zum anderen. Wenn ein Teilnehmer eine Verbindung zum Netzwerk herstellt, ordnet das Paketgateway dem Abonnenten eine IP-Adresse zu und leitet das Datenpaket an die Citrix ADC Appliance weiter. Die Appliance kommuniziert mit dem PCRF-Server über die GX-Schnittstelle, um die Richtlinieninformationen abrufen zu können. Abhängig von den Richtlinieninformationen führt die Appliance eine der folgenden Aktionen aus:

- Weiterleiten des Datenpakets an einen anderen Satz von Diensten (wie in der folgenden Abbildung gezeigt).
- Lassen Sie das Paket fallen.
- Führen Sie nur Large Scale NAT (LSN) aus, wenn LSN auf der Appliance konfiguriert ist.

Die in der folgenden Abbildung dargestellten Werte werden in der CLI-Prozedur konfiguriert, die der Abbildung folgt. Ein virtueller Content Switching-Server auf der Citrix ADC Appliance leitet Anforderungen an die Value Added Services oder überspringt sie, abhängig von der definierten Regel, und sendet das Paket dann nach dem Ausführen von LSN an das Internet.



So konfigurieren Sie die Verkehrssteuerung für die obige Bereitstellung mit der Befehlszeilenschnittstelle

Fügen Sie die Subnetz-IP (SNIP) -Adressen der Appliance hinzu.

Beispiel:

```
add ns ip 192.168.10.1 255.255.255.0 -type snip

add ns ip 192.168.20.1 255.255.255.0 -type snip

add ns ip 100.100.100.1 255.0.0.0 -type snip

add ns ip 200.200.200.1 255.0.0.0 -type snip

add ns ip 100.1.1.1 255.0.0.0 -type snip

add ns ip 200.201.1.1 255.0.0.0 -type snip
<!--NeedCopy-->
```

Fügen Sie die VLANs hinzu. VLANs helfen der Appliance, die Quelle des Datenverkehrs zu identifizieren. Binden Sie die VLANs an die Schnittstellen und Subnetz-IP-Adressen.

Beispiel:


```
add vlan 10

add vlan 20

add vlan 100

add vlan 200

bind vlan 10 -ifnum 1/4 -tagged -IPAddress 192.168.10.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.20.1 255.255.255.0

bind vlan 100 -ifnum 1/2 -tagged -IPAddress 100.1.1.1 255.0.0.0

bind vlan 200 -ifnum 1/3 -tagged -IPAddress 200.1.1.1 255.0.0.0
<!--NeedCopy-->
```

Geben Sie das VLAN an, in dem der Teilnehmerdatenverkehr auf der Appliance eintrifft. Geben Sie den Dienstpfad AVP an, der der Appliance mitteilt, wo in der Teilnehmersitzung nach dem Dienstpfadnamen suchen soll. Geben Sie für die primäre PCEF-Funktionalität den InterfaceType als RadiusAndGX an.

Beispiel:

```
set ns param -servicePathIngressVLAN 100

set subscriber gxinterface -servicepathAVP 1001 1005 -
    servicepathVendorid 10415

set subscriber param -interfaceType RadiusAndGx
<!--NeedCopy-->
```

Konfigurieren Sie einen Dienst und einen virtuellen Server vom Typ Durchmesser, und binden Sie den Dienst an den virtuellen Server. Geben Sie dann die PCRF-Realm und Subscriber Gx Schnittstellenparameter an. Konfigurieren Sie für die primäre PCEF-Funktionalität einen RADIUS-Listener-Dienst und eine RADIUS-Schnittstelle.

Beispiel:

```
add service sd1 10.102.232.200 DIAMETER 3868

```



```
add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
    persistAVPno 263

bind lb vserver vdiam sd1

set ns diameter -identity netscaler.sc1.net -realm pcrf1.net

set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf1.net -
    holdOnSubscriberAbsence YES -idleTTL 1200 -negativeTTL 120

add service srad1 10.102.232.236 RADIUSListener 1813

set subscriber radiusInterface -listeningService srad1
<!--NeedCopy-->
```

Fügen Sie Dienstfunktionen hinzu, um ein VAS mit einem eindringenden VLAN zu verknüpfen. Fügen Sie einen Dienstpfad hinzu, um die Kette zu definieren, das heißt, geben Sie den VAS an, an den das Paket gesendet werden muss, und die Reihenfolge, in der es zu diesem VAS gehen muss. Der Dienstpfadname wird normalerweise vom PCRF gesendet. Der Dienstpfad des Standardabonnentenprofils (*) gilt jedoch, wenn einer der folgenden Punkte zutrifft:

- PCRF verfügt nicht über die Teilnehmerinformationen.
- Die Teilnehmerinformationen enthalten diesen AVP nicht.
- Die Appliance kann den PCRF nicht abfragen. Beispielsweise ist der Dienst, der den PCRF darstellt, DOWN.

Der Dienstpfad AVP, der diesen Namen enthält, muss bereits als Teil der globalen Konfiguration konfiguriert sein. Binden Sie die Dienstfunktion an den Dienstpfad. Der Service-Index gibt die Reihenfolge an, in der das VAS der Kette hinzugefügt wird. Die höchste Zahl (255) gibt den Beginn der Kette an.

Beispiel:

```
add ns servicefunction SF1 -ingressVLAN 20

add ns servicepath pol1

bind ns servicepath pol1 -servicefunction SF1 -index 255

add subscriber profile * -subscriberrules default_path
<!--NeedCopy-->
```

Fügen Sie die LSN-Konfiguration hinzu. Definieren Sie also den NAT-Pool und identifizieren Sie die Clients, für die die Appliance LSN ausführen muss.


```
add lsn pool pool1

bind lsn pool pool1 200.201.1.1

add lsn client client1

bind lsn client client1 -network 100.0.0.0 -netmask 255.0.0.0

add lsn group group1 -clientname client1

bind lsn group group1 -poolname pool1
<!--NeedCopy-->
```

Die Appliance führt standardmäßig LSN aus. Um LSN außer Kraft zu setzen, müssen Sie ein Netzprofil mit aktiviertem Parameter OverridelsN erstellen und dieses Profil an alle virtuellen Lastausgleichsserver binden, die für Value Added Services (VAS) konfiguriert sind.

Beispiel:

```
add netprofile np1

set netprofile np1 -overrideLsn ENABLED

set lb vserver vs1 -netprofile np1
<!--NeedCopy-->
```

Konfigurieren Sie das VAS auf der Appliance. Dazu gehört das Erstellen der Dienste und der virtuellen Server und das Anbinden der Dienste an die virtuellen Server.

```
add service vas1 192.168.10.2 ANY 80 -usip YES

add service sint 200.10.1.10 ANY 80 -usip YES

add lb vserver vs1 ANY -m MAC -l2Conn ON

add lb vserver vint ANY -m MAC -l2Conn ON

bind lb vserver vs1 vas1

bind lb vserver vint sint
```



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

Fügen Sie die Content Switching (CS)-Konfiguration hinzu. Dazu gehören virtuelle Server, Richtlinien und zugehörige Aktionen. Der Datenverkehr kommt beim virtuellen CS Server an und wird dann an den entsprechenden virtuellen Lastausgleichsserver umgeleitet. Definieren Sie Ausdrücke, die einen virtuellen Server einer Dienstfunktion zuordnen.

Beispiel:

```
add cs vserver cs1 ANY * 80 -l2Conn ON

add cs action csact1 -targetLBVserver vs1

add cs action csactint -targetLBVserver vint

add cs policy cspol1 -rule  SUBSCRIBER.SERVICEPATH.IS_NEXT("SF1") &&
   SYS.VSERVER("vs1").STATE.EQ(UP)" -action csact1

bind cs vserver cs1 -policyName cspol1 -priority 110

bind cs vserver cs1 -lbvserver vint
<!--NeedCopy-->
```

So konfigurieren Sie die Verkehrssteuerung auf der Appliance mit der GUI

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs**, und fügen Sie die Subnetz-IP-Adressen hinzu.
2. Navigieren Sie zu System > Netzwerk > **VLANs** und fügen Sie VLANs hinzu, binden Sie die VLANs an die Schnittstellen und Subnetz-IP-Adressen.
3. Navigieren Sie zu **Traffic Management** > **Service Chaining** > **Service Path Ingress VLAN konfigurieren**, und geben Sie ein eindringendes VLAN an.
4. Navigieren Sie zu **Traffic Management** > **Subscriber** > **Parameters** > **Subscriber Parameters konfigurieren**, und geben Sie Folgendes an:
   - Schnittstellentyp: Geben Sie **RadiusAndGX** an.
   - Konfigurieren Sie einen virtuellen Server mit Durchmesser, PCRF-Bereich und die Parameter der GX-Schnittstelle des Teilnehmers.
   - Geben Sie die RADIUS-Schnittstellenparameter an.
5. Navigieren Sie zu **Traffic Management** > **Service Chaining** > **Service Function**, und fügen Sie Service-Funktionen hinzu, um einen Value Added Service mit einem eingehenden VLAN zu verknüpfen.
6. Navigieren Sie zu **System** > **Netzwerk** > **Large Scale NAT**. Klicken Sie auf **Pools**, und fügen Sie einen Pool hinzu. Klicken Sie auf **Clients**, und fügen Sie einen Client hinzu. Klicken Sie auf

Gruppen, fügen Sie eine Gruppe hinzu, und geben Sie den Client an. Bearbeiten Sie die Gruppe und binden Sie den Pool an diese Gruppe.

7. Navigieren Sie zu **System** > **Netzwerk** > **Netzprofile** und fügen Sie ein Netzprofil hinzu. Wählen Sie **LSN überschreiben**. Navigieren Sie optional zu **System** > **Netzwerk** > **Einstellungen** > **Layer-3-Parameter konfigurieren**, und stellen Sie sicher, dass **LSN überschreiben** nicht ausgewählt ist.
8. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und konfigurieren Sie die virtuellen Server und Mehrwertdienste auf der Appliance. Binden Sie die Dienste und das Netzprofil an den virtuellen Server.
9. Navigieren Sie zu **Traffic Management** > **Content Switching** > **Virtuelle Server**, und konfigurieren Sie einen virtuellen Server, eine Richtlinie und eine Aktion. Geben Sie den virtuellen Zielserver für Lastenausgleich an.

So konfigurieren Sie die Dienstverkettung auf der Appliance mit der GUI

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs**, und fügen Sie die Subnetz-IP-Adressen hinzu.
2. Navigieren Sie zu System > Netzwerk > **VLANs** und fügen Sie VLANs hinzu, binden Sie die VLANs an die Schnittstellen und Subnetz-IP-Adressen.
3. Navigieren Sie zu **Traffic Management** > **Service Chaining** > **Service Path Ingress VLAN konfigurieren**, und geben Sie ein eindringendes VLAN an.
4. Navigieren Sie zu **Traffic Management** > **Subscriber** > **Parameters** > **Subscriber Parameters konfigurieren**, und geben Sie Folgendes an:
   - Schnittstellentyp: Geben Sie **RadiusAndGX** an.
   - Konfigurieren Sie einen virtuellen Server mit Durchmesser, PCRF-Bereich und die Parameter der GX-Schnittstelle des Teilnehmers.
   - Geben Sie die RADIUS-Schnittstellenparameter an.
5. Navigieren Sie zu **Traffic Management** > **Service Chaining** > **Service Function**, und fügen Sie Service-Funktionen hinzu, um einen Value Added Service mit einem eingehenden VLAN zu verknüpfen.
6. Navigieren Sie zu **System** > **Netzwerk** > **Large Scale NAT**. Klicken Sie auf **Pools**, und fügen Sie einen Pool hinzu. Klicken Sie auf **Clients**, und fügen Sie einen Client hinzu. Klicken Sie auf **Gruppen**, fügen Sie eine Gruppe hinzu, und geben Sie den Client an. Bearbeiten Sie die Gruppe und binden Sie den Pool an diese Gruppe.
7. Navigieren Sie zu **System** > **Netzwerk** > **Netzprofile** und fügen Sie ein Netzprofil hinzu. Wählen Sie **LSN überschreiben**. Navigieren Sie optional zu **System** > **Netzwerk** > **Einstellungen** > **Layer-3-Parameter konfigurieren**, und stellen Sie sicher, dass **LSN überschreiben** nicht ausgewählt ist.
8. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und konfigurieren Sie die virtuellen Server und Mehrwertdienste auf der Appliance. Binden Sie die Dienste und das Netzprofil an den virtuellen Server.

9. Navigieren Sie zu **Traffic Management** > **Content Switching** > **Virtuelle Server**, und konfigurieren Sie einen virtuellen Server, eine Richtlinie und eine Aktion. Geben Sie den virtuellen Zielserver für Lastenausgleich an.

Abonnentenbewusste Service-Verkettung

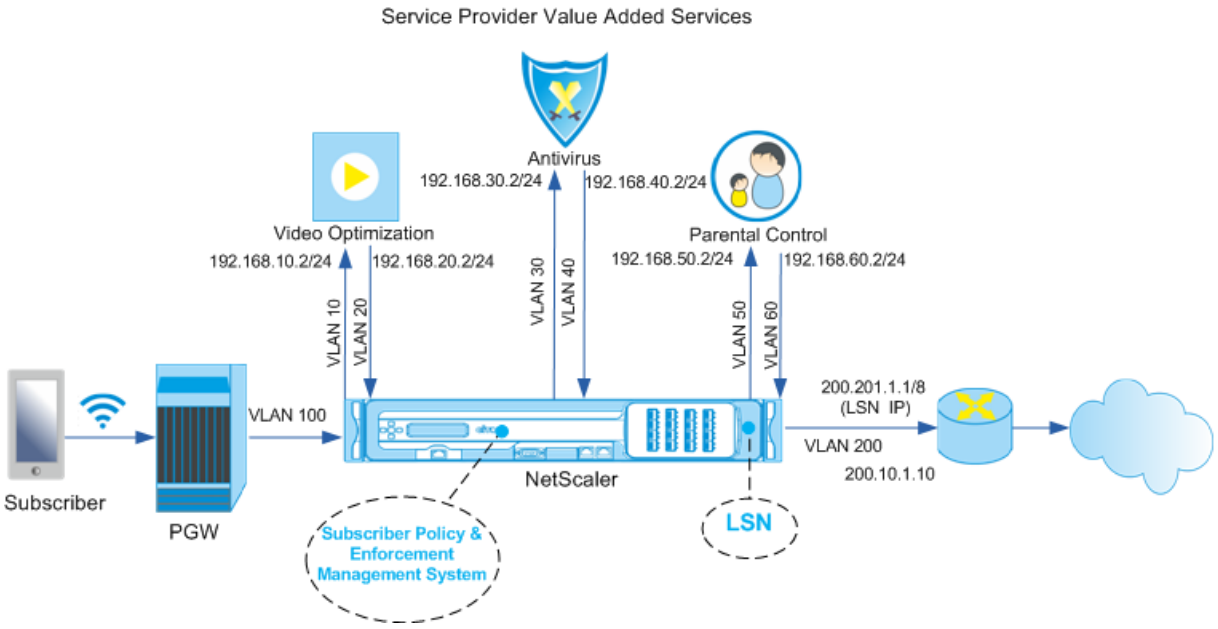
October 5, 2021

Mit dem enormen Anstieg des Datenverkehrs durch Telekommunikationsnetze ist es für Dienstleister nicht mehr möglich, den gesamten Datenverkehr über alle Value Added Services (VAS) zu steuern. Ein Dienstleister sollte in der Lage sein, die Nutzung von VAS zu optimieren und den Datenverkehr intelligent zu steuern, um die Benutzererfahrung zu verbessern. Beispielsweise ist eine Videooptimierung für Datenverkehr, der kein Video enthält, nicht erforderlich. Wenn ein Teilnehmer mit einem 4G-Netzwerk verbunden ist, können Inhalte in High Definition (HD) gestreamt werden, und eine Videooptimierung ist möglicherweise nicht erforderlich. Die Videooptimierung verbessert jedoch die Benutzererfahrung in einem 3G-Netzwerk. Ebenso bietet das Caching eine schnellere und bessere Benutzererfahrung und kann je nach Abonnentenplan aktiviert werden. Ein weiteres Beispiel für VAS ist die Kindersicherung. Wenn Eltern einem minderjährigen Kind ein mobiles Mobiltelefon zur Verfügung stellen, möchten sie eine Art Kontrolle über die Websites, die ihr Kind besucht.

Um dies und mehr zu tun, müssen Dienstleister in der Lage sein, Mehrwertdienste pro Teilnehmer anzubieten. Mit anderen Worten, Entitäten im Dienstanbieternetz müssen in der Lage sein, die Teilnehmerinformationen zu extrahieren und das Paket auf der Grundlage dieser Informationen intelligent zu steuern.

Die Dienstverkettung bestimmt den Satz von Diensten, über die der Datenverkehr von einem Teilnehmer passieren muss, bevor Sie zum Internet gehen. Anstatt den gesamten Datenverkehr an alle Dienste zu senden, leitet Citrix ADC auf der Grundlage der für diesen Abonnenten definierten Richtlinie alle Anforderungen eines Abonnenten intelligent an einen bestimmten Satz von Diensten weiter.

Die folgende Abbildung zeigt die Entitäten, die an der Service-Verkettung beteiligt sind. Die angezeigten Werte werden in der Prozedur konfiguriert, die der Abbildung folgt. Ein virtueller Content Switching-Server auf der Citrix ADC Appliance leitet Anforderungen an die Value Added Services oder überspringt sie, abhängig von der definierten Regel, und sendet das Paket dann nach dem Ausführen von LSN an das Internet.



So konfigurieren Sie die Dienstverkettung für die obige Bereitstellung mit der CLI

Fügen Sie die Subnetz-IP (SNIP) -Adressen der Appliance hinzu.

Beispiel:

```
add ns ip 192.168.10.1 255.255.255.0 -type snip

add ns ip 192.168.20.1 255.255.255.0 -type snip

add ns ip 192.168.30.1 255.255.255.0 -type snip

add ns ip 192.168.40.1 255.255.255.0 -type snip

add ns ip 192.168.50.1 255.255.255.0 -type snip

add ns ip 192.168.60.1 255.255.255.0 -type snip

add ns ip 100.1.1.1 255.0.0.0 -type snip

add ns ip 200.201.1.1 255.0.0.0 -type snip
<!--NeedCopy-->
```

Fügen Sie die VLANs hinzu. VLANs helfen der Appliance, die Quelle des Datenverkehrs zu identifizieren. Binden Sie die VLANs an die Schnittstellen und Subnetz-IP-Adressen. Fügen Sie für jedes VAS ein Eingangs- und ein Egress-VLAN hinzu.

Beispiel:

```
add vlan 10

add vlan 20

add vlan 30

add vlan 40

add vlan 50

add vlan 60

add vlan 100

add vlan 200

bind vlan 10 -ifnum 1/4 -tagged -IPAddress 192.168.10.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.20.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.30.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.40.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.50.1 255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.60.1 255.255.255.0

bind vlan 100 -ifnum 1/2 -tagged -IPAddress 100.1.1.1 255.0.0.0

bind vlan 200 -ifnum 1/3 -tagged -IPAddress 200.201.1.1 255.0.0.0
<!--NeedCopy-->
```

Geben Sie das VLAN an, in dem der Teilnehmerdatenverkehr auf der Appliance eintrifft. Geben Sie den Dienstpfad AVP an, der der Appliance mitteilt, wo in der Teilnehmersitzung nach dem Dienstpfadnamen suchen soll. Geben Sie für die primäre PCEF-Funktionalität den InterfaceType als RadiusAndGX an.

Beispiel:


```
set ns param -servicePathIngressVLAN 100

set subscriber gxinterface -servicepathAVP 1001 1005 -
    servicepathVendorid 10415

set subscriber param -interfaceType RadiusAndGx
<!--NeedCopy-->
```

Konfigurieren Sie einen Dienst und einen virtuellen Server vom Typ Durchmesser, und binden Sie den Dienst an den virtuellen Server. Geben Sie dann die PCRF-Realm und Subscriber Gx Schnittstellenparameter an. Konfigurieren Sie für die primäre PCEF-Funktionalität einen RADIUS-Listener-Dienst und eine RADIUS-Schnittstelle.

Beispiel:

```
add service sd1 10.102.232.200 DIAMETER 3868

add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER -
    persistAVPno 263

bind lb vserver vdiam sd1

set ns diameter -identity netscaler.sc1.net -realm pcrf1.net

set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf1.net -
    holdOnSubscriberAbsence YES -idleTTL 1200 -negativeTTL 120

add service srad1 10.102.232.236 RADIUSListener 1813

set subscriber radiusInterface -listeningService srad1
<!--NeedCopy-->
```

Fügen Sie Dienstfunktionen hinzu, um ein VAS mit einem eindringenden VLAN zu verknüpfen. Fügen Sie einen Dienstpfad hinzu, um die Kette zu definieren, das heißt, geben Sie den VAS an, an den das Paket gesendet werden muss, und die Reihenfolge, in der es zu diesem VAS gehen muss. Der Dienstpfadname wird normalerweise vom PCRF gesendet. Der Dienstpfad des Standardabonnentenprofils (*) gilt jedoch, wenn einer der folgenden Punkte zutrifft:

- PCRF verfügt nicht über die Teilnehmerinformationen.
- Die Teilnehmerinformationen enthalten diesen AVP nicht.
- Die Appliance kann den PCRF nicht abfragen. Beispielsweise ist der Dienst, der den PCRF darstellt, DOWN.

Der Dienstpfad AVP, der diesen Namen enthält, muss zuvor als Teil der globalen Konfiguration konfiguriert werden. Binden Sie die Dienstfunktion an den Dienstpfad. Der Service-Index gibt die Reihenfolge an, in der das VAS der Kette hinzugefügt wird. Die höchste Zahl (255) gibt den Beginn der Kette an.

Beispiel:

```
add ns servicefunction SF1 -ingressVLAN 20

add ns servicefunction SF2 -ingressVLAN 40

add ns servicefunction SF3 -ingressVLAN 60

add ns servicepath pol1

bind ns servicepath pol1 -servicefunction SF1 -index 255

bind ns servicepath pol1 -servicefunction SF2 -index 254

bind ns servicepath pol1 -servicefunction SF3 -index 253

add ns servicepath pol2

bind ns servicepath pol2 -servicefunction SF2 -index 255

add ns servicepath pol3

bind ns servicepath pol3 -servicefunction SF1 -index 255

add subscriber profile * -subscriberrules default_path
<!--NeedCopy-->
```

Fügen Sie die LSN-Konfiguration hinzu. Definieren Sie also den NAT-Pool und identifizieren Sie die Clients, für die die Appliance LSN ausführen muss.

Beispiel:

```
add lsn pool pool1

bind lsn pool pool1 200.201.1.1

add lsn client client1

```



```
bind lsn client client1 -network 100.0.0.0 -netmask 255.0.0.0

add lsn group group1 -clientname client1

bind lsn group group1 -poolname pool1
<!--NeedCopy-->
```

Die Appliance führt standardmäßig LSN aus. Um LSN außer Kraft zu setzen, müssen Sie ein Netzprofil mit aktiviertem OverridelsN-Parameter erstellen und dieses Profil an alle virtuellen Lastausgleichsserver binden, die für Value Added Services (VAS) konfiguriert sind.

Beispiel:

```
add netprofile np1

set netprofile np1 -overrideLsn ENABLED

set lb vserver vs1 -netprofile np1
<!--NeedCopy-->
```

Konfigurieren Sie das VAS auf der Appliance. Dazu gehört das Erstellen der Dienste und der virtuellen Server und das Anbinden der Dienste an die virtuellen Server.

Beispiel:

```
add service vas1 192.168.10.2 ANY 80 -usip YES

add service vas2 192.168.30.2 ANY 80 -usip YES

add service vas3 192.168.50.2 ANY 80 -usip YES

add service sint 200.10.1.10 ANY 80 -usip YES

add lb vserver vs1 ANY -m MAC -l2Conn ON

add lb vserver vs2 ANY -m MAC -l2Conn ON

add lb vserver vs3 ANY -m MAC -l2Conn ON

add lb vserver vint ANY -m MAC -l2Conn ON

bind lb vserver vs1 vas1

```



```
bind lb vserver vs2 vas2

bind lb vserver vs3 vas3

bind lb vserver vint sint
<!--NeedCopy-->
```

Fügen Sie die Content Switching (CS)-Konfiguration hinzu. Dazu gehören virtuelle Server, Richtlinien und zugehörige Aktionen. Der Datenverkehr kommt beim virtuellen CS Server an und wird dann an den entsprechenden virtuellen Lastausgleichsserver umgeleitet. Definieren Sie Ausdrücke, die einen virtuellen Server einer Dienstfunktion zuordnen.

Beispiel:

```
add cs vserver cs1 ANY * 80 -l2Conn ON

add cs action csact1 -targetLBVserver vs1

add cs action csact2 -targetLBVserver vs2

add cs action csact3 -targetLBVserver vs3

add cs action csactint -targetLBVserver vint

add cs policy cspol1 -rule "SUBSCRIBER.SERVICEPATH.IS_NEXT("SF1") &&
   SYS.VSERVER("vs1").STATE.EQ(UP)" -action csact1

add cs policy cspol2 -rule "SUBSCRIBER.SERVICEPATH.IS_NEXT("SF2") &&
   SYS.VSERVER("vs2").STATE.EQ(UP)" -action csact2

add cs policy cspol3 -rule "SUBSCRIBER.SERVICEPATH.IS_NEXT("SF3") &&
   SYS.VSERVER("vs3").STATE.EQ(UP)" -action csact3

bind cs vserver cs1 -policyName cspol1 -priority 110

bind cs vserver cs1 -policyName cspol2 -priority 120

bind cs vserver cs1 -policyName cspol3 -priority 130

bind cs vserver cs1 -lbvserver vint
<!--NeedCopy-->
```


So konfigurieren Sie die Dienstverkettung auf der Appliance mit der GUI

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs**, und fügen Sie die Subnetz-IP-Adressen hinzu.
2. Navigieren Sie zu **System** > **Netzwerk** > **VLANs** und fügen Sie VLANs hinzu, binden Sie die VLANs an die Schnittstellen und Subnetz-IP-Adressen.
3. Navigieren Sie zu **Traffic Management** > **Service Chaining** > **Service Path Ingress VLAN konfigurieren**, und geben Sie ein eindringendes VLAN an.
4. Navigieren Sie zu **Traffic Management** > **Subscriber** > **Parameters** > **Subscriber Parameters konfigurieren**, und geben Sie Folgendes an:
   - Schnittstellentyp: Geben Sie **RadiusAndGX** an.
   - Konfigurieren Sie einen virtuellen Server mit Durchmesser, PCRF-Bereich und die Parameter der GX-Schnittstelle des Teilnehmers.
   - Geben Sie die RADIUS-Schnittstellenparameter an.
5. Navigieren Sie zu **Traffic Management** > **Service Chaining** > **Service Function**, und fügen Sie Service-Funktionen hinzu, um einen Value Added Service mit einem eingehenden VLAN zu verknüpfen.
6. Navigieren Sie zu **System** > **Netzwerk** > **Large Scale NAT**. Klicken Sie auf **Pools**, und fügen Sie einen Pool hinzu. Klicken Sie auf **Clients**, und fügen Sie einen Client hinzu. Klicken Sie auf **Gruppen**, fügen Sie eine Gruppe hinzu, und geben Sie den Client an. Bearbeiten Sie die Gruppe und binden Sie den Pool an diese Gruppe.
7. Navigieren Sie zu **System** > **Netzwerk** > **Netzprofile** und fügen Sie ein Netzprofil hinzu. Wählen Sie **LSN überschreiben**. Navigieren Sie optional zu **System** > **Netzwerk** > **Einstellungen** > **Layer-3-Parameter konfigurieren**, und stellen Sie sicher, dass **LSN überschreiben** nicht ausgewählt ist.
8. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und konfigurieren Sie die virtuellen Server und Mehrwertdienste auf der Appliance. Binden Sie die Dienste und das Netzprofil an den virtuellen Server.
9. Navigieren Sie zu **Traffic Management** > **Content Switching** > **Virtuelle Server**, und konfigurieren Sie einen virtuellen Server, eine Richtlinie und eine Aktion. Geben Sie den virtuellen Zielserver für Lastenausgleich an.

Abonnentenbewusste Verkehrssteuerung mit TCP-Optimierung

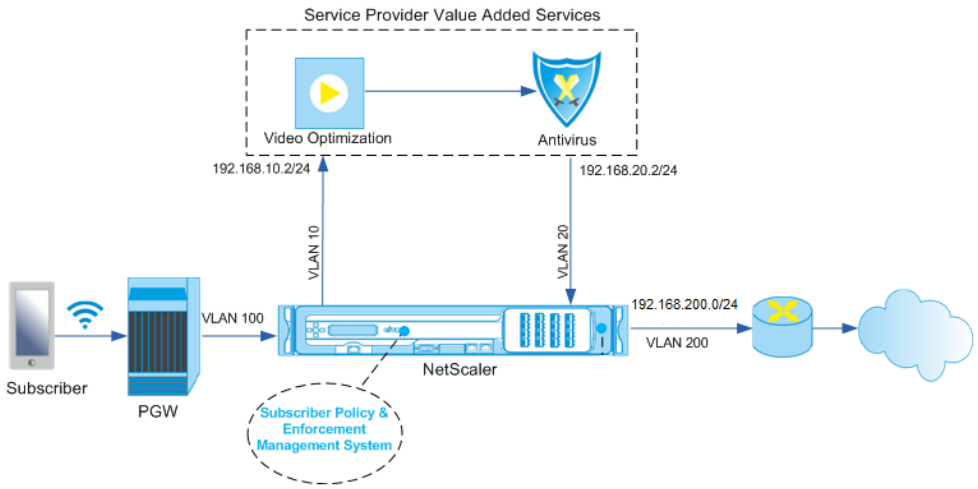
October 5, 2021

Die Verkehrssteuerung leitet den Teilnehmerverkehr von einem Punkt zum anderen. Wenn ein Teilnehmer eine Verbindung zum Netzwerk herstellt, ordnet das Paketgateway dem Abonnenten eine IP-Adresse zu und leitet das Datenpaket an die Citrix ADC Appliance weiter. Die Appliance kommuniziert mit dem PCRF-Server über die GX-Schnittstelle, um die Informationen zur Abonnen-

tenrichtlinie abrufen zu können. Abhängig von den Richtlinieninformationen führt die Appliance eine der folgenden Aktionen aus:

- Weiterleiten des Datenpakets an einen anderen Satz von Diensten (wie in der folgenden Abbildung gezeigt).
- Führen Sie nur TCP-Optimierung durch.

Die in der folgenden Abbildung dargestellten Werte werden in der CLI-Prozedur konfiguriert, die der Abbildung folgt. Ein virtueller Content Switching-Server auf der Citrix ADC Appliance leitet Anforderungen an die Value Added Services oder überspringt sie und führt je nach definierter Regel TCP-Optimierung durch und sendet das Paket dann an das Internet.



> **Hinweis:**
>
> Die Unterstützung für die unten dargestellte Konfiguration wurde in Version 11.1 Build 50.10 eingeführt.

So konfigurieren Sie die Verkehrssteuerung für die obige Bereitstellung mit der Befehlszeilenschnittstelle:

1. Fügen Sie die Subnetz-IP (SNIP) -Adressen der Appliance hinzu.

```
add ns ip 192.168.10.1 255.255.255.0 -type snip

add ns ip 192.168.20.1 255.255.255.0 -type snip

add ns ip 192.168.100.1 255.255.255.0 -type snip

add ns ip 192.168.200.1 255.255.255.0 -type snip

```



```
add ns ip 10.102.232.236 255.255.255.0 -type snip
<!--NeedCopy-->
```

2. Fügen Sie die VLANs hinzu. VLANs helfen der Appliance, die Quelle des Datenverkehrs zu identifizieren. Binden Sie die VLANs an die Schnittstellen und Subnetz-IP-Adressen.

```
add vlan 10

add vlan 20

add vlan 100

add vlan 200

add vlan 102

bind vlan 10 -ifnum 1/4 -tagged -IPAddress 192.168.10.1
   255.255.255.0

bind vlan 20 -ifnum 1/4 -tagged -IPAddress 192.168.20.1
   255.255.255.0

bind vlan 100 -ifnum 1/2 -tagged -IPAddress 192.168.100.1
   255.255.255.0

bind vlan 200 -ifnum 1/2 -tagged -IPAddress 192.168.200.1
   255.255.255.0

bind vlan 102 -ifnum 1/1 -tagged -IPAddress 10.102.232.236
   255.255.255.0
<!--NeedCopy-->
```

3. Konfigurieren Sie einen Dienst und einen virtuellen Server vom Typ Durchmesser, und binden Sie den Dienst an den virtuellen Server. Geben Sie die PCRF-Realm und die Werte für die Gx-Schnittstellenparameter des Abonnenten an. Geben Sie außerdem den Dienstpfad AVP an, der angibt, wo die Appliance den Dienstpfadnamen in der Teilnehmersitzung finden kann. Konfigurieren Sie für die primäre PCEF-Funktionalität einen RADIUS-Listener-Dienst und eine RADIUS-Schnittstelle und geben Sie den Schnittstellentyp als “RadiusAndGX” an.

```
add service sd1 10.102.232.200 DIAMETER 3868

```



```
add lb vserver vdiam DIAMETER 0.0.0.0 0 -persistenceType DIAMETER
   -persistAVPno 263

bind lb vserver vdiam sd1

set ns diameter -identity netscaler.sc1.net -realm pcrf1.net

set extendedmemoryparam -memLimit 2558

set subscriber gxInterface -vServer vdiam -pcrfRealm pcrf1.net

set subscriber gxinterface -servicepathAVP 1001 1005 -
   servicepathVendorid 10415

add service srad1 10.102.232.236 RADIUSListener 1813

set subscriber radiusInterface -listeningService srad1

set subscriber param -interfaceType RadiusAndGx
<!--NeedCopy-->
```

4. Geben Sie ein Standardabonnentenprofil (*) an, das angewendet werden soll, wenn eine der folgenden Punkte zutrifft:

   - PCRF verfügt nicht über die Teilnehmerinformationen.
   - Die Teilnehmerinformationen enthalten nicht den Dienstpfad AVP.
   - Die Appliance kann den PCRF nicht abfragen. Beispielsweise ist der Dienst, der den PCRF darstellt, DOWN.

```
add subscriber profile * -subscriberrules default_path
<!--NeedCopy-->
```

5. Erstellen Sie TCP-Profile für den VAS bzw. TCP-Optimierungspfad. Der an VAS gelenkte Verkehr wird vor oder nach dem Verlassen des VAS keiner TCP-Optimierung unterzogen. Daher sollte der TCP-Modus des VAS-Profils auf TRANSPARENT gesetzt werden, während der TCP-Modus des TCPopt-Profils auf ENDPOINT gesetzt werden sollte.

   add ns tcpProfile VAS –tcpMode TRANSPARENT

   add ns tcpProfile TCPOpt -WS ENABLED -SACK ENABLED -WSVal 8 -mss 1460 -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -bufferSize 4000000 -flavor BIC -dynamicReceiveBuffering ENABLED -KA ENABLED -sendBuffsize 4000000 -rstWindowAttenuate ENABLED -spoofSynDrop ENABLED -ecn ENABLED -frto ENABLED -maxcwnd 1000000 -fack ENABLED -rstMaxAck

enABLED -tcpmode ENDPOINT

6. Konfigurieren Sie den Lastausgleich für die VAS-Server. Erstellen Sie einen nicht adressierbaren virtuellen Server vom Typ TCP. Erstellen Sie TCP-Dienste mit den IP-Adressen der VAS-Server und binden Sie die Dienste an den virtuellen Server. Der virtuelle Server und die Dienste verwenden das transparente TCP-Profil, das für den VAS-Pfad erstellt wurde:

```
add service vas1 192.168.10.2 TCP * -usip YES -useproxyport NO -
    TCPB NO -tcpProfileName VAS

add service vas2 192.168.10.3 TCP * -usip YES -useproxyport NO -
    TCPB NO -tcpProfileName VAS

add lb vserver vs1 TCP -m MAC -l2Conn ON  - tcpProfileName VAS

bind lb vserver vs1 vas1

bind lb vserver vs1 vas2
<!--NeedCopy-->
```

7. Fügen Sie einen virtuellen Lastausgleichsserver hinzu, um den Datenverkehr des VAS zu erfassen. Dieser vserver überwacht das VAS Egress VLAN und verwendet das transparente TCP-Profil:

```
add lb vserver vsint TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ(20)"
     - Listenpriority 30  - l2Conn ON  - tcpProfileName VAS
<!--NeedCopy-->
```

8. Fügen Sie einen virtuellen Server zur TCP-Optimierung hinzu, der auf jeden Datenverkehr im drahtlosen VLAN wartet und das für den TCP-Optimierungspfad erstellte Endpunktprofil verwendet:

```
add lb vserver vs-TcpOpt TCP * * -Listenpolicy "client.vlan.id.eq
    (100)"  - Listenpriority 20 -l2Conn ON -tcpProfileName TCPOpt
<!--NeedCopy-->
```

9. Fügen Sie die Content Switching (CS)-Konfiguration hinzu. Dazu gehören virtuelle Server, Richtlinien und zugehörige Aktionen. Der virtuelle CS Server empfängt den Datenverkehr und leitet ihn gemäß definierten CS-Richtlinien an den entsprechenden virtuellen Lastausgleichsserver weiter. Erstellen Sie einen virtuellen CS TCP Server, der jeden Datenverkehr

im drahtlosen VLAN mit höchster Priorität überwacht und das TCP-Profil des Endpunkts verwendet. Erstellen Sie eine CS-Richtlinie, die als TRUE ausgewertet wird, wenn “vas” die Teilnehmerregel ist, und geben Sie eine CS-Aktion an, die den Datenverkehr zu VAS steuert. Machen Sie den virtuellen TCP-Optimierungsserver zum standardmäßigen LB-vserver. Jeder Teilnehmerdatenverkehr mit einer anderen Regel als “vas” durchläuft den Standard-LB-vserver.

```
add cs vserver cs1 TCP * * -Listenpolicy "client.vlan.id.eq(100)"
    -Listenpriority 10 -l2Conn ON  -tcpProfileName TCPOpt

add cs action csact1 -targetLBVserver vs1

add cs policy cspol1 -rule  SUBSCRIBER.RULE_ACTIVE("vas") && SYS.
    VSERVER("vs1").STATE.EQ(UP)" -action csact1

bind cs vserver cs1 -policyName cspol1

bind cs vserver cs1 -lbvserver vs-TcpOpt
<!--NeedCopy-->
```

10. Fügen Sie statische oder richtlinienbasierte Routen zum Internet hinzu. Dynamisches Routing wird ebenfalls in dieser Konfiguration unterstützt. Im folgenden Beispiel werden richtlinienbasierte Routen verwendet:

```
add ns pbr pbr-vlan100-to-vlan200 ALLOW -nextHop 192.168.200.10 -
    vlan 100 -priority 10

add ns pbr pbr-vlan20-to-vlan200 ALLOW -nextHop 192.168.200.10 -
    vlan 20 -priority 11

apply ns pbrs
<!--NeedCopy-->
```

Hinweis:

- Die CS-Richtlinien können neben den Abonnentenausdrücken auch IP-Adressen und Portnummern enthalten, z. B. SUBSCRIBER.RULE_ACTIVE (“vas”) && && (CLIENT.TCP.DSTPORT.EQ (80) || CLIENT.TCP.DSTPORT.EQ (443). Sie können auch HTTP-basierte Ausdrücke enthalten, z. B. HTTP.REQ.HOSTNAME.DOMAIN.EQ (“somedomain.com”). Ersetzen Sie in diesem Fall TCP-Entitäten (vserver, Dienst usw.) durch HTTP. Die TCP-Profilkonfiguration bleibt gleich.

- Fügen Sie IPv6-Konfiguration (Adressen, Routen, PBRs) hinzu, um IPv6-Abonnenten zu unterstützen. Happy Eyeballs Client-Anwendungen funktionieren reibungslos sowohl für VAS als auch für TCP Optimierungspfade.
- Fügen Sie VLANs, IP-Adressen, PBRs und virtuelle LB-Server vor VAS (vs1, vs2 usw.) hinzu, um mehrere Teilnehmerflüsse zu unterstützen. Ändern Sie die Listenrichtlinien von CS vserver “cs1” und LB vserver “vsint”, um die zusätzlichen VLANs einzuschließen.

Richtlinienbasierte TCP-Profilauswahl

January 28, 2022

Sie können die Citrix ADC Appliance so konfigurieren, dass sie die TCP-Optimierung basierend auf Abonnentenattributen durchführt. Beispielsweise kann die Appliance zur Laufzeit verschiedene TCP-Profile auswählen, basierend auf dem Netzwerk, mit dem das Benutzergerät (UE) verbunden ist. Auf diese Weise können Sie die Benutzererfahrung eines mobilen Benutzers verbessern, indem Sie einige Parameter in den TCP-Profilen festlegen und dann eine Richtlinie verwenden, um das entsprechende Profil auszuwählen.

Erstellen Sie separate TCP-Profile für Abonnenten, die sich über ein 4G-Netzwerk verbinden, und für Benutzer, die sich über ein anderes Netzwerk verbinden. Definieren Sie eine Richtlinienregel, die basierend auf einem Teilnehmerparameter wie dem Typ der Funkzugriffstechnologie (RAT-Typ) ausgewählt wird. Wenn in den folgenden Beispielen der RAT-Typ EUTRAN ist, wird ein TCP-Profil ausgewählt, das eine schnellere Verbindung unterstützt (Beispiel 1). Für alle anderen Werte vom Typ RAT wird ein anderes TCP-Profil ausgewählt (Beispiel 2).

Weitere Informationen zur Funkzugriffstechnologie und ihrer Richtlinienkonfiguration finden Sie in RFC 29.212.

> **Hinweis**
>
> Der AVP vom Typ RAT (AVP-Code 1032) ist vom Typ “Enumerated” und dient zur Identifizierung der Funkzugangstechnologie, die das UE bedient.
>
> Der Wert “1004” zeigt an, dass RAT EUTRAN ist.

Beispiel 1:

```
1 add ns tcpProfile tcp2 -WS ENABLED -SACK ENABLED -WSVal 8 -initialCwnd
      16 - oooQSize 15000 -slowStartIncr 1 -bufferSize 1000000 -flavor BIC
       - dynamicReceiveBuffering DISABLED -sendBuffsize 1000000 -dsack
      DISABLED -maxcwnd 4000000 -fack ENABLED -minRTO 500 -maxburst 15
2
```



```
add appqoe action appact2 -priority HIGH -tcpprofile tcp2

add appqoe policy apppol2 -rule ”SUBSCRIBER.AVP(1032).VALUE.
    GET_UNSIGNED32(0, BIG_ENDIAN).EQ(1004)” -action appact2

bind cs vserver <name>  -policyname apppol2 -priority 20 -type request
<!--NeedCopy-->
```

Beispiel 2:

```
add ns tcpProfile tcp1 -WS ENABLED -SACK ENABLED -WSVal 8 -initialCwnd
    16 - oooQSize 15000 -slowStartIncr 1 -bufferSize 150000 -flavor BIC
    - dynamicReceiveBuffering DISABLED -sendBuffsize 150000 -dsack
    DISABLED -maxcwnd 4000000 -fack ENABLED -minRTO 200 -maxburst 15

add appqoe action appact1 -priority HIGH -tcpprofile tcp1

add appqoe policy apppol1 -rule ”SUBSCRIBER.AVP(1032).VALUE.
    GET_UNSIGNED32(0, BIG_ENDIAN).NE(1004)” -action appact1

bind cs vserver <name>  -policyname apppol1 -priority 10 -type request
<!--NeedCopy-->
```

Lastausgleich Control-Ebenenverkehr, der auf Durchmesser-, SIP- und SMPP-Protokollen basiert

October 5, 2021

Mit dem zunehmenden Verkehr in der Steuerungsebene können die Server zu einem Engpass werden, da der Datenverkehr nicht optimal auf die Server verteilt wird. Daher müssen Nachrichten Lastenausgleich sein. Die Citrix ADC Appliance unterstützt Diameter, SIP und SMPP Load Balancing.

SIP

Mit Citrix ADC können Sie SIP-Nachrichten über UDP oder über TCP (einschließlich TLS) zu einer Gruppe von Proxyservern ausgleichen. Citrix ADC bietet auch Call-ID-basierte Persistenz und Call-ID-Hash-Lastausgleichsmethode, mit der Sie Pakete für eine bestimmte SIP-Sitzung auf denselben Lastausgleich SIP-Server weiterleiten.

Die Citrix ADC Standardausdruckssprache enthält eine Reihe von Ausdrücken, die auf SIP-Verbindungen (Session Initiation Protocol) ausgeführt werden. Diese Ausdrücke sollen in Richtlinien für das SIP-Protokoll verwendet werden, das auf Anfrage-/Antwortbasis arbeitet. Diese Ausdrücke können für Content Switching, Ratenbegrenzung, Responder und Umschreibrichtlinien verwendet werden.

Weitere Informationen finden Sie unter Load Balancing einer Gruppe von SIP-Servern.

SMPP

Millionen von Kurznachrichten werden täglich zwischen Einzelpersonen und Mehrwertdienstleistern wie Banken, Werbetreibenden und Verzeichnisdiensten ausgetauscht, indem das Short Message Peer to Peer (SMPP) -Protokoll verwendet wird. Häufig verzögert sich die Nachrichtenübermittlung, da Server überlastet sind und der Datenverkehr nicht optimal auf die Server verteilt wird.
Die Citrix ADC Appliance bietet eine optimale Verteilung der Nachrichten auf Ihre Server und verhindert so eine schlechte Leistung und Ausfälle. Die Citrix ADC Appliance:

- Lastverteilung Nachrichten, die vom Server und vom Client stammen
- Überwacht den Zustand der Message Centers
- Bietet Unterstützung für Content Switching für Message Center
- Verkettete Nachrichten werden verarbeitet

Einschränkung: Meldungs-IDs aus dem Nachrichtencenter, die länger als 59 Bytes sind, werden nicht unterstützt. Wenn die vom Nachrichtencenter zurückgegebene Nachrichtenkennungslänge mehr als 59 Byte beträgt, schlagen Nebenvorgänge fehl, und die Citrix ADC Appliance antwortet mit einer Fehlermeldung.

Weitere Informationen finden Sie unter SMPP Load Balancing

Diameter

Durchmesser ist ein Basisprotokoll mit mehr als 50 Protokollen (auch Anwendungen genannt) darüber gebaut. Daher ist der Durchmesserverkehr, der in einem Telco-Netzwerk erzeugt wird, hoch. Um diesen Durchmesserverkehr optimal aufrechtzuerhalten, führt die Citrix ADC Appliance Lastausgleich, Content Switching durch und fungiert als Relay-Agent. Darüber hinaus bietet die Appliance Rewrite und Responder Funktionalität. Die Appliance unterstützt die Begrenzung der Durchmessermeldungen.

Weitere Informationen finden Sie unter Konfigurieren des Durchmesser-Lastenausgleichs.

Bereitstellung von DNS-Infrastruktur-/Verkehrsdiensten wie Lastenausgleich, Caching und Protokollierung für Telekommunikationsdienstanbieter

October 5, 2021

Telekommunikationsdienstanbieter können die Citrix ADC Appliance so konfigurieren, dass sie als DNS-Proxy fungiert. Die Zwischenspeicherung von DNS-Einträgen, die eine wichtige Funktion eines DNS-Proxy darstellt, ist standardmäßig auf der Citrix ADC Appliance aktiviert. Auf diese Weise kann die Citrix ADC Appliance schnelle Antworten auf wiederholte Übersetzungen bereitstellen, wodurch die Kundenerfahrung verbessert und die Bandbreite gespart wird. Die Zwischenspeicher der Antworten von DNS-Nameservern. Wenn die Appliance eine DNS-Abfrage empfängt, sucht sie in ihrem Cache nach der abgefragten Domäne. Wenn die Adresse der abgefragten Domäne im Cache vorhanden ist, gibt die Citrix ADC Appliance die entsprechende Adresse an den Client zurück. Andernfalls wird die Abfrage an einen DNS-Nameserver weitergeleitet, der die Verfügbarkeit der Adresse überprüft und an die Citrix ADC Appliance zurückgibt. Die Citrix ADC Appliance gibt dann die Adresse an den Client zurück.

Bei Anforderungen für eine Domäne, die zuvor zwischengespeichert wurde, dient die Citrix ADC Appliance den Adressdatensatz der Domäne aus dem Cache, ohne den konfigurierten DNS-Server abzufragen und speichert somit die Bandbreite.

Ab Version 11.0 protokolliert Citrix ADC auch die empfangenen DNS-Anforderungen sowie die an den Client gesendeten Antworten. Telekommunikationsdienstanbieter können dieses Protokoll verwenden, um:

- Überwachen der DNS-Antworten auf den Client
- Überwachen von DNS-Clients
- DNS-Angriffe erkennen und verhindern
- Problembehandlung

Weitere Informationen finden Sie unter Domänennamensystem.

Bereitstellung der Lastverteilung des Teilnehmers mittels GSLB über Kernnetzwerke eines Telekommunikationsdienstanbieters

October 5, 2021

Skalierbarkeit, hohe Verfügbarkeit und Leistung sind für Bereitstellungen von Service Providern entscheidend. Während viele Dienstanbieter dort Infrastruktur an einem einzelnen Standort oder an

mehreren Standorten bereitstellen, unterliegen diese Bereitstellungen einer Reihe von inhärenten Einschränkungen, z. B.:

- Wenn die Site die Konnektivität mit dem gesamten öffentlichen Internet oder einem Teil verliert, ist es für Benutzer und Kunden unzugänglich, was erhebliche Auswirkungen auf das Unternehmen haben kann.
- Benutzer, die von geografisch entfernten Standorten aus auf die Site zugreifen, können große und sehr variable Verzögerungen auftreten, die durch die große Anzahl von Roundtrips, die HTTP für die Übertragung von Inhalten benötigt, verschlimmert werden.

Der Global Server Load Balancing (GSLB) der Citrix ADC Appliance bewältigt diese Probleme, indem der Datenverkehr auf Standorte verteilt wird, die an mehreren geografischen Standorten bereitgestellt werden. Durch die Bereitstellung von Inhalten aus vielen verschiedenen Punkten im Internet lindert GSLB die Auswirkungen von Engpässen der Netzwerkbandbreite und bietet Robustheit bei Netzwerkausfällen an einem bestimmten Standort. Benutzer können zum Zeitpunkt der Anfrage automatisch zur nächstgelegenen oder am wenigsten geladenen Site weitergeleitet werden, wodurch die Wahrscheinlichkeit langer Downloadverzögerungen und/oder Serviceunterbrechungen minimiert wird.

Sie können den globalen Server-Lastausgleich der Citrix ADC Appliance für folgende Zwecke verwenden:

- Disaster Recovery oder hohe Verfügbarkeit durch Konfigurieren einer Active-Standby-Rechenzentrumseinrichtung, die aus einem aktiven und einem Standby-Rechenzentrum besteht. Wenn ein Failover als Folge eines Notfallereignisses auftritt, wird das Standby-Rechenzentrum betriebsbereit.
- Hohe Verfügbarkeit und Geschwindigkeit durch Konfigurieren eines Active-Active-Active-Rechenzentrums, das aus mehreren aktiven Rechenzentren besteht. Clientanforderungen werden über aktive Rechenzentren hinweg Lastausgleich durchgeführt.
- Verweisen von Clientanforderungen an das Rechenzentrum, das in geografischer Entfernung oder Netzwerkentfernung am nächsten ist, indem Sie eine Näherungseinrichtung konfigurieren.
- Voll-DNS-Auflösungen, GSLB verarbeitet DNS-Abfragen der Typen A, AAAA und CNAME, und die DNS-Funktionsoption kann DNS-Abfragen aller anderen Typen verarbeiten, wie MX und PTR. Wenn die rekursive Auflösung aktiviert ist, leitet die Appliance DNS-Abfragen für Domänennamen weiter, die nicht auf der Citrix ADC Appliance konfiguriert sind.

Weitere Informationen finden Sie unter Globaler Server-Lastenausgleich.

Bandbreitenauslastung mit Cache-Umleitungsfunktionalität

October 5, 2021

Das Datenvolumen im Internet ist enorm, und ein großer Prozentsatz des Datenverkehrs ist überflüssig. Mehrere Clients fragen Webserver immer wieder nach demselben Inhalt, was zu einer ineffizienten Nutzung der Bandbreite führt. Um den Ursprungswebserver bei der Verarbeitung jeder Anforderung zu entlasten, können Internetdienstanbieter (ISPs) die Cache-Umleitungsfunktion der Citrix ADC Appliance verwenden und den Inhalt von einem Cacheserver anstelle vom Ursprungsserver bereitstellen. Die Citrix ADC Appliance analysiert eingehende Anforderungen, sendet Anforderungen für zwischenspeicherbare Daten an Cacheserver und sendet nicht zwischenspeicherbare Anforderungen und dynamische HTTP-Anforderungen an Ursprungsserver. Die Cache-Umleitungsfunktion von Citrix ADC ist richtlinienbasiert. Standardmäßig werden Anforderungen, die einer Richtlinie entsprechen, an den Ursprungsserver gesendet, und alle anderen Anforderungen werden an einen Cacheserver gesendet. Sie können Content Switching mit Cache-Umleitung kombinieren, um selektive Inhalte zwischenzuspeichern und Inhalte von bestimmten Cacheservern für bestimmte Arten von angeforderten Inhalten bereitzustellen.

Weitere Informationen finden Sie unter Cache-Umleitung.

Citrix ADC TCP-Optimierung

October 5, 2021

Die Citrix ADC Appliance bietet fortschrittliche TCP-Tuning- und Optimierungstechniken und -funktionen, die sich gut für moderne 3,5- und 4G-Netzwerke eignen, wodurch die Benutzererfahrung und die wahrgenommenen Download-Geschwindigkeiten deutlich verbessert werden.

Dieser Abschnitt konzentriert sich auf detaillierte Anweisungen, die relevant sind für:

- Auswählen und Einfügen eines geeigneten Citrix ADC T1000 Series Modells in ein mobiles Netzwerk zur TCP-Optimierung
- Vollständige Konfigurationsanweisungen nicht nur zur TCP-Optimierung sondern auch zur entsprechenden Layer-2- und Layer-3-Konfiguration des T1-Geräts

Der Abschnitt enthält die folgenden Themen:

- Schnelleinstieg
- Management-Netzwerk
- Lizenzierung
- Hohe Verfügbarkeit
- Gi-LAN-Integration

Schnelleinstieg

October 5, 2021

Hardware

Citrix bietet eine Vielzahl von Citrix ADC Modellen, die locker auf zwei Faktoren basieren können:

- Kapazität, die derzeit von Hunderten von Mbit/s für die Low-End-VPX-Appliance bis zu 160 Gbit/s für die High-End-Appliance der 25000 MPX-Serie reicht
- Telekommunikationsgrad, mit der Verfügbarkeit der T1000-Serie für Telco-Rechenzentren.

Ihr Citrix Vertriebs- oder Support-Mitarbeiter unterstützt Sie bei der Auswahl der geeigneten Hardware für Ihre Demo-, Test- oder Produktionsanforderungen.

Der Rest dieses Abschnitts verwendet einen Citrix ADC T1200 als Referenzhardware. Beachten Sie, dass oberflächliche Unterschiede* in Bezug auf Anzahl und Notation verfügbarer Schnittstellen (siehe Anmerkung) oder gut dokumentierte Einschränkungen von Citrix ADC VPX (siehe* Anmerkung) die Anweisungen gelten sollten. meist wörtlich unabhängig vom ausgewählten Citrix ADC Modell.

> **Hinweis:**
>
> * Zum Beispiel hat ein T1010-Modell nur 12x1GbE typischerweise als 1/1-1/12 markiert und nicht die in diesem Dokument verwendete 10/x-Notation.
>
> ** Eine Citrix ADC VPX Instanz unterstützt normalerweise keine LACP-Aggregation. Möglicherweise unterstützt sie auch kein VLAN-Tagging.

Erstinstallation

Über die serielle Konsole

Nachdem ein serielles Kabel angeschlossen ist, können Sie sich mit den folgenden Anmeldeinformationen bei der Citrix ADC Appliance anmelden:

- Benutzername:nsroot
- Kennwort:nsroot

Konfigurieren Sie nach der Anmeldung die grundlegenden Details der Citrix ADC Appliance, wie in der folgenden Bildschirmaufzeichnung dargestellt.

Beispiel:

```
set ns config  - IPAddress <ip_addr> -netmask <netmask>

saveconfig

reboot -warm
<!--NeedCopy-->
```

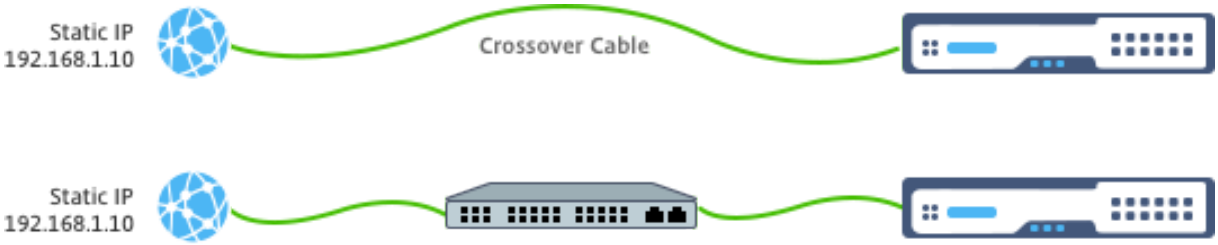
Nach dem Neustart der Appliance können Sie SSH für die weitere Konfiguration der T1100-Knoten verwenden.

Über LOM

Lights out Management (LOM) Port auf der Vorderseite der Citrix ADC Appliance ermöglicht es dem Bediener, die Appliance unabhängig vom Betriebssystem remote zu überwachen und zu verwalten. Der Betreiber kann die IP-Adresse, den Energiesparzyklus ändern und einen Codeabzug durchführen, indem er über den LOM-Port eine Verbindung mit der Citrix ADC Appliance herstellt.

Standard-IP-Adresse des LOM-Ports ist 192.168.1.3

Abbildung. Intiale Konfiguration des LOM-Moduls



Legen Sie eine statische IP auf Ihrem Laptop fest und schließen Sie sie direkt an die LOM-Schnittstelle mit einem Crossover-Kabel oder an einen Switch in derselben Broadcast-Domäne wie die LOM-Schnittstelle an.

Geben Sie zur Erstkonfiguration die Standardadresse des Ports ein: http://192.168.1.3 in einem Webbrowser, und ändern Sie die Standard-IP-Adresse des LOM-Ports.

Weitere Informationen finden Sie in den Konfigurationshandbüchern.

Software

Die Citrix ADC TCP-Optimierung für mobile Netzwerke wird ständig weiterentwickelt. Die in diesem Dokument beschriebenen Funktionen und Tunings erfordern einen Citrix ADC-Telco-Build. Hier ist ein Beispiel, das den Citrix ADC Telco Build zeigt.

Beispiel:

```
show ver

NetScaler NS11.0: Build 64.957.nc, Date: Aug 26 2016, 02:00:23
<!--NeedCopy-->
```

Wenn der T1000 nicht mit der entsprechenden Build-Revision ausgeliefert wurde, wenden Sie sich an den Citrix ADC Customer Support.

> **Wichtig**
>
> Beide Appliances sollten das gleiche Software-Image haben.

SSH-Client

Eine Citrix ADC Appliance kann mit der CLI oder der HTML5-GUI konfiguriert werden. Dieser Abschnitt enthält jedoch nur CLI-basierte Anweisungen.

Während auf die CLI über die serielle Citrix ADC Konsole zugegriffen wird, wird normalerweise ein SSH-Client empfohlen, um die Citrix ADC-Remotekonfiguration zu ermöglichen.

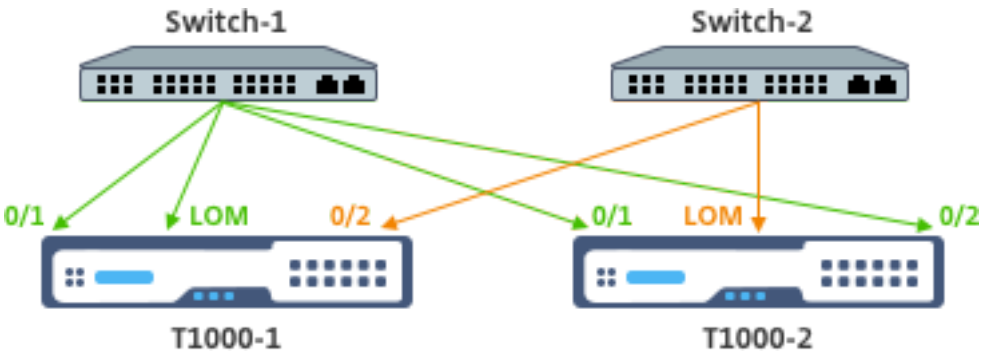
Management-Netzwerk

October 5, 2021

Verbindungen

Die meisten Citrix ADC Geräte bieten redundante 1-GbE-OAM-Ports, die als 0/1 und 0/2 notiert werden. Um bei einem Switch-Ausfall Redundanz zu gewährleisten, sollten Sie die entsprechenden Ports an verschiedene Upstream-Switches anschließen.

Eine Übersicht über die empfohlenen Konnektivität finden Sie im folgenden Diagramm:



Nachdem die Citrix ADC Appliance mit dem Verwaltungsnetzwerk verbunden ist, können nachfolgende Konfigurationsschritte remote über SSH- oder Webkonnektivität mit CLI bzw. GUI durchgeführt werden.

Routing

Der Befehl route hinzufügen kann verwendet werden, um Routen zu konfigurieren, die für das Verwaltungsnetzwerk geeignet sind. Das relevante Gateway sollte im NSIP-Subnetz erreichbar sein, wie unten gezeigt.

Beispiel:

```
add route <network>  <netmask>  <gateway>
<!--NeedCopy-->
```

Lizenzierung

October 5, 2021

Eine gültige Lizenzdatei sollte auf der Citrix ADC Appliance installiert werden. Die Lizenz sollte mindestens so viele Gbit/s unterstützen wie der erwartete maximale Gi-LAN-Durchsatz.

Lizenzdateien sollten über einen SCP-Client in die /nsconfig/license der Appliance kopiert werden, wie in der Bildschirmaufnahme unten gezeigt.

Beispiel:

```
shell ls /nsconfig/license/

CNS_V3000_SERVER_PLT_Retail.lic ssl
```



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

Führen Sie einen warmen Neustart durch, um die neue Lizenz anzuwenden, wie in der Bildschirmaufnahme unten gezeigt.

Beispiel:

```
reboot -warm

Are you sure you want to restart NetScaler (Y/N)? [N]:y

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

Nachdem der Neustart abgeschlossen ist, stellen Sie sicher, dass die Lizenz ordnungsgemäß angewendet wurde, indem Sie die Show License CLI verwenden.

Im folgenden Beispiel wurde eine 3Gbps Premium-Lizenz erfolgreich installiert.

Beispiel:

```
> show license

              License status:

                                    Web Logging: YES

                                             ...

                                 Model Number ID: 3000

                                    License Type: Premium License

Done

<!--NeedCopy-->
```

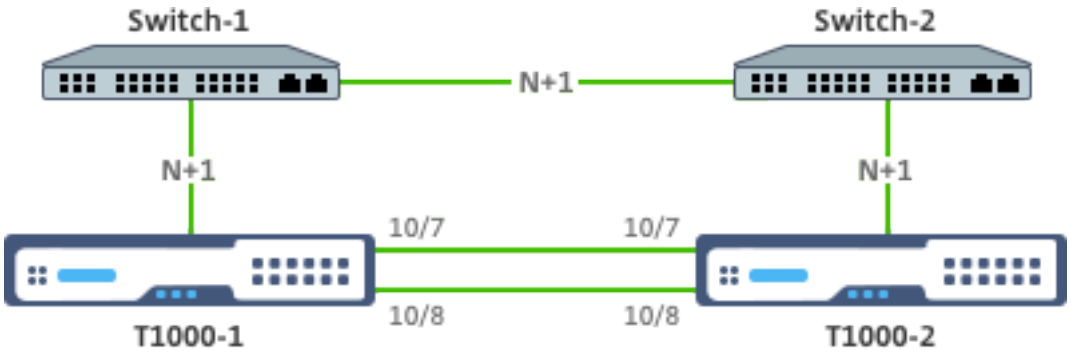
Hohe Verfügbarkeit

October 5, 2021

Hochverfügbarkeit (HA) bezieht sich auf einen Aktiv-Standby-Betriebsmodus eines Citrix ADC Gerätepaares. Jedes Gerät verfügt über eine eigene dedizierte Verwaltungs-IP-Adresse. Alle anderen IP-Adressen gehören dem aktiven Gerät im Paar.

Verbindungen

Zwar gibt es mehrere Konnektivitätsoptionen für ein Citrix ADC HA-Paar, die am häufigsten empfohlene ist im folgenden Diagramm dargestellt:



Im obigen Diagramm implizieren die roten N+1-Verbindungen zwischen jedem T1000 und dem jeweiligen Switch N+1-Redundanz - wie in Konnektivitäterläutert. Zum Beispiel ist ein 45 Gbps Gi-LAN N=5 ein geeigneter Wert, mit 6x10GbE LACP-Kanälen zwischen jedem Switch und dem entsprechenden T1000 sowie zwischen den beiden Switches.

Es wird ein zusätzliches Verknüpfungspaar zwischen dem Citrix ADC Paar empfohlen, um die HA-Kommunikation vom OAM-Netzwerk zu isolieren.

Gi-LAN-Integration

December 3, 2021

In der Regel wird eine Citrix ADC Appliance als separater L3-Inline-Knoten in das Gi-LAN eingefügt, ähnlich einem L3-Router.

Abbildung: Eine einfache Darstellung eines Gi-LAN

Verbindungen

Eine physische Citrix ADC-Konnektivität zu Upstream-Switches wird empfohlen, um eine ausreichende Redundanz zu gewährleisten. Angenommen, eine Citrix ADC Appliance ist in ein Gi-LAN eingefügt, das insgesamt 24 Gbit/s (Uplink+Downlink) verarbeitet, wird eine Konnektivität mit 4x10GbE oder mehr Schnittstellen empfohlen. Dies sorgt effektiv für eine N+1-Redundanz bei einem Verbindungsausfall.

Die entsprechenden Ports auf dem Upstream-Switch sollten für die LACP-Port-Aggregation konfiguriert werden. Die entsprechende Konfiguration auf Citrix ADC ist unten beschrieben:

Konnektivität Konfiguration:

```
set interface 10/1 -tagall ON -lacpMode ACTIVE -lacpKey 1

set interface 10/2 -tagall ON -lacpMode ACTIVE -lacpKey 1

set interface 10/3 -tagall ON -lacpMode ACTIVE -lacpKey 1

set interface 10/4 -tagall ON -lacpMode ACTIVE -lacpKey 1
<!--NeedCopy-->
```

Sie können die entsprechenden Funktionen von LACP mit dem Befehl “show interface” überprüfen:

Schnittstelle zeigen:

```
sh interface LA/1

    1)      Interface LA/1 (802.3ad Link Aggregate) #39

             flags=0x4100c020 <ENABLED, UP, AGGREGATE, UP, HAMON, 802.1
                q>

             MTU=1500, native vlan=1, MAC=02:e0:ed:33:88:b0, uptime 340
                h11m56s

             Requested: media NONE, speed AUTO, duplex NONE, fctl NONE,

             throughput 0

             Actual: throughput 4000

             LLDP Mode: NONE,
```



```
16
17              RX: Pkts(918446) Bytes(110087414) Errs(0) Drops(795989)
                    Stalls(0)
18
19              TX: Pkts(124113) Bytes(15255532) Errs(0) Drops(0) Stalls
                    (0)
20
21              NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0)
                    Muted(0)
22
23              Bandwidth thresholds are not set.
24
25 Disable the remaining unused interfaces and turn off the monitor.
26
27 set interface 10/5  -haMonitor OFF
28 <!--NeedCopy-->
```

Befehl:

```
1 set interface 10/24  -haMonitor OFF
2
3 disable interface 10/5
4
5 disable interface 10/24
6 <!--NeedCopy-->
```

Die Konfiguration physischer Schnittstellen wird nicht von den beiden Citrix ADC-Einheiten gemeinsam genutzt. Daher müssen die obigen Befehle im Falle einer HA-Paarbereitstellung auf beiden Citrix ADC-Knoten ausgeführt werden.

HA-Konfiguration

Alle anderen Konfigurationsparameter werden von den Citrix ADC Knoten eines HA-Paars gemeinsam genutzt. Daher sollte die HA-Synchronisierung vor der Ausführung anderer Konfigurationsbefehle aktiviert werden. Die grundlegende HA-Konfiguration umfasst die folgenden Schritte:

1. Verwendung der exakt gleichen Citrix ADC Hardware, Software und Lizenz: HA-Paare werden nicht zwischen verschiedenen Modellen (z. B. einem T1100 und einem MPX21550) oder denselben Modellen mit unterschiedlichen Firmware-Levels unterstützt. Lesen Sie die entsprechenden Anweisungen zum Upgrade eines vorhandenen HA-Paares - Upgrade auf Release 11.1.

2. Gründung des HA-Paars.

Beispiel:

```
netscaler-1> add HA node 1 <netscaler-2-NSIP>

netscaler-2> add HA node 1 <netscaler-1-NSIP>
<!--NeedCopy-->
```

3. Überprüfen Sie, ob die HA-Paar-Einrichtung den folgenden Befehl in beiden Knoten ausführt. Beide Knoten sollten sichtbar sein, einer von ihnen als Primär (aktiv), der andere als sekundärer (Standby).

Beispiel:

```
show HA node
<!--NeedCopy-->
```

4. Aktivieren Sie den ausfallsicheren Modus und MaxFlips. Dadurch wird sichergestellt, dass bei einem Ausfall des Routenmonitors auf beiden Knoten mindestens ein Knoten aktiv bleibt, ohne dass der Aktiv-/Standby-Status ständig wechselt.

Beispiel:

```
set HA node  - failsafe ON

set HA node -maxFlips 3 -maxFlipTime 1200
<!--NeedCopy-->
```

5. Aktivieren Sie abschließend die HA-Synchronisierung über die dedizierten Intra-Citrix ADC-Ports und nicht über das OAM-Netzwerk.

Beispiel:

```
add vlan 4080 -aliasName syncVlan

set HA node -syncvlan 4080
<!--NeedCopy-->
```

> **Hinweis**

> Das VLAN 4080 in den Befehlen im obigen Beispiel sollte nicht wörtlich genommen werden. Jede nicht verwendete VLAN-ID kann reserviert sein.

VLAN-Konfiguration

Nachdem die physikalischen Schnittstellen entsprechend konfiguriert wurden, können Sie die entsprechenden Gi-LAN-VLANs konfigurieren. Stellen Sie sich zum Beispiel eine ziemlich einfache Gi-LAN-Umgebung mit einem Ingress/Egress-VLAN-Paar mit 100/101-VLAN-Kennung vor.

Mit den folgenden Befehlen werden die entsprechenden VLANs über dem im vorherigen Schritt erstellten LACP-Kanal konfiguriert.

```
add vlan 100
add vlan 101
bind vlan 100 -ifnum LA/1 -tagged
bind vlan 101 -ifnum LA/1 -tagged
<!--NeedCopy-->
```

IPv4-Konfiguration

In der Regel benötigt eine Citrix ADC Appliance ein SNIP pro VLAN. Im folgenden Beispiel wird davon ausgegangen, dass die Netzwerke, die im Gi-LAN-Integrationsdiagramm am Anfang dieser Seite beschrieben sind, eine /24-Subnetzmaske haben:

```
add ns ip 192.168.1.254 255.255.255.0 -vserver DISABLED -mgmtAccess
    DISABLED
add ns ip 192.168.2.254 255.255.255.0 -vserver DISABLED -mgmtAccess
    DISABLED
<!--NeedCopy-->
```

Nachdem die SNIPs konfiguriert wurden, sollten sie mit dem entsprechenden VLAN verknüpft werden:

```
bind vlan 100 -IPAddress 192.168.1.254 255.255.255.0
bind vlan 101 -IPAddress 192.168.2.254 255.255.255.0
<!--NeedCopy-->
```


Statisches IPv4-Routing

Das im Abschnitt Management Network beschriebene Beispiel erfordert nur ein paar statische Routing-Regeln:

- Eine statische Route 10.0.0.0/8 zu den Clients über den Eingangs-Router
- Eine Standardroute zum Internet über den Egress-Router

Beispiel:

```
add route 0.0.0.0 0.0.0.0 192.168.2.1
add route 10.0.0.0 255.0.0.0 192.168.1.1
<!--NeedCopy-->
```

IPv4-richtlinienbasiertes (VLAN - VLAN) -Routing

Eine Citrix ADC Appliance ermöglicht richtlinienbasiertes Routing anstelle von statischem Routing, wobei Routing-Entscheidungen normalerweise eher mit der eingehenden Schnittstelle und/oder dem VLAN als mit der Ziel-IP vergeben werden. Richtlinienbasiertes Routing ist entweder eine bequeme Alternative, falls der IP-Adressbereich der Clientquelle regelmäßigen Änderungen unterliegt, oder eine zwingende Überlegung, falls die Ziel-IP-Adresse eines Pakets allein nicht ausreicht, um eine Routingentscheidung zu treffen (d. h. bei sich überlappenden Client-IP-Adressen über mehrere VLANs hinweg).

Beispiel:

```
add ns pbr fromWirelessToInternet ALLOW -nextHop 192.168.2.1 -vlan
    100 -priority 10

Done

 add ns pbr fromInternetToWireless ALLOW -nextHop 192.168.1.1 -vlan
     200 -priority 20

Done

apply ns pbrs
<!--NeedCopy-->
```


IPv6-Konfiguration

Die folgenden Befehle weisen IPv6 SNIP pro VLAN zu. Im folgenden Beispiel wird davon ausgegangen, dass die in der Abbildung skizzierten Netzwerke: Eine einfache Darstellung eines Gi-LAN auf dieser Seite eine /64-Subnetzmaske haben:

Befehl:

```
add ns ip6 fd00:192:168:1::254/64 -vServer DISABLED  - mgmtAccess
    DISABLED
add ns ip6 fd00:192:168:2::254/64 -vServer DISABLED  - mgmtAccess
    DISABLED
bind vlan 100 -IPAddress fd00:192:168:1::254/64
bind vlan 200 -IPAddress fd00:192:168:2::254/64
<!--NeedCopy-->
```

IPv6-Routing

Nachdem die IPv6-Adressierung abgeschlossen ist, kann das statische IPv6-Routing konfiguriert werden:

- Eine fd 00:10: :/64 statische Route zu den Clients über den Ingress-Router
- Eine Standardroute zum Internet über den Egress-Router

Beispiel:

```
add route6 fd00:10::/64 fd00:192:168:1::1
add route6 ::/0 fd00:192:168:2::1
<!--NeedCopy-->
```

Oder mit richtlinienbasiertem Routing:

Beispiel:

```
add ns pbr6 fromWirelessToInternetv6 ALLOW -vlan 100 -priority 10 -
    nextHop fd00:192:168:2::1

add ns pbr6 fromInternetToWirelessv6 ALLOW -vlan 200 -priority 20 -
    nextHop fd00:192:168:1::1

apply ns pbr6
<!--NeedCopy-->
```


LACP-Redundanz und Failover

Im Falle einer HA-Konfiguration wird empfohlen, die Durchsatzoption zu nutzen, um einen niedrigen Schwellenwert für den LACP-Kanal zu konfigurieren. Stellen Sie sich beispielsweise ein 25-Gbit/s-Gi-LAN und einen 4x10GbE-Kanal zwischen jeder Citrix ADC Appliance im HA-Paar und dem Upstream-Switch vor, um eine N+1-Link-Redundanz bereitzustellen:

Beispiel:

```
1 set interface LA/1 -haMonitor ON -throughput 29000
2 <!--NeedCopy-->
```

Im Falle eines Double-Link-Ausfalls zwischen dem primären Gerät und dem Upstream-Switch würde der maximal unterstützte Gi-LAN-Durchsatz auf 20 Gbit/s sinken. Ein niedriger Schwellenwert von 29 Gbit/s gemäß dem obigen Beispiel würde zu einem Redundanz-Switchover-Ereignis zum sekundären Gerät führen (das keine ähnlichen Verbindungsausfälle erlitten hat), sodass der Gi-LAN-Verkehr nicht beeinträchtigt wird.

Routen-Monitore

Zusätzlich zur LACP-Redundanz können Routenüberwachungsprüfungen konfiguriert und mit der HA-Paar-Konfiguration verknüpft werden. Routenüberwachungsprüfungen können nützlich sein, um Fehler zwischen der Citrix ADC Appliance und den Next-Hop-Routern zu erkennen, insbesondere wenn diese Router nicht direkt, sondern über einen Upstream-Switch verbunden sind.

Eine typische Konfiguration des HA-Routenmonitors gemäß dem Beispiel Gi-LAN in Abschnitt 2.5.1 ist nachstehend beschrieben:

```
1 add route 192.168.1.0 255.255.255.0 192.168.1.1 -msr ENABLED -monitor
     arp
2 add route 192.168.2.0 255.255.255.0 192.168.2.1 -msr ENABLED -monitor
     arp
3 bind HA node -routeMonitor 192.168.1.0 255.255.255.0
4 bind HA node -routeMonitor 192.168.2.0 255.255.255.0
5 <!--NeedCopy-->
```

TCP-Optimierungskonfiguration

October 5, 2021

Wenden Sie vor der Konfiguration der TCP-Optimierung die folgenden grundlegenden Konfigurationseinstellungen auf der Citrix ADC Appliance an:

Erstkonfiguration:

```
enable ns feature LB IPv6PT
enable ns mode FR L3 USIP MBF Edge USNIP PMTUD
disable ns feature SP
disable ns mode TCPB
set lb parameter -preferDirectRoute NO
set lb parameter -vServerSpecificMac ENABLED
set l4param -l2ConnMethod Vlan
set rsskeytype -rsstype SYMMETRIC
set ns param -useproxyport DISABLED
<!--NeedCopy-->
```

> **Hinweis:**
>
> Starten Sie die Citrix ADC Appliance neu, wenn Sie den Systemparameter rsskeytype ändern.

TCP-Beendigung

Damit Citrix ADC T1 TCP-Optimierung anwenden kann, muss der eingehende TCP-Datenverkehr zuerst beendet werden. Zu diesem Zweck sollte ein Platzhalter-TCP-vserver erstellt und konfiguriert werden, um eingehenden Datenverkehr abzufangen und dann an den Internet-Router weiterzuleiten.

Statische oder dynamische Routing-Umgebung

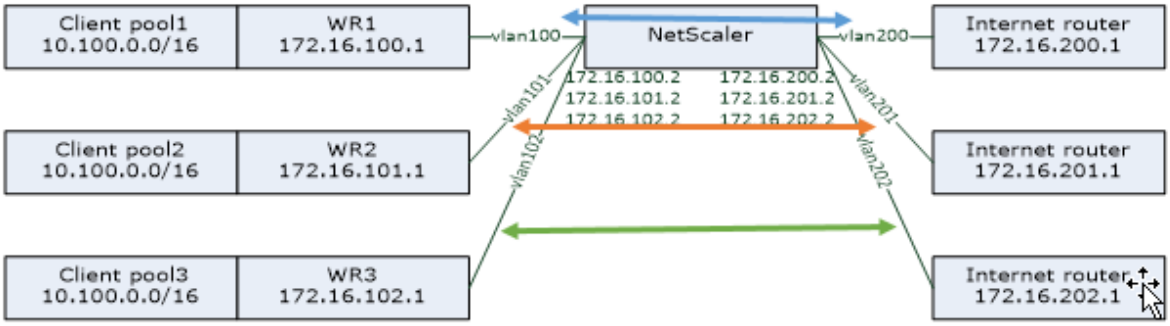
In Umgebungen mit statischem oder dynamischem Routing kann vserver auf Routingtabelleninformationen verlassen, um Pakete an den Internet-Router weiterzuleiten. Die Standardroute muss auf den Internet-Router zeigen und auch Routingeinträge für Client-Subnetze zum drahtlosen Router sollten vorhanden sein:

Beispiel:

```
add lb vserver vsrv-wireless TCP * * -persistenceType NONE -
    Listenpolicy "CLIENT.VLAN.ID.EQ(100) && SYS.VSERVER("vsrv-wireless")
    .STATE.EQ(UP)" -m IP -cltTimeout 9000
add route 0.0.0.0 0.0.0.0 192.168.2.1
add route 10.0.0.0 255.0.0.0 192.168.1.1
<!--NeedCopy-->
```


VLAN-zu-VLAN-Umgebung (PBR)

Es gibt Kundenumgebungen, in denen Teilnehmerdatenverkehr in mehrere Flows segmentiert wird und basierend auf eingehenden Datenverkehrsparametern an verschiedene Router weitergeleitet werden muss. Policy Based Routing (PBR) kann verwendet werden, um Pakete basierend auf eingehenden Paketparametern wie VLAN, MAC-Adresse, Schnittstelle, Quell-IP, Quell-Port, Ziel-IP-Adresse und Ziel-Port weiterzuleiten.



Beispiel:

```
add lb vserver vsrv-wireless TCP * * -m IP -l2Conn ON -listenpolicy "
    CLIENT.VLAN.ID.EQ(100) || CLIENT.VLAN.ID.EQ(101) || CLIENT.VLAN.ID.
    EQ(102)"

add ns pbr pbr-vlan100-to-vlan200 ALLOW -vlan 100 -nexthop 172.16.200.1

add ns pbr pbr-vlan101-to-vlan201 ALLOW -vlan 101 -nexthop 172.16.201.1

add ns pbr pbr-vlan102-to-vlan202 ALLOW -vlan 102 -nexthop 172.16.202.1
<!--NeedCopy-->
```

Die Verwendung von richtlinienbasiertem Routing zur Weiterleitung von TCP-optimiertem Datenverkehr ist eine neue Funktion, die in Version 11.1 50.10 hinzugefügt wurde. Für frühere Versionen ist die Verwendung mehrerer Modus MAC -vServer-Entitäten pro VLAN eine alternative Lösung für Multi-VLAN-Umgebungen. Jeder vserver verfügt über einen gebundenen Dienst, der den Internet-Router für den jeweiligen Fluss darstellt.

Beispiel:

```
add server internet_router_1 172.16.200.1

add server internet_router_2 172.16.201.1
```



```
4
5  add server internet_router_3 172.16.202.1
6
7  add service svc-internet-1 internet_router_1 TCP * -usip YES -
       useproxyport NO
8
9  add service svc-internet-2 internet_router_2 TCP * -usip YES -
       useproxyport NO
10
11 add service svc-internet-3 internet_router_3 TCP * -usip YES -
       useproxyport NO
12
13 bind service svc-internet-1 -monitorName arp
14
15 bind service svc-internet-2 -monitorName arp
16
17 bind service svc-internet-3 -monitorName arp
18
19 add lb vserver vsrv-wireless-1 TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ
       (100) && SYS.VSERVER("vsrv-wireless-1").STATE.EQ(UP)" -m MAC -l2Conn
        ON
20
21 add lb vserver vsrv-wireless-2 TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ
       (101) && SYS.VSERVER("vsrv-wireless-2").STATE.EQ(UP)" -m MAC -l2Conn
        ON
22
23 add lb vserver vsrv-wireless-3 TCP * * -Listenpolicy "CLIENT.VLAN.ID.EQ
       (102) && SYS.VSERVER("vsrv-wireless-3").STATE.EQ(UP)" -m MAC -l2Conn
        ON
24
25 bind lb vserver vsrv-wireless-1 svc-internet-1
26
27 bind lb vserver vsrv-wireless-2 svc-internet-2
28
29 bind lb vserver vsrv-wireless-3 svc-internet-3
30 <!--NeedCopy-->
```

Hinweis:

Der vserver-Modus ist MAC im Gegensatz zu früheren Beispielen, bei denen es sich um Mode IP handelt. Dies ist erforderlich, um die Ziel-IP-Informationen beizubehalten, wenn wir Dienste an vserver gebunden haben. Außerdem muss die zusätzliche PBR-Konfiguration nicht optimierten Datenverkehr weitergeleitet werden.

TCP-Optimierung

Die vorkonfigurierte Citrix ADC TCP-Beendigung ist für die TCP-Passthrough-Funktionalität konfiguriert. TCP-Pass-Through bedeutet im Wesentlichen, dass Citrix ADC T1 einen Client-Server-TCP-Stream transparent abfangen kann, aber keine separaten Client/Server-Puffer behält oder anderweitig Optimierungstechniken angewendet werden.

Um die TCP-Optimierung zu aktivieren, wird ein TCP-Profil mit dem Namen nstcpprofile verwendet, um TCP-Konfigurationen anzugeben, die verwendet werden, wenn keine TCP-Konfigurationen auf Dienst- oder virtueller Serverebene bereitgestellt werden, und es sollte wie folgt geändert werden:

Befehl:

```
1 add ns tcpProfile nstcpprofile -WS ENABLED -SACK ENABLED -WSVal 8 -mss
      1460 -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
      bufferSize 4000000 -flavor BIC -dynamicReceiveBuffering ENABLED -KA
      ENABLED -sendBuffsize 4000000 -rstWindowAttenuate ENABLED -
      spoofSynDrop ENABLED -ecn ENABLED -frto ENABLED -maxcwnd 1000000 -
      fack ENABLED -rstMaxAck enABLED -tcpmode ENDPOINT
2 <!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn kein Profil explizit erstellt und an vserver und service gebunden ist, ist das Profil nstcp_default_profile standardmäßig gebunden.
>
> Bei mehreren TCP-Profilen können zusätzliche TCP-Profile erstellt und mit dem entsprechenden virtuellen Server verknüpft werden.

Befehl:

```
1 add ns tcpProfile custom_profile -WS ENABLED -SACK ENABLED -WSVal 8 -
      mss 1460 -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
      bufferSize 4000000 -flavor BIC -dynamicReceiveBuffering ENABLED -KA
      ENABLED -sendBuffsize 4000000 -rstWindowAttenuate ENABLED -
      spoofSynDrop ENABLED -ecn ENABLED -frto ENABLED -maxcwnd 1000000 -
      fack ENABLED -rstMaxAck enABLED -tcpmode ENDPOINT
2
3 set lb vserver vsrv-wireless -tcpProfileName custom_profile
4 <!--NeedCopy-->
```


> **Hinweis:**
>
> Bei Bereitstellungen mit vserver -m MAC und Service sollte dasselbe Profil dem Dienst zugeordnet werden.

```
set service svc-internet -tcpProfileName custom_profile
<!--NeedCopy-->
```

TCP-Optimierungsfunktionen

Die meisten relevanten TCP-Optimierungsfunktionen einer Citrix ADC Appliance werden über ein entsprechendes TCP-Profil bereitgestellt. Typische CLI-Parameter, die beim Erstellen eines TCP-Profils berücksichtigt werden sollten, sind die folgenden:

1. **Window Scaling (WS)**: Die TCP-Fensterskalierung ermöglicht die Erhöhung der TCP-Empfangsfenstergröße über 65535 Bytes hinaus. Es hilft, die TCP-Leistung insgesamt und speziell in Netzwerken mit hoher Bandbreite und langer Verzögerung zu verbessern. Es hilft, die Latenz zu reduzieren und die Reaktionszeit über TCP zu verbessern.
2. **Selective Acknowledgment (SACK)**: TCP SACK löst das Problem des Mehrfachpaketverlustes, wodurch die Gesamtdurchsatzkapazität reduziert wird. Mit selektiver Quittierung kann der Empfänger den Absender über alle erfolgreich empfangenen Segmente informieren, sodass der Absender nur die verlorenen Segmente weiterleiten kann. Diese Technik hilft T1, den Gesamtdurchsatz zu verbessern und die Verbindungslatenz zu reduzieren.
3. **Window Scaling Factor (WSVal)**: Faktor, der zur Berechnung der neuen Fenstergröße verwendet wird. Es muss mit einem hohen Wert konfiguriert werden, damit das angekündigte Fenster von NS mindestens der Puffergröße entspricht.
4. **Maximale Segmentgröße (MSS)**: MSS eines einzelnen TCP-Segments. Dieser Wert hängt von der MTU-Einstellung auf Zwischenroutern und Endclients ab. Ein Wert von 1460 entspricht einer MTU von 1500.
5. **MaxBurst**: Maximale Anzahl zulässiger TCP-Segmente in einer Aufgliederung.
6. **Initial Congestion Window Size (InitialCWnd)**: Die Größe des anfänglichen TCP-Staufensters bestimmt die Anzahl der Bytes, die zu Beginn der Transaktion ausstehen können. Es ermöglicht T1, diese vielen Bytes zu senden, ohne sich für Staus auf der Leitung zu belästigen.
7. **Maximale Größe der OOO-Paketwarteschlange (OOQSize)**: TCP verwaltet die Warteschlange Out Of Order, um die OOO-Pakete in der TCP-Kommunikation beizubehalten. Diese Einstellung wirkt sich auf den Systemspeicher aus, wenn die Warteschlangengröße lang ist, wie die Pakete im Laufzeitspeicher aufbewahrt werden müssen. Dies muss daher auf der Grundlage der Netzwerk- und Anwendungseigenschaften optimiert gehalten werden.
8. **Minimaler RTO (minRTO)**: Der TCP-Neuübertragungs-Timeout wird auf jeder empfangenen ACK basierend auf der internen Implementierungslogik berechnet. Das Standard-Timeout für

die erneute Übertragung erfolgt bei 1 Sekunde, um mit zu beginnen und dies kann mit dieser Einstellung optimiert werden. Für die zweite Weiterleitung dieser Pakete wird RTO von N*2 berechnet und dann N*4… N*8… geht bis zum letzten erneuten Übermittlungsversuch weiter.

9. **BufferSize/SendBuffSize**: Diese beziehen sich auf die maximale Datenmenge, die der T1 vom Server empfangen und intern Puffer empfangen kann, ohne an den Client zu senden. Sie sollten auf einen Wert gesetzt werden, der größer (mindestens doppelt) ist als das Bandbreitenverzögerungsprodukt des zugrunde liegenden Übertragungskanals.
10. **flavor**: Dies bezieht sich auf den TCP-Staukontrollalgorithmus. Gültige Werte sind Default, BIC, CUBIC, Westwood und Nile.
11. **Dynamische Empfangspufferung**: Ermöglicht die dynamische Anpassung des Empfangspuffers basierend auf Speicher- und Netzwerkbedingungen. Es füllt den Puffer so viel, wie es erforderlich ist, um die Download-Pipe des Clients voll zu halten, anstatt zu füllen, indem Sie vorab vom Server einen Puffer mit fester Größe lesen, wie letzterer im TCP-Profil angegeben ist und normalerweise auf Kriterien wie 2*BDP für eine Verbindung basiert. Citrix ADC T1 überwacht die Netzwerkbedingungen für den Client und schätzt, wie viel es vom Server vorgelesen werden soll.
12. **Keep-Alive (KA)**: Senden Sie periodische TCP-Keep-Alive-Prüfpunkte (KA), um zu überprüfen, ob Peer noch aktiv ist.
13. RSTWindowAttenuate: Verteidigung von TCP gegen Spoofing-Angriffe. Es wird mit korrigierenden ACK antworten, wenn eine Sequenznummer ungültig ist.
14. **RstMaxack**: Aktivieren oder deaktivieren Sie die Akzeptanz von RST, die außerhalb des Fensters ist, aber die höchste ACK-Sequenznummer widerspiegelt.
15. **SpoofSyndrop: Löschen**ungültiger SYN-Pakete zum Schutz vor Spoofing.
16. **Explizite Congestion Notification (ecn)**: Es sendet eine Benachrichtigung über den Netzwerkstau an den Absender der Daten und ergreift Korrekturmaßnahmen für Datenstaus oder Datenbeschädigung.
17. **Vorwärts-RTO-Recovery**: Im Falle von unechten Wiederübertragungen werden die Congestion Control-Konfigurationen in ihren ursprünglichen Zustand zurückgesetzt.
18. **TCP-Maximalüberlastungsfenster (maxcwnd)**: Maximale TCP-Staufenstergröße, die vom Benutzer konfigurierbar ist.
19. **Forward Acknowledgment (FACK)**: Um TCP-Überlastung zu vermeiden, indem explizit die Gesamtzahl der im Netzwerk ausstehenden Datenbytes gemessen und dem Sender (entweder T1 oder einen Client) dabei geholfen wird, die Menge der Daten zu kontrollieren, die während der Zeitüberschreitung in das Netzwerk injiziert wurden.
20. **tcpmode**: TCP-Optimierungsmodi für ein bestimmtes Profil. Es gibt zwei TCP-Optimierungsmodi - Transparent und Endpunkt.

- Endpunkt. In diesem Modus verwaltet die Appliance die Client- und Serververbindungen separat.
- Transparent. Im transparenten Modus müssen die Clients direkt auf die Server zugreifen, ohne

den dazwischen liegenden virtuellen Server. Die Server-IP-Adressen müssen öffentlich sein, da die Clients darauf zugreifen können müssen. Im Beispiel in der folgenden Abbildung wird eine NetScaler Appliance zwischen dem Client und dem Server platziert, sodass der Datenverkehr durch die Appliance geleitet werden muss.

Leerlauf-Verbindungen stillschweigend löschen

In einem Telekommunikationsnetzwerk sind fast 50 Prozent der TCP-Verbindungen einer Citrix ADC Appliance im Leerlauf, und die Appliance sendet RST-Pakete, um sie zu schließen. Die über Funkkanäle gesendeten Pakete aktivieren diese Kanäle unnötig, was zu einer Flut von Nachrichten führt, die wiederum dazu führen, dass die Appliance eine Flut von Service-Reject-Nachrichten generiert. Das standardmäßige TCP-Profil enthält jetzt die Parameter DropHalfClosedConnOnTimeout und DropEstConnOnTimeout, die standardmäßig deaktiviert sind. Wenn Sie beide aktivieren, bewirkt weder eine halb geschlossene Verbindung noch eine etablierte Verbindung, dass ein RST-Paket an den Client gesendet wird, wenn die Verbindung Timeout. Die Appliance lässt die Verbindung einfach fallen.

```
set ns tcpProfile nstcpprofile  -DropHalfClosedConnOnTimeout ENABLED
set ns tcpProfile nstcpprofile  -DropEstConnOnTimeout ENABLED
<!--NeedCopy-->
```

Analytics und Reporting

October 5, 2021

Das TCP Speed Reporting ist eine Citrix ADC-Funktion, die TCP-Verbindungsstatistiken als Maß für die Download- und Upload-Leistung von TCP extrahiert und in TCP Insight-Berichten des Citrix Application Delivery Management (ADM) verwendet wird. Um dies zu erreichen, überwacht Citrix ADC jede TCP-Verbindung, sucht Paketaufbrüche im Leerlaufzeitlimit und meldet Schlüsselmetriken (z. B. Byteanzahl, Anzahl der wiederübertragenen Byte und Dauer) für die identifizierte maximale Burst. TCP-Geschwindigkeitsberichterstattungsfunktion ist standardmäßig aktiviert, unterstützt sowohl TCP- als auch HTTP-vServer und hängt von der AppFlow/ULFD-Berichtsinfrastruktur ab.

Echtzeit-Statistiken

October 5, 2021

Der Befehl stat kann verwendet werden, um zu überprüfen, ob die TCP-Optimierung ordnungsgemäß angewendet wird:

Befehl:

```
> stat lb vserver vsrv-wireless
Virtual Server Summary
                      vsvrIP  port     Protocol        State   Health
                         actSvcs
vsrv...eless              *     0          TCP           UP      100
           1

            inactSvcs
vsrv...eless       0
Virtual Server Statistics
                                          Rate (/s)
                                             Total
Vserver hits                                    0
    10
Requests                                        0
                      0
Responses                                       0
                      0
Request bytes                                   0
    1580
Response bytes                                  0
    532594360
Total Packets rcvd                              0
    216463
Total Packets sent                              0
    369898
Current client connections                     --
                      0
Current Client Est connections                 --
                      0
Current server connections                     --
                      0
Requests in surge queue                        --
                      0
Requests in vserver's surgeQ                   --
                      0
Requests in service's surgeQs                  --
                      0
Spill Over Threshold                           --
```



```
                          0
24 Spill Over Hits                                --
                          0
25 Labeled Connection                             --
                          0
26 Push Labeled Connection                        --
                          0
27 Deferred Request                                0
                          0
28 Invalid Request/Response                       --
                          0
29 Invalid Request/Response Dropped               --
                          0
30 Bound Service(s) Summary
31                            IP  port         Type        State     Hits
                                    Hits/s
32 svc-internet     192.168.2.2     0          TCP           UP       10
          0/s
33
34                  Req    Req/s      Rsp    Rsp/s Throughp ClntConn
                       SurgeQ
35 svc-internet       0      0/s        0      0/s        0        0
             0
36                   SvrConn   ReuseP  MaxConn ActvTran  SvrTTFB     Load
37 svc-internet         0        0        0        0        0        0
```

Die Gesamtzähler sollten für ein operatives System ständig steigen. Darüber hinaus sollten die Kurszähler ungleich Null sein.

> **Hinweis:**
>
> Die vorhergehende Ausgabe stammt aus einem betriebsbereiten Laborsystem, das die Nullrate erklärt.

SNMP

October 5, 2021

SNMP-Agent kann von einem Remote-Gerät (SNMP-Manager) nach systemspezifischen Informationen abgefragt werden. Basierend auf der Abfrage sucht der Agent nach dem Equal Object Identifier (OID) in der Management Information Base (MIB) für die angeforderten Daten und sendet die Informationen an den SNMP-Manager. Im Folgenden sind die nützlichsten SNMP-OIDs für Telekommunikationsbereitstellungen aufgeführt:

Speicher

- **resMemUsage (1.3.6.1.4.1.5951.4.1.1.41.2)**

Prozentsatz der Speicherauslastung auf Citrix ADC.

Paket-Engine-CPU

- **resCpuUsage (1.3.6.1.4.1.5951.4.1.1.41.1)**

Prozentsatz der CPU-Auslastung.

- **nsCPUTable (1.3.6.1.4.1.5951.4.1.1.41.6)**

Diese Tabelle enthält Informationen zu jeder CPU in Citrix ADC.

Indiziert auf: nsCPUname

- **nsCPUname (1.3.6.1.4.1.5951.4.1.1.41.6.1.1)**

Der Name der CPU.

- **nsCPUusage (1.3.6.1.4.1.5951.4.1.1.41.6.1.2)**

Prozentsatz der CPU-Auslastung.

Durchsatz

- **allNicTotRxMbits (1.3.6.1.4.1.5951.4.1.1.71.1)**

Anzahl der Megabits, die von der Citrix ADC Appliance empfangen werden.

- **allNicTotTxMbits (1.3.6.1.4.1.5951.4.1.1.71.2)**

Anzahl der von der Citrix ADC Appliance übertragenen Megabits.

- **ipTotRxPkts (1.3.6.1.4.1.5951.4.1.1.43.25)**

IP-Pakete empfangen.

- **ipTotRxMbits (1.3.6.1.4.1.5951.4.1.1.43.27)**

Megabit IP-Daten empfangen.

- **ipTotTxPkts (1.3.6.1.4.1.5951.4.1.1.43.28)**

IP-Pakete übertragen.

- **ipTotTxMbits (1.3.6.1.4.1.5951.4.1.1.43.30)**

Megabit IP-Daten übertragen.

Verbindungen

Aktive Verbindungen:

- **tcpActiveServerConn (1.3.6.1.4.1.5951.4.1.1.46.8)**

Verbindungen zu einem Server, der derzeit auf Anforderungen reagiert.

Verbindungen insgesamt:

- **tcpCurServerConn (1.3.6.1.4.1.5951.4.1.1.46.1)**

Serververbindungen, einschließlich Verbindungen im Status Öffnen, Gegründet und Schließen.

- **tcpCurClientConn (1.3.6.1.4.1.5951.4.1.1.46.2)**

Clientverbindungen, einschließlich Verbindungen im Status Öffnen, Gegründet und Schließen.

Hinweis: Aufgrund von SYN-Cookie enthält dies Client nicht im Öffnungszustand

- **tcpTotZombieCltConnFlushed (1.3.6.1.4.1.5951.4.1.1.46.26)**

Clientverbindungen, die geleert werden, weil der Client seit einiger Zeit im Leerlauf war.

- **tcpTotZombieSvrConnFlushed (1.3.6.1.4.1.5951.4.1.1.46.27)**

Serververbindungen, die geleert werden, weil seit einiger Zeit keine Clientanforderungen in der Warteschlange vorhanden sind.

Fehler

- **tcpErrSynGiveUp (1.3.6.1.4.1.5951.4.1.1.46.37)**

Versucht, eine Verbindung mit dem Citrix ADC herzustellen, bei der ein Zeitlimit überschritten wurde.

- **tcpErrRetransmitGiveUp (1.3.6.1.4.1.5951.4.1.1.46.60)**

Häufigkeit, wie oft Citrix ADC eine Verbindung beendet, nachdem das Paket sieben Mal auf dieser Verbindung erneut übertragen wurde. Die erneute Übertragung erfolgt, wenn das Paket nicht bestätigt wird.

- **ifInDiscards (1.3.6.1.2.1.2.2.1.13)**

Die Anzahl der eingehenden Pakete, die für das Verwerfen ausgewählt wurden, obwohl keine Fehler erkannt wurden, um zu verhindern, dass sie in ein höheres Protokoll geliefert werden können. Ein möglicher Grund für das Verwerfen eines solchen Pakets könnte darin liegen, Pufferspeicher freizugeben.

- **ifOutDiscards (1.3.6.1.2.1.2.2.1.19)**

Die Anzahl der ausgehenden Pakete, die für die Verwerfung ausgewählt wurden, obwohl keine Fehler festgestellt wurden, um deren Übertragung zu verhindern. Ein möglicher Grund für das Verwerfen eines solchen Pakets könnte darin liegen, Pufferspeicher freizugeben.

- **ifErrTxOverflow (1.3.6.1.4.1.5951.4.1.1.54.1.36)**

Anzahl der Pakete, die während der Übertragung auf der angegebenen Schnittstelle die Überlaufwarteschlangen durchlaufen haben, da die Citrix ADC Appliance gestartet wurde oder die Schnittstellenstatistiken gelöscht wurden. Dies wird nur bei überlasteten Ports erhöht.

Optimierte/Umgehung von Verbindungen

- **tcpOptimizationEnabled (1.3.6.1.4.1.5951.4.1.1.46.131)**

Gesamtzahl der mit TCP-Optimierung aktivierten Verbindungen.

- **tcpOptimizationBypassed (1.3.6.1.4.1.5951.4.1.1.46.132)**

Die Gesamtanzahl der Verbindungen wurde TCP-Optimierung umgangen.

Technische Rezepte

October 5, 2021

Die Citrix ADC T1-Modelle bieten erweiterte Funktionen und eine leistungsstarke Richtlinienkonfigurationssprache, mit der komplexe Entscheidungen während der Laufzeit ausgewertet werden können.

Obwohl es nicht möglich ist, alle Funktionen zu bewerten, die möglicherweise durch den T1000-Funktionen- und Richtlinienkonfigurationshandbuch freigeschaltet werden, erwägen technische Empfangs die Implementierung verschiedener Anforderungen, die von Telekommunikationsbetreibern eingeführt werden. Fühlen Sie sich frei, die Rezepte wie sie sind wiederzuverwenden oder sich an Ihre Umgebung anzupassen.

Verbindungsgrenze pro Benutzer

Das Citrix ADC T1-Modell kann so konfiguriert werden, dass die Anzahl der Verbindungen pro eindeutiger Teilnehmer-IP begrenzt wird. Bei der folgenden Konfiguration sind N gleichzeitige TCP-Verbindungen pro IP (CLIENT.IP.SRC) zulässig. Für jeden Verbindungsversuch über den konfigurierten Schwellenwert hinaus sendet T1 einen RST. Für maximal 2 gleichzeitige Verbindungen pro Benutzer:

Befehl:

```
1 add stream selector streamSel_usrlimit CLIENT.IP.SRC
2 add ns limitIdentifier limitId_usrlimit -threshold 2 -mode CONNECTION -
      selectorName streamSel_usrlimit
```



```
3 add responder policy respPol_usrlimit "SYS.CHECK_LIMIT("
    limitId_usrlimit")" RESET
4 bind lb vserver vsrv-wireless -policyName respPol_usrlimit -priority 1
    -gotoPriorityExpression END
5 <!--NeedCopy-->
```

Glattes Einfügen/Löschen von Vserver

Viele Betreiber befürchten die Unterbrechung von TCP-Verbindungen, wenn das Citrix ADC T1-Modell für die TCP-Optimierung inline aktiviert ist oder wenn es für Wartungszwecke deaktiviert ist. Um zu vermeiden, dass vorhandene Verbindungen unterbrochen werden, wenn vserver eingeführt wird, muss die folgende Konfiguration angewendet werden, bevor vserver für die TCP-Optimierung konfiguriert oder aktiviert wird:

Befehl:

```
1 add ns acl acl-ingress ALLOW -vlan 100
2 add forwardingSession fwd-ingress -aclname acl-ingress
3 apply ns acls
4 <!--NeedCopy-->
```

Weiterleitungssitzungen sind zusätzlich zum Routing wirksam (statisch oder dynamisch oder PBR) und erstellen Sitzungseinträge für den gerouteten Datenverkehr (L3-Modus). Jede vorhandene Verbindung wird durch Weiterleiten der Sitzung aufgrund entsprechender Sitzungen behandelt, und nach Einführung von vserver beginnt es nur neue TCP-Verbindungen zu erfassen.

ACLs können so konfiguriert werden, dass nur bestimmte Ports wie vserver erfasst werden, um zu vermeiden, dass Sitzungen für unnötigen Datenverkehr erstellt werden, der Speicher verbraucht. Eine weitere Möglichkeit besteht darin, bestimmte Konfiguration nach der Aktivierung von vserver zu entfernen.

Für Wartungszwecke sollte vserver deaktiviert sein und sein Status als OUT OF SERVICE angezeigt wird. In diesem Fall beendet der vserver standardmäßig alle Verbindungen sofort. Damit vserver die vorhandenen Verbindungen weiterhin bedient und keine neuen Verbindungen akzeptiert, sollte die folgende Konfiguration angewendet werden:

Befehl:

```
1 set lb vserver vsrv-wireless -downStateFlush DISABLED
2 <!--NeedCopy-->
```


Neue Verbindungen durchlaufen die Routing-Tabelle, und entsprechende Sitzungseinträge werden aufgrund von Weiterleitungssitzungen erstellt.

Richtlinienbasierte TCP-Profilerstellung

Die Richtlinienbasierte TCP-Profilauswahl ermöglicht es Operatoren, TCP-Profil dynamisch für Clients aus verschiedenen Traffic-Domänen (z. B. 3G oder 4G) zu konfigurieren. Einige QoS-Metriken unterscheiden sich für diese Datenverkehrsdomänen. Um eine bessere Leistung zu erzielen, müssen Sie einen Teil des TCP-Parameters dynamisch ändern. Betrachten Sie einen Fall, in dem Clients von 3G und 4G denselben vserver treffen und dasselbe TCP-Profil verwenden, was sich negativ auf die Leistung einiger Clients auswirkt. AppQoE-Funktionalität kann diese Clients klassifizieren und TCP-Profil dynamisch auf vserver ändern.

Beispiel:

```
enable feature AppQoE

add ns tcpProfile nstcpprofile1 -WS ENABLED -SACK ENABLED -WSVal 8 -mss
     1460 -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
    slowStartIncr 1 -bufferSize 4000000 -flavor BIC -KA ENABLED -
    sendBuffsize 4000000 -rstWindowAttenuate ENABLED -spoofSynDrop
    ENABLED -frto ENABLED -maxcwnd 1000000 -fack ENABLED -tcpmode
    ENDPOINT

add ns tcpProfile nstcpprofile2 -WS ENABLED -SACK ENABLED -WSVal 8 -mss
     1460 -maxBurst 15 -initialCwnd 16 -oooQSize 15000 -minRTO 800 -
    slowStartIncr 1 -bufferSize 128000 -flavor BIC -KA ENABLED -
    sendBuffsize 6000000 -rstWindowAttenuate ENABLED -spoofSynDrop
    ENABLED -frto ENABLED -maxcwnd 64000 -fack ENABLED -tcpmode ENDPOINT

add appqoe action action_1 -priority HIGH -tcpprofile nstcpprofile1

add appqoe action action_2 -priority HIGH -tcpprofile nstcpprofile2

add appqoe policy appqoe_4G -rule "CLIENT.VLAN.ID.EQ(100)" -action
    action_1

add appqoe policy appqoe_3G -rule "CLIENT.VLAN.ID.EQ(200)" -action
    action_2

bind lb vserver vsrv-wireless -policyName appqoe_4G -priority 100

bind lb vserver vsrv-wireless -policyName appqoe_3G -priority 110
```



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

Das Citrix ADC T1-Modell kann die Teilnehmerinformationen dynamisch über die Gx- oder Radius- oder Radius- und GX-Schnittstelle empfangen und verschiedene TCP-Profile pro Teilnehmerbasis anwenden.

Befehl:

```
add appqoe action action_1 -priority HIGH -tcpprofile nstcpprofile1

add appqoe action action_2 -priority HIGH -tcpprofile nstcpprofile2

add appqoe policy appqoe_4G -rule "SUBSCRIBER.RULE_ACTIVE("3G")" -
   action action_1

add appqoe policy appqoe_3G -rule "SUBSCRIBER.RULE_ACTIVE("4G")" -
   action action_2
<!--NeedCopy-->
```

Informationen zur Integration des Citrix ADC T1-Modells in das Steuerungsebenennetz des Bedieners finden Sie unter Telco Subscriber Management.

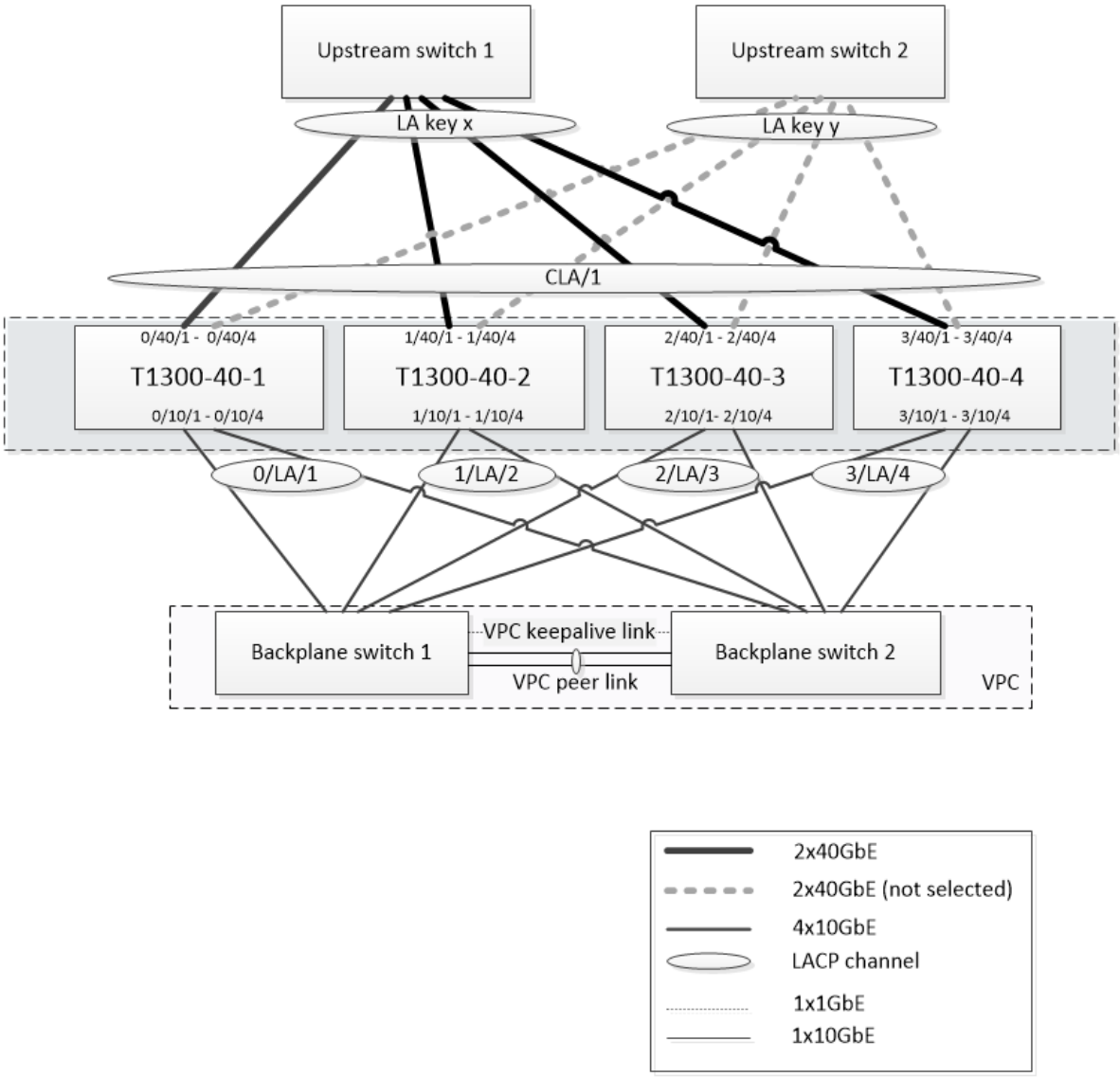
Skalierbarkeit

October 5, 2021

Da die TCP-Optimierung ressourcenintensiv ist, kann eine einzelne Citrix ADC Appliance, selbst eine High-End-Appliance, möglicherweise keinen hohen Gi-LAN-Durchsatz aufrechterhalten. Um die Kapazität Ihres Netzwerks zu erweitern, können Sie Citrix ADC Appliances in einer N+1-Clusterformation bereitstellen. In einer Clusterbereitstellung arbeiten die Citrix ADC Appliances als einzelnes Systemimage zusammen. Der Client-Datenverkehr wird über die Clusterknoten mit Hilfe eines externen Switch-Geräts verteilt.

Topologie

Abbildung 1 ist ein Beispiel für einen Cluster, der aus vier T1300-40G-Knoten besteht.



Das in Abbildung 1 gezeigte Setup weist folgende Eigenschaften auf:

1. Alle Clusterknoten gehören zum selben Netzwerk (auch als L2-Cluster bezeichnet).
2. Datenebene und Backplane-Datenverkehr werden von verschiedenen Switches abgewickelt.
3. Unter der Annahme, dass der Gi-LAN-Durchsatz 200 Gbit/s beträgt und eine T1300-40G-Appliance 80 Gbit/s Durchsatz aufrechterhalten kann, benötigen wir drei T1300-40G-Appliances. Um Redundanz im Falle eines Ausfalls eines einzelnen Clusterknotens bereitzustellen, stellen wir insgesamt vier Appliances bereit.
4. Jeder Knoten erhält bis zu 67 Gbit/s Datenverkehr (50 Gbit/s unter normalen Betriebsbedingungen und 67 Gbit/s im Falle eines Ausfalls eines einzelnen Clusterknotens). Daher benötigt er 2 x 40 Gbit/s Verbindungen zum Upstream-Switch. Um Redundanz im Falle eines Switch-Ausfalls bereitzustellen, stellen wir einige Upstream-Switches bereit und verdoppeln die Anzahl der Verbindungen.

5. Cluster Link Aggregation (CLAG) wird verwendet, um den Datenverkehr über Clusterknoten zu verteilen. Ein einzelner CLAG verarbeitet sowohl den Client- als auch den Serververkehr. Link-Redundanz ist auf der CLAG aktiviert, so dass zu einem bestimmten Zeitpunkt nur ein "Subchannel" ausgewählt wird und den Datenverkehr verarbeitet. Wenn ein Link fehlschlägt oder der Durchsatz unter den angegebenen Schwellenwert fällt, wird der andere Unterkanal ausgewählt.
6. Der Upstream-Switch führt einen symmetrischen Port-Channel-Lastausgleich durch (z. B. Quell-Dest-IP-Algorithmus von Cisco IOS 7.0 (8) N1 (1)), sodass Vorwärts- und Rückwärtsverkehr von demselben Clusterknoten verarbeitet werden. Diese Eigenschaft ist wünschenswert, da sie die Paketneuordnung eliminiert, was die TCP-Leistung beeinträchtigen würde.
7. Es wird erwartet, dass 50 Prozent des Datenverkehrs auf die Backplane gelenkt werden, was bedeutet, dass jeder Knoten bis zu 34 Gbit/s zu anderen Clusterknoten steuert (25 Gbit/s unter normalen Betriebsbedingungen und 34 Gbit/s im Falle eines Ausfalls eines einzelnen Clusterknotens). Daher benötigt jeder Knoten mindestens 4x10G-Verbindungen zum Backplane-Switch. Um Redundanz im Falle eines Switch-Ausfalls bereitzustellen, stellen wir einige Backplane-Switches bereit und verdoppeln die Anzahl der Verbindungen. Link-Redundanz wird derzeit nicht für Backplane unterstützt. Daher ist Cisco VPC oder gleichwertige Technologie erwünscht, um Redundanz auf Switchebene zu erreichen.
8. Die MTU-Größe der gesteuerten Pakete beträgt 1578 Byte, daher müssen Backplane-Switches eine MTU mehr als 1500 Byte unterstützen.

Hinweis: Das in Abbildung 1 dargestellte Design gilt auch für T1120- und T1310-Geräte. Für T1310 würden wir 40GbE-Schnittstellen für die Backplane-Verbindungen verwenden, da es 10GbE-Ports fehlen.

Hinweis: Während in diesem Dokument Cisco VPC als Beispiel verwendet wird, können alternative äquivalente Lösungen wie Junipers MLAG verwendet werden.

Hinweis: Während andere Topologien wie ECMP anstelle von CLAG möglich sind, werden sie derzeit für diesen speziellen Anwendungsfall nicht unterstützt.

Konfigurieren der TCP-Optimierung in einem Citrix ADC T1000-Cluster

Nach Abschluss der physischen Installation, der physischen Konnektivität, der Softwareinstallation und der Lizenzierung können Sie mit der tatsächlichen Clusterkonfiguration fortfahren. Die unten beschriebenen Konfigurationen gelten für den Cluster, der in Abbildung 1 dargestellt ist.

Hinweis: Weitere Informationen zur Clusterkonfiguration finden Sie unter Einrichten eines Citrix ADC-Clusters.

Angenommen, die vier T1300-Knoten in Abbildung 1 haben die folgenden NSIP-Adressen:

Vier T1300 Knoten mit NSIP-Adresse:

```
1 T1300-40-1: 10.102.29.60
```



```
2 T1300-40-2: 10.102.29.70
3 T1300-40-3: 10.102.29.80
4 T1300-40-4: 10.102.29.90
```

Der Cluster wird über die Cluster-IP (CLIP) -Adresse verwaltet, die als 10.78.16.61 angenommen wird.

Einrichten des Clusters

Um mit der Konfiguration des in Abbildung 1 gezeigten Clusters zu beginnen, melden Sie sich bei der ersten Appliance an, die Sie dem Cluster hinzufügen möchten (z. B. T1300-40-1), und führen Sie die folgenden Schritte aus.

1. Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

   Befehl:

   ```
   1 > add cluster instance 1
   2 > add cluster node 0 10.102.29.60 -state ACTIVE
   3 > add ns ip 10.102.29.61 255.255.255.255 -type clip
   4 > enable cluster instance 1
   5 > save ns config
   6 > reboot  - warm
   ```

2. Nach dem Neustart der Appliance stellen Sie eine Verbindung zur Cluster-IP-Adresse (CLIP) her, und fügen Sie den Rest der Knoten zum Cluster hinzu:

   Befehl:

   ```
   1 > add cluster node 1 10.102.29.70 -state ACTIVE
   2 > add cluster node 2 10.102.29.80 -state ACTIVE
   3 > add cluster node 3 10.102.29.90  - state ACTIVE
   4 > save ns config
   ```

3. Stellen Sie eine Verbindung mit der NSIP-Adresse jedes der neu hinzugefügten Knoten her, und treten Sie dem Cluster bei:

   Befehl:

   ```
   1 > join cluster -clip 10.102.29.61 -password nsroot
   2 > save ns config
   3 > reboot  - warm
   ```


4. Fahren Sie nach dem Neustart der Knoten mit der Backplane-Konfiguration fort. Geben Sie unter der Cluster-IP-Adresse die folgenden Befehle ein, um einen LACP-Kanal für die Backplane-Verknüpfung jedes Clusterknotens zu erstellen:

   Befehl:

```
> set interface 0/10/[1-8] -lacpkey 1 -lacpmode ACTIVE
> set interface 1/10/[1-8] -lacpkey 2 -lacpmode ACTIVE
> set interface 2/10/[1-8] -lacpkey 3 -lacpmode ACTIVE
> set interface 3/10/[1-8] -lacpkey 4 -lacpmode ACTIVE
```

5. Konfigurieren Sie in ähnlicher Weise dynamische LA und VPC auf den Backplane-Switches. Stellen Sie sicher, dass die MTU der Backplane-Switch-Schnittstellen mindestens 1578 Byte beträgt.
6. Überprüfen Sie, ob die Kanäle funktionsfähig sind:

   Befehl:

```
> show channel 0/LA/1
> show channel 1/LA/2
> show channel 2/LA/3
> show channel 3/LA/4
```

7. Konfigurieren Sie die Backplane-Schnittstellen des Cluster-Knotens.

   Befehl:

```
> set cluster node 0 -backplane 0/LA/1
> set cluster node 1 -backplane 1/LA/2
> set cluster node 2 -backplane 2/LA/3
> set cluster node 3 -backplane 3/LA/4
```

8. Überprüfen Sie den Clusterstatus, und stellen Sie sicher, dass der Cluster funktionsfähig ist:

```
> show cluster instance
> show cluster node
```

Weitere Informationen zum Cluster-Setup finden Sie unter Einrichten eines Citrix ADC-Clusters

Verteilung des Datenverkehrs über Clusterknoten

Nachdem Sie den Citrix ADC-Cluster gebildet haben, stellen Sie Cluster Link Aggregation (CLAG) bereit, um den Datenverkehr über Clusterknoten zu verteilen. Ein einzelner CLAG-Link behandelt sowohl den Client- als auch den Serververkehr.

Führen Sie unter der Cluster-IP-Adresse die folgenden Befehle aus, um die CLAG-Gruppe (Cluster Link Aggregation) zu erstellen, die in Abbildung 1 dargestellt ist:

Befehl:

```
> set interface 0/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 1/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 2/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 3/40/[1-4] -lacpMode active -lacpKey 5 -lagType Cluster
```

Konfigurieren Sie die dynamische Linkaggregation auf den externen Switches.

Aktivieren Sie dann Link-Redundanz wie folgt:

Code:

```
> set channel CLA/1 -linkRedundancy ON -lrMinThroughput 240000
```

Überprüfen Sie schließlich den Kanalstatus, indem Sie Folgendes eingeben:

Befehl:

```
> show channel CLA/1
```

Der Kanal sollte UP sein und der tatsächliche Durchsatz sollte 320000 betragen.

Weitere Informationen zur Cluster-Link-Aggregation finden Sie in den folgenden Themen:

- Dynamische Cluster-Link-Aggregation
- Verknüpfen Sie Redundanz in einem Cluster mit LACP.

Da wir MAC-basierte Weiterleitung (MBF) verwenden, konfigurieren Sie einen Linkset und binden ihn wie folgt an die CLAG-Gruppe:

Befehl:


```
> add linkset LS/1
> bind linkset LS/1 -ifnum CLA/1
```

Weitere Informationen zu Linksets finden Sie in den folgenden Themen:

- Konfigurieren von Linksets
- Cluster-LA Channel mit Linksets verwenden

Konfigurieren von VLAN- und IP-Adressen

Wir werden Striped IP-Konfiguration verwenden, was bedeutet, dass IP-Adressen auf allen Knoten aktiv sind (Standardeinstellung). Weitere Informationen zu diesem Thema finden Sie unter Gestreifte, teilweise gestreifte und gepunktete Konfigurationen .

1. Fügen Sie die Ein- und Ausgangs-SNIPs hinzu:

   Befehl:

```
> add ns ip 172.16.30.254 255.255.255.0 -type SNIP
> add ns ip 172.16.31.254 255.255.255.0 -type SNIP
> add ns ip6 fd00:172:16:30::254/112 -type SNIP
> add ns ip6 fd00:172:16:31::254/112 -type SNIP
```

2. Fügen Sie die entsprechenden VLANs hinzu:

   Befehl:

```
> add vlan 30 -aliasName wireless
> add vlan 31 -aliasName internet
```

3. Binden Sie VLANs mit IPs und Linkset:

   Befehl:

```
> bind vlan 31 -ifnum LS/1 -tagged
> bind vlan 30 -ifnum LS/1 -tagged
> bind vlan 30 -IPAddress 172.16.30.254 255.255.255.0
> bind vlan 31 -IPAddress 172.16.31.254 255.255.255.0
> bind vlan 30 -IPAddress fd00:172:16:30::254/112
> bind vlan 31 -IPAddress fd00:172:16:31::254/112
```

Bei Bedarf können mehr Ein- und Ausstieg VLANs hinzugefügt werden.

Konfigurieren der TCP-Optimierung

An dieser Stelle haben wir alle clusterspezifischen Befehle angewendet. Um die Konfiguration abzuschließen, führen Sie die in TCP-Optimierungskonfigurationbeschriebenen Schritte aus.

Dynamisches Routing konfigurieren

Ein Citrix ADC Cluster kann in die dynamische Routing-Umgebung des Kundennetzwerks integriert werden. Es folgt ein Beispiel für dynamische Routing-Konfiguration mit BGP-Routing-Protokoll (OSPF wird auch unterstützt).

1. Aktivieren Sie über die CLIP-Adresse BGP und dynamisches Routing für Ein- und Ausgänge von IP-Adressen:

   Befehl:

```
> enable ns feature bgp
> set ns ip 172.16.30.254 -dynamicRouting ENABLED
> set ns ip 172.16.31.254 -dynamicRouting ENABLED
```

2. Öffnen Sie vtysh und konfigurieren Sie BGP für die Egress-Seite:

   Code:

```
> shell
root@ns# vtysh
ns# configure terminal
ns(config)# router bgp 65531
ns(config-router)# network 10.0.0.0/24
ns(config-router)# neighbor 172.16.31.100 remote-as 65530
ns(config-router)# neighbor 172.16.31.100 update-source
    172.16.31.254
ns(config-router)# exit
ns(config)# ns route-install propagate
ns(config)# ns route-install default
ns(config)# ns route-install bgp
ns(config)# exit
```

3. Konfigurieren Sie den egress-seitigen BGP-Peer, um die Standardroute zum Citrix ADC Cluster anzukündigen. Beispiel:

   Befehl:


```
router bgp 65530
 bgp router-id 172.16.31.100
 network 0.0.0.0/0
 neighbor 172.16.31.254 remote-as 65531
```

4. Führen Sie ähnliche Schritte aus, um die Eindringseite zu konfigurieren.
5. Stellen Sie in vtysh sicher, dass die Konfiguration an alle Clusterknoten weitergegeben wird, indem Sie Folgendes eingeben:

   Befehl:

```
ns# show running-config
```

6. Melden Sie sich schließlich bei der NSIP-Adresse jedes Clusterknotens an und überprüfen Sie die von BGP-Peer angekündigten Routen:

   Befehl:

```
> show route | grep BGP
```

Optimierung der TCP-Leistung mit TCP Nil

October 5, 2021

TCP verwendet die folgenden Optimierungstechniken und Engpasskontrollstrategien (oder Algorithmen), um Netzwerküberlastung bei der Datenübertragung zu vermeiden.

Engpasskontrollstrategien

Das Transmission Control Protocol (TCP) wird seit langem verwendet, um Internetverbindungen herzustellen und zu verwalten, Übertragungsfehler zu behandeln und Webanwendungen problemlos mit Client-Geräten zu verbinden. Der Netzwerkverkehr ist jedoch schwieriger zu kontrollieren, da der Paketverlust nicht nur von der Staus im Netzwerk abhängt und Staus nicht notwendigerweise zu Paketverlust führt. Daher sollte sich ein TCP-Algorithmus auf Paketverlust und Bandbreite konzentrieren, um Engpässe zu messen.

NILE-Algorithmus

Citrix Systems hat einen neuen Engpass-Congestion-Control-Algorithmus entwickelt, NILE, einen TCP-Optimierungsalgorithmus für Hochgeschwindigkeitsnetze wie LTE, LTE advanced und 3G. Nil befasst sich mit einzigartigen Herausforderungen, die durch Fading, zufällige oder überlastete Verluste, Link-Layer-Neuübertragungen und Trägeraggregation verursacht werden.

Der NILE-Algorithmus:

- Basiert Schätzungen der Warteschlangenlatenz auf Round-Trip-Zeitmessungen.
- Verwendet eine Funktion zum Erhöhen von Staufenstern, die umgekehrt proportional zur gemessenen Warteschlangenlatenz ist. Diese Methode führt dazu, dass sich der Netzwerküberlastungspunkt langsamer nähert als die Standard-TCP-Methode, und reduziert die Paketverluste während der Staus.
- Kann zwischen zufälligen Verlusten und überlastungsbasierten Verlust im Netzwerk unterscheiden, indem die geschätzte Warteschlangenlatenz verwendet wird.

Die Telekommunikationsdienstanbieter können den NILE-Algorithmus in ihrer TCP-Infrastruktur verwenden, um:

- Optimieren Sie mobile und Fernnetze — Der NILE-Algorithmus erzielt einen höheren Durchsatz im Vergleich zu Standard-TCP. Diese Funktion ist besonders wichtig für mobile und Fernnetze.
- Verringern Sie die empfangene Latenz der Anwendung und verbessern Sie die Nutzererfahrung— Der Nil-Algorithmus verwendet Paketverlust-Informationen, um festzustellen, ob die Größe des Übertragungsfensters erhöht oder verringert werden soll, und verwendet Informationen zur Warteschlangenverzögerung, um die Größe des Inkrements oder Dekrements zu bestimmen. Diese dynamische Einstellung der Übertragungsfenstergröße verringert die Anwendungslatenz im Netzwerk.

So konfigurieren Sie die NILE-Unterstützung über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns tcpProfile <name> [-flavor NILE]
<!--NeedCopy-->
```

Konfigurieren der NILE-Unterstützung mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **System** > **Profile** > **TCP-Profile**, und klicken Sie auf **TCP-Profile** .
2. Wählen Sie in der Dropdownliste **TCP-Flavor** die Option **NILE** aus.

Beispiel:


```
set ns tcpProfile tcpprofile1 -flavor NILE
<!--NeedCopy-->
```

PRR-Algorithmus (Proportional Rate Recovery)

TCP Fast Recovery-Mechanismen reduzieren die Weblatenz, die durch Paketverluste verursacht wird. Der neue PRR-Algorithmus (Proportional Rate Recovery) ist ein schneller Recovery-Algorithmus, der TCP-Daten während einer Verlustwiederherstellung auswertet. Es wird nach der Rate-Halving gemustert, indem der Bruch verwendet wird, der für das Zielfenster geeignet ist, das vom Algorithmus zur Staus gewählt wird. Es minimiert die Fensteranpassung, und die tatsächliche Fenstergröße am Ende der Wiederherstellung liegt nahe am Slow-Start-Schwellenwert (ssthresh).

TCP Fast Open (TFO)

TCP Fast Open (TFO) ist ein TCP-Mechanismus, der einen schnellen und sicheren Datenaustausch zwischen einem Client und einem Server während des ersten Handshakes von TCP ermöglicht. Diese Funktion ist als TCP-Option im TCP-Profil verfügbar, das an einen virtuellen Server einer Citrix ADC Appliance gebunden ist. TFO verwendet ein TCP Fast Open Cookie (ein Sicherheits-Cookie), das die Citrix ADC Appliance generiert, um den Client zu validieren und zu authentifizieren, der eine TFO Verbindung zum virtuellen Server initiiert. Durch die Verwendung des TFO Mechanismus können Sie die Netzwerklatenz einer Anwendung um die Zeit reduzieren, die für eine vollständige Hin- und Rückfahrt erforderlich ist, was die Verzögerung bei kurzen TCP-Übertragungen erheblich reduziert.

Funktionsweise von TFO

Wenn ein Client versucht, eine TFO Verbindung herzustellen, enthält er ein TCP Fast Open Cookie mit dem anfänglichen SYN-Segment, um sich selbst zu authentifizieren. Wenn die Authentifizierung erfolgreich ist, kann der virtuelle Server auf der Citrix ADC Appliance Daten in das SYN-ACK-Segment aufnehmen, obwohl er nicht das endgültige ACK-Segment des Dreiwege-Handshakes erhalten hat. Dies spart bis zu einer vollständigen Hin- und Rückfahrt im Vergleich zu einer normalen TCP-Verbindung, die einen Dreiwege-Handshake erfordert, bevor Daten ausgetauscht werden können.

Ein Client und ein Backend-Server führen die folgenden Schritte aus, um eine TFO-Verbindung herzustellen und Daten während des ersten TCP-Handshake sicher auszutauschen.

1. Wenn der Client über kein TCP Fast Open Cookie verfügt, um sich selbst zu authentifizieren, sendet er eine Fast Open Cookie-Anforderung im SYN-Paket an den virtuellen Server auf der Citrix ADC Appliance.

2. Wenn die TFO Option im TCP-Profil aktiviert ist, das an den virtuellen Server gebunden ist, generiert die Appliance ein Cookie (indem sie die IP-Adresse des Clients unter einem geheimen Schlüssel verschlüsselt) und antwortet mit einem SYN-ACK auf den Client, das das generierte Fast Open Cookie in einem TCP-Optionsfeld enthält.
3. Der Client speichert das Cookie für zukünftige TFO-Verbindungen mit demselben virtuellen Server auf der Appliance.
4. Wenn der Client versucht, eine TFO Verbindung mit demselben virtuellen Server herzustellen, sendet er SYN, die das zwischengespeicherte Fast Open Cookie (als TCP-Option) zusammen mit HTTP-Daten enthält.
5. Die Citrix ADC Appliance validiert das Cookie, und wenn die Authentifizierung erfolgreich ist, akzeptiert der Server die Daten im SYN-Paket und bestätigt das Ereignis mit einem SYN-ACK, TFO Cookie und HTTP Response.

Hinweis: Wenn die Clientauthentifizierung fehlschlägt, löscht der Server die Daten und bestätigt das Ereignis nur mit einem SYN, der ein Sitzungszeitlimit angibt.

1. Wenn auf Serverseite die TFO Option in einem an einen Dienst gebundenen TCP-Profil aktiviert ist, bestimmt die Citrix ADC Appliance, ob das TCP Fast Open Cookie in dem Dienst vorhanden ist, zu dem es versucht, eine Verbindung herzustellen.
2. Wenn das TCP Fast Open Cookie nicht vorhanden ist, sendet die Appliance eine Cookie-Anfrage im SYN-Paket.
3. Wenn der Backend-Server das Cookie sendet, speichert die Appliance das Cookie im Serverinformations-Cache.
4. Wenn die Appliance bereits ein Cookie für das angegebene Ziel-IP-Paar hat, wird das alte Cookie durch das neue ersetzt.
5. Wenn das Cookie im Serverinformations-Cache verfügbar ist, wenn der virtuelle Server versucht, mithilfe derselben SNIP-Adresse eine erneute Verbindung mit demselben Backend-Server herzustellen, kombiniert die Appliance die Daten im SYN-Paket mit dem Cookie und sendet es an den Backend-Server.
6. Der Backend-Server bestätigt das Ereignis sowohl mit Daten als auch mit einem SYN.

Hinweis: Wenn der Server das Ereignis nur mit einem SYN-Segment bestätigt, sendet die Citrix ADC Appliance das Datenpaket sofort erneut, nachdem das SYN-Segment und die TCP-Optionen aus dem ursprünglichen Paket entfernt wurden.

Konfigurieren von TCP Fast Open

Um die TCP-Funktion Fast Open (TFO) zu verwenden, aktivieren Sie die Option TCP Fast Open im entsprechenden TCP-Profil und setzen Sie den Parameter TFO Cookie Timeout auf einen Wert, der der Sicherheitsanforderung für dieses Profil entspricht.

So aktivieren oder deaktivieren Sie TFO mit der Befehlszeile

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um TFO in einem neuen oder vorhandenen Profil zu aktivieren oder zu deaktivieren.

Hinweis: Der Standardwert ist DEAKTIVIERT.

```
add tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
set tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
unset tcpprofile <TCP Profile Name> - tcpFastOpen
<!--NeedCopy-->
```

Beispiele:

add tcpprofile Profile1 – tcpFastOpen
Set tcpprofile Profile1 – tcpFastOpen Enabled
unset tcpprofile Profile1 – tcpFastOpen

So legen Sie den Timeout-Wert für TCP Fast Open Cookie mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set tcpparam  - tcpfastOpenCookieTimeout <Timeout Value>
<!--NeedCopy-->
```

Beispiel:

```
set tcpprofile  - tcpfastOpenCookieTimeout 30secs
<!--NeedCopy-->
```

So konfigurieren Sie TCP Fast Open mit der GUI

1. Navigieren Sie zu **Konfiguration** > **System** > **Profile** >, und klicken Sie dann auf **Bearbeiten**, um ein TCP-Profil zu ändern.
2. Aktivieren Sie auf der Seite **TCP-Profil konfigurieren** das Kontrollkästchen **TCP Fast Open**.
3. Klicken Sie auf **OK** und dann auf **Fertig**.

So konfigurieren Sie den TCP Fast Cookie Timeout-Wert mit der GUI

Navigieren Sie zu **Konfiguration** > **System** > **Einstellungen** > **TCP-Parameter ändern** und dann Seite **TCP-Parameter konfigurieren**, um den TCP-Zeitüberschreitungswert für TCP Fast Open Cookie festzulegen.

TCP Hystart

Ein neuer TCP-Profilparameter, hystart, ermöglicht den Hystart-Algorithmus, bei dem es sich um einen Slow-Start-Algorithmus handelt, der dynamisch einen sicheren Punkt bestimmt, an dem beendet werden soll (ssthresh). Es ermöglicht einen Übergang zur Stauvermeidung ohne hohe Paketverluste. Dieser neue Parameter ist standardmäßig deaktiviert.

Wenn Staus festgestellt wird, tritt Hystart in eine Staus Vermeidungsphase ein. Durch die Aktivierung erhalten Sie einen besseren Durchsatz in Hochgeschwindigkeitsnetzen mit hohem Paketverlust. Dieser Algorithmus hilft, bei der Verarbeitung von Transaktionen nahezu die maximale Bandbreite beizubehalten. Dadurch kann der Durchsatz verbessert werden.

TCP-Hystart konfigurieren

Um die Hystart-Funktion zu verwenden, aktivieren Sie die Option Cubic Hystart im entsprechenden TCP-Profil.

So konfigurieren Sie Hystart mit der Befehlszeilenschnittstelle (CLI)

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um Hystart in einem neuen oder vorhandenen TCP-Profil zu aktivieren oder zu deaktivieren.

```
add tcpprofile <profileName> -hystart ENABLED
set tcpprofile <profileName> -hystart ENABLED
unset tcprofile <profileName> -hystart
<!--NeedCopy-->
```

Beispiele:

```
add tcpprofile Profile1 - tcpFastOpen
Set tcpprofile Profile1 - tcpFastOpen Enabled
unset tcpprofile Profile1 - tcpFastOpen
<!--NeedCopy-->
```


So konfigurieren Sie die Hystart-Unterstützung mit der GUI

1. Navigieren Sie zu **Konfiguration** > **System** > **Profile** > und klicken Sie auf **Bearbeiten**, um ein TCP-Profil zu ändern.
2. Aktivieren Sie auf der Seite **TCP-Profil konfigurieren** das Kontrollkästchen **Cubic Hystart**.
3. Klicken Sie auf **OK** und dann auf **Fertig**.

Optimierungstechniken

TCP verwendet die folgenden Optimierungstechniken und -methoden für optimierte Flusssteuerungen.

Richtlinienbasierte TCP-Profilauswahl

Der Netzwerkverkehr ist heute vielfältiger und bandbreitenintensiver als je zuvor. Mit dem erhöhten Datenverkehr ist die Wirkung, die Quality of Service (QoS) auf die TCP-Leistung hat, signifikant. Um QoS zu verbessern, können Sie jetzt AppQoE-Richtlinien mit unterschiedlichen TCP-Profilen für verschiedene Klassen von Netzwerkverkehr konfigurieren. Die AppQoE-Richtlinie klassifiziert den Datenverkehr eines virtuellen Servers, um ein TCP-Profil zu verknüpfen, das für einen bestimmten Typ von Datenverkehr optimiert ist, z. B. 3G, 4G, LAN oder WAN.

Um dieses Feature zu verwenden, erstellen Sie für jedes TCP-Profil eine Richtlinienaktion, ordnen Sie eine Aktion AppQoE-Richtlinien zu und binden Sie die Richtlinien an die virtuellen Server mit Lastenausgleich.

Konfigurieren der Richtlinienbasierten TCP-Profilauswahl

Die Konfiguration der richtlinienbasierten TCP-Profilauswahl umfasst die folgenden Aufgaben:

- AppQoE wird aktiviert. Bevor Sie das TCP-Profilfeature konfigurieren, müssen Sie die AppQoE -Funktion aktivieren.
- AppQoE-Aktion hinzufügen. Nachdem Sie die AppQoE-Funktion aktiviert haben, konfigurieren Sie eine AppQoE-Aktion mit einem TCP-Profil.
- Konfigurieren der AppQoE-basierten TCP-Profilauswahl. Um die TCP-Profilauswahl für verschiedene Datenverkehrsklassen zu implementieren, müssen Sie AppQoE-Richtlinien konfigurieren, mit denen Ihre Citrix ADC Appliance die Verbindungen unterscheiden und die richtige AppQoE-Aktion an jede Richtlinie binden kann.
- Binden der AppQoE -Richtlinie an den virtuellen Server. Nachdem Sie die AppQoE-Richtlinien konfiguriert haben, müssen Sie sie an einen oder mehrere virtuelle Load Balancing-, Content Switching- oder Cache-Umleitungsserver binden.

Konfiguration über die Befehlszeilenschnittstelle

So aktivieren Sie AppQoE mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um das Feature zu aktivieren, und überprüfen Sie, ob es aktiviert ist:

```
enable ns feature appqoe

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

So binden Sie ein TCP-Profil beim Erstellen einer AppQoE-Aktion mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden AppQoE-Aktionsbefehl mit der Option tcpprofiletobind ein.

Binden eines TCP-Profils:

```
add appqoe action <name> [-priority <priority>] [-respondWith ( ACS |
    NS ) [<CustomFile>] [-altContentSvcName <string>] [-altContentPath <
    string>] [-maxConn <positive_integer>] [-delay <usecs>]] [-polqDepth
     <positive_integer>] [-priqDepth <positive_integer>] [-
    dosTrigExpression <expression>] [-dosAction ( SimpleResponse |
    HICResponse )] [-tcpprofiletobind <string>]

show appqoe action
<!--NeedCopy-->
```

So konfigurieren Sie eine AppQoE-Richtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add appqoe policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```


So binden Sie eine AppQoE-Richtlinie an virtuelle Lastausgleichs-, Cache-Umleitungs- oder Content Switching-Server mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind cs vserver cs1 -policyName <appqoe_policy_name> -priority <
    priority>
bind lb vserver <name> - policyName <appqoe_policy_name> -priority <
    priority>
bind cr vserver <name> -policyName <appqoe_policy_name> -priority <
    priority>
<!--NeedCopy-->
```

Beispiel:

```
add ns tcpProfile tcp1 -WS ENABLED -SACK ENABLED -WSVal 8 -nagle
    ENABLED -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 500 -
    slowStartIncr 1 -bufferSize 4194304 -flavor BIC -KA ENABLED -
    sendBuffsize 4194304 -rstWindowAttenuate ENABLED -spoofSynDrop
    ENABLED -dsack enabled -frto ENABLED -maxcwnd 4000000 -fack ENABLED
    -tcpmode ENDPOINT

add appqoe action appact1 -priority HIGH -tcpprofile tcp1

add appqoe policy apppol1 -rule "client.ip.src.eq(10.102.71.31)" -
    action appact1

bind lb vserver lb2 -policyName apppol1 -priority 1 -
    gotoPriorityExpression END -type REQUEST

bind cs vserver cs1 -policyName apppol1 -priority 1 -
    gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

Konfigurieren der richtlinienbasierten TCP-Profilerstellung mit der GUI

So aktivieren Sie AppQoE mit der GUI

1. Navigieren Sie zu **System** > **Einstellungen**.
2. Klicken Sie im Detailbereich auf **Erweiterte Funktionen konfigurieren**.
3. Aktivieren Sie im Dialogfeld **Erweiterte Funktionen konfigurieren** das Kontrollkästchen **AppQoE**.

4. Klicken Sie auf **OK**.

So konfigurieren Sie die AppQoE -Richtlinie mit der GUI

1. Navigieren Sie zu **App-Expert** > **AppQoe** > **Aktionen** .
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
3. Um eine neue Aktion zu erstellen, klicken Sie auf **Hinzufügen**.
4. Um eine vorhandene Aktion zu ändern, wählen Sie die Aktion aus, und klicken Sie dann auf **Bearbeiten**.
5. Geben **Sie im Bildschirm AppQoE-Aktion erstellen** oder im Fenster **AppQoE-Aktion konfigurieren** Werte für die Parameter ein oder wählen Sie sie aus. Der Inhalt des Dialogfensters entspricht den unter Parameter für die Konfiguration der AppQoE-Aktion beschriebenen Parametern wie folgt (Sternchen gibt einen erforderlichen Parameter an):
   a) Name — Name
   b) Aktionstyp: RespondWith
   c) Priorität — Priorität
   d) Richtlinienwarteschlangentiefe — polqDepth
   e) Warteschlangentiefe — priqDepth
   f) DOS-Aktion — dosAction
6. Klicken Sie auf **Erstellen**.

So binden Sie AppQoE-Richtlinie mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, wählen Sie einen Server aus, und klicken Sie dann auf **Bearbeiten** .
2. Klicken Sie im Abschnitt **Richtlinien** auf (+), um eine AppQoE-Richtlinie zu binden.
3. Führen Sie im Schieberegler **Richtlinien** die folgenden Schritte aus:
   a) Wählen Sie einen Richtlinientyp als AppQoe aus der Dropdownliste aus.
   b) Wählen Sie einen Datenverkehrstyp aus der Dropdownliste aus.
4. Gehen Sie im Abschnitt **Richtlinienbindung** folgendermaßen vor:
   a) Klicken Sie auf **Neu**, um eine neue AppQoE-Richtlinie zu erstellen.
   b) Klicken Sie auf **Vorhandene Richtlinie**, um eine AppQoE-Richtlinie aus der Dropdownliste auszuwählen.
5. Legen Sie die **Bindungspriorität fest, und klicken Sie auf An die Richtlinie an den virtuellen Server binden** .
6. Klicken Sie auf **Fertig**.

SACK-Blockgenerierung

Die TCP-Leistung verlangsamt sich, wenn mehrere Pakete in einem Datenfenster verloren gehen. In einem solchen Szenario überwindet ein selektives Acknowledgement (SACK) -Mechanismus in Kombination mit einer selektiven Wiederholungsrichtlinie diese Einschränkung. Für jedes eingehende Out-of-Order-Paket müssen Sie einen SACK-Block generieren.

Wenn das Paket nicht in den Warteschlangenblock passt, fügen Sie Paketinformationen in den Block ein, und legen Sie die vollständigen Blockinformationen als SACK-0 fest. Wenn ein nicht bestelltes Paket nicht in den Wiederzusammenbaublock passt, senden Sie das Paket als SACK-0 und wiederholen Sie die früheren SACK-Blocks. Wenn ein nicht bestelltes Paket ein Duplikat ist und Paketinfo als SACK-0 gesetzt ist, dann ist D-SACK der Block.

Hinweis: Ein Paket gilt als D-SACK, wenn es sich um ein quittiertes Paket handelt, oder um ein veraltetes Paket, das bereits empfangen wurde.

Client-Abtrennung

Eine Citrix ADC Appliance kann das Reneging von Clients während der SACK-basierten Wiederherstellung verarbeiten.

Speicherüberprüfungen zur Markierung von end_point auf PCB berücksichtigen nicht den gesamten verfügbaren Speicher

Wenn in einer Citrix ADC Appliance der Schwellenwert für die Speichernutzung auf 75 Prozent festgelegt ist, anstatt den gesamten verfügbaren Speicher zu verwenden, bewirkt dies, dass neue TCP-Verbindungen TCP-Optimierung umgehen.

Unnötige Weiterübertragungen durch fehlende SACK-Blocks

Wenn Sie in einem Nicht-Endpunkt-Modus DUPACKS senden, werden beim Senden von SACK-Blocks für wenige Pakete außerhalb der Ordnung fehlen, zusätzliche Neuübertragungen vom Server ausgelöst.

SNMP für die Anzahl der Verbindungen wurde durch Überlastung optimiert

Die folgenden SNMP-IDs wurden zu einer Citrix ADC Appliance hinzugefügt, um die Anzahl der Verbindungen nachzuverfolgen, die TCP-Optimierung aufgrund von Überlastung umgangen wurden.

1. 1.3.6.1.4.1.5951.4.1.1.46.13 (tcpOptimizationEnabled). Um die Gesamtzahl der Verbindungen zu verfolgen, die mit TCP-Optimierung aktiviert sind.
2. 1.3.6.1.4.1.5951.4.1.1.46.132 (tcpOptimizationBypassed). Um die Gesamtzahl der Verbindungen zu verfolgen, wurde TCP-Optimierung umgangen.

Dynamischer Empfangspuffer

Um die TCP-Leistung zu maximieren, kann eine Citrix ADC Appliance nun die Größe des TCP-Empfangspuffers dynamisch anpassen.

Richtlinien zur Fehlerbehebung

October 5, 2021

Technischer Support

Alle Fehlerbehebungs- und Eskalationsabfragen erfordern ein aktuelles Citrix ADC Tech-Support-Paket, das die aktuelle Konfiguration, installierte Firmware-Version, Protokolldateien, ausstehende Kerne usw. erfasst.

Beispiel:

```
show techsupport

showtechsupport data collector tool - $Revision: #5 $!
...
<!--NeedCopy-->
```

Alle Daten werden unter

```
...
Archiving all the data into "/var/tmp/support/collector_P_192
   .168.121.117_18Jun2015_09_53.tar.gz" ....
Created a symbolic link for the archive with /var/tmp/support/support.
   tgz
/var/tmp/support/support.tgz  ---- points to ---> /var/tmp/support/
   collector_P_192.168.121.117_18Jun2015_09_53.tar.gz
<!--NeedCopy-->
```

Nachdem ein Tech-Support-Paket generiert wurde, kann es mithilfe von SCP kopiert werden.

Spuren

Citrix ADC TCP-Optimierungsprobleme erfordern normalerweise eine ordnungsgemäße Fehlerbehebung von Citrix ADC C-Traces. Beachten Sie, dass man versuchen sollte, Spuren unter ähnlichen Be-

dingungen zu erfassen, d. h. auf derselben Zelle, während derselben Tageszeit, mit der gleichen Benutzerausrüstung und Anwendung und anderen.

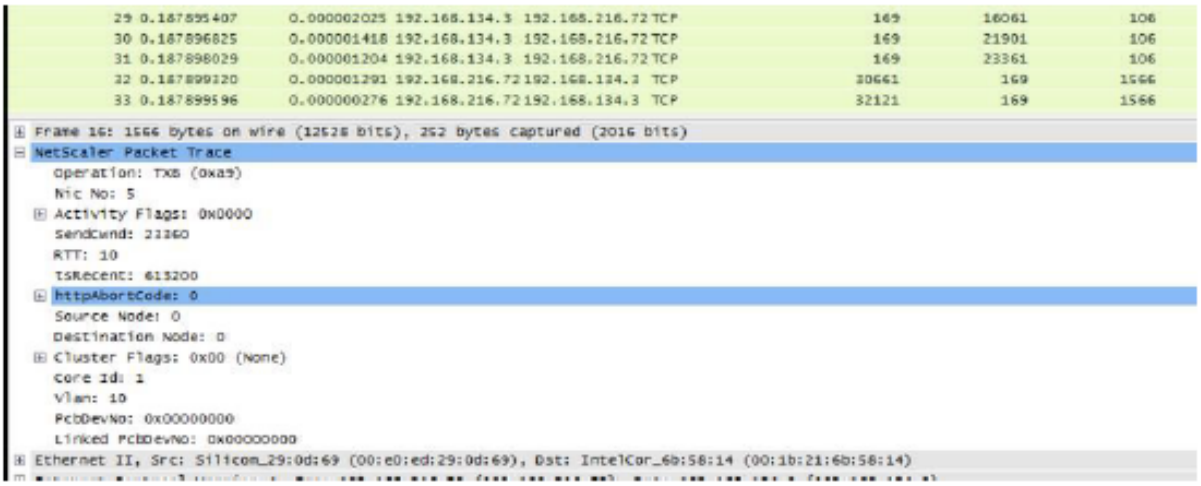
Die Befehle start nstrace und stop nstrace können verwendet werden, um Traces zu erfassen:

- Es wird dringend empfohlen, dass der entsprechende Filter verwendet wird, um zu vermeiden, dass fremde, unnötige Pakete auf der Trace erfasst werden. Verwenden Sie zum Beispiel start nstrace -filter 'IP == 10.20.30.40', um nur Pakete zu erfassen, die an die IP-Adresse 10.20.30.40 gesendet oder von dieser empfangen werden. Dies ist die IP-Adresse der Benutzerausrüstung.
- Verwenden Sie nicht die Option -tcpdump, da sie die nstrace-Header, die zum Debuggen benötigt werden, entfernt.

Trace-Analyse

Nachdem eine Citrix ADC Ablaufverfolgung erfasst wurde, wird sie möglicherweise mit Wireshark 1.12 oder höher angezeigt. Stellen Sie sicher, dass die erfassten Leiterbahnen die entsprechenden Citrix ADC Packet Trace-Header enthalten, wie in der folgenden Bildschirmaufzeichnung dargestellt:

Die zusätzlichen Debug-Header sind auch in der folgenden Abbildung sichtbar:



Verbindungstabelle

Wenn das Problem mit der TCP-Optimierung zusammenhängt und es reproduziert werden kann oder es läuft, ist es am besten, auch die Verbindungstabelle zu erhalten, wenn das Problem vom primären T1-Knoten auftritt.

Um die Tabelle zu erhalten, müssen Sie auf die BSD-Shell wechseln und den folgenden Befehl ausführen:

```
shell
...

nscli -U 127.0.0.1:nsroot:nsroot show connectiontable -detail full link
    > /var/tmp/contable.log
<!--NeedCopy-->
```

> **Hinweis:**
>
> Der Befehl wird möglicherweise für einen längeren Zeitraum ausgeführt, und die Verwaltungs-CPU ist möglicherweise zu diesem Zeitpunkt belastet (hängt von der Anzahl der Verbindungstabelleneinträge ab), aber er hat keinen Einfluss auf den Dienst.

Häufig gestellte Fragen

October 5, 2021

Timeouts

> **Wichtig**
>
> Wenden Sie *sich an den Citrix Customer Support, bevor Sie einen nsapimgr-Regler* verwenden.

Im Folgenden finden Sie eine Liste verschiedener Timeouts für Leerlaufverbindungen, die auf virtuellen Servern und Diensten von Citrix ADC T1 festgelegt werden können. Das für Client- oder Serververbindungen auf der vserver- oder Dienstebene festgelegte Leerlaufzeitlimit gilt nur für Verbindungen mit dem Status TCP ESTABLISHED und sind im Leerlauf.

- Der Parameter CLTTimeout für den Load Balancing des virtuellen Servers gibt die Zeit in Sekunden an, in der eine Verbindung von einem Client zu einem virtuellen Load Balancing-Server im Leerlauf sein muss, bevor die Appliance die Verbindung schließt.

- Der Parameter Service svrTimeout gibt die Zeit in Sekunden an, in der eine Verbindung von der Appliance zu einem Dienst oder Server im Leerlauf sein muss, bevor die Appliance die Verbindung schließt.
- Der Parameter Service CLTTimeout gibt die Zeit in Sekunden an, in der eine Verbindung von einem Client zu einem Dienst im Leerlauf sein muss, bevor die Appliance die Verbindung schließt.

Wenn ein Dienst an einen virtuellen Load Balancing-Server gebunden ist, hat der CLTTimeout für den virtuellen Load Balancing-Server Vorrang, und der Dienst CLTTimeout für Dienst wird ignoriert.

Falls kein Dienst an den virtuellen Load Balancing Server gebunden ist, wird das globale Leerlauf-Timeout, nämlich TCPServer, für serverseitige Verbindungen verwendet. Es kann wie folgt konfiguriert werden:

Befehl:

```
set ns timeout -tcpServer 9000
<!--NeedCopy-->
```

Verbindungen in einem anderen Zustand haben unterschiedliche Zeitüberschreitungswerte:

- Halb offene Verbindungen Leerlaufzeitüberschreitung: 120 Sekunden (hartcodierter Wert)
- TIME_WAIT Verbindungen Leerlauf-Timeout: 40 Sekunden (hartcodierter Wert)
- Zeitüberschreitung bei halber Schließung von Verbindungen im Leerlauf. Standardmäßig ist es 10s und kann zwischen 1s und 600s mit dem Snippet konfiguriert werden

Befehl:

```
 set ns timeout -halfclose 10
<!--NeedCopy-->
```

Wenn Timeout für die halbe Schließung ausgelöst wird, wird die Verbindung in den Zombie-Status verschoben. Wenn das Zombie-Timeout abläuft, tritt die Zombie-Bereinigung ein und T1 sendet standardmäßig RST auf Client- und Serverseite für eine bestimmte Verbindung.

- Zombie-Timeout: Intervall, in dem der Zombie-Cleanup-Prozess ausgeführt werden muss, um inaktive TCP-Verbindungen zu bereinigen. Der Standardwert für den Timeout beträgt 120s und kann zwischen 1s und 600s konfiguriert werden.

Befehl:

```
set ns timeout -zombie 120
```



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

Tabelle Maximale Segmentgröße

Eine Citrix ADC T1-Appliance schützt gegen SYN-Flutangriffe, indem sie SYN-Cookies verwendet, anstatt halboffene Verbindungen auf dem Systemspeicher-Stack beizubehalten. Die Appliance sendet ein Cookie an jeden Client, der eine TCP-Verbindung anfordert, aber die Zustände halboffener Verbindungen werden nicht beibehalten. Stattdessen weist die Appliance Systemspeicher für eine Verbindung nur bei Empfang des endgültigen ACK-Pakets oder bei HTTP-Datenverkehr beim Empfang einer HTTP-Anforderung zu. Dadurch werden SYN-Angriffe verhindert und die normale TCP-Kommunikation mit legitimen Clients unterbrechungsfrei fortgesetzt. Spezifische Funktion ist standardmäßig ohne Option zum Deaktivieren aktiviert.

Es gibt jedoch einen Vorbehalt, da Standard-SYN-Cookies Verbindungen auf die Verwendung von nur acht Maximum Segment Size (MSS) -Werten beschränken. Wenn Verbindungs-MMS nicht mit einem vordefinierten Wert übereinstimmt, wird der nächste verfügbare niedrigere Wert sowohl auf Client- als auch auf Serverseite aufgenommen.

Die vordefinierten TCP Maximum Segment Size (MSS) -Werte sind die folgenden und können über einen neuen nsapimgr-Regler konfiguriert werden.

1460	1440	1330	1220	956	536	384	128

Die neue MSS-Tabelle:

- Muss keine Jumbo-Frame-Unterstützung enthalten. Obwohl standardmäßig 8 Werte in der MSS-Tabelle für Jumbo-Frames reserviert sind, können die Tabelleneinstellungen so geändert werden, dass nur Standard-Ethernet-Frames enthalten sind.
- Sollte 16 Werte haben
- Sollte Werte in absteigender Reihenfolge haben
- Sollte 128 als letzten Wert enthalten

Wenn die neue MSS-Tabelle gültig ist, wird die Tabelle gespeichert und die alten Werte werden zur SYN-Cookie-Rotationszeit ausgeschaltet. Andernfalls gibt die neue Tabelle einen Fehler zurück. Änderungen werden auf neue Verbindungen angewendet, während vorhandene Verbindungen die alte MSS-Tabelle beibehalten, bis die Verbindungen ablaufen oder beendet werden.

Geben Sie den folgenden Befehl ein, um die aktuelle MSS-Tabelle in einer Citrix ADC Appliance anzuzeigen.

Befehl:


```
>shell

#nsapimgr -d mss_table
```

Beispiel:

```
#nsapimgr -d mss_table

MSS table

{
 9176,9156,8192,7168,6144,4196,3072,2048,1460,1440,1330,1212,956,536,384,128
     }


Done.
```

Um die MSS-Tabelle zu ändern, geben Sie den folgenden Befehl ein:

Befehl:

```
>shell

#nsapimgr -s mss_table=<16 comma seperated values>
```

Beispiel:

```
#nsapimgr -ys mss_table
   =9176,9156,8192,7168,6144,4196,3072,2048,1460,1400,1330,1212,956,536,384,128


# nsapimgr -d mss_table

MSS table

{
 9176,9156,8192,7168,6144,4196,3072,2048,1460,1400,1330,1212,956,536,384,128
     }

```



```
10
11 Done.
```

Ein Beispiel, das Standardwerte für Ethernet-Größe verwendet, ist unten dargestellt:

Beispiel:

```
1  #nsapimgr -ys mss_table
      =1460,1440,1420,1400,1380,1360,1340,1320,1300,1280,1260,1212,956,536,384,128
2
3  # nsapimgr -d mss_table
4
5  MSS table
6
7  {
8   1460,1440,1420,1400,1380,1360,1340,1320,1300,1280,1260,1212,956,536,384,128
        }
9
10
11 Done.
```

Um diese Änderung auch nach dem Neustart der Citrix ADC Appliance dauerhaft zu machen, fügen Sie den Befehl `##nsapimgr -ys mss_table=<16 comma seperated values>` in die Datei "/nsconfig/rc.netscaler" ein. Wenn die Datei rc.netscaler nicht vorhanden ist, erstellen Sie sie im Ordner /nsconfig und hängen Sie dann den Befehl an.

Speicherüberlastungsschutz

Eine Citrix ADC Packet Processing Engine (PPE) beginnt, Verbindungen von TCP-Optimierung zu umgehen, wenn der von dieser PPE verwendete Speicher mehr als ein spezifizierter hoher Wasserzeichenwert ist. Wenn eine PPE-Speicherauslastung über ~2,6 GB geht, beginnt sie, *alle neuen* Verbindungen von der Optimierung zu umgehen. Die bestehenden Verbindungen (die zuvor zur Optimierung zugelassen wurden) werden weiter optimiert. Dieser Wasserzeichenwert wurde gezielt ausgewählt und wird nicht zum Tuning empfohlen.

> **Hinweis:**
>
> Wenn Sie der Meinung sind, dass es einen guten Grund gibt, diesen Wasserzeichenwert zu ändern, wenden Sie sich an den Kundendienst.

Unterstützung für Happy Eyeballs-Clienst

Wenn die Citrix ADC Appliance ein SYN für ein Ziel empfängt, für das der Status unbekannt ist, überprüft die Appliance zunächst die Erreichbarkeit des Servers und bestätigt dann den Client. Dieser Probing-Mechanismus ermöglicht es Clients mit zwei IP-Stacks, die Erreichbarkeit von Dual-Stack-Internet-Servern zu erkennen. Wenn der Client erkennt, dass sowohl IPv6- als auch IPv4-Zugriff verfügbar ist, stellt er eine Verbindung zum Server her, die schneller reagiert, und setzt den anderen zurück. Wenn die Verbindung für die Citrix ADC Appliance einen Reset erhält, wird die entsprechende serverseitige Verbindung zurückgesetzt.

Hinweis: Diese Funktion verfügt über keine vom Benutzer konfigurierbaren TCP-Einstellungen, die auf der Citrix ADC Appliance deaktiviert bzw. aktiviert werden können.

Weitere Informationen zur Unterstützung von Happy Eyeballs finden Sie unter RFC 6555.

Citrix ADC Videooptimierung

October 5, 2021

Die Citrix ADC Appliance bietet Optimierungstechniken und Funktionen zur Optimierung des ABR-Videoverkehrs für den Videoverkehr über Mobilfunknetze. Dies verbessert die Benutzerfreundlichkeit und reduziert den gesamten Netzwerkbandbreitenverbrauch.

Der Abschnitt enthält die folgenden Themen:

- Schnelleinstieg
- Lizenzierung
- Konfigurieren der Videooptimierung über TCP
- Konfigurieren der Videooptimierung über UDP

Schnelleinstieg

October 5, 2021

Mediendateien treiben immer mehr Datenverkehr über Mobilfunknetze an, und die Migration zu schnelleren Netzwerktechnologien hat das Volumen des verschlüsselten Videoverkehrs drastisch erhöht. Die traditionelle Medienbereitstellungstechnologie (Progressive Download) liefert keine akzeptablen Erfahrungsqualität (QoE) bei hoher Übertragungsrate. Dies hat zur Einführung des Adaptive Bit Rate (ABR) -Protokolls geführt. Es kann die Streaming-Bitrate an die verfügbare Netzwerkbandbreite anpassen und die Streaming-Qualität an die Fähigkeit des Hörers, das das Video

empfängt, einschränken. Das ABR-Protokoll funktioniert jedoch nicht so gut in Mobilfunknetzen wie über das Internet. Mobilfunkbetreiber müssen daher den ABR-Verkehr optimieren.

Eine Citrix ADC Appliance verfügt über einzigartige Funktionen, um eingehenden Videoverkehr zu erkennen und ABR-Videos selektiv zu optimieren.

Funktionsweise der Citrix ADC Videooptimierung

Eine Citrix ADC Appliance kann verschlüsselten ABR-Datenverkehr (einschließlich Facebook-Videoverkehr) über TCP und YouTube ABR-Datenverkehr über QUIC identifizieren und optimieren. Die Appliance verfügt über folgende Funktionen:

1. Erkennen Sie Progressive Download (PD) Videos über HTTP.
2. Erkennen und optimieren Sie ABR-Videos über HTTP.
3. Erkennen und optimieren Sie ABR-Videos über HTTPS.
4. Erkennen und optimieren Sie YouTube ABR-Videos über QUIC.

Außerdem verwendet die Appliance die folgenden Unterstützungsdomänen, um Videoverkehr über TCP und QUIC-Protokolle zu erkennen.

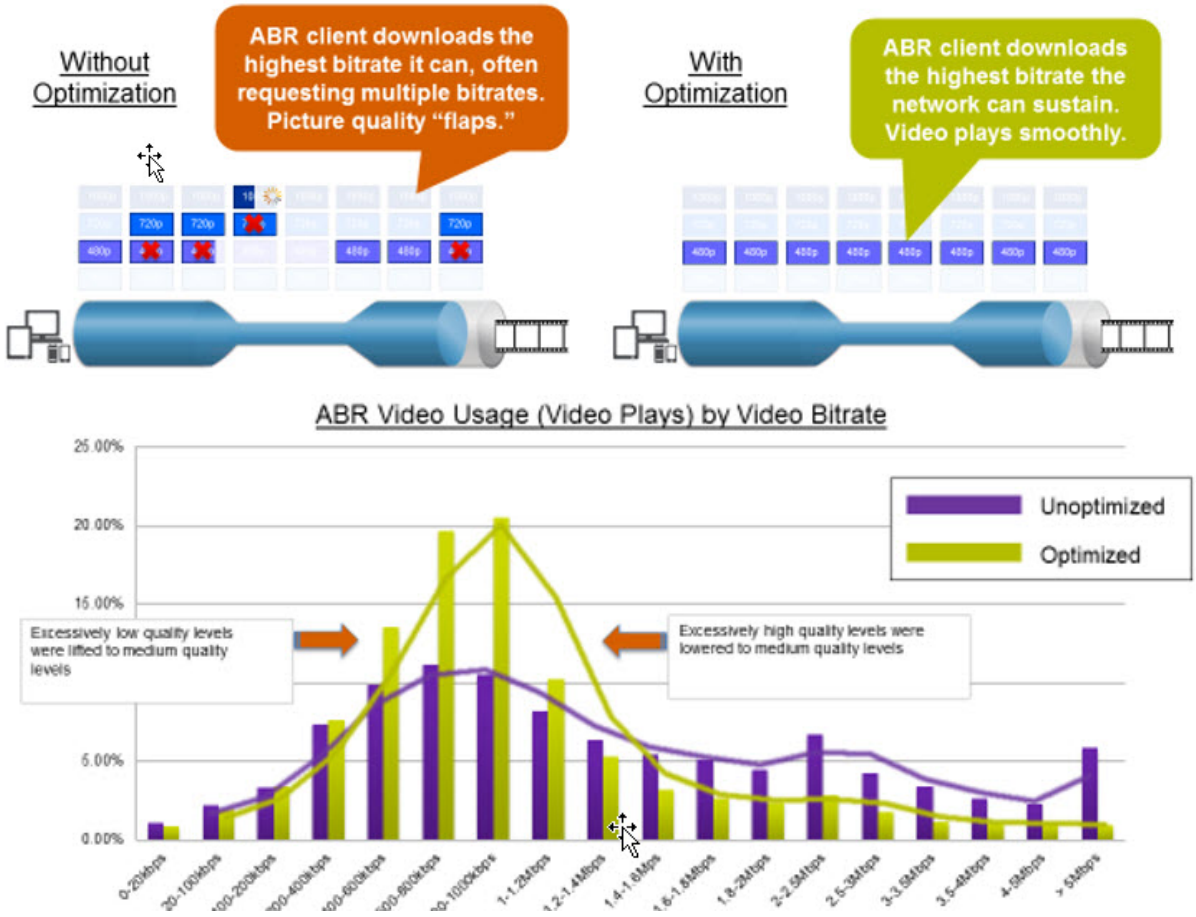
- Unverschlüsselte ABR-Videos über TCP. Die Appliance erkennt alle standardkonformen Video-Streaming-Websites. Die Appliance erkennt ABR-Sitzungen, indem sie die Antwort-Video-Nutzlast-Header, URL- und HTTP-Header überprüft.
- Verschlüsseltes ABR-Video über TCP. Appliance erkennt ABR-Sitzungen mit einem generischen und heuristischen Algorithmus, der auf Domäne, SSL-Header und Verkehrsmustern basiert. Auf diese Weise verfügt die Appliance über eine integrierte Unterstützung, um Top-Video-Websites mit 95 Prozent Genauigkeit zu erkennen, und wir fügen weiterhin Unterstützung für neue Video-Typen hinzu. Citrix ADC verfügt außerdem über ein Programm, mit dem Sie zusätzliche Verifizierung für Top-verschlüsselte ABR-Standorte für eine Region oder ein Land bereitstellen können, um die Netzwerkabdeckung sicherzustellen.
- Verschlüsselte ABR-Videos über QUIC. Die Appliance erkennt ABR-Sitzungen für QUIC-basierte Videoanbieter wie YouTube. Der Erkennungsalgorithmus basiert auf einer heuristischen Nutzung der QUIC-Header und Domäne. Citrix ADC wird weiterhin Unterstützung für neuere Videosites mit QUIC hinzufügen.

Vorteile

Die Optimierung des ABR-Videoverkehrs kann folgende Vorteile bieten:

- Verwalten Sie das Netzwerk während der Überlastung in Spitzenzeiten.
- Verbessern Sie die Konsistenz der Videowiedergabe und reduzieren Sie die Videoabspielung.
- Aktivieren Sie neue Videodienstangebote (z. B. Binge-on-Videodienste).
- Ermöglichen Sie Kunden, die beste nachhaltige Videoqualität auszuwählen.

- Bieten Sie eine konsistente Benutzererfahrung für den Abonnenten.



Videooptimierung über TCP

Citrix ADC Optimierung des ABR-Datenverkehrs über TCP funktioniert wie folgt:

1. HTTP- oder HTTPS-Datenverkehr, den die Appliance über TCP empfängt, wird an den entsprechenden virtuellen Lastausgleichsserver gesendet.
2. Die integrierten Erkennungsrichtlinien, die an den virtuellen Server gebunden sind, in Kombination mit anderen proprietären Erkennungsalgorithmen bewerten den Datenverkehr.
3. Die Richtlinien verwenden eine Reihe integrierter Videoerkennungssignaturen, um den Videotyp zu erkennen. Die Richtlinie, die dem Datenverkehr entspricht, wendet eine Aktion an, die den Videotyp als eine der folgenden Kategorien kategorisiert:
   a) Klartext PD
   b) Klartext ABR
   c) Verschlüsselte ABR
   d) Sonstiges
4. Die an denselben virtuellen Server gebundenen Optimierungsrichtlinien bewerten den Datenverkehr und bestimmen die Optimierungsbitrate für den Datenverkehr.

5. Die Optimierungsbitrate wird angewendet, wenn der Datenverkehr entweder Klartext-ABR oder verschlüsselt ABR ist.

Ein Mobilfunkanbieter kann die Qualität der Erfahrung (QoE) verbessern, indem er die Download-Geschwindigkeit für 2G-, 3G- und 4G-Mobilfunkverkehr einstellt. Dadurch werden die Startzeiten des Videos oder die Pufferung von Ereignissen reduziert. Die Optimierung kann auch die Menge der Netzwerkbandbreite reduzieren, die von Videositzungen belegt wird.

Die Optimierungstechniken umfassen dynamische Burststeuerung und Zufallsabtastung.

Dynamische Burststeuerung

Die Citrix ADC ABR-Optimierung passt sich dynamisch an veränderte Netzwerkbedingungen an. Es ermöglicht eine anfängliche Burstrate von 1,3-fachen der konfigurierten Schrittfrequenz für 15 Sekunden. Die anfängliche Aufteilungsrate gilt für den Beginn jeder optimierten ABR-Videositzung, selbst wenn mehrere Sitzungen dieselbe TCP-Verbindung oder eine Gruppe von TCP-Verbindungen verwenden.

Die Appliance unterstützt auch Wiederherstellungs-Bursts, falls die vom Netzwerk unterstützte Bitrate unter die konfigurierte Schrittfrequenz fällt. Wenn beispielsweise die effektive Bitrate bei der 7. Sekunde abfällt und sich bei der 15. Sekunde des anfänglichen Bursts erholt, stellt die Appliance den Verlust während des nächsten Burst-Zyklus wieder her. Dadurch optimiert die Appliance die Netzwerkbandbreite für alle Teilnehmer dynamisch, sodass die Videoqualität pro Pixel konsistent bleibt.

Hinweis: Wenn ein Wiederherstellungsaufbruch während einer anfänglichen Burst stattfindet, darf die Schrittbitrate die maximalen Recovery-Burst- und Initial-Burst-Raten nicht überschreiten (Sie dürfen den Recovery-Burst-Faktor nicht zusätzlich zum Initial-Burst-Faktor hinzufügen). Andernfalls kann es so schnell sein, dass der Media Player in einen Modus mit höherer Qualität wechselt. Bei Bedarf können Sie jedoch die Dauer der Initial Burst verlängern, um die nicht genutzte Bandbreite zu kompensieren.

Zufallsprobenahme

Um die Einsparungen durch die Videooptimierung abzuschätzen, implementiert die Citrix ADC Appliance Zufallsstichproben. Bei dieser Technik wählt die Appliance nach dem Zufallsprinzip einen konfigurierbaren Prozentsatz des erkannten Videoverkehrs aus (der Parameter Zufallsabtastung ist eine ganze Zahl von 0 bis 100, so dass weniger als 1 Prozent nicht möglich sind). Diese zufällig ausgewählten und nicht optimierten Transaktionen (und Sitzungen) werden zu einer Referenzgruppe, und sie werden in den Transaktionsprotokollen identifiziert (zusammen mit anderen Merkmalen wie Bytegröße und Zeitgeberfelder. Die Eigenschaften der optimierten Sitzungen werden ebenfalls protokolliert, und die Reporting-Engine vergleicht Statistiken der optimierten und Referenzgruppen, um die Einsparungen aus der Optimierung (einschließlich der Einsparungen durch die ABR-Optimierung) abzuschätzen.

Videooptimierung über UDP

Google hat ein neues Transportprotokoll namens QUIC eingeführt. Das QUIC-Protokoll von Google ist TCP+TLS+HTTP/2 sehr ähnlich und wird zusätzlich zu UDP implementiert. Citrix ADC kann YouTube-ABR-Videos erkennen, die über das QUIC-Protokoll gestreamt werden, und die ABR-Videooptimierung auf ähnliche Weise anwenden wie ABR über TCP.

Lizenzierung

October 5, 2021

Die Videooptimierung funktioniert auf Telco-Plattformen mit dem Kauf einer grundlegenden CBM-Lizenz und einer CBM Premium-Lizenz. Für andere Citrix ADC Plattformen funktioniert die Funktion mit dem Kauf einer CNS Premium-Lizenz. Bevor Sie die Videooptimierungsfunktion konfigurieren, muss Ihre Appliance über eine geeignete Lizenz verfügen.

Lizenzunterstützung für Telco-Plattformen:

- **CBM_TXXX_SERVER_Retail.lic**
- **CBM_TPRE_SERVER_Retail.lic**
- **CNS_WEBF_SSERVER_Retail.lic**

Dabei ist XXX der Durchsatz, z. B. Citrix ADC T1000.

Lizenzunterstützung für andere Citrix ADC Plattformen:

- **CNS_XXX_SERVER_PLT_Retail.lic**

Dabei ist XXX der Durchsatz.

Gehen Sie folgendermaßen vor, um eine Premium-Lizenzdatei hochzuladen:

1. Eine gültige Lizenzdatei sollte auf der Citrix ADC Appliance installiert werden. Die Lizenz sollte mindestens so viele Gbit/s unterstützen wie der erwartete maximale Gi-LAN-Durchsatz.

   Lizenzdateien sollten über einen SCP-Client in die /nsconfig/license der Appliance kopiert werden, wie in der Bildschirmaufnahme unten gezeigt.

```
1 > shell ls /nsconfig/license/
2 CNS_V3000_SERVER_PLT_Retail.lic ssl
3 <!--NeedCopy-->
```

2. Führen Sie einen warmen Neustart durch, um sich für die neue Lizenz zu bewerben, wie in der Bildschirmaufnahme unten gezeigt.


```
> reboot -warm
Are you sure you want to restart NetScaler (Y/N)? [N]:y
 Done
<!--NeedCopy-->
```

3. Nachdem der Neustart abgeschlossen ist, stellen Sie sicher, dass die Lizenz ordnungsgemäß angewendet wurde, indem Sie die Show License CLI verwenden.

Im folgenden Beispiel wurde eine Premium-Lizenz mit Premium Edition erfolgreich installiert.

```
    > show license

                License status:

                                        Video Optimization: YES

                                                  ...

                                    Model Number ID: 110050

                                       License Type: Premium License
<!--NeedCopy-->
```

Konfigurieren der Videooptimierung über TCP

December 7, 2021

Um den Videoverkehr über TCP zu optimieren, aktivieren Sie zunächst die Videooptimierungsfunktion. Anschließend aktiviert die Appliance die integrierten Erkennungsrichtlinien, um den eingehenden Videoverkehr zu erkennen und den Videotyp zu identifizieren. Benutzerkonfigurierbare Optimierungsrichtlinien für jeden Videotyp geben die Optimierungsbitrate an, die für die Optimierung des Datenverkehrs erforderlich ist.

Konfigurieren der Videooptimierung über TCP mit der CLI

Um die Videooptimierung auf einer Citrix ADC Appliance zu konfigurieren, führen Sie die folgenden Aufgaben aus:

1. Aktivieren Sie die Videooptimierungsfunktion.
2. Fügen Sie virtuelle Server für HTTP- und HTTPS-Datenverkehr hinzu.

3. Binden Sie alle integrierten Erkennungsrichtlinien an einen virtuellen Lastausgleichsserver für HTTP-Datenverkehr.
4. Binden Sie alle integrierten Erkennungsrichtlinien an einen virtuellen SSL-Bridge-Load Balancing Server für HTTPS-Datenverkehr.
5. Fügen Sie die gewünschten Optimierungsrichtlinien für HTTP- und HTTPS-Datenverkehr hinzu.
6. Binden Sie Optimierungsrichtlinien an einen virtuellen Lastausgleichsserver für HTTP-Datenverkehr.
7. Binden Sie Optimierungsrichtlinien an einen virtuellen SSL-Bridge-Lastausgleichsserver für HTTPS-Datenverkehr.

Aktivieren der Videooptimierung

Wenn die Citrix ADC Appliance Videoverkehr erkennen, optimieren und melden soll, müssen Sie die Videooptimierungsfunktion aktivieren und die Optimierung auf ON festlegen. Nach dem Aktivieren der Funktion können Sie integrierte Erkennungsrichtlinien verwenden, um den eingehenden Videoverkehr zu identifizieren, und Sie können Optimierungsrichtlinien konfigurieren, um verschlüsselten ABR-Datenverkehr zu optimieren. Um den ABR-Videoverkehr zu optimieren, müssen Sie die Download-Bitrate konfigurieren (auch als *Schrittfrequenz*bezeichnet).

Sie müssen auch die Lastenausgleichsfunktion aktivieren, und wenn Sie die Videooptimierung für HTTPS-Datenverkehr verwenden möchten, müssen Sie die SSL-Funktion aktivieren.

So aktivieren Sie die Videooptimierungsfunktion

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
enable ns feature VideoOptimization
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn Sie die Videooptimierungsleistung und Videoeinsichtsberichte überwachen möchten, müssen Sie die AppFlow Funktion aktivieren und dann auf die Video Analytics-Funktion in Citrix Application Delivery Management (ADM) zugreifen. Weitere Informationen finden Sie in der Video Insight-Dokumentation .

Erstellen von virtuellen Servern für HTTP- und HTTPS-Videoverkehr

Eine Citrix ADC Appliance verwendet verschiedene virtuelle Server zum Erkennen und Optimieren der verschiedenen Typen des eingehenden Videoverkehrs. Die Appliance unterstützt die folgenden Typen von virtuellen Servern für TCP-Datenverkehr.

- **Virtueller Server für den HTTP-Lastenausgleich**. Zum Erkennen des HTTP-Videoverkehrs verwendet die Appliance einen virtuellen HTTP-Lastausgleichsserver. Es verwaltet HTTP-Videoanforderungen, die die Appliance von Clients empfängt.
- **SSL-Bridge-Load Balancing virtueller Server**. Um verschlüsselten Videoverkehr zu erkennen, müssen Sie einen virtuellen SSL-Bridge-Server auf der Appliance konfigurieren.

So fügen Sie einen virtuellen HTTP-Load Balancing-Server zum Erkennen von HTTP-Videoverkehr hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb vserver <name> HTTP * 80 -persistenceType NONE
2 <!--NeedCopy-->
```

Beispiel:

```
1 add lb vserver ProxyVserver-HTTP HTTP * 80 -persistenceType NONE -
     cltTimeout 120
2 <!--NeedCopy-->
```

So fügen Sie einen virtuellen SSL Bridge-Server zum Erkennen von HTTPS-Videoverkehr hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb vserver <name> SSL_BRIDGE * 443 -persistenceType NONE
2 <!--NeedCopy-->
```

Beispiel:

```
1 add lb vserver ProxyVserver-SSL SSL_BRIDGE * 443 -persistenceType NONE
     -cltTimeout 180
2 <!--NeedCopy-->
```


Binden integrierter Erkennungsrichtlinien an einen virtuellen HTTP-Lastausgleichsserver

Um den Videoverkehr über eine HTTP-Verbindung zu erkennen, müssen Sie alle integrierten Erkennungsrichtlinien an einen virtuellen Lastausgleichsserver binden. Sie müssen die Richtlinien je nach Richtlinientyp entweder an die Anforderungs- oder Antwortzeitverarbeitung binden.

> **Hinweis:**
>
> Die Richtlinie zur `ns_videoopt_http_body_detection` Videooptimierung unterstützt die `CONNECT` HTTP-Anforderungsmethode nicht.

So binden Sie Erkennungsrichtlinien für verschiedene Videotypen an einen virtuellen HTTP-Lastausgleichsserver

Geben Sie an der Eingabeaufforderung den entsprechenden Befehl für jeden Typ ein. Die verfügbaren Befehle sind:

```
bind lb vserver <name> -policyName ns_videoopt_http_abr_netflix -
    priority <integer> -type (REQUEST | RESPONSE)

bind lb vserver <name>   -policyName ns_videoopt_http_abr_netflix2 -
    priority <integer> -type (REQUEST | RESPONSE)

bind lb vserver <name>   -policyName ns_videoopt_http_abr_youtube -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver <name>    -policyName ns_videoopt_http_pd_youtube -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver <name>    -policyName ns_videoopt_http_pd_youtube2  -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver  <name>   -policyName ns_videoopt_http_pd_youtube3 -
    priority <integer>  -type (REQUEST | RESPONSE)

bind lb vserver  <name>  -policyName ns_videoopt_http_abr_generic -
    priority <integer> -type (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Beispiel:


```
bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_abr_netflix -priority 400  type RESPONSE

bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_abr_netflix2 -priority 500 -type RESPONSE

bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_abr_youtube -priority 600  -type RESPONSE

bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_pd_youtube -priority 800  -type RESPONSE

bind lb vserver ProxyVserver-HTTP    -policyName
    ns_videoopt_http_pd_youtube2 -priority 900 -type RESPONSE

bind lb vserver  ProxyVserver-HTTP   -policyName
    ns_videoopt_http_pd_youtube3 -priority 1000 -type REQUEST

bind lb vserver  ProxyVserver-HTTP   -policyName
    ns_videoopt_http_abr_generic -priority 1100 -type RESPONSE
<!--NeedCopy-->
```

Binden der HTTP-Richtlinie zur Erkennung von Körperinhalten an den virtuellen Lastenausgleich

Um den Videoverkehr über HTTP zu erkennen, müssen Sie die Richtlinie zur Erkennung von Körperinhalten an den virtuellen Lastausgleichsserver binden. Sie können den folgenden Befehl verwenden:

```
bind lb vserver <name> -policyName ns_videoopt_http_body_detection -
    priority <integer> -type (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver ProxyVserver-HTTP -policyName
    ns_videoopt_http_body_detection -priority 1500 -type REQUEST
<!--NeedCopy-->
```


Binden integrierter Erkennungsrichtlinien an einen virtuellen SSL-Bridge-Load Balancing Server

Um den Videoverkehr über eine HTTPS-Verbindung zu erkennen, müssen Sie integrierte Erkennungsrichtlinien an einen virtuellen SSL Bridge-Lastenausgleichsserver binden.

So binden Sie eine Erkennungsrichtlinie an einen virtuellen SSL-Bridge-Lastausgleichsserver

Geben Sie an der Eingabeaufforderung den entsprechenden Befehl für jeden Typ ein. Die verfügbaren Befehle sind:

```
bind lb vserver <name> -policyName ns_videoopt_https_abr_netflix -
    priority <positive_integer> -type (REQUEST | RESPONSE)

bind lb vserver <name> -policyName ns_videoopt_https_abr_youtube -
    priority <positive_integer> -type (REQUEST | RESPONSE)

bind lb vserver <name> -policyName ns_videoopt_https_abr_generic -
    priority <positive_integer> -type (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver ProxyVserver-SSL -policyName
    ns_videoopt_https_abr_netflix -priority 120 -type REQUEST

bind lb vserver ProxyVserver-SSL -policyName
    ns_videoopt_https_abr_youtube -priority 140 -type REQUEST

bind lb vserver ProxyVserver-SSL -policyName
    ns_videoopt_https_abr_generic -priority 150 -type REQUEST
<!--NeedCopy-->
```

Hinzufügen von Optimierungsrichtlinien für den schrittweisen ABR-Datenverkehr

Um den ABR-Datenverkehr zu optimieren, müssen Sie Optimierungsrichtlinien und die zugehörigen Aktionen konfigurieren. Anschließend binden Sie die Richtlinien an dieselben virtuellen Server mit Lastenausgleich, an die Sie die Erkennungsrichtlinien gebunden haben. Erstellen Sie für jede Richtlinie zuerst die Aktion, damit Sie sie beim Erstellen der Richtlinie einschließen können.

So fügen Sie eine Optimierungsaktion hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add videooptimization pacingaction <action Name> -rate <integer> [-
     comment <string>]
2 <!--NeedCopy-->
```

Dabei gibt der Parameter **rate** die Rate in Kbps an, mit der der Datenverkehr gesendet werden soll (die Schrittfrequenz).

Beispiel:

```
1 add videooptimization pacingaction MyOptAct2000 -rate 2000
2 <!--NeedCopy-->
```

So fügen Sie eine Optimierungsrichtlinie hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add videooptimization pacingpolicy <name> -rule <expression> -action <
     string>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add videooptimization pacingpolicy myOptPolicy2000 -rule TRUE -action
     MyOptAct2000
2 <!--NeedCopy-->
```

Binden von Optimierungsrichtlinien an einen virtuellen HTTP-Lastausgleichsserver

Um den ABR-Videoverkehr über eine HTTP-Verbindung zu optimieren, müssen Sie die Optimierungsrichtlinien an einen virtuellen Lastausgleichsserver binden, an den die Erkennungsrichtlinien gebunden sind.

So binden Sie eine Optimierungsrichtlinie an einen virtuellen Load Balancing-Server

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
bind lb vserver <name> -policyName <policy_name> -priority <
    positive_integer> -type  (REQUEST | RESPONSE)
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver ProxyVserver-HTTP -policyName myOptPolicy2000 -priority
     3400 -type  REQUEST
<!--NeedCopy-->
```

Binden von Optimierungsrichtlinien an virtuelle SSL-Bridge-Server

Um den ABR-Videoverkehr über eine HTTPS-Verbindung zu optimieren, müssen Sie die Optimierungsrichtlinien an den virtuellen SSL Bridge-Server binden, an den die integrierten Erkennungsrichtlinien gebunden sind.

So binden Sie eine Optimierungsrichtlinie an den virtuellen SSL Bridge-Server, um verschlüsselten Datenverkehr schrittweise zu erreichen

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
bind lb vserver <name> -policyName <policy_name> -priority <
    positive_integer> -type  (REQUEST |RESPONSE)
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver ProxyVserver-SSL -policyName myOptPolicy2000 -priority
    3400 -type  REQUEST
<!--NeedCopy-->
```

Einstellung der Schrittparameter für die Videooptimierung

Mit der CLI können Sie die Schrittparameter für die Videooptimierung festlegen, z. B.

So legen Sie den Prozentsatz der Zufallsstichproben fest

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set videooptimization parameter  - RandomSamplingPercentage <realNumber>
<!--NeedCopy-->
```

Wo ist eine RealNumber ein Wert zwischen 0,0 und 100,0.

Beispiel:

```
set videooptimization parameter -RandomSamplingPercentage 50
<!--NeedCopy-->
```

Konfigurieren der Videooptimierung über TCP mit der GUI

Mit der GUI können Sie:

- Aktivieren Sie die Videooptimierungsfunktion.
- Erstellen Sie einen virtuellen HTTP-Lastausgleichsserver.
- Erstellen Sie einen virtuellen SSL-Bridge-Load Balancing Server.
- Binden Sie integrierte Erkennungsrichtlinien an den virtuellen HTTP-Lastausgleichsserver.
- Binden Sie integrierte Erkennungsrichtlinien an den virtuellen SSL-Bridge-Load Balancing Server.
- Erstellen Sie eine Optimierungsrichtlinie.
- Erstellen Sie eine Optimierungsaktion.
- Konfigurieren des Optimierungsschrittparameters.
- Binden Sie die Optimierungsrichtlinie zum Lastenausgleich virtueller Server für HTTP-Datenverkehr.
- Binden Sie die Optimierungsrichtlinie an den virtuellen SSL-Bridge-Load Balancing Server für HTTPS-Datenverkehr.

So aktivieren Sie die Videooptimierungsfunktion

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie auf der Seite **Einstellungen** auf den Link **Erweiterte Funktionen konfigurieren** .
3. Aktivieren Sie auf der Seite **Erweiterte Funktionen konfigurieren** das Kontrollkästchen **Videooptimierung** .
4. Klicken Sie auf **OK**und dann auf **Schließen**.

So erstellen Sie einen virtuellen Lastausgleichsserver für HTTP-Datenverkehr

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zur Seite **Traffic Management** > **Load Balancing** > **Virtuelle Server** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie im Fenster Load Balancing Virtual Server die folgenden Parameter fest:
   a) **Name**. Name des virtuellen Lastenausgleichsservers.
   b) **Protokoll**. Protokolltyp als HTTP auswählen
   c) **Typ der IP-Adresse**. IP-Adresstyp: IPv4 oder IPv6.
   d) **IP Adresse**. IPv4- oder IPv6-Adresse, die dem virtuellen Server zugewiesen ist.
   e) **Port**. Portnummer des virtuellen Servers.
4. Klicken Sie auf **OK**, um mit der Konfiguration anderer optionaler Parameter fortzufahren. Weitere Informationen finden Sie unter Erstellen eines virtuellen Servers.
5. Klicken Sie auf **Erstellen** und **Schließen**.

So erstellen Sie einen virtuellen Lastausgleichsserver für HTTPS-Datenverkehr

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zur Seite **Traffic Management** > **Load Balancing** > **Virtuelle Server** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. **Legen Sie im Fenster Load Balancing Virtual Server** die folgenden Parameter fest:
   a) **Name**. Name des virtuellen Lastenausgleichsservers.
   b) **Protokoll**. Wählen Sie den Protokolltyp als SSL-Bridge aus.
   c) **Typ der IP-Adresse**. IP-Adresstyp: IPv4 oder IPv6.
   d) **IP Adresse**. IPv4- oder IPv6-Adresse, die dem virtuellen Server zugewiesen ist.
   e) **Port**. Portnummer des virtuellen Servers.
4. Klicken Sie auf **OK**, um mit der Konfiguration anderer optionaler Parameter fortzufahren. Weitere Informationen finden Sie unter Erstellen eines virtuellen Servers.
5. Klicken Sie auf **Erstellen** und dann auf **Schließen**.

So binden Sie eine integrierte Erkennungsrichtlinie an einen virtuellen Lastausgleichsserver

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zum Fenster **Datenverkehrsverwaltung** > **Lastenausgleich** > **Virtuelle Server** .
2. Wählen Sie im Detailbereich den virtuellen Lastausgleichsserver aus, und klicken Sie auf **Bearbeiten**.
   a) Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.
   b) Klicken Sie im Abschnitt **Richtlinien** auf das Symbol **+**, um auf den Schieberegler **Richtlinien** zuzugreifen.
   c) Legen Sie im Abschnitt **Richtlinien** die folgenden Parameter fest.

   d) Wählen Sie Richtlinie. Wählen Sie eine Richtlinie zur Erkennung von Videooptimierungen aus der Dropdownliste aus.
   e) Wählen Sie Typ aus. Wählen Sie den Richtlinientyp als Anforderung aus.
   f) Klicken Sie auf **Weiter**.
3. Wählen Sie die Richtlinie zur Videoerkennung aus der Liste aus, und klicken Sie auf **Schließen**.

So binden Sie eine integrierte Erkennungsrichtlinie an einen virtuellen SSL-Bridge-Lastausgleichsserver

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zum Fenster **Traffic Management** > **Load Balancing** > **Virtuelle Server** .
2. Wählen Sie im Detailbereich den virtuellen SSL-Bridge-Load Balancing Server aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.
4. Klicken Sie im Abschnitt **Richtlinien** auf das Symbol **+**, um auf den Schieberegler **Richtlinien** zuzugreifen.
5. Legen Sie im Abschnitt **Richtlinien** die folgenden Parameter fest.
   a) Wählen Sie Richtlinie. Wählen Sie die Richtlinie zur Erkennung von Videooptimierungen aus der Dropdownliste aus.
   b) Wählen Sie Typ aus. Wählen Sie den Richtlinientyp als Anforderung aus.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie die Richtlinie zur Videoerkennung aus der Liste aus, und klicken Sie auf **Schließen**.

So erstellen Sie eine Videooptimierungsaktion

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zu **Konfiguration** > **Optimierung** > **Videooptimierung** > **Schrittfolge** > **Aktionen** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **Videooptimierungsschritt erstellen** die folgenden Parameter fest.
   a) **Name**. Name der Optimierungsaktion.
   b) **ABR-Optimierungsrate (Kbps).** Schrittfrequenz, mit der der ABR-Videoverkehr gesendet werden soll. Die Standardrate für die ABR-Optimierung beträgt 1000 Kbps. Der Mindestwert ist 1 und der Maximalwert 2147483647.
   c) **Kommentar**. Eine kurze Beschreibung der Aktion.
4. Klicken Sie auf **Erstellen** und **Schließen**.

So erstellen Sie eine Richtlinie zur Videooptimierung

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zu **Konfiguration** > **Optimierung** > **Videooptimierung** > **Schrittfolge** > **Richtlinien**.

2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **Richtlinie zur Videooptimierung erstellen** die folgenden Parameter fest.
   a) **Name**. Name der Optimierungsrichtlinie
   b) **Ausdruck**. Benutzerdefinierte Regex-Ausdrücke, die die Richtlinie implementieren.
   c) **Aktion:** Optimierungsaktion, die mit der Richtlinie für die Verarbeitung des eingehenden Videoverkehrs verknüpft ist.
   d) **UNDEF-Aktion.** Undefiniertes Ereignis, wenn die eingehende Anforderung nicht mit der Optimierungsrichtlinie übereinstimmt.
   e) **Kommentar**. Eine kurze Beschreibung der Richtlinie.
   f) **Aktion protokollieren.** Wählen Sie die Überwachungsprotokollaktion aus, die die gewünschten Protokollmeldungen erstellt.
4. Klicken Sie auf **Erstellen**und dann auf **Schließen.**

So legen Sie Schrittparameter für die Videooptimierung fest

1. Melden Sie sich bei der Citrix ADC Appliance an und navigieren Sie zu **Konfiguration** > **Optimierung** > **Videooptimierung.**
2. Klicken Sie auf der Seite **Videooptimierung** auf **Video Optimierungseinstellungen ändern** .
3. Legen Sie auf der Seite **Videooptimierungseinstellungen** den folgenden Parameter fest.
   a) **Zufallsstichprobenprozentsatz (%)**. Prozentsatz der Pakete, die für die Zufallsstichprobe ausgewählt wurden.
4. Klicken Sie auf **OK** und **schließen**.

So binden Sie eine Richtlinie zur Videooptimierung an einen virtuellen HTTP-Lastausgleichsserver

1. Melden Sie sich bei der Citrix ADC Appliance an und navigieren Sie zu **Konfiguration** > **Optimierung** > **Videooptimierung**.
2. Klicken Sie auf der Seite **Videooptimierung** auf den Link **Richtlinien-Manager für Videooptimierung** .
3. Legen Sie die folgenden Parameter fest.
   a) **Bind-Punkt**. Der Punkt, an dem die Optimierungsrichtlinie während der Anforderungs- oder Antwortverarbeitung angewendet werden soll.
   b) **Verbindungstyp**. Verbindungstyp als Anforderung oder Antwort.
   c) **Virtueller Server**. Der virtuelle Lastausgleichsserver, an den die Richtlinie gebunden werden soll.
   d) Klicken Sie auf **Weiter**.
4. Führen Sie im Abschnitt **Bindepunkt** eine der folgenden Aktionen aus:
   a) Wählen Sie eine Richtlinie aus der Liste aus.

b) Klicken Sie auf **Bindung hinzufügen**, um auf den Schieberegler **Richtlinienbindung** zuzugreifen.
   i. Wählen Sie eine vorhandene Richtlinie aus, oder fügen Sie eine neue Richtlinie hinzu.
   ii. Geben Sie Bindungsdetails ein, und klicken Sie auf **Binden**.

5. Klicken Sie auf **Schließen**.

So binden Sie eine Richtlinie zur Videooptimierung an einen virtuellen SSL-Bridge Lastausgleichsserver

1. Melden Sie sich bei der Citrix ADC Appliance an und navigieren Sie zu **Konfiguration** > **Optimierung** > **Videooptimierung**.
2. Klicken Sie auf der Seite **Videooptimierung** auf den Link **Richtlinien-Manager für Videooptimierung** .
3. Legen Sie auf der Seite **Richtlinien-Manager für die Videooptimierung** die folgenden Parameter fest.
   a) Verbindungspunkt. Der Punkt, an dem die Optimierungsrichtlinie während der Anforderung/Antwortverarbeitung angewendet werden soll.
   b) Verbindungstyp. Verbindungstyp als Anforderung oder Antwort.
   c) Virtueller Server. Der virtuelle SSL-Bridge-Load Balancing Server, an den die Richtlinie gebunden werden soll.
4. Klicken Sie auf **Weiter**.
5. Führen Sie im Abschnitt **Bindepunkt** eine der folgenden Aktionen aus:
   a) Wählen Sie eine Richtlinienbindung aus der Liste aus.
   b) Klicken Sie auf **Bindung hinzufügen**, um auf den Schieberegler **Richtlinienbindung** zuzugreifen.
      i. Wählen Sie eine vorhandene Richtlinie aus, oder fügen Sie eine neue Richtlinie hinzu.
      ii. Geben Sie Bindungsdetails ein, und klicken Sie auf **Binden**.
6. Klicken Sie auf **Schließen**.

Konfigurieren der Videooptimierung über UDP

December 7, 2021

Um den QUIC ABR-Videoverkehr über UDP zu optimieren, aktivieren Sie zunächst die Videooptimierungsfunktion. Nachdem Sie die Konfiguration abgeschlossen haben, erkennt die Appliance den QUIC-basierten ABR-Videoverkehr und wendet die Optimierungsbitrate an, die auf der Appliance konfiguriert ist.

Konfigurieren der Videooptimierung für QUIC mit der CLI

Um die Videooptimierung für den QUIC-Videoverkehr über UDP zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

1. Aktivieren Sie die Videooptimierung.
2. Erstellen Sie einen QUIC-Dienst.
3. Erstellen Sie einen virtuellen QUIC-Lastenausgleichsserver.
4. Binden Sie den QUIC-Webdienst an den virtuellen Server für den Lastenausgleich.
5. Erstellen Sie eine Richtlinie zur Videooptimierung, um QUIC-basierten UDP-Datenverkehr schrittweise zu gestalten.
6. Binden Sie die Optimierungsrichtlinie an einen virtuellen QUIC-basierten Lastausgleichsserver.

Aktivieren der Videooptimierung für QUIC-Datenverkehr

Wenn die Citrix ADC Appliance Videoverkehr erkennen, optimieren und melden soll, müssen Sie die Videooptimierungsfunktion aktivieren und die Optimierung aktivieren.

> **Hinweis:**
>
> Wenn Sie die Videooptimierung für den QUIC-Datenverkehr verwenden möchten, müssen Sie die Lastenausgleichs- und AppFlow Funktionen aktivieren.

So aktivieren Sie die Videooptimierung

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1 enable ns feature VideoOptimization
2 <!--NeedCopy-->
```

Erstellen eines Dienstes für QUIC-Datenverkehr

Eine Citrix ADC Appliance verwendet einen QUIC-Dienst für den Lastausgleichsserver, um eine Verbindung mit dem Egress-Router im statischen Routing-Modus herzustellen.

> **Hinweis:**
>
> Momentan wird dynamisches Routing nicht unterstützt.

So erstellen Sie einen Lastausgleichs-Webdienst für den QUIC-Videoverkehr

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add service <name> <router-IP> <serviceType> <port> -usip yes -
   useproxyport  [yes | no]
<!--NeedCopy-->
```

Beispiel:

```
add service svc-quic 10.102.29.200 QUIC 443  - usip yes  - useproxyport
   no

where IP address is the internet router address.
<!--NeedCopy-->
```

Erstellen eines virtuellen Lastausgleichsservers für den QUIC-Datenverkehr

Eine Citrix ADC Appliance verwendet einen virtuellen Lastausgleichsserver, um den QUIC-Videoverkehr über UDP zu erkennen und zu optimieren.

So erstellen Sie einen virtuellen Lastausgleichsserver für den QUIC-Videoverkehr

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <serviceType> <ip> <port> -m MAC
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver vs-quic QUIC * 443 -persistenceType NONE -m MAC -
   cltTimeout 120
<!--NeedCopy-->
```

Binden eines QUIC-Webdiensts an den virtuellen Lastausgleichsserver

Nachdem Sie die Webdienste und den Lastenausgleichsserver für den QUIC-Datenverkehr erstellt haben, müssen Sie die Dienste an den virtuellen Server binden.

So binden Sie einen Webdienst an den Lastenausgleich virtueller Server für den QUIC-Videoverkehr

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel:

```
bind lb vserver vs-quic svc-quic
<!--NeedCopy-->
```

Erstellen von Videooptimierungsrichtlinien für QUIC-basierten UDP-Datenverkehr

Um den QUIC-basierten UDP-Datenverkehr zu optimieren, müssen Sie Richtlinien für Optimierungsschritte und deren Aktionen konfigurieren. Anschließend müssen Sie die Richtlinien an virtuelle QUIC-basierte Lastenausgleichsserver binden. Erstellen Sie für jede Richtlinie zuerst eine Aktion, damit Sie sie der Richtlinie zuordnen können.

So fügen Sie eine Optimierungsaktion hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add videooptimization pacingaction <action Name> -rate <integer> [-
   comment <string>]
<!--NeedCopy-->
```

Dabei gibt der Parameter **rate** die Rate in Kbps an, mit der der Datenverkehr gesendet werden soll (die Schrittfrequenz).

Beispiel:

```
set videooptimization parameter -QUICPacingRate 1000
<!--NeedCopy-->
```

wobei 1000 die gewünschte Schrittgeschwindigkeit in kBit/s darstellt.

So fügen Sie eine Optimierungsrichtlinie hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add videooptimization pacingpolicy <name> -rule <expression> -action <
     string>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add videooptimization pacingpolicy myOptPolicy2000 -rule TRUE -action
     MyOptAct2000
2 <!--NeedCopy-->
```

Binden von Optimierungsrichtlinien an einen virtuellen QUIC-Load Balancing Server

Um den QUIC-Videoverkehr über eine UDP-Verbindung zu optimieren, müssen Sie die Optimierungsrichtlinien an einen virtuellen QUIC-Lastausgleichsserver binden.

So binden Sie eine Optimierungsrichtlinie an einen virtuellen QUIC-Load Balancing-Server

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1 bind lb vserver <name> -policyName <policy_name> -priority <
     positive_integer> -type (REQUEST)
2 <!--NeedCopy-->
```

> **Hinweis:**
>
> Die Schrittrichtlinien müssen nur zum Anforderungszeitpunkt an einen virtuellen QUIC-Lastausgleichsserver gebunden sein.

Beispiel:

```
1 bind lb vserver vs-quic -policyName myOptPolicy2000 -priority 3400 -
     type  REQUEST
2 <!--NeedCopy-->
```


Konfigurieren der Videooptimierung für QUIC mit der GUI

Um die Funktion auf der Appliance über die GUI zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

1. Videooptimierung aktivieren
2. Konfigurieren eines QUIC-Servers
3. Konfigurieren des QUIC-Dienstes
4. Konfigurieren eines virtuellen QUIC-Lastausgleichsservers
5. Binden Sie den QUIC-Webdienst an den virtuellen Lastausgleichsserver
6. Optimierungsrichtlinie erstellen.
7. Optimierungsaktion erstellen.
8. Konfigurieren des Optimierungsschrittparameters.
9. Binden Sie die Optimierungsrichtlinie zum Lastenausgleich virtueller Server für QUIC-Datenverkehr.

So aktivieren Sie die Videooptimierung

1. Melden Sie sich bei der Citrix ADC Appliance an und navigieren Sie zu **System** > **Einstellungen.**
2. Wählen Sie auf der Detailseite den Link **Erweiterte Funktionen konfigurieren** aus.
3. Aktivieren Sie auf der Seite **Erweiterte Funktionen konfigurieren** das Kontrollkästchen **Videooptimierung** .

So erstellen Sie einen QUIC-Server

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zum Fenster **Traffic Management** > **Load Balancing** > **Server** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **Server erstellen** die folgenden Parameter fest:
   a) Name. Name des QUIC-Servers.
   b) IP-Adresse. IP-Adresse des QUIC-Servers
   c) Traffic-Domain. Domänenname des Servers.
   d) Aktivieren nach dem Erstellen. Anfangszustand des Servers.
   e) Kommentare. Kurze Informationen über den Server.
4. Klicken Sie auf **Erstellen**.

So erstellen Sie einen QUIC-Dienst

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zum Fenster **Traffic Management** > **Load Balancing** > **Services**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.

3. Legen Sie auf der Seite **Load Balancing Service** die folgenden Parameter fest:
   a) **Name des Dienstes**. Name des QUIC-Dienstes.
   b) **IP-Adresse**. IP-Adresse, die dem QUIC-Dienst zugewiesen ist.
   c) **Protokoll**. Wählen Sie das Protokoll als QUIC aus.
   d) **Port**. Portnummer des Webdienstes.
4. Klicken Sie auf **OK**, um fortzufahren. Sie können dann andere optionale Parameter konfigurieren. Weitere Informationen finden Sie unter Dienste konfigurieren.
5. Nachdem Sie die optionalen Parameter konfiguriert haben, klicken Sie auf **OK** und **Schließen** .

So erstellen Sie einen virtuellen Lastausgleichsserver

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zum Fenster **Traffic Management** > **Load Balancing** > **Virtuelle Server** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **Virtueller Server für den Lastausgleich** die folgenden Parameter fest:
   a) **Name**. Name des virtuellen Lastenausgleichsservers.
   b) **Protokoll**. Das Protokoll, das vom Dienst zum Senden von QUIC-Anforderungen verwendet wird.
   c) IP-Adresstyp. IP-Adresstyp: IPv4 oder IPv6.
   d) **IP Adresse**. IP 4 oder IP6 IP-Adresse, die dem virtuellen Server zugewiesen ist.
   e) **Port**. Portnummer des virtuellen Servers.
4. Klicken Sie auf OK, um mit der Konfiguration anderer optionaler Parameter fortzufahren. Weitere Informationen finden Sie unter Erstellen eines virtuellen Servers.

So binden Sie einen virtuellen Lastausgleichsserver an einen QUIC-Dienst

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und wählen Sie einen virtuellen Server aus.
2. Klicken Sie auf **Dienste und Dienstgruppen**, um das Fenster **Load Balancing Virtual Server Service Binding** aufzurufen.
3. Wählen Sie einen QUIC-basierten Webdienst aus, und klicken Sie auf **Binden**.
4. Klicken Sie auf **Fertig**.

So binden Sie einen virtuellen Lastausgleichsserver an einen QUIC-Dienst

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und wählen Sie einen virtuellen Server aus.
2. Klicken Sie auf **Dienste und Dienstgruppen** , um das Fenster **Load Balancing Virtual Server Service Binding**aufzurufen.
3. Wählen Sie einen QUIC-basierten Webdienst aus, und klicken Sie auf **Binden**.

4. Klicken Sie auf **Fertig**.

So erstellen Sie eine Videooptimierungsaktion für den QUIC-Datenverkehr

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zu **Konfiguration** > **Optimierung** > **Videooptimierung** > **Schrittfolge** > **Aktionen** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **Videooptimierungsschritt erstellen** die folgenden Parameter fest.
   a) **Name**. Name der Optimierungsaktion.
   b) **ABR-Optimierungsrate (Kbps).** Schrittfrequenz, mit der der ABR-Videoverkehr gesendet werden soll. Die Standardrate für die ABR-Optimierung beträgt 1000 Kbps. Der Mindestwert ist 1 und der Maximalwert 2147483647.
   c) **Kommentar**. Eine kurze Beschreibung der Aktion.
4. Klicken Sie auf **Erstellen** und **Schließen**.

So erstellen Sie eine Richtlinie zur Videooptimierung für den QUIC-Datenverkehr

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zu **Konfiguration** > **Optimierung** > **Videooptimierung** > **Schrittfolge** > **Richtlinien**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **Richtlinie zur Videooptimierung erstellen** die folgenden Parameter fest.
   a) Name. Name der Optimierungsrichtlinie
   b) Ausdruck. Benutzerdefinierte Bedauern Ausdrücke, die die Richtlinie implementieren.
   c) Aktion: Optimierungsaktion, die mit der Richtlinie für die Verarbeitung des eingehenden Videoverkehrs verknüpft ist.
   d) UNDEF Aktion. Undefiniertes Ereignis, wenn die eingehende Anforderung nicht mit der Optimierungsrichtlinie übereinstimmt.
   e) Kommentieren. Eine kurze Beschreibung der Richtlinie.
   f) Aktion protokollieren. Wählen Sie die Überwachungsprotokollaktion aus, die die gewünschten Protokollmeldungen erstellt.
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So binden Sie eine Richtlinie zur Videooptimierung an einen virtuellen QUIC-Lastausgleichsserver

1. Melden Sie sich bei der Citrix ADC Appliance an und navigieren Sie zu **Konfiguration** > **Optimierung** > **Videooptimierung**.
2. Klicken Sie auf der Seite **Videooptimierung** auf den Link **Richtlinien-Manager für Videooptimierung** .

3. Legen Sie auf der Seite **Richtlinien-Manager für die Videooptimierung** die folgenden Parameter fest.
   a) Verbindungspunkt. Der Punkt, an dem die Optimierungsrichtlinie während der Anforderungsverarbeitung angewendet werden soll. **Hinweis**: Die Schrittrichtlinien müssen nur zum Anforderungszeitpunkt an einen virtuellen QUIC-Lastausgleichsserver gebunden sein.
   b) Verbindungstyp. Verbindungstyp als Anforderung oder Antwort.
   c) Virtueller Server. Der virtuelle Lastausgleichsserver, an den die Richtlinie gebunden werden soll.
4. Klicken Sie auf **Weiter**.
5. Führen Sie im Abschnitt **Bindepunkt** eine der folgenden Aktionen aus:
   a) Wählen Sie eine Richtlinie aus der Liste aus.
   b) Klicken Sie auf **Bindung hinzufügen**, um auf den Schieberegler **Richtlinienbindung** zuzugreifen.
      i. Wählen Sie eine vorhandene Richtlinie aus, oder fügen Sie eine neue Richtlinie hinzu.
      ii. Geben Sie Bindungsdetails ein, und klicken Sie auf **Binden**.
6. Klicken Sie auf **Schließen**.

Citrix ADC URL-Filter

October 5, 2021

Die URL-Filterung ermöglicht die richtlinienbasierte Steuerung von Websites mithilfe der in URLs enthaltenen Informationen. Diese Funktion hilft Netzwerkadministratoren, den Benutzerzugriff auf bösartige Websites in Mobilfunknetzen zu überwachen und zu steuern.

Als Administrator können Sie eine URL-Filterrichtlinie mithilfe der URL-Kategorisierungsfunktion oder der URL-Liste konfigurieren.

URL-Liste. Steuert den Zugriff auf Websites und Webseiten in der Sperrliste, indem der Zugriff auf URLs blockiert wird, die sich in einem in die Appliance importierten URL-Satz befinden.

URL-Kategorisierung. Steuert den Zugriff auf Websites und Webseiten, indem der Datenverkehr anhand einer vordefinierten Liste von Kategorien gefiltert wird.

URL-Liste

December 7, 2021

Mit der URL-Listen-Funktion können Sie den Zugriff auf benutzerdefinierte URL-Listen (bis zu einer Million Einträge) steuern. Das Feature filtert Websites, indem eine URL-Filterrichtlinie angewendet wird, die an einen virtuellen Server gebunden ist.

Als Administrator müssen Sie die URL-Liste in die Citrix ADC Appliance importieren. Diese importierte Liste wird intern als Richtliniendatensatz gespeichert, der als *URL-Set*bezeichnet wird. Die Appliance wendet dann einen eindeutigen schnellen URL-Übereinstimmungsalgorithmus auf die eingehenden URL-Anforderungen an. Wenn die eingehende URL-Anforderung mit einem Eintrag in der Gruppe übereinstimmt, wendet die Appliance die zugeordnete Richtlinienaktion an, um den Zugriff zu steuern.

URL-Listentypen

Jeder Eintrag in einem URL-Satz kann eine URL und optional deren Metadaten (URL-Kategorie, Kategoriegruppen oder andere verwandte Daten) enthalten. Bei URLs mit Metadaten verwendet die Appliance einen Richtlinienausdruck, der die Metadaten auswertet. Weitere Informationen finden Sie unter URL-Sets.

Benutzerdefinierte URL-Liste. Sie können einen benutzerdefinierten URL-Satz mit bis zu 1.000.000 URL-Einträgen erstellen und als Textdatei in Ihre Appliance importieren. Die Liste kann URLs mit oder ohne Metadaten enthalten (was wie eine URL-Kategorie sein könnte). Die Citrix ADC-Plattform erkennt automatisch, ob Metadaten vorhanden sind. Es unterstützt auch das sichere Speichern der importierten Listen. Weitere Informationen finden Sie unter URL-Set.

Sie können die URL-Liste hosten und die Citrix ADC Appliance so konfigurieren, dass die Liste regelmäßig aktualisiert wird, ohne dass ein manueller Eingriff erforderlich ist. Sobald die URL-Liste aktualisiert wurde, kann die Appliance automatisch die Metadaten und Kategorien erkennen, indem sie Richtlinienausdrücke verwenden, um jede eingehende URL auszuwerten und dann Aktionen wie Zulassen, Blockieren, Umleiten oder Benachrichtigen des Benutzers anwenden.

URL-Listen-Richtlinienausdrücke

In der folgenden Tabelle werden die grundlegenden Ausdrücke beschrieben, die Sie zum Auswerten des eingehenden Datenverkehrs verwenden können. Nachdem Sie eine URL-Liste in die Appliance importiert haben, wird sie als *URL-Set*bezeichnet.

Ausdruck	Vorgang
`<URL expression>.URLSET_MATCHES_ANY (<URLSET>)`	Wertet TRUE aus, wenn die URL genau mit einem Eintrag im URL-Set übereinstimmt.

Ausdruck	Vorgang
<URL expression>. GET_URLSET_METADATA(<URLSET>)	Der Ausdruck GET_URLSET_METADATA () gibt die zugeordneten Metadaten zurück, wenn die URL genau einem Muster innerhalb des URL-Sets entspricht. Eine leere Zeichenfolge wird zurückgegeben, wenn keine Übereinstimmung vorhanden ist.
<URL expression>.GET_ URLSET_METADATA(<URLSET>).EQ(< METADATA>)	Wertet TRUE aus, wenn die übereinstimmenden Metadaten gleich sind <METADATA>.
<URLexpression>.GET_URLSET_METADATA (<URLSET>).TYPECAST_LIST_T(‘,’).GET (0).EQ(<CATEGORY>)	Wertet TRUE aus, wenn sich die übereinstimmenden Metadaten am Anfang der Kategorie befindet. Dieses Muster kann verwendet werden, um separate Felder innerhalb von Metadaten zu kodieren, aber nur mit dem1st Feld übereinstimmen.
HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL)	Verbindet die Host- und URL-Parameter, die dann als<URL expression> Abgleich verwendet werden können.

URL-Listen-Richtlinienaktionen

Die häufigste Erzwingungsaktion für URLs, die einer URL-Liste entsprechen, besteht darin, den Zugriff zu beschränken. Erstellen Sie eine URL-Listenrichtlinie mit einem gewünschten URL-Listenausdruck und Erzwingungsaktion. Die Verwendung der Richtliniengruppe hängt vom Typ des eingehenden Datenverkehrs (HTTP oder HTTPS) und dem auf der Appliance konfigurierten virtuellen Server ab. Sie können eine Responder-Richtlinie für HTTP-Datenverkehr oder eine Videooptimierungsrichtlinie für HTTPS-Datenverkehr verwenden. Geben Sie Aktionen an, die auf die URLs angewendet werden sollen, die mit den Ausdrücken in den Richtlinien übereinstimmen. In der folgenden Tabelle sind die verfügbaren Aktionen aufgeführt.

Aktionstyp	Richtlinie	Beschreibung
ALLOW	Responder	Erlauben Sie der Anforderung, auf die Ziel-URL zuzugreifen.

Aktionstyp	Richtlinie	Beschreibung
REDIRECT	Responder	Leiten Sie die Anforderung an die URL um, die als Ziel angegeben ist.
DENY	Responder	Verweigern Sie die Anfrage.
RESET	Responder, VideoOptimization	Setzen Sie die Verbindung zurück.
DROP	Responder, VideoOptimization	Verlassen Sie die Verbindung.

Voraussetzungen

Um die URL-Listen-Funktion zu konfigurieren, stellen Sie sicher, dass Sie den folgenden Server konfiguriert haben.

DNS-Server für DNS-Anforderungen

Sie müssen einen DNS-Server konfigurieren, wenn Sie einen URL-Satz von einer Hostnamen-URL importieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add dns nameServer ((<IP> [-local]) | <dnsVserverName>) [-state (
     ENABLED | DISABLED )] [-type <type>] [-dnsProfileName <string>]
2 <!--NeedCopy-->
```

Beispiel:

```
1 add dns nameServer 10.140.50.5
2 <!--NeedCopy-->
```

Importieren einer benutzerdefinierten URL-Liste

Informationen zum Importieren eines URL-Sets finden Sie unter Thema “URL-Sets” .

Konfigurieren einer URL-Liste für HTTP-Datenverkehr

Die Citrix ADC Appliance unterstützt HTTP- und HTTPS-Datenverkehr. Gehen Sie wie folgt vor, um einen virtuellen Lastausgleichsserver für HTTP-Datenverkehr zu konfigurieren und URL-Listenrichtlinien an den Server zu binden:

- URL-Listen-Aktionen hinzufügen.
- URL-Listen-Richtlinien hinzufügen.
- Hinzufügen eines virtuellen HTTP-Lastausgleichsservers für HTTP-Datenverkehr
- Binden Sie die URL-Listen-Richtlinien an den virtuellen HTTP-Lastausgleichsserver für HTTP-Datenverkehr

So fügen Sie eine URL-Listenaktion hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add responder action <name> <type> (<target> | <htmlpage>) [-comment <
     string>] [-responseStatusCode <positive_integer>] [-reasonPhrase <
     string>]
2 <!--NeedCopy-->
```

So fügen Sie einen virtuellen HTTP-Lastausgleichsserver für HTTP-Datenverkehr hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb vserver <name> [-td <positive_integer>] <serviceType> [-cltT
     imeout <secs>]
2 <!--NeedCopy-->
```

Beispiel:

```
1 add lb vserver vsrv-HTTP HTTP * 80 -persistenceType NONE -cltTimeout
     120
2 <!--NeedCopy-->
```

So binden Sie URL-Listenrichtlinie an den virtuellen HTTP-Lastausgleichsserver

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
bind lb vserver <vServerName> -policyName <string> [-priority <
    positive_integer>]
<!--NeedCopy-->
```

URL-Liste für HTTPS-Datenverkehr konfigurieren

Die Citrix ADC Appliance unterstützt HTTP- und HTTPS-Datenverkehr. Gehen Sie folgendermaßen vor, um einen virtuellen SSL-Bridge-Lastausgleichsserver für HTTPS-Datenverkehr zu konfigurieren und URL-Listenrichtlinien an den Server zu binden:

- URL-Listen-Aktionen hinzufügen.
- URL-Listen-Richtlinien hinzufügen.
- Hinzufügen eines virtuellen SSL-Bridge-Lastausgleichsservers für HTTP-Datenverkehr
- Binden Sie die URL-Listen-Richtlinien an den virtuellen SSL-Bridge-Load Balancing Server für HTTP-Datenverkehr

So fügen Sie eine URL-Listen-Richtlinie für HTTPS-Datenverkehr hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add videooptimization detectionpolicy <name> -rule <expression> -action
     <string> [-undefAction <string>] [-comment <string>] [-logAction <
    string>]
<!--NeedCopy-->
```

So fügen Sie einen virtuellen SSL-Bridge-Lastausgleichsserver hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> [-td <positive_integer>] <serviceType> [-cltT
    imeout <secs>]
<!--NeedCopy-->
```

Beispiel:


```
add lb vserver vsrv-HTTPS SSL_BRIDGE * 443 -persistenceType NONE -
    cltTimeout 180
<!--NeedCopy-->
```

So binden Sie URL-Listen-Richtlinie mit SSL-Bridge-Lastenausgleich mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <vServerName> -policyName <string> [-priority <
    positive_integer>]
<!--NeedCopy-->
```

Konfigurieren einer URL-Liste mit der GUI

Mit der GUI können Sie:

- Importieren Sie eine URL-Liste.
- Fügen Sie eine URL-Liste hinzu.
- URL-Listenaktionen konfigurieren.
- Konfigurieren Sie URL-Listenrichtlinien für HTTP-Datenverkehr.
- Fügen Sie einen virtuellen HTTP-Lastausgleichsserver für HTTP-Datenverkehr hinzu.
- Fügen Sie einen virtuellen SSL-Bridge-Load Balancing Server für HTTPS-Datenverkehr hinzu.
- Binden Sie URL-Listenrichtlinien an den virtuellen HTTP-Lastausgleichsserver.
- Binden Sie eine URL-Listen-Richtlinien an den virtuellen SSL-Bridge-Load Balancing Server.

So importieren Sie eine URL-Liste

1. Erweitern Sie im Navigationsbereich **AppExpert** > **URL-Sets**.
2. Klicken Sie im Detailbereich auf **Importieren**.
3. Legen Sie auf der Seite **URL-Set konfigurieren** die folgenden Parameter fest.
   a) **Name**. Name des URL-Sets.
   b) **URL**. Webadresse des Speicherorts, an dem auf das URL-Set zugegriffen werden soll.
   c) **Überschreiben**. Überschreiben Sie einen zuvor importierten URL-Satz.
   d) **Trennzeichen**. Zeichensequenz, die einen CSV-Dateidatensatz abgrenzt.
   e) **Zeilentrennzeichen**. Zeilentrennzeichen, das in der CSV-Datei verwendet wird. Ein einzelner Zeichenwert ist zulässig, z. B. /n.
   f) **Intervall**. Intervall in Sekunden, abgerundet auf die nächsten 15 Minuten, in denen die URL-Einstellung aktualisiert wird.

g) **Privates Set.** Option, um den Export des URL-Sets zu verhindern
h) **Kanarische URL**. Interne URL zum Testen, ob der Inhalt des URL-Sets vertraulich behandelt werden soll. Die maximale Länge der URL beträgt 2047 Zeichen

4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So fügen Sie eine URL-Liste hinzu

1. Erweitern Sie im Navigationsbereich **AppExpert** > **URL-Sets**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **URL-Set erstellen** die folgenden Parameter fest.
   a) **Name**. Der Name des URL-Sets, der beim Importieren angegeben wurde.
   b) **Kommentare**. Eine kurze Beschreibung des URLs.
4. Klicken Sie auf **Erstellen**.

So konfigurieren Sie eine URL-Listenaktion

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zur Registerkarte **Konfiguration** .
2. Navigieren Sie im Menübereich zu **AppExpert** > **Responder** > **Aktionen** .
3. Klicken Sie im Detailbereich auf **Hinzufügen**.
4. Legen Sie auf der Seite **Responder-Aktion erstellen** die folgenden Parameter fest.
   a) **Name**. Name der Richtlinienaktion URL-Liste.
   b) **Geben Sie ein**. Wählen Sie einen Aktionstyp aus.
   c) **Ausdruck**. Verwenden Sie den Ausdrucksеditor, um den Richtlinienausdruck zu erstellen.
   d) **Kommentare**. Eine kurze Beschreibung der Richtlinienaktion.
5. Klicken Sie auf **Erstellen** und **Schließen**.

So konfigurieren Sie eine URL-Listenrichtlinie

1. Erweitern Sie im Navigationsbereich **AppExpert** > **Responder** > **Richtlinien** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **Responder-Richtlinie erstellen** die folgenden Parameter fest.
   a) **Name**. Name der Richtlinienaktion URL-Liste.
   b) **Aktion:** Wählen Sie die URL-Liste Aktion aus, die Sie der Richtlinie zuordnen möchten.
   c) **Aktion protokollieren**. Wählen Sie die Protokollaktion aus.
   d) **AppFlow**. Wählen Sie eine AppFlow Aktion aus.
   e) **Ausdruck**. Verwenden Sie den Ausdrucksеditor, um den Richtlinienausdruck zu erstellen.
   f) **Kommentare**. Eine kurze Beschreibung der Richtlinie.
4. Klicken Sie auf **Erstellen** und **Schließen**.

So fügen Sie einen virtuellen HTTP-Lastausgleichsserver hinzu

1. Navigieren Sie zur Seite **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. **Legen Sie im Fenster Load Balancing Virtual Server** die folgenden Parameter fest:
   a) **Name**. Name des virtuellen Lastenausgleichsservers.
   b) **Protokoll**. Wählen Sie den Protokolltyp als HTTP.
   c) **Typ der IP-Adresse**. IP-adressierbarer Typ.
   d) **IP Adresse**. IP 4 oder IP6 IP-Adresse, die dem virtuellen Server zugewiesen ist.
   e) **Port**. Portnummer des virtuellen Servers.
4. Klicken Sie auf **OK**, um mit der Konfiguration anderer optionaler Parameter fortzufahren. Weitere Informationen finden Sie unter Erstellen eines virtuellen Servers.

So binden Sie eine URL-Listen-Richtlinie an den virtuellen HTTP-Lastausgleichsserver

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Lastausgleichsserver aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.
4. Klicken Sie im Abschnitt **Richtlinien** auf das Symbol **+**, um auf den Schieberegler **Richtlinien** zuzugreifen.
5. Legen Sie im Abschnitt **Richtlinien** die folgenden Parameter fest.
   a) Wählen Sie Richtlinie. Wählen Sie eine URL-Kategorisierungsrichtlinie aus der Dropdownliste aus.
   b) Wählen Sie Typ aus. Wählen Sie den Richtlinientyp als Anforderung aus.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie auf der Seite Richtlinien die URL-Listen-Richtlinie aus der Liste aus, und klicken Sie auf **Auswählen**.
8. Klicken Sie im Schieberegler **Richtlinien** auf **Binden** und **Schließen** .

So fügen Sie URL-Listen-Richtlinie für HTTPS-Datenverkehr hinzu

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zu **Konfiguration** > **Optimierung** > **Videooptimierung** > **Erkennung** .
2. Klicken Sie auf der Seite **Erkennung** auf den Link **Richtlinien für die Erkennung von Videooptimierungen** .
3. Klicken Sie auf der Seite " **Richtlinien zur Videooptimierung** " auf **Hinzufügen**.
4. Legen Sie auf der Seite **Richtlinie zur Videooptimierung erstellen** die folgenden Parameter fest.
   a) **Name**. Name der Optimierungsrichtlinie

b) **Ausdruck**. Konfigurieren Sie die Richtlinie mithilfe benutzerdefinierter Ausdrücke.
c) **Aktion:** Optimierungsaktion, die mit der Richtlinie für die Verarbeitung des eingehenden Videoverkehrs verknüpft ist.
d) **UNDEF Aktion**. Undefiniertes Ereignis, wenn die eingehende Anforderung nicht mit der Optimierungsrichtlinie übereinstimmt.
e) **Kommentar**. Eine kurze Beschreibung der Richtlinie.
f) **Aktion protokollieren**. Wählen Sie eine Überwachungsprotokollaktion aus, die die Aktion angibt, die für die Protokollmeldungen ausgeführt werden soll.

5. Klicken Sie auf **Erstellen** und **Schließen**.

So fügen Sie einen virtuellen SSL-Bridge-Lastausgleichsserver für HTTPS-Datenverkehr hinzu

1. Navigieren Sie zur Seite **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. **Legen Sie im Fenster Load Balancing Virtual Server** die folgenden Parameter fest:
   a) **Name**. Name des virtuellen Lastenausgleichsservers.
   b) **Protokoll**. Wählen Sie den Protokolltyp als SSL-Bridge aus.
   c) **Typ der IP-Adresse**. IP-Adresstyp: IPv4 oder IPv6.
   d) **IP Adresse**. IPv4- oder IP6VIP-Adresse, die dem virtuellen Server zugewiesen ist.
   e) **Port**. Portnummer des virtuellen Servers.
4. Klicken Sie auf **OK**, um mit der Konfiguration anderer optionaler Parameter fortzufahren. Weitere Informationen finden Sie unter “Erstellen eines virtuellen Servers”.

So binden Sie eine URL-Listen-Richtlinie an den virtuellen SSL-Bridge-Lastausgleichsserver

1. Navigieren Sie in das Fenster **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen SSL-Bridge-Load Balancing Server aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.
4. Klicken Sie im Abschnitt **Richtlinien** auf das Symbol **+**, um auf den Schieberegler **Richtlinien** zuzugreifen.
5. Legen Sie die folgenden Parameter fest.
   a) **Wählen Sie Richtlinie.** Wählen Sie in der Dropdownliste die Richtlinie zur Videoerkennung aus.
   b) **Wählen Sie Typ aus**. Wählen Sie den Richtlinientyp als Anforderung aus.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie die Richtlinie zur Videoerkennung aus der Liste aus, und klicken Sie auf **Schließen**.

Konfigurieren von Überwachungsprotokoll-Messaging

Mit der Auditprotokollierung können Sie eine Bedingung oder eine Situation in einer beliebigen Phase des URL-Listenprozesses überprüfen. Wenn eine Citrix ADC-Appliance eine eingehende URL empfängt und die Responderrichtlinie über einen erweiterten Richtlinienausdruck URL-Sets verfügt, erfasst das Auditprotokoll-Feature URL-Set-Informationen in der URL und speichert die Details als Protokollnachricht für jedes Ziel, das durch die Auditprotokollierung zulässig ist.

Die Protokollmeldung enthält die folgenden Informationen:

1. Zeitstempel.
2. Protokollnachrichtentyp.
3. Die vordefinierten Protokollstufen (Critical, Error, Notice, Warning, Informational, Debug, Alert und Emergency).
4. Meldungsinformationen wie URL-Setname, Richtlinienaktion, URL protokollieren.

Um die Auditprotokollierung für URL-Listenfunktion zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

1. Überwachungsprotokoll aktivieren.
2. Aktion “Auditprotokoll erstellen”
3. Legen Sie die Richtlinie für URL-Listen-Responder mit Auditprotokoll-Nachrichtenaktion fest.

Weitere Informationen finden Sie unter Audit-Protokollierung.

URL-Liste Semantik

In der folgenden Tabelle werden die URL-Übereinstimmungsmuster aufgeführt und beschrieben, wie die URLs in einer URL-Liste mit den URLs für einkommende Anfragen abgeglichen werden. Beispielsweise entspricht das Muster www.example.com/bar nur einer Seite unter www.example.com/bar. Um alle Seiten abzugleichen, deren URL mit ‘www.example.com/bar’ beginnt, fügen Sie am Ende der URL ein Sternchen (*) hinzu.

Semantik	URL-Muster	Abgestimmt	Unübertroffen
Subdomain-Matching	domain.com	domain.com; www.domain.com; sub.one.domain.com	yourdomain.com; wwwdomain.com
URL-Übereinstimmung, exakter Pfad	domain.com/example/bar/index.html	domain.com/example/bar/index.html; www.domain.com/example/bar/index.html; sub.domain.com/example/bar/index.html	www.domain.com/example/bar/index.html/
URL-Übereinstimmung, exakter Pfad	domain.com/example/l	domain.com/example/l www.domain.com/exar sub.domain.com/example	wwwdomaincom/example/bar/index.html; do-main.com/example/bar/index.html/

Semantik	URL-Muster	Abgestimmt	Unübertroffen
URL-Abgleich, Unterpfadabgleich	domain.com/example/bar/	domain.com/beispiel/bar/; do-main.com/beispiel/bar/index.html; www.domain.com/ example/bar/ index.html; do-main.com/beispiel/bar/index.html/one.jpg	www.domaincom/example/bar/index

URL-Kategorisierung

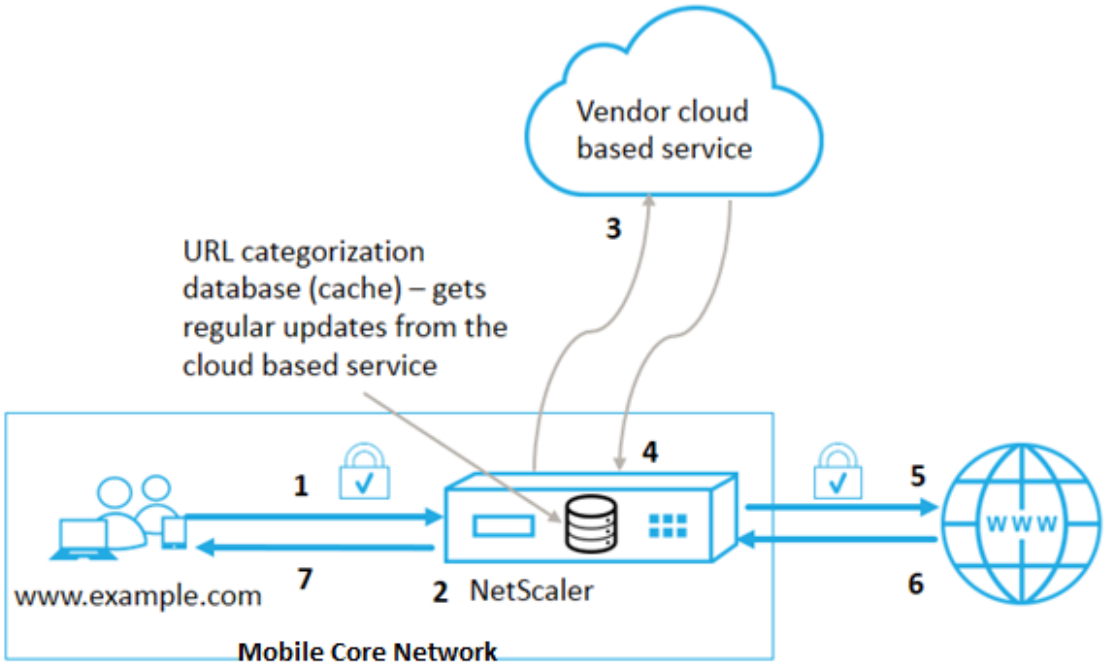
December 7, 2021

Die URL-Kategorisierung schränkt den Benutzerzugriff auf bestimmte Websites und Websitekategorien ein. Als abonnierter Dienst in Zusammenarbeit mit NetSTAR ermöglicht die Funktion Unternehmenskunden die Filterung von Webverkehr mithilfe einer kommerziellen Kategorisierungsdatenbank. Die Datenbank NetSTAR hat eine große Anzahl (Milliarden) von URLs, die in verschiedene Kategorien eingeteilt sind, wie soziale Netzwerke, Glücksspiele, Inhalte für Erwachsene, neue Medien und Shopping. Zusätzlich zur Kategorisierung verfügt jede URL über eine Reputationsbewertung, die auf dem historischen Risikoprofil der Website basiert. Wir können NetSTAR-Daten verwenden, um den Datenverkehr zu filtern, indem wir erweiterte Richtlinien basierend auf Kategorien, Kategoriegruppen (wie Terrorismus, illegale Drogen) oder Site-Reputation-Bewertungen konfigurieren.

Beispielsweise können Sie den Zugriff auf gefährliche Websites blockieren, z. B. Websites, die mit Malware infiziert sind, oder selektiv den Zugriff auf Inhalte für Erwachsene oder Entertainment-Streaming-Medien einschränken.

Funktionsweise der URL-Kategorisierung

Die folgende Abbildung zeigt, wie der Citrix ADC URL-Filterdienst in eine kommerzielle URL-Kategorisierungsdatenbank und Clouddienste für häufige Updates integriert ist.



Die Komponenten interagieren wie folgt:

1. Der Client sendet eine Internet-gebundene URL-Anfrage.
2. Eine Citrix ADC Richtlinie versucht, die Anforderung anhand von Kategorisierungsdetails (wie Kategorie, Kategoriegruppe und Standortreputationsbewertung) auszuwerten, die aus der URL-Kategorisierungsdatenbank abgerufen wurden. Wenn die Datenbank die Kategoriedetails zurückgibt, springt der Prozess zu Schritt 5.
3. Wenn die Datenbank keine Kategorisierungsdetails zurückgibt, wird die Anforderung an einen cloudbasierten Lookup-Dienst gesendet, der von einem URL-Kategorisierungsanbieter verwaltet wird. Die Appliance wartet jedoch nicht auf eine Antwort. Stattdessen markiert sie die URL als Uncategorized und springt zu Schritt 5. Es überwacht jedoch weiterhin das Feedback zur Cloud-Abfrage und verwendet es, um den Cache zu aktualisieren, damit zukünftige Anforderungen von der Cloud-Suche profitieren können.
4. Die Citrix ADC Appliance empfängt die URL-Kategoriedetails (Kategorie, Kategoriegruppe und Reputationsbewertung) vom cloudbasierten Dienst und speichert sie im Cloud-Cache.
5. Wenn die Richtlinie die URL zulässt, wird die Anforderung an den Ursprungsserver gesendet. Andernfalls löscht die Appliance die Anforderung oder leitet sie um oder antwortet mit einer benutzerdefinierten HTML-Seite.
6. Der Ursprungsserver antwortet mit den angeforderten Daten an die Citrix ADC Appliance.
7. Die Appliance sendet die Antwort an den Client.

Sie können die URL-Filterfunktion verwenden, um Websites zu erkennen, die gegen sichere Internetnutzungsmandate der Regierung verstoßen, und Richtlinien zum Blockieren dieser Websites imple-

mentieren. Websites, auf denen Inhalte für Erwachsene, Streaming-Medien oder soziale Netzwerke gehostet werden, die als unsicher für Kinder oder als illegal eingestuft wurden.

Voraussetzungen

Die Funktion funktioniert auf Telco-Plattformen mit dem Kauf einer grundlegenden CBM-Lizenz und einer CBM Premium-Lizenz und für andere Citrix ADC Plattformen funktioniert die Funktion mit dem Kauf einer CNS Premium-Lizenz.

Hinweis: Zusätzlich zu einer Basic CBM-Lizenz und einer CBM Premium-Lizenz muss die Appliance über eine URL Threat Intelligence-Lizenz mit einem Abonnementservice für 1 Jahr oder 3 Jahre verfügen. Bevor Sie das Feature aktivieren und konfigurieren, müssen Sie die folgenden Lizenzen installieren:

Lizenzunterstützung für Telco-Plattformen:

- **CBM_TXXX_SERVER_Retail.lic**
- **CBM_TPRE_SERVER_Retail.lic**
- **CNS_WEBF_SSERVER_Retail.lic**

Dabei ist XXX der Durchsatz, z. B. Citrix ADC T1000.

Lizenzunterstützung für andere Citrix ADC Plattformen:

- **CNS_XXX_SERVER_PLT_Retail.lic**

Dabei ist XXX der Durchsatz.

URL-Kategorisierungsrichtlinienausdrücke

In der folgenden Tabelle werden die verschiedenen URL-Kategorisierungsrichtlinienausdrücke zum Identifizieren eingehender URLs aufgeführt und eine konfigurierte Aktion angewendet.

Ausdruck	Vorgang
<text>. URL_CATEGORIZE (< min_reputation>, <max_reputation>)	Gibt ein URL_CATEGORY -Objekt zurück. Reputation Score ist eine Zahl von 1 bis 4. Um Objekte zu erhalten, verwenden Sie alle Reputationswerte 0,0 als <min reputation> und <max_reputation>. Wenn <min_reputation> ist größer als 0, das zurückgegebene Objekt enthält keine Kategorie mit einem niedrigeren Ruf als <min_reputation>. Wenn <max_reputation> ist größer als 0, das zurückgegebene Objekt enthält keine Kategorie mit einem höheren Ruf als <max_reputation>. Wenn die Kategorie nicht rechtzeitig aufgelöst wird, wird der undef-Wert zurückgegeben.
<url_category>. CATEGORY	Gibt die Kategoriezeichenfolge für dieses Objekt zurück. Wenn die URL keine Kategorie hat oder wenn die URL falsch formatiert ist, lautet der zurückgegebene Wert “Uncategorized”.
<url_category>. GROUP	Gibt einen String zurück, der die Kategoriegruppe des Objekts identifiziert. Dies ist eine Gruppierung von Kategorien auf höherer Ebene, die bei Operationen nützlich ist, die weniger detaillierte Informationen über die URL-Kategorie erfordern. Wenn die URL keine Kategorie hat oder wenn die URL falsch formatiert ist, lautet der zurückgegebene Wert “Uncategorized”.
<url_category>. REPUTATION	Gibt den Reputationswert als Zahl von 1 bis 4 zurück, wobei 4 den risikoreichsten Ruf angibt. Wenn die Kategorie “Uncategorized” lautet, lautet der Reputationswert 2.

Beispielrichtlinienausdrücke

Richtlinie	Richtlinienausdrücke
Richtlinie zum Auswählen von Anforderungen für URLs, die in der Suchmaschinenkategorie sind	add responder policy p1 ‘HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGO CATEGORY.EQ(“Search Engine”)
Richtlinie zum Auswählen von Anfragen für URLs, die sich in der Kategoriegruppe Erwachsene befinden	add responder policy p1 ‘HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGO GROUP.EQ (“Erwachsene”) ‘
Richtlinie zum Auswählen von Anforderungen für Suchmaschinen-URLs mit einer Reputationsbewertung von 4	Add Responderrichtlinie p2 ‘HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL) .URL_CATEGORIZE (4,0). CATEGORY.EQ (“Suchmaschine”) ‘
Richtlinie zum Auswählen von Anfragen für Suchmaschinen- und Shopping-URLs	Richtlinienpatset good_categories hinzufügen; Richtlinie good_categories “Search Engine” binden; Richtlinie good_categories “Shopping” binden; Responderrichtlinie p3 ‘HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL) .URL_CATEGORIZE (0,0) hinzufügen. CATEGORY .EQUALS_ANY(“good_categories”)
Richtlinie zum Auswählen von Anforderungen für Suchmaschinen-URLs mit einer Reputationsbewertung von 4	add responder policy p5 ‘CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE (4,0). CATEGORY.EQ(“Search Engine”)

URL-Kategorisierungsrichtlinienaktionen

Eine URL-Filterrichtlinie wertet den Datenverkehr aus, um Anforderungen zu identifizieren, die zu einer bestimmten Kategorie gehören. In der folgenden Tabelle sind die Aktionen aufgeführt, die Sie einer URL-Filterrichtlinie zuweisen können.

Richtlinienaktion	Richtliniengruppe	Beschreibung
ALLOW	Responder	Zugriff der eingehenden Anforderung auf die Ziel-URL zulassen
REDIRECT	Responder	Leiten Sie die eingehende Anforderung an die als Ziel angegebene URL um.

Richtlinienaktion	Richtliniengruppe	Beschreibung
DENY	Responder	Eingehende Anfrage ablehnen.
RESET	Responder, VideoOptimization	Verbindung zurücksetzen.
DROP	Responder, VideoOptimization	Verbindung fallen lassen.

> **Hinweis:**
>
> Für verschlüsselten Datenverkehr enthält die Richtlinie VideoOptimization Aktionen, die die URL-Filteraktionen implementieren.

URL-Kategorisierung konfigurieren

Um die URL-Kategorisierung zu konfigurieren, aktivieren Sie zunächst die URL-Filterfunktion. Anschließend müssen Sie die Cache-Speicherlimits, die Kategorisierungsrichtlinie und die virtuellen Server für HTTP- und HTTPS-Datenverkehr konfigurieren. Konfigurieren der URL-Kategorisierung mit der CLI.

Gehen Sie folgendermaßen vor, um die CLI-Konfigurations-URL-Kategorisierung auf einer Citrix ADC Appliance zu verwenden:

- Richten Sie die URL-Kategorisierung ein.
  - Aktivieren Sie die URL-Filterfunktion.
  - Konfigurieren Sie Shared Memory, um den Cache-Speicher zu begrenzen.
  - Konfigurieren Sie URL-Kategorisierungsparameter.
- Konfigurieren Sie die URL-Kategorisierung für HTTP-Datenverkehr.
  - URL-Kategorisierungsaktionen hinzufügen.
  - URL-Kategorisierungsrichtlinien hinzufügen.
  - Fügen Sie einen virtuellen Lastausgleichsserver für HTTP-Datenverkehr hinzu.
  - Binden Sie URL-Kategorisierungsrichtlinien an den virtuellen Lastausgleichsserver.
- Konfigurieren Sie die URL-Kategorisierung für HTTPS-Datenverkehr.
  - URL-Kategorisierungsrichtlinien hinzufügen.
  - Fügen Sie einen virtuellen SSL-Bridge-Load Balancing Server hinzu.
  - Binden Sie URL-Kategorisierungsrichtlinien an den virtuellen Lastausgleichsserver.

URL-Kategorisierung einrichten

Um das Feature einzurichten, müssen Sie die URL-Kategorisierungsfunktion aktivieren, die Filterparameter konfigurieren und das Limit für den gemeinsamen Speicher festlegen.

So aktivieren Sie die URL-Filterfunktion

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns feature URLFiltering VideoOptimization Responder IC SSL AppFlow
```

So konfigurieren Sie die Begrenzung des freigegebenen Speichers

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set cache parameter [-memLimit <megaBytes>]
2 <!--NeedCopy-->
```

Wobei memLimit das Speicherlimit für das Zwischenspeichern ist.

Beispiel:

```
set cache parameter -memLimit 10
```

So konfigurieren Sie URL-Kategorisierungsparameter

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>]
     [-TimeOfDayToUpdateDB <HH:MM>]
2 <!--NeedCopy-->
```

***Beispiel:**

```
set urlfiltering parameter -HoursBetweenDBUpdates 3 -TimeOfDayToUpdateDB
03:00
```

Konfigurieren der URL-Kategorisierung für HTTP-Datenverkehr

Um die URL-Kategorisierungsfunktion für HTTP-Datenverkehr zu konfigurieren, müssen Sie einen virtuellen Server für Lastenausgleich konfigurieren, URL-Kategorisierungsrichtlinien hinzufügen und die Richtlinien an den virtuellen Server binden. Auf diese Weise erhält der virtuelle Server den

HTTP-Datenverkehr und basierend auf der Richtlinienauswertung weist das System eine Filteraktion zu.

So fügen Sie URL-Kategorisierungsaktion für HTTP-Datenverkehr hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add responder action <name> <type> (<target> | <htmlpage>)[-comment <string
>] [-responseStatusCode <positive_integer>] [-reasonPhrase <string>]
```

Beispiel:

```
add responder action act_url_categorize respondwith "\"HTTP/1.1 200 OK\r\n\
r\n\" + HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY
 + \"\n\""
```

So fügen Sie URL-Kategorisierungsrichtlinie für HTTP-Datenverkehr hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add responder policy <name> <rule> <action> [<undefAction>] [-comment <
string>] [-logAction <string>] [-appflowAction <string>]
```

Beispiel:

```
add responder policy pol_url_categorize_http "HTTP.REQ.HOSTNAME.APPEND(
HTTP.REQ.URL).URL_CATEGORIZE(0,0).GROUP.EQ(\"Adult\")|| HTTP.REQ.HOSTNAME.
APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).GROUP.EQ(\"Gambling\")"RESET
```

So fügen Sie einen virtuellen HTTP-Lastausgleichsserver hinzu

Wenn ein virtueller Server für HTTP-Datenverkehr noch nicht konfiguriert ist, geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> [-td <positive_integer>] <serviceType> [-clt Timeout
<secs>]
```

Beispiel:

```
add lb vserver vsrv-HTTP HTTP * 80 -persistenceType NONE -cltTimeout 120
```

So binden Sie URL-Kategorisierungsrichtlinie mit dem virtuellen Lastenausgleichsserver

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name> -policyName <string> [-priority <positive_integer>]
```


Beispiel:

```
bind lb vserver vsrv-HTTP -policyName pol_url_categorize_http -priority 10
-gotoPriorityExpression END -type REQUEST
```

Konfigurieren der URL-Kategorisierung für HTTPS-Datenverkehr

Um die URL-Kategorisierungsfunktion für HTTPS-Datenverkehr zu konfigurieren, müssen Sie einen virtuellen SSL-Bridge-Server konfigurieren, URL-Kategorisierungsrichtlinien hinzufügen und die Richtlinien an den virtuellen SSL-Bridge-Server binden. Auf diese Weise erhält der Server den HTTPS-Datenverkehr und basierend auf der Richtlinienbewertung weist das System eine Filteraktion zu.

So fügen Sie URL-Kategorisierungsrichtlinie für HTTPS-Datenverkehr hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add videooptimization detectionpolicy <name> -rule <expression> -action <
string> [-undefAction <string>] [-comment <string>] [-logAction <string>]
```

Beispiel:

```
add videooptimization detectionpolicy pol_url_categorize_https_block_adult -
rule "CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE(0,0).CATEGORY.EQ("Adult")' -
action RESET
```

So fügen Sie einen virtuellen SSL-Bridge-Lastausgleichsserver hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> [-td <positive_integer>] <serviceType> [-cltT imeout
<secs>]
```

Beispiel:

```
add lb vserver vsrv-HTTPS SSL_BRIDGE * 443 -persistenceType NONE -cltTimeout
 180
```

So binden Sie Kategorisierungsrichtlinien an den virtuellen SSL-Bridge-Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name> -policyName <string> [-priority <positive_integer>]
```

Beispiel:


```
bind lb vserver vsrv-HTTPS -policyName pol_url_categorize_https_block_adult
 -priority 20 -type REQUEST
```

Konfigurieren der URL-Kategorisierung mit der GUI

Mit der GUI können Sie:

- Aktivieren Sie die URL-Kategorisierungsfunktion.
- URL-Kategorisierungsaktionen für HTTP-Datenverkehr hinzufügen.
- URL-Kategorisierungsrichtlinien für HTTP-Datenverkehr hinzufügen.
- URL-Kategorisierungsrichtlinien für HTTPS-Datenverkehr hinzufügen.
- Fügen Sie einen virtuellen Lastausgleichsserver für HTTP-Datenverkehr hinzu.
- Fügen Sie einen virtuellen SSL-Bridge-Load Balancing Server für HTTPS-Datenverkehr hinzu.
- Binden Sie URL-Kategorisierungsrichtlinien an den virtuellen Lastausgleichsserver.
- Binden Sie URL-Kategorisierungsrichtlinien an den virtuellen SSL-Bridge-Load Balancing Server.
- Konfigurieren Sie das Limit des gemeinsamen Speichers.
- Konfigurieren Sie URL-Kategorisierungsparameter.

So aktivieren Sie die URL-Kategorisierung

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen** .
2. Klicken Sie auf der Seite **Einstellungen** auf **Erweiterte Funktionen konfigurieren** .
3. Aktivieren Sie auf der Seite **Erweiterte Funktionen konfigurieren** das Kontrollkästchen **URL-Filterung** .
4. Klicken Sie auf **OK** und **schließen**.

So fügen Sie eine URL-Kategorisierungsaktion hinzu

1. Erweitern Sie im Navigationsbereich **AppExpert** > **Responder** > **Aktion** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **Responder-Aktion erstellen** die folgenden Parameter fest.
   a) **Name**. Name der URL-Kategorisierungsrichtlinienaktion.
   b) **Geben Sie ein**. Wählen Sie einen Aktionstyp aus.
   c) **Ausdruck**. Verwenden Sie den Ausdrucksеditor, um den Richtlinienausdruck zu erstellen.
   d) **Kommentare**. Eine kurze Beschreibung der politischen Aktion.
4. Klicken Sie auf **Erstellen** und **Schließen**.

So fügen Sie eine URL-Kategorisierungsrichtlinie für HTTP-Datenverkehr hinzu

1. Erweitern Sie im Navigationsbereich **AppExpert** > **Responder** > **Richtlinien** .

2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **Responder-Richtlinie erstellen** die folgenden Parameter fest.
   a) **Name**. Name der URL-Kategorisierungsrichtlinienaktion.
   b) **Aktion:** Wählen Sie die URL-Kategorisierungsaktion aus, die Sie der Richtlinie zuordnen möchten.
   c) **Aktion protokollieren**. Wählen Sie die Protokollaktion aus.
   d) **AppFlow**. Wählen Sie eine AppFlow Aktion aus.
   e) **Ausdruck**. Verwenden Sie den Ausdrucksеditor, um den Richtlinienausdruck zu erstellen.
   f) **Kommentare**. Eine kurze Beschreibung der Richtlinienaktion.
4. Klicken Sie auf **Erstellen** und **Schließen**.

So fügen Sie eine Kategorisierungsrichtlinie für HTTPS-Datenverkehr hinzu

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zu **Konfiguration** > **Optimierung** > **Videooptimierung** > **Erkennung** .
2. Klicken Sie auf der Seite **Erkennung** auf den Link **Richtlinien für die Erkennung von Videooptimierungen** .
3. Klicken Sie auf der Seite Richtlinien zur Videooptimierung auf **Hinzufügen**.
4. Legen Sie auf der Seite **Richtlinie zur Videooptimierung erstellen** die folgenden Parameter fest.
   a) **Name**. Name der Optimierungsrichtlinie
   b) **Ausdruck**. Konfigurieren Sie die Richtlinie mithilfe benutzerdefinierter Ausdrücke.
   c) **Aktion:** Optimierungsaktion, die mit der Richtlinie für die Verarbeitung des eingehenden Videoverkehrs verknüpft ist.
   d) **UNDEF Aktion**. Undefiniertes Ereignis, wenn die eingehende Anforderung nicht mit der Optimierungsrichtlinie übereinstimmt.
   e) **Kommentar**. Eine kurze Beschreibung der Richtlinie.
   f) **Aktion protokollieren.** Wählen Sie eine Überwachungsprotokollaktion aus, die die Aktion angibt, die für die Protokollmeldungen ausgeführt werden soll.
5. Klicken Sie auf **Erstellen** und **Schließen**.

So fügen Sie einen virtuellen Lastausgleichsserver für HTTP-Datenverkehr hinzu

1. Navigieren Sie zur Seite **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **Load Balancing Virtual Server** die folgenden Parameter fest:
   a) **Name**. Name des virtuellen Lastenausgleichsservers.
   b) **Protokoll**. Wählen Sie den Protokolltyp als HTTP.
   c) **IP-Adresstyp.** IPv4 oder IPv6.
   d) **IP-Adresse.** IPv4 oder IPv6, dem virtuellen Server zugewiesene VIP-Adresse.

e) **Port**. Portnummer des virtuellen Servers.

4. Klicken Sie auf **OK**, um mit der Konfiguration anderer optionaler Parameter fortzufahren.
5. Klicken Sie auf **Erstellen** und **Schließen**.

So fügen Sie einen virtuellen SSL-Bridge-Lastausgleichsserver hinzu

1. Navigieren Sie zur Seite **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **Virtueller Server für den Lastausgleich** die folgenden Parameter fest:
   a) **Name**. Name des virtuellen Lastenausgleichsservers.
   b) **Protokoll**. Wählen Sie den Protokolltyp als SSL-Bridge aus.
   c) **Typ der IP-Adresse**. IP-adressierbarer Typ.
   d) **IP Adresse**. IP 4 oder IP6 IP-Adresse, die dem virtuellen Server zugewiesen ist.
   e) **Port**. Portnummer des virtuellen Servers.
4. Wählen Sie **OK**, um die Konfiguration anderer optionaler Parameter fortzusetzen.
5. Klicken Sie auf **Erstellen** und dann auf **Schließen**.

So binden Sie eine URL-Kategorisierungsrichtlinie an den virtuellen HTTP-Lastausgleichsserver

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Lastausgleichsserver aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.
4. Klicken Sie im Abschnitt **Richtlinien** auf das Symbol **+**, um auf den Schieberegler **Richtlinien** zuzugreifen.
5. Legen Sie die folgenden Parameter fest.
   a) **Wählen Sie Richtlinie aus**. Wählen Sie URL-Kategorisierungsrichtlinie aus der Dropdownliste aus.
   b) **Wählen Sie Typ aus**. Wählen Sie den Richtlinientyp als Anforderung aus.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie die URL-Kategorisierungsrichtlinie aus der Liste aus, und klicken Sie auf **Schließen**.

So binden Sie eine Kategorisierungsrichtlinie an den virtuellen SSL-Bridge Lastausgleichsserver

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen SSL-Bridge-Load Balancing Server aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.

4. Klicken Sie im Abschnitt **Richtlinien** auf das Symbol **+**, um auf den Schieberegler **Richtlinien** zuzugreifen.
5. Legen Sie im Abschnitt **Richtlinien** die folgenden Parameter fest.
   a) **Wählen Sie Richtlinie aus**. Wählen Sie in der Dropdownliste die Richtlinie zur Videoerkennung aus.
   b) **Wählen Sie Typ aus**. Wählen Sie den Richtlinientyp als Anforderung aus.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie die Richtlinie zur Videoerkennung aus der Liste aus, und klicken Sie auf **Schließen**.

So konfigurieren Sie das Limit für den gemeinsamen Speicher

1. Melden Sie sich bei der Appliance an und navigieren Sie zu **Optimierung** > **Integriertes Caching**.
2. Klicken Sie im Detailbereich auf Link **Cache-Einstellungen ändern** .
3. Legen Sie auf der Seite **Globale Cache-Einstellungen** die folgenden Parameter fest.
   a) **Speicherauslastung (MB).**
   b) **Aktives Speicherauslastungslimit**.
   c) **Über Header**.
   d) **Maximale Länge des Post-Body, die zwischengespeichert werden soll**
   e) **Globale Aktion mit nicht definiertem Ergebnis**
   f) **HA-Objekt Persistenz aktivieren**
   g) **Überprüfen der Persistenz des gecachten Objekts**
   h) **Prefetches**
4. Klicken Sie auf **OK** und **schließen**.

So konfigurieren Sie URL-Kategorisierungsparameter

1. Melden Sie sich bei der Appliance an und navigieren Sie zu **Sicherheit**.
2. Klicken Sie im Detailbereich auf **URL-Filtereinstellungen ändern** .
3. Legen **Sie auf der Seite URL-Filterparameter konfigurieren** die folgenden Parameter fest.
   a) Stunden zwischen DB-Updates. URL-Filterung Stunden zwischen Datenbankaktualisierungen. Mindestwert: 0 und Maximalwert: 720.
   b) Tageszeit für die Aktualisierung der DB. URL-Filterzeit, um die Datenbank zu aktualisieren.
4. Klicken Sie auf **OK** und **Schließen.**

Konfigurieren von Überwachungsprotokoll-Messaging

Wenn eine Citrix ADC Appliance eine eingehende URL empfängt und die Responderrichtlinie einen URL-Filterausdruck aufweist, sammelt das Überwachungsprotokoll-Feature Kategorisierungsinfor-

mationen und zeigt sie als Protokollmeldungen an jedem konfigurierten Ziel-Überwachungsprotokollserver an. Die Info wird protokolliert.

- Quell-IP-Adresse (die IP-Adresse des Clients, der die Anforderung gestellt hat).
- Ziel-IP-Adresse (die IP-Adresse des angeforderten Servers).
- Angeforderte URL, die das Schema, den Host und den Domänennamen (`http://www.example.com`) enthält.
- URL-Kategorie, die das URL-Filterframework zurückgibt.
- URL-Kategoriegruppe, die vom URL-Filterframework zurückgegeben wurde.
- URL-Reputationsnummer, die vom URL-Filterframework zurückgegeben wurde.
- Überwachungsprotokollaktion, die von der URL-Kategorisierungsrichtlinie durchgeführt wird.

Um die Überwachungsprotokollierung für die URL-Liste zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

1. Überwachungsprotokoll aktivieren.
2. Aktion “Auditprotokoll erstellen”
3. Legen Sie die Richtlinie für URL-Listen-Responder mit Auditprotokoll-Nachrichtenaktion fest.

Weitere Informationen finden Sie unter Thema Überwachungsprotokollierung .

Speichern von Fehlern mit SYSLOG Messaging

Bei einem Ausfall auf Systemebene verwendet die Citrix ADC-Appliance in jeder Phase des URL-Filter-Prozesses den Auditprotokollmechanismus, um Protokolle in der Datei ns.log zu speichern. Die Fehler werden als Textnachrichten im SYSLOG-Format gespeichert, sodass ein Administrator sie später in chronologischer Reihenfolge des Ereignisses anzeigen kann. Diese Protokolle werden auch zur Archivierung an einen externen SYSLOG-Server gesendet. Weitere Informationen finden Sie im Artikel CTX229399.

Wenn beispielsweise ein Fehler auftritt, wenn Sie das URL-Filter-SDK initialisieren, wird die Fehlermeldung im folgenden Nachrichtenformat gespeichert.

3. Oktober 15:43:40 <`local0.err`> ns URLFilterung[1349]: Fehler beim Initialisieren des NetStar SDK (SDK-Fehler = -1). (Status = 1).

Die Citrix ADC-Appliance speichert die Fehlermeldungen in vier verschiedenen Fehlerkategorien:

- Download-Versagen. Wenn ein Fehler auftritt, wenn Sie versuchen, die Kategorisierungsdatenbank herunterzuladen.
- Integrationsfehler. Wenn ein Fehler auftritt, wenn Sie ein Update in die vorhandene Kategorisierungsdatenbank integrieren.
- Fehler bei der Initialisierung Wenn ein Fehler auftritt, wenn Sie die URL-Kategorisierungsfunktion initialisieren, Kategorisierungsparameter festlegen oder einen Kategorisierungsdienst beenden.

- Fehler beim Abrufen. Wenn ein Fehler auftritt, wenn die Appliance die Kategorisierungsdetails der Anforderung abruft.

URL-Reputationsbewertung

Die URL-Kategorisierungsfunktion bietet richtlinienbasierte Steuerung, um URLs in der Sperrliste einzuschränken. Sie können den Zugriff auf Websites basierend auf URL-Kategorie, Reputationsbewertung oder URL-Kategorie und Reputationsbewertung steuern. Wenn ein Netzwerkadministrator einen Benutzer überwacht, der auf hochriskante Websites zugreift, kann er eine Responderrichtlinie verwenden, die an die URL-Reputationsbewertung gebunden ist, um solche riskanten Websites zu blockieren.

Nach Erhalt einer eingehenden URL-Anforderung ruft die Appliance die Kategorie- und Reputationsbewertung aus der URL-Kategorisierungsdatenbank ab. Basierend auf der von der Datenbank zurückgegebenen Reputationsbewertung weist die Appliance Websites eine Reputationsbewertung zu. Der Wert kann zwischen 1 und 4 liegen, wobei 4 der risikoreichste Typ von Websites ist, wie in der folgenden Tabelle dargestellt.

URL-Reputationsbewertung	Reputationskommentar
1	Saubere Site.
2	Unbekannter Standort.
3	Potenziell gefährlich oder mit gefährlicher Site verbunden.
4	Bösartige Site.

FAQ

October 5, 2021

In diesem Abschnitt finden Sie die FAQ zu den folgenden Citrix ADC-Funktionen

- Admin-Partition
- AppFlow
- Call Home
- Clustering
- Verbindungsverwaltung
- Content Switching

Admin-Partition

October 5, 2021

Wo erhalte ich die Citrix ADC Konfigurationsdatei für eine Partition?

Die Konfigurationsdatei (*ns.conf*) für die Standardpartition ist im Verzeichnis */nsconfig*verfügbar. Für Admin-Partitionen ist die Datei im **<partitionName> Verzeichnis /nsconfig/partitions/ verfügbar.

Wie kann ich das integrierte Caching in einer partitionierten Citrix ADC Appliance konfigurieren?

> **Hinweis:**
>
> Integriertes Caching in Admin-Partitionen wird ab NetScaler 11.0 unterstützt.

Um das integrierte Caching (IC) auf einem partitionierten Citrix ADC zu konfigurieren, kann der Superuser nach der Definition des IC-Speichers auf der Standardpartition den IC-Speicher auf jeder Admin-Partition so konfigurieren, dass der gesamte IC-Speicher, der allen Admin-Partitionen zugewiesen ist, den auf der Standardpartition definierten IC-Speicher nicht überschreitet. Der Speicher, der nicht für die Admin-Partitionen konfiguriert ist, bleibt für die Standardpartition verfügbar.

Wenn beispielsweise einer Citrix ADC-Appliance mit zwei Admin-Partitionen 10 GB IC-Speicher der Standardpartition zugewiesen sind und die IC-Speicherzuweisung für die beiden Admin-Partitionen wie folgt lautet:

- Partition1: 4 GB
- Partition2: 3 GB

Dann hat die Standardpartition 10 - (4 + 3) = 3 GB verfügbaren IC-Speicher.

> **Hinweis:**
>
> Wenn der gesamte IC-Speicher von den Admin-Partitionen verwendet wird, ist für die Standardpartition kein IC-Speicher verfügbar.

Was ist der Umfang für L2- und L3-Parameter in Admin-Partitionen?

> **Hinweis:**
>
> - Gilt ab NetScaler 11.0.
> - Damit ARP in einer nicht standardmäßigen Partition funktioniert, müssen Sie den Parameter “proxyARP” im Befehl “set l2param” aktivieren.

Auf einer partitionierten Citrix ADC Appliance können die Parameter L2 und L3 wie folgt aktualisiert werden:

- Für L2-Parameter, die mit dem Befehl set L2Param festgelegt werden, können die folgenden Parameter nur von der Standardpartition aktualisiert werden, und ihre Werte gelten für alle Admin-Partitionen:

  maxBridgeCollision, bdgSetting, garpOnVridIntf, garpReply, proxyArp, resetInterfaceOnHAfailover, and skip_proxying_bsd_traffic.

  Die anderen L2-Parameter können in bestimmten Adminpartitionen aktualisiert werden, und ihre Werte sind lokal für diese Partitionen.

- Für L3-Parameter, die mit dem Befehl set L3Param festgelegt werden, können alle Parameter in bestimmten Adminpartitionen aktualisiert werden, und ihre Werte sind lokal für diese Partitionen. Ebenso gelten die Werte, die in der Standardpartition aktualisiert werden, nur für die Standardpartition.

Wie aktiviere ich dynamisches Routing in einer Admin-Partition?

> **Hinweis:**
>
> Dynamisches Routing in Admin-Partitionen wird ab NetScaler 11.0 unterstützt.

Während dynamisches Routing (OSPF, RIP, BGP, ISIS, BGP+) standardmäßig auf der Standardpartition aktiviert ist, muss es in einer Administratorpartition mithilfe des folgenden Befehls aktiviert werden:

```
> set L3Param -dynamicRouting ENABLED
```

> **Hinweis:**
>
> Maximal 63 Partitionen können dynamisches Routing ausführen (62 Admin-Partitionen und eine Standardpartition).

Beim Aktivieren des dynamischen Routing auf einer Admin-Partition wird ein virtueller Router (VR) erstellt.

- Jede VR verfügt über eine eigene vlan0, die als vlan0_ angezeigt wird <partition-name>.
- Alle ungebundenen IP-Adressen, die ZebOS verfügbar gemacht werden, sind an vlan0 gebunden.
- Die Standard-VR (der Standardpartition) zeigt alle konfigurierten VRs an.
- Die Standard-VR zeigt die VLANs an, die an diese VRs gebunden sind (außer Standard-VLANs).

Wo finde ich die Protokolle für eine Partition?

Citrix ADC Protokolle sind nicht partitionsspezifisch. Protokolleinträge für alle Partitionen müssen im Verzeichnis */var/log/* gespeichert werden.

Wie kann ich Audit-Logs für eine Admin-Partition erhalten?

In einem partitionierten Citrix ADC können keine spezifischen Protokollserver für eine bestimmte Partition vorhanden sein. Die Server, die auf der Standardpartition definiert sind, sind für alle Administratorpartitionen anwendbar. Um die Überwachungsprotokolle für eine bestimmte Partition anzuzeigen, müssen Sie daher den Befehl “Audit-Nachrichten anzeigen” verwenden.

> **Hinweis:**
>
> Die Benutzer einer Admin-Partition haben keinen Zugriff auf die Shell und können daher nicht auf die Protokolldateien zugreifen.

Wie erhalte ich Weblogs für eine Admin-Partition?

Sie können die Webprotokolle für eine Admin-Partition wie folgt abrufen:

- **Für NetScaler 11.0 und höhere Versionen**

  Die Webprotokollierungsfunktion muss auf jeder Partition aktiviert sein, für die eine Webprotokollierung erforderlich ist. Mit dem Citrix ADC Web Logging (NSWL) -Client ruft Citrix ADC die Webprotokolle für alle Partitionen ab, denen der Benutzer zugeordnet ist.

- **Für Versionen vor NetScaler 11.0**

  Weblogs können nur von `nsroot` und anderen Superbenutzern bezogen werden. Auch wenn die Webprotokollierung auf der Standardpartition aktiviert ist, ruft der Citrix ADC Web Logging (NSWL) Client Webprotokolle für alle Partitionen ab.

Um die Partition für jeden Protokolleintrag anzuzeigen, passen Sie das Protokollformat so an, dass die Option%P enthalten ist. Anschließend können Sie die Protokolle filtern, um die Protokolle für eine bestimmte Partition anzuzeigen.

Wie bekomme ich den Trace für eine Admin-Partition?

Sie können die Ablaufverfolgung für eine Admin-Partition wie folgt abrufen:

- **Für NetScaler 11.0 und höhere Versionen**

  In einer partitionierten Citrix ADC Appliance kann der `nstrace` Vorgang auf einzelnen Admin-Partitionen durchgeführt werden. Die Trace-Dateien werden im Verzeichnis /var/partitions/<partitionName>/nstrace/ gespeichert.

  Hinweis: Sie können die Ablaufverfolgung einer Admin-Partition nicht über die GUI abrufen. Sie müssen die CLI verwenden.

- **Für Versionen vor NetScaler 11.0**

  Der `nstrace` Vorgang kann nur auf der Standardpartition durchgeführt werden. Daher sind Paketerfassungen für das gesamte Citrix ADC -System verfügbar. Um partitionsspezifische Paketaufnahmen zu erhalten, verwenden Sie VLAN-ID-basierte Filter.

Wie erhalte ich das technische Support-Paket, das für eine Admin-Partition spezifisch ist?

Um das technische Supportpaket für eine bestimmte Partition zu erhalten, müssen Sie den folgenden Befehl von der Standardpartition ausführen:

```
> show techsupport -scope partition -partitionname <string>
```

Hinweis: Dieser Befehl enthält auch systemspezifische Informationen.

AppFlow

October 5, 2021

- **Welcher Build von Citrix ADC unterstützt AppFlow?**

  AppFlow wird auf Citrix ADC Appliances mit Version 9.3 und höher mit nCore Build unterstützt.

- **Welches Format wird von AppFlow verwendet, um Daten zu übertragen?**

  AppFlow überträgt Informationen im IPFIX-Format (Internet Protocol Flow Information Export), bei dem es sich um einen offenen IETF-Standard (Internet Engineering Task Force) handelt, der in RFC 5101 definiert ist. IPFIX (die standardisierte Version von NetFlow von Cisco) wird häufig zur Überwachung von Netzwerkflussinformationen verwendet.

- **Was enthalten AppFlow Datensätze?**

AppFlow Datensätze enthalten standardmäßige NetFlow- oder IPFIX-Informationen, z. B. Zeitstempel für Anfang und Ende eines Flows, Paketanzahl und Byteanzahl. AppFlow Datensätze enthalten auch Informationen auf Anwendungsebene (z. B. HTTP-URLs, HTTP-Anforderungsmethoden und Antwortstatuscodes, Server-Antwortzeit und Latenz). IPFIX-Flow-Datensätze basieren auf Vorlagen, die vor dem Senden von Flow-Datensätzen gesendet werden müssen.

- **Warum führt ein Versuch, einen virtuellen Server von der GUI aus zu öffnen, nach einem Upgrade auf NetScaler Version 9.3 Build 48.6 Cl die Fehlermeldung Die AppFlow Funktion ist nur auf Citrix ADC Ncore verfügbar?**

  AppFlow wird nur auf nCore Appliances unterstützt. Deaktivieren Sie beim Öffnen der Registerkarte “Konfiguration des virtuellen Servers” das Kontrollkästchen **AppFlow** .

- **Was enthält die Transaktions-ID in AppFlow Datensätzen?**

  Eine Transaktions-ID ist eine 32-Bit-Nummer ohne Vorzeichen, die eine Transaktion auf Anwendungsebene identifiziert. Bei HTTP entspricht eine Transaktion einem Anforderungs- und Antwortpaar. Alle Flow-Datensätze, die diesem Anforderungs- und Antwortpaar entsprechen, haben dieselbe Transaktions-ID. Eine typische Transaktion hat vier Flow-Datensätze. Wenn der Citrix ADC die Antwort selbst generiert (bereitgestellt aus dem integrierten Cache oder durch eine Sicherheitsrichtlinie), gibt es möglicherweise nur zwei Flow-Datensätze für die Transaktion.

- **Was ist eine AppFlow Aktion?**

  Eine AppFlow-Aktion ist eine Reihe von Collectors, an die die Flow-Datensätze gesendet werden, wenn die zugehörige AppFlow-Richtlinie übereinstimmt.

- **Welche Befehle kann ich auf der Citrix ADC Appliance ausführen, um zu überprüfen, ob die AppFlow Aktion ein Treffer ist?**

  Die Aktion “AppFlow anzeigen”. Beispiel:

```
> show appflow action
1) Name: aFL-act-collector-1
   Collectors: collector-1
   Hits: 0
   Action Reference Count: 2
  2) Name: apfl-act-collector-2-and-3
   Collectors: collector-2, collecter-3
   Hits: 0
   Action Reference Count: 1
  3) Name: apfl-act-collector-1-and-3
   Collectors: collector-1, collecter-3
```



```
    Hits: 0
    Action Reference Count: 1
<!--NeedCopy-->
```

- **Was ist ein AppFlow -Kollektor?**

Ein Kollektor empfängt Flow-Datensätze, die von der Citrix ADC Appliance generiert werden. Um Flow-Datensätze senden zu können, müssen Sie mindestens einen Collector angeben. Sie können bis zu vier angeben. Sie können nicht verwendete Kollektoren entfernen.

- **Welche Citrix ADC Version ist für die Verwendung von AppFlow erforderlich?**

  Verwenden Sie NetScaler Version 9.3.49.5 oder höher, und denken Sie daran, dass AppFlow nur in den nCore Builds verfügbar ist.

- **Welches Transportprotokoll verwendet AppFlow?**

  AppFlow verwendet UDP als Transportprotokoll.

- **Welche Ports müssen geöffnet werden, wenn ich eine Firewall im Netzwerk habe?**

  Port 4739. Es ist der Standard-UDP-Port, den der AppFlow -Kollektor zum Abhören von IPFIX-Nachrichten verwendet. Wenn der Benutzer den Standardport ändert, muss dieser Port an der Firewall geöffnet werden.

- **Wie kann ich den Standardport ändern, den AppFlow verwendet?**

  Wenn Sie einen AppFlow Collector mithilfe des Befehls add AppFlowCollector hinzufügen, können Sie den zu verwendenden Port angeben.

```
> add appflowCollector coll1 -IPAddress 10.102.29.251 -port 8000
 Done
<!--NeedCopy-->
```

- **Was macht die Einstellung ClientTrafficOnly?**

  Citrix ADC generiert AppFlow Datensätze nur für clientseitigen Datenverkehr.

- **Wie viele Kollektoren können gleichzeitig konfiguriert werden?**

  Sie können auf der Citrix ADC Appliance bis zu vier AppFlow-Kollektoren gleichzeitig konfigurieren. Beachten Sie, dass die maximale Anzahl von Collectors, die auf einer Citrix ADC Appliance konfiguriert werden können, vier beträgt.

Call Home

October 5, 2021

- **Was ist Call Home auf einer Citrix ADC Appliance?**

  Call Home überwacht und benachrichtigt kritische Ereignisse auf einer Citrix ADC Appliance. Durch Aktivieren von Call Home können Sie die Fehlerbenachrichtigung automatisieren. Sie vermeiden nicht nur den Citrix Support aufrufen, eine Serviceanfrage auslösen und Systemdaten hochladen, bevor Citrix Support das Problem beheben kann, sondern identifizieren und beheben Sie auch Probleme, bevor es auftritt.

- **Ist Call Home auf einer Citrix ADC Appliance standardmäßig aktiviert?**

  Ja, Call Home ist auf der Appliance standardmäßig aktiviert. Wenn Sie von einer älteren Version, in der Call Home standardmäßig deaktiviert wurde, auf die neueste Software aktualisieren, wird die Funktion beim Upgrade automatisch aktiviert. Wenn Sie es später deaktivieren, wird die aktualisierte Einstellung für alle weiteren Upgrades gespeichert. Weitere Informationen finden Sie unter Call Home.

- **Was sind die Voraussetzungen für die Arbeit von Call Home?**

  Zugang zu einer Internetverbindung.

  Hinweis: Wenn Ihre Citrix ADC Appliance über keine Internetverbindung verfügt, können Sie einen Proxy-Server konfigurieren, über den Citrix ADC Systemprotokolle generieren und auf den Citrix Technical Support Server (CIS) hochladen kann.

- **Was sind die Vorteile der Verwendung von Call Home?**

  - Überwachen Sie Hardware- und Software-Fehlerbedingungen.
  - Benachrichtigen Sie das Auftreten kritischer Ereignisse, die sich auf Ihr Netzwerk auswirken.
  - Senden Sie Leistungsdaten und Systemprotokolle an Citrix an:
    * Analysieren und verbessern Sie die Produktqualität.
    * Bereitstellung von Informationen zur Fehlerbehebung in Echtzeit für proaktive Problemerkennung und schnellere Problemlösung.

- **Welche Version der Citrix ADC Software unterstützt Call Home?**

  Citrix ADC Version 10.0 und höher.

- **Welche Citrix ADC Plattformmodelle unterstützen Call Home?**

  Die Call Home Funktion ist standardmäßig auf allen Citrix ADC Plattformen und allen Appliance-Modellen (MPX, VPX und SDX) aktiviert.

  - Citrix ADC MPX: Alle MPX-Modelle.

  - Citrix ADC VPX: Alle VPX-Modelle. Darüber hinaus wird es auf VPX-Appliances unterstützt, die ihre Lizenzen von externen oder zentralen Lizenzierungspools beziehen. Die Funktion bleibt jedoch die gleiche wie bei einer Standard-VPX-Appliance.
  - Citrix ADC SDX: Überwacht das Laufwerk und die zugewiesenen SSL-Chips auf Fehler oder Fehler. Die VPX-Instanzen haben jedoch keinen Zugriff auf das Netzteil (Power Supply Unit) und daher wird ihr Status nicht überwacht. In einer SDX-Plattform können Sie Call Home entweder direkt auf einer einzelnen Instanz oder über die SVM konfigurieren.

- **Soll ich SNMP-Alarm konfigurieren, damit Call Home Fehlerbedingungen benachrichtigt werden?**

  Nein, Sie müssen SNMP nicht für Call Home konfigurieren, um Fehlerbedingungen zu überwachen, da SNMP- und Call Home-Uploads voneinander unabhängig sind. Wenn Sie jedes Mal benachrichtigt werden möchten, wenn eine Fehlerbedingung auftritt, können Sie den SNMP-Alarm CALLHOME-UPLOAD-EVENT so konfigurieren, dass bei jedem Upload von Call Home eine SNMP-Warnung generiert wird. Die SNMP-Warnung benachrichtigt den lokalen Administrator über das Auftreten kritischer Ereignisse.

- **Wie kontaktiere ich einen technischen Support?**

  Bei allen kritischen hardwarebezogenen Ereignissen erstellt Call Home automatisch eine Serviceanfrage an Citrix. Bei anderen Fehlern können Sie sich nach Überprüfung der Systemprotokolle an das Team des technischen Supports von Citrix wenden, um eine Serviceanfrage für weitere Untersuchungen zu öffnen. Weitere Informationen finden Sie unter http://support.citrix.com/article/CTX200021.

- **Welche Fehlerbedingungen überwacht Call Home in einer Citrix ADC Appliance?**

  Call Home unterstützt die Überwachung der folgenden Ereignisse in einer Citrix ADC Appliance:

  - Kompakte Flash-Laufwerkfehler
  - Festplattenfehler
  - Netzteilausfall
  - SSL-Kartenfehler
  - Warmer Neustart
  - Speicheranomalien
  - Zinsbegrenzung sinkt

- **Benötigen Sie eine separate Lizenz für Call Home?**

  Nein, Call Home benötigt keine separate Lizenz. Sie können es in allen Citrix ADC Plattformlizenzen aktivieren.

- **Welche Daten sendet Call Home an den Citrix Support Server und wie häufig werden diese gesendet?**

  Call Home sammelt und sendet zwei Arten von Daten an die CIS. Sie sind:

  - Grundlegende Systeminformationen (Ausführung der Citrix ADC Version, Bereitstellungsmodus (Standalone, HA, Cluster), Hardwareinformationen usw.). Es wird zum Zeitpunkt der Call Home Registrierung und als Teil von periodischen Herzschlägen gesendet. Der Heartbeat wird einmal alle 30 Tage gesendet, aber Sie können dieses Intervall von 1 bis 30 Tagen konfigurieren. Ein Wert von weniger als 5 Tagen wird jedoch nicht empfohlen, da häufige Uploads normalerweise nicht sehr nützlich sind.
  - Eine abgekürzte Version von, `show tech support bundle` wenn eine Fehlerbedingung vorliegt. Sie wird beim ersten Auftreten einer bestimmten Fehlerbedingung seit dem letzten Start der Appliance gesendet. Das heißt, ein erneutes Auftreten derselben Fehlerbedingung löst keinen weiteren Upload aus, es sei denn, die Appliance wurde nach dem vorherigen Auftreten neu gestartet.

- **Kann Call Home Systemprotokolle über einen Proxyserver generieren und hochladen?**

  Ja. Wenn Ihre Citrix ADC Appliance über keine direkte Internetverbindung verfügt, können Sie einen Proxy-Server konfigurieren und Systemprotokolle auf den Citrix Technical Support Server (CIS) hochladen.

- **Kann ich Call Home Daten überprüfen, bevor sie an CIS gesendet werden?**

  Leider können Sie Call Home Daten nicht überprüfen, bevor sie an CIS gesendet werden. Call Home sammelt zusätzlich zu den Daten, die Sie bei der Kontaktaufnahme mit dem Citrix Support-Team angeben, keine anderen Daten.

- **Wie sicher und privat sind die Call Home Uploads?**

  Call Home bietet Datensicherheit und Datenschutz auf folgende Weise:

  - Verwendet einen sicheren SSL/TLS-Kanal, um Daten an Citrix -Server zu übertragen.
  - Hochgeladene Daten werden nur von autorisiertem Personal überprüft und nicht an Dritte weitergegeben.

Clustering

October 5, 2021

Klicken Sie hier für häufig gestellte Fragen zum Clustering.

Verbindungsverwaltung

October 5, 2021

- **Was ist eine Admin-Verbindung?**

  Eine Admin-Verbindung stellt eine Verbindung zur NSIP-Adresse her und ermöglicht Administratoren die Konfiguration und Überwachung der Citrix ADC Appliance.

- **Was sind die Arten von Admin-Verbindungen?**

  Es gibt zwei Arten von Admin-Verbindungen:

  - SSH-Verbindung — Admin-Benutzer verwenden einen SSH-Client, um sich über die NSIP-Adresse anzumelden.
  - NITRO-API-Verbindung — Admin-Benutzer verwenden NITRO-APIs, um den Anmeldeprozess bei der Citrix ADC Appliance zu automatisieren.

> **Hinweis:**
>
> Admin-Benutzer können sich auch über die GUI anmelden, um sich anzumelden, indem sie einen Browser verwenden, um sich mit der NSIP-Adresse zu verbinden. Die GUI öffnet intern eine NITRO API-Verbindung. Daher entspricht eine GUI-Sitzung einer NITRO-API-Verbindung, und FAQs im Zusammenhang mit der NITRO-API gelten für die GUI.

- **Wie viele gleichzeitige Administratorverbindungen sind auf einer Citrix ADC Appliance zulässig?**

  Die Appliance ermöglicht bis zu 20 gleichzeitige Administratorverbindungen.

- **Welche Anmeldedaten werden für eine Administratoranmeldung benötigt?**

  Administratoranmeldung erfordert einen Benutzernamen und ein Kennwort.

  Hinweis: Ein Authentifizierungsschlüssel kann anstelle eines Kennworts verwendet werden.

- **Welche externen Authentifizierungsmethoden unterstützt eine Citrix ADC Appliance?**

  Die Appliance unterstützt die folgenden externen Authentifizierungsmethoden:

  - RADIUS
  - LDAP
  - TACACS

- **Was ist ein Kunde?**

  Ein Client ist ein Gerät (Laptop oder Desktop), das vom Admin-Benutzer verwendet wird, um eine Admin-Verbindung zu öffnen.

- **Was ist ein Sitzungstoken?**

  Ein Sitzungstoken ist ein eindeutiger Bezeichner, den die Citrix ADC Appliance an einen Client ausgibt, der eine NITRO-API-Anmeldeanforderung sendet.

  - API-Clients können das Sitzungstoken wiederverwenden, wenn es nicht abgelaufen ist, für nachfolgende API-Anforderungen für neue TCP-Verbindungen

  - GUI-Clients öffnen intern NITRO-API-Verbindungen und halten das Sitzungstoken während der GUI-Sitzung aktiv.

- **Was ist eine aktive Sitzung auf einer Citrix ADC Appliance?**

  Eine CLI-Sitzung gilt als aktiv, wenn die Sitzung noch nicht abgelaufen ist und über eine offene SSH-Verbindung mit einer Citrix ADC Appliance verfügt.

  Eine NITRO-API-Sitzung gilt als aktiv, wenn das Timeout des Sitzungstoken auf der Citrix ADC Appliance noch nicht abgelaufen ist.

- **Wie erzwingt Citrix ADC das Limit für gleichzeitige Verbindungen?**

  Jedes Mal, wenn die Citrix ADC Appliance eine Administratorverbindungsanforderung (SSH oder NITRO API) empfängt, überprüft sie die Anzahl der geöffneten Administratorverbindungen. Wenn die Nummer kleiner als 20 ist, wird eine neue Verbindung geöffnet.

- **Welcher Leistungsindikator spiegelt die Anzahl der Adminverbindungen auf einer Citrix ADC Appliance wider?**

  Der Verbindungszähler (nsconfigd_cur_clients) gibt die Anzahl der aktiven Verbindungen an. Dieser Leistungsindikator wird erhöht, wenn ein Client eine neue Verbindung zur Appliance öffnet, und wird verringert, wenn eine Verbindung geschlossen wird.

- **Welcher Leistungsindikator spiegelt die Anzahl der aktiven Token auf der Citrix ADC Appliance wider?**

  Der Zähler *configd_cur_tokens* spiegelt die Anzahl der aktiven Token auf der Citrix ADC Appliance wider.

- **Wie behandelt Citrix ADC Appliance Fehler bei einer Verbindung?**

  Die Citrix ADC Appliance schließt sofort die Clientverbindung (CLI, API und GUI), wenn bei einer Verbindung Fehler auftreten.

- **Zählt eine CLI- oder GUI-Sitzung für eine Verbindung mit der Verwaltungsadresse auf das Admin-Verbindungslimit?**

  Ja, alle CLI- und GUI-Verbindungen sind TCP-basierte Verbindungen, und jede TCP-Verbindung mit der Verwaltungsadresse zählt mit dem Admin-Verbindungslimit.

- **Zählt eine NITRO -Sitzung auf das Admin-Verbindungslimit?**

  Eine NITRO -Sitzung zählt auf das Admin-Verbindungslimit, wenn eine offene TCP-Verbindung mit dem von der Citrix ADC Appliance ausgestellten Sitzungstoken vorhanden ist.

- **Was ist der standardmäßige Zeitüberschreitungszeitraum für API-, GUI- und CLI-Sitzungen auf der Citrix ADC Appliance?**

  In der folgenden Tabelle wird der Standard-Timeout-Zeitraum für API-, GUI- und CLI-Sitzungen auf der Citrix ADC Appliance aufgeführt:

Citrix ADC Versionen	CLI-Standard-Timeout-Zeitraum (min)	API-Standard-Timeout-Zeitraum (min)	GUI-Standard-Timeout-Periode (min)
NetScaler 9,3	Ohne	30 Minuten	30 Minuten
NetScaler 10.1	Ohne	30 Minuten	30 Minuten
NetScaler ab 10.5	15 Minuten	30 Minuten	15 Minuten

- **Wie können Sie das Timeout der CLI-Sitzungen auf einer Citrix ADC Appliance festlegen?**

  Das CLI-Sitzungs-Timeout kann konfiguriert werden, indem Sie den folgenden Befehl an der CLI-Eingabeaufforderung ausführen:

  ```
  set cli mode -timeout \<xx seconds>
  ```

- **Wie überschreiben Sie die standardmäßige Zeitüberschreitung bei Verwendung der NITRO API?**

  Sie können den Standard-Timeout-Zeitraum für eine NITRO-API überschreiben, indem Sie die Zeitüberschreitungsdauer im Feld “timeout” des Anmeldeobjekts festlegen. Wenn das Sitzungstimeout auf Null festgelegt ist, hat das Sitzungstoken ein unbegrenztes Timeout.

  Hinweis: Ein unbegrenztes Timeout ist nicht ratsam, da Sitzungen, die keine Zeitüberschreitung aufweisen, weiterhin auf die Anzahl der Admin-Verbindungen zählen.

- **Was passiert, wenn ein Benutzerkonto aus der Citrix ADC Appliance gelöscht wird, nachdem eine Administratorsitzung erstellt wurde?**

  Für interne Systembenutzer schließt die Citrix ADC Appliance die vorhandene CLI- oder NITRO-API-Sitzung.

  Für externe Systembenutzer bleibt die Sitzung aktiv, bis sie abläuft.

- **Können NITRO API-Clients ein einzelnes Session-Token verwenden, um mehrere Admin-Verbindungen auf der Citrix ADC Appliance zu öffnen?**

  Ja. Jede solche Verbindung zählt mit dem Admin-Verbindungslimit.

- **Wenn der Verwaltungszugriff für eine SNIP-Adresse aktiviert ist, werden Admin-Verbindungen zu dieser Adresse mit dem Limit für die Anzahl der Admin-Verbindungen angerechnet?**

  Ja, Administratorverbindungen zur Verwaltungsadresse (SNIP) zählen auf das Admin-Verbindungslimit von Citrix ADC.

- **Kann sich ein Citrix ADC Administrator bei der Citrix ADC Appliance anmelden, nachdem die maximale Verbindungsgrenze erreicht ist?**

Ja. Eine weitere Admin-Verbindung ist zulässig, nachdem das maximale Verbindungslimit erreicht wurde.

- **Können NITRO API-Endpunkte mehrere Admin-Verbindungen auf Citrix ADC der Appliance öffnen?**

  Ja, NITRO API-Endpunkte können mehrere Admin-Verbindungen öffnen und das Limit für die gleichzeitige Admin-Verbindung auf einer Citrix ADC Appliance ausschöpfen. In solchen Situationen ist eine zusätzliche SSH/CLI-Verbindung zulässig, und der Administrator kann das Schließen alter API-Sitzungen erzwingen oder die Dauer des Sitzungstimeouts für die vorhandenen API-Sitzungen reduzieren.

- **Kann ein Client mehrere API-Sitzungen auf einer Citrix ADC Appliance öffnen?**

  Ja, ein Client kann mehrere API-Sitzungen öffnen, indem er sich wiederholt anmeldet. Beispielsweise kann sich der Client nach einem Neustart wieder anmelden.
  Hinweis: Wiederholte Clientanmeldungen werden auf das Admin-Verbindungslimit der Citrix ADC Appliance angerechnet.

- **Können API-Clients das gesamte API-Sitzungstoken Limit verwenden?**

  Ja, API-Clients können das gesamte API-Sitzungstoken Limit verwenden, indem sie sich wiederholt anmelden, ohne ein zuvor ausgestelltes Token zu verwenden.

  Hinweis: Wenn das Session-Timeout eines Clients Null ist, ist das Token für immer gültig. Wiederholte Anmeldungen mit neuen Sitzungstoken können gegen das Limit für API-Sitzungstoken zählen.

- **Zählen CLI-Sitzungen auf das API-Sitzungstoken Limit?**

  Nein, CLI-Sitzungen werden nicht für das API-Sitzungstoken Limit gezählt.

- **Können Administratorbenutzer telnet verwenden, um eine CLI-Sitzung zu öffnen?**

  Nein. Nur ein SSH-Client kann eine CLI-Sitzung öffnen.

- **Was sind Verbindungslimit und API-Sitzungslimit für verschiedene Citrix ADC Versionen anwendbar?**

  In der folgenden Tabelle sind die maximalen Grenzwerte für die gleichzeitige Adminverbindung und aktive API-Sitzungen aufgeführt, die für verschiedene Citrix ADC Versionen gelten:

Citrix ADC Versionen	9.3	10.1 (Vor 130.x)	10.1 (Vor 130.10)	10.1 (Von 130.10)
Maximale Anzahl gleichzeitiger Admin-Verbindungen	20	20	20	20

Citrix ADC Versionen	9.3	10.1 (Vor 130.x)	10.1 (Vor 130.10)	10.1 (Von 130.10)
Maximale Anzahl aktiver API-Sitzungen*	1000	20	1000	1000

Hinweis:

- API-Sitzungen gelten als aktiv, wenn sie kein Timeout überschritten haben. Wenn beispielsweise 500 API-Sitzungen erstellt wurden, 100 aber abgelaufen sind, sind 400 API-Sitzungen aktiv.
- Eine API-Sitzung muss keine TCP-Verbindung mit der Citrix ADC Appliance öffnen.

Content Switching

October 5, 2021

- **Ich habe eine Nicht-Citrix ADC-Load Balancing-Appliance im Netzwerk installiert. Ich möchte jedoch Content Switching der Citrix ADC Appliance verwenden, um die Clientanforderungen an die Load Balancing-Appliance weiterzuleiten. Ist es möglich, die Content Switching-Funktion der Citrix ADC Appliance mit einer Nicht-Citrix ADC-Load Balancing-Appliance zu verwenden?**

  Ja. Sie können die Content Switching-Funktion der Citrix ADC Appliance mit der Lastausgleichsfunktion der Citrix ADC-Appliance oder einer Nicht-Citrix ADC-Load Balancing-Appliance verwenden. Stellen Sie jedoch bei Verwendung der Nicht-Citrix ADC-Load Balancing-Appliance sicher, dass Sie einen virtuellen Lastausgleichsserver auf der Citrix ADC Appliance erstellen und diesen als Service an die Nicht-Citrix ADC-Load Balancing-Appliance binden.

- **Wie unterscheidet sich ein virtueller Content Switching-Server von einem virtuellen Lastenausgleichsserver?**

  Ein virtueller Content Switching-Server kann die Clientanforderungen nur an andere virtuelle Server senden. Es kommuniziert nicht mit den Servern.

  Ein virtueller Lastausgleichsserver gleicht die Clientlast zwischen den Servern aus und kommuniziert mit den Servern. Es überwacht die Serververfügbarkeit und kann verwendet werden, um verschiedene Lastausgleichsalgorithmen anzuwenden, um die Datenverkehrslast zu verteilen.

  Content Switching ist eine Methode, mit der Clientanforderungen für bestimmte Inhaltstypen mittels Lastenausgleich virtuelle Server an Zielserver geleitet werden. Sie können die Clientanforderungen an die Server weiterleiten, die am besten geeignet sind, um sie zu bearbeiten.

Dies führt zu geringeren Gemeinkosten für die Verarbeitung der Clientanforderungen auf den Servern.

- **Ich möchte die Content Switching-Funktion der Citrix ADC Appliance implementieren, um die Clientanforderungen zu leiten. Welche Arten von Clientanfragen kann ich mit Content Switching umleiten?**

  Sie können nur HTTP, HTTPS, FTP, TCP, Secure TCP- und RTSP-Clientanforderungen mit Content Switching umleiten. Um HTTPS-Clientanforderungen zu leiten, müssen Sie die SSL-Offload-Funktion auf der Appliance konfigurieren.

- **Ich möchte Content Switching-Regeln für die Citrix ADC Appliance erstellen. Was sind die verschiedenen Elemente der Clientanforderung, auf denen ich eine Content Switching-Regel erstellen kann?**

  Sie können die Content Switching-Regeln basierend auf den folgenden Elementen und deren Werten in der Clientanforderung erstellen:

  - URL
  - URL-Token
  - HTTP-Version
  - HTTP-Header
  - Quell-IP-Adresse des Clients
  - Client-Version
  - Ziel-TCP-Port

- **Ich verstehe, dass die Content Switching-Funktion der Citrix ADC Appliance dazu beiträgt, die Leistung des Netzwerks zu verbessern. Ist das richtig?**

  Ja. Sie können die Clientanfragen an die Server richten, die am besten geeignet sind, um sie zu behandeln. Das Ergebnis ist ein reduzierter Overhead für die Verarbeitung der Clientanforderungen auf den Servern.

- **Welche Funktion der Citrix ADC Appliance sollte ich auf der Citrix ADC-Appliance konfigurieren, um die Standortverwaltung und die Reaktionszeit auf die Clientanforderungen zu verbessern?**

  Sie können die die Content Switching-Funktion der Citrix ADC Appliance konfigurieren, um die Standortverwaltung und die Reaktionszeit auf die Clientanforderung zu verbessern. Mit dieser Funktion können Sie Inhaltsgruppen innerhalb desselben Domänennamens und derselben IP-Adresse erstellen. Dieser Ansatz ist flexibel, im Gegensatz zu dem üblichen Ansatz, den Inhalt explizit in verschiedene Domänennamen und IP-Adressen zu partitionieren, die für den Benutzer sichtbar sind.

  Mehrere Partitionen, die eine Website in verschiedene Domänennamen und IP-Adressen aufteilen, zwingen den Browser, für jede Domäne, die sie beim Rendern und Abrufen des

Inhalts einer Webseite findet, eine separate Verbindung herzustellen. Diese zusätzlichen WAN-Verbindungen beeinträchtigen die Reaktionszeit für die Webseite.

- **Ich habe eine Website in einer Webserverfarm gehostet. Welche Vorteile bietet die Citrix ADC Content Switching-Funktion für diese Art von Setup?**

  Die die Content Switching-Funktion bietet die folgenden Vorteile auf einer Citrix ADC Appliance an einer Site, die in einer Webserverfarm basiert:

  - Verwalten Sie den Websiteinhalt, indem Sie eine Content-Gruppe innerhalb derselben Domäne und derselben IP-Adresse erstellen.
  - Erhöhen Sie die Antwortzeit auf Clientanforderungen, indem Sie die Inhaltsgruppe innerhalb derselben Domäne und derselben IP-Adresse verwenden.
  - Vermeiden Sie die Notwendigkeit einer vollständigen Content-Replikation über Domänen hinweg.
  - Aktivieren Sie anwendungsspezifische Content-Partitionierung. Beispielsweise können Sie Clientanforderungen an einen Server weiterleiten, der nur dynamische Inhalte oder nur statische Inhalte verarbeitet, je nach Anforderung.
  - Unterstützen Sie Multi-Homing von mehreren Domänen auf demselben Server und verwenden Sie die gleiche IP-Adresse.
  - Wiederverwenden von Verbindungen zu den Servern.

- **Ich möchte die die Content Switching-Funktion auf der Citrix ADC Appliance implementieren. Ich möchte die Client-Anfragen an die verschiedenen Server leiten, nachdem ich die verschiedenen Parameter jeder Anfrage ausgewertet habe. Welchen Ansatz sollte ich beachten, um dieses Setup bei der Konfiguration der die Content Switching-Funktion zu implementieren?**

  Sie können Richtlinienausdrücke verwenden, um Richtlinien für die die Content Switching-Funktion zu erstellen. Ein Ausdruck ist eine Bedingung, die durch den Vergleich der Kriterien der Clientanforderung mit einem Operanden ausgewertet wird, indem ein Operator verwendet wird. Sie können die folgenden Parameter der Clientanforderung verwenden, um einen Ausdruck zu erstellen:

  - **Methode**- HTTP-Anforderungsmethode.
  - **URL**- URL im HTTP-Header.
  - **URL TOKENS**- Spezielle Token in der URL.
  - **VERSION**- HTTP-Anforderungsversion.
  - **URL-QUERY**- Enthält die URL-Abfrage LEN, URL-LEN und HTTP-Header.
  - **SOURCEIP**- IP-Adresse des Clients.

  Im Folgenden finden Sie eine vollständige Liste der Operatoren, die Sie verwenden können, um einen Ausdruck zu erstellen:

  - == (entspricht)

- ! = (nicht gleich)
- EXISTS
- NOT EXISTS
- CONTAINS
- NOT CONTAINS
- GT (größer als)
- LT (kleiner als)

Sie können auch verschiedene Regeln erstellen, bei denen es sich um logische Aggregationen einer Reihe von Ausdrücken handelt. Sie können mehrere Ausdrücke kombinieren, um Regeln zu erstellen. Um Ausdrücke zu kombinieren, können Sie && (UND) und	(OR) -Operatoren. Sie können auch Klammern verwenden, um verschachtelte und komplexe Regeln zu erstellen.

- **Ich möchte eine regelbasierte Richtlinie zusammen mit einer URL-basierten Richtlinie für denselben virtuellen Content Switching-Server konfigurieren. Ist es möglich, beide Arten von Richtlinien für denselben virtuellen Content Switching-Server zu erstellen?**

  Ja. Sie können beide Richtlinientypen für denselben virtuellen Content Switching-Server erstellen. Stellen Sie jedoch sicher, dass Sie Prioritäten zuweisen, um eine angemessene Priorität für die Richtlinien festzulegen.

- **Ich möchte Content Switching-Richtlinien erstellen, die den Domänennamen zusammen mit einem Präfix und einem Suffix einer URL auswerten und die Clientanforderungen entsprechend leiten. Welche Art von Content Switching-Richtlinien sollte ich erstellen?**

  Sie können eine Domänen- und Exakt-URL-Richtlinie erstellen. Wenn dieser Richtlinientyp ausgewertet wird, wählt die Citrix ADC Appliance eine Inhaltsgruppe aus, wenn der vollständige Domänenname und die URL in der Clientanforderung mit den konfigurierten übereinstimmen. Die Clientanforderung muss mit dem konfigurierten Domänennamen übereinstimmen und exakt mit dem Präfix und dem Suffix der URL übereinstimmen, wenn sie konfiguriert sind.

- **Ich möchte Content Switching-Richtlinien erstellen, die den Domänennamen zusammen mit einem Teilpräfix und einem Suffix der URL auswerten und die Clientanforderungen entsprechend leiten. Welche Art von Content Switching-Richtlinien sollte ich erstellen?**

  Sie können eine Domänen- und Platzhalter-URL-Richtlinie für den virtuellen Content Switching-Server erstellen. Wenn dieser Richtlinientyp ausgewertet wird, wählt die Citrix ADC Appliance

eine Inhaltsgruppe aus, wenn die Anforderung mit dem vollständigen Domänennamen übereinstimmt und teilweise mit dem URL-Präfix übereinstimmt.

- **Was ist eine Wildcard-URL-Richtlinie?**

  Sie können Platzhalter verwenden, um partielle URLs in Clientanforderungen an die URL auszuwerten, die Sie auf der Citrix ADC Appliance konfiguriert haben. Sie können Platzhalter in den folgenden URL-basierten Richtlinien verwenden:

  - Nur Präfix. Der Ausdruck /sports/* entspricht beispielsweise allen URLs, die unter der URL /sports verfügbar sind. In ähnlicher Weise stimmt der Ausdruck /sports * mit allen URLs überein, deren Präfix /sports lautet.
  - Nur Suffix. Zum Beispiel stimmt der Ausdruck /*.jsp mit allen URLs mit einer Dateinamenerweiterung von jsp überein.
  - Präfix und Suffix. Der Ausdruck /sports/ *.jsp entspricht beispielsweise allen URLs unter der /sports/ URL, die auch die JSP-Dateinamenerweiterung haben. In ähnlicher Weise entspricht der Ausdruck /sports *.jsp alle URLs mit einem Präfix von /sports * und einer Dateinamenerweiterung von jsp.

- **Was ist eine Domänen- und Regelrichtlinie?**

  Wenn Sie eine Domänen- und Regelrichtlinie erstellen, muss die Clientanforderung mit der vollständigen Domäne und der auf der Citrix ADC Appliance konfigurierten Regel übereinstimmen.

- **Wie lautet die Standardpriorität für die Auswertung von Richtlinien?**

  Standardmäßig werden die regelbasierten Richtlinien zuerst ausgewertet.

- **Wenn ein Teil des Inhalts für alle Clientanforderungen identisch ist, welche Art von Priorität sollte ich für die Bewertung von Richtlinien verwenden?**

  Wenn ein Teil des Inhalts für alle Benutzer gleich ist und verschiedene Inhalte auf der Grundlage von Clientattributen bereitgestellt werden müssen, können Sie die URL-basierte Priorität für die Richtlinienbewertung verwenden.

- **Welche Policy-Express-Syntax wird beim Content Switching unterstützt?**

  Die Content Switching unterstützt zwei Arten von Richtlinienausdrücken:

  - **Klassische Syntax** - Klassische Syntax beim Content Switching beginnt mit dem Schlüsselwort REQ und ist fortgeschrittener als die Standardsyntax. Klassische Richtlinien können nicht an eine Aktion gebunden werden. Daher kann der virtuelle Zielserver für Lastenausgleich erst hinzugefügt werden, nachdem der virtuelle Content Switching-Server gebunden wurde.
  - **Standardsyntax:** Die Standardsyntax beginnt im Allgemeinen mit dem Schlüsselwort HTTP und ist einfacher zu konfigurieren. Eine Ziel-Lastenausgleichsaktion für virtuelle Server kann an eine Standard-Syntaxrichtlinie gebunden werden, und die Richtlinie kann auf mehreren virtuellen Content Switching-Servern verwendet werden.

- **Kann ich eine einzelne Content Switching-Richtlinie an mehrere virtuelle Server binden?**

  Ja. Sie können eine einzelne Content Switching-Richtlinie an mehrere virtuelle Server binden, indem Sie Richtlinien mit definierten Aktionen verwenden. Content Switching-Richtlinien, die eine Aktion verwenden, können an mehrere virtuelle Server gebunden werden, da der virtuelle Zielserver für den Lastenausgleich nicht mehr in der Content Switching-Richtlinie angegeben ist. Die Möglichkeit, eine einzelne Richtlinie an mehrere virtuelle Content Switching-Server zu binden, trägt dazu bei, die Größe der Content Switching-Konfiguration weiter zu reduzieren.

  Weitere Informationen finden Sie in den folgenden Knowledge Center-Artikeln und Themen zur Citrix Dokumentation:

  - Siehe CTX122918 - Binden der gleichen Content Switching-Richtlinie an einen virtuellen Server mit zwei Content Switching auf einer Citrix ADC Appliance.
  - Weitere Informationen finden Sie unter CTX122736 - Binden derselben erweiterten Richtlinie an mehrere virtuelle Server mit Content Switching mithilfe von Richtlinienbeschriftungen.
  - Konfigurieren von Basic Content Switching

- **Kann ich eine aktionsbasierte Richtlinie mit klassischen Ausdrücken erstellen?**

  Nein. Ab sofort unterstützt Citrix ADC keine Richtlinien, die klassische Syntaxausdrücke mit Aktionen verwenden. Der virtuelle Ziel-Lastenausgleichsserver muss beim Binden der Richtlinie hinzugefügt werden, anstatt ihn in einer Aktion zu definieren.

Debugging

October 5, 2021

- **Wie kann ich die Schnittstelle (CLI, GUI oder API) bestimmen, über die eine Operation ausgeführt wurde?**

  Der Citrix ADC verfolgt die Schnittstellen, über die Vorgänge ausgeführt werden. Sie können diese Informationen in syslogs (in der Benutzeroberfläche, navigieren Sie zu Konfiguration > System > Auditing > Überwachungsmeldungen > Syslog-Nachrichten) oder in der Datei ns.log (im Verzeichnis /var/log/) anzeigen.

  Beispielsweise werden Vorgänge, die über die API ausgeführt werden, als API CMD_EXECUTED gekennzeichnet.

Hardware

October 5, 2021

Klicken Sie hier für häufig gestellte Fragen zur MPX-Hardware.

Hohe Verfügbarkeit

October 5, 2021

- **Welche Ports werden verwendet, um die HA-bezogenen Informationen zwischen den Knoten in einer HA-Konfiguration auszutauschen?**

  In einer HA-Konfiguration verwenden beide Knoten die folgenden Ports, um Informationen für HA auszutauschen:

  - UDP-Port 3003, zum Austausch von Heartbeat-Paketen
  - Port 3010, für Synchronisation und Befehlsausbreitung

- **Welche Konfigurationen werden nicht in einer HA-Konfiguration im INC- oder Nicht-INC-Modus synchronisiert oder weitergegeben?**

  Konfigurationen, die mit den folgenden Befehlen implementiert werden, werden weder propagiert noch mit dem sekundären Knoten synchronisiert:

  - Alle knotenspezifischen HA-Konfigurationsbefehle. Zum Beispiel `add ha nodeset ha node`, und `bind ha node`.
  - Alle Interface-bezogenen Konfigurationsbefehle. Zum Beispiel, setzen Sie Schnittstelle und unset interface.
  - Alle kanalbezogenen Konfigurationsbefehle. Fügen Sie beispielsweise Kanal hinzu, setzen Sie den Kanal ein und binden Sie den Kanal ein.

  Weitere Informationen zur HA-Konfiguration im INC-Modus finden Sie unter Konfigurieren von Hochverfügbarkeitsknoten in verschiedenen Subnetzen.

- **Welche Konfigurationen werden in einer HA-Konfiguration im INC-Modus nicht synchronisiert oder weitergegeben?**

  Die folgenden Konfigurationen werden weder synchronisiert noch weitergegeben. Jeder Knoten hat seinen eigenen.

  - MIPs
  - SNIPs
  - VLANs

- Routen (außer LLB-Routen)
- Routenüberwachung
- RNAT Regeln (außer RNAT Regel mit VIP als NAT IP)
- Dynamische Routing-Konfigurationen.

- **Was sind die Bedingungen, die die Synchronisation auslösen?**

  Die Synchronisierung wird durch eine der folgenden Bedingungen ausgelöst:

  - Die Inkarnationsnummer des primären Knotens, der vom sekundären empfangen wird, stimmt nicht mit der des sekundären Knotens überein.
    Hinweis: Beide Knoten in einer HA-Konfiguration behalten einen Leistungsindikator namens *Inkarnationsnummer*, der die Anzahl der Konfigurationen in der Konfigurationsdatei des Knotens zählt. Jeder Knoten sendet seine Inkarnationsnummer an jeden anderen Knoten in den Heartbeat-Nachrichten. Die Inkarnationsnummer wird für die folgenden Befehle nicht erhöht:
    * Alle HA-Konfigurationsbefehle. Zum Beispiel `add ha nodeset ha node`, und `bind ha node`.
    * Alle Interface-bezogenen Befehle. Zum Beispiel, setzen Sie Schnittstelle und unset interface.
    * Alle kanalbezogenen Befehle. Fügen Sie beispielsweise Kanal hinzu, setzen Sie den Kanal ein und binden Sie den Kanal ein.
  - Der sekundäre Knoten wird nach einem Neustart angezeigt.
  - Der primäre Knoten wird nach einem Failover sekundär.

- **Wird eine dem sekundären Knoten hinzugefügte Konfiguration auf dem primären Knoten synchronisiert?**

  Nein, eine dem sekundären Knoten hinzugefügte Konfiguration wird nicht mit dem primären Knoten synchronisiert.

- **Was könnte der Grund dafür sein, dass beide Knoten die primäre in einer HA-Konfiguration sein?**

  Der wahrscheinlichste Grund ist, dass der primäre und sekundäre Knoten beide fehlerfrei sind, aber der sekundäre nicht die Heartbeat-Pakete vom primären erhalten. Das Problem kann mit dem Netzwerk zwischen den Knoten liegen.

- **Steht bei einer HA-Konfiguration Probleme auf, wenn Sie die beiden Knoten mit unterschiedlichen Systemtakteinstellungen bereitstellen?**

  Unterschiedliche Systemtakteinstellungen auf den beiden Knoten können folgende Probleme verursachen:

  - Die Zeitstempel in den Protokolldateieinträgen stimmen nicht überein. Diese Situation macht es schwierig, die Protokolleinträge auf Probleme zu analysieren.

  - Nach einem Failover können Probleme mit jeder Art von Cookie-basierte Persistenz für den Lastenausgleich auftreten. Ein signifikanter Unterschied zwischen den Zeiten kann dazu führen, dass ein Cookie früher als erwartet abläuft, was zur Beendigung der Persistenzsitzung führt.
  - Ähnliche Überlegungen gelten für zeitbezogene Entscheidungen auf den Knoten.

- **Was sind die Bedingungen für den Ausfall des Befehls *force HA-Synchronisierung* ?**

  Die erzwungene Synchronisierung schlägt unter folgenden Umständen fehl:

  - Sie erzwingen die Synchronisierung, wenn die Synchronisation bereits ausgeführt wird.
  - Der sekundäre Knoten ist deaktiviert.
  - HA-Synchronisierung ist auf dem aktuellen sekundären Knoten deaktiviert.
  - Die HA-Propagierung ist auf dem aktuellen primären Knoten deaktiviert, und Sie erzwingen die Synchronisierung vom primären Knoten.

- **Was sind die Bedingungen für den Ausfall des Befehls " *HA-Dateien synchronisieren* "?**

  Die Synchronisierung von Konfigurationsdateien schlägt fehl, wenn der sekundäre Knoten deaktiviert ist.

- **Wenn der sekundäre Knoten in einer HA-Konfiguration als primärer Knoten übernimmt, wechselt er in den sekundären Status zurück, wenn der ursprüngliche primäre Knoten wieder online ist?**

  Nein. Nachdem der sekundäre Knoten als primärer Knoten übernommen hat, bleibt er auch dann als primär, wenn der ursprüngliche primäre Knoten wieder online ist. Führen Sie zum Austausch des primären und sekundären Status der Knoten den Befehl *force failover* aus.

- **Was sind die Bedingungen für den Ausfall des *Force-Failover-Befehls*?**

  Ein erzwungenes Failover schlägt unter folgenden Umständen fehl:

  - Der sekundäre Knoten ist deaktiviert.
  - Der sekundäre Knoten ist so konfiguriert, dass er sekundär bleibt.
  - Der primäre Knoten ist so konfiguriert, dass er primär bleibt.
  - Der Status des Peer-Knotens ist unbekannt.

Integriertes Caching

October 5, 2021

Content-Gruppen

- **Wie unterscheidet sich eine DEFAULT Content-Gruppe von anderen Inhaltsgruppen?**

Das Verhalten der DEFAULT-Content-Gruppe ist das gleiche wie bei jeder anderen Gruppe. Das einzige Attribut, das die DEFAULT-Content-Gruppe besonders macht, ist das, wenn ein Objekt zwischengespeichert wird und keine Content-Gruppe erstellt wurde. Das Objekt wird in der Gruppe DEFAULT zwischengespeichert.

- **Was ist die Option Cache-Control auf der Content-Gruppenebene?**

  Sie können jeden Cache-Control-Header an den Browser senden. Es gibt die Option -cacheControl auf Inhaltsgruppenebene, mit der Sie den Cache-Control-Header angeben können, der in die Antwort an den Browser eingefügt werden soll.

- **Was ist die Option Minhit auf der Ebene der Inhaltsgruppen?**

  `Minhit` ist ein ganzzahliger Wert, der die Mindestanzahl der Auswahl für eine Cache-Richtlinie angibt, bevor das Objekt zwischengespeichert wird. Dieser Wert ist auf Inhaltsgruppenebene konfigurierbar. Es folgt die Syntax, um diesen Wert von der CLI zu konfigurieren.

  ```
  add/set cache contentGroup \<Content_Group_Name> [-minHits \<Integer>]
  ```

- **Was ist die Verwendung der Option ExpireAtLastByte?**

  Die Option expireatLastByte ermöglicht es dem integrierten Cache, das Objekt beim Herunterladen abzulaufen. Nur Anfragen, bei denen es sich um ausstehende Anfragen handelt, werden dann aus dem Cache bedient. Alle neuen Anfragen werden an den Server gesendet. Diese Einstellung ist nützlich, wenn das Objekt häufig geändert wird, wie bei Aktienkursen. Dieser Ablaufmechanismus funktioniert zusammen mit der Flash-Cache-Funktion. Um eine expireatLastByte-Option zu konfigurieren, führen Sie den folgenden Befehl von der CLI aus:

  ```
  add cache contentGroup \<Group_Name> -expireAtLastByte YES
  ```

Cache-Richtlinie

- **Was ist eine Caching-Richtlinie?**

  Richtlinien bestimmen, welche Transaktionen zwischenspeicherbar sind und welche nicht. Außerdem fügen Richtlinien das standardmäßige HTTP-Caching-Verhalten hinzu oder überschreiben es. Richtlinien bestimmen eine Aktion, wie CACHE oder NOCACHE, abhängig von den spezifischen Eigenschaften der Anforderung oder Antwort. Wenn eine Antwort mit den Richtlinienregeln übereinstimmt, wird das Objekt in der Antwort der in der Richtlinie konfigurierten Content-Gruppe hinzugefügt. Wenn Sie keine Inhaltsgruppe konfiguriert haben, wird das Objekt der Inhaltsgruppe DEFAULT hinzugefügt.

- **Was ist ein politischer Treffer?**

  Eine Auswahl erfolgt, wenn eine Anfrage oder Antwort mit einer Cache-Richtlinie übereinstimmt.

- **Was ist ein Fräulein?**

  Ein Fehler tritt auf, wenn eine Anforderung oder Antwort keiner Cache-Richtlinie entspricht. Ein Fehler kann auch auftreten, wenn die Anforderung oder Antwort einer Cache-Richtlinie entspricht, aber eine Überschreibung des RFC-Verhaltens verhindert, dass das Objekt im Cache gespeichert wird.

- **Ich habe die integrierte Caching-Funktion der Citrix ADC Appliance konfiguriert. Beim Hinzufügen der folgenden Richtlinie wird eine Fehlermeldung angezeigt. Gibt es einen Fehler im Befehl?**

  ```
  add cache policy image_caching -rule exp1 | ns_ext_not_jpeg -action
  cache
  ```

  ```
  \> ERROR: No such command
  ```

  Im vorhergehenden Befehl muss der Ausdruck innerhalb der Anführungszeichen stehen. Ohne Anführungszeichen gilt der Operator als der Rohroperator.

Speicheranforderungen

- **Welche Befehle kann ich auf der Citrix ADC Appliance ausführen, um den dem Cache zugewiesenen Speicher zu überprüfen?**

  Um den für den Cache in der Citrix ADC Appliance zugewiesenen Speicher anzuzeigen, führen Sie einen der folgenden Befehle von der Befehlszeilenschnittstelle aus:

  - `show cache parameter`

    Überprüfen Sie in der Ausgabe den Wert des Parameters Speichernutzungslimit. Dies ist der maximale Speicher, der für den Cache zugewiesen wird.

  - `show cache \<Content_Group_Name>`

    Prüfen Sie in der Ausgabe die Werte der Parameter Speicherauslastung und Speicherauslastung, die den für die einzelne Content-Gruppe verwendeten und zugewiesenen Speicher angeben.

- **Meine Citrix ADC Appliance verfügt über 2 GB Arbeitsspeicher. Gibt es eine empfohlene Speicherbegrenzung für den Cache?**

  Für jedes Modell der Citrix ADC Appliance können Sie dem Cache die Hälfte des Speichers zuweisen. Citrix empfiehlt jedoch, aufgrund der internen Speicherabhängigkeit etwas weniger als die Hälfte des Speichers zuzuweisen. Sie können den folgenden Befehl ausführen, um dem Cache 1 GB Arbeitsspeicher zuzuweisen:

  ```
  set cache parameter -memLimit 1024
  ```


- **Ist es möglich, Speicher für einzelne Content-Gruppen zu reservieren?**

  Ja. Obwohl Sie Speicher für den integrierten Cache global zuweisen, indem Sie den set-cache-Parameter —memlimit ausführen <Integer>, können Sie einzelnen Inhaltsgruppen Speicher zuweisen, indem Sie den <Content_Group_Name> <Integer> Befehl set cache —memLimit ausführen. Der maximale Arbeitsspeicher, den Sie Inhaltsgruppen (kombiniert) zuweisen können, darf nicht den Speicher überschreiten, den Sie dem integrierten Cache zugewiesen haben.

- **Was ist die Abhängigkeit von Speicher zwischen integriertem Cache und TCP-Puffer?**

  Wenn die Citrix ADC Appliance über 2 GB Speicher verfügt, reserviert die Appliance etwa 800 MB bis 900 MB Arbeitsspeicher und der Rest wird dem Betriebssystem FreeBSD zugewiesen. Daher können Sie dem integrierten Cache bis zu 512 MB Speicher zuweisen und der Rest wird dem TCP-Puffer zugewiesen.

- **Beeinflusst es den Caching-Prozess, wenn ich dem integrierten Cache keinen globalen Speicher zuweise?**

  Wenn Sie dem integrierten Cache keinen Speicher zuweisen, werden alle Anfragen an den Server gesendet. Um sicherzustellen, dass Sie dem integrierten Cache Speicher zugewiesen haben, führen Sie den Befehl show cache-Parameter aus. Tatsächlich werden keine Objekte zwischengespeichert, wenn der globale Speicher 0 ist, also muss er zuerst festgelegt werden.

Überprüfungsbefehle

- **Welche Optionen gibt es für die Anzeige von Cache-Statistiken?**

  Sie können eine der folgenden Optionen verwenden, um die Statistiken für den Cache anzuzeigen:

  - `stat cache`

    So zeigen Sie die Zusammenfassung der Cache-Statistiken an.

  - `stat cache -detail`

    Um die vollständigen Details der Cache-Statistiken anzuzeigen.

- **Welche Optionen gibt es für die Anzeige des zwischengespeicherten Inhalts?**

  Um den zwischengespeicherten Inhalt anzuzeigen, können Sie den`show cache object` Befehl ausführen.

- **Was ist der Befehl, den ich ausführen kann, um die Eigenschaften eines im Cache gespeicherten Objekts anzuzeigen?**

Wenn das im Cache gespeicherte Objekt beispielsweise GET //10.102.12.16:80/index.html lautet, können Sie die Details zum Objekt anzeigen, indem Sie den folgenden Befehl von der Befehlszeilenschnittstelle der Appliance ausführen:

```
show cache object -url '/index.html'-host 10.102.3.96 -port 80
```

- **Ist es zwingend erforderlich, den Gruppennamen als Parameter anzugeben, um die parametrisierten Objekte im Cache anzuzeigen?**

  Ja. Es ist zwingend erforderlich, den Gruppennamen als Parameter anzugeben, um die parametrisierten Objekte im Cache anzuzeigen. Angenommen, Sie haben die folgenden Richtlinien mit derselben Regel hinzugefügt:

```
1 add cache policy p2 -rule ns_url_path_cgibin -action CACHE -
     storeInGroup g1
2 add cache policy p1 -rule ns_url_path_cgibin -action CACHE -
     storeInGroup g2
3 <!--NeedCopy-->
```

  In diesem Fall wird für die mehrfachen Anforderungen, wenn die Richtlinie p1 ausgewertet wird, ihr Auswahlzähler erhöht, und die Richtlinie speichert das Objekt in der g1-Gruppe, die ausgewählte Parameter enthält. Daher müssen Sie den folgenden Befehl ausführen, um die Objekte aus dem Cache anzuzeigen:

```
show cache object -url ”/cgi-bin/setCookie.pl”-host 10.102.18.152
groupName g1
```

  In ähnlicher Weise wird für einen anderen Satz von mehreren Anforderungen, wenn die Richtlinie p2 ausgewertet wird, ihr Auswahlzähler erhöht und die Richtlinie speichert das Objekt in der Gruppe g2, die keine ausgewählten Parameter hat. Daher müssen Sie den folgenden Befehl ausführen, um die Objekte aus dem Cache anzuzeigen:

```
show cache object -url ”/cgi-bin/setCookie2.pl”-host 10.102.18.152
```

- **Ich stelle fest, dass es einige leere Einträge in der Ausgabe des nscachemgr-Befehls gibt. Was sind das für Einträge?**

  Betrachten Sie die folgende Beispielausgabe des `nscachemgr` Befehls. Die leeren Einträge in dieser Ausgabe werden für Ihre Referenz fett hervorgehoben:

```
1 root@ns# /netscaler/nscachemgr -a
2 //10.102.3.89:80/image8.png
3 //10.102.3.97:80/staticdynamic.html
4 //10.102.3.97:80/
```



```
5   //10.102.3.89:80/image1.png
6   //10.102.3.89:80/file5.html
7   //10.102.3.96:80/
8   //10.102.3.97:80/bg_logo_segue.png
9   //10.102.3.89:80/file500.html
10  //10.102.3.92:80/
11  //10.102.3.96:80/cgi-bin/rfc/ccProxyReval.pl
12  Total URLs in IC = 10
13  <!--NeedCopy-->
```

Die leeren Einträge in der Ausgabe sind auf die Standard-Caching-Eigenschaften für GET/HTTP/1.1 zurückzuführen.

Leeren von Objekten

- **Wie kann ich ein selektives Objekt aus dem Cache leeren?**

  Sie können ein Objekt anhand der vollständigen URL eindeutig identifizieren. Um ein solches Objekt zu leeren, können Sie eine der folgenden Aufgaben ausführen:

  - Cache leeren
  - Inhaltsgruppe leeren
  - Spezifische Objekt leeren

  Um das spezifische Objekt zu leeren, müssen Sie die Abfrageparameter angeben. Sie geben den Parameter InvalParam an, um das Objekt zu leeren. Dieser Parameter gilt nur für eine Abfrage.

- **Löst eine Änderung in der Cachekonfiguration das Löschen des Caches aus?**

  Ja. Wenn Sie zur Cachekonfiguration wechseln, leeren alle SET-Cache-Befehle die entsprechenden Content-Gruppen inhärent.

- **Ich habe die Objekte auf dem Server aktualisiert. Muss ich die zwischengespeicherten Objekte leeren?**

  Ja. Wenn Sie Objekte auf dem Server aktualisieren, müssen Sie die zwischengespeicherten Objekte oder zumindest die relevanten Objekte und Inhaltsgruppen leeren. Der integrierte Cache ist von einem Update auf den Server nicht betroffen. Die zwischengespeicherten Objekte werden weiterhin bedient, bis sie ablaufen.

Flash-Cache

- **Was ist die Flash-Cache-Funktion der Citrix ADC Appliance?**

  Das Phänomen der Flash-Massen tritt auf, wenn viele Kunden auf dieselben Inhalte zugreifen. Das Ergebnis ist ein plötzlicher Anstieg des Datenverkehrs zum Server. Die Flash Cache-

Funktion ermöglicht es der Citrix ADC Appliance, die Leistung in einer solchen Situation zu verbessern, indem sie nur eine Anfrage an den Server sendet. Alle anderen Anfragen werden auf der Appliance in die Warteschlange gestellt, und die einzelne Antwort wird auf die Anfragen zugestellt. Sie können einen der folgenden Befehle verwenden, um die Funktion Schneller Cache zu aktivieren:

- `add cache contentGroup \<Group_Name> -flashCache YES`
- `set cache contentGroup \<Group_Name> -flashCache YES`

- **Was ist die Grenze für Flash Cache-Clients?**

  Die Anzahl der Flash Cache-Clients hängt von der Verfügbarkeit der Ressourcen auf der Citrix ADC Appliance ab.

Standard-Verhalten

- **Empfangen die Citrix ADC Appliance nach Ablauf proaktiv Objekte?**

  Die Citrix ADC Appliance empfängt niemals proaktiv Objekte nach Ablauf. Dies gilt auch für die negativen Objekte. Der erste Zugriff nach Ablauf löst eine Anforderung an den Server aus.

- **Fügt der integrierte Cache Clients zur Warteschlange hinzu, bevor er die Antwort erhält?**

  Ja. Der integrierte Cache fügt Clients zur Warteschlange hinzu, um sie zu bedienen, noch bevor die Antwort empfangen wird.

- **Was ist der Standardwert für das zwischengespeicherte Objekt überprüfen mit dem Parameter der Cachekonfiguration?**

  HOSTNAME_AND_IP ist der Standardwert.

- **Erstellt die Citrix ADC Appliance Protokolleinträge in den Protokolldateien?**

  Ja. Die Citrix ADC Appliance erstellt Protokolleinträge in den Protokolldateien.

- **Werden komprimierte Objekte im Cache gespeichert?**

  Ja. Komprimierte Objekte werden im Cache gespeichert.

Interoperabilität mit anderen Funktionen

- **Was passiert mit Objekten, die derzeit im Cache gespeichert sind und auf die über SSL VPN zugegriffen wird?**

  Objekte, die im Cache gespeichert sind und auf die regelmäßig zugegriffen werden, werden als Cache bereitgestellt, wenn Sie über das SSL-VPN aufgerufen werden.

- **Was passiert mit Objekten, die im Cache gespeichert sind, wenn über SSL VPN zugegriffen und später über eine reguläre Verbindung zugegriffen wird?**

Die über den SSL-VPN-Zugriff gespeicherten Objekte werden als Auswahl dienen, wenn über die reguläre Verbindung zugegriffen wird.

- **Wie unterscheide ich bei der Verwendung von Weblogs Einträge, die auf eine vom Cache bereitgehaltene Antwort hinweisen, von denen, die vom Server bedient werden?**

  Bei Antworten, die aus dem integrierten Cache bereitgestellt werden, enthält das Serverprotokollfeld den Wert IC. Bei Antworten, die von einem Server bereitgestellt werden, enthält das Serverprotokollfeld den vom Server gesendeten Wert. Es folgt ein Beispielprotokolleintrag für eine integrierte Caching-Transaktion:

  ```
  ”10.102.1.52 - ”Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 4.0; .NET
   CLR 1.0.3705)””GET /”200 0 ”IC”10.102.1.45”
  ```

  Zusammen mit einer Clientanforderung ist die protokollierte Antwort diejenige, die an den Client gesendet wird und nicht notwendigerweise die vom Server gesendete Antwort.

> **Hinweis:**
>
> Bei Verwendung der Webprotokollierung enthalten die Antworten aus dem integrierten Cache den Wert-IC im Feld Serverprotokoll. Das Feld für das Serverprotokoll befindet sich im NSWL-Client mit dem Formatbezeichner “%o1”.

Sonstiges

- **Was meinst du mit relexpiry und absexpiry?**

  Durch die Konfiguration `relexpiry` und bedeutet dies `absexpiry`, dass Sie den Header unabhängig davon, was in der Kopfzeile angezeigt wird, überschreiben. Sie können eine andere Ablaufeinstellung und die Ebene der Inhaltsgruppe konfigurieren. Mit `relexpiry`basiert der Ablauf des Headers auf dem Zeitpunkt, zu dem das Objekt vom Citrix ADC empfangen wird. Mit basiert der Ablauf auf der Zeit `absexpiry`, die auf dem Citrix ADC konfiguriert ist. `Relexpiry` ist in Sekundenschnelle konfiguriert. `Absexpiry` ist eine Tageszeit.

- **Was meinen Sie mit der Konfiguration von weakpos und heuristisch?**

  Die `weakpos` und Heuristik sind wie Fallback-Werte. Wenn es einen Ablauf-Header gibt, wird es nur berücksichtigt, wenn der zuletzt geänderte Header vorhanden ist. Die Citrix ADC Appliance legt den Ablauf basierend auf dem zuletzt geänderten Header und dem heuristischen Parameter fest. Die heuristische Ablaufberechnung bestimmt die Ablaufzeit, indem der zuletzt geänderte Header überprüft wird. Ein gewisser Prozentsatz der Dauer seit der letzten Änderung des Objekts wird als Ablaufzeit verwendet. Die Heuristik eines Objekts, das über längere Zeiträume unverändert bleibt und wahrscheinlich längere Verfallszeiten aufweisen wird. –heurExpiryParam gibt an, welchen Prozentwert in dieser Berechnung verwendet werden soll. Andernfalls verwendet die Appliance den `weakpos` Wert.

- **Was sollte ich beachten, bevor ich das dynamische Caching konfigurieren?**

  Wenn ein Parameter in Name-Wert-Form vorhanden ist und nicht über die vollständige URL-Abfrage verfügt oder die Appliance den Parameter in einem Cookie-Header oder POST-Body empfängt, sollten Sie das dynamische Caching konfigurieren. Um dynamisches Caching zu konfigurieren, müssen Sie den HitParams-Parameter konfigurieren.

- **Wie wird die hexadezimale Kodierung in den Parameternamen unterstützt?**

  Auf der Citrix ADC Appliance wird die %HEXHEX-Codierung in den Parameternamen unterstützt. In den Namen, die Sie für HitParams oder InvalParams angeben, können Sie einen Namen angeben, der in den Namen die Kodierung %HEXHEX enthält. Zum Beispiel sind Name, Name%65 und n%61m%65 gleichwertig.

- **Wie erfolgt die Auswahl eines hitParam-Parameters?**

  Betrachten Sie den folgenden Auszug eines HTTP-Headers für eine POST-Anforderung:

```
POST /data2html.asp?param1=value1&param2=&param3&param4=value4
HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-powerpoint, application/vnd.ms-excel,
application/msword, application/x-shockwave-flash, \*/\*
Referer: http://10.102.3.97/forms.html
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: 10.102.3.97
Content-Length: 153
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDQGQGGRNY=NNLLKDADEENOAFLCCDGFGDMO
S1=This+text+is+only+text%2C+not+more+and+not+less%2C+%0D%0Ajust+
   text+to+be+itself%2C+namely+%22Text%22+to+be+posted+as+text
   +%28what+else...%29&B1=Submit
<!--NeedCopy-->
```

  In der vorherigen Anfrage können Sie S1 und B1, die als Referenz fett hervorgehoben sind, als HitParams verwenden, je nach Ihren Anforderungen. Wenn Sie -matchCookies YES in der ASPSESSIONIDQGQGGRNY Content-Gruppe verwenden, können Sie diese Parameter auch als hitParams verwenden.

- **Was passiert mit den Clients in der Warteschlange, wenn die Antwort nicht zwischengespeichert werden kann?**

Wenn die Antwort nicht cachefähig ist, erhalten alle Clients in der Warteschlange dieselbe Antwort, die der erste Client erhält.

- **Kann ich die PET- und Flash-Cache-Funktionen für dieselbe Content-Gruppe aktivieren?**

  Nein. Sie können PET und Flash Cache nicht in derselben Inhaltsgruppe aktivieren. Der integrierte Cache führt die AutoPet-Funktion für Flash Cache-Inhaltsgruppen nicht aus. Die PET-Funktion stellt sicher, dass der integrierte Cache kein gespeichertes Objekt bereitstellt, ohne den Server zu konsultieren. Sie können PET explizit für eine Content-Gruppe konfigurieren.

- **Wann werden die Protokolleinträge für die Clients in der Warteschlange erstellt?**

  Die Protokolleinträge werden für die Clients in der Warteschlange erstellt, sobald die Appliance den Antwortheader erhält. Die Protokolleinträge werden nur erstellt, wenn der Antwort-Header das Objekt nicht nicht zwischenspeichern lässt.

- **Was ist die Bedeutung der DNS-, HOSTNAME- und HOSTNAME_AND_IP-Werte des zwischengespeicherten Objekts Verify unter Verwendung des Parameters der Cachekonfiguration?**

  Die Bedeutungen sind wie folgt:

  - `set cache parameter -verifyUsing HOSTNAME`

    Der Befehl ignoriert die Ziel-IP-Adresse.

  - `set cache parameter -verifyUsing HOSTNAME_AND_IP`

    Der Befehl stimmt mit der Ziel-IP-Adresse überein.

  - `set cache parameter -verifyUsing DNS`

    Der Befehl verwendet den DNS-Server.

- **Ich habe weakNegRelExpiry auf 600 gesetzt, das ist 10 Minuten. Ich habe bemerkt, dass 404 Antworten nicht zwischengespeichert werden. Was ist der Grund?**

  Dies hängt vollständig von Ihrer Konfiguration ab. Standardmäßig werden 404 Antworten für 10 Minuten zwischengespeichert. Wenn Sie möchten, dass alle 404 Antworten vom Server abgerufen werden, geben Sie an: WeaknegrelexPiry 0. Sie können die —weaknegrelexPIRY auf einen gewünschten Wert einstellen, z. B. höher oder niedriger, um die 404-Antworten entsprechend zwischengespeichert zu bekommen. Wenn Sie —absExpiry für positive Antworten konfiguriert haben, führt dies möglicherweise nicht zu den gewünschten Ergebnissen.

- **Wenn der Benutzer über den Mozilla Firefox-Browser auf die Website zugreift, wird der aktualisierte Inhalt bereitgestellt. Wenn der Benutzer jedoch mithilfe des Microsoft Internet Explorer-Browsers auf die Website zugreift, wird veralteter Inhalt bereitgestellt. Was könnte der Grund sein?**

Der Microsoft Internet Explorer-Browser nimmt möglicherweise den Inhalt aus seinem lokalen Cache anstelle des integrierten Citrix ADC Cache. Der Grund kann sein, dass der Microsoft Internet Explorer-Browser den Ablauf-bezogenen Header in der Antwort nicht berücksichtigt.

Um dieses Problem zu beheben, können Sie den lokalen Cache des Internet Explorers deaktivieren und den Offlineinhalt löschen. Nach dem Löschen der Offlineinhalte muss der Browser den aktualisierten Inhalt anzeigen.

- **Was ist, wenn Hits null sind?**

  Überprüfen Sie, ob die Serverzeit und die NS-Zeit synchronisiert sind. Und das Limit von WeakPosRelexPiry muss den Zeitunterschied zwischen NS und Server wie folgt tragen:

```
root@ns180# date
Tue May 15 18:53:52 IST 2012
<!--NeedCopy-->
```

- **Warum erhalten Richtlinien Treffer, aber nichts wird zwischengespeichert?**

  Stellen Sie sicher, dass dem integrierten Cache Speicher zugewiesen ist und dass die Zuweisung größer als Null ist.

- **Ist es möglich, die Cache-Zähler zu Null?**

  Es gibt keine Befehlszeilen- oder GUI-Option, um die Cache-Zähler auf Null zu setzen, und das Leeren des Caches tut dies auch nicht. Wenn Sie das Feld neu starten, werden diese Leistungsindikatoren automatisch auf Null gesetzt.

Installieren, Aktualisieren und Downgrade

October 5, 2021

Installation und Upgrade

Wie lade ich ein bestimmtes Citrix ADC Release-Build-Paket herunter?

Informationen zum Herunterladen eines bestimmten Citrix ADC Release-Build-Pakets finden Sie unter Herunterladen eines Citrix ADC-Versionspakets.

Wie aktualisiert man die Systemsoftware einer Citrix ADC Appliance?

Informationen zum Upgrade der Systemsoftware einer Citrix ADC Appliance finden Sie unter Upgrade einer eigenständigen Citrix ADC Appliance.

Wo finde ich die Versionshinweise für einen Citrix ADC Release Build?

Das Dokument mit den Versionshinweisen für einen Build mit Citrix ADC Versionen listet Folgendes für den Release-Build auf:

- Verbesserungen
- Behobene Probleme
- Bekannte Probleme

Das Dokument mit den Versionshinweisen für einen Citrix ADC Release-Build befindet sich an folgenden Speicherorten:

- Citrix ADC Firmware oder virtuelle Appliance lädt die Seite eines bestimmten Release-Builds herunter.
- Seite "Citrix ADC Versionshinweise" auf der Citrix Docs-Site

Wo finde ich Sicherheitsupdates für Citrix ADC Appliances?

Das Citrix Sicherheitsteam veröffentlicht regelmäßig Sicherheitsbulletins zu Common Vulnerabilities and Exposures (CVE) für alle zugehörigen Citrix Produkte. Diese Informationen finden Sie im Citrix Sicherheitsbulletin. Alternativ können Sie auf der Citrix Support-Sitenach einem bestimmten CVE suchen.

Was ist die Verwendung der zebos.conf-Datei, die in einer Citrix ADC Version verfügbar ist?

Eine Citrix ADC Appliance verwendet ZeBOS als Routing-Suite. Die in einem Citrix ADC Release verfügbare Datei zebos.conf ist die Konfigurationsdatei für ZeBOS.

Ich möchte den SSH-Port (22) der Citrix ADC Appliance in einen anderen Port ändern. Ist es möglich, den SSH-Port der Appliance zu ändern?

Ja. Sie können den SSH-Port der Citrix ADC Appliance ändern, indem Sie die Datei sshd_config im Verzeichnis /nsconfig bearbeiten. Wenn die Datei nicht im Verzeichnis /nsconfig vorhanden ist, kopieren Sie sie aus dem Verzeichnis /etc.

Bearbeiten Sie in der Datei sshd_config den Eintrag für Port 22 in Port <Number>, wobei <Number> die Zielportnummer ist. Wenn Sie die Appliance nicht neu starten und die Änderungen wirksam machen möchten, beenden Sie den `sshd` Prozess mit dem Befehl kill, und starten Sie den Prozess dann neu.

Das Flash-Verzeichnis fehlt in der Citrix ADC Appliance. Welches Verfahren muss ich befolgen, um das Flash-Verzeichnis zu mounten?

Gehen Sie folgendermaßen vor, um das Flash-Verzeichnis einzuhängen:

1. Starten Sie die Citrix ADC Appliance im Einzelbenutzermodus.

   Wenn die Appliance gestartet wird, wird die folgende Meldung angezeigt:

   Wählen Sie [Enter], um sofort zu booten, oder eine andere Taste für die Eingabeaufforderung. [Kernel] wird in 10 Sekunden gebootet…" Wählen Sie Leerzeichen aus und Sie müssen die folgende Aufforderung sehen:

   Geben Sie '?' ein für eine Liste von Befehlen, 'help' für detailliertere Hilfe.

2. Geben Sie den folgenden Befehl ein, um FreeBSD im Einzelbenutzermodus zu starten:

   boot –s

   Nach dem Start der Appliance wird die folgende Meldung angezeigt:

   Geben Sie den vollständigen Pfadnamen der Shell oder RETURN für /bin/sh ein:

3. Drücken Sie die Eingabetaste, um die Eingabeaufforderung # anzuzeigen.
4. Führen Sie den folgenden Befehl aus, um das Flash-Verzeichnis zu mounten:

```
mount /dev/ad0s1a /flash

Note: If the preceding command displays an error message about
   permissions, run the following command to check the disk for
   consistency:

fsck /dev/ad0s1a

Run the mount command again to mount the flash directory.
```

5. Starten Sie die Appliance neu.
6. Führen Sie an der Shell-Eingabeaufforderung den folgenden Befehl aus, um zu überprüfen, ob das Flash-Verzeichnis bereitgestellt ist:

```
df -kh
```

Ich möchte mich bei der Citrix ADC Appliance anmelden, ohne das Kennwort einzugeben. Ist es möglich, SSH auf der Appliance so zu konfigurieren?

Ja. Sie können SSH auf der Citrix ADC Appliance so konfigurieren, dass sie sich ohne Kennwort anmelden. Sie müssen jedoch Ihren Benutzernamen angeben. Gehen Sie folgendermaßen vor, um SSH für die Anmeldung ohne Kennwort zu konfigurieren:

1. Führen Sie den folgenden Befehl aus, um die öffentlichen und privaten Schlüssel zu generieren:

```
\# ssh-keygen -t rsa
```

2. Führen Sie den folgenden Befehl aus, um die Datei id_rsa.pub in das Verzeichnis .ssh des Remotehosts zu kopieren, an dem Sie sich anmelden möchten:

```
\# scp id_dsa.pub \<user>@\<remote_host>/.ssh/id_dsa.pub
```

3. Melden Sie sich beim Remotehost an.
4. Wechseln Sie in das Verzeichnis .ssh.
5. Führen Sie die folgenden Befehle aus, um den öffentlichen Schlüssel des Clients zu den bekannten öffentlichen Schlüsseln hinzuzufügen:

```
\# cat id_dsa.pub >> authorized_keys2

\# chmod 640 authorized_keys2

\# rm id_dsa.pub
```

Wie wird das BIOS der Citrix ADC Appliance zurückgesetzt? Unter welchen Umständen muss ich das BIOS zurücksetzen?

Führen Sie das folgende Verfahren aus, um das BIOS der Citrix ADC Appliance zurückzusetzen:

1. Verbinden Sie die Appliance über den seriellen Port.
2. Starten Sie die Appliance und drücken Sie Löschen, wenn der Startvorgang beginnt.

   Durch Drücken von Löschen während des POST-Prozesses werden die BIOS-Einstellungen der Appliance angezeigt.
3. Aktivieren Sie die Seite Beenden der BIOS-Einstellungen.
4. Wählen Sie die Option Optimale Standardwerte laden. Das Meldungsfeld Optimale Einstellungen laden wird angezeigt.
5. Wählen Sie OK.
6. Nehmen Sie die folgenden Änderungen an den BIOS-Einstellungen auf den verschiedenen Registerkarten vor:

Tabulatortaste

7. Aktivieren Sie die Seite Beenden der BIOS-Einstellungen.
8. Wählen Sie Änderungen speichern und Beenden aus.
9. Wählen Sie zur Bestätigung OK aus.
10. Stellen Sie sicher, dass die Appliance sauber gestartet wird und die serielle Konsole nach dem Start der Appliance die Ausgabe anzeigt.

    Sie müssen das BIOS zurücksetzen, wenn die serielle Konsole nicht reagiert. Dies geschieht normalerweise, nachdem Sie die Appliance aktualisiert haben und die serielle Konsole deaktiviert ist. Sie können jedoch weiterhin auf die Appliance zugreifen, indem Sie das Dienstprogramm telnet oder SSH verwenden.

Ich muss die Citrix ADC Appliance auf die Werkseinstellungen zurücksetzen. Welches Verfahren muss ich befolgen?

Um die Citrix ADC Appliance auf die Werkseinstellungen zurückzusetzen, müssen Sie zwei Umgebungen zurücksetzen: die Citrix ADC Anwendungsumgebung und die FreeBSD-Basisumgebung.Gehen Sie folgendermaßen vor, um die Citrix ADC Anwendungsumgebung der Appliance auf die Werkseinstellungen zurückzusetzen:

1. Erstellen Sie ein Backup der /nsconfig/ns.conf der Appliance.
2. Löschen Sie die Datei /nsconfig/ns.conf.
3. Starten Sie die Appliance neu. Um die FreeBSD-Umgebung der Appliance auf die Werkseinstellungen zurückzusetzen, gehen Sie wie folgt vor:
    a) Installieren Sie ein neues Citrix ADC Codeabbild auf der Appliance. Dies überschreibt mehrere Konfigurationsdateien auf FreeBSD-Ebene mit Standardwerten.
    b) Löschen Sie alle Benutzer und Gruppen, die der Appliance hinzugefügt werden, d. h. alle mit Ausnahme der Standardbenutzer.
    c) Löschen Sie die Datei /etc/resolv.conf.
    d) Löschen Sie die Einträge, die Sie der Datei /etc/hosts hinzugefügt haben.
    e) Wenn die Datei /etc/rc.netscaler vorhanden ist, löschen Sie sie.
    f) Öffnen Sie die Datei /etc/nsperm_group_suser und stellen Sie sicher, dass alle IOCTL-Einträge Kommentareinträge sind.
    g) Öffnen Sie die Datei /etc/rc.conf und stellen Sie sicher, dass der Eintrag syslogd_enable=No nicht in syslogd_enable=yes geändert wird.
    h) Öffnen Sie die Datei /etc/syslog.conf und stellen Sie sicher, dass keine zusätzlichen Einträge in der Datei vorhanden sind.
    i) Löschen Sie den Inhalt der Dateien /var/nslog, /var/nstrace und /var/crash.
    j) Wenn der syslog-Prozess auf der Appliance aktiviert ist und die Appliance Protokolldateien lokal erstellt, löschen Sie den Inhalt der Protokolldateien, die in der Datei /etc/syslog.conf

aufgeführt sind. Die Dateien werden im Verzeichnis /var/log erstellt. Wenn der Syslog-Prozess beispielsweise Systemereignisse in die Datei /var/log/events schreibt und `sslvpn` auf Ereignisse auf die /var/log/sslvpnevents-Datei zugreift, löschen Sie diese Dateien.

Die Appliance zeigt eine Meldung ähnlich der Meldung "Jun 21 12:20:18 ns /flash/ns-10.0-47,15: [1/2]dc0: NIC hängt Bedingung #663: TX 10000/10000, RX 0, HF 0" auf der Konsole an. Was ist die Bedeutung dieser Botschaft?

Die Meldung besteht aus folgenden Komponenten (hier als Beispiele dargestellt):

- #663: Anzahl der Fälle, in denen dieser Zustand auf der Appliance aufgetreten ist.
- TX 10000/10000: Anzahl der Pakete, die die Appliance zu übertragen versucht hat, und Anzahl der übertragenen Pakete. Wenn beide Zahlen identisch sind, wie in diesem Beispiel, hat die Netzwerkkarte alle Pakete übertragen, die die Appliance zu übertragen versucht hat.
- RX 0: Anzahl der empfangenen Pakete. In diesem Beispiel wurde kein Paket empfangen.
- HF0: Anzahl der von der Netzwerkkarte gemeldeten Hardwareprobleme. In diesem Beispiel hat die Netzwerkkarte kein Hardwareproblem gemeldet.

Wenn die Appliance keine Pakete empfängt, meldet sie eine Hang-Bedingung, da sie in einem Netzwerk wahrscheinlich keine Pakete erhält. Wenn die Appliance jedoch an die Schnittstelle angeschlossen ist, können Sie diese Fehlermeldung ignorieren.

Nachdem ich die Citrix ADC Version auf der Appliance aktualisiert habe, zeigt die Appliance weiterhin die frühere Release/Build an. Was kann der Grund sein?

Die Appliance zeigt die Softwareversionsnummer aus der Datei /flash/boot/loader.conf an. Wenn der Kernel-Eintrag für die aktuelle Citrix ADC Version in dieser Datei fehlt, zeigt die Appliance die letzte Citrix ADC-Release-Version an, für die der Eintrag verfügbar war.
Führen Sie folgende Schritte aus, um das Problem zu beheben:

1. Stellen Sie sicher, dass die Kerneldatei im Verzeichnis /nsconfig vorhanden ist.
2. Überprüfen Sie die Datei /flash/boot/loader.conf auf einen Eintrag für den Kernel.

   (Sie können davon ausgehen, dass der Eintrag für den Kernel der von Ihnen installierten Release/Build in der Datei fehlt.)
3. Öffnen Sie die Datei loader.conf in einem Texteditor, z. B. im vi-Editor, und aktualisieren Sie den Kernel-Eintrag für das neue Release/build.
4. Speichern und schließen Sie die Datei.
5. Wiederholen Sie Schritt 2 bis Schritt 4 für die Datei /flash/boot/loader.conf.local.
6. Aktualisieren Sie den Eintrag release/build in der Datei ns.conf.
7. Starten Sie die Appliance neu.

Da ich die Citrix ADC Version auf der Appliance aktualisiert habe, zeigt das LCD-Display auf der Vorderseite der Appliance die Out-of Service-Meldung an oder zeigt nichts an. Wie kann ich dieses Problem beheben?

Führen Sie den folgenden Befehl an der Shell-Eingabeaufforderung der Appliance aus:

```
/netscaler/nslcd  - k
```

Ich habe das Citrix ADC Release/Build aktualisiert. Nach dem Upgrade kann die Appliance jedoch nicht gestartet werden. Kann ich die Software der Appliance auf die vorherige Release/Build-Version herabstufen?

Ja. Sie können die Appliance mit der Kernel-Datei kernel.old starten. Wenn Sie die Appliance neu starten, drücken Sie die Taste F1, wenn die Appliance-Konsole die Meldung F1 drücken anzeigt. Geben Sie kernel.old ein und drücken **Sie die Eingabetaste**.

Nach dem Upgrade der Citrix ADC Version auf der Appliance habe ich die Kerneldatei versehentlich aus dem Verzeichnis /flash gelöscht. Daher kann ich die Appliance nicht starten. Gibt es in dieser Situation eine Methode zum Starten der Appliance?

Ja. Sie können die Appliance wie folgt mit der `kernel.GENERIC` Kerneldatei starten:

1. Wenn Sie die Appliance neu starten, drücken Sie die Taste F1, wenn die Appliance-Konsole die Meldung F1 drücken anzeigt.
2. Geben Sie Kernel ein. GENERIC und drücken Sie Enter.
3. Melden Sie sich als Root-Benutzer an.
4. Installieren Sie die Citrix ADC Version neu.
5. Starten Sie die Appliance neu.

Nach dem Upgrade der Appliance-Software kann ich mich nicht bei der Appliance anmelden, und die folgende Meldung wird angezeigt. Ich habe versucht, dieses Problem mit der Kennwortwiederherstellungsprozedur zu beheben, aber ich war nicht erfolgreich. Habe ich etwas falsch gemacht?

```
```
login: nsroot
Password:
connect: No such file or directory
nsnet_connect: No such file or directory
Login incorrect
```

 
```

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

Sie können dieses Problem nicht mit der Kennwortwiederherstellungsprozedur beheben. Citrix ADC Release 12.1 oder höher verwendet das neue Lizenzierungssystem, das auf dem `Imgrd` Daemon basiert und während des Startvorgangs ausgeführt wird. Damit dieser Daemon ordnungsgemäß funktioniert, muss der Hostname der Citrix ADC Appliance, der in der Datei /nsconfig/rc.conf festgelegt ist, von einem Nameserver an die NSIP-Adresse aufgelöst werden. Alternativ können Sie eine hosts-Datei im Verzeichnis /nsconfig erstellen und den <Host_Name> Eintrag 127.0.0.1 in der Datei hinzufügen.

Stellen Sie außerdem sicher, dass Sie die Lizenzdateien in das Verzeichnis /nsconfig/license/ kopiert haben.

Während eines Upgrades eines Hochverfügbarkeitspaares wird wiederholt die folgende Meldung angezeigt. Was kann der Grund sein?

ns sshd[5035]: error: Ungültiger Benutzername oder Kennwort
Diese Fehlermeldung wird angezeigt, wenn die an der Hochverfügbarkeitspaarung beteiligten Appliances entweder eine andere Citrix ADC Version oder einen anderen Build desselben Release haben. Auf den Appliances kann eine andere Version installiert sein, wenn Sie eine Appliance aktualisiert oder heruntergestuft haben, aber nicht die andere Appliance.
Ich möchte die Netzmaske der NSIP-Adresse auf einer Citrix ADC Appliance ändern. Kann ich das tun, ohne einen Ausfall zu verursachen?
Das Ändern der Netzmaske der Citrix ADC IP kann zu einem kurzen Ausfall führen. Stellen Sie sicher, dass Sie die Netzmaske auf der sekundären Appliance ändern und dann die Hochverfügbarkeitspairing unterbrechen. Überprüfen Sie die Funktionalität der Appliance. Wenn alles wie erwartet funktioniert, erstellen Sie die Hochverfügbarkeitspairing neu.
Um die Netzmaske auf der Appliance zu ändern, führen Sie den ‘config ns‘ Befehl an der CLI-Eingabeaufforderung aus und wählen Sie dann die zweite Option im Menü aus.
Ich habe ein High Availability Paar von Citrix ADC Appliances konfiguriert. Nach dem Upgrade der Softwareversion von einer Vorschauversion auf eine endgültige Version stellte ich fest, dass einige der Appliance-Konfigurationen fehlen. Kann ich die verlorenen Konfigurationen abrufen?
Sie können das folgende Verfahren verwenden, um die Konfiguration wiederherzustellen:
1. Melden Sie sich an der Citrix ADC Befehlszeile der primären Appliance an.
2. Führen Sie die folgenden Befehle aus:
save config
shell
\#cp /nsconfig/ns.conf /nsconfig/ns.conf.bkup
The ns.conf.bkup file is a backup for the running configuration.
3. Aktualisieren Sie die Software beider Appliances auf die endgültige Version.

4. Melden Sie sich an der Citrix ADC Befehlszeile der primären Appliance an.
Können die primäre Appliance und die sekundäre Appliance über separate Builds verfügen?
Es wird empfohlen, dieselbe Version und dieselbe Buildnummer sowohl auf der primären als auch auf der sekundären Appliance zu verwenden.
Können beide Appliances in einem High Availability (HA) -Paar gleichzeitig aktualisiert werden?
Nein. Aktualisieren Sie in einem HA-Paar zuerst den sekundären Knoten, und aktualisieren Sie dann den primären Knoten.
Weitere Informationen finden Sie unter [Upgrade eines Hochverfügbarkeitspaares](/de-de/citrix-adc/13/upgrade-downgrade-citrix-adc-appliance/upgrade-downgrade-HA-pair.html).
Unterstützt Citrix Firmware-Upgrades in der Amazon Web Services Cloud?
Ja.
Kann ich die Citrix ADC Instanz unabhängig von der SDX-Version aktualisieren?
Es ist nicht erforderlich, die SDX-Version zu aktualisieren, wenn die Citrix ADC Appliance aktualisiert wird. Einige Funktionen funktionieren jedoch möglicherweise nicht.
Kann ich den FTP-Server verwenden, um die Citrix ADC Appliance zu aktualisieren?
Nein. Sie müssen zuerst die Firmware von der Citrix Download-Site herunterladen, sie auf Ihrem lokalen Computer speichern und dann die Appliance aktualisieren.
unterscheidet sich das Verfahren zum Aktualisieren der Citrix ADC Appliance mit GSLB-Konfigurationen von einem Upgrade einer Appliance, die nicht an GSLB beteiligt ist?
Nein. Das Upgrade-Verfahren ähnelt dem grundlegenden Upgrade-Verfahren. Der einzige Unterschied besteht darin, dass Sie die eigenständigen oder HA-Appliances an verschiedenen Standorten stufenweise aktualisieren können.
Herabstufen
Ich habe eine Citrix ADC Appliance erhalten, auf der die neueste Citrix ADC-Version installiert ist. Ich möchte jedoch die Software-Version herabstufen. Kann ich das tun?
Nein. Wenn Sie versuchen, die Softwareversion herunterzustufen, funktioniert die Appliance möglicherweise nicht wie erwartet, da die Datei ns.conf der späteren Version möglicherweise nicht mit der früheren Version kompatibel ist und die Appliance möglicherweise die Werkseinstellungen wiederherstellt.
Beim Herabstufen der Citrix ADC Version habe ich die Anweisungen befolgt. Die Appliance zeigt jedoch die folgende Meldung an. Wie wird das Rollback-Verfahren auf einer Citrix ADC Appliance durchgeführt?
root@LBCOL03B# ./installns
installns version (10.0-47.7) kernel (ns-10.0-47.7.gz)
Note:
Installation may pause for up to 3 minutes while data is written to the flash.
Caution:
Do not interrupt the installation process.
Doing so may cause the system to become unusable.

Installation will proceed in 5 seconds, CTRL-C to abort
No Valid Citrix ADC Version Detected
root@LBCOL03B#
Das Rollback-Verfahren ähnelt dem grundlegenden Upgrade-Verfahren. Wählen Sie den Ziel-Build aus, zu dem Sie zurücksetzen möchten, und führen Sie das Downgrade durch. Bevor Sie zu einer anderen Version zurückkehren, empfiehlt Citrix, eine Kopie Ihrer aktuellen Konfigurationsdateien zu erstellen. Informationen zum Downgrade von einer Version finden Sie unter [Downgrade einer Citrix ADC Standalone Appliance](/de-de/citrix-adc/13/upgrade-downgrade-citrix-adc-appliance/downgrade-standalone-appliance.html).

Lastausgleich

October 5, 2021

- **Welche verschiedenen Lastausgleichsrichtlinien kann ich auf der Citrix ADC Appliance erstellen?**

  Sie können die folgenden Typen von Lastausgleichsrichtlinien auf der Citrix ADC Appliance erstellen:

  - Geringste Verbindungen
  - Runde Robin
  - Geringste Reaktionszeit
  - Geringste Bandbreite
  - Am wenigsten Pakete
  - URL-Hashing
  - Domänennamen-Hashing
  - Quell-IP-Adress-Hashing
  - Ziel-IP-Adress-Hashing
  - Quell-IP - Ziel-IP-Hashing
  - Zeichen
  - LRTM

- **Kann ich die Sicherheit der Webfarm erreichen, indem ich den Lastausgleich mit der Citrix ADC Appliance implementiere?**

  Ja. Sie können die Sicherheit der Webfarm erreichen, indem Sie den Lastausgleich mit der Citrix ADC Appliance implementieren. Mit der Citrix ADC Appliance können Sie die folgenden Optionen der Lastausgleichsfunktion implementieren:

  - Verstecken von IP-Adressen: Ermöglicht die Installation der tatsächlichen Server, die sich aus Sicherheitsgründen und zur Erhaltung der IP-Adresse im privaten IP-Adressraum

befinden. Dieser Prozess ist für den Endbenutzer transparent, da die Citrix ADC Appliance Anforderungen im Auftrag des Servers akzeptiert. Im Adressenausblendmodus isoliert die Appliance die beiden Netzwerke vollständig. Daher kann ein Client über eine andere VIP auf der Appliance für diesen Dienst auf einen Dienst zugreifen, der im privaten Subnetz ausgeführt wird, z. B. FTP oder einen Telnet-Server.

- Portzuordnung: Ermöglicht, dass die tatsächlichen TCP-Dienste aus Sicherheitsgründen auf nicht standardmäßigen Ports gehostet werden. Dieser Vorgang ist für den Endbenutzer transparent, da die Citrix ADC Appliance Anforderungen im Namen des Servers an die standardmäßige angekündigte IP-Adresse und Portnummer annimmt.

- **Welche Geräte kann ich zum Lastausgleich mit einer Citrix ADC Appliance verwenden?**

  Sie können die folgenden Geräte mit einer Citrix ADC Appliance ausgleichen:

  - Serverfarmen
  - Caches oder Reverse-Proxys
  - Firewall-Geräte
  - Intrusion Detection Systeme
  - SSL-Abladungsgeräte
  - Kompressionsgeräte
  - Content Inspection Server

- **Warum sollte ich die Load Balancing-Funktion für die Website implementieren?**

  Sie können die Funktion Lastenausgleich für die Website implementieren, um folgende Vorteile zu nutzen:

  - Reduzieren Sie die Reaktionszeit: Wenn Sie die Load Balancing-Funktion für die Website implementieren, ist einer der Hauptvorteile, auf die Sie sich in der Ladezeit freuen können. Wenn zwei oder mehr Server die Last des Webdatenverkehrs gemeinsam nutzen, führt jeder Server weniger Datenverkehr aus als ein einzelner Server allein. Dies bedeutet, dass mehr Ressourcen verfügbar sind, um die Client-Anforderungen zu erfüllen. Dies führt zu einer schnelleren Website.
  - Redundanz: Durch das Implementieren der Load Balancing-Funktion wird ein wenig Redundanz geboten. Wenn die Website beispielsweise über drei Server ausgeglichen ist und einer von ihnen überhaupt nicht reagiert, können die anderen beiden weiterhin laufen und die Websitebesucher bemerken keine Ausfallzeiten. Jede Load Balancing-Lösung sendet sofort den Datenverkehr an den Back-End-Server, der nicht verfügbar ist.

- **Warum muss ich die Mac Based Forwarding (MBF) Option für Link Load Balancing (LLB) deaktivieren?**

  - Wenn Sie die MBF-Option aktivieren, berücksichtigt die Citrix ADC Appliance, dass der eingehende Datenverkehr vom Client und der ausgehende Datenverkehr zum selben

Client über denselben Upstream-Router fließt. Die LLB-Funktion erfordert jedoch, dass der beste Pfad für den Rückkehrverkehr gewählt wird.
  - Das Aktivieren der MBF-Option unterbricht diesen Topologieentwurf, indem der ausgehende Datenverkehr über den Router gesendet wird, der den eingehenden Clientdatenverkehr weitergeleitet hat.

- **Welche Persistenztypen sind auf der Citrix ADC Appliance verfügbar?**

  Die Citrix ADC Appliance unterstützt die folgenden Persistenztypen:

  - Quell-IP
  - Cookie-Einsatz
  - SSL-Sitzungs-ID
  - URL passiv
  - Benutzerdefinierte Server-ID
  - Regel
  - DESTIP

Grafische Benutzeroberfläche (GUI)

January 28, 2022

- **Wenn ich Firefox verwende, um zwei Citrix ADC-Konfigurationen zu vergleichen, scheint der Browser einzufrieren?**

  Firefox zeigt schließlich den Unterschied in den Konfigurationen an, aber der Vorgang dauert sehr lange, wenn es mehr als 1000 Unterschiede gibt. Verwenden Sie Chrome für eine schnellere Reaktion.

- **Ich verwende einen MAC Safari-Browser, um einen Citrix ADC zu aktualisieren. Wenn ich im Upgrade-Assistenten auf die Schaltfläche Durchsuchen klicke, um die Build-Datei aus der Appliance auszuwählen, werden im Dialogfeld keine Dateien oder Ordner angezeigt. Wenn ich zurück zum Stammordner navigiere, zeigt das Dialogfeld den Ordner der obersten Ebene an, aber ich kann ihn nicht durchsuchen. Was soll ich tun?**

  Klicken Sie im Safari-Browser auf das Symbol Einstellungen und navigieren Sie zu **Einstellungen > Sicherheit > Website-Einstellungen verwalten > Java**. Ändern Sie den Wert der Einstellung **Beim Besuch anderer Websites** auf Im unsicheren Modus ausführen.

- **Was soll ich tun, bevor ich auf die GUI zugreife?**

  Bevor Sie auf eine neue Version der Citrix ADC-Software zugreifen:

  - Löschen Sie den Browser-Cache einschließlich Cookies.

  - Greifen Sie im Inkognitomodus des Browsers auf die GUI zu.
  - Greifen Sie auf GUI in einem anderen Browser zu.
  - Deaktivieren **Sie die Option Softwarebeschleunigung verwenden** in der Einstellung und starten Sie den Browser neu
  - Zugriff auf **Chrome: Erweiterungen**, löschen **Sie das Feld Aktivieren** und starten Sie den Chrome-Browser neu

- **Welchen Port sollte ich öffnen, um über HTTP oder HTTPS auf GUI zuzugreifen?**

  Im Folgenden werden die Standardportnummern für HTTP- und HTTPS-Verwaltungsdienste (GUI) in den Citrix ADC MPX-, VPX- und CPX-Appliances aufgeführt:

  - Citrix ADC MPX- und VPX-Appliances: 80 (HTTP) und 443 (HTTPS)
  - Citrix ADC CPX-Appliances: 9080 (HTTP) und 9443 (HTTPS)

  Außerdem können Sie Ports für HTTP- und HTTPS-Verwaltungsdienste (GUI) außer Port 80 und 443 konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von HTTP- und HTTPS-Management-Ports.

- **Mit welchen Browsern ist die GUI für verschiedene Betriebssysteme kompatibel?**

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

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

SSL

October 5, 2021

Klicken Sie hier für häufig gestellte Fragen zu SSL.

Authentifizierung, Autorisierung und Auditing des Anwendungsdatenverkehrs

October 5, 2021

Viele Unternehmen beschränken den Website-Zugriff nur auf gültige Benutzer und kontrollieren die für jeden Benutzer zulässige Zugriffsebene. Die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion ermöglicht es einem Standortadministrator, Zugriffskontrollen mit der Citrix ADC Appliance zu verwalten, anstatt diese Steuerelemente für jede Anwendung separat zu verwalten. Die Authentifizierung auf der Appliance ermöglicht auch die Weitergabe dieser Informationen auf allen Websites innerhalb derselben Domäne, die durch die Appliance geschützt sind.

Um Authentifizierung, Autorisierung und Überwachung zu verwenden, müssen Sie virtuelle Authentifizierungsserver so konfigurieren, dass sie den Authentifizierungsprozess und die virtuelle Datenverkehrsverwaltung verarbeiten, um den Datenverkehr zu Webanwendungen zu verarbeiten, die eine Authentifizierung erfordern. Sie konfigurieren Ihr DNS auch so, dass jedem virtuellen Server FQDNs zugewiesen werden. Nach der Konfiguration der virtuellen Server konfigurieren Sie für jeden Benutzer, der sich über die Citrix ADC Appliance authentifiziert, ein Benutzerkonto. Optional erstellen Sie Gruppen und weisen Benutzerkonten Gruppen zu. Nach dem Erstellen von Benutzerkonten und Gruppen konfigurieren Sie Richtlinien, die der Appliance mitteilen, wie Benutzer authentifiziert werden, auf welche Ressourcen Benutzer zugreifen können und wie Benutzersitzungen protokolliert werden. Um die Richtlinien in Kraft zu setzen, binden Sie jede Richtlinie global, an einen bestimmten virtuellen Server oder an die entsprechenden Benutzerkonten oder -gruppen. Nachdem Sie Ihre Richtlinien konfiguriert haben, passen Sie Benutzersitzungen an, indem Sie Sitzungseinstellungen konfigurieren und Ihre Sitzungsrichtlinien an den virtuellen Server für die Datenverkehrsverwaltung binden. Wenn Ihr Intranet Clientzertifikate verwendet, richten Sie schließlich die Clientzertifikatkonfiguration ein.

Um zu verstehen, wie Authentifizierung, Autorisierung und Auditing in einer verteilten Umgebung funktioniert, sollten Sie eine Organisation mit einem Intranet berücksichtigen, auf das ihre Mitarbeiter im Büro, zu Hause und auf Reisen zugreifen. Der Inhalt im Intranet ist vertraulich und erfordert einen sicheren Zugriff. Jeder Benutzer, der auf das Intranet zugreifen möchte, muss über einen gültigen Benutzernamen und ein gültiges Kennwort verfügen. Um diese Anforderungen zu erfüllen, führt der ADC folgende Schritte aus:

- Leitet den Benutzer auf die Anmeldeseite um, wenn der Benutzer auf das Intranet zugreift, ohne sich angemeldet zu haben.
- Sammelt die Anmeldeinformationen des Benutzers, liefert sie an den Authentifizierungsserver und speichert sie in einem Verzeichnis im Cache, auf das über das Lightweight Directory Access Protocol (LDAP) zugegriffen werden kann. Weitere Informationen finden Sie unter Bestimmen von Attributen in Ihrem LDAP-Verzeichnis.

- Überprüft, ob der Benutzer berechtigt ist, auf bestimmte Intranetinhalte zuzugreifen, bevor er die Anforderung des Benutzers an den Anwendungsserver übermittelt.
- Behält ein Sitzungszeitlimit bei, nach dem sich Benutzer erneut authentifizieren müssen, um den Zugriff auf das Intranet wiederherzustellen. (Sie können das Timeout konfigurieren.)
- Protokolliert die Zugriffsberechtigung des Benutzers, einschließlich ungültiger Anmeldeversuche, in einem Überwachungsprotokoll.

Unterstützte Authentifizierungsarten

- Lokal
- LDAP
- RADIUS
- SAML
- TACACS+
- Clientzertifikatauthentifizierung (einschließlich Smartcard-Authentifizierung)
- Web-Site
- Fortgeschrittene Authentifizierung
- Formularbasierte Authentifizierung
- 401-basierte Authentifizierung
- Natives OTP
- Push-Benachrichtigung
- E-Mail OTP
- reCAPTCHA

Citrix Gateway unterstützt auch RSA SecurID, Gemalto Protiva und SafeWord. Sie verwenden einen RADIUS-Server, um diese Authentifizierungstypen zu konfigurieren.

Bevor Sie Authentifizierung, Autorisierung und Auditing konfigurieren, müssen Sie mit der Konfiguration von Load Balancing, Content Switching und SSL auf der Citrix ADC Appliance vertraut sein.

Authentifizierung ohne Autorisierung

Die Autorisierung gibt die Netzwerkressourcen an, auf die Benutzer Zugriff haben, wenn sie sich bei der Appliance anmelden. Die Standardeinstellung für die Autorisierung besteht darin, den Zugriff auf alle Netzwerkressourcen zu verweigern. Citrix empfiehlt, die globale Standardeinstellung zu verwenden und dann Autorisierungsrichtlinien zu erstellen, um die Netzwerkressourcen zu definieren, auf die Benutzer zugreifen können.

Sie konfigurieren die Autorisierung auf der Appliance mithilfe einer Autorisierungsrichtlinie und Ausdrücke. Nachdem Sie eine Autorisierungsrichtlinie erstellt haben, können Sie sie an die Benutzer oder Gruppen binden, die Sie auf der Appliance konfiguriert haben.

Sie können die Appliance so konfigurieren, dass sie nur die Authentifizierung ohne Autorisierung verwendet. Wenn Sie die Authentifizierung ohne Autorisierung konfigurieren, führt die Appliance keine Gruppenautorisierungsprüfung durch. Die Richtlinien, die Sie für den Benutzer oder die Gruppe konfigurieren, werden dem Benutzer zugewiesen.

Aktivieren von Authentifizierung, Autorisierung und Überwachung

Um die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion verwenden zu können, müssen Sie sie aktivieren. Sie können Authentifizierungs-, Autorisierungs- und Auditing-Entitäten wie die virtuellen Server für Authentifizierung und Verkehrsmanagement konfigurieren, bevor Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion aktivieren, aber die Entitäten funktionieren erst, wenn die Funktion aktiviert ist.

So aktivieren Sie Authentifizierung, Autorisierung und Auditing mit der CLI

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

```
1 enable ns feature AAA
2 <!--NeedCopy-->
```

So aktivieren Sie Authentifizierung, Autorisierung und Auditing mit der GUI

1. Navigieren Sie zu **System > Einstellungen**.
2. Klicken Sie im Detailbereich unter **Modi und Features**auf **Grundfunktionen ändern**.
3. Aktivieren Sie im Dialogfeld **Grundfunktionen konfigurieren** das Kontrollkästchen **Authentifizierung, Autorisierung und Überwachung**.
4. Klicken Sie auf **OK**.

Deaktivieren der Authentifizierung

Wenn Ihre Bereitstellung keine Authentifizierung erfordert, können Sie sie deaktivieren. Sie können die Authentifizierung für jeden virtuellen Server deaktivieren, für den keine Authentifizierung erforderlich ist.

> **Wichtig:**
>
> **Wichtig:** Citrix empfiehlt, die Authentifizierung mit Vorsicht zu deaktivieren. Wenn Sie keinen externen Authentifizierungsserver verwenden, erstellen Sie lokale Benutzer und Gruppen, damit die Appliance Benutzer authentifizieren kann. Die Deaktivierung der Authentifizierung

> stoppt die Verwendung von Authentifizierungs-, Autorisierungs- und Buchhaltungsfunktionen, die Verbindungen mit der Appliance steuern und überwachen. Wenn Benutzer eine Webadresse eingeben, um eine Verbindung mit der Appliance herzustellen, wird die Anmeldeseite nicht angezeigt.

So deaktivieren Sie die Authentifizierung

1. Navigieren Sie zu **Konfiguration > Citrix Gateway > Virtuelle Server**.
2. Klicken Sie im Detailbereich auf einen virtuellen Server und dann auf **Öffnen**.
3. Deaktivieren Sie auf der Seite **Grundeinstellungen** das Kontrollkästchen **Authentifizierung aktivieren**.

Funktionsweise von Authentifizierung, Autorisierung und Auditing

October 5, 2021

Authentifizierung, Autorisierung und Überwachung bieten Sicherheit für eine verteilte Internetumgebung, da jedem Client mit den richtigen Anmeldeinformationen eine sichere Verbindung zu geschützten Anwendungsservern von überall im Internet ermöglicht wird. Diese Funktion enthält die drei Sicherheitsfunktionen Authentifizierung, Autorisierung und Überwachung. Mit der Authentifizierung kann Citrix ADC die Anmeldeinformationen des Clients entweder lokal oder mit einem Authentifizierungsserver eines Drittanbieters überprüfen und nur genehmigten Benutzern den Zugriff auf geschützte Server ermöglichen. Autorisierung ermöglicht es dem ADC, zu überprüfen, auf welchen Inhalt auf einem geschützten Server jeder Benutzer zugreifen kann. Die Überwachung ermöglicht es dem ADC, die Aktivitäten jedes Benutzers auf einem geschützten Server aufzuzeichnen.

Um zu verstehen, wie Authentifizierung, Autorisierung und Auditing in einer verteilten Umgebung funktioniert, sollten Sie eine Organisation mit einem Intranet berücksichtigen, auf das ihre Mitarbeiter im Büro, zu Hause und auf Reisen zugreifen. Der Inhalt im Intranet ist vertraulich und erfordert einen sicheren Zugriff. Jeder Benutzer, der auf das Intranet zugreifen möchte, muss über einen gültigen Benutzernamen und ein gültiges Kennwort verfügen. Um diese Anforderungen zu erfüllen, führt der ADC folgende Schritte aus:

- Leitet den Benutzer auf die Anmeldeseite um, wenn der Benutzer auf das Intranet zugreift, ohne sich angemeldet zu haben.
- Sammelt die Anmeldeinformationen des Benutzers, übermittelt sie an den Authentifizierungsserver und speichert sie in einem Verzeichnis, auf das über LDAP zugegriffen werden kann. Weitere Informationen finden Sie unter Bestimmen von Attributen in Ihrem LDAP-Verzeichnis.

- Überprüft, ob der Benutzer berechtigt ist, auf bestimmte Intranetinhalte zuzugreifen, bevor er die Anforderung des Benutzers an den Anwendungsserver übermittelt.
- Behält ein Sitzungszeitlimit bei, nach dem sich Benutzer erneut authentifizieren müssen, um den Zugriff auf das Intranet wiederherzustellen. (Sie können das Timeout konfigurieren.)
- Protokolliert die Zugriffsberechtigung des Benutzers, einschließlich ungültiger Anmeldeversuche, in einem Überwachungsprotokoll.

Konfigurieren von Authentifizierungsautorisierungs- und Überwachungsrichtlinien

Nachdem Sie Ihre Benutzer und Gruppen eingerichtet haben, konfigurieren Sie als Nächstes Authentifizierungsrichtlinien, Autorisierungsrichtlinien und Überwachungsrichtlinien, um festzulegen, welche Benutzer auf Ihr Intranet zugreifen dürfen, auf welche Ressourcen jeder Benutzer oder Gruppe zugreifen darf und welche Detailgenauigkeit Authentifizierung, Autorisierung und Überwachung wird in den Überwachungsprotokollen beibehalten. Eine Authentifizierungsrichtlinie definiert den Typ der Authentifizierung, die angewendet werden soll, wenn ein Benutzer versucht, sich anzumelden. Wenn eine externe Authentifizierung verwendet wird, gibt die Richtlinie auch den externen Authentifizierungsserver an. Autorisierungsrichtlinien geben die Netzwerkressourcen an, auf die Benutzer und Gruppen nach der Anmeldung zugreifen können. Überwachungsrichtlinien definieren den Typ und den Speicherort des Überwachungsprotokolls.

Sie müssen jede Richtlinie binden, um sie in Kraft zu setzen. Sie binden Authentifizierungsrichtlinien an virtuelle Authentifizierungsserver, Autorisierungsrichtlinien an ein oder mehrere Benutzerkonten oder Gruppen und Überwachungsrichtlinien sowohl global als auch an ein oder mehrere Benutzerkonten oder Gruppen.

Wenn Sie eine Richtlinie binden, weisen Sie ihr eine Priorität zu. Die Priorität bestimmt die Reihenfolge, in der die von Ihnen definierten Richtlinien ausgewertet werden. Sie können die Priorität auf eine beliebige positive Ganzzahl festlegen. Im Citrix ADC Betriebssystem funktionieren Richtlinienprioritäten in umgekehrter Reihenfolge: Je höher die Zahl, desto niedriger die Priorität. Wenn Sie beispielsweise drei Richtlinien mit den Prioritäten 10, 100 und 1000 haben, wird zuerst die Richtlinie ausgeführt, die eine Priorität von 10 zugewiesen hat, dann wird die Richtlinie mit einer Priorität von 100 und schließlich der Richtlinie eine Reihenfolge von 1000 zugewiesen. Das Authentifizierungs-, Autorisierungs- und Überwachungsfeature implementiert nur den ersten von jedem Richtlinientyp, dem eine Anforderung entspricht, und keine zusätzlichen Richtlinien dieses Typs, mit denen eine Anforderung auch übereinstimmen könnte. Daher ist die Richtlinienpriorität wichtig, um die gewünschten Ergebnisse zu erhalten.

Sie können sich viel Platz lassen, um andere Richtlinien in beliebiger Reihenfolge hinzuzufügen und sie dennoch in der gewünschten Reihenfolge auszuwerten, indem Sie Prioritäten mit Intervallen von 50 oder 100 zwischen jeder Richtlinie festlegen, wenn Sie die Richtlinien binden. Sie können dann

jederzeit zusätzliche Richtlinien hinzufügen, ohne die Priorität einer vorhandenen Richtlinie neu zuweisen zu müssen.

Weitere Informationen zum Binden von Richtlinien auf der Citrix ADC Appliance finden Sie in der Citrix ADC-Produktdokumentation.

Konfigurieren Sie die Richtlinie “No_Auth”, um bestimmten Datenverkehr zu umgehen

Sie können jetzt No_Auth Richtlinie so konfigurieren, dass bestimmten Datenverkehr von der Authentifizierung umgangen wird, wenn 401-basierte Authentifizierung auf dem virtuellen Server der Datenverkehrsverwaltung aktiviert ist. Für diesen Verkehr müssen Sie eine “No_Auth” -Richtlinie binden.

So konfigurieren Sie die No_Auth Richtlinie, um bestimmten Datenverkehr mit der CLI zu umgehen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

Beispiel:

```
add authentication policy ldap -rule ldapAct1 -action No_Auth
<!--NeedCopy-->
```

Grundkomponenten der Authentifizierungs-, Autorisierungs- und Überwachungskonfiguration

October 5, 2021

Die grundlegenden Komponenten der Authentifizierungs-, Autorisierungs- und Überwachungskonfiguration lauten wie folgt:

- **Virtueller Authentifizierungsserver** - Alle Authentifizierungsanfragen werden vom virtuellen Server der Verkehrsverwaltung (Lastenausgleich oder Content Switching) an den virtuellen Authentifizierungsserver umgeleitet. Dieser virtuelle Server verarbeitet die zugehörigen Authentifizierungsrichtlinien und bietet dementsprechend Zugriff auf die Anwendung. Weitere Informationen finden Sie unter Virtueller Authentifizierungsserver.

- **Authentifizierungsprofile** — Ein Authentifizierungsprofil gibt den virtuellen Authentifizierungsserver, den Authentifizierungshost, die Authentifizierungsdomäne und eine Authentifizierungsebene an.

Sie können ein oder mehrere Authentifizierungsprofile erstellen, um verschiedene Authentifizierungseinstellungen anzugeben und diese Authentifizierungsprofile basierend auf Ihren Anforderungen an relevante Traffic-Management-Server zu binden. Weitere Informationen finden Sie unter Authentifizierungsprofile.

- **Authentifizierungsrichtlinien** - Wenn sich Benutzer bei der Citrix ADC oder Citrix Gateway Appliance anmelden, werden sie gemäß einer von Ihnen erstellten Richtlinie authentifiziert. Eine Authentifizierungsrichtlinie besteht aus einem Ausdruck und einer Aktion. Authentifizierungsrichtlinien verwenden Citrix ADC Ausdrücke. Weitere Informationen finden Sie unter Authentifizierungsrichtlinien.
- **Autorisierungsrichtlinien** - Wenn Sie eine Autorisierungsrichtlinie konfigurieren, können Sie sie so einstellen, dass sie den Zugriff auf Netzwerkressourcen im internen Netzwerk zulässt oder verweigert. Weitere Informationen finden Sie unter Autorisierungsrichtlinien.
- **Benutzer und Gruppen:** - Nachdem Sie die grundlegende Einrichtung für Authentifizierung, Autorisierung und Überwachung konfiguriert haben, erstellen Sie Benutzer und Gruppen. Sie erstellen zunächst ein Benutzerkonto für jede Person, die sich über die Citrix ADC Appliance authentifiziert. Wenn Sie die lokale Authentifizierung verwenden, die von der Citrix ADC Appliance selbst gesteuert wird, erstellen Sie lokale Benutzerkonten und weisen jedem dieser Konten Kennwörter zu. Weitere Informationen finden Sie unter Benutzer und Gruppen.

Virtueller Authentifizierungsserver

October 5, 2021

Der virtuelle Server für die Verkehrsverwaltung (Load Balancing oder Content Switching) leitet alle Authentifizierungsanfragen an den virtuellen Authentifizierungsserver um. Dieser virtuelle Server verarbeitet die zugehörigen Authentifizierungsrichtlinien und bietet dementsprechend Zugriff auf die Anwendung.

Hinweis: Sie können Verkehrsverwaltungsrichtlinien nicht an virtuelle Authentifizierungs-, Autorisierungs- und Überwachungsserver binden.

Einrichten des virtuellen Authentifizierungsservers

Die Schritte zur Einrichtung eines virtuellen Authentifizierungsservers sind:

1. Aktivieren Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion.

```
enable ns feature AAA
<!--NeedCopy-->
```

2. Konfigurieren Sie einen virtuellen Authentifizierungsserver. Es muss vom Typ SSL sein und sicherstellen, dass das SSL-Zertifikatschlüsselpaar an den virtuellen Server gebunden wird.

```
add authentication vserver <name> SSL <ipaddress> <port>

bind ssl certkey <auth-vserver-name> <certkey>
<!--NeedCopy-->
```

3. Geben Sie den FQDN der Domäne für den virtuellen Authentifizierungsserver an.

```
set authentication vserver <name> -authenticationDomain <FQDN>
<!--NeedCopy-->
```

4. Ordnen Sie den virtuellen Authentifizierungsserver dem relevanten virtuellen Server zur Datenverkehrsverwaltung zu.

   Punkte zu beachten:

   - Der FQDN des virtuellen Servers zur Datenverkehrsverwaltung muss sich in derselben Domäne wie der FQDN des virtuellen Authentifizierungsservers befinden, damit das Domänensitzungscookie ordnungsgemäß funktioniert. Auf dem virtuellen Server für die Datenverkehrsverwaltung:
     - Authentifizierung aktivieren.
     - Geben Sie den FQDN des virtuellen Authentifizierungsservers als Authentifizierungshost des virtuellen Servers für die Datenverkehrsverwaltung an.
     - [Optional] Geben Sie die Authentifizierungsdomäne auf dem virtuellen Datenverkehrsverwaltungsserver an.
     - Wenn Sie die Authentifizierungsdomäne nicht konfigurieren, weist die Appliance einen FQDN zu, der aus dem FQDN des virtuellen Authentifizierungsservers ohne den Teil des Hostnamens besteht. Wenn der Domänenname des virtuellen Authentifizierungsservers beispielsweise **tm.xyz.bar.com**lautet, weist die Appliance **xyz.bar.com** als Authentifizierungsdomäne zu.
       * Für Lastausgleich:


```
set lb vserver <name> -authentication ON -
    authenticationhost <FQDN> [-authenticationdomain <
    authdomain>]
<!--NeedCopy-->
```

* Für Content Switching:

```
set cs vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

- Wenn Sie ein domänenbreites Cookie für eine Authentifizierungsdomäne festlegen müssen, müssen Sie das Authentifizierungsprofil auf einem virtuellen Lastenausgleichsserver aktivieren.

5. Stellen Sie sicher, dass beide virtuellen Server UP sind und ordnungsgemäß konfiguriert sind.

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

So richten Sie einen virtuellen Authentifizierungsserver mit der GUI ein

1. Aktivieren Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion.

   Navigieren Sie zu **System > Einstellungen**, klicken Sie auf **Basisfunktionen konfigurieren**, und aktivieren Sie **Authentifizierung, Autorisierung und Überwachung**.

2. Konfigurieren Sie den virtuellen Authentifizierungsserver.

   Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Virtuelle Server**und konfigurieren Sie sie nach Bedarf.

3. Konfigurieren Sie den virtuellen Server für die Datenverkehrsverwaltung für die Authentifizierung.

   - **Für Lastausgleich:**

     Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und konfigurieren Sie den virtuellen Server nach Bedarf.

   - **Für Content Switching:**

     Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und konfigurieren Sie den virtuellen Server nach Bedarf.

4. • Überprüfen Sie das Authentifizierungs-Setup.

   Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Virtuelle Server**, und überprüfen Sie die Details des relevanten virtuellen Authentifizierungsservers.

Konfigurieren Sie den virtuellen Authentifizierungsserver

Um Authentifizierung, Autorisierung und Überwachung zu konfigurieren, konfigurieren Sie zunächst einen virtuellen Authentifizierungsserver für die Verarbeitung des Authentifizierungsdatenverkehrs. Binden Sie als Nächstes ein SSL-Zertifikatschlüsselpaar an den virtuellen Server, damit es SSL-Verbindungen verarbeiten kann.
Weitere Informationen zum Konfigurieren von SSL und zum Erstellen eines Zertifikatschlüsselpaars finden Sie unter SSL-Zertifikate.

Konfigurieren eines virtuellen Authentifizierungsservers mit der CLI

Um einen virtuellen Authentifizierungsserver zu konfigurieren und die Konfiguration zu überprüfen, geben Sie an der Eingabeaufforderung die folgenden Befehle in der gleichen Reihenfolge ein:

```
dd authentication vserver <name> ssl <ipaddress>

show authentication vserver <name>

bind ssl certkey <certkeyName>

show authentication vserver <name>

set authentication vserver <name>

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

Beispiel:

```
add authentication vserver Auth-Vserver-2 SSL 10.102.29.77 443 Done

show authentication vserver Auth-Vserver-2 Auth-Vserver-2
    (10.102.29.77:443) - SSL Type: CONTENT State: DOWN[Certkey not bound
    ] Client Idle Timeout: 180 sec Down state flush: DISABLED Disable
    Primary Vserver On Down : DISABLED Authentication : ON Current AAA
    Users: 0 Done
```



```
4
5 bind ssl certkey Auth-Vserver-2 Auth-Cert-1 Done
6
7 show authentication vserver Auth-Vserver-2 Auth-Vserver-2
    (10.102.29.77:443) - SSL Type: CONTENT State: UP Client Idle Timeout
    : 180 sec Down state flush: DISABLED Disable Primary Vserver On Down
     : DISABLED Authentication : ON Current AAA Users: 0 Done
8
9 show authentication vserver Auth-Vserver-2 Auth-Vserver-2
    (10.102.29.77:443) - SSL Type: CONTENT State: DOWN[Certkey not bound
    ] Client Idle Timeout: 180 sec Down state flush: DISABLED Disable
    Primary Vserver On Down : DISABLED Authentication : ON Current AAA
    Users: 0 Done
10 <!--NeedCopy-->
```

> **Hinweis:**
>
> Der Parameter Authentifizierungsdomäne ist veraltet. Verwenden Sie das Authentifizierungsprofil zum Setzen von domänenweiten Cookies.

Konfigurieren eines virtuellen Authentifizierungsservers mit der GUI

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Virtuelle Server**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Klicken Sie auf **Hinzufügen**, um einen neuen virtuellen Authentifizierungsserver zu erstellen.
   - Um einen vorhandenen virtuellen Authentifizierungsserver zu ändern, wählen Sie den virtuellen Server aus, und klicken Sie dann auf **Bearbeiten**. Das Dialogfeld Konfiguration wird geöffnet und der Bereich Grundeinstellungen erweitert.
3. Geben Sie die Werte für die Parameter wie folgt an (Sternchen gibt einen erforderlichen Parameter an):
   - Name* — Name (Kann nicht für einen zuvor erstellten virtuellen Server geändert werden)
   - IP Address Type* — IP-Adresstyp des virtuellen Authentifizierungsservers
   - IP-Adresse*— IP-Adresse des virtuellen Authentifizierungsservers
   - Port* — TCP-Port, auf dem der virtuelle Server Verbindungen akzeptiert.
   - Timeout für fehlgeschlagene Anmeldung — failedLoginTimeout (Sekunden zulässig, bevor die Anmeldung fehlschlägt und der Benutzer den Anmeldeprozess erneut starten muss.)
   - Max. Anmeldeversuche — maxLoginAttempts (Anzahl der erlaubten Anmeldeversuche, bevor der Benutzer gesperrt wird)

> **Hinweis:**
>
> Der virtuelle Authentifizierungsserver verwendet nur das SSL-Protokoll und den Port 443, sodass diese Optionen ausgegraut sind. Alle Optionen, die nicht erwähnt werden, können ignoriert werden.

4. Klicken Sie auf **Weiter**, um den Bereich Zertifikate anzuzeigen.
5. Konfigurieren Sie im Bereich **Zertifikate** alle SSL-Zertifikate, die Sie mit diesem virtuellen Server verwenden möchten.
    - Um ein Zertifizierungsstellenzertifikat zu konfigurieren, klicken Sie auf den Pfeil rechts neben Zertifizierungsstellenzertifikat, um das Dialogfeld Zertifizierungsstellenschlüssel anzuzeigen, wählen Sie das Zertifikat aus, das Sie an diesen virtuellen Server binden möchten, und klicken Sie auf **Speichern**.
    - Um ein Serverzertifikat zu konfigurieren, klicken Sie auf den Pfeil rechts von Serverzertifikat und folgen Sie demselben Prozess wie für das CA-Zertifikat.
6. Klicken Sie auf **Weiter**, um den Bereich **Erweiterte Authentifizierungsrichtlinien** anzuzeigen.
7. Wenn Sie eine erweiterte Authentifizierungsrichtlinie an den virtuellen Server binden möchten, klicken Sie auf den Pfeil rechts neben der Zeile, um das Dialogfeld **Authentifizierungsrichtlinie** anzuzeigen, wählen Sie die Richtlinie aus, die Sie an den Server binden möchten, legen Sie die Priorität fest, und klicken Sie dann auf **OK** .
8. Klicken Sie auf **Weiter**, um den Bereich **Grundauthentifizierungsrichtlinien** anzuzeigen.
9. Wenn Sie eine grundlegende Authentifizierungsrichtlinie erstellen und an den virtuellen Server binden möchten, klicken Sie auf das Pluszeichen, um das Dialogfeld **Richtlinien** anzuzeigen, und folgen Sie den Anweisungen, um die Richtlinie zu konfigurieren und sie an diesen virtuellen Server zu binden.
10. Klicken Sie auf **Weiter**, um den Bereich 401-basierte virtuelle Server anzuzeigen.
11. Konfigurieren Sie im Bereich für 401-basierte virtuelle Server alle virtuellen Lastausgleichs- oder Content Switching-Server, die Sie an diesen virtuellen Server binden möchten.
    - Um einen virtuellen Lastausgleichsserver zu binden, klicken Sie auf den Pfeil rechts neben dem virtuellen Lastausgleichsserver, um das Dialogfeld “Virtuelle Server für Lastenausgleich anzuzeigen, und befolgen Sie die Anweisungen.
    - Um einen virtuellen Content Switching-Server zu binden, klicken Sie auf den Pfeil rechts neben dem virtuellen Content Switching-Server, um das Dialogfeld “Content Switching Virtual Servers” anzuzeigen, und folgen Sie demselben Prozess wie das Binden eines virtuellen LB-Servers.
12. Wenn Sie eine Gruppe erstellen oder konfigurieren möchten, klicken Sie im Bereich Gruppen auf den Pfeil, um das Dialogfeld Gruppen anzuzeigen, und folgen Sie den Anweisungen.

13. Überprüfen Sie Ihre Einstellungen, und klicken Sie auf **Fertig**. Das Dialogfeld wird geschlossen. Wenn Sie einen neuen virtuellen Authentifizierungsserver erstellt haben, wird er nun in der Liste des **Konfigurationsfensters** angezeigt.

Virtueller Server für die Verkehrsverwaltung

Nachdem Sie Ihren virtuellen Authentifizierungsserver erstellt und konfiguriert haben, erstellen oder konfigurieren Sie als Nächstes einen virtuellen Server für die Verkehrsverwaltung und ordnen Ihren virtuellen Authentifizierungsserver damit zu. Sie können entweder einen virtuellen Lastausgleichs- oder Content Switching-Server für einen virtuellen Server zur Datenverkehrsverwaltung verwenden. Weitere Informationen zum Erstellen und Konfigurieren eines virtuellen Servers finden Sie im *Citrix Traffic Management Guide* bei Traffic Management.

> **Hinweis:**
>
> Der FQDN des virtuellen Servers für die Verkehrsverwaltung muss sich in derselben Domäne wie der FQDN des virtuellen Authentifizierungsservers befinden, damit das Cookie für die Domänensitzung ordnungsgemäß funktioniert.

Sie konfigurieren einen virtuellen Server für die Datenverkehrsverwaltung für die Authentifizierung, Autorisierung und Überwachung, indem Sie die Authentifizierung aktivieren und dann den FQDN des Authentifizierungsservers dem virtuellen Server für die Datenverkehrsverwaltung zuweisen. Sie können die Authentifizierungsdomäne derzeit auch auf dem virtuellen Server für die Verkehrsverwaltung konfigurieren. Wenn Sie diese Option nicht konfigurieren, weist die Citrix ADC Appliance dem virtuellen Server der Verkehrsverwaltung einen FQDN zu, der aus dem FQDN des virtuellen Authentifizierungsservers ohne den Teil des Host-Namens besteht. Wenn der Domänenname des virtuellen Authentifizierungsservers beispielsweise tm.xyz.bar.com lautet, weist die Appliance xyz.bar.com. als Authentifizierungsdomäne zu.

So konfigurieren Sie einen virtuellen Server für die Verkehrsverwaltung mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehlssätze ein:

```
1 set lb vserver <name>  -authentication ON -authenticationhost <FQDN> [-
     authenticationdomain <authdomain>]
2 show lb vserver <name>
3 set cs vserver <name>  -authentication ON -authenticationhost <FQDN> [-
     authenticationdomain <authdomain>]
4 show cs vserver <name>
5 <!--NeedCopy-->
```


Beispiel:

```
set lb vserver vs-cont-sw -Authentication ON -AuthenticationHost mywiki
    .index.com Done

show lb vserver vs-cont-sw vs-cont-sw (0.0.0.0:0) - TCP Type: ADDRESS
    State: DOWN Last state change was at Wed Aug 19 10:03:15 2009 (+410
    ms) Time since last state change: 5 days, 20:00:40.290 Effective
    State: DOWN Client Idle Timeout: 9000 sec Down state flush: ENABLED
    Disable Primary Vserver On Down : DISABLED No. of Bound Services : 0
     (Total) 0 (Active) Configured Method: LEASTCONNECTION Mode: IP
    Persistence: NONE Connection Failover: DISABLED Authentication: ON
    Host: mywiki.index.com
Done
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Server für die Verkehrsverwaltung mit der GUI

1. Führen Sie im Navigationsbereich eine der folgenden Aktionen aus.
   - Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
   - Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**
   - Wählen Sie im Detailbereich den virtuellen Server aus, auf dem Sie die Authentifizierung aktivieren möchten, und klicken Sie dann auf **Bearbeiten**.
   - Geben Sie im Textfeld Domäne die Authentifizierungsdomäne ein.
   - Wählen Sie im Menü **Erweitert** auf der rechten Seite die Option **Authentifizierung** aus.
   - Wählen Sie entweder **formularbasierte Authentifizierung** oder **401 Based Authentication**, und geben Sie die Authentifizierungsinformationen ein.
     - Geben Sie für Formularbasierte Authentifizierung den Authentifizierungs-FQDN (den vollqualifizierten Domänennamen des Authentifizierungsservers), den virtuellen Authentifizierungsserver (die IP-Adresse des virtuellen Authentifizierungsservers) und das Authentifizierungsprofil (das für die Authentifizierung zu verwendende Profil) ein.
     - Geben Sie für 401 Based Authentication nur den virtuellen Authentifizierungsserver und das Authentifizierungsprofil ein.
   - Klicken Sie auf **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass der virtuelle Server erfolgreich konfiguriert wurde.

Vereinfachte Login-Protokollunterstützung für Authentifizierung, Autorisierung und Überwachung

Das Login-Protokoll zwischen Authentifizierung, Autorisierung und Überwachung der Datenverkehrsverwaltung virtuellen Servern und Authentifizierung, Autorisierung und Überwachung virtueller Server wird vereinfacht, um interne Mechanismen zu verwenden, anstatt die verschlüsselten Daten über Abfrageparameter zu senden. Mit dieser Funktion wird die Wiederholung von Anfragen verhindert.

Konfigurieren von DNS

Damit das im Authentifizierungsprozess verwendete Domänensitzungscookie ordnungsgemäß funktioniert, müssen Sie DNS so konfigurieren, dass sowohl die Authentifizierungs- als auch die virtuellen Server für die Verkehrsverwaltung FQDNs in derselben Domäne zugewiesen werden. Informationen zum Konfigurieren von DNS-Adressdatensätzen finden Sie unter Domänennamensystem.

Überprüfen der Authentifizierung virtueller Server

Nachdem Sie die virtuellen Server für die Authentifizierung und Verkehrsverwaltung konfiguriert haben und bevor Sie Benutzerkonten erstellen, müssen Sie sicherstellen, dass beide virtuellen Server korrekt konfiguriert sind und sich im Status UP befinden.

Konfigurieren einer NoAuth-Authentifizierung mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

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

Beispiel:

```
show authentication vserver Auth-Vserver-2
Auth-Vserver-2 (10.102.29.77:443) - SSL Type: CONTENT
State: UP
Client Idle Timeout: 180 sec
Down state flush: DISABLED
Disable Primary Vserver On Down : DISABLED
Authentication : ON
Current AAA Users: 0
Authentication Domain: myCompany.employee.com
```



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

Konfigurieren einer NoAuth- Authentifizierung mit der GUI

1. Navigieren Sie zu **Sicherheit > Citrix ADC AAA - Anwendungsdatenverkehr > Virtuelle Server**. Hinweis: Navigieren Sie von Citrix Gateway zu **Citrix Gateway > Virtual Servers**.
2. Überprüfen Sie die Informationen im Bereich **Virtuelle AAA-Server**, um zu überprüfen, ob Ihre Konfiguration korrekt ist und Ihr virtueller Authentifizierungsserver Datenverkehr akzeptiert. Sie können einen bestimmten virtuellen Server auswählen, um detaillierte Informationen im Detailbereich anzuzeigen.

Autorisierungsrichtlinien

October 5, 2021

Wenn Sie eine Autorisierungsrichtlinie konfigurieren, können Sie sie so einstellen, dass der Zugriff auf Netzwerkressourcen im internen Netzwerk zugelassen oder verweigert wird. Um Benutzern beispielsweise den Zugriff auf das 10.3.3.0-Netzwerk zu ermöglichen, verwenden Sie den folgenden Ausdruck:

CLIENT.IP.DST.IN_SUBNET(10.3.0.0/16)

Autorisierungsrichtlinien werden auf Benutzer und Gruppen angewendet. Nachdem ein Benutzer authentifiziert wurde, führt Citrix Gateway eine Gruppenautorisierungsprüfung durch, indem die Gruppeninformationen des Benutzers von einem RADIUS-, LDAP- oder TACACS+-Server abrufen. Wenn Gruppeninformationen für den Benutzer verfügbar sind, überprüft Citrix Gateway die für die Gruppe zulässigen Netzwerkressourcen.

Um zu steuern, auf welche Ressourcen Benutzer zugreifen können, müssen Sie Autorisierungsrichtlinien erstellen. Wenn Sie keine Autorisierungsrichtlinien erstellen müssen, können Sie die globale Standardautorisierung konfigurieren.

Wenn Sie innerhalb der Autorisierungsrichtlinie einen Ausdruck erstellen, der den Zugriff auf einen Dateipfad verweigert, können Sie nur den Unterverzeichnispfad und nicht das Stammverzeichnis verwenden. Verwenden Sie beispielsweise fs.path enthält “\\dir1\\dir2” anstelle von fs.path enthält “\\rootdir\\dir1\\dir2”. Wenn Sie in diesem Beispiel die zweite Version verwenden, schlägt die Richtlinie fehl.

Nachdem Sie die Autorisierungsrichtlinie konfiguriert haben, binden Sie sie dann an einen Benutzer oder eine Gruppe.

Standardmäßig werden Autorisierungsrichtlinien zuerst anhand von Richtlinien überprüft, die Sie an den virtuellen Server binden, und dann gegen global gebundene Richtlinien. Wenn Sie eine Richtlinie

global binden und möchten, dass die globale Richtlinie Vorrang vor einer Richtlinie hat, die Sie an einen Benutzer, eine Gruppe oder einen virtuellen Server binden, können Sie die Prioritätsnummer der Richtlinie ändern. Prioritätsnummern beginnen bei Null. Eine niedrigere Prioritätszahl gibt der Richtlinie eine höhere Priorität.

Wenn die globale Richtlinie beispielsweise die Prioritätsnummer eins hat und der Benutzer eine Priorität von zwei hat, wird zuerst die globale Authentifizierungsrichtlinie angewendet.

> **Wichtig:**
>
> - Klassische Autorisierungsrichtlinien werden nur auf TCP-Datenverkehr angewendet.
> - Erweiterte Autorisierungsrichtlinie kann auf alle Arten von Datenverkehr (TCP/UDP/ICMP/DNS) angewendet werden.
>   - To apply policy on UDP/ICMP/DNS traffic, policies must be bound at type UDP_REQUEST, ICMP_REQUEST, and DNS_REQUEST respectively.
>   - While binding, if “type” is not explicitly mentioned or “type” is set to REQUEST, the behavior does not change from earlier builds, that is these policies are applied only to TCP traffic.
>   - The policies bound at UDP_REQUEST do not apply for DNS traffic. For DNS, policies must be explicitly bound to DNS_REQUEST TCP_DNS is similar to other TCP requests.

Weitere Informationen zu erweiterten Autorisierungsrichtlinien finden Sie im Artikel https://support.citrix.com/article/CTX232237.

Konfigurieren und binden Sie eine Autorisierungsrichtlinie

Konfigurieren einer Autorisierungsrichtlinie mit der GUI

1. Navigieren Sie zu **Citrix Gateway > Richtlinien > Autorisierung**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie unter **Name** einen Namen für die Richtlinie ein.
4. Wählen Sie unter **Aktion**die Option **Zulassen** oder **Verweigern**aus.
5. Klicken Sie unter **Ausdruck** auf **Ausdrucksеditor**.
6. Um mit der Konfiguration des Ausdrucks zu beginnen, klicken Sie auf **Auswählen**, und wählen Sie die erforderlichen Elemente aus.
7. Klicken Sie auf **Fertig**, wenn der Ausdruck abgeschlossen ist.
8. Klicken Sie auf **Erstellen**.

Binden einer Autorisierungsrichtlinie an einen Benutzer über die GUI

1. Navigieren Sie zu **Citrix Gateway > Benutzerverwaltung.**

2. Klicken Sie auf **AAA Benutzer**.
3. Wählen Sie im Detailbereich einen Benutzer aus, und klicken Sie dann auf **Bearbeiten**.
4. Klicken Sie unter **Erweiterte Einstellungen** auf **Autorisierungsrichtlinien**.
5. Wählen Sie auf der Seite **Richtlinienbindung** eine Richtlinie aus, oder erstellen Sie eine Richtlinie.
6. Legen Sie unter **Priorität**die Prioritätsnummer fest.
7. Wählen Sie unter **Typ**den Anforderungstyp aus, und klicken Sie dann auf **OK**.

Binden einer Autorisierungsrichtlinie an eine Gruppe über die GUI

1. Navigieren Sie zu **Citrix Gateway > Benutzeradministration**.
2. Klicken Sie auf **AAA-Gruppen**.
3. Wählen Sie im Detailbereich eine Gruppe aus, und klicken Sie dann auf **Bearbeiten**.
4. Klicken Sie unter **Erweiterte Einstellungen** auf **Autorisierungsrichtlinien**.
5. Wählen Sie auf der Seite **Richtlinienbindung** eine Richtlinie aus, oder erstellen Sie eine Richtlinie.
6. Legen Sie unter **Priorität**die Prioritätsnummer fest.
7. Wählen Sie unter **Typ**den Anforderungstyp aus, und klicken Sie dann auf **OK**.

Autorisierung gibt die Netzwerkressourcen an, auf die Benutzer zugreifen können, wenn sie sich bei Citrix Gateway anmelden. Die Standardeinstellung für die Autorisierung besteht darin, den Zugriff auf alle Netzwerkressourcen zu verweigern. Citrix empfiehlt, die globale Standardeinstellung zu verwenden und dann Autorisierungsrichtlinien zu erstellen, um die Netzwerkressourcen zu definieren, auf die Benutzer zugreifen können.

Sie konfigurieren die Autorisierung für Citrix Gateway mit einer Autorisierungsrichtlinie und Ausdrücke. Nachdem Sie eine Autorisierungsrichtlinie erstellt haben, können Sie sie an die Benutzer oder Gruppen binden, die Sie auf der Appliance konfiguriert haben.

Standardmäßige globale Autorisierung

Um die Ressourcen zu definieren, auf die Benutzer im internen Netzwerk zugreifen können, können Sie die globale Standardautorisierung konfigurieren. Sie konfigurieren die globale Autorisierung, indem Sie den Zugriff auf Netzwerkressourcen global im internen Netzwerk zulassen oder verweigern.

Jede von Ihnen erstellte globale Autorisierungsaktion wird auf alle Benutzer angewendet, denen noch keine Autorisierungsrichtlinie zugeordnet ist, entweder direkt oder über eine Gruppe. Eine Benutzer- oder Gruppenautorisierungsrichtlinie überschreibt immer die globale Autorisierungsaktion. Wenn die Standardautorisierungsaktion auf Verweigern festgelegt ist, müssen Sie Autorisierungsrichtlinien für alle Benutzer oder Gruppen anwenden, um Netzwerkressourcen für diese Benutzer oder Gruppen zugänglich zu machen. Diese Anforderung trägt zur Verbesserung der Sicherheit bei.

So legen Sie die globale Standardautorisierung fest:

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte “Configuration” im Navigationsbereich “Citrix Gateway” und klicken Sie auf “Global Settings”.
2. Klicken Sie im Detailbereich unter Einstellungenauf Globale Einstellungen ändern.
3. Wählen Sie auf der Registerkarte Sicherheit neben Standardautorisierungsaktion Zulassen oder Verweigern aus, und klicken Sie auf OK.

Authentifizierungs-Profile

January 25, 2022

Wenn Sie möchten, dass dieselben Authentifizierungseinstellungen von mehreren virtuellen Verkehrsverwaltungsservern verwendet werden, können Sie ein Authentifizierungsprofil erstellen, das den virtuellen Authentifizierungsserver, den Authentifizierungshost, die Authentifizierungsdomäne und die Authentifizierungsebene angibt.

Dieses Authentifizierungsprofil kann den relevanten virtuellen Servern des Verkehrsmanagements zugeordnet werden.

Konfigurieren eines Authentifizierungsprofils

Konfigurieren eines Authentifizierungsprofils mit der CLI

- Erstellen Sie das Authentifizierungsprofil und legen Sie die erforderlichen Parameter fest.

  Zum Beispiel, um ein Profil mit einem virtuellen Authentifizierungsserver namens “authVS” zu erstellen.

```
1  add authentication authnProfile authProfile1 -authnVsName authVS
      -authenticationHost authnVS.example.com -authenticationDomain
      example.com -authenticationLevel
2  <!--NeedCopy-->
```

> **Hinweis:**
>
> Das Authentifizierungsgewicht oder -level hängt von dem virtuellen Server ab, an den der Datenverkehr gebunden ist. Eine Sitzung, die durch die Authentifizierung gegen den virtuellen Server der Verkehrsverwaltung auf einer bestimmten Ebene erstellt wird, kann nicht für den Zugriff auf den virtuellen Server für die Verkehrsverwaltung auf einer höheren Ebene verwendet werden.

- Binden Sie das Authentifizierungsprofil an die relevanten virtuellen Server des Verkehrsmanagements.

Zum Beispiel, um AuthProfile1 an einen virtuellen Lastausgleichsserver mit dem Namen “vserver1” zu binden.

```
set lb vserver vserver1 -authnProfile authProfile1
<!--NeedCopy-->
```

Konfigurieren eines Authentifizierungsprofils mit der GUI

Navigieren Sie auf der Registerkarte **Konfiguration** zu **Sicherheit > AAA - Anwendungsverkehr > Authentifizierungsprofil**, und konfigurieren Sie das Authentifizierungsprofil nach Bedarf.

> **Hinweis:**
>
> - Sie können ein Authentifizierungsprofil erstellen, indem Sie den Citrix Gateway - Assistenten ebenfalls verwenden. Das Profil enthält alle Einstellungen für die Authentifizierungsrichtlinie. Sie konfigurieren das Profil, wenn Sie die Authentifizierungsrichtlinie erstellen.
> - Mit dem Citrix Gateway-Assistenten können Sie den ausgewählten Authentifizierungstyp verwenden, um die Authentifizierung zu konfigurieren. Wenn Sie nach dem Ausführen des Assistenten andere Authentifizierungsrichtlinien konfigurieren möchten, können Sie das Konfigurationsdienstprogramm verwenden. Weitere Informationen zum Citrix Gateway-Assistenten finden Sie unter Konfigurieren von Einstellungen mit dem Citrix Gateway-Assistenten].

Authentifizierungsrichtlinien

February 24, 2022

Wenn sich Benutzer bei der Citrix ADC- oder Citrix Gateway-Appliance anmelden, werden sie gemäß einer von Ihnen erstellten Richtlinie authentifiziert. Eine Authentifizierungsrichtlinie umfasst einen Ausdruck und eine Aktion. Authentifizierungsrichtlinien verwenden Citrix ADC Ausdrücke.

Nachdem Sie eine Authentifizierungsaktion und eine Authentifizierungsrichtlinie erstellt haben, binden Sie sie an einen virtuellen Authentifizierungsserver und weisen Sie ihr eine Priorität zu. Wenn Sie es binden, benennen Sie es auch als primäre oder sekundäre Richtlinie. Primäre Richtlinien werden vor sekundären Richtlinien bewertet. In Konfigurationen, die beide Richtlinientypen verwenden, sind primäre Richtlinien normalerweise spezifischere Richtlinien, während sekundäre Richtlinien normalerweise allgemeinere Richtlinien sind. Es ist für die Authentifizierung aller Benutzerkonten vorgesehen, die die spezifischeren Kriterien nicht erfüllen. Die Richtlinie

definiert den Authentifizierungstyp. Eine einzige Authentifizierungsrichtlinie kann für einfache Authentifizierungsanforderungen verwendet werden und ist normalerweise auf globaler Ebene gebunden. Sie können auch den Standardauthentifizierungstyp verwenden, der lokal ist. Wenn Sie die lokale Authentifizierung konfigurieren, müssen Sie auch Benutzer und Gruppen auf der Appliance konfigurieren.

Sie können mehrere Authentifizierungsrichtlinien konfigurieren und binden, um ein detailliertes Authentifizierungsverfahren und virtuelle Server zu erstellen. Sie können beispielsweise die Kaskadierung und die Zwei-Faktor-Authentifizierung konfigurieren, indem Sie mehrere Richtlinien konfigurieren. Sie können auch die Priorität der Authentifizierungsrichtlinien festlegen, um zu bestimmen, welche Server und die Reihenfolge, in der die Appliance die Benutzeranmeldeinformationen überprüft. Eine Authentifizierungsrichtlinie beinhaltet einen Ausdruck und eine Aktion. Wenn Sie beispielsweise den Ausdruck auf True festlegen, wird bei der Benutzeranmeldung durch die Aktion die Benutzeranmeldung auf true ausgewertet, und Benutzer haben Zugriff auf Netzwerkressourcen.

Nachdem Sie eine Authentifizierungsrichtlinie erstellt haben, binden Sie die Richtlinie entweder auf globaler Ebene oder an virtuelle Server. Wenn Sie mindestens eine Authentifizierungsrichtlinie an einen virtuellen Server binden, werden alle Authentifizierungsrichtlinien, die Sie an die globale Ebene gebunden haben, nicht verwendet, wenn sich Benutzer am virtuellen Server anmelden, es sei denn, der globale Authentifizierungstyp hat eine höhere Priorität als die an den virtuellen Server gebundene Richtlinie.

Wenn sich ein Benutzer an der Appliance anmeldet, wird die Authentifizierung in der folgenden Reihenfolge ausgewertet:

- Der virtuelle Server wird auf gebundene Authentifizierungsrichtlinien überprüft.
- Wenn Authentifizierungsrichtlinien nicht an den virtuellen Server gebunden sind, prüft die Appliance nach globalen Authentifizierungsrichtlinien.
- Wenn eine Authentifizierungsrichtlinie nicht an einen virtuellen Server oder global gebunden ist, wird der Benutzer über den Standardauthentifizierungstyp authentifiziert.

Wenn Sie LDAP- und RADIUS-Authentifizierungsrichtlinien konfigurieren und die Richtlinien für die Zwei-Faktor-Authentifizierung global binden möchten, können Sie die Richtlinie im Konfigurationsdienstprogramm auswählen und dann auswählen, ob es sich bei der Richtlinie um den primären oder sekundären Authentifizierungstyp handelt. Sie können auch eine Gruppenextraktionsrichtlinie konfigurieren.

> **Hinweis:**
>
> Der Citrix ADC oder das Citrix Gateway-Gerät codiert nur UTF-8-Zeichen für die Authentifizierung und ist nicht mit Servern kompatibel, die ISO-8859-1-Zeichen verwenden.

Erstellen einer Authentifizierungsrichtlinie

Erstellen einer Authentifizierungsrichtlinie mit der GUI

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Richtlinien > Authentifizierung**, und wählen Sie dann den Richtlinientyp aus, den Sie erstellen möchten.
   Navigieren Sie für Citrix Gateway zu **Citrix Gateway > Richtlinien > Authentifizierung**.
2. Führen Sie im Detailbereich auf der Registerkarte **Richtlinien** eine der folgenden Aktionen aus:
   - Um eine neue Richtlinie zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Richtlinie zu ändern, wählen Sie die Aktion aus, und klicken Sie dann auf **Bearbeiten**.
3. Geben Sie im Dialogfeld Authentifizierungsrichtlinie erstellen oder Authentifizierungsrichtlinie konfigurieren die Werte für die Parameter ein oder wählen Sie sie aus.
   - **Name** — Richtlinienname (kann für eine zuvor konfigurierte Aktion nicht geändert werden)
   - **Authentifizierungstyp** — `authtype`
   - **Server** — `authVsName`
   - **Ausdruck** — Regel (Sie geben Ausdrücke ein, indem Sie zuerst den Ausdruckstyp in der Dropdown-Liste ganz links unter dem Fenster Ausdruck auswählen und dann den Ausdruck direkt in den Ausdruckstextbereich eingeben, oder indem Sie auf Hinzufügen klicken, um das Dialogfeld Ausdruck hinzufügen zu öffnen und das Dropdown-Menü verwenden listet darin auf, um Ihren Ausdruck zu konstruieren.)
4. Klicken Sie auf **Erstellen** oder **auf OK**. Die von Ihnen erstellte Richtlinie wird auf der Seite Richtlinien angezeigt.
5. Klicken Sie auf die Registerkarte **Server**, und führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um einen vorhandenen Server zu verwenden, wählen Sie ihn aus, und klicken Sie dann auf.
   - Um einen Server zu erstellen, klicken Sie auf Hinzufügen und befolgen Sie die Anweisungen.
6. Wenn Sie diese Richtlinie als sekundäre Authentifizierungsrichtlinie festlegen möchten, klicken Sie auf der Registerkarte Authentifizierung auf Sekundär. Wenn Sie diese Richtlinie als primäre Authentifizierungsrichtlinie festlegen möchten, überspringen Sie diesen Schritt.
7. Klicken Sie auf **Richtlinie einfügen**.
8. Wählen Sie in der Dropdown-Liste die Richtlinie aus, die Sie an den virtuellen Authentifizierungsserver binden möchten.
9. Ändern Sie in der Spalte **Priorität** links die Standardpriorität, um sicherzustellen, dass die Richtlinie in der richtigen Reihenfolge ausgewertet wird.

10. Klicken Sie auf **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich konfiguriert wurde.

Ändern einer Authentifizierungsrichtlinie mithilfe der GUI

Sie können konfigurierte Authentifizierungsrichtlinien und -profile ändern, z. B. die IP-Adresse des Authentifizierungsservers oder den Ausdruck.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration **Citrix Gateway > Richtlinien > Authentifizierung**.
   Hinweis: Sie können die Richtlinie auch unter **Sicherheit > AAA - Anwendungsverkehr > Richtlinien > Authentifizierung**konfigurieren und dann den Richtlinientyp auswählen, den Sie ändern möchten.
2. Wählen Sie im Navigationsbereich unter Authentifizierung einen Authentifizierungstyp aus.
3. Wählen Sie im Detailbereich auf der Registerkarte Server einen Server aus und klicken Sie dann auf Öffnen.

Entfernen einer Authentifizierungsrichtlinie mithilfe der GUI

Wenn Sie einen Authentifizierungsserver aus Ihrem Netzwerk geändert oder entfernt haben, entfernen Sie die entsprechende Authentifizierungsrichtlinie aus Citrix Gateway.

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration **Citrix Gateway > Richtlinien > Authentifizierung**.
   Hinweis: Um über ADC zu konfigurieren, navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Richtlinien > Authentifizierung**, und wählen Sie dann den Richtlinientyp aus, den Sie entfernen möchten.
2. Wählen Sie im Navigationsbereich unter Authentifizierung einen Authentifizierungstyp aus.
3. Wählen Sie im Detailbereich auf der Registerkarte Richtlinien eine Richtlinie aus und klicken Sie dann auf Entfernen.

Erstellen einer Authentifizierungsrichtlinie mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
add authentication negotiatePolicy <name> <rule> <reqAction>

show authentication localPolicy <name>

bind authentication vserver <name> -policy <policyname> [-priority <
   priority>][-secondary]]
```



```
6
7 show authentication vserver <name>
8 <!--NeedCopy-->
```

Beispiel:

```
1 add authentication localPolicy Authn-Pol-1 ns_true
2 Done
3
4 show authentication localPolicy
5 1)      Name: Authn-Pol-1       Rule: ns_true          Request action:
     LOCAL   Done
6
7 bind authentication vserver Auth-Vserver-2 -policy Authn-Pol-1
8 Done
9
10 show authentication vserver Auth-Vserver-2
11 Auth-Vserver-2 (10.102.29.77:443) - SSL Type: CONTENT State: UP Client
     Idle
12 Timeout: 180 sec Down state flush: DISABLED
13 Disable Primary Vserver On Down : DISABLED
14 Authentication : ON
15 Current AAA Users: 0
16 Authentication Domain: myCompany.employee.com
17 1)  Primary authentication policy name:  Authn-Pol-1 Priority: 0
18 Done
19 <!--NeedCopy-->
```

Ändern einer Authentifizierungsrichtlinie mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine vorhandene Authentifizierungsrichtlinie zu ändern:

```
1 set authentication localPolicy <name> <rule> [-reqaction <action>]
2 <!--NeedCopy-->
```

Beispiel

```
1 set authentication localPolicy Authn-Pol-1 'ns_true'
2 <!--NeedCopy-->
```


Entfernen einer Authentifizierungsrichtlinie mithilfe der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine Authentifizierungsrichtlinie zu entfernen:

```
rm authentication localPolicy <name>
<!--NeedCopy-->
```

Beispiel

```
rm authentication localPolicy Authn-Pol-1
<!--NeedCopy-->
```

Binden einer Authentifizierungsrichtlinie

Nachdem Sie die Authentifizierungsrichtlinien konfiguriert haben, binden Sie die Richtlinie entweder global oder an einen virtuellen Server. Sie können entweder das Konfigurationsdienstprogramm verwenden, um eine Authentifizierungsrichtlinie zu binden.

So binden Sie eine Authentifizierungsrichtlinie global mithilfe des Konfigurationsdienstprogramms:

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration **Citrix Gateway > Richtlinien > Authentifizierung**.
   Hinweis: Um von ADC aus zu konfigurieren, navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Richtlinien > Authentifizierung**
2. Klicken Sie auf eine Authentifizierungsart.
3. Klicken Sie im Detailbereich auf der Registerkarte Richtlinien auf einen Server, und klicken Sie dann unter Aktion auf **Globale Bindungen**.
4. Klicken Sie auf der Registerkarte Primär oder Sekundär unter Details auf **Richtlinie einfügen**.
5. Wählen Sie unter Richtlinienname die Richtlinie aus, und klicken Sie dann auf **OK**.

   Hinweis: Wenn Sie die Richtlinie auswählen, setzt Citrix Gateway den Ausdruck automatisch auf den Wert True.

So heben Sie die Bindung einer globalen Authentifizierungsrichtlinie mithilfe des Konfigurationsdienstprogramms auf:

1. Erweitern Sie im Konfigurationsprogramm auf der Registerkarte Konfiguration **Citrix Gateway > Richtlinien > Authentifizierung**.
   Hinweis: Um von ADC aus zu konfigurieren, navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Richtlinien > Authentifizierung**

2. Klicken Sie auf der Registerkarte Richtlinien in Aktion auf **Globale Bindungen**.
3. Wählen Sie im Dialogfeld Authentifizierungsrichtlinien an Global binden/unbind auf der Registerkarte Primär oder Sekundär unter Richtlinienname die Richtlinie aus, klicken Sie auf Richtlinie **aufheben**, und klicken Sie dann auf **OK**.

Hinzufügen einer Authentifizierungsaktion

Hinzufügen einer Authentifizierungsaktion mithilfe der CLI

Wenn Sie die LOCAL-Authentifizierung nicht verwenden, müssen Sie eine explizite Authentifizierungsaktion hinzufügen. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1 add authentication tacacsAction <name> -serverip <IP> [-serverPort <
     port>][-authTimeout <positive_integer>][ ... ]
2 <!--NeedCopy-->
```

Beispiel

```
1 add authentication tacacsaction Authn-Act-1 -serverip 10.218.24.65 -
     serverport 1812 -authtimeout 15 -tacacsSecret "minotaur" -
     authorization OFF -accounting ON -auditFailedCmds OFF -
     defaultAuthenticationGroup "users"
2 <!--NeedCopy-->
```

Konfigurieren einer Authentifizierungsaktion mithilfe der CLI

Um eine vorhandene Authentifizierungsaktion zu konfigurieren, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1 set authentication tacacsAction <name> -serverip <IP> [-serverPort <
     port>][-authTimeout <positive_integer>][ ... ]
2 <!--NeedCopy-->
```

Beispiel


```
set authentication tacacsaction Authn-Act-1 -serverip 10.218.24.65 -
    serverport 1812 -authtimeout 15 -tacacsSecret ”minotaur” -
    authorization OFF -accounting ON -auditFailedCmds OFF -
    defaultAuthenticationGroup ”users”
<!--NeedCopy-->
```

Entfernen einer Authentifizierungsaktion mithilfe der Befehlszeilenschnittstelle

Um eine vorhandene RADIUS-Aktion zu entfernen, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
rm authentication radiusAction <name>
<!--NeedCopy-->
```

Beispiel

```
rm authentication tacacsaction Authn-Act-1
<!--NeedCopy-->
```

Die NoAuth Authentifizierung

Die Citrix ADC-Appliance unterstützt die NoAuth-Authentifizierungsfunktion, mit der der Kunde einen DefaultAuthenticationGroup-Parameter im `noAuthAction` Befehl konfigurieren kann, wenn ein Benutzer diese Richtlinie ausführt. Der Administrator kann überprüfen, ob diese Gruppe in der Benutzergruppe vorhanden ist, um die Navigation des Benutzers durch die NoAuth-Richtlinie zu bestimmen.

So konfigurieren Sie eine NoAuth-Authentifizierung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication noAuthAction <name> [-defaultAuthenticationGroup <
    string>]
<!--NeedCopy-->
```

Beispiel


```
1 add authentication noAuthAction noauthact -defaultAuthenticationGroup
     mynoauthgroup
2 <!--NeedCopy-->
```

Standardtypen für globale Authentifizierung

Wenn Sie Citrix Gateway installiert und den Citrix Gateway-Assistenten ausgeführt haben, haben Sie die Authentifizierung innerhalb des Assistenten konfiguriert. Diese Authentifizierungsrichtlinie ist automatisch an die globale Ebene von Citrix Gateway gebunden. Der Authentifizierungstyp, den Sie im Citrix Gateway-Assistenten konfigurieren, ist der Standardauthentifizierungstyp. Sie können den Standardautorisierungstyp ändern, indem Sie den Citrix Gateway-Assistenten erneut ausführen, oder Sie können die globalen Authentifizierungseinstellungen im Konfigurationsdienstprogramm ändern.

Wenn Sie weitere Authentifizierungstypen hinzufügen müssen, können Sie Authentifizierungsrichtlinien auf Citrix Gateway konfigurieren und die Richtlinien mithilfe des Konfigurationsdienstprogramms an Citrix Gateway binden. Wenn Sie die Authentifizierung global konfigurieren, definieren Sie die Art der Authentifizierung, konfigurieren die Einstellungen und legen die maximale Anzahl von Benutzern fest, die authentifiziert werden können.

Nachdem Sie die Richtlinie konfiguriert und gebunden haben, können Sie die Priorität festlegen, um zu definieren, welcher Authentifizierungstyp Vorrang hat. Beispielsweise konfigurieren Sie LDAP- und RADIUS-Authentifizierungsrichtlinien. Wenn die LDAP-Richtlinie eine Prioritätsnummer von 10 hat und die RADIUS-Richtlinie eine Prioritätsnummer von 15 hat, hat die LDAP-Richtlinie Vorrang, unabhängig davon, wo Sie die einzelnen Richtlinien binden. Dies wird als kaskadierende Authentifizierung bezeichnet.

Sie können Anmeldeseiten aus dem In-Memory-Cache von Citrix Gateway oder vom HTTP-Server bereitstellen, der auf Citrix Gateway ausgeführt wird. Wenn Sie die Anmeldeseite aus dem In-Memory-Cache bereitstellen möchten, erfolgt die Bereitstellung der Anmeldeseite von Citrix Gateway schneller als vom HTTP-Server. Wenn Sie die Anmeldeseite aus dem In-Memory-Cache bereitstellen, wird die Wartezeit reduziert, wenn sich viele Benutzer gleichzeitig anmelden. Sie können die Bereitstellung von Anmeldeseiten aus dem Cache nur als Teil einer globalen Authentifizierungsrichtlinie konfigurieren.

Sie können auch die IP-Adresse der Netzwerkadressübersetzung (NAT) konfigurieren, bei der es sich um eine bestimmte IP-Adresse für die Authentifizierung handelt. Diese IP-Adresse ist für die Authentifizierung eindeutig und nicht das Citrix Gateway-Subnetz, zugeordnete oder virtuelle IP-Adressen. Dies ist eine optionale Einstellung.

> **Hinweis:**
>
> - Sie können den Citrix Gateway-Assistenten nicht zum Konfigurieren der SAML-Authentifizierung

> verwenden.
>
> - Sie können den Schnellkonfigurations-Assistenten verwenden, um die LDAP-, RADIUS- und Clientzertifikatauthentifizierung zu konfigurieren. Wenn Sie den Assistenten ausführen, können Sie aus einem vorhandenen LDAP- oder RADIUS-Server auswählen, der auf Citrix Gateway konfiguriert ist. Sie können die Einstellungen auch für LDAP oder RADIUS konfigurieren. Wenn Sie die Zwei-Faktor-Authentifizierung verwenden, empfiehlt Citrix die Verwendung von LDAP als primären Authentifizierungstyp.

Konfigurieren der globalen Standardauthentifizierung

1. Erweitern Sie in der GUI auf der Registerkarte Konfiguration im Navigationsbereich **Citrix Gateway,** und klicken Sie dann auf **Globale Einstellungen**.
2. Klicken Sie im Detailbereich unter Einstellungen auf **Authentifizierungseinstellungen ändern**.
3. Geben Sie im **Feld Maximale Anzahl an Benutzern**die Anzahl der Benutzer ein, die mit diesem Authentifizierungstyp authentifiziert werden können.
4. Geben Sie im **Feld NAT-IP-Adresse**die eindeutige IP-Adresse für die Authentifizierung ein.
5. Wählen Sie**Statisches Caching aktivieren aus, um Anmeldeseiten schneller bereitzustellen**.
6. Wählen Sie **Erweitertes Authentifizierungsfeedback aktivieren aus, um Benutzern eine Nachricht zu senden, falls die Authentifizierung fehlschlägt** Die Nachricht, die Benutzer erhalten, enthält Kennwortfehler, Konto deaktiviert oder gesperrt, oder der Benutzer wurde nicht gefunden, um nur einige zu nennen.
7. Wählen Sie unter **Standard-Authentifizierungstyp**den Authentifizierungstyp aus.
8. Konfigurieren Sie die Einstellungen für Ihren Authentifizierungstyp, und klicken Sie dann auf **OK**.

Unterstützung für das Abrufen aktueller Anmeldeversuche für einen Benutzer

Die Citrix ADC Appliance bietet eine Option zum Abrufen des Werts der aktuellen Anmeldeversuche für einen Benutzer durch einen neuen Ausdruck `aaa.user.login_attempts`. Der Ausdruck akzeptiert entweder ein Argument (Benutzername) oder kein Argument. Wenn es kein Argument gibt, holt der Ausdruck den Benutzernamen aus dem `aaa_session` oder `aaa_info`.

Sie können den `aaa.user.login_attempts` Ausdruck mit Authentifizierungsrichtlinien für die weitere Verarbeitung verwenden.

So konfigurieren Sie die Anzahl der Anmeldeversuche pro Benutzer mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add expression er aaa.user.login_attempts
```


Benutzer und Gruppen

October 5, 2021

Nach dem Konfigurieren der grundlegenden Einrichtung für Authentifizierung, Autorisierung und Überwachung erstellen Sie Benutzer und Gruppen. Sie erstellen zuerst ein Benutzerkonto für jede Person, die sich über die Citrix ADC Appliance authentifiziert. Wenn Sie die lokale Authentifizierung verwenden, die von der Citrix ADC Appliance selbst gesteuert wird, erstellen Sie lokale Benutzerkonten und weisen jedem dieser Konten Kennwörter zu.

Sie erstellen auch Benutzerkonten auf der Citrix ADC Appliance, wenn Sie einen externen Authentifizierungsserver verwenden. In diesem Fall muss jedoch jedes Benutzerkonto exakt mit einem Konto für diesen Benutzer auf dem externen Authentifizierungsserver übereinstimmen, und Sie weisen den Benutzerkonten, die Sie auf dem Citrix ADC erstellen, keine Kennwörter zu. Der externe Authentifizierungsserver verwaltet die Kennwörter für Benutzer, die sich beim externen Authentifizierungsserver authentifizieren.

Wenn Sie einen externen Authentifizierungsserver verwenden, können Sie weiterhin lokale Benutzerkonten auf der Citrix ADC Appliance erstellen, wenn Sie z. B. temporäre Benutzer (z. B. Besucher) zulassen möchten, sich anzumelden, aber keine Einträge für diese Benutzer auf dem Authentifizierungsserver erstellen möchten. Sie weisen jedem lokalen Benutzerkonto ein Kennwort zu, wie Sie es tun würden, wenn Sie die lokale Authentifizierung für alle Benutzerkonten verwenden würden.

Jedes Benutzerkonto muss an Richtlinien für die Authentifizierung und Autorisierung gebunden sein. Um diese Aufgabe zu vereinfachen, können Sie eine oder mehrere Gruppen erstellen und ihnen Benutzerkonten zuweisen. Anschließend können Sie Richtlinien an Gruppen und nicht an einzelne Benutzerkonten binden.

Konfigurieren von Richtlinien mit Gruppen

Nachdem Sie Gruppen konfiguriert haben, können Sie das Dialogfeld " **Gruppe** " verwenden, um Richtlinien und Einstellungen anzuwenden, die den Benutzerzugriff festlegen. Wenn Sie die lokale Authentifizierung verwenden, erstellen Sie Benutzer und fügen sie zu Gruppen hinzu, die auf Citrix Gateway konfiguriert sind. Die Benutzer erben dann die Einstellungen für diese Gruppe.

Sie können die folgenden Richtlinien oder Einstellungen für eine Gruppe von Benutzern im Dialogfeld **Gruppe** konfigurieren:

- Benutzer
- Autorisierungsrichtlinien
- Überwachungsrichtlinien
- Sitzungsrichtlinien

- Verkehrsrichtlinien
- Lesezeichen
- Intranetanwendungen
- Intranet-IP-Adressen

In Ihrer Konfiguration haben Sie möglicherweise Benutzer, die zu mehr als einer Gruppe gehören. Darüber hinaus verfügt jede Gruppe möglicherweise über eine oder mehrere gebundene Sitzungsrichtlinien mit unterschiedlichen Parametern. Benutzer, die zu mehr als einer Gruppe gehören, erben die Sitzungsrichtlinien, die allen Gruppen zugewiesen sind, zu denen der Benutzer gehört. Um sicherzustellen, welche Sitzungsrichtlinienbewertung Vorrang vor der anderen hat, müssen Sie die Priorität der Sitzungsrichtlinie festlegen.

Beispielsweise haben Sie Gruppe 1, die mit einer Sitzungsrichtlinie gebunden ist, die mit der Homepage www.homepage1.com konfiguriert ist. Group2 ist mit einer Sitzungsrichtlinie gebunden, die mit der Homepage www.homepage2.com konfiguriert ist. Wenn diese Richtlinien an bestimmte Gruppen ohne Prioritätsnummer oder mit derselben Prioritätsnummer gebunden sind, hängt die Homepage, die Benutzern angezeigt wird, die beiden Gruppen angehören, davon ab, welche Richtlinie zuerst verarbeitet wird. Indem Sie eine niedrigere Prioritätsnummer festlegen, die für die Sitzungsrichtlinie mit der Homepage www.homepage1.com eine niedrigere Prioritätsnummer bietet, können Sie sicherstellen, dass Benutzer, die zu beiden Gruppen gehören, die Homepage www.homepage1.com erhalten.

Wenn Sitzungsrichtlinien keine Prioritätsnummer zugewiesen oder dieselbe Prioritätsnummer haben, wird die Priorität in der folgenden Reihenfolge ausgewertet:

- Benutzer
- Gruppe
- Virtueller Server
- Global

Wenn Richtlinien an dieselbe Ebene gebunden sind, ohne Prioritätsnummer oder wenn die Richtlinien dieselbe Prioritätsnummer haben, erfolgt die Reihenfolge der Auswertung nach der Richtlinienverbindungsreihenfolge. Richtlinien, die zuerst an eine Ebene gebunden sind, erhalten Vorrang vor Richtlinien, die später gebunden sind.

Wenn wir einen Benutzer haben, der an mehrere Gruppen gebunden ist, wobei jede Gruppe IIP gebunden ist, kann der Benutzer kostenlose IP von jeder der gebundenen Gruppen erhalten.

Benutzer und Gruppen erstellen

Konfigurieren Sie die Authentifizierung, Autorisierung und Überwachung lokaler Benutzer über die GUI

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Benutzer**
   von Citrix Gateway, erweitern Sie **Citrix Gateway > User Administration**, und klicken Sie dann auf **AAA Users**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Klicken Sie auf **Hinzufügen**, um ein neues Benutzerkonto zu erstellen.
   - Um ein vorhandenes Benutzerkonto zu ändern, wählen Sie das Benutzerkonto aus, und klicken Sie dann auf **Öffnen**.
3. Geben **Sie im Dialogfeld AAA Benutzer erstellen** im Textfeld **Benutzername** einen Namen für den Benutzer ein.
4. Wenn Sie ein lokal authentifiziertes Benutzerkonto erstellen, deaktivieren Sie das Kontrollkästchen **Externe Authentifizierung** und geben Sie ein lokales Kennwort ein, mit dem sich der Benutzer anmeldet.
5. Klicken Sie auf **Erstellen** oder **OK**und dann auf **Schließen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass der Benutzer erfolgreich konfiguriert wurde.

Konfigurieren Sie lokale Gruppen der Authentifizierung, Autorisierung und Überwachung von lokalen Gruppen und fügen Sie ihnen Benutzer hinzu, indem Sie das Konfigurationsdienstprogramm verwenden

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Gruppen**
   Von Citrix Gateway, erweitern Sie **Citrix Gateway > Benutzerverwaltung**, und klicken Sie dann auf **AAA-Gruppen**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine neue Gruppe zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Gruppe zu ändern, wählen Sie die Gruppe aus, und klicken Sie dann auf **Bearbeiten**.
3. Wenn Sie eine neue Gruppe **erstellen, geben Sie im Dialogfeld AAA-Gruppe** erstellen im Textfeld **Gruppenname** einen Namen für die Gruppe ein.
4. Klicken Sie rechts im Bereich **Erweitert** auf **AAA Users** .
   - Um der Gruppe einen Benutzer hinzuzufügen, wählen Sie den Benutzer aus, und klicken Sie dann auf **Hinzufügen**.

- Um einen Benutzer aus der Gruppe zu entfernen, wählen Sie den Benutzer aus, und klicken Sie dann auf **Entfernen**.
- Um ein neues Benutzerkonto zu erstellen und es der Gruppe hinzuzufügen, klicken Sie auf das **Plus-Symbol**, und folgen Sie dann den Anweisungen unter “So konfigurieren Sie Authentifizierung, Autorisierung und Überwachung lokaler Benutzer mit dem Konfigurationsdienstprogramm. “

5. Klicken Sie auf **Erstellen** oder **OK**. Die von Ihnen erstellte Gruppe wird auf der Seite **AAA Gruppen** angezeigt.

Löschen einer Gruppe mit der GUI

Sie können Benutzergruppen auch aus Citrix Gateway löschen.

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Gruppen**
   von Citrix Gateway, ExpandCitrix **Gateway > Benutzerverwaltung,** und klicken Sie dann auf **AAA-Gruppen**.
   Wählen Sie im Detailbereich die Gruppe aus und klicken Sie dann auf Entfernen.

Konfigurieren Sie die Authentifizierung, Autorisierung und Überwachung lokaler Benutzer über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
1 add aaa group <groupname>
2
3 bind aaa group <groupname> -username <username>
4 <!--NeedCopy-->
```

Beispiel:

```
1 add aaa group group-2
2
3 bind aaa group group-2 -username user-2
4 <!--NeedCopy-->
```


Entfernen Sie Benutzer aus einer Authentifizierungs-, Autorisierungs- und Überwachungsgruppe mithilfe der Befehlszeilenschnittstelle

Entbinden Sie an der Eingabeaufforderung Benutzer von der Gruppe, indem Sie den folgenden Befehl einmal für jedes Benutzerkonto eingeben, das an die Gruppe gebunden ist:

```
unbind aaa group <groupname> -username <username><!--NeedCopy-->
```

```
**Beispiel:**

<!--NeedCopy-->
```

unbind aaa group group-hr -username user-hr-1

```
### Entfernen einer Authentifizierungs-, Autorisierungs- und Ü
    berwachungsgruppe mithilfe der Befehlszeilenschnittstelle

Entfernen Sie zuerst alle Benutzer aus der Gruppe. Geben Sie dann an
    der Eingabeaufforderung den folgenden Befehl ein, um eine Citrix ADC
     AAA-Gruppe zu entfernen und die Konfiguration zu überprüfen:

<!--NeedCopy-->
```

rm aaa group

```
**Beispiel:**

<!--NeedCopy-->
```

rm aaa group group-hr

```
> **Hinweis**
>
>Sie können keinen Benutzernamen mit Domäne hinzufügen, wenn der
    Benutzername bereits ohne Domäne hinzugefügt wurde. Wenn der
    Benutzername mit Domäne zuerst hinzugefügt wird, gefolgt von
    demselben Benutzernamen ohne Domäne, fügt die Citrix ADC Appliance
    den Benutzernamen zur Benutzerliste hinzu.
```



```
4
5 Das folgende Beispiel zeigt, dass das Hinzufügen eines Benutzernamens
     mit Domäne nicht zulässig ist, wenn derselbe Benutzername ohne Domä
     ne hinzugefügt wird.
6
7 <!--NeedCopy-->
```

```
add aaa user u47985
Done
show aaa users
1) UserName: u47985
Done
add aaa user u47985@domain.com
ERROR: User already exists
‘‘‘
```

Das folgende Beispiel zeigt, wenn der Benutzername mit Domäne zuerst gefolgt von demselben Benutzernamen ohne Domäne hinzugefügt wird, dann fügt die Citrix ADC Appliance den Benutzernamen zur Benutzerliste hinzu.

```
1 > add aaa user u47985@domain.com
2 Done
3 > add aaa user u47985
4 Done
5 > sh aaa user
6 1)   UserName: u47985@domain.com
7 2)   UserName: u47985
```

‘‘‘

Authentifizierungsmethoden

October 5, 2021

Die Citrix ADC Appliance kann Benutzer mit lokalen Benutzerkonten oder mithilfe eines externen Authentifizierungsservers authentifizieren. Die Appliance unterstützt die folgenden Authentifizierungstypen:

- **LOKAL:** Authentifiziert sich bei der Citrix ADC Appliance mit einem Kennwort, ohne Bezug auf einen externen Authentifizierungsserver. Benutzerdaten werden lokal auf der Citrix ADC Appliance gespeichert.

- **RADIUS:** Authentifizieren Sie sich bei einem externen RADIUS-Server.
- **LDAP:** Authentifiziert sich bei einem externen LDAP-Authentifizierungsserver.
- **TACACS:** Authentifiziert sich bei einem externen Terminal Access Controller Access-Control System (TACACS) -Authentifizierungsserver.
- **CERT:** Authentifiziert sich bei der Citrix ADC Appliance mithilfe eines Clientzertifikats ohne Bezug auf einen externen Authentifizierungsserver.
- **NEGOTIATE:** Authentifiziert sich bei einem Kerberos-Authentifizierungsserver. Wenn bei der Kerberos-Authentifizierung ein Fehler auftritt, verwendet Citrix ADC die NTLM-Authentifizierung.
- **SAML:** Authentifiziert sich bei einem Server, der die Security Assertion Markup Language (SAML) unterstützt.
- **SAML IDP:** Konfiguriert den Citrix ADC so, dass er als Security Assertion Markup Language (SAML) Identity Provider (IdP) dient.
- **WEB:** Authentifiziert sich bei einem Webserver, stellt die Anmeldeinformationen bereit, die der Webserver in einer HTTP-Anfrage benötigt, und analysiert die Antwort des Webservers, um festzustellen, dass die Benutzerauthentifizierung erfolgreich war.
- **Natives OTP:** Die Citrix ADC Appliance unterstützt Einmalkennwörter (OTPs), ohne einen Server eines Drittanbieters verwenden zu müssen.
- **Push-Benachrichtigung:** Citrix Gateway unterstützt Push-Benachrichtigungen für OTP. Benutzer müssen den auf ihren registrierten Geräten empfangenen OTP nicht manuell eingeben, um sich bei Citrix Gateway anzumelden. Administratoren können Citrix Gateway so konfigurieren, dass Anmeldebenachrichtigungen über Push-Benachrichtigungsdienste an registrierte Geräte gesendet werden.
- **E-Mail-OTP:** Mit der E-Mail-OTP-Methode können Sie sich mit dem Einmalkennwort (OTP) authentifizieren, das an die registrierte E-Mail-Adresse gesendet wird. Wenn Sie versuchen, sich für einen Dienst zu authentifizieren, sendet der Server ein OTP an die registrierte E-Mail-Adresse des Benutzers.
- **reCAPTCHA-Authentifizierung** - Citrix Gateway unterstützt eine neue erstklassige Aktion “CaptchaAction”, die die reCAPTCHA-Konfiguration vereinfacht. Da reCAPTCHA eine erstklassige Aktion ist, kann es ein Faktor für sich sein. Sie können reCAPTCHA überall im nFactor Flow injizieren.
- **nFaktor-Authentifizierung:** Die Multifaktor-Authentifizierung erhöht die Sicherheit einer Anwendung, da Benutzer mehrere Identifikationsnachweise bereitstellen müssen, um Zugriff zu erhalten. Die Citrix ADC Appliance bietet einen erweiterbaren und flexiblen Ansatz zur Konfiguration der Multifaktor-Authentifizierung. Dieser Ansatz wird als nFactor authentication bezeichnet.

- **OAuth-Authentifizierung:** Die OAuth-Authentifizierung autorisiert und authentifiziert Benutzer gegenüber Diensten, die auf Anwendungen wie Google, Facebook und Twitter gehostet werden.

nFactor-Authentifizierung

December 3, 2021

> **Wichtig**
>
> - Die nFactor-Authentifizierung wird ab NetScaler 11.0 Build 62.x unterstützt.
> - Damit die nFactor-Authentifizierung mit Citrix ADC arbeitet, ist eine Advanced-Lizenz oder eine Premium-Lizenz erforderlich.
> - Ab Release 13.0 Build 67.x wird die nFactor-Authentifizierung nur mit der Standardlizenz für virtuelle Gateway/VPN-Server unterstützt. Weitere Informationen zur nFactor-Authentifizierung mit Citrix Gateway finden Sie unter nFactor for Gateway-Authentifizierung.
> - Die nFactor-Authentifizierung wird für den Linux-Client nicht unterstützt.

Die mehrstufige Authentifizierung erhöht die Sicherheit einer Anwendung, da Benutzer mehrere Identifikationsnachweise bereitstellen müssen, um Zugriff zu erhalten. Die Citrix ADC-Appliance bietet einen erweiterbaren und flexiblen Ansatz zur Konfiguration der Multifaktor-Authentifizierung. Dieser Ansatz wird als *nFactor-Authentifizierung*bezeichnet.

So funktioniert die nFactor-Authentifizierung

Jeder Authentifizierungsfaktor führt die folgenden Aufgaben aus:

- Sammelt Anmeldeinformationen vom Benutzer. Zu den von Citrix ADC unterstützten Authentifizierungsmechanismen gehören LDAP, RADIUS, SAML-Assertion, Clientzertifikat, OAuth OpenID Connect, Kerberos und so weiter.
- Wertet die bereitgestellten Anmeldeinformationen aus, um zu entscheiden, ob die Authentifizierung erfolgreich war, fehlgeschlagen ist oder die Aktionen wie Gruppenextraktion, Attributextraktion durchgeführt werden sollen.
- Basierend auf den Bewertungsergebnissen wird der Zugriff entweder gewährt, verweigert oder ein nächster Faktor wird ausgewählt.
- Wiederholen Sie diese Schritte, bis keine nächsten Faktoren mehr bewertet werden müssen.

Mit der nFactor-Authentifizierung können Sie:

- Konfigurieren Sie eine beliebige Anzahl von Authentifizierungsfaktoren.

- Basieren Sie die Auswahl des nächsten Faktors auf das Ergebnis der Ausführung des vorherigen Faktors.
- Passen Sie die Login-Schnittstelle an. Sie können beispielsweise die Labelnamen, Fehlermeldungen und den Hilfetext anpassen.
- Extrahieren Sie Benutzergruppeninformationen ohne Authentifizierung.
- Konfigurieren Sie Passthrough für einen Authentifizierungsfaktor. Dies bedeutet, dass für diesen Faktor keine explizite Login-Interaktion erforderlich ist.
- Konfigurieren Sie die Reihenfolge, in der verschiedene Authentifizierungstypen angewendet werden. Jeder der Authentifizierungsmechanismen, die auf der Citrix ADC-Appliance unterstützt werden, kann als jeder Faktor des nFactor-Authentifizierungs-Setups konfiguriert werden. Diese Faktoren werden in der Reihenfolge ausgeführt, in der sie konfiguriert sind.
- Konfigurieren Sie den Citrix ADC so, dass er mit einem Authentifizierungsfaktor fortfährt, der ausgeführt werden muss, wenn die Authentifizierung fehlschlägt. Dazu konfigurieren Sie eine andere Authentifizierungsrichtlinie mit genau derselben Bedingung, jedoch mit der nächsthöchsten Priorität und mit der Aktion auf "NO_AUTH". Sie müssen den nächsten Faktor konfigurieren, der den anzuwendenden alternativen Authentifizierungsmechanismus angeben muss.

Verschlüsselung von Citrix Gateway-Anmeldeinformationen zur nFactor-Authentifizierung

Citrix Gateway mit nFactor-Authentifizierung kann die Anmeldeanforderungsfelder verschlüsseln, die von einem Client (Browser oder SSO-Apps) während des Authentifizierungsprozesses eingereicht werden. Die Felder für verschlüsselte Anmeldeanfragen bieten eine zusätzliche Sicherheitsebene, um die sensiblen Daten des Benutzers vor der Offenlegung zu schützen.

Kompatible Browser

In der folgenden Tabelle sind die Browser zusammen mit Versionsdetails aufgeführt, die die Anmeldeverschlüsselung unterstützen.

Browser	Version
Chrome	78 und höher
Firefox	69 und höher
Internet Explorer	11
Kante	42 und höher
Safari	11.0 und höher

Browser	Version
Oper	66

Kompatible Clients

Im folgenden Abschnitt werden die Clients zusammen mit Versionsdetails aufgeführt, die die Verschlüsselung von Citrix Gateway-Anmeldeinformationen unterstützen.

- Die Citrix Workspace-App unter Mac unterstützt die Verschlüsselung nur, wenn die Betriebssystemversion 10.14.x und höher ist.
- Die Citrix SSO App unter Mac unterstützt die Verschlüsselung nur, wenn die Betriebssystemversion 10.14.x und höher ist.
- Die Windows SSO-App hat keine Einschränkungen hinsichtlich der Kompatibilität.
- Die Kennwortverschlüsselung in der Citrix Workspace-App für Windows-Clients wird nur in der Version von Internet Explorer 11 unterstützt.

So aktivieren Sie die Login-Verschlüsselung mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set aaa parameter [-loginEncryption (ENABLED | DISABLED)]
```

> **Hinweis:**
>
> Der Parameter loginEncryption ist standardmäßig auf DISABLED gesetzt. Sie müssen ihn auf ENABLE setzen.

So aktivieren Sie die Anmeldungsverschlüsselung mit der GUI

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr**und klicken Sie im Abschnitt **Authentifizierungseinstellungen auf AAA-Einstellungen**für Authentifizierungseinstellungen**ändern** .
2. Scrollen Sie auf der Seite **AAA-Parameter konfigurieren** nach unten zur Option **Login Encryption** und aktivieren Sie sie.

nFactor Konzepte, Entitäten und Terminologie

March 8, 2022

In diesem Thema werden einige der wichtigsten an der nFactor-Authentifizierung beteiligten Entitäten und ihre Bedeutung beschrieben.

Login-Schema

nFactor entkoppelt die 'Ansicht', die Benutzeroberfläche, mit dem 'Modell', das die Laufzeitbehandlung darstellt. Die Ansicht von nFactor wird durch das Anmeldeschema definiert. Das Anmeldeschema ist eine Entität, die definiert, was der Benutzer sieht, und angibt, wie die Daten aus dem Benutzer extrahiert werden.

Zum Definieren einer Ansicht verweist das Anmeldeschema auf eine Datei auf dem Datenträger, der das Anmeldeformular definiert. Diese Datei muss der Spezifikation des "Citrix Common Forms Protocol" entsprechen. Diese Datei ist im Wesentlichen eine XML-Definition des Anmeldeformulars.

Zusätzlich zur XML-Datei enthält das Anmeldeschema erweiterte Richtlinienausdrücke, um Benutzernamen und Kennwort aus der Anmeldeanforderung des Benutzers abzurufen. Diese Ausdrücke sind optional und können weggelassen werden, wenn Benutzername und Kennwort des Benutzers mit den erwarteten Variablennamen in Form kommen.

Das Anmeldeschema definiert auch, ob der aktuelle Satz von Anmeldeinformationen als standardmäßige SingleSignOn-Anmeldeinformationen verwendet werden muss.

Das Anmeldeschema kann durch Ausführen des folgenden CLI-Befehls erstellt werden:

```
1    add authentication loginSchema <name> -authenticationSchema <string>
         [-userExpression <string>] [-passwdExpression <string>] [-
        userCredentialIndex <positive_integer>] [-passwordCredentialIndex
         <positive_integer>] [-authenticationStrength <positive_integer>]
         [-SSOCredentials ( YES | NO )]
2 <!--NeedCopy-->
```

> **Hinweis:**
>
> **SSOCredentials** geben an, ob die aktuellen Faktor-Anmeldeinformationen die standardmäßigen SSO-Anmeldeinformationen sind. Der Standardwert ist NEIN.
>
> In der nFactor-Authentifizierungskonfiguration werden die letzten Faktor-Anmeldeinformationen standardmäßig für SSO verwendet. Mithilfe der Konfiguration " **ssoCredentials** " können Anmeldeinformationen für den aktuellen Faktor verwendet werden. Falls diese Konfiguration auf verschiedene Faktoren festgelegt ist, hat der letzte Faktor, für den diese Konfiguration festgelegt ist, die Priorität.

Einzelheiten zu den einzelnen Parametern finden Sie unter https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/13/authentication/authentication-loginSchema/#add-

authentication-loginS.

Bezeichnung der Richtlinie

Ein Policy Label ist eine Sammlung von Richtlinien. Es ist ein Konstrukt, das der Richtlinieninfrastruktur von Citrix ADC nicht fremd ist. Die Richtlinienbezeichnung definiert einen Authentifizierungsfaktor. Das heißt, es enthält alle Richtlinien, die erforderlich sind, um festzustellen, ob die Anmeldeinformationen des Benutzers erfüllt sind. Alle Richtlinien in einem Policy Label können als homogen angenommen werden. Die Richtlinienbezeichnung für die Authentifizierung kann keine Richtlinien unterschiedlichen Typs annehmen, z. B. Um es anders auszudrücken, überprüfen alle Richtlinien in einem Policy Label meistens dasselbe Kennwort/dieselben Anmeldeinformationen des Benutzers. Das Ergebnis von Richtlinien in einem PolicyLabel folgt der logischen ODER-Bedingung. Wenn die in der ersten Richtlinie angegebene Authentifizierung erfolgreich ist, werden andere darauf folgende Richtlinien übersprungen.

Die Richtlinienbezeichnung kann durch Ausführen des folgenden CLI-Befehls erstellt werden:

```
1 add authentication policy label mylabel  - loginSchema <>
2 <!--NeedCopy-->
```

Ein Policy Label verwendet das Anmeldeschema als Eigenschaft. Das Anmeldeschema definiert die Ansicht für dieses Policy Label. Wenn das Anmeldeschema nicht angegeben ist, wird ein implizites Anmeldeschema, LSCHEMA_INT, mit dieser Policy Label verknüpft. Das Anmeldeschema entscheidet, ob ein Policy Label zu einem Passthrough wird oder nicht.

Virtuelles Serverlabel

In der erweiterten Richtlinieninfrastruktur von Citrix ADC ist ein virtueller Server auch eine implizite Policy Label. Das liegt daran, dass der virtuelle Server auch mit mehr als einer Richtlinie gebunden werden kann. Ein virtueller Server ist jedoch etwas Besonderes, da er der Einstiegspunkt für den Clientverkehr ist und Richtlinien eines anderen Typs annehmen kann. Jede der Richtlinien, die es unter einem eigenen Label innerhalb des virtuellen Servers platziert hat. Daher ist der virtuelle Server ein Konglomerat von Labels.

Der nächste Faktor

Immer wenn eine Richtlinie an einen virtuellen Server oder eine Policy Label gebunden ist, kann sie mit dem nächsten Faktor angegeben werden. Der nächste Faktor bestimmt, was getan werden muss, wenn eine bestimmte Authentifizierung erfolgreich ist. Wenn es keinen nächsten Faktor gibt, ist damit der Authentifizierungsprozess für diesen Benutzer abgeschlossen.

Jede Richtlinie, die an einen virtuellen Server oder eine Policy Label gebunden ist, kann einen anderen nächsten Faktor haben. Dies ermöglicht ultimative Flexibilität, bei der der Erfolg jeder Richtlinie einen neuen Pfad für die Benutzerauthentifizierung definieren kann. Der Administrator kann diese Tatsache nutzen und clevere Fallback-Faktoren für Benutzer erstellen, die bestimmte Richtlinien nicht erfüllen.

Richtlinie ohne Authentifizierung

nFactor führt eine spezielle integrierte Richtlinie namens NO_AUTHN ein. Die Richtlinie NO_AUTHN gibt immer Erfolg als Authentifizierungsergebnis zurück. `No-auth` Policy kann erstellt werden, indem der folgende CLI-Befehl ausgeführt wird:

```
1 add authentication policy noauthpolicy  - rule <> -action NO_AUTHN
2 <!--NeedCopy-->
```

Gemäß dem Befehl benötigt die `no-authentication` Richtlinie eine Regel, die ein beliebiger erweiterter Richtlinienausdruck sein kann. Das Authentifizierungsergebnis ist von NO_AUTHN immer erfolgreich.

Eine `no-auth`-Richtlinie an sich scheint keinen Mehrwert zu bieten. Wenn sie jedoch zusammen mit Passthrough-Richtlinienbezeichnungen verwendet wird, bietet es eine große Flexibilität, logische Entscheidungen zu treffen, um den Fluss der Benutzerauthentifizierung zu fördern. NO_AUTHN-Richtlinien und Passthrough-Faktoren bieten eine neue Dimension der Flexibilität von nFactor.

Hinweis: Sehen Sie sich die Beispiele für die Verwendung von `no-auth` und Passthrough in den nachfolgenden Abschnitten an.

Durchgangsfaktor/Etikett

Sobald der Benutzer die Authentifizierung auf dem virtuellen Server bestanden hat (für den ersten Faktor), erfolgen nachfolgende Authentifizierungen bei Richtlinienbezeichnungen oder benutzerdefinierten (sekundären) Faktoren.
Jede Richtlinienbeschriftung/jeder Faktor ist mit einer Anmeldeschemaentität verknüpft, um die Ansicht für diesen Faktor anzuzeigen. Auf diese Weise können Ansichten basierend auf dem Pfad angepasst werden, den der Benutzer eingeschlagen hätte, um zu einem bestimmten Faktor zu gelangen.

Es gibt spezielle Arten von Richtlinienbezeichnungen, die nicht explizit auf ein Anmeldeschema verweisen. Spezialisierte Richtlinienbezeichnungen verweisen auf ein Anmeldeschema, das nicht wirklich auf die XML-Datei für die Ansicht verweist. Diese Richtlinienbezeichnungen/-faktoren werden als “Passthrough” -Faktoren bezeichnet.

Passthrough-Faktoren können durch Ausführen der folgenden CLI-Befehle erstellt werden:

Beispiel 1:

```
1 add authentication policylabel example1
2 <!--NeedCopy-->
```

Beispiel 2:

```
1 add loginschema passthrough_schema  -authenticationSchema noschema
2
3 add authentication policylabel example2  -loginschema
     passthrough_schema
4 <!--NeedCopy-->
```

Der Passthrough-Faktor impliziert, dass das Authentifizierungs-, Autorisierungs- und Überwachungssubsystem nicht an den Benutzer zurückgehen darf, um die für diesen Faktor festgelegten Anmeldeinformationen abzurufen. Stattdessen ist es ein Hinweis für Authentifizierung, Autorisierung und Überwachung, um mit bereits erhaltenen Anmeldeinformationen fortzufahren. Dies ist nützlich in Fällen, in denen ein Benutzereingriff nicht erwünscht ist. Zum Beispiel:

- Wenn dem Benutzer zwei Kennwortfelder angezeigt werden, benötigt der zweite Faktor nach dem ersten Faktor keinen Benutzereingriff.
- Wenn die Authentifizierung eines Typs (z. B. eines Zertifikats) abgeschlossen ist und der Administrator Gruppen für diesen Benutzer extrahieren muss.

Der Passthrough-Faktor kann mit `NO_AUTH` Richtlinien verwendet werden, um bedingte Sprünge zu erstellen.

nFactor-Authentifizierungsablauf

Die Authentifizierung beginnt immer auf dem virtuellen Server in nFactor. Virtueller Server definiert den ersten Faktor für den Benutzer. Das erste Formular, das der Benutzer sieht, wird vom virtuellen Server bedient. Das Anmeldeformular, das der Benutzer sieht, kann auf dem virtuellen Server mithilfe von Anmeldeschemarichtlinien angepasst werden. Wenn es keine Richtlinien für Anmeldeschemas gibt, werden dem Benutzer ein einziger Benutzername und ein Kennwortfeld angezeigt.

Wenn dem Benutzer mehr als ein Kennwortfeld in einem angepassten Formular angezeigt werden muss, müssen Richtlinien für das Anmeldeschema verwendet werden. Sie ermöglichen die Anzeige verschiedener Formulare basierend auf den konfigurierten Regeln (z. B. Intranetbenutzer im Vergleich zu externen Benutzern, Dienstanbieter A im Vergleich zu Dienstanbieter B).

Sobald die Benutzeranmeldeinformationen veröffentlicht wurden, beginnt die Authentifizierung beim virtuellen Authentifizierungsserver, dem ersten Faktor. Da der virtuelle Authentifizierungsserver mit mehreren Richtlinien konfiguriert werden kann, wird jede von ihnen in einer Reihenfolge ausgewertet. Zu einem bestimmten Zeitpunkt, wenn eine Authentifizierungsrichtlinie erfolgreich ist, wird der nächste dafür angegebene Faktor verwendet. Wenn es keinen nächsten Faktor gibt, wird der Authentifizierungsvorgang beendet. Wenn der nächste Faktor existiert, wird geprüft, ob dieser Faktor ein Passthrough-Faktor oder ein regulärer Faktor ist. Wenn das Passthrough ist, werden Authentifizierungsrichtlinien für diesen Faktor ohne Benutzereingriff ausgewertet. Andernfalls wird das mit diesem Faktor verknüpfte Anmeldeschema dem Benutzer angezeigt.

Beispiel für die Verwendung von Passthrough-Faktor und Richtlinien ohne Authentifizierung, um logische Entscheidungen zu treffen

Der Administrator möchte NextFactor basierend auf Gruppen entscheiden.

```
add authentication policylabel group check

add authentication policy admin group -rule http.req.user.is_member_of("Administrators") -action NO_AUTHN

add authentication policy nonadmins -rule true -action NO_AUTHN

bind authentication policy label group check -policy admingroup -pri 1 -nextFactor factor-for-admin

bind authentication policy label groupcheck -policy nonadmins -pri 10 -nextfactor factor-for-others

add authentication policy first_factor_policy -rule <> -action <>

bind authentication vserver <> -policy first_factor_policy -priority 10 -nextFactor groupcheck
<!--NeedCopy-->
```

NFactor-Authentifizierung konfigurieren

September 28, 2022

Mit der nFactor-Konfiguration können Sie mehrere Authentifizierungsfaktoren konfigurieren. Die nFactor-Konfiguration wird nur in Citrix ADC Advanced- und Premium-Editionen unterstützt.

Methoden zur Konfiguration von nFactor

Sie können die nFactor-Authentifizierung mit einer der folgenden Methoden konfigurieren:

- **nFactor Visualizer:** nFactor Visualizer ermöglicht es Ihnen, Faktoren oder Richtlinienbeschriftungen einfach in einem einzigen Bereich miteinander zu verknüpfen und auch die Verknüpfung der Faktoren im selben Bereich zu ändern. Sie können mit dem Visualizer einen nFactor-Flow erstellen und diesen Fluss an einen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver binden. Einzelheiten zu nFactor Visualizer und ein Beispiel für eine nFactor-Konfiguration mit dem Visualizer finden Sie unter nFactor Visualizer für eine vereinfachte Konfiguration.
- **Citrix ADC GUI:** Einzelheiten finden Sie im Abschnitt **Konfigurationselemente, die an der nFactor Konfiguration beteiligt sind**.
- **Citrix ADC CLI:** Ein Beispielausschnitt zur nFactor-Konfiguration mit der Citrix ADC CLI finden Sie unter Beispielausschnitt zur nFactor-Konfiguration unter Verwendung der Citrix ADC CLI.

> **Wichtig:** Dieses Thema enthält Details zum Konfigurieren von nFactor über die Citrix ADC GUI.

An der nFactor-Konfiguration beteiligte Konfigurationselemente

Die folgenden Elemente sind an der Konfiguration von nFactor beteiligt. Ausführliche Schritte finden Sie in den entsprechenden Abschnitten in diesem Thema.

Konfigurations-Element	Zu erledigende Aufgaben
Virtueller AAA-Server	Erstellen Sie einen virtuellen AAA-Server
	Binden Sie das Portal-Thema an den virtuellen AAA-Server
	Clientzertifikatauthentifizierung
Login-Schema	Konfigurieren eines Anmeldeschemaprofils
	Erstellen und Binden einer Login-Schemarichtlinie
Erweiterte Authentifizierungsrichtlinien	Erstellen erweiterter Authentifizierungsrichtlinien
	Binden Sie die erweiterte Authentifizierungsrichtlinie für den ersten Faktor an den virtuellen Citrix ADC AAA-Server
	Verwenden Sie extrahierte LDAP-Gruppen, um den nächsten Authentifizierungsfaktor auszuwählen

Konfigurations-Element	Zu erledigende Aufgaben
Bezeichnung für Authentifizierungsricht	Erstellen einer Authentifizierungsrichtlinien
	Beschriftung der Authentifizierungsrichtlinie binden
nFactor für Citrix Gateway	Erstellen Sie ein Authentifizierungsprofil, um einen virtuellen Citrix ADC AAA-Server mit dem virtuellen Citrix Gateway-Server zu verbinden
	Konfigurieren von SSL-Parametern und CA-Zertifikat für Citrix Gateway
	Konfigurieren der Citrix Gateway-Verkehrsrichtlinie für nFactor Single Sign-On bei StoreFront

So funktioniert nFactor

Wenn ein Benutzer eine Verbindung mit dem Authentifizierungs-, Autorisierungs- und Überwachungsserver oder dem virtuellen Citrix Gateway-Server herstellt, ist die Reihenfolge der Ereignisse wie folgt:

1. Wenn die formularbasierte Authentifizierung verwendet wird, wird das Anmeldeschema angezeigt, das an den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver gebunden ist.
2. Erweiterte Authentifizierungsrichtlinien, die an den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver gebunden sind, werden ausgewertet
    - Wenn die erweiterte Authentifizierungsrichtlinie erfolgreich ist und wenn der nächste Faktor (Bezeichnung der Authentifizierungsrichtlinie) konfiguriert ist, wird der nächste Faktor ausgewertet. Wenn Next Factor nicht konfiguriert ist, ist die Authentifizierung abgeschlossen und erfolgreich.
    - Wenn die erweiterte Authentifizierungsrichtlinie fehlschlägt und Gehe zu Ausdruck auf Weiter festgelegt ist, wird die nächste gebundene erweiterte Authentifizierungsrichtlinie ausgewertet. Wenn keine der erweiterten Authentifizierungsrichtlinien erfolgreich ist, schlägt die Authentifizierung fehl.
3. Wenn an das Label der nächsten Faktor-Authentifizierungsrichtlinie ein Login-Schema gebunden ist, wird es dem Benutzer angezeigt.
4. Die erweiterten Authentifizierungsrichtlinien, die an die Bezeichnung der nächsten Faktor-Authentifizierungsrichtlinie gebunden sind, werden ausgewertet

- Wenn die erweiterte Authentifizierungsrichtlinie erfolgreich ist und wenn der nächste Faktor (Bezeichnung der Authentifizierungsrichtlinie) konfiguriert ist, wird der nächste Faktor ausgewertet.
- Wenn Next Factor nicht konfiguriert ist, ist die Authentifizierung abgeschlossen und erfolgreich.

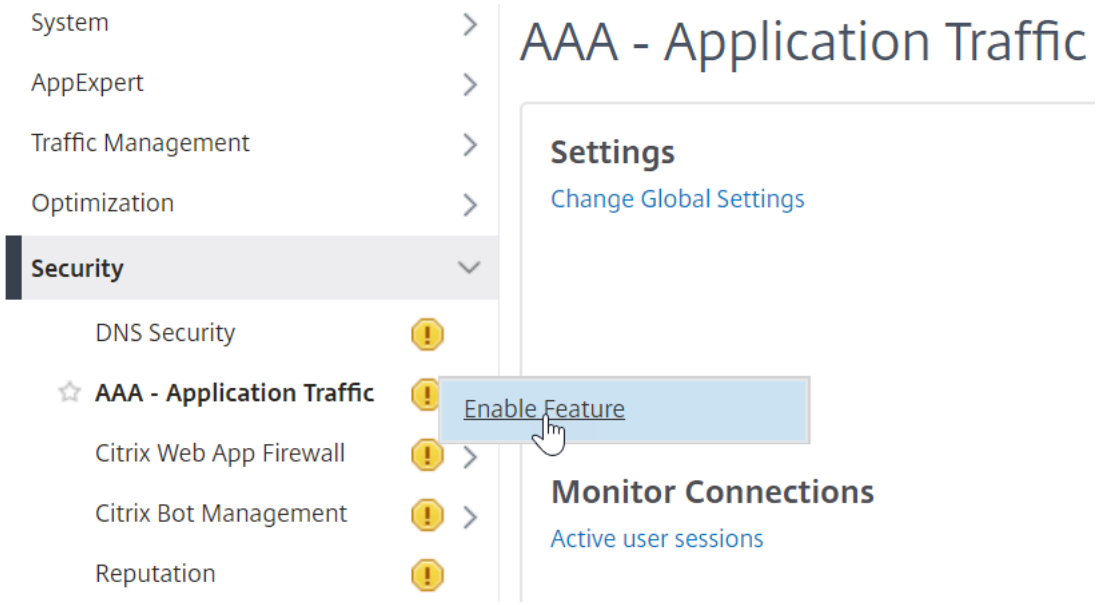
5. Wenn die erweiterte Authentifizierungsrichtlinie fehlschlägt und Gehe zu Ausdruck Weiter ist, wird die nächste gebundene erweiterte Authentifizierungsrichtlinie ausgewertet.
6. Wenn die Richtlinien erfolgreich sind, schlägt die Authentifizierung fehl.

Authentifizierung, Autorisierung und Überwachung des virtuellen Servers

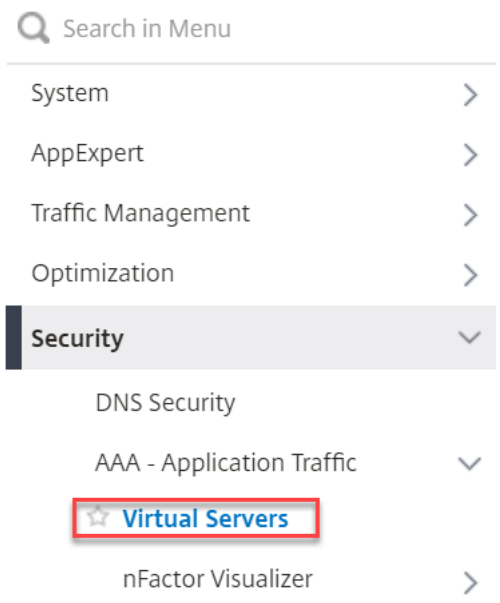
Um nFactor mit Citrix Gateway zu verwenden, konfigurieren Sie es zunächst auf einem virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver. Anschließend verknüpfen Sie später den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver mit dem virtuellen Citrix Gateway-Server.

Erstellen von Authentifizierung, Autorisierung und Überwachung von Virtual Server

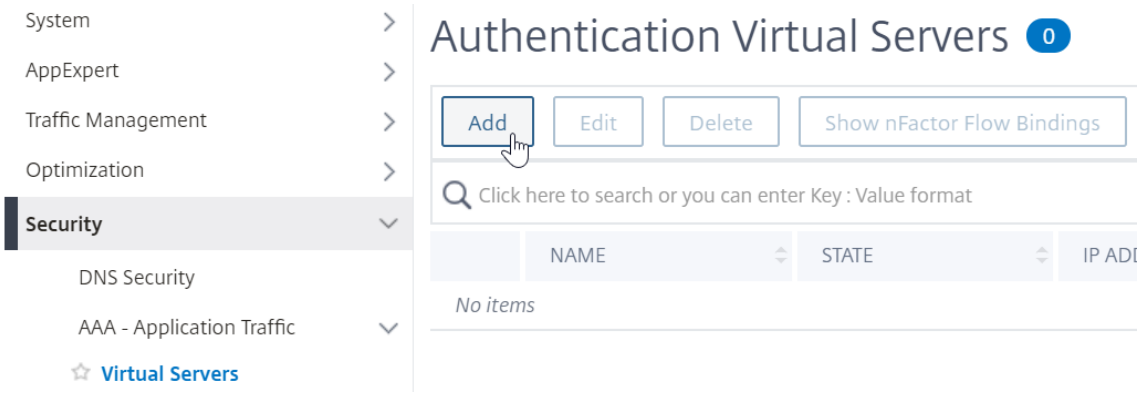
1. Wenn die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion noch nicht aktiviert ist, navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr**, und klicken Sie mit der rechten Maustaste, um die Funktion zu aktivieren.



2. Navigieren Sie zu **Konfiguration > Sicherheit > AAA - Anwendungsverkehr > Virtuelle Server**.

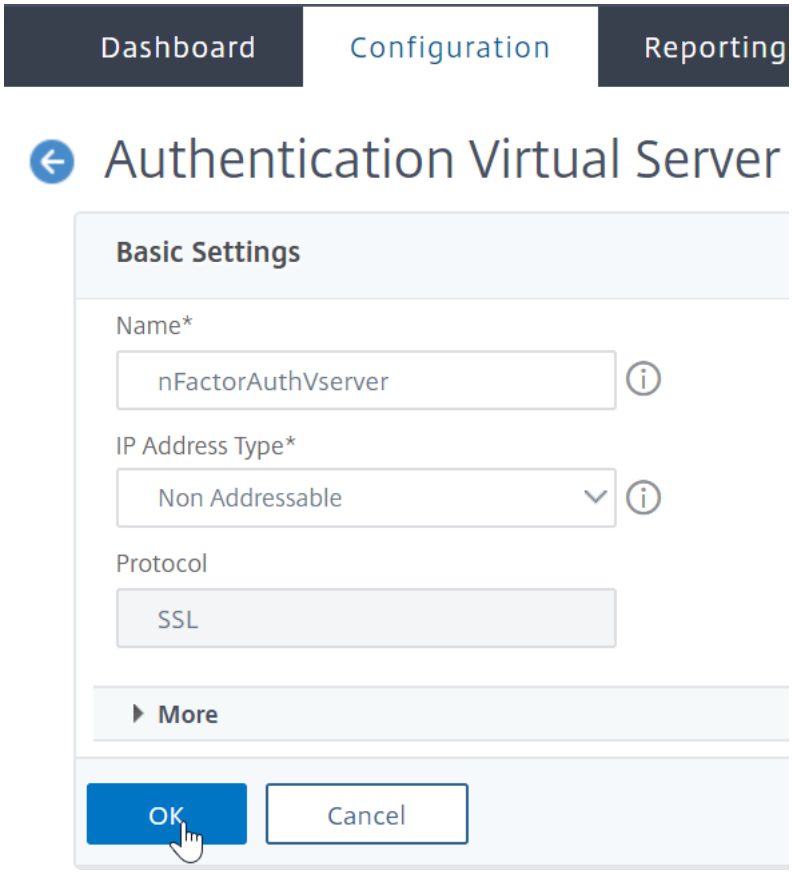


3. Klicken Sie auf **Hinzufügen**, um einen virtuellen Authentifizierungsserver zu erstellen.

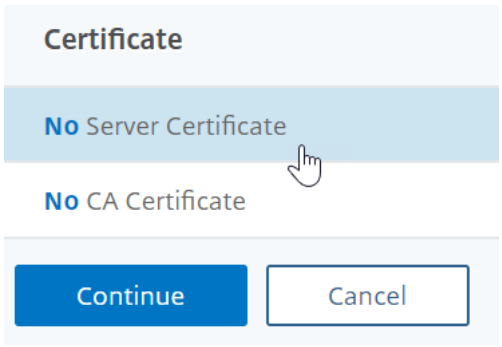


4. Geben Sie die folgenden Informationen ein und klicken Sie auf **OK**.

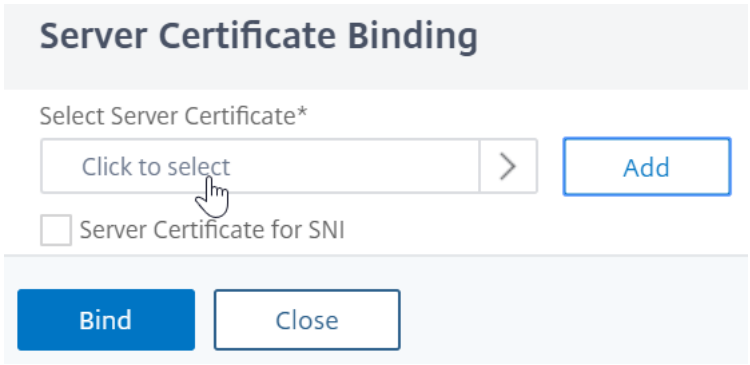
Name des Parameters	Beschreibung des Parameters
Name	Name für den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver.
Typ der IP-Adresse	Ändern Sie den IP-Adresstyp in **Nicht adressierbar**, wenn dieser virtuelle Server nur für Citrix Gateway verwendet wird.



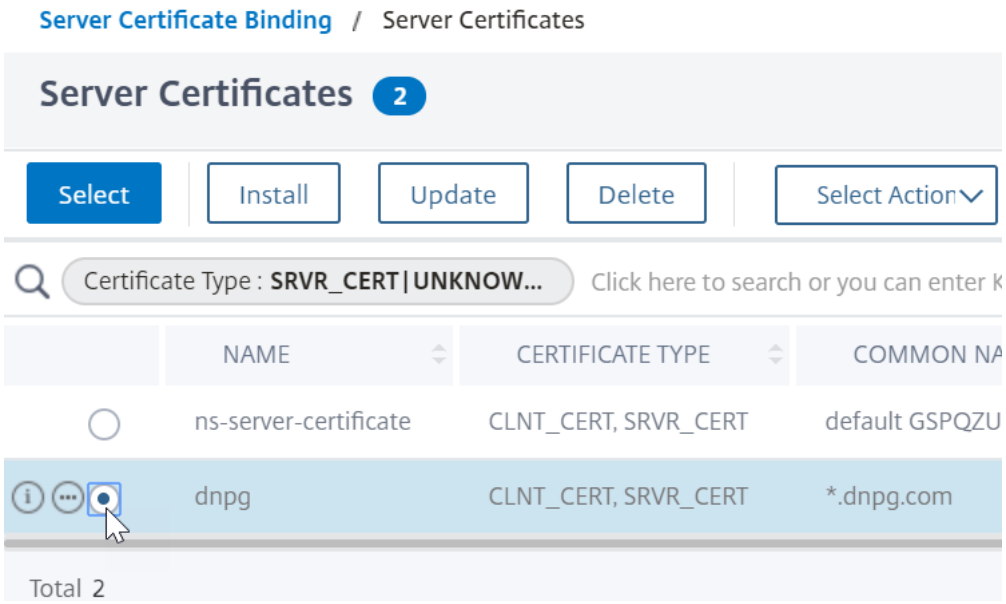
5. Wählen Sie unter Zertifikat **Kein Serverzertifikat**aus.



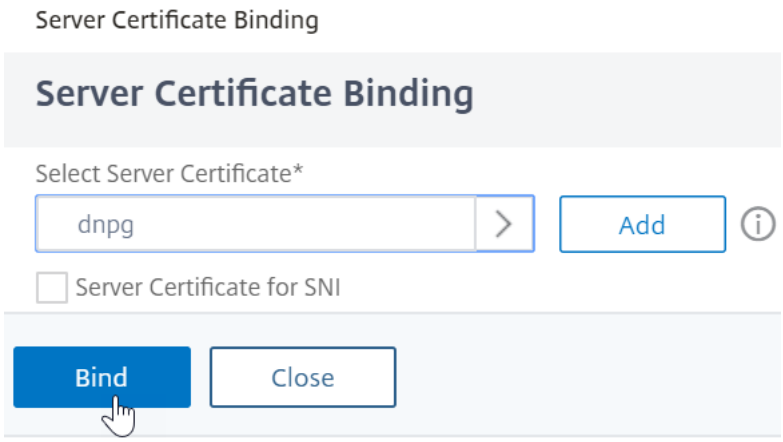
6. Klicken Sie auf den Text, **Klicken Sie**, um das Serverzertifikat auszuwählen.



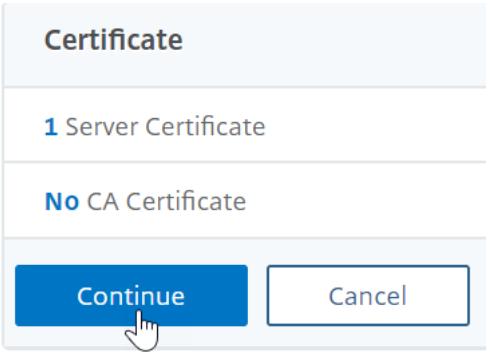
7. Klicken Sie auf das Optionsfeld neben einem Zertifikat für die Authentifizierung, Autorisierung und Überwachung von Virtual Server, und klicken Sie auf **Auswählen**. Das gewählte Zertifikat spielt keine Rolle, da auf diesen Server nicht direkt zugegriffen werden kann.



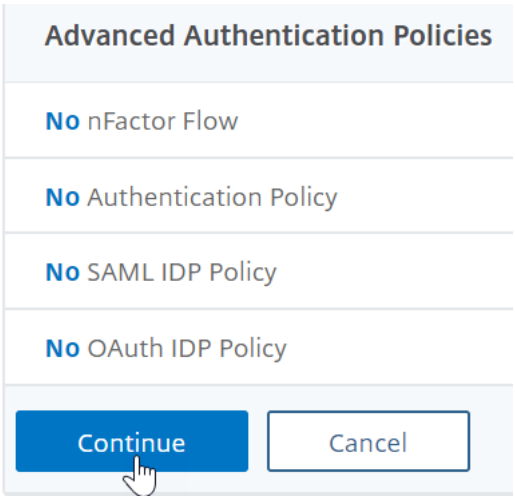
8. Klicken Sie auf **Bind**.



9. Klicken Sie auf **Weiter**, um den Abschnitt **Zertifikat** zu schließen.

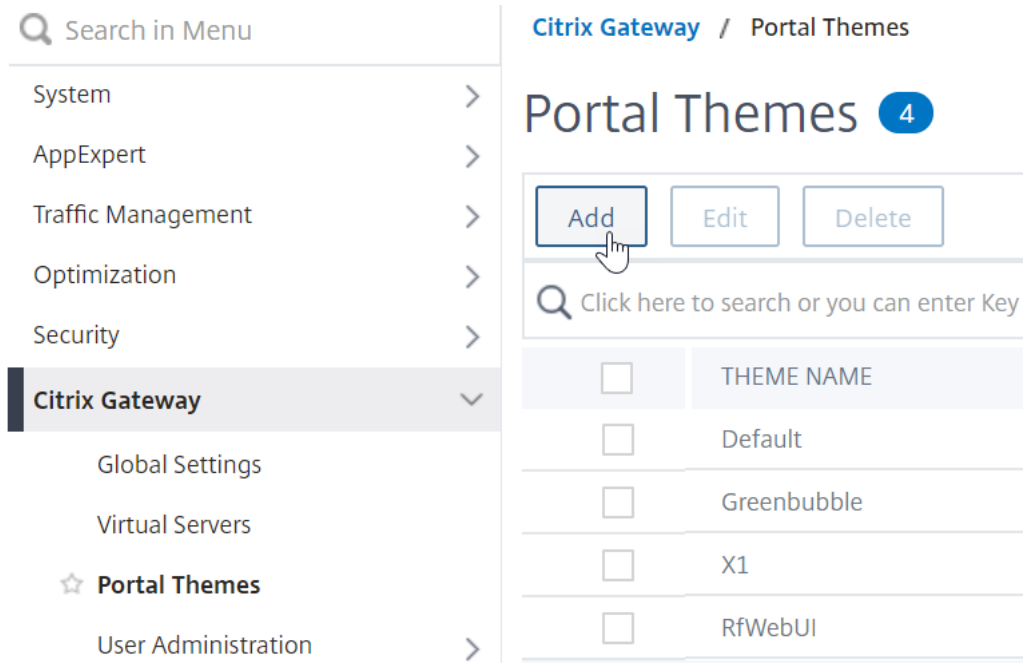


10. Klicken Sie auf **Weiter**.

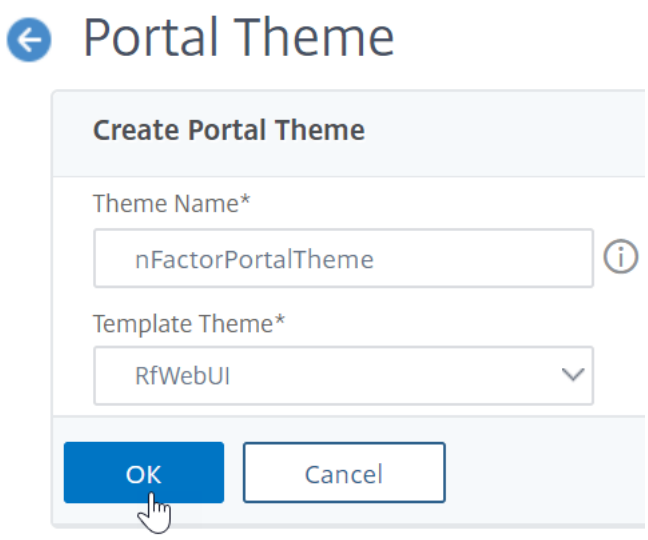


Binden Sie das Portaldesign an den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver

1. Navigieren Sie zu **Citrix Gateway > Portal Themes**, und fügen Sie ein Thema hinzu. Sie erstellen das Design unter Citrix Gateway und binden es später an den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver.

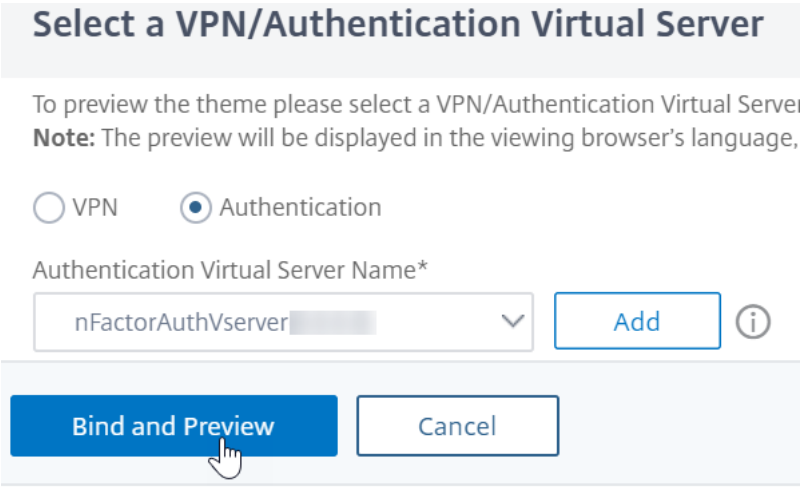


2. Erstellen Sie ein Thema basierend auf dem RfWebUI-Vorlagenthema.



3. Nachdem Sie das Thema wie gewünscht angepasst haben, klicken Sie oben auf der Bearbeitungsseite des Portal-Themas auf **Klicken, um das konfigurierte Thema zu binden und anzuzeigen**.

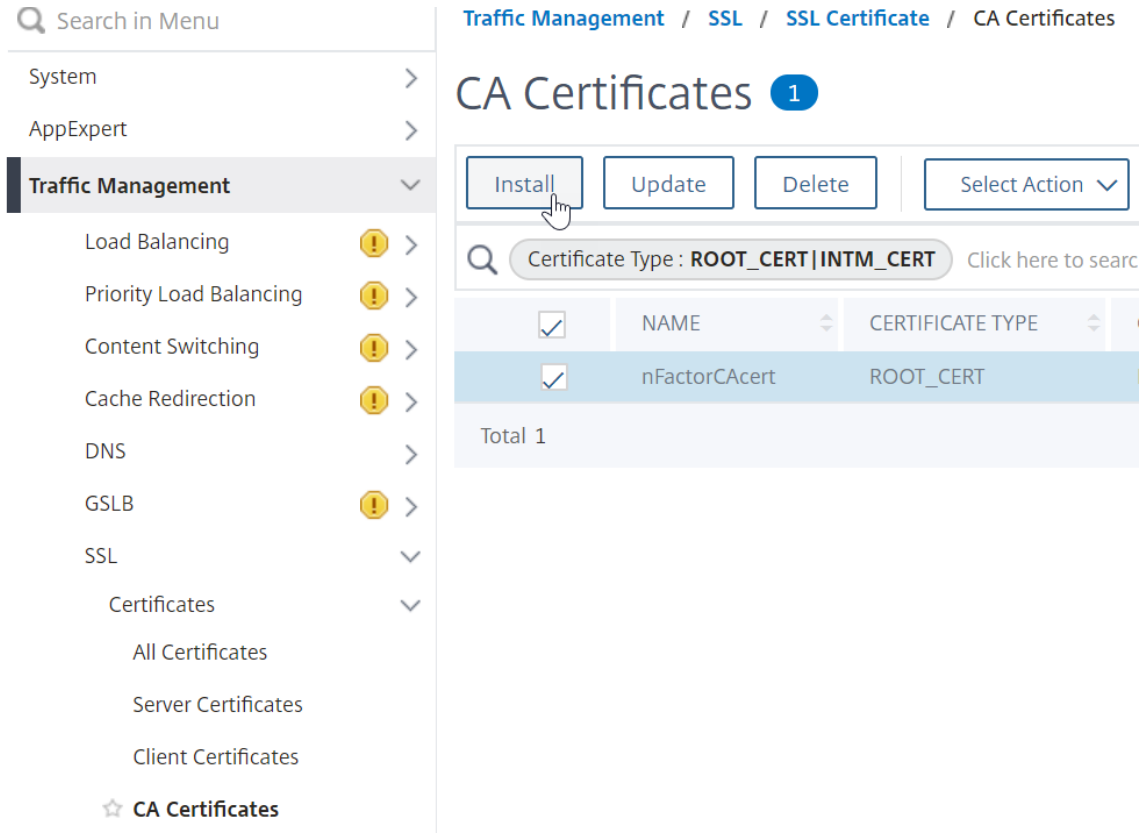
4. Ändern Sie die Auswahl auf Authentifizierung. Wählen Sie im Dropdown-Menü **Name des virtuellen Authentifizierungsservers** den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver aus, klicken Sie auf **Binden und Vorschau**, und schließen Sie das Vorschaufenster.

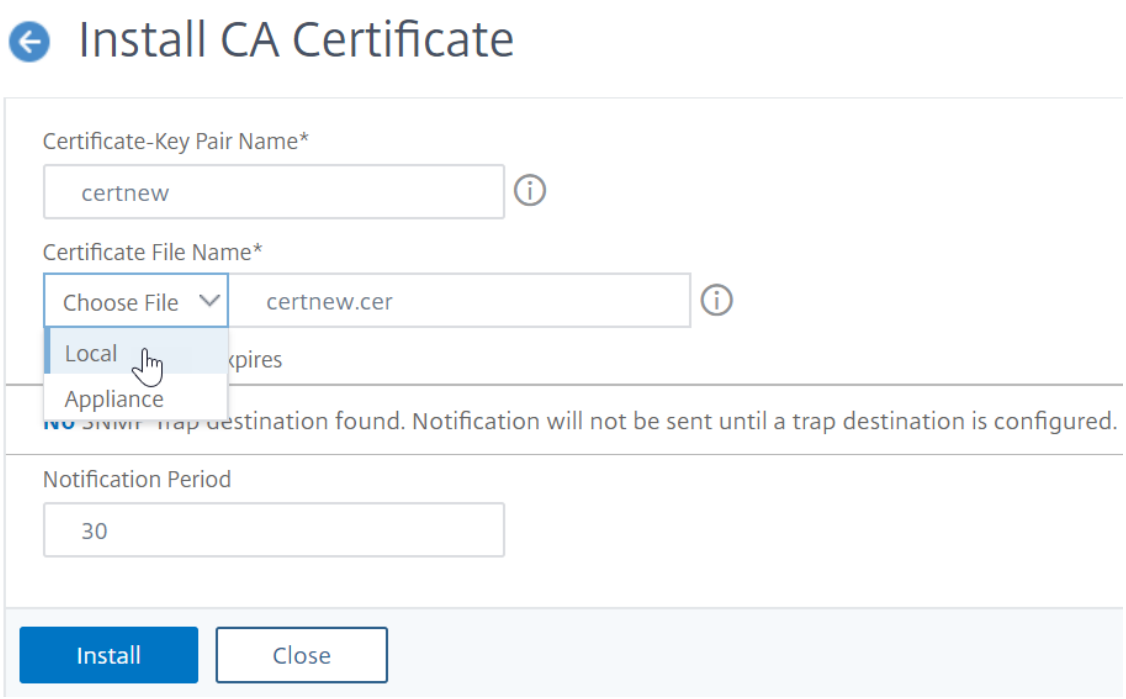


Aktivieren der Clientzertifikatauthentifizierung

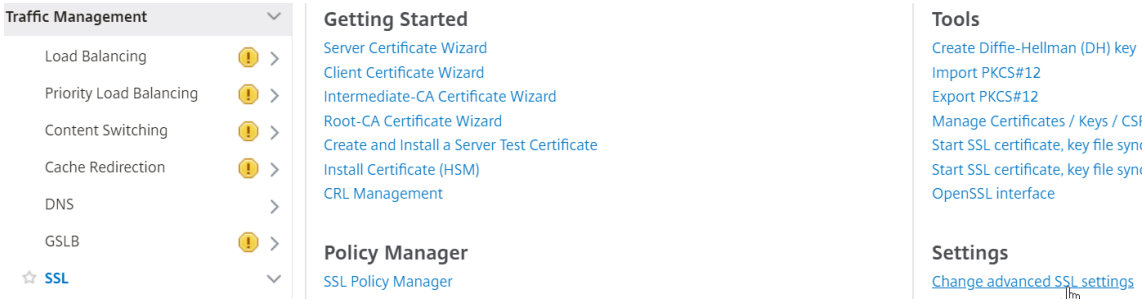
Wenn einer Ihrer Authentifizierungsfaktoren das Clientzertifikat ist, müssen Sie eine SSL-Konfiguration für den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver durchführen:

1. Navigieren Sie zu **Traffic Management > SSL > Certificates > CA Certificates**, und installieren Sie das Stammzertifikat für den Aussteller der Clientzertifikate. Stammzertifikate haben keine Schlüsseldatei.





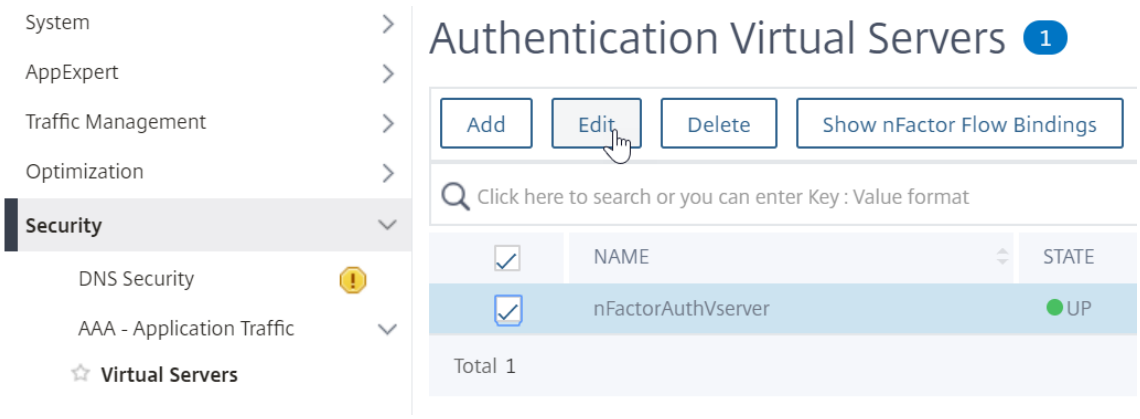
2. Navigieren Sie zu **Traffic Management > SSL > Erweiterte SSL-Einstellungen ändern**.



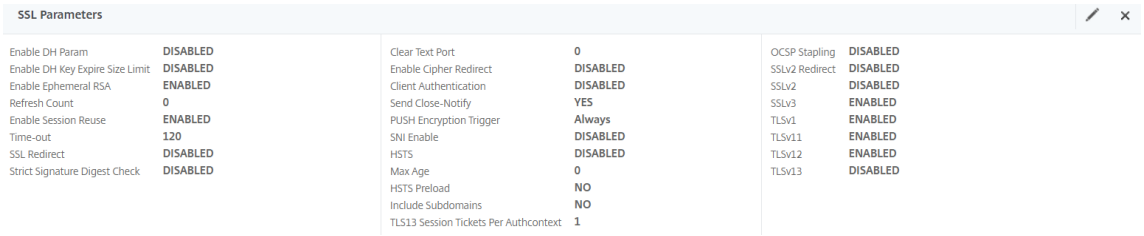
   a) Scrollen Sie nach unten, um zu überprüfen, ob **StandardprofilAKTIVIERT**ist Wenn ja, müssen Sie ein SSL-Profil verwenden, um die Clientzertifikatauthentifizierung zu aktivieren. Andernfalls können Sie die Clientzertifikatauthentifizierung direkt auf dem virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver im Abschnitt SSL-Parameter aktivieren.

3. Wenn Standard-SSL-Profile nicht aktiviert sind:

   a) Navigieren Sie zu **Sicherheit > AAA — Anwendung > Virtuelle Server**, und bearbeiten Sie einen vorhandenen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver.

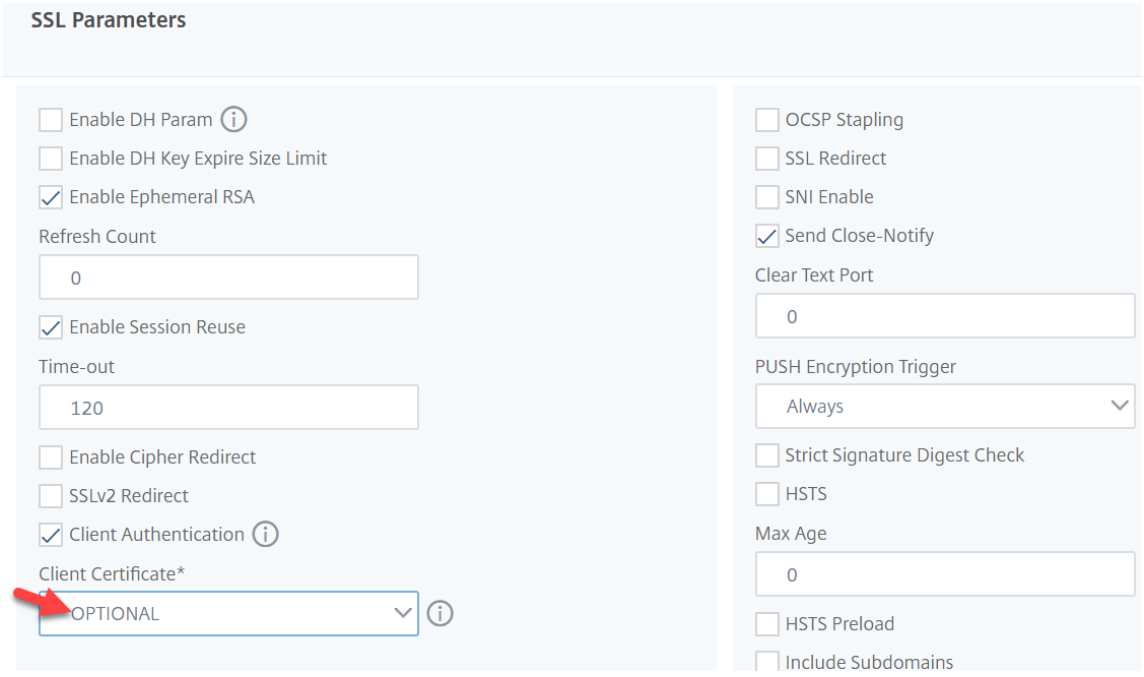


a) Klicken Sie links im Abschnitt **SSL-Parameter** auf das Stiftsymbol.



a) Markieren Sie das Kästchen neben **Clientauthentifizierung**.

b) Stellen Sie sicher, dass im Dropdown-Menü **ClientzertifikatOptional**ausgewählt ist, und klicken Sie auf**OK**.



4. Wenn Standard-SSL-Profile aktiviert sind, erstellen Sie ein SSL-Profil mit aktivierter Clientauthentifizierung:

   a) Erweitern Sie im linken Menü System, und klicken Sie auf Profile.

b) Wechseln Sie rechts oben zur Registerkarte SSL-Profil.

c) Klicken Sie mit der rechten Maustaste auf das Profil ns_default_ssl_profile_frontend, und klicken Sie auf Hinzufügen. Dadurch werden Einstellungen aus dem Standardprofil kopiert.

d) Gib dem Profil einen Namen. Der Zweck dieses Profils besteht darin, Clientzertifikate zu aktivieren.

e) Scrollen Sie nach unten und suchen Sie das Kontrollkästchen Clientauthentifizierung Markieren Sie das Kästchen.

f) Ändern Sie das Dropdown-Menü Clientzertifikat in OPTIONAL.

g) Beim Kopieren des Standard-SSL-Profils werden die SSL-Verschlüsselungen nicht kopiert. Sie müssen sie wiederholen.

h) Klicken Sie auf Fertig, wenn Sie das SSL-Profil erstellt haben.

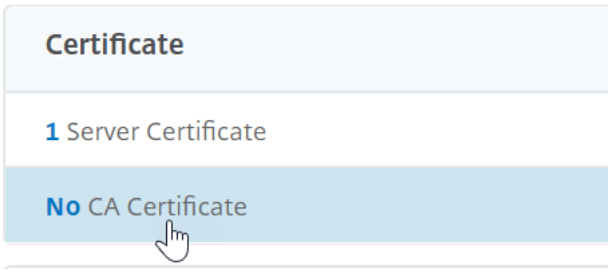
i) Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server**, und bearbeiten Sie einen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver.

j) Scrollen Sie nach unten zum Abschnitt SSL-Profil und klicken Sie auf den Stift.

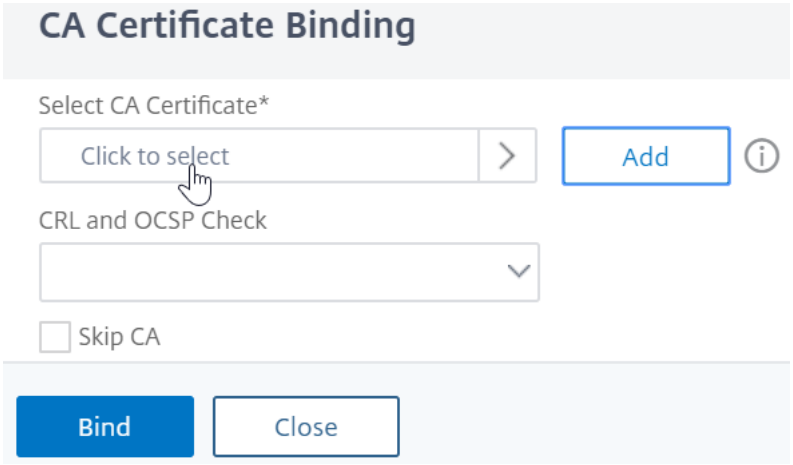
k) Ändern Sie das Dropdown-Menü SSL-Profil in das Profil, für das Clientzertifikate aktiviert sind. Klicken Sie auf OK.

l) Scrollen Sie in diesem Artikel nach unten, bis Sie die Anweisungen zum Binden des CA-Zertifikats erreichen.

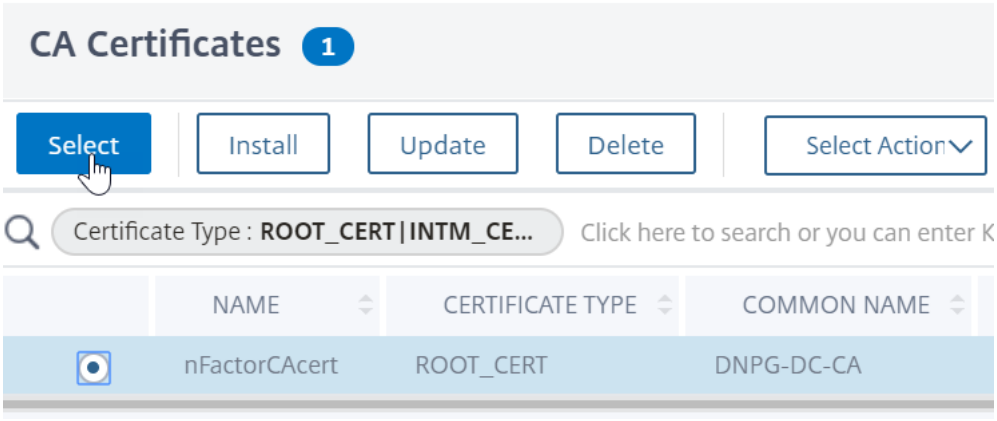
5. Klicken Sie links im Abschnitt **Zertifikate** auf die Stelle, an der **kein CA-Zertifikat**steht.



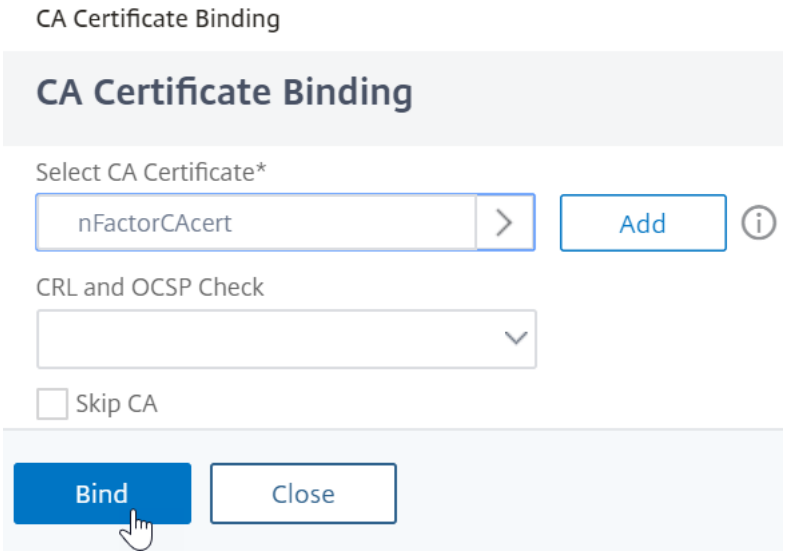
6. Klicken Sie auf den Text, **klicken Sie zum Auswählen**.



7. Klicken Sie auf das Optionsfeld neben dem Stammzertifikat für den Aussteller der Clientzertifikate, und klicken Sie auf **Auswählen**.



8. Klicken Sie auf **Bind**.



Anmeldeschema-XML-Datei

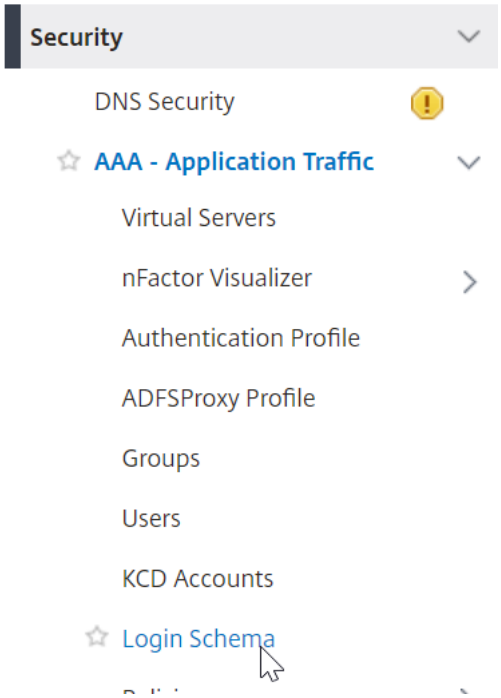
Das Anmeldeschema ist eine XML-Datei, die die Struktur formularbasierter Authentifizierungs-Anmeldeseiten bereitstellt.

nFactor impliziert mehrere Authentifizierungsfaktoren, die miteinander verkettet sind. Jeder Faktor kann verschiedene Login-Schema-Seiten/Dateien haben. In einigen Authentifizierungsszenarien können Benutzern mehrere Anmeldebildschirme angezeigt werden.

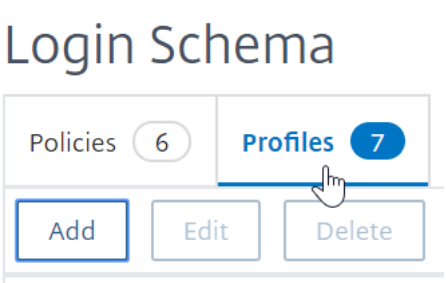
Konfigurieren eines Anmeldeschemaprofils

So konfigurieren Sie ein Login-Schema-Profil:

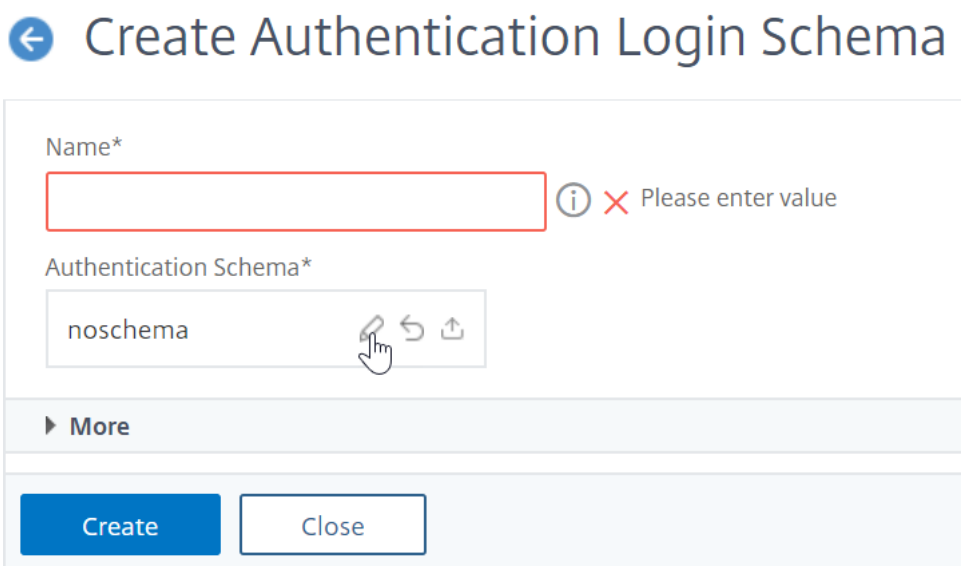
1. Erstellen oder bearbeiten Sie eine .XML-Datei für das Login Schema basierend auf Ihrem nFactor-Design.
2. Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Anmeldeschema**.



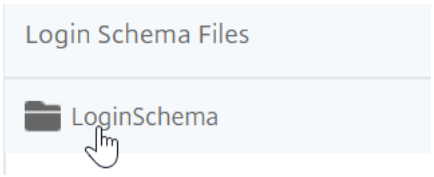
3. Wechseln Sie rechts zur Registerkarte **Profile** und klicken Sie auf **Hinzufügen**.



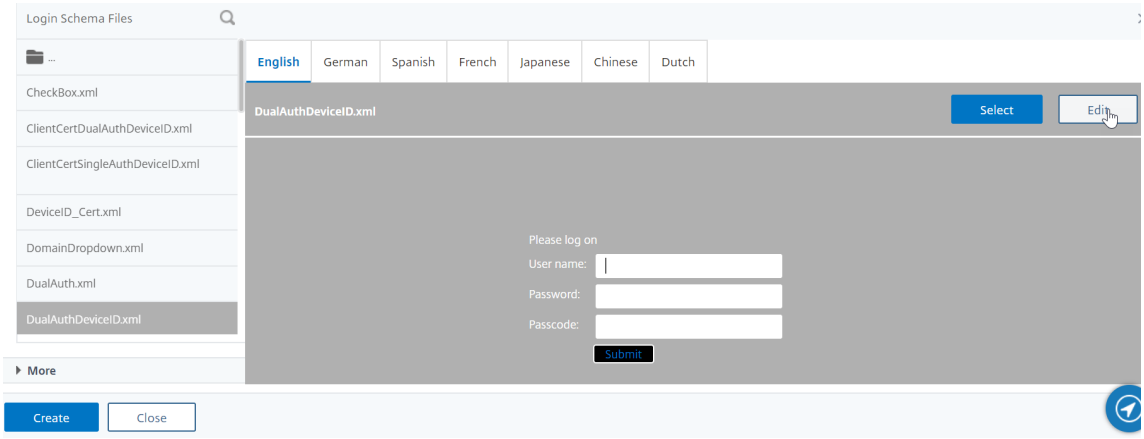
4. Klicken Sie im Feld **Authentifizierungsschema** auf das Stiftsymbol.



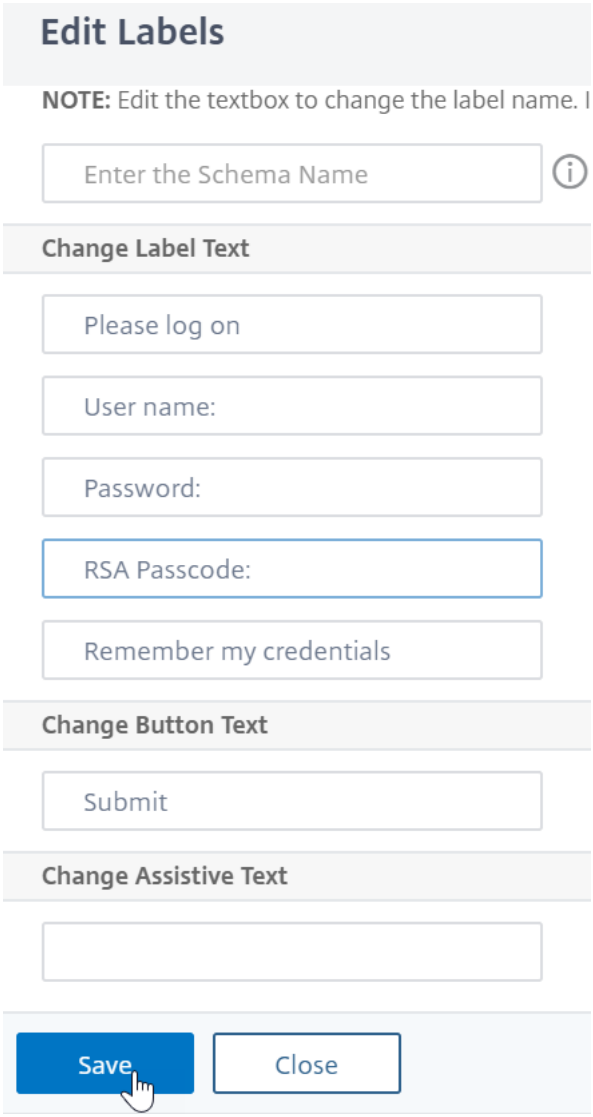
5. Klicken Sie auf den Ordner LoginSchema, um die darin enthaltenen Dateien zu sehen.



6. Markieren Sie eine der Dateien. Auf der rechten Seite sehen Sie eine Vorschau. Die Beschriftungen können geändert werden, indem Sie oben rechts auf die Schaltfläche **Bearbeiten** klicken.

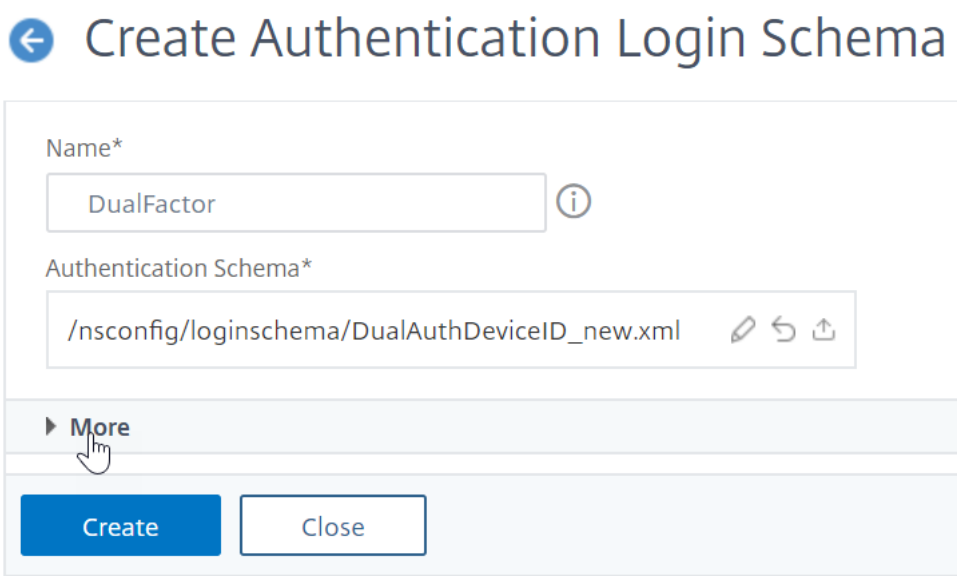


7. Wenn Sie die Änderungen speichern, wird unter /NSConfig/loginSchema eine neue Datei erstellt.



8. Klicken Sie rechts oben auf **Auswählen**.

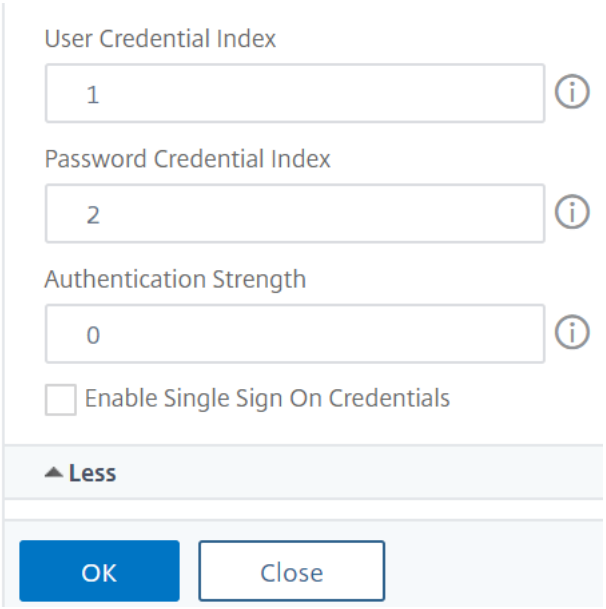
9. Geben Sie dem Anmeldeschema einen Namen und klicken Sie auf " **Mehr**".



10. Verwenden Sie den Benutzernamen und das Kennwort, die im Anmeldeschema für Single Sign-On (SSO) für einen Back-End-Dienst, z. B. StoreFront, eingegeben wurden.

    Sie können die im Anmeldeschema eingegebenen Anmeldeinformationen als Single Sign-On-Anmeldeinformationen verwenden, indem Sie eine der folgenden Methoden verwenden.

    - Klicken Sie unten auf der Seite **Authentifizierungsanmeldeschema erstellen** auf **Mehr** und wählen Sie **Single Sign On Credentials aktivieren**aus.
    - Klicken Sie unten auf der Seite **Authentifizierungsanmeldeschema erstellen** auf **Mehr**, und geben Sie eindeutige Werte für den Index der Benutzeranmeldeinformationen und den Index für Kennwort-Anmeldeinformationen ein. Diese Werte können zwischen 1 und 16 liegen. Später verweisen Sie auf diese Indexwerte in einer Verkehrsrichtlinien/einem Profil, indem Sie den Ausdruck AAA.USER.ATTRIBUTE (#) verwenden.



11. Klicken Sie auf **OK**, um das Login-Schemaprofil zu erstellen.

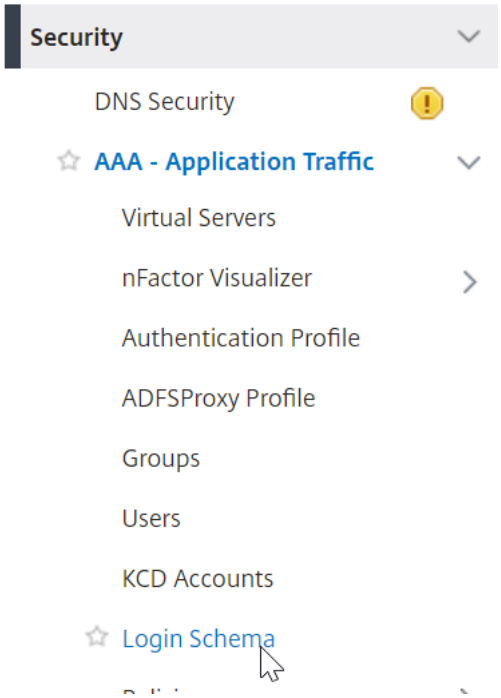
> **Hinweis:** Wenn Sie die Anmeldeschemadatei (.xml) später bearbeiten, müssen Sie das Anmeldeschemaprofil bearbeiten und die Anmeldeschemadatei (.xml-Datei) erneut auswählen, damit Änderungen übernommen werden.

Erstellen und Binden einer Login-Schemarichtlinie

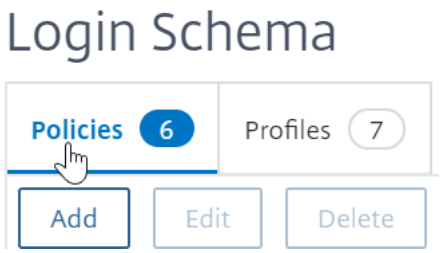
Um ein Anmeldeschemaprofil an einen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver zu binden, müssen Sie zunächst eine Richtlinie für das Anmeldeschema erstellen. Login-Schema-Richtlinien sind nicht erforderlich, wenn das Anmeldeschemaprofil an eine Authentifizierungsrichtlinienbezeichnung gebunden wird, wie später beschrieben.

So erstellen und binden Sie eine Login-Schema-Richtlinie:

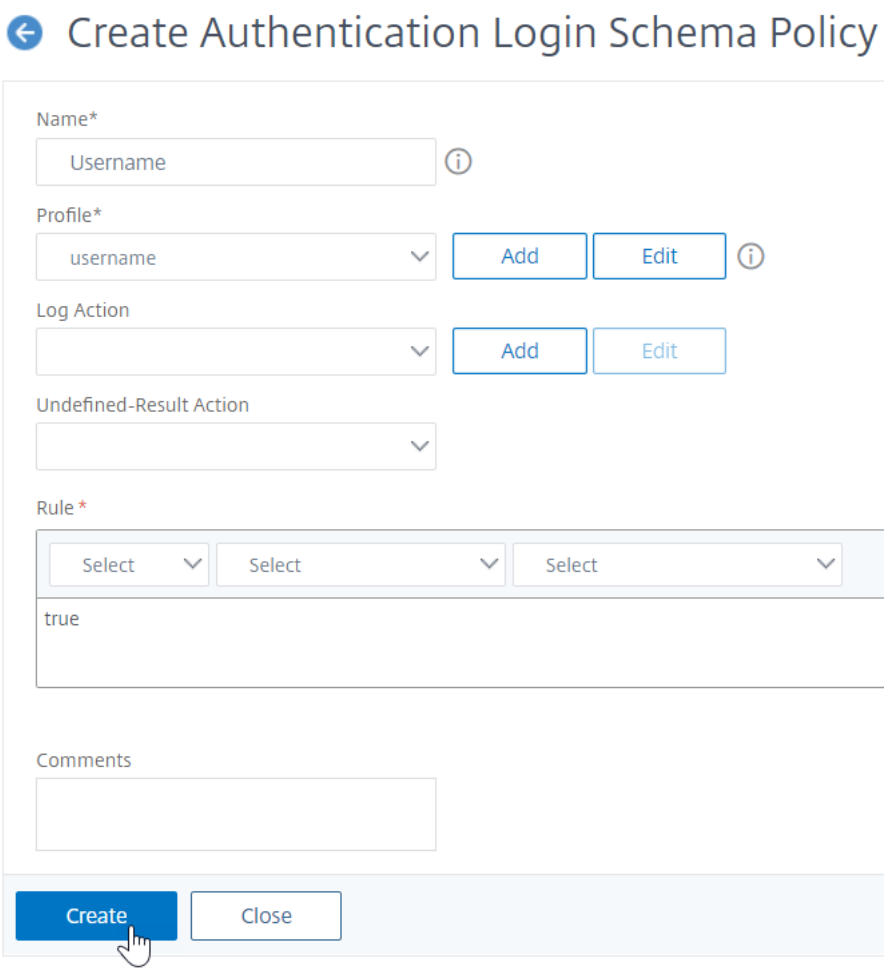
1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Anmeldeschema**.



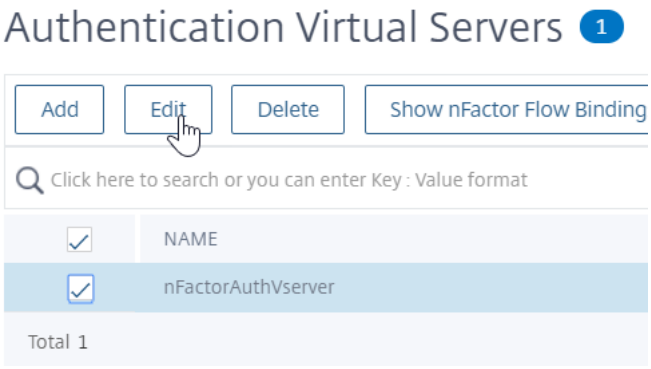
2. Klicken Sie auf der Registerkarte **Policies** auf **Add**.



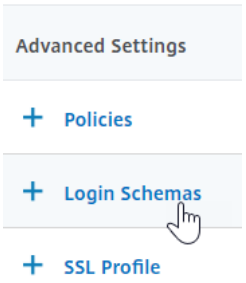
3. Verwenden Sie das Dropdown-Menü **Profil**, um das Anmeldeschema-Profil auszuwählen, das Sie bereits erstellt haben.
4. Geben Sie in das Feld **Regel** einen erweiterten Richtlinienausdruck ein und klicken Sie auf **Erstellen**.



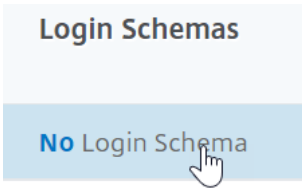
5. Navigieren Sie auf der linken Seite zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server**, und bearbeiten Sie einen vorhandenen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver.



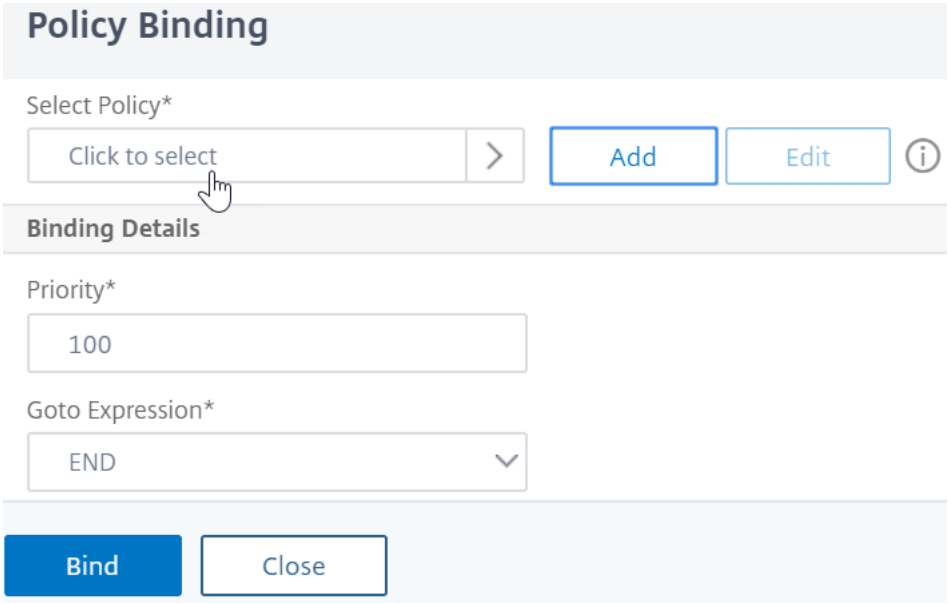
6. Klicken Sie in der Spalte Erweiterte Einstellungen auf **Anmeldeschemas**.



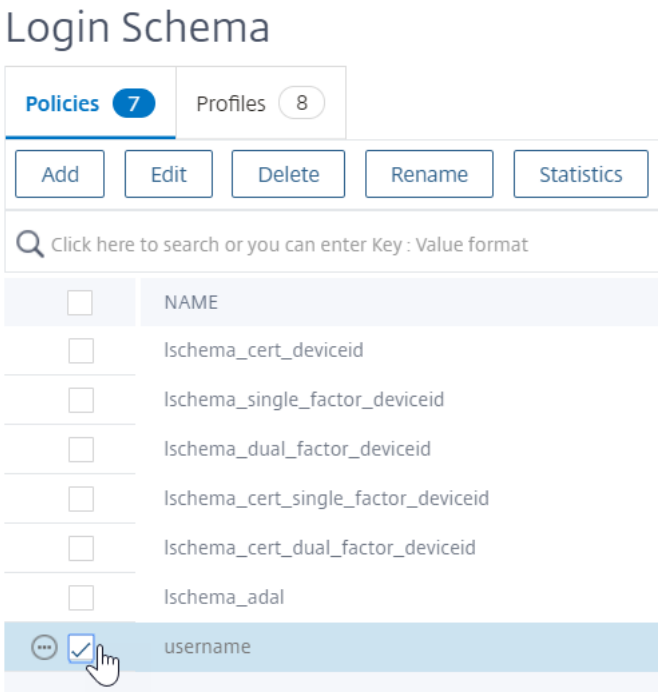
7. Klicken Sie im Abschnitt Anmeldeschemas auf den Text **Kein Anmeldeschema**.



8. Klicken Sie auf den Text, **klicken Sie zum Auswählen**.



9. Klicken Sie auf das Optionsfeld neben der Richtlinie für das Anmeldeschema und dann auf **Auswählen**. In dieser Liste werden nur Login-Schema-Richtlinien angezeigt. Login-Schemaprofile (ohne Richtlinie) werden nicht angezeigt.



10. Klicken Sie auf **Bind**.

Erweiterte Authentifizierungsrichtlinien

Authentifizierungsrichtlinien sind eine Kombination aus Richtlinienausdruck und Richtlinienmaßnahmen. Wenn der Ausdruck wahr ist, dann bewerten Sie die Authentifizierungsaktion.

Erstellen erweiterter Authentifizierungsrichtlinien

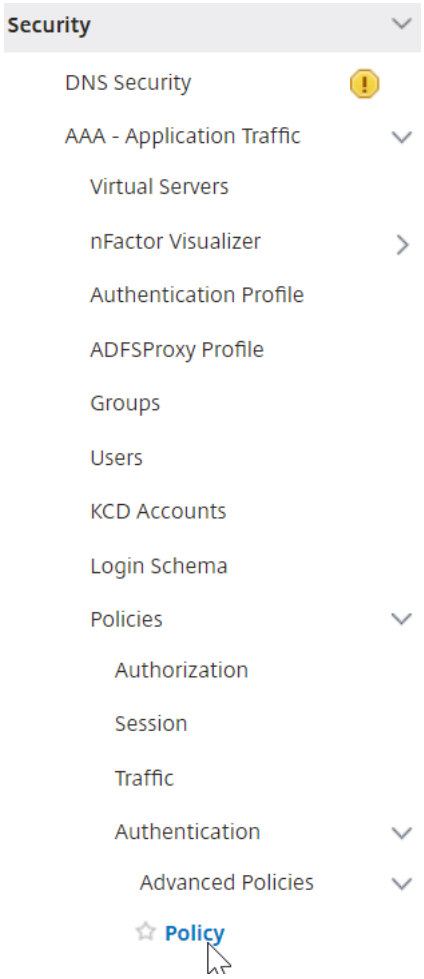
Authentifizierungsrichtlinien sind eine Kombination aus Richtlinienausdruck und Richtlinienaktion. Wenn der Ausdruck wahr ist, dann bewerten Sie die Authentifizierungsaktion.

Sie benötigen Authentifizierungsaktionen/Server (z. B. LDAP, RADIUS, CERT, SAML usw.)
Beim Erstellen einer erweiterten Authentifizierungsrichtlinie gibt es ein Pluszeichen (Hinzufügen), mit dem Sie Authentifizierungsaktionen/Server erstellen können.

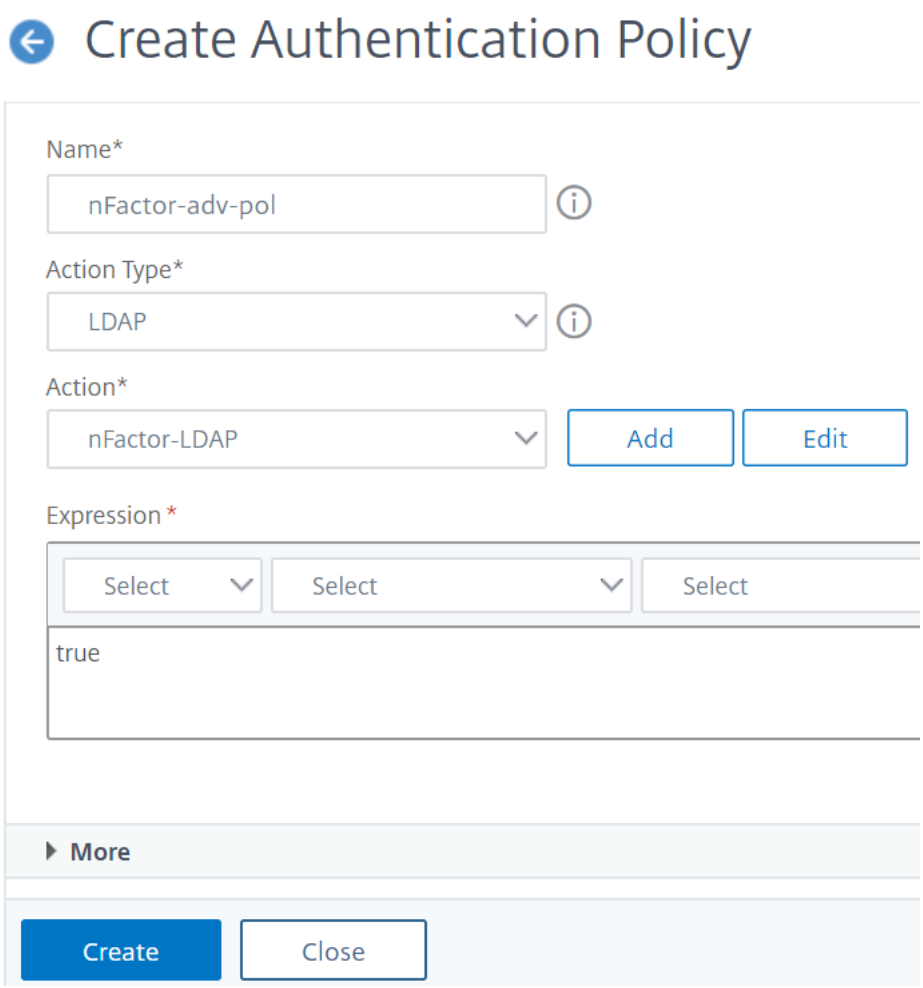
Oder Sie können Authentifizierungsaktionen (Server) erstellen, bevor Sie die erweiterte Authentifizierungsrichtlinie erstellen. Die Authentifizierungsserver befinden sich unter **Authentifizierung > Dashboard**. Klicken Sie auf der rechten Seite auf Hinzufügen, und wählen Sie einen Servertyp aus. Die Anweisungen zum Erstellen dieser Authentifizierungsserver sind hier nicht detailliert. Siehe die Verfahren Authentifizierung — NetScaler 12/Citrix ADC 12.1.

So erstellen Sie eine erweiterte Authentifizierungsrichtlinie:

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinie**



2. Führen Sie im Detailbereich einen der folgenden Schritte aus:
   - Um eine Richtlinie zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus und klicken dann auf **Bearbeiten**.
3. Geben **Sie im Dialogfeld Authentifizierungsrichtlinie erstellen** oder **Authentifizierungsrichtlinie konfigurieren** Werte für die Parameter ein oder wählen Sie sie aus.



- **Name** — Der Name der Richtlinie. Für eine zuvor konfigurierte Richtlinie kann nicht geändert werden.
- **Aktionstyp** - Der Richtlinientyp: Cert, Negotiate, LDAP, RADIUS, SAML, SAMLIDP, TACACS oder WEBAUTH.
- **Aktion** — Die Authentifizierungsaktion (Profil), die mit der Richtlinie verknüpft werden soll. Sie können eine bestehende Authentifizierungsaktion auswählen oder auf das Plus klicken und eine Aktion des richtigen Typs erstellen.
- **Protokollaktion** — Die Überwachungsaktion, die mit der Richtlinie verknüpft werden soll. Sie können eine bestehende Audit-Aktion auswählen oder auf das Plus klicken und eine Aktion erstellen.
  Sie haben keine Aktionen konfiguriert, oder um eine Aktion zu erstellen, klicken Sie auf **Hinzufügen** und führen Sie die Schritte aus.
- **Ausdruck** - Die Regel, die Verbindungen auswählt, auf die Sie die angegebene Aktion anwenden möchten. Die Regel kann einfach (“wahr” wählt den gesamten Verkehr aus) oder komplex sein. Sie geben Ausdrücke ein, indem Sie zuerst den Ausdruckstyp in der Dropdownliste ganz links unter dem Ausdrucksfenster auswählen und dann Ihren Ausdruck di-

rekt in den Ausdruckstextbereich eingeben, oder indem Sie auf Hinzufügen klicken, um das Dialogfeld Ausdruck hinzufügen zu öffnen, und die darin bezeichnenden Dropdownlisten verwenden, um Ihre Ausdruck.)

- **Kommentar** - Sie können einen Kommentar eingeben, der die Art des Datenverkehrs beschreibt, für den diese Authentifizierungsrichtlinie gilt. Optional.

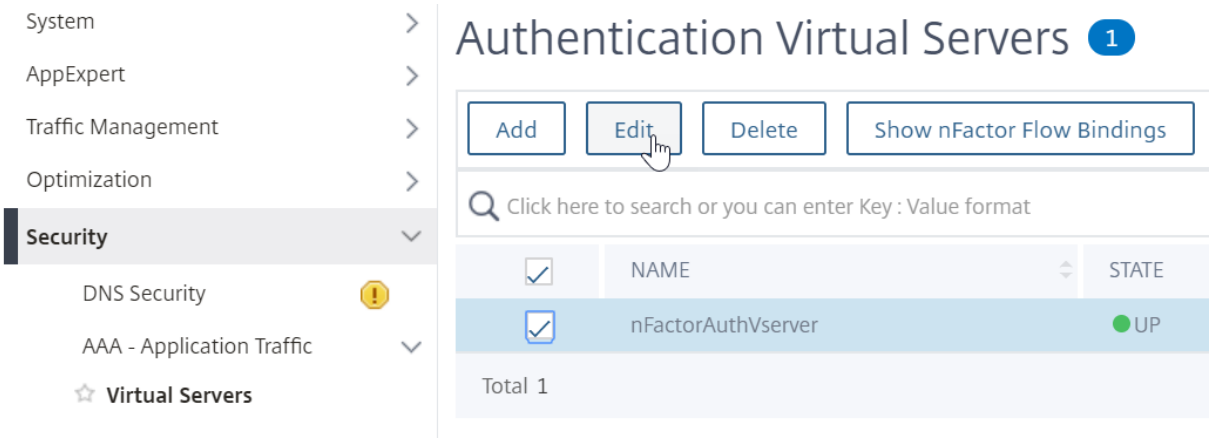
4. Klicken Sie auf **Create** und dann auf **Close**. Wenn Sie eine Richtlinie erstellt haben, wird diese Richtlinie auf der Seite Authentifizierungsrichtlinien und Server angezeigt.

Erstellen Sie je nach Bedarf zusätzliche erweiterte Authentifizierungsrichtlinien basierend auf Ihrem nFactor-Design.

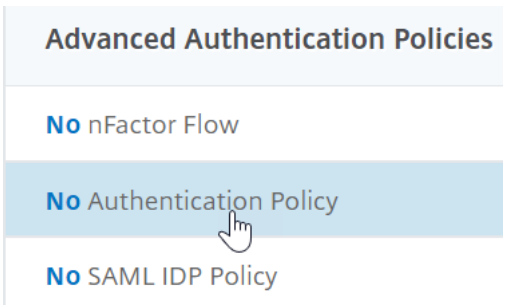
Binden Sie die erweiterte Authentifizierungsrichtlinie des ersten Faktors an Authentifizierung, Autorisierung und Überwachung

Sie können erweiterte Authentifizierungsrichtlinien direkt für den ersten virtuellen Faktor-Authentifizierungs-, Autorisierungs- und Überwachungsserver binden. Für die nächsten Faktoren müssen Sie die erweiterten Authentifizierungsrichtlinien an die Bezeichnungen der Authentifizierungsrichtlinie binden.

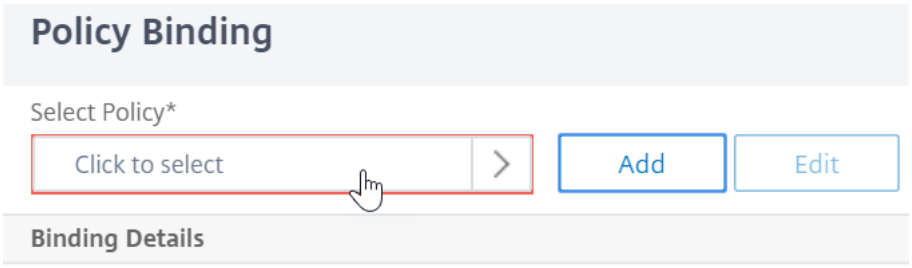
1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Virtuelle Server**. Bearbeiten Sie einen vorhandenen virtuellen Server.



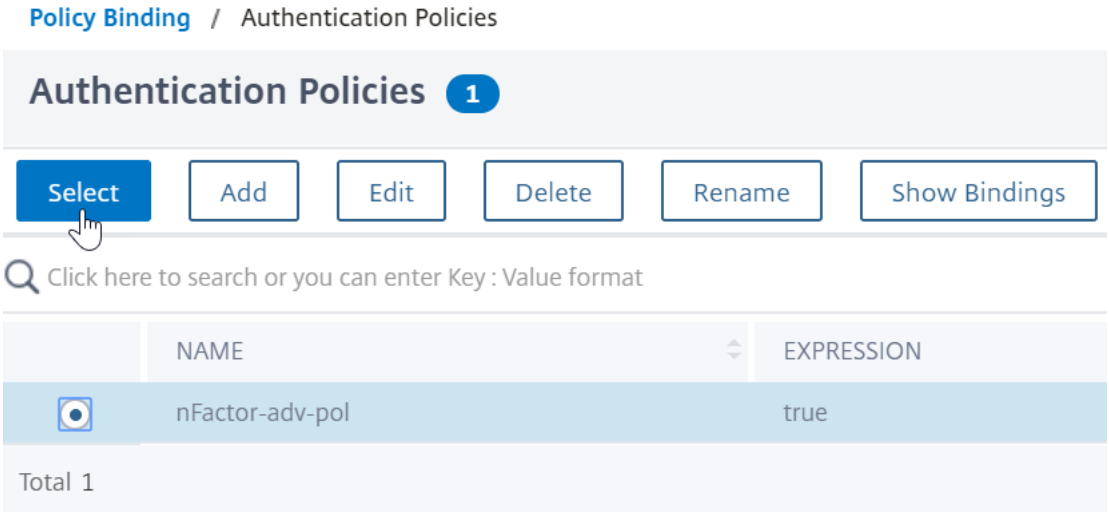
1. Klicken Sie links im Abschnitt Erweiterte Authentifizierungsrichtlinien auf **Keine Authentifizierungsrichtlinie**.



2. Klicken Sie unter **Richtlinie auswählen**auf den Text und **klicken Sie zum Auswählen**.

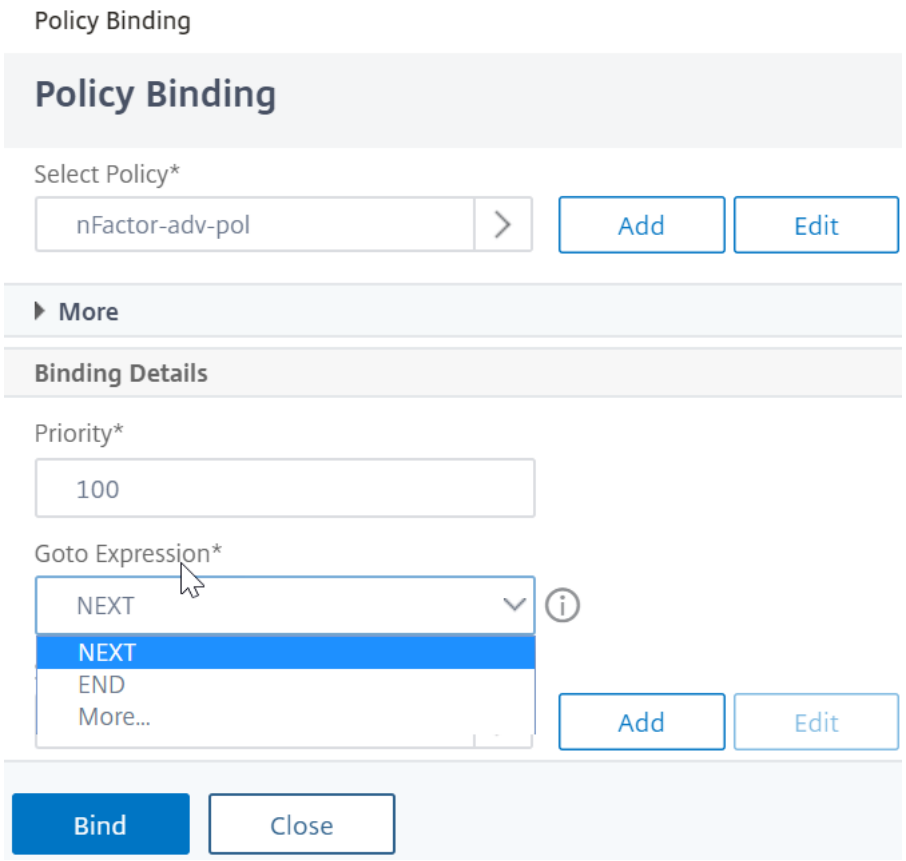


3. Klicken Sie auf das Optionsfeld neben der **erweiterten Authentifizierungsrichtlinie**und dann auf **Auswählen**.

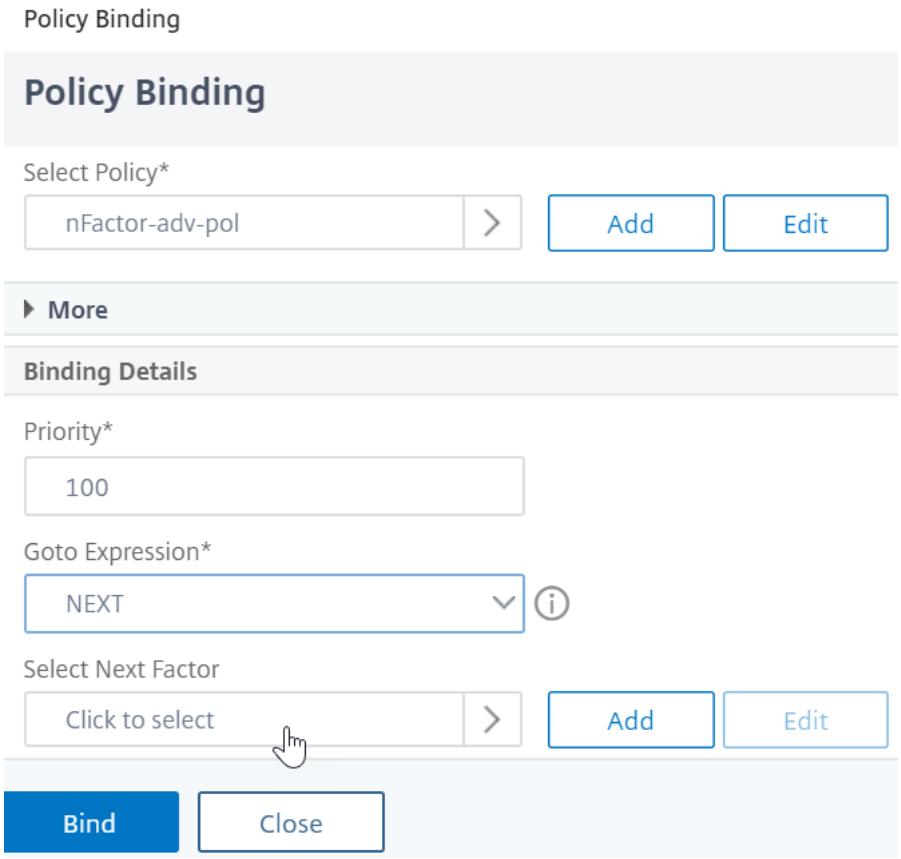


4. Im Abschnitt “Bindungsdetails” bestimmt der **Gehe zu Ausdruck**, was als Nächstes passiert, wenn diese erweiterte Authentifizierungsrichtlinie fehlschlägt.

   - Wenn **Gehe zu Ausdruck aufNEXT**festgelegt ist, wird die nächste erweiterte Authentifizierungsrichtlinie ausgewertet, die an diesen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver gebunden ist.
   - Wenn **Gehe zu Ausdruck aufEND**gesetzt ist oder wenn keine erweiterten Authentifizierungsrichtlinien mehr an diesen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver gebunden sind, wird die Authentifizierung abgeschlossen und als fehlgeschlagen markiert.



5. Unter **Nächsten Faktor auswählen**können Sie auswählen, dass auf eine Authentifizierungsrichtlinienbeschriftung verweisen kann. Der nächste Faktor wird nur bewertet, wenn die erweiterte Authentifizierungsrichtlinie erfolgreich ist. Klicken Sie abschließend auf **Bind**.



Verwenden Sie extrahierte LDAP-Gruppen, um den nächsten Authentifizierungsfaktor auszuwählen

Sie können extrahierte LDAP-Gruppen verwenden, um den nächsten Authentifizierungsfaktor ohne tatsächliche Authentifizierung mit LDAP auszuwählen.

1. Deaktivieren Sie beim Erstellen oder Bearbeiten eines LDAP-Servers oder einer LDAP-Aktion das Kontrollkästchen **Authentifizierung** .
2. Wählen Sie **unter Andere Einstellungen**die entsprechenden Werte in **Gruppenattribut** und **Unterattributname**aus.

Authentifizieren Sie das Policy Label

Wenn Sie eine erweiterte Authentifizierungsrichtlinie an den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver binden und einen nächsten Faktor ausgewählt haben, wird der nächste Faktor nur ausgewertet, wenn die erweiterte Authentifizierungsrichtlinie erfolgreich ist. Der nächste Faktor, der ausgewertet wird, ist ein Label für die Authentifizierungsrichtlinie.

Das Label der Authentifizierungsrichtlinie gibt eine Sammlung von Authentifizierungsrichtlinien für einen bestimmten Faktor an. Jedes Policy Label entspricht einem einzelnen Faktor. Es gibt auch

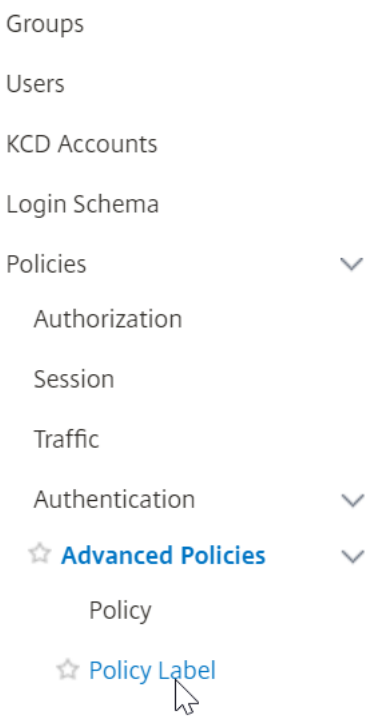
das Anmeldeformular an, das dem Benutzer vorgelegt werden muss. Die Bezeichnung der Authentifizierungsrichtlinie muss als nächster Faktor einer Authentifizierungsrichtlinie oder einer anderen Authentifizierungsrichtlinienbezeichnung gebunden sein.

Hinweis: Jeder Faktor benötigt kein Login-Schema. Das Anmeldeschemaprofil ist nur erforderlich, wenn Sie ein Anmeldeschema an ein Authentifizierungsrichtlinienlabel binden.

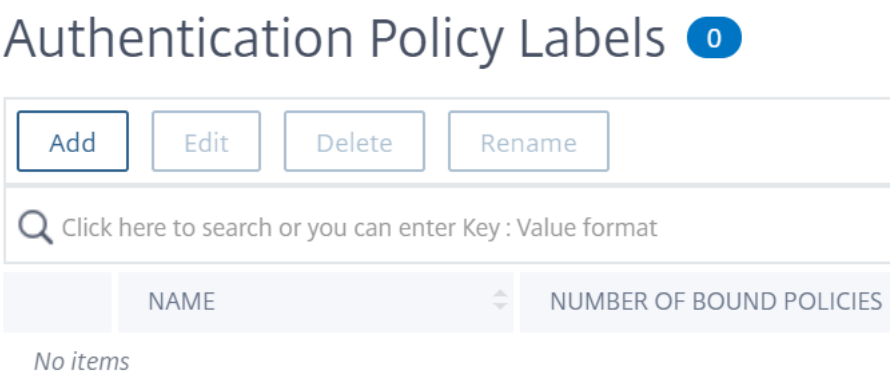
Erstellen einer Bezeichnung für die Authentifizierungsrichtlinie

Ein Policy Label gibt die Authentifizierungsrichtlinien für einen bestimmten Faktor an. Jedes Policy Label entspricht einem einzelnen Faktor. Das Policy Label gibt das Anmeldeformular an, das dem Benutzer vorgelegt werden muss. Das Policy Label muss als nächster Faktor einer Authentifizierungsrichtlinie oder einer anderen Authentifizierungsrichtlinienbezeichnung gebunden sein. In der Regel enthält ein Policy Label Authentifizierungsrichtlinien für einen bestimmten Authentifizierungsmechanismus. Sie können jedoch auch ein Policy Label haben, das Authentifizierungsrichtlinien für verschiedene Authentifizierungsmechanismen enthält.

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinienbezeichnung**.



2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

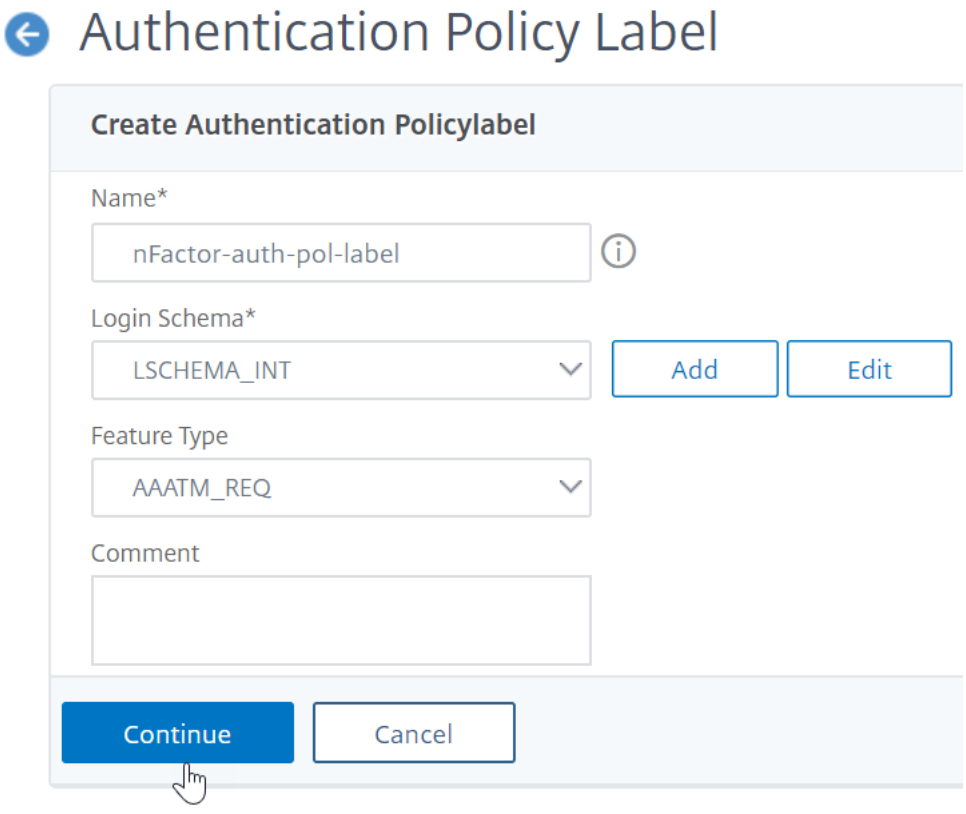


3. Füllen Sie die folgenden Felder aus, um ein Authentifizierungsrichtlinienlabel zu erstellen:

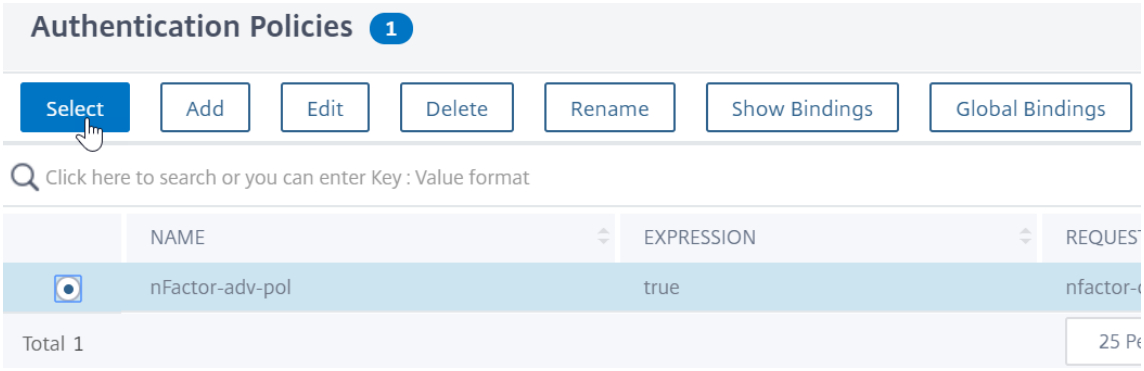
   a) Geben Sie den **Namen** für das neue Label für die Authentifizierungsrichtlinie ein.

   b) Wählen Sie das **Login-Schema** aus, das der Bezeichnung der Authentifizierungsrichtlinie WENN Sie dem Benutzer nichts anzeigen möchten, können Sie ein Anmeldeschemaprofil auswählen, das auf kein Schema festgelegt ist (LSCHEMA_INT).

   c) Klicken Sie auf " **Weiter**".



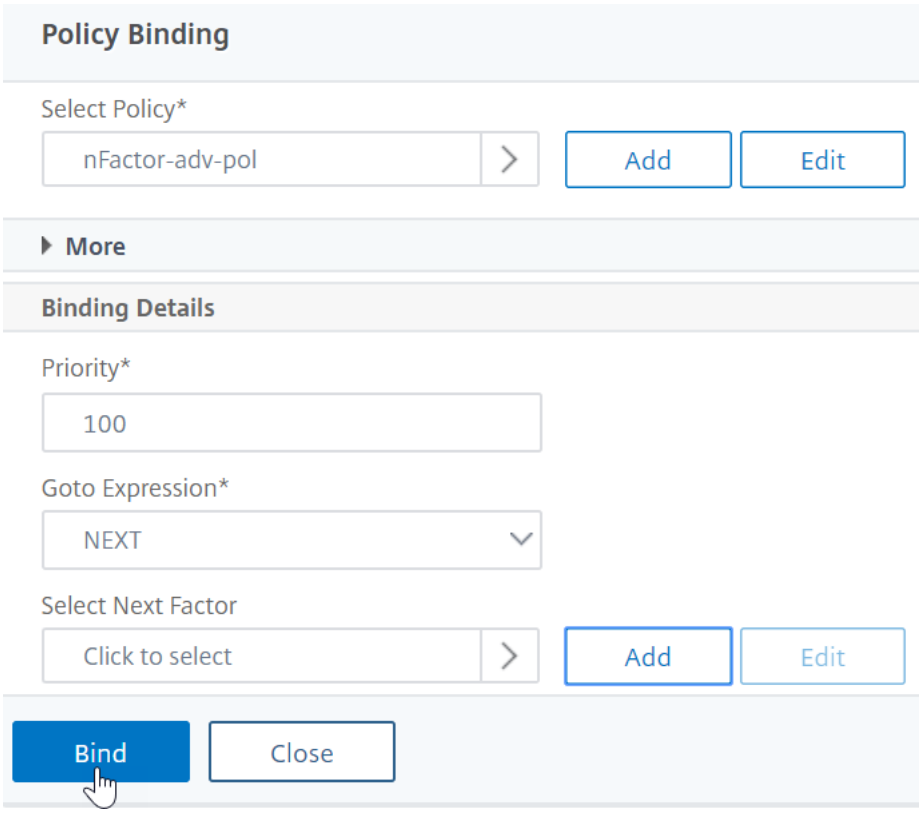
4. Klicken Sie im Abschnitt **Richtlinienbindung** auf die Stelle, an der **zum Auswählen klicken angezeigt**wird.
5. Wählen Sie die Authentifizierungsrichtlinie aus, die diesen Faktor auswertet.



6. Füllen Sie die folgenden Felder aus:

   a) Geben Sie die **Priorität** der Policy-Bindung ein.

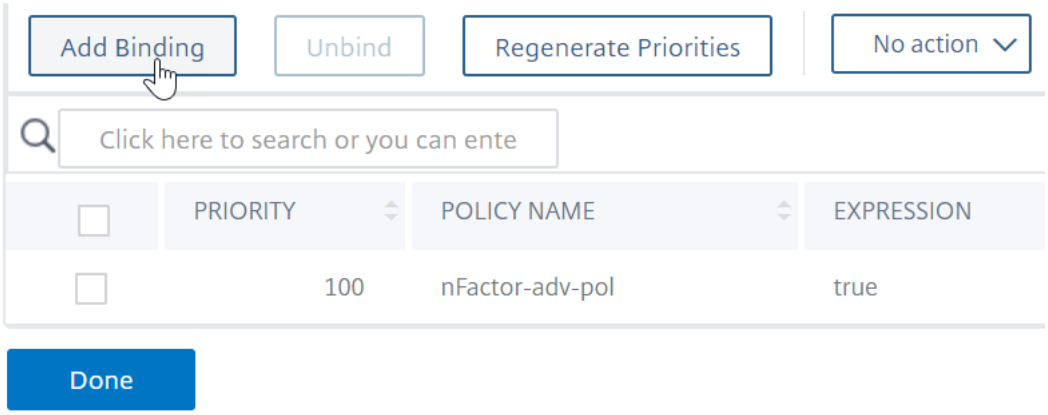
   b) Wählen Sie in **Gehe zu Ausdruck** die Option **NEXT** aus, wenn Sie erweiterte Authentifizierungsrichtlinien an diesen Faktor binden möchten, oder wählen Sie **END**.



7. Wenn Sie unter **Nächsten Faktor auswählen**einen weiteren Faktor hinzufügen möchten, klicken Sie auf, um das nächste Authentifizierungsrichtlinienlabel auszuwählen und zu binden (nächster Faktor).
   Wenn Sie den nächsten Faktor nicht auswählen und diese erweiterte Authentifizierungsrichtlinie erfolgreich ist, ist die Authentifizierung erfolgreich und abgeschlossen.

8. Klicken Sie auf **Bind**.

9. Sie können auf **Bindung hinzufügen** klicken, um dieser Richtlinienbezeichnung (Faktor) erweiterte Authentifizierungsrichtlinien hinzuzufügen. Klicken Sie nach **Abschluss auf Fertig** .



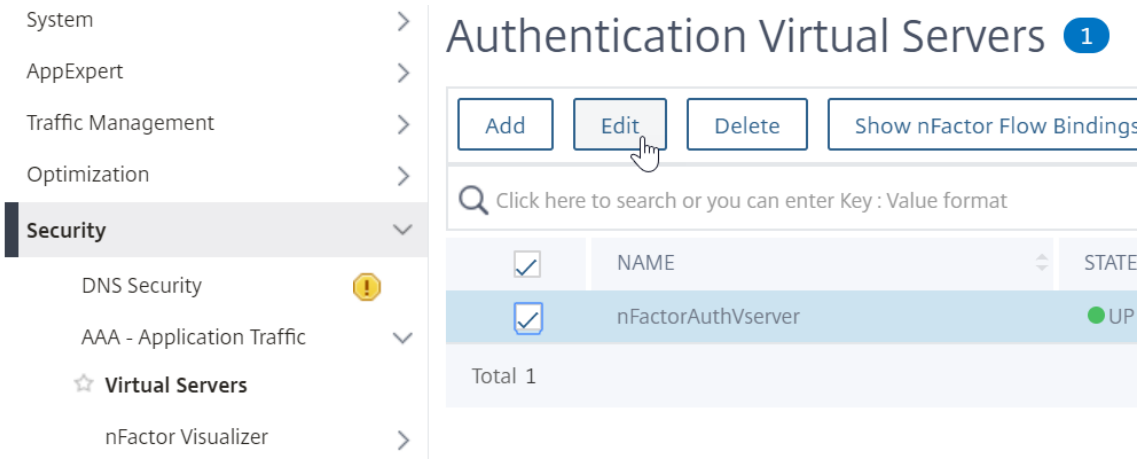
Beschriftung der Authentifizierungsrichtlinie binden

Nachdem Sie das Policy Label erstellt haben, binden Sie es an eine vorhandene erweiterte Authentifizierungsrichtlinienbindung, um die Faktoren miteinander zu verketten.

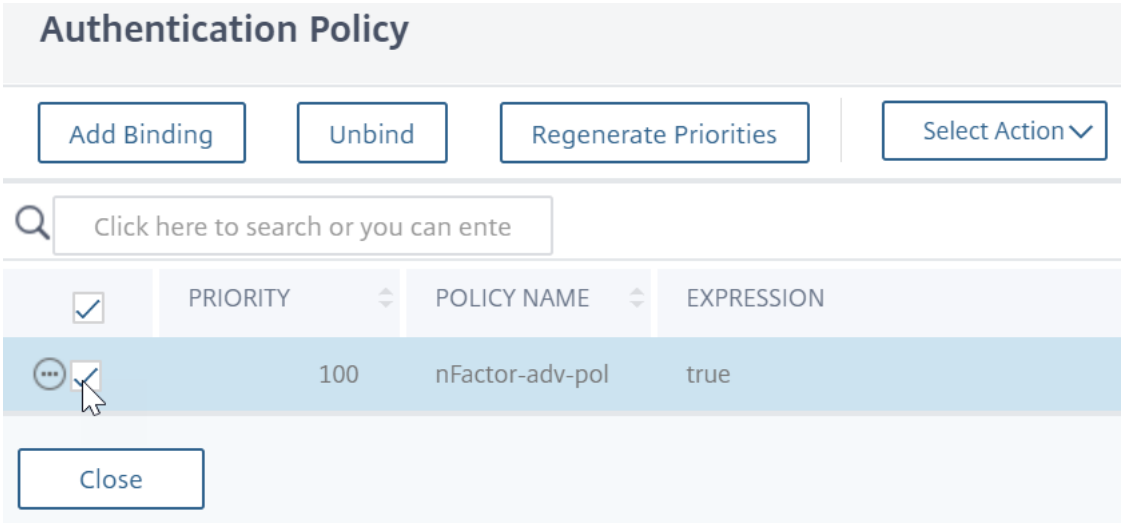
Sie können den nächsten Faktor auswählen, wenn Sie einen vorhandenen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver bearbeiten, der über eine erweiterte Authentifizierungsrichtlinie gebunden ist, oder wenn Sie eine andere Policy Label bearbeiten, um den nächsten Faktor einzubeziehen.

So bearbeiten Sie einen vorhandenen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver, an den bereits eine erweiterte Authentifizierungsrichtlinie gebunden ist

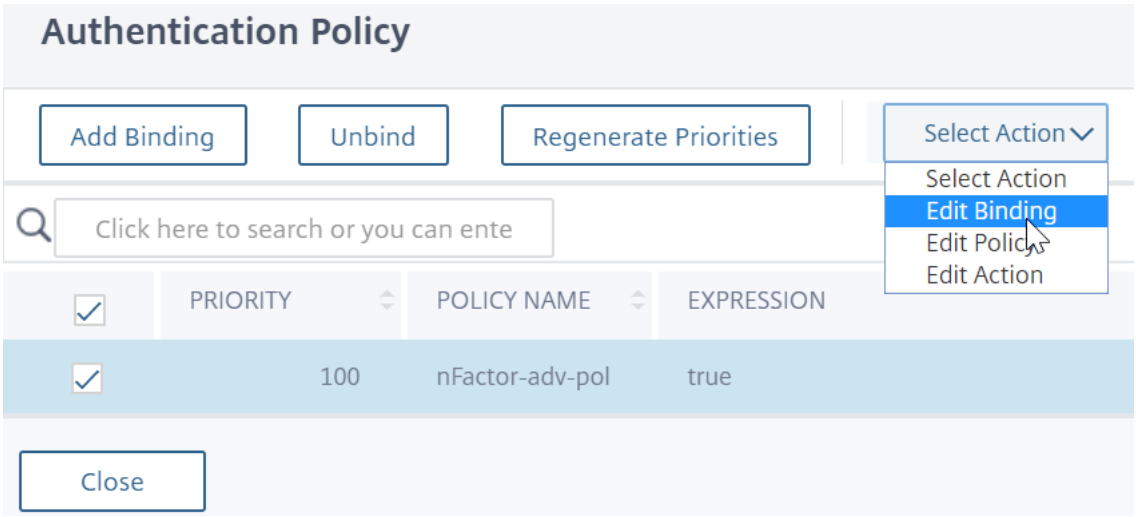
1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Virtuelle Server.** Wählen Sie den virtuellen Server aus und klicken Sie auf **Bearbeiten**.



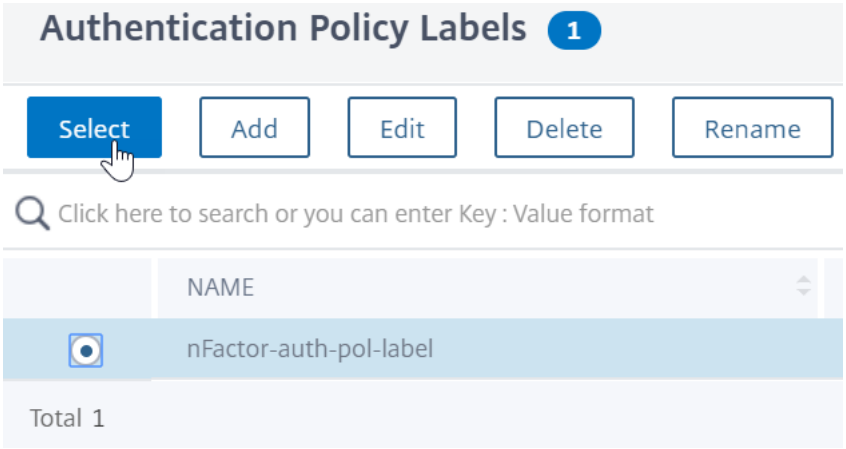
2. Klicken Sie links im Abschnitt **Erweiterte Authentifizierungsrichtlinien** auf eine bestehende Authentifizierungsrichtlinienbindung.



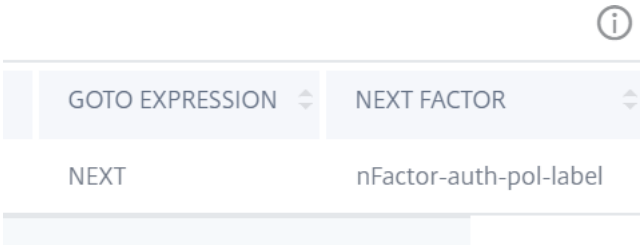
3. Klicken Sie unter **Aktion auswählen**auf **Bindung bearbeiten**.



4. Klicken Sie unter **Nächsten Faktor auswählen**auf und wählen Sie ein vorhandenes Authentifizierungsrichtlinienlabel aus (nächster Faktor).

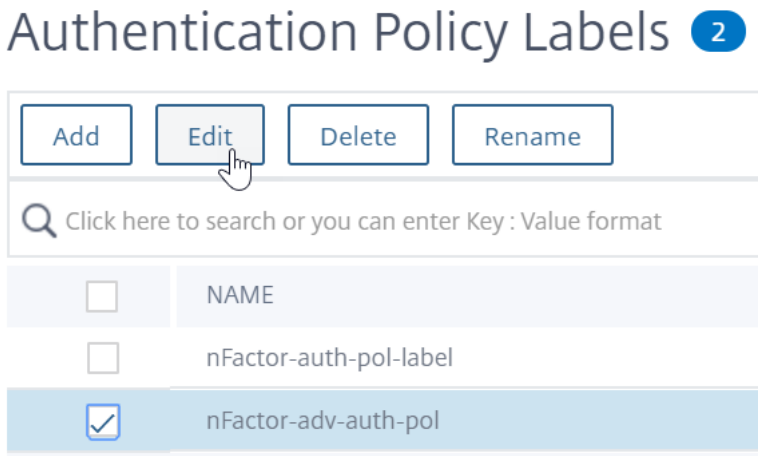


5. Klicken Sie auf **Bind**. Den nächsten Faktor sehen Sie ganz rechts.

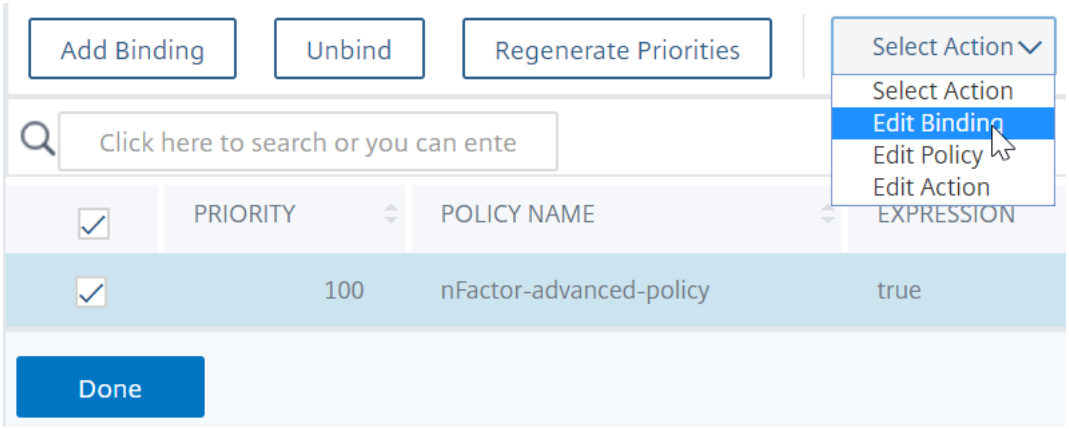


So fügen Sie eine Policy Label als nächsten Faktor zu einem anderen Policy Label hinzu

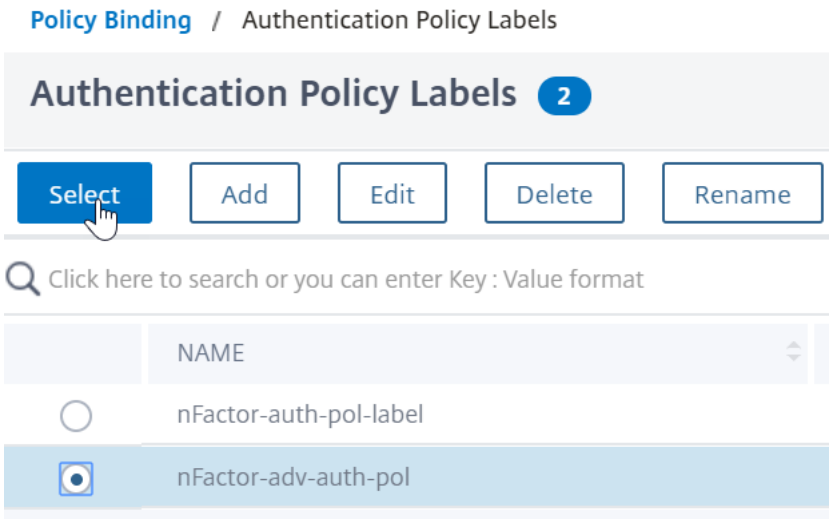
1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinienbezeichnung**. Wählen Sie ein anderes Policy Label aus und klicken Sie auf **Bearbeiten.**



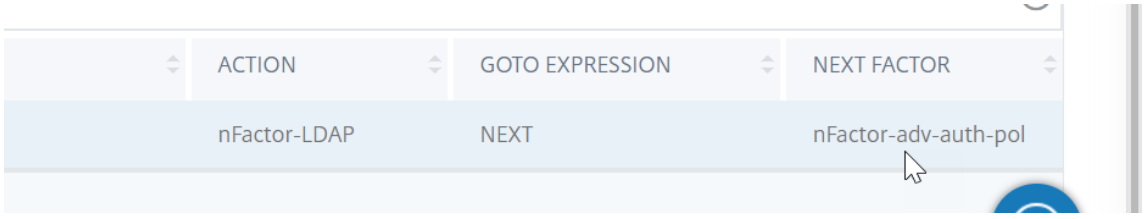
2. Klicken Sie unter **Aktion auswählen**auf **Bindung bearbeiten**.



3. Klicken **Sie unter Bindungsdetails > Nächsten Faktor**auswählen auf, um den nächsten Faktor auszuwählen.
4. Wählen Sie das Policy Label für den nächsten Faktor und klicken Sie auf die Schaltfläche **Auswählen** .



5. Klicken Sie auf **Binden.** Den nächsten Faktor sehen Sie auf der rechten Seite.

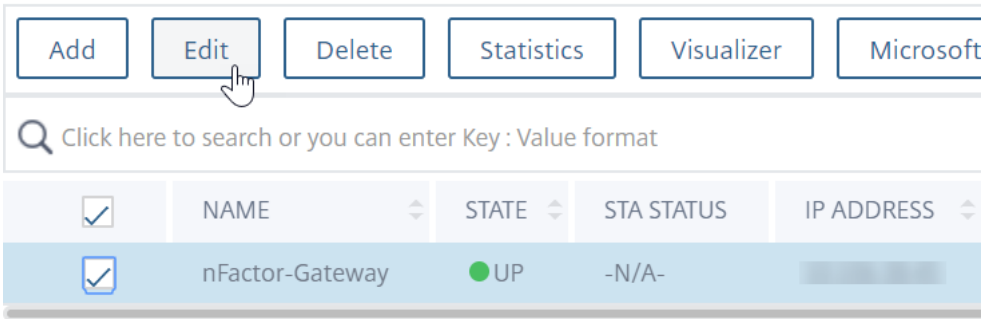


nFactor für Citrix Gateway

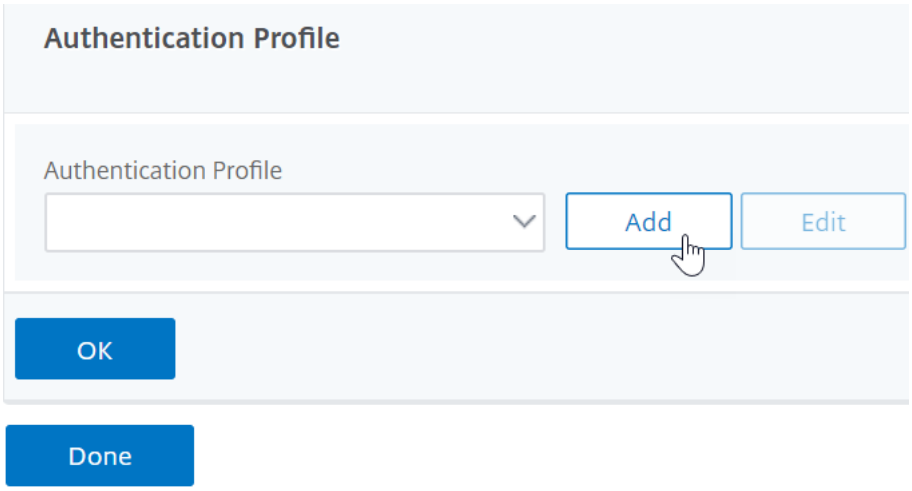
Um nFactor auf dem Citrix Gateway zu aktivieren, muss ein Authentifizierungsprofil mit einem virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver verknüpft sein.

Erstellen eines Authentifizierungsprofils, um einen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver mit dem virtuellen Citrix Gateway

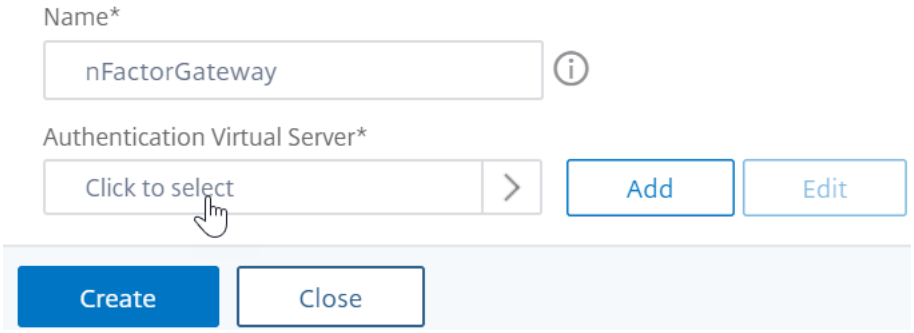
1. Navigieren Sie zu **Citrix Gateway > Virtuelle Server** und wählen Sie einen vorhandenen virtuellen Gateway-Server aus, der bearbeitet werden soll.



2. Klicken Sie in **Erweiterte Einstellungen**auf **Authentifizierungsprofil**.
3. Klicken Sie unter **Authentifizierungsprofil** auf **Hinzufügen**.

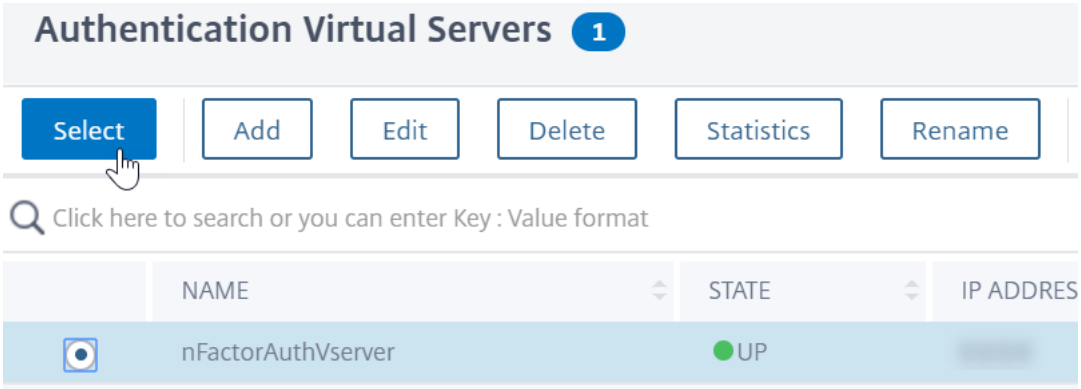


4. Geben Sie den Namen für das Authentifizierungsprofil ein und klicken Sie auf die Stelle, an der es heißt **Klicken zur Auswahl**

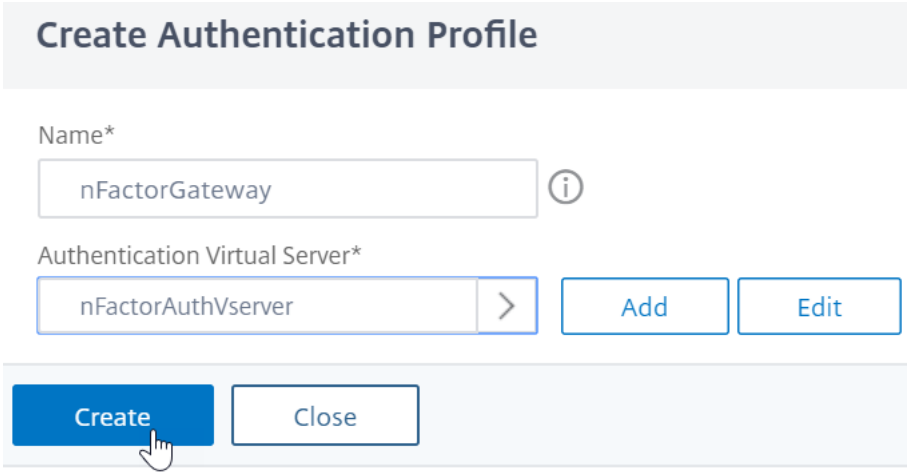


5. Wählen Sie unter **Virtueller Authentifizierungsserver** einen vorhandenen Server aus, auf dem das Anmeldeschema, eine erweiterte Authentifizierungsrichtlinie und Bezeichnun-

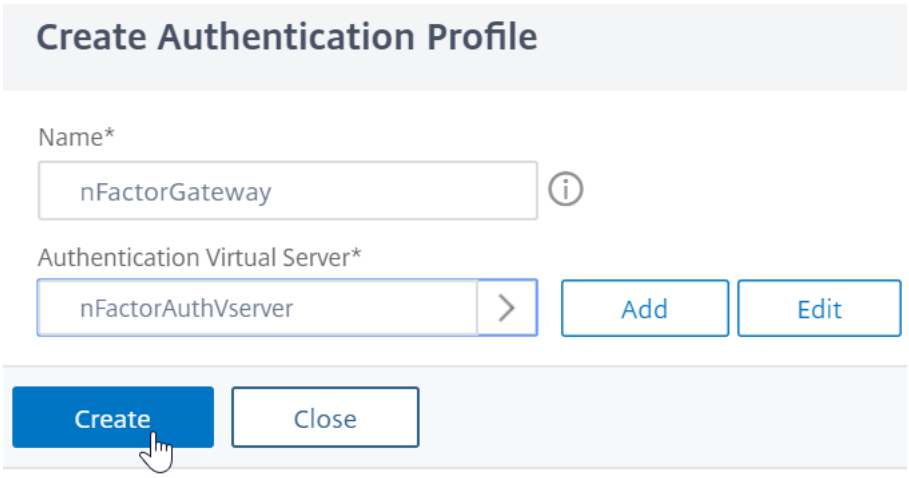
gen für Authentifizierungsrichtlinien konfiguriert sind. Sie können auch einen virtuellen Authentifizierungsserver erstellen. Der virtuelle Authentifizierungs-, Autorisierungs- und Überwachungsserver benötigt keine IP-Adresse. Klicken Sie auf **Select**.



6. Klicken Sie auf **Erstellen**.



7. Klicken Sie auf **OK** um den Abschnitt Authentifizierungsprofil zu schließen.



Hinweis: Wenn Sie einen der Faktoren als Client-Zertifikate konfiguriert haben, müssen Sie die SSL-

Parameter und das CA-Zertifikat konfigurieren.

Nachdem Sie das Authentifizierungsprofil mit einem virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver verknüpft haben und wenn Sie zu Ihrem Citrix Gateway navigieren, können Sie die nFactor-Authentifizierungsbildschirme anzeigen.

Konfigurieren von SSL-Parametern und CA-Zertifikat

Wenn einer der Authentifizierungsfaktoren ein Zertifikat ist, müssen Sie eine SSL-Konfiguration auf dem virtuellen Citrix Gateway-Server durchführen.

1. Navigieren Sie zu **Traffic Management > SSL > Certificates > CA Certificates**, und installieren Sie das Stammzertifikat für den Aussteller der Clientzertifikate. Zertifikate von Certificate Authority benötigen keine Schlüsseldateien.

   Wenn Standard-SSL-Profile aktiviert sind, haben Sie bereits ein SSL-Profil erstellt, für das die Clientauthentifizierung aktiviert ist.

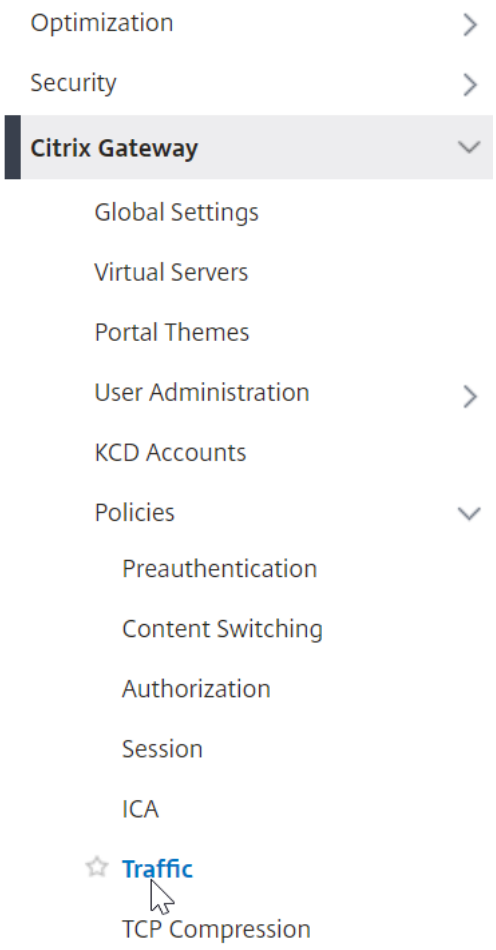
2. Navigieren Sie zu **Citrix Gateway > Virtuelle Server**, und bearbeiten Sie einen vorhandenen virtuellen Citrix Gateway-Server, der für nFactor aktiviert ist.
   - Wenn Standard-SSL-Profile aktiviert sind, klicken Sie auf das Bearbeitungssymbol.
   - Wählen Sie in der Liste SSL-Profil das SSL-Profil aus, für das die Clientauthentifizierung aktiviert und auf OPTIONAL festgelegt ist.
   - Wenn Standard-SSL-Profile nicht aktiviert sind, klicken Sie auf das Bearbeitungssymbol.
   - Aktivieren Sie das Kontrollkästchen Clientauthentifizierung.
   - Stellen Sie sicher, dass das Clientzertifikat auf Optional festgelegt ist
3. Klicken Sie auf OK.
4. Klicken Sie im Abschnitt Zertifikate auf **Kein CA-Zertifikat.**
5. Klicken Sie unter Select CA Certificate auf, um das Stammzertifikat für den Aussteller der Clientzertifikate auszuwählen und auszuwählen.
6. Klicken Sie auf Bind.

Hinweis: Möglicherweise müssen Sie auch alle Zwischen-CA-Zertifikate binden, die die Clientzertifikate ausgestellt haben.

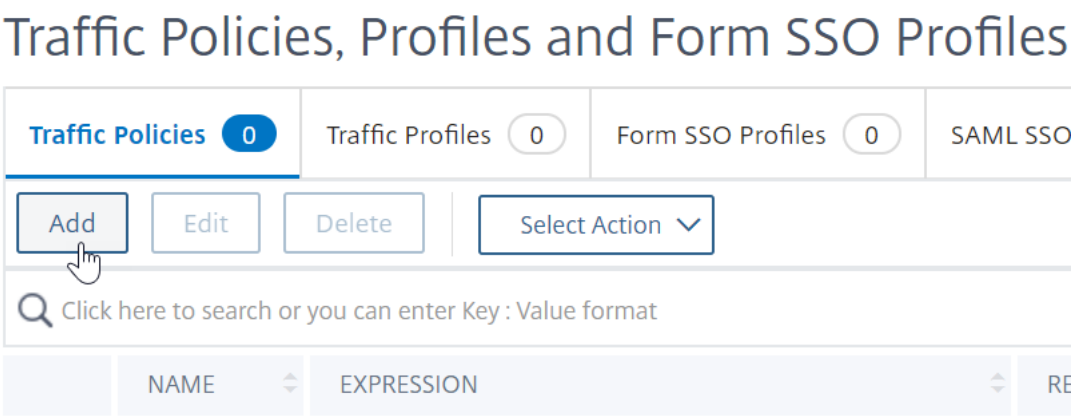
Konfigurieren der Citrix Gateway-Verkehrsrichtlinie für nFactor Single Sign-On bei StoreFront

Für die einmalige Anmeldung bei StoreFront verwendet nFactor standardmäßig das zuletzt eingegebene Kennwort. Wenn LDAP nicht das zuletzt eingegebene Kennwort ist, müssen Sie eine Verkehrsrichtlinie/ein Profil erstellen, um das standardmäßige nFactor-Verhalten zu überschreiben.

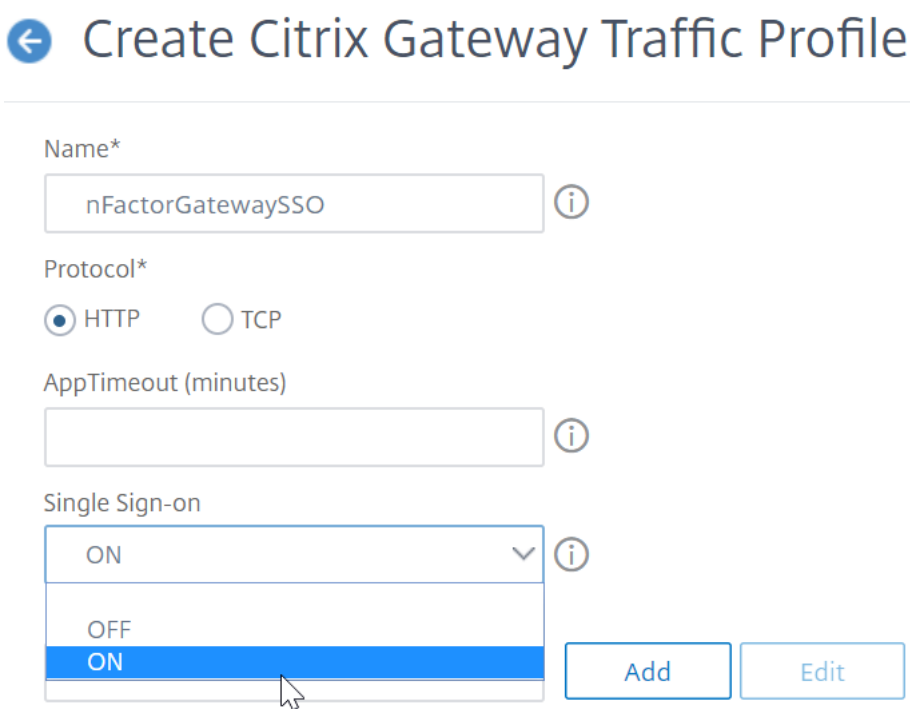
1. Navigieren Sie zu **Citrix Gateway > Richtlinien > Verkehr**.



2. Klicken Sie auf der Registerkarte **Verkehrsprofile** auf **Hinzufügen**.

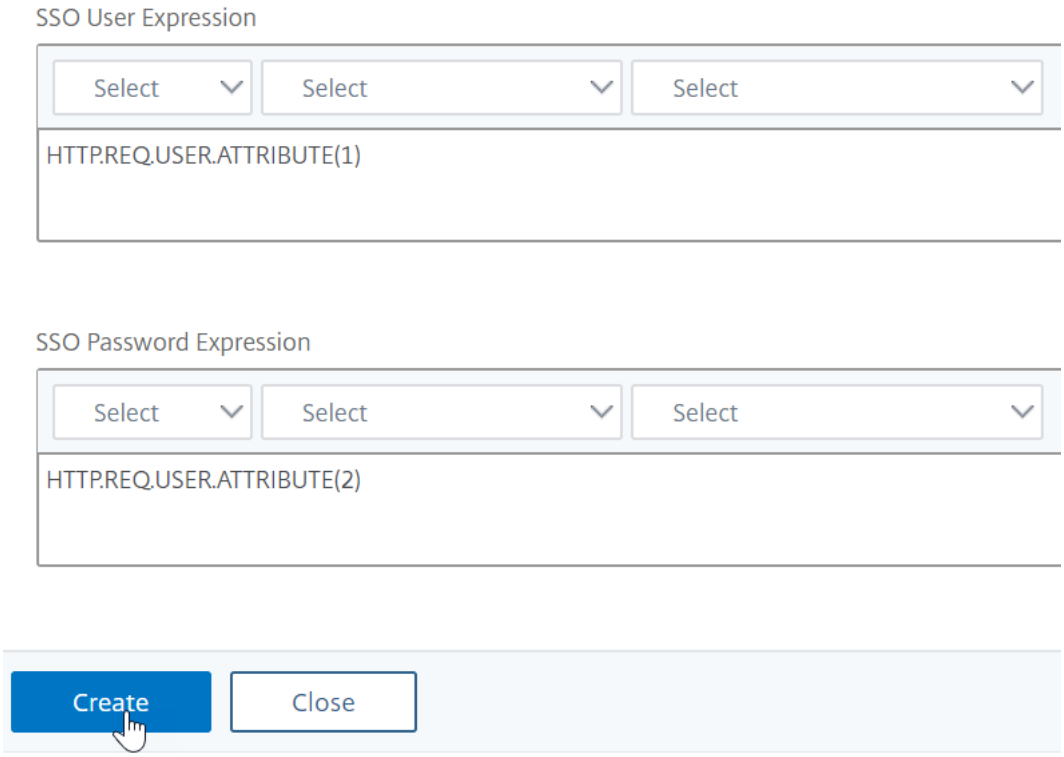


3. Geben Sie einen Namen für das Verkehrsprofil ein. Wählen Sie das **HTTP-Protokoll** aus. Wählen Sie unter **Einmaliges Anmelden** die Option **ON** aus.



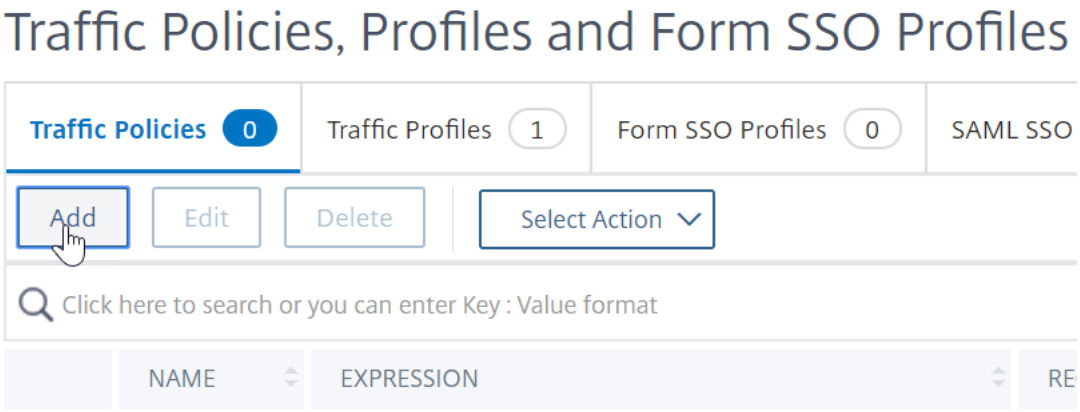
4. Geben Sie im **SSO-Ausdruck**einen AAA.USER.ATTRIBUTE (#) -Ausdruck ein, der den im Anmeldeschema angegebenen Indizes entspricht, und klicken Sie auf **Erstellen**.

> **Hinweis**
> Der AAA.USER-Ausdruck ist jetzt implementiert, um die veralteten HTTP.REQ.USER-Ausdrücke zu ersetzen.



5. Klicken Sie auf **die Registerkarte Verkehrsrichtlinien** und dann auf **Hinzufügen**.

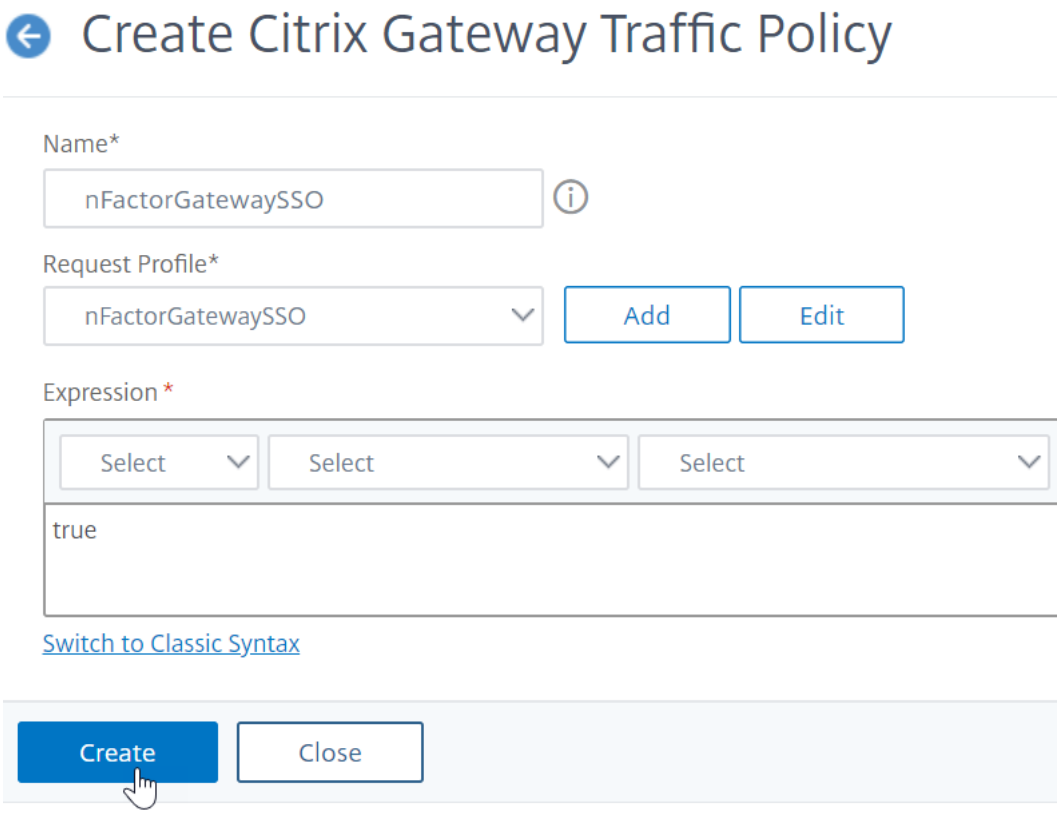
   Geben Sie einen Namen für die Richtlinie ein.
   Wählen Sie das im vorherigen Schritt erstellte Verkehrsprofil aus.
   Geben Sie unter **Ausdruck** einen erweiterten Ausdruck ein, z. B. wahr.
   Klicken Sie auf **Erstellen**.



6. Navigieren Sie zu **Citrix Gateway > Citrix Gateway Virtual Server**.

   - Wählen Sie einen vorhandenen virtuellen Server aus und klicken Sie auf **Bearbeiten**.
   - Klicken Sie im Abschnitt **Richtlinien** auf das **+-Zeichen**.
   - Wählen Sie unter **Richtlinie wählen** die Option **Traffic** aus.
   - Wählen Sie unter **Typ wählen** die Option **Anfrage** aus.

- Wählen Sie die von Ihnen erstellte Traffic-Richtlinie aus und klicken Sie dann auf **Bind**.



Beispiel-Snippet zur nFactor-Konfiguration über die Citrix ADC CLI

Um die schrittweisen Konfigurationen für die nFactor-Authentifizierung zu verstehen, sollten wir eine Zwei-Faktor-Authentifizierungsbereitstellung in Betracht ziehen, bei der der erste Faktor die LDAP-Authentifizierung und der zweite Faktor die RADIUS-Authentifizierung ist.

Bei dieser Beispielbereitstellung muss sich der Benutzer mit einem einzigen Anmeldeformular bei beiden Faktoren anmelden. Daher definieren wir ein einziges Anmeldeformular, das zwei Kennwörter akzeptiert. Das erste Kennwort wird für die LDAP-Authentifizierung und das andere für die RADIUS-Authentifizierung verwendet.
Hier sind die Konfigurationen, die ausgeführt werden:

1. Konfigurieren des virtuellen Lastausgleichsservers für die Authentifizierung

   add lb vserver lbvs89 HTTP 1.136.19.55 80 -AuthenticationHost auth56.aaatm.com -Authentication ON

2. Konfigurieren Sie den virtuellen Authentifizierungsserver.

   add authentication vserver auth56 SSL 10.106.30.223 443 -AuthenticationDomain aaatm.com

3. Konfigurieren Sie das Anmeldeschema für das Anmeldeformular und binden Sie es an eine Richtlinie für das Anmeldeschema.

add authentication loginSchema login1 -authenticationSchema login-2passwd.xml -userCredentialIndex 1 -passwordCredentialIndex 2

Hinweis:

Verwenden Sie den Benutzernamen und eines der Kennwörter, die im Anmeldeschema für Single Sign-On (SSO) für einen Back-End-Dienst eingegeben wurden, z. B. StoreFront. Sie können diese Indexwerte in der Verkehrsaktion referenzieren, indem Sie den Ausdruck AAA.USER.ATTRIBUTE (#) verwenden. Die Werte können zwischen 1 und 16 liegen.

Alternativ können Sie die im Anmeldeschema eingegebenen Anmeldeinformationen als Single Sign-On-Anmeldeinformationen verwenden, indem Sie den folgenden Befehl verwenden.

```
1 add authentication loginSchema login1 -authenticationSchema login
     -2passwd.xml -SSOCredentials YES
2
3  add authentication loginSchemaPolicy login1 -rule true -action
      login1
4 <!--NeedCopy-->
```

4. Konfigurieren Sie ein Anmeldeschema für den Passthrough und binden Sie es an ein Policy Label

```
1 add authentication loginSchema login2 -authenticationSchema
     noschema
2
3 add authentication policylabel label1 -loginSchema login2
4 <!--NeedCopy-->
```

5. Konfigurieren Sie die LDAP- und RADIUS-Richtlinien.

```
1 add authentication ldapAction ldapAct1 -serverIP 10.17.103.28 -
     ldapBase "dc=aaatm, dc=com" -ldapBindDn administrator@aaatm.com
      -ldapBindDnPassword 81
     qw1b99ui971mn1289op1abc12542389b1f6c111n0d98e1d78ae90c8545901 -
     encrypted -encryptmethod ENCMTHD_3 -ldapLoginName
     samAccountName -groupAttrName memberOf -subAttributeName CN
2
3 add authentication Policy ldap -rule true -action ldapAct1
4
5 add authentication radiusAction radius -serverIP 10.101.14.3 -
     radKey
```



```
    n231d9a8cao8671or4a9ace940d8623babca0f092gfv4n5598ngc40b18876hj32
     -encrypted -encryptmethod ENCMTHD_3 -radNASip ENABLED -
    radNASid NS28.50 -radAttributeType 11 -ipAttributeType 8

add authentication Policy radius -rule true -action radius
<!--NeedCopy-->
```

6. Binden Sie die Richtlinie für das Anmeldeschema an den virtuellen Authentifizierungsserver

```
bind authentication vserver auth56 -policy login1 -priority 1 -
    gotoPriorityExpression END
<!--NeedCopy-->
```

7. Binden Sie die LDAP-Richtlinie (erster Faktor) an den virtuellen Authentifizierungsserver.

```
bind authentication vserver auth56 -policy ldap -priority 1 -
    nextFactor label1 -gotoPriorityExpression next
<!--NeedCopy-->
```

8. Binden Sie die RADIUS-Richtlinie (zweiter Faktor) an die Bezeichnung der Authentifizierungsrichtlinie.

```
bind authentication policylabel label1 -policyName radius -
    priority 2 -gotoPriorityExpression end
<!--NeedCopy-->
```

nFactor Visualizer für vereinfachte Konfiguration

February 24, 2022

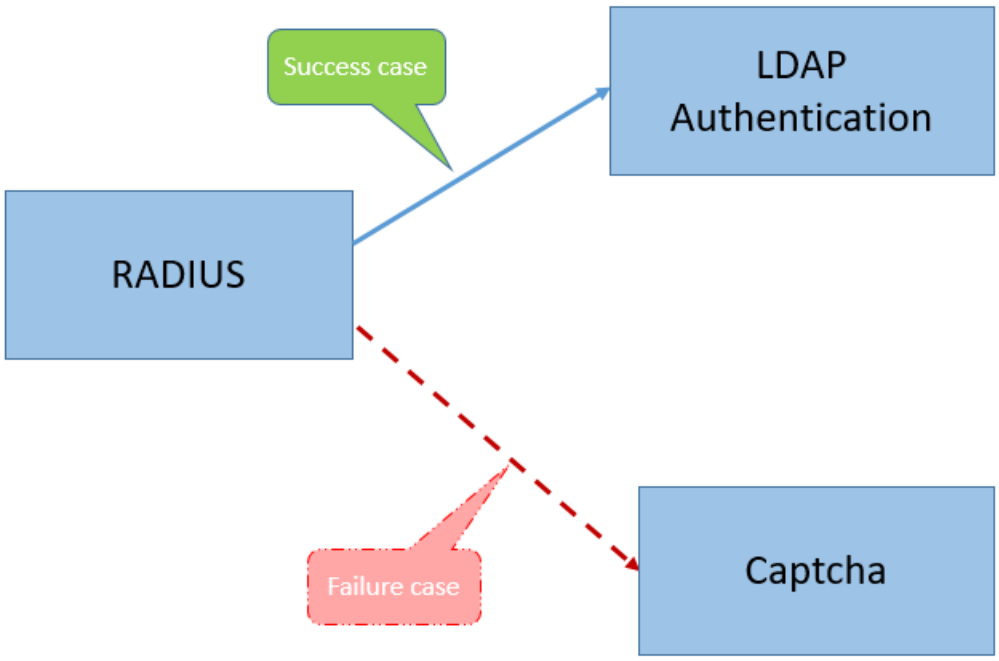
Ausgehend von Citrix ADC Release 13.0 Build 36.27 wird die nFactor Konfiguration über die GUI durch die Verwendung des nFactor Visualizer vereinfacht. Der nFactor Visualizer hilft Administratoren, mehrere Faktoren hinzuzufügen, ohne den Überblick über jeden Faktor zu verlieren. Die Gruppe von Faktoren, die im Fluss erstellt werden, wird an einer Stelle angezeigt. Administratoren können Authentifizierungserfolgs- und Fehlerpfade separat hinzufügen. Nach dem Erstellen des Flows müssen Administratoren den nFactor-Flow an einen virtuellen Authentifizierungsserver binden.

> **Hinweis:**
>
> - Alle Faktoren, die von einem Administrator im nFactor-Flow erstellt werden, werden für jede zukünftige Verwendung beibehalten.
> - Ab Citrix ADC Feature Release 13.0 Build 64.35 und höher können Sie mit dem nFactor Visualizer den nFactor-Flow mit einem Entscheidungsblock starten.

Zuvor war die Konfiguration von nFactor umständlich, wobei die Administratoren viele Seiten besuchen mussten, um sie zu konfigurieren. Wenn eine Änderung erforderlich war, mussten die Administratoren die konfigurierten Abschnitte jedes Mal erneut besuchen. Außerdem gab es keine Möglichkeit, die vollständige Konfiguration an einem Ort anzuzeigen.

Anwendungsfall 1: RADIUS gefolgt von LDAP-Authentifizierung, andernfalls Fallback auf Captcha über nFactor Visualizer

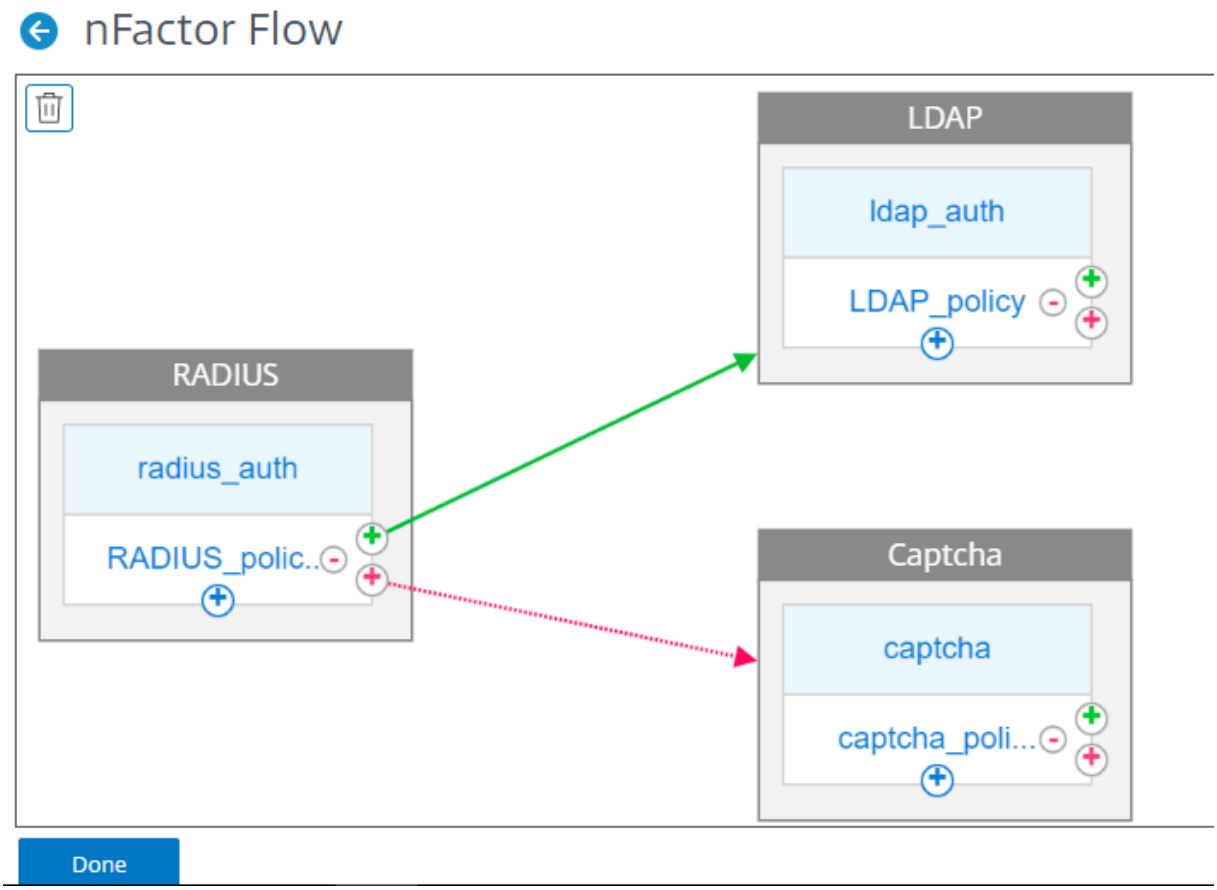
Erreichen Sie die RADIUS-Authentifizierung als Authentifizierung der ersten Ebene, gefolgt von der LDAP-Authentifizierung. Falls RADIUS fehlschlägt, muss die Authentifizierung auf Captcha zurückgreifen.



Um diesen Anwendungsfall zu erreichen, können Sie den nFactor Visualizer verwenden. Der Visualizer bietet verschiedene Steuerelemente, die verwendet werden können, um diesen Fluss und die zugehörigen Elemente hinzuzufügen.

Die folgende Abbildung zeigt den nFactor-Fluss, der für den zuvor erwähnten Anwendungsfall mithilfe

des Visualizers erstellt wurde.

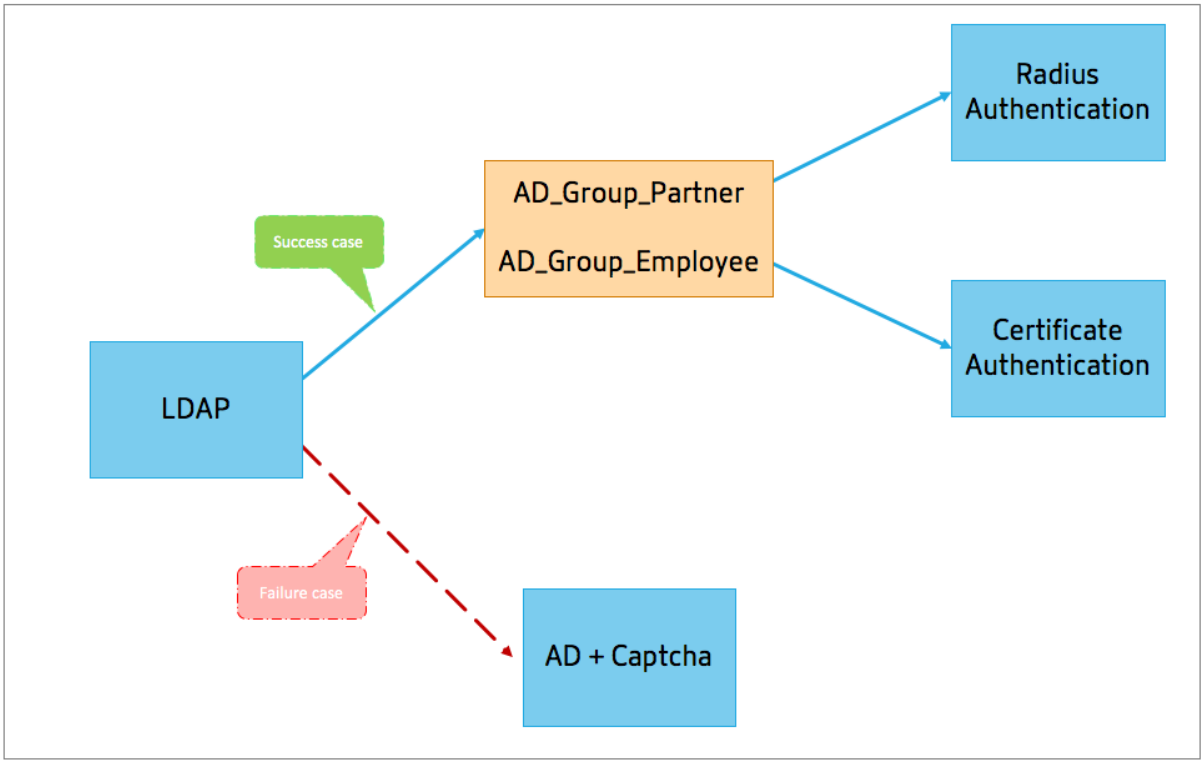


- **RADIUS.** Sie konfigurieren RADIUS als ersten Faktor. Fügen Sie ein Anmeldeschema und eine Richtlinie hinzu. In diesem Beispiel sind radius_auth und radius_policy das hinzugefügte Anmeldeschema und -richtlinie. Für die Radius_Policy können Sie einen weiteren Faktor für den Erfolgsfall hinzufügen. In diesem Beispiel wird ein LDAP-Faktorblock für den Erfolgsfall hinzugefügt. Für den Fehlerfall können Sie einen Captcha-Faktor hinzufügen.
- **LDAP.** Sie konfigurieren die LDAP-Authentifizierung als zweiten Faktor. Fügen Sie ein Anmeldeschema und eine Richtlinie hinzu. In diesem Beispiel sind ldap_auth und ldap_policy das Login-Schema und die Richtlinie, die hinzugefügt wird.
- **Captcha.** Für den RADIUS-Richtlinienfehler erstellen Sie einen Captcha-Faktor. In diesem Beispiel sind captcha und captcha_policy das Login-Schema und die Richtlinie, die hinzugefügt wird.

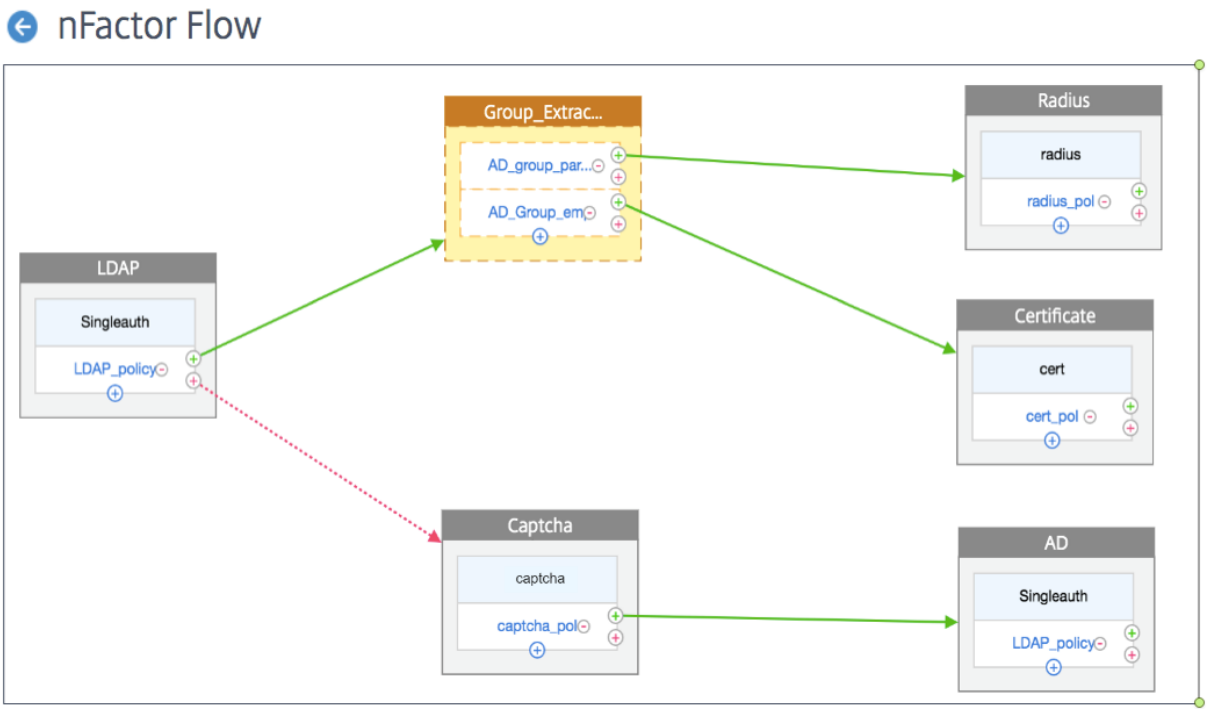
Anwendungsfall 2: LDAP gefolgt von RADIUS/Zertifikatauthentifizierung mit Captcha basierend auf LDAP-Gruppenmitgliedschaft über nFactor Visualizer

Erreichen Sie die RADIUS-Authentifizierung als Authentifizierung der ersten Ebene, gefolgt von der LDAP-Authentifizierung. Falls RADIUS fehlschlägt, muss die Authentifizierung auf Captcha zurück-

greifen.



Die folgende Abbildung zeigt den nFactor-Fluss, der für den zuvor erwähnten Anwendungsfall mithilfe des Visualizers erstellt wurde.



- **LDAP.** LDAP wird als erster Faktor konfiguriert. Fügen Sie ein Anmeldeschema und eine

Richtlinie hinzu. In diesem Beispiel sind SingleAuth und ldap_policy das Login-Schema und die Richtlinie, die hinzugefügt wird. Für die LDAP_Policy können Sie einen weiteren Faktor für den Erfolgsfall hinzufügen. In diesem Beispiel wird ein Entscheidungsblock für den Erfolgsfall hinzugefügt. Für den Fehlerfall können Sie Captcha gefolgt von AD-Faktor hinzufügen.

- **Gruppenextraktion LDAP.** Wird der Entscheidungsblock für den LDAP-Erfolgsfall hinzugefügt. Der Entscheidungsblock wird als Verzweigungsfaktor verwendet, um die Benutzer basierend auf den Richtlinienregeln zu verzweigen. Visualizer ermöglicht die Konfiguration nur einer NO_AUTHN-Richtlinie für den Entscheidungsblock.

  In diesem Beispiel ist Group_Extraction_LDAP der Entscheidungsblock. Sie fügen diesem Entscheidungsblock zwei Richtlinien (`AD_Group_Partner and AD_Group_Employee`) hinzu. Wie in den Anwendungsfällen erläutert, verwenden alle Anforderungen, die über die Richtlinie AD_group_partner weitergeleitet werden, die RADIUS-Authentifizierung. Daher verbinden Sie den Erfolgsfall dieser Richtlinie mit dem nächsten Faktor, der RADIUS-Faktor ist. Ebenso verwenden alle Anforderungen, die über die Richtlinie AD_group_Employee weitergeleitet werden, die Zertifizierungsauthentifizierung. Daher verbinden Sie den Erfolgsfall dieser Richtlinie mit dem nächsten Faktor, der der Zertifizierungsauthentifizierungsfaktor ist.

  - **RADIUS.** Für den Erfolgsfall der Richtlinie AD_group_Partner erstellen Sie den RADIUS-Authentifizierungsfaktor.
  - **Zertifikat.** Für den Erfolgsfall AD_group_Employee Policy erstellen Sie den Zertifikatauthentifizierungsfaktor.

- **Captcha.** Für den LDAP-Richtlinienfehler erstellen Sie zwei nächste Faktoren, Captcha und AD-Faktor.

> **Hinweis:**
>
> - Wenn Sie einen Anwendungsfall haben, um als erstes zu verzweigen, können Sie entweder zwei Flows erstellen und separat binden oder einen Flow mit dem ersten als Zweig out erstellen und an den virtuellen Server binden.
> - Wenn Sie mehrere Blöcke haben und den gesamten Flow im nFactor Flow-Bildschirm anzeigen möchten, klicken Sie auf den Visualizer und ziehen Sie den Flow nach ganz links.
> - Citrix empfiehlt, die nFactor-Flows nur mit der Seite nFactor Flows zu ändern.

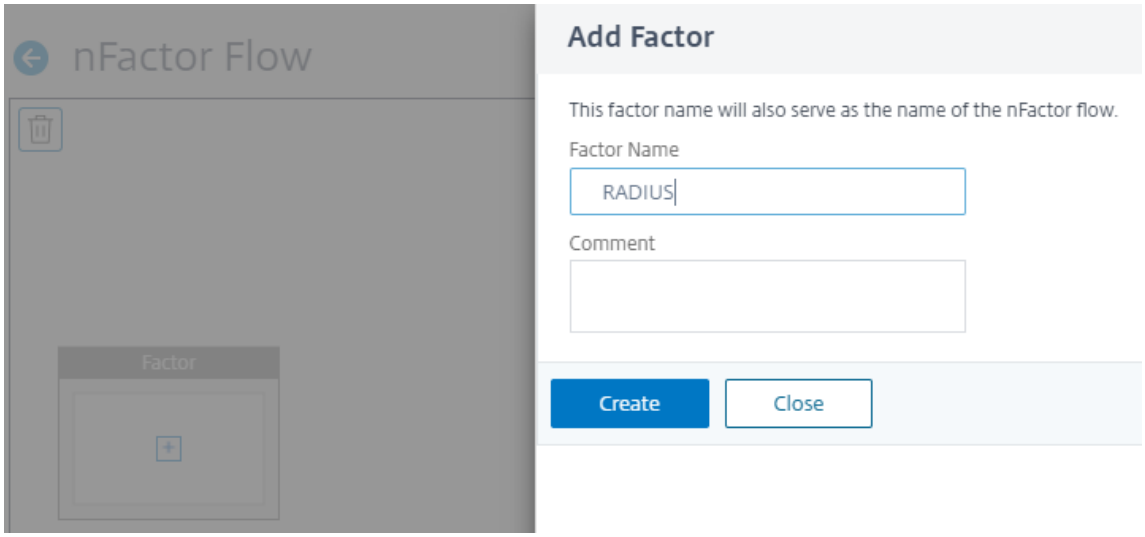
So konfigurieren Sie nFactor mithilfe des nFactor Visualizers

> **Hinweis**
>
> Die folgende nFactor-Konfiguration ist ein einfaches Beispiel, mit dem Sie die Szenariokonfigurationen für Anwendungsfall 1 durchführen können.

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > nFactor Visualizer > nFactor Flows**.

2. Klicken Sie auf **Hinzufügen**.
3. Klicken Sie auf der Seite **nFactor Flows** auf **+**, um einen ersten Faktor für den Flow hinzuzufügen. Der erste Faktor dient auch als Bezeichner für diesen nFactor Fluss.

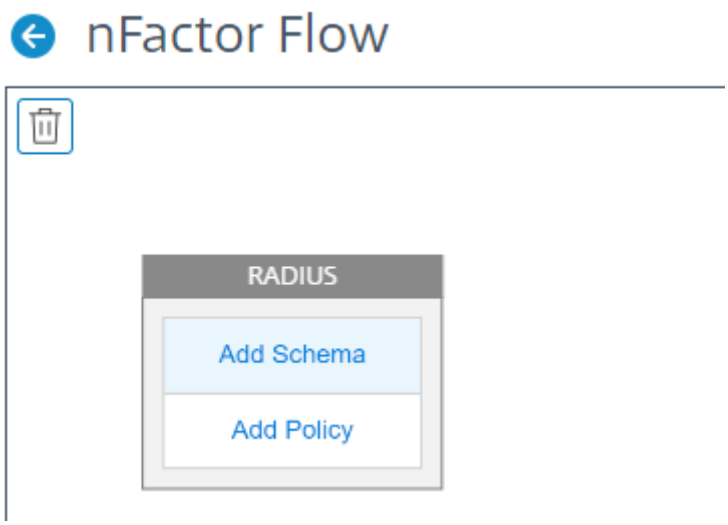
4. Geben Sie den Faktornamen ein, und klicken Sie auf **Erstellen**.



Der Faktorname wird im Faktorblock auf der Seite nFactor Flow angezeigt.

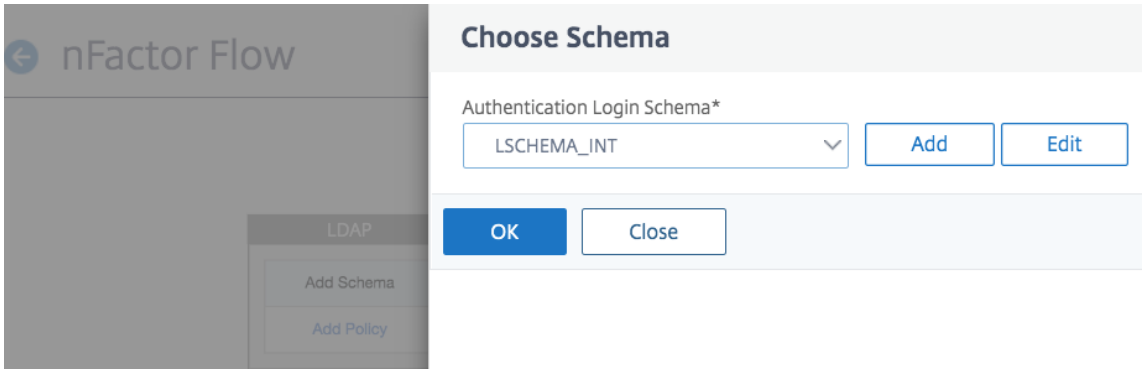
> **Hinweis**
>
> Citrix empfiehlt, dass Sie keine Richtlinienbeschriftungsnamen wie,`__root`und`__<flow_name>`als Suffix und`_db_`als Präfix verwenden dürfen. Es wird als Faktornamen verwendet, die im nFactor-Flow erstellt werden.

5. Sobald der RADIUS-Faktor erstellt wurde, müssen die Richtlinie Schema hinzufügen und Richtlinie hinzufügen erstellt werden.

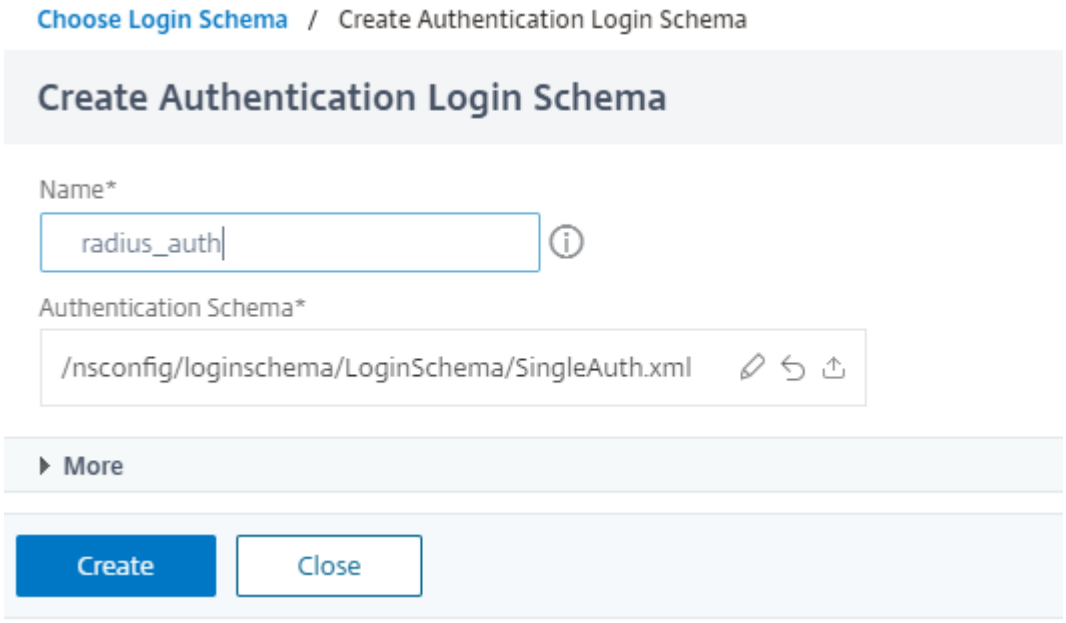


> **Hinweis:**
>
> Weitere Informationen finden Sie unter nFactor-Konzepte, Entitäten und Terminologie

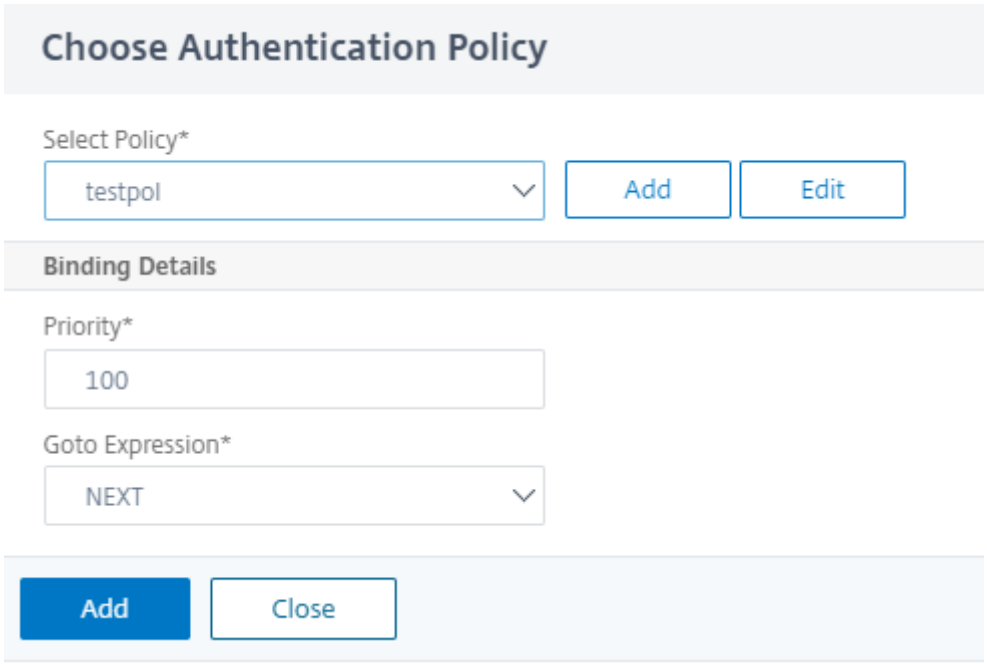
6. Klicken Sie auf **Schema hinzufügen**. Sie können entweder ein neues Anmeldeschema hinzufügen oder ein vorhandenes Anmeldeschema aus der Liste **Authentifizierungsanmeldeschema** auswählen.



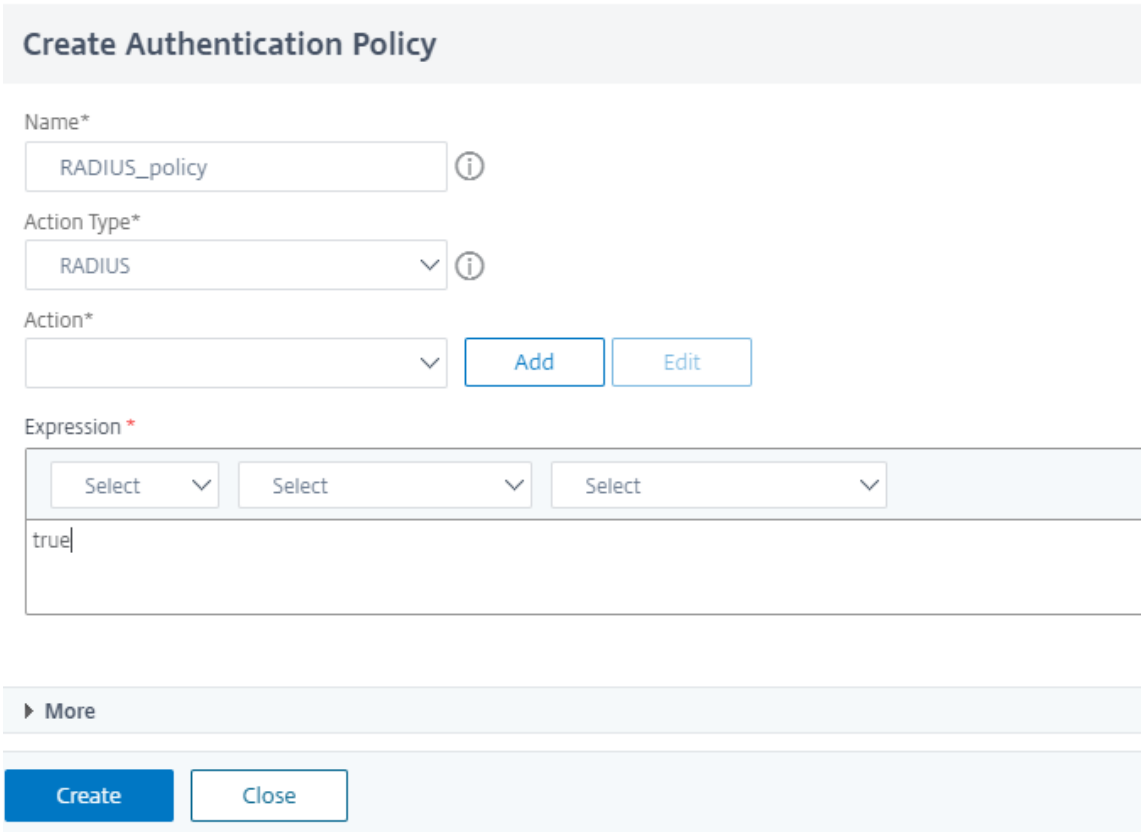
7. Um ein Anmeldeschema zu erstellen, klicken Sie auf **Hinzufügen**, und geben Sie auf der Seite **Authentifizierungsanmeldeschema erstellen** den Namen für das Schema ein. Klicken Sie auf **Bearbeiten** (Bleistiftsymbol), um die **Anmeldeschemadateien** aus der Liste auszuwählen.



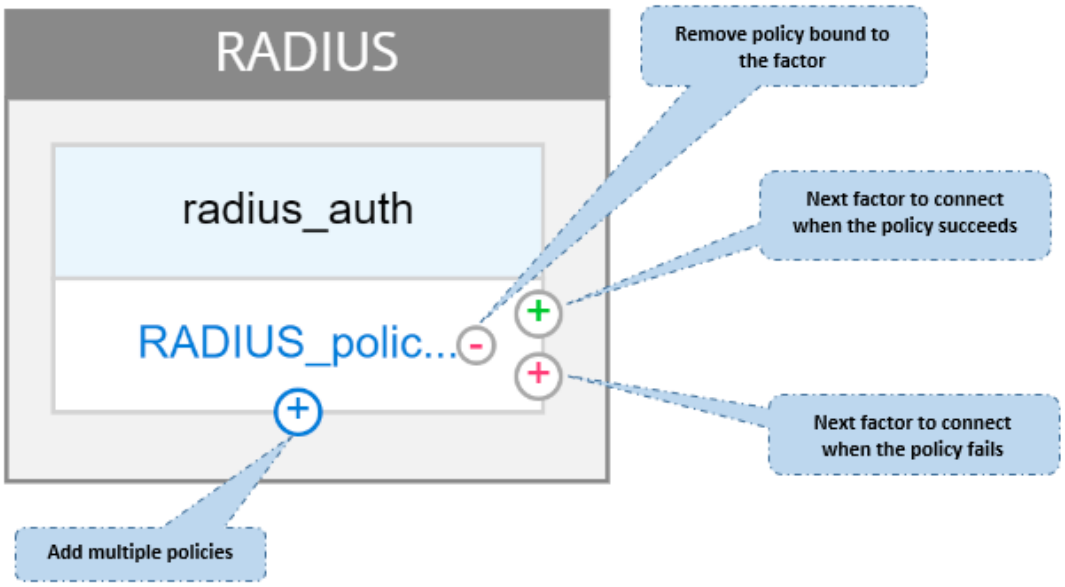
8. Klicken Sie auf **Richtlinie hinzufügen**. Sie können eine Authentifizierungsrichtlinie erstellen oder eine vorhandene Authentifizierungsrichtlinie auswählen.



9. Um eine neue Richtlinie zu erstellen, klicken Sie auf **Hinzufügen**, geben Sie auf der Seite **Authentifizierungsrichtlinie erstellen** den Namen für die Richtlinie ein, und klicken Sie auf **Erstellen** .



10. Nachdem Sie dem Faktor ein Anmeldeschema und eine Richtlinie hinzugefügt haben, werden das Anmeldeschema und die Richtlinie auf dem Faktor im Visualizer angezeigt, wie in der folgenden Abbildung dargestellt. Für jeden Faktor können Sie mehrere Richtlinien hinzufügen und den nächsten Faktor für den Erfolg und Misserfolg jeder Richtlinie definieren. Sie können auch die Richtlinien entfernen, die Teil des Faktors sind.



11. Nachdem Sie den Flow erstellt haben, können Sie den nFactor-Flow an einen virtuellen Authentifizierungsserver binden.

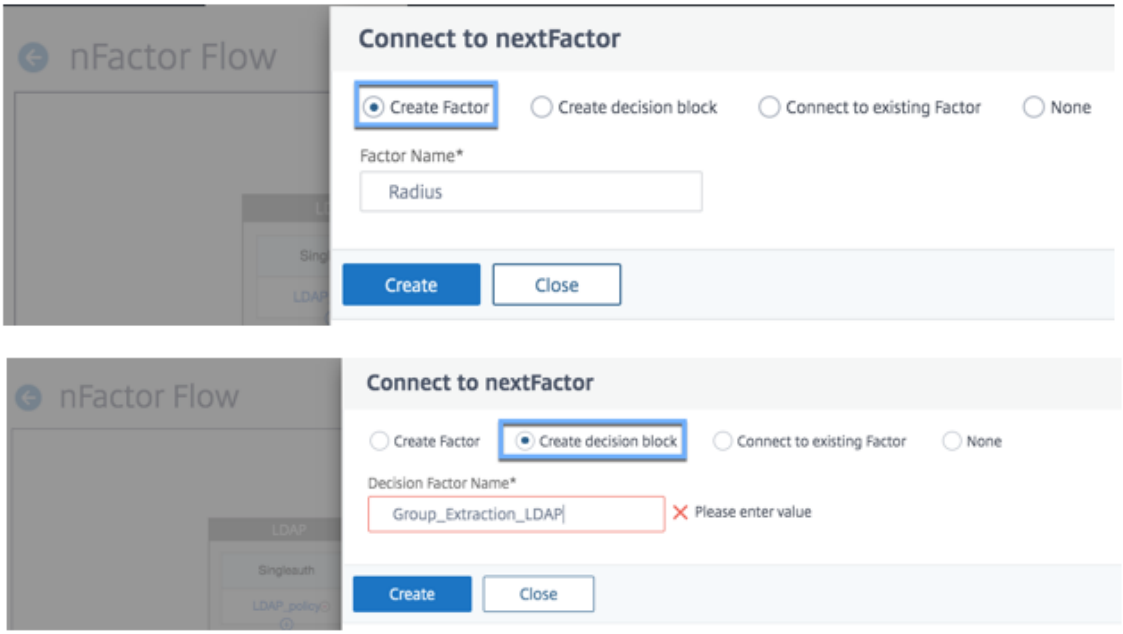
Hinzufügen des nächsten Faktors

Um den nächsten Faktor hinzuzufügen, können Sie je nach Anforderung eine der folgenden Optionen auswählen:

- **Faktor erstellen**. Erstellen Sie einen Faktor. Jeder Faktor, der in einem Flow erstellt wird, ist exklusiv für diesen Flow.
- **Erstellen Sie einen Entscheidungsblock.** Erstellen Sie einen Entscheidungsblock, der als Verzweigungsfaktor dient. Sie können dem Entscheidungsblock kein Anmeldeschema hinzufügen. Visualizer ermöglicht die Konfiguration nur einer NO_AUTHN-Richtlinie für den Entscheidungsblock.

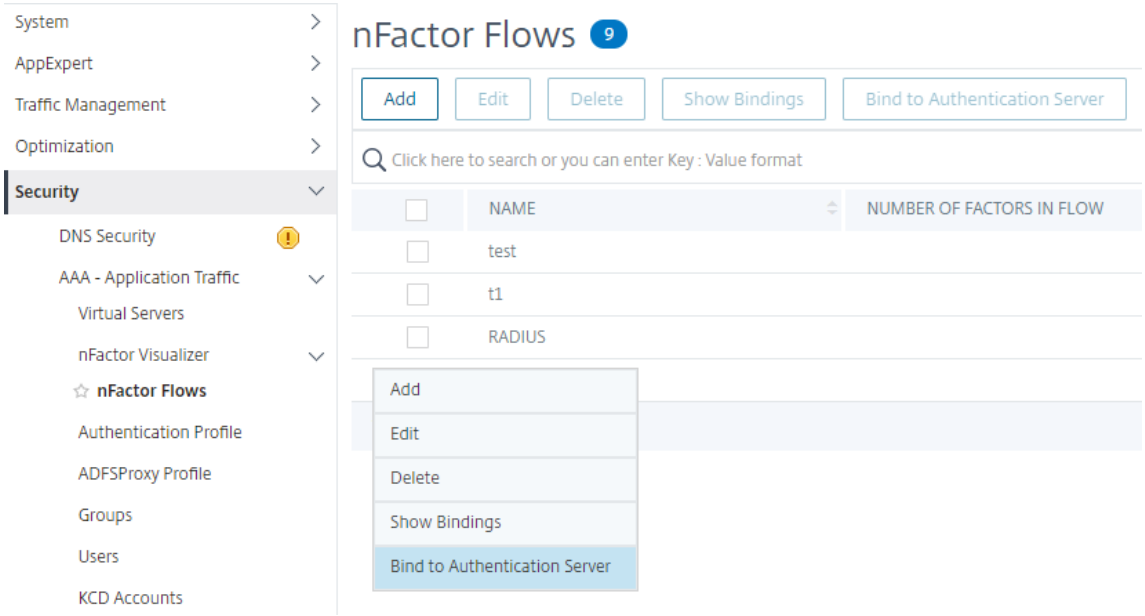
  > **Hinweis:**
  >
  > Sie können den Entscheidungsblock nur über die Citrix ADC GUI hinzufügen oder bearbeiten. Es gibt keine Möglichkeit, den Entscheidungsblock über den CLI-Befehl zu konfigurieren.

- Stellen Sie**eine Verbindung mit einem vorhandenen Faktor**her. Wählen Sie einen vorhandenen Faktor als nächsten Faktor aus. Alle Faktoren, die in der bestehenden Liste erscheinen, werden ausschließlich für diesen Flow erstellt.
- **Keine.** Entfernen Sie eine vorhandene Verbindung.



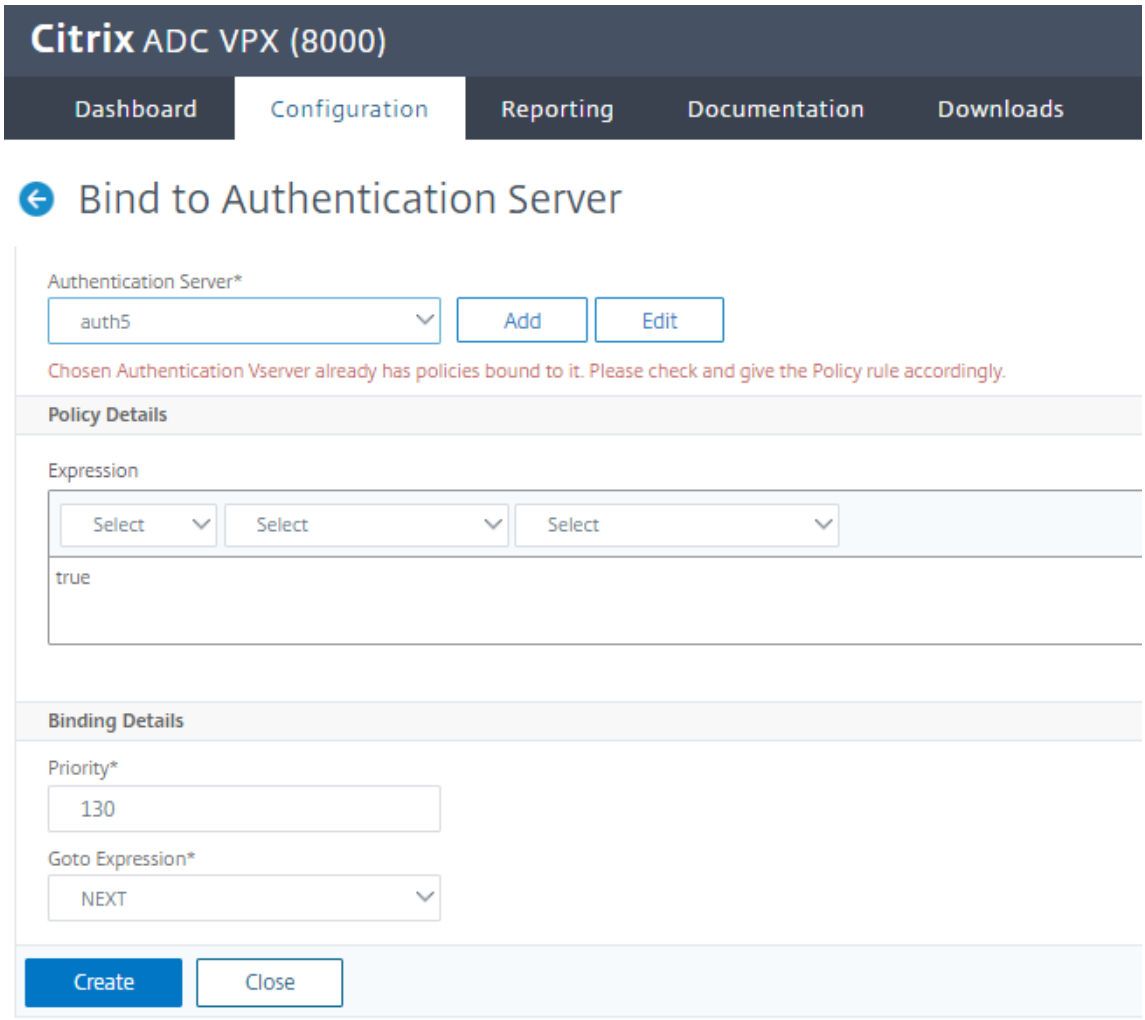
So binden Sie den nFactor-Flow an den Authentifizierungsserver

1. Wählen Sie auf der Seite **nFactor Flows** einen nFactor Flow aus, den Sie an einen virtuellen Authentifizierungsserver binden möchten.
2. Klicken Sie auf das Hamburger-Symbol, **um die Option An Authentifizierungsserver binden** auszuwählen, oder klicken Sie im Detailbereich **auf An Authentifizierungsserver binden** .

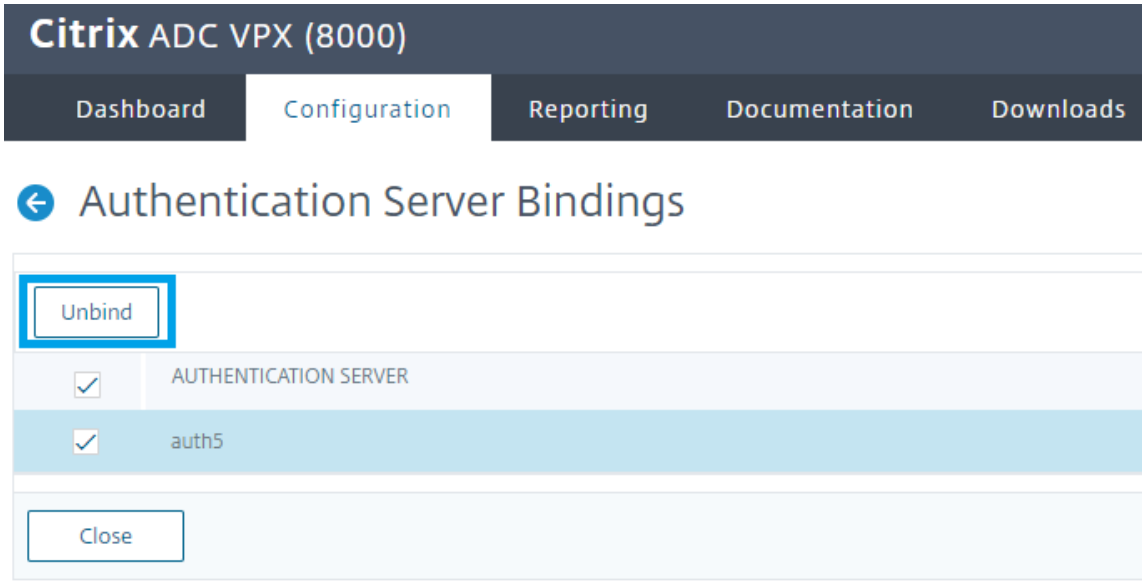


3. Auf der Seite **An Authentifizierungsserver binden** können Sie die folgenden Aktionen ausführen:

- Um einen **virtuellen Authentifizierungsserver**hinzuzufügen, klicken Sie auf **Hinzufügen**.
- Um einen vorhandenen Authentifizierungsserver aus der Liste auszuwählen, klicken Sie auf das Feld **Authentifizierungsserver** .



4. Klicken Sie im Hamburger-Symbol auf **Bindungen** anzeigen, um die Bindungen anzuzeigen.
5. So heben Sie die Bindung des Authentifizierungsservers an den spezifischen nFactor-Flow auf:
   - Klicken Sie auf der Seite **nFactor-Flows** im Hamburger-Symbol auf **Bindungen anzeigen**.
   - Wählen Sie auf der Seite **Authentifizierungsserverbindungen** den Authentifizierungsserver aus, der die Bindung aufgehoben werden soll, und klicken Sie auf **Bindung aufheben** . Klicken Sie auf **Schließen**.



Weitere Informationen zur nFactor-Authentifizierung finden Sie in den folgenden Themen:

- Konzept: Multi-Factor (nFactor) Authentifizierung.
- Workflow: Wie die nFactor-Authentifizierung funktioniert.
- Konfiguration: Konfigurieren der nFactor-Authentifizierung.

Verbesserungen am nFactor Visualizer

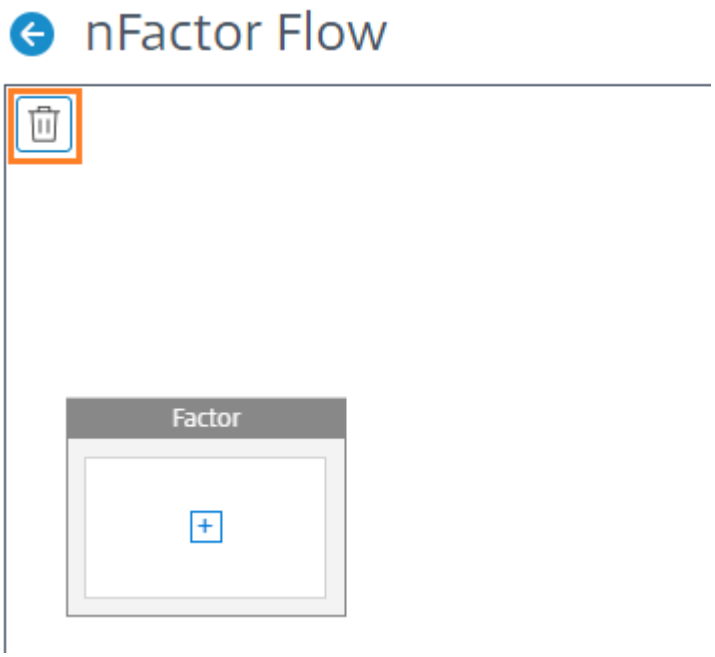
Ab Citrix ADC Version 13.0 Build 41.20 werden die folgenden Verbesserungen im nFactor Visualizer vorgenommen.

- Administratoren können die erstellten Faktoren auf das Papierkorbsymbol verschieben.
- Zeigen Sie die nFactor-Flows auf der Seite Virtueller Authentifizierungsserver an.

Papierkorbsymbol. Administratoren können nur Knoten löschen, die keine Verbindungen haben. Die zugrunde liegenden Richtlinien oder Schemas, die für den Faktor erstellt werden, werden jedoch nicht gelöscht, wenn der Faktor in den Papierkorb verschoben wird.

So zeigen Sie das Papierkorbsymbol an:

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > nFactor Visualizer > nFactor Flows**.

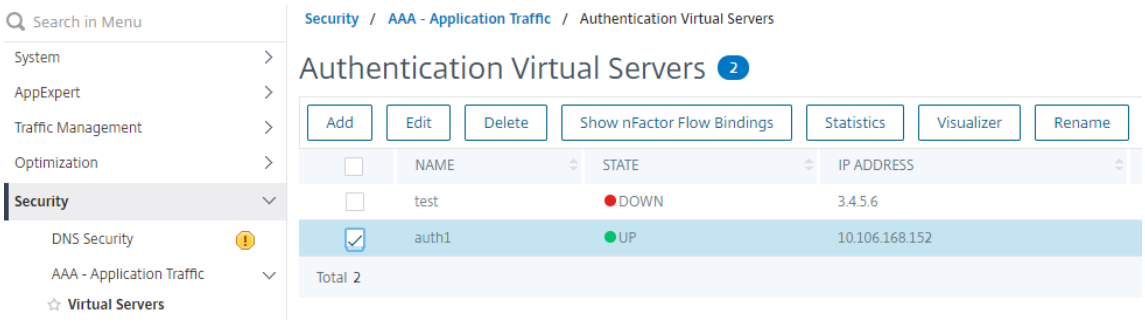


2. Um den Faktor zu löschen, klicken Sie auf den Faktorblock und ziehen ihn in den Papierkorb.

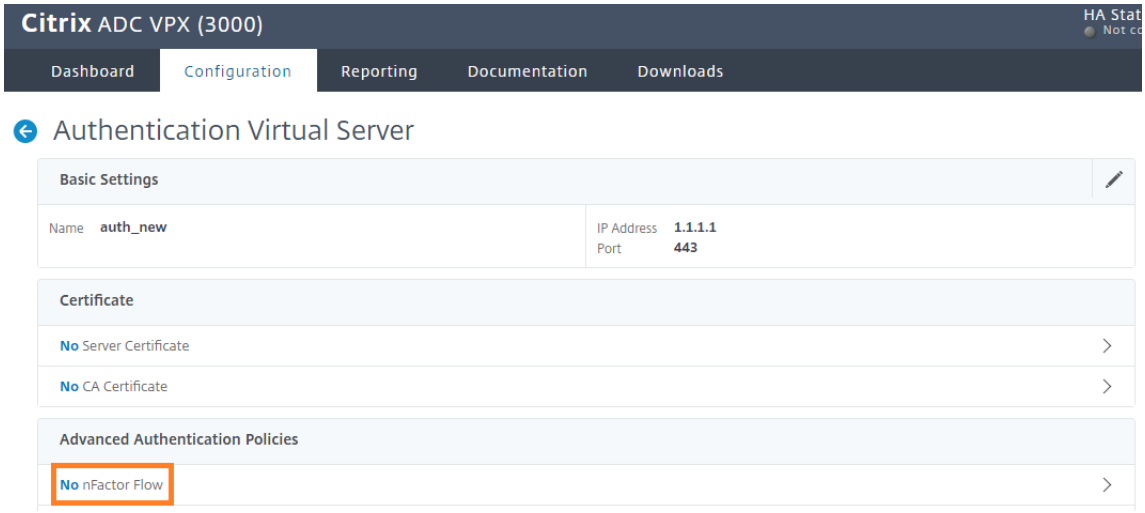
Zeigen Sie den nFactor-Fluss vom virtuellen Authentifizierungsserveran. Administratoren können die erstellten nFactor-Flows auch auf der Seite Authentication Virtual Server anzeigen.

So zeigen Sie den nFactor-Flow von der Seite Virtual Authentication Server an:

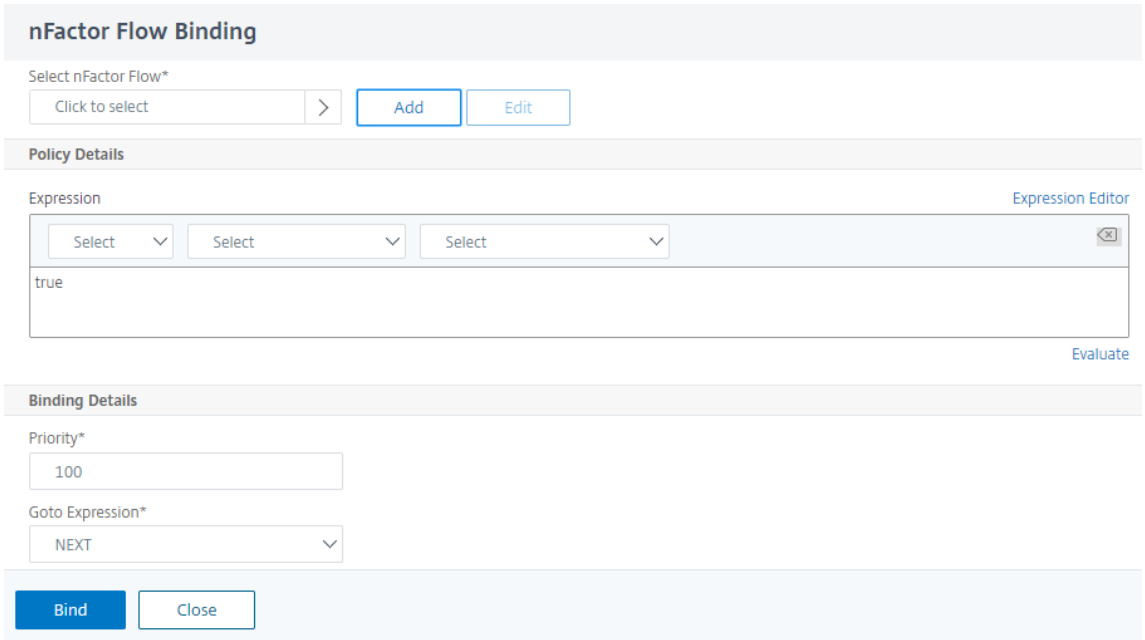
1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Virtuelle Server**. Auf der Seite **Virtuelle Authentifizierungsserver** können Sie die folgenden Schritte ausführen:
   - Um einen virtuellen Authentifizierungsserver hinzuzufügen, klicken Sie auf **Hinzufügen**.
   - Um einen vorhandenen virtuellen Authentifizierungsserver zu **bearbeiten, klicken Sie im Detailbereich auf Option Bearbeiten** .



2. Auf der Seite **Virtueller Authentifizierungsserver** können Sie die Option **nFactor Flow** unter **Erweiterte Authentifizierungsrichtlinien** anzeigen.



3. Wenn kein nFactor-Flow an den virtuellen Server gebunden ist, können Sie im Abschnitt **Erweiterte Authentifizierungsrichtlinien** auf **Keine nFactor-Flow-Option** klicken, um entweder einen neuen nFactor-Flow hinzuzufügen oder den vorhandenen nFactor-Flow aus der Liste auszuwählen.



nFactor Erweiterbarkeit

April 7, 2022

Das nFactor-Authentifizierungsframework bietet die Flexibilität, Anpassungen hinzuzufügen, um die Anmeldeoberfläche für eine umfangreiche Benutzererfahrung intuitiver zu gestalten. Sie können be-

nutzerdefinierte Anmeldebeschriftungen, benutzerdefinierte Anmeldeinformationen, Benutzeroberflächenanzeigen usw. hinzufügen.

Mit nFactor kann jeder Faktor seinen eigenen Anmeldebildschirm haben. In jedem Anmeldebildschirm können Sie Informationen aus einem der vorherigen Faktoren oder weitere Informationen anzeigen, die in anderen Faktoren nicht sichtbar sind. Ihr letzter Faktor kann beispielsweise eine informative Seite sein, auf der der Benutzer die Anweisungen liest und auf Weiter klickt.

Vor nFactor waren benutzerdefinierte Anmeldeseiten begrenzt und Anpassungen und benötigten Unterstützung. Es war möglich, die tmindex.html zu ersetzen oder Umschreibregeln anzuwenden, um einen Teil seines Verhaltens zu ändern. Es war jedoch nicht möglich, die zugrunde liegende Funktionalität zu erreichen.

Die folgenden nFactor-bezogenen Anpassungen werden in diesem Thema ausführlich erfasst.

- Anmelde-Labels
- Benutzeroberfläche anpassen, um Images anzuzeigen
- Anpassen des Citrix ADC nFactor-Anmeldeformulars

Annahmen

Sie sind mit nFactor, Shell-Befehlen, XML und Texteditoren vertraut.

Voraussetzungen

- Die in diesem Thema beschriebene Anpassung ist nur möglich, wenn das RFWeb-UI-Thema (oder themenbasiert) auf Citrix ADC konfiguriert ist.
- Die Authentifizierungsrichtlinie muss an den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver gebunden sein, andernfalls funktioniert der Flow nicht wie vorgesehen.
- Sie haben folgende Artikel im Zusammenhang mit nFactor
  - XML-Schema
  - JavaScript
  - Aktionen zur Authentifizierung
  - Virtueller Authentifizierungsserver
  - Citrix ADC Version 11.1 und höher

Anmeldebeschriftungen anpassen

Um Anmeldebeschriftungen anzupassen, benötigen Sie Folgendes:

- Das XML-Schema, das beschreibt, wie die Anmeldeseite aussieht.
- Die Datei script.js, die das JavaScript enthält, das verwendet wird, um den Rendering-Prozess zu ändern.

> **Hinweis:**
>
> Die Datei script.js befindet sich im Verzeichnis /var/netscaler/logon/themes/<custom_theme>/.

Funktionsweise

Das JavaScript analysiert die XML-Datei und rendert jedes Element innerhalb des <Requirements>-Tags. Jedes Element entspricht einer Zeile im HTML-Formular. Zum Beispiel ist ein Anmeldefeld eine Zeile, das Kennwortfeld ist eine weitere Zeile, ebenso wie die Anmeldeschaltfläche. Um neue Zeilen einzuführen, müssen Sie sie mithilfe des StoreFront-SDK in der XML-Schemadatei angeben. Das StoreFront-SDK ermöglicht es der Anmeldeseite mit einem XML-Schema, das <Requirement>-Tag zu verwenden und Elemente darauf zu definieren. Diese Elemente ermöglichen die Verwendung von JavaScript, um in diesem Bereich alle benötigten HTML-Elemente einzuführen. In diesem Fall wird eine Zeile mit etwas Text in Form von HTML erstellt.

Das XML, das verwendet werden kann, lautet wie folgt:

```
<Requirement>
<Credential>
<Type>nsg-custom-cred</Type>
<ID>passwd</ID>
</Credential>
<Label>
<Type>nsg-custom-label</Type>
</Label>
</Requirement>
<!--NeedCopy-->
```

<Requirement>: Auf der Anmeldeseite bereitgestellter Speicherplatz. Der Berechtigungsnachweis füllt den Raum, und die anderen Teile leiten den Motor an die richtigen Informationen weiter. In diesem Fall geben Sie ein nsg-custom-cred. Dies ist als einfacher Text definiert und die Beschriftung ist für seinen Hauptteil definiert.
Die XML-Anforderung wird mit dem JavaScript-Code gekoppelt, um die erforderlichen Ergebnisse zu erzielen.

```
// Custom Label Handler for Self Service Links
CTXS.ExtensionAPI.addCustomAuthLabelHandler({

getLabelTypeName: function () {
```



```
5    return "nsg-custom-label";  }
6   ,
7  getLabelTypeMarkup: function (requirements) {
8
9  return $("< Enter your HTML code here>");
10  }
11  ,
12 // Instruction to parse the label as if it was a standard type
13 parseAsType: function () {
14
15 return "plain";
16  }
17
18  }
19  );
20 //Custom Credential Handler for Self Service Links
21 CTXS.ExtensionAPI.addCustomCredentialHandler({
22
23 getCredentialTypeName: function () {
24   return "nsg-custom-cred";  }
25  ,
26 getCredentialTypeMarkup: function (requirements) {
27
28 return $("<div/>");
29  }
30  ,
31  }
32  );
33 <!--NeedCopy-->
```

> **Wichtig:**
>
> Wenn Sie den HTML-Code hinzufügen, stellen Sie sicher, dass der Rückgabewert mit einem HTML-Tag beginnt.

Der XML-Teil gibt auf der Anmeldeseite an, was angezeigt werden soll, und der JavaScript-Code liefert den eigentlichen Text. Der Anmeldeinformationshandler öffnet den Raum und das Etikett füllt den Raum. Da der gesamte Authentifizierungsverkehr jetzt für das Umschreiben und den Responder unsichtbar ist, können Sie das Erscheinungsbild der Seite ändern.
Konfiguration zum Anpassen von Anmeldelab

1. Erstellen und binden Sie ein Thema basierend auf RFWeb.

```
1 add vpn portaltheme RfWebUI_MOD -basetheme RfWebUI
```



```
2
3 bind vpn vserver TESTAAA  - portaltheme RfWebUI_MOD
4 <!--NeedCopy-->
```

Der Pfad für die auf dem Thema basierenden Dateien ist im Verzeichnis verfügbar; /var/netscaler/logon/themes/rfwebui_mod

2. Fügen Sie am Ende der Datei script.js das folgende Snippet hinzu:

> **Hinweis**:
>
> Wenn die vorhergehenden Zeilen nicht in die richtige Datei aufgenommen werden oder keine JavaScript-Funktionen enthalten sind, kann die XML nicht geladen werden. Der Fehler kann nur in der Entwicklerkonsole des Browsers mit dem folgenden Text angezeigt werden: “Undefinierter Typ `nsg-custom-cred`. “

```
1 // Custom Label Handler for Self Service Links
2 CTXS.ExtensionAPI.addCustomAuthLabelHandler({
3
4 getLabelTypeName: function () {
5   return "nsg-custom-label";  }
6  ,
7 getLabelTypeMarkup: function (requirements) {
8
9 return $("<a href="https://identity.test.com/identity/faces/
     register" style="font-size: 16px;" style="text-align: center;">
     Self Registration</a><br><a href="https://identity.test.com/
     identity/faces/forgotpassword" style="font-size: 16px;" style="
     text-align: center;">Forgot Password</a><br><a href="https://
     identity.test.com/identity/faces/forgotuserlogin" style="font-
     size: 16px;" style="text-align: center;">Forgot User Login</a
     >");
10  }
11  ,
12 // Instruction to parse the label as if it was a standard type
13 parseAsType: function () {
14
15 return "plain";
16  }
17
18  }
19  );
20 //Custom Credential Handler for Self Service Links
21 CTXS.ExtensionAPI.addCustomCredentialHandler({
```



```
22
23 getCredentialTypeName: function () {
24   return ”nsg-custom-cred”;  }
25  ,
26 getCredentialTypeMarkup: function (requirements) {
27
28 return $(”<div/>”);
29  }
30  ,
31  }
32  );
33 <!--NeedCopy-->
```

> **Wichtig:**
>
> Wenn Sie den HTML-Code hinzufügen, stellen Sie sicher, dass der Rückgabewert mit einem HTML-Tag beginnt.

In diesem Beispiel verwendetes Anmeldeschema

```
1  <?xml version=”1.0” encoding=”utf-8”?>
2  <AuthenticateResponse xmlns=”http://citrix.com/authentication/response
      /1”>
3  <Status>success</Status>
4  <Result>more-info</Result>
5  <StateContext/>
6  <AuthenticationRequirements>
7  <PostBack>/nf/auth/doAuthentication.do</PostBack>
8  <CancelPostBack>/Citrix/Authentication/ExplicitForms/CancelAuthenticate
      </CancelPostBack>
9  <CancelButtonText>Cancel</CancelButtonText>
10 <Requirements>
11 <Requirement>
12 <Credential>
13 <ID>login</ID>
14 <SaveID>Username</SaveID>
15 <Type>username</Type>
16 </Credential>
17 <Label>
18 <Text>User name</Text>
19 <Type>plain</Type>
20 </Label>
21 <Input>
```



```
<AssistiveText>Please supply either domain\username or user@fully.
   qualified.domain</AssistiveText>
<Text>
<Secret>false</Secret>
<ReadOnly>false</ReadOnly>
<InitialValue></InitialValue>
<Constraint>.+</Constraint>
</Text>
</Input>
</Requirement>
<Requirement>
<Credential>
<ID>passwd</ID>
<SaveID>Password</SaveID>
<Type>password</Type>
</Credential>
<Label>
<Text>Password:</Text>
<Type>plain</Type>
</Label>
<Input>
<Text>
<Secret>true</Secret>
<ReadOnly>false</ReadOnly>
<InitialValue/>
<Constraint>.+</Constraint>
</Text>
</Input>
</Requirement>
<Requirement>
<Credential>
<Type>nsg-custom-cred</Type>
<ID>passwd</ID>
</Credential>
<Label>
<Type>nsg-custom-label</Type>
</Label>
</Requirement>
<Requirement>
<Credential>
<ID>loginBtn</ID>
<Type>none</Type>
</Credential>
<Label>
<Type>none</Type>
```



```
</Label>
<Input>
<Button>Please Log On</Button>
</Input>
</Requirement>
</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

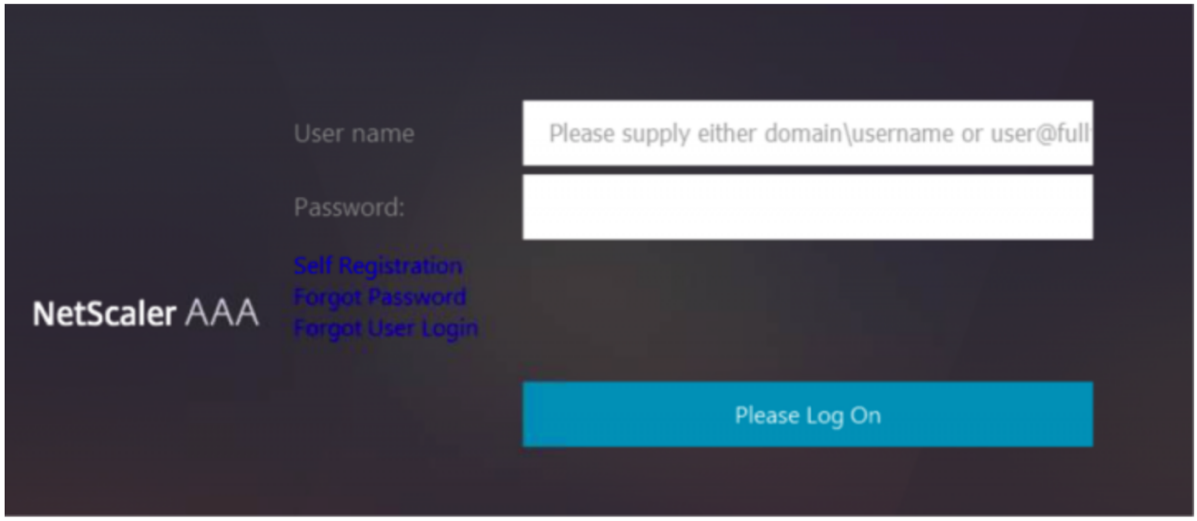
Führen Sie die folgenden Befehle aus, um das benutzerdefinierte Schema in die Konfiguration zu laden.

```
add authentication loginSchema custom -authenticationSchema custom.xml

add authentication loginSchemaPolicy custom -rule true -action custom

bind authentication vserver AAATEST -policy custom -priority 100 -
    gotoPriorityExpression END
<!--NeedCopy-->
```

In der folgenden Abbildung wird die Anmeldeseite angezeigt, die mit dieser Konfiguration gerendert wird.



Benutzeroberfläche anpassen, um Images anzuzeigen

nFactor ermöglicht eine benutzerdefinierte Anzeige mithilfe von Anmeldeschemadateien. Möglicherweise sind weitere Anpassungen erforderlich, die nicht in den integrierten Anmeldeschemadateien

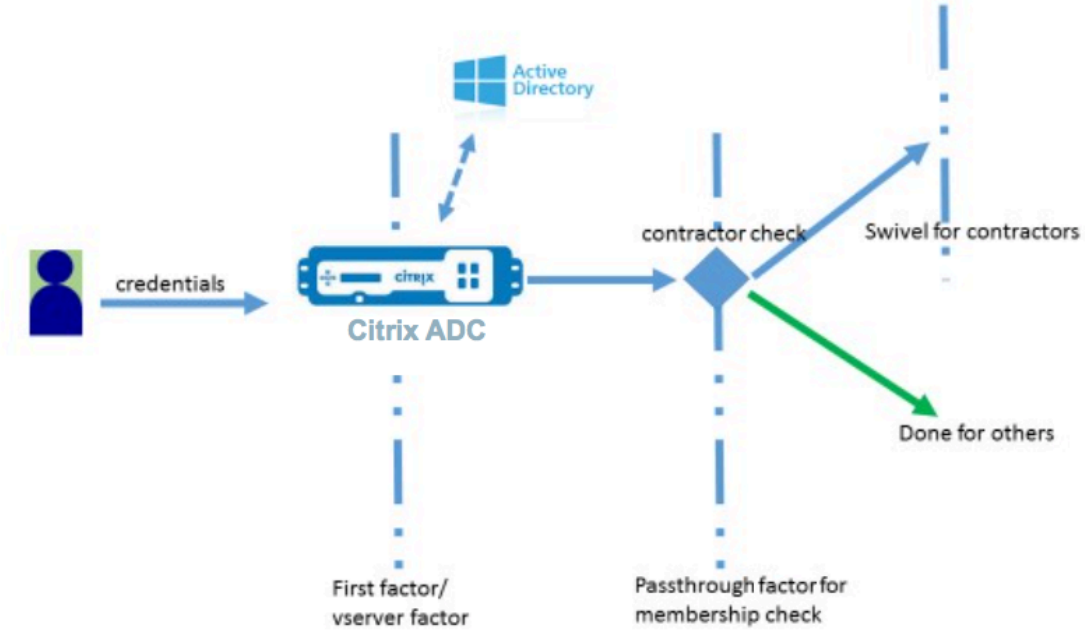
angeboten werden. Zum Beispiel das Anzeigen eines Hyperlinks oder das Schreiben einer benutzerdefinierten Logik in der Benutzeroberfläche. Diese können mithilfe von “benutzerdefinierten Anmeldeinformationen” erreicht werden, die die Erweiterung des Anmeldeschemas und die entsprechende Javascript-Datei umfassen.

Anmeldeschemadateien befinden sich im Verzeichnis `/nsconfig/loginschema/LoginSchema`.

Für die Benutzeroberflächenanpassung zur Anzeige von Images wird ein Bereitstellungsablauf in der Integration “Citrix ADC-Swivel” als Beispiel verwendet.

Dieser Ablauf hat zwei Faktoren.

- Erster Faktor: Überprüft die AD-Anmeldeinformationen des Benutzers.
- Zweiter Faktor: Aufforderung zur Benutzeranmeldung basierend auf der Gruppenzugehörigkeit.



In diesem Ablauf durchlaufen alle Benutzer den ersten Faktor. Vor dem zweiten Faktor gibt es einen Pseudofaktor, um zu überprüfen, ob einige Benutzer im “Swivel” -Faktor weggelassen werden können. Wenn der Benutzer den “Swivel” -Faktor benötigt, werden ein Bild und ein Textfeld angezeigt, um den Code einzugeben.

Lösung

Die Lösung zum Anpassen der Benutzeroberfläche für die Anzeige von Bildern besteht aus zwei Teilen.

- Erweiterung des Anmeldeschemas
- Benutzerdefiniertes Skript zur Verarbeitung der Anmeldeschemaerweiterung.

Erweiterung des Anmeldeschemas

Um das Rendern von Formularen zu steuern, wird eine benutzerdefinierte “ID” /” Berechtigungsnachweis” in das Anmeldeschema eingefügt. Dies kann erreicht werden, indem das vorhandene Schema wiederverwendet und gemäß der Anforderung geändert wird.

In diesem Beispiel wird ein Anmeldeschema mit nur einem Textfeld (z. B. /nsconfig/loginschema/LoginSchema/OnlyPassword.xml) berücksichtigt.
Das folgende Snippet wurde dem Anmeldeschema hinzugefügt.

```
<Requirement><Credential><ID>swivel_cred</ID><Type>swivel_cred</Type><
   Input><Text><Hidden>true</Hidden><InitialValue>${
 http.req.user.name }
 </InitialValue></Text></Input></Credential></Requirement>
<!--NeedCopy-->
```

Im Snippet wird “swivel_cred” als “Typ” des Berechtigungsnachweises angegeben. Da dies nicht als integrierter “Berechtigungsnachweis” erkannt wird, sucht die Benutzeroberfläche nach einem Handler für diesen Typ und ruft ihn auf, falls er vorhanden ist.
Für diese Anmeldeinformationen wird ein Anfangswert gesendet, bei dem es sich um einen Ausdruck handelt, den Citrix ADC dynamisch ausfüllt. Im Beispiel ist es der Name des Benutzers, der verwendet wird, um den Swivel-Server über den Benutzernamen zu informieren. Es wird möglicherweise nicht ständig benötigt oder kann mit einigen anderen Daten ergänzt werden. Diese Angaben müssen nach Bedarf hinzugefügt werden.

Javascript zur Verarbeitung von benutzerdefinierten Anmeldeinformationen

Wenn die UI benutzerdefinierte Anmeldeinformationen findet, sucht sie nach einem Handler. Alle benutzerdefinierten Handler sind in /var/netscaler/logon/LogonPoint/custom/script.js für das Standardportaldesign geschrieben.

Für die benutzerdefinierten Portal-Themen befindet sich script.js im Verzeichnis `/var/netscaler/logon/themes/<custom_theme>/`.

Das folgende Skript wurde hinzugefügt, um Markup für benutzerdefinierte Anmeldeinformationen zu rendern.

```
CTXS.ExtensionAPI.addCustomCredentialHandler({

    // The name of the credential, must match the type returned by the
       server
    getCredentialTypeName: function () {
```



```
5    return "swivel_cred";  }
6   ,
7      // Generate HTML for the custom credential
8      getCredentialTypeMarkup: function (requirements) {
9
10         var div = $("<div></div>");
11         var image = $("<img/>");
12         var username = requirements.input.text.initialValue; //Get the
               secret from the response
13         image.attr({
14
15             "style" : "width:200px;height:200px;",
16             "id" : "qrcodeimg",
17             "src" : "https://myswivelserver.citrix.com:8443/pinsafe/
                   SCImage?username=" + username
18          }
19  );
20         div.append(image);
21         return div;
22       }
23
24  }
25  );
26 <!--NeedCopy-->
```

Dieses Snippet dient zur Behandlung des Markups für "swivel_cred". Der hervorgehobene Anmeldeinformationsname muss mit dem zuvor in der Anmeldeschemaerweiterung angegebenen 'Typ' übereinstimmen.
Um Markup zu generieren, muss ein Bild hinzugefügt werden, dessen Quelle auf den Swivel-Server zeigt. Sobald dies erledigt ist, lädt die UI das Bild vom angegebenen Ort. Da dieses Anmeldeschema auch über ein Textfeld verfügt, rendert die Benutzeroberfläche dieses Textfeld.

> **Hinweis:**
>
> Der Administrator kann den "Stil" des Bildelements ändern, um die Größe des Bilds zu ändern. Derzeit ist es für 200x200 Pixel konfiguriert.

Konfiguration zum Anpassen der Benutzeroberfläche zur Anzeige von Bildern

Die nFactor-Konfiguration ist besser von unten nach oben aufgebaut, das ist der letzte Faktor zuerst, denn wenn Sie versuchen, 'NextFactor' für die vorherigen Faktoren anzugeben, benötigen Sie den Namen des nachfolgenden Faktors.

Konfiguration des Schwenkfaktors:


```
add loginschema swivel_image -authenticationSchema /nsconfig/loginschema/SwivelImage.xml

add authentication policylabel SwivelFactor -loginSchema swivel_image

bind authentication policylabel SwivelFactor -policy <policy-to-check-swivel-image> -priority 10
<!--NeedCopy-->
```

> **Hinweis:**
>
> Laden Sie SwivelImage.xml aus dem im Beispiel verwendeten Anmeldeschema herunter.

Pseudofaktor für die Konfiguration der Gruppenprüfung:

```
add authentication policylabel GroupCheckFactor

add authentication policy contractors_auth_policy -rule 'http.req.user.is_member_of( "contractors" )' -action NO_AUTHN

add authentication policy not_contractors _auth_policy -rule true -action NO_AUTHN

bind authentication policylabel GroupCheckFactor -policy contractors_auth_policy -pri 10 -nextFactor SwivelFactor

bind authentication policylabel GroupCheckFactor -policy not_contractors_auth_policy -pri 20
<!--NeedCopy-->
```

Erster Faktor für die Active Directory-Anmeldung:

```
add ldapAction <>

add authentication policy user_login_auth_policy -rule true -action <>

bind authentication vserver <> -policy user_login_auth_policy -pri 10 -nextFactor GroupCheckFactor
<!--NeedCopy-->
```


In der Konfiguration werden drei Faktoren angegeben, von denen einer implizit/pseudo ist.

In diesem Beispiel verwendetes Anmeldeschema

Das Folgende ist ein Beispielschema mit Swivel-Anmeldeinformationen und einem Textfeld.

> **Hinweis:**
>
> Beim Kopieren von Daten für einen Webbrowser werden Angebote möglicherweise anders angezeigt. Kopieren Sie Daten in Editoren wie Notepad, bevor Sie sie in Dateien speichern.

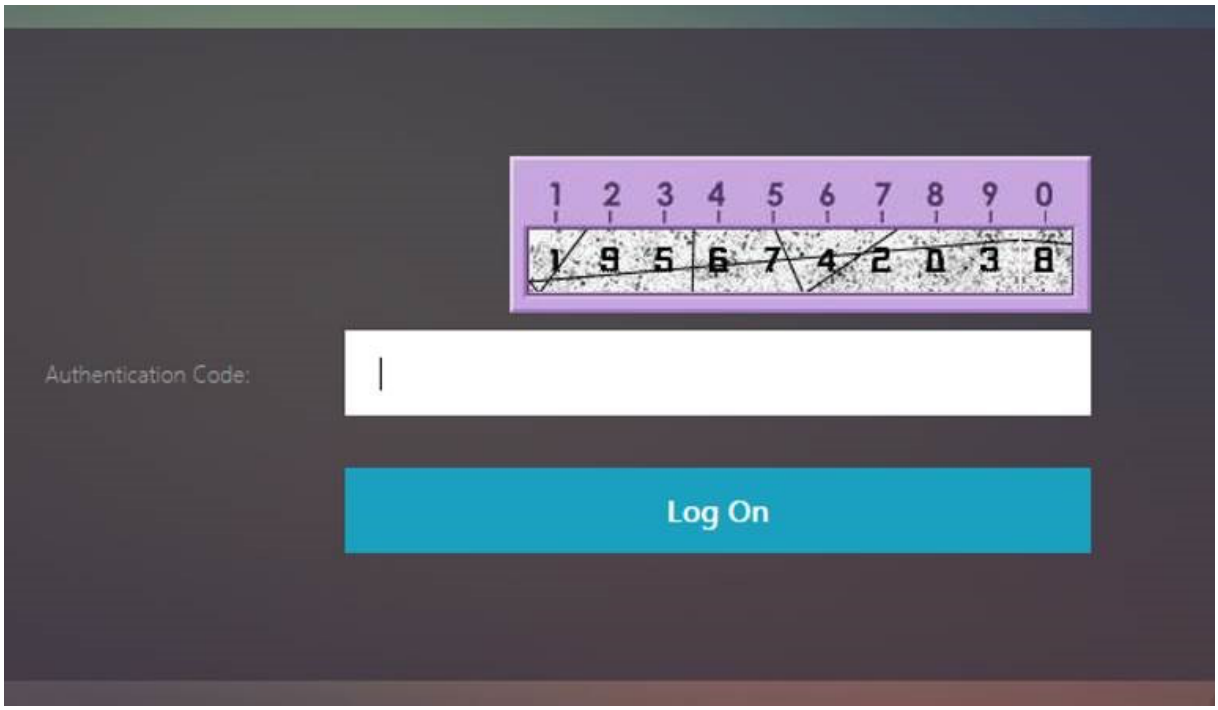
```
<?xml version="1.0" encoding="UTF-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response/1">
<Status>success</Status>
<Result>more-info</Result>
<StateContext></StateContext>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>
<Requirement><Credential><ID>swivel_cred</ID><Type>swivel_cred</Type><Input><Text><Hidden>true</Hidden><InitialValue>${
 http.req.user.name }
 </InitialValue></Text></Input></Credential></Requirement>
<Requirement><Credential><ID>passwd</ID><SaveID>ExplicitForms-Password</SaveID><Type>password</Type></Credential><Label><Text>Password:</Text><Type>plain</Type></Label><Input><Text><Secret>true</Secret><ReadOnly>false</ReadOnly><InitialValue></InitialValue><Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><Type>none</Type></Credential><Label><Text>Hello ${
 http.req.user.name }
 , Please enter passcode from above image.</Text><Type>confirmation</Type></Label><Input /></Requirement>
<Requirement><Credential><ID>saveCredentials</ID><Type>savecredentials</Type></Credential><Label><Text>Remember my password</Text><Type>plain</Type></Label><Input><CheckBox><InitialValue>false</InitialValue></CheckBox></Input></Requirement>
<Requirement><Credential><ID>loginBtn</ID><Type>none</Type></Credential><Label><Type>none</Type></Label><Input><Button>Log On</Button></Input></Requirement>
</Requirements>
```



```
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

Ausgabe

Sobald die Konfiguration durchgeführt wurde, wird das folgende Bild angezeigt.



> **Hinweis:**
>
> Bildhöhe und -platzierung können im JavaScript geändert werden.

Anpassen des Citrix ADC nFactor-Anmeldeformulars, um Felder ein- oder auszublenden

Die RFWeb UI von Citrix Gateway ermöglicht eine Vielzahl von Anpassungen. Diese Funktion in Kombination mit dem nFactor-Authentifizierungsframework ermöglicht es Kunden, komplexe Abläufe zu konfigurieren, ohne bestehende Workflows zu beeinträchtigen.

In diesem Beispiel sind zwei Authentifizierungsoptionen, OAuth und LDAP, in der Liste Anmeldetyp verfügbar. Wenn das Formular zum ersten Mal geladen wird, werden die Felder Benutzername und Kennwort (LDAP wird zuerst angezeigt) angezeigt. Wenn OAuth ausgewählt ist, werden alle Felder ausgeblendet, da OAuth eine Auslagerung der Authentifizierung an einen Drittanbieterserver impliziert. Auf diese Weise kann ein Administrator intuitive Workflows gemäß Benutzerkomfort konfigurieren.

> **Hinweis:**
>
> - Die Werte in der Liste Anmeldetyp können mit einfachen Änderungen an der Skriptdatei geändert werden.
> - In diesem Abschnitt wird nur der UI-Teil des Flows beschrieben. Die Laufzeitbehandlung der Authentifizierung liegt außerhalb des Geltungsbereichs dieses Artikels. Benutzern wird empfohlen, die nFactor-Dokumentation zur Authentifizierungskonfiguration zu lesen.

So passen Sie das nFactor-Anmeldeformular an

Das Anpassen des nFactor-Anmeldeformulars kann in zwei Teile unterteilt werden.

- Das richtige Anmeldeschema an die Benutzeroberfläche senden
- Schreiben eines Handlers zur Interpretation des Anmeldeschemas und der Benutzerauswahl

Senden Sie das richtige Anmeldeschema an die UI

In diesem Beispiel wird ein einfacher Anspruch/Anforderung im Anmeldeschema gesendet.

Dazu wird die Datei SingleAuth.xml geändert. Die SingleAuth.xml wird mit Citrix ADC-Firmware geliefert und befindet sich im Verzeichnis `/nsconfig/loginschema/LoginSchema`.

Schritte zum Senden des Anmeldeschemas:

1. Melden Sie sich über SSH an und legen Sie auf die Shell (Typ “Shell”).
2. Kopieren Sie SingleAuth.xml zur Änderung in eine andere Datei.

   > **Hinweis**:
   >
   > Der Zielordner unterscheidet sich vom Standardordner für Citrix ADC-Anmeldeschemas.
   >
   > cp /nsconfig/loginschema/LoginSchema/SingleAuth.xml /nsconfig/loginschema/SingleAuthDynamic.xml

3. Fügen Sie den folgenden Anspruch zu SingleAuthDynamic.xml hinzu.

```
1 <Requirement><Credential><ID>nsg_dropdown</ID><Type>nsg_dropdown</
     Type></Credential><Label><Text>Logon Type:</Text><Type>plain</
     Type></Label></Requirement>
2 <!--NeedCopy-->
```

4. Konfigurieren Sie Citrix ADC so, dass dieses Anmeldeschema zum Laden des ersten Formulars gesendet wird.


```
add loginschema single_auth_dynamic -authenticationSchema
    SingleAuthDynamic.xml

add loginschemaPolicy single_auth_dynamic -rule true -action
    single_auth_dynamic

bind authentication vserver aaa_nfactor -policy
    single_auth_dynamic -pri 10
<!--NeedCopy-->
```

Änderungen an Skripten zum Laden von Formularen und zur Behandlung

Sie können das JavaScript ändern, das es einem Administrator ermöglicht, die Anzeige für das Anmeldeformular anzupassen. In diesem Beispiel werden der Benutzername und das Kennwortfeld angezeigt, wenn LDAP ausgewählt ist, und werden ausgeblendet, wenn OAuth ausgewählt ist. Der Administrator kann auch nur das Kennwort verbergen.

Administratoren müssen das folgende Snippet an “script.js” anhängen, das sich im Verzeichnis “/var/NetScaler/logon/logonpoint/custom” befindet.

> **Hinweis:**
>
> Da es sich bei diesem Verzeichnis um ein globales Verzeichnis handelt, erstellen Sie ein Portaldesign und bearbeiten Sie die Datei “script.js” in diesem Ordner unter ”/var/netscaler/logon/themes/<THEME_NAME>”.

```
CTXS.ExtensionAPI.addCustomCredentialHandler({

    // The name of the credential, must match the type returned by the
       server
    getCredentialTypeName: function () {
  return ”nsg_dropdown”;  }
 ,
    // Generate HTML for the custom credential
    getCredentialTypeMarkup: function (requirements) {

        var div = $(”<div></div>”);
        var select = $(”<select name='nsg_dropdown'></select>”).attr(”
           id”, ”nsg_dropdown”);

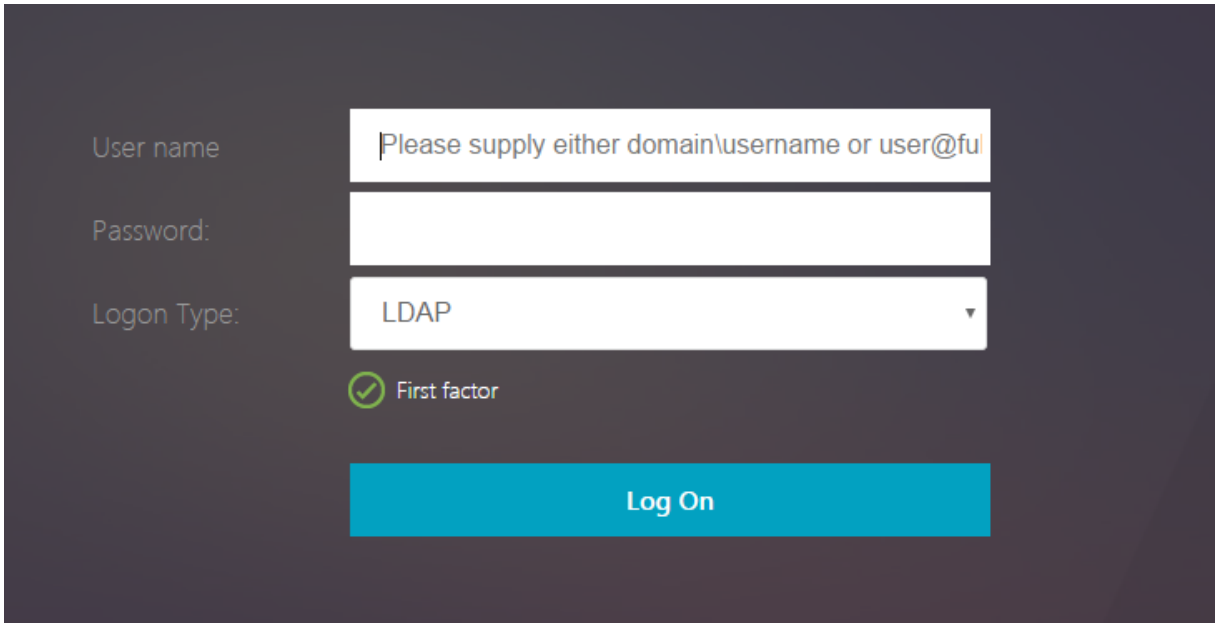
        var rsa = $(”<option></option>”).attr(”selected”, ”selected”).
           text(”LDAP”).val(”LDAP”);
```



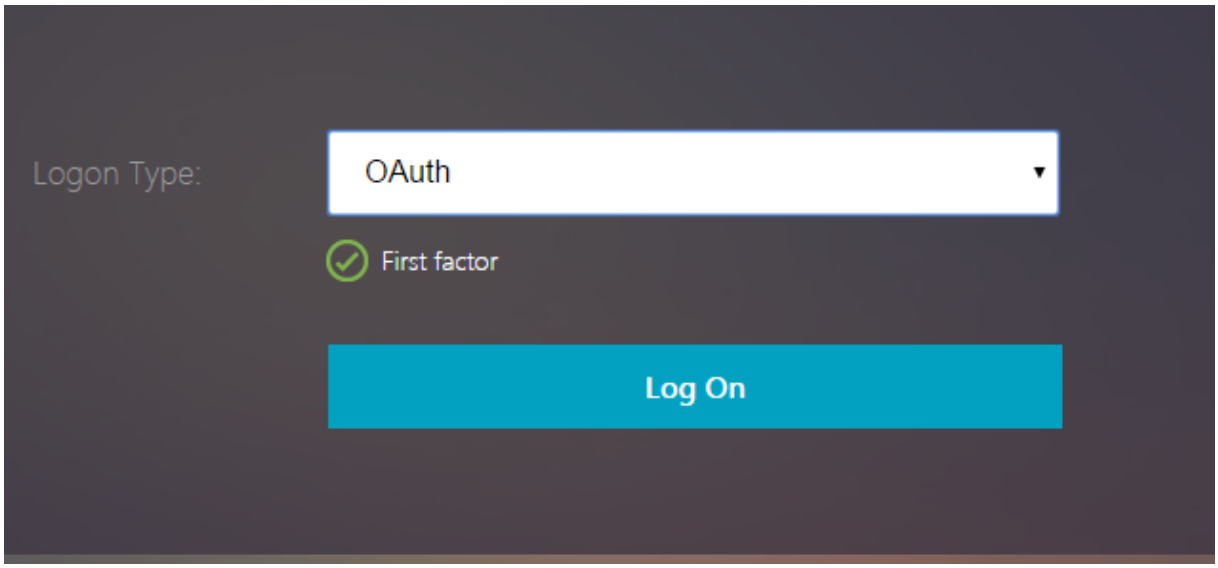
```
14          var OAuthID = $("<option></option>").text("OAuth").val("OAuth")
                ;
15          select.append(rsa, OAuthID);
16
17          select.change(function(e) {
18
19              var value = $(this).val();
20              var ldapPwd = $($(".credentialform").find(".
                    CredentialTypepassword")[0]);
21              var ldapUname = $($(".credentialform").find(".
                    CredentialTypeusername"));
22              if(value == "OAuth") {
23
24                  if (ldapPwd.length)
25                          ldapPwd.hide();
26                  if (ldapUname.length)
27                          ldapUname.hide();
28               }
29    else if(value == "LDAP") {
30
31                  if (ldapPwd.length)
32                          ldapPwd.show();
33                  if (ldapUname.length)
34                          ldapUname.show();
35               }
36
37           }
38  );
39        div.append(select);
40         return div;
41      }
42
43  }
44  );
45 <!--NeedCopy-->
```

Erfahrung für Endbenutzer

Wenn ein Endbenutzer die Anmeldeseite zum ersten Mal lädt, wird der folgende Bildschirm angezeigt.



Wenn **OAuth** in **Anmeldetyp**ausgewählt ist, werden die Felder Benutzername und Kennwort ausgeblendet.



Wenn **LDAP** ausgewählt ist, werden Benutzername und Kennwort angezeigt. Auf diese Weise kann die Anmeldeseite basierend auf der Benutzerauswahl dynamisch geladen werden.

In diesem Beispiel verwendetes Anmeldeschema

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <AuthenticateResponse xmlns="http://citrix.com/authentication/response
     /1">
3 <Status>success</Status>
```



```
<Result>more-info</Result>
<StateContext></StateContext>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>
<Requirement><Credential><ID>login</ID><SaveID>ExplicitForms-Username</SaveID><Type>username</Type></Credential><Label><Text>User name</Text><Type>plain</Type></Label><Input><AssistiveText>Please supply either domain\username or user@fully.qualified.domain</AssistiveText><Text><Secret>false</Secret><ReadOnly>false</ReadOnly><InitialValue></InitialValue><Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><ID>passwd</ID><SaveID>ExplicitForms-Password</SaveID><Type>password</Type></Credential><Label><Text>Password:</Text><Type>plain</Type></Label><Input><Text><Secret>true</Secret><ReadOnly>false</ReadOnly><InitialValue></InitialValue><Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><ID>nsg_dropdown</ID><Type>nsg_dropdown</Type></Credential><Label><Text>Logon Type:</Text><Type>plain</Type></Label></Requirement>
<Requirement><Credential><Type>none</Type></Credential><Label><Text>First factor</Text><Type>confirmation</Type></Label><Input /></Requirement>
<Requirement><Credential><ID>saveCredentials</ID><Type>savecredentials</Type></Credential><Label><Text>Remember my password</Text><Type>plain</Type></Label><Input><CheckBox><InitialValue>false</InitialValue></CheckBox></Input></Requirement>
<Requirement><Credential><ID>loginBtn</ID><Type>none</Type></Credential><Label><Type>none</Type></Label><Input><Button>Log On</Button></Input></Requirement>
</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

> **Hinweis:**
>
> Weitere Informationen zu verschiedenen nFactor-bezogenen Themen finden Sie unter nFactor-Authentifizierung.

Setzen eines Cookies mit nFactor

February 24, 2022

Sie können die benutzerdefinierten nFactor-Labels anwenden und ein Cookie als Faktor des Authentifizierungsflusses festlegen. Durch benutzerdefinierte Labels können Sie JavaScript verwenden, um das Anmeldeschema zu manipulieren.

Um ein Cookie als Faktor festzulegen, müssen Sie dem Benutzer keine Informationen anzeigen, die ohne Schema-Anmeldung ausgeführt werden. Stattdessen müssen Sie mit dem Browser des Benutzers interagieren, um das Anmeldeschema anzuweisen, die gewünschten Daten zu speichern. Ein Anmeldeschema ist erforderlich, um das Cookie zu setzen, wenn die Seite geladen wird. Das Cookie wird mit einem benutzerdefinierten Label und JavaScript-Code gesetzt.

Um einen Faktor zu implementieren, der ein Cookie setzt, erstellen Sie eine XML-Datei mit dem Namen cookie.xml, um das Schema im Verzeichnis /nsconfig/loginschema/ mit folgendem Inhalt zu speichern:

```
<?xml version="1.0" encoding="UTF-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response/1">
<Status>success</Status>
<Result>more-info</Result>
<StateContext></StateContext>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>

<Requirement>
<Credential><ID>nsg_cookie</ID><Type>nsg_cookie</Type></Credential>
<Label><Text>Logon Type:</Text><Type>Plain</Type></Label>
</Requirement>

<Requirement>
<Credential><ID>loginBtn</ID><Type>none</Type></Credential>
<Label><Type>none</Type></Label><Input><Button>Log On</Button></Input>
</Requirement>

</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
```



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

In diesem XML;

- Das benutzerdefinierte Label nsg_cookie wird verwendet, um das Cookie zu erstellen und das Formular sowie die Formularschaltfläche abzusenden.
- Das RFWebUI_Custom ist das neue Portal-Thema, das auf dem RFWebUI-Thema basiert.

Schritte zum Setzen eines Cookie mit nFactor

1. Erstellen Sie ein Portal-Thema basierend auf dem RFWebUI-Thema.

```
1 add vpn portaltheme RfWebUI_custom -basetheme RfWebUI
2 <!--NeedCopy-->
```

Dieser Befehl erstellt einen Ordner für dieses Thema unter /var/netscaler/logon/themes/RfWebUI_Custom

2. Bearbeiten Sie die Datei /var/netscaler/logon/themes/RfWebUI_custom/script.js und fügen Sie das folgende Skript hinzu:

```
1  CTXS.ExtensionAPI.addCustomCredentialHandler({
2
3      // The name of the credential, must match the type returned by
           the server
4      getCredentialTypeName: function () {
5    return "nsg_cookie";  }
6   ,
7      // Generate HTML for the custom credential
8      getCredentialTypeMarkup: function (requirements) {
9
10         var div = $("<div></div>");
11         $(document).ready(function() {
12
13         //Set cookie valid for 1000 days
14         var exdays = 1000;
15         var d = new Date();
16         d.setTime(d.getTime() + (exdays\*24\*60\*60\*1000));
17         var expires = "expires="+ d.toUTCString();
18         document.cookie = "NSC_COOKIE_NAME=CookieValue;" + expires
               + ";path=/";
19
```



```
20          //Submit form
21          document.getElementById('loginBtn').click();
22           }
23   );
24          return div;
25       }
26
27   }
28   );
29  <!--NeedCopy-->
```

Dieser Code führt Folgendes aus:

- Wartet darauf, dass der Browser das Laden der Seite abgeschlossen hat
- Setzt ein Cookie namens NSC_COOKIE_NAME mit dem Wert CookieValue, gültig für 1000 Tage
- Sendet das Formular automatisch.

Das Cookie wird erstellt und der Benutzer muss nicht mit der Seite interagieren.

3. Erstellen Sie ein Anmeldeschema, das an die Policy Label gebunden wird, die den festgelegten Cookie-Faktor darstellt

```
1  add authentication loginSchema Cookie_LS -authenticationSchema "/
      nsconfig/loginschema/cookie.xml"
2  <!--NeedCopy-->
```

4. Erstellen Sie eine NO_AUTHN-Authentifizierungsrichtlinie, um sie an die Policy Label zu binden, die den festgelegten Cookie-Faktor darstellt.

```
1  add authentication Policy NO_AUTHN_POL -rule TRUE -action NO_AUTHN
2  <!--NeedCopy-->
```

Diese Richtlinie wird immer als wahr ausgewertet und führt den Benutzer zum nächsten Faktor oder schließt den Authentifizierungsablauf ab.

5. Binden Sie das Portaldesign RFWebUI_Custom an den virtuellen Citrix Gateway -Server oder den virtuellen Citrix ADC AAA-Server.

Beispielbereitstellungen mit nFactor-Authentifizierung

July 27, 2022

Im Folgenden sind die Beispielbereitstellungen mit nFactor-Authentifizierung aufgeführt:

- Zwei Kennwörter im Voraus erhalten, Passthrough im nächsten Faktor. Read
- Gruppenextraktion gefolgt von Zertifikat- oder LDAP-Authentifizierung, basierend auf der Gruppenmitgliedschaft. Read
- SAML gefolgt von LDAP- oder Zertifikatauthentifizierung, basierend auf Attributen, die während SAML extrahiert wurden Read
- SAML im ersten Faktor, gefolgt von Gruppenextraktion und dann LDAP- oder Zertifikatauthentifizierung, basierend auf extrahierten Gruppen. Read
- Vorfüllen des Benutzernamens aus dem Zertifikat. Read
- Zertifikatauthentifizierung gefolgt von Gruppenextraktion für 401 virtuelle Server mit aktiviertem Verkehrsmanagement. Read
- Benutzername und zwei Kennwörter mit Gruppenextraktion im dritten Faktor. Read
- Fallback von Zertifikaten auf LDAP in derselben Kaskade; ein virtueller Server für Zertifikat- und LDAP-Authentifizierung. Read
- LDAP im ersten Faktor und WebAuth im zweiten Faktor. Read
- Domänen-Dropdown im ersten Faktor, dann verschiedene Policy-Bewertungen basierend auf der Gruppe. Read

Alle Wie-Macht-Man-Artikel

October 5, 2021

Die Authentifizierung, Autorisierung und Auditing “How to articles” sind einfach, relevant und einfach zu implementierende Artikel. Diese Artikel enthalten Informationen zu einigen der gängigen Authentifizierungs-, Autorisierungs- und Überwachungsfunktionen wie LDAP-Authentifizierung und Multifaktor-Authentifizierung. Einige der beliebten Artikel zur Konfiguration und Fehlerbehebung bei der Authentifizierung über Citrix ADC finden Sie unter Citrix ADC Authentication: Wie mache ich?

Endpunkt-Analyse

Konfigurieren Sie den Endpunktanalyse-Scan vor der Authentifizierung als Faktor in der nFactor-Authentifizierung

Konfigurieren der Endpunktanalyse nach der Authentifizierung als Faktor in der Citrix ADC nFactor-Authentifizierung

Konfigurieren Sie den EPA-Scan vor der Authentifizierung und nach der Authentifizierung als Faktor der nFactor-Authentifizierung

Konfigurieren des periodischen Endpunktanalyse-Scans als Faktor bei der nFactor-Authentifizierung

Konfigurationskombinationen erster Faktor und zweiter Faktor

Konfigurieren von nFactor für Citrix Gateway mit WebAuth im ersten Faktor und LDAP mit Kennwortänderung im zweiten Faktor

Konfigurieren Sie SAML, gefolgt von LDAP- oder Zertifikatauthentifizierung basierend auf SAML-Attributextraktion in der nFactor-Authentifizierung

Konfigurieren der Zertifikatauthentifizierung als erster Faktor und LDAP als zweiter Faktor in der Citrix ADC nFactor-Authentifizierung

Konfigurieren der Zwei-Faktor-Authentifizierung mit einem Anmeldeschema und einem Passthrough-Schema in Citrix ADC nFactor-Authentifizierung

Konfigurieren von Benutzernamen und zwei Kennwörtern mit Gruppenextraktion im dritten Faktor durch nFactor-Authentifizierung

Konfigurieren Sie das Dropdownmenü für Domäne, Benutzername und Kennwort in der ersten Faktor- und Richtlinienbewertung basierend auf Gruppen im nächsten Faktor

Konfigurieren Sie die eingabebasierte Gruppenextraktion der E-Mail-ID (oder des Benutzernamens) beim ersten Faktor, um den nächsten Faktor-Authentifizierungsablauf zu entscheiden

Konfigurieren Sie eine Domänen-Dropdownliste für Benutzereingaben im ersten Faktor, um den nächsten Faktor-Authentifizierungsablauf zu entscheiden

EULA als Authentifizierungsfaktor

EULA als Authentifizierungsfaktor im Citrix ADC nFactor-System konfigurieren

Benutzernamen aus Zertifikat vorfüllen

Konfigurieren des Vorfüllbenutzernamens aus dem Zertifikat in der Citrix ADC nFactor-Authentifizierung

Step-up-Authentifizierung

Konfigurieren Sie nFactor für Anwendungen mit unterschiedlichen Anforderungen an die Anmeldesite einschließlich Step-up-Authentifizierung

SAML-Authentifizierung

October 5, 2021

Security Assertion Markup Language (SAML) ist ein XML-basierter Authentifizierungsmechanismus, der Single Sign-On-Funktionen bietet und vom OASIS Security Services Technical Committee definiert wird.

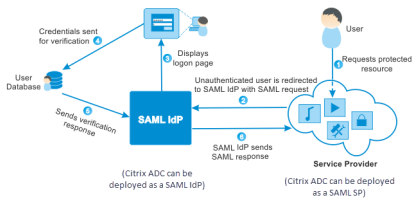
> Hinweis:
>
> Ab NetScaler 12.0 Build 51.x füllt die Citrix ADC Appliance, die als SAML-Dienstanbieter (SP) mit Multi-Factor (nFactor) -Authentifizierung verwendet wird, jetzt das Feld Benutzername auf der Anmeldeseite vorab aus. Die Appliance sendet ein NameID-Attribut als Teil einer SAML-Autorisierungsanforderung, ruft den NameID-Attributwert vom Citrix ADC SAML-Identitätsanbieter (IdP) ab und füllt das Feld Benutzername vorab aus.

Warum die SAML-Authentifizierung verwenden?

Betrachten Sie ein Szenario, in dem ein Dienstanbieter (LargeProvider) eine Reihe von Anwendungen für einen Kunden (BigCompany) hostet. BigCompany hat Benutzer, die nahtlos auf diese Anwendungen zugreifen müssen. In einem traditionellen Setup müsste LargeProvider eine Datenbank mit Benutzern von BigCompany pflegen. Dies wirft Bedenken für jeden der folgenden Interessengruppen auf:

- LargeProvider muss die Sicherheit der Benutzerdaten gewährleisten.
- BigCompany muss die Benutzer validieren und die Benutzerdaten auf dem neuesten Stand halten, nicht nur in der eigenen Datenbank, sondern auch in der von LargeProvider verwalteten Benutzerdatenbank. Beispielsweise muss ein Benutzer, der aus der BigCompany-Datenbank entfernt wurde, ebenfalls aus der LargeProvider-Datenbank entfernt werden.
- Ein Benutzer muss sich bei jeder der gehosteten Anwendungen einzeln anmelden.

Der SAML-Authentifizierungsmechanismus bietet einen alternativen Ansatz. Das folgende Deployment-Diagramm zeigt, wie SAML funktioniert (SP-initiierter Flow).



Die durch traditionelle Authentifizierungsmechanismen aufgeworfenen Bedenken werden wie folgt gelöst:

- LargeProvider muss keine Datenbank für BigCompany Benutzer pflegen. Von der Identitätsverwaltung befreit, kann sich LargeProvider auf die Bereitstellung besserer Services konzentrieren.
- BigCompany trägt nicht die Last, sicherzustellen, dass die LargeProvider-Benutzerdatenbank mit ihrer eigenen Benutzerdatenbank synchronisiert ist.
- Ein Benutzer kann sich einmal bei einer Anwendung anmelden, die auf LargeProvider gehostet wird, und automatisch bei den anderen dort gehosteten Anwendungen angemeldet werden.

Die Citrix ADC-Appliance kann als SAML Service Provider (SP) und SAML Identity Provider (IdP) bereitgestellt werden. Lesen Sie die relevanten Themen, um die Konfigurationen zu verstehen, die auf der Citrix ADC-Appliance ausgeführt werden müssen.

Eine Citrix ADC Appliance, die als SAML-Dienstanbieter konfiguriert ist, kann nun eine Überprüfung der Zielgruppeneinschränkung erzwingen. Die Zielgruppeneinschränkungsbedingung wird nur dann als Gültig ausgewertet, wenn die SAML-antwortende Partei Mitglied mindestens einer der angegebenen Zielgruppen ist.

Sie können eine Citrix ADC Appliance so konfigurieren, dass Attribute in SAML-Assertionen als Gruppenattribute analysiert werden. Wenn Sie sie als Gruppenattribute analysieren, kann die Appliance Richtlinien an die Gruppen binden.

Citrix ADC als SAML-SP

October 5, 2021

Der SAML-Dienstanbieter (SP) ist eine SAML-Entität, die vom Dienstanbieter bereitgestellt wird. Wenn ein Benutzer versucht, auf eine geschützte Anwendung zuzugreifen, wertet der SP die Clientanforderung aus. Wenn der Client nicht authentifiziert ist (hat kein gültiges NSC_TMAA oder NSC_TMAS Cookie), leitet der SP die Anforderung an den SAML Identity Provider (IdP) um.

Der SP validiert auch SAML-Assertions, die vom IdP empfangen werden.

Wenn die Citrix ADC Appliance als SP konfiguriert ist, werden alle Benutzeranforderungen von einem virtuellen Server zur Datenverkehrsverwaltung (Lastausgleich oder Content Switching) empfangen, der der entsprechenden SAML-Aktion zugeordnet ist.

Die Citrix ADC Appliance unterstützt auch POST- und Umleitungs-Bindungen während der Abmeldung.

> **Hinweis:**
>
> Eine Citrix ADC Appliance kann als SAML-SP in einer Bereitstellung verwendet werden, in der der SAML-IdP entweder auf der Appliance oder auf einem externen SAML-IdP konfiguriert ist.

Bei Verwendung als SAML-SP gilt eine Citrix ADC Appliance:

- Kann die Benutzerinformationen (Attribute) aus dem SAML-Token extrahieren. Diese Informationen können dann in den Richtlinien verwendet werden, die auf der Citrix ADC Appliance konfiguriert sind. Wenn Sie beispielsweise die Attribute GroupMember und Emailaddress extrahieren möchten, geben Sie im SAMLAction den Parameter **Attribute2** als GroupMember und den Parameter **Attribute3** als emailaddress an.

  > **Hinweis:**
  >
  > Standardattribute wie Benutzername, Kennwort und Abmelde-URL dürfen nicht in den Attributen 1—16 extrahiert werden, da sie implizit analysiert und in der Sitzung gespeichert werden.

- Kann Attributnamen von bis zu 127 Byte aus einer eingehenden SAML-Assertion extrahieren. Die vorherige Grenze betrug 63 Bytes.
- Unterstützt Post-, Umleitungs- und Artefakt-Bindungen.

  > **Hinweis:**
  >
  > Umleitungsbindung sollte nicht für große Datenmengen verwendet werden, wenn die Assertion nach dem Aufblasen oder Decodieren größer als 10K ist.

- Kann Behauptungen entschlüsseln.
- Kann mehrwertige Attribute aus einer SAML-Assertion extrahieren. Diese Attribute werden gesendet verschachtelte XML-Tags wie:

  <AttributeValue> <AttributeValue>Wert1
  </AttributeValue> <AttributeValue> Wert2
  </AttributeValue> </AttributeValue>

  > **Hinweis:**
  >
  > Ab Citrix ADC 13.0 Build 63.x und höher wurde die individuelle maximale Länge für SAML-Attribute erhöht, um ein Maximum von 40.000 Byte zu ermöglichen. Die Größe aller Attribute darf 40.000 Bytes nicht überschreiten.

  Wenn die Citrix ADC-Appliance mit vorherigem XML dargestellt wird, kann die Citrix ADC-Appliance sowohl Value1 als auch Value2 als Werte eines bestimmten Attributs extrahieren, im Gegensatz zu der alten Firmware, die nur Value1 extrahiert.

- Kann die Gültigkeit einer SAML-Assertion angeben.

  Wenn die Systemzeit für Citrix ADC-SAML-IdP und der Peer-SAML-SP nicht synchron ist, werden die Nachrichten möglicherweise von beiden Parteien ungültig. Um solche Fälle zu vermeiden, können Sie jetzt die Zeitdauer konfigurieren, für die die Assertions gültig sind.

  Diese Dauer, die als “Verzerrungszeit” bezeichnet wird, gibt die Anzahl der Minuten an, für die

die Nachricht akzeptiert werden soll. Die Verzerrungszeit kann auf dem SAML-SP und dem SAML-IdP konfiguriert werden.

- Kann ein zusätzliches Attribut namens 'ForceAuth' in der Authentifizierungsanforderung an externen IdP (Identity Provider) senden. Standardmäßig ist ForceAuthn auf Falsch gesetzt. Es kann auf 'True' gesetzt werden, um IdP vorzuschlagen, um die Authentifizierung trotz vorhandener Authentifizierungskontext zu erzwingen. Außerdem führt Citrix ADC SP Authentifizierungsanforderung im Abfrageparameter durch, wenn mit Artefaktbindung konfiguriert wird.

So konfigurieren Sie die Citrix ADC Appliance mit der Befehlszeilenschnittstelle als SAML-SP

1. Konfigurieren Sie eine SAML-SP-Aktion.

   Beispiel

   Mit dem folgenden Befehl wird eine SAML-Aktion hinzugefügt, die nicht authentifizierte Benutzeranforderungen umleitet.

   ```
   add authentication samlAction SamlSPAct1 -samlIdPCertName nssp -samlSigningCertNa
    nssp -samlRedirectUrl https://auth1.example.com -relaystateRule "AAA.
   LOGIN.RELAYSTATE.EQ(\"https://lb.example1.com/\")"
   ```

   Punkte zu beachten

   - Das `-samlIdPCertName` im SamlAction-Befehl angegebene Zertifikat muss mit dem entsprechenden Zertifikat von IdP übereinstimmen, damit die Signaturüberprüfung erfolgreich ist.
   - SAML unterstützt nur das RSA-Zertifikat. Andere Zertifikate wie HSM, FIPS usw. werden nicht unterstützt.
   - Citrix empfiehlt, einen vollständigen Domänennamen mit dem nachfolgenden '/' im Ausdruck zu haben.
   - Administratoren müssen einen Ausdruck für **RelaysStateRule** im Befehl samlAction konfigurieren. Der Ausdruck muss die Liste der veröffentlichten Domänen enthalten, mit denen der Benutzer eine Verbindung herstellt, bevor er zum virtuellen Authentifizierungsserver umgeleitet wird. Der Ausdruck muss beispielsweise die Domänen des virtuellen Front-End-Servers (VPN, LB oder CS) enthalten, die diese SAML-Aktion zur Authentifizierung verwenden.

   Weitere Informationen zum Befehl finden Sie unter https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlAction und https://support.citrix.com/article/CTX316577.

2. Konfigurieren Sie die SAML-Richtlinie.

Beispiel

Der folgende Befehl definiert eine SAML-Richtlinie, die die zuvor definierte SAML-Aktion auf den gesamten Datenverkehr anwendet.

```
add authentication policy SamlSPPol1 -rule true -action SamlSPAct1
```

3. Binden Sie die SAML-Richtlinie an den virtuellen Authentifizierungsserver.

   Beispiel

   Der folgende Befehl bindet die SAML-Richtlinie an einen virtuellen Authentifizierungsserver mit dem Namen av_saml.

   ```
   bind authentication vserver av_saml -policy SamlSPPol1
   ```

4. Binden Sie den virtuellen Authentifizierungsserver an den entsprechenden virtuellen Server für die Datenverkehrsverwaltung.

   Beispiel

   Der folgende Befehl fügt einen virtuellen Lastausgleichsserver mit dem Namen lb1_ssl hinzu und ordnet den virtuellen Authentifizierungsserver mit dem Namen av_saml dem virtuellen Lastausgleichsserver zu.

   ```
   add lb vserver lb1_ssl SSL 10.217.28.224 443 -persistenceType NONE -
   cltTimeout 180 -AuthenticationHost auth1.example.com -Authentication ON
    -authnVsName av_saml
   ```

   Weitere Informationen zum Befehl finden Sie unter https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlAction

So konfigurieren Sie eine Citrix ADC Appliance als SAML-SP mit der GUI

1. Navigieren Sie zu **Sicherheit>AAA-Richtlinien>Authentifizierung> Grundrichtlinien>SAML**.
2. Wählen Sie die Registerkarte **Server** aus, klicken Sie auf **Hinzufügen**, geben Sie Werte für die folgenden Parameter ein und klicken Sie auf **Erstellen**.

   Parameter-Beschreibung:

   Name - Name des Servers

   URL umleiten - URL, gegen die sich Benutzer authentifizieren werden. Einige IdPs haben spezielle URLs, die nur unter SAML-Setup erreichbar sind.

   Single Logout-URL - Eine URL wurde angegeben, damit der Citrix ADC erkennen kann, wann der Client zurück an den IdP gesendet werden muss, um den Abmeldevorgang abzuschließen. Wir werden es in dieser einfachen Bereitstellung nicht verwenden.

SAML Binding - Methode, die verwendet wird, um den Client vom SP auf den IdP zu verschieben. Dies muss auf dem IdP gleich sein, damit er versteht, wie sich der Client mit ihm verbinden wird. Wenn der Citrix ADC als SP fungiert, unterstützt er POST-Bindungen, REDIRECT und ARTIFACT.

Logout Bindung - REDIRECT

Name des IDP-Zertifikats - IDPcert-Zertifikat (Base64) unter SAML-Signaturzertifikat vorhanden.

Benutzerfeld - Abschnitt des SAML-Authentifizierungsformulars des IdP, der den Benutzernamen enthält, den SP bei Bedarf extrahieren soll.

Signieren des Zertifikatsnamens - Wählen Sie das SAML SP-Zertifikat (mit privatem Schlüssel) aus, das Citrix ADC verwendet, um Authentifizierungsanforderungen an den IdP zu signieren. Das gleiche Zertifikat (ohne privaten Schlüssel) muss in den IdP importiert werden, damit der IdP die Signatur der Authentifizierungsanforderung überprüfen kann. Dieses Feld wird von den meisten IDPs nicht benötigt.

Name des Ausstellers - Identifikator. Eindeutige ID, die sowohl auf dem SP als auch im IdP angegeben ist, um den Dienstanbieter untereinander zu identifizieren.

Unsignierte Assertion ablehnen - Option, die Sie angeben können, wenn die Assertions vom IdP signiert werden müssen. Sie können sicherstellen, dass nur die Behauptung unterschrieben werden muss (ON) oder sowohl die Behauptung als auch die Antwort des IdP unterschrieben werden müssen (STRICT).

Zielgruppe - Zielgruppe, für die vom IdP gesendete Assertion anwendbar ist. Dies ist normalerweise der Entitätsname oder die URL, die ServiceProvider repräsentiert.

Signaturalgorithmus - RSA-SHA256

Digest-Methode - SHA256

Standard-Authentifizierungsgruppe - Die Standardgruppe, die ausgewählt wird, wenn die Authentifizierung zusätzlich zu extrahierten Gruppen erfolgreich ist.

Gruppennamenfeld - Name des Tags in Assertion, das Benutzergruppen enthält.

Skew Time (min) - Diese Option gibt die zulässige Taktverzerrung in der Anzahl von Minuten an, die Citrix ADC ServiceProvider für eine eingehende Assertion zulässt.

3. Erstellen Sie in ähnlicher Weise eine entsprechende SAML-Richtlinie und binden Sie sie an den virtuellen Authentifizierungsserver.

   Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Virtuelle Server**, und ordnen Sie die SAML-Richtlinie dem virtuellen Authentifizierungsserver zu.

4. Ordnen Sie den Authentifizierungsserver dem entsprechenden virtuellen Server zur Datenverkehrsverwaltung zu.

Navigieren Sie zu **Traffic Management > Load Balancing** (oder **Content Switching**) > **Virtuelle Server**, wählen Sie den virtuellen Server aus, und ordnen Sie ihm den virtuellen Authentifizierungsserver zu.

Citrix ADC als SAML-IdP

October 5, 2021

Der SAML-IdP (Identity Provider) ist eine SAML-Entität, die im Kundennetzwerk bereitgestellt wird. Der IdP empfängt Anforderungen vom SAML-SP und leitet Benutzer auf eine Anmeldeseite um, auf der sie ihre Anmeldeinformationen eingeben müssen. Der IdP authentifiziert diese Anmeldeinformationen beim Active Directory (externer Authentifizierungsserver wie LDAP) und generiert dann eine SAML-Assertion, die an den SP gesendet wird.

Der SP überprüft das Token, und dem Benutzer wird dann Zugriff auf die angeforderte geschützte Anwendung gewährt.

Wenn die Citrix ADC Appliance als IdP konfiguriert ist, werden alle Anforderungen von einem virtuellen Authentifizierungsserver empfangen, der dem relevanten SAML-IdP-Profil zugeordnet ist.

> **Hinweis:**
>
> Eine Citrix ADC Appliance kann als IdP in einer Bereitstellung verwendet werden, in der der SAML-SP entweder auf der Appliance oder auf einem externen SAML-SP konfiguriert ist.

Bei Verwendung als SAML-IdP gilt eine Citrix ADC-Appliance:

- Unterstützt alle Authentifizierungsmethoden, die für herkömmliche Anmeldungen unterstützt werden.
- Signiert Behauptungen digital.
- Unterstützt Ein-Faktor- und Zwei-Faktor-Authentifizierung. SAML darf nicht als sekundärer Authentifizierungsmechanismus konfiguriert werden.
- Kann Assertionen mit dem öffentlichen Schlüssels des SAML-SP verschlüsseln. Dies wird empfohlen, wenn die Assertion vertrauliche Informationen enthält.
- Kann so konfiguriert werden, dass nur digital signierte Anforderungen vom SAML-SP akzeptiert werden.
- Kann sich mit den folgenden 401-basierten Authentifizierungsmechanismen beim SAML-IdP anmelden: Negotiate, NTLM und Certificate.
- Kann so konfiguriert werden, dass zusätzlich zum NameID-Attribut 16 Attribute gesendet werden. Die Attribute müssen vom entsprechenden Authentifizierungsserver extrahiert werden.

Für jeden von ihnen können Sie den Namen, den Ausdruck, das Format und einen Anzeigenamen im SAML-IdP-Profil angeben.

- Wenn die Citrix ADC-Appliance als SAML-IdP für mehrere SAML-SP konfiguriert ist, kann ein Benutzer Zugriff auf Anwendungen auf den verschiedenen SPs erhalten, ohne sich jedes Mal explizit zu authentifizieren. Die Citrix ADC-Appliance erstellt ein Sitzungscookie für die erste Authentifizierung, und jede weitere Anforderung verwendet dieses Cookie zur Authentifizierung.
- Kann mehrwertige Attribute in einer SAML-Assertion senden.
- Unterstützt Post- und Umleitungsbindungen. Die Unterstützung für die Artefaktbindung wird in Citrix ADC Version 13.0 Build 36.27 eingeführt.
- Kann die Gültigkeit einer SAML-Assertion angeben.

  Wenn die Systemzeit für Citrix ADC-SAML-IdP und der Peer-SAML-SP nicht synchron ist, werden die Nachrichten möglicherweise von beiden Parteien ungültig. Um solche Fälle zu vermeiden, können Sie jetzt die Zeitdauer konfigurieren, für die die Assertions gültig sind.

  Diese Dauer, die sogenannte Schrägzeit, gibt die Anzahl der Minuten an, für die die Nachricht akzeptiert werden muss. Die Verzerrungszeit kann auf dem SAML-SP und dem SAML-IdP konfiguriert werden.
- Kann so konfiguriert werden, dass Assertions nur für SAML-SPs bereitgestellt werden, die auf dem IdP vorkonfiguriert oder vom IdP vertrauenswürdig sind. Für diese Konfiguration muss der SAML-IdP die Dienstanbieter-ID (oder Name des Ausstellers) der relevanten SAML-SPs haben.

  > **Hinweis:**
  >
  > Bevor Sie fortfahren, stellen Sie sicher, dass Sie über einen virtuellen Authentifizierungsserver verfügen, der mit einem LDAP-Authentifizierungsserver verknüpft ist.

So konfigurieren Sie eine Citrix ADC Appliance als SAML-IdP mit der Befehlszeilenschnittstelle

1. Konfigurieren Sie ein SAML-IdP-Profil.

   Beispiel

   Hinzufügen von Citrix ADC Appliance als IdP mit SiteMinder als SP.

   ```
   add authentication samlIdPProfile samlIDPProf1 -samlSPCertName siteminder
   -cert -encryptAssertion ON -samlIdPCertName ns-cert -assertionConsumerServiceURL
    http://sm-proxy.nsi-test.com:8080/affwebservices/public/saml2assertionconsumer
    -rejectUnsignedRequests ON -signatureAlg RSA-SHA256 -digestMethod
   SHA256 -acsUrlRule AAA.LOGIN.SAML_REQ_ACS_URL.REGEX_MATCH(re##^https://
   example2\.com/cgi/samlauth$##)
   ```


Punkte zu beachten

- Konfigurieren Sie im SAML-IdP-Profil **AcsURLRule**, die einen Ausdruck der Liste der anwendbaren Dienstanbieter-URLs für diesen IdP verwendet. Dieser Ausdruck hängt vom verwendeten SP ab. Wenn Citrix ADC als SP konfiguriert ist, wird die ACS-URL angezeigt `https://<SP-domain_name>/cgi/samlauth`. Citrix empfiehlt, eine vollständige URL im Ausdruck zum Abgleichen zu haben.
- SAML unterstützt nur das RSA-Zertifikat. Andere Zertifikate wie HSM, FIPS usw. werden nicht unterstützt.
- Sie müssen den Start der Domain mit dem Zeichen "^" (Beispiel: ^https) zusammen mit dem Dollarzeichen "$" am Ende der Zeichenfolge angeben (Beispiel: samlauth$).

Weitere Informationen zum Befehl finden Sie unter https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlAction und https://support.citrix.com/article/CTX316577.

2. Konfigurieren Sie die SAML-Authentifizierungsrichtlinie, und ordnen Sie das SAML-IdP-Profil als Aktion der Richtlinie zu.

```
add authentication samlIdPPolicy samlIDPPol1 -rule true -action samlIDPProf1
```

3. Binden Sie die Richtlinie an den virtuellen Authentifizierungsserver.

```
bind authentication vserver saml-auth-vserver -policy samlIDPPol1 -
priority 100
```

Weitere Informationen zum Befehl finden Sie unter https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/authentication/authentication-samlIdPProfile.

So konfigurieren Sie eine Citrix ADC Appliance als SAML-IdP mit der GUI

1. Navigieren Sie zu **Sicherheit>AAA-Richtlinien>Authentifizierung> Erweiterte Richtlinien>SAML IdP**.
2. Wählen Sie die Registerkarte **Server** aus, klicken Sie auf **Hinzufügen**, geben Sie Werte für die folgenden Parameter ein und klicken Sie auf **Erstellen**.

Parameter-Beschreibung:

Assertion Consumer Service URL - URL, an die der authentifizierte Benutzer weitergeleitet wird.

IdP-Zertifikatname - Zertifikatschlüsselpaar, das für die Authentifizierungsseite verwendet wird.

Name des SP-Zertifikats - Zertifikat des Dienstanbieters In diesem Szenario ist der Schlüssel dafür nicht erforderlich.

Assertion signieren - Die Option, die Behauptung und die Antwort zu signieren, wenn der Client zurück zum Dienstanbieter weitergeleitet wird.

Name des Ausstellers - Identifikator. Eindeutige ID, die sowohl auf dem SP als auch im IdP angegeben ist, um den Dienstanbieter untereinander zu identifizieren.

Dienstanbieter-ID - Eindeutige ID, die sowohl auf dem SP als auch im IdP angegeben wird, um den Dienstanbieter untereinander zu identifizieren. Dies kann alles sein und muss nicht die unten angegebene URL sein, sondern muss sowohl im SP- als auch im IdP-Profil identisch sein.

Unsignierte Anfragen ablehnen - Option, die Sie angeben können, um sicherzustellen, dass nur mit dem SP-Zertifikat signierte Behauptungen akzeptiert werden.

Signaturalgorithmus - Algorithmus zum Signieren und Überprüfen der Behauptungen zwischen IdP und SP. Dies muss sowohl im IdP- als auch im SP-Profil identisch sein.

Digest-Methode - Algorithmus, der verwendet wird, um die Integrität der Assertions zwischen IdP und SP zu überprüfen. Dies muss sowohl im IdP- als auch im SP-Profil identisch sein.

SAML-Binding - Wie im SP-Profil beschrieben, muss es sowohl für SP als auch im IdP identisch sein.

3. Ordnen Sie die SAML-IdP-Richtlinie einem virtuellen Authentifizierungsserver zu.

   Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Virtuelle Server**, und ordnen Sie die SAML-IdP-Richtlinie dem virtuellen Authentifizierungsserver zu.

Konfigurieren von SAML-Single-Sign-On

May 10, 2022

Um Single-Sign-On-Funktionen für Anwendungen bereitzustellen, die auf dem Dienstanbieter gehostet werden, können Sie SAML-Single-Sign-On auf dem SAML-SP konfigurieren.

Konfigurieren von SAML Single Sign-On über die Befehlszeile

1. Konfigurieren Sie das SAML-SSO-Profil.

   Beispiel

   Im folgenden Befehl ist Beispiel der virtuelle Lastenausgleichsserver, der über einen Weblink vom SharePoint-Portal verfügt. Nssp.example.com ist der virtuelle Datenverkehrsverwaltungsserver, der den SharePoint-Server Lastenausgleich ausgleicht.


```
add tm samlSSOProfile tm-saml-sso -samlSigningCertName nssp -
    assertionConsumerServiceURL "https://nssp2.example.com/cgi/
    samlauth" -relaystateRule "\\"https://nssp2.example.com/
    samlsso.html\\"" -sendPassword ON -samlIssuerName nssp.example
    .com
<!--NeedCopy-->
```

2. Verknüpfen Sie das SAML-SSO-Profil mit der Traffic-Aktion.

   Beispiel

   Der folgende Befehl aktiviert SSO und bindet das oben erstellte SAML-SSO-Profil an eine Verkehrsaktion.

```
add tm trafficAction html_act -SSO ON -samlSSOProfile tm-saml-sso
<!--NeedCopy-->
```

3. Konfigurieren Sie die Verkehrsrichtlinie, die angibt, wann die Aktion ausgeführt werden muss.

   Beispiel

   Mit dem folgenden Befehl wird die Verkehrsaktion einer Verkehrsrichtlinie zugeordnet.

```
add tm trafficPolicy html_pol "HTTP.REQ.URL.CONTAINS(\\"abc.html\\
    ")" html_act
<!--NeedCopy-->
```

4. Binden Sie die zuvor erstellte Verkehrsrichtlinie an einen virtuellen Datenverkehrsverwaltungsserver (Load Balancing oder Content Switching). Alternativ kann die Verkehrsrichtlinie global zugeordnet werden.

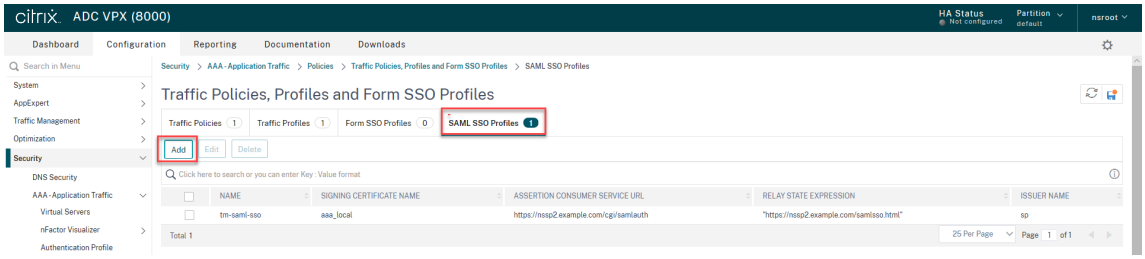
   > **Hinweis**
   >
   > Dieser virtuelle Datenverkehrsverwaltungsserver muss mit dem relevanten virtuellen Authentifizierungsserver verknüpft sein, der mit der SAML-Aktion verknüpft ist.

```
bind lb vserver lb1_ssl -policyName html_pol -priority 100 -
    gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```


Konfigurieren von SAML Single Sign-On mit der GUI

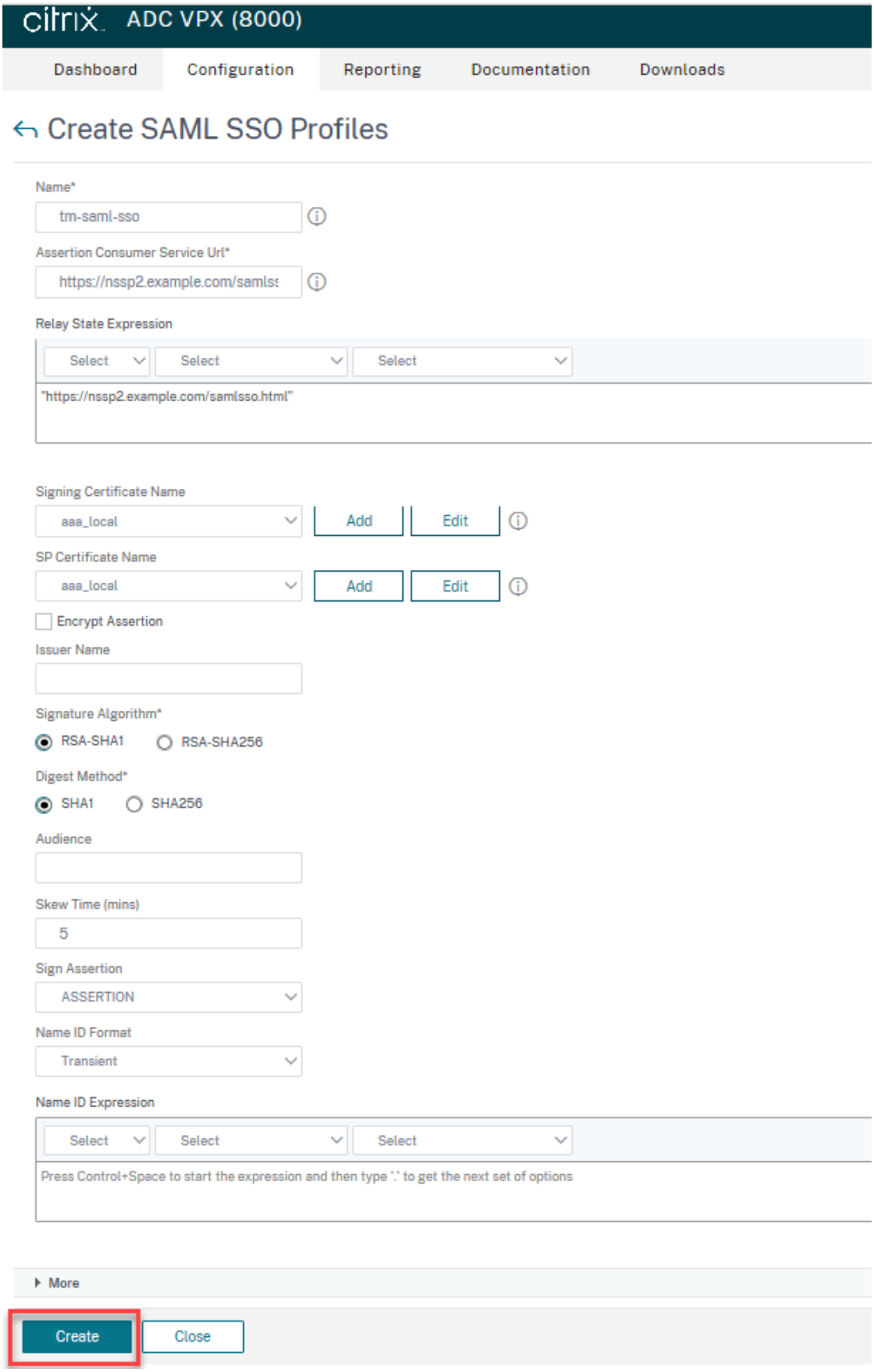
Um SAML Single Sign-On zu konfigurieren, müssen Sie das SAML-SSO-Profil, das Verkehrsprofil und die Datenverkehrsrichtlinie definieren und die Datenverkehrsrichtlinie an einen virtuellen Datenverkehrsverwaltungsserver oder global an die Citrix ADC-Appliance binden.

1. Navigieren Sie zu **Sicherheit > AAA-Anwendungsverkehr > Richtlinien > Traffic > SAML-SSO-Profile** und klicken Sie auf **Hinzufügen**.

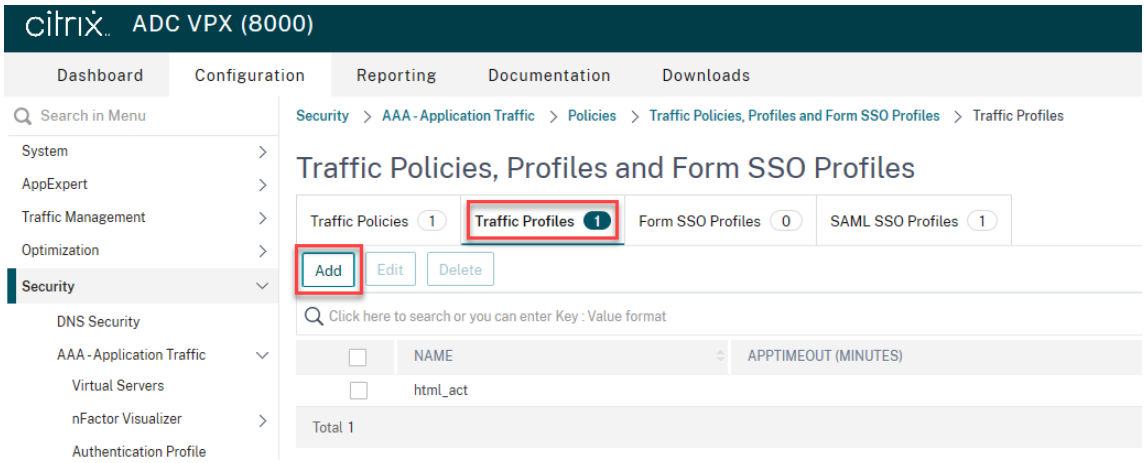


2. Geben Sie auf der Seite **SAML-SSO-Profile erstellen** Werte für die folgenden Felder ein und klicken Sie auf **Erstellen**.

   - Name - Name für das SAML SSO-Profil
   - Assertion Consumer Service Url - URL, an die die Behauptung gesendet werden soll
   - Signierzertifikatname - Name des SSL-Zertifikats, das zum Signieren von Assertion verwendet wird
   - Name des SP-Zertifikats - Name des SSL-Zertifikats einer Peer/empfangenden Partei, mit der Assertion verschlüsselt ist
   - Name des Ausstellers - Der Name, der in Anfragen verwendet werden soll, die von Citrix ADC an IdP gesendet werden, um Citrix ADC eindeutig zu identifizieren
   - Signaturalgorithmus - Algorithmus zur Signieren/Verifizierung von SAML-Transaktionen
   - Digest-Methode — Algorithmus zur Berechnung/Verifizierung von Digest für SAML-Transaktionen
   - Zielgruppe - Zielgruppe, für die eine vom IdP gesendete Assertion anwendbar ist. Dies ist normalerweise ein Entitätsname oder eine URL, die einen ServiceProvider darstellt
   - Skew Time (min) - Die Anzahl der Minuten auf beiden Seiten der aktuellen Zeit, für die die Assertion gültig wäre
   - Assertion signieren - Option zum Signieren von Teilen der Behauptung, wenn Citrix ADC IDP einen sendet. Basierend auf der Benutzerauswahl kann entweder Assertion oder Response oder Beide oder keine signiert werden.
   - Name ID Format - Format der in Assertion gesendeten Namenskennung
   - Name ID Expression - Ausdruck, der ausgewertet wird, um zu erhalten, dass NameIdentifier in Assertion gesendet werden soll

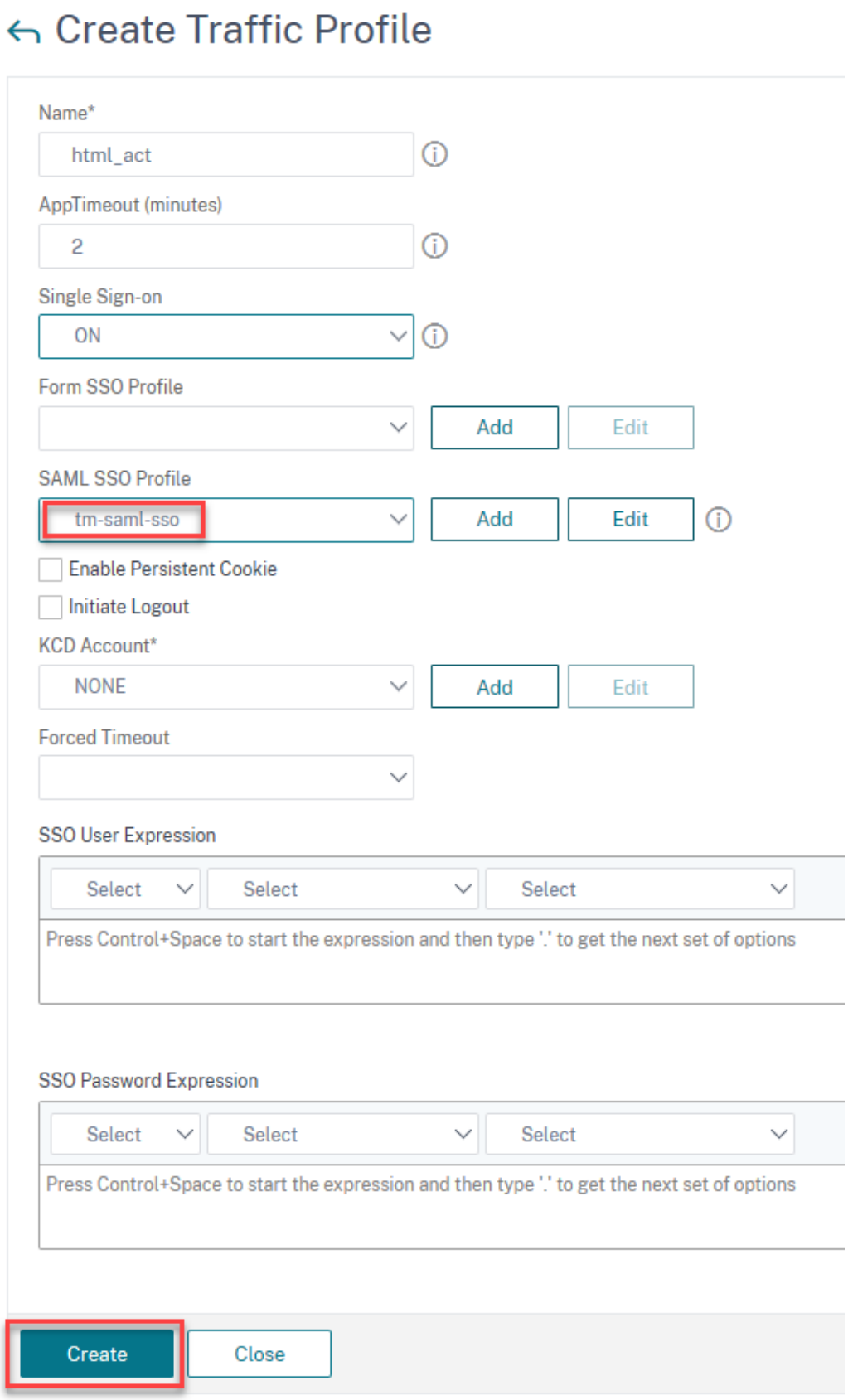


3. Navigieren Sie zu **Sicherheit > AAA-Anwendungsverkehr > Richtlinien>Traffic > Verkehrsprofile** und klicken Sie auf **Hinzufügen**.

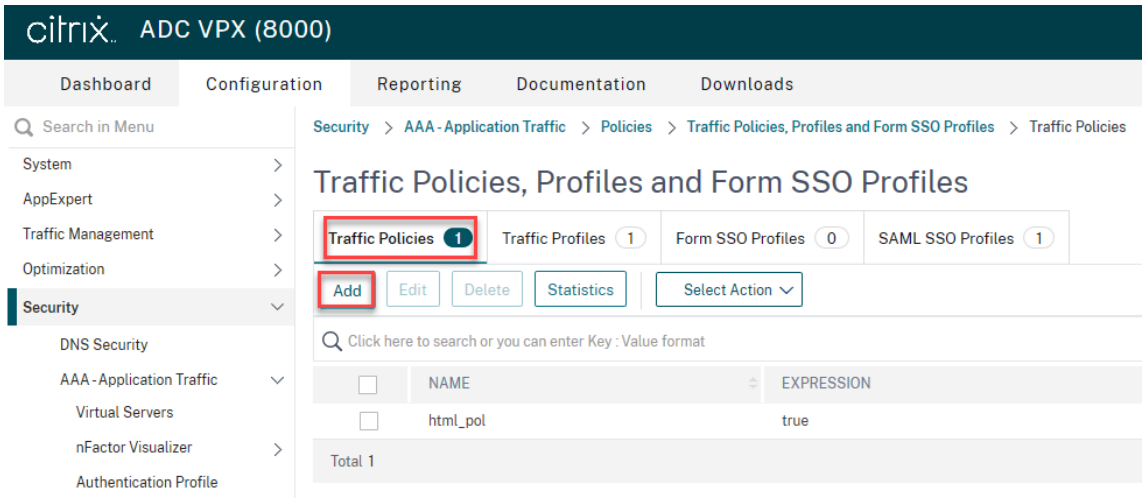


4. Geben Sie auf der Seite " **Verkehrsprofil erstellen** " Werte für die folgenden Felder ein und klicken Sie auf **Erstellen**.

   - Name - Name für die Verkehrsaktion.
   - AppTimeout (Minuten) - Zeitintervall der Benutzerinaktivität in Minuten, nach dem die Verbindung geschlossen wird.
   - Single Sign-On - Wählen Sie EIN
   - SAML SSO-Profil - Wählen Sie das erstellte SAML SSSO-Profil aus
   - KCD-Konto - Kerberos eingeschränkter Kontoname der Delegation
   - SSO User Expression - Ausdruck, der ausgewertet wird, um den Benutzernamen für Single-Signon zu erhalten
   - SSO Password Expression - Ausdruck, der ausgewertet wird, um ein Kennwort für Single-Signon zu erhalten

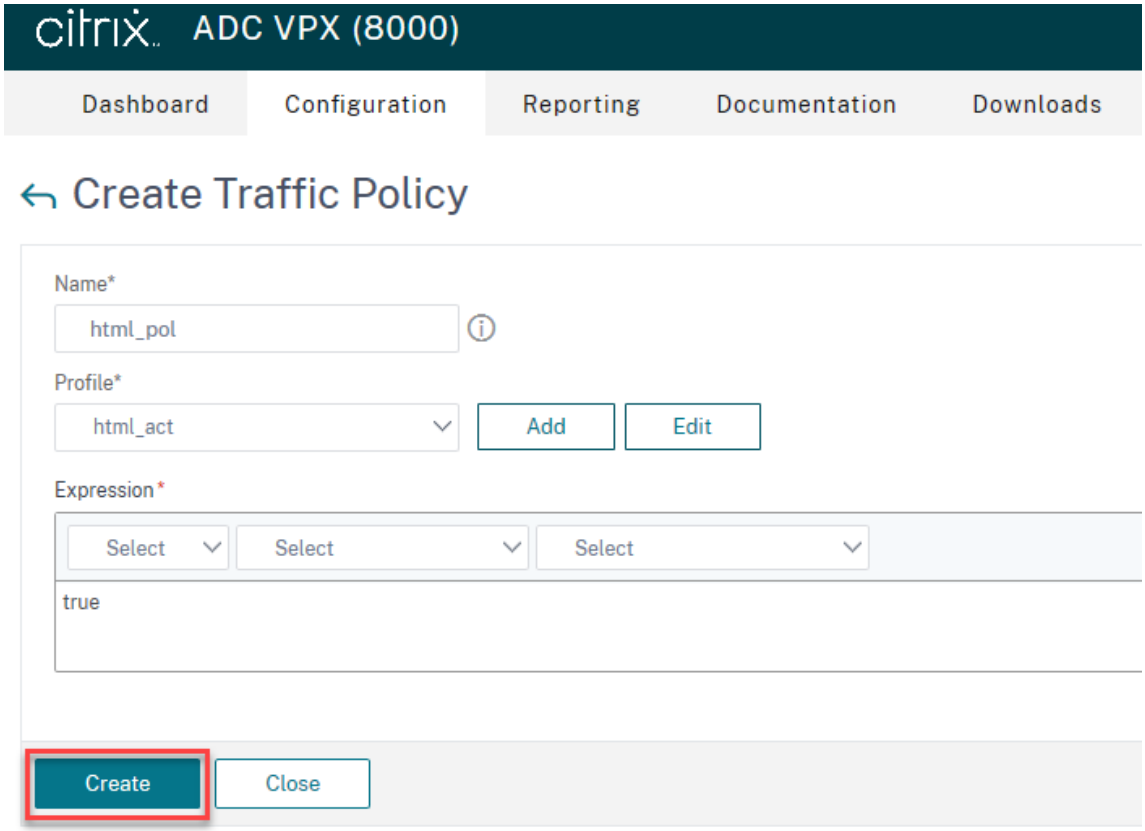


5. Navigieren Sie zu **Sicherheit > AAA-Anwendungsverkehr > Richtlinien > Traffic > Traffic Policys** und klicken Sie auf **Hinzufügen**.

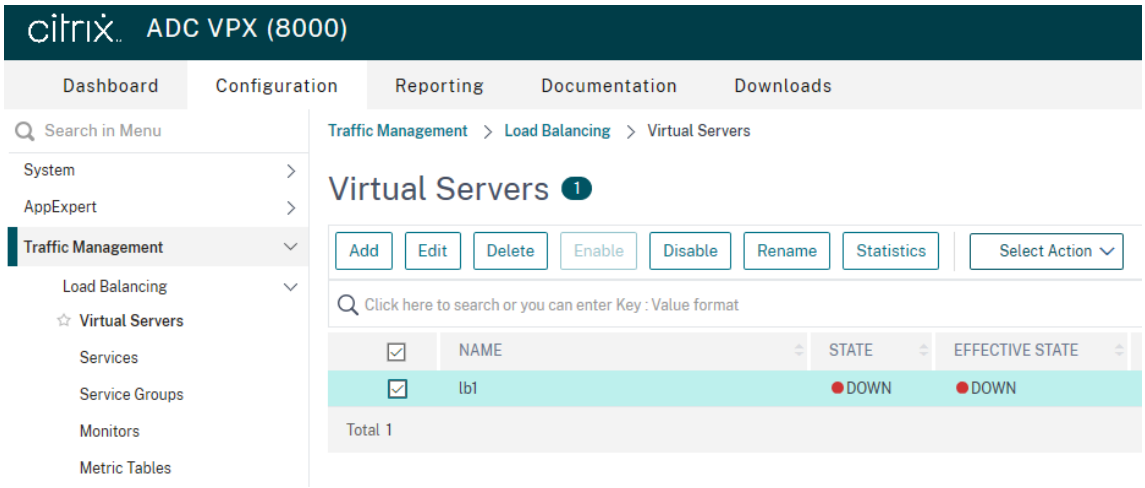


6. Geben Sie auf der Seite **Traffic-Richtlinie erstellen** Werte für Folgendes ein, und klicken Sie auf **Erstellen**.

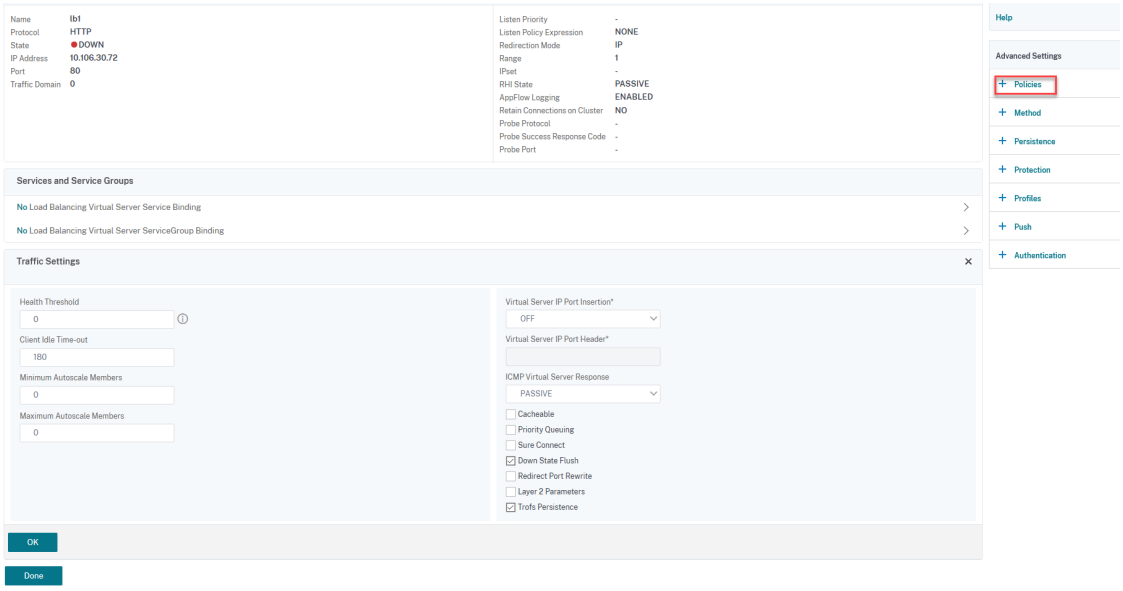
   - Name — Name der zu erstellenden Verkehrsrichtlinie
   - Profil — Wählen Sie das erstellte Verkehrsprofil
   - Ausdruck — Standard-Syntaxausdruck, den die Richtlinie verwendet, um auf eine bestimmte Anfrage zu antworten. Zum Beispiel stimmt.



7. Um die Verkehrsrichtlinie an einen virtuellen Datenverkehrsverwaltungsserver zu binden, wählen Sie einen virtuellen Server aus.



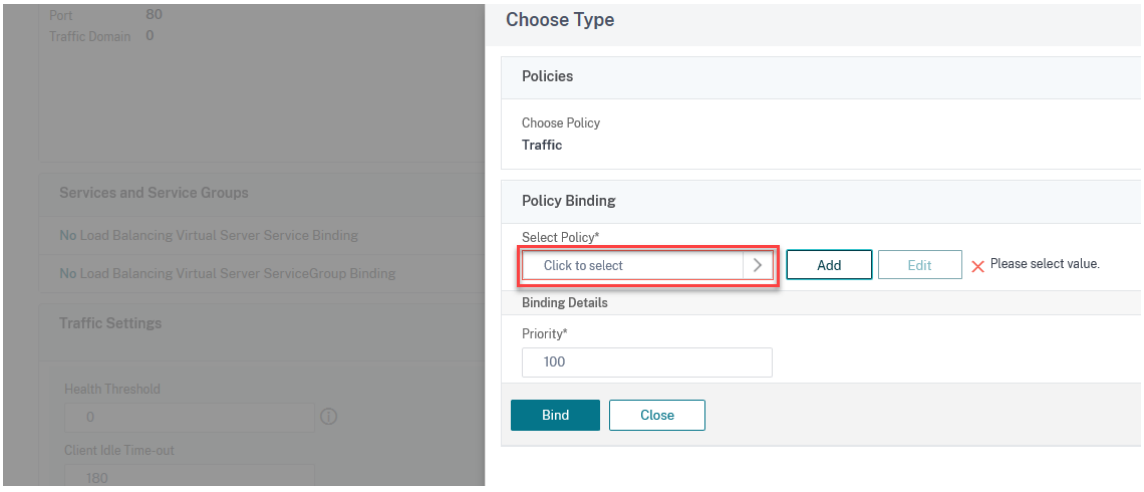
8. Klicken Sie auf **Richtlinien**.



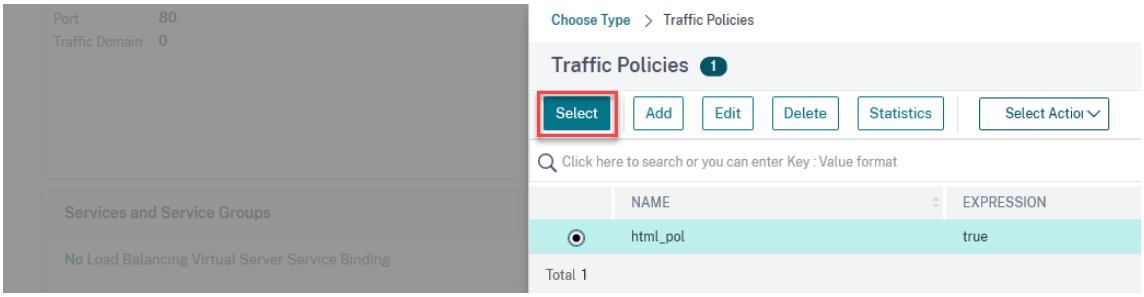
9. Wählen Sie im Feld **Richtlinie auswählen** die Option **Traffic** aus, wählen Sie im Feld **Typ auswählen** die Option **Anforderung** aus, und klicken Sie auf **Weiter**.

   ! [Klicken Sie hier, um eine Richtlinie hinzuzufügen (/en-us/citrix-adc/media/saml-9.png)

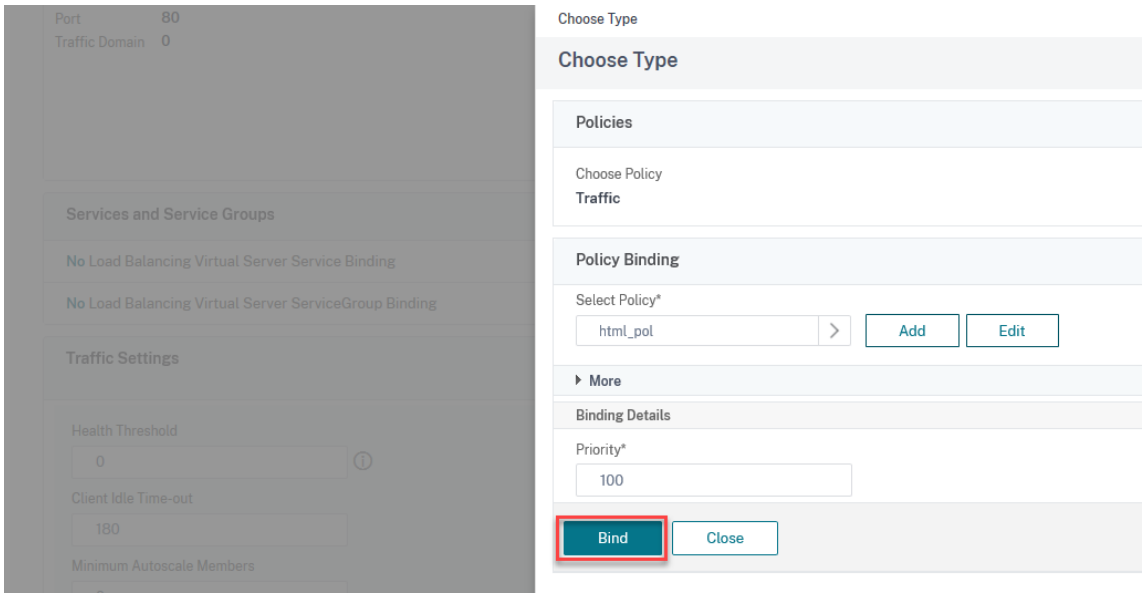
10. Klicken Sie unter **Richtlinie auswählen**, um den erstellten Datenverkehr auszuwählen.



11. Klicken Sie auf **Select**.



12. Klicken Sie auf **Binden**, um die Datenverkehrsrichtlinie an den virtuellen Server zu binden.



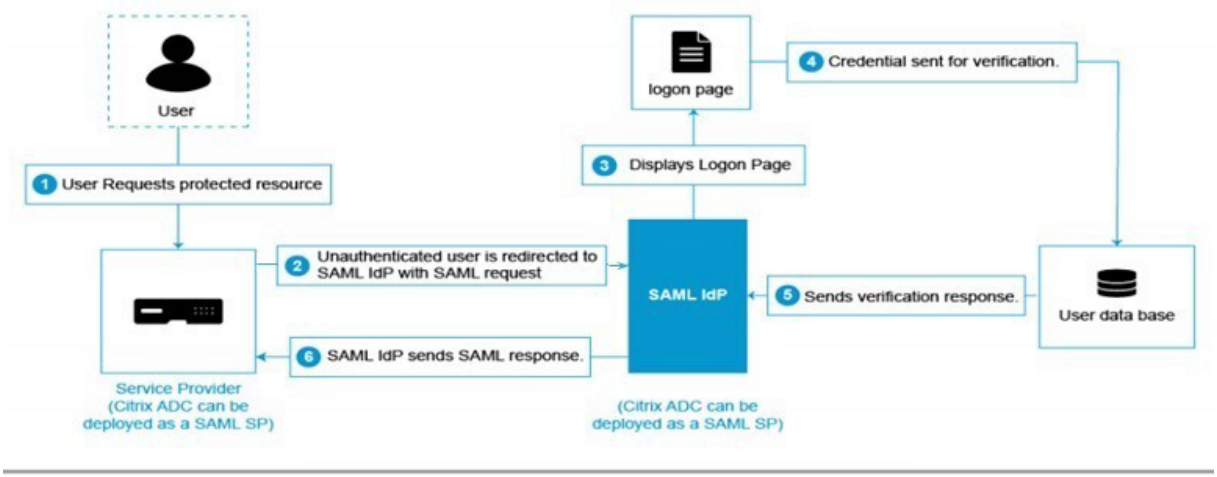
Konfigurieren von Azure AD als SAML IdP und Citrix ADC als SAML SP

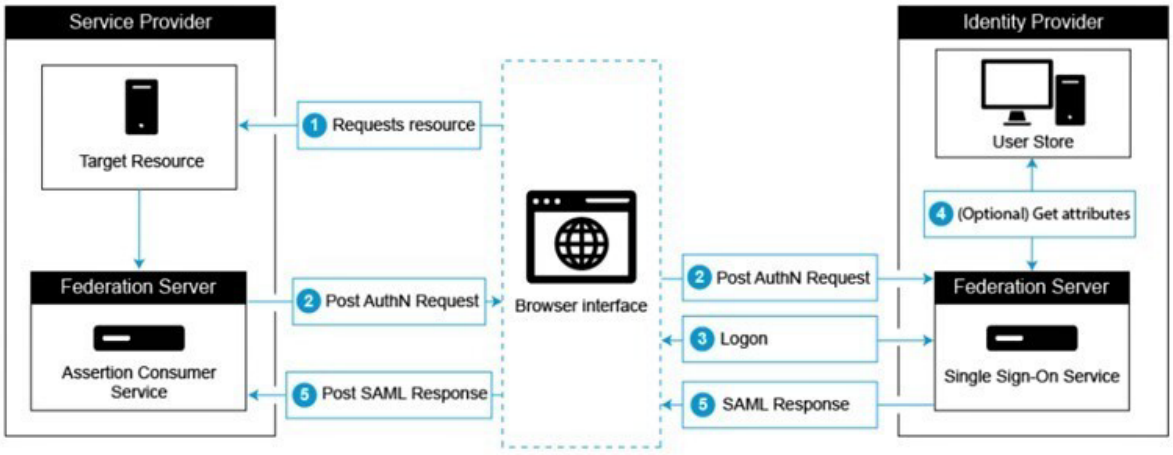
October 4, 2022

Der SAML Service Provider (SP) ist eine SAML-Entität, die vom Dienstanbieter bereitgestellt wird. Wenn ein Benutzer versucht, auf eine geschützte Anwendung zuzugreifen, wertet der SP die Clientanforderung aus. Wenn der Client nicht authentifiziert ist (kein gültiges NSC_TMAA- oder NSC_TMAS-Cookie hat), leitet der SP die Anfrage an den SAML Identity Provider (IdP) weiter. Der SP validiert auch SAML-Assertions, die vom IdP empfangen werden.

Der SAML-IdP (Identity Provider) ist eine SAML-Entität, die im Kundennetzwerk bereitgestellt wird. Der IdP erhält Anfragen vom SAML-SP und leitet Benutzer zu einer Anmeldeseite weiter, auf der sie ihre Anmeldeinformationen eingeben müssen. Der IdP authentifiziert diese Anmeldeinformationen mit dem Benutzerverzeichnis (externer Authentifizierungsserver wie LDAP) und generiert dann eine SAML-Assertion, die an den SP gesendet wird. Der SP überprüft das Token, und dem Benutzer wird dann Zugriff auf die angeforderte geschützte Anwendung gewährt.

Das folgende Diagramm zeigt den SAML-Authentifizierungsmechanismus.

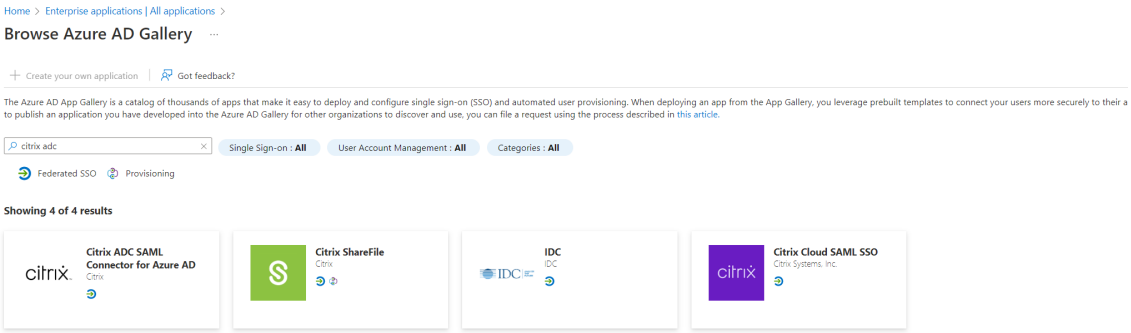




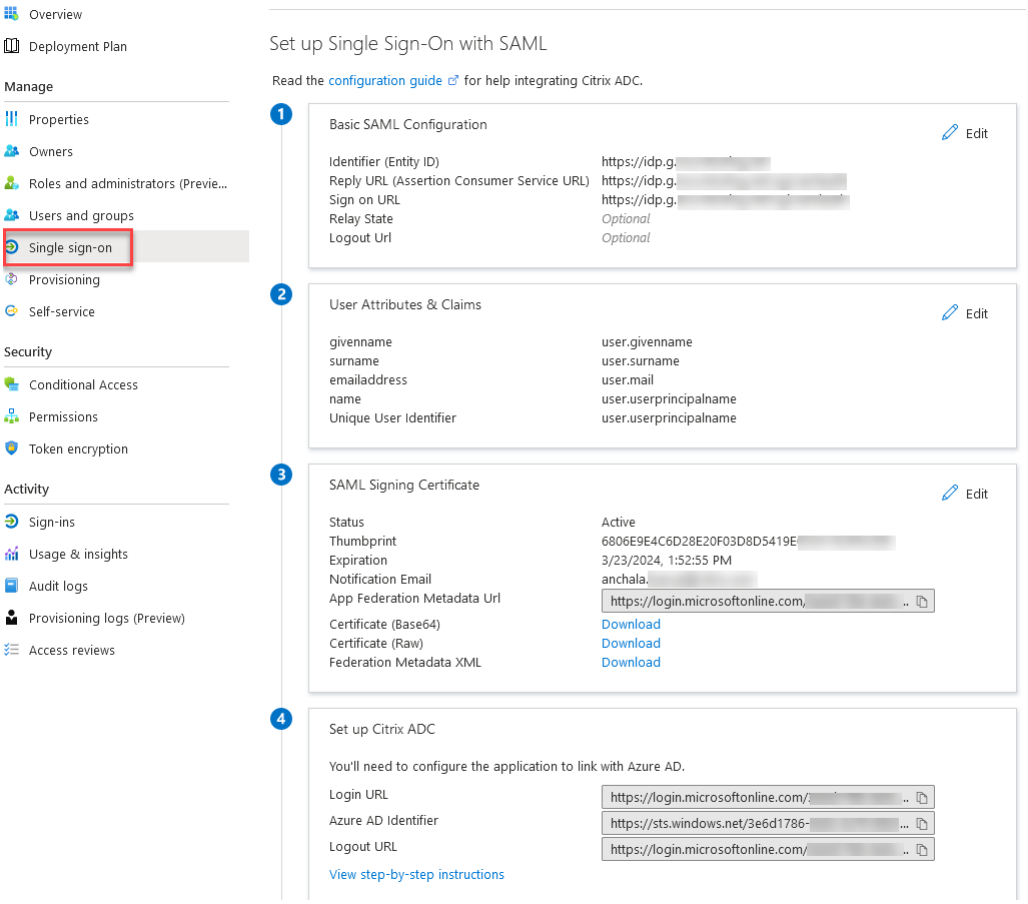
Azure AD-Seitige Konfigurationen

Konfigurieren Sie Single-Sign-On-Einstellungen:

1. Klicken Sie im Azure-Portal auf **Azure Active Directory**.
2. Klicken Sie im Navigationsbereich unter dem Abschnitt **Verwalten** auf **Unternehmensanwendungen**. Ein Zufallsbeispiel der Anwendungen in Ihrem Azure AD-Mandanten wird angezeigt.
3. Geben Sie in der Suchleiste **Citrix ADC SAML Connector for Azure AD** ein.



4. Wählen Sie im Abschnitt **Verwalten** die Option **Single Sign-On** aus.
5. Wählen Sie **SAML** aus, um Single Sign-On zu konfigurieren. Die Seite **Single Sign-On mit SAML einrichten - Vorschau** wird angezeigt. Hier fungiert Azure als SAML-IdP.
6. Laden Sie das Zertifikat (Base64) herunter, das unter dem **SAML-Signaturzertifikat** vorhanden ist, um als samlidPCertName verwendet zu werden, während Citrix ADC als SAML-SP konfiguriert wird.



7. **Konfigurieren Sie grundlegende SAML-Optionen:**

Identifikator (Entity ID) - Für einige Apps erforderlich. Identifiziert eindeutig die Anwendung, für die Single Sign-On konfiguriert wird. Azure AD sendet den Bezeichner als Zielgruppenparameter des SAML-Tokens an die Anwendung. Es wird erwartet, dass die Anwendung sie validiert. Dieser Wert wird auch als Entitäts-ID in allen SAML-Metadaten angezeigt, die von der Anwendung bereitgestellt werden.

Antwort URL - Obligatorisch. Gibt an, wo die Anwendung das SAML-Token erwartet. Die Antwort-URL wird auch als Assertion Consumer Service (ACS) -URL bezeichnet.

Anmelde-URL - Wenn ein Benutzer diese URL öffnet, leitet der Dienstanbieter zu Azure AD um, um sich zu authentifizieren und den Benutzer anzumelden.

Relay-Status - Gibt an die Anwendung an, in die der Benutzer nach Abschluss der Authentifizierung umgeleitet werden soll.

Citrix ADC seitliche Konfigurationen

1. Navigieren Sie zu **Sicherheit>AAA-Richtlinien>Authentifizierung> Grundrichtlinien>SAML**.
2. Wählen Sie die Registerkarte **Server** aus, klicken Sie auf **Hinzufügen**, geben Sie Werte für die folgenden Parameter ein und klicken Sie auf **Erstellen**.

   Parameter-Beschreibung:

   Der Wert für fettgedruckte Parameter muss aus den Azure-Seitenkonfigurationen übernommen werden.

   Name - Name des Servers

   URL umleiten - Geben Sie die zuvor verwendete Anmelde-URL im Abschnitt Azure AD “Setup Citrix ADC” ein. `https://login.microsoftonline.com/3e6d1786-4e0c-4c70-86d2-ae7811f97f79/saml2`

   Einzelne Abmelde-URL - `https://login.microsoftonline.com/3e6d1786-4e0c-4c70-86d2-ae7811f97f79/saml2`

   SAML-Bindung - POST

   Logout Bindung - REDIRECT

   IDP-Zertifikatsname — IdPCert-Zertifikat (Base64) unter SAML-Signaturzertifikat.

   Benutzerfeld - userprincipalName. Aus dem Abschnitt “Benutzerattribute und Ansprüche” von Azure IdP entnommen.

   Signierzertifikatname - Für Azure AD nicht erforderlich. Wählen Sie das SAML SP-Zertifikat (mit privatem Schlüssel) aus, das Citrix ADC verwendet, um Authentifizierungsanforderungen an den IdP zu signieren. Das gleiche Zertifikat (ohne privaten Schlüssel) muss in den IdP importiert

werden, damit der IdP die Signatur der Authentifizierungsanforderung überprüfen kann. Dieses Feld wird von den meisten IDPs nicht benötigt.

IssuerName — Identifier. `https://idp.g.nssvctesting.net`

Unsignierte Assertion ablehnen - EIN

Zielgruppe — Zielgruppe, für die die vom IdP gesendete Assertion gilt. Dies ist normalerweise ein Entitätsname oder eine URL, die den Dienstanbieter repräsentiert.

Signaturalgorithmus - RSA-SHA256

Digest-Methode - SHA256

Standardauthentifizierungsgruppe — Die Standardgruppe, die zusätzlich zu den extrahierten Gruppen ausgewählt wird, wenn die Authentifizierung erfolgreich ist.

Gruppennamenfeld - Name des Tags in Assertion, das Benutzergruppen enthält.

Zeitverzerrung (Minuten) - Diese Option gibt die zulässige Taktverzerrung in Minuten an, die der Citrix ADC ServiceProvider für eine eingehende Assertion zulässt.

Zwei-Faktor - AUS

Angeforderter Authentifizierungskontext - genau

Typ der Authentifizierung - Keine

Fingerabdruck senden - AUS

Benutzernamen erzwingen - EIN

Authentifizierung erzwingen - AUS

SAML Response speichern - AUS

Erstellen Sie auf ähnliche Weise eine entsprechende SAML-Richtlinie und binden Sie sie an den virtuellen Authentifizierungsserver.

Hinweis:

- Azure AD erwartet das Feld Betreff-ID in der SAML-Anforderung nicht.
- Damit Citrix ADC das Feld Betreff-ID nicht sendet, geben Sie den folgenden Befehl in der Citrix ADC CLI ein.
  `nsapimgr_wr.sh -ys call=”ns_saml_dont_send_subject”`
  Dieser Befehl ist nur in nFactor-Authentifizierungs-Workflows anwendbar.

Weitere Funktionen, die für SAML unterstützt werden

March 8, 2022

Die folgenden Funktionen werden für SAML unterstützt.

Metadaten-Lese- und Generierungsunterstützung für SAML SP und IdP Konfiguration

Die Citrix ADC-Appliance unterstützt jetzt Metadatendateien als Konfigurationsentitäten für SAML Service Provider (SP) und Identity Provider (IdP). Die Metadatendatei ist eine strukturierte XML-Datei, die die Konfiguration einer Entität beschreibt. Die Metadatendateien für SP und IdP sind getrennt. Je nach Bereitstellung kann ein SP oder eine IdP-Entität manchmal mehrere Metadatendateien haben.
Als Administrator können Sie Metadatendateien (SAML SP und IdP) in Citrix ADC exportieren und importieren.
Die Funktionen des Metadaten-Exports und -Imports für SAML SP und IdP werden in den folgenden Abschnitten erläutert.

Metadatenexport für SAML SP

Stellen Sie sich ein Beispiel vor, in dem der Citrix ADC als SAML SP konfiguriert ist und ein SAML-IdP Metadaten importieren möchte, die die Citrix ADC SP-Konfiguration enthalten. Angenommen, die Citrix ADC-Appliance ist bereits mit einem “SAMLAction” -Attribut konfiguriert, das die SAML SP-Konfiguration angibt.

Um Metadaten von Benutzern oder Administratoren zu exportieren, fragen Sie das Citrix Gateway oder den virtuellen Authentifizierungsserver wie unten gezeigt ab:

```
1 https://vserver.company.com/metadata/samlsp/<action-name>
```

Metadatenimport für SAML SP

Derzeit verwendet die SAML Action-Konfiguration auf der Citrix ADC-Appliance verschiedene Parameter. Der Administrator gibt diese manuell an. Administratoren sind sich jedoch häufig der Nomenklatur nicht bewusst, wenn es darum geht, mit verschiedenen SAML-Systemen zu interagieren. Wenn Metadaten von IdP verfügbar sind, kann ein Großteil der Konfiguration in der Entität ‘samlAction’ vermieden werden. Tatsächlich könnte die gesamte IdP-spezifische Konfiguration weggelassen werden, wenn die IdP-Metadatendatei angegeben wird. Die ‘samlAction’-Entität benötigt jetzt einen zusätzlichen Parameter, um die Konfiguration aus der Metadatendatei zu lesen.

Wenn Sie Metadaten in eine Citrix ADC-Appliance importieren, enthalten die Metadaten keine zu verwendenden Signaturalgorithmen, sondern die Endpunktdetails. Metadaten können mit bestimmten Algorithmen signiert werden, mit denen die Metadaten selbst überprüft werden können. Die Algorithmen werden nicht in der Entität ‘SAMLAction’ gespeichert.

Daher wird das, was Sie in der Entität 'SAMLAction' angeben, beim Senden der Daten verwendet. Eingehende Daten können einen anderen Algorithmus enthalten, den eine Citrix ADC-Appliance verarbeiten muss.
Sie können eine maximale Größe von 64 K Byte an Metadaten importieren.

Abrufen der Metadatendateien mit der Befehlszeilenschnittstelle.

```
set samlAction <name> [-metadataUrl <url> [-metadataRefreshInterval <
    int>] https://idp.citrix.com/samlidp/metadata.xml
```

> **Hinweis**
>
> Der Parameter metadataRefreshInterval ist das Intervall in Minuten zum Abrufen von Metadateninformationen von der angegebenen Metadaten-URL. Standardwert 36000.

Metadatenimport für SAML-IdP

Der Parameter "samlIdPProfile" benötigt ein neues Argument, um die gesamte Konfiguration zu lesen, die für SP spezifisch ist. Die SAML-IdP-Konfiguration kann vereinfacht werden, indem SP-spezifische Eigenschaften durch eine SP-Metadatendatei ersetzt werden. Diese Datei wird über HTTP abgefragt.

So lesen Sie die Metadatendatei über die Befehlszeilenschnittstelle:

```
set samlIdPProfile <name> [-metadataUrl <url>] [-
    metadataRefreshInterval <int>]
```

Name-Wert-Attribut-Unterstützung für SAML-Authentifizierung

Sie können jetzt SAML-Authentifizierungsattribute mit einem eindeutigen Namen zusammen mit Werten konfigurieren. Die Namen werden im SAML-Aktionsparameter konfiguriert und die Werte werden durch Abfragen der Namen abgerufen. Durch Angabe des Attributwerts für den Namen können Administratoren einfach nach dem Attributwert suchen, der dem Attributnamen zugeordnet ist. Außerdem müssen sich Administratoren das Attribut nicht mehr nur anhand seines Wertes merken.

> **Wichtig**
>
> - Im Befehl SAMLAction können Sie maximal 64 durch Komma getrennte Attribute mit einer Gesamtgröße von weniger als 2048 Byte konfigurieren.
> - Citrix empfiehlt die Verwendung der Attributliste. Die Verwendung von "Attribut 1 zu Attribut 16" führt zu einem Sitzungsfehler, wenn die Größe des extrahierten Attributs groß

> ist.

So konfigurieren Sie die Name-Wert-Attribute mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication samlAction <name> [-Attributes <string>]
```

Beispiel:

```
add authentication samlAction samlAct1 -attributes  “mail,sn,
   userprincipalName”
```

Assertion Consumer Service-URL-Unterstützung für SAML-IdP

Eine Citrix ADC-Appliance, die als SAML Identity Provider (IdP) konfiguriert ist, unterstützt jetzt die Assertion Consumer Service (ACS) -Indizierung, um die SAML Service Provider (SP) -Anforderung Der SAML-IdP importiert die ACS-Indizierungskonfiguration aus SP-Metadaten oder ermöglicht die manuelle Eingabe von ACS-Indexinformationen.
In der folgenden Tabelle sind einige Artikel aufgeführt, die sich speziell auf Bereitstellungen beziehen, bei denen die Citrix ADC-Appliance als SAML-SP oder SAML-IdP verwendet wird.

In der folgenden Tabelle sind einige Artikel aufgeführt, die sich speziell auf Bereitstellungen beziehen, bei denen die Citrix ADC-Appliance als SAML-SP oder SAML-IdP verwendet wird.

SAML SP	SAML-Identitätsanbieter	Link “Informationen”
Citrix ADC	Microsoft Azure AD	Citrix Support
Okta	Citrix ADC	Citrix Support
AWS	Citrix ADC	Citrix Support

Einige Informationen zu anderen spezifischen Bereitstellungen:

- NetScaler als SAML SP auf FIPS-Gerät
- Konfigurieren von Office365 für Single Sign-On mit NetScaler als SAML-IdP

Unterstützung von WebView-Anmeldeinformationen für Authentifizierungsmechanismen

Die Authentifizierung einer Citrix ADC-Appliance kann jetzt das AuthV3-Protokoll unterstützen. Der WebView-Anmeldeinformationstyp im AuthV3-Protokoll unterstützt alle Arten von Authentifizierungsmechanismen (einschließlich SAML und OAuth). Der WebView-Anmeldeinformationstyp ist Teil von AuthV3, das von Citrix Receiver und Browser in Webanwendungen implementiert wird.

Im folgenden Beispiel wird der Ablauf von WebView-Ereignissen durch Citrix Gateway und Citrix Receiver erläutert:

1. Der Citrix Receiver verhandelt mit Citrix Gateway für die Unterstützung des AuthV3-Protokolls.
2. Die Citrix ADC-Appliance reagiert positiv und schlägt eine bestimmte Start-URL vor.
3. Citrix Receiver stellt dann eine Verbindung zum spezifischen Endpunkt (URL) her.
4. Das Citrix Gateway sendet eine Antwort an den Client, um das WebView zu starten.
5. Citrix Receiver startet WebView und sendet eine erste Anfrage an die Citrix ADC-Appliance.
6. Citrix ADC-Appliance leitet den URI zum Anmeldeendpunkt des Browsers
7. Sobald die Authentifizierung abgeschlossen ist, sendet die Citrix ADC-Appliance eine Antwort auf den Abschluss an WebView.
8. Das WebView wird jetzt beendet und gibt die Steuerung an Citrix Receiver zurück, um das AuthV3-Protokoll für den Sitzungsaufbau fortzusetzen.

Erhöhung der SessionIndex-Größe in SAML SP

Die SessionIndex-Größe des SAML Service Providers (SP) wurde auf 96 Byte erhöht. Zuvor betrug die standardmäßige maximale Größe von SessionIndex 63 Byte.

> **Hinweis**
>
> Unterstützung in NetScaler 13.0 Build 36.x eingeführt

Unterstützung für benutzerdefinierte Authentifizierungsklassenreferenzen für SAML SP

Sie können ein benutzerdefiniertes Referenzattribut für die Authentifizierungsklasse im **SAML-Aktionsbefehl** konfigurieren. Mit dem benutzerdefinierten Klassenreferenzattribut für die Authentifizierung können Sie die Klassennamen in den entsprechenden SAML-Tags anpassen. Das benutzerdefinierte Authentifizierungsklassenreferenzattribut zusammen mit dem Namespace wird als Teil der SAML SP-Authentifizierungsanforderung an den SAML-IdP gesendet.

Zuvor konnten Sie mit dem SAML-Aktionsbefehl nur einen Satz vordefinierter Klassen konfigurieren, die im authnCtxClassRef-Attribut definiert sind.

> **Wichtig**
>
> Stellen Sie beim Konfigurieren des Attributs customAuthnCtxClassRef Folgendes sicher:

- Die Namen der Klassen müssen alphanumerische Zeichen oder eine gültige URL mit den richtigen XML-Tags enthalten.
- Wenn Sie mehrere benutzerdefinierte Klassen konfigurieren müssen, muss jede Klasse durch Kommas getrennt werden

So konfigurieren Sie die customAuthnctxClassRef-Attribute über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

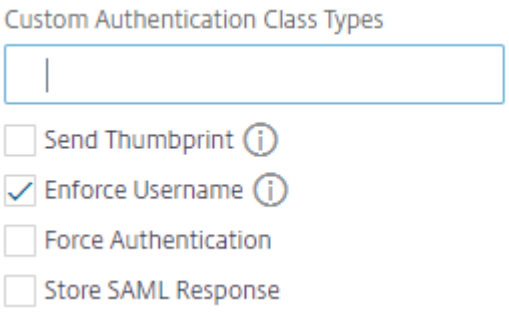
- Authentifizierung hinzufügen samlAction <name> [-customAuthnctxClassRef <string>]
- setze Authentifizierung samlAction <name> [-customAuthnctxClassRef <string>]

Beispiel:

- `add authentication samlAction samlact1 -customAuthnCtxClassRef http://www.class1.com/LoA1,http://www.class2.com/LoA2`
- `set authentication samlAction samlact2 -customAuthnCtxClassRef http://www.class3.com/LoA1,http://www.class4.com/LoA2`

So konfigurieren Sie die customAuthnctxClassRef-Attribute mit der GUI

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Aktionen > SAML**.
2. Wählen Sie auf der SAML-Seite die Registerkarte **Server** aus und klicken Sie auf **Hinzufügen**.
3. Geben Sie auf der Seite **Create Authentication SAML Server** den Namen für die SAML-Aktion ein.
4. Scrollen Sie nach unten, um die Klassentypen im Abschnitt **Benutzerdefinierte Authentifizierungsklassen** zu konfigurieren.



Unterstützung für Artefakt-Bindung in SAML IdP

Die als SAML Identity Provider (IdP) konfigurierte Citrix ADC-Appliance unterstützt die Artefaktbindung. Die Artefaktbindung erhöht die Sicherheit von SAML IdP und hindert die böswilligen Benutzer daran, die Assertion zu überprüfen.

Assertion Consumer Service-URL-Unterstützung für SAML-IdP

Eine Citrix ADC-Appliance, die als SAML Identity Provider (IdP) konfiguriert ist, unterstützt jetzt die Assertion Consumer Service (ACS) -Indizierung, um die SAML Service Provider (SP) -Anforderung Der SAML-IdP importiert die ACS-Indizierungskonfiguration aus SP-Metadaten oder ermöglicht die manuelle Eingabe von ACS-Indexinformationen.

FIPS-Offload-Unterstützung

Eine Citrix ADC MPX FIPS-Appliance, die als SAML-Dienstanbieter verwendet wird, unterstützt jetzt verschlüsselte Zusicherungen. Außerdem kann eine Citrix ADC MPX FIPS-Appliance, die als SAML-Dienstanbieter oder SAML-Identitätsanbieter fungiert, jetzt für die Verwendung der SHA2-Algorithmen auf FIPS-Hardware konfiguriert werden.

> **Hinweis**
>
> Im FIPS-Modus wird nur der RSA-V1_5-Algorithmus als Schlüsseltransportalgorithmus unterstützt.

Konfigurieren der FIPS-Offload-Unterstützung mithilfe der Befehlszeilenschnittstelle:

1. SSL FIPS hinzufügen

   add ssl fipsKey fips-key

2. Erstellen Sie eine CSR und verwenden Sie sie auf dem CA-Server, um ein Zertifikat zu generieren. Sie können das Zertifikat dann in **/nsconfig/ssl**kopieren. Nehmen wir an, die Datei ist *fips3cert.cer*.

   ```
   add ssl certKey fips-cert -cert fips3cert.cer -fipsKey fips-key<!--
   NeedCopy-->
   ```

3. Geben Sie dieses Zertifikat in der SAML-Aktion für das SAML-SP-Modul an

   ```
   set samlAction <name> -samlSigningCertName fips-cert<!--NeedCopy-->
   ```

4. Verwenden Sie das Zertifikat in samlIdpProfile für das SAML-IdP-Modul

   ```
   set samlidpprofile fipstest -samlIdpCertName fips-cert<!--NeedCopy-->
   ```


Gängige SAML-Terminologien

Im Folgenden sind einige gebräuchliche SAML-Terminologien aufgeführt:

- **Assertion:** Eine SAML-Assertion ist ein XML-Dokument, das vom Identitätsanbieter nach der Authentifizierung des Benutzers an den Service Provider zurückgegeben wird. Die Assertion hat eine spezifische Struktur, wie im SAML-Standard definiert.
- **Arten von Assertions:** Im Folgenden sind die Arten von Assertion.
  - Authentifizierung - der Benutzer wird zu einem bestimmten Zeitpunkt mit einem bestimmten Mittel authentifiziert
  - Autorisierung - dem Benutzer wurde der Zugriff auf eine angegebene Ressource gewährt oder verweigert
  - Attribute - der Benutzer ist mit den angegebenen Attributen verknüpft
- **Assertion Consumer Service (ACS):** Der Endpunkt (URL) des Dienstanbieters, der für den Empfang und das Parsen einer SAML-Assertion verantwortlich ist
- **Zielgruppenbeschränkung:** Ein Wert innerhalb der SAML-Zusicherung, der angibt, für wen (und nur für wen) die Assertion bestimmt ist. Das "Publikum" ist der Dienstanbieter und ist normalerweise eine URL, kann aber technisch als eine beliebige Datenfolge formatiert werden.
- **Identitätsanbieter (IdP):** In Bezug auf SAML ist der Identitätsanbieter die Entität, die die Identität des Benutzers als Antwort auf eine Anfrage des Dienstanbieters überprüft.

  Der Identitätsanbieter ist für die Pflege und Authentifizierung der Benutzeridentität verantwortlich.
- **Service Provider (SP):** In Bezug auf SAML bietet der Service Provider (SP) dem Benutzer einen Dienst an und ermöglicht es dem Benutzer, sich mithilfe von SAML anzumelden. Wenn der Benutzer versucht, sich anzumelden, sendet der SP eine SAML-Authentifizierungsanforderung an den Identitätsanbieter (IdP)
- **SAML-Bindung:** SAML-Anforderer und Responder kommunizieren durch den Austausch von Nachrichten. Der Mechanismus zum Transportieren dieser Nachrichten wird als SAML-Bindung bezeichnet.
- **HTTP-Artefakt:** Eine der vom SAML-Protokoll unterstützten Bindungsoptionen. HTTP-Artefakt ist nützlich in Szenarien, in denen der SAML-Requester und der Responder einen HTTP-User-Agent verwenden und nicht die gesamte Nachricht übertragen möchten, weder aus technischen noch aus Sicherheitsgründen. Stattdessen wird ein SAML-Artefakt gesendet, bei dem es sich um eine eindeutige ID für die vollständigen Informationen handelt. Der IdP kann dann das Artefakt verwenden, um die vollständigen Informationen abzurufen. Der Artefakt-Aussteller muss den Status beibehalten, solange das Artefakt noch aussteht. Ein Artifact Resolution Service (ARS) muss eingerichtet werden.

Das HTTP-Artefakt sendet das Artefakt als Abfrageparameter.

- **HTTP POST:** Eine der vom SAML-Protokoll unterstützten Bindungsoptionen.

  HTTP POST sendet den Nachrichteninhalt als POST-Parameter in der Nutzlast.

- **HTTP-Umleitung:** Eine der vom SAML-Protokoll unterstützten Bindungsoptionen.

  Wenn die HTTP-Umleitung verwendet wird, leitet der Dienstanbieter den Benutzer zum Identitätsanbieter weiter, wo die Anmeldung erfolgt, und der Identitätsanbieter leitet den Benutzer zurück zum Dienstanbieter. Die HTTP-Umleitung erfordert ein Eingreifen des Benutzeragenten (des Browsers).

  Die HTTP-Umleitung sendet den Nachrichteninhalt in der URL. Aus diesem Grund kann es nicht für die SAML-Antwort verwendet werden, da die Größe der Antwort normalerweise die von den meisten Browsern zulässige URL-Länge überschreitet.

  Hinweis: Die Citrix ADC-Appliance unterstützt POST- und Redirect-Bindungen während der Abmeldung.

- Metadaten: Metadaten sind die Konfigurationsdaten in SP und IdP, um zu wissen, wie man miteinander kommuniziert, was in XML-Standards enthalten sein wird

Weitere nützliche Citrix Artikel zur SAML-Authentifizierung

Möglicherweise finden Sie die folgenden Artikel zur SAML-Authentifizierung hilfreich.

- https://support.citrix.com/article/CTX277558
- https://support.citrix.com/article/CTX259127
- https://support.citrix.com/article/CTX228135
- https://support.citrix.com/article/CTX221631
- https://support.citrix.com/article/CTX138988

OAuth-Authentifizierung

October 5, 2021

Die Funktion für Authentifizierung, Autorisierung und Überwachung des Datenverkehrsmanagements unterstützt die OAuth und OpenID Connect (OIDC) -Authentifizierung. Es autorisiert und authentifiziert Benutzer für Dienste, die in Anwendungen wie Google, Facebook und Twitter gehostet werden.

Punkte zu beachten

- Citrix ADC Advanced Edition und höher ist erforderlich, damit die Lösung funktioniert.
- Eine Citrix ADC Appliance muss Version 12.1 oder höher sein, damit die Appliance mit OIDC als OAuth IdP funktioniert.
- OAuth auf einer Citrix ADC Appliance ist für alle SAML-IDPs qualifiziert, die mit "OpenID connect 2.0" kompatibel sind.

Eine Citrix ADC Appliance kann so konfiguriert werden, dass sie sich mit SAML und OIDC als Service Provider (SP) oder Identity Provider (IdP) verhält. Zuvor unterstützte eine Citrix ADC Appliance, die als IdP konfiguriert war, nur das SAML-Protokoll. Ab der Citrix ADC 12.1-Version unterstützt Citrix ADC auch den OIDC.

OIDC ist eine Erweiterung der OAuth-Autorisierung/Delegierung. Eine Citrix ADC Appliance unterstützt OAuth- und OIDC-Protokolle in derselben Klasse anderer Authentifizierungsmechanismen. OIDC ist ein Add-on für OAuth, da es eine Möglichkeit bietet, Benutzerinformationen vom Autorisierungsserver abzurrufen, im Gegensatz zu OAuth, das nur ein Token erhält, das nicht für Benutzerinformationen abgerufen werden kann.

Der Authentifizierungsmechanismus erleichtert die Inline-Überprüfung von OpenID-Token. Eine Citrix ADC Appliance kann so konfiguriert werden, dass Zertifikate abgerufen und Signaturen auf dem Token überprüft werden.

Ein wesentlicher Vorteil der Verwendung der OAuth- und OIDC-Mechanismen besteht darin, dass die Benutzerinformationen nicht an die gehosteten Anwendungen gesendet werden. Daher wird das Risiko eines Identitätsdiebstahls erheblich reduziert.

Die für die Authentifizierung, Autorisierung und Überwachung konfigurierte Citrix ADC Appliance akzeptiert jetzt eingehende Token, die mit dem HMAC HS256-Algorithmus signiert wurden. Darüber hinaus werden die öffentlichen Schlüssel des SAML-Identitätsanbieters (IdP) aus einer Datei gelesen, anstatt von einem URL-Endpunkt zu lernen.

In der Citrix ADC Implementierung wird auf die Anwendung durch den virtuellen Server für die Authentifizierung, Autorisierung und Überwachung der Datenverkehrsverwaltung zugegriffen. Um OAuth zu konfigurieren, müssen Sie also eine OAuth-Richtlinie konfigurieren, die dann einem virtuellen Server zur Authentifizierung, Autorisierung und Überwachung der Verkehrsverwaltung zugeordnet werden muss.

Konfigurieren Sie das OpenID Connect-Protokoll

Eine Citrix ADC Appliance kann jetzt mithilfe des OIDC-Protokolls als Identitätsanbieter konfiguriert werden. Das OIDC-Protokoll stärkt die Identitätsbereitstellungsfunktionen der Citrix ADC Appliance. Sie können jetzt mit einem Single Sign-On auf die unternehmensweite gehostete Anwendung zugreifen. Der OIDC bietet mehr Sicherheit, indem es kein Benutzerkennwort überträgt, sondern

mit Token mit einer bestimmten Lebensdauer arbeitet. OIDC ist auch für die Integration in Nicht-Browser-Clients wie Apps und Dienste konzipiert. Daher nehmen viele Implementierungen OIDC weit an.

Vorteile der OpenID Connect Unterstützung

- OIDC eliminiert den Aufwand für die Verwaltung mehrerer Authentifizierungskennwörter, da der Benutzer eine einzige Identität im gesamten Unternehmen hat.
- OIDC bietet eine robuste Sicherheit für Ihr Kennwort, da das Kennwort nur mit Ihrem Identitätsanbieter und nicht mit einer Anwendung, auf die Sie zugreifen, geteilt wird.
- OIDC verfügt über eine große Interoperabilität mit verschiedenen Systemen, die es den gehosteten Anwendungen erleichtert, OpenID zu akzeptieren.
- OIDC ist ein einfaches Protokoll, das es nativen Clients ermöglicht, sich einfach in Server zu integrieren.

So konfigurieren Sie eine Citrix ADC Appliance mit dem OpenID Connect-Protokoll über die GUI als IdP

1. Navigieren Sie zu **Konfiguration > Sicherheit > AAA-Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > OAuth-IdP**.
2. Klicken Sie auf **Profil**, und klicken Sie auf **Hinzufügen.**

   Legen Sie im Bildschirm Authentifizierungs-OAuth-IDP-Profil erstellen Werte für die folgenden Parameter fest, und klicken Sie auf **Erstellen** .

   - **Name** — Name des Authentifizierungsprofils.
   - **Client-ID** — Eindeutige Zeichenfolge, die SP identifiziert.
   - **Client Secret** — Eindeutiges Geheimnis, das SP identifiziert.
   - **Umleitungs-URL** — Endpunkt auf SP, auf den Code/Token gepostet werden muss.
   - **Name des Ausstellers** — Zeichenfolge, die den IdP identifiziert.
   - **Zielgruppe** — Zielempfänger für das Token, das vom IdP gesendet wird. Dies kann vom Empfänger überprüft werden.
   - **Skew Time** — Die Zeit, für die das Token gültig bleibt.
   - **Standardauthentifizierungsgruppe** — Eine Gruppe, die der Sitzung für dieses Profil hinzugefügt wurde, um die Richtlinienbewertung zu vereinfachen und beim Anpassen von Richtlinien zu helfen.
3. Klicken Sie auf **Richtlinien**, und klicken Sie auf **Hinzufügen.**
4. **Legen Sie im Bildschirm Authentifizierungs-OAuth-IDP-Richtlinie erstellen** Werte für die folgenden Parameter fest, und klicken Sie auf **Erstellen** .

   - **Name —** Der Name der Authentifizierungsrichtlinie.

- **Aktion** — Name des zuvor erstellten Profils.
- **Log-Aktion** : Name der Nachrichtenprotokollaktion, die verwendet wird, wenn eine Anforderung mit dieser Richtlinie übereinstimmt. Kein Pflichtfeld eingereicht.
- Aktion **Undefiniertes Ergebnis** — Aktion, die ausgeführt wird, wenn das Ergebnis der Policy-Evaluierung unbestraft ist (UNDEF). Kein Pflichtfeld.
- **Ausdruck** — Standardsyntaxausdruck, den die Richtlinie verwendet, um auf eine bestimmte Anforderung zu antworten. Zum Beispiel ist es wahr.
- **Kommentare** — Alle Kommentare zu der Richtlinie.

Binden der OAuthIDP-Richtlinie und der LDAP-Richtlinie an den virtuellen Authentifizierungsserver

1. Navigieren Sie zu **Konfiguration > Sicherheit > AAA-Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Aktionen > LDAP**.
2. Klicken Sie auf dem Bildschirm **LDAP-Aktionen** auf **Hinzufügen** .
3. **Legen Sie im Bildschirm Authentifizierungs-LDAP-Server erstellen** die Werte für die folgenden Parameter fest, und klicken Sie auf **Erstellen** .
   - **Name —** Der Name der LDAP-Aktion
   - **Servername/ServerIP —** Bereitstellen von FQDN oder IP des LDAP-Servers
   - Wählen Sie geeignete Werte **für Sicherheitstyp, Port, Servertyp, Timeout**
   - Stellen Sie sicher, dass die **Authentifizierung** aktiviert ist
   - **Basis-DN —** Basis, von der aus die LDAP-Suche gestartet werden soll. Beispiel: dc=aaa, dc=local.
   - **Administrator Bind DN:** Benutzername der Bindung an LDAP-Server. Zum Beispiel admin@aaa.local.
   - **Administratorkennwort/Kennwort bestätigen: Kennwort zum Binden von LDAP**
   - Klicken Sie auf **Verbindung testen**, um Ihre Einstellungen zu testen.
   - **Serveranmeldename Attribut:** Wählen Sie **sAMAccountName**
   - Andere Felder sind nicht obligatorisch und können daher nach Bedarf konfiguriert werden.
4. Navigieren Sie zu **Konfiguration > Sicherheit > AAA-Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinie.**
5. Klicken Sie auf dem Bildschirm **Authentifizierungsrichtlinien** auf **Hinzufügen** .
6. **Legen Sie auf der Seite Authentifizierungsrichtlinie erstellen** die Werte für die folgenden Parameter fest, und klicken Sie auf **Erstellen.**
   - **Name —** Name der LDAP-Authentifizierungsrichtlinie.
   - **Aktionstyp —** Wählen Sie **LDAP.**
   - **Aktion —** Wählen Sie die LDAP-Aktion aus.

- **Ausdruck —** Standardsyntaxausdruck, den die Richtlinie verwendet, um auf eine bestimmte Anfrage zu antworten. Zum Beispiel ist es wahr**.

So konfigurieren Sie die Citrix ADC Appliance mithilfe des OpenID Connect-Protokolls mit CLI als IdP

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add authentication OAuthIDPProfile <name> [-clientID <string>][-clientSecret ][-redirectURL <URL>][-issuer <string>][-audience <string>][-skewTime <mins>] [-defaultAuthenticationGroup <string>]<!--NeedCopy-->`
- `add authentication OAuthIdPPolicy <name> -rule <expression> [-action < string> [-undefAction <string>] [-comment <string>][-logAction <string >]<!--NeedCopy-->`
- `add authentication ldapAction aaa-ldap-act -serverIP 10.0.0.10 -ldapBase "dc=aaa,dc=local"<!--NeedCopy-->`
- `ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password> - ldapLoginName sAMAccountName<!--NeedCopy-->`
- `add authentication policy aaa-ldap-adv-pol -rule true -action aaa-ldap-act<!--NeedCopy-->`
- `bind authentication vserver auth_vs -policy <ldap_policy_name> -priority 100 -gotoPriorityExpression NEXT<!--NeedCopy-->`
- `bind authentication vserver auth_vs -policy <OAuthIDPPolicyName> - priority 5 -gotoPriorityExpression END<!--NeedCopy-->`
- `bind vpn global -certkey <><!--NeedCopy-->`

> **Hinweis:**
>
> Sie können mehrere Schlüssel binden. Öffentliche Teile von Zertifikaten, die gebunden sind, werden als Antwort auf gesendet `jwks\\_uri query (https://gw/oauth/idp/certs)`.

Citrix ADC als OAuth SP

April 25, 2022

Die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion zur Verkehrsverwaltung unterstützt die OAuth-Authentifizierung zur Authentifizierung von Benutzern gegenüber Anwendungen, die auf Anwendungen wie Google, Facebook und Twitter gehostet werden.

Wichtige Hinweise

- Citrix ADC Advanced Edition und höher ist erforderlich, damit die Lösung funktioniert.
- OAuth auf der Citrix ADC Appliance ist für alle SAML-IdPs qualifiziert, die mit “OpenID Connect 2.0” kompatibel sind.

> **Wichtig:**
>
> Die Citrix ADC Appliance reagiert möglicherweise mit einem CSRF-Fehler, wenn eine inhaltsreiche Website nach Ablauf der Sitzung mehrere Authentifizierungsanforderungen sendet. Als Problemumgehung wird empfohlen, dass Sie bei der Konfiguration der OAuth-Richtlinie sicherstellen, dass die Richtlinie sowohl für den Hostnamen als auch für den Pfad konfiguriert ist, die die Haupteintrittspunkte sind.

Konfigurieren von OAuth über die GUI

1. Konfigurieren Sie die OAuth -Aktion und -Richtlinie.

   Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinie**, erstellen Sie eine Richtlinie mit OAuth als Aktionstyp, und verknüpfen Sie die erforderliche OAuth-Aktion mit der Richtlinie.

2. Ordnen Sie die OAuth-Richtlinie einem virtuellen Authentifizierungsserver zu.

   Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Virtuelle Server**, und ordnen Sie die OAuth-Richtlinie dem virtuellen Authentifizierungsserver zu.

> **Hinweis:**
>
> Attribute (1 bis 16) können in der OAuth-Antwort extrahiert werden. Derzeit werden diese Attribute nicht ausgewertet. Sie werden zur zukünftigen Bezugnahme hinzugefügt.

Konfigurieren von OAuth über die CLI

1. Definieren Sie eine OAuth-Aktion.

```
1 add authentication OAuthAction <name> -authorizationEndpoint <URL>
      -tokenEndpoint <URL> [-idtokenDecryptEndpoint <URL>] -clientID
      <string> -clientSecret <string> [-defaultAuthenticationGroup <
     string>][-tenantID <string>][-GraphEndpoint <string>][-
     refreshInterval <positive_integer>] [-CertEndpoint <string>][-
     audience <string>][-userNameField <string>][-skewTime <mins>][-
     issuer <string>][-Attribute1 <string>][-Attribute2 <string>][-
     Attribute3 <string>]
2 <!--NeedCopy-->
```


2. Ordnen Sie die Aktion einer erweiterten Authentifizierungsrichtlinie zu.

```
add authentication Policy <name> -rule <expression> -action <
    string>
<!--NeedCopy-->
```

Beispiel:

```
add authentication oauthAction a -authorizationEndpoint https://
    example.com/ -tokenEndpoint https://example.com/ -clientiD sadf
     -clientsecret df
<!--NeedCopy-->
```

Weitere Informationen zur Authentifizierung von OAuthAction-Parametern finden Sie unter Authentifizierung OAuthAction.

> **Hinweis:**
>
> Wenn ein CertEndPoint angegeben wird, fragt die Citrix ADC Appliance diesen Endpunkt mit der konfigurierten Frequenz ab, um die Schlüssel zu lernen.

Um einen Citrix ADC so zu konfigurieren, dass er die lokale Datei liest und Schlüssel aus dieser Datei analysiert, wird eine neue Konfigurationsoption wie folgt eingeführt:

```
set authentication OAuthAction <> -CertFilePath <path to local file
    with jwks>
<!--NeedCopy-->
```

Die OAuth-Funktion unterstützt jetzt die folgenden Funktionen in der Token-API von Relying Party (RP) und von der IdP-Seite von Citrix Gateway und Citrix ADC.

- Unterstützung von PKCE (Proof Key for Code Exchange)
- Unterstützung für client_assertion

Unterstützung von Name-Wert-Attributen für OAuth-Authentifizierung

Sie können jetzt OAuth-Authentifizierungsattribute mit einem eindeutigen Namen zusammen mit den Werten konfigurieren. Die Namen werden im Aktionsparameter von OAuth entweder als “Attribute” konfiguriert und die Werte werden durch Abfragen der Namen abgerufen. Die extrahierten Attribute

werden in der Authentifizierungs-, Autorisierungs- und Überwachungssitzung gespeichert. Administratoren können diese Attribute entweder mit `http.req.user.attribute("attribute name")` oder `http.req.user.attribute(1)` abfragen, basierend auf der ausgewählten Methode zur Angabe von Attributnamen.

Durch Angabe des Attributnamens können Administratoren einfach nach dem Attributwert suchen, der mit diesem Attributnamen verknüpft ist. Außerdem müssen sich Administratoren das "attribute1 to attribute16" nicht mehr allein anhand seiner Nummer merken.

> **Wichtig**
>
> In einem OAuth-Befehl können Sie maximal 64 durch Komma getrennte Attribute mit einer Gesamtgröße von weniger als 1024 Byte konfigurieren.
>
> **Hinweis**
>
> Der Sitzungsfehler kann vermieden werden, wenn die Gesamtwertgröße von "Attribut 1 bis Attribut 16" und die Werte der in "Attribute" angegebenen Attribute nicht mehr als 10 KB betragen.

So konfigurieren Sie die Name-Wert-Attribute mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication OAuthAction <name> [-Attributes <string>]

set authentication OAuthAction <name> [-Attributes <string>]
<!--NeedCopy-->
```

Beispiele:

```
add authentication OAuthAction a1  - attributes "email,company"  -
    attribute1 email

set authentication OAuthAction oAuthAct1 -attributes "mail,sn,
    userprincipalName"
<!--NeedCopy-->
```

Citrix ADC als OAuth IdP

July 8, 2022

Eine Citrix ADC-Appliance kann jetzt mithilfe des OpenID-Connect (OIDC) -Protokolls als Identitätsanbieter konfiguriert werden. Das OIDC-Protokoll stärkt die Funktionen zur Identitätsbereitstellung der Citrix ADC-Appliance. Sie können jetzt mit einem Single Sign-On auf die unternehmensweit gehostete Anwendung zugreifen, da OIDC mehr Sicherheit bietet, indem das Benutzerkennwort nicht übertragen wird, sondern Token mit einer bestimmten Lebensdauer verwendet werden. OpenID wurde auch für die Integration mit Nicht-Browser-Clients wie Apps und Diensten entwickelt. Daher wird das OIDC-Protokoll von vielen Implementierungen weitgehend übernommen.

> **Hinweis**
>
> Citrix ADC muss auf Version 12.1 oder höher sein, damit die Appliance unter Verwendung des OIDC-Protokolls als OAuth-IdP funktioniert.

Vorteile der Verwendung von Citrix ADC als OAuth IdP

- Eliminiert den Aufwand für die Pflege mehrerer Authentifizierungskennwörter, da der Benutzer über eine einzige Identität in einer Organisation verfügt.
- Bietet eine robuste Sicherheit für Ihr Kennwort, da das Kennwort nur mit Ihrem Identitätsanbieter und nicht mit einer Anwendung, auf die Sie zugreifen, freigegeben wird.
- Vorausgesetzt, enorme Interoperabilität mit verschiedenen Systemen, die es den gehosteten Anwendungen erleichtern, OpenID zu akzeptieren.

> **Hinweis**
>
> Citrix ADC Advanced Edition und höher ist erforderlich, damit die Lösung funktioniert.

So konfigurieren Sie die Citrix ADC-Appliance mit der GUI als OAuth IdP

1. Navigieren Sie zu **Konfiguration > Sicherheit > AAA-Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > OAuth IdP**.
2. Klicken Sie auf **Profil** und dann auf **Hinzufügen.**

   Legen Sie im Bildschirm **Authentifizierung erstellen OAuth IDP-Profil** Werte für die folgenden Parameter fest und klicken Sie auf **Erstellen**.

   - **Name** — Name des Authentifizierungsprofils. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und darf nur Buchstaben, Zahlen und den Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), Leerzeichen (), bei (@), gleich (=), Doppelpunkt (:) und Unterstriche enthalten. Kann nicht geändert werden, nachdem das Profil erstellt wurde.
   - **Client-ID** — Eindeutige Zeichenfolge, die SP identifiziert. Der Autorisierungsserver leitet die Clientkonfiguration von dieser ID ab. Maximale Länge: 127.
   - **Client Secret:** Geheime Zeichenfolge, die vom Benutzer und Autorisierungsserver erstellt wird. Maximale Länge: 239

- **URL umleiten** — Endpunkt für SP, an dem Code/Token gepostet werden muss.
- **Name des Ausstellers** — Identität des Servers, dessen Token akzeptiert werden sollen. Maximale Länge: 127
- **Zielgruppe** — Zielempfänger für das Token, das vom IdP gesendet wird. Dies könnte vom Empfänger überprüft werden.
- **Skew Time** — Diese Option gibt die zulässige Taktverzerrung in der Anzahl von Minuten an, die Citrix ADC für ein eingehendes Token zulässt. Wenn skewTime beispielsweise 10 ist, wäre das Token von (aktuelle Zeit - 10) min bis (aktuelle Zeit + 10) min gültig, das sind insgesamt 20 Minuten. Standardwert: 5.
- **Standard-Authentifizierungsgruppe** — Eine Gruppe, die der internen Gruppenliste der Sitzung hinzugefügt wurde, wenn dieses Profil von IdP ausgewählt wird, das im nFactor Flow verwendet werden kann. Es kann im Ausdruck (AAA.USER.IS_MEMBER_OF (“xxx”)) für Authentifizierungsrichtlinien verwendet werden
  Identifizieren Sie den nFactor-Flow der vertrauenden Partei. Maximale Länge: 63

A group added to the session for this profile to simplify policy evaluation and help in customizing policies. This is the default group that is chosen when the authentication succeeds in addition to the extracted groups. Maximum Length: 63.

3. Klicken Sie auf **Richtlinien**, und klicken Sie auf **Hinzufügen.**
4. Legen Sie im Fenster **Richtlinie für OAuth IDP-Authentifizierung erstellen** Werte für die folgenden Parameter fest und klicken Sie auf **Erstellen**.
   - **Name** — Der Name der Authentifizierungsrichtlinie.
   - **Action:** Name des zuvor erstellten Profils.
   - **Log Action:** Name der Nachrichtenprotokollaktion, die verwendet werden soll, wenn eine Anforderung mit dieser Richtlinie übereinstimmt. Keine obligatorische Einreichung.
   - Aktion mit**undefiniertem Ergebnis — Aktion**, die ausgeführt werden soll, wenn das Ergebnis der Richtlinienbewertung nicht bestraft wird (UNDEF). Kein Pflichtfeld.
   - **Expression:** Standardsyntaxausdruck, den die Richtlinie verwendet, um auf eine bestimmte Anfrage zu antworten. Zum Beispiel stimmt.
   - **Kommentare** - Irgendwelche Kommentare zu den Richtlinien.

Binden der OAuthIDP-Richtlinie und der LDAP-Richtlinie an den virtuellen Authentifizierungsserver

1. Navigieren Sie zu **Konfiguration > Sicherheit > AAA-Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Aktionen > LDAP**.
2. Klicken Sie im Bildschirm **LDAP-Aktionen** auf **Hinzufügen**.

3. Legen Sie im Bildschirm **Authentifizierungs-LDAP-Server erstellen** die Werte für die folgenden Parameter fest und klicken Sie auf **Erstellen**.
    - **Name —** Der Name der LDAP-Aktion
    - **Servername/ServerIP —** Bereitstellung von FQDN oder IP des LDAP-Servers
    - Wählen Sie geeignete Werte **für Sicherheitstyp, Port, Servertyp, Timeout**
    - Stellen Sie sicher, dass **Authentifizierung** aktiviert ist
    - **Basis-DN —** Basis, von der aus die LDAP-Suche gestartet werden soll. Zum Beispiel dc=aaa, dc = local.
    - **Administrator Bind DN:** Benutzername der Bindung an den LDAP-Server. Zum Beispiel admin@aaa.local.
    - **Administratorkennwort/Kennwort bestätigen: Kennwort zum Binden von LDAP**
    - Klicken Sie auf **Verbindung testen**, um Ihre Einstellungen zu testen.
    - **Attribut für Server-Anmeldename:** Wählen Sie **“sAMAccountName”**
    - Andere Felder sind nicht Pflichtfelder und können daher nach Bedarf konfiguriert werden.
4. Navigieren Sie zu **Konfiguration > Sicherheit > AAA-Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinie.**
5. Klicken Sie im Bildschirm **Authentifizierungsrichtlinien** auf **Hinzufügen**.
6. Legen Sie auf der Seite **Authentifizierungsrichtlinie erstellen** die Werte für die folgenden Parameter fest und klicken Sie auf **Erstellen.**
    - **Name —** Name der LDAP-Authentifizierungsrichtlinie.
    - **Aktionstyp —** Wählen Sie **LDAP aus.**
    - **Aktion —** Wählen Sie die LDAP-Aktion aus.
    - **Ausdruck —** Standard-Syntaxausdruck, den die Richtlinie verwendet, um auf bestimmte Anforderungen zu antworten. Zum Beispiel stimmt**.

Die OAuth-Funktion unterstützt jetzt die folgenden Funktionen in der Token-API von Relying Party (RP) und von der IdP-Seite von Citrix Gateway und Citrix ADC.

- Unterstützung von PKCE (Proof Key for Code Exchange)
- Unterstützung für client_assertion

So konfigurieren Sie die Citrix ADC-Appliance als IdP mithilfe des OIDC-Protokolls mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
add authentication OAuthIDPProfile <name> [-clientID <string>][-
    clientSecret ][-redirectURL <URL>][-issuer <string>][-audience <
    string>][-skewTime <mins>] [-defaultAuthenticationGroup <string>]
```



```
2
3 add authentication OAuthIdPPolicy <name> -rule <expression> [-action <
    string> [-undefAction <string>] [-comment <string>][-logAction <
    string>]
4
5 add authentication ldapAction aaa-ldap-act -serverIP 10.0.0.10 -
    ldapBase "dc=aaa,dc=local"
6
7 ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password> -
    ldapLoginName sAMAccountName
8
9 add authentication policy aaa-ldap-adv-pol -rule true -action aaa-ldap-
    act
10
11 bind authentication vserver auth_vs -policy <ldap_policy_name> -
    priority 100 -gotoPriorityExpression NEXT
12
13 bind authentication vserver auth_vs -policy <OAuthIDPPolicyName> -
    priority 5 -gotoPriorityExpression END
14
15 bind vpn global  - certkey <>
16 <!--NeedCopy-->
```

Hinweis

- Sie können mehr als einen Schlüssel binden. Öffentliche Teile von Zertifikaten, die gebunden sind, werden als Antwort auf gesendet `jwks\\_uri query (https://gw/oauth/idp/certs)`.
- Ab Version Citrix ADC 13.0—85.19 unterstützt der introspektive OAuth-IdP-Endpunkt die Eigenschaft `active: true`

Unterstützung von verschlüsselten Token im OIDC-Protokoll

Die Citrix ADC-Appliance mit dem OIDC-Mechanismus unterstützt jetzt das Senden von verschlüsselten Token zusammen mit signierten Token. Die Citrix ADC-Appliance verwendet JSON-Webverschlüsselungsspezifikationen zur Berechnung der verschlüsselten Token und unterstützt nur die kompakte Serialisierung von verschlüsselten Token. Um ein OpenID-Token zu verschlüsseln, benötigt eine Citrix ADC-Appliance den öffentlichen Schlüssel der angehörenden Partei (RP). Der öffentliche Schlüssel wird dynamisch erhalten, indem der bekannte Konfigurationsendpunkt der angehörenden Partei abgerufen wird.

Eine neue Option "relyingPartyMetadataURL" wurde im Profil "authentication OAuthIDPProfile" eingeführt.

So konfigurieren Sie den Endpunkt der Anbieterpartei mit CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

“‘set authentication OAuthIDPProfile [-relyingPartyMetadataURL] [-refreshInterval] [-status < >]

```
- **relyingPartyMetadataURL** - Endpunkt, an dem Citrix ADC IdP
  Details über die konfigurierte Anbietergesellschaft abrufen kann.
  Die Metadatenantwort muss Endpunkte für jwks_uri für öffentliche RP-
  Schlüssel enthalten.

- **refreshInterval** - Definiert die Rate, mit der dieser Endpunkt
  abgefragt werden muss, um die Zertifikate in Minuten zu
  aktualisieren.

- **status** - Spiegelt den Status des Abrufvorgangs wider. Der Status
   ist abgeschlossen, sobald die Citrix ADC-Appliance die öffentlichen
   Schlüssel erfolgreich abgerufen hat.

   **Beispiel**

   ```
   set authentication OAuthIDPProfile sample_profile -
      relyingPartyMetadataURL https://rp.customer.com/metadata -
      refreshInterval 50 -status < >
   <!--NeedCopy-->
```

Nachdem der Endpunkt konfiguriert wurde, fragt eine Citrix ADC-Appliance zuerst den bekannten Endpunkt der vertrauenden Partei zum Lesen der Konfiguration ab. Derzeit verarbeitet die Citrix ADC-Appliance nur den Endpunkt “jwks_uri”.

- Wenn der ‘jwks_uri’ in der Antwort nicht vorhanden ist, ist der Status des Profils nicht vollständig.
- Wenn der ‘jwks_uri’ in der Antwort vorhanden ist, fragt Citrix ADC diesen Endpunkt auch ab, um die öffentlichen Schlüssel der angehörenden Partei zu lesen.

> **Hinweis:** Für die Token-Verschlüsselung werden nur Algorithmen des Verschlüsselungstyps RSAES-OAEP und AES GCM unterstützt.

Unterstützung von benutzerdefinierten Attributen auf OpenID Connect

OpenID-vertrauende Parteien benötigen möglicherweise mehr als einen Benutzernamen oder einen Benutzerprinzipalnamen (UPN) im Token, um das Benutzerprofil zu erstellen oder Autorisierungsentscheidungen zu treffen. In den meisten Fällen müssen die Benutzergruppen


```

Autorisierungsrichtlinien für den Benutzer anwenden. Manchmal sind weitere Details wie der Vor- oder Nachname für die Bereitstellung eines Benutzerkontos erforderlich.

Citrix ADC-Appliance, die als IdP konfiguriert ist, kann verwendet werden, um zusätzliche Attribute im OIDCid_token über Ausdrücke zu senden. Erweiterte Richtlinienausdrücke werden verwendet, um die benutzerdefinierten Attribute gemäß der Anforderung zu senden. Der Citrix IdP wertet die Ausdrücke aus, die den Attributen entsprechen, und berechnet dann das endgültige Token.

Citrix ADC-Appliance jSonify die Ausgabedaten automatisch. Beispielsweise sind Zahlen (wie SSN) oder boolesche Werte (true oder false) nicht von Anführungszeichen umgeben. Mehrwertige Attribute, wie Gruppen, werden innerhalb einer Array-Markierung platziert ("[" und "]"). Die komplexen Typattribute werden nicht automatisch berechnet, und Sie können den PI-Ausdruck dieser komplexen Werte entsprechend Ihrer Anforderung konfigurieren.

#### So konfigurieren Sie den Endpunkt der Anbieterpartei mit CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set oauthidpprofile <name> -attributes <AAA-custom-attribute-pattern>
<!--NeedCopy-->
```

Die<AAA-custom-attribute-pattern> kann beschrieben werden als:

Attribute1=PI-Expression@@@attribute2=PI-Expression@@@

'attribute1','attribute2' are literal strings that represent the name of the attribute to be inserted in the id_token.

> **Hinweis:** Sie können bis zu 2.000 Byte an Attributen konfigurieren.

Beispiel: `set oauthidpprofile sample_1 -attributes q{ myname=http.req.user.name@@@ssn="123456789"@@@jit="false"@@@groups=http.req.user.groups }`

- Der vorangegangene PI-Ausdruck ist ein erweiterter Richtlinienausdruck, der den Wert darstellt, der für das Attribut verwendet werden soll. Der PI-Ausdruck kann verwendet werden, um ein String-Literal zu senden, z. B. "'hartcodierter String" '. Das Stringliteral ist von doppelten Anführungszeichen um einfache Anführungszeichen oder doppelte Anführungszeichen um einen Anfang und ein Muster herum umgeben (wie bereits erwähnt, ist das Startmuster "q {"). Wenn der Wert des Attributs kein String-Literal ist, wird der Ausdruck zur Laufzeit ausgewertet und sein Wert wird im Token gesendet. Wenn der Wert zur Laufzeit leer ist, wird das entsprechende Attribut dem ID-Token nicht hinzugefügt.
- Wie im Beispiel definiert, ist "false" eine literale Zeichenfolge für das Attribut "jit". Außerdem hat `ssn` einen hartcodierten Wert als Referenz. Gruppen und `myname` sind PI-Ausdrücke, die Zeichenfolgen ergeben.

Unterstützung für aktiv-aktive GSLB-Bereitstellungen auf Citrix Gateway

Citrix Gateway, das mit dem OIDC-Protokoll als Identity Provider (IdP) konfiguriert ist, kann aktiv-aktive GSLB-Bereitstellungen unterstützen. Die aktiv-aktive GSLB-Bereitstellung auf dem Citrix Gateway IdP ermöglicht den Lastausgleich einer eingehenden Benutzeranmeldeanforderung an mehreren geografischen Standorten.

> **Wichtig**
>
> Citrix empfiehlt, Zertifizierungsstellenzertifikate an den SSL-Dienst zu binden und die Zertifikatvalidierung für den SSL-Dienst zu aktivieren, um die Sicherheit zu erhöhen.

Weitere Informationen zum Konfigurieren des GSLB-Setups finden Sie unter Beispiel für eine GSLB-Setup und -Konfiguration.

API-Authentifizierung mit der Citrix ADC Appliance

October 5, 2021

Es gibt einen Paradigmenwechsel in der Art und Weise, wie moderne Anwendungen mit ihren Kunden interagieren. Traditionell wurden Browser-Clients verwendet, um auf Dienste zuzugreifen. Anwendungen setzen in der Regel Session-Cookies, um den Benutzerkontext zu verfolgen. Moderne und verteilte Anwendungen machen es schwierig, Benutzersitzungen über Microservices hinweg zu verwalten. Aus diesem Grund sind die meisten Anwendungszugriffe API-basiert.
Kunden, die mit diesen verteilten Diensten kommunizieren, haben sich ebenfalls weiterentwickelt. Die meisten Clients erhalten Token von einer vertrauenswürdigen Entität namens Autorisierungsserver, um die Benutzeridentität und den Zugriff zu beweisen. Diese Clients präsentieren dann das Token der Anwendung mit jeder Zugriffsanforderung. Daher müssen herkömmliche Proxy-Geräte wie Citrix ADC weiterentwickelt werden, um diese Clients zu unterstützen. Eine Citrix ADC Appliance bietet Administratoren die Möglichkeit, solchen Datenverkehr zu verarbeiten. Citrix ADC kann als API-Gateway bereitgestellt werden, um den gesamten Datenverkehr, der für die veröffentlichten Dienste bestimmt ist, zu Front-End zu ermöglichen. Ein API Gateway kann für herkömmliche (Hybrid Multi Cloud oder HMC) oder Cloud-native Umgebungen bereitgestellt werden. Das API Gateway beendet den gesamten eingehenden Datenverkehr, um mehrere Dienste wie Authentifizierung, Autorisierung, Ratenbegrenzung, Routing, Caching, SSL-Offload, Anwendungsfirewall usw. anzubieten. Daher wird es zu einer kritischen Komponente in der Infrastruktur.

Token-Typen

Token, die während des API-Zugriffs ausgetauscht werden, entsprechen größtenteils dem OAuth/OpenID Connect (OIDC) -Protokoll. Zugriffstoken, die nur für “delegierten Zugriff” verwendet

werden, entsprechen dem OAuth-Protokoll, während ID-Token, die OIDC entsprechen, ebenfalls Benutzerinformationen enthalten.
Zugriffstoken sind normalerweise ein undurchsichtiger oder zufälliger Datenblöcke. Sie können jedoch manchmal Sing-Token sein, die den JWT-Standards (Json Web Token) entsprechen. ID-Token sind immer signierte JWTs.

API-Zugriff mit OAuth

Der OAuth-Authentifizierungstyp auf einer Citrix ADC Appliance kann verwendet werden, um sowohl OAuth- als auch OIDC-Protokolle zu verarbeiten. OIDC ist eine Erweiterung des OAuth-Protokolls.

OAuthAction auf einer Citrix ADC Appliance kann verwendet werden, um interaktive Clients wie Browser und native Clients wie Clientanwendungen zu verarbeiten. Interaktive Clients werden zum Identity Provider für die Anmeldung mithilfe des OIDC-Protokolls umgeleitet. Native Clients können Token Out-of-Band-Abrufen und diese Token auf einer Citrix ADC Appliance für den Zugriff bereitstellen.

> **Hinweis:**
>
> Das von Endpunkten erhaltene Zugriffstoken kann für nachfolgende Anforderungen zwischengespeichert werden, wodurch die API-Performance verbessert wird.

Um die Token-Caching-Unterstützung über die Befehlszeile zu konfigurieren, geben Sie den folgenden Befehl an der Eingabeaufforderung ein:

```
1 set aaaparameter  - apITokenCache <ENABLED>
2
3 <!--NeedCopy-->
```

In den folgenden Abschnitten wird die API-Zugriffsmethode beschrieben, die von nativen Clients ausgeführt wird.

Virtueller Server für API-Zugriff

Um eine Citrix ADC Appliance für einen API-Zugriff bereitzustellen, wird ein virtueller Traffic Management (TM) Server mit 401-Authentifizierung bereitgestellt. Er ist mit einem virtuellen Authentifizierungsserver (Authentifizierung, Autorisierung und Überwachung) verknüpft, um die Authentifizierungs- und Sitzungsrichtlinien zu speichern. Nach Konfiguration Snippet erstellt einen solchen virtuellen Server.


```
Add lb vserver lb-api-access SSL <IP> 443 -authn401 On -AuthnVsName
    auth-api-access

Bind ssl vserver lb-api-access -certkeyName <ssl-cert-entity>

Add authentication vserver auth-api-access SSL
<!--NeedCopy-->
```

> **Hinweis:**
>
> Sie müssten einen Dienst an den TM-vserver und eine Authentifizierungsrichtlinie (mit OAuthAction wie folgt beschrieben) an den virtuellen Authentifizierungsserver binden, um die Konfiguration abzuschließen.

Nach dem Erstellen des virtuellen Servers muss eine OAuthAction zusammen mit der entsprechenden Richtlinie hinzugefügt werden. Es gibt mehrere andere Optionen innerhalb einer OAuth-Aktion, abhängig vom Tokentyp und anderen Sicherheitsmechanismen.

OAuth-Konfiguration für ID-Tokens

ID-Token sind immer signierte JWTs. Das heißt, sie tragen Header, Payload und Signatur. Da es sich um eigenständige Token handelt, kann eine Citrix ADC Appliance diese Token lokal validieren. Um diese Token zu validieren, müsste die Appliance den öffentlichen Schlüssel des entsprechenden privaten Schlüssels kennen, der zum Signieren dieser Token verwendet wird.

Es folgt ein Beispiel für OAuthAction mit bestimmten obligatorischen Argumenten zusammen mit “certEndpoint”.

```
Add authentication OAuthAction oauth-api-access -clientid <your-client-
    id> -clientsecret <your-client-secret> -authorizationEndpoint <URL
    to which users would be redirected for login> -tokenEndpoint <
    endpoint at which tokens could be obtained> -certEndpoint <uri at
    which public keys of IdP are published>
<!--NeedCopy-->
```

Hierbei gilt:

- **Client-ID** — Eindeutige Zeichenfolge, die SP identifiziert. Der Autorisierungsserver leitet die Clientkonfiguration mit dieser ID ab. Maximale Länge: 127.
- **Client Secret** — Geheime Zeichenfolge, die vom Benutzer und Autorisierungsserver eingerichtet wurde. Maximale Länge: 239.
- **authorizationEndpoint** - URL, unter der sich Benutzer normalerweise anmelden würden (bei Verwendung interaktiver Clients).

- **tokenEndpoint** - URL auf dem Autorisierungsserver, auf dem Token/Code erhalten/ausgetauscht werden
- **certEndpoint** - URL, unter der der Autorisierungsserver öffentliche Schlüssel veröffentlicht, die zum Signieren der Token verwendet werden. Autorisierungsserver kann mehr als einen Schlüssel veröffentlichen und einen von ihnen auswählen, um Token zu signieren.

> **Hinweis:** Client ID/Client Secret/authorizationEndpoint/TokenEndpoint sind optionale Parameter für API-Zugriff. Es ist jedoch empfehlenswert, Werte für diese Parameter bereitzustellen, da die Aktions-Entität für verschiedene Zwecke wiederverwendet werden kann.

In der vorhergehenden Konfiguration ist 'CertEndPointPoint' für die ID-Token-Validierung unerlässlich. Dieser Endpunkt enthält öffentliche Schlüssel des Zertifikats, das zum Signieren der Token verwendet wird. Diese öffentlichen Schlüssel müssen der JWKs (Json Web Keys) Spezifikation entsprechen.

Sobald der CertEndPoint auf der Citrix ADC Appliance konfiguriert ist, wird der Endpunkt regelmäßig abgefragt (mit dem Standardintervall von 1 Tag, das in der Konfiguration angepasst werden kann), um die öffentlichen Schlüssel auf dem neuesten Stand zu halten. Nachdem die öffentlichen Schlüssel verfügbar sind, kann ADC eine lokale Validierung der eingehenden ID-Token durchführen.

OAuth-Konfiguration für undurchsichtige Zugriffstoken

Undurchsichtige Token können nicht lokal auf der Citrix ADC Appliance überprüft werden. Diese müssen auf dem Autorisierungsserver validiert werden. Eine Citrix ADC Appliance verwendet das in den OAuth-Spezifikationen genannte Introspektionsprotokoll, um diese Token zu überprüfen. Eine neue Option, IntroSpectURL, wird in der OAuth-Konfiguration zur Überprüfung undurchsichtiger Token bereitgestellt.

```
1 set oauthAction oauth-api-acccess -introspectURL <uri of the
     Authorization Server for introspection>
2
3 <!--NeedCopy-->
```

Das Format der Introspektion-API entspricht der Spezifikation unter `https://tools.ietf.org/html/rfc7662##section-2.1` wie folgt:

```
1 POST /introspect HTTP/1.1
2 Host: server.example.com
3 Accept: application/json
4 Content-Type: application/x-www-form-urlencoded
```



```
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
token=mF_9.B5f-4.1JqM&token_type_hint=access_token

<!--NeedCopy-->
```

Bindungsrichtlinie an Authentifizierungs-vserver

Sobald OAuthAction erstellt wurde, muss die entsprechende Richtlinie erstellt werden, um sie aufzurufen.

```
add authentication policy oauth-api-access -rule <> -action <oauth-api-access><!--NeedCopy-->
```

bind authentication vserver auth-api-access -policy oauth-api-access -pri 100

```
## Zusätzliche Sicherheitseinstellungen auf einer Citrix ADC Appliance

Die Token-Validierung umfasst Token Lebensdauerprüfungen. Tokens außerhalb der akzeptablen Zeit werden abgelehnt. Im Folgenden finden Sie die zusätzlichen Einstellungen für zusätzliche Sicherheit. Einige von diesen wird empfohlen, immer konfiguriert zu werden.

**Zielgruppe**: OAuth-Aktion kann mit einem beabsichtigten Empfänger des Token konfiguriert werden. Alle Token werden mit dieser konfigurierten URL abgeglichen. Eine Citrix ADC Appliance verfügt über eine zusätzliche Funktion, bei der das Zielgruppenfeld tatsächlich auf ein Muster verweist, das auf der Appliance festgelegt ist. Mit diesem Mustersatz kann ein Administrator mehr als eine URL für die Zielgruppe konfigurieren.

<!--NeedCopy-->
```

add policy patset oauth_audiences

bind patset oauth_audiences https://app1.company.com

bind patset oauth_audiences https://app2.company.com

bind patset oauth_audiences httpsL//app1.company.com/path1

set oAuthAccess oauth-api-access -audience oauth_audiences


```
Im vorangegangenen Beispiel wird mehr als eine Zielgruppe in einem
    Mustersatz angegeben. Daher ist ein eingehendes Token nur zulässig,
    wenn es eine der konfigurierten URLs im Mustersatz enthält.

**Aussteller**: Identität des Servers, dessen Token akzeptiert werden
    sollen.  Maximale Länge: 127. Es ist eine gute Praxis, den
    Aussteller der Token in OAuth Aktion zu konfigurieren. Dadurch wird
    sichergestellt, dass Token, die von einem falschen
    Autorisierungsserver ausgegeben werden, nicht zulässig sind.

**SkeWTime**: Gibt die zulässige Taktverzerrung in Minuten an, die eine
     Citrix ADC Appliance für ein eingehendes Token zulässt. Wenn
    beispielsweise SkewTime 10 ist, wäre das Token gültig von (aktuelle
    Zeit - 10) min bis (aktuelle Zeit + 10) min, also 20 min.
    Standardwert: 5

**AllowedAlgorithms**: Diese Option ermöglicht es dem Administrator,
    bestimmte Algorithmen in den eingehenden Token zu beschränken.
    Standardmäßig sind alle unterstützten Methoden zulässig. Diese kö
    nnen jedoch mit dieser Option gesteuert werden.

Die folgende Konfiguration stellt sicher, dass nur Token zulässig sind,
     die RS256 und RS512 verwenden:

<!--NeedCopy-->
```

set oAuthAction oauth-api-access -allowedAlgorithms RS256 RS512

```
Nach der obigen Konfiguration sind nur Token zulässig, die RS256 und
    RS512 verwenden.

## Umgehen bestimmter Datenverkehr von der Authentifizierung

In vielen Fällen gibt es einige Ermittlungs-APIs, die für die Clients ö
    ffentlich zugänglich sind. Diese APIs zeigen in der Regel die
    Konfiguration und die Funktionen des Dienstes selbst an. Ein
    Administrator kann die Citrix ADC Appliance so konfigurieren, dass
    die Authentifizierung von diesen Metadaten-URLs umgangen wird, indem
     die Richtlinie "Keine Authentifizierung" wie folgt beschrieben wird
    :

<!--NeedCopy-->
```


add authentication policy auth-bypass-policy -rule <> -action NO_AUTHN

bind authentication vserver auth-api-access -policy auth-bypass-policy -pri 110

```
1 NO_AUTHN ist eine implizite Aktion, die dazu führt, dass die
     Authentifizierung abgeschlossen wird, wenn die Regel übereinstimmt.
     Es gibt andere Verwendungen der NO_AUTHN Aktion über den Bereich des
      API-Zugriffs hinaus.
2 <!--NeedCopy-->
```

LDAP-Authentifizierung

April 7, 2022

Wie bei anderen Arten von Authentifizierungsrichtlinien umfasst eine LDAP-Authentifizierungsrichtlinie (Lightweight Directory Access Protocol) einen Ausdruck und eine Aktion. Nachdem Sie eine Authentifizierungsrichtlinie erstellt haben, binden Sie sie an einen virtuellen Authentifizierungsserver und weisen ihm eine Priorität zu. Wenn Sie es binden, bezeichnen Sie es auch als primäre oder sekundäre Richtlinie. Zusätzlich zu den Standardauthentifizierungsfunktionen kann LDAP auch andere Active Directory-Server (AD) nach Benutzerkonten für Benutzer durchsuchen, die nicht lokal existieren. Diese Funktion wird als Empfehlungsunterstützung oder Empfehlungsjagd bezeichnet.

Normalerweise konfigurieren Sie den Citrix ADC so, dass er die IP-Adresse des Authentifizierungsservers während der Authentifizierung verwendet. Mit LDAP-Authentifizierungsservern können Sie den ADC auch so konfigurieren, dass er den FQDN des LDAP-Servers anstelle seiner IP-Adresse verwendet, um Benutzer zu authentifizieren. Die Verwendung eines FQDN kann eine ansonsten viel komplexere Authentifizierungs-, Autorisierungs- und Überwachungskonfiguration in Umgebungen vereinfachen, in denen sich der Authentifizierungsserver möglicherweise an einer von mehreren IP-Adressen befindet, aber immer einen einzigen FQDN verwendet. Um die Authentifizierung mithilfe des FQDN eines Servers anstelle seiner IP-Adresse zu konfigurieren, folgen Sie dem normalen Konfigurationsprozess, außer wenn Sie die Authentifizierungsaktion erstellen. Beim Erstellen der Aktion verwenden Sie den **ServerName-Parameter** anstelle des **ServerIP-Parameters** und ersetzen den FQDN des Servers durch seine IP-Adresse.

Bevor Sie entscheiden, ob Sie den ADC so konfigurieren, dass er die IP oder den FQDN Ihres LDAP-Servers zur Authentifizierung von Benutzern verwendet, sollten Sie bedenken, dass die Konfiguration von Authentifizierung, Autorisierung und Überwachung zur Authentifizierung bei einem FQDN anstelle einer IP-Adresse einen zusätzlichen Schritt zum Authentifizierungsprozess darstellt. Jedes Mal, wenn der ADC einen Benutzer authentifiziert, muss er den FQDN auflösen. Wenn sehr viele Be-

nutzer versuchen, sich gleichzeitig zu authentifizieren, verlangsamen die daraus resultierenden DNS-Lookups möglicherweise den Authentifizierungsprozess.

Die LDAP-Empfehlungsunterstützung ist standardmäßig deaktiviert und kann nicht global aktiviert werden. Es muss explizit für jede LDAP-Aktion aktiviert sein. Stellen Sie sicher, dass der AD-Server dieselben akzeptiert `binddn credentials`, die mit dem verweisenden Server (GC) verwendet werden. Um die Empfehlungsunterstützung zu aktivieren, konfigurieren Sie eine LDAP-Aktion, um Verweisen zu folgen, und geben Sie die maximale Anzahl von Empfehlungen an, die folgen sollen.

Wenn die Empfehlungsunterstützung aktiviert ist und der Citrix ADC eine LDAP_REFERRAL-Antwort auf eine Anforderung erhält, folgt Authentifizierung, Autorisierung und Überwachung der Verweisung an den in der Empfehlung enthaltenen Active Directory-Server (AD) und führt das Update auf diesem Server durch. Zunächst sucht Authentifizierung, Autorisierung und Überwachung den Empfehlungsserver in DNS und stellt eine Verbindung zu diesem Server her. Wenn die Empfehlungsrichtlinie SSL/TLS erfordert, stellt sie eine Verbindung über SSL/TLS her. Es bindet dann an den neuen Server mit dem `binddn credentials`, den es mit dem vorherigen Server verwendet hat, und führt den Vorgang aus, der die Empfehlung generiert hat. Diese Funktion ist für den Benutzer transparent.

Die Portnummern für LDAP-Verbindungen lauten:

- 389 für unsichere LDAP-Verbindungen (für Nur-Text-LDAP)
- 636 für sichere LDAP-Verbindungen (für SSL LDAP)
- 3268 für unsichere LDAP-Verbindungen von Microsoft (für Global Catalog Server im Klartext)
- 3269 für sichere LDAP-Verbindungen von Microsoft (für SSL Global Catalog Server)

Die folgende Tabelle enthält Beispiele für Benutzerattributfelder für LDAP-Server:

LDAP-Server	Benutzer-Attribut	Case sensitiv
Microsoft Active Directory-Server	sAMAccountName	Nein
Novell eDirectory	ou	Ja
IBM Verzeichnisserver	uid	Ja
Lotus-Domino	CN	Ja
Sun ONE Verzeichnis (ehemals iPlanet)	uid oder cn	Ja

Diese Tabelle enthält Beispiele für den Basis-DN:

LDAP-Server	Basis-DN
Microsoft Active Directory-Server	DC =citrix, DC = lokal
Novell eDirectory	ou=Benutzer, ou=dev
IBM Verzeichnisserver	cn=Nutzer
Lotus-Domino	OU=Stadt, O=Citrix, C=US
Sun ONE Verzeichnis (ehemals iPlanet)	ou = Menschen, dc =citrix, dc = com

Die folgende Tabelle enthält Beispiele für Bind-DN:

LDAP-Server	Bind DN
Microsoft Active Directory-Server	CN=Administrator, CN=Benutzer, DC=citrix, DC = lokal
Novell eDirectory	cn=admin, o=citrix
IBM Verzeichnisserver	ldap_DN
Lotus-Domino	CN=Notes Administrator, O=Citrix, C=US
Sun ONE Verzeichnis (ehemals iPlanet)	uid=admin,ou=Administrators, ou=TopologyManagement,o=NetscapeRoot

Weitere Informationen zum Einrichten von Authentifizierungsrichtlinien im Allgemeinen finden Sie unter Authentifizierungsrichtlinien. Weitere Informationen zu Citrix ADC-Ausdrücken, die in der Richtlinienregel verwendet werden, finden Sie unter Richtlinien und Ausdrücke.

So erstellen Sie einen LDAP-Authentifizierungsserver mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

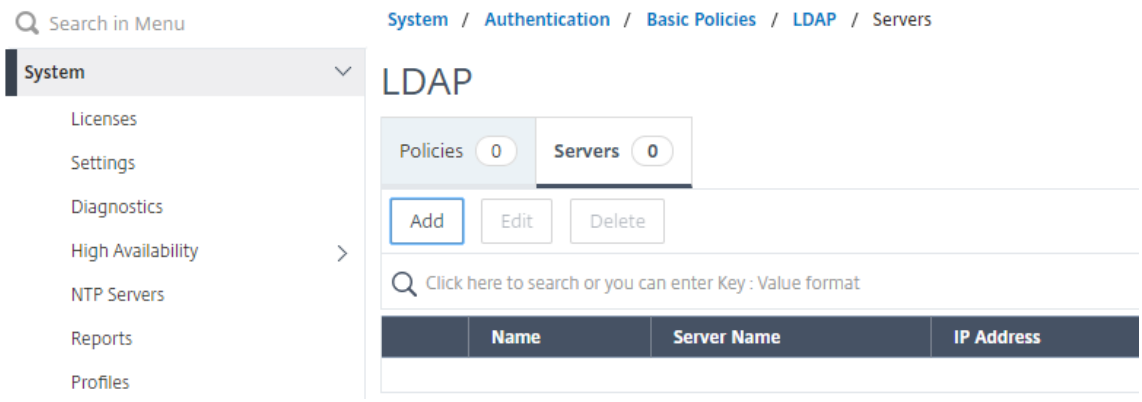
```
add authentication ldapAction <name> {
 -serverIP }
  <ip_addr|ipv6_addr|> | {
 -serverName <string> }
  }
```

Beispiel


```
add authentication ldapAction ldap_server -serverip 1.1.1.1 -serverName
    ldap_test
```

So erstellen Sie einen LDAP-Authentifizierungsserver mit der GUI

1. Navigieren Sie zu **System > Authentifizierung > Grundlegende Richtlinien > LDAP > Server > Hinzufügen**.



2. Konfigurieren Sie auf der Seite **Create Authentication LDAP Server** die Parameter für den LDAP-Server.
3. Klicken Sie auf **Erstellen**.

So aktivieren Sie eine Authentifizierungsrichtlinie mithilfe der CLI

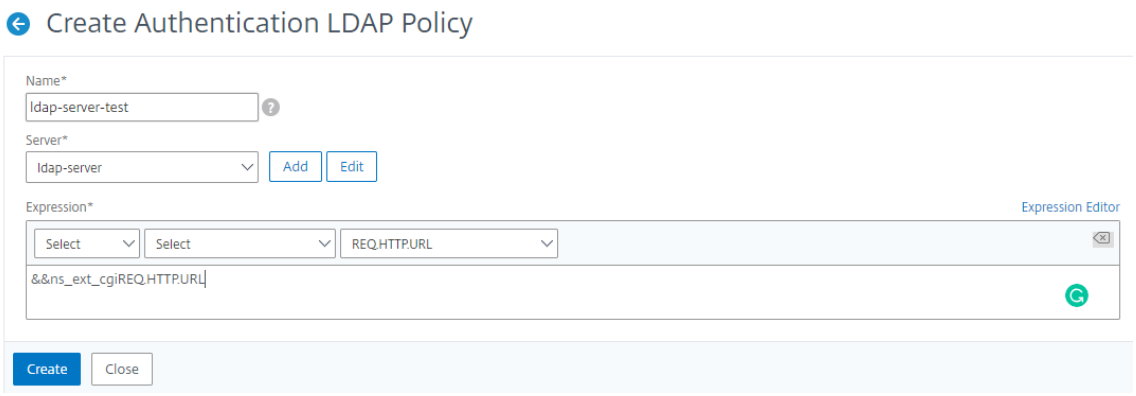
```
add authentication ldappolicy <name> <rule> [<reqAction>]
```

Beispiel:

```
add authentication ldappolicy ldap-service-policy ns_true ldap_Server
```

So erstellen Sie eine LDAP-Authentifizierungsrichtlinie mit der GUI

1. Navigieren Sie zu **System > Authentifizierung > Grundlegende Richtlinien > LDAP > Richtlinien > Hinzufügen**
2. Konfigurieren Sie auf der Seite **LDAP-Authentifizierungsrichtlinie erstellen** die Parameter für die LDAP-Richtlinie.



3. Klicken Sie auf **Erstellen**.

> **Hinweis**
>
> Sie können LDAP-Server/-Richtlinien über die Registerkarte **Sicherheit** konfigurieren. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Grundlegende Richtlinien > LDAP > Server/Richtlinien**.

So aktivieren Sie die LDAP-Empfehlungsunterstützung mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
set authentication ldapAction <name> -followReferrals ON
set authentication ldapAction <name> -maxLDAPReferrals <integer>
<!--NeedCopy-->
```

Beispiel

```
set authentication ldapAction ldapAction-1 -followReferrals ON
set authentication ldapAction ldapAction-1 -maxLDAPReferrals 2
<!--NeedCopy-->
```

Schlüsselbasierte Authentifizierungsunterstützung für die LDAP-Benutzer

Mit der schlüsselbasierten Authentifizierung können Sie jetzt die Liste der öffentlichen Schlüssel abrufen, die auf dem Benutzerobjekt im LDAP-Server über SSH gespeichert sind. Die Citrix ADC Appliance muss während des rollenbasierten Authentifizierungsprozesses (RBA) öffentliche SSH-Schlüssel vom LDAP-Server extrahieren. Der abgerufene öffentliche Schlüssel, der mit SSH kompatibel ist, muss es Ihnen ermöglichen, sich über die RBA-Methode anzumelden.

Ein neues Attribut “sshPublicKey” wird in den Befehlen “add authentication ldapAction” und “set authentication ldapAction” eingeführt. Wenn Sie dieses Attribut verwenden, können Sie die folgenden Vorteile erhalten:

- Kann den abgerufenen öffentlichen Schlüssel speichern, und die LDAP-Aktion verwendet dieses Attribut, um SSH-Schlüsselinformationen vom LDAP-Server abzurufen.
- Kann Attributnamen von bis zu 24 KB extrahieren.

> Hinweis
>
> Der externe Authentifizierungsserver wie LDAP wird nur zum Abrufen von SSH-Schlüsselinformationen verwendet. Es wird nicht für den Authentifizierungszweck verwendet.

Es folgt ein Beispiel für den Ablauf von Ereignissen durch SSH:

- Der SSH-Daemon sendet eine AAA_AUTHENTICATE-Anforderung mit leerem Kennwortfeld an den Authentifizierungs-, Autorisierungs- und Überwachungs-Daemonport
- Wenn LDAP für das Speichern des öffentlichen SSH-Schlüssels konfiguriert ist, antworten Authentifizierung, Autorisierung und Überwachung mit dem Attribut “sshPublicKey” zusammen mit anderen Attributen.
- Der SSH-Daemon überprüft diese Schlüssel mit den Clientschlüsseln.
- Der SSH-Daemon übergibt den Benutzernamen in der Anforderungsnutzlast, und Authentifizierung, Autorisierung und Überwachung geben die für diesen Benutzer spezifischen Schlüssel zusammen mit generischen Schlüsseln zurück.

Um das sshPublicKey -Attribut zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- Mit dem Add-Vorgang können Sie das Attribut “sshPublicKey” während der Konfiguration des Befehls `ldapAction` hinzufügen.

```
1  add authentication ldapAction <name> {
2  -serverIP <ip_addr|ipv6_addr|*> | {
3  -serverName <string> }
4   }
5   [-serverPort <port>] … [-Attribute1 <string>] … [-Attribute16
       <string>][-sshPublicKey <string>][-authentication off]
6  <!--NeedCopy-->
```

- Mit dem set-Vorgang können Sie das “sshPublicKey” -Attribut für einen bereits hinzugefügten ldapAction-Befehl konfigurieren.


```
set authentication ldapAction <name> [-sshPublicKey <string>][-
   authentication off]
<!--NeedCopy-->
```

Unterstützung von Namenswert-Attributen für LDAP-Authentifizierung

Sie können jetzt die Attribute der LDAP-Authentifizierung mit einem eindeutigen Namen zusammen mit Werten konfigurieren. Die Namen werden im LDAP-Aktionsparameter konfiguriert, und die Werte werden durch Abfrage des Namens abgerufen. Durch die Verwendung dieser Funktion kann ein Citrix ADC Appliance-Administrator nun die folgenden Vorteile erzielen:

- Minimiert den Aufwand für Administratoren, indem sie sich das Attribut nach Namen merken (nicht nur nach Wert)
- Verbessert die Suche, um den mit einem Namen verknüpften Attributwert abzufragen
- Bietet eine Option zum Extrahieren mehrerer Attribute

Um diese Funktion an der Eingabeaufforderung der Citrix ADC Appliance zu konfigurieren, geben Sie Folgendes ein:

```
add authentication ldapAction <name> [-Attribute1 <string>]
<!--NeedCopy-->
```

Beispiel

```
add authentication ldapAction ldapAct1 attribute1 mail
<!--NeedCopy-->
```

Unterstützung für die Validierung der End-to-End-LDAP-Authentifizierung

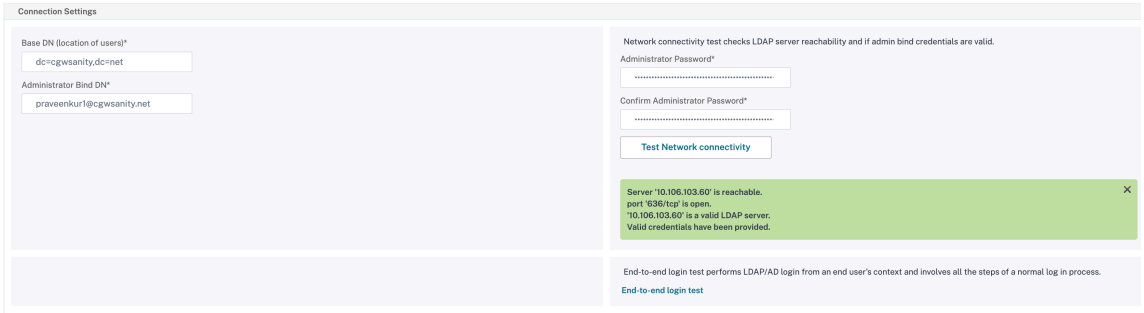
Die Citrix ADC Appliance kann jetzt die End-to-End-LDAP-Authentifizierung über die GUI validieren. Um diese Funktion zu überprüfen, wird eine neue “Test” -Schaltfläche in der GUI eingeführt. Ein Citrix ADC Appliance-Administrator kann diese Funktion verwenden, um die folgenden Vorteile zu erzielen:

- Konsolidiert den gesamten Fluss (Paket-Engine — Citrix ADC AAA-Daemon — externer Server) für eine bessere Analyse
- Verkürzt die Zeit bei der Überprüfung und Behebung von Problemen im Zusammenhang mit einzelnen Szenarien

Sie haben zwei Möglichkeiten, die Testergebnisse der LDAP-End-to-End-Authentifizierung über die grafische Benutzeroberfläche zu konfigurieren und anzuzeigen.

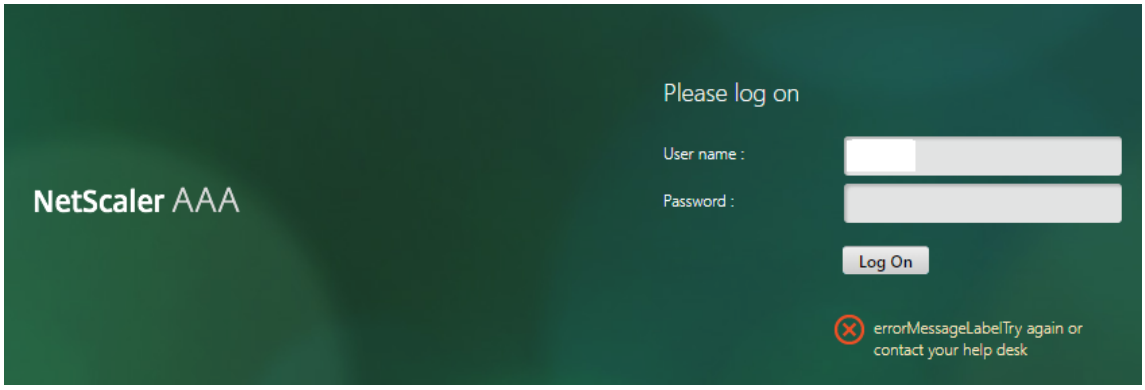
Von der Systemoption

1. Navigieren Sie zu **System > Authentifizierung > Grundlegende Richtlinien > LDAP,** und klicken Sie auf die Registerkarte **Server** .
2. Wählen Sie die verfügbare **LDAP-Aktion** aus der Liste aus.
3. Scrollen Sie auf der Seite **Configure Authentication LDAP Server** nach unten zum Abschnitt **Verbindungseinstellungen** .
4. Klicken Sie auf **Netzwerkkonnektivität testen** , um die LDAP-Serververbindung Sie können eine Popup-Meldung über eine erfolgreiche Verbindung zum LDAP-Server mit TCP-Portdetails und der Authentizität gültiger Anmeldeinformationen anzeigen.



5. Um die End-to-End-LDAP-Authentifizierung anzuzeigen, klicken Sie auf den Link **Ende-zu-Ende-Anmeldetest** .
6. Klicken Sie auf der Seite **Ende-zu-Ende-Anmeldetestauf Testen**.
   - Geben Sie auf der Authentifizierungsseite die gültigen Anmeldeinformationen für die Anmeldung ein. Der Erfolgsbildschirm wird angezeigt.

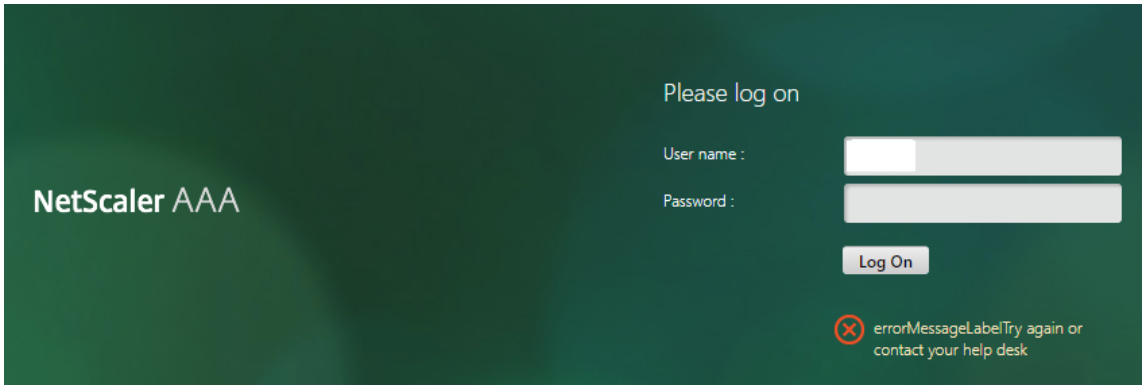
   - Wenn die Authentifizierung fehlschlägt, wird der Fehlerbildschirm angezeigt.



Über die Option Authentifizierung

1. Navigieren Sie zu **Authentifizierung > Dashboard**und wählen Sie die verfügbare LDAP-Aktion aus der Liste aus.
2. Auf der Seite **Configure Authentication LDAP Server** haben Sie im Abschnitt **Verbindungseinstellungen** zwei Optionen.
3. Um die LDAP-Server-Verbindung zu überprüfen, klicken Sie auf **LDAP-Erreichbarkeit testen** . Sie können eine Popup-Meldung über eine erfolgreiche Verbindung zum LDAP-Server mit TCP-Portdetails und der Authentizität gültiger Anmeldeinformationen anzeigen.
4. Um den End-to-End-LDAP-Authentifizierungsstatus anzuzeigen, klicken Sie auf den Link **Endbenutzerverbindung testen** .
5. Klicken Sie auf der Seite **Endbenutzerverbindungtesten auf Test**.
   - Geben Sie auf der Authentifizierungsseite die gültigen Anmeldeinformationen für die Anmeldung ein. Der Erfolgsbildschirm wird angezeigt.

   - Wenn die Authentifizierung fehlschlägt, wird der Fehlerbildschirm angezeigt.



Benachrichtigung 14 Tage vor Kennwortablauf für LDAP-Authentifizierung

Die Citrix ADC Appliance unterstützt jetzt eine 14-tägige Benachrichtigung zum Ablauf des Kennworts für die LDAP-basierte Authentifizierung. Mit dieser Funktion können Administratoren die Endbenutzer über den Ablauf des Kennworts informieren. Der Schwellenwert wird in Tagen angegeben. Die 14-tägige Benachrichtigung über den Ablauf des Kennworts ist ein Vorläufer des Self-Service-Kennwort-Reset (SSPR).

> **Hinweis**
>
> Der Höchstwert oder Schwellenwert für die Benachrichtigung über den Ablauf des Kennworts in Tagen beträgt 255 Tage.

Vorteile der Benachrichtigung über Ablauf des Kennworts

- Ermöglichen Sie Benutzern, ihre Passwörter selbst zurückzusetzen, und bieten Sie Administratoren eine flexible Möglichkeit, den Endbenutzer innerhalb von Tagen über den Ablauf ihres Kennworts zu informieren.
- Eliminiert die Abhängigkeit von Endbenutzern, ihre Kennwort-Ablauftage zu verfolgen
- Sendet Benachrichtigungen an die VPN-Portalseite an die Benutzer (basierend auf der Anzahl der Tage), um ihr Kennwort vor Ablauf zu ändern.

> **Hinweis**
>
> Diese Funktion gilt nur für LDAP-basierte Authentifizierungsschemata, nicht für RADIUS oder TACACS.

Grundlegendes zur 14-tägigen Kennwort-Benachrichtigung

Die Citrix ADC Appliance ruft zwei Attribute (`Max-Pwd-Age and Pwd-Last-Set`) vom LDAP-Authentifizierungsserver ab.

- **Max-Pwd-Alter.** Dieses Attribut gibt die maximale Zeit in Intervallen von 100 Nanosekunden an, bis das Kennwort gültig ist. Der Wert wird als große Ganzzahl gespeichert, die die Anzahl der 100-Nanosekunden-Intervalle ab dem Zeitpunkt darstellt, an dem das Kennwort vor Ablauf des Kennworts festgelegt wurde.
- **Pwd-Letzter Satz.** Dieses Attribut bestimmt das Datum und die Uhrzeit, zu der das Kennwort für ein Konto zuletzt geändert wurde.

Durch das Abrufen der beiden Attribute vom LDAP-Authentifizierungsserver bestimmt die Citrix ADC Appliance die verbleibende Zeit, bis das Kennwort für einen bestimmten Benutzer abläuft. Diese Informationen werden gesammelt, wenn Benutzeranmeldeinformationen auf dem Authentifizierungsserver überprüft werden und eine Benachrichtigung an den Benutzer zurückgesendet wird.

Ein neuer Parameter "pwdExpiryNotification" wird für den Befehl `set aaa parameter` eingeführt. Mithilfe dieses Parameters kann ein Administrator die Anzahl der verbleibenden Tage bis zum Ablauf des Kennworts verfolgen. Die Citrix ADC Appliance kann jetzt den Endbenutzer über den Ablauf seines Kennworts informieren.

> **Hinweis**
>
> Derzeit funktioniert diese Funktion nur für Authentifizierungsserver mit Microsoft AD-Servern mit LDAP-Implementierung. Die Unterstützung für OpenLDAP-basierte Server wird später ins Visier genommen.

Es folgt ein Beispiel für den Ablauf der Ereignisse zum Festlegen einer 14-tägigen Benachrichtigung über den Ablauf des Kennworts:

1. Ein Administrator legt mithilfe der Citrix ADC Appliance eine Zeit (14 Tage) für den Ablauf des Kennworts fest.
2. Der Benutzer sendet eine HTTP- oder HTTPS-Anforderung, um auf eine Ressource auf dem Backend-Server zuzugreifen.
3. Vor dem Bereitstellen des Zugriffs überprüft die Citrix ADC Appliance die Benutzeranmeldeinformationen mit den auf dem LDAP-Authentifizierungsserver konfigurierten Informationen.
4. Zusammen mit dieser Abfrage an den Authentifizierungsserver führt die Citrix ADC Appliance die Anforderung aus, die Details der beiden Attribute abzurufen (`Max-Pwd-Age and Pwd-Last-Set`).
5. Abhängig von der verbleibenden Zeit bis zum Ablauf des Kennworts wird eine Ablaufbenachrichtigung angezeigt.
6. Der Benutzer ergreift dann geeignete Maßnahmen, um das Kennwort zu aktualisieren.

So konfigurieren Sie eine 14-tägige Ablaufbenachrichtigung mithilfe der Befehlszeilenschnittstelle

> **Hinweis**
>
> Die 14-tägige Ablaufbenachrichtigung kann für clientlose VPN- und Voll-VPN-Anwendungsfälle und nicht für ICA-Proxy konfiguriert werden.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
set aaa parameter  - pwdExpiryNotificationDays <positive_integer>

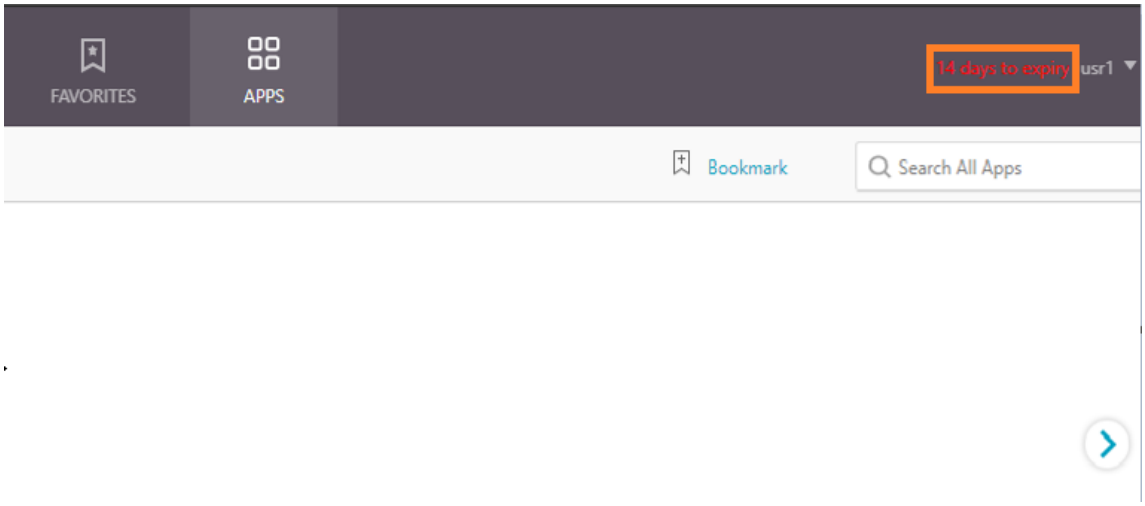
show aaa parameter
<!--NeedCopy-->
```

Beispiel

```
    > set aaa parameter -pwdExpiryNotificationDays 14
    Done
    > show aaa parameter                              Configured AAA
       parameters  EnableStaticPageCaching: YES
       EnableEnhancedAuthFeedback: NO  DefaultAuthType: LOCAL
       MaxAAAUsers:           Unlimited
                                              AAAD nat ip: None
                  EnableSessionStickiness : NO  aaaSessionLoglevel :
       INFORMATIONAL               AAAD Log Level : INFORMATIONAL
                      Dynamic address: OFF
       GUI mode: ON
       Max Saml Deflate Size: 1024             Password Expiry
          Notification Days: 14
<!--NeedCopy-->
```

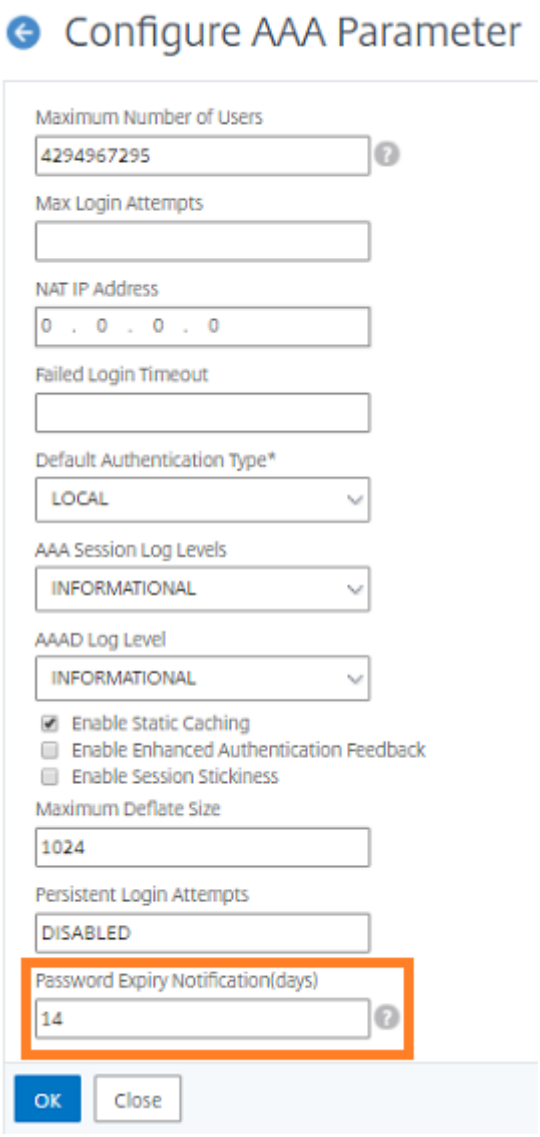
So konfigurieren Sie 14-Tage-Ablaufbenachrichtigung mit der GUI

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Authentifizierungseinstellungen**.
2. Klicke auf **AAA-Authentifizierungseinstellungen ändern**.
3. Geben Sie auf der Seite **AAA-Parameter konfigurieren** die Tage im Feld **Kennwortablaufbenachrichtigung (Tage)** an.



4. Klicken Sie auf **OK.**

   Die Benachrichtigung wird in der oberen rechten Ecke der VPN-Portalseite angezeigt.



Konfigurieren der LDAP-Authentifizierung auf der Citrix ADC-Appliance für Verwaltungszwecke

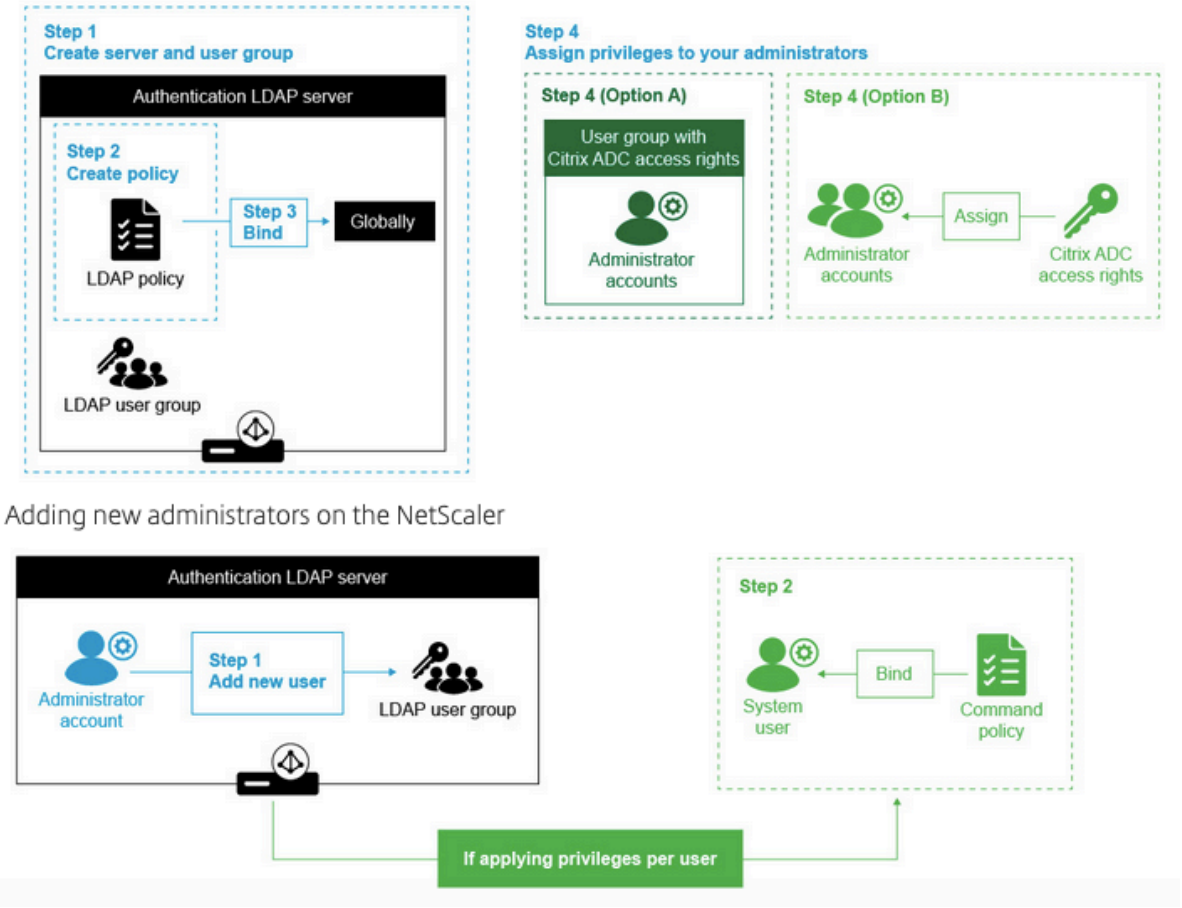
December 3, 2021

Sie können die Benutzeranmeldung bei der Citrix ADC Appliance mithilfe der Active Directory-Anmeldeinformationen (Benutzername und Kennwort) für Verwaltungszwecke (Superuser, schreibgeschützt, Netzwerkberechtigungen und alle anderen) konfigurieren.

Voraussetzungen

- Windows Active Directory-Domänencontroller
- Eine dedizierte Domänengruppe für NetScaler-Administratoren
- Citrix Gateway 10.1 und höhere Versionen

Die folgenden Abbildungen veranschaulichen die LDAP-Authentifizierung auf der Citrix ADC Appliance.

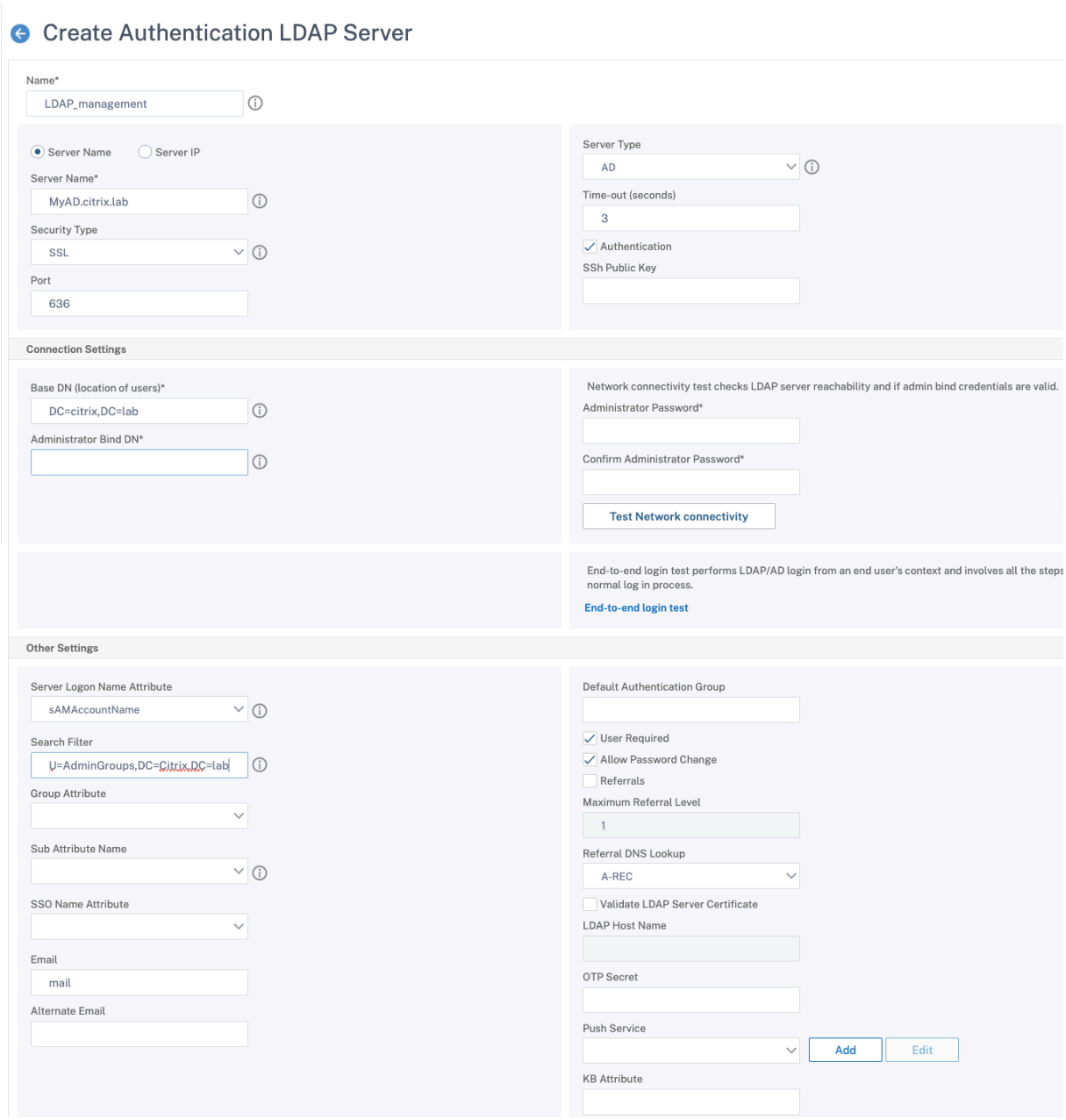


Konfigurationsschritte auf hoher Ebene

1. Erstellen Sie einen LDAP-Server
2. Erstellen einer LDAP-Richtlinie
3. Binden Sie die LDAP-Richtlinie
4. Weisen Sie Ihren Administratoren auf eine der folgenden Arten Berechtigungen zu
    - Berechtigungen auf Gruppe anwenden
    - Wenden Sie Berechtigungen für jeden Benutzer einzeln an

Erstellen eines Authentifizierungs-LDAP-Servers

1. Navigieren Sie zu **System > Authentifizierung > LDAP**.
2. Klicken Sie auf die Registerkarte **Server** und dann auf **Hinzufügen**.
3. Schließen Sie die Konfiguration ab, und klicken Sie dann auf **Erstellen**.



Hinweis:

In diesem Beispiel ist der Zugriff auf die Citrix ADC Appliance beschränkt, indem die Authentifizierung für die Benutzergruppenmitgliedschaft durch Festlegen des Suchfilters gefiltert wird. Der für dieses Beispiel verwendete Wert ist - & (memberof=CN=NSG_Admin, OU=AdminGroup,

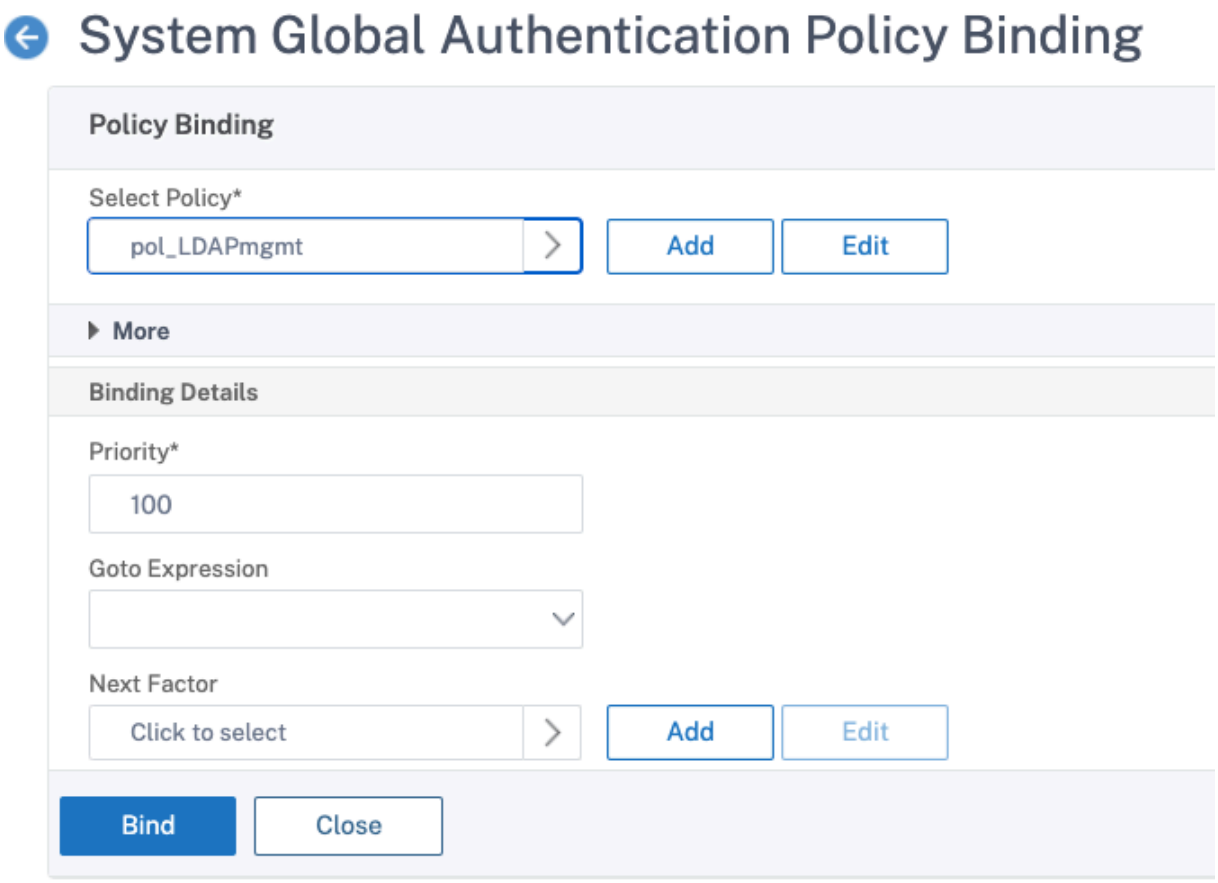
> dc=Citrix, dc=Lab)

Erstellen einer LDAP-Richtlinie

1. Navigieren Sie zu **System > Authentifizierung > Erweiterte Richtlinien > Richtlinie**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie einen Namen für die Richtlinie ein und wählen Sie den Server aus, den Sie in den vorherigen Schritten erstellt haben.
4. Geben Sie im Feld Ausdruckstext den entsprechenden Ausdruck ein, und klicken Sie dann auf **Erstellen**.

Binden Sie die LDAP-Richtlinie global

1. Navigieren Sie zu **System > Authentifizierung > Erweiterte Richtlinien > Richtlinie**.
2. Klicken Sie auf der Seite Authentifizierungsrichtlinien auf **Globale Bindungen**.
3. Wählen Sie die Richtlinie aus, die Sie erstellt haben (in diesem Beispiel pol_LDAPmgmt).
4. Wählen Sie entsprechend eine Priorität (je niedriger die Zahl, desto höher die Priorität)
5. Klicken Sie auf **Binden** und dann auf **Fertig**. In der Spalte **Global gebunden** wird ein grünes Häkchen angezeigt.



Weisen Sie Ihren Administratoren Berechtigungen zu

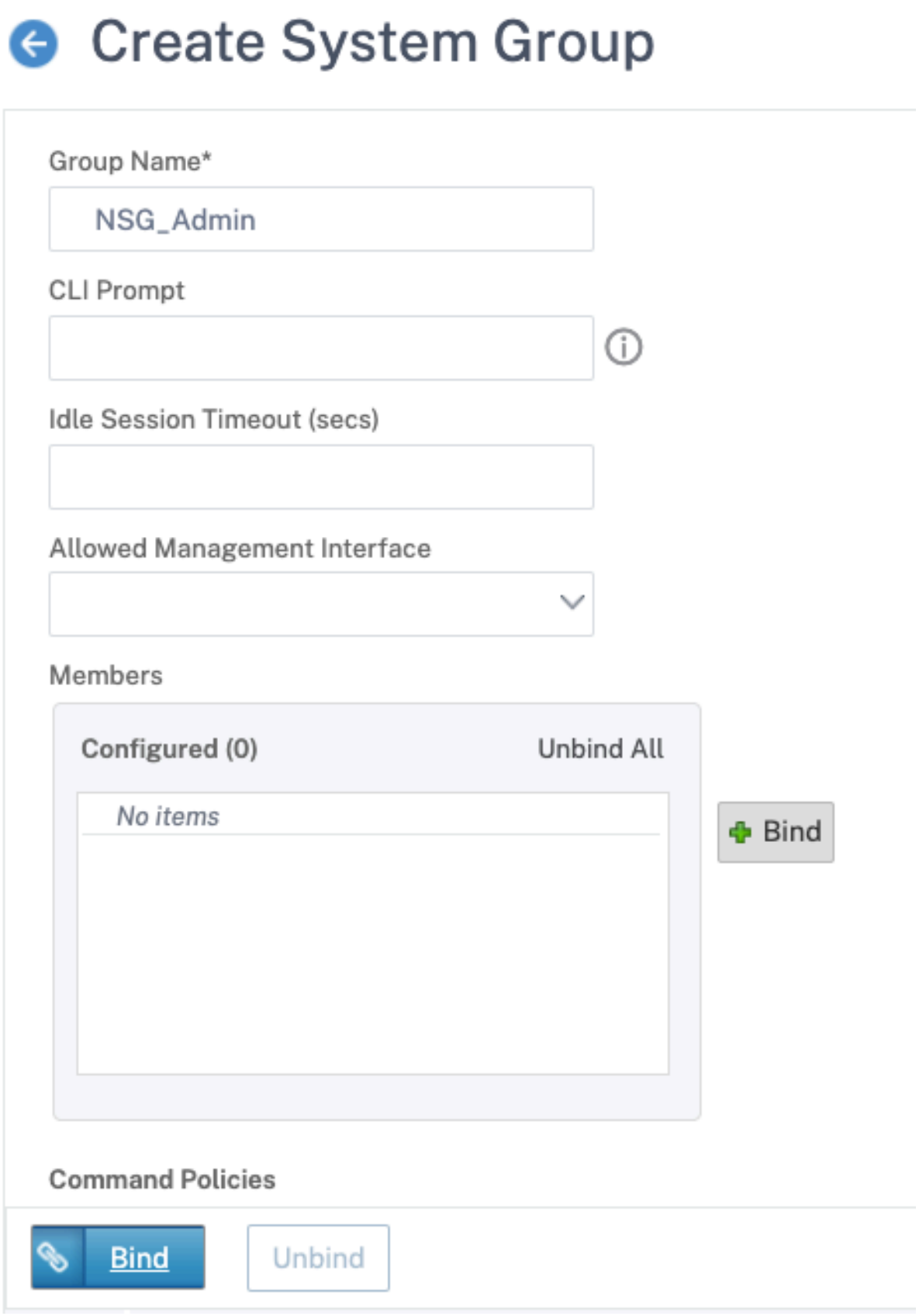
Sie können eine der beiden folgenden Optionen wählen.

- **Berechtigungen auf eine Gruppe anwenden:** Fügen Sie eine Gruppe in der Citrix ADC Appliance hinzu und weisen Sie jedem Benutzer, der Mitglied dieser Gruppe ist, dieselben Zugriffsrechte zu.
- **Wenden Sie Berechtigungen individuell für jeden Benutzer an:** Erstellen Sie jedes Benutzeradministratorkonto und weisen Sie jedem Benutzer Rechte zu.

Berechtigungen auf eine Gruppe anwenden

Wenn Sie Berechtigungen auf eine Gruppe anwenden, können Benutzer, die Mitglied der im Suchfilter konfigurierten Active Directory-Gruppe sind (in diesem Beispiel NSG_Admin), eine Verbindung zur Citrix ADC Management-Schnittstelle herstellen und über eine Superuser-Befehlsrichtlinie verfügen.

1. Navigieren Sie zu **System > Benutzerverwaltung > Gruppen**.
2. Geben Sie die Details gemäß der Anforderung ein und klicken Sie dann auf **Erstellen**.



Sie haben die Active Directory-Gruppe definiert, zu der die Benutzer gehören, und auch die Befehlsrichtlinienebene, die dem Konto bei der Anmeldung zugeordnet werden muss. Sie können der LDAP-Gruppe, die Sie im Suchfilter konfiguriert haben, neue Administratorbenutzer hinzufügen.

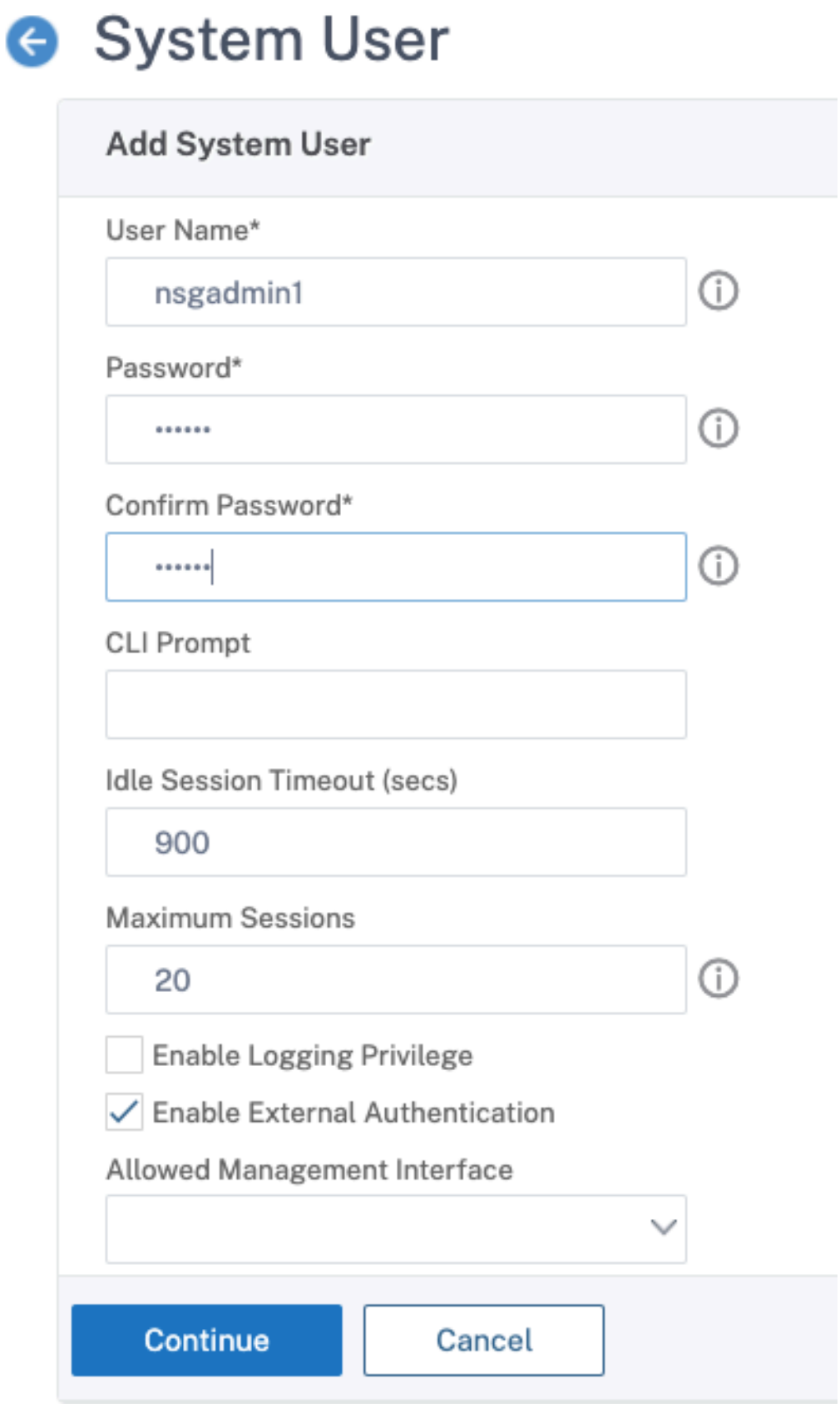
> **Hinweis:**
>
> Der Gruppenname muss mit dem Active Directory-Datensatz übereinstimmen.

Wenden Sie Berechtigungen für jeden Benutzer einzeln an

In diesem Szenario können Benutzer, die Mitglied Ihrer im Suchfilter konfigurierten Active Directory-Gruppe sind (in diesem Beispiel NSG_Admin), eine Verbindung zur Citrix ADC-Verwaltungsschnittstelle herstellen, haben jedoch keine Berechtigungen, bis Sie den bestimmten Benutzer auf der Citrix ADC Appliance erstellen und die Befehlsrichtlinie daran binden.

1. Navigieren Sie zu **System > Benutzeradministration > Benutzer**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie die Details gemäß der Anforderung ein.

   Hinweis: Achten Sie darauf, **Externe Authentifizierung aktivieren**auszuwählen.



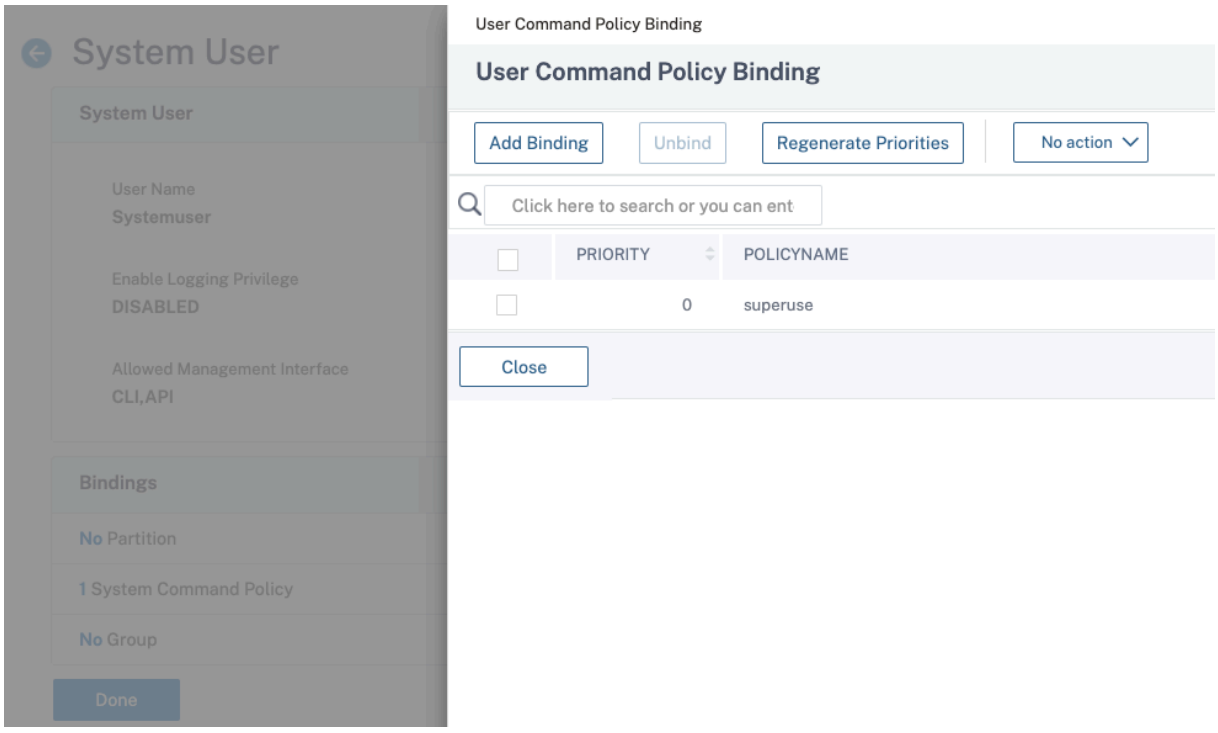
1. Klicken Sie auf **Weiter**.

Sie haben den Active Directory-Benutzer und die Befehlsrichtlinienebene definiert, die beim Anmelden mit dem Konto verknüpft werden müssen.

> **Hinweis:**
>
> - Der Benutzername muss mit dem Active Directory-Datensatz des vorhandenen Benutzers übereinstimmen.
> - Wenn Sie dem Citrix ADC einen Benutzer für die externe Authentifizierung hinzufügen, müssen Sie ein Kennwort angeben, falls die externe Authentifizierung nicht verfügbar ist. Damit die externe Authentifizierung ordnungsgemäß funktioniert, darf das interne Kennwort nicht mit dem LDAP-Kennwort des Benutzerkontos übereinstimmen.

Befehlsrichtlinie zum Benutzer hinzufügen

1. Navigieren Sie zu **System > Benutzeradministration > Benutzer**.
2. Wählen Sie den Benutzer aus, den Sie erstellt haben, und klicken Sie dann auf **Bearbeiten.**
3. Klicken Sie unter Bindungen auf **Systembefehlsrichtlinie**.
4. Wählen Sie die richtige Befehlsrichtlinie für Ihren Benutzer aus.
5. Klicken Sie auf **Binden**und dann auf **Schließen**.



Um weitere Administratoren hinzuzufügen;

- Fügen Sie die Administratorbenutzer der LDAP-Gruppe hinzu, die Sie im Suchfilter konfiguriert haben.

- Erstellen Sie den Systembenutzer in Citrix ADC und weisen Sie die richtige Befehlsrichtlinie zu.

So konfigurieren Sie die LDAP-Authentifizierung auf der Citrix ADC Appliance für Verwaltungszwecke mithilfe der CLI

Verwenden Sie die folgenden Befehle als Referenz, um die Anmeldung für eine Gruppe mit Superuser-Rechten auf der CLI der Citrix ADC Appliance zu konfigurieren.

1. Erstellen Sie einen LDAP-Server

```
add authentication ldapAction LDAP_mgmt -serverIP myAD.citrix.lab
    -serverPort 636 -ldapBase "DC=citrix,DC=lab" -ldapBindDn
    readonly@citrix.lab -ldapBindDnPassword -ldapLoginName
    sAMAccountName -searchFilter "&(memberof=CN=NSG_Admin,OU=
    AdminGroups,DC=citrix,DC=lab)" -groupAttrName memberOf
<!--NeedCopy-->
```

2. Richtlinie erstellen und LDAP

```
add authentication policy pol_LDAPmgmt -rule true -action
    LDAP_mgmt
<!--NeedCopy-->
```

3. Bindung der LDAP-Richtlinie

```
bind system global pol_LDAPmgmt -priority 110
<!--NeedCopy-->
```

4. Weisen Sie Ihren Administratoren Berechtigungen zu
   - So wenden Sie Berechtigungen auf die Gruppe an

```
add system group NSG_Admin
bind system group NSG_Admin -policyName superuser 100
<!--NeedCopy-->
```

   - So wenden Sie Berechtigungen für jeden Benutzer einzeln an


```
add system user admyoa
bind system user admyoa superuser 100
<!--NeedCopy-->
```

RADIUS-Authentifizierung

October 5, 2021

Wie bei anderen Typen von Authentifizierungsrichtlinien besteht eine RADIUS-Authentifizierungsrichtlinie (Remote Authentication Dial In User Service) aus einem Ausdruck und einer Aktion. Nachdem Sie eine Authentifizierungsrichtlinie erstellt haben, binden Sie sie an einen virtuellen Authentifizierungsserver und weisen ihm eine Priorität zu. Wenn Sie es binden, legen Sie es auch als primäre oder sekundäre Richtlinie fest. Das Einrichten einer RADIUS-Authentifizierungsrichtlinie hat jedoch bestimmte spezielle Anforderungen, die im Folgenden beschrieben werden.

Normalerweise konfigurieren Sie Citrix ADC für die Verwendung der IP-Adresse des Authentifizierungsservers während der Authentifizierung. Bei RADIUS-Authentifizierungsservern können Sie nun den ADC so konfigurieren, dass der FQDN des RADIUS-Servers anstelle seiner IP-Adresse zur Authentifizierung von Benutzern verwendet wird. Die Verwendung eines FQDN kann eine ansonsten viel komplexere Authentifizierungs-, Autorisierungs- und Überwachungskonfiguration in Umgebungen vereinfachen, in denen sich der Authentifizierungsserver möglicherweise an einer von mehreren IP-Adressen befindet, aber immer einen einzigen FQDN verwendet. Um die Authentifizierung mithilfe des FQDN eines Servers anstelle der IP-Adresse zu konfigurieren, führen Sie den normalen Konfigurationsprozess aus, außer wenn Sie die Authentifizierungsaktion erstellen. Beim Erstellen der Aktion ersetzen Sie den **ServerName-Parameter** durch den **ServerIP-Parameter** .

Bevor Sie entscheiden, ob Citrix ADC für die Verwendung der IP oder des FQDN des RADIUS-Servers zur Authentifizierung von Benutzern konfiguriert werden soll, sollten Sie berücksichtigen, dass das Konfigurieren von Authentifizierung, Autorisierung und Überwachung für die Authentifizierung bei einem FQDN anstelle einer IP-Adresse einen zusätzlichen Schritt zum Authentifizierungsprozess hinzufügt. Jedes Mal, wenn der ADC einen Benutzer authentifiziert, muss er den FQDN auflösen. Wenn sehr viele Benutzer versuchen, sich gleichzeitig zu authentifizieren, können die resultierenden DNS-Lookups den Authentifizierungsprozess verlangsamen.

> **Hinweis:**
>
> Diese Anweisungen gehen davon aus, dass Sie bereits mit dem RADIUS-Protokoll vertraut sind und Ihren gewählten RADIUS-Authentifizierungsserver bereits konfiguriert haben.

So fügen Sie mit der Befehlszeilenschnittstelle eine Authentifizierungsaktion für einen RADIUS-Server hinzu

Wenn Sie sich bei einem RADIUS-Server authentifizieren, müssen Sie eine explizite Authentifizierungsaktion hinzufügen. Geben Sie hierzu an der Eingabeaufforderung den folgenden Befehl ein:

```
add authentication radiusAction <name> [-serverip <IP> | -serverName] <
    FQDN>][-serverPort <port>] [-authTimeout <positive_integer>] {
 -radKey  }
  [-radNASip ( ENABLED | DISABLED )][-radNASid <string>] [-radVendorID
     <positive_integer>][-radAttributeType <positive_integer>][-
     radGroupsPrefix <string>] [-radGroupSeparator <string>][-
     passEncoding <passEncoding>][-ipVendorID <positive_integer>] [-
     ipAttributeType <positive_integer>][-accounting ( ON | OFF )][-
     pwdVendorID <positive_integer> [-pwdAttributeType <
     positive_integer>]] [-defaultAuthenticationGroup <string>] [-
     callingstationid ( ENABLED | DISABLED )]

<!--NeedCopy-->
```

Im folgenden Beispiel wird eine RADIUS-Authentifizierungsaktion mit dem Namen **Authn-Act-1**hinzugefügt, wobei die Server-IP **10.218.24.65**, der Serverport **1812**, das Authentifizierungszeitlimit **15**Minuten, der Radiusschlüssel **WareTheLorax**, NAS-IP deaktiviert und NAS-ID **NAS1**.

```
add authentication radiusaction Authn-Act-1 -serverip 10.218.24.65 -
    serverport 1812 -authtimeout 15 -radkey WareTheLorax -radNASip
    DISABLED -radNASid NAS1
Done

<!--NeedCopy-->
```

Im folgenden Beispiel wird dieselbe RADIUS-Authentifizierungsaktion hinzugefügt, wobei jedoch der Server-FQDN **rad01.example.com** anstelle der IP-Adresse verwendet wird.

```
add authentication radiusaction Authn-Act-1 -serverName rad01.example.
    com -serverport 1812 -authtimeout 15 -radkey WareTheLorax -radNASip
    DISABLED -radNASid NAS1
Done

```



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

So konfigurieren Sie eine Authentifizierungsaktion für einen externen RADIUS-Server mit der Befehlszeile

Um eine vorhandene RADIUS-Aktion zu konfigurieren, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set authentication radiusAction <name> [-serverip <IP> | -serverName] <
    FQDN>][-serverPort <port>] [-authTimeout <positive_integer>] {
 -radKey  }
  [-radNASip ( ENABLED | DISABLED )][-radNASid <string>] [-radVendorID
     <positive_integer>][-radAttributeType <positive_integer>][-
     radGroupsPrefix <string>] [-radGroupSeparator <string>][-
     passEncoding <passEncoding>][-ipVendorID <positive_integer>] [-
     ipAttributeType <positive_integer>][-accounting ( ON | OFF )][-
     pwdVendorID <positive_integer> [-pwdAttributeType <
     positive_integer>]] [-defaultAuthenticationGroup <string>] [-
     callingstationid ( ENABLED | DISABLED )]

<!--NeedCopy-->
```

So entfernen Sie eine Authentifizierungsaktion für einen externen RADIUS-Server mit der Befehlszeilenschnittstelle

Um eine vorhandene RADIUS-Aktion zu entfernen, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
rm authentication radiusAction <name>

<!--NeedCopy-->
```

Beispiel

```
rm authentication radiusaction Authn-Act-1
Done

<!--NeedCopy-->
```


So konfigurieren Sie einen RADIUS-Server mit dem Konfigurationsdienstprogramm

> **Hinweis:**
>
> Im Konfigurationsdienstprogramm wird der Termserver anstelle von Aktion verwendet, bezieht sich aber auf dieselbe Aufgabe.

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Radius**
2. Führen Sie im Detailbereich auf der Registerkarte **Server** eine der folgenden Aktionen aus:
   - Klicken Sie auf **Hinzufügen**, um einen neuen RADIUS-Server zu erstellen.
   - Um einen vorhandenen RADIUS-Server zu ändern, wählen Sie den Server aus, und klicken Sie dann auf **Bearbeiten**.
3. Geben Sie im Dialogfeld **Authentifizierungs-RADIUS-Server erstellen** oder **Authentifizierungs-RADIUS-Server konfigurieren** Werte für die Parameter ein oder wählen Sie sie aus. Um Parameter auszufüllen, die unter " **Anrufstation-ID senden**" angezeigt werden, erweitern Sie **Details**.
   - Name* — radiusActionName (Kann für eine zuvor konfigurierte Aktion nicht geändert werden)
   - Authentifizierungstyp * — authtype (auf RADIUS gesetzt, kann nicht geändert werden)
   - Servername/IP-Adresse* — Wählen Sie entweder den Servernamen oder die Server-IP.
     - Servername*—serverName <FQDN>
     - IP-Adresse* — ServerIP <IP> Wenn dem Server eine IPv6-IP-Adresse zugewiesen ist, aktivieren Sie das Kontrollkästchen IPv6.
   - Port*—serverPort
   - Timeout (Sekunden) *— authTimeout
   - Geheimschlüssel* — Radkey (RADIUS Shared Secret.)
   - Geheimen Schlüssel bestätigen* — Geben Sie den gemeinsam genutzten RADIUS-Schlüssel ein zweites Mal ein. (Keine Befehlszeilenäquivalent.)
   - Rufstellen-ID senden — callingstationid
   - Gruppen-Anbieter-Identifizierung—radVendorID
   - Gruppen-Attributtyp — radAttributeType
   - IP-Adresse Anbieter-Identifizierung—ipVendorID
   - pwdVendorID—pwdVendorID
   - Kennwort-Codierung — passEncoding

- Standardauthentifizierungsgruppe — defaultAuthenticationGroup
- NAS-ID — radNASid
- NAS-IP-Adressenextrahierung aktivieren — radNASip
- Gruppenpräfix — radGroupsPrefix
- Gruppentrennzeichen — radGroupSeparator
- IP-Adressattributtyp — ipAttributeType
- Kennwortattributtyp — pwdAttributeType
- Accounting—accounting

4. Klicken Sie auf **Erstellen** oder **OK**. Die von Ihnen erstellte Richtlinie wird auf der Seite Server angezeigt.

Unterstützung für die Durchleitung des RADIUS-Attributs 66 (Tunnel-Client-Endpunkt)

Die Citrix ADC Appliance ermöglicht nun die Durchleitung des RADIUS-Attributs 66 (Tunnel-Client-Endpunkt) während der RADIUS-Authentifizierung. Durch die Anwendung dieser Funktion wird die IP-Adresse des Clients von der zweiten Faktor-Authentifizierung empfangen, indem sie die risikobasierte Authentifizierungsentscheidung anvertraut.

Ein neues Attribut “TunnelEndPointClientIP” wird sowohl im Befehl “add authentication radiusAction” als auch im Befehl “set radiusParams” eingeführt.

Um dieses Feature zu verwenden, geben Sie an der Eingabeaufforderung der Citrix ADC Appliance Folgendes ein:

```
add authentication radiusAction <name> {
 -serverIP <ip_addr|ipv6_addr|*> | {
 -serverName <string> }
  }
  [-serverPort <port>] … [-tunnelEndpointClientIP (ENABLED|DISABLED)]

set radiusParams {
 -serverIP <ip_addr|ipv6_addr|*> |{
 -serverName <string> }
  }
  [-serverPort<port>] … [-tunnelEndpointClientIP(ENABLED|DISABLED)]

<!--NeedCopy-->
```

Beispiel


```
add authentication radiusAction radius -severIP 1.217.22.20 -serverName
     FQDN -serverPort 1812 -tunnelEndpointClientIp ENABLED

set radiusParams -serverIp 1.217.22.20 -serverName FQDN1 -serverPort
    1812 -tunnelEndpointClientIP ENABLED

<!--NeedCopy-->
```

Unterstützung für die Validierung der End-to-End-RADIUS-Authentifizierung

Die Citrix ADC Appliance kann jetzt die End-to-End-RADIUS-Authentifizierung über eine GUI überprüfen. Um diese Funktion zu validieren, wird eine neue Schaltfläche “Test” in GUI eingeführt. Ein Citrix ADC Appliance-Administrator kann diese Funktion nutzen, um folgende Vorteile zu erzielen:

- Konsolidiert den vollständigen Ablauf (Paket-Engine - aaa Daemon - externer Server), um eine bessere Analyse zu ermöglichen
- Verkürzt die Zeit bei der Überprüfung und Behebung von Problemen im Zusammenhang mit einzelnen Szenarien

Sie haben zwei Optionen zum Konfigurieren und Anzeigen der Testergebnisse der RADIUS-End-to-End-Authentifizierung mit der GUI.

Von Systemoption

1. Navigieren Sie zu **System > Authentifizierung > Grundlegende Richtlinien > RADIUS, und** klicken Sie auf die Registerkarte **Server**.
2. Wählen Sie die verfügbare **RADIUS-Aktion** aus der Liste aus.
3. Auf der Seite **Authentifizierungs-RADIUS-Server konfigurieren** haben Sie zwei Optionen im Abschnitt **Verbindungseinstellungen**.
4. Um die RADIUS-Serververbindung zu überprüfen, klicken Sie auf **RADIUS-Erreichbarkeit testen**.
5. Um die End-to-End-RADIUS-Authentifizierung anzuzeigen, klicken Sie auf **Endbenutzerverbindung testen** .

Von Authentifizierungsoption

1. Navigieren Sie zu **Authentifizierung > Dashboard**, und wählen Sie die verfügbare RADIUS-Aktion aus der Liste aus.
2. Auf der Seite **Authentifizierungs-RADIUS-Server konfigurieren** haben Sie zwei Optionen im Abschnitt **Verbindungseinstellungen**.

3. Um die RADIUS-Serververbindung zu überprüfen, klicken Sie auf **RADIUS-Erreichbarkeit testen**.
4. Um den End-to-End-RADIUS-Authentifizierungsstatus anzuzeigen, klicken Sie auf **Endbenutzerverbindung testen** .

TACACS-Authentifizierung

October 5, 2021

Die TACACS-Authentifizierungsrichtlinie authentifiziert sich bei einem externen Terminal Access Controller Access-Control System (TACACS) -Authentifizierungsserver.
Nachdem sich ein Benutzer bei einem TACACS-Server authentifiziert hat, stellt der Citrix ADC eine Verbindung mit demselben TACACS-Server für alle nachfolgenden Berechtigungen her. Wenn ein primärer TACACS-Server nicht verfügbar ist, verhindert diese Funktion Verzögerungen, während der ADC auf das Timeout des ersten TACACS-Servers wartet. Dies geschieht, bevor die Autorisierungsanforderung erneut an den zweiten TACACS-Server gesendet wird.

> **Hinweis:**
>
> Der TACACS-Autorisierungsserver unterstützt keine Befehle, deren Zeichenfolgenlänge 255 Zeichen überschreitet.
>
> **Problemumgehung:** Verwenden Sie die lokale Autorisierung anstelle eines TACACS-Autorisierungsservers.

Bei der Authentifizierung über einen TACACS-Server führen Authentifizierung, Autorisierung und Überwachung von Verkehrsmanagementprotokollen nur erfolgreich TACACS-Befehle aus. Es verhindert, dass die Protokolle TACACS-Befehle anzeigen, die von den Benutzern eingegeben wurden, die nicht autorisiert waren, sie auszuführen.

Ab NetScaler 12.0 Build 57.x blockiert das Terminal Access Controller Access Control System (TACACS) den Authentifizierungs-, Autorisierungs- und Auditing-Daemon beim Senden der TACACS-Anfrage nicht. Die erlauben LDAP- und RADIUS-Authentifizierung, mit der Anforderung fortzufahren. Die TACACS-Authentifizierungsanforderung wird fortgesetzt, sobald der TACACS-Server die TACACS-Anforderung bestätigt.

> **Wichtig:**
>
> - Citrix empfiehlt, keine TACACS-bezogenen Konfigurationen zu ändern, wenn Sie einen Befehl “clear ns config” ausführen.
> - TACACS bezogene Konfiguration in Bezug auf erweiterte Richtlinien wird gelöscht und erneut angewendet, wenn der Parameter “rbaConfig” im Befehl “clear ns config” für

> erweiterte Richtlinien auf NO gesetzt ist.

Name-Wert-Attribut-Unterstützung für die TACACS-Authentifizierung

Sie können nun TACACS Authentifizierungsattribute mit einem eindeutigen Namen zusammen mit Werten konfigurieren. Die Namen werden im Aktionsparameter TACACS konfiguriert und die Werte werden durch Abfrage der Namen ermittelt. Durch Angabe des Name-Attributwerts können Administratoren problemlos nach dem Attributwert suchen, der dem Attributnamen zugeordnet ist. Außerdem müssen sich Administratoren das Attribut nicht mehr allein nach seinem Wert merken.

> **Wichtig**
>
> - Im tacacsAction-Befehl können Sie maximal 64 durch Komma getrennte Attribute mit einer Gesamtgröße von weniger als 2048 Byte konfigurieren.

So konfigurieren Sie die Name-Wert-Attribute mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication tacacsAction <name> [-Attributes <string>]
<!--NeedCopy-->
```

Beispiel:

```
add authentication tacacsAction tacacsAct1 -attributes  “mail,sn,
   userprincipalName”
<!--NeedCopy-->
```

So fügen Sie mit der Befehlszeilenschnittstelle eine Authentifizierungsaktion hinzu

Wenn Sie keine LOCAL-Authentifizierung verwenden, müssen Sie eine explizite Authentifizierungsaktion hinzufügen. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
add authentication tacacsAction <name> -serverip <IP> [-serverPort <
   port>][-authTimeout <positive_integer>][ ... ]
<!--NeedCopy-->
```

Beispiel


```
add authentication tacacsaction Authn-Act-1 -serverip 10.218.24.65 -
    serverport 1812                  -authtimeout 15 -tacacsSecret ”
    minotaur” -authorization OFF -accounting ON -auditFailedCmds OFF -
    defaultAuthenticationGroup ”users”
<!--NeedCopy-->
```

So konfigurieren Sie eine Authentifizierungsaktion mit der Befehlszeilenschnittstelle

Um eine vorhandene Authentifizierungsaktion zu konfigurieren, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set authentication tacacsAction <name> -serverip <IP> [-serverPort <
    port>][-authTimeout <positive_integer>][ ... ]
<!--NeedCopy-->
```

Beispiel

```
     > set authentication tacacsaction Authn-Act-1 -serverip
        10.218.24.65 -serverport 1812                  -authtimeout 15
        -tacacsSecret ”minotaur” -authorization OFF -accounting ON -
        auditFailedCmds OFF -defaultAuthenticationGroup ”users”    Done
<!--NeedCopy-->
```

So entfernen Sie eine Authentifizierungsaktion mit der Befehlszeilenschnittstelle

Um eine vorhandene RADIUS-Aktion zu entfernen, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
rm authentication radiusAction <name>
<!--NeedCopy-->
```

Beispiel

```
rm authentication tacacsaction Authn-Act-1
<!--NeedCopy-->
```


Clientzertifikatauthentifizierung

May 10, 2022

Websites, die vertrauliche Inhalte enthalten, wie Online-Banking-Websites oder Websites mit persönlichen Daten von Mitarbeitern, benötigen manchmal Kundenzertifikate zur Authentifizierung. Um Authentifizierung, Autorisierung und Überwachung für die Authentifizierung von Benutzern basierend auf clientseitigen Zertifikatattributen zu konfigurieren, aktivieren Sie zunächst die Clientauthentifizierung auf dem virtuellen Verkehrsmanagementserver und binden das Stammzertifikat an den virtuellen Authentifizierungsserver. Dann implementieren Sie eine von zwei Optionen. Sie können den Standardauthentifizierungstyp auf dem virtuellen Authentifizierungsserver als CERT konfigurieren, oder Sie können eine Zertifikataktion erstellen, die definiert, was der Citrix ADC tun muss, um Benutzer basierend auf einem Clientzertifikat zu authentifizieren. In beiden Fällen muss Ihr Authentifizierungsserver CRLs unterstützen. Sie konfigurieren den ADC so, dass er den Benutzernamen aus dem Feld **subjectCN** oder einem anderen angegebenen Feld im Clientzertifikat extrahiert.

Wenn der Benutzer versucht, sich bei einem virtuellen Authentifizierungsserver anzumelden, für den keine Authentifizierungsrichtlinie konfiguriert ist, und eine globale Kaskade nicht konfiguriert ist, werden die Benutzernameninformationen aus dem angegebenen Feld des Zertifikats extrahiert. Wenn das erforderliche Feld extrahiert wird, ist die Authentifizierung erfolgreich. Stellt der Benutzer während des SSL-Handshakes kein gültiges Zertifikat zur Verfügung oder schlägt die Extraktion des Benutzernamens fehl, schlägt die Authentifizierung fehl. Nach der Validierung des Clientzertifikats zeigt der ADC dem Benutzer eine Anmeldeseite an.

Bei den folgenden Verfahren wird davon ausgegangen, dass Sie bereits eine funktionierende Authentifizierungs-, Autorisierungs- und Überwachungskonfiguration erstellt haben. Daher wird nur erläutert, wie die Authentifizierung mithilfe von Clientzertifikaten aktiviert wird. Bei diesen Verfahren wird auch davon ausgegangen, dass Sie Ihr Root-Zertifikat und Ihre Clientzertifikate erhalten und diese auf dem ADC im Verzeichnis /nsconfig/ssl abgelegt haben.

Konfigurieren der Clientzertifikatauthentifizierung

So konfigurieren Sie die Authentifizierungs-, Autorisierungs- und Auditing-Zertifikatsparameter des Clients über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein, um das Zertifikat zu konfigurieren und die Konfiguration zu überprüfen:


```
add ssl certKey <certkeyName> -cert <certFile> -key <keyFile> -password
    -inform <inform> -expiryMonitor <expiryMonitor> -notificationPeriod
    <notificationPeriod>

bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
   positive_integer>]

show ssl certKey [<certkeyName>]

set aaa parameter -defaultAuthType CERT

show aaa parameter

set aaa certParams -userNameField "Subject:CN"

show aaa certParams
<!--NeedCopy-->
```

So konfigurieren Sie die Authentifizierungs-, Autorisierungs- und Auditing-Clientzertifikatparameter mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server.**
2. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie für die Authentifizierung von Clientzertifikaten konfigurieren möchten, und klicken Sie dann auf **Bearbeiten.**
3. Klicken Sie auf der Seite **Konfiguration** unter **Certificates**auf den Rechtspfeil (>), um das CA Cert Key-Installationsdialogfeld zu öffnen.
4. Klicken Sie im Dialogfeld **CA Cert Key** auf **Insert.**
5. Klicken Sie im Dialogfeld **CA Cert Key — SSL Certificates** auf **Install.**
6. Legen **Sie im Dialogfeld Zertifikat installieren** die folgenden Parameter fest, deren Namen den CLI-Parameternamen entsprechen, wie in der Abbildung gezeigt:
   - Name des Zertifikatschlüsselpaars* — certkeyName
   - Dateiname des Zertifikats — certFile
   - Name der Schlüsseldatei — keyFile
   - Zertifikatsformat — inform
   - Kennwort — password
   - Zertifikatspaket — bundle
   - Bei Ablauf benachrichtigen — expiryMonitor
   - Meldezeitraum — notificationPeriod
7. Klicken Sie auf **Installieren**, und klicken Sie dann auf **Schließen**.
8. Wählen Sie im Dialogfeld **CA Cert Key** in der Liste **Certificate** das Stammzertifikat aus.
9. Klicken Sie auf **Speichern**.

10. Klicken Sie auf **Zurück**, um zum Hauptkonfigurationsbildschirm zurückzukehren.
11. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Authentifizierung > CERT**.
12. Wählen Sie im Detailbereich die Richtlinie aus, die Sie für die Authentifizierung von Clientzertifikaten konfigurieren möchten, und klicken Sie dann auf **Bearbeiten**.
13. Wählen **Sie im Dialogfeld Configure Authentication CERT Policy** in der Dropdownliste Server den virtuellen Server aus, den Sie für die Authentifizierung von Clientzertifikaten konfiguriert haben.
14. Klicken Sie auf **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Konfiguration erfolgreich abgeschlossen wurde.

Authentifizierung von Clientzertifikaten mithilfe erweiterter Richtlinien

Im Folgenden finden Sie die Schritte zum Konfigurieren der Clientzertifikatauthentifizierung auf Citrix ADC mithilfe erweiterter Richtlinien.

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie für die Authentifizierung von Clientzertifikaten konfigurieren möchten, und klicken Sie auf **Bearbeiten**.

   > **Hinweis:**
   >
   > Wenn Sie ein gültiges CA-Zertifikat und ein Serverzertifikat für den virtuellen Server importiert haben, können Sie **Schritt 3 bis Schritt 10**überspringen.

3. Klicken Sie auf der Seite **Configuration** unter **Certificates**auf ****, um das **CA Cert Key-Installationsdialogfeld** zu öffnen.
4. Klicken Sie im Dialogfeld **CA Cert Key** auf **Insert.**
5. Klicken Sie im Dialogfeld **CA Cert Key — SSL Certificates** auf **Install.**
6. Legen **Sie im Dialogfeld Zertifikat installieren** die folgenden Parameter fest, deren Namen den CLI-Parameternamen entsprechen, wie in der Abbildung gezeigt:
   - Name des Zertifikatschlüsselpaars — certKeyName
   - Dateiname des Zertifikats — certFile
   - Name der Schlüsseldatei — keyFile
   - Zertifikatsformat — inform
   - Kennwort — password
   - Zertifikatspaket — bundle
   - Bei Ablauf benachrichtigen — expiryMonitor
   - Meldezeitraum — notificationPeriod
7. Klicken Sie auf **Installieren**und dann auf Schließen.

8. Wählen Sie im Dialogfeld **CA Cert Key** in der Liste Certificate das Stammzertifikat aus.
9. Klicken Sie auf **Speichern**.
10. Klicken Sie auf **Zurück**, um zum Hauptkonfigurationsbildschirm zurückzukehren.
11. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien**, und wählen Sie dann **Richtlinie**aus.
12. Führen Sie im Detailbereich einen der folgenden Schritte aus:
    - Um eine neue Richtlinie zu erstellen, klicken Sie auf **Hinzufügen**.
    - Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus und klicken dann auf **Bearbeiten**.
13. Geben **Sie im Dialogfeld Authentifizierungsrichtlinie erstellen** oder **Authentifizierungsrichtlinie konfigurieren** Werte für die Parameter ein oder wählen Sie sie aus.
    - Name — Der Name der Richtlinie. Für eine zuvor konfigurierte Richtlinie kann nicht geändert werden.
    - Aktionstyp — Zertifikat auswählen
    - Aktion - Die Authentifizierungsaktion (Profil), die mit der Richtlinie verknüpft werden soll. Sie können eine vorhandene Authentifizierungsaktion auswählen oder auf das Plus klicken und eine neue Aktion des richtigen Typs erstellen.
    - Protokollaktion — Die mit der Richtlinie zu verknüpfen Überwachungsaktion. Sie können eine vorhandene Überprüfungsaktion auswählen oder auf das Plus klicken und eine neue Aktion erstellen.
    - Ausdruck — Die Regel, die Verbindungen auswählt, auf die Sie die angegebene Aktion anwenden möchten. Die Regel kann einfach (“wahr” wählt den gesamten Verkehr aus) oder komplex sein. Sie geben Ausdrücke ein, indem Sie zuerst den Ausdruckstyp in der Dropdownliste ganz links unter dem Ausdrucksfenster auswählen und dann Ihren Ausdruck direkt in den Ausdruckstextbereich eingeben, oder indem Sie auf Hinzufügen klicken, um das Dialogfeld Ausdruck hinzufügen zu öffnen, und die darin bezeichnenden Dropdownlisten verwenden, um Ihre Ausdruck.)
    - Kommentar - Sie können einen Kommentar eingeben, der die Art des Datenverkehrs beschreibt, für den diese Authentifizierungsrichtlinie gilt. Optional.
14. Klicken Sie auf **Erstellen** oder **OK**und dann auf **Schließen**. Wenn Sie eine Richtlinie erstellt haben, wird diese Richtlinie auf der Seite Authentifizierungsrichtlinien und Server angezeigt.

Passthrough für Clientzertifikate

Der Citrix ADC kann jetzt so konfiguriert werden, dass Clientzertifikate an geschützte Anwendungen weitergegeben werden, die Clientzertifikate für die Benutzerauthentifizierung benötigen. Der ADC au-

thentifiziert zuerst den Benutzer, fügt dann das Clientzertifikat in die Anforderung ein und sendet es an die Anwendung. Diese Funktion wird durch Hinzufügen geeigneter SSL-Richtlinien konfiguriert.

Das genaue Verhalten dieser Funktion, wenn ein Benutzer ein Clientzertifikat vorlegt, hängt von der Konfiguration des virtuellen VPN-Servers ab.

- Wenn der virtuelle VPN-Server so konfiguriert ist, dass er Clientzertifikate akzeptiert, diese aber nicht benötigt, fügt der ADC das Zertifikat in die Anforderung ein und leitet die Anfrage dann an die geschützte Anwendung weiter.
- Wenn auf dem virtuellen VPN-Server die Authentifizierung des Clientzertifikats deaktiviert ist, verhandelt der ADC das Authentifizierungsprotokoll neu und authentifiziert den Benutzer erneut, bevor er das Clientzertifikat in den Header einfügt und die Anforderung an die geschützte Anwendung weiterleitet.
- Wenn der virtuelle VPN-Server so konfiguriert ist, dass er eine Authentifizierung des Clientzertifikats erfordert, verwendet der ADC das Clientzertifikat, um den Benutzer zu authentifizieren, fügt dann das Zertifikat in den Header ein und leitet die Anforderung an die geschützte Anwendung weiter.

In all diesen Fällen konfigurieren Sie das Passthrough des Clientzertifikats wie folgt.

Erstellen und Konfigurieren des Passthrough für Clientzertifikate über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
1 add vpn vserver <name> SSL <IP> 443
2 <!--NeedCopy-->
```

Ersetzen Sie **Name** durch einen Namen für den virtuellen Server. Der Name muss aus einem bis 127 ASCII-Zeichen bestehen, beginnend mit einem Buchstaben oder Unterstrich (_) und nur Buchstaben, Zahlen und Unterstrich, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-). Ersetzen Sie <IP> durch die dem virtuellen Server zugewiesene IP-Adresse.

```
1 set ssl vserver <name> -clientAuth ENABLED -clientCert <clientcert>
2 <!--NeedCopy-->
```

Ersetzen Sie <name> durch den Namen des virtuellen Servers, den Sie erstellt haben. Ersetzen Sie <clientCert> durch einen der folgenden Werte:

- disabled — Deaktiviert die Authentifizierung des Clientzertifikats auf dem virtuellen VPN-Server.

- mandatory — konfiguriert den virtuellen VPN-Server so, dass Clientzertifikate für die Authentifizierung erforderlich sind.
- optional — konfiguriert den virtuellen VPN-Server so, dass er die Authentifizierung des Clientzertifikats zulässt, diese aber nicht erfordert.

```
1 bind vpn vserver <name> -policy local
2 <!--NeedCopy-->
```

Ersetzen Sie <name> durch den Namen des virtuellen VPN-Servers, den Sie erstellt haben.

```
1 bind vpn vserver <name> -policy cert
2 <!--NeedCopy-->
```

Ersetzen Sie <name> druch den Namen des virtuellen VPN-Servers, den Sie erstellt haben.

```
1 bind ssl vserver <name> -certkeyName <certkeyname>
2 <!--NeedCopy-->
```

Ersetzen Sie <name> durch den Namen des virtuellen Servers, den Sie erstellt haben. Ersetzen Sie <certkeyName> druch den Schlüssel des Clientzertifikats.

```
1 bind ssl vserver <name> -certkeyName <cacertkeyname> -CA -ocspCheck
     Optional
2 <!--NeedCopy-->
```

Ersetzen Sie <name> durch den Namen des virtuellen Servers, den Sie erstellt haben. Ersetzen Sie <cacertkeyName> durch den Schlüssel des CA-Zertifikats.

```
1 add ssl action <actname> -clientCert ENABLED -certHeader CLIENT-CERT
2 <!--NeedCopy-->
```

Ersetzen Sie <actname> durch einen Namen für die SSL-Aktion.

```
1 add ssl policy <polname> -rule true -action <actname>
2 <!--NeedCopy-->
```


Ersetzen Sie <polname> durch einen Namen für Ihre neue SSL-Richtlinie. Ersetzen Sie <actname> durch den Namen der SSL-Aktion, die Sie erstellt haben.

```
bind ssl vserver <name> -policyName <polname> -priority 10
<!--NeedCopy-->
```

Ersetzen Sie <name> durch den Namen des virtuellen VPN-Servers.

Beispiel

```
add vpn vserver vs-certpassthru SSL 10.121.250.75 443
set ssl vserver vs-certpassthru -clientAuth ENABLED -clientCert
    optional
bind vpn vserver vs-certpassthru -policy local
bind vpn vserver vs-certpassthru -policy cert
bind ssl vserver vs-certpassthru -certkeyName mycertKey
bind ssl vserver vs-certpassthru -certkeyName mycertKey -CA -ocspCheck
    Optional
add ssl action act-certpassthru -clientCert ENABLED -certHeader CLIENT-
    CERT
add ssl policy pol-certpassthru -rule true -action act-certpassthru
bind ssl vserver vs-certpassthru -policyName pol-certpassthru -priority
     10
<!--NeedCopy-->
```

Verhandeln der Authentifizierung

October 5, 2021

Wie bei anderen Typen von Authentifizierungsrichtlinien besteht eine Negotiate-Authentifizierungsrichtlinie aus einem Ausdruck und einer Aktion. Nachdem Sie eine Authentifizierungsrichtlinie erstellt haben, binden Sie sie an einen virtuellen Authentifizierungsserver und weisen ihm eine Priorität zu. Wenn Sie es binden, legen Sie es auch als primäre oder sekundäre Richtlinie fest.

Zusätzlich zu den Standardauthentifizierungsfunktionen kann der Befehl Aktion aushandeln nun Benutzerinformationen aus einer Keytab-Datei extrahieren, anstatt dass Sie diese Informationen manuell eingeben müssen. Wenn ein Keytab über mehr als einen SPN verfügt, wählt Authentifizierung, Autorisierung und Überwachung den richtigen SPN aus. Sie können diese Funktion in der Befehlszeile oder mit dem Konfigurationsdienstprogramm konfigurieren.

> **Hinweis:**
>
> Diese Anweisungen gehen davon aus, dass Sie bereits mit dem LDAP-Protokoll vertraut sind und Ihren gewählten LDAP-Authentifizierungsserver bereits konfiguriert haben.

So konfigurieren Sie Authentifizierung, Autorisierung und Überwachung, um Benutzerinformationen aus einer Keytab-Datei mit der Befehlszeilenschnittstelle zu extrahieren

Geben Sie an der Eingabeaufforderung den entsprechenden Befehl ein:

```
add authentication negotiateAction <name> {
 -domain <string> }
  {
 -domainUser <string> }
  {
 -domainUserPasswd  }
  [-defaultAuthenticationGroup <string>] [-keytab <string>] [-NTLMPath
     <string>]

set authentication negotiateAction <name> {
 -domain <string> }
  {
 -domainUser <string> }
  {
 -domainUserPasswd }
  [-defaultAuthenticationGroup <string>] [-keytab <string>] [-NTLMPath
     <string>]
<!--NeedCopy-->
```

Parameter description

- **name** - Name der zu verwendenden Verhandlungsaktion.
- **domain** - Domänenname des Dienstprinzipals, der Citrix ADC unterdrückt.
- **domainUser** - Benutzername des Kontos, das dem Citrix ADC Principal zugeordnet ist. Dies kann zusammen mit Domäne und Kennwort gegeben werden, wenn die Keytab-Datei nicht verfügbar ist. Wenn der Benutzername zusammen mit der keytab-Datei angegeben wird, wird diese keytab-Datei nach den Anmeldeinformationen dieses Benutzers durchsucht. Maximale Länge: 127
- **domainUserPassWD** - Kennwort des Kontos, das dem Citrix ADC-Prinzipal zugeordnet ist.

- **DefaultAuthenticationGroup** - Dies ist die Standardgruppe, die ausgewählt wird, wenn die Authentifizierung zusätzlich zu den extrahierten Gruppen erfolgreich ist. Maximale Länge: 63
- **keytab** - Der Pfad zur Keytab-Datei, die zum Entschlüsseln von Kerberos-Tickets verwendet wird, die Citrix ADC präsentiert werden. Wenn keytab nicht verfügbar ist, kann in der Konfiguration der Verhandlungsaktion domain/username/password angegeben werden. Maximale Länge: 127
- **ntlmPath** - Der Pfad zu der Site, die für die NTLM-Authentifizierung aktiviert ist, einschließlich FQDN des Servers. Dies wird bei einem Clientfallback auf NTLM verwendet. Maximale Länge: 127

So konfigurieren Sie Authentifizierung, Autorisierung und Überwachung, um Benutzerinformationen aus einer Keytab-Datei mit dem Konfigurationsdienstprogramm zu extrahieren

> Hinweis:
>
> Im Konfigurationsdienstprogramm wird der Termserver anstelle von Aktion verwendet, bezieht sich aber auf dieselbe Aufgabe.

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Authentifizierung > Erweiterte Richtlinien > Aktionen > NEGOTIATE-Aktionen**.
2. Führen Sie im Detailbereich auf der Registerkarte **Server** eine der folgenden Aktionen aus:
   - Wenn Sie eine neue **Verhandlungsaktion** erstellen möchten, klicken Sie auf **Hinzufügen**.
   - Wenn Sie eine vorhandene **Verhandlungsaktion** ändern möchten, wählen Sie im Datenbereich die Aktion aus, und klicken Sie dann auf **Bearbeiten**.
3. Wenn Sie eine neue **Verhandlungsaktion** erstellen, geben Sie im Textfeld **Name** einen Namen für die neue Aktion ein. Der Name kann von einem bis 127 Zeichen lang sein und kann aus Groß- und Kleinbuchstaben, Zahlen sowie Bindestrich (-) und Unterstrich (_) bestehen. Wenn Sie eine vorhandene Verhandlungsaktion ändern, überspringen Sie diesen Schritt. Der Name ist schreibgeschützt. Sie können ihn nicht ändern.
4. Aktivieren Sie es unter **Negotiate**, wenn das Kontrollkästchen Keytab-Datei verwenden noch nicht aktiviert ist.
5. Geben Sie im Textfeld Keytab-Dateipfad den vollständigen Pfad und den Dateinamen der Keytab-Datei ein, die Sie verwenden möchten.
6. Geben Sie im Textfeld Standardauthentifizierungsgruppe die Authentifizierungsgruppe ein, die Sie als Standard für diesen Benutzer festlegen möchten.
7. Klicken Sie auf **Erstellen** oder **OK**, um die Änderungen zu speichern.

Punkte zu beachten, wann erweiterte Verschlüsselungen für die Kerberos-Authentifizierung verwendet werden

- **Beispielkonfiguration bei Verwendung von Keytab:** add authentication negotiateAction neg_act_aes256 -keytab “/nsconfig/krb/lbvs_aes256.keytab”
- **Verwenden Sie den folgenden Befehl, wenn keytab mehrere Verschlüsselungstypen hat.** Der Befehl erfasst zusätzlich Domänenbenutzerparameter: add authentication negotiateAction neg_act_keytab_all -keytab “/nsconfig/krb/lbvs_all.keytab” -domainUser “http/lbvs.aaa.local”
- **Verwenden Sie die folgenden Befehle, wenn Benutzeranmeldeinformationen verwendet werden:** add authentication negotiateAction neg_act_user -domain AAA.LOCAL -domainUser “http/lbvs.aaa.local” -domainUserPasswd <password>
- Stellen Sie sicher, dass die richtigen **domainUser**-Informationen bereitgestellt werden. Sie können in AD nach dem Anmeldenamen des Benutzers suchen.

Web-Authentifizierung

October 5, 2021

Authentifizierung, Autorisierung und Überwachung können nun einen Benutzer bei einem Webserver authentifizieren, indem die Anmeldeinformationen bereitgestellt werden, die der Webserver in einer HTTP-Anforderung benötigt, und die Webserverantwort analysiert wird, um festzustellen, dass die Benutzerauthentifizierung erfolgreich war. Wie bei anderen Typen von Authentifizierungsrichtlinien besteht eine Webauthentifizierungsrichtlinie aus einem Ausdruck und einer Aktion. Nachdem Sie eine Authentifizierungsrichtlinie erstellt haben, binden Sie sie an einen virtuellen Authentifizierungsserver und weisen ihm eine Priorität zu. Wenn Sie es binden, legen Sie es auch als primäre oder sekundäre Richtlinie fest.

Um die webbasierte Authentifizierung mit einem bestimmten Webserver einzurichten, erstellen Sie zunächst eine Webauthentifizierungsaktion. Da die Authentifizierung bei Webservern kein starres Format verwendet, müssen Sie beim Erstellen der Aktion genau angeben, welche Informationen der Webserver benötigt und in welchem Format benötigt. Dazu erstellen Sie einen Ausdruck in der Standardsyntax der Citrix ADC Appliance, der die folgenden Elemente enthält:

- **Server-IP**— Die IP-Adresse des Authentifizierungswebservers.
- **Serverport**— Der Port des Authentifizierungswebservers.
- **Authentifizierungsregel**— Ein Ausdruck in der Standardsyntax der Citrix ADC Appliance, der die Anmeldeinformationen des Benutzers in dem vom Webserver erwarteten Format enthält.
- **Schema**— HTTP (für unverschlüsselte Webauthentifizierung) oder HTTPS (für verschlüsselte Webauthentifizierung).

- **Erfolgsregel**— Ein Ausdruck in der Standardsyntax der Citrix ADC Appliance, der mit der Antwortzeichenfolge des Webservers übereinstimmt, die angibt, dass der Benutzer erfolgreich authentifiziert wurde.

Befolgen Sie für alle anderen Parameter die normalen Regeln für den Befehl Authentifizierungsaktion hinzufügen.

Als Nächstes erstellen Sie eine Richtlinie, die dieser Aktion zugeordnet ist. Die Richtlinie ähnelt einer LDAP-Richtlinie, und wie LDAP-Richtlinien verwendet die Citrix ADC Appliance-Syntax.

> **Hinweis:**
>
> Diese Anweisungen gehen davon aus, dass Sie bereits mit den Authentifizierungsanforderungen der Webserver, auf denen Sie sich authentifizieren möchten, vertraut sind und den Webauthentifizierungsserver bereits konfiguriert haben.

So konfigurieren Sie eine Webauthentifizierungsaktion mit der Befehlszeilenschnittstelle

Um eine Webauthentifizierungsaktion in der Befehlszeile zu erstellen, geben Sie in der Befehlszeile den folgenden Befehl ein:

```
1 add authentication webAuthAction <name> -serverIP <ip_addr|ipv6_addr
    |\*> -serverPort <port|\*> [-fullReqExpr <string>] -scheme ( http |
    https ) -successRule <expression> [-defaultAuthenticationGroup <
    string>][-Attribute1 <string>][-Attribute2 <string>] [-Attribute3 <
    string>][-Attribute4 <string>] [-Attribute5 <string>][-Attribute6 <
    string>] [-Attribute7 <string>][-Attribute8 <string>] [-Attribute9 <
    string>][-Attribute10 <string>] [-Attribute11 <string>][-Attribute12
     <string>] [-Attribute13 <string>][-Attribute14 <string>] [-
    Attribute15 <string>][-Attribute16 <string>]
2 <!--NeedCopy-->
```

Beispiel

```
1 add policy expression post_data ""username=" + http.REQ.BODY(1000).
    SET_TEXT_MODE(IGNORECASE).AFTER_STR("login=").BEFORE_STR("&") + "&
    passwort=" + http.REQ.BODY(1000).SET_TEXT_MODE(IGNORECASE).AFTER_STR
    ("passwd=")"
2
3 add policy expression length_post_data "("username= " + http.REQ.BODY
    (1000).SET_TEXT_MODE(IGNORECASE).AFTER_STR("login=").BEFORE_STR("&")
```



```
      + "passwort=" + http.REQ.BODY(1000).SET_TEXT_MODE(IGNORECASE).
     AFTER_STR("passwd=")).length"
4
5 add authentication webAuthAction webAuth_POST -serverIP 10.106.187.54 -
     serverPort 80 -fullReqExpr q{
6  "POST /MyPHP/auth.php HTTP/" + http.req.version.major + "." + http.req
     .version.major + "\r\nAccept:\*/\*\r\nHost: 10.106.187.54\r\
     nReferer: http://10.106.187.54/MyPHP/auth.php\r\nAccept-Language:
     en-US\r\nUser-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT
     6.1; Trident/5.0)\r\nContent-Type: application/x-www-form-
     urlencoded\r\n" + "Content-Length: " + length_post_data + "\r\
     nConnection: Keep-Alive\r\n\r\n" + post_data }
7   -scheme http -successRule "http.res.status.eq(200)"
8 <!--NeedCopy-->
```

So konfigurieren Sie eine Webauthentifizierungsaktion mit dem Konfigurationsdienstprogramm

> **Hinweis:**
>
> Im Konfigurationsdienstprogramm wird der Termserver anstelle von Aktion verwendet, bezieht sich aber auf dieselbe Aufgabe.

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Richtlinien > LDAP**.
2. Führen Sie im Detailbereich auf der Registerkarte **Server** eine der folgenden Aktionen aus:
   - Wenn Sie eine neue Webauthentifizierungsaktion erstellen möchten, klicken Sie auf **Hinzufügen**.
   - Wenn Sie eine vorhandene Webauthentifizierungsaktion ändern möchten, wählen Sie im Datenbereich die Aktion aus, und klicken Sie dann auf **Bearbeiten**.
3. Wenn Sie eine neue Webauthentifizierungsaktion erstellen, geben Sie im Dialogfeld **Authentifizierungswebserver erstellen** im Textfeld **Name** einen Namen für die neue Webauthentifizierungsaktion ein. Der Name kann von einem bis 127 Zeichen lang sein und kann aus Groß- und Kleinbuchstaben, Zahlen sowie Bindestrich (-) und Unterstrich (_) bestehen. Wenn Sie eine vorhandene Webauthentifizierungsaktion ändern, überspringen Sie diesen Schritt. Der Name ist schreibgeschützt. Sie können ihn nicht ändern.
4. Geben Sie im Textfeld **IP-Adresse des Webservers** die IPv4- oder IPv6-IP-Adresse des Authentifizierungswebservers ein. Wenn es sich bei der Adresse um eine IPv6-IP-Adresse handelt, aktivieren Sie zuerst das Kontrollkästchen IPv6.
5. Geben Sie im Textfeld Port die Portnummer ein, auf der der Webserver Verbindungen akzeptiert.
6. Wählen Sie **HTTP** oder **HTTPS** in der Dropdownliste **Protokoll** aus.

7. Geben Sie im Textbereich HTTP-Anforderungsausdruck einen regulären Ausdruck im PCRE-Format ein, der die Webserveranforderung erstellt, die die Anmeldeinformationen des Benutzers im genauen Format enthält, das vom Authentifizierungswebserver erwartet wird.
8. Geben Sie im Textbereich Ausdruck zum Überprüfen der Authentifizierung einen Standardsyntax der Citrix ADC Appliance ein, der die Informationen in der Webserverantwort beschreibt, die angibt, dass die Benutzerauthentifizierung erfolgreich war.
9. Füllen Sie die verbleibenden Felder aus, wie in der Dokumentation zur allgemeinen Authentifizierungsaktion beschrieben.
10. Klicken Sie auf **OK**.

SMS Zwei-Faktor-Authentifizierung mit Webauthentifizierung

June 1, 2022

Citrix ADC kann jetzt in einen SMS-Anbieter eines Drittanbieters integriert werden, um eine zusätzliche Authentifizierungsebene bereitzustellen.

Die Citrix ADC Appliance kann so konfiguriert werden, dass ein OTP auf dem Handy des Benutzers als zweiten Authentifizierungsfaktor gesendet wird. Die Appliance legt dem Benutzer ein Anmeldeformular zur Eingabe des OTP nach erfolgreicher AD-Anmeldung vor. Erst nach der erfolgreichen Validierung der SMS-OTP-Authentifizierung wird dem Benutzer die angeforderte Ressource angezeigt.

Um die SMS-OTP-Authentifizierung zu erreichen, stützt sich die Citrix ADC Appliance auf die folgenden Faktoren im Backend.

1. Authentifizieren Sie den Benutzer über die LDAP-Authentifizierung und extrahieren Sie die Handynummer des Benutzers.
2. Erstellen Sie OTP und speichern Sie es in der NS-Variablen. Konfiguration und Verwendung von Variablen.
3. Senden Sie das OTP über die WebAuth-Authentifizierungsmethode an die aus LDAP extrahierte Handynummer.
4. Validieren Sie das OTP.

Voraussetzungen

OTP Store konfigurieren

Administratoren richten eine Datenbank/einen Store ein, um OTPs zu speichern, die für die SMS-Authentifizierung verwendet werden, indem sie den folgenden CLI-Befehl verwenden.


```
add ns variable otp_store -type "map(text(65),text(6),100000)" -
    ifValueTooBig undef -ifNoValue undef -expires 5
<!--NeedCopy-->
```

Generieren Sie zufälliges OTP pro Benutzersitzung

Verwenden Sie den folgenden Befehl, um ein 6-stelliges zufälliges OTP pro Benutzersitzung zu generieren und im OTP-Store zu speichern.

```
add ns assignment generate_otp -variable "$otp_store[AAA.USER.SESSIONID
    ]" -set ("000000" + SYS.RANDOM.MUL(1000000).
    TYPECAST_UNSIGNED_LONG_AT.TYPECAST_TEXT_T).SUFFIX(6)
<!--NeedCopy-->
```

Konfigurieren Sie die SMS-OTP-Authentifizierung mit Citrix ADC

- Bevor Sie die Funktion zur Zwei-Faktor-Authentifizierung von SMS-Zwei-Faktor-Authentifizierung konfigurieren, müssen Sie eine LDAP-Authentifizierung auf einer Citrix ADC Appliance als ersten Faktor bei aktivierter Authentifizierung konfiguriert haben. Anweisungen zum Konfigurieren der LDAP-Authentifizierung finden Sie unter So konfigurieren Sie die LDAP-Authentifizierung mit dem Konfigurationsdienstprogramm.
- Konfigurieren Sie LDAP und extrahieren Sie die Handynummer, die für die SMS-OTP-Authentifizierung verwendet werden soll.

Beispielkonfiguration für den ersten Faktor

```
add authentication ldapAction ldap_action -serverIP 1.1.1.1 -serverPort
     3268 -authTimeout 30 -ldapBase "dc=nsi-test,dc=com" -ldapBindDn
    Administrator@nsi-test.com -ldapBindDnPassword freebsd -
    ldapLoginName samaccountname -groupAttrName memberOf -
    ssoNameAttribute samaccountname  -Attribute1 mobile -email mail

add authentication Policy ldap_policy -rule true -action ldap_action
<!--NeedCopy-->
```

> **Hinweis**
>
> Die Handynummer kann mit AAA.USER.ATTRIBUTE (1) extrahiert und beim Senden an den

> Backend-Server einbezogen werden.

Beispielkonfiguration für den zweiten Faktor

Mit der folgenden Beispielkonfiguration wird ein OTP generiert, das an den Endbenutzer gesendet werden soll.

```
add authentication Policy set_otp -rule true -action generate_otp

add authentication policylabel set_otp -loginSchema LSCHEMA_INT

add authentication policy cascade_noauth -rule true -action NO_AUTHN

bind authentication policylabel set_otp -policyName set_otp -priority 1
    -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

Beispielkonfiguration für einen dritten Faktor

Unter Verwendung der folgenden Beispielkonfiguration wird das in der Konfiguration des zweiten Faktors generierte OTP mithilfe der Webauthentifizierungsmethode an den Endbenutzer gesendet. Einzelheiten zur Webauthentifizierung finden Sie unter Webauthentifizierung.

- Beispiel einer Webauthentifizierungskonfiguration, wenn der SMS-Server die API über die GET-Methode verfügbar

```
add policy expression otp_exp_get ""method=sendMessage&send_to="
    + AAA.USER.ATTRIBUTE(1) + "&msg=OTP is " + $otp_store[AAA.USER
    .SESSIONID] + "for login into secure access  gateway. Valid
    till EXPIRE_TIME. Do not share the OTP with anyone for
    security reasons.&userid=######&password=###=1.0""

add authentication webAuthAction webAuth_Get -serverIP
    10.106.168.210 -serverPort 8080 -fullReqExpr q{
"GET /GatewayAPI/rest?" + otp_exp_get + "HTTP/" + http.req.
    version.major + "." + http.req.version.minor.sub(1) + "\r\
    nAccept:\*/\*\r\nHost: <FQDN>\r\n" }
 -successRule "http.res.status.eq(200)" -scheme http
<!--NeedCopy-->
```


- Beispiel einer Webauthentifizierungskonfiguration, wenn der SMS-Server die API über die GET-Methode verfügbar

```
add policy expression otp_exp_post ""Message: OTP is " +
    $otp_store[AAA.USER.SESSIONID] + "for login into secure access
      gateway. Valid till EXPIRE_TIME. Do not share the OTP with
    anyone for security reasons&Mobile:" + AAA.USER.ATTRIBUTE(1)"

add authentication webAuthAction webAuth_POST -serverIP
    10.106.168.210 -serverPort 8080 -fullReqExpr q{
"POST /MyPHP/auth.php HTTP/" + http.req.version.major + "." +
    http.req.version.major + "\r\nAccept:\*/\*\r\nHost:
    10.106.168.210 \r\nContent-Length: 10\r\n\r\n" + otp_exp_post
    }
 -scheme http -successRule true
<!--NeedCopy-->
```

```
add authentication webAuthAction webAuth_Get -serverIP
    10.106.168.210 -serverPort 8080 -fullReqExpr q{
"GET /GatewayAPI/rest?" + otp_exp_get + "HTTP/" + http.req.
    version.major + "." + http.req.version.minor.sub(1) + "\r\
    nAccept:/\r\nHost: <FQDN>\r\n" }
 -successRule "http.res.status.eq(200)" -scheme http

add policy expression otp_exp_post "$otp_store[AAA.USER.SESSIONID
    ]"
<!--NeedCopy-->
```

- Senden Sie abschließend das OTP.

```
add authentication Policy wpp -rule true -action webAuth_POST

add authentication policylabel send_otp -loginSchema LSCHEMA_INT
bind authentication policylabel send_otp -policyName wpp -
    priority 1 -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

Beispielkonfiguration für den vierten Faktor

Überprüfen Sie anhand der folgenden Beispielkonfiguration das an den Endbenutzer gesendete OTP.

In dieser Konfiguration wird eine Richtlinienregel verwendet, um das OTP anhand des OTP zu validieren, das an den Endbenutzer gesendet wird.

```
add authentication Policy otp_verify -rule ”AAA.LOGIN.PASSWORD.EQ(
    $otp_store[AAA.USER.SESSIONID])” -action NO_AUTHN

add authentication policylabel otp_verify -loginSchema onlyPassword

bind authentication policylabel otp_verify -policyName otp_verify -
    priority 1 -gotoPriorityExpression NEXT

<!--NeedCopy-->
```

Verwenden Sie den folgenden Befehl, um das OnlyPassword-Anmeldeschema hinzuzufügen:

```
add authentication loginSchema onlypassword -authenticationschema /
    nsconfig/loginschema/LoginSchema/OnlyPassword.xml”
<!--NeedCopy-->
```

Verknüpfen Sie alle Faktoren für eine erfolgreiche SMS-OTP-Authentifizierung

Verwenden Sie die folgenden CLI-Befehle, um alle Faktoren miteinander zu verknüpfen.

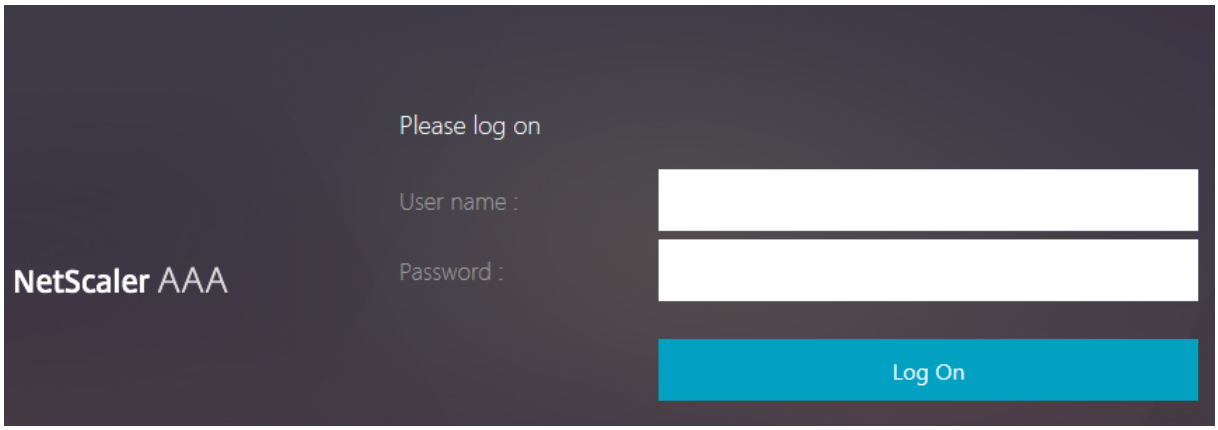
```
bind authentication policylabel send_otp -policyName wpp -priority 1 -
    gotoPriorityExpression NEXT -nextFactor otp_verify
<!--NeedCopy-->
```

> **Hinweis:**
>
> Die Richtlinie für die kaskadierende Authentifizierung wurde hinzugefügt, um eine zuverlässige und kontinuierliche Authentifizierung für die Endbenutzer zu ermöglichen. Wenn der aktuelle Faktor ausfällt, wird der nächste Faktor so bewertet, dass das Benutzererlebnis nicht beeinträchtigt wird.

Formularbasierte Authentifizierung

October 5, 2021

Bei der formularbasierten Authentifizierung wird dem Endbenutzer ein Anmeldeformular angezeigt. Diese Art von Authentifizierungsformular unterstützt sowohl die Multifaktor-Authentifizierung (nFactor) als auch die klassische Authentifizierung.



Stellen Sie sicher, dass die formularbasierte Authentifizierung funktioniert:

- Auf dem virtuellen Lastausgleichsserver muss die Authentifizierung **eingeschaltet**sein.
- Der Parameter 'AuthenticationHost' muss angegeben werden, an den der Benutzer zur Authentifizierung umgeleitet werden muss. Der Befehl zum Konfigurieren des gleichen lautet wie folgt:

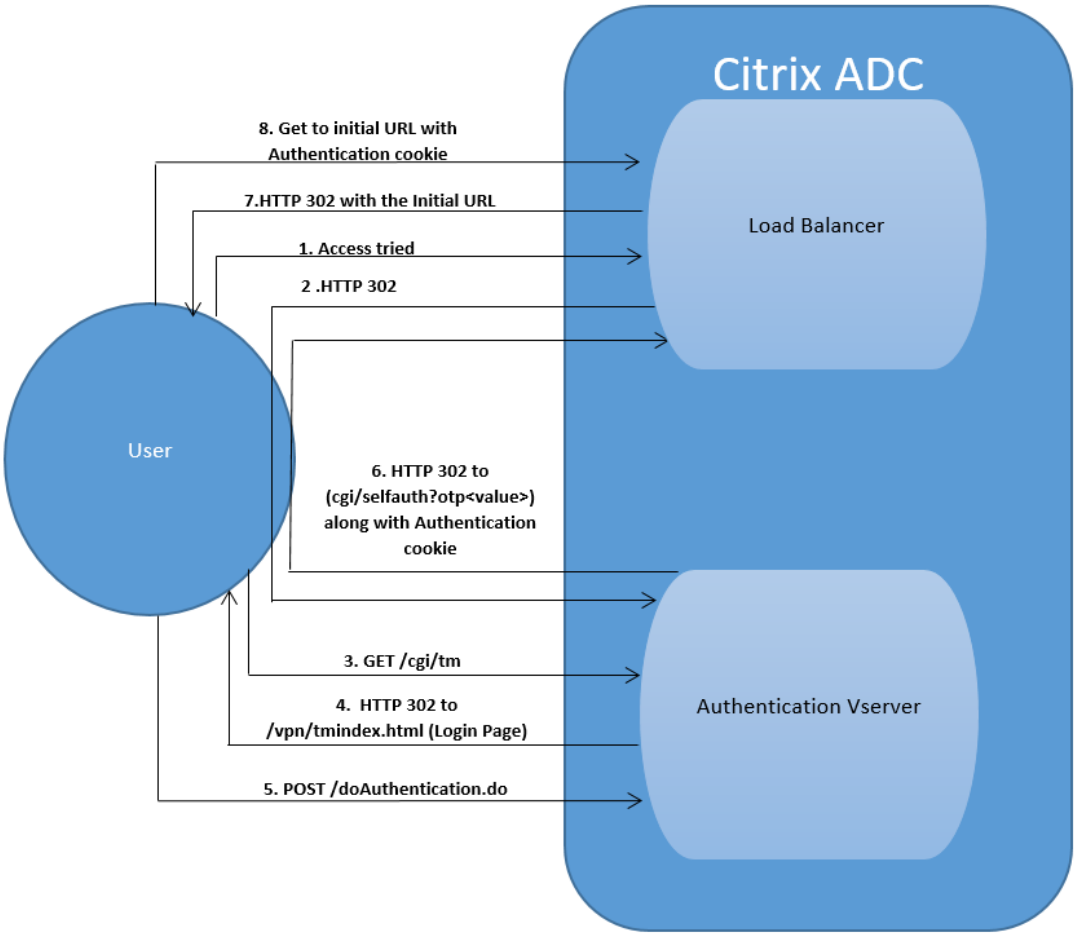
```
1  set lb vs lb1 -authentication on  - authenticationhost aaavs-ip/
      fqdn
```

- Die formularbasierte Authentifizierung ist mit einem Browser kompatibel, der HTML unterstützt

In den folgenden Schritten wird erläutert, wie die formularbasierte Authentifizierung funktioniert:

1. Der Client (Browser) sendet eine GET-Anforderung für eine URL auf dem virtuellen TM-Server (Load Balancing/CS).
2. Der virtuelle TM-Server ermittelt, dass der Client nicht authentifiziert wurde, und sendet eine HTTP 302-Antwort an den Client. Die Antwort enthält ein verstecktes Skript, das bewirkt, dass der Client eine GET-Anforderung für /cgi/tm an den virtuellen Authentifizierungsserver ausgibt.
3. Der Client sendet GET /cgi/tm mit der Ziel-URL an den virtuellen Authentifizierungsserver.
4. Der virtuelle Authentifizierungsserver sendet eine Umleitung an die Anmeldeseite.
5. Der Benutzer sendet seine Anmeldeinformationen mit POST /DoAuthentication.do an den virtuellen Authentifizierungsserver. Die Authentifizierung erfolgt durch den virtuellen Authentifizierungsserver.
6. Wenn die Anmeldeinformationen korrekt sind, sendet der virtuelle Authentifizierungsserver eine HTTP 302-Antwort an die cgi/selfauth-URL auf dem Lastausgleichsserver mit einem One-Token (OTP).

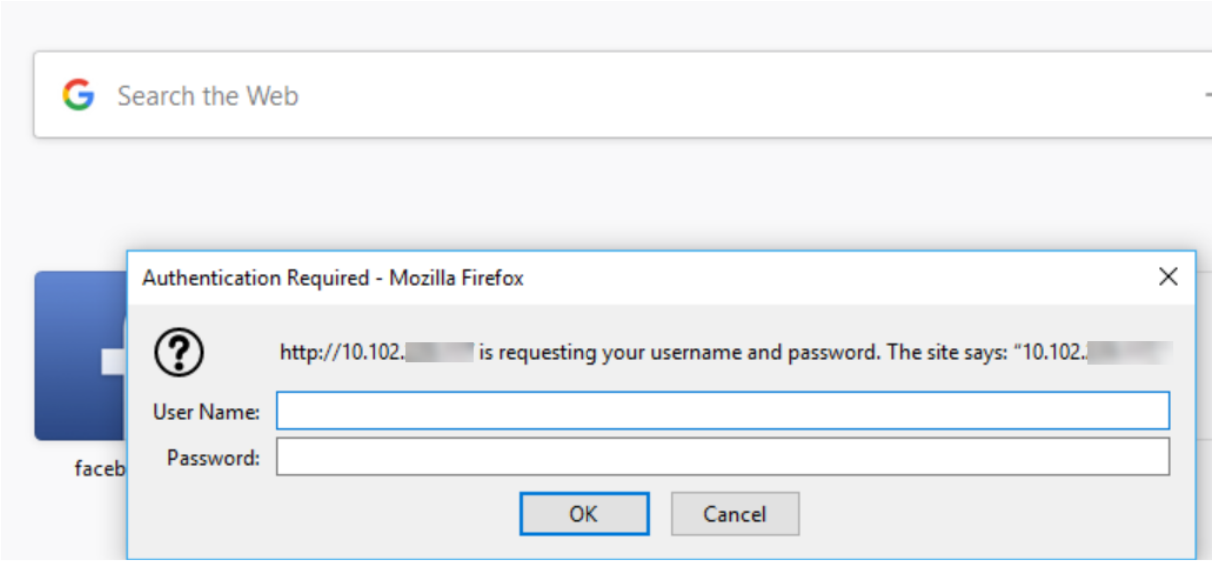
7. Der Lastausgleichsserver sendet HTTP 302 an den Client.
8. Der Client sendet eine GET-Anforderung für ihre ursprüngliche URL-Ziel-URL zusammen mit einem 32-Byte-Cookie.



401-basierte Authentifizierung

May 10, 2022

Mit der 401-basierten Authentifizierung zeigt die Citrix ADC-Appliance dem Endbenutzer ein Popup-Dialogfeld an.



Das formularbasierte AAA-TM arbeitet mit den Umleitungsnachrichten. Einige Anwendungen unterstützen jedoch keine Weiterleitungen. In solchen Anwendungen wird 401-Authentifizierung aktiviertes AAA-TM verwendet.

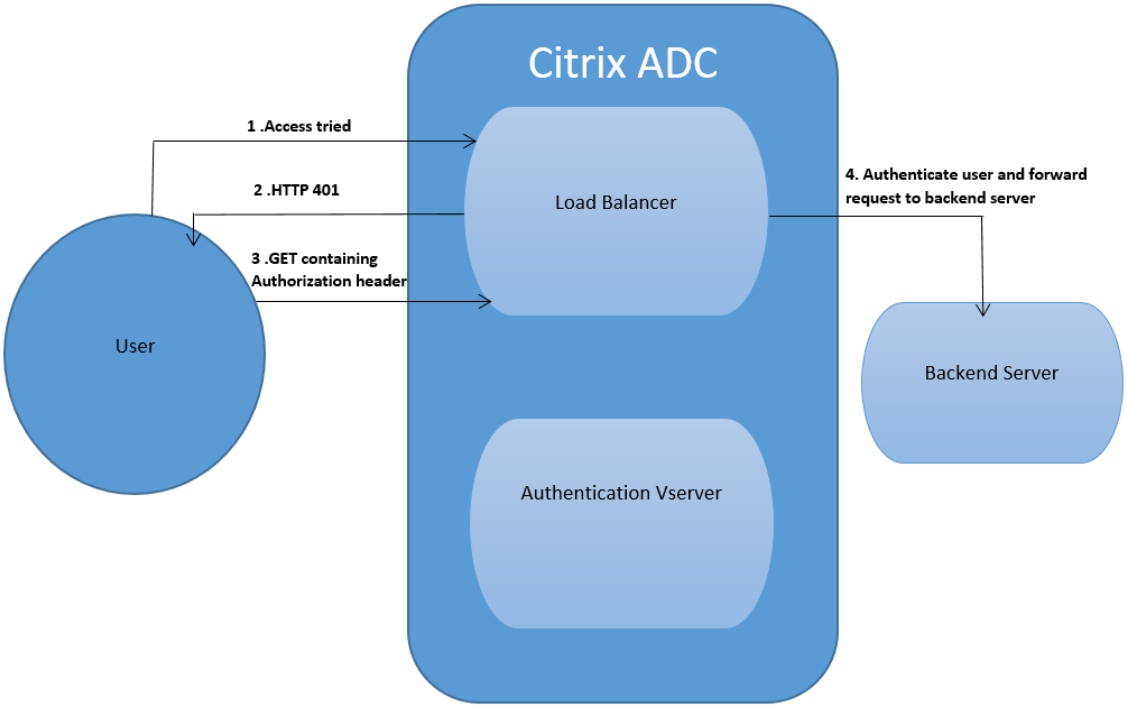
Stellen Sie Folgendes sicher, damit AAA-TM mit 401-Authentifizierung aktiviert ist:

- Der 'AuthNVSName' -Parameterwert für den virtuellen Lastausgleichsserver muss der Name des virtuellen Authentifizierungsservers sein, der zur Authentifizierung von Benutzern verwendet werden soll.
- 'authn401' -Parameter muss aktiviert sein. Der Befehl zum Konfigurieren des gleichen lautet wie folgt:

```
1  set lb vs lb1 -authn401 on -authnvsName <aaavs-name>
```

Die folgenden Schritte führen Sie durch, wie die 401-Authentifizierung funktioniert:

1. Der Benutzer versucht, über den virtuellen Lastausgleichsserver auf eine bestimmte URL zuzugreifen.
2. Der virtuelle Lastausgleichsserver sendet eine 401-HTTP-Antwort an den Benutzer zurück und gibt an, dass für den Zugriff eine Authentifizierung erforderlich ist.
3. Der Benutzer sendet seine Anmeldeinformationen im Autorisierungsheader an den virtuellen Lastausgleichsserver.
4. Der virtuelle Lastausgleichsserver authentifiziert den Benutzer und verbindet den Benutzer dann mit den Back-End-Servern.



> **Wichtig:**
>
> Für einen virtuellen Lastausgleichsserver mit eingeschalteter 401-Authentifizierung können in kurzer Zeit mehrere Authentifizierungs- und Autorisierungssitzungen für denselben Benutzer erstellt werden. Dies könnte zu einem Anstieg des Speichers führen. In diesem Fall können Sie die folgende Konfiguration auf der Citrix ADC-Appliance anwenden, um die Endclientanwendung zu debuggen und zu identifizieren.

```
>set syslogparams -userDefinedAuditlog yes
>
>add audit messageaction 401_log_act InFORMATIONAL '"LB-401 accessed:
    User: <" + AAA.USER.NAME + "> SessionID <"+ AAA.USER.SESSIONID + ">
    Client :<" + CLIENT.IP.SRC + "> accessed URL: <" + HTTP.REQ.URL +
    ">"'
>
>add rewritepolicy rewrite_401_log true NOREWRITE -logAction 401
    _log_act
>
>bind lb vserver <lb_name> -policyName rewrite_401_log -priority 100 -
    type reqUEST

<!--NeedCopy-->
```


reCAPTCHA Konfiguration für nFactor Authentifizierung

October 5, 2021

Citrix Gateway unterstützt eine neue First-Class-Aktion 'CaptChaAction', die die reCAPTCHA-Konfiguration vereinfacht. Da reCAPTCHA eine erstklassige Aktion ist, kann es ein Faktor für sich sein. Sie können reCAPTCHA überall im nFactor Flow injizieren.

Zuvor mussten Sie benutzerdefinierte WebAuth Richtlinien mit Änderungen an der RFWeb UI schreiben. Mit der Einführung von CaptChaAction müssen Sie das JavaScript nicht ändern.

> **Wichtig**
>
> Wenn reCAPTCHA zusammen mit Benutzernamen oder Kennwortfeldern im Schema verwendet wird, wird die Schaltfläche Senden deaktiviert, bis reCAPTCHA erfüllt ist.

reCAPTCHA Konfiguration

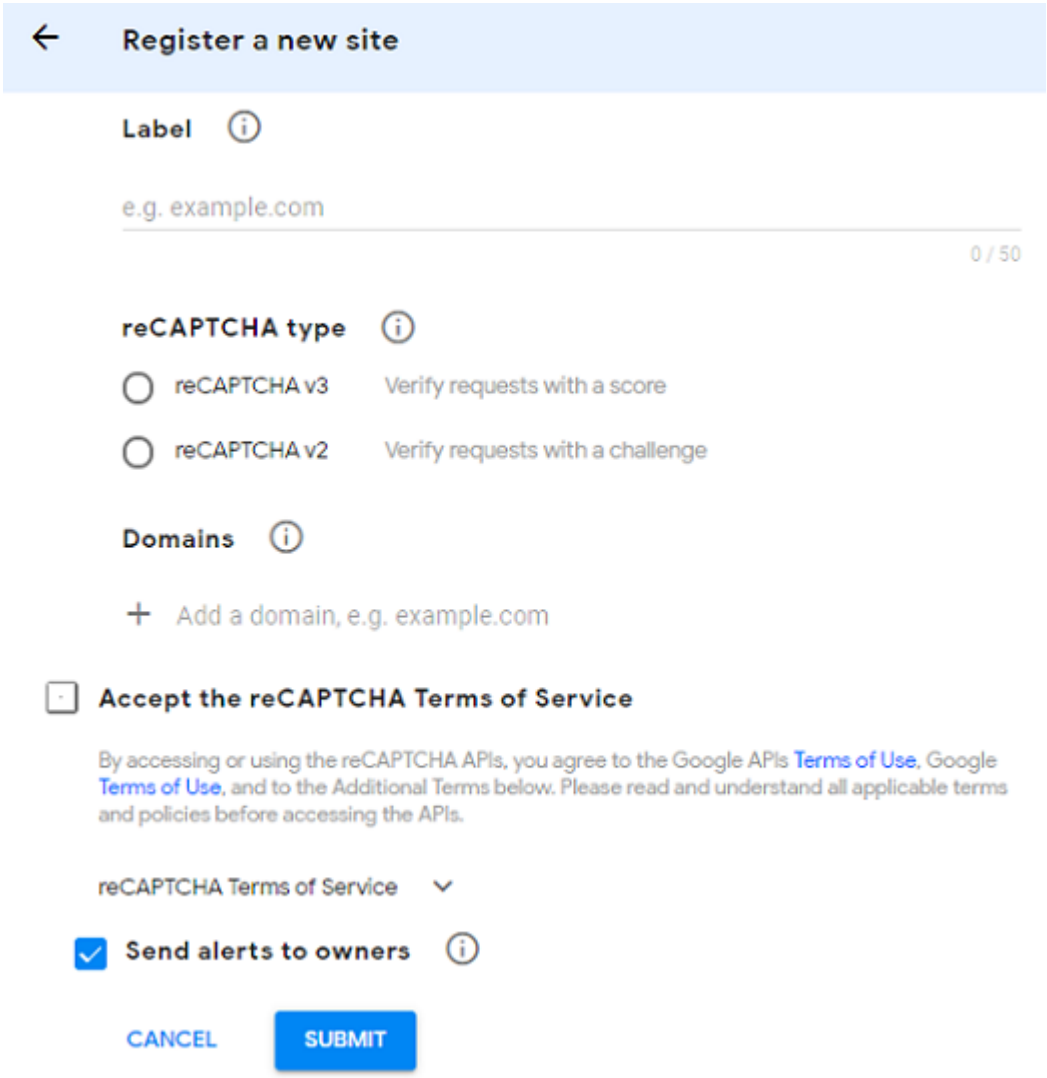
Die reCAPTCHA Konfiguration besteht aus zwei Teilen.

1. Konfiguration auf Google für die Registrierung von reCAPTCHA.
2. Konfiguration auf der Citrix ADC Appliance zur Verwendung von reCAPTCHA als Teil des Anmeldeflusses.

reCAPTCHA Konfiguration auf Google

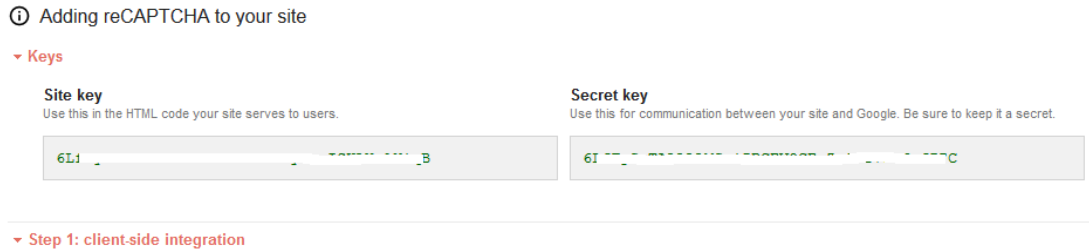
Registrieren Sie eine Domain für reCAPTCHA unter https://www.google.com/recaptcha/admin.

1. Wenn Sie zu dieser Seite navigieren, wird der folgende Bildschirm angezeigt.



> **Hinweis:**
>
> Verwenden Sie reCAPTCHA v2 nur. Unsichtbares reCAPTCHA befindet sich noch in der Beta.

2. Nach der Registrierung einer Domain werden der SiteKey und SecretKey angezeigt.



> **Hinweis:**
>
> Der SiteKey und SecretKey sind aus Sicherheitsgründen ausgegraut. SecretKey muss

> sicher aufbewahrt werden.

reCAPTCHA Konfiguration auf der Citrix ADC Appliance

Die reCAPTCHA Konfiguration auf der Citrix ADC Appliance kann in drei Teile unterteilt werden:

- Bildschirm reCAPTCHA anzeigen
- Senden Sie die reCAPTCHA Antwort auf den Google-Server
- LDAP-Konfiguration ist der zweite Faktor für die Benutzeranmeldung (optional)

Bildschirm reCAPTCHA anzeigen

Die Anpassung des Anmeldeformulars erfolgt über das Loginschema SingleAuthCaptcha.xml. Diese Anpassung wird auf dem virtuellen Authentifizierungsserver angegeben und an die Benutzeroberfläche zum Rendern des Anmeldeformulars gesendet. Das integrierte Anmeldeschema SingleAuthCaptcha.xml befindet sich im Verzeichnis /nsconfig/loginschema/loginSchema auf der Citrix ADC Appliance.

> **Wichtig**
>
> - Basierend auf Ihrem Anwendungsfall und verschiedenen Schemas können Sie das vorhandene Schema ändern. Zum Beispiel, wenn Sie nur reCAPTCHA Faktor (ohne Benutzername oder Kennwort) oder doppelte Authentifizierung mit reCAPTCHA benötigen.
> - Wenn benutzerdefinierte Änderungen durchgeführt oder die Datei umbenannt wird, empfiehlt Citrix, alle LoginSchemas aus dem Verzeichnis /nsconfig/loginschema/loginSchema in das übergeordnete Verzeichnis /nsconfig/loginschema zu kopieren.

So konfigurieren Sie die Anzeige von reCAPTCHA mit CLI

- `add authentication loginSchema singleauthcaptcha -authenticationSchema /nsconfig/loginschema/SingleAuthCaptcha.xml`
- `add authentication loginSchemaPolicy singleauthcaptcha -rule true -action singleauthcaptcha`
- `add authentication vserver auth SSL <IP> <Port>`
- `add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to-key-file>`
- `bind ssl vserver auth -certkey vserver-cert`
- `bind authentication vserver auth -policy singleauthcaptcha -priority 5 -gotoPriorityExpression END`

Senden Sie die reCAPTCHA Antwort auf den Google-Server

Nachdem Sie die reCAPTCHA konfiguriert haben, die den Benutzern angezeigt werden muss, fügen Administratoren Post die Konfiguration auf den Google-Server hinzu, um die reCAPTCHA Antwort vom Browser zu überprüfen.

So überprüfen Sie reCAPTCHA Antwort vom Browser

- `add authentication captchaAction myrecaptcha -sitekey <sitekey-copied-from-google> -secretkey <secretkey-from-google>`
- `add authentication policy myrecaptcha -rule true -action myrecaptcha`
- `bind authentication vserver auth -policy myrecaptcha -priority 1`

Die folgenden Befehle sind erforderlich, um zu konfigurieren, ob AD-Authentifizierung gewünscht ist. Andernfalls können Sie diesen Schritt ignorieren.

- `add authentication ldapAction ldap-new -serverIP x.x.x.x -serverPort 636 -ldapBase "cn=users,dc=aaatm,dc=com"-ldapBindDn adminuser@aaatm.com -ldapBindDnPassword <password> -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName memberof -subAttributeName CN -secType SSL -passwdChange ENABLED -defaultAuthenticationGroup ldapGroup`
- `add authenticationpolicy ldap-new -rule true -action ldap-new`

LDAP-Konfiguration ist der zweite Faktor für die Benutzeranmeldung (optional)

Die LDAP-Authentifizierung erfolgt nach reCAPTCHA, Sie fügen sie dem zweiten Faktor hinzu.

- `add authentication policylabel second-factor`
- `bind authentication policylabel second-factor -policy ldap-new -priority 10`
- `bind authentication vserver auth -policy myrecaptcha -priority 1 -nextFactor second-factor`

Der Administrator muss entsprechende virtuelle Server hinzufügen, je nachdem, ob der virtuelle Lastenausgleich oder die Citrix Gateway Appliance für den Zugriff verwendet wird. Der Administrator muss den folgenden Befehl konfigurieren, wenn ein virtueller Lastausgleichsserver erforderlich ist:

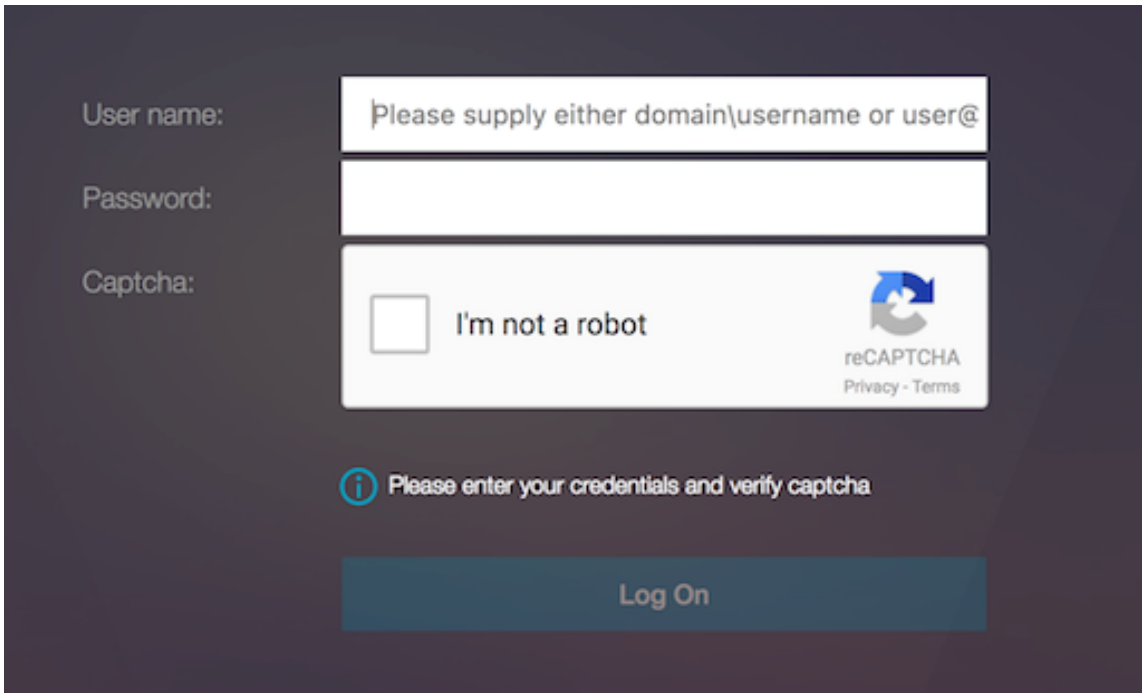
- `add lb vserver lbtest HTTP <IP> <Port> -authentication ON -authenticationHost nssp.aaatm.com`

  nssp.aaatm.com — Löst den virtuellen Authentifizierungsserver auf.

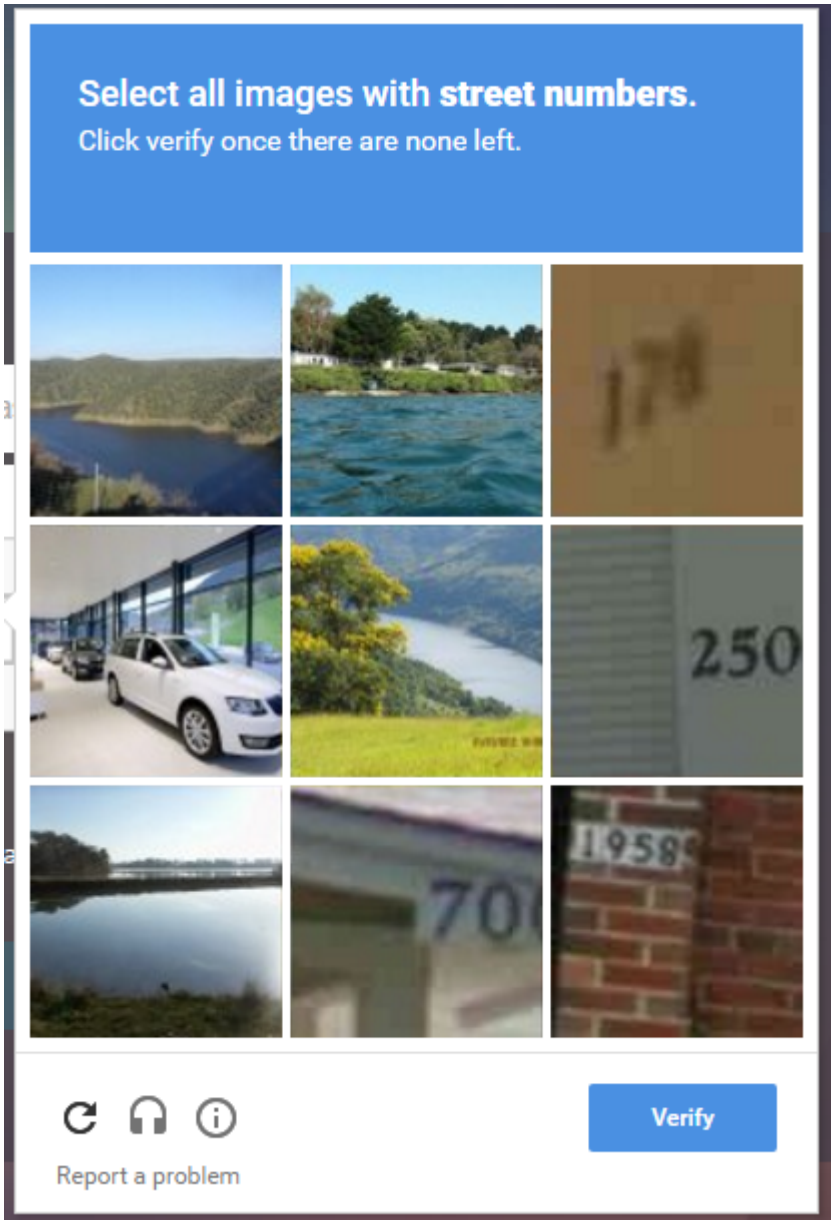
Benutzervalidierung von reCAPTCHA

Nachdem Sie alle Schritte konfiguriert haben, die in den vorherigen Abschnitten erwähnt wurden, müssen Sie die unten angezeigten UI-Screenshots sehen.

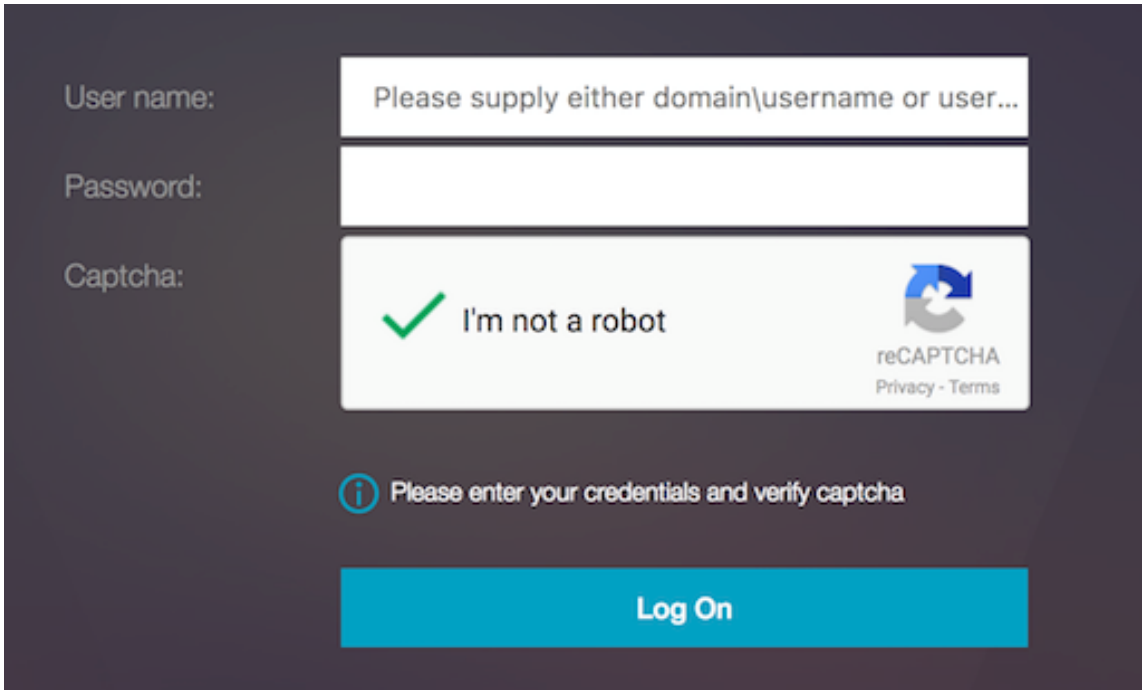
1. Sobald der virtuelle Authentifizierungsserver die Anmeldeseite lädt, wird der Anmeldebildschirm angezeigt. Die **Anmeldung** ist deaktiviert, bis reCAPTCHA abgeschlossen ist.



2. Wählen Sie Ich bin keine Roboteroption aus. Das reCAPTCHA Widget wird angezeigt.



3. Sie werden durch eine Reihe von reCAPTCHA Bildern navigiert, bevor die Fertigstellungsseite angezeigt wird.
4. Geben Sie die AD-Anmeldeinformationen ein, aktivieren Sie das Kontrollkästchen **Ich bin kein Roboter**, und klicken Sie **auf Anmelden** . Wenn die Authentifizierung erfolgreich ist, werden Sie zur gewünschten Ressource umgeleitet.



Hinweise

- Wenn reCAPTCHA mit der AD-Authentifizierung verwendet wird, wird die Schaltfläche Senden für Anmeldeinformationen deaktiviert, bis reCAPTCHA abgeschlossen ist.
- Das reCAPTCHA geschieht in einem eigenen Faktor. Daher müssen alle nachfolgenden Validierungen wie AD im 'nextfactor' von reCAPTCHA erfolgen.

Native OTP-Unterstützung für die Authentifizierung

July 8, 2022

Citrix ADC unterstützt Einmalkennwörter (OTPs), ohne einen Server eines Drittanbieters verwenden zu müssen. Das Einmalkennwort ist eine hochsichere Option für die Authentifizierung bei sicheren Servern, da die generierte Nummer oder der generierte Passcode zufällig ist. Zuvor boten spezialisierte Unternehmen wie RSA mit bestimmten Geräten, die Zufallszahlen generieren, die OTPs an.

Zusätzlich zur Reduzierung der Kapital- und Betriebskosten verbessert diese Funktion die Kontrolle des Administrators, indem die gesamte Konfiguration auf der Citrix ADC-Appliance beibehalten wird.

Hinweis:

Da Server von Drittanbietern nicht mehr benötigt werden, muss der Citrix ADC Administrator eine Schnittstelle zum Verwalten und Überprüfen von Benutzergeräten konfigurieren.

Der Benutzer muss bei einem virtuellen Citrix ADC -Server registriert sein, um die OTP-Lösung ver-

wenden zu können. Eine Registrierung ist nur einmal pro Gerät erforderlich und kann auf bestimmte Umgebungen beschränkt werden. Die Konfiguration und Validierung eines registrierten Benutzers ähnelt der Konfiguration einer zusätzlichen Authentifizierungsrichtlinie.

Vorteile einer nativen OTP-Unterstützung

- Reduziert die Betriebskosten, da zusätzlich zum Active Directory keine zusätzliche Infrastruktur auf einem Authentifizierungsserver erforderlich ist.
- Konsolidiert die Konfiguration nur auf der Citrix ADC-Appliance und bietet so Administratoren eine hervorragende Kontrolle.
- Eliminiert die Abhängigkeit des Clients von einem zusätzlichen Authentifizierungsserver zur Generierung einer von Clients erwarteten Zahl.

Nativer OTP-Workflow

Die native OTP-Lösung ist ein zweifacher Prozess und der Workflow wird wie folgt klassifiziert:

- Geräteregistrierung
- Login für Endbenutzer

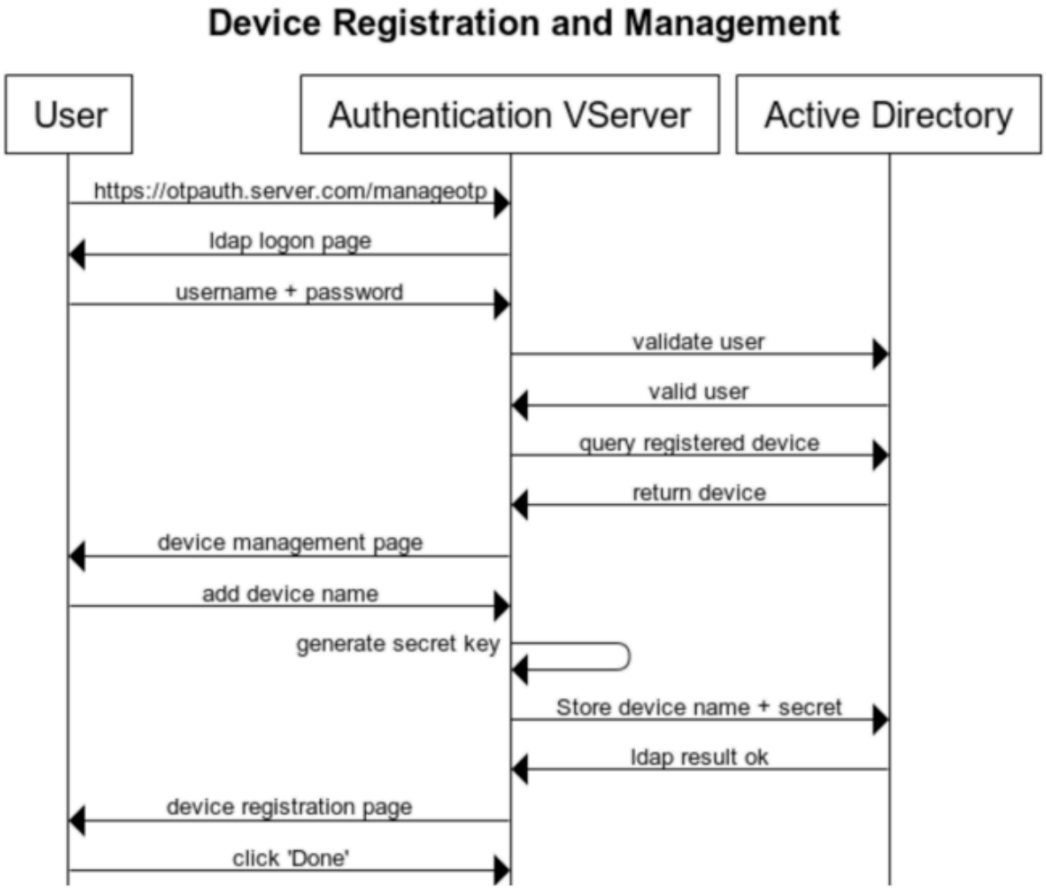
> **Wichtig:**
>
> Sie können den Registrierungsprozess überspringen, wenn Sie Lösungen von Drittanbietern verwenden oder andere Geräte außer der Citrix ADC-Appliance verwalten. Die letzte Zeichenfolge, die Sie hinzufügen, muss im von Citrix ADC angegebenen Format vorliegen.

Die folgende Abbildung zeigt den Ablauf der Geräteregistrierung zur Registrierung eines neuen Geräts für den Empfang von OTP.

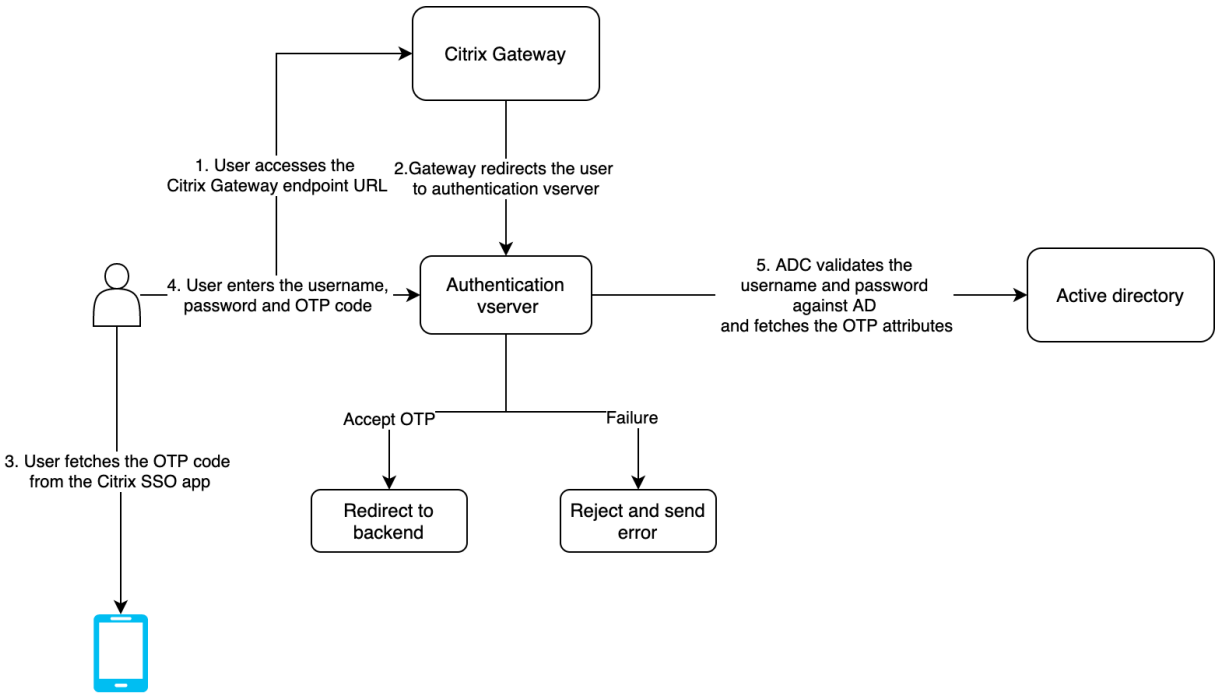
Hinweis: Die Geräteregistrierung kann mit einer beliebigen Anzahl von Faktoren erfolgen. Der einzelne Faktor (wie in der vorherigen Abbildung angegeben) wird als Beispiel verwendet, um den Geräteregistrierungsprozess zu erklären.

Die folgende Abbildung zeigt die Überprüfung von OTP durch das registrierte Gerät.

Die folgende Abbildung zeigt den Ablauf der Geräteregistrierung und den Verwaltungsablauf.



Die folgende Abbildung zeigt den Endbenutzerfluss für die native OTP-Funktion.



Voraussetzungen

Um die native OTP-Funktion zu verwenden, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind.

- Citrix ADC Feature Release-Version ist 12.0 Build 51.24 und höher.
- Die Advanced- oder Premium Edition-Lizenz ist auf Citrix Gateway installiert.
- Citrix ADC ist mit Management-IP konfiguriert und auf die Verwaltungskonsole kann sowohl über einen Browser als auch über eine Befehlszeile zugegriffen werden.
- Citrix ADC ist mit Authentifizierung, Autorisierung und Überwachung virtueller Server zur Authentifizierung von Benutzern konfiguriert. Weitere Informationen finden Sie unter Virtueller Authentifizierungsserver
- Citrix ADC-Appliance ist mit Unified Gateway konfiguriert, und das Authentifizierungs-, Autorisierungs- und Überwachungsprofil wird dem virtuellen Gatewayserver zugewiesen.
- Die native OTP-Lösung ist auf den nFactor-Authentifizierungsfluss beschränkt. Erweiterte Richtlinien sind erforderlich, um die Lösung zu konfigurieren. Weitere Informationen finden Sie unter Natives OTP

Stellen Sie außerdem Folgendes für Active Directory sicher:

- Eine minimale Attributlänge von 256 Zeichen.
- Der Attributtyp muss ‘DirectoryString’ wie UserParameters sein. Diese Attribute können Zeichenfolgenwerte enthalten.
- Der Typ der Attributzeichenfolge muss Unicode sein, wenn der Gerätename nicht-englische Zeichen enthält.

- Der Citrix ADC LDAP-Administrator muss Schreibzugriff auf das ausgewählte AD-Attribut haben.
- Citrix ADC-Appliance und Clientcomputer müssen mit einem gemeinsamen Netzwerkzeitserver synchronisiert werden.

Konfigurieren Sie Natives OTP über die GUI

Die native OTP-Registrierung ist nicht nur eine Ein-Faktor-Authentifizierung. Die folgenden Abschnitte helfen Ihnen bei der Konfiguration der Single- und Second-Factor-Authentifizierung.

Erstellen eines Anmeldeschemas für den ersten Faktor

1. Navigieren Sie zu **Sicherheit AAA > Anwendungsverkehr > Anmeldeschema**.
2. Gehen Sie zu **Profile** und klicken Sie auf **Hinzufügen**.
3. Geben Sie auf der Seite **Authentifizierungs-Login-Schema erstellen** unter dem Feld **Name***lschema_single_auth_manage_otp* ein und klicken Sie neben **noschema** auf **Bearbeiten**.
4. Klicken Sie auf den Ordner **LoginSchema** .
5. Scrolle nach unten, um **SingleAuth.xml** auszuwählen und klicke auf **Auswählen**
6. Klicken Sie auf **Erstellen**.
7. Klicken Sie auf **Richtlinien** und dann auf **Hinzufügen**.
8. Geben **Sie im Fenster Create Authentication Login Schema Policy** die folgenden Werte ein.

   Vorname: lpol_single_auth_manage_otp_by_url

   Profil: Wählen Sie lschema_single_auth_manage_otp aus der Liste aus.

   Regel: HTTP.REQ.COOKIE.VALUE (“NSC_TASS”) .EQ (“`manageotp`”)

Konfigurieren des virtuellen Servers für Authentifizierung, Autorisierung und Überwachung

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Virtuelle Authentifizierungsserver**. Klicken Sie hier, um den vorhandenen virtuellen Server zu bearbeiten. Weitere Informationen finden Sie unter Virtueller Authentifizierungsserver
2. Klicken Sie auf das **+**-Symbol neben **Anmeldeschemas** unter **Erweiterte Einstellungen** im rechten Fensterbereich.
3. Wählen Sie **Kein Anmeldeschema**.
4. Klicken Sie auf den Pfeil und wählen Sie die **lpol_single_auth_manage_otp_by_url** Policy aus, klicken Sie auf **Auswählen**und dann auf **Binden**.

5. Scrollen Sie nach oben und wählen Sie unter **Erweiterte Authentifizierungsrichtlinie** die Option **1 Authentifizierungsrichtlinie** aus.
6. Klicken Sie mit der rechten Maustaste auf die **nFactor-Richtlinie**, und wählen Sie **Bindung bearbeiten** aus. Klicken Sie mit der rechten Maustaste auf die bereits konfigurierte nFactor-Richtlinie oder beziehen Sie sich auf nFactor, um eine zu erstellen, und wählen Sie
7. Klicken Sie auf den Pfeil unter **Nächsten Faktor wählen**, um eine vorhandene Konfiguration auszuwählen, oder klicken Sie auf **Hinzufügen**, um einen neuen Faktor zu erstellen.
8. Geben Sie auf dem Bildschirm **Authentifizierungsrichtlinienlabel erstellen** Folgendes ein, und klicken Sie auf **Weiter** :

   Vorname: manage_otp_flow_label

   Anmeldeschema: Lschema_Int
9. Klicken Sie im Bildschirm **Authentication PolicyLabel** auf **Hinzufügen**, um eine Richtlinie zu erstellen.

   ```
   Create a policy for a normal LDAP server.
   ```
10. Geben Sie auf dem Bildschirm **Authentifizierungsrichtlinie erstellen** Folgendes ein:

    Vorname: auth_pol_ldap_native_otp
11. Wählen Sie den Aktionstyp als **LDAP** in der Liste **Aktionstyp** aus.
12. Klicken Sie im Feld **Aktion** auf **Hinzufügen**, um eine Aktion zu erstellen.

    ```
    Create the first LDAP action with authentication enabled to be used for
     single factor.
    ```
13. Aktivieren Sie auf der Seite **Create Authentication LDAP-Serverdas Optionsfeld Server-IP**, deaktivieren Sie das Kontrollkästchen neben**Authentifizierung**, geben Sie die folgenden Werte ein und wählen Sie**Verbindung testen**aus. Im Folgenden finden Sie eine Beispielkonfiguration.

    Vorname: ldap_native_otp

    IP-Adresse: 192.168.xx.xx

    Base DN: DC = Training, DC = Labor

    Verwaltungsrätin: Administrator@training.lab

    Kennwort: `xxxxx`

    ```
    Create a policy for OTP .
    ```
14. Geben Sie auf dem Bildschirm **Authentifizierungsrichtlinie erstellen** Folgendes ein:

    Vorname: auth_pol_ldap_otp_action
15. Wählen Sie den Aktionstyp als **LDAP** in der Liste **Aktionstyp** aus.

16. Klicken Sie im Feld **Aktion** auf **Hinzufügen**, um eine Aktion zu erstellen.

    ```
    Create the second LDAP action to set OTP authenticator with OTP secret
    configuration and authentication unchecked.
    ```

17. Aktivieren Sie auf der Seite **Create Authentication LDAP-Serverdas Optionsfeld Server-IP**, deaktivieren Sie das Kontrollkästchen neben**Authentifizierung**, geben Sie die folgenden Werte ein und wählen Sie**Verbindung testen**aus. Im Folgenden finden Sie eine Beispielkonfiguration.

    Vorname: ldap_otp_action

    IP-Adresse: 192.168.xx.xx

    Base DN: DC = Training, DC = Labor

    Verwaltungsrätin: Administrator@training.lab

    Kennwort: `xxxxx`

18. Scrollen Sie nach unten zum Abschnitt **Andere Einstellungen** . Verwenden Sie das Dropdownmenü, um die folgenden Optionen auszuwählen.
    Server-Anmeldename Attribut als **Neu** und geben Sie **userprincipalname ein**.

19. Verwenden Sie das Dropdownmenü, um **SSO-Namensattribut** als **Neu** auszuwählen und **userprincipalname**einzugeben.

20. Geben Sie “UserParameters” in das Feld **OTP Secret** ein und klicken Sie auf **Mehr**.

21. Geben Sie die folgenden Attribute ein.

    Attribute 1 = mail
    Attribute 2 = objectGUID
    Attribute 3 = immutableID

22. Klicken Sie auf **OK**.

23. Legen Sie auf der Seite **Authentifizierungsrichtlinie erstellen** den Ausdruck auf **true** fest und klicken Sie auf **Erstellen**.

24. Klicken Sie auf der Seite **Create Authentication Policylabel** auf **Binden**und dann auf **Fertig.**

25. Klicken Sie auf der Seite **Policy Binding** auf **Bind**.

26. Klicken Sie auf der Seite **Authentifizierungsrichtlinie** auf **Schließen**, und klicken Sie auf **Fertig**.

    ```
    Create OTP for OTP verification.
    ```

27. Geben Sie auf dem Bildschirm **Authentifizierungsrichtlinie erstellen** Folgendes ein:

    Name: auth_pol_ldap_otp_verifizieren

28. Wählen Sie den Aktionstyp als **LDAP** in der Liste **Aktionstyp** aus.

29. Klicken Sie im Feld **Aktion** auf **Hinzufügen**, um eine Aktion zu erstellen.

    `Create the third LDAP action to verify OTP.`

30. Aktivieren Sie auf der Seite **Create Authentication LDAP-Serverdas Optionsfeld Server-IP**, deaktivieren Sie das Kontrollkästchen neben**Authentifizierung**, geben Sie die folgenden Werte ein und wählen Sie**Verbindung testen**aus. Im Folgenden finden Sie eine Beispielkonfiguration.

    Vorname: ldap_verify_otp

    IP-Adresse: 192.168.xx.xx

    Base DN: DC = Training, DC = Labor

    Verwaltungsrätin: Administrator@training.lab

    Kennwort: `xxxxx`

31. Scrollen Sie nach unten zum Abschnitt **Andere Einstellungen** . Verwenden Sie das Dropdownmenü, um die folgenden Optionen auszuwählen.
    Server-Anmeldename Attribut als **Neu** und geben Sie **userprincipalname ein**.

32. Verwenden Sie das Dropdownmenü, um **SSO-Namensattribut** als **Neu** auszuwählen und **userprincipalname**einzugeben.

33. Geben Sie “UserParameters” in das Feld **OTP Secret** ein und klicken Sie auf **Mehr**.

34. Geben Sie die folgenden Attribute ein.

    Attribute 1 = mail
    Attribute 2 = objectGUID
    Attribute 3 = immutableID

35. Klicken Sie auf **OK**.

36. Legen Sie auf der Seite **Authentifizierungsrichtlinie erstellen** den Ausdruck auf **true** fest und klicken Sie auf **Erstellen**.

37. Klicken Sie auf der Seite **Create Authentication Policylabel** auf **Binden**und dann auf **Fertig.**

38. Klicken Sie auf der Seite **Policy Binding** auf **Bind**.

39. Klicken Sie auf der Seite **Authentifizierungsrichtlinie** auf **Schließen**, und klicken Sie auf **Fertig**.

Sie haben wahrscheinlich noch keine erweiterte Authentifizierungsrichtlinie für Ihren normalen LDAP-Server.
Ändern Sie den Aktionstyp in LDAP.
Wählen Sie Ihren normalen LDAP-Server aus, bei dem die Authentifizierung aktiviert ist.
Geben Sie als Ausdruck true ein. Dies verwendet die Standardsyntax anstelle der klassischen Syntax.
Klicken Sie auf Erstellen.

> **Hinweis:**
>
> Der virtuelle Authentifizierungsserver muss an das RfWebUI-Portalthema gebunden sein. Binden Sie ein Serverzertifikat an den Server. Die Server-IP '1.2.3.5' muss über einen entsprechenden FQDN verfügen, also otpauth.server.com, für die spätere Verwendung.

Erstellen eines Anmeldeschemas für OTP des zweiten Faktors

1. Navigieren Sie zu **Sicherheit > AAA-Anwendungsverkehr > Virtuelle Server**. Wählen Sie den zu bearbeitenden virtuellen Server aus.
2. Scrollen Sie nach unten und wählen Sie **1 Login**
3. Klicken Sie auf **Bindung hinzufügen**.
4. Klicken Sie im Abschnitt **Richtlinienbindung** auf **Hinzufügen**, um eine Richtlinie hinzuzufügen.
5. Geben Sie auf der Seite **Richtlinie für Authentifizierungsanmeldeschema erstellen** den Namen als OTP ein, und klicken Sie auf **Hinzufügen**, um ein Profil zu erstellen.
6. Geben Sie auf der Seite **Authentifizierungsanmeldeschema erstellen** Name als OTP ein, und klicken Sie auf das Stiftsymbol neben **noschema**.
7. Klicken Sie auf den Ordner **LoginSchema**, wählen Sie **DualAuthManageOTP.xml** aus, und klicken Sie dann auf **Auswählen**.
8. Klicke auf **Mehr** und scrolle nach unten.
9. Geben Sie im Feld **Index für Kennwortanmeldeinformationen** 1 ein. Dadurch speichert nFactor das Kennwort des Benutzers im Citrix ADC AAA-Attribut #1, das später in einer Verkehrsrichtlinie für Single Sign-On bei StoreFront verwendet werden kann. Wenn Sie dies nicht tun, versucht Citrix Gateway, den Passcode zur Authentifizierung bei StoreFront zu verwenden, was nicht funktioniert.
10. Klicken Sie auf **Erstellen**.
11. Geben Sie im Abschnitt **Regel** die Option **True** ein. Klicken Sie auf **Erstellen**.
12. Klicken Sie auf **Bind**.
13. Beachten Sie die beiden Faktoren der Authentifizierung. Klicken Sie auf **Schließen**, und klicken Sie auf **Fertig**.

Traffic-Richtlinie für einmaliges Anmelden

1. Navigieren Sie zu **Citrix Gateway > Richtlinien > Datenverkehr**
2. Klicken Sie auf der Registerkarte **Verkehrsprofile** auf **Hinzufügen**.
3. Geben Sie einen Namen für das Verkehrsprofil für OTP ein.
4. Scrollen Sie im Feld SSO Password Expression nach unten und klicken Sie auf **Erstellen**. Hier verwenden wir das Kennwortattribut für das Login-Schema-Kennwort, das für den zweiten Faktor OTP angegeben ist.


```
http.REQ.USER.ATTRIBUTE(1)
```

5. Klicken Sie auf der Registerkarte **Traffic-Richtlinien** auf **Hinzufügen**.
6. Geben Sie im Feld **Name** einen Namen für die Verkehrsrichtlinie ein.
7. Wählen Sie im Feld **Anforderungsprofil** das von Ihnen erstellte Verkehrsprofil aus.
8. Geben Sie im Feld Ausdruck **True**ein. Wenn Ihr virtueller Citrix Gateway-Server das vollständige VPN zulässt, ändern Sie den Ausdruck in den folgenden Wert.

   ```
   http.req.method.eq(post)||http.req.method.eq(get)&& false
   ```

9. Klicken Sie auf **Erstellen**.

Content Switching-Richtlinie für die Verwaltung von OTP konfigurieren

Die folgenden Konfigurationen sind erforderlich, wenn Sie Unified Gateway verwenden.

1. Navigieren Sie zu **Traffic Management > Content Switching > Richtlinien**. Wählen Sie die Richtlinie für den Content Switching aus, klicken Sie mit der rechten Maustaste und wählen Sie **Bearbeiten**.
2. Bearbeiten Sie den Ausdruck, um die folgende OR-Anweisung auszuwerten, und klicken Sie auf **OK**:

   ```
   is_vpn_url\|\|HTTP.REQ.URL.CONTAINS( “manageotp” )
   ```

Konfigurieren Sie natives OTP über die CLI

Sie benötigen die folgenden Informationen, um die OTP-Geräteverwaltungsseite zu konfigurieren:

- IP wird dem virtuellen Authentifizierungsserver zugewiesen
- FQDN entspricht der zugewiesenen IP
- Serverzertifikat für Authentifizierung virtueller Server

> **Hinweis:**
>
> Native OTP ist nur eine webbasierte Lösung.

So konfigurieren Sie die Registrierungs- und Verwaltungsseite für OTP-Geräte

Erstellen eines virtuellen Authentifizierungsservers

```
1 ```
2 add authentication vserver authvs SSL 1.2.3.5 443
3 bind authentication vserver authvs -portaltheme RFWebUI
```



```
4 bind ssl vserver authvs -certkeyname otpauthcert
5 <!--NeedCopy--> ```
```

> **Hinweis:**
>
> Der virtuelle Authentifizierungsserver muss an das RFWebUI-Portalthema gebunden sein. Binden Sie ein Serverzertifikat an den Server. Die Server-IP '1.2.3.5' muss über einen entsprechenden FQDN verfügen, also otpauth.server.com, für die spätere Verwendung.

So erstellen Sie eine LDAP-Anmeldeaktion

```
1 add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP>
    -  serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
    ldapBindDnPassword <PASSWO> -ldapLoginName <USER FORMAT>
```

Beispiel:

```
1 add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4 -
    serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
    administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
    ldapLoginName userprincipalname
```

So fügen Sie eine Authentifizierungsrichtlinie für LDAP-Anmeldung hinzu

```
1 add authentication Policy auth_pol_ldap_logon -rule true -action
    ldap_logon_action
```

So präsentieren Sie die Benutzeroberfläche über LoginSchema

Benutzernamenfeld und Kennwortfeld für Benutzer bei der Anmeldung anzeigen

```
1 add authentication loginSchema lschema_single_auth_manage_otp -
    authenticationSchema "/nsconfig/loginschema/LoginSchema/
    SingleAuthManageOTP.xml"
```


Seite zur Geräteregistrierung und -verwaltung anzeigen

Citrix empfiehlt zwei Möglichkeiten, den Bildschirm für die Geräteregistrierung und -verwaltung anzuzeigen: URL oder Hostname.

- **Verwenden von URL**

  Wenn die URL '/manageotp' enthält

  - `add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_url -rule "http.req.cookie.value("NSC_TASS").contains("manageotp")"-action lschema_single_auth_manage_otp`
  - `bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_url -priority 10 -gotoPriorityExpression END`

- **Verwenden des Hostnamens**

  Wenn der Hostname 'alt.server.com' lautet

  - `add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_host -rule "http.req.header("host").eq("alt.server.com")"-action lschema_single_auth_manage_otp`
  - `bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_host -priority 20 -gotoPriorityExpression END`

So konfigurieren Sie die Benutzeranmeldeseite über die CLI

Sie benötigen die folgenden Informationen, um die Seite Benutzeranmeldung zu konfigurieren:

- IP für einen virtuellen Lastausgleichsserver
- Entsprechender FQDN für den virtuellen Lastausgleichsserver
- Serverzertifikat für den virtuellen Lastausgleichsserver

```
bind ssl vserver lbvs_https -certkeyname lbvs_server_cert
<!--NeedCopy-->
```

Back-End-Dienst im Lastenausgleich wird wie folgt dargestellt:

```
```
add service iis_backendsso_server_com 1.2.3.210 HTTP 80
bind lb vserver lbvs_https iis_backendsso_server_com
<!--NeedCopy--> ```
```

 
```

So erstellen Sie eine OTP-Passcode-Validierungsaktion

```
1 add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP>
      -serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
      ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT> -
      authentication DISABLED -OTPSecret <LDAP ATTRIBUTE>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add authentication ldapAction ldap_otp_action -serverIP 1.2.3.4 -
      serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
      administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
      ldapLoginName userprincipalname -authentication DISABLED -OTPSecret
      userParameters
2 <!--NeedCopy-->
```

> **Wichtig:**
>
> Der Unterschied zwischen der LDAP-Anmeldung und der OTP-Aktion besteht darin, dass die Authentifizierung deaktiviert und ein neuer Parameter `OTPSecret` eingeführt werden muss. Verwenden Sie den AD-Attributwert nicht.

So fügen Sie Authentifizierungsrichtlinien für die OTP-Kenncodevalidierung hinzu

```
1 add authentication Policy auth_pol_otp_validation -rule true -action
      ldap_otp_action
```

Präsentation der Zwei-Faktor-Authentifizierung durch LoginSchema

Fügen Sie die Benutzeroberfläche für die Zwei-Faktor-Authentifizierung hinzu.

```
1 add authentication loginSchema lscheme_dual_factor -
      authenticationSchema "/nsconfig/loginschema/LoginSchema/DualAuth.xml
      "
2 add authentication loginSchemaPolicy lpol_dual_factor -rule true -
      action lscheme_dual_factor
```


So erstellen Sie einen Passcode-Validierungsfaktor über die Richtlinien

Erstellen einer Beschriftung für die Verwaltung von OTP-Flussrichtlinien für den nächsten Faktor (der erste Faktor ist die LDAP-Anmeldung)

```
add authentication loginSchema lschema_noschema -authenticationSchema
    noschema
add authentication policylabel manage_otp_flow_label -loginSchema
    lschema_noschema
```

So binden Sie die OTP-Richtlinie an das Richtlinienlabel

```
bind authentication policylabel manage_otp_flow_label -policyName
    auth_pol_otp_validation -priority 10 -gotoPriorityExpression NEXT
```

So binden Sie den UI-Flow

Binden Sie die LDAP-Anmeldung gefolgt von der OTP-Validierung mit dem virtuellen Authentifizierungsserver.

```
bind authentication vserver authvs -policy auth_pol_ldap_logon -
    priority 10 -nextFactor  manage_otp_flow_label -
    gotoPriorityExpression NEXT
bind authentication vserver authvs -policy lpol_dual_factor -priority
    30 -gotoPriorityExpression END
```

Registrieren Sie Ihr Gerät bei Citrix ADC

1. Navigieren Sie mit dem Suffix /manageotp zu Ihrem Citrix ADC FQDN (erste öffentliche IP). Zum Beispiel Login bei https://otpauth.server.com/manageotp mit Benutzeranmeldeinformationen.
2. Klicken Sie auf das **+-Symbol**, um ein Gerät hinzuzufügen.
3. Geben Sie einen Gerätenamen ein und drücken Sie **Los**. Ein Barcode erscheint auf dem Bildschirm.
4. Klicken Sie auf **Setup beginnen** und dann auf **Barcode scannen**.
5. Bewegen Sie die Gerätekamera über den QR-Code. Sie können den Code optional eingeben.

> **Hinweis**:
>
> Der angezeigte QR-Code ist 3 Minuten gültig.

6. Nach erfolgreichem Scan wird Ihnen ein 6-stelliger, zeitsensitiver Code angezeigt, mit dem Sie sich anmelden können.
7. Klicken Sie zum Testen auf dem QR-Bildschirm auf **Fertig** und dann auf das grüne Häkchen rechts.
8. Wählen Sie Ihr Gerät aus dem Dropdownmenü aus, geben Sie den Code von Google Authenticator ein (muss blau und nicht rot sein) und klicken Sie auf **Los**.
9. Stellen Sie sicher, dass Sie sich über das Dropdownmenü oben rechts auf der Seite abmelden.

Melden Sie sich mit dem OTP bei Citrix ADC an

1. Navigieren Sie zu Ihrer ersten öffentlich zugänglichen URL und geben Sie Ihr OTP über Google Authenticator ein, um sich anzumelden.
2. Authentifizieren Sie sich bei der Citrix ADC Splash-Seite.

Speichern von geheimen OTP-Daten in einem verschlüsselten Format

December 7, 2021

Ab Citrix ADC Version 13.0 Build 41.20 können die geheimen OTP-Daten in einem verschlüsselten Format statt Klartext gespeichert werden.

Zuvor hat die Citrix ADC Appliance OTP-Geheimnis als Nur-Text in AD gespeichert. Das Speichern von OTP-Geheimnissen im Klartext stellt eine Sicherheitsbedrohung dar, da ein böswilliger Angreifer oder ein Administrator die Daten ausnutzen kann, indem er das gemeinsame Geheimnis anderer Benutzer anzeigt.

Der Verschlüsselungsparameter aktiviert die Verschlüsselung des OTP-Geheimnisses in AD. Wenn Sie ein neues Gerät mit Citrix ADC Version 13.0 Build 41.20 registrieren und den Verschlüsselungsparameter aktivieren, wird der OTP-Schlüssel standardmäßig in einem verschlüsselten Format gespeichert. Wenn der Verschlüsselungsparameter jedoch deaktiviert ist, wird der OTP-Schlüssel im Nur-Text-Format gespeichert.

Für Geräte, die vor 13.0 Build 41.20 registriert sind, müssen Sie die folgenden Schritte ausführen:

1. Aktualisieren Sie die 13.0 Citrix ADC Appliance auf 13.0 Build 41.20.
2. Aktivieren Sie den Verschlüsselungsparameter auf der Appliance.

3. Verwenden Sie das geheime OTP-Migrationstool, um geheime OTP-Daten vom Nur-Text-Format in ein verschlüsseltes Format zu migrieren.

Weitere Informationen zum geheimen OTP-Migrationstool finden Sie unter OTP-Verschlüsselungstool.

> **Wichtig**
>
> Citrix empfiehlt Ihnen als Administrator, um sicherzustellen, dass die folgenden Kriterien erfüllt sind:
>
> - Ein neues Zertifikat muss so konfiguriert werden, dass OTP-Geheimnisse verschlüsselt werden, wenn Sie KBA nicht als Teil der Self-Service-Kennwortrücksetzfunktion verwenden.
>   - To bind the certificate to VPN global, you can use the following command:
>
>     ```
>     bind vpn global -userDataEncryptionKey <certificate name>
>     ```
>
> - Wenn Sie bereits ein Zertifikat zum Verschlüsseln von KBA verwenden, können Sie dasselbe Zertifikat zum Verschlüsseln von OTP-Geheimnissen verwenden.

So aktivieren Sie OTP-Verschlüsselungsdaten mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set aaa otpparameter [-encryption ( ON | OFF )]
```

Beispiel

```
set aaa otpparameter -encryption ON
```

So konfigurieren Sie die OTP-Verschlüsselung mit der GUI

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr**, und klicken Sie im Abschnitt **Authentifizierungseinstellungen** auf **Authentifizierung AAA OTP-Parameter ändern**.
2. Wählen Sie auf der Seite **AAA OTP-Parameter konfigurieren** die Option **OTP Secret encryption** aus.
3. Klicken Sie auf OK.

Konfigurieren der Anzahl der Endbenutzergeräte für den Empfang von OTP-Benachrichtigungen

Administratoren können nun die Anzahl der Geräte konfigurieren, die ein Endbenutzer für den Empfang von OTP-Benachrichtigungen oder -Authentifizierung registrieren kann.

So konfigurieren Sie die Anzahl der Geräte in OTP mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

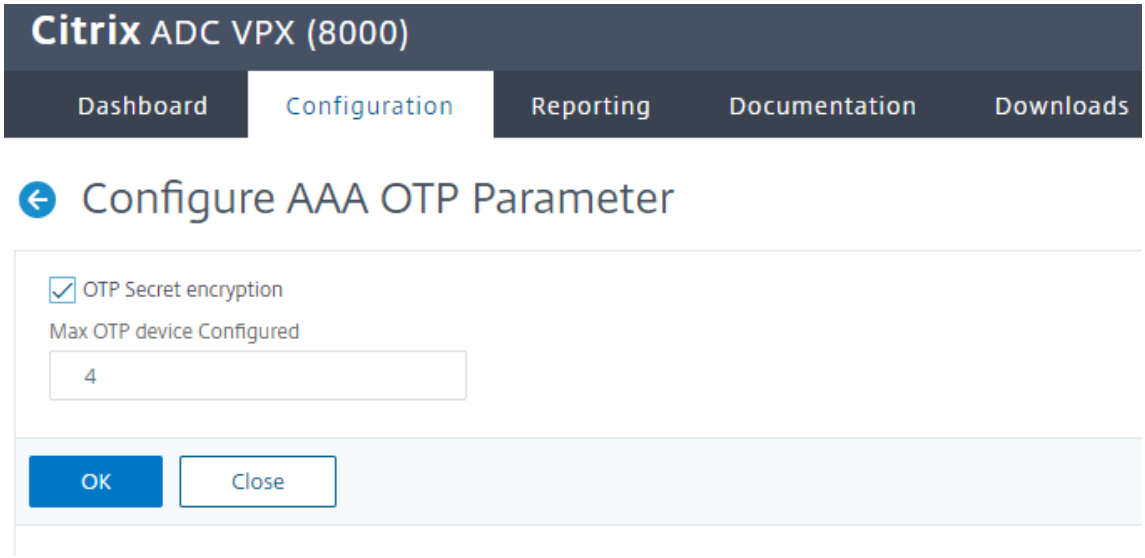

```
set aaa otpparameter [-maxOTPDevices <positive_integer>]
```

Beispiel

```
set aaa otpparameter -maxOTPDevices 4
```

So konfigurieren Sie die Anzahl der Geräte mit der GUI

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr**, und klicken Sie im Abschnitt **Authentifizierungseinstellungen** auf **Authentifizierung AAA OTP-Parameter ändern**.
2. Geben Sie auf der Seite **AAA OTP-Parameter konfigurieren** den Wert für **Max. OTP-Gerät konfiguriert** ein.
3. Klicken Sie auf **OK**.



OTP-Verschlüsselungstool

June 1, 2022

Ab Citrix ADC Release 13.0 Build 41.20 werden die geheimen OTP-Daten für erhöhte Sicherheit in einem verschlüsselten Format anstelle von Klartext gespeichert. Das Speichern des OTP-Geheimnisses in verschlüsseltem Format erfolgt automatisch und erfordert keinen manuellen Eingriff.

Zuvor hat die Citrix ADC Appliance das OTP-Geheimnis als Nur-Text im Active Directory gespeichert. Das Speichern des OTP-Geheimnisses in einem Nur-Text-Format stellte eine Sicherheitsbedrohung dar, da ein böswilliger Angreifer oder ein Administrator die Daten ausnutzen kann, indem er das gemeinsame Geheimnis anderer Benutzer anzeigt.

Das OTP-Verschlüsselungstool bietet folgende Vorteile:

- Führt nicht zu Datenverlust, selbst wenn Sie alte Geräte haben, die ein altes Format (Nur-Text) verwenden.
- Die Abwärtskompatibilitätsunterstützung mit alten Citrix Gateway-Versionen hilft bei der Integration und Unterstützung der vorhandenen Geräte zusammen mit dem neuen Gerät.
- Mit dem OTP-Verschlüsselungstool können Administratoren alle geheimen OTP-Daten aller Benutzer gleichzeitig migrieren.

> **Hinweis:**
>
> Das OTP-Verschlüsselungstool verschlüsselt oder entschlüsselt keine KBA-Registrierungs- oder E-Mail-Registrierungsdaten.

Verwendung des OTP-Verschlüsselungswerkzeugs

Das OTP-Verschlüsselungstool kann für Folgendes verwendet werden:

- **Verschlüsselung**. Speichern Sie das OTP-Geheimnis in verschlüsseltem Format. Das Tool extrahiert die OTP-Daten der bei Citrix ADC registrierten Geräte und konvertiert dann die OTP-Daten im Nur-Text-Format in ein verschlüsseltes Format.
- **Entschlüsselung**. Setzen Sie das OTP-Geheimnis auf das Nur-Text-Format zurück.
- **Zertifikate aktualisieren**. Administratoren können das Zertifikat jederzeit auf ein neues Zertifikat aktualisieren. Administratoren können das Tool verwenden, um das neue Zertifikat einzugeben und alle Einträge mit den neuen Zertifikatsdaten zu aktualisieren. Der Zertifikatpfad muss entweder ein absoluter Pfad oder ein relativer Pfad sein.

> **Wichtig**
>
> - Sie müssen den Verschlüsselungsparameter in der Citrix ADC-Appliance aktivieren, um das OTP-Verschlüsselungstool verwenden zu können.
> - Für Geräte, die vor dem Build 41.20 mit Citrix ADC registriert sind, müssen Sie Folgendes ausführen:
>   - Upgrade the 13.0 Citrix ADC appliance to 13.0 build 41.20.
>   - Enable the encryption parameter on the appliance.
>   - Use the OTP Secret migration tool to migrate OTP secret data from plain text format to encrypted format.

OTP-Geheimdaten im Nur-Text-Format

Beispiel:

```
##@devicename=<16 or more bytes>&tag=<64bytes>&,
```

Wie Sie sehen können, ist das Startmuster für ein altes Format immer “#@” und das Endmuster ist immer “&”. Alle Daten zwischen ”devicename=” und dem Endmuster stellen OTP-Daten des Benutzers

dar.

Geheime OTP-Daten im verschlüsselten Format

Das neue verschlüsselte Format von OTP-Daten hat das folgende Format:

Beispiel:

```
    {

         ”otpdata” : {

          “devices” : {

                          “device1” :  “value1” ,
                          “device2” :  “value2” , ···
                      }

             }

     }

<!--NeedCopy-->
```

Dabei ist Wert1 der base64-codierte Wert von kid + IV +chiffre Daten

Verschlüsselungsdaten sind wie folgt strukturiert:

```
    {

      secret:<16-byte secret>,
      tag : <64-byte tag value>
      alg: <algorithm used> (not mandatory, default is sha1, specify
         the algorithm only if it is not default)
     }

<!--NeedCopy-->
```

- In “Geräten” haben Sie einen Wert für jeden Namen. Der Wert ist base64encode(kid).base64encode(IV).base6
- In Standard-AES-Algorithmen wird IV immer als die ersten 16 Byte oder 32 Byte an Verschlüsselungsdaten gesendet. Sie können demselben Modell folgen.
- IV unterscheidet sich für jedes Gerät, obwohl der Schlüssel gleich bleibt.

Einrichtung des OTP-Verschlüsselungstools

Das OTP-Verschlüsselungstool befindet sich im Verzeichnis `\var\netscaler\otptool`. Sie müssen den Code von der Citrix ADC-Quelle herunterladen und das Tool mit den erforderlichen AD-Anmeldeinformationen ausführen.

- Voraussetzungen für die Verwendung des OTP-Verschlüsselungstools:
  - Installieren Sie Python 3.5 oder höher in der Umgebung, in der dieses Tool ausgeführt wird.
  - Installieren Sie pip3 oder neuere Versionen.
- Führen Sie die folgenden Befehle aus:
  - **pip install requirements.txt**. Installiert automatisch die Anforderungen
  - **python main.py**. Ruft das OTP-Verschlüsselungstool auf. Sie müssen die erforderlichen Argumente angeben, die Ihren Anforderungen für die Migration von geheimen OTP-Daten entsprechen.
- Das Werkzeug ist in der Shell-Eingabeaufforderung `\var\netscaler\otptool`.
- Führen Sie das Tool mit den erforderlichen AD-Anmeldeinformationen aus.

OTP-Verschlüsselungstool-Schnittstelle

Die folgende Abbildung zeigt ein Beispiel für eine OTP-Verschlüsselungs-Tool-Schnittstelle. Die Schnittstelle enthält alle Argumente, die für die Verschlüsselung/Entschlüsselung/Zertifikatsaktualisierung definiert werden müssen. Außerdem wird eine kurze Beschreibung jedes Arguments erfasst.

Argument OPERATION

Sie müssen das Argument OPERATION definieren, um das OTP-Verschlüsselungstool für Verschlüsselung, Entschlüsselung oder Zertifikatsaktualisierung zu verwenden.

In der folgenden Tabelle sind einige Szenarien zusammengefasst, in denen Sie das OTP-Verschlüsselungstool und die entsprechenden Argumentwerte OPERATION verwenden können.

Szenario	Operations-Argumentwert und andere Argumente
Konvertieren Sie OTP-Schlüssel im Klartext in ein verschlüsseltes Format mit demselben Attribut	Geben Sie den Argumentwert OPERATION als 0 ein und geben Sie denselben Wert für das Quell- und Zielattribut an. **Beispiel:** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -target_attribute unixhomedirectory -operation 0 -cert_path aaatm_wild_all.cert`
Konvertieren Sie OTP-Schlüssel im Klartext-Format in ein verschlüsseltes Format mit einem anderen Attribut	Geben Sie den Argumentwert OPERATION als 0 ein und geben Sie die entsprechenden Werte für das Quell- und Zielattribut an. **Beispiel:** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -target_attribute userparameters -operation 0 -cert_path aaatm_wild_all.cert`
Konvertiere die verschlüsselten Einträge zurück in Klartext	Geben Sie den Argumentwert OPERATION als 1 ein und geben Sie die entsprechenden Werte für das Quell- und Zielattribut an. **Beispiel:** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -target_attribute userparameters -operation 1 -cert_path aaatm_wild_all.cert`

Szenario	Operations-Argumentwert und andere Argumente
Aktualisieren Sie das Zertifikat auf ein neues Zertifikat	Geben Sie den Argumentwert OPERATION als 2 ein und geben Sie das gesamte vorherige Zertifikat und die Details des neuen Zertifikats in den entsprechenden Argumenten an. **Beispiel:** `python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local -search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -operation 2 -cert_path aaatm_wild_all.cert -new_cert_path aaatm_wild_all_new.cert`

CERT_PATH Argument

Das Argument CERT_PATH ist eine Datei, die das Zertifikat enthält, das im Citrix ADC zum Verschlüsseln der Daten verwendet wird. Der Benutzer muss dieses Argument für alle drei Vorgänge angeben, nämlich **Verschlüsselung**, **Entschlüsselung**und **Update-Zertifikate**.

Die CERT_PATH-Argumentdatei muss sowohl das Zertifikat als auch den zugehörigen privaten Schlüssel im PEM- oder CERT-Format enthalten (PFX wird nicht unterstützt).

Wenn beispielsweise die Zertifikate.cert- und certificate.key- Dateien der Zertifikatsdatei und ihrem privaten Schlüssel entsprechen, erstellt der folgende Befehl in einem Unix-ähnlichen System die Datei `certkey.merged`, die als Wert für das Flag cert_path verwendet werden kann.

```
$ cat certificate.cert certificate.key > certkey.merged
$
<!--NeedCopy-->
```

> **Zu beachtende Punkte zum Zertifikat**
>
> - Der Benutzer muss dasselbe Zertifikat bereitstellen, das global in der Citrix ADC Appliance für die Verschlüsselung von Benutzerdaten gebunden ist.
> - Das Zertifikat muss das Base64-codierte öffentliche Zertifikat und den entsprechenden privaten RSA-Schlüssel in derselben Datei enthalten.

> - Das Format des Zertifikats muss entweder PEM oder CERT sein. Das Zertifikat muss dem X509-Format entsprechen.
> - Das kennwortgeschützte Zertifikatsformat und die *PFX-Datei* werden von diesem Tool nicht akzeptiert. Der Benutzer muss die PFX-Zertifikate in *.cert* konvertieren, bevor er die Zertifikate an das Tool bereitstellt.

SEARCH_FILTER Argument

Das Argument SEARCH_FILTER wird verwendet, um die AD-Domänen oder Benutzer zu filtern. Das Format dieses Suchfilters entspricht dem LDAP-Suchfilterformat, das im LDAP-Aktionsbefehl in der Citrix ADC Appliance verwendet wird.

Aktivieren der Verschlüsselungsoption in der Citrix ADC-Appliance

Um das Nur-Text-Format zu verschlüsseln, müssen Sie die Verschlüsselungsoption in der Citrix ADC-Appliance aktivieren.

Um OTP-Verschlüsselungsdaten mithilfe der CLI zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein:

```
set aaa otpparameter [-encryption ( ON | OFF )]
```

Beispiel:

```
set aaa otpparameter -encryption ON
```

Anwendungsfälle des OTP-Verschlüsselungstools

Das OTP-Verschlüsselungstool kann für die folgenden Anwendungsfälle verwendet werden.

Registrieren neuer Geräte bei der Citrix ADC-Appliance Version 13.0 Build 41.20

Wenn Sie Ihr neues Gerät bei der Citrix ADC-Appliance Version 13.0 Build 41.x registrieren und wenn die Verschlüsselungsoption aktiviert ist, werden die OTP-Daten in einem verschlüsselten Format gespeichert. Sie können einen manuellen Eingriff vermeiden.

Wenn die Verschlüsselungsoption nicht aktiviert ist, werden die OTP-Daten im Nur-Text-Format gespeichert.

Migrieren Sie OTP-Daten für die Geräte, die vor 13.0 Build 41.20 registriert wurden

Sie müssen Folgendes ausführen, um die geheimen OTP-Daten für die Geräte zu verschlüsseln, die zuvor bei der Citrix ADC Appliance registriert wurden 13.0 Build 41.20.

- Migrieren Sie mit dem Konvertierungstool OTP-Daten vom Nur-Text-Format in das verschlüsselte Format.
- Aktivieren Sie den Parameter “Encryption” auf der Citrix ADC Appliance.
  - So aktivieren Sie die Verschlüsselungsoption mithilfe der CLI:
    * `set aaa otpparameter -encryption ON`
  - So aktivieren Sie Verschlüsselungsoptionen mit der GUI:
    * Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr** und klicken Sie im Abschnitt ****Authentifizierungseinstellungen auf Authentifizierung** ändern AAA OTP-Parameter** .
    * Wählen Sie auf der Seite **AAA-OTP-Parameter konfigurieren** die Option **Geheime OTP-Verschlüsselung**aus, und klicken Sie auf **OK**.
  - Melden Sie sich mit den gültigen AD-Anmeldeinformationen an.
  - Falls erforderlich, registrieren Sie zusätzliche Geräte (optional).

Migrieren Sie verschlüsselte Daten vom alten Zertifikat zum neuen Zertifikat

Wenn Administratoren das Zertifikat auf ein neues Zertifikat aktualisieren möchten, bietet das Tool die Möglichkeit, die neuen Zertifikatsdateneinträge zu aktualisieren.

So aktualisieren Sie das Zertifikat mithilfe der CLI auf ein neues Zertifikat

Geben Sie an der Eingabeaufforderung Folgendes ein:

Beispiel:

```
python3 main.py -Host 192.0.2.1 -Port 636 -username ldapbind_user@aaa.local
-search_base cn=users,dc=aaa,dc=local -source_attribute unixhomedirectory -
target_attribute userparameters -operation 2 -cert_path aaatm_wild_all.cert
 -new_cert_path aaatm_wild_all_new.cert
```

> **Hinweis**
>
> - Die Zertifikate müssen sowohl private als auch öffentliche Schlüssel enthalten.
> - Derzeit wird die Funktion nur für OTP bereitgestellt.

Erneutes Verschlüsseln oder Migrieren auf neues Zertifikat für Geräte, die nach dem Upgrade der Appliance auf 13.0 Build 41.20 mit Verschlüsselung registriert wurden

Der Administrator kann das Tool auf Geräten verwenden, die bereits mit einem Zertifikat verschlüsselt sind, und dieses Zertifikat mit einem neuen Zertifikat aktualisieren.

Verschlüsselte Daten zurück in das Nur-Text-Format umwandeln

Der Administrator kann das OTP-Geheimnis entschlüsseln und auf das ursprüngliche Nur-Text-Format zurücksetzen. Das OTP-Verschlüsselungstool durchsucht alle Benutzer verschlüsselt nach dem OTP-Geheimnis und wandelt sie in das entschlüsselte Format um.

So aktualisieren Sie das Zertifikat mithilfe der CLI auf ein neues Zertifikat

Geben Sie an der Eingabeaufforderung Folgendes ein:

Beispiel:

```
python3 main.py -Host 192.0.2.1 - Port 636 -username ldapbind_user@aaa
    .local -search_base cn=users,dc=aaa,dc=local -source_attribute
    unixhomedirectory -target_attribute userparameters -operation 1
<!--NeedCopy-->
```

Problembehandlung

Das Tool generiert die folgenden Protokolldateien.

- **app.log**. Protokolliert alle wichtigen Ausführungsschritte und Informationen zu Fehlern, Warnungen und Ausfällen.
- **unmodified_users.txt**. Enthält eine Liste von Benutzer-DNs, die nicht vom reinen Text auf das verschlüsselte Format aktualisiert wurden. Diese Protokolle werden zu einem Fehler im Format generiert oder aus einem anderen Grund.

Pushbenachrichtigung für OTP

May 10, 2022

Citrix Gateway unterstützt Pushbenachrichtigungen für OTP. Benutzer müssen das auf ihren registrierten Geräten empfangene OTP nicht manuell eingeben, um sich bei Citrix Gateway anzumelden. Administratoren können Citrix Gateway so konfigurieren, dass Anmeldebenachrichtigungen mithilfe von Pushbenachrichtigungsdiensten an die registrierten Geräte der Benutzer gesendet werden. Wenn Benutzer die Benachrichtigung erhalten, müssen sie einfach in der Benachrichtigung auf Zulassen tippen, um sich bei Citrix Gateway anzumelden. Wenn das Gateway eine Bestätigung vom Benutzer erhält, identifiziert es die Quelle der Anfrage und sendet eine Antwort an diese Browserverbindung.

Wenn die Benachrichtigungsantwort nicht innerhalb des Timeout-Zeitraums (30 Sekunden) empfangen wird, werden Benutzer zur Citrix Gateway-Anmeldeseite weitergeleitet. Die Benutzer können das

OTP dann manuell eingeben oder auf Benachrichtigung **erneut senden klicken, um die Benachrichtigung** erneut auf dem registrierten Gerät zu erhalten.

Administratoren können mithilfe der für Pushbenachrichtigungen erstellten Anmeldeschemas die Pushbenachrichtigung als Standardauthentifizierung vornehmen.

> **Wichtig:**
>
> Die Pushbenachrichtigungsfunktion ist mit einer Citrix ADC Premium Edition-Lizenz verfügbar.

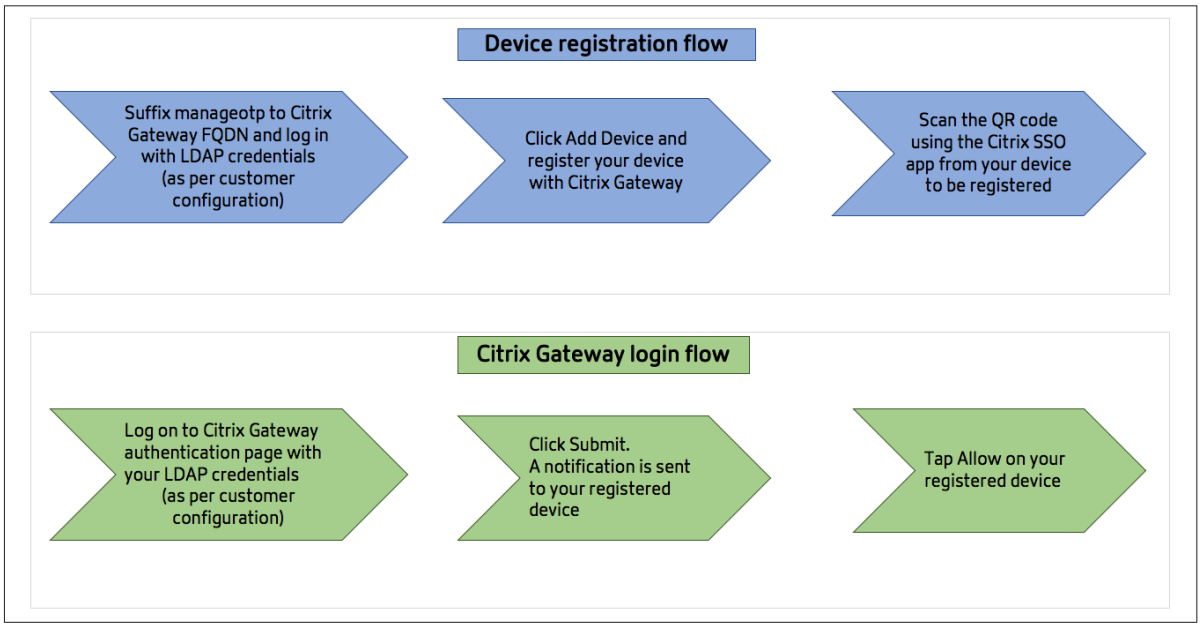
Vorteile von Pushbenachrichtigungen

- Pushbenachrichtigungen bieten einen sichereren Multifaktor-Authentifizierungsmechanismus. Die Authentifizierung bei Citrix Gateway ist erst erfolgreich, wenn der Benutzer den Anmeldeversuch genehmigt.
- Pushbenachrichtigungen sind einfach zu verwalten und zu verwenden. Benutzer müssen die Citrix SSO Mobile App herunterladen und installieren, für die keine Administratorunterstützung erforderlich ist.
- Benutzer müssen den Code nicht kopieren oder sich merken. Sie müssen einfach auf das Gerät tippen, um sich authentifizieren zu lassen.
- Benutzer können mehrere Geräte registrieren.

Funktionsweise von Pushbenachrichtigungen

Der Workflow für Pushbenachrichtigungen kann in zwei Kategorien eingeteilt werden:

- Geräteregistrierung
- Login für Endbenutzer



Voraussetzungen für die Verwendung von Pushbenachrichtigungen

- Schließen Sie den Citrix Cloud-Onboarding-Prozess ab.
    1. Erstellen Sie ein Citrix Cloud-Unternehmenskonto oder treten Sie einem vorhandenen bei. Detaillierte Verfahren und Anweisungen zum weiteren Vorgehen finden Sie unter Anmeldung für Citrix Cloud.
    2. Melden Sie sich bei an https://citrix.cloud.comund wählen Sie den Kunden aus.
    3. Wählen Sie im Menü **Identitäts- und Zugriffsmanagement** aus und navigieren Sie dann zur Registerkarte **API-Zugriff**, um einen Client für das Konto zu erstellen.
    4. Kopieren Sie die ID, das Geheimnis und die Kunden-ID. Die ID und das Geheimnis sind erforderlich, um den Push-Dienst in Citrix ADC als “ClientID” bzw. “ClientSecret” zu konfigurieren.

> **Wichtig:**
>
> - Dieselben API-Anmeldeinformationen können in mehreren Rechenzentren verwendet werden.
> - Lokale Citrix ADC Appliances müssen in der Lage sein, die Serveradressen mfa.cloud.com und trust.citrixworkspacesapi.net aufzulösen und sind von der Appliance aus zugänglich. Dies soll sicherstellen, dass es keine Firewalls oder IP-Adressblöcke für diese Server über Port 443 gibt.

- Laden Sie die mobile Citrix SSO App aus dem App Store und Play Store für iOS-Geräte bzw. Android-Geräte herunter. Pushbenachrichtigungen werden auf iOS ab Build 1.1.13 auf Android ab 2.3.5 unterstützt.

- Stellen Sie Folgendes für das Active Directory sicher.
  - Die minimale Attributlänge muss mindestens 256 Zeichen betragen.
  - Der Attributtyp muss 'DirectoryString' wie UserParameters sein. Diese Attribute können Zeichenfolgenwerte enthalten.
  - Der Typ der Attributzeichenfolge muss Unicode sein, wenn der Gerätename nicht-englische Zeichen enthält.
  - Der Citrix ADC LDAP-Administrator muss Schreibzugriff auf das ausgewählte AD-Attribut haben.
  - Citrix ADC und der Clientcomputer müssen mit einem gemeinsamen Netzwerkzeitserver synchronisiert werden.

Konfiguration von Pushbenachrichtigungen

Im Folgenden sind die übergeordneten Schritte aufgeführt, die ausgeführt werden müssen, um die Pushbenachrichtigungsfunktion verwenden zu können.

- Der Citrix Gateway-Administrator muss die Schnittstelle für die Verwaltung und Validierung von Benutzern konfigurieren.
  1. Konfigurieren Sie einen Push-Dienst.
  2. Konfigurieren Sie Citrix Gateway für die OTP-Verwaltung und die Endbenutzer-Anmeldung.

     Benutzer müssen ihre Geräte beim Gateway registrieren, um sich bei Citrix Gateway anmelden zu können.
  3. Registrieren Sie Ihr Gerät bei Citrix Gateway.
  4. Melden Sie sich bei Citrix Gateway an.

Erstellen Sie einen Push-Dienst

1. Navigieren Sie zu **Sicherheit** > **AAA-Anwendungsverkehr** > **Richtlinien** > **Authentifizierung** > **Erweiterte Richtlinien** > **Aktionen** > **Push-Dienst** und klicken Sie auf **Hinzufügen**.
2. Geben Sie **unter Name**den Namen des Push-Dienstes ein.
3. Geben Sie im Feld **Client-ID**die eindeutige Identität der vertrauenden Partei für die Kommunikation mit dem Citrix Push-Server in der Cloud ein.
4. Geben Sie in **Client Secret**das eindeutige Geheimnis der vertrauenden Partei für die Kommunikation mit dem Citrix Push-Server in der Cloud ein.
5. Geben Sie im Feld **Kunden-ID**die Kunden-ID oder den Namen des Kontos in der Cloud ein, das zum Erstellen der Client-ID und des Client Secret-Paares verwendet wird.

> **Wichtig**
>
> Die TLS 1.2-Version wird für den Push-Service benötigt. Weitere Informationen finden Sie unter TLS 1.2-Konfigurationsdetails.

Konfigurieren von Citrix Gateway für OTP-Verwaltung und Endbenutzeranmeldung

Führen Sie die folgenden Schritte für die OTP-Verwaltung und die Endbenutzer-Anmeldung aus.

- Erstellen eines Anmeldeschemas für die OTP-Verwaltung
- Konfigurieren des virtuellen Servers für Authentifizierung, Autorisierung und Überwachung
- Konfigurieren von VPN- oder Lastausgleichs-Servern
- Konfigurieren des Policy Label
- Anmeldeschema für Endbenutzer-Anmeldung erstellen

Weitere Informationen zur Konfiguration finden Sie unter Native OTP-Unterstützung.

Wichtig: Für Pushbenachrichtigungen müssen Administratoren Folgendes explizit konfigurieren:

- Erstellen Sie einen Push-Dienst.
- Wählen Sie beim Erstellen eines Anmeldeschemas für die OTP-Verwaltung je nach Bedarf das Anmeldeschema SingleAuthManageOTP.xml oder ein Äquivalent aus.
- Wählen Sie beim Erstellen eines Anmeldeschemas für die Endbenutzeranmeldung je nach Bedarf das Anmeldeschema DualAuthOrPush.xml oder ein Äquivalent aus.

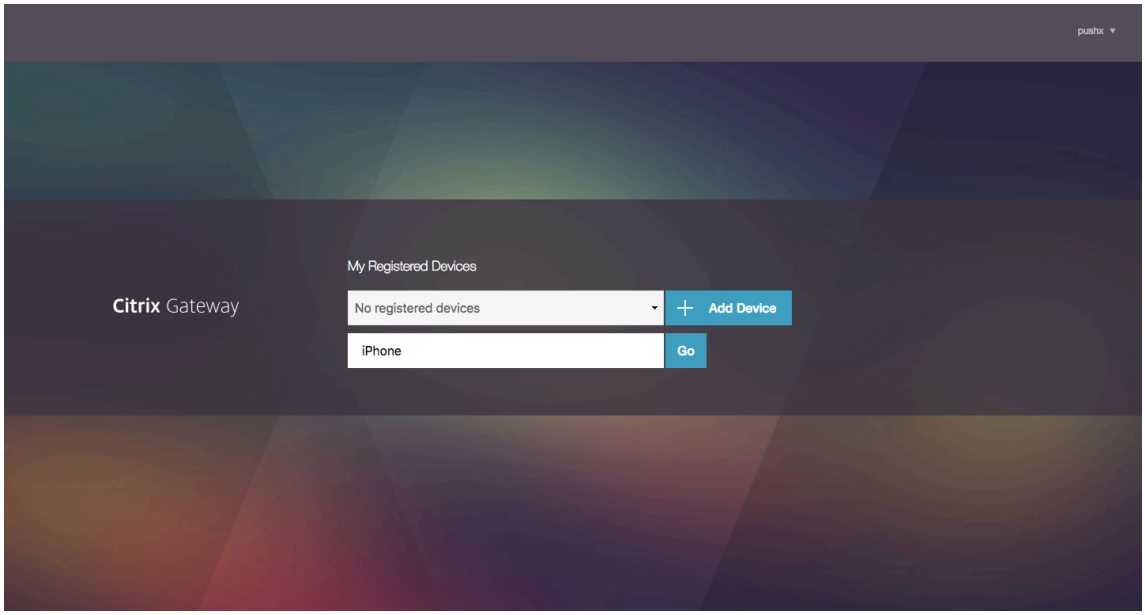
Registrieren Sie Ihr Gerät bei Citrix Gateway

Benutzer müssen ihre Geräte bei Citrix Gateway registrieren, um die Pushbenachrichtigungsfunktion nutzen zu können.

1. Navigieren Sie in Ihrem Webbrowser zu Ihrem Citrix Gateway FQDN und setzen Sie **/manageotp** an den FQDN an.

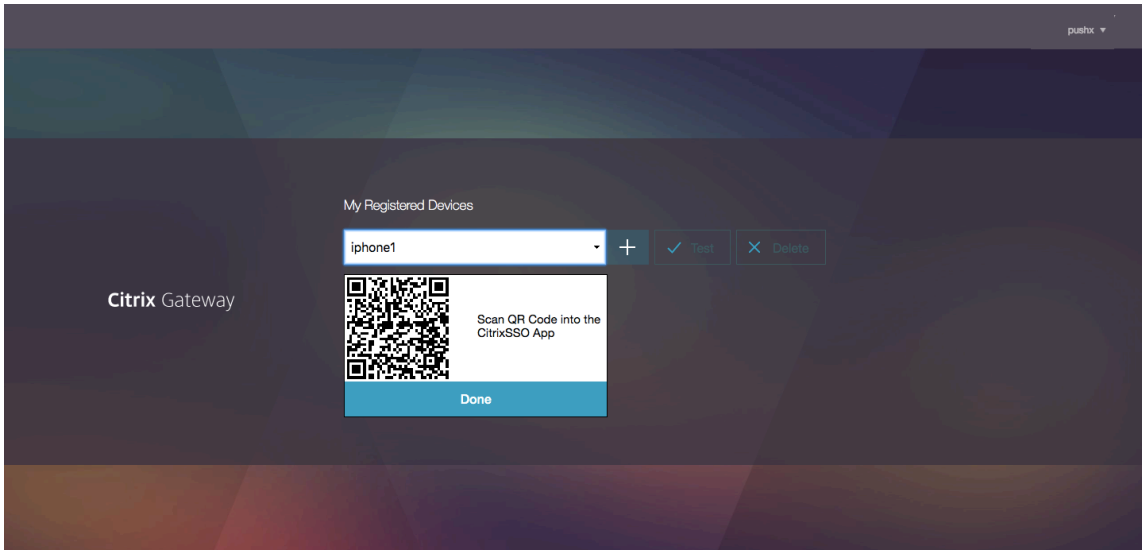
   Dadurch wird die Authentifizierungsseite geladen.
   Beispiel:https://gateway.company.com/manageotp

2. Melden Sie sich je nach Bedarf mit Ihren LDAP-Anmeldeinformationen oder geeigneten Zwei-Faktor-Authentifizierungsmechanismen an.



3. Klicken Sie auf **Gerät hinzufügen**.
4. Geben Sie einen Namen für Ihr Gerät ein und klicken Sie auf **Start**.

   Ein QR-Code wird auf der Citrix Gateway-Browserseite angezeigt.

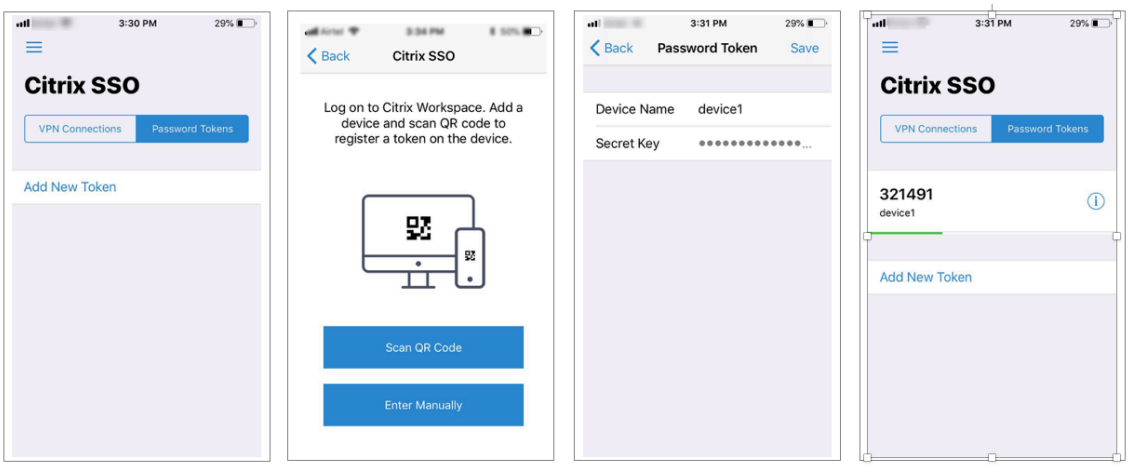


5. Scannen Sie diesen QR-Code mit der Citrix SSO-App von dem zu registrierenden Gerät.

   Citrix SSO validiert den QR-Code und registriert sich dann beim Gateway für Pushbenachrichtigungen. Wenn der Registrierungsprozess keine Fehler aufweist, wird das Token erfolgreich zur Kennwort-Token-Seite hinzugefügt.

   > **Wichtig:**
   >
   > Die Anmeldung schlägt fehl, wenn Sie den im QR-Code angegebenen geheimen Schlüssel

manuell eingeben.



6. Wenn es keine zusätzlichen Geräte zum Hinzufügen/Verwalten gibt, melden Sie sich mit der Liste oben rechts auf der Seite ab.

Testen der Einmalkennwort-Authentifizierung

1. Um das OTP zu testen, klicken Sie in der Liste auf Ihr Gerät und dann auf **Testen**.
2. Geben Sie das OTP ein, das Sie auf Ihrem Gerät erhalten haben, und klicken Sie auf **Los**.

   Die Meldung “OTP-Überprüfung erfolgreich” wird angezeigt.
3. Melden Sie sich mit der Liste oben rechts auf der Seite ab.

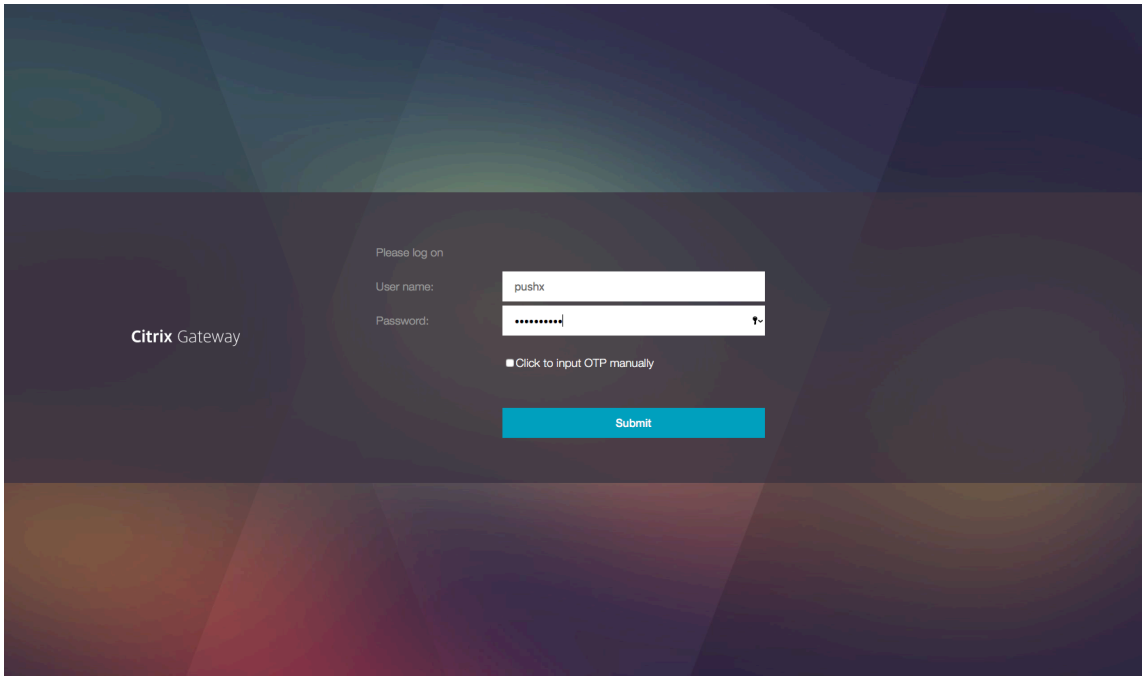
Hinweis: Sie können das OTP-Verwaltungsportal jederzeit verwenden, um die Authentifizierung zu testen, registrierte Geräte zu entfernen oder weitere Geräte zu registrieren.

Melden Sie sich bei Citrix Gateway an

Nach der Registrierung ihrer Geräte bei Citrix Gateway können Benutzer die Pushbenachrichtigungs-funktion für die Authentifizierung verwenden.

1. Navigieren Sie zu Ihrer Citrix Gateway-Authentifizierungsseite (z. B.: https://gateway.company.com)

   Abhängig von der Konfiguration des Anmeldeschemas werden Sie aufgefordert, nur Ihre LDAP-Anmeldeinformationen einzugeben.

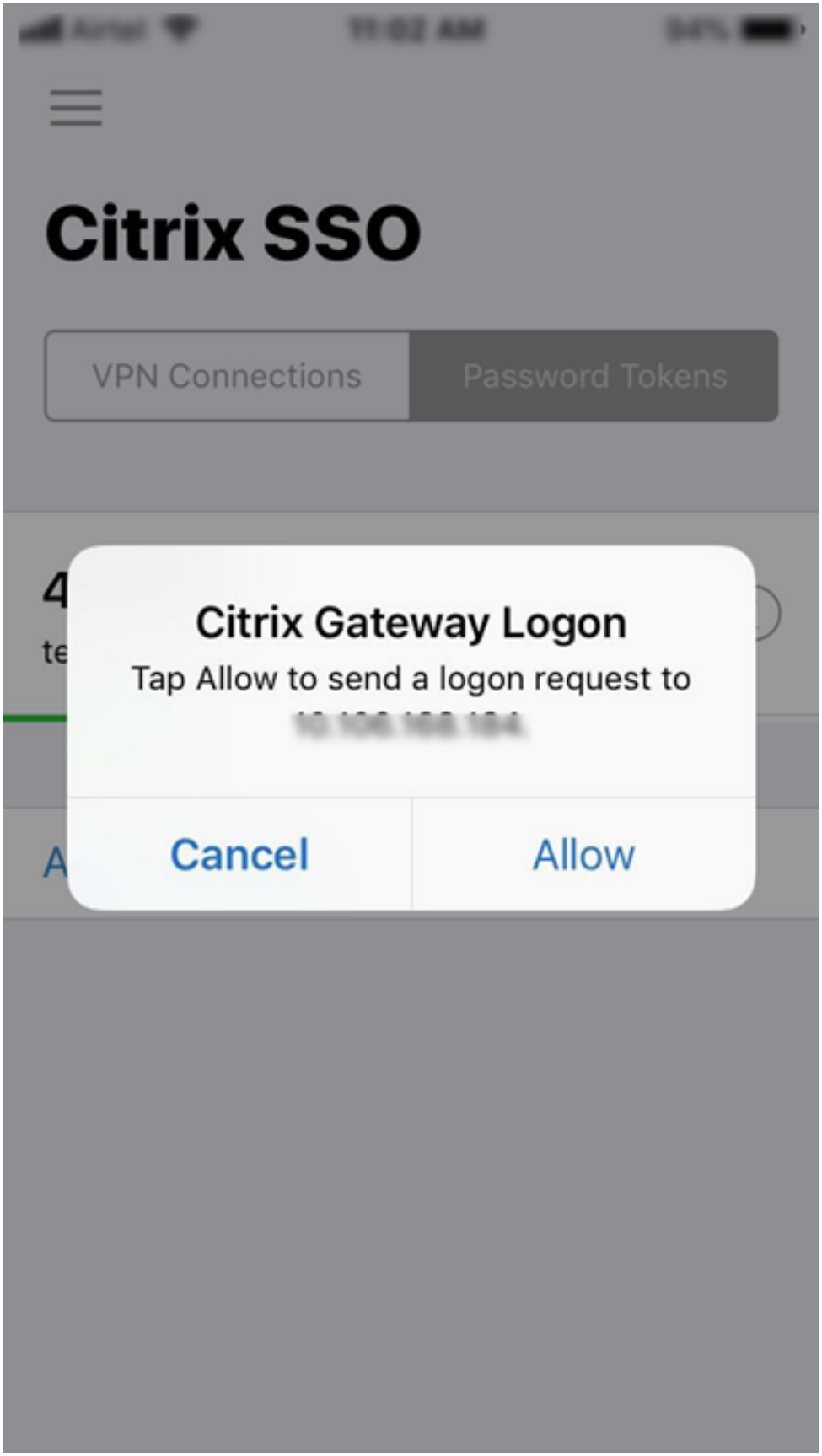


2. Geben Sie Ihren LDAP-Benutzernamen und Ihr Kennwort ein und wählen Sie dann **Senden**aus.

   Eine Benachrichtigung wird an Ihr registriertes Gerät gesendet.

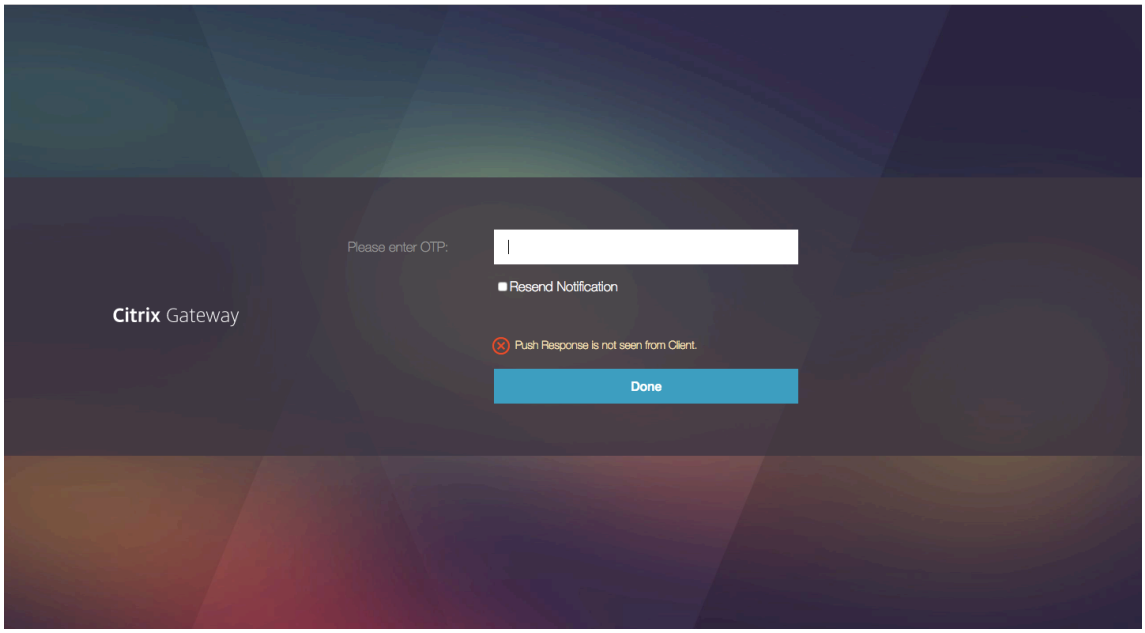
   Hinweis: Wenn Sie das OTP manuell eingeben möchten, müssen Sie **Klicken** auswählen, um OTP manuell einzugeben, und das OTP in das Feld **TOTP** eingeben.

3. Öffnen Sie die Citrix SSO-App auf Ihrem registrierten Gerät und tippen Sie auf **Zulassen**.



Hinweis:

- Auf einem iOS-Gerät werden Sie als zusätzlichen Authentifizierungsfaktor zur Eingabe von Touch-ID/Face-ID/Passcode aufgefordert.
- Der Authentifizierungsserver wartet auf die Antwort der Push-Server-Benachrichtigung, bis der konfigurierte Timeout-Zeitraum abgelaufen ist. Nach dem Timeout zeigt Citrix Gateway die Anmeldeseite an. Die Benutzer können das OTP dann manuell eingeben oder auf Benachrichtigung **erneut senden klicken, um die Benachrichtigung** erneut auf dem registrierten Gerät zu erhalten. Basierend auf der von Ihnen ausgewählten Option validiert das Gateway das von Ihnen eingegebene OTP oder sendet die Benachrichtigung erneut auf Ihrem registrierten Gerät.



- Es wird keine Benachrichtigung über einen Fehler bei der Anmeldung an Ihr registriertes Gerät gesendet.

Bedingungen für Ausfälle

- Die Geräteregistrierung schlägt in den folgenden Fällen möglicherweise fehl.
  - Das Serverzertifikat kann vom Endbenutzergerät nicht vertrauenswürdig sein.
  - Citrix Gateway, das zur Registrierung für OTP verwendet wird, ist für den Client nicht erreichbar.
- Die Benachrichtigungen können in den folgenden Fällen fehlschlagen.
  - Das Benutzergerät ist nicht mit dem Internet verbunden
  - Benachrichtigungen auf dem Benutzergerät sind blockiert
  - Der Benutzer genehmigt die Benachrichtigung auf dem Gerät nicht

In diesen Fällen wartet der Authentifizierungsserver, bis der konfigurierte Timeout-Zeitraum abläuft. Nach dem Timeout zeigt Citrix Gateway eine Anmeldeseite mit den Optionen an, das OTP manuell einzugeben oder die Benachrichtigung erneut auf Ihrem registrierten Gerät zu senden. Basierend auf der ausgewählten Option erfolgt eine weitere Validierung.

Fehler-Protokolle

Im Folgenden sind die erwarteten Protokolle aufgeführt, wenn der OTP-Push-Dienst nicht erreichbar ist.

- Pushbenachrichtigung fehlgeschlagen, wenn das Benutzergerät nicht mit dem Internet verbunden ist - Push: Push Request konnte nicht auf "`client name`" für den Push-Dienst vorbereitet werden.
- Fehlerprotokoll für Geräteregistrierung - Push: Es sind keine Geräte registriert, um die Push-Anfrage an die Cloud für "`client name`" zu senden.
- Falls der Benutzer den Push nicht akzeptiert - Push: Antwort wird vom Client nicht gesehen, für "`user name`", überprüfen Sie die Wiederholungsoptionen.

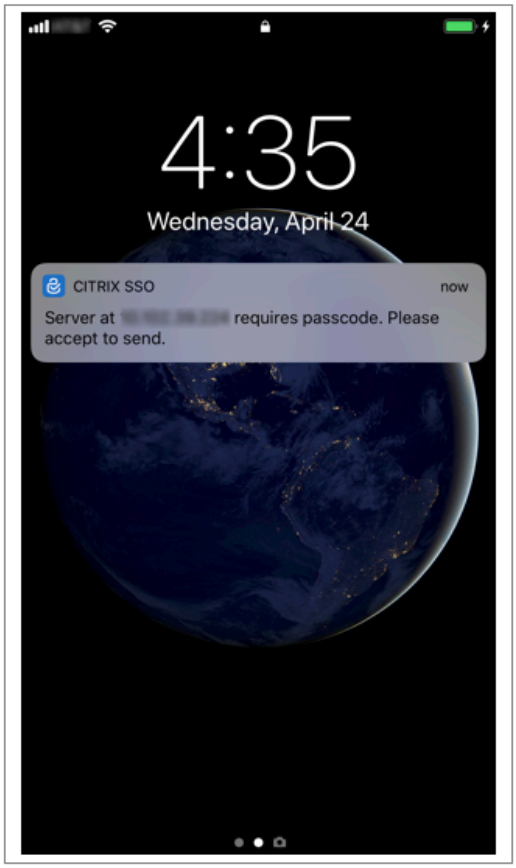
Citrix SSO-App-Verhalten unter iOS — weist darauf hin

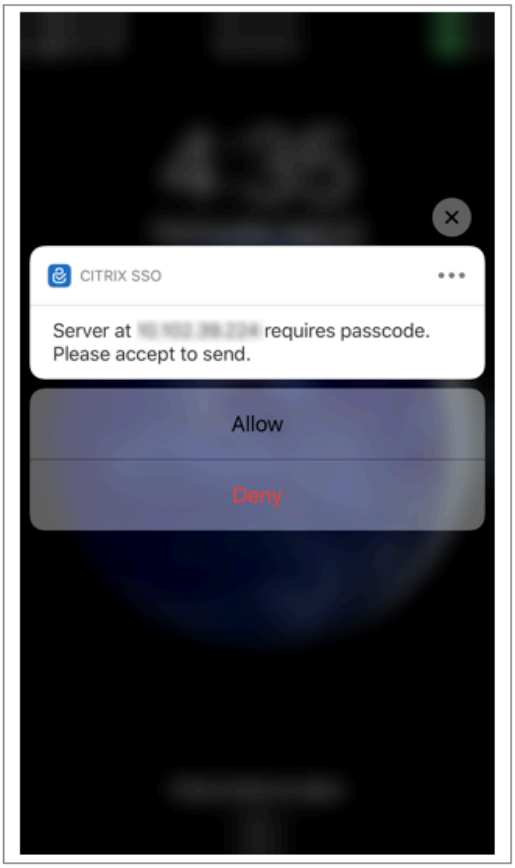
Verknüpfungen für Benachrichtigungen

Die Citrix SSO iOS-App bietet Unterstützung für umsetzbare Benachrichtigungen, um die Benutzerfreundlichkeit zu verbessern. Sobald eine Benachrichtigung auf einem iOS-Gerät eingegangen ist und das Gerät gesperrt ist oder sich die Citrix SSO-App nicht im Vordergrund befindet, können Benutzer die in der Benachrichtigung integrierten Verknüpfungen verwenden, um die Anmeldeanfrage entweder zu genehmigen oder abzulehnen.

Um auf Benachrichtigungsverknüpfungen zuzugreifen, müssen Benutzer je nach Hardware des Geräts entweder eine Berührung erzwingen (3D-Touch) oder die Benachrichtigung lange drücken. Durch Auswahl der Aktion Verknüpfung zulassen wird eine Anmeldeanfrage an Citrix ADC gesendet. Abhängig davon, wie die Authentifizierungsrichtlinie für den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver konfiguriert ist;

- Die Anmeldeanfrage kann im Hintergrund gesendet werden, ohne dass die App im Vordergrund gestartet oder das Gerät entsperrt werden muss.
- Die App fordert möglicherweise als zusätzlichen Faktor zur Eingabe von Touch-ID/Face-ID/Passcode auf. In diesem Fall wird die App in den Vordergrund gestartet.



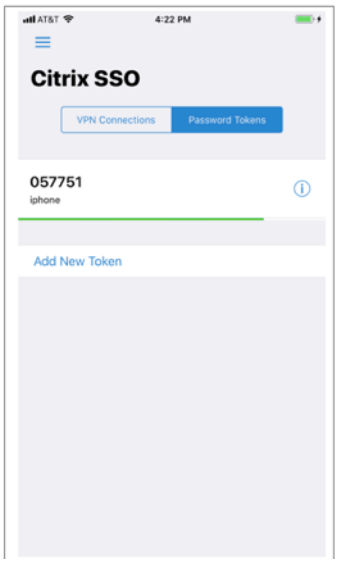


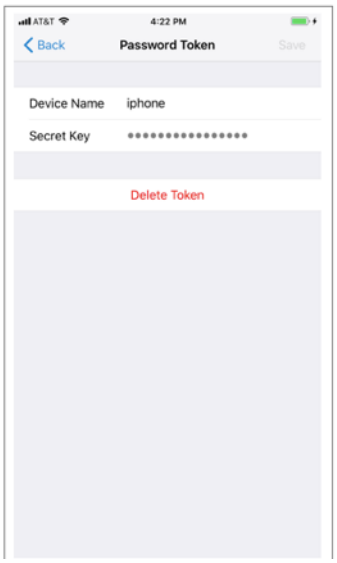
Löschen von Kennwort-Token von Citrix SSO

1. Um ein für Push registriertes Kennwort-Token in der Citrix SSO-App zu löschen, müssen Benutzer die folgenden Schritte ausführen:
2. Heben Sie die Registrierung des iOS/Android-Geräts auf dem Gateway auf (entfernen). Der QR-Code zum Entfernen der Registrierung vom Gerät wird angezeigt.
3. Öffnen Sie die Citrix SSO-App und tippen Sie auf die Info-Schaltfläche des zu löschenden Kennwort-Tokens.
4. Tippen **Sie auf Token löschen** und scannen Sie den QR-Code.

Hinweis:

- Wenn der QR-Code gültig ist, wird das Token erfolgreich aus der Citrix SSO-App entfernt.
- Benutzer können auf Löschen erzwingen tippen, um ein Kennwort-Token zu löschen, ohne den QR-Code scannen zu müssen, wenn das Gerät bereits aus dem Gateway entfernt wurde. Erzwungenes Löschen kann dazu führen, dass das Gerät weiterhin Benachrichtigungen erhält, wenn das Gerät nicht aus Citrix Gateway entfernt wurde.





E-Mail-OTP-Authentifizierung

March 8, 2022

E-Mail-OTP wird mit Citrix ADC 12.1 Build 51.x eingeführt. Mit der E-Mail-OTP-Methode können Sie sich mit dem Einmalkennwort (OTP) authentifizieren, das an die registrierte E-Mail-Adresse gesendet wird. Wenn Sie versuchen, sich bei einem Dienst zu authentifizieren, sendet der Server ein OTP an die registrierte E-Mail-Adresse des Benutzers.

Um die E-Mail-OTP-Funktion nutzen zu können, müssen Sie zuerst Ihre alternative E-Mail-ID registrieren. Eine alternative E-Mail-ID-Registrierung ist erforderlich, damit das OTP an diese E-Mail-ID gesendet werden kann, da Sie bei einer Kontosperrung oder wenn Sie das AD-Kennwort vergessen haben, nicht auf die primäre E-Mail-ID zugreifen können.

Sie können die E-Mail-OTP-Validierung ohne E-Mail-ID-Registrierung verwenden, wenn Sie die alternative E-Mail-ID bereits als Teil eines AD-Attributs angegeben haben. Sie können in der E-Mail-Aktion auf dasselbe Attribut verweisen, anstatt die alternative E-Mail-ID im Abschnitt E-Mail-Adresse anzugeben.

Voraussetzungen

Bevor Sie die E-Mail-OTP-Funktion konfigurieren, sollten Sie die folgenden Voraussetzungen prüfen:

- Citrix ADC Feature Release 12.1 Build 51.28 und höher
- Die E-Mail-OTP-Funktion ist nur im nFactor-Authentifizierungsablauf verfügbar.
  - Weitere Einzelheiten finden Sie unter https://support.citrix.com/pages/citrix-adc-authentication-how#nfactor

- Unterstützt für AAA-TM, Citrix Gateway (Browser, Native Plug-in und Receiver).

Active Directory-Einstellung

- Unterstützte Version ist 2016/2012 und 2008 Active Directory-Domänenfunktionsebene
- Der Benutzername von Citrix ADC LdapBind muss Schreibzugriff auf den AD-Pfad des Benutzers haben

E-Mail Server

- Stellen Sie sicher, dass die Anmeldungsbasierte Authentifizierung auf dem SMTP-Server aktiviert ist, damit die E-Mail-OTP-Lösung funktioniert. Citrix ADC unterstützt nur die auf AUTH LOGIN basierende Authentifizierung, damit E-Mail-OTP funktioniert.
- Um sicherzustellen, dass die auf AUTH LOGIN basierende Authentifizierung aktiviert ist, geben Sie den folgenden Befehl auf dem SMTP-Server ein. Wenn die anmeldungsbasierte Authentifizierung aktiviert ist, stellen Sie fest, dass der Text AUTH LOGIN in der Ausgabe **fett** angezeigt wird.

```
root@ns# telnet <IP address of the SMTP server><Port number of the server>
ehlo
root@ns# telnet 10.106.3.
Trying 10.106.  ...
Connected to 10.106.  .
Escape character is '^]'.
220 E2K13.NSGSanity.com Microsoft ESMTP MAIL Service ready at Fri, 22 Nov
2019 16:24:17 +0530
ehlo
250-E2K13.NSGSanity.com Hello [10.221.  ]
250-SIZE 37748736
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-X-ANONYMOUSTLS
250-AUTH LOGIN
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 XRDST
For information on how to enable login based authentication, see
https://support.microfocus.com/kb/doc.php?id=7020367
```

Einschränkungen

- Diese Funktion wird nur unterstützt, wenn das Authentifizierungs-Backend LDAP ist.
- Die bereits registrierte alternative E-Mail-ID wurde nicht angezeigt.
- Nur die alternative E-Mail-ID von der KBA-Registrierungsseite kann nicht aktualisiert werden.
- Die E-Mail-OTP-Authentifizierung kann nicht der erste Faktor im Authentifizierungsablauf sein. Dies ist beabsichtigt, um eine robuste Authentifizierung zu erreichen.

- Wenn sowohl alternative E-Mail-ID als auch KBA mit derselben Authentifizierungsaktion konfiguriert wurden, muss das Attribut für beide identisch sein.
- Für das native Plug-in und Receiver wird die Registrierung nur über einen Browser unterstützt.

Active Directory-Konfiguration

- E-Mail-OTP verwendet das Active Directory-Attribut als Benutzerdatenspeicher.
- Nachdem Sie die alternative E-Mail-ID registriert haben, wird die E-Mail-ID an die Citrix ADC-Appliance gesendet, und die Appliance speichert sie im konfigurierten KB-Attribut im AD-Benutzerobjekt.
- Die alternative E-Mail-ID wird verschlüsselt und im konfigurierten AD-Attribut gespeichert.

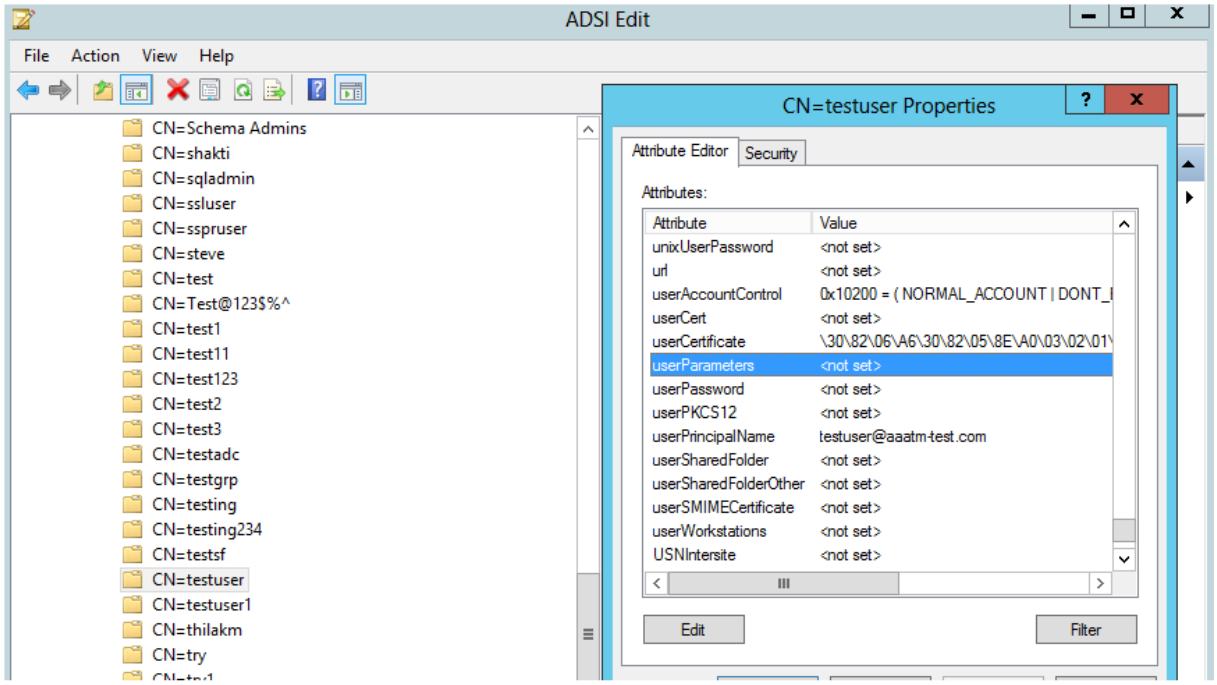
Beachten Sie beim Konfigurieren eines AD-Attributs Folgendes:

- Die unterstützte Länge des Attributnamens muss mindestens 128 Zeichen lang sein.
- Der Attributtyp muss “DirectoryString” sein.
- Dasselbe AD-Attribut kann für Native OTP- und E-Mail-OTP-Registrierungsdaten verwendet werden.
- Der LDAP-Administrator muss Schreibzugriff auf das ausgewählte AD-Attribut haben.

Verwenden vorhandener Attribute

Das in diesem Beispiel verwendete Attribut ist `Userparameters`. Da es sich um ein vorhandenes Attribut innerhalb des AD-Benutzers handelt, müssen Sie keine Änderungen am AD selbst vornehmen. Sie müssen jedoch sicherstellen, dass das Attribut nicht verwendet wird.

Um sicherzustellen, dass das Attribut nicht verwendet wird, navigieren Sie zu **ADSI** und wählen Sie Benutzer aus, klicken Sie mit der rechten Maustaste auf den Benutzer und scrollen Sie nach unten zur Attributliste. Sie müssen sehen, dass der Attributwert für **UserParametersnicht festgelegt ist**. Dies deutet darauf hin, dass das Attribut derzeit nicht verwendet wird.



Konfigurieren von E-Mail-OTP

Die E-Mail-OTP-Lösung besteht aus den folgenden zwei Teilen:

- E-Mail-Registrierung
- E-Mail-Validierung

Registrierung der E-Mail-ID

Führen Sie die folgende Konfiguration über die CLI durch, nachdem das KBA-Registrierungsschema erfolgreich erstellt wurde:

1. Binden Sie das Portalthema und das Zertifikat an VPN Global.

```
bind authentication vserver authvs -portaltheme RfWebUI
bind vpn global -userDataEncryptionKey c1
<!--NeedCopy-->
```

> **Hinweis:**
>
> Eine vorhergehende Zertifikatsbindung ist erforderlich, um die im AD-Attribut gespeicherten Benutzerdaten (KB Q&A und alternative Mail-ID registriert) zu verschlüsseln.

2. Erstellen Sie eine LDAP-Authentifizierungsrichtlinie.


```
add authentication ldapAction ldap -serverIP 10.102.2.2 -
    serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -ldapBindDn
    administrator@aaatm-test.com -ldapBindDnPassword freebsd -
    ldapLoginName samAccountName -secType SSL
add authentication Policy ldap -rule true -action ldap
<!--NeedCopy-->
```

3. Erstellen Sie eine LDAP-Authentifizierungsrichtlinie für die E-Mail-Registrierung.

```
add authentication ldapAction ldap_email_registration -serverIP
    10.102.2.2 -serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -
    ldapBindDn administrator@aaatm-test.com -ldapBindDnPassword
    freebsd -ldapLoginName samAccountName -secType SSL -KBAttribute
     userParameters -alternateEmailAttr userParameters
add authentication Policy ldap_email_registration -rule true -
    action ldap_email_registration
<!--NeedCopy-->
```

4. Erstellen Sie ein Anmeldeschema für die E-Mail-Registrierung und eine Policy Label.

```
add authentication loginSchema onlyEmailRegistration -
    authenticationSchema /nsconfig/loginschema/LoginSchema/
    AltEmailRegister.xml
add authentication policylabel email_Registration_factor -
    loginSchema onlyEmailRegistration
bind authentication policylabel email_Registration_factor -
    policyName ldap_email_registration -priority 1 -
    gotoPriorityExpression NEXT
<!--NeedCopy-->
```

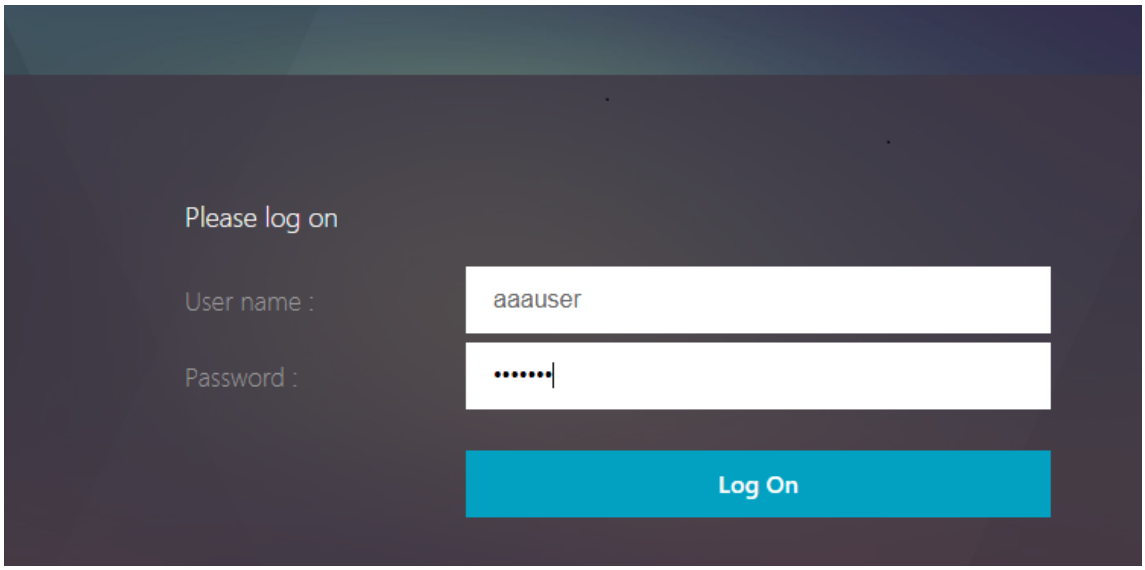
5. Binden Sie die Authentifizierungsrichtlinie an den virtuellen Authentifizierungsserver.

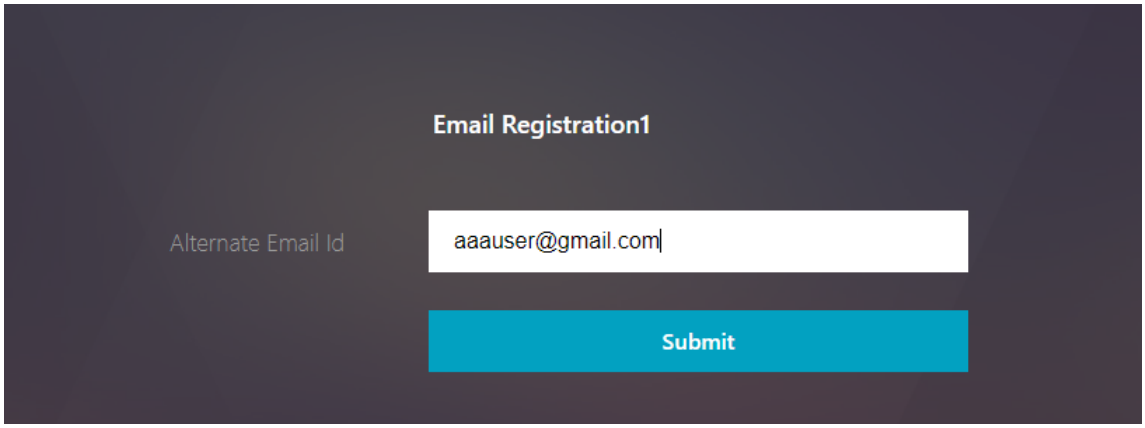
```
bind authentication vserver authvs  - policy ldap -priority 1 -
    nextFactor email_Registration_factor -gotoPriorityExpression
    NEXT
<!--NeedCopy-->
```

6. Nachdem Sie alle in den vorherigen Abschnitten genannten Schritte konfiguriert haben, müssen Sie den folgenden GUI-Bildschirm sehen. Wenn Sie beispielsweise über die URL

zugreifen, wird https://lb1.server.com/ Ihnen eine erste Anmeldeseite angezeigt, für die nur die LDAP-Anmeldeinformationen erforderlich sind, gefolgt von einer alternativen E-Mail-Registrierungsseite.

Hinweis: Die Domäne https://lb1.server.com/ kann entweder zum Gateway oder zu einem virtuellen Authentifizierungsserver gehören.





Hinweis:

- Sie können dasselbe Authentifizierungsschema sowohl für die KBA-Registrierung als auch für die E-Mail-ID-Registrierung verwenden.
- Bei der Konfiguration der KBA-Registrierung können Sie im Abschnitt **E-Mail-Registrierung die Option Alternative E-Mail registrieren** wählen, um eine alternative E-Mail-ID zu registrieren.

E-Mail-Validierung

Führen Sie die folgenden Schritte für die E-Mail-Validierung aus.

1. Binden Sie das Portal-Thema und das Zertifikat an VPN Global

```
bind authentication vserver authvs -portaltheme RfWebUI
bind vpn global -userDataEncryptionKey c1
<!--NeedCopy-->
```

> **Hinweis:**
>
> Die vorherige Zertifikatsbindung ist erforderlich, um die im AD-Attribut gespeicherten Benutzerdaten (KB Q&A und alternative E-Mail-ID registriert) zu entschlüsseln.

2. Erstellen Sie eine LDAP-Authentifizierungsrichtlinie. LDAP muss ein wichtiger Faktor für den E-Mail-Validierungsfaktor sein, da Sie die E-Mail-ID oder die alternative E-Mail-ID des Benutzers für die E-Mail-OTP-Validierung benötigen.

```
add authentication ldapAction ldap1 -serverIP 10.102.2.2 -
    serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -   ldapBindDn
    administrator@aaatm-test.com -ldapBindDnPassword freebsd -
    ldapLoginName samAccountName -secType SSL -KBAttribute
    userParameters -alternateEmailAttr userParameters
add authentication Policy ldap1 -rule true -action ldap1
<!--NeedCopy-->
```

3. Erstellen Sie eine E-Mail-Authentifizierungsrichtlinie.

```
add authentication emailAction email -userName sqladmin@aaa.com -
    password freebsd-encrypted -encryptmethod ENCMTHD_3 -serverURL
    "smtps://10.2.3.3:25" -content "OTP is $code" -
    defaultAuthenticationGroup emailgrp -emailAddress "aaa.user.
    attribute("alternate_mail")"
add authentication Policy email -rule true  - action email
<!--NeedCopy-->
```

In dem zuvor erwähnten Befehl ist die **E-Mail-Adresse** die alternative E-Mail-ID, die bei der KBA-Registrierung angegeben wurde.

4. Erstellen Sie eine E-Mail-OTP-Validierungsrichtlinienbezeichnung.

```
add authentication policylabel email_Validation_factor
```



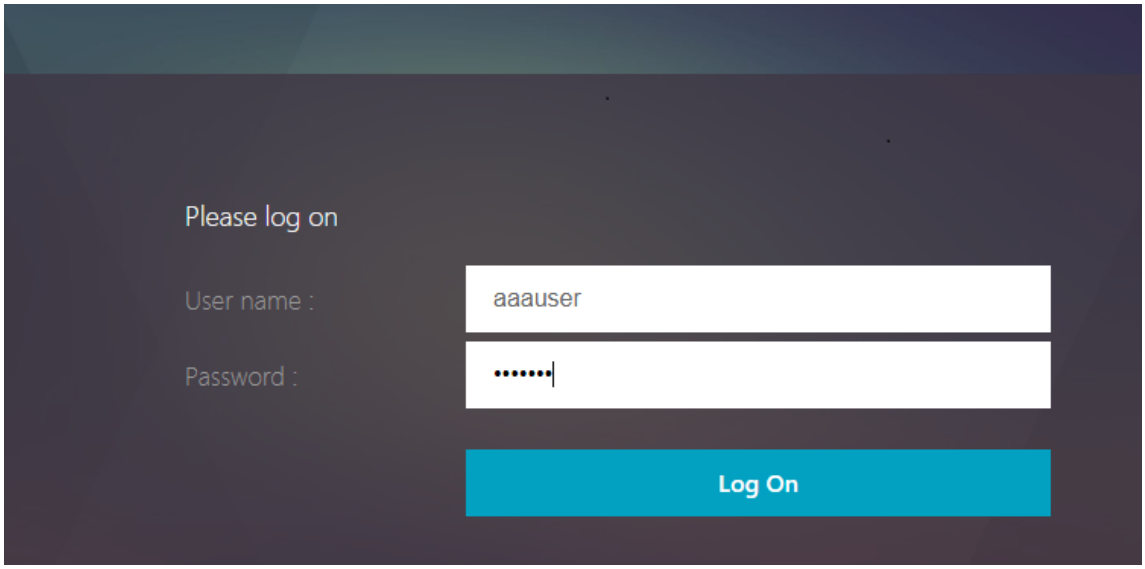
```
2 bind authentication policylabel email_Validation_factor -
     policyName email -priority 1 -gotoPriorityExpression NEXT
3 <!--NeedCopy-->
```

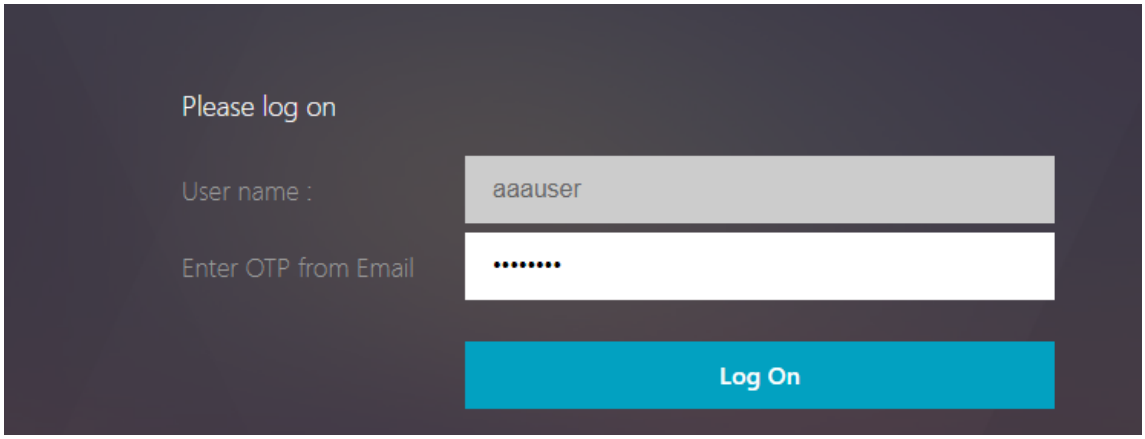
5. Binden Sie die Authentifizierungsrichtlinie an den virtuellen Authentifizierungsserver.

```
1 bind authentication vserver authvs - policy ldap1 -priority 1 -
     nextFactor email_Validation_factor -gotoPriorityExpression NEXT
2 <!--NeedCopy-->
```

6. Nachdem Sie alle in den vorherigen Abschnitten genannten Schritte konfiguriert haben, müssen Sie den folgenden GUI-Bildschirm für die E-Mail-OTP-Validierung sehen. Wenn Sie beispielsweise über die URL zugreifen, wird https://lb1.server.com/ Ihnen eine erste Anmeldeseite angezeigt, für die nur die LDAP-Anmeldeinformationen erforderlich sind, gefolgt von der Seite “EMAIL OTP-Validierung”.

> **Hinweis:**
>
> In der LDAP-Richtlinie muss konfiguriert werden, dass `alternateEmailAttr` die E-Mail-ID des Benutzers vom AD-Attribut abgefragt werden kann.





Problembehandlung

Bevor Sie das Protokoll analysieren, ist es besser, die Protokollebene wie folgt auf Debuggen festzulegen.

```
set syslogparams -loglevel DEBUG
<!--NeedCopy-->
```

Registrierung - Erfolgreiches Szenario

Die folgenden Einträge weisen auf eine erfolgreiche Benutzerregistrierung hin.

```
”ns_aaa_insert_hash_keyValue_entry key:kba_registered value:1”
Nov 14 23:35:51 <local0.debug> 10.102.229.76 11/14/2018:18:05:51 GMT
    0-PPE-1 : default SSLVPN Message 1588 0 :  ”
    ns_aaa_insert_hash_keyValue_entry key:alternate_mail value:
    eyJ2ZXJzaW9uIjoiMSIsICJraWQiOiIxbk1oWjN0T2NjLVVvZUx6NDRwZFhxdS01dTA9IiwgImtleS
    ==.oKmvOalaOJ3a9z7BcGCSegNPMw==”

<!--NeedCopy-->
```

Registrierung — Ausfallszenario

Auf der Benutzeranmeldeseite wird die folgende Fehlermeldung angezeigt: “Ihre Anfrage kann nicht abgeschlossen werden”. Dies deutet darauf hin, dass der Cert-Key, der zum Verschlüsseln der Benutzerdaten an das globale VPN gebunden werden soll, fehlt.


```
Jul 31 08:51:46 <local0.info> 10.102.229.79 07/31/2020:03:21:4 6 GMT 0-PPE-1 : default SSLVPN Message 696 0 :  "Encrypt UserData: No Encryption cert is bound to vpn global"
Jul 31 08:51:46 <local0.info> 10.102.229.79 07/31/2020:03:21:46 GMT  0-PPE-1 : default SSLVPN Message 697 0 :  "KBA Register: Alternate email id Encrypted blob length is ZERO aaauser"
<!--NeedCopy-->
```

E-Mail-Validierung — Erfolgreiches Szenario

Die folgenden Einträge weisen auf eine erfolgreiche E-Mail-OTP-Validierung hin.

```
"NFactor: Successfully completed email auth, nextfactor is pwd_reset"
<!--NeedCopy-->
```

E-Mail-Validierung — Ausfallszenario

Auf der Benutzeranmeldeseite wird die Fehlermeldung "Ihre Anfrage kann nicht abgeschlossen werden" angezeigt. Dies bedeutet, dass die anmeldungsbasierte Authentifizierung auf dem E-Mail-Server nicht aktiviert ist und dasselbe aktiviert werden muss.

```
" /home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/pocomail.cpp [100]: void ThreadWorker_SendMailJob(SMTPJob*) 0-215: [POCO][JobID: 8]SMTP Configuration is Secure..
/home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/pocomail.cpp[108]: void ThreadWorker_SendMailJob(SMTPJob*) 0-215: [POCO][JobID: 8] First login succeeded
Wed Mar  4 17:16:28 2020
/home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/naaad.c[697]: main 0-0: timer 2 firing...
/home/build/rs_130_36_15_RTM/usr.src/netscaler/aaad/pocomail.cpp[127]: void ThreadWorker_SendMailJob(SMTPJob*) 0-0: [POCO-ERROR][JobID: 8] Poco SMTP Mail Dispatch  Failed. SMTP TYPE:1, SMTPException: Exception occurs. SMTP Exception: The mail service does not support LOGIN authentication: 250-smtprelay.citrix.com Hello [10.9.154.239]
250-SIZE 62914560
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
```



```
250-8BITMIME
250-BINARYMIME
250 CHUNKING
<!--NeedCopy-->
```

reCAPTCHA Konfiguration für nFactor Authentifizierung

October 5, 2021

Citrix Gateway unterstützt eine neue First-Class-Aktion 'CaptChaAction', die die reCAPTCHA-Konfiguration vereinfacht. Da reCAPTCHA eine erstklassige Aktion ist, kann es ein Faktor für sich sein. Sie können reCAPTCHA überall im nFactor Flow injizieren.

Zuvor mussten Sie benutzerdefinierte WebAuth Richtlinien mit Änderungen an der RFWeb UI schreiben. Mit der Einführung von CaptChaAction müssen Sie das JavaScript nicht ändern.

> **Wichtig**
>
> Wenn reCAPTCHA zusammen mit Benutzernamen oder Kennwortfeldern im Schema verwendet wird, wird die Schaltfläche Senden deaktiviert, bis reCAPTCHA erfüllt ist.

reCAPTCHA Konfiguration

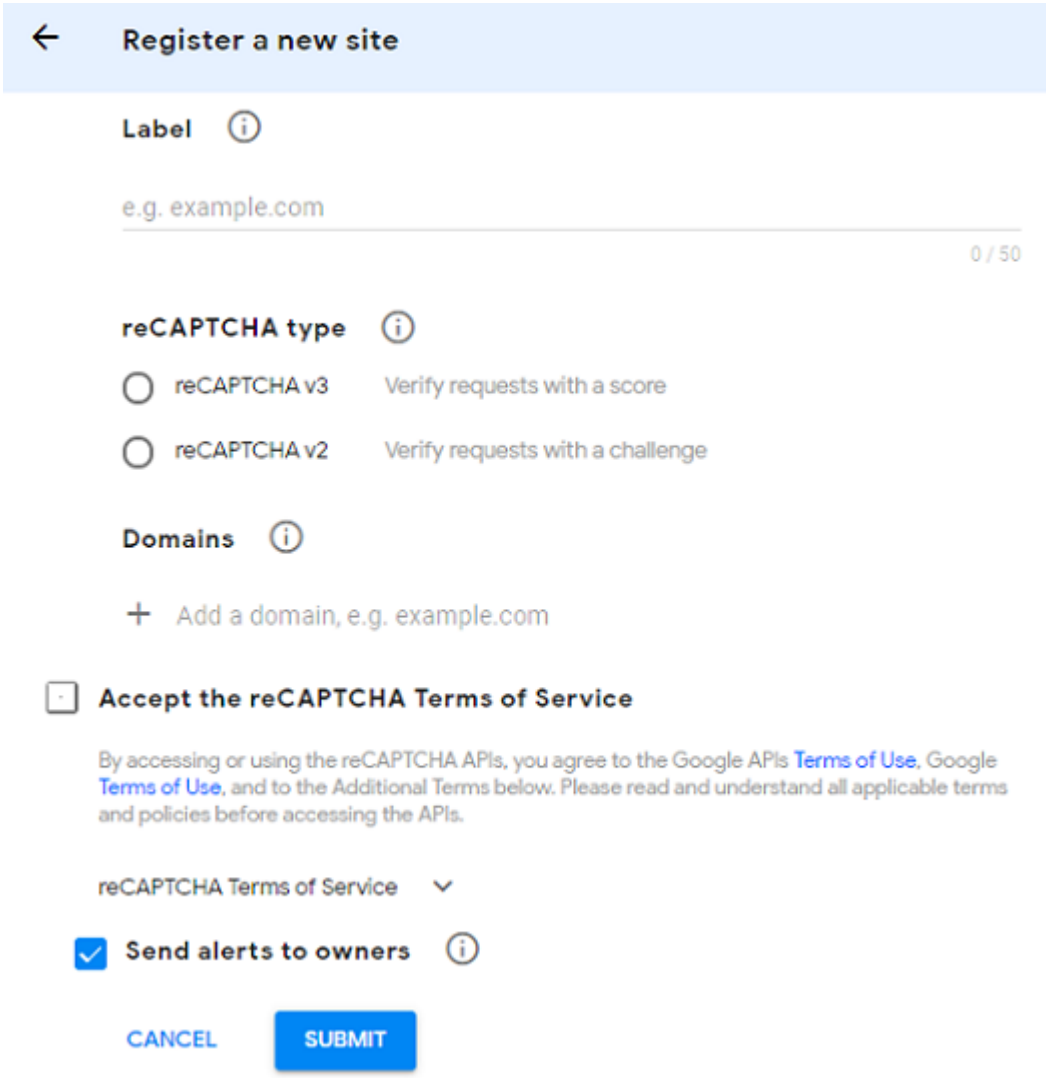
Die reCAPTCHA Konfiguration besteht aus zwei Teilen.

1. Konfiguration auf Google für die Registrierung von reCAPTCHA.
2. Konfiguration auf der Citrix ADC Appliance zur Verwendung von reCAPTCHA als Teil des Anmeldeflusses.

reCAPTCHA Konfiguration auf Google

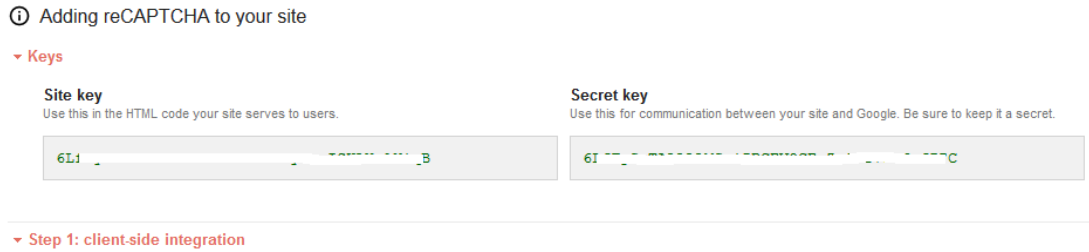
Registrieren Sie eine Domain für reCAPTCHA unter https://www.google.com/recaptcha/admin.

1. Wenn Sie zu dieser Seite navigieren, wird der folgende Bildschirm angezeigt.



> **Hinweis:**
>
> Verwenden Sie reCAPTCHA v2 nur. Unsichtbares reCAPTCHA befindet sich noch in der Beta.

2. Nach der Registrierung einer Domain werden der SiteKey und SecretKey angezeigt.



> **Hinweis:**
>
> Der SiteKey und SecretKey sind aus Sicherheitsgründen ausgegraut. SecretKey muss

> sicher aufbewahrt werden.

reCAPTCHA Konfiguration auf der Citrix ADC Appliance

Die reCAPTCHA Konfiguration auf der Citrix ADC Appliance kann in drei Teile unterteilt werden:

- Bildschirm reCAPTCHA anzeigen
- Senden Sie die reCAPTCHA Antwort auf den Google-Server
- LDAP-Konfiguration ist der zweite Faktor für die Benutzeranmeldung (optional)

Bildschirm reCAPTCHA anzeigen

Die Anpassung des Anmeldeformulars erfolgt über das Loginschema SingleAuthCaptcha.xml. Diese Anpassung wird auf dem virtuellen Authentifizierungsserver angegeben und an die Benutzeroberfläche zum Rendern des Anmeldeformulars gesendet. Das integrierte Anmeldeschema SingleAuthCaptcha.xml befindet sich im Verzeichnis /nsconfig/loginschema/loginSchema auf der Citrix ADC Appliance.

> **Wichtig**
>
> - Basierend auf Ihrem Anwendungsfall und verschiedenen Schemas können Sie das vorhandene Schema ändern. Zum Beispiel, wenn Sie nur reCAPTCHA Faktor (ohne Benutzername oder Kennwort) oder doppelte Authentifizierung mit reCAPTCHA benötigen.
> - Wenn benutzerdefinierte Änderungen durchgeführt oder die Datei umbenannt wird, empfiehlt Citrix, alle LoginSchemas aus dem Verzeichnis /nsconfig/loginschema/loginSchema in das übergeordnete Verzeichnis /nsconfig/loginschema zu kopieren.

So konfigurieren Sie die Anzeige von reCAPTCHA mit CLI

- `add authentication loginSchema singleauthcaptcha -authenticationSchema /nsconfig/loginschema/SingleAuthCaptcha.xml`
- `add authentication loginSchemaPolicy singleauthcaptcha -rule true -action singleauthcaptcha`
- `add authentication vserver auth SSL <IP> <Port>`
- `add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to-key-file>`
- `bind ssl vserver auth -certkey vserver-cert`
- `bind authentication vserver auth -policy singleauthcaptcha -priority 5 -gotoPriorityExpression END`

Senden Sie die reCAPTCHA Antwort auf den Google-Server

Nachdem Sie die reCAPTCHA konfiguriert haben, die den Benutzern angezeigt werden muss, fügen Administratoren Post die Konfiguration auf den Google-Server hinzu, um die reCAPTCHA Antwort vom Browser zu überprüfen.

So überprüfen Sie reCAPTCHA Antwort vom Browser

- `add authentication captchaAction myrecaptcha -sitekey <sitekey-copied-from-google> -secretkey <secretkey-from-google>`
- `add authentication policy myrecaptcha -rule true -action myrecaptcha`
- `bind authentication vserver auth -policy myrecaptcha -priority 1`

Die folgenden Befehle sind erforderlich, um zu konfigurieren, ob AD-Authentifizierung gewünscht ist. Andernfalls können Sie diesen Schritt ignorieren.

- `add authentication ldapAction ldap-new -serverIP x.x.x.x -serverPort 636 -ldapBase "cn=users,dc=aaatm,dc=com"-ldapBindDn adminuser@aaatm.com -ldapBindDnPassword <password> -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName memberof -subAttributeName CN -secType SSL -passwdChange ENABLED -defaultAuthenticationGroup ldapGroup`
- `add authenticationpolicy ldap-new -rule true -action ldap-new`

LDAP-Konfiguration ist der zweite Faktor für die Benutzeranmeldung (optional)

Die LDAP-Authentifizierung erfolgt nach reCAPTCHA, Sie fügen sie dem zweiten Faktor hinzu.

- `add authentication policylabel second-factor`
- `bind authentication policylabel second-factor -policy ldap-new -priority 10`
- `bind authentication vserver auth -policy myrecaptcha -priority 1 -nextFactor second-factor`

Der Administrator muss entsprechende virtuelle Server hinzufügen, je nachdem, ob der virtuelle Lastenausgleich oder die Citrix Gateway Appliance für den Zugriff verwendet wird. Der Administrator muss den folgenden Befehl konfigurieren, wenn ein virtueller Lastausgleichsserver erforderlich ist:

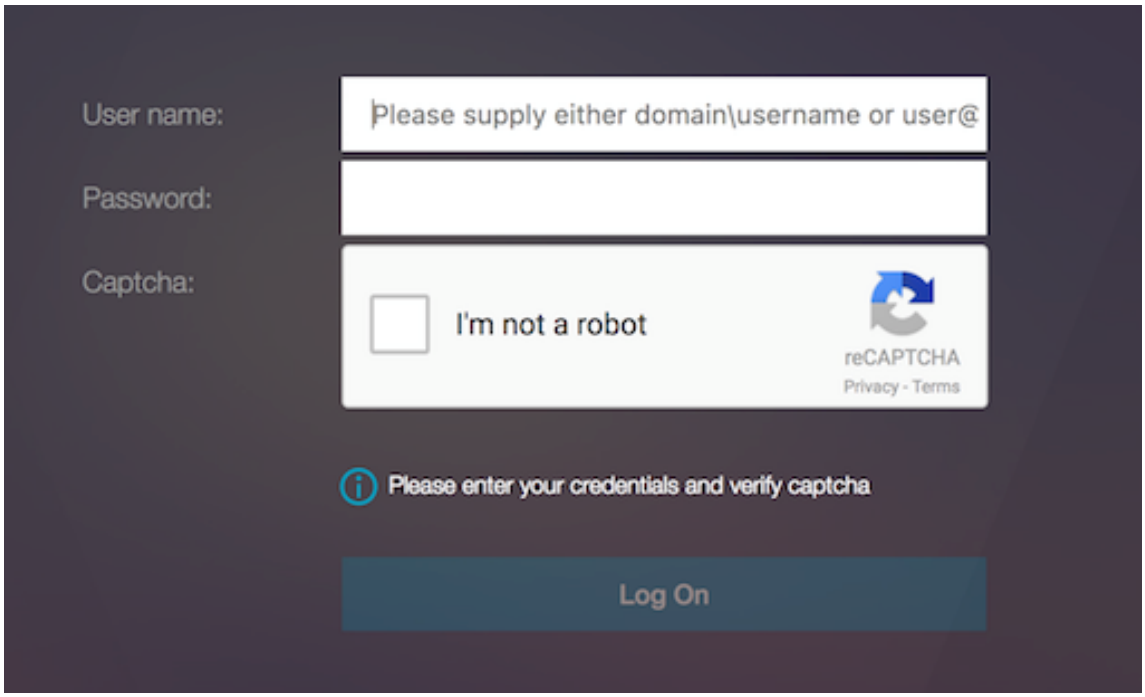
- `add lb vserver lbtest HTTP <IP> <Port> -authentication ON -authenticationHost nssp.aaatm.com`

  nssp.aaatm.com — Löst den virtuellen Authentifizierungsserver auf.

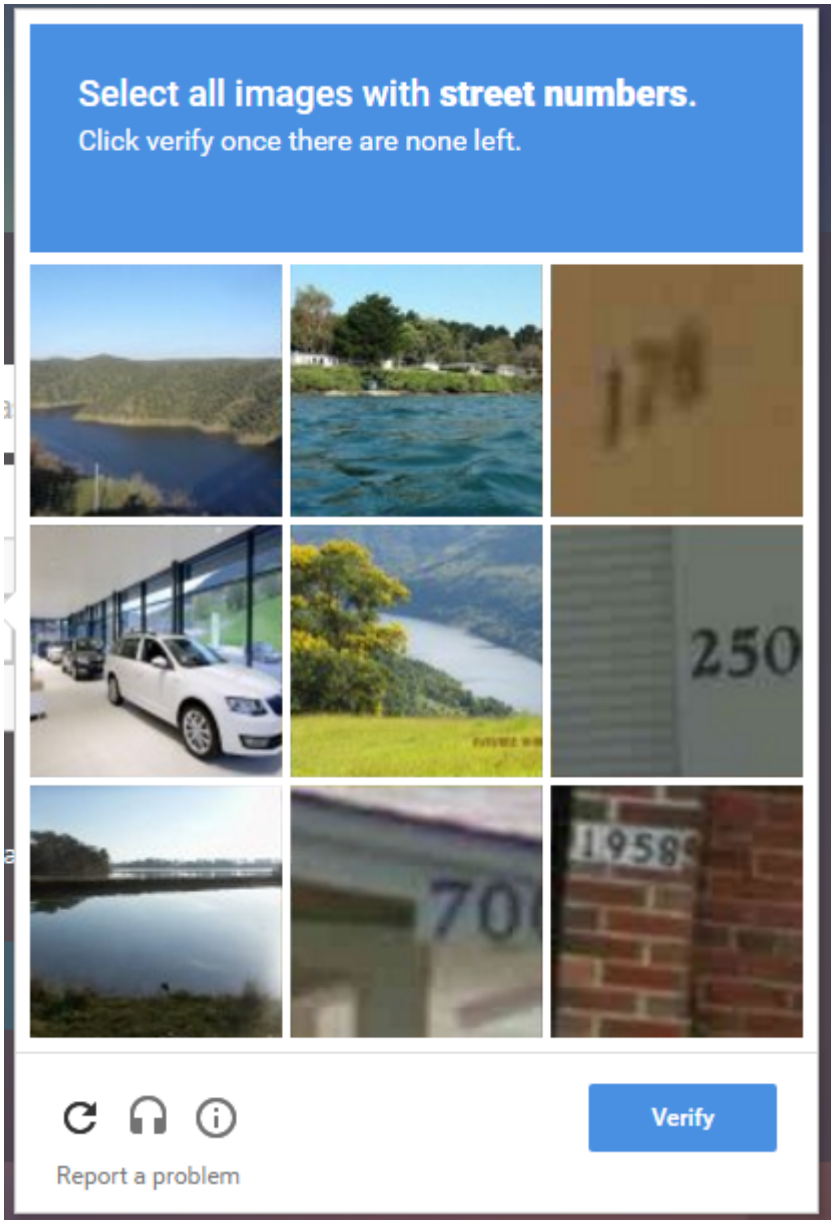
Benutzervalidierung von reCAPTCHA

Nachdem Sie alle Schritte konfiguriert haben, die in den vorherigen Abschnitten erwähnt wurden, müssen Sie die unten angezeigten UI-Screenshots sehen.

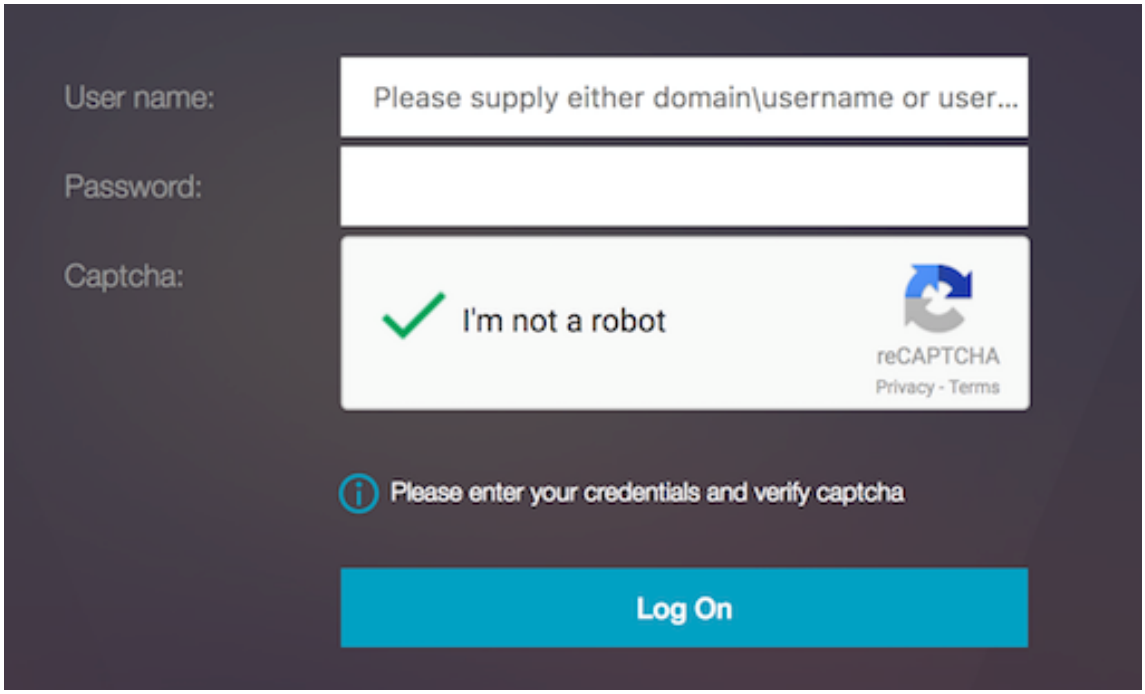
1. Sobald der virtuelle Authentifizierungsserver die Anmeldeseite lädt, wird der Anmeldebildschirm angezeigt. Die **Anmeldung** ist deaktiviert, bis reCAPTCHA abgeschlossen ist.



2. Wählen Sie Ich bin keine Roboteroption aus. Das reCAPTCHA Widget wird angezeigt.



3. Sie werden durch eine Reihe von reCAPTCHA Bildern navigiert, bevor die Fertigstellungsseite angezeigt wird.
4. Geben Sie die AD-Anmeldeinformationen ein, aktivieren Sie das Kontrollkästchen **Ich bin kein Roboter**, und klicken Sie **auf Anmelden** . Wenn die Authentifizierung erfolgreich ist, werden Sie zur gewünschten Ressource umgeleitet.



Hinweise

- Wenn reCAPTCHA mit der AD-Authentifizierung verwendet wird, wird die Schaltfläche Senden für Anmeldeinformationen deaktiviert, bis reCAPTCHA abgeschlossen ist.
- Das reCAPTCHA geschieht in einem eigenen Faktor. Daher müssen alle nachfolgenden Validierungen wie AD im 'nextfactor' von reCAPTCHA erfolgen.

Authentifizierung, Autorisierung und Auditing-Konfiguration für häufig verwendete Protokolle

February 24, 2022

Für die Konfiguration der Citrix ADC Appliance für Authentifizierung, Autorisierung und Überwachung ist eine spezielle Einrichtung in der Citrix ADC Appliance und den Browsern der Clients erforderlich. Die Konfiguration variiert je nach Protokoll, das für die Authentifizierung, Autorisierung und Überwachung verwendet wird.

Weitere Informationen zum Konfigurieren der Citrix ADC Appliance für die Kerberos-Authentifizierung finden Sie unter Umgang mit Authentifizierung, Autorisierung und Auditing mit Kerberos/NTLM.

Umgang mit Authentifizierung, Autorisierung und Auditing mit Kerberos/NTLM

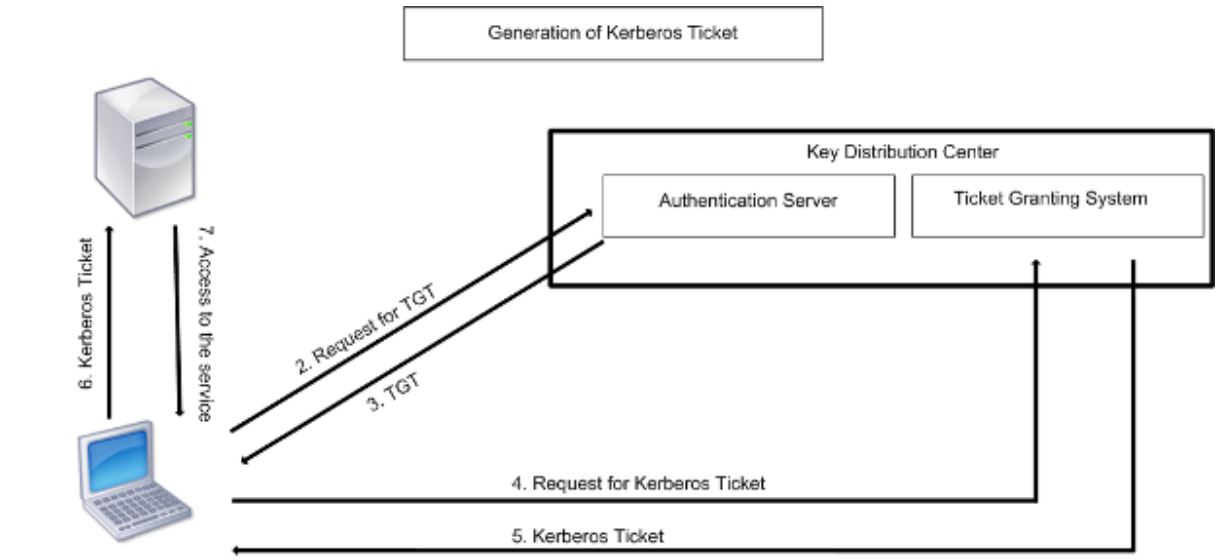
October 5, 2021

Kerberos, ein Computer-Netzwerkauthentifizierungsprotokoll, bietet eine sichere Kommunikation über das Internet. Sie wurde hauptsächlich für Client-Server-Anwendungen entwickelt und bietet eine gegenseitige Authentifizierung, mit der Client und Server die Authentizität des anderen sicherstellen können. Kerberos verwendet einen vertrauenswürdigen Drittanbieter, der als Key Distribution Center (KDC) bezeichnet wird. Ein KDC besteht aus einem Authentifizierungsserver (AS), der einen Benutzer authentifiziert, und einem Ticket Granting Server (TGS).

Jede Entität im Netzwerk (Client oder Server) verfügt über einen geheimen Schlüssel, der nur sich selbst und dem KDC bekannt ist. Die Kenntnis dieses Schlüssels impliziert Authentizität der Entität. Für die Kommunikation zwischen zwei Entitäten im Netzwerk generiert der KDC einen Sitzungsschlüssel, der als Kerberos-Ticket oder Serviceticket bezeichnet wird. Der Client stellt eine Anforderung an den AS für Anmeldeinformationen für einen bestimmten Server. Der Kunde erhält dann ein Ticket, das als Ticket Granting Ticket (TGT) bezeichnet wird. Der Kunde kontaktiert dann die TGS, verwendet den TGT, den er vom AS erhalten hat, um seine Identität zu beweisen, und bittet um einen Service. Wenn der Kunde für den Service berechtigt ist, gibt der TGS dem Kunden ein Kerberos-Ticket aus. Der Client kontaktiert dann den Server, der den Dienst hostet (als Serviceserver bezeichnet) und verwendet das Kerberos-Ticket, um nachzuweisen, dass er berechtigt ist, den Dienst zu empfangen. Das Kerberos-Ticket hat eine konfigurierbare Lebensdauer. Der Client authentifiziert sich nur einmal mit dem AS. Wenn er den physischen Server mehrmals kontaktiert, wird das AS-Ticket wiederverwendet.

Die folgende Abbildung zeigt die grundlegende Funktionsweise des Kerberos-Protokolls.

Abbildung 1. **Funktionieren von Kerberos**



Die Kerberos-Authentifizierung hat folgende Vorteile:

- Schnellere Authentifizierung. Wenn ein physischer Server ein Kerberos-Ticket von einem Client erhält, verfügt der Server über genügend Informationen, um den Client direkt zu authentifizieren. Es muss keinen Domänencontroller für die Clientauthentifizierung kontaktieren, und daher ist der Authentifizierungsprozess schneller.
- Gegenseitige Authentifizierung. Wenn der KDC ein Kerberos-Ticket an einen Client ausgibt und der Client das Ticket für den Zugriff auf einen Dienst verwendet, können nur authentifizierte Server das Kerberos-Ticket entschlüsseln. Wenn der virtuelle Server auf der Citrix ADC Appliance das Kerberos-Ticket entschlüsseln kann, können Sie feststellen, dass sowohl der virtuelle Server als auch der Client authentifiziert sind. Somit erfolgt die Authentifizierung des Servers zusammen mit der Authentifizierung des Clients.
- Single Sign-On zwischen Windows und anderen Betriebssystemen, die Kerberos unterstützen.

Kerberos-Authentifizierung kann folgende Nachteile haben:

- Kerberos hat strenge Zeitanforderungen. Die Uhren der beteiligten Hosts müssen mit der Kerberos-Serveruhr synchronisiert werden, um sicherzustellen, dass die Authentifizierung nicht fehlschlägt. Sie können diesen Nachteil verringern, indem Sie die Network Time Protocol Daemons verwenden, um die Host-Uhren synchronisieren zu lassen. Kerberos-Tickets haben einen Verfügbarkeitszeitraum, den Sie konfigurieren können.
- Kerberos benötigt den zentralen Server, um kontinuierlich verfügbar zu sein. Wenn der Kerberos-Server heruntergefahren ist, kann sich niemand anmelden. Sie können dieses Risiko verringern, indem Sie mehrere Kerberos-Server und Fallback-Authentifizierungsmechanismen verwenden.
- Da die gesamte Authentifizierung von einem zentralen KDC gesteuert wird, können alle Kompromisse in dieser Infrastruktur, z. B. das Kennwort des Benutzers für eine gestohlene lokale

Arbeitsstation, einem Angreifer die Identität eines beliebigen Benutzers ermöglichen. Sie können dieses Risiko in gewissem Maße verringern, indem Sie nur einen Desktop-Computer oder Laptop verwenden, dem Sie vertrauen, oder indem Sie die Vorauthentifizierung mittels eines Hardware-Token erzwingen.

Um die Kerberos-Authentifizierung verwenden zu können, müssen Sie sie auf der Citrix ADC Appliance und auf jedem Client konfigurieren.

Optimierung der Kerberos-Authentifizierung bei Authentifizierung, Autorisierung und Überwachung

Die Citrix ADC Appliance optimiert und verbessert jetzt die Systemleistung während der Kerberos-Authentifizierung. Der Authentifizierungs-, Autorisierungs- und Auditing-Daemon merkt sich die ausstehende Kerberos-Anfrage für denselben Benutzer, um die Belastung des Key Distribution Centers (KDC) zu vermeiden, wodurch doppelte Anforderungen vermieden werden.

Wie Citrix ADC Kerberos für die Clientauthentifizierung implementiert

October 5, 2021

> **Wichtig**
>
> Kerberos/NTLM-Authentifizierung wird nur in NetScaler 9.3 nCore Version oder höher unterstützt und kann nur für die Authentifizierung, Autorisierung und Überwachung von virtuellen Servern zur Datenverkehrsverwaltung verwendet werden.

Citrix ADC behandelt die Komponenten, die an der Kerberos-Authentifizierung beteiligt sind, folgendermaßen:

Schlüsselverteilungszentrum (KDC)

In Windows 2000 Server oder höher sind der Domänencontroller und der KDC Teil des Windows Servers. Wenn der Windows Server UP ist und ausgeführt wird, gibt es an, dass der Domänencontroller und KDC konfiguriert sind. Der KDC ist auch der Active Directory -Server.

> **Hinweis:**
>
> Alle Kerberos-Interaktionen werden mit dem Windows Kerberos-Domänencontroller validiert.

Authentifizierungsdienst und Protokollverhandlung

Eine Citrix ADC Appliance unterstützt die Kerberos-Authentifizierung auf den virtuellen Servern zur Authentifizierung, Autorisierung und Überwachung der Datenverkehrsverwaltung. Wenn die Kerberos-Authentifizierung fehlschlägt, verwendet Citrix ADC die NTLM-Authentifizierung.

Standardmäßig verwenden Windows 2000 Server und höhere Windows Server-Versionen Kerberos für Authentifizierung, Autorisierung und Überwachung. Wenn Sie eine Authentifizierungsrichtlinie mit Negotiate als Authentifizierungstyp erstellen, versucht Citrix ADC, das Kerberos-Protokoll für die Authentifizierung, Autorisierung und Überwachung zu verwenden. Wenn der Browser des Clients kein Kerberos-Ticket empfängt, verwendet Citrix ADC die NTLM-Authentifizierung. Dieser Prozess wird als Verhandlung bezeichnet.

Der Kunde kann ein Kerberos-Ticket in einem der folgenden Fälle nicht erhalten:

- Kerberos wird auf dem Client nicht unterstützt.
- Kerberos ist auf dem Client nicht aktiviert.
- Der Client befindet sich in einer anderen Domäne als der KDC.
- Auf das Access Directory auf dem KDC kann der Client nicht zugegriffen werden.

Für die Kerberos/NTLM-Authentifizierung verwendet Citrix ADC nicht die Daten, die lokal auf der Citrix ADC-Appliance vorhanden sind.

Ermächtigung

Der virtuelle Server für die Datenverkehrsverwaltung kann ein virtueller Lastausgleichsserver oder ein virtueller Content Switching-Server sein.

Überwachung

Die Citrix ADC Appliance unterstützt die Überwachung der Kerberos-Authentifizierung mit der folgenden Überwachungsprotokollierung:

- Vollständiger Audit-Pfad der Traffic-Management-Endbenutzeraktivität
- SYSLOG- und Hochleistungs-TCP-Protokollierung
- Vollständiger Prüfpfad der Systemadministratoren
- Alle Systemereignisse
- Skriptfähiges Protokollformat

Unterstützte Umgebung

Die Kerberos-Authentifizierung erfordert keine spezifische Umgebung auf dem Citrix ADC. Der Client (Browser) muss Unterstützung für die Kerberos-Authentifizierung bereitstellen.

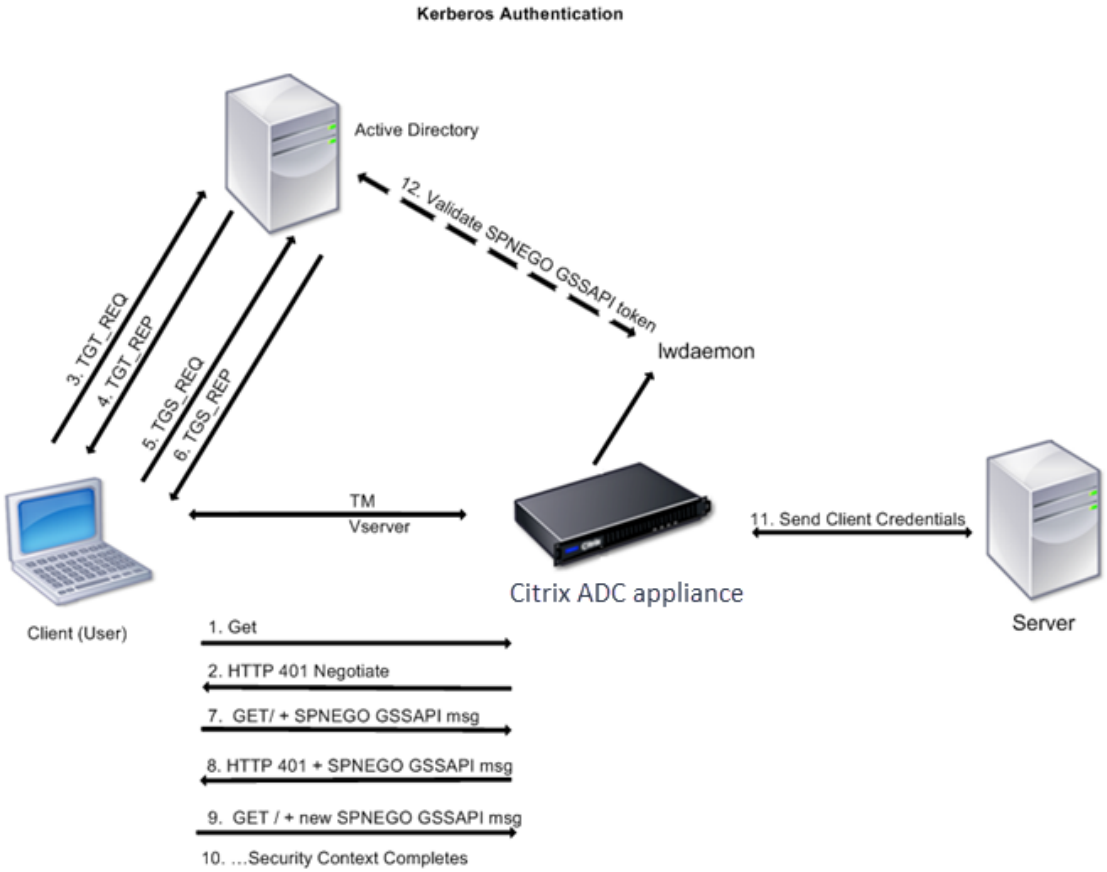
Hohe Verfügbarkeit

Bei einem Hochverfügbarkeitssetup tritt nur der aktive Citrix ADC der Domäne bei. Im Falle eines Failovers verbindet der Citrix ADC lwagent Daemon die sekundäre Citrix ADC-Appliance mit der Domäne. Für diese Funktionalität ist keine spezifische Konfiguration erforderlich.

Kerberos-Authentifizierungsprozess

Die folgende Abbildung zeigt einen typischen Prozess für die Kerberos-Authentifizierung in der Citrix ADC Umgebung.

Abbildung 1. Kerberos-Authentifizierungsprozess auf Citrix ADC



Die Kerberos-Authentifizierung erfolgt in den folgenden Phasen:

Client authentifiziert sich beim KDC

1. Die Citrix ADC Appliance empfängt eine Anforderung von einem Client.
2. Der virtuelle Server zur Datenverkehrsverwaltung (Load Balancing oder Content Switching) auf der Citrix ADC Appliance sendet eine Herausforderung an den Client.
3. Um auf die Herausforderung zu reagieren, erhält der Kunde ein Kerberos-Ticket.

- Der Client sendet dem Authentifizierungsserver des KDC eine Anforderung für ein Ticket Granting Ticket (TGT) und erhält den TGT. (Siehe 3, 4 in der Abbildung Kerberos-Authentifizierungsprozess.)
- Der Client sendet den TGT an den Ticket Granting Server des KDC und erhält ein Kerberos-Ticket. (Siehe 5, 6 in der Abbildung Kerberos-Authentifizierungsprozess.)

> **Hinweis:**
>
> Der oben genannte Authentifizierungsprozess ist nicht erforderlich, wenn der Client bereits über ein Kerberos-Ticket verfügt, dessen Lebensdauer noch nicht abgelaufen ist. Darüber hinaus erhalten Clients wie Webdienste, .NET oder J2EE, die SPNEGO unterstützen, ein Kerberos-Ticket für den Zielserver, erstellen ein SPNEGO-Token und fügen das Token in den HTTP-Header ein, wenn sie eine HTTP-Anforderung senden. Sie durchlaufen nicht den Clientauthentifizierungsprozess.

Der Client fordert einen Dienst an.

1. Der Client sendet das Kerberos-Ticket, das das SPNEGO-Token und die HTTP-Anforderung enthält, an den virtuellen Server für die Datenverkehrsverwaltung auf dem Citrix ADC. Das SPNEGO-Token verfügt über die notwendigen GSSAPI-Daten.
2. Die Citrix ADC-Appliance erstellt einen Sicherheitskontext zwischen dem Client und dem Citrix ADC. Wenn Citrix ADC die im Kerberos-Ticket angegebenen Daten nicht akzeptieren kann, wird der Client aufgefordert, ein anderes Ticket zu erhalten. Dieser Zyklus wiederholt sich, bis die GSSAPI-Daten akzeptabel sind und der Sicherheitskontext eingerichtet ist. Der virtuelle Server zur Datenverkehrsverwaltung auf dem Citrix ADC fungiert als HTTP-Proxy zwischen dem Client und dem physischen Server.

Die Citrix ADC Appliance schließt die Authentifizierung ab.

1. Nachdem der Sicherheitskontext abgeschlossen ist, überprüft der virtuelle Server für die Datenverkehrsverwaltung das SPNEGO-Token.
2. Aus dem gültigen SPNEGO-Token extrahiert der virtuelle Server die Benutzer-ID und die GSS-Anmeldeinformationen und übergibt sie an den Authentifizierungsdaemon.
3. Eine erfolgreiche Authentifizierung schließt die Kerberos-Authentifizierung ab.

Konfigurieren der Kerberos-Authentifizierung auf der Citrix ADC Appliance

October 5, 2021

In diesem Thema finden Sie detaillierte Schritte zum Konfigurieren der Kerberos-Authentifizierung auf der Citrix ADC Appliance mit der CLI und der GUI.

Konfigurieren der Kerberos-Authentifizierung auf der CLI

1. Aktivieren Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion, um die Authentifizierung des Datenverkehrs auf der Appliance sicherzustellen.

   ns-cli-prompt> **enable ns feature** AAA

2. Fügen Sie der Citrix ADC Appliance die Keytab-Datei hinzu. Eine Keytab-Datei ist für die Entschlüsselung des Geheimnisses erforderlich, der vom Client während der Kerberos-Authentifizierung empfangen wurde. Eine einzelne Keytab-Datei enthält Authentifizierungsdetails für alle Dienste, die an den virtuellen Server für die Datenverkehrsverwaltung auf der Citrix ADC Appliance gebunden sind.

   Generieren Sie zuerst die Keytab-Datei auf dem Active Directory -Server und übertragen Sie sie dann an die Citrix ADC Appliance.

   - Melden Sie sich beim Active Directory -Server an, und fügen Sie einen Benutzer für die Kerberos-Authentifizierung hinzu. Um beispielsweise einen Benutzer mit dem Namen Kerb-SVC-Konto hinzuzufügen:

     net user kerb-SVC-account freebsd! @ #456 /hinzufügen

     > **Hinweis:**
     >
     > Stellen Sie im Abschnitt **Benutzereigenschaften** sicher, dass die Option “Kennwort bei der nächsten Anmeldung ändern” nicht ausgewählt ist und die Option “Kennwort läuft nicht ab” ausgewählt ist.

   - Ordnen Sie den HTTP-Dienst dem obigen Benutzer zu und exportieren Sie die keytab-Datei. Führen Sie beispielsweise den folgenden Befehl auf dem Active Directory -Server aus:

     ktpass /out keytabfile /princ HTTP/owa.newacp.com@NEWACP.COM /pass freebsd!@#456 /mapuser newacp\dummy /ptype KRB5_NT_PRINCIPAL

     > **Hinweis:**
     >
     > Sie können mehrere Dienste zuordnen, wenn eine Authentifizierung für mehrere Dienste erforderlich ist. Wenn Sie weitere Dienste zuordnen möchten, wiederholen Sie den obigen Befehl für jeden Dienst. Sie können den gleichen Namen oder andere Namen für die Ausgabedatei angeben.

   - Übertragen Sie die keytab-Datei mithilfe des Befehls unix **ftp** oder eines anderen Dateiübertragungsdienstprogramms Ihrer Wahl auf die Citrix ADC Appliance.

3. Die Citrix ADC Appliance muss die IP-Adresse des Domänencontroller aus dem vollqualifizierten Domänennamen (FQDN) abrufen. Daher empfiehlt Citrix die Konfiguration des Citrix ADC mit einem DNS-Server.

ns-cli-prompt> **add dns nameserver** <ip-address>

> **Hinweis:**
>
> Alternativ können Sie statische Hosteinträge hinzufügen oder andere Mittel verwenden, damit die Citrix ADC Appliance den FQDN-Namen des Domänencontroller in eine IP-Adresse auflösen kann.

4. Konfigurieren Sie die Authentifizierungsaktion, und ordnen Sie sie dann einer Authentifizierungsrichtlinie zu.

   - Konfigurieren Sie die Aushandlungsaktion.

     ns-cli-prompt **Authentifizierung hinzufügen negotiateAction** <name>-domain <domain name>-domainUser <domain user name>-DomainUserPasswd <domain user password>-DefaultAuthenticationGroup <default authentication group>-keytab <string>-ntlmPath <string>

     Hinweis: Wechseln Sie für die Konfiguration von Domänenbenutzern und Domänennamen zum Client und verwenden Sie den Befehl klist wie im folgenden Beispiel gezeigt:

     Kunde: Benutzername @ AAA.LOCAL

     Server: http/onprem_idp.AAA.Local @ AAA.LOCAL

     Authentifizierung hinzufügen NegotiateAction <name>-domain -DomainUser \<HTTP/onprem_idp.aaa.local>

   - Konfigurieren Sie die Verhandlungsrichtlinie, und ordnen Sie die Verhandlungsaktion dieser Richtlinie zu.

     ns-cli-prompt> **add authentication negotiatePolicy** <name> <rule> <reqAction>

5. Erstellen Sie einen virtuellen Authentifizierungsserver, und ordnen Sie ihm die Verhandlungsrichtlinie zu.

   - Erstellen Sie einen virtuellen Authentifizierungsserver.

     ns-cli-prompt> **add authentication vserver** <name> SSL <ipAuthVserver> 443 -authenticationDomain <domainName>

   - Binden Sie die Verhandlungsrichtlinie an den virtuellen Authentifizierungsserver.

     ns-cli-prompt> **bind authentication vserver** <name> -policy <negotiatePolicyName>

6. Ordnen Sie den virtuellen Authentifizierungsserver dem virtuellen Server zur Datenverkehrsverwaltung (Lastausgleich oder Content Switching) zu.

   ns-cli-prompt> **set lb vserver** <name> -authn401 ON -authnVsName <string>

> **Hinweis:**
>
> Ähnliche Konfigurationen können auch auf dem virtuellen Content Switching-Server vorgenommen werden.

7. Überprüfen Sie die Konfigurationen, indem Sie die folgenden Schritte ausführen:
   - Greifen Sie mithilfe des FQDN auf den virtuellen Server zur Datenverkehrsverwaltung zu. Beispiel: Sample
   - Zeigen Sie die Details der Sitzung auf der CLI an.

     ns-cli-prompt> **show aaa session**

Konfigurieren der Kerberos-Authentifizierung auf der GUI

1. Aktivieren Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion.

   Navigieren Sie zu **System** > **Einstellungen**, klicken Sie auf **Basisfunktionen konfigurieren**, und aktivieren Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion.

2. Fügen Sie die Keytab-Datei wie in Schritt 2 der oben genannten CLI-Prozedur beschrieben hinzu.
3. Fügen Sie einen DNS-Server hinzu.

   Navigieren Sie zu **Verkehrsverwaltung > DNS > Namensserver**, und geben Sie die IP-Adresse für den DNS-Server an.

4. Konfigurieren Sie die Aktion und die Richtlinie **aushandeln** .

   Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinie**, und erstellen Sie eine Richtlinie mit **Negotiate**als Aktionstyp. Klicken Sie auf **Hinzufügen**, um einen neuen Authentifizierungsverhandlungsserver zu erstellen, oder klicken Sie auf **Bearbeiten**, um die vorhandenen Details zu konfigurieren.

5. Binden Sie die Verhandlungsrichtlinie an den virtuellen Authentifizierungsserver.

   Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Virtuelle Server**, und ordnen Sie die **Negotiate-Richtlinie**dem virtuellen Authentifizierungsserver zu.

6. Ordnen Sie den virtuellen Authentifizierungsserver dem virtuellen Server zur Datenverkehrsverwaltung (Lastausgleich oder Content Switching) zu.

   Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und geben Sie die entsprechenden Authentifizierungseinstellungen an.

   > **Hinweis:**

> Ähnliche Konfigurationen können auch auf dem virtuellen Content Switching-Server vorgenommen werden.

7. Überprüfen Sie die Konfigurationen wie in Schritt 7 der oben genannten CLI-Prozedur beschrieben.

Konfigurieren der Kerberos-Authentifizierung auf einem Client

October 5, 2021

Die Kerberos-Unterstützung muss im Browser konfiguriert werden, um Kerberos für die Authentifizierung zu verwenden. Sie können jeden Kerberos-kompatiblen Browser verwenden. Anweisungen zum Konfigurieren der Kerberos-Unterstützung in Internet Explorer und Mozilla Firefox folgen. Weitere Browser finden Sie in der Dokumentation des Browsers.

So konfigurieren Sie Internet Explorer für die Kerberos-Authentifizierung

1. Wählen Sie im Menü **Extras** die Option **Internetoptionen**.
2. Klicken Sie auf der Registerkarte **Sicherheit** auf **Lokales Intranet**, und klicken Sie dann auf **Sites**.
3. Stellen Sie im Dialogfeld **Lokales Intranet** sicher, dass die Option Intranetnetzwerk automatisch erkennen aktiviert ist, und klicken Sie dann auf **Erweitert**.
4. Fügen Sie im Dialogfeld **Lokales Intranet** die Websites der Domänen des virtuellen Servers zur Datenverkehrsverwaltung auf der Citrix ADC Appliance hinzu. Die angegebenen Sites werden zu lokalen Intranetsites.
5. Klicken Sie auf **Schließen** oder **OK**, um die Dialogfelder zu schließen.

So konfigurieren Sie Mozilla Firefox für die Kerberos-Authentifizierung

1. Stellen Sie sicher, dass Kerberos ordnungsgemäß auf Ihrem Computer konfiguriert ist.
2. Geben Sie about:config in die URL-Leiste ein.
3. Geben Sie im Textfeld Filter den Wert network.negotiate ein.
4. Ändern Sie network.negotiate-auth.delegation-uris in die Domäne, die Sie hinzufügen möchten.
5. Ändern Sie network.negotiate-auth.trusted-uris in die Domäne, die Sie hinzufügen möchten.

> **Hinweis:** Wenn Sie Windows ausführen, müssen Sie auch sspi in das Filtertextfeld eingeben und die network.auth.use-sspi Option auf Falsch ändern.

Offload der Kerberos-Authentifizierung von physischen Servern

February 24, 2022

Die Citrix ADC Appliance kann Authentifizierungsaufgaben von Servern auslagern. Anstatt die physischen Server die Anforderungen von Clients authentifizieren, authentifiziert der Citrix ADC alle Clientanforderungen, bevor er sie an einen der an ihn gebundenen physischen Server weiterleitet. Die Benutzerauthentifizierung basiert auf Active Directory Token.

Es gibt keine Authentifizierung zwischen Citrix ADC und dem physischen Server, und die Authentifizierungsabladung ist für die Endbenutzer transparent. Nach der ersten Anmeldung an einem Windows-Computer muss der Endbenutzer keine zusätzlichen Authentifizierungsinformationen in einem Pop-up oder auf einer Anmeldeseite eingeben.

In der aktuellen Version der Citrix ADC Appliance ist die Kerberos-Authentifizierung nur für die Authentifizierung, Autorisierung und Überwachung virtueller Server zur Datenverkehrsverwaltung verfügbar. Die Kerberos-Authentifizierung wird für SSL-VPN in der Citrix Gateway Advanced Edition-Appliance oder für die Citrix ADC Appliance-Verwaltung nicht unterstützt.

Die Kerberos-Authentifizierung erfordert eine Konfiguration auf der Citrix ADC Appliance und in Clientbrowsern.

So konfigurieren Sie die Kerberos-Authentifizierung auf der Citrix ADC Appliance

1. Erstellen Sie ein Benutzerkonto in Active Directory. Überprüfen Sie beim Erstellen eines Benutzerkontos die folgenden Optionen im Abschnitt Benutzereigenschaften:
    - Stellen Sie sicher, dass Sie die Option Kennwort bei der nächsten Anmeldung ändern nicht auswählen.
    - Stellen Sie sicher, dass Sie die Option Kennwort nicht ablaufen auswählen.
2. Geben Sie auf dem AD-Server an der CLI-Eingabeaufforderung Folgendes ein:
    - ktpass -princ HTTP/kerberos.crete.lab.net@crete.lab.net -ptype KRB5_NT_PRINCIPAL -mapuser kerbuser@crete.lab.net -mapop set -pass <password> -out C:\kerbtabfile.txt

    > **Hinweis:**
    >
    > Stellen Sie sicher, dass Sie den obigen Befehl in einer einzigen Zeile eingeben. Die Ausgabe des obigen Befehls wird in die Datei C:KerbTabFile.txt geschrieben.
3. Laden Sie die Datei kerbtabfile.txt in das Verzeichnis /etc der Citrix ADC Appliance mit einem Secure Copy (SCP) -Client hoch.
4. Führen Sie den folgenden Befehl aus, um der Citrix ADC Appliance einen DNS-Server hinzuzufügen.

- add dns nameserver 1.2.3.4

Die Citrix ADC Appliance kann Kerberos-Anforderungen ohne den DNS-Server nicht verarbeiten. Stellen Sie sicher, dass Sie denselben DNS-Server verwenden, der in der Microsoft Windows-Domäne verwendet wird.

5. Wechseln Sie zur Befehlszeilenschnittstelle von Citrix ADC.
6. Führen Sie den folgenden Befehl aus, um einen Kerberos-Authentifizierungsserver zu erstellen:

   - add authentication negotiateAction KerberosServer -domain “crete.lab.net” -domainUser kerbuser -domainUserPasswd <password> -keytab /var/mykcd.keytab

   > **Hinweis**
   >
   > Wenn keytab nicht verfügbar ist, können Sie die Parameter domain, domainUser und -domainUserPasswd angeben.

7. Führen Sie den folgenden Befehl aus, um eine Verhandlungsrichtlinie zu erstellen:

   - `add authentication negotiatePolicy Kerberos-Policy ”REQ.IP.DESTIP == 192.168.17.200”KerberosServer<!--NeedCopy-->`

8. Führen Sie den folgenden Befehl aus, um einen virtuellen Authentifizierungsserver zu erstellen.

   - `add authentication vserver Kerb-Auth SSL 192.168.17.201 443 -AuthenticationDomain crete.lab.net<!--NeedCopy-->`

9. Führen Sie den folgenden Befehl aus, um die Kerberos-Richtlinie an den virtuellen Authentifizierungsserver zu binden:

   - `bind authentication vserver Kerb-Auth -policy Kerberos-Policy -priority 100<!--NeedCopy-->`

10. Führen Sie den folgenden Befehl aus, um ein SSL-Zertifikat an den virtuellen Authentifizierungsserver zu binden. Sie können eines der Testzertifikate verwenden, das Sie über die GUI Citrix ADC Appliance installieren können. Führen Sie den folgenden Befehl aus, um das Beispielzertifikat ServerTestCert zu verwenden.

    - `bind ssl vserver Kerb-Auth -certkeyName ServerTestCert<!--NeedCopy-->`

11. Erstellen Sie einen virtuellen HTTP-Lastausgleichsserver mit der IP-Adresse 192.168.17.200.

    Stellen Sie sicher, dass Sie über die Befehlszeilenschnittstelle für NetScaler 9.3-Releases einen virtuellen Server erstellen, wenn sie älter als 9.3.47.8 sind.

12. Führen Sie den folgenden Befehl aus, um einen virtuellen Authentifizierungsserver zu konfigurieren:

- `set lb vserver <name>-authn401 ON -authnVsName Kerb-Auth<!--NeedCopy -->`

13. Geben Sie den Hostnamen Example in die Adressleiste des Webbrowsers ein.

    Der Webbrowser zeigt ein Authentifizierungsdialogfeld an, da die Kerberos-Authentifizierung nicht im Browser eingerichtet ist.

    > **Hinweis:**
    >
    > Die Kerberos-Authentifizierung erfordert eine bestimmte Konfiguration auf dem Client. Stellen Sie sicher, dass der Client den Hostnamen auflösen kann. Dies führt dazu, dass der Webbrowser eine Verbindung zu einem virtuellen HTTP-Server herstellt.

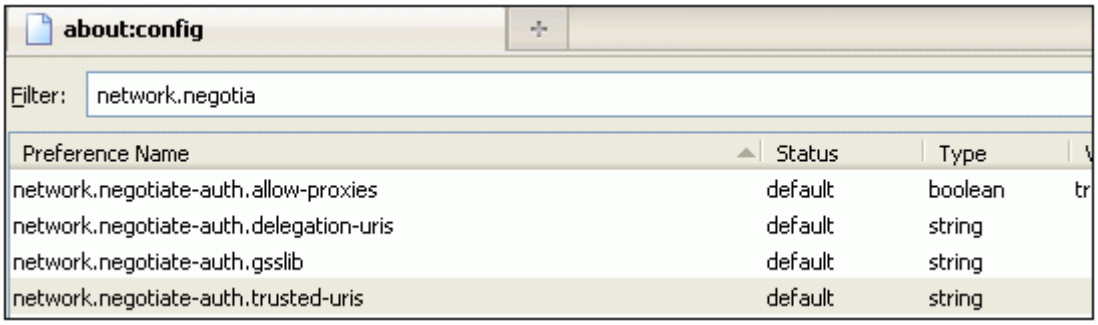
14. Konfigurieren Sie Kerberos im Webbrowser des Clientcomputers.
    - Informationen zur Konfiguration in Internet Explorer finden Sie unter Konfigurieren von Internet Explorer für die Kerberos-Authentifizierung.
    - Informationen zur Konfiguration in Mozilla Firefox finden Sie unter Konfigurieren von Internet Explorer für die Kerberos-Authentifizierung.
15. Überprüfen Sie, ob Sie ohne Authentifizierung auf den physischen Backend-Server zugreifen können.

So konfigurieren Sie Internet Explorer für die Kerberos-Authentifizierung

1. Wählen Sie im Menü **Extras** die Option **Internetoptionen** aus.
2. Aktivieren Sie die Registerkarte **Sicherheit**.
3. Wählen Sie **Lokales Intranet** im Abschnitt “Wählen Sie eine Zone”, um Sicherheitseinstellungen zu ändern.
4. Klicken Sie auf **Sites**.
5. Klicken Sie auf **Erweitert**.
6. Geben Sie die URL an, Beispiel, und klicken Sie auf **Hinzufügen**.
7. Starten Sie **Internet Explorer**neu.

So konfigurieren Sie Mozilla Firefox für die Kerberos-Authentifizierung

1. Geben Sie about:config in die Adressleiste des Browsers ein.
2. Klicken Sie auf den Warnhinweis.
3. Geben Sie **Network.Negotiate-auth.trusted-uris** in das Feld **Filter** ein.
4. Doppelklicken Sie auf **Network.Negotiate-auth.trusted-uris**. Ein Beispielbildschirm wird unten gezeigt.



5. Geben Sie im Dialogfeld Zeichenfolgenwert eingeben www.crete.lab.net ein.
6. Starten Sie Firefox neu.

Single-Sign-On-Typen

May 10, 2022

Die Citrix ADC Authentifizierungs-, Autorisierungs- und Überwachungsfunktionen unterstützen die folgenden Single Sign-On-Typen.

- **Citrix ADC Kerberos Single Sign-On:** Citrix ADC Appliances unterstützen jetzt Single Sign-On (SSO) mit dem Kerberos 5-Protokoll. Benutzer melden sich bei einem Proxy an, dem Application Delivery Controller (ADC), der dann Zugriff auf geschützte Ressourcen ermöglicht. Weitere Informationen finden Sie unter Citrix ADC Kerberos Single Sign-On.
- **SSO für Basic-, Digest- und NTLM-Authentifizierung:** Die Single Sign-On (SSO) -Konfiguration in Citrix ADC und Citrix Gateway kann auf globaler Ebene und auch pro Traffic-Ebene aktiviert werden. Standardmäßig ist die SSO-Konfiguration AUS und ein Administrator kann das SSO pro Datenverkehr oder global aktivieren. Aus Sicherheitsgründen empfiehlt Citrix Administratoren, SSO global auszuschalten und pro Traffic-Basis zu aktivieren. Diese Verbesserung soll die SSO-Konfiguration sicherer machen, indem bestimmte Arten von SSO-Methoden global deaktiviert werden. Weitere Informationen finden Sie unter SSO für Basic-, Digest- und NTLM-Authentifizierung.

Citrix ADC Kerberos Single Sign-On

October 5, 2021

Citrix ADC Appliances unterstützen jetzt Single Sign-On (SSO) mithilfe des Kerberos 5-Protokolls. Benutzer melden sich bei einem Proxy an, dem Application Delivery Controller (ADC), der dann Zugriff auf geschützte Ressourcen ermöglicht.

Für die Citrix ADC Kerberos-SSO-Implementierung ist das Kennwort des Benutzers für SSO-Methoden erforderlich, die auf der Basis-, NTLM- oder formularbasierten Authentifizierung basieren. Das Kennwort des Benutzers ist für Kerberos SSO nicht erforderlich. Wenn Kerberos SSO fehlschlägt und die Citrix ADC Appliance über das Kennwort des Benutzers verfügt, wird das Kennwort verwendet, um NTLM SSO zu versuchen.

Wenn das Kennwort des Benutzers verfügbar ist, wird das KCD-Konto mit einem Bereich (Realm) konfiguriert und keine delegierten Benutzerinformationen vorhanden sind, gibt das Citrix AD Kerberos-SSO-Modul den Namen des Benutzers an, um Zugriff auf autorisierte Ressourcen zu erhalten. Der Identitätswechsel wird auch als nicht eingeschränkte Delegierung bezeichnet.

Das Citrix ADC Kerberos-SSO-Modul kann auch so konfiguriert werden, dass ein delegiertes Konto verwendet wird, um Zugriff auf geschützte Ressourcen im Namen des Benutzers zu erhalten. Diese Konfiguration erfordert delegierte Benutzeranmeldeinformationen, eine Schlüsseltabelle oder ein delegiertes Benutzerzertifikat und ein entsprechendes Zertifizierungsstellenzertifikat. Konfiguration, die ein delegiertes Konto verwendet, wird als eingeschränkte Delegierung bezeichnet.

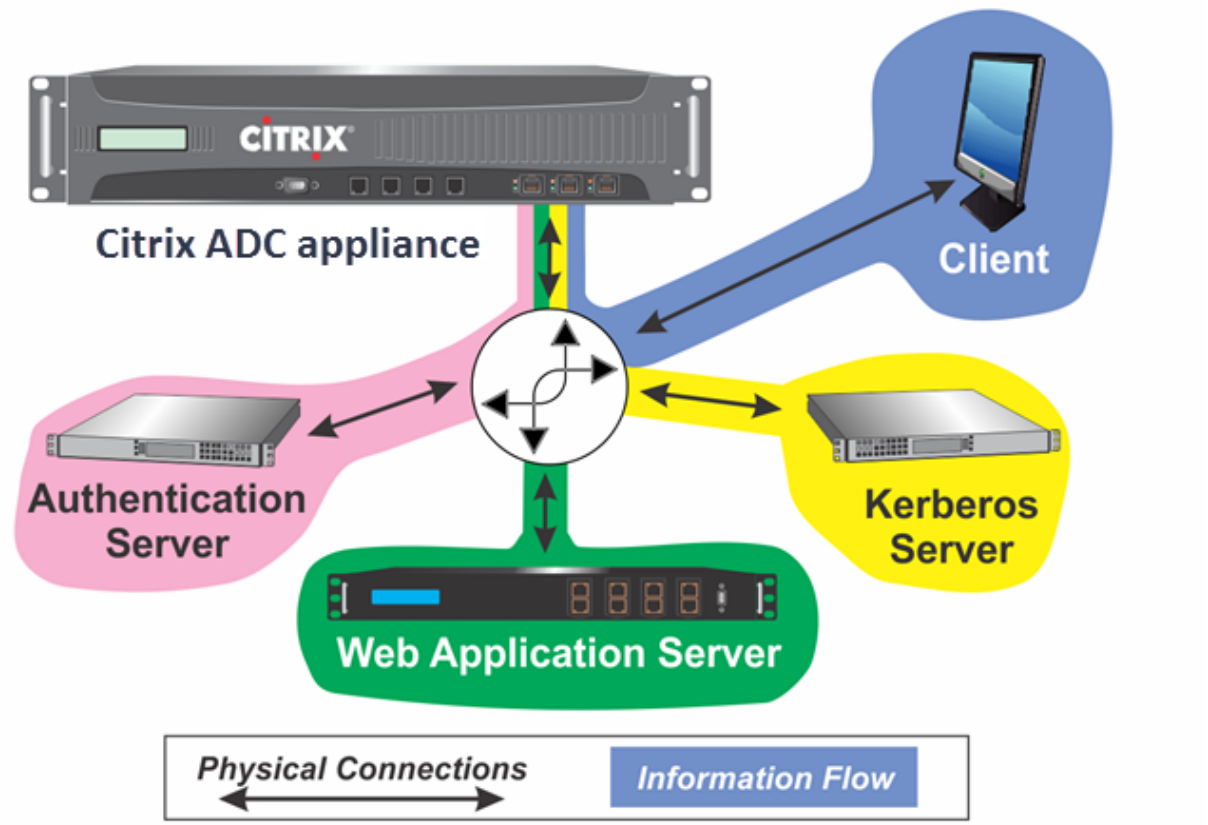
Überblick über das SSO von Citrix ADC Kerberos

October 5, 2021

Um die Citrix ADC Kerberos-SSO-Funktion zu verwenden, authentifizieren sich Benutzer zuerst bei Kerberos oder einem unterstützten Authentifizierungsserver von Drittanbietern. Nach der Authentifizierung fordert der Benutzer Zugriff auf eine geschützte Webanwendung an. Der Webserver antwortet mit einer Anforderung zum Nachweis, dass der Benutzer berechtigt ist, auf diese Webanwendung zuzugreifen. Der Browser des Benutzers kontaktiert den Kerberos-Server, der überprüft, ob der Benutzer berechtigt ist, auf diese Ressource zuzugreifen, und stellt dann dem Browser des Benutzers ein Serviceticket zur Verfügung, das einen Nachweis liefert. Der Browser sendet die Anfrage des Benutzers erneut an den Webanwendungsserver mit dem angehängten Serviceticket. Der Webanwendungsserver überprüft das Serviceticket und ermöglicht dem Benutzer dann den Zugriff auf die Anwendung.

Authentifizierung, Autorisierung und Auditing Traffic Management implementiert diesen Prozess, wie im folgenden Diagramm dargestellt. Das Diagramm veranschaulicht den Informationsfluss über die Citrix ADC Appliance sowie die Verwaltung des Authentifizierungs-, Autorisierungs- und Überwachungsverkehrs in einem sicheren Netzwerk mit LDAP-Authentifizierung und Kerberos-Autorisierung. Authentifizierungs-, Autorisierungs- und Überwachungsumgebungen, die andere Authentifizierungstypen verwenden, haben im Wesentlichen denselben Informationsfluss, obwohl sie sich in einigen Details unterscheiden können.

Abbildung 1. Ein sicheres Netzwerk mit LDAP und Kerberos



Die Verwaltung der Authentifizierung, Autorisierung und Überwachung des Datenverkehrs mit Authentifizierung und Autorisierung in einer Kerberos-Umgebung erfordert, dass die folgenden Aktionen durchgeführt werden.

1. Der Client sendet eine Anforderung für eine Ressource an den virtuellen Server zur Datenverkehrsverwaltung auf der Citrix ADC Appliance.
2. Der virtuelle Server zur Datenverkehrsverwaltung übergibt die Anforderung an den virtuellen Authentifizierungsserver, der den Client authentifiziert und dann die Anforderung an den virtuellen Server der Datenverkehrsverwaltung weiterleitet.
3. Der virtuelle Server zur Datenverkehrsverwaltung sendet die Anforderung des Clients an den Webanwendungsserver.
4. Der Webanwendungsserver reagiert auf den virtuellen Server der Datenverkehrsverwaltung mit einer 401-Nachricht, die die Kerberos-Authentifizierung anfordert, mit Fallback auf die NTLM-Authentifizierung, wenn der Client Kerberos nicht unterstützt.
5. Der virtuelle Server zur Datenverkehrsverwaltung kontaktiert den Kerberos-SSO-Daemon.
6. Der Kerberos-SSO-Daemon kontaktiert den Kerberos-Server und erhält ein Ticket, das ihm erlaubt, Servicetickets anzufordern (TGT), die den Zugriff auf geschützte Anwendungen autorisieren.
7. Der Kerberos-SSO-Daemon ruft ein Dienstticket für den Benutzer ab und sendet dieses Ticket an den virtuellen Server für die Datenverkehrsverwaltung.

8. Der virtuelle Server zur Datenverkehrsverwaltung fügt das Ticket an die anfängliche Anforderung des Benutzers an und sendet die geänderte Anforderung zurück an den Webanwendungsserver.
9. Der Webanwendungsserver antwortet mit einer 200-OK-Nachricht.

Diese Schritte sind für den Client transparent, der nur eine Anforderung sendet und die angeforderte Ressource empfängt.

Integration von Citrix ADC Kerberos SSO mit Authentifizierungsmethoden

Alle Authentifizierungsmechanismen für die Authentifizierung, Autorisierung und Überwachung des Datenverkehrs unterstützen Citrix ADC Kerberos SSO. Authentifizierungs-, Autorisierungs- und Überwachungsdatenverkehrs-Management unterstützt den Kerberos-SSO-Mechanismus mit den Kerberos-, CAC- (Smartcard-) und SAML-Authentifizierungsmechanismen mit jeder Form der Clientauthentifizierung an der Citrix ADC Appliance. Es unterstützt auch die SSO-Mechanismen HTTP-Basic, HTTP-Digest, Forms-based und NTLM (Versionen 1 und 2), wenn der Client zur Anmeldung an der Citrix ADC Appliance entweder die HTTP-Basic- oder die formularbasierte Authentifizierung verwendet.

Die folgende Tabelle zeigt jede unterstützte clientseitige Authentifizierungsmethode und die unterstützte serverseitige Authentifizierungsmethode für diese clientseitige Methode.

Tabelle 1. Unterstützte Authentifizierungsmethoden

	Basis/Digest/NTLM	Eingeschränkte Kerberos-Delegierung	Identitätswechsel
CAC (Smartcard): bei SSL/T LS Layer		X	X
Formularbasiert (LDAP/RADIUS/TACACS)	X	X	X
HTTP Basic (LDAP/RADIUS/TACACS)	X	X	X
Kerberos		X	
NT LM v1/v2		X	X
SAML		X	
SAML Zwei-Faktor-Faktor	X	X	X
Zwei-Faktor-Zertifikat	X	X	X

Einrichten von Citrix ADC SSO

February 24, 2022

Sie können Citrix ADC SSO so konfigurieren, dass es auf zwei Arten funktioniert: durch Identitätswechsel oder Delegierung. SSO nach Identitätswechsel ist eine einfachere Konfiguration als SSO durch Delegierung und ist daher in der Regel vorzuziehen, wenn Ihre Konfiguration dies zulässt. Um Citrix ADC SSO nach Identitätswechsel zu konfigurieren, müssen Sie über den Benutzernamen und das Kennwort des Benutzers verfügen.

Um Citrix ADC SSO nach Delegierung zu konfigurieren, müssen Sie die Anmeldeinformationen des delegierten Benutzers in einem der folgenden Formate haben: Benutzername und Kennwort des Benutzers, Keytab-Konfiguration, die den Benutzernamen und ein verschlüsseltes Kennwort enthält, oder das delegierte Benutzerzertifikat und das zugehörige Zertifizierungsstellenzertifikat.

Voraussetzungen für die Konfiguration von Citrix ADC SSO

Bevor Sie Citrix ADC SSO konfigurieren, müssen Sie Ihre Citrix ADC Appliance vollständig für die Verwaltung des Datenverkehrs und der Authentifizierung Ihrer Webanwendungsserver konfigurieren. Daher müssen Sie für diese Webanwendungsserver entweder den Lastausgleich oder das Content Switching und dann die Authentifizierung, Autorisierung und Überwachung konfigurieren. Sie sollten auch das Routing zwischen der Appliance, dem LDAP-Server und dem Kerberos-Server überprüfen.

Wenn Ihr Netzwerk noch nicht auf diese Weise konfiguriert ist, führen Sie die folgenden Konfigurationsaufgaben aus:

- Konfigurieren Sie einen Server und einen Dienst für jeden Webanwendungsserver.
- Konfigurieren Sie einen virtuellen Server zur Datenverkehrsverwaltung, um Datenverkehr zu und von Ihrem Webanwendungsserver zu verarbeiten.

Im Folgenden finden Sie kurze Anweisungen und Beispiele für die Ausführung dieser Aufgaben über die Citrix ADC Befehlszeile. Weitere Unterstützung finden Sie unter Einrichten eines virtuellen Authentifizierungsservers.

So erstellen Sie einen Server und einen Dienst mit der CLI

Damit Citrix ADC SSO ein TGS (Serviceticket) für einen Dienst abrufen kann, muss entweder der FQDN, der der Serverentität auf der Citrix ADC Appliance zugewiesen ist, mit dem FQDN des Webanwendungsservers übereinstimmen, oder der Serverentitätsname muss mit dem NetBIOS-Namen des Webanwendungsservers übereinstimmen. Sie können einen der folgenden Ansätze verwenden:

- Konfigurieren Sie die Citrix ADC -Serverentität, indem Sie den FQDN des Webanwendungsservers angeben.

- Konfigurieren Sie die Citrix ADC -Serverentität, indem Sie die IP-Adresse des Webanwendungsservers angeben, und weisen Sie der Serverentität denselben Namen wie der NetBIOS-Name des Webanwendungsservers zu.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
1 -  add server name <serverFQDN>
2
3 -  add service name serverName serviceType port
4 <!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **serverName**. Ein Name für die Citrix ADC Appliance, die verwendet wird, um auf diesen Server zu verweisen.
- **serverFQDN**. Der FQDN des Servers. Wenn dem Server keine Domäne zugewiesen ist, verwenden Sie die IP-Adresse des Servers und stellen Sie sicher, dass der Serverentitätsname mit dem NetBIOS-Namen des Webanwendungsservers übereinstimmt.
- **serviceName**. Ein Name für die Citrix ADC Appliance, die verwendet wird, um auf diesen Dienst zu verweisen.
- **type**. Das vom Dienst verwendete Protokoll, entweder HTTP oder MSSQLSVC.
- **port**. Der Port, auf dem der Dienst abhört. HTTP-Dienste hören normalerweise auf Port 80. Sichere HTTPS-Dienste hören normalerweise auf Port 443 ab.

Beispiel:

In den folgenden Beispielen werden Server- und Diensteinträge auf der Citrix ADC Appliance für den Webanwendungsserver was1.example.com hinzugefügt. Im ersten Beispiel wird der FQDN des Webanwendungsservers verwendet, im zweiten wird die IP-Adresse verwendet.

Um den Server und den Dienst mithilfe des FQDN des Webanwendungsservers, was1.example.com, hinzuzufügen, geben Sie die folgenden Befehle ein:

```
1 add server was1 was1.example.com
2 add service was1service was1 HTTP 80
3 <!--NeedCopy-->
```

Um den Server und den Dienst unter Verwendung der IP-Adresse des Webanwendungsservers und des NetBIOS-Namens hinzuzufügen, wobei die IP-Adresse des Webanwendungsservers 10.237.64.87 und der NetBIOS-Name WAS1 lautet, geben Sie die folgenden Befehle ein:


```
add server WAS1 10.237.64.87
add service was1service WAS1 HTTP 8
<!--NeedCopy-->
```

So erstellen Sie einen virtuellen Server für die Verkehrsverwaltung mit der CLI

Der virtuelle Server für die Datenverkehrsverwaltung verwaltet den Datenverkehr zwischen dem Client und dem Webanwendungsserver. Sie können entweder einen Lastenausgleichs- oder einen virtuellen Content Switching-Server als Traffic Management Server verwenden. Die SSO-Konfiguration ist für beide Typen gleich.

Um einen virtuellen Lastausgleichsserver zu erstellen, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
add lb vserver <vserverName> <type> <IP> <port>
<!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **vServerName**— Ein Name für die Citrix ADC Appliance, die verwendet wird, um auf diesen virtuellen Server zu verweisen.
- **type**—Das vom Dienst verwendete Protokoll, entweder HTTP oder MSSQLSVC.
- **IP**—Die IP-Adresse, die dem virtuellen Server zugewiesen ist. Dies wäre normalerweise eine IANA reservierte, nicht öffentliche IP-Adresse in Ihrem LAN.
- **port**: Der Port, auf dem der Dienst wartet. HTTP-Dienste hören normalerweise auf Port 80. Sichere HTTPS-Dienste hören normalerweise auf Port 443 ab.

Beispiel:

Um einen virtuellen Lastausgleichsserver namens tmvserver1 zu einer Konfiguration hinzuzufügen, die den HTTP-Datenverkehr an Port 80 verwaltet, ihm eine LAN-IP-Adresse von 10.217.28.20 zuweist und dann den virtuellen Lastausgleichsserver an den Dienst wasservice1 zu binden, geben Sie die folgenden Befehle ein:

```
add lb vserver tmvserver1 HTTP 10.217.28.20 80
bind lb vserver tmvserv1 wasservice1
<!--NeedCopy-->
```


So erstellen Sie einen virtuellen Authentifizierungsserver mit der CLI

Der virtuelle Authentifizierungsserver verwaltet den Authentifizierungsdatenverkehr zwischen dem Client und dem Authentifizierungsserver (LDAP). Um einen virtuellen Authentifizierungsserver zu erstellen, geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
1 add authentication vserver <authvserverName> SSL <IP> 443
2 <!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **AuthVServerName** — Ein Name für die Citrix ADC Appliance, die verwendet wird, um auf diesen virtuellen Authentifizierungsserver zu verweisen. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und nur Buchstaben, Zahlen und Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), at (@), Gleich (=), Doppelpunkt (:) und Unterstrich enthalten. Kann geändert werden, nachdem der virtuelle Authentifizierungsserver mithilfe des Befehls rename authentication vserver hinzugefügt wurde.
- **IP**—Die IP-Adresse, die dem virtuellen Authentifizierungsserver zugewiesen ist. Wie beim virtuellen Server für die Datenverkehrsverwaltung wäre diese Adresse normalerweise eine IANA-reservierte, nicht öffentliche IP-Adresse in Ihrem LAN.
- **domain**: Die dem virtuellen Server zugewiesene Domäne. Dies wäre normalerweise die Domäne Ihres Netzwerks. Bei der Konfiguration des virtuellen Authentifizierungsservers ist es üblich, wenn auch nicht erforderlich, die Domäne in allen Großbuchstaben einzugeben.

Beispiel:

Um einen virtuellen Authentifizierungsserver namens authverver1 zu Ihrer Konfiguration hinzuzufügen und ihm die LAN IP 10.217.28.21 und die Domäne EXAMPLE.COM zuzuweisen, geben Sie die folgenden Befehle ein:

```
1 add authentication vserver authvserver1 SSL 10.217.28.21 443
2 <!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Server zur Datenverkehrsverwaltung für die Verwendung eines Authentifizierungsprofils

Der virtuelle Authentifizierungsserver kann so konfiguriert werden, dass die Authentifizierung für eine einzelne Domäne oder für mehrere Domänen verarbeitet wird. Wenn es für die Unterstützung der Authentifizierung für mehrere Domänen konfiguriert ist, müssen Sie auch die Domäne für Citrix ADC

SSO angeben, indem Sie ein Authentifizierungsprofil erstellen und dann den virtuellen Server für die Datenverkehrsverwaltung so konfigurieren, dass dieses Authentifizierungsprofil verwendet wird.

> **Hinweis:**
>
> Der virtuelle Server zur Datenverkehrsverwaltung kann entweder ein virtueller Load Balancing- (lb) oder Content Switching-Server (cs) sein. In den folgenden Anweisungen wird davon ausgegangen, dass Sie einen virtuellen Lastausgleichsserver verwenden. Um einen virtuellen Content Switching-Server zu konfigurieren, verwenden Sie einfach
> set cs vserver statt set lb vserver. Das Verfahren ist ansonsten gleich.

Um das Authentifizierungsprofil zu erstellen und dann das Authentifizierungsprofil auf einem virtuellen Server zur Datenverkehrsverwaltung zu konfigurieren, geben Sie die folgenden Befehle ein:

```
1 -  add authentication authnProfile <authnProfileName> {
2  -authvserverName <string> }
3   {
4  -authenticationHost <string> }
5   {
6  -authenticationDomain <string> }
7
8 -  set lb vserver <vserverName> -authnProfile <authnprofileName>
9 <!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **authnProfileName**— Ein Name für das Authentifizierungsprofil. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und aus einem bis einunddreißig alphanumerischen oder Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), at (@), Gleich (=), Doppelpunkt (:) und Unterstrich bestehen.
- **AuthVServerName**— Der Name des virtuellen Authentifizierungsservers, den dieses Profil für die Authentifizierung verwendet.
- **AuthenticationHost**— Hostname des virtuellen Authentifizierungsservers.
- **AuthenticationDomain**— Domäne, für die Citrix ADC SSO die Authentifizierung verarbeitet. Erforderlich, wenn der virtuelle Authentifizierungsserver die Authentifizierung für mehr als eine Domäne durchführt, sodass die richtige Domäne eingeschlossen wird, wenn die Citrix ADC Appliance das Cookie des virtuellen Servers für die Datenverkehrsverwaltung festlegt.

Beispiel:

Um ein Authentifizierungsprofil namens AuthnProfile1 für die Authentifizierung der Domäne example.com zu erstellen und den virtuellen Lastausgleichsserver vserver1 für die Verwendung des Authentifizierungsprofils AuthnProfile1 zu konfigurieren, geben Sie die folgenden Befehle ein:


```
add authentication authnProfile authnProfile1 -authnvsName
   authvsesrver1
     -authenticationHost authvsesrver1 -authenticationDomain example.
        com
set lb vserver vserver1 -authnProfile authnProfile1
<!--NeedCopy-->
```

Single Sign-On konfigurieren

July 8, 2022

Das Konfigurieren von Citrix ADC Single Sign-On (SSO) für die Authentifizierung durch Identitätswechsel ist einfacher als die Konfiguration von SSO für die Authentifizierung durch Delegierung und ist daher vorzuziehen, wenn Ihre Konfiguration dies zulässt. Sie erstellen ein KCD-Konto. Sie können das Kennwort des Benutzers verwenden.

Wenn Sie das Kennwort des Benutzers nicht haben, können Sie Citrix ADC SSO so konfigurieren, dass es sich durch Delegierung authentifiziert. Obwohl die Delegierungsmethode komplexer ist als die Konfiguration von SSO für die Authentifizierung durch Identitätswechsel, bietet sie Flexibilität, da die Anmeldeinformationen eines Benutzers möglicherweise nicht unter allen Umständen für die Citrix ADC-Appliance verfügbar sind.

Für Identitätswechsel oder Delegierung müssen Sie auch die integrierte Authentifizierung auf dem Webanwendungsserver aktivieren.

Integrierte Authentifizierung auf dem Webanwendungsserver aktivieren

Um Citrix ADC Kerberos SSO auf jedem Webanwendungsserver einzurichten, den Kerberos SSO verwaltet, verwenden Sie die Konfigurationsoberfläche auf diesem Server, um den Server so zu konfigurieren, dass eine Authentifizierung erforderlich ist. Wählen Sie die Kerberos-Authentifizierung (Aushandeln) nach Präferenz aus, mit Fallback auf NTLM für Clients, die Kerberos nicht unterstützen.

Im Folgenden finden Sie Anweisungen zum Konfigurieren des Microsoft Internet Information Server (IIS), sodass eine Authentifizierung erforderlich ist. Wenn Ihr Webanwendungsserver eine andere Software als IIS verwendet, finden Sie Anweisungen in der Dokumentation zu dieser Webserver-Software.

So konfigurieren Sie Microsoft IIS für die Verwendung der integrierten Authentifizierung

1. Melden Sie sich beim IIS-Server an und öffnen Sie **Internet Information Services Manager.**

2. Wählen Sie die Website aus, für die Sie die integrierte Authentifizierung aktivieren möchten. Um die integrierte Authentifizierung für alle von IISM verwalteten IIS-Webserver zu aktivieren, konfigurieren Sie die Authentifizierungseinstellungen für die Standardwebsite. Um die integrierte Authentifizierung für einzelne Dienste (wie Exchange, Exadmin, ExchWeb und Public) zu ermöglichen, konfigurieren Sie diese Authentifizierungseinstellungen für jeden Dienst einzeln.
3. Öffnen Sie das **Eigenschaften-Dialogfeld** für die Standardwebsite oder für den einzelnen Dienst, und klicken Sie auf die Registerkarte **Verzeichnissicherheit** .
4. Wählen Sie neben **Authentifizierung** und **Zugriffssteuerung**die Option **Bearbeiten aus.**
5. Deaktivieren Sie den anonymen Zugriff.
6. Aktivieren Sie die integrierte Windows-Authentifizierung (nur). Durch die Aktivierung der integrierten Windows-Authentifizierung muss die Protokollaushandlung für den Webserver automatisch auf Negotiate (NTLM) festgelegt werden, wodurch die Kerberos-Authentifizierung mit Fallback auf NTLM für nicht Kerberos-fähige Geräte angegeben wird. Wenn diese Option nicht automatisch ausgewählt wird, setzen Sie die Protokollaushandlung manuell auf Aushandeln, NTLM.

Richten Sie SSO durch Identitätswechsel ein

Sie können das KCD-Konto für Citrix ADC SSO durch Identitätswechsel konfigurieren. In dieser Konfiguration erhält die Citrix ADC-Appliance den Benutzernamen und das Kennwort des Benutzers, wenn sich der Benutzer beim Authentifizierungsserver authentifiziert, und verwendet diese Anmeldeinformationen, um sich als Benutzer auszugeben, um ein Ticket Granting Ticket (TGT) zu erhalten. Wenn der Benutzername im UPN-Format vorliegt, bezieht die Appliance den Bereich des Benutzers von UPN. Andernfalls erhält es den Namen und den Bereich des Benutzers, indem es ihn aus der SSO-Domäne extrahiert, die bei der Erstauthentifizierung verwendet wurde, oder aus dem Sitzungsprofil.

> **Hinweis**
>
> Sie können keinen Benutzernamen mit Domäne hinzufügen, wenn der Benutzername bereits ohne Domäne hinzugefügt wurde. Wenn der Benutzername mit Domäne zuerst hinzugefügt wird, gefolgt von demselben Benutzernamen ohne Domäne, fügt die Citrix ADC-Appliance den Benutzernamen zur Benutzerliste hinzu.

Bei der Konfiguration des KCD-Kontos müssen Sie den Realm-Parameter auf den Bereich des Dienstes festlegen, auf den der Benutzer zugreift. Derselbe Bereich wird auch als Bereich des Benutzers verwendet, wenn der Bereich des Benutzers nicht durch Authentifizierung mit der Citrix ADC-Appliance oder aus dem Sitzungsprofil abgerufen werden kann.

So erstellen Sie das KCD-Konto für SSO durch Identitätswechsel mit einem Kennwort

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:


```
add aaa kcdaccount <accountname> -realmStr <realm>

<!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **accountname**. Der KCD-Kontoname.
- **realm**. Die Domäne, die dem Citrix ADC SSO zugewiesen ist.

Beispiel

Um ein KCD-Konto mit dem Namen kcdccount1 hinzuzufügen und das Schlüsselregister kcdvserver.keytab zu verwenden, geben Sie den folgenden Befehl ein:

```
add aaa kcdAccount kcdaccount1 -keytab kcdvserver.keytab

<!--NeedCopy-->
```

Informationen zum Konfigurieren des Kerberos-Identitätswechsels über die Citrix ADC GUI finden Sie unter Citrix Support.

SSO durch Delegierung konfigurieren

Um SSO nach Delegation zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

- Wenn Sie die Delegierung durch ein delegiertes Benutzerzertifikat konfigurieren, installieren Sie die entsprechenden CA-Zertifikate auf der Citrix ADC-Appliance und fügen Sie sie der Citrix ADC-Konfiguration hinzu.
- Erstellen Sie das KCD-Konto auf der Appliance. Die Appliance verwendet dieses Konto, um Servicetickets für Ihre geschützten Anwendungen zu erhalten.
- Konfigurieren Sie den Active Directory-Server.

> **Hinweis**
>
> Weitere Informationen zum Erstellen eines KCD-Kontos und zum Konfigurieren auf der NetScaler-Appliance finden Sie in den folgenden Themen:
>
> - Authentifizierung, Autorisierung und Audits mit Kerberos/NTLM
> - Wie Citrix ADC Kerberos für die Clientauthentifizierung implementiert
> - Konfigurieren der Kerberos-Authentifizierung auf der Citrix ADC-Appliance

Installieren des Client-CA-Zertifikats auf der Citrix ADC-Appliance

Wenn Sie das Citrix ADC SSO mit einem Clientzertifikat konfigurieren, müssen Sie das entsprechende CA-Zertifikat für die Clientzertifikatdomäne (das Clientzertifizierungsstellenzertifikat) auf die Citrix ADC-Appliance kopieren und dann das CA-Zertifikat installieren. Verwenden Sie zum Kopieren des Clientzertifizierungsstellenzertifikats das Dateiübertragungsprogramm Ihrer Wahl, um das Zertifikat und die Privatschlüsseldatei auf die Citrix ADC-Appliance zu übertragen und die Dateien in /nsconfig/ssl zu speichern.

So installieren Sie das Client-CA-Zertifikat auf der Citrix ADC-Appliance

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1 add ssl certKey <certkeyName> -cert <cert> [(-key <key> [-password]) |
     -fipsKey <fipsKey>][-inform ( DER | PEM )][-expiryMonitor ( ENABLED
     | DISABLED | UNSET ) [-notificationPeriod <positive_integer>]] [-
     bundle ( YES | NO )]
2
3 <!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **certkeyName**. Ein Name für das Client-CA-Zertifikat. Muss mit einem alphanumerischen ASCII-Zeichen oder einem Unterstrich (_) beginnen und muss aus einem bis einunddreißig Zeichen bestehen. Zulässige Zeichen sind alphanumerische ASCII-Zeichen, Unterstrich, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), Gleichheitszeichen (=) und Bindestrich (-). Kann nicht geändert werden, nachdem das Zertifikat-Schlüsselpaar erstellt wurde. Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “mein Zertifikat” oder “mein Zertifikat”).
- **cert**. Vollständiger Pfadname und Dateiname der X509-Zertifikatsdatei, die zur Bildung des Zertifikatsschlüsselpaars verwendet wurde. Die Zertifikatsdatei muss auf der Citrix ADC-Appliance im Verzeichnis /nsconfig/ssl/ gespeichert werden.
- **Schlüssel**. Vollständiger Pfadname und Dateiname der Datei, die den privaten Schlüssel zur X509-Zertifikatsdatei enthält. Die Schlüsseldatei muss auf der Citrix ADC-Appliance im Verzeichnis /nsconfig/ssl/ gespeichert werden.
- **password**. Wenn ein privater Schlüssel angegeben ist, wird die Passphrase verwendet, um den privaten Schlüssel zu verschlüsseln. Verwenden Sie diese Option, um verschlüsselte private Schlüssel im PEM-Format zu laden.
- **fipsKey**. Name des FIPS-Schlüssels, der im Hardware Security Module (HSM) einer FIPS-Appliance erstellt wurde, oder eines Schlüssels, der in das HSM importiert wurde.

> **Hinweis**
>
> Sie können entweder einen Schlüssel oder einen FIPSkey angeben, aber nicht beide.

- **inform**. Format des Zertifikats und der Privatschlüsseldateien, entweder PEM oder DER.
- **passplain**. Passphrase, die zum Verschlüsseln des privaten Schlüssels verwendet wird. Erforderlich für das Hinzufügen eines verschlüsselten privaten Schlüssels im PEM-Format.
- **expiryMonitor**. Konfigurieren Sie die Citrix ADC-Appliance so, dass eine Warnung ausgegeben wird, wenn das Zertifikat bald abläuft. Mögliche Werte: ENABLED, DISABLED, UNSET.
- **notificationPeriod**. Wenn `expiryMonitor` ENABLED ist, die Anzahl der Tage, bis das Zertifikat abläuft, um eine Warnung auszustellen.
- **bundle**. Analysieren Sie die Zertifikatkette als einzelne Datei, nachdem Sie das Serverzertifikat mit dem Zertifikat seines Ausstellers in der Datei verknüpft haben. Mögliche Werte: YES, NO.

Beispiel

Im folgenden Beispiel wird das angegebene delegierte Benutzerzertifikat customer-cert.pem zusammen mit dem Schlüssel customer-key.pem zur Citrix ADC-Konfiguration hinzugefügt und das Kennwort, das Zertifikatsformat, die Ablaufüberwachung und die Benachrichtigungsfrist festgelegt.

Um das delegierte Benutzerzertifikat hinzuzufügen, geben Sie die folgenden Befehle ein:

```
1 add ssl certKey customer -cert "/nsconfig/ssl/customer-cert.pem"
2 -key "/nsconfig/ssl/customer-key.pem" -password "dontUseDefaultPWs!"
3 -inform PEM -expiryMonitor ENABLED [-notificationPeriod 14]
4
5 <!--NeedCopy-->
```

Erstellen des KCD-Kontos

Wenn Sie Citrix ADC SSO durch Delegierung konfigurieren, können Sie das KCD-Konto so konfigurieren, dass es den Anmeldenamen und das Kennwort des Benutzers verwendet, den Anmeldenamen und die Keytab des Benutzers verwendet oder das Clientzertifikat des Benutzers verwendet. Wenn Sie SSO mit Benutzernamen und Kennwort konfigurieren, verwendet die Citrix ADC-Appliance das delegierte Benutzerkonto, um ein Ticket Granting Ticket (TGT) zu erhalten, und verwendet dann das TGT, um Servicetickets für die spezifischen Dienste zu erhalten, die jeder Benutzer anfordert. Wenn Sie SSO mit der Keytab-Datei konfigurieren, verwendet die Citrix ADC-Appliance das delegierte Benutzerkonto und die Keytab-Informationen. Wenn Sie SSO mit einem delegierten Benutzerzertifikat konfigurieren, verwendet die Citrix ADC-Appliance das delegierte Benutzerzertifikat.

> **Hinweis:**
>
> Bereichsübergreifend muss der servicePrincipalName des delegierten Benutzers das Format `host/<name>` haben. Wenn er nicht in diesem Format vorliegt, ändern Sie den servicePrincipalName des delegierten Benutzers `<servicePrincipalName>` in `host/<service-account-samaccountname>`. Sie können das Attribut des delegierten Benutzerkontos im Domänencontroller überprüfen. Eine Methode zum Ändern besteht darin, das Attribut `logonName` des delegierten Benutzers zu ändern.

So erstellen Sie das KCD-Konto für SSO durch Delegierung mit einem Kennwort

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
add aaa kcdAccount <kcdAccount> {
 -realmStr <string> }
  {
 -delegatedUser <string> }
  {
 -kcdPassword  }
  [-userRealm <string>]
[-enterpriseRealm <string>] [-serviceSPN <string>]
<!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **kcdAccount** — Ein Name für das KCD-Konto. Dies ist ein zwingendes Argument. Maximale Länge: 31
- **realmStr** - Der Bereich von Kerberos. Maximale Länge: 255
- **delegatedUser** — Der Benutzername, der die eingeschränkte Kerberos-Delegierung durchführen kann. Der delegierte Benutzername wird vom servicePrincipalName Ihres Domänencontrollers abgeleitet. Für Cross-Realm muss der servicePrincipalName des delegierten Benutzers das Format haben `host/<name>`. Maximale Länge: 255
- **kcdPassword** - Kennwort für delegierten Benutzer. Maximale Länge: 31
- **userRealm** - Bereich des Benutzers. Maximale Länge: 255
- **enterpriseRealm** - Enterprise-Bereich des Benutzers. Dies ist nur in bestimmten KDC-Bereitstellungen gegeben, in denen KDC den Enterprise-Benutzernamen anstelle von Principal Name erwartet. Maximale Länge: 255
- **serviceSPN** — Dienst-SPN. Wenn angegeben, wird dies zum Abrufen von Kerberos-Tickets verwendet. Wenn nicht angegeben, erstellt Citrix ADC SPN mit dem Dienst-FQDN. Maximale Länge: 255

Beispiel (UPN-Format):

Um ein KCD-Konto mit dem Namen kcdaccount1 zur Citrix ADC-Appliance-Konfiguration mit dem Kennwort Kennwort1 und einem Bereich von EXAMPLE.COM hinzuzufügen und das delegierte Benutzerkonto im UPN-Format (als root) anzugeben, geben Sie die folgenden Befehle ein:

```
1 add aaa kcdaccount kcdaccount1  - delegatedUser root
2 -kcdPassword password1 -realmStr EXAMPLE.COM
3
4 <!--NeedCopy-->
```

Beispiel (SPN-Format):

Um ein KCD-Konto mit dem Namen kcdaccount1 zur Citrix ADC-Appliance-Konfiguration mit dem Kennwort Kennwort1 und einem Bereich von EXAMPLE.COM hinzuzufügen und das delegierte Benutzerkonto im SPN-Format anzugeben, geben Sie die folgenden Befehle ein:

```
1 add aaa kcdAccount kcdaccount1 -realmStr EXAMPLE.COM
2 -delegatedUser "host/kcdvserver.example.com" -kcdPassword password1
3
4 <!--NeedCopy-->
```

Erstellen des KCD-Kontos für SSO durch Delegation mit einer Keytab

Wenn Sie eine Keytab-Datei für die Authentifizierung verwenden möchten, erstellen Sie zuerst die Keytab-Datei. Sie können die Keytab-Datei manuell erstellen, indem Sie sich am AD-Server anmelden und das Dienstprogramm `ktpass` verwenden, oder Sie können das Citrix ADC-Konfigurationsdienstprogramm verwenden, um ein Batchskript zu erstellen und dieses Skript dann auf dem AD-Server auszuführen, um die Keytab-Datei zu generieren. Verwenden Sie als Nächstes FTP oder ein anderes Dateiübertragungsprogramm, um die Keytab-Datei auf die Citrix ADC-Appliance zu übertragen und im Verzeichnis /nsconfig/krb abzulegen. Konfigurieren Sie abschließend das KCD-Konto für Citrix ADC SSO durch Delegierung und geben Sie der Citrix ADC-Appliance den Pfad und den Dateinamen der Keytab-Datei an.

> **Hinweis:**
>
> Wenn Sie für Cross-Realm die Keytab-Datei als Teil des KCD-Kontos abrufen möchten, verwenden Sie den folgenden Befehl für den aktualisierten delegierten Benutzernamen.
>
> Erstellen Sie im Domänencontroller eine aktualisierte Keytab-Datei.
>
> `ktpass /princ <servicePrincipalName-with-prefix<host/>Of-delegateUser >@<DC REALM in uppercase> /ptype KRB5_NT_PRINCIPAL /mapuser <DC REALM`

> in uppercase>\<sAMAccountName> /pass <delegatedUserPassword> -out filepathfor.keytab
>
> Die Datei `filepathfor.keytab` kann in der Citrix ADC-Appliance abgelegt und als Teil der Keytab-Konfiguration im ADC KCD-Konto verwendet werden.

So erstellen Sie die Keytab-Datei manuell

Melden Sie sich an der AD-Server-Befehlszeile an und geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
ktpass princ <SPN> ptype KRB5_NT_PRINCIPAL mapuser <DOMAIN><username>
   pass <password> -out <File_Path>
<!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **SPN**. Der Dienstprinzipalname für das KCD-Dienstkonto.
- **DOMAIN**. Die Domäne des Active Directory-Servers.
- **username**. Der Benutzername des KSA-Kontos.
- **password**. Das Kennwort für das KSA-Konto.
- **path**. Der vollständige Pfadname des Verzeichnisses, in dem die Keytab-Datei gespeichert werden soll, nachdem sie generiert wurde.

So erstellen Sie mit dem Citrix ADC-Konfigurationsdienstprogramm ein Skript zum Generieren der Keytab-Datei

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr.**
2. Klicken Sie im Datenbereich unter **Kerberos Constrained Delegation**auf **Batch-Datei**, um Keytab zu generieren.
3. Legen Sie im Dialogfeld **KCD (Kerberos Constrained Delegation)-Keytab-Skript generieren** die folgenden Parameter fest:
   - **Domänenbenutzername**. Der Benutzername des KSA-Kontos.
   - **Domänenkennwort**. Das Kennwort für das KSA-Konto.
   - **Dienstprinzipal**. Der Name des Dienstprinzipals für die KSA.
   - **Name der Ausgabedatei**. Der vollständige Pfad und Dateiname, unter dem die Keytab-Datei auf dem AD-Server gespeichert werden soll.
4. Deaktivieren **Sie das Kontrollkästchen Domänenbenutzerkonto erstellen** .
5. Klicken Sie auf **Skript generieren**.
6. Melden Sie sich beim Active Directory-Server an und öffnen Sie ein Befehlszeilenfenster.

7. Kopieren Sie das Skript aus dem Fenster **Generiertes Skript** und fügen Sie es direkt in das Befehlszeilenfenster des Active Directory-Servers ein. Die keytab wird generiert und im Verzeichnis unter dem Dateinamen gespeichert, den Sie als **Ausgabedateiname** angegeben haben.
8. Verwenden Sie das Dateiübertragungsprogramm Ihrer Wahl, um die Keytab-Datei vom Active Directory-Server auf die Citrix ADC-Appliance zu kopieren und im Verzeichnis /nsconfig/krb abzulegen.

So erstellen Sie das KCD-Konto

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1 add aaa kcdaccount <accountname>  -keytab <keytab>
2 <!--NeedCopy-->
```

Beispiel

Um ein KCD-Konto mit dem Namen kcdccount1 hinzuzufügen und das Keytab mit dem Namen kcdvserver.keytab zu verwenden, geben Sie die folgenden Befehle ein:

```
1 add aaa kcdaccount kcdaccount1  -keytab kcdvserver.keytab
2 <!--NeedCopy-->
```

So erstellen Sie das KCD-Konto für SSO durch Delegation mit einem delegierten Benutzerzertifikat

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1 add aaa kcdaccount <accountname> -realmStr <realm> -delegatedUser <
     user_nameSPN> -usercert <cert> -cacert <cacert>
2 <!--NeedCopy-->
```

Ersetzen Sie für die Variablen die folgenden Werte:

- **accountname**. Ein Name für das KCD-Konto.
- **realmStr**. Der Bereich für das KCD-Konto, normalerweise die Domäne, für die SSO konfiguriert ist.
- **delegatedUser**. Der delegierte Benutzername im SPN-Format.
- **usercert**. Der vollständige Pfad und Name der delegierten Benutzerzertifikatdatei auf der Citrix ADC-Appliance. Das delegierte Benutzerzertifikat muss sowohl das Clientzertifikat als auch

den privaten Schlüssel enthalten und muss im PEM-Format vorliegen. Wenn Sie die Smartcard-Authentifizierung verwenden, müssen Sie eine Smartcard-Zertifikatsvorlage erstellen, damit Zertifikate mit dem privaten Schlüssel importiert werden können.

- **cacert**. Der vollständige Pfad und der Name der CA-Zertifikatsdatei auf der Citrix ADC-Appliance.

Beispiel

Um ein KCD-Konto mit dem Namen kcdccount1 hinzuzufügen und das Schlüsselregister kcdvserver.keytab zu verwenden, geben Sie den folgenden Befehl ein:

```
1 add aaa kcdaccount kcdaccount1 -realmStr EXAMPLE.COM
2      -delegatedUser ”host/kcdvserver.example.com” -usercert /certs/
          usercert
3      -cacert /cacerts/cacert
4 <!--NeedCopy-->
```

Active Directory für Citrix ADC SSO einrichten

Wenn Sie SSO durch Delegierung konfigurieren, müssen Sie nicht nur das KCD-Konto auf der Citrix ADC-Appliance erstellen, sondern auch ein passendes Kerberos-Dienstkonto (KSA) auf Ihrem LDAP-Active Directory-Server erstellen und den Server für SSO konfigurieren. Verwenden Sie zum Erstellen des KSA den Kontoerstellungsprozess auf dem Active Directory-Server. Um SSO auf dem Active Directory-Server zu konfigurieren, öffnen Sie das Eigenschaftenfenster für den KSA. Auf der Registerkarte **Delegierung** aktivieren Sie die folgenden Optionen: Vertrauen Sie diesem Benutzer für die Delegierung nur an bestimmte Dienste und Verwenden Sie ein beliebiges Authentifizierungsprotokoll. (Die Option “Nur Kerberos” funktioniert nicht, da sie keinen Protokollübergang oder eingeschränkte Delegierung ermöglicht.) Fügen Sie abschließend die Dienste hinzu, die Citrix ADC SSO verwaltet.

> **Hinweis:**
>
> Wenn die Registerkarte Delegierung im Dialogfeld Eigenschaften des KSA-Kontos nicht angezeigt wird, müssen Sie den Active Directory-Server mit dem Befehlszeilentool Microsoft setspn so konfigurieren, dass die Registerkarte sichtbar ist, bevor Sie den KSA wie beschrieben konfigurieren können.

Konfigurieren der Delegierung für das Kerberos-Dienstkonto

1. Klicken Sie im Dialogfeld zur Konfiguration des LDAP-Kontos für das Kerberos-Dienstkonto, das Sie erstellt haben, auf die Registerkarte **Delegierung** .

2. Wählen Sie **Diesem Benutzer nur für die Delegierung an die angegebenen Dienste vertrauen**.
3. Wählen Sie unter Nur diesem Benutzer für die Delegierung an die angegebenen Dienste vertrauen die Option **Beliebiges Authentifizierungsprotokoll verwenden**.
4. Klicken Sie unter Dienste, denen dieses Konto delegierte Anmeldeinformationen präsentieren kann, auf **Hinzufügen.**
5. Klicken **Sie im Dialogfeld Dienste hinzufügen** auf **Benutzer** oder **Computer**, wählen Sie den Server aus, der die Ressourcen hostet, die dem Dienstkonto zugewiesen werden sollen, und klicken Sie dann auf **OK.**

   > **Hinweis:**
   >
   > - Die eingeschränkte Delegierung unterstützt keine Dienste, die in anderen Domänen als der dem Konto zugewiesenen Domäne gehostet werden, obwohl Kerberos möglicherweise eine Vertrauensbeziehung zu anderen Domänen hat.
   > - Verwenden Sie den folgenden Befehl, um `setspn` zu erstellen, wenn ein neuer Benutzer im Active Directory erstellt wird: `setspn -A host/kcdvserver.example.com example\kcdtest`

6. Zurück im Dialogfeld **Dienste hinzufügen** in der Liste Verfügbare Dienste wählen Sie die Dienste aus, die dem Dienstkonto zugewiesen sind. Citrix ADC SSO unterstützt die HTTP- und MSSQLSVC-Dienste.
7. Klicken Sie auf **OK.**

Konfigurationsänderungen, damit KCD untergeordnete Domänen unterstützen kann

Wenn das KCD-Konto mit `samAccountName` für `-delegatedUser` konfiguriert ist, funktioniert KCD nicht für Benutzer, die auf Dienste aus untergeordneten Domänen zugreifen. In diesem Fall können Sie die Konfiguration auf der Citrix ADC-Appliance und im Active Directory ändern.

- Ändern Sie den Anmeldenamen des Dienstkontos `<service-account-samaccountname>` (das im KCD-Konto als delegateUser konfiguriert ist) in AD in das Format `host/<service-account-samaccountname>.<completeUSERDNSDOMAIN>` (z. B. `host/svc_act.child.parent.com`).

  Sie können das Dienstkonto manuell oder über den Befehl `ktpass` ändern. Das aktualisiert das Dienstkonto `ktpass` automatisch.

  ```
  ktpass /princ host/svc_act.child.parent.com@CHILD.PARENT.COM /ptype KRB5_NT_PRINCIPAL /mapuser CHILD\sv_act /pass serviceaccountpassword -out filepathfor.keytab
  ```

- Ändern Sie delegatedUser im KCD-Konto auf der Citrix ADC-Appliance.

- Ändern Sie den Parameter -delegatedUser im KCD-Konto in `host/svc_act.child.parent.com`

Zu beachtende Punkte, wenn erweiterte Verschlüsselungen zur Konfiguration des KCD-Kontos verwendet werden

- **Beispielkonfiguration bei Verwendung von Keytab:** `add kcdaccount lbvs_keytab_aes256 -keytab "/nsconfig/krb/kcd2_aes256.keytab"`
- **Verwenden Sie den folgenden Befehl, wenn keytab über mehrere Verschlüsselungstypen verfügt.** Der Befehl erfasst auch Domänenbenutzerparameter: `add kcdaccount lbvs_keytab_aes256 -keytab "/nsconfig/krb/kcd2_aes256.keytab"-domainUser "HTTP/lbvs.aaa.local"`
- **Verwenden Sie die folgenden Befehle, wenn Benutzeranmeldeinformationen verwendet werden:** `add kcdaccount kslb2_user -realmStr AAA.LOCAL -delegatedUser lbvs -kcdPassword <password>`
- Stellen Sie sicher, dass die richtigen **domainUser**-Informationen bereitgestellt werden. Sie können in AD nach dem Benutzeranmeldenamen suchen.

Generieren des KCD Keytab-Skripts

October 5, 2021

Im Dialogfeld KCD-Keytab-Skript wird das Keytab-Skript generiert, das wiederum die für die Konfiguration von KCD im Citrix ADC erforderliche Keytab-Datei generiert.

So generieren Sie das KCD-Keytab-Skript mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr.**
2. Klicken Sie im Detailbereich unter **Kerberos-eingeschränkte Delegierung** auf Batchdatei, um Keytab zu generieren.
3. Füllen Sie im Dialogfeld KCD generieren (Kerberos Constrained Delegation) **Keytab Skript** die Felder wie unten beschrieben aus.
   - **Domänenbenutzername:** Der Name des Domänenbenutzers.
   - **Domänenkennwort:** Das Kennwort für den Domänenbenutzer.
   - **Service Principal:** Der Service-Principal.
   - **Ausgabedateiname:** Ein Dateiname für die KCD-Skriptdatei.
   - **Domänenbenutzerkonto erstellen:** Aktivieren Sie dieses Kontrollkästchen, um das angegebene Domänenbenutzerkonto zu erstellen.

4. Klicken Sie auf **Skript generieren**, um das Skript zu generieren. Das Skript wird generiert und wird im Textfeld **Generiertes Skript** unterhalb der Schaltfläche **Skript generieren** angezeigt.
5. Kopieren Sie das Skript, und speichern Sie es als Datei auf dem AD-Domänencontroller. Sie müssen dieses Skript nun auf dem Domänencontroller ausführen, um die keytab-Datei zu generieren, und dann die keytab-Datei in das Verzeichnis /nsconfig/krb/auf der Citrix ADC Appliance kopieren.
6. Klicken Sie auf **OK.**

SSO für Basic-, Digest- und NTLM-Authentifizierung

October 5, 2021

Die Single Sign-On (SSO) -Konfiguration in Citrix ADC und Citrix Gateway kann auf globaler Ebene und auch pro Traffic-Ebene aktiviert werden. Standardmäßig ist die SSO-Konfiguration **AUS**, und ein Administrator kann das SSO pro Datenverkehr oder global aktivieren. Aus Sicherheitsgründen empfiehlt Citrix Administratoren, SSO global **auszuschalten** und pro Traffic-Basis zu aktivieren. Diese Verbesserung soll die SSO-Konfiguration sicherer machen, indem bestimmte Arten von SSO-Methoden weltweit entehrt werden.

> **Hinweis:**
>
> Ab dem Citrix ADC Feature Release 13.0 Build 64.35 und höher werden die folgenden SSO-Typen weltweit entehrt.
>
> - Basic-Authentifizierung
> - Digest-Zugriffs-Authentifizierung
> - NTLM ohne NTLM2 Schlüssel oder Negotiate Sign

Nicht betroffene SSO-Typen

Die folgenden SSO Typen sind von dieser Verbesserung nicht betroffen.

- Kerberos-Authentifizierung
- SAML-Authentifizierung
- Formularbasierte Authentifizierung
- OAuth Bearer-Authentifizierung
- NTLM mit Negotiate NTLM2-Schlüssel oder Negotiate-Zeichen

Beeinträchtigte Single Sign-On-Konfigurationen

Im Folgenden sind die betroffenen (entehrten) SSO-Konfigurationen aufgeführt.

Globale Konfigurationen

```
set tmsessionparam -SSO ON
set vpnparameter -SSO ON
add tmsessionaction tm_act -SSO ON
add vpn sessionaction tm_act -SSO ON
Per traffic configurations
add vpn trafficaction tf_act http -SSO ON
add tm trafficaction tf_act -SSO ON
<!--NeedCopy-->
```

Konfigurationen pro Datenverkehr

```
add vpn trafficaction tf_act http -SSO ON
add tm trafficaction tf_act -SSO ON
<!--NeedCopy-->
```

> Sie können SSO als Ganzes aktivieren/deaktivieren und können einzelne SSO-Typen nicht ändern.

Zu beantragende Sicherheitsmaßnahmen

Im Rahmen der Sicherheitsmaßnahmen werden sicherheitsrelevante SSO-Typen in der globalen Konfiguration entehrt, sind jedoch nur über eine Traffic-Aktionskonfiguration zulässig.
Wenn also ein Back-End-Server Basic, Digest oder NTLM ohne Negotiate NTLM2 Key oder Negotiate Sign erwartet, kann der Administrator SSO nur über die folgende Konfiguration zulassen.

Traffic-Aktion

```
add vpn trafficaction tf_act  http -SSO ON
add tm trafficaction tf_act -SSO ON
<!--NeedCopy-->
```

Verkehrsrichtlinie

```
add tm trafficpolicy <name> <rule> tf_act
add vpn trafficpolicy <name> <rule> tf-act
<!--NeedCopy-->
```


> Der Administrator muss eine entsprechende Regel für die Verkehrsrichtlinie konfiguriert haben, um sicherzustellen, dass SSO nur für vertrauenswürdige Backend-Server aktiviert ist.

AAA-TM

Szenarien basierend auf globaler Konfiguration:

```
set tmsessionparam -SSO ON
<!--NeedCopy-->
```

Workaround:

```
add tm trafficaction tf_act -SSO ON
add tm trafficpolicy tf_pol true tf_act
<!--NeedCopy-->
```

Binden Sie die folgende Verkehrsrichtlinie an alle virtuellen LB-Server, auf denen SSO erwartet wird:

```
bind lb vserver <LB VS Name> -policy tf_pol -priority 65345
<!--NeedCopy-->
```

Szenarien basierend auf der Konfiguration der Sitzungsrichtlinien:

```
add tmsessionaction tm_act -SSO ON
add tmsession policy <name> <rule> tm_act
add tm trafficaction tf_act -SSO ON
add tm trafficpolicy tf_pol <same rule as session Policy> tf_act
<!--NeedCopy-->
```

Punkte der Hinweis:

- Der Citrix ADC AAA-Benutzer/die Gruppe für die vorhergehende Sitzungsrichtlinie muss durch eine Verkehrsrichtlinie ersetzt werden.
- Binden Sie die folgende Richtlinie an die virtuellen Lastausgleichsserver für die vorangegangene Sitzungsrichtlinie,


```
bind lb vserver [LB VS Name] -policy tf_pol -priority 65345
<!--NeedCopy-->
```

- Wenn eine Verkehrsrichtlinie mit anderer Priorität konfiguriert ist, ist der vorhergehende Befehl nicht gut.

Der folgende Abschnitt befasst sich mit Szenarien, die auf Konflikten mit mehreren Verkehrsrichtlinien im Zusammenhang mit einem Traffic basieren:

Für einen bestimmten TM-Verkehr wird nur eine TM-Verkehrsrichtlinie angewendet. Aufgrund der globalen Einstellung von SSO-Funktionsänderungen ist die Anwendung einer zusätzlichen TM-Verkehrsrichtlinie mit niedriger Priorität möglicherweise nicht anwendbar, wenn eine TM-Verkehrsrichtlinie mit hoher Priorität (die keine erforderliche SSO-Konfiguration hat) bereits angewendet wird. Im folgenden Abschnitt wird die Methode beschrieben, mit der sichergestellt wird, dass solche Fälle behandelt werden.

Bedenken Sie, dass die folgenden drei Verkehrsrichtlinien mit höherer Priorität auf virtuellen Lastausgleichsserver (LB) angewendet werden:

```
add tm trafficaction tf_act1 <Addition config>
add tm trafficaction tf_act2 <Addition config>
add tm trafficaction tf_act3 <Addition config>

add tm trafficpolicy tf_pol1 <rule1> tf_act1
add tm trafficpolicy tf_pol2 <rule2> tf_act2
add tm trafficpolicy tf_pol3 <rule3> tf_act3

bind lb vserver <LB VS Name> -policy tf_pol1 -priority 100
bind lb vserver <LB VS Name> -policy tf_pol2 -priority 200
bind lb vserver <LB VS Name> -policy tf_pol3 -priority 300
<!--NeedCopy-->
```

Fehleranfällige Methode - Um die globale SSO-Konfiguration zu lösen, fügen Sie die folgende Konfiguration hinzu:

```
add tm trafficaction tf_act_default -SSO ON
add tm trafficpolicy tf_pol_default true tf_act_default

bind lb vserver <LB VS Name> -policy tf_pol_default -priority 65345
<!--NeedCopy-->
```


Hinweis: Die vorhergehende Änderung kann SSO für Traffic, der trifft, <tf_pol1/tf_pol2/tf_pol3> wie für diese Traffic- und Verkehrsrichtlinie unterbrechen <tf_pol_default> wird nicht angewendet.

Richtige Methode - Um dies zu mindern, muss die SSO-Eigenschaft für jede der entsprechenden Verkehrsaktionen einzeln angewendet werden:

Zum Beispiel muss im vorhergehenden Szenario die folgende Konfiguration zusammen mit angewendet werden, damit SSO für den Datenverkehr auf tf_pol1/tf_pol3 trifft <tf_pol_default>.

```
add tm trafficaction tf_act1 <Addition config> -SSO ON
add tm trafficaction tf_act3 <Addition config> -SSO ON
<!--NeedCopy-->
```

Citrix Gateway -Fälle

Szenarien basierend auf globaler Konfiguration:

```
set vpnparameter -SSO ON
<!--NeedCopy-->
```

Workaround:

```
add vpn trafficaction vpn_tf_act http  -SSO ON
add vpn trafficpolicy vpn_tf_pol  true vpn_tf_act
bind the following traffic policy to all VPN virtual server where SSO
   is expected:
bind vpn vserver vpn_vs -policy vpn_tf_pol -priority 65345
<!--NeedCopy-->
```

Szenarien basierend auf der Konfiguration der Sitzungsrichtlinien:

```
add vpn sessionaction vpn_sess_act -SSO ON
add vpnsession policy <name> <rule> vpn_sess_act
<!--NeedCopy-->
```

Zu beachtenswerte Punkte:

- Der Citrix ADC AAA-Benutzer/die Gruppe für die vorhergehende Sitzungsrichtlinie muss durch eine Verkehrsrichtlinie ersetzt werden.

- Binden Sie die folgende Richtlinie an die virtuellen LB-Server für die vorangehende Sitzungsrichtlinie `bind lb virtual server [LB VS Name] -policy tf_pol -priority 65345`.
- Wenn eine Verkehrsrichtlinie mit anderer Priorität konfiguriert ist, ist der vorhergehende Befehl nicht gut. Der folgende Abschnitt befasst sich mit Szenarien, die auf Konflikten mit mehreren Verkehrsrichtlinien im Zusammenhang mit dem Datenverkehr basieren.

Funktionale Szenarien, die auf Konflikten mit mehreren Verkehrsrichtlinien basieren, die mit einem Datenverkehr verbunden sind:

Für einen bestimmten Citrix Gateway Verkehr wird nur eine VPN-Verkehrsrichtlinie angewendet. Aufgrund der globalen Einstellung von SSO-Funktionsänderungen ist die Anwendung einer zusätzlichen VPN-Verkehrsrichtlinie mit niedriger Priorität möglicherweise nicht anwendbar, wenn es andere VPN-Verkehrsrichtlinien mit hoher Priorität gibt, die keine erforderliche SSO-Konfiguration haben.

Im folgenden Abschnitt wird die Methode beschrieben, mit der sichergestellt wird, dass solche Fälle behandelt werden:

Bedenken Sie, dass es drei Verkehrsrichtlinien mit höherer Priorität gibt, die auf einen virtuellen VPN-Server angewendet werden

```
add vpn trafficaction tf_act1 <Addition config>
add vpn trafficaction tf_act2 <Addition config>
add vpn trafficaction tf_act3 <Addition config>

add vpn trafficpolicy tf_pol1 <rule1> tf_act1
add vpn trafficpolicy tf_pol2 <rule2> tf_act2
add vpn trafficpolicy tf_pol3 <rule3> tf_act3

bind vpn vserver <VPN VS Name> -policy tf_pol1 -priority 100
bind vpn vserver <VPN VS Name> -policy tf_pol2 -priority 200
bind vpn vserver <VPN VS Name> -policy tf_pol3 -priority 300
<!--NeedCopy-->
```

Fehleranfällige Methode: Um die globale SSO-Konfiguration zu lösen, fügen Sie die folgende Konfiguration hinzu:

```
add vpn trafficaction tf_act_default -SSO ON
add vpn trafficpolicy tf_pol_default true tf_act_default

bind vpn vserver <VPN VS Name> -policy tf_pol_default -priority 65345
<!--NeedCopy-->
```


Hinweis: Die vorhergehende Änderung kann SSO für den Traffic, der trifft, <tf_pol1/tf_pol2/tf_pol3> wie für diesen Traffic und die Verkehrsrichtlinie unterbrechen <tf_pol_default> wird nicht angewendet.

Richtige Methode: Um dies zu mindern, muss die SSO-Eigenschaft für jede der entsprechenden Verkehrsaktionen einzeln angewendet werden.

Zum Beispiel im vorherigen Szenario muss die folgende Konfiguration zusammen mit angewendet werden, damit SSO für Datenverkehr auf tf_pol1/tf_pol3 trifft <tf_pol_default>.

```
add vpn trafficaction tf_act1 [Additional config] -SSO ON

add vpn trafficaction tf_act3 [Additional config] -SSO ON
<!--NeedCopy-->
```

Rewrite für Citrix Gateway und Authentifizierungsserver generierte Antworten

October 5, 2021

Rewrite bezieht sich auf das Umschreiben einiger Informationen in den Anforderungen oder Antworten, die von der Citrix ADC Appliance verarbeitet werden. Das Umschreiben kann dazu beitragen, Zugriff auf die angeforderten Inhalte zu gewähren, ohne unnötige Details über die tatsächliche Konfiguration der Website preiszugeben. Ausführliche Informationen zum Rewrite-Konzept finden Sie unter Rewrite

Ausgehend von Citrix ADC Release Build 13.0-76.29 wurde die Unterstützung für Rewrite-Richtlinien auf den virtuellen Citrix Gateway-Server und vom Authentifizierungsserver generierte Antworten ausgeweitet.

> **Hinweis**
>
> Ein Bind-Typ **AAA_Response** wird eingeführt, um Rewrite-Richtlinien für virtuelle Citrix Gateway-Server und vom Authentifizierungsserver generierte Antworten zu unterstützen.

Ein Beispiel für die Verwendung von Rewrite

Sie können Rewrite verwenden, um die on-premises verfügbaren Ressourcen Citrix ADC für die Citrix Cloud-Bereitstellung freizugeben. Dies kann durch die Implementierung von CORS Origin Resource Sharing sicher erreicht werden. Rewrite kann wie folgt verwendet werden, um den CORS-Header zu implementieren.

Beispielkonfiguration

```
add rewrite action cors_header_action insert_http_header access-control
    -allow-credentials ”true”

add rewrite policy cors_header_pol true cors_header_action

add rewrite action non_cors_header_action insert_http_header X-Frame-
    Options '”DENY”'

add rewrite policy non_cors_header_pol true non_cors_header_action

bind authentication vserver av_cors -policy cors_header_pol -priority
    100 -type AAA_RESPONSE

bind vpn vserver av_cors -policy cors_header_pol -priority 100 -type
    AAA_RESPONSE
```

Unterstützung für Antwortheader der Inhaltssicherheitsrichtlinie für Citrix Gateway und von virtuellen Servern generierte Authentifizierungsantworten

July 8, 2022

Ab Citrix ADC Release Build 13.0—76.29 wird der Content-Security-Policy (CSP) -Antwortheader für von Citrix Gateway und virtuelle Authentifizierungsserver generierte Antworten unterstützt.

Der Content-Security-Policy (CSP) Response-Header ist eine Kombination von Richtlinien, die der Browser verwendet, um Cross-Site-Scripting (CSS) -Angriffe zu vermeiden.
Der HTTP-CSP-Antwortheader ermöglicht es Website-Administratoren, die Ressourcen zu steuern, die der Benutzeragent für eine bestimmte Seite laden darf. Mit wenigen Ausnahmen beinhalten Richtlinien hauptsächlich die Angabe von Serverursprüngen und Skript-Endpunkten. Dies schützt vor Cross-Site-Scripting-Angriffen.
Der CSP-Header wurde entwickelt, um die Art und Weise zu ändern, wie Browser Seiten rendern, und schützt damit vor verschiedenen standortübergreifenden Einschleusungen, einschließlich CSS. Es ist wichtig, den Header-Wert korrekt einzustellen, so dass der ordnungsgemäße Betrieb der Website nicht verhindert wird. Wenn der Header beispielsweise so eingestellt ist, dass er die Ausführung von Inline-JavaScript verhindert, darf die Website auf ihren Seiten kein Inline-JavaScript verwenden.

Im Folgenden sind die Vorteile des CSP-Antwort-Headers aufgeführt.

- Die Hauptfunktion eines CSP-Antwortheaders besteht darin, CSS-Angriffe zu verhindern.
- Neben der Einschränkung der Domänen, aus denen Inhalte geladen werden können, kann der Server angeben, welche Protokolle verwendet werden dürfen. Zum Beispiel (und idealerweise aus Sicherheitssicht) kann ein Server angeben, dass alle Inhalte unter Verwendung von HTTPS geladen werden müssen.
- CSP hilft dabei, Citrix ADC vor standortübergreifenden Scripting-Angriffen zu schützen, indem er Dateien wie “tmindex.html” und “homepage.html” sichert. Die Datei “tmindex.html” bezieht sich auf die Authentifizierung und die Datei “homepage.html” bezieht sich auf die veröffentlichten Apps/Links.

Konfigurieren des Content-Security-Policy-Headers für Citrix Gateway und Authentifizierung von virtuellen Servern generierten Antworten

Um den CSP-Header zu aktivieren, müssen Sie Ihren Webserver so konfigurieren, dass er den CSP-HTTP-Header zurückgibt.

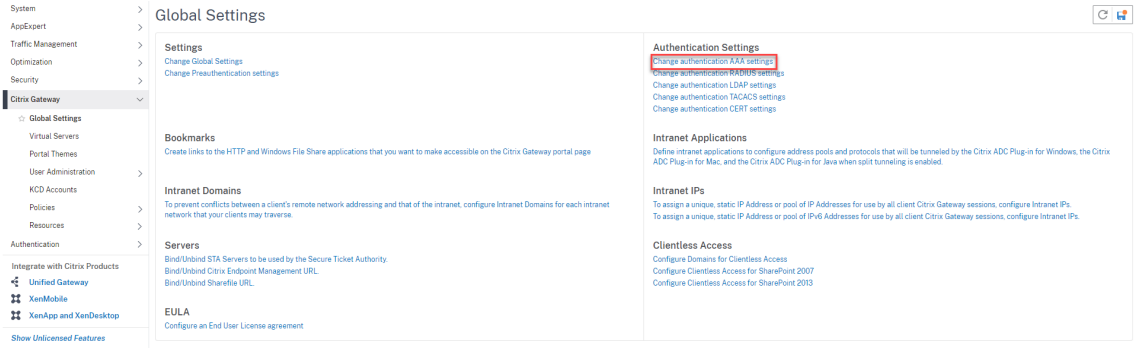
> **Wichtige Hinweise**
>
> - Standardmäßig ist der CSP-Header deaktiviert.
> - Beim Aktivieren oder Deaktivieren der Standard-CSP-Richtlinie wird empfohlen, den folgenden Befehl auszuführen. `Flush cache contentgroup loginstaticobjects`
> - Um den CSP für /logon/LogonPoint/index.html zu ändern, ändern Sie den Wert “Header set Content-Security-Policy” wie erforderlich in dem Abschnitt, der dem Anmeldeverzeichnis entspricht, das unter dem Verzeichnis `/var/netscaler/logon` ist.

Um CSP für den Authentifizierungsserver und von Citrix Gateway generierte Antworten mit CLI zu konfigurieren, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

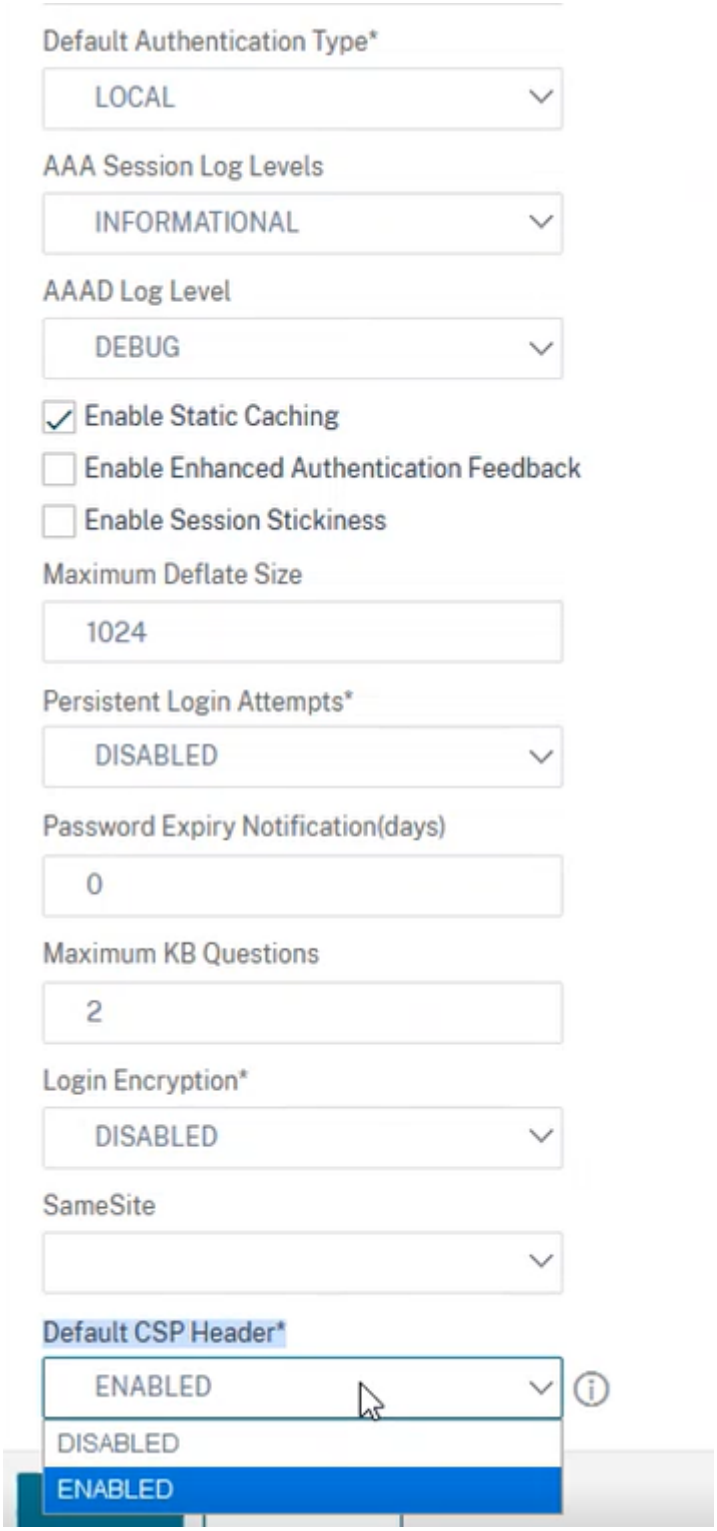
```
1 set aaa parameter -defaultCSPHeader <ENABLE/DISABLE>
```

So konfigurieren Sie CSP für Citrix Gateway und Authentifizierung von virtuellen Servern generierten Antworten über die GUI.

1. Navigieren Sie zu **Citrix Gateway > Globale Einstellungen** und klicken Sie unter **Authentifizierungseinstellungen auf AAA-Einstellungen für Authentifizierung ändern**.



2. Wählen Sie auf der Seite **AAA-Parameter konfigurieren** das Feld **In Standard-CSP-Header aktiviert** aus.



Ein Beispiel für die Anpassung der Kopfzeile von Content-Security-Policy

Im Folgenden finden Sie ein Beispiel für die Anpassung von CSP-Headern, um Images und Skripts nur aus den folgenden beiden angegebenen Quellen einzuschließen: `https://company.fqdn.com`, `https://example.com`.

Beispiel-Konfiguration

```
1 add rewrite action modify_csp insert_http_header Content-Security-
     Policy ”\”default-src 'self'; script-src 'self' https://company.fqdn
     .com 'unsafe-inline' 'unsafe-eval'; connect-src 'self'; img-src http
     ://localhost:* https://example.com 'self' data: http: https:; style-
     src 'self' 'unsafe-inline'; font-src 'self'; frame-src 'self'; child
     -src 'self' com.citrix.agmacepa://* citrixng://* com.citrix.
     nsgclient://*; form-action 'self'; object-src 'self'; report-uri /
     nscsp_violation/report_uri\””
2
3 add rewrite policy add_csp true modify_csp
4
5 bind authentication vserver auth1 -policy add_csp -priority 1 -
     gotoPriorityExpression NEXT -type AAA_RESPONSE
```

Benutzerseitige Kennwortzurücksetzung

September 28, 2022

Das Self-Service-Kennwort-Zurücksetzen ist eine webbasierte Kennwortverwaltungslösung. Es ist sowohl in der Authentifizierungs-, Autorisierungs- und Überwachungsfunktion der Citrix ADC-Appliance als auch in Citrix Gateway verfügbar. Dadurch entfällt die Abhängigkeit des Benutzers von der Unterstützung des Administrators beim Ändern des Kennworts.

Das Self-Service-Kennwort-Reset bietet dem Endbenutzer die Möglichkeit, ein Kennwort in den folgenden Szenarien sicher zurückzusetzen oder zu erstellen:

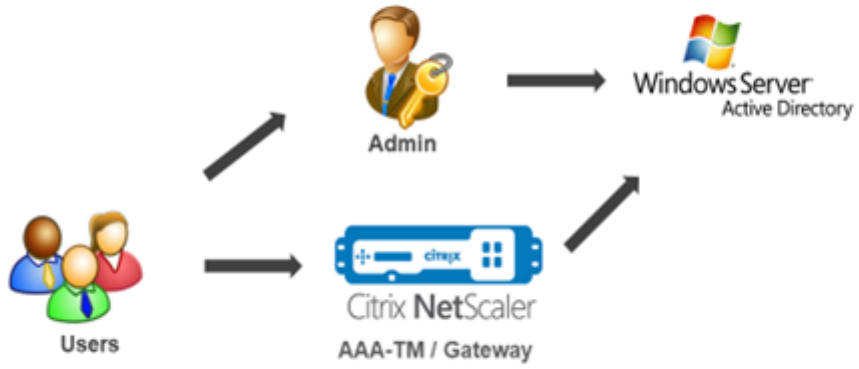
- Der Benutzer hat das Kennwort vergessen.
- Der Benutzer kann sich nicht anmelden.

Wenn ein Endbenutzer ein AD-Kennwort vergisst, musste sich der Endbenutzer an den AD-Administrator wenden, um das Kennwort zurückzusetzen. Mit der Self-Service-Funktion zum Zurücksetzen des Kennworts kann ein Endbenutzer das Kennwort ohne Eingreifen eines Administrators zurücksetzen.

Im Folgenden sind einige der Vorteile der Verwendung des Self-Service-Kennwort-Resets aufgeführt:

- Erhöhte Produktivität durch den automatischen Mechanismus zur Kennwortänderung, wodurch die Vorlaufzeit für Benutzer zum Zurücksetzen des Kennworts entfällt.
- Mit dem automatischen Kennwortänderungsmechanismus können sich Administratoren auf andere wichtige Aufgaben konzentrieren.

Die folgende Abbildung zeigt den Ablauf des Self-Service-Kennwortrücksetzens zum Zurücksetzen des Kennworts



Um das Self-Service-Kennwortrücksetzen verwenden zu können, muss ein Benutzer entweder bei der Citrix Authentifizierung, Autorisierung und Überwachung oder beim virtuellen Citrix Gateway-Server registriert sein.

Das Self-Service-Kennwort-Reset bietet folgende Funktionen:

- **Selbstregistrierung neuer Benutzer.** Sie können sich selbst als neuer Benutzer registrieren.
- **Konfigurieren Sie wissensbasierte Fragen.** Als Administrator können Sie eine Reihe von Fragen für Benutzer konfigurieren.
- **Alternative E-Mail-ID-Registrierung.** Sie müssen bei der Registrierung eine alternative E-Mail-ID angeben. Das OTP wird an die alternative E-Mail-ID gesendet, da der Benutzer das primäre E-Mail-ID-Kennwort vergessen hat.

  > **Hinweis:**
  >
  > Ab Version 12.1 Build 51.xx kann eine alternative E-Mail-ID-Registrierung als eigenständige Registrierung durchgeführt werden. Ein neues Anmeldeschema, **AltEmailRegister.xml**, wurde eingeführt, um nur eine alternative E-Mail-ID-Registrierung durchzuführen. Bisher

> konnte eine alternative E-Mail-ID-Registrierung nur während der KBA-Registrierung durchgeführt werden.

- **Kennwort vergessen zurücksetzen.** Der Benutzer kann das Kennwort zurücksetzen, indem er die wissensbasierten Fragen beantwortet. Als Administrator können Sie die Fragen konfigurieren und speichern.

Das Self-Service-Kennwort-Reset bietet die folgenden zwei neuen Authentifizierungsmechanismen:

- **Wissensbasierte Frage und Antwort.** Sie müssen sich bei der Authentifizierung, Autorisierung und Überwachung von Citrix oder bei einem Citrix Gateway registrieren, bevor Sie das wissensbasierte Frage- und Antwortschema auswählen.
- **E-Mail-OTP-Authentifizierung.** Ein OTP wird an die alternative E-Mail-ID gesendet, die der Benutzer bei der Self-Service-Registrierung zum Zurücksetzen des Kennworts registriert hat.

> **Hinweis**
>
> Diese Authentifizierungsmechanismen können für die Self-Service-Anwendungsfälle zum Zurücksetzen des Kennworts und für beliebige Authentifizierungszwecke verwendet werden, die einem der vorhandenen Authentifizierungsmechanismen ähneln.

Voraussetzungen

Bevor Sie das Self-Service-Zurücksetzen des Kennworts konfigurieren, sollten Sie die folgenden Voraussetzungen prüfen:

- Citrix ADC Feature Release 12.1, Build 50.28.
- Die unterstützte Version ist die AD-Domänenfunktionsebene 2016, 2012 und 2008.
- Der an den Citrix ADC gebundene ldapBind-Benutzername muss Schreibzugriff auf den AD-Pfad des Benutzers haben.

  > **Hinweis**
  >
  > Self-Service-Kennwortrücksetzung wird nur im nFactor-Authentifizierungsfluss unterstützt. Weitere Informationen finden Sie unter nFactor-Authentifizierung über Citrix ADC.

Einschränkungen

Im Folgenden sind einige Einschränkungen beim Zurücksetzen des Self-Service-Kennworts aufgeführt:

- Self-Service-Kennwortrücksetzung wird auf LDAPS unterstützt. Self-Service-Kennwortrücksetzung ist nur verfügbar, wenn das Authentifizierungs-Backend LDAP (LDAP-Protokoll) ist.

- Der Benutzer kann die bereits registrierte alternative E-Mail-ID nicht sehen.
- Wissensbasierte Fragen und Antworten sowie die E-Mail-OTP-Authentifizierung und -Registrierung können nicht der erste Faktor im Authentifizierungsablauf sein.
- Für Native Plug-in und Receiver wird die Registrierung nur über den Browser unterstützt.
- Die Mindestzertifikatgröße, die für das Zurücksetzen von Self-Service-Kennwörtern verwendet wird, beträgt 1024 Byte und muss dem x.509-Standard entsprechen.
- Nur ein RSA-Zertifikat wird für das Self-Service-Kennwortrücksetzen unterstützt.

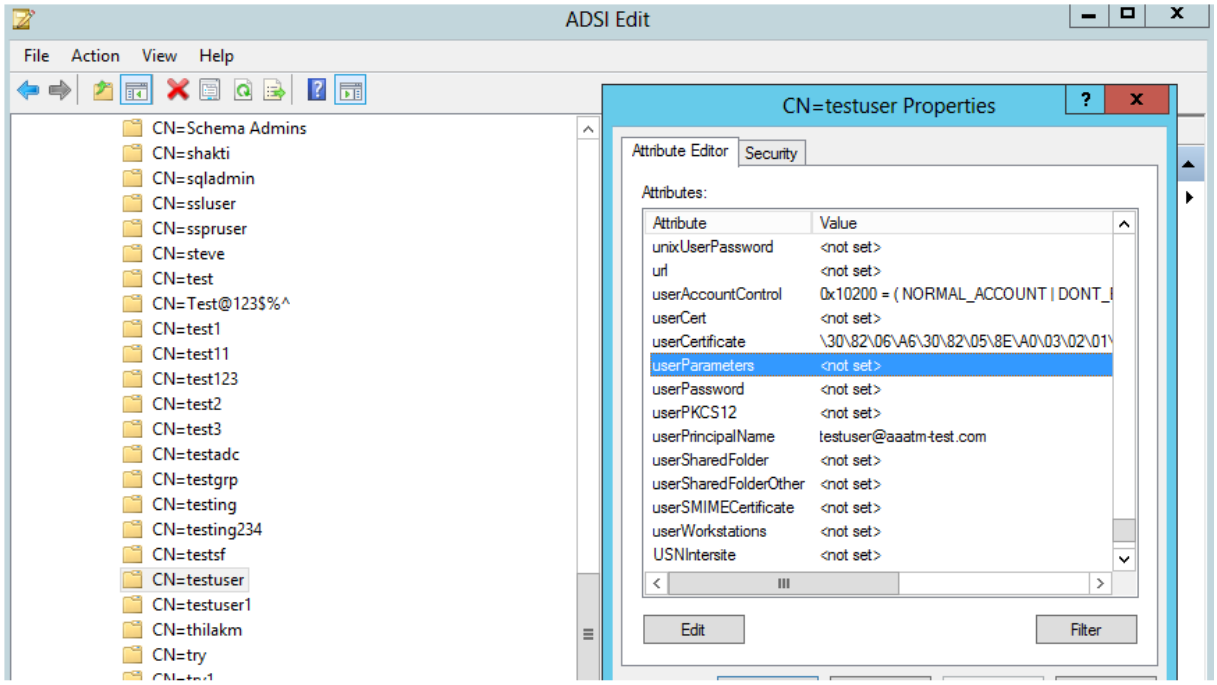
Active Directory-Einstellung

Die wissensbasierte Frage und Antwort von Citrix ADC sowie das E-Mail-OTP verwenden ein AD-Attribut zum Speichern von Benutzerdaten. Sie müssen ein AD-Attribut konfigurieren, um die Fragen und Antworten zusammen mit der alternativen E-Mail-ID zu speichern. Die Citrix ADC-Appliance speichert es im konfigurierten KB-Attribut im AD-Benutzerobjekt. Beachten Sie beim Konfigurieren eines AD-Attributs Folgendes:

- Die Attributlänge muss mindestens 128 Zeichen lang sein.
- Das AD-Attribut muss eine maximale Länge von 32k unterstützen.
- Der Attributtyp muss ein 'DirectoryString' sein.
- Ein einzelnes AD-Attribut kann für wissensbasierte Fragen und Antworten sowie eine alternative E-Mail-ID verwendet werden.
- Ein einzelnes AD-Attribut kann nicht für Native OTP und wissensbasierte Fragen und Antworten oder alternative E-Mail-ID-Registrierung verwendet werden.
- Der Citrix ADC LDAP-Administrator muss Schreibzugriff auf das ausgewählte AD-Attribut haben.

Sie können auch ein vorhandenes AD-Attribut verwenden. Stellen Sie jedoch sicher, dass das Attribut, das Sie verwenden möchten, nicht für andere Fälle verwendet wird. UserParameters ist beispielsweise ein vorhandenes Attribut innerhalb des AD-Benutzers, das Sie verwenden können. Um dieses Attribut zu überprüfen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **ADSI > Benutzer auswählen**.
2. Rechtsklicken Sie und scrollen Sie nach unten zur Attributliste.
3. Im Fensterbereich **cn=TestUser Properties** können Sie sehen, dass das **UserParameters-Attribut** nicht festgelegt ist.



Self-Service-Kennwort-Reset-

Um die Self-Service-Lösung zum Zurücksetzen des Kennworts auf einer Citrix ADC-Appliance zu implementieren, müssen Sie Folgendes ausführen:

- Self-Service-Kennwortrücksetzung (wissensbasierte Frage und Antwort/E-Mail-ID).
- Benutzeranmeldeseite (zum Zurücksetzen des Kennworts, einschließlich wissensbasierter Frage und Antwort sowie OTP-Validierung per E-Mail und endgültigem Kennwortrücksetzfaktor).

Ein Satz vordefinierter Fragenkatalog wird als JSON-Datei bereitgestellt. Als Administrator können Sie die Fragen auswählen und das Anmeldeschema zum Zurücksetzen des Self-Service-Kennwortrücksetzens über die Citrix ADC GUI erstellen. Sie können eine der folgenden Optionen wählen:

- Wählen Sie maximal vier systemdefinierte Fragen aus.
- Bieten Sie Benutzern die Möglichkeit, zwei Fragen und Antworten anzupassen.

So zeigen Sie die standardmäßige JSON-Datei für wissensbasierte Fragen von CLI an

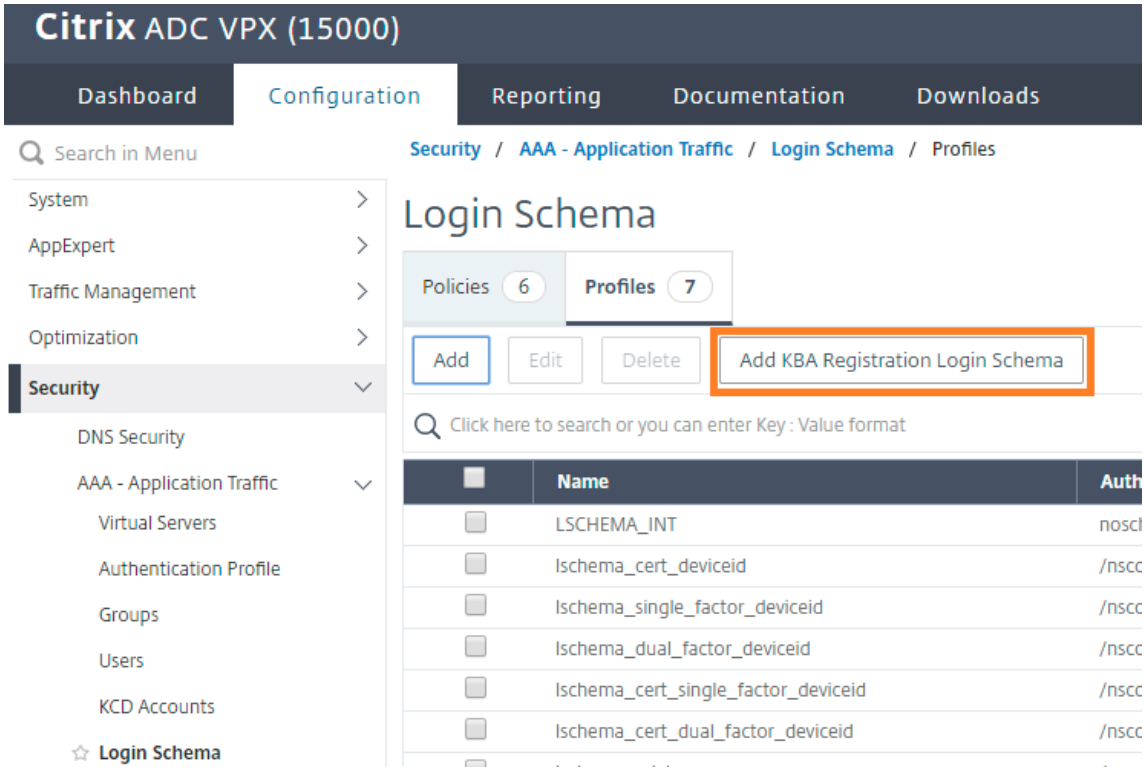
```
root@ns# cd /nsconfig/loginschema/LoginSchema/
root@ns# cat KBQuestions.json
[
    {"question":"What is the last name of the teacher who gave you your first failing
grade?"},
    {"question":"What is the name of your favourite childhood friend?"},
    {"question":"Where were you when you first heard about 9/11?"},
    {"question":"What is the name of a college you applied to but didn't attend?"},
    {"question":"What was the last name of your third grade teacher?"},
    {"question":"What was the name of your first stuffed animal?"},
    {"question":"What is the name of the teacher who gave you your first A?"},
    {"question":"What is the name of the city where you got lost?"},
    {"question":"In what city or town did your mother and father meet?"},
    {"question":"What was your most hated food as a child?"},
    {"question":"What was your most favourite food as a child?"},
    {"question":"What is your favourite website?"},
    {"question":"What is your most disliked website?"},
    {"question":"What is your dream job?"},
    {"question":"Why did the chicken cross the road?"},
    {"question":"Name your first boss."},
    {"question":"What is the name of your favorite school teacher?"},
    {"question":"What is the name of your favorite actor or actress?"},
    {"question":"What is the title of your favorite movie?"},
    {"question":"In what city or town did you spend most of your youth?"}
]
```

Hinweis

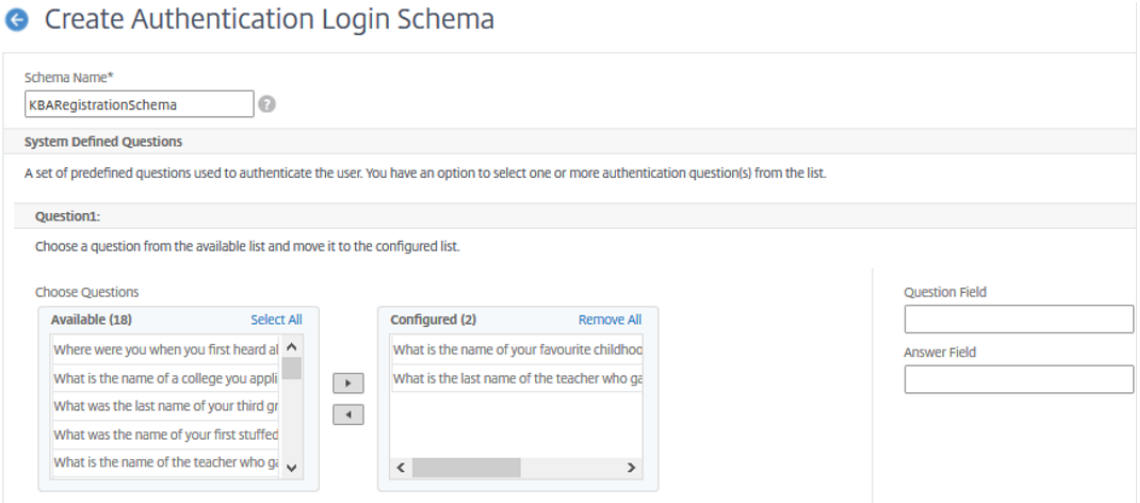
- Citrix Gateway enthält standardmäßig den Satz systemdefinierter Fragen. Der Administrator kann die Datei “KbQuestions.json” bearbeiten, um die gewünschten Fragen aufzunehmen.
- Systemdefinierte Fragen werden nur auf Englisch angezeigt, und für diese Fragen ist keine Sprachlokalisierung verfügbar.

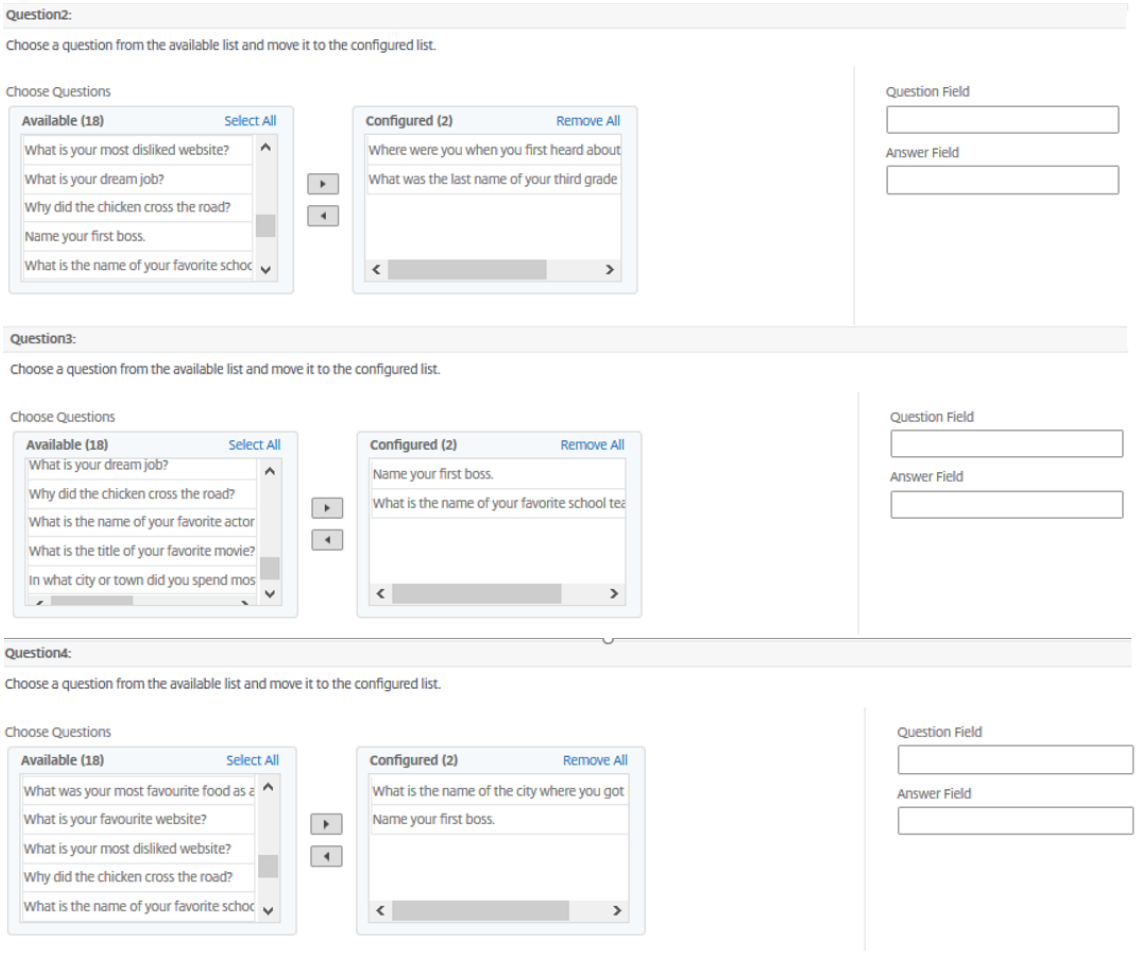
Um das wissensbasierte Frage-und-Antwort-Registrierungsschema über die GUI abzuschließen

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Anmeldeschema**.

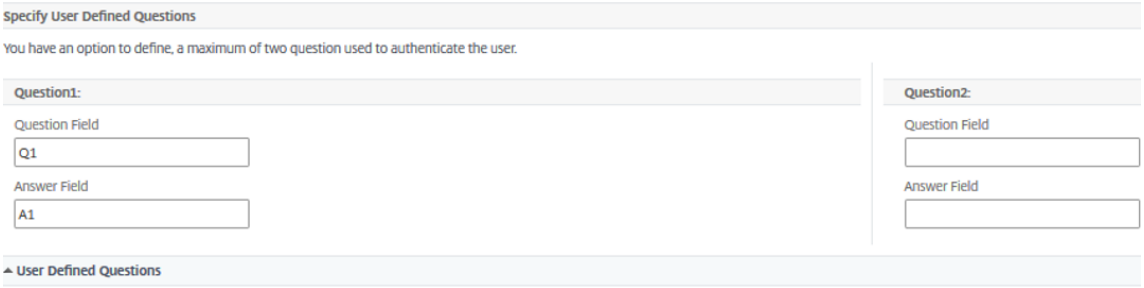


2. Klicken Sie auf der Seite **Anmeldeschema** auf **Profile**.
3. Klicken Sie auf **Anmeldeschema für die KBA-Registrierung hinzufügen**.
4. Geben Sie auf der Seite **Anmeldeschema für die Authentifizierung erstellen** einen Namen in das Feld **Schemaname** ein.

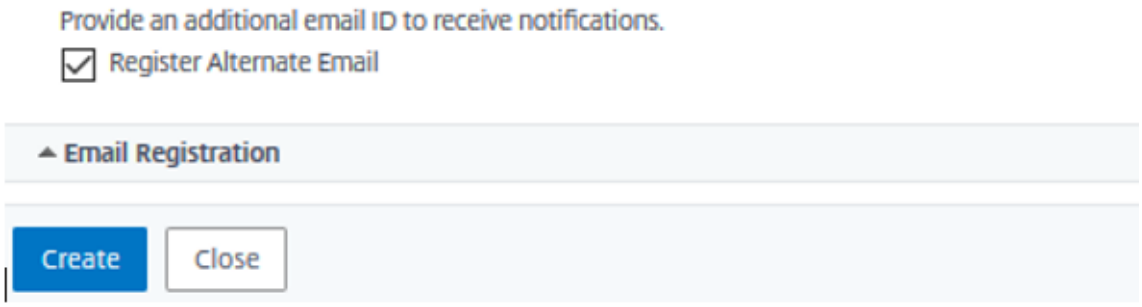




5. Wählen Sie die Fragen Ihrer Wahl aus und verschieben Sie sie in die Liste **Konfiguriert** .
6. Im Abschnitt **Benutzerdefinierte Fragen** können Sie Fragen und Antworten in den Feldern Q1 und A1 angeben.



7. Aktivieren Sie im Abschnitt **E-Mail-Registrierung** die Option **Alternative E-Mail registrieren** . Sie können die **alternative E-Mail-ID** auf der Anmeldeseite der Benutzerregistrierung registrieren, um das OTP zu erhalten.



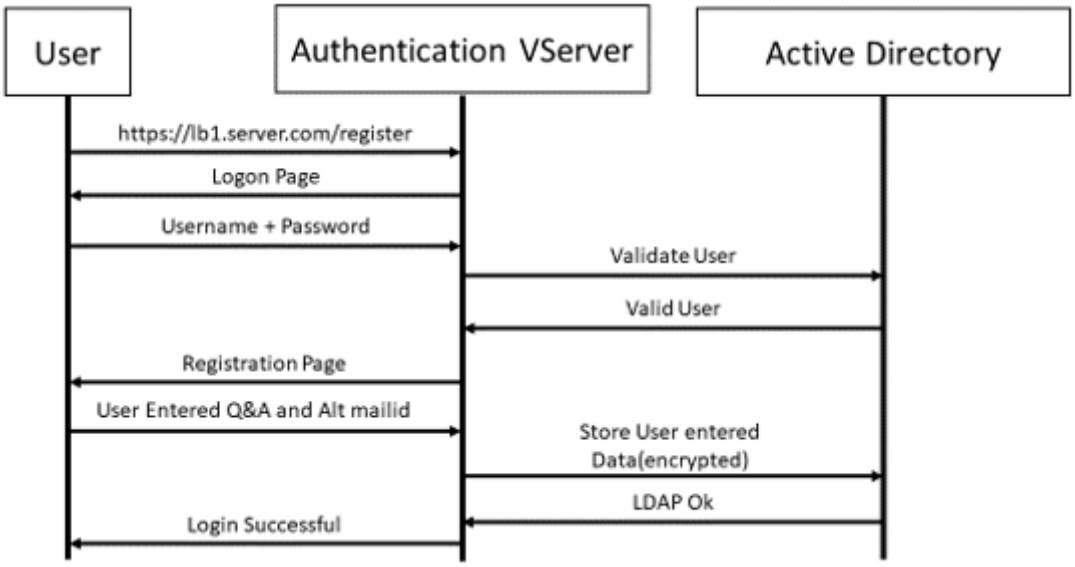
8. Klicken Sie auf **Erstellen**. Das einmal generierte Anmeldeschema zeigt dem Endbenutzer während des Registrierungsvorgangs alle konfigurierten Fragen an.

Workflow für die Benutzerregistrierung und -verwaltung über die CLI erstellen

Folgendes ist erforderlich, bevor Sie mit der Konfiguration beginnen:

- Dem virtuellen Authentifizierungsserver zugewiesene IP-Adresse
- FQDN entspricht der zugewiesenen IP-Adresse
- Serverzertifikat für Authentifizierung virtueller Server

Um die Geräteregistrierungs- und Verwaltungsseite einzurichten, benötigen Sie einen virtuellen Authentifizierungsserver. Die folgende Abbildung veranschaulicht die Benutzerregistrierung.



So erstellen Sie einen virtuellen Authentifizierungsserver

1. Konfigurieren Sie einen virtuellen Authentifizierungsserver. Es muss vom Typ SSL sein und stellen Sie sicher, dass Authentifizierungsserver mit Portalthema zu binden.


```
> add authentication vserver <vServerName> SSL <ipaddress> <port>
> bind authentication vserver <vServerName> [-portaltheme<string>]
```

2. Binden Sie SSL Virtual Server Certificate-Key-Paar.

```
> bind ssl vserver <vServerName> certkeyName <string>
```

Beispiel:

```
> add authentication vserver authvs SSL 1.2.3.4 443
> bind authentication vserver authvs -portaltheme RFWebUI
> bind ssl vserver authvs -certkeyname c1
```

So erstellen Sie eine LDAP-Anmeldeaktion

```
    > add authentication ldapAction <name> {
-serverIP <ipaddr|ipv6_addr|> [-serverPort <port>] [-ldapBase <BASE> ]
     [-ldapBindDn <AD USER>] [-ldapBindDnPassword <PASSWORD>] [-
    ldapLoginName <USER FORMAT>]
```

> **Hinweis**
>
> Sie können jede Authentifizierungsrichtlinie als ersten Faktor konfigurieren.

Beispiel:

```
    > add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4
        -serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -
       ldapBindDn administrator@ctxnsdev.com -ldapBindDnPassword
       PASSWORD -ldapLoginName samAccountName -serverport 636 -sectype
       SSL -KBAttribute userParameters
```

So erstellen Sie eine Authentifizierungsrichtlinie für die LDAP-Anmeldung

```
    > add authentication policy <name> <rule> [<reqAction]
```


Beispiel:

```
1      > add authentication policy ldap_logon -rule true -action
          ldap_logon_action
```

So erstellen Sie eine wissensbasierte Frage- und Antwortregistrierungsaktion

Zwei neue Parameter werden in `ldapAction` eingeführt. `KBAttribute` für die KBA-Authentifizierung (Registrierung und Validierung) und `alternateEmailAttr` für die Registrierung der alternativen E-Mail-ID des Benutzers.

```
1      > add authentication ldapAction <name> {
2   -serverIP  <ipaddr|ipv6_addr|> [-serverPort <port>] [-ldapBase <BASE>
       ] [-ldapBindDn <AD USER>] [-ldapBindDnPassword <PASSWORD>] [-
       ldapLoginName <USER FORMAT>] [-KBAttribute <LDAP ATTRIBUTE>] [-
       alternateEmailAttr <LDAP ATTRIBUTE>]
```

Beispiel:

```
1      > add authentication ldapAction ldap1 -serverIP 1.2.3.4 -sectype
          ssl -serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -
          ldapBindDn administrator@ctxnsdev.com -ldapBindDnPassword
          PASSWORD -ldapLoginName samAccountName -KBAttribute
          userParameters -alternateEmailAttr userParameters
```

Anzeige der Benutzerregistrierung und -verwaltung

Das Anmeldeschema "KBARegistrationSchema.xml" wird verwendet, um dem Endbenutzer die Benutzerregistrierungsseite anzuzeigen. Verwenden Sie die folgende Befehlszeilenschnittstelle, um das Anmeldeschema anzuzeigen.

```
1  > add authentication loginSchema <name> -authenticationSchema <string>
```

Beispiel:


```
> add authentication loginSchema kba_register -authenticationSchema /
    nsconfig/loginschema/LoginSchema/KBARegistrationSchema.xml
```

Citrix empfiehlt zwei Möglichkeiten zur Anzeige der Benutzerregistrierung und -verwaltung: URL oder LDAP-Attribut.

Verwenden von URL

Wenn der URL-Pfad "/register" enthält (z. B. https://lb1.server.com/register), wird die Benutzerregistrierungsseite unter Verwendung der URL angezeigt.

So erstellen und binden Sie Registrierungsrichtlinien

```
> add authentication policylabel user_registration -loginSchema
    kba_register
> add authentication policy ldap1 -rule true -action ldap1
> bind authentication policylabel user_registration -policy ldap1 -
    priority 1
```

So binden Sie die Authentifizierungsrichtlinie an Authentifizierungs-, Autorisierungs- und Überwachungsserver, wenn die URL '/register' enthält

```
> add authentication policy ldap_logon -rule "http.req.cookie.value(\"
    NSC_TASS\").contains(\"register\")" -action ldap_logon
> bind authentication vserver authvs -policy ldap_logon -nextfactor
    user_registration -priority 1
```

So binden Sie Zertifikat an VPN global

```
bind vpn global -userDataEncryptionKey c1
```

> **Hinweis**
>
> - Sie müssen das Zertifikat binden, um die Benutzerdaten (KB Q&A und registrierte alternative E-Mail-ID) zu verschlüsseln, die im AD-Attribut gespeichert sind.

- Wenn das Zertifikat abläuft, müssen Sie ein neues Zertifikat binden und die Registrierung erneut durchführen.

Verwenden des Attributs

Sie können eine Authentifizierungsrichtlinie an den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver binden, um zu überprüfen, ob der Benutzer bereits registriert ist oder nicht. In diesem Ablauf muss jede der vorhergehenden Richtlinien vor dem wissensbasierten Frage- und Antwortregistrierungsfaktor LDAP mit dem konfigurierten KBA-Attribut sein. Hiermit wird überprüft, ob der AD-Benutzer registriert ist oder nicht ein AD-Attribut verwendet.

Wichtig

Die Regel “AAA.USER.ATTRIBUTE (“kba_registered”) .EQ (“0”)” zwingt neue Benutzer, sich für wissensbasierte Fragen zu registrieren und alternative E-Mails zu beantworten.

So erstellen Sie eine Authentifizierungsrichtlinie, um zu überprüfen, ob der Benutzer noch nicht registriert ist

```
1 > add authentication policy switch_to_kba_register -rule ”AAA.USER.
    ATTRIBUTE(\”kba_registered\”).EQ(\”0\”)” -action NO_AUTHN
2 > add authentication policy first_time_login_forced_kba_registration -
    rule true -action ldap1
```

So erstellen Sie ein Registrierungsrichtlinienlabel und binden es an die LDAP-Registrierungsrichtlinie

```
1 > add authentication policylabel auth_or_switch_register -loginSchema
    LSCHEMA_INT
2 > add authentication policylabel kba_registration -loginSchema
    kba_register
3
4 > bind authentication policylabel auth_or_switch_register -policy
    switch_to_kba_register -priority 1 -nextFactor kba_registration
5 > bind authentication policylabel kba_registration -policy
    first_time_login_forced_kba_registration -priority 1
```

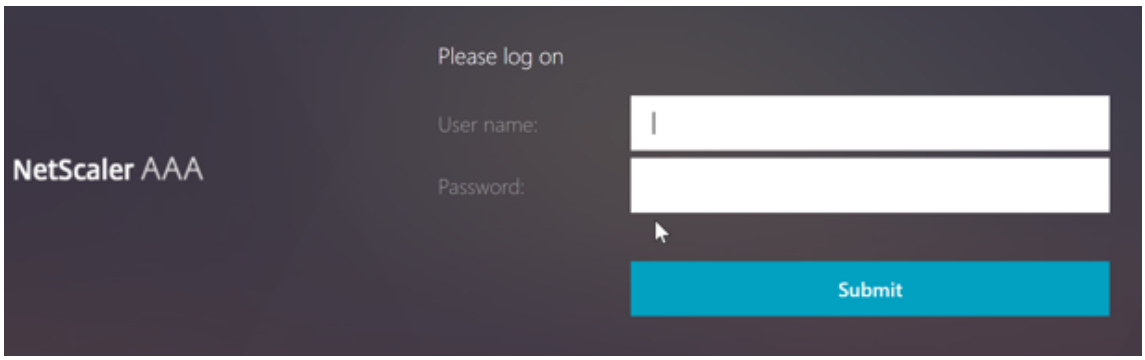

So binden Sie die Authentifizierungsrichtlinie an Authentifizierungs-, Autorisierungs- und Überwachungsserver des virtuellen Servers

```
bind authentication vserver authvs -policy ldap_logon -nextfactor
    auth_or_switch_register -priority 2
```

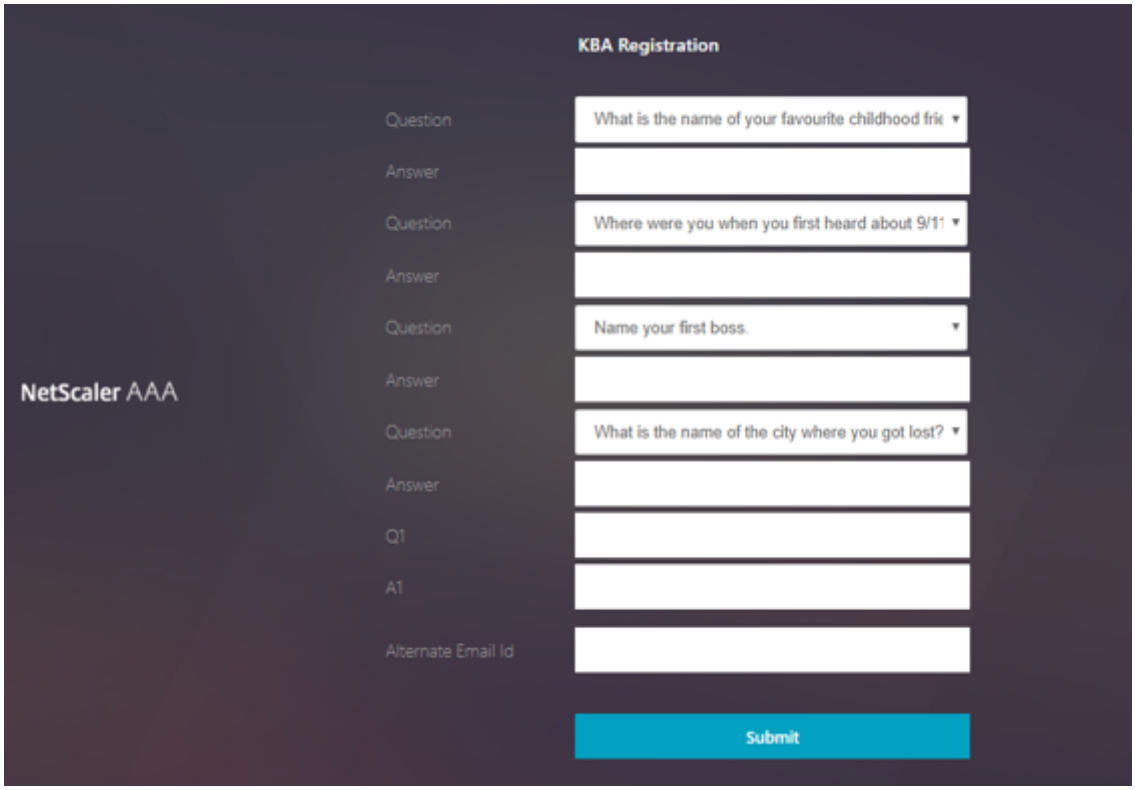
Benutzerregistrierung und Management-Validierung

Nachdem Sie alle in den vorherigen Abschnitten genannten Schritte konfiguriert haben, muss der folgende UI-Bildschirm angezeigt werden.

1. Geben Sie die URL des virtuellen Servers lb ein, https://lb1.server.comz. B. Der Anmeldebildschirm wird angezeigt.



2. Geben Sie den Benutzernamen und das Kennwort ein. Klicken Sie auf **Submit**. Der Bildschirm **Benutzerregistrierung** wird angezeigt.



3. Wählen Sie die bevorzugte Frage aus der Dropdown-Liste aus und geben Sie die **Antwort**ein.
4. Klicken Sie auf **Submit**. Der Bildschirm mit der erfolgreichen Benutzerregistrierung wird angezeigt.

Benutzeranmeldeseite konfigurieren

In diesem Beispiel geht der Administrator davon aus, dass der erste Faktor die LDAP-Anmeldung ist (für die der Endbenutzer das Kennwort vergessen hat). Der Benutzer folgt dann der wissensbasierten Frage- und Antwortregistrierung und der OTP-Validierung der E-Mail-ID und setzt das Kennwort schließlich mithilfe des Self-Service-Kennwortrücksetzens zurück.

Sie können jeden der Authentifizierungsmechanismen für das Zurücksetzen des Self-Service-Kennworts verwenden. Citrix empfiehlt, entweder eine wissensbasierte Frage und Antwort zu haben und OTP per E-Mail oder beides zu senden, um einen starken Datenschutz zu gewährleisten und unrechtmäßige Rücksetzungen von Benutzerkennwörtern zu vermeiden.

Folgendes ist erforderlich, bevor Sie mit der Konfiguration der Benutzeranmeldeseite beginnen:

- IP für virtuellen Load-Balancer-Server
- Entsprechender FQDN für den virtuellen Load Balancer-Server
- Serverzertifikat für den Load Balancer

Erstellen eines virtuellen Load Balancer-Servers über die CLI

Um auf die interne Website zuzugreifen, müssen Sie einen virtuellen LB-Server erstellen, um den Back-End-Dienst zu starten und die Authentifizierungslogik an den virtuellen Authentifizierungsserver zu delegieren.

```
> add lb vserver lb1 SSL 1.2.3.162 443 -persistenceType NONE -
   cltTimeout 180 -AuthenticationHost otpauth.server.com -
   Authentication ON -authnVsName authvs

> bind ssl vserver lb1 -certkeyname c1
```

So stellen Sie den Back-End-Dienst beim Lastenausgleich dar:

```
> add service iis_backendsso_server_com 1.2.3.4 HTTP 80

> bind lb vserver lb1 iis_backendsso_server_com
```

LDAP-Aktion mit deaktivierter Authentifizierung als erste Richtlinie erstellen

```
> add authentication ldapAction ldap3 -serverIP 1.2.3.4 -serverPort 636
    -ldapBase ”OU=Users,DC=server,DC=com” -ldapBindDn
   administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
   ldapLoginName samAccountName -authentication disabled

> add authentication policy ldap3 -rule aaa.LOGIN.VALUE(”passwdreset”).
   EQ(”1”) -action ldap3
```

Erstellen einer wissensbasierten Frage- und Antwortvalidierungsaktion

Für die wissensbasierte Frage- und Antwortvalidierung im Self-Service-Ablauf zum Zurücksetzen des Kennworts müssen Sie den LDAP-Server mit deaktivierter Authentifizierung konfigurieren.

```
> add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP
   > -serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -
   ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT> -
   KBAttribute  <LDAP ATTRIBUTE> - alternateEmailAttr <LDAP ATTRIBUTE>
   -authentication DISABLED
```


Beispiel:

```
> add authentication ldapAction ldap2 -serverIP 1.2.3.4 -serverPort 636
    -ldapBase ”OU=Users,DC=server,DC=com” -ldapBindDn
   administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -
   ldapLoginName samAccountName -KBAttribute userParameters -
   alternateEmailAttr userParameters -authentication disabled
```

So erstellen Sie eine Authentifizierungsrichtlinie für die wissensbasierte Frage- und Antwortvalidierung mit CLI

```
add authentication policy kba_validation -rule true -action ldap2
```

Erstellen einer E-Mail-Validierungsaktion

LDAP muss ein wichtiger Faktor für den E-Mail-Validierungsfaktor sein, da Sie die E-Mail-ID oder die alternative E-Mail-ID des Benutzers als Teil der Registrierung zum Zurücksetzen des Kennworts im Self-Service benötigen.

> **Hinweis:**
>
> Damit die E-Mail-OTP-Lösung funktioniert, stellen Sie sicher, dass die anmeldungsbasierte Authentifizierung auf dem SMTP-Server aktiviert ist.

Um sicherzustellen, dass die anmeldungsbasierte Authentifizierung aktiviert ist, geben Sie den folgenden Befehl auf dem SMTP-Server ein. Wenn die Login-basierte Authentifizierung aktiviert ist, stellen Sie fest, dass der Text **AUTH LOGIN** in der Ausgabe fett gedruckt erscheint.

```
root@ns# telnet <IP address of the SMTP server><Port number of the
   server>
ehlo
```

Beispiel:

```
root@ns# telnet 10.106.3.66 25
Trying 10.106.3.66...
Connected to 10.106.3.66.
Escape character is '^]'.
```



```
220 E2K13.NSGSanity.com Microsoft ESMTP MAIL Service ready at Fri, 22
    Nov 2019 16:24:17 +0530
ehlo
250-E2K13.NSGSanity.com Hello [10.221.41.151]
250-SIZE 37748736
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-X-ANONYMOUSTLS
250-AUTH LOGIN
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 XRDST
```

Weitere Informationen zum Aktivieren der anmeldungsbasierten Authentifizierung finden Sie unter https://support.microfocus.com/kb/doc.php?id=7020367.

So konfigurieren Sie E-Mail-Aktion mit CLI

```
add authentication emailAction emailact -userName sender@example.com -
    password <Password> -serverURL "smtps://smtp.example.com:25" -
    content "OTP is $code"
```

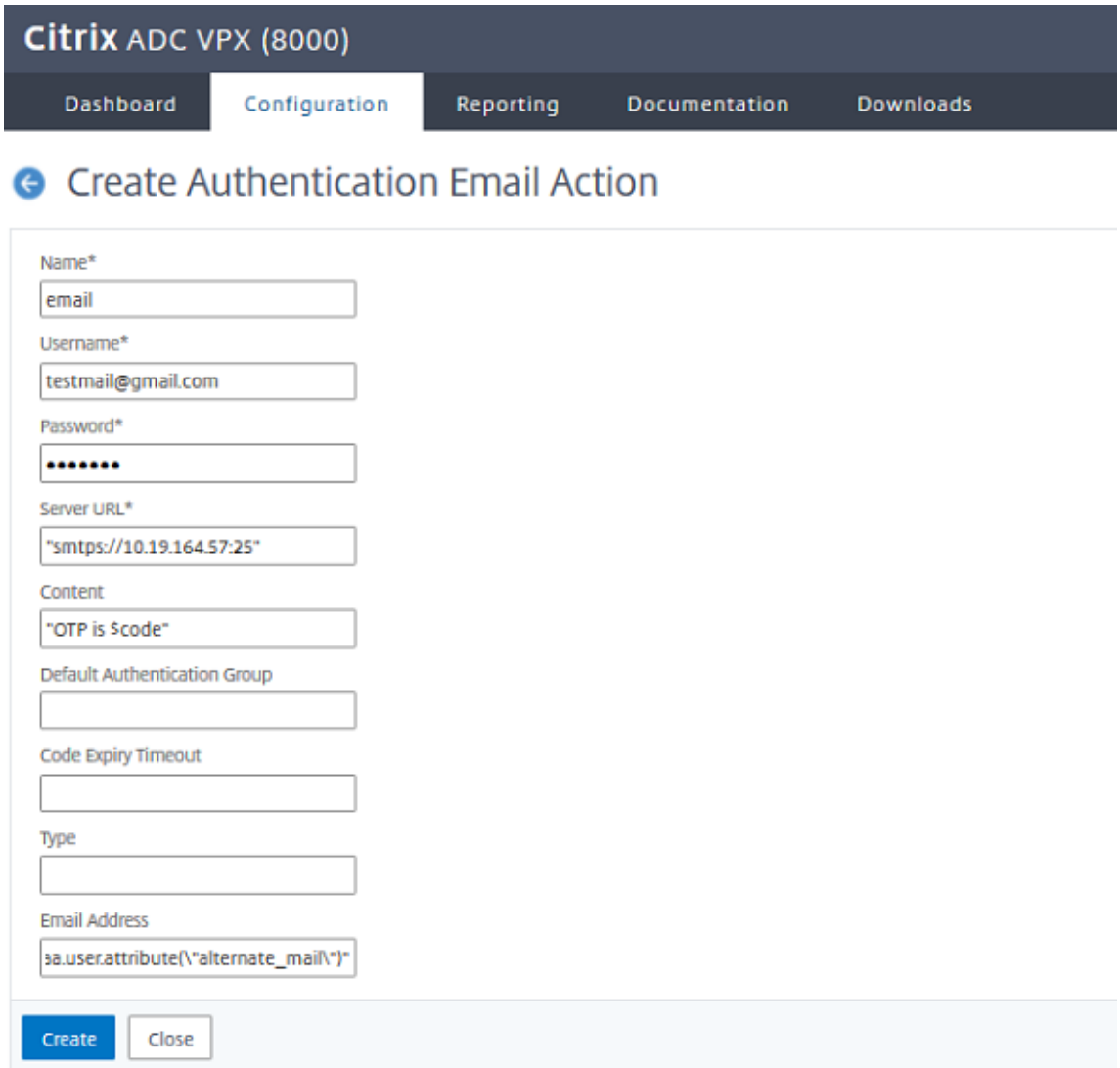
Beispiel:

```
add authentication emailAction email -userName testmail@gmail.com -
    password 298
    a34b1a1b7626cd5902bbb416d04076e5ac4f357532e949db94c0534832670 -
    encrypted -encryptmethod ENCMTHD_3 -serverURL "smtps
    ://10.19.164.57:25" -content "OTP is $code" -emailAddress "aaa.user.
    attribute(\"alternate_mail\")"
```

> **Hinweis**
>
> Der Parameter "EmailAddress" in der Konfiguration ist ein PI-Ausdruck. Daher ist dies so konfiguriert, dass entweder die standardmäßige Benutzer-E-Mail-ID aus der Sitzung oder die bereits registrierte alternative E-Mail-ID übernommen wird.

Konfigurieren der E-Mail-ID über die GUI

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Aktionen > E-Mail-Aktion für Authentifizierung**. Klicken Sie auf **Hinzufügen**.
2. Füllen Sie auf der Seite **Authentifizierungs-E-Mail-Aktion erstellen** die Details aus und klicken Sie auf **Erstellen**.



So erstellen Sie über die CLI eine Authentifizierungsrichtlinie für die E-Mail-Validierung

```
1 add authentication policy email_validation -rule true -action email
```

Erstellen einer Authentifizierungsrichtlinie für den Kennwortrücksetzfaktor


```
add authentication policy ldap_pwd -rule true -action ldap_logon_action
```

Präsentieren der Benutzeroberfläche über das Anmeldeschema

Es gibt drei LoginSchemas zum Zurücksetzen des Kennworts im Self-Service, um das Kennwort zurückzusetzen. Verwenden Sie die folgenden CLI-Befehle, um die drei Login-Schema anzuzeigen:

```
root@ns# cd  /nsconfig/loginschema/LoginSchema/
root@ns# ls -ltr | grep -i password
-r--r--r--  1 nobody  wheel  2088 Nov 13 08:38
   SingleAuthPasswordResetRem.xml
-r--r--r--  1 nobody  wheel  1541 Nov 13 08:38
   OnlyUsernamePasswordReset.xml
-r--r--r--  1 nobody  wheel  1391 Nov 13 08:38 OnlyPassword.xml
```

So erstellen Sie das Zurücksetzen einzelner Authentifizierungskennworte mit der CLI

```
> add authentication loginSchema lschema_password_reset -
   authenticationSchema ”/nsconfig/loginschema/LoginSchema/
   SingleAuthPasswordResetRem.xml”

> add authentication loginSchemaPolicy lpol_password_reset -rule true -
   action lschema_password_reset
```

Erstellen eines wissensbasierten Frage-, Antwort- und E-Mail-OTP-Validierungsfaktors über Richtlinienlabel

Wenn der erste Faktor die LDAP-Anmeldung ist, können Sie mit der folgenden Befehle eine wissensbasierte Frage erstellen und OTP-Richtlinienbeschriftungen für den nächsten Faktor senden.

```
> add authentication loginSchema lschema_noschema -authenticationSchema
    noschema

> add authentication policylabel kba_validation -loginSchema
   lschema_noschema

> add authentication policylabel email_validation -loginSchema
   lschema_noschema
```


Kennwortrücksetzungsfaktor über Richtlinienbezeichnung erstellen

Sie können den Kennwortrücksetzfaktor mithilfe der folgenden Befehle über die Policy Label erstellen.

```
> add authentication loginSchema lschema_noschema -authenticationSchema
    noschema

> add authentication policylabel password_reset -loginSchema
    lschema_noschema

> bind authentication policylabel password_reset -policyName ldap_pwd -
    priority 10 -gotoPriorityExpression NEXT
```

Binden Sie die wissensbasierte Frage-, Antwort- und E-Mail-Richtlinie mit den vorherigen erstellten Richtlinien mit den folgenden Befehlen.

```
> bind authentication policylabel email_validation -policyName
    email_validation -nextfactor password_reset -priority 10 -
    gotoPriorityExpression NEXT

> bind authentication policylabel kba_validation -policyName
    kba_validation -nextfactor email_validation -priority 10 -
    gotoPriorityExpression NEXT
```

Flow binden

Sie müssen den LDAP-Anmeldeablauf gemäß der Authentifizierungsrichtlinie für die LDAP-Anmeldung erstellt haben. In diesem Ablauf klickt der Benutzer auf den Link Kennwort vergessen, der auf der ersten LDAP-Anmeldeseite angezeigt wird, dann auf die KBA-Validierung, gefolgt von der OTP-Validierung und schließlich auf die Seite zum Zurücksetzen des Kennworts.

```
bind authentication vserver authvs -policy ldap3 -nextfactor
    kba_validation -priority 10 -gotoPriorityExpression NEXT
```

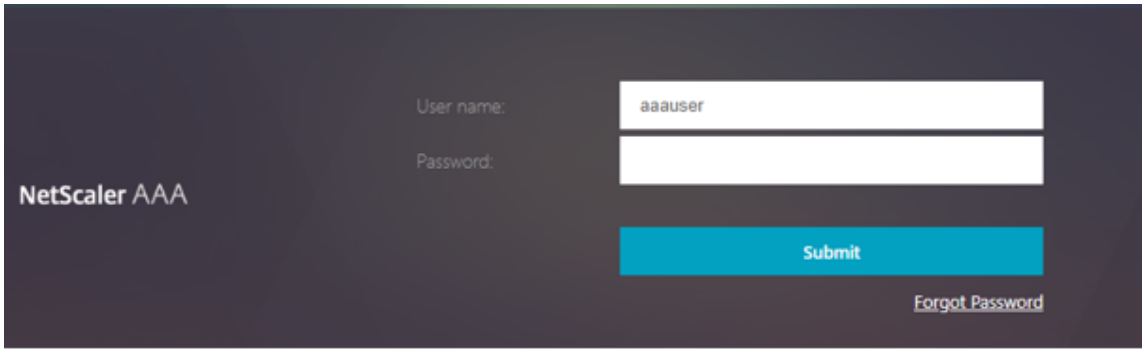
So binden Sie den gesamten UI-Flow


```
bind authentication vserver authvs -policy lpol_password_reset -
    priority 20 -gotoPriorityExpression END
```

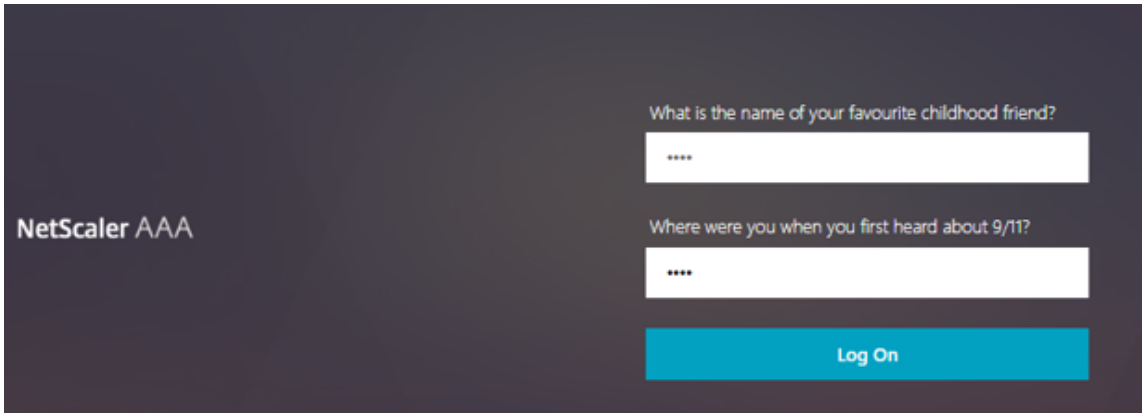
Workflow für Benutzeranmeldung zum Zurücksetzen des Kennworts

Es folgt ein Workflow für die Benutzeranmeldung, wenn der Benutzer das Kennwort zurücksetzen muss:

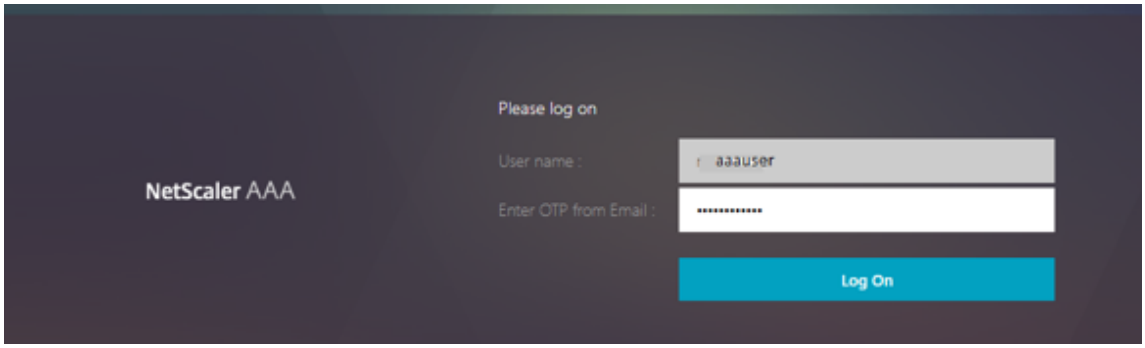
1. Geben Sie die URL des virtuellen Servers lb ein, https://lb1.server.comz. B. Der Anmeldebildschirm wird angezeigt.



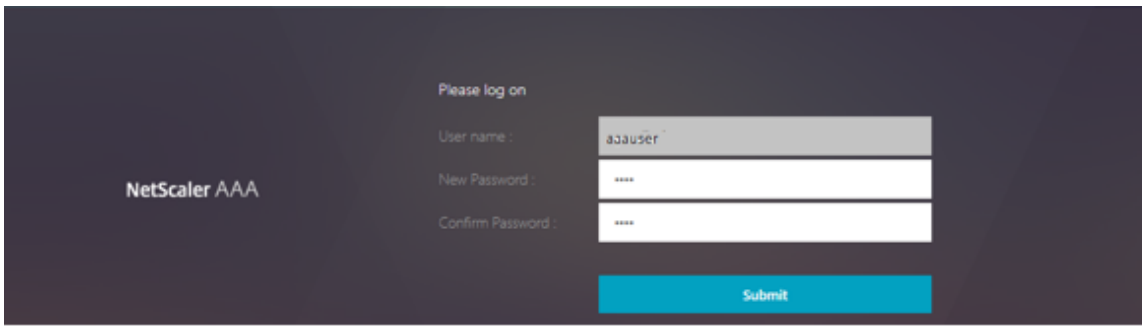
2. Klicken Sie auf **Kennwort vergessen**. Auf einem Validierungsbildschirm werden zwei Fragen von maximal sechs Fragen und Antworten angezeigt, die für einen AD-Benutzer registriert wurden.



3. Beantworten Sie die Fragen und klicken Sie **auf Anmelden**. Ein E-Mail-OTP-Validierungsbildschirm, in dem Sie das OTP eingeben müssen, das Sie mit der registrierten alternativen E-Mail-ID erhalten haben, wird angezeigt.



4. Geben Sie die E-Mail OTP ein. Sobald die E-Mail-OTP-Validierung erfolgreich war, wird die Seite zum Zurücksetzen des Kennworts angezeigt.



5. Gib ein neues Kennwort ein und bestätige das neue Kennwort. Klicken Sie auf **Submit**. Nachdem das Zurücksetzen des Kennworts erfolgreich war, wird der Bildschirm zum erfolgreichen Zurücksetzen des Kennworts angezeigt.

Sie können sich jetzt mit dem Kennwort zum Zurücksetzen anmelden.

Problembehandlung

Citrix bietet eine Option zur Behebung einiger grundlegender Probleme, die bei der Verwendung des Self-Service-Kennwortrücksetzens auftreten können. Der folgende Abschnitt hilft Ihnen bei der Behebung einiger Probleme, die in bestimmten Bereichen auftreten können.

NS-Protokoll

Vor der Analyse des Protokolls wird empfohlen, die Protokollstufe mit dem folgenden Befehl zu debuggen:

```
> set syslogparams -loglevel DEBUG
```

Registrierung

Die folgende Meldung weist auf eine erfolgreiche Benutzerregistrierung hin.

```
”ns_aaa_insert_hash_keyValue_entry key:kba_registered value:1”
Nov 14 23:35:51 <local0.debug> 10.102.229.76 11/14/2018:18:05:51 GMT
    0-PPE-1 : default SSLVPN Message 1588 0 :  ”
    ns_aaa_insert_hash_keyValue_entry key:alternate_mail value:
    eyJ2ZXJzaW9uIjoiMSIsICJraWQiOiIxbk1oWjN0T2NjLVVvZUx6NDRwZFhxdS01dTA9IiwgImtleS
    ==.oKmvOalaOJ3a9z7BcGCSegNPMw==”
```

Wissensbasierte Frage- und Antwortvalidierung

Die folgende Meldung zeigt eine erfolgreiche wissensbasierte Frage- und Antwortvalidierung an.

```
”NFactor: Successfully completed KBA Validation, nextfactor is email”
```

E-Mail-ID-Validierung

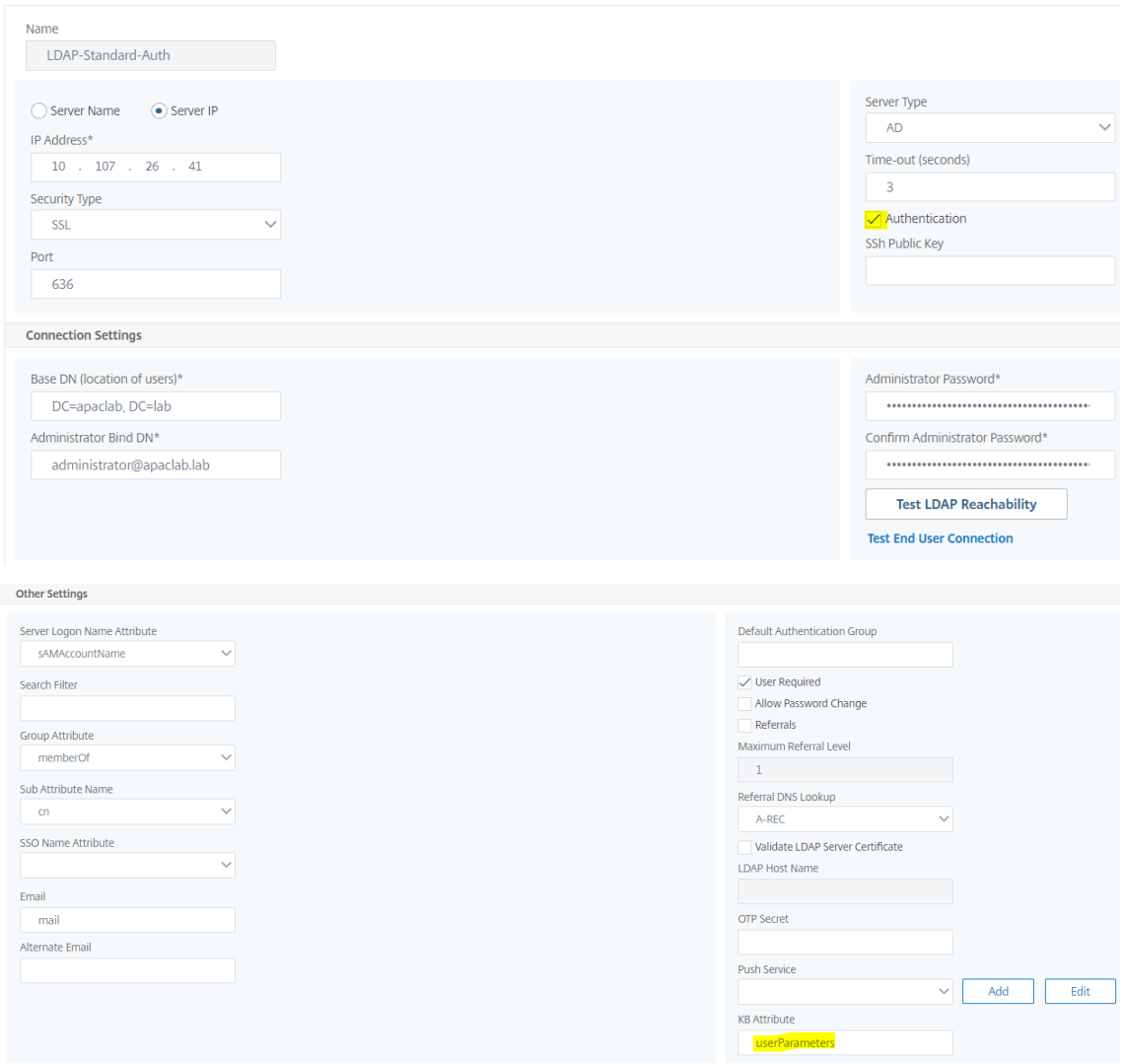
Die folgende Meldung zeigt an, dass das Kennwort erfolgreich zurückgesetzt wurde.

```
”NFactor: Successfully completed email auth, nextfactor is pwd_reset”
```

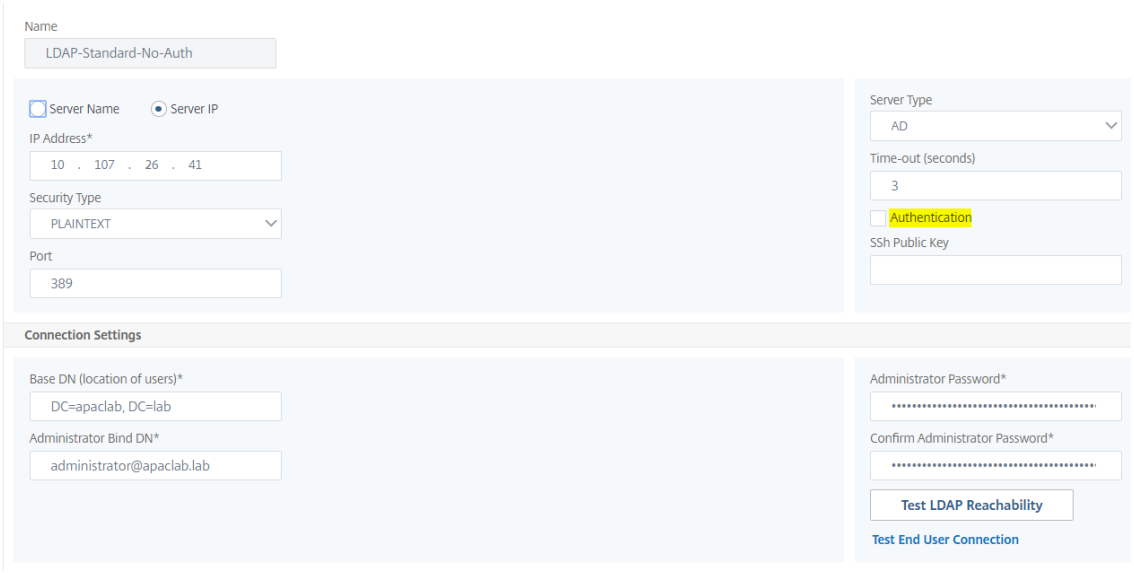
Konfigurieren von SSPR mit nFactor Visualizer

Bevor wir mit der SSPR-Konfiguration beginnen, müssen wir die folgenden LDAP-Server hinzufügen:

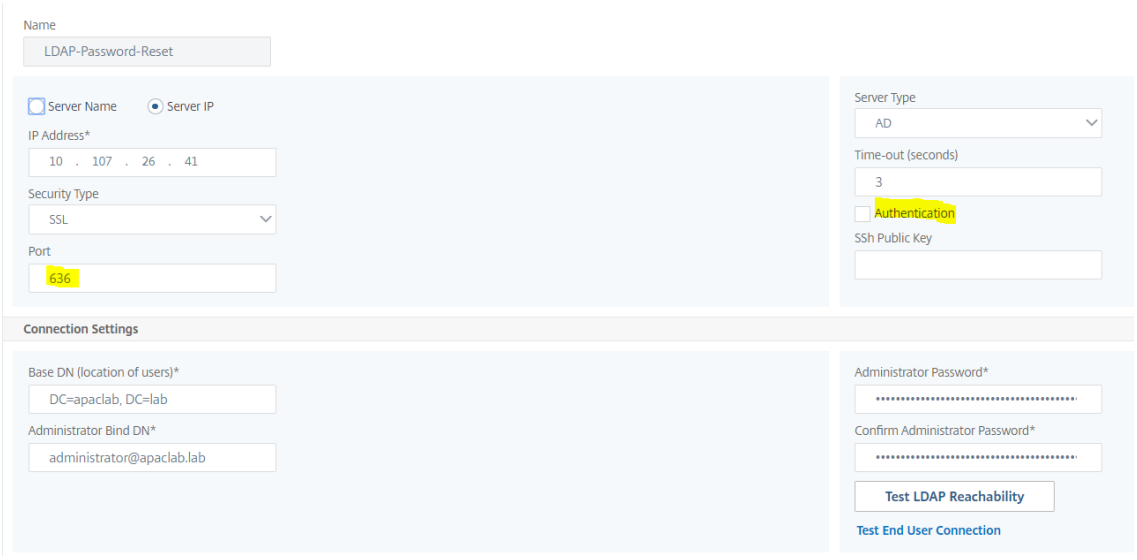
1. Standard-LDAP-Server mit aktivierter Authentifizierung für Benutzerauthentifizierung und angegebenem AD-Attribut.

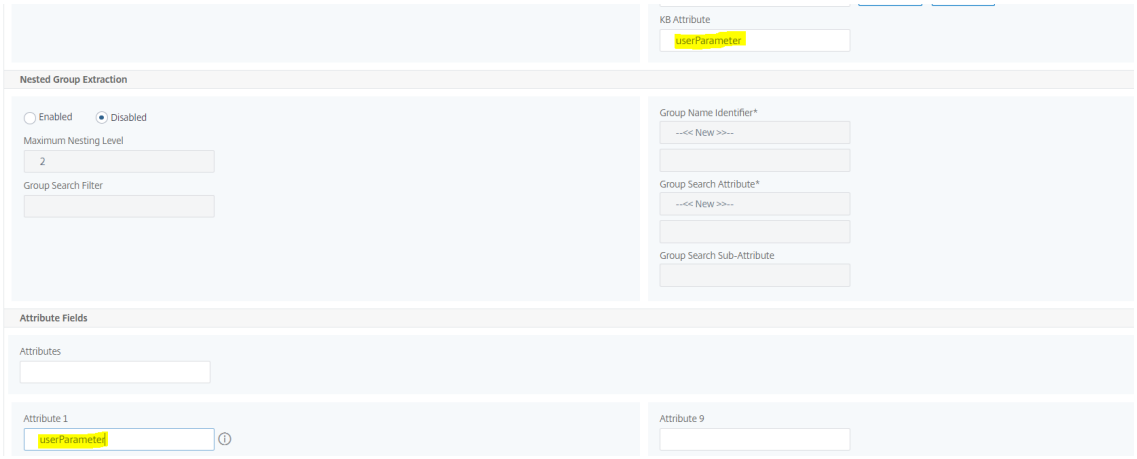


2. LDAP-Server für die Extraktion von Benutzerparametern ohne Authentifizierung.

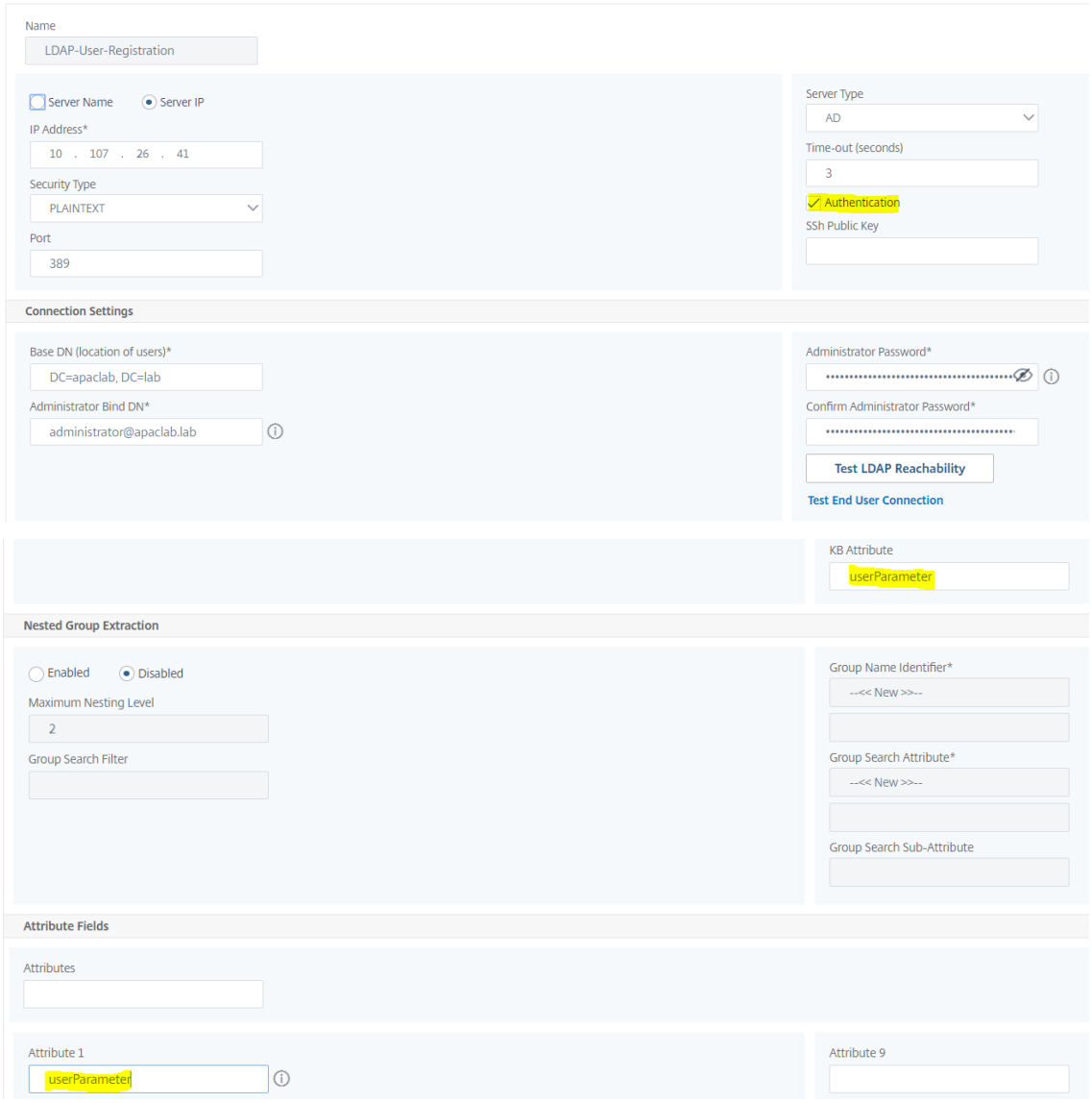


3. LDAP-Server zum Zurücksetzen des Kennworts auf SSL ohne Auth. Außerdem muss das AD-Attribut, das zum Speichern der Benutzerdetails verwendet werden soll, in diesem Server definiert werden.

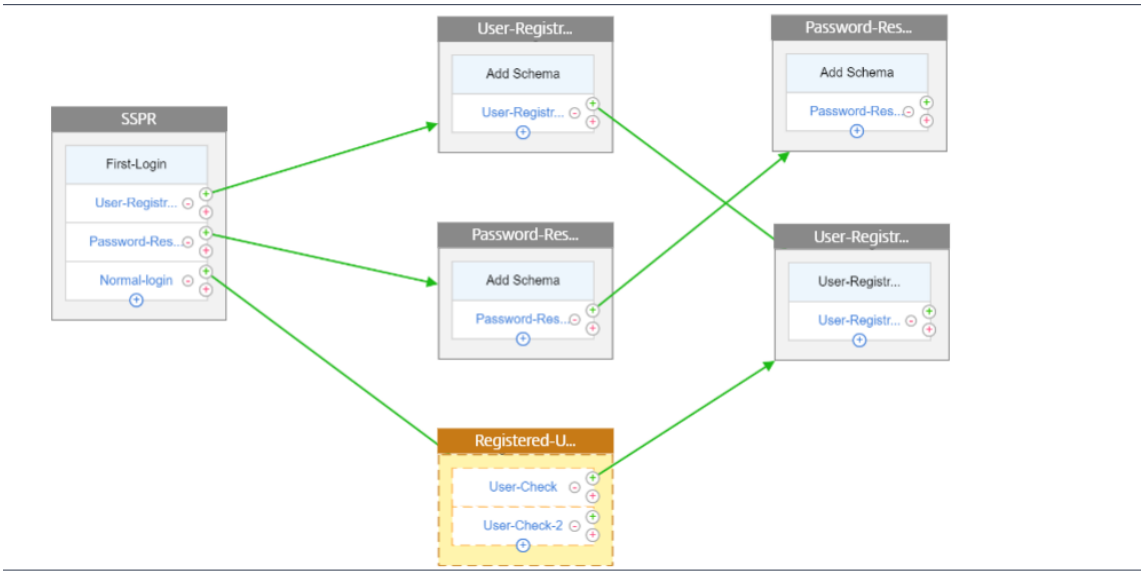




4. LDAP-Server für Benutzerregistrierung mit aktivierter Authentifizierung und angegebenem AD-Attribut



5. Die folgende Abbildung zeigt den vollständigen Ablauf:



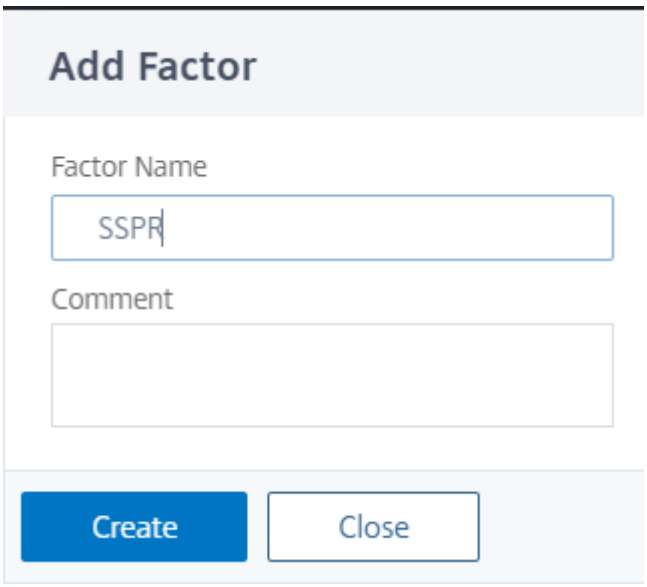
6. Binden Sie das Zertifikat global mithilfe des folgenden CLI-Befehls:

```
1 bind vpn global -userDataEncryptionKey Wildcard
```

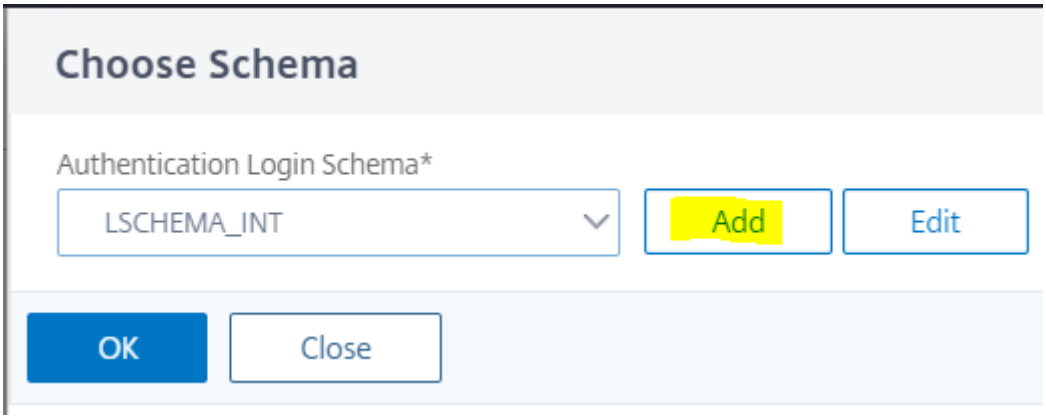
Nachdem die LDAP-Server hinzugefügt wurden, fahren Sie mit der nFactor-Konfiguration mit dem Visualizer fort

1. Navigieren Sie zu, **Sicherheit > AAA > Anwendungsdatenverkehr > nFactor Visualizer > nFactor Flows**, klicken Sie auf **Hinzufügen** und klicken Sie auf das Plus-Symbol im Feld.

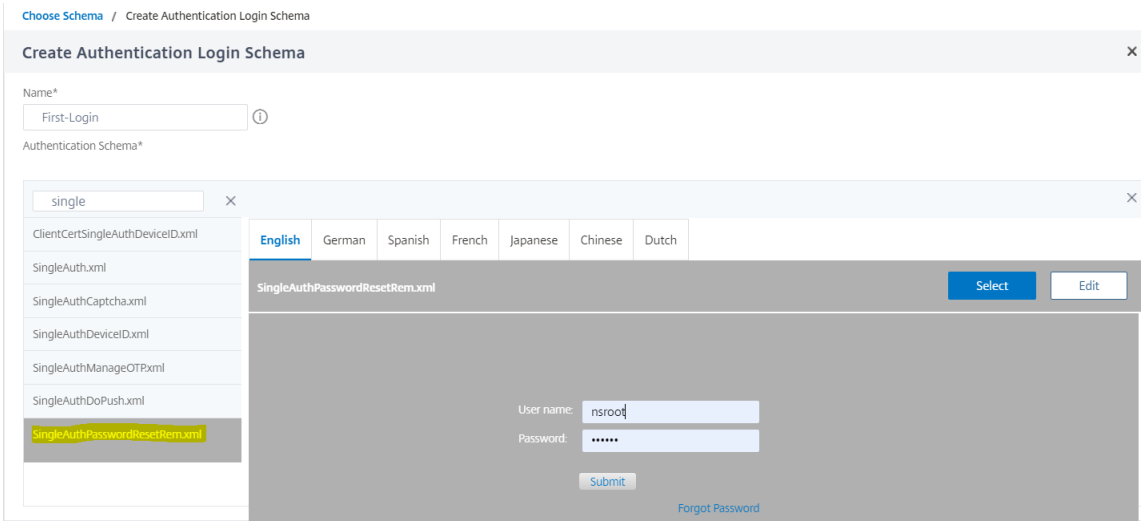
2. Gib dem Flow einen Namen.



3. Klicken Sie auf **Schema hinzufügen**, das als Standardschema dient. Klicken Sie auf der Anmeldeschemaseite auf **Hinzufügen** .



4. Nachdem Sie dem Schema einen Namen gegeben haben, wählen Sie das Schema aus. Klicken **Sie in der oberen rechten Ecke auf Auswählen**, um das Schema auszuwählen.



5. Klicken Sie auf **Erstellen** und dann auf **OK**.

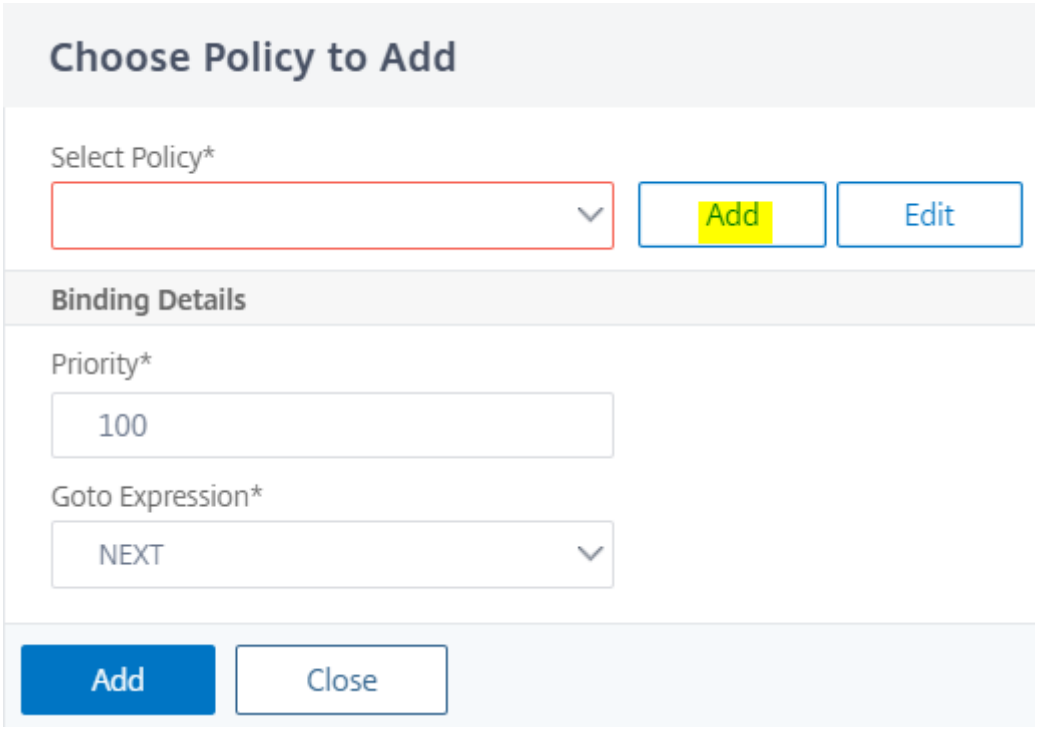
Sobald das Standardschema hinzugefügt wurde, müssen wir die folgenden drei Abläufe konfigurieren:

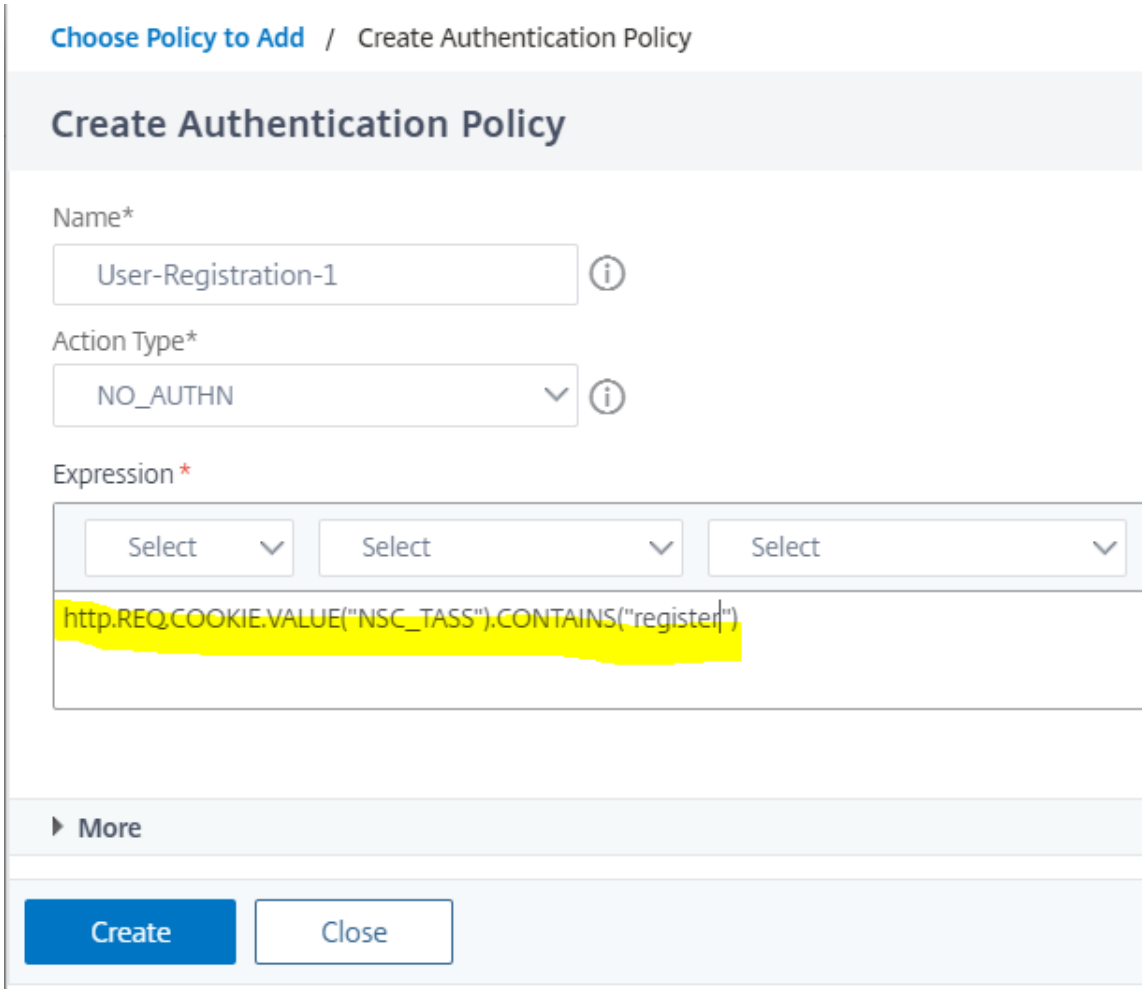
- **Benutzerregistrierung**: Für explizite Benutzerregistrierung
- **Kennwort zurücksetzen**: Zum Zurücksetzen des Kennworts
- **Normale Anmeldung + Prüfung registrierter Benutzer**: Falls der Benutzer registriert ist und das richtige Kennwort eingibt, ist der Benutzer angemeldet. Falls der Benutzer nicht registriert ist, wird der Benutzer zur Registrierungsseite weitergeleitet.

Registrierung von Benutzern

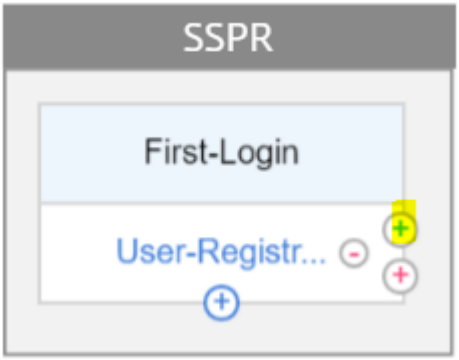
Lassen Sie uns dort weitermachen, wo wir nach dem Hinzufügen des Schemas gegangen sind.

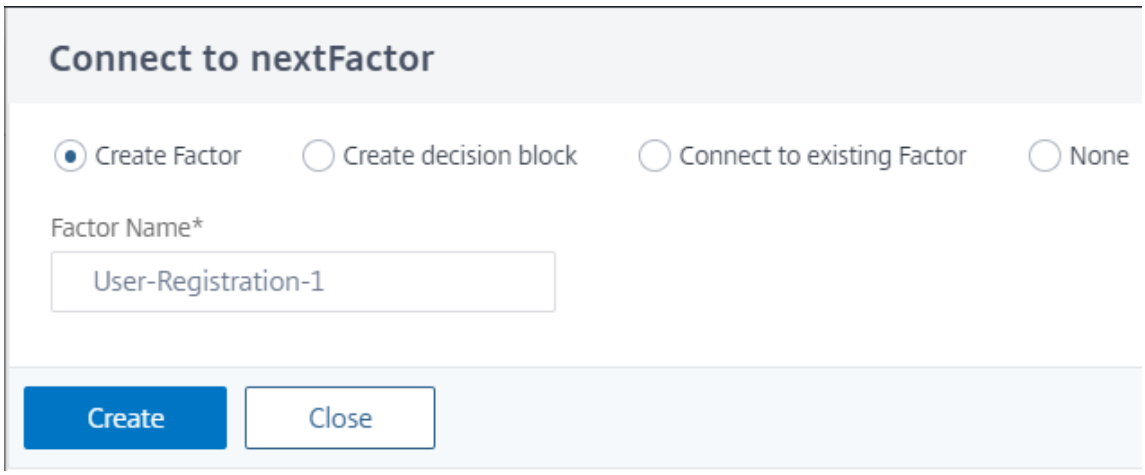
1. Klicken Sie auf **Richtlinie hinzufügen**, um zu überprüfen, ob der Benutzer versucht, sich explizit zu registrieren.



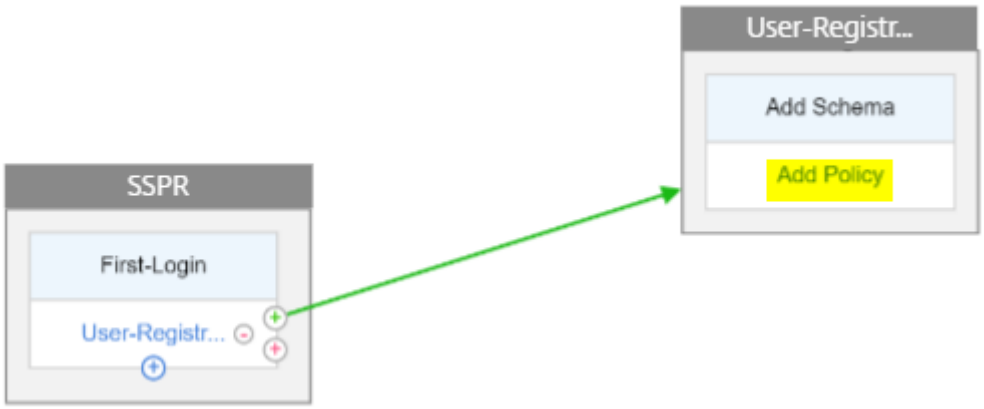


2. Klicken Sie auf **Erstellen** und dann auf **Hinzufügen**.
3. Klicken Sie auf das hervorgehobene grüne “+” -Symbol, um den nächsten Authentifizierungsfaktor zum Ablauf der Benutzerregistrierung hinzuzufügen.

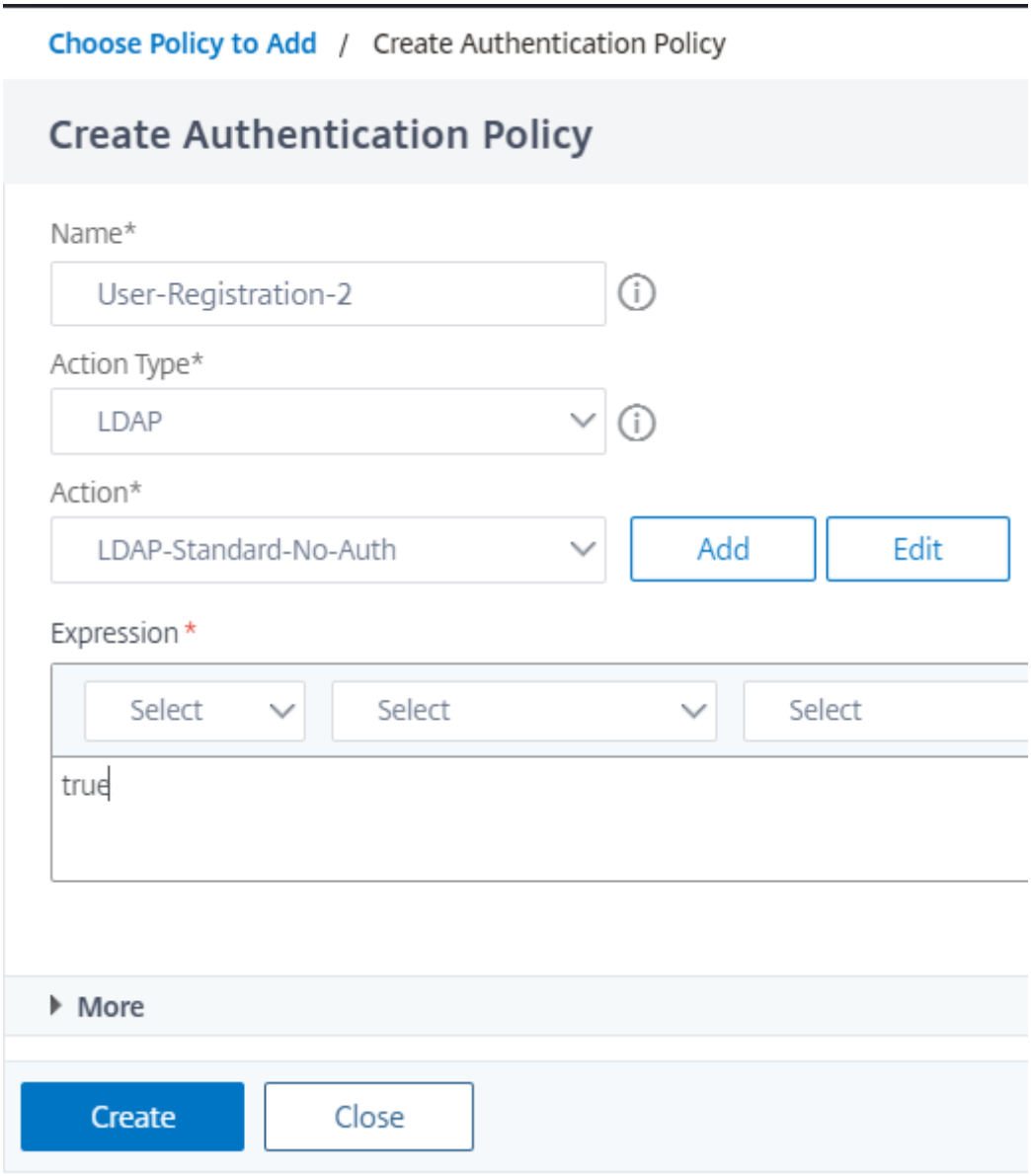




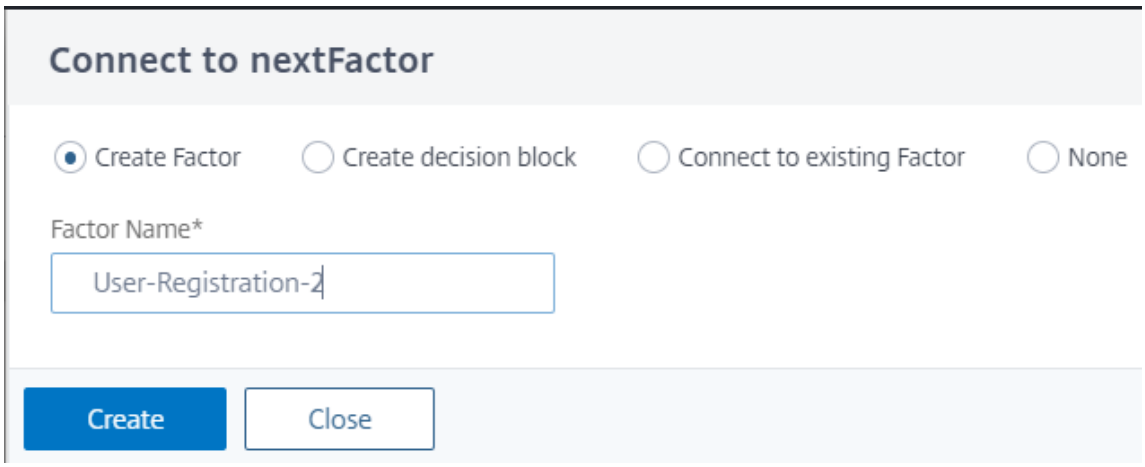
4. Klicken Sie auf **Erstellen**.
5. Klicken Sie auf **Richtlinie für den Faktor Benutzerregistrierung hinzufügen-1** .



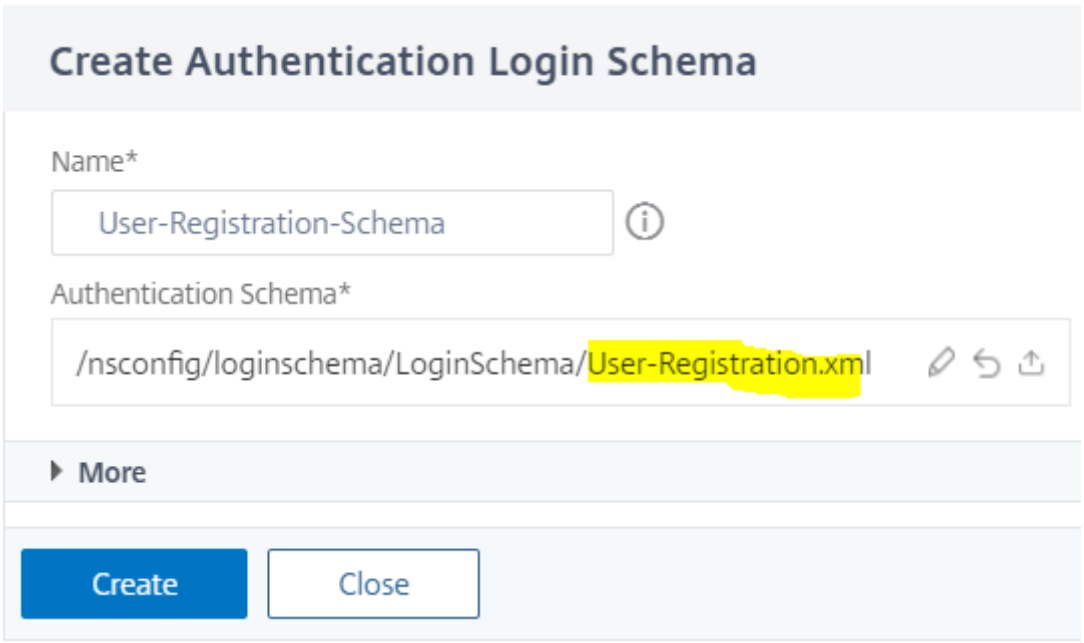
6. Erstellen Sie die Authentifizierungsrichtlinie. Diese Richtlinie extrahiert die Benutzerinformationen und validiert sie, bevor sie auf die Registrierungsseite umgeleitet werden.



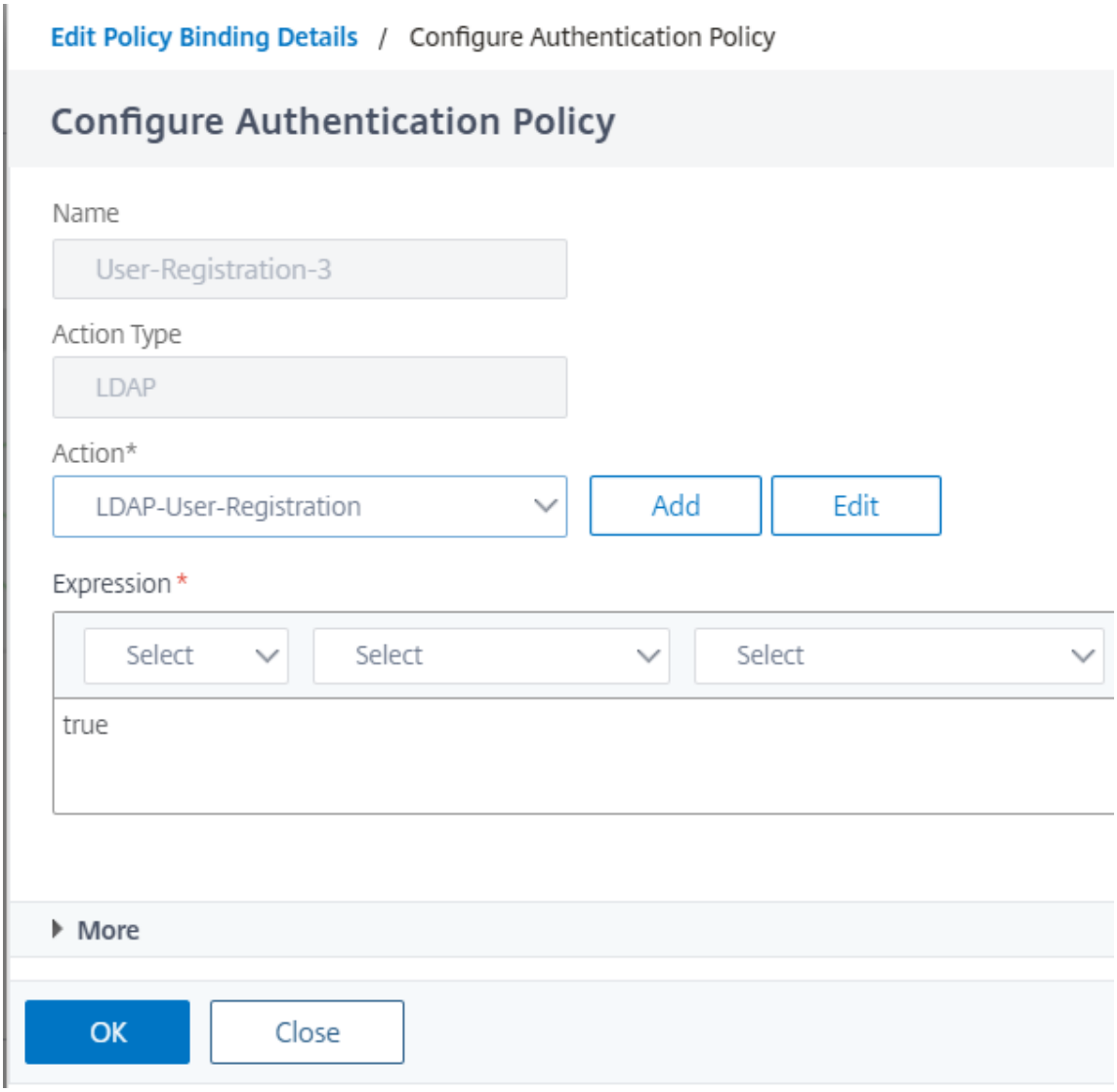
7. Klicken Sie auf **Erstellen** und dann auf **Hinzufügen**.
8. Klicken Sie nun auf das grüne “+” -Symbol, um einen weiteren Faktor für die Benutzerregistrierung zu erstellen, und klicken Sie auf **Erstellen**. Klicken Sie auf **Schema hinzufügen**.



9. Erstellen Sie das folgende Schema.



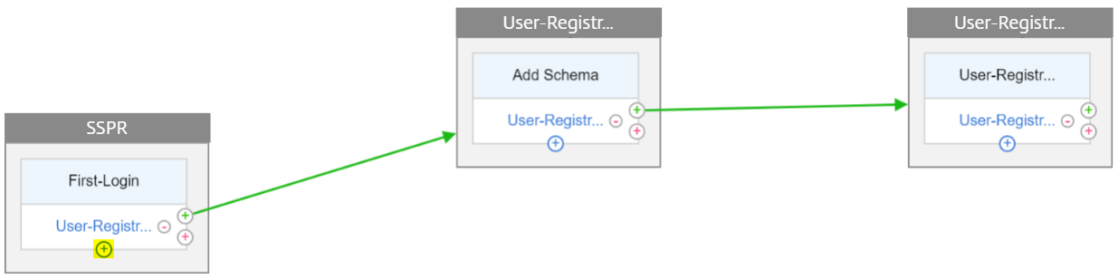
10. Klicken Sie auf **Richtlinie hinzufügen** und erstellen Sie die folgende Authentifizierungsrichtlinie.



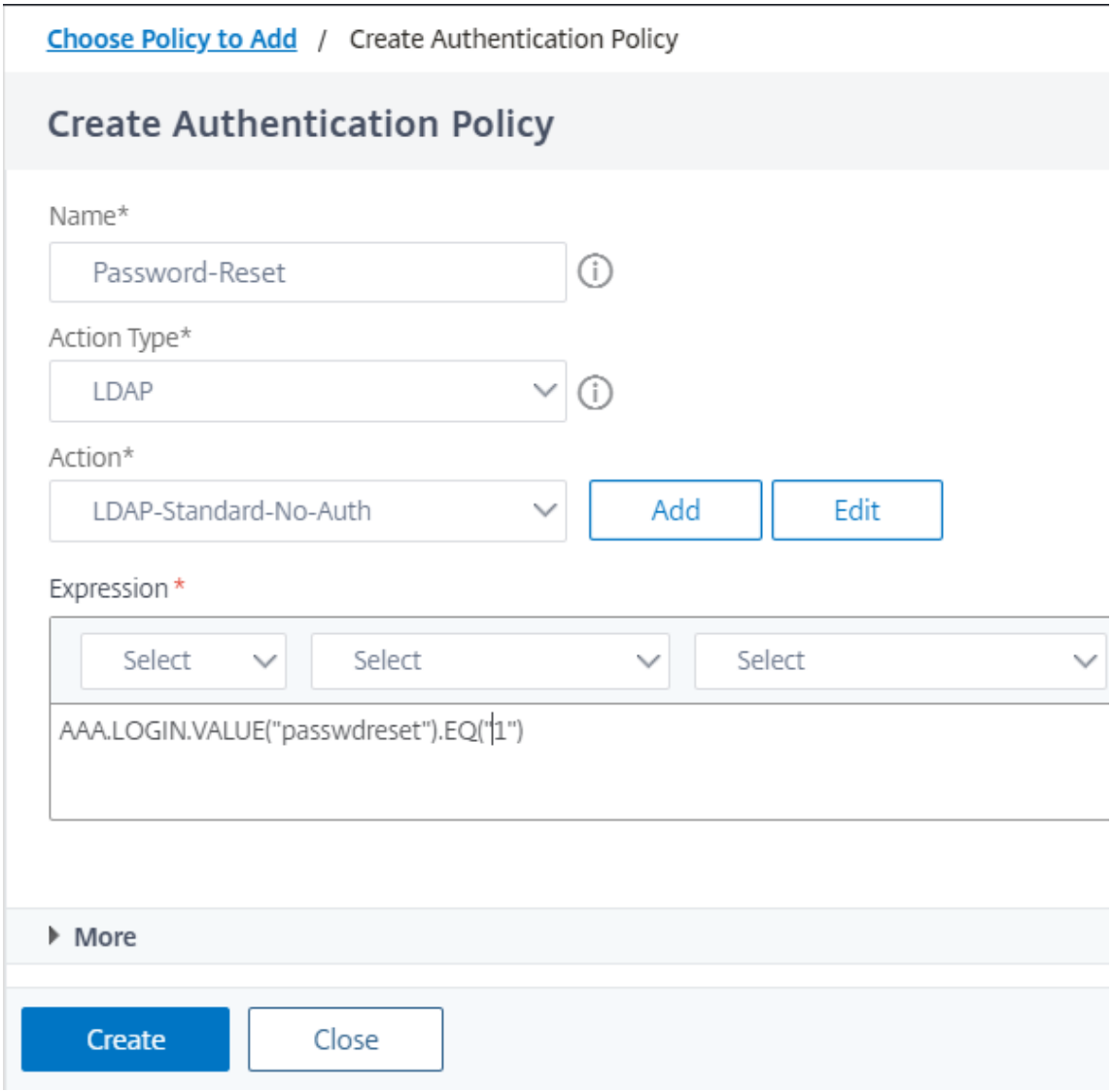
11. Klicken Sie auf **Erstellen** und dann auf **Hinzufügen**.

Kennwort zurücksetzen

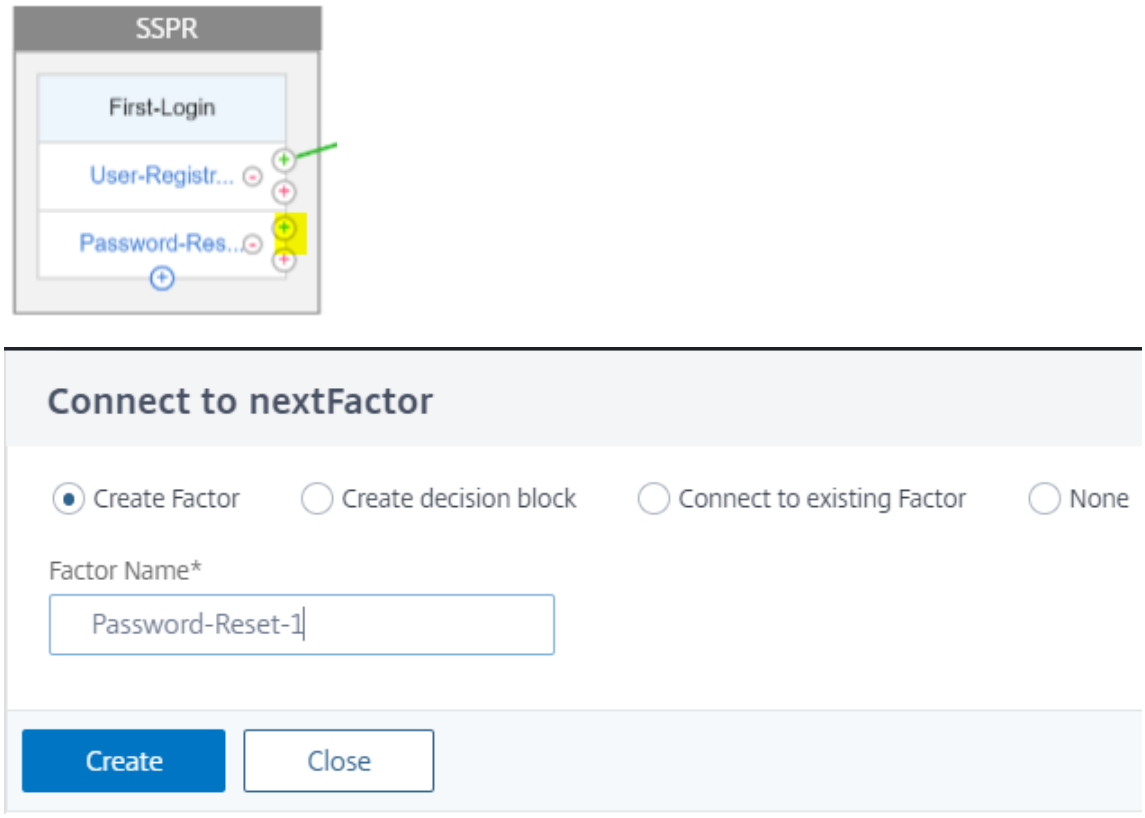
1. Klicken Sie auf das blaue “+” -Symbol, um eine weitere Richtlinie (Password Reset Flow) für den übergeordneten SSPR-Faktor hinzuzufügen.



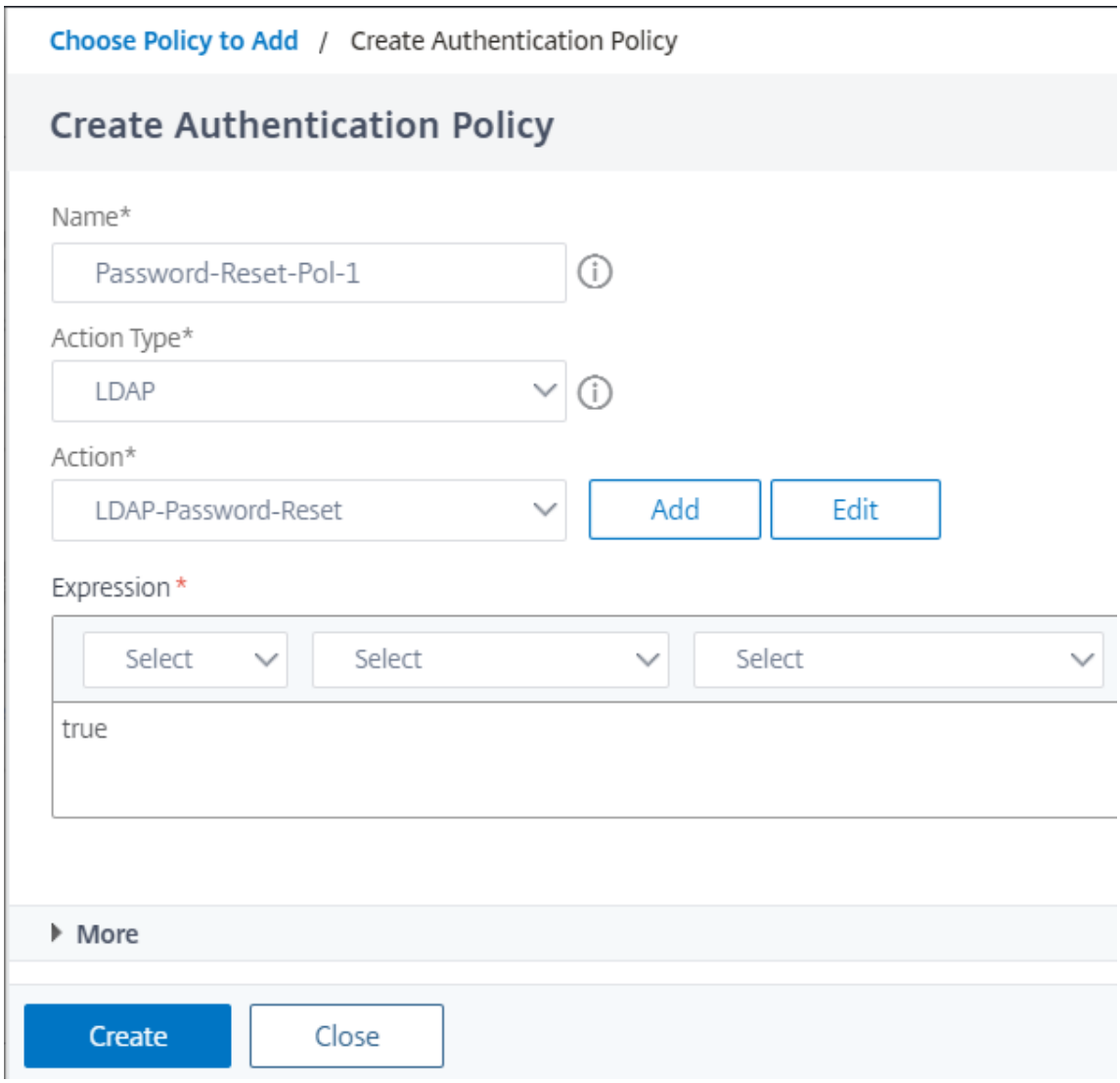
2. Klicken Sie auf **Hinzufügen** und erstellen Sie eine Authentifizierungsrichtlinie. Diese Richtlinie wird ausgelöst, wenn der Benutzer auf der Anmeldeseite auf “Kennwort vergessen” klickt.



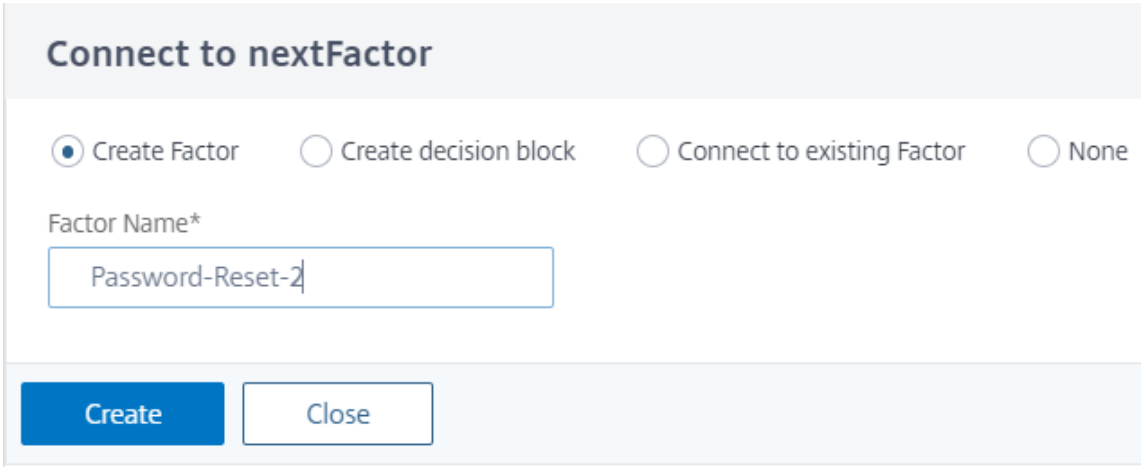
3. Klicken Sie auf **Erstellen** und dann auf **Hinzufügen**.
4. Klicken Sie auf das grüne “+” -Symbol für die Authentifizierungsrichtlinie zum Zurücksetzen des Kennworts, um einen weiteren Faktor hinzuzufügen.



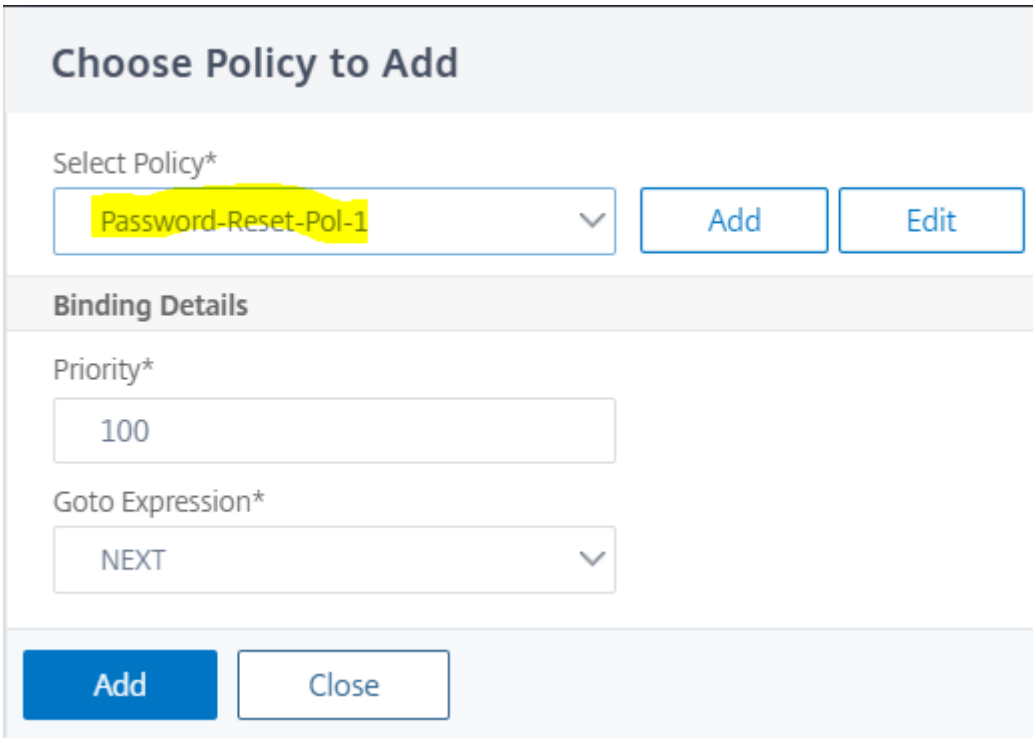
5. Klicken Sie auf **Erstellen**.
6. Klicken Sie auf **Richtlinie hinzufügen**, um eine Authentifizierungsrichtlinie für den zuvor erstellten Faktor zu erstellen. Dieser Faktor dient zur Validierung des Benutzers.



7. Klicken Sie auf **Erstellen** und dann auf **Hinzufügen**.
8. Klicken Sie auf das grüne “+” -Symbol, um einen weiteren Faktor für den Kennwortfaktorfluss hinzuzufügen. Dadurch werden die Antworten zum Zurücksetzen des Kennworts überprüft. Klicken Sie auf **Erstellen**.

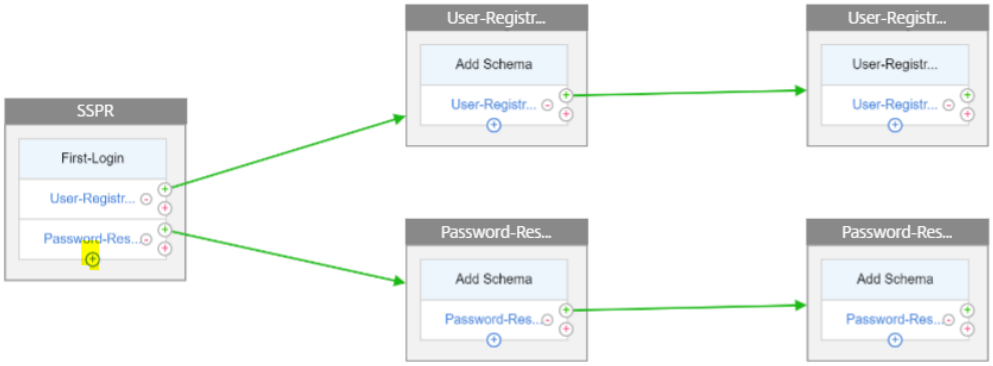


9. Klicken Sie auf **Richtlinie hinzufügen**, um eine Authentifizierungsrichtlinie für den Faktor hinzuzufügen.
10. Wählen Sie im Dropdown-Menü dieselbe Authentifizierungsrichtlinie aus, die wir zuvor erstellt haben, und klicken Sie auf **Hinzufügen**.

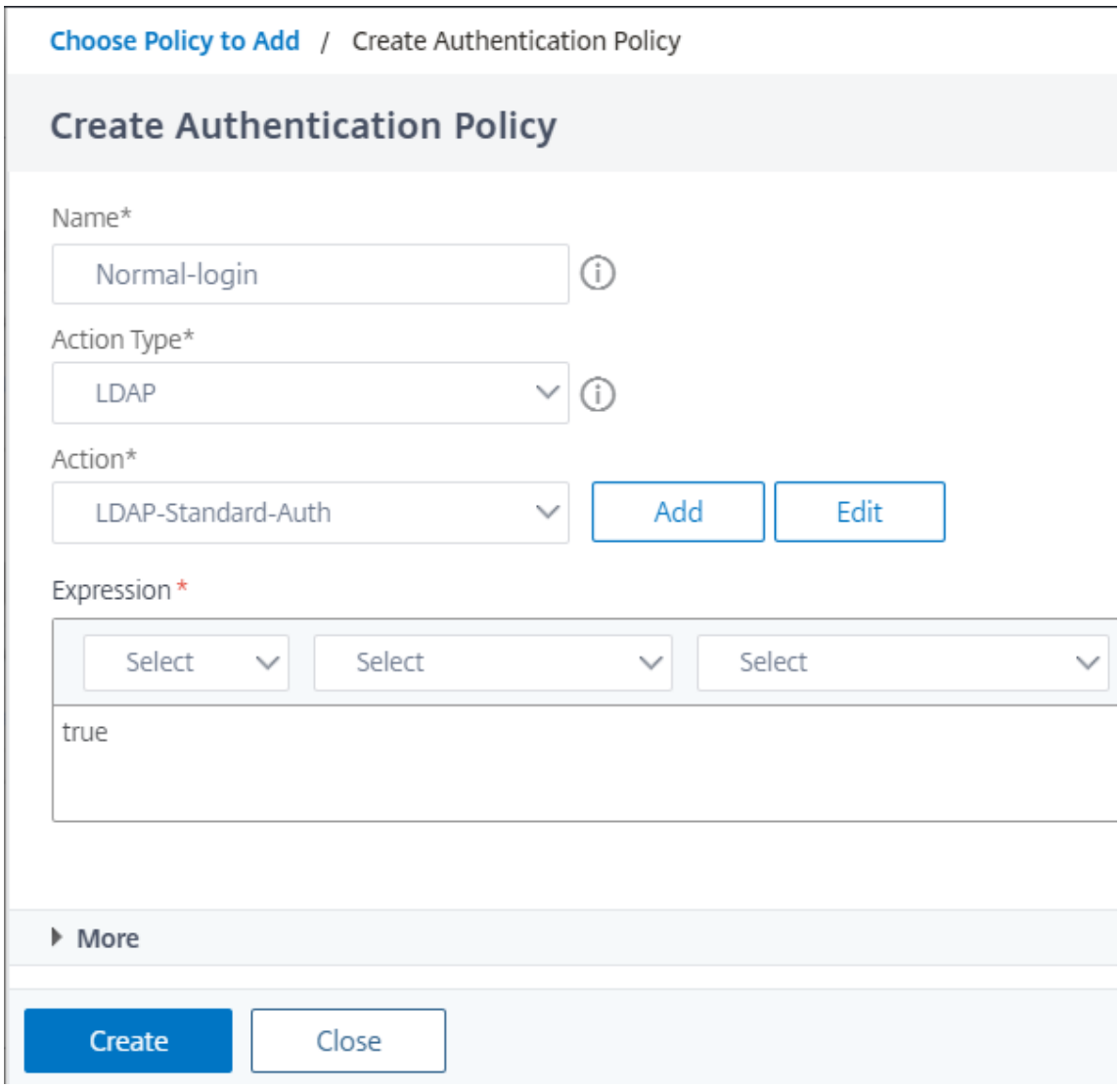


Normale Anmeldung + Überprüfung durch registrierte Benutzer

1. Klicken Sie auf das blaue “+” -Symbol, um dem übergeordneten SSPR-Faktor eine weitere Authentifizierungsrichtlinie (normaler Anmeldeablauf) hinzuzufügen.

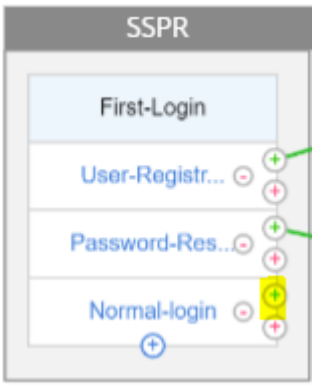


2. Klicken Sie auf **Hinzufügen**, um eine Authentifizierungsrichtlinie für die normale Benutzeranmeldung zu erstellen.

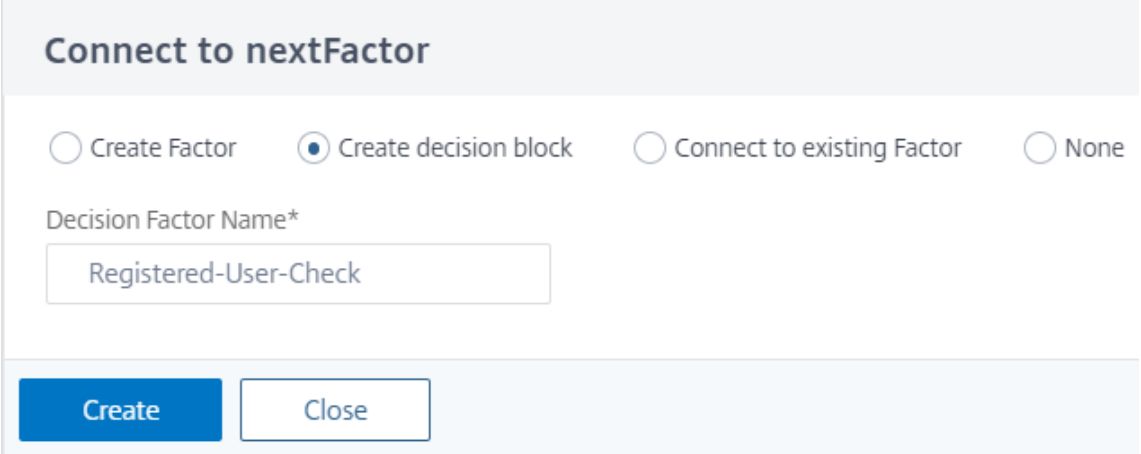


3. Klicken Sie auf **Erstellen** und dann auf **Hinzufügen**.

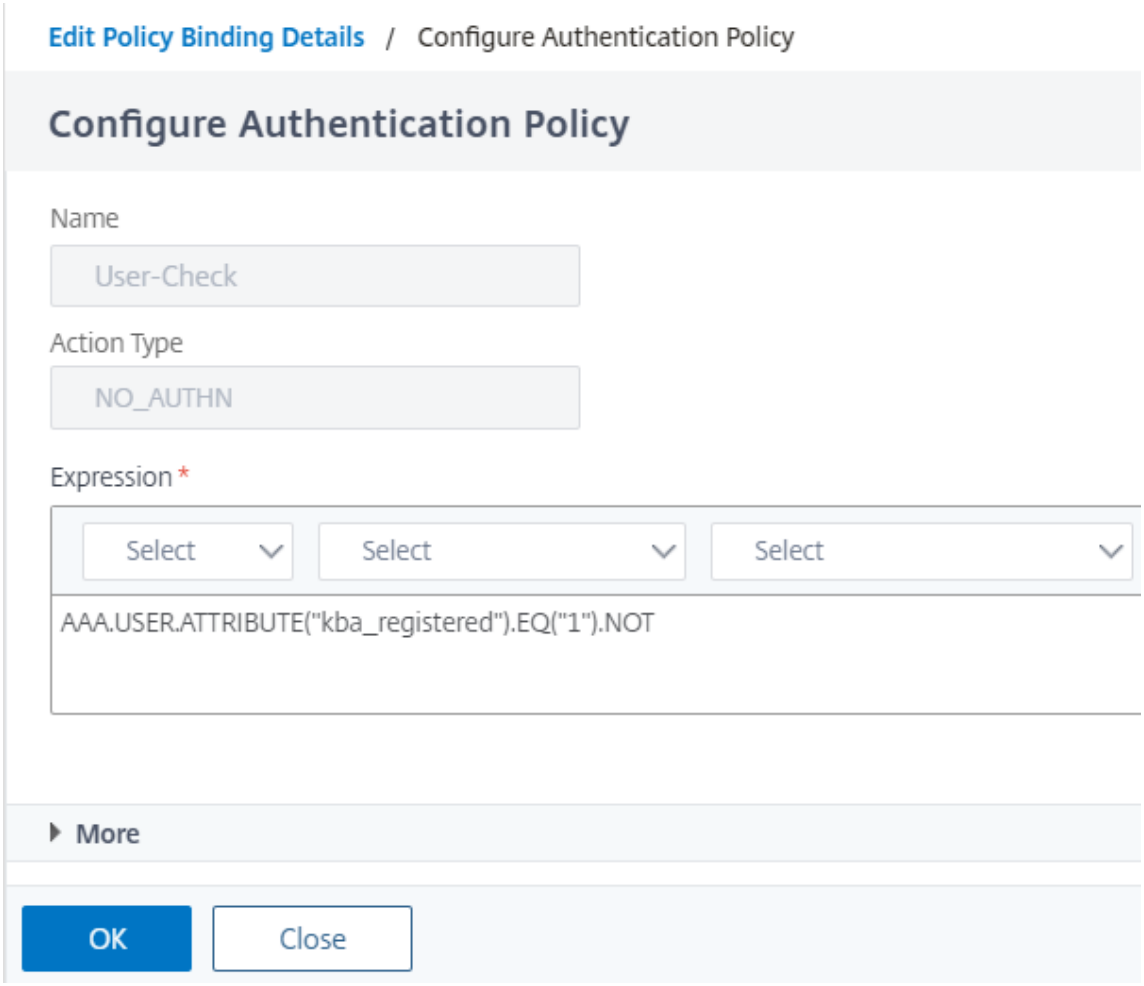
4. Klicken Sie auf das grüne “+” -Symbol für die zuvor erstellte Richtlinie, um einen weiteren Faktor hinzuzufügen, nämlich den Entscheidungsblock. Klicken Sie auf **Erstellen**.



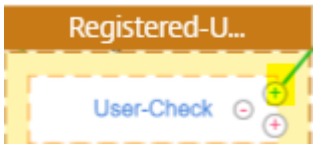
5. Klicken Sie auf **Erstellen**.



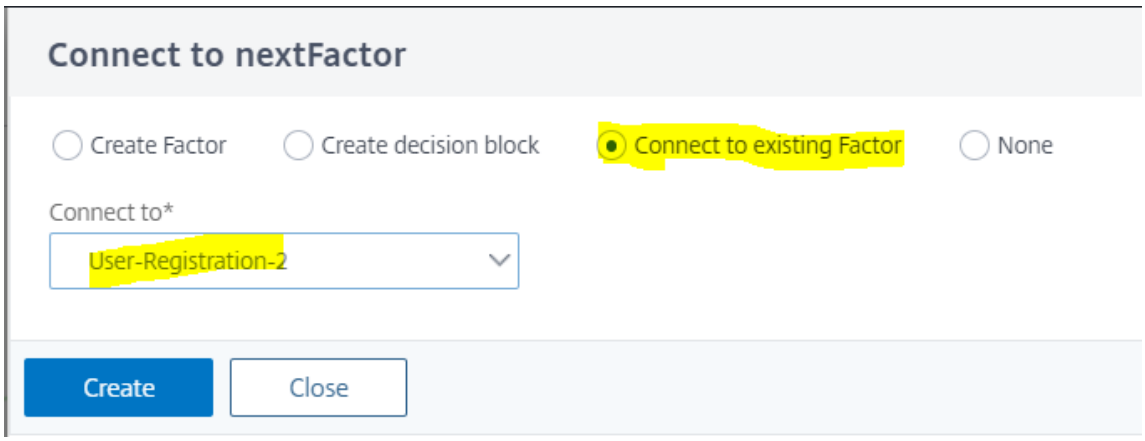
6. Klicken Sie auf **Richtlinie hinzufügen**, um eine Authentifizierungsrichtlinie für diesen Entscheidungsfaktor zu erstellen.



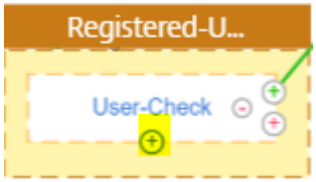
7. Klicken Sie auf **Erstellen** und dann auf **Hinzufügen**. Dadurch wird geprüft, ob der Benutzer registriert ist oder nicht.
8. Klicken Sie auf das grüne “+” -Symbol, um den Benutzer auf die Registrierungsrichtlinie hinzuweisen.



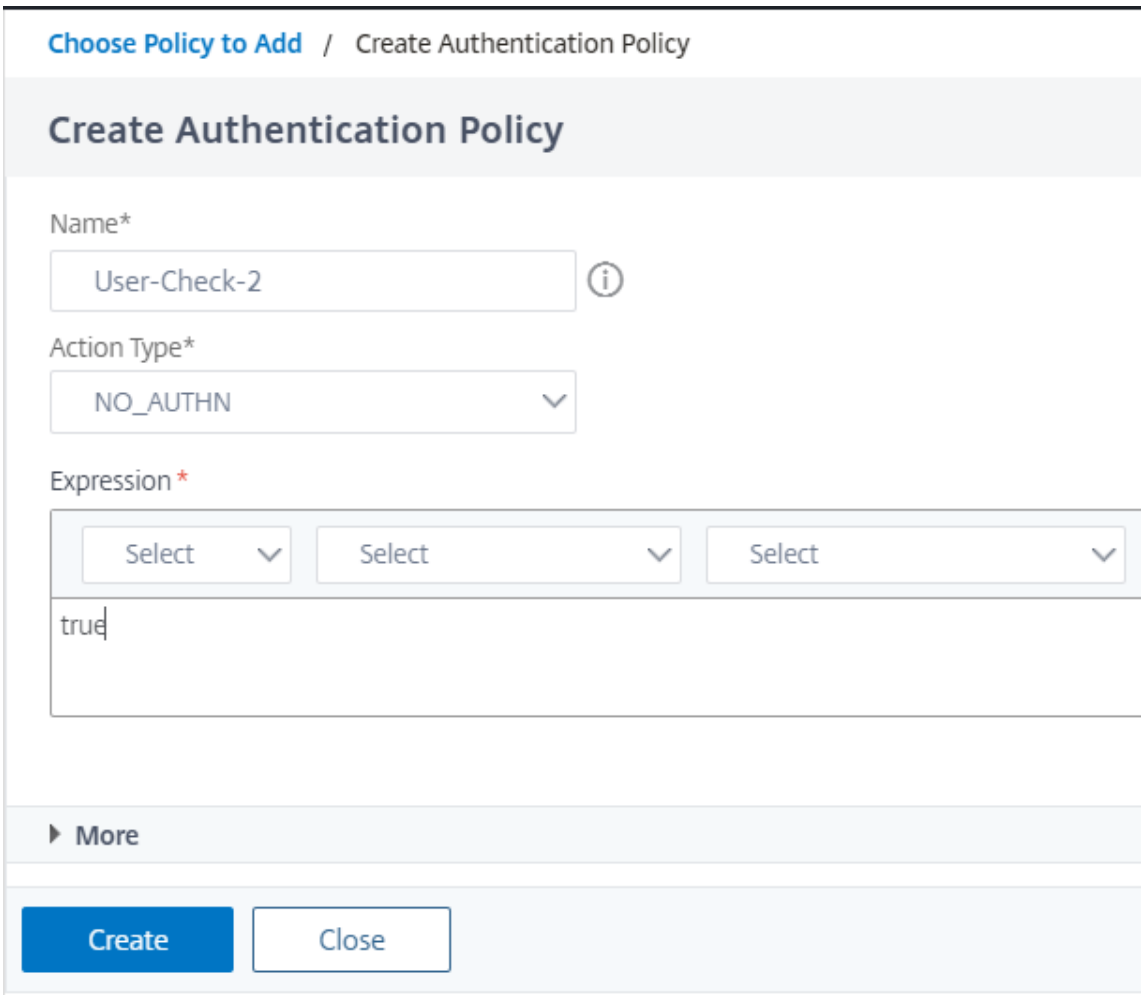
9. Wählen Sie den Registrierungsfaktor aus dem Dropdown-Menü aus und klicken Sie auf **Erstellen**.



10. Klicken Sie nun auf das blaue “+” -Symbol, um dem Entscheidungsblock eine weitere Richtlinie hinzuzufügen. Mit dieser Richtlinie kann der registrierte Benutzer die Authentifizierung beenden.



11. Klicke auf **Richtlinie hinzufügen**, um eine Authentifizierungsrichtlinie zu erstellen.



12. Klicken Sie auf **Erstellen** und dann auf **Hinzufügen**.

Abfragen während der Authentifizierung

October 5, 2021

Ausgehend von Citrix ADC Release Build 13.0.79.64 kann eine Citrix ADC Appliance während der Multifaktor-Authentifizierung für den Polling-Mechanismus konfiguriert werden.

Wenn Polling auf einer Citrix ADC Appliance konfiguriert ist, können Endpunkte (wie ein Webbrowser oder eine App) die Appliance während der Authentifizierung in den konfigurierten Intervallen abfragen (untersuchen), um den Status der übermittelten Authentifizierungsanforderung abzurufen.

Die Abfrage kann so konfiguriert werden, dass Authentifizierungen verarbeitet werden, wenn ein Endpunkt eine TCP-Verbindung während der Authentifizierung bei einer Citrix ADC Appliance unterbricht.

Punkte zu beachten

- Die Polling-Konfiguration wird für LDAP-, RADIUS- und TACACS-Authentifizierungsmethoden unterstützt.
- Der Client kann Authentifizierungsanfragen ab dem zweiten Faktor untersuchen.

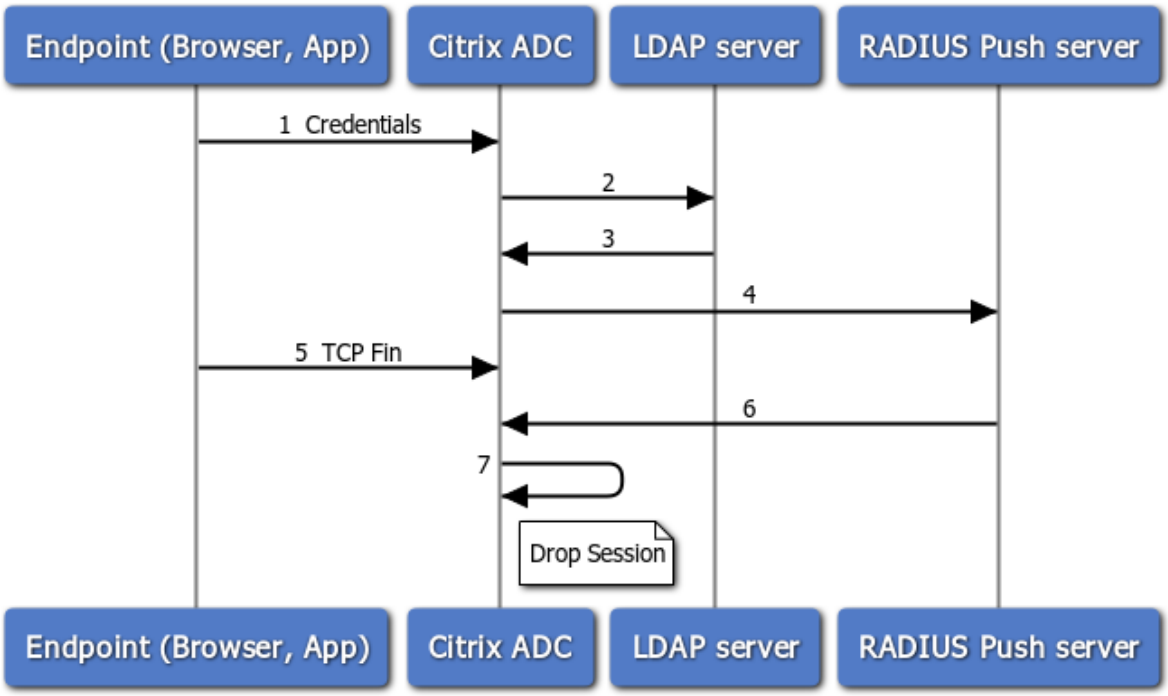
Warum sollte Polling konfiguriert werden?

Manchmal führt der Wechsel zwischen den Apps (z. B. einer Anmelde-App und einer Authentifikator-App) dazu, dass Endpunkte die Verbindung zur Citrix ADC Appliance verlieren, was zu einer Unterbrechung des Authentifizierungsflusses führt. Wenn Polling konfiguriert ist, kann diese Unterbrechung der Authentifizierung vermieden werden.

Den Polling-Mechanismus verstehen

Im Folgenden finden Sie ein Beispiel für den Ereignisfluss während der Authentifizierung, ohne dass Polling konfiguriert ist.

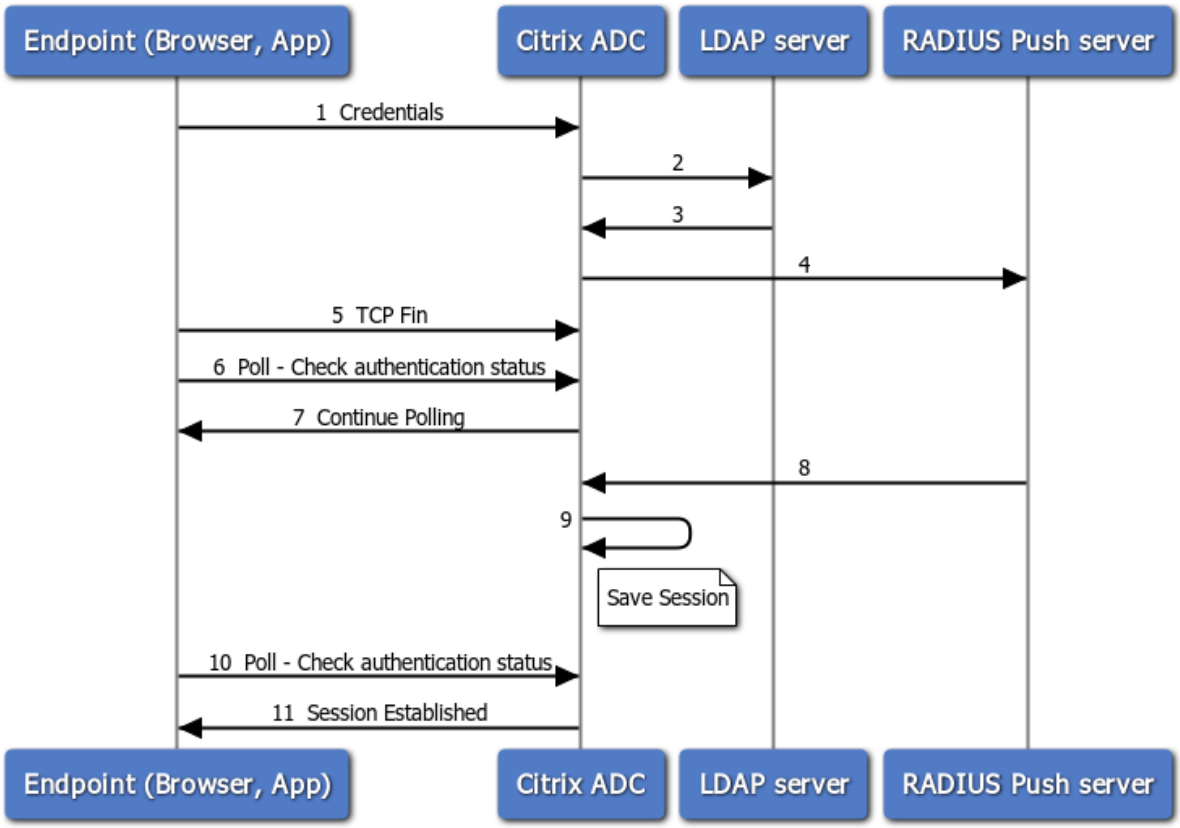
Der Abfragemechanismus ermöglicht es einer Citrix ADC Appliance, eine laufende Authentifizierung mit dem Endpunkt fortzusetzen, ohne den Authentifizierungsprozess in einem seltenen Fall eines Zurücksetzens der TCP-Verbindung am Endpunkt neu starten zu müssen.



1. Ein Endpunkt (App oder Webbrowser) authentifiziert sich mit Anmeldeinformationen.

2. Der Benutzername und das Kennwort werden mit einem vorhandenen First-Faktor-Verzeichnis (LDAP/Active Directory) überprüft.
3. Wenn die richtigen Anmeldeinformationen angegeben werden, wechselt die Authentifizierung zum nächsten Faktor.
4. Zu diesem Zeitpunkt sendet die Citrix ADC Appliance eine Anfrage an den RADIUS-Push-Server.
5. Während die Citrix ADC Appliance auf eine Antwort vom RADIUS-Server wartet, unterbricht der Endpunkt die TCP-Verbindung.
6. Der Citrix ADC erhält eine Antwort vom RADIUS-Push-Server.
7. Da keine Client-TP-Verbindung gefunden wird, bricht die Citrix ADC Appliance die Sitzung ab und die Anmeldung schlägt fehl.

Im Folgenden finden Sie ein Beispiel für den Ereignisfluss während der Authentifizierung mit konfiguriertem Polling.



1. Ein Endpunkt (App oder Webbrowser) authentifiziert sich mit Anmeldeinformationen.
2. Der Benutzername und das Kennwort werden mit einem vorhandenen First-Faktor-Verzeichnis (LDAP/Active Directory) überprüft.
3. Wenn die richtigen Anmeldeinformationen angegeben werden, wechselt die Authentifizierung zum nächsten Faktor.
4. Zu diesem Zeitpunkt sendet die Citrix ADC Appliance eine Anfrage an den RADIUS-Push-Server.
5. Während die Citrix ADC Appliance auf eine Antwort vom RADIUS-Server wartet, unterbricht der

Endpunkt die TCP-Verbindung.

6. Endpoint sendet eine Umfrage (Probe) an die Citrix ADC Appliance, um nach dem Authentifizierungsstatus zu suchen.
7. Da die Citrix ADC Appliance keine Rückmeldung vom RADIUS-Server hört, fordert sie den Endpunkt auf, die Abfrage fortzusetzen.
8. Die Citrix ADC Appliance erhält eine Antwort vom RADIUS-Push-Server.
9. Da keine Client-TP-Verbindung gefunden wird, speichert ADC den Sitzungsstatus.
10. Endpoint fragt erneut ab, um nach dem Authentifizierungsstatus zu suchen.
11. Die Citrix ADC Appliance richtet die Sitzung ein und die Anmeldung ist erfolgreich.

Konfigurieren von Polling mit CLI

Im Folgenden finden Sie eine Beispiel-CLI Konfiguration.

Konfigurieren Sie den ersten Faktor

```
add authentication ldapAction ldap-new -serverIP 10.106.40.65 -
    serverPort 636 -ldapBase "dc=aaatm-test,dc=com" -ldapBindDn
    administrator@aaatm-test.com -ldapBindDnPassword 2
    f63d3659103464a4fad0ade65e2ccfd4e8440e36ddff941d29796af03e01139 -
    encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -
    groupAttrName memberof -subAttributeName CN -secType SSL -
    alternateEmailAttr userParameters

add authentication Policy ldap-new -rule true -action ldap-new

bind authentication vserver avs -policy ldap-new -priority 1 -
    nextFactor rad_factor
<!--NeedCopy-->
```

Konfigurieren Sie den zweiten Faktor

```
add authentication radiusAction rad1 -serverIP 10.102.229.120 -radKey 1
    b1613760143ce2371961e9a9eb5392c86a4954a62397f29a01b5d12b42ce232 -
    encrypted -encryptmethod ENCMTHD_3

add authentication Policy rad -rule true -action rad1
<!--NeedCopy-->
```


Konfigurieren Sie das Anmeldesschema Poll.xml

```
add authentication loginSchema polling_schema -authenticationSchema
    LoginSchema/Poll.xml

add authentication policylabel rad_factor -loginSchema polling_schema

bind authentication policylabel rad_factor -policyName rad -priority 1
    -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

Konfigurieren von Polling mit GUI

Ausführliche Schritte zum Konfigurieren der Multifaktor-Authentifizierung mit der GUI finden Sie unter Konfigurieren der nFactor-Authentifizierung

Im Folgenden finden Sie die Beispielschritte auf hoher Ebene, die für die Konfiguration von Citrix ADC für Polling ab dem zweiten Faktor erforderlich sind.

1. Erstellen Sie einen ersten Faktor für die Authentifizierung, zum Beispiel LDAP.
2. Erstellen Sie einen zweiten Faktor für die Authentifizierung, z. B.
3. Fügen Sie **Poll.xml** in Citrix ADC (/nsConfig/loginschema/loginschema/) als Anmeldeschema für den zweiten Faktor hinzu.

Sitzungs- und Verkehrsmanagement

October 5, 2021

Sitzungseinstellungen

Nachdem Sie Ihre Authentifizierungs-, Autorisierungs- und Überwachungsprofile konfiguriert haben, konfigurieren Sie Sitzungseinstellungen, um Ihre Benutzersitzungen anzupassen. Die Sitzungseinstellungen sind:

- **Das Sitzungszeitlimit.**

  Steuert den Zeitraum, nach dem der Benutzer automatisch getrennt wird, und muss sich erneut authentifizieren, um auf das Intranet zuzugreifen.

- **Die Standardeinstellung für die Autorisierung.**

  Bestimmt, ob die Citrix ADC Appliance standardmäßig den Zugriff auf Inhalte zulässt oder verweigert, für die keine spezifische Autorisierungsrichtlinie vorhanden ist.

- **Die Einstellung für einmaliges Anmelden.**

  Bestimmt, ob die Citrix ADC Appliance Benutzer automatisch bei allen Webanwendungen anmeldet, nachdem sie sich authentifiziert haben, oder übergibt Benutzer an die Anmeldeseite der Webanwendung, um sich für jede Anwendung zu authentifizieren.

- **Die Indexeinstellung für Anmeldeinformationen.**

  Bestimmt, ob die Citrix ADC Appliance die primären oder sekundären Authentifizierungsanmeldeinformationen für Single Sign-On verwendet.

Um die Sitzungseinstellungen zu konfigurieren, können Sie einen von zwei Ansätzen verwenden. Wenn Sie unterschiedliche Einstellungen für verschiedene Benutzerkonten oder Gruppen wünschen, erstellen Sie ein Profil für jedes Benutzerkonto oder jede Gruppe, für die Sie benutzerdefinierte Sitzungseinstellungen konfigurieren möchten. Außerdem erstellen Sie Richtlinien, um die Verbindungen auszuwählen, auf die bestimmte Profile angewendet werden sollen, und binden die Richtlinien an Benutzer oder Gruppen. Sie können auch eine Richtlinie an den virtuellen Authentifizierungsserver binden, der den Datenverkehr verarbeitet, auf den Sie das Profil anwenden möchten.

Wenn Sie dieselben Einstellungen für alle Sitzungen wünschen oder die Standardeinstellungen für Sitzungen anpassen möchten, für die keine spezifischen Profile und Richtlinien konfiguriert sind, können Sie einfach die globalen Sitzungseinstellungen konfigurieren.

Sitzungsprofile

Um Ihre Benutzersitzungen anzupassen, erstellen Sie zunächst ein Sitzungsprofil. Mit dem Sitzungsprofil können Sie globale Einstellungen für einen der Sitzungsparameter außer Kraft setzen.

> **Hinweis:**
>
> Die Begriffe “Sitzungsprofil” und “Sitzungsaktion” bedeuten dasselbe.

So erstellen Sie ein Sitzungsprofil mit der Befehlszeilenschnittstelle

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

```
1 add tm sessionAction <name> [-sessTimeout <mins>] [-
     defaultAuthorizationAction ( ALLOW | DENY )][-SSO ( ON | OFF )][-
     ssoCredential ( PRIMARY | SECONDARY )] [-ssoDomain <string>][-
     httpOnlyCookie ( YES | NO )] [-persistentCookie ( ENABLED | DISABLED
      )] [-persistentCookieValidity <minutes>]
2
```



```
show tm sessionAction <name>
<!--NeedCopy-->
```

Beispiel

```
> add tm sessionAction session-profile -sessTimeout 30 -
   defaultAuthorization ALLOW
 Done
> show tm sessionAction session-profile
1)      Name: session-profile
        Authorization action : ALLOW
        Session timeout: 30 minutes
 Done
<!--NeedCopy-->
```

So ändern Sie ein Sitzungsprofil mit der Befehlszeilenschnittstelle

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

```
set tm sessionAction <name> [-sessTimeout <mins>] [-
   defaultAuthorizationAction ( ALLOW | DENY )][-SSO ( ON | OFF )][-
   ssoCredential ( PRIMARY | SECONDARY )] [-ssoDomain <string>][-
   httpOnlyCookie ( YES | NO )] [-persistentCookie ( ENABLED | DISABLED
    )] [-persistentCookieValidity <minutes>]

show tm sessionAction
<!--NeedCopy-->
```

Beispiel

```
> set tm sessionAction session-profile -sessTimeout 30 -
   defaultAuthorization ALLOW
 Done
> show tm sessionAction session-profile
1)      Name: session-profile
        Authorization action : ALLOW
        Session timeout: 30 minutes
 Done
<!--NeedCopy-->
```


So entfernen Sie ein Sitzungsprofil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um ein Sitzungsprofil zu entfernen:

```
rm tm sessionAction <name>
<!--NeedCopy-->
```

So konfigurieren Sie Sitzungsprofile mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Sitzung.**
2. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Richtlinien > Sitzung.**
3. Klicken Sie im Detailbereich auf die Registerkarte **Profile**.
4. Führen Sie auf der Registerkarte **Profile** einen der folgenden Schritte aus:
   - Um ein neues Sitzungsprofil zu erstellen, klicken Sie auf **Hinzufügen.**
   - Um ein vorhandenes Sitzungsprofil zu ändern, wählen Sie das Profil aus, und klicken Sie dann auf **Bearbeiten.**
5. Geben Sie im Dialogfeld TM-Sitzungsprofil erstellen oder TM-Sitzungsprofil konfigurieren Werte für die Parameter ein oder wählen Sie sie aus.
   - Name* — actionname (Kann für eine zuvor konfigurierte Sitzungsaktion nicht geändert werden.)
   - Sitzungstimeout — sesstimeout
   - Single Sign-On bei Webanwendungen — SSO
   - Standardautorisierungsaktion — defaultAuthorizationAction
   - Anmeldeinformationsindex — ssocredential
   - Single Sign-On-Domäne — ssoDomain
   - HttpOnly Cookie — httpOnlyCookie
   - Persistent Cookie aktivieren — persistentCookie
   - Gültigkeit von dauerhaften Cookies — persistentCookieValidity
6. Klicken Sie auf **Erstellen** oder **OK**. Das von Ihnen erstellte Sitzungsprofil wird im Bereich Sitzungsrichtlinien und -profile angezeigt.

Sitzungsrichtlinien

Nachdem Sie ein oder mehrere Sitzungsprofile erstellt haben, erstellen Sie Sitzungsrichtlinien und binden die Richtlinien dann global oder an einen virtuellen Authentifizierungsserver, um sie in Kraft zu setzen.

So erstellen Sie eine Sitzungsrichtlinie mit der Befehlszeilenschnittstelle

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

```
-  add tm sessionPolicy <name> <rule> <action>
-  show tm sessionPolicy <name>
<!--NeedCopy-->
```

Beispiel

```
> add tm sessionPolicy session-pol ”URL == /\*.png” session-profile
Done
> show tm sessionPolicy session-pol
1)      Name: session-pol       Rule: URL == '/\*.png'
        Action: session-profile
 Done
<!--NeedCopy-->
```

So ändern Sie eine Sitzungsrichtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Sitzungsrichtlinie zu ändern und die Konfiguration zu überprüfen:

```
-  set tm sessionPolicy <name> [-rule <expression>] [-action <action>]
-  show tm sessionPolicy <name>
<!--NeedCopy-->
```

Beispiel

```
> set tm sessionPolicy session-pol ”URL == /\*.png” session-profile
 Done
> show tm sessionPolicy session-pol
1)      Name: session-pol       Rule: URL == '/\*.png'
        Action: session-profile
 Done
<!--NeedCopy-->
```


So binden Sie eine Sitzungsrichtlinie global mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Sitzungsrichtlinie global zu binden und die Konfiguration zu überprüfen:

```
bind tm global -policyName <policyname> [-priority <priority>]
<!--NeedCopy-->
```

Beispiel

```
> bind tm global -policyName session-pol
 Done

> show tm sessionPolicy session-pol
1)      Name: session-pol       Rule: URL == '/*.png'
        Action: session-profile
        Policy is bound to following entities
        1) TM GLOBAL    PRIORITY : 0
 Done

<!--NeedCopy-->
```

So binden Sie eine Sitzungsrichtlinie über die Befehlszeilenschnittstelle an einen virtuellen Authentifizierungsserver

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine Sitzungsrichtlinie an eine virtuelle Authentifizierung zu binden und die Konfiguration zu überprüfen:

```
bind authentication vserver <name> -policy <policyname> [-priority <
    priority>]
<!--NeedCopy-->
```

Beispiel

```
bind authentication vserver auth-vserver-1 -policyName Session-Pol-1 -
    priority 1000
Done
<!--NeedCopy-->
```


So heben Sie die Bindung einer Sitzungsrichtlinie von einem virtuellen Authentifizierungsserver mit der Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Bindung einer Sitzungsrichtlinie von einem virtuellen Authentifizierungsserver aufzuheben und die Konfiguration zu überprüfen:

```
unbind authentication vserver <name> -policy <policyname>
<!--NeedCopy-->
```

Beispiel

```
unbind authentication vserver auth-vserver-1 -policyName Session-Pol-1
Done
<!--NeedCopy-->
```

So heben Sie die Bindung einer global gebundenen Sitzungsrichtlinie mit der Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Bindung einer global gebundenen Sitzungsrichtlinie aufzuheben:

```
unbind tm global -policyName <policyname>
<!--NeedCopy-->
```

Beispiel

```
unbind tm global -policyName Session-Pol-1
Done
<!--NeedCopy-->
```

So entfernen Sie eine Sitzungsrichtlinie mit der Befehlszeilenschnittstelle

Trennen Sie zuerst die Bindung der Sitzungsrichtlinie von global, und geben Sie dann an der Eingabeaufforderung die folgenden Befehle ein, um eine Sitzungsrichtlinie zu entfernen und die Konfiguration zu überprüfen:


```
rm tm sessionPolicy <name>
<!--NeedCopy-->
```

Beispiel

```
rm tm sessionPolicy Session-Pol-1
Done

<!--NeedCopy-->
```

So konfigurieren und binden Sie Sitzungsrichtlinien mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Sitzung**.
2. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Richtlinien > Sitzung**.
3. Führen Sie im Detailbereich auf der Registerkarte **Richtlinien** eine der folgenden Aktionen aus:
   - Um eine neue Sitzungsrichtlinie zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Sitzungsrichtlinie zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Bearbeiten**.
4. Geben **Sie im Dialogfeld "Sitzungsrichtlinie erstellen** " oder " **Sitzungsrichtlinie konfigurieren** " die Werte für die Parameter ein oder wählen Sie sie aus.
   - Name* — PolicyName (Für eine zuvor konfigurierte Sitzungsrichtlinie kann nicht geändert werden.)
   - Anforderungsprofil* — Aktionsname
   - Ausdruck* — Regel (Sie geben Ausdrücke ein, indem Sie zuerst den Ausdruckstyp in der Dropdownliste ganz links unterhalb des Textbereichs Ausdruck auswählen und anschließend den Ausdruck direkt in den Ausdruckstextbereich eingeben, oder indem **Sie auf Hinzufügen** klicken, um das Dialogfeld Ausdruck hinzufügen zu öffnen und das Dropdownmenü unten Listen darin, um Ihren Ausdruck zu konstruieren.)
5. Klicken Sie auf **Erstellen** oder **OK**. Die erstellte Richtlinie wird im Detailbereich der Seite **Sitzungsrichtlinien** und **-profile** angezeigt.
6. Um eine Sitzungsrichtlinie global zu binden, wählen Sie im Detailbereich **Globale Bindungen** aus der Dropdownliste **Aktion** aus, und füllen Sie das Dialogfeld aus.
   - Wählen Sie den Namen der Sitzungsrichtlinie aus, die global gebunden werden soll.
   - Klicken Sie auf **OK**.
7. Um eine Sitzungsrichtlinie an einen virtuellen Authentifizierungsserver zu binden, klicken Sie im Navigationsbereich auf **Virtuelle Server**, und fügen Sie diese Richtlinie zur Richtlinienliste hinzu.

- Wählen Sie im Detailbereich den virtuellen Server aus, und klicken Sie dann auf **Bearbeiten**.
- Klicken Sie im Bereich **Erweiterte Auswahl** rechts neben dem Detailbereich auf **Richtlinien** .
- Wählen Sie eine Richtlinie aus, oder klicken Sie auf das **Plussymbol**, um eine Richtlinie hinzuzufügen.
- Ändern Sie in der Spalte **Priorität** auf der linken Seite die Standardpriorität, um sicherzustellen, dass die Richtlinie in der richtigen Reihenfolge ausgewertet wird.
- Klicken Sie auf **OK**.
  In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich konfiguriert wurde.

Globale Sitzungseinstellungen

Zusätzlich zum oder anstelle des Erstellen von Sitzungsprofilen und -richtlinien können Sie globale Sitzungseinstellungen konfigurieren. Diese Einstellungen steuern die Sitzungskonfiguration, wenn keine explizite Richtlinie sie überschreibt.

So konfigurieren Sie die Sitzungseinstellungen mit der Befehlszeilenschnittstelle

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

```
set tm sessionParameter [-sessTimeout <mins>][-
    defaultAuthorizationAction ( ALLOW | DENY )][-SSO ( ON | OFF )][-
    ssoCredential ( PRIMARY | SECONDARY )][-ssoDomain <string>][-
    httpOnlyCookie ( YES | NO )][-persistentCookie ( ENABLED | DISABLED
    )] [-persistentCookieValidity <minutes>]
<!--NeedCopy-->
```

Beispiel

```
> set tm sessionParameter -sessTimeout 30
  Done
> set tm sessionParameter -defaultAuthorizationAction DENY
  Done
> set tm sessionParameter -SSO ON
  Done
> set tm sessionParameter -ssoCredential PRIMARY
  Done
```



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

So konfigurieren Sie die Sitzungseinstellungen mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr**
2. Klicken Sie im Detailbereich unter **Einstellungen**auf Globale Einstellungen ändern.
3. Geben Sie im Dialogfeld **Globale Sitzungseinstellungen** Werte für die Parameter ein oder wählen Sie sie aus.
   - Sitzungstimeout — sessTimeout
   - Standardautorisierungsaktion — defaultAuthorizationAction
   - Single Sign-On bei Webanwendungen — sso
   - Anmeldeinformationsindex — ssoCredential
   - Single Sign-On-Domäne — ssoDomain
   - HttpOnly Cookie — httpOnlyCookie
   - Persistent Cookie aktivieren — persistentCookie
   - Persistent-Cookie-Gültigkeit (Minuten) — persistentCookieValidity
   - Startseite — home page
4. Klicken Sie auf **OK**.

Verkehrseinstellungen

Wenn Sie formularbasierte oder SAML Single Sign-On (SSO) für Ihre geschützten Anwendungen verwenden, konfigurieren Sie diese Funktion in den Verkehrseinstellungen. SSO ermöglicht es Ihren Benutzern, sich einmal anzumelden, um auf alle geschützten Anwendungen zuzugreifen, anstatt dass sie sich separat anmelden müssen, um auf die einzelnen Anwendungen zuzugreifen.

Formularbasiertes SSO ermöglicht es Ihnen, ein Webformular Ihres eigenen Entwurfs als Anmeldemethode anstelle eines generischen Popup-Fensters zu verwenden. Sie können daher Ihr Firmenlogo und andere Informationen, die Ihre Benutzer möglicherweise sehen sollen, im Anmeldeformular angeben. Mit SAML SSO können Sie eine Citrix ADC Appliance oder eine virtuelle Appliance-Instanz für die Authentifizierung bei einer anderen Citrix ADC-Appliance im Namen von Benutzern konfigurieren, die sich bei der ersten Appliance authentifiziert haben.

Um einen der beiden SSO-Typen zu konfigurieren, erstellen Sie zunächst ein Formular oder ein SAML-SSO-Profil. Als Nächstes erstellen Sie ein Verkehrsprofil und verknüpfen es mit dem SSO-Profil, das Sie erstellt haben. Als Nächstes erstellen Sie eine Richtlinie und verknüpfen sie mit dem Verkehrsprofil. Schließlich binden Sie die Richtlinie global oder an einen virtuellen Authentifizierungsserver, um Ihre Konfiguration in Kraft zu setzen.

Verkehrsprofile

Nachdem Sie mindestens ein Formular oder ein SAML-Profil erstellt haben, müssen Sie als nächstes ein Verkehrsprofil erstellen.

> **Hinweis:**
>
> In dieser Funktion bedeuten die Begriffe “Profil” und “Aktion” dasselbe.

So erstellen Sie mit der Befehlszeilenschnittstelle ein Verkehrsprofil

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add tm trafficAction <name> [-appTimeout <mins>][-SSO ( ON | OFF ) [-
    formSSOAction <string>]][-persistentCookie ( ENABLED | DISABLED )][-
    InitiateLogout ( ON | OFF )]
<!--NeedCopy-->
```

Beispiel

```
add tm trafficAction Traffic-Prof-1  -appTimeout 10 -SSO ON -
    formSSOAction SSO-Prof-1
<!--NeedCopy-->
```

So ändern Sie ein Sitzungsprofil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set tm trafficAction <name> [-appTimeout <mins>] [-SSO ( ON | OFF ) [-
    formSSOAction <string>]] [-persistentCookie ( ENABLED | DISABLED )]
    [-InitiateLogout ( ON | OFF )]
<!--NeedCopy-->
```

Beispiel

```
set tm trafficAction Traffic-Prof-1  -appTimeout 10 -SSO ON -
    formSSOAction SSO-Prof-1
<!--NeedCopy-->
```


So entfernen Sie ein Sitzungsprofil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm tm trafficAction <name>
<!--NeedCopy-->
```

Beispiel

```
rm tm trafficAction Traffic-Prof-1
<!--NeedCopy-->
```

So konfigurieren Sie Datenverkehrsprofile mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Datenverkehr.**
2. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Richtlinien > Traffic.**
3. Klicken Sie im Detailbereich auf die Registerkarte Profile.
4. Führen Sie auf der Registerkarte Profile einen der folgenden Schritte aus:
   - Um ein neues Verkehrsprofil zu erstellen, klicken Sie auf **Hinzufügen.**
   - Um ein vorhandenes Verkehrsprofil zu ändern, wählen Sie das Profil aus, und klicken Sie dann auf **Bearbeiten.**
5. Geben **Sie im Dialogfeld Verkehrsprofil erstellen** oder **Verkehrsprofil konfigurieren** Werte für die Parameter an.
   - Name* — name (Kann für eine zuvor konfigurierte Sitzungsaktion nicht geändert werden.)
   - AppTimeout — appTimeout
   - Single Sign-On — SSO
   - Formular-SSO-Aktion — formSSOAction
   - SAML-SSO-Aktion — samlSSOAction
   - Persistent Cookie aktivieren — persistentCookie
   - Abmeldung initiieren — InitiateLogout
6. Klicken Sie auf **Erstellen** oder **OK**. Das von Ihnen erstellte Verkehrsprofil wird in den Verkehrsrichtlinien, Profilen und je nach Bedarf im Bereich SSO-Profile Formular oder SAML-SSO-Profile angezeigt.

Unterstützung für AAA.USER und AAA.LOGIN Ausdrücke

Der AAA.USER-Ausdruck wird nun implementiert, um die vorhandenen HTTP.REQ.USER-Ausdrücke zu ersetzen. Der AAA.USER-Ausdruck ist anwendbar für den Umgang mit Nicht-HTTP-Datenverkehr

wie Secure Web Gateway (SWG) und dem rollenbasierten Zugriffsmechanismus (RBA). Die AAA.USER-Ausdrücke entsprechen HTTP.REQ.USER-Ausdrücken.

Sie können den Ausdruck bei verschiedenen Aktionen oder Profilkonfigurationen verwenden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add tm trafficAction <name> [SSO (ON|OFF)] [-userExpression <string>]

add tm trafficAction <name> [SSO (ON|OFF)] [-passwdExpression <string>]

<!--NeedCopy-->
```

Beispiel

```
add tm trafficAction tm_act -SSO ON -userExpression ”AAA.USER.NAME”

add tm trafficAction tm_act -SSO ON -userExpression ”AAA.USER.PASSWD”

add tm trafficPolicy tm_pol true tm_act

bind lb vserver lb1 -policyName tm_pol -priority 2
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn Sie HTTP.REQ.USER Ausdruck verwenden, wurde die Warnmeldung HTTP.REQ.USER veraltet. Verwenden Sie stattdessen AAA.USER wird an der Eingabeaufforderung angezeigt.

- **AAA.LOGIN Expression.** Der LOGIN-Ausdruck stellt die Pre-Login dar, die auch als Anmeldeanforderung bezeichnet wird. Die Anmeldeanforderung kann von Citrix Gateway, SAML-IdP oder von der OAuth-Authentifizierung stammen. Der Citrix ADC wird die erforderlichen Attribute aus der Richtlinienkonfiguration abstrahieren. Der AAA.LOGIN-Ausdruck enthält die Attribute, die auf folgender Grundlage abgerufen werden können:
  - **AAA.LOGIN.USERNAME.** Der Benutzername (falls gefunden) wird von der aktuellen Anmeldeanfrage abgerufen. Derselbe Ausdruck, der auf eine Nicht-Login-Anfrage angewendet wird (bestimmt durch eine Authentifizierung, Autorisierung und Überwachung), ergibt eine leere Zeichenfolge.
  - **AAA.LOGIN.PASSWORD.** Das Benutzerkennwort (falls gefunden) wird aus der aktuellen Anmeldeanforderung abgerufen. Der Ausdruck führt zu einer leeren Zeichenfolge, wenn das Kennwort nicht gefunden wird.

  - **AAA.LOGIN.PASSWORD2.** Das zweite Kennwort (falls gefunden) wird aus der Anmeldeanfrage abgerufen.
  - **AAA.LOGIN.DOMAIN.** Die Domäneninformationen werden aus der Anmeldeanfrage abgerufen.
- **AAA.USER.ATTRIBUTE (“#”).** Der Ausdruck wird verwendet, um das Benutzerattribut zu speichern. Hier kann # entweder ein ganzzahliger Wert (zwischen 1 und 16) oder ein Zeichenfolgenwert sein. Sie können diese Indexwerte verwenden, indem Sie den Ausdruck AAA.USER.ATTRIBUTE (“#”) verwenden. Das Authentifizierungs-, Autorisierungs- und Überwachungsmodul sucht das Benutzersitzungsattribut und `AAA.USER.ATTRIBUTE(”##”)` würde die Hash-Tabelle nach diesem bestimmten Attribut abfragen. Wenn beispielsweise `Attributes(”samaccountname”)` festgelegt ist, würde `AAA.USER.ATTRIBUTE(”samaccountname”)` die Hash-Map abfragen und würde den `samaccountname` entsprechenden Wert abrufen.

Verkehrsrichtlinien

Nachdem Sie ein oder mehrere Formular-SSO- und Verkehrsprofile erstellt haben, erstellen Sie Datenverkehrsrichtlinien und binden die Richtlinien dann global oder an einen virtuellen Server für die Datenverkehrsverwaltung, um sie in Kraft zu setzen.

So erstellen Sie eine Verkehrsrichtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add tm trafficPolicy <name> <rule> <action>
2 <!--NeedCopy-->
```

Beispiel

```
1 add tm trafficPolicy Traffic-Pol-1 ”HTTP.REQ.HEADER(”Cookie”).CONTAINS(
     ”login=true”)” Traffic-Prof-1
2 <!--NeedCopy-->
```

So ändern Sie eine Verkehrsrichtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set tm trafficPolicy <name> <rule> <action>
<!--NeedCopy-->
```

Beispiel

```
set tm trafficPolicy Traffic-Pol-1 ”HTTP.REQ.HEADER(”Cookie”).CONTAINS(
   ”login=true”)” Traffic-Prof-1
<!--NeedCopy-->
```

So binden Sie eine Verkehrsrichtlinie global mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind tm global -policyName <string> [-priority <priority>]
<!--NeedCopy-->
```

Beispiel

```
bind tm global -policyName Traffic-Pol-1
<!--NeedCopy-->
```

So binden Sie eine Verkehrsrichtlinie über die Befehlszeilenschnittstelle an einen virtuellen Lastausgleichs- oder Content Switching-Server

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
bind lb vserver <name> -policy <policyName> [-priority <priority>]

bind cs vserver <name> -policy <policyName> [-priority <priority>]
<!--NeedCopy-->
```

Beispiel

```
bind authentication vserver auth-vserver-1 -policyName Traffic-Pol-1 -
   priority 1000
```



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

So heben Sie die Bindung einer global gebundenen Verkehrsrichtlinie mit der Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
unbind tm global -policyName <policyname>
<!--NeedCopy-->
```

Beispiel

```
unbind tm global -policyName Traffic-Pol-1
<!--NeedCopy-->
```

So heben Sie die Bindung einer Verkehrsrichtlinie für einen virtuellen Lastenausgleichs- oder Content Switching-Server über die Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
unbind lb vserver <name> -policy <policyname>

unbind cs vserver <name> -policy <policyname>
<!--NeedCopy-->
```

Beispiel

```
unbind authentication vserver auth-vserver-1 -policyName Traffic-Pol-1
<!--NeedCopy-->
```

So entfernen Sie eine Verkehrsrichtlinie mit der Befehlszeilenschnittstelle

Entbinden Sie zuerst die Sitzungsrichtlinie von global, und geben Sie dann an der Eingabeaufforderung Folgendes ein:


```
rm tm trafficPolicy <name>
<!--NeedCopy-->
```

Beispiel

```
rm tm trafficPolicy Traffic-Pol-1
<!--NeedCopy-->
```

So konfigurieren und binden Sie Verkehrsrichtlinien mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Datenverkehr.**
2. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Richtlinien > Traffic.**
3. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine neue Sitzungsrichtlinie zu erstellen, klicken Sie auf **Hinzufügen.**
   - Um eine vorhandene Sitzungsrichtlinie zu ändern, wählen Sie die Richtlinie aus und klicken Sie dann auf **Bearbeiten.**
4. Geben **Sie im Dialogfeld Verkehrsrichtlinie erstellen** oder **Verkehrsrichtlinie konfigurieren** Werte für die Parameter an.
   - Name* — policyName (Für eine zuvor konfigurierte Sitzungsrichtlinie kann nicht geändert werden.)
   - Profil* — actionName
   - Ausdruck — Regel (Sie geben Ausdrücke ein, indem Sie zuerst den Ausdruckstyp in der Dropdownliste ganz links unter dem Textbereich Ausdruck auswählen und anschließend den Ausdruck direkt in den Ausdruckstextbereich eingeben, oder indem Sie auf Hinzufügen klicken, um das Dialogfeld Ausdruck hinzufügen zu öffnen und die Dropdownlisten in diesem Feld zu verwenden. konstruieren Sie Ihren Ausdruck.)
5. Klicken Sie auf **Erstellen** oder **OK**. Die erstellte Richtlinie wird im Detailbereich der Seite **Sitzungsrichtlinien** und **-profile** angezeigt.

Formular-SSO-Profile

Um formularbasierte SSO zu aktivieren und zu konfigurieren, erstellen Sie zunächst ein SSO-Profil.

> **Hinweis:**
>
> - Formularbasiertes einmaliges Anmelden funktioniert nicht, wenn das Formular so angepasst ist, dass es Javascript enthält.
> - In dieser Funktion bedeuten die Begriffe Profil und Aktion dasselbe.

So erstellen Sie ein Formular-SSO-Profil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add tm formSSOAction <name> -actionURL <URL> -userField <string> -
    passwdField <string> -ssoSuccessRule <expression> [-nameValuePair <
    string>] [-responsesize <positive_integer>][-nvtype ( STATIC |
    DYNAMIC )][-submitMethod ( GET | POST )]

show tm formSSOAction [<name>]
<!--NeedCopy-->
```

Beispiel

```
add tm formSSOAction SSO-Prof-1 -actionURL "/logon.php"
-userField "loginID" -passwdField "passwd"
-nameValuePair "loginID passwd" -responsesize "9096"
-ssoSuccessRule "HTTP.RES.HEADER("Set-Cookie").CONTAINS("LogonID")"
-nvtype STATIC -submitMethod GET
 - sessTimeout 10 -defaultAuthorizationAction ALLOW
<!--NeedCopy-->
```

So ändern Sie eine Formular-SSO mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set tm formSSOAction <name> -actionURL <URL> -userField <string> -
    passwdField <string> -ssoSuccessRule <expression> [-nameValuePair <
    string>] [-responsesize <positive_integer>][-nvtype ( STATIC |
    DYNAMIC )][-submitMethod ( GET | POST )]
<!--NeedCopy-->
```

Beispiel

```
set tm formSSOAction SSO-Prof-1 -actionURL "/logon.php"
-userField "loginID" -passwdField "passwd"
-ssoSuccessRule "HTTP.RES.HEADER("Set-Cookie").CONTAINS("LogonID")"
-nameValuePair "loginID passwd" -responsesize "9096"
-nvtype STATIC -submitMethod GET
```



```
6  - sessTimeout 10 -defaultAuthorizationAction ALLOW
7  <!--NeedCopy-->
```

So entfernen Sie ein Formular-SSO-Profil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1  rm tm formSSOAction <name>
2  <!--NeedCopy-->
```

Beispiel

```
1  rm tm sessionAction SSO-Prof-1
2  <!--NeedCopy-->
```

So konfigurieren Sie Formular-SSO-Profile mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Richtlinien > Datenverkehr**.
2. Klicken Sie im Detailbereich auf die Registerkarte **SSO-Profile Formular** .
3. Führen Sie auf der Registerkarte Formular-SSO-Profile eine der folgenden Aktionen aus:
   - Klicken Sie auf **Hinzufügen**, um ein neues SSO-Profil zu erstellen.
   - Um ein vorhandenes SSO-Profil zu ändern, wählen Sie das Profil aus, und klicken Sie dann auf Bearbeiten.
4. Geben **Sie im Dialogfeld Formular-SSO-Profil erstellen** oder **Formular-SSO-Profil konfigurieren** die Werte für die Parameter an:
   - Name* — name (Kann für eine zuvor konfigurierte Sitzungsaktion nicht geändert werden.)
   - Aktions-URL*—ActionURL
   - Benutzernamenfeld*—userField
   - Kennwortfeld*—passField
   - Ausdruck*—ssoSuccessRule
   - Namenswertpaar—nameValuePair
   - Antwortgröße — responsesize
   - Extraktion — nvtype
   - Submit-Methode — submitMethod
5. Klicken Sie auf **Erstellen** oder **OK**und dann auf **Schließen**. Das von Ihnen erstellte Formular-SSO-Profil wird im Bereich **Verkehrsrichtlinien**, **Profile** und **Form SSO-Profile** angezeigt.

SAML SSO-Profile

Um SAML-basierte SSO zu aktivieren und zu konfigurieren, erstellen Sie zunächst ein SAML-SSO-Profil.

So erstellen Sie ein SAML-SSO-Profil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add tm samlSSOProfile <name> -samlSigningCertName <string> -
    assertionConsumerServiceURL <URL> -relaystateRule <expression> -
    sendPassword (ON | OFF) [-samlIssuerName <string>]
2 <!--NeedCopy-->
```

Beispiel

```
1 add tm samlSSOProfile saml-SSO-Prof-1 -samlSigningCertName "Example,
    Inc."  -assertionConsumerServiceURL "https://service.example.com" -
    relaystateRule "true"  -sendPassword "ON" -samlIssuerName "Example,
    Inc."
2 <!--NeedCopy-->
```

So ändern Sie ein SAML SSO mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set tm samlSSOProfile <name> -samlSigningCertName <string> -
    assertionConsumerServiceURL <URL> -relaystateRule <expression> -
    sendPassword (ON | OFF) [-samlIssuerName <string>]
2 <!--NeedCopy-->
```

Beispiel

```
1 set tm samlSSOProfile saml-SSO-Prof-1 -samlSigningCertName "Example,
    Inc."  -assertionConsumerServiceURL "https://service.example.com" -
    relaystateRule "true"  -sendPassword "ON" -samlIssuerName "Example,
    Inc."
2 <!--NeedCopy-->
```


So entfernen Sie ein SAML-SSO-Profil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm tm samlSSOProfile <name>
<!--NeedCopy-->
```

Beispiel

```
rm tm sessionAction saml-SSO-Prof-1
<!--NeedCopy-->
```

So konfigurieren Sie ein SAML-SSO-Profil mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Richtlinien > Traffic.**
2. Klicken Sie im Detailbereich auf die Registerkarte **SAML-SSO-Profile** .
3. Führen Sie auf der Registerkarte **SAML-SSO-Profile** eine der folgenden Aktionen aus:
   - Um ein neues SAML-SSO-Profil zu erstellen, klicken Sie auf **Hinzufügen.**
   - Um ein vorhandenes SAML-SSO-Profil zu ändern, wählen Sie das Profil aus, und klicken Sie dann auf **OpenEdit**.
4. **Legen Sie im Dialogfeld SAML-SSO-Profile erstellen** oder im Dialogfeld **SAML-SSO-Profile konfigurieren** die folgenden Parameter fest:
   - Namen*
   - Signaturzertifikatsname*
   - ACS-URL*
   - Relay-Zustandsregel*
   - Kennwort senden
   - Name des Ausstellers
5. Klicken Sie auf **Erstellen** oder **OK**und dann auf **Schließen.** Das von Ihnen erstellte SAML-SSO-Profil wird im Bereich Verkehrsrichtlinien, Profile und SAML-SSO-Profile angezeigt.

Sitzungszeitüberschreitung für OWA 2010

Sie können jetzt erzwingen, dass OWA 2010-Verbindungen nach einem bestimmten Zeitraum der Inaktivität Timeout. OWA sendet wiederholte Keepalive-Anforderungen an den Server, um Timeouts zu verhindern. Wenn die Verbindungen geöffnet bleiben, kann das einmalige Anmelden beeinträchtigen.

So zwingen Sie OWA 2010 mit der Befehlszeilenschnittstelle nach einem bestimmten Zeitraum ein Timeout

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
add tm trafficAction <actname> [-forcedTimeout <forcedTimeout> -
    forcedTimeoutVal <mins>]
<!--NeedCopy-->
```

Für <actname> ersetzen Sie einen Namen für Ihre Verkehrsrichtlinie. <mins> Ersetzen Sie für die Anzahl der Minuten, nach denen ein erzwungenes Timeout ausgelöst werden soll. Für <forcedTimeout> ersetzen Sie einen der folgenden Werte:

-**START** — Startet den Timer für erzwungenes Timeout, wenn noch kein Timer gestartet wurde. Wenn ein laufender Timer vorhanden ist, hat keine Wirkung.
-**STOP** — Stoppt einen laufenden Timer. Wenn kein laufender Timer gefunden wird, hat keine Wirkung.
-**RESET** — Startet einen laufenden Timer neu. Wenn kein laufender Timer gefunden wird, startet einen Timer, als ob die START-Option verwendet worden wäre.

```
add tm trafficPolicy <polname> <rule> <actname>
<!--NeedCopy-->
```

<polname>Ersetzen Sie für einen Namen für Ihre Traffic-Richtlinie. Für <rule> ersetzen Sie eine Regel in der Citrix ADC Standardsyntax.

```
bind lb vserver <vservername>  - policyName <name> -priority <number>
<!--NeedCopy-->
```

<vservername> Ersetzen Sie für den Namen des virtuellen Servers für die Authentifizierung, Autorisierung und Überwachung der Datenverkehrsverwaltung. <priority> Ersetzen Sie für eine ganze Zahl, die die Priorität der Richtlinie angibt.

Beispiel

```
add tm trafficAction act-owa2010timeout -forcedTimeout RESET -
    forcedTimeoutVal 10
add tm trafficPolicy pol-owa2010timeout true act-owa2010timeout
bind lb vserver vs-owa2010 -policyName pol-owa2010timeout -priority 10
<!--NeedCopy-->
```


Ratenbegrenzung für Citrix Gateway

March 8, 2022

Mit der Ratenbegrenzungsfunktion für Citrix Gateway können Sie die maximale Last für eine bestimmte Netzwerkeinheit oder virtuelle Entität auf der Citrix Gateway-Appliance definieren. Da das Citrix Gateway-Gerät den gesamten nicht authentifizierten Datenverkehr verbraucht, ist das Gerät häufig Prozessanforderungen mit hoher Geschwindigkeit ausgesetzt. Mit der Ratenbegrenzungsfunktion können Sie das Citrix Gateway Gerät so konfigurieren, dass die Datenverkehrsrate einer Entität überwacht und basierend auf dem Datenverkehr in Echtzeit vorbeugende Maßnahmen ergriffen werden. Weitere Informationen zur Funktionsweise der Ratenbegrenzung in einer Citrix ADC-Appliance finden Sie unter Ratenbegrenzung.

Citrix ADC verfügt über die Funktion zur Begrenzung der Rate, die Back-End-Server mit einer unvorhergesehenen Geschwindigkeit schützt. Da die Funktion für Citrix ADC den nicht authentifizierten Datenverkehr, den Citrix Gateway verarbeitet, nicht bereitstellte, benötigte Citrix Gateway seine eigenen ratenbegrenzenden Funktionen. Dies ist erforderlich, um eine unvorhergesehene Rate von Anfragen aus verschiedenen Quellen zu überprüfen, denen das Citrix Gateway-Gerät ausgesetzt ist. Zum Beispiel nicht authentifizierte/Anmelde-/Steuerungsanfragen und bestimmte APIs, die für Endbenutzer- oder Gerätevalidierungen offengelegt wurden.

Häufige Anwendungsfälle für die Tarifbegrenzung

- Beschränken Sie die Anzahl der Anfragen pro Sekunde von einer URL.
- Trennen Sie eine Verbindung basierend auf Cookies, die auf Anfrage von einem bestimmten Host empfangen wurden, wenn die Anfrage das Ratenlimit überschreitet.
- Beschränken Sie die Anzahl der HTTP-Anfragen, die von demselben Host (mit einer bestimmten Subnetzmaske) eingehen und dieselbe Ziel-IP-Adresse haben.

Konfigurieren der Ratenbegrenzung für Citrix Gateway

Voraussetzungen

Ein konfigurierter virtueller Authentifizierungsserver.

Wichtige Hinweise

- In den Konfigurationsschritten wird ein Sample-Limit Identifier konfiguriert. Dasselbe kann mit allen unterstützten Parametern wie Stream-Selektor, Modus konfiguriert werden. Eine

erschöpfende Beschreibung der Ratenbegrenzungsfunktionen finden Sie unter Ratenbegrenzung.

- Die Richtlinie kann auch wie folgt an einen virtuellen VPN-Server gebunden werden. Sie benötigen einen konfigurierten virtuellen VPN-Server, um die Richtlinien mit dem folgenden Befehl zu binden.

```
bind vpn vserver  -policy denylogin  - pri 1  - type aaa_request
<!--NeedCopy-->
```

- AAA_REQUEST ist ein neu eingeführter Bindepunkt für Responder-Richtlinien. Die an diesem Bindepunkt konfigurierten Richtlinien werden auf alle eingehenden Anforderungen auf dem angegebenen virtuellen Server angewendet. Die Richtlinien werden für den nicht authentifizierten/kontrollierten Verkehr zuerst vor jeder anderen Verarbeitung verarbeitet.
- Das Binden der Richtlinie an den virtuellen Citrix Gateway-Server ermöglicht die Ratenbegrenzung am AAA_REQUEST-Bindpunkt für den gesamten von Citrix Gateway verbrauchten Datenverkehr, einschließlich nicht authentifizierter Anforderungen.
- Durch das Binden der Richtlinie an einen virtuellen Authentifizierungsserver werden die nicht authentifizierten/kontrollierten Anforderungen begrenzt, die den virtuellen Authentifizierungsserver treffen.

Um die Ratenbegrenzung über die Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
add limitIdentifier <limitIdentifier name> -threshold <positive_integer
    > -timeslice <positive_integer> -mode <mode type>
<!--NeedCopy-->
```

Beispiel:

```
add limitIdentifier limit_one_login -threshold 10 -timeslice 4294967290
    -mode REQUEST_RATE
<!--NeedCopy-->
```

```
add responderaction denylogin respondwith  ' "HTTP/1.1 200 OK\r\n\r\n"
    +  "Request is denied due to unusual rate" '
<!--NeedCopy-->
```



```
add responder policy denylogin 'sys.check_limit(”limit_one_login”)'
    denylogin
<!--NeedCopy-->
```

```
bind authentication vserver <vserver name> -policy denylogin  - pri 1  -
    type aaa_request
<!--NeedCopy-->
```

Beispiel:

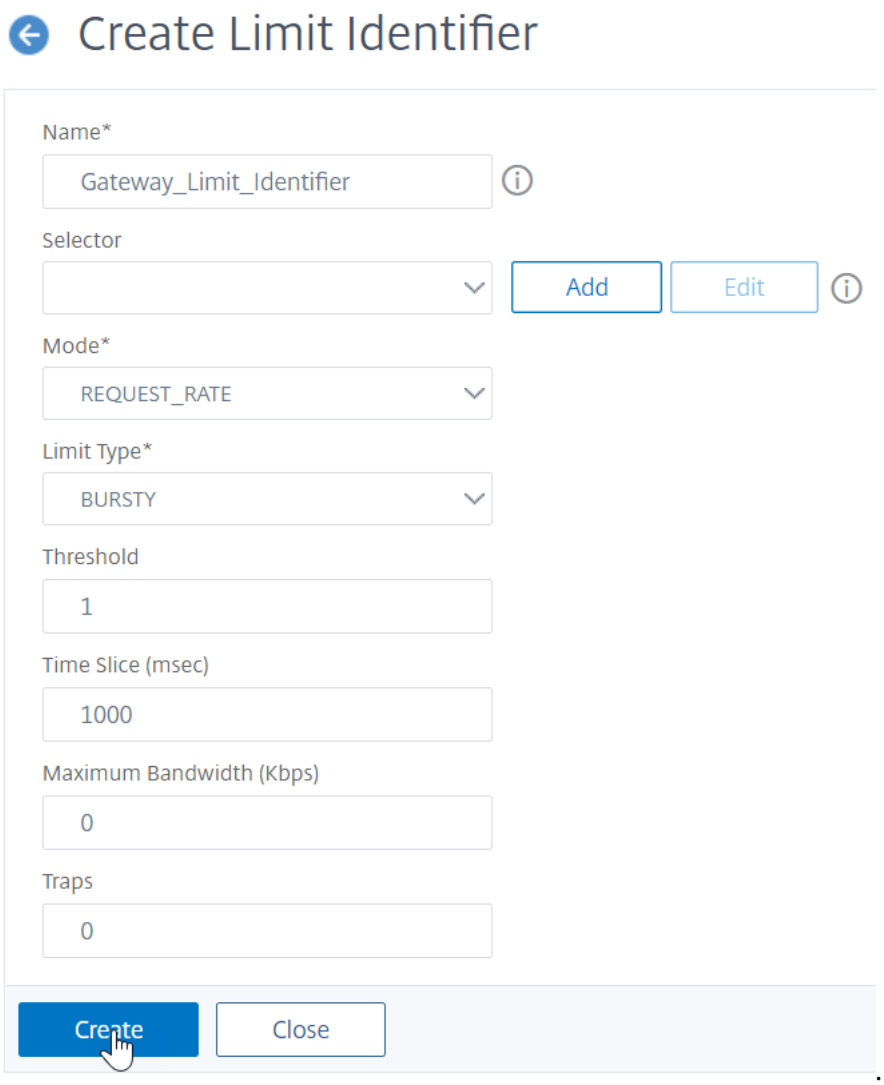
```
bind authentication vserver authvserver -policy denylogin  - pri 1  -
    type aaa_request
<!--NeedCopy-->
```

Beschreibung des Parameters

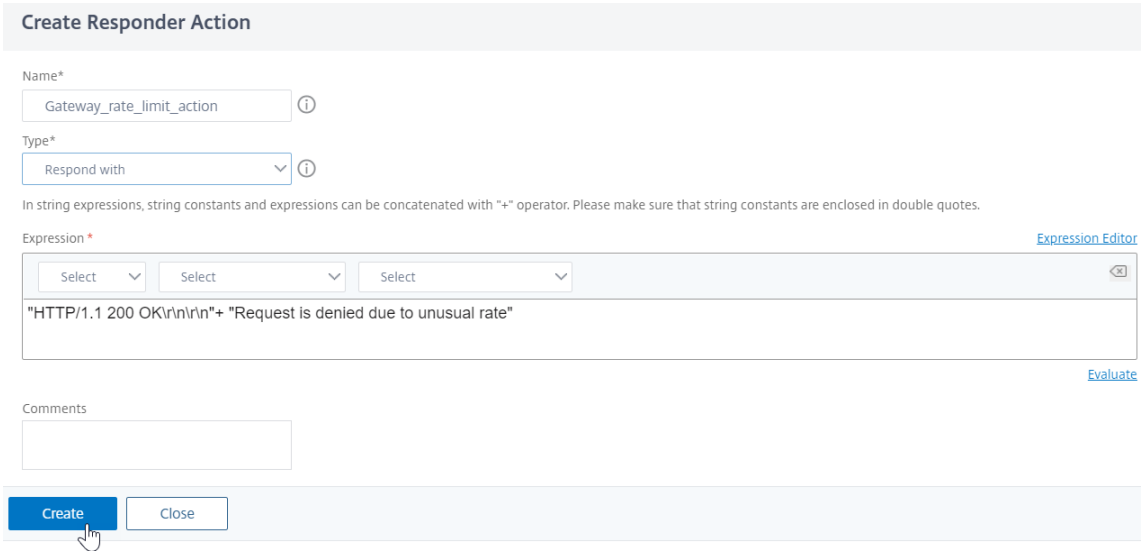
- **LimitIdentifier -** Name für eine Ratenbegrenzungs-ID. Muss mit einem ASCII-Buchstaben oder Unterstrich (_) beginnen und darf nur aus alphanumerischen ASCII-Zeichen oder Unterstrichen bestehen. Reservierte Wörter dürfen nicht verwendet werden. Dies ist ein zwingendes Argument. Maximale Länge: 31
- **Schwellenwert -** Eine maximale Anzahl von Anforderungen, die in der angegebenen Zeitleiste zulässig sind, wenn Anfragen (Modus ist als REQUEST_RATE festgelegt) pro Timeslice verfolgt werden. Wenn Verbindungen (Modus ist als CONNECTION eingestellt) verfolgt werden, ist dies die Gesamtzahl der Verbindungen, die durchgelassen würden. Standardwert: 1 Minimalwert: 1 Maximalwert: 4294967295
- **TimeSlice -** Zeitintervall in Millisekunden, angegeben in Vielfachen von 10, in dem Anfragen verfolgt werden, um zu überprüfen, ob sie den Schwellenwert überschreiten. Das Argument wird nur benötigt, wenn der Modus auf REQUEST_RATE gesetzt ist. Standardwert: 1000 Mindestwert: 10 Maximalwert: 4294967295
- **mode -** Definiert die Art des Traffics, der verfolgt werden soll.
  - REQUEST_RATE - Verfolgt Anforderungen/Timeslice.
  - CONNECTION - Verfolgt aktive Transaktionen.

So konfigurieren Sie die Ratenbegrenzung über die Citrix ADC-GUI:

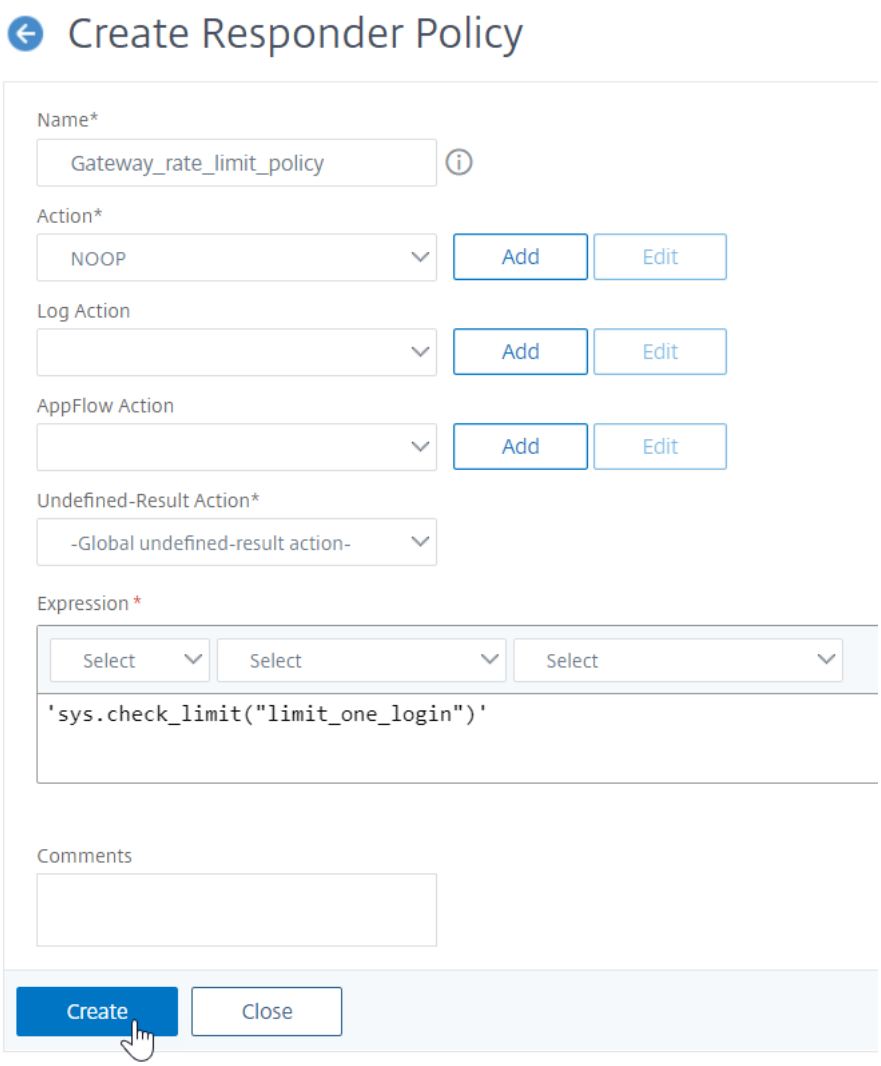
1. Navigieren Sie zu **AppExpert > Ratenbegrenzung > Limitkennungen**, klicken Sie auf **Hinzufügen**, und geben Sie die entsprechenden Details an, wie im CLI-Abschnitt angegeben.



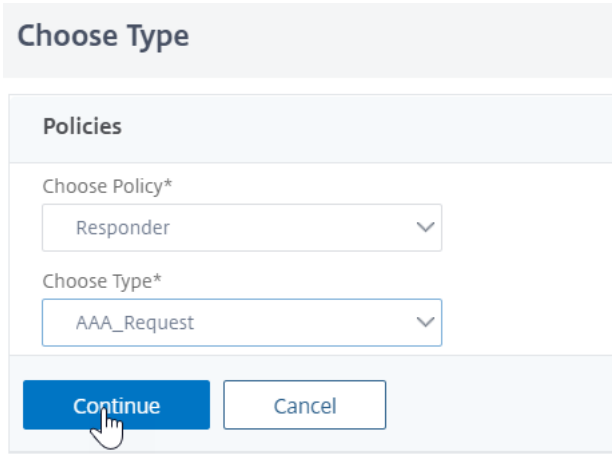
2. Navigieren Sie zu **AppExpert>Responder>Richtlinien**. Klicken Sie auf der Seite **Responder-Richtlinien** auf **Hinzufügen**.
3. Erstellen Sie auf der Seite **Responder Policy erstellen** eine Responder-Richtlinie mit einer Responder Action, die über die Limit-ID verfügt.
4. Um eine Responder Action zu erstellen, klicken Sie neben **Aktion** auf **Hinzufügen** und geben Sie einen Namen für die Responder Action ein.
5. Wählen Sie im Dropdown-Menü den Typ als **Antworten mit** aus, geben Sie den folgenden Ausdruck an: “HTTP/1.1 200 OK\ r\ n\ r\ n”+ “Anforderung wird aufgrund ungewöhnlicher Rate verweigert”, und klicken Sie auf **Erstellen**.



6. Um eine Responder Policy zu **erstellen, geben Sie auf der Seite Responder Policy** erstellen einen Namen für die Responder-Richtlinie ein, geben Sie den folgenden Ausdruck an: ‘sys.check_limit (“limit_one_login”) ‘, und klicken Sie auf **Erstellen**.



7. Binden Sie die Responder Policy an den virtuellen Authentifizierungsserver.
   - Gehen Sie zu **Sicherheit> AAA-Anwendungsverkehr> Virtueller Server**.
   - Wählen Sie den virtuellen Server aus.
   - Fügen Sie eine Richtlinie hinzu.
   - Wählen Sie die Responder Policy aus, die Sie an den Server binden möchten, und legen Sie die Priorität fest.
   - Wählen Sie den Typ als **AAA-REQUEST** und klicken Sie auf **Weiter**.



> **Hinweis:** Sie können die Ratenbegrenzung auch am AAA_REQUEST-Bindpunkt für den virtuellen VPN-Server aktivieren.

Konfiguration für die gängigen Anwendungsfälle zum Anwenden von Ratenbegrenzung auf Citrix Gateway

Im Folgenden sind die Beispiele für Befehle zum Konfigurieren allgemeiner Anwendungsfälle aufgeführt.

- Beschränken Sie die Anzahl der Anfragen pro Sekunde von einer URL.

```
1  add stream selector ipStreamSelector http.req.url  “client.ip.src
       ”
2
3  add ns limitIdentifier ipLimitIdentifier  -threshold 4  -
       timeslice 1000  -mode request_rate  -limitType smooth  -
       selectorName ip StreamSelector
4
5  add responder policy ipLimitResponderPolicy  “http.req.url.
       contains(\” myasp.asp\” ) && sys.check_limit(\”
       ipLimitIdentifier\” )”  myWebSiteRedirectAction
6
7  bind authentication virtual server authvserver -policy denylogin
       -pri 1  -type aaa_request
8  <!--NeedCopy-->
```

- Lösen Sie eine Verbindung basierend auf Cookies, die auf Anfrage von www.yourcompany.com erhalten wurden, wenn die Anfrage das Tariflimit überschreitet.


```
add stream selector cacheStreamSelector  “http.req.cookie.value(\” mycookie\” )”  “client.ip.src.subnet(24)”

add ns limitIdentifier myLimitIdentifier  -Threshold 2  -timeSlice 3000  -selectorName reqCookieStreamSelector

add responder action sendRedirectURL redirect `”http://www.mycompany.com”` + http.req.url'  -bypassSafetyCheck Yes

add responder policy rateLimitCookiePolicy

 “http.req.url.contains(\www.yourcompany.com) && sys.check_limit(\” myLimitIdentifier\” )”  sendRedirectUrl

<!--NeedCopy-->
```

- Beschränken Sie die Anzahl der HTTP-Anfragen, die vom selben Host (mit einer Subnetzmaske von 32) eingehen und dieselbe Ziel-IP-Adresse haben.

```
add stream selector ipv6_sel  “CLIENT.IPv6.src.subnet(32)” CLIENT.IPv6.dst

add ns limitIdentifier ipv6_id  -imeSlice 20000  -selectorName ipv6_sel

add lb vserver ipv6_vip HTTP 3ffe:: 209 80  -persistenceType NONE  -cltTime

add responder action redirect_page redirect  “\” `http://redirectpage.com/\” ”`

add responder policy ipv6_resp_pol  “SYS.CHECK_LIMIT(\” ipv6_id\” )”  redirect_page

bind responder global ipv6_resp_pol 5 END  -type DEFAULT
<!--NeedCopy-->
```

Autorisieren des Benutzerzugriffs auf Anwendungsressourcen

October 5, 2021

Sie können die Ressourcen steuern, auf die ein authentifizierter Benutzer innerhalb einer Anwendung zugreifen kann.

Ordnen Sie dazu jedem Benutzer eine Autorisierungsrichtlinie zu, entweder einzeln oder durch Zuordnen der Richtlinie zu einer Gruppe von Benutzern. Die Autorisierungsrichtlinie muss Folgendes angeben:

- **Regel.** Die Ressource, auf die der Zugriff autorisiert werden muss. Dies kann mit einfachen oder erweiterten Ausdrücken angegeben werden.
- **Aktion.** Gibt an, ob der Zugriff auf die Ressource zulässig oder verweigert werden muss.

Standardmäßig wird der Zugriff auf alle Ressourcen innerhalb einer Anwendung allen Benutzern **verweigert**. Sie können diese Standardautorisierungsaktion jedoch ändern, um Zugriff für alle Benutzer zu **erlauben** (indem Sie die Sitzungsparameter im Sitzungsprofil festlegen oder die globalen Sitzungsparameter festlegen).

> **Warnung**
>
> Zur optimalen Sicherheit empfiehlt Citrix, die Standardautorisierungsaktion von DENY in ALLOW nicht zu ändern. Stattdessen wird empfohlen, spezifische Autorisierungsrichtlinien für Benutzer zu erstellen, die Zugriff auf bestimmte Ressourcen benötigen.

So konfigurieren Sie die Autorisierung mit der CLI

1. Konfigurieren Sie die Autorisierungsrichtlinie.

   ns-cli-prompt> **add authorization policy <name> <rule> <action>**

2. Ordnen Sie die Richtlinie dem entsprechenden Benutzer oder der entsprechenden Gruppe zu.
   - Binden Sie die Richtlinie an einen bestimmten Benutzer.

     ns-cli-prompt> **bind aaa user <username> -policy** <policyname>
   - Binden Sie die Richtlinie an eine bestimmte Gruppe.

     ns-cli-prompt> **bind aaa group <groupName> -policy** <policyname>

So konfigurieren Sie die Autorisierung mit der GUI (Registerkarte Konfiguration)

1. Erstellen Sie die Autorisierungsrichtlinie.

   Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Richtlinien > Autorisierung**, klicken Sie auf **Hinzufügen**und definieren Sie die Richtlinie nach Bedarf.

2. Ordnen Sie die Richtlinie dem entsprechenden Benutzer oder der entsprechenden Gruppe zu.

Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Benutzer** oder **Gruppen**, und bearbeiten Sie den entsprechenden Benutzer oder die Gruppe, um ihn der Autorisierungsrichtlinie zuzuordnen.

Beispielautorisierungskonfigurationen

Im Folgenden finden Sie einige Beispielkonfigurationen, um den Benutzerzugriff auf einige Anwendungsressourcen zu autorisieren. Beachten Sie, dass dies CLI-Befehle sind. Sie können ähnliche Konfigurationen mit der GUI durchführen, obwohl Sie den Ausdruck nicht in Anführungszeichen () einschließen dürfen.

- `add authorization policy authzpol1 ”HTTP.REQ.URL.SUFFIX.EQ(\”gif\”)” ALLOW<!--NeedCopy-->`
- `bind aaa user user1 -policy authzpol1<!--NeedCopy-->`
- `add authorization policy authzpol2 ”HTTP.REQ.URL.SUFFIX.EQ(\”png\”)” DENY<!--NeedCopy-->`
- `bind aaa group group1 -policy authzpol2<!--NeedCopy-->`

Audit authentifizierte Sitzungen

October 5, 2021

Sie können die Citrix ADC Appliance so konfigurieren, dass alle Ereignisse protokolliert werden, die in einer authentifizierten Sitzung ausgelöst werden. Mithilfe dieser Informationen können Sie Status- und Statusinformationen überwachen, um die Historie für Benutzer in chronologischer Reihenfolge anzuzeigen.

Definieren Sie dazu eine Überwachungsrichtlinie, die Folgendes angibt:

- **Protokolltyp.** Die Protokolle können remote (syslog) oder lokal auf der Citrix ADC Appliance (nslog) gespeichert werden.
- **Regel.** Die Bedingungen, unter denen die Protokolle gespeichert werden.
- **Aktion.** Details des Protokollservers und weitere Details zum Erstellen der Protokolleinträge.

Diese Überwachungsrichtlinie kann auf verschiedenen Ebenen konfiguriert werden: Benutzerebene, Gruppenebene, Authentifizierung, Autorisierung und Überwachung virtueller Server sowie globale Systemebene. Die auf Benutzerebene konfigurierten Richtlinien haben die höchste Priorität.

> **Hinweis:**
>
> In diesem Thema werden die Schritte zur Verwendung von syslog beschrieben. Nehmen Sie

> notwendige Änderungen vor, um nslog zu verwenden.

So konfigurieren Sie die Syslog-Überwachung mit der CLI

1. Konfigurieren Sie den Überwachungsserver mit den entsprechenden Protokolleinstellungen.

   ns-cli-prompt> **add audit syslogAction <name> <serverIP> ...**

2. Konfigurieren Sie die Überwachungsrichtlinie, indem Sie den Überwachungsserver zuordnen.

   ns-cli-prompt> **add audit syslogPolicy <name> <rule> <action>**

3. Ordnen Sie die Überwachungsrichtlinie einer der folgenden Entitäten zu:

   - Binden Sie die Richtlinie an einen bestimmten Benutzer.

     ns-cli-prompt> **bind aaa user <userName>-policy** <policyname> …

   - Binden Sie die Richtlinie an eine bestimmte Gruppe.

     ns-cli-prompt> **bind aaa group <groupName>-policy** <policyname> …

   - Binden Sie die Richtlinie an einen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver.

     ns-cli-prompt> **bind authentication vserver <name> -policy** <policyname> …

   - Binden Sie die Richtlinie global an die Citrix ADC Appliance.

     ns-cli-prompt> **bind tm global -policyName** <policyname> …

So konfigurieren Sie die Syslog-Auditing mit der GUI (Registerkarte Konfiguration)

1. Konfigurieren Sie den Überwachungsserver und die Richtlinie.

   Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Richtlinien > Überwachung > Syslog**, und konfigurieren Sie den Server und die Richtlinie in den entsprechenden Registerkarten.

2. Ordnen Sie die Richtlinie einer der folgenden Punkte zu:

   - Binden Sie die Richtlinie an einen bestimmten Benutzer.

     Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Benutzer**, und ordnen Sie die Autorisierungsrichtlinie dem relevanten Benutzer zu.

   - Binden Sie die Richtlinie an eine bestimmte Gruppe.

     Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Gruppen**, und ordnen Sie die Autorisierungsrichtlinie der entsprechenden Gruppe zu.

- Binden Sie die Richtlinie an einen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver.

  Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Virtuelle Server**, und ordnen Sie die Autorisierungsrichtlinie dem relevanten virtuellen Server zu.

- Binden Sie die Richtlinie global an die Citrix ADC Appliance.

  Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Richtlinien > Überwachung > Syslog** oder **Nslog**, wählen Sie die Autorisierungsrichtlinie aus und klicken Sie auf **Aktion > Globale Bindungen**, um die Richtlinie global zu binden.

Citrix ADC als Active Directory Verbunddienste-Proxy

February 24, 2022

Active Directory Verbunddienste (ADFS) sind ein Microsoft-Dienst, der SSO (Single Sign-On) für Active Directory-authentifizierte Clients auf Ressourcen außerhalb des Enterprise-Rechenzentrums ermöglicht. Eine ADFS-Serverfarm ermöglicht internen Benutzern den Zugriff auf externe Cloud-gehostete Dienste. Aber in dem Moment, in dem externe Benutzer in den Mix gebracht werden, müssen die externen Benutzer eine Möglichkeit erhalten, Remote-Verbindung herzustellen und auf cloudbasierte Dienste über Federated Identity zuzugreifen. Die meisten Unternehmen bevorzugen es nicht, den ADFS-Server in der DMZ verfügbar zu halten. Daher spielt ADFS-Proxy eine wichtige Rolle bei der Remotebenutzerkonnektivität und dem Anwendungszugriff.

Seit mehr als einem Jahrzehnt spielt die Citrix ADC Appliance ähnliche Rollen wie Remotebenutzerkonnektivität und Anwendungszugriff. Citrix ADC Appliance wird zur bevorzugten Lösung, die als ADFS-Proxy für die Unterstützung einer neuen ADFS-Implementierung verwendet werden kann, um die folgenden Dienste zu ermöglichen:

- Sichere Konnektivität.
- Authentifizierung und Behandlung von Federated Identity.

Weitere Informationen über Citrix ADC als SAML-IdP finden Sie unter Citrix ADC as a SAML IdP.

Vorteile des ADFS-Proxy

- Reduziert den Platzbedarf in DMZ, um den Bedarf der meisten Unternehmen gerecht zu werden.
- Bietet eine SSO-Erfahrung für Endbenutzer.
- Unterstützt umfassende Methoden für die Vorauthentifizierung und ermöglicht die Multifaktor-Authentifizierung.
- Unterstützt sowohl aktive als auch passive Clients.

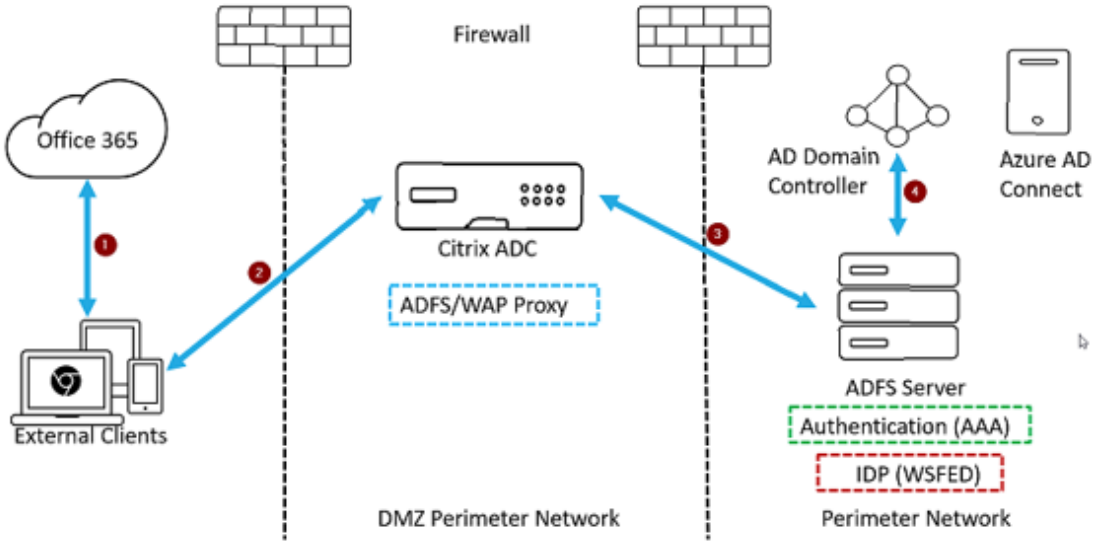
Voraussetzungen für die Verwendung von Citrix ADC als ADFS-Proxy

Bevor Sie die Citrix ADC Appliance als ADFS-Proxy konfigurieren, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind.

- Eine Citrix ADC Appliance mit 12.1-Build oder höher.
- Domänen-ADFS-Server.
- Domänen-SSL-Zertifikat.
- Virtuelle IP für den virtuellen Content Switching-Server.
- Aktivieren Sie Lastenausgleich, SSL-Offload, Content Switching, Umschreiben und Authentifizierungs-, Autorisierungs- und Überwachungsfunktionen für den Datenverkehr auf der Citrix ADC Appliance.

Konfigurieren der Citrix ADC Appliance als ADFS-Proxy

Um diesen Anwendungsfall zu erreichen, konfigurieren Sie Citrix ADC als ADFS-Proxy in der DMZ-Zone. Der ADFS-Server wird zusammen mit dem AD-Domänencontroller im Back-End konfiguriert.



1. Eine Clientanforderung für den Zugriff auf Microsoft Office365 wird an Citrix ADC umgeleitet, der als ADFS-Proxy bereitgestellt wird.
2. Die Anmeldeinformationen des Benutzers werden an den ADFS-Server übergeben.
3. ADFS-Server authentifiziert die Anmeldeinformationen mit lokalen AD der Domäne.
4. ADFS-Server nach erfolgreicher Validierung der Anmeldeinformationen mit AD generiert ein Token, das an Microsoft Office365 für die Einrichtung der Sitzung übergeben wird.

Im Folgenden werden die High-Level-Schritte beschrieben, die bei der Konfiguration der Citrix ADC Appliance erforderlich sind, bevor Sie als ADFS-Proxy konfigurieren.

Geben Sie an der Citrix ADC Eingabeaufforderung die folgenden Befehle ein:

1. Erstellen Sie ein SSL-Profil für das Back-End und aktivieren Sie SNI im SSL-Profil. Deaktivieren Sie SSLv3/TLS1.

   ```
   add ssl profile <new SSL profile> -sniEnable ENABLED -ssl3 DISABLED -
   tls1 DISABLED -commonName <FQDN of ADFS>
   ```

2. Deaktivieren Sie SSLv3/TLS1 für den Dienst.

   ```
   set ssl service <adfs service name> -sslProfile <SSL profile created in
    the above step>
   ```

3. Aktivieren Sie die SNI-Erweiterung für Back-End-Server-Handshakes.

   - `set vpn parameter -backendServerSni ENABLED`
   - `set ssl parameter -denySSLReneg NONSECURE`

Konfigurieren der Citrix ADC Appliance als ADFS-Proxy mit der CLI

Die folgenden Abschnitte werden nach der Anforderung für die Ausführung der Konfigurationsschritte kategorisiert.

So konfigurieren Sie den ADFS-Dienst

1. Konfigurieren Sie den ADFS-Dienst auf Citrix ADC für ADFS-Server.

   ```
   add service <Domain_ADFS_Service> <ADFS Server IP> SSL 443 -gslb NONE -
   maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF
   -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
   ```

   Beispiel

   add service CTXTEST_ADFS_Service 1.1.1.1 SSL 443 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO

2. Konfigurieren Sie den FQDN für den virtuellen Content Switching-Server und aktivieren Sie SNI.

   ```
   set ssl service <Domain_ADFS_Service> -SNIEnable ENABLED -commonName <
   sts.domain.com>
   ```

   Beispiel

   set ssl service CTXTEST_ADFS_Service -SNIEnable ENABLED -commonName sts.ctxtest.com

So konfigurieren Sie den virtuellen ADFS-Server für Lastenausgleich

> **Wichtig**
>
> Domänen-SSL-Zertifikat (SSL_CERT) ist für den sicheren Datenverkehr erforderlich.

1. Konfigurieren Sie den virtuellen ADFS-Server für Lastenausgleich.

   ```
   add lb vserver <Domain_ADFS_LBVS> SSL <IP_address> -persistenceType
   NONE -cltTimeout 180
   ```

   Beispiel

   ```
   add lb vserver CTXTEST_ADFS_LBVS SSL 192.168.1.0 -persistenceType NONE
   -cltTimeout 180
   ```

2. Binden Sie den ADFS-Lastenausgleichsserver an den ADFS-Dienst.

   ```
   bind lb vserver <Domain_ADFS_LBVS> <Domain_ADFS_Service>
   ```

   Beispiel

   ```
   bind lb vserver CTXTEST_ADFS_LBVS CTXTEST_ADFS_Service
   ```

3. Binden Sie ein virtuelles SSL-Server-Zertifikatschlüsselpaar.

   ```
   bind ssl vserver <Domain_ADFS_LBVS> -certkeyName <SSL_CERT>
   ```

   Beispiel

   ```
   bind ssl vserver CTXTEST_ADFS_LBVS -certkeyName ctxtest_newcert_2019
   ```

So konfigurieren Sie den virtuellen Content Switching-Server für die Domäne

> **Hinweis:**
>
> Eine freie virtuelle IP (z. B. 2.2.2.2), die per NAT einer öffentlichen IP zugewiesen wird, ist für den virtuellen Content Switching-Server erforderlich. Es muss sowohl für den externen als auch für den internen Datenverkehr erreichbar sein.

1. Erstellen Sie einen virtuellen Content Switching-Server mit kostenlosem VIP.

   ```
   add cs vserver <Domain_CSVS> SSL <FREE VIP> 443 -cltTimeout 180 -
   persistenceType NONE
   ```

   Beispiel

   ```
   add cs vserver CTXTEST_CSVS SSL 2.2.2.2 443 -cltTimeout 180 -persistenceType
    NONE
   ```

2. Binden Sie den virtuellen Content Switching-Server an den virtuellen Lastausgleichsserver.

   ```
   bind cs vserver <Domain_CSVS> -lbvserver <Domain_ADFS_LBVS>
   ```

   Beispiel

- `bind cs vserver CTXTEST_CSVS -lbvserver CTXTEST_ADFS_LBVS`
- `set ssl vserver CTXTEST_CSVS -sessReuse DISABLED`

3. Binden Sie ein virtuelles SSL-Server-Zertifikatschlüsselpaar.

   ```
   bind ssl vserver <Domain_CSVS> -certkeyName <SSL_CERT>
   ```

   Beispiel

   ```
   bind ssl vserver CTXTEST_CSVS -certkeyName ctxtest_newcert_2019
   ```

Unterstützte Protokolle

Die von Microsoft bereitgestellten Protokolle spielen eine wichtige Rolle bei der Integration mit Citrix ADC Appliance. Citrix ADC als ADFS-Proxy unterstützt die folgenden Protokolle:

- **WS-Verbund**. Weitere Informationen finden Sie unter Protokoll des Web Services Federation.
- **ADFSPIP**. Weitere Informationen finden Sie unter Compliance des Active Directory-Verbunddienst-Proxy Integration Protocol

> **Hinweis:**
>
> Die Citrix ADC Appliance unterstützt keine Gerätezertifikatsauthentifizierung, wenn sie als ADFS-Proxy bereitgestellt wird.

Web Services Federation Protokoll

May 10, 2022

Web Services Federation (WS-Federation) ist ein Identitätsprotokoll, das es einem Security Token Service (STS) in einer Vertrauensdomäne ermöglicht, Authentifizierungsinformationen an einen STS in einer anderen Vertrauensdomäne bereitzustellen, wenn eine Vertrauensbeziehung zwischen den beiden Domänen besteht.

Vorteile von WS-Federation

WS-Federation unterstützt sowohl aktive als auch passive Clients, während SAML IdP nur passive Clients unterstützt.

- Aktive Clients sind native Microsoft-Clients wie Outlook- und Office-Clients (Word, PowerPoint, Excel und OneNote).
- Passive Clients sind browserbasierte Clients wie Google Chrome, Mozilla Firefox und Internet Explorer.

Voraussetzungen für die Verwendung von Citrix ADC als WS-Federation

Bevor Sie die Citrix ADC Appliance als ADFS-Proxy konfigurieren, überprüfen Sie Folgendes:

- Active Directory
- Domain-SSL-Zertifikat.
- Das Citrix ADC SSL-Zertifikat und das ADFS-Tokensignaturzertifikat auf dem ADFS-Server müssen identisch sein.

> **Wichtig**
>
> SAML IdP ist jetzt in der Lage, das WS-Federation-Protokoll zu verarbeiten. Um den WS-Federation IdP zu konfigurieren, müssen Sie daher den SAML-IdP tatsächlich konfigurieren. Sie sehen keine Benutzeroberfläche, in der WS-Federation explizit erwähnt wird.

Von Citrix ADC unterstützte Funktionen bei Konfiguration als ADFS-Proxy und WS-Federation IdP

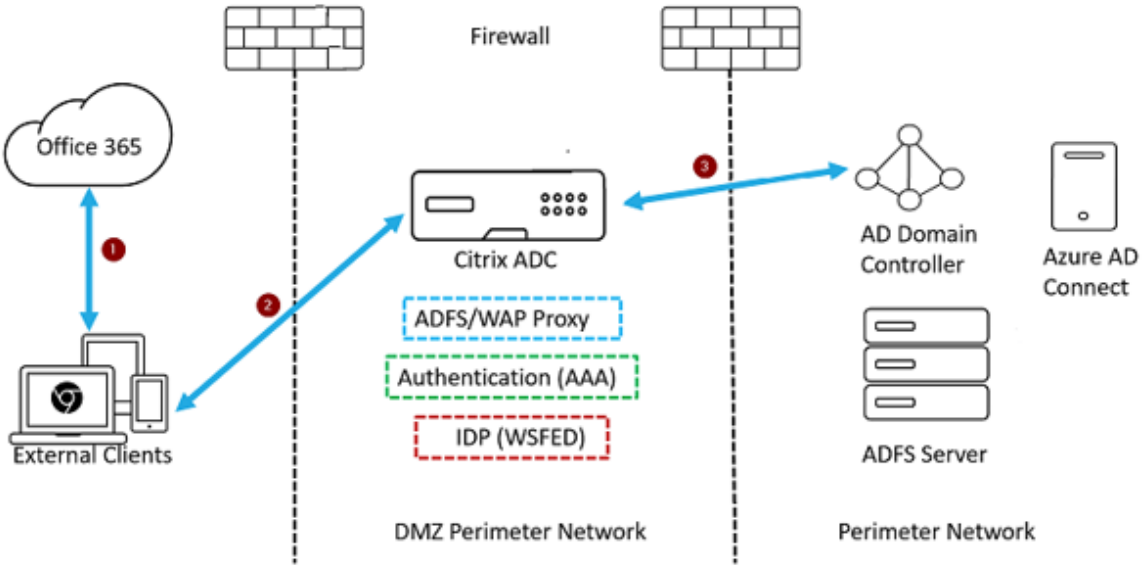
In der folgenden Tabelle sind die Funktionen aufgeführt, die von der Citrix ADC Appliance unterstützt werden, wenn sie als ADFS-Proxy und WS-Federation IdP konfiguriert

Funktionen	Citrix ADC Appliance als ADFS-Proxy konfigurieren	Citrix ADC als WS-Federation IdP	Citrix ADC als ADFSPIP
Lastausgleich	Ja	Ja	Ja
SSL Kündigung	Ja	Ja	Ja
Ratenbegrenzung	Ja	Ja	Ja
Konsolidierung (reduziert den Platzbedarf des DMZ-Servers und spart öffentliche IP)	Ja	Ja	Ja
Webanwendungs-Firewall (WAF)	Ja	Ja	Ja
Authentication Offload auf Citrix ADC Appliance	Ja	Ja (aktive und passive Clients)	Ja
Single Sign-On (SSO)	Ja	Ja (aktive und passive Clients)	Ja

Funktionen	Citrix ADC Appliance als ADFS-Proxy konfigurieren	Citrix ADC als WS-Federation IdP	Citrix ADC als ADFSPIP
Mehrstufige Authentifizierung (nFactor)	Nein	Ja (aktive und passive Clients)	Ja
Azure Multifaktor-Authentifizierung	Nein	Ja (aktive und passive Clients)	Ja
ADFS-Serverfarm kann vermieden werden	Nein	Ja	Ja

Citrix ADC Appliance als WS-Federation IdP konfigurieren

Konfigurieren Sie Citrix ADC als WS-Federation IdP (SAML IdP) in einer DMZ-Zone. Der ADFS-Server wird zusammen mit dem AD-Domänencontroller im Backend konfiguriert.



1. Die Client-Anfrage an Microsoft Office365 wird an die Citrix ADC Appliance umgeleitet.
2. Der Benutzer gibt die Anmeldeinformationen für die Multifaktor-Authentifizierung ein.
3. Citrix ADC validiert die Anmeldeinformationen mit AD und generiert nativ ein Token auf der Citrix ADC Appliance. Die Anmeldeinformationen werden für den Zugriff an Office365 weitergegeben.

> **Hinweis**
>
> Die Unterstützung von WS-Federation IdP erfolgt im Vergleich zum F5 Networks Load Balancer nativ über die Citrix ADC Appliance.

Konfigurieren Sie die Citrix ADC Appliance mit der CLI als WS-Federation IdP (SAML IdP)

Die folgenden Abschnitte sind basierend auf den Anforderungen zum Abschließen der Konfigurationsschritte kategorisiert.

So konfigurieren Sie die LDAP-Authentifizierung und fügen Richtlinien hinzu

> **Wichtig**
>
> Damit Domänenbenutzer sich mit ihren Unternehmens-E-Mail-Adressen an der Citrix ADC Appliance anmelden können, müssen Sie Folgendes konfigurieren:

- Konfigurieren Sie den LDAP-Authentifizierungsserver und die Richtlinie auf der Citrix ADC Appliance.
- Binden Sie es an Ihre virtuelle Authentifizierungs-, Autorisierungs- und Auditing-IP-Adresse (die Verwendung einer vorhandenen LDAP-Konfiguration wird ebenfalls unterstützt).

```
1 add authentication ldapAction <Domain_LDAP_Action> -serverIP <Active
     Directory IP> -serverPort 636 -ldapBase "cn=Users,dc=domain,dc=com"
     -ldapBindDn "cn=administrator,cn=Users,dc=domain,dc=com" -
     ldapBindDnPassword <administrator password> -encrypted -
     encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName
      memberOf -subAttributeName cn -secType SSL -ssoNameAttribute
     UserPrincipalName -followReferrals ON -Attribute1 mail -Attribute2
     objectGUID
2
3 add authentication Policy <Domain_LDAP_Policy> -rule true -action <
     Domain_LDAP_Action>
4 <!--NeedCopy-->
```

Beispiel

```
1 add authentication ldapAction CTXTEST_LDAP_Action -serverIP 3.3.3.3 -
     serverPort 636 -ldapBase "cn=Users,dc=ctxtest,dc=com" -ldapBindDn "
     cn=administrator,cn=Users,dc=ctxtest,dc=com" -ldapBindDnPassword
     xxxxxxxxxxx -encrypted -encryptmethod ENCMTHD_3 -ldapLoginName
     sAMAccountName -groupAttrName memberOf -subAttributeName cn -secType
```



```
        SSL -ssoNameAttribute UserPrincipalName -followReferrals ON -
    Attribute1 mail -Attribute2 objectGUID
2
3 add authentication Policy CTXTEST_LDAP_Policy -rule true -action
    CTXTEST_LDAP_Action
4 <!--NeedCopy-->
```

So konfigurieren Sie Citrix ADC als WS-Federation IdP oder SAML IdP

Erstellen Sie eine WS-Federation IdP-Aktion (SAML IdP) und Richtlinie für die Token-Generierung Binden Sie es später an den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver.

```
1 add authentication samlIdPProfile <Domain_SAMLIDP_Profile> -
    samlIdPCertName <SSL_CERT> -assertionConsumerServiceURL "https://
    login.microsoftonline.com/login.srf" -samlIssuerName <Issuer Name
    for Office 365 in ADFS Server> -rejectUnsignedRequests OFF -audience
     urn:federation:MicrosoftOnline -NameIDFormat persistent -NameIDExpr
     "HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE" -Attribute1 IDPEmail -
    Attribute1Expr "HTTP.REQ.USER.ATTRIBUTE(1)"
2
3 add authentication samlIdPPolicy <Domain_SAMLIDP_Policy> -rule "HTTP.
    REQ.HEADER("referer").CONTAINS("microsoft") || true" -action <
    Domain_SAMLIDP_Profile>
4 <!--NeedCopy-->
```

Beispiel

```
1 add authentication samlIdPProfile CTXTEST_SAMLIDP_Profile -
    samlIdPCertName ctxtest_newcert_2019 -assertionConsumerServiceURL "
    https://login.microsoftonline.com/login.srf" -samlIssuerName "http
    ://ctxtest.com/adfs/services/trust/" -rejectUnsignedRequests OFF -
    audience urn:federation:MicrosoftOnline -NameIDFormat persistent -
    NameIDExpr "HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE" -Attribute1
    IDPEmail -Attribute1Expr "HTTP.REQ.USER.ATTRIBUTE(1)"
2
3 add authentication samlIdPPolicy CTXTEST_SAMLIDP_Policy -rule "HTTP.REQ
    .HEADER("referer").CONTAINS("microsoft") || true" -action
    CTXTEST_SAMLIDP_Profile
4 <!--NeedCopy-->
```


So konfigurieren Sie einen virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver zur Authentifizierung der Mitarbeiter, die sich mit Unternehmensanmeldeinformationen bei Office365 anmelden

```
add authentication vserver <Domain_AAA_VS> SSL <IP_address>`
<!--NeedCopy-->
```

Beispiel

```
add authentication vserver CTXTEST_AAA_VS SSL 192.168.1.0

bind authentication vserver CTXTEST_AAA_VS -portaltheme RfWebUI
<!--NeedCopy-->
```

So binden Sie den virtuellen Authentifizierungsserver und die Richtlinie

```
bind authentication vserver <Domain_AAA_VS> -policy <
    Domain_SAMLIDP_Policy> -priority 100 -gotoPriorityExpression NEXT

bind authentication vserver <Domain_AAA_VS> -policy <Domain_LDAP_Policy
    > -priority 100 -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

Beispiel

```
bind authentication vserver CTXTEST_AAA_VS -policy
    CTXTEST_SAMLIDP_Policy -priority 100 -gotoPriorityExpression NEXT

bind authentication vserver CTXTEST_AAA_VS -policy CTXTEST_LDAP_Policy
    -priority 100 -gotoPriorityExpression NEXT

bind ssl vserver CTXTEST_AAA_VS -certkeyName ctxtest_newcert_2019
<!--NeedCopy-->
```

So konfigurieren Sie Content Switching

```
add cs action <Domain_CS_Action> -targetVserver <Domain_AAA_VS>

```



```
3 add cs policy <Domain_CS_Policy> -rule "is_vpn_url || http.req.url.
    contains("/adfs/ls") || http.req.url.contains("/adfs/services/trust"
    ) || -action <Domain_CS_Action>
4 <!--NeedCopy-->
```

Beispiel

```
1 add cs action CTXTEST_CS_Action -targetVserver CTXTEST_AAA_VS
2
3 add cs policy CTXTEST_CS_Policy -rule "is_vpn_url || http.req.url.
    contains("/adfs/ls") || http.req.url.contains("/adfs/services/trust"
    ) || -action CTXTEST_CS_Action
4 <!--NeedCopy-->
```

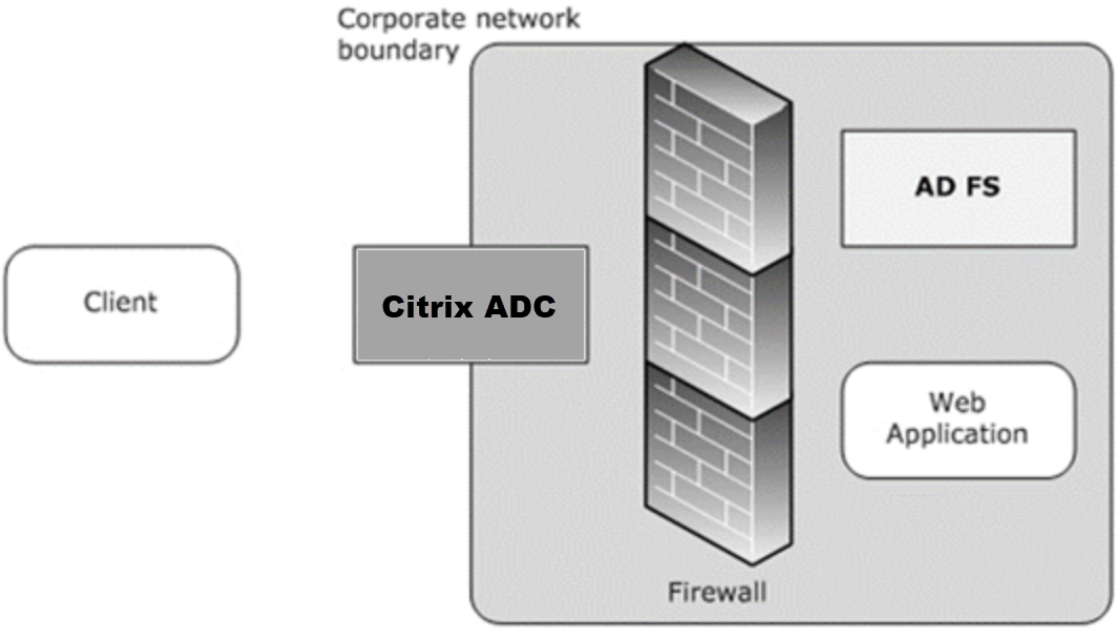
So binden Sie den virtuellen Content Switching Server an die Richtlinie

```
1 bind cs vserver CTXTEST_CSVS -policyName CTXTEST_CS_Policy -priority
    100
2 <!--NeedCopy-->
```

Compliance des Active Directory-Verbunddienstproxy-

March 8, 2022

Wenn Drittanbieter-Proxys anstelle des Webanwendungsproxys verwendet werden sollen, müssen sie das MS-ADFSPIP-Protokoll unterstützen, das die ADFS- und WAP-Integrationsregeln festlegt. ADFSPIP integriert Active Directory Federation Services mit einem Authentifizierungs- und Anwendungsproxy, um Clients, die sich außerhalb dieser Grenze befinden, Zugriff auf Dienste innerhalb der Grenzen des Unternehmensnetzwerks zu ermöglichen.



Voraussetzungen

Um erfolgreich Vertrauen zwischen dem Proxyserver und der ADFS-Farm herzustellen, überprüfen Sie die folgende Konfiguration in der Citrix ADC-Appliance:

- Erstellen Sie ein SSL-Profil für das Backend und aktivieren Sie SNI im SSL-Profil. Deaktivieren Sie SSLv3/TLS1. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1  add ssl profile <new SSL profile> -sniEnable ENABLED -ssl3
      DISABLED -tls1 DISABLED -commonName <FQDN of ADFS>
2  <!--NeedCopy-->
```

- Deaktivieren Sie SSLv3/TLS1 für den Dienst. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1  set ssl service <adfs service name> -sslProfile
      ns_default_ssl_profile_backend
2  <!--NeedCopy-->
```

- SNI-Erweiterung für Back-End-Server-Handshakes aktivieren. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:


```
set vpn parameter  - backendServerSni ENABLED

set ssl parameter -denySSLReneg NONSECURE
<!--NeedCopy-->
```

> **Wichtig**
>
> Für Home Realm Discovery (HRD) -Szenarien, in denen die Authentifizierung auf den ADFS-Server verlagert werden muss, empfiehlt Citrix, sowohl die Authentifizierung als auch SSO auf der Citrix ADC-Appliance zu deaktivieren.

Mechanismus der Authentifizierung

Im Folgenden werden die Ereignisse auf hoher Ebene für die Authentifizierung beschrieben.

1. **Vertrauen mit dem ADFS-Server herstellen** — Der Citrix ADC-Server richtet Vertrauen zum ADFS-Server ein, indem er ein Clientzertifikat registriert. Sobald der Trust eingerichtet ist, stellt die Citrix ADC-Appliance das Vertrauen nach dem Neustart ohne Benutzereingriff wieder her.

   Nach Ablauf des Zertifikats müssen Sie die Vertrauensstellung erneut herstellen, indem Sie das ADFS-Proxy-Profil entfernen und erneut hinzufügen.

2. **Veröffentlichte Endpoints** — Die Citrix ADC-Appliance ruft nach der Vertrauensstellung automatisch die Liste der veröffentlichten Endpunkte auf dem ADFS-Server ab. Diese veröffentlichten Endpunkte filtern die Anforderungen, die an den ADFS-Server weitergeleitet wurden.

3. **Einfügen von Headern in Clientanforderungen** - Wenn die Citrix ADC-Appliance Clientanforderungen tunnelt, werden die mit ADFSPIP verbundenen HTTP-Header dem Paket hinzugefügt, während sie an den ADFS-Server gesendet werden. Sie können die Zugriffssteuerung auf dem ADFS-Server basierend auf diesen Header-Werten implementieren. Die folgenden Header werden unterstützt.

   - X-MS-Proxy
   - X-MS-Endpoint-Absolute-Pfad
   - X-MS-weitergeleitete Client-IP
   - X-MS-Proxy
   - X-MS-Target-Rolle
   - X-MS-ADFS-Proxy-Client-IP

4. **Verwalten des Datenverkehrs** von Endbenutzern — Der Datenverkehr der Endbenutzer wird sicher an die gewünschten Ressourcen weitergeleitet.

> **Hinweis**
>
> Die Citrix ADC-Appliance verwendet die formularbasierte Authentifizierung.

Konfigurieren Sie Citrix ADC für die Unterstützung des ADFS-Servers

Voraussetzungen

- Konfigurieren Sie den Context Switching (CS) -Server als Front-End mit Authentifizierungs-, Autorisierungs- und Überwachungsserver hinter CS. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cs vserver <cs vserver name> SSL 10.220.xxx.xx 443
-cltTimeout 180 -AuthenticationHost <adfs server hostname> -
   Authentication OFF -persistenceType NONE
<!--NeedCopy-->
```

```
add cs action <action name1> -targetLBVserver <lb vserver name>
<!--NeedCopy-->
```

```
add cs action <action name2> -targetLBVserver <lb vserver name>
<!--NeedCopy-->
```

```
add cs policy <policy name1> -rule " http.req.url.contains("/adfs
   /services/trust") || http.req.url.contains("federationmetadata
   /2007-06/federationmetadata.xml")" -action <action name1>
<!--NeedCopy-->
```

```
add cs policy <policy name2> -rule "HTTP.REQ.URL.CONTAINS("/adfs/
   ls")" -action <action name2>
<!--NeedCopy-->
```

```
bind cs vserver <cs vserver name> -policyName <policy name1> -
   priority 100
```



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

```
bind cs vserver <cs vserver name> -policyName <policy name2> -
   priority 110
<!--NeedCopy-->
```

```
bind cs vserver <cs vserver name> -lbvserver <lb vserver name>
<!--NeedCopy-->
```

- Fügen Sie einen ADFS-Dienst hinzu. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <adfs service name> <adfs server ip> SSL 443
<!--NeedCopy-->
```

```
set ssl service <adfs service name> -sslProfile
   ns_default_ssl_profile_backend
<!--NeedCopy-->
```

- Fügen Sie einen virtuellen Server mit Lastausgleich hinzu. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <lb vserver name> SSL 0.0.0.0 0
<!--NeedCopy-->
```

```
set ssl vserver <lb vserver name> -sslProfile
   ns_default_ssl_profile_frontend
<!--NeedCopy-->
```

- Binden Sie den Dienst an den Server mit Lastausgleich. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <lb vserver name> <adfs service name>
<!--NeedCopy-->
```


Um Citrix ADC für die Arbeit mit dem ADFS-Server zu konfigurieren, müssen Sie Folgendes tun:

1. Erstellen eines SSL-CertKey-Profilschlüssels zur Verwendung mit dem ADFS-Proxy-Profil
2. Erstellen eines ADFS-Proxyprofils
3. Ordnen Sie das ADFS-Proxyprofil dem virtuellen LB-Server zu

Erstellen Sie ein SSL-Zertifikat mit privatem Schlüssel zur Verwendung mit dem ADFS-Proxy-Profil

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1     add ssl certkey <certkeyname>  - cert <certificate path> -key <
         keypath>
2 <!--NeedCopy-->
```

Hinweis: Die Zertifikatsdatei und die Schlüsseldatei müssen in der Citrix ADC-Appliance vorhanden sein.
Erstellen eines ADFS-Proxyprofils mit CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add authentication adfsProxyProfile  <profile name> -serverUrl <https:
     //<server FQDN or IP address>/> -username <adfs admin user name> -
     password <password for admin user> -certKeyName <name of the CertKey
      profile created above>
2 <!--NeedCopy-->
```

Wo;

Profilname — Name des zu erstellenden AFDS-Proxy-Profils

ServerUrl — Vollqualifizierter Domainname des ADFS-Dienstes einschließlich Protokoll und Port. Zum Beispiel `https://adfs.citrix.com`

`Username` — Benutzername eines Admin-Kontos, das auf dem ADFS-Server existiert

Kennwort — Kennwort des Admin-Kontos, das als Benutzername verwendet wird

certKeyName — Name des zuvor erstellten SSL certKey-Profils

Ordnen Sie das ADFS-Proxyprofil über die CLI dem virtuellen Lastausgleichsserver zu

In der ADFS-Bereitstellung werden zwei virtuelle Lastausgleichsserver verwendet, einer für den Clientdatenverkehr und der andere für den Metadatenaustausch. Das ADFS-Proxyprofil muss mit

dem virtuellen Lastausgleichsserver verknüpft sein, der den ADFS-Server mit Front-End beendet.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <adfs-proxy-lb> -adfsProxyProfile <name of the ADFS
   proxy profile>
<!--NeedCopy-->
```

Unterstützung der Erneuerung des Vertrauens für ADFSPIP

Sie können das Vertrauen der vorhandenen Zertifikate erneuern, die kurz vor dem Ablauf stehen oder wenn das vorhandene Zertifikat nicht gültig ist. Die Vertrauenserneuerung von Zertifikaten erfolgt nur, wenn die Vertrauensstellung zwischen der Citrix ADC-Appliance und dem ADFS-Server hergestellt wird. Um die Vertrauensstellung des Zertifikats zu erneuern, müssen Sie das neue Zertifikat bereitstellen.

> **Wichtig**
>
> Für die Erneuerung neuer Zertifikate ist ein manuelles Eingreifen erforderlich.

Im folgenden Beispiel werden die Schritte zur Erneuerung des Zertifikatsvertrauens aufgeführt:

1. Die Citrix ADC-Appliance sendet sowohl alte (SerializedTrustCertificate) als auch neue (SerializedReplacementCertificate) Zertifikate in POST-Anforderung an den ADFS-Server zur Erneuerung des Vertrauens.
2. Der ADFS-Server reagiert mit 200 OK erfolgreich, wenn das Vertrauen erfolgreich erneuert wurde.
3. Die Citrix ADC-Appliance aktualisiert den Status “ESTABLISHED_RENEW_SUCCESS”, wenn die Erneuerung des Vertrauens erfolgreich ist. Wenn die Erneuerung des Vertrauens fehlschlägt, wird der Status als “ESTABLISHED_RENEW_FAILED” aktualisiert und die Citrix ADC-Appliance verwendet weiterhin das alte Zertifikat.

> **Hinweis**
>
> Sie können den Cert-Schlüssel nicht aktualisieren, wenn er bereits an ein ADFS-Proxy-Profil gebunden ist.

So konfigurieren Sie die Vertrauenserneuerung von Zertifikaten über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set authentication adfsProxyProfile <name> [-CertKeyName <string>]
```



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

Beispiel:

```
set authentication adfsProxyProfile adfs_2 -CertKeyName ca_cert1
<!--NeedCopy-->
```

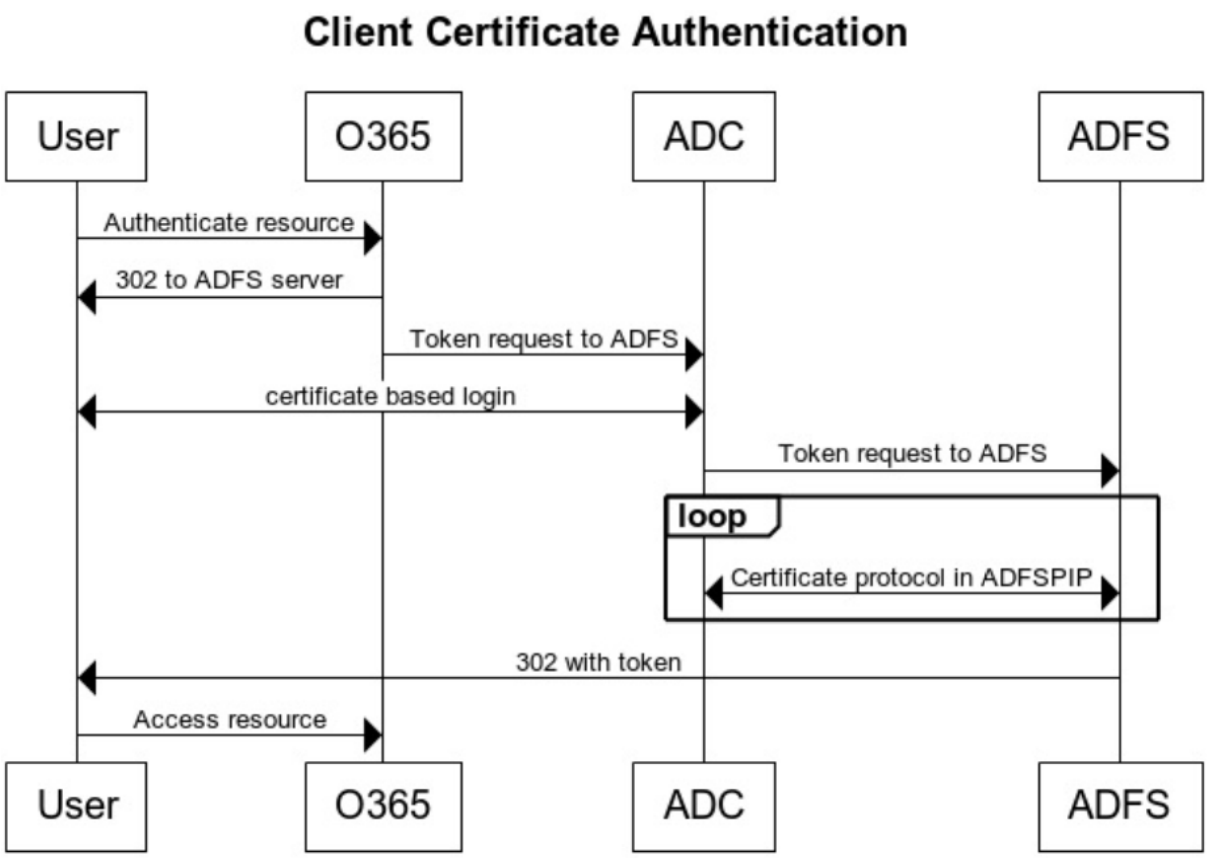
Clientzertifikatbasierte Authentifizierung auf dem ADFS-Server

Ab Windows Server 2016 führte Microsoft eine neue Methode zur Authentifizierung von Benutzern ein, wenn über Proxyserver auf ADFS zugegriffen wird. Endbenutzer können sich jetzt mit ihren Zertifikaten anmelden und vermeiden so die Verwendung eines Kennworts.

Endbenutzer greifen häufig über einen Proxy auf ADFS zu, insbesondere wenn sie sich nicht in den Räumlichkeiten befinden. Daher müssen ADFS-Proxyserver die Clientzertifikatauthentifizierung über das ADFSPIP-Protokoll unterstützen.

Wenn ADFS mit einer Citrix ADC-Appliance Lastenausgleich durchgeführt wird, müssen sich Benutzer zur Unterstützung der zertifikatbasierten Authentifizierung auf dem ADFS-Server ebenfalls mit dem Zertifikat bei der Citrix ADC-Appliance anmelden. Auf diese Weise kann Citrix ADC das Benutzerzertifikat an ADFS übergeben, um SSO für den ADFS-Server bereitzustellen.

Das folgende Diagramm zeigt den Ablauf der Clientzertifikatauthentifizierung.



Konfigurieren von SSO für den ADFS-Server mithilfe des Clientzertifikats

Um SSO für den ADFS-Server mithilfe des Clientzertifikats zu konfigurieren, müssen Sie zuerst die Clientzertifikatauthentifizierung auf der Citrix ADC-Appliance konfigurieren. Anschließend müssen Sie die Richtlinie zur Zertifikatsauthentifizierung an den virtuellen Authentifizierungs-, Autorisierungs- und Überwachungsserver binden.

Darüber hinaus müssen Sie die folgenden Schritte ausführen.

- Ein zusätzlicher virtueller Kontextswitching-Server mit Port 49443 muss konfiguriert werden, und dieser virtuelle Kontextswitching-Server muss auf denselben virtuellen Lastausgleichsserver zeigen, der für alle Ports geöffnet ist, die Sie zuvor erstellt haben.
- Der Port 49443 muss zur Authentifizierung auf der Citrix ADC-Appliance geöffnet werden.
- Die Kontextswitching-Richtlinie muss an denselben virtuellen Lastausgleichsserver mit geöffnetem Port 443 gebunden sein, den Sie zuvor erstellt haben.
- Sie müssen denselben SSL-Dienst, den Sie zuvor erstellt haben, an den virtuellen Lastausgleichsserver binden.
- Wenn Sie bereits ein SSL-Profil für das Backend erstellt haben, müssen Sie dieses Profil verwenden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cs vserver <name> <serviceType> <port>

bind cs vserver <name> (-lbvserver <string> | -vServer <string> | [-
    targetLBVserver <string>]

set ssl vserver <vServerName [-sslProfile <string>]

bind ssl vserver <vServerName -certkeyName <string>

add authentication certAction <action name>

add authentication Policy <policy name> -rule <expression> -action <
    action name>

add authentication policylable <label Name>

bind authentication policylabel <label Name> -policyName <name of the
    policy> -priority<integer>

<!--NeedCopy-->
```

Beispiel:

```
add cs vserver srv123_adfsproxy_csvs_tls SSL $VIP_1 49443

bind cs vserver srv123_adfsproxy_csvs_tls -lbvserver
    srv123_adfs_lbvserver

set ssl vserver srv123_adfsproxy_csvs_tls -sslProfile
    ns_default_ssl_profile_frontend

bind ssl vserver srv123_adfsproxy_csvs_tls -certkeyName
    srv123_wildcardcert

add authentication certAction adfsproxy-cert

add authentication Policy cert1 -rule TRUE -action adfsproxy-cert

add authentication policylable certfactor

```



```
15 bind authentication policylabel certfactor -policyName cert1 -
      priority 100
16
17 <!--NeedCopy-->
```

Informationen zum Konfigurieren des Clientzertifikats auf der Citrix ADC-Appliance finden Sie unter Konfigurieren der Clientzertifikatauthentifizierung mithilfe erweiterter Richtlinien.

Use an on-premises Citrix Gateway as the identity provider for Citrix Cloud

October 5, 2021

Citrix Cloud unterstützt die Verwendung eines on-premises Citrix Gateway als Identitätsanbieter für die Authentifizierung von Abonnenten, wenn diese sich bei ihrem Workspace anmelden.

Vorteile der Authentifizierung mit Citrix Gateway:

- Fortdauernde Authentifizierung von Benutzern über das vorhandene Citrix Gateway, damit sie über Citrix Workspace auf die Ressourcen in der On-Premises-Bereitstellung von Virtual Apps and Desktops zugreifen können.
- Verwenden Sie die Citrix Gateway-Authentifizierungs-, Autorisierungs- und Überwachungsfunktionen mit Citrix Workspace.
- Verwendung von Features wie Passthrough-Authentifizierung, Smartcards, Sicherheitstoken, Richtlinien für bedingten Zugriff, Verbund usw. für den Benutzerzugriff auf erforderliche Ressourcen über Citrix Workspace.

Die Authentifizierung mit Citrix Gateway wird für folgende Produktversionen unterstützt:

- Citrix Gateway 13.0 41.20 Advanced Edition oder höher
- Citrix Gateway 12.1 54.13 Advanced Edition oder höher

Voraussetzungen

- Cloud Connectors - Sie benötigen mindestens zwei Server, auf denen Sie die Citrix Cloud Connector-Software installieren können.
- Active Directory - Führen Sie die erforderlichen Prüfungen durch.
- Anforderungen für Citrix Gateway
  - Verwenden Sie erweiterte Richtlinien auf dem on-premises Gateway aufgrund der Veraltung klassischer Richtlinien.

- Bei der Konfiguration des Gateway für die Authentifizierung von Abonnenten von Citrix Workspace fungiert das Gateway als OpenID Connect-Anbieter. Nachrichten zwischen Citrix Cloud und Gateway entsprechen dem OIDC-Protokoll, was auch die digitale Signatur von Token umfasst. Daher müssen Sie ein Zertifikat zur Signatur dieser Token konfigurieren.
- Taktsynchronisation - Das Gateway muss mit der NTP-Zeit synchronisiert sein.

Details finden Sie unter Voraussetzungen.

Erstellen einer OAuth IdP-Richtlinie auf dem lokalen Citrix Gateway

> **Wichtig:**
>
> Sie müssen die Client-ID, die geheime und die Umleitungs-URL auf der Registerkarte **Citrix Cloud > Identitäts- und Zugriffsmanagement > Authentifizierung** generiert haben. Weitere Informationen finden Sie unter Verbinden eines on-premises Citrix Gateway mit Citrix Cloud.

Das Erstellen einer OAuth IdP-Authentifizierungsrichtlinie umfasst die folgenden Aufgaben:

1. Erstellen Sie ein OAuth IdP-Profil.
2. Fügen Sie eine OAuth IdP-Richtlinie hinzu.
3. Binden Sie die OAuth IdP-Richtlinie an einen virtuellen Authentifizierungsserver.
4. Binden Sie das Zertifikat global.

Erstellen eines OAuth IdP-Profils mit der CLI

Geben Sie an der Eingabeaufforderung;

```
add authentication OAuthIDPProfile <name> [-clientID <string>][-
    clientSecret ][-redirectURL <URL>][-issuer <string>][-audience <
    string>][-skewTime <mins>] [-defaultAuthenticationGroup <string>]

add authentication OAuthIdPPolicy <name> -rule <expression> [-action <
    string> [-undefAction <string>] [-comment <string>][-logAction <
    string>]

add authentication ldapAction <name> -serverIP <IP> -ldapBase "dc=aaa,
    dc=local"

ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password> -
    ldapLoginName sAMAccountName

```



```
add authentication policy <name> -rule <expression> -action <string>

bind authentication vserver auth_vs -policy <ldap_policy_name> -
    priority <integer> -gotoPriorityExpression NEXT

bind authentication vserver auth_vs -policy <OAuthIDPPolicyName> -
    priority <integer> -gotoPriorityExpression END

bind vpn global  - certkey <>
<!--NeedCopy-->
```

Erstellen eines OAuth IdP-Profils mit der GUI

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > OAuth IDP**.

   ![Oauth-IDP-navigation](/en-us/citrix-adc/media/oauth-navigation-to-idp.png)

2. Wählen Sie auf der **OAuth IDP-Seite** die Registerkarte **Profile** aus und klicken Sie auf **Hinzufügen**.

3. Konfigurieren Sie das OAuth IdP-Profil.

   > **Hinweis:**
   >
   > - Kopieren Sie die Werte für Client-ID, Secret und Redirect URL aus der Registerkarte **Citrix Cloud > Identitäts- und Zugriffsmanagement > Authentifizierung** und fügen Sie sie ein, um die Verbindung zu Citrix Cloud herzustellen.
   > - Geben Sie die Gateway-URL im Beispiel für den **Ausstellernamen** korrekt ein: https://GatewayFQDN.com
   > - Kopieren Sie auch die Client-ID und fügen Sie sie auch in das Feld **Zielgruppe** ein.
   > - **Kennwort senden**: Aktivieren Sie diese Option für Single-Sign-On-Unterstützung. Standardmäßig ist diese Option deaktiviert.

4. Legen Sie im Bildschirm **Authentifizierung erstellen OAuth IDP-Profil** Werte für die folgenden Parameter fest und klicken Sie auf **Erstellen**.

   - **Name** — Name des Authentifizierungsprofils. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und darf nur Buchstaben, Zahlen und den Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), Leerzeichen (), bei (@), gleich (=), Doppelpunkt (:) und Unterstriche enthalten. Kann nicht geändert werden, nachdem das Profil erstellt wurde.
   - **Client-ID** — Eindeutige Zeichenfolge, die SP identifiziert. Der Autorisierungsserver führt die Clientkonfiguration mit dieser ID ab. Maximale Länge: 127

- **Client Secret** — Geheime Zeichenfolge, die vom Benutzer und Autorisierungsserver festgelegt wurde. Maximale Länge: 239
- **URL umleiten** — Endpunkt für SP, an dem Code/Token gepostet werden muss.
- **Name des Ausstellers** — Identität des Servers, dessen Token akzeptiert werden sollen. Maximale Länge: 127 Beispiel:https://GatewayFQDN.com
- **Zielgruppe** — Zielempfänger für das Token, das vom IdP gesendet wird. Dies könnte vom Empfänger überprüft werden.
- **Skew Time** — Diese Option gibt die zulässige Taktverzerrung in Minuten an, die Citrix ADC für ein eingehendes Token zulässt. Wenn SkewTime beispielsweise 10 ist, wäre das Token von (aktuelle Zeit - 10) min bis (aktuelle Zeit + 10) min gültig, das sind insgesamt 20 Minuten. Standardwert: 5.
- **Standard-Authentifizierungsgruppe** — Eine Gruppe, die der internen Gruppenliste der Sitzung hinzugefügt wurde, wenn dieses Profil von IdP ausgewählt wird, das im nFactor Flow verwendet werden kann. Es kann im Ausdruck (AAA.USER.IS_MEMBER_OF (“xxx”)) für Authentifizierungsrichtlinien verwendet werden, um den zugehörigen nFactor-Flow zu identifizieren. Maximale Länge: 63

Der Sitzung für dieses Profil wird eine Gruppe hinzugefügt, um die Richtlinienbewertung zu vereinfachen und beim Anpassen von Richtlinien zu helfen. Dies ist die Standardgruppe, die ausgewählt wird, wenn die Authentifizierung zusätzlich zu den extrahierten Gruppen erfolgreich ist. Maximale Länge: 63.

![Oauth-IDP-profile-parameters](/en-us/citrix-adc/media/oauth-idp-profile.png)

5. Klicken Sie auf **Richtlinien**, und klicken Sie auf **Hinzufügen.**
6. Legen Sie im Fenster **Richtlinie für OAuth IDP-Authentifizierung erstellen** Werte für die folgenden Parameter fest und klicken Sie auf **Erstellen**.
   - **Name** — Der Name der Authentifizierungsrichtlinie.
   - **Aktion** — Name des zuvor erstellten Profils.
   - **Log Action** — Name der Nachrichtenprotokollaktion, die verwendet werden soll, wenn eine Anforderung mit dieser Richtlinie übereinstimmt. Keine obligatorische Einreichung.
   - Aktion mit**undefiniertem Ergebnis — Aktion**, die ausgeführt werden soll, wenn das Ergebnis der Richtlinienbewertung nicht bestraft wird (UNDEF). Kein Pflichtfeld.
   - **Ausdruck** — Standardsyntaxausdruck, den die Richtlinie verwendet, um auf eine bestimmte Anforderung zu antworten. Zum Beispiel ist es wahr.
   - **Kommentare** - Irgendwelche Kommentare zu den Richtlinien.

   ![Oauth-IDP-policy](/en-us/citrix-adc/media/oauth-idp-policy.png)

> **Hinweis:**
>
> Wenn **sendPassword** auf ON (standardmäßig OFF) eingestellt ist, werden Benutzeranmeldeinformationen verschlüsselt und über einen sicheren Kanal an Citrix Cloud weitergeleitet. Wenn Sie Benutzeranmeldeinformationen über einen sicheren Kanal übergeben, können Sie SSO an Citrix Virtual Apps and Desktops nach dem Start aktivieren.

Binden der OAuthIDP-Richtlinie und der LDAP-Richtlinie an den virtuellen Authentifizierungsserver

1. Navigieren Sie zu **Konfiguration > Sicherheit > AAA-Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Aktionen > LDAP**.
2. Klicken Sie im Bildschirm **LDAP-Aktionen** auf **Hinzufügen**.
3. Legen Sie im Bildschirm **Authentifizierungs-LDAP-Server erstellen** die Werte für die folgenden Parameter fest und klicken Sie auf **Erstellen**.
   - **Name —** Der Name der LDAP-Aktion
   - **Servername/ServerIP —** Bereitstellung von FQDN oder IP des LDAP-Servers
   - Wählen Sie geeignete Werte **für Sicherheitstyp, Port, Servertyp, Timeout**
   - Stellen Sie sicher, dass **Authentifizierung** aktiviert ist
   - **Basis-DN —** Basis, von der aus die LDAP-Suche gestartet werden soll. Beispiel: `dc=aaa`, `dc=local`.
   - **Administrator Bind DN:** Benutzername der Bindung an den LDAP-Server. Zum Beispiel admin@aaa.local.
   - **Administratorkennwort/Kennwort bestätigen: Kennwort zum Binden von LDAP**
   - Klicken Sie auf **Verbindung testen**, um Ihre Einstellungen zu testen.
   - **Attribut für Server-Anmeldename:** Wählen Sie **“samAccountName”**
   - Andere Felder sind nicht Pflichtfelder und können daher nach Bedarf konfiguriert werden.
4. Navigieren Sie zu **Konfiguration > Sicherheit > AAA-Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinie.**
5. Klicken Sie im Bildschirm **Authentifizierungsrichtlinien** auf **Hinzufügen**.
6. Legen Sie auf der Seite **Authentifizierungsrichtlinie erstellen** die Werte für die folgenden Parameter fest und klicken Sie auf **Erstellen.**
   - **Name —** Name der LDAP-Authentifizierungsrichtlinie.
   - **Aktionstyp —** Wählen Sie **LDAP aus.**
   - **Aktion —** Wählen Sie die LDAP-Aktion aus.
   - **Ausdruck —** Standardsyntaxausdruck, den die Richtlinie verwendet, um auf eine bestimmte Anforderung zu antworten. Zum Beispiel stimmt**.

Unterstützung für aktiv-aktive GSLB-Bereitstellungen auf Citrix Gateway

Citrix Gateway, das mit dem OIDC-Protokoll als Identity Provider (IdP) konfiguriert ist, kann aktiv-aktive GSLB-Bereitstellungen unterstützen. Die aktiv-aktive GSLB-Bereitstellung auf dem Citrix Gateway IdP ermöglicht den Lastausgleich einer eingehenden Benutzeranmeldeanforderung an mehreren geografischen Standorten.

> **Wichtig**
>
> Citrix empfiehlt, Zertifizierungsstellenzertifikate an den SSL-Dienst zu binden und die Zertifikatvalidierung für den SSL-Dienst zu aktivieren, um die Sicherheit zu erhöhen.

Weitere Informationen zum Konfigurieren des GSLB-Setups finden Sie unter Beispiel für eine GSLB-Setup und -Konfiguration.

Konfigurationsunterstützung für SameSite-Cookie-Attribut

May 10, 2022

Das SameSite-Attribut gibt dem Browser an, ob das Cookie für standortübergreifenden Kontext oder nur für den gleichen Site-Kontext verwendet werden kann. Wenn auf eine Anwendung in einem standortübergreifenden Kontext zugegriffen werden soll, kann sie dies auch nur über die HTTPS-Verbindung tun. Einzelheiten siehe RFC6265.

Bis Februar 2020 wurde das SameSite-Attribut in Citrix ADC nicht explizit festgelegt. Der Browser nahm den Standardwert (Keine). Die Nichteinstellung des SameSite-Attributs hatte keine Auswirkungen auf das Citrix Gateway und die Authentifizierungs-, Autorisierungs- und Überwachungsbereitstellungen.

Bei bestimmten Browser-Upgrades wie Google Chrome 80 ändert sich das standardmäßige domänenübergreifende Verhalten von Cookies. Das SameSite-Attribut kann auf einen der folgenden Werte festgelegt werden. Der Standardwert für Google Chrome ist auf Lax festgelegt. Bei bestimmten Versionen anderer Browser ist der Standardwert für das SameSite-Attribut möglicherweise immer noch auf None festgelegt.

- **Keine**: Weist darauf hin, dass der Browser ein Cookie im standortübergreifenden Kontext nur bei sicheren Verbindungen verwendet.
- **Lax**: Weist darauf hin, dass der Browser ein Cookie für Anfragen auf derselben Domain und für Cross-Sites verwendet. Für standortübergreifende Zwecke können nur sichere HTTP-Methoden wie GET-Anfrage das Cookie verwenden. Beispielsweise kann eine GET-Anfrage einer Ein-Subdomain abc.beispiel.com das Cookie einer anderen Subdomain xyz.beispiel.com mithilfe eines GET lesen.

Für standortübergreifende Anwendungen werden nur sichere HTTP-Methoden verwendet, da sichere HTTP-Methoden den Serverstatus nicht verändern. Weitere Einzelheiten finden Sie unter https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite#lax

- **Streng**: Verwenden Sie das Cookie nur im selben Site-Kontext.

Wenn das Cookie kein sameSite-Attribut enthält, geht Google Chrome von der Funktionalität von sameSite = Lax aus.
Daher teilt Google Chrome bei Bereitstellungen innerhalb eines iframes mit standortübergreifendem Kontext, bei dem Cookies vom Browser eingefügt werden müssen, keine standortübergreifenden Cookies. Infolgedessen wird der Iframe auf der Website möglicherweise nicht geladen.

SameSite-Cookie-Attribut konfigurieren

Ein neues Cookie-Attribut namens SameSite wird dem VPN und der Authentifizierung, Autorisierung und Überwachung virtueller Server hinzugefügt. Dieses Attribut kann auf globaler Ebene und auf virtueller Serverebene festgelegt werden.

Um das sameSite-Attribut zu konfigurieren, müssen Sie Folgendes tun:

1. Setzt das sameSite-Attribut für den virtuellen Server
2. Binden Sie Cookies an den Patset (wenn der Browser Site-übergreifende Cookies ablegt)

Festlegen des sameSite-Attributs mithilfe der CLI

Verwenden Sie die folgenden Befehle, um das sameSite-Attribut auf virtueller Serverebene festzulegen.

```
set vpn vserver VP1 -SameSite [STRICT | LAX | None]
set authentication vserver AV1 -SameSite [STRICT | LAX | None]
<!--NeedCopy-->
```

Verwenden Sie die folgenden Befehle, um das sameSite-Attribut auf globaler Ebene festzulegen.

```
set aaa parameter -SameSite [STRICT | LAX | None]
set vpn parameter -SameSite [STRICT | LAX | None]
<!--NeedCopy-->
```

Hinweis: Die Einstellung auf virtueller Serverebene nimmt den Vorzug gegenüber der Einstellung auf globaler Ebene vor. Citrix empfiehlt, das SameSite-Cookie-Attribut auf der Ebene des virtuellen Servers festzulegen.

Binden von Cookies an den Patset mithilfe der CLI

Wenn der Browser Site-übergreifende Cookies löscht, können Sie diese Cookie-Zeichenfolge an das vorhandene NS_Cookies_SameSite-Patset binden, sodass das sameSite-Attribut dem Cookie hinzugefügt wird.

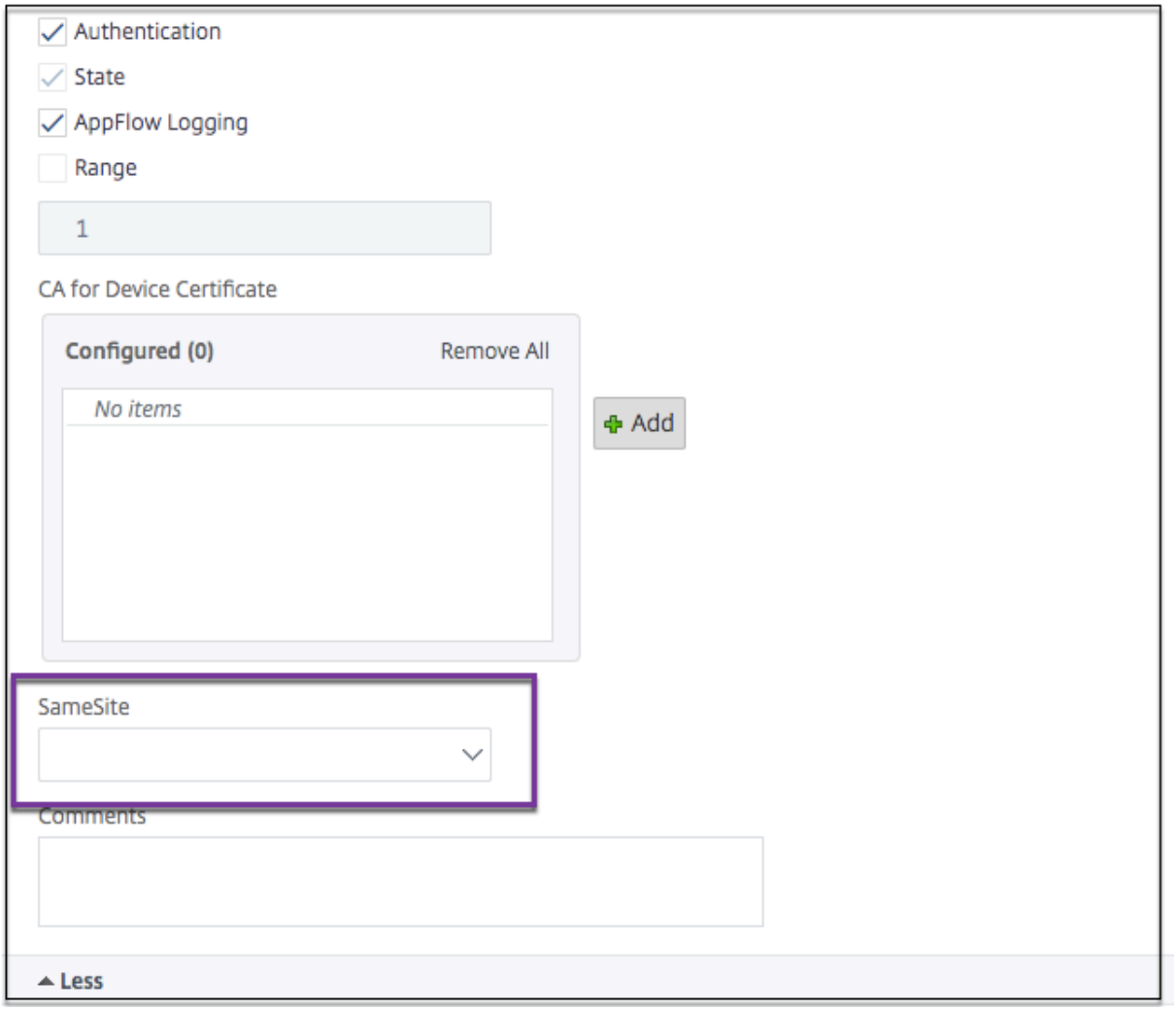
Beispiel:

```
bind patset ns_cookies_SameSite ”NSC_TASS”
bind patset ns_cookies_SameSite ”NSC_TMAS”
<!--NeedCopy-->
```

Festlegen des SameSite-Attributs über die GUI

So legen Sie das sameSite-Attribut auf virtueller Serverebene fest:

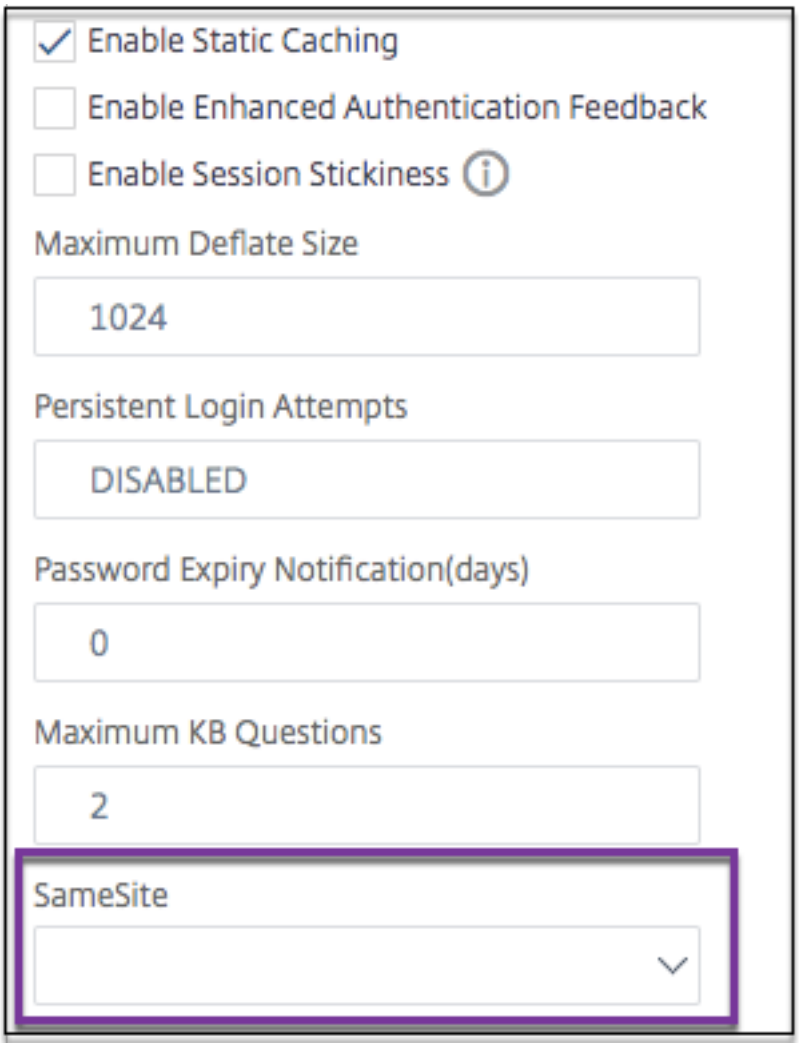
1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsdatenverkehr > Virtuelle Server.**
2. Wählen Sie einen virtuellen Server aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Grundeinstellungen**auf das Bearbeitungssymbol und dann auf **Mehr**.
4. Wählen Sie in **SameSite**die Option nach Bedarf aus.



So legen Sie das sameSite-Attribut auf globaler Ebene fest:

1. Navigieren Sie zu **Sicherheit > AAA — Anwendungsverkehr > Authentifizierungseinstellungen ändern.**

2. Klicken Sie auf der Seite **AAA-Parameter konfigurieren** auf die **SameSite-Liste** und wählen Sie die gewünschte Option aus.



Authentifizierung, Autorisierung und Auditing-Konfiguration für häufig verwendete Protokolle

February 24, 2022

Für die Konfiguration der Citrix ADC Appliance für Authentifizierung, Autorisierung und Überwachung ist eine spezielle Einrichtung in der Citrix ADC Appliance und den Browsern der Clients erforderlich. Die Konfiguration variiert je nach Protokoll, das für die Authentifizierung, Autorisierung und Überwachung verwendet wird.

Weitere Informationen zum Konfigurieren der Citrix ADC Appliance für die Kerberos-Authentifizierung finden Sie unter Umgang mit Authentifizierung, Autorisierung und Auditing mit Kerberos/NTLM.

Umgang mit Authentifizierung, Autorisierung und Auditing mit Kerberos/NTLM

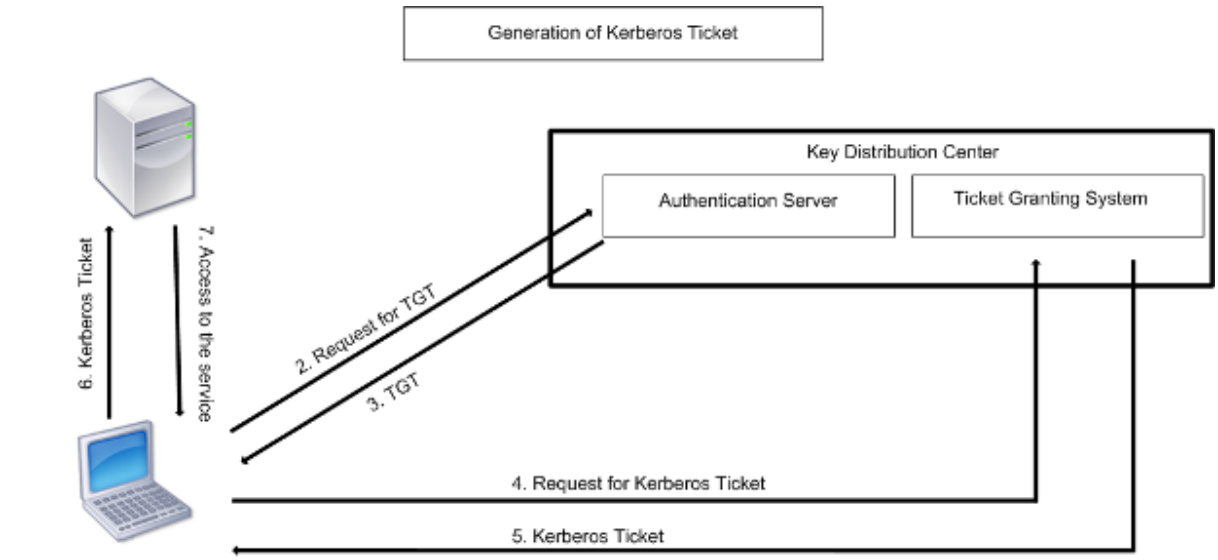
October 5, 2021

Kerberos, ein Computer-Netzwerkauthentifizierungsprotokoll, bietet eine sichere Kommunikation über das Internet. Sie wurde hauptsächlich für Client-Server-Anwendungen entwickelt und bietet eine gegenseitige Authentifizierung, mit der Client und Server die Authentizität des anderen sicherstellen können. Kerberos verwendet einen vertrauenswürdigen Drittanbieter, der als Key Distribution Center (KDC) bezeichnet wird. Ein KDC besteht aus einem Authentifizierungsserver (AS), der einen Benutzer authentifiziert, und einem Ticket Granting Server (TGS).

Jede Entität im Netzwerk (Client oder Server) verfügt über einen geheimen Schlüssel, der nur sich selbst und dem KDC bekannt ist. Die Kenntnis dieses Schlüssels impliziert Authentizität der Entität. Für die Kommunikation zwischen zwei Entitäten im Netzwerk generiert der KDC einen Sitzungsschlüssel, der als Kerberos-Ticket oder Serviceticket bezeichnet wird. Der Client stellt eine Anforderung an den AS für Anmeldeinformationen für einen bestimmten Server. Der Kunde erhält dann ein Ticket, das als Ticket Granting Ticket (TGT) bezeichnet wird. Der Kunde kontaktiert dann die TGS, verwendet den TGT, den er vom AS erhalten hat, um seine Identität zu beweisen, und bittet um einen Service. Wenn der Kunde für den Service berechtigt ist, gibt der TGS dem Kunden ein Kerberos-Ticket aus. Der Client kontaktiert dann den Server, der den Dienst hostet (als Serviceserver bezeichnet) und verwendet das Kerberos-Ticket, um nachzuweisen, dass er berechtigt ist, den Dienst zu empfangen. Das Kerberos-Ticket hat eine konfigurierbare Lebensdauer. Der Client authentifiziert sich nur einmal mit dem AS. Wenn er den physischen Server mehrmals kontaktiert, wird das AS-Ticket wiederverwendet.

Die folgende Abbildung zeigt die grundlegende Funktionsweise des Kerberos-Protokolls.

Abbildung 1. **Funktionieren von Kerberos**



Die Kerberos-Authentifizierung hat folgende Vorteile:

- Schnellere Authentifizierung. Wenn ein physischer Server ein Kerberos-Ticket von einem Client erhält, verfügt der Server über genügend Informationen, um den Client direkt zu authentifizieren. Es muss keinen Domänencontroller für die Clientauthentifizierung kontaktieren, und daher ist der Authentifizierungsprozess schneller.
- Gegenseitige Authentifizierung. Wenn der KDC ein Kerberos-Ticket an einen Client ausgibt und der Client das Ticket für den Zugriff auf einen Dienst verwendet, können nur authentifizierte Server das Kerberos-Ticket entschlüsseln. Wenn der virtuelle Server auf der Citrix ADC Appliance das Kerberos-Ticket entschlüsseln kann, können Sie feststellen, dass sowohl der virtuelle Server als auch der Client authentifiziert sind. Somit erfolgt die Authentifizierung des Servers zusammen mit der Authentifizierung des Clients.
- Single Sign-On zwischen Windows und anderen Betriebssystemen, die Kerberos unterstützen.

Kerberos-Authentifizierung kann folgende Nachteile haben:

- Kerberos hat strenge Zeitanforderungen. Die Uhren der beteiligten Hosts müssen mit der Kerberos-Serveruhr synchronisiert werden, um sicherzustellen, dass die Authentifizierung nicht fehlschlägt. Sie können diesen Nachteil verringern, indem Sie die Network Time Protocol Daemons verwenden, um die Host-Uhren synchronisieren zu lassen. Kerberos-Tickets haben einen Verfügbarkeitszeitraum, den Sie konfigurieren können.
- Kerberos benötigt den zentralen Server, um kontinuierlich verfügbar zu sein. Wenn der Kerberos-Server heruntergefahren ist, kann sich niemand anmelden. Sie können dieses Risiko verringern, indem Sie mehrere Kerberos-Server und Fallback-Authentifizierungsmechanismen verwenden.
- Da die gesamte Authentifizierung von einem zentralen KDC gesteuert wird, können alle Kompromisse in dieser Infrastruktur, z. B. das Kennwort des Benutzers für eine gestohlene lokale

Arbeitsstation, einem Angreifer die Identität eines beliebigen Benutzers ermöglichen. Sie können dieses Risiko in gewissem Maße verringern, indem Sie nur einen Desktop-Computer oder Laptop verwenden, dem Sie vertrauen, oder indem Sie die Vorauthentifizierung mittels eines Hardware-Token erzwingen.

Um die Kerberos-Authentifizierung verwenden zu können, müssen Sie sie auf der Citrix ADC Appliance und auf jedem Client konfigurieren.

Optimierung der Kerberos-Authentifizierung bei Authentifizierung, Autorisierung und Überwachung

Die Citrix ADC Appliance optimiert und verbessert jetzt die Systemleistung während der Kerberos-Authentifizierung. Der Authentifizierungs-, Autorisierungs- und Auditing-Daemon merkt sich die ausstehende Kerberos-Anfrage für denselben Benutzer, um die Belastung des Key Distribution Centers (KDC) zu vermeiden, wodurch doppelte Anforderungen vermieden werden.

Wie Citrix ADC Kerberos für die Clientauthentifizierung implementiert

October 5, 2021

> **Wichtig**
>
> Kerberos/NTLM-Authentifizierung wird nur in NetScaler 9.3 nCore Version oder höher unterstützt und kann nur für die Authentifizierung, Autorisierung und Überwachung von virtuellen Servern zur Datenverkehrsverwaltung verwendet werden.

Citrix ADC behandelt die Komponenten, die an der Kerberos-Authentifizierung beteiligt sind, folgendermaßen:

Schlüsselverteilungszentrum (KDC)

In Windows 2000 Server oder höher sind der Domänencontroller und der KDC Teil des Windows Servers. Wenn der Windows Server UP ist und ausgeführt wird, gibt es an, dass der Domänencontroller und KDC konfiguriert sind. Der KDC ist auch der Active Directory -Server.

> **Hinweis:**
>
> Alle Kerberos-Interaktionen werden mit dem Windows Kerberos-Domänencontroller validiert.

Authentifizierungsdienst und Protokollverhandlung

Eine Citrix ADC Appliance unterstützt die Kerberos-Authentifizierung auf den virtuellen Servern zur Authentifizierung, Autorisierung und Überwachung der Datenverkehrsverwaltung. Wenn die Kerberos-Authentifizierung fehlschlägt, verwendet Citrix ADC die NTLM-Authentifizierung.

Standardmäßig verwenden Windows 2000 Server und höhere Windows Server-Versionen Kerberos für Authentifizierung, Autorisierung und Überwachung. Wenn Sie eine Authentifizierungsrichtlinie mit Negotiate als Authentifizierungstyp erstellen, versucht Citrix ADC, das Kerberos-Protokoll für die Authentifizierung, Autorisierung und Überwachung zu verwenden. Wenn der Browser des Clients kein Kerberos-Ticket empfängt, verwendet Citrix ADC die NTLM-Authentifizierung. Dieser Prozess wird als Verhandlung bezeichnet.

Der Kunde kann ein Kerberos-Ticket in einem der folgenden Fälle nicht erhalten:

- Kerberos wird auf dem Client nicht unterstützt.
- Kerberos ist auf dem Client nicht aktiviert.
- Der Client befindet sich in einer anderen Domäne als der KDC.
- Auf das Access Directory auf dem KDC kann der Client nicht zugegriffen werden.

Für die Kerberos/NTLM-Authentifizierung verwendet Citrix ADC nicht die Daten, die lokal auf der Citrix ADC-Appliance vorhanden sind.

Ermächtigung

Der virtuelle Server für die Datenverkehrsverwaltung kann ein virtueller Lastausgleichsserver oder ein virtueller Content Switching-Server sein.

Überwachung

Die Citrix ADC Appliance unterstützt die Überwachung der Kerberos-Authentifizierung mit der folgenden Überwachungsprotokollierung:

- Vollständiger Audit-Pfad der Traffic-Management-Endbenutzeraktivität
- SYSLOG- und Hochleistungs-TCP-Protokollierung
- Vollständiger Prüfpfad der Systemadministratoren
- Alle Systemereignisse
- Skriptfähiges Protokollformat

Unterstützte Umgebung

Die Kerberos-Authentifizierung erfordert keine spezifische Umgebung auf dem Citrix ADC. Der Client (Browser) muss Unterstützung für die Kerberos-Authentifizierung bereitstellen.

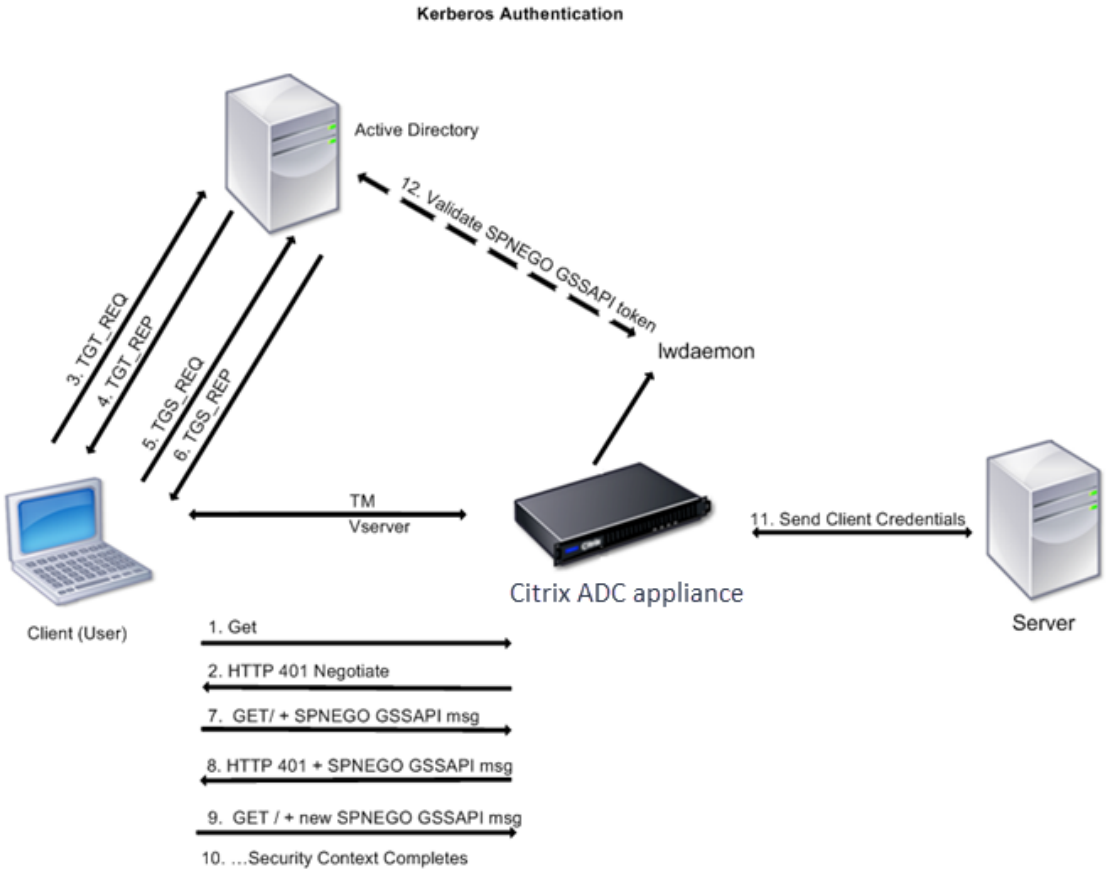
Hohe Verfügbarkeit

Bei einem Hochverfügbarkeitssetup tritt nur der aktive Citrix ADC der Domäne bei. Im Falle eines Failovers verbindet der Citrix ADC lwagent Daemon die sekundäre Citrix ADC-Appliance mit der Domäne. Für diese Funktionalität ist keine spezifische Konfiguration erforderlich.

Kerberos-Authentifizierungsprozess

Die folgende Abbildung zeigt einen typischen Prozess für die Kerberos-Authentifizierung in der Citrix ADC Umgebung.

Abbildung 1. Kerberos-Authentifizierungsprozess auf Citrix ADC



Die Kerberos-Authentifizierung erfolgt in den folgenden Phasen:

Client authentifiziert sich beim KDC

1. Die Citrix ADC Appliance empfängt eine Anforderung von einem Client.
2. Der virtuelle Server zur Datenverkehrsverwaltung (Load Balancing oder Content Switching) auf der Citrix ADC Appliance sendet eine Herausforderung an den Client.
3. Um auf die Herausforderung zu reagieren, erhält der Kunde ein Kerberos-Ticket.

- Der Client sendet dem Authentifizierungsserver des KDC eine Anforderung für ein Ticket Granting Ticket (TGT) und erhält den TGT. (Siehe 3, 4 in der Abbildung Kerberos-Authentifizierungsprozess.)
- Der Client sendet den TGT an den Ticket Granting Server des KDC und erhält ein Kerberos-Ticket. (Siehe 5, 6 in der Abbildung Kerberos-Authentifizierungsprozess.)

> **Hinweis:**
>
> Der oben genannte Authentifizierungsprozess ist nicht erforderlich, wenn der Client bereits über ein Kerberos-Ticket verfügt, dessen Lebensdauer noch nicht abgelaufen ist. Darüber hinaus erhalten Clients wie Webdienste, .NET oder J2EE, die SPNEGO unterstützen, ein Kerberos-Ticket für den Zielserver, erstellen ein SPNEGO-Token und fügen das Token in den HTTP-Header ein, wenn sie eine HTTP-Anforderung senden. Sie durchlaufen nicht den Clientauthentifizierungsprozess.

Der Client fordert einen Dienst an.

1. Der Client sendet das Kerberos-Ticket, das das SPNEGO-Token und die HTTP-Anforderung enthält, an den virtuellen Server für die Datenverkehrsverwaltung auf dem Citrix ADC. Das SPNEGO-Token verfügt über die notwendigen GSSAPI-Daten.
2. Die Citrix ADC-Appliance erstellt einen Sicherheitskontext zwischen dem Client und dem Citrix ADC. Wenn Citrix ADC die im Kerberos-Ticket angegebenen Daten nicht akzeptieren kann, wird der Client aufgefordert, ein anderes Ticket zu erhalten. Dieser Zyklus wiederholt sich, bis die GSSAPI-Daten akzeptabel sind und der Sicherheitskontext eingerichtet ist. Der virtuelle Server zur Datenverkehrsverwaltung auf dem Citrix ADC fungiert als HTTP-Proxy zwischen dem Client und dem physischen Server.

Die Citrix ADC Appliance schließt die Authentifizierung ab.

1. Nachdem der Sicherheitskontext abgeschlossen ist, überprüft der virtuelle Server für die Datenverkehrsverwaltung das SPNEGO-Token.
2. Aus dem gültigen SPNEGO-Token extrahiert der virtuelle Server die Benutzer-ID und die GSS-Anmeldeinformationen und übergibt sie an den Authentifizierungsdaemon.
3. Eine erfolgreiche Authentifizierung schließt die Kerberos-Authentifizierung ab.

Konfigurieren der Kerberos-Authentifizierung auf der Citrix ADC Appliance

October 5, 2021

In diesem Thema finden Sie detaillierte Schritte zum Konfigurieren der Kerberos-Authentifizierung auf der Citrix ADC Appliance mit der CLI und der GUI.

Konfigurieren der Kerberos-Authentifizierung auf der CLI

1. Aktivieren Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion, um die Authentifizierung des Datenverkehrs auf der Appliance sicherzustellen.

   ns-cli-prompt> **enable ns feature** AAA

2. Fügen Sie der Citrix ADC Appliance die Keytab-Datei hinzu. Eine Keytab-Datei ist für die Entschlüsselung des Geheimnisses erforderlich, der vom Client während der Kerberos-Authentifizierung empfangen wurde. Eine einzelne Keytab-Datei enthält Authentifizierungsdetails für alle Dienste, die an den virtuellen Server für die Datenverkehrsverwaltung auf der Citrix ADC Appliance gebunden sind.

   Generieren Sie zuerst die Keytab-Datei auf dem Active Directory -Server und übertragen Sie sie dann an die Citrix ADC Appliance.

   - Melden Sie sich beim Active Directory -Server an, und fügen Sie einen Benutzer für die Kerberos-Authentifizierung hinzu. Um beispielsweise einen Benutzer mit dem Namen Kerb-SVC-Konto hinzuzufügen:

     net user kerb-SVC-account freebsd! @ #456 /hinzufügen

     > **Hinweis:**
     >
     > Stellen Sie im Abschnitt **Benutzereigenschaften** sicher, dass die Option “Kennwort bei der nächsten Anmeldung ändern” nicht ausgewählt ist und die Option “Kennwort läuft nicht ab” ausgewählt ist.

   - Ordnen Sie den HTTP-Dienst dem obigen Benutzer zu und exportieren Sie die keytab-Datei. Führen Sie beispielsweise den folgenden Befehl auf dem Active Directory -Server aus:

     ktpass /out keytabfile /princ HTTP/owa.newacp.com@NEWACP.COM /pass freebsd!@#456 /mapuser newacp\dummy /ptype KRB5_NT_PRINCIPAL

     > **Hinweis:**
     >
     > Sie können mehrere Dienste zuordnen, wenn eine Authentifizierung für mehrere Dienste erforderlich ist. Wenn Sie weitere Dienste zuordnen möchten, wiederholen Sie den obigen Befehl für jeden Dienst. Sie können den gleichen Namen oder andere Namen für die Ausgabedatei angeben.

   - Übertragen Sie die keytab-Datei mithilfe des Befehls unix **ftp** oder eines anderen Dateiübertragungsdienstprogramms Ihrer Wahl auf die Citrix ADC Appliance.

3. Die Citrix ADC Appliance muss die IP-Adresse des Domänencontroller aus dem vollqualifizierten Domänennamen (FQDN) abrufen. Daher empfiehlt Citrix die Konfiguration des Citrix ADC mit einem DNS-Server.

ns-cli-prompt> **add dns nameserver** <ip-address>

> **Hinweis:**
>
> Alternativ können Sie statische Hosteinträge hinzufügen oder andere Mittel verwenden, damit die Citrix ADC Appliance den FQDN-Namen des Domänencontroller in eine IP-Adresse auflösen kann.

4. Konfigurieren Sie die Authentifizierungsaktion, und ordnen Sie sie dann einer Authentifizierungsrichtlinie zu.

   - Konfigurieren Sie die Aushandlungsaktion.

     ns-cli-prompt **Authentifizierung hinzufügen negotiateAction** <name>-domain <domain name>-domainUser <domain user name>-DomainUserPasswd <domain user password>-DefaultAuthenticationGroup <default authentication group>-keytab <string>-ntlmPath <string>

     Hinweis: Wechseln Sie für die Konfiguration von Domänenbenutzern und Domänennamen zum Client und verwenden Sie den Befehl klist wie im folgenden Beispiel gezeigt:

     Kunde: Benutzername @ AAA.LOCAL

     Server: http/onprem_idp.AAA.Local @ AAA.LOCAL

     Authentifizierung hinzufügen NegotiateAction <name>-domain -DomainUser \<HTTP/onprem_idp.aaa.local>

   - Konfigurieren Sie die Verhandlungsrichtlinie, und ordnen Sie die Verhandlungsaktion dieser Richtlinie zu.

     ns-cli-prompt> **add authentication negotiatePolicy** <name> <rule> <reqAction>

5. Erstellen Sie einen virtuellen Authentifizierungsserver, und ordnen Sie ihm die Verhandlungsrichtlinie zu.

   - Erstellen Sie einen virtuellen Authentifizierungsserver.

     ns-cli-prompt> **add authentication vserver** <name> SSL <ipAuthVserver> 443 -authenticationDomain <domainName>

   - Binden Sie die Verhandlungsrichtlinie an den virtuellen Authentifizierungsserver.

     ns-cli-prompt> **bind authentication vserver** <name> -policy <negotiatePolicyName>

6. Ordnen Sie den virtuellen Authentifizierungsserver dem virtuellen Server zur Datenverkehrsverwaltung (Lastausgleich oder Content Switching) zu.

   ns-cli-prompt> **set lb vserver** <name> -authn401 ON -authnVsName <string>

> **Hinweis:**
>
> Ähnliche Konfigurationen können auch auf dem virtuellen Content Switching-Server vorgenommen werden.

7. Überprüfen Sie die Konfigurationen, indem Sie die folgenden Schritte ausführen:
   - Greifen Sie mithilfe des FQDN auf den virtuellen Server zur Datenverkehrsverwaltung zu. Beispiel: Sample
   - Zeigen Sie die Details der Sitzung auf der CLI an.

     ns-cli-prompt> **show aaa session**

Konfigurieren der Kerberos-Authentifizierung auf der GUI

1. Aktivieren Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion.

   Navigieren Sie zu **System** > **Einstellungen**, klicken Sie auf **Basisfunktionen konfigurieren**, und aktivieren Sie die Authentifizierungs-, Autorisierungs- und Überwachungsfunktion.

2. Fügen Sie die Keytab-Datei wie in Schritt 2 der oben genannten CLI-Prozedur beschrieben hinzu.
3. Fügen Sie einen DNS-Server hinzu.

   Navigieren Sie zu **Verkehrsverwaltung > DNS > Namensserver**, und geben Sie die IP-Adresse für den DNS-Server an.

4. Konfigurieren Sie die Aktion und die Richtlinie **aushandeln** .

   Navigieren Sie zu **Sicherheit > AAA - Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Richtlinie**, und erstellen Sie eine Richtlinie mit **Negotiate**als Aktionstyp. Klicken Sie auf **Hinzufügen**, um einen neuen Authentifizierungsverhandlungsserver zu erstellen, oder klicken Sie auf **Bearbeiten**, um die vorhandenen Details zu konfigurieren.

5. Binden Sie die Verhandlungsrichtlinie an den virtuellen Authentifizierungsserver.

   Navigieren Sie zu **Sicherheit > AAA - Anwendungsdatenverkehr > Virtuelle Server**, und ordnen Sie die **Negotiate-Richtlinie**dem virtuellen Authentifizierungsserver zu.

6. Ordnen Sie den virtuellen Authentifizierungsserver dem virtuellen Server zur Datenverkehrsverwaltung (Lastausgleich oder Content Switching) zu.

   Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und geben Sie die entsprechenden Authentifizierungseinstellungen an.

   > **Hinweis:**

> Ähnliche Konfigurationen können auch auf dem virtuellen Content Switching-Server vorgenommen werden.

7. Überprüfen Sie die Konfigurationen wie in Schritt 7 der oben genannten CLI-Prozedur beschrieben.

Konfigurieren der Kerberos-Authentifizierung auf einem Client

October 5, 2021

Die Kerberos-Unterstützung muss im Browser konfiguriert werden, um Kerberos für die Authentifizierung zu verwenden. Sie können jeden Kerberos-kompatiblen Browser verwenden. Anweisungen zum Konfigurieren der Kerberos-Unterstützung in Internet Explorer und Mozilla Firefox folgen. Weitere Browser finden Sie in der Dokumentation des Browsers.

So konfigurieren Sie Internet Explorer für die Kerberos-Authentifizierung

1. Wählen Sie im Menü **Extras** die Option **Internetoptionen**.
2. Klicken Sie auf der Registerkarte **Sicherheit** auf **Lokales Intranet**, und klicken Sie dann auf **Sites**.
3. Stellen Sie im Dialogfeld **Lokales Intranet** sicher, dass die Option Intranetnetzwerk automatisch erkennen aktiviert ist, und klicken Sie dann auf **Erweitert**.
4. Fügen Sie im Dialogfeld **Lokales Intranet** die Websites der Domänen des virtuellen Servers zur Datenverkehrsverwaltung auf der Citrix ADC Appliance hinzu. Die angegebenen Sites werden zu lokalen Intranetsites.
5. Klicken Sie auf **Schließen** oder **OK**, um die Dialogfelder zu schließen.

So konfigurieren Sie Mozilla Firefox für die Kerberos-Authentifizierung

1. Stellen Sie sicher, dass Kerberos ordnungsgemäß auf Ihrem Computer konfiguriert ist.
2. Geben Sie about:config in die URL-Leiste ein.
3. Geben Sie im Textfeld Filter den Wert network.negotiate ein.
4. Ändern Sie network.negotiate-auth.delegation-uris in die Domäne, die Sie hinzufügen möchten.
5. Ändern Sie network.negotiate-auth.trusted-uris in die Domäne, die Sie hinzufügen möchten.

> **Hinweis:** Wenn Sie Windows ausführen, müssen Sie auch sspi in das Filtertextfeld eingeben und die network.auth.use-sspi Option auf Falsch ändern.

Offload der Kerberos-Authentifizierung von physischen Servern

February 24, 2022

Die Citrix ADC Appliance kann Authentifizierungsaufgaben von Servern auslagern. Anstatt die physischen Server die Anforderungen von Clients authentifizieren, authentifiziert der Citrix ADC alle Clientanforderungen, bevor er sie an einen der an ihn gebundenen physischen Server weiterleitet. Die Benutzerauthentifizierung basiert auf Active Directory Token.

Es gibt keine Authentifizierung zwischen Citrix ADC und dem physischen Server, und die Authentifizierungsabladung ist für die Endbenutzer transparent. Nach der ersten Anmeldung an einem Windows-Computer muss der Endbenutzer keine zusätzlichen Authentifizierungsinformationen in einem Pop-up oder auf einer Anmeldeseite eingeben.

In der aktuellen Version der Citrix ADC Appliance ist die Kerberos-Authentifizierung nur für die Authentifizierung, Autorisierung und Überwachung virtueller Server zur Datenverkehrsverwaltung verfügbar. Die Kerberos-Authentifizierung wird für SSL-VPN in der Citrix Gateway Advanced Edition-Appliance oder für die Citrix ADC Appliance-Verwaltung nicht unterstützt.

Die Kerberos-Authentifizierung erfordert eine Konfiguration auf der Citrix ADC Appliance und in Clientbrowsern.

So konfigurieren Sie die Kerberos-Authentifizierung auf der Citrix ADC Appliance

1. Erstellen Sie ein Benutzerkonto in Active Directory. Überprüfen Sie beim Erstellen eines Benutzerkontos die folgenden Optionen im Abschnitt Benutzereigenschaften:
    - Stellen Sie sicher, dass Sie die Option Kennwort bei der nächsten Anmeldung ändern nicht auswählen.
    - Stellen Sie sicher, dass Sie die Option Kennwort nicht ablaufen auswählen.
2. Geben Sie auf dem AD-Server an der CLI-Eingabeaufforderung Folgendes ein:
    - ktpass -princ HTTP/kerberos.crete.lab.net@crete.lab.net -ptype KRB5_NT_PRINCIPAL -mapuser kerbuser@crete.lab.net -mapop set -pass <password> -out C:\kerbtabfile.txt

    > **Hinweis:**
    >
    > Stellen Sie sicher, dass Sie den obigen Befehl in einer einzigen Zeile eingeben. Die Ausgabe des obigen Befehls wird in die Datei C:KerbTabFile.txt geschrieben.
3. Laden Sie die Datei kerbtabfile.txt in das Verzeichnis /etc der Citrix ADC Appliance mit einem Secure Copy (SCP) -Client hoch.
4. Führen Sie den folgenden Befehl aus, um der Citrix ADC Appliance einen DNS-Server hinzuzufügen.

- add dns nameserver 1.2.3.4

Die Citrix ADC Appliance kann Kerberos-Anforderungen ohne den DNS-Server nicht verarbeiten. Stellen Sie sicher, dass Sie denselben DNS-Server verwenden, der in der Microsoft Windows-Domäne verwendet wird.

5. Wechseln Sie zur Befehlszeilenschnittstelle von Citrix ADC.
6. Führen Sie den folgenden Befehl aus, um einen Kerberos-Authentifizierungsserver zu erstellen:

   - add authentication negotiateAction KerberosServer -domain “crete.lab.net” -domainUser kerbuser -domainUserPasswd <password> -keytab /var/mykcd.keytab

   > **Hinweis**
   >
   > Wenn keytab nicht verfügbar ist, können Sie die Parameter domain, domainUser und -domainUserPasswd angeben.

7. Führen Sie den folgenden Befehl aus, um eine Verhandlungsrichtlinie zu erstellen:

   - `add authentication negotiatePolicy Kerberos-Policy ”REQ.IP.DESTIP == 192.168.17.200”KerberosServer<!--NeedCopy-->`

8. Führen Sie den folgenden Befehl aus, um einen virtuellen Authentifizierungsserver zu erstellen.

   - `add authentication vserver Kerb-Auth SSL 192.168.17.201 443 -AuthenticationDomain crete.lab.net<!--NeedCopy-->`

9. Führen Sie den folgenden Befehl aus, um die Kerberos-Richtlinie an den virtuellen Authentifizierungsserver zu binden:

   - `bind authentication vserver Kerb-Auth -policy Kerberos-Policy -priority 100<!--NeedCopy-->`

10. Führen Sie den folgenden Befehl aus, um ein SSL-Zertifikat an den virtuellen Authentifizierungsserver zu binden. Sie können eines der Testzertifikate verwenden, das Sie über die GUI Citrix ADC Appliance installieren können. Führen Sie den folgenden Befehl aus, um das Beispielzertifikat ServerTestCert zu verwenden.

    - `bind ssl vserver Kerb-Auth -certkeyName ServerTestCert<!--NeedCopy-->`

11. Erstellen Sie einen virtuellen HTTP-Lastausgleichsserver mit der IP-Adresse 192.168.17.200.

    Stellen Sie sicher, dass Sie über die Befehlszeilenschnittstelle für NetScaler 9.3-Releases einen virtuellen Server erstellen, wenn sie älter als 9.3.47.8 sind.

12. Führen Sie den folgenden Befehl aus, um einen virtuellen Authentifizierungsserver zu konfigurieren:

- `set lb vserver <name>-authn401 ON -authnVsName Kerb-Auth<!--NeedCopy -->`

13. Geben Sie den Hostnamen Example in die Adressleiste des Webbrowsers ein.

    Der Webbrowser zeigt ein Authentifizierungsdialogfeld an, da die Kerberos-Authentifizierung nicht im Browser eingerichtet ist.

    > **Hinweis:**
    >
    > Die Kerberos-Authentifizierung erfordert eine bestimmte Konfiguration auf dem Client. Stellen Sie sicher, dass der Client den Hostnamen auflösen kann. Dies führt dazu, dass der Webbrowser eine Verbindung zu einem virtuellen HTTP-Server herstellt.

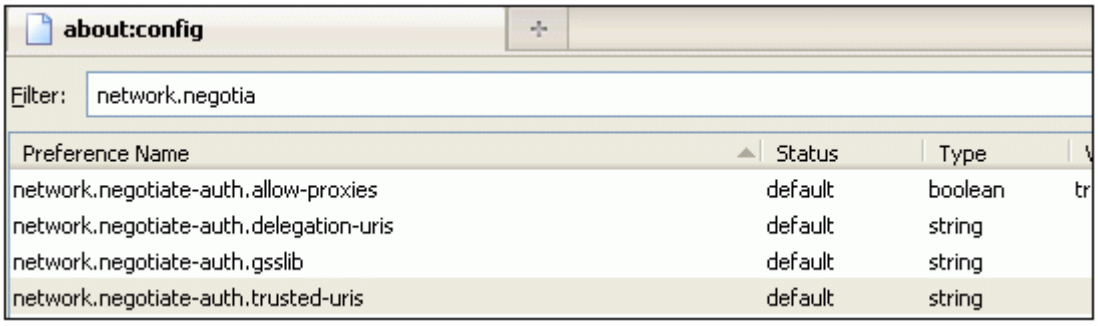
14. Konfigurieren Sie Kerberos im Webbrowser des Clientcomputers.
    - Informationen zur Konfiguration in Internet Explorer finden Sie unter Konfigurieren von Internet Explorer für die Kerberos-Authentifizierung.
    - Informationen zur Konfiguration in Mozilla Firefox finden Sie unter Konfigurieren von Internet Explorer für die Kerberos-Authentifizierung.
15. Überprüfen Sie, ob Sie ohne Authentifizierung auf den physischen Backend-Server zugreifen können.

So konfigurieren Sie Internet Explorer für die Kerberos-Authentifizierung

1. Wählen Sie im Menü **Extras** die Option **Internetoptionen** aus.
2. Aktivieren Sie die Registerkarte **Sicherheit**.
3. Wählen Sie **Lokales Intranet** im Abschnitt “Wählen Sie eine Zone”, um Sicherheitseinstellungen zu ändern.
4. Klicken Sie auf **Sites**.
5. Klicken Sie auf **Erweitert**.
6. Geben Sie die URL an, Beispiel, und klicken Sie auf **Hinzufügen**.
7. Starten Sie **Internet Explorer**neu.

So konfigurieren Sie Mozilla Firefox für die Kerberos-Authentifizierung

1. Geben Sie about:config in die Adressleiste des Browsers ein.
2. Klicken Sie auf den Warnhinweis.
3. Geben Sie **Network.Negotiate-auth.trusted-uris** in das Feld **Filter** ein.
4. Doppelklicken Sie auf **Network.Negotiate-auth.trusted-uris**. Ein Beispielbildschirm wird unten gezeigt.



5. Geben Sie im Dialogfeld Zeichenfolgenwert eingeben www.crete.lab.net ein.
6. Starten Sie Firefox neu.

Problembehandlung für Authentifizierung und Autorisierung

September 1, 2022

Lokalisieren von Fehlermeldungen

Lokalisieren Sie Fehlermeldungen, die vom Citrix ADC nFactor-System generiert wurden

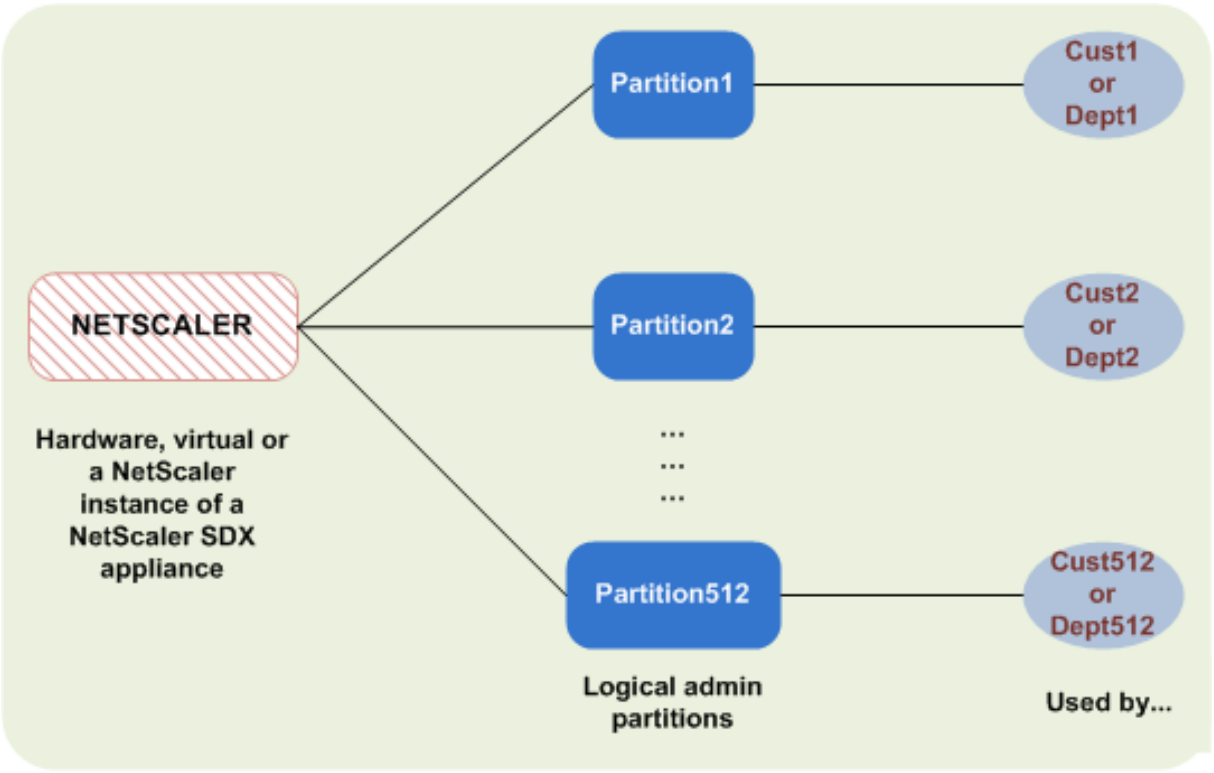
Beheben Sie Authentifizierungsprobleme mit dem Modul aaad.debug

Beheben von Authentifizierungsproblemen in Citrix ADC und Citrix Gateway mit dem Modul aaad.debug

Administrator-Partition

October 5, 2021

Eine Citrix ADC-Appliance kann in logische Entitys partitioniert werden, die als Admin-Partitionen bezeichnet werden Jede Partition kann konfiguriert und als separate Citrix ADC-Appliance verwendet werden. Die folgende Abbildung zeigt die Partitionen eines Citrix ADC, die von verschiedenen Kunden und Abteilungen verwendet werden:



Eine partitionierte Citrix ADC-Appliance verfügt über eine einzelne Standardpartition und eine oder mehrere Admin-Partitionen. Die folgende Tabelle enthält weitere Details zu den beiden Partitionstypen:

> **Hinweis:**
>
> In einer partitionierten Appliance kann der Modus BridgeGPDUs nur in der Standardpartition und nicht in den Administratorpartitionen aktiviert werden.

Verfügbarkeit:

Die Citrix ADC-Appliance wird mit einer einzigen Partition ausgeliefert, die als Standardpartition bezeichnet wird. Die Standardpartition wird auch nach der Partitionierung der Citrix ADC-Appliance beibehalten.

Muss explizit erstellt werden, wie unter Admin-Partitionen konfigurierenbeschrieben.

Anzahl der Partitionen:

Eins

Eine Citrix ADC-Appliance kann eine oder mehrere (maximal 512) Admin-Partitionen haben.

Benutzerzugriff und Rollen:

Alle Citrix ADC-Benutzer, die nicht mit einer *partitionsspezifischen* Befehlsrichtlinie verknüpft sind, können auf die Standardpartition zugreifen und diese konfigurieren. Wie immer schränkt die zugehörige Befehlsrichtlinie die Vorgänge ein, die ein Benutzer ausführen kann.

Der Benutzerzugriff und die Rollen werden von Citrix ADC Superusers erstellt, die auch die Benutzer für diese Partition angeben. Nur Superuser und zugehörige Benutzer der Partition können auf die Admin-Partition zugreifen und diese konfigurieren.

> **Hinweis:**
>
> Partitionsbenutzer haben keinen Shell-Zugriff.

Datei-Struktur:

Alle Dateien in einer Standardpartition werden in der standardmäßigen Citrix ADC-Dateistruktur gespeichert.

Das Verzeichnis */nsconfig* speichert beispielsweise die Citrix ADC-Konfigurationsdatei und das Verzeichnis */var/log/* speichert die Citrix ADC-Protokolle.

Alle Dateien in einer Admin-Partition werden in Verzeichnispfaden gespeichert, die den Namen der Admin-Partition haben.

Beispielsweise wird die Citrix ADC-Konfigurationsdatei (ns.conf) im `/nsconfig/partitions/<partitionName>` Verzeichnis gespeichert. Andere partitionsspezifische Dateien werden in den `/var/partitions/<partitionName>` Verzeichnissen gespeichert.

Einige andere Pfade in einer Admin-Partition:

- Heruntergeladene Dateien: `/var/partitions/<partitionName>/download/`
- Log-Dateien: `/var/partitions/<partitionName>/log/`

> **Hinweis:**
>
> Derzeit wird die Protokollierung auf Partitionsebene nicht unterstützt. Daher ist dieses Verzeichnis leer und alle Protokolle werden im `/var/log/` Verzeichnis gespeichert.

- Dateien im Zusammenhang mit dem SSL-CRL-Zertifikat: `/var/partitions/<partitionName>/netscaler/ssl`

Verfügbare Ressourcen:

Alle Citrix ADC-Ressourcen.

Citrix ADC-Ressourcen, die explizit der Admin-Partition zugewiesen sind.

Benutzerzugriff und Rollen

Bei der Authentifizierung und Autorisierung einer partitionierten Citrix ADC-Appliance kann ein Root-Administrator einer oder mehreren Partitionen einen Partitionsadministrator zuweisen. Der Partitionsadministrator kann Benutzer für diese Partition autorisieren, ohne andere Partitionen zu beeinträchtigen. Die Partitionsbenutzer sind berechtigt, nur über die SNIP-Adresse auf diese Partition zuzugreifen. Sowohl der Root-Administrator als auch der Partitionsadministrator können

den rollenbasierten Zugriff (RBA konfigurieren, indem Benutzer für den Zugriff auf verschiedene Anwendungen autorisiert werden.

Administratoren und Benutzerrollen können wie folgt beschrieben werden:

Root-Administrator. Greift über ihre NSIP-Adresse auf die partitionierte Appliance zu und kann dem Benutzer Zugriff auf eine oder mehrere Partitionen gewähren. Der Administrator kann auch Partitionsadministratoren einer oder mehreren Partitionen zuweisen. Der Administrator kann einen Partitionsadministrator von der Standardpartition mithilfe einer NSIP-Adresse erstellen oder zu einer Partition wechseln und dann einen Benutzer erstellen und einen Partitionsadministratorzugriff mit einer SNIP-Adresse zuweisen.

Partitions-Administrator. Greift über eine vom Root-Administrator zugewiesene NSIP-Adresse auf die angegebene Partition zu. Der Administrator kann rollenbasierten Zugriff auf den Partitionsbenutzerzugriff auf diese Partition zuweisen und auch die externe Serverauthentifizierung mithilfe einer partitionsspezifischen Konfiguration konfigurieren.

Systembenutzer. Greift über die NSIP-Adresse auf Partitionen zu. Hat Zugriff auf die vom Root-Administrator angegebenen Partitionen und Ressourcen.

Benutzer partitionieren. Greift über eine SNIP-Adresse auf eine Partition zu. Das Benutzerkonto wird vom Partitionsadministrator erstellt und der Benutzer hat Zugriff auf Ressourcen, nur innerhalb der Partition.

Wichtige Punkte

Im Folgenden sind einige Punkte aufgeführt, die Sie beim Bereitstellen eines rollenbasierten Zugriffs in einer Partition beachten sollten.

1. Citrix ADC-Benutzer, die über die NSIP-Adresse auf die GUI zugreifen, verwenden die Standard-Partitionsauthentifizierungskonfiguration, um sich bei der Appliance anzumelden.
2. Benutzer von Partitionssystemen, die über eine Partitions-SNIP-Adresse auf die GUI zugreifen, verwenden eine partitionsspezifische Authentifizierungskonfiguration, um sich bei der Appliance anzumelden.
3. Der in einer Partition erstellte Partitionsbenutzer kann sich nicht mit der NSIP-Adresse anmelden.
4. Der an eine Partition gebundene Citrix ADC-Benutzer kann sich nicht mit der SNIP-Adresse der Partition anmelden.
5. Systembenutzer, die sich über einen externen Authentifizierungsserver authentifizieren (z. B. LDAP, RADIUS, TACACS), müssen über eine SNIP-Adresse auf eine Partition zugreifen.

Anwendungsfall für die Verwaltung des rollenbasierten Zugriffs in einem partitionierten Setup

Betrachten Sie ein Szenario, in dem eine Unternehmensorganisation www.example.com mehrere Geschäftseinheiten und einen zentralisierten Administrator hat, der alle Instanzen in ihrem Netzwerk verwaltet. Sie möchten jedoch exklusive Benutzerberechtigungen und -umgebungen für jede Geschäftseinheit bereitstellen.

Im Folgenden finden Sie die Administratoren und Benutzer, die von der Standardkonfiguration für die Partitionsauthentifizierung und partitionenspezifische Konfiguration in einer partitionierten Appliance verwaltet

John: Root-Administrator

George: Partitionsadministrator

Adam: Systembenutzer

Jane: Partitions-Benutzer

John, ist der Root-Administrator einer partitionierten Citrix ADC-Appliance. John verwaltet alle Benutzerkonten und Administratorbenutzerkonten über Partitionen (z. B. P1, P2, P3, P4 und P5) innerhalb der Appliance. John bietet granularen rollenbasierten Zugriff auf Entitäten von der Standardpartition der Appliance. John erstellt Benutzerkonten und weist jedem Konto Partitionszugriff zu. George, der ein Netzwerkingenieur innerhalb der Organisation ist, bevorzugt einen rollenbasierten Zugriff auf wenige Anwendungen, die auf der Partition P2 ausgeführt werden. Basierend auf der Benutzerverwaltung erstellt John eine Partitionsadministratorrolle für George und verknüpft sein Benutzerkonto mit einer Partition-Admin-Befehlsrichtlinie in der P2-Partition. Adam ist ein weiterer Netzwerkingenieur, zieht es vor, auf eine Anwendung zuzugreifen, die auf P2 ausgeführt wird. John erstellt ein Systembenutzerkonto für Adam und verknüpft sein Benutzerkonto einer P2-Partition. Sobald das Konto erstellt wurde, kann sich Adam bei der Appliance anmelden, um über die NSIP-Adresse auf die Citrix ADC-Verwaltungsschnittstelle zuzugreifen, und kann basierend auf der Benutzer-/Gruppenbindung zur Partition P2 wechseln.

Angenommen, Jane, die eine andere Netzwerkingenieurin ist, möchte direkt auf eine Anwendung zugreifen, die nur auf der Partition P2 ausgeführt wird, George (Partitionsadministrator) kann ein Partitionsbenutzerkonto für sie erstellen und ihr Konto mit Befehlsrichtlinien für Autorisierungsberechtigungen verknüpfen. Janes Benutzerkonto, das in der Partition erstellt wurde, ist jetzt direkt mit P2 verknüpft. Jetzt kann Jane über die SNIP-Adresse auf die Citrix ADC-Verwaltungsschnittstelle zugreifen und kann nicht zu einer anderen Partition wechseln.

> **Hinweis:**
>
> Wenn Janes Benutzerkonto von einem Partitionsadministrator in der Partition P2 erstellt wird, kann der Administrator nur über die SNIP-Adresse (die innerhalb der Partition erstellt wurde)

> auf die Citrix ADC-Verwaltungsschnittstelle zugreifen. Dem Administrator ist es nicht gestattet, über die NSIP-Adresse auf die Schnittstelle zuzugreifen. Ebenso, wenn Adams Benutzerkonto von einem Root-Administrator in der Standardpartition erstellt und an eine P2-Partition gebunden ist. Der Administrator kann auf die Citrix ADC-Verwaltungsschnittstelle nur über die NSIP-Adresse oder SNIP-Adresse zugreifen, die in der Standardpartition erstellt wurde (mit aktiviertem Verwaltungszugriff). Und es ist nicht gestattet, über die in der Administratorpartition erstellte SNIP-Adresse auf die Partitionsoberfläche zuzugreifen.

Konfigurieren von Rollen und Zuständigkeiten für Partitionsadministratoren

Im Folgenden finden Sie die Konfigurationen, die von einem Root-Administrator in einer Standardpartition durchgeführt werden.

Erstellen von Administratorpartitionen und Systembenutzern — Ein Root-Administrator erstellt Administratorpartitionen und Systembenutzer in der Standardpartition der Appliance. Der Administrator verknüpft die Benutzer dann verschiedenen Partitionen. Wenn Sie an eine oder mehrere Partitionen gebunden sind, können Sie basierend auf Benutzerbindungen von einer Partition zur anderen wechseln. Außerdem wird Ihr Zugriff auf eine oder mehrere gebundene Partitionen nur vom Root-Administrator autorisiert.

Autorisieren des Systembenutzers als Partitionsadministrator für eine bestimmte Partition — Sobald ein Benutzerkonto erstellt wurde, wechselt der Root-Administrator zu einer bestimmten Partition und autorisiert den Benutzer als Partitionsadministrator. Dies geschieht durch Zuweisen der Partition-Admin-Befehlsrichtlinie dem Benutzerkonto. Jetzt kann der Benutzer als Partitionsadministrator auf die Partition zugreifen und Entitäten innerhalb der Partition verwalten.

Im Folgenden finden Sie die Konfigurationen, die von einem Partitionsadministrator in einer administrativen Partition durchgeführt werden.

Konfigurieren der SNIP-Adresse in einer Administratorpartition- Der Partitionsadministrator meldet sich bei der Partition an und erstellt eine SNIP-Adresse und bietet Verwaltungszugriff auf die Adresse.

Erstellen und Binden eines Partitionssystembenutzers mit Partitionsbefehlsrichtlinie - Der Partitionsadministrator erstellt Partitionsbenutzer und definiert den Umfang des Benutzerzugriffs. Dies geschieht durch Binden des Benutzerkontos an Partitionsbefehlsrichtlinien.

Erstellen und Binden einer Partitionssystem-Benutzergruppen mit Partitionsbefehlsrichtlinie -Der Partitionsadministrator erstellt Partitionsbenutzergruppen und definiert den Umfang des Zugriffs auf Benutzergruppen. Dies geschieht durch Binden des Benutzergruppenkontos an Partitionsbefehlsrichtlinien.

Konfigurieren der externen Serverauthentifizierung für externe Benutzer (optional) -Diese Konfiguration dient zur Authentifizierung externer TACACS-Benutzer, die mit der SNIP-Adresse auf die Partition zugreifen.

Im Folgenden werden die Aufgaben aufgeführt, die beim Konfigurieren des rollenbasierten Zugriffs für Partitionsbenutzer in einer Administratorpartition ausgeführt werden

1. Erstellen einer administrativen Partition — Bevor Sie Partitionsbenutzer in einer Administratorpartition erstellen, müssen Sie zuerst die Partition erstellen. Als Root-Administrator können Sie mit dem Konfigurationsdienstprogramm oder einer Befehlszeilenschnittstelle eine Partition von der Standardpartition erstellen.
2. Benutzerzugriff von der Standardpartition auf Partition P2 wechseln - Wenn Sie Partitionsadministrator von der Standardpartition aus auf die Appliance zugreifen, können Sie von der Standardpartition zu einer bestimmten Partition wechseln. Partitionieren Sie beispielsweise P2 basierend auf Benutzerbindung.
3. Hinzufügen einer SNIP-Adresse zum Partitions-Benutzerkonto mit aktiviertem Verwaltungszugriff - nachdem Sie Ihren Zugriff auf eine Administrationspartition umgestellt haben. Sie erstellen eine SNIP-Adresse und gewähren Verwaltungszugriff auf die Adresse.
4. Erstellen und Binden eines Partitionssystembenutzers mit Partitionsbefehlsrichtlinie - Wenn Sie ein Partitionsadministrator sind, können Sie Partitionsbenutzer erstellen und den Umfang des Benutzerzugriffs definieren. Dies geschieht durch Binden des Benutzerkontos an Partitionsbefehlsrichtlinien.
5. Erstellen und Binden von Partitionsbenutzergruppen mit Partitionsbefehlsrichtlinie - Wenn Sie ein Partitionsadministrator sind, können Sie Partitionsbenutzergruppen erstellen und den Umfang der Benutzerzugriffssteuerung definieren. Dies geschieht durch Binden des Benutzergruppenkontos an Partitionsbefehlsrichtlinien.

Konfigurieren der externen Serverauthentifizierung für externe Benutzer (optional) -Diese Konfiguration dient zur Authentifizierung externer TACACS-Benutzer, die mit einer SNIP-Adresse auf die Partition zugreifen.

Vorteile der Verwendung von Admin-Partitionen

Sie können die folgenden Vorteile nutzen, indem Sie Admin-Partitionen für Ihre Bereitstellung verwenden:

- Ermöglicht die Delegierung des Verwaltungseigentums an eine Anwendung an den Kunden.
- Reduziert die Kosten des ADC-Eigentums, ohne Kompromisse bei Leistung und Benutzerfreundlichkeit einzugehen.
- Schützt vor ungerechtfertigten Konfigurationsänderungen. In einer nicht partitionierten Citrix ADC-Appliance können autorisierte Benutzer der anderen Anwendung absichtlich oder unbeabsichtigt Konfigurationen ändern, die für Ihre Anwendung erforderlich sind. Es kann zu unerwünschtem Verhalten führen. Diese Möglichkeit ist in einer partitionierten Citrix ADC-Appliance reduziert.
- Isoliert den Datenverkehr zwischen verschiedenen Anwendungen durch Verwendung dedizierter VLANs für jede Partition.

- Beschleunigt und ermöglicht die Skalierung von Anwendungsbereitstellungen.
- Ermöglicht die Verwaltung und Berichterstellung auf Anwendungsebene oder lokalisiert.

Lassen Sie uns einige Fälle analysieren, um die Szenarien zu verstehen, in denen Sie Admin-Partitionen verwenden können.

Anwendungsfall 1: Wie Admin-Partition in einem Unternehmensnetzwerk verwendet wird

Betrachten wir ein Szenario, dem ein Unternehmen namens **Foo.com**gegenübersteht.

- **Foo.com** hat einen einzigen Citrix ADC.
- Es gibt fünf Abteilungen und jede Abteilung hat eine Anwendung, die mit dem Citrix ADC bereitgestellt werden muss.
- Jede Anwendung muss unabhängig von einer anderen Gruppe von Benutzern oder Administratoren verwaltet werden.
- Andere Benutzer müssen vom Zugriff auf die Konfigurationen ausgeschlossen werden.
- Die Anwendung oder das Back-End muss Ressourcen wie IP-Adressen teilen können.
- Die globale IT-Abteilung muss in der Lage sein, Einstellungen auf Citrix ADC-Ebene zu steuern, die allen Partitionen gemeinsam sein müssen.
- Die Anwendungen müssen unabhängig voneinander sein. Ein Fehler bei der Konfiguration einer Anwendung darf sich nicht auf die andere auswirken.

Ein nicht partitionierter Citrix ADC könnte diese Anforderungen nicht erfüllen. Sie können jedoch all diese Anforderungen erfüllen, indem Sie einen Citrix ADC partitionieren.

Erstellen Sie einfach eine Partition für jede der Anwendungen, weisen Sie den Partitionen die erforderlichen Benutzer zu, geben Sie für jede Partition ein VLAN an und definieren Sie globale Einstellungen auf der Standardpartition.

Anwendungsfall 2: Wie eine Admin-Partition von einem Dienstanbieter verwendet wird

Betrachten wir ein Szenario, dem ein Dienstanbieter namens **BigProvider**gegenübersteht:

- BigProvider hat 5 Kunden: 3 kleine Unternehmen und 2 große Unternehmen.
- **SmallBiz**, **SmallerBiz**und **StartupBiz** benötigen nur die grundlegendste Citrix ADC-Funktionalität.
- **BigBiz** und **LargeBiz** sind größere Unternehmen und haben Anwendungen, die starken Verkehr anziehen. Sie möchten einige der komplexeren Citrix ADC-Funktionalität nutzen.

In einem nicht partitionierten Ansatz würde der Citrix ADC-Administrator normalerweise eine Citrix ADC SDX-Appliance verwenden und für jeden Kunden eine Citrix ADC-Instanz bereitstellen.

Die Lösung passt zu **BigBiz** und **LargeBiz**, da ihre Anwendungen die unverminderte Leistungsfähigkeit der gesamten nicht partitionierten Citrix ADC-Appliance benötigen. Diese Lösung ist jedoch möglicherweise nicht so kostengünstig für die Wartung von **SmallBiz**, **SmallerBiz**und **StartupBiz**.

Daher entscheidet **BigProvider** für folgende Lösung:

- Verwenden einer Citrix ADC SDX-Appliance zum Aufrufen dedizierter Citrix ADC-Instanzen für **BigBiz** und **LargeBz**.
- Verwenden eines einzelnen Citrix ADC, der in drei Partitionen partitioniert ist, jeweils eine für **SmallBiz**, **SmallerBiz**und **StartupBiz**.

Der Citrix ADC Administrator (Superuser) erstellt eine Admin-Partition für jeden dieser Kunden und gibt die Benutzer für die Partitionen an. Gibt auch die Citrix ADC-Ressourcen für die Partitionen an und gibt das VLAN an, das von dem Datenverkehr verwendet werden soll, der für jede der Partitionen bestimmt ist.

Unterstützung von Citrix ADC-Konfigurationen in der Admin-Partition

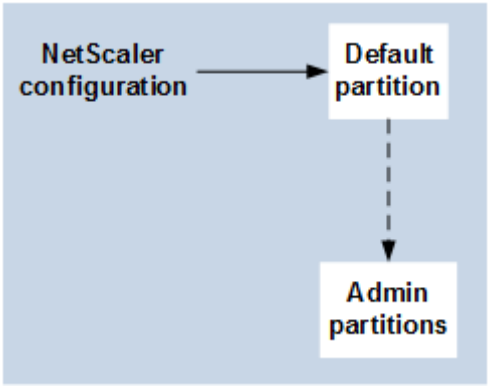
October 5, 2021

Citrix ADC-Konfigurationen können in die folgenden drei Arten von Konfigurationen unterteilt werden. Dies hängt von der Citrix-Konfiguration und der Partition ab, in der die Konfiguration ausgeführt wird.

> **Hinweis:**
>
> - Admin-Partitionen können nicht in einem Citrix ADC-Cluster eingerichtet werden. Dies bedeutet, dass ein Citrix ADC-Cluster nicht partitioniert werden kann.
> - Admin-Partitionen können nicht auf einer Citrix ADC 14000 FIPS-Appliance eingerichtet werden.
> - Fall 3 listet die Citrix ADC-Funktionen auf, die in Admin-Partitionen nicht unterstützt werden.
> - Load Balancing-Vorlagen werden in Admin-Partitionen nicht unterstützt.

Fall 1 (globale Konfigurationen)

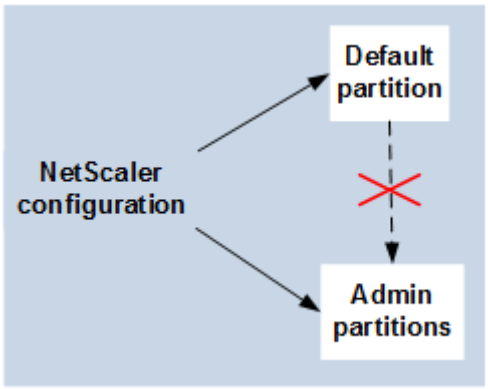
Konfigurationen, die NUR in der Standardpartition ausgeführt werden können und die verfügbar sind oder sich auf alle Admin-Partitionen auswirken.



- Aktualisierungen von integrierten Entitäten für Monitore, TCP-Profile, HTTP-Profile usw.
- Aktualisierungen globaler Parameter für Syslog, NSLOG, Weblog, Content Switching, IPSEC, SIP, DHCP, Überspannungsschutz, TCP-Pufferung und Systemerfassung.
- Hochverfügbarkeits-Konfigurationen (HA)
- Änderungen an Schnittstellen und VLAN
- Benutzerkonfigurationen

Fall 2 (partitionsspezifische Konfigurationen)

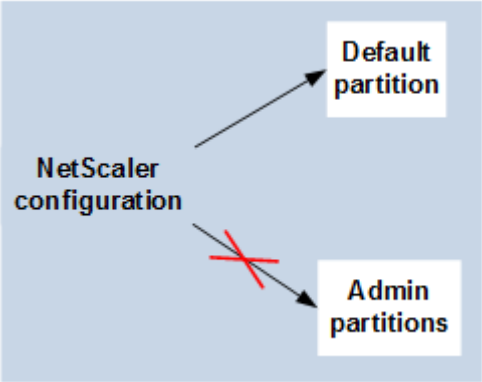
Konfigurationen, die unabhängig in Standard- und Admin-Partitionen durchgeführt werden können. Diese Konfigurationen gelten nur für die Partition, in der sie ausgeführt werden.



- Abrufen von Statistiken zum Verkehrsniveau für eine Partition.
- Der Partitionsadministrator kann IP-Bindungen für VLAN aktualisieren, das an diese Partition gebunden ist. Die Schnittstellenbindungen können jedoch nicht aktualisiert werden.
- Löschen von Citrix ADC-Konfigurationen.
- Funktionsspezifische Parameter für die folgenden Funktionen: AppFlow, AppQoE, HTTP-Komprimierung, DNS, TCP, HTTP, Verschlüsselung, Responder, Rewrite und SSL.
- Funktionsspezifische Konfigurationen wie virtuelle Server, Dienste, Monitore.

Fall 3

Konfigurationen, die auf Admin-Partitionen nicht durchgeführt werden können. Diese Funktionen können in der Standardpartition konfiguriert werden, haben jedoch keine Auswirkungen auf Admin-Partitionen.



> **Hinweis:**
>
> Konfigurationen, die auf Admin-Partitionen für eine bestimmte Version unterstützt werden, werden mit **Ja**gekennzeichnet.

Feature-Komponente	Citrix ADC Feature	NetScaler 11.1	NetScaler 12.0	Citrix ADC 12.1	Citrix ADC 13.0
Netzwerke	Datenverkehrs-Dom	Nein (ab Build 60.13 nicht unterstützt)	Nein	Nein	Nein
Richtlinie	Erweiterbarkeit	Ja	Ja	Ja	Ja
Lastausgleich	DBS Autoscale	Ja	Ja	Ja	Ja
Lastausgleich	DNSSEC	Nein	Nein	Ja	Ja
Lastausgleich	Diameter	Ja	Ja	Ja	Ja
Lastausgleich	RTSP	Nein	Nein	Nein	Nein
Lastausgleich	Sicher Verbinden	Ja	Ja	Ja	Ja
Lastausgleich	Autoscale Servicegruppe	Ja	Ja	Ja	Ja
Verwaltbarkeit	Externe RBA-Authentifizieru	Ja	Ja	Ja	Ja

Feature-Komponente	Citrix ADC Feature	NetScaler 11.1	NetScaler 12.0	Citrix ADC 12.1	Citrix ADC 13.0
Verwaltbarkeit	RISE Cisco	Nein	Nein	Nein	Nein
Verwaltbarkeit	ACI-Cisco	Ja	Ja	Ja	Ja
Verwaltbarkeit	AppExpert	Ja	Ja	Ja	Ja
Verwaltbarkeit	HDX Insight	Nein	Nein	Nein	Nein
Verwaltbarkeit	Insight	Nein	Nein	Nein	Nein
VPN	Citrix CloudBridge Connector	Nein	Nein	Nein	Nein
VPN	Citrix Gateway oder SSL VPN	Nein	Nein	Nein	Nein
VPN	SSL VPN ICA-Proxy	Nein	Nein	Nein	Nein
VPN	Webinterface auf Citrix ADC	Nein	Nein	Nein	Nein
SSL	SSL-Profil	Ja	Ja	Ja	Ja
SSL	SSL-FIPS	Nein	Nein	Nein	Nein
SSL	External-HSM	Nein	Nein	Nein	Nein
Infrarot	Cacheumleitung	Nein	Nein	Nein	Nein
Infrarot	Integriertes Caching	Ja	Ja	Ja	Ja
Netzwerk	VXLAN	Ja	Ja	Ja	Ja
Netzwerk	Ordnungsgemä Herunter-fahren	Ja	Ja	Ja	Ja
Netzwerk	LSN	Nein	Nein	Nein	Nein
Netzwerk	IPv6 Ready Logo	Ja	Ja	Ja	Ja
Network	vPath	Ja	Ja	Ja	Ja
Lastausgleich	Datastream	Ja	Ja	Ja	Ja

Feature-Komponente	Citrix ADC Feature	NetScaler 11.1	NetScaler 12.0	Citrix ADC 12.1	Citrix ADC 13.0
Protokollierung	Web-Protokollierung	Ja	Ja	Ja	Ja
Network	L2 Param/L3 Param	Ja	Ja	Ja	Ja
Network	GRE Tunnel	Ja	Ja	Ja	Ja
Balancing wird geladen	Skriptable-Überwachung	Ja	Ja	Ja	Ja
Lastausgleich	GSLB	Ja	Ja	Ja	Ja
Infrarot	Verbindungsspi	Ja	Ja	Ja	Ja
Infrarot	FEO	Ja	Ja	Ja	Ja
Infrarot	Ns-Spur	Ja	Ja	Ja	Ja
Lastausgleich	Priorität Queuing	Ja	Ja	Ja	Ja
Network	HDOSP	Ja	Ja	Ja	Ja
Network	Netto-Profil	Ja	Ja	Ja	Ja
Network	Netzwerk (eingeschränkte Funktion)	Ja	Ja	Ja	Ja
Network	VRRP (eingeschränkte Funktion)	Ja	Ja	Ja	Ja
Protokollierung	Audit-Protokollierung (SYSLOG-TCP, LB von Syslog-Servern, SNIP-Unterstützung und FQDN-Unterstützung für Syslog)	Ja	Ja	Ja	Ja

Feature-Komponente	Citrix ADC Feature	NetScaler 11.1	NetScaler 12.0	Citrix ADC 12.1	Citrix ADC 13.0
VPN	Citrix Gateway	Nein	Nein	Nein	Nein
VPN	AAA-TM	Ja	Ja	Ja	Ja
AppFlow	AppFlow	Nein	Ja (nur IPFIX)	Ja (nur IPFIX)	Ja
appFW	Anwendungs-Firewall	Nein	Nein	Nein	Nein
URL-Transformation	URL-Transformation	Nein	Nein	Nein	Nein
Lastausgleich	TCP-Pufferung	Nein	Nein	Nein	Nein
Richtlinien	OCSP-Responder	Ja	Ja	Ja	Ja
Auditprotokoll	SYSLOG-TCP	Nein	Ja	Ja	Ja
Optimierung	Front-End-Optimierung	Nein	Ja	Ja	Ja
AppQoE	AppQoE	Ja	Ja	Ja	Ja
BOT	BOT-Verwaltung	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	NEIN

In der vorherigen Tabelle sind einige der Funktionen im Setup der Admin-Partition als **eingeschränkte Funktionen** aufgeführt. Der folgende Abschnitt enthält den Grund, warum einige der Funktionen als **eingeschränkte Funktionen**bezeichnet werden.

- **VRRP**. Das VRRP ist eine eingeschränkte Funktion in der Admin-Partition aufgrund der folgenden Eigenschaften:
  - Das Hinzufügen oder Löschen von VRID kann nur über den Standardpartitionskontext erfolgen. Sobald jedoch eine VRID erstellt wurde, kann sie in nicht standardmäßigen Partitionen verwendet werden.
  - Die VRRP-Funktionalität wird nur über die dedizierten VLANs unterstützt.
  - Die VRRP-Funktionalität wird auf freigegebenen VLANs, die von der Admin-Partition verwendet werden, nicht unterstützt. Es ist intern blockiert. Während der Konfiguration wird keine Fehlermeldung angezeigt. Das Protokoll ist in einem freigegebenen VLAN (markiert oder nicht markiert) blockiert, das an eine Standard- oder eine administrative Partition gebunden ist.

> **Wichtig**
>
> Um die aktiv-aktive Bereitstellung mit VRRP zu unterstützen, müssen Haupt- und Backup-VIP dieselbe VRID verwenden. Verschiedene VRIDs können nicht verwendet werden.

- **Vernetzung**. Einige der Netzwerkkonfigurationen (L2 Param und L3 Param) werden im Partitionskontext nicht unterstützt oder gültig. Wenn Sie auf solche Konfigurationen stoßen, wird die folgende Fehlermeldung angezeigt. "FEHLER: Diese Konfigurationsoption wird auf der nicht standardmäßigen Partition nicht unterstützt. "

Konfigurieren von Administratorpartitionen

October 5, 2021

> **Wichtig**
>
> - Nur Superuser sind berechtigt, Admin-Partitionen zu erstellen und zu konfigurieren.
> - Sofern nicht anders angegeben, müssen Konfigurationen zum Einrichten einer Admin-Partition von der Standardpartition aus erfolgen.

Durch die Partitionierung einer Citrix ADC-Appliance erstellen Sie effektiv mehrere Instanzen einer einzelnen Citrix ADC-Appliance. Jede Instanz hat ihre eigenen Konfigurationen und der Datenverkehr jeder dieser Partitionen ist von der anderen isoliert. Dies geschieht, indem jeder Partition ein dediziertes VLAN oder ein freigegebenes VLAN zugewiesen wird.

Ein partitionierter Citrix ADC verfügt über eine Standardpartition und die erstellten Admin-Partitionen. Um eine Admin-Partition einzurichten, müssen Sie zuerst eine Partition mit den relevanten Ressourcen (Speicher, maximale Bandbreite und Verbindungen) erstellen. Geben Sie dann die Benutzer an, die auf die Partition zugreifen können, und die Berechtigungsstufe für jeden Benutzer auf der Partition.

Der Zugriff auf einen partitionierten Citrix ADC entspricht dem Zugriff auf einen nicht partitionierten Citrix ADC: über die NSIP-Adresse oder eine andere Verwaltungs-IP-Adresse. Nachdem Sie Ihre gültigen Anmeldeinformationen angegeben haben, werden Sie als Benutzer zu der Partition weitergeleitet, an die Sie gebunden sind. Alle von Ihnen erstellten Konfigurationen werden auf dieser Partition gespeichert. Wenn Sie mit mehr als einer Partition verknüpft sind, werden Sie zur ersten Partition weitergeleitet, mit der Sie verknüpft waren. Wenn Sie Entitäten auf einer Ihrer anderen Partitionen konfigurieren möchten, müssen Sie explizit zu dieser Partition wechseln.

Nach dem Zugriff auf die entsprechende Partition werden die von Ihnen durchführenden Konfigurationen auf dieser Partition gespeichert und sind spezifisch für diese Partition.

> **Hinweis:**
>
> - Citrix ADC Superuser und andere Nicht-Partitionsbenutzer werden zur Standardpartition weitergeleitet.
> - Benutzer aller 512 Partitionen können sich gleichzeitig anmelden.

Tipp

Um mithilfe des SNIP (mit aktiviertem Verwaltungszugriff) über HTTPS auf eine partitionierte Citrix ADC-Appliance zuzugreifen, stellen Sie sicher, dass jede Partition über das Zertifikat ihres Partitionsadministrators verfügt. Innerhalb der Partition muss der Partitionsadministrator Folgendes tun:

1. Fügen Sie das Zertifikat dem Citrix ADC hinzu.

   ```
   add ssl certKey ns-server-certificate -cert ns-server.cert-key ns-server.key
   ```

2. Binden Sie es an einen Dienst mit dem Namen `nshttps-<SNIP>-3009`, der durch die SNIP-Adresse ersetzt werden `<SNIP>` muss, in diesem Fall 100.10.10.1.

   ```
   bind ssl service nshttps-100.10.10.1-3009 -certkeyName ns-server-certificate
   ```

Begrenzung der Partitionierung

In einer partitionierten Citrix ADC-Appliance kann ein Netzwerkadministrator eine Partition mit Partitionsressourcen wie Speicher, Bandbreite und Verbindungslimit erstellen, die als unbegrenzt konfiguriert sind. Dies geschieht, indem Null als Partitionsressourcenwert angegeben wird. Wobei Zero angibt, dass die Ressource auf der Partition unbegrenzt ist und bis zu Systemgrenzen verbraucht werden kann. Die Konfiguration von Partitionsressourcen ist nützlich, wenn Sie eine Datenverkehrsdomänenbereitstellung auf eine administrative Partition migrieren oder wenn Sie nichts über das Ressourcenzuweisungslimit für eine Partition in einer bestimmten Bereitstellung wissen.

Das Ressourcenlimit für eine administrative Partition ist wie folgt:

1. **Speicher partitionieren**. Es ist der maximal zugewiesene Speicher für eine Partition. Sie stellen sicher, dass Sie die Werte beim Erstellen einer Partition angeben.

   > **Hinweis:**
   >
   > Ab NetScaler 12.0 können Sie beim Erstellen einer Partition das Speicherlimit auf Null setzen. Wenn bereits eine Partition mit einem bestimmten Speicherlimit erstellt wurde, können Sie das Limit auf einen beliebigen Wert reduzieren oder das Limit auf Null setzen.

   Parameter: MaxMemLimit

Maximaler Speicher wird in MB in einer Partition zugewiesen. Ein Nullwert gibt an, dass der Speicher auf der Partition unbegrenzt ist und bis zu den Systemgrenzen verbraucht werden kann.

Standardwert: 10

2. **Partitionsbandbreite**. Maximal zugewiesene Bandbreite für eine Partition. Wenn Sie ein Limit angeben, stellen Sie sicher, dass es sich innerhalb des lizenzierten Durchsatzes der Appliance befindet. Andernfalls beschränken Sie die Bandbreite, die von der Partition verwendet wird, nicht. Der angegebene Grenzwert ist für die Bandbreite verantwortlich, die die Anwendung benötigt. Wenn die Anwendungsbandbreite das angegebene Limit überschreitet, werden Pakete gelöscht.

   > **Hinweis:**
   >
   > Wenn Sie ab NetScaler 12.0 eine Partition erstellen können, können Sie das Partitionsbandbreitenlimit auf Null setzen. Wenn bereits eine Partition mit einer bestimmten Bandbreite erstellt wurde, können Sie die Bandbreite reduzieren oder das Limit auf Null setzen.

   Parameter: MaxBandWidth

   Die maximale Bandbreite wird in Kbit/s in einer Partition zugewiesen. Ein Nullwert gibt an, dass die Bandbreite uneingeschränkt ist. Das heißt, die Partition kann bis zu den Systemgrenzen verbrauchen.

   Standardwert: 10240

   Maximaler Wert: 4294967295

3. **Partitions-Verbindung**. Maximale Anzahl gleichzeitiger Verbindungen, die in einer Partition geöffnet sein können. Der Wert muss den maximalen gleichzeitigen Fluss berücksichtigen, der innerhalb der Partition erwartet wird. Die Partitionsverbindungen werden aus dem Partitionskontingentspeicher berücksichtigt. Zuvor wurden die Verbindungen aus dem Standardkontingentspeicher der Partition berücksichtigt. Es ist nur clientseitig konfiguriert, nicht für serverseitige Back-End-TCP-Verbindungen. Neue Verbindungen können nicht über diesen konfigurierten Wert hinaus hergestellt werden.

   > **Hinweis:**
   >
   > Ab NetScaler 12.0 können Sie eine Partition erstellen, bei der die Anzahl der offenen Verbindungen auf Null festgelegt ist. Wenn Sie bereits eine Partition mit einer bestimmten Anzahl offener Verbindungen erstellt haben, können Sie das Verbindungslimit reduzieren oder das Limit auf Null setzen.

   Parameter: MaxConnections

   Maximale Anzahl gleichzeitiger Verbindungen, die in der Partition geöffnet sein können. Ein Nullwert gibt an, dass die Anzahl der offenen Verbindungen nicht begrenzt ist.

   Standardwert: 1024

Mindestwert: 0

Maximaler Wert: 4294967295

Konfigurieren Sie eine Administratorpartition

Um eine Admin-Partition zu konfigurieren, führen Sie die folgenden Aufgaben aus.

So greifen Sie mit der CLI auf eine Admin-Partition zu

1. Melden Sie sich bei der Citrix ADC-Appliance an.
2. Prüfen Sie, ob Sie sich in der richtigen Partition befinden. In der Eingabeaufforderung wird der Name der aktuell ausgewählten Partition angezeigt.
3. Wenn ja, fahren Sie mit dem nächsten Schritt fort.
4. Wenn nein, rufen Sie eine Liste der Partitionen auf, mit denen Sie verknüpft sind, und wechseln Sie zur entsprechenden Partition.
   - `show system user <username>`
   - `switch ns partition <partitionName>`
5. Jetzt können Sie die erforderlichen Konfigurationen genauso wie ein nicht partitionierter Citrix ADC durchführen.

So greifen Sie mit der GUI auf eine Admin-Partition zu

1. Melden Sie sich bei der Citrix ADC-Appliance an.
2. Prüfen Sie, ob Sie sich in der richtigen Partition befinden. In der oberen Leiste der GUI wird der Name der aktuell ausgewählten Partition angezeigt.
   - Wenn ja, fahren Sie mit dem nächsten Schritt fort.
   - Wenn nein, navigieren Sie zu **Konfiguration > System > Partitionsverwaltung > Partitionen**, klicken Sie mit der rechten Maustaste auf die Partition, zu der Sie wechseln möchten, und wählen Sie **Wechseln**aus.
3. Jetzt können Sie die erforderlichen Konfigurationen genauso wie ein nicht partitionierter Citrix ADC durchführen.

Eine Admin-Partition hinzufügen

Der Root-Administrator fügt eine Administratorpartition von der Standardpartition hinzu und bindet die Partition an VLAN 2.

So erstellen Sie eine Administratorpartition mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add partition <partitionname>
```

Wechseln des Benutzerzugriffs von der Standardpartition zu einer Admin-Partition

Jetzt können Sie den Benutzerzugriff von der Standardpartition auf die Partition Par1 umstellen.

So wechseln Sie ein Benutzerkonto mit der CLI von der Standardpartition zu einer Admin-Partition:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
Switch ns partition <pname>
```

Hinzufügen von SNIP-Adresse zu einem Partitions-Benutzerkonto mit aktiviertem Verwaltungszugriff

Erstellen Sie in der Partition eine SNIP-Adresse mit aktiviertem Verwaltungszugriff.

So fügen Sie dem Partitions-Benutzerkonto eine SNIP-Adresse hinzu, wobei der Verwaltungszugriff über die Befehlszeilenschnittstelle aktiviert ist:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
> add ns ip <ip address> <subnet mask> -mgmtAccess enabled
```

Erstellen und Binden eines Partitionsbenutzers mit Partitionsbefehlsrichtlinie

Erstellen Sie in der Partition einen Partitionssystembenutzer und binden Sie den Benutzer mit Partition-Admin-Befehlsrichtlinien.

So erstellen und binden Sie einen Partitionssystembenutzer mit der Partitionsbefehlerrichtlinie mithilfe der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
> add system user <username> <password>

Done
```


Erstellen und Binden von Partitionsbenutzergruppen mit Partitionsbefehlsrichtlinie

Erstellen Sie in Partition Par1 eine Partitionssystem-Benutzergruppe und binden Sie die Gruppe mit Partitionsbefehlsrichtlinien wie Partitionsadministrator, Schreibgeschützt Partition, Partitionsoperator oder Partitionsnetzwerk.

So erstellen und binden Sie eine Partitionsbenutzergruppe mit der Befehlszeilenschnittstelle mit der Partitionsbefehlsrichtlinie:

```
1 > add system group <groupName>
2 > bind system group <groupname> (-userName | -policyName <cmdpolicy> <
    priority> | -partitionName)
```

Konfigurieren der externen Serverauthentifizierung für externe Benutzer

In der Partition Par1 können Sie eine externe Serverauthentifizierung konfigurieren, um externe TACACS-Benutzer zu authentifizieren, die über eine SNIP-Adresse auf die Partition zugreifen.

So konfigurieren Sie die externe Serverauthentifizierung für externe Benutzer mithilfe der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 > add authentication tacacsaction <name> -serverip <IP> -tacacsSecret <
    secret key> -authorization ON -accounting ON
2 > add authentication policy <policname> -rule true -action <name>
3 > bind system global <policyname> -priority <value>1
```

Konfigurieren Sie ein Partitionssystem-Benutzerkonto in einer Partition mit der GUI

Um ein Partitionsbenutzerkonto in einer Administratorpartition zu konfigurieren, müssen Sie einen Partitionsbenutzer oder eine Partitionsbenutzergruppe erstellen und diese Partitionsbefehlsrichtlinien binden. Sie können auch die externe Serverauthentifizierung für einen externen Benutzer konfigurieren.

So erstellen Sie ein Partitionsbenutzerkonto in einer Partition mit der GUI

Navigieren Sie zu **System > Benutzerverwaltung**, klicken Sie auf **Benutzer**, um einen Benutzer des Partitionssystems hinzuzufügen, und binden Sie den Benutzer an Befehlsrichtlinien (partitionadmin/partitionread-nur/Partitionoperator/Partitions-Netzwerk).

So erstellen Sie ein Partitions-Benutzergruppenkonto in einer Partition mithilfe der GUI

Navigieren Sie zu **System > Benutzerverwaltung**, klicken Sie auf **Gruppen**, um eine Partitionssystem-Benutzergruppe hinzuzufügen und die Benutzergruppe an Befehlsrichtlinien (partitionadmin/partitionread-nur/Partitionoperator/Partitions-Netzwerk) zu binden.

So konfigurieren Sie die externe Serverauthentifizierung für externe Benutzer mit der GUI

Navigieren Sie zu **System > Authentifizierung > Basisaktionen** und klicken Sie auf **TACACS**, um einen TACACS-Server für die Authentifizierung externer Benutzer zu konfigurieren, die auf die Partition zugreifen.

Beispielkonfiguration

Die folgende Konfiguration zeigt, wie Sie einen Partitionsbenutzer oder eine Partitionsbenutzergruppe erstellen und diese Partitionsbefehlsrichtlinien binden. Außerdem, wie Sie die externe Serverauthentifizierung für die Authentifizierung eines externen Benutzers konfigurieren.

```
1  > add partition Par1
2  > switch ns partition Par1
3  > add ns ip 10.102.29.203 255.255.255.0 -mgmtAccessenabled
4  > add system user John Password
5  > bind system user Jane partition-read-only -priority 1
6  > add system group Retail
7  > bind system group Retail -policyname partition-network 1 (where 1 is
     the priority number)
8  > bind system group Retail -username Jane
9  > add authentication tacacssaction tacuser -serverip 10.102.29.200 -
     tacacsSecret Password -authorization ON -accounting ON
10 > add authentication policy polname -rule true -action tacacsAction
11 > bind system global polname -priority 1
```

Befehlsrichtlinien für eine Partitionsbenutzer und Partitionsbenutzergruppen in administrativer Partition

Befehle zum Autorisieren eines Benutzerkontos innerhalb der Administratorpartition	Befehlsrichtlinien, die in einer Administratorpartition verfügbar sind (integrierte Richtlinien)	Zugriffsart des Benutzerkontos
Systembenutzer hinzufügen	Partition-Admin	SNIP (mit aktiviertem Verwaltungszugriff)
Systemgruppe hinzufügen	Partitions-Netzwerk	SNIP (mit aktiviertem Verwaltungszugriff)
Authentifizierung hinzufügen `<action, policy>`, System global binden `<policy name>`	Partition schreibgeschützt	SNIP (mit aktiviertem Verwaltungszugriff)
Systembenutzer entfernen	Partition-Admin	SNIP (mit aktiviertem Verwaltungszugriff)
Systemgruppe entfernen	Partition-Admin	SNIP (mit aktiviertem Verwaltungszugriff)
`bind system cmdpolicy` an Systembenutzer; `bind system cmdpolicy` zur Systemgruppe	Partition-Admin	SNIP (mit aktiviertem Verwaltungszugriff)

Konfigurieren Sie einen LACP Ethernet-Kanal auf der Standard-Admin-Partition

Mit dem Link Aggregation Control Protocol (LACP) können Sie mehrere Ports zu einer einzigen Hochgeschwindigkeitsverbindung (auch Kanal genannt) kombinieren. Eine LACP-fähige Appliance tauscht LACP Data Units (LACPDU) über den Kanal aus.

Es gibt drei LACP-Konfigurationsmodi, die Sie in der Standardpartition einer Citrix ADC-Appliance aktivieren können:

1. Aktiv. Ein Port im aktiven Modus sendet LACPDUs. Die Link-Aggregation wird gebildet, wenn sich das andere Ende der Ethernet-Verbindung im aktiven oder passiven LACP-Modus befindet.
2. Passiv. Ein Port im passiven Modus sendet LACPDUs nur, wenn er LACPDUs empfängt. Die Link-Aggregation wird gebildet, wenn sich das andere Ende der Ethernet-Verbindung im aktiven LACP-Modus befindet.
3. Deaktivieren: Link-Aggregation wird nicht gebildet.

> **Hinweis:**
>
> Standardmäßig ist die Link-Aggregation in der Standardpartition der Appliance deaktiviert.

LACP tauscht LACPDU zwischen Geräten aus, die über eine Ethernet-Verbindung verbunden sind. Diese Geräte werden normalerweise als Akteur oder Partner bezeichnet.

Eine LACPDU-Dateneinheit enthält die folgenden Parameter:

- LACP-Modus. Aktiv, passiv oder deaktiviert.
- LACP-Timeout. Die Wartezeit vor dem Timing des Partners oder Schauspielers. Mögliche Werte: Long und Short. Standardeinstellung: Long.
- Port-Schlüssel. Um zwischen den verschiedenen Kanälen zu unterscheiden. Wenn der Schlüssel 1 ist, wird LA/1 erstellt. Wenn der Schlüssel 2 ist, wird LA/2 erstellt. Mögliche Werte: Integer von 1 bis 8. 4 bis 8 ist für Cluster CLAG.
- Port-Priorität. Mindestwert: 1. Maximaler Wert: 65535 Standardwert: 32768.
- Systempriorität. Verwendet diese Priorität zusammen mit dem System-MAC, um die System-ID zu bilden, um das System während der LACP-Verhandlungen mit dem Partner eindeutig zu identifizieren. Legt die Systempriorität von 1 und 65535 fest. Der Standardwert ist auf 32768 festgelegt.
- Schnittstelle. Unterstützt 8 Schnittstellen pro Kanal auf NetScaler 10.1 Appliance und unterstützt 16 Schnittstellen pro Kanal auf NetScaler 10.5- und 11.0 Appliances.

Nach dem Austausch von LACPDUs verhandeln Akteur und Partner die Einstellungen und entscheiden, ob die Ports zur Aggregation hinzugefügt werden sollen.

Konfigurieren und überprüfen Sie LACP

Der folgende Abschnitt zeigt, wie LACP in der Admin-Partition konfiguriert und überprüft wird.

So konfigurieren und überprüfen Sie LACP auf einer Citrix ADC-Appliance mithilfe der CLI

1. Aktivieren Sie LACP auf jeder Schnittstelle.

   ```
   set interface <Interface_ID> -lacpMode PASSIVE -lacpKey 1<!--NeedCopy
   -->
   ```

   Wenn Sie LACP auf einer Schnittstelle aktivieren, werden die Kanäle dynamisch erstellt. Wenn Sie LACP auf einer Schnittstelle aktivieren und LacpKey auf 1 setzen, wird die Schnittstelle automatisch an den Kanal LA/1 gebunden.

   > **Hinweis:**
   >
   > Wenn Sie eine Schnittstelle an einen Kanal binden, haben die Kanalparameter Vorrang vor den Schnittstellenparametern, sodass die Interface-Parameter ignoriert werden. Wenn

> ein Kanal dynamisch von LACP erstellt wird, können Sie die Operationen zum Hinzufügen, Binden, Aufheben oder Entfernen auf dem Kanal nicht ausführen. Ein dynamisch von LACP erstellter Kanal wird automatisch gelöscht, wenn Sie LACP auf allen Schnittstellen des Kanals deaktivieren.

2. Legen Sie die Systempriorität fest.

   ```
   set lacp -sysPriority <Positive_Integer><!--NeedCopy-->
   ```

3. Stellen Sie sicher, dass LACP wie erwartet funktioniert.

   “‘show interface

   ```
   ```show channel<!--NeedCopy-->
   ```

   ```
   show LACP<!--NeedCopy-->
   ```

   > **Hinweis:**
   >
   > In einigen Versionen von Cisco Internetwork Operating System (iOS) führt das Ausführen des nativen <VLAN_ID>VLAN-Befehls Switchport trunk dazu, dass der Cisco-Switch LACP-PDUs taggt. Dies führt dazu, dass der LACP-Kanal zwischen dem Cisco-Switch und der Citrix ADC-Appliance ausfällt. Dieses Problem wirkt sich jedoch nicht auf die im vorherigen Verfahren konfigurierten statischen Link-Aggregationskanäle aus.

Speichern Sie die Konfiguration aller Admin-Partitionen von der Standardpartition

Administratoren können die Konfiguration aller Admin-Partitionen gleichzeitig von der Standardpartition aus speichern.

Speichern Sie alle Admin-Partitionen von der Standardpartition mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
save ns config -all
```

Unterstützung für partitions- und clusterbasierte benutzerdefinierte Berichte

Die Citrix ADC GUI zeigt nur die benutzerdefinierten Berichte an, die in der aktuellen Anzeigepartition oder im Cluster erstellt wurden.

Zuvor wurde die Citrix ADC GUI verwendet, um die Namen des benutzerdefinierten Berichts direkt in der Back-End-Datei zu speichern, ohne die zu differenzierende Partition oder den Clusternamen zu erwähnen.


```

**So zeigen Sie die benutzerdefinierten Berichte der aktuellen Partition oder des aktuellen Clusters in der GUI an**

- Navigieren Sie zur Registerkarte **Reporting** .
- Klicken Sie auf **Benutzerdefinierte Berichte**, um die Berichte anzuzeigen, die in der aktuellen Partition oder im Cluster erstellt wurden.

### Unterstützung zum Binden globaler VPN-Zertifikate in einem partitionierten Setup für OAuth IdP

In einem partitionierten Setup können Sie die Zertifikate jetzt für OAuth-IdP-Bereitstellungen an VPN global binden.

**So binden Sie die Zertifikate im Partitiontion-Setup mit der CLI**

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind vpn global [-certkeyName <string>] [-userDataEncryptionKey <string
    >]
```

VLAN-Konfiguration für Admin-Partitionen

October 5, 2021

VLANs können als “dediziertes” VLAN oder als “freigegebenes” VLAN an eine Partition gebunden werden. Basierend auf Ihrer Bereitstellung können Sie ein VLAN an eine Partition binden, um den Netzwerkverkehr von anderen Partitionen zu isolieren.

Dediziertes VLAN — Ein VLAN, das nur an eine Partition gebunden ist und die Option “Sharing” deaktiviert ist und ein getaggtes VLAN sein muss. Beispielsweise erstellt ein Systemadministrator in einer Client-Server-Bereitstellung aus Sicherheitsgründen für jede Partition auf der Serverseite ein dediziertes VLAN.

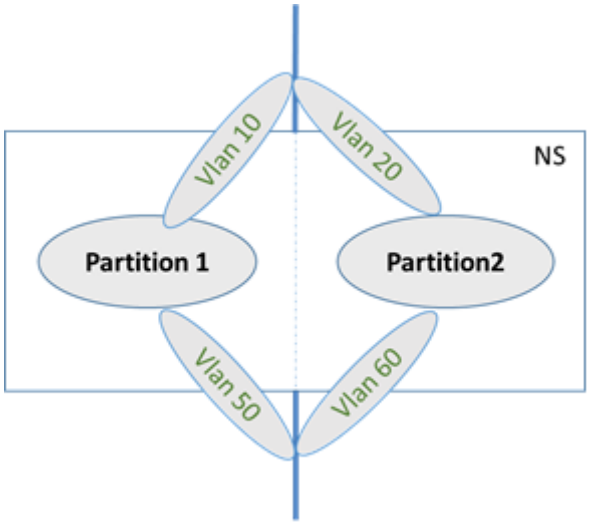
Gemeinsames VLAN — Ein VLAN, das mit aktivierter Option “Sharing” an mehrere Partitionen gebunden (gemeinsam genutzt) ist. Wenn der Systemadministrator beispielsweise in einer Client-Server-Bereitstellung keine Kontrolle über das clientseitige Netzwerk hat, wird ein VLAN erstellt und über mehrere Partitionen freigegeben.

Gemeinsames VLAN kann über mehrere Partitionen hinweg verwendet werden. Es wird in der Standardpartition erstellt und Sie können ein freigegebenes VLAN an mehrere Partitionen binden. Standardmäßig ist ein freigegebenes VLAN implizit an die Standardpartition gebunden und kann daher nicht explizit gebunden werden.

> **Hinweis:**
>
> - Eine Citrix ADC Appliance, die auf einer beliebigen Hypervisor-Plattform (ESX, KVM, Xen und Hyper-V) bereitgestellt wird, muss sowohl die folgenden Bedingungen in einer Partitionseinrichtung als auch in einer Datenverkehrsdomäne erfüllen:
>   - Enable the promiscuous mode, MAC changes, MAC spoofing, or forged transmit for shared VLANs with partition.
>   - Enable the VLAN with port group properties of the virtual switch, if the traffic is through a dedicated VLAN.
> - In einer partitionierten (mandantenanten) Citrix ADC Appliance kann ein Systemadministrator den Datenverkehr isolieren, der zu einer bestimmten Partition oder Partitionen fließt. Dies geschieht durch Binden eines oder mehrerer VLANs an jede Partition. Ein VLAN kann für eine Partition oder für mehrere Partitionen freigegeben werden.

Dedizierte VLANs

Um den Datenverkehr zu isolieren, der in eine Partition fließt, erstellen Sie ein VLAN und ordnen es der Partition zu. Das VLAN ist dann nur für die zugeordnete Partition sichtbar, und der Datenverkehr, der durch das VLAN fließt, wird nur in der zugeordneten Partition klassifiziert und verarbeitet.



Gehen Sie folgendermaßen vor, um ein dediziertes VLAN für eine bestimmte Partition zu implementieren.

1. Fügen Sie ein VLAN (V1) hinzu.

2. Binden Sie eine Netzwerkschnittstelle an VLAN als getaggte Netzwerkschnittstelle.
3. Erstellen Sie eine Partition (P1).
4. Binden Sie Partition (P1) an das dedizierte VLAN (V1).

Konfigurieren Sie Folgendes mit der CLI

- Erstellen Sie ein VLAN

  ```
  add vlan <id>
  ```

Beispiel

```
1     add vlan 100
```

- Binden Sie ein VLAN

  ```
  bind vlan <id> -ifnum <interface> -tagged
  ```

Beispiel

```
1     bind vlan 100  - ifnum 1/8 -tagged
```

- Erstellen Sie eine Partition

  ```
  Add ns partition <partition name> [-maxBandwidth <positive_integer>][-
  maxConn <positive_integer>] [-maxMemLimit <positive_integer>]
  ```

Beispiel

```
1     Add ns partition P1  - maxBandwidth 200  - maxconn 50  - maxmemlimit
         90
2
3     Done
```

- Binden einer Partition an ein VLAN

  ```
  bind partition <partition-id> -vlan <id>
  ```

Beispiel

```
1     bind partition P1  - vlan 100
```


Konfigurieren eines dedizierten VLAN mit der Citrix ADC GUI

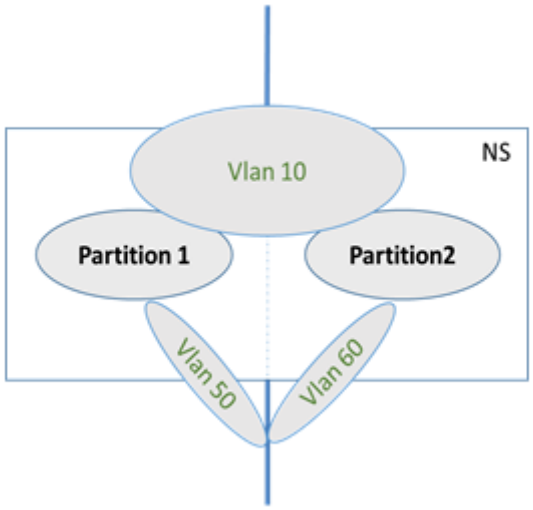
1. Navigieren Sie zu **Konfiguration > System > Netzwerk > VLANs*** und klicken Sie auf **Hinzufügen**, um ein VLAN zu erstellen.
2. Legen Sie auf der Seite **VLAN erstellen** die folgenden Parameter fest:
   - VLAN-ID
   - Aliasname
   - Maximale Übertragungseinheit
   - Dynamisches Routing
   - Dynamisches IPv6-Routing
   - Partitionenfreigabe
3. Wählen Sie im Abschnitt **Schnittstellenbindungen** eine oder mehrere Schnittstellen aus und binden Sie sie an das VLAN.
4. Wählen Sie im Abschnitt **IP-Bindings** eine oder mehrere IP-Adressen aus und binden Sie an das VLAN.
5. Klicken Sie auf **OK** und **Fertig**.

Gemeinsames VLAN

In einer freigegebenen VLAN-Konfiguration verfügt jede Partition über eine MAC-Adresse, und der im freigegebenen VLAN empfangene Datenverkehr wird nach MAC-Adresse klassifiziert. Es wird nur ein Layer3-VLAN empfohlen, da es den Subnetzdatenverkehr einschränken kann. Eine Partitions-MAC-Adresse ist nur für eine gemeinsam genutzte VLAN-Bereitstellung anwendbar und wichtig.

> **Hinweis:**
>
> Ab Citrix ADC Version 12.1 Build 51.16 unterstützt gemeinsam genutztes VLAN in einer partitionierten Appliance dynamisches Routingprotokoll.

Das folgende Diagramm zeigt, wie ein VLAN (VLAN 10) über zwei Partitionen gemeinsam genutzt wird.



Gehen Sie folgendermaßen vor, um eine freigegebene VLAN-Konfiguration bereitzustellen:

1. Erstellen Sie ein VLAN mit der Freigabeoption ‘aktiviert’, oder aktivieren Sie die Freigabeoption in einem vorhandenen VLAN. Standardmäßig ist die Option deaktiviert.
2. Binden Sie die Partitionsschnittstelle an gemeinsam genutztes VLAN.
3. Erstellen Sie die Partitionen mit jeweils einer eigenen PartitionMac-Adresse.
4. Binden Sie die Partitionen an das gemeinsam genutzte VLAN.

Konfigurieren eines gemeinsam genutzten VLANs mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um VLAN hinzuzufügen oder den Freigabe-Parameter eines vorhandenen VLANs festzulegen:

```
add vlan <id> [-sharing (ENABLED | DISABLED)]

set vlan <id> [-sharing (ENABLED | DISABLED)]

add vlan 100  - sharing ENABLED

set vlan 100  - sharing ENABLED
```

Binden einer Partition an ein freigegebenes VLAN mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind partition <partition-id> -vlan <id>
```



```
2
3 bind partition P1 -vlan 100
4
5 add ns partition P1 -maxBandwidth 200 -maxconn 50 -maxmemlimit 90
    -partitionMAC<mac_addr
6
7 Done
```

Konfigurieren einer Partition MAC-Adresse mit der CLI

```
1 set ns partition <partition name> [-partitionMAC<mac_addr>]
2
3 set ns partition P1 -partitionMAC 22:33:44:55:66:77
```

Binden von Partitionen an ein freigegebenes VLAN über die Befehlszeilenschnittstelle

```
1 bind partition <partition-id> -vlan <id>
2
3 bind partition <partition-id> -vlan <id>
4
5 bind partition P1 -vlan 100
6
7 bind partition P2 -vlan 100
8
9 bind partition P3 -vlan 100
10
11 bind partition P4 -vlan 100
```

Konfigurieren von freigegebenem VLAN mit der Citrix ADC GUI

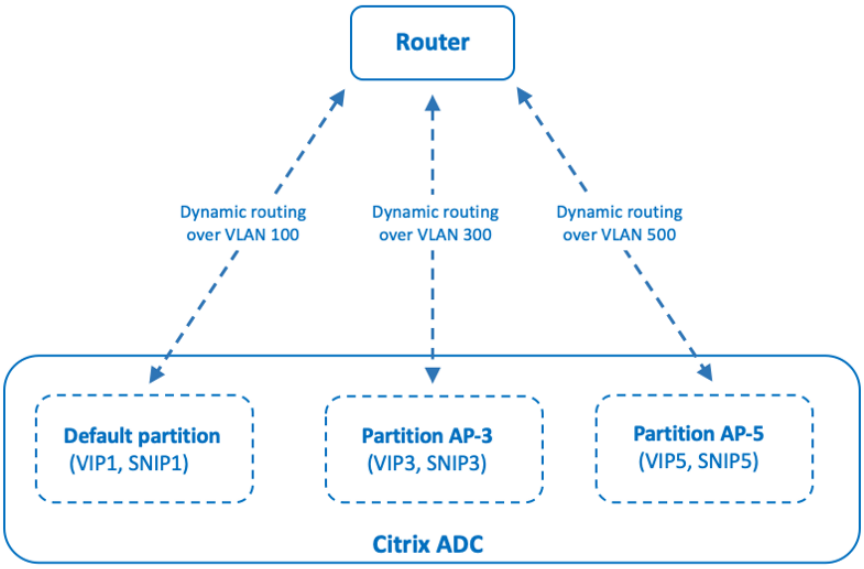
1. Navigieren Sie zu **Konfiguration > System > Netzwerk > VLANs**, wählen Sie ein **VLAN-Profil** aus, und klicken Sie auf **Bearbeiten**, um den Partitionsparameter festzulegen.
2. Aktivieren Sie auf der Seite **VLAN erstellen** das Kontrollkästchen **Partitionsfreigabe**.
3. Klicken Sie auf **OK** und dann auf **Fertig**.

Dynamisches Routing über ein gemeinsames VLAN über Admin-Partitionen

Admin-Partitionen in einer Citrix ADC Appliance bieten eine Möglichkeit, mehrere Mandanten zu hosten.

Ab Citrix ADC Version 12.1 Build 51.16 unterstützt ein gemeinsam genutztes VLAN in einer partitionierten Appliance das dynamische Routing-Protokoll. Routing kann in dedizierten oder gemeinsam genutzten VLANs konfiguriert werden, die mit Admin-Partitionen verknüpft sind.

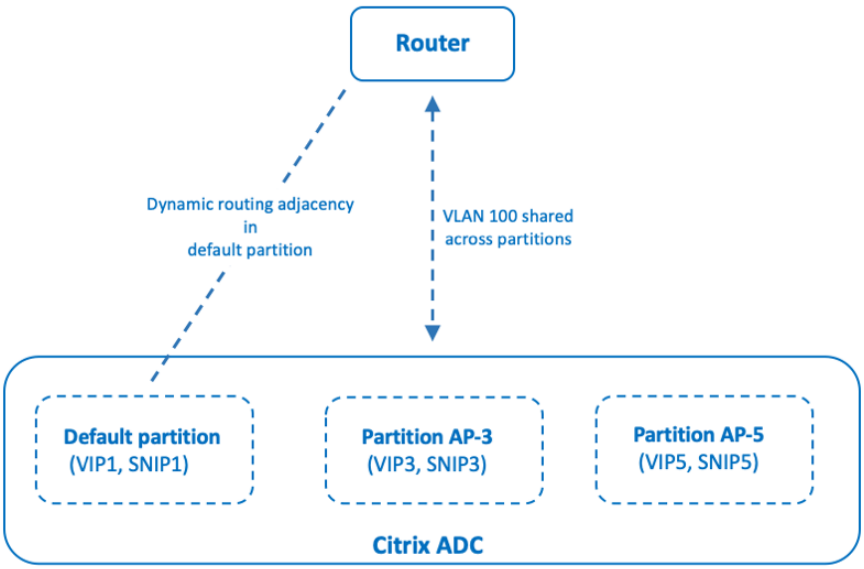
Dediziertes VLAN einer Admin-Partition. In einem dedizierten VLAN wird der Datenpfad für den Mandanten mithilfe eines oder mehrerer VLANs identifiziert. Dies führt zu einer strengen Konfiguration und Datenpfad-Isolation für den Mandanten. Um den Zustand einer VIP-Adresse zu bewerben, ist dynamisches Routing in jeder Partition aktiviert und die Routing-Nachbarschaft wird pro Partition festgelegt.



Dynamic routing over a dedicated VLAN per partition

Ein gemeinsames VLAN für Admin-Partitionen. In einem freigegebenen VLAN können VIP-Adressen, die in einer nicht standardmäßigen Partition konfiguriert sind, über eine einzige Adjacency oder ein Peering in der Standardpartition angekündigt werden. Eine SNIP-Adresse in der nicht standardmäßigen Partition wird als Next-Hop für alle VIP-Adressen (konfiguriert mit der Option **advertiseOnDefaultPartition**) in dieser nicht standardmäßigen Partition verwendet. Die konfigurierte SNIP-Adresse wird in den Routing-Advertisements als Next-Hop-IP-Adresse gekennzeichnet.

Betrachten Sie ein Beispiel-Setup von Admin-Partitionen in einer Citrix ADC Appliance, VLAN 100 wird über die Standardpartition und nicht standardmäßige Partitionen freigegeben: AP-3 und AP-5. SNIP-Adressen SNIP1 wird in der Standardpartition hinzugefügt, SNIP3 wird in AP-3 hinzugefügt und SNIP5 wird in AP-5 hinzugefügt. SNIP1, SNIP3 und SNIP5 sind über den VLAN-100 erreichbar. VIP-Adressen VIP1 wird in der Standardpartition hinzugefügt, VIP3 wird in AP-3 hinzugefügt und VIP5 wird in AP-5 hinzugefügt. VIP3 und VIP5 werden über die einzelne Nachbarschaft oder das Peering in der Standardpartition beworben.



Dynamic routing over a shared VLAN across partitions

Voraussetzungen

Bevor Sie dynamisches Routing über ein freigegebenes VLAN in einer nicht standardmäßigen Admin-Partition konfigurieren, sollten Sie Folgendes sicherstellen:

- **Dynamisches Routing wird auf dem gemeinsam genutzten VLAN in der Standardpartition konfiguriert**. Die Konfiguration des dynamischen Routings für das freigegebene VLAN in der Standardpartition umfasst die folgenden Schritte:
  1. Aktivieren Sie dynamisches Routing auf dem gemeinsam genutzten VLAN.
  2. Fügen Sie eine SNIP-IP-Adresse mit aktiviertem dynamischem Routing hinzu. Diese SNIP-IP-Adresse wird für dynamisches Routing mit dem Upstream verwendet.
  3. Binden Sie das SNIP-IP-Subnetz an das freigegebene VLAN.
- **Ein oder mehrere dynamische Routingprotokolle ist auf der Standardpartition konfiguriert**. Weitere Informationen finden Sie unter Konfigurieren dynamischer Routingprotokolle.

Konfigurationsschritte

Die Konfiguration des dynamischen Routings über ein freigegebenes VLAN in einer nicht standardmäßigen Admin-Partition umfasst die folgenden Schritte:

1. **Fügen Sie eine SNIP-IP-Adresse in der nicht standardmäßigen Partition**hinzu. Diese SNIP-IP-Adresse muss sich im selben Subnetz der SNIP-IP-Adresse befinden, die für dynamisches Routing in der Standardpartition verwendet wird.

2. **Legen Sie die folgenden Parameter für die Werbung für eine VIP-Adresse in einer nicht standardmäßigen Partition mithilfe von dynamischem Routing fest oder aktivieren Sie sie**.
    - Host-Routen-Gateway (hostRtGw). Setzen Sie diesen Parameter auf die im vorherigen Schritt hinzugefügte SNIP-Adresse.
    - Werben auf Standardpartition (advertiseOnDefaultPartition). Aktivieren Sie diesen Parameter.

Beispielkonfiguration

Betrachten Sie ein Beispiel für ein Admin-Partitions-Setup in einer Citrix ADC Appliance. Auf dieser Appliance ist eine nicht standardmäßige Admin-Partition AP-3 konfiguriert. Ein gemeinsames VLAN-VLAN100 ist an AP-3 gebunden. Die folgende Beispielkonfiguration konfiguriert das dynamische Routing über VLAN100 in AP-3.

Schritte	Beispielkonfiguration
Auf Standard-Admin-Partition	-
Aktivieren Sie dynamisches Routing auf gemeinsam genutztem VLAN 100.	`set vlan 100 -dynamicRouting enabled`
Fügen Sie die SNIP-IP-Adresse 192.0.2.10 mit aktiviertem dynamischem Routing hinzu.Diese SNIP-IP-Adresse wird für dynamisches Routing mit dem Upstream verwendet.	`add ns ip 192.0.2.10 255.255.255.0 -type SNIP -dynamicRouting enabled`
Binden Sie ein Subnetz von 192.0.2.10 an gemeinsam genutztes VLAN 100.	`bind vlan 100 -IPAddress 192.0.2.10 255.255.255.0`
Auf nicht standardmäßiger Admin-Partition AP-3	-
Fügen Sie die SNIP-IP-Adresse 192.0.2.30 hinzu. Diese SNIP-IP-Adresse befindet sich im selben Subnetz wie die SNIP-IP-Adresse 192.0.2.10 auf der Standardpartition.	`add ns ip 192.0.2.30 255.255.255.0 -type SNIP`
Um die VIP-Adresse 203.0.113.300 mit dynamischem Routing zu bewerben, aktivieren Sie den `advertiseOnDefaultPartition` Parameter und setzen Sie den `hostRtGw`Parameter auf 192.0.2.30.	`set ns ip 203.0.113.300 255.255.255.255 -hostRoute enabled -advertiseOnDefaultPartition enabled -hostRtGw 192.0.2.30`

Dynamisches Routing von IPv6 über ein freigegebenes VLAN über eine Admin-Partition

Die `set L3Param -ipv6DynamicRouting ENABLED` Befehle `enable ns feature IPv6PT` und müssen aktiviert sein, damit eine IPv6-Adresse dynamisch über ein freigegebenes VLAN in einer Admin-Partition weiterleiten kann. Die folgenden Beispielkonfigurationen helfen Ihnen, das dynamische Routing von IPv6 über gemeinsam genutztes VLAN zu konfigurieren.

Beispielkonfiguration

Die folgende Beispielkonfiguration konfiguriert das dynamische Routing über VLAN 100 in AP-3.

Schritte	Beispielkonfiguration
Auf Standard-Admin-Partition	-
Aktivieren Sie dynamisches Routing auf gemeinsam genutztem VLAN 100.	`set vlan 100 -dynamicRouting enabled`
Fügen Sie die SNIP-IP-Adresse 2001:b:c:d 1/64 hinzu, wobei dynamisches Routing aktiviert ist.Die SNIP-IP-Adresse wird für das dynamische Routing mit dem Upstream verwendet.	`add ns ip6 2001:b:c:d::1/64 -type SNIP -dynamicRouting enabled`
Binden Sie Subnetz von 2001:b:c:d 1/64 an gemeinsam genutztes VLAN 100.	`bind vlan 100 -IPAddress 2001:b:c:d::1/64`
Auf nicht standardmäßiger Admin-Partition AP-3	-
Fügen Sie die SNIP-IP-Adresse 2001:b:c:d 2/64 hinzu. Diese SNIP-IP-Adresse befindet sich im selben Subnetz wie die SNIP-IP-Adresse 2001:b:c:d 2/64 auf der Standardpartition.	`add ns ip6 2001:b:c:d::2/64 -type SNIP`
Aktivieren Sie für Werbung VIP-Adresse 2002 1/128 mit dynamischem Routing den `advertiseOnDefaultPartition` Parameter und setzen Sie den `ip6hostRtGw`Parameter auf 2001:b:c:d 2.	`set ns ip6 2002::1/128 -hostRoute enabled -advertiseOnDefaultPartition enabled -ip6hostRtGw 2001:b:c:d::2`

Der in der Admin-Partition vorhandene VIP muss auf VTYSH der Standardpartition als Kernel-Route angezeigt werden.


```
> switch partition default
Done

>vtysh
ns#

ns# sh ipv6 route kernel

IPv6 routing table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
   IA - OSPF inter area, E1 - OSPF external type 1,
   E2 - OSPF external type 2, I - IS-IS, B - BGP
Timers: Uptime

K      2002::1/128 via 2001:b:c:d::2, vlan0, 01:24:15
                                  >> on Default Partition, VIP : 2002::1
   present in AP known via SNIP6 : 2001:b:c:d::2 is present in AP as a
   Kernel Route
```

Es kann im Upstream angekündigt werden, indem die Option “Kernel weiterverteilen” unter OspFv3/BGP+ in der Standardpartition verwendet wird.

```
ns# sh run router ipv6 ospf
!
router ipv6 ospf 1
redistribute kernel
!
```

Gemeinsames VLAN mit Admin-Partition auf der Citrix ADC SDX-Appliance

Auf der SDX-Appliance müssen Sie die PMAC-Adresse über die Benutzeroberfläche des Verwaltungsdienstes generieren und konfigurieren, bevor Sie die Administratorpartitionen mit gemeinsam genutzten VLANs verwenden. Mit dem Verwaltungsdienst können Sie Partitions-MAC-Adressen wie folgt generieren:

- Verwenden einer Basis-MAC-Adresse
- Angeben benutzerdefinierter MAC-Adressen
- Zufällige Generierung von MAC-Adressen

Hinweis:

- Die zufällig generierenden MAC-Adressen werden für andere Bereitstellungen als Hochverfügbarkeit verwendet.
- Nachdem Sie die MAC-Adressen der Partition generiert haben, müssen Sie die Citrix ADC Instanz neu starten, bevor Sie die Admin-Partitionen konfigurieren. Weitere Informationen zum Generieren von Partitions-MAC-Adressen von der SDX-Appliance finden Sie unter Generieren von PartitionsMAC-Adressen zum Konfigurieren der Admin-Partition auf einer Citrix ADC-Instanz in der SDX Appliance

VXLAN-Unterstützung für Admin-Partitionen

October 5, 2021

In einer partitionierten Citrix ADC Appliance, ähnlich wie beim Konfigurieren eines VLAN, können Sie ein VXLAN in der Standardpartition konfigurieren. Nachdem Sie ein VXLAN konfiguriert haben, können Sie es an eine administrative Partition binden oder wenn ein VXLAN ein VLAN erweitert, das an eine Partition gebunden ist, bindet die Appliance das VXLAN an die Partition unter derselben Broadcastdomäne. Es ist anwendbar, um ein VLAN aufzuheben, das ein VXLAN von der Partition entbindet.

Weitere Informationen zur Funktionsweise von VXLAN in einer Citrix ADC Appliance finden Sie unter VXLAN.

Weitere Informationen zur Funktionsweise von VLAN in einer partitionierten Citrix ADC Appliance finden Sie unter Admin-Partitionierung.

Punkte, die vor der Konfiguration eines VXLAN zu beachten sind

Beachten Sie die folgenden Punkte, bevor Sie ein VXLAN in einer partitionierten Citrix ADC Appliance konfigurieren:

- Wenn Sie ein VLAN über VXLAN erweitern, stellen Sie sicher, dass VLAN an die Partition gebunden ist.
- Nur ein Partitionsadministrator muss die IP und das dynamische Routing für den VXAN in der administrativen Partition konfigurieren.

Ein freigegebenes VXLAN wird in einer partitionierten Appliance nicht unterstützt und daher kann ein VXLAN nicht mit einem freigegebenen VLAN gekennzeichnet werden, oder Sie können ein VLAN nicht zu einem freigegebenen VLAN machen, wenn es mit einem VXLAN gekennzeichnet ist.

Unterstützbare VXLAN-Konfigurationen

Im Folgenden sind die unterstützbaren VXLAN-Konfigurationen.

Erweiterung des VLANs über ein VXLAN in derselben Broadcast-Domain

Die folgenden CLI-Schritte helfen Ihnen, ein VLAN über ein VXLAN und umgekehrt innerhalb derselben Broadcast-Domain zu erweitern.

1. Hinzufügen eines VLAN in der Standardpartition

```
add vlan <id>
```

2. Erweitern Sie VLAN über ein VXLAN innerhalb derselben Broadcastdomäne.

```
add vxlan <vxlan id>  - vlan <id>
```

3. Konfigurieren Sie einen Peer `vtep`, der den gesamten BUM-Verkehr (Broadcast unbekannten Multicast) trägt.

> **Hinweis:**
>
> Die Adresse `vtep` kann eine Multicast-Adresse sein.

```
add bridgetable -mac <mac_addr> -vxlan <positive_integer> -vtep <
   ip_addr> [-vni <positive_integer>][-deviceVlan <
   positive_integer>]
```

4. Binden Sie IP-Adressen an VXLAN.

```
bind vxlan <id> [-srcIP <ip_addr>][-IPAddress <ip_addr|ipv6_addr
   |*> [<netmask>]]
```

5. Binden Sie VLAN an eine administrative Partition.

```
bind partition <partition-id> -vxlan <id>

add vlan 3000

```



```
add vxlan 3000  -vlan 10

add bridgetable  -mac 00:00:00:00:00:00  -vxlan 3000 -vtep
    10.102.58.8  -vni 11

bind vxlan 3000  -  srcIP 10.102.101.15

bind partition p1  -vlan 10
```

SNMP-Unterstützung für Administratorpartitionen

October 5, 2021

Eine partitionierte Citrix ADC Appliance verwendet die SNMP-Infrastruktur zur Begrenzung der Partitionsrate und zur Überwachung der Details zur Nutzung von Partitionsressourcen.

SNMP-Traps für die Begrenzung der Admin-Partitionsrate

Bei einer partitionierten Citrix ADC Appliance kann ein PARTITION-RATE-LIMIT neun SNMP-Traps generieren, um zu benachrichtigen, dass eine Partitionsressource (z. B. Bandbreite, Verbindung oder Speicher) ihre Grenze erreicht oder wieder normal ist.

Die folgenden neun SNMP-Traps werden generiert, wenn:

- **partitionCONNThresholdReached**. Die Anzahl der aktiven Verbindungen für eine Partition überschreitet ihren hohen Schwellenwert.
- **partitionCONNThresholdNormal**. Die Anzahl der aktiven Verbindungen ist kleiner oder gleich dem normalen Schwellenwert Prozentsatz.
- **partitionBWThresholdReached**. Die Bandbreitenauslastung der Partition erreicht ihren hohen Schwellenwert.
- **partitionMEMThresholdReached**. Die aktuelle Speicherbelegung der Partition überschreitet ihren hohen Schwellenwert.
- **partitionMEMThresholdNormal**. Die aktuelle Speicherbelegung der Partition wird kleiner oder gleich dem normalen Schwellenwert Prozentsatz.
- **partitionMEMLimitExceeded.** Die aktuelle Speicherbelegung der Partition überschreitet den Prozentsatz des Speichergrenzwerts.
- **partitionCONNLimitExceeded**. Die Anzahl der aktiven Verbindungen für eine Partition überschreitet das konfigurierte Limit, und neue Verbindungen werden gelöscht.
- **partitionCONNLimitNormal**. Die Anzahl der aktiven Verbindungen für eine Partition unterschreitet die konfigurierte Grenze und die Partition kann nun eine neue Verbindung akzeptieren.

- **partitionBWLimitExceeded**. Die aktuelle Bandbreitenauslastung für eine Partition hat das konfigurierte Limit überschritten.

Die Schwellenwerte für die SNMP-Traps sind nicht konfigurierbar und lauten wie folgt:

- Hoher Schwellenwert = 80% (gilt für alle Partitionsraten-Limit Traps)
- Niedriger Schwellenwert = 60% (gilt für alle Partitionsbegrenzungsfallen)
- Speicherlimit = 95% (gilt nur für Partitionsspeicher-Traps)

Configuring PARTITION-RATE-LIMIT alarm

Um den ARM PARTITION-RATE-LIMIT in einer bestimmten Partition zu konfigurieren und die Generierung der SNMP-Trap-Nachrichten zu ermöglichen.

1. Enable PARTITION-RATE-LIMIT Alarm
2. Configure PARTITION-RATE-LIMIT Alarm
3. SNMP-Trap-Ziel konfigurieren

So aktivieren Sie den PARTITION-RATE-LIMIT-Alarm mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
enable snmp alarm PARTITION-RATE-LIMIT

show snmp alarm PARTITION-RATE-LIMIT
```

So konfigurieren Sie den PARTITION-RATE-LIMIT-Alarm mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set snmp alarm PARTITION-RATE-LIMIT [-state ( ENABLED | DISABLED )] [-
    severity <severity>] [-logging ( ENABLED | DISABLED )]
```

So konfigurieren Sie das SNMP-Trap-Ziel mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:


```
add snmp trap <trapClass> <trapDestination> [-version <version>] [-td <
    positive_integer>] [-destPort <port>] [-communityName <string>] [-
    srcIP <ip_addr|ipv6_addr>] [-severity <severity>] [-allPartitions (
    ENABLED | DISABLED )]
```

So konfigurieren Sie den Alarm für Partitionsraten-Limit mit der GUI

Navigieren Sie zu **System > SNMP > Alarms**, wählen Sie **PARTITION-RATE-LIMIT-Alarm** und konfigurieren Sie die Alarmparameter.

So konfigurieren Sie das SNMP-Trap-Ziel mit der GUI

Navigieren Sie zu **System > SNMP > Trap**und geben Sie die IP-Adresse des Zielgeräts an.

SNMP-Überwachung für Partitionsressourcennutzung

Mithilfe von SNMP können Sie die Ressourcennutzung (z. B. Bandbreite, Verbindung und Speicher) einer Partition in Echtzeit auf einer Citrix ADC Appliance überwachen. Dies geschieht durch Senden einer SNMP-Anforderung (wie SNMP GET, SNMP GET BULK, SNMP GETNEXT oder SNMP WALK) vom SNMP-Manager.

> **Hinweis:**
>
> Um die Partitionsressourcen zu überwachen, müssen Sie die SNMP-Community in der Standardpartition konfigurieren. Dabei wird die *PartitionTable* in der Standardpartition beibehalten, und die SNMP-Kommunikation erfolgt über die NSIP-Adresse der Appliance.

Stellen Sie sich ein Szenario vor, in dem ein Citrix ADC Administrator die Bandbreitenauslastung der Partition P1 auf der Appliance wissen möchte. Der SNMP-Manager ruft diese Informationen ab, indem er eine SNMP-GET-Anforderung für die entsprechende OID (PartitionCurrentBandWidth) an die NSIP-Adresse der Appliance sendet. Der SNMP-Agent auf der Standardpartition ruft die aktuelle Bandbreitennutzung von P1 über die NSIP-Adresse ab und sendet sie an den SNMP-Manager.

Die folgende Tabelle listet die SNMP-Leistungsindikatoren, die Teil von *PartitionTable* sind, und ihre Beschreibung auf:

SNMP-Parameter	SNMP OID	Beschreibung
partitionName	1.3.6.1.4.1.5951.4.1.1.88.1.1	Partitionsname
partitionCurrentBandwidth	1.3.6.1.4.1.5951.4.1.1.88.1.2	Aktuelle Bandbreitennutzung der Partition.

SNMP-Parameter	SNMP OID	Beschreibung
partitionCurrentConnections	1.3.6.1.4.1.5951.4.1.1.88.1.3	Aktuelle Anzahl der aktiven Verbindungen der Partition.
partitionMemoryUsagePcnt	1.3.6.1.4.1.5951.4.1.1.88.1.4	Aktuelle Speichernutzung (in Prozent) der Partition.

Überwachungsprotokollunterstützung für Administratorpartitionen

October 5, 2021

Auf einer partitionierten Citrix ADC Appliance können Sie zur Verbesserung der Datensicherheit die Überwachungsprotokollierung in einer administrativen Partition mithilfe erweiterter Richtlinien konfigurieren. Beispielsweise möchten Sie möglicherweise Protokolle (Zustände und Statusinformationen) einer bestimmten Partition anzeigen. Es hat mehrere Benutzer, die basierend auf ihren Berechtigungsstufen in der Partition auf verschiedene Funktionen zugreifen.

Wichtige Punkte

1. Die von der Partition generierten Audit-Logs werden als eine einzige Protokolldatei (/var/log/ns.log) gespeichert.
2. Konfigurieren Sie die Subnetzadresse des Audit Log-Servers (Syslog oder NS-Log) als Quell-IP-Adresse in der Partition zum Senden der Audit-Log-Nachrichten.
3. Die Standardpartition verwendet den NSIP als Quell-IP-Adresse für die Überwachungsprotokollmeldungen standardmäßig.
4. Sie können die Audit-Protokoll-Meldung anzeigen, indem Sie den Befehl “Audit-Nachrichten anzeigen” verwenden.

Informationen zur Konfiguration des Audit-Logs finden Sie unter Konfigurieren der NetScaler Appliance für die Audit-Protokollierung.

Konfigurieren der Überwachungsprotokollierung in partitionierter Citrix ADC Appliance

Führen Sie die folgenden Aufgaben aus, um die Überwachungsprotokollierung in einer administrativen Partition zu konfigurieren.

1. Konfigurieren Sie die IP-Adresse des Partitionssubnetzes. Eine IPv4 SNIP-Adresse einer administrativen Partition.

2. Konfigurieren Sie die audit-log-Aktion (Syslog und ns log). Eine Überwachungsaktion ist eine Sammlung von Informationen, die die zu protokollierenden Nachrichten und die Protokollierung der Nachrichten auf dem externen Protokollserver angibt.
3. Konfigurieren Sie Audit-Log (Syslog und NS-Log) -Richtlinien. Audit-Log-Richtlinien definieren Protokollmeldungen für die Quellpartition auf den Syslog- oder nslog-Server.
4. Binden Sie die Überwachungsprotokollrichtlinie an die Entität SysGlobal und NSGlobal. Binden Sie eine Audit-Log-Richtlinie an eine globale Systemeinheit.
5. Überprüfen der Audit-Protokoll-Statistiken. Zeigt die Audit-Log-Statistiken an und wertet die Konfiguration aus.

Konfigurieren Sie Folgendes mit der CLI

1. Erstellen der Subnetz-IP-Adresse einer Partition

   ```
   add ns ip <ip address> <subnet mask>
   ```

2. Erstellen einer Syslog-Aktion

   ```
   add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel
    <logLevel> [-dateFormat (MMDDYYYY | DDMMYYYY )] [-transport ( TCP |
   UDP )]
   ```

3. Erstellen einer NS-Protokollaktion

   ```
   add audit nslogAction <name> <serverIP> [-serverPort <port>] -logLevel
   <logLevel> [-dateFormat (MMDDYYYY | DDMMYYYY )]
   ```

4. Erstellen einer Syslog-Audit-Log-Richtlinien

   ```
   add audit syslogpolicy syslog-pol1 true audit-action1
   ```

5. Erstellen einer ns-Log-Audit-Protokoll-Richtlinien

   ```
   add audit nslogpolicy nslog-pol1 true audit-action1
   ```

6. Binden einer Audit-Log-Richtlinie an die SysLogGlobal-Entität

   ```
   bind audit sysloglobal -policyName <name> -priority <priority_integer>
    -globalBindType SYSTEM_GLOBAL
   ```

7. Binden einer Audit-Log-Richtlinie an NSLOGGlobal-Entität

   ```
   bind audit nslogglobal -policyName <name> -priority <priority_integer>
   -globalBindType SYSTEM_GLOBAL
   ```

8. Anzeigen einer Audit-Log-Statistiken

   ```
   stat audit -detail
   ```


Beispiel

```
add ns ip 10.102.1.1 255.255.255.0
add audit syslogAction syslog_action1 10.102.1.2 -logLevel
    INFORMATIONAL -dateFormat MMDDYYYY -transport UDP
add audit syslogpolicy syslog-pol1 true syslog_action1
bind audit sysloggloba l -policyName syslog-pol1 -priority 1 -
    globalBindType SYSTEM_GLOBAL
```

Speichern von Protokollen

Wenn der SYSLOG- oder NSLOG-Server Protokollinformationen von allen Partitionen sammelt, werden sie als Protokollmeldungen in der Datei ns.log gespeichert. Die Protokollmeldungen enthalten die folgenden Informationen:

- Partitionsname.
- Die IP-Adresse.
- Ein Zeitstempel.
- Meldungstyp
- Die vordefinierten Protokollebenen (Kritisch, Fehler, Hinweis, Warnung, Information, Debug, Alert und Emergency)
- Die Nachrichteninformationen.

Anzeige konfigurierter PMAC-Adressen für freigegebene VLAN-Konfiguration

October 5, 2021

Um ein Partitions-Setup mit freigegebener VLAN-Konfiguration zu verwenden, benötigen Sie eine virtuelle MAC-Adresse, die als Partitions-MAC-Adresse (PMAC) bezeichnet wird. Die Partition verwendet die PMAC-Adresse für ihre Kommunikation im freigegebenen VLAN. Für jede Partition wird eine eindeutige PMAC-Adresse konfiguriert und sie wird über alle gemeinsam genutzten VLANs verwendet, die an diese Partition gebunden sind. Bei einer Nicht-SDX-Plattform (VPX oder MPX) kann die PMAC-Adresse entweder vom Benutzer angegeben oder intern von einer Citrix ADC Appliance generiert werden. Wenn die PMAC-Adresse für eine Partition nicht angegeben ist, wird sie intern generiert, wenn die Partition an das erste freigegebene VLAN gebunden ist. Während im Fall einer SDX-Plattform die PMAC-Adressen immer zuerst vom SVM Tool konfiguriert und dann einer Partition zugewiesen werden müssen.

Um eine Liste der konfigurierten PMACs anzuzeigen, können Sie den Befehl **Show ns PartitionMac** verwenden. Mit dem Befehl können Sie die konfigurierten PMACs entweder über die Citrix ADC CLI oder GUI überprüfen. Der Befehl zeigt alle PMAC-Adressen und die entsprechenden Partitionen an (falls zugewiesen). Im Fall einer Nicht-SDX-Plattform zeigt der Befehl alle PMAC-Adressen und ihre entsprechenden Partitionen an, da die PMAC-Adresse einer Partition nur auf Bedarfsbasis zugewiesen wird (wenn eine Partition ein gemeinsam genutztes VLAN gebunden ist). Im Fall einer SDX-Plattform haben Sie jedoch möglicherweise einige nicht zugewiesene PMACs in der Liste.

Informationen zum Generieren von PMAC für die SDX-Plattform finden Sie unter Generieren von Partitions-MAC-Adressen .

Anzeige von PMACs mit der Citrix ADC CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
show ns partitionMAC
```

```
1 Partition MAC Partition Name
2
3 1) f2:0c:64:da:f6:d7
4
5 2) b4:0c:43:da:f6:d2
6
7 3) a6:e7:b2:6c:48:e0
8
9 Done
```

Anzeige von PMAC-Adressen mit der Citrix ADC GUI

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zu **Konfiguration > System > Partition MAC**.
2. Auf der Seite Partition MAC wird eine Liste der PMACs und ihrer Partitionen angezeigt.

AppExpert

October 5, 2021

Die folgenden Themen enthalten eine konzeptionelle Referenz und Konfigurationsanweisungen für AppExpert und andere Funktionen der Citrix ADC Appliance.

> **Hinweis:**
>
> Informationen zu Richtlinienerweiterungen finden Sie unter Richtlinienerweiterungen.

- Action Analytics: Sammelt Laufzeitstatistiken auf der Grundlage vordefinierter Kriterien. Wenn Sie mit Richtlinien verwendet werden, bietet Ihnen die Funktion auch die Infrastruktur für die automatische Optimierung des Datenverkehrs in Echtzeit.
- AppExpert AppExpert Applications and Templates: Vereinfachen Sie Konfigurationsschritte für die Citrix® NetScaler® Appliance mithilfe von Anwendungen, Anwendungsvorlagen, Citrix Gateway-Anwendungen und Entitätsvorlagen.
- AppQoe: Quality of Experience (AppQoE) auf Anwendungsebene integriert mehrere vorhandene richtlinienbasierte Sicherheitsfunktionen der Citrix ADC Appliance in ein einziges integriertes Feature, das einen neuen Warteschlangenmechanismus, Fair Queuing, nutzt.
- Entitätsvorlage: Beschreibt, wie Entitätsvorlagen zum Einrichten und Konfigurieren einzelner Citrix ADC-Entitäten wie eine Richtlinie oder ein virtueller Server verwendet werden. Eine Entitätsvorlage stellt eine Spezifikation und eine Reihe von Standardeinstellungen für das Objekt bereit.
- HTTP-Callouts: Eine HTTP-Anforderung, die die Citrix ADC Appliance generiert und an eine externe Anwendung sendet, wenn bestimmte Kriterien bei der Richtlinienbewertung erfüllt sind.
- Pattern-Sets: Erlaubt den Zeichenfolgenabgleich während der Auswertung einer Standardsyntaxrichtlinie.
- Richtlinien und Ausdrücke: Regeln, die die Vorgänge bestimmen, die die Citrix ADC Appliance ausführen muss.
- Ratenbegrenzung: Definiert die maximale Last für eine bestimmte Netzwerkentität oder eine virtuelle Entität auf der Citrix ADC Appliance.
- Responder: Basiert Antworten darauf, wer die Anfrage sendet, woher sie gesendet wird, und andere Kriterien mit Auswirkungen auf die Sicherheit und das Systemmanagement.
- Umschreiben: Schreibt Informationen in den von der Citrix ADC Appliance behandelten Anfragen oder Antworten neu.
- String-Maps: Führen Sie einen Musterabgleich in allen Citrix ADC-Features durch, die die Standardrichtlinie verwenden.

Aktionsanalysen

October 5, 2021

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

Wenn sich die Website oder Anwendung nicht häufig ändert, können Sie Produkte verwenden, die statistische Daten sammeln, und dann die Statistiken manuell analysieren und die Bereitstellung von Inhalten optimieren. Wenn Sie jedoch keine manuellen Optimierungen durchführen möchten oder wenn Ihre Website oder Anwendung dynamisch ist, benötigen Sie eine Infrastruktur, die nicht nur statistische Daten sammeln kann, sondern auch automatisch die Bereitstellung von Ressourcen auf Basis der Statistiken optimieren kann. Auf der Citrix ADC Appliance wird diese Funktionalität durch die Aktionsanalysefunktion bereitgestellt. Das Feature funktioniert auf einer einzelnen Citrix ADC Appliance und sammelt Laufzeitstatistiken auf der Grundlage von Kriterien, die Sie definieren. Bei Verwendung mit Citrix ADC Richtlinien bietet das Feature auch die Infrastruktur, die Sie für die automatische Optimierung des Datenverkehrs in Echtzeit benötigen.

Beim Konfigurieren der Aktionsanalyse-Funktion geben Sie die Anforderungsattribute an, für die Sie statistische Daten sammeln möchten, z. B. URLs und HTTP-Methoden, indem Sie Standard-Syntaxausdrücke in einer Entität, die als Selektor bezeichnet wird, konfigurieren. Anschließend konfigurieren Sie einen Bezeichner, um Einstellungen wie das Stichprobenintervall und die Anzahl der Stichproben zu konfigurieren. Außerdem konfigurieren Sie eine Richtlinie, die es der Appliance ermöglicht, den Datenverkehr gemäß dem Selektor-Bezeichner-Paar auszuwerten. Schließlich binden Sie die Richtlinie an einen Bindepunkt, um mit dem Sammeln von Statistiken zu beginnen.

Die Appliance stellt Ihnen außerdem eine Reihe integrierter Selektoren, Bezeichner und Responder-Richtlinien zur Verfügung, die Sie verwenden können, um mit der Funktion zu beginnen.

Die Appliance aggregiert die folgenden Statistiken:

- Die Anzahl der Anforderungen.
- Die Bandbreite, die von den Anforderungen verbraucht wird.
- Die Reaktionszeit.
- Die Anzahl gleichzeitiger Verbindungen.

Sie können die Funktion so konfigurieren, dass die Datensätze für ein Attribut Ihrer Wahl Laufzeitsortierung ausgeführt werden. Sie können die statistischen Daten mit der Befehlszeilenschnittstelle oder des Tools Stream-Sitzungen im Konfigurationsdienstprogramm anzeigen.

Konfigurieren eines Selektors

October 5, 2021

Ein Selektor ist ein Filter zur Identifizierung von Anforderungen. Es besteht aus bis zu fünf einzelnen Standardsyntaxausdrücken, die Anforderungsattribute wie die Client-IP-Adresse und die URL in der Anforderung identifizieren. Jeder Ausdruck ist ein nicht zusammengesetzter Standardsyntaxausdruck und wird als in einer AND- Beziehung zu den anderen Ausdrücken betrachtet. Im Folgenden sind einige Beispiele für Selektorausdrücke:

- `HTTP.REQ.URL`
- `CLIENT.IP.SRC`
- `HTTP.RES.BODY(1000).AFTER_STR("<string>").BEFORE_STR("<string>")"`
- `CLIENT.IP.SRC.SUBNET(24)`

Selektoren werden in Konfigurationen mit Ratenbegrenzung und Aktionsanalysen verwendet. Ein Selektor ist in einer ratenbegrenzenden Konfiguration optional, ist aber in einer Action-Analytics-Konfiguration erforderlich.

Die Reihenfolge, in der Sie Parameter angeben, ist signifikant. Wenn Sie beispielsweise eine IP-Adresse und eine Domäne (in dieser Reihenfolge) in einem Selektor konfigurieren und dann die Domäne und die IP-Adresse (in umgekehrter Reihenfolge) in einem anderen Selektor angeben, betrachtet Citrix ADC diese Werte als eindeutig. Dies kann dazu führen, dass dieselbe Transaktion zweimal gezählt wird. Wenn mehrere Richtlinien denselben Selektor aufrufen, kann der Citrix ADC erneut dieselbe Transaktion mehrmals zählen.

Wenn Sie einen Ausdruck in einem Selektor ändern, erhalten Sie möglicherweise einen Fehler, wenn eine Richtlinie, die ihn aufruft, an eine neue Richtlinienbezeichnung oder einen neuen Bindepunkt gebunden ist. Angenommen, Sie erstellen einen Selektor namens MyLimitSelector1, rufen ihn aus MyLimitid1 auf und rufen den Bezeichner aus einer DNS-Richtlinie namens DNSrateLimit1 auf. Wenn Sie den Ausdruck in MyLimitSelector1 ändern, wird möglicherweise eine Fehlermeldung angezeigt, wenn Sie DNSrateLimit1 an einen neuen Bindepunkt binden. Die Problemumgehung besteht darin, diese Ausdrücke zu ändern, bevor die Richtlinien erstellt werden, die sie aufrufen.

Die Citrix ADC Appliance bietet integrierte Selektoren pdf für einige der häufigsten Anwendungsfälle. Siehe PDF.

Sie können auch einen Selektor mit Ausdrücken konfigurieren, die die Anforderungsattribute Ihrer Wahl identifizieren. Beispielsweise können Sie einen Datensatz für eine Anforderung erstellen, die mit einer bestimmten Kopfzeile eintrifft. Um die Kopfzeile auszuwerten, können `HTTP.REQ.HEADER("<header_name>")` Sie dem Selektor hinzufügen, den Sie verwenden möchten.

So konfigurieren Sie einen Selektor mit der Befehlszeilenschnittstelle:

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

- `add stream selector <name> <rule> ...`
- `show stream selector`

Beispiel

```
> add stream selector myselector HTTP.REQ.URL CLIENT.IP.SRC
 Done
> show stream selector myselector
    Name: myselector
    Expressions:
        1) HTTP.REQ.URL
        2) CLIENT.IP.SRC
 Done
>
<!--NeedCopy-->
```

So ändern oder entfernen Sie einen Selektor mit der Befehlszeilenschnittstelle:

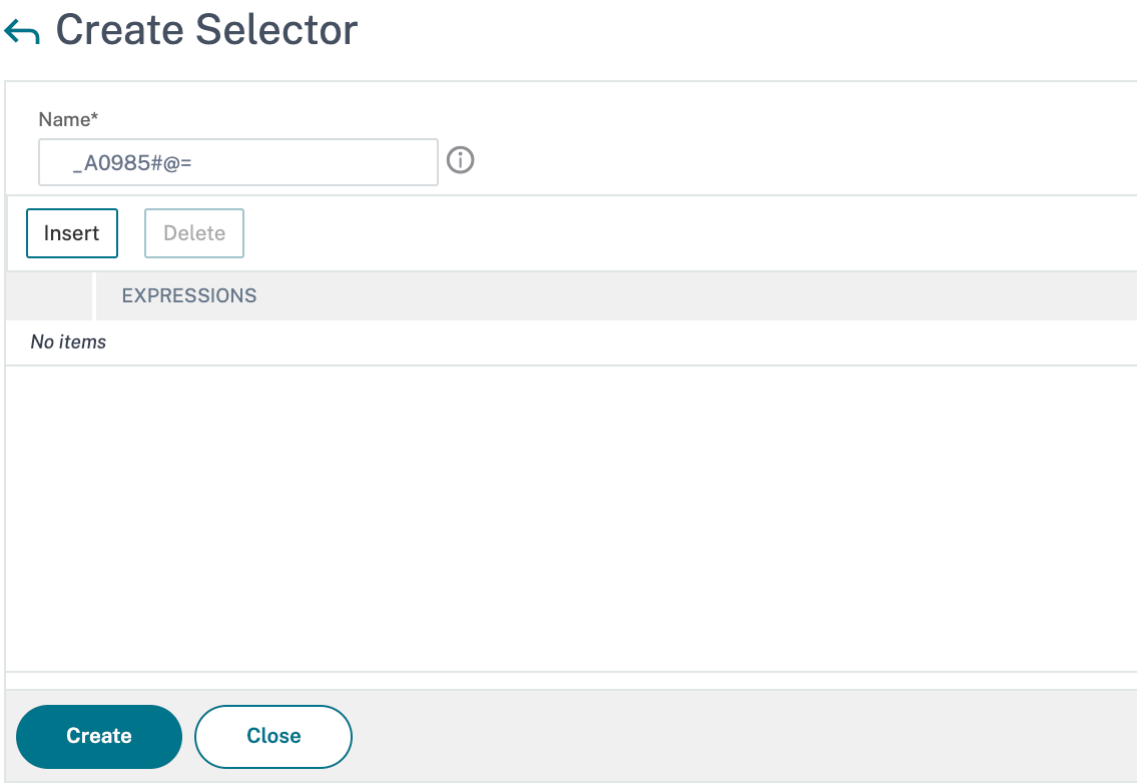
- Um einen Selektor zu ändern, geben Sie den Befehl set stream selector, den Namen des Selektors und den Regelparameter mit den Ausdrücken ein. Geben Sie die vorhandenen Ausdrücke ein, die Sie behalten möchten, zusammen mit den neuen Ausdrücken, die Sie hinzufügen möchten.
- Um einen Selektor zu entfernen, geben Sie den Befehl rm stream selector und den Namen des Selektors ein.

So konfigurieren Sie einen Selektor mit der GUI:

1. Navigieren Sie zu **AppExpert** > **Action Analytics** > **Selektoren** .
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um einen Selektor zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um einen Selektor zu ändern, wählen Sie den Selektor aus, und klicken Sie dann auf **Bearbeiten**.
3. **Legen Sie auf der Seite Auswahl erstellen** oder **Auswahl konfigurieren** die folgenden Parameter fest:
   - Name. Um einen Namen für den Selektor hinzuzufügen, geben Sie den Namen in das Feld **Name** ein. Der Name muss mit ASCII, alphanumerischem Zeichen oder Unterstrichen beginnen. Der Name darf nur alphanumerische ASCII-, Unterstrich-, Hash-, Punkt-, Leerzeichen-, Doppelpunkt-, Gleich- und Bindestriche enthalten.
   - Ausdrücke. Um den Ausdruck zur Selektorkonfiguration hinzuzufügen, klicken Sie auf **Einfügen**. Um einen Ausdruck aus der Selektorkonfiguration zu entfernen, wählen Sie im Feld

Ausdruck den Ausdruck aus, und klicken Sie dann auf **Löschen**. Hinweis: Geben Sie im Feld Ausdrücke einen gültigen Parameter ein. Geben Sie beispielsweise HTTP ein. Geben Sie dann einen Punkt nach diesem Parameter ein. Es wird ein Dropdownmenü angezeigt. Der Inhalt dieses Menüs enthält die Schlüsselwörter, die dem von Ihnen eingegebenen Anfangsschlüsselwort folgen können. Um das nächste Schlüsselwort in diesem Ausdruckspräfix auszuwählen, doppelklicken Sie im Dropdownmenü auf die Auswahl. Das Textfeld **Ausdrücke** zeigt sowohl das erste als auch das zweite Schlüsselwort für das Ausdruckspräfix an, beispielsweise HTTP.REQ. Fahren Sie mit dem Hinzufügen von Ausdruckskomponenten fort, bis der vollständige Ausdruck gebildet wird.

4. Klicken Sie auf **Einfügen**.
5. Fügen Sie bis zu fünf nicht zusammengesetzte Ausdrücke hinzu.
6. Klicken Sie auf **Erstellen** und dann auf **Schließen**.



Konfigurieren eines Stream-Bezeichners

October 5, 2021

Sie konfigurieren einen Stream-Bezeichner, um Parameter für das Sammeln statistischer Daten aus Anforderungen anzugeben, die von einem bestimmten Selektor identifiziert wurden. Ein Bezeichner

gibt den zu verwendenden Selektor, das Statistikerfassungsintervall, die Stichprobenanzahl und das Feld an, nach dem die Datensätze sortiert werden sollen.

Die Citrix ADC Appliance enthält die folgenden integrierten Stream-Bezeichner für häufig verwendete Anwendungsfälle. Alle integrierten Bezeichner geben eine Stichprobenanzahl von 1 und ein Intervall von 1 Minute an. Darüber hinaus sortieren sie die Daten auf dem Attribut
REQUESTS. Sie unterscheiden sich nur darin, dass sie mit verschiedenen eingebauten Selektoren verbunden sind. Jeder integrierte Bezeichner ist einem integrierten Selektor mit demselben Namen zugeordnet (z. B. ist der integrierte Bezeichner
top_url mit dem integrierten Selektor
top_url verknüpft). Im Folgenden sind die integrierten Bezeichner:

- Top_URL
- Top_CLIENTS
- Top_URL_CLIENTS_LBVSERVER
- Top_URL_CLIENTS_CSVSERVER
- Top_MSSQL_QUERY_DB_LBVSERVER
- Top_MYSQL_QUERY_DB_LBVSERVER

Weitere Informationen zu den integrierten Selektoren finden Sie unter Konfigurieren eines Selektors.

Hinweis: Die maximale Länge für das Speichern von Zeichenfolgenergebnissen von Selektoren (z. B. HTTP.REQ.URL) beträgt 60 Zeichen. Wenn die Zeichenfolge (z. B. URL) 1000 Zeichen lang ist, von denen 50 Zeichen ausreichen, um eine Zeichenfolge eindeutig zu identifizieren, verwenden Sie einen Ausdruck, um nur die erforderlichen 50 Zeichen zu extrahieren.

Die Konfiguration eines integrierten Bezeichners kann nicht geändert werden. Sie können jedoch einen Bezeichner mit einer Konfiguration Ihrer Wahl erstellen.

So konfigurieren Sie einen Stream-Bezeichner mit der Befehlszeilenschnittstelle

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

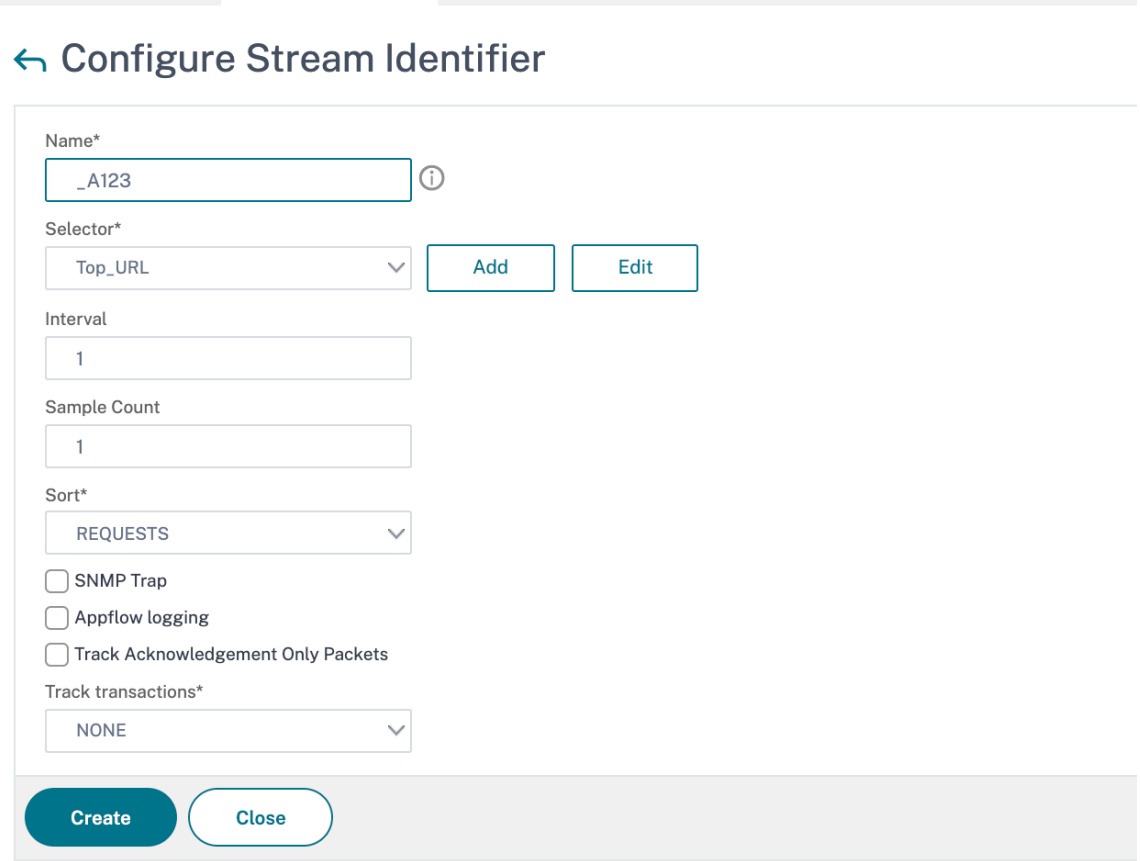
- `add stream identifier <name> <selectorName> [-interval <positive_integer>] [-SampleCount <positive_integer>] [-sort <sort>]`
- `show stream identifier <name>`

Beispiel

```
1 > add stream identifier myidentifier Top_URL -interval 10 -sampleCount
     100
2  Done
3 <!--NeedCopy-->
```


So konfigurieren Sie einen Stream-Bezeichner mit der GUI

1. Navigieren Sie zu **AppExpert** > **Action Analytics** > **Stream Identifiers**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine Stream-ID zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um einen Stream-Bezeichner zu ändern, wählen Sie den Bezeichner aus, und klicken Sie dann auf **Bearbeiten**.
3. Legen Sie auf der Seite Stream Identifier konfigurieren die folgenden Parameter fest:
   - Name
   - Wähler
   - Intervall
   - Stichprobenanzahl
   - Sortieren
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.



Statistiken anzeigen

October 5, 2021

Sie können die gesammelten Statistiken im tabellarischen Format in der Befehlszeilenschnittstelle und im grafischen Format im Konfigurationsprogramm anzeigen.

Die folgende Tabelle beschreibt die gesammelten Statistiken:

Statistik	Spaltenname in der Ausgabe des Befehls <identifier name> stat stream identifier	Beschreibung
Anzahl der Anfragen	**Req**	Die Anzahl der Anforderungen, für die Datensätze in den letzten <interval> Minuten erstellt wurden.

Statistik	Spaltenname in der Ausgabe des Befehls <identifier name> stat stream identifier	Beschreibung
Verbraucht Bandbreite	**BandW**	Die Gesamtbandbreite, die von den Anforderungen belegt wurde, die in der letzten<interval> Anzahl von Minuten empfangen wurden. Die Gesamtbandbreite einer Anforderung ist die Bandbreite, die von der Anforderung und ihrer Antwort belegt wird. Der Wert wird auf den nächst höheren oder nächstniedrigeren Ganzzahlwert abgerundet. Es kann also geringfügig vom erwarteten Wert abweichen. Wenn der gesamte Bandbreitenverbrauch einer Anfrage beispielsweise 2,2 KB beträgt. Eine Instanz der Anforderung könnte angezeigt werden, dass sie 2 KB verbraucht hat. Es kann angezeigt werden, dass zwei Instanzen 4 KB verbraucht haben, aber drei Instanzen könnten angezeigt werden, dass sie 7 KB verbraucht haben.
Response time	**RspTime**	Die durchschnittliche Antwortzeit für alle Anforderungen, die in der letzten <interval> Anzahl von Minuten empfangen wurden.

Statistik	Spaltenname in der Ausgabe des Befehls <identifier name> stat stream identifier	Beschreibung
Gleichzeitige Verbindungen	**Conn**	Die Gesamtanzahl gleichzeitiger Verbindungen, die derzeit geöffnet sind.

So zeigen Sie die statistischen Daten an, die über die Befehlszeile für einen Stream-Bezeichner erfasst wurden

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat stream identifier <name> [<pattern> ...] [-detail] [-fullValues] [-ntimes <positive_integer>] [-logFile <input_filename>] [-sortBy <sortBy> [<sortOrder>]
```

Beispiele

Beispiel 1 sortiert die Ausgabe in der BandW-Spalte in absteigender Reihenfolge. Beispiel 2 sortiert die Ausgabe in Beispiel 1, in der Spalte **Req** und in aufsteigender Reihenfolge

Beispiel 1

```
1  > stat stream identifier myidentifier -sortBy BandW Descending -
       fullValues
2  Stream Session statistics
3                       Req                 BandW
4  User1                508                125924
5  User2               5020                 12692
6  User3               2025                  4316
7
8                   RspTime                  Conn
9  User1               5694                     0
10 User2                109                     0
11 User3                  3                     0
12  Done
13 <!--NeedCopy-->
```

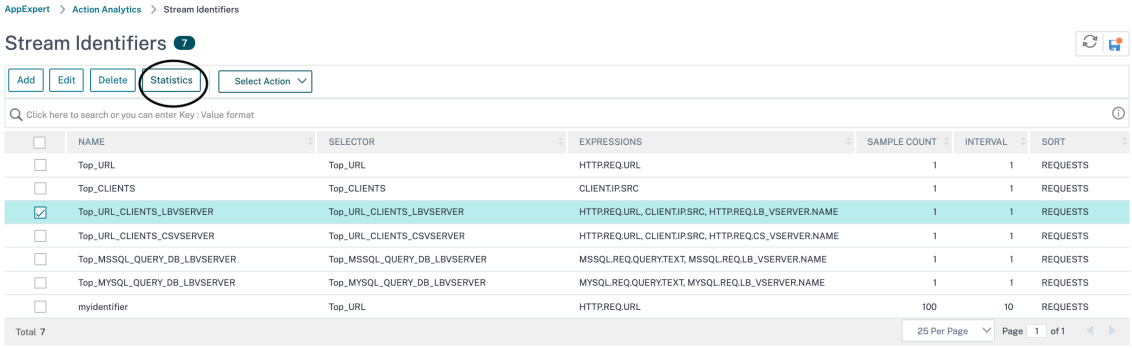
Beispiel 2


```
> stat stream identifier myidentifier -sortBy Req Ascending -
    fullValues
Stream Session statistics
                     Req                  BandW
User1                508                 125924
User3               2025                   4316
User2               5020                  12692

                  RspTime                   Conn
User1                5694                      0
User3                   3                      0
User2                 109                      0
 Done
<!--NeedCopy-->
```

So zeigen Sie die statistischen Daten an, die für einen Stream-Bezeichner mit der GUI erfasst wurden

1. Navigieren Sie zu **AppExpert** > **Action Analytics** > **Stream Identifiers**.
2. Wählen Sie den Stream-Bezeichner aus, dessen Sitzungen Sie anzeigen möchten, und klicken Sie dann auf Statistiken. Informationen dazu, wie Sie die Ausgabe anhand der für verschiedene Selektorausdrücke gesammelten Werte gruppieren können.



Gruppieren von Datensätzen nach Attributwerten

October 5, 2021

Statistische Informationen wie die Anzahl der Zugriffe auf eine bestimmte URL insgesamt und pro Client sowie die Gesamtzahl der GET und POST-Anfragen pro Client können wertvolle Einblicke in die Frage geben, ob Ihre Ressourcen erweitert werden müssen, um den Bedarf zu erfüllen oder für die Lieferung optimiert zu werden. Um solche Statistiken zu erhalten, müssen Sie einen entsprechenden Satz von Selektorausdrücken verwenden und dann den Pattern-Parameter im Befehl stat stream

identifier verwenden. Die Gruppierung basiert auf dem Muster, das im Befehl angegeben ist. Die Gruppierung kann gleichzeitig für die Werte mehrerer Ausdrücke durchgeführt werden.

In der Befehlszeilenschnittstelle können Sie die Ausgabe anhand von Mustern Ihrer Wahl gruppieren. Im Konfigurationsprogramm hängt das Muster von den Auswahlmöglichkeiten ab, die Sie beim Drilldown durch die Werte verschiedener Selektorausdrücke treffen. Betrachten Sie beispielsweise einen Selektor, der die Ausdrücke `HTTP.REQ.URL`, `CLIENT.IP.SRC` und `HTTP.REQ.LB_VSERVER.NAME` in dieser Reihenfolge hat. Auf der Statistik-Homepage werden Symbole für jeden dieser Ausdrücke angezeigt. Wenn Sie auf das Symbol für klicken `CLIENT.IP.SRC`, basiert die Ausgabe auf den Mustern *?*. Die Ausgabe zeigt Statistiken für jede Client-IP-Adresse an. Wenn Sie auf eine IP-Adresse klicken, basiert die Ausgabe auf den Muster* `<IP address> ?` und? `<IP address> *` wobei die IP-Adresse `<IP address>` ist, die Sie ausgewählt haben. Wenn Sie in der resultierenden Ausgabe auf eine URL klicken, wird das verwendete Muster verwendet`<URL> <IP address> ?`.

So gruppieren Sie die Datensätze anhand der Werte von Selektorausdrücken mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die Datensätze anhand eines Selektorausdrucks zu gruppieren:

```
stat stream identifier <name> [<pattern> ...]
```

In den folgenden Beispielen wird ein anderes Muster verwendet, um die Auswirkungen des Musters auf die Ausgabe des Befehls stat stream identifier zu demonstrieren. Die Selektorausdrücke sind HTTP.REQ.URL und HTTP.REQ.HEADER (UserHeader) in dieser Reihenfolge. Die Anforderungen enthalten einen benutzerdefinierten Header, dessen Name UserHeader ist. Beachten Sie, dass sich in den Beispielen ein bestimmter statistischer Wert ändert, wie durch die Gruppierung bestimmt, aber die Summe der Werte für ein bestimmtes Feld bleibt gleich.

Beispiel 1

Im folgenden Befehl ist das verwendete Muster? ?. Die Appliance gruppiert die Ausgabe nach den Werten, die für beide Selektorausdrücke gesammelt wurden. Die Zeilenüberschriften bestehen aus den Ausdruckswerten, die durch ein Fragezeichen (?) getrennt sind. Die Zeile mit dem Header /mysite/mypage1.html? Ed zeigt Statistiken für Anfragen des Benutzers Ed für die URL /mysite/mypage1.html.

> **Hinweis:**
>
> Sie müssen sicherstellen, dass Sie den folgenden Befehl mit “?”statt “?”. Beispiel: Wenn Selektor einen Ausdruck verwendet - client.ip.src und client.tcp.srcport. Der Stat-Befehl, um die Ausgabe auf den für den Selektor gesammelten Werten zu gruppieren, ist ‘stat stream identifier myidentifier? ? -FullValues’ wie unten angegeben.


```
> stat stream identifier myidentifier ? ? -fullValues
Stream Session statistics
                                          Req                  BandW
/mysite/mypage2.html?Grace                  1                   2553
/mysite/mypage1.html?Grace                  2                      4
/mysite/mypage1.html?Ed                     8                     16
/mysite/mypage2.html?Joe                    1                   2554
/mysite/mypage1.html?Joe                    5                     10
/mysite/?Joe                                1                      4

                                       RspTime                  Conn
/mysite/mypage2.html?Grace                  0                      0
/mysite/mypage1.html?Grace                  0                      0
/mysite/mypage1.html?Ed                     0                      0
/mysite/mypage2.html?Joe                    0                      0
/mysite/mypage1.html?Joe                    0                      0
/mysite/?Joe                                6                      0
 Done
<!--NeedCopy-->
```

Beispiel 2

Im folgenden Befehl ist das verwendete Muster *?. Die Appliance gruppiert die Ausgabe nach den Werten, die für den zweiten Ausdruck HTTP.REQ.HEADER (UserHeader) gesammelt wurden. Die Zeilen zeigen Statistiken für alle Anfragen von Benutzern Grace, Ed und Joe an.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie den folgenden Befehl mit “?”statt “?”.

```
> stat stream identifier myidentifier * ?
Stream Session statistics
                  Req     BandW  RspTime     Conn
Grace               3      2557        0        0
Ed                  8        16        0        0
Joe                 7      2568        6        0
 Done
<!--NeedCopy-->
```

Beispiel 3

Im folgenden Befehl ist das verwendete Muster? *, das ist das Standardmuster. Die Ausgabe wird nach den Werten gruppiert, die für den ersten Selektorausdruck gesammelt wurden. Jede Zeile zeigt Statistiken für eine URL an.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie den folgenden Befehl mit “?”statt “?”.

```
> stat stream identifier myidentifier ? * -fullValues
Stream Session statistics
                                          Req                  BandW
/mysite/mypage2.html                        2                   5107
/mysite/mypage1.html                       15                     30
/mysite/                                    1                      4

                                       RspTime                  Conn
/mysite/mypage2.html                          0                      0
/mysite/mypage1.html                          0                      0
/mysite/                                      6                      0
 Done
<!--NeedCopy-->
```

Beispiel 4

Im folgenden Befehl wird das verwendete Muster verwendet `* *`. Die Appliance zeigt einen Satz kollektiver Statistiken für alle empfangenen Anforderungen ohne Zeilentitel an.

```
> stat stream identifier myidentifier * *
Stream Session statistics
                  Req     BandW  RspTime      Conn
                   18      5141         6         0
 Done
<!--NeedCopy-->
```

Beispiel 5

Im folgenden Befehl lautet das Muster /mysite/mypage1.html *. Die Appliance zeigt einen Satz kollektiver Statistiken für alle Anfragen an, die für die URL /mysite/mypage1.html empfangen wurden, ohne Zeilentitel.

```
> stat stream identifier myidentifier /mysite/mypage1.html *
Stream Session statistics
                  Req     BandW  RspTime      Conn
                   15        30         0         0
 Done
```



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

Löschen einer Stream-Sitzung

October 5, 2021

Sie können alle Datensätze leeren, die für einen Stream-Bezeichner gesammelt wurden.

So löschen Sie eine Stream-Sitzung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Streamsitzung zu löschen und die Ergebnisse zu überprüfen:

- clear stream session
- stat stream identifier

Beispiel

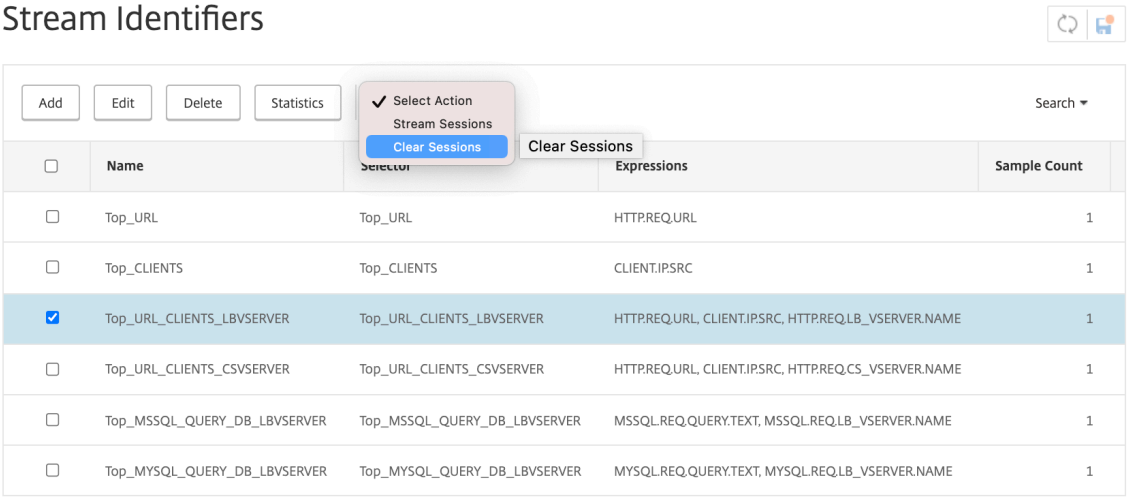
In diesem Beispiel wird zuerst der Befehl stat stream identifier verwendet, sodass ein Vergleich mit dem Befehl stat stream identifier durchgeführt werden kann, der zum Überprüfen des Ergebnisses des Befehls clear stream session verwendet wird.

```
>stat stream identifier myidentifier
Stream Session statistics
                  Req    BandW  RspTime     Conn
/aed....html        2        0        0        0
/                 636      303       12        0
 Done
>clear stream session myidentifier
 Done
>stat stream identifier myidentifier
 Done
<!--NeedCopy-->
```

So löschen Sie eine Stream-Sitzung mit der GUI

1. Navigieren Sie zu **AppExpert** > **Action Analytics** > **Stream Identifiers**.

2. Wählen Sie den Stream-Bezeichner aus, dessen Sitzungen Sie löschen möchten, und klicken Sie dann auf **Sitzungen löschen**.



Konfigurieren der Richtlinie für die Optimierung des Datenverkehrs

October 5, 2021

Um das Selektor-Identifizierer-Paar in Ihrer Aktions-Analytics-Konfiguration in Kraft zu setzen, müssen Sie das Paar dem Punkt im Verkehrsfluss zuordnen, an dem Sie Statistiken sammeln möchten. Sie können dies tun, indem Sie eine Standard-Syntaxrichtlinie konfigurieren und auf den Stream-Bezeichner aus der Richtlinienregel verweisen. Sie können Komprimierungsrichtlinien, Caching-Richtlinien, Umschreiben von Richtlinien, Anwendungs-Firewall-Richtlinien, Responder-Richtlinien und alle anderen Richtlinien verwenden, deren Aktion auf einem booleschen Ausdruck basiert.

Die Aktionsanalysefunktion führt eine Reihe von Standard-Syntaxausdrücken und -funktionen zum Sammeln und Auswerten von Daten ein. Der Ausdruck `ANALYTICS.STREAM(<identifier_name>)` wird verwendet, um den Bezeichner zu referenzieren, den Sie verwenden möchten. Der Ausdruck COLLECT_STATS wird verwendet, um statistische Daten zu sammeln. Funktionen wie `IS_TOP(<uint>)` und `IS_TOP_FREQUENTS(<uint>)` werden verwendet, um automatische, Echtzeit-Verkehrsoptimierungsentscheidungen zu treffen.

- **IS_TOP(<number>).** Findet, ob ein gegebenes Objekt in der Oberseite <number> der Elemente ist. Zum Beispiel ist das Element unter den Top 10 Elementen. Wenn mehrere Elemente die Zählung haben, werden sie in der Natur als ähnlich angesehen. Die Sortierfunktion muss aktiviert sein, um eine undef-Bedingung zu vermeiden.
- **IS_TOP_FREQUENTS(<frequency>).** Findet, ob ein gegebenes Objekt im oberen Teil <frequency> der Elemente ist, die in den oberen Elementen sind. Zum Beispiel ist das Element unter den obersten 50% aller obersten Elemente beibehalten. Elemente mit den gleichen

Werten werden in der Natur als ähnlich angesehen. Die Sortierfunktion muss aktiviert sein, um eine undef-Bedingung zu vermeiden.

Es ist Ihre Richtlinienkonfiguration, die bestimmt, ob die Citrix ADC Appliance nur Daten aus dem Datenverkehr erfassen oder auch eine Aktion ausführen darf. Wenn die Appliance nur statistische Daten erfassen muss, können Sie eine Richtlinie mit der Regel `ANALYTICS.STREAM(<identifier_name>).COLLECT_STATS` und der Aktion NOOP konfigurieren. Die NOOP-Richtlinie muss die Richtlinie mit der höchsten Priorität am Bindepunkt sein. Diese Richtlinie ist ausreichend, wenn Sie nur Statistiken sammeln. Entscheidungen zur Verkehrsoptimierung, wie zum Beispiel, was komprimiert oder zwischengespeichert werden soll, müssen auf einer manuellen, periodischen Auswertung der statistischen Daten beruhen.

Wenn die Appliance neben der Erfassung von Statistiken auch eine Aktion für den Datenverkehr ausführen muss, müssen Sie den gotoPriorityExpression-Parameter der NOOP-Richtlinie so konfigurieren, dass eine andere Richtlinie mit der gewünschten Regel und Aktion nachträglich ausgewertet wird. Diese zweite Richtlinie muss eine Regel haben, die mit dem Präfix `ANALYTICS.STREAM(<identifier_name>)` beginnt, und eine Funktion, die die Daten auswertet.

Es folgt ein Beispiel für zwei Responder-Richtlinien, die global konfiguriert und gebunden sind. Die Richtlinie responder_stat_collection ermöglicht es der Appliance, Statistiken basierend auf dem Bezeichner myidentifier zu sammeln. Die Richtlinie responder_notify wertet die gesammelten Daten aus.

Beispiel

```
> add responder action send_notification respondwith '"You are in the Top 10 list for bandwidth consumption"'
 Done
> add responder policy responder_stat_collection' ANALYTICS.STREAM("myidentifier").COLLECT_STATS' NOOP
Done
> add responder policy responder_notify 'ANALYTICS.STREAM("myidentifier").BANDWIDTH.IS_TOP(10)' send_notification
 Done
> bind responder global responder_stat_collection 10 NEXT
 Done
> bind responder global responder_notify 20 END
 Done
<!--NeedCopy-->
```


So begrenzen Sie den Bandbreitenverbrauch pro Benutzer oder Client-Gerät

October 5, 2021

Ihre Website, Anwendung oder Datei-Hosting-Dienst verfügt über endliche Netzwerk- und Server-Ressourcen, um alle ihre Benutzer zu bedienen. Eine der wichtigsten Ressourcen ist die Bandbreite. Ein erheblicher Bandbreitenverbrauch durch nur eine Teilmenge der Benutzerbasis kann zu einer Netzwerküberlastung und einer geringeren Ressourcenverfügbarkeit für andere Benutzer führen. Um Netzwerküberlastung zu verhindern, müssen Sie möglicherweise den Bandbreitenverbrauch eines Clients einschränken, indem Sie temporäre Dienstverweigerungsmethoden verwenden, z. B. die Reaktion auf eine Clientanforderung mit einer HTML-Seite, wenn dieser einen vorkonfigurierten Bandbreitenwert über einen bestimmten Zeitraum vor der Anforderung überschritten hat.

Im Allgemeinen können Sie den Bandbreitenverbrauch entweder pro Clientgerät oder pro Benutzer regulieren. Dieser Anwendungsfall zeigt, wie Sie den Bandbreitenverbrauch pro Client über einen Zeitraum von einer Stunde auf 100 MB begrenzen können. Der Anwendungsfall zeigt auch, wie Sie den Bandbreitenverbrauch pro Benutzer über einen Zeitraum von einer Stunde auf 100 MB regeln können, indem Sie einen benutzerdefinierten Header verwenden, der den Benutzernamen bereitstellt. In beiden Fällen wird die Verfolgung des Bandbreitenverbrauchs über einen bewegten Zeitraum von einer Stunde erreicht, indem der Intervallparameter in der Stream-ID auf 60 Minuten gesetzt wird. Die Anwendungsfälle zeigen auch, wie Sie eine HTML-Seite importieren können, die an einen Client gesendet werden soll, der den Grenzwert überschritten hat. Das Importieren einer HTML-Seite vereinfacht nicht nur die Konfiguration der Responder-Aktion in diesen Anwendungsfällen, sondern vereinfacht auch die Konfiguration aller Responder-Aktionen, die dieselbe Antwort benötigen.

So beschränken Sie den Bandbreitenverbrauch pro Benutzer oder Clientgerät mit der Befehlszeilenschnittstelle

Führen Sie in der Befehlszeilenschnittstelle die folgenden Aufgaben aus, um Aktionsanalysen für die Begrenzung des Bandbreitenverbrauchs eines Clients oder Benutzers zu konfigurieren. Jeder Schritt enthält Beispielbefehle und deren Ausgabe.

1. **Richten Sie Ihre Lastausgleichskonfiguration ein.** Konfigurieren Sie den Lastenausgleich virtuellen Server mysitevip, und konfigurieren Sie dann alle Dienste, die Sie benötigen. Binden Sie die Dienste an den virtuellen Server. Im folgenden Beispiel werden zehn Dienste erstellt und die Dienste an mysitevip gebunden.

```
> add lb vserver mysitevip HTTP 192.0.2.17 80
 Done
> add service service[1-10] 192.0.2.[240-249] HTTP 80
```



```
service "service1" added
service "service2" added
service "service3" added
.
.
.
service "service10" added
 Done
> bind lb vserver vserver1 service[1-10]
service "service1" bound
service "service2" bound
service "service3" bound
.
.
.
service "service10" bound
 Done
<!--NeedCopy-->
```

2. **Konfigurieren Sie den Stream-Selektor.** Konfigurieren Sie einen der folgenden Stream-Selektoren:

   - Um den Bandbreitenverbrauch pro Client zu begrenzen, konfigurieren Sie einen Stream-Selektor, der die Client-IP-Adresse identifiziert.

     ```
     > add stream selector myselector CLIENT.IP.SRC
      Done
     <!--NeedCopy-->
     ```

   - Um den Bandbreitenverbrauch pro Benutzer auf der Grundlage des Wertes eines Anforderungs-Headers, der den Benutzernamen bereitstellt, zu begrenzen, konfigurieren Sie einen Stream-Selektor, der den Header identifiziert. Im folgenden Beispiel lautet der Name der Kopfzeile UserHeader.

     ```
     > add stream selector myselector HTTP.REQ.HEADER( "UserHeader
         " )
      Done
     <!--NeedCopy-->
     ```

3. **Konfigurieren Sie einen Stream-Bezeichner.** Konfigurieren Sie einen Stream-Bezeichner, der den Stream-Selektor verwendet. Stellen Sie den Intervallparameter auf 60 Minuten ein.


```
> add stream identifier myidentifier myselector -interval 60 -
   sampleCount 1 -sort BANDWIDTH
 Done
<!--NeedCopy-->
```

4. **Konfigurieren Sie die Responderaktion.** Importieren Sie die HTML-Seite, die Sie an Benutzer oder Clients senden möchten, die das Bandbreitenverbrauchslimit überschritten haben, und verwenden Sie dann die Seite in Responderaktion crossed_limits.

```
> import responder htmlpage http://.1.1.1/stdpages/wait.html
   crossed-limits.html
This operation may take some time, Please wait...

 Done
> add responder action crossed_limits respondwithhtmlpage crossed-
   limits.html
 Done
<!--NeedCopy-->
```

5. **Konfigurieren Sie die Responder-Richtlinien.** Konfigurieren Sie die Responderrichtlinie myrespol1 mit der Regel ANALYTICS.STREAM (myidentifier) .COLLECT_STATS und der Aktion NOOP. Konfigurieren Sie dann die Richtlinie myrespol2, um zu bestimmen, ob ein Client oder Benutzer die Grenze von 100 MB überschritten hat. Die Richtlinie myrespol2 ist mit der Responderaktion crossed_limits konfiguriert.

```
> add responder policy myrespol1 'ANALYTICS.STREAM(”myidentifier”)
   .COLLECT_STATS' NOOP
 Done
> add responder policy myrespol2 'ANALYTICS.STREAM(”myidentifier”)
   .BANDWIDTH.GT(104857600)' crossed_limits
 Done
<!--NeedCopy-->
```

6. **Binden Sie die Responderrichtlinien an den virtuellen Lastausgleichsserver.** Die Richtlinie myrespol1, die nur statistische Daten sammelt, muss die höhere Priorität und einen GOTO-Ausdruck von NEXT haben.


```
> bind lb vserver mysitevip -policyName myrespol1 -priority 1 -
   gotoPriorityExpression NEXT
 Done
> bind lb vserver mysitevip -policyName myrespol2 -priority 2 -
   gotoPriorityExpression END
 Done
<!--NeedCopy-->
```

7. **Testen Sie die Konfiguration.** Testen Sie die Konfiguration, indem Sie HTTP-Testanforderungen von mehreren Clients oder Benutzern an den virtuellen Lastausgleichsserver senden und mithilfe des Befehls stat stream identifier die Statistiken anzeigen, die für den angegebenen Bezeichner gesammelt werden. Die folgende Ausgabe zeigt Statistiken für Clients an.

```
> stat stream identifier myidentifier -sortBy BandW  - fullValues
Stream Session statistics
                            Req             BandW
192.0.2.30                  5000            3761
192.0.2.31                  29              2602
192.0.2.32                  25              51

                            RspTime         Conn
192.0.2.30                  2               0
192.0.2.31                  0               0
192.0.2.32                  0               0
 Done
>
<!--NeedCopy-->
```

AppExpert Anwendungen und Vorlagen

October 5, 2021

> **Warnung**
>
> Die Funktionalität der Anwendungsvorlage ist ab Citrix ADC 13.0 Build 82.x veraltet und empfiehlt Citrix alternativ, die Style Books zu verwenden. Weitere Informationen finden Sie unter Thema Stilbücher .

Eine AppExpert-Anwendung ist eine Sammlung von Konfigurationen, die Sie auf der Citrix ADC Appliance einrichten. Die Verwaltung von AppExpert-Anwendungen wird durch eine GUI (GUI) vereinfacht,

mit der Sie Teilmengen des Anwendungsverkehrs und eine bestimmte Reihe von Sicherheits- und Optimierungsrichtlinien für die Verarbeitung jeder Verkehrsuntermenge angeben können. Außerdem konsolidiert es Bereitstellungsschritte in einer Ansicht, sodass Sie schnell Ziel-IP-Adressen für Clients konfigurieren und Hostserver angeben können.

Um mit einer AppExpert t-Anwendung zu beginnen, müssen Sie zuerst die entsprechende Anwendungsvorlage abrufen und die Vorlage in die Citrix ADC Appliance importieren. Nachdem die AppExpert Anwendung eingerichtet wurde, müssen Sie überprüfen, ob die Anwendung ordnungsgemäß funktioniert. Bei Bedarf können Sie die Konfiguration an Ihre Anforderungen anpassen.

In regelmäßigen Abständen können Sie die Konfiguration überprüfen und überwachen, indem Sie die Zähler für verschiedene Anwendungskomponenten, Statistiken und den Application Visualizer anzeigen. Sie können auch Authentifizierungs-, Autorisierungs- und Überwachungsrichtlinien (Authentifizierung, Autorisierung und Überwachung) für die Anwendung konfigurieren.

AppExpert Anwendungsterminologie

Im Folgenden werden die Begriffe in der AppExpert Anwendungsfunktion verwendet und die Beschreibungen der Entitäten, für die die Begriffe verwendet werden:

Öffentlicher Endpunkt. Die Kombination zwischen IP-Adresse und Port, bei der die Citrix ADC Appliance Clientanforderungen für die zugehörige Webanwendung empfängt. Ein öffentlicher Endpunkt kann so konfiguriert werden, dass er entweder HTTP- oder HTTP-Datenverkehr (HTTPS) empfängt. Alle Clientanforderungen für die Webanwendung müssen an einen öffentlichen Endpunkt gesendet werden. Eine AppExpert Anwendung kann mehrere Endpunkte zugewiesen werden. Öffentliche Endpunkte werden konfiguriert, nachdem Sie eine Vorlage importiert haben.

Anwendungseinheit. Eine AppExpert Anwendungsentität, die eine Teilmenge des Webanwendungsdatenverkehrs verarbeitet und eine Reihe von Diensten ausgleicht, die den zugeordneten Inhalt hosten. Die Teilmenge des Datenverkehrs, die eine Anwendungseinheit verwalten muss, wird durch eine Regel definiert. Jede Anwendungseinheit definiert außerdem einen eigenen Satz von Verkehrsoptimierungs- und Sicherheitsrichtlinien für die von ihr verwalteten Anforderungen und Antworten. Die Citrix ADC Dienste, die diesen Richtlinien zugeordnet sind, sind Komprimierung, Caching, Rewrite, Responder und Anwendungsfirewall.

Standardmäßig enthält jede AppExpert t-Anwendung mit mindestens einer Anwendungseinheit eine Standardanwendungseinheit, die nicht gelöscht werden kann. Die Standardanwendungseinheit ist keiner Regel zur Identifizierung von Anforderungen zugeordnet und wird immer zuletzt in der Reihenfolge der Anwendungseinheiten platziert. Es definiert eine Reihe von Richtlinien für die Verarbeitung von Anfragen, die nicht mit den Regeln übereinstimmen, die für die anderen Anwendungseinheiten konfiguriert sind. Damit wird sichergestellt, dass alle Kundenanfragen bearbeitet werden.

Anwendungseinheiten und die zugehörigen Regeln, Richtlinien und Aktionen sind in AppExpert Anwendungsvorlagen enthalten.

Service. Die Kombination aus der IP-Adresse des Servers, der die Webanwendungsinstanz hostet, und dem Port, dem die Anwendung auf dem Server zugeordnet ist, im Format \<IP address\>:\<Port\>. Eine Webanwendung, die viele Anfragen erfüllt, wird auf mehreren Servern gehostet. Jeder Server soll eine Instanz der Webanwendung hosten, und jede Instanz der Webanwendung wird durch einen Dienst auf der Citrix ADC Appliance dargestellt. Services sind bereitstellungsspezifisch und daher nicht in Vorlagen enthalten. Sie müssen Dienste konfigurieren, nachdem Sie eine Vorlage importiert haben.

Anwendungseinheitenregel. Entweder ein klassischer Ausdruck oder ein Standard-Syntaxausdruck, der die Merkmale einer Datenverkehrsuntermenge für eine Anwendungseinheit definiert. Die folgende Beispielregel ist ein Standard-Syntaxausdruck, der eine Datenverkehrsuntermenge identifiziert, die aus vier Bildtypen besteht:

```
HTTP.REQ.URL.SUFFIX.EQ("bmp")|| HTTP.REQ.URL.SUFFIX.EQ("gif")|| HTTP.REQ.
URL.SUFFIX.EQ("png")|| HTTP.REQ.URL.SUFFIX.EQ("jpg")
```

Weitere Informationen zu Standardsyntaxausdrücken und klassischen Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke.

Teilmenge des Datenverkehrs. Eine Reihe von Clientanforderungen, die einen gemeinsamen Satz von Verkehrsoptimierungs- und Sicherheitsrichtlinien erfordern. Eine Datenverkehrsuntermenge wird von einer Anwendungseinheit verwaltet und durch eine Regel definiert.

Funktionsweise der AppExpert Anwendung

October 5, 2021

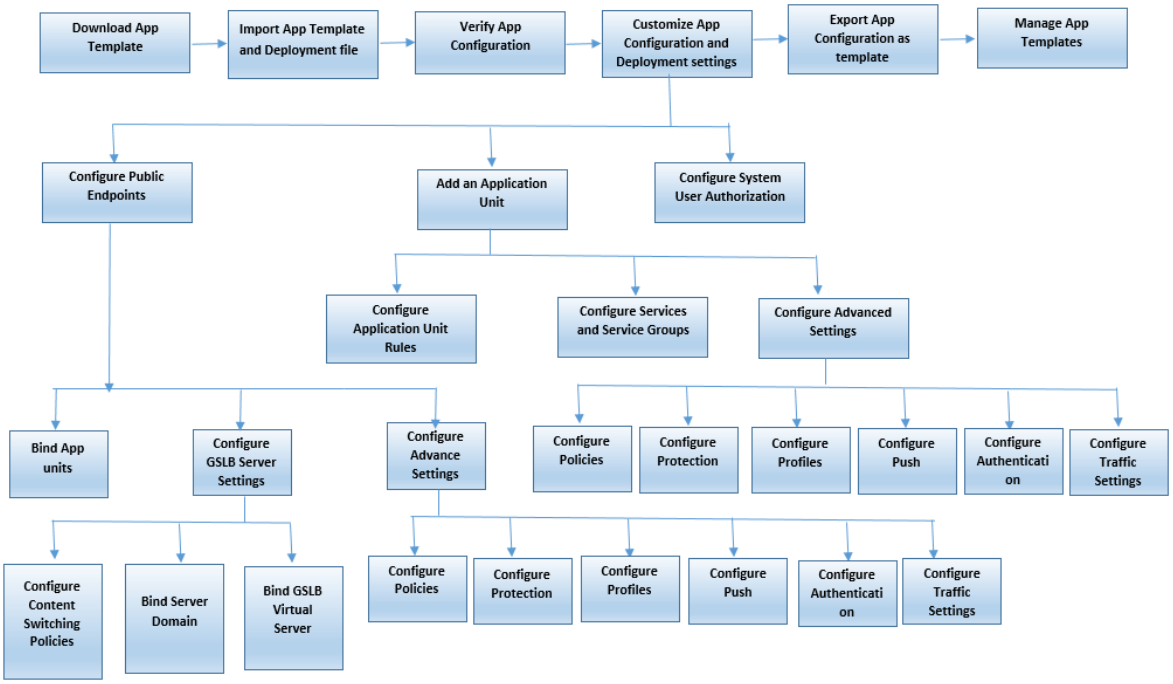
Wenn der Endpunkt eine Clientanforderung empfängt, wertet die Citrix ADC Appliance die Anforderung anhand der Regel aus, die für die oberste Anwendungseinheit konfiguriert ist. Wenn die Anforderung diese Regel erfüllt, wird die Anforderung von den Richtlinien verarbeitet, die für die Anwendungseinheit konfiguriert sind, und dann an einen Dienst weitergeleitet. Die Wahl des Dienstes hängt davon ab, welche Dienste für die Anwendung konfiguriert sind, und von Einstellungen wie dem Lastausgleichsalgorithmus und der Persistenzmethode, die für die Anwendungseinheit konfiguriert sind.

Wenn die Anforderung die Regel nicht erfüllt, wird die Anforderung anhand der Regel für die nächste oberste Anwendungseinheit ausgewertet. In dieser Reihenfolge wird die Anforderung für jede Anwendungseinheitenregel ausgewertet, bis die Anforderung eine Regel erfüllt. Wenn die Anforderung keine der konfigurierten Regeln erfüllt, wird sie von der Standardanwendungseinheit verarbeitet, die immer die letzte Anwendungseinheit ist.

Sie können mehrere öffentliche Endpunkte für eine AppExpert Anwendung konfigurieren. In einer solchen Konfiguration verarbeitet jede Anwendungseinheit standardmäßig Anforderungen, die von

allen öffentlichen Endpunkten empfangen werden, und Lastverteilung aller Dienste, die für die Anwendung konfiguriert sind. Sie können jedoch angeben, dass eine Anwendungseinheit Datenverkehr nur aus einer Teilmenge der öffentlichen Endpunkte verarbeitet und nur eine Teilmenge der Dienste ausgleicht, die für die AppExpert Anwendung konfiguriert sind.

Das folgende Flussdiagramm veranschaulicht die Ablaufsequenz AppExpert Application für die Verwendung einer integrierten Anwendungsvorlage.



Wenn Sie eine benutzerdefinierte Anwendung ohne Vorlage erstellen möchten, gehen Sie folgendermaßen vor:

1. Erstellen Sie eine benutzerdefinierte Anwendung.
2. Konfigurieren Sie die Anwendungs- und Bereitstellungseinstellungen.
3. Exportieren Sie die Konfiguration in neue Vorlagendateien (optional).
4. Importieren der Vorlagendateien in andere Citrix ADC Appliances, die eine ähnliche AppExpert Anwendungskonfiguration erfordern

Erste Schritte mit AppExpert

October 5, 2021

Um mit einer AppExpert t-Anwendung zu beginnen, müssen Sie zunächst eine Anwendungsvorlage abrufen und die Vorlage in eine Citrix ADC Appliance importieren. Nachdem die AppExpert Anwen-

dung eingerichtet wurde, müssen Sie überprüfen, ob die Anwendung ordnungsgemäß funktioniert. Bei Bedarf können Sie die Konfiguration an Ihre Anforderungen anpassen.

In regelmäßigen Abständen können Sie die Konfiguration überprüfen und überwachen, indem Sie die Trefferindikatoren für verschiedene Anwendungskomponenten anzeigen. Sie können auch Authentifizierungs-, Autorisierungs- und Überwachungsrichtlinien (AAA) für die Anwendung konfigurieren.

Das Einrichten einer Anwendung kann auf zwei Arten erfolgen:

- Verwenden einer vordefinierten Anwendungsvorlage
- Erstellen einer benutzerdefinierten Anwendung ohne Verwendung einer Vorlage.

Wenn Sie die Anwendung mithilfe einer vordefinierten Anwendungsvorlage einrichten möchten, gehen Sie wie folgt vor:

1. Laden Sie eine Anwendungsvorlage herunter.
2. Importieren Sie Vorlagendateien in die Citrix ADC Appliance.
3. Überprüfen Sie die Anwendungseinrichtung.
4. Konfigurieren Sie die Anwendungs- und Bereitstellungseinstellungen.
5. Exportieren Sie die Konfiguration in neue Vorlagendateien (optional).
6. Importieren Sie die Vorlagendateien in andere Citrix ADC Appliances, für die eine ähnliche AppExpert Anwendungskonfiguration erforderlich ist.

Mit den Video-Tutorials von Citrix ADC können Sie Citrix ADC Funktionen auf einfache und einfache Weise verstehen. Sehen Sie sich dashttps://www.youtube.com/watch?v=aqayflvCR_0 Video an, um zu erfahren, wie Sie eine Anwendung mit der AppExpert Application Template einrichten.

Herunterladen einer Anwendungsvorlage

October 5, 2021

Hinweis: Citrix unterstützt AppExpert-Anwendungsvorlagen nicht mehr und erlaubt es Ihnen nicht, eine Kopie herunterzuladen. Wenn Sie Citrix ADC Version 13.0 oder früher verwenden, können Sie sich an den Citrix Support wenden, um eine Kopie einer Anwendungsvorlage zu erhalten.

Um die AppExpert-Anwendung einzurichten, müssen Sie zuerst eine Anwendungsvorlage von der Citrix Community-Website http://community.citrix.com auf Ihren lokalen Computer oder Ihre Citrix ADC Appliance herunterladen. Die Anwendungsvorlagen werden importiert und exportiert, sodass Sie anwendungsspezifische Konfigurationen einfach innerhalb einer Organisation oder zwischen Organisationen freigeben können. Eine Anwendungsvorlage enthält die folgenden Entitäten:

1. Anwendungskomponenten (z. B. Webseiten, Dateien, Archive und Webservices)

2. Verkehrsverwaltungsentitäten (z. B. IP-Adressen des virtuellen Servers und zugehörige Lastausgleichsalgorithmen und SSL-Offload-Einstellungen) für die Anwendungskomponenten.
3. Citrix ADC Richtlinien zur Optimierung des Anwendungsdatenverkehrs.

Hinweis: Anwendungsvorlagen sind in verschiedenen Versionen zum Konfigurieren verschiedener Typen von Citrix ADC Appliances verfügbar.

Importieren einer Anwendungsvorlage

October 5, 2021

Für Citrix ADC -Softwareversion 9.3 oder höher verfügt jede AppExpert Vorlage über zwei XML-Dateien: eine Vorlagendatei und eine Bereitstellungsdatei. Sie müssen beide Dateien von Ihrem lokalen Computer in eine Citrix ADC Appliance importieren. Sie können die Vorlagendateien entweder von Ihrem Computer in das AppExpert t-Anwendungsvorlagen-Verzeichnis in der Citrix ADC Appliance importieren oder Dateien auf eine Citrix ADC-Appliance hochladen und dann von der Appliance importieren.

Hinweis: Wenn Sie eine Vorlage von einer Appliance importieren, müssen Sie den in der Vorlage verfügbaren Variablenwert angeben. Standardmäßig wird der vorkonfigurierte Wert angezeigt/de-de/citrix-adc/13/appexpert/appexpert-application-templates/creating-managing-templates/citrix-adc-application-template-deployment-files.html

Nachdem Sie die Vorlagendateien importiert haben, füllt die Anwendungskonfigurations- und Bereitstellungsinformationen die Zielanwendung automatisch auf. Die Appliance importiert die gesamte Konfiguration aus den Vorlagendateien über die NITRO -API. Wenn Sie die Bereitstellungsdatei nicht importieren, generiert das System eine Anwendung, die mit der Konfiguration des virtuellen Content Switching-Servers ausgefüllt ist. Weitere Informationen zum Format von Anwendungsvorlagen und Bereitstellungsdateien finden Sie unter Grundlegendes zu Citrix ADC Anwendungsvorlagen und Bereitstellungsdateien.

Wenn Sie eine Vorlage importieren und keine Bereitstellungsdatei einschließen, müssen Sie die öffentlichen Endpunkte in der Anwendung konfigurieren, die das System automatisch aus der Vorlage generiert. Ein Endpunkt für HTTP und ein weiterer Endpunkt für HTTPS. Stellen Sie beim Konfigurieren eines öffentlichen Endpunkts vom Typ HTTPS sicher, dass Sie die SSL-Funktion aktivieren, das Serverzertifikat binden und die Serverzertifikat- und Zertifikatschlüsseldateien einschließen.

Weitere Informationen zum Konfigurieren von Endpoints nach dem Importieren einer Vorlage finden Sie unter Konfigurieren von öffentlichen Endpoints.

So importieren Sie AppExpert Anwendungsvorlagendateien in eine Citrix ADC Appliance mit der grafischen Benutzeroberfläche:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich auf **Vorlage importieren**.
3. Legen Sie auf der Seite **Importieren** die folgenden Parameter fest:
   a) Anwendungsname (obligatorisch)
   b) Vorlagendatei (obligatorisch)
   c) Bereitstellungsdatei verwenden
4. Klicken Sie auf **Weiter**, um Anwendungskonfigurations- und Bereitstellungsinformationen automatisch in eine Anwendung aufzufüllen.

Mit den Video-Tutorials von Citrix ADC können Sie Citrix ADC Funktionen auf einfache und einfache Weise verstehen. Sehen Sie sich dashttps://www.youtube.com/watch?v=AR9TwSD9uJM Video an, um zu erfahren, wie Sie eine Anwendungsvorlage importieren.

Überprüfen und Testen der Anwendungskonfiguration

October 5, 2021

Die GUI enthält Symbole, die die Zustände der Entitäten in der AppExpert Anwendung anzeigen. Diese Symbole werden für Anwendungen und Anwendungseinheiten angezeigt und basieren auf den Integritätsprüfungen, die die Citrix ADC Appliance regelmäßig für Dienste und Entitäten durchführt. In der folgenden Tabelle werden die Symbole aufgeführt und deren Bedeutung beschrieben.

Symbol	Entität	Gibt an, dass
	Anwendung	Mindestens ein öffentlicher Endpunkt ist hochgesetzt. Die Anwendung akzeptiert Clientanforderungen von den öffentlichen Endpunkten, die hochgesetzt sind.
	Anwendungseinheit	Die Applikationseinheit ist oben. Die Anwendungseinheit ist aktiviert, wenn mindestens ein Dienst oder eine Servicegruppe hochgesetzt ist.

Symbol	Entität	Gibt an, dass
	Anwendung	Der öffentliche Endpunkt ist außer Betrieb (deaktiviert). Dieser Indikator wird angezeigt, wenn nur ein öffentlicher Endpunkt für die AppExpert t-Anwendung konfiguriert ist.
	Anwendung	Alle für die Anwendung konfigurierten Endpunkte sind außer Betrieb. Dieser Indikator wird nur angezeigt, wenn mehrere Endpunkte für die Anwendung konfiguriert sind.
	Anwendungseinheit	Alle für die Anwendungseinheit konfigurierten Dienste sind ausgefallen.

Sie müssen sicherstellen, dass die Symbole für jede Anwendung und ihre Anwendungseinheiten jederzeit grün sind. Wenn das Symbol, das für eine Anwendung angezeigt wird, nicht grün ist, überprüfen Sie, ob Sie die öffentlichen Endpunkte richtig konfiguriert haben. Wenn das Symbol, das für eine Anwendungseinheit angezeigt wird, nicht grün ist, überprüfen Sie, ob die Dienste korrekt konfiguriert sind. Beachten Sie jedoch, dass ein grüner Indikator nicht bedeutet, dass der Status aller zugeordneten Entitäten UP ist. Dies bedeutet nur, dass die Anwendung über ausreichende Ressourcen (Endpunkte und Dienste) verfügt, um Clientanforderungen zu erfüllen. Um zu überprüfen, ob der Status aller zugeordneten Entitäten UP ist, überprüfen Sie die Integrität aller Entitäten auf der Statistikseite für die Anwendung.

Anpassen der Konfiguration

October 5, 2021

Nachdem Sie überprüft haben, dass die AppExpert Anwendung ordnungsgemäß funktioniert, können Sie die Konfiguration an Ihre Anforderungen anpassen.

Nachdem Sie überprüft haben, dass die AppExpert Anwendungskonfiguration ordnungsgemäß funktioniert, können Sie die Anwendung und die Bereitstellungseinstellungen entsprechend Ihren Anforderungen konfigurieren. Wenn Sie eine Anwendungsvorlage und eine Bereitstellungsdatei importieren, füllt das System die Zielanwendung automatisch mit den verfügbaren Konfigurationseinstellungen (z. B. Anwendungseinheiten, Anwendungseinheitenregeln, Richtlinien, Persistenzeinstellungen, Lastausgleichsmethoden, Profile und Verkehrseinstellungen). In dieser Anwendung können Sie Bereitstellungseinstellungen wie öffentliche Endpunkte, Dienste und Dienstgruppen für jede Datenverkehrsuntermenge konfigurieren. Wenn Sie möchten, dass die AppExpert Anwendung eine Datenverkehrsuntermenge verwalten soll, die nicht in der Vorlage enthalten ist, können Sie entweder eine Anwendungseinheit für eine Datenverkehrsuntermenge hinzufügen oder die vorhandene Anwendungseinheit ändern. Nachdem Sie die Konfiguration angepasst haben, können Sie auch die Reihenfolge der Auswertung für jede Datenverkehrs-Teilmenge angeben, die von der Anwendung verwaltet wird.

Die Konfiguration einer AppExpert Anwendung besteht aus den folgenden Schritten:

1. Öffentliche Endpunkte konfigurieren
2. Anwendungseinheiten konfigurieren
3. Angeben der Evaluierungsreihenfolge
4. Anzeigen der Anwendungskonfiguration mit Visualizer

Außerdem können Sie die Richtlinien konfigurieren, die von der Vorlage bereitgestellt wurden. Wenn die AppExpert Anwendungsvorlage keine Richtlinien für ein bestimmtes Citrix ADC Feature enthält, z. B. Rewrite oder Anwendungsfirewall, können Sie eigene Richtlinien konfigurieren.

Konfigurieren von öffentlichen Endpunkten

October 5, 2021

Wenn Sie beim Importieren einer AppExpert t-Anwendung keinen öffentlichen Endpunkt angegeben haben, können Sie nach dem Erstellen der Anwendung öffentliche Endpunkte angeben. Sie können einen öffentlichen Endpunkt vom Typ HTTP und einen öffentlichen Endpunkt vom Typ HTTPS für Ihre AppExpert t-Anwendung konfigurieren.

Wenn Endpunkte bereits für die Anwendung konfiguriert sind, können Sie Endpunkte von der AppExpert Anwendung trennen und alle Endpunkte löschen, die Sie nicht mehr benötigen. Beachten Sie, dass beim Trennen eines öffentlichen Endpunkts von der AppExpert t-Anwendung der Endpunkt automatisch von der zugeordneten Anwendungseinheit aufgehoben wird, aber nicht aus dem System gelöscht wird.

So konfigurieren Sie öffentliche Endpunkte für eine AppExpert Anwendung:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.

2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendung, für die Sie öffentliche Endpunkte konfigurieren möchten, und klicken Sie dann auf Bearbeiten.
3. Wechseln Sie auf der Seite **Anwendungen** zum Abschnitt **Öffentlicher Endpunkt** und klicken Sie auf das Stiftsymbol.
4. Legen Sie im Schieberegler **Öffentlicher Endpunkt** die folgenden Parameter fest.
   a) Öffentlicher Endpunkttyp. Wählen Sie das Optionsfeld, um den Endpunkttyp zu definieren.
   b) Name. Name des öffentlichen Endpunkts.
   c) IP-Adresse. IP-Adresse des öffentlichen Endpunkts.
   d) Port. Portnummer des öffentlichen Endpunkts.
   e) -Protokoll. Wählen Sie einen Protokolltyp als HTTP oder HTTPS aus.
5. Klicken Sie auf **Weiter.**
6. Wählen Sie im Abschnitt **Anwendungseinheiten** eine Anwendungseinheit aus der Liste aus.
7. Klicken Sie auf **Weiter**, um die Richtlinien- und Serverdetails festzulegen.
8. Klicken Sie auf **OK** und dann auf Fertig.
9. Klicken Sie auf Schließen.

Weitere Informationen zu den Parametern im Dialogfeld **Öffentlichen Endpunkt konfigurieren** finden Sie unter Content Switching.

Konfigurieren von Diensten und Servicegruppen für eine Anwendungseinheit

October 5, 2021

Wenn Sie einen Dienst oder eine Dienstgruppe konfigurieren, ändern Sie entweder einen vorhandenen Dienst oder eine vorhandene Dienstgruppe oder fügen der AppExpert Anwendung neue Dienste hinzu. Sie fügen Dienste oder Dienstgruppen hinzu, wenn Sie sie beim Importieren der Anwendungsvorlage nicht angegeben haben. Außerdem fügen Sie Dienste und Dienstgruppen hinzu, wenn Sie die Anzahl der Server erhöhen, auf denen Instanzen der Anwendung gehostet werden. Sie können eine Dienst- und Dienstgruppe für eine Anwendungseinheit erst konfigurieren, nachdem Sie den Dienst oder die Dienstgruppe für die AppExpert Anwendung konfiguriert haben.

So konfigurieren Sie einen Dienst oder eine Dienstgruppe für die AppExpert Anwendung:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendung, und klicken Sie dann auf **Bearbeiten.**
3. Wählen Sie auf der Seite **Anwendungen** eine Anwendungseinheit aus, und klicken Sie dann auf **Weiter** .

4. Gehen Sie im Abschnitt **Dienste und Dienstgruppen** folgendermaßen vor:
   a) Legen Sie im Schieberegler Dienstbindung die folgenden Parameter fest.
      i. Dienst. Wählen Sie einen Lastausgleichsdienst aus der Liste aus, oder erstellen Sie einen neuen Dienst.
      ii. Gewicht: Geben Sie einen Gewichtswert für den Service an.
   b) Klicken Sie auf **Binden** und dann auf **Fertig.**
   c) Legen Sie im Schieberegler ServiceGroup-Bindung die folgenden Parameter fest:
      i. Dienstgruppenname. Wählen Sie eine Lastausgleichsdienstgruppe aus, oder erstellen Sie eine neue Servicegruppe.
      ii. Klicken Sie auf **Bind** und dann auf **Done**.
   d) Klicken Sie auf **Fertig**.
5. Klicken Sie auf **Weiter**, um andere Konfigurationen festzulegen.

Anwendungseinheiten erstellen

October 5, 2021

Möglicherweise müssen Sie Anwendungseinheiten für Traffic-Teilmengen hinzufügen, die entweder spezifisch für Ihre Webanwendungsimplementierung sind oder nicht in der Vorlage definiert sind. Beim Erstellen einer Anwendungseinheit müssen Sie eine Regel für die Anwendungseinheit konfigurieren.

So erstellen Sie eine Anwendungseinheit für die AppExpert Anwendung:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendung, für die Sie eine Anwendungseinheit hinzufügen möchten, und klicken Sie dann auf **Hinzufügen**.
3. Wechseln Sie auf der Seite **Anwendungen** zum Abschnitt **Anwendungseinheiten** und klicken Sie auf das **Bleistiftsymbol** .

So konfigurieren Sie Richtlinienausdrücke für eine Anwendungseinheit:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendung, für die Sie eine Anwendungseinheit hinzufügen möchten, und klicken Sie dann auf **Hinzufügen**.
3. ****Wechseln Sie auf der Seite Anwendungen zum** Abschnitt Anwendungseinheiten** und klicken Sie auf das **Symbol **+, um eine Einheit zu erstellen und Richtlinienausdrücke hinzuzufügen.
4. Führen Sie einen der folgenden Schritte aus, um das Format des neuen Ausdrucks anzugeben:
   a) Um anzugeben, dass Sie einen klassischen Ausdruck im Feld Regel konfigurieren möchten, klicken Sie auf Klassische Syntax.

b) Klicken Sie auf Standardsyntax, um anzugeben, dass Sie einen erweiterten Ausdruck im Feld Regel konfigurieren möchten.
c) Konfigurieren Sie im Feld Regel den Ausdruck.

5. Klicken Sie auf **OK**.

Konfigurieren von Anwendungseinheitenregeln

October 5, 2021

Sie können eine Anwendungseinheitenregel so konfigurieren, dass bestimmte Arten von Datenverkehr eingeschlossen oder ausgeschlossen werden. Wenn Sie die Regel konfigurieren, können Sie auch die Syntax des Ausdrucks definieren.

So konfigurieren Sie eine Anwendungseinheitenregel:

1. Erweitern Sie im Navigationsbereich der GUI AppExpert, und klicken Sie dann auf **Anwendungen**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendungseinheit, für die Sie die Regel ändern möchten, und klicken Sie dann auf **Öffnen**.
3. Gehen Sie im Dialogfeld Anwendungseinheit konfigurieren folgendermaßen vor:
   a) Führen Sie einen der folgenden Schritte aus, um das Format des neuen Ausdrucks anzugeben:
      - Um anzugeben, dass Sie einen klassischen Ausdruck im Feld Regel konfigurieren möchten, klicken Sie auf **Klassische Syntax**.
      - Klicken Sie auf **Standardsyntax**, um anzugeben, dass Sie einen erweiterten Ausdruck im Feld Regel konfigurieren möchten.
   b) Konfigurieren Sie im Feld Regel den Ausdruck.
4. Klicken Sie auf **OK**.

Konfigurieren von Richtlinien für Anwendungseinheiten

October 5, 2021

Für eine AppExpert t-Anwendung können Sie Richtlinien für Komprimierung, Caching, Rewrite, Responder und Application Firewall konfigurieren. Die Vorlagen, die Sie von der Citrix Community-Website herunterladen, enthalten eine Reihe von Richtlinien, die die gängigsten Anwendungsverwaltungsanforderungen erfüllen. Möglicherweise möchten Sie diese Richtlinien optimieren oder anpassen. Wenn der Richtliniensatz für eine bestimmte Anwendungseinheit keine Richtlinien für ein bestimmtes Feature enthält, können Sie eigene Richtlinien für dieses Feature erstellen und binden.

Wenn Sie eine AppExpert Anwendung ohne Vorlage erstellen, müssen Sie alle Richtlinien konfigurieren, die die Webanwendung benötigt.

Die GUI verwendet verschiedene Symbole, um anzugeben, ob Richtlinien für ein Feature konfiguriert sind. Wenn für eine Anwendungseinheit eine Richtlinie für ein bestimmtes Feature konfiguriert ist, wird ein Symbol angezeigt, das das Feature darstellt. Wenn beispielsweise eine Komprimierungsrichtlinie für eine Anwendungseinheit konfiguriert ist, wird in der Spalte Komprimierung für die Anwendungseinheit ein Komprimierungssymbol angezeigt. Für Features, für die keine Richtlinie konfiguriert ist, wird ein Symbol mit einem Pluszeichen (+) angezeigt.

Hinweis: Wenn Sie Richtlinien für Anwendungseinheiten konfigurieren, müssen Sie möglicherweise Richtlinien und Ausdrücke konfigurieren, die entweder in der klassischen oder der Standardsyntax enthalten sind. Wenn Sie Standard-Syntaxrichtlinien konfigurieren, müssen Sie möglicherweise Parameter wie Goto-Ausdrücke angeben und Richtlinienbanken aufrufen.

Informationen zum Konfigurieren von Richtlinien und Ausdrücken in beiden Formaten finden Sie unter Richtlinien und Ausdrücke.

Komprimierungsrichtlinien konfigurieren

Sie können entweder klassische Richtlinien oder erweiterte Richtlinien verwenden, um die Komprimierung zu konfigurieren, aber Sie können keine Komprimierungsrichtlinien beider Typen an dieselbe Anwendungseinheit binden.

So konfigurieren Sie eine Komprimierungsrichtlinie für eine Anwendungseinheit:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich in der Zeile für die zu konfigurierende Anwendungseinheit auf das Symbol in der Spalte Komprimierung.
3. Führen Sie im Dialogfeld Komprimierungsrichtlinien konfigurieren eine oder mehrere der folgenden Aktionen aus, abhängig von den Konfigurationsaufgaben, die Sie ausführen möchten:
    - Klicken Sie auf Zur Standardsyntax wechseln, wenn Sie eine Standard-Syntaxkomprimierungsrichtlinie konfigurieren möchten. Wenn Sie klassische Komprimierungsrichtlinien binden oder konfigurieren möchten und sich in der Standardsyntax befinden, können Sie auf Zur klassischen Syntax wechseln klicken, um zur klassischen Richtlinienansicht zurückzukehren und mit dem Ändern gebundener klassischer Richtlinien zu beginnen oder neue klassische Komprimierungsrichtlinien zu erstellen und zu binden.
      Wichtig: Diese Einstellung bestimmt auch, welche Richtlinien angezeigt werden, wenn Sie eine Richtlinie einfügen möchten. Wenn Sie sich beispielsweise in der Standardsyntaxansicht befinden und auf Richtlinie einfügen klicken, enthält die Liste, die in der Spalte Richtlinienname angezeigt wird, nur Standard-Syntaxrichtlinien. Richtlinien beider Typen können nicht an eine Anwendungseinheit gebunden werden.

- Wenn Sie klassische Richtlinien konfigurieren möchten, klicken Sie entweder auf Anfrage oder Antwort, je nachdem, ob die Richtlinie zur Anforderungszeit oder zur Antwortzeit ausgewertet werden soll.
  Sie können sowohl klassische Komprimierungsrichtlinien für die Anforderungszeit als auch für die Antwortzeit für eine Anwendungseinheit konfigurieren. Wenn keine Übereinstimmung gefunden wurde, wertet die Appliance nach der Auswertung aller Anforderungszeitrichtlinien die Antwortzeitrichtlinien aus.
- Um eine Komprimierungsrichtlinie zu ändern, die bereits an die Anwendungseinheit gebunden ist, klicken Sie auf den Namen der Richtlinie, und klicken Sie dann auf Richtlinie ändern. Ändern Sie dann im Dialogfeld Komprimierungsrichtlinie konfigurieren die Richtlinie, und klicken Sie dann auf OK.
  Informationen zum Ändern einer Komprimierungsrichtlinie finden Sie unter Komprimierung.
- Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf den Namen der Richtlinie und dann auf Richtlinie aufheben.
- Um die Priorität zu ändern, die einer Richtlinie zugewiesen ist, doppelklicken Sie auf den Prioritätswert, und geben Sie dann einen neuen Wert ein.
- Um zugewiesene Prioritäten neu zu generieren, klicken Sie auf Prioritäten neu generieren.
- Um eine neue Richtlinie einzufügen, klicken Sie auf **Richtlinie einfügen** und in der Liste, die in der Spalte Richtlinienname angezeigt wird, auf **Neue Richtlinie**. Konfigurieren Sie dann im Dialogfeld Komprimierungsrichtlinie erstellen die Richtlinie, und klicken Sie dann auf **Erstellen**.
  Informationen zum Ändern einer Komprimierungsrichtlinie finden Sie unter Komprimierung.
- Wenn Sie einen Standardsyntaxausdruck konfigurieren, gehen Sie wie folgt vor:
  - Wählen Sie in der Spalte Gehe zu Ausdruck einen Gehe zu -Ausdruck aus.
  - Geben Sie in der Spalte Invoke die Richtlinienbank an, die Sie aufrufen möchten, wenn die aktuelle Richtlinie TRUE ergibt.

4. Klicken Sie auf **Änderungen übernehmen**und dann auf **Schließen**.

Konfigurieren von Caching-Richtlinien

Sie können nur Standard-Syntaxrichtlinien und -ausdrücke zum Konfigurieren von Caching-Richtlinien verwenden.

So konfigurieren Sie Caching-Richtlinien für eine Anwendungseinheit:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich in der Zeile für die zu konfigurierende Anwendungseinheit auf das Symbol in der Spalte Caching.
3. Führen Sie im Dialogfeld Cache-Richtlinien konfigurieren je nach den Konfigurationsaufgaben,

die Sie ausführen möchten, eine oder mehrere der folgenden Aktionen aus:

- Klicken Sie entweder auf Anfrage oder Antwort, je nachdem, ob die Richtlinie zur Anforderungszeit oder zur Antwortzeit ausgewertet werden soll.
  Sie können sowohl Anforderungs- als auch Antwortzeit-Caching-Richtlinien für eine Anwendungseinheit konfigurieren. Wenn keine Übereinstimmung gefunden wurde, wertet die Appliance nach der Auswertung aller Anforderungszeitrichtlinien die Antwortzeitrichtlinien aus.
- Um eine Caching-Richtlinie zu ändern, die bereits an die Anwendungseinheit gebunden ist, klicken Sie auf den Namen der Richtlinie, und klicken Sie dann auf Richtlinie ändern. Ändern Sie dann im Dialogfeld **Cache-Richtlinie konfigurieren** die Richtlinie, und klicken Sie dann auf **OK** .
  Informationen zum Ändern einer Caching-Richtlinie finden Sie unter Integriertes Caching.
- Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf den Namen der Richtlinie und dann auf **Richtlinie aufheben**.
- Um die Priorität zu ändern, die einer Richtlinie zugewiesen ist, doppelklicken Sie auf den Prioritätswert, und geben Sie dann einen neuen Wert ein.
- Um zugewiesene Prioritäten neu zu generieren, klicken Sie auf **Prioritäten neu generieren**.
- Um eine neue Richtlinie einzufügen, klicken Sie auf **Richtlinie einfügen** und in der Liste, die in der Spalte Richtlinienname angezeigt wird, auf **Neue Richtlinie**. Konfigurieren Sie dann im Dialogfeld **Cache-Richtlinie erstellen** die Richtlinie, und klicken Sie dann auf **Erstellen** .
  Informationen zum Ändern einer Caching-Richtlinie finden Sie unter Integriertes Caching.
- Wählen Sie in der Spalte Gehe zu Ausdruck einen Gehe zu -Ausdruck aus.
- Geben Sie in der Spalte Invoke die Richtlinienbank an, die Sie aufrufen möchten, wenn die aktuelle Richtlinie TRUE ergibt.

4. Klicken Sie auf **Änderungen übernehmen**und dann auf **Schließen**.

Konfigurieren von Rewrite-Richtlinien

Sie können nur Standard-Syntaxrichtlinien und -ausdrücke zum Konfigurieren von Umschreibrichtlinien verwenden.

So konfigurieren Sie Umschreibrichtlinien für eine Anwendungseinheit:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich in der Zeile für die zu konfigurierende Anwendungseinheit auf das Symbol in der Spalte Umschreiben.
3. Führen Sie im Dialogfeld **Rewrite-Richtlinien konfigurieren** eine oder mehrere der folgenden Aktionen aus, je nach den Konfigurationsaufgaben, die Sie ausführen möchten:
   - Klicken Sie entweder auf Anfrage oder Antwort, je nachdem, ob die Richtlinie zur

Anforderungszeit oder zur Antwortzeit ausgewertet werden soll.
Sie können sowohl Anforderungs- als auch Antwortzeit-Rewrite-Richtlinien für eine Anwendungseinheit konfigurieren. Wenn keine Übereinstimmung gefunden wurde, wertet die Appliance nach der Auswertung aller Anforderungszeitrichtlinien die Antwortzeitrichtlinien aus.

- Um eine Richtlinie zum Umschreiben zu ändern, die bereits an die Anwendungseinheit gebunden ist, klicken Sie auf den Namen der Richtlinie, und klicken Sie dann auf **Richtlinie ändern**. Ändern Sie dann im Dialogfeld Richtlinie neu schreiben konfigurieren die Richtlinie, und klicken Sie dann auf **OK**.
  Informationen zum Ändern einer Rewrite-Richtlinie finden Sie unter Umschreiben.
- Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf den Namen der Richtlinie und dann auf **Richtlinie aufheben**.
- Um die Priorität zu ändern, die einer Richtlinie zugewiesen ist, doppelklicken Sie auf den Prioritätswert, und geben Sie dann einen neuen Wert ein.
- Um zugewiesene Prioritäten neu zu generieren, klicken Sie auf **Prioritäten neu generieren**.
- Um eine neue Richtlinie einzufügen, klicken Sie auf **Richtlinie einfügen** und klicken Sie in der Liste, die in der Spalte **Richtlinienname** angezeigt wird, auf **Neue Richtlinie.** Konfigurieren Sie dann im Dialogfeld **Rewrite-Richtlinie erstellen** die Richtlinie, und klicken Sie dann auf **Erstellen** .
  Informationen zum Ändern einer Rewrite-Richtlinie finden Sie unter Umschreiben.
- Wählen Sie in der Spalte Gehe zu Ausdruck einen Gehe zu -Ausdruck aus.
- Geben Sie in der Spalte Invoke die Richtlinienbank an, die Sie aufrufen möchten, wenn die aktuelle Richtlinie TRUE ergibt.

4. Klicken Sie auf **Änderungen übernehmen**und dann auf **Schließen**.

Konfigurieren von Responderrichtlinien

Sie können nur Standard-Syntaxrichtlinien und -ausdrücke zum Konfigurieren von Responder-Richtlinien verwenden.

So konfigurieren Sie Responder-Richtlinien für eine Anwendungseinheit:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich in der Zeile für die zu konfigurierende Anwendungseinheit auf das Symbol in der Spalte Responder.
3. **Führen Sie im Dialogfeld Responderrichtlinien konfigurieren** eine oder mehrere der folgenden Aktionen aus, abhängig von den Konfigurationsaufgaben, die Sie ausführen möchten:
   - Um eine Filterrichtlinie zu ändern, die bereits an die Anwendungseinheit gebunden ist, klicken Sie auf den Namen der Richtlinie, und klicken Sie dann auf **Richtlinie ändern**. Ändern Sie dann im Dialogfeld Responderrichtlinie konfigurieren die Richtlinie, und klicken

Sie dann auf **OK**.
Informationen zum Ändern einer Responder-Richtlinie finden Sie unter Responder.

- Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf den Namen der Richtlinie und dann auf **Richtlinie aufheben**.
- Um die Priorität zu ändern, die einer Richtlinie zugewiesen ist, doppelklicken Sie auf den Prioritätswert, und geben Sie dann einen neuen Wert ein.
- Um zugewiesene Prioritäten neu zu generieren, klicken Sie auf **Prioritäten neu generieren**.
- Um eine neue Richtlinie einzufügen, klicken Sie auf Richtlinie einfügen und klicken Sie in der Liste, die in der Spalte Richtlinienname angezeigt wird, auf Neue Richtlinie. Konfigurieren Sie dann im Dialogfeld Responder-Richtlinie erstellen die Richtlinie, und klicken Sie dann auf Erstellen.
  Informationen zum Ändern einer Responder-Richtlinie finden Sie unter Responder.
- Wählen Sie in der Spalte Gehe zu Ausdruck einen Gehe zu -Ausdruck aus.
- Geben Sie in der Spalte Invoke die Richtlinienbank an, die Sie aufrufen möchten, wenn die aktuelle Richtlinie TRUE ergibt.

4. Klicken Sie auf **Änderungen übernehmen**und dann auf **Schließen**.

Konfigurieren von Richtlinien für die Anwendungsfirewall

Sie können sowohl klassische als auch standardmäßige Syntaxrichtlinien und Ausdrücke für die Anwendungsfirewall konfigurieren. Wenn jedoch eine Richtlinie eines Typs bereits global oder an einen virtuellen Server gebunden ist, der auf der Appliance konfiguriert ist, können Sie eine Richtlinie des anderen Typs nicht an eine Anwendungseinheit binden. Wenn beispielsweise eine Standard-Syntaxrichtlinie bereits global oder an einen virtuellen Server gebunden ist, können Sie keine klassische Richtlinie an eine Anwendungseinheit binden.

So konfigurieren Sie die Application Firewall-Richtlinien für eine Anwendungseinheit:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich in der Zeile für die zu konfigurierende Anwendungseinheit auf das Symbol in der Spalte **Anwendungsfirewall** .
3. **Führen Sie im Dialogfeld Anwendungsfirewall Richtlinien konfigurieren** je nach den Konfigurationsaufgaben, die Sie ausführen möchten, eine oder mehrere der folgenden Aktionen aus:
   - Klicken Sie entweder auf Klassischer Ausdruck oder auf Erweiterter Ausdruck, abhängig vom Ausdruckstyp, den Sie für die Anwendungsfirewall konfigurieren möchten.
     Wichtig: Diese Einstellung legt auch fest, welche Richtlinien angezeigt werden, wenn Sie eine Richtlinie einfügen möchten. Wenn Sie beispielsweise “Erweiterter Ausdruck” auswählen und auf **Richtlinie einfügen**klicken, enthält die Liste, die in der Spalte **Richtlinienname** angezeigt wird, nur Standard-Syntaxrichtlinien. Richtlinien beider Typen können nicht an eine Anwendungseinheit gebunden werden. Diese Option ist

nicht verfügbar, wenn eine Richtlinie eines beliebigen Typs bereits global oder an einen virtuellen Server gebunden ist.

- Um eine Anwendungsfirewall Richtlinie zu ändern, die bereits an die Anwendungseinheit gebunden ist, klicken Sie auf den Namen der Richtlinie, und klicken Sie dann auf Richtlinie ändern. Ändern Sie dann im Dialogfeld Anwendungsfirewall Richtlinie konfigurieren die Richtlinie, und klicken Sie dann auf OK.
  Informationen zum Ändern einer Anwendungs-Firewall-Richtlinie finden Sie unter Richtlinien.
- Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf den Namen der Richtlinie und dann auf Richtlinie aufheben.
- Um die Priorität zu ändern, die einer Richtlinie zugewiesen ist, doppelklicken Sie auf den Prioritätswert, und geben Sie dann einen neuen Wert ein.
- Um zugewiesene Prioritäten neu zu generieren, klicken Sie auf Prioritäten neu generieren.
- Um eine neue Richtlinie einzufügen, klicken Sie auf **Richtlinie einfügen** und in der Liste, die in der Spalte **Richtlinienname** angezeigt wird, auf Neue Richtlinie. Konfigurieren Sie dann im Dialogfeld **Anwendungs-Firewall-Richtlinie erstellen** die Richtlinie, und klicken Sie dann auf **Erstellen** .
  Informationen zum Ändern einer Anwendungs-Firewall-Richtlinie finden Sie unter Richtlinien.

4. Klicken Sie auf **Änderungen übernehmen**und dann auf **Schließen**.

Anwendungseinheiten konfigurieren

October 5, 2021

So konfigurieren Sie eine Anwendungseinheit mit der GUI:

1. Navigieren Sie zu **AppExpert** > **Anwendungen** > **Anwendungseinheit**, und klicken Sie dann auf das Plus-Symbol, um eine neue Anwendungseinheit für eine Datenverkehrsuntermenge hinzuzufügen.
2. Legen Sie im Schieberegler **Anwendungseinheit** die folgenden Parameter fest:
   - Name
   - Ausdruck

   Sie können einen Ausdruck einfügen, indem Sie die Ausdruckskomponenten manuell hinzufügen oder den Link Ausdrucksеditor verwenden. Um einen Ausdruck manuell hinzuzufügen, geben Sie eine Selektorkomponente ein, und geben Sie dann einen Punkt (.) ein, um eine Liste anzuzeigen, aus der Sie die nächste Komponente auswählen können. Geben Sie beispielsweise HTTP ein, und geben Sie dann einen Punkt ein. Es wird ein Dropdownmenü angezeigt. Der

Inhalt dieses Menüs enthält die Schlüsselwörter, die dem von Ihnen eingegebenen Anfangsschlüsselwort folgen können. Wählen Sie eine Komponente aus dem Dropdownmenü aus. Im Textfeld Ausdruck* werden nun die Komponenten angezeigt, die Sie dem Ausdruck hinzugefügt haben (z. B. HTTP.REQ). Fügen Sie weiterhin Komponenten hinzu, bis der vollständige Ausdruck gebildet wird.

Wenn Sie Unterstützung beim Erstellen des Ausdrucks bevorzugen, können Sie den Link Ausdrucksеditor verwenden. Auf der Seite Ausdrucksеditor können Sie einen Ausdruck bilden, indem Sie Komponenten aus den Dropdownfeldern auswählen. Wählen Sie die Komponenten aus, und klicken Sie auf Fertig, um den Ausdruck auf der Seite Anwendungseinheit einzufügen.

3. Klicken Sie auf **Weiter**, um Dienste und Dienstgruppen zu binden.
4. Klicken Sie auf den Abschnitt **Service**, um einen virtuellen Dienst auszuwählen oder hinzuzufügen und ihn an die Anwendungseinheit zu binden.
5. Klicken Sie auf **Weiter**, und klicken Sie auf den Abschnitt **Dienstgruppe**, um eine virtuelle Dienstgruppe auszuwählen oder hinzuzufügen und sie an die Anwendungseinheit zu binden.
6. Klicken Sie auf **Binden** und **Fortfahren**, um Erweiterte Einstellungen (wie Richtlinien, Methode, Persistenz, Schutz, Profile, Push, Authentifizierung und Verkehrseinstellungen) für die Anwendungseinheit zu konfigurieren.
7. Klicken Sie auf das **Plus-Symbol** in jedem Abschnitt, um die Konfigurationsparameter festzulegen.
8. Klicken Sie auf **OK** und dann auf **Fertig**.

So bearbeiten Sie eine Anwendungseinheit für eine Anwendung mit der GUI:

Navigieren Sie zu **AppExpert** > **Anwendungen**, wählen Sie eine Anwendung aus und klicken Sie auf **Bearbeiten**. Wählen Sie im Abschnitt **Anwendungseinheit** eine Entität aus, klicken Sie auf das Symbol Bearbeiten, und ändern Sie die Einstellungen der Anwendungseinheit.

Hinweis: Sie können den Namen und den Regelausdruck für eine vorhandene Anwendungseinheit nicht ändern.

Mit den Video-Tutorials von Citrix ADC können Sie Citrix ADC Funktionen auf einfache und einfache Weise verstehen. Sehen Sie sichhttps://www.youtube.com/watch?v=bJ5_i8fV2hc Video an, um zu erfahren, wie Sie eine Anwendungseinheit konfigurieren.

Konfigurieren von öffentlichen Endpunkten für eine Anwendung

October 5, 2021

So konfigurieren Sie öffentliche Endpunkte für eine Anwendung mit der GUI:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**, wählen Sie eine Anwendungsentität aus, und klicken Sie dann auf **Bearbeiten**.
2. Klicken Sie im Abschnitt **Öffentlicher Endpunkt** auf **+**, um einen neuen öffentlichen Endpunkt zu konfigurieren.
3. Führen Sie im Schieberegler **Öffentlicher Endpunkt** eine der folgenden Aktionen aus:
   a) Klicken Sie auf **Neu**, um einen neuen Endpunkt zu erstellen.
   b) Klicken Sie auf **Vorhandener öffentlicher Endpunkt**, um einen Endpunkt aus der Dropdownliste auszuwählen.
4. Legen Sie die folgenden Endpunktparameter fest:
   a) Name
   b) IP-Adresse
   c) Protokoll
   d) Port
5. Klicken Sie auf **Weiter**, um zusätzliche Einstellungen wie Anwendungseinheiten, GSLB-Serverbindungen, Richtlinien, Profile, Push, Verkehrseinstellungen und Authentifizierung zu konfigurieren.
6. Klicken Sie auf **OK** und dann auf **Fertig**.
7. Klicken Sie auf **Weiter** und dann **Fertig**.

So bearbeiten Sie einen öffentlichen Endpunkt für eine Anwendung mit der GUI:

Navigieren Sie zu **AppExpert** > **Anwendungen**, wählen Sie eine Anwendung aus, und klicken Sie auf **Bearbeiten** . Wählen Sie im Abschnitt **Öffentlicher Endpunkt** einen Endpunkt aus, klicken Sie auf das Stiftsymbol, und ändern Sie die Endpunkteinstellungen.

So löschen Sie einen öffentlichen Endpunkt für eine Anwendung mit der GUI:

Navigieren Sie zu **AppExpert** > **Anwendungen** > **Öffentlicher Endpunkt,** klicken Sie auf das Stiftsymbol, um das Löschsymbol neben der Entität anzuzeigen.

Mit den Video-Tutorials von Citrix ADC können Sie Citrix ADC Funktionen auf einfache und einfache Weise verstehen. Sehen Sie sichhttps://www.youtube.com/watch?v=z4v-edQiVpw Video an, um zu erfahren, wie Sie einen öffentlichen Endpunkt konfigurieren.

Angeben der Reihenfolge der Auswertung von Anwendungseinheiten

October 5, 2021

Anwendungseinheitenregeln werden in der Reihenfolge ausgewertet, in der sie in der GUI platziert werden. Die Regel, die für die oberste Anwendungseinheit konfiguriert ist, wird immer zuerst konfiguriert, gefolgt von der Regel, die für die zweite oberste Anwendungseinheit konfiguriert ist usw. Die Standardanwendungseinheit wird immer zuletzt ausgewertet.

Wenn eine Anforderung mit der Regel übereinstimmt, die für eine Anwendungseinheit konfiguriert ist, wird die Anforderung von der Anwendungseinheit verarbeitet, und es wird kein weiterer Abgleich durchgeführt. Daher wird die Reihenfolge der Auswertung von Anwendungseinheiten zu einem wichtigen Faktor, wenn sich die Verkehrsuntermengen für zwei oder mehr Anwendungseinheiten überschneiden. Wenn sich die Verkehrsuntermengen für zwei oder mehr Anwendungseinheiten überschneiden, müssen Sie die Reihenfolge angeben, in der eine eingehende Anforderung mit den Regeln der Anwendungseinheit abgeglichen wird.

So legen Sie die Reihenfolge der Auswertung der Anwendungseinheiten fest:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**, wählen Sie eine Anwendung aus und klicken Sie auf **Bearbeiten**. Klicken Sie im Abschnitt **Anwendungseinheit** auf das **Bleistiftsymbol**, und bewegen Sie den Cursor über das Kontrollkästchen links neben dem Namen der Anwendungseinheit. Klicken Sie auf das Symbol, das neben dem Kontrollkästchen angezeigt wird, und halten Sie die Maus gedrückt, um die Anwendung an eine neue Position in der Prioritätsliste nach oben oder unten zu ziehen.

Persistenzgruppen für Anwendungseinheiten konfigurieren

October 5, 2021

Sie können eine Persistenzgruppe für die Anwendungseinheiten in einer AppExpert Anwendung konfigurieren. Im Kontext einer AppExpert t-Anwendung ist eine Persistenzgruppe eine Gruppe von Anwendungseinheiten, die Sie als einzelne Entität behandeln können, um allgemeine Persistenzeinstellungen anzuwenden. Wenn die Anwendung in eine Anwendungsvorlagendatei exportiert wird, werden die Persistenzgruppeneinstellungen berücksichtigt, die beim Importieren der AppExpert t-Anwendung automatisch auf die Anwendungseinheiten angewendet werden.

So konfigurieren Sie eine Persistenzgruppe für eine Anwendung mit der GUI:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Dialogfeld **Anwendungsansicht** auf den Namen der Anwendung, für deren Anwendungseinheiten Sie eine Persistenzgruppe konfigurieren möchten, und klicken Sie dann auf **Persistenzgruppen** konfigurieren.
3. **Führen Sie im Dialogfeld Persistenzgruppen konfigurieren** eine der folgenden Aktionen aus:
   - Klicken Sie auf Hinzufügen, um eine Persistenzgruppe **hinzuzufügen**.
   - Um eine Persistenzgruppe zu ändern, klicken Sie auf **Öffnen**.
4. **Legen Sie im Dialogfeld Persistenzgruppe erstellen** oder **Persistenzgruppe konfigurieren** die folgenden Parameter fest:
   - Gruppenname — Name der Persistenzgruppe. Damit die Citrix ADC Appliance die Persistenzgruppe als Teil der Anwendungskonfiguration erkennt, muss der Name der AppExpert

Anwendung als Präfix im Namen der Persistenzgruppe enthalten sein. Daher zeigt die Appliance standardmäßig das Präfix im Feld Gruppenname an, und Sie können dieses Präfix nicht entfernen. Geben Sie nach dem Präfix einen Namen Ihrer Wahl ein.

- Persistenz — Typ der Persistenz für den virtuellen Server. Wenn Sie SOURCEIP auswählen, geben Sie im Feld IPv4-Netzmaske eine Netzwerkmaske ein, die die Anzahl der Bits angibt, die die Appliance beim Erstellen von Persistenzsitzungen berücksichtigen muss. Wenn Sie COOKIEINSERT auswählen, geben Sie in den Feldern Cookie-Domain und Cookie-Name ein Domänenattribut an, das in der Set-Cookie-Direktive gesendet werden soll, und einen Namen für das Cookie an.
- Timeout — Zeitraum, für den eine Persistenzsitzung gültig ist.
- Backup-Persistenz — Typ der Backup-Persistenz für die Gruppe.
- Backup-Timeout — Zeitraum in Minuten, für die die Backup-Persistenz wirksam ist.
- Anwendungseinheiten — Um der Persistenzgruppe eine Anwendungseinheit hinzuzufügen, klicken Sie im Feld Verfügbare Anwendungseinheiten auf die Anwendungseinheit, und klicken Sie dann auf Hinzufügen. Um eine Anwendungseinheit aus der Persistenzgruppe zu entfernen, klicken Sie im Feld Konfigurierte Anwendungseinheiten auf die Anwendungseinheit, und klicken Sie dann auf **Entfernen**.

5. Klicken Sie auf **OK**.

Anzeigen von AppExpert Anwendungen und Konfigurieren von Entitäten mithilfe des Anwendungsvisualizers

October 5, 2021

Die Visualizer-Funktion zeigt Ihnen eine grafische Darstellung der Konfiguration einer Anwendung. Sie enthält den Namen des öffentlichen Endpunkts, die dem öffentlichen Endpunkt zugewiesenen Anwendungseinheiten und die Anzahl der an die Anwendung gebundenen Richtlinien und Dienste. Sie können den Visualizer verwenden, um einen visuellen Überblick über die Konfiguration einer AppExpert Anwendung zu erhalten und einige der angezeigten Entitäten zu konfigurieren. Standardmäßig zeigt Visualizer Anwendungseinheiten, Dienste und Monitore für die ausgewählte Anwendung an.

So zeigen Sie eine AppExpert Anwendung mithilfe des Application Visualizers an:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**, wählen Sie eine Anwendungsentität aus, und klicken Sie auf **Visualizer** .

Konfigurieren der Benutzerauthentifizierung, Autorisierung und Überwachung

October 5, 2021

Sie können die Autorisierung für Benutzer und Gruppen konfigurieren, um dann den Zugriff auf eine AppExpert Anwendung zu ermöglichen. Wenn der AAA-Benutzer oder die Gruppe, für die Sie Berechtigungen konfigurieren möchten, noch nicht erstellt wurde, können Sie ihn über AppExpert erstellen und dann Berechtigungen für den Anwendungszugriff konfigurieren.

So konfigurieren Sie AAA-Benutzer und AAA-Benutzergruppen für eine Anwendung mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **AppExpert** > **Anwendungen**, wählen Sie eine Anwendungsentität aus, und klicken Sie dann auf **Bearbeiten**.
2. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Autorisierung**, und konfigurieren Sie autorisierte Benutzer und Benutzergruppen.
3. Klicken Sie auf den Abschnitt **AAA** Benutzer, um autorisierte Benutzer an die Anwendung zu binden.
4. Legen Sie im Schieberegler **AAA User** die Parameter fest.
5. Klicken Sie auf **Weiter**, und klicken Sie dann im Abschnitt **Erweiterte Einstellungen** auf **Autorisierungsrichtlinien**.
6. Binden Sie im Schieberegler **Autorisierungsrichtlinie** eine Autorisierungsrichtlinie an die Anwendung.
7. Klicken Sie auf **Weiter**, und klicken Sie dann im Abschnitt **Erweiterte Einstellungen** auf den Abschnitt **Autorisierungsgruppe**.
8. Binden Sie im Schieberegler **AAA-Gruppenbindung** eine Autorisierungsbenutzergruppe an die Anwendung.
9. Klicken Sie auf **Weiter**, und klicken Sie dann im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.
10. Binden Sie im Schieberegler " **Richtlinien** " eine **Audit Syslog-** oder **Audit NSlog-Richtlinie** an die Anwendung.
11. Klicken Sie auf **Weiter** und dann **Fertig**.

So bearbeiten Sie AAA-Benutzer und AAA-Benutzergruppen für eine Anwendung mit der GUI:

Navigieren Sie zu **AppExpert** > **Anwendungen** > **Erweiterte Einstellungen** und klicken Sie auf **Autorisierung**. Klicken Sie dann auf das Symbol Bearbeiten, und geben Sie Werte für die Autorisierungseinstellungen für Benutzer oder Benutzergruppen an.

So löschen Sie AAA-Benutzer und AAA-Benutzergruppen mit der GUI:

Navigieren Sie zu **AppExpert** > **Anwendungen**, wählen Sie eine Anwendung aus und klicken Sie auf

Bearbeiten. Klicken Sie auf der Seite **Anwendungen** auf **Erweiterte Einstellungen** und dann auf **Autorisierung**. Klicken Sie auf das Löschsymbol neben der Entität.

Überwachung einer Citrix ADC Anwendung

October 5, 2021

Nachdem Sie die AppExpert Anwendung angepasst haben, können Sie Anwendungsstatistiken anzeigen, um sicherzustellen, dass die Anwendung und alle zugehörigen Entitäten ordnungsgemäß funktionieren. Sie können den Application Visualizer auch verwenden, um Statistiken zu überwachen, die bestimmten Entitäten wie Richtlinien und virtuellen Servern zugeordnet sind.

Sie können auch die Trefferindikatoren für verschiedene Entitäten in regelmäßigen Abständen anzeigen, um sicherzustellen, dass Leistungsindikatoren aktualisiert werden.

Anwendungsstatistiken anzeigen

Im Knoten **Anwendungen** können Sie eine Anwendung auswählen und die Seite Statistiken für die Anwendung anzeigen. Auf der Seite Statistiken können Sie den Zustand und Status von öffentlichen Endpunkten und Anwendungseinheiten überwachen und die folgenden statistischen Informationen anzeigen:

- Anfragen und Antworten pro Sekunde für alle öffentlichen Endpunkte und Anwendungseinheiten.
- Bytes pro Sekunde an jedem Endpunkt für eingehenden und ausgehenden Datenverkehr.
- Die Anwendungseinheit trifft Zähler und die Anzahl der Client- und Serververbindungen für jede Anwendungseinheit.
- Statistiken für die Dienste, die an die Anwendungseinheiten gebunden sind.

Auf der Seite Statistiken können Sie auch CPU-Auslastung, Speicherauslastung und Systemprotokolle anzeigen.

So zeigen Sie Statistiken für eine Anwendung an:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich auf die Anwendung, für die Sie Statistiken anzeigen möchten, und klicken Sie dann auf **Statistiken**.

Überwachen einer Anwendung mit dem Application Visualizer

Sie können den Application Visualizer verwenden, um die Anzahl der Anfragen, die pro Sekunde zu einem bestimmten Zeitpunkt von den vservern empfangen werden, und die Anzahl der Treffer

pro Sekunde zu einem bestimmten Zeitpunkt für Rewrite, Responder und Cache-Richtlinien zu überwachen.

So zeigen Sie Statistikinformationen für vServer, Umschreibrichtlinien, Responder-Richtlinien und Cache-Richtlinien im Visualizer an:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Wählen Sie im Detailbereich die Anwendung aus, für die Sie statistische Informationen anzeigen möchten, und klicken Sie dann auf **Visualizer**.
3. Führen Sie im Fenster **Application Visualizer** die folgenden Schritte aus:
   - Um die Statistiken anzuzeigen, klicken Sie auf **Statistiken anzeigen**.
     Die statistischen Informationen werden auf den jeweiligen Knoten im Visualizer angezeigt. Diese Informationen werden nicht in Echtzeit aktualisiert und müssen manuell aktualisiert werden.
   - Um die statistischen Informationen zu aktualisieren, klicken Sie auf **Statistiken aktualisieren**.

Treffer anzeigen

Die Trefferindikatoren, die für verschiedene AppExpert Anwendungsentitäten bereitgestellt werden, ermöglichen es Ihnen, das Funktionieren öffentlicher Endpunkte und Anwendungseinheiten zu überwachen. Für eine Anwendung zeigt das Dialogfeld Treffer die Gesamtzahl der Anforderungen an, die von jedem konfigurierten öffentlichen Endpunkt empfangen werden. Für eine Anwendungseinheit zeigt das Dialogfeld Treffer die Anzahl der Anforderungen an, die die Anwendungseinheit von jedem öffentlichen Endpunkt verarbeitet hat, sowie die Gesamtanzahl der Treffer an. Anweisungen zum Anzeigen von Trefferzählern finden Sie unter Überprüfen und Testen der Konfiguration.

Löschen einer Anwendung

October 5, 2021

Wenn Sie eine Anwendung und ihre Anwendungseinheiten nicht mehr benötigen, können Sie sie löschen. Wenn Sie eine AppExpert Anwendung löschen, werden Back-End-Dienste nicht gelöscht, und alle öffentlichen Endpunkte, die von der Anwendung verwendet werden, werden für andere Anwendungen verfügbar.

Beim Löschen einer Anwendung werden Sie außerdem aufgefordert anzugeben, ob gebundene Richtlinien und Aktionen gelöscht werden sollen, die an anderer Stelle nicht verwendet werden.

So löschen Sie eine Anwendungseinheit für eine Anwendung mit der GUI:

Navigieren Sie zu **AppExpert** > **Anwendungen**, wählen Sie eine Anwendung aus und klicken Sie auf **Bearbeiten**. Klicken Sie im Abschnitt **Anwendungseinheit** auf das Löschsymbol neben der Entität

Konfigurieren der Anwendungsauthentifizierung, -autorisierung und -überwachung

October 5, 2021

Sie können Authentifizierung, Autorisierung und Überwachung (AAA) für die Anwendungen konfigurieren, die Sie auf der Appliance konfigurieren. Eine Authentifizierungsrichtlinie, die für eine Anwendung konfiguriert ist, definiert den Authentifizierungstyp, der angewendet werden soll, wenn ein Benutzer oder eine Gruppe versucht, auf die Anwendung zuzugreifen. Wenn eine externe Authentifizierung verwendet wird, gibt die Richtlinie auch den externen Authentifizierungsserver an. Für eine Anwendung konfigurierte Autorisierungsrichtlinien geben an, ob ein bestimmter Benutzer oder eine bestimmte Gruppe auf die Anwendung zugreifen kann. Überwachungsrichtlinien definieren den Typ des Überwachungsprotokolls, die Ebene, auf der die Protokollierung ausgeführt wird, und andere Überwachungsservereinstellungen. Authentifizierungs- und Überwachungsrichtlinien verwenden das klassische Richtlinienformat.

Authentifizierungsrichtlinien, Autorisierungsrichtlinien und Überwachungsrichtlinien können in beliebiger Reihenfolge konfiguriert werden. Bevor Sie AAA für eine Anwendung konfigurieren, müssen Sie jedoch einen öffentlichen Endpunkt für die Anwendung konfigurieren.

Das Konfigurieren der Authentifizierung für eine Anwendung umfasst die Angabe eines Authentifizierungs-FQDN, eines virtuellen Authentifizierungsservers, eines Serverzertifikats sowie Authentifizierungs- und Sitzungsrichtlinien. Authentifizierungsrichtlinien werden automatisch an den für die Anwendung angegebenen virtuellen Authentifizierungsserver gebunden.

So konfigurieren Sie die Authentifizierung für eine AppExpert Anwendung:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   a) Klicken Sie auf Hinzufügen, um eine Authentifizierung für eine neue Anwendung hinzuzufügen.
   b) Klicken Sie auf Bearbeiten, um eine vorhandene Anwendung zu ändern.
3. Wählen Sie auf der Seite **Anwendungen** eine Anwendungseinheit aus.
4. Klicken Sie auf der Schiebereglerseite **Anwendungseinheit** im Abschnitt **Erweiterte Einstellungen** auf Authentifizierung.
5. Wählen Sie im Abschnitt **Authentifizierung** den Authentifizierungstyp wie folgt aus:
   a) Formularbasierte Authentifizierung
   b) 401-basierte Authentifizierung

c) Ohne

6. Klicken Sie auf **OK** und dann auf **Fertig**.

Konfigurieren der Anwendungsautorisierung

Sie können die Autorisierung für Benutzer und Gruppen konfigurieren, um dann den Zugriff auf eine AppExpert Anwendung zu ermöglichen. Wenn der AAA-Benutzer oder die Gruppe, für die Sie Berechtigungen konfigurieren möchten, noch nicht erstellt wurde, können Sie ihn über AppExpert erstellen und dann Berechtigungen für den Anwendungszugriff konfigurieren.

So konfigurieren Sie Berechtigungen für einen AAA-Benutzer oder -Gruppe für den Zugriff auf eine AppExpert Anwendung:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich auf die AppExpert Anwendung, für die Sie einen Benutzer- oder Gruppenzugriff konfigurieren möchten.
3. Klicken Sie auf der Seite **Anwendungen**, und klicken Sie dann im Abschnitt **Erweiterte Einstellungen** auf Autorisierung.
4. Führen Sie einen der folgenden Schritte aus:
   - Wenn sich der AAA-Benutzer oder die Gruppe, für die Sie Berechtigungen konfigurieren möchten, bereits in der Gruppe Gruppen/Benutzer befindet, ziehen Sie den Benutzer oder die Gruppe aus der Struktur Gruppen/Benutzer auf den Knoten Benutzer oder Gruppen in der Anwendungsstruktur. Klicken Sie dann mit der rechten Maustaste auf den Benutzer oder die Gruppe, und klicken Sie auf Allow.
   - Wenn der AAA-Benutzer oder die Gruppe, für die Sie Berechtigungen konfigurieren möchten, auf der Appliance nicht konfiguriert ist, klicken Sie in der Anwendungsstruktur mit der rechten Maustaste auf Benutzer oder Gruppen, und klicken Sie dann auf Hinzufügen. Geben Sie im Dialogfeld AAA-Gruppe erstellen oder AAA-Benutzer erstellen die Werte ein, klicken Sie auf Erstellen, und klicken Sie dann auf Schließen.
     Der Benutzer oder die Gruppe wird mit dem Berechtigungssatz “Zulassen” erstellt. Um die Berechtigungseinstellung zu ändern, klicken Sie mit der rechten Maustaste auf die Gruppe oder den Benutzer, und klicken Sie dann auf die Berechtigungseinstellung.
5. Klicken Sie auf **Fertig**, und klicken Sie dann auf **Schließen** .

Konfigurieren der Anwendungsüberwachung

Wenn Sie Überwachungsrichtlinien für eine Anwendung konfigurieren, müssen Sie den Server angeben, auf den die Protokollmeldungen gerichtet werden müssen, das Format der protokollierten Nachrichten und die Protokollebene. Optional können Sie weitere Einstellungen konfigurieren, z. B. die Protokollfunktion und das Datumsformat. Überwachungsrichtlinien werden automatisch an alle öffentlichen Endpunkte der AppExpert Anwendung gebunden.

So konfigurieren Sie Überwachungsrichtlinien für eine Anwendung:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich auf die Anwendung, für die Sie Überwachungsrichtlinien konfigurieren möchten.
3. Klicken Sie auf der Schiebereglerseite der Anwendungseinheit im Abschnitt **Richtlinien** auf +, um die Überwachungsrichtlinien zu konfigurieren.
4. Wählen Sie auf der Schiebereglerseite **Richtlinien** den Richtlinientyp Syslog-Auditing oder Nslog-Auditing aus, und klicken Sie auf **Weiter** .
5. Legen Sie im Abschnitt Richtlinienbindung die folgenden Parameter fest.
   a) Wählen Sie eine Richtlinie für die Bindung aus. Wenn Sie keine Richtlinie zum Binden haben, klicken Sie auf +, um eine neue Richtlinie zu erstellen.
   b) Um eine neue Überwachungsrichtlinie zu erstellen, klicken Sie unter Richtlinienname auf **Neue Richtlinie,** und führen Sie dann auf der Seite **Richtlinie** die folgenden Schritte aus:
      i. Geben Sie im Feld Name einen Namen für die Richtlinie ein.
      ii. Das Feld Name enthält bereits die Zeichenfolge, die am Anfang des Servernamens erforderlich ist. Sie können die Zeichenfolge nicht ändern.
      iii. Wählen Sie in der Liste Überwachungstyp den Überwachungstyp aus (SYSLOG oder NSLOG).
      iv. Wenn der Überwachungsserver, den Sie angeben möchten, bereits in der Liste Server aufgeführt ist, wählen Sie den Server aus der Liste aus, und klicken Sie dann auf Ändern, wenn Sie die Servereinstellungen ändern möchten. Ändern Sie im Dialogfeld Überwachungsserver konfigurieren die Einstellungen entsprechend, und klicken Sie dann auf OK. Weitere Informationen zu den Einstellungen im Dialogfeld Überwachungsserver konfigurieren finden Sie unter Auditing Authenticated Sessions.
      v. Wenn Sie einen neuen Überwachungsserver konfigurieren möchten, klicken Sie auf Neu, und geben Sie dann im Dialogfeld Überwachungsserver erstellen einen Namen für den Server ein, geben Sie die IP-Adresse des Servers, die Portnummer und andere Einstellungen an. Wenn Sie fertig sind, klicken Sie auf **OK**.
      vi. Klicken Sie auf **Erstellen**.
   c) Um die Prioritäten für die neuen Überwachungsrichtlinien zu ändern, die Sie erstellt haben, klicken Sie unter Priorität für jede Richtlinie, für die Sie die Priorität ändern möchten, doppelklicken Sie auf den Prioritätswert, und geben Sie einen neuen Prioritätswert ein.
   d) Um Prioritäten zu regenerieren, klicken Sie auf **Prioritäten neu generieren**.
   e) Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf die Richtlinie, und klicken Sie dann auf **Richtlinie aufheben**.
   f) Um eine Richtlinie zu ändern, klicken Sie auf die Richtlinie und dann auf **Richtlinie ändern.**

6. Klicken Sie auf **Änderungen anwenden** und dann auf **Schließen**.

Deaktivieren von AAA für eine Anwendung

Nachdem Sie AAA für eine Anwendung konfiguriert haben, können Sie die AAA-Konfiguration für diese Anwendung deaktivieren. Wenn Sie AAA für eine Anwendung deaktivieren, geht die Konfiguration nicht verloren. Sie können AAA für die Anwendung aktivieren, wenn Sie die Konfiguration erneut anwenden möchten.

So aktivieren oder deaktivieren Sie AAA für eine Anwendung:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich auf die Anwendung, für die Sie AAA aktivieren oder deaktivieren möchten, und führen Sie dann eine der folgenden Aktionen aus:
3. Um AAA für die Anwendung zu deaktivieren, klicken Sie auf **AAA ausschalten.**
4. Um AAA für die Anwendung zu aktivieren, klicken Sie **auf AAA aktivieren**.

Einrichten einer benutzerdefinierten Citrix ADC Anwendung

December 7, 2021

Wenn eine AppExpert Anwendungsvorlage für die Webanwendung, die Sie über die Citrix ADC Appliance verwalten möchten, nicht verfügbar ist oder wenn verfügbare AppExpert Anwendungsvorlagen Ihren Anforderungen nicht entsprechen, können Sie eine AppExpert-Anwendung ohne Vorlage erstellen.

Um eine AppExpert Anwendung ohne Vorlage zu erstellen, müssen Sie zunächst eine Anwendung und Anwendungseinheiten erstellen. Anschließend konfigurieren Sie öffentliche Endpunkte, Dienste und Dienstgruppen. Schließlich konfigurieren Sie die Richtlinien, die bestimmen, wie der Anwendungsdatenverkehr ausgewertet und verarbeitet wird.

Nachdem Sie die Anwendungs- und Anwendungseinheiten erstellt und Richtlinien konfiguriert haben, müssen Sie die Konfiguration überprüfen und testen, um sicherzustellen, dass sie ordnungsgemäß funktioniert, genau wie beim Konfigurieren einer Anwendung mithilfe einer vordefinierten AppExpert Anwendungsvorlage. Anschließend müssen Sie die Anwendung überwachen, um sicherzustellen, dass die Anwendung und ihre Entitäten ordnungsgemäß funktionieren.

Erstellen einer Anwendung

Wenn Sie eine AppExpert Anwendung erstellen, erstellt die Appliance einen Container, dem Sie Anwendungseinheiten hinzufügen können. Die Standardanwendungseinheit wird erst erstellt, wenn Sie die erste Anwendungseinheit erstellt haben.

So erstellen Sie eine AppExpert Anwendung mit der GUI:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf **Anwendungen**, und klicken Sie dann auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld Anwendung erstellen** unter Name einen Namen für die Anwendung ein, und klicken Sie dann auf **OK** .

Anwendungseinheiten erstellen

Für jede Teilmenge des Datenverkehrs, die Ihrer Webanwendung zugeordnet ist, müssen Sie eine Anwendungseinheit erstellen.

So erstellen Sie mit der GUI eine Anwendungseinheit für die AppExpert t-Anwendung:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendung, für die Sie eine Anwendungseinheit hinzufügen möchten, und klicken Sie dann auf **Hinzufügen**.
3. Klicken Sie auf **Erstellen**.

Konfigurieren von öffentlichen Endpunkten für eine AppExpert Anwendung

Nachdem Sie alle benötigten Anwendungseinheiten erstellt haben, müssen Sie einen oder mehrere öffentliche Endpunkte konfigurieren, damit Clients über die Citrix ADC Appliance auf die Webanwendung zugreifen können.

So konfigurieren Sie öffentliche Endpunkte für eine AppExpert Anwendung mit der GUI:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendung, für die Sie öffentliche Endpunkte konfigurieren möchten, und klicken Sie dann auf **Öffentliche Endpunkte konfigurieren**.
3. Führen Sie im Dialogfeld Öffentliche Endpunkte auswählen für die Anwendung eine der folgenden Aktionen aus:
    - Wenn die gewünschten Endpunkte im Dialogfeld aufgeführt sind, aktivieren Sie die entsprechenden Kontrollkästchen.
    - Wenn Sie alle öffentlichen Endpunkte angeben möchten, klicken Sie auf **Alle aktivieren**.
    - Wenn Sie Endpunkte von der AppExpert Anwendung trennen möchten, deaktivieren Sie die entsprechenden Kontrollkästchen.
    - Wenn Sie einen neuen öffentlichen Endpunkt erstellen möchten, klicken Sie auf **Hinzufügen**. Konfigurieren Sie dann im Dialogfeld Öffentliche Endpunkte erstellen Endpunkteinstellungen, und klicken Sie dann auf **OK**.

Im Dialogfeld **Öffentliche Endpunkte erstellen** können Sie nur den Namen, die IP-Adresse, den Port und das Protokoll für den Endpunkt angeben. Sie können zusätzliche Endpunkteinstellungen angeben, nachdem Sie den öffentlichen Endpunkt erstellt haben. Wenn Sie zusätzliche Endpunkteinstellungen angeben möchten, klicken Sie nach dem Erstellen des Endpunkts im Dialogfeld Öffentliche Endpunkte auswählen auf den Endpunkt, und klicken Sie dann auf **Öffnen**. Geben Sie dann im Dialogfeld **Öffentliche Endpunkte konfigurieren** zusätzliche Einstellungen ein, und klicken Sie dann auf **OK** .
Weitere Informationen zu den Parametern in den Dialogfeldern **Public Endpoint erstellen** und **Public Endpoint konfigurieren** finden Sie unter Content Switching.

- Wenn Sie einen öffentlichen Endpunkt ändern möchten, klicken Sie auf den Endpunkt, und klicken Sie dann auf **Öffnen**. Ändern Sie dann im Dialogfeld **Öffentlichen Endpunkt konfigurieren** die Einstellungen für den Endpunkt, und klicken Sie dann auf **OK**.
Weitere Informationen zu den Parametern im Dialogfeld Öffentlichen Endpunkt konfigurieren finden Sie unter Content Switching.

4. Klicken Sie auf **Schließen**.

Konfigurieren von öffentlichen Endpunkten für eine Anwendungseinheit

Für eine Anwendungseinheit geben Sie öffentliche Endpunkte wie öffentliche Endpunkte für eine Anwendung an, die aus einer AppExpert Anwendungsvorlage erstellt wird. Weitere Informationen zum Angeben einer Teilmenge der Endpunkte für eine Anwendungseinheit finden Sie unter Konfigurieren von Endpoints für eine Anwendungseinheit.

So konfigurieren Sie Endpunkte für eine Anwendungseinheit mit der GUI:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendungseinheit, für die Sie öffentliche Endpunkte angeben möchten, und klicken Sie dann auf **Öffentliche Endpunkte konfigurieren**.
3. Führen **Sie im Dialogfeld Öffentliche Endpunkte auswählen** für die Anwendungseinheit eine der folgenden Aktionen aus:
   - Wenn Sie Endpunkte für die Anwendungseinheit zum ersten Mal angeben, deaktivieren Sie die Kontrollkästchen, die den Endpunkten entsprechen, die nicht an die Anwendungseinheit gebunden werden sollen.
   - Wenn Sie Endpunkte angeben möchten, die im Dialogfeld aufgeführt sind, aber derzeit nicht an die Anwendungseinheit gebunden sind, aktivieren Sie die entsprechenden Kontrollkästchen.
4. Klicken Sie auf **OK**.

Konfigurieren von Services und Servicegruppen für eine AppExpert Anwendung

Dienste und Dienstgruppen sind nur für Anwendungseinheiten verfügbar, nachdem Sie die Dienste und Dienstgruppen für die AppExpert Anwendung konfiguriert haben. Daher müssen Sie Dienste und Dienstgruppen für die AppExpert Anwendung konfigurieren, bevor Sie die Dienste für die Anwendungseinheiten konfigurieren. Alle Dienste und Dienstgruppen, die Sie für eine AppExpert Anwendung konfigurieren, müssen dasselbe Protokoll verwenden (entweder HTTP oder HTTPS). Das Verfahren zum Konfigurieren von Diensten und Dienstgruppen für eine AppExpert Anwendung, die nicht aus einer Vorlage erstellt wird, entspricht dem für eine Anwendung, die aus einer Vorlage erstellt wurde.

So konfigurieren Sie einen Dienst oder eine Dienstgruppe für die AppExpert Anwendung mit der GUI:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendung, für die Sie Dienste oder Dienstgruppen konfigurieren möchten, und klicken Sie dann auf **Backend-Dienste konfigurieren**.
3. Führen Sie im Dialogfeld Backend Services konfigurieren einen der folgenden Schritte aus:
   - Um Dienste zu konfigurieren, klicken Sie auf die Registerkarte **Dienste** .
   - Um Dienstgruppen zu konfigurieren, klicken Sie auf die Registerkarte **Dienstgruppen**.
4. Führen Sie auf der Registerkarte **Dienst** oder **Dienstgruppen** eine der folgenden Aktionen aus:
   - Wenn die gewünschten Dienste oder Servicegruppen auf der Registerkarte aufgeführt sind, klicken Sie auf die entsprechenden Kontrollkästchen.
   - Wenn Sie alle Dienste oder Dienstgruppen angeben möchten, klicken Sie auf **Alle aktivieren**.
   - Wenn Sie einen neuen Dienst oder eine neue Dienstgruppe erstellen möchten, klicken Sie auf **Hinzufügen**. Konfigurieren Sie dann im Dialogfeld **Dienst erstellen**oder **Dienstgruppe** erstellen Einstellungen für den Dienst bzw. die Dienstgruppe, und klicken Sie dann auf **Erstellen**.
   - Wenn Sie einen Dienst ändern möchten, klicken Sie auf den Dienst, und klicken Sie dann auf Öffnen. Konfigurieren Sie dann im Dialogfeld **Dienst konfigurieren** oder **Dienstgruppe erstellen** Einstellungen für den Dienst bzw. die Dienstgruppe, und klicken Sie dann auf **OK**.

Informationen zu den Einstellungen in den Dialogfeldern Service erstellen, Dienst konfigurieren und **Dienstgruppe erstellen** finden Sie unter Lastenausgleich.

Konfigurieren von Diensten und Servicegruppen für eine Anwendungseinheit

Nachdem Sie Dienste und Dienstgruppen konfiguriert haben, müssen Sie Dienste und Dienstgruppen für jede Anwendungseinheit konfigurieren. Dieser Schritt ist jedoch nicht erforderlich, wenn jeder Backend-Dienst alle Inhalte hostet, die mit der Webanwendung verknüpft sind. Sie konfigurieren Dienste und Dienstgruppen für eine Anwendungseinheit, wenn der mit der Anwendungseinheit verknüpfte

Inhalt nur auf einer Teilmenge der Backend-Server gehostet wird.

So konfigurieren Sie Dienste oder Dienstgruppen für eine Anwendungseinheit mit der GUI:

1. Navigieren Sie zu **AppExpert** > **Anwendungen**.
2. Klicken Sie im Detailbereich mit der rechten Maustaste auf die Anwendungseinheit, für die Sie einen Dienst oder eine Dienstgruppe konfigurieren möchten, und klicken Sie dann auf **Backend-Dienste konfigurieren**.
3. **Führen Sie im Dialogfeld Backend Services konfigurieren** einen der folgenden Schritte aus:
   - Um Dienste zu konfigurieren, klicken Sie auf die Registerkarte **Dienste** .
   - Um Dienstgruppen zu konfigurieren, klicken Sie auf die Registerkarte **Dienstgruppen**.
4. Führen Sie auf der Registerkarte **Dienste** oder **Dienstgruppen** einen der folgenden Schritte aus:
   - Deaktivieren Sie die Kontrollkästchen, die den Diensten oder Dienstgruppen entsprechen, die für die Anwendungseinheit nicht konfiguriert werden sollen. Stellen Sie sicher, dass die Kontrollkästchen, die den Diensten oder Dienstgruppen entsprechen, die Sie für die Anwendungseinheit konfigurieren möchten, aktiviert sind. Geben Sie dann in der Spalte Gewicht die Gewichtung an, die Sie jedem konfigurierten Dienst zuweisen möchten.
   - Um alle Dienste oder Dienstgruppen anzugeben, klicken Sie auf **Alle aktivieren**.
5. Geben Sie auf den Registerkarten **Methode**, **Persistenz** und **Erweitert** die gewünschten Parameter an.
6. Klicken Sie auf **OK**.

Konfigurieren von Richtlinien

Die Verfahren zum Konfigurieren von Richtlinien für eine AppExpert Anwendung, die ohne Verwendung einer Vorlage erstellt wird, entsprechen denen für eine AppExpert-Anwendung, die aus einer Vorlage erstellt wurde. Weitere Informationen finden Sie unter Konfigurieren von Richtlinien für Anwendungseinheiten.

Erstellen und Verwalten von Vorlagendateien

October 5, 2021

Nachdem Sie eine AppExpert Anwendung eingerichtet und an Ihre Anforderungen angepasst haben, können Sie eine Vorlage aus der Konfiguration erstellen und dann die Vorlage für andere Administratoren freigeben. Sie können auch eine Vorlage erstellen und die Vorlage dann in andere Citrix ADC Appliances importieren, die eine ähnliche AppExpert t-Anwendungskonfiguration erfordern. Dies vereinfacht und beschleunigt das Einrichten ähnlicher Anwendungen auf anderen Appliances.

AppExpert Anwendungsvorlagendateien können entweder in das Vorlagenverzeichnis der Citrix ADC Appliance oder in einen Ordner auf Ihrem lokalen Computer exportiert werden. Anschließend können

Sie die Vorlagen hochladen und von der Citrix ADC Appliance herunterladen und herunterladen und die Vorlagen umbenennen, die im AppExpert-Anwendungsvorlagen-Verzeichnis auf Ihrer Appliance gespeichert sind.

AppExpert Anwendungsvorlagendateien können entweder in das Vorlagenverzeichnis der Citrix ADC Appliance oder in einen Ordner auf Ihrem lokalen Computer exportiert werden. Anschließend können Sie die Vorlagen hochladen und von der Citrix ADC Appliance herunterladen und herunterladen und die Vorlagen umbenennen, die im AppExpert-Anwendungsvorlagen-Verzeichnis auf Ihrer Appliance gespeichert sind.

Exportieren einer AppExpert Anwendung in eine Vorlagendatei

October 5, 2021

Wenn Sie eine AppExpert t-Anwendung exportieren, werden alle Anwendungskonfigurationsinformationen in eine Vorlagendatei exportiert, und alle bereitstellungsspezifischen Informationen werden in eine Bereitstellungsdatei exportiert. Die Zeichenfolge _deployment wird automatisch an den Namen der Vorlagendatei angehängt, um den Namen der Bereitstellungsdatei zu erstellen. Beide Dateien sind im XML-Format. Wenn Sie die Anwendungsvorlagendatei in die Citrix ADC Appliance exportieren möchten, wird die Vorlagendatei im Verzeichnis /nsconfig/nstemplates/applications gespeichert und die Bereitstellungsdatei im Verzeichnis /nsconfig/nstemplates/applications/deployment_files/ gespeichert. Wenn Sie eine Citrix Gateway Anwendung konfiguriert haben, können Sie die Citrix Gateway-Richtlinien in die Vorlage aufnehmen.

So exportieren Sie eine AppExpert t-Anwendung mit der GUI in eine Vorlagendatei:

1. Navigieren Sie zu **AppExpert** > **Anwendung**, wählen Sie eine Anwendungsentität aus, und klicken Sie dann auf **Bearbeiten** .
2. Klicken Sie auf der Seite **Anwendungen** auf den Link Als Vorlage **exportieren**, um die Anwendungskonfigurations- und Bereitstellungseinstellungen als Vorlage zu exportieren.
3. Legen Sie im Schieberegler **Anwendung exportieren** die folgenden Parameter fest:
   a) Vorlagendateiname
   b) Bereitstellungsdateiname
4. Klicken Sie auf **Weiter** und **Fertig** .
5. Navigieren Sie zu **AppExpert** > **Anwendung**, und klicken Sie auf **Vorlagen verwalten**, um die exportierte Konfiguration auf den Registerkarten **Vorlagendatei** und **Bereitstellungsdatei** als Dateien anzuzeigen.

Exportieren der Konfiguration eines virtuellen Content Switching-Servers in eine Vorlagendatei

October 5, 2021

Sie können auch eine Content Switching-Konfiguration als Anwendungsvorlage exportieren. Sie können eine Konfiguration für den virtuellen Content Switching-Server in eine Anwendungsvorlage exportieren, entweder im Bereich “Content Switching Virtual Servers” oder unter Content Switching Visualizer. Konfigurationsinformationen, einschließlich des virtuellen Content Switching-Servers, aller zugeordneten virtuellen Server, Dienste, Dienstgruppen und Richtlinien für den Lastenausgleich, werden in eine Vorlagendatei exportiert, und alle bereitstellungsspezifischen Informationen werden in eine Bereitstellungsdatei exportiert. Die Zeichenfolge _deployment wird automatisch an den Namen der Vorlagendatei angehängt, um den Namen der Bereitstellungsdatei zu erstellen. Beide Dateien sind im XML-Format. Wenn Sie die Anwendungsvorlagendatei in die Citrix ADC Appliance exportieren möchten, wird die Vorlagendatei im Verzeichnis /nsconfig/nstemplates/applications auf der Citrix ADC-Appliance gespeichert und die Bereitstellungsdatei im Verzeichnis /nsconfig/nstemplates/applications/deployment_files/ gespeichert.

Weitere Informationen zum Format von Anwendungsvorlagen und Bereitstellungsdateien finden Sie unter Grundlegendes zu Citrix ADC Anwendungsvorlagen und Bereitstellungsdateien. Zu den exportierten Konfigurationsinformationen gehören der virtuelle Content Switching-Server, alle zugeordneten virtuellen Server, Dienste, Dienstgruppen und Richtlinien für den Lastenausgleich.

Wenn der virtuelle Content Switching-Server jedoch bereits als öffentlicher Endpunkt für eine AppExpert t-Anwendung konfiguriert ist, können Sie die Konfiguration nicht in eine Vorlagendatei exportieren. In diesem Szenario müssen Sie die zugeordnete AppExpert t-Anwendung in eine Vorlage exportieren.

Weitere Informationen zum Exportieren einer AppExpert-Anwendung in eine Vorlagendatei finden Sie unter Exportieren einer AppExpert-Anwendung in eine Vorlagendatei.

So exportieren Sie eine Content Switching-Konfiguration aus dem Content Switching Visualizer über die GUI in eine Anwendungsvorlagendatei:

1. Navigieren Sie zu Traffic Management > Content Switching > Virtuelle Server.
2. Klicken Sie im Detailbereich auf den Namen des virtuellen Content Switching-Servers, dessen Konfiguration Sie als Vorlagendatei exportieren möchten, und klicken Sie dann auf Visualizer.
3. Klicken Sie im Content Switching Visualizer auf das Symbol für den Content Switching vserver, klicken Sie auf Verwandte Aufgaben, und klicken Sie dann auf Vorlage erstellen.
4. Geben Sie im Dialogfeld Als Vorlage exportieren… einen Namen für die Vorlagendatei ein, und führen Sie dann eine der folgenden Aktionen aus:
    - Stellen Sie sicher, dass Durchsuchen (Appliance) angezeigt wird, um die Vorlagendatei in die Appliance zu exportieren.

- Um die Vorlagendatei auf den Computer zu exportieren, klicken Sie auf das Dropdownmenü Durchsuchen (Appliance), klicken Sie auf Lokal, navigieren Sie zu dem Speicherort, an dem die Datei gespeichert werden soll, und klicken Sie dann auf Speichern.

5. Geben Sie die folgenden Informationen an:
   - **Einleitungsbeschreibung**— Jeder Text, der während des Imports die AppExpert t-Anwendungsvorlage einführt. Dieser Text wird beim Importieren der Vorlage auf der Seite Anwendungsname angeben des AppExpert Vorlagenassistenten angezeigt.
   - **Zusammenfassung Beschreibung**— Jede Zusammenfassung, die Sie möglicherweise auf der Seite Zusammenfassung des AppExpert Vorlagenassistenten anzeigen möchten, wenn die Vorlage importiert wird.
   - **Autor**— Der Name des Autors der Vorlage.
   - **Major**— Die Hauptversionsnummer der Vorlage.
   - **Minor**— Die Nebenversionsnummer der Vorlage. Diese Nummer wird an die Hauptversionsnummer angehängt und auf der Seite Zusammenfassung des AppExpert Vorlagenassistenten während des Imports im Format Major.Minor angezeigt.
6. Klicken Sie auf OK.

So exportieren Sie eine Content Switching-Konfiguration in eine Anwendungsvorlagendatei aus dem Bereich Virtuelle Server mit der GUI:

1. Navigieren Sie zu Traffic Management > Content Switching > Virtuelle Server.
2. Klicken Sie im Detailbereich auf den Namen des virtuellen Content Switching-Servers, dessen Konfiguration Sie als Vorlagendatei exportieren möchten, und klicken Sie dann auf AppExpert Template erstellen.
3. Führen Sie die Schritte 4 bis 6 aus, die unter **So exportieren Sie eine Content Switching-Konfiguration in eine Anwendungsvorlagendatei mit dem Content Switching Visualizer** beschrieben werden.

Variablen in Anwendungsvorlagen erstellen

October 5, 2021

Anwendungsvorlagen unterstützen die Deklaration von Variablen in den Richtlinienausdrücken und -aktionen, die für eine Anwendung konfiguriert sind. Durch die Möglichkeit, Variablen in Richtlinienausdrücken und -aktionen zu deklarieren, können Sie vorkonfigurierte Werte in Ausdrücken (z. B. konfigurierbare Parameter wie der Hostname eines Servers oder das Ziel für eine Umschreibungsaktion) durch Werte ersetzen, die der Umgebung entsprechen, in die Sie die Vorlage importieren. Wenn Variablen für eine AppExpert t-Anwendungsvorlage konfiguriert wurden, enthält der AppExpert-Vorlagen-Assistent, der beim Importieren einer AppExpert-Anwendungsvorlage angezeigt wird, eine Seite Variablenwerte angeben, auf der Sie geeignete Werte für die für die Vorlage konfigurierten

Variablen angeben können.

Betrachten Sie als Beispiel den folgenden Richtlinienausdruck, der konfiguriert ist, um den Wert des Host-Headers in einer HTTP-Anforderung auszuwerten:

```
1 HTTP.REQ.HEADER("Host").CONTAINS("server1")
2 <!--NeedCopy-->
```

Wenn der Servername zum Importzeitpunkt konfigurierbar sein soll, können Sie die Zeichenfolge "server1" als Variable angeben. Beim Importieren der Vorlage können Sie auf der Registerkarte Variablen einen neuen Wert für die Variable angeben.

Nachdem Sie eine Variable erstellt haben, können Sie Folgendes tun:

- Weisen Sie einer vorhandenen Variablen zusätzliche Zeichenfolgen zu. Nachdem Sie eine Variable für eine Zeichenfolge erstellt haben, können Sie andere Teile desselben oder eines anderen Ausdrucks auswählen und der Variablen zuweisen. Die Zeichenfolgen, die Sie einer Variablen zuweisen, müssen nicht identisch sein. Beim Importieren werden alle Zeichenfolgen, die der Variablen zugewiesen sind, durch den von Ihnen angegebenen Wert ersetzt.
- Zeigen Sie die Zeichenfolge (en) an, die der Variablen zugewiesen sind.
- Zeigen Sie eine Liste aller Entitäten und Parameter an, die die Variable verwenden.

Im Assistenten zum Exportieren von Anwendungsvorlagen können Sie Variablen in bestimmten Feldern für die folgenden Entitäten definieren:

- Cache-Richtlinien
- Richtlinien umschreiben
- Umschreiben von Aktionen
- Responder-Richtlinien
- Responder-Aktionen

So konfigurieren Sie eine Variable in einem Richtlinienausdruck oder -aktion mit der GUI:

1. Navigieren Sie zu **AppExpert > Variablen**.
2. Klicken Sie auf der Seite **Variablen** auf **Hinzufügen**.
3. **Legen Sie auf der Seite Variablen erstellen** die folgenden Parameter fest.
   Name. Name der Variablen.

   Geltungsbereich. Wählen Sie den Bereich als Global oder Transaktion aus.

   Geben Sie ein. Wählen Sie den Variablentyp als Text, ulong, map.

   Läuft in ab. Geben Sie das Ablaufdatum ein.

   Wenn Voll*. Aktion, die ausgeführt werden soll, wenn eine Zuweisung zu einer Karte die konfigurierten Max-Einträge überschreitet:

lru - (Standard) Wiederverwendung des zuletzt verwendeten Eintrags in der Karte.
undef - Erzwingen Sie die Zuweisung, ein undefiniertes Ergebnis (Undef) an die Richtlinie zurückzugeben, die die Zuweisung ausführt.
Mögliche Werte: undef, lru
Standardwert: lru.

wenn kein Wert vorhanden ist. Wert Ablaufdatum in Sekunden. Wenn der Wert nicht innerhalb des Ablaufzeitraums referenziert wird, wird er gelöscht. 0 (Standardeinstellung) bedeutet kein Ablaufdatum. Mindestwert: 0, Maximalwert: 31622400

Init-Wert. Initialisierungswert für diese Variable, auf den eine Singleton-Variable oder ein Map-Eintrag gesetzt wird, wenn sie referenziert wird, bevor eine Zuweisungsaktion ihr einen Wert zugewiesen hat. Wenn der Singleton-Variable oder dem Map-Eintrag bereits ein Wert zugewiesen wurde, hat das Setzen dieses Parameters keine Auswirkung auf diesen Variablenwert. Standard: 0 für ulong, NULL für Text Maximale Länge: 127

Kommentare. Eine kurze Beschreibung der Variablen.

4. Klicken Sie auf **Schließen**.

Vorlagendateien hochladen und herunterladen

October 5, 2021

Vorlagendateien können von Ihrem lokalen Computer auf die Citrix ADC Appliance hochgeladen oder von der Appliance auf Ihren lokalen Computer heruntergeladen werden. Auf der AppAppliance werden AppExpert-Anwendungsvorlagen immer im AppExpert-Anwendungsvorlagen-Verzeichnis gespeichert, dh `/nsconfig/nstemplates/applications/`.

So laden Sie eine AppExpert Anwendungsvorlage von Ihrem lokalen Computer auf die Citrix ADC Appliance hoch:

1. Navigieren Sie zu **AppExpert > Anwendungen**.
2. Klicken Sie im Detailbereich auf **Vorlagen verwalten**.
3. Klicken Sie im Dialogfeld Anwendungsvorlagen auf **Hochladen**.
4. Navigieren Sie zu dem Verzeichnis, in dem die Vorlagendatei gespeichert ist, klicken Sie auf die Vorlagendatei und dann auf **Auswählen**.

   Die Vorlagendatei wird in das Anwendungsvorlagenverzeichnis AppExpert auf der Appliance hochgeladen.

So laden Sie eine AppExpert Anwendungsvorlage von der Citrix ADC Appliance auf Ihren lokalen Computer herunter:

1. Navigieren Sie zu **AppExpert > Anwendungen**.
2. Klicken Sie im Detailbereich auf **Vorlagen verwalten**.
3. Klicken Sie im Dialogfeld Anwendungsvorlagen auf die AppExpert-Anwendungsvorlage, die Sie herunterladen möchten, und klicken Sie auf **Herunterladen**.
4. Navigieren Sie zu dem Verzeichnis, in dem Sie die Datei speichern möchten, und klicken Sie dann auf **Speichern**.

Grundlegendes zu Citrix ADC Anwendungsvorlagen und Bereitstellungsdateien

October 5, 2021

Wenn Sie eine Citrix ADC Anwendung exportieren, werden die folgenden beiden Dateien automatisch erstellt:

- **Citrix ADC Anwendungsvorlagendatei**. Enthält Informationen zur Anwendungskonfiguration wie Anwendungseinheiten, Regeln und konfigurierte Richtlinien.
- **Bereitstellungsdatei**. Enthält bereitstellungsspezifische Informationen wie öffentliche Endpunkte, Dienste, zugeordnete IP-Adressen und konfigurierte Variablen.

In einer Vorlagendatei oder Bereitstellungsdatei ist jede Einheit der Anwendungskonfigurationsinformationen in einem bestimmten XML-Element gekapselt, das für diesen Einheitentyp bestimmt ist. Beispielsweise werden jeder öffentliche Endpunkt und die zugehörigen Endpunktdetails in den Tags <appendpoint> und </appendpoint> gekapselt, und alle Endpunktelemente sind in den Tags <appendpoint_list> und </appendpoint_list> eingekapselt.

Hinweis: Nachdem Sie eine Citrix ADC Anwendung exportiert haben, können Sie Elemente hinzufügen, Elemente entfernen und vorhandene Elemente ändern, bevor Sie die Anwendung in eine Citrix ADC-Appliance importieren.

Beispiel für eine Citrix ADC Anwendungsvorlage

Es folgt ein Beispiel für eine Vorlagendatei, die aus einer Citrix ADC Anwendung namens **SharePoint_Team_Site**erstellt wurde:

```
<?xml version="1.0" encoding="UTF-8" ?>
<template>
<template_info>
   <application_name>SharePoint_Team_Site</application_name>
```



```
    <templateversion_major>1</templateversion_major>
    <templateversion_minor>1</templateversion_minor>
    <author>Ed</author>
    <introduction>An application for managing a SharePoint team site
       with images, reports, and, XML content.</introduction>
    <summary>This template includes variables</summary>
    <version_major>9</version_major>
    <version_minor>3</version_minor>
    <build_number>38</build_number>
</template_info>
<apptemplate>
   <rewrite>
      <rewriteaction_list>
         <rewriteaction>
            <name>Rw_name</name>
            <type>replace</type>
            <target>HTTP.REQ.BODY(10000).AFTER_REGEX(re/number/).
               BEFORE_REGEX(re/address/)</target>
            <stringbuilderexpr>”NA”</stringbuilderexpr>
            <allow_unsafe_pi1>NO</allow_unsafe_pi1>
         </rewriteaction>
         <rewriteaction>
            .
            .
            .
         </rewriteaction>
         .
         .
         .
      </rewriteaction_list>
      <rewritepolicy_list>
         <rewritepolicy>
            <name>Rw_number_NA</name>
            <rule>HTTP.REQ.BODY(100000).CONTAINS(”admin”)</rule>
            <action>Rw_name</action>
         </rewritepolicy>
         <rewritepolicy>
            .
            .
            .
         </rewritepolicy>
         .
         .
         .
      </rewritepolicy_list>
```



```
    </rewrite>
    <appunit_list>
       <appunit>
          <name>SharePoint_Team_Sitedefault</name>
          <rule />
          <expressiontype>PE</expressiontype>
          <servicetype>HTTP</servicetype>
          <ipv46>0.0.0.0</ipv46>
          <ipmask>*</ipmask>
          <port>0</port>
          <range>1</range>
          <persistencetype>NONE</persistencetype>
          <timeout>2</timeout>
          <persistencebackup>NONE</persistencebackup>
          <backuppersistencetimeout>2</backuppersistencetimeout>
          <lbmethod>LEASTCONNECTION</lbmethod>
          <persistmask>255.255.255.255</persistmask>
          <v6persistmasklen>128</v6persistmasklen>
          <pq>OFF</pq>
          <sc>OFF</sc>
          <m>IP</m>
          <datalength>0</datalength>
          <dataoffset>0</dataoffset>
          <sessionless>DISABLED</sessionless>
          <state>ENABLED</state>
          <connfailover>DISABLED</connfailover>
          <clttimeout>180</clttimeout>
          <somethod>NONE</somethod>
          <sopersistence>DISABLED</sopersistence>
          <redirectportrewrite>DISABLED</redirectportrewrite>
          <downstateflush>DISABLED</downstateflush>
          <gt2gb>DISABLED</gt2gb>
          <ipmapping>0.0.0.0</ipmapping>
          <disableprimaryondown>DISABLED</disableprimaryondown>
          <insertvserveripport>OFF</insertvserveripport>
          <authentication>OFF</authentication>
          <authn401>OFF</authn401>
          <push>DISABLED</push>
          <pushlabel>none</pushlabel>
          <l2conn>OFF</l2conn>
       </appunit>
       <appunit>
          .
          .
          .
```



```
        </appunit>
        .
        .
        .
    </appunit_list>
    </apptemplate>
    <parameters>
       <property_list>
          <property>
             <variable_definition_list>
                <variable_definition>
                   <name>body_size</name>
                   <defaultvalue>10000</defaultvalue>
                   <description>Evaluation Scope</description>
                   <startindex>14</startindex>
                   <length>5</length>
                </variable_definition>
                .
                .
                .
             </variable_definition_list>
             <object_type>rewriteaction</object_type>
             <object_name>Rw_name</object_name>
             <name>target</name>
          </property>
          .
          .
          .
       </property_list>
    </parameters>
</template>
<!--NeedCopy-->
```

Beispiel einer Bereitstellungsdatei

Im Folgenden finden Sie die Bereitstellungsdatei, die mit der Anwendung **SharePoint_Team_site** im vorherigen Beispiel verknüpft ist:

```
<?xml version="1.0" encoding="UTF8" ?>
<template_deployment>
   <template_info>
      <application_name>SharePoint_Team_Site</application_name>
```



```
        <templateversion_major>1</templateversion_major>
        <templateversion_minor>1</templateversion_minor>
        <author>Ed</author>
        <introduction>An application for managing a SharePoint team site
            with images, reports, and, XML content.</introduction>
        <summary>This template includes variables</summary>
        <version_major>9</version_major>
        <version_minor>3</version_minor>
        <build_number>38</build_number>
    </template_info>
    <appendpoint_list>
        <appendpoint>
            <ipv46>10.111.111.1</ipv46>
            <port>80</port>
            <servicetype>HTTP</servicetype>
        </appendpoint>
    </appendpoint_list>
    <service_list>
        <service>
            <ip>10.102.29.5</ip>
            <port>80</port>
            <servicetype>HTTP</servicetype>
        </service>
        <service>
            .
            .
            .
        </service>
        .
        .
        .
    </service_list>
    <variable_list>
        <variable>
            <name>body_size</name>
            <description>Evaluation Scope</description>
            <value>10000</value>
        </variable>
        <variable>
            .
            .
            .
        </variable>
        .
        .
```



```
49         .
50       </variable_list>
51   </template_deployment>
52   <!--NeedCopy-->
```

Löschen einer Vorlagendatei

October 5, 2021

Wenn Sie eine Anwendungsvorlage und deren Konfiguration nicht mehr benötigen, können Sie sie löschen. Wenn Sie eine Vorlage löschen, wird die im Anwendungsvorlagenverzeichnis gespeicherte XML-Datei gelöscht. Wenn Sie eine Vorlagendatei löschen, werden Sie aufgefordert, den Löschvorgang zu bestätigen. Klicken Sie auf **Ja**, um die ausgewählte Datei aus dem Verzeichnis zu bestätigen und zu löschen.

So löschen Sie eine Vorlagendatei mit der GUI aus dem Anwendungsvorlagenverzeichnis:

1. Navigieren Sie zu **AppExpert > Anwendungen**, und klicken Sie dann auf **Vorlage verwalten** . Wählen Sie eine Datei auf der Registerkarte **Vorlagendateien** oder auf der Registerkarte **Bereitstellungsdateien** aus, und klicken Sie auf **Löschen** .

Citrix Gateway-Anwendungen

October 5, 2021

Wenn Sie eine AppExpert Anwendung für die Verwaltung einer Webanwendung über die Citrix® Citrix ADC®-Appliance konfigurieren, erstellen Sie außerdem eine Reihe von Anwendungseinheiten und konfigurieren für jede Einheit eine Reihe von Verkehrsoptimierungs- und Sicherheitsrichtlinien. Die Richtlinien, die Sie für jede Anwendungseinheit konfigurieren (Richtlinien für Features wie Komprimierung, Caching und Rewrite), bewerten den Datenverkehr, der nur für diese Einheit bestimmt ist. Zusätzlich zu diesen Richtlinien können Sie Access Gateway-Richtlinien für die gesamte Anwendung konfigurieren, um den Anwendungsdatenverkehr zu optimieren, wenn über Access Gateway zugegriffen wird. Mit der Funktion Access Gateway-Anwendungen können Sie Access Gateway-Richtlinien (Autorisierung, Datenverkehr, Clientloser Zugriff und TCP-Komprimierung) für eine AppExpert t-Anwendung konfigurieren. Nachdem Sie Citrix Gateway Richtlinien für AppExpert Anwendungen konfiguriert haben, können Sie die Richtlinienkonfiguration in die von Ihnen erstellten AppExpert-Anwendungsvorlagen aufnehmen.

Sie können Citrix Gateway Richtlinien auch für Intranetsubnetze, Dateifreigaben und andere Netzwerkressourcen konfigurieren. Schließlich können Sie Lesezeichen für AppExpert Anwendungen und

bestimmte Ressourcen erstellen, wenn Benutzer über die Citrix Gateway Homepage darauf zugreifen können.

Sie können die Entitäten in der Citrix Gateway Anwendung nur mit der GUI konfigurieren.

Funktionsweise einer Citrix Gateway Anwendung

Wenn Sie eine AppExpert Anwendung im Knoten Anwendungen in der GUI erstellen, wird automatisch eine entsprechende Access Gateway-Anwendung im Knoten Access Gateway Applications erstellt. Darüber hinaus wird automatisch eine Regel, die den konfigurierten öffentlichen Endpunkt der AppExpert t-Anwendung verwendet, für den Access Gateway-Anwendungseintrag erstellt. Wenn mehrere Endpunkte für die AppExpert Anwendung konfiguriert sind, enthält die Regel alle konfigurierten öffentlichen Endpunkte. Die Citrix ADC Appliance verwendet diese Regel, um konfigurierte Access Gateway-Richtlinien auf den Datenverkehr anzuwenden, der am öffentlichen Endpunkt der AppExpert t-Anwendung empfangen wird. Der am öffentlichen Endpunkt der AppExpert t-Anwendung empfangene Datenverkehr wird zunächst anhand der Citrix Gateway Richtlinien ausgewertet und anschließend anhand der Richtlinien ausgewertet, die für die Anwendungseinheiten der AppExpert Anwendung konfiguriert sind.

Die Regel, die für die Clientless-Access-Richtlinien für eine Access Gateway-Anwendung erstellt wird, ist ein erweiterter Ausdruck, der auch den öffentlichen Endpunkt verwendet, der für die AppExpert t-Anwendung konfiguriert ist. Bevor Sie Citrix Gateway Richtlinien für eine AppExpert Anwendung konfigurieren, müssen Sie daher öffentliche Endpunkte für die AppExpert-Anwendung konfigurieren.

Wenn Sie die Citrix Gateway Konfiguration in eine Anwendungsvorlage aufnehmen, werden bereitstellungsspezifische Informationen wie IP-Adresse und Portinformationen sowie die aus diesen Informationen erstellte Regel nicht in der Vorlage enthalten.

Funktionsweise einer Citrix ADC Konfiguration für eine Dateifreigabe

Auf der Citrix ADC Appliance können Sie Autorisierungsrichtlinien für eine Dateifreigabe konfigurieren, die im Netzwerk Ihrer Organisation gehostet wird.

Wenn Sie eine Dateifreigabe erstellen, geben Sie einen Namen für die Dateifreigabe und den Netzwerkpfad zur Dateifreigabe an. Im Netzwerkpfad können Sie entweder den Namen des Servers oder die Server-IP-Adresse angeben. Eine Regel, die die Komponenten des Dateifreigabepfads verwendet, wird automatisch für die Dateifreigabe erstellt. Diese Regel ermöglicht es der Appliance, Anforderungen für Dateien zu identifizieren, die auf dem Dateifreigabe-Server gehostet werden. Alle Autorisierungsrichtlinien, die für die Dateifreigabe konfiguriert sind, werden auf eingehende Anforderungen angewendet.

Die Citrix ADC Konfiguration für eine Dateifreigabe kann nicht in AppExpert Anwendungsvorlagen gespeichert werden.

Funktionsweise einer Citrix ADC Konfiguration für ein Intranet-Subnetz

Für die Intranetsubnetze, die Teil des Netzwerks sind, können Sie Richtlinien für Autorisierung, Verkehr und TCP-Komprimierung auf der Citrix ADC Appliance konfigurieren. Beim Hinzufügen eines Intranetsubnetzes geben Sie die IP-Adresse und die Netzmaske des Intranetsubnetzes an. Eine Regel, die diese beiden Parameter verwendet, wird automatisch für das Intranetsubnetz erstellt. Die Appliance wendet die konfigurierten Richtlinien auf jede Anforderung an, für die eine Ziel-IP-Adresse und Netzmaske auf die IP-Adresse des Subnetzes bzw. die Netzmaske festgelegt sind.

Die Citrix ADC Konfiguration für ein Intranetsubnetz kann nicht in AppExpert Anwendungsvorlagen gespeichert werden.

Funktionsweise der Kategorie Andere Ressourcen

In der Kategorie Andere Ressourcen können Sie Access Gateway-Richtlinien für jede Netzwerkressource mithilfe einer Regel Ihrer Wahl konfigurieren. Wenn Sie die Citrix ADC Appliance für die Verarbeitung von Anforderungen für die Netzwerkressource konfigurieren, konfigurieren Sie einen klassischen Ausdruck, um die Anforderungen zu identifizieren, die der Netzwerkressource zugeordnet sind. Sie können Autorisierungs-, Datenverkehrs-, Clientless- und TCP-Komprimierungsrichtlinien für eine Netzwerkressource in Weitere Ressourcen konfigurieren. Die Citrix ADC Appliance wendet die konfigurierten Citrix Gateway Richtlinien auf alle Anforderungen an, die der konfigurierten Regel entsprechen.

Die Citrix ADC Konfiguration für eine Netzwerkressource unter Andere Ressourcen kann nicht in AppExpert Anwendungsvorlagen gespeichert werden.

Benennungskonventionen für Entitäten

Das Feature Citrix Gateway Anwendungen erzwingt eine Namenskonvention für einige der Entitäten, die Sie in diesem Feature erstellen. Beispielsweise beginnen die Namen der Profile, die Sie für Verkehrsrichtlinien für ein Intranetsubnetz erstellen, immer mit einer Zeichenfolge, die aus dem Namen des Intranetsubnetzes gefolgt von einem Unterstrich (_) besteht. Der Name, den Sie für die Entität angeben, wird an diese Zeichenfolge angehängt. Wenn der Name eines Subnetzes subnet1 ist, beginnt der Name des Profils mit subnet1_. Wenn eine solche Namenskonvention erforderlich ist (z. B. in das Textfeld, in das Sie den Namen einer Entität eingeben), fügt die Benutzeroberfläche automatisch die Zeichenfolge ein, mit der der Name der Entität beginnen muss, und Sie können sie nicht ändern.

Hinzufügen von Intranet-Subnetzen

October 5, 2021

Sie können Autorisierungs- und Verkehrsrichtlinien für den Datenverkehr angeben, der für die im Netzwerk konfigurierten Intranet-Subnetze gebunden ist. Die Regeln für diese Richtlinien werden automatisch mit der Parameter erstellt, die Sie für das Subnetz angeben.

So konfigurieren Sie ein Intranet-Subnetz mit der GUI:

1. Erweitern Sie im Navigationsbereich der GUI **AppExpert**, und klicken Sie dann auf Access Gateway Applications.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um ein Intranetsubnetz hinzuzufügen, klicken Sie auf **Intranetsubnetze**, und klicken Sie dann auf **Hinzufügen**.
   - Um ein Intranetsubnetz zu ändern, klicken Sie auf ein Intranetsubnetz, und klicken Sie dann auf **Öffnen**.
3. Gehen **Sie im Dialogfeld Intranet-Subnetz erstellen** oder **Intranet-Subnetz konfigurieren** folgendermaßen vor:
   a) Geben Sie im Feld Name einen Namen für das Intranetsubnetz ein, das Sie hinzufügen. Dieser Parameter kann für ein vorhandenes Intranetsubnetz nicht geändert werden.
   b) Geben Sie im Feld IP-Adresse die IP-Adresse des Intranetsubnetzes ein.
   c) Geben Sie im Feld Netzmaske die Netzmaske ein, die für das Intranetsubnetz verwendet wird.
   d) Klicken Sie auf **Erstellen** oder **OK**und dann auf **Schließen**.

Hinzufügen anderer Ressourcen

October 5, 2021

Für eine Netzwerkressource, die Sie zu Weitere Ressourcen hinzufügen, müssen Sie einen klassischen Ausdruck konfigurieren, der die Teilmenge des Datenverkehrs identifiziert, der der Ressource zugeordnet ist. Weitere Informationen zum Konfigurieren eines klassischen Ausdrucks finden Sie unter.

So konfigurieren Sie eine Ressource in anderen Ressourcen mit der GUI:

1. Erweitern Sie im Navigationsbereich der Benutzeroberfläche AppExpert, und klicken Sie dann auf **Access Gateway Applications**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine Ressource hinzuzufügen, klicken Sie auf **Weitere Ressourcen**, und klicken Sie dann auf **Hinzufügen**.

- Um eine Ressource zu ändern, klicken Sie auf eine Ressource, und klicken Sie dann auf **Öffnen**.

3. Gehen **Sie im Dialogfeld Ressource erstellen** oder **Ressource konfigurieren** folgendermaßen vor:
   a) Geben Sie im Feld Name einen Namen für die Ressource ein, die Sie hinzufügen möchten. Dieser Parameter kann für eine vorhandene Ressource nicht geändert werden.
   b) Geben Sie im Feld Regel die Regel ein, die die Teilmenge des Datenverkehrs identifiziert, die der hinzuzufügenden Ressource zugeordnet ist.
   Klicken Sie alternativ auf **Konfigurieren**, und erstellen Sie dann die Regel im Dialogfeld **Ausdruck erstellen**.
   c) Klicken Sie auf **Erstellen** oder **OK**und dann auf **Schließen**.

Konfigurieren von Autorisierungsrichtlinien

October 5, 2021

Sie können Citrix Gateway Autorisierungsrichtlinien für AAA-Benutzer und -Gruppen für den Zugriff auf eine Ressource konfigurieren.

So konfigurieren Sie Berechtigungen für einen AAA-Benutzer oder -Gruppe für den Zugriff auf eine Ressource mit der GUI:

1. Erweitern Sie im Navigationsbereich der Benutzeroberfläche AppExpert, und klicken Sie dann auf **Access Gateway Applications**.
2. Klicken Sie im Detailbereich in der Spalte Autorisierung auf das Symbol für die Anwendung, die Dateifreigabe, das Intranetsubnetz oder die Ressource, für die Sie Autorisierungsrichtlinien für AAA-Benutzer und -Gruppen konfigurieren möchten.
3. Führen Sie einen der folgenden Schritte aus:
   - Wenn sich der AAA-Benutzer oder die Gruppe, für die Sie Berechtigungen konfigurieren möchten, bereits in der Gruppe Gruppen/Benutzer befindet, ziehen Sie den Benutzer oder die Gruppe aus der Struktur Gruppen/Benutzer auf den Knoten Benutzer oder Gruppen in der <application name>-Struktur. Klicken Sie dann mit der rechten Maustaste auf den Benutzer oder die Gruppe, und klicken Sie auf **Allow**.
   - Wenn der AAA-Benutzer oder die Gruppe, für die Sie Berechtigungen konfigurieren möchten, auf der Appliance nicht konfiguriert ist, klicken Sie in der <application name >-Struktur mit der rechten Maustaste auf Benutzer oder Gruppen, und klicken Sie dann auf **Hinzufügen** . Geben Sie im Dialogfeld **AAA-Gruppe erstellen** oder **AAA-Benutzer erstellen** die Werte ein, klicken Sie auf **Erstellen**, und klicken Sie dann auf **Schließen**.
   Der Benutzer oder die Gruppe wird mit dem Berechtigungssatz “Zulassen” erstellt. Um die Berechtigungseinstellung zu ändern, klicken Sie mit der rechten Maustaste auf die Gruppe

oder den Benutzer, und klicken Sie dann auf die Berechtigungseinstellung.

4. Klicken Sie auf **Schließen**.

Konfigurieren von Verkehrsrichtlinien

December 7, 2021

Die Datenverkehrsrichtlinien, die Sie für die Ressourcen im Knoten Citrix Gateway Anwendungen konfigurieren, steuern Clientverbindungen zur Anwendung. Sie müssen keine Regel für die Ressource konfigurieren. Die Regel, die beim Erstellen der Ressource automatisch erstellt wurde. Sie müssen nur ein Anforderungsprofil mit der Verkehrsrichtlinie verknüpfen. Im Verkehrsprofil geben Sie Parameter wie Protokoll, Anwendungszeitüberschreitung und Dateitypzuordnung an.

So konfigurieren Sie Verkehrsrichtlinien für eine Ressource

1. Erweitern Sie im Navigationsbereich der Benutzeroberfläche AppExpert, und klicken Sie dann auf Access Gateway Applications.
2. Klicken Sie im Detailbereich in der Spalte Verkehr auf das Symbol für die Anwendung, die Dateifreigabe, das Intranetsubnetz oder die Ressource, für die Sie Verkehrsrichtlinien konfigurieren möchten.
3. **Gehen Sie im Dialogfeld Verkehrsrichtlinien konfigurieren** folgendermaßen vor:
   - Um eine vorhandene Verkehrsrichtlinie anzugeben, klicken Sie auf **Richtlinie einfügen**, und klicken Sie dann in der Spalte Richtlinienname auf den Namen der Richtlinie.
   - Klicken Sie zum Konfigurieren einer neuen Richtlinie auf Richtlinie einfügen, und klicken Sie dann in der Spalte Richtlinienname auf Neue Richtlinie. Geben Sie im Dialogfeld Verkehrsrichtlinie erstellen im Feld Name nach dem Unterstrich (_) einen Namen für die Richtlinie ein. Wählen Sie dann unter Anforderungsprofil entweder ein vorhandenes Anforderungsprofil aus, oder klicken Sie auf Neu, um ein neues Anforderungsprofil zu konfigurieren. Sie können auch ein vorhandenes Profil auswählen und dann auf Ändern klicken, um das Profil zu ändern.
     Weitere Informationen zum Konfigurieren einer Verkehrsrichtlinie oder eines Profils finden Sie unter Citrix Gateway.
   - Um eine eingefügte Richtlinie zu ändern, klicken Sie in der Spalte Richtlinienname auf den Richtliniennamen, und klicken Sie dann auf Richtlinie ändern. Um nur das zugeordnete Profil zu ändern, klicken Sie in der Spalte Profil auf den Namen des Profils und dann auf **Profil ändern**.
   - Um die Prioritäten neu zu generieren, die den Richtlinien zugewiesen sind, klicken Sie auf **Prioritäten neu generieren** .
   - Um einen neuen Prioritätswert für eine Richtlinie anzugeben, doppelklicken Sie in der Spalte Priorität auf die zugewiesene Priorität, und geben Sie dann den gewünschten Wert

ein.

- Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf die Richtlinie, und klicken Sie dann auf **Richtlinie aufheben**.

4. Klicken Sie auf **Änderungen übernehmen**und dann auf **Schließen**.

Konfigurieren von Richtlinien für den Clientlosen Zugriff

October 5, 2021

Der clientlose Zugriff ermöglicht Endbenutzern den Zugriff auf die Ressource, wenn er für eine Ressource auf der Citrix ADC Appliance konfiguriert ist, ohne die Citrix Gateway Clientsoftware zu verwenden. Benutzer können Webbrowser verwenden, um auf Ressourcen wie Outlook Web Access zuzugreifen. Sie konfigurieren den clientlosen Zugriff für eine Ressource, indem Sie eine clientlose Zugriffsrichtlinie konfigurieren, die einem clientlosen Zugriffsprofil zugeordnet ist.

So konfigurieren Sie eine clientlose Zugriffsrichtlinie für eine Ressource im Knoten Citrix Gateway Applications:

1. Erweitern Sie im Navigationsbereich der GUI **AppExpert**, und klicken Sie dann auf **Access Gateway Applications**.
2. Klicken Sie im Detailbereich in der Spalte **Clientloser Zugriff** auf das Symbol für die Anwendung, die Dateifreigabe, das Intranetsubnetz oder die Ressource, für die Sie eine clientlose Zugriffsrichtlinie konfigurieren möchten.
3. **Führen Sie im Dialogfeld Clientlose Zugriffsrichtlinien konfigurieren** die folgenden Schritte aus:
   - Um eine vorhandene Richtlinie ohne Clientzugriff anzugeben, klicken Sie auf **Richtlinie einfügen**, und klicken Sie dann in der Spalte **Richtliniennameauf** den Namen der Richtlinie.
   - Um eine neue Richtlinie ohne Clientzugriff zu konfigurieren, klicken Sie auf **Richtlinie einfügen**, und klicken Sie dann in der Spalte **Richtliniennameauf** **Neue Richtlinie**. Geben **Sie im Dialogfeld Clientlose Zugriffsrichtlinie erstellen** im Feld Name nach dem Unterstrich (_) einen Namen für die Richtlinie ein. Wählen Sie dann unter Profil entweder ein vorhandenes Profil aus, oder klicken Sie auf Neu, um ein neues Profil zu konfigurieren. Sie können auch ein vorhandenes Profil auswählen und dann auf **Ändern** klicken, um das Profil zu ändern.
     Weitere Informationen zum Konfigurieren einer Richtlinie oder eines Profils für clientlosen Zugriff finden Sie unter Citrix Gateway.
   - Um eine eingefügte Richtlinie zu ändern, klicken Sie in der Spalte Richtlinienname auf den Richtliniennamen, und klicken Sie dann auf **Richtlinie ändern**. Um nur das zugeordnete Profil zu ändern, klicken Sie in der Spalte Profil auf den Namen des Profils und dann auf

Profil ändern.

- Um einen neuen Prioritätswert für eine Richtlinie anzugeben, doppelklicken Sie in der Spalte Priorität auf die zugewiesene Priorität, und geben Sie dann den gewünschten Wert ein.
- Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf die Richtlinie, und klicken Sie dann auf **Richtlinie aufheben**.

4. Klicken Sie auf **Änderungen übernehmen**und dann auf **Schließen**.

Konfigurieren von TCP-Komprimierungsrichtlinien

December 7, 2021

Sie können TCP-Komprimierungsrichtlinien für eine Anwendung konfigurieren, um die Leistung der Anwendung zu erhöhen. Die TCP-Komprimierung reduziert die Netzwerklatenz, reduziert die Bandbreitenanforderungen und erhöht die Übertragungsgeschwindigkeit. Wenn Sie eine TCP-Komprimierungsrichtlinie konfigurieren, ordnen Sie der Richtlinie eine Komprimierungsaktion zu. Die Komprimierungsaktion gibt entweder Komprimieren, GZIP, Deflate oder NoCompress als Komprimierungstyp an. Weitere Informationen zu den Komprimierungsrichtlinien und Komprimierungsaktionen finden Sie unter Citrix Gateway.

So konfigurieren Sie eine TCP-Komprimierungsrichtlinie für eine Ressource im Knoten Citrix Gateway Applications

1. Erweitern Sie im Navigationsbereich der GUI **AppExpert**, und klicken Sie dann auf **Access Gateway Applications**.
2. Klicken Sie im Detailbereich in der Spalte TCP-Komprimierung auf das Symbol für die Anwendung, die Dateifreigabe, das Intranetsubnetz oder die Ressource, für die Sie eine TCP-Komprimierungsrichtlinie konfigurieren möchten.
3. **Gehen Sie im Dialogfeld TCP-Komprimierungsrichtlinien konfigurieren** folgendermaßen vor:
    - Um eine vorhandene TCP-Komprimierungsrichtlinie anzugeben, klicken Sie auf **Richtlinie einfügen**, und klicken Sie dann in der Spalte **Richtliniennameauf** den Namen der Richtlinie.
    - Um eine neue TCP-Komprimierungsrichtlinie zu erstellen, klicken Sie auf Richtlinie einfügen, und klicken Sie dann in der Spalte Richtliniennameauf Neue Richtlinie. Geben Sie im Dialogfeld TCP-Komprimierungsrichtlinie erstellen im Feld Richtliniennameauf nach dem Unterstrich (_) einen Namen für die Richtlinie ein. Wählen Sie dann in Aktion entweder eine vorhandene Aktion aus, oder klicken Sie auf Neu, und konfigurieren Sie eine neue Aktion. Sie können auch auf Ansicht klicken, um den konfigurierten Komprimierungstyp anzuzeigen.

Weitere Informationen zum Konfigurieren einer TCP-Komprimierungsrichtlinie oder -aktion finden Sie unter Citrix Gateway, Advanced Edition at Citrix Gateway.

- Um eine eingefügte Richtlinie zu ändern, klicken Sie in der Spalte Richtlinienname auf den Richtliniennamen, und klicken Sie dann auf **Richtlinie ändern**.
- Um die Prioritäten neu zu generieren, die den Richtlinien zugewiesen sind, klicken Sie auf **Prioritäten neu generieren** .
- Um einen neuen Prioritätswert für eine Richtlinie anzugeben, doppelklicken Sie in der Spalte Priorität auf die zugewiesene Priorität, und geben Sie dann den gewünschten Wert ein.
- Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf die Richtlinie, und klicken Sie dann auf **Richtlinie aufheben**.

4. Klicken Sie auf **Änderungen anwenden** und dann auf **Schließen**.

Konfigurieren von Lesezeichen

January 25, 2022

Sie können Lesezeichen für interne Anwendungen oder Ressourcen konfigurieren, die für einen berechtigten Benutzer verfügbar sind. Sie können das Lesezeichen dann global an einen Benutzer, eine Benutzergruppe oder einen virtuellen Server binden und für den Benutzer im Access Interface aktivieren. Die von Ihnen erstellten Lesezeichenverknüpfungen werden in den Website-Bereichen unter Unternehmenswebsites angezeigt.

Weitere Informationen finden Sie unter Erstellen und Anwenden von Weblinks .

AppQoE

October 5, 2021

AppQoE (Quality of Experience) auf Anwendungsebene integriert mehrere vorhandene richtlinienbasierte Sicherheitsfunktionen der Citrix ADC Appliance in eine einzige integrierte Funktion, die die Vorteile eines neuen Warteschlangenmechanismus, Fair Queuing, nutzt. Fair Queuing verwaltet Anfragen an Webserver und Anwendungen mit Lastausgleich auf virtueller Serverebene statt auf Service-Ebene, sodass es vor dem Lastenausgleich die Warteschlange aller Anfragen an eine Website oder Anwendung als eine Gruppe vor dem Lastenausgleich bearbeiten kann, anstatt als separate Streams nach dem Lastausgleich.

Die Funktionen, die in AppQoe integriert sind, sind HTTP Denial-of-Service Protection (HDOSP) und Priority Queuing (PQ). Gemeinsam bieten diese Dienste Schutz vor verschiedenen Problemen:

- **Einfache Überlastung.** Jeder Server, egal wie robust, kann nur eine begrenzte Anzahl von Verbindungen gleichzeitig akzeptieren. Wenn eine geschützte Website oder Anwendung zu viele Anfragen gleichzeitig erhält, erkennt die Überspannungsschutzfunktion die Überlastung und stellt die überschüssigen Verbindungen in die Warteschlange, bis der Server sie akzeptieren kann. Die Funktion Prioritätswarteschlange stellt sicher, dass jedem, der Zugriff auf eine Ressource am meisten benötigt, Zugriff gewährt wird, ohne auf andere Anforderungen mit niedrigerer Priorität warten zu müssen. Die AppQoe-Funktion zeigt eine alternative Webseite an, die Benutzer darüber informiert, dass die von ihnen angeforderte Ressource nicht verfügbar ist.
- **Denial-of-Service-Angriffe (DOS).** Jede öffentlich zugängliche Ressource ist anfällig für Angriffe, deren Zweck es ist, diesen Dienst zu senken und legitimen Benutzern den Zugriff darauf zu verweigern. Die Funktionen Überspannungsschutz und Priority Queuing helfen bei der Verwaltung von DOS-Angriffen zusätzlich zu anderen Arten von hoher Belastung. Darüber hinaus zielt die Funktion "HTTP Denial-of-Service Protection" auf DOS-Angriffe auf Ihre Websites ab, sendet Herausforderungen an mutmaßliche Angreifer und löscht Verbindungen, wenn die Clients keine entsprechende Antwort senden.

Bis zur aktuellen Version des Citrix ADC Betriebssystems wurden diese Features auf Service-Ebene implementiert, was bedeutet, dass jedem Dienst seine eigenen Warteschlangen zugewiesen wurden. Während Warteschlangen auf Service-Ebene funktionieren, haben sie auch einige Nachteile. Die meisten davon sind darauf zurückzuführen, dass die Citrix ADC Appliance Lastausgleich vor der Implementierung der Schutzfunktionen, die auf Warteschlangen basieren, Anforderungen ausgleichen muss. Die Implementierung von Schutzfunktionen vor der Warteschlange hat verschiedene Vorteile, von denen einige unten aufgeführt sind:

- Die absolute Priorität der Verbindungen, wie sie in der Prioritätswarteschlangenfunktion konfiguriert ist, kann beibehalten werden.
- Verbindungen werden nicht geleert, wenn ein Dienst den Status wechselt, wie sie sich in einer Warteschlange auf Dienstebene befinden.
- In Zeiten hoher Belastung, wie z. B. einem Denial-of-Service-Angriff, kommen HTTP-DoS vor dem Lastenausgleich ins Spiel, sodass diese Funktionen unerwünschten oder niedrigeren Datenverkehr vom Load Balancer erkennen und umleiten können, bevor der Load Balancer damit zurechtkommen muss.

Zusätzlich zur Implementierung von Fair Queuing integriert AppQoe eine Reihe von Funktionen, die jeweils einen anderen Satz von Tools bieten, um ein gemeinsames Ziel zu erreichen: Schutz Ihrer vernetzten Ressourcen vor übermäßiger oder unangemessener Nachfrage. Wenn Sie diese Funktionen in ein gemeinsames Framework integrieren, können Sie sie einfacher konfigurieren und implementieren.

Aktivieren von AppQoE

October 5, 2021

Um AppQoE zu konfigurieren, müssen Sie zuerst die Funktion aktivieren.

So aktivieren Sie AppQoE mit der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- enable ns feature appqoe
- show ns feature

Beispiel:

```
> enable ns feature appqoe
 Done
> show ns feature

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

So aktivieren Sie AppQoE mit der GUI

1. Navigieren Sie zu **System** > **Einstellungen**.
2. Klicken Sie im Detailbereich auf **Erweiterte Funktionen konfigurieren**.
3. Aktivieren Sie im Dialogfeld **Erweiterte Funktionen konfigurieren** das Kontrollkästchen **AppQoE**.
4. Klicken Sie auf **OK**.

AppQoE-Aktionen

October 5, 2021

Nachdem Sie die AppQoE-Funktion aktiviert haben, müssen Sie eine oder mehrere Aktionen für die Bearbeitung der Anforderung konfigurieren.

> **Wichtig:**
>
> Zum Erstellen einer Aktion sind keine spezifischen individuellen Parameter erforderlich, Sie müssen jedoch mindestens einen Parameter angeben, oder Sie können die Aktion nicht erstellen.

So konfigurieren Sie eine AppQoE-Aktion mit der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appqoe action <name> [-priority <priority>] [-respondWith (ACS|NS)[<customfile>] [-altContentSvcName <string>] [-altContentPath <string>] [-maxConn <positive_integer>] [-delay <usecs>] [-polqDepth <positive_integer>] [-priqDepth <positive_integer>] [-dosTrigExpression <expression>] [-dosAction (**SimpleResponse** | **HICResponse**)]`
- `show appqoe action`

Beispiel

So konfigurieren Sie Prioritätswarteschlangen mit Richtlinienwarteschlangentiefen von 10 bzw. 1000 für Warteschlangen mit mittlerer und niedrigster Priorität:

```
> add appqoe action appqoe-act-basic-prhigh -priority HIGH
 Done

> add appqoe action appqoe-act-basic-prmedium -priority MEDIUM -
    polqDepth 10
 Done

> add appqoe action appqoe-act-basic-prlow -priority LOW -polqDepth
    1000
 Done

> show appqoe action

1.       Name: appqoe-act-basic-prhigh
        ActionType: PRIORITY_QUEUING
        Priority: HIGH
        PolicyQdepth: 0
        Qdepth: 0

```



```
1.      Name: appqoe-act-basic-prmedium
        ActionType: PRIORITY_QUEUING
        Priority: MEDIUM
        PolicyQdepth: 10
        Qdepth: 0

1.      Name: appqoe-act-basic-prlow
        ActionType: PRIORITY_QUEUING
        Priority: LOW
        PolicyQdepth: 1000
        Qdepth: 0
Done
<!--NeedCopy-->
```

So ändern Sie eine vorhandene AppQoE-Aktion mit der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appqoe action <name> [-priority <priority>] [-altContentSvcName <string>] [-altContentPath <string>] [-polqDepth <positive_integer>] [-priqDepth <positive_integer>] [-maxConn <positive_integer>] [-delay <usecs>] [-dosTrigExpression <expression>] [-dosAction ( SimpleResponse | HICResponse )]`
- `show appqoe action`

So entfernen Sie eine AppQoE-Aktion mit der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `rm appqoe action <name>`
- `show appqoe action`

Parameter für die Konfiguration einer AppQoE-Aktion

- ein. Ein Name für die neue Aktion oder der Name der vorhandenen Aktion, die Sie ändern möchten. Der Name kann mit einem Buchstaben, einer Zahl oder einem Unterstrich beginnen und kann aus einem Buchstaben, Zahlen und dem Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), At-Zeichen (@), Gleich (=), Doppelpunkt (:) und Unterstrich (_) bestehen.
- priority. Die Prioritätswarteschlange, der die Anforderung zugewiesen ist. Wenn ein geschützter Webserver oder eine geschützte Anwendung stark geladen ist und keine zusätzlichen Anforderungen annehmen kann, gibt die Reihenfolge an, in der Wartungsanforderungen erfüllt werden sollen, wenn Ressourcen verfügbar sind. Folgende Möglichkeiten stehen zur Auswahl:

1. **HIGH.** Erfüllt die Anfrage, sobald Ressourcen verfügbar sind.
2. **MEDIUM.** Erfüllt die Anforderung, nachdem sie alle Anforderungen in der HIGH Prioritätswarteschlange erfüllt hat.
3. **LOW.** Erfüllt die Anforderung, nachdem sie alle Anforderungen in den Prioritätswarteschlangen HIGH und MEDIUM erfüllt hat.
4. **LOWEST.** Erfüllt die Anforderung erst, nachdem sie alle Anforderungen in Warteschlangen mit höherer Priorität erfüllt hat.

Wenn die Priorität nicht konfiguriert ist, weist die Citrix ADC Appliance die Anforderung standardmäßig der Warteschlange für die niedrigste Priorität zu.

- respondWith. Konfiguriert Citrix ADC so, dass die angegebene Responder-Aktion ausgeführt wird, wenn der angegebene Schwellenwert erreicht ist. Muss mit einer der folgenden Einstellungen verwendet werden:
  - **ACS:** Stellt Inhalte aus einem alternativen Content-Dienst bereit. Schwellenwert: maxConn (maximale Verbindungen) oder Verzögerung.
  - **NS:** Stellt eine integrierte Antwort vom Citrix ADC bereit. Schwellenwert: maxConn (maximale Verbindungen) oder Verzögerung.
  - **NO ACTION:** Kein alternativer Inhalt wird bereitgestellt. Weist Verbindungen der niedrigsten Prioritätswarteschlange zu, wenn der MaxConn (maximale Verbindungen) oder der Verzögerungsschwellenwert erreicht ist.
- altContentSvcName. Wenn -responseWith ACS angegeben ist, ist der Name des alternativen Content-Dienstes, normalerweise eine absolute URL zu dem Webserver, der den alternativen Inhalt hostet.
- altContentPath. Wenn -responseWith (ACS | NS) angegeben ist, ist der Pfad zum alternativen Inhalt.
- olqDepth. Schwellenwert für die Richtlinienwarteschlangentiefe für die Richtlinienwarteschlange, die dieser Aktion zugeordnet ist. Wenn die Anzahl der Verbindungen in der Richtlinienwarteschlange, die mit dieser Aktion verknüpft ist, auf die angegebene Anzahl erhöht, werden nachfolgende Anforderungen der LOWEST Richtlinienwarteschlange zugewiesen. Mindestwert: 1 Maximalwert: 4.294.967.294
- priqDepth. Schwellenwert für die Richtlinienwarteschlangentiefe für die angegebene Prioritätswarteschlange. Wenn die Anzahl der Anforderungen in der angegebenen Warteschlange auf dem virtuellen Server, an die die mit der aktuellen Aktion verknüpfte Richtlinie gebunden ist, auf die angegebene Anzahl erhöht, werden nachfolgende Anforderungen der Warteschlange mit der niedrigsten Priorität zugewiesen. Mindestwert: 1 Maximalwert: 4.294.967.294
- maxConn. Die maximale Anzahl von Verbindungen, die für Anforderungen geöffnet werden können, die der Richtlinienregel entsprechen. Mindestwert: 1 Maximalwert: 4.294.967.294

- delay. Der Verzögerungsschwellenwert in Mikrosekunden für Anforderungen, die der Richtlinienregel entsprechen. Wenn eine Übereinstimmungsanforderung länger als der Schwellenwert verzögert wurde, führt die
  Citrix ADC Appliance die angegebene Aktion aus. Wenn NO ACTION angegeben ist, weist die Appliance Anforderungen der Warteschlange für die niedrigste Priorität zu. Mindestwert: 1 Maximalwert: 599999,999
- dosTrigExpression. Fügt eine optionale Prüfung der zweiten Ebene hinzu, um DoS-Aktionen auszulösen.
- dosAction. Aktion, die ausgeführt wird, wenn die Appliance feststellt, dass sie oder ein geschützter Server unter DoS-Angriff ist. Mögliche Werte: SimpleResponse, HICResponse.

Diese Werte geben HTTP-Challenge-Response-Methoden an, um die Authentizität eingehender Anforderungen zu überprüfen, um einen HTTP-DDoS-Angriff zu mildern.

Im HTTP-Challenge-Response-Generierungs- und Validierungsprozess verwendet AppQoe Cookies, um die Antwort des Clients zu validieren und zu überprüfen, ob der Client echt zu sein scheint. Beim Senden einer Herausforderung generiert eine Citrix ADC Appliance zwei Cookies:

Header cookie (_DOSQ). Enthält clientspezifische Informationen, damit die Citrix ADC Appliance die Antwort überprüfen kann.

Body cookie (_DOSH). Informationen, die zur Validierung des Client-Computers verwendet werden. Der Browser des Clients (oder der Benutzer, im Fall von HIC) berechnet einen Wert für dieses Cookie. Die Citrix ADC Appliance vergleicht diesen Wert mit dem erwarteten Wert, um den Client zu überprüfen.

Die Informationen, die die Appliance zum Berechnen des _DOSH-Werts an den Client sendet, basieren auf der DoS-Aktionskonfiguration.

1. SimpleReponse: In diesem Fall teilt eine Citrix ADC Appliance den Wert auf und generiert einen JavaScript-Code, um den endgültigen Wert zu kombinieren. Ein Clientcomputer, der den ursprünglichen Wert berechnen kann, gilt als echt.
2. HiCResponse: In diesem Fall generiert eine Citrix ADC Appliance zwei einstellige Zahlen und generiert Bilder für diese Nummern. Anschließend fügt die Appliance mithilfe eines Backpatch-Frameworks diese Bilder als Base64-Zeichenfolgen ein.

Einschränkungen

1. Dies ist keine triviale CAPTCHA-Implementierung, weshalb dieser Begriff nicht verwendet wird.
2. Die Validierungsnummer basiert auf einer von Citrix ADC generierten Nummer, die sich für 120s nicht ändert. Diese Zahl sollte dynamisch oder kundenspezifisch sein.

So konfigurieren Sie eine AppQoE-Aktion mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **App-Expert** > **AppQoe** > **Aktionen** .
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine neue Aktion zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Aktion zu ändern, wählen Sie die Aktion aus, und klicken Sie dann auf **Bearbeiten**.
3. Geben **Sie im Bildschirm AppQoE-Aktion erstellen** oder im Fenster **AppQoE-Aktion konfigurieren** Werte für die Parameter ein oder wählen Sie sie aus. Der Inhalt des Dialogfensters entspricht den unter Parameter für die Konfiguration der AppQoE-Aktion beschriebenen Parametern wie folgt (Sternchen gibt einen erforderlichen Parameter an):
   - Name — Name
   - Aktionstyp: RespondWith
   - Priorität — Priorität
   - Richtlinienwarteschlangentiefe — polqDepth
   - Warteschlangentiefe — priqDepth
   - DOS-Aktion — dosAction
4. Klicken Sie auf **Erstellen** oder **OK**.

AppQoE-Parameter

October 5, 2021

In den AppQoE-Parametern konfigurieren Sie die Sitzungsdauer einer AppQoE-Sitzung, den Dateinamen der Datei, die die angepasste Antwort enthält, und die Anzahl der Clientverbindungen, die in einer Warteschlange platziert werden können.

So konfigurieren Sie die AppQoE-Parametereinstellungen mit der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appqoe parameter [-sessionLife <secs>] [-avgwaitingclient <positive_integer>] [-MaxAltRespBandWidth <positive_integer>] [-dosAttackThresh <positive_integer>]`
- `show appqoe parameter`

Parameter für die Konfiguration der AppQoE-Parameter

- sessionLife

Anzahl der Sekunden, die nach der Anzeige alternativer Inhalte gewartet werden müssen, bevor die Appliance denselben Inhalt erneut anzeigt. Standardwert: 300 Maximum Minimalwert: 1 Maximaler Wert: 4.294.967.294

- avgwaitingclient

  Die durchschnittliche Anzahl von Clientanforderungen, die sich in der Warteschlange des Dienstes befinden können. Standardwert: 1000000 Maximalwert: 4.294.967.294

- MaxAltRespBandWidth

  Die maximale Bandbreite, die beim Senden alternativer Antworten benötigt wird. Wenn das Maximum erreicht ist, beendet die Appliance das Senden des alternativen Inhalts, bis der Bandbreitenverbrauch sinkt. Standardwert: 100 Mindestwert: 1 Maximaler Wert: 4.294.967.294

- dosAtckThrsh

  Der Denial-of-Service-Angriffsschwellenwert. Die Anzahl der Verbindungen, die in Warteschlangen warten müssen, bevor die Appliance mit DoS-Schutzmaßnahmen reagiert. Standardwert: 2000 Mindestwert: 0 Maximaler Wert: 4.294.967.294

So konfigurieren Sie die AppQoE-Parametereinstellungen mit der GUI

1. Navigieren Sie zu **AppExpert** > **AppQoe**.
2. Klicken Sie im Detailbereich auf **AppQoE -Parameter konfigurieren**.
3. Geben Sie im Bildschirm **AppQoE-Parameter konfigurieren** Werte für die Parameter ein oder wählen Sie sie aus. Der Inhalt des Dialogfensters entspricht den unter Parameter zur Konfiguration der AppQoE-Parameter beschriebenen Parametern wie folgt (Sternchen gibt einen erforderlichen Parameter an):
   - Sitzungsdauer (Sekunden)
   - sessionLife
   - Durchschnitt Clientwarten — avgwaitingclient
   - Begrenzung der alternativen Antwortbandbreite (Mbit/s) — MaxAltRespBandWidth
   - DOS-Angriffsschwelle —dosAttackThresh
4. Klicken Sie auf **OK**.

AppQoE-Richtlinien

October 5, 2021

Um AppQoE zu implementieren, müssen Sie mindestens eine Richtlinie konfigurieren, um Ihrem Citrix ADC mitzuteilen, wie die Verbindungen zu unterscheiden sind, die in einer bestimmten Warteschlange in die Warteschlange gestellt werden sollen.

So konfigurieren Sie eine AppQoE -Richtlinie mit der Befehlszeile

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
add appqoe policy <name> -rule <expression> -action <string>
```

Beispiel:

Im folgenden Beispiel werden Anforderungen mit einem User-Agent-Header ausgewählt, der “Android” enthält, und sie der Warteschlange mit mittlerer Priorität zugewiesen. Diese Anfragen kommen von Smartphones und Tablets, auf denen das Google Android Betriebssystem ausgeführt wird.

```
1  > add appqoe action appqoe-act-primd -priority MEDIUM
2  Done
3  > add appqoe policy appqoe-pol-primd -rule ”HTTP.REQ.HEADER(”User-Agent
       ”).CONTAINS(”Android”)” -action appqoe-act-primd
4  Done
5  > sh appqoe policy appqoe-pol-primd
6          Name: appqoe-pol-primd
7          Rule: HTTP.REQ.HEADER(”User-Agent”).CONTAINS(”Android”)
8          Action: appqoe-act-primd
9          Hits: 0
10
11 Done
12 <!--NeedCopy-->
```

Parameter für die Konfiguration einer AppQoE -Richtlinie

- ein. Ein Name für die AppQoE-Richtlinie. Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrich beginnen und kann aus einem bis 127 Buchstaben, Zahlen und dem Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), am Zeichen (@), gleich (=), Doppelpunkt (:) und Unterstrich (_) bestehen. Sie sollten einen Namen auswählen, der die Art der Aktion identifiziert.
- -Regel. Ein Citrix ADC Ausdruck, der der Appliance mitteilt, welche Verbindungen sie verarbeiten soll.
- -Aktion. Die AppQoE -Aktion, die ausgeführt wird, wenn eine Verbindung mit der Richtlinie übereinstimmt.

So konfigurieren Sie eine AppQoE -Richtlinie mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **App-Expert** > **AppQoE** > **Richtlinien**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:

- Um eine Richtlinie zu erstellen, klicken Sie auf **Hinzufügen**.
- Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Bearbeiten**.

3. Wenn Sie eine Richtlinie **erstellen, geben Sie im Dialogfeld AppQoE-Richtlinie** erstellen im Textfeld Name einen Namen für die neue Richtlinie ein.

   Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrich beginnen und kann aus einem bis 127 Buchstaben, Zahlen und dem Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), am Zeichen (@), gleich (=), Doppelpunkt (:) und Unterstrich (_) bestehen. Sie sollten einen Namen auswählen, der den Zweck und die Auswirkungen dieser Richtlinie identifiziert.

   Wenn Sie eine vorhandene Richtlinie ändern, überspringen Sie diesen Schritt. Sie können den Namen einer vorhandenen Richtlinie nicht ändern.

4. Wählen Sie in der Dropdownliste **Aktion** die AppQoE-Aktion aus, die ausgeführt werden soll, wenn die Richtlinie mit einer Verbindung übereinstimmt. Klicken Sie auf das Pluszeichen (+), um das Dialogfeld **AppQoE-Aktion** hinzufügen zu öffnen und eine neue Aktion hinzuzufügen.

5. Geben Sie im Textfeld **Regel** entweder den Richtlinienausdruck direkt ein, oder klicken Sie auf Neu, um einen Richtlinienausdruck zu erstellen. Wenn Sie auf Neu klicken, führen Sie die folgenden Schritte aus:

   a) Klicken **Sie im Dialogfeld Ausdruck erstellen** auf **Hinzufügen**.
   1 Wählen **Sie im Dialogfeld Ausdruck hinzufügen** einen gemeinsamen Ausdruck aus der Dropdownliste **Häufig verwendete Ausdrücke** aus, oder verwenden Sie die Dropdownlisten Ausdruck **erstellen, um den Ausdruck** zu erstellen, der definiert, welcher Datenverkehr gefiltert werden soll.
   Wenn Sie einen eigenen Ausdruck erstellen möchten, wählen Sie zunächst den ersten Begriff aus der ersten Dropdownliste auf der linken Seite des Bereichs “Ausdruck konstruieren” aus. Die Auswahlmöglichkeiten in dieser Liste sind:

   - HTTP
   - SYS
   - CLIENT
   - SERVER
   - ANALYTICS
   - Text

   Die Standardeinstellung ist HTTP. Nachdem Sie eine Auswahl in der ersten Dropdownliste getroffen haben (oder den Standardwert akzeptieren), können Sie den nächsten Begriff in Ihrem Ausdruck aus der Dropdownliste rechts daneben auswählen. Die Begriffe in dieser Liste und andere Listen, die folgen, ändern sich je nach vorheriger Auswahl. Die Listen bieten nur Begriffe an, bei denen es sich um gültige Auswahlmöglichkeiten handelt. Fahren Sie mit der Auswahl von Begriffen fort, bis Sie den Ausdruck beendet haben.

a) Wenn Sie den gewünschten Ausdruck erstellt haben, klicken Sie auf **OK**. Der Ausdruck wird im Textfeld **Ausdruck** hinzugefügt.

6. Klicken Sie auf **Erstellen**. Der Ausdruck wird im Textfeld **Regel** angezeigt.

Entitätsvorlage für den Lastausgleich virtueller Server

October 5, 2021

> **Warnung**
>
> Die Funktionalität der Entitätsvorlage ist ab Citrix ADC 13.0 Build 82.x veraltet und empfiehlt Citrix alternativ, die Style Books zu verwenden. Weitere Informationen finden Sie unter Thema Stilbücher .

Eine Entitätsvorlage ist eine Sammlung von Informationen zum Erstellen einer Vorlage für den Lastausgleich eines virtuellen Servers auf einer Citrix ADC Appliance. Es enthält eine Spezifikation und eine Reihe von Standardeinstellungen, die für einen virtuellen Lastausgleichsserver konfiguriert werden sollen. Mithilfe einer Vorlage, die einen Satz von Standardeinstellungen definiert, können Sie schnell mehrere virtuelle Server konfigurieren, für die eine ähnliche Konfiguration erforderlich ist, während mehrere Konfigurationsschritte eliminiert werden.

Sie können eine Entitätsvorlage erstellen, indem Sie die Details des virtuellen Lastausgleichsservers in eine Vorlagendatei exportieren. Dies kann nur über die Citrix ADC GUI erfolgen. Sie verwenden die Citrix ADC GUI zum Exportieren, Importieren und Verwalten von Entitätsvorlagen. Sie können Entitätsvorlagen für andere Administratoren freigeben und Vorlagen verwalten, die lokal auf Ihrer Appliance oder Maschine gespeichert sind. Sie können auch Entitätsvorlagen von der Appliance oder Ihrem lokalen Computer importieren.

Bevor Sie eine Vorlage erstellen, sollten Sie mit der Konfiguration des virtuellen Lastausgleichsservers vertraut sein.

Vorlage für den Lastausgleich virtueller Server

Load Balancing Entity Templates werden auf die gleiche Weise erstellt wie Citrix ADC Anwendungsvorlagen. Wenn Sie einen virtuellen Lastausgleichsserver in eine Vorlagendatei exportieren, werden die folgenden beiden Dateien automatisch erstellt:

- Vorlagendatei für den Lastenausgleich des virtuellen Servers. Enthält XML-Elemente, in denen die Werte der Parameter gespeichert werden, die für den virtuellen Lastausgleichsserver konfiguriert sind. Die Datei enthält auch XML-Elemente zum Speichern von Informationen über gebundene Richtlinien.

- Bereitstellungsdatei. Enthält XML-Elemente, die bereitstellungsspezifische Informationen wie Dienste, Dienstgruppen und konfigurierte Variablen speichern.
  In den Vorlagen- und Bereitstellungsdateien wird jede Einheit von Konfigurationsinformationen in ein bestimmtes XML-Element gekapselt, das für diesen Einheitentyp vorgesehen ist. Beispielsweise wird der Parameter für die Lastausgleichsmethode, LBMethod, in den <lbmethod> Tags </lbmethod> und gekapselt.

> **Hinweis:**
>
> Nachdem Sie einen virtuellen Lastausgleichsserver exportiert haben, können Sie Elemente hinzufügen, Elemente entfernen und vorhandene Elemente ändern, bevor Sie die Konfigurationsinformationen in eine Citrix ADC Appliance importieren.

Funktionsweise einer Vorlage für den Lastausgleich eines virtuellen Servers

Wenn Sie eine Vorlage für einen virtuellen Lastausgleichsserver erstellen, geben Sie Standardwerte für den Server an. Sie geben an, welche Werte schreibgeschützt sein müssen, welche Werte nicht angezeigt werden dürfen und welche Werte Benutzer konfigurieren können. Sie konfigurieren auch die Seiten, die den Vorlagenimport-Assistenten zusammenstellen. Alle von Ihnen angegebenen Informationen und Einstellungen werden in der Vorlagendatei gespeichert.
Wenn ein Benutzer die Vorlage in eine Citrix ADC Appliance importiert, führt die GUI den Benutzer durch die verschiedenen Seiten, die Sie für die Vorlage konfiguriert haben. Die GUI zeigt die schreibgeschützten Parameterwerte an und fordert den Benutzer auf, Werte für die konfigurierbaren Parameter anzugeben. Nachdem der Benutzer die Anweisungen befolgt hat, erstellt die Appliance die Entität mit den konfigurierten Werten.
Sie können eine Entitätsvorlage für einen virtuellen Lastausgleichsserver vom Knoten Traffic Management aus erstellen oder ändern.
Um Details des virtuellen Servers in eine Vorlage zu exportieren, müssen Sie die folgenden Optionen und Einstellungen für die Vorlage angeben:

- Der Standardwert eines Parameters.
- Gibt an, ob die Standardwerte für Benutzer sichtbar sind.
- Gibt an, ob die Standardwerte von Benutzern geändert werden können.
- Die Anzahl der Seiten im Entitätsimport-Assistenten, einschließlich der Seitennamen, des Textes und der verfügbaren Parameter.
- Die Entitäten, die an die Entität gebunden werden müssen, für die die Vorlage erstellt wird.

Wenn Sie beispielsweise eine Vorlage für den virtuellen Lastenausgleich erstellen, können Sie die Richtlinien angeben, die Sie an den virtuellen Server binden möchten, den Sie aus der Vorlage erstellen. In der Vorlage sind jedoch nur verbindliche Informationen enthalten. Die gebundenen Entitäten sind nicht enthalten. Wenn die Entitätsvorlage in eine andere Citrix ADC Appliance importiert wird, müssen die gebundenen Entitäten zur Importzeit auf der Appliance vorhanden sein, damit die

Bindung erfolgreich ist. Wenn keine der gebundenen Entitäten auf der Ziel-Appliance vorhanden sind, wird die Entität (für die die Vorlage konfiguriert wurde) ohne Bindungen erstellt. Wenn nur eine Teilmenge der gebundenen Entitäten auf der Ziel-Appliance vorhanden sind, sind sie an die Entität gebunden, die aus der Vorlage erstellt wird.
Wenn Sie eine Vorlage für den virtuellen Lastausgleichsserver exportieren, werden die Konfigurationseinstellungen der Entität in der Vorlage angezeigt. Alle gebundenen Elemente sind standardmäßig ausgewählt, aber Sie können Bindungen nach Bedarf ändern. Wie bei einer Vorlage, die nicht auf einer vorhandenen Entität basiert, werden nur Bindungsinformationen und nicht die Entitäten enthalten. Sie können die Vorlage entweder mit den vorhandenen Konfigurationseinstellungen speichern oder die Einstellungen als Grundlage für die Erstellung einer neuen Konfiguration für eine Vorlage verwenden.

Konfigurieren von Variablen in der Vorlage für den Lastausgleich virtueller Server

Vorlagen für den Lastausgleich für virtuelle Server unterstützen die Deklaration von Variablen in den konfigurierten Lastausgleichsparametern sowie in gebundenen Richtlinien und Aktionen. Mit der Möglichkeit, Variablen zu deklarieren, können Sie vorkonfigurierte Werte durch Werte ersetzen, die der Umgebung entsprechen, in die Sie die Vorlage importieren.

Betrachten Sie beispielsweise den folgenden Ausdruck, der für eine Richtlinie konfiguriert ist, die an einen virtuellen Lastausgleichsserver gebunden ist, für den Sie eine Vorlage erstellen. Der Ausdruck wertet den Wert des Accept-Language-Headers in einer HTTP-Anforderung aus.

```
HTTP.REQ.HEADER("Accept-Language").CONTAINS("en-us")
```

Wenn der Wert des Headers zum Importzeitpunkt konfigurierbar sein soll, können Sie den String en-us als Variable angeben.

Nachdem Sie eine Variable erstellt haben, können Sie Folgendes tun:

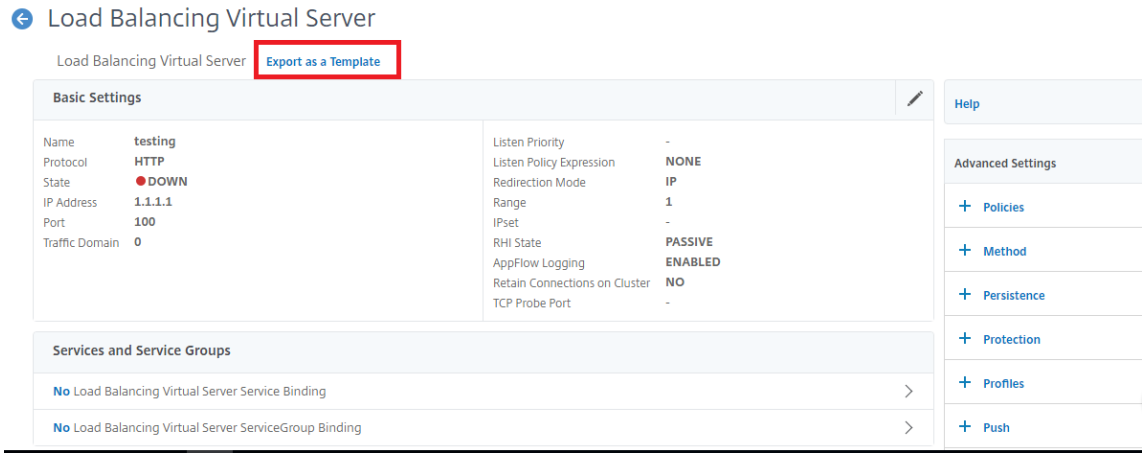
- Weisen Sie einer vorhandenen Variablen mehr Strings zu. Nachdem Sie eine Variable für eine Zeichenfolge erstellt haben, können Sie andere Teile desselben oder eines anderen Ausdrucks auswählen und der Variablen zuweisen. Die Zeichenfolgen, die Sie einer Variablen zuweisen, müssen nicht identisch sein. Beim Importieren werden alle Zeichenfolgen, die der Variablen zugewiesen sind, durch den von Ihnen angegebenen Wert ersetzt.
- Zeigen Sie die Zeichenfolge (en) an, die der Variablen zugewiesen sind.
- Anzeigen einer Liste aller Entitäten und Parameter, die die Variable

So konfigurieren Sie Variablen in einer Vorlage für den Lastausgleich für virtuelle Server

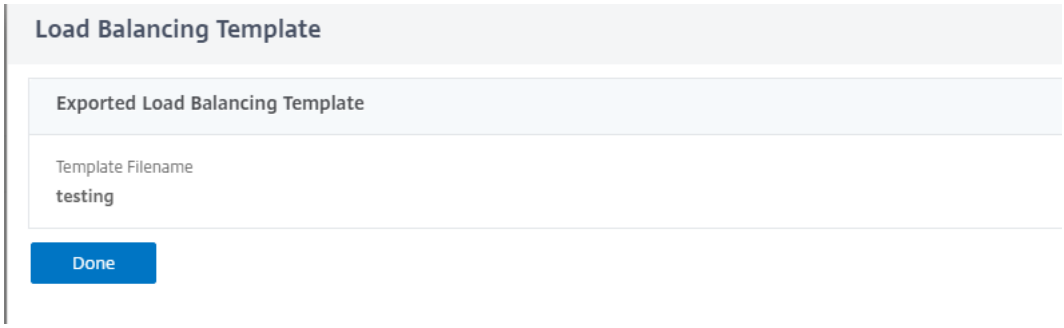
Führen Sie das folgende Verfahren aus, um Variablen für eine Vorlage für den Lastausgleich mit der Citrix ADC GUI zu konfigurieren.

1. Navigieren Sie zu **Verkehrsverwaltung** > **Lastenausgleich** > **Virtuelle Server**

2. Klicken Sie im Detailbereich mit der rechten Maustaste auf den virtuellen Server, den Sie in eine Vorlagendatei exportieren möchten, und klicken Sie dann auf **Hinzufügen**.
3. Legen Sie auf der Seite **Virtueller Load Balancing Server erstellen** die Parameter des virtuellen Servers fest. Weitere Informationen zum Konfigurieren eines virtuellen Lastausgleichsservers finden Sie unter Funktionsweise des Lastenausgleichs
4. Wenn Sie die Parameter für den virtuellen Lastausgleichsserver festgelegt haben, klicken Sie auf **Fertig**.



5. Klicken Sie oben auf den Link **Als Vorlage** exportieren, um die Serverdetails als Vorlagendatei zu exportieren.
6. Geben **Sie auf der Seite Load Balancing Vorlage erstellen** die Vorlageneinstellungen ein.
7. Klicken Sie auf **Fertig**.



Ändern einer Vorlage für den Lastausgleich eines virtuellen Servers

Sie können nur die Parameter, Bindungen und Seiten ändern, die für eine Vorlage konfiguriert sind. Der Name und der Speicherort der Vorlage, die beim Erstellen der Vorlage angegeben wurde, können nicht geändert werden. Die Citrix ADC Appliance bietet Ihnen nicht die Möglichkeit, eine Vorlage für den Lastausgleich für virtuelle Server zu ändern.

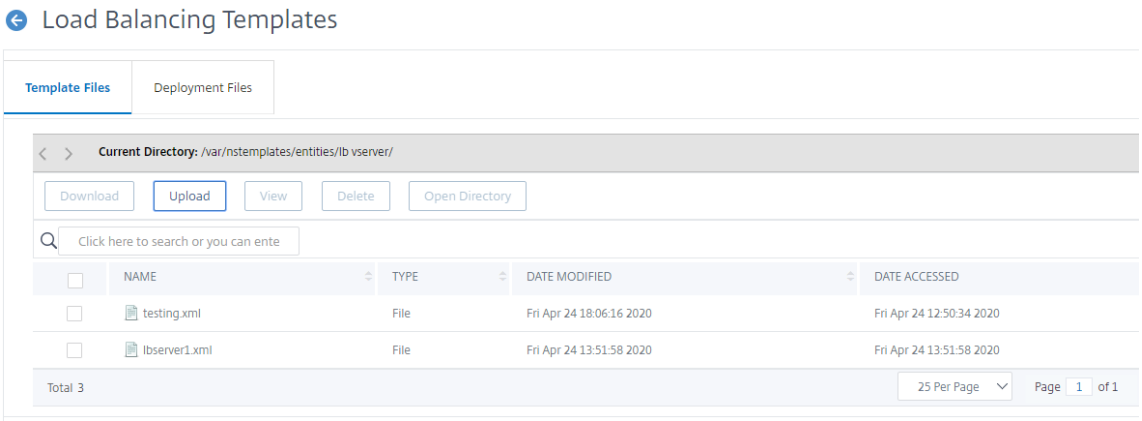
So ändern Sie einen virtuellen Lastausgleichsserver über die Citrix ADC GUI

1. Navigieren Sie zu **Datenverkehrsverwaltung** > **Lastausgleich** > **Virtuelle Server**.
2. Ändern Sie auf der Seite **Virtueller Server für den Lastausgleich** die Entitätsparameter.
3. Klicken Sie auf Fertig.
4. Klicken Sie auf **Als Vorlage exportieren**.
5. Die geänderten Änderungen sind jetzt in der Vorlagendatei für den Lastausgleich des virtuellen Servers verfügbar.
6. Klicken Sie auf der Seite **Exportierte Lastausgleichsvorlage** auf **Fertig**.

Verwalten von Vorlagen für den Lastausgleich virtueller Server

Mit der Citrix ADC GUI können Sie Vorlagendateien für den Lastenausgleich und Bereitstellungsdateien für virtuelle Server organisieren.

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Wählen Sie auf der Seite **Virtuelle Server** die Option **Vorlage verwalten aus**.
3. Klicken Sie auf der Seite **Lastausgleichsvorlagen** auf die Registerkarte **Vorlagendatei**.
4. Auf der Registerkarte **Vorlagendateien** können Sie eine Vorlage aus dem und in den Vorlagenordner der Appliance hochladen oder herunterladen.

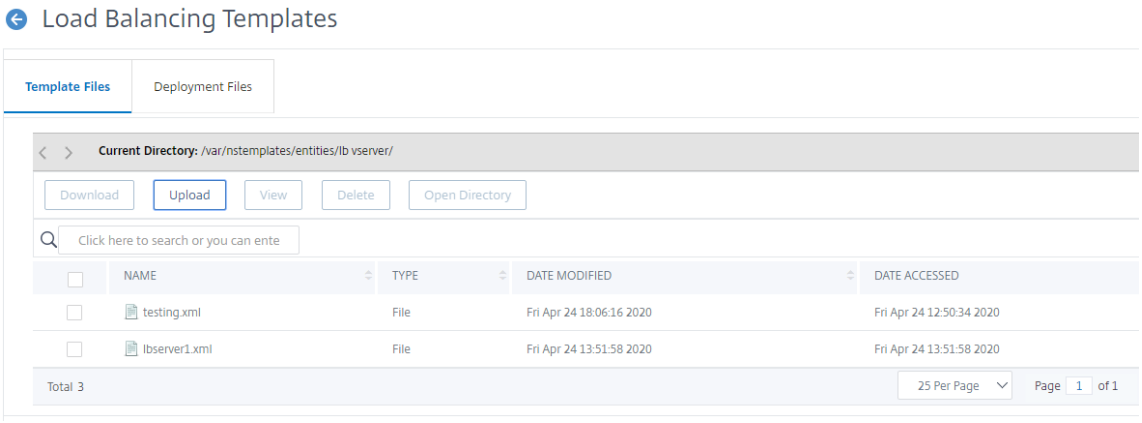


5. Klicken Sie auf **Schließen**.

So laden Sie eine Vorlage für den Lastausgleich virtueller Server über die Citrix ADC GUI hoch

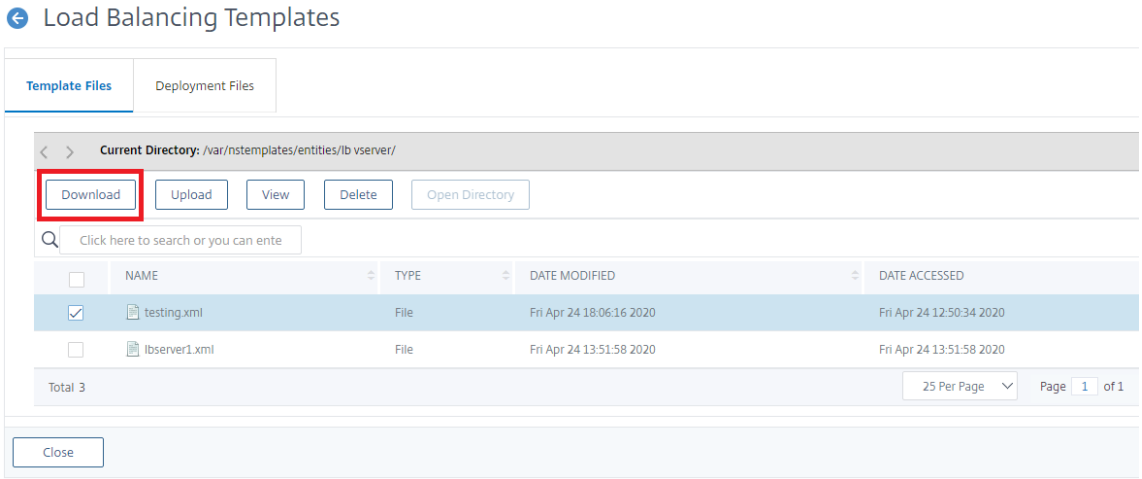
1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Klicken Sie auf der Seite **Virtuelle Server** auf **Aktion auswählen**, und wählen Sie dann **Vorlage verwalten**aus.
3. Klicken Sie auf der Seite Load Balancing-Vorlagen auf die Registerkarte **Vorlagendateien** .
4. Klicken Sie auf der Registerkarte **Vorlagendateien** auf **Hochladen**, um eine Vorlage hochzuladen.

5. Klicken Sie auf **Schließen**.



So laden Sie die Entity-Vorlage für den Lastausgleich eines virtuellen Servers über die Citrix ADC GUI herunter

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Klicken Sie auf der Seite **Virtuelle Server** auf **Aktion auswählen**, und wählen Sie dann **Vorlage verwalten**aus.
3. Klicken Sie auf der Seite **Load Balancing-Vorlagen** auf die Registerkarte **Vorlagendateien**.
4. Wählen Sie auf der Registerkarte Vorlagendateien eine Vorlagendatei aus, und klicken Sie auf Herunterladen.
5. Klicken Sie auf Schließen.



Beispiel für die Vorlage für den Lastausgleich virtueller Server und die Bereitstellungsvorlage

Es folgt ein Beispiel für eine Vorlagendatei, die aus einem virtuellen Lastausgleichsserver namens “Lb-vip” erstellt wurde:


```
COPY

<?xml version=”1.0” encoding=”UTF-8” ?>
  <template>
    <template_info>
      <entity_name>Lbvip</entity_name>
      <version_major>10</version_major>
      <version_minor>0</version_minor>
      <build_number>40.406</build_number>
    </template_info>
    <entitytemplate>
      <lbvserver_list>
        <lbvserver>
          <name>Lbvip</name>
          <servicetype>HTTP</servicetype>
          <ipv46>0.0.0.0</ipv46>
          <ipmask>*</ipmask>
          <port>0</port>
          <range>1</range>
          <persistencetype>NONE</persistencetype>
          <timeout>2</timeout>
          <persistencebackup>NONE</persistencebackup>
          <backuppersistencetimeout>2</backuppersistencetimeout>
          <lbmethod>LEASTCONNECTION</lbmethod>
          <persistmask>255.255.255.255</persistmask>
          <v6persistmasklen>128</v6persistmasklen>
          <pq>OFF</pq>
          <sc>OFF</sc>
          <m>IP</m>
          <datalength>0</datalength>
          <dataoffset>0</dataoffset>
          <sessionless>DISABLED</sessionless>
          <state>ENABLED</state>
          <connfailover>DISABLED</connfailover>
          <clttimeout>180</clttimeout>
          <somethod>NONE</somethod>
          <sopersistence>DISABLED</sopersistence>
          <sopersistencetimeout>2</sopersistencetimeout>
          <redirectportrewrite>DISABLED</redirectportrewrite>
          <downstateflush>DISABLED</downstateflush>
          <gt2gb>DISABLED</gt2gb>
          <ipmapping>0.0.0.0</ipmapping>
          <disableprimaryondown>DISABLED</disableprimaryondown>
```



```
            <insertvserveripport>OFF</insertvserveripport>
            <authentication>OFF</authentication>
            <authn401>OFF</authn401>
            <push>DISABLED</push>
            <pushlabel>none</pushlabel>
            <l2conn>OFF</l2conn>
            <appflowlog>DISABLED</appflowlog>
            <icmpvsrresponse>PASSIVE</icmpvsrresponse>
            <lbvserver_cmppolicy_binding_list>
              <lbvserver_cmppolicy_binding>
                <name>Lbvip</name>
                <policyname>NOPOLICY-COMPRESSION</policyname>
                <priority>100</priority>
                <gotopriorityexpression>END</gotopriorityexpression>
                <bindpoint>REQUEST</bindpoint>
              </lbvserver_cmppolicy_binding>
            </lbvserver_cmppolicy_binding_list>
          </lbvserver>
        </lbvserver_list>
      </entitytemplate>
    </template>
<!--NeedCopy-->
```

Beispiel einer Bereitstellungsdatei

Im vorangegangenen Beispiel folgt die Bereitstellungsdatei, die dem virtuellen Server zugeordnet ist: COPY

```
<?xml version="1.0" encoding="UTF-8" ?>
  <template_deployment>
    <template_info>
      <entity_name>Lbvip</entity_name>
      <version_major>10</version_major>
      <version_minor>0</version_minor>
      <build_number>40.406</build_number>
    </template_info>
    <service_list>
      <service>
      <ip>1.2.3.4</ip>
      <port>80</port>
      <servicetype>HTTP</servicetype>
      </service>
    </service_list>
```



```
16      <servicegroup_list>
17        <servicegroup>
18          <name>svcgrp</name>
19          <servicetype>HTTP</servicetype>
20          <servicegroup_servicegroupmember_binding_list>
21            <servicegroup_servicegroupmember_binding>
22              <ip>1.2.3.90</ip>
23              <port>80</port>
24            </servicegroup_servicegroupmember_binding>
25          <servicegroup_servicegroupmember_binding>
26            <ip>1.2.8.0</ip>
27            <port>80</port>
28          </servicegroup_servicegroupmember_binding>
29          <servicegroup_servicegroupmember_binding>
30            <ip>1.2.8.1</ip>
31            <port>80</port>
32          </servicegroup_servicegroupmember_binding>
33          <servicegroup_servicegroupmember_binding>
34            <ip>1.2.9.0</ip>
35            <port>80</port>
36          </servicegroup_servicegroupmember_binding>
37        </servicegroup_servicegroupmember_binding_list>
38      </servicegroup>
39    </servicegroup_list>
40  </template_deployment>
41
42  <!--NeedCopy-->
```

HTTP-Callouts

October 5, 2021

Für bestimmte Arten von Anforderungen oder wenn bestimmte Kriterien während der Richtlinienbewertung erfüllt sind, sollten Sie die Richtlinienbewertung kurz abhalten, Informationen von einem Server abrufen und dann eine bestimmte Aktion ausführen, die von den abgerufenen Informationen abhängt. Zu anderen Zeiten, wenn Sie bestimmte Arten von Anforderungen erhalten, sollten Sie möglicherweise eine Datenbank oder den auf einem Webserver gehosteten Inhalt aktualisieren. HTTP-Callouts ermöglichen es Ihnen, all diese Aufgaben auszuführen.

ein HTTP-Callout ist eine HTTP- oder HTTPS-Anforderung, die die Citrix ADC Appliance generiert und an eine externe Anwendung sendet, wenn bestimmte Kriterien während der Richtlinienbewertung erfüllt werden. Die vom Server abgerufenen Informationen können durch Standardausdrücke der Syn-

taxrichtlinie analysiert werden, und eine entsprechende Aktion kann ausgeführt werden. Sie können HTTP-Callouts für HTTP-Content Switching, TCP-Content Switching, Rewrite, Responder und für die token-basierte Methode des Lastenausgleichs konfigurieren.

Bevor Sie ein HTTP-Callout konfigurieren, müssen Sie eine Anwendung auf dem Server einrichten, an die das Callout gesendet wird. Die Anwendung, die als *HTTP-Callout-Agent* bezeichnet wird, muss so konfiguriert sein, dass sie auf die HTTP-Callout-Anforderung mit den erforderlichen Informationen reagiert. Der HTTP-Callout-Agent kann auch ein Webserver sein, der die Daten bereitstellt, für die die Citrix ADC Appliance das Callout sendet. Sie müssen sicherstellen, dass sich das Format der Antwort auf ein HTTP-Callout nicht von einem Aufruf zu einem anderen ändert.

Nachdem Sie den HTTP-Callout-Agent eingerichtet haben, konfigurieren Sie das HTTP-Callout auf der Citrix ADC Appliance. Zum Aufrufen des Callouts schließen Sie das Callout in eine Standard-Syntaxrichtlinie in die entsprechende Citrix ADC Funktion ein und binden die Richtlinie dann an den Bindepunkt, an dem die Richtlinie ausgewertet werden soll.

Nachdem Sie das HTTP-Callout konfiguriert haben, müssen Sie die Konfiguration überprüfen, um sicherzustellen, dass das Callout ordnungsgemäß funktioniert.

Funktionsweise eines HTTP-Callouts

October 5, 2021

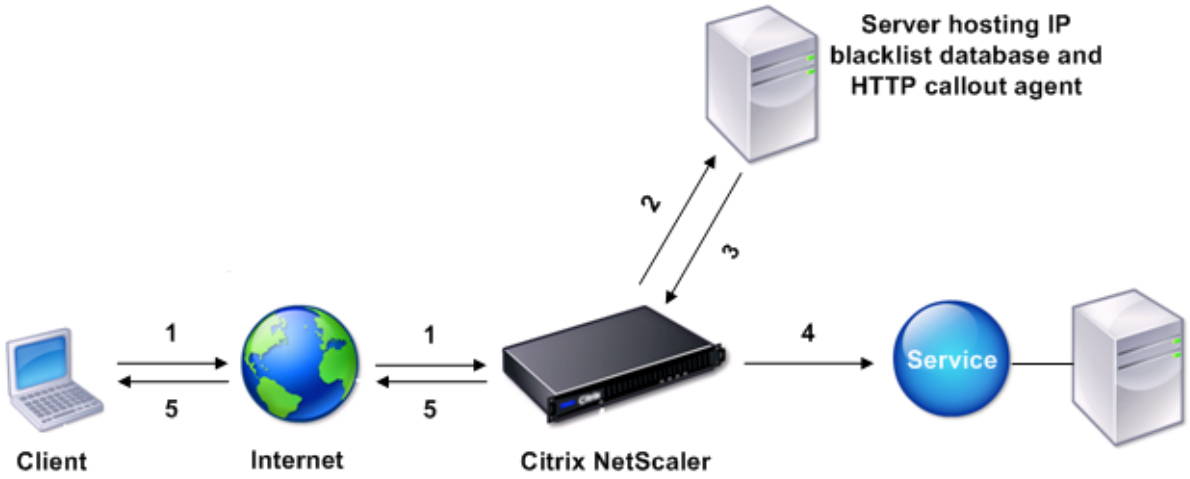
Wenn die Citrix ADC Appliance eine Clientanforderung empfängt, wertet die Appliance die Anforderung anhand der Richtlinien aus, die an verschiedene Bindungspunkte gebunden sind. Wenn die Appliance während dieser Auswertung auf den HTTP-Callout-Ausdruck stößt`SYS.HTTP_CALLOUT(<name>)`, wird die Richtlinienauswertung kurz angehalten und eine Anforderung an den HTTP-Callout-Agent sendet, indem die für das angegebene HTTP-Callout konfigurierten Parameter verwendet werden. Nach Erhalt der Antwort überprüft die Appliance den angegebenen Teil der Antwort und führt dann entweder eine Aktion aus oder wertet die nächste Richtlinie aus, je nachdem, ob die Auswertung der Antwort vom HTTP-Callout-Agent TRUE bzw. FALSE ergibt. Wenn beispielsweise das HTTP-Callout in einer Responder-Richtlinie enthalten ist und die Auswertung der Antwort auf TRUE ausgewertet wird, führt die Appliance die Aktion aus, die der Responder-Richtlinie zugeordnet ist.

Wenn die HTTP-Callout-Konfiguration falsch oder unvollständig ist oder wenn sich das Callout rekursiv selbst aufruft, löst die Appliance eine UNDEF-Bedingung aus und aktualisiert den nicht definierten Treffer-Zähler.

Die folgende Abbildung veranschaulicht die Funktionsweise eines HTTP-Callouts, die von einer global gebundenen Responderrichtlinie aufgerufen wird. Das HTTP-Callout ist so konfiguriert, dass sie die IP-Adresse des Clients enthält, der einer eingehenden Anforderung zugeordnet ist. Wenn

die Citrix ADC Appliance eine Anforderung von einem Client empfängt, generiert die Appliance die Callout-Anforderung und sendet sie an den Callout-Server, der eine Datenbank mit IP-Adressen in der Sperrliste hostet, und einen HTTP-Callout-Agent, der prüft, ob die IP-Adresse des Clients in der Datenbank aufgeführt ist. Der HTTP-Callout-Agent empfängt die Callout-Anforderung, überprüft, ob die IP-Adresse des Clients aufgeführt ist, und sendet eine Antwort, die von der Citrix ADC Appliance ausgewertet wird. Wenn die Antwort darauf hinweist, dass die IP-Adresse des Clients nicht auf der Sperrliste ist, leitet die Appliance die Antwort an den konfigurierten Dienst weiter. Wenn die IP-Adresse des Clients auf die Sperrliste gesetzt wird, setzt die Appliance die Clientverbindung zurück.

Abbildung 1. HTTP-Callout-Entitätsmodell



Hinweise zum Format von HTTP-Anfragen und -Antworten

October 5, 2021

Die Citrix ADC Appliance überprüft nicht die Gültigkeit der HTTP-Callout-Anforderung. Bevor Sie HTTP-Callouts konfigurieren, müssen Sie daher das Format einer HTTP-Anforderung kennen. Sie müssen auch das Format einer HTTP-Antwort kennen, da beim Konfigurieren eines HTTP-Callouts Ausdrücke konfiguriert werden, die die Antwort vom HTTP-Callout-Agent auswerten.

Dieser Abschnitt umfasst die folgenden Abschnitte:

- Format einer HTTP-Anfrage
- Format einer HTTP-Antwort

Format einer HTTP-Anfrage

Eine HTTP-Anforderung enthält eine Reihe von Zeilen, die jeweils mit einem Wagenrücklauf und einem Zeilenvorschub versehen sind <CR><LF> or \r\n.

Die erste Zeile einer Anforderung (die *Nachrichtenzeile*) enthält die HTTP-Methode und das Ziel. Beispielsweise enthält eine Nachrichtenzeile für eine GET-Anforderung das Schlüsselwort GET und eine Zeichenfolge, die das abzurufende Objekt darstellt, wie im folgenden Beispiel gezeigt:

```
GET /mysite/mydirectory/index.html HTTP/1.1\r\n
<!--NeedCopy-->
```

Der Rest der Anforderung enthält HTTP-Header, einschließlich eines erforderlichen Host-Headers und gegebenenfalls eines Nachrichtentextes.

Die Anfrage endet mit einer Bankverbindung (ein Extra<CR><LF> or \r\n).

Es folgt ein Beispiel für eine Anfrage:

```
Get /mysite/index.html HTTP/1.1\r\n
Host: 10.101.101.10\r\n
Accept: \*/\*\r\n
\r\n
<!--NeedCopy-->
```

Format einer HTTP-Antwort

Eine HTTP-Antwort enthält eine Statusmeldung, HTTP-Header der Antwort-Antwort und das angeforderte Objekt oder, wenn das angeforderte Objekt nicht bereitgestellt werden kann, eine Fehlermeldung.

Es folgt ein Beispiel für eine Antwort:

```
HTTP/1.1 200 OK\r\n
Content-Length: 55\r\n
Content-Type: text/html\r\n
Last-Modified: Wed, 12 Aug 1998 15:03:50 GMT\r\n
Accept-Ranges: bytes\r\n
ETag:  “04f97692cbd1:377” \r\n
Date: Thu, 19 Jun 2008 19:29:07 GMT\r\n
\r\n
```



```
<55-character response>
<!--NeedCopy-->
```

Konfigurieren eines HTTP-Callouts

October 5, 2021

Bei der Konfiguration eines HTTP-Callouts geben Sie den Typ der Anforderung (HTTP oder HTTPS), das Ziel und das Format der Anforderung an. Das erwartete Format der Antwort und schließlich der Teil der Antwort, den Sie analysieren möchten.

Für das Ziel geben Sie entweder die IP-Adresse und den Port des HTTP-Callout-Agenten an. Oder betreiben Sie einen Lastenausgleich, einen Content Switching oder einen virtuellen Cache-Umleitungsserver, um die HTTP-Callout-Anforderungen zu verwalten.

Im ersten Fall werden die HTTP-Callout-Anfragen direkt an den HTTP-Callout-Agent gesendet. Im zweiten Fall werden die HTTP-Callout-Anfragen an die virtuelle IP-Adresse (VIP) des angegebenen virtuellen Servers gesendet. Der virtuelle Server verarbeitet die Anforderung auf die gleiche Weise, wie er eine Clientanforderung verarbeitet. Wenn Sie beispielsweise erwarten, dass viele Callouts generiert werden, können Sie Instanzen des HTTP-Callout-Agenten auf mehreren Servern konfigurieren, diese Instanzen (als Dienste) an einen virtuellen Lastausgleichsserver binden und dann den virtuellen Lastausgleichsserver in der HTTP-Callout-Konfiguration angeben. Der virtuelle Lastausgleichsserver gleicht dann die Last auf den konfigurierten Instanzen aus, wie durch den Lastausgleichsalgorithmus bestimmt.

Für das Format der HTTP-Callout-Anforderung können Sie die einzelnen Attribute der HTTP-Calloutanforderung (eine attributbasierte HTTP-Callout) angeben oder die gesamte HTTP-Callout-Anforderung als erweiterten Richtlinienausdruck (eine ausdrucksbasierte HTTP-Callout) angeben.

In der folgenden Tabelle werden die Elemente in einer HTTP-Callout-Richtlinie beschrieben:

Weitere Informationen finden Sie unter Policy-HttpCallout

Parameter	Beschreibung
Name	Name des Callouts, maximal 127 Zeichen

Parameter	Beschreibung
IP-Adresse und Port (*IP-Adresse/Port*) oder Name des virtuellen Servers (vserver)	IPv4- oder IPv6-Adresse des Servers, an den das Callout gesendet wird, oder ein Platzhalter und des Port auf dem Server, an den das Callout gesendet wird, oder ein Platzhalter. Oder der Name eines virtuellen Load Balancing-, Content Switching- oder Cache-Umleitungsservers mit einem Diensttyp von HTTP.
HTTP-Methode (HttpMethod)	HTTP-Methode (HttpMethod). Methode, die in der HTTP-Anforderung verwendet wird, die dieser Callout sendet. Gültige Werte: GET oder POST. Standardwert: GET.
Host-Ausdruck (HostExpr)	Host-Ausdruck (HostExpr). Erweiterter Textausdruck zum Konfigurieren des Host-Headers. Maximale Länge: 255 Der Ausdruck kann ein Literalwert sein oder ein erweiterter Ausdruck sein, der den Wert ableitet. Beispiele: “10.101.10.11”, “http.req.header (“Host”)”
URL-Stammausdruck (urlStemExpr)	URL-Stammausdruck (urlStemExpr) Ein erweiterter Zeichenfolgenausdruck zum Generieren des URL-Stammes. Maximale Länge: 8191 Der Ausdruck kann eine literale Zeichenfolge oder ein Ausdruck sein, der den Wert ableitet. Beispiele: “” /mysite/index.html “” “http.req.url”

Parameter	Beschreibung
HTTP-Header (Header)	HTTP-Header (Header). Erweiterter Textausdruck zum Einfügen von HTTP-Headern und deren Werten in die HTTP-Calloutanforderung. Geben Sie für jeden Header einen Wert an. Sie geben den Header-Namen als String und den Header-Wert als erweiterten Ausdruck an. Geben Sie die Header durch Leerzeichen getrennt an. Wie -Header cip (client.ip.src) hdr (http.req.header (“HDR”)). Die Anzahl der Header kann 8 betragen
Ausdruckbasierte Anfrage zum Senden an den Server (FullReqExpr)	Exakte HTTP-Anforderung, die der Citrix ADC als erweiterter Ausdruck an 8191 Zeichen senden soll. Wenn Sie diesen Parameter angeben, müssen Sie die Argumente HttpMethod, HostExpr, urlStemExpr, Header und Parameter weglassen. Der Anforderungsausdruck wird durch das Feature eingeschränkt, in dem das Callout verwendet wird. Beispielsweise kann ein HTTP.RES-Ausdruck nicht in einer Richtlinienbank zur Anforderungszeit oder in einer TCP-Content Switching-Richtlinienbank verwendet werden.
Ausdruckbasierte Anfrage zum Senden an den Server (BodyExpr)	Ein erweiterter Zeichenfolgenausdruck zum Generieren des Hauptkörpers der Anforderung. Der Ausdruck kann eine literale Zeichenfolge oder einen Ausdruck enthalten, der den Wert ableitet (z. B. client.ip.src). Schließt sich gegenseitig mit -FullReqExpr aus.

Parameter	Beschreibung
Parameter	Erweiterter Ausdruck zum Einfügen von Abfrageparametern in die HTTP-Anforderung, die der Callout sendet. Geben Sie einen Wert für jeden Parameter an, den Sie konfigurieren. Wenn die Callout-Anfrage die GET-Methode verwendet, werden diese Parameter in die URL eingefügt. Wenn die Callout-Anfrage die POST-Methode verwendet, werden diese Parameter in den POST-Text eingefügt. Sie konfigurieren den Namen des Abfrageparameters als String und den Wert als erweiterten Ausdruck. Die Parameterwerte sind URL-codiert. Geben Sie die durch Leerzeichen getrennten Parameter wie ⊠parameter name1 (“name1”) name2 (http.req.header (“hdr”)) an. Die maximal 8 Parameter können konfiguriert werden.
Rückgabetyp (ReturnType)	Typ der Daten, die die Zielanwendung in der Antwort auf den Callout zurückgibt. Gültige Werte: TEXT: Behandeln Sie den zurückgegebenen Wert als Textzeichenfolge. NUM: Behandeln Sie den zurückgegebenen Wert als Zahl. BOOL: Behandelt den zurückgegebenen Wert als booleschen Wert. Hinweis: Sie können den Rückgabetyp nicht ändern, nachdem er festgelegt wurde.

Parameter	Beschreibung
Ausdruck zum Extrahieren von Daten aus der Antwort (ResultExPR)	Erweiterter Ausdruck, der HTTP.RES-Objekte aus der Antwort auf die HTTP-Callout extrahiert. Die maximale Länge beträgt 8191. Die Operationen in diesem Ausdruck müssen mit dem Rückgabetyp übereinstimmen. Wenn Sie beispielsweise einen Rückgabetyp von Text konfigurieren, muss der Ergebnisausdruck ein textbasierter Ausdruck sein. Wenn der Rückgabetyp num ist, muss der Ergebnisausdruck (resultExpr) einen numerischen Wert ähnlich dem folgenden zurückgeben: “http.res.body (10000) .length” Hinweis: Wenn Sie manchmal einen Rückgabetyp von TEXT festlegen und das vom Server gesendete Ergebnis 16 KB überschreitet, kann der Ergebnisausdruck NULL zurückgeben. Wenn das Ergebnis beispielsweise eine verkettete Zeichenfolge ist, die 16 KB überschreitet.
Schema	Die Art des Schemas für den Callout-Server. Beispiel: HTTP, https
CacheForSecs	Dauer in Sekunden, für die die Callout-Antwort zwischengespeichert wird. Die zwischengespeicherten Antworten werden in einer integrierten Caching-Content-Gruppe namens “CalloutContentGroup” gespeichert. Wenn keine Dauer konfiguriert ist, werden die Callout-Antworten nur zwischengespeichert, es sei denn, eine normale Caching-Konfiguration wird verwendet, um sie zu zwischenspeichern. Dieser Parameter hat Vorrang vor jeder normalen Caching-Konfiguration, die sonst für diese Antworten gelten würde.

Hinweis: Die Appliance überprüft nicht die Gültigkeit der Anforderung. Sie müssen sicherstellen, dass es sich bei der Anfrage um eine gültige Anfrage handelt und keine vertraulichen Informationen en-

thält. Eine falsche oder unvollständige HTTP-Callout-Konfiguration führt zu einer Runtime-UNDEF-Bedingung, die keiner Aktion zugeordnet ist. Die UNDEF-Bedingung aktualisiert lediglich den Zähler Undefined Hits, wodurch Sie eine falsch konfigurierte HTTP-Callout beheben können. Die Appliance analysiert jedoch die HTTP-Callout-Anforderung, damit Sie bestimmte Citrix ADC-Funktionen für den Callout konfigurieren können. Dies kann zu einem HTTP-Callout führen, der sich selbst aufruft. Informationen zur Callout-Rekursion und wie Sie sie vermeiden können, finden Sie unter Vermeiden von HTTP-Callout-Rekursion.

Unabhängig davon, ob Sie HTTP-Anforderungsattribute oder einen Ausdruck verwenden, um das Format der HTTP-Callout-Anforderung zu definieren, müssen Sie das Format der Antwort vom HTTP-Callout-Agent und den Teil der Antwort angeben, den Sie auswerten möchten. Der Antworttyp kann ein boolescher Wert, eine Zahl oder Text sein. Nur basierend auf diesem Rückgabetyp können Sie die weiteren Ausdrucksmethoden für die Callout-Antwort verwenden. Wenn der Rückgabetyp eine Zahl ist, können Sie den zahlenbasierten Ausdruck für die Callout-Antwort verwenden. Der Teil der Antwort, den Sie auswerten möchten, wird durch einen Ausdruck angegeben. Wenn Sie beispielsweise angeben, dass die Antwort Text enthält, können `HTTP.RES.BODY(<unit>)` Sie angeben, dass die Appliance nur die ersten <unit>Bytes der Antwort des Callout-Agenten auswerten darf.

In der Befehlszeile erstellen Sie zunächst ein HTTP-Callout mit dem Befehl
add. Wenn Sie ein Callout hinzufügen, werden alle Parameter auf den Standardwert NONE festgelegt, mit Ausnahme der HTTP-Methode, die auf den Standardwert GET festgelegt ist. Anschließend konfigurieren Sie die Parameter des mit dem Befehl set. Der Befehl set wird verwendet, um beide Arten von Callouts zu konfigurieren (attributsbasiert und ausdrucksbasiert). Der Unterschied liegt in den Parametern, die für die Konfiguration der beiden Arten von Callouts verwendet werden. Die folgenden Befehlszeilenanweisungen enthalten also einen set-Befehl zum Konfigurieren eines attributbasierten Callouts und einen set-Befehl zum Konfigurieren eines ausdrucksbasierten Callouts. Im Konfigurationsprogramm werden alle diese Konfigurationsaufgaben in einem einzigen Dialogfeld ausgeführt.

Hinweis: Bevor Sie ein HTTP-Callout in eine Richtlinie einfügen, können Sie alle konfigurierten Parameter mit Ausnahme des Rückgabetyps ändern. Sobald sich ein HTTP-Callout in einer Richtlinie befindet, können Sie einen Ausdruck, der in dem Callout konfiguriert ist, nicht vollständig ändern. Beispielsweise können Sie HTTP.REQ.HEADER (“myval”) nicht in CLIENT.IP.SRC ändern. Sie können die Operatoren und Argumente ändern, die an den Ausdruck übergeben werden. Sie können z. B. `HTTP.REQ.HEADER(”myVal1”)` in `HTTP.REQ.HEADER(”myVal2”)` oder `HTTP.REQ.HEADER(”myVal”)` in `HTTP.REQ.HEADER(”myVal”).AFTER_STR(<string>)` ändern. Wenn der Befehl set fehlschlägt, erstellen Sie eine HTTP-Callout.

Die HTTP-Callout-Konfiguration beinhaltet das Konfigurieren erweiterter Richtlinienausdrücke Weitere Informationen zum Konfigurieren erweiterter Richtlinienausdrücke finden Sie unter Konfigurieren des erweiterten Richtlinienausdrucks: Erste Schritte.

So konfigurieren Sie ein HTTP-Callout mit der Befehlszeilenschnittstelle

Führen Sie an der Eingabeaufforderung die folgenden Schritte aus:

Erstellen Sie ein HTTP-Callout.

```
add policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr>] [-port<
    port>] [-vServer <string>] [-returnType <returnType>] [-httpMethod (
    GET | POST )] [-hostExpr <expression>]  [-urlStemExpr <expression>]
    [-headers <name(value)> ...] [-parameters <name(value)> ...] [-
    bodyExpr <expression>] [-fullReqExpr <expression>] [-scheme ( http |
     https )] [-resultExpr <expression>] [-cacheForSecs <secs>] [-
    comment <string>]

<!--NeedCopy-->
```

Beispiel:

```
add policy httpCallout mycallout -vserver lbv1 -returnType num -
    httpMethod GET -hostExpr 'http.req.header("Host")'-urlStemExpr "http
    .req.url" -parameters Name("My Name") -headers Name("MyHeader")-
    resultExpr "http.res.body(10000).length"

<!--NeedCopy-->
```

Ändern Sie die HTTP-Callout-Konfiguration.

```
set policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr|\*>] [-
    port <port|\*>] [-vServer <string>] [-returnType <returnType>] [-
    httpMethod ( GET | POST )] [-hostExpr <string>] [-urlStemExpr <
    string>] [-headers <name(value)> ...] [-parameters <name(value)>
    ...] [-resultExpr <string>]

<!--NeedCopy-->
```

Beispiel:

```
> set policy httpCallout mycallout -vserver lbv1 -returnType num -
    httpMethod GET -hostExpr 'http.req.header("Host")'-urlStemExpr "http
    .req.url" -parameters Name("My Name") -headers Name("MyHeader") -
    resultExpr "http.res.body(10000).length"
```



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

Konfigurieren Sie die HTTP-Callout mit dem FullReqExpr-Parameter.

```
set policy httpCallout <name> [-vServer <string>] [-returnType <
    returnType>] [-fullReqExpr <string>] [-resultExpr <string>]
<!--NeedCopy-->
```

Beispiel:

```
> set policy httpCallout mycallout1 -vserver lbv1 -returnType num
    fullReqExpr q{
 "GET " + http.req.url + "HTTP/" + http.req.version.major + "." + http.
    req.version.minor.sub(1) + "r\nHost:10.101.10.10\r\nAccept: \*/\*\r
    \n\r\n" }


<!--NeedCopy-->
```

Überprüfen Sie die Konfigurationen des HTTP-Callout.

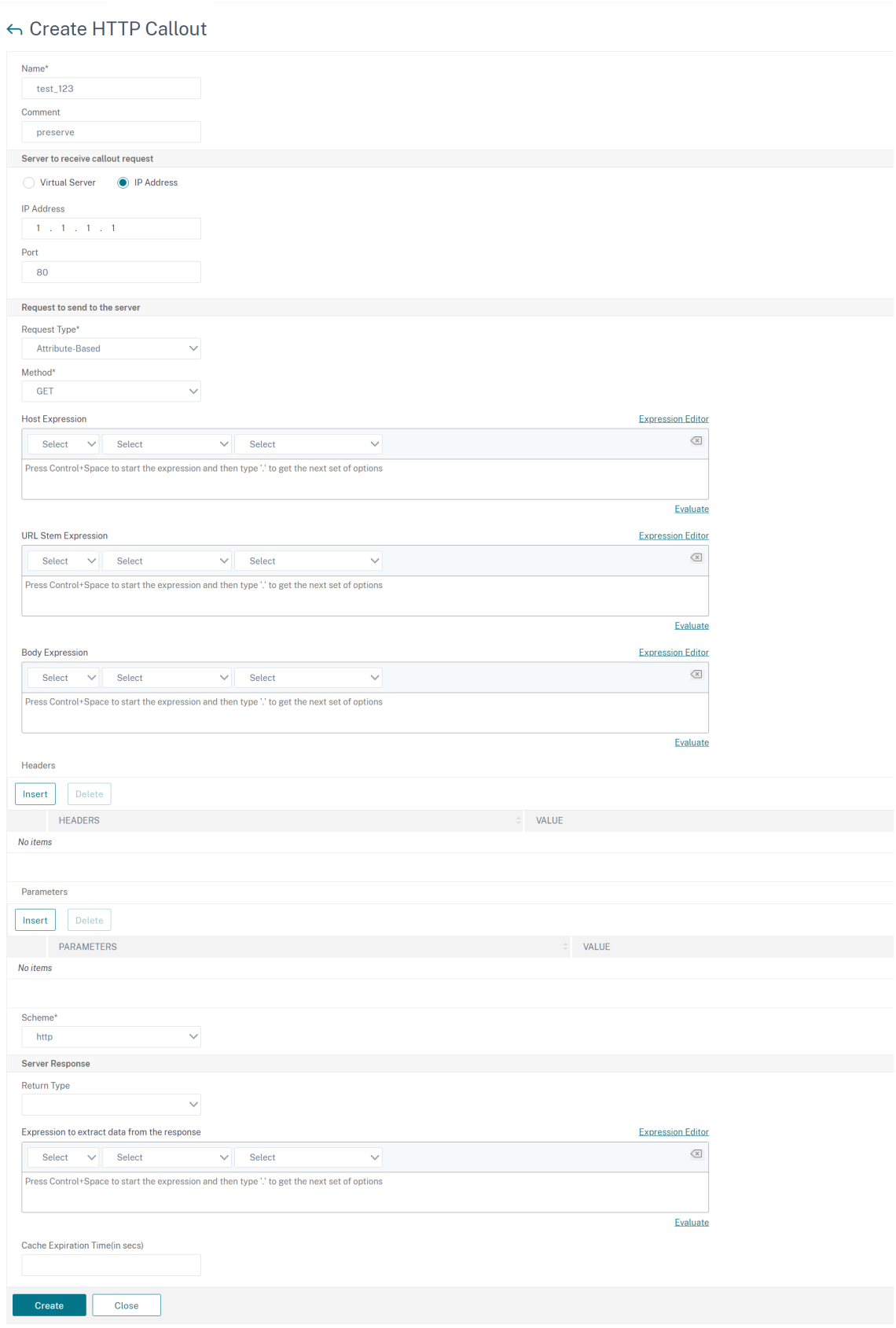
```
show policy httpCallout `<name>`

sh policy httpCallout mycallout1
> Name: mycallout1
>Vserver: lbv1 (UP)
Effective Vserver state: UP
Return type: TEXT
Scheme: HTTP
Full REQ expr: "GET " + http.req.url + "HTTP/" + http.req.version.major
    + "." + http.req.version.minor.sub(1)+ "r\nHost:10.101.10.10\r\
    nAccept: \*/\*\r\n\r\n"
Result expr: http.res.body(100)
Hits: 0
Undef Hits: 0
Done
>

<!--NeedCopy-->
```


So konfigurieren Sie ein HTTP-Callout mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **AppExpert** > **HTTP-Callouts**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Konfigurieren Sie im Dialogfeld **HTTP-Callout erstellen** die Parameter des HTTP-Callouts. Um eine Beschreibung des Parameters zu erhalten, bewegen Sie den Mauszeiger über das Kontrollkästchen.
4. Klicken Sie auf **Create** und dann auf **Close**.



Überprüfen der Konfiguration

October 5, 2021

Damit ein HTTP-Callout ordnungsgemäß funktioniert, müssen alle HTTP-Callout-Parameter und die Entitäten, die mit dem Callout verknüpft sind, korrekt konfiguriert werden. Obwohl die Citrix ADC Appliance die Gültigkeit der HTTP-Callout-Parameter nicht überprüft, gibt sie den Status der gebundenen Entitäten an, nämlich den Server oder virtuellen Server, an den das HTTP-Callout gesendet wird. In der folgenden Tabelle werden die Symbole aufgeführt und die Bedingungen beschrieben, unter denen die Symbole angezeigt werden.

Symbol	Gibt an, dass
	Der Status des Servers, der den HTTP-Callout-Agent hostet, oder der virtuelle Server zum Lastenausgleich, Content Switching oder Cache-Umleitung, an den das HTTP-Callout gesendet wird, ist UP.
	Der Status des Servers, der den HTTP-Callout-Agent hostet, oder der virtuelle Server zum Lastenausgleich, Content Switching oder Cache-Umleitung, an den die HTTP-Callout gesendet wird, ist OUT OF SERVICE.
	Der Status des Servers, der den HTTP-Callout-Agent hostet, oder der virtuelle Server zum Lastenausgleich, Content Switching oder Cache-Umleitung, an den die HTTP-Callout gesendet wird, ist DOWN.

Tabelle 1. Symbole, die die Zustände von Entitäten angeben, die an ein HTTP-Callout gebunden sind

Damit ein HTTP-Callout korrekt funktioniert, muss das Symbol immer grün sein. Wenn das Symbol nicht grün ist, überprüfen Sie den Status des Callout-Servers oder des virtuellen Servers, an den das HTTP-Callout gesendet wird. Wenn das HTTP-Callout nicht wie erwartet funktioniert, obwohl das Symbol grün ist, überprüfen Sie die für das Callout konfigurierten Parameter.

Sie können die Konfiguration auch überprüfen, indem Sie Testanforderungen senden, die der Richtlinie entsprechen, von der aus das HTTP-Callout aufgerufen wird, den Treffer-Zähler für die Richtlinie und das HTTP-Callout überprüfen und die Antworten überprüfen, die die Citrix ADC

Appliance an den Client sendet.

Hinweis: ein HTTP-Callout kann sich manchmal ein zweites Mal rekursiv aufrufen. In diesem Fall wird der Treffer-Zähler für jedes Callout, die von der Appliance generiert wird, um zwei Zählungen erhöht. Damit der Treffer-Zähler den richtigen Wert anzeigt, müssen Sie das HTTP-Callout so konfigurieren, dass sie sich nicht ein zweites Mal aufruft. Weitere Informationen darüber, wie Sie die Rekursion von HTTP-Callouts vermeiden können, finden Sie unter Vermeiden von HTTP-Callout-Rekursion.

So zeigen Sie den Treffer-Zähler für ein HTTP-Callout an

1. Navigieren Sie zu **AppExpert** > **HTTP-Callouts**.
2. Klicken Sie im Detailbereich auf das HTTP-Callout, für die Sie den Treffer-Zähler anzeigen möchten, und zeigen Sie dann die Treffer im Bereich **Details** an.

HTTP-Callout aufrufen

October 5, 2021

Nachdem Sie ein HTTP-Callout konfiguriert haben, rufen Sie das Callout auf, indem Sie den Ausdruck `SYS.HTTP_CALLOUT(<name>)` in eine Standardsyntax Richtlinienregel einschließen. In diesem Ausdruck ist `<name>` der Name der HTTP-Callout, die Sie aufrufen möchten.

Sie können Standard-Syntaxausdruck-Operatoren mit dem Calloutausdruck verwenden, um die Antwort zu verarbeiten und dann eine entsprechende Aktion auszuführen. Der Rückgabetyp der Antwort vom HTTP-Callout-Agent bestimmt die Menge der Operatoren, die Sie für die Antwort verwenden können. Wenn der Teil der Antwort, den Sie analysieren möchten, Text ist, können Sie die Antwort mit einem Textoperator analysieren. Beispielsweise können Sie den <string> Operator CONTAINS () verwenden, um zu überprüfen, ob der angegebene Teil der Antwort eine bestimmte Zeichenfolge enthält, wie im folgenden Beispiel:

```
SYS.HTTP_CALLOUT(mycallout).contains(”Good IP address”)
<!--NeedCopy-->
```

Wenn Sie den vorherigen Ausdruck in einer Responderrichtlinie verwenden, können Sie eine entsprechende Responderaktion konfigurieren.

Wenn der Teil der Antwort, den Sie auswerten möchten, eine Zahl ist, können Sie einen numerischen Operator wie GT (int) verwenden. Wenn die Antwort einen booleschen Wert enthält, können Sie einen booleschen Operator verwenden.

Hinweis: ein HTTP-Callout kann sich rekursiv aufrufen. HTTP-Callout-Rekursion kann vermieden werden, indem der HTTP-Callout-Ausdruck mit einem Standard-Syntaxausdruck kombiniert wird, der Rekursion verhindert. Informationen darüber, wie Sie die Rekursion von HTTP-Callouts vermeiden können, finden Sie unter Vermeiden von HTTP-Callout-Rekursion.

Sie können HTTP-Callouts auch kaskadieren, indem Sie Richtlinien konfigurieren, die jeweils ein Callout aufrufen, nachdem zuvor generierte Callouts ausgewertet wurden. Wenn in diesem Szenario nach dem Aufruf einer Callout eine Richtlinie die Citrix ADC allout analysiert, bevor die Callout an den Callout-Server gesendet wird, kann ein zweiter Satz von Richtlinien die Callout auswerten und zusätzliche Callouts aufrufen, die wiederum durch einen dritten Satz von Richtlinien ausgewertet werden können usw. Eine solche Implementierung wird im folgenden Beispiel beschrieben.

Zuerst können Sie ein HTTP-Callout namens MyCallout1 konfigurieren und dann eine Responder-Richtlinie Pol1 konfigurieren, um myCallout1 aufzurufen. Anschließend können Sie ein zweites HTTP-Callout , MyCallout2 und eine Responder-Richtlinie Pol2 konfigurieren. Sie konfigurieren Pol2, um myCallout1 auszuwerten und myCallout2 aufzurufen. Sie binden beide Responder-Richtlinien global.

Um HTTP-Callout-Rekursion zu vermeiden, wird myCallout1 mit einem eindeutigen benutzerdefinierten HTTP-Header namens Request1 konfiguriert. Pol1 ist so konfiguriert, dass HTTP-Callout-Rekursion vermieden wird, indem der Standard-Syntaxausdruck verwendet wird.

```
1 HTTP.REQ.HEADER(”Request1”).EQ(”Callout Request”).NOT.
2 <!--NeedCopy-->
```

Pol2 verwendet denselben Standard-Syntaxausdruck, schließt jedoch den Operator .NOT aus, sodass die Richtlinie MyCallout1 auswertet, wenn sie von der Citrix ADC Appliance analysiert wird. Beachten Sie, dass MyCallout2 seinen eigenen eindeutigen Header namens Request2 identifiziert und Pol2 einen Standard-Syntaxausdruck enthält, um zu verhindern, dass sich MyCallout2 rekursiv aufruft.

Beispiel:

```
1 > add policy httpCallout myCallout1
2
3 Done
4
5 > set policy httpCallout myCallout1 -IPAddress 10.102.3.95 -port 80 -
     returnType TEXT -hostExpr
6  ””10.102.3.95”” -urlStemExpr ””/cgi-bin/check_clnt_from_database.pl””
      -headers Request1
7 (”Callout Request”) -parameters cip(CLIENT.IP.SRC) -resultExpr ”HTTP.
     RES.BODY(100)”
```



```
8
9  Done
10
11 > add responder policy Pol1 ”HTTP.REQ.HEADER(”Request1”).EQ(”Callout
       Request”).NOT &&
12 SYS.HTTP_CALLOUT(myCallout1).CONTAINS(”IP Matched”)” RESET
13
14 Done
15
16 > bind responder global Pol1 100 END -type OVERRIDE
17
18 Done
19
20 > add policy httpCallout myCallout2
21
22 Done
23
24 > set policy httpCallout myCallout2 -IPAddress 10.102.3.96 -port 80 -
       returnType TEXT -hostExpr
25 ””10.102.3.96”” -urlStemExpr ””/cgi-bin/
       check_clnt_location_from_database.pl”” -headers Request2
26 (”Callout Request”) -parameters cip(CLIENT.IP.SRC) -resultExpr ”HTTP.
       RES.BODY(200)”
27
28  Done
29
30 > add responder policy Pol2 ”HTTP.REQ.HEADER(”Request2”).EQ(”Callout
       Request”).NOT &&
31  HTTP.REQ.HEADER(”Request1”).EQ(”Callout Request”) && SYS.HTTP_CALLOUT(
       myCallout2).CONTAINS
32 (”APAC”)” RESET
33
34  Done
35
36 > bind responder global Pol2 110 END -type OVERRIDE
37
38 Done
39 <!--NeedCopy-->
```

Vermeiden von HTTP-Callout-Rekursion

October 5, 2021

Obwohl die Citrix ADC Appliance nicht auf die Gültigkeit der HTTP-Callout-Anforderung überprüft, analysiert sie die Anforderung einmal, bevor sie die Anforderung an den HTTP-Callout-Agent sendet. Diese Analyse ermöglicht es der Appliance, die Callout-Anforderung wie jede andere eingehende Anforderung zu behandeln, wodurch Sie mehrere nützliche Citrix ADC Funktionen (z. B. das integrierte Caching) für die Bearbeitung der Callout-Anforderung konfigurieren können.

Während dieser Analyse kann die HTTP-Callout-Anforderung jedoch dieselbe Richtlinie auswählen und sich daher rekursiv aufrufen. Die Appliance erkennt den rekursiven Aufruf und löst eine undefinierte (UNDEF) -Bedingung aus. Der rekursive Aufruf führt jedoch dazu, dass die Richtlinien- und HTTP-Callout-Select-Leistungsindikatoren um jeweils zwei Zählungen erhöht werden, anstatt je eine Zählung.

Um zu verhindern, dass sich ein Callout selbst aufruft, müssen Sie mindestens ein eindeutiges Merkmal der HTTP-Callout-Anforderung identifizieren und dann alle Anforderungen mit diesem Merkmal von der Richtlinienregel ausschließen, die das Callout aufruft. Sie können dies tun, indem Sie einen weiteren Standard-Syntaxausdruck in die Richtlinienregel einfügen. Der Ausdruck muss dem `SYS.HTTP_CALLOUT(<name>)` Ausdruck vorangestellt sein, damit er ausgewertet wird, bevor der Calloutausdruck ausgewertet wird. Beispiel:

```
<Expression that prevents callout recursion> OR SYS.HTTP_CALLOUT(<name
   >)
<!--NeedCopy-->
```

Wenn Sie eine Richtlinienregel auf diese Weise konfigurieren, wenn die Appliance die Anforderung generiert und analysiert, wird die Verbundregel auf FALSE ausgewertet, das Callout wird nicht ein zweites Mal generiert, und die Auswahlindikatoren werden korrekt erhöht.

Eine Möglichkeit, mit der Sie einer HTTP-Callout-Anforderung ein eindeutiges Merkmal zuweisen können, besteht darin, einen eindeutigen benutzerdefinierten HTTP-Header einzubeziehen, wenn Sie das Callout konfigurieren. Es folgt ein Beispiel für ein HTTP-Callout namens MyCallout. Das Callout generiert eine HTTP-Anforderung, die prüft, ob die IP-Adresse eines Clients in einer Datenbank mit IP-Adressen auf der Sperrliste vorhanden ist. Das Callout enthält einen benutzerdefinierten Header namens Request, der auf den Wert Callout Request gesetzt ist. Eine global gebundene Responderrichtlinie, Pol1, ruft das HTTP-Callout auf, schließt jedoch alle Anforderungen aus, deren Request-Header auf diesen Wert gesetzt ist, und verhindert so einen zweiten Aufruf von MyCallout. Der Ausdruck, der einen zweiten Aufruf verhindert, ist HTTP.REQ.HEADER (Request) .EQ (Callout Request) .NOT.

Beispiel:

```
> add policy httpCallout myCallout
```



```
 Done

> set policy httpCallout myCallout -IPAddress 10.102.3.95 -port 80 -
    returnType TEXT -hostExpr ""10.102.3.95"" -urlStemExpr ""/cgi-bin/
    check_clnt_from_database.pl"" -headers Request("Callout Request") -
    parameters cip(CLIENT.IP.SRC) -resultExpr "HTTP.RES.BODY(100)"
Done

> add responder policy Pol1 "HTTP.REQ.HEADER("Request").EQ("Callout
    Request").NOT && SYS.HTTP_CALLOUT(myCallout).CONTAINS("IP Matched")"
     RESET
Done

> bind responder global Pol1 100 END -type OVERRIDE
Done
<!--NeedCopy-->
```

Hinweis:
Sie können einen Ausdruck auch konfigurieren, um zu überprüfen, ob die Anforderungs-URL den für das HTTP-Callout konfigurierten Stammausdruck enthält. Um die Lösung zu implementieren, stellen Sie sicher, dass der HTTP-Callout-Agent nur auf HTTP-Callouts und nicht auf andere Anforderungen reagieren kann, die über die Appliance geleitet werden. Wenn der HTTP-Callout-Agent eine Anwendung oder ein Webserver ist, der andere Clientanforderungen bedient, verhindert ein solcher Ausdruck, dass die Appliance diese Clientanforderungen verarbeitet. Verwenden Sie stattdessen einen eindeutigen benutzerdefinierten Header wie oben beschrieben.

HTTP-Callout-Antworten zwischenspeichern

October 5, 2021

Um die Leistung bei der Verwendung von Callouts zu verbessern, können Sie die integrierte Caching-Funktion verwenden, um Callout-Antworten zwischenzuspeichern. Die Antworten werden in einer integrierten Caching-Content-Gruppe namens CalloutContentGroup für eine bestimmte Zeit gespeichert.

Hinweis: Um Callout-Antworten zwischenzuspeichern, stellen Sie sicher, dass die integrierte Caching-Funktion aktiviert ist.

So legen Sie die Cache-Dauer mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set policy httpCallout <name> -cacheForSecs <secs>
```

Beispiel:

```
1 > set httpcallout httpcallout1 -cacheForSecs 120
2 <!--NeedCopy-->
```

So legen Sie die Cache-Dauer mit dem Konfigurationsdienstprogramm fest

1. Navigieren Sie zu **AppExpert > HTTP-Callouts**.
2. Wählen Sie im Detailbereich das HTTP-Callout aus, für die Sie die Cache-Dauer festlegen möchten, und klicken Sie auf **Öffnen**.
3. Geben Sie im Dialogfeld **HTTP-Callout konfigurieren** die **Cache-Ablaufzeit** an.
4. Stellen Sie sicher, dass Sie die richtige Zeitdauer eingegeben haben, und klicken Sie dann auf **OK**.

Anwendungsfall: Filtern von Clients über eine IP-Sperrliste

December 7, 2021

HTTP-Callouts können verwendet werden, um Anfragen von Clients zu blockieren, die vom Administrator auf die Sperrliste gesetzt werden. Die Liste der Clients kann eine öffentlich bekannte Sperrliste, eine Sperrliste, die Sie für Ihre Organisation pflegen, oder eine Kombination aus beiden sein.

Die Citrix ADC Appliance überprüft die IP-Adresse des Clients anhand der vorkonfigurierten Sperrliste und blockiert die Transaktion, wenn die IP-Adresse auf die Sperrliste gesetzt wurde. Wenn sich die IP-Adresse nicht in der Liste befindet, verarbeitet die Appliance die Transaktion.

Um diese Konfiguration zu implementieren, müssen Sie die folgenden Aufgaben ausführen:

1. Aktivieren Sie den Responder auf der Citrix ADC Appliance.
2. Erstellen Sie ein HTTP-Callout auf der Citrix ADC Appliance, und konfigurieren Sie sie mit Details zum externen Server und anderen erforderlichen Parametern.
3. Konfigurieren Sie eine Responder-Richtlinie, um die Antwort auf das HTTP-Callout zu analysieren und dann die Richtlinie global zu binden.
4. Erstellen Sie einen HTTP-Callout-Agent auf dem Remoteserver.

Responder aktivieren

Sie müssen den Responder aktivieren, bevor Sie ihn verwenden können.

So aktivieren Sie den Responder mit der GUI

1. Stellen Sie sicher, dass Sie die Responderlizenz installiert haben.
2. Erweitern Sie im Konfigurationsdienstprogramm AppExpert, klicken Sie mit der rechten Maustaste **auf Responder**, und klicken Sie dann auf **Responder-Funktion aktivieren** .

Erstellen eines HTTP-Callouts auf der Citrix ADC Appliance

Erstellen Sie ein HTTP-Callout, HTTP_Callout, mit den Parametereinstellungen in der folgenden Tabelle. Weitere Informationen zum Erstellen einer HTTP-Callout finden Sie unter Konfigurieren einer HTTP-Callout-PDF-Datei .

Konfigurieren einer Responder-Richtlinie und globales Binden

Nachdem Sie das HTTP-Callout konfiguriert haben, überprüfen Sie die Callout-Konfiguration, und konfigurieren Sie dann eine Responder-Richtlinie, um das Callout aufzurufen. Sie können zwar eine Responder-Richtlinie im Unterknoten
Richtlinien erstellen und sie dann global mithilfe des
Responder-Richtlinien-Managers binden, diese Demonstration verwendet den
Responder-Richtlinien-Manager, um die Responder-Richtlinie zu erstellen und die Richtlinie global zu binden.

So erstellen Sie eine Responder-Richtlinie und binden sie global von uns

1. Navigieren Sie zu **AppExpert** > **Responder**.
2. Klicken Sie im Detailbereich unter **Richtlinien-Manager**auf **Richtlinien-Manager**.
3. Klicken Sie im Dialogfeld **Responder Policy Manager** auf **Global überschreiben** .
4. Klicken Sie auf **Richtlinie einfügen**, und klicken Sie dann unter **Richtliniennam**auf **Neue Richtlinie**.
5. Gehen Sie im Dialogfeld **Responder-Richtlinie erstellen** folgendermaßen vor:
   a) Geben Sie unter Name den Wert **PolicyResponder1**ein.
   b) Wählen Sie in Aktion **RESET**aus.
   c) Wählen Sie unter **Undefiniertes Ergebnis Aktion**die Option **Globale Aktion mit nicht definiertem Ergebnis** aus.
   d) Geben Sie unter **Ausdruck**den folgenden Standard-Syntaxausdruck ein:


```
”HTTP.REQ.HEADER(”Request”).EQ(”Callout Request”).NOT && SYS.
   HTTP_CALLOUT(HTTP_Callout).CONTAINS(”IP Matched”)”
<!--NeedCopy-->
```

e) Klicken Sie auf **Erstellen**und dann auf **Schließen**.

6. Klicken Sie auf **Änderungen übernehmen**und dann auf **Schließen**.

Erstellen eines HTTP-Callout-Agents auf dem Remoteserver

Sie müssen nun einen HTTP-Callout-Agent auf dem Remote-Server erstellen, der Callout-Anforderungen von der Citrix ADC Appliance empfängt und entsprechend reagiert. Der HTTP-Callout-Agent ist ein Skript, das sich für jede Bereitstellung unterscheidet und unter Berücksichtigung der Serverspezifikationen geschrieben werden muss, z. B. des Datenbanktyps und der unterstützten Skriptsprache.

Es folgt ein Beispiel-Callout-Agent, der überprüft, ob die angegebene IP-Adresse Teil einer IP-Sperrliste ist. Der Agent wurde in der Perl-Skriptsprache geschrieben und verwendet eine MySQL-Datenbank.

Das folgende CGI-Skript prüft auf dem Callout-Server nach einer bestimmten IP-Adresse.

```
#!/usr/bin/perl -w
print ”Content-type: text/html\n\n”;
        use DBI();
        use CGI qw(:standard);
#Take the Client IP address from the request query
        my $ip_to_check = param('cip');
# Where a MYSQL database is running
        my $dsn = 'DBI:mysql:BAD_CLIENT:localhost';
# Database username to connect with
        my $db_user_name =  ‘dbuser’ ;
# Database password to connect with
        my $db_password = 'dbpassword';
        my ($id, $password);
# Connecting to the database
        my $dbh = DBI->connect($dsn, $db_user_name, $db_password);
        my $sth = $dbh->prepare(qq{
  select * from bad_clnt  }
 );
        $sth->execute();
        while (my ($ip_in_database) = $sth->fetchrow_array()) {

        chomp($ip_in_database);
```



```
# Check for IP match
        if ($ip_in_database eq $ip_to_check) {

              print "\n IP Matched\n";
                                                    $sth->finish();
                                                exit;
                 }

         }

        print "\n IP Failed\n";
        $sth->finish();
        exit;
<!--NeedCopy-->
```

Anwendungsfall: ESI-Unterstützung für dynamisches Abrufen und Aktualisieren von Inhalten

October 5, 2021

Edge Side Includes (ESI) ist eine Markupsprache für dynamische Webinhaltsassembly auf Kantenebene. Es hilft bei der Beschleunigung dynamischer webbasierter Anwendungen, indem eine einfache Markupsprache definiert wird, um zwischenspeicherbare und nicht zwischenspeicherbare Webseitenkomponenten zu beschreiben, die am Netzwerkrand aggregiert, zusammengebaut und bereitgestellt werden können. Mithilfe von HTTP-Callouts auf der Citrix ADC Appliance können Sie die ESI-Konstrukte durchlesen und Inhalte dynamisch aggregieren oder zusammenstellen.

Um diese Konfiguration zu implementieren, müssen Sie die folgenden Aufgaben ausführen:

1. Aktivieren Sie das Rewrite auf der Citrix ADC Appliance.
2. Erstellen Sie ein HTTP-Callout auf der Appliance, und konfigurieren Sie sie mit Details zum externen Server und anderen erforderlichen Parametern.
3. Konfigurieren Sie eine Rewrite-Aktion, um den ESI-Inhalt durch den Calloutantworttext zu ersetzen.
4. Konfigurieren Sie eine Umschreibungsrichtlinie, um die Bedingungen anzugeben, unter denen die Aktion ausgeführt wird, und binden Sie dann die Umschreibungsrichtlinie global.

Umschreiben aktivieren

Rewrite muss aktiviert sein, bevor es auf der Citrix ADC Appliance verwendet wird. Im folgenden Verfahren werden die Schritte zum Aktivieren des Umschreiben-Features beschrieben.

So aktivieren Sie das Rewrite mit der GUI

1. Stellen Sie sicher, dass Sie die Rewrite-Lizenz installiert haben.
2. Erweitern Sie im Konfigurationsprogramm AppExpert, und klicken Sie mit der rechten Maustaste auf Umschreiben, und klicken Sie dann auf Funktion Umschreiben aktivieren.

Erstellen eines HTTP-Callouts auf der Citrix ADC Appliance

Weitere Informationen zum Erstellen einer HTTP-Callout finden Sie unter Konfigurieren einer HTTP-Callout.
Weitere Informationen zu den Parameterwerten finden Sie unter Parameter und Werte für HTTP-Callout-2 pdf.

Konfigurieren der Aktion Umschreiben

Erstellen Sie eine Rewrite-Aktion, Action-Rewrite-1, um den ESI-Inhalt durch den Calloutantworttext zu ersetzen. Verwenden Sie die Parametereinstellungen in der folgenden Tabelle.

Tabelle 2. Parameter und Werte für Action-Rewrite-1

Parameter	Wert
Name	Action-Rewrite-1
Typ	Ersetzen
Ausdruck zur Auswahl der Zieltextreferenz	“HTTP.RES.BODY(500).AFTER_STR (\”<example>\”).BEFORE_STR (\”</example>\”)”
Zeichenfolgenausdruck für Ersetzungstext	“SYS.HTTP_CALLOUT(HTTP-Callout-2)”

So konfigurieren Sie die Umschreibungsaktion mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **AppExpert** > **Umschreiben** > **Aktionen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Rewrite-Aktion erstellen** unter Name die Zeichenfolge **Action-Rewrite-1** ein.
4. Wählen Sie unter Typ die Option **REPLACE**aus.
5. Geben Sie unter **Ausdruck**, um Zieltextreferenz auszuwählen, den folgenden Standard-Syntaxausdruck ein:


```
1 ”HTTP.RES.BODY(500).AFTER_STR(”<example>”).BEFORE_STR(”<example>”)
    ”
2 <!--NeedCopy-->
```

6. Geben Sie im Zeichenfolgenausdruck für Ersetzungstext den folgenden Zeichenfolgenausdruck ein:

```
1 ”SYS.HTTP_CALLOUT(HTTP-Callout-2)”
2 <!--NeedCopy-->
```

7. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Erstellen der Richtlinie Umschreiben und global binden

Erstellen Sie eine Richtlinie zum Umschreiben, Policy-Rewrite-1, mit den Parametereinstellungen in der folgenden Tabelle. Sie können eine Richtlinie zum Umschreiben im Unterknoten Richtlinien erstellen und sie dann global mit dem Richtlinien-Manager umschreiben binden. Alternativ können Sie den Richtlinien-Manager umschreiben verwenden, um beide Aufgaben gleichzeitig auszuführen. In dieser Demonstration wird der Richtlinien-Manager umschreiben verwendet, um beide Aufgaben auszuführen.

Tabelle 3. Parameter und Werte für Policy-Rewrite-1

Parameter	Wert
Name	Policy-Rewrite-1
Aktion	Action_Rewrite-1
Nicht definierte Ergebnisaktion	-Global undefined-result action-
Ausdruck	HTTP.REQ.HEADER (Name) .CONTAINS (Callout) .NOT

So konfigurieren Sie eine Umschreibungsrichtlinie und binden sie global mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **AppExpert** > **Neu schreiben**.
2. Klicken Sie im Detailbereich unter **Richtlinien-Manager**auf **Richtlinien-Manager neu schreiben**.

3. Klicken Sie im Dialogfeld **Richtlinien-Manager neu schreiben** auf **Global überschreiben** .
4. Klicken Sie auf **Richtlinie einfügen**, und klicken Sie dann in der Spalte **Richtlinienname** auf **Neue Richtlinie**.
5. Führen Sie im Dialogfeld **Rewrite-Richtlinie erstellen** die folgenden Schritte aus:
   1. Geben Sie unter Name Policy-Rewrite-1 ein.
      a) Wählen Sie unter Aktion die Option Aktions-Rewrite-1 aus.
      b) Wählen Sie unter Undefiniertes Ergebnis Aktiondie Option Globale Aktion mit nicht definiertem Ergebnis aus.
      c) Geben Sie unter Ausdruckden folgenden Standard-Syntaxausdruck ein:

```
1 ”HTTP.REQ.HEADER(”Name”).CONTAINS(”Callout”).NOT”
2 <!--NeedCopy-->
```

      a) Klicken Sie auf **Erstellen**und dann auf **Schließen**.
6. Klicken Sie auf **Änderungen übernehmen**und dann auf **Schließen**.

Anwendungsfall: Zugriffskontrolle und Authentifizierung

October 5, 2021

In Hochsicherheitszonen ist es zwingend erforderlich, den Benutzer extern zu authentifizieren, bevor Clients auf eine Ressource zugreifen. Auf der Citrix ADC Appliance können Sie HTTP-Callouts verwenden, um den Benutzer extern zu authentifizieren, indem Sie die angegebenen Anmeldeinformationen auswerten. In diesem Beispiel wird davon ausgegangen, dass der Client den Benutzernamen und das Kennwort über HTTP-Header in der Anforderung sendet. Die gleichen Informationen könnten jedoch von der URL oder dem HTTP-Körper abgerufen werden.

Um diese Konfiguration zu implementieren, müssen Sie die folgenden Aufgaben ausführen:

1. Aktivieren Sie die Responder-Funktion auf der Citrix ADC Appliance.
2. Erstellen Sie ein HTTP-Callout auf der Appliance, und konfigurieren Sie sie mit Details zum externen Server und anderen erforderlichen Parametern.
3. Konfigurieren Sie eine Responder-Richtlinie, um die Antwort zu analysieren und dann die Richtlinie global zu binden.
4. Erstellen Sie einen Callout-Agent auf dem Remoteserver.

Responder aktivieren

Die Responder-Funktion muss aktiviert sein, bevor sie auf der Citrix ADC Appliance verwendet wird.

So aktivieren Sie den Responder mit dem Konfigurationsdienstprogramm

1. Stellen Sie sicher, dass die Responderlizenz installiert ist.
2. Erweitern Sie im Konfigurationsdienstprogramm AppExpert, klicken Sie mit der rechten Maustaste auf Responder, und klicken Sie dann auf **Responder-Funktion aktivieren**.

Erstellen eines HTTP-Callouts auf der Citrix ADC Appliance

Erstellen Sie ein HTTP-Callout, HTTP-Callout-3, mit den Parametereinstellungen in der folgenden Tabelle. Weitere Informationen zum Erstellen einer HTTP-Callout finden Sie unter Konfigurieren einer HTTP-Callout.

Tabelle 1. Parameter und Werte für HTTP-Callout-3

Parameter	Wert	Name
Name	Policy-Responder-3	

Parameter

Wert

Name

HTTP-Callout-3

Server für den Empfang einer Callout-Anfrage:

IP-Adresse

10.103.9.95

Port

80

Anfrage zum Senden an den Server:

Methode

GET

Hostausdruck

10.102.3.95

URL-Stammausdruck

/cgi-bin/authenticate.pl

Kopfzeilen:

Name

Anforderung

Wertausdruck

Callout-Anfrage

Parameter:

Name

Benutzername

Wertausdruck

HTTP.REQ.HEADER (Benutzername) .VALUE (0)

Name

Kennwort

Wertausdruck

HTTP.REQ.HEADER (Kennwort) .VALUE (0)

Serverantwort:

Rückgabetyp

Text

Ausdruck zum Extrahieren von Daten aus der Antwort

HTTP.RES.BODY (100)

Erstellen einer Responder-Richtlinie zum Analysieren der Antwort

Erstellen Sie eine Responder-Richtlinie, Policy-Responder-3, die die Antwort vom Callout-Server überprüft und die Verbindung zurückgesetzt, wenn die Quell-IP-Adresse auf die Sperrliste gesetzt wurde. Erstellen Sie die Richtlinie mit den in der folgenden Tabelle angezeigten Parametereinstellungen. Sie können zwar eine Responder-Richtlinie im Unterknoten
Richtlinien erstellen und sie dann global mithilfe des
Responder-Richtlinien-Managers binden, diese Demonstration verwendet den
Responder-Richtlinien-Manager, um die Responder-Richtlinie zu erstellen und die Richtlinie global zu binden.

Tabelle 2. Parameter und Werte für Policy-Responder-3

Parameter	Wert
Name	Policy-Responder-3

Parameter	Wert
Aktion	RESET
Undefined-Result-Action	-Global undefined-result action-
Ausdruck	“HTTP.REQ.HEADER(\“Request\”).EQ(\“Callout Request\”).NOT && SYS.HTTP_CALLOUT(HTTP-Callout-3).CONTAINS(\“Authentication Failed\”)”

So erstellen Sie eine Responder-Richtlinie und binden sie global mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **AppExpert** > **Responder**.
2. Klicken Sie im Detailbereich unter **Richtlinien-Manager**auf **Responder Policy Manager**.
3. Klicken Sie im Dialogfeld **Responder Policy Manager** auf **Global überschreiben**.
4. Klicken Sie auf **Richtlinie einfügen**, und klicken Sie dann in der Spalte **Richtlinienname** auf **Neue Richtlinie**.
5. Gehen Sie im Dialogfeld **Responder-Richtlinie erstellen** folgendermaßen vor:
   a) Geben Sie unter Name den Wert Policy-Responder-3 ein.
   b) Wählen Sie unter Aktion die Option **ZURÜCKSETZEN**aus.
   c) Wählen Sie unter Aktion Nicht definiertes Ergebnis die Option Globale Aktion mit nicht definiertem Ergebnis aus.
   d) Geben Sie im Textfeld Ausdruck Folgendes ein:

```
1 ”HTTP.REQ.HEADER(”Request”).EQ(”Callout Request”).NOT && SYS.
     HTTP_CALLOUT(HTTP-Callout-3).CONTAINS(”Authentication Failed”)”
2 <!--NeedCopy-->
```

   a) Klicken Sie auf **Erstellen**und dann auf **Schließen**.
6. Klicken Sie auf **Änderungen übernehmen**und dann auf **Schließen**.

Erstellen eines HTTP-Callout-Agents auf dem Remoteserver

Sie müssen nun einen HTTP-Callout-Agent auf dem Remote-Callout-Server erstellen. Der HTTP-Callout-Agent empfängt Callout-Anforderungen von der Citrix ADC Appliance und reagiert entsprechend. Der Callout-Agent ist ein Skript, das für jede Bereitstellung unterschiedlich ist und

unter Berücksichtigung der Serverspezifikationen geschrieben werden muss, z. B. der Datenbanktyp und die unterstützte Skriptsprache.

Im Folgenden finden Sie Beispiel-Callout-Agent-Pseudo-Code, der überprüft, ob der angegebene Benutzername und das Kennwort gültig sind. Der Agent kann in jeder Programmiersprache Ihrer Wahl implementiert werden. Der Pseudocode soll nur als Richtschnur für die Entwicklung des Callout-Agenten verwendet werden. Sie können zusätzliche Funktionen in das Programm einbauen.

So überprüfen Sie den angegebenen Benutzernamen und das angegebene Kennwort mithilfe von Pseudo-Code

1. Akzeptieren Sie den in der Anfrage angegebenen Benutzernamen und das Kennwort und formatieren Sie diese entsprechend.
2. Stellen Sie eine Verbindung mit der Datenbank her, die alle gültigen Benutzernamen und Kennwörter enthält.
3. Überprüfen Sie die angegebenen Anmeldeinformationen für Ihre Datenbank.
4. Formatieren Sie die Antwort wie für das HTTP-Callout erforderlich.
5. Senden Sie die Antwort an die Citrix ADC Appliance.

Anwendungsfall: OWA-basierte Spam-Filterung

October 5, 2021

Spam-Filterung ist die Fähigkeit, E-Mails dynamisch zu blockieren, die nicht von einer bekannten oder vertrauenswürdigen Quelle stammen oder die unangemessene Inhalte haben. Spam-Filterung erfordert eine zugehörige Geschäftslogik, die angibt, dass eine bestimmte Art von Nachricht Spam ist. Wenn die Citrix ADC Appliance Outlook Web Access (OWA) -Nachrichten basierend auf dem HTTP-Protokoll verarbeitet, können HTTP-Callouts zum Filtern von Spam verwendet werden.

Sie können HTTP-Callouts verwenden, um einen beliebigen Teil der eingehenden Nachricht zu extrahieren und mit einem externen Callout-Server zu überprüfen, der mit Regeln konfiguriert wurde, um festzustellen, ob eine Nachricht legitim oder Spam ist. Im Falle von Spam-E-Mails benachrichtigt die Citrix ADC Appliance den Absender aus Sicherheitsgründen nicht, dass die E-Mail als Spam markiert ist.

Das folgende Beispiel führt eine sehr einfache Überprüfung auf verschiedene gelistete Schlüsselwörter im E-Mail-Betreff durch. Diese Prüfungen können in einer Produktionsumgebung komplexer sein.

Um diese Konfiguration zu implementieren, müssen Sie die folgenden Aufgaben ausführen:

1. Aktivieren Sie die Responder-Funktion auf der Citrix ADC Appliance.

2. Erstellen Sie ein HTTP-Callout auf der Citrix ADC Appliance, und konfigurieren Sie sie mit Details zum externen Server und anderen erforderlichen Parametern.
3. Erstellen Sie eine Responder-Richtlinie, um die Antwort zu analysieren und dann die Richtlinie global zu binden.
4. Erstellen Sie einen Callout-Agent auf dem Remoteserver.

Responder aktivieren

Die Responder-Funktion muss aktiviert sein, bevor sie auf der Citrix ADC Appliance verwendet werden kann.

So aktivieren Sie den Responder mit der GUI

1. Stellen Sie sicher, dass die Responderlizenz installiert ist.
2. Erweitern Sie im Konfigurationsdienstprogramm AppExpert, klicken Sie mit der rechten Maustaste **auf Responder**, und klicken Sie dann auf **Responder-Funktion aktivieren** .

Erstellen eines HTTP-Callouts auf der Citrix ADC Appliance

Erstellen Sie ein HTTP-Callout, HTTP-Callout-4, mit den Parametereinstellungen in der folgenden Tabelle. Weitere Informationen zum Erstellen einer HTTP-Callout finden Sie unter Konfigurieren einer HTTP-Callout.

Weitere Informationen finden Sie unter Parameter und Werte für HTTP-Callout-4 pdf.

Erstellen einer Responderaktion

Erstellen Sie eine Responder-Aktion, Action-Responder-4. Erstellen Sie die Aktion mit den Parametereinstellungen in der folgenden Tabelle.

Parameter	Wert
Name	Action-Responder-4
Typ	Antworten mit
Ziel	””HTTP/1.1 200 OK\r\nServer: Microsoft-IIS/6.0\r\nX-Powered-By: ASP.NET\r\nContent-Length: 0\r\nMS-WebStorage: 6.5.6944\r\nCache-Control: no-cache\r\n\r\n””

Tabelle 2. Parameter und Werte für Action-Responder-4

So erstellen Sie eine Responderaktion mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **AppExpert** > **Responder** > **Aktionen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld Responder-Aktion erstellen** unter Name den Eintrag **Action-Responder-4** ein.
4. Klicken Sie unter Typ auf **Antworten mit**.
5. Geben Sie unter Ziel Folgendes ein:

```
1 ""HTTP/1.1 200 OK\r\nServer: Microsoft-IIS/6.0\r\nX-Powered-By:
     ASP.NET\r\nContent-Length: 0\r\nMS-WebStorage: 6.5.6944\r\
     nCache-Control: no-cache\r\n\r\n""
2 <!--NeedCopy-->
```

6. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Erstellen einer Responder-Richtlinie zum Aufrufen des HTTP-Callouts

Erstellen Sie eine Responder-Richtlinie, Policy-Responder-4, die den Anforderungskörper überprüft und, wenn der Text das Wort
Betreff enthält, das HTTP-Callout aufrufen, um die E-Mail zu überprüfen. Erstellen Sie die Richtlinie mit den Parametereinstellungen in der folgenden Tabelle. Sie können zwar eine Responder-Richtlinie im Unterknoten
Richtlinien erstellen und sie dann global mithilfe des
Responderrichtlinien-Managers binden, diese Demonstration verwendet den
Responderrichtlinien-Manager, um die Responderrichtlinie zu erstellen und global zu binden.

Parameter	Wert
Name	Policy-Responder-4
Aktion	Action-Responder-4
Undefined-Result-Action	-Global undefined-result action-
Ausdruck	HTTP.REQ.BODY (1000) .CONTAINS (urn:schemas:httpmail:subject) && SYS.HTTP_CALLOUT (HTTP-Callout-4)

So erstellen Sie eine Responder-Richtlinie mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **AppExpert** > **Responder**.
2. Klicken Sie im Detailbereich unter **Richtlinien-Manager**auf **Responder-Richtlinien-Manager**.
3. Klicken Sie im Dialogfeld **Responder Policy Manager** auf **Global überschreiben**.
4. Klicken Sie auf **Richtlinie einfügen**, und klicken Sie dann in der Spalte **Richtlinienname** auf **Neue Richtlinie**.
5. Gehen Sie im Dialogfeld **Responder-Richtlinie erstellen** folgendermaßen vor:
   a) Geben Sie unter Name den Wert **Policy-Responder-4**ein.
   b) Klicken Sie unter Aktion auf **Aktions-Responder-4**.
   c) Klicken Sie in Aktion mit nicht definiertem Ergebnis auf **Globale Aktion mit nicht definiertem Ergebnis**.
   d) Geben Sie im Textfeld **Ausdruck** Folgendes ein:

```
1 ”HTTP.REQ.BODY(1000).CONTAINS(”urn:schemas:httpmail:subject”)
     && SYS.HTTP_CALLOUT(HTTP-Callout-4)”
2 <!--NeedCopy-->
```

   e) Klicken Sie auf **Erstellen**und dann auf **Schließen**.
6. Klicken Sie auf **Änderungen übernehmen**und dann auf **Schließen**.

Erstellen eines HTTP-Callout-Agents auf dem Remoteserver

Sie müssen nun einen HTTP-Callout-Agent auf dem Remote-Server erstellen. Der HTTP-Callout-Agent empfängt Callout-Anforderungen von der Citrix ADC Appliance und reagiert entsprechend. Der Callout-Agent ist ein Skript, das für jede Bereitstellung unterschiedlich ist und unter Berücksichtigung der Serverspezifikationen geschrieben werden muss, z. B. der Datenbanktyp und die unterstützte Skriptsprache.

Der folgende Pseudo-Code enthält Anweisungen zum Erstellen eines Callout-Agenten, der eine Liste von Wörtern prüft, die allgemein als Spam-Mails verstanden werden. Der Agent kann in jeder Programmiersprache Ihrer Wahl implementiert werden. Der Pseudocode soll nur als Richtschnur für die Entwicklung des Callout-Agenten verwendet werden. Sie können zusätzliche Funktionen in das Programm einbauen.

So identifizieren Sie Spam-E-Mails mithilfe von Pseudo-Code

1. Akzeptieren Sie den von der Citrix ADC Appliance bereitgestellten E-Mail-Betreff.
2. Stellen Sie eine Verbindung mit der Datenbank her, die alle Begriffe enthält, gegen die der E-Mail-Betreff überprüft wird.
3. Überprüfen Sie die Wörter im E-Mail-Betreff gegen die Spam-Wortliste.

4. Formatieren Sie die Antwort wie für das HTTP-Callout erforderlich.
5. Senden Sie die Antwort an die Citrix ADC Appliance.

Anwendungsfall: Dynamic Content Switching

October 5, 2021

Dieser Anwendungsfall ermöglicht ein dynamisches Content Switching über ein HTTP-Callout, um den Namen des virtuellen Lastenausgleichsservers zu erhalten, an den die Anforderung weitergeleitet wird.

1. Fügen Sie einen virtuellen Content Switching-Server hinzu.

```
add cs vserver cs_vserver1 HTTP 10.102.29.196 80
<!--NeedCopy-->
```

2. Erstellen Sie ein HTTP-Callout.

```
add policy httpCallout http_callout1
<!--NeedCopy-->
```

3. Konfigurieren Sie das HTTP-Callout so, dass sie mit dem Namen des virtuellen Lastausgleichsservers aus einer Anforderung reagiert, die die Client-IP-Adresse im HTTP-Header X-CLIENT-IP enthält.

```
> set policy httpCallout http_callout1 -IPAddress 10.217.14.23 -
   port 80 -returnType TEXT -hostExpr ””www.get-lbvip.com”” -
   urlStemExpr ””/index.html”” -headers X-CLIENT-IP(CLIENT.IP.SRC)
    -resultExpr ”HTTP.RES.BODY(1000).AFTER_STR(”<lbvip>”).
   BEFORE_STR(”<lbvip”)”
<!--NeedCopy-->
```

4. Konfigurieren Sie die Content Switching-Aktion, um die Calloutantwort abzurufen.

```
add cs action cs_action1 -targetVserverExpr 'SYS.HTTP_CALLOUT(
   http_callout1)'
<!--NeedCopy-->
```


> Hinweis:
>
> Sie müssen einen virtuellen Lastausgleichsserver an den virtuellen Content Switching-Server binden, um Folgendes zu berücksichtigen:

- Die Nichtverfügbarkeit des virtuellen Lastausgleichsservers, auf den das Callout aufgelöst wird.
- Eine UNDEF-Bedingung, die sich aus dem Ausführen des Callouts ergibt.

```
> bind cs vserver cs_vserver1 -lbvserver default_lbvip
<!--NeedCopy-->
```

5. Konfigurieren Sie die Content Switching-Richtlinie.

```
add cs policy cs_policy1 -rule true -action cs_action1
<!--NeedCopy-->
```

6. Binden der Content Switching-Richtlinie an den virtuellen Content Switching-Server.

```
bind cs vserver cs_vserver1 -policyName cs_policy1 -priority 10
<!--NeedCopy-->
```

Mustersätze und Datensätze

January 25, 2022

Richtlinienausdrücke für Zeichenfolgenabgleichsoperationen bei einer großen Menge von Zeichenfolgenmustern werden tendenziell lang und komplex. Ressourcen, die durch die Auswertung solcher komplexen Ausdrücke verbraucht werden, sind in Bezug auf Verarbeitungszyklen, Speicher und Konfigurationsgröße von Bedeutung. Mithilfe des Musterabgleichs können Sie einfachere, weniger ressourcenintensive Ausdrücke erstellen.

Abhängig von der Art der Muster, die Sie abgleichen möchten, können Sie eine der folgenden Funktionen verwenden, um den Musterabgleich zu implementieren:

- Ein Mustersatz ist ein Array indizierter Muster, die für den Zeichenfolgenabgleich bei der Auswertung der Standard-Syntaxrichtlinie verwendet werden. Beispiel für einen Mustersatz: Bildtypen {svg, bmp, PNG, GIF, tiff, jpg}.

- Ein Datensatz ist eine spezielle Form von Mustersatz. Es ist ein Array von Mustern der Typen Zahl (Integer), IPv4-Adresse oder IPv6-Adresse.

Der Unterschied zwischen `patset` und `dataset` besteht darin, dass wir in `dataset` die Randbedingung vergleichen. Wenn die Eingabezeichenfolge beispielsweise 1.1.1.11 lautet und davon ausgeht, dass das 1.1.1.1-Muster an `patset` und ein Datensatz vom Typ IPv4 gebunden ist, wird `patset` und der Datensatz konfiguriert, um zu überprüfen, ob die IP-Adresse in der Anforderung vorhanden ist. `patset` gibt nach der Auswertung zurück, dass 1.1.1.1 in der Eingabe vorhanden ist, die Auswertung `dataset` jedoch falsch ist. Dies liegt an einem Boundary-Check-in, bei dem die IP-Adresse nicht Teil einer anderen IP-Adresse war. Das bedeutet, dass es nach dem gebundenen Muster keine ganze Zahl geben darf.

Oft können Sie entweder Mustersätze oder Datensätze verwenden. In Fällen, in denen Sie jedoch bestimmte Übereinstimmungen für numerische Daten oder IPv4- und IPv6-Adressen wünschen, müssen Sie Datensätze verwenden.

> **Hinweis:**
>
> Mustersätze und Datensätze können nur in Standard-Syntaxrichtlinien verwendet werden.

Um Mustersätze oder Datensätze zu verwenden, erstellen Sie zuerst den Mustersatz oder den Datensatz und binden Sie Muster an ihn. Wenn Sie dann eine Richtlinie zum Vergleichen einer Zeichenfolge in einem Paket konfigurieren, verwenden Sie einen geeigneten Operator und übergeben Sie den Namen des Mustersatzes oder Datensatzes als Argument.

Funktionsweise von Zeichenfolgenabgleich mit Mustersätzen und Datensätzen

October 5, 2021

Ein Mustersatz oder ein Datensatz enthält einen Satz von Mustern, und jedem Muster wird ein eindeutiger Index zugewiesen. Wenn eine Richtlinie auf ein Paket angewendet wird, identifiziert ein Ausdruck eine Zeichenfolge, die ausgewertet werden soll, und der Operator vergleicht die Zeichenfolge mit den Mustern, die im Mustersatz oder im Datensatz definiert sind, bis eine Übereinstimmung gefunden oder alle Muster verglichen wurden. Anschließend gibt der Operator je nach Funktion entweder einen booleschen Wert zurück, der angibt, ob ein übereinstimmendes Muster gefunden wurde oder nicht, oder den Index des Musters, das mit der Zeichenfolge übereinstimmt.

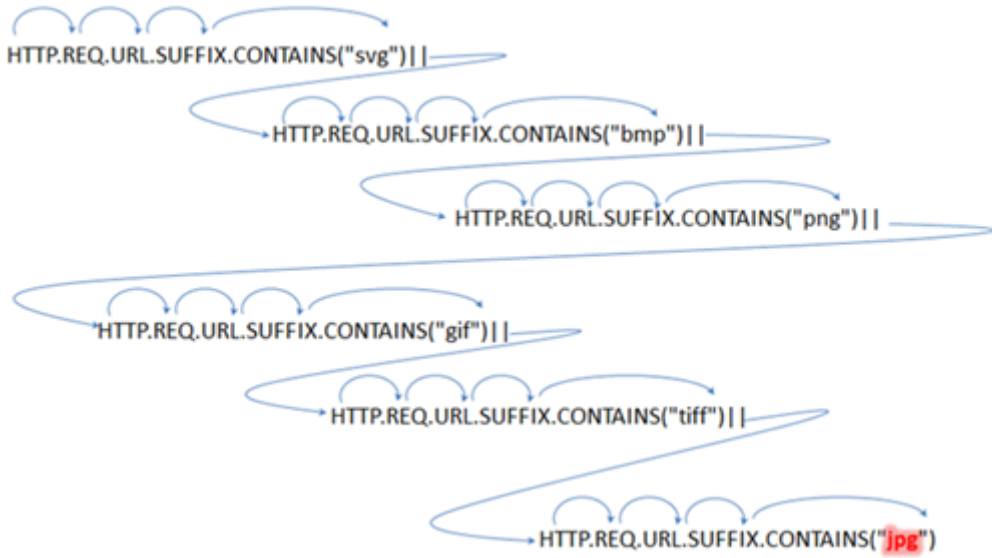
Hinweis: In diesem Thema wird die Arbeit eines Mustersatzes erläutert. Datensätze funktionieren auf die gleiche Weise. Der einzige Unterschied zwischen Mustersätzen und Datensätzen ist die Art der Muster, die in der Menge definiert sind.

Betrachten Sie den folgenden Anwendungsfall, um zu verstehen, wie Muster für String-Matching verwendet werden können.

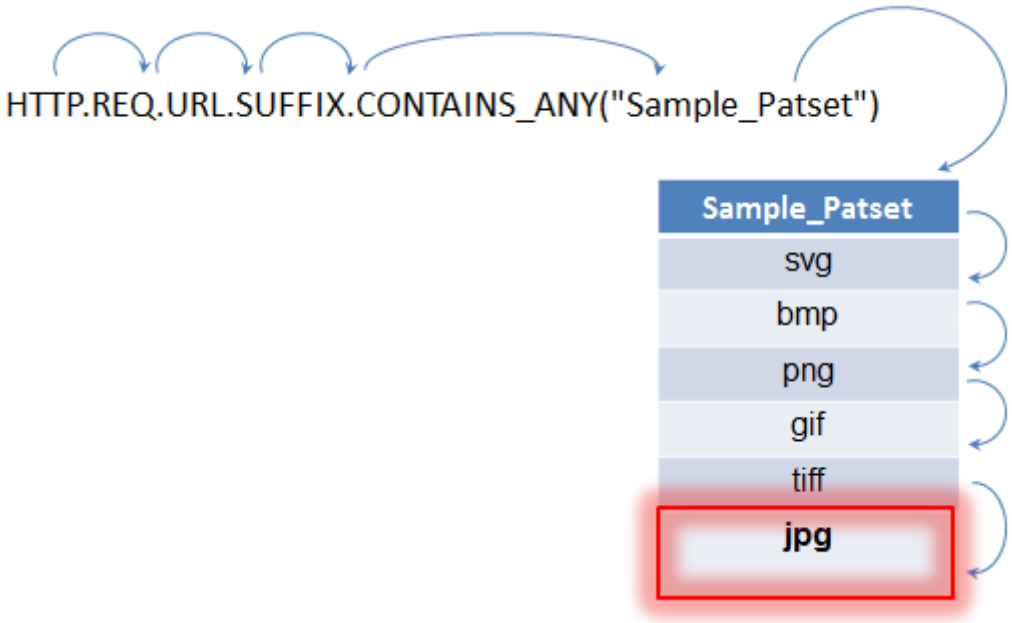
Sie möchten ermitteln, ob das URL-Suffix (Zieltext) eine der Bilddateierweiterungen enthält. Ohne Mustersätze zu verwenden, müssten Sie einen komplexen Ausdruck wie folgt definieren:

```
1 HTTP.REQ.URL.SUFFIX.CONTAINS(”svg”) ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS(”
     bmp”) ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS(”png”) ¦¦
2 HTTP.REQ.URL.SUFFIX.CONTAINS(”gif”) ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS(”
     tiff”) ¦¦ HTTP.REQ.URL.SUFFIX.CONTAINS(”jpg”)
3 <!--NeedCopy-->
```

Wenn die URL das Suffix jpg mit dem obigen zusammengesetzten Ausdruck aufweist, muss die Citrix ADC Appliance den gesamten zusammengesetzten Ausdruck sequenziell von einem Unterausdruck zum nächsten durchlaufen, um festzustellen, dass sich die Anforderung auf ein jpg-Bild bezieht. Die folgende Abbildung zeigt die Schritte im Prozess.



Wenn ein zusammengesetzter Ausdruck Hunderte von Unterausdrücken enthält, ist der obige Prozess ressourcenintensiv. Eine bessere Alternative ist ein Ausdruck, der einen Mustersatz aufruft, wie in der folgenden Abbildung gezeigt.



Während der Richtlinienauswertung, wie oben dargestellt, vergleicht der Operator (CONTAINS_ANY) die in der Anforderung identifizierte Zeichenfolge mit den Mustern, die im Mustersatz definiert sind, bis eine Übereinstimmung gefunden wird. Mit dem Sample_Patset-Ausdruck werden die mehrfachen Iterationen durch sechs Unterausdrücke auf nur einen reduziert.

Da keine Notwendigkeit besteht, zusammengesetzte Ausdrücke zu konfigurieren, die String-Matching mit mehreren ODER Operationen durchführen, vereinfachen Mustersätze oder Datensätze die Konfiguration und beschleunigen die Verarbeitung von Anfragen und Antworten.

Konfigurieren eines Mustersatzes

October 5, 2021

Um einen Mustersatz zu konfigurieren, müssen Sie die Zeichenfolgen angeben, die als Muster dienen sollen. Sie können jedem dieser Muster manuell einen eindeutigen Indexwert zuweisen, oder Sie können zulassen, dass die Indexwerte automatisch zugewiesen werden.

Hinweis: Bei Mustersätzen wird zwischen Groß- und Kleinschreibung unterschieden (es sei denn, Sie geben den Ausdruck an, der Groß-/Kleinschreibung ignoriert). Daher entspricht das Zeichenfolgenmuster product1 beispielsweise nicht dem Zeichenfolgenmuster Product1.

Punkte, die Sie sich über Indexwerte erinnern sollten:

- Sie können denselben Indexwert nicht an mehr als ein Muster binden.
- Ein automatisch zugewiesener Indexwert ist eine Zahl größer als der höchste Indexwert der vorhandenen Muster innerhalb des Mustersatzes. Wenn beispielsweise der höchste

Indexwert bestehender Muster in einer Mustergruppe 104 ist, beträgt der nächste automatisch zugewiesene Indexwert 105.

- Wenn Sie keinen Index für das erste Muster angeben, wird diesem Muster automatisch der Indexwert 1 zugewiesen.
- Indexwerte werden nicht automatisch neu generiert, wenn ein oder mehrere Muster gelöscht oder geändert werden. Wenn die Menge beispielsweise fünf Muster enthält, mit Indizes von 1 bis 5, und wenn das Muster mit dem Index 3 gelöscht wird, werden die anderen Indexwerte im Mustersatz nicht automatisch regeneriert, um Werte von 1 bis 4 zu erzeugen.
- Der maximale Indexwert, der einem Muster zugewiesen werden kann, ist 4294967290. Wenn dieser Wert bereits einem Muster in der Menge zugewiesen ist, müssen Sie neu hinzugefügten Mustern Indexwerte manuell zuweisen. Ein nicht verwendeter Indexwert, der niedriger als ein aktuell verwendeter Wert ist, kann nicht automatisch zugewiesen werden.

So konfigurieren Sie einen Mustersatz mit der Befehlszeilenschnittstelle

Führen Sie an der Eingabeaufforderung die folgenden Schritte aus:

1. Erstellen Sie einen Mustersatz.

```
add policy patset <name>
```

Beispiel:

```
add policy patset samplepatset
```

1. Binden Sie Muster an den Mustersatz.

```
bind policy patset <name> <string> [-index <positive_integer>][-charset
 ( ASCII | UTF_8 )] [-comment <string>]
```

Beispiel:

```
bind policy patset samplepatset product1 -index 1 -comment short description
 about the pattern bound to the pattern set
```

Hinweis: Wiederholen Sie diesen Schritt für alle Muster, die Sie an den Mustersatz binden möchten.

1. Überprüfen Sie die Konfiguration.

```
show policy patset <name>
```

So konfigurieren Sie einen Mustersatz mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **AppExpert** > **Mustersätze** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**, um das Dialogfeld **Mustersatz erstellen** zu öffnen.
3. Geben Sie im Textfeld Name einen Namen für das Muster an.

4. Geben Sie unter Muster angeben das erste Muster ein, und geben Sie optional Werte für die folgenden Parameter an:
   - Rückwärtsstriche als Escapezeichen behandeln — Aktivieren Sie dieses Kontrollkästchen, um anzugeben, dass alle umgekehrten Schrägstriche, die Sie möglicherweise in das Muster aufnehmen, als Escapezeichen behandelt werden sollen.
   - Index — Ein vom Benutzer zugewiesener Indexwert von 1 bis 4294967290.
5. Stellen Sie sicher, dass Sie die richtigen Zeichen eingegeben haben, und klicken Sie dann auf **Hinzufügen**.
6. Wiederholen Sie die Schritte 4 und 5, um weitere Muster hinzuzufügen, und klicken Sie dann auf **Erstellen**.

Konfigurieren von dateibasierten Mustersätzen

Die Citrix ADC Appliance unterstützt dateibasierte Pattern-Sets.

So konfigurieren Sie dateibasierte Pattern-Sets mit CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- Importieren Sie eine neue Pattern-Set-Datei in die Citrix ADC Appliance.

```
import policy patsetfile <src> <name> -delimiter <char> -charset
   <ASCII | UTF_8>
<!--NeedCopy-->
```

Beispiel:

```
import policy patsetfile local:test.csv clientids_list -
   delimiter ,
<!--NeedCopy-->
```

Sie können eine Datei von einem lokalen Gerät, HTTP-Server oder FTP-Server importieren. Um die Datei von Ihrem lokalen Gerät hinzuzufügen, muss die Datei am `/var/tmp` Speicherort verfügbar sein.

- Aktualisieren Sie eine vorhandene Pattern-Set-Datei auf der Citrix ADC Appliance.

```
update policy -patsetfile <patset filename>
<!--NeedCopy-->
```


Beispiel:

```
update policy -patsetfile clientids_list
<!--NeedCopy-->
```

- Fügen Sie der Paket-Engine eine Pattern-Set-Datei hinzu.

```
add policy -patsetfile <patset filename>
<!--NeedCopy-->
```

Beispiel:

```
add policy -patsetfile clientids_list
<!--NeedCopy-->
```

- Binden Sie Muster an den Mustersatz.

```
add policy patset <patset name> -patsetfile <patset filename>
<!--NeedCopy-->
```

Beispiel:

```
add policy patset clientid_patset -patsetfile clientids_list
<!--NeedCopy-->
```

- Überprüfen Sie die Konfiguration.

```
show policy patsetfile clientids_list

Name: clientids_list
Patset Name: clientid_patset
Number of Imported Patterns: 8
Number of Bound Patterns: 8
(All the patterns bound successfully)

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


So konfigurieren Sie dateibasierte Pattern-Sets mit GUI

1. Navigieren Sie zu **AppExpert-> Pattern-Set-Dateien**.
2. Klicken Sie im Bereich **Importiert** auf **Importieren**.
3. Wählen Sie auf der Seite " **Richtlinien-Patset-Datei konfigurieren** " die Datei aus, die Sie importieren möchten, und klicken Sie auf **OK**.
4. Wählen Sie die importierte Datei aus und klicken Sie auf **Hinzufügen**.
5. Geben Sie auf der Seite " **Policy-Patset-Datei erstellen** " die Details ein, und klicken Sie auf **Erstellen**, um ein Richtlinienmusterset hinzuzufügen.

Konfigurieren eines Datensatzes

October 5, 2021

Um einen Datensatz zu konfigurieren, müssen Sie die Zeichenfolgen angeben, die Server als Muster verwenden, einen Typ (Nummer, IPv4-Adresse oder IPv6-Adresse) zuweisen und den Dataset-Bereich konfigurieren. Sie können dem Muster manuell einen eindeutigen Indexwert zuweisen, oder Sie können zulassen, dass die Indexwerte automatisch zugewiesen werden. Dataset ist nicht mit HTTP oder einem 7-Layer-Protokoll verbunden. Es funktioniert nur auf Text oder String. Es gibt verschiedene Datasetypen wie NUM, ULONG, IPv4, IPv6, MAC, DOUBLE. Sie können einen Typ auswählen und den Dataset-Bereich basierend auf dem angegebenen Typ definieren.

> **Hinweis:**
>
> Bei Richtliniendatensätzen wird zwischen Groß- und Kleinschreibung unterschieden (es sei denn, Sie geben an, die Groß-/Kleinschreibung zu ignorieren). Daher ist beispielsweise die MAC-Adresse ff:ff:ff:ff:ff:ff nicht identisch mit der MAC-Adresse FF:FF:FF:FF:FF:FF.

Die Regeln, die für Indexwerte von Datensätzen angewendet werden, sind ähnlich wie Mustersätze. Informationen zu Indexwerten finden Sie unter Konfigurieren eines Mustersatzes.

So konfigurieren Sie einen Datensatz

Sie müssen die folgenden Schritte ausführen, um einen Datensatz zu konfigurieren:

1. Hinzufügen eines Richtliniendatensets
2. Binden des Musters an ein Richtliniendatenset
3. Hinzufügen eines Richtlinienausdrucks
4. Überprüfen der Richtlinienkonfiguration

Hinzufügen eines Richtliniendatensets

Führen Sie an der Eingabeaufforderung die folgenden Schritte aus:

```
add policy dataset <name> <type>
```

Beispiel:

```
add policy dataset ds1 ipv4 -comment numbers
```

Binden eines Musters an den Datensatz

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind policy dataset <name> <value> [-index <positive_integer>] [-endRange <
string>] [-comment <string>]
```

Beispiel:

```
bind policy dataset ds1 1.1.1.1 -endRange 1.1.1.10 -comment short description
 about the pattern bound to the data set
```

> **Hinweis:**
>
> Sie müssen diesen Schritt für alle Muster wiederholen, die Sie an den Datensatz binden möchten. Sie können nur bis zu 5000 Muster an ein Dataset binden.
>
> Ein Dataset-Bereich darf sich nicht mit anderen Bereichen überschneiden, die an ein Dataset gebunden sind, und darf keine einzelnen Werte enthalten, die an das Dataset gebunden sind. Wenn Sie ein Dataset mit einem überlappenden Bereich binden, führt dies zu einem Fehler.

Beispiel:

```
1 add policy dataset ip_set ipv4
2  Done
3 bind policy dataset ip_set 2.2.2.25
4  Done
5 bind policy dataset ip_set 2.2.2.20 -endRange 2.2.2.30
6 ERROR: The range overlaps an existing range or includes a value bound
     to the dataset.
7 <!--NeedCopy-->
```

Ein Wert wird als im Dataset betrachtet, wenn er entweder einem einzelnen Wert entspricht, der an den Datensatz gebunden ist, oder zwischen dem niedrigeren und dem oberen Wert (niedrigerer Wert <= Wert && Wert <- oberer Wert) für einen Bereich liegt, der an den Datensatz gebunden ist.

Verwenden von Richtlinienausdrücken in einem Richtliniendatensatz

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add policy expression exp1 http.req.body(100).contains_any(”ds1”)
```

Wo,
Der Ausdruck prüft, ob Muster (oder Muster innerhalb des Bereichs) an die Datenmenge ds1 gebunden ist, in den ersten 100 Bytes des HTTP-Anforderungskörpers vorhanden ist.

Überprüfen der Dataset-Konfiguration

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show policy dataset ds1
> show policy dataset ds1
```

Beispiel:

```
1         Dataset:        ds1
2          Type:   IPV4
3 1)       Bound Dataset Range from: 1.1.1.1       through: 1.1.1.10
            Index:  1
4 <!--NeedCopy-->
```

So konfigurieren Sie einen Datensatz mit dem Konfigurationsdienstprogramm

Führen Sie die unten angegebenen Schritte aus, um ein Richtliniendataset zu konfigurieren:

1. Navigieren Sie zu **AppExpert > Datensätze**.
2. Klicken Sie im Detailbereich unter Datensätze auf **Hinzufügen**.
3. Legen Sie auf der Seite **Datensatz konfigurieren** die folgenden Parameter fest.
   a) Name. Name des Richtliniendatensets.
   b) Geben Sie ein. Typ des Wertes, der an das Dataset gebunden werden soll.

   Konfigurieren des Datensets
4. Klicken Sie auf **Einfügen**, um den Dataset-Wert eines bestimmten Typs zu binden.
   a) Wert. Wert des angegebenen Typs, der dem Dataset zugeordnet ist.
   b) Index. Der Indexwert des Datasets.
   c) End-Bereich. Der Datensatzeintrag. Dies ist ein Bereich <value> zu <end_range>.
   d) Kommentare. Eine kurze Beschreibung über den Datensatz.

Dataset-Bindung

5. Klicken Sie auf **Einfügen** und **Schließen**.
6. Geben Sie Kommentare ein.
7. Klicken Sie auf **Erstellen** und **Schließen**.

Verwenden von Mustersätzen und Datensätzen

October 5, 2021

Standard-Syntaxrichtlinienausdrücke, die Mustersätze oder Datensätze als Argument verwenden, können zum Ausführen von Zeichenfolgenabgleichsoperationen verwendet werden.

Die Verwendung ist wie folgt:

```
<text>.<operator>(”<name>”)
<!--NeedCopy-->
```

Wobei:

- <text> ist der Ausdruck, der eine Zeichenfolge in einem Paket identifiziert. Beispiel: HTTP.REQ.HEADER(“Host”).
- <operator> ist einer der in der Tabelle Pattern Set Types beschriebenen Operatoren pdf.

Informationen zur Verwendung von Beispielen finden Sie unter Beispielverwendung.

Beispiel für Verwendung

October 5, 2021

Um die Verwendung von Mustersätzen in Ausdrücken zu verstehen, betrachten Sie das Beispiel eines Mustersatzes namens imagetypes.

Muster	Indexwert
svg	1
bmp	2
png	3

Muster	Indexwert
gif	4
tiff	5
jpg	6

Tabelle 1. Mustersatz Bildtypen

Beispiel 1: Bestimmen Sie, ob das Suffix einer HTTP-Anforderung eine der Dateierweiterungen ist, die im Mustersatz imagetypes definiert sind.

- **Ausdruck.** HTTP.REQ.URL.SUFFIX.EQUALS_ANY(“imagetypes”)
- **Beispiel-URL.** `http://www.example.com/homepageicon.jpg`
- **Ergebnis.** TRUE

Beispiel 2: Bestimmen Sie, ob das Suffix einer HTTP-Anforderung eine der Dateierweiterungen ist, die im Mustersatz imagetypes definiert sind, und geben Sie den Index dieses Musters zurück.

- **Ausdruck.** HTTP.REQ.URL.SUFFIX.EQUALS_INDEX(“imagetypes”)
- **Beispiel-URL.** `http://www.example.com/mylogo.png`
- **Ergebnis.** 4 (Der Indexwert des Musters gif.)

Beispiel 3: Verwenden Sie den Indexwert eines Musters, um zu bestimmen, ob sich das URL-Suffix innerhalb eines angegebenen Indexwertebereichs befindet.

- **Ausdruck.** HTTP.REQ.URL.SUFFIX.EQUALS_INDEX(“imagetypes”).GE(3) && HTTP.REQ.URL.SUFFIX.EQUALS_
- **Beispiel-URL.** `http://www.example.com/mylogo.png`
- **Ergebnis.** TRUE (Der Indexwert von GIF-Dateitypen ist 4.)

Beispiel 4: Implementieren Sie einen Satz von Richtlinien für Dateierweiterungen bmp, jpg und png und einen anderen Satz von Richtlinien für GIF-, TIFF- und SVG-Dateien.

Ein Ausdruck, der den Index eines übereinstimmenden Musters zurückgibt, kann verwendet werden, um Verkehrsuntermengen für eine Webanwendung zu definieren. Die folgenden beiden Ausdrücke könnten in Content Switching-Richtlinien für einen virtuellen Content Switching-Server verwendet werden:

- HTTP.REQ.URL.SUFFIX.EQUALS_INDEX(“imagetypes”).LE(3)
- HTTP.REQ.URL.SUFFIX.EQUALS_INDEX(“imagetypes”).GE(4)

Variablen

October 5, 2021

Variablen sind benannte Objekte, die Informationen in Form von Token speichern. Diese Token werden innerhalb und über verschiedene Transaktionen auf der Citrix ADC Appliance für die interne Berechnung und Richtlinienverarbeitung verwendet.

Die Citrix ADC Appliance unterstützt die Erstellung von Variablen der folgenden Typen:

- **Singleton-Variablen.** Kann einen einzelnen Wert von einem der folgenden Typen haben: ulong und text (max-size). Der ulong-Typ ist eine 64-Bit-Ganzzahl ohne Vorzeichen, der Texttyp ist eine Folge von Bytes und max-size ist die maximale Anzahl von Bytes in der Sequenz.
- **Variablen zuordnen.** Karten enthalten Werte, die mit Schlüsseln verknüpft sind: Jedes Schlüssel-Wert-Paar wird als Karteneintrag bezeichnet. Der Schlüssel für jeden Eintrag ist innerhalb der Karte eindeutig. Karten werden wie folgt angegeben:

  Map (key_type, value_type, max-values).

  Wobei:

  - *key_type* ist der Datentyp des Schlüssels. Es ist vom Typ Text (max-size).
  - *value_type* ist der Datentyp der Werte der Karte. Es kann vom Typ ulong oder Text (max-size) sein.
  - *max-values* ist die maximale Anzahl von Einträgen, die die Karte enthalten kann. Es ist vom Typ ulong.

Werte für diese Variablen werden mithilfe von Zuweisungen festgelegt, die für Richtlinienaktionen aufgerufen werden müssen.

> **Hinweis**: Variablen werden in einem Hochverfügbarkeitssetup oder in einem Cluster noch nicht unterstützt.

Variablenbereich

Eine Kartenvariable oder eine Singleton-Variable kann einen globalen Bereich haben. Alternativ kann der Umfang einer Singleton-Variablen auf eine einzelne Transaktion beschränkt werden.

- **Globale Bereichsvariable** : Eine Variable mit globalem Gültigkeitsbereich (Standardwert) hat nur eine Instanz, und diese Instanz hat denselben Wert über alle Kerne einer Citrix ADC Appliance und über alle Knoten einer Cluster- oder HA-Konfiguration hinweg. Globale Variablenwerte existieren, bis sie explizit gelöscht werden, bis sie ablaufen oder bis eine eigenständige Appliance neu gestartet wird oder alle Knoten einer Cluster- oder HA-Konfiguration neu gestartet werden.
- **Transaktionsbereichsvariable** : Eine Variable mit Transaktionsbereich verfügt über eine separate Instanz mit einem eigenen Wert für jede Transaktion, die von der Citrix ADC Appliance verarbeitet wird. Wenn die Transaktionsverarbeitung abgeschlossen ist, wird der Transaktionsvariablenwert gelöscht.

> **Hinweis**: Transaktionsbereichsvariablen sind in Citrix ADC Version 10.5.e oder höher verfügbar.

Konfigurieren und Verwenden von Variablen

October 5, 2021

Sie müssen zuerst eine Variable erstellen und dann einen Wert zuweisen oder den Vorgang angeben, der für die Variable ausgeführt werden muss. Nachdem Sie diese Vorgänge ausgeführt haben, können Sie die Zuweisung als Richtlinienaktion verwenden.

Hinweis: Nach der Konfiguration können die Einstellungen einer Variablen nicht geändert oder zurückgesetzt werden. Wenn die Variable geändert werden muss, müssen die Variable und alle Referenzen auf die Variable (Ausdrücke und Zuweisungen) gelöscht werden. Die Variable kann dann mit neuen Einstellungen neu hinzugefügt werden und die Referenzen (Ausdrücke und Zuweisungen) können neu hinzugefügt werden.

So konfigurieren Sie Variablen mit der Befehlszeilenschnittstelle

1. Erstellen Sie eine Variable.

```
add ns variable <name> -type <string> [-scope global] [-ifFull ( undef
    | lru )] [-ifValueTooBig ( undef | truncate )] [-ifNoValue ( undef |
     init )] [-init <string>] [-expires <positive_integer>] [-comment <
    string>]
<!--NeedCopy-->
```

Hinweis: Beschreibung der Befehlsparameter finden Sie auf der Manpage man add ns variable.

Beispiel 1: Erstellen Sie eine ulong-Variable namens my_counter und initialisieren Sie sie mit 1.

```
add ns variable my_counter  - type ulong -init 1
<!--NeedCopy-->
```

Beispiel 2: Erstellen Sie eine Karte mit dem Namen user_privilege_map. Die Karte enthält Schlüssel mit einer maximalen Länge von 15 Zeichen und Textwerte mit einer maximalen Länge von 10 Zeichen, mit maximal 10000 Einträgen.


```
add ns variable user_privilege_map -type map(text(15),text(10),10000)
<!--NeedCopy-->
```

Hinweis: Wenn die Karte 10000 nicht abgelaufene Einträge enthält, verwenden Zuweisungen für neue Schlüssel einen der zuletzt verwendeten Einträge. Standardmäßig initialisiert ein Ausdruck, der versucht, einen Wert für einen nicht vorhandenen Schlüssel zu erhalten, einen leeren Textwert.

Weisen Sie den Wert zu, oder geben Sie den Vorgang an, der für die Variable ausgeführt werden soll. Dies geschieht durch Erstellen einer Zuweisung.

```
add ns assignment <name> -variable <expression> [-set <expression> | -
    add <expression> | -sub <expression> | -append <expression> | -clear
    ] [-comment <string>]
<!--NeedCopy-->
```

Hinweis: Eine Variable wird mit dem Variablenselektor ($) referenziert. Daher wird **$variable1** verwendet, um auf Text- oder ulong-Variablen zu verweisen. In ähnlicher Weise wird **$variable2[key-expression]**verwendet, um auf Map-Variablen zu verweisen.

Beispiel 1: Definieren Sie eine Zuweisung mit dem Namen inc_my_counter, die automatisch 1 zur Variablen my_counter hinzufügt.

```
add ns assignment inc_my_counter -variable $my_counter -add 1
<!--NeedCopy-->
```

Beispiel 2: Definieren Sie eine Zuweisung mit dem Namen set_user_privilege, die der Variablen user_privilege_map einen Eintrag für die IP-Adresse des Clients mit dem Wert hinzufügt, der von dem HTTP-Callout get_user_privilege zurückgegeben wird.

```
add ns assignment set_user_privilege -variable $user_privilege_map[
    client.ip.src.typecast_text_t] -set sys.http.callout(
    get_user_privilege)
<!--NeedCopy-->
```

Hinweis: Wenn bereits ein Eintrag für diesen Schlüssel vorhanden ist, wird der Wert ersetzt. Andernfalls wird ein neuer Eintrag für Schlüssel und Wert hinzugefügt. Basierend auf der vorherigen Deklaration für user_privilege_map, wenn die Karte bereits 10000 Einträge enthält, wird einer der zuletzt verwendeten Einträge für den neuen Schlüssel und Wert wiederverwendet.

1. Rufen Sie die Variablenzuweisung in einer Richtlinie auf.

   Es gibt zwei Funktionen, die auf Kartenvariablen arbeiten können.

   - **$name.valueExists(key-expression).** Gibt true zurück, wenn ein Wert in der vom Schlüsselausdruck ausgewählten Karte vorhanden ist. Andernfalls wird false zurückgegeben. Diese Funktion aktualisiert die Ablauf- und LRU-Informationen, wenn der Karteneintrag vorhanden ist, erstellt aber keinen neuen Karteneintrag, wenn der Wert nicht vorhanden ist.
   - **$name.valueCount.** Gibt die Anzahl der Werte zurück, die derzeit von der Variablen gehalten werden. Dies ist die Anzahl der Einträge in einer Karte. Für eine Singleton-Variable ist dies 0, wenn die Variable nicht initialisiert ist, oder 1 andernfalls.

   Beispiel: Rufen Sie die Zuweisung set_user_privilege mit einer Komprimierungsrichtlinie auf.

```
1 add cmp policy set_user_privilege_pol -rule $user_privilege_map.
     valueExists(client.ip.src.typecast_text_t).not -resAction
     set_user_privilege
2 <!--NeedCopy-->
```

Verwenden Sie Case, um HTTP-Header in die Antwortseite einzufügen

Das folgende Beispiel zeigt ein Beispiel für eine Singleton-Variable.

Fügen Sie eine Singleton-Variable vom Typ Text hinzu. Diese Variable kann maximal 100 Bytes Daten enthalten.

```
1 add ns variable http_req_data -type text(100) -scope transaction
2 <!--NeedCopy-->
```

Fügen Sie eine Zuweisungsaktion hinzu, mit der die HTTP-Anforderungsdaten in der Variablen gespeichert werden.

```
1 add ns assignment set_http_req_data -variable $http_req_data -set http.
     req.body(100)
2 <!--NeedCopy-->
```

Fügen Sie eine Rewrite-Aktion zum Einfügen des HTTP-Headers hinzu, dessen Wert aus der Variablen abgerufen wird.


```
add rewrite action act_ins_header insert_http_header user_name
    $http_req_data.after_str("user_name").before_str("password")
<!--NeedCopy-->
```

Fügen Sie eine Rewrite-Richtlinie hinzu, die in der Anforderungszeit ausgewertet wird, und ergreifen Sie Zuweisungsaktionen, um Daten zu speichern. Wenn wir diese Richtlinie treffen, ergreifen wir Zuweisungsaktion und speichern die Daten in der ns-Variable (http_req_data)

```
add rewrite policy pol_set_variable true set_http_req_data

bind rewrite global pol_set_variable 10 -type req_dEFAULT
<!--NeedCopy-->
```

Fügen Sie eine Rewrite-Richtlinie hinzu, die in der Antwortzeit ausgewertet wird, und fügen Sie einen HTTP-Header in der Antwort hinzu.

```
add rewrite policy pol_ins_header true act_ins_header

bind rewrite global pol_ins_header 10 -type res_dEFAULT
<!--NeedCopy-->
```

Zuweisungsaktion

In einer Citrix ADC Appliance wird eine an die Richtlinie gebundene Zuweisungsaktion ausgelöst, wenn die Richtlinienregel als true ausgewertet wird. Die Aktion aktualisiert den Wert in der Variablen, der in nachfolgenden Richtlinienregelauswertungen verwendet werden kann. Auf diese Weise kann dieselbe Variable aktualisiert und für nachfolgende Richtlinienauswertungen in derselben Funktion verwendet werden. Zuvor hat die Appliance Zuweisungsaktionen nur ausgeführt, nachdem alle Richtlinien im Feature ausgewertet wurden, wenn die Richtlinien der zugeordneten Zuweisungsaktionen auf true ausgewertet wurden. Daher kann der von der Zuweisungsaktion festgelegte Variablenwert nicht in den nachfolgenden Richtlinienregelauswertungen innerhalb des Features verwendet werden.

Diese Funktionalität kann mit einem Anwendungsfall besser verstanden werden, der die Zugriffsliste für Clients auf einer Citrix ADC Appliance steuert. Die Zugriffsentscheidung wird von einem separaten Webdienst bereitgestellt, mit der Anfrage `GET /client-access?<client-IP-address>`, die eine Antwort mit BLOCK oder ALLOW im Körper zurückgibt. Das HTTP-Callout ist so konfiguriert, dass sie die IP-Adresse des Clients enthält, der einer eingehenden Anforderung zugeordnet ist. Wenn die Cit-

rix ADC Appliance eine Anforderung von einem Client empfängt, generiert die Appliance die Callout-Anforderung und sendet sie an den Callout-Server, der eine Datenbank mit IP-Adressen in der Sperrliste hostet, und einen HTTP-Callout-Agent, der prüft, ob die IP-Adresse des Clients in der Datenbank aufgeführt ist. Der HTTP-Callout-Agent empfängt die Callout-Anforderung, überprüft, ob die IP-Adresse des Clients aufgelistet ist, und sendet eine Antwort. Die Antwort ist ein Statuscode, 200, 302 zusammen mit BLOCK oder ALLOW im Körper. Basierend auf dem Statuscode führt die Appliance die Richtlinienbewertung durch. Wenn die Richtlinienbewertung wahr ist, wird die Zuweisungsaktion sofort ausgelöst, und die Aktion setzt den Wert auf die Variable. Die Appliance verwendet diesen Variablenwert für die nachfolgende Richtlinienbewertung im selben Modul und legt ihn fest.

Anwendungsfall zum Konfigurieren der Zuweisungsaktion

Führen Sie die folgenden Schritte aus, um die Zuweisungsaktion zu konfigurieren und die Variable für nachfolgende Richtlinien zu verwenden:

1. Die Zugriffsentscheidung wird von einem separaten Webdienst bereitgestellt, mit der Anforderung, die eine Antwort mit BLOCK oder ALLOW im Körper zurückgibt.

   ```
   GET /url-service>/url-allowed?<URL path>
   ```

2. Richten Sie eine Zuordnungsvariable ein, um die Zugriffsentscheidungen für URLs zu speichern.

   ```
   add ns variable url_list_map -type 'map(text(1000),text(10),10000)'
   ```

3. Richten Sie ein HTTP-Callout ein, um die Zugriffsanforderung an den Webdienst zu senden.

   ```
   add policy httpCallout url_list_callout -vserver url_vs -returnType
   TEXT -urlStemExpr '"/url-allowed?" + HTTP.REQ.URL.PATH'-resultExpr '
   HTTP.RES.BODY(10)'
   ```

4. Richten Sie eine Zuweisungsaktion ein, um das Callout aufzurufen, um die Zugriffsentscheidung abzurufen, und weisen Sie sie dem Zuordnungseintrag für die URL zu.

   ```
   add ns assignment client_access_assn -variable '$client_access_map[
   CLIENT.IP.SRC.TYPECAST_TEXT_T]'-set SYS.HTTP_CALLOUT(client_access_callout
   )
   ```

5. Richten Sie eine Responder-Aktion ein, um eine 403-Antwort zu senden, wenn eine URL-Anforderung blockiert ist.

   ```
   add responder action url_list_block_act respondwith '"HTTP/1.1 403
   Forbidden\\r\\n\\r\\n"'
   ```

6. Richten Sie eine Responder-Richtlinie ein, um den Zuordnungseintrag für die URL festzulegen, wenn dieser nicht bereits festgelegt ist. Mit der sofortigen Aktionsverbesserung wird der Karteneintragswert festgelegt, wenn diese Richtlinie ausgewertet wird. Vor der Erweiterung

wurde die Zuweisung erst durchgeführt, wenn alle Responder-Richtlinien ausgewertet wurden, wird die Entscheidung durch einen separaten Webdienst bereitgestellt.

```
add responder policy url_list_assn_pol '!$url_list_map.VALUEEXISTS(HTTP
.REQ.URL.PATH)'url_list_assn
```

7. Richten Sie eine Responder-Richtlinie ein, um den Zugriff auf eine URL zu blockieren, wenn der Karteneintragswert BLOCK ist. Mit der sofortigen Aktionsverbesserung ist der von der vorherigen Richtlinie festgelegte Karteneintrag für die Verwendung in dieser Richtlinie verfügbar. Vor der Erweiterung wäre der Karteneintrag an diesem Punkt noch aufgehoben.

   ```
   add responder policy client_access_block_pol '$client_access_map[CLIENT
   .IP.SRC.TYPECAST_TEXT_T] == ”BLOCK”'client_access_block_act
   ```

8. Binden Sie die Responder-Richtlinien an den virtuellen Server. **Hinweis**: Wir können die Richtlinien nicht global binden, da wir sie nicht für das HTTP-Callout auf einem separaten virtuellen Server ausführen möchten.

   ```
   bind lb vserver vs -policyName client_access_assn_pol -priority 10 -
   gotoPriorityExpression NEXT -type REQUEST
   bind lb vserver vs -policyName client_access_block_pol -priority 20 -
   gotoPriorityExpression END -type REQUEST
   ```

So konfigurieren Sie Variablen mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **AppExpert > NS-Variablen**, um eine Variable zu erstellen.
2. Navigieren Sie zu **AppExpert > NS-Zuweisungen**, um der Variablen Werte zuzuweisen.
3. Navigieren Sie zu dem entsprechenden Feature-Bereich, in dem Sie die Zuweisung als Aktion konfigurieren möchten.

Anwendungsfall: Benutzerberechtigungen zwischenspeichern

October 5, 2021

In diesem Anwendungsfall müssen Benutzerberechtigungen (GOLD, SILVER usw.) von einem externen Webdienst abgerufen werden.

Um diesen Anwendungsfall zu erreichen, führen Sie die folgenden Operationen aus

Erstellen Sie ein HTTP-Callout, um die Benutzerberechtigungen vom externen Webdienst abzurufen.


```
add policy httpcallout <name> [-IPAddress <ip_addr|ipv6_addr>] [-port <
    port>] [-vServer <string>] [-returnType <returnType>] [-httpMethod (
    GET | POST )] [-hostExpr <string>] [-urlStemExpr <string>] [-headers
     <name(value)> ...] [-parameters <name(value)> ...] [-bodyExpr <
    string>][-fullReqExpr <string>] [-scheme ( http | https )] [-
    resultExpr <string>] [-cacheForSecs <secs>] [-comment <string>]

add policy httpcallout get_user_privilege -ipaddress 10.217.193.84 -
    port 80 -returnType text -httpMethod GET -hostExpr '"/
    get_user_privilege"' -resultExpr 'http.res.body(5)'
<!--NeedCopy-->
```

Speichern Sie die Berechtigungen in einer Variablen.

```
add ns variable <name> -type <string> [-scope ( global | transaction )
    ][-ifFull ( undef | lru )] [-ifValueTooBig ( undef | truncate )][-
    ifNoValue ( undef | init )] [-init <string>] [-expires <
    positive_integer>] [-comment <string>]

add ns variable user_privilege_map -type map(text(15),text(10),10000) -
    expires 1200

add ns assignment set_user_privilege -variable $user_privilege_map[
    client.ip.src] -set sys.http_callout(get_user_privilege)
<!--NeedCopy-->
```

Erstellen Sie eine Richtlinie, um zu überprüfen, ob bereits ein zwischengespeicherter Eintrag für die IP-Adresse des Clients vorhanden ist. Andernfalls wird das HTTP-Callout aufgerufen, um einen Zuordnungseintrag für den Client festzulegen.

```
add cmp policy <name> -rule <expression> -resAction <string>

add cmp policy set_user_privilege_pol -rule $user_privilege_map.
    valueExists(client.ip.src).not -resAction set_user_privilege>
<!--NeedCopy-->
```

Erstellen Sie eine Richtlinie, die komprimiert wird, wenn der zwischengespeicherte Berechtigungseintrag für den Client GOLD lautet.


```
add cmp policy <name> -rule <expression> -resAction <string>

add cmp policy compress_if_gold_privilege_pol -rule '
   $user_privilege_map[client.ip.src].eq(”GOLD”)' -resAction compress
<!--NeedCopy-->
```

Binden Sie die Komprimierungsrichtlinien global.

```
bind cmp global <policyName> [-priority <positive_integer>] [-state (
   ENABLED | DISABLED )] [-gotoPriorityExpression <expression>] [-type
   <type>] [-invoke (<labelType> <labelName>) ]

bind cmp global set_user_privilege_pol -priority 10 NEXT

bind cmp global compress_if_gold_privilege_pol -priority 20 END
<!--NeedCopy-->
```

Anwendungsfall: Begrenzung der Anzahl von Sitzungen

June 1, 2022

In diesem Anwendungsfall besteht die Anforderung darin, die Anzahl der aktiven Backend-Sitzungen zu begrenzen. In der Bereitstellung hat jede Sitzungsanmeldung eine Anmeldung in der URL und jede Sitzungsabmeldung hat eine Abmeldung in der URL. Bei erfolgreicher Anmeldung setzt das Backend ein Sessionid-Cookie mit einem eindeutigen 10-Zeichen-Wert.

Führen Sie die folgenden Schritte aus, um diesen Anwendungsfall zu erreichen:

1. Erstellen Sie eine Map-Variable, die jede aktive Sitzung speichern kann. Der Schlüssel der Map ist die Sessionid. Die Ablaufzeit für die Variable ist auf 600 Sekunden (10 Minuten) festgelegt.

   ```
   > add ns variable session_map -type map(text(10),ulong,100) -
      expires 600
   <!--NeedCopy-->
   ```

2. Erstellen Sie die folgenden Zuweisungen für die Map-Variable:

   - Erstellen Sie einen Eintrag für die Sessionid und setzen Sie diesen Wert auf 1 (dieser Wert wird nicht wirklich verwendet).


```
> add ns assignment add_session -variable '$session_map[http.
    req.cookie.value("sessionid")]' -set 1
<!--NeedCopy-->
```

- Gibt den Eintrag für eine Sitzungs-ID frei, wodurch die Wertanzahl für session_map implizit verringert wird.

```
> add ns assignment delete_session -variable '$session_map[
    http.req.cookie.value("sessionid")]' -clear
<!--NeedCopy-->
```

3. Erstellen Sie Responder-Richtlinien für Folgendes:

   - Um zu überprüfen, ob ein Zuordnungseintrag für diese Sessionid in der HTTP-Anforderung existiert. Die Add_Session-Zuweisung wird ausgeführt, wenn der Zuordnungseintrag nicht existiert.

```
> add responder policy add_session_pol 'http.req.url.contains
    ("example") || $session_map.valueExists(http.req.cookie.
    value("abc"))' add_session
<!--NeedCopy-->
```

   Hinweis: Die Funktion
   valueExists () in der Richtlinie
   add_session_pol zählt als Referenz auf den Zuordnungseintrag der Sitzung, sodass jede Anforderung das Ablauf-Timeout für ihre Sitzung zurücksetzt. Wenn nach 10 Minuten keine Anfragen für eine Sitzung eingehen, wird der Eintrag der Sitzung freigegeben.

   - Um zu überprüfen, wann die Sitzung abgemeldet ist. Die delete_session Zuweisung wird ausgeführt.

```
add responder policy delete_session_pol "http.req.url.
    contains("Logout")" delete_session
<!--NeedCopy-->
```

   - Um zu überprüfen, ob Anmeldeanfragen vorliegen und ob die Anzahl der aktiven Sitzungen 100 überschreitet. Wenn diese Bedingungen erfüllt sind, wird der Benutzer zur Begrenzung der Anzahl der Sitzungen auf eine Seite umgeleitet, die anzeigt, dass der Server ausgelastet ist.


```
add responder action redirect_too_busy redirect ”/too_busy.
   html”
add responder policy check_login_pol ”http.req.url.contains(”
   example”) && $session_map.valueCount > 100”
   redirect_too_busy
<!--NeedCopy-->
```

4. Binden Sie die Responder-Richtlinien global.

```
bind responder global add_session_pol 30 next
bind responder global delete_session_pol 10
bind responder global check_login_pol 20
<!--NeedCopy-->
```

Richtlinien und Ausdrücke

October 5, 2021

Die folgenden Themen enthalten die Konzept- und Referenzinformationen, die Sie für die Konfiguration erweiterter Richtlinien auf der Citrix® Citrix ADC® -Appliance benötigen.

Informationen über alle erweiterten Richtlinienausdrücke, die auf der Citrix ADC Appliance unterstützt werden, finden Sie unter Richtlinienausdrücke

Einführung in Richtlinien und Ausdrücke	Beschreibt den Zweck von Ausdrücken, Richtlinien und Aktionen sowie deren Verwendung von verschiedenen Citrix ADC Anwendungen.

Erweiterte Richtlinien konfigurieren	Beschreibt die Struktur erweiterter Richtlinien und deren Konfiguration einzeln und als Richtlinienbanken.
Erweiterte Ausdrücke konfigurieren: Erste Schritte	Beschreibt Ausdruckssyntax und Semantik und stellt kurz vor, wie Ausdrücke und Richtlinien konfiguriert werden.
Erweiterte Ausdrücke: Auswerten von Text	Beschreibt Ausdrücke, die Sie konfigurieren, wenn Sie Text bearbeiten möchten (z. B. den Text einer HTTP-POST-Anforderung oder den Inhalt eines Benutzerzertifikats).

Erweiterte Ausdrücke: Arbeiten mit Datum-sangaben, Uhrzeiten und Zahlen	Beschreibt Ausdrücke, die Sie konfig-urieren, wenn Sie mit beliebigen numerischen Daten arbeiten möchten (z. B. die Länge einer URL, die IP-Adresse eines Clients oder das Datum und die Uhrzeit, zu der eine HTTP-Anforderung gesendet wurde).
Erweiterte Ausdrücke: Analysieren von HTTP-, TCP- und UDP-Daten	Beschreibt Ausdrücke zum Analysieren von IP- und IPv6-Adressen, MAC-Adressen und Daten, die für HTTP- und TCP-Datenverkehr spezifisch sind.

Erweiterte Ausdrücke: SSL-Zertifikate analysieren	Beschreibt, wie Ausdrücke für SSL-Datenverkehr und Clientzertifikate konfiguriert werden, z. B. wie das Ablaufdatum eines Zertifikats oder des Zertifikatausstellers abgerufen wird.				
Advanced Expressions: IP and MAC Addresses, Throughput, VLAN IDs	Describes expressions that you can use to work with any other client- or server-related data not discussed in other chapters.	Typecasting Data	Describes expressions for transforming data of one type to another.	Regular Expressions	Describes how to pass regular expressions as arguments to operators in advanced expressions.

Configuring Classic Policies and Expressions	Provides details on how to configure the simpler policies and expressions known as classic policies and classic expressions.	Expressions Reference	A reference for classic and advanced expression arguments.	Summary Examples of Advanced Expressions and Policies	Examples of classic and advanced expressions and policies, in both quick reference and tutorial format, that you can customize for your own use.
Tutorial Examples of Advanced Policies for Rewrite	Examples of advanced policies for use in the Rewrite feature.				
Tutorial Examples of Classic Policies	Examples of classic policies for Citrix ADC features such as application firewall and SSL.				

Migration of Apache mod_rewrite Rules to Advanced Policies	Examples of functions that were written using the Apache HTTP Server mod_rewrite engine, with examples of these functions after translation into Rewrite and Responder policies on the Citrix ADC.

Einführung in Richtlinien und Ausdrucksformen

October 5, 2021

Bei vielen Citrix ADC Features steuern Richtlinien, wie Daten durch ein Feature ausgewertet werden. Eine Richtlinie verwendet einen logischen Ausdruck, der als Regel aufgerufen wird, um Daten auszuwerten, und wendet eine oder mehrere Aktionen basierend auf der Auswertung an. Alternativ kann eine Richtlinie ein Profil anwenden, das eine komplexe Aktion definiert.

Einige Citrix ADC Funktionen verwenden Standard-Syntaxrichtlinien, die mehr Funktionen bieten als ältere klassische Richtlinien. Wenn Sie zu einer neueren Version der Citrix ADC -Software migriert und klassische Richtlinien für Features konfiguriert haben, die Standard-Syntaxrichtlinien verwenden, müssen Sie Richtlinien manuell in die erweiterte Richtlinieninfrastruktur migrieren.

Klassische und erweiterte Richtlinien

October 5, 2021

> **Warnung**
>
> Klassische Richtlinienausdrücke sind ab Citrix ADC 12.0 Build 56.20 veraltet. Alternativ empfiehlt Citrix die Verwendung von erweiterten Richtlinien. Weitere Informationen finden Sie unter Erweiterte Richtlinien

Klassische Richtlinien bewerten die grundlegenden Merkmale des Verkehrs und anderer Daten. Klassische Richtlinien können beispielsweise identifizieren, ob eine HTTP-Anforderung oder -Antwort einen bestimmten Header- oder URL-Typ enthält.

Erweiterte Richtlinien können denselben Typ von Auswertungen durchführen wie klassische Richtlinien. Darüber hinaus können Sie mit der Advanced Policy Infrastructure (PI) mehr Daten (z. B. den Hauptteil einer HTTP-Anforderung) analysieren und weitere Vorgänge in der Richtlinienregel konfigurieren (z. B. die Umwandlung von Daten im Hauptteil einer Anforderung in einen HTTP-Header).

Zusätzlich zum Zuweisen einer Richtlinie eine Aktion oder ein Profil binden Sie die Richtlinie an einen bestimmten Punkt in der Verarbeitung, der den Citrix ADC Features zugeordnet ist. Der Bindepunkt ist ein Faktor, der bestimmt, wann die Richtlinie ausgewertet wird.

Vorteile der Verwendung erweiterter Richtlinien

Standard-Syntaxrichtlinien verwenden eine leistungsstarke Ausdruckssprache, die auf einem Klassen-Objektmodell basiert, und sie bieten mehrere Optionen, mit denen Sie das Verhalten verschiedener Citrix ADC Features konfigurieren können. Mit Advanced Policy Infrastructure (PI) können Sie Folgendes tun:

- Führen Sie feinkörnige Analysen des Netzwerkverkehrs aus den Layern 2 bis 7 durch.
- Bewerten Sie einen beliebigen Teil des Headers oder des Hauptteils einer HTTP- oder HTTPS-Anforderung oder -Antwort.
- Binden Sie Richtlinien an die mehreren Bindepunkte, die die Advanced Policy Infrastructure (PI) auf Standard-, Override- und virtuellen Serverebene unterstützt.
- Verwenden Sie goto Ausdrücke, um die Steuerung an andere Richtlinien zu übertragen und Punkte zu binden, die durch das Ergebnis der Ausdrucksauswertung bestimmt werden.
- Verwenden Sie spezielle Tools wie Mustersätze, Richtlinienbeschriftungen, Ratengrenzbezeichner und HTTP-Callouts, mit denen Sie Richtlinien für komplexe Anwendungsfälle effektiv konfigurieren können.

Außerdem erweitert das Konfigurationsdienstprogramm die robuste Unterstützung der grafischen Benutzeroberfläche für erweiterte Richtlinieninfrastruktur (PI) und Ausdrücke und ermöglicht

Benutzern, die über eingeschränkte Kenntnisse in Netzwerkprotokollen verfügen, Richtlinien schnell und einfach zu konfigurieren. Das Konfigurationsdienstprogramm enthält auch eine Funktion zur Richtlinienauswertung für erweiterte Richtlinien Sie können diese Funktion verwenden, um eine erweiterte Richtlinie auszuwerten und ihr Verhalten zu testen, bevor Sie sie festlegen, wodurch das Risiko von Konfigurationsfehlern reduziert wird.

Grundkomponenten einer erweiterten Richtlinie

Im Folgenden sind einige Merkmale einer erweiterten Richtlinie aufgeführt:

- Name. Jede Richtlinie hat einen eindeutigen Namen.
- Regel. Die Regel ist ein logischer Ausdruck, der es der Citrix ADC Funktion ermöglicht, einen Datenverkehr oder ein anderes Objekt auszuwerten. Mit einer Regel kann Citrix ADC beispielsweise bestimmen, ob eine HTTP-Anforderung von einer bestimmten IP-Adresse stammt oder ob ein Cache-Control-Header in einer HTTP-Anforderung den Wert No-Cache aufweist.

Erweiterte Richtlinien können alle Ausdrücke verwenden, die in einer klassischen Richtlinie verfügbar sind, mit Ausnahme von klassischen Ausdrücken für den SSL-VPN-Client. Darüber hinaus können Sie mit erweiterten Richtlinien komplexere Ausdrücke konfigurieren.

- Bindungen. Um sicherzustellen, dass Citrix ADC bei Bedarf eine Richtlinie aufrufen kann, ordnen Sie die Richtlinie zu oder binden sie an einen oder mehrere Bindungspunkte.

Sie können eine Richtlinie global oder an einen virtuellen Server binden. Weitere Informationen finden Sie unter Informationen zu Richtlinienbindungen.

- Eine zugeordnete Aktion. Eine Aktion ist eine separate Entität von einer Richtlinie. Die Richtlinienbewertung führt letztendlich dazu, dass Citrix ADC eine Aktion ausführt.

Beispielsweise kann eine Richtlinie im integrierten Cache HTTP-Anforderungen für GIF- oder JPEG-Dateien identifizieren. Eine Aktion, die Sie dieser Richtlinie zuordnen, bestimmt, dass die Antworten auf diese Arten von Anforderungen aus dem Cache bereitgestellt werden.

Bei einigen Features konfigurieren Sie Aktionen als Teil einer komplexeren Reihe von Anweisungen, die als Profil bezeichnet werden.

Wie unterschiedliche Citrix ADC Funktionen Richtlinien verwenden

Citrix ADC unterstützt verschiedene Funktionen, die auf Richtlinien für den Betrieb basieren. In der folgenden Tabelle wird erläutert, wie die Citrix ADC Features Richtlinien verwenden.

Featurename	Richtlinientyp	Verwendung von Richtlinien im Feature
System	Klassisch	Für die Authentifizierungsfunktion enthalten Richtlinien Authentifizierungsschemata für verschiedene Authentifizierungsmethoden. Sie können beispielsweise LDAP- und zertifikatbasierte Authentifizierungsschemata konfigurieren. Außerdem konfigurieren Sie Richtlinien in der Überwachungsfunktion.
DNS	Erweitert	So bestimmen Sie, wie die DNS-Auflösung für Anforderungen ausgeführt wird.
SSL	Klassisch und Fortgeschrittene	So bestimmen Sie, wann eine Verschlüsselungsfunktion angewendet werden soll, und fügen Sie dem Klartext Zertifikatsinformationen hinzu. Um eine End-to-End-Sicherheit zu gewährleisten, verschlüsselt die SSL-Funktion nach der Entschlüsselung einer Nachricht Klartext erneut und verwendet SSL für die Kommunikation mit Webservern.
Komprimierung	Klassisch und Fortgeschrittene	Um zu bestimmen, welche Art von Datenverkehr komprimiert wird.

Featurename	Richtlinientyp	Verwendung von Richtlinien im Feature
Integriertes Caching	Erweitert	Um festzustellen, ob HTTP-Antworten zwischenspeicherbar sind.
Responder	Erweitert	Konfigurieren des Verhaltens der Responder-Funktion.
Schutzfunktionen	Klassisch	So konfigurieren Sie das Verhalten der Funktionen Filter, SureConnect und Priority Queuing.
Content Switching	Klassisch und Fortgeschrittene	Um zu bestimmen, welcher Server oder eine Gruppe von Servern für die Bereitstellung von Antworten verantwortlich ist, basierend auf den Merkmalen einer eingehenden Anforderung. Anforderungsmerkmale umfassen Gerätetyp, Sprache, Cookies, HTTP-Methode, Inhaltstyp und zugehörige Cacheserver.
AAA - Verkehrsmanagement	Klassisch. Ausnahmen: Verkehrsrichtlinien unterstützen nur die Advanced Policy Infrastructure (PI) und Autorisierungsrichtlinien unterstützen sowohl die klassische als auch die erweiterte Richtlinieninfrastruktur (PI).	So überprüfen Sie die clientseitige Sicherheit, bevor sich Benutzer anmelden und eine Sitzung einrichten. Verkehrsrichtlinien, die bestimmen, ob Single Sign-On (SSO) erforderlich ist, verwenden nur die Standardsyntax. Autorisierungsrichtlinien autorisieren Benutzer und Gruppen, die über die Appliance auf Intranetressourcen zugreifen.

Featurename	Richtlinientyp	Verwendung von Richtlinien im Feature
Cacheumleitung	Klassisch	Bestimmen Sie, ob Antworten von einem Cache oder von einem Ursprungsserver bereitgestellt werden.
Neuschreiben	Erweitert	So identifizieren Sie HTTP-Daten, die Sie vor dem Servieren ändern möchten. Die Richtlinien enthalten Regeln zum Ändern der Daten. Beispielsweise können Sie HTTP-Daten ändern, um eine Anforderung an eine neue Homepage oder einen neuen Server oder einen ausgewählten Server basierend auf der Adresse der eingehenden Anforderung umzuleiten, oder Sie können die Daten so ändern, dass Serverinformationen in einer Antwort aus Sicherheitsgründen maskiert werden. Die URL-Transformator-Funktion identifiziert URLs in HTTP-Transaktionen und Textdateien, um zu bewerten, ob eine URL transformiert werden soll.
Anwendungs-Firewall	Klassisch und Fortgeschrittene	Identifizieren von Merkmalen von Datenverkehr und Daten, die über die Firewall zugelassen werden sollen oder nicht.

Featurename	Richtlinientyp	Verwendung von Richtlinien im Feature
Citrix Gateway, Clientless Access-Funktion	Erweitert	So definieren Sie Rewrite-Regeln für den allgemeinen Webzugriff mit Citrix Gateway.
Citrix Gateway	Klassisch	So bestimmen Sie, wie Citrix Gateway Authentifizierung, Autorisierung, Überwachung und andere Funktionen ausführt.

Informationen zu Aktionen und Profilen

Die Richtlinien selbst ergreifen keine Maßnahmen in den Bereichen Daten. Richtlinien bieten schreibgeschützte Logik für die Auswertung des Datenverkehrs. Um eine Funktion für die Ausführung eines Vorgangs auf der Grundlage einer Richtlinienbewertung zu aktivieren, konfigurieren Sie Aktionen oder Profile und ordnen sie Richtlinien zu.

Hinweis: Aktionen und Profile sind spezifisch für bestimmte Features. Informationen zum Zuweisen von Aktionen und Profilen zu Features finden Sie in der Dokumentation zu den einzelnen Features.

Informationen zu Aktionen

Aktionen sind Schritte, die der Citrix ADC durchführt, abhängig von der Auswertung des Ausdrucks in der Richtlinie. Wenn beispielsweise ein Ausdruck in einer Richtlinie mit einer bestimmten Quell-IP-Adresse in einer Anforderung übereinstimmt, bestimmt die Aktion, die dieser Richtlinie zugeordnet ist, ob die Verbindung zulässig ist.

Die Arten von Aktionen, die der Citrix ADC ausführen kann, sind featurespezifisch. Beispielsweise können Aktionen in Umschreiben Text in einer Anforderung ersetzen, die Ziel-URL für eine Anforderung ändern usw. In integriertem Caching legen Aktionen fest, ob HTTP-Antworten aus dem Cache oder einem Ursprungsserver bereitgestellt werden.

In einigen Citrix ADC Funktionen sind Aktionen vordefiniert und in anderen sind sie konfigurierbar. In einigen Fällen (z. B. Umschreiben) konfigurieren Sie die Aktionen mit denselben Ausdruckstypen, die Sie zum Konfigurieren der zugeordneten Richtlinienregel verwenden.

Übersicht über Profile

Mit einigen Citrix ADC Funktionen können Sie Profile oder beide Aktionen und Profile einer Richtlinie zuordnen. Ein Profil ist eine Sammlung von Einstellungen, mit denen das Feature eine komplexe Funktion ausführen kann. Beispielsweise kann ein Profil für XML-Daten in der Anwendungsfirewall mehrere Screening-Vorgänge ausführen, z. B. das Überprüfen der Daten auf unzulässige XML-Syntax oder den Nachweis einer SQL-Injection.

Verwendung von Aktionen und Profilen insbesondere Funktionen

In der folgenden Tabelle wird die Verwendung von Aktionen und Profilen in verschiedenen Citrix ADC Features zusammengefasst. Der Tisch ist nicht erschöpfend. Weitere Informationen zu bestimmten Verwendungszwecken von Aktionen und Profilen für ein Feature finden Sie in der Dokumentation des Features.

Feature	Verwendung einer Aktion	Verwendung eines Profils
Anwendungs-Firewall	Synonym mit einem Profil	Alle Anwendungs-Firewall-Funktionen verwenden Profile, um komplexe Verhaltensweisen zu definieren, einschließlich Muster-basiertes Lernen. Sie fügen diese Profile Richtlinien hinzu.

Feature	Verwendung einer Aktion	Verwendung eines Profils
Citrix Gateway	Die folgenden Funktionen von Citrix Gateway verwenden Aktionen: Vorauthentifizierung. Verwendet Aktionen Zulassen und Verweigern. Sie fügen diese Aktionen zu einem Profil hinzu., Autorisierung. Verwendet Aktionen Zulassen und Verweigern. Sie fügen diese Aktionen zu einer Richtlinie hinzu. TCP-Komprimierung. Verwendet verschiedene Aktionen. Sie fügen diese Aktionen zu einer Richtlinie hinzu.	Die folgenden Features verwenden ein Profil: Vorauthentifizierung, Sitzung, Datenverkehr und Clientloser Zugriff. Nachdem Sie die Profile konfiguriert haben, fügen Sie sie den Richtlinien hinzu.
Neuschreiben	Sie konfigurieren URL-Umschreibungsaktionen und fügen sie einer Richtlinie hinzu.	Nicht benutzt.
Integriertes Caching	Konfigurieren von Cache- und Invalidierungsaktionen innerhalb einer Richtlinie	Nicht benutzt.
AAA - Verkehrsmanagement	Sie wählen einen Authentifizierungstyp aus, legen eine Autorisierungsaktion von ALLOW oder DENY fest oder legen die Überwachung auf SYSLOG oder NSLOG fest.	Sie können Sitzungsprofile mit einer standardmäßigen Zeitüberschreitung und Autorisierungsaktion konfigurieren.
Schutzfunktionen	Sie konfigurieren Aktionen innerhalb von Richtlinien für die folgenden Funktionen: Filter, Komprimierung, Responder und SureConnect.	Nicht benutzt.

Feature	Verwendung einer Aktion	Verwendung eines Profils
SSL	Sie konfigurieren Aktionen innerhalb von SSL-Richtlinien	Nicht benutzt.
System	Die Aktion ist impliziert. Für die Authentifizierungsfunktion ist es entweder Zulassen oder Verweigern. Bei Auditing ist es Auditing On oder Auditing Off.	Nicht benutzt.
DNS	Die Aktion ist impliziert. Es handelt sich entweder um Drop Packets oder um den Speicherort eines DNS-Servers.	Nicht benutzt.
SSL-Offload	Die Aktion ist impliziert. Es basiert auf einer Richtlinie, die Sie einem virtuellen SSL-Server oder einem Dienst zuordnen.	Nicht benutzt.
Komprimierung	Bestimmen Sie den Komprimierungstyp, der auf die Daten angewendet werden soll	Nicht benutzt.
Content Switching	Die Aktion ist impliziert. Wenn eine Anforderung mit der Richtlinie übereinstimmt, wird die Anforderung an den virtuellen Server geleitet, der der Richtlinie zugeordnet ist.	Nicht benutzt.
Cacheumleitung	Die Aktion ist impliziert. Wenn eine Anforderung mit der Richtlinie übereinstimmt, wird die Anforderung an den Ursprungsserver weitergeleitet.	Nicht benutzt.

Informationen zu Richtlinienbindungen

Eine Richtlinie ist einer Entität zugeordnet oder gebunden, mit der die Richtlinie aufgerufen werden kann. Beispielsweise können Sie eine Richtlinie an die Auswertung der Anforderungszeit binden, die für alle virtuellen Server gilt. Eine Sammlung von Richtlinien, die an einen bestimmten Bindepunkt gebunden sind, stellt eine Richtlinienbank dar.

Im Folgenden finden Sie eine Übersicht über verschiedene Arten von Bindungspunkten für eine Richtlinie:

- Anforderungszeit global. Eine Richtlinie kann für alle Komponenten in einem Feature zum Anforderungszeitpunkt verfügbar sein.
- Reaktionszeit global. Eine Richtlinie kann für alle Komponenten eines Features zur Reaktionszeit verfügbar sein.
- Anforderungszeit, virtuell serverspezifisch.

Eine Richtlinie kann an die Anforderungszeitverarbeitung für einen bestimmten virtuellen Server gebunden werden. Beispielsweise können Sie eine Anforderungszeitrichtlinie an einen virtuellen Cache-Umleitungsserver binden, um sicherzustellen, dass bestimmte Anforderungen an einen virtuellen Lastausgleichsserver für den Cache weitergeleitet werden und andere Anforderungen an einen virtuellen Lastausgleichsserver für den Ursprung gesendet werden.

- Reaktionszeit, virtuell serverspezifisch. Eine Richtlinie kann auch an die Reaktionszeitverarbeitung für einen bestimmten virtuellen Server gebunden werden.
- Benutzerdefinierte Richtlinienbezeichnung. Für Advanced Policy Infrastructure (PI) können Sie benutzerdefinierte Gruppierungen von Richtlinien (Richtlinienbanken) konfigurieren, indem Sie ein Policy Label definieren und eine Reihe verwandter Richtlinien unter dem Policy Label sammeln.
- Andere Bindungspunkte. Die Verfügbarkeit zusätzlicher Bindepunkte hängt von der Art der Richtlinie (klassische oder erweiterte Richtlinien) und den Besonderheiten der relevanten Citrix ADC-Funktion ab. Klassische Richtlinien, die Sie für Citrix Gateway konfigurieren, verfügen beispielsweise über Benutzer- und Gruppen-Bindungspunkte.

Weitere Informationen zu erweiterten Richtlinienbindungen finden Sie unter Binden von Richtlinien, die die erweiterten Richtlinien verwenden, und Konfigurieren einer Richtlinienbank für einen virtuellen Server. Weitere Informationen zu klassischen Richtlinienbindungen finden Sie unter Konfigurieren einer klassischen Richtlinie.

Informationen zur Evaluierungsreihenfolge von Richtlinien

Bei klassischen Richtlinien werden Richtliniengruppen und Richtlinien innerhalb einer Gruppe in einer bestimmten Reihenfolge ausgewertet, je nach den folgenden Kriterien:

- Der Bindepunkt für die Richtlinie, z. B. ob die Richtlinie an die Anforderungszeitverarbeitung

für einen virtuellen Server oder eine globale Antwortzeitverarbeitung gebunden ist. Beispielsweise wertet Citrix ADC zum Anforderungszeitpunkt alle klassischen Richtlinien aus, bevor alle virtuellen serverspezifischen Richtlinien ausgewertet werden.

- Die Prioritätsstufe für die Richtlinie. Für jeden Punkt im Evaluierungsprozess bestimmt eine Prioritätsstufe, die einer Richtlinie zugewiesen ist, die Reihenfolge der Evaluierung relativ zu anderen Richtlinien, die denselben Bindepunkt haben. Wenn Citrix ADC beispielsweise eine Gruppe virtueller serverspezifischer Richtlinien für die Anforderungszeit auswertet, beginnt er mit der Richtlinie, die dem niedrigsten Prioritätswert zugewiesen ist. Bei klassischen Richtlinien müssen Prioritätsstufen über alle Bindepunkte hinweg eindeutig sein.

Bei erweiterten Richtlinien wählt Citrix ADC wie bei klassischen Richtlinien eine Gruppierung oder Bank von Richtlinien an einem bestimmten Punkt der Gesamtverarbeitung aus. Im Folgenden finden Sie die Reihenfolge der Bewertung der grundlegenden Gruppierungen oder Banken von Advanced Policies:

1. Globale Anforderungszeitüberschreibung
2. Anforderungszeit, virtuell serverspezifisch (ein Bindepunkt pro virtueller Server)
3. Globale Anforderungszeit-Standardeinstellung
4. Globale Überschreibung der Antwortzeit
5. Antwortzeit virtuell serverspezifisch
6. Globaler Standardwert für die Antwortzeit

Innerhalb einer der vorangegangenen Richtliniebanken ist die Reihenfolge der Evaluierung jedoch flexibler als in der klassischen Richtlinie. Innerhalb einer Richtlinienbank können Sie auf die nächste zu bewertende Richtlinie verweisen, unabhängig von der Prioritätsstufe, und Sie können Richtlinienbanken aufrufen, die zu anderen Bindpunkten und benutzerdefinierten Richtlinienbanken gehören.

Reihenfolge der Auswertung basierend auf Verkehrsfluss

Da der Datenverkehr durch den Citrix ADC fließt und von verschiedenen Features verarbeitet wird, führt jedes Feature eine Richtlinienbewertung durch. Wenn eine Richtlinie mit dem Datenverkehr übereinstimmt, speichert das Citrix ADC die Aktion und setzt die Verarbeitung fort, bis die Daten den Citrix ADC verlassen werden. Zu diesem Zeitpunkt wendet Citrix ADC in der Regel alle übereinstimmenden Aktionen an. Integriertes Caching, das nur eine abschließende Cache- oder NoCache-Aktion anwendet, ist eine Ausnahme.

Einige Richtlinien beeinflussen das Ergebnis anderer Richtlinien. Im Folgenden finden Sie Beispiele:

- Wenn eine Antwort aus dem integrierten Cache bereitgestellt wird, verarbeiten einige andere Citrix ADC Funktionen die Antwort oder die Anforderung, die sie initiiert hat, nicht.
- Wenn die Inhaltsfilter-Funktion verhindert, dass eine Antwort bereitgestellt wird, wird die Antwort durch keine nachfolgenden Features ausgewertet.

Wenn die Anwendungsfirewall eine eingehende Anforderung ablehnt, können sie von anderen Features nicht verarbeitet werden.

Klassische und erweiterte Richtlinienausdrücke

October 5, 2021

Einer der grundlegendsten Komponenten einer Richtlinie ist ihre Regel. Eine Richtlinienregel ist ein logischer Ausdruck, der es der Richtlinie ermöglicht, Datenverkehr zu analysieren. Der Großteil der Funktionalität der Richtlinie wird von ihrem Ausdruck abgeleitet.

Ein Ausdruck entspricht den Merkmalen von Datenverkehr oder anderen Daten mit einem oder mehreren Parametern und Werten. Beispielsweise kann ein Ausdruck den Citrix ADC ermöglichen, Folgendes zu erreichen:

- Bestimmen Sie, ob eine Anforderung ein Zertifikat enthält.
- Bestimmen Sie die IP-Adresse eines Clients, der eine TCP-Anforderung gesendet hat.
- Identifizieren Sie die Daten, die eine HTTP-Anforderung enthält (z. B. eine beliebte Kalkulationstabelle oder Textverarbeitungsanwendung).
- Berechnen Sie die Länge einer HTTP-Anforderung.

Allgemeine Informationen zu klassischen Ausdrücken

Klassische Ausdrücke ermöglichen es Ihnen, grundlegende Merkmale von Daten auszuwerten. Sie haben eine strukturierte Syntax, die String-Matching und andere Operationen durchführt.

Im Folgenden sind ein paar einfache Beispiele für klassische Ausdrücke:

- Eine HTTP-Antwort enthält einen bestimmten Typ von Cache Control-Header.

res.http.header Cache-Control contains public

- Eine HTTP-Antwort enthält Bilddaten.

res.http.header Content-Type contains image

- Eine SSL-Anforderung enthält ein Zertifikat.

req.ssl.client.cert exists

Informationen zu erweiterten Richtlinienausdrücken

Jedes Feature, das Standard-Syntaxrichtlinien verwendet, verwendet auch erweiterte Ausdrücke. Informationen darüber, welche Funktionen erweiterte Richtlinien verwenden, finden Sie in der Tabelle Citrix ADC Feature, Richtlinientyp und Richtlinienverwendung.

Erweiterte Richtlinienausdrücke haben einige andere Verwendungszwecke. Zusätzlich zum Konfigurieren von erweiterten Ausdrücken in Richtlinienregeln konfigurieren Sie erweiterte Ausdrücke in den folgenden Situationen:

- Integriertes Caching:

  Sie verwenden erweiterte Richtlinienausdrücke, um einen Selektor für eine Inhaltsgruppe im integrierten Cache zu konfigurieren.

- Lastenausgleich:

  Sie verwenden erweiterte Richtlinienausdrücke, um Tokenextraktion für einen virtuellen Lastausgleichsserver zu konfigurieren, der die TOKEN-Methode für den Lastenausgleich verwendet.

- Umschreiben:

  Sie verwenden erweiterte Richtlinienausdrücke, um Umschreibaktionen zu konfigurieren.

- Preisbasierte Richtlinien:

  Sie verwenden erweiterte Richtlinienausdrücke, um Limitselektoren zu konfigurieren, wenn Sie eine Richtlinie konfigurieren, um die Rate des Datenverkehrs zu verschiedenen Servern zu steuern.

Im Folgenden finden Sie einige einfache Beispiele für erweiterte Richtlinienausdrücke:

- Eine HTTP-Anforderungs-URL enthält nicht mehr als 500 Zeichen.

```
http.req.url.length \<= 500
```

- Eine HTTP-Anforderung enthält ein Cookie, das weniger als 500 Zeichen enthält.

```
http.req.cookie.length \< 500
```

- Eine HTTP-Anforderungs-URL enthält eine bestimmte Textzeichenfolge.

```
http.req.url.contains(".html")
```

Konvertieren von Richtlinienausdrücken mit dem NSPEPI-Tool

October 11, 2022

> **Hinweis:**
>
> Sie können das NSPEPI- und Preconfig-Check-Tool vom öffentlichen GitHub herunterladen. Weitere Informationen finden Sie auf der Github NEPEPI-Seite und auf der GitHub-Vorkonfigurationsseite für detaillierte Anweisungen zum Herunterladen der Tools. Wir empfehlen Kunden, die in GitHub verfügbaren Tools für die vollständigste und aktuellste

> Version zu verwenden.

Klassische richtlinienbasierte Merkmale und Funktionen sind ab NetScaler 12.0 Build 56.20 veraltet. Als Alternative empfiehlt Citrix die Verwendung der erweiterten Richtlinieninfrastruktur. Im Rahmen dieser Bemühungen müssen Sie beim Upgrade auf Citrix ADC 12.1 Build 56.20 oder höher die richtlinienbasierten Funktionen und Funktionen von Classic durch die entsprechenden nicht veralteten Funktionen und Funktionen ersetzen. Außerdem müssen Sie klassische Richtlinien und Ausdrücke in erweiterte Richtlinien und Ausdrücke konvertieren. Außerdem unterstützen alle neuen Citrix ADC-Funktionen nur erweiterte Richtlinieninfrastruktur.

Das Tool `nspepi` kann Folgendes ausführen:

1. Konvertieren Sie klassische Richtlinienausdrücke in erweiterte Richtlinienausdrücke.
2. Konvertieren Sie bestimmte Classic-Richtlinien und deren Entitätsbindungen in erweiterte Richtlinien und Bindungen.
3. Konvertieren Sie ein paar weitere veraltete Funktionen in ihre entsprechenden nicht veralteten Funktionen.
4. Konvertieren Sie klassische Filterbefehle in erweiterte Filterbefehle.

> **Hinweis:**
>
> Nachdem das Tool `nspepi` die ns.conf-Konfigurationsdatei erfolgreich konvertiert hat, zeigt das Tool die konvertierte Datei als neue Datei mit dem Präfix “new_” an. Wenn die konvertierte Konfigurationsdatei Fehler oder Warnungen enthält, müssen Sie diese im Rahmen des Konvertierungsprozesses manuell beheben. Nach der Konvertierung müssen Sie die Datei in der Testumgebung testen und dann verwenden, um die eigentliche ns.conf-Konfigurationsdatei zu ersetzen. Nach dem Testen müssen Sie die Appliance für die neu konvertierte oder feste ns.conf-Konfigurationsdatei neu starten.

Funktionen, die nur klassische Richtlinien oder Ausdrücke unterstützen, sind veraltet und können durch die entsprechenden nicht veralteten Funktionen ersetzt werden.

> **Hinweis:**
>
> Informationen zur älteren Version des Tools `nspepi` sind in einem PDF-Format verfügbar. Weitere Informationen finden Sie unter Klassische Richtlinienkonvertierung mithilfe des nspepi-Tool vor 12.1-51.16 PDF.

Konvertierungswarnungen und Fehlerdateien

Bevor Sie das Tool für Ihre Konvertierung verwenden, sollten Sie nur wenige Warnungen beachten:

1. Alle Warnungen und Fehler werden an die Konsole ausgegeben. Es wird eine Warndatei erstellt, in der die Konfigurationsdateien gespeichert werden.
2. Die Warnungs- und Fehlerdatei hat den gleichen Namen wie die Eingabedatei, jedoch mit dem Präfix “warn_”, das dem Dateinamen hinzugefügt wurde. Während der Ausdrucksumwandlung

(bei Verwendung von -e) werden die Warnungen im aktuellen Verzeichnis mit dem Namen “warn_expr” angezeigt.

> **Hinweis:**
>
> Diese Datei hat ein Standard-Protokolldateiformat mit Datums-/Zeitstempel und Protokollebene. Frühere Instanzen der Datei werden mit Suffixen wie “.1”, “.2” usw. beibehalten, da das Tool mehrmals ausgeführt wird. Es werden höchstens 10 Instanzen beibehalten.

Konvertiertes Dateiformat

Beim Konvertieren einer Konfigurationsdatei (mit “-f”) wird die konvertierte Datei in dasselbe Verzeichnis abgelegt, in dem die Eingabekonfigurationsdatei mit demselben Namen, aber einem Präfix “neu_” existiert.

Befehle oder Funktionen, die vom nspepi-Konvertierungstool verarbeitet werden

Im Folgenden werden die Befehle aufgeführt, die während des automatischen Konvertierungsprozesses verarbeitet werden.

- Die folgenden Classic-Richtlinien und ihre Ausdrücke werden in erweiterte Richtlinien und Ausdrücke umgewandelt. Die Konvertierung umfasst Entitätsbindungen und globale Bindungen.

1. add appfw policy
2. add cmp policy
3. add cr policy
4. add cs policy
5. add tm sessionPolicy
6. add filter action
7. add filter policy
8. Filterrichtlinienbindung an Lastenausgleich, Content Switching, Cache-Umleitung und global.

> **Hinweis:**
>
> Für “add tm sessionPolicy” können Sie jedoch nicht an globale Überschreibungen in erweiterten Richtlinien binden.

- Der in “Add lb virtuellen Server hinzufügen” konfigurierte Regelparameter wird vom klassischen Ausdruck in den erweiterten Ausdruck konvertiert.
- Der im Befehl “add ns httpProfile” oder “set ns httpProfile” konfigurierte SPDY-Parameter wird in “-http2 ENABLED” geändert.
- Benannte Ausdrücke (Befehle “Richtlinienausdruck hinzufügen”). Jeder klassische benannte Richtlinienausdruck wird in den entsprechenden benannten erweiterten Ausdruck umgewandelt, wobei “nspepi_adv_” als Präfix festgelegt ist. Darüber hinaus wird die Verwendung be-

nannter Ausdrücke für die konvertierten Classic-Ausdrücke in die entsprechenden erweiterten benannten Ausdrücke geändert. Darüber hinaus hat jeder benannte Ausdruck zwei benannte Ausdrücke, wobei einer Classic und der andere Advanced ist (wie unten gezeigt).

- Tunnel TrafficPolicy Konvertierung wird unterstützt.
- Umgang mit integrierten klassischen Richtlinienbindungen in CMP, CR und Tunnel.
- Patclass Feature wird in Pat Set Feature umgewandelt.
- Der Parameter "-pattern" im Befehl "add rewrite action" wird umgewandelt, um den Parameter "-search" zu verwenden.
- SYS.EVAL_CLASSIC_EXPR wird in den entsprechenden nicht veralteten erweiterten Ausdruck umgewandelt. Diese Ausdrücke sind in jedem Befehl zu sehen, in dem erweiterte Ausdrücke zulässig sind.
- Q- und S-Präfixe von erweiterten Ausdrücken werden in äquivalente, nicht veraltete erweiterte Ausdrücke umgewandelt. Diese Ausdrücke sind in jedem Befehl zu sehen, in dem erweiterte Ausdrücke zulässig sind.

Beispiel:

```
add policy expression classic_expr ns_true
Converts to:
add policy expression classic_expr ns_true
add policy expression nspepi_adv_classic_expr TRUE
<!--NeedCopy-->
```

- Der im Befehl "set cmp parameter" konfigurierte policyType-Parameter wird entfernt. Standardmäßig ist der Richtlinientyp "Advanced".

Konvertieren von klassischen Filterbefehlen in erweiterte Filterbefehle

Das Tool `nspepi` kann Befehle basierend auf klassischen Filteraktionen wie Hinzufügen, Binden usw. in erweiterte Filterbefehle konvertieren.

Das nepepi-Tool unterstützt jedoch die folgenden Filterbefehle nicht.

1. add filter action <`action Name`> FORWARD <`service name`>
2. add filter action <`action name`> ADD prebody
3. add filter action <`action name`> ADD postbody

> **Hinweis:**
>
> 1. Wenn es in ns.conf Rewrite- oder Responder-Features gibt und ihre Richtlinien global mit dem Ausdruck `GOTO` als `END` oder `USER_INVOCATION_RESULT`gebunden sind und der Bindetyp ist `REQ_X` oder `RES_X` dann konvertiert das Tool Bindungsfilterbefehle teilweise

> und kommentiert. Eine Warnung wird angezeigt, um manuellen Aufwand zu unternehmen.
> 2. Wenn es vorhandene Rewrite- oder Responder-Funktionen gibt und deren Richtlinien an virtuelle Server (z. B. Load Balancing, Content Switching oder Cache-Umleitung) vom Typ HTTPS mit `GOTO - END` oder `USER_INVOCATION_RESULT` gebunden sind , konvertiert das Tool Bindungsfilterbefehle teilweise und kommentiert dann Kommentare aus. Eine Warnung wird angezeigt, um manuellen Aufwand zu unternehmen.

Beispiel

Es folgt eine Beispieleingabe:

```
add lb vserver v1 http 1.1.1.1 80 -persistenceType NONE -cltTimeout
    9000
add cs vserver csv1 HTTP 1.1.1.2 80 -cltTimeout 180 -persistenceType
    NONE
add cr vserver crv1 HTTP 1.1.1.3 80 -cacheType FORWARD
add service svc1 1.1.1.4 http 80
add filter action fact_add add 'header:value'
add filter action fact_variable add 'H1:%%HTTP.TRANSID%%'
add filter action fact_prebody add prebody
add filter action fact_error_act1 ERRORCODE 200 ”<HTML>Good URL</HTML>”
add filter action fact_forward_act1 FORWARD svc1
add filter policy fpol_add_res -rule ns_true -resAction fact_add
add filter policy fpol_error_res -rule ns_true -resAction
    fact_error_act1
add filter policy fpol_error_req -rule ns_true -reqAction
    fact_error_act1
add filter policy fpol_add_req -rule ns_true -reqAction fact_add
add filter policy fpol_variable_req -rule ns_true -reqAction
    fact_variable
add filter policy fpol_variable_res -rule ns_true -resAction
    fact_variable
add filter policy fpol_prebody_req -rule ns_true -reqAction
    fact_prebody
add filter policy fpol_prebody_res -rule ns_true -resAction
    fact_prebody
add filter policy fpol_forward_req -rule ns_true -reqAction
    fact_forward_act1
bind lb vserver v1 -policyName fpol_add_res
bind lb vserver v1 -policyName fpol_add_req
bind lb vserver v1 -policyName fpol_error_res
bind lb vserver v1 -policyName fpol_error_req
bind lb vserver v1 -policyName fpol_variable_res
```



```
bind lb vserver v1 -policyName fpol_variable_req
bind lb vserver v1 -policyName fpol_forward_req
bind cs vserver csv1 -policyName fpol_add_req
bind cs vserver csv1 -policyName fpol_add_res
bind cs vserver csv1 -policyName fpol_error_res
bind cs vserver csv1 -policyName fpol_error_req
bind cr vserver crv1 -policyName fpol_add_req
bind cr vserver crv1 -policyName fpol_add_res
bind cr vserver crv1 -policyName fpol_error_res
bind cr vserver crv1 -policyName fpol_error_req
bind cr vserver crv1 -policyName fpol_forward_req
bind filter global fpol_add_req
bind filter global fpol_add_res
bind filter global fpol_error_req
bind filter global fpol_error_res
bind filter global fpol_variable_req
bind filter global fpol_variable_res
bind filter global fpol_variable_res -state DISABLED
bind filter global fpol_prebody_req
bind filter global fpol_forward_req
After conversion, warning/error messages will be displayed for manual
   effort.
Warning files:
cat warn_<input file name>:
2019-11-07 17:13:34,724: ERROR - Conversion of [add filter action
   fact_prebody add prebody] not supported in this tool.
2019-11-07 17:13:34,739: ERROR - Conversion of [add filter action
   fact_forward_act1 FORWARD svc1] not supported in this tool.
2019-11-07 17:13:38,042: ERROR - Conversion of [add filter policy
   fpol_prebody_req -rule ns_true -reqAction fact_prebody] not
   supported in this tool.
2019-11-07 17:13:38,497: ERROR - Conversion of [add filter policy
   fpol_prebody_res -rule ns_true -resAction fact_prebody] not
   supported in this tool.
2019-11-07 17:13:39,035: ERROR - Conversion of [add filter policy
   fpol_forward_req -rule ns_true -reqAction fact_forward_act1] not
   supported in this tool.
2019-11-07 17:13:39,060: WARNING - Following bind command is commented
   out because state is disabled. Advanced expressions only have a
   fixed ordering of the types of bindings without interleaving, except
    that global bindings are allowed before all other bindings and
   after all bindings. If you have global bindings in the middle of non
   -global bindings or any other interleaving then you will need to
   reorder all your bindings for that feature and direction. Refer to
   nspepi documentation. If command is required please take a backup
```



```
      because comments will not be saved in ns.conf after triggering 'save
       ns config': bind filter global fpol_variable_res -state DISABLED
53
54
55 <!--NeedCopy-->
```

Es folgt eine Beispielausgabe. Alle konvertierten Befehle werden kommentiert.

```
1  cat new_<input file name>
2  add rewrite action fact_add insert_http_header header ””value””
3  add filter action fact_prebody add prebody
4  add filter action fact_forward_act1 FORWARD svc1
5  add filter policy fpol_prebody_req -rule ns_true -reqAction
      fact_prebody
6  add filter policy fpol_prebody_res -rule ns_true -resAction
      fact_prebody
7  add filter policy fpol_forward_req -rule ns_true -reqAction
      fact_forward_act1
8  bind lb vserver v1 -policyName fpol_forward_req
9  bind cr vserver crv1 -policyName fpol_forward_req
10 #bind filter global fpol_variable_res -state DISABLED
11 bind filter global fpol_prebody_req
12 bind filter global fpol_forward_req
13 add rewrite action nspepi_adv_fact_variable insert_http_header H1 HTTP.
      RES.TXID
14 add rewrite action fact_variable insert_http_header H1 HTTP.REQ.TXID
15 add responder action fact_error_act1 respondwith ”HTTP.REQ.VERSION.
      APPEND(” 200 OK\r
16 nConnection: close\r
17 nContent-Length: 21\r\n\r
18 n<HTML>Good URL</HTML>”)”
19 add rewrite action nspepi_adv_fact_error_act1 replace_http_res ”HTTP.
      REQ.VERSION.APPEND(” 200 OK\r
20 nConnection: close\r
21 nContent-Length: 21\r\n\r
22 n<HTML>Good URL</HTML>”)”
23 add rewrite policy fpol_add_res TRUE fact_add
24 add rewrite policy fpol_error_res TRUE nspepi_adv_fact_error_act1
25 add responder policy fpol_error_req TRUE fact_error_act1
26 add rewrite policy fpol_add_req TRUE fact_add
27 add rewrite policy fpol_variable_req TRUE fact_variable
28 add rewrite policy fpol_variable_res TRUE nspepi_adv_fact_variable
29 set cmp parameter -policyType ADVANCED
```



```
bind rewrite global fpol_add_req 100 NEXT -type REQ_DEFAULT
bind rewrite global fpol_variable_req 200 NEXT -type REQ_DEFAULT
bind rewrite global fpol_add_res 100 NEXT -type RES_DEFAULT
bind rewrite global fpol_error_res 200 NEXT -type RES_DEFAULT
bind rewrite global fpol_variable_res 300 NEXT -type RES_DEFAULT
bind responder global fpol_error_req 100 END -type REQ_DEFAULT
bind lb vserver v1 -policyName fpol_add_res -type RESPONSE -priority
    100 -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_error_res -type RESPONSE -priority
    200 -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_variable_res -type RESPONSE -
    priority 300 -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_add_req -type REQUEST -priority 100
     -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_variable_req -type REQUEST -
    priority 200 -gotoPriorityExpression NEXT
bind lb vserver v1 -policyName fpol_error_req -type REQUEST -priority
    100 -gotoPriorityExpression END
bind cs vserver csv1 -policyName fpol_add_req -type REQUEST -priority
    100 -gotoPriorityExpression NEXT
bind cs vserver csv1 -policyName fpol_add_res -type RESPONSE -priority
    100 -gotoPriorityExpression NEXT
bind cs vserver csv1 -policyName fpol_error_res -type RESPONSE -
    priority 200 -gotoPriorityExpression NEXT
bind cs vserver csv1 -policyName fpol_error_req -type REQUEST -priority
     100 -gotoPriorityExpression END
bind cr vserver crv1 -policyName fpol_add_req -type REQUEST -priority
    100 -gotoPriorityExpression NEXT
bind cr vserver crv1 -policyName fpol_add_res -type RESPONSE -priority
    100 -gotoPriorityExpression NEXT
bind cr vserver crv1 -policyName fpol_error_res -type RESPONSE -
    priority 200 -gotoPriorityExpression NEXT
bind cr vserver crv1 -policyName fpol_error_req -type REQUEST -priority
     100 -gotoPriorityExpression END

<!--NeedCopy-->
```

Konvertieren Sie klassische Filterbefehle in erweiterte Feature-Befehle, wenn vorhandene Rewrite- oder Responder-Richtlinienbindungen den goto Ausdruck END oder USE_INNVOCATION haben

Wenn bei dieser Konvertierung eine Rewriterichtlinie an einen oder mehrere virtuelle Server gebunden ist und der Server über END oder USE_INVOCATION_RESULT verfügt, kommentiert das Tool die

Befehle.

Beispiel

Es folgt ein Beispiel für einen Eingabebefehl:

```
COPY
add filter policy fpol1 -rule ns_true -resAction reset
add filter policy fpol2 -rule ns_true -reqAction reset
add rewrite policy pol1 true NOREWRITE
add rewrite policylabel pl http_res
bind rewrite policylabel pl pol1 1
bind rewrite global NOPOLICY 1 USE_INVOCATION_RESULT -type RES_DEFAULT
    -invoke policylabel pl
add responder policy pol2 true NOOP
add responder policylabel pl -policylabeltype HTTP
bind responder policylabel pl pol2 1
bind responder global NOPOLICY 1 USE_INVOCATION_RESULT -type
    REQ_DEFAULT -invoke policylabel pl
bind lb vserver v1_tcp -policyName pol1 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
bind cs vserver csv1_tcp -policyName pol1 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
bind lb vserver v1_tcp -policyName pol2 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
bind cs vserver csv1_tcp -policyName pol2 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
bind cr vserver crv1_tcp -policyName pol2 -priority 100 -
    gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
bind lb vserver v1_http -policyName fpol1
bind cs vserver csv1_http -policyName fpol1
bind lb vserver v2_http -policyName fpol2
bind cs vserver csv2_http -policyName fpol2
bind cr vserver crv2_http -policyName fpol2
bind filter global fpol1 -priority 100
bind filter global fpol2 -priority 100
<!--NeedCopy-->
```

Es folgt ein Beispiel für einen Ausgabebefehl:

```
COPY
add rewrite policy pol1 true NOREWRITE
```



```
add rewrite policylabel pl http_res
bind rewrite policylabel pl pol1 1
add responder policy pol2 true NOOP
add responder policylabel pl -policylabeltype HTTP
bind responder policylabel pl pol2 1
add rewrite policy fpol1 TRUE RESET
add responder policy fpol2 TRUE RESET
#bind lb vserver v1_http -policyName fpol1 -type RESPONSE
#bind cs vserver csv1_http -policyName fpol1 -type RESPONSE
#bind rewrite global fpol1 100 -type RES_DEFAULT
#bind lb vserver v2_http -policyName fpol2 -type REQUEST
#bind cs vserver csv2_http -policyName fpol2 -type REQUEST
#bind cr vserver crv2_http -policyName fpol2 -type REQUEST
#bind responder global fpol2 100 -type REQ_DEFAULT
bind rewrite global NOPOLICY 1 USE_INVOCATION_RESULT -type RES_DEFAULT
   -invoke policylabel pl
bind responder global NOPOLICY 1 USE_INVOCATION_RESULT -type
   REQ_DEFAULT -invoke policylabel pl
bind lb vserver v1_tcp -policyName pol1 -priority 100 -
   gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
bind lb vserver v1_tcp -policyName pol2 -priority 100 -
   gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
bind cs vserver csv1_tcp -policyName pol1 -priority 100 -
   gotoPriorityExpression USE_INVOCATION_RESULT -type RESPONSE
bind cs vserver csv1_tcp -policyName pol2 -priority 100 -
   gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST
bind cr vserver crv1_tcp -policyName pol2 -priority 100 -
   gotoPriorityExpression USE_INVOCATION_RESULT -type REQUEST-

<!--NeedCopy-->
```

Befehle oder Funktionen, die nicht vom nspepi-Konvertierungstool verarbeitet werden

Im Folgenden sind einige Befehle aufgeführt, die im Rahmen des automatischen Konvertierungsprozesses nicht behandelt werden.

- Einige Bindungen können nicht konvertiert werden, wenn es ein gewisses Überlappen von Prioritäten zwischen globalen und nicht-globalen Bindungspunkten, zwischen Benutzern und Gruppen sowie zwischen Bindungen an verschiedene Entitäten gibt. Bei diesen wurde die betroffene Konfiguration auskommentiert und ein Fehler erzeugt. Solche Konfigurationen müssen manuell umgewandelt werden.
- Sowohl klassische als auch erweiterte Richtlinien können an cmp global gebunden werden. Es gibt viele Fälle, in denen sich die Funktionalität ändert, sobald Classic-Richtlinien in erweiterte

Richtlinien umgewandelt wurden. Wir haben Befehle umgewandelt, die durch das Auskommentieren einiger Richtlinien gelöst werden können. Dennoch gibt es einige Befehle, die nicht konvertiert werden können. In solchen Fällen wird ein Fehler erzeugt und die Konvertierung muss manuell erfolgen.

- Nicht alle Verwendungen von in Classic integrierten benannten Ausdrücken werden in äquivalente erweiterte benannte Ausdrücke umgewandelt.
- Client-Sicherheitsausdrücke werden nicht behandelt.
- Die Option "-precedence" für virtuelle Server für Content Switching und Cache-Umleitung wird nicht behandelt.
- Sicher verbinden (SC)
- Prioritäts-Warteschlange (PQ)
- HTTP-Denial-of-Service-Angriff (HDOS)
- HTML-Einschleusung
- Authentifizierung
- Autorisierung
- VPN
- Syslog
- Nslog
- Dateibasierte Classic-Ausdrücke werden nicht behandelt.

> **Hinweis:**
>
> Für einige Funktionen wie Patclass/filter wird die Befehlssyntax geändert. Wenn es cmd-Richtlinien gibt, müssen die cmd-Richtlinien möglicherweise je nach Kundenanforderung geändert werden.

Bekannte Probleme

Die folgenden Fehler können durch das Tool `nspepi` verursacht werden:

- Wenn beim Konvertieren eines Ausdrucks ein Problem auftritt.
- Wenn ein benannter Richtlinienausdruck den Parameter -clientSecurityMessage verwendet, da dieser Parameter im erweiterten Richtlinienausdruck nicht unterstützt wird.

> **Hinweis:**
>
> Alle klassischen Richtlinienbindungen mit deaktivierter Option -state werden auskommentiert. Die Option -state ist für erweiterte Richtlinienbindungen nicht verfügbar.

Ausführen des nspepi-Tools

Das Folgende ist ein Befehlszeilenbeispiel zum Ausführen des Tools `nspepi`. Dieses Tool wird von der Befehlszeile der Shell aus ausgeführt (Sie müssen den Befehl "Shell" an den NetScaler"CLI" eingeben,

um dorthin zu gelangen). Entweder “-f” oder “-e” muss angegeben werden, um eine Konvertierung durchzuführen. Die Verwendung von “-d” ist für Citrix Mitarbeiter vorgesehen, um sie zu Support-zwecken zu analysieren.

```
usage: nspepi [-h] (-e <classic policy expression> | -f <path to ns
    config file>)[-d] [-v] [-V

Convert classic policy expressions to advanced policy expressions and
    deprecated commands to non-deprecated
commands.

optional arguments:
-h, --help show this help message and exit
-e <classic policy expression>, --expression <classic policy expression
    >
convert classic policy expression to advanced policy
expression (maximum length of 8191 allowed)
-f <path to ns config file>, --infile <path to ns config file>
convert netscaler config file
-d, --debug log debug output
-v, --verbose show verbose output
-V, --version show program's version number and exit
<!--NeedCopy-->
```

Beispiele für die Verwendung:

1. `nspepi -e ”req.tcp.destport == 80”`
2. `nspepi -f ns.conf`

Im Folgenden finden Sie einige Beispiele für das Ausführen des Tools `nspepi` über die CLI

Beispielausgabe für den Parameter —e:

```
root@ns# nspepi -e ”req.http.header foo == ”bar””
”HTTP.REQ.HEADER(”foo”).EQ(”bar”)”
<!--NeedCopy-->
```

Beispielausgabe für den Parameter -f:

```
root@ns# cat sample.conf
add cr vserver cr_vs HTTP -cacheType TRANSPARENT -cltTimeout 180 -
    originUSIP OFF
```



```
3 add cr policy cr_pol1 -rule ns_true
4 bind cr vserver cr_vs -policyName cr_pol1
5 <!--NeedCopy-->
```

Ausführen von nspepi mit dem Parameter -f:

```
1 nspepi -f sample.conf
2 <!--NeedCopy-->
```

Die konvertierte Konfiguration ist in einer neuen Datei verfügbar `new_sample.conf`.
Überprüfen Sie die Datei `warn_sample.conf` auf Warnungen oder Fehler, die möglicherweise generiert wurden.

Beispielausgabe des Parameters -f zusammen mit dem Parameter -v

```
1 nspepi -f sample.conf -v
2 INFO - add cr vserver cr_vs HTTP -cacheType TRANSPARENT -cltTimeout 180
      -originUSIP OFF
3 INFO - add cr policy cr_pol1 -rule TRUE -action ORIGIN
4 INFO - bind cr vserver cr_vs -policyName cr_pol1 -priority 100 -
     gotoPriorityExpression END -type REQUEST
5 <!--NeedCopy-->
```

Die konvertierte Konfiguration ist in einer neuen Datei verfügbar `new_sample.conf`.
Überprüfen Sie die Datei `warn_sample.conf` auf Warnungen oder Fehler, die möglicherweise generiert wurden.

Konvertierte Config-Datei:

```
1 root@ns# cat new_sample.conf
2 add cr vserver cr_vs HTTP -cacheType TRANSPARENT -cltTimeout 180 -
     originUSIP OFF
3 add cr policy cr_pol1 -rule TRUE -action ORIGIN
4 set cmp parameter -policyType ADVANCED
5 bind cr vserver cr_vs -policyName cr_pol1 -priority 100 -
     gotoPriorityExpression END -type REQUEST
6
7 <!--NeedCopy-->
```

Beispielausgabe einer Beispielkonfiguration ohne Fehler oder Warnungen:


```
nspepi -f sample_2.conf
<!--NeedCopy-->
```

Die konvertierte Konfiguration ist in einer neuen Datei verfügbar `new_sample_2.conf`.
Überprüfen Sie die Datei `warn_sample_2.conf` auf Warnungen oder Fehler, die möglicherweise generiert wurden.

Beispielausgabe einer Beispielkonfiguration mit Warnungen:

```
root@ns# cat sample_2.conf
add policy expression security_expr ”req.tcp.destport == 80” -
    clientSecurityMessage ”Not allowed”
set cmp parameter -policyType CLASSIC
add cmp policy cmp_pol1 -rule ns_true -resAction COMPRESS
add cmp policy cmp_pol2 -rule ns_true -resAction COMPRESS
add cmp policy cmp_pol3 -rule TRUE -resAction COMPRESS
bind cmp global cmp_pol1
bind cmp global cmp_pol2 -state DISABLED
bind cmp global cmp_pol3 -priority 1 -gotoPriorityExpression END -type
    RES_DEFAULT
bind lb vserver lb_vs -policyName cmp_pol2
root@ns#
<!--NeedCopy-->
```

Beispiel für das Ausführen von nspepi mit dem Parameter -f:

```
root@ns# nspepi -f sample_2.conf
ERROR - Error in converting expression security_expr : conversion of
    clientSecurityMessage based expression is not supported.
WARNING - Following bind command is commented out because state is
    disabled. Advanced expressions only have a fixed ordering of the
    types of bindings without interleaving, except that global bindings
    are allowed before all other bindings and after all bindings. If you
     have global bindings in the middle of non-global bindings or any
    other interleaving then you will need to reorder all your bindings
    for that feature and direction. Refer to nspepi documentation. If
    command is required please take a backup because comments will not
    be saved in ns.conf after triggering 'save ns config': bind cmp
    global cmp_pol2 -state DISABLED
Warning - Bindings of advanced CMP policies to cmp global are commented
     out, because initial global cmp parameter is classic but advanced
    policies are bound. Now global cmp parameter policy type is set to
```



```
    advanced. If commands are required please take a backup because
    comments will not be saved in ns.conf after triggering 'save ns
    config'. Advanced expressions only have a fixed ordering of the
    types of bindings without interleaving, except that global bindings
    are allowed before all other bindings and after all bindings. If you
     have global bindings in the middle of non-global bindings or any
    other interleaving then you will need to reorder all your bindings
    for that feature and direction. Refer to nspepi documentation.
root@ns#
<!--NeedCopy-->
```

Konvertierte Datei:

```
root@ns# cat new_sample_2.conf
add policy expression security_expr ”req.tcp.destport == 80” -
    clientSecurityMessage ”Not allowed”
set cmp parameter -policyType ADVANCED
add cmp policy cmp_pol1 -rule TRUE -resAction COMPRESS
add cmp policy cmp_pol2 -rule TRUE -resAction COMPRESS
add cmp policy cmp_pol3 -rule TRUE -resAction COMPRESS
#bind cmp global cmp_pol2 -state DISABLED
#bind cmp global cmp_pol3 -priority 1 -gotoPriorityExpression END -type
     RES_DEFAULT
bind cmp global cmp_pol1 -priority 100 -gotoPriorityExpression END -
    type RES_DEFAULT
bind lb vserver lb_vs -policyName cmp_pol2 -priority 100 -
    gotoPriorityExpression END -type RESPONSE
root@ns#
<!--NeedCopy-->
```

Warn-Datei:

```
root@ns# cat warn_sample_2.conf
2019-02-28 06:20:10,590: ERROR - Error in converting expression
    security_expr : conversion of clientSecurityMessage based expression
     is not supported.
2019-02-28 06:20:12,187: WARNING - Following bind command is commented
    out because state is disabled. Advanced expressions only have a
    fixed ordering of the types of bindings without interleaving, except
     that global bindings are allowed before all other bindings and
    after all bindings. If you have global bindings in the middle of non
    -global bindings or any other interleaving then you will need to
```



```
      reorder all your bindings for that feature and direction. Refer to
      nspepi documentation. If command is required please take a backup
      because comments will not be saved in ns.conf after triggering 'save
       ns config': bind cmp global cmp_pol2 -state DISABLED
4 2019-02-28 06:20:12,191: WARNING - Bindings of advanced CMP policies to
       cmp global are commented out, because initial global cmp parameter
      is classic but advanced policies are bound. Now global cmp parameter
       policy type is set to advanced. If commands are required please
      take a backup because comments will not be saved in ns.conf after
      triggering 'save ns config'. Advanced expressions only have a fixed
      ordering of the types of bindings without interleaving, except that
      global bindings are allowed before all other bindings and after all
      bindings. If you have global bindings in the middle of non-global
      bindings or any other interleaving then you will need to reorder all
       your bindings for that feature and direction. Refer to nspepi
      documentation.
5 root@ns#
6 <!--NeedCopy-->
```

Verbindliche Prioritäten

Erweiterte Richtlinien erlauben kein willkürliches Interleaving nach Priorität zwischen global und nicht-global sowie zwischen verschiedenen Bindungstypen. Wenn Sie sich auf ein solches Interleaving von Classic-Richtlinienprioritäten verlassen, müssen Sie die Prioritäten anpassen, um den erweiterten Richtlinienregeln zu entsprechen und das gewünschte Verhalten zu erzielen.
Prioritäten in erweiterten Richtlinien sind lokal an einem Bindepunkt. Ein Bindepunkt ist eine eindeutige Kombination aus Protokoll, Feature, Richtung und Entität (Entitäten sind bestimmte virtuelle Server, Benutzer, Gruppen, Dienste und entweder globale Überschreibung oder globale Standardeinstellung). Politische Prioritäten werden nicht über Bindepunkte hinweg befolgt.

Für ein bestimmtes Protokoll, eine bestimmte Funktion und eine bestimmte Richtung ist die Reihenfolge der Bewertung von erweiterten Richtlinien unten angegeben:

- Globale Überschreibung.
- (Aktueller) Authentifizierungs-, Autorisierungs- und Überwachungsbenutzer.
- Authentifizierungs-, Autorisierungs- und Überwachungsgruppen (bei denen der Benutzer Mitglied ist) in der Reihenfolge des Gewichts - die Reihenfolge ist nicht definiert, wenn zwei oder mehr Gruppen das gleiche Gewicht haben.
- Virtueller LB-Server, auf dem entweder die Anforderung empfangen wurde oder der Content Switching ausgewählt hat.
- Virtueller Content Switching-Server, virtueller Cache-Umleitungsserver, auf dem die Anforderung empfangen wurde.

- Durch Load Balancing ausgewählter Dienst.
- Globale Standardeinstellung.

Für die Bewertung der Autorisierungsrichtlinie lautet die Reihenfolge:

- Systeme überschreiben.
- Virtueller Lastausgleichsserver, auf dem entweder die Anforderung empfangen wurde oder der CS ausgewählt hat.
- Virtueller Content Switching-Server, auf dem die Anforderung empfangen wurde.
- Standardeinstellung des Systems.

Innerhalb jedes Bindepunkts werden die Richtlinien in der Reihenfolge ihrer Priorität von der niedrigsten bis zur höchsten Nummerierung ausgewertet. Richtlinien werden nur für das verwendete Protokoll und die Richtung ausgewertet, von der die Nachricht empfangen wurde.

Klassische Richtlinienbindungen, die eine manuelle Neupriorisierung erfordern

Hier sind einige Arten von Classic-Richtlinienbindungen, die eine manuelle Neupriorisierung erfordern, um Ihre Anforderungen zu erfüllen. All dies ist für ein bestimmtes Merkmal und die Richtung.

- Klassische Prioritäten, die die Prioritätszahl gegenüber der Richtung der oben genannten Entitätstyplisten erhöhen. Zum Beispiel ist eine Bindung eines virtuellen Content Switching-Servers niedriger als eine Bindung eines virtuellen Lastausgleichsservers.
- Klassische Prioritäten, die mit Authentifizierungs-, Autorisierungs- und Überwachungsgruppen überlappen. Ein Teil einer Gruppe steht vor einer anderen Gruppe und ein weiterer Teil ist hinter einem Teil dieser anderen Gruppe her.
- Klassische Prioritäten, deren Anzahl außer der Reihenfolge der Gewichtungen von Authentifizierungs-, Autorisierungs- und Überwachungsgruppen zunimmt.
- Klassische globale Prioritäten, die weniger als einige nicht-globale Priorität und dieselben globalen Prioritäten sind größer als einige andere nicht-globale Priorität (d. h. jedes Segment von Prioritäten, das eine nicht-globale Priorität ist, gefolgt von einem oder mehreren Globals, gefolgt von einem nicht-globalen).

Häufig gestellte Fragen zur Standardrichtlinienveraltung

October 5, 2021

- **Welche klassischen Richtlinien sind ab Citrix ADC ab Version 12.0 veraltet?**

  Alle Funktionen und Funktionen, die in der Tabelle “ Veraltete Richtlinien “ erwähnt werden, sind von Citrix ADC Release 12.0 Build 56.20 veraltet. Citrix empfiehlt Ihnen, die folgenden Tabellen

(im PDF-Format) für veraltete Feature- und Richtliniendetails anzuzeigen.

- Tabelle 1 für veraltete Richtlinien und ihre Alternative.
- Tabelle 2 für veraltete Citrix ADC-Funktionalitäten und ihre Alternative mit Konfigurationsdetails.

- **Wie kann ich klassische richtlinienbasierte Funktionen und Funktionen in Advanced Policy konvertieren?**

  Sie können das proprietäre `nspepi` Tool von Citrix ADC verwenden, um Befehle, Ausdrücke und Konfigurationen zu konvertieren. `nspepi` -Tool hilft dabei, alle klassischen Ausdrücke in der Citrix ADC-Konfiguration in die erweiterten Richtlinienausdrücke zu konvertieren. Weitere Informationen zum `nspepi` Tool finden Sie unter Konvertieren von Richtlinienausdrücken mit dem NSPEPI-Tool.

- **Aus welcher Version sind klassische richtlinienbasierte Funktionen und Funktionalitäten veraltet?**

  Citrix ADC 12.0 Build 56.20 und höher.

- **Welche Schritte müssen ausgeführt werden, wenn ich meine Appliance auf einen Build aktualisiere, der die klassischen richtlinienbasierten Funktionen nicht unterstützt?**

  Citrix empfiehlt, erweiterte Richtlinien zu verwenden, bevor Sie Ihre Appliance auf Releases später als Citrix ADC Release 13.0 aktualisieren. Weitere Informationen finden Sie unter Erweiterte Richtlinien.

- **Wie lange werden die veralteten Funktionen auf einer Citrix ADC Appliance unterstützt?**

  Citrix wird die klassische Richtlinie und ihre Verwendung in Releases später als Citrix ADC Release 13.0 nicht unterstützen.

- **Muss ich meine Appliance neu starten, nachdem ich die Konfigurationsdatei konvertiert habe?**

  Ja, Sie müssen die Citrix ADC-Instanz nach erfolgreicher Konvertierung der `ns.config` Datei neu starten.

Bevor Sie fortfahren

October 5, 2021

Stellen Sie vor der Konfiguration von Ausdrücken und Richtlinien sicher, dass Sie die relevante Citrix ADC Funktion und die Struktur Ihrer Daten folgendermaßen kennen:

- Lesen Sie die Dokumentation zu der entsprechenden Funktion.

- Suchen Sie im Datenstrom nach dem Datentyp, den Sie konfigurieren möchten.

Möglicherweise möchten Sie eine Ablaufverfolgung für den Typ des Datenverkehrs oder Inhalts ausführen, den Sie konfigurieren möchten. Dies gibt Ihnen eine Vorstellung von den Parametern und Werten sowie Operationen für diese Parameter und Werte, die Sie in einem Ausdruck angeben müssen.

Hinweis: Citrix ADC unterstützt entweder klassische oder erweiterte Richtlinien innerhalb eines Features. Sie können nicht beide Typen im selben Feature haben. In den letzten Versionen wurden einige Citrix ADC Funktionen von der Verwendung klassischer Richtlinien und Ausdrücke zu erweiterten Richtlinien und Ausdrücken migriert. Wenn eine für Sie interessante Funktion in das Richtlinienformat Erweitert geändert wurde, müssen Sie die älteren Informationen möglicherweise manuell migrieren. Im Folgenden finden Sie Richtlinien für die Entscheidung, ob Sie Ihre Richtlinien migrieren müssen:

- Wenn Sie klassische Richtlinien in einer Version des integrierten Caching-Features vor Version 9.0 konfiguriert haben und dann auf Version 9.0 oder höher aktualisieren, haben Sie keine Auswirkungen. Alle Legacy-Richtlinien werden in das erweiterte Richtlinienformat migriert.
- Bei anderen Features müssen Sie klassische Richtlinien und Ausdrücke manuell in die erweiterte Syntax migrieren, wenn das Feature zur erweiterten Richtlinie migriert wurde.

Konfigurieren der erweiterten Richtlinieninfrastruktur

October 5, 2021

Sie können erweiterte Richtlinien für verschiedene Citrix ADC Funktionen erstellen, einschließlich DNS, Rewrite, Responder und Integrated Caching sowie die clientlose Zugriffsfunktion im Citrix Gateway. Richtlinien steuern das Verhalten dieser Features.

Wenn Sie eine Richtlinie erstellen, weisen Sie ihr einen Namen, eine Regel (einen Ausdruck), Feature-spezifische Attribute und eine Aktion zu, die ausgeführt wird, wenn Daten mit der Richtlinie übereinstimmen. Nach dem Erstellen der Richtlinie bestimmen Sie, wann sie aufgerufen wird, indem Sie sie global binden oder entweder an die Anforderungs- oder Antwortzeitverarbeitung für einen virtuellen Server.

Richtlinien, die denselben Bindepunkt haben, werden als *Richtlinienbank* bezeichnet. Beispielsweise bilden alle Richtlinien, die an einen virtuellen Server gebunden sind, die Richtlinienbank für den virtuellen Server. Wenn Sie die Richtlinie binden, weisen Sie ihr eine Prioritätsstufe zu, um anzugeben, wann sie im Verhältnis zu anderen Richtlinien in der Bank aufgerufen wird. Zusätzlich zur Zuweisung einer Prioritätsstufe können Sie eine beliebige Evaluierungsreihenfolge für Richtlinien in einer Bank konfigurieren, indem Sie Goto-Ausdrücke angeben.

Zusätzlich zu den Richtlinienbanken, die einem integrierten Bindpunkt oder einem virtuellen Server zugeordnet sind, können Sie *Richtlinienbeschriftungen* konfigurieren. Ein Policy-Label ist eine Richtlinienbank, die durch einen beliebigen Namen identifiziert wird. Sie rufen eine Richtlinienbezeichnung und die darin dargestellten Richtlinien von einer globalen oder virtuell-serverspezifischen Richtlinienbank auf. Ein Policy-Label oder eine Virtual-Server-Richtlinienbank kann von mehreren Richtlinienbanken aufgerufen werden.

Für einige Features können Sie den Richtlinien-Manager verwenden, um Richtlinien zu konfigurieren und zu binden.

Regeln für Namen in Bezeichnern, die in Richtlinien verwendet werden

October 5, 2021

Die ID-Namen in den benannten Ausdruck, HTTP-Callout, Mustersatz und Ratenbegrenzungsfunktionen müssen mit einem ASCII-Alphabet oder einem Unterstrich (_) beginnen. Die verbleibenden Zeichen können alphanumerische ASCII-Zeichen oder Unterstriche (_) sein.

Die Namen dieser Bezeichner dürfen nicht mit den folgenden reservierten Wörtern beginnen:

- Die Wörter ALT, TRUE oder FALSE oder der Einzeichen-Bezeichner Q oder S.
- Der spezielle Syntaxindikator RE (für reguläre Ausdrücke) oder XP (für XPath-Ausdrücke).
- Ausdruckspräfixe, die derzeit die folgenden sind:
  - CLIENT
  - EXTEND
  - HTTP
  - SERVER
  - SYS
  - TARGET
  - Text
  - URL
  - MYSQL
  - MSSQL

Darüber hinaus dürfen die Namen dieser Bezeichner nicht mit den Namen von Enumerierungskonstanten übereinstimmen, die in der Richtlinieninfrastruktur verwendet werden. Beispielsweise kann der Name eines Bezeichners nicht IGNORECASE, YEAR oder LATIN2_CZECH_CS (ein MySQL Zeichensatz) sein.

Hinweis: Die Citrix ADC Appliance führt einen Vergleich von Bezeichnern mit diesen Wörtern und Enumerierungskonstanten durch. Beispielsweise können Namen der Bezeichner nicht mit TRUE, TRUE

oder TRUE beginnen.

Erstellen oder Ändern einer Richtlinie

October 8, 2021

Alle Richtlinien haben einige gemeinsame Elemente. Das Erstellen einer Richtlinie besteht zumindest darin, die Richtlinie zu benennen und eine Regel zu konfigurieren. Die Richtlinienkonfigurationstools für die verschiedenen Features weisen Überlappungsbereiche auf, aber auch Unterschiede auf. Weitere Informationen zum Konfigurieren einer Richtlinie für ein bestimmtes Feature, einschließlich der Zuordnung einer Aktion mit der Richtlinie, finden Sie in der Dokumentation des Features.

Um eine Richtlinie zu erstellen, legen Sie zunächst den Zweck der Richtlinie fest. Beispielsweise können Sie eine Richtlinie definieren, die HTTP-Anforderungen für Bilddateien identifiziert, oder Clientanforderungen, die ein SSL-Zertifikat enthalten. Sie müssen nicht nur den Informationstyp kennen, mit dem die Richtlinie arbeiten soll, sondern auch das Format der Daten kennen, die von der Richtlinie analysiert werden.

Bestimmen Sie als Nächstes, ob die Richtlinie global anwendbar ist oder ob sie sich auf einen bestimmten virtuellen Server bezieht. Berücksichtigen Sie auch die Auswirkung, die die Reihenfolge, in der Ihre Richtlinien ausgewertet werden (die durch die Bindung der Richtlinien bestimmt wird) auf die Richtlinie hat, die Sie konfigurieren möchten.

Erstellen einer Richtlinie mit der CLI

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

```
1 -  add responder|dns|cs|rewrite|cache policy <policyName> -rule <
     expression> [<feature-specific information>]
2
3 -  show rewrite policy <name>
4 <!--NeedCopy-->
```

Beispiel 1:

```
1 add rewrite policy "pol_remove-ae" true "act_remove-ae"
2 Done
3 > show rewrite policy pol_remove-ae
```



```
            Name: pol_remove-ae
            Rule: true
            RewriteAction: act_remove-ae
            UndefAction: Use Global
            Hits: 0
            Undef Hits: 0
            Bound to: GLOBAL RES_OVERRIDE
            Priority: 90
            GotoPriorityExpression: END
Done
<!--NeedCopy-->
```

Beispiel 2:

```
add cache policy BranchReportsCachePolicy -rule q{
 http.req.url.query.value(”actionoverride”).contains(”branchReport s”)
    }
  -action cache
Done
show cache policy BranchReportsCachePolicy
            Name: BranchReportsCachePolicy
            Rule: http.req.url.query.value(”actionoverride”).contains(”
               branchReports”)
            CacheAction: CACHE
            Stored in group: DEFAULT
            UndefAction: Use Global
            Hits: 0
            Undef Hits: 0
Done
<!--NeedCopy-->
```

Hinweis: In der Befehlszeile müssen Anführungszeichen innerhalb einer Richtlinienregel (dem Ausdruck) maskiert oder durch das Trennzeichen q getrennt werden. Weitere Informationen finden Sie unter Konfigurieren von erweiterten Richtlinienausdrücken: Erste Schritte.

Erstellen oder Ändern einer Richtlinie mit der GUI

1. Erweitern Sie im Navigationsbereich den Namen des Features, für das Sie eine Richtlinie konfigurieren möchten, und klicken Sie dann auf **Richtlinien**. Sie können beispielsweise **Content Switching, Integriertes Caching, DNS, Umschreiben oder Responder** auswählen.
2. Klicken Sie im Detailbereich auf **Hinzufügen**, oder wählen Sie eine vorhandene Richtlinie aus, und klicken Sie auf **Öffnen**. Ein Dialogfeld zur Richtlinienkonfiguration wird angezeigt.

3. Geben Sie Werte für die folgenden Parameter an. (Ein Sternchen gibt einen erforderlichen Parameter an. Für einen Begriff in Klammern finden Sie im entsprechenden Parameter unter Parameter zum Erstellen oder Ändern einer Richtlinie.)
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.
5. Klicken Sie auf **Speichern**. Eine Richtlinie wird hinzugefügt.
   Hinweis: Nachdem Sie eine Richtlinie erstellt haben, können Sie die Details der Richtlinie anzeigen, indem Sie im Konfigurationsbereich auf den Richtlinieneintrag klicken. Details, die hervorgehoben und unterstrichen sind, sind Links zu der entsprechenden Entität (z. B. einem benannten Ausdruck).

Beispiele für Richtlinienkonfiguration

October 5, 2021

In diesen Beispielen wird gezeigt, wie Richtlinien und die zugehörigen Aktionen an der Befehlszeilenschnittstelle eingegeben werden. Im Konfigurationsdienstprogramm werden die Ausdrücke im Fenster Ausdruck des Dialogfelds Feature-Konfiguration für das integrierte Cache- oder Rewrite-Feature angezeigt.

Es folgt ein Beispiel für die Erstellung einer Caching-Richtlinie. Beachten Sie, dass Aktionen zum Zwischenspeichern von Richtlinien integriert sind, sodass Sie sie nicht getrennt von der Richtlinie konfigurieren müssen.

```
1   add cache policy BranchReportsCachePolicy -rule q{
2  http.req.url.query.value(”actionoverride”).contains(”branchReports”) }
3   -action cache
4 <!--NeedCopy-->
```

Es folgt ein Beispiel für eine Richtlinie zum Umschreiben und eine Aktion:

```
1  add rewrite action myAction1 INSERT_HTTP_HEADER ”myHeader” ”
      valueForMyHeader”
2  add rewrite policy myPolicy1 ”http.req.url.contains(”myURLstring”)”
      myAction1
3 <!--NeedCopy-->
```

Hinweis: In der Befehlszeile müssen Anführungszeichen innerhalb einer Richtlinienregel (dem Ausdruck) maskiert oder durch das Trennzeichen q getrennt werden. Weitere Informationen finden Sie unter Konfigurieren von erweiterten Richtlinienausdrücken: Erste Schritte.

Konfigurieren und Binden von Richtlinien mit dem Richtlinien-Manager

October 8, 2021

> **Warnung:**
>
> Klassische Richtlinienausdrücke werden ab Citrix ADC 12.0 Build 56.20 nicht mehr unterstützt. Alternativ empfiehlt Citrix die Verwendung von erweiterten Richtlinien. Weitere Informationen finden Sie unter Erweiterte Richtlinien.

Einige Anwendungen bieten einen spezialisierten Policy Manager im Citrix ADC Konfigurationsprogramm, um die Konfiguration von Richtlinienbanken zu vereinfachen. Außerdem können Sie Richtlinien und Aktionen finden und löschen, die nicht verwendet werden.

Der Richtlinien-Manager ist derzeit für die Funktionen Umschreiben, Integriertes Caching, Responder und Komprimierung verfügbar.

Im Folgenden finden Sie Tastenkombinationen für die Prozeduren in diesem Abschnitt:

- Um eine Zelle im Richtlinien-Manager zu bearbeiten, können Sie eine Tabulatortaste zu der Zelle und auf F2 klicken oder die Leertaste auf der Tastatur drücken.
- Um einen Eintrag in einem Dropdownmenü auszuwählen, können Sie mit der Tabulatortaste zu dem Eintrag wechseln, die Leertaste drücken, um das Dropdownmenü anzuzeigen, mit den NACH-OBEN-TASTE und NACH-UNTEN-TASTE zu dem gewünschten Eintrag zu navigieren, und erneut die Leertaste drücken, um den Eintrag auszuwählen.
- Um eine Auswahl in einem Dropdownmenü abzubrechen, drücken Sie die Escape-Taste.
- Um eine Richtlinie einzufügen, klicken Sie auf die Zeile oberhalb der Einfügemarke, und drücken Sie Steuerelement + Einfügen, oder klicken Sie auf Richtlinie einfügen.
- Um eine Richtlinie zu entfernen, klicken Sie auf die Zeile, die die Richtlinie enthält, und drücken Sie die Entf-Taste.

Hinweis: Beachten Sie, dass Citrix ADC beim Löschen der Richtlinie die Goto Expression-Werte anderer Richtlinien in der Bank durchsucht. Wenn einer dieser Werte Gehe zu Ausdrücke der Prioritätsstufe der gelöschten Richtlinie entspricht, werden sie entfernt.

Konfigurieren von Richtlinienbindungen mithilfe des Richtlinienmanagers

1. Klicken Sie im Navigationsbereich auf das Feature, für das Sie Richtlinien konfigurieren möchten. Die Optionen sind Responder, Integriertes Caching, Rewrite oder Compression.
2. Klicken Sie im Detailbereich auf **Richtlinien-Manager**.
3. Wenn Sie klassische Richtlinienbindungen für die Komprimierung konfigurieren, klicken Sie im Dialogfeld Komprimierungsrichtlinien-Manager auf **Zur klassischen Syntax wechseln**. Das Dialogfeld wechselt zur klassischen Syntaxansicht und zeigt die Schaltfläche Zu erweiterten

Richtlinien wechseln an. Wenn Sie Bindungen für Richtlinien konfigurieren möchten, die die erweiterte Richtlinie verwenden, klicken Sie jederzeit, bevor Sie die Konfiguration von Richtlinienbindungen abgeschlossen haben, auf die Schaltfläche Zu erweiterten Richtlinien wechseln.

4. Wenn Sie für andere Features als Responder den Bindepunkt angeben möchten, klicken Sie auf Anfrage oder Antwort, und klicken Sie dann auf einen der Anforderungs- oder Antwortzeit-Bindungspunkte. Die Optionen sind Override Global, LB Virtual Server, CS Virtual Server, Standard Global oder Policy Label. Wenn Sie den Responder konfigurieren, sind die Flow-Typen Request und Response nicht verfügbar.
5. Um eine Richtlinie an diesen Bindepunkt zu binden, klicken Sie auf Richtlinie einfügen, und wählen Sie eine zuvor konfigurierte Richtlinie, ein NOPOLICY-Label oder die Option Neue Richtlinie aus. Je nach ausgewählter Option haben Sie die folgenden Möglichkeiten:
   - **Neue Richtlinie:** Erstellen Sie die Richtlinie wie unter "Richtlinie erstellen oder ändern" beschrieben, und konfigurieren Sie dann die Prioritätsstufe, den GoTo-Ausdruck und den Richtlinienaufruf, wie in der Tabelle beschrieben, "Format jedes Eintrags in einer Richtlinienbank. "
   - **Bestehende Richtlinie**, **NOPOLICY**, oder `NOPOLICY\<feature name\>`: Konfigurieren Sie die Prioritätsstufe, den GoTo-Ausdruck und den Richtlinienaufruf wie in der Tabelle beschrieben "Format jedes Eintrags in einer Richtlinienbank. " Die **NOPOLICY-** oder `NOPOLICY\<feature name\>` Optionen sind nur für Richtlinien verfügbar, die erweiterte Richtlinien verwenden.
6. Wiederholen Sie die vorstehenden Schritte, um dieser Richtlinienbank Einträge hinzuzufügen.
7. Um die Prioritätsstufe für einen Eintrag zu ändern, können Sie einen der folgenden Schritte ausführen:
   - Doppelklicken Sie auf das Feld Priorität für einen Eintrag, und bearbeiten Sie den Wert.
   - Klicken Sie auf eine Richtlinie, und ziehen Sie sie in eine andere Zeile in der Tabelle.
   - Klicken Sie auf Prioritäten neu generieren.

   In allen drei Fällen werden die Prioritätsstufen aller anderen Richtlinien nach Bedarf geändert, um dem neuen Wert Rechnung zu tragen. Gehe zu Ausdrücke mit ganzzahligen Werten werden ebenfalls automatisch aktualisiert. Wenn Sie beispielsweise einen Prioritätswert von 10 in 100 ändern, werden alle Richtlinien mit dem Wert Gehe zu Ausdruck von 10 auf den Wert 100 aktualisiert.
8. Um den Richtlinien-, Aktions- oder Richtlinienbankaufruf für eine Zeile in der Tabelle zu ändern, klicken Sie auf den Pfeil nach unten rechts neben dem Eintrag, und führen Sie eine der folgenden Aktionen aus:
   - Um die Richtlinie zu ändern, wählen Sie einen anderen Richtliniennamen aus oder wählen Sie Neue Richtlinie aus und führen Sie die Schritte unter Richtlinie erstellen oder ändernaus.

- Um den Springen-Ausdruck zu ändern, wählen Sie Weiter, Ende, USE_INVOCATION_RESULT, oder wählen Sie mehr aus, und geben Sie einen Ausdruck ein, dessen Ergebnis die Prioritätsstufe eines anderen Eintrags in dieser Richtlinienbank zurückgibt.
- Um einen Aufruf zu ändern, wählen Sie eine vorhandene Richtlinienbank aus, oder klicken Sie auf Neues Policy Label, und führen Sie die Schritte unter Richtlinie an eine Richtlinienbezeichnung bindenaus.

9. Um die Bindung einer Richtlinie oder eines Richtlinienbezeichnungsaufrufs von dieser Bank aufzuheben, klicken Sie auf ein beliebiges Feld in der Zeile, das die Richtlinie oder die Richtlinienbezeichnung enthält, und klicken Sie dann auf Richtlinie aufheben.
10. Wenn Sie fertig sind, klicken Sie auf Änderungen übernehmen. Eine Meldung in der Statusleiste zeigt an, dass die Richtlinie erfolgreich gebunden ist.

Entfernen nicht verwendeter Richtlinien mithilfe des Richtlinien-Managers

1. Klicken Sie im Navigationsbereich auf das Feature, für das Sie die Richtlinienbank konfigurieren möchten. Die Optionen sind Responder, Integriertes Caching oder Rewrite.
2. Klicken Sie im Detailbereich auf den Richtlinienmanager für <Feature Name>.
3. Klicken Sie im Dialogfeld **Feature-Name** > **Richtlinie verwalten**r auf **Bereinigungskonfiguration**.
4. Wählen Sie im Dialogfeld **Bereinigungskonfiguration** die Elemente aus, die Sie löschen möchten, und klicken Sie dann auf **Entfernen**.
5. Klicken Sie im Dialogfeld Entfernen auf **Ja**.
6. Klicken Sie auf **Schließen**. Eine Meldung in der Statusleiste zeigt an, dass die Richtlinie erfolgreich entfernt wurde.

Bindung einer Richtlinie aufheben

October 5, 2021

Wenn Sie eine Richtlinie neu zuweisen oder löschen möchten, müssen Sie zunächst die Bindung entfernen.

Aufheben der Bindung einer integrierten Caching-, Umschreibe- oder Komprimierungsrichtlinie weltweit mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine integrierte Caching-, Umschreibe- oder Komprimierungsrichtlinie global aufzuheben und die Konfiguration zu überprüfen:


```
- unbind cache|rewrite|cmp global <policyName> [-type req_override|
   req_default|res_override|res_default] [-priority <positiveInteger>]

- show cache|rewrite|cmp global
<!--NeedCopy-->
```

Beispiel:

```
> unbind cache global_nonPostReq
Done
> show cache global
    1)      Global bindpoint: REQ_DEFAULT
            Number of bound policies: 1

    2)      Global bindpoint: RES_DEFAULT
            Number of bound policies: 1

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

Die Priorität ist nur für die Richtlinie Dummy mit dem Namen NOPOLICY erforderlich.

Aufheben der Bindung einer Responder-Richtlinie global mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Bindung einer Responder-Richtlinie global aufzuheben und die Konfiguration zu überprüfen:

```
- unbind responder global <policyName> [-type override|default] [-
   priority <positiveInteger>]

- show responder global
<!--NeedCopy-->
```

Beispiel:

```
> unbind responder global pol404Error
Done
> show responder global
```



```
4      1)      Global bindpoint: REQ_DEFAULT
5              Number of bound policies: 1
6  Done
7  <!--NeedCopy-->
```

Die Priorität ist nur für die Richtlinie Dummy mit dem Namen NOPOLICY erforderlich.

Bindung einer DNS-Richtlinie global mit der CLI aufheben

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Bindung einer DNS-Richtlinie global aufzuheben und die Konfiguration zu überprüfen:

```
1  -  unbind responder global <policyName>
2
3  -  unbind responder global
4  <!--NeedCopy-->
```

Beispiel:

```
1  unbind dns global dfgdfg
2  Done
3  show dns global
4      Policy name : dfgdfggfhg
5              Priority : 100
6              Goto expression : END
7  Done
8  <!--NeedCopy-->
```

Aufheben der Bindung einer erweiterten Richtlinie von einem virtuellen Server mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Bindung einer erweiterten Richtlinie von einem virtuellen Server zu lösen und die Konfiguration zu überprüfen:

```
1  -  unbind cs vserver <name> -policyName <policyName> [-priority <
       positiveInteger>] [-type REQUEST|RESPONSE]
2
3  -  show lb vserver <name>
4  <!--NeedCopy-->
```


Beispiel:

```
unbind cs vserver vs-cont-switch  -policyName pol1
Done
> show cs vserver vs-cont-switch
            vs-cont-switch (10.102.29.10:80) - HTTP Type: CONTENT
            State: UP
            Last state change was at Wed Aug 19 08:56:55 2009 (+18 ms)
            Time since last state change: 0 days, 02:47:55.750
            Client Idle Timeout: 180 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            Port Rewrite : DISABLED
            State Update: DISABLED
            Default:        Content Precedence: RULE
            Vserver IP and Port insertion: OFF
            Case Sensitivity: ON
            Push: DISABLED  Push VServer:
            Push Label Rule: none
Done
<!--NeedCopy-->
```

Die Priorität ist nur für die Richtlinie Dummy mit dem Namen NOPOLICY erforderlich.

Aufheben der Bindung einer integrierten Caching-, Responder-, Rewrite- oder Komprimierungsrichtlinie Advanced Policy global mit der GUI

1. Klicken Sie im Navigationsbereich auf das Feature mit der Richtlinie, die Sie aufheben möchten (z. B. Integrated Caching)
2. Klicken Sie im Detailbereich auf den Richtlinienmanager für <Feature Name>.
3. Wählen Sie im Dialogfeld **Richtlinien-Manager** den Bindepunkt mit der Richtlinie aus, die Sie aufheben möchten, z. B. Advanced Global.
4. Klicken Sie auf den Richtliniennamen, den Sie die Bindung aufheben möchten, und klicken Sie dann auf Richtlinie aufheben.
5. Klicken Sie auf **Änderungen übernehmen**.
6. Klicken Sie auf **Schließen**. Eine Meldung in der Statusleiste zeigt an, dass die Richtlinie erfolgreich aufgehoben wurde.

Bindung einer DNS-Richtlinie global mit der GUI aufheben

1. Navigieren Sie zu **Traffic Management** > **DNS** > **Richtlinien**.

2. Klicken Sie im Detailbereich auf **Globale Bindungen**.
3. Wählen Sie im Dialogfeld **Globale Bindungen** die Richtlinie aus und klicken Sie auf **Richtlinie aufheben**.
4. Klicken Sie auf **OK**. Eine Meldung in der Statusleiste zeigt an, dass die Richtlinie erfolgreich aufgehoben wurde.

Aufheben der Bindung einer erweiterten Richtlinie von einem virtuellen Lastausgleichs- oder Content Switching-Server über die GUI

1. Navigieren Sie zu **Verkehrsverwaltung**, erweitern Sie Load Balancing oder Content Switching, und klicken Sie dann auf **Virtuelle Server**.
2. Doppelklicken Sie im Detailbereich auf den virtuellen Server, von dem Sie die Bindung der Richtlinie aufheben möchten.
3. Deaktivieren Sie auf der Registerkarte **Richtlinien** in der Spalte **Aktiv** das Kontrollkästchen neben der Richtlinie, die Sie aufheben möchten.
4. Klicken Sie auf **OK**. Eine Meldung in der Statusleiste zeigt an, dass die Richtlinie erfolgreich aufgehoben wurde.

Erstellen von Richtlinienbeschriftungen

October 5, 2021

Zusätzlich zu den integrierten Bindpunkten, in denen Sie Richtlinienbanken einrichten, können Sie auch benutzerdefinierte Policy-Labels konfigurieren und Richtlinien zuordnen.

Innerhalb einer Richtlinienbezeichnung binden Sie Richtlinien und geben die Reihenfolge der Bewertung jeder Richtlinie im Verhältnis zu anderen in der Richtlinienbank für das Policy-Label an. Mit dem Citrix ADC können Sie außerdem eine beliebige Auswertungsreihenfolge wie folgt definieren:

- Sie können goto -Ausdrücke verwenden, um auf den nächsten Eintrag in der Bank zu zeigen, der nach dem aktuellen ausgewertet werden soll.
- Sie können einen Eintrag in einer Richtlinienbank verwenden, um eine andere Bank aufzurufen.

Jedes Feature bestimmt den Richtlinientyp, den Sie an eine Richtlinienbezeichnung binden können, den Typ des virtuellen Lastenausgleichsservers, an den Sie die Bezeichnung binden können, und den Typ des virtuellen Content Switching-Servers, von dem die Bezeichnung aufgerufen werden kann. Beispielsweise kann eine TCP-Richtlinienbezeichnung nur an einen virtuellen TCP-Lastenausgleichsserver gebunden werden. HTTP-Richtlinien können nicht an eine Richtlinienbezeichnung dieses Typs gebunden werden. Und Sie können eine TCP-Richtlinienbezeichnung nur von einem virtuellen TCP-Content Switching-Server aufrufen.

Nachdem Sie eine neue Richtlinienbezeichnung konfiguriert haben, können Sie sie von einer oder mehreren Banken für die integrierten Bindungspunkte aufrufen.

Erstellen einer Caching-Richtlinienbezeichnung mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Caching-Richtlinienbezeichnung zu erstellen und die Konfiguration zu überprüfen:

```
1 -  add cache policylabel <labelName> -evaluates req|res
2
3 -  show cache policylabel<labelName>
4 <!--NeedCopy-->
```

Beispiel:

```
1 > add cache policylabel lbl-cache-pol -evaluates req
2 Done
3
4 > show cache policylabel lbl-cache-pol
5             Label Name: lbl-cache-pol
6             Evaluates: REQ
7             Number of bound policies: 0
8             Number of times invoked: 0
9 Done
10 <!--NeedCopy-->
```

Erstellen einer Richtlinienbezeichnung für Content Switching über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Content Switching-Richtlinienbezeichnung zu erstellen und die Konfiguration zu überprüfen:

```
1 -  add cs policylabel <labelName> http|tcp|rtsp|ssl
2
3 -  show cs policylabel <labelName>
4 <!--NeedCopy-->
```

Beispiel:


```
> add cs policylabel lbl-cs-pol http
Done
> show cs policylabel lbl-cs-pol
            Label Name: lbl-cs-pol
            Label Type: HTTP
            Number of bound policies: 0
            Number of times invoked: 0
Done
<!--NeedCopy-->
```

Erstellen eines Umschreibungsrichtlinienbezeichens mit der CLI

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

```
-  add rewrite policylabel <labelName> http_req|http_res|url|text|
   clientless_vpn_req|clientless_vpn_res

-  show rewrite policylabel <labelName>
<!--NeedCopy-->
```

Beispiel:

```
> add rewrite policylabel lbl-rewrt-pol http_req
Done

> show rewrite policylabel lbl-rewrt-pol
            Label Name: lbl-rewrt-pol
            Transform Name: http_req
            Number of bound policies: 0
            Number of times invoked: 0
Done
<!--NeedCopy-->
```

Erstellen einer Responder-Richtlinienbezeichnung mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Responder-Richtlinienbezeichnung zu erstellen und die Konfiguration zu überprüfen:


```
-  add responder policylabel <labelName>

-  show responder policylabel <labelName>
<!--NeedCopy-->
```

Beispiel:

```
> add responder policylabel lbl-respndr-pol
Done

> show responder policylabel lbl-respndr-pol
            Label Name: lbl-respndr-pol
            Number of bound policies: 0
            Number of times invoked: 0
Done
<!--NeedCopy-->
```

Hinweis: Rufen Sie dieses Policy-Label von einer Richtlinienbank auf. Weitere Informationen finden Sie im Abschnitt Binden einer Richtlinie an ein Richtlinienlabel.

Erstellen einer Richtlinienbezeichnung mit der GUI

1. Erweitern Sie im Navigationsbereich das Feature, für das Sie eine Richtlinienbezeichnung erstellen möchten, und klicken Sie dann auf **Richtlinienbezeichnungen**. Die Optionen sind integriertes Caching, Rewrite, Content Switching oder Responder.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im Feld Name einen eindeutigen Namen für diese Richtlinienbezeichnung ein.
4. Geben Sie funktionsspezifische Informationen für die Richtlinienbezeichnung ein. Beispielsweise wählen Sie für Integriertes Caching im Dropdownmenü Auswertungen die Option REQ aus, wenn diese Richtlinienbezeichnung Richtlinien für die Anforderungszeit enthalten soll, oder wählen Sie RES aus, wenn diese Richtlinienbezeichnung Antwortzeitrichtlinien enthalten soll. Wählen Sie für Umschreiben einen Transformationsnamen aus.
5. Klicken Sie auf **Erstellen**.
6. Konfigurieren Sie eine der integrierten Richtlinienbanken, um diese Richtlinienbezeichnung aufzurufen. Weitere Informationen finden Sie im Abschnitt Binden einer Richtlinie an ein Richtlinienlabel. Eine Meldung in der Statusleiste zeigt an, dass die Richtlinienbezeichnung erfolgreich erstellt wurde.

Binden einer Richtlinie an ein Richtlinienlabel

Wie bei Richtlinienbanken, die an die integrierten Bindungspunkte gebunden sind, ist jeder Eintrag in einem Policy-Label eine Richtlinie, die an das Policy-Label gebunden ist. Wie bei Richtlinien, die global oder an einen vserver gebunden sind, kann jede Richtlinie, die an das Policy-Label gebunden ist, auch eine Richtlinienbank oder ein Policy-Label aufrufen, das nach der Verarbeitung des aktuellen Eintrags ausgewertet wird. In der folgenden Tabelle werden die Einträge in einer Richtlinienbezeichnung zusammengefasst.

- **Name**. Der Name einer Richtlinie oder, um eine andere Richtlinienbank aufzurufen, ohne eine Richtlinie zu bewerten, der Dummy -Richtlinienname NOPOLICY.

  Sie können NOPOLICY mehrmals in einer Richtlinienbank angeben, aber Sie können eine benannte Richtlinie nur einmal angeben.

- **Priority**. Eine ganze Zahl. Diese Einstellung kann mit dem Goto-Ausdruck funktionieren.

- **Goto-Ausdruck**. Legt die nächste Richtlinie fest, die in dieser Bank ausgewertet werden soll. Sie können einen der folgenden Werte angeben:

  - **ALS NÄCHSTES**. Gehen Sie zur Richtlinie mit der nächsthöheren Priorität.
  - **ENDE**. Auswertung beenden.
  - **USE_INVOCATION_RESULT**. Gilt, wenn dieser Eintrag eine andere Richtlinienbank aufruft. Wenn der endgültige Gehe in der aufgerufenen Bank den Wert END aufweist, wird die Auswertung beendet. Wenn der endgültige Goto etwas anderes als END ist, führt die aktuelle Richtlinienbank eine NEXT durch.
  - **Positive Zahl:** Die Prioritätsnummer der nächsten zu bewertenden Richtlinie.
  - **Numerischer Ausdruck**. Ein Ausdruck, der die Prioritätsnummer der nächsten auszuwertenden Richtlinie erzeugt.

  Der Gehe kann nur in einer Richtlinienbank vorwärts gehen.

  Wenn Sie den Goto-Ausdruck weglassen, entspricht er der Angabe von END.

- **Aufruftyp**. Gibt einen Richtlinienbanktyp an. Der Wert kann einer der folgenden Werte sein:

  - **Vserver anfordern**. Ruft Anforderungszeitrichtlinien auf, die einem virtuellen Server zugeordnet sind.
  - **Antwort-Vserver**. Ruft Antwortzeitrichtlinien auf, die einem virtuellen Server zugeordnet sind.
  - **Richtlinienbezeichnung**. Ruft eine andere Policy-Bank auf, wie sie durch das Richtlinienlabel für die Bank gekennzeichnet ist.

- **Name des Aufrufs**. Der Name eines virtuellen Servers oder einer Richtlinienbezeichnung, abhängig vom Wert, den Sie für den Aufruftyp angegeben haben.

Konfigurieren einer Richtlinienbezeichnung oder einer virtuellen Serverrichtlinienbank

October 5, 2021

Nachdem Sie Richtlinien erstellt und Richtlinienbanken durch Binden der Richtlinien erstellt haben, können Sie eine zusätzliche Konfiguration von Richtlinien innerhalb einer Bezeichnung oder einer Richtlinienbank durchführen. Bevor Sie beispielsweise den Aufruf einer externen Richtlinienbank konfigurieren, sollten Sie warten, bis Sie diese Richtlinienbank konfiguriert haben.

Dieses Artikel enthält die folgenden Abschnitte:

- Konfigurieren einer Richtlinienbezeichnung
- Konfigurieren einer Richtlinienbank für einen virtuellen Server

Konfigurieren einer Richtlinienbezeichnung

Ein Richtlinienlabel besteht aus einer Reihe von Richtlinien und Aufrufen anderer Richtlinienlabels und virtueller serverspezifischer Richtlinienbanken. Mit dem Invoke-Parameter können Sie eine Richtlinienbezeichnung oder eine virtuelle serverspezifische Richtlinienbank von jeder anderen Richtlinienbank aufrufen. Mit einem speziellen NoPolicy-Eintrag können Sie eine externe Bank aufrufen, ohne einen Ausdruck (eine Regel) zu verarbeiten. Der NoPolicy-Eintrag ist eine Dummy -Richtlinie, die keine Regel enthält.

Beachten Sie zum Konfigurieren von Richtlinienbeschriftungen über die Citrix ADC Befehlszeile die folgenden Ausführungen der Befehlssyntax:

- gotoPriorityExpression wird wie in Tabelle 2 beschrieben konfiguriert. Format jedes Eintrags in einer Richtlinienbank des Abschnitts “Einträge in einer Richtlinienbank” in Bind-Richtlinien mit erweiterten Richtlinien.
- Das Argument type ist erforderlich. Dies ist anders als die Bindung einer herkömmlichen Richtlinie, bei der dieses Argument optional ist.
- Sie können die Richtlinienbank aufrufen, die an einen virtuellen Server gebunden sind, indem Sie dieselbe Methode verwenden, die Sie zum Aufrufen einer Richtlinienbezeichnung verwenden.

Konfigurieren einer Richtlinienbezeichnung mit der CLI

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


```
-  bind cache|rewrite|responder policylabel <policylabelName> -
   policyName <policyName> -priority <priority> [-
   gotoPriorityExpression <gotopriorityExpression>] [-invoke reqvserver
   |resvserver|policylabel <policyLabelName>|<vserverName>]

-  show cache|rewrite|responder policylabel <policylabelName>
<!--NeedCopy-->
```

Beispiel:

```
bind cache policylabel _reqBuiltinDefaults -policyName  _nonGetReq -
   priority 100
Done
show cache policylabel _reqBuiltinDefaults
            Label Name: _reqBuiltinDefaults
            Evaluates: REQ
            Number of bound policies: 3
            Number of times invoked: 0
    1)      Policy Name: _nonGetReq
            Priority: 100
            GotoPriorityExpression: END
    2)      Policy Name: _advancedConditionalReq
            Priority: 200
            GotoPriorityExpression: END

    3)      Policy Name: _personalizedReq
            Priority: 300
            GotoPriorityExpression: END
Done
<!--NeedCopy-->
```

Aufrufen eines Policy-Labels von einer Richtlinienbank mit einem NOPOLICY Eintrag mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Richtlinienbezeichnung von einer Richtlinienbank Rewrite mit einem NOPOLICY-Eintrag aufzurufen und die Konfiguration zu überprüfen:

```
-  bind rewrite global <policyName> <priority> <gotoPriorityExpression>
    -type REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT -invoke
   reqvserver|resvserver|policylabel <policyLabelName>|<vserverName>
```



```
2
3 -  show rewrite global
4 <!--NeedCopy-->
```

Beispiel:

```
1 > bind rewrite global NOPOLICY 100 -type REQ_DEFAULT -invoke
     policylabel lbl-rewrt-pol
2 Done
3 > show rewrite global
4     1)      Global bindpoint: REQ_DEFAULT
5             Number of bound policies: 1
6
7     2)      Global bindpoint: REQ_OVERRIDE
8             Number of bound policies: 1
9 Done
10 <!--NeedCopy-->
```

Aufrufen eines Richtlinienbezeichens von einer integrierten Caching-Richtlinienbank mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Richtlinienbezeichnung von einer integrierten Caching-Richtlinienbank aufzurufen und die Konfiguration zu überprüfen:

```
1 -  bind cache global NOPOLICY -priority <priority> -
     gotoPriorityExpression <gotoprioritыExpression> -type REQ_OVERRIDE|
     REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT -invoke reqvserver|resvserver|
     policylabel <policyLabelName>|<vserverName>
2
3 -  show cache global
4 <!--NeedCopy-->
```

Beispiel:

```
1 bind cache global NOPOLICY -priority 100 -gotoPriorityExpression END -
     type REQ_DEFAULT -invoke policylabel lbl-cache-pol
2 Done
3 > show cache global
4     1)      Global bindpoint: REQ_DEFAULT
```



```
5               Number of bound policies: 2
6
7      2)       Global bindpoint: RES_DEFAULT
8               Number of bound policies: 1
9
10 Done
11 <!--NeedCopy-->
```

Aufrufen eines Policy-Labels von einer Responder-Richtlinienbank mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Richtlinienbezeichnung von einer Responder-Richtlinienbank aufzurufen und die Konfiguration zu überprüfen:

```
1 -  bind responder global NOPOLICY <priority> <gotopriorityExpression> -
     type OVERRIDE|DEFAULT -invoke vserver|policylabel <policyLabelName
     >|<vserverName>
2
3 -  show responder global
4 <!--NeedCopy-->
```

Beispiel:

```
1 > bind responder global NOPOLICY 100 NEXT -type DEFAULT -invoke
     policylabel lbl-respndr-pol
2 Done
3 > show responder global
4      1)       Global bindpoint: REQ_DEFAULT
5               Number of bound policies: 2
6
7 Done
8 <!--NeedCopy-->
```

Konfigurieren einer Richtlinienbezeichnung mit der GUI

1. Erweitern Sie im Navigationsbereich das Feature, für das Sie eine Richtlinienbezeichnung konfigurieren möchten, und klicken Sie dann auf Richtlinienbezeichnungen. Die Optionen sind Integriertes Caching, Rewrite oder Responder.
2. Doppelklicken Sie im Detailbereich auf die Bezeichnung, die Sie konfigurieren möchten.

3. Wenn Sie dieser Richtlinienbezeichnung eine neue Richtlinie hinzufügen, klicken Sie auf Richtlinie einfügen, und wählen Sie im Feld Richtlinienname die Option Neue Richtlinie aus. Weitere Informationen zum Hinzufügen einer Richtlinie finden Sie unter Erstellen oder Ändern einer Richtlinie. Wenn Sie eine Richtlinienbank aufrufen und keine Regel vor dem Aufruf ausgewertet werden soll, klicken Sie auf Richtlinie einfügen, und wählen Sie im Feld Richtlinienname die Option NOPOLICY aus.
4. Konfigurieren Sie für jeden Eintrag in dieser Richtlinienbezeichnung Folgendes:
   - **Richtlinienname:**

     Dies wird bereits durch den Richtliniennamen, die neue Richtlinie oder den Eintrag NOPOLICY bestimmt, den Sie in diese Bank eingefügt haben.
   - **Priorität:**

     Ein numerischer Wert, der entweder eine absolute Reihenfolge der Auswertung innerhalb der Bank bestimmt oder in Verbindung mit einem Goto-Ausdruck verwendet wird.
   - **Ausdruck:**

     Die Richtlinienregel. Richtlinienausdrücke werden in den folgenden Kapiteln ausführlich beschrieben. Eine Einführung finden Sie unter Konfigurieren von erweiterten Richtlinienausdrücken: Erste Schritte.
   - **Aktion:**

     Die Aktion, die ergriffen werden soll, wenn diese Richtlinie TRUE ergibt.
   - **Gehe zu Ausdruck:**

     Optional. Wird verwendet, um die Prioritätsstufe zu erweitern, um die nächste Policy oder Richtlinienbank zu bestimmen, die bewertet werden soll. Weitere Informationen zu möglichen Werten für einen Goto-Ausdruck finden Sie in Tabelle 2. Format jedes Eintrags in einer Richtlinienbank des Abschnitts “Einträge in einer Richtlinienbank” in Bind-Richtlinien mit erweiterten Richtlinien.
   - **Aufrufen:**

     Optional. Ruft eine andere Richtlinienbank an.
5. Klicken Sie auf **OK**. Eine Meldung in der Statusleiste zeigt an, dass die Richtlinienbezeichnung erfolgreich konfiguriert wurde.

Konfigurieren einer Richtlinienbank für einen virtuellen Server

Sie können eine Richtlinienbank für einen virtuellen Server konfigurieren. Die Richtlinienbank kann einzelne Richtlinien enthalten, und jeder Eintrag in der Richtlinienbank kann optional eine Policy-Bezeichnung oder eine Richtlinienbank aufrufen, die Sie für einen anderen virtuellen Server konfig-

uriert haben. Wenn Sie ein Richtlinienlabel oder eine Richtlinienbank aufrufen, können Sie dies tun, ohne einen Ausdruck (eine Regel) auszulösen, indem Sie anstelle eines Richtliniennamens einen NOP-OLICY Dummy -Eintrag auswählen.

Hinzufügen von Richtlinien zu einer virtuellen Serverrichtlinienbank mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um Richtlinien zu einer virtuellen Server-Richtlinienbank hinzuzufügen und die Konfiguration zu überprüfen:

```
- bind lb|cs vserver <virtualServerName> <serviceType> [-policyName <
   policyName>] [-priority <positiveInteger>] [-gotoPriorityExpression
   <expression>] [-type REQUEST|RESPONSE]

- show lb|cs vserver <virtualServerName>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver vs-cont-sw TCP
Done
show lb vserver vs-cont-sw
            vs-cont-sw (0.0.0.0:0) - TCP    Type: ADDRESS
            State: DOWN
            Last state change was at Wed Aug 19 10:04:02 2009 (+279 ms)
            Time since last state change: 0 days, 00:02:14.420
            Effective State: DOWN
            Client Idle Timeout: 9000 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            No. of Bound Services :  0 (Total)       0 (Active)
            Configured Method: LEASTCONNECTION
            Mode: IP
            Persistence: NONE
            Connection Failover: DISABLED
Done
<!--NeedCopy-->
```


Aufrufen einer Richtlinienbezeichnung von einer virtuellen Serverrichtlinienbank mit einem NOPOLICY Eintrag mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Richtlinienbezeichnung von einer virtuellen Serverrichtlinienbank mit einem NOPOLICY-Eintrag aufzurufen und die Konfiguration zu überprüfen:

```
1 -  bind lb|cs vserver <virtualServerName> -policyName NOPOLICY-REWRITE|
     NOPOLICY-CACHE|NOPOLICY-RESPONDER -priority <integer> -type REQUEST|
     RESPONSE -gotoPriorityExpression <gotoprioritыExpression> -invoke
     reqVserver|resVserver|policyLabel <vserverName>|<labelName>
2
3 -  show lb vserver
4 <!--NeedCopy-->
```

Beispiel:

```
1 > bind lb vserver vs-cont-sw -policyname NOPOLICY-REWRITE -priority 200
      -type REQUEST -gotoPriorityExpression NEXT -invoke policyLabel lbl-
     rewrt-pol
2 Done
3 <!--NeedCopy-->
```

Konfigurieren einer virtuellen Serverrichtlinienbank mit der GUI

1. Erweitern Sie im linken Bereich ** **Traffic Management** > **Load Balancing**, **Traffic Management** > **Content Switching**, **Traffic Management** > **SSL Offload**, **Security** > **AAA - Application Traffic** oder **Citrix Gateway**, wie zutreffend, und klicken Sie dann auf **Virtual Servers**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie konfigurieren möchten, und klicken Sie dann auf **Öffnen**.
3. Klicken **Sie im Dialogfeld Virtuellen Server konfigurieren** auf die Registerkarte **Richtlinien**.
4. Um eine neue Richtlinie in dieser Bank zu erstellen, klicken Sie auf das Symbol für den Richtlinien- oder Richtlinienbezeichnungstyp, den Sie der Richtlinienbank des virtuellen Servers hinzufügen möchten, und klicken Sie auf **Richtlinie einfügen**. Wenn Sie eine Richtlinienbezeichnung aufrufen möchten, ohne eine Richtlinienregel auszuwerten, wählen Sie die NOPOLICY Dummy-Richtlinie aus.
5. Um einen vorhandenen Eintrag in dieser Richtlinienbank zu konfigurieren, geben Sie Folgendes ein:

- **Priorität:**

  Ein numerischer Wert, der entweder eine absolute Reihenfolge der Auswertung innerhalb der Bank bestimmt oder in Verbindung mit einem Goto-Ausdruck verwendet wird.

- **Ausdruck:**

  Die Richtlinienregel. Richtlinienausdrücke werden in den folgenden Kapiteln ausführlich beschrieben. Eine Einführung finden Sie unter Konfigurieren von erweiterten Richtlinienausdrücken: Erste Schritte.

- **Aktion:**

  Die Aktion, die ergriffen werden soll, wenn diese Richtlinie TRUE ergibt.

- **Gehe zu Ausdruck:**

  Optional. Legt die nächste Policy-Bewertung oder Richtlinienbank fest. Weitere Informationen zu möglichen Werten für einen Goto-Ausdruck finden Sie im Abschnitt "Einträge in einer Richtlinienbank" unter Bind-Richtlinien mit erweiterten Richtlinien.

- **Aufrufen:**

  Optional. Um eine andere Richtlinienbank aufzurufen, wählen Sie den Namen der Policy Label oder der virtuellen Server Richtlinienbank, die Sie aufrufen möchten.

6. Klicken Sie auf **OK**. Eine Meldung in der Statusleiste zeigt an, dass die Richtlinie erfolgreich konfiguriert wurde.

Aufrufen oder Entfernen einer Richtlinienbezeichnung oder einer virtuellen Serverrichtlinienbank

October 8, 2021

Im Gegensatz zu einer Richtlinie, die nur einmal gebunden werden kann, können Sie eine Richtlinienbezeichnung oder die Richtlinienbank eines virtuellen Servers beliebig oft verwenden, indem Sie sie aufrufen. Der Aufruf kann von zwei Stellen ausgeführt werden:

- Von der Bindung für eine benannte Policy in einer Richtlinienbank.
- Aus der Bindung für einen NOPOLICY Dummy Eintrag in einer Richtlinienbank.

In der Regel muss die Richtlinienbezeichnung vom gleichen Typ wie die Richtlinie sein, von der sie aufgerufen wird. Beispielsweise würden Sie eine Responderrichtlinienbezeichnung aus einer Responderrichtlinie aufrufen.

Hinweis: Wenn Sie einen globalen NOPOLICY-Eintrag in einer Richtlinienbank in der Befehlszeile binden oder aufheben, geben Sie eine Priorität an, um einen NOPOLICY-Eintrag von einem anderen zu unterscheiden.

Aufrufen eines Umschreibens oder einer integrierten Caching-Richtlinienbezeichnung mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um eine Umschreib- oder integrierte Caching-Richtlinienbezeichnung aufzurufen und die Konfiguration zu überprüfen:

```
- bind cache global <policy> -priority <positive_integer> [-
   gotoPriorityExpression <expression>] -type REQ_OVERRIDE|REQ_DEFAULT|
   RES_OVERRIDE|RES_DEFAULT] -invoke reqvserver|resvserver|policylabel
   <label_name>

- bind rewrite global<policy> -priority <positive_integer> [-
   gotoPriorityExpression <expression>] -type REQ_OVERRIDE|REQ_DEFAULT|
   RES_OVERRIDE|RES_DEFAULT] -invoke reqvserver|resvserver|policylabel
   <label_name>

- show cache global|show rewrite global
<!--NeedCopy-->
```

Beispiel:

```
> bind cache global _nonPostReq2 -priority 100 -type req_override -
   invoke
    policylabel lbl-cache-pol
Done
> show cache global
    1)      Global bindpoint: REQ_DEFAULT
            Number of bound policies: 2

    2)      Global bindpoint: RES_DEFAULT
            Number of bound policies: 1

    3)      Global bindpoint: REQ_OVERRIDE
            Number of bound policies: 1

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


Aufrufen einer Responder-Richtlinienbezeichnung mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Responder-Richtlinienbezeichnung aufzurufen und die Konfiguration zu überprüfen:

```
1 -  bind responder global <policy_Name> <priority_as_positive_integer>
     [<gotoPriorityExpression>] -type REQ_OVERRIDE|REQ_DEFAULT|OVERRIDE|
     DEFAULT -invoke vserver|policylabel <label_name>
2
3 -  show responder global
4 <!--NeedCopy-->
```

Beispiel:

```
1 > bind responder global pol404Error1 300 -invoke policylabel lbl-
     respndr-pol
2 Done
3 > show responder global
4     1)      Global bindpoint: REQ_DEFAULT
5             Number of bound policies: 2
6
7 Done
8 <!--NeedCopy-->
```

Aufrufen einer virtuellen Serverrichtlinienbank mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Virtual Server Richtlinienbank aufzurufen und die Konfiguration zu überprüfen:

```
1 -  bind lb vserver <vserver_name> -policyName <policy_Name> -priority <
     positive_integer> [-gotoPriorityExpression <expression>] -type
     REQUEST|RESPONSE -invoke reqvserver|resvserver|policylabel <
     policy_Label_Name>
2
3 -  bind lb vserver <vserver_name>
4 <!--NeedCopy-->
```

Beispiel:


```
> bind lb vserver lbvip -policyName ns_cmp_msapp -priority 100
Done

> show lb vserver lbvip
            lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
            State: DOWN
            Last state change was at Wed Jul 15 05:54:24 2009 (+166 ms)
            Time since last state change: 28 days, 06:37:49.250
            Effective State: DOWN
            Client Idle Timeout: 180 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            Port Rewrite : DISABLED
            No. of Bound Services :  0 (Total)       0 (Active)
            Configured Method: LEASTCONNECTION
            Mode: IP
            Persistence: NONE
            Vserver IP and Port insertion: OFF
            Push: DISABLED  Push VServer:
            Push Multi Clients: NO
            Push Label Rule: none

    1)      CSPolicy: pol-cont-sw   CSVserver: vs-cont-sw   Priority:
       100   Hits: 0

    2)      Policy : pol-ssl Priority:0
    3)      Policy : ns_cmp_msapp Priority:100
    4)      Policy : cf-pol Priority:1      Inherited
Done
<!--NeedCopy-->
```

Entfernen eines Umschreibens oder einer integrierten Caching-Richtlinienbezeichnung mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um eine Richtlinienbezeichnung für das Umschreiben oder integrierte Caching zu entfernen und die Konfiguration zu überprüfen:

```
-  unbind rewrite global <policyName> -priority <positiveInteger> -type
    REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT

-  unbind cache global <policyName> -priority <positiveInteger> -type
   REQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT
```



```
4
5 -  show rewrite global|show cache global
6 <!--NeedCopy-->
```

Beispiel:

```
1 > unbind rewrite global NOPOLICY -priority 100 -type REQ_OVERRIDE
2 > show rewrite global
3 Done
4     1)      Global bindpoint: REQ_DEFAULT
5             Number of bound policies: 1
6
7 Done
8 <!--NeedCopy-->
```

Entfernen einer Responder-Richtlinienbezeichnung mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Responder-Richtlinienbezeichnung zu entfernen und die Konfiguration zu überprüfen:

```
1 -  unbind responder global <policyName> -priority <positiveInteger> -
     type OVERRIDE|DEFAULT
2
3 -  show responder global
4 <!--NeedCopy-->
```

Beispiel:

```
1 > unbind responder global NOPOLICY -priority 100 -type REQ_DEFAULT
2 Done
3 > show responder global
4     1)      Global bindpoint: REQ_DEFAULT
5             Number of bound policies: 1
6
7 Done
8 <!--NeedCopy-->
```


Entfernen einer virtuellen Server-Richtlinienbezeichnung mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um eine Virtual Server-Richtlinienbezeichnung zu entfernen und die Konfiguration zu überprüfen:

```
- unbind lb vserver <virtualServerName> -policyName NOPOLICY-REWRITE|NOPOLICY-RESPONDER|NOPOLICY-CACHE -type REQUEST|RESPONSE -priority <positiveInteger>

- unbind cs vserver <virtualServerName> -policyName NOPOLICY-REWRITE|NOPOLICY-RESPONDER|NOPOLICY-CACHE -type REQUEST|RESPONSE -priority <positiveInteger>

- show lb vserver|show cs vserver
<!--NeedCopy-->
```

Beispiel:

```
> unbind lb vserver lbvip -policyName ns_cmp_msapp -priority 200
Done
> show lb vserver lbvip
            lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
            State: DOWN
            Last state change was at Wed Jul 15 05:54:24 2009 (+161 ms)
            Time since last state change: 28 days, 06:47:54.600
            Effective State: DOWN
            Client Idle Timeout: 180 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            Port Rewrite : DISABLED
            No. of Bound Services :  0 (Total)       0 (Active)
            Configured Method: LEASTCONNECTION
            Mode: IP
            Persistence: NONE
            Vserver IP and Port insertion: OFF
            Push: DISABLED  Push VServer:
            Push Multi Clients: NO
            Push Label Rule: none

    1)      CSPolicy: pol-cont-sw   CSVserver: vs-cont-sw   Priority:
        100   Hits: 0

```



```
24      1)      Policy : pol-ssl Priority:0
25      2)      Policy : cf-pol Priority:1      Inherited
26  Done
27  <!--NeedCopy-->
```

Aufrufen einer Richtlinienbezeichnung oder einer virtuellen Serverrichtlinienbank mit der GUI

1. Binden Sie eine Richtlinie, wie unter Richtlinie global bindenbeschrieben, Binden Sie eine Richtlinie an einen virtuellen Serveroder Binden Sie eine Richtlinie an eine Policy Label. Alternativ können Sie anstelle eines Richtliniennamens einen NOPOLICY Dummy -Eintrag eingeben. Dies geschieht, wenn Sie vor der Auswertung der Richtlinienbank keine Policy evaluieren möchten.
2. Wählen Sie im Feld Invoke den Namen der Richtlinienbezeichnung oder der virtuellen Serverrichtlinienbank aus, die ausgewertet werden soll, ob der Datenverkehr mit der gebundenen Richtlinie übereinstimmt. Eine Meldung in der Statusleiste zeigt an, dass die Richtlinienbezeichnung oder die virtuelle Serverrichtlinienbank erfolgreich aufgerufen wurde.

Entfernen eines Richtlinienbezeichnungsaufrufs mit der GUI

1. Öffnen Sie die Richtlinie, und deaktivieren Sie das Feld Invoke. Durch das Aufheben der Bindung der Richtlinie wird auch der Aufruf der Beschriftung entfernt. Eine Meldung in der Statusleiste zeigt an, dass die Richtlinienbezeichnung erfolgreich entfernt wurde.

Konfigurieren des erweiterten Richtlinienausdrucks: Erste Schritte

October 5, 2021

Erweiterte Richtlinien werten Daten basierend auf Informationen aus, die Sie in Erweiterte Richtlinienausdrücke bereitstellen. Ein erweiterter Richtlinienausdruck analysiert Datenelemente (z. B. HTTP-Header, Quell-IP-Adressen, die Citrix ADC -Systemzeit und POST-Body-Daten). Zusätzlich zum Konfigurieren eines erweiterten Richtlinienausdrucks in einer Richtlinie konfigurieren Sie in einigen Citrix ADC Features den erweiterten Richtlinienausdruck außerhalb des Kontexts einer Richtlinie.

Um einen erweiterten Richtlinienausdruck zu erstellen, wählen Sie ein Präfix aus, das eine Datenmenge identifiziert, die Sie analysieren möchten, und geben Sie dann einen Vorgang an, der für die Daten ausgeführt werden soll. Beispielsweise kann ein Vorgang eine Datenmenge mit einer von Ihnen angegebenen Textzeichenfolge abgleichen oder eine Textzeichenfolge in einen HTTP-Header transformieren. Andere Operationen entsprechen einer zurückgegebenen Zeichenfolge mit einer Reihe

von Strings oder einem String-Muster. Sie konfigurieren zusammengesetzte Ausdrücke, indem Sie boolesche und arithmetische Operatoren angeben und die Reihenfolge der Auswertung mithilfe von Klammern steuern.

Erweiterter Richtlinienausdruck kann auch klassische Ausdrücke enthalten. Sie können einem häufig verwendeten Ausdruck einen Namen zuweisen, um den Ausdruck nicht wiederholt erstellen zu müssen.

Richtlinien und einige andere Entitäten enthalten Regeln, die der Citrix ADC verwendet, um ein Paket im Datenverkehr auszuwerten, Daten aus dem Citrix ADC-System selbst zu extrahieren, eine Anforderung (ein Callout) an eine externe Anwendung zu senden oder ein anderes Datenelement zu analysieren. Eine Regel hat die Form eines logischen Ausdrucks, der mit dem Verkehr verglichen wird und letztendlich die Werte TRUE oder FALSE zurückgibt.

Die Elemente der Regel können selbst TRUE oder FALSE, String oder numerische Werte zurückgeben.

Bevor Sie einen erweiterten Richtlinienausdruck konfigurieren, müssen Sie die Merkmale der Daten verstehen, die von der Richtlinie oder einer anderen Entität ausgewertet werden sollen. Wenn Sie beispielsweise mit der integrierten Caching-Funktion arbeiten, legt eine Richtlinie fest, welche Daten im Cache gespeichert werden können. Mit integriertem Caching müssen Sie die URLs, Header und andere Daten in den HTTP-Anforderungen und -Antworten kennen, die der Citrix ADC empfängt. Mit diesem Wissen können Sie Richtlinien konfigurieren, die den tatsächlichen Daten entsprechen, und Citrix ADC das Caching für HTTP-Datenverkehr ermöglichen. Diese Informationen helfen Ihnen, den Ausdruckstyp zu bestimmen, den Sie in der Richtlinie konfigurieren müssen.

Grundlegende Elemente eines erweiterten Richtlinienausdrucks

October 5, 2021

Ein erweiterter Richtlinienausdruck besteht mindestens aus einem Präfix (oder einem einzelnen Element, das anstelle eines Präfixes verwendet wird). Die meisten Ausdrücke geben auch eine Operation an, die für die Daten ausgeführt werden soll, die vom Präfix identifiziert werden. Sie formatieren einen Ausdruck mit bis zu 1.499 Zeichen wie folgt:

```
<prefix>.<operation> [<compound-operator> <prefix>.<operation>. . .]
```

wobei

- <prefix>

  ist ein Ankerpunkt zum Starten eines Ausdrucks.

  Das Präfix ist ein periodenbegrenzter Schlüssel, der eine Dateneinheit identifiziert. Das folgende Präfix untersucht beispielsweise HTTP-Anforderungen auf das Vorhandensein eines Headers namens Content-Type:

http.req.header (Content-Type)

Präfixe können auch alleine verwendet werden, um den Wert des Objekts zurückzugeben, das das Präfix identifiziert.

- <operation>

  identifiziert eine Auswertung, die mit den durch das Präfix identifizierten Daten durchgeführt werden soll.

  Betrachten Sie beispielsweise den folgenden Ausdruck:

  http.req.header (Content-Type) .eq (text/html)

  In diesem Ausdruck ist der folgende Operator Komponente:

  eq (text/html)

  Dieser Operator bewirkt, dass Citrix ADC alle HTTP-Anforderungen auswertet, die einen Content-Type-Header enthalten, und insbesondere, um festzustellen, ob der Wert dieses Headers gleich der Zeichenfolge text/html ist. Weitere Informationen finden Sie unter “Operationen. “

- <compound-operator>

  ist ein boolescher oder arithmetischer Operator, der einen zusammengesetzten Ausdruck aus mehreren Präfix- oder prefix.operationselementen bildet.

  Betrachten Sie beispielsweise den folgenden Ausdruck:

  http.req.header (Content-Type) .eq (text/html) && http.req.url.contains (.html)

Präfixe

Ein Ausdruckspräfix stellt eine diskrete Datenmenge dar. Ein Ausdruckspräfix kann beispielsweise eine HTTP-URL, einen HTTP-Cookie-Header oder eine Zeichenfolge im Textkörper einer HTTP-POST-Anforderung darstellen. Ein Ausdruckspräfix kann eine Vielzahl von Datentypen identifizieren und zurückgeben, einschließlich der folgenden:

- Eine Client-IP-Adresse in einem TCP/IP-Paket
- Citrix ADC -Systemzeit
- Ein externes Callout über HTTP
- Ein TCP- oder UDP-Datensatztyp

In den meisten Fällen beginnt ein Ausdruckspräfix mit einem der folgenden Schlüsselwörter:

- CLIENT:
  - Identifiziert ein Merkmal des Clients, der entweder eine Anfrage sendet oder eine Antwort empfängt, wie in den folgenden Beispielen:
  - Das Präfix client.ip.dst gibt die Ziel-IP-Adresse in der Anforderung oder Antwort an.

  - Das Präfix client.ip.src gibt die Quell-IP-Adresse an.

- HTTP:
  - Identifiziert ein Element in einer HTTP-Anforderung oder einer Antwort, wie in den folgenden Beispielen:
  - Das Präfix http.req.body (integer) bezeichnet den Körper der HTTP-Anforderung als mehrzeiliges Textobjekt, bis zu der in Integer angegebenen Zeichenposition.
  - Das Präfix http.req.header (header_name) bezeichnet einen HTTP-Header, wie in header_name angegeben.
  - Das Präfix http.req.url bezeichnet eine HTTP-URL im URL-kodierten Format.

- SERVER:

  Identifiziert ein Element auf dem Server, das entweder eine Anforderung verarbeitet oder eine Antwort sendet.

- SYS:

  Identifiziert ein Merkmal des Citrix ADC, das den Datenverkehr verarbeitet.

  Hinweis: Beachten Sie, dass DNS-Richtlinien nur SYS, CLIENT und SERVER-Objekte unterstützen.

  Darüber hinaus kann die Clientless-VPN-Funktion in Citrix Gateway die folgenden Arten von Präfixen verwenden:

- TEXT:

  Identifiziert ein beliebiges Textelement in einer Anforderung oder einer Antwort.

- TARGET:

  Identifiziert das Ziel einer Verbindung.

- URL:

  Identifiziert ein Element im URL-Teil einer HTTP-Anforderung oder -Antwort.

Als allgemeine Faustregel kann jedes Ausdruckspräfix ein eigenständiger Ausdruck sein. Das folgende Präfix ist beispielsweise ein vollständiger Ausdruck, der den Inhalt des HTTP-Headers zurückgibt, der im String-Argument angegeben ist (in Anführungszeichen eingeschlossen):

```
http.res.header.("myheader")
```

Oder Sie können Präfixe mit einfachen Operationen kombinieren, um TRUE und FALSE Werte zu bestimmen. Der folgende Wert gibt beispielsweise den Wert TRUE oder FALSE zurück:

```
http.res.header.("myheader").exists
```

Sie können auch komplexe Operationen für einzelne Präfixe und mehrere Präfixe innerhalb eines Ausdrucks verwenden, wie im folgenden Beispiel:


```
http.req.url.length + http.req.cookie.length <= 500
```

Welche Ausdruckspräfixe Sie angeben können, hängt von der Citrix ADC Funktion ab. In der folgenden Tabelle werden die Ausdruckspräfixe beschrieben, die auf Feature-Basis von Interesse sind.

Feature	Typen von Ausdruckspräfix, die im Feature verwendet werden
DNS	SYS, CLIENT, SERVER
Responder in Schutzfunktionen	HTTP, SYS, CLIENT
Content Switching	HTTP, SYS, CLIENT
Neuschreiben	HTTP, SYS, CLIENT, SERVER, URL, TEXT, TARGET, VPN
Integriertes Caching	HTTP, SYS, CLIENT, SERVER
Citrix Gateway, Clientloser Zugriff	HTTP, SYS, CLIENT, SERVER, URL, TEXT, TARGET, VPN

Tabelle 1. Zulässige Typen von Ausdruckspräfixen in verschiedenen Citrix ADC Features

Hinweis: Einzelheiten zu den zulässigen Ausdruckspräfixen in einem Feature finden Sie in der Dokumentation zu diesem Feature.

Ausdrücke mit einem Element

Der einfachste Typ des erweiterten Richtlinienausdrucks enthält ein einzelnes Element. Dieses Element kann eines der folgenden sein:

- wahr. Ein erweiterter Richtlinienausdruck kann einfach aus dem Wert true bestehen. Dieser Ausdruckstyp gibt immer den Wert TRUE zurück. Es ist nützlich, um Richtlinienaktionen zu verketten und Goto-Ausdrücke auszulösen.
- falsch. Ein erweiterter Richtlinienausdruck kann einfach aus dem Wert false bestehen. Dieser Ausdruckstyp gibt immer den Wert FALSE zurück.
- Ein Präfix für einen zusammengesetzten Ausdruck. Beispielsweise ist das Präfix HTTP.REQ.HOSTNAME ein vollständiger Ausdruck, der einen Hostnamen zurückgibt, und HTTP.REQ.URL ist ein vollständiger Ausdruck, der eine URL zurückgibt. Das Präfix könnte auch in Verbindung mit Operationen und zusätzlichen Präfixen verwendet werden, um einen zusammengesetzten Ausdruck zu bilden.

Vorgänge

In den meisten Ausdrücken geben Sie auch eine Operation für die Daten an, die vom Präfix identifiziert werden. Angenommen, Sie geben das folgende Präfix an:

```
http.req.url
```

Dieses Präfix extrahiert URLs in HTTP-Anforderungen. Für dieses Ausdruckspräfix müssen keine Operatoren in einem Ausdruck verwendet werden. Wenn Sie jedoch einen Ausdruck konfigurieren, der HTTP-Anforderungs-URLs verarbeitet, können Sie Vorgänge angeben, die bestimmte Merkmale der URL analysieren. Im Folgenden sind ein paar Möglichkeiten:

- Suchen Sie in der URL nach einem bestimmten Hostnamen.
- Suchen Sie in der URL nach einem bestimmten Pfad.
- Bewerten Sie die Länge der URL.
- Suchen Sie in der URL nach einer Zeichenfolge, die einen Zeitstempel angibt, und konvertieren Sie ihn in GMT.

Im Folgenden finden Sie ein Beispiel für ein Präfix, das einen HTTP-Header namens Server und einen Vorgang identifiziert, der im Headerwert nach der Zeichenfolge IIS sucht:

```
http.res.header(”Server”).contains(”IIS”)
```

Es folgt ein Beispiel für ein Präfix, das Hostnamen identifiziert und eine Operation, die nach der Zeichenfolge www.mycompany.com als Wert des Namens sucht:

```
http.req.hostname.eq(”www.mycompany.com”)
```

Grundlegende Operationen für Ausdruckspräfixe

In der folgenden Tabelle werden einige der grundlegenden Operationen beschrieben, die für Ausdruckspräfixe ausgeführt werden können.

Vorgang	Bestimmt, ob
CONTAINS(<string>)	Das Objekt mit <string> übereinstimmt. Es folgt ein Beispiel: http.req.header(“Cache-Control”).contains(“no-cache”)
EXISTS	Ein bestimmtes Element ist in einem Objekt vorhanden. Es folgt ein Beispiel: http.res.header (“MyHDR”) .exists
EQ(<text>)	Ein bestimmter nicht-numerischer Wert ist in einem Objekt vorhanden. Es folgt ein Beispiel: http.req.method.eq(post)

Vorgang	Bestimmt, ob
EQ(<integer>)	Ein bestimmter numerischer Wert ist in einem Objekt vorhanden. Es folgt ein Beispiel: client.ip.dst.eq(10.100.10.100)
LT(<integer>)	Der Wert eines Objekts ist kleiner als ein bestimmter Wert. Es folgt ein Beispiel: http.req.content_length.lt(5000)
GT(<integer>)	Der Wert eines Objekts ist größer als ein bestimmter Wert. Es folgt ein Beispiel: http.req.content_length.gt(5)

In der folgenden Tabelle werden einige der verfügbaren Arten von Vorgängen zusammengefasst.

Arbeitsvorgangsart	Beschreibung
Textoperationen	Passen Sie einzelne Strings und Sätze von Strings mit einem beliebigen Teil eines Ziels an. Das Ziel kann eine ganze Zeichenfolge, der Anfang einer Zeichenfolge oder ein beliebiger Teil des Textes zwischen dem Anfang und dem Ende der Zeichenfolge sein. Beispielsweise können Sie die Zeichenfolge XYZ aus XYZsoMEText extrahieren. Oder Sie können einen HTTP-Header-Wert mit einem Array verschiedener Zeichenfolgen vergleichen. Sie können Text auch in einen anderen Datentyp umwandeln. Im Folgenden sind Beispiele: Transformieren Sie eine Zeichenfolge in einen Ganzzahlwert, erstellen Sie eine Liste aus den Abfragezeichenfolgen in einer URL und transformieren Sie eine Zeichenfolge in einen Zeitwert.
Numerische Operationen	Numerische Operationen umfassen das Anwenden von arithmetischen Operatoren, das Auswerten der Inhaltslänge, die Anzahl der Elemente in einer Liste, Datums-, Uhrzeit- und IP-Adressen.

Zusammengesetzte erweiterte Richtlinienausdrücke

October 8, 2021

Sie können einen erweiterten Richtlinienausdruck mit booleschen oder arithmetischen Operatoren und atomaren Operationen konfigurieren. Der folgende zusammengesetzte Ausdruck hat ein boolesches UND:

```
http.req.hostname.eq("mycompany.com")&& http.req.method.eq(post)
```

Der folgende Ausdruck fügt den Wert zweier Ziele hinzu und vergleicht das Ergebnis mit einem dritten Wert:

```
http.req.url.length + http.req.cookie.length \<= 500
```

Ein zusammengesetzter Ausdruck kann eine beliebige Anzahl von logischen und arithmetischen Operatoren haben.

Der folgende Ausdruck wertet die Länge einer HTTP-Anforderung aus. Dieser Ausdruck basiert auf der URL und dem Cookie.
Dieser Ausdruck wertet den Text in der Kopfzeile aus. Führt auch ein boolesches UND für diese beiden Ergebnisse aus:

```
http.req.url.length + http.req.cookie.length \<= 500 && http.req.header.
contains("some text")
```

Sie können Klammern verwenden, um die Reihenfolge der Auswertung in einem zusammengesetzten Ausdruck zu steuern.

Booleans in zusammengesetzten Ausdrücken

Sie konfigurieren zusammengesetzte Ausdrücke mit den folgenden Operatoren:

- &&.

  Dieser Operator ist ein logisches AND. Damit der Ausdruck auf TRUE ausgewertet werden kann, müssen alle Komponenten auf TRUE ausgewertet werden.

  Beispiel:

  http.req.url.hostname.eq (MyHost) && http.req.header (MyHeader) .exists

- ||.

  Dieser Operator ist ein logisches ODER. Wenn eine Komponente des Ausdrucks zu TRUE ausgewertet wird, ist der gesamte Ausdruck TRUE.

- !.

  P Ist ein logisches NICHT für den Ausdruck.

Manchmal bietet das Citrix ADC-Konfigurationsdienstprogramm Operatoren UND, NICHT und ODER im Dialogfeld **Ausdruck hinzufügen** an. Diese zusammengesetzten Ausdrücke sind jedoch von eingeschränktem Nutzen. Citrix empfiehlt die Verwendung der Operatoren &&, || und! So konfigurieren Sie zusammengesetzte Ausdrücke, die Boolesche Logik verwenden.

Klammern in zusammengesetzten Ausdrücken

Sie können Klammern verwenden, um die Reihenfolge der Auswertung eines Ausdrucks zu steuern. Ein Beispiel:

```
http.req.url.contains(”myCompany.com”)|| (http.req.url.hostname.eq(”myHost”
)&& http.req.header(”myHeader”).exists)
```

Das folgende Beispiel ist ein weiteres Beispiel:

```
(http.req.header(”Content-Type”).exists && http.req.header(”Content-Type”).
eq(”text/html”))|| (http.req.header(”Transfer-Encoding”).exists || http.req
.header(”Content-Length”).exists)
```

Zusammengesetzte Operationen für Zeichenfolgen

In der folgenden Tabelle werden Operatoren beschrieben, mit denen Sie zusammengesetzte Operationen für Zeichenfolgendaten konfigurieren können.

Vorgänge, die einen Zeichenfolgenwert erzeugen	Beschreibung
str + str	Verkettet den Wert des Ausdrucks links vom Operator mit dem Wert auf der rechten Seite. Beispiel: http.req.hostname + http.req.url.protocol
str + num	Verkettet den Wert des Ausdrucks links vom Operator mit einem numerischen Wert auf der rechten Seite. Beispiel: http.req.hostname + http.req.url.content_length
num + str	Verkettet den numerischen Wert des Ausdrucks auf der linken Seite des Operators mit einem Zeichenfolgenwert auf der rechten Seite. Beispiel: http.req.url.content_length + http.req.url.hostname

Vorgänge, die einen Zeichenfolgenwert erzeugen	Beschreibung
str + IP	Verkettet den Zeichenfolgenwert des Ausdrucks auf der linken Seite des Operators mit einem IP-Adresswert auf der rechten Seite. Beispiel: http.req.hostname + 10.00.000.00
IP + str	Verkettet den IP-Adresswert des Ausdrucks links vom Operator mit einem Zeichenfolgenwert auf der rechten Seite. Beispiel: client.ip.dst + http.req.url.hostname
str1 ALT str2	Verwendet string2, wenn die Auswertung von String1 zu einer undef-Ausnahme führt oder das Ergebnis eine Nullzeichenfolge ist. Ansonsten verwendet string1 und wertet niemals String2 aus. Beispiel: http.req.hostname alt client.ip.src

Operationen an Zeichenfolgen, die ein Ergebnis von TRUE oder FALSE erzeugen	Beschreibung
str == str	Prüft, ob die Zeichenfolgen auf beiden Seiten des Operators identisch sind. Es folgt ein Beispiel: http.req.header (myheader) == http.res.header (myheader)
str <= str	Prüft, ob die Zeichenfolge auf der linken Seite des Operators mit der Zeichenfolge auf der rechten oder alphabetisch vorangestellt ist.
str >= str	Prüft, ob die Zeichenfolge auf der linken Seite des Operators mit der Zeichenfolge auf der rechten Seite übereinstimmt oder alphabetisch folgt.
str < str	Prüft, ob die Zeichenfolge auf der linken Seite des Operators der Zeichenfolge auf der rechten Seite alphabetisch vorausgeht.
str > str	Prüft, ob die Zeichenfolge auf der linken Seite des Operators der Zeichenfolge rechts alphabetisch folgt.

Operationen an Zeichenfolgen, die ein Ergebnis von TRUE oder FALSE erzeugen	Beschreibung
str!! = str	Prüft, ob die Strings auf beiden Seiten des Operators unterschiedlich sind.

Logische Operationen an Strings	Beschreibung
bool && bool	Dieser Operator ist ein logisches AND. Bei der Auswertung der Komponenten des zusammengesetzten Ausdrucks müssen alle Komponenten, die durch das UND verbunden sind, mit TRUE ausgewertet werden. Es folgt ein Beispiel: http.req.method.eq (GET) && http.req.url.query.contains (“viewReport && my_pagelabel”)
bool || bool	Dieser Operator ist ein logisches ODER. Wenn bei der Auswertung der Komponenten des zusammengesetzten Ausdrucks eine Komponente des Ausdrucks, der zu OR gehört, mit TRUE ausgewertet wird, ist der gesamte Ausdruck WAHR. Es folgt ein Beispiel: http.req.url.contains (“.js”) || http.res.header. (“Inhaltstyp”). Enthält (“Javascript”)
bool	Führt ein logisches NOT für den Ausdruck aus.

Zusammengesetzte Operationen für Zahlen

Sie können zusammengesetzte numerische Ausdrücke konfigurieren. Der folgende Ausdruck gibt beispielsweise einen numerischen Wert zurück, der die Summe einer HTTP-Headerlänge und einer URL-Länge ist:

```
http.req.header.length + http.req.url.length
```

In den folgenden Tabellen werden Operatoren beschrieben, mit denen Sie zusammengesetzte Ausdrücke für numerische Daten konfigurieren können.

Arithmetische Operationen auf Zahlen	Beschreibung
num + num	Fügen Sie den linken Ausdruckswert des Operators zum rechten Ausdruckswert hinzu. Beispiel: http.req.content_length + http.req.url.length
num — num	Subtrahieren Sie den rechten Ausdruckswert des Operators vom linken Ausdruckswert.
num x num	Multiplizieren Sie den linken Ausdruckswert des Operators mit dem rechten Ausdruckswert. Beispiel: client.interface.rxthroughput * 9
num/num	Teilen Sie den linken Ausdruckswert des Operators durch den rechten Ausdruckswert.
Anzahl% num	Berechnen Sie den Modulo oder den numerischen Rest einer Division des Wertes des Ausdrucks links vom Operator durch den Wert des Ausdrucks auf der rechten Seite. Zum Beispiel sind die Werte “15 mod 4” gleich 3 und “12 mod 4” gleich 0.

Arithmetische Operationen auf Zahlen	Beschreibung
~Zahl	Gibt eine Zahl zurück, nachdem eine bitweise logische Negation der Zahl angewendet wurde. Im folgenden Beispiel wird davon ausgegangen, dass numeric.expression 12 (binär 1100) zurückgibt: ~numeric.expression. Das Ergebnis der Anwendung des Operator ~ ist -11 (ein binärer 1110011, insgesamt 32 Bit mit allen nach links). Alle zurückgegebenen Werte von weniger als 32 Bit vor der Anwendung des Operators haben implizit Nullen auf der linken Seite, um sie 32 Bit breit zu machen.

Arithmetische Operationen auf Zahlen	Beschreibung
Zahl ^ Zahl	Vergleicht zwei Bitmuster gleicher Länge und führt eine XOR-Operation für jedes Paar der entsprechenden Bits in jedem Zahlenargument durch, wobei 1 zurückgegeben wird, wenn die Bits unterschiedlich sind, und 0, wenn sie identisch sind. Gibt eine Zahl zurück, nachdem ein bitweises XOR auf das ganzzahlige Argument und den aktuellen Zahlenwert angewendet wurde. Wenn die Werte im bitweisen Vergleich identisch sind, ist der zurückgegebene Wert 0. Im folgenden Beispiel wird davon ausgegangen, dass numeric.expression1 12 (binär 1100) zurückgibt und numeric.expression2 10 (binär 1010) zurückgibt: numeric.expression1 ^ numeric.expression2 Das Ergebnis der Anwendung des Operator ^ auf den gesamten Ausdruck ist 6 (binär 0110). Alle zurückgegebenen Werte von weniger als 32 Bit vor der Anwendung des Operators haben implizit Nullen auf der linken Seite, um sie 32 Bit breit zu machen.

Arithmetische Operationen auf Zahlen	Beschreibung	
Anzahl | Anzahl	Gibt eine Zahl nach dem Anwenden eines bitweisen ODER auf die Zahlenwerte zurück. Wenn einer der Werte im bitweisen Vergleich eine 1 ist, ist der zurückgegebene Wert ein 1. Im folgenden Beispiel wird davon ausgegangen, dass numeric.expression1 12 (binär 1100) und numeric.expression2 10 (binär 1010) zurückgibt: numeric.expression1 | numeric.expression2 Das Ergebnis der Anwendung des Operator	auf den gesamten Ausdruck ist 14 (binär 1110). Alle zurückgegebenen Werte von weniger als 32 Bit vor der Anwendung des Operators haben implizit Nullen auf der linken Seite, um sie 32 Bit breit zu machen.

Arithmetische Operationen auf Zahlen	Beschreibung
Nummer & Nummer	Vergleicht zwei Bitmuster gleicher Länge und führt eine bitweise UND -Operation für jedes Paar entsprechender Bits aus, wobei 1 zurückgegeben wird, wenn beide Bits den Wert 1 enthalten, und 0, wenn eine der Bits 0 sind. Im folgenden Beispiel wird davon ausgegangen, dass numeric.expression1 12 (binär 1100) und numeric.expression2 10 (binär 1010) zurückgibt: numeric.expression1 & numeric.expression2 Der gesamte Ausdruck wird als 8 (binär 1000) ausgewertet. Alle zurückgegebenen Werte von weniger als 32 Bit vor der Anwendung des Operators haben implizit Nullen auf der linken Seite, um sie 32 Bit breit zu machen.

Arithmetische Operationen auf Zahlen	Beschreibung
num « num	Gibt eine Zahl nach einer bitweisen linken Verschiebung des Zahlenwertes um die rechte Zahl Argument Anzahl der Bits zurück. Die Anzahl der verschobenen Bits ist Integer Modulo 32. Im folgenden Beispiel wird davon ausgegangen, dass numeric.expression1 12 (binär 1100) zurückgibt und numeric.expression2 3 zurückgibt: numeric.expression1 « numeric.expression2 Das Ergebnis der Anwendung des LSHIFT-Operators ist 96 (ein binäres 1100000). Alle zurückgegebenen Werte von weniger als 32 Bit vor der Anwendung des Operators haben implizit Nullen auf der linken Seite, um sie 32 Bit breit zu machen.

Arithmetische Operationen auf Zahlen	Beschreibung
num » num	Gibt eine Zahl nach einer bitweisen rechten Verschiebung des Zahlenwertes um die ganzzahlige Argumentanzahl der Bits zurück. Die Anzahl der verschobenen Bits ist Integer Modulo 32. Im folgenden Beispiel wird davon ausgegangen, dass numeric.expression1 12 (binär 1100) und numeric.expression2 3 zurückgibt: numeric.expression1 » numeric.expression2 Das Ergebnis der Anwendung des RSHIFT-Operators ist 1 (binär 0001). Alle zurückgegebenen Werte von weniger als 32 Bit vor der Anwendung des Operators haben implizit Nullen auf der linken Seite, um sie 32 Bit breit zu machen.

Numerische Operatoren, die ein Ergebnis von TRUE oder FALSE erzeugen	Beschreibung
num == num	Bestimmen Sie, ob der Wert des Ausdrucks links vom Operator dem Wert des Ausdrucks auf der rechten Seite entspricht.

Numerische Operatoren, die ein Ergebnis von TRUE oder FALSE erzeugen	Beschreibung
num! = num	Bestimmen Sie, ob der Wert des Ausdrucks links vom Operator nicht dem Wert des Ausdrucks auf der rechten Seite entspricht.
num > num	Bestimmen Sie, ob der Wert des Ausdrucks links vom Operator größer ist als der Wert des Ausdrucks auf der rechten Seite.
num < num	Bestimmen Sie, ob der Wert des Ausdrucks links vom Operator kleiner ist als der Wert des Ausdrucks auf der rechten Seite.
num >= num	Bestimmen Sie, ob der Wert des Ausdrucks links vom Operator größer oder gleich dem Wert des Ausdrucks auf der rechten Seite ist.
num <= num	Bestimmen Sie, ob der Wert des Ausdrucks links vom Operator kleiner oder gleich dem Wert des Ausdrucks auf der rechten Seite ist

Funktionen für Datentypen in der Richtlinieninfrastruktur

Die Citrix ADC Richtlinieninfrastruktur unterstützt die folgenden numerischen Datentypen:

- Ganzzahl (32 Bit)
- Langes Vorzeichen (64 Bit)
- Doppel (64 Bit)

Einfache Ausdrücke können alle diese Datentypen zurückgeben. Sie können auch zusammengesetzte Ausdrücke erstellen, die arithmetische Operatoren und logische Operatoren verwenden, um die Werte

dieser Datentypen auszuwerten oder zurückzugeben. Sie können alle diese Werte auch in Richtlinienausdrücken verwenden. Literal Konstanten vom Typ unsigned long können durch Anhängen der Zeichenfolge ul an die Zahl angegeben werden. Literale Konstanten vom Typ double enthalten einen Punkt (.), einen Exponenten oder beides.

Arithmetische Operatoren, logische Operatoren und Typerhöhung

In zusammengesetzten Ausdrücken können die folgenden standardmäßigen arithmetischen und logischen Operatoren für die langen Datentypen double und unsigned signed verwendet werden:

- +, -, * und/
- %, ~, ^, &, |, <><, and > (gelten nicht für Double)
- ==,! =, >, <, >= und <=

Alle diese Operatoren haben die gleiche Bedeutung wie in der Programmiersprache C.

In allen Fällen von gemischten Operationen zwischen Operanden vom Typ integer, unsigned long und double. Die Typenförderung wird durchgeführt, um die Operation an den Operanden desselben Typs durchzuführen. Die Operation fördert einen Typ mit niedrigerer Rangfolge für den Operanden mit der höchsten Rangfolge. Die Rangfolge (höher nach niedriger) lautet wie folgt:

- Doppelt
- Nicht signiert lang
- Ganzzahl

Eine Operation, die ein numerisches Ergebnis zurückgibt, gibt also ein Ergebnis des höchsten Typs zurück, der an der Operation beteiligt ist.

Beispiel: Wenn die Operanden vom Typ Integer und Long ohne Vorzeichen sind, wird der Integer-Operand automatisch in den Typ unsigned long konvertiert. Diese Typkonvertierung erfolgt in einfachen Ausdrücken. Der durch das Ausdruckspräfix identifizierte Datentyp stimmt nicht mit dem Datentyp überein, der als Argument an die Funktion übergeben wird. In der Operation HTTP.REQ.CONTENT_LENGTH.DIV (3ul) gibt das Präfix HTTP.REQ.CONTENT_LENGTH eine Ganzzahl zurück, die zu einem Long ohne Vorzeichen wird. Unsigned long: Der Datentyp, der als Argument an die DIV () -Funktion übergeben wird, wird eine lange Division ohne Vorzeichen ausgeführt. Ebenso kann das Argument in einem Ausdruck heraufgestuft werden. Zum Beispiel fördert HTTP.REQ.HEADER (“MyHeader”) .TYPECAST_DOUBLE_AT.DIV (5) die ganze Zahl 5 zur Eingabe von Double und führt eine Division mit doppelter Genauigkeit durch.

Informationen zu Ausdrücken zum Umwandeln von Daten eines Typs in Daten eines anderen Typs finden Sie unter Typecasting von Daten.

Festlegen des Zeichensatzes in Ausdrücken

October 5, 2021

Die Richtlinieninfrastruktur auf der Citrix ADC Appliance unterstützt ASCII- und UTF-8-Zeichensätze. Der Standardzeichensatz ist ASCII. Wenn der Datenverkehr, für den Sie einen Ausdruck konfigurieren, nur aus ASCII-Zeichen besteht, müssen Sie den Zeichensatz im Ausdruck nicht angeben. Die Appliance erlaubt alle Zeichenfolgen- und Zeichenliterale, die binäre Zeichen enthalten. Die UTF-8-Zeichensätze erfordern jedoch immer noch die Zeichenfolgen- und Zeichenliterale, um ein gültiges UTF-8 zu sein.

```
CLIENT.TCP.PAYLOAD(100).CONTAINS("\xff\x02")
```

In einem Ausdruck muss die Funktion SET_CHAR_SET () an der Stelle des Ausdrucks eingeführt werden, nach der die Datenverarbeitung im angegebenen Zeichensatz durchgeführt werden muss. Beispielsweise müssen Sie im Ausdruck HTTP.REQ.BODY (1000) .AFTER_REGEX (re/folgendes Beispiel/) .BEFORE_REGEX (re/im vorhergehenden Beispiel/) .CONTAINS_ANY (Greek_ alphabet), wenn die im Mustersatz Greek_alphabet gespeicherten Strings in UTF-8 enthalten sind, die SET_CHAR_SET (UTF_8) Funktion unmittelbar vor der <string> Funktion CONTAINS_ANY ( ) wie folgt:

```
HTTP.REQ.BODY(1000).AFTER_REGEX(re/following example/).BEFORE_REGEX(re/In
the preceding example/).SET_CHAR_SET(UTF_8).CONTAINS_ANY("Greek_ alphabet")
```

Die Funktion SET_CHAR_SET () setzt den Zeichensatz für die weitere Verarbeitung (d. h. für alle nachfolgenden Funktionen) im Ausdruck, es sei denn, er wird später im Ausdruck durch eine andere SET_CHAR_SET () -Funktion überschrieben, die den Zeichensatz ändert. Wenn also alle Funktionen eines bestimmten einfachen Ausdrucks für UTF-8 vorgesehen sind, können Sie die Funktion SET_CHAR_SET (UTF_8) unmittelbar nach Funktionen einschließen, die Text identifizieren (z. B. die <name> <int> Funktionen HEADER ( ) oder BODY ()). Wenn die ASCII-Argumente, die an die Funktionen AFTER_REGEX () und BEFORE_REGEX () übergeben werden, in UTF-8-Zeichenfolgen geändert werden, können Sie die Funktion SET_CHAR_SET (UTF_8) unmittelbar nach der Funktion BODY (1000) wie folgt einschließen:

```
HTTP.REQ.BODY(1000).SET_CHAR_SET(UTF_8).AFTER_REGEX(re/Bücher/).BEFORE_REGEX
(re/Wörterbuch/).CONTAINS_ANY("Greek_alphabet")
```

Der UTF-8-Zeichensatz ist eine Obermenge des ASCII-Zeichensatzes. Daher funktionieren Ausdrücke, die für den ASCII-Zeichensatz konfiguriert sind, wie erwartet, wenn Sie den Zeichensatz in UTF-8 ändern.

Zusammengesetzte Ausdrücke mit verschiedenen Zeichensätzen

Wenn in einem zusammengesetzten Ausdruck eine Teilmenge von Ausdrücken so konfiguriert ist, dass sie mit Daten im ASCII-Zeichensatz arbeitet und die restlichen Ausdrücke so konfiguriert sind, dass

sie mit Daten im UTF-8-Zeichensatz arbeiten, wird der für jeden einzelnen Ausdruck angegebene Zeichensatz berücksichtigt, wenn die Ausdrücke ausgewertet werden einzeln. Bei der Verarbeitung des zusammengesetzten Ausdrucks wird jedoch kurz vor der Verarbeitung der Operatoren der Zeichensatz der zurückgegebenen ASCII-Werte auf UTF-8 heraufstuft. Beispiel: Im folgenden zusammengesetzten Ausdruck wertet der erste einfache Ausdruck Daten im ASCII-Zeichensatz aus, während der zweite einfache Ausdruck Daten im UTF-8-Zeichensatz auswertet:

```
HTTP.REQ.HEADER(”MyHeader”)== HTTP.REQ.BODY(10).SET_CHAR_SET(UTF_8)
```

Bei der Verarbeitung des zusammengesetzten Ausdrucks wird jedoch kurz vor der Auswertung des booleschen Operators is equal to die Citrix ADC Appliance den Zeichensatz des von HTTP.REQ.HEADER (MyHeader) zurückgegebenen Werts zu UTF-8 heraufstuft.

Der erste einfache Ausdruck im folgenden Beispiel wertet Daten im ASCII-Zeichensatz aus. Wenn die Citrix ADC Appliance den zusammengesetzten Ausdruck jedoch unmittelbar vor dem Verketten der Ergebnisse der beiden einfachen Ausdrücke verarbeitet, fördert die Appliance den Zeichensatz des von HTTP.REQ.BODY (10) zurückgegebenen Werts zu UTF-8.

```
HTTP.REQ.BODY(10)+ HTTP.REQ.HEADER(”MyHeader”).SET_CHAR_SET(UTF_8)
```

Daher gibt der zusammengesetzte Ausdruck Daten im UTF-8-Zeichensatz zurück.

Festlegen des Zeichensatzes basierend auf dem Zeichensatz des Datenverkehrs

Sie können den Zeichensatz auf UTF-8 basierend auf Verkehrsmerkmalen festlegen. Wenn Sie nicht sicher sind, ob der Zeichensatz des ausgewerteten Datenverkehrs UTF-8 ist, können Sie einen zusammengesetzten Ausdruck konfigurieren, in dem der erste Ausdruck auf UTF-8-Datenverkehr überprüft und nachfolgende Ausdrücke den Zeichensatz auf UTF-8 setzen. Es folgt ein Beispiel für einen zusammengesetzten Ausdruck, der zuerst den Wert von charset im Content-Type-Header der Anforderung für UTF-8 überprüft, bevor überprüft wird, ob die ersten 1000 Bytes in der Anforderung die UTF-8-Zeichenfolge Bücher enthalten:

```
HTTP.REQ.HEADER(”Content-Type”).SET_TEXT_MODE(IGNORECASE).TYPECAST_NVLIST_T
('=', '; ', '”').VALUE(”charset”).EQ(”UTF-8”)&& HTTP.REQ.BODY(1000).SET_CHAR_SET
(UTF_8).CONTAINS(”Bücher”)
```

Wenn Sie sicher sind, dass der Zeichensatz des ausgewerteten Datenverkehrs UTF-8 ist, ist der zweite Ausdruck im Beispiel ausreichend.

Zeichen- und Zeichenfolgenliterale in Ausdrücken

Auch wenn der aktuelle Zeichensatz ASCII ist, werden während der Ausdrucksauswertung Zeichenliterale und Zeichenfolgenliterale, die in einfache Anführungszeichen (‘) und Anführungszeichen ()

eingeschlossen sind, als Literale im UTF-8-Zeichensatz betrachtet. Wenn in einem bestimmten Ausdruck eine Funktion für Zeichen- oder Zeichenfolgenliterale im ASCII-Zeichensatz arbeitet und Sie ein Nicht-ASCII-Zeichen in das Literal einfügen, wird ein Fehler zurückgegeben.

> **Hinweis**:
>
> Die Zeichenfolgenliterale in erweiterten Richtlinienausdrücken sind jetzt so lang wie der Richtlinienausdruck. Der Ausdruck darf 1499 Bytes oder 8191 Bytes lang sein.

Werte im Hexadezimal- und Oktalformat

Beim Konfigurieren eines Ausdrucks können Sie Werte in oktaler und hexadezimaler Form eingeben. Jedes hexadezimale oder oktales Byte gilt jedoch als UTF-8-Byte. Ungültige UTF-8-Bytes führen zu Fehlern, unabhängig davon, ob der Wert manuell eingegeben oder aus der Zwischenablage eingefügt wird. Beispiel: "\xce\x20" ist ein ungültiges UTF-8-Zeichen, da "c8" nicht von "20" gefolgt werden kann (jedes Byte in einem Multi-Byte-UTF-8-String muss das hohe Bit gesetzt haben). Ein weiteres Beispiel für ein ungültiges UTF-8-Zeichen ist xce xa9, da die hexadezimalen Zeichen durch ein Leerzeichen getrennt sind.

Funktionen, die UTF-8-Strings zurückgeben

Nur die `text>.XPATH` Funktionen `<text>.XPATH_JSON` und geben immer UTF-8-Strings zurück. Die folgenden MYSQL-Routinen bestimmen zur Laufzeit, welcher Zeichensatz zurückgegeben werden soll, abhängig von den Daten im Protokoll:

- `MYSQL_CLIENT_T.USER`
- `MYSQL_CLIENT_T.DATABASE`
- `MYSQL_REQ_QUERY_T.COMMAND`
- `MYSQL_REQ_QUERY_T.TEXT`
- `MYSQL_REQ_QUERY_T.TEXT(<unsigned int>)`
- `MYSQL_RES_ERROR_T.SQLSTATE`
- `MYSQL_RES_ERROR_T.MESSAGE`
- `MYSQL_RES_FIELD_T.CATALOG`
- `MYSQL_RES_FIELD_T.DB`
- `MYSQL_RES_FIELD_T.TABLE`
- `MSQL_RES_FIELD_T.ORIGINAL_TABLE`
- `MYSQL_RES_FIELD_T.NAME`
- `MYSQL_RES_FIELD_T.ORIGINAL_NAME`
- `MYSQL_RES_OK_T.MESSAGE`
- `MYSQL_RES_ROW_T.TEXT_ELEM(<unsigned int>)`

Terminalverbindungseinstellungen für UTF-8

Wenn Sie eine Verbindung zur Citrix ADC Appliance mithilfe einer Terminalverbindung (z. B. mithilfe von PuTTY) einrichten, müssen Sie den Zeichensatz für die Übertragung von Daten an UTF-8 festlegen.

Minimale und maximale Funktionen in einem erweiterten Richtlinienausdruck

Die erweiterten Richtlinienausdrücke unterstützen die folgenden minimalen und maximalen Funktionen.

1. (<expression1>.max(<expression2>) - gibt das Maximum der beiden Werte zurück.
2. (<expression1>.min(<expression2>) - gibt das Minimum der beiden Werte zurück.

Klassische Ausdrücke in erweiterten Richtlinienausdrücken

September 1, 2022

> **Warnung:**
>
> Klassische Richtlinienausdrücke werden ab Citrix ADC 12.0 Build 56.20 nicht mehr unterstützt. Alternativ empfiehlt Citrix die Verwendung von erweiterten Richtlinien. Weitere Informationen finden Sie unter Konfigurieren von erweiterten Richtlinienausdrücken: Erste Schritte.

Klassische Ausdrücke beschreiben die grundlegenden Eigenschaften von Traffic. Manchmal möchten Sie möglicherweise einen klassischen Ausdruck in einem erweiterten Richtlinienausdruck verwenden.

Im Folgenden finden Sie die Syntax für alle erweiterten Richtlinienausdrücke, die einen klassischen Ausdruck verwenden:

SYS.EVAL_CLASSIC_EXPR(“expression”)

> **Hinweis:**
>
> Die Syntax und die Metadaten für den SYS.EVAL_CLASSIC_EXPR-Ausdruck werden veraltet. Sie können den klassischen Ausdruck manuell konvertieren oder das Werkzeug nspepi verwenden, um den klassischen Ausdruck in den erweiterten Ausdruck zu konvertieren.

Im Folgenden finden Sie Beispiele für den Ausdruck SYS.EVAL_CLASSIC_EXPR(“expression”):

```
1 sys.eval_classic_expr(”req.ssl.client.cipher.bits > 1000”)
2 sys.eval_classic_expr(”url contains abc”)
3 sys.eval_classic_expr(”req.ip.sourceip == 10.102.1.61 -netmask
     255.255.255.255”)
```



```
4 sys.eval_classic_expr(”time >= *:30:00GMT”)
5 sys.eval_classic_expr(”e1 || e2”)
6 sys.eval_classic_expr(”req.http.urllen > 50”)
7 sys.eval_classic_expr(”dayofweek == wedGMT”)
8 <!--NeedCopy-->
```

Konfigurieren erweiterter Richtlinienausdrücke in einer Richtlinie

December 7, 2021

Sie können einen erweiterten Richtlinienausdruck mit bis zu 1.499 Zeichen in einer Richtlinie konfigurieren. Die Benutzeroberfläche für erweiterte Richtlinienausdrücke hängt in gewissem Maße von der Funktion ab, für die Sie den Ausdruck konfigurieren, und davon, ob Sie einen Ausdruck für eine Richtlinie oder für eine andere Verwendung konfigurieren.

Wenn Sie Ausdrücke in der Befehlszeile konfigurieren, grenzen Sie den Ausdruck mithilfe von Anführungszeichen (.. oder ..) ab. Innerhalb eines Ausdrucks können Sie zusätzliche Anführungszeichen mit einem umgekehrten Schrägstrich () umgehen. Zum Beispiel sind die folgenden Standardmethoden zum Escapieren von Anführungszeichen in einem Ausdruck:

```
”\”abc\””
```

```
‘\”abc\”’
```

Sie müssen auch einen umgekehrten Schrägstrich verwenden, um Fragezeichen und andere umgekehrte Schrägstriche in der Befehlszeile zu entkommen. Zum Beispiel der Ausdruck http.req.url.contains (?) erfordert einen umgekehrten Schrägstrich, damit das Fragezeichen analysiert wird. Beachten Sie, dass der umgekehrte Schrägstrich nicht in der Befehlszeile angezeigt wird, nachdem Sie das Fragezeichen eingegeben haben. Auf der anderen Seite, wenn Sie einen umgekehrten Schrägstrich entweichen (zum Beispiel im Ausdruck ‘http.req.url.contains (http) ‘), werden die Escape-Zeichen in der Befehlszeile wiedergegeben.

Um einen Eintrag besser lesbar zu machen, können Sie die Anführungszeichen für einen gesamten Ausdruck umgehen. Am Anfang des Ausdrucks geben Sie die Escape-Sequenz q plus eines der folgenden Sonderzeichen ein:/{<	~$^+=&%@‘?.

Sie geben nur das Sonderzeichen am Ende des Ausdrucks wie folgt ein:


```
q@http.req.url.contains(”sometext”) && http.req.cookie.exists@

q~http.req.url.contains(”sometext”) && http.req.cookie.exists~
<!--NeedCopy-->
```

Beachten Sie, dass ein Ausdruck, der das Trennzeichen { verwendet, mit } geschlossen wird.

Einige Features (z. B. Integriertes Caching und Responder) stellt das Dialogfeld zur Richtlinienkonfiguration ein sekundäres Dialogfeld zum Konfigurieren von Ausdrücken bereit. In diesem Dialogfeld können Sie aus Dropdownlisten auswählen, in denen die verfügbaren Optionen an jedem Punkt während der Ausdruckskonfiguration angezeigt werden. Sie können keine arithmetischen Operatoren verwenden, wenn Sie diese Konfigurationsdialoge verwenden, aber die meisten anderen erweiterten Richtlinienausdrucksfeatures sind verfügbar. Um arithmetische Operatoren zu verwenden, schreiben Sie Ihre Ausdrücke im Freiformformat.

Konfigurieren einer erweiterten Richtlinien-Syntaxregel mit der CLI

> **Hinweis:**
>
> Standard-Syntaxrichtlinie wird jetzt in Erweiterte Richtlinie umbenannt.

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

1. `add cache|dns|rewrite|cs policy policyName **-rule** expression featureSpecificPa **-action**`
2. `show cache|dns|rewrite|cs policy policyName`
   Es folgt ein Beispiel für die Konfiguration einer Caching-Richtlinie:

   Beispiel:

```
> add cache policy pol-cache -rule http.req.content_length.le(5) -
    action INVAL
 Done

> show cache policy pol-cache
        Name: pol-cache
        Rule: http.req.content_length.le(5)
        CacheAction: INVAL
        Invalidate groups: DEFAULT
        UndefAction: Use Global
        Hits: 0
        Undef Hits: 0
```



```
12
13   Done
14 <!--NeedCopy-->
```

Konfigurieren eines standardmäßigen Syntaxrichtlinienausdrucks mit der GUI

1. Klicken Sie im Navigationsbereich auf den Namen des Features, in dem Sie eine Richtlinie konfigurieren möchten. Sie können z. B. integrierte Zwischenspeicherung, Responder, DNS, Umschreiben oder Content Switching auswählen und dann auf **Richtlinien** klicken.
2. Klicken Sie auf Hinzufügen.
3. Klicken Sie für die meisten Features in das Feld **Ausdruck**. Klicken Sie für das Content Switching auf **Konfigurieren**.
4. Klicken Sie auf das **Präfixsymbol** (das Haus) und wählen Sie das erste Ausdruckspräfix aus der Dropdownliste aus. Beispielsweise sind in Responder die Optionen HTTP, SYS und CLIENT. Der nächste Satz anwendbarer Optionen wird in einer Dropdownliste angezeigt.
5. Doppelklicken Sie auf die nächste Option, um sie auszuwählen, und geben Sie dann einen Punkt (.) ein. Auch hier wird eine Reihe von anwendbaren Optionen in einer anderen Dropdownliste angezeigt.
6. Setzen Sie die Auswahl der Optionen fort, bis ein Eingabefeld (durch Klammern signalisiert) angezeigt wird. Wenn ein Eingabefeld angezeigt wird, geben Sie einen entsprechenden Wert in die Klammern ein. Wenn Sie z. B. GT (int) (größer als, ganzzahliges Format) auswählen, geben Sie eine ganze Zahl in den Klammern an. Textzeichenfolgen werden durch Anführungszeichen getrennt. Es folgt ein Beispiel:

   ```
   HTTP.REQ.BODY(1000).BETWEEN("this","that")
   ```

7. Um einen Operator zwischen zwei Teilen eines zusammengesetzten Ausdrucks einzufügen, klicken Sie auf das Symbol Operatoren (das Sigma), und wählen Sie den Operatortyp aus. Es folgt ein Beispiel für einen konfigurierten Ausdruck mit einem booleschen OR (signalisiert durch doppelte vertikale Balken, ||):

   ```
   HTTP.REQ.URL.EQ("www.mycompany.com")||HTTP.REQ.BODY(1000).BETWEEN("this
   ","that")
   ```

8. Um einen benannten Ausdruck einzufügen, klicken Sie auf den Pfeil nach unten neben dem Symbol Hinzufügen (das Pluszeichen), und wählen Sie einen benannten Ausdruck aus.
9. Um einen Ausdruck mithilfe von Dropdownmenüs zu konfigurieren und integrierte Ausdrücke einzufügen, klicken Sie auf das Symbol Hinzufügen (das Pluszeichen). Das Dialogfeld **Ausdruck hinzufügen** funktioniert ähnlich wie das Hauptdialogfeld, enthält jedoch Dropdownlisten für die Auswahl von Optionen und stellt Textfelder für die Dateneingabe anstelle von Klammern

bereit. Dieses Dialogfeld enthält auch eine Dropdownliste Häufig verwendete Ausdrücke, in der häufig verwendete Ausdrücke eingefügt werden. Wenn Sie mit dem Hinzufügen des Ausdrucks fertig sind, klicken Sie auf **OK**.

10. Wenn Sie fertig sind, klicken Sie auf **Erstellen**. Eine Meldung in der Statusleiste zeigt an, dass der Richtlinienausdruck erfolgreich konfiguriert wurde.

Testen eines Standard-Syntaxausdrucks mit der GUI

1. Klicken Sie im Navigationsbereich auf den Namen des Features, für das Sie eine Richtlinie konfigurieren möchten (z. B. können Sie Integriertes Caching, Responder, DNS, Umschreiben oder Content Switching auswählen), und klicken Sie dann auf Richtlinien.
2. Wählen Sie eine Richtlinie aus, und klicken Sie auf **Öffnen**.
3. Um den Ausdruck zu testen, klicken Sie auf das Symbol Auswerten (das Häkchen).
4. Wählen Sie im Dialogfeld Ausdrucksauswerter den Flow Type aus, der dem Ausdruck entspricht.
5. Fügen Sie im Feld **HTTP-Anforderungsdaten** oder **HTTP-Antwortdaten** die HTTP-Anforderung oder Antwort ein, die Sie mit dem Ausdruck analysieren möchten, und klicken Sie auf**Auswerten**. Beachten Sie, dass Sie eine vollständige HTTP-Anforderung oder Antwort angeben müssen, und der Header und der Text sollten durch eine Leerzeile getrennt werden. Einige Programme, die HTTP-Header abfangen, fangen die Antwort nicht auch ab. Wenn Sie nur den Header kopieren und einfügen, fügen Sie eine leere Zeile am Ende der Kopfzeile ein, um eine vollständige HTTP-Anforderung oder Antwort zu bilden.
6. Klicken Sie auf **Schließen**, um dieses Dialogfeld zu schließen.

Konfigurieren von benannten erweiterten Richtlinienausdrücken

October 5, 2021

Anstatt denselben Ausdruck mehrmals in mehreren Richtlinien erneut einzugeben, können Sie einen benannten Ausdruck konfigurieren und jederzeit auf den Namen verweisen, wenn Sie den Ausdruck in einer Richtlinie verwenden möchten. Beispielsweise können Sie die folgenden benannten Ausdrücke erstellen:

- ThisExpression:

  ```
  http.req.body(100).contains("this")
  ```

- ThatExpression:

  ```
  http.req.body(100).contains("that")
  ```


Sie können diese benannten Ausdrücke dann in einem Richtlinienausdruck verwenden. Der folgende Ausdruck ist beispielsweise ein rechtlicher Ausdruck, der auf den vorangegangenen Beispielen basiert:

ThisExpression	ThatExpression

Sie können den Namen eines erweiterten Richtlinienausdrucks als Präfix einer Funktion verwenden. Der benannte Ausdruck kann entweder ein einfacher Ausdruck oder ein zusammengesetzter Ausdruck sein. Die Funktion muss eine Funktion sein, die für den Datentyp arbeiten kann, der vom benannten Ausdruck zurückgegeben wird.

Beispiel 1: Einfacher benannter Ausdruck als Präfix

Der folgende einfache benannte Ausdruck, der eine Textzeichenfolge identifiziert, kann als Präfix für die <string> Funktion AFTER_STR ( ) verwendet werden, die mit Textdaten arbeitet:

```
HTTP.REQ.BODY(1000)
```

Wenn der Name des Ausdrucks Top1kB lautet, können Sie Top1kB.after_str (username) anstelle von HTTP.REQ.BODY (1000) .AFTER_STR (username) verwenden.

Beispiel 2: Zusammengesetzte benannte Ausdrücke als Präfix

Sie können einen zusammengesetzten benannten Ausdruck namens basic_header_value erstellen, um den Benutzernamen in einer Anforderung, einen Doppelpunkt (:) und das Kennwort des Benutzers wie folgt zu verketten:

```
add policy expression basic_header_value ”HTTP.REQ.USER.NAME + \”:\” + HTTP
.REQ.USER.PASSWD”
```

Sie können dann den Namen des Ausdrucks in einer Umschreibaktion verwenden, wie im folgenden Beispiel gezeigt:

```
add rewrite action insert_b64encoded_authorization insert_http_header
authorization '”Basic ” + basic_header_value.b64encode'-bypassSafetyCheck
 YES
```

Im Beispiel wird in dem Ausdruck, der zum Erstellen des Werts des benutzerdefinierten Headers verwendet wird, der B64-Kodierungsalgorithmus auf die Zeichenfolge angewendet, die von der zusammengesetzten benannten Ausdruck zurückgegeben wird.

Sie können auch einen benannten Ausdruck (entweder selbst oder als Präfix einer Funktion) verwenden, um den Textausdruck für das Ersetzungsziel in einem Umschreiben zu erstellen.

Konfigurieren eines benannten Standard-Syntaxausdrucks mit der CLI

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

```
1 -  add policy expression <name><value>
2
3 -  show policy expression <name>
4 <!--NeedCopy-->
```

Beispiel:

```
1 > add policy expression myExp ”http.req.body(100).contains(”the other”)
     ”
2 Done
3
4 > show policy expression myExp
5     1)      Name: myExp  Expr: ”http.req.body(100).contains(”the other”
          )”  Hits: 0 Type : ADVANCED
6 Done
7 <!--NeedCopy-->
```

Der Ausdruck kann bis zu 1.499 Zeichen lang sein.

Konfigurieren eines benannten Ausdrucks mit der GUI

1. Erweitern Sie im Navigationsbereich **AppExpert**, und klicken Sie dann auf **Ausdrücke**.
2. Klicken Sie auf **Erweiterte Ausdrücke**.
3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie einen Namen und eine Beschreibung für den Ausdruck ein.
5. Konfigurieren Sie den Ausdruck mithilfe des unter Erweiterten Richtlinienausdruck konfigurierenbeschriebenen Prozess. Eine Meldung in der Statusleiste zeigt an, dass der Richtlinienausdruck erfolgreich konfiguriert wurde.

Konfigurieren erweiterter Richtlinienausdrücke außerhalb des Kontexts einer Richtlinie

October 5, 2021

Eine Reihe von Funktionen, einschließlich der folgenden, kann einen erweiterten Richtlinienausdruck erfordern, der nicht Teil einer Richtlinie ist:

- Integrierte Caching-Auswahlen:

  In der Definition des Selektors definieren Sie mehrere nicht-zusammengesetzte Ausdrücke (Selectlets). Jedes Selectlet befindet sich in einer impliziten logischen UND-Beziehung zu den anderen.

- Lastenausgleich:

  Sie konfigurieren einen Ausdruck für die TOKEN-Methode des Lastenausgleichs für einen virtuellen Lastausgleichsserver.

- Aktionen umschreiben:

  Ausdrücke definieren den Speicherort der Umschreibaktion und den Typ des durchzuführenden Umschreibens, abhängig vom Typ der Umschreibaktion, die Sie konfigurieren. Beispielsweise verwendet eine DELETE -Aktion nur einen Zielausdruck. Eine REPLACE -Aktion verwendet einen Zielausdruck und einen Ausdruck, um den Ersetzungstext zu konfigurieren.

- Preisbasierte Richtlinien:

  Sie verwenden erweiterte Richtlinienausdrücke, um Limit-Selektoren zu konfigurieren. Sie können diese Selektoren verwenden, wenn Sie Richtlinien konfigurieren, um die Rate des Datenverkehrs auf verschiedene Server zu drosseln. In der Definition des Selektors definieren Sie bis zu fünf nicht-zusammengesetzte Ausdrücke (Selectlets). Jedes Selectlet befindet sich in einem impliziten logischen UND mit den anderen.

Konfigurieren eines erweiterten Richtlinienausdrucks außerhalb einer Richtlinie mit der CLI (Beispiel für die Cache-Auswahl)

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen erweiterten Richtlinienausdruck außerhalb einer Richtlinie zu konfigurieren und die Konfiguration zu überprüfen:

```
1 -  add cache selector <selectorName> <rule>
2 -  show cache selector <selectorName>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add cache selector mainpageSelector "http.req.cookie.value("ABC_def")
    "
2     "http.req.url.query.value("_ghi")"selector "mainpageSelector" added
```



```
Done
> show cache selector mainpageSelector
            Name: mainpageSelector
            Expressions:
                    1) http.req.cookie.value(”ABC_def”)
                    2) http.req.url.query.value(”_ghi”)
Done
<!--NeedCopy-->
```

Es folgt ein äquivalenter Befehl, der das lesbarere q-Trennzeichen verwendet, wie unter Konfigurieren von erweiterten Richtlinienausdrücken in einer Richtlinie beschrieben:

```
> add cache selector mainpageSelector2 q~http.req.cookie.value(”ABC_def
   ”)~
    q~http.req.url.query.value(”_ghi”)~selector ”mainpageSelector2”
       added
Done
> show cache selector mainpageSelector2
            Name: mainpageSelector2
            Expressions:
                    1) http.req.cookie.value(”ABC_def”)
                    2) http.req.url.query.value(”_ghi”)
Done
<!--NeedCopy-->
```

Erweiterte Richtlinienausdrücke: Auswerten von Text

October 5, 2021

Sie können eine Richtlinie mit einem erweiterten Richtlinienausdruck konfigurieren, der Text in einer Anforderung oder Antwort auswertet. Erweiterte Richtlinien-Textausdrücke können von einfachen Ausdrücken reichen, die Zeichenfolgenabgleich in HTTP-Headern durchführen, bis hin zu komplexen Ausdrücken, die Text kodieren und dekodieren. Sie können Textausdrücke so konfigurieren, dass zwischen Groß- und Kleinschreibung unterschieden wird und Leerzeichen verwendet oder ignoriert werden. Sie können komplexe Textausdrücke auch konfigurieren, indem Sie Textausdrücke mit booleschen Operatoren kombinieren

Sie können Ausdruckspräfixe und Operatoren für die Auswertung von HTTP-Anforderungen, HTTP-Antworten sowie VPN- und Clientless-VPN-Daten verwenden. Textausdruck-Präfixe sind jedoch nicht auf die Auswertung dieser Elemente Ihres Datenverkehrs beschränkt.

Informationen zu Textausdrücken

October 5, 2021

Sie können verschiedene Ausdrücke für die Arbeit mit Text konfigurieren, der durch die Citrix ADC Appliance fließt. Im Folgenden finden Sie einige Beispiele, wie Sie Text mithilfe eines Standard-Syntaxausdrucks analysieren können:

- Bestimmen Sie, dass ein bestimmter HTTP-Header vorhanden ist.

  Beispielsweise können Sie HTTP-Anforderungen identifizieren, die einen bestimmten Accept-Language-Header enthalten, um die Anforderung an einen bestimmten Server weiterzuleiten.

- Bestimmen Sie, dass eine bestimmte HTTP-URL eine bestimmte Zeichenfolge enthält.

  Beispielsweise können Sie Anforderungen für bestimmte URLs blockieren. Beachten Sie, dass die Zeichenfolge am Anfang, in der Mitte oder am Ende einer anderen Zeichenfolge auftreten kann.

- Identifizieren Sie eine POST-Anforderung, die an eine bestimmte Anwendung gerichtet ist.

  Beispielsweise können Sie alle POST-Anforderungen identifizieren, die an eine Datenbankanwendung weitergeleitet werden, um zwischengespeicherte Anwendungsdaten zu aktualisieren.

Beachten Sie, dass es spezielle Tools zum Anzeigen des Datenstroms für HTTP-Anforderungen und -Antworten gibt. Sie können die Werkzeuge verwenden, um den Datenstrom anzuzeigen.

Informationen zu Textvorgängen

Ein textbasierter Ausdruck besteht aus mindestens einem Präfix zum Identifizieren eines Datenelements und normalerweise (wenn auch nicht immer) einer Operation für dieses Präfix. Textbasierte Vorgänge können auf jeden Teil einer Anforderung oder einer Antwort angewendet werden. Grundlegende Operationen für Text umfassen verschiedene Arten von Zeichenfolgenübereinstimmungen.

Der folgende Ausdruck vergleicht beispielsweise einen Headerwert mit einer Zeichenfolge:

```
http.req.header("myHeader").contains("some-text")
```

Die folgenden Ausdrücke sind Beispiele für die Übereinstimmung mit einem Dateityp in einer Anforderung:

```
http.req.url.suffix.contains("jpeg")
```

```
http.req.url.suffix.eq("jpeg")
```

In den obigen Beispielen erlaubt der contains Operator eine partielle Übereinstimmung und der eq Operator sucht nach einer exakten Übereinstimmung.

Andere Operationen stehen zur Verfügung, um die Zeichenfolge zu formatieren, bevor sie ausgewertet wird. Sie können beispielsweise Textoperationen verwenden, um Anführungszeichen und Leerzeichen zu entfernen, die Zeichenfolge in Kleinbuchstaben zu konvertieren oder Zeichenfolgen zu verketten.

> **Hinweis**:
>
> Komplexe Operationen sind verfügbar, um Abgleich basierend auf Mustern durchzuführen oder einen Typ von Textformat in einen anderen Typ zu konvertieren.

Weitere Informationen finden Sie in den folgenden Themen:

- Mustersätze und Datensätze.
- Reguläre Ausdrücke.
- Typecasting von Daten.

Compounding und Rangfolge in Textausdrücken

Sie können verschiedene Operatoren anwenden, um Textpräfixe oder Ausdrücke zu kombinieren. Der folgende Ausdruck verkettet beispielsweise die zurückgegebenen Werte jedes Präfixes:

```
http.req.hostname + http.req.url
```

Es folgt ein Beispiel für einen zusammengesetzten Textausdruck, der eine logische AND verwendet. Beide Komponenten dieses Ausdrucks müssen TRUE sein, damit eine Anforderung mit dem Ausdruck übereinstimmt:

```
http.req.method.eq(post)&& http.req.body(1024).startswith(”destination=”)
```

> **Hinweis:**
>
> Weitere Informationen zu Operatoren für die Compoundierung finden Sie unter Zusammengesetzte erweiterte Ausdrücke.

Kategorien von Textausdrücken

Die primären Kategorien von Textausdrücken, die Sie konfigurieren können, sind:

- Informationen in HTTP-Headern, HTTP-URLs und dem POST-Text in HTTP-Anforderungen.

  Weitere Informationen finden Sie unter Ausdruckspräfixe für Text in HTTP-Anfragen und -Antworten.

- Informationen zu einem VPN oder einem clientlosen VPN.

  Weitere Informationen finden Sie unter Ausdruckspräfixe für VPNs und clientlose VPNs.

- TCP-Nutzlastinformationen.

Weitere Informationen zu TCP-Nutzlastausdrücken finden Sie unter Erweiterte Richtlinienausdrücke: Analysieren von HTTP-, TCP- und UDP-Daten.

- Text in einem SSL-Zertifikat (Secure Sockets Layer).

  Informationen zu Textausdrücken für SSL- und SSL-Zertifikatsdaten finden Sie unter Erweiterte Richtlinienausdrücke: Analysieren von SSL-Zertifikaten und Ausdrücken für SSL-Zertifikatdaten.

> **Hinweis:**
>
> Das Analysieren eines Dokumentkörpers, z. B. des Hauptteils einer POST-Anforderung, kann sich auf die Leistung auswirken. Sie können die Auswirkungen auf die Leistung von Richtlinien testen, die einen Dokumentkörper auswerten.

Richtlinien für Textausdrücke

Aus Performance-Sicht ist es in der Regel am besten, protokollbasierte Funktionen in einem Ausdruck zu verwenden. Der folgende Ausdruck verwendet beispielsweise eine protokollunterstützende Funktion:

```
HTTP.REQ.URL.QUERY
```

Der vorherige Ausdruck ist besser als der folgende äquivalente Ausdruck, der auf der Zeichenfolgenanalyse basiert:

```
HTTP.REQ.URL.AFTER_STR("?")
```

Im ersten Fall betrachtet der Ausdruck speziell die URL-Abfrage. Im zweiten Fall scannt der Ausdruck die Daten auf das erste Vorkommen eines Fragezeichens.

Es gibt auch einen Leistungsvorteil von strukturiertem Analysieren von Text, wie im folgenden Ausdruck:

```
HTTP.REQ.HEADER("Example").TYPECAST_LIST_T(',').GET(1)
```

(Weitere Informationen zum Typecasting finden Sie unter Typecasting von Daten. Der Typecast-Ausdruck, der kommagetrennte Daten sammelt und sie in eine Liste strukturiert, würde normalerweise besser funktionieren als das folgende unstrukturierte Äquivalent:

```
HTTP.REQ.HEADER("Example").AFTER_STR(",").BEFORE_STR(",")
```

Schließlich haben unstrukturierte Textausdrücke in der Regel eine bessere Leistung als reguläre Ausdrücke. Der folgende Text ist beispielsweise ein unstrukturierter Textausdruck:

```
HTTP.REQ.HEADER("Example").AFTER_STR("more")
```

Der vorherige Ausdruck würde im Allgemeinen eine bessere Leistung bieten als das folgende Äquivalent, bei dem ein regulärer Ausdruck verwendet wird:


```
HTTP.REQ.HEADER("Example").AFTER_REGEX(re/more/)
```

Weitere Informationen zu regulären Ausdrücken finden Sie unter Reguläre Ausdrücke.

Ausdruckspräfixe für Text in HTTP-Anfragen und Antworten

June 21, 2022

Eine HTTP-Anforderung oder -Antwort enthält typischerweise Text, z. B. in Form von Headern, Header-Werten, URLs und POST-Haupttext. Sie können Ausdrücke so konfigurieren, dass sie mit einem oder mehreren dieser textbasierten Elemente in einer HTTP-Anforderung oder -Antwort arbeiten.

Weitere Informationen zu Parametern finden Sie unter Referenz zum erweiterten Richtlinienausdruck von Citrix ADC.

In den folgenden Themen finden Sie weitere Informationen zur Konfiguration mit erweitertem Ausdruck.

- Zusammengesetzte erweiterte Richtlinienausdrücke
- Erweiterte Richtlinienausdrücke: IP- und MAC-Adressen, Durchsatz, VLAN-IDs
- Erweiterte Richtlinienausdrücke: SSL parsen
- Erweiterte Richtlinienausdrücke: Arbeiten mit Datum, Uhrzeit und Zahlen
- Grundelemente eines erweiterten Richtlinienausdrucks
- Erweiterte Richtlinienausdrücke: Text auswerten
- Erweiterte Richtlinienausdrücke: Parsen von HTTP-, TCP- und UDP-Daten
- Zusammenfassende Beispiele für Standard-Syntaxausdrücke und Richtlinien

Ausdruckspräfixe für VPNs und clientlose VPNs

October 5, 2021

Das erweiterte Richtlinienmodul enthält Präfixe, die spezifisch für das Parsen von VPN- oder clientlosen VPN-Daten sind. Diese Daten umfassen Folgendes:

- Hostnamen, Domänen und URLs im VPN-Datenverkehr.
- Protokolle im VPN-Datenverkehr.
- Abfragen im VPN-Datenverkehr.

Diese Textelemente sind oft URLs und Komponenten von URLs. Zusätzlich zum Anwenden der textbasierten Vorgänge auf diese Elemente können Sie diese Elemente mithilfe von Operationen analysieren, die für das Analysieren von URLs spezifisch sind. Weitere Informationen finden Sie unter Ausdrücke zum Extrahieren von URL-Segmenten

Informationen zu VPN-Ausdruckspräfixen finden Sie unter VPN-Ausdruckstabelle.

Grundlegende Operationen auf Text

October 5, 2021

Zu den grundlegenden Operationen für Text gehören Operationen für den Zeichenfolgenabgleich, die Berechnung der Länge einer Zeichenfolge und die Kontrolle der Groß-/Kleinschreibung. Sie können Leerzeichen in eine Zeichenfolge einfügen, die als Argument an einen Ausdruck übergeben wird, aber die Zeichenfolge darf 255 Zeichen nicht überschreiten.

Zeichenfolgenvergleichsfunktionen

Die folgende Tabelle listet grundlegende Zeichenfolgenabgleichsoperationen auf, bei denen die Funktionen einen booleschen Wert TRUE oder FALSE zurückgeben.

Funktion	Beschreibung
`<text>.CONTAINS(<string>)`	Gibt einen booleschen TRUE Wert zurück, wenn das Ziel `<string>` enthält. Beispiel:`http.req.url.contains(".jpeg")`
`<text>.EQ(<string>)`	Gibt einen booleschen TRUE Wert zurück, wenn das Ziel eine genaue Übereinstimmung mit `<string>` ist. Der folgende Ausdruck gibt beispielsweise einen booleschen TRUE für eine URL mit dem Hostnamen “myhostabc” zurück:`http.req.url.hostname.eq("myhostabc")`
`<text>.STARTSWITH(<string>)`	Gibt einen booleschen TRUE Wert zurück, wenn das Ziel mit beginnt`<string>`. Der folgende Ausdruck gibt beispielsweise einen booleschen TRUE für eine URL mit dem Hostnamen “myhostabc” zurück:`http.req.url.hostname.startswith("myhost")`

Funktion	Beschreibung
`<text>.ENDSWITH(<string>)`	Gibt einen booleschen TRUE Wert zurück, wenn das Ziel mit endet <string>. Der folgende Ausdruck gibt beispielsweise einen booleschen TRUE für eine URL mit dem Hostnamen “myhostabc” zurück:`http.req.url.hostname.endswith(”abc”)`
`<text>.NE(<string>)`	Gibt einen booleschen TRUE-Wert zurück, wenn das Präfix nicht dem String-Argument entspricht. Wenn das Präfix einen Nicht-String-Wert zurückgibt, wird das Funktionsargument mit der Zeichenfolgendarstellung des vom Präfix zurückgegebenen Wertes verglichen. Sie können die Funktionen mit`SET_TEXT_MODE(IGNORECASE)or SET_TEXT_MODE(NOIGNORECASE)`, und mit ASCII- und UTF-8-Zeichensätzen verwenden.
`<text>.GT(<string>)`	Gibt einen booleschen TRUE-Wert zurück, wenn das Präfix alphabetisch größer als das Zeichenfolgenargument ist. Wenn das Präfix einen Nicht-String-Wert zurückgibt, wird das Funktionsargument mit der Zeichenfolgendarstellung des vom Präfix zurückgegebenen Wertes verglichen. Sie können die Funktionen mit `SET_TEXT_MODE(IGNORECASE)` oder `SET_TEXT_MODE(NOIGNORECASE)`, und mit ASCII- und UTF-8-Zeichensätzen verwenden.

Funktion	Beschreibung
`<text>.GE(<string>)`	Gibt einen booleschen TRUE-Wert zurück, wenn das Präfix alphabetisch größer oder gleich dem String-Argument ist. Wenn das Präfix einen Nicht-String-Wert zurückgibt, wird das Funktionsargument mit der Zeichenfolgendarstellung des vom Präfix zurückgegebenen Wertes verglichen. Sie können die Funktionen mit `SET_TEXT_MODE(IGNORECASE)` oder `SET_TEXT_MODE(NOIGNORECASE)`, und mit ASCII- und UTF-8-Zeichensätzen verwenden.
`<text>.LT(<string>)`	Gibt einen booleschen TRUE-Wert zurück, wenn das Präfix alphabetisch kleiner als das Zeichenfolgenargument ist. Wenn das Präfix einen Nicht-String-Wert zurückgibt, wird das Funktionsargument mit der Zeichenfolgendarstellung des vom Präfix zurückgegebenen Wertes verglichen. Sie können die Funktionen mit `SET_TEXT_MODE(IGNORECASE)` oder `SET_TEXT_MODE(NOIGNORECASE)`, und mit ASCII- und UTF-8-Zeichensätzen verwenden.
`<text>.LE(<string>)`	Gibt einen booleschen TRUE-Wert zurück, wenn das Präfix alphabetisch kleiner oder gleich dem String-Argument ist. Wenn das Präfix einen Nicht-String-Wert zurückgibt, wird das Funktionsargument mit der Zeichenfolgendarstellung des vom Präfix zurückgegebenen Wertes verglichen. Sie können die Funktionen mit `SET_TEXT_MODE(IGNORECASE)` oder `SET_TEXT_MODE(NOIGNORECASE)`, und mit ASCII- und UTF-8-Zeichensätzen verwenden.

Berechnen Sie die Länge einer Zeichenfolge

Der`<text>.LENGTH` Vorgang gibt einen numerischen Wert zurück, der der Anzahl der Zeichen (nicht Bytes) in einer Zeichenfolge entspricht:

```
<text>.LENGTH
```

Beispielsweise können Sie Anforderungs-URLs identifizieren, die eine bestimmte Länge überschreiten. Es folgt ein Ausdruck, der dieses Beispiel implementiert:

```
HTTP.REQ.URL.LENGTH < 500
```

Nachdem Sie die Zeichen oder Elemente in einer Zeichenfolge gezählt haben, können Sie numerische Operationen darauf anwenden. Weitere Informationen finden Sie unter Standardsyntaxausdrücke: Arbeiten mit Datumsangaben, Zeiten und Zahlen.

Betrachten, ignorieren und Ändern von Groß- und Kleinschreibung

Die folgenden Funktionen arbeiten für die Groß- oder Kleinschreibung der Zeichen in der Zeichenfolge.

Funktion	Beschreibung	
`<text>.SET_TEXT_MODE` (IGNORECASE	NOIGNORECASE)	This function turns case sensitivity on or off for all text operations.
`<text>.TO_LOWER`	Converts the target to lowercase for a text block of up to 2 kilobyte (KB). Gibt UNDEF zurück, wenn das Ziel 2 KB überschreitet. For example, the string “ABCd:” is converted to “abcd:”.	
`<text>.TO_UPPER`	Converts the target to uppercase. Gibt UNDEF zurück, wenn das Ziel 2 KB überschreitet. For example, the string “abcD:” is converted to “ABCD:”.	

Strippen bestimmter Zeichen aus einer Zeichenfolge

Sie können die STRIP_CHARS (<string>) -Funktion verwenden, um bestimmte Zeichen aus dem Text zu entfernen, der von einem Standard-Syntaxausdruckpräfix (der Eingabezeichenfolge) zurückgegeben wird. Alle Instanzen der Zeichen, die Sie im Argument angeben, werden aus der Eingabezeichenfolge entfernt. Sie können jede Textmethode für die resultierende Zeichenfolge verwenden, einschließlich der Methoden, die zum Abgleich der Zeichenfolge mit einem Mustersatz verwendet werden.

Im Ausdruck CLIENT.UDP.DNS.DOMAIN.STRIP_CHARS (.-_) entfernt die Funktion STRIP_CHARS (<string>) alle Punkte (.), Bindestriche (-) und Unterstriche (_) vom Domänennamen, der vom Präfix CLIENT.UDP.DNS.DOMAIN zurückgegeben wird. Wenn der zurückgegebene Domänenname a.dom_ai_n-name ist, gibt die Funktion den String adomainname zurück.

Im folgenden Beispiel wird die resultierende Zeichenfolge mit einem Mustersatz namens listofdomains verglichen:

```
CLIENT.UDP.DNS.DOMAIN.STRIP_CHARS(".-_").CONTAINS_ANY("listofdomains")
```

Hinweis: Sie können keine Neuschreibung für die Zeichenfolge durchführen, die von der STRIP_CHARS(<string>) Funktion zurückgegeben wird.

Die folgenden Funktionen entfernen übereinstimmende Zeichen vom Anfang und Ende einer gegebenen Zeichenfolgeneingabe.

Funktion	Beschreibung
<text>.STRIP_START_CHARS(s)	Strips übereinstimmende Zeichen vom Anfang der Eingabezeichenfolge, bis das erste nicht übereinstimmende Zeichen gefunden wird, und gibt den Rest der Zeichenfolge zurück. Sie müssen die Zeichen angeben, die Sie als einzelne Zeichenfolge in Anführungszeichen entfernen möchten. Wenn der Name eines Headers beispielsweise testLang ist und:*/en_us:sein Wert ist, wird HTTP.RES.HEADER ("testLang") .STRIP_START_CHARS (":")* die angegebenen Zeichen vom Anfang des Wertes des Headers entfernt, bis das erste nicht übereinstimmende Zeichen e gefunden wird und zurücksen_us: als -Zeichenkette.

Funktion	Beschreibung
<text>.STRIP_END_CHARS (s)	Strips übereinstimmende Zeichen vom Ende der Eingabezeichenfolge bis zum ersten nicht übereinstimmenden Zeichen gefunden wird und gibt den Rest der Zeichenfolge zurück. Sie müssen die Zeichen angeben, die Sie als einzelne Zeichenfolge in Anführungszeichen entfernen möchten. Wenn der Name eines Headers beispielsweise testLang ist und:*/en_us:sein Wert ist, wird HTTP.RES.HEADER ("testLang") .STRIP_START_CHARS (":"*) die angegebenen Zeichen vom Ende des Wertes der Kopfzeile entfernt, bis das erste nicht übereinstimmende Zeichen s gefunden wird und zurückgibt: /_de_us als -Zeichenkette.

Anfügen einer Zeichenfolge an eine andere Zeichenfolge

Sie können die APPEND () -Funktion verwenden, um die Zeichenfolgendarstellung des Arguments an die Zeichenfolgendarstellung des von der vorherigen Funktion zurückgegebenen Werts anzuhängen. Die vorhergehende Funktion kann eine Funktion sein, die eine Zahl, einen unsigned long, double, einen Zeitwert, eine IPv4-Adresse oder eine IPv6-Adresse zurückgibt. Das Argument kann eine Textzeichenfolge, eine Zahl, ein unsigned long, double, ein Zeitwert, eine IPv4-Adresse oder eine IPv6-Adresse sein. Der resultierende Zeichenfolgenwert ist derselbe Zeichenfolgenwert, der mit dem Operator + erhalten wird.

Komplexe Operationen an Text

July 15, 2022

Zusätzlich zum einfachen Zeichenfolgenabgleich können Sie Ausdrücke konfigurieren, die die Zeichenfolgenlänge und den Textblock auf Muster statt auf bestimmte Zeichenfolgen untersuchen.

Beachten Sie bei jeder textbasierten Operation Folgendes:

- Für jede Operation, die ein Zeichenfolgenargument akzeptiert, darf die Zeichenfolge 255 Zeichen nicht überschreiten.

- Sie können Leerraum einschließen, wenn Sie eine Zeichenfolge in einen Ausdruck angeben.

Operationen an der Länge einer Zeichenfolge

Die folgenden Operationen extrahieren Zeichenfolgen nach einer Zeichenanzahl.

Zeichenzähler-Operation	Beschreibung
`<text>.TRUNCATE(<count>)`	Gibt eine Zeichenfolge zurück, nachdem das Ende des Ziels um die Anzahl der Zeichen in abgeschnitten wurde `<count>`. Wenn die gesamte Zeichenfolge kürzer als ist `<count>`, wird nichts zurückgegeben.
`<text>.TRUNCATE(<character>, <count>)`	Gibt eine Zeichenfolge zurück, nachdem der Text nach `<character>` um die in `<count>` angegebene Anzahl von Zeichen abgeschnitten wurde.
`<text>.PREFIX(<character>, <count>)`	Wählt das längste Präfix im Ziel aus, das höchstens `<count>` Vorkommen von `<character>` hat.
`<text>.SUFFIX(<character>, <count>)`	Wählt das längste Suffix im Ziel aus, das höchstens `<count>` Vorkommen von `<character>` hat. Betrachten Sie beispielsweise den folgenden Antworttext: `peninsula`. Der folgende Ausdruck gibt den Wert zurück `sula: http.res.body(100).suffix('n',0)`. Der folgende Ausdruck wird zurückgegeben `insula: http.res.body(100).suffix('n',1)`. Der folgende Ausdruck gibt den Wert zurück `peninsula: http.res.body(100).suffix('n',2)`. Der folgende Ausdruck gibt den Wert zurück `peninsula: http.res.body(100).suffix('n',3)`.

Zeichenzähler-Operation	Beschreibung
<text>.SUBSTR(<starting_offset>, <length>)	Wählen Sie eine Zeichenfolge mit der <length>Anzahl von Zeichen aus dem Zielobjekt aus. Beginne mit dem Extrahieren der Zeichenfolge nach dem <starting_offset>. Wenn die Anzahl der Zeichen nach dem Offset unter dem Wert des Arguments <length> liegt, wählen Sie alle verbleibenden Zeichen aus.
<text>.SKIP(<character>, <count>)	Wählen Sie eine Zeichenfolge aus dem Ziel aus, nachdem Sie das längste Präfix übersprungen haben, das höchstens <count> Vorkommen von <character> hat.

Operationen für einen Teil einer Zeichenfolge

In der Tabelle String-Operationen erfahren Sie, wie Sie eine Teilmenge einer größeren Zeichenfolge extrahieren, indem Sie eine der Operationen verwenden.

Operationen zum Vergleich der alphanumerischen Reihenfolge zweier Strings

Die COMPARE-Operation untersucht das erste nicht übereinstimmende Zeichen zweier verschiedener Zeichenfolgen. Diese Operation basiert auf der lexikografischen Reihenfolge, die bei der Bestellung von Begriffen in Wörterbüchern verwendet wird.

Diese Operation gibt die arithmetische Differenz zwischen den ASCII-Werten der ersten nicht übereinstimmenden Zeichen in den verglichenen Zeichenfolgen zurück. Die folgenden Unterschiede sind Beispiele:

- Der Unterschied zwischen “abc” und “und” ist -1 (basierend auf dem dritten paarweisen Zeichenvergleich).
- Der Unterschied zwischen “@” und “abc” beträgt -33.
- Der Unterschied zwischen “1” und “abc” beträgt -47.

Es folgt die Syntax für die COMPARE-Operation.

```
<text>.COMPARE(<string>)
```


Extrahieren einer Ganzzahl aus einer Zeichenfolge von Bytes, die Text darstellen

In der Integer-Extraktionstabelle erfahren Sie, wie Sie eine Bytezeichenfolge behandeln, die Text als eine Folge von Bytes darstellt, 8 Bit, 16 Bit oder 32 Bit aus der Sequenz extrahiert und dann die extrahierten Bits in eine Ganzzahl konvertiert.

Konvertieren von Text in einen Hash-Wert

Sie können eine Textzeichenfolge mithilfe der HASH-Funktion in einen Hash-Wert konvertieren. Diese Funktion gibt als Ergebnis der Operation eine positive 31-Bit-Ganzzahl zurück. Es folgt das Format des Ausdrucks:

```
<text>.HASH
```

Diese Funktion ignoriert Groß- und Leerräume. Beispielsweise würden die beiden Zeichenfolgen Ab c und bc nach der Operation denselben Hash-Wert erzeugen.

Kodieren und dekodieren Sie Text durch Anwenden des Base64-Codierungsalgorithmus

Die folgenden beiden Funktionen codieren und dekodieren eine Textzeichenfolge, indem sie den Base64-Codierungsalgorithmus anwenden.

Funktion	Beschreibung
text.B64ENCODE	Kodiert die Textzeichenfolge (durch Text gekennzeichnet) durch Anwendung des Base64-Codierungsalgorithmus.
text.B64DECODE	Dekodiert die Base64-codierte Zeichenfolge (durch Text gekennzeichnet) durch Anwendung des Base64-Decodierungsalgorithmus. Die Operation löst ein UNDEF aus, wenn Text nicht im B64-codierten Format vorliegt.

Verfeinern Sie die Suche in einer Rewrite-Aktion mithilfe der Funktion EXTEND

Die Funktion EXTEND wird in Rewrite-Aktionen verwendet, die Muster oder Mustersätze angeben und auf die Körper von HTTP-Paketen abzielen. Wenn eine Musterübereinstimmung gefunden wird, erweitert die Funktion EXTEND den Suchbereich um eine vordefinierte Anzahl von Byte auf beiden Seiten der übereinstimmenden Zeichenfolge. Ein regulärer Ausdruck kann dann verwendet werden, um Übereinstimmungen in dieser erweiterten Region neu zu schreiben. Rewrite-Aktionen, die mit

der Funktion EXTEND konfiguriert sind, führen Rewrites schneller durch als Rewrite-Aktionen, bei denen ganze HTTP-Bodies nur mit regulären Ausdrücken ausgewertet werden.

Das Format der EXTEND-Funktion ist EXTEND (m, n), wobei m und n die Anzahl der Byte sind, um die der Umfang der Suche vor bzw. nach dem übereinstimmenden Muster erweitert wird. Wenn eine Übereinstimmung gefunden wird, umfasst der neue Suchbereich m Byte, die unmittelbar vor der übereinstimmenden Zeichenfolge stehen, die Zeichenfolge selbst und die n Byte, die der Zeichenfolge folgen. Ein regulärer Ausdruck kann dann verwendet werden, um einen Teil dieser neuen Zeichenfolge neu zu schreiben.

Die Funktion EXTEND kann nur verwendet werden, wenn die Rewrite-Aktion , in der sie verwendet wird, die folgenden Anforderungen erfüllt:

- Die Suche erfolgt mithilfe von Mustern oder Mustersätzen (keine regulären Ausdrücke)
- Die Rewriteaktion wertet nur die Körper von HTTP-Paketen aus.

Außerdem kann die Funktion EXTEND nur mit den folgenden Arten von Rewrite-Aktionen verwendet werden:

- replace_all
- insert_after_all
- delete_all
- insert_before_all

Beispielsweise möchten Sie möglicherweise alle Instanzen von “” undhttp://exampleurl.com/“http://exampleurl.au/” in den ersten 1000 Byte des Körpers löschen. Zu diesem Zweck können Sie eine Rewriteaktion konfigurieren, um nach allen Instanzen der Zeichenfolge exampleurl zu suchen, den Suchbereich auf beiden Seiten der Zeichenfolge zu erweitern, wenn eine Übereinstimmung gefunden wird, und dann einen regulären Ausdruck verwenden, um das Rewrite in der erweiterten Region durchzuführen. Das folgende Beispiel erweitert den Umfang der Suche um 20 Byte nach links und 50 Byte rechts von der übereinstimmenden Zeichenfolge:

```
add rewrite action delurl_example delete_all 'HTTP.REQ.BODY(1000)'-pattern
exampleurl -refineSearch 'extend(20,50).regex_select(re##http://exampleurl
.(com|au)##)'
```

Konvertieren von Text in Hexadezimalformat

Die folgende Funktion wandelt Text in das Hexadezimalformat um und extrahiert die resultierende Zeichenfolge:

```
<text>.BLOB_TO_HEX(<string>)
```

Zum Beispiel wandelt diese Funktion die Bytezeichenfolge “abc” in “61:62:63” um.

Verschlüsseln und Entschlüsseln von Text

In Standard-Syntaxausdrücken können Sie die Funktionen ENCRYPT und DECRYPT verwenden, um Text zu ver- und entschlüsseln. Daten, die von der ENCRYPT-Funktion auf einer bestimmten Citrix ADC-Appliance oder einem Hochverfügbarkeitspaar (HA) verschlüsselt wurden, sind für die Entschlüsselung durch die DECRYPT-Funktion auf derselben Citrix ADC-Appliance oder demselben HA-Paar vorgesehen. Die Appliance unterstützt die Verschlüsselungsmethoden RC4, DES3, AES128, AES192 und AES256. Der für die Verschlüsselung erforderliche Schlüsselwert ist nicht vom Benutzer spezifizierbar. Wenn eine Verschlüsselungsmethode festgelegt ist, generiert die Appliance automatisch einen zufälligen Schlüsselwert, der für die angegebene Methode geeignet ist. Die Standardmethode ist die AES256-Verschlüsselung, die die sicherste und von Citrix empfohlene Verschlüsselungsmethode ist.

Sie müssen die Verschlüsselung nicht konfigurieren, es sei denn, Sie möchten die Verschlüsselungsmethode ändern oder die Appliance soll einen neuen Schlüsselwert für die aktuelle Verschlüsselungsmethode generieren.

Hinweis: Sie können auch XML-Nutzlasten verschlüsseln und entschlüsseln. Informationen zu den Funktionen zum Verschlüsseln und Entschlüsseln von XML-Nutzlasten finden Sie unter Verschlüsseln und Entschlüsseln von XML-Nutzlasten.

Verschlüsselung konfigurieren

Während des Starts führt die Appliance den Befehl set ns EncryptionParams mit standardmäßig der AES256-Verschlüsselungsmethode aus und verwendet einen zufällig generierten Schlüsselwert, der für die AES256-Verschlüsselung geeignet ist. Die Appliance verschlüsselt auch den Schlüsselwert und speichert den Befehl mit dem verschlüsselten Schlüsselwert in der Citrix ADC-Konfigurationsdatei. Daher ist die Verschlüsselungsmethode AES256 standardmäßig für die Funktionen ENCRYPT und DECRYPT aktiviert. Der Schlüsselwert, der in der Konfigurationsdatei gespeichert wird, bleibt bei Neustarts bestehen, obwohl die Appliance den Befehl bei jedem Neustart ausführt.

Sie können den Befehl set ns EncryptionParams manuell ausführen oder das Konfigurationsdienstprogramm verwenden, wenn Sie die Verschlüsselungsmethode ändern möchten oder wenn die Appliance einen neuen Schlüsselwert für die aktuelle Verschlüsselungsmethode generieren soll. Um die CLI zum Ändern der Verschlüsselungsmethode zu verwenden, legen Sie nur den Methodenparameter fest, wie in “**Beispiel 1: Ändern der Verschlüsselungsmethode**gezeigt. “ Wenn Sie möchten, dass die Appliance einen neuen Schlüsselwert für die aktuelle Verschlüsselungsmethode generiert, setzen Sie den Methodenparameter auf die aktuelle Verschlüsselungsmethode und den KeyValue-Parameter auf eine leere Zeichenfolge (“”), wie in “**Beispiel 2: Generieren eines neuen Schlüsselwerts für die aktuelle Verschlüsselungsmethode**gezeigt. “ Nachdem Sie einen neuen Schlüsselwert generiert haben, müssen Sie die Konfiguration speichern. Wenn Sie die Konfiguration nicht speichern, verwendet die Appliance den neu generierten Schlüsselwert nur bis zum nächsten Neustart, woraufhin sie

auf den Schlüsselwert in der gespeicherten Konfiguration zurückkehrt.

Konfigurieren Sie die Verschlüsselung über die GUI

1. Navigieren Sie zu **System** > **Einstellungen**.
2. Klicken Sie im Bereich **Einstellungen** auf **Verschlüsselungsparameter ändern** .
3. Führen **Sie im Dialogfeld Verschlüsselungsparameter ändern** einen der folgenden Schritte aus:
   - Um die Verschlüsselungsmethode zu ändern, wählen Sie in der Liste Methode die gewünschte Verschlüsselungsmethode aus.
   - Um einen neuen Schlüsselwert für die aktuelle Verschlüsselungsmethode zu generieren, klicken Sie auf Neuen Schlüssel für die ausgewählte Methode generieren.
4. Klicken Sie auf **OK**.

Verwenden Sie die Funktionen ENCRYPT und DECRYPT

Sie können die Funktionen ENCRYPT und DECRYPT mit jedem Ausdruck-Präfix verwenden, das Text zurückgibt. Beispielsweise können Sie die Funktionen ENCRYPT und DECRYPT in Rewriterichtlinien für die Cookie-Verschlüsselung verwenden. Im folgenden Beispiel verschlüsseln die Rewrite-Aktionen ein Cookie namens MyCookie, das von einem Back-End-Dienst gesetzt wird, und entschlüsseln dasselbe Cookie, wenn es von einem Client zurückgegeben wird:

```
1 add rewrite action my-cookie-encrypt-action replace "HTTP.RES.
    SET_COOKIE.COOKIE("MyCookie").VALUE(0)" "HTTP.RES.SET_COOKIE.COOKIE(
    "MyCookie").VALUE(0).ENCRYPT" -bypassSafetyCheck YES
2
3 add rewrite action my-cookie-decrypt-action replace "HTTP.REQ.COOKIE.
    VALUE("MyCookie")" "HTTP.REQ.COOKIE.VALUE("MyCookie").DECRYPT" -
    bypassSafetyCheck YES
4 <!--NeedCopy-->
```

Nachdem Sie Richtlinien für die Verschlüsselung und Entschlüsselung konfiguriert haben, speichern Sie die Konfiguration, um die Richtlinien in Kraft zu setzen.

Konfiguration des Verschlüsselungsschlüssels für die Verschlüsselung

In Standard-Syntaxausdrücken können Sie die Funktionen ENCRYPT und DECRYPT zum Ver- und Entschlüsseln von Text in einer Anforderung oder Antwort verwenden. Die von der ENCRYPT-Funktion auf einer Appliance verschlüsselten Daten (Standalone, Hochverfügbarkeit oder Cluster) sollen von derselben Appliance durch die DECRYPT-Funktion entschlüsselt werden. Die Appliance unterstützt

die Verschlüsselungsmethoden RC4, DES, Triple-DES, AES92 und AES256, und jede dieser Methoden verwendet einen geheimen Schlüssel für die Verschlüsselung und Entschlüsselung von Daten. Sie können jede dieser Methoden verwenden, um Daten auf zwei Arten zu verschlüsseln und zu entschlüsseln - Selbstverschlüsselung und Verschlüsselung durch Dritte.

Die Selbstverschlüsselungsfunktion in einer Appliance (Standalone, Hochverfügbarkeit oder Cluster) verschlüsselt und entschlüsselt Daten durch Auswertung des Header-Werts. Ein Beispiel, um dies zu verstehen, ist die HTTP-Cookie-Verschlüsselung. Der Ausdruck wertet den Header aus, verschlüsselt den HTTP-Cookie-Wert im Set-Cookie-Header in der ausgehenden Antwort und entschlüsselt dann den Cookie-Wert, wenn er im Cookie-Header einer nachfolgenden eingehenden Anforderung des Clients zurückgegeben wird. Der Schlüsselwert ist nicht vom Benutzer konfigurierbar. Wenn stattdessen eine Verschlüsselungsmethode im Befehl set ns EncryptionParams konfiguriert ist, generiert die Appliance automatisch einen zufälligen Schlüsselwert für die konfigurierte Methode. Standardmäßig verwendet der Befehl die Verschlüsselungsmethode AES256, die die hochsichere Methode ist, und Citrix empfiehlt diese Methode.

Die Verschlüsselungsfunktion eines Drittanbieters verschlüsselt oder entschlüsselt Daten mit einer Drittanbieteranwendung. Beispielsweise kann ein Client Daten in einer Anforderung verschlüsseln und die Appliance entschlüsselt die Daten, bevor sie an den Back-End-Server gesendet werden oder umgekehrt. Um dies durchzuführen, müssen die Appliance und die Drittanbieteranwendung einen geheimen Schlüssel gemeinsam nutzen. Auf der Appliance können Sie den geheimen Schlüssel direkt mithilfe eines Verschlüsselungsschlüsselobjekts konfigurieren, und der Schlüsselwert wird automatisch von der Appliance für eine stärkere Verschlüsselung generiert. Derselbe Schlüssel wird manuell auf der Appliance eines Drittanbieters konfiguriert, sodass sowohl Appliance als auch Drittanbieteranwendungen denselben Schlüssel zum Verschlüsseln und Entschlüsseln von Daten verwenden können.

Hinweis: Mithilfe der Verschlüsselung von Drittanbietern können Sie auch XML-Nutzdaten verschlüsseln und entschlüsseln. Informationen zu den Funktionen zum Verschlüsseln und Entschlüsseln von XML-Nutzdaten finden Sie unter “Verschlüsseln und Entschlüsseln von XML-Nutzlasten.

Verschlüsselungsmethoden

Eine Verschlüsselungsmethode bietet zwei Funktionen: eine Verschlüsselungsfunktion, die eine Klartext-Bytesequenz in eine Chiffretext-Bytesequenz umwandelt, und eine Entschlüsselungsfunktion, die den Chiffretext zurück in den Klartext umwandelt. Verschlüsselungsmethoden verwenden Bytesequenzen, die als Schlüssel bezeichnet werden, um Verschlüsselung und Entschlüsselung durchzuführen. Verschlüsselungsmethoden, die denselben Schlüssel für die Verschlüsselung und Entschlüsselung verwenden, werden als symmetrisch bezeichnet. Verschlüsselungsmethoden, die unterschiedliche Schlüssel für die Verschlüsselung und Entschlüsselung verwenden, sind asymmetrisch. Die bemerkenswertesten Beispiele für asymmetrische Verschlüsselungen sind die Kryptographie mit öffentlichen Schlüsseln, bei der ein öffentlicher Schlüssel verwendet wird,

der jedem zur Verschlüsselung zur Verfügung steht, und einen privaten Schlüssel, der nur dem Entschlüsseler bekannt ist.

Eine gute Verschlüsselungsmethode macht es unmöglich, Chiffretext zu entschlüsseln (“knacken”), wenn Sie den Schlüssel nicht besitzen. “Unmachbar” bedeutet wirklich, dass das Knacken des Verschlüsselungstextes mehr Zeit und Rechenressourcen in Anspruch nehmen würde, als es wert ist. Wenn Computer leistungsfähiger und billiger werden, werden Verschlüsselungen, die früher nicht geknackt werden konnten, praktikabler. Im Laufe der Zeit werden auch Fehler in Verschlüsselungsmethoden (oder deren Implementierungen) festgestellt, die das Knacken erleichtern. Neuere Verschlüsselungsmethoden werden daher älteren vorgezogen. Im Allgemeinen bieten Schlüssel mit längerer Länge eine bessere Sicherheit als kürzere Schlüssel, auf Kosten längerer Verschlüsselungs- und Entschlüsselungszeiten.

Eine Verschlüsselungsmethode kann Stream-Chiffren oder Blockchiffren verwenden. RC4 ist die meist gesicherte Stream-Chiffrers und wird nur für Legacy-Anwendungen verwendet. Blockchiffren können Polsterung enthalten.

Stream-Chiffren

Eine Stream-Verschlüsselungsmethode arbeitet mit einzelnen Bytes. Auf Citrix ADC -Appliances ist nur eine Stream-Verschlüsselung verfügbar: RC4, das eine Schlüssellänge von 128 Bit (16 Byte) verwendet. Für einen bestimmten Schlüssel generiert RC4 eine pseudozufällige Bytefolge, rufen Sie einen Keystream auf, der mit dem Klartext X-ored ist, um den Chiffretext zu erzeugen. RC4 gilt nicht mehr als sicher und sollte nur verwendet werden, wenn dies von älteren Anwendungen erforderlich ist.

Blockchiffren

Eine Blockchiffrierungsmethode arbeitet mit einem festen Byte-Block. Eine Citrix ADC-Appliance bietet zwei Blockchiffren: Data Encryption Standard (DES) und den Advanced Encryption Standard (AES). DES verwendet eine Blockgröße von 8 Byte und (auf einer Citrix ADC-Appliance) zwei Optionen für die Schlüssellänge: 64 Bit (8 Byte), von denen 56 Bit Daten und 8 Bit Parität sind, und Triple-DES, eine Schlüssellänge von 192 Bit (24 Byte). AES hat eine Blockgröße von 16 Byte und (auf Citrix ADC) drei Möglichkeiten für die Schlüssellänge: 128 Bit (16 Byte), 192 Bit (24 Byte) und 256 Bit (32 Byte).

Padding

Wenn der Klartext für eine Blockchiffre keine ganzzahlige Anzahl von Blöcken ist, kann das Auffüllen mit mehr Bytes erforderlich sein. Angenommen, der Klartext lautet “xyzzy” (Hex 78797a7a79). Für einen 8-Byte-Triple-DES-Block müsste dieser Wert aufgefüllt werden, um 8 Byte zu erzeugen. Das Füllschema muss es der Entschlüsselungsfunktion ermöglichen, die Länge des ursprünglichen

Klartextes nach der Entschlüsselung zu bestimmen. Im Folgenden sind einige derzeit verwendete Füllschemata aufgeführt (n ist die Anzahl der hinzugefügten Byte):

- PKCS7: Addiert jeweils n Byte Wert. Zum Beispiel 78797a7a79030303. Dies ist das Füllschema, das von der Richtlinienfunktion OpenSSL und ENCRYPT () verwendet wird. Das PKCS5-Polsterschema ist dasselbe wie bei PKCS7.
- ANSI X.923: Addiert n-1 Nullbyte und ein letztes Byte des Wertes n. Zum Beispiel 78797a7a79000003.
- ISO 10126: Addiert n-1 zufällige Byte und ein letztes Byte des Wertes n. Zum Beispiel 78797a7a79xxxx03, wobei xx ein beliebiger Bytewert sein kann. Die Richtlinienfunktion DECRYPT () akzeptiert dieses Füllschema, das es ihr auch ermöglicht, die Schemata PKCS7 und ANSI X.923 zu akzeptieren.
- ISO/IEC 7816-4: Fügt ein 0x80 Byte und n-1 Nullbyte hinzu. Zum Beispiel 78797a7a79800000. Dies wird auch OneAndZeros-Polsterung genannt.
- Null: Fügt n Nullbyte hinzu. Beispiel: 78797a7a79000000. Dies kann nur mit Klartext verwendet werden, der keine NUL-Bytes enthält.

Wenn eine Füllung verwendet wird und der Klartext eine ganzzahlige Anzahl von Blöcken ist, wird normalerweise ein zusätzlicher Block hinzugefügt, damit die Entschlüsselungsfunktion die ursprüngliche Klartext-Länge eindeutig bestimmen kann. Für PCKS7 und 8-Byte-Block wäre dies 0808080808080808.

Betriebsmodi

Es gibt eine Reihe verschiedener Betriebsmodi für Blockchiffren, die angeben, wie mehrere Klartext-Blöcke verschlüsselt werden. Einige Modi verwenden einen Initialisierungsvektor (IV), einen Datenblock außer dem Klartext, der zum Starten des Verschlüsselungsprozesses verwendet wird. Es empfiehlt sich, für jede Verschlüsselung eine andere IV zu verwenden, damit derselbe Klartext einen anderen Chiffretext erzeugt. Die IV muss nicht geheim sein und wird daher dem Chiffretext vorangestellt. Zu den Modi gehören:

- Elektronisches Codebuch (EZB): Jeder Klartext-Block wird unabhängig verschlüsselt. Eine IV wird nicht verwendet. Das Auffüllen ist erforderlich, wenn der Klartext kein Vielfaches der Verschlüsselungsblockgröße ist. Derselbe Klartext und Schlüssel erzeugen immer denselben Chiffretext. Aus diesem Grund gilt die EZB als weniger sicher als andere Modi und sollte nur für Legacy-Anwendungen verwendet werden.
- Cipher Block Chaining (CBC): Jeder Klartextblock wird mit dem vorherigen Chiffretext-Block oder der IV für den ersten Block xored, bevor er verschlüsselt wird. Das Auffüllen ist erforderlich, wenn der Klartext kein Vielfaches der Verschlüsselungsblockgröße ist. Dies ist der Modus, der mit der Citrix ADC EncryptionParams-Methode verwendet wird.
- Verschlüsselungsfeedback (CFB): Der vorherige Chiffretextblock oder die IV für den ersten Block wird verschlüsselt und die Ausgabe wird mit dem aktuellen Klartext-Block XORed, um den aktuellen Chiffretext-Block zu erstellen. Die Rückkopplung kann 1 Bit, 8 Bit oder 128 Bit betragen.

Da der Klartext mit dem Chiffretext XORed ist, ist kein Auffüllen erforderlich.

- Ausgabe-Feedback (OFB): Ein Keystream wird generiert, indem die Chiffre nacheinander auf die IV angewendet wird und die Keystream-Blöcke mit dem Klartext XORing. Eine Polsterung ist nicht erforderlich.

Konfigurieren von Verschlüsselungsschlüsseln für die Verschlüsselung

Im Folgenden werden die Konfigurationsaufgaben aufgeführt, die bei der Konfiguration des Verschlüsselungsschlüssels ausgeführt

1. Hinzufügen eines Verschlüsselungsschlüssels. Konfiguriert einen Verschlüsselungsschlüssel für eine angegebene Verschlüsselungsmethode mit einem bestimmten Schlüsselwert.
2. Änderung eines Verschlüsselungsschlüssels. Sie können Parameter für einen konfigurierten Verschlüsselungsschlüssel bearbeiten.
3. Einen Verschlüsselungsschlüssel aufheben. Setzt Parameter für einen konfigurierten Verschlüsselungsschlüssel auf ihre Standardwerte. Ein EncryptionKey-Wert mit dem Namen muss existieren. Setzt das Auffüllen auf DEFAULT (bestimmt durch die Methode), Löscht eine vorhandene IV, wodurch ENCRYPT () eine zufällige IV generiert. Löscht einen vorhandenen Kommentar. Die Methode und der Schlüsselwert können nicht zurückgesetzt werden.
4. Einen Verschlüsselungsschlüssel entfernen. Löscht einen konfigurierten Verschlüsselungsschlüssel. Der Schlüssel kann keine Referenzen haben.
5. Zeigt einen Verschlüsselungsschlüssel an. Zeigt Parameter für den konfigurierten Verschlüsselungsschlüssel oder alle konfigurierten Schlüssel an. Wenn der Name weggelassen wird, wird der Schlüsselwert nicht angezeigt.

Fügen Sie über die CLI einen Verschlüsselungsschlüssel hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns encryptionKey <name> -method <method> [-keyValue <keyvalue>][-
padding (OFF | ON)] [-iv <hexstring>] -keyValue <keyvalue> [-comment <
string>]
```

Hierbei gilt:

```
1 <method> = ( NONE | RC4 | DES3 | AES128 | AES192 | AES256 | DES | DES-
     CBC | DES-CFB | DES-OFB | DES-ECB | DES3-CBC | DES3-CFB | DES3-OFB |
      DES3-ECB | AES128-CBC | AES128-CFB | AES128-OFB | AES128-ECB |
     AES192-CBC | AES192-CFB | AES192-OFB | AES192-ECB | AES256-CBC |
     AES256-CFB | AES256-OFB | AES256-ECB ) <hexstring> = hex-encoded
     byte sequence
2 <!--NeedCopy-->
```


Die obigen Verschlüsselungsmethoden spezifizieren den Betriebsmodus mit CBC als Standardbetriebsmodus. Daher entsprechen die Methoden DES, DES2, AES128, AES192 und AES256 den Methoden DES-CBC, DES3-CBC, AES128-CBC, AES192-CBC und AES256-CBC.

Ändern eines Verschlüsselungsschlüssels über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns encryptionKey <name> [-method <method>] [-keyValue <keyvalue>] [-padding ( OFF | ON )] [-iv <string>] [-comment <string>]
```

Einen Verschlüsselungsschlüssel über die CLI aufheben

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
unset ns encryptionKey <name> [-padding] [-iv] [-comment]
```

Entfernen Sie einen Verschlüsselungsschlüssel über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm ns encryptionKey <name>
```

Zeigen Sie einen Verschlüsselungsschlüssel über die CLI an

Geben Sie an der Eingabeaufforderung Folgendes ein:

Beispiel:

```
1  show ns encryptionKey [<name>]
2
3  add ns encryptionKey my_key -method aes256 -keyValue 26
       ea5537b7e0746089476e5658f9327c0b10c3b4778c673a5b38cee182874711  -iv
       c2bf0b2e15c15004d6b14bcdc7e5e365
4  set ns encryptionKey my_key -keyValue
       b8742b163abcf62d639837bbee3cef9fb5842d82d00dfe6548831d2bd1d93476
5  unset ns encryptionKey my_key -iv
6  rm ns encryptionKey my_key
7  show ns encryptionKey my_key
8  Name: my_key
9  Method: AES256
10 Padding: DEFAULT
11 Key Value: (not disclosed)
12 <!--NeedCopy-->
```


Fügen Sie über die GUI einen Verschlüsselungsschlüssel hinzu

Navigieren Sie zu **System** > **Verschlüsselungsschlüssel** und klicken Sie auf **Hinzufügen**, um einen Verschlüsselungsschlüssel zu erstellen.

Ändern Sie einen Verschlüsselungsschlüssel über die GUI

Navigieren Sie zu **System** > **Encryption Keys** und klicken Sie auf **Bearbeiten**, um Parameter für einen konfigurierten Verschlüsselungsschlüssel zu ändern.

Entfernen Sie einen Verschlüsselungsschlüssel über die GUI

Navigieren Sie zu **System** > **Verschlüsselungsschlüssel** und klicken Sie auf **Löschen**.

ENCRYPT- und DECRYPT-Funktionen für die Verschlüsselung von Drittanbietern

Es folgt die ENCRYPT-Funktion, die für die Verschlüsselung von Drittanbietern verwendet wird.

```
ENCRYPT (encryptionKey, out_encoding)
```

Hierbei gilt:

Eingabedaten für die Appliance sind der zu verschlüsselnde Text

EncryptionKey: Ein optionaler Zeichenfolgenparameter, der das konfigurierte Verschlüsselungsschlüsselobjekt zur Bereitstellung der Verschlüsselungsmethode, des geheimen Schlüsselwerts und anderer Verschlüsselungsparameter angibt. Wenn diese nicht angegeben wird, verwendet die Methode den automatisch generierten Schlüsselwert, der mit dem Befehl set ns EncryptionParams verknüpft ist.

out_encoding: Dieser Wert gibt an, wie die Ausgabe codiert wird. Wenn weggelassen, wird die BASE64-Codierung verwendet.

Eingabe:

```
1 BASE64: original PEM base64-encoding: 6 bits (0..63) encoded as one
     ASCII character:
2                 0..23 = 'A'..'Z', 24..51 = 'a'..'z', 52..61 = '0'..'9
                      ', 62 = '+', 63 = '/', '=' = pad byte.
3       BASE64URL:  URL and Filename safe base64-encoding: same as BASE64
            except 62 = '-', 63 = '_'
4       HEX_UPPER:  Hexadecimal with 0..9 = '0'..'9' and 10..15 = 'A'..'F
          '.
5       HEX_LOWER:  Hexadecimal with 0..9 = '0'..'9' and 10..15 = 'a'..'f
          '.
```



```
6       HEX_COLONS: Hexadecimal with 0..9 = '0'..'9' and 10..15 = 'A'..'F
            '; ':' between each hex byte. Matches BLOB_TO_HEX() output
            format
7       HEX:  For input, accepts HEX_UPPER, HEX_LOWER, and HEX_COLONS
            format. For output, produces HEX_LOWER format
8   <!--NeedCopy-->
```

Ausgabe: Die Ausgabe ist ein Text, der mit der angegebenen Methode und dem angegebenen Schlüssel verschlüsselt und mit einer bestimmten Ausgabecodierung codiert wurde. Es fügt eine generierte IV vor dem verschlüsselten Text für Blockmethoden und -modi ein, die eine IV erfordern, und entweder wird keine IV für den EncryptionKey angegeben oder der EncryptionKey wird weggelassen.

Es folgt die DECRYPT-Funktion, die für die Entschlüsselung durch Dritte verwendet wird.

```
DECRYPT(encryptionKey, in_encoding)
```

Hierbei gilt:

Eingabedaten sind ein verschlüsselter Text mit der angegebenen Methode und Schlüssel, der mit der angegebenen Eingabecodierung codiert ist. Es wird erwartet, dass dieser Text eine generierte IV enthält, bevor der verschlüsselte Text für Blockmethoden und -modi, die eine IV erfordern, und entweder wird keine IV für den EncryptionKey angegeben oder der EncryptionKey weggelassen wird.

encryptionKey — Ein optionaler Zeichenfolgenparameter, der das konfigurierte EncryptionKey-Objekt zur Bereitstellung der Verschlüsselungsmethode, des geheimen Schlüssels und anderer Verschlüsselungsparameter angibt. Wenn nicht angegeben, werden die Methode und der automatisch generierte Schlüssel verwendet, die mit der EncryptionParams-Einstellung verknüpft sind.

in_encoding — Ein optionaler Aufzählungsparameter, der angibt, wie die Eingabe voraussichtlich codiert wird. Die Werte entsprechen der out_encoding von ENCRYPT. Wenn es weggelassen wird, wird die BASE64-Codierung erwartet.

Die Ausgabedaten sind ein uncodierter entschlüsselter Text.

Varianten und optionale Parameter

Im Folgenden sind die Varianten dieser Funktionen mit den optionalen Parametern aufgeführt:

Variante	Beschreibung
ENCRYPT	Verwenden Sie den Befehl EncryptionParams und den Ausgabecodierungsparameter BASE64.
ENCRYPT(out_encoding)	Verwenden Sie EncryptionParams und den angegebenen Ausgabe-Kodierungsparameter.

Variante	Beschreibung
ENCRYPT(encryptionKey)	Verwenden Sie den angegebenen EncryptionKey- und BASE64-Ausgabecodierungsparameter.
ENCRYPT(encryptionKey, out_encoding)	Verwenden Sie den angegebenen EncryptionKey und den Ausgabecodierungsparameter.
DECRYPT	Verwenden Sie den Befehl EncryptionParams und den BASE64-Eingabecodierungsparameter
DECRYPT(out_encoding)	Verwenden Sie den EncryptionParams-Befehl und den angegebenen Eingabecodierungsparameter.
DECRYPT(encryptionKey)	Verwenden Sie den angegebenen EncryptionKey- und BASE64-Eingabecodierungsparameter
DECRYPT(encryptionKey, out_encoding)	Verwenden Sie den angegebenen EncryptionKey und den Eingabecodierungsparameter

Konfigurieren Sie HMAC-Schlüssel

Citrix ADC-Appliances unterstützen eine Funktion Hashed Message Authentication Code (HMAC), die eine Digest-Methode oder einen Hash von Eingabetext mithilfe eines geheimen Schlüssels berechnet, der zwischen einem Nachrichtenabsender und einem Nachrichtenempfänger gemeinsam genutzt wird. Die Digest-Methode (abgeleitet von einer RFC 2104-Technik) authentifiziert den Absender und stellt sicher, dass der Nachrichteninhalt nicht verändert wurde. Wenn ein Client beispielsweise eine Nachricht mit dem freigegebenen HMAC-Schlüssel an eine Citrix ADC-Appliance sendet, verwenden erweiterte Richtlinienausdrücke (PI) die HMAC-Funktion, um den Hash-basierten Code für den ausgewählten Text zu berechnen. Wenn der Empfänger die Nachricht dann mit dem geheimen Schlüssel erhält, berechnet er den HMAC neu, indem er ihn mit dem ursprünglichen HMAC vergleicht, um festzustellen, ob die Nachricht geändert wurde. Die HMAC-Funktion wird von Standalone-Appliances und von Appliances in einer Hochverfügbarkeitskonfiguration oder in einem Cluster unterstützt. Die Verwendung ähnelt der Konfiguration eines Verschlüsselungsschlüssels.

Die Befehle add ns hmackey und set ns hmackey enthalten einen Parameter, der die Digest-Methode und den gemeinsamen geheimen Schlüssel angibt, die für die HMAC-Berechnung verwendet werden sollen.

Um einen HMAC-Schlüssel zu konfigurieren, müssen Sie Folgendes ausführen:

1. Hinzufügen eines HMAC-Schlüssels. Konfiguriert einen HMAC-Schlüssel mit einem bestimmten Schlüsselwert.
2. Ändern eines HMAC-Schlüssels. Ändert Parameter für einen konfigurierten HMAC-Schlüssel. Die Digest-Methode kann geändert werden, ohne den Schlüsselwert zu ändern, da die Länge des Schlüsselwerts nicht durch den Digest bestimmt wird. Es ist jedoch ratsam, beim Ändern des Digest einen neuen Schlüssel anzugeben.
3. Einen HMAC-Schlüssel aufheben. Setzt Parameter für einen konfigurierten HMAC-Schlüssel auf ihre Standardwerte. Ein HMacKey Objekt mit dem Namen muss existieren. Der einzige Parameter, der nicht gesetzt werden kann, ist der Kommentar, der gelöscht wird.
4. Einen HMAC-Schlüssel entfernen. Löscht einen konfigurierten Schlüssel. Der Schlüssel kann keine Referenzen haben.
5. Zeigen Sie einen HMAC-Schlüssel an. Zeigt Parameter für den konfigurierten HMAC-Wechselstromschlüssel oder alle konfigurierten Tasten an. Wenn der Name weggelassen wird, wird der Schlüsselwert nicht angezeigt.

Konfigurieren Sie einen eindeutigen und zufälligen HMAC-Schlüssel

Sie können automatisch einen eindeutigen HMAC-Schlüssel generieren. Wenn es sich bei Ihrer Appliance um eine Clusterkonfiguration handelt, wird der HMAC-Schlüssel zu Beginn des Prozesses generiert und an alle Knoten und Paket-Engines verteilt. Dadurch wird sichergestellt, dass der HMAC-Schlüssel für alle Paket-Engines und alle Knoten im Cluster gleich ist.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns hmacKey <your_key> -digest <digest> -keyValue <keyvalue>
```

Beispiel:

```
add ns hmacKey <name> -digest sha1 -keyValue AUTO
```

Hierbei gilt:

- Die Namenssyntax ist korrekt und dupliziert nicht den Namen eines vorhandenen Schlüssels.
- Der “AUTO” KeyValue kann in den set-Befehlen verwendet werden, um neue Schlüssel für bestehende EncrytionKey- und HMacKey-Objekte zu generieren.

> **Hinweis:**
>
> Die automatische Schlüsselgenerierung ist nützlich, wenn die Citrix ADC-Appliance Daten mit dem Schlüssel verschlüsselt und entschlüsselt oder einen HMAC-Schlüssel generiert und überprüft. Da der Schlüsselwert selbst bei der Anzeige bereits verschlüsselt ist, können Sie den generierten Schlüsselwert nicht zur Verwendung durch eine andere Partei abrufen.

Beispiel:


```
add ns hmacKey my_hmac_key -digest sha1 -keyValue 0c753c6c5ef859189cacdf95b506d02c179
```

Die obigen Verschlüsselungsmethoden spezifizieren den Betriebsmodus mit CBC als Standardbetriebsmodus. Daher entsprechen die Methoden DES, DES2, AES128, AES192 und AES256 den Methoden DES-CBC, DES3-CBC, AES128-CBC, AES192-CBC und AES256-CBC.

Ändern eines HMAC-Schlüssels über die CLI

Dieser Befehl ändert die für einen HMAC-Schlüssel konfigurierten Parameter. Sie können den Digest ändern, ohne den Schlüsselwert zu ändern, da die Länge des Schlüsselwerts nicht durch den Digest bestimmt wird. Es ist jedoch ratsam, beim Ändern des Digest einen neuen Schlüssel anzugeben. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set ns hmacKey <name> [-digst <digest>] [-keyValue <keyvalue>]
2 [-comment <string>]
3
4 <!--NeedCopy-->
```

HMAC-Schlüssel über die CLI aufheben

Mit diesem Befehl werden für einen HMAC-Schlüssel konfigurierte Parameter mit ihren Standardwerten festgelegt. Ein HMacKey Objekt mit dem Namen muss existieren. Der einzige Parameter, den Sie aufheben können, ist die Kommentaroption, die gelöscht wird. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
unset ns hmacKey <name> -comment
```

Entfernen Sie einen HMAC-Schlüssel über die CLI

Dieser Befehl löscht den konfigurierten Hmac-Schlüssel. Der Schlüssel kann keine Referenzen haben. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm ns hmacKey <name>
```

Zeigen Sie einen HMAC-Schlüssel über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
show ns encryptionKey [<name>]

add ns hmacKey my_hmac_key -digest sha1 -keyValue 0
    c753c6c5ef859189cacdf95b506d02c1797407d
set ns hmacKey my_hmac_key -keyValue
    f348c594341a840a1f641a1cf24aa24c15eb1317
rm ns hmacKey my_hmac_key
show ns hmacKey my_hmac_key
           Name: my_hmac_key
     Digest: SHA1
     Key Value: (not disclosed)
<!--NeedCopy-->
```

Erweiterte Richtlinienausdrücke: Arbeiten mit Datumsangaben, Uhrzeiten und Zahlen

October 5, 2021

Die meisten numerischen Daten, die von der Citrix ADC Appliance verarbeitet werden, bestehen aus Datums- und Uhrzeitangaben. Neben der Arbeit mit Datums- und Uhrzeiten verarbeitet die Appliance andere numerische Daten, z. B. die Längen von HTTP-Anfragen und -Antworten. Um diese Daten zu verarbeiten, können Sie erweiterte Richtlinienausdrücke konfigurieren, die Nummern verarbeiten.

Ein numerischer Ausdruck besteht aus einem Ausdruckspräfix, das eine Zahl zurückgibt, und manchmal, aber nicht immer, einem Operator, der eine Operation für die Nummer ausführen kann. Beispiele für Ausdruckspräfixe, die Zahlen zurückgeben, sind `SYS.TIME.DAY`, `HTTP.REQ.CONTENT_LENGTH` und `HTTP.RES.BODY.LENGTH`. `Numeric`. Operatoren können mit jedem Präfixausdruck arbeiten, der Daten in numerisches Format. Der Operator `GT(<int>)` kann beispielsweise mit jedem Präfixausdruck verwendet werden, z. B. HTTP.REQ.CONTENT_LENGTH, der eine ganze Zahl zurückgibt.

Format von Datums- und Uhrzeiten in einem Ausdruck

October 5, 2021

Wenn Sie einen erweiterten Richtlinienausdruck in einer Richtlinie konfigurieren, die mit Datums- und Uhrzeitangaben arbeitet (z. B. die Citrix ADC -Systemzeit oder ein Datum in einem SSL-Zertifikat), geben Sie ein Zeitformat wie folgt an:

`GMT|LOCAL [<yyyy>] [<month>] [<d>] [<h>] [<m>] [<s>]`

Wobei:

- <yyyy>ist ein vierstelliges Jahr nach GMT oder LOCAL.
- <month>ist eine dreistellige Abkürzung für den Monat, zum Beispiel Jan, Dez.
- <d>ist ein Wochentag oder eine Ganzzahl für das Datum.

  Sie können den Tag nicht als Montag, Dienstag usw. angeben. Sie geben entweder eine ganze Zahl für einen bestimmten Tag des Monats an, oder Sie geben ein Datum als erster, zweiter, dritter Wochentag des Monats usw. an. Im Folgenden finden Sie Beispiele für die Angabe eines Wochentages:

  - Sun_1 ist der erste Sonntag im Monat.
  - Sun_3 ist der dritte Sonntag im Monat.
  - Wed_3 ist der dritte Mittwoch im Monat.
  - 30 ist ein Beispiel für ein genaues Datum in einem Monat.
- <h>ist die Stunde, zum Beispiel 10h.
- <s> ist die Anzahl der Sekunden, z. B. 30s.

Der folgende Beispielausdruck ist true, wenn das Datum zwischen 2008 Jan und 2009 Jan liegt, basierend auf GMT.

```
http.req.date.between(GMT 2008 Jan, GMT 2009 Jan)
```

Der folgende Beispielausdruck gilt für März und alle Monate, die März im Kalenderjahr folgen, basierend auf GMT:

```
sys.time.ge(GMT 2008 Mar)
```

Wenn Sie ein Datum und eine Uhrzeit angeben, beachten Sie, dass das Format Groß-/Kleinschreibung beachtet und die genaue Anzahl der Leerzeichen zwischen den Einträgen beibehalten muss.

```
**Note:**

In an expression that requires two time values, both must use GMT or
    both must use LOCAL. You cannot mix the two in an expression.

Unlike when you use the SYS.TIME prefix in an advanced policy
    expression, if you specify SYS.TIME in a rewrite action, the Citrix
    ADC returns a string in conventional date format (for example, Sun,
    06 Nov 1994 08:49:37 GMT). For example, the following rewrite action
     replaces the http.res.date header with the Citrix ADC system time
    in a conventional date format:

add rewrite action sync_date replace http.res.date sys.time
```


Ausdrücke für die Citrix ADC -Systemzeit

October 5, 2021

Das SYS.TIME-Ausdruckspräfix extrahiert die Citrix ADC -Systemzeit. Sie können Ausdrücke konfigurieren, die anhand der Citrix ADC -Systemzeit festlegen, ob ein bestimmtes Ereignis zu einem bestimmten Zeitpunkt oder innerhalb eines bestimmten Zeitraums aufgetreten ist.

In der folgenden Tabelle werden die Ausdrücke beschrieben, die Sie mit dem SYS.TIME-Präfix erstellen können.

- **SYS.TIME.BETWEEN(<time1>, <time2>):**

  Gibt einen booleschen TRUE zurück, wenn der zurückgegebene Wert später als <time1> und früher ist <time2>.

  Sie formatieren die <time1> <time2> Argumente, wie folgt:

  - Sie müssen beide GMT oder beide LOCAL sein.
  - <time2>muss später sein als <time1>.

  Wenn die aktuelle Zeit beispielsweise GMT 2005 Mai 1 10h 15m 30s ist, und es ist der erste Sonntag des Monats, können Sie Folgendes angeben:

  - sys.time.between (GMT 2004, GMT 2006)
  - sys.time.between (GMT 2004 Jan, GMT 2006 Nov)
  - sys.time.between (GMT 2004 Jan, GMT 2006)
  - sys.time.between (GMT 2005 Mai Sun_1, GMT 2005 Mai Sun_3)
  - sys.time.between (GMT 2005 1. Mai, GMT Mai 2005 1)
  - sys.time.between (LOCAL 2005 1. Mai, LOCAL Mai 2005 1)

- **SYS.TIME.DAY:**

  Gibt den aktuellen Tag des Monats als Zahl von 1 bis 31.

- **SYS.TIME.EQ(<time>):**

  Gibt einen booleschen TRUE zurück, wenn die aktuelle Uhrzeit dem <time> Argument entspricht.

  Wenn die aktuelle Zeit beispielsweise GMT 2005 Mai 1 10h 15m 30s ist und der erste Sonntag des Monats ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung werden in Klammern angezeigt):

  - sys.time.eq (GMT 2005) (TRUE in diesem Beispiel.)
  - sys.time.eq (GMT 2005 Dec) (FALSE in diesem Beispiel.)
  - sys.time.eq (LOCAL 2005 May) (In diesem Beispiel wird TRUE oder FALSE ausgewertet, abhängig von der aktuellen Zeitzone.)

- sys.time.eq (GMT 10h) (TRUE in diesem Beispiel.)
- sys.time.eq (GMT 10h 30s) (TRUE in diesem Beispiel.)
- sys.time.eq (GMT May 10h) (TRUE in diesem Beispiel.)
- sys.time.eq (GMT Sun) (TRUE in diesem Beispiel.)
- sys.time.eq (GMT May Sun_1) (TRUE in diesem Beispiel.)

- **SYS.TIME.NE(<time>):**

  Gibt einen booleschen TRUE zurück, wenn die aktuelle Uhrzeit nicht dem <time> Argument entspricht.

- **SYS.TIME.GE (<time>):**

  Gibt einen booleschen TRUE zurück, wenn die aktuelle Uhrzeit später oder gleich ist <time>.

  Wenn die aktuelle Zeit beispielsweise GMT 2005 Mai 1 10h 15m 30s ist und der erste Sonntag des Monats ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung werden in Klammern angezeigt):

  - sys.time.ge (GMT 2004) (TRUE in diesem Beispiel.)
  - sys.time.ge (GMT 2005 Jan) (TRUE in diesem Beispiel.)
  - sys.time.ge (LOCAL 2005 May) (TRUE oder FALSE in diesem Beispiel, abhängig von der aktuellen Zeitzone.)
  - sys.time.ge (GMT 8h) (TRUE in diesem Beispiel.)
  - sys.time.ge (GMT 30m) (FALSE in diesem Beispiel.)
  - sys.time.ge (GMT May 10h) (TRUE in diesem Beispiel.)
  - sys.time.ge (GMT May 10h 0m) (TRUE in diesem Beispiel.)
  - sys.time.ge (GMT Sun) (TRUE in diesem Beispiel.)
  - sys.time.ge (GMT May Sun_1) (TRUE in diesem Beispiel.)

- **SYS.TIME.GT (<time>):**

  Gibt einen booleschen TRUE zurück, wenn der Zeitwert später als das <time> Argument liegt.

  Wenn die aktuelle Zeit beispielsweise GMT 2005 Mai 1 10h 15m 30s ist und der erste Sonntag des Monats ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung werden in Klammern angezeigt):

  - sys.time.gt (GMT 2004) (TRUE in diesem Beispiel.)
  - sys.time.gt (GMT 2005 Jan) (TRUE in diesem Beispiel.)
  - sys.time.gt (LOCAL 2005 Mai) (TRUE oder FALSE, abhängig von der aktuellen Zeitzone.)
  - sys.time.gt (GMT 8h) (TRUE in diesem Beispiel.)
  - sys.time.gt (GMT 30m) (FALSE in diesem Beispiel.)
  - sys.time.gt (GMT Mai 10h) (FALSE in diesem Beispiel.)
  - sys.time.gt (GMT Mai 10h 0m) (TRUE in diesem Beispiel.)
  - sys.time.gt(GMT Sun) (FALSE in this example.)

  - sys.time.gt(GMT May Sun_1) (FALSE in this example.)

- **SYS.TIME.HOURS:**

  Gibt die aktuelle Stunde als Ganzzahl von 0 bis 23.

- **SYS.TIME.LE(<time>):**

  Gibt einen booleschen Wert TRUE zurück, wenn der aktuelle Zeitwert dem <time> Argument vorausgeht oder gleich ist.

  Wenn die aktuelle Zeit beispielsweise GMT 2005 Mai 1 10h 15m 30s ist und der erste Sonntag des Monats ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung werden in Klammern angezeigt):

  - sys.time.le(GMT 2006) (TRUE in this example.)
  - sys.time.le(GMT 2005 Dec) (TRUE in this example.)
  - sys.time.le(LOCAL 2005 May) (TRUE or FALSE depending on the current timezone.)
  - sys.time.le(GMT 8h) (FALSE in this example.)
  - sys.time.le(GMT 30m) (TRUE in this example.)
  - sys.time.le(GMT May 10h) (TRUE in this example.)
  - sys.time.le(GMT Jun 11h) (TRUE in this example.)
  - sys.time.le(GMT Wed) (TRUE in this example.)
  - sys.time.le(GMT May Sun_1) (TRUE in this example.)

- **SYS.TIME.LT(<time>):**

  Gibt einen booleschen Wert TRUE zurück, wenn der aktuelle Zeitwert dem <time> Argument vorausgeht.

  Wenn die aktuelle Zeit beispielsweise GMT 2005 Mai 1 10h 15m 30s ist und der erste Sonntag des Monats ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung werden in Klammern angezeigt):

  - sys.time.lt(GMT 2006) (TRUE in this example.)
  - sys.time.lt.time.lt(GMT 2005 Dec) (TRUE in this example.)
  - sys.time.lt(LOCAL 2005 May) (TRUE or FALSE depending on the current time zone.)
  - sys.time.lt(GMT 8h) (FALSE in this example.)
  - sys.time.lt(GMT 30m) (TRUE in this example.)
  - sys.time.lt(GMT May 10h) (FALSE in this example.)
  - sys.time.lt(GMT Jun 11h) (TRUE in this example.)
  - sys.time.lt(GMT Wed) (TRUE in this example.)
  - sys.time.lt(GMT May Sun_1) (FALSE in this example.)

- **SYS.TIME.MINUTES:**

  Gibt die aktuelle Minute als Ganzzahl von 0 bis 59.

- **SYS.TIME.MONTH:**

  Extrahiert den aktuellen Monat und gibt eine ganze Zahl von 1 (Januar) bis 12 (Dezember) zurück.

- **SYS.TIME.RELATIVE_BOOT:**

  Berechnet die Anzahl der Sekunden bis zum nächsten vorherigen oder geplanten Neustart und gibt eine ganze Zahl zurück.

  Wenn die nächste Startzeit in der Vergangenheit liegt, ist die ganze Zahl negativ. Wenn es in der Zukunft ist, ist die ganze Zahl positiv.

- **SYS.TIME.RELATIVE_NOW:**

  Berechnet die Anzahl der Sekunden zwischen der aktuellen Citrix ADC -Systemzeit und der angegebenen Zeit und gibt eine ganze Zahl zurück, die die Differenz anzeigt.

  Wenn die angegebene Zeit in der Vergangenheit liegt, ist die ganze Zahl negativ; wenn sie in der Zukunft ist, ist die ganze Zahl positiv.

- **SYS.TIME.SECONDS:**

  Extrahiert die Sekunden aus der aktuellen Citrix ADC -Systemzeit und gibt diesen Wert als Ganzzahl von 0 bis 59.

- **SYS.TIME.WEEKDAY:**

  Gibt den aktuellen Wochentag als Wert von 0 (Sonntag) bis 6 (Samstag) zurück.

- **SYS.TIME.WITHIN (<time1>, <time2>):**

  Wenn Sie ein Element der Zeit <time1> beispielsweise in dem Tag oder der Stunde weglassen, wird davon ausgegangen, dass es den niedrigsten Wert in seinem Bereich hat. Wenn Sie ein Element in weglassen <time2>, wird angenommen, dass es den höchsten Wert seines Bereichs hat.

  Die Bereiche für die Elemente der Zeit sind wie folgt: Monat 1-12, Tag 1-31, Wochentag 0-6, Stunde 0-23, Minuten 0-59 und Sekunden 0-59. Wenn Sie das Jahr angeben, müssen Sie dies sowohl in als <time1> auch tun <time2>.

  Wenn die Zeit beispielsweise GMT 2005 10. Mai 10h 15m 30s ist, und es ist der zweite Dienstag des Monats, können Sie Folgendes angeben (die Ergebnisse der Auswertung werden in Klammern angezeigt):

  - sys.time.within(GMT 2004, GMT 2006) (TRUE in this example.)
  - sys.time.within(GMT 2004 Jan, GMT 2006 Mar) (FALSE, May is not in the range of January to March.)
  - sys.time.within(GMT Feb, GMT) (TRUE, May is in the range of February to December.)
  - sys.time.within(GMT Sun_1, GMT Sun_3) (TRUE, the second Tuesday is between the first Sunday and the third Sunday.)

  - sys.time.within(GMT 2005 May 1 10h, GMT May 2005 1 17h) (TRUE in this example.)
  - sys.time.within(LOCAL 2005 May 1, LOCAL May 2005 1) (TRUE or FALSE, depending on the Citrix ADC system time zone.)

- **SYS.TIME.YEAR:**

  Extrahiert das Jahr aus der aktuellen Systemzeit und gibt diesen Wert als vierstellige Ganzzahl zurück.

Ausdrücke für SSL-Zertifikatsdaten

October 5, 2021

Sie können den Gültigkeitszeitraum für SSL-Zertifikate bestimmen, indem Sie einen Ausdruck konfigurieren, der das folgende Präfix enthält:

```
CLIENT.SSL.CLIENT_CERT
```

Der folgende Beispielausdruck entspricht einer bestimmten Ablaufzeit mit den Informationen im Zertifikat:

```
client.ssl.client_cert.valid_not_after.eq(GMT 2009)
```

In der folgenden Tabelle werden zeitbasierte Vorgänge mit SSL-Zertifikaten beschrieben. Um den gewünschten Ausdruck zu erhalten, ersetzen Sie das *Zertifikat* im Ausdruck in der ersten Spalte durch den Präfixausdruck CLIENT.SSL.CLIENT_CERT.

- `<certificate>.VALID_NOT_AFTER`:

  Gibt den letzten Tag vor dem Zertifikatablauf zurück. Das Rückgabeformat ist die Anzahl der Sekunden seit GMT 1. Januar 1970 (0 Stunden, 0 Minuten, 0 Sekunden).

- **<certificate>.VALID_NOT_AFTER.BETWEEN(<time1>, <time2>):**

  Gibt einen booleschen TRUE Wert zurück, wenn die Gültigkeit des Zertifikats zwischen den <time1> <time2> Argumenten und liegt. Beide <time1> und <time2> müssen vollständig angegeben sein. Im Folgenden finden Sie Beispiele:

  GMT 1995 Jan ist vollständig spezifiziert.

  GMT Jan ist nicht vollständig angegeben

  GMT 1995 20 ist nicht vollständig spezifiziert.

  GMT Jan Mon_2 ist nicht vollständig angegeben.

  Die <time1> <time2> Argumente und müssen sowohl GMT als auch beide LOCAL <time2> sein und größer sein als <time1>.

Wenn es sich beispielsweise um GMT 2005 Mai 1 10h 15m 30s handelt, und der erste Sonntag des Monats, können Sie Folgendes angeben (die Ergebnisse der Auswertung sind in Klammern).

- . . .between(GMT 2004, GMT 2006) (TRUE)
- . . .between(GMT 2004 Jan, GMT 2006 Nov) (TRUE)
- . . .between(GMT 2004 Jan, GMT 2006) (TRUE)
- . . .between(GMT 2005 May Sun_1, GMT 2005 May Sun_3) (TRUE)
- . . .between(GMT 2005 May 1, GMT May 2005 1) (TRUE)
- . . .between(LOCAL 2005 May 1, LOCAL May 2005 1) (TRUE or FALSE, depending on the Citrix ADC system time zone.)

- **.VALID_NOT_AFTER.DAY:**<certificate>

  Extrahiert den letzten Tag des Monats, in dem das Zertifikat gültig ist, und gibt je nach Datum eine Zahl zwischen 1 und 31 zurück.

- **<certificate>.VALID_NOT_AFTER.EQ (<time>):**

  Gibt einen booleschen TRUE zurück, wenn die Zeit dem <time> Argument entspricht.

  Wenn die aktuelle Zeit beispielsweise GMT 2005 Mai 1 10h 15m 30s ist und der erste Sonntag des Monats ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung sind in Klammern):

  - . . .eq(GMT 2005) (TRUE)
  - . . .eq(GMT 2005 Dec) (FALSE)
  - . .eq (LOCAL 2005 Mai) (TRUE oder FALSE, abhängig von der aktuellen Zeitzone)
  - . . .eq(GMT 10h) (TRUE)
  - . . .eq(GMT 10h 30s) (TRUE)
  - . . .eq(GMT May 10h) (TRUE)
  - . . .eq(GMT Sun) (TRUE)
  - . . .eq(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_AFTER.GE (<time>):**

  Gibt einen booleschen TRUE zurück, wenn der Zeitwert größer oder gleich dem Argument ist <time>.

  Wenn der Zeitwert beispielsweise GMT 2005 Mai 1 10h 15m 30s ist und der erste Sonntag im Monat Mai 2005 ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung sind in Klammern):

  - . . .ge(GMT 2004) (TRUE)
  - . . .ge(GMT 2005 Jan) (TRUE)
  - . . .ge(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone.)
  - . . .ge(GMT 8h) (TRUE)
  - . . .ge(GMT 30m) (FALSE)
  - . . .ge(GMT May 10h) (TRUE)

- . . .ge(GMT May 10h 0m) (TRUE)
- . . .ge(GMT Sun) (TRUE)
- . . .ge(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_AFTER.GT (<time>):**

  Gibt einen booleschen TRUE zurück, wenn der Zeitwert größer als das Argument ist <time>.

  Wenn der Zeitwert beispielsweise GMT 2005 Mai 1 10h 15m 30s ist und der erste Sonntag im Monat Mai 2005 ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung sind in Klammern):

  - . . .gt(GMT 2004) (TRUE)
  - . . .gt(GMT 2005 Jan) (TRUE)
  - . . .gt(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone.)
  - . . .gt(GMT 8h) (TRUE)
  - . . .gt(GMT 30m) (FALSE)
  - . . .gt(GMT May 10h) (FALSE)
  - . . .gt(GMT Sun) (FALSE)
  - . . .gt(GMT May Sun_1) (FALSE)

- **.VALID_NOT_AFTER.HOURS:**<certificate>

  Extrahiert die letzte Stunde, in der das Zertifikat gültig ist, und gibt diesen Wert als Ganzzahl von 0 bis 23.

- **<certificate>.VALID_NOT_AFTER.LE (<time>):**

  Gibt einen booleschen TRUE zurück, wenn die Zeit dem <time> Argument vorausgeht oder gleich ist.

  Wenn der Zeitwert beispielsweise GMT 2005 Mai 1 10h 15m 30s ist und der erste Sonntag im Monat Mai 2005 ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung sind in Klammern):

  - . . .le(GMT 2006) (TRUE)
  - . . .le(GMT 2005 Dec) (TRUE)
  - . .le (LOCAL 2005 Mai) (TRUE oder FALSE, abhängig von der aktuellen Zeitzone.)
  - . .le (GMT 8h) (FALSE)
  - . .le (GMT 30m) (TRUE)
  - . . .le(GMT May 10h) (TRUE)
  - . . .le(GMT Jun 11h) (TRUE)
  - . . .le(GMT Wed) (TRUE)
  - . . .le(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_AFTER.LT (<time>):**

Gibt einen booleschen TRUE zurück, wenn die Zeit dem <time> Argument vorausgeht.

Wenn die aktuelle Zeit beispielsweise GMT 2005 Mai 1 10h 15m 30s ist, und es ist der erste Sonntag des Monats, können Sie Folgendes angeben:

- . . .lt(GMT 2006) (TRUE)
- . . .lt(GMT 2005 Dec) (TRUE)
- . . .lt(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone.)
- . . .lt(GMT 8h) (FALSE)
- . . .lt(GMT 30m) (TRUE)
- . . .lt(GMT May 10h) (FALSE)
- . . .lt(GMT Jun 11h) (TRUE)
- . . .lt(GMT Wed) (TRUE)
- . . .lt(GMT May Sun_1) (FALSE)

- **<certificate>.VALID_NOT_AFTER.MINUTES:**

  Extrahiert die letzte Minute, in der das Zertifikat gültig ist, und gibt diesen Wert als Ganzzahl von 0 bis 59.

- **<certificate>.VALID_NOT_AFTER.MONTH:**

  Extrahiert den letzten Monat, in dem das Zertifikat gültig ist, und gibt diesen Wert als Ganzzahl von 1 (Januar) bis 12 (Dezember) zurück.

- **<certificate>.VALID_NOT_AFTER.RELATIVE_BOOT:**

  Berechnet die Anzahl der Sekunden bis zum nächsten vorherigen oder geplanten Neustart und gibt eine ganze Zahl zurück. Wenn die nächste Startzeit in der Vergangenheit liegt, ist die ganze Zahl negativ. Wenn es in der Zukunft ist, ist die ganze Zahl positiv.

- **<certificate>.VALID_NOT_AFTER.RELATIVE_NOW;**

  Berechnet die Anzahl der Sekunden zwischen der aktuellen Systemzeit und der angegebenen Zeit und gibt eine ganze Zahl zurück. Wenn die Zeit in der Vergangenheit liegt, ist die ganze Zahl negativ; wenn sie in der Zukunft ist, ist die ganze Zahl positiv.

- **<certificate>.VALID_NOT_AFTER.SECONDS:**

  Extrahiert die letzte Sekunde, in der das Zertifikat gültig ist, und gibt diesen Wert als Ganzzahl von 0 bis 59.

- **<certificate>.VALID_NOT_AFTER.WEEKDAY:**

  Extrahiert den letzten Wochentag, an dem das Zertifikat gültig ist. Gibt eine Zahl zwischen 0 (Sonntag) und 6 (Samstag) zurück, um den Wochentag im Zeitwert anzugeben.

- **<certificate>.VALID_NOT_AFTER.WITHIN(<time1>, <time2>):**

Gibt einen booleschen TRUE zurück, wenn die Zeit innerhalb aller Bereiche liegt, die durch die Elemente in <time1> und definiert <time2> werden.

Wenn Sie ein Zeitelement weglassen <time1>, wird davon ausgegangen, dass es den niedrigsten Wert in seinem Bereich hat. Wenn Sie ein Element weglassen <time2>, wird davon ausgegangen, dass es den höchsten Wert seines Bereichs hat. Wenn Sie ein Jahr in angeben <time1>, müssen Sie es unter angeben <time2>.

Die Bereiche für Elemente der Zeit sind wie folgt: Monat 1-12, Tag 1-31, Wochentag 0-6, Stunde 0-23, Minuten 0-59 und Sekunden 0-59. Damit das Ergebnis TRUE ist, muss jedes Element in der Zeit in dem entsprechenden Bereich vorhanden sein, den Sie in <time1>, angeben <time2>.

Wenn Zeit beispielsweise GMT 2005 10. Mai 10h 15m 30s ist, und es ist der zweite Dienstag des Monats, können Sie Folgendes angeben (die Ergebnisse der Auswertung sind in Klammern):

- . . .within(GMT 2004, GMT 2006) (TRUE)
- . . .within(GMT 2004 Jan, GMT 2006 Mar) (FALSE, May is not in the range of January to March.)
- . . .within(GMT Feb, GMT) (TRUE, May is in the range for February to December)
- . . .within(GMT Sun_1, GMT Sun_3) (TRUE, the second Tuesday lies within the range of the first Sunday through the third Sunday)
- . . .within(GMT 2005 May 1 10h, GMT May 2005 1 17h) (TRUE)
- . . .within(LOCAL 2005 May 1, LOCAL May 2005 1) (TRUE or FALSE, depending on the Citrix ADC system time zone)

- **<certificate>.VALID_NOT_AFTER.YEAR:**

  Extrahiert das letzte Jahr, in dem das Zertifikat gültig ist, und gibt eine vierstellige Ganzzahl zurück.

- **<certificate>.VALID_NOT_BEFORE:**

  Gibt das Datum zurück, an dem das Clientzertifikat gültig wird.

  Das Rückgabeformat ist die Anzahl der Sekunden seit GMT 1. Januar 1970 (0 Stunden, 0 Minuten, 0 Sekunden).

- **<certificate>.VALID_NOT_BEFORE.BETWEEN(<time1>, <time2>):**

  Gibt einen booleschen TRUE zurück, wenn der Zeitwert zwischen den beiden Zeitargumenten liegt. Beide <time1> <time2> Argumente und Argumente müssen vollständig angegeben werden.

  Im Folgenden finden Sie Beispiele:

  GMT 1995 Jan ist vollständig spezifiziert.
  GMT Jan is not fully specified.
  GMT 1995 20 ist nicht vollständig spezifiziert.

GMT Jan Mon_2 ist nicht vollständig angegeben.
Die Zeitargumente müssen sowohl GMT als auch LOCAL sein und <time2> müssen größer sein als <time1>.

Wenn der Zeitwert beispielsweise GMT 2005 Mai 1 10h 15m 30s ist und der erste Sonntag im Monat Mai 2005 ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung sind in Klammern):

- . . .between(GMT 2004, GMT 2006) (TRUE)
- . . .between(GMT 2004 Jan, GMT 2006 Nov) (TRUE)
- . . .between(GMT 2004 Jan, GMT 2006) (TRUE)
- . . .between(GMT 2005 May Sun_1, GMT 2005 May Sun_3) (TRUE)
- . . .between(GMT 2005 May 1, GMT May 2005 1) (TRUE)
- . . .between(LOCAL 2005 May 1, LOCAL May 2005 1) (TRUE or FALSE, depending on the Citrix ADC system time zone.)

- **<certificate>.VALID_NOT_BEFORE.DAY:**

  Extrahiert den letzten Tag des Monats, in dem das Zertifikat gültig ist, und gibt diesen Wert als Zahl von 1 bis 31 zurück, die diesen Tag darstellt.

- **<certificate>.VALID_NOT_BEFORE.EQ (<time>):**

  Gibt einen booleschen TRUE zurück, wenn die Zeit dem <time> Argument entspricht.

  Wenn der Zeitwert beispielsweise GMT 2005 Mai 1 10h 15m 30s ist und der erste Sonntag im Monat Mai 2005 ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung sind in Klammern):

  - . . .eq(GMT 2005) (TRUE)
  - . . .eq(GMT 2005 Dec) (FALSE)
  - . .eq (LOCAL 2005 Mai) (TRUE oder FALSE, abhängig von der aktuellen Zeitzone.)
  - . . .eq(GMT 10h) (TRUE)
  - . . .eq(GMT 10h 30s) (TRUE)
  - . . .eq(GMT May 10h) (TRUE)
  - . . .eq(GMT Sun) (TRUE)
  - . . .eq(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_BEFORE.GE(<time>):**

  Gibt einen booleschen TRUE zurück, wenn die Zeit größer als (nachher) oder gleich dem <time> Argument ist.

  Wenn der Zeitwert beispielsweise GMT 2005 Mai 1 10h 15m 30s ist und der erste Sonntag im Monat Mai 2005 ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung sind in Klammern):

- . . .ge(GMT 2004) (TRUE)
- . . .ge(GMT 2005 Jan) (TRUE)
- . . .ge(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone.)
- . . .ge(GMT 8h) (TRUE)
- . . .ge(GMT 30m) (FALSE)
- . . .ge(GMT May 10h) (TRUE)
- . . .ge(GMT May 10h 0m) (TRUE)
- . . .ge(GMT Sun) (TRUE)
- . . .ge(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_BEFORE.GT (<time>):**

  Gibt einen booleschen TRUE zurück, wenn die Zeit nach dem <time> Argument eintritt.

  Wenn der Zeitwert beispielsweise GMT 2005 Mai 1 10h 15m 30s ist und der erste Sonntag im Monat Mai 2005 ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung sind in Klammern):

  - . . .gt(GMT 2004) (TRUE)
  - . . .gt(GMT 2005 Jan) (TRUE)
  - . . .gt(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone.)
  - . . .gt(GMT 8h) (TRUE)
  - . . .gt(GMT 30m) (FALSE)
  - . . .gt(GMT May 10h) (FALSE)
  - . .gt (GMT Mai 10h 0m) (TRUE)
  - . . .gt(GMT Sun) (FALSE)
  - . . .gt(GMT May Sun_1) (FALSE)

- **.VALID_NOT_BEFORE.HOURS:**<certificate>

  Extrahiert die letzte Stunde, in der das Zertifikat gültig ist, und gibt diesen Wert als Ganzzahl von 0 bis 23.

- **<certificate>.VALID_NOT_BEFORE.LE (<time>)

  Gibt einen booleschen TRUE zurück, wenn die Zeit dem <time> Argument vorausgeht oder gleich ist.

  Wenn der Zeitwert beispielsweise GMT 2005 Mai 1 10h 15m 30s ist und der erste Sonntag im Monat Mai 2005 ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung sind in Klammern):

  - . . .le(GMT 2006) (TRUE)
  - . . .le(GMT 2005 Dec) (TRUE)
  - . .le (LOCAL 2005 Mai) (TRUE oder FALSE, abhängig von der aktuellen Zeitzone.)

- . .le(GMT 8h) (FALSE)
  . - . .le(GMT 30m) (TRUE)
- . . .le(GMT May 10h) (TRUE)
- . . .le(GMT Jun 11h) (TRUE)
- . . .le(GMT Wed) (TRUE)
- . . .le(GMT May Sun_1) (TRUE)

- **<certificate>.VALID_NOT_BEFORE.LT (<time>):**

  Gibt einen booleschen TRUE zurück, wenn die Zeit dem <time> Argument vorausgeht.

  Wenn der Zeitwert beispielsweise GMT 2005 Mai 1 10h 15m 30s ist und der erste Sonntag im Monat Mai 2005 ist, können Sie Folgendes angeben (die Ergebnisse der Auswertung sind in Klammern):

  - . . .lt(GMT 2006) (TRUE)
  - . . .lt(GMT 2005 Dec) (TRUE)
  - . . .lt(LOCAL 2005 May) (TRUE or FALSE, depending on the current time zone.)
  - . . .lt(GMT 8h) (FALSE)
  - . . .lt(GMT 30m) (TRUE)
  - . . .lt(GMT May 10h) (FALSE)
  - . . .lt(GMT Jun 11h) (TRUE)
  - . . .lt(GMT Wed) (TRUE)
  - . . .lt(GMT May Sun_1) (FALSE)

- **<certificate>.VALID_NOT_BEFORE.MINUTES:**

  Extrahiert die letzte Minute, in der das Zertifikat gültig ist. Gibt die aktuelle Minute als Ganzzahl von 0 bis 59.

- **<certificate>.VALID_NOT_BEFORE.MONTH:**

  Extrahiert den letzten Monat, in dem das Zertifikat gültig ist. Gibt den aktuellen Monat als Ganzzahl von 1 (Januar) bis 12 (Dezember) zurück.

- **<certificate>.VALID_NOT_BEFORE.RELATIVE_BOOT:**

  Berechnet die Anzahl der Sekunden bis zum nächsten vorherigen oder geplanten Citrix ADC Neustart und gibt eine ganze Zahl zurück. Wenn die nächste Startzeit in der Vergangenheit liegt, ist die ganze Zahl negativ; wenn sie in der Zukunft ist, ist die ganze Zahl positiv.

- **<certificate>.VALID_NOT_BEFORE.RELATIVE_NOW:**

  Gibt die Anzahl der Sekunden zwischen der aktuellen Citrix ADC -Systemzeit und der angegebenen Zeit als Ganzzahl zurück. Wenn die angegebene Zeit in der Vergangenheit liegt, ist die ganze Zahl negativ. Wenn es in der Zukunft ist, ist die ganze Zahl positiv.

- **<certificate>.VALID_NOT_BEFORE.SECONDS:**

Extrahiert die letzte Sekunde, in der das Zertifikat gültig ist. Gibt die aktuelle Sekunde als Ganzzahl von 0 bis 59.

- **<certificate>.VALID_NOT_BEFORE.WEEKDAY:**

  Extrahiert den letzten Wochentag, an dem das Zertifikat gültig ist. Gibt den Wochentag als Zahl zwischen 0 (Sonntag) und 6 (Samstag) zurück.

- **<certificate>.VALID_NOT_BEFORE.WITHIN(<time1>, <time2>):**

  Gibt einen booleschen TRUE zurück, wenn jedes Element der Zeit innerhalb des Bereichs existiert, der in den <time1> <time2> Argumenten, definiert ist.

  Wenn Sie ein Zeitelement weglassen <time1>, wird davon ausgegangen, dass es den niedrigsten Wert in seinem Bereich hat. Wenn Sie ein Element der Zeit aus weglassen <time2>, wird davon ausgegangen, dass es den höchsten Wert in seinem Bereich hat. Wenn Sie ein Jahr in angeben <time1>, muss es in angegeben werden <time2>. Die Bereiche für Elemente der Zeit sind wie folgt: Monat 1-12, Tag 1-31, Wochentag 0-6, Stunde 0-23, Minuten 0-59 und Sekunden 0-59.

  Wenn die Zeit beispielsweise GMT 2005 10. Mai 10h 15m 30s ist, und es ist der zweite Dienstag des Monats, können Sie Folgendes angeben (die Ergebnisse der Auswertung sind in Klammern):

  - . . .within(GMT 2004, GMT 2006) (TRUE)
  - . . .within(GMT 2004 Jan, GMT 2006 Mar) (FALSE, May is not in the range of January to March.)
  - . . .within(GMT Feb, GMT) (TRUE, May is in the range of February to December.)
  - . . .within(GMT Sun_1, GMT Sun_3) (TRUE, the second Tuesday is between the first Sunday and the third Sunday.)
  - . . .within(GMT 2005 May 1 10h, GMT May 2005 1 17h) (TRUE)
  - . . .within(LOCAL 2005 May 1, LOCAL May 2005 1) (TRUE or FALSE, depending on the Citrix ADC system time zone)

- **<certificate>.VALID_NOT_BEFORE.YEAR:**

  Extrahiert das letzte Jahr, in dem das Zertifikat gültig ist. Gibt das aktuelle Jahr als vierstellige Ganzzahl zurück.

Ausdrücke für HTTP-Anforderungs- und Antwortdaten

October 5, 2021

Die folgenden Ausdruckspräfixe geben den Inhalt des HTTP Date-Headers als Text oder als Datumsobjekt zurück. Diese Werte können wie folgt ausgewertet werden:

- Als Nummer. Der numerische Wert eines HTTP Date-Headers wird in Form der Anzahl der Sekunden seit dem 1. Januar 1970 zurückgegeben.

  Beispielsweise gibt der Ausdruck http.req.date.mod (86400) die Anzahl der Sekunden seit dem Beginn des Tages zurück. Diese Werte können mit denselben Operationen ausgewertet werden wie andere nicht datumsbezogene numerische Daten. Weitere Informationen finden Sie unter Ausdruckspräfixe für andere numerische Daten als Datum und Uhrzeit.

- Als HTTP-Header. Datum-Header können mit den gleichen Operationen wie andere HTTP-Header ausgewertet werden.

  Weitere Informationen finden Sie unter Standardsyntaxausdrücke: Analysieren von HTTP-, TCP- und UDP-Daten.

- Als Text. Datumskopfzeilen können mit den gleichen Operationen wie andere Zeichenfolgen ausgewertet werden.

Weitere Informationen finden Sie unter Erweiterte Richtlinienausdrücke: Text auswerten.

Prefix	Beschreibung
HTTP.REQ.DATE	Gibt den Inhalt des HTTP Date-Headers als Text oder als Datumsobjekt zurück. Die erkannten Datumsformate sind: RFC822. Sun, 06 Jan 1980 08:49:37 GMT, RFC850. Sunday, 06-Jan-80 09:49:37 GMT, and ASCTIME. Sun Jan 6 08:49:37 1980.
HTTP.RES.DATE	Gibt den Inhalt des HTTP Date-Headers als Text oder als Datumsobjekt zurück. Die erkannten Datumsformate sind: RFC822. Sun, 06 Jan 1980 8:49:37 GMT, RFC850. Sunday, 06-Jan-80 9:49:37 GMT, and ASCTIME. Sun Jan 6 08:49:37 1980.

Generieren Sie den Wochentag als String in kurzen und langen Formaten

October 5, 2021

Die Funktionen `WEEKDAY_STRING_SHORT` und `WEEKDAY_STRING` erzeugen den Wochentag als String in kurzen und langen Formaten. Die zurückgegebenen Strings sind immer in Englisch. Das Präfix, das mit diesen Funktionen verwendet wird, muss den Wochentag im ganzzahligen Format zurückgeben und der akzeptable Bereich für den vom Präfix zurückgegebenen Wert ist 0-6. Daher können Sie

ein beliebiges Präfix verwenden, das eine ganze Zahl im zulässigen Bereich zurückgibt. Eine UNDEF-Bedingung wird ausgelöst, wenn der zurückgegebene Wert nicht in diesem Bereich liegt oder wenn die Speicherzuweisung fehlschlägt.

Im Folgenden sind die Beschreibungen der Funktionen:

Funktion	Beschreibung
`<prefix>.WEEKDAY_STRING_SHORT`	Gibt den Wochentag im Kurzformat zurück. Die Kurzform ist immer 3 Zeichen lang mit einem Anfangssatz und die restlichen Zeichen in Kleinbuchstaben. Beispiel: SYS.TIME.WEEKDAY.WEEKDAY_STRING_SHORT gibt Sun zurück, wenn der von der Funktion WEEKDAY zurückgegebene Wert 0 ist, und Sat, wenn der vom Präfix zurückgegebene Wert 6 lautet.
`<prefix>.WEEKDAY_STRING`	Gibt den Wochentag im Langformat zurück. Die lange Form hat immer ein Anfangsbuchstaben, wobei die restlichen Zeichen in Kleinbuchstaben enthalten sind. SYS.TIME.WEEKDAY.WEEKDAY_STRING“ Gibt beispielsweise Sonntag zurück, wenn der von der Funktion WEEKDAY zurückgegebene Wert 0 ist, und Samstag, wenn der vom Präfix zurückgegebene Wert 6 ist.

Ausdruckspräfixe für numerische Daten außer Datum und Uhrzeit

October 5, 2021

Sie können nicht nur Ausdrücke konfigurieren, die pünktlich ausgeführt werden, sondern auch Ausdrücke für die folgenden numerischen Datentypen konfigurieren:

- Die Länge der HTTP-Anforderungen, die Anzahl der HTTP-Header in einer Anforderung usw.

  Weitere Informationen finden Sie unter Ausdrücke für numerische HTTP-Nutzlastdaten außer Datumsangaben.

- IP- und MAC-Adressen.

  Weitere Informationen finden Sie unter Ausdrücke für IP-Adressen und IP-Subnetze.

- Client- und Serverdaten in Bezug auf Schnittstellen-IDs und Transaktionsdurchsatzrate.

  Weitere Informationen finden Sie unter Ausdrücke für numerische Client- und Serverdaten.

- Numerische Daten in Clientzertifikaten mit Ausnahme von Datumsangaben.

  Informationen zu diesen Präfixen, einschließlich der Anzahl der Tage bis zum Ablauf des Zertifikats und der Größe des Verschlüsselungsschlüssels, finden Sie unter Präfixe für numerische Daten in SSL-Zertifikaten.

Konvertieren von Zahlen in Text

October 5, 2021

Die folgenden Funktionen erzeugen binäre Zeichenfolgen aus einer Zahl, die von einem Ausdruckspräfix zurückgegeben wird. Diese Funktionen sind besonders nützlich in der TCP-Rewrite-Funktion als Ersatzzeichenfolgen für Binärdaten. Weitere Informationen zur Funktion zum Umschreiben von TCP finden Sie unter Umschreiben.

Alle Funktionen geben einen Wert vom Typ Text zurück. Die Endiannität, die einige Funktionen als Parameter akzeptieren, ist entweder LITTLE_ENDIAN oder BIG_ENDIAN.

Funktion	Beschreibung
<number>.SIGNED8_STRING	Erzeugt eine 8-Bit-binäre Zeichenfolge mit Vorzeichen, die die Zahl darstellt. Wenn der Wert außerhalb des Bereichs liegt, wird eine undef Bedingung ausgelöst. Beispiel: HTTP.REQ.BODY (100) .GET_SIGNED8 (16) .SUB (3) .SIGNED8_STRING
<number>.UNSIGNED8_STRING	Erzeugt eine 8-Bit-binäre Zeichenfolge ohne Vorzeichen, die die Zahl darstellt. Wenn der Wert außerhalb des Bereichs liegt, wird eine undef Bedingung ausgelöst. Beispiel: HTTP.REQ.BODY (100) .GET_UNSIGNED8 (31) .ADD (3) .UNSIGNED8_STRING

Funktion	Beschreibung
<number>.SIGNED16_STRING (<endianness>)	Erzeugt eine 16-Bit-binäre Zeichenfolge mit Vorzeichen, die die Zahl darstellt. Wenn der Wert außerhalb des Bereichs liegt, wird eine undef Bedingung ausgelöst. Beispiel: HTTP.REQ.BODY (100) .SKIP (12) .GET_SIGNED16 (0, BIG_ENDIAN) .SUB (4) .SIGNED16_STRING (BIG_ENDIAN)
<number>.UNSIGNED16_STRING (<endianness>)	Erzeugt eine 16-Bit-binäre Zeichenfolge ohne Vorzeichen, die die Zahl darstellt. Wenn der Wert außerhalb des Bereichs liegt, wird eine undef Bedingung ausgelöst. Beispiel: HTTP.REQ.BODY (100) .GET_UNSIGNED16 (47, LITTLE_ENDIAN) .ADD (7) .UNSIGNED16_STRING (LITTLE_ENDIAN)
<number>.SIGNED32_STRING (<endianness>)	Erzeugt eine 32-Bit-Binärzeichenfolge mit Vorzeichen, die die Zahl darstellt. Beispiel: HTTP.REQ.BODY (100) .AFTER_STR (“delim”) .GET_SIGNED32 (0, BIG_ENDIAN) .SUB (1) .SIGNED32_STRING (BIG_ENDIAN)
<unsigned_long_number>.UNSIGNED8_STRING	Erzeugt eine 8-Bit-binäre Zeichenfolge ohne Vorzeichen, die die Zahl darstellt. Wenn der Wert außerhalb des Bereichs liegt, wird eine undef Bedingung ausgelöst. Beispiel: HTTP.REQ.BODY (100) .GET_UNSIGNED8 (24) .TYPECAST_UNSIGNED_LONG_AT.ADD (12) .UNSIGNED8_STRING
<unsigned_long_number>.UNSIGNED16_STRING (<endianness>)	Erzeugt eine 16-Bit-binäre Zeichenfolge ohne Vorzeichen, die die Zahl darstellt. Wenn der Wert außerhalb des Bereichs liegt, wird eine undef Bedingung ausgelöst. Beispiel: HTTP.REQ.BODY (100) .GET_UNSIGNED16 (23, LITTLE_ENDIAN) .TYPECAST_UNSIGNED_LONG_AT.ADD (10) .UNSIGNED16_STRING (LITTLE_ENDIAN)

Funktion	Beschreibung
<unsigned_long_number>.UNSIGNED32_STRING (<endianness>)	Erzeugt eine 32-Bit-Binärzeichenfolge ohne Vorzeichen, die die Zahl darstellt. Wenn der Wert außerhalb des Bereichs liegt, wird eine undef Bedingung ausgelöst. Beispiel: HTTP.REQ.BODY (100) .AFTER_STR (“delim2”) .GET_UNSIGNED32 (0, BIG_ENDIAN) .ADD (2) .UNSIGNED32_STRING (BIG_ENDIAN)

Virtuelle serverbasierte Ausdrücke

October 5, 2021

Mit dem`SYS.VSERVER(”<vserver-name>”)` Ausdruckspräfix können Sie einen virtuellen Server identifizieren. Sie können die folgenden Funktionen mit diesem Präfix verwenden, um Informationen zu dem angegebenen virtuellen Server abzurufen:

- **THROUGHPUT.** Gibt den Durchsatz des virtuellen Servers in Mbit/s (Megabits pro Sekunde) zurück. Der zurückgegebene Wert ist eine lange Zahl ohne Vorzeichen.

  Syntax: SYS.VSERVER(“vserver”).THROUGHPUT

- **CONNECTIONS.** Gibt die Anzahl der Verbindungen zurück, die vom virtuellen Server verwaltet werden. Der zurückgegebene Wert ist eine lange Zahl ohne Vorzeichen.

  Syntax: SYS.VSERVER(“vserver”).CONNECTIONS

- **STATE.** Gibt den Status des virtuellen Servers zurück. Der zurückgegebene Wert ist UP, DOWN oder OUT_OF_SERVICE. Einer dieser Werte kann daher als Argument an den EQ () -Operator übergeben werden, um einen Vergleich durchzuführen, der zu einem booleschen TRUE oder FALSE führt.

  Verwendung: SYS.VSERVER(“vserver”).STATE

- **HEALTH.** Gibt den Prozentsatz der Dienste in einem UP Status für den angegebenen virtuellen Server zurück. Der zurückgegebene Wert ist eine ganze Zahl.

  Verwendung: SYS.VSERVER(“vserver”).HEALTH

- **RESPTIME.** Gibt die Antwortzeit als Ganzzahl zurück, die die Anzahl der Mikrosekunden darstellt. Die Antwortzeit ist die durchschnittliche TTFB (Time To First Byte) aller Dienste, die an den virtuellen Server gebunden sind.

  Verwendung: SYS.VSERVER(“vserver”).RESPTIME

- **SURGECOUNT.** Gibt die Anzahl der Anforderungen in der Überspannungswarteschlange des virtuellen Servers zurück. Der zurückgegebene Wert ist eine ganze Zahl.

  Verwendung: SYS.VSERVER(“vserver”).SURGECOUNT

Beispiel 1:

Die folgende Rewrite-Richtlinie bricht die Rewrite-Verarbeitung ab, wenn die Anzahl der Verbindungen auf dem virtuellen Lastausgleichsserver LBVServer 10000 überschreitet:

```
add rewrite policy norewrite_pol sys.vserver(”LBvserver”).connections.gt
(10000)norewrite
```

Beispiel 2:

Die folgende Umschreibaktion fügt einen benutzerdefinierten Header, TP, ein, dessen Wert der gesamte Wert auf dem virtuellen Server LbvServer ist:

```
add rewrite action tp_header insert_http_header TP SYS.VSERVER(”LBvserver”)
.THROUGHPUT
```

Beispiel 3:

Die folgende Überwachungsprotokollnachrichtigungsaktion schreibt den durchschnittlichen TTFB der Dienste, die an einen virtuellen Server gebunden sind, in die newslog-Protokolldatei:

```
add audit messageaction log_vserver_resptime_act INFORMATIONAL ”\”NS
Response Time to Servers:\” + sys.vserver(\”ssllb\”).resptime + \” millisec
\””-logtoNewnslog YES -bypassSafetyCheck YES
```

Erweiterte Richtlinienausdrücke: Analysieren von HTTP-, TCP- und UDP-Daten

February 24, 2022

Sie können erweiterte Richtlinienausdrücke konfigurieren, um die Nutzlast in einer HTTP-Anforderung oder -Antwort auszuwerten. Die Nutzlast, die einer HTTP-Verbindung zugeordnet ist, umfasst HTTP-Header (Standard- oder benutzerdefinierte Header), Textkörper und Verbindungs-URL. Sie können die Nutzlast auch in einem TCP- oder einem UDP-Paket auswerten und verarbeiten. Bei HTTP-Verbindungen können Sie beispielsweise überprüfen, ob ein bestimmter HTTP-Header vorhanden ist oder ob die URL einen bestimmten Abfrageparameter enthält.

Sie können Ausdrücke konfigurieren, um die URL-Codierung zu transformieren und HTML- oder XML-Code für die nachfolgende Auswertung anzuwenden. Sie können auch XPATH- und JSON-Präfixe verwenden, um das Datum in XML- bzw. JSON-Dateien auszuwerten.

Weitere Informationen zu Authentifizierungsausdrücken wie AAA.USER, AAA.LOGIN finden Sie unter Authentifizierung, Autorisierung und Audit-Anmeldung sowie für den Ausdruck AAA.AUTHENTIFIZIERUNG finden Sie unter Themen zur Benutzerauthentifizierung von Citrix ADC AAA .

Sie können auch textbasierte und numerische erweiterte Richtlinienausdrücke verwenden, um HTTP-Anforderungs- und Antwortdaten auszuwerten. Weitere Informationen finden Sie unter Erweiterte Richtlinienausdrücke: Auswerten von Text und Standardsyntaxausdrücken: Arbeiten mit Datumsangaben, Zeiten und Zahlen.

Ausdrücke zur Identifizierung des Protokolls in einem eingehenden IP-Paket

October 5, 2021

In der folgenden Tabelle sind die Ausdrücke aufgeführt, mit denen Sie das Protokoll in einem eingehenden Paket identifizieren können.

Ausdruck	Beschreibung
CLIENT.IP.PROTOCOL	Identifiziert das Protokoll in IPv4-Paketen, die von Clients gesendet werden.
CLIENT.IPV6.PROTOCOL	Identifiziert das Protokoll in IPv6-Paketen, die von Clients gesendet werden.
SERVER.IP.PROTOCOL	Identifiziert das Protokoll in IPv4-Paketen, die von Servern gesendet werden.
SERVER.IPV6.PROTOCOL	Identifiziert das Protokoll in IPv6-Paketen, die von Servern gesendet werden.

Argumente für die PROTOCOL-Funktion

Sie können die IANA-Protokollnummer (Internet Assigned Numbers Authority) an die PROTOCOL-Funktion übergeben. Wenn Sie beispielsweise ermitteln möchten, ob das Protokoll in einem eingehenden Paket TCP ist, können Sie CLIENT.IP.PROTOCOL.EQ(6) verwenden, wobei 6 die IANA zugewiesene Protokollnummer für TCP ist. Bei einigen Protokollen können Sie anstelle der Protokollnummer einen Aufzählungswert übergeben. Anstelle von CLIENT.IP.PROTOCOL.EQ(6) können Sie beispielsweise CLIENT.IP.PROTOCOL.EQ(TCP) verwenden. In der folgenden Tabelle sind die Protokolle aufgeführt, für die Sie Aufzählungswerte verwenden können, sowie die entsprechenden Aufzählungswerte für die Verwendung mit der PROTOCOL-Funktion.

Protokoll	Aufzählungswert
Übertragungssteuerungsprotokoll (TCP)	TCP
Benutzer-Datagram-Protokoll (UDP)	UDP
Internet Control Message Protocol (ICMP)	ICMP
IP Authentication Header (AH), zur Bereitstellung von Authentifizierungsdiensten in IPv4 und IPv6	AH
Encapsulating Security Payload (ESP) -Protokoll	ESP
Allgemeine Rohrleitungskapselung (GRE)	GRE
IP-within-IP-Kapselungsprotokoll	IPIP
Internet Control Message Protocol für IPv6 (ICMPv6)	ICMPv6
Fragment-Header für IPv6	FRAGMENT

Anwendungsfallszenarien

Die Protokollausdrücke können sowohl in anforderungsbasierten als auch in antwortbasierten Richtlinien verwendet werden. Sie können die Ausdrücke in verschiedenen Citrix ADC Features verwenden, z. B. Lastenausgleich, WAN-Optimierung, Content Switching, Umschreiben und Abhören. Sie können die Ausdrücke mit Funktionen wie EQ () und NE () verwenden, um das Protokoll in einer Richtlinie zu identifizieren und eine Aktion auszuführen.

Im Folgenden sind einige Anwendungsfälle für die Ausdrücke:

- In Branch Repeater-Lastausgleichskonfigurationen können Sie die Ausdrücke in einer Listenrichtlinie für den virtuellen Platzhalterserver verwenden. Beispielsweise können Sie den virtuellen Wildcard-Server mit der Listenrichtlinie CLIENT.IP.PROTOCOL.EQ (TCP) so konfigurieren, dass der virtuelle Server nur TCP-Datenverkehr verarbeitet und einfach den gesamten Nicht-TCP-Datenverkehr überbrückt. Auch wenn Sie anstelle der Listenrichtlinie eine Zugriffssteuerungsliste verwenden können, bietet die Listenrichtlinie eine bessere Kontrolle darüber, welcher Datenverkehr verarbeitet wird.
- Für virtuelle Server mit dem Content Switching vom Typ ANY können Sie Content Switching-Richtlinie n konfigurieren, die Anforderungen auf der Grundlage des Protokolls in eingehenden Paketen wechseln. Beispielsweise können Sie Content Switching-Richtlinien konfigurieren, um den gesamten TCP-Datenverkehr auf einen virtuellen Lastausgleichsserver und den gesamten Nicht-TCP-Datenverkehr auf einen anderen virtuellen Lastausgleichsserver zu leiten.

- Sie können die clientbasierten Ausdrücke verwenden, um die Persistenz basierend auf dem Protokoll zu konfigurieren. Beispielsweise können Sie CLIENT.IP.PROTOCOL verwenden, um Persistenz auf der Grundlage der Protokolle in eingehenden IPv4-Paketen zu konfigurieren.

Ausdrücke für HTTP- und Cache-Control-Header

October 5, 2021

Eine gängige Methode zur Auswertung des HTTP-Datenverkehrs besteht darin, die Header in einer Anforderung oder einer Antwort zu untersuchen. Ein Header kann eine Reihe von Funktionen ausführen, einschließlich der folgenden:

- Geben Sie Cookies an, die Daten über den Absender enthalten.
- Identifizieren Sie den Datentyp, der übertragen wird.
- Identifizieren Sie die Route, die die Daten zurückgelegt haben (die Via Header).

> **Hinweis:**
>
> Wenn eine Operation verwendet wird, um Kopf- und Textdaten auszuwerten, überschreibt die kopfbasierte Operation immer den textbasierten Vorgang. Beispielsweise überschreibt die AFTER_STR-Operation, wenn sie auf einen Header angewendet wird, textbasierte AFTER_STR-Operationen für alle Instanzen des aktuellen Headertyps.

Präfixe für HTTP-Header

Die Tabelle Präfixe für HTTP-Header für Ausdruckspräfixe, die HTTP-Header extrahieren.

Operationen für HTTP-Header

Die Tabelle Operationen für HTTP-Header für Operationen, die Sie mit den Präfixen für HTTP-Header angeben können.

Präfixe für Cache-Control-Header

Die folgenden Präfixe gelten speziell für Cache-Control-Header.

HTTP-Header-Präfix	Beschreibung
HTTP.REQ.CACHE_CONTROL	Gibt einen Cache-Control-Header in einer HTTP-Anforderung zurück.

HTTP-Header-Präfix	Beschreibung
HTTP.RES.CACHE_CONTROL	Gibt einen Cache-Control-Header in einer HTTP-Antwort zurück.

Operationen für Cache-Control-Header

Sie können jede der Operationen für HTTP-Header auf Cache-Control-Header anwenden.

Darüber hinaus identifizieren die folgenden Vorgänge bestimmte Typen von Cache-Control-Headern. Informationen zu diesen Header-Typen finden Sie unter RFC 2616.

HTTP-Header-Vorgang	Beschreibung
`Cache-Control header.NAME(<integer>)`	Gibt als Textwert den Namen des Cache-Control-Headers zurück, der der n-ten Komponente in einer Name-Wert-Liste entspricht, wie von angegeben`<integer>`. Der Index der Name-Wert-Komponente ist 0-basiert. Wenn der Wert `<integer>`, der durch das Argument Integer angegeben wird, größer ist als die Anzahl der Komponenten in der Liste, wird ein leeres Textobjekt zurückgegeben. Es folgt ein Beispiel: `http.req.cache_control.name(3).contains("some_text")`
Cache-Control header.IS_INVALID	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header nicht in der Anforderung oder Antwort vorhanden ist. Es folgt ein Beispiel: `http.req.cache_control.is_invalid`
`Cache-Control header.IS_PRIVATE`	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert Privat hat. Es folgt ein Beispiel: `http.req.cache_control.is_private`
Cache-Control header.IS_PUBLIC	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert Privat hat. Es folgt ein Beispiel: http.req.cache_control.is_public

HTTP-Header-Vorgang	Beschreibung
Cache-Control header.IS_NO_STORE	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert No-Store hat. Es folgt ein Beispiel: http.req.cache_control.is_no_store
Cache-Control header.IS_NO_CACHE	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert No-Cache hat. Es folgt ein Beispiel: http.req.cache_control.is_no_cache
Cache-Control header.IS_MAX_AGE	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert Max-Age hat. Es folgt ein Beispiel: http.req.cache_control.is_max_age
Cache-Control header.IS_MIN_FRESH	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert Min-Fresh hat. Es folgt ein Beispiel: http.req.cache_control.is_min_fresh
Cache-Control header.IS_MAX_STALE	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert Max-Stale hat. Es folgt ein Beispiel: http.req.cache_control.is_max_stale
Cache-Control header.IS_MUST_REVALIDATE	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert Must-Revalidate hat. Es folgt ein Beispiel: http.req.cache_control.is_must_revalidate
Cache-Control header.IS_NO_TRANSFORM	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert No-Transform hat. Es folgt ein Beispiel: http.req.cache_control.is_no_transform
Cache-Control header.IS_ONLY_IF_CACHED	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert Only-If-Cached aufweist. Es folgt ein Beispiel: http.req.cache_control.is_only_if_cached
Cache-Control header.IS_PROXY_REVALIDATE	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert Proxy-Revalidate aufweist. Es folgt ein Beispiel: http.req.cache_control.is_proxy_revalidate

HTTP-Header-Vorgang	Beschreibung
Cache-Control header.IS_S_MAXAGE	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header den Wert S-Maxage hat. Es folgt ein Beispiel: http.req.cache_control.is_s_maxage
Cache-Control header.IS_UNKNOWN	Gibt einen booleschen TRUE zurück, wenn der Cache-Control-Header einen unbekannten Typ hat. Es folgt ein Beispiel: http.req.cache_control.is_unknown
Cache-Control header.MAX_AGE	Gibt den Wert des Cache-Control-Headers Max-Age zurück. Wenn dieser Header nicht vorhanden ist oder ungültig ist, wird 0 zurückgegeben. Es folgt ein Beispiel: http.req.cache_control.max_age.le(3)
Cache-Control header.MAX_STALE	Gibt den Wert des Cache-Control-Headers Max-Stale zurück. Wenn dieser Header nicht vorhanden ist oder ungültig ist, wird 0 zurückgegeben. Es folgt ein Beispiel: http.req.cache_control.max_stale.le(3)
Cache-Control header.MIN_FRESH	Gibt den Wert des Cache-Control-Headers Min-Fresh zurück. Wenn dieser Header nicht vorhanden ist oder ungültig ist, wird 0 zurückgegeben. Es folgt ein Beispiel: http.req.cache_control.min_fresh.le(3)
Cache-Control header.S_MAXAGE	Gibt den Wert des Cache-Control-Headers S-Maxage zurück. Wenn dieser Header nicht vorhanden oder ungültig ist, wird 0 zurückgesendet. Es folgt ein Beispiel: http.req.cache_control.s_maxage.eq(2)

Ausdrücke zum Extrahieren von URLs

October 5, 2021

Sie können URLs und Teile von URLs extrahieren, z. B. den Hostnamen oder ein Segment des URL-Pfads. Der folgende Ausdruck identifiziert beispielsweise HTTP-Anforderungen für Bilddateien, indem

Bilddatei-Suffixe aus der URL extrahiert werden:

```
http.req.url.suffix.eq("jpeg")|| http.req.url.suffix.eq("gif")
```

Die meisten Ausdrücke für URLs arbeiten mit Text und werden unter Ausdruckspräfixe für Text in HTTP-Anfragen und Antwortenbeschrieben. In diesem Abschnitt wird die GET-Operation erläutert. Die GET-Operation extrahiert Text, wenn sie mit den folgenden Präfixen verwendet wird:

- HTTP.REQ.URL.PATH
- VPN.BASEURL.PATH
- VPN.CLIENTLESS_BASEURL.PATH

In der folgenden Tabelle werden Präfixe für HTTP-URLs beschrieben.

URL-Präfix	Beschreibung
HTTP.REQ.URL.PATH.GET (<n>)	Gibt einen Schrägstrich (/) getrennte Liste aus dem URL-Pfad zurück. Betrachten Sie beispielsweise die folgende URL:<`http://www.mycompany.com/dir1/dir2/dir3/index.html?a=1`>. Der folgende Ausdruck gibt dir1 von dieser URL zurück:<`http.req.url.path.get(1)`>. Der folgende Ausdruck gibt dir2 zurück: http.req.url.path.get (2)
HTTP.REQ.URL.PATH.GET_REVERSE (<n>)	Gibt einen Schrägstrich (/) getrennte Liste vom URL-Pfad zurück, beginnend am Ende des Pfades. Betrachten Sie beispielsweise die folgende URL:<`http://www.mycompany.com/dir1/dir2/dir3/index.html?a=1`>. Der folgende Ausdruck gibt index.html von dieser URL zurück:<`http.req.url.path.get_reverse(0)`>. Der folgende Ausdruck gibt dir3 zurück: http.req.url.path.get_reverse (1)

Ausdrücke für HTTP-Statuscodes und numerische HTTP-Nutzlastdaten außer Datumsangaben

October 5, 2021

In der folgenden Tabelle werden Präfixe für numerische Werte in anderen HTTP-Daten als Datumsangaben beschrieben.

Prefix	Beschreibung
HTTP.REQ.CONTENT_LENGTH	Gibt die Länge einer HTTP-Anforderung als Zahl zurück. Es folgt ein Beispiel: http.req.content_length < 500
HTTP.RES.CONTENT_LENGTH	Gibt die Länge der HTTP-Antwort als Zahl zurück. Es folgt ein Beispiel: http.res.content_length <= 1000
HTTP.RES.STATUS	Gibt den Antwortstatuscode zurück
HTTP.RES.IS_REDIRECT	Gibt einen booleschen TRUE zurück, wenn der Antwortcode einer Umleitung zugeordnet ist. Im Folgenden sind die Redirect-Antwortcodes: 300 (Multiple Choices), 301 (Permanent verschoben), 302 (Found), 303 (Siehe Andere), 305 (Proxy verwenden) und 307 (Temporäre Umleitung). Hinweis: Statuscode 304 gilt nicht als Umleitungs-HTTP-Antwortstatuscode. Statuscode 306 wird nicht verwendet.

SIP-Ausdrücke

October 5, 2021

Die Citrix ADC Advanced Richtlinienausdruckssprache enthält eine Reihe von Ausdrücken, die auf SIP-Verbindungen (Session Initiation Protocol) ausgeführt werden. Diese Ausdrücke sollen in Richtlinien für alle unterstützten Protokolle verwendet werden, die auf Anforderung/Antwortbasis ausgeführt werden. Diese Ausdrücke können für Content Switching, Ratenbegrenzung, Responder und Umschreibrichtlinien verwendet werden.

Bestimmte Einschränkungen gelten für SIP-Ausdrücke, die mit Responder-Richtlinien verwendet werden. Nur die Aktionen DROP, NOOP oder RESPONDWITH sind auf einem virtuellen SIP-Load Balancing Server zulässig. Responderrichtlinien können an einen virtuellen Lastausgleichsserver, einen globalen Überschreibungspunkt, einen globalen Standardbindungspunkt oder eine sip_udp-Richtlinienbezeichnung gebunden werden.

Das Header-Format, das vom SIP-Protokoll verwendet wird, ähnelt dem vom HTTP-Protokoll, so dass

viele der neuen Ausdrücke ähnlich wie ihre HTTP-Analoga aussehen und funktionieren. Jeder SIP-Header besteht aus einer Zeile, die die SIP-Methode, die URL und die Version enthält, gefolgt von einer Reihe von Name-Wert-Paaren, die wie HTTP-Header aussehen.

Es folgt ein Beispiel SIP-Header, die in den Ausdruckstabellen darunter verwiesen wird:

```
INVITE sip:16@www.sip.com:5060;transport=udp SIP/2.0
Record-Route: <sip:200.200.100.22;lr=on>
Via: SIP/2.0/UDP 200.200.100.22;branch=z9hG4bK444b.c8e103d1.0;rport
   =5060;
    received=10.102.84.18
Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;
    received=10.102.84.160
From: "12" <sip:12@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53
   cc0185
To: "16" <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185
Call-ID: 00127f54-ec850017-0e46f5b9-5ec149c2@10.102.84.180
Max-Forwards: 69CSeq: 101 INVITE
User-Agent: Cisco-CP7940G/8.0
Contact: <sip:12@10.102.84.180:5060;transport=udp>
Expires: 180
Accept: application/sdp
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE
Supported: replaces,join,norefersub
Content-Length: 277
Content-Type: application/sdp
Content-Disposition: session;handling=optiona
<!--NeedCopy-->
```

SIP-Referenztabellen

Die folgenden Tabellen enthalten Listen von Ausdrücken, die auf SIP-Headern ausgeführt werden. Die erste Tabelle enthält Ausdrücke, die für Anforderungsheader gelten. Die meisten antwortbasierten Ausdrücke sind fast identisch mit den entsprechenden anforderungsbasierten Ausdrücken. Um einen Antwortausdruck aus dem entsprechenden Anforderungsausdruck zu erstellen, ändern Sie die ersten beiden Abschnitte des Ausdrucks von SIP.REQ in SIP.RES und nehmen andere offensichtliche Anpassungen vor. Die zweite Tabelle enthält die Antwortausdrücke, die für Antworten eindeutig sind und keine Anforderungsäquivalente aufweisen. Sie können jedes Element in den folgenden Tabellen selbst als vollständiger Ausdruck verwenden, oder Sie können verschiedene Operatoren verwenden, um diese Ausdruckselemente mit anderen zu kombinieren, um komplexere Ausdrücke zu bilden.

SIP-Anforderungsausdrücke

Ausdruck	Beschreibung
SIP.REQ.METHOD	Arbeitet auf der Methode der SIP-Anforderung. Unterstützte SIP-Anforderungen sind ACK, BYE, CANCEL, INFO, INVITE, MESSAGE, NOTIFY, OPTIONS, PRACK, PUBLISH, REFER, REGISTER, SUBSCRIBE und UPDATE. Dieser Ausdruck ist eine Ableitung der Textklasse, so dass alle Vorgänge, die auf Text anwendbar sind, auf diese Methode anwendbar sind. Beispielsweise gibt dieser Ausdruck für eine SIP-Anforderung von INVITE sip:16@10.102.84.181:5060;transport=udp SIP/2.0 INVITE zurück.
SIP.REQ.URL	Funktioniert mit der SIP-Anforderungs-URL. Dieser Ausdruck ist eine Ableitung der Textklasse, so dass alle Vorgänge, die auf Text anwendbar sind, auf diese Methode anwendbar sind. Beispiel: Für eine SIP-Anforderung von INVITE sip:16@10.102.84.181:5060;transport=udp SIP/2.0 gibt dieser Ausdruck sip:16@10.102.84.181:5060;transport=udp zurück.
SIP.REQ.URL.PROTOCOL	Gibt das URL-Protokoll zurück. Beispiel: Für eine SIP-URL von sip:16@www.sip.com:5060;transport=udp gibt dieser Ausdruck sip zurück.
SIP.REQ.URL.HOSTNAME	Gibt den Hostname-Teil der SIP-URL zurück. Beispiel: Für eine SIP-URL von sip:16@www.sip.com:5060;transport=udp gibt dieser Ausdruck www.sip.com:5060 zurück.

Ausdruck	Beschreibung
SIP.REQ.URL.HOSTNAME.PORT	Gibt den Port-Teil des SIP-URL-Hostnamens zurück. Wenn kein Port angegeben wird, gibt dieser Ausdruck den Standard-SIP-Port 5060 zurück. Beispielsweise gibt dieser Ausdruck für den SIP-Hostnamen www.sip.com:5060 den Wert 5060 zurück.
SIP.REQ.URL.HOSTNAME.DOMAIN	Gibt den Domänennamenteil des SIP-URL-Hostnamens zurück. Wenn der Host eine IP-Adresse ist, gibt dieser Ausdruck ein falsches Ergebnis zurück. Beispiel: Für einen SIP-Hostnamen www.sip.com:5060 gibt dieser Ausdruck sip.com zurück. Bei einem SIP-Hostnamen 192.168.43. 15:5060 gibt dieser Ausdruck einen Fehler zurück.
SIP.REQ.URL.HOSTNAME.SERVER	Gibt den Serverteil des Hosts zurück. Beispiel: Für einen SIP-Hostnamen www.sip.com:5060 gibt dieser Ausdruck www zurück.
SIP.REQ.URL.USERNAME	Gibt den Benutzernamen zurück, der dem Zeichen @ vorausgeht. Beispielsweise gibt dieser Ausdruck für eine SIP-URL von sip: 16@www.sip.com:5060; transport=udp 16 zurück.
SIP.REQ.VERSION	Gibt die SIP-Versionsnummer in der Anforderung zurück. Beispiel: Für eine SIP-Anforderung von INVITE sip:16@10.102.84.181:5060;transport=udp SIP/2.0 gibt dieser Ausdruck SIP/2.0 zurück.
SIP.REQ.VERSION.MAJOR	Gibt die Hauptversionsnummer zurück (die Nummer links vom Punkt). Beispielsweise gibt dieser Ausdruck für eine SIP-Versionsnummer von SIP/2.0 2 zurück.
SIP.REQ.VERSION.MINOR	Gibt die Nebenversionsnummer zurück (die Zahl rechts vom Punkt). Beispielsweise gibt dieser Ausdruck für eine SIP-Versionsnummer von SIP/2.0 0 zurück.

Ausdruck	Beschreibung
SIP.REQ.CONTENT_LENGTH	Gibt den Inhalt des Content-Length-Headers zurück. Dieser Ausdruck ist eine Ableitung der Klasse thesip_header_t, so dass alle Operationen, die für SIP-Header verfügbar sind, verwendet werden können. Für einen SIP-Content-Length-Header von Content-Length: 277 gibt dieser Ausdruck beispielsweise 277 zurück.
SIP.REQ.TO	Gibt den Inhalt des To Headers zurück. Beispiel: Für einen SIP To Header von To: “16” <sip:16@sip_example.com>; tag=00127f54ec85a6d90cc14f45-53cc0185 gibt dieser Ausdruck “16” <sip:16@sip_example.com>; tag=00127f54ec85a6d90cc14f45-53cc0185 zurück.
SIP.REQ.TO.ADDRESS	Gibt den SIP-URI zurück, der im Objekt sip_url gefunden wird. Alle Vorgänge, die für SIP-URIs verfügbar sind, können verwendet werden. Beispiel: Für einen SIP To Header von To: “16” <sip:16@sip_example.com>; tag=00127f54ec85a6d90cc14f45-53cc0185 gibt dieser Ausdruck sip:16@sip_example.com zurück.
SIP.REQ.TO.DISPLAY_NAME	Gibt den Anzeigenamen Teil der To Header zurück. Beispiel: Für einen SIP To Header von To: “16” <sip:16@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185 gibt dieser Ausdruck 16 zurück.

Ausdruck	Beschreibung
SIP.REQ.TO.TAG	Gibt den Wert “tag” aus dem Namenspaar “tag” im TO Header zurück. Beispiel: Für einen SIP To Header von To: “16” <sip:16@sip_example.com>; tag=00127f54ec85a6d90cc14f45-53cc0185 gibt dieser Ausdruck 00127f54ec85a6d90cc14f45-53cc0185 zurück.
SIP.REQ.FROM	Gibt den Inhalt der From Header zurück. Beispiel: Für einen SIP From Header von From: “12” <sip:12@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185, gibt diese Ausdruck sip:12@sip_example.com zurück.
SIP.REQ.FROM.ADDRESS	Gibt den SIP-URI zurück, der im Objekt sip_url gefunden wird. Alle Vorgänge, die für SIP-URIs verfügbar sind, können verwendet werden. Beispiel: Für einen SIP From Header von From: “12” <sip:12@sip_example.com>;tag=00127f54ec85a6d90cc14f45-53cc0185, gibt diese Ausdruck sip:12@sip_example.com zurück.
SIP.REQ.FROM.DISPLAY_NAME	Gibt den Anzeigenamen Teil der To Header zurück. Beispiel: Für einen SIP From Header von From: “12” <sip:12@sip_example.com>; Tag = 00127f54ec85a6d90cc14f45-53cc0185 gibt dieser Ausdruck 12 zurück.
SIP.REQ.FROM.TAG	Gibt den “tag” -Wert aus dem “tag” Name/Wert-Paar im TO Header zurück. Für einen SIP-Fom-Header von From: “12”<sip:12@sip_example.com>; tag=00127f54ec85a6d90cc14f45-53cc0185 gibt dieser Ausdruck beispielsweise 00127f54ec85a6d90cc14f45-53cc0185 zurück.

Ausdruck	Beschreibung
SIP.REQ.VIA	Gibt den vollständigen Via Header zurück. Wenn mehrere Via Header in der Anfrage vorhanden sind, gibt die letzte Via Header zurück. Beispielsweise gibt dieser Ausdruck für die beiden Va-Header im Beispiel-SIP-Header Via zurück: SIP/2.0/UDP 10.102.84. 180:5060; Branch=Z9hg4bk03e76d0b; rport=5060; received=10.102.84.160.
SIP.REQ.VIA.SENTBY_ADDRESS	Gibt die Adresse zurück, die die Anforderung gesendet hat. Beispiel: Für den Via Header Via: SIP/2.0/UDP 10.102.84.180:5060; Branch=Z9hg4bk03e76d0b; rport=5060; received=10.102.84.160 gibt dieser Ausdruck 10.102.84.180 zurück.
SIP.REQ.VIA.SENTBY_PORT	Gibt den Port zurück, der die Anforderung gesendet hat. Beispiel: Für den Via Header Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re gibt dieser Ausdruck 5060 zurück.
SIP.REQ.VIA.RPORT	Gibt den Wert aus dem Rport-Name/Wert-Paar zurück. Beispiel: Für den Via Header Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re gibt dieser Ausdruck 5060 zurück.
SIP.REQ.VIA.BRANCH	Gibt den Wert aus dem Zweigname/Wert-Paar zurück. Beispiel: Für den Via Header Via: SIP/2.0/UDP 10.102.84.180:5060; Branch=Z9hg4bk03e76d0b; rport=5060; received=10.102.84.160 gibt dieser Ausdruck Z9hg4bk03e76d0b zurück.
SIP.REQ.VIA.RECEIVED	Gibt den Wert aus dem empfangenen Name/Wert-Paar zurück. Beispiel: Für den Via Header Via: SIP/2.0/UDP 10.102.84.180:5060; Branch=Z9hg4bk03e76d0b; rport=5060; received=10.102.84.160 gibt dieser Ausdruck 10.102.84.160 zurück.

Ausdruck	Beschreibung
SIP.REQ.CALLID	Gibt den Inhalt des Callid-Headers zurück. Dieser Ausdruck ist eine Ableitung der Klasse sip_header_t, so dass alle Operationen, die für SIP-Header verfügbar sind, verwendet werden können. Beispielsweise gibt dieser Ausdruck für einen SIP-Callid-Header der Call-ID: 00127f54-ec850017-0e46f5b9-5ec149c2@10.102.84.180 den Wert 00127f54-ec850017-0e46f5b9-5ec149c2@10.102.84.180 zurück.
SIP.REQ.CSEQ	Gibt die CSEQ-Nummer aus dem CSEQ als Ganzzahl zurück. Für einen SIP-CSEQ-Header von CSeQ: 101 INVITE gibt dieser Ausdruck beispielsweise 101 zurück.
SIP.REQ.HEADER(<header_name>)	Gibt den angegebenen SIP-Header zurück. <header_name>Ersetzen Sie für den Namen der gewünschten Kopfzeile. Um beispielsweise den SIP From Header zurückzugeben, geben Sie SIP.REQ.HEADER (“Von”) ein.

Ausdruck	Beschreibung
SIP.REQ.HEADER(<header_name>).INSTANCE(<line_number>)	Gibt die angegebene Instanz des angegebenen SIP-Headers zurück. Mehrere Instanzen desselben SIP-Headers können auftreten. Wenn Sie eine bestimmte Instanz eines solchen SIP-Headers wünschen (z. B. einen bestimmten Va-Header), können Sie diesen Header angeben, indem Sie eine Nummer als eingeben <line_number>. Header-Instanzen werden vom letzten (0) bis zum ersten zugeordnet. Mit anderen Worten, SIP.REQ.HEADER (“Via”) .INSTANCE (0) gibt die letzte Instanz des Via-Headers zurück, während SIP.REQ.HEADER (“Via”) .INSTANCE (1) die letzte Instanz mit Ausnahme des Va-Headers usw. Bei dem SIP-Header aus dem Beispiel SIP.REQ.HEADER(“Via”).INSTANCE(1) gibt es Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060 zurück.
SIP.REQ.HEADER(<header_name>).VALUE(<line_	Gibt den Inhalt der angegebenen Instanz des angegebenen SIP-Headers zurück. Die Verwendung ist fast die gleiche wie der vorherige Ausdruck. Beispiel: Wenn SIP-Header-Beispiel im vorherigen Tabelleneintrag verwendet wird, gibt SIP.REQ.HEADER (“Via”) .VALUE (1) SIP/2.0/UDP 10.102.84 zurück. 180:5060; Branch=Z9HG4BK03E76D0b; rport=5060.
SIP.REQ.HEADER(<header_name>).COUNT	Gibt die Anzahl der Instanzen eines bestimmten Headers als Ganzzahl zurück. Beispiel: Wenn SIP-Header-Beispiel oben verwendet wird, gibt SIP.REQ.HEADER (“Via”) .COUNT 2 zurück.

Ausdruck	Beschreibung
SIP.REQ.HEADER(<header_name>).EXISTS	Gibt einen booleschen Wert von true oder false zurück, abhängig davon, ob der angegebene Header existiert oder nicht. Beispiel: Wenn SIP-Header Beispiel oben verwendet wird, gibt SIP.REQ.HEADER (“Expires”) .EXISTS “true” zurück, während SIP.REQ.HEADER (“Caller-ID”).EXISTS “false” zurückgibt.
SIP.REQ.HEADER(<header_name>).LIST	Gibt die durch Kommas getrennte Parameterliste im angegebenen Header zurück. Wenn SIP.REQ.HEADER (“Zulassen”) verwendet wird, gibt SIP.REQ.HEADER (“Zulassen”) .LIST zurück: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,U Sie können die Zeichenfolge anhängen. GET (<list_item_number>), um ein bestimmtes Listenelement auszuwählen. Um beispielsweise das erste Element (ACK) aus der obigen Liste zu erhalten, geben Sie SIP.REQ.HEADER (“Zulassen”) .LIST.GET (0) ein. Um das zweite Element (BYE) zu extrahieren, geben Sie SIP.REQ.HEADER (“Allow”) .LIST.GET (1) ein. Hinweis: Wenn der angegebene Header eine Liste von Name/Wert-Paaren enthält, wird das gesamte Name/Wert-Paar zurückgegeben.

Ausdruck	Beschreibung
SIP.REQ.HEADER(<header_name>).TYPECAST_SI	Typumwandlung <header_name> an <in_header_name>. Jeder Text kann in die Klasse thesip_header_t geschrieben werden, nach der alle Header-basierten Operationen verwendet werden können. Nachdem Sie diesen Vorgang ausgeführt haben, können Sie alle Vorgänge anwenden, die mit verwendet werden können <in_header_name>. Der Ausdruck SIP.REQ.CONTENT_LENGTH.TYPECAST_SIP_HEADER_T enthält beispielsweise alle Instanzen des Content-Length-Headers. Nachdem Sie diesen Vorgang ausgeführt haben, können Sie alle Header-Operationen auf alle Instanzen des angegebenen Headers anwenden.
SIP.REQ.HEADER(<header_name>).CONTAINS(<string>)	Gibt boolean true zurück, wenn die angegebene Textzeichenfolge in einer beliebigen Instanz der angegebenen Kopfzeile vorhanden ist. Funktioniert auf allen Instanzen des angegebenen Headers. Header-Instanzen werden vom letzten (0) bis zum ersten zugeordnet.
SIP.REQ.HEADER(<header_name>).EQUALS_ANY	Gibt boolean true zurück, wenn ein Muster zugeordnet mit einem <patset> Inhalt in einer Instanz der angegebenen Header übereinstimmt. Funktioniert auf allen Instanzen des angegebenen Headers. Header-Instanzen werden vom letzten (0) bis zum ersten zugeordnet.
SIP.REQ.HEADER(<header_name>).CONTAINS_ANY(<patset>)	Gibt boolean true zurück, wenn ein Muster zugeordnet mit einem <patset> Inhalt in einer Instanz der angegebenen Kopfzeile übereinstimmt. Funktioniert auf allen Instanzen des angegebenen Headers. Header-Instanzen werden vom letzten (0) bis zum ersten zugeordnet.

Ausdruck	Beschreibung
SIP.REQ.HEADER(<header_name>).CONTAINS_IN	Gibt den Index des übereinstimmenden Musters zurück <patset>, wenn dieses Muster mit einem Inhalt in einer Instanz der angegebenen Kopfzeile übereinstimmt. Funktioniert auf allen Instanzen des angegebenen Headers. Header-Instanzen werden vom letzten (0) bis zum ersten zugeordnet.
SIP.REQ.HEADER(<header_name>).EQUALS_INDEX(<patset>)	Gibt den Index des übereinstimmenden Musters zurück <patset>, wenn dieses Muster mit einer Instanz der angegebenen Kopfzeile übereinstimmt. Funktioniert auf allen Instanzen des angegebenen Headers. Header-Instanzen werden vom letzten (0) bis zum ersten zugeordnet.
SIP.REQ.HEADER(<header_name>).SUBSTR(<stri	Wenn die angegebene Zeichenfolge in einer Instanz des angegebenen Headers vorhanden ist, gibt dieser Ausdruck diese Zeichenfolge zurück. Beispiel: für den SIP-Header Via: SIP/2.0/UDP 10.102.84. 180:5060; Branch=Z9hg4bk03e76d0b; rport=5060; received=10.102.84.160”, SIP.REQ.HEADER (“Via”) .SUBSTR (“rport=5060”) gibt “rport=5060”.sip.req.sip.req.header (“Via”) .SUBSTR (“rport=5061”) gibt einen leeren String zurück.
SIP.REQ.HEADER(<header_name>).AFTER_STR(<string>)	Wenn die angegebene Zeichenfolge in einer Instanz des angegebenen Headers vorhanden ist, gibt dieser Ausdruck die Zeichenfolge unmittelbar nach dieser Zeichenfolge zurück. Beispiel: Für den SIP-Header Via: SIP/2.0/UDP 10.102.84. 180:5060; Branch=Z9HG4BK03E76D0b; rport=5060; received=10.102.84.160 gibt der Ausdruck SIP.REQ.HEADER (“Via”) .AFTER_STR (“rport=”) 5060 zurück.

Ausdruck	Beschreibung
SIP.REQ.HEADER(<header_name>).REGEX_MATC	Gibt boolean true zurück, wenn der angegebene reguläre Ausdruck (regex) mit einer beliebigen Instanz des angegebenen Headers übereinstimmt. Sie müssen den regulären Ausdruck im folgenden Format angeben: re <delimiter> reguläre Ausdruck <same delimiter>. Der reguläre Ausdruck darf nicht größer als 1499 Zeichen sein. Sie muss der PCRE-Bibliothek für reguläre Ausdrücke entsprechen. Dokumentationhttp://www.pcre.org/pcre.txt zur Syntax für reguläre PCRE-Ausdrücke finden Sie unter. Die Manpage pcrepattern enthält auch nützliche Informationen zur Angabe von Mustern mithilfe von regulären PCRE-Ausdrücken. Die Syntax für reguläre Ausdrücke, die in diesem Ausdruck unterstützt wird, weist einige Unterschiede zu PCRE auf. Rückverweise sind nicht zulässig. Sie sollten rekursive reguläre Ausdrücke vermeiden; obwohl einige funktionieren, viele nicht. Der Punkt (.) -Metazeichen entspricht Zeilenumbrüchen. Unicode wird nicht unterstützt.SET_TEXT_MODE (IGNORECASE) überschreibt die (? i) interne Option im regulären Ausdruck angegeben.
SIP.REQ.HEADER(<header_name>).REGEX_SELECT(<regex>)	Wenn die angegebene Regex mit einem beliebigen Text in einer Instanz der angegebenen Kopfzeile übereinstimmt, gibt dieser Ausdruck den Text zurück. Zum Beispiel für den SIP-Header Via: SIP/2.0/UDP 10.102.84.180:5060; Branch=Z9HG4BK03E76D0b; rport=5060; empfangen=10.102.84.160, der Ausdruck SIP.REQ.HEADER (“Via”) .REGEX_SELECT (“erhalten =[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}”) gibt Received=10.102.84.160 zurück.

Ausdruck	Beschreibung
SIP.REQ.HEADER(<header_name>).AFTER_REGE	Wenn die angegebene Regex mit einem beliebigen Text in einer Instanz der angegebenen Kopfzeile übereinstimmt, gibt dieser Ausdruck die Zeichenfolge unmittelbar nach diesem Text zurück. Beispiel: Für den SIP-Header Via: SIP/2.0/UDP 10.102.84.180:5060;branch=z9hG4bK03e76d0b;rport=5060;re gibt der Ausdruck SIP.REQ.HEADER(“Via”).AFTER_REGEX(“received=”) den Wert 10.102.84.160 zurück.
SIP.REQ.HEADER(<header_name>).BEFORE_REGEX(<regex>)	Wenn die angegebene Regex mit einem beliebigen Text in einer Instanz der angegebenen Kopfzeile übereinstimmt, gibt dieser Ausdruck die Zeichenfolge unmittelbar vor diesem Text zurück. Beispielsweise für den SIP-Header Via: SIP/2.0/UDP 10.102.84.180:5060; Branch=Z9hg4bk03e76d0b; rport=5060; received=10.102.84.160, der Ausdruck SIP.REQ.HEADER (“Via”) .BEFORE_REGEX (“[0-9]{1,3}. [0-9]{ 1,3}. [0-9]{ 1,3}. [0-9]{ 1,3}”) gibt empfangen= zurück.
SIP.REQ.FULL_HEADER	Gibt den gesamten SIP-Header zurück, einschließlich des abschließenden CR/LF.
SIP.REQ.IS_VALID	Gibt boolean true zurück, wenn das Anforderungsformat gültig ist.
SIP.REQ.BODY(<length>)	Gibt den Anforderungskörper bis zur angegebenen Länge zurück. Wenn die angegebene Länge größer als die Länge des Anforderungskörpers ist, gibt dieser Ausdruck den gesamten Anforderungskörper zurück.
SIP.REQ.LB_VSERVER	Gibt den Namen des virtuellen Lastenausgleichsservers (LB vserver) zurück, der die aktuelle Anforderung bedient.

Ausdruck	Beschreibung
SIP.REQ.CS_VSERVER	Gibt den Namen des virtuellen Content Switching-Servers (CS vserver) zurück, der die aktuelle Anforderung bedient.

SIP-Antwortausdrücke

Ausdruck	Beschreibung
SIP.RES.STATUS	Gibt den SIP-Antwortstatuscode zurück. Wenn beispielsweise die erste Zeile der Antwort SIP/2.0 100 versucht ist, gibt dieser Ausdruck 100 zurück.
SIP.RES.STATUS_MSG	Gibt die SIP-Antwortstatusmeldung zurück. Wenn die erste Zeile der Antwort beispielsweise SIP/2.0 100 Versuchen lautet, gibt dieser Ausdruck Versuchen zurück.
SIP.RES.IS_REDIRECT	Gibt boolean true zurück, wenn der Antwortcode eine Umleitung ist.
SIP.RES.METHOD	Gibt die Antwortmethode zurück, die aus der Anforderungsmethodenzeichenfolge im CSEq-Header extrahiert wurde.

Operationen für HTTP-, HTML- und XML-Codierung und “sichere” Zeichen

December 7, 2021

Die folgenden Vorgänge arbeiten mit der Kodierung von HTML-Daten in einer Anforderung oder Antwort und XML-Daten in einem POST-Text.

- **<text>.HTML_XML_SAFE:**
  Wandelt Sonderzeichen wie in den folgenden Beispielen in ein sicheres XML-Format um:

  Eine nach links zeigende Winkelklammer (<) wird in < umgewandelt Eine nach rechts zeigende Winkelklammer (>)
  wird in > Ein kaufmännisches Und-Zeichen (&) umgewandelt wird
  in & Diese Operation schützt vor

Cross-Site-Scripting-Angriffen. Die maximale Länge des transformierten Textes beträgt 2048 Byte. Dies ist ein schreibgeschützter Vorgang.

Nach dem Anwenden der Transformation werden zusätzliche Operatoren, die Sie im Ausdruck angeben, auf den ausgewählten Text angewendet. Es folgt ein Beispiel:

http.req.url.query.html_xml_safe. contains(“myQueryString”)

- **<text>.HTTP_HEADER_SAFE:**
  Konvertiert alle neuen Zeilenzeichen (‘n’) im Eingabetext in ‘%0A’, damit die Eingabe sicher in HTTP-Headern verwendet werden kann.

  Diese Operation schützt vor Response-Splitting Angriffen.

  Die maximale Länge des transformierten Textes beträgt 2048 Byte. Dies ist ein schreibgeschützter Vorgang.

- **<text>.HTTP_URL_SAFE:**
  Konvertiert unsichere URL-Zeichen in ‘%xx’ Werte, wobei “xx” eine hexbasierte Darstellung des Eingabezeichens ist. Beispielsweise wird das kaufmännische Und-Zeichen (&) als %26 in der URL-sicheren Kodierung dargestellt. Die maximale Länge des transformierten Textes beträgt 2048 Byte. Dies ist ein schreibgeschützter Vorgang.

  Im Folgenden sind URL-sichere Zeichen. Alle anderen sind unsicher:

  - Alpha-numerische Zeichen: a-z, A-Z, 0-9
  - Asterix: *
  - kaufmännisches Und-Zeichen: &
  - AT-Zeichen: @
  - Doppelpunkt: :
  - Komma: ,
  - Dollar: $
  - Punkt: .
  - Gleich: =
  - Ausrufezeichen: !
  - Bindestrich: -
  - Klammer öffnen und schließen: (,)
  - Prozent: %
  - Plus: +
  - Semikolon: ;
  - Einzelnes Zitat: ‘
  - Schrägstrich: /
  - Fragezeichen: ?
  - Tilde: ~
  - Unterstrich: _

- **.MARK_SAFE:**<text>

  Markiert den Text als sicher, ohne irgendeine Art von Datentransformation anzuwenden.

- **<text>.SET_TEXT_MODE (URLENCODED|NOURLENCODED)**

  Transformiert alle %HH-Kodierung im Byte-Stream. Dieser Vorgang funktioniert mit Zeichen (nicht Bytes). Standardmäßig stellt ein einzelnes Byte ein Zeichen in der ASCII-Codierung dar. Wenn Sie jedoch den URLENCODED-Modus angeben, können drei Bytes ein Zeichen darstellen.

  Im folgenden Beispiel wählt ein PREFIX(3)-Vorgang die ersten 3 Zeichen in einem Ziel aus.

  ```
  http.req.url.hostname.prefix(3)
  ```

  Im folgenden Beispiel kann Citrix ADC bis zu 9 Bytes aus dem Ziel auswählen:

  ```
  http.req.url.hostname.set_text_mode(urlencoded).prefix(3)
  ```

- **<text>.SET_TEXT_MODE (PLUS_AS_SPACE|NO_PLUS_AS_SPACE):**

  Gibt an, wie das Pluszeichen (+) behandelt werden soll. Die Option PLUS_AS_SPACE ersetzt ein Pluszeichen durch Leerzeichen. Zum Beispiel wird der Text “Hallo+Welt” zu “hallo Welt. “ Die Option NO_PLUS_AS_SPACE lässt Pluszeichen wie sie sind.

- **<text>.SET_TEXT_MODE (BACKSLASH_ENCODED|NO_BACKSLASH_ENCODED):**

  Gibt an, ob eine umgekehrte Schrägstriche Decodierung für das Textobjekt durchgeführt wird, das von dargestellt wird <text>.

  Wenn BACKSLASH_ENCODED angegeben ist, führt der SET_TEXT_MODE Operator die folgenden Operationen für das Textobjekt aus:

  - Alle Vorkommen von “XXX” werden durch das Zeichen “Y” ersetzt (wobei XXX eine Zahl im Oktalsystem darstellt und Y das ASCII-Äquivalent von XXX darstellt). Der gültige Bereich der Oktalwerte für diesen Codierungstyp beträgt 0 bis 377. Zum Beispiel wird der codierte Text “http\72//” und http\072//” in beide dekodiert in <http://>, wobei der Doppelpunkt (:) das ASCII-Äquivalent des Oktalwerts “72” ist.
  - Alle Vorkommen von “xHH” werden durch das Zeichen “Y” ersetzt (HH steht für eine Zahl im Hexadezimalsystem und Y bezeichnet das ASCII-Äquivalent von HH. Zum Beispiel wird der codierte Text “http\x3a//” dekodiert in <http://>, wobei der Doppelpunkt (:) das ASCII-Äquivalent des hexadezimalen Wertes “3a” ist.
  - Alle Vorkommen von “UWWxx” werden durch die Zeichensequenz “YZ” ersetzt (wobei WW und XX zwei unterschiedliche hexadezimale Werte darstellen und Y und Z ihre ASCII-Äquivalente von WW bzw. XX darstellen. Zum Beispiel werden der codierte Text “http%u3a2f/” und “http%u003a//” dekodiert<http://>, wobei “3a” und “2f” zwei hexadezimale Werte sind und der Doppelpunkt (:) und der Schrägstrich (“/”) ihre ASCII-Äquivalente darstellen. jeweils.

- Alle Vorkommen von b, n, t, f und r werden durch die entsprechenden ASCII-Zeichen ersetzt.

Wenn NO_BACKSLASH_ENCODED angegeben ist, wird für das Textobjekt keine Rückwärtsdekodierung durchgeführt.

- **<text>.SET_TEXT_MODE(BAD_ENCODE_RAISE_UNDEF|NO_BAD_ENCODE_RAISE_UNDEF):**

  Führt die zugeordnete undefinierte Aktion aus, wenn entweder der URLENCODED oder der BACKSLASH_ENCODED Modus gesetzt ist und eine fehlerhafte Kodierung, die dem angegebenen Codierungsmodus entspricht, im Textobjekt gefunden wird, das von repräsentiert wird <text>.

  Wenn NO_BAD_ENCODE_RAISE_UNDEF angegeben ist, wird die zugeordnete undefinierte Aktion nicht ausgeführt, wenn eine fehlerhafte Kodierung im Textobjekt auftritt, das von repräsentiert wird <text>.

Ausdrücke für TCP-, UDP- und VLAN-Daten

October 5, 2021

TCP- und UDP-Daten haben die Form einer Zeichenfolge oder einer Zahl. Für Ausdruckspräfixe, die Zeichenfolgenwerte für TCP- und UDP-Daten zurückgeben, können Sie beliebige textbasierte Vorgänge anwenden. Weitere Informationen finden Sie unter Erweiterte Richtlinienausdrücke: Text auswerten.

Für Ausdruckspräfixe, die numerischen Wert zurückgeben, z. B. einen Quellport, können Sie eine arithmetische Operation anwenden. Weitere Informationen finden Sie unter Grundlegende Operationen für Ausdruckspräfixe und Zusammengesetzte Operationen für Zahlen.

In der folgenden Tabelle werden Präfixe beschrieben, die TCP- und UDP-Daten extrahieren.

GET Operation	Beschreibung
`CLIENT.TCP.PAYLOAD(<integer>)`	Gibt TCP-Nutzlastdaten als Zeichenfolge zurück, beginnend mit dem ersten Zeichen in der Nutzlast und fortgesetzt für die Anzahl der Zeichen im`<integer>` Argument. Sie können jede textbasierte Operation auf dieses Präfix anwenden.
CLIENT.TCP.SRCPORT	Gibt die ID des Quellports des aktuellen Pakets als Zahl zurück.
CLIENT.TCP.DSTPORT	Gibt die ID des Zielports des aktuellen Pakets als Zahl zurück.

GET Operation	Beschreibung
CLIENT.TCP.OPTIONS	Gibt die vom Client festgelegten TCP-Optionen zurück. Beispiele für TCP-Optionen sind Maximum Segment Size (MSS), Fensterskalierung, Selective Acknowledgements (SACK) und Zeitstempel Option. Die Operatoren COUNT, TYPE(<type>), and TYPE_NAME(<m>) können mit diesem Präfix verwendet werden. Die vom Server festgelegten TCP-Optionen finden Sie im Präfix SERVER.TCP.OPTIONS.
CLIENT.TCP.OPTIONS.COUNT	Gibt die Anzahl der TCP-Optionen zurück, die der Client festgelegt hat.
CLIENT.TCP.OPTIONS.TYPE (<type>)	Gibt den Wert der TCP-Option zurück, deren Typ (oder Optionstyp) als Argument angegeben wird. Der Wert wird als Bytezeichenfolge im Big Endian-Format (oder Netzwerk-Byte-Reihenfolge) zurückgegeben. Parameter: type - Typwert
CLIENT.TCP.OPTIONS.TYPE_NAME (<m>)	Gibt den Wert der TCP-Option zurück, deren Enumerierungskonstante als Argument angegeben wird. Die Enumerierungskonstanten, die Sie als Argument übergeben können, sind REPEATER, TIMESTAMP, SACK_PERMITTED, WINDOW und MAXSEG. Um anstelle dieser Enumerierungskonstanten den TCP-Optionstyp anzugeben, verwenden Sie CLIENT.TCP.OPTIONS.TYPE(<type>). Für andere TCP-Optionen müssen Sie CLIENT.TCP.OPTIONS.TYPE(<type>) verwenden. Parameter: m - TCP-Optionsaufzählungskonstante
CLIENT.TCP.REPEATER_OPTION.EXISTS	Gibt einen booleschen TRUE zurück, wenn Repeater TCP-Optionen vorhanden sind.
CLIENT.TCP.REPEATER_OPTION.IP	Gibt die IPv4-Adresse des Zweistellenrepeaters aus den Repeater-TCP-Optionen zurück.

GET Operation	Beschreibung
CLIENT.TCP.REPEATER_OPTION.MAC	Gibt die MAC-Adresse des Zweistellenrepeaters aus den Repeater-TCP-Optionen zurück.
CLIENT.UDP.DNS.DOMAIN	Gibt den DNS-Domänennamen zurück.
CLIENT.UDP.DNS.DOMAIN.EQ(“<hostname>”)	Gibt einen booleschen TRUE zurück, wenn der Domänenname mit dem <hostname> Argument übereinstimmt. Bei dem Vergleich wird die Groß- und Kleinschreibung nicht berücksichtigt. Es folgt ein Beispiel: client.udp.dns.domain.eq (“www.mycompany.com”)
CLIENT.UDP.DNS.IS_AAAAREC	Gibt einen booleschen TRUE zurück, wenn der Datensatztyp AAAA ist. Diese Datensatztypen geben eine IPv6-Adresse in Forward-Lookups an.
CLIENT.UDP.DNS.IS_ANYREC	Gibt einen booleschen TRUE zurück, wenn er einen Datensatztyp hat.
CLIENT.UDP.DNS.IS_AREC	Gibt einen booleschen TRUE zurück, wenn der Datensatz Typ A ist. Geben Sie die Hostadresse ein.
CLIENT.UDP.DNS.IS_CNAMEREC	Gibt einen booleschen TRUE zurück, wenn der Datensatz vom Typ CNAME ist. In Systemen, die mehrere Namen verwenden, um eine Ressource zu identifizieren, gibt es einen kanonischen Namen und eine Anzahl von Aliasen. Der CNAME gibt den kanonischen Namen an.
CLIENT.UDP.DNS.IS_MXREC	Gibt einen booleschen TRUE zurück, wenn der Datensatz vom Typ MX (Mail Exchanger) ist. Dieser DNS-Eintrag beschreibt eine Priorität und einen Hostnamen. Die MX-Einträge für denselben Domänennamen geben die E-Mail-Server in der Domäne und die Priorität für jeden Server an.

GET Operation	Beschreibung
CLIENT.UDP.DNS.IS_NSREC	Gibt einen booleschen TRUE zurück, wenn der Datensatz vom Typ NS ist. Dies ist ein Namenserver-Datensatz, der einen Hostnamen mit einem zugeordneten A-Datensatz enthält. Dies ermöglicht das Suchen des Domänennamens, der dem NS-Eintrag zugeordnet ist.
CLIENT.UDP.DNS.IS_PTRREC	Gibt einen booleschen TRUE zurück, wenn der Datensatz vom Typ PTR ist. Dies ist ein Domänennamenzeiger und wird häufig verwendet, um einen Domänennamen mit einer IPv4-Adresse zu verknüpfen.
CLIENT.UDP.DNS.IS_SOAREC	Gibt einen booleschen TRUE zurück, wenn der Datensatz vom Typ SOA ist. Das ist ein Anfang der Autoritätsakte.
CLIENT.UDP.DNS.IS_SRVREC	Gibt einen booleschen TRUE zurück, wenn der Datensatz vom Typ SRV ist. Dies ist eine allgemeinere Version des MX-Datensatzes.
CLIENT.UDP.DSTPORT	Gibt die numerische ID des UDP-Zielports des aktuellen Pakets zurück.
CLIENT.UDP.SRCPORT	Gibt die numerische ID des UDP-Quellports des aktuellen Pakets zurück.
CLIENT.UDP.RADIUS	Gibt RADIUS-Daten für das aktuelle Paket zurück.
CLIENT.UDP.RADIUS.ATTR_TYPE (<type>)	Gibt den Wert für den als Argument angegebenen Attributtyp zurück.
CLIENT.UDP.RADIUS.USERNAME	Gibt den RADIUS-Benutzernamen zurück.
CLIENT.TCP.MSS	Gibt die maximale Segmentgröße (MSS) für die aktuelle Verbindung als Zahl zurück.
CLIENT.VLAN.ID	Gibt die numerische ID des VLAN zurück, über das das aktuelle Paket den Citrix ADC eingegeben hat.
SERVER.TCP.DSTPORT	Gibt die numerische ID des Zielports des aktuellen Pakets zurück.

GET Operation	Beschreibung
SERVER.TCP.SRCPORT	Gibt die numerische ID des Quellports des aktuellen Pakets zurück.
SERVER.TCP.OPTIONS	Gibt die vom Server festgelegten TCP-Optionen zurück. Beispiele für TCP-Optionen sind Maximum Segment Size (MSS), Fensterskalierung, Selective Acknowledgements (SACK) und Zeitstempel Option. Die Operatoren COUNT, TYPE(<type>), and TYPE_NAME(<m>) können mit diesem Präfix verwendet werden. Die vom Client festgelegten TCP-Optionen finden Sie im Präfix CLIENT.TCP.OPTIONS.
SERVER.TCP.OPTIONS.COUNT	Gibt die Anzahl der TCP-Optionen zurück, die der Server festgelegt hat.
SERVER.TCP.OPTIONS.TYPE (<type>)	Gibt den Wert der TCP-Option zurück, deren Typ (oder Optionstyp) als Argument angegeben wird. Der Wert wird als Bytezeichenfolge im Big Endian-Format (oder Netzwerk-Byte-Reihenfolge) zurückgegeben. Parameter: type - Typwert
SERVER.TCP.OPTIONS.TYPE_NAME (<m>)	Gibt den Wert der TCP-Option zurück, deren Enumerierungskonstante als Argument angegeben wird. Die Enumerierungskonstanten, die Sie als Argument übergeben können, sind REPEATER, TIMESTAMP, SACK_PERMITTED, WINDOW und MAXSEG. Um anstelle dieser Enumerierungskonstanten den TCP-Optionstyp anzugeben, verwenden Sie CLIENT.TCP.OPTIONS.TYPE(<type>). Für andere TCP-Optionen müssen Sie CLIENT.TCP.OPTIONS.TYPE(<type>) verwenden. Parameter: m - TCP-Optionsaufzählungskonstante

GET Operation	Beschreibung
SERVER.VLAN	Funktioniert auf dem VLAN, über das das aktuelle Paket in den Citrix ADC eingegeben wurde.
SERVER.VLAN.ID	Gibt die numerische ID des VLAN zurück, über das das aktuelle Paket den Citrix ADC eingegeben hat.

Ausdrücke zum Auswerten einer DNS-Nachricht und Identifizieren des Trägerprotokolls

October 5, 2021

Sie können DNS-Anforderungen und -Antworten mithilfe von Ausdrücken auswerten, die mit DNS.REQ bzw. DNS.RES beginnen. Sie können auch das Transportschichtprotokoll identifizieren, das zum Senden der DNS-Nachrichten verwendet wird.

Die folgenden Funktionen geben den Inhalt einer DNS-Abfrage zurück.

Funktion	Beschreibung
DNS.REQ.QUESTION.DOMAIN	Gibt den Domänennamen (den Wert des QNAME-Felds) im Frageabschnitt der DNS-Abfrage zurück. Der Domänenname wird als Textzeichenfolge zurückgegeben, die an EQ (), NE () und alle anderen Funktionen, die mit Text arbeiten, übergeben werden kann.

Funktion	Beschreibung
DNS.REQ.QUESTION.TYPE	Gibt den Abfragetyp (den Wert des QTYPE-Felds) in der DNS-Abfrage zurück. Das Feld gibt den Typ des Ressourceneintrags an (z. B. A, NS oder CNAME), für den der Namenserver abgefragt wird. Der zurückgegebene Wert kann mit den Funktionen EQ () und NE () mit einem der folgenden Werte verglichen werden: A, AAAA, NS, SRV, PTR, CNAME, SOA, MX und ANY. Hinweis: Sie können nur die Funktionen EQ () und NE () mit der Funktion TYPE verwenden. Beispiel: DNS.REQ.QUESTION.TYPE.EQ(MX)

Die folgenden Funktionen geben den Inhalt einer DNS-Antwort zurück.

Funktion	Beschreibung
DNS.RES.HEADER.RCODE	Gibt den Antwortcode (den Wert des RCODE-Felds) im Header-Abschnitt der DNS-Antwort zurück. Sie können nur die Funktionen EQ () und NE () mit der Funktion RCODE verwenden. Im Folgenden sind die möglichen Werte: NOERROR, FORMERR, SERVFAIL, NXDOMAIN, NOTIMP und REFUSED.
DNS.RES.QUESTION.DOMAIN	Gibt den Domänennamen (den Wert des QNAME-Felds) im Frageabschnitt der DNS-Antwort zurück. Der Domänenname wird als Textzeichenfolge zurückgegeben, die an EQ (), NE () und alle anderen Funktionen, die mit Text arbeiten, übergeben werden kann.

Funktion	Beschreibung
DNS.RES.QUESTION.TYPE	Gibt den Abfragetyp (den Wert des QTYPE-Felds) im Frageabschnitt der DNS-Antwort zurück. Das Feld gibt den Typ des Ressourceneintrags an (z. B. A, NS oder CNAME), der in der Antwort enthalten ist. Der zurückgegebene Wert kann mit den Funktionen EQ () und NE () mit einem der folgenden Werte verglichen werden: A, AAAA, NS, SRV, PTR, CNAME, SOA, MX und ANY. Sie können nur die Funktionen EQ () und NE () mit der Funktion TYPE verwenden. Beispiel: DNS.RES.QUESTION.TYPE.EQ(SOA)

Die folgenden Funktionen geben den Namen des Transportschichtprotokolls zurück.

Funktion	Beschreibung
DNS.REQ.TRANSPORT	Gibt den Namen des Transportschichtprotokolls zurück, das zum Senden der DNS-Abfrage verwendet wurde. Mögliche zurückgegebene Werte sind TCP und UDP. Mit der TRANSPORT können Sie nur die Funktionen EQ () und NE () verwenden. Beispiel: DNS.REQ.TRANSPORT.EQ (TCP)
DNS.RES.TRANSPORT	Gibt den Namen des Transportschichtprotokolls zurück, das für die DNS-Antwort verwendet wurde. Mögliche zurückgegebene Werte sind TCP und UDP. Mit der TRANSPORT können Sie nur die Funktionen EQ () und NE () verwenden. Beispiel: DNS.RES.TRANSPORT.EQ (TCP)

XPath- und HTML-, XML- oder JSON-Ausdrücke

October 5, 2021

Die erweiterte Richtlinieninfrastruktur unterstützt Ausdrücke zum Auswerten und Abrufen von Daten aus HTML-, XML- und JavaScript-Object Notation (JSON) -Dateien. Auf diese Weise können Sie bestimmte Knoten in einem HTML-, XML- oder JSON-Dokument suchen, feststellen, ob ein Knoten in der Datei vorhanden ist, Knoten in XML-Kontexten suchen (z. B. Knoten mit bestimmten Eltern oder ein bestimmtes Attribut mit einem bestimmten Wert) und den Inhalt dieser Knoten zurückgeben. Darüber hinaus können Sie XPath-Ausdrücke in Rewrite-Ausdrücken verwenden.

Die Implementierung des erweiterten Richtlinienausdrucks für XPath umfasst ein Präfix für erweiterte Richtlinienausdrücke (z. B. “HTTP.REQ.BODY”), das HTML- oder XML-Text bezeichnet, und den XPATH-Operator, der den XPath-Ausdruck als Argument verwendet.

HTML-Dateien sind eine weitgehend freie Sammlung von Tags und Textelementen. Sie können den XPATH_HTML-Operator verwenden, der einen XPath-Ausdruck als Argument verwendet, um HTML-Dateien zu verarbeiten. JSON-Dateien sind entweder eine Sammlung von Namen/Wert-Paaren oder eine geordnete Liste von Werten. Sie können den XPATH_JSON-Operator verwenden, der einen XPath-Ausdruck als Argument verwendet, um JSON-Dateien zu verarbeiten.

- **<text>.XPATH(xpathex):**

  Verwenden Sie eine XML-Datei und geben Sie einen booleschen Wert zurück.

  Der folgende Ausdruck gibt beispielsweise einen booleschen TRUE zurück, wenn ein Knoten namens “creator” innerhalb der ersten 1000 Byte der XML-Datei unter dem Knoten “Book” existiert.

  ```
  HTTP.REQ.BODY(1000).XPATH(xp%boolean(//Book/creator)%)
  ```

  Parameter:

  xpathex - XPath Boolescher Ausdruck

- **<text>.XPATH(xpathex):**

  Arbeiten Sie auf einer XML-Datei und geben Sie einen Wert des Datentyps “double. “

  Der folgende Ausdruck konvertiert beispielsweise die Zeichenfolge “36” (ein Preiswert) in einen Wert vom Datentyp “double”, wenn sich die Zeichenfolge in den ersten 1000 Byte der XML-Datei befindet:

  ```
  HTTP.REQ.BODY(1000).XPATH(xp%number(/Book/price)%)
  ```

  Parameter:

  xpathex - XPath - numerischer Ausdruck

Beispiel:

```
1       <Book>
```



```
    <creator>
        <Person>
            <name>Milton</name>
        </Person>
    </creator>
    <title>Paradise Lost</title>
    </Book>
<!--NeedCopy-->
```

- **<text>.XPATH(xpathex):**

  Arbeiten Sie an einer XML-Datei und geben Sie einen Knotensatz oder eine Zeichenfolge zurück. Knotensätze werden mit der Standard-XPath-String-Konvertierungsroutine in entsprechende Strings konvertiert.

  Der folgende Ausdruck wählt beispielsweise alle Knoten aus, die von "/book/creator" (einem Knotensatz) in den ersten 1000 Bytes des Körpers eingeschlossen sind:

  ```
  HTTP.REQ.BODY(1000).XPATH(xp%/Book/creator%)
  ```

  Parameter:

  xpathex - XPath-Ausdruck

- **<text>.XPATH_HTML(xpathex)**

  Arbeiten Sie an einer HTML-Datei und geben Sie einen Textwert zurück.

  Der folgende Ausdruck funktioniert beispielsweise für eine HTML-Datei und gibt den Text zurück, der in `<title\></title\>` Tags eingeschlossen ist, wenn das title-HTML-Element in den ersten 1000 Bytes gefunden wird:

  ```
  HTTP.REQ.BODY(1000).XPATH_HTML(xp%/html/head/title%)
  ```

  Parameter:

  xpathex - XPath-Textausdruck

- **<text>.XPATH_HTML_WITH_MARKUP(xpathex)**

  Arbeiten Sie an einer HTML-Datei und geben Sie eine Zeichenfolge zurück, die den gesamten ausgewählten Teil des Dokuments enthält, einschließlich Markups, z. B. das Einschließen der umschließenden Element-Tags.

  Der folgende Ausdruck wirkt auf die HTML-Datei und wählt den gesamten Inhalt innerhalb des <\title>-Tags, einschließlich Markup.

  ```
  HTTP.REQ.BODY(1000).XPATH_HTML_WITH_MARKUP( xp%/html/head/title%)
  ```

  Der durch den Ausdruck ausgewählte Teil des HTML-Body wird zur weiteren Verarbeitung markiert.

Parameter:

xpathex - XPath-Ausdruck

- **<text>.XPATH_JSON(xpathex)**

  Arbeiten Sie an einer JSON-Datei und geben Sie einen booleschen Wert zurück.

  Betrachten Sie beispielsweise die folgende JSON-Datei:

  {”Buch”: {”creator”: {”person”: {”name” :’<name>’}}, ”title” :’<title>’ } }

  Der folgende Ausdruck arbeitet für die JSON-Datei und gibt einen booleschen TRUE zurück, wenn die JSON-Datei einen Knoten namens “creator” enthält, dessen übergeordneter Knoten “Book” in den ersten 1000 Bytes lautet:

  ```
  HTTP.REQ.BODY(1000).XPATH_JSON(xp%boolean(/Book/creator)%)
  ```

  Parameter:

  xpathex - XPath Boolescher Ausdruck

- **<text>.XPATH_JSON(xpathex)**

  Arbeiten Sie auf einer JSON-Datei und geben Sie einen Wert vom Datentyp “double. “

  Betrachten Sie beispielsweise die folgende JSON-Datei:

  {”Buch”: {”creator”: {”person”: {”name” :’<name>’}}, ”title” :’<title>’, ”preis” :”36”}}

  Der folgende Ausdruck arbeitet für die JSON-Datei und konvertiert die Zeichenfolge “36” in einen Wert vom Datentyp “double”, wenn die Zeichenfolge in den ersten 1000 Bytes der JSON-Datei vorhanden ist.

  ```
  HTTP.REQ.BODY(1000).XPATH_JSON(xp%number(/Book/price)%)
  ```

  Parameter:

  xpathex - XPath - numerischer Ausdruck

- **<text>.XPATH_JSON(xpathex)**

  Arbeiten Sie an einer JSON-Datei und geben Sie einen Knotensatz oder eine Zeichenfolge zurück. Knotensätze werden mit der Standard-XPath-String-Konvertierungsroutine in entsprechende Strings konvertiert.

  Betrachten Sie beispielsweise die folgende JSON-Datei:

  {”Buch”: {”creator”: {”person”: {”name” :’<name>’}}, ”title” :’<title>’ } }

  Der folgende Ausdruck wählt alle Knoten aus, die in den ersten 1000 Bytes des Hauptteils der JSON-Datei von ”/Book” (einem Knotensatz) eingeschlossen sind, und gibt den entsprechenden String-Wert zurück, der ist”<name><title>”:


```
HTTP.REQ.BODY(1000).XPATH_JSON(xp%/Book%)
```

Parameter:

xpathex - XPath-Ausdruck

- **<text>XPATH_JSON_WITH_MARKUP (xpathex)**

  Verwenden Sie eine XML-Datei, und geben Sie eine Zeichenfolge zurück, die den gesamten Teil des Dokuments für den Ergebnisknoten enthält, einschließlich Markups, z. B. das Einschließen der umschließenden Element-Tags.

  Betrachten Sie beispielsweise die folgende JSON-Datei:

  {”Buch”: {”creator”: {”person”: {”name” :’<name>’}}, ”title” :’<title>’ } }

  Der folgende Ausdruck arbeitet auf der JSON-Datei und wählt alle Knoten aus, die von “/book/creator” in den ersten 1000 Bytes des Körpers eingeschlossen sind, also “creator: {person: {name: <name> ‘}}. “

  ```
  HTTP.REQ.BODY(1000).XPATH_JSON_WITH_MARKUP(xp%/Book/creator%)
  ```

  Der Teil des JSON-Body, der durch den Ausdruck ausgewählt wird, wird zur weiteren Verarbeitung markiert.

  Parameter:

  xpathex - XPath-Ausdruck

- **<text>XPATH_WITH_MARKUP (xpathex):**

  Verwenden Sie eine XML-Datei, und geben Sie eine Zeichenfolge zurück, die den gesamten Teil des Dokuments für den Ergebnisknoten enthält, einschließlich Markups, z. B. das Einschließen der umschließenden Element-Tags.

  Der folgende Ausdruck arbeitet beispielsweise mit einer XML-Datei und wählt alle Knoten aus, die von “/book/creator” in den ersten 1000 Byte des Hauptteils eingeschlossen sind.

  ```
  HTTP.REQ.BODY(1000).XPATH_WITH_MARKUP(xp%/Book/creator%)
  ```

  Der Teil des JSON-Body, der durch den Ausdruck ausgewählt wird, wird zur weiteren Verarbeitung markiert.

  Parameter:

  xpathex - XPath-Ausdruck

XML-Nutzlasten verschlüsseln und entschlüsseln

October 5, 2021

Sie können die Funktionen XML_ENCRYPT () und XML_DECRYPT () in erweiterten Richtlinienausdrücken verwenden, um XML-Daten zu verschlüsseln bzw. zu entschlüsseln. Diese Funktionen entsprechen dem W3C XML Encryption Standard, der unter http://www.w3.org/TR/2001/PR-xmldsig-core-20010820/ definiert ist. XML_ENCRYPT () und XML_DECRYPT () unterstützen eine Teilmenge der XML-Verschlüsselungsspezifikation. In der Teilmenge verwendet die Datenverschlüsselung eine Massenverschlüsselungsmethode (RC4, DES3, AES128, AES192 oder AES256), und ein öffentlicher RSA-Schlüssel wird zum Verschlüsseln des Bulk-Chiffrierschlüssels verwendet.

Hinweis: Wenn Sie Text in einer Nutzlast verschlüsseln und entschlüsseln möchten, müssen Sie die Funktionen ENCRYPT und DECRYPT verwenden. Weitere Informationen zu diesen Funktionen finden Sie unter Verschlüsseln und Entschlüsseln von Text.

Die Funktionen XML_ENCRYPT() und XML_DECRYPT() sind nicht abhängig vom Verschlüsselungs- und Entschlüsselungsdienst, der von den Befehlen ENCRYPT und DECRYPT für Text verwendet wird. Die Verschlüsselungsmethode wird explizit als Argument für die Funktion XML_ENCRYPT() angegeben. Die Funktion `XML_DECRYPT()` erhält die Informationen über die angegebene Verschlüsselungsmethode aus dem Element `<xenc:EncryptedData>`. Im Folgenden finden Sie Synopsen der XML-Verschlüsselungs- und Entschlüsselungsfunktionen:

- Element `XML_ENCRYPT(<certKeyName>, <method> [, <flags>])**. Returns an< xenc:EncryptedData>`, das den verschlüsselten Eingabetext und den Verschlüsselungsschlüssel enthält, der selbst mithilfe von RSA verschlüsselt wird.
- `XML_DECRYPT(<certKeyName>)`. Gibt den entschlüsselten Text aus dem Eingabeelement `<xenc:EncryptedData>` zurück, das die Verschlüsselungsmethode und den RSA-verschlüsselten Schlüssel enthält.

Hinweis: Das Element `<xenc:EncryptedData>` ist in der W3C XML Encryption Spezifikation definiert.

Im Folgenden sind Beschreibungen der Argumente:

- **CertKeyName:** Wählt ein X.509-Zertifikat mit einem öffentlichen RSA-Schlüssel für XML_ENCRYPT () oder einen privaten RSA-Schlüssel für XML_DECRYPT (). Der Zertifikatschlüssel muss zuvor durch einen `add ssl certKey` Befehl erstellt worden sein.
- **Methode:** Gibt an, welche Verschlüsselungsmethode für die Verschlüsselung der XML-Daten verwendet werden soll. Mögliche Werte: RC4, DES3, AES128, AES192, AES256.
- **flags:** Eine Bitmaske, die die folgenden optionalen Schlüsselinformationen (`<ds:KeyInfo>`) angibt, die in das `<xenc:EncryptedData>` Element aufgenommen werden sollen, das von generiert wird `XML_ENCRYPT()`:
  - **1** - Fügen Sie ein KeyName-Element mit dem CertKeyName. Das Element ist `<ds:KeyName >`.
  - **2** - Fügen Sie ein KeyValue-Element mit dem öffentlichen RSA-Schlüssel aus dem Zertifikat ein. Das Element ist `<ds:KeyValue>`.

- **4** - Fügen Sie ein X509IssuerSerial-Element mit der Zertifikatsseriennummer und dem Aussteller-DN ein. Das Element ist <ds:X509IssuserSerial>.
- **8** - Fügen Sie ein X509SubjectName-Element mit dem Zertifikat-Subjekt-DN ein. Das Element ist <ds:X509SubjectName>.
- **16** - Fügen Sie ein X509Certificate-Element in das gesamte Zertifikat ein. Das Element ist <ds:X509Certificate>.

Verwenden der Funktionen XML_ENCRYPT() und XML_DECRYPT() in Ausdrücken

Die XML-Verschlüsselungsfunktion verwendet SSL-Zertifikatschlüsselpaare, um X.509-Zertifikate (mit öffentlichen RSA-Schlüsseln) für die Schlüsselverschlüsselung und private RSA-Schlüssel für die Schlüsselentschlüsselung bereitzustellen. Bevor Sie die Funktion XML_ENCRYPT() in einem Ausdruck verwenden, müssen Sie daher ein SSL-Zertifikatschlüsselpaar erstellen. Mit dem folgenden Befehl wird das SSL-Zertifikatschlüsselpaar my-certkey mit dem X.509-Zertifikat my-cert.pem und der privaten Schlüsseldatei my-key.pem erstellt.

```
add ssl certKey my-certkey -cert my-cert.pem -key my-key.pem -passcrypt
kxPeMRYnitY=
```

Die folgenden CLI-Befehle erstellen Umschreibaktionen und Richtlinien zum Verschlüsseln und Entschlüsseln von XML-Inhalten.

```
1  add rewrite action my-xml-encrypt-action replace "HTTP.RES.BODY(10000).
       XPATH_WITH_MARKUP(xp%/%)" "HTTP.RES.BODY(10000).XPATH_WITH_MARKUP(xp
       %/%).XML_ENCRYPT("my-certkey", AES256, 31)" -bypassSafetyCheck YES
2
3  add rewrite action my-xml-decrypt-action replace "HTTP.REQ.BODY(10000).
       XPATH_WITH_MARKUP(xp%//xenc:EncryptedData%)" "HTTP.REQ.BODY(10000).
       XPATH_WITH_MARKUP(xp%//xenc:EncryptedData%).XML_DECRYPT("my-certkey"
       )" -bypassSafetyCheck YES
4
5  add rewrite policy my-xml-encrypt-policy "HTTP.REQ.URL.CONTAINS("xml-
       encrypt")" my-xml-encrypt-action
6
7  add rewrite policy my-xml-decrypt-policy "HTTP.REQ.BODY(10000).XPATH(xp
       %boolean(//xenc:EncryptedData)%)" my-xml-decrypt-action
8
9  bind rewrite global my-xml-encrypt-policy 30
10
11 bind rewrite global my-xml-decrypt-policy 30
12 <!--NeedCopy-->
```


Im obigen Beispiel verschlüsselt die Rewrite-Aktion my-xml-encrypt-action das gesamte XML-Dokument (XPATH_WITH_MARKUP (xp%/%)) in der Anforderung mit der AES-256-Massenverschlüsselungsmethod und des öffentlichen RSA-Schlüssels von my-certkey zum Verschlüsseln des Massenverschlüsselungsschlüssels. Die Aktion ersetzt das Dokument durch ein<xenc:EncryptedData> Element, das die verschlüsselten Daten und einen verschlüsselten Schlüssel enthält. Die Flags, die durch 31 dargestellt werden, enthalten alle optionalen<ds:KeyInfo> Elemente.

Die Aktion my-xml-decrypt-action entschlüsselt das erste<xenc:EncryptedData> Element in der Antwort (XPATH_WITH_MARKUP (XP%//XENC:EncryptedData%)). Dies erfordert das vorherige Hinzufügen des xenc XML-Namespace mithilfe des folgenden CLI-Befehls:

```
add ns xmlnamespace xenc http://www.w3.org/2001/04/xmlenc##
```

Die Aktion my-xml-decrypt-action verwendet den privaten RSA-Schlüssel in my-certkey, um den verschlüsselten Schlüssel zu entschlüsseln und verwendet dann die im Element angegebene Massenverschlüsselungsmethode, um den verschlüsselten Inhalt zu entschlüsseln. Schließlich ersetzt die Aktion das verschlüsselte Datenelement durch den entschlüsselten Inhalt.

Die Rewrite-Richtlinie my-xml-encrypt-policy wendet my-xml-encrypt-action auf Anfragen für URLs an, die xml-encrypt enthalten. Die Aktion verschlüsselt die gesamte Antwort eines auf der Citrix ADC Appliance konfigurierten Dienstes.

Die Rewrite-Richtlinie my-xml-decrypt-policy wendet my-xml-decrypt-action auf Anforderungen an, die ein<xenc:EncryptedData> Element enthalten ((XPATH (XP%//XENC:EncryptedData%) gibt eine nicht leere Zeichenfolge zurück). Die Aktion entschlüsselt die verschlüsselten Daten in Anforderungen, die für einen Dienst gebunden sind, der auf der Citrix ADC Appliance konfiguriert ist.

Erweiterte Richtlinienausdrücke: SSL analysieren

October 5, 2021

Es gibt erweiterte Richtlinienausdrücke, um SSL-Zertifikate und SSL-Client-Hallo Nachrichten zu analysieren.

SSL-Zertifikate analysieren

Sie können erweiterte Richtlinienausdrücke verwenden, um X.509 Secure Sockets Layer (SSL) -Clientzertifikate auszuwerten. Ein Clientzertifikat ist ein elektronisches Dokument, mit dem die Identität eines Benutzers authentifiziert werden kann. Ein Clientzertifikat enthält (mindestens) Versionsinformationen, eine Seriennummer, eine Signaturalgorithmus-ID, einen Ausstellernamen, einen Gültigkeitszeitraum, einen Betreff (Benutzername), einen öffentlichen Schlüssel und Signaturen.

Sie können sowohl SSL-Verbindungen als auch Daten in Clientzertifikaten untersuchen. Beispielsweise können Sie SSL-Anforderungen senden, die Low-Strength Chiffre verwenden, an eine bestimmte Lastenausgleichsfarm. Der folgende Befehl ist ein Beispiel für eine Content Switching-Richtlinie, die die Verschlüsselungsstärke in einer Anforderung analysiert und die Verschlüsselungsstärken von kleiner oder gleich 40 abgleicht:

```
1 add cs policy p1 -rule "client.ssl.cipher_bits.le(40)"
2 <!--NeedCopy-->
```

Als weiteres Beispiel können Sie eine Richtlinie konfigurieren, die bestimmt, ob eine Anforderung ein Clientzertifikat enthält:

```
1 add cs policy p2 -rule "client.ssl.client_cert exists"
2 <!--NeedCopy-->
```

Sie können auch eine Richtlinie konfigurieren, die bestimmte Informationen in einem Clientzertifikat untersucht. Die folgende Richtlinie überprüft beispielsweise, ob das Zertifikat einen oder mehrere Tage vor Ablauf hat:

```
1 add cs policy p2 -rule "client.ssl.client_cert exists && client.ssl.
     client_cert.days_to_expire.ge(1)"
2 <!--NeedCopy-->
```

> **Hinweis:**
>
> Informationen zum Analysieren von Datums und Uhrzeiten in einem Zertifikat finden Sie unter Format von Datums und Zeiten in einem Ausdruck und Ausdrücke für SSL-Zertifikatdaten.

Präfixe für textbasierte SSL- und Zertifikatsdaten

In der folgenden Tabelle werden Ausdruckspräfixe beschrieben, die textbasierte Elemente in SSL-Transaktionen und Clientzertifikaten identifizieren.

Tabelle 1. Präfixe, die Text- oder boolesche Werte für SSL- und Clientzertifikatdaten zurückgeben

Prefix	Beschreibung
CLIENT.SSL.CLIENT_CERT	Gibt das SSL-Clientzertifikat in der aktuellen SSL-Transaktion zurück.

Prefix	Beschreibung
CLIENT.SSL.CLIENT_CERT.TO_PEM	Gibt das SSL-Clientzertifikat im Binärformat zurück.
CLIENT.SSL.CIPHER_EXPORTABLE	Gibt einen booleschen TRUE zurück, wenn die kryptografische SSL-Verschlüsselung exportierbar ist.
CLIENT.SSL.CIPHER_NAME	Gibt den Namen der SSL-Cipher zurück, wenn sie von einer SSL-Verbindung aufgerufen wird, und eine NULL-Zeichenfolge, wenn sie von einer Nicht-SSL-Verbindung aufgerufen wird.
CLIENT.SSL.IS_SSL	Gibt einen booleschen TRUE zurück, wenn die aktuelle Verbindung SSL-basiert ist.

Präfixe für numerische Daten in SSL-Zertifikaten

In der folgenden Tabelle werden Präfixe beschrieben, die numerische Daten außer Datumsangaben in SSL-Zertifikaten auswerten. Diese Präfixe können mit den Operationen verwendet werden, die unter Grundlegende Operationen für Ausdruckspräfixe und zusammengesetzte Operationen für Zahlenbeschrieben sind.

Tabelle 2. Präfixe, die numerische Daten außer Datumsangaben in SSL-Zertifikaten auswerten

Prefix	Beschreibung
CLIENT.SSL.CLIENT_CERT.DAYS_TO_EXPIRE	Gibt die Anzahl der Tage zurück, in denen das Zertifikat gültig ist, oder gibt -1 für abgelaufene Zertifikate zurück.
CLIENT.SSL.CLIENT_CERT.PK_SIZE	Gibt die Größe des öffentlichen Schlüssels zurück, der im Zertifikat verwendet wird.
CLIENT.SSL.CLIENT_CERT.VERSION	Gibt die Versionsnummer des Zertifikats zurück. Wenn die Verbindung nicht SSL-basiert ist, gibt Null (0) zurück.
CLIENT.SSL.CIPHER_BITS	Gibt die Anzahl der Bits im kryptografischen Schlüssel zurück. Gibt 0 zurück, wenn die Verbindung nicht SSL-basiert ist.

Prefix	Beschreibung
CLIENT.SSL.VERSION	Gibt eine Zahl zurück, die die SSL-Protokollversion darstellt: 0. Die Transaktion ist nicht SSL-basiert.; 0x002. Die Transaktion lautet SSLv2.; 0x300. Die Transaktion lautet SSLv3.; 0x301. Die Transaktion ist TLSv1.; 0x302. Die Transaktion lautet TLS 1.1.; 0x303. Die Transaktion ist TLS 1.2; 0x304. Die Transaktion ist TLS 1.3.

> **Hinweis:**
>
> Informationen zu Ausdrücken im Zusammenhang mit Ablaufdatum in einem Zertifikat finden Sie unter Ausdrücke für SSL-Zertifikatdaten.

Ausdrücke für SSL-Zertifikate

Sie können SSL-Zertifikate analysieren, indem Sie Ausdrücke konfigurieren, die das folgende Präfix verwenden:

CLIENT.SSL.CLIENT_CERT

In diesem Abschnitt werden die Ausdrücke beschrieben, die Sie für Zertifikate konfigurieren können, ausgenommen Ausdrücke, die den Zertifikatablauf untersuchen. Zeitbasierte Vorgänge werden unter Erweiterte Richtlinienausdrücke: Arbeiten mit Datumsangaben, Zeiten und Zahlenbeschrieben.

In der folgenden Tabelle werden Vorgänge beschrieben, die Sie für das Präfix CLIENT.SSL.CLIENT_CERT angeben können.

Tabelle 3. Vorgänge, die mit dem Präfix CLIENT.SSL.CLIENT_CERT angegeben werden können

SSL-Zertifikatvorgang	Beschreibung
`<certificate>.EXISTS`	Gibt einen booleschen TRUE zurück, wenn der Client über ein SSL-Zertifikat verfügt.

SSL-Zertifikatvorgang	Beschreibung
`<certificate>.ISSUER`	Gibt den Distinguished Name (DN) des Ausstellers im Zertifikat als Name-Wert-Liste zurück. Ein Gleichheitszeichen (“=”) ist das Trennzeichen für den Namen und den Wert, und der Schrägstrich (“/”) ist das Trennzeichen, das die Name-Wert-Paare trennt. Es folgt ein Beispiel für den zurückgegebenen DN: `/C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@mycompany.com`
`<certificate>.ISSUER.IGNORE_EMPTY_ELEMENTS`	Gibt den Aussteller zurück und ignoriert die leeren Elemente in einer Name-Wert-Liste. Betrachten Sie beispielsweise Folgendes: Cert-Issuer: /c=in/st=kar//l=bangelore //o=mycompany/ou=sales/ /emailAddress=myuserid@mycompany.com. Die folgende Rewrite-Aktion gibt basierend auf der vorhergehenden Emittentendefinition eine Anzahl von 6 zurück: `sh rewrite action insert_ssl_header Name: insert_ssl Operation: insert_http_header Target:Cert-Issuer Value:CLIENT.SSL.CLIENT_CERT.ISSUER.COUNT`. Wenn Sie jedoch den Wert in den folgenden ändern, ist die zurückgegebene Anzahl 9: `CLIENT.SSL.CLIENT_CERT.ISSUER.IGNORE_EMPTY_ELEMENTS.COUNT`

Parse SSL client hello

Sie können die SSL-Client-Hallo Nachricht analysieren, indem Sie Ausdrücke konfigurieren, die das folgende Präfix verwenden:

Prefix	Beschreibung
CLIENT.SSL.CLIENT_HELLO.CIPHERS.HAS_HEXC(	Entspricht dem im Ausdruck angegebenen Hex-Code mit den Hex-Codes der Chiffre Suites, die in der Client-Hallo Nachricht empfangen wurden.
CLIENT.SSL.CLIENT_HELLO.CLIENT_VERSION	Version, die in der Client-Hello Nachrichtenkopfzeile empfangen wurde.
CLIENT.SSL.CLIENT_HELLO.IS_RENEGOTIATE	Gibt true zurück, wenn ein Client oder Server eine Sitzungsneuverhandlung initiiert.
CLIENT.SSL.CLIENT_HELLO.IS_REUSE	Gibt true zurück, wenn die Appliance die SSL-Sitzung basierend auf der in der Client-hallo-Nachricht empfangenen Sitzungs-ID, die nicht Null ist, wiederverwendet.
CLIENT.SSL.CLIENT_HELLO.IS_SCSV	Gibt true zurück, wenn Signaling Cipher Suite Value (SCSV) Funktion in der Client-Hallo Nachricht angekündigt wird. Der Hex-Code für Fallback SCSV ist 0x5600.
CLIENT.SSL.CLIENT_HELLO.IS_SESSION_TICKET	Gibt true zurück, wenn die Sitzungsticketerweiterung ungleich Null in der Client-hallo-Nachricht angekündigt wird.
CLIENT.SSL.CLIENT_HELLO.LENGTH	Empfangene Länge in der Client-Hello Nachrichtenkopfzeile.
CLIENT.SSL.CLIENT_HELLO.SNI	Gibt den Servernamen zurück, der in der Servernamen-Erweiterung der Clienthallo empfangen wurde.
CLIENT.SSL.CLIENT_HELLO.ALPN.HAS_NEXTPRC	Gibt true zurück, wenn das in der Clienthallo empfangene Anwendungsprotokoll in der ALPN-Erweiterung mit dem Protokoll übereinstimmt, das im Ausdruck angegeben ist.

Diese Ausdrücke können am Bindpunkt CLIENTHELLO_REQ verwendet werden. Weitere Informationen finden Sie unter Bindung von SSL-Richtlinien.

Erweiterte Richtlinienausdrücke: IP- und MAC-Adressen, Durchsatz, VLAN-IDs

October 5, 2021

Sie können Präfixe für erweiterte Richtlinienausdrücke verwenden, die IPv4- und IPv6-Adressen, MAC-Adressen, IP-Subnetze, nützliche Client- und Serverdaten zurückgeben, z. B. die Durchsatzraten an den Schnittstellenports (Rx, Tx und RxTX) und die IDs der VLANs, über die Pakete empfangen werden. Anschließend können Sie verschiedene Operatoren verwenden, um die Daten auszuwerten, die von diesen Ausdruckspräfixen zurückgegeben werden.

Ausdrücke für IP-Adressen und IP-Subnetze

Sie können erweiterte Richtlinienausdrücke verwenden, um Adressen und Subnetze im IPv4-Format (Internet Protocol Version 4) oder IPv6 (Internet Protocol Version 6) auszuwerten. Ausdruckspräfixe für IPv6-Adressen und Subnetze enthalten IPv6 im Präfix. Ausdruckspräfixe für IPv4-Adressen und Subnetze enthalten IP im Präfix. Es folgt ein Beispiel für einen Ausdruck, der angibt, ob eine Anforderung aus einem bestimmten IPv4-Subnetz stammt.

```
client.ip.src.in_subnet(147.1.0.0/16)
<!--NeedCopy-->
```

Im Folgenden finden Sie zwei Beispiele für Rewrite-Richtlinien, die das Subnetz untersuchen, aus dem das Paket empfangen wird, und eine Rewrite-Aktion für den Host-Header ausführen. Wenn diese beiden Richtlinien konfiguriert sind, hängt die durchgeführte Umschreibaktion vom Subnetz in der Anforderung ab. Diese beiden Richtlinien bewerten IP-Adressen, die im IPv4-Adressformat sind.

```
- add rewrite action URL1-rewrite-action replace "http.req.header("Host
   ")" ""www.mycompany1.com""
- add rewrite policy URL1-rewrite-policy "http.req.header("Host").
   contains("www.test1.com") && client.ip.src.in_subnet(147.1.0.0/16)"
   URL1-rewrite-action
- add rewrite action URL2-rewrite-action replace "http.req.header("Host
   ")" ""www.mycompany2.com""
- add rewrite policy URL2-rewrite-policy "http.req.header("Host").
   contains("www.test2.com") && client.ip.src.in_subnet(10.202.0.0/16)"
    URL2-rewrite-action
<!--NeedCopy-->
```


> **Hinweis:**
>
> Die vorangegangenen Beispiele sind Befehle, die Sie an der Citrix ADC Befehlszeilenschnittstelle (CLI) eingeben. Daher muss jedem Anführungszeichen ein umgekehrter Schrägstrich (\) vorangestellt werden. Weitere Informationen finden Sie unter Konfigurieren von erweiterten Richtlinienausdrücken in einer Richtlinie. “

Präfixe für IPV4-Adressen und IP-Subnetze

In der folgenden Tabelle werden Präfixe beschrieben, die IPv4-Adressen und Subnetze sowie Segmente von IPv4-Adressen zurückgeben. Sie können numerische Operatoren und Operatoren verwenden, die für IPv4-Adressen spezifisch sind. Weitere Informationen zu numerischen Operationen finden Sie unter “Grundoperationen für Ausdruckspräfixe” und “Zusammengesetzte Operationen für Zahlen. “

Tabelle 1. Präfixe, die IP- und MAC-Adressen auswerten

Prefix	Beschreibung
CLIENT.IP.SRC	Gibt die Quell-IP des aktuellen Pakets als IP-Adresse oder als Zahl zurück.
CLIENT.IP.DST	Gibt die Ziel-IP des aktuellen Pakets als IP-Adresse oder als Zahl zurück.
SERVER.IP.SRC	Gibt die Quell-IP des aktuellen Pakets als IP-Adresse oder als Zahl zurück.
SERVER.IP.DST	Gibt die Ziel-IP des aktuellen Pakets als IP-Adresse oder als Zahl zurück.

Operationen für IPV4-Adressen

In der Tabelle Präfix für IPV4-Operationen werden die Operatoren beschrieben, die mit Präfixen verwendet werden können, die eine IPv4-Adresse zurückgeben.

Informationen zu IPv6-Ausdrücken

Das IPv6-Adressformat ermöglicht mehr Flexibilität als das ältere IPv4-Format. IPv6-Adressen haben das hexadezimale Format (RFC 2373). In den folgenden Beispielen ist Beispiel 1 eine IPv6-Adresse, Beispiel 2 eine URL, die die IPv6-Adresse enthält, und Beispiel 3 enthält die IPv6-Adresse und eine Portnummer.

Beispiel 1:


```
9901:0ab1:22a2:88a3:3333:4a4b:5555:6666
<!--NeedCopy-->
```

Beispiel 2:

```
http://[9901:0ab1:22a2:88a3:3333:4a4b:5555:6666]/
<!--NeedCopy-->
```

Beispiel 3:

```
https://[9901:0ab1:22a2:88a3:3333:4a4b:5555:6666]:8080/
<!--NeedCopy-->
```

In Beispiel 3 trennen die Klammern die IP-Adresse von der Portnummer (8080).

Beachten Sie, dass Sie den Operator '+' nur verwenden können, um IPv6-Ausdrücke mit anderen Ausdrücken zu kombinieren. Die Ausgabe ist eine Verkettung der Zeichenfolgenwerte, die von den einzelnen Ausdrücken zurückgegeben werden. Sie können keinen anderen arithmetischen Operator mit einem IPv6-Ausdruck verwenden. Die folgende Syntax ist ein Beispiel:

```
client.ipv6.src + server.ip.dst
<!--NeedCopy-->
```

Wenn beispielsweise die Clientquell-IPv6-Adresse lautet`ABCD:1234::ABCD`und die Serverzieladresse IPv4 lautet`10.100.10.100`, wird der vorhergehende Ausdruck zurückgegeben"`ABCD:1234::ABCD10.100.10.100`".

Beachten Sie, dass die Citrix ADC Appliance ein IPv6-Paket empfängt, eine temporäre IPv4-Adresse aus einem nicht verwendeten IPv4-Adressbereich zuweist und die Quelladresse des Pakets in diese temporäre Adresse ändert. Zur Reaktionszeit wird die Quelladresse des ausgehenden Pakets durch die ursprüngliche IPv6-Adresse ersetzt.

> **Hinweis:**
>
> Sie können einen IPv6-Ausdruck mit einem beliebigen anderen Ausdruck kombinieren, außer einem Ausdruck, der ein boolesches Ergebnis erzeugt.

Ausdruckspräfixe für IPv6-Adressen

Die IPv6-Adressen, die von den Ausdruckspräfixen in der folgenden Tabelle zurückgegeben werden, können als Textdaten behandelt werden. Beispielsweise gibt das Präfix client.ipv6.dst die Ziel-IPv6-Adresse als Zeichenfolge zurück, die als Text ausgewertet werden kann.

In der folgenden Tabelle werden Ausdruckspräfixe beschrieben, die eine IPv6-Adresse zurückgeben.

Tabelle 3. IPv6-Ausdruckspräfixe, die Text zurückgeben

Prefix	Beschreibung
CLIENT.IPV6	Arbeitet auf der IPv6-Adresse mit dem aktuellen Paket.
CLIENT.IPV6.DST	Gibt die IPv6-Adresse im Zielfeld des IP-Headers zurück.
CLIENT.IPV6.SRC	Gibt die IPv6-Adresse im Quellfeld des IP-Headers zurück. Im Folgenden sind Beispiele: `client.ipv6.src.in_subnet (2007::2008/64)` `client.ipv6.src.get1.le(2008)`
SERVER.IPV6	Arbeitet auf der IPv6-Adresse mit dem aktuellen Paket.
SERVER.IPV6.DST	Gibt die IPv6-Adresse im Zielfeld des IP-Headers zurück.
SERVER.IPV6.SRC	Gibt die IPv6-Adresse im Quellfeld des IP-Headers zurück. Im Folgenden sind Beispiele: `server.ipv6.src.in_subnet (2007::2008/64)` `server.ipv6.src.get1.le(2008)`

Operationen für IPv6-Präfixe

In der folgenden Tabelle werden die Operatoren beschrieben, die mit Präfixen verwendet werden können, die eine IPv6-Adresse zurückgeben:

Tabelle 4. Vorgänge, die IPv6-Adressen auswerten

IPv6-Betrieb	Beschreibung
<ipv6>.EQ(<IPv6_address>	Gibt einen booleschen TRUE zurück, wenn der Wert der IP-Adresse mit dem Argument <IPv6_address> identisch ist. Es folgt ein Beispiel: client.ipv6.dst.eq(ABCD:1234::ABCD)
<ipv6>.GET1. . .GET8	Gibt ein Segment einer IPv6-Adresse als Zahl zurück. Die folgenden Beispielausdrücke rufen Segmente aus der IPv6-Adresse 1000:1001:CD10:0000:0000:89AB:4567:CDEF: client.ipv6.dst.get5 extracts 0000 ab. Dies ist der fünfte Satz von Bits in der Adresse. client.ipv6.dst.get6 extracts 89AB. client.ipv6.dst.get7 extracts 4567. Sie können numerische Operationen für diese Segmente ausführen. Beachten Sie, dass Sie beim Abrufen einer vollständigen IPv6-Adresse keine numerischen Vorgänge ausführen können. Dies liegt daran, dass Ausdrücke, die eine vollständige IPv6-Adresse zurückgeben, z. B. CLIENT.IPV6.SRC, die Adresse im Textformat zurückgeben.
<ipv6>.IN_SUBNET(<subnet>)	Gibt einen booleschen TRUE zurück, wenn sich der IPv6-Adresswert im durch das Argument <subnet> angegebenen Subnetz befindet. Es folgt ein Beispiel: client.ipv6.dst.eq(1000:1001:CD10 :0000:0000:89AB:4567:CDEF/60)
<ipv6>.IS_IPV4	Gibt einen booleschen TRUE zurück, wenn dies ein IPv4-Client ist, und gibt einen booleschen FALSE zurück, wenn dies nicht der Fall ist.
<ipv6>.SUBNET(<n>)	Gibt die IPv6-Adresse zurück, nachdem die als Argument angegebene Subnetzmaske angewendet wurde. Die Subnetzmaske kann Werte zwischen 0 und 128 annehmen. Beispiel: CLIENT.IPV6.SRC.SUBNET(24)

Ausdrücke für MAC-Adressen

Eine MAC-Adresse besteht aus durch Doppelpunkte getrennten Hexadezimalwerten im Format ##: ##: ##: ##: ##, wobei jedes # entweder eine Zahl von 0 bis 9 oder einen Buchstaben von A bis F darstellt. Standard-Syntaxausdruckpräfixe und -operatoren sind für die Auswertung von Quell- und Ziel-MAC-Adressen verfügbar.

Präfixe für MAC-Adressen

In der folgenden Tabelle werden Präfixe beschrieben, die MAC-Adressen zurückgeben.

Tabelle 5. Präfixe, die MAC-Adressen auswerten

Prefix	Beschreibung
`client.ether.dstmac`	Gibt die MAC-Adresse im Zielfeld des Ethernet-Headers zurück.
`client.ether.srcmac`	Gibt die MAC-Adresse im Quellfeld des Ethernet-Headers zurück.

Operationen für MAC-Adressen

In der folgenden Tabelle werden die Operatoren beschrieben, die mit Präfixen verwendet werden können, die eine MAC-Adresse zurückgeben.

Tabelle 6. Operationen auf MAC-Adressen

Prefix	Beschreibung
`<mac address>.EQ(<address>)`	Gibt einen booleschen TRUE zurück, wenn der MAC-Adresswert mit dem Argument `<address>` übereinstimmt.
`<mac address>.GET1. . .GET4`	Gibt einen numerischen Wert zurück, der aus dem Segment der MAC-Adresse extrahiert wird, die in der GET-Operation angegeben ist. Wenn die MAC-Adresse beispielsweise 12:34:56:78:9a:bc ist, gibt Folgendes 34 zurück: `client.ether.dstmac.get2`

Ausdrücke für numerische Client- und Serverdaten

In der folgenden Tabelle werden Präfixe für die Arbeit mit numerischen Client- und Serverdaten beschrieben, einschließlich Durchsatz, Portnummern und VLAN-IDs.

Tabelle 7. Präfixe, die numerische Client- und Serverdaten auswerten

Prefix	Beschreibung
client.interface.rxthroughput	Gibt eine ganze Zahl zurück, die den rohen empfangenen Datenverkehrsdurchsatz in Kilobyte pro Sekunde (KBps) für die letzten sieben Sekunden darstellt.
client.interface.txthroughput	Gibt eine ganze Zahl zurück, die den rohen übertragenen Datenverkehr Durchsatz in KBps für die letzten sieben Sekunden darstellt.
client.interface.rxtxthroughput	Gibt eine ganze Zahl zurück, die den rohen empfangenen und übertragenen Datenverkehr in KBps für die letzten sieben Sekunden darstellt.
server.interface.rxthroughput	Gibt eine Ganzzahl zurück, die den rohen empfangenen Datenverkehr in KBps für die letzten sieben Sekunden darstellt.
server.interface.txthroughput	Gibt eine ganze Zahl zurück, die den rohen übertragenen Datenverkehr Durchsatz in KBps für die letzten sieben Sekunden darstellt.
server.interface.rxtxthroughput	Gibt eine ganze Zahl zurück, die den rohen empfangenen und übertragenen Datenverkehr in KBps für die letzten sieben Sekunden darstellt.
server.vlan.id	Gibt eine numerische ID des VLAN zurück, über das das aktuelle Paket den Citrix ADC eingegeben hat.
client.vlan.id	Gibt eine numerische ID für das VLAN zurück, über das das aktuelle Paket den Citrix ADC eingegeben hat.

Erweiterte Richtlinienausdrücke: Stream Analytics Funktionen

October 5, 2021

Stream Analytics-Ausdrücke beginnen mit dem <identifier_name> Präfix ANALYTICS.STREAM (). In der folgenden Liste werden die Funktionen beschrieben, die mit diesem Präfix verwendet werden können.

- **COLLECT_STATS**

  Sammeln Sie statistische Daten aus den Anforderungen, die anhand der Richtlinie ausgewertet werden, und erstellen Sie für jede Anforderung einen Datensatz.

- **REQUESTS**

  Gibt die Anzahl der Anforderungen zurück, die für die angegebene Datensatzgruppierung vorhanden sind. Der zurückgegebene Wert ist vom Typ long ohne Vorzeichen.

- **BANDWIDTH**

  Gibt die Bandbreitenstatistik für die angegebene Datensatzgruppierung zurück. Der zurückgegebene Wert ist vom Typ long ohne Vorzeichen.

- **RESPTIME**

  Gibt die Antwortzeitstatistik für die angegebene Datensatzgruppierung zurück. Der zurückgegebene Wert ist vom Typ long ohne Vorzeichen.

- **CONNECTIONS**

  Gibt die Anzahl der gleichzeitigen Verbindungen zurück, die für die angegebene Datensatzgruppierung vorhanden sind. Der zurückgegebene Wert ist vom Typ long ohne Vorzeichen.

- **IS_TOP(n)**

  Gibt einen booleschen TRUE zurück, wenn der statistische Wert für die angegebene Datensatzgruppierung einer der obersten n Gruppen ist. Andernfalls geben Sie einen booleschen FALSE zurück.

- **CHECK_LIMIT**

  Gibt einen booleschen TRUE zurück, wenn die Statistik für die angegebene Datensatzgruppierung das vorkonfigurierte Limit erreicht hat. Andernfalls geben Sie einen booleschen FALSE zurück.

Erweiterte Richtlinienausdrücke: DataStream

October 5, 2021

Die Richtlinieninfrastruktur der Citrix ADC Appliance enthält Ausdrücke, die Sie zum Auswerten und Verarbeiten des Datenverkehrs des Datenbankservers verwenden können, wenn die Appliance zwischen einer Farm von Anwendungsservern und den zugehörigen Datenbankservern bereitgestellt wird.

Dieses Artikel enthält die folgenden Abschnitte:

- Ausdrücke für das MySQL Protokoll
- Ausdrücke zum Auswerten von Microsoft SQL Server-Verbindungen

Ausdrücke für das MySQL Protokoll

Die folgenden Ausdrücke bewerten den Datenverkehr, der mit MySQL Datenbankservern verbunden ist. Sie können die anforderungsbasierten Ausdrücke (Ausdrücke, die mit MYSQL.CLIENT und MYSQL.REQ beginnen) in Richtlinien verwenden, um Anforderungswechselentscheidungen am Bindungspunkt des virtuellen Content Switching-Servers zu treffen und die antwortbasierten Ausdrücke (Ausdrücke, die mit MYSQL.RES beginnen), um Serverantworten an Benutzer auszuwerten. konfigurierte Integritätsüberwachungen.

- **MYSQL.CLIENT.** Funktioniert mit den Client-Eigenschaften einer MySQL Verbindung.
- **MYSQL.CLIENT.CAPABILITIES.** Gibt den Satz von Flags zurück, die der Client im Capabilities-Feld des Handshake-Initialisierungspakets während der Authentifizierung festgelegt hat. Beispiele für die gesetzten Flags sind CLIENT_FOUND_ROWS, CLIENT_COMPRESS und CLIENT_SSL.
- **MYSQL.CLIENT.CHAR_SET.** Gibt die Enumerierungskonstante zurück, die dem Zeichensatz zugewiesen ist, den der Client verwendet. Die Operatoren EQ(<m>) und NE(<m>), die boolesche Werte zurückgeben, um das Ergebnis eines Vergleichs anzugeben, werden mit diesem Präfix verwendet. Im Folgenden sind die Zeichensatzaufzählungskonstanten:
  - LATIN2_CZECH_CS
  - DEC8_SWEDISH_CI
  - CP850_GENERAL_CI
  - GREEK_GENERAL_CI
  - LATIN1_GERMAN1_CI
  - HP8_ENGLISH_CI
  - KOI8R_GENERAL_CI
  - LATIN1_SWEDISH_CI
  - LATIN2_GENERAL_CI
  - SWE7_SWEDISH_CI
  - ASCII_GENERAL_CI
  - CP1251_BULGARIAN_CI
  - LATIN1_DANISH_CI
  - HEBREW_GENERAL_CI

- LATIN7_ESTONIAN_CS
- LATIN2_HUNGARIAN_CI
- KOI8U_GENERAL_CI
- CP1251_UKRAINIAN_CI
- CP1250_GENERAL_CI
- LATIN2_CROATIAN_CI
- CP1257_LITHUANIAN_CI
- LATIN5_TURKISH_CI
- LATIN1_GERMAN2_CI
- ARMSCII8_GENERAL_CI
- UTF8_GENERAL_CI
- CP1250_CZECH_CS
- CP866_GENERAL_CI
- KEYBCS2_GENERAL_CI
- MACCE_GENERAL_CI
- MACROMAN_GENERAL_CI
- CP852_GENERAL_CI
- LATIN7_GENERAL_CI
- LATIN7_GENERAL_CS
- MACCE_BIN
- CP1250_CROATIAN_CI
- LATIN1_BIN
- LATIN1_GENERAL_CI
- LATIN1_GENERAL_CS
- CP1251_BIN
- CP1251_GENERAL_CI
- CP1251_GENERAL_CS
- MACROMAN_BIN
- CP1256_GENERAL_CI
- CP1257_BIN
- CP1257_GENERAL_CI
- ARMSCII8_BIN
- ASCII_BIN
- CP1250_BIN
- CP1256_BIN
- CP866_BIN
- DEC8_BIN
- GREEK_BIN
- HEBREW_BIN

  - HP8_BIN
  - KEYBCS2_BIN
  - KOI8R_BIN
  - KOI8U_BIN
  - LATIN2_BIN
  - LATIN5_BIN
  - LATIN7_BIN
  - CP850_BIN
  - CP852_BIN
  - SWE7_BIN
  - UTF8_BIN
  - GEOSTD8_GENERAL_CI
  - GEOSTD8_BIN
  - LATIN1_SPANISH_CI
  - UTF8_UNICODE_CI
  - UTF8_ICELANDIC_CI
  - UTF8_LATVIAN_CI
  - UTF8_ROMANIAN_CI
  - UTF8_SLOVENIAN_CI
  - UTF8_POLISH_CI
  - UTF8_ESTONIAN_CI
  - UTF8_SPANISH_CI
  - UTF8_SWEDISH_CI
  - UTF8_TURKISH_CI
  - UTF8_CZECH_CI
  - UTF8_DANISH_CI
  - UTF8_LITHUANIAN_CI
  - UTF8_SLOVAK_CI
  - UTF8_SPANISH2_CI
  - UTF8_ROMAN_CI
  - UTF8_PERSIAN_CI
  - UTF8_ESPERANTO_CI
  - UTF8_HUNGARIAN_CI
  - INVAL_CHARSET

- **MYSQL.CLIENT.DATABASE.** Gibt den Namen der Datenbank zurück, die im Authentifizierungspaket angegeben ist, das der Client an den Datenbankserver sendet. Dies ist das Attribut databasename.
- MYSQL.CLIENT.USER. Gibt den Benutzernamen (im Authentifizierungspaket) zurück, mit dem der Client versucht, eine Verbindung zur Datenbank herzustellen. Dies ist das Benutzerattribut.

- **MYSQL.REQ.** Funktioniert auf einer MySQL Anfrage.
- **MYSQL.REQ.COMMAND.** Gibt die Enumerierungskonstante an, die dem Befehlstyp in der Anforderung zugewiesen ist. Die Operatoren EQ(<m>) und NE(<m>), die boolesche Werte zurückgeben, um das Ergebnis eines Vergleichs anzugeben, werden mit diesem Präfix verwendet. Im Folgenden sind die Enumerationskonstantenwerte:
  - SLEEP
  - QUIT
  - INIT_DB
  - QUERY
  - FIELD_LIST
  - CREATE_DB
  - DROP_DB
  - REFRESH
  - SHUTDOWN
  - STATISTICS
  - PROCESS_INFO
  - CONNECT
  - PROCESS_KILL
  - DEBUG
  - PING
  - TIME
  - DELAYED_INSERT
  - CHANGE_USER
  - BINLOG_DUMP
  - TABLE_DUMP
  - CONNECT_OUT
  - REGISTER_SLAVE
  - STMT_PREPARE
  - STMT_EXECUTE
  - STMT_SEND_LONG_DATA
  - STMT_CLOSE
  - STMT_RESET
  - SET_OPTION
  - STMT_FETCH
- **MYSQL.REQ.QUERY.** Identifiziert die Abfrage in der MySQL Anfrage.
- **MYSQL.REQ.QUERY.COMMAND.** Gibt das erste Schlüsselwort in der MySQL Abfrage zurück.
- **MYSQL.REQ.QUERY.SIZE.** Gibt die Größe der Anforderungsabfrage im ganzzahligen Format zurück. Die SIZE-Methode ähnelt der CONTENT_LENGTH -Methode, die die Länge einer

HTTP-Anforderung oder -Antwort zurückgibt.

- **MYSQL.REQ.QUERY.TEXT.** Gibt eine Zeichenfolge zurück, die die gesamte Abfrage abdeckt.
- **MYSQL.REQ.QUERY.TEXT(<n>).** Gibt die ersten n Bytes der MySQL Abfrage als String zurück. Dies ähnelt HTTP.BODY(<n>).

  Parameter:

  n - Anzahl der Bytes, die zurückgegeben werden sollen
- **MYSQL.RES.** Funktioniert mit einer MySQL Antwort.
- **MYSQL.RES.ATLEAST_ROWS_COUNT(<i>).** Überprüft, ob die Antwort mindestens i Anzahl von Zeilen hat und gibt einen booleschen TRUE oder FALSE zurück, um das Ergebnis anzuzeigen.

  Parameter:

  i - Anzahl der Zeilen
- **MYSQL.RES.ERROR.** Identifiziert das MySQL Fehlerobjekt. Das Fehlerobjekt enthält die Fehlernummer und die Fehlermeldung.
- **MYSQL.RES.ERROR.MESSAGE.** Gibt die Fehlermeldung zurück, die von der Fehlerantwort des Servers abgerufen wird.
- **MYSQL.RES.ERROR.NUM.** Gibt die Fehlernummer zurück, die von der Fehlerantwort des Servers abgerufen wird.
- **MYSQL.RES.ERROR.SQLSTATE.** Gibt den Wert des SQLSTATE-Felds in der Fehlerantwort des Servers zurück. Der MySQL -Server übersetzt Fehlernummernwerte in SQLSTATE-Werte.
- **MYSQL.RES.FIELD(<i>).** Identifiziert das Paket, das dem i^{th entspricht} individuelles Feld in der Antwort des Servers. Jedes Feldpaket beschreibt die Eigenschaften der zugeordneten Spalte. Die Anzahl der Pakete (i) beginnt bei 0.

  Parameter:

  i - Paketnummer
- **MYSQL.RES.FIELD(<i>).CATALOG.** Gibt die katalog-Eigenschaft des Feldpakets zurück.
- **MYSQL.RES.FIELD(<i>).CHAR_SET.** Gibt den Zeichensatz der Spalte zurück. Die Operatoren EQ(<m>) und NE(<m>), die boolesche Werte zurückgeben, um das Ergebnis eines Vergleichs anzugeben, werden mit diesem Präfix verwendet.
- **MYSQL.RES.FIELD(<i>).DATATYPE.** Gibt eine Enumerierungskonstante zurück, die den Datentyp der Spalte darstellt. Dies ist das Attribut type (auch enum_field_type genannt) der Spalte. Die Operatoren EQ(<m>) und NE(<m>), die boolesche Werte zurückgeben, um das Ergebnis eines Vergleichs anzugeben, werden mit diesem Präfix verwendet. Mögliche Werte für die verschiedenen Datentypen sind:

  - DECIMAL
  - TINY
  - SHORT
  - LONG
  - FLOAT
  - DOUBLE
  - NULL
  - TIMESTAMP
  - LONGLONG
  - INT24
  - DATUM
  - TIME
  - DATETIME
  - YEAR
  - NEWDATE
  - VARCHAR (neu in MySQL 5.0)
  - BIT (neu in MySQL 5.0)
  - NEWDECIMAL (neu in MySQL 5.0)
  - ENUM
  - SET
  - TINY_BLOB
  - MEDIUM_BLOB
  - LONG_BLOB
  - BLOB
  - VAR_STRING
  - STRING
  - GEOMETRY

- **MYSQL.RES.FIELD(<i>).DB.** Gibt die Datenbank-ID (db) -Attribut des Feldpakets zurück.
- **MYSQL.RES.FIELD(<i>).DECIMALS.** Gibt die Anzahl der Positionen nach dem Dezimalpunkt zurück, wenn der Typ DECIMAL oder NUMERIC ist. Dies ist das decimals Attribut des Feldpakets.
- **MYSQL.RES.FIELD(<i>).FLAGS.** Gibt die Eigenschaft flags des Feldpakets zurück. Im Folgenden sind die möglichen hexadezimalen Flag-Werte:

  - 0001: NOT_NULL_FLAG
  - 0002: PRI_KEY_FLAG
  - 0004: UNIQUE_KEY_FLAG
  - 0008: MULTIPLE_KEY_FLAG
  - 0010: BLOB_FLAG
  - 0020: UNSIGNED_FLAG

  - 0040: ZEROFILL_FLAG
  - 0080: BINARY_FLAG
  - 0100: ENUM_FLAG
  - 0200: AUTO_INCREMENT_FLAG
  - 0400: TIMESTAMP_FLAG
  - 0800: SET_FLAG

- **MYSQL.RES.FIELD(<i>).LENGTH.** Gibt die Länge der Spalte zurück. Dies ist der Wert des Längenattributs des Feldpakets. Der zurückgegebene Wert ist möglicherweise größer als der tatsächliche Wert. Beispielsweise kann eine Instanz einer VARCHAR (2) -Spalte den Wert 2 zurückgeben, selbst wenn sie nur ein Zeichen enthält.
- **MYSQL.RES.FIELD(<i>).NAME.** Gibt den Spaltenbezeichner zurück (der Name nach der AS-Klausel, falls vorhanden). Dies ist das Name-Attribut des Feldpakets.
- **MYSQL.RES.FIELD(<i>).ORIGINAL_NAME.** Gibt den ursprünglichen Spaltenbezeichner zurück (falls vorhanden vor der AS-Klausel). Dies ist das org_name-Attribut des Feldpakets.
- **MYSQL.RES.FIELD(<i>).ORIGINAL_TABLE.** Gibt den ursprünglichen Tabellenbezeichner der Spalte zurück (falls vorhanden vor der AS-Klausel). Dies ist das org_table-Attribut des Feldpakets.
- **MYSQL.RES.FIELD(<i>).TABLE.** Gibt den Tabellenbezeichner der Spalte zurück (nach der AS-Klausel, falls vorhanden). Dies ist das Tabellenattribut des Feldpakets.
- **MYSQL.RES.FIELDS_COUNT.** Gibt die Anzahl der Feldpakete in der Antwort zurück (das Attribut field_count des OK-Pakets).
- **MYSQL.RES.OK.** Identifiziert das vom Datenbankserver gesendete OK-Paket.
- **MYSQL.RES.OK.AFFECTED_ROWS.** Gibt die Anzahl der Zeilen zurück, die von einer INSERT-, UPDATE- oder DELETE-Abfrage betroffen sind. Dies ist der Wert des attributs affected_rows des OK-Pakets.
- **MYSQL.RES.OK.INSERT_ID.** Identifiziert das Attribut unique_id des OK-Pakets. Wenn keine automatische Inkrementierung von der aktuellen MySQL Anweisung oder Abfrage generiert wird, ist der Wert von unique_id und damit der vom Ausdruck zurückgegebene Wert 0.
- **MYSQL.RES.OK.MESSAGE.** Gibt die Nachrichteneigenschaft des OK-Pakets zurück.
- **MYSQL.RES.OK.STATUS.** Identifiziert die Bitzeichenfolge im server_status-Attribut des OK-Pakets. Clients können den Serverstatus verwenden, um zu überprüfen, ob der aktuelle Befehl Teil einer laufenden Transaktion ist. Die Bits im Bitstring server_status entsprechen den folgenden Feldern (in der angegebenen Reihenfolge):
  - IN TRANSACTION
  - AUTO_COMMIT

- MORE RESULTS
- MULTI QUERY
- BAD INDEX USED
- NO INDEX USED
- CURSOR EXISTS
- LAST ROW SEEN
- DATABASE DROPPED
- NO BACKSLASH ESCAPES

- **MYSQL.RES.OK.WARNING_COUNT.** Gibt das Attribut warning_count des OK-Pakets zurück.
- **MYSQL.RES.ROW(<i>).** Identifiziert das Paket, das dem i^{th entspricht} einzelne Zeile in der Antwort des Datenbankservers.

  Parameter:

  i - Zeilennummer

- **MYSQL.RES.ROW(<i>).DOUBLE_ELEM(<j>).** Prüft, ob das jth Spalte des Ith Zeile der Tabelle ist NULL. Nach C-Konventionen beginnen beide Indizes i und j bei 0. Deshalb sind Zeile i und Spalte j tatsächlich das (i+1)th row und der (j+1)th spalte jeweils.

  Parameter:

  i - Zeilennummer

  j - Spaltennummer

- **MYSQL.RES.ROW(<i>).IS_NULL_ELEM(j).** Prüft, ob das jth Spalte des Ith Zeile der Tabelle ist NULL. Nach C-Konventionen beginnen beide Indizes i und j bei 0. Deshalb sind Zeile i und Spalte j tatsächlich das (i+1)th row und der (j+1)th spalte jeweils.

  Parameter:

  i - Zeilennummer

  j - Spaltennummer

- **MYSQL.RES.ROW(<i>).NUM_ELEM(<j>).** Gibt einen ganzzahligen Wert aus dem jth Spalte des Ith Zeile der Tabelle. Nach C-Konventionen beginnen beide Indizes i und j bei 0. Deshalb sind Zeile i und Spalte j tatsächlich das (i+1)th row und der (j+1)th spalte jeweils.

  Parameter:

  i - Zeilennummer

  j - Spaltennummer

- **MYSQL.RES.ROW(<i>).TEXT_ELEM(j).** Gibt einen String aus dem j^{th zurück} Spalte des Ith Zeile der Tabelle. Nach C-Konventionen beginnen beide Indizes i und j bei 0. Deshalb sind Zeile i und Spalte j tatsächlich das (i+1)th row und der (j+1)th spalte jeweils.

  Parameter:

  i - Zeilennummer

  j - Spaltennummer

- **MYSQL.RES.TYPE.** Gibt eine Enumerierungskonstante für den Antworttyp zurück. Seine Werte können ERROR, OK und RESULT_SET sein. Die Operatoren EQ(<m>) und NE(<m>), die boolesche Werte zurückgeben, um das Ergebnis eines Vergleichs anzugeben, werden mit diesem Präfix verwendet.

Ausdrücke für die Auswertung von Microsoft SQL Server-Verbindungen

Die folgenden Ausdrücke bewerten den Datenverkehr, der mit Microsoft SQL Server-Datenbankservern verknüpft ist. Sie können die anforderungsbasierten Ausdrücke (Ausdrücke, die mit MSSQL.CLIENT und MSSQL.REQ beginnen) in Richtlinien verwenden, um Anforderungswechselentscheidungen am Bindungspunkt des virtuellen Content Switching-Servers zu treffen und die antwortbasierten Ausdrücke (Ausdrücke, die mit MSSQL.RES beginnen), um Serverantworten an Benutzer auszuwerten. konfigurierte Integritätsüberwachungen.

Ausdruck	Beschreibung
MSSQL.CLIENT.CAPABILITIES	Gibt die Felder OptionFlags1, OptionFlags2, OptionFlags3 und TypeFlags des Login7Authentication-Pakets in dieser Reihenfolge als Ganzzahl von 4 Byte zurück. Jedes Feld ist 1 Byte lang und gibt eine Reihe von Clientfunktionen an.
MSSQL.CLIENT.DATABASE	Gibt den Namen der Client-Datenbank zurück. Der zurückgegebene Wert ist vom Typ Text.
MSSQL.CLIENT.USER	Gibt den Benutzernamen zurück, mit dem der Client authentifiziert hat. Der zurückgegebene Wert ist vom Typ Text.

Ausdruck	Beschreibung
MSSQL.REQ.COMMAND	Gibt eine Enumerierungskonstante zurück, die den Typ des Befehls in der Anforderung angibt, die an einen Microsoft SQL Server-Datenbankserver gesendet wird. Der zurückgegebene Wert ist vom Typ Text. Beispiele für die Werte der Enumerierungskonstante sind QUERY, RESPONSE, RPC und ATTENTION. Die <m> <m> Operatoren EQ () und NE (), die boolesche Werte zurückgeben, um das Ergebnis eines Vergleichs anzuzeigen, werden mit diesem Ausdruck verwendet.
MSSQL.REQ.QUERY.COMMAND	Gibt das erste Schlüsselwort in der SQL-Abfrage zurück. Der zurückgegebene Wert ist vom Typ Text.
MSSQL.REQ.QUERY.SIZE	Gibt die Größe der SQL-Abfrage in der Anforderung zurück. Der zurückgegebene Wert ist eine Zahl.
MSSQL.REQ.QUERY.TEXT	Gibt die gesamte SQL-Abfrage als Zeichenfolge zurück. Der zurückgegebene Wert ist vom Typ Text.
MSSQL.REQ.QUERY.TEXT (<n>)	Gibt die ersten n Bytes der SQL-Abfrage zurück. Der zurückgegebene Wert ist vom Typ Text. Parameter: n - Anzahl der Bytes
MSSQL.REQ.RPC.NAME	Gibt den Namen der Prozedur zurück, die in einer RPC-Anforderung (Remote Procedure Call) aufgerufen wird. Der Name wird als Zeichenfolge zurückgegeben.
MSSQL.REQ.RPC.IS_PROCID	Gibt einen booleschen Wert zurück, der angibt, ob die RPC-Anforderung (Remote Procedure Call) eine Prozedur-ID oder einen RPC-Namen enthält. Ein Rückgabewert von TRUE zeigt, dass die Anforderung eine Prozedur-ID enthält. Ein Rückgabewert von FALSE, gibt an, dass die Anforderung einen RPC-Namen enthält.

Ausdruck	Beschreibung
MSSQL.REQ.RPC.PROCID	Gibt die Prozedur-ID der RPC-Anforderung (Remote Procedure Call) als Ganzzahl zurück.
MSSQL.REQ.RPC.BODY **Hinweis:** Nicht verfügbar für Versionen vor 10.1.	Gibt den Körper der SQL-Anforderung als String in Form von Parametern zurück, die als “a=b” -Klauseln durch Kommas getrennt dargestellt werden, wobei “a” der RPC-Parametername und “b” der Wert ist.
MSSQL.REQ.RPC.BODY(n) **Hinweis:** Nicht verfügbar für Versionen vor 10.1.	Gibt einen Teil des Körpers der SQL-Anforderung als String in Form von Parametern zurück, die als “a=b” -Klauseln durch Kommas getrennt dargestellt werden, wobei “a” der RPC-Parametername und “b” der Wert ist. Parameter werden nur von den ersten n Bytes der Anforderung zurückgegeben, wobei der SQL-Header übersprungen wird. Es werden nur vollständige Name-Wert-Paare zurückgegeben.
MSSQL.RES.ATLEAST_ROWS_COUNT(i)	Überprüft, ob die Antwort mindestens i Anzahl von Zeilen hat. Der zurückgegebene Wert ist ein boolescher TRUE oder FalseValue. Parameter: i - Anzahl der Zeilen
MSSQL.RES.DONE.ROWCOUNT	Gibt eine Anzahl der Zeilen zurück, die von einer INSERT-, UPDATE- oder DELETE-Abfrage betroffen sind. Der zurückgegebene Wert ist vom Typ long ohne Vorzeichen.
MSSQL.RES.DONE.STATUS	Gibt das Statusfeld aus dem Token DONE zurück, das von einem Microsoft SQL Server-Datenbankserver gesendet wird. Der zurückgegebene Wert ist eine Zahl.
MSSQL.RES.ERROR.MESSAGE	Gibt die Fehlermeldung aus dem FEHLER Token zurück, das von einem Microsoft SQL Server-Datenbankserver gesendet wird. Dies ist der Wert des MsgText-Feldes im FEHLER Token. Der zurückgegebene Wert ist vom Typ Text.

Ausdruck	Beschreibung
MSSQL.RES.ERROR.NUM	Gibt die Fehlernummer des ERROR Token zurück, das von einem Microsoft SQL Server-Datenbankserver gesendet wird. Dies ist der Wert des Feldes Zahl im FEHLER Token. Der zurückgegebene Wert ist eine Zahl.
MSSQL.RES.ERROR.STATE	Gibt den Fehlerstatus des ERROR Token zurück, das von einem Microsoft SQL Server-Datenbankserver gesendet wird. Dies ist der Wert des Feldes Status im FEHLER Token. Der zurückgegebene Wert ist eine Zahl.
MSSQL.RES.FIELD (<i>) .DATATYPE	Gibt den Datentyp des i-ten Felds in der Serverantwort zurück. Mit <m> <m> diesem Präfix werden die Funktionen EQ () und NE () verwendet, die boolesche Werte zurückgeben, um das Ergebnis eines Vergleichs anzuzeigen. Der folgende Ausdruck gibt beispielsweise einen booleschen TRUE zurück, wenn die DATATYPE-Funktion den Wert datetime für das dritte Feld in der Antwort zurückgibt: MSSQL.RES.FIELD (<2>) .DATATYPE.EQ (datetime) Parameter: i - Zeilennummer
MSSQL.RES.FIELD (<i>) .LENGTH	Gibt die maximal mögliche Länge des i-ten Felds in der Serverantwort zurück. Der zurückgegebene Wert ist eine Zahl. Parameter: i - Zeilennummer
MSSQL.RES.FIELD (<i>) .NAME	Gibt den Namen des ith-Felds in der Serverantwort zurück. Der zurückgegebene Wert ist vom Typ Text. Parameter: i - Zeilennummer

Ausdruck	Beschreibung
MSSQL.RES.ROW (<i>) .DOUBLE_ELEM (<j>)	Gibt einen Wert vom Typ double aus der jten Spalte der iten Zeile der Tabelle zurück. Wenn der Wert kein doppelter Wert ist, wird eine UNDEF-Bedingung ausgelöst. Nach C-Konventionen beginnen beide Indizes i und j bei 0 (Null). Daher sind Zeile i und Spalte j tatsächlich die (i + 1) te Zeile bzw. die (j + 1) te Spalte. Parameter: i - Zeilennummer j - Spaltennummer
MSSQL.RES.ROW (<i>) .NUM_ELEM (j)	Gibt einen ganzzahligen Wert aus der jten Spalte der i-ten Zeile der Tabelle zurück. Wenn der Wert kein ganzzahliger Wert ist, wird eine UNDEF-Bedingung ausgelöst. Nach C-Konventionen beginnen beide Indizes i und j bei 0 (Null). Daher sind Zeile i und Spalte j tatsächlich die (i + 1) te Zeile bzw. die (j + 1) te Spalte. Parameter: i - Zeilennummer j - Spaltennummer
MSSQL.RES.ROW (<i>) .IS_NULL_ELEM (j)	Überprüft, ob die jte Spalte der i-ten Zeile der Tabelle NULL ist und gibt einen booleschen TRUE oder FALSE zurück, um das Ergebnis anzuzeigen. Nach C-Konventionen beginnen beide Indizes i und j bei 0 (Null). Daher sind Zeile i und Spalte j tatsächlich die (i + 1) te Zeile bzw. die (j + 1) te Spalte. Parameter: i - Zeilennummer j - Spaltennummer
MSSQL.RES.ROW (<i>) .TEXT_ELEM (j)	Gibt eine Textzeichenfolge aus der jten Spalte der i-ten Zeile der Tabelle zurück. Nach C-Konventionen beginnen beide Indizes i und j bei 0 (Null). Daher sind Zeile i und Spalte j tatsächlich die (i + 1) te Zeile bzw. die (j + 1) te Spalte. Parameter: i - Zeilennummer j - Spaltennummer

Ausdruck	Beschreibung
MSSQL.RES.TYPE	Gibt eine Enumerierungskonstante zurück, die den Antworttyp identifiziert. Im Folgenden sind die möglichen Rückgabewerte: ERROR, OK und RESULT_SET. Die <m> <m> Operatoren EQ () und NE (), die boolesche Werte zurückgeben, um das Ergebnis eines Vergleichs anzuzeigen, werden mit diesem Ausdruck verwendet.

Typumwandlung von Daten

October 5, 2021

Sie können Daten eines Typs (z. B. Text oder Ganzzahl) aus Anfragen und Antworten extrahieren und in Daten eines anderen Typs transformieren. Beispielsweise können Sie eine Zeichenfolge extrahieren und die Zeichenfolge in ein Zeitformat umwandeln. Sie können auch eine Zeichenfolge aus einem HTTP-Anforderungskörper extrahieren und sie wie ein HTTP-Header behandeln oder einen Wert aus einem Anforderungsheader extrahieren und in einen Antwort-Header eines anderen Typs einfügen.

Nach dem Typumstellen der Daten können Sie jeden Vorgang anwenden, der für den neuen Datentyp geeignet ist. Wenn Sie beispielsweise Text in einen HTTP-Header eingeben, können Sie jeden Vorgang anwenden, der auf HTTP-Header anwendbar ist, auf den zurückgegebenen Wert.

Weitere Informationen zum Typecasting von Daten finden Sie in der PDF-Datei Typecasting Operations .

Reguläre Ausdrücke

October 5, 2021

Wenn Sie Zeichenfolgenabgleichvorgänge ausführen möchten, die komplexer sind als die Operationen, die Sie mit den Operatoren CONTAINS (”<string>”) oder EQ (”<string>”) ausführen, verwenden Sie reguläre Ausdrücke. Die Richtlinieninfrastruktur der Citrix® Citrix ADC® -Appliance umfasst Operatoren, an die Sie reguläre Ausdrücke als Argumente für den Textabgleich übergeben können. Die Namen der Operatoren, die mit regulären Ausdrücken arbeiten, umfassen die Zeichenfolge REGEX. Die regulären Ausdrücke, die Sie als Argumente übergeben, müssen der Syntax für reguläre Ausdrücke

entsprechen, die unter beschrieben wird. Weitere Informationen zu regulären Ausdrücken finden "<http://www.pcre.org/pcre.txt>." Sie unter "<http://www.regular-expressions.info/quickstart.html>" und unter "<http://www.silverstones.com/thebat/Regex.html>."

Der Zieltext für einen Operator, der mit regulären Ausdrücken arbeitet, kann entweder Text oder der Wert eines HTTP-Headers sein. Es folgt das Format eines Standard-Syntaxausdrucks, der einen Operator für reguläre Ausdrücke verwendet, um Text zu arbeiten:

```
<text>.<regex_operator>(re<delimiter><regex_pattern><delimiter>)
```

Die Zeichenfolge <text> stellt das standardmäßige Syntaxausdruckpräfix dar, das eine Textzeichenfolge in einem Paket identifiziert (z. B. HTTP.REQ.URL). Die Zeichenfolge <regex_operator> stellt den Operator für reguläre Ausdrücke dar. Der reguläre Ausdruck beginnt immer mit der Zeichenfolge re. Ein Paar übereinstimmender Trennzeichen, dargestellt durch <delimiter>, umschließt die Zeichenfolge <regex_pattern>, die den regulären Ausdruck darstellt.

Der folgende Beispielausdruck überprüft, ob die URL in einem HTTP-Paket die Zeichenfolge *.jpeg enthält (wobei * ein Platzhalter ist) und gibt einen booleschen Wert TRUE oder FALSE zurück, um das Ergebnis anzuzeigen. Der reguläre Ausdruck wird in ein Paar von Schrägstrichen (/) eingeschlossen, die als Trennzeichen fungieren.

```
http.req.url.regex_match(re/.<asterisk>\.jpeg/)
```

Operatoren für reguläre Ausdrücke können kombiniert werden, um den Bereich einer Suche zu definieren oder zu verfeinern. <text>.AFTER_REGEX(reregex_pattern1).BEFORE_REGEX(reregex_pattern2) Gibt beispielsweise an, dass das Ziel für den Zeichenfolgenabgleich der Text zwischen den Mustern regex_pattern1 und regex_pattern2 ist. Sie können einen Textoperator für den Bereich verwenden, der von den Operatoren für reguläre Ausdrücke definiert wird. Beispielsweise können Sie den Operator CONTAINS ("<string>") verwenden, um zu überprüfen, ob der definierte Bereich die Zeichenfolge abc enthält:

```
<text>.AFTER_REGEX(re/regex_pattern1).BEFORE_REGEX(re/regex_pattern2/).
CONTAINS("abc")
```

> **Hinweis:**
>
> Die Auswertung eines regulären Ausdrucks dauert inhärent mehr Zeit als die für einen Operator wie CONTAINS ("<string>") oder EQ ("<string>"), die mit einfachen String-Argumenten arbeiten. Sie sollten reguläre Ausdrücke nur verwenden, wenn Ihre Anforderung außerhalb des Bereichs anderer Operatoren liegt.

Grundlegende Merkmale regulärer Ausdrücke

October 5, 2021

Im Folgenden finden Sie bemerkenswerte Merkmale regulärer Ausdrücke, die auf der Citrix ADC Appliance definiert sind:

- Ein regulärer Ausdruck beginnt immer mit der Zeichenfolge re gefolgt von einem Paar von Trennzeichen (als Trennzeichen bezeichnet), die den regulären Ausdruck einschließen, den Sie verwenden möchten.

Beispielsweise <regex_pattern> verwendet re# # das Nummernzeichen (#) als Trennzeichen.

- Ein regulärer Ausdruck darf 1499 Zeichen nicht überschreiten.
- Der Zahlenvergleich kann mit der Zeichenfolge d (ein umgekehrter Schrägstrich gefolgt von d) erfolgen.
- Leerzeichen können durch Verwendung von s (ein umgekehrter Schrägstrich gefolgt von s) dargestellt werden.
- Ein regulärer Ausdruck kann Leerzeichen enthalten.

Im Folgenden sind die Unterschiede zwischen der Citrix ADC tax und der PCRE-Syntax aufgeführt:

- Citrix ADC erlaubt keine Rückverweise in regulären Ausdrücken.
- Sie sollten keine rekursiven regulären Ausdrücke verwenden.
- Das Punkt-Meta-Zeichen stimmt auch mit dem Zeilenumbruch überein.
- Unicode wird nicht unterstützt.
- Die Operation SET_TEXT_MODE (IGNORECASE) überschreibt die (?i) interne Option im regulären Ausdruck.

Operationen für reguläre Ausdrücke

October 5, 2021

In der folgenden Tabelle werden die Operatoren beschrieben, die mit regulären Ausdrücken arbeiten. Die Operation, die von einem Operator für reguläre Ausdrücke in einem bestimmten Standard-Syntaxausdruck ausgeführt wird, hängt davon ab, ob das Ausdruckspräfix Text oder HTTP-Header identifiziert. Vorgänge, die Header auswerten, überschreiben textbasierte Vorgänge für alle Instanzen des angegebenen Headertyps. Wenn Sie einen Operator verwenden, <text> ersetzen Sie durch das standardmäßige Syntaxausdruckpräfix, das Sie für die Identifizierung von Text konfigurieren möchten.

Regulärer Ausdruck	Beschreibung
<text>.BEFORE_REGEX (<regular expression>)	Wählt den Text aus, der vor der Zeichenfolge steht, die dem <regular expression> Argument entspricht. Wenn der reguläre Ausdruck keinen Daten im Ziel entspricht, gibt der Ausdruck ein Textobjekt der Länge 0 zurück. Der folgende Ausdruck wählt die Zeichenfolge “text” aus “text/plain”. http.res.header (“content-type”) .before_regex (re#/#)
<text>.AFTER_REGEX (<regular expression>)	Wählt den Text aus, der der Zeichenfolge folgt, die dem <regular expression> Argument entspricht. Wenn der reguläre Ausdruck keinem Text im Ziel entspricht, gibt der Ausdruck ein Textobjekt der Länge 0 zurück. Der folgende Ausdruck extrahiert “Beispiel” aus “MyExample”: http.req.header (“etag”) .after_regex (re/mein/)
<text>.REGEX_SELECT (<regular expression>)	Wählt eine Zeichenfolge aus, die dem <regular expression> Argument entspricht. Wenn der reguläre Ausdruck nicht mit dem Ziel übereinstimmt, wird ein Textobjekt der Länge 0 zurückgegeben. Das folgende Beispiel extrahiert die Zeichenfolge “NS-CACHE-9.0:90” aus einem Via-Header: http.req.header (“via”) .regex_select (re! NS-cache-d.d:s*d {1,3}!)

Regulärer Ausdruck	Beschreibung
<text>.REGEX_MATCH (<regular expression>)	Gibt TRUE zurück, wenn das Ziel einem <regular expression> Argument von bis zu 1499 Zeichen entspricht. Der reguläre Ausdruck muss das folgende Format haben: re <delimiter> regulärer Ausdruck< delimiter> Beide Trennzeichen müssen gleich sein. Darüber hinaus muss der reguläre Ausdruck der PERL-kompatiblen (PCRE) Library Syntax für reguläre Ausdrücke entsprechen. Weitere Information finden Sie unter http://www.pcre.org/pcre.txt. Siehe insbesondere die Handbuchseite pcrepattern. Beachten Sie jedoch Folgendes: Rückverweise sind nicht zulässig. Rekursive reguläre Ausdrücke werden nicht empfohlen. Der Punkt-Metazeichen entspricht auch dem Zeilenumbruch. Der Unicode-Zeichensatz wird nicht unterstützt. SET_TEXT_MODE (IGNORECASE) überschreibt die (? i) interne Option im regulären Ausdruck angegeben. Im Folgenden sind Beispiele: http.req.hostname.regex_match (re/[[:alpha:]] + (abc) {2,3}/) und http.req.url.set_text_mode (urlencoded) .regex_match (re# (a*b+c*) #) Das folgende Beispiel stimmt mit ab und Ab überein: http.req.url.rex_match (regex_match (regex_match (regex_match (regex_match (regex_match /ein (? i) b/) Das folgende Beispiel stimmt mit ab, ab, Ab und AB überein: http.req.url.set_text_mode (ignorecase) .regex_match (re/ab/) Das folgende Beispiel führt eine mehrzeilige Übereinstimmung ohne Berücksichtigung der Groß- und Kleinschreibung durch, bei der das Punkt-Meta-Zeichen auch mit einem Zeilenzeilenzeichen übereinstimmt: http.req.body.regex_match (re/ (? ixm) (^ab (.*) cd$)/)

Regulärer Ausdruck	Beschreibung

Konfigurieren klassischer Richtlinien und Ausdrücke

October 5, 2021

Einige Citrix ADC Funktionen verwenden klassische Richtlinien und klassische Ausdrücke. Wie bei Standard-Syntaxrichtlinien können klassische Richtlinien entweder global oder spezifisch für einen virtuellen Server sein. In gewissem Maße unterscheiden sich die Konfigurationsmethode und die Bindpunkte für klassische Richtlinien jedoch von denen der Standard-Syntaxrichtlinien. Wie bei Standard-Syntaxausdrücken können Sie benannte Ausdrücke konfigurieren und einen benannten Ausdruck in mehreren klassischen Richtlinien verwenden.

In der folgenden Tabelle werden Citrix ADC Features zusammengefasst, die mithilfe klassischer Richtlinien konfiguriert werden können.

Klicken Sie hier um die Tabelle zu sehen.

Konfigurieren einer klassischen Richtlinie

October 5, 2021

Sie können klassische Richtlinien und klassische Ausdrücke mit dem Konfigurationsdienstprogramm oder der Befehlszeilenschnittstelle konfigurieren. Eine Richtlinienregel darf 1.499 Zeichen lang sein. Beim Konfigurieren der Richtlinienregel können Sie benannte klassische Ausdrücke verwenden. Weitere Informationen zu benannten Ausdrücken finden Sie unter Erstellen benannter klassischer Ausdrücke. Nachdem Sie die Richtlinie konfiguriert haben, binden Sie sie entweder global oder an einen virtuellen Server.

Beachten Sie, dass die Richtlinienkonfigurationsmethoden für verschiedene Citrix ADC Features kleine Unterschiede aufweisen.

Hinweis: Sie können einen klassischen Ausdruck in einen Standard-Syntaxausdruck einbetten, indem Sie die Syntax SYS.EVAL_CLASSIC_EXPR (classic_expression) verwenden und den classic_expression als Argument angeben.

Erstellen einer klassischen Richtlinie mit der CLI

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


```
-  add cmp policy <name> -rule <expression> -action <action>

-  show cmp policy [<policyName>]
<!--NeedCopy-->
```

Beispiel

Mit den folgenden Befehlen wird zuerst eine Komprimierungsaktion erstellt und dann eine Komprimierungsrichtlinie erstellt, die die Aktion anwendet:

```
> add cmp action cmp-act-compress compress
 Done
> show cmp action cmp-act-compress
1)      Name: cmp-act-compress  Compression Type: compress
 Done
> add cmp pol cmp-pol-compress -rule ExpCheckIp -resAction cmp-act-
   compress
 Done
> show cmp pol cmp-pol-compress
1)      Name: cmp-pol-compress  Rule: ExpCheckIp
        Response action: cmp-act-compress       Hits: 0
 Done
>
<!--NeedCopy-->
```

Erstellen einer Richtlinie mit klassischen Ausdrücken mit der GUI

1. Erweitern Sie im Navigationsbereich das Feature, für das Sie eine Richtlinie konfigurieren möchten, und führen Sie je nach Funktion folgende Schritte aus:
   - Klicken Sie für Content Switching, Cache-Umleitung und die Anwendungsfirewall auf **Richtlinien**.
   - Klicken Sie für SSL auf Richtlinien, und klicken Sie dann im Detailbereich auf die Registerkarte **Richtlinien**.
   - Klicken Sie für **Systemauthentifizierung** auf **Authentifizierung**, und klicken Sie dann im Detailbereich auf die Registerkarte **Richtlinien**.
   - Erweitern Sie unter Filter, SureConnect und Priority Queuing die Option Schutzfunktionen, wählen Sie die gewünschte Funktion aus, und klicken Sie dann im Detailbereich auf die Registerkarte **Richtlinien**.

- Erweitern Sie für Citrix Gateway Citrix Gateway, erweitern Sie Richtlinien, wählen Sie die gewünschte Funktion aus, und klicken Sie dann im Detailbereich auf die Registerkarte **Richtlinien**.

2. Klicken Sie für die meisten Features auf die Schaltfläche **Hinzufügen**.
3. Geben Sie im Dialogfeld **Richtlinie erstellen** <feature name> im Textfeld Name* einen Namen für die Richtlinie ein.

   Hinweis: Sie müssen einen Richtliniennamen mit einem Buchstaben oder einem Unterstrich beginnen. Ein Richtlinienname kann aus 1 bis 31 Zeichen bestehen, einschließlich Buchstaben, Zahlen, Bindestrich (-), Punkt (.), Pfundzeichen (#), Leerzeichen () und Unterstrich (_).
4. Bei den meisten Features verknüpfen Sie eine Aktion oder ein Profil. Beispielsweise müssen Sie möglicherweise eine Aktion auswählen, oder im Falle einer Citrix Gateway - oder Anwendungsfirewall ein Profil auswählen, das der Richtlinie zugeordnet werden soll. Ein Profil ist eine Gruppe von Konfigurationsoptionen, die als eine Reihe von Aktionen fungieren, die angewendet werden, wenn die analysierten Daten mit der Richtlinienregel übereinstimmen.
5. Erstellen Sie einen Ausdruck, der den Datentyp beschreibt, mit dem diese Richtlinie übereinstimmen soll.

   Je nach Art der Richtlinie, die Sie erstellen möchten, können Sie einen vordefinierten Ausdruck auswählen oder einen neuen Ausdruck erstellen.

   Benannte Ausdrücke sind vordefinierte Ausdrücke, auf die Sie in einer Richtlinienregel nach Namen verweisen können.
6. Klicken Sie auf **Erstellen**, um Ihre neue Richtlinie zu erstellen.
7. Klicken Sie auf **Schließen**, um zum Fenster Richtlinien für den von Ihnen erstellten Richtlinientyp zurückzukehren.

Konfigurieren eines klassischen Ausdrucks

October 5, 2021

Klassische Ausdrücke bestehen aus den folgenden Ausdruckselementen, die in hierarchischer Reihenfolge aufgeführt sind:

- **Strömungsart.** Gibt an, ob die Verbindung ein- oder ausgehend ist. Der Flow-Typ ist REQ für eingehende Verbindungen und RES für ausgehende Verbindungen.
- **-Protokoll.** Gibt das Protokoll an, dessen Optionen HTTP, SSL, TCP und IP sind.
- **Qualifikator.** Das Protokollattribut, das vom ausgewählten Protokoll abhängt.

- **Operator.** Der Typ des Tests, den Sie für die Verbindungsdaten durchführen möchten. Ihre Wahl des Betreibers hängt von den Verbindungsinformationen ab, die Sie testen. Wenn die Verbindungsinformationen, die Sie testen, Text sind, verwenden Sie Text-Operatoren. Wenn es sich um eine Zahl handelt, verwenden Sie standardmäßige numerische Operatoren.
- **Wert.** Die Zeichenfolge oder Zahl, mit der das Verbindungsdatenelement (definiert durch den Flusstyp, das Protokoll und die Qualifikation) getestet wird. Der Wert kann entweder ein Literal oder ein Ausdruck sein. Das Literal oder der Ausdruck muss mit dem Datentyp des Verbindungsdatenelements übereinstimmen.

In einer Richtlinie können klassische Ausdrücke kombiniert werden, um komplexere Ausdrücke mit booleschen und vergleichenden Operatoren zu erstellen.

Ausdruckselemente werden von links nach rechts analysiert. Das Element ganz links ist entweder REQ oder RES und bezeichnet eine Anfrage bzw. eine Antwort. Aufeinanderfolgende Begriffe definieren einen bestimmten Verbindungstyp und ein bestimmtes Attribut für diesen Verbindungstyp. Jeder Term ist durch einen Zeitraum von einem vorhergehenden oder folgenden Term getrennt. Argumente werden in Klammern angezeigt und folgen dem Ausdruckselement, an das sie übergeben werden.

Das folgende klassische Ausdrucks-Fragment gibt die Client-Quell-IP für eine eingehende Verbindung zurück.

```
REQ.IP.SOURCEIP
```

Das Beispiel identifiziert eine IP-Adresse in einer Anforderung. Das Ausdruckselement SOURCEIP gibt die Quell-IP-Adresse an. Dieses Ausdrucksfragment ist möglicherweise nicht von selbst nützlich. Sie können ein zusätzliches Ausdruckselement, einen Operator, verwenden, um zu bestimmen, ob der zurückgegebene Wert bestimmte Kriterien erfüllt. Der folgende Ausdruck testet, ob sich die Client-IP im Subnetz 200.0.0.0/8 befindet und gibt einen booleschen TRUE oder FALSE zurück:

```
REQ.IP.SOURCEIP == 200.0.0.0 -netmask 255.0.0.0
```

Erstellen eines klassischen Richtlinienausdrucks mit der CLI

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

```
1 -  set appfw policy <name> -rule <expression> -action <action>
2
3 -  show appfw policy <name>
4 <!--NeedCopy-->
```

Beispiel


```
> set appfw policy GenericApplicationSSL_ 'HTTP.REQ.METHOD.EQ(”get”)'
   APPFW_DROP
 Done
> show appfw policy GenericApplicationSSL_
        Name: GenericApplicationSSL_    Rule: HTTP.REQ.METHOD.EQ(”get”)
        Profile: APPFW_DROP     Hits: 0
        Undef Hits: 0
        Policy is bound to following entities
        1) REQ VSERVER app_u_GenericApplicationSSLPortalPages
           PRIORITY : 100
 Done
<!--NeedCopy-->
```

Hinzufügen eines Ausdrucks für eine klassische Richtlinie mit der GUI

Diese Prozedur dokumentiert das Dialogfeld Ausdruck hinzufügen. Abhängig von der Funktion, für die Sie eine Richtlinie konfigurieren, kann die Route, über die Sie zu diesem Dialogfeld gelangen, unterschiedlich sein.

1. Führen Sie die Schritte 1-4 unter “So erstellen Sie eine Richtlinie mit klassischen Ausdrücken mit der GUI” aus.
2. Klicken **Sie im Dialogfeld Ausdruck hinzufügen** unter Ausdruckstyp auf den Ausdruckstyp, den Sie erstellen möchten.
3. Klicken Sie unter **Flow-Typ** auf den Pfeil nach unten, und wählen Sie einen Flow-Typ aus.

Der Flow-Typ ist in der Regel REQ oder RES. Die Option REQ gibt an, dass die Richtlinie für alle eingehenden Verbindungen oder Anforderungen gilt. Die Option RES wendet die Richtlinie auf alle ausgehenden Verbindungen oder Antworten an.

Für Richtlinien der Anwendungsfirewall sollten Sie den Ausdruckstyp auf Allgemeiner Ausdruck und den Flow-Typ auf REQ festlegen. Die Anwendungsfirewall behandelt jede Anforderung und Antwort als einzelne gepaarte Entität. Daher beginnen alle Richtlinien der Anwendungsfirewall mit REQ.

1. Klicken Sie unter Protokoll auf den Pfeil nach unten, und wählen Sie das Protokoll aus, das Sie für den Richtlinienausdruck verwenden möchten. Ihre Auswahlmöglichkeiten:
   - HTTP Bewertet HTTP-Anforderungen, die an einen Webserver gesendet werden. Bei klassischen Ausdrücken enthält HTTP HTTPS-Anforderungen.
   - SSL. Bewertet SSL-Daten, die der aktuellen Verbindung zugeordnet sind.
   - TCP. Bewertet die TCP-Daten, die der aktuellen Verbindung zugeordnet sind.
   - IP. Bewertet die IP-Adressen, die der aktuellen Verbindung zugeordnet sind.
2. Klicken Sie unter Qualifier auf den Pfeil nach unten, und wählen Sie einen Qualifier für Ihre Richtlinie aus.

Der Qualifier definiert den Typ der auszuwertenden Daten. Die angezeigte Liste der Kriterien hängt davon ab, welches Protokoll Sie in Schritt 4 ausgewählt haben.
Für das HTTP-Protokoll werden folgende Optionen angezeigt:

- METHOD. Filtert HTTP-Anforderungen, die eine bestimmte HTTP-Methode verwenden.
- -URL. Filtert HTTP-Anforderungen für eine bestimmte Webseite.
- URLQUERY. Filtert HTTP-Anforderungen, die eine bestimmte Abfragezeichenfolge enthalten.
- VERSION. Filtert HTTP-Anforderungen auf der Grundlage der angegebenen HTTP-Protokollversion.
- HEADER. Filtert auf der Basis eines bestimmten HTTP-Headers.
- URLLEN. Filtert auf der Grundlage der Länge der URL.
- URLQUERY. Filtert auf Basis des Query-Teils der URL.
- URLQUERYLEN. Filtert nur anhand der Länge des Abfrageabschnitts der URL.

3. Klicken Sie unter Operator auf den Pfeil nach unten, und wählen Sie den Operator für Ihren Richtlinienausdruck aus. Einige gängige Operatoren sind:

Operator	Beschreibung
==	Entspricht dem angegebenen Wert genau oder ist genau gleich dem angegebenen Wert.
!=	Entspricht nicht dem angegebenen Wert.
>	Ist größer als der angegebene Wert.
<	Ist kleiner als der angegebene Wert.
>=	Ist größer oder gleich dem angegebenen Wert.
<=	Ist kleiner oder gleich dem angegebenen Wert.
CONTAINS	Enthält den angegebenen Wert.
CONTENTS	Gibt den Inhalt der angegebenen Header-, URL- oder URL-Abfrage zurück.
EXISTS	Der angegebene Header oder die angegebene Abfrage ist vorhanden.
NOTCONTAINS	Enthält nicht den angegebenen Wert.
NOTEXISTS	Der angegebene Header oder die angegebene Abfrage ist nicht vorhanden.

1. Wenn ein Textfeld Wert angezeigt wird, geben Sie gegebenenfalls eine Zeichenfolge oder einen numerischen Wert ein. Wählen Sie z. B. REQ als Flow-Typ, HTTP als Protokoll und HEADER als

Qualifizierer, und geben Sie dann den Wert der Kopfzeilenzeichenfolge in das Feld Wert und den Headertyp ein, für den Sie der Zeichenfolge im Textfeld Kopfzeilenname entsprechen möchten.

2. Klicken Sie auf **OK**.
3. Klicken Sie auf Hinzufügen, um einen zusammengesetzten Ausdruck zu erstellen. Beachten Sie, dass die Art der Zusammensetzung, die durchgeführt wird, von den folgenden Optionen im Dialogfeld Richtlinie erstellen abhängt:
   - **Übereinstimmung mit einem beliebigen Ausdruck.** Die Ausdrücke befinden sich in einer logischen OR-Beziehung.
   - **Übereinstimmung mit allen Ausdrücken.** Die Ausdrücke befinden sich in einer logischen UND-Beziehung.
   - **Tabellarische Ausdrücke.** Klicken Sie auf die Schaltflächen UND, OR und Klammern, um die Auswertung zu steuern.
   - **Fortgeschrittene Freiform.** Geben Sie die Ausdruckskomponenten direkt in das Feld Ausdruck ein, und klicken Sie auf die Schaltflächen UND, OR und Klammern, um die Auswertung zu steuern.

Binden einer klassischen Richtlinie

October 5, 2021

Je nach Richtlinientyp können Sie eine klassische Richtlinie entweder global oder an einen virtuellen Server binden. Richtlinienbindpunkte werden in der Tabelle Richtlinientyp und Bindpunkte für Richtlinien in Features, die klassische Richtlinien verwenden beschrieben.

Hinweis: Sie können eine klassische Richtlinie an mehrere Bindungspunkte binden.

Binden einer klassischen Richtlinie global mit der CLI

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

```
1 -  bind cmp global <policyName> [-priority <positive_integer>]
2
3 -  show cmp global
4 <!--NeedCopy-->
```


Beispiel

```
> bind cmp global cmp-pol-compress -priority 2
 Done
> show cmp global
1)      Policy Name: cmp-pol-compress   Priority: 2
2)      Policy Name: ns_nocmp_xml_ie    Priority: 8700
3)      Policy Name: ns_nocmp_mozilla_47        Priority: 8800
4)      Policy Name: ns_cmp_mscss       Priority: 8900
5)      Policy Name: ns_cmp_msapp       Priority: 9000
6)      Policy Name: ns_cmp_content_type        Priority: 10000
 Done
>
<!--NeedCopy-->
```

Binden einer klassischen Richtlinie an einen virtuellen Server mit der CLI

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

```
-  bind lb vserver <name> [<targetVserver>] [-policyName <string> [-
   priority <positive_integer>]

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

Beispiel

```
> bind lb vserver lbtemp -policyName cmp-pol-compress -priority 1
 Done
> show lb vserver lbtemp
        lbtemp (10.102.29.101:80) - HTTP        Type: ADDRESS
        State: UP
        Last state change was at Tue Oct 27 06:40:38 2009 (+557 ms)
        Time since last state change: 0 days, 02:00:40.330
        Effective State: UP
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
```



```
13          No. of Bound Services :  1 (Total)       1 (Active)
14          Configured Method: LEASTCONNECTION
15          Current Method: Round Robin, Reason: Bound service's state
               changed to UP
16          Group: vserver-grp
17          Mode: IP
18          Persistence: COOKIEINSERT (version 0)   Persistence Backup:
               SOURCEIP   Persistence Mask: 255.255.255.255
19          Persistence Timeout: 2 min      Backup Persistence Timeout: 2
               min
20          Vserver IP and Port insertion: OFF
21          Push: DISABLED  Push VServer:
22          Push Multi Clients: NO
23          Push Label Rule: none
24  1) http-one (10.102.29.252: 80) - HTTP State: UP        Weight: 1
25          Persistence Cookie Value : NSC_wtfswfs-hsq=
               ffffffff096e03ed45525d5f4f58455e445a4a423660
26  1)      Policy : cmp-pol-compress Priority:1
27   Done
28  >
29  <!--NeedCopy-->
```

Binden Sie eine klassische Richtlinie global mit der GUI

Hinweis: Dieses Verfahren dokumentiert das Dialogfeld Globale Bindungen. Abhängig von der Funktion, für die Sie eine Richtlinie global binden möchten, kann die Route, nach der Sie zu diesem Dialogfeld gelangen, unterschiedlich sein.

1. Erweitern Sie im Navigationsbereich das Feature, für das Sie eine klassische Richtlinie global binden möchten, und suchen Sie dann die Richtlinie, die Sie global binden möchten.

   Hinweis: Sie können keine Richtlinien für Content Switching, Cache-Umleitung, SureConnect, Priority Queuing oder
   Citrix Gateway Autorisierung global binden.

2. Klicken Sie im Detailbereich auf Globale Bindungen.
3. Klicken Sie im Dialogfeld<feature name> Richtlinie (en) an Global binden/Unbind-Richtlinie (en) auf **Richtlinie einfügen** .
4. Klicken Sie in der Spalte **Richtlinienname** auf den Namen einer vorhandenen Richtlinie, die Sie global binden möchten, oder klicken Sie auf Neue Richtlinie, um das <feature name> Dialogfeld Richtlinie erstellen zu öffnen.
5. Nachdem Sie die Richtlinie ausgewählt oder eine neue Richtlinie erstellt haben, geben Sie in der Spalte Priorität den Prioritätswert ein.

Je niedriger die Zahl ist, desto früher wird diese Richtlinie im Vergleich zu anderen Richtlinien angewendet. Beispielsweise wird eine Richtlinie mit der Priorität 10 vor einer Richtlinie mit der Priorität 100 angewendet. Sie können dieselbe Priorität für verschiedene Richtlinien verwenden. Alle Features, die klassische Richtlinien verwenden, implementieren nur die erste Richtlinie, mit der eine Verbindung übereinstimmt. Daher ist die Richtlinienpriorität wichtig, um die gewünschten Ergebnisse zu erhalten.

Lassen Sie als bewährte Methode Raum, um Richtlinien hinzuzufügen, indem Sie Prioritäten mit Intervallen von 50 (oder 100) zwischen den einzelnen Richtlinien festlegen.

6. Klicken Sie auf **OK**.

Binden einer klassischen Richtlinie an einen virtuellen Server mit der GUI

1. Erweitern Sie im Navigationsbereich das Feature, das den virtuellen Server enthält, an den Sie eine klassische Richtlinie binden möchten (z. B. wenn Sie eine klassische Richtlinie an einen virtuellen Content Switching-Server binden möchten, erweitern Sie Datenverkehrsverwaltung > Content Switching), und klicken Sie dann auf Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, und klicken Sie dann auf Öffnen.
3. <Feature>Klicken Sie im Dialogfeld Virtuellen Server konfigurieren auf der Registerkarte Richtlinien auf das Feature-Symbol für die gewünschte Typrichtlinie, und klicken Sie dann auf Richtlinie einfügen.
4. Klicken Sie in der Spalte Richtlinienname auf den Namen einer vorhandenen Richtlinie, die Sie an einen virtuellen Server binden möchten, oder klicken Sie auf A, um das <feature name> Dialogfeld Richtlinie erstellen zu öffnen.
5. Nachdem Sie die Richtlinie ausgewählt oder eine neue Richtlinie erstellt haben, legen Sie in der Spalte Priorität die Priorität fest.

   Wenn Sie eine Richtlinie an einen virtuellen Content Switching-Server binden, wählen Sie in der Spalte Ziel einen virtuellen Lastausgleichsserver aus, an den Datenverkehr gesendet werden soll, der der Richtlinie entspricht.

6. Klicken Sie auf **OK**.

Klassische Richtlinien anzeigen

October 5, 2021

Sie können klassische Richtlinien entweder mit dem Konfigurationsdienstprogramm oder der Befehlszeile anzeigen. Sie können Details wie Name, Ausdruck und Bindungen der Richtlinie

anzeigen.

Anzeigen einer klassischen Richtlinie und ihrer Bindungsinformationen mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine klassische Richtlinie und ihre Bindungsinformationen anzuzeigen:

```
show <featureName> policy [policyName]
```

Beispiel

```
> show appfw policy GenericApplicationSSL_
        Name: GenericApplicationSSL_    Rule: ns_only_get_adv
        Profile: GenericApplicationSSL_Prof1    Hits: 0
        Undef Hits: 0
        Policy is bound to following entities
        1) REQ VSERVER app_u_GenericApplicationSSLPortalPages
           PRIORITY : 100
 Done
<!--NeedCopy-->
```

Hinweis: Wenn Sie den Richtliniennamen weglassen, werden alle Richtlinien ohne die Bindungsdetails aufgeführt.

Anzeigen klassischer Richtlinien und Richtlinienbindungen mit der GUI

1. Erweitern Sie im Navigationsbereich das Feature, dessen Richtlinien Sie anzeigen möchten (z. B. wenn Sie Anwendungsfirewall Richtlinien anzeigen möchten, erweitern Sie Anwendungsfirewall), und klicken Sie dann auf Richtlinien.
2. Führen Sie im Detailbereich eine oder mehrere der folgenden Aktionen aus:
   - Klicken Sie auf die Richtlinie, um Details zu einer bestimmten Richtlinie anzuzeigen. Details werden im Bereich Details des Konfigurationsbereichs angezeigt.
   - Um Bindungen für eine bestimmte Richtlinie anzuzeigen, klicken Sie auf die Richtlinie, und klicken Sie dann auf Bindungen anzeigen.
   - Um globale Bindungen anzuzeigen, klicken Sie auf die Richtlinie, und klicken Sie dann auf Globale Bindungen. Beachten Sie, dass Sie keine Richtlinien für Content Switching, Cache-Umleitung, SureConnect, Priority Queuing oder Citrix Gateway Authorization global binden können.

Erstellen von benannten klassischen Ausdrücken

October 5, 2021

Ein benannter klassischer Ausdruck ist ein klassischer Ausdruck, der über einen zugewiesenen Namen referenziert werden kann. Oft müssen Sie klassische Ausdrücke konfigurieren, die groß oder komplex sind und Teil eines größeren zusammengesetzten Ausdrucks sind. Sie können auch klassische Ausdrücke konfigurieren, die häufig und in mehreren zusammengesetzten Ausdrücken oder klassischen Richtlinien verwendet werden müssen. In diesen Szenarien können Sie den gewünschten klassischen Ausdruck erstellen, ihn unter einem Namen Ihrer Wahl speichern und dann über seinen Namen auf den Ausdruck aus zusammengesetzten Ausdrücken oder Richtlinien verweisen. Dies spart Konfigurationszeit und verbessert die Lesbarkeit komplexer zusammengesetzter Ausdrücke. Darüber hinaus müssen Änderungen an einem benannten klassischen Ausdruck nur einmal vorgenommen werden.

Einige benannte Ausdrücke sind integriert, und eine Teilmenge dieser Ausdrücke ist schreibgeschützt. Integrierte benannte Ausdrücke sind in vier Kategorien unterteilt: Allgemein, Anti-Virus, Personal Firewall und Internet Security. Allgemeine benannte Ausdrücke haben eine Vielzahl von Verwendungen. Beispielsweise können Sie aus der Kategorie Allgemein die Ausdrücke ns_true und ns_false verwenden, um den Wert TRUE bzw. FALSE anzugeben, der für den gesamten Datenverkehr zurückgegeben werden soll. Sie können auch Daten eines bestimmten Typs identifizieren (z. B. HTM-, DOC- oder GIF-Dateien), bestimmen, ob Caching-Header vorhanden sind, oder ermitteln, ob die RoundTrip-Zeit für Pakete zwischen einem Client und dem Citrix ADC hoch ist (über 80 Millisekunden).

Anti-Virus, Personal Firewall und Internet Security benannte Ausdrücke testen Clients auf das Vorhandensein eines bestimmten Programms und einer bestimmten Version und werden hauptsächlich in Citrix Gateway Richtlinien verwendet.

Hinweis: Sie können integrierte benannte Ausdrücke nicht ändern oder löschen.

Erstellen eines benannten klassischen Ausdrucks mit der CLI

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

```
1 - add expression <name> <value> [-comment <string>] [-
    clientSecurityMessage <string>]
2 - show expression [<name> | -type CLASSIC
3 <!--NeedCopy-->
```

Beispiel


```
> add expression classic_ne "REQ.HTTP.URL CONTAINS www.example1.com" -
    comment "Checking the URL for www.example1.com"
 Done
> show expression classic_ne
1)      Name: classic_ne  Expr: REQ.HTTP.URL CONTAINS www.example1.com
     Hits: 0 Type : CLASSIC
        Comment: "Checking the URL for www.example1.com"
 Done
>
<!--NeedCopy-->
```

Erstellen eines benannten klassischen Ausdrucks mit der GUI

1. Erweitern Sie im Navigationsbereich AppExpert, erweitern Sie Ausdrücke, und klicken Sie dann auf Klassische Ausdrücke.
2. Klicken Sie im Detailbereich auf "Hinzufügen".

   Hinweis: Einige der integrierten Ausdrücke in der Liste Ausdrücke sind schreibgeschützt.
3. Geben Sie im Dialogfeld Richtlinienausdruck erstellen Werte für die folgenden Parameter an:

   - Ausdrucksname* — Name
   - Client-Sicherheitsmeldung — ClientSecurityMessage
   - Kommentare—comment

   * Ein erforderlicher Parameter
4. Führen Sie einen der folgenden Schritte aus, um den Ausdruck zu erstellen:

   - Sie können die Eingaben für diesen Ausdruck in der Dropdownliste Benannte Ausdrücke auswählen.
   - Sie können einen neuen Ausdruck erstellen, wie unter Hinzufügen eines Ausdrucks für eine klassische Richtlinie über die grafische Benutzeroberflächebeschrieben.
5. Wenn Sie fertig sind, klicken Sie auf **Schließen**. Stellen Sie sicher, dass der neue Ausdruck erstellt wurde, indem Sie zum Ende der Liste Klassische Ausdrücke scrollen, um ihn anzuzeigen.

Ausdrücke verweisen auf erweiterte Richtlinienausdrücke

October 5, 2021

> **Warnung**
>
> Q- und S-Präfixe sind ab Citrix ADC 12.0 Build 56.20 veraltet und werden in erweiterten Richtlinienausdrücken nicht mehr unterstützt.

Die folgende Tabelle enthält eine Auflistung der Standard-Syntaxausdruckpräfixe mit Querverweisen auf Beschreibungen dieser Präfixe und die Operatoren, die Sie für sie angeben können. Beachten Sie, dass einige Präfixe mit mehreren Operatortypen arbeiten können. Beispielsweise kann ein Cookie mithilfe von Operatoren für Text oder Operatoren für HTTP-Header analysiert werden.

Sie können jedes Element in den folgenden Tabellen selbst als vollständiger Ausdruck verwenden, oder Sie können verschiedene Operatoren verwenden, um diese Ausdruckselemente mit anderen zu kombinieren, um komplexere Ausdrücke zu bilden.

Hinweis: Die Spalte Beschreibung in der folgenden Tabelle enthält Querverweise auf zusätzliche Informationen zur Präfixverwendung und den entsprechenden Operatoren für das Präfix.

Weitere Informationen finden Sie unter Expression PDF, um die Tabelle anzuzeigen.

Ausdrücke referenz-klassische Ausdrücke

October 5, 2021

> **Warnung**
>
> Klassische Richtlinienausdrücke werden ab Citrix ADC 12.0 Build 56.20 nicht mehr unterstützt. Alternativ empfiehlt Citrix die Verwendung von erweiterten Richtlinien. Weitere Informationen finden Sie unter Erweiterte Richtlinien

Die Unterthemen, die im Inhaltsverzeichnis auf der linken Seite des Bildschirms aufgeführt sind, enthalten Tabellen mit den klassischen Citrix ADC Ausdrücken.

In der Operatortabelle wird der Ergebnistyp jedes Operators am Anfang der Beschreibung angezeigt. In den anderen Tabellen wird die Ebene jedes Ausdrucks am Anfang der Beschreibung angezeigt. Bei benannten Ausdrücken wird jeder Ausdruck als Ganzes angezeigt.

Operatoren

Ausdruckselement	Beschreibung
==	Boolescher Wert. Gibt TRUE zurück, wenn der aktuelle Ausdruck dem Argument entspricht. Bei Textoperationen müssen die zu vergleichenden Elemente genau übereinstimmen. Bei numerischen Operationen müssen die Elemente auf die gleiche Zahl ausgewertet werden.
!=	Boolescher Wert. Gibt TRUE zurück, wenn der aktuelle Ausdruck dem Argument nicht entspricht. Bei Textoperationen dürfen die zu vergleichenden Elemente nicht genau übereinstimmen. Bei numerischen Operationen dürfen die Elemente nicht auf dieselbe Zahl ausgewertet werden.
CONTAINS	Boolescher Wert. Gibt TRUE zurück, wenn der aktuelle Ausdruck die Zeichenfolge enthält, die im Argument angegeben ist.
NOTCONTAINS	Boolescher Wert. Gibt TRUE zurück, wenn der aktuelle Ausdruck nicht die Zeichenfolge enthält, die im Argument angegeben ist.
CONTENTS	Text. Gibt den Inhalt des aktuellen Ausdrucks zurück.
EXISTS	Boolescher Wert. Gibt TRUE zurück, wenn das vom aktuellen Ausdruck angegebene Element vorhanden ist.
NOTEXISTS	Boolescher Wert. Gibt TRUE zurück, wenn das vom aktuellen Ausdruck angegebene Element nicht vorhanden ist.
>	Boolescher Wert. Gibt TRUE zurück, wenn der aktuelle Ausdruck zu einer Zahl ausgewertet wird, die größer als das Argument ist.
<	Boolescher Wert. Gibt TRUE zurück, wenn der aktuelle Ausdruck zu einer Zahl ausgewertet wird, die kleiner als das Argument ist.

Ausdruckselement	Beschreibung
>=	Boolescher Wert. Gibt TRUE zurück, wenn der aktuelle Ausdruck eine Zahl ergibt, die größer oder gleich dem Argument ist.
<=	Boolescher Wert. Gibt TRUE zurück, wenn der aktuelle Ausdruck eine Zahl ergibt, die kleiner oder gleich dem Argument ist.

Allgemeine Ausdrücke

Ausdruckselement	Definition
REQ	Strömungsart. Funktioniert auf eingehenden (oder anfordernden) Paketen.
REQ.HTTP	-Protokoll. Funktioniert auf HTTP-Anforderungen.
REQ.HTTP.METHOD	Qualifikator. Gibt die HTTP-Methode an.
REQ.HTTP.URL	Qualifikator. Gibt die URL an.
REQ.HTTP.URLTOKENS	Qualifikator. Gibt das URL-Token an.
REQ.HTTP.VERSION	Qualifikator. Gibt die HTTP-Version an.
REQ.HTTP.HEADER	Qualifikator. Gibt den HTTP-Header an.
REQ.HTTP.URLLEN	Qualifikator. Gibt die Anzahl der Zeichen in der URL an.
REQ.HTTP.URLQUERY	Qualifikator. Gibt den Abfrageteil der URL an.
REQ.HTTP.URLQUERYLEN	Qualifikator. Gibt die Länge des Abfrageabschnitts der URL an.
REQ.SSL	-Protokoll. Funktioniert auf SSL-Anfragen.
REQ.SSL.CLIENT.CERT	Qualifikator. Gibt das gesamte Clientzertifikat an.
REQ.SSL.CLIENT.CERT.SUBJECT	Qualifikator. Gibt den Betreff des Clientzertifikats an.
REQ.SSL.CLIENT.CERT.ISSUER	Qualifikator. Gibt den Aussteller des Clientzertifikats an.
REQ.SSL.CLIENT.CERT.SIGALGO	Qualifikator. Gibt den Validierungsalgorithmus an, der vom Clientzertifikat verwendet wird.

Ausdruckselement	Definition
REQ.SSL.CLIENT.CERT.VERSION	Qualifikator. Gibt die Clientzertifikatversion an.
REQ.SSL.CLIENT.CERT.VALIDFROM	Qualifikator. Gibt das Datum an, vor dem das Clientzertifikat ungültig ist.
REQ.SSL.CLIENT.CERT.VALIDTO	Qualifikator. Gibt das Datum an, nach dem das Clientzertifikat ungültig ist.
REQ.SSL.CLIENT.CERT.SERIALNUMBER	Qualifikator. Gibt die Seriennummer des Clientzertifikats an.
REQ.SSL.CLIENT.CIPHER.TYPE	Qualifikator. Gibt das vom Client verwendete Verschlüsselungsprotokoll an.
REQ.SSL.CLIENT.CIPHER.BITS	Qualifikator. Gibt die Anzahl der Bits an, die vom SSL-Schlüssel des Clients verwendet werden.
REQ.SSL.CLIENT.SSL.VERSION	Qualifikator. Gibt die vom Client verwendete SSL-Version an.
REQ.TCP	-Protokoll. Funktioniert mit eingehenden TCP-Paketen.
REQ.TCP.SOURCEPORT	Qualifikator. Gibt den Quellport des eingehenden Pakets an.
REQ.TCP.DESTPORT	Qualifikator. Gibt den Zielport des eingehenden Pakets an.
REQ.IP	-Protokoll. Funktioniert mit eingehenden IP-Paketen.
REQ.IP.SOURCEIP	Qualifikator. Gibt die Quell-IP des eingehenden Pakets an.
REQ.IP.DESTIP	Qualifizier.Gibt die Ziel-IP des eingehenden Pakets an.
RES	Strömungsart. Funktioniert mit ausgehenden (oder Antwortpaketen) Paketen.
RES.HTTP	-Protokoll. Funktioniert mit HTTP-Antworten.
RES.HTTP.VERSION	Qualifikator. Gibt die HTTP-Version an.
RES.HTTP.HEADER	Qualifikator. Gibt den HTTP-Header an.
RES.HTTP.STATUSCODE	Qualifikator. Gibt den Statuscode der HTTP-Antwort an.

Ausdruckselement	Definition
RES.TCP	-Protokoll. Funktioniert mit eingehenden TCP-Paketen.
RES.TCP.SOURCEPORT	Qualifikator. Gibt den Quellport des ausgehenden Pakets an.
RES.TCP.DESTPORT	Qualifikator. Gibt den Zielport des ausgehenden Pakets an.
RES.IP	-Protokoll. Funktioniert mit ausgehenden IP-Paketen.
RES.IP.SOURCEIP	Qualifikator. Gibt die Quell-IP des ausgehenden Pakets an. Dies kann im IPv4- oder IPv6-Format vorliegen. Beispiel: add expr exp3 “sourceip == 10.102.32.123 –netmask 255.255.255.0 && destip == 2001::23/120”.
RES.IP.DESTIP	Qualifikator. Gibt die Ziel-IP des ausgehenden Pakets an.

Client-Sicherheitsausdrücke

Die Ausdrücke zum Konfigurieren der Clienteinstellungen auf dem Access Gateway mit der folgenden Software:

- Antivirus
- Persönliche Firewall
- Anti-Spam
- Internet-Sicherheit

Beispiel: Verwendung finden Sie unterhttp://support.citrix.com/article/CTX112599.

Tatsächlicher Ausdruck	Definition
CLIENT.APPLICATION.AV(<NAME>.VERSION == <VERSION>)	Überprüft, ob der Client das dafür vorgesehene Antivirenprogramm und -version ausführt.
CLIENT.APPLICATION.AV(<NAME>.VERSION != <VERSION>)	Überprüft, ob der Client das angegebene Antivirenprogramm und -version nicht ausführt.
CLIENT.APPLICATION.PF(<NAME>.VERSION == <VERSION>)	Überprüft, ob der Client das angegebene Personal Firewall-Programm und -Version ausführt.

Tatsächlicher Ausdruck	Definition
CLIENT.APPLICATION.PF(<NAME>.VERSION != <VERSION>)	Überprüft, ob der Client nicht das angegebene Personal Firewall-Programm und -Version ausführt.
CLIENT.APPLICATION.IS(<NAME>.VERSION == <VERSION>)	Überprüft, ob der Client das dafür vorgesehene Internet-Sicherheitsprogramm und -version ausführt.
CLIENT.APPLICATION.IS(<NAME>.VERSION != <VERSION>)	Überprüft, ob der Client nicht das dafür vorgesehene Internet-Sicherheitsprogramm und -version ausführt.
CLIENT.APPLICATION.AS(<NAME>.VERSION == <VERSION>)	Überprüft, ob der Client das angegebene Anti-Spam-Programm und -Version ausführt.
CLIENT.APPLICATION.AS(<NAME>.VERSION != <VERSION>)	Überprüft, ob der Client das angegebene Anti-Spam-Programm und -Version nicht ausführt.

Netzwerkbasierte Ausdrücke

Ausdruck	Definition
REQ	Strömungsart. Funktioniert bei eingehenden oder anfordernden Paketen.
REQ.VLANID	Qualifikator. Funktioniert mit der virtuellen LAN (VLAN) ID.
REQ.INTERFACE.ID	Qualifikator. Funktioniert mit der ID der angegebenen Citrix ADC Schnittstelle.
REQ.INTERFACE.RXTHROUGHPUT	Qualifikator. Funktioniert mit dem rohen empfangenen Paketdurchsatz der designierten Citrix ADC Schnittstelle.
REQ.INTERFACE.TXTHROUGHPUT	Qualifikator. Funktioniert mit dem rohen übertragenen Paketdurchsatz der designierten Citrix ADC Schnittstelle.
REQ.INTERFACE.RXTXTHROUGHPUT	Qualifikator. Funktioniert mit dem rohen empfangenen und übertragenen Paketdurchsatz der designierten Citrix ADC Schnittstelle.

Ausdruck	Definition
REQ.ETHER.SOURCEMAC	Qualifikator. Arbeitet auf der Quell-MAC-Adresse.
REQ.ETHER.DESTMAC	Qualifikator. Arbeitet auf der Ziel-MAC-Adresse.
RES	Strömungsart. Funktioniert mit ausgehenden (oder Antwortpaketen) Paketen.
RES.VLANID	Qualifikator. Funktioniert mit der virtuellen LAN (VLAN) ID.
RES.INTERFACE.ID	Qualifikator. Funktioniert mit der ID der angegebenen Citrix ADC Schnittstelle.
RES.INTERFACE.RXTHROUGHPUT	Qualifikator. Funktioniert mit dem rohen empfangenen Paketdurchsatz der designierten Citrix ADC Schnittstelle.
RES.INTERFACE.TXTHROUGHPUT	Qualifikator. Funktioniert mit dem rohen übertragenen Paketdurchsatz der designierten Citrix ADC Schnittstelle.
RES.INTERFACE.RXTXTHROUGHPUT	Qualifikator. Funktioniert mit dem rohen empfangenen und übertragenen Paketdurchsatz der designierten Citrix ADC Schnittstelle.
RES.ETHER.SOURCEMAC	Qualifikator. Arbeitet auf der Quell-MAC-Adresse.
RES.ETHER.DESTMAC	Qualifikator. Arbeitet auf der Ziel-MAC-Adresse.

Datum/Uhrzeit Ausdrücke

Ausdruck	Definition
TIME	Qualifikator. Funktioniert am Datum und Uhrzeit des Tages, GMT.
DATUM	Qualifikator. Funktioniert am Datum, GMT.
DAYOFWEEK	Funktioniert am angegebenen Tag in der Woche, GMT.

Dateisystemausdrücke

Sie können Dateisystemausdrücke in Autorisierungsrichtlinien für Benutzer und Gruppen angeben, die über das Citrix Gateway Dateiübertragungsprogramm (VPN-Portal) auf die Dateifreigabe zugreifen. Diese Ausdrücke funktionieren mit der Citrix Gateway Dateiübertragungsautorisierungsfunktion, um den Benutzerzugriff auf Dateiserver, Ordner und Dateien zu steuern. Sie können diese Ausdrücke beispielsweise in Autorisierungsrichtlinien verwenden, um den Zugriff basierend auf Dateityp und -größe zu steuern.

Weitere Informationen finden Sie im PDF zum Dateinamenausdruck .

Hinweis: Dateisystemausdrücke unterstützen keine regulären Ausdrücke.

Integrierte benannte Ausdrücke (Allgemein)

Ausdruck	Definition
ns_all_apps_ncomp	Tests für Verbindungen mit Zielports zwischen 0 und 65535. Mit anderen Worten, Tests für alle Anwendungen.
ns_cachecontrol_nocache	Tests auf Verbindungen mit einem HTTP-Cache-Control-Header, der den Wert no-cache enthält.
ns_cachecontrol_nostore	Tests auf Verbindungen mit einem HTTP-Cache-Control-Header, der den Wert no-store enthält.
ns_cmpclient	Testet den Client, um festzustellen, ob er komprimierte Inhalte akzeptiert.
ns_content_type	Tests auf Verbindungen mit einem HTTP-Content-Type-Header, der Text enthält.
ns_css	Tests auf Verbindungen mit einem HTTP-Content-Type-Header, der text/css enthält.
ns_ext_asp	Testet auf HTTP-Verbindungen zu allen URLs, die die Zeichenfolge ASP- mit anderen Worten, jede Verbindung zu einer aktiven Serverseite (ASP) enthält.
ns_ext_cfm	Tests auf HTTP-Verbindungen zu jeder URL, die die Zeichenfolge .cfm enthält

Ausdruck	Definition
ns_ext_cgi	Tests auf HTTP-Verbindungen zu jeder URL, die die Zeichenfolge .cgi enthält, d. h. jede Verbindung zu einem CGI-Skript (Common Gateway Interface).
ns_ext_ex	Tests auf HTTP-Verbindungen zu jeder URL, die die Zeichenfolge .ex enthält
ns_ext_exe	Testet auf HTTP-Verbindungen zu jeder URL, die die Zeichenfolge EXE enthält, d. h. jede Verbindung zu einer ausführbaren Datei.
ns_ext_htx	Tests auf HTTP-Verbindungen zu jeder URL, die die Zeichenfolge .htx enthält
ns_ext_not_gif	Tests auf HTTP-Verbindungen zu allen URLs, die nicht die Zeichenfolge GIF enthalten, d. h. jede Verbindung zu einer URL, die kein GIF-Bild ist.
ns_ext_not_jpeg	Testet auf HTTP-Verbindungen zu allen URLs, die nicht die Zeichenfolge JPEG enthalten, d. h. jede Verbindung zu einer URL, die kein JPEG-Bild ist.
ns_ext_shtml	Tests auf HTTP-Verbindungen zu jeder URL, die die Zeichenfolge .shtml enthält, d. h. jede Verbindung zu einer vom Server analysierten HTML-Seite.
ns_false	Gibt immer den Wert FALSE zurück.

Ausdruck	Definition
ns_farclient	Der Client befindet sich in einer anderen geografischen Region als der Citrix ADC, wie er durch die geografische Region in der IP-Adresse des Clients bestimmt wird. Folgende Regionen sind vordefiniert: 192.0.0.0 – 193.255.255.255: Multi-regional, 194.0.0.0 – 195.255.255.255: European Union, 196.0.0.0 – 197.255.255.255: Other1, 198.0.0.0 – , 199.255.255.255: North America, 200.0.0.0 – 201.255.255.255: Central and South America, 202.0.0.0 – 203.255.255.255: Pacific Rim, 204.0.0.0 – 205.255.255.255: Other2, and 206.0.0.0 – 207.255.255.255: Other3
ns_header_cookie	Tests auf HTTP-Verbindungen, die einen Cookie-Header enthalten.
ns_header_pragma	Tests auf HTTP-Verbindungen, die einen Pragma: no-cache-Header enthalten.
ns_mozilla_47	Tests auf HTTP-Verbindungen, deren User-Agent-Header die Zeichenfolge Mozilla/4.7 enthält, d. h. jede Verbindung von einem Client über den Mozilla 4.7-Webbrowser.
ns_msexcel	Tests auf HTTP-Verbindungen, deren Content-Type-Header die Zeichenfolge application/vnd.msexcel- mit anderen Worten, jede Verbindung, die eine Microsoft Excel-Kalkulationstabelle übertragen.
ns_msie	Tests auf HTTP-Verbindungen, deren User-Agent-Header die Zeichenfolge MSIE enthält, d. h. jede Verbindung von einem Client, die eine beliebige Version des Internet Explorer-Webbrowsers verwendet.
ns_msppt	Tests auf HTTP-Verbindungen, deren Content-Type-Header die Zeichenfolge application/vnd.ms-powerpoint enthält, d. h. jede Verbindung, die eine Microsoft PowerPoint-Datei sendet.

Ausdruck	Definition
ns_msword	Tests auf HTTP-Verbindungen, deren Content-Type-Header die Zeichenfolge application/vnd.msword enthält, d. h. jede Verbindung, die eine Microsoft Word-Datei sendet.
ns_non_get	Tests für HTTP-Verbindungen, die eine beliebige HTTP-Methode außer GET verwenden.
ns_slowclient	Gibt TRUE zurück, wenn die durchschnittliche Roundtrip Zeit zwischen dem Client und dem Citrix ADC mehr als 80 Millisekunden beträgt.
ns_true	Gibt TRUE für den gesamten Datenverkehr zurück.
ns_url_path_bin	Prüft den URL-Pfad, um zu sehen, ob er auf das Verzeichnis /bin/ verweist.
ns_url_path_cgibin	Prüft den URL-Pfad, um zu sehen, ob er auf das CGI-BIN-Verzeichnis verweist.
ns_url_path_exec	Prüft den URL-Pfad, um zu sehen, ob er auf das Verzeichnis /exec/verweist.
ns_url_token	Tests auf das Vorhandensein von URL-Tokens.
ns_xmldata	Tests auf das Vorhandensein von XML-Daten.

Integrierte benannte Ausdrücke (Anti-Virus)

Ausdruck	Definition
McAfee Virensuche 11	Prüft, ob auf dem Client die neueste Version von McAfee VirusScan ausgeführt wird.
McAfee Antivirus	Prüft, ob auf dem Client eine beliebige Version von McAfee Antivirus ausgeführt wird.
Symantec AntiVirus 10 (mit aktualisierten Definitionsdatei)	Prüft, ob auf dem Client die aktuellste Version von Symantec AntiVirus ausgeführt wird.
Symantec AntiVirus 6.0	Prüft, ob auf dem Client Symantec AntiVirus 6.0 ausgeführt wird.

Ausdruck	Definition
Symantec AntiVirus 7.5	Prüft, ob auf dem Client Symantec AntiVirus 7.5 ausgeführt wird.
TrendMicro OfficeScan 7.3	Prüft, ob auf dem Client OfficeScan Version 7.3 von Trend Microsystems ausgeführt wird.
TrendMicro AntiVirus 11.25	Prüft, ob auf dem Client AntiVirus von Trend Microsystems, Version 11.25, ausgeführt wird.
Sophos Antivirus 4	Prüft, ob auf dem Client Sophos Antivirus, Version 4 ausgeführt wird.
Sophos Antivirus 5	Prüft, ob auf dem Client Sophos Antivirus, Version 5 ausgeführt wird.
Sophos Antivirus 6	Prüft, ob auf dem Client Sophos Antivirus, Version 6 ausgeführt wird.

Integrierte benannte Ausdrücke (Personal Firewall)

Ausdruck	Definition
TrendMicro OfficeScan 7.3	Prüft, ob auf dem Client OfficeScan Version 7.3 von Trend Microsystems ausgeführt wird.
Sygate Personal Firewall 5.6	Prüft, ob auf dem Client die Sygate Personal Firewall, Version 5.6, ausgeführt wird.
ZoneAlarm Personal Firewall 6.5	Prüft, ob auf dem Client die ZoneAlarm Personal Firewall, Version 6.5, ausgeführt wird.

Integrierte benannte Ausdrücke (Client Security)

Ausdruck	Definition
Norton-Internet-Sicherheit	Prüft, ob auf dem Client eine Version von Norton Internet Security ausgeführt wird.

Zusammenfassende Beispiele für Standard-Syntaxausdrücke und -richtlinien

October 5, 2021

Die folgende Tabelle enthält Beispiele für Standardsyntax Ausdrücke, die Sie als Grundlage für eigene Standardsyntax verwenden können.

Tabelle 1. Beispiele für Standard-Syntaxausdrücke

Ausdruckstyp	Beispielausdrücke
Sehen Sie sich die Methode an, die in der HTTP-Anforderung verwendet wird.	`http.req.method.eq(post)http.req.method.eq(get)`

Überprüfen Sie den Cache-Control- oder Pragma-Header-Wert in einer HTTP-Anforderung (req) oder Antwort (res).	`http.req.header("Cache-Control").contains("no-store")`
	`http.req.header("Cache-Control").contains("no-cache")`
	`http.req.header("Pragma").contains("no-cache")`
	`http.res.header("Cache-Control").contains("private")`
	`http.res.header("Cache-Control").contains("public")`
	`http.res.header("Cache-Control").contains("must-revalidate")http.res.header("Cache-Control").contains ("proxy-revalidate")`
	`http.res.header("Cache-Control").contains("max-age")`

Überprüfen Sie, ob ein Header in einer Anfrage (req) oder Antwort (res) vorhanden ist.	`http.req.header("myHeader").exists` `http.res.header("myHeader").exists`

Ausdruckstyp	Beispielausdrücke
Suchen Sie in einer HTTP-Anforderung basierend auf der Dateierweiterung nach einem bestimmten Dateityp.	`http.req.url.contains(".html")http.req.url.contains(".cgi")http.req.url.contains(".asp")http.req.url.contains(".exe")http.req.url.contains(".cfm")http.req.url.contains(".ex")http.req.url.contains(".shtml")http.req.url.contains(".htx")http.req.url.contains("/cgi-bin/")http.req.url.contains("/exec/")http.req.url.contains("/bin/")`
Suchen Sie in einer HTTP-Anforderung nach allem, was außer einem bestimmten Dateityp ist.	`http.req.url.contains(".png").not; http.req.url.contains(".jpeg").not`
Überprüfen Sie den Dateityp, der in einer HTTP-Antwort gesendet wird, basierend auf dem Content-Type-Header.	`http.res.header("Content-Type").contains("text")http.res.header("Content-Type").contains "application/msword")http.res.header("Content-Type").contains("vnd.ms-excel")http.res.header("Content-Type").contains("application/vnd.ms-powerpoint"); http.res.header("Content-Type").contains("text/css"); http.res.header("Content-Type").contains("text/xml"); http.res.header("Content-Type").contains("image/")`
Überprüfen Sie, ob diese Antwort einen Ablaufheader enthält.	`http.res.header("Expires").exists`
Überprüfen Sie in einer Antwort auf einen Set-Cookie-Header.	`http.res.header("Set-Cookie").exists`
Überprüfen Sie den Agenten, der die Antwort gesendet hat.	`http.res.header("User-Agent").contains("Mozilla/4.7")http.res.header("User-Agent").contains("MSIE")`

Ausdruckstyp	Beispielausdrücke
Überprüfen Sie, ob die ersten 1024 Bytes des Body einer Anfrage mit der Zeichenfolge “some text” beginnen.	`http.req.body(1024).contains(”some text”)`

Die folgende Tabelle zeigt Beispiele für Richtlinienkonfigurationen und Bindungen für häufig verwendete Funktionen.

Tabelle 2. Beispiele für Standard-Syntaxausdrücke und -richtlinien

Zweck	Beispiel
Verwenden Sie die Funktion Umschreiben, um Vorkommen von `http://with https://` im Textkörper einer HTTP-Antwort zu ersetzen.	`add rewrite action httpRewriteAction replace_all http.res.body(50000)”\”https://\””-pattern http://add rewrite policy demo_rep34312 ”http.res.body(50000).contains(\”http://\”)” httpRewriteAction`
Ersetzen Sie alle Vorkommen von “abcd” durch “1234” in den ersten 1000 Bytes des HTTP-Body.	`add rewrite action abcdTo1234Action replace_all ”http.req.body(1000)”” \”1234\””-pattern abcd add rewrite policy abcdTo1234Policy ”http.req.body(1000).contains(\”abcd\”)” abcdTo1234Action bind rewrite global abcdTo1234Policy 100 END -type REQ_OVERRIDE`
Herabstufen der HTTP-Version auf 1.0, um zu verhindern, dass der Server HTTP-Antworten abschottet.	`add rewrite action downgradeTo1.0Action replace http.req.version.minor ”\”0\””add rewrite policy downgradeTo1.0Policy ”http.req.version.minor.eq(1)”downgradeTo1.0Action bind lb vserver myLBVserver -policyName downgradeTo1.0Policy -priority 100 -gotoPriorityExpression NEXT -type REQUEST`

Zweck	Beispiel
Entfernen Sie Verweise auf das HTTP- oder HTTPS-Protokoll in allen Antworten, sodass, wenn die Verbindung des Benutzers HTTP ist, die Verknüpfung mithilfe von HTTP geöffnet wird und wenn die Verbindung des Benutzers HTTPS ist, die Verknüpfung mithilfe von HTTPS geöffnet wird.	`add rewrite action remove_http_https replace_all "http.res.body(1000000).set_text_mode(ignorecase)""\"//\""-pattern "re~https?://|HTTPS?://~"add rewrite policy remove_http_https true remove_http_https bind lb vserver test_vsvr -policyName remove_http_https -priority 20 -gotoPriorityExpression NEXT -type RESPONSE`
Instanzen von http: in https: in allen URLs neu schreiben.	`add responder action httpToHttpsAction redirect "\"https://\" + http.req.hostname + http.req.url"-bypassSafetyCheck YES add responder policy httpToHttpsPolicy "!CLIENT.SSL.IS_SSL" httpToHttpsAction bind responder global httpToHttpsPolicy 1 END -type OVERRIDE`
Ändern Sie eine URL, um von URL A zu URL B umzuleiten. In diesem Beispiel wird “file5.html” an den Pfad angehängt.	`add responder action appendFile5Action redirect \"http://\" + http.req.hostname + http.req.url + \"/file5.html\""-bypassSafetyCheck YES add responder policy appendFile5Policy "http.req.url.eq(\"/testsite\")" appendFile5Action bind responder global appendFile5Policy 1 END -type OVERRIDE`

Zweck	Beispiel
Umleiten einer externen URL zu einer internen URL.	`add rewrite action act_external_to_internal REPLACE 'http.req.hostname.server''”www.my.host.com”'add rewrite policy pol_external_to_internal 'http.req.hostname.server.eq(”www.external.host.com”)'act_external_to_internal bind rewrite global pol_external_to_internal 100 END -type REQ_OVERRIDE`
Umleiten von Anforderungen an www.example.com, die eine Abfragezeichenfolge haben, an www.webn.example.com. Der Wert n wird von einem Serverparameter in der Abfragezeichenfolge abgeleitet, z. B. server=5.	`add rewrite action act_redirect_query REPLACE q##http.req.header(”Host”).before_str(”.example.com”)''”Web”+ http.req.url.query.value(”server”)## add rewrite policy pol_redirect_query q##http.req.header(”Host”).eq(”www.example.com”)&& http.req.url.contains(”?”)'act_redirect_query##`
Begrenzen Sie die Anzahl der Anfragen pro Sekunde von einer URL.	`add ns limitSelector ip_limit_selector http.req.url ”client.ip.src”add ns limitIdentifier ip_limit_identifier -threshold 4 -timeSlice 3600 -mode request_rate -limitType smooth -selectorName ip_limit_selector add responder action my_Web_site_redirect_action redirect ”\”http://www.mycompany.com/\””add responder policy ip_limit_responder_policy ”http.req.url.contains(\”myasp.asp\”)&& sys.check_limit (\”ip_limit_identifier\”)”my_Web_site_redirect_action bind responder global ip_limit_responder_policy 100 END -type default`

Zweck	Beispiel
Überprüfen Sie die Client-IP-Adresse, aber übergeben Sie die Anforderung, ohne die Anforderung zu ändern.	`add rewrite policy check_client_ip_policy 'HTTP.REQ. HEADER (”x-forwarded-for”).EXISTS HTTP.REQ.HEADER (”client-ip”). EXISTS'NOREWRITE bind rewrite global check_client_ip_policy 100 END`
Entfernen Sie alte Header aus einer Anforderung und fügen Sie einen NS-Client-Header ein.	`add rewrite action del_x_forwarded_for delete_http_header x-forwarded-for add rewrite action del_client_ip delete_http_header client-ip add rewrite policy check_x_forwarded_for_policy 'HTTP. REQ.HEADER(”x-forwarded-for”). EXISTS'del_x_forwarded_for add rewrite policy check_client_ip_policy 'HTTP.REQ. HEADER(”client-ip”).EXISTS' del_client_ip add rewrite action insert_ns_client_header insert_http_header NS-Client ' CLIENT.IP.SRC'add rewrite policy insert_ns_client_policy 'HTTP.REQ. HEADER(”x-forwarded-for”).EXISTS HTTP.REQ.HEADER(”client-ip”).EXISTS 'insert_ns_client_header bind rewrite global check_x_forwarded_for_policy 100 200 bind rewrite global check_client_ip_policy 200 300 bind rewrite global insert_ns_client_policy 300 END`

Zweck	Beispiel
Entfernen Sie alte Header aus einer Anforderung, fügen Sie einen NS-Client-Header ein, und ändern Sie dann die Aktion “Header einfügen”, sodass der Wert des eingefügten Headers die Client-IP-Werte aus den alten Headern und der Verbindungs-IP-Adresse der Citrix ADC Appliance enthält. Beachten Sie, dass in diesem Beispiel das vorherige Beispiel wiederholt wird, mit Ausnahme der Aktion zum Umschreiben des endgültigen Satzes.	`add rewrite action del_x_forwarded_for delete_http_header x-forwarded-for add rewrite action del_client_ip delete_http_header client-ip add rewrite policy check_x_forwarded_for_policy 'HTTP.REQ.HEADER(”x-forwarded-for”).EXISTS'del_x_forwarded_for add rewrite policy check_client_ip_policy 'HTTP.REQ.HEADER(”client-ip”).EXISTS' del_client_ip add rewrite action insert_ns_client_header insert_http_header NS-Client 'CLIENT.IP.SRC'add rewrite policy insert_ns_client_policy 'HTTP.REQ.HEADER(”x-forwarded-for”).EXISTS HTTP.REQ.HEADER(”client-ip”).EXISTS 'insert_ns_client_header bind rewrite global check_x_forwarded_for_policy 100 200 bind rewrite global check_client_ip_policy 200 300 bind rewrite global insert_ns_client_policy 300 END set rewrite action insert_ns_client_header -stringBuilderExpr 'HTTP.REQ.HEADER(”x-forwarded-for”).VALUE(0)+ ” ” + HTTP.REQ.HEADER(”client-ip”).VALUE(0)+ ” ” + CLIENT.IP.SRC'-bypassSafetyCheck YES`

Tutorialbeispiele für Standard-Syntaxrichtlinien für das Umschreiben

October 5, 2021

Mit der Funktion Umschreiben können Sie einen beliebigen Teil eines HTTP-Headers ändern, und für Antworten können Sie den HTTP-Hauptteil ändern. Sie können diese Funktion verwenden, um mehrere nützliche Aufgaben auszuführen, z. B. das Entfernen unnötiger HTTP-Header, das Maskieren interner URLs, das Umleiten von Webseiten und das Umleiten von Abfragen oder Schlüsselwörtern.

In den folgenden Beispielen erstellen Sie zunächst eine Umschreibaktion und eine Umschreibrichtlinie. Dann binden Sie die Richtlinie global.

Dieses Dokument enthält die folgenden Details:

- Umleiten einer externen URL zu einer internen URL
- Umleiten einer Abfrage
- Umschreiben von HTTP in HTTPS
- Entfernen unerwünschter Kopfzeilen
- Reduzieren von Webserver-Weiterleitungen
- Maskieren des Server-Headers
- Konvertieren von Klartext in eine URL-codierte Zeichenfolge und auf entgegengesetzte Weise

Weitere Informationen zu den Befehlen und Syntaxbeschreibungen finden Sie auf der Seite "Befehlsreferenz umschreiben".

Umleiten einer externen URL zu einer internen URL

In diesem Beispiel wird beschrieben, wie Sie eine Umschreibaktion erstellen und eine Richtlinie neu schreiben, die eine externe URL an eine interne URL umleitet. Sie erstellen eine Aktion namens act_external_to_internal, die das Umschreiben durchführt. Anschließend erstellen Sie eine Richtlinie namens pol_external_to_internal.

So leiten Sie eine externe URL über die Befehlszeilenschnittstelle an eine interne URL um

- Um die Umschreibungsaktion zu erstellen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
add rewrite action act_external_to_internal REPLACE "http.req.hostname.
server" "\" host_name_of_internal_Web_server\" "
```

- Um die Richtlinie zum Umschreiben zu erstellen, geben Sie an der Citrix ADC Eingabeaufforderung Folgendes ein:

```
add rewrite policy pol_external_to_internal "http.req.hostname.server.eq(\"
host_name_of_external_Web_server\")"act_external_to_internal
```


- Binden Sie die Richtlinie global.

So leiten Sie eine externe URL mit dem Konfigurationsdienstprogramm an eine interne URL um

1. Navigieren Sie zu **AppExpert** > **Umschreiben** > **Aktionen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Rewrite Action erstellen** den Namen act_external_to_internal ein.
4. Um den Hostnamen des HTTP-Servers durch den internen Servernamen zu **ersetzen, wählen Sie im Listenfeld Typ die Option Ersetzen** aus.
5. Geben Sie im Feld Header-Name **Host**ein.
6. Geben Sie im Zeichenfolgenausdruck für ein Ersetzungstextfeld den internen Hostnamen Ihres Webservers ein.
7. Klicken Sie auf **Create** und dann auf **Close**.
8. Klicken Sie im Navigationsbereich auf **Richtlinien**.
9. Klicken Sie im Detailbereich auf **Hinzufügen**.
10. Geben Sie im Feld Name pol_external_to_internal ein. Diese Richtlinie erkennt Verbindungen zum Webserver.
11. **Wählen Sie im Dropdownmenü Aktion die Aktion act_external_to_internal aus.**
12. Erstellen Sie im Ausdrucksеditor den folgenden Ausdruck:

```
HTTP.REQ.HOSTNAME.SERVER.EQ("www.example.com")
<!--NeedCopy-->
```

1. Binden Sie Ihre neue Richtlinie global.

Umleiten einer Abfrage

In diesem Beispiel wird beschrieben, wie eine Umschreibungsaktion und eine Umschreibungsrichtlinie erstellt wird, die eine Abfrage an die richtige URL umleitet. Im Beispiel wird davon ausgegangen, dass die Anforderung einen Host-Header enthält, der auf **www.example.com** festgelegt ist, und eine GET-Methode mit der **Zeichenfolge /query.cgi?server=5**. Die Umleitung extrahiert den Domänennamen aus dem Host-Header und die Nummer aus der Abfragezeichenfolge und leitet die Abfrage des Benutzers an den Server **Web5.example.com**um, wo der Rest der Abfrage des Benutzers verarbeitet wird.

> **Hinweis:**
>
> Obwohl die folgenden Befehle in mehreren Zeilen angezeigt werden, müssen Sie sie in einer einzigen Zeile ohne Zeilenumbrüche eingeben.

So leiten Sie eine Abfrage mit der CLI an die entsprechende URL um

- Um eine Rewrite-Aktion namens act_redirect_query zu erstellen, die den Hostnamen des HTTP-Servers durch den internen Servernamen ersetzt, geben Sie Folgendes ein:

```
add rewrite action act_redirect_query REPLACE http.req.header("Host").
before_str(".example.com")'"Web" + http.req.url.query.value("server")'
```

- Um eine Rewrite-Richtlinie mit dem Namen pol_redirect_query zu erstellen, geben Sie die folgenden Befehle an der Citrix ADC-Eingabeaufforderung ein. Diese Richtlinie erkennt Verbindungen zum Webserver, die eine Abfragezeichenfolge enthalten. Wenden Sie diese Richtlinie nicht auf Verbindungen an, die keine Abfragezeichenfolge enthalten:

```
add rewrite policy pol_redirect_query 'http.req.header("Host").eq(www.
example.com)&& http.req.url.contains("?")'act_redirect_query
```

- Binden Sie Ihre neue Richtlinie global.

Da diese Rewrite-Richtlinie sehr spezifisch ist und vor anderen Umschreibungsrichtlinien ausgeführt werden muss, ist es ratsam, ihr eine hohe Priorität zuzuweisen. Wenn Sie ihm eine Priorität von 1 zuweisen, wird sie zuerst ausgewertet.

Umschreiben von HTTP in HTTPS

In diesem Beispiel wird beschrieben, wie Webserver-Antworten neu geschrieben werden, um alle URLs zu finden, die mit der Zeichenfolge "HTTP" beginnen, und diese Zeichenfolge durch "https" ersetzen. Sie können damit vermeiden, Webseiten aktualisieren zu müssen, nachdem Sie einen Server von HTTP auf HTTPS verschoben haben.

So leiten Sie HTTP-URLs mit der CLI an HTTPS um

- Um eine Rewrite-Aktion namens act_replace_http_with_https zu erstellen, die alle Instanzen der Zeichenfolge "HTTP" durch die Zeichenfolge "https" ersetzt, geben Sie den folgenden Befehl ein:

```
add rewrite action act_replace_http_with_https replace_all 'http.res.body
(100)''"https"'-pattern http
```

- Um eine Rewrite-Richtlinie mit dem Namen pol_replace_http_with_https zu erstellen, die Verbindungen zum Webserver erkennt, geben Sie den folgenden Befehl ein:

```
add rewrite policy pol_replace_http_with_https TRUE act_replace_http_with_https
 NOREWRITE
```

- Binden Sie Ihre neue Richtlinie global.

Informationen zur Behebung dieses Umschreibungsvorgangs finden Sie unter “Fallstudie: Richtlinie zum Umschreiben von HTTP-Links in HTTPS funktioniert nicht. “

Entfernen unerwünschter Kopfzeilen

In diesem Beispiel wird erläutert, wie Sie eine Richtlinie zum Umschreiben verwenden, um unerwünschte Kopfzeilen zu entfernen. Insbesondere zeigt das Beispiel, wie die folgenden Header entfernt werden:

- **Akzeptieren Sie die Kodierungskopfzeile.** Wenn Sie den Header Accept Encoding aus HTTP-Antworten entfernen, wird die Komprimierung der Antwort verhindert.
- **Kopfzeile des Inhaltsspeicherorts.** Wenn Sie den Content Location-Header aus HTTP-Antworten entfernen, wird verhindert, dass Ihr Server einem Hacker Informationen zur Verfügung stellt, die eine Sicherheitsverletzung ermöglichen könnten.

Um Header aus HTTP-Antworten zu löschen, erstellen Sie eine Umschreibungsaktion und eine Umschreibungsrichtlinie und binden die Richtlinie global.

So erstellen Sie die entsprechende Rewrite-Aktion mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um entweder den Header Accept Encoding zu entfernen und die Antwortkomprimierung zu verhindern, oder den Inhaltsspeicher-Header zu entfernen:

- `add rewrite action ”act_remove-ae”delete_http_header ”Accept-Encoding”`
- `add rewrite action ”act_remove-cl”delete_http_header ”Content-Location”`

So erstellen Sie die entsprechende Rewrite-Richtlinie mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um entweder den Header Encoding akzeptieren oder den Header Content Location zu entfernen:

- `add rewrite policy ”pol_remove-ae”true ”act_remove-ae”`
- `add rewrite policy ”pol_remove-cl”true ”act_remove-cl”`

So binden Sie die Richtlinie global mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um die erstellte Richtlinie global zu binden:

- `bind rewrite global pol_remove_ae 100`
- `bind rewrite global pol_remove_cl 200`

Reduzieren von Webserver-Weiterleitungen

In diesem Beispiel wird erläutert, wie Sie eine Richtlinie zum Umschreiben verwenden, um Verbindungen zu Ihrer Homepage und anderen URLs zu ändern, die mit einem Schrägstrich (/) auf die Standardindexseite für den Server enden, wodurch Umleitungen vermieden und die Belastung des Servers verringert wird.

So ändern Sie HTTP-Anfragen auf Verzeichnisebene so, dass sie die Standard-Homepage mit der CLI einschließen

- Geben Sie Folgendes ein, um eine Aktion Umschreiben mit dem Namen action-default-homepage zu erstellen, die URLs, die mit einem Schrägstrich enden, so dass sie die Standardstartseite index.html enthält:

```
add rewrite action ”action-default-homepage”replace http.req.url.path ”\”/
index.html\””
```

- Um eine Richtlinie zum Umschreiben mit dem Namen policy-default-homepage zu erstellen, die Verbindungen zu Ihrer Homepage erkennt und die neue Aktion anwendet, geben Sie Folgendes ein:

```
add rewrite policy ”policy-default-homepage”q\##http.req.url.path.EQ(”/”)”
action-default-homepage”\##
```

- Binden Sie Ihre neue Richtlinie global, um sie in Kraft zu setzen.

Maskieren des Server-Headers

In diesem Beispiel wird erläutert, wie Sie eine Richtlinie zum Umschreiben verwenden, um die Informationen im Server-Header in HTTP-Antworten vom Webserver zu maskieren. Dieser Header enthält Informationen, mit denen Hacker Ihre Website gefährden können. Während das Maskieren des Headers einen erfahrenen Hacker nicht daran hindert, Informationen über Ihren Server zu finden, erschwert dies das Hacken Ihres Webservers und ermutigt Hacker, weniger gut geschützte Ziele auszuwählen.

So maskieren Sie den Server-Header in Antworten von der CLI

1. Um eine Rewrite -Aktion namens act_mask-server zu erstellen, die den Inhalt des Server-Headers durch eine nicht informative Zeichenfolge ersetzt, geben Sie Folgendes ein:

```
add rewrite action ”act_mask-server”replace ”http.RES.HEADER(\”Server\”)””
\”Web Server 1.0\””
```

1. Geben Sie Folgendes ein, um eine Rewrite-Richtlinie mit dem Namen pol_mask-server zu erstellen, die alle Verbindungen erkennt:


```
add rewrite policy ”pol_mask-server”true ”act_mask-server”
```

1. Binden Sie Ihre neue Richtlinie global, um sie in Kraft zu setzen.

Wie konvertiert man Nur-Text in eine URL-codierte Zeichenfolge und auf entgegengesetzte Weise

Die folgenden Ausdrücke wandeln Nur-Text in eine URL-codierte Zeichenfolge und umgekehrt um:

1. URL_RESERVED_CHARS_SAFE (string to URL ENCODED).

Beispiel:

```
(”abc def&123”).URL_RESERVED_CHARS_SAFE
Output will be
 “abc%20def%26123”  which is url encoded.
<!--NeedCopy-->
```

1. SET_TEXT_MODE (URLENCODED) .DECODE_USING_TEXT_MODE. (URL ENCODED to string)

Beispiel:

```
(”abc%20def%26123”).SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE
Output will be
 “abc def&123”
<!--NeedCopy-->
```

Tutorialbeispiele für klassische Richtlinien

October 5, 2021

In den folgenden Beispielen werden nützliche Beispiele für die klassische Richtlinienkonfiguration für bestimmte Citrix ADC Features wie Citrix Gateway, Anwendungsfirewall und SSL beschrieben.

Dieses Dokument enthält die folgenden Details:

- Citrix Gateway Richtlinie zur Überprüfung auf ein gültiges Clientzertifikat
- Anwendungs-Firewall-Richtlinie zum Schutz einer Warenkorb-Anwendung
- Anwendungs-Firewall-Richtlinie zum Schutz von skriptbasierten Webseiten
- DNS-Richtlinie zum Löschen von Paketen von bestimmten IPs
- SSL-Richtlinie zum Anfordern gültiger Clientzertifikate

Citrix Gateway Richtlinie zum Überprüfen eines gültigen Clientzertifikats

Mit den folgenden Richtlinien kann Citrix ADC sicherstellen, dass ein Client vor dem Herstellen einer Verbindung mit dem SSL-VPN eines Unternehmens ein gültiges Zertifikat vorlegt.

So prüfen Sie mit der Befehlszeilenschnittstelle nach einem gültigen Clientzertifikat

- Fügen Sie eine Aktion zum Ausführen der Clientzertifikatauthentifizierung hinzu.

  ```
  add ssl action act1 -clientAuth DOCLIENTAUTH
  ```

- Erstellen Sie eine SSL-Richtlinie, um die Clientanforderungen auszuwerten.

  ```
  add ssl policy pol1 -rule "REQ.HTTP.METHOD == GET"-action act1
  ```

- Fügen Sie eine Rewrite-Aktion hinzu, um die Details des Zertifikatausstellers in den HTTP-Header der Anforderungen einzufügen, die an den Webserver gesendet werden.

  ```
  add rewrite action act2 insert_http_header "CertDN"CLIENT.SSL.CLIENT_CERT
  .SUBJECT
  ```

- Erstellen Sie eine Rewrite-Richtlinie, um die Details des Zertifikatausstellers einzufügen, falls das Clientzertifikat vorhanden ist.

  ```
  add rewrite policy pol2 "CLIENT.SSL.CLIENT_CERT.EXISTS"act2
  ```

  Binden Sie diese neuen Richtlinien an den Citrix ADC VIP, um sie in Kraft zu setzen.

Anwendungs-Firewall-Richtlinie zum Schutz einer Warenkorb-Anwendung

Einkaufswagen-Anwendungen verarbeiten vertrauliche Kundeninformationen, z. B. Kreditkartennummern und Ablaufdaten, und sie greifen auf Back-End-Datenbankserver zu. Viele Warenkorb-Anwendungen verwenden auch ältere CGI-Skripts, die Sicherheitslücken enthalten können, die zu der Zeit, als sie geschrieben wurden, aber jetzt Hackern und Identitätsdieben bekannt sind.

Eine Warenkorb-Anwendung ist besonders anfällig für folgende Angriffe:

- **Cookie Manipulation.** Wenn eine Einkaufswagen-Anwendung Cookies verwendet und nicht die entsprechenden Kontrollen der Cookies durchführt, die Benutzer an die Anwendung zurückkehren, kann ein Angreifer ein Cookie ändern und unter den Anmeldeinformationen eines anderen Benutzers Zugriff auf die Warenkorb-Anwendung erhalten. Sobald er sich als dieser Benutzer angemeldet hat, kann der Angreifer vertrauliche private Informationen über den legitimen Benutzer abrufen oder Bestellungen über das Konto des legitimen Benutzers aufgeben.
- **SQL-Injection.** Eine Einkaufswagenanwendung greift normalerweise auf einen Back-End-Datenbankserver zu. Wenn die Anwendung die entsprechenden Sicherheitsprüfungen für die Daten durchführt, die Benutzer in den Formularfeldern ihrer Webformulare zurückgeben, bevor sie diese Informationen an die SQL-Datenbank weitergibt, kann ein Angreifer ein Webformular

verwenden, um nicht autorisierte SQL-Befehle in den Datenbankserver einzuleiten. Angreifer verwenden diese Art von Angriff normalerweise, um vertrauliche private Informationen aus der Datenbank zu erhalten oder Informationen in der Datenbank zu ändern.

Die folgende Konfiguration schützt eine Warenkorb-Anwendung vor diesen und anderen Angriffen.

So schützen Sie eine Warenkorb-Anwendung mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Sicherheit > Anwendungsfirewall > Profile**, und klicken Sie dann auf **Hinzufügen.**
2. Geben **Sie im Dialogfeld Anwendungs-Firewall-Profil erstellen** im Feld Profilname den Wert shopping_cart ein.
3. Wählen Sie in der Dropdownliste Profiltyp die Option Webanwendung aus.
4. In den Standardeinstellungen Erweiterte Auswahl konfigurieren.
5. Klicken Sie auf **Erstellen** und dann auf **Schließen.**
6. Doppelklicken Sie in der Detailansicht auf das neue Profil.
7. Konfigurieren Sie im Dialogfeld Webanwendungsprofil konfigurieren Ihr neues Profil wie unten beschrieben:

   - Klicken Sie auf die Registerkarte Überprüfungen, doppelklicken Sie auf die Überprüfung URL starten, und klicken Sie im Dialogfeld Start URL Check ändern auf die Registerkarte Allgemein, deaktivieren Sie das Blockieren und aktivieren Sie das Lernen, Protokollieren, Statistiken und URL-Verschluss. Klicken Sie auf OK, und klicken Sie dann auf Schließen.

     Beachten Sie, dass Sie diese Einstellungen konfigurieren, wenn Sie die Befehlszeile verwenden, indem Sie Folgendes an der Eingabeaufforderung eingeben und die EINGABETASTE drücken:

     ```
     set appfw profile shopping_cart -startURLAction LEARN LOG STATS -
     startURLClosure ON
     ```

   - Deaktivieren Sie für die Cookie-Konsistenzprüfung und Formularfeldkonsistenzprüfungen das Blockieren und aktivieren Sie das Lernen, Protokollieren und Statistiken. Verwenden Sie eine ähnliche Methode wie die Konfiguration Start URL Check ändern.

     Wenn Sie die Befehlszeile verwenden, konfigurieren Sie diese Einstellungen, indem Sie die folgenden Befehle eingeben:

     ```
     set appfw profile shopping_cart -cookieConsistencyAction LEARN LOG
     STATS
     ```

     ```
     set appfw profile shopping_cart -fieldConsistencyAction LEARN LOG
     STATS
     ```


- Deaktivieren Sie für die SQL-Injection-Prüfung das Blockieren, und aktivieren Sie das Lernen, Protokollieren, Statistiken und Transformation von Sonderzeichen im Dialogfeld SQL-Injectionsprüfung ändern auf der Registerkarte Allgemein im Abschnitt Aktionen überprüfen.

  Wenn Sie die Befehlszeile verwenden, konfigurieren Sie diese Einstellungen, indem Sie Folgendes an der Eingabeaufforderung eingeben und die EINGABETASTE drücken:

  ```
  set appfw profile shopping_cart -SQLInjectionAction LEARN LOG STATS
   -SQLInjectionTransformSpecialChars ON
  ```

- Deaktivieren Sie die Sperre für die Kreditkartenprüfung, aktivieren Sie die Protokollierung, Statistiken und Maskierung von Kreditkartennummern und aktivieren Sie den Schutz für Kreditkarten, die Sie als Zahlungsmittel akzeptieren.

  - Wenn Sie das Konfigurationsprogramm verwenden, konfigurieren Sie das Blockieren, Protokollieren, Statistiken und Maskierung (oder x-out) im Dialogfeld Kreditkartenprüfung ändern auf der Registerkarte Allgemein im Abschnitt Aktionen überprüfen. Sie konfigurieren den Schutz für bestimmte Kreditkarten auf der Registerkarte Einstellungen desselben Dialogfelds.
  - Wenn Sie die Befehlszeile verwenden, konfigurieren Sie diese Einstellungen, indem Sie Folgendes an der Eingabeaufforderung eingeben und die EINGABETASTE drücken:

  ```
  set appfw profile shopping_cart -creditCardAction LOG STATS -
  creditCardXOut ON -creditCard <name> [<name>...]
  ```

  Für <name> Sie ersetzen Sie den Namen der Kreditkarte, die Sie schützen möchten. Für Visa ersetzen Sie VISA. Für Master Card ersetzen Sie MasterCard. Für American Express ersetzen Sie Amex. Für Discover ersetzen Sie Discover. Für Diners Club ersetzen Sie DinersClub. Für JCB ersetzen Sie JCB.

8. Erstellen Sie eine Richtlinie mit dem Namen shopping_cart, die Verbindungen zu Ihrer Einkaufswagen-Anwendung erkennt und das Profil shopping_cart auf diese Verbindungen anwendet.

   Um Verbindungen zum Warenkorb zu erkennen, untersuchen Sie die URL eingehender Verbindungen. Wenn Sie Ihre Warenkorb-Anwendung auf einem separaten Host hosten (eine kluge Maßnahme aus Sicherheitsgründen und anderen Gründen), können Sie einfach nach der Anwesenheit dieses Hosts in der URL suchen. Wenn Sie Ihren Warenkorb in einem Verzeichnis auf einem Host hosten, der auch andere Traffic verarbeitet, müssen Sie feststellen, dass die Verbindung zum entsprechenden Verzeichnis und/oder HTML-Seite erfolgt.

   Der Prozess zum Erkennen einer dieser beiden ist identisch. Sie erstellen eine Richtlinie auf der Grundlage des folgenden Ausdrucks und ersetzen den richtigen Host oder URL <string>.


```
REQ.HTTP.HEADER URL CONTAINS <string>
<!--NeedCopy-->
```

- Wenn Sie das Konfigurationsdienstprogramm verwenden, navigieren Sie zur Seite Richtlinien der Anwendungsfirewall, klicken Sie auf die Schaltfläche Hinzufügen…, um eine neue Richtlinie hinzuzufügen, und führen Sie den Richtlinienerstellungsprozess durch, der unter So erstellen Sie eine Richtlinie mit klassischen Ausdrücken mit dem Konfigurationsdienstprogramm beschrieben wird.
- Wenn Sie die Befehlszeile verwenden, geben Sie den folgenden Befehl an der Eingabeaufforderung ein und drücken Sie die EINGABETASTE:

  ```
  add appfw policy shopping_cart ”REQ.HTTP.HEADER URL CONTAINS <
  string>”shopping_cart
  ```

2. Binden Sie Ihre neue Richtlinie global, um sie in Kraft zu setzen.

Da Sie sicherstellen möchten, dass diese Richtlinie allen Verbindungen zum Warenkorb entspricht und nicht von einer anderen allgemeineren Richtlinie unterstellt wird, sollten Sie ihr eine hohe Priorität zuweisen. Wenn Sie eine (1) als Priorität zuweisen, kann diese Richtlinie von keiner anderen Richtlinie abbrechen.

Anwendungs-Firewall-Richtlinie zum Schutz von skriptbasierten Webseiten

Webseiten mit eingebetteten Skripten, insbesondere ältere JavaScripts, verletzen häufig die gleiche Ursprungsregel, die es Skripts nicht erlaubt, auf Inhalte auf einem Server außer auf dem Server, auf dem sie sich befinden, zuzugreifen oder zu ändern. Diese Sicherheitsanfälligkeit wird als siteübergreifendes Scripting bezeichnet. Die Anwendungsfirewall Cross-Site Scripting Regel filtert normalerweise Anforderungen heraus, die siteübergreifendes Scripting enthalten.

Leider kann dies dazu führen, dass Webseiten mit älteren JavaScripts nicht mehr funktionieren, selbst wenn Ihr Systemadministrator diese Skripts überprüft und weiß, dass sie sicher sind. Im folgenden Beispiel wird erläutert, wie Sie die Anwendungsfirewall so konfigurieren, dass websiteübergreifende Skripterstellung in Webseiten aus vertrauenswürdigen Quellen ermöglicht wird, ohne diesen wichtigen Filter für die restlichen Websites zu deaktivieren.

So schützen Sie Webseiten mit websiteübergreifender Skripterstellung mit der Befehlszeilenschnittstelle

- Geben Sie in der Befehlszeile Folgendes ein, um ein erweitertes Profil zu erstellen:

  ```
  add appfw profile pr_xssokay -defaults advanced
  ```


- Geben Sie Folgendes ein, um das Profil zu konfigurieren:

```
set appfw profile pr_xssokay -startURLAction NONE -startURLClosure OFF
-cookieConsistencyAction LEARN LOG STATS -fieldConsistencyAction LEARN
LOG STATS -crossSiteScriptingAction LEARN LOG STATS$"
```

- Erstellen Sie eine Richtlinie, die Verbindungen zu Ihren skriptbasierten Webseiten erkennt und das pr_xssokay-Profil anwendet, geben Sie Folgendes ein:

```
add appfw policy pol_xssokay "REQ.HTTP.HEADER URL CONTAINS ^\\.pl\\?$
|| REQ.HTTP.HEADER URL CONTAINS ^\\.js$"pr_xssokay
```

- Globale Bindung der Richtlinie.

So schützen Sie Webseiten mit websiteübergreifender Skripterstellung mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Sicherheit > Anwendungsfirewall > Profile.**
2. Klicken Sie in der Detailansicht auf **Hinzufügen.**
3. **Erstellen Sie im Dialogfeld Anwendungs-Firewall-Profil** erstellen ein Webanwendungsprofil mit erweiterten Standardeinstellungen, und benennen Sie es pr_xssokay. Klicken Sie auf **Erstellen** und dann auf **Schließen.**
4. Klicken Sie in der Detailansicht auf das Profil, klicken Sie auf Öffnen, und konfigurieren Sie im Dialogfeld Webanwendungsprofil konfigurieren das pr_xssokay-Profil wie unten dargestellt.

   URL-Prüfung starten: Alle Aktionen löschen.

   - Cookie-Konsistenzprüfung: Sperren deaktivieren.
   - Formularfeldkonsistenzprüfung: Sperren deaktivieren.
   - Websiteübergreifende Skriptüberprüfung: Sperren deaktivieren.

   Dadurch sollte verhindert werden, dass legitime Anforderungen an Webseiten mit websiteübergreifendem Skripting blockiert werden, von denen Sie wissen, dass sie dennoch sicher sind.
5. Klicken Sie auf **Richtlinien**, und klicken Sie dann auf **Hinzufügen.**
6. **Erstellen Sie im Dialogfeld Anwendungs-Firewall-Richtlinie** erstellen eine Richtlinie, die Verbindungen zu Ihren skriptbasierten Webseiten erkennt und das pr_xssokay-Profil anwendet:

   - Richtlinienname: pol_xssokay
   - Zugehöriges Profil: pr_xssokay

Richtlinienausdruck: REQ.HTTP.HEADER URL CONTAINS ^\.pl\?$	REQ.HTTP.HEADER URL CONTAINS ^\.js$”

7. Binden Sie Ihre neue Richtlinie global, um sie in Kraft zu setzen.

DNS-Richtlinie zum Löschen von Paketen von bestimmten IPs

Im folgenden Beispiel wird beschrieben, wie Sie eine DNS-Aktion und eine DNS-Richtlinie erstellen, die Verbindungen von unerwünschten IPs oder Netzwerken erkennt, z. B. bei einem DDOS-Angriff verwendet, und alle Pakete von diesen Speicherorten löscht. Das Beispiel zeigt Netzwerke innerhalb des reservierten IANA-IP-Blocks 192.168.0.0/16. Ein feindliches Netzwerk wird normalerweise auf öffentlich routingfähigen IP-Adressen sein.

So löschen Sie Pakete von bestimmten IPs mit der Befehlszeilenschnittstelle

- Um eine DNS-Richtlinie mit dem Namen pol_ddos_drop zu erstellen, die Verbindungen aus feindlichen Netzwerken erkennt und diese Pakete löscht, geben Sie Folgendes ein:

  ```
  add dns policy pol_ddos_drop 'client.ip.src.in_subnet(192.168.253.128/25)
  || client.ip.src.in_subnet(192.168.254.32/27)'-drop YES'
  ```

  Für die Beispielnetzwerke im Bereich 192.168.0.0/16 ersetzen Sie die IP und die Netzmaske im Format ##.##.##.##.###/## jedes Netzwerks, das Sie blockieren möchten. Sie können beliebig viele Netzwerke einschließen und jeden Befehl CLIENT.IP.SRC.IN_SUBNET (###.##.##.##.##.#./##) mit dem Operator OR trennen.

- Binden Sie Ihre neue Richtlinie global, um sie in Kraft zu setzen.

SSL-Richtlinie zum Anfordern gültiger Clientzertifikate

Das folgende Beispiel zeigt eine SSL-Richtlinie, die die Gültigkeit des Clientzertifikats des Benutzers überprüft, bevor eine SSL-Verbindung mit einem Client initiiert wird.

So sperren Sie Verbindungen von Benutzern mit abgelaufenen Clientzertifikaten

- Melden Sie sich an der Befehlszeilenschnittstelle an.

  Wenn Sie die GUI verwenden, navigieren Sie zur Seite SSL-Richtlinien, und klicken Sie dann im Bereich Daten auf die Registerkarte Aktionen.

- Erstellen Sie eine SSL-Aktion namens act_current_client_cert, die erfordert, dass Benutzer über ein aktuelles Clientzertifikat verfügen, um eine SSL-Verbindung mit dem Citrix ADC herzustellen.

  ```
  add ssl action act_current_client_cert-clientAuth DOCLIENTAUTH -clientCert
   ENABLED -certHeader "clientCertificateHeader"-clientCertNotBefore
  ENABLED -certNotBeforeHeader "Mon, 01 Jan 2007 00:00:00 GMT"
  ```

- Erstellen Sie eine SSL-Richtlinie mit dem Namen pol_current_client_cert, die Verbindungen mit dem Webserver erkennt, die eine Abfragezeichenfolge enthalten.

  ```
  add ssl policy pol_current_ client_cert 'REQ.SSL.CLIENT.CERT.VALIDFROM
  \>= "Mon, 01 Jan 2007 00:00:00 GMT"'act_block_ssl
  ```

- Binden Sie Ihre neue Richtlinie global.

  Da diese SSL-Richtlinie für die SSL-Verbindung eines beliebigen Benutzers gelten sollte, es sei denn, eine spezifischere SSL-Richtlinie gilt, sollten Sie ihr eine niedrige Priorität zuweisen. Wenn Sie ihm eine Priorität von tausend (1000) zuweisen, sollten Sie sicherstellen, dass andere SSL-Richtlinien zuerst ausgewertet werden. Dies bedeutet, dass diese Richtlinie nur für Verbindungen gilt, die nicht spezifischeren Richtlinienkriterien entsprechen.

Migration von Apache mod_rewrite Regeln auf die Standardsyntax

October 5, 2021

Der Apache HTTP-Server stellt eine Engine namens mod_rewrite zum Umschreiben von HTTP-Anforderungs-URLs bereit. Wenn Sie die mod_rewrite-Regeln von Apache auf Citrix ADC migrieren, erhöhen Sie die Back-End-Serverleistung. Da der Citrix ADC normalerweise mehrere (manchmal Tausende) Webserver ausgleicht, haben Sie nach der Migration der Regeln zum Citrix ADC einen einzigen Kontrollpunkt für diese Regeln.

Im Folgenden finden Sie Beispiele für mod_rewrite-Funktionen und Übersetzungen dieser Funktionen in Rewrite- und Responder-Richtlinien auf dem Citrix ADC.

Konvertieren von URL-Variationen in kanonische URLs

Auf einigen Webservern können Sie mehrere URLs für eine Ressource verwenden. Obwohl die kanonischen URLs verwendet und verteilt werden sollten, können andere URLs als Verknüpfungen oder interne URLs vorhanden sein. Sie können sicherstellen, dass Benutzer die kanonische URL sehen, unabhängig von der URL, die verwendet wird, um eine erste Anfrage zu stellen.

In den folgenden Beispielen wird die URL /~user in /u/user konvertiert.

Apache mod_rewrite Lösung zum Konvertieren einer URL

```
RewriteRule ^/~([^/]+)/?(.*) /u/$1/$2[R]
<!--NeedCopy-->
```

Citrix ADC Lösung zum Konvertieren einer URL

```
add responder action act1 redirect '"/u/"+HTTP.REQ.URL.AFTER_STR("/~")'
    -bypassSafetyCheck yes
add responder policy pol1 'HTTP.REQ.URL.STARTSWITH("/~") && HTTP.REQ.
   URL.LENGTH.GT(2)' act1
bind responder global pol1 100
<!--NeedCopy-->
```

Konvertieren von Hostnamen-Variationen in kanonische Hostnamen

Sie können die Verwendung eines bestimmten Hostnamens zum Erreichen einer Site erzwingen. Beispielsweise können Sie die Verwendung von www.example.com anstelle von example.com erzwingen.

Apache mod_rewrite Lösung zum Erzwingen eines bestimmten Hostnamens für Sites, die auf einem anderen Port als 80 ausgeführt werden

```
RewriteCond %{
 HTTP_HOST }
    !^www.example.com
RewriteCond %{
 HTTP_HOST }
    !^$
RewriteCond %{
 SERVER_PORT }
  !^80$
RewriteRule ^/(.*)         http://www.example.com:%{
 SERVER_PORT }
 /$1 [L,R]
<!--NeedCopy-->
```

Apache mod_rewrite Lösung zum Erzwingen eines bestimmten Hostnamens für Sites, die auf Port 80 ausgeführt werden


```
RewriteCond %{
 HTTP_HOST }
    !^www.example.com
RewriteCond %{
 HTTP_HOST }
    !^$
RewriteRule ^/(.*)         http://www.example.com/$1 [L,R]
<!--NeedCopy-->
```

Citrix ADC Lösung zum Erzwingen eines bestimmten Hostnamens für Sites, die auf einem anderen Port als 80 ausgeführt werden

```
add responder action act1 redirect '"http://www.example.com:"+CLIENT.
   TCP.DSTPORT+HTTP.REQ.URL' -bypassSafetyCheck yes
add responder policy pol1 '!HTTP.REQ.HOSTNAME.CONTAINS("www.example.com
   ")&&!HTTP.REQ.HOSTNAME.EQ("")&&!HTTP.REQ.HOSTNAME.PORT.EQ(80)&&HTTP.
   REQ.HOSTNAME.CONTAINS("example.com")' act1
bind responder global pol1 100 END
<!--NeedCopy-->
```

Citrix ADC Lösung zum Erzwingen eines bestimmten Hostnamens für Sites, die auf Port 80 ausgeführt werden

```
add responder action act1 redirect '"http://www.example.com"+HTTP.REQ.
   URL' -bypassSafetyCheck yes
add responder policy pol1  '!HTTP.REQ.HOSTNAME.CONTAINS("www.example.
   com")&&!HTTP.REQ.HOSTNAME.EQ("")&&HTTP.REQ.HOSTNAME.PORT.EQ(80)&&
   HTTP.REQ.HOSTNAME.CONTAINS("example.com")' act1
bind responder global  pol1 100 END
<!--NeedCopy-->
```

Verschieben eines Dokumentstammes

Normalerweise basiert der Dokumentenstamm eines Webservers auf der URL /. Der Dokumentstamm kann jedoch ein beliebiges Verzeichnis sein. Sie können den Datenverkehr zum Dokumentstamm umleiten, wenn er sich vom obersten Verzeichnis / in ein anderes Verzeichnis ändert.

In den folgenden Beispielen ändern Sie den Dokumentstamm von/in /e/www. Die ersten beiden Beispiele ersetzen einfach eine Zeichenfolge durch eine andere. Das dritte Beispiel ist universeller,

da neben dem Ersetzen des Stammverzeichnisses der Rest der URL (Pfad und Abfragezeichenfolge) beibehalten wird, z. B. /example/file.html nach /e/www/example/file.htmlumgeleitet wird.

Apache mod_rewrite Lösung zum Verschieben des Dokumentstammes

```
RewriteEngine on
RewriteRule   ^/$  /e/www/  [R]
<!--NeedCopy-->
```

Citrix ADC Lösung zum Verschieben des Dokumentstammes

```
add responder action act1 redirect '"/e/www/"' -bypassSafetyCheck yes
add responder policy pol1 'HTTP.REQ.URL.EQ("/")' act1
bind responder global pol1 100
<!--NeedCopy-->
```

Citrix ADC Lösung zum Verschieben des Dokumentstammes und Anhängen von Pfadinformationen an die Anforderung

```
add responder action act1 redirect '"/e/www"+HTTP.REQ.URL' -
   bypassSafetyCheck yes
add responder policy pol1 '!HTTP.REQ.URL.STARTSWITH("/e/www/")' act1
bind responder global pol1 100 END
<!--NeedCopy-->
```

Verschieben von Basisverzeichnissen auf einen neuen Webserver

Möglicherweise möchten Sie Anforderungen, die an Basisverzeichnisse auf einem Webserver gesendet werden, an einen anderen Webserver umleiten. Wenn beispielsweise ein neuer Webserver einen alten Webserver im Laufe der Zeit ersetzt, müssen Sie beim Migrieren von Basisverzeichnissen an den neuen Speicherort Anforderungen für die migrierten Basisverzeichnisse an den neuen Webserver umleiten.

In den folgenden Beispielen ist der Hostname für den neuen Webserver newserver.

Apache mod_rewrite Lösung zum Umleiten auf einen anderen Webserver


```
RewriteRule   ^/(.+)  http://newserver/$1     [R,L]
<!--NeedCopy-->
```

Citrix ADC Lösung zum Umleiten auf einen anderen Webserver (Methode 1)

```
add responder  action act1 redirect '"http://newserver"+HTTP.REQ.URL' -
    bypassSafetyCheck yes
add responder policy pol1 'HTTP.REQ.URL.REGEX_MATCH(re#^/(.+)#)'   act1
bind responder global pol1 100 END
<!--NeedCopy-->
```

Citrix ADC Lösung zum Umleiten auf einen anderen Webserver (Methode 2)

```
add responder  action act1 redirect '"http://newserver"+HTTP.REQ.URL' -
    bypassSafetyCheck yes
add responder policy pol1 'HTTP.REQ.URL.LENGTH.GT(1)' act1
bind responder global pol1 100 END
<!--NeedCopy-->
```

Arbeiten mit strukturierten Home-Verzeichnissen

Normalerweise hat eine Site mit Tausenden von Benutzern ein strukturiertes Home-Verzeichnislayout. Beispielsweise kann sich jedes Basisverzeichnis unter einem Unterverzeichnis befinden, das mit dem ersten Zeichen des Benutzernamens benannt wird. Beispielsweise könnte das Home-Verzeichnis für jsmith (/~jsmith/anypath) /home/j/smith/.www/anypath sein, und das Home-Verzeichnis für rvalveti (/~rvalveti/anypath) könnte /home/r/rvalveti/.www/anypath sein.

In den folgenden Beispielen werden Anforderungen an das Basisverzeichnis umgeleitet.

Apache mod_rewrite Lösung für strukturierte Home-Verzeichnisse

```
RewriteRule   ^/~(([a-z])[a-z0-9]+)(.*)  /home/$2/$1/.www$3
<!--NeedCopy-->
```

Citrix ADC Lösung für strukturierte Basisverzeichnisse

Citrix ADC Lösung für strukturierte Basisverzeichnisse


```
add rewrite action act1 replace 'HTTP.REQ.URL'  '"/home/"+ HTTP.REQ.URL
    .AFTER_STR("~").PREFIX(1)+"/"+ HTTP.REQ.URL.AFTER_STR("~").
    BEFORE_STR("/")+"/.www"+HTTP.REQ.URL.SKIP('/',1)'  -
    bypassSafetyCheck yes
add rewrite policy pol1  'HTTP.REQ.URL.PATH.STARTSWITH("/~")' act1
bind rewrite global pol1 100

<!--NeedCopy-->
```

Umleiten ungültiger URLs zu anderen Webservern

Wenn eine URL ungültig ist, sollte sie auf einen anderen Webserver umgeleitet werden. Sie sollten beispielsweise zu einem anderen Webserver umleiten, wenn eine Datei, die in einer URL benannt ist, auf dem Server, der in der URL benannt ist, nicht vorhanden ist.

Auf Apache können Sie diese Prüfung mit mod_rewrite durchführen. Auf dem Citrix ADC kann ein HTTP-Callout nach einer Datei auf einem Server suchen, indem ein Skript auf dem Server ausgeführt wird. In den folgenden Citrix ADC Beispielen verarbeitet ein Skript mit dem Namen file_check.cgi die URL und verwendet diese Informationen, um zu überprüfen, ob die Zieldatei auf dem Server vorhanden ist. Das Skript gibt TRUE oder FALSE zurück, und Citrix ADC verwendet den Wert, den das Skript zurückgibt, um die Richtlinie zu überprüfen.

Zusätzlich zur Durchführung der Umleitung kann Citrix ADC benutzerdefinierte Header hinzufügen oder, wie im zweiten Citrix ADC-Beispiel, Text im Antworttext hinzufügen.

Apache mod_rewrite Lösung für die Umleitung, wenn eine URL falsch ist

```
RewriteCond   /your/docroot/%{
 REQUEST_FILENAME }
  !-f
RewriteRule   ^(.+)      http://webserverB.com/$1 [R]

<!--NeedCopy-->
```

Citrix ADC Lösung für die Umleitung, wenn eine URL falsch ist (Methode 1)

```
add HTTPCallout Call
set policy httpCallout Call -IPAddress 10.102.59.101 -port 80 -hostExpr
     '"10.102.59.101"' -returnType BOOL -ResultExpr 'HTTP.RES.BODY(100).
    CONTAINS("True")'  -urlStemExpr '"/cgi-bin/file_check.cgi"'   -
    parameters query=http.req.url.path -headers Name("ddd")
```



```
add responder action act1 redirect '"http://webserverB.com"+HTTP.REQ.URL' -bypassSafetyCheck yes
add responder policy pol1 '!HTTP.REQ.HEADER("Name").EXISTS && !SYS.HTTP_CALLOUT(call)' act1
bind responder global pol1 100

<!--NeedCopy-->
```

Citrix ADC Lösung für die Umleitung, wenn eine URL falsch ist (Methode 2)

```
add HTTPCallout Call
set policy httpCallout Call -IPAddress 10.102.59.101 -port 80 -hostExpr '"10.102.59.101"' -returnType BOOL -ResultExpr 'HTTP.RES.BODY(100).CONTAINS("True")' -urlStemExpr '"/cgi-bin/file_check.cgi"' -parameters query=http.req.url.path -headers Name("ddd")
add responder action act1 respondwith '"HTTP/1.1 302 Moved Temporarily\r\nLocation: http://webserverB.com"+HTTP.REQ.URL+"\r\n\r\nHTTPCallout Used"' -bypassSafetyCheck yes
add responder policy pol1 '!HTTP.REQ.HEADER("Name").EXISTS && !SYS.HTTP_CALLOUT(call)' act1
bind responder global pol1 100

<!--NeedCopy-->
```

Umschreiben einer URL basierend auf der Zeit

Sie können eine URL basierend auf der Zeit neu schreiben. In den folgenden Beispielen wird eine Anforderung für example.html in example.day.html oder example.night.html geändert, abhängig von der Tageszeit.

Apache mod_rewrite Lösung zum Umschreiben einer URL basierend auf der Zeit

```
RewriteCond %{
 TIME_HOUR }
 %{
 TIME_MIN }
  >0700
RewriteCond %{
 TIME_HOUR }
 %{
 TIME_MIN }
```



```
  <1900
RewriteRule    ^example.html$ example.day.html [L]
RewriteRule    ^example.html$ example.night.html

<!--NeedCopy-->
```

Citrix ADC Lösung zum Umschreiben einer URL basierend auf der Zeit

```
add rewrite action act1 insert_before 'HTTP.REQ.URL.PATH.SUFFIX('.',0)'
     '"day."'
add rewrite action act2  insert_before 'HTTP.REQ.URL.PATH.SUFFIX('.',0)
    ' '"night."'
add rewrite  policy pol1 'SYS.TIME.WITHIN(LOCAL 07h 00m,LOCAL 18h 59m)'
     act1
add rewrite policy pol2 'true'  act2
bind rewrite global pol1 101
bind rewrite global pol2 102

<!--NeedCopy-->
```

Umleitung zu einem neuen Dateinamen (für den Benutzer unsichtbar)

Wenn Sie eine Webseite umbenennen, können Sie die alte URL aus Gründen der Abwärtskompatibilität weiterhin unterstützen, während Benutzer daran hindern, dass die Seite umbenannt wurde.

In den ersten beiden der folgenden Beispiele ist das Basisverzeichnis /~quux/. Das dritte Beispiel enthält alle Basisverzeichnisse und das Vorhandensein von Abfragezeichenfolgen in der URL.

Apache mod_rewrite Lösung zur Verwaltung einer Dateinamenänderung an einem festen Speicherort

```
RewriteEngine  on
RewriteBase    /~quux/
RewriteRule    ^foo.html$  bar.html

<!--NeedCopy-->
```

Citrix ADC Lösung zur Verwaltung einer Dateinamenänderung an einem festen Speicherort


```
add rewrite action act1 replace 'HTTP.REQ.URL.AFTER_STR("/~quux").
    SUBSTR("foo.html")' '"bar.html"'
add rewrite policy pol1 'HTTP.REQ.URL.ENDSWITH("/~quux/foo.html")' act1
bind rewrite global pol1 100

<!--NeedCopy-->
```

Citrix ADC Lösung zur Verwaltung einer Dateinamenänderung unabhängig vom Basisverzeichnis oder Abfragezeichenfolgen in der URL

```
add rewrite action act1 replace 'HTTP.REQ.URL.PATH.SUFFIX('/',0)' '"bar
    .html"'
Add rewrite policy pol1 'HTTP.REQ.URL.PATH.CONTAINS("foo.html")' act1
Bind rewrite global pol1 100

<!--NeedCopy-->
```

Umleitung zu neuen Dateinamen (vom Benutzer sichtbare URL)

Wenn Sie eine Webseite umbenennen, sollten Sie die alte URL aus Gründen der Abwärtskompatibilität weiterhin unterstützen und Benutzern erlauben, zu erkennen, dass die Seite umbenannt wurde, indem Sie die URL ändern, die im Browser angezeigt wird.

In den ersten beiden der folgenden Beispiele erfolgt die Umleitung, wenn das Basisverzeichnis /~quux/ ist. Das dritte Beispiel enthält alle Basisverzeichnisse und das Vorhandensein von Abfragezeichenfolgen in der URL.

Apache mod_rewrite Lösung zum Ändern des Dateinamens und der URL im Browser angezeigt

```
RewriteEngine on
RewriteBase    /~quux/
RewriteRule    ^old.html$ new.html  [R]

<!--NeedCopy-->
```

Citrix ADC Lösung zum Ändern des Dateinamens und der im Browser angezeigten URL


```
add responder action act1 redirect 'HTTP.REQ.URL.BEFORE_STR("foo.html")
   +"new.html"' -bypassSafetyCheck yes
add responder policy pol1 'HTTP.REQ.URL.ENDSWITH("/~quux/old.html")'
   act1
bind responder global pol1 100

<!--NeedCopy-->
```

Citrix ADC Lösung zum Ändern des Dateinamens und der im Browser angezeigten URL unabhängig vom Basisverzeichnis oder den Abfragezeichenfolgen in der URL

```
add responder action act1 redirect 'HTTP.REQ.URL.PATH.BEFORE_STR("old.
   html")+"new.html"+HTTP.REQ.URL.AFTER_STR("old.html")' -
   bypassSafetyCheck yes
add responder policy pol1 'HTTP.REQ.URL.PATH.CONTAINS("old.html")' act1
bind responder global pol1 100

<!--NeedCopy-->
```

Browserabhängige Inhalte aufnehmen

Um browserspezifische Einschränkungen — zumindest für wichtige Seiten der obersten Ebene — zu berücksichtigen, ist es manchmal notwendig, Einschränkungen für den Browsertyp und die Version festzulegen. Sie können beispielsweise eine maximale Version für die neuesten Netscape-Varianten, eine Mindestversion für Lynx-Browser und eine durchschnittliche Feature-Version für alle anderen festlegen.

Die folgenden Beispiele wirken auf den HTTP-Header "User-Agent", so dass, wenn dieser Header mit "Mozilla/3" beginnt, die Seite MyPage.html in MyPage.NS.html umgeschrieben wird. Wenn der Browser Lynx oder Mozilla Version 1 oder 2 ist, wird die URL myPage.20.html. Alle anderen Browser erhalten Seite myPage.32.html.

Apache mod_rewrite Lösung für browserspezifische Einstellungen

```
RewriteCond %{
 HTTP_USER_AGENT }
   ^Mozilla/3.*
RewriteRule ^MyPage.html$ MyPage.NS.html [L]
RewriteCond %{
 HTTP_USER_AGENT }
```



```
    ^Lynx/.* [OR]
RewriteCond %{
 HTTP_USER_AGENT }
    ^Mozilla/[12].*
RewriteRule ^MyPage.html$ MyPage.20.html [L]
RewriteRule ^fMyPage.html$ MyPage.32.html [L]
Citrix ADC solution for browser-specific settings
add patset pat1
bind patset pat1 Mozilla/1
bind Patset pat1 Mozilla/2
bind patset pat1 Lynx
bind Patset pat1 Mozilla/3
add rewrite action act1 insert_before 'HTTP.REQ.URL.SUFFIX' '"NS."'
add rewrite action act2 insert_before 'HTTP.REQ.URL.SUFFIX' '"20."'
add rewrite action act3 insert_before 'HTTP.REQ.URL.SUFFIX' '"32."'
add rewrite policy pol1 'HTTP.REQ.HEADER("User-Agent").STARTSWITH_INDEX
    ("pat1").EQ(4)' act1
add rewrite policy pol2 'HTTP.REQ.HEADER("User-Agent").STARTSWITH_INDEX
    ("pat1").BETWEEN(1,3)' act2
add rewrite policy pol3 '!HTTP.REQ.HEADER("User-Agent").STARTSWITH_ANY
    ("pat1")' act3
bind rewrite global pol1 101 END
bind rewrite global pol2 102 END
bind rewrite global pol3 103 END

<!--NeedCopy-->
```

Sperren des Zugriffs durch Roboter

Sie können einen Roboter davon abhalten, Seiten aus einem bestimmten Verzeichnis oder einer Reihe von Verzeichnissen abzurufen, um den Datenverkehr zu und von diesen Verzeichnissen zu erleichtern. Sie können den Zugriff basierend auf dem bestimmten Speicherort einschränken oder Anfragen basierend auf Informationen in HTTP-Headern des User-Agent blockieren.

In den folgenden Beispielen ist der zu blockierende Webspeicherort /~quux/foo/arc/, die zu blockierenden IP-Adressen sind 123.45.67.8 und 123.45.67.9, und der Name des Roboters lautet NameOfBadRobot.

Apache mod_rewrite Lösung zum Blockieren eines Pfades und eines User-Agent-Headers

```
RewriteCond %{
```



```
 HTTP_USER_AGENT }
    ^NameOfBadRobot.*
RewriteCond %{
 REMOTE_ADDR }
        ^123.45.67.[8-9]$
RewriteRule ^/~quux/foo/arc/.+   -   [F]

<!--NeedCopy-->
```

Citrix ADC Lösung zum Blockieren eines Pfades und eines User-Agent-Headers

```
add responder action act1 respondwith '"HTTP/1.1 403 Forbidden\r\n\r\n"
   '
add responder policy pol1 'HTTP.REQ.HEADER("User_Agent").STARTSWITH("
   NameOfBadRobot")&&CLIENT.IP.SRC.EQ(123.45.67.8)&&CLIENT.IP.SRC.EQ
   (123.45.67.9) && HTTP.REQ.URL.STARTSWITH("/~quux/foo/arc")' act1
bind responder global pol1 100

<!--NeedCopy-->
```

Blockieren des Zugriffs auf Inline-Images

Wenn Sie feststellen, dass Personen häufig auf Ihren Server gehen, um Inline-Grafiken für den eigenen Gebrauch zu kopieren (und unnötigen Datenverkehr zu generieren), sollten Sie die Fähigkeit des Browsers einschränken, einen HTTP-Referer-Header zu senden.

Im folgenden Beispiel befinden sich die Grafiken in Example.

Apache mod_rewrite Lösung zum Blockieren des Zugriffs auf ein Inline-Image

```
RewriteCond %{
 HTTP_REFERER }
  !^$
RewriteCond %{
 HTTP_REFERER }
  !^http://www.quux-corp.de/~quux/.\*$
RewriteRule .\*.png$ - [F]

<!--NeedCopy-->
```


Citrix ADC Lösung zum Blockieren des Zugriffs auf ein Inline-Image

```
add patset pat1
bind patset pat1 .png
bind patset pat1 .jpeg
add responder action act1 respondwith '"HTTP/1.1 403 Forbidden\r\n\r\n"
    '
add responder policy pol1 '!HTTP.REQ.HEADER("Referer").EQ("") && !HTTP.
    REQ.HEADER("Referer").STARTSWITH("http://www.quux-corp.de/~quux/")&&
    HTTP.REQ.URL.ENDSWITH_ANY("pat1")' act1
bind responder global pol1 100

<!--NeedCopy-->
```

Erstellen von erweiterungslosen Links

Um zu verhindern, dass Benutzer Anwendungs- oder Skriptdetails auf der Serverseite kennen, können Sie Dateierweiterungen vor Benutzern ausblenden. Um dies zu tun, möchten Sie möglicherweise erweiterungslose Links unterstützen. Sie können dieses Verhalten erreichen, indem Sie Rewrite-Regeln verwenden, um eine Erweiterung zu allen Anforderungen hinzuzufügen oder um selektiv Erweiterungen zu Anforderungen hinzuzufügen.

Die ersten beiden der folgenden Beispiele zeigen das Hinzufügen einer Erweiterung zu allen Anforderungs-URLs. Im letzten Beispiel wird eine von zwei Dateierweiterungen hinzugefügt. Beachten Sie, dass im letzten Beispiel das Modul mod_rewrite die Dateierweiterung leicht finden kann, da sich dieses Modul auf dem Webserver befindet. Im Gegensatz dazu muss Citrix ADC ein HTTP-Callout aufrufen, um die Erweiterung der angeforderten Datei auf dem Webserver zu überprüfen. Basierend auf der Callout-Antwort fügt Citrix ADC die Erweiterung .html oder .php zur Anforderungs-URL hinzu.

> **Hinweis:**
>
> Im zweiten Citrix ADC Beispiel wird ein HTTP-Callout verwendet, um ein Skript namens file_check.cgi abzufragen, das auf dem Server gehostet wird. Dieses Skript überprüft, ob das Argument, das im Callout angegeben wird, ein gültiger Dateiname ist.

Apache mod_rewrite Lösung zum Hinzufügen einer PHP-Erweiterung zu allen Anfragen

```
RewriteRule ^/?([a-z]+)$ $1.php [L]

<!--NeedCopy-->
```


Citrix ADC Richtlinie zum Hinzufügen einer PHP-Erweiterung zu allen Anforderungen

```
add rewrite action act1 insert_after 'HTTP.REQ.URL' '".php"'
add rewrite policy pol1 'HTTP.REQ.URL.PATH.REGEX_MATCH(re#^/([a-z]+)$#)
    ' act1
bind rewrite global pol1 100
<!--NeedCopy-->
```

Apache mod_rewrite Lösung zum Hinzufügen von HTML- oder PHP-Erweiterungen zu Anfragen

```
RewriteCond %{
 REQUEST_FILENAME }
 .php -f
RewriteRule ^/?([a-zA-Z0-9]+)$ $1.php [L]
RewriteCond %{
 REQUEST_FILENAME }
 .html  - f
RewriteRule ^/?([a-zA-Z0-9]+)$ $1.html [L]
<!--NeedCopy-->
```

Citrix ADC Richtlinie zum Hinzufügen von HTML- oder PHP-Erweiterungen zu Anforderungen

```
add HTTPCallout Call_html
add HTTPCallout Call_php
set policy httpCallout Call_html -IPAddress 10.102.59.101 -port 80 -
    hostExpr '"10.102.59.101"' -returnType BOOL -ResultExpr 'HTTP.RES.
    BODY(100).CONTAINS("True")'  -urlStemExpr '"/cgi-bin/file_check.cgi"
    '   -parameters query=http.req.url+".html"
set policy httpCallout Call_php -IPAddress 10.102.59.101 -port 80 -
    hostExpr '"10.102.59.101"' -returnType BOOL -ResultExpr 'HTTP.RES.
    BODY(100).CONTAINS("True")'  -urlStemExpr '"/cgi-bin/file_check.cgi"
    ' -parameters query=http.req.url+".php"
add patset pat1
bind patset pat1 .html
bind patset pat1 .php
bind patset pat1 .asp
bind patset pat1 .cgi
add rewrite  action act1 insert_after 'HTTP.REQ.URL.PATH'  '".html"'
add rewrite  action act2 insert_after "HTTP.REQ.URL.PATH"  '".php"'
```



```
12 add rewrite policy pol1 '!HTTP.REQ.URL.CONTAINS_ANY(”pat1”) && SYS.
      HTTP_CALLOUT(Call_html)' act1
13 add rewrite policy pol2 '!HTTP.REQ.URL.CONTAINS_ANY(”pat1”) && SYS.
      HTTP_CALLOUT(Call_php)' act2
14 bind rewrite global pol1 100 END
15 bind rewrite global pol2 101 END
16
17 <!--NeedCopy-->
```

Umleiten eines Working URI in ein neues Format

Angenommen, Sie haben eine Reihe von funktionierenden URLs, die der folgenden ähneln:

```
1 /index.php?id=nnnn
2
3 <!--NeedCopy-->
```

Um diese URLs in /nnnn zu ändern und sicherzustellen, dass Suchmaschinen ihre Indizes auf das neue URI-Format aktualisieren, müssen Sie Folgendes tun:

- Leiten Sie die alten URIs auf die neuen um, damit Suchmaschinen ihre Indizes aktualisieren.
- Schreiben Sie den neuen URI zurück in den alten, so dass das Skript index.php korrekt ausgeführt wird.

Um dies zu erreichen, können Sie Markercode in die Abfragezeichenfolge einfügen (sicherstellen, dass der Markercode von Besuchern nicht gesehen wird) und dann den Markercode für das Skript index.php entfernen.

Die folgenden Beispiele leiten nur dann von einem alten Link in ein neues Format um, wenn kein Marker in der Abfragezeichenfolge vorhanden ist. Der Link, der das neue Format verwendet, wird in das alte Format zurückgeschrieben, und der Abfragezeichenfolge wird ein Marker hinzugefügt.

Apache mod_rewrite Lösung

```
1 RewriteCond %{
2  QUERY_STRING }
3   !marker
4 RewriteCond %{
5  QUERY_STRING }
6   id=([-a-zA-Z0-9_+]+)
7 RewriteRule ^/?index.php$ %1? [R,L]
8 RewriteRule ^/?([-a-zA-Z0-9_+]+)$  index.php?marker&id=$1 [L]
```



```
Citrix ADC solution
add responder action act_redirect redirect 'HTTP.REQ.URL.PATH.
    BEFORE_STR(”index.php”)+HTTP.REQ.URL.QUERY.VALUE(”id”)' -
    bypassSafetyCheck yes
add responder policy pol_redirect '!HTTP.REQ.URL.QUERY.CONTAINS(”marker
    ”)&& HTTP.REQ.URL.QUERY.VALUE(”id”).REGEX_MATCH(re/[-a-zA-Z0-9_+]+/)
     && HTTP.REQ.URL.PATH.CONTAINS(”index.php”)' act_redirect
bind responder global pol_redirect 100 END
add rewrite action act1 replace 'HTTP.REQ.URL.PATH.SUFFIX('/',0)' '”
    index.phpmarker&id=”+HTTP.REQ.URL.PATH.SUFFIX('/',0)' -
    bypassSafetyCheck yes
add rewrite policy pol1 '!HTTP.REQ.URL.QUERY.CONTAINS(”marker”)'  act1
bind rewrite global pol1 100 END

<!--NeedCopy-->
```

Sicherstellen, dass ein sicherer Server für ausgewählte Seiten verwendet wird

Um sicherzustellen, dass nur sichere Server für ausgewählte Webseiten verwendet werden, können Sie die folgenden Apache mod_rewrite Code oder Citrix ADC Responder-Richtlinien verwenden.

Apache mod_rewrite Lösung

```
RewriteCond %{
 SERVER_PORT }
  !^443$
RewriteRule ^/?(page1|page2|page3|page4|page5)$  https://www.example.
    com/%1 [R,L]

<!--NeedCopy-->
```

Citrix ADC Lösung mit regulären Ausdrücken

```
add responder action res_redirect redirect  '”https://www.example.com”+
    HTTP.REQ.URL' -bypassSafetyCheck yes
add responder policy pol_redirect '!CLIENT.TCP.DSTPORT.EQ(443)&&HTTP.
    REQ.URL.REGEX_MATCH(re/page[1-5]/)'  res_redirect
bind responder global pol_redirect 100 END

<!--NeedCopy-->
```


Citrix ADC Lösung mit Mustersätzen

```
add patset pat1
bind patset pat1 page1
bind patset pat1 page2
bind patset pat1 page3
bind patset pat1 page4
bind patset pat1 page5
add responder action res_redirect redirect  '"https://www.example.com"+
   HTTP.REQ.URL' -bypassSafetyCheck yes
add responder policy pol_redirect '!CLIENT.TCP.DSTPORT.EQ(443)&&HTTP.
   REQ.URL.CONTAINS_ANY("pat1")'  res_redirect
bind responder global pol_redirect 100 END

<!--NeedCopy-->
```

Beispiele für Rewrite und Responder Policy

October 5, 2021

Im Folgenden finden Sie einige Beispiele für Rewrite- und Responder-Richtlinien:

Beispiel 1: So fügen Sie einen lokalen Client-IP-Header mit der Befehlszeilenschnittstelle hinzu

```
add rewrite action act_ins_client insert_http_header NS-Client 'CLIENT.
   IP.SRC'
add rewrite policy pol_ins_client http.req.is_valid act_ins_client
bind rewrite global pol_ins_client 300 END

namem@obelix:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
< HTTP/1.1 200 OK
< Date: Tue, 10 Nov 2020 10:06:48 GMT
```



```
* Server Apache/2.2.15 (CentOS) is not blacklisted
< Server: Apache/2.2.15 (CentOS)
< Last-Modified: Thu, 20 Jun 2019 07:16:04 GMT
< ETag: ”816c5-5-58bbc1e73cdd3”
< Accept-Ranges: bytes
< Content-Length: 5
< Content-Type: text/html; charset=UTF-8
< NS-Client: 10.102.1.98
<
* Connection #0 to host 10.10.10.10 left intact
JLEwxt_namem@obelix:~$

<!--NeedCopy-->
```

Beispiel 2: Maskieren Sie den HTTP-Servertyp

```
add rewrite action Action-Rewrite-Server_Mask REPLACE HTTP.RES.HEADER(”Server”) ””Web Server 1.0””
add rewrite policy Policy-Rewrite-Server_Mask HTTP.RES.IS_VALID Action-Rewrite-Server_Mask NOREWRITE
namem@obelix:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
< HTTP/1.1 200 OK
< Date: Tue, 10 Nov 2020 10:15:42 GMT
* Server Web Server 1.0 is not blacklisted
< Server: Web Server 1.0
< Last-Modified: Thu, 20 Jun 2019 07:16:04 GMT
< ETag: ”816c5-5-58bbc1e73cdd3”
< Accept-Ranges: bytes
< Content-Length: 5
< Content-Type: text/html; charset=UTF-8
<
* Connection #0 to host 10.10.10.10 left intact
JLEwxt_namem@obelix:~$
<!--NeedCopy-->
```


Beispiel 3: Reagieren Sie, indem Sie zu einer anderen URL umleiten, wenn eine URL empfangen wird

```
> add responder action act1 redirect ””www.google.com””
 Done
> add responder policy pol1 'HTTP.REQ.URL.CONTAINS(”file”)' act1
 Done
> bind responder global pol1 1
 Done
>

name:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
< HTTP/1.1 302 Found : Moved Temporarily
< Location: www.google.com
< Connection: close
< Cache-Control: no-cache
< Pragma: no-cache
<
* Closing connection 0
name@obelix:~$
<!--NeedCopy-->
```

Beispiel 4: Antworte mit einer Nachricht, die ein beliebiger Ausdruck oder ein Text sein kann

```
add responder action act123 respondwith ””Please reach out to
   administrator””
add responder policy pol1 ”HTTP.REQ.URL.CONTAINS(”file”)” act123
bind responder global pol1 100 END

name@obelix:~$ curl -v http://10.10.10.10/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10..Responder Action and Policy:

```



```
>add responder action Redirect-Action redirect ""https://xyz.abc.com/dispatcher/SAML2AuthService?siteurl=wmav"" -responseStatusCode 302

>add responder policy Redirect-Policy "HTTP.REQ.HOSTNAME.CONTAINS("abc")" Redirect-Action

Binding to LB Virtual Server:

>bind lb vserver Test1_SF -policyName Redirect-Policy -priority 100 -gotoPriorityExpression END -type REQUEST.
* Connected to 10.10.10.10 (10.10.10.10) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.10.10.10
> Accept: \*/\*
>
* Connection #0 to host 10.10.10.10 left intact
Please reach out to administratort_name@obelix:~$
<!--NeedCopy-->
```

Beispiel 5: Reagieren Sie mit einer importierten HTML-Seite

```
import responder htmlpage http://10.10.10.10)/testsite/file5.html page112
add responder action act1 respondwithHtmlpage page1
add responder policy pol1 true act1
bind responder global pol1 100

name@obelix:~$ curl -v http://10.10.10.10)/testsite/file5.html
* Hostname was NOT found in DNS cache
*   Trying 10.10.10.10...
* Connected to 10.10.10.10 (10.10.10.10)) port 80 (#0)
> GET /testsite/file5.html HTTP/1.1
> User-Agent: curl/7.35.0
> Host: 10.102.58.140
> Accept: \*/\*
>
< HTTP/1.1 200 OK
< Content-Length: 5
< Content-Type: text/html
<
* Connection #0 to host 10.10.10.10 left intact
JLEwxt_name@obelix:~$
```



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

Beispiel 6: Umleitung von URL basierend auf HOSTNAME mithilfe der Responder-Richtlinie

```
Responder Action and Policy:

>add responder action Redirect-Action redirect ""https://xyz.abc.com/dispatcher/SAML2AuthService?siteurl=wmav"" -responseStatusCode 302

>add responder policy Redirect-Policy "HTTP.REQ.HOSTNAME.CONTAINS("abc")" Redirect-Action

Binding to LB Virtual Server:

>bind lb vserver Test1_SF -policyName Redirect-Policy -priority 100 -gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

Ratenbegrenzung

October 5, 2021

Mit der Ratenbegrenzungsfunktion können Sie die maximale Last für eine bestimmte Netzwerkentität oder eine virtuelle Entität auf der Citrix ADC Appliance definieren. Mit der Funktion können Sie die Appliance so konfigurieren, dass die Datenverkehrsrate der Entität überwacht und Präventivmaßnahmen in Echtzeit basierend auf der Datenverkehrsrate ergriffen werden. Diese Funktion ist besonders nützlich, wenn das Netzwerk von einem feindlichen Client angegriffen wird, der der Appliance eine Flut von Anfragen sendet. Sie können die Risiken verringern, die sich auf die Verfügbarkeit von Ressourcen für Clients auswirken, und Sie können die Zuverlässigkeit des Netzwerks und der von der Appliance verwalteten Ressourcen verbessern.

Sie können die Datenverkehrsrate überwachen und steuern, die virtuellen und benutzerdefinierten Entitäten zugeordnet ist, einschließlich virtueller Server, URLs, Domänen und Kombinationen von URLs und Domänen. Sie können die Datenverkehrsrate einschränken, wenn sie zu hoch ist, die Datenspeicherung anhand der Datenverkehrsrate zugrunde legen und den Datenverkehr an einen bestimmten virtuellen Lastausgleichsserver umleiten, wenn die Datenverkehrsrate einen vordefinierten Grenzwert überschreitet. Sie können ratenbasierte Überwachung auf HTTP-, TCP- und DNS-Anforderungen anwenden.

Um die Rate des Datenverkehrs für ein bestimmtes Szenario zu überwachen, konfigurieren Sie eine *Rate Limit Identifier*. Ein Ratengrenzbezeichner gibt numerische Schwellenwerte an, z. B. die maximale Anzahl von Anforderungen oder Verbindungen (eines bestimmten Typs), die in einem bestimmten Zeitraum, der als *Zeitscheibe*bezeichnet wird, zulässig sind.

Optional können Sie Filter, sogenannte *Stream-Selektoren*, konfigurieren und diese bei der Konfiguration der Bezeichner mit Ratenbegrenzungskennungen verknüpfen. Nachdem Sie den optionalen Stream-Selektor und den Grenzbezeichner konfiguriert haben, müssen Sie den Grenzbezeichner aus einer Standard-Syntaxrichtlinie aufrufen. Sie können Bezeichner von jedem Feature aufrufen, in dem der Bezeichner nützlich sein kann, einschließlich Rewrite, Responder, DNS und integriertem Caching.

Sie können SNMP-Traps für Ratengrenzbezeichner global aktivieren und deaktivieren. Jedes Trap enthält kumulative Daten für das konfigurierte Datenerfassungsintervall (Zeitabschnitt) des Grenzwertbezeichners, es sei denn, Sie haben mehrere Traps angegeben, die pro Zeitabschnitt generiert werden sollen. Weitere Informationen zum Konfigurieren von SNMP-Traps und -Managern finden Sie unter SNMP.

Konfigurieren eines Stream-Selektors

October 5, 2021

Ein Traffic-Stream-Selektor ist ein optionaler Filter zum Identifizieren einer Entität, für die Sie den Zugriff drosseln möchten. Der Selektor wird auf eine Anforderung oder eine Antwort angewendet und wählt Datenpunkte (Schlüssel) aus, die mit einer Rate Stream Identifier analysiert werden können. Diese Datenpunkte können auf fast jedem Merkmal des Datenverkehrs basieren, einschließlich IP-Adressen, Subnetze, Domänennamen, TCP- oder UDP-Bezeichner und bestimmten Strings oder Erweiterungen in URLs.

Ein Stream-Selektor besteht aus einzelnen Standard-Syntaxausdrücken, die selectlets genannt werden. Jedes Selectlet ist ein nicht zusammengesetzter Standard-Syntaxausdruck. Ein Traffic-Stream-Selektor kann bis zu fünf nicht-zusammengesetzte Ausdrücke enthalten, die als selectlets bezeichnet werden. Jedes Selectlet wird als in einer AND- Beziehung mit den anderen Ausdrücken betrachtet. Im Folgenden sind einige Beispiele für Selektlets:

```
1 http.req.url
2 http.res.body(1000>after_str(”car_model”).before_str(”made_in”)”
3 ”client.ip.src.subnet(24)”
4 <!--NeedCopy-->
```


Die Reihenfolge, in der Sie Parameter angeben, ist signifikant. Wenn Sie beispielsweise eine IP-Adresse und eine Domäne (in dieser Reihenfolge) in einem Selektor konfigurieren und dann die Domäne und die IP-Adresse (in umgekehrter Reihenfolge) in einem anderen Selektor angeben, betrachtet Citrix ADC diese Werte als eindeutig. Dies kann dazu führen, dass dieselbe Transaktion zweimal gezählt wird. Wenn mehrere Richtlinien denselben Selektor aufrufen, kann der Citrix ADC erneut dieselbe Transaktion mehrmals zählen.

Hinweis: Wenn Sie einen Ausdruck in einem Stream-Selektor ändern, erhalten Sie möglicherweise einen Fehler, wenn eine Richtlinie, die ihn aufruft, an eine neue Richtlinienbezeichnung oder einen neuen Bindepunkt gebunden ist. Angenommen, Sie erstellen einen Stream-Selektor namens myStreamSelector1, rufen ihn aus myLimitID1 auf und rufen den Bezeichner aus einer DNS-Richtlinie namens dnsRateLimit1 auf. Wenn Sie den Ausdruck in myStreamSelector1 ändern, wird möglicherweise eine Fehlermeldung angezeigt, wenn Sie dnsRateLimit1 an einen neuen Bindepunkt binden. Die Problemumgehung besteht darin, diese Ausdrücke zu ändern, bevor die Richtlinien erstellt werden, die sie aufrufen.

So konfigurieren Sie einen Traffic-Stream-Selektor mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add stream selector <name> <rule> ...
<!--NeedCopy-->
```

Beispiel:

```
add stream selector myStreamSel HTTP.REQ.URL CLIENT.IP.SRC
<!--NeedCopy-->
```

So konfigurieren Sie einen Stream-Selektor mit dem Konfigurationsdienstprogramm

Navigieren Sie zu AppExpert > Ratenbegrenzung > Selektoren, klicken Sie auf Hinzufügen und geben Sie die relevanten Details an.

Konfigurieren eines Grenzwertbezeichners für Traffic Rate Limit

October 5, 2021

Ein Ratenlimit-Bezeichner prüft, ob der Datenverkehr innerhalb eines bestimmten Zeitintervalls einen bestimmten Wert überschreitet. Der Bezeichner gibt einen "Booleschen TRUE" zurück, wenn der Datenverkehr innerhalb eines bestimmten Zeitintervalls einen Grenzwert überschreitet. Wenn Sie einen Grenzwertbezeichner in den zusammengesetzten Standardsyntaxausdruck in eine Richtlinienregel einfügen, müssen Sie einen Streamselektor einschließen. Wenn Sie nicht angeben, wird die Limitkennung auf alle Anforderungen oder Antworten angewendet, die durch die zusammengesetzten Ausdrücke identifiziert werden.

> **Hinweis:**
>
> Die maximale Länge zum Speichern von Zeichenfolgenergebnissen (z. B. HTTP.REQ.URL) beträgt 60 Zeichen. Wenn die Zeichenfolge (z. B. URL) 1000 Zeichen lang ist, von denen 50 Zeichen lang genug sind, um eine Zeichenfolge eindeutig zu identifizieren, können Sie einen Ausdruck verwenden, um erforderliche 50 Zeichen zu extrahieren.

So konfigurieren Sie einen Grenzbezeichner über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add ns limitIdentifier <limitIdentifier> -threshold <positive_integer>
      -timeSlice <positive_integer> -mode <mode> -limitType ( BURSTY |
      SMOOTH ) -selectorName <string> -maxBandwidth <positive_integer> -
      trapsInTimeSlice <positive_integer>
2 <!--NeedCopy-->
```

Argumentbeschreibung

limitIdentifier. Name für einen Zinsgrenzbezeichner. Muss mit einem ASCII-Buchstaben oder einem Unterstrich (_) beginnen und nur aus alphanumerischen ASCII-Zeichen oder Unterstrichen bestehen. Reservierte Wörter dürfen nicht verwendet werden. Dies ist ein obligatorisches Argument. Maximale Länge: 31

threshold. Eine maximale Anzahl von Anforderungen, die in der angegebenen Zeitdauer zulässig sind, wenn Anforderungen (Modus ist als REQUEST_RATE festgelegt) pro Zeiteinheit verfolgt werden. Wenn Verbindungen (Modus wird als CONNECTION festgelegt) verfolgt werden, ist dies die Gesamtzahl der Verbindungen, die durchgelassen werden würden. Standardwert: 1 Mindestwert: 1 Maximaler Wert: 4294967295

timeSlice. Zeitintervall, in Millisekunden, angegeben in Vielfaches von 10, während dessen Anforderungen verfolgt werden, um zu überprüfen, ob sie den Schwellenwert überschreiten. Dieses Argument wird nur benötigt, wenn der Modus auf REQUEST_RATE gesetzt ist. Standardwert: 1000 Mindestwert: 10 Maximalwert: 4294967295

mode. Definiert den Typ des Datenverkehrs, der verfolgt werden soll.

1. REQUEST_RATE. Verfolgt Anforderungen/Zeitlice.
2. CONNECTION. Verfolgt aktive Transaktionen.

limitType. Anforderungstyp Smooth oder Bursty.

selectorName. Name des Steuerungsgrenzwerts. Wenn dieses Argument NULL ist, wird die Ratenbegrenzung auf den gesamten Datenverkehr angewendet, der vom virtuellen Server oder vom Citrix ADC empfangen wird (je nachdem, ob der Grenzbezeichner an einen virtuellen Server oder global gebunden ist) ohne **Filterung. Maximale Länge: 31**

maxBandwidth. Maximale zulässige Bandbreite, in kbps. Mindestwert: 0 Maximalwert: 4294967287

Beispiel:

Konfigurieren der Begrenzungskennung für die Verkehrsrate im BURSTY Modus:

```
add ns limitIdentifier 100_request_limit -threshold 100 -timeSlice 1000
     -mode REQUEST_RATE -limitType BURSTY -selectorName
    limit_100_requests_selector -trapsInTimeSlice 30
<!--NeedCopy-->
```

Konfigurieren der Begrenzungskennung für die Verkehrsrate im SMOOTH-Modus:

```
add ns limitidentifier limit_req -mode request_rate -limitType smooth -
    timeslice 1000 -Threshold 2000 -trapsInTimeSlice 200
<!--NeedCopy-->
```

So konfigurieren Sie eine Datenverkehrslimit-ID mit dem Konfigurationsdienstprogramm

Navigieren Sie zu AppExpert > Rate Limiting > Limit Identifiers, klicken Sie auf Hinzufügen und geben Sie die relevanten Details an.

Konfigurieren und Binden einer Traffic Rate Policy

October 5, 2021

Sie implementieren ratenbasiertes Anwendungsverhalten, indem Sie eine Richtlinie in einem geeigneten Citrix ADC Feature konfigurieren. Das Feature muss Standard-Syntaxrichtlinien unter-

stützen. Der Richtlinienausdruck muss das folgende Ausdruckspräfix enthalten, damit das Feature die Datenverkehrsrate analysieren kann:

```
sys.check_limit(<limit_identifier>)
<!--NeedCopy-->
```

Dabei ist limit_identifier der Name eines Grenzbezeichners.

Der Richtlinienausdruck muss ein zusammengesetzter Ausdruck sein, der mindestens zwei Komponenten enthält:

- Ein Ausdruck, der den Datenverkehr angibt, auf den der Grenzwertbezeichner angewendet wird. Beispiel:

```
    http.req.url.contains("my_aspx.aspx").
<!--NeedCopy-->
```

- Ein Ausdruck, der einen Grenzwertbezeichner identifiziert, z. B. sys.check_limit (my_limit_identifier). Dies muss der letzte Ausdruck im Richtlinienausdruck sein.

So konfigurieren Sie eine ratenbasierte Richtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine ratenbasierte Richtlinie zu konfigurieren und die Konfiguration zu überprüfen:

```
add cache|dns|rewrite|responder policy <policy_name> -rule expression
    && sys.check_limit("<LimitIdentifierName>") [<feature-specific
    information>]
<!--NeedCopy-->
```

Es folgt ein vollständiges Beispiel für eine ratenbasierte Richtlinienregel. Beachten Sie, dass in diesem Beispiel davon ausgegangen wird, dass Sie die Responder-Aktion send_direct_url konfiguriert haben, die der Richtlinie zugeordnet ist. Beachten Sie, dass der Parameter sys.check_limit das letzte Element des Richtlinienausdrucks sein muss:

```
add responder policy responder_threshold_policy "http.req.url.contains(
    "myindex.html") && sys.check_limit("my_limit_identifier")"
    send_direct_url
<!--NeedCopy-->
```


Informationen zum globalen Binden einer Richtlinie oder an einen virtuellen Server finden Sie unter “Binden von Standardsyntaxrichtlinien. “

So konfigurieren Sie eine ratenbasierte Richtlinie mit dem Konfigurationsdienstprogramm

1. Erweitern Sie im Navigationsbereich das Feature, in dem Sie eine Richtlinie konfigurieren möchten (z. B. Integriertes Caching, Umschreiben oder Responder), und klicken Sie dann auf Richtlinien.
2. Klicken Sie im Detailbereich auf “Hinzufügen”. Geben Sie unter Name einen eindeutigen Namen für die Richtlinie ein.
3. Geben Sie unter Ausdruck die Richtlinienregel ein, und stellen Sie sicher, dass Sie den Parameter sys.check_limit als letzte Komponente des Ausdrucks einschließen. Beispiel:

```
1 http.req.url.contains(”my_aspx.aspx”) && sys.check_limit(”
     my_limit_identifier”)
2 <!--NeedCopy-->
```

4. Geben Sie funktionsspezifische Informationen zur Richtlinie ein.

   Beispielsweise müssen Sie die Richtlinie einer Aktion oder einem Profil zuordnen. Weitere Informationen finden Sie in der funktionsspezifischen Dokumentation.
5. Klicken Sie auf Erstellenund dann auf Schließen.
6. Klicken Sie auf Speichern.

Traffic Rate anzeigen

October 5, 2021

Wenn der Datenverkehr über einen oder mehrere virtuelle Server einer ratenbasierten Richtlinie entspricht, können Sie die Rate dieses Datenverkehrs anzeigen. Die Kursstatistiken werden in der Limit-ID verwaltet, die Sie in der Regel für die ratenbasierte Richtlinie benannt haben. Wenn mehr als eine Richtlinie denselben Grenzbezeichner verwendet, können Sie die Datenverkehrsrate anzeigen, wie sie durch Treffer für alle Richtlinien definiert ist, die den jeweiligen Grenzbezeichner verwenden.

So zeigen Sie die Datenverkehrsrate mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die Datenverkehrsrate anzuzeigen:

```
show ns limitSessions <limitIdentifier>
<!--NeedCopy-->
```

Beispiel:

```
sh limitsession myLimitSession
<!--NeedCopy-->
```

So zeigen Sie die Datenverkehrsrate mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu AppExpert > Ratenbegrenzung > Limit-Kennungen.
2. Wählen Sie einen Grenzbezeichner aus, dessen Verkehrsrate Sie anzeigen möchten.
3. Klicken Sie auf die Schaltfläche Sitzungen anzeigen. Wenn der Datenverkehr über einen oder mehrere virtuelle Server einer Richtlinie zur Begrenzung der Rate entspricht, die diesen Grenzbezeichner verwendet (und die Treffer innerhalb des konfigurierten Zeitabschnitts für diesen Bezeichner liegen), wird das Dialogfeld Sitzungsdetails angezeigt. Andernfalls erhalten Sie eine Meldung Keine Sitzung vorhanden.

Testen einer ratenbasierten Richtlinie

October 5, 2021

Zum Testen einer ratenbasierten Richtlinie können Sie Datenverkehr an jeden virtuellen Server senden, an den eine ratenbasierte Richtlinie gebunden ist.

Aufgabenübersicht: Testen einer ratenbasierten Policy

1. Konfigurieren Sie einen Stream-Selektor (optional) und eine Rate Limit Identifier (erforderlich). Beispiel:

```
add stream selector sel_subnet Q.URL ”CLIENT.IP.SRC.SUBNET(24)”
```



```
2 add ns limitIdentifier k_subnet -Threshold 4 -timeSlice 3600 -mode
      REQUEST_RATE  -limittype smooth  -selectorName sel_subnet  -
     trapsInTimeSlice 8
3 <!--NeedCopy-->
```

2. Konfigurieren Sie die Aktion, die Sie der Richtlinie zuordnen möchten, die den Steuerbeschränkungsbezeichner verwendet. Beispiel:

```
1 add responder action resp_redirect redirect ""http://response_site
     .com/""
2 <!--NeedCopy-->
```

3. Konfigurieren Sie eine Richtlinie, die das Ausdruckspräfix sys.check_limit verwendet, um den Grenzwertbezeichner aufzurufen. Beispielsweise kann die Richtlinie einen Zinsgrenzbezeichner auf alle Anforderungen anwenden, die aus einem bestimmten Subnetz eintreffen, wie folgt:

```
1 add responder policy resp_subnet "SYS.CHECK_LIMIT("k_subnet")"
     resp_redirect
2 <!--NeedCopy-->
```

4. Binden Sie die Richtlinie global oder an einen virtuellen Server. Beispiel:

```
1 bind responder global resp_subnet 6 END -type DEFAULT
2 <!--NeedCopy-->
```

5. Senden Sie in einer Browser-Adressleiste eine Test-HTTP-Abfrage an einen virtuellen Server. Beispiel:

```
1 http://<IP of a vserver>/testsite/test.txt
2 <!--NeedCopy-->
```

6. Geben Sie an der Citrix ADC Eingabeaufforderung Folgendes ein:

```
1 show ns limitSessions <limitIdentifier>
2 <!--NeedCopy-->
```

Beispiel


```
> sh limitsession k_subnet
1)      Time Remaining:       98 secs  Hits: 2
                             Action Taken: 0
        Total Hash:    1718618  Hash String: /test.txt
        IPs gathered:
                1) 10.217.253.0
        Active Transactions: 0
 Done
>
<!--NeedCopy-->
```

7. Wiederholen Sie die Abfrage, und überprüfen Sie erneut die Statistik der Begrenzungskennung, um zu überprüfen, ob die Statistiken korrekt aktualisiert werden.

Beispiele für ratenbasierte Richtlinien

October 5, 2021

Die folgende Tabelle zeigt Beispiele für ratenbasierte Richtlinien.

Table 1. Examples of Rate-Based Policies

Purpose	Example

Limit the number of requests per second from a URL	`add stream selector ipStreamSelector http.req.url "client.ip.src"`
	`add ns limitIdentifier ipLimitIdentifier -threshold 4 -timeSlice 1000`
	`-mode request_rate -limitType smooth -selectorName ipStreamSelector`
	
	`add responder action myWebSiteRedirectAction redirect`
	`"\"http://www.mycompany.com/\""`
	
	`add responder policy ipLimitResponderPolicy "http.req.url.contains(\"myasp.asp\")`
	`&& sys.check_limit(\"ipLimitIdentifier\")" myWebSiteRedirectAction`
	
	`bind responder global ipLimitResponderPolicy 100 END -type default`

Cache a response if the request URL rate exceeds 5 per 20000 milliseconds	`add stream selector cacheStreamSelector http.req.url`
	`add ns limitidentifier cacheRateLimitIdentifier -threshold 5 -timeSlice 2000`
	`-selectorName cacheStreamSelector`
	
	`add cache policy cacheRateLimitPolicy -rule "http.req.method.eq(get)`
	`&& sys.check_limit(\"cacheRateLimitIdentifier\")" -action cache`
	
	`bind cache global cacheRateLimitPolicy -priority 10`

Drop a connection on the basis of cookies received in requests from www.yourcompany.com if the requests exceed the rate limit	`add stream selector reqCookieStreamSelector "http.req.cookie`
	`.value(\"mycookie\")" "client.ip.src.subnet(24)"`
	
	`add ns limitIdentifier myLimitIdentifier -Threshold 2 -timeSlice 3000`
	`-selectorName reqCookieStreamSelector`
	
	`add responder action sendRedirectUrl redirect '\"http://www.mycompany.com\"`
	`+ http.req.url' -bypassSafetyCheck YES`
	
	`add responder policy rateLimitCookiePolicy`
	`"http.req.url.contains(\"www.yourcompany.com\")`
	`&& sys.check_limit(\"myLimitIdentifier\")" sendRedirectUrl`

Drop a DNS packet if the requests from a particular client IP address and DNS domain exceed the rate limit	`add stream selector dropDNSStreamSelector client.udp.dns.domain client.ip.src`
	`add ns limitIdentifier dropDNSRateIdentifier -timeslice 20000 -mode request_rate`
	`-selectorName dropDNSStreamSelector -maxBandwidth 1 -trapsintimeslice 20`
	
	`add dns policy dnsDropOnClientRatePolicy "sys.check_limit`
	`(\"dropDNSRateIdentifier\")" -drop yes`

Limit the number of HTTP requests that arrive from the same host (with a subnet mask of 32) and that have the same destination IP address.	`add stream selector ipv6_sel "CLIENT.IPv6.src.subnet(32)" CLIENT.IPv6.dst Q.URL`
	`add ns limitIdentifier ipv6_id -imeSlice 20000 -selectorName ipv6_sel`
	`add lb vserver ipv6_vip HTTP 3ffe::209 80 -persistenceType NONE -cltTimeout 180`
	`add responder action redirect_page redirect "\"http://redirectpage.com/\""`
	`add responder policy ipv6_resp_pol "SYS.CHECK_LIMIT(\"ipv6_id\")" redirect_page`
	`bind responder global ipv6_resp_pol 5 END -type DEFAULT`

Anwendungsbeispiele für ratenbasierte Richtlinien

October 5, 2021

In den folgenden Szenarien werden zwei Verwendungen ratenbasierter Richtlinien im globalen Server Load Balancing (GSLB) beschrieben:

- Im ersten Szenario wird die Verwendung einer ratenbasierten Richtlinie beschrieben, die Datenverkehr an ein neues Rechenzentrum sendet, wenn die Rate von DNS-Anforderungen 1000 pro Sekunde überschreitet.
- Wenn im zweiten Szenario mehr als fünf DNS-Anforderungen für einen lokalen DNS-Client (LDNS) innerhalb eines bestimmten Zeitraums eintreffen, werden die zusätzlichen Anforderungen gelöscht.

Umleiten von Traffic auf Basis der Traffic Rate

In diesem Szenario konfigurieren Sie eine Proximity-basierte Load Balancing-Methode und eine ratenbegrenzende Richtlinie, die DNS-Anforderungen für eine bestimmte Region identifiziert. In der Richtlinie zur Ratenbegrenzung geben Sie einen Schwellenwert von 1000 DNS-Anforderungen pro Sekunde an. Eine DNS-Richtlinie wendet die Richtlinie zur Begrenzung der Rate auf DNS-Anfragen für die Region Europe.GB.17.London.UK-East.ISP-UK. In der DNS-Richtlinie werden DNS-Anforderungen, die den Schwellenwert überschreiten, beginnend mit Anforderung 1001 bis zum Ende des Intervalls von einer Sekunde, an die IP-Adressen weitergeleitet, die mit der Region North America.us.tx.Dallas.US-East.ISP-US verbunden sind.

Die folgende Konfiguration veranschaulicht dieses Szenario:

```
add stream selector DNSSelector1 client.udp.dns.domain

add ns limitIdentifier DNSLimitIdentifier1 -threshold 5 -timeSlice 1000
    -selectorName DNSSelector1

add dns policy DNSLimitPolicy1 "client.ip.src.matches_location("Europe.
   GB.17.London.\*.\*") &&
sys.check_limit("DNSLimitIdentifier1")" -preferredLocation "North
   America.US.TX.Dallas.\*.\*"

bind dns global DNSLimitPolicy1 5
<!--NeedCopy-->
```


Löschen von DNS-Anforderungen auf der Grundlage der Datenverkehrsrate

Im folgenden Beispiel für den globalen Server-Lastausgleich konfigurieren Sie eine Richtlinie zur Begrenzung der Rate, die es zulässt, dass maximal fünf DNS-Anforderungen in einem bestimmten Intervall pro Domäne zur Auflösung an einen LDNS-Client weitergeleitet werden. Alle Anforderungen, die diese Rate überschreiten, werden gelöscht. Diese Art von Richtlinie kann den Citrix ADC vor Ressourcenausnutzung schützen. In diesem Szenario beispielsweise, wenn die Zeit zum Leben (TTL) für eine Verbindung fünf Sekunden beträgt, verhindert diese Richtlinie, dass LDNS eine Domäne anfordern. Stattdessen werden Daten verwendet, die auf dem Citrix ADC zwischengespeichert werden.

```
1  add stream selector LDNSSelector1 client.udp.dns.domain client.ip.src
2
3  add ns limitIdentifier LDNSLimitIdentifier1 -threshold 5 -timeSlice
       1000 -selectorName LDNSSelector1
4
5  add dns policy LDNSPolicy1 "client.udp.dns.domain.contains(".") && sys.
       check_limit("LDNSLimitIdentifier1")" -drop YES
6
7  bind dns global LDNSPolicy1 6
8
9  show gslb vserver gvip
10
11 gvip - HTTP     State: UP
12 Last state change was at Mon Sep  8 11:50:48 2008 (+711 ms)
13 Time since last state change: 1 days, 02:55:08.830
14 Configured Method: STATICPROXIMITY
15 BackupMethod: ROUNDROBIN
16 No. of Bound Services :  3 (Total)       3 (Active)
17 Persistence: NONE       Persistence ID: 100
18 Disable Primary Vserver on Down: DISABLED       Site Persistence: NONE
19 Backup Session Timeout: 0
20 Empty Down Response: DISABLED
21 Multi IP Response: DISABLED Dynamic Weights: DISABLED
22 Cname Flag: DISABLED
23 Effective State Considered: NONE
24 1.     site11_svc(10.100.00.00: 80)- HTTP State: UP    Weight: 1
25 Dynamic Weight: 0       Cumulative Weight: 1
26 Effective State: UP
27 Threshold : BELOW
28 Location: Europe.GB.17.London.UK-East.ISP-UK
29 2.      site12_svc(10.101.00.100: 80)- HTTP State: UP   Weight: 1
30 Dynamic Weight: 0       Cumulative Weight: 1
31 Effective State: UP
```



```
Threshold : BELOW
Location: North America.US.TX.Dallas.US-East.ISP-US
3.      site13_svc(10.102.00.200: 80)- HTTP State: UP   Weight: 1
Dynamic Weight: 0       Cumulative Weight: 1
Effective State: UP
Threshold : BELOW
Location: North America.US.NJ.Salem.US-Mid.ISP-US
4.      www.gslbindia.com        TTL: 5 secn
Cookie Timeout: 0 min   Site domain TTL: 3600 sec
Done
<!--NeedCopy-->
```

Preisbegrenzung für Traffic-Domains

October 5, 2021

Sie können die Begrenzung der Rate für Traffic-Domains konfigurieren. Der folgende Ausdruck in der Citrix ADC Ausdruckssprache für identifiziert den Datenverkehr, der mit Verkehrsdomänen verknüpft ist.

- client.traffic_domain.id

Sie können die Begrenzung der Rate für den Datenverkehr konfigurieren, der einer bestimmten Verkehrsdomäne, einer Gruppe von Verkehrsdomänen oder allen Verkehrsdomänen zugeordnet ist.

Zum Konfigurieren der Ratenbegrenzung für Datenverkehrsdomänen führen Sie die folgenden Schritte auf einer Citrix ADC Appliance mit dem Konfigurationsdienstprogramm oder der Citrix ADC-Befehlszeile aus:

1. Konfigurieren Sie einen Stream-Selektor, der den Ausdruck client.traffic_domain.id verwendet, um den Datenverkehr zu identifizieren, der mit Verkehrsdomänen verknüpft ist, zu bewerten.
2. Konfigurieren Sie einen Ratengrenzbezeichner, der Parameter wie den maximalen Schwellenwert für den Datenverkehr angibt, der die Rate begrenzt werden soll. In diesem Schritt ordnen Sie dem Ratenbegrenzer auch einen Stream-Selektor zu.
3. Konfigurieren Sie eine Aktion, die Sie der Richtlinie zuordnen möchten, die den Steuerbeschränkungsbezeichner verwendet.
4. Konfigurieren Sie eine Richtlinie, die das Ausdruckspräfix sys.check_limit verwendet, um den Grenzwertbezeichner aufzurufen, und ordnen Sie die Aktion dieser Richtlinie zu.
5. Binden Sie die Richtlinie global.

Betrachten Sie ein Beispiel, in dem zwei Verkehrsdomänen mit IDs 10 und 20 auf Citrix ADC NS1 konfiguriert sind. In der Verkehrsdomäne 10 ist LB1-TD-1 für den Lastenausgleich Server S1 und S2 konfiguriert; LB2-TD1 ist für den Lastausgleich Server S3 und S4 konfiguriert.

In der Verkehrsdomäne 20 ist LB1-TD-2 für den Lastausgleich der Server S5 und S6 konfiguriert; LB2-TD2 ist für den Lastausgleich der Server S7 und S8 konfiguriert.

In der folgenden Tabelle sind einige Beispiele für Richtlinien zur Begrenzung der Rate für Verkehrsdomänen im Beispiel-Setup aufgeführt.

Zweck	CLI-Befehle
Begrenzen Sie die Anzahl der Anforderungen auf 10 pro Sekunde für jede der Verkehrsdomänen.	add stream selector tdratelimit-1 CLIENT.TRAFFIC_DOMAIN.ID add ns limitIdentifier limitidf-1 -threshold 10 -selectorName tdratelimit-1 -trapsInTimeSlice 0 add responder policy ratelimit-pol “sys.check_limit(\“limitidf-1\”)” DROP bind responder global ratelimit-pol 1
Begrenzen Sie die Anzahl der Anforderungen auf 5 pro Client pro Sekunde für jede der Datenverkehrsdomänen.	add stream selector tdandclientip CLIENT.IP.SRC,CLIENT.TRAFFIC_DOMAIN.ID add ns limitIdentifier td_limitidf -threshold 5 -selectorName tdandclientip -trapsInTimeSlice 5 add responder policy tdratelimit-pol “sys.check_limit(\“td_limitidf\”)” DROP bind responder global tdratelimit-pol 2
Begrenzen Sie die Anzahl der Anforderungen, die für eine bestimmte Verkehrsdomäne (z. B. Verkehrsdomäne 10) gesendet wurden, auf 30 Anforderungen alle 3 Sekunden.	add stream selector tdratelimit CLIENT.TRAFFIC_DOMAIN.ID add ns limitIdentifier td10_limitidf -threshold 30 -timeSlice 3000 -selectorName tdratelimit -trapsInTimeSlice 5 add responder policy td10ratelimit “client.traffic_domain.id==10 && sys.check_limit(\“td10_limitidf\”)” DROP bind responder global td10ratelimit 3
Begrenzen Sie die Anzahl der Verbindungen auf 5 pro Client pro Sekunde für eine bestimmte Verkehrsdomäne (z. B. Verkehrsdomäne 20).	add stream selector tdandclientip CLIENT.IP.SRC CLIENT.TRAFFIC_DOMAIN.ID add ns limitIdentifier td20_limitidf -threshold 5 -mode CONNECTION -selectorName tdandclientip -trapsInTimeSlice 5 add responder policy td20_ratelimit “client.traffic_domain.id==20 && sys.check_limit(\“td20_limitidf\”)” DROP bind responder global td20_ratelimit 4

Konfigurieren der Ratengrenze auf Paketebene

October 5, 2021

Sie können einen Stream-Selektor und eine Responder-Richtlinie konfigurieren, um Statistiken auf Paketebene zu sammeln, die alle vom Selektor identifizierten Verbindungen durchlaufen. Wenn die Anzahl der Pakete pro Sekunde den konfigurierten Schwellenwert überschreitet, wendet die Richtlinie die konfigurierte Aktion an (RESET oder DROP). Sie können diese Richtlinien für alle Arten von virtuellen Servern konfigurieren. Pakete aller Größen werden berücksichtigt.

Führen Sie die folgenden Aufgaben aus, um die Begrenzung der Rate auf Paketebene zu konfigurieren

1. Lastenausgleich aktivieren
2. Streamauswahl hinzufügen
3. Datenstromkennung hinzufügen
4. Responder-Richtlinie hinzufügen
5. Hinzufügen eines virtuellen Lastausgleichsservers
6. Bind-Responder-Richtlinie

So aktivieren Sie die Lastausgleichs-Funktion

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns feature lb
<!--NeedCopy-->
```

So fügen Sie einen Stream-Selektor hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add stream selector packetlimitselector client.ip.src client.tcp.
   srcport client.ip.dst client.tcp.dstport
<!--NeedCopy-->
```


So fügen Sie einen Stream-Bezeichner hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add stream identifier packetlimitidentifier packetlimitselector -
     interval 1
2 <!--NeedCopy-->
```

So aktivieren Sie die Nachverfolgung nur von ACK-Paketen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set stream identifier packetlimitidentifier  - trackAckOnlyPackets
     ENABLED
2 <!--NeedCopy-->
```

So fügen Sie eine Responder-Richtlinie hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add responder policy packet_rate_sessionpolicy "ANALYTICS.STREAM("
     packetlimitidentifier").COLLECT_STATS("PACKET_LIMIT", <
     max_threshold_PPS>, ACTION, 0/1)" NOOP
2 <!--NeedCopy-->
```

Hierbei gilt:

- <max_threshold_PPS> ist die maximale Anzahl von Paketen, die über die Verbindung pro Sekunde zulässig sind.
- ACTION kann DROP oder RESET sein.
- 0 oder 1 steht für den Grenztyp; 0 steht für den Grenztyp BURSTY und 1 für den Grenztyp SMOOTH.

Beispiel:

```
1 add responder policy packet_rate_sessionpolicy "ANALYTICS.STREAM("
     packetlimitidentifier").COLLECT_STATS("PACKET_LIMIT", 40, RESET, 0)"
      NOOP
```



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

So fügen Sie einen virtuellen Lastausgleichsserver hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <serviceType> <ip> <port>

add lb vserver Vserver-lb-1 HTTP 10.102.20.200 80
<!--NeedCopy-->
```

So binden Sie eine Responder-Richtlinie

Nachdem der Selektor und die Responder-Richtlinie konfiguriert wurden, kann die Richtlinie global oder an den spezifischen virtuellen Server gebunden werden.

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
bind responder global <policyName> <priority> [<gotoPriorityExpression
   >] [-type <type>] [-invoke  (<labelType>  <labelName>) ]
<!--NeedCopy-->
```

ODER

```
bind lb vserver <name>@  (-policyName <string>@ [-priority <
   positive_integer>]
<!--NeedCopy-->
```

Beispiele:

```
bind responder global packet_rate_sessionpolicy 101 END -type
   REQ_DEFAULT

bind responder global packet_rate_sessionpolicy 102 END -type

bind lb vserver v1 -policyname packet_rate_sessionpolicy -priority 10
<!--NeedCopy-->
```


Responder

October 5, 2021

> **Warnung**
>
> Filterfunktionen mit klassischen Richtlinien sind veraltet, und als Alternative empfiehlt Citrix die Verwendung der Rewrite- und Responder-Features mit erweiterter Richtlinieninfrastruktur.

Die heutigen komplexen Webkonfigurationen erfordern oft unterschiedliche Antworten auf HTTP-Anfragen, die auf der Oberfläche erscheinen, um ähnlich zu sein. Wenn Benutzer eine Webseite anfordern, möchten Sie möglicherweise eine andere Seite bereitstellen, abhängig vom geografischen Standort des Benutzers, der Browserspezifikation oder den Sprachen, die der Browser akzeptiert, und der Reihenfolge der Präferenzen. Möglicherweise möchten Sie die Verbindung löschen, wenn die Anforderung aus einem IP-Bereich stammt, der DDoS-Angriffe erzeugt oder Hacking-Versuche initiiert hat.

Responder unterstützt Protokolle wie TCP, DNS (UDP) und HTTP. Wenn der Responder auf Ihrer Appliance aktiviert ist, können Serverantworten darauf basieren, wer die Anforderung sendet, wohin sie gesendet wird, und andere Kriterien mit Auswirkungen auf die Sicherheit und die Systemverwaltung. Die Funktion ist einfach und schnell zu bedienen. Durch das Vermeiden des Aufrufs komplexerer Funktionen reduziert es die CPU-Zyklen und den Zeitaufwand für die Verarbeitung von Anforderungen, die keine komplexe Verarbeitung erfordern.

Wenn Sie beim Umgang mit sensiblen Daten wie Finanzinformationen sicherstellen möchten, dass der Client eine sichere Verbindung verwendet, um eine Site zu durchsuchen, können Sie die Anforderung an eine sichere Verbindung umleiten, indem Sie `https://` anstelle von verwenden `http://`.

Gehen Sie wie folgt vor, um einen Responder zu verwenden:

- Aktivieren Sie eine Responderfunktion auf der Appliance.
- Konfigurieren Sie eine Responder-Aktion. Die Aktion kann darin bestehen, eine benutzerdefinierte Antwort zu generieren, eine Anforderung an eine andere Webseite umzuleiten oder eine Verbindung zurückzusetzen.
- Konfigurieren Sie eine Responderrichtlinie. Die Richtlinie bestimmt die Anforderungen (Datenverkehr), für die eine Aktion ausgeführt werden muss.
- Binden Sie jede Richtlinie an einen Bindepunkt, um sie in Kraft zu setzen. Ein Bindpunkt bezieht sich auf eine Entität, bei der die Citrix ADC Appliance den Datenverkehr überprüft, um festzustellen, ob er mit einer Richtlinie übereinstimmt. Ein Bindepunkt kann beispielsweise ein virtueller Lastausgleichsserver sein.

Sie können eine Standardaktion für Anforderungen angeben, die keiner Richtlinie entsprechen, und Sie können die Sicherheitsprüfung für Aktionen umgehen, die andernfalls Fehlermeldungen generieren würden.

Die Funktion Umschreiben von Citrix ADC hilft beim Umschreiben einiger Informationen in den Anforderungen oder Antworten, die von Citrix ADC verarbeitet werden. Der folgende Abschnitt zeigt einige Unterschiede zwischen den beiden Features.

Vergleich zwischen Rewrite und Responder Optionen

Der Hauptunterschied zwischen dem Rewrite-Feature und dem Responder-Feature ist wie folgt:

Responder kann nicht für Antwort- oder serverbasierte Ausdrücke verwendet werden. Responder kann nur für die folgenden Szenarien verwendet werden, abhängig von Client-Parametern:

- Umleiten einer HTTP-Anfrage auf neue Websites oder Webseiten
- Reagieren mit einer benutzerdefinierten Antwort
- Löschen oder Zurücksetzen einer Verbindung auf Anforderungsebene

Wenn eine Responderrichtlinie vorhanden ist, prüft Citrix ADC die Anforderung vom Client, führt Maßnahmen gemäß den entsprechenden Richtlinien aus, sendet die Antwort an den Client und schließt die Verbindung mit dem Client.

Wenn eine Richtlinie zum Neuschreiben vorliegt, prüft Citrix ADC die Anforderung des Clients oder der Antwort vom Server, führt Maßnahmen gemäß den entsprechenden Richtlinien aus und leitet den Datenverkehr an den Client oder den Server weiter.

Im Allgemeinen wird empfohlen, einen Responder zu verwenden, wenn Sie möchten, dass die Appliance eine Verbindung basierend auf einem anforderungsbasierten Parameter zurücksetzt oder ablegt. Verwenden Sie einen Responder, um den Datenverkehr umzuleiten oder mit benutzerdefinierten Nachrichten zu antworten. Verwenden Sie Rewrite zum Bearbeiten von Daten auf HTTP-Anforderungen und -Antworten.

Aktivieren der Responder-Funktion

October 5, 2021

Um die Responder-Funktion verwenden zu können, müssen Sie sie zuerst aktivieren.

So aktivieren Sie das Responder-Feature mit der Citrix ADC Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um das Responder-Feature zu aktivieren und die Konfiguration zu überprüfen:

- `enable ns feature <feature>`
- `show ns feature`

Beispiel:

```
enable ns feature Responder
 Done
> show ns feature

        Feature                         Acronym              Status
        -------                         -------              ------
 1)     Web Logging                     WL                   ON
 2)     Surge Protection                SP                   ON
 .
 .
 .
 1)     Responder                       RESPONDER            ON
 2)     HTML Injection                  HTMLInjection        ON
 3)     Citrix ADC Push                  push                 OFF
 Done
>
<!--NeedCopy-->
```

So aktivieren Sie die Responder-Funktion mit der GUI:

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie im Detailbereich unter **Modi** und **Features** auf **Erweiterte Features ändern** .
3. Aktivieren **Sie im Dialogfeld Erweiterte Funktionen konfigurieren** das Kontrollkästchen **Responder**, und klicken Sie dann auf **OK** .
4. In der **aktivieren/deaktivieren Funktion(en)?** auf **JA**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das Feature aktiviert wurde.

Aktion Responder konfigurieren

October 5, 2021

Nachdem Sie die Responder-Funktion aktiviert haben, müssen Sie eine oder mehrere Aktionen für die Verarbeitung von Anforderungen konfigurieren. Der Responder unterstützt die folgenden Arten von Aktionen:

- **Antworte mit**. Sendet die vom Zielausdruck definierte Antwort, ohne die Anforderung an einen Webserver weiterzuleiten. (Die Citrix ADC Appliance ersetzt und fungiert als Webserver.) Verwenden Sie diese Art von Aktion, um eine einfache HTML-basierte Antwort manuell zu

definieren. Normalerweise besteht der Text für eine Antwort mit Aktion aus einem Webserver Fehlercode und einer kurzen HTML-Seite.

- **Antworten Sie mit SQL OK**. Sendet die angegebene SQL-OK-Antwort, die durch den Zielausdruck definiert wird. Verwenden Sie diese Art von Aktion, um eine SQL-OK-Antwort an eine SQL-Abfrage zu senden.
- **Beantworten Sie mit SQL-Fehler**. Sendet die angegebene SQL-Fehlerantwort, die durch den Zielausdruck definiert wird. Verwenden Sie diese Art von Aktion, um eine SQL-Fehlerantwort an eine SQL-Abfrage zu senden.
- **Antwort mit HTML-Seite**. Sendet die angegebene HTML-Seite als Antwort. Sie können aus einer Dropdownliste der zuvor hochgeladenen HTML-Seiten auswählen oder eine neue HTML-Seite hochladen. Verwenden Sie diese Art von Aktion, um eine importierte HTML-Seite als Antwort zu senden. Die Appliance antwortet mit einem benutzerdefinierten Header in der Aktion responsewithhtmlpage Responder. Sie können bis zu acht benutzerdefinierte Header konfigurieren.
- **Umleiten**. Leitet die Anforderung an eine andere Webseite oder einen anderen Webserver um. Eine Umleitungsaktion kann Anfragen, die ursprünglich an eine "Dummy-Website" gesendet wurden, die in DNS vorhanden ist, aber für die kein tatsächlicher Webserver vorhanden ist, an eine tatsächliche Website umleiten. Es kann auch Suchanfragen an eine entsprechende URL umleiten. Normalerweise besteht das Umleitungsziel für eine Umleitungsaktion aus einer vollständigen URL.

So konfigurieren Sie eine Responderaktion mit der Citrix ADC Befehlszeile:

Zeigt die aktuellen Einstellungen für die angegebene Responder-Aktion an. Wenn kein Aktionsname angegeben wird, zeigen Sie eine Liste aller Responderaktionen an, die derzeit auf der Citrix ADC Appliance konfiguriert sind, mit abgekürzten Einstellungen an.

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

- `add responder action <name> <type> <target> [-bypassSafetyCheck (YES | NO)]`
- `show responder action`

Die Parameter:

- **Name**. Name der Responderaktion. Maximale Länge: 127
- **type**. Art der Responderaktion. Es kann sein: (respondwith).
- **target**. Ein Ausdruck, der angibt, mit was reagiert werden soll
- **htmlpage**. Option, die angeben, um mit HTMLpage zu antworten

- **bypassSafetyCheck**. Die Sicherheitsprüfung, um unsichere Ausdrücke zu ermöglichen. **Hinweis:** Dieses Attribut ist veraltet.
- **hits**. Gibt an, wie oft die Aktion ergriffen wurde.
- **referenceCount**. Die Anzahl der Verweise auf die Aktion.
- **undefHits**. Gibt an, wie oft die Aktion zu UNDEF geführt hat.
- **comment**. Jede Art von Informationen zu dieser Responder-Aktion.
- **builtin**. Flag, um zu bestimmen, ob die Responderaktion integriert ist oder nicht

Beispiel:

```
To create a responder action that displays a “Not Found” error page for URLs that do not exist:

> add responder action act404Error respondWith '”HTTP/1.1 404 Not Found\r\n\r\n”+ HTTP.REQ.URL.HTTP_URL_SAFE + ” does not exist on the web server.”'
Done

> show responder action

1) Name: act404Error
Operation: respondwith
Target: ”HTTP/1.1 404 Not Found” + HTTP.REQ.URL.HTTP_URL_SAFE + ” does not exist on the web server.”
BypassSafetyCheck : NO
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

To create a responder action that displays a “Not Found” error page for URLs that do not exist:

add responder action act404Error respondWith '”HTTP/1.1 404 Not Found\r\n\r\n”+ HTTP.REQ.URL.HTTP_URL_SAFE + ” does not exist on the web server.”'
Done
> show responder action

1) Name: act404Error
Operation: respondwith
```



```
25 Target: ”HTTP/1.1 404 Not Found” + HTTP.REQ.URL.HTTP_URL_SAFE + ” does
      not exist on the web server.”
26 BypassSafetyCheck : NO
27 Hits: 0
28 Undef Hits: 0
29 Action Reference Count: 0
30 Done
31 <!--NeedCopy-->
```

So ändern Sie eine vorhandene Responderaktion mit der Citrix ADC Befehlszeile:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine vorhandene Responderaktion zu ändern und die Konfiguration zu überprüfen:

- `set responder action <name> -target <string> [-bypassSafetyCheck ( YES | NO )]`
- `show responder action`

Beispiel:

```
1 set responder action act404Error  -target '”HTTP/1.1 404 Not Found\r\n\
     r\n”+ HTTP.REQ.URL.HTTP_URL_SAFE + ” does not exist on the web
     server.”'
2  Done
3 > show responder action
4
5 1)      Name: act404Error
6         Operation: respondwith
7         Target: ”HTTP/1.1 404 Not Found” + HTTP.REQ.URL.HTTP_URL_SAFE +
              ” does not exist on the web server.”
8         BypassSafetyCheck : NO
9         Hits: 0
10        Undef Hits: 0
11        Action Reference Count: 0
12  Done
13 <!--NeedCopy-->
```

So entfernen Sie eine Responderaktion mit der Citrix ADC Befehlszeile:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine Responderaktion zu entfernen und die Konfiguration zu überprüfen:

- `rm responder action <name>`
- `show responder action`

Beispiel:

```
rm responder action act404Error
 Done

> show responder action
 Done
<!--NeedCopy-->
```

So fügen Sie benutzerdefinierte Header in responsewithhtmlpage Responderaktion mit der Citrix ADC Befehlszeile hinzu:

Eine Citrix ADC Appliance kann nun mit benutzerdefinierten Headern in der Aktion responsewithhtmlpage antworten. Sie können bis zu acht benutzerdefinierte Header konfigurieren. Zuvor reagierte die Appliance nur mit `Content-type:text/html` und `Content-Length:<value>` statischen Headern.

> **Hinweis:**
>
> In der benutzerdefinierten Header-Konfiguration können Sie auch den Header-Wert "Content-Type" überschreiben.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
add responder action <name> <type> (<target> | <htmlpage>)[-comment <string
>] [-responseStatusCode <positive_integer>] [-reasonPhrase <expression>] [-
headers <name(value)> ...]
```

Hierbei gilt:

ein. Name für die Responderaktion. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und nur Buchstaben, Zahlen und Bindestrich (-), Punkt (.) Hash (#), Leerzeichen (), at (@), equals (=), Doppelpunkt (:) und Unterstrich enthalten. Kann geändert werden, nachdem die Responder-Richtlinie hinzugefügt wurde.

Geben Sie ein. Art der Responderaktion. Verfügbare Einstellungen funktionieren wie folgt:

1. respondwith<target> - Reagieren Sie auf die Anforderung mit dem Ausdruck, der als Ziel angegeben ist.
2. respondwithhtmlpage - Reagieren Sie auf die Anfrage mit dem hochgeladenen HTML-Seitenobjekt, das als Ziel angegeben ist.
3. redirect - Leiten Sie die Anforderung an die URL um, die als Ziel angegeben ist.
4. sqlresponse_ok - Senden Sie eine SQL OK Antwort.
5. sqlresponse_error - Senden Sie eine SQL-ERROR Antwort. Dies ist ein obligatorisches Argument. Mögliche Werte: noop, respondwith, redirect, respondwithhtmlpage, sqlresponse_ok, sqlresponse_error

Ziel. Ausdruck, der angibt, worauf reagiert werden soll. In der Regel eine URL für Umleitungsrichtlinien oder einen Standardsyntaxausdruck. Zusätzlich zu Citrix ADC Default-Syntaxausdrücken, die sich auf Informationen in der Anfrage beziehen, kann ein StringBuilder-Ausdruck Text und HTML sowie einfache Escape-Codes enthalten, die neue Zeilen und Absätze definieren. Schließen Sie jedes stringbuilder-Ausdruckselement (entweder einen Citrix ADC-Standardsyntaxausdruck oder eine Zeichenfolge) in doppelte Anführungszeichen ein. Verwenden Sie das Pluszeichen (+), um die Elemente zu verbinden.

htmlpage. Für respondwithhtmlpage Richtlinien Name des HTML-Seitenobjekts, das als Antwort verwendet werden soll. Sie müssen zuerst das Seitenobjekt importieren. Maximale Länge: 31

Kommentieren. Jede Art von Informationen zu dieser Responder-Aktion. Maximale Länge: 255

responseStatusCode. HTTP-Antwortstatuscode, z. B. 200, 302, 404 usw. Der Standardwert für den Umleitungsaktionstyp ist 302 und für respondwithhtmlpage ist 200 Minimalwert: 100 Maximalwert: 599

reasonPhrase. Ausdruck, der den Ursachensatz der HTTP-Antwort angibt. Der Grund Phrase kann ein String-Literal mit Anführungszeichen oder einem PI-Ausdruck sein. Beispiel: “Ungültige URL:” + HTTP.REQ.URL Maximale Länge: 8191

Headers. Ein oder mehrere Header, die in die HTTP-Antwort eingefügt werden sollen. Jeder Header wird als “name (expr)” angegeben, wobei expr ein Ausdruck ist, der zur Laufzeit ausgewertet wird, um den Wert für den benannten Header bereitzustellen. Sie können maximal acht Header für eine Responder-Aktion konfigurieren.

So konfigurieren Sie eine Responderaktion mit der GUI:

1. Navigieren Sie zu **AppExpert > Responder > Aktionen**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine Aktion zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Aktion zu ändern, wählen Sie die Aktion aus, und klicken Sie dann auf **Öffnen**.
3. Klicken Sie auf **Erstellen** oder **OK**, je nachdem, ob Sie eine Aktion erstellen oder eine vorhandene Aktion ändern möchten.
4. Klicken Sie auf **Schließen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das Feature aktiviert wurde.
5. Um eine Responder-Aktion zu löschen, wählen Sie die Aktion aus, und klicken Sie dann auf **Entfernen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das Feature deaktiviert wurde.

So fügen Sie einen Ausdruck mithilfe des Dialogfelds **Ausdruck hinzufügen hinzu**

1. Klicken Sie im Dialogfeld **Responderaktion erstellen** oder **Responderaktion konfigurieren** auf **Hinzufügen**.

2. Wählen **Sie im Dialogfeld Ausdruck hinzufügen** im ersten Listenfeld den ersten Begriff für Ihren Ausdruck aus.

    - HTTP Das HTTP-Protokoll. Wählen Sie diese Option, wenn Sie einen Aspekt der Anforderung untersuchen möchten, die sich auf das HTTP-Protokoll bezieht.
    - SYS. Eine oder mehrere geschützte Websites. Wählen Sie diese Option, wenn Sie einen Aspekt der Anforderung untersuchen möchten, der sich auf den Empfänger der Anforderung bezieht.
    - CLIENT. Der Computer, der die Anforderung gesendet hat. Wählen Sie diese Option, wenn Sie einen Aspekt des Absenders der Anfrage untersuchen möchten.
    - ANALYTICS. Die Analytics-Daten, die mit der Anforderung verknüpft sind. Wählen Sie diese Option, wenn Sie Anforderungsmetadaten untersuchen möchten.
    - SIP. Eine SIP-Anfrage. Wählen Sie diese Option, wenn Sie einen Aspekt einer SIP-Anfrage untersuchen möchten. Wenn Sie Ihre Wahl treffen, werden im Listenfeld ganz rechts die entsprechenden Begriffe für den nächsten Teil des Ausdrucks aufgeführt.

3. Wählen Sie im zweiten Listenfeld den zweiten Begriff für Ihren Ausdruck aus. Die Auswahlmöglichkeiten hängen davon ab, welche Auswahl Sie im vorherigen Schritt getroffen haben, und sind dem Kontext angemessen. Nachdem Sie Ihre zweite Wahl getroffen haben, zeigt das Hilfefenster unterhalb des Fensters Ausdruck erstellen (das leer war) Hilfe an, in dem der Zweck und die Verwendung des gerade ausgewählten Begriffs beschrieben wird.

4. Fahren Sie fort, Begriffe aus den Listenfeldern auszuwählen, die rechts neben dem vorherigen Listenfeld angezeigt werden, oder geben Sie Zeichenfolgen oder Zahlen in die Textfelder ein, die Sie zur Eingabe eines Werts auffordern, bis der Ausdruck beendet ist.

Konfigurieren der globalen HTTP-Aktion

Sie können die globale HTTP-Aktion so konfigurieren, dass eine Responder-Aktion aufgerufen wird, wenn eine HTTP-Anforderung Timeout auskommt. Um diese Funktion zu konfigurieren, müssen Sie zuerst die Responder-Aktion erstellen, die Sie aufrufen möchten. Anschließend konfigurieren Sie die globale HTTP-Zeitüberschreitungsaktion, um mit dieser Responderaktion auf ein Timeout zu reagieren.

So konfigurieren Sie die globale HTTP-Aktion mit der Citrix ADC Befehlszeile:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

- `set ns httpProfile -reqTimeoutAction <responder action name>`
- `save ns config`

Ersetzen Sie für `<responder action name>` den Namen der Responderaktion.

Importieren von HTML-Seiten konfigurieren

Wenn eine Citrix ADC Appliance mit einer benutzerdefinierten Nachricht antwortet, können wir mit einer HTML-Datei antworten. Sie können die Datei mit dem `import responder htmlpage` Befehl importieren und diese Datei dann im `add responder action <act name> respondwithhtmlpage <file name>` Befehl verwenden. Sie können die Datei auch über die Citrix ADC GUI importieren. Sie können eine gewünschte HTML-Seite in den Appliance-Ordner importieren und die Seite während der Laufzeit des Responders hochladen.

HTML-Seite über die Befehlszeile importieren

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import responder htmlpage [<src>] <name> [-comment <string>] [-overwrite][-
CAcertFile <string>]
```

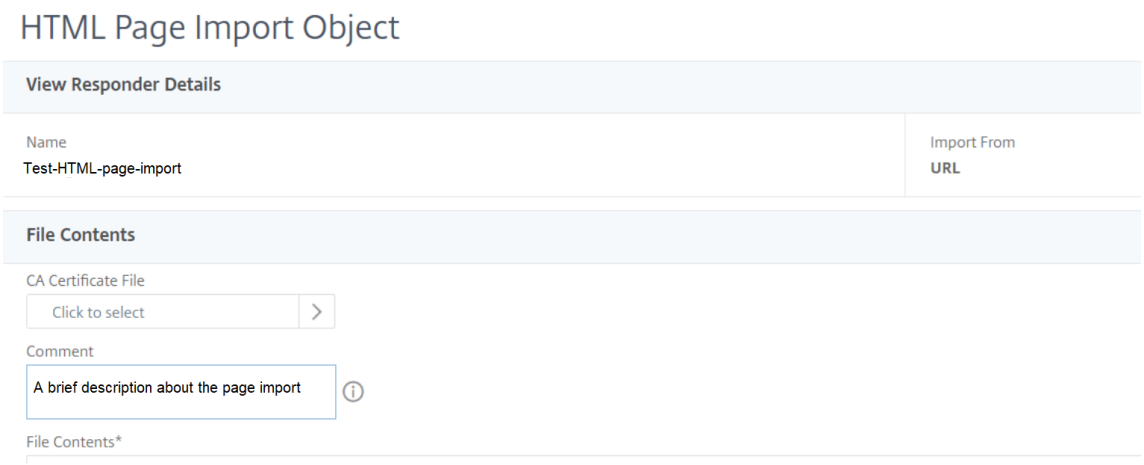
Beispiel:

```
import responder htmlpage http://www.example.com/page.html my-responder-
page -CAcertFile my_root_ca_cert
```

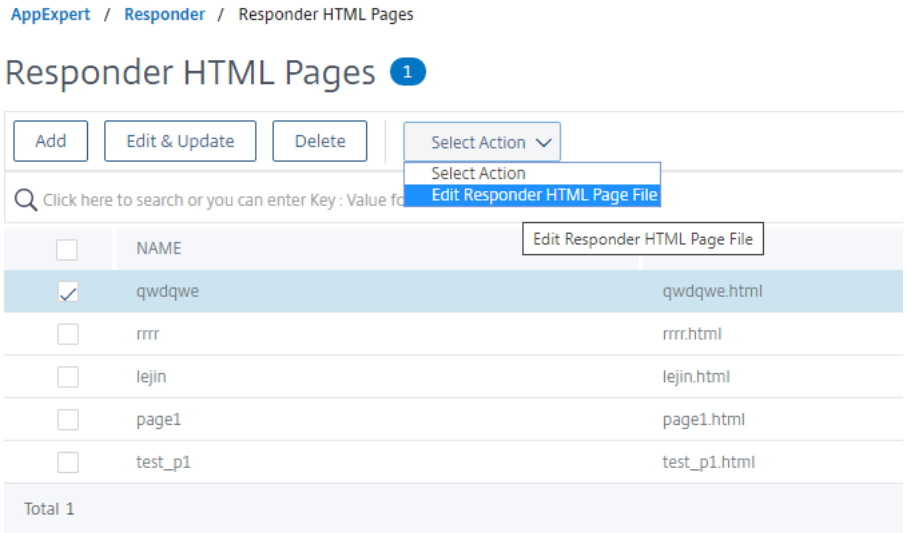
Hierbei wird das
Zertifizierungsstellenzertifikat für die Überprüfung des Clientzertifikats verwendet. Das Zertifikat sollte mit dem CLI-Befehl “import ssl certfile” oder einem entsprechenden Befehl über API oder GUI importiert werden. Wenn der Zertifikatname nicht konfiguriert ist, werden Standard-Stammzertifizierungsstellenzertifikate für die Zertifikatüberprüfung verwendet.

HTML-Seite über die Citrix ADC GUI importieren

1. Navigieren Sie zu **AppExpert** > **Responder** > **HTML-Seitenimporte**.
2. Klicken Sie im Detailbereich des **Responder-HTML-Imports** auf **Hinzufügen**.
3. Legen Sie auf der **Seite HTML-Seite Importobjekt** die folgenden Parameter fest:
    a) Name. Name der HTML-Seite.
    b) Importieren von. Importiert aus Datei, Text oder Text.
    c) -URL. Wählen Sie diese Option, um den URL-Speicherort der HTML-Datei einzugeben.
    d) Akte. Wählen Sie die HTML-Datei aus dem Appliance-Verzeichnis aus.
    e) Text. Wählen Sie die HTML-Datei als Text aus.
4. Klicken Sie auf **Weiter**.
5. Überprüfen Sie die Details der HTML-Seite des Responders.
6. Klicken Sie auf **Fertig**.



Um eine HTML-Seite zu bearbeiten, können Sie eine Datei auswählen und in der Dropdownliste **Aktion auswählen** auf **Responder-HTML-Seitendatei bearbeiten** klicken.



Konfigurieren einer Responder-Richtlinie

October 5, 2021

Nachdem Sie eine Responder-Aktion konfiguriert haben, müssen Sie als nächstes eine Responder-Richtlinie konfigurieren, um die Anforderungen auszuwählen, auf die die Citrix ADC Appliance antworten soll. Eine Responderrichtlinie basiert auf einer Regel, die aus einem oder mehreren Ausdrücken besteht. Die Regel ist einer Aktion zugeordnet, die ausgeführt wird, wenn eine Anforderung mit der Regel übereinstimmt.

Hinweis: Zum Erstellen und Verwalten von Responderrichtlinien bietet die grafische Benutzeroberfläche Unterstützung, die an der Citrix ADC Eingabeaufforderung nicht verfügbar ist.

So konfigurieren Sie eine Responder-Richtlinie mit der Citrix ADC Befehlszeile:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add responder policy <name> <expression> <action> [<undefaction>]-appFlowaction <actionName>`
- `show responder policy <name>`

Beispiel:

```
> add responder policy policyThree ”CLIENT.IP.SRC.IN_SUBNET
   (222.222.0.0/16)” RESET
 Done
> show responder policy policyThree

        Name: policyThree
        Rule: CLIENT.IP.SRC.IN_SUBNET(222.222.0.0/16)
        Responder Action: RESET
        UndefAction: Use Global
        Hits: 0
        Undef Hits: 0
 Done
<!--NeedCopy-->
```

So ändern Sie eine vorhandene Responder-Richtlinie mit der Citrix ADC Befehlszeile:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `set responder policy <name> [-rule <expression>] [-action <string>] [-undefAction <string>]`
- `show responder policy <name>`

So entfernen Sie eine Responderrichtlinie mit der Citrix ADC Befehlszeile:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `rm responder policy <name>`
- `show responder policy`

Beispiel:

```
>rm responder policy pol404Error
 Done

> show responder policy
```



```
5   Done
6 <!--NeedCopy-->
```

So konfigurieren Sie eine Responder-Richtlinie mit der GUI:

1. Navigieren Sie zu **AppExpert > Responder > Richtlinien**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine neue Richtlinie zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Öffnen**.
3. Klicken Sie auf **Erstellen** oder **OK**, je nachdem, ob Sie eine neue Richtlinie erstellen oder eine vorhandene Richtlinie ändern.
4. Klicken Sie auf **Schließen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das Feature konfiguriert wurde.

Binden einer Responder-Richtlinie

February 24, 2022

Um eine Richtlinie in Kraft zu setzen, müssen Sie sie entweder global binden, sodass sie für den gesamten Datenverkehr gilt, der durch den Citrix ADC fließt, oder für einen bestimmten virtuellen Server, sodass die Richtlinie nur für Anforderungen gilt, deren Ziel-IP-Adresse der VIP dieses virtuellen Servers ist.

Wenn Sie eine Richtlinie binden, weisen Sie ihr eine Priorität zu. Die Priorität bestimmt die Reihenfolge, in der die von Ihnen definierten Richtlinien ausgewertet werden. Sie können die Priorität auf jede positive Ganzzahl festlegen.

Im Citrix ADC-Betriebssystem arbeiten Richtlinienprioritäten in umgekehrter Reihenfolge - je höher die Zahl, desto niedriger die Priorität. Wenn Sie beispielsweise drei Richtlinien mit Prioritäten von 10, 100 und 1000 haben, wird der Richtlinie zuerst eine Priorität von 10 zugewiesen, dann wird der Richtlinie eine Priorität von 100 zugewiesen, und schließlich hat die Richtlinie eine Reihenfolge von 1000 zugewiesen. Die Responderfunktion implementiert nur die erste Richtlinie, mit der eine Anforderung übereinstimmt, und keine zusätzlichen Richtlinien, mit denen sie möglicherweise auch übereinstimmt. Daher ist die Richtlinienpriorität wichtig, um die von Ihnen beabsichtigten Ergebnisse zu erzielen.

Sie können sich ausreichend Raum lassen, um weitere Richtlinien in beliebiger Reihenfolge hinzuzufügen, und sie dennoch so festlegen, dass sie in der von Ihnen gewünschten Reihenfolge ausgewertet werden, indem Sie Prioritäten mit Intervallen von 50 oder 100 zwischen den einzelnen Richtlinien festlegen, wenn Sie sie global binden. Sie können dann jederzeit zusätzliche Richtlinien hinzufügen, ohne die Priorität einer vorhandenen Richtlinie neu zuweisen zu müssen.

Weitere Informationen zum Binden von Richtlinien im Citrix ADC finden Sie unter Richtlinien und Ausdrücke.

> **Hinweis:**
>
> Responder-Richtlinien sind an TCP-basierte virtuelle Server gebunden.

So binden Sie eine Responder Policy global mithilfe der Citrix ADC-Befehlszeile:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine Responder Policy global zu binden und die Konfiguration zu überprüfen:

- `bind responder global <policyName> <priority> [<gotoPriorityExpression> [-type <type>] [-invoke (<labelType> <labelName>)]`
- `show responder global`

Beispiel:

```
> bind responder global poliError 100
 Done
> show responder global
1)      Global bindpoint: REQ_DEFAULT
        Number of bound policies: 1

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

So binden Sie die Responder Policy mithilfe der Citrix ADC-Befehlszeile an einen bestimmten virtuellen Server:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `bind lb vserver <name> -policyname <policy_name> -priority <priority>`
- `show lb vserver vs-loadbal <name>`

Beispiel:

```
> bind lb vserver vs-loadbal -policyName policyTwo -priority 100
 Done
> show lb vserver
1)      vs-loadbal (10.102.29.20:80) - HTTP     Type: ADDRESS
        State: OUT OF SERVICE
        Last state change was at Wed Aug 19 09:05:47 2009 (+211 ms)
        Time since last state change: 2 days, 00:58:03.260
        Effective State: DOWN
```



```
9           Client Idle Timeout: 180 sec
10          Down state flush: ENABLED
11          Disable Primary Vserver On Down : DISABLED
12          Port Rewrite : DISABLED
13          No. of Bound Services :  0 (Total)       0 (Active)
14          Configured Method: LEASTCONNECTION
15          Mode: IP
16          Persistence: NONE
17          Vserver IP and Port insertion: OFF
18          Push: DISABLED  Push VServer:
19          Push Multi Clients: NO
20          Push Label Rule: none
21  2)      vs-cont-sw (0.0.0.0:0) - TCP    Type: ADDRESS
22          State: DOWN
23          Last state change was at Wed Aug 19 10:03:46 2009 (+213 ms)
24          Time since last state change: 2 days, 00:00:04.260
25          Effective State: DOWN
26          Client Idle Timeout: 9000 sec
27          Down state flush: ENABLED
28          Disable Primary Vserver On Down : DISABLED
29          No. of Bound Services :  0 (Total)       0 (Active)
30          Configured Method: LEASTCONNECTION
31          Mode: IP
32          Persistence: NONE
33          Connection Failover: DISABLED
34   Done
35  <!--NeedCopy-->
```

So binden Sie eine Responder Policy global mithilfe der GUI:

1. Navigieren Sie zu **AppExpert** > **Responder** > **Richtlinien**.
2. Wählen Sie auf der Seite **Responderrichtlinien** eine Responder Policy aus, und klicken Sie dann auf **Richtlinien-Manager**.
3. Wählen Sie im Dialogfeld “ **Responder-Richtlinien-Manager** “ “Punkte binden” die Option “Global”
4. Klicken Sie auf **Richtlinie einfügen**, um eine neue Zeile einzufügen und eine Dropdown-Liste aller Richtlinien für ungebundene Responders anzuzeigen.
5. Klicken Sie auf eine der Richtlinien in der Liste. Diese Richtlinie wird in die Liste der global gebundenen Responder-Richtlinien aufgenommen.
6. Klicken Sie auf **Änderungen übernehmen**.
7. Klicken Sie auf **Schließen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Konfiguration erfolgreich abgeschlossen wurde.

So binden Sie eine Responder Policy mithilfe der GUI an einen bestimmten virtuellen Server:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Wählen Sie auf der Seite **Load Balancing Virtual** Servers den virtuellen Server aus, an den Sie die Responder Policy binden möchten, und klicken Sie dann auf **Öffnen**.
3. Wählen **Sie im Dialogfeld Virtuellen Server (Load Balancing) konfigurieren** die Registerkarte **Richtlinien**, auf der eine Liste aller auf Ihrer Citrix ADC Appliance konfigurierten Richtlinien angezeigt wird.
4. Aktivieren Sie das Kontrollkästchen neben dem Namen der Richtlinie, die Sie an diesen virtuellen Server binden möchten.
5. Klicken Sie auf **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Konfiguration erfolgreich abgeschlossen wurde.

Festlegen der Standardaktion für eine Responder-Richtlinie

October 5, 2021

Die Citrix ADC Appliance generiert ein nicht definiertes Ereignis (UNDEF-Ereignis), wenn eine Anforderung nicht mit einer Responderrichtlinie übereinstimmt. Die Appliance führt dann die Standardaktion aus, die nicht definierten Ereignissen zugewiesen ist. Standardmäßig leitet die Aktion die Anforderung an die nächste Funktion wie Lastenausgleich, Inhaltsfilterung usw. weiter. Dieses Standardverhalten stellt sicher, dass für die Anforderungen keine spezifische Responderaktion an Ihre Webserver gesendet werden muss. Außerdem erhalten die Clients Zugriff auf die angeforderten Inhalte.

Wenn eine oder mehrere Websites, die von der Citrix ADC Appliance geschützt werden, eine beträchtliche Anzahl ungültiger oder bösartiger Anfragen erhalten, können Sie die Standardaktion ändern, um entweder die Clientverbindung zurückzusetzen oder die Anforderung zu löschen. Bei dieser Konfiguration schreiben Sie eine oder mehrere Antwortrichtlinien, die allen legitimen Anforderungen entsprechen, und leiten diese Anforderungen einfach an ihre ursprünglichen Ziele um. Ihre Citrix ADC Appliance sperrt dann alle anderen Anforderungen, wie in der von Ihnen konfigurierten Standardaktion angegeben.

Sie können einem nicht definierten Ereignis eine der folgenden Aktionen zuweisen:

- **NOOP**. Die NOOP-Aktion bricht die Responderverarbeitung ab, ändert aber nicht den Paketfluss. Damit die Appliance weiterhin Anforderungen verarbeitet, die keiner Responderrichtlinie entsprechen, und sie schließlich an die angeforderte URL weiterleitet, es sei denn, ein anderes Feature greift ein und blockiert oder leitet die Anforderung um. Diese Aktion ist für normale Anforderungen an Ihre Webserver geeignet und ist die Standardeinstellung.
- **RESET**. Wenn die nicht definierte Aktion auf RESET festgelegt ist, setzt die Appliance die Clientverbindung zurück und informiert den Client, dass die Sitzung mit dem Webserver

wieder hergestellt werden muss. Die Aktion eignet sich für wiederholte Anfragen für Webseiten, die nicht vorhanden sind, oder für Verbindungen, die versuchen könnten, Ihre geschützten Websites zu hacken oder zu testen.

- **DROP**. Wenn die undefinierte Aktion auf DROP festgelegt ist, löscht die Appliance die Anforderung im Hintergrund, ohne auf den Client zu antworten. Diese Aktion eignet sich für Anfragen, die anscheinend Teil eines DDoS-Angriffs oder eines anderen anhaltenden Angriffs auf Ihre Server zu sein scheinen.

Hinweis: UNDEF-Ereignisse werden nur für Clientanforderungen ausgelöst. Für Antworten werden keine UNDEF-Ereignisse ausgelöst.

So legen Sie die nicht definierte Aktion mit der Citrix ADC Befehlszeile fest:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die nicht definierte Aktion festzulegen und die Konfiguration zu überprüfen:

- `set responder param -undefAction (RESET|DROP|NOOP)[-timeout <msecs>]`
- `show responder param`

Hierbei gilt:

timeout - Maximale Zeit in Millisekunden, um die Verarbeitung aller Richtlinien und ihrer ausgewählten Aktionen ohne Unterbrechung zu ermöglichen. Wenn das Timeout erreicht ist, führt die Auswertung dazu, dass ein UNDEF ausgelöst wird und keine weitere Verarbeitung durchgeführt wird.

Mindestwert: 1

Maximalwert: 5000

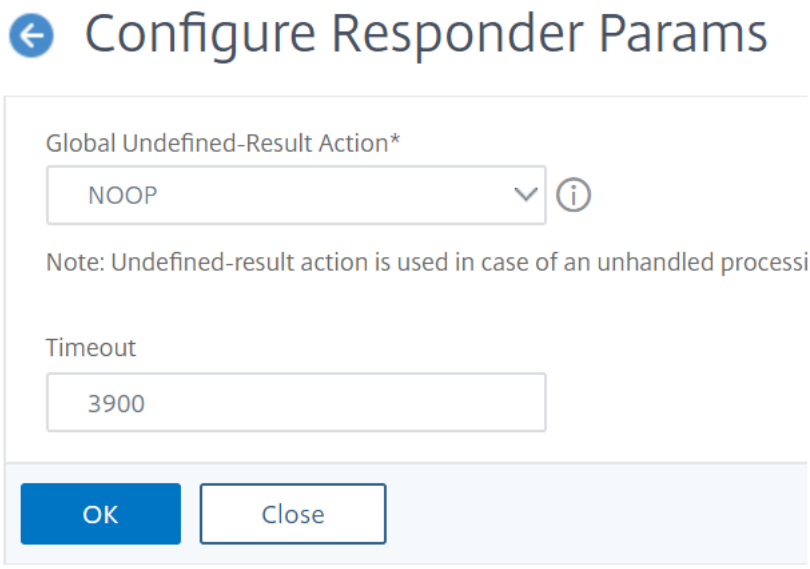
Beispiel:

```
>set responder param -undefAction RESET -timeout 3900
 Done
> show responder param
Action Name: RESET
Timeout: 3900
 Done
>
<!--NeedCopy-->
```

Legen Sie die undefinierte Aktion mit der GUI fest

1. Navigieren Sie zu **AppExpert** > **Responder**, und klicken Sie dann unter **Einstellungen** auf den Link **Respondereinstellungen ändern** .

2. **Legen Sie auf der Seite Responderparameter** festlegen die folgenden Parameter fest:
   a) Globale Aktion für nicht definiertes Ergebnis. Nicht definiertes Ergebnis wird bei einer nicht behandelten Verarbeitungsausnahme in den Responder-Richtlinien und -Aktionen bevorzugt. Wählen Sie **NOOP**, **RESET**oder **DROP**.
   b) Timeout. Maximale Zeit in Millisekunden, um die Verarbeitung aller Richtlinien und ihrer ausgewählten Aktionen ohne Unterbrechung zu ermöglichen. Wenn das Timeout erreicht ist, führt die Auswertung dazu, dass ein UNDEF ausgelöst wird und keine weitere Verarbeitung durchgeführt wird.
3. Klicken Sie auf **OK**.



Beispiele für Responder Action und Policy

January 25, 2022

Aktionen und Richtlinien der Responder sind leistungsstark und komplex, aber Sie können mit relativ einfachen Anwendungen beginnen.

Beispiel: Blockieren des Zugriffs von bestimmten IPs

Die folgenden Verfahren blockieren den Zugriff auf Ihre geschützte Website (n) durch Clients, die vom CIDR 222.222.0.0/16 stammen. Der Responder sendet eine Fehlermeldung, dass der Client nicht berechtigt ist, auf die angeforderte URL zuzugreifen.

So blockieren Sie den Zugriff mithilfe der Citrix ADC-Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den Zugriff zu blockieren:

- Responder Action hinzufügen act_unauthorized response mit “HTTP/1.1 403 Forbidden\ r\ n\ r\ n” + “Client:” + CLIENT.IP.SRC + “ist nicht berechtigt, auf URL zuzugreifen:” + “HTTP.REQ.URL.HTTP_URL_SAFE”’
- Responder Policy hinzugefügt pol_un “CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)” act_unauthorized
- binden Responder global pol_un 10

So blockieren Sie den Zugriff mit der GUI:

1. Erweitern Sie im Navigationsbereich **Responder**, und klicken Sie dann auf **Aktionen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Gehen **Sie im Dialogfeld Responderaktion erstellen** wie folgt vor:
   a) Geben Sie in das Textfeld **Name** act_unauthorized ein.
   b) Wählen Sie unter Typ die Option Antworten mit aus.
   c) Geben Sie im Bereich Zieltext die folgende Zeichenfolge ein: “HTTP/1.1 403 Forbidden\ r\ n\ r\ n” + “Client:” + CLIENT.IP.SRC + “ist nicht berechtigt, auf die URL zuzugreifen:” + HTTP.REQ.URL.HTTP_URL_SAFE
   d) Klicken Sie auf **Erstellen**, und klicken Sie dann auf **Schließen**.
   Die von Ihnen konfigurierte Responder Action mit dem Namen act_unauthorized wird jetzt auf der Seite **Responderaktionen** angezeigt.
4. Klicken Sie im Navigationsbereich auf **Richtlinien**.
5. Klicken Sie im Detailbereich auf **Hinzufügen**.
6. Gehen **Sie im Dialogfeld Responder-Richtlinie erstellen** wie folgt vor:
   a) Geben Sie in das Textfeld Name pol_unauthorized ein.
   b) Wählen Sie unter **Aktion**die Option act_unauthorized aus.
   c) Geben Sie im Fenster **Ausdruck** die folgende Regel ein: CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)
   d) Klicken Sie auf **Erstellen**und dann auf **Schließen**.
   Die von Ihnen konfigurierte Responder-Richtlinie mit dem Namen pol_unauthorized wird nun auf der Seite **Responder-Richtlinien** angezeigt.
7. Binden Sie Ihre neue Richtlinie pol_unauthorized global, wie unter Binding a Responder Policybeschrieben.

Beispiel: Umleiten eines Clients zu einer neuen URL

Mit den folgenden Verfahren werden Clients, die innerhalb des CIDR 222.222.0.0/16 auf Ihre geschützte Website (s) zugreifen, zu einer angegebenen URL umgeleitet.

So leiten Sie Clients mithilfe der Citrix ADC-Befehlszeile um:

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

- Responder Action hinzufügen act_redirect Weiterleitung ”<http://www.example.com/404.html>”
- Responder Action anzeigen act_redirect
- Responder Policy hinzufügen pol_redirect “CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)” act_redirect
- Responder Policy anzeigen pol_redirect
- binden Responder global pol_redirect 10

Beispiel:

```
> add responder action act_redirect redirect `” http ://www.example.com /404.html ”`
Done

> add responder policy pol_redirect ”CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)” act_redirect
Done
<!--NeedCopy-->
```

So leiten Sie Clients mit der GUI um:

1. Navigieren Sie zu **AppExpert** > **Responder** > **Aktionen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Gehen **Sie im Dialogfeld Responderaktion erstellen** wie folgt vor:
   a) Geben Sie im Textfeld **Name** den Text act_redirect ein.
   b) Wählen Sie unter Typ die Option **Umleitung**aus.
   c) Geben Sie im Bereich **Zieltext** die folgende Zeichenfolge ein: ”<http://www.example.com/404.html>”
   d) Klicken Sie auf **Erstellen**und dann auf **Schließen**.
   Die von Ihnen konfigurierte Responder Action mit dem Namen act_redirect wird jetzt auf der Seite **Responderaktionen** angezeigt.
4. Klicken Sie im Navigationsbereich auf **Richtlinien**.
5. Klicken Sie im Detailbereich auf **Hinzufügen**.
6. Gehen **Sie im Dialogfeld Responder-Richtlinie erstellen** wie folgt vor:
   a) Geben Sie in das Textfeld **Name** pol_redirect ein.
   b) Wählen Sie unter **Aktion**die Option act_redirect aus.
   c) Geben Sie im Fenster **Ausdruck** die folgende Regel ein: CLIENT.IP.SRC.IN_SUBNET (222.222.0.0/16)
   d) Klicken Sie auf **Erstellen**und dann auf **Schließen**.
   Die von Ihnen konfigurierte Responder-Richtlinie mit dem Namen pol_redirect wird nun auf der Seite **Responder-Richtlinien** angezeigt.

7. Binden Sie Ihre neue Richtlinie pol_redirect global, wie unter Binding a Responder Policybeschrieben.

Diameter Unterstützung für Responder

October 5, 2021

Die Responder-Funktion unterstützt jetzt das Diameter Protokoll. Sie können Responder so konfigurieren, dass sie auf Diameter Requests wie HTTP und TCP Requests reagiert. Beispielsweise können Sie den Responder so konfigurieren, dass er auf Anfragen eines bestimmten Durchmesserursprungs mit einer Weiterleitung zu einer für mobile Geräte erweiterten Webseite reagiert. Es wurden mehrere Citrix ADC Ausdrücke hinzugefügt, die die Prüfung des Diameter Headers und der Attribute-Wert-Paare (AVPs) unterstützen. Diese Ausdrücke unterstützen die Suche nach bestimmten AVPs nach Index, ID oder Name, untersuchen die Informationen in jedem AVP und senden eine entsprechende Antwort.

So konfigurieren Sie den Responder für die Beantwortung einer Durchmesseranforderung:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add responder action <actname> RESPONDWITH "DIAMETER.NEW_REDIRECT(\"aaa://host.example.com\")"`

  Ersetzen Sie <actname> durch einen Namen für Ihre neue Aktion. Der Name kann aus einem bis 127 Zeichen bestehen und kann Buchstaben, Zahlen sowie Bindestriche (-) und Unterstriche (_) enthalten. Ersetzen Sie füraaa://host.example.comdie URL des Durchmesserhosts, zu dem Sie Verbindungen umleiten möchten.

- Responderrichtlinie hinzufügen<polname> diameter.req.avp (264) .value.eq (host1.example.net)<actname>

  Ersetzen Sie <polname> durch einen Namen für Ihre neue Richtlinie. Wie bei<actname>kann der Name aus einem bis 127 Zeichen bestehen und kann Buchstaben, Zahlen sowie Bindestriche (-) und Unterstriche (_) enthalten. Ersetzen Sie für host1.example.net den Namen des ursprünglichen Hosts der Anforderungen, die Sie umleiten möchten. Ersetzen Sie <actname> durch den Namen der Aktion, die Sie gerade erstellt haben.

- `bind lb vserver <vservername> -policyName <polname> -priority <priority> -type REQUEST`

  Ersetzen Sie den Namen des virtuellen Lastenausgleichsservers, an den Sie die Richtlinie binden möchten.<vservername> Ersetzen Sie den Namen der Richtlinie<polname>, die Sie gerade erstellt haben. Für<priority>ersetzen Sie eine Priorität für die Richtlinie.

Beispiel:

Um eine Responder-Aktion und -Richtlinie zu erstellen, um auf Durchmesseranforderungen zu antworten, die von host1.example.net mit einer Umleitung zu host.example.com stammen, können Sie die folgende Aktion und Richtlinie hinzufügen und die Richtlinie wie gezeigt binden.

```
1 > add responder action act_resp-dm-redirect RESPONDWITH "DIAMETER.
     NEW_REDIRECT("aaa://host.example.com")"
2 Done
3
4 > add responder pol_resp-dm-redirect "diameter.req.avp(264).value.eq("
     host1.example.net")" act_resp-dm-redirect
5 Done
6
7 > bind lb vserver vs1 -policyName pol_resp-dm-redirect -priority 10 -
     type REQUEST
8 Done
9 <!--NeedCopy-->
```

RADIUS-Unterstützung für Responder

October 5, 2021

Die Sprache von Citrix ADC Ausdrücken enthält Ausdrücke, die Informationen aus RADIUS-Anforderungen extrahieren und bearbeiten können. Mit diesen Ausdrücken können Sie die Funktion Responder verwenden, um auf RADIUS-Anforderungen zu antworten. Ihre Responderrichtlinien und -aktionen können jeden Ausdruck verwenden, der für eine RADIUS-Anforderung geeignet oder relevant ist. Die verfügbaren Ausdrücke ermöglichen es Ihnen, den RADIUS-Nachrichtentyp zu identifizieren, ein beliebiges Attributwertpaar (AVP) aus der Verbindung zu extrahieren und auf der Grundlage dieser Informationen unterschiedliche Antworten zu senden. Sie können auch Richtlinienbeschriftungen erstellen, die alle Responderrichtlinien für RADIUS-Verbindungen aufrufen.

Sie können RADIUS-Ausdrücke verwenden, um einfache Antworten zu erstellen, die keine Kommunikation mit dem RADIUS-Server erfordern, an den die Anforderung gesendet wurde. Wenn eine Responder-Richtlinie mit einer Verbindung übereinstimmt, erstellt und sendet Citrix ADC die entsprechende RADIUS-Antwort, ohne den RADIUS-Authentifizierungsserver zu kontaktieren. Wenn beispielsweise die Quell-IP-Adresse einer RADIUS-Anforderung aus einem Subnetz stammt, das in der Responderrichtlinie angegeben ist, kann Citrix ADC auf diese Anforderung mit einer Zugriffsablehnungsnachricht antworten oder die Anforderung einfach löschen.

Sie können auch Richtlinienbeschriftungen erstellen, um bestimmte Arten von RADIUS-Anforderungen durch eine Reihe von Richtlinien weiterzuleiten, die für diese Anforderungen geeignet sind.

Hinweis: Die aktuellen RADIUS-Ausdrücke funktionieren nicht mit RADIUS-IPv6-Attributen.

Die Citrix ADC Dokumentation für Ausdrücke, die RADIUS unterstützen, setzt voraus, dass sie mit der grundlegenden Struktur und dem Zweck der RADIUS-Kommunikation vertraut sind. Wenn Sie weitere Informationen zu RADIUS benötigen, lesen Sie Ihre RADIUS-Serverdokumentation oder suchen Sie online nach einer Einführung in das RADIUS-Protokoll.

Konfigurieren von Responderrichtlinien für RADIUS

Das folgende Verfahren verwendet die Citrix ADC Befehlszeile, um eine Responder-Aktion und -Richtlinie zu konfigurieren und die Richtlinie an einen RADIUS-spezifischen globalen Bindungspunkt zu binden.

So konfigurieren Sie eine Responder-Aktion und -Richtlinie und binden Sie die Richtlinie:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add responder action <actName> <actType>`
- `add responder policy <polName> <rule> <actName>`
- `bind responder policy <polName> <priority> <nextExpr> -type <bindPoint>`
  wo `<bindPoint>` wobei einen der radius-spezifischen globalen Bindungspunkte darstellt.

RADIUS-Ausdrücke für Responder

In einer Responderkonfiguration können Sie die folgenden Citrix ADC Ausdrücke verwenden, um auf verschiedene Teile einer RADIUS-Anforderung zu verweisen.

Identifizieren der Art der Verbindung:

- RADIUS.IS_CLIENT. Gibt TRUE zurück, wenn die Verbindung eine RADIUS-Client-Meldung (Anfrage) ist.
- RADIUS.IS_SERVER. Gibt TRUE zurück, wenn die Verbindung eine RADIUS-Servermeldung (Antwort) ist.

Ausdrücke anfordern:

- `RADIUS.REQ.CODE`. Gibt die Nummer zurück, die dem RADIUS-Anforderungstyp entspricht. Eine Ableitung der num_at-Klasse. Beispielsweise würde eine RADIUS-Zugriffsanforderung 1 (eins) zurückgeben. Eine RADIUS-Buchhaltungsanforderung würde 4 zurückgeben.
- `RADIUS.REQ.LENGTH`. Gibt die Länge der RADIUS-Anforderung einschließlich des Headers zurück. Eine Ableitung der num_at-Klasse.
- `RADIUS.REQ.IDENTIFIER`. Gibt die RADIUS-Anforderungskennung zurück, eine Nummer, die jeder Anforderung zugewiesen ist, die es ermöglicht, die Anforderung mit der entsprechenden Antwort abzugleichen. Eine Ableitung der num_at-Klasse.

- `RADIUS.REQ.AVP(<AVP Code No>).VALUE`. Gibt den Wert des ersten Vorkommens dieses AVP als Zeichenfolge vom Typ text_t zurück.
- `RADIUS.REQ.AVP(<AVP code no>).INSTANCE(instance number)`. Gibt die angegebene Instanz des AVP als Zeichenfolge vom Typ RAVP_t zurück. Ein bestimmter RADIUS-AVP kann mehrmals in einer RADIUS-Meldung auftreten. INSTANCE (0) gibt die erste Instanz zurück, INSTANCE (1) gibt die zweite Instanz zurück usw. bis zu sechzehn Instanzen.
- `RADIUS.REQ.AVP(<AVP code no>).VALUE(instance number)`. Gibt den Wert der angegebenen Instanz des AVP als Zeichenfolge vom Typ text_t zurück.
- `RADIUS.REQ.AVP(<AVP code no>).COUNT`. Gibt die Anzahl der Instanzen eines bestimmten AVP in einer RADIUS-Verbindung als Ganzzahl zurück.
- `RADIUS.REQ.AVP(<AVP code no>).EXISTS`. Gibt TRUE zurück, wenn der angegebene Typ von AVP in der Nachricht vorhanden ist, oder FALSE, wenn dies nicht der Fall ist.

Antwortausdrücke:

RADIUS-Antwortausdrücke sind identisch mit RADIUS-Anforderungsausdrücken, mit der Ausnahme, dass RES REQ ersetzt.

Typecasts von AVP-Werten:

Der ADC unterstützt Ausdrücke, um RADIUS-AVP-Werte für Text, Ganzzahl, Ganzzahl ohne Vorzeichen, lang, unsigned long, ipv4-Adresse, ipv6-Adresse, ipv6-Präfix und Zeitdatentypen zu typisieren. Die Syntax ist die gleiche wie bei anderen Citrix ADC -Typecast-Ausdrücken.

Beispiel:

Der ADC unterstützt Ausdrücke, um RADIUS-AVP-Werte für Text, Ganzzahl, Ganzzahl ohne Vorzeichen, lang, unsigned long, ipv4-Adresse, ipv6-Adresse, ipv6-Präfix und Zeitdatentypen zu typisieren. Die Syntax ist die gleiche wie bei anderen Citrix ADC -Typecast-Ausdrücken.

```
1 RADIUS.REQ.AVP(8).VALUE(0).typecast_ip_address_at
2 <!--NeedCopy-->
```

Ausdrücke vom Typ AVP:

Citrix ADC unterstützt Ausdrücke zum Extrahieren von RADIUS-AVP-Werten mit der zugewiesenen Ganzzahlcodes, die in RFC2865 und RFC2866 beschrieben sind. Sie können auch Textaliase verwenden, um dieselbe Aufgabe auszuführen. Einige Beispiele folgen.

- RADIUS.REQ.AVP (1).VALUE oder RADIUS.REQ.USERNAME.value. Extrahiert den RADIUS-Benutzernamenwert.
- RADIUS.REQ.AVP (4). VALUE oder RADIUS.REQ. ACCT_SESSION_ID.value. Extrahiert die Acct-Session-ID AVP (Code 44) aus der Nachricht.

- RADIUS.REQ.AVP (26). VALUE oder RADIUS.REQ.VENDOR_SPECIFIC.VALUE. Extrahiert den herstellerspezifischen Wert.

Die Werte der am häufigsten verwendeten RADIUS-AVPs können auf die gleiche Weise extrahiert werden.

RADIUS-Bind-Punkte:

Für Richtlinien, die RADIUS-Ausdrücke enthalten, stehen vier globale Bindpunkte zur Verfügung.

- RADIUS_REQ_OVERRIDE. Priorität/Überschreiben der Anforderungsrichtlinienwarteschlange.
- RADIUS_REQ_DEFAULT. Standardanforderungsrichtlinienwarteschlange.
- RADIUS_RES_OVERRIDE. Priorität/Überschreiben der Antwortrichtlinienwarteschlange.
- RADIUS_RES_DEFAULT. Standardwarteschlange für Antwortrichtlinien.

RADIUS-Responder-spezifische Ausdrücke:

- RADIUS_RESPONDWITH. Reagieren Sie mit der angegebenen RADIUS-Antwort. Die Antwort wird mit Citrix ADC Ausdrücken erstellt, sowohl RADIUS-Ausdrücken als auch anderen anwendbaren Ausdrücken.
- RADIUS.NEW_ANSWER. Sendet eine neue RADIUS-Antwort an den Benutzer.
- RADIUS.NEW_ACCESSREJECT. Weist die RADIUS-Anforderung zurück.
- RADIUS.NEW_AVP. Fügt der Antwort den angegebenen neuen AVP hinzu.

Anwendungsfälle

Im Folgenden sind Anwendungsfälle für RADIUS mit Responder.

Blockieren von RADIUS-Anforderungen aus einem bestimmten Netzwerk

Um das Responder-Feature so zu konfigurieren, dass Authentifizierungsanforderungen von einem bestimmten Netzwerk blockiert werden, erstellen Sie zunächst eine Responder-Aktion, die Anforderungen ablehnt. Verwenden Sie die Aktion in einer Richtlinie, die Anforderungen aus den Netzwerken auswählt, die Sie blockieren möchten. Binden Sie die Responderrichtlinie an einen RADIUS-spezifischen globalen Bindungspunkt und geben Sie Folgendes an:

- Die Priorität
- END als nextExpr-Wert, um sicherzustellen, dass die Richtlinienbewertung beendet wird, wenn diese Richtlinie übereinstimmt
- RADIUS_REQ_OVERRIDE als Warteschlange, der Sie die Richtlinie zuweisen, so dass sie vor Richtlinien ausgewertet wird, die der Standardwarteschlange zugewiesen sind.

So konfigurieren Sie Responder, um Anmeldungen von einem bestimmten Netzwerk** zu blockieren

- `add responder action <actName> <actType>`
- `add responder policy <polName> <rule> <actName>`

- `bind responder global <polName> <priority> <nextExpr> -type <bindPoint>`

Beispiel:

```
1 > add responder action rspActRadiusReject respondwith radius.
     new_accessreject
2 Done
3
4 > add responder policy rspPolRadiusReject client.ip.src.in_subnet
     (10.224.85.0/24) rspActRadiusReject
5 Done
6
7 > bind responder global rspPolRadiusReject 1 END -type
     RADIUS_REQ_OVERRIDE
8 <!--NeedCopy-->
```

DNS-Unterstützung für die Responder-Funktion

October 5, 2021

Sie können die Responder-Funktion so konfigurieren, dass sie auf DNS-Anforderungen reagiert, wie auf HTTP- und TCP-Anforderungen. Sie können es beispielsweise so konfigurieren, dass DNS-Antworten über UDP gesendet werden und sicherstellen, dass die DNS-Anforderungen des Clients über TCP gesendet werden. Eine Reihe von Citrix ADC Ausdrücken unterstützen die Prüfung des DNS-Headers in der Anforderung. Diese Ausdrücke untersuchen bestimmte Header-Felder und senden eine entsprechende Antwort.

- **DNS-Ausdrücke**. In einer Responderkonfiguration können Sie die folgenden Citrix ADC Ausdrücke verwenden, um auf verschiedene Teile einer DNS-Anforderung zu verweisen:

Ausdrücke	Beschreibungen
DNS.NEW_RESPONSE	Erstellt eine neue leere DNS-Antwort basierend auf der Anforderung.
DNS.NEW_RESPONSE <AA, TC, rcode>	Erstellt eine neue DNS-Antwort basierend auf den angegebenen Parametern.

- **DNS-Bindungspunkte**. Die folgenden globalen Bindungspunkte sind für Richtlinien verfügbar, die DNS-Ausdrücke enthalten.

Punkte binden	Beschreibungen
DNS_REQ_OVERRIDE	Priorität/Überschreiben der Anforderungsrichtlinienwarteschlange.
DNS_REQ_DEFAULT	Standardanforderungsrichtlinienwarteschlange.

Zusätzlich zu den Standardverbindungspunkten können Sie Richtlinienbeschriftungen vom Typ DNS erstellen und DNS-Richtlinien an diese binden.

Konfigurieren von Responderrichtlinien für DNS

Das folgende Verfahren verwendet die Citrix ADC Befehlszeile, um eine Responder-Aktion und -Richtlinie zu konfigurieren und die Richtlinie an einen Responder-spezifischen globalen Bindungspunkt zu binden.

So konfigurieren Sie den Responder für die Beantwortung einer DNS-Anforderung:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

1. `add responder action <actName> <actType>`

   Ersetzen Sie `<actname>` durch einen Namen für Ihre neue Aktion. Der Name kann 1 bis 127 Zeichen lang sein und kann Buchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten. Ersetzen Sie `<actType>` durch den Responderaktionstyp *RespondWith*.

2. `add responder policy <polName> <rule> <actName>`

   Ersetzen Sie `<polname>` durch einen Namen für Ihre neue Richtlinie. Für `<actname>` kann der Name 1 bis 127 Zeichen lang sein und kann Buchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten. Ersetzen Sie `<actname>` durch den Namen der Aktion, die Sie gerade erstellt haben.

3. `bind responder policy <polName> <priority> <nextExpr> -type <bindPoint>`

   Geben Sie für `<bindPoint>` einen der Responder-spezifischen globalen Bindungspunkte an. Ersetzen Sie `<polName>` durch den Namen der Richtlinie, die Sie gerade erstellt haben. Geben Sie für `<priority>` die Priorität der Richtlinie an.

Beispielkonfiguration - Erzwingen Sie alle DNS-Anfragen über TCP:

Um alle DNS-Anforderungen über TCP zu erzwingen, erstellen Sie eine Responder-Aktion, die das TC-Bit und rcode als NOERROR setzt.


```
> add responder action resp_act_set_tc_bit respondwith DNS.NEW_RESPONSE
   (true, true, NOERROR)
Done

> add responder policy enforce_tcp  dns.REQ.TRANSPORT.EQ(udp)
   resp_act_set_tc_bit
Done

>bind lb vserver dns_udp  - policyName  enforce_tcp   -type request  -
   priority 100
Done
<!--NeedCopy-->
```

MQTT-Unterstützung für Responder

October 5, 2021

Die Responder-Funktion unterstützt das MQTT-Protokoll. Sie können Responder-Richtlinien so konfigurieren, dass sie eine Aktion basierend auf den Parametern in der eingehenden MQTT-Nachricht ausführen.

Die Aktion reagiert mit einem der folgenden Punkte auf eine neue Verbindung:

- DROP
- RESET
- NOOP
- Eine Responder-Aktion, um eine neue MQTT CONNACK-Antwort einzuleiten.

Konfigurieren von Responder-Richtlinien für MQTT

Nachdem Sie die Responder-Funktion aktiviert haben, müssen Sie eine oder mehrere Aktionen für die Bearbeitung von MQTT-Anfragen konfigurieren. Konfigurieren Sie dann eine Responder-Richtlinie. Sie können die Responder-Richtlinien global oder an einen bestimmten virtuellen Lastausgleichsserver oder virtuellen Content Switching-Server binden.

Die folgenden Bindepunkte stehen zur Verfügung, um die Responder-Richtlinien global zu binden:

- MQTT_REQ_DEFAULT
- MQTT_REQ_OVERRIDE
- MQTT_JUMBO_REQ_DEFAULT
- MQTT_JUMBO_REQ_OVERRIDE

Die folgenden Bindepunkte sind verfügbar, um die Responder-Richtlinien an einen virtuellen Content Switching- oder Lastenausgleichsserver zu binden:

- REQUEST
- MQTT_JUMBO_REQ (dieser Bindepunkt wird nur für Jumbo-Pakete verwendet)

So konfigurieren Sie den Responder so, dass er mit CLI auf eine MQTT-Anfrage antwortet

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

Konfigurieren Sie eine Responder-Aktion.

```
add responder action <actName> <actType>
<!--NeedCopy-->
```

- Ersetzen Sie `actname` durch einen Namen für Ihre neue Aktion. Der Name kann 1—127 Zeichen lang sein und kann Buchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.
- Ersetzen Sie für `actType`einen Responder-Aktionstyp respondwith.

Beispiel:

```
add responder action mqtt_connack_unsup_ver respondwith MQTT.
   NEW_CONNACK(132)
<!--NeedCopy-->
```

Konfigurieren Sie eine Responderrichtlinie. Die Citrix ADC Appliance reagiert auf die MQTT-Anforderungen, die in dieser Responder-Richtlinie ausgewählt werden.

```
add responder policy <polName> <rule> <actname>
<!--NeedCopy-->
```

- Ersetzen Sie `polname` durch einen Namen für Ihre neue Richtlinie.
- Ersetzen Sie für `actname`den Namen der Aktion, die Sie erstellt haben.

Beispiel:

```
add responder policy reject_lower_version "MQTT.HEADER.COMMAND.EQ(
   CONNECT) && MQTT.VERSION.LT(3)" mqtt_connack_unsup_ver
<!--NeedCopy-->
```


Binden Sie die Responder-Richtlinie an einen bestimmten virtuellen Lastausgleichsserver oder virtuellen Content Switching-Server. Die Richtlinie gilt nur für die MQTT-Anfragen, deren Ziel-IP-Adresse der VIP dieses virtuellen Servers ist.

```
bind lb vserver <name> -policyName <policy_name> -priority <priority>

bind cs vserver <name> -policyName <policy_name> -priority <priority>
<!--NeedCopy-->
```

- Ersetzen Sie für `policy_name`den Namen der Richtlinie, die Sie erstellt haben.
- Geben Sie für `priority` die Priorität der Richtlinie an.

Beispiel:

```
bind lb vserver lb1 -policyName reject_lower_version -priority 50

bind cs vserver mqtt_frontend_cs -policyName reject_lower_version -
   priority 5
<!--NeedCopy-->
```

Anwendungsfall1: Filtern Sie Clients basierend auf dem Benutzernamen oder der Client-ID

Der Administrator kann eine MQTT-Responder-Richtlinie konfigurieren, um die Verbindung basierend auf dem Benutzernamen oder der Client-ID in der MQTT CONNECT-Nachricht abzulehnen.

Beispielkonfiguration zum Filtern von Clients basierend auf der Client-ID

```
add policy patset filter_clients
bind policy patset filter_clients client1

add responder action mqtt_connack_invalid_client respondwith MQTT.
   NEW_CONNACK(2)

add responder policy reject_clients "MQTT.HEADER.COMMAND.EQ(CONNECT) &&
    mqtt.connect.clientid.equals_any("filter_clients")"
   mqtt_connack_invalid_client

bind cs vserver mqtt_frontend_cs -policyName reject_clients -priority 5
<!--NeedCopy-->
```


Verwenden Sie case2: Begrenzen Sie die maximale Nachrichtenlänge von MQTT-Nachrichten, um Jumbo-Pakete zu verarbeiten

Der Administrator kann eine MQTT-Responder-Richtlinie konfigurieren, um die Clientverbindung zu löschen, wenn die Länge der Nachricht einen bestimmten Schwellenwert überschreitet, oder die erforderlichen Maßnahmen basierend auf der Anforderung ergreifen.

Um Jumbo-Pakete zu behandeln, sind die Responder-Richtlinien mit einem der folgenden Regelmuster an den Jumbo-Bind-Punkt gebunden:

- MQTT.MESSAGE_LENGTH
- MQTT.COMMAND
- MQTT.FROM_CLIENT
- MQTT.FROM_SERVER

Richtlinien, die an Jumbo-Bindepunkte gebunden sind, werden nur für Jumbo-Pakete ausgewertet.

Beispielkonfiguration zur Begrenzung der maximalen Nachrichtenlänge von MQTT-Nachrichten

```
1 set lb parameter -dropmqttjumbomessage no
2
3 add responder policy drop_large_message MQTT.MESSAGE_LENGTH.GT(100000)
     reset
4
5 bind cs vserver mqtt_frontend_cs -policyName drop_large_message -
     priority 10
6 <!--NeedCopy-->
```

In diesem Beispiel ist der `dropmqttjumbomessage` Parameter auf NO festgelegt. Daher verarbeitet die ADC-Appliance die Nachrichten mit einer Länge von mehr als 64.000 Byte und weniger als 1.00.000 Byte. Die Nachrichten mit einer Länge von mehr als 1.00.000 Bytes werden zurückgesetzt.

Wie man HTTP-Anfrage mit Responder an HTTPS umleitet

October 5, 2021

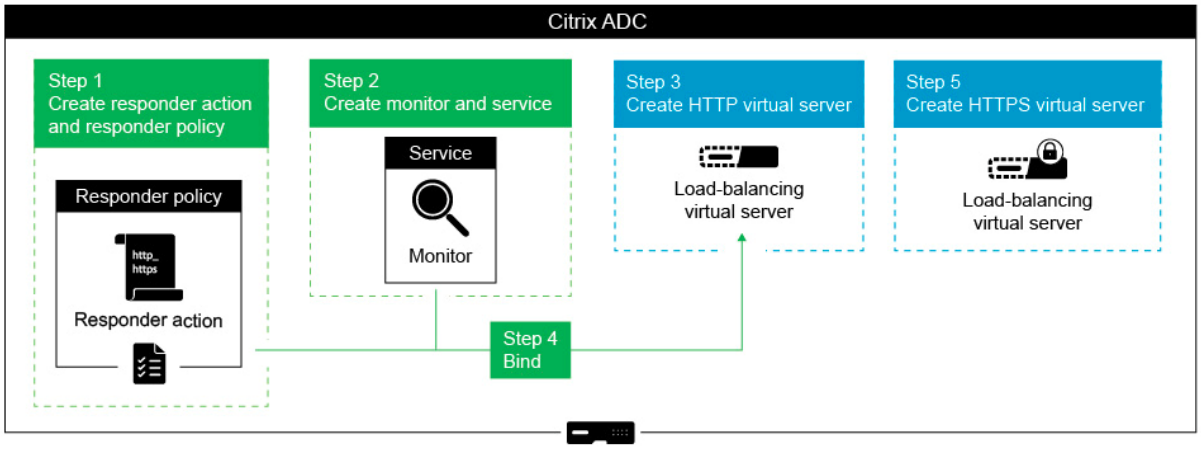
In diesem Artikel wird erläutert, wie Sie das Responder-Feature mit einem Lastenausgleich virtuellen Server-IP-Adressen konfigurieren und Clientanforderungen von HTTP an HTTPS umleiten.

Betrachten Sie ein Szenario, in dem ein Benutzer versuchen könnte, durch Senden einer HTTP-Anforderung auf eine sichere Website zuzugreifen. Anstatt die Anforderung zu löschen, sollten Sie

die Anforderung möglicherweise an eine sichere Website umleiten. Sie können die Responder-Funktion verwenden, um die Anforderung an die sichere Website umzuleiten, ohne den Pfad und die URL-Abfrage zu ändern, auf die der Benutzer zugreifen möchte.

Wie Citrix ADC Responder eine Anforderung von HTTP an HTTPS umleitet

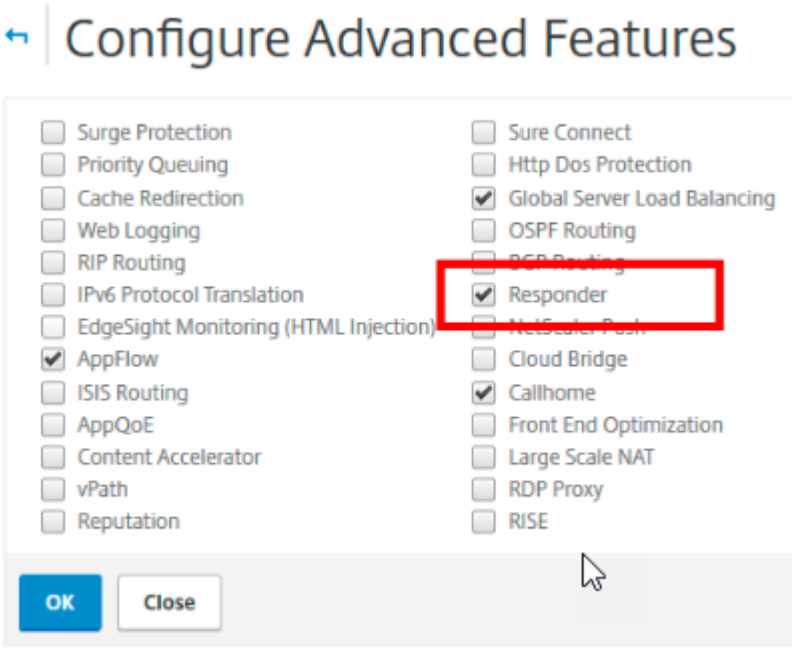
Die folgende Abbildung zeigt einen Schritt für Schritt, wie die Appliance eine Anforderung umleitet.



> **Hinweis**: Die Navigationspfade und Screenshots werden von NetScaler 11.0 abgeleitet.

Führen Sie das folgende Verfahren aus, um die Responder-Funktion zusammen mit den Load Balancing VIP-Adressen einer NetScaler Appliance so zu konfigurieren, dass Clientanforderungen von HTTP an HTTPS umgeleitet werden.

1. Aktivieren Sie die Responder-Funktion auf der Appliance. Navigieren Sie zu **System** > **Einstellungen** > **Erweiterte Funktionen konfigurieren** > **Responder**.



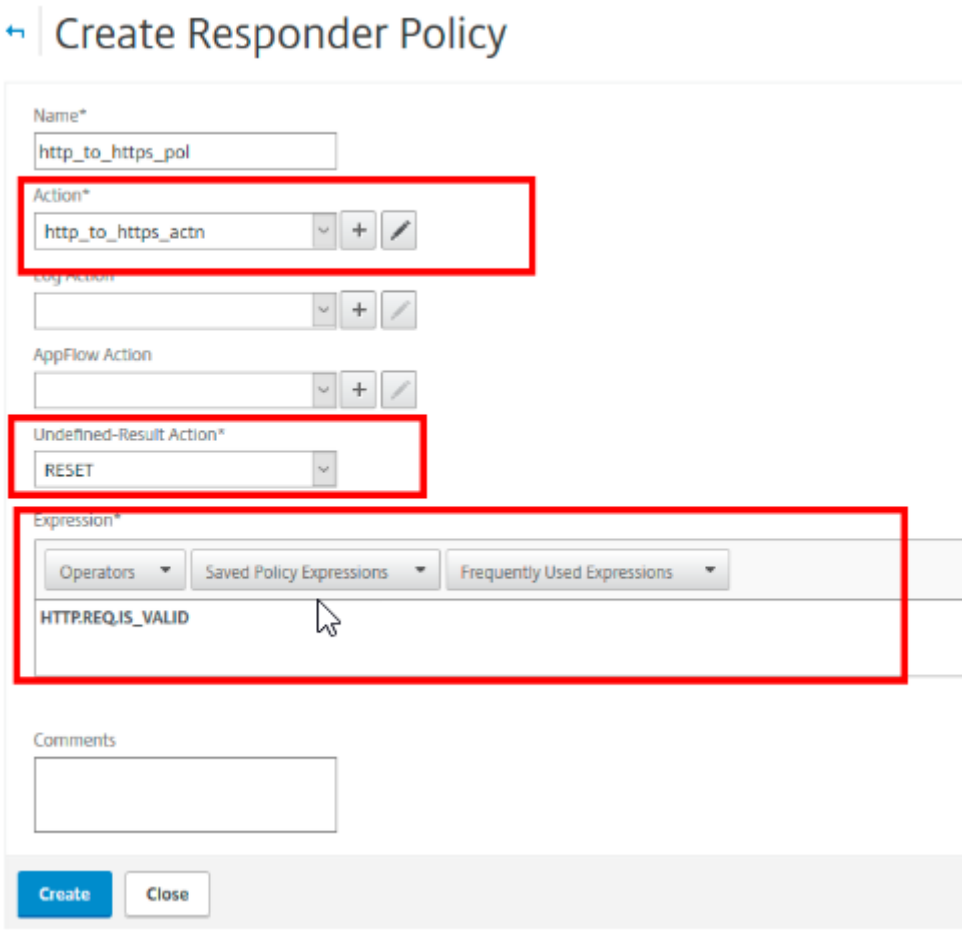
2. Erstellen Sie eine Responder-Aktion, und geben Sie im Feld Name einen entsprechenden Namen an, z. B. http_to_https_actn.
3. Um eine Responder-Aktion zu erstellen, erweitern Sie im Navigationsbereich **AppExpert** > **Responder**, klicken Sie auf **Aktionen**, und klicken Sie dann auf **Hinzufügen** .
4. Wählen Sie Als Typ umleiten aus.
5. Geben Sie im Feld **Ausdruck** den folgenden Ausdruck ein:

   ```
   "https://"+ HTTP.REQ.HOSTNAME.HTTP_URL_SAFE + HTTP.REQ.URL.PATH_AND_QUERY
   .HTTP_URL_SAFE.
   ```

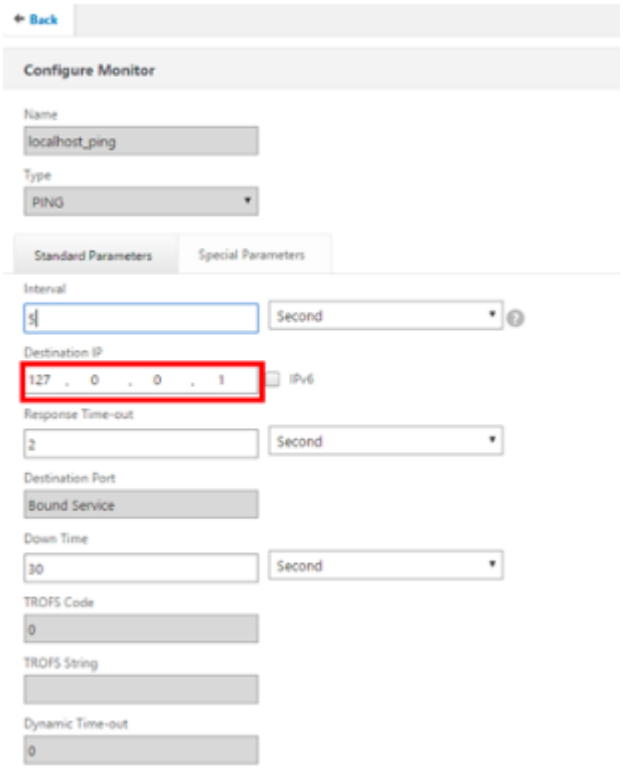
6. Stellen Sie in NetScaler Version 9.0 und 10.0 sicher, dass die Option **Sicherheitsprüfung umgehen** deaktiviert ist.

   Hinweis: Diese Option ist ab NetScaler 11.0 nicht vorhanden.

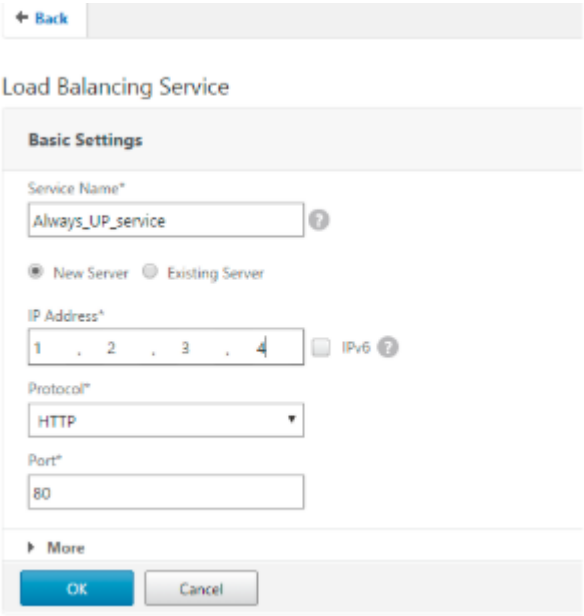
7. Erstellen Sie eine **Responder-Richtlinie**, und geben Sie im Feld Name einen entsprechenden Namen an, z. B. http_to_https_pol.
8. Um eine Responder-Richtlinie zu erstellen, erweitern Sie im Navigationsbereich **AppExpert** > **Responder**, klicken Sie auf **Richtlinien** und dann auf **Hinzufügen** .
9. Wählen Sie in der Liste Aktion den Aktionsnamen aus, den Sie erstellt haben.
10. Wählen Sie in der Liste Nicht definierte Aktion die Option RESET aus.
11. Geben Sie den **HTTP.REQ.IS_VALID** Ausdruck in das Feld **Ausdruck** ein, wie im folgenden Screenshot gezeigt.



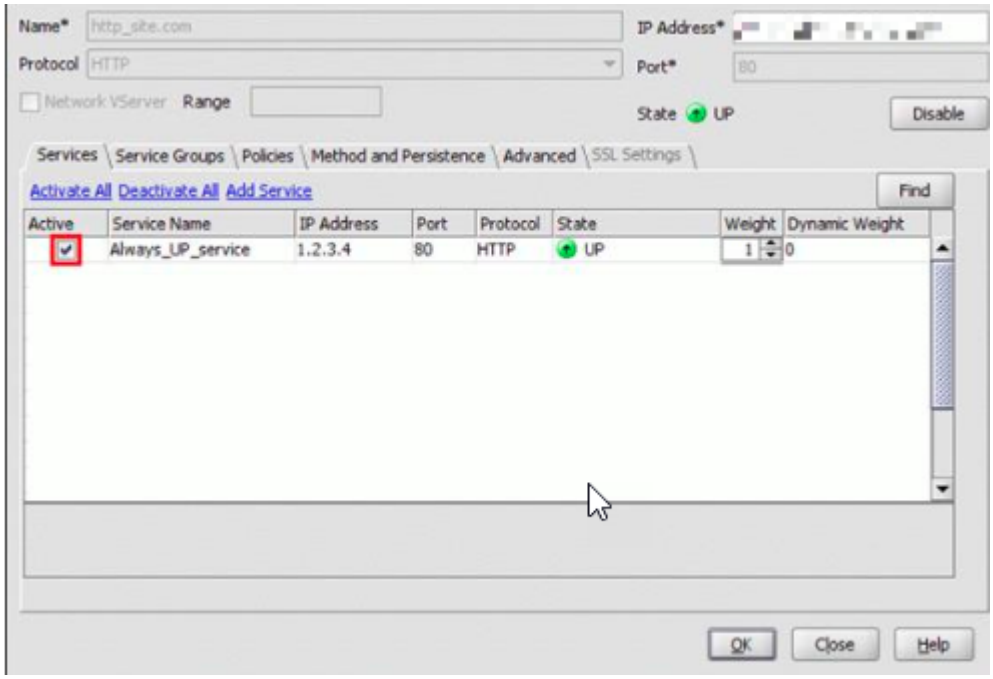
1. Erstellen Sie einen Monitor, für den der Status immer als UP markiert ist, und geben Sie im Feld Name einen entsprechenden Namen an, z. B. localhost_ping.
2. Erweitern Sie zum Erstellen eines Monitors im Navigationsbereich **Lastenausgleich**, klicken Sie auf **Monitore**, und klicken Sie dann auf **Hinzufügen**.
3. Geben Sie im Feld **Ziel-IP** die IP-Adresse 127.0.0.1 an, wie im folgenden Screenshot gezeigt.



4. **Erstellen Sie einen Dienst, und geben Sie im Feld Name einen entsprechenden Namen an, z. B. Always_UP_Service.**
5. Um einen Dienst zu erstellen, erweitern Sie im Navigationsbereich **Lastenausgleich**, klicken Sie auf **Dienste**, und klicken Sie dann auf **Hinzufügen**.
6. Geben Sie im Feld **Server** eine nicht vorhandene IP-Adresse an.



7. Geben Sie im Feld **Port** 80 ein.
8. Fügen Sie den erstellten Monitor aus der Liste **Verfügbare Monitore** hinzu.
9. Erstellen Sie einen virtuellen Load Balancing Server, und geben Sie einen entsprechenden Namen im Feld **Name** an.
10. Um einen virtuellen Lastenausgleichsserver zu erstellen, erweitern Sie im Navigationsbereich **Lastenausgleich**, klicken Sie auf **Dienste**, und klicken Sie dann auf **Hinzufügen**.
11. Geben Sie die IP-Adresse der Website im Feld IP-Adresse an.
12. Wählen Sie HTTP aus der Protokollliste.
13. Geben Sie 80 in das Feld Port ein.
14. Wählen Sie in NetScaler Version 9.0 und 10.0 die Option Aktiv für den Dienst, den Sie auf der Registerkarte Dienste erstellt haben, wie im folgenden Screenshot gezeigt. Diese Option ist in NetScaler Version 11.0 veraltet.



15. Klicken Sie auf die Registerkarte **Richtlinien**.
16. Binden Sie die von Ihnen erstellte Responder-Richtlinie an die HTTP-Load Balancing-VIP-Adresse der Website.
17. Erstellen Sie einen sicheren virtuellen Load Balancing-Server, der die IP-Adresse der Website und Port als 443 aufweist.

Führen Sie folgende Befehle aus, um eine Konfiguration ähnlich der vorherigen Prozedur über die Befehlszeilenschnittstelle der Appliance zu erstellen:


```
enable ns feature responder
add responder action http_to_https_actn redirect ""https://" + http.req
    .hostname.HTTP_URL_SAFE + http.REQ.URL.PATH_AND_QUERY.HTTP_URL_SAFE"
add responder policy http_to_https_pol HTTP.REQ.IS_VALID
    http_to_https_actn RESET
add lb monitor localhost_ping PING -LRTM ENABLED -destIP 127.0.0.1
add service Always_UP_service 1.2.3.4 HTTP 80 -gslb NONE -maxClient 0 -
    maxReq 0 -cip ENABLED dummy -usip NO -sp OFF -cltTimeout 180 -
    svrTimeout 360 -CKA NO -TCPB NO -CMP YES
bind lb monitor localhost_ping Always_UP_service
add lb vserver http_site.com HTTP 10.217.96.238 80 -persistenceType
    COOKIEINSERT -timeout 0 -cltTimeout 180
bind lb vserver http_site.com Always_UP_service
bind lb vserver http_site.com -policyName http_to_https_pol -priority 1
     -gotoPriorityExpression END
<!--NeedCopy-->
```

Hinweise:

- Der Status des virtuellen Port80 Load Balancing Redirect Servers muss UP sein, damit die Umleitung funktioniert.
- Webbrowser werden möglicherweise nicht korrekt umgeleitet, wenn der virtuelle HTTPS-Server nicht aktiv ist.
- Diese Umleitungseinrichtung ermöglicht Situationen, in denen mehrere Domänen an dieselbe IP-Adresse gebunden sind.
- Wenn der Client eine ungültige HTTP-Anforderung an den virtuellen Umleitungsserver sendet, sendet die Appliance einen RESET Meldungscode.

Problembehandlung

October 5, 2021

Wenn das Responder-Feature nach der Konfiguration nicht wie erwartet funktioniert, können Sie einige gängige Tools verwenden, um auf Citrix ADC Ressourcen zuzugreifen und das Problem zu diagnostizieren.

Ressourcen für die Fehlerbehebung

Verwenden Sie die folgenden Ressourcen zur Behebung eines integrierten Cache-Problems auf einer Citrix ADC Appliance, um optimale Ergebnisse zu erzielen:

- Die Datei ns.conf
- Die relevanten Trace-Dateien vom Client und der Citrix ADC Appliance

Zusätzlich zu den oben genannten Ressourcen beschleunigen die folgenden Tools die Fehlerbehebung:

- Die iehttpheader oder ein ähnliches Dienstprogramm
- Die für Citrix ADC C-Trace-Dateien angepasste Wireshark-Anwendung

Beheben von Responderproblemen

- **Problem**

  Die Responder-Funktion ist konfiguriert, aber die Responder-Aktion funktioniert nicht.

  Lösung

  - Stellen Sie sicher, dass das Feature aktiviert ist.
  - Überprüfen Sie die Trefferzähler einer der Richtlinien, um zu sehen, ob die Zähler erhöht werden.
  - Stellen Sie sicher, dass die Richtlinien und Aktionen korrekt konfiguriert sind.
  - Stellen Sie sicher, dass die Aktionen und Richtlinien entsprechend gebunden sind.
  - Zeichnen Sie die Paketverfolgungen auf dem Client und der Citrix ADC Appliance auf, und analysieren Sie diese, um einen Zeiger auf das Problem zu erhalten.
  - Notieren Sie die iehttpHeaters-Paketverfolgungen auf dem Client und überprüfen Sie die HTTP-Anforderungen und Antworten, um einen Zeiger auf das Problem zu erhalten.

- **Problem**

  Sie müssen eine Wartungsseite erstellen.

  Lösung

1. Konfigurieren Sie die Dienste und den virtuellen Server.
2. Konfigurieren Sie einen virtuellen Sicherungsserver mit einem an ihn gebundenen Dienst. Dadurch wird sichergestellt, dass der Status der Website immer als UP angezeigt wird.
3. Konfigurieren Sie den primären virtuellen Server so, dass er den virtuellen Sicherungsserver als Sicherung verwendet.
4. Erstellen Sie eine Responder-Aktion mit einem geeigneten Ziel. Es folgt ein Beispiel für Ihre Referenz:

   ```
   add responder action sorry_page respondwith q{ ”HTTP/1.0 200 OK”+”\r\n\
   r\n”+ ”<html><body>Sorry, this page is not available\</body>\</html>”+
   ”\r\n”}
   ```

5. Erstellen Sie eine Responderrichtlinie und binden Sie die Aktion daran.

6. Binden Sie die Responder-Richtlinie an den virtuellen Sicherungsserver.

Neuschreiben

October 5, 2021

> **Warnung**
>
> Filterfunktionen mit klassischen Richtlinien sind veraltet, und als Alternative empfiehlt Citrix die Verwendung der Rewrite- und Responder-Features mit erweiterter Richtlinieninfrastruktur.

Rewrite bezieht sich auf das Umschreiben einiger Informationen in den Anforderungen oder Antworten, die von der Citrix ADC Appliance verarbeitet werden. Das Umschreiben kann dabei helfen, Zugriff auf den angeforderten Inhalt zu gewähren, ohne unnötige Details über die tatsächliche Konfiguration der Website offenzulegen. Einige Situationen, in denen das Rewrite-Feature nützlich ist, werden im Folgenden beschrieben:

- Zur Verbesserung der Sicherheit kann Citrix ADC alle`http://links` in`https://` den Antworttext umschreiben.
- In der SSL-Offload-Bereitstellung müssen die unsicheren Links in der Antwort in sichere Links umgewandelt werden. Mit der Option Umschreiben können Sie alle in umschreiben, `http://links` um`https://` sicherzustellen, dass die ausgehenden Antworten von Citrix ADC an den Client über die gesicherten Verknüpfungen verfügen.
- Wenn eine Website eine Fehlerseite anzeigen muss, können Sie anstelle der standardmäßigen 404-Fehlerseite eine benutzerdefinierte Fehlerseite anzeigen. Wenn Sie beispielsweise die Homepage oder die Sitemap der Website anstelle einer Fehlerseite anzeigen, bleibt der Besucher auf der Website, anstatt sich von der Website zu entfernen.
- Wenn Sie eine neue Website starten möchten, aber die alte URL verwenden möchten, können Sie die Option Umschreiben verwenden.
- Wenn ein Thema in einer Website über eine komplizierte URL verfügt, können Sie es mit einer einfachen, leicht zu merkenden URL umschreiben (auch als “coole URL” bezeichnet).
- Sie können den Standardseitennamen an die URL einer Website anhängen. Wenn die Standardseite der Website eines Unternehmens beispielsweise lautet`http://www.abc.com/index.php`, wenn der Benutzer ‘abc.com’ in der Adressleiste des Browsers eingibt, können Sie die URL in ‘abc.com/index.php’ umschreiben.

Wenn Sie das Rewrite-Feature aktivieren, kann Citrix ADC die Header und den Hauptteil von HTTP-Anforderungen und -Antworten ändern.

Um HTTP-Anforderungen und -Antworten neu zu schreiben, können Sie protokollfähige Citrix ADC Richtlinienausdrücke in den von Ihnen konfigurierten Umschreibrichtlinien verwenden. Die virtuellen Server, die die HTTP-Anforderungen und -Antworten verwalten, müssen vom Typ

HTTP oder
SSL sein. Im HTTP-Datenverkehr können Sie die folgenden Aktionen ausführen:

- Ändern der URL einer Anfrage
- Hinzufügen, Ändern oder Löschen von Kopfzeilen
- Fügen Sie eine bestimmte Zeichenfolge innerhalb des Hauptteils oder der Kopfzeilen hinzu, ersetzen oder löschen Sie sie.

Um TCP-Nutzlasten neu zu schreiben, betrachten Sie die Nutzlast als Rohstrom von Bytes. Jeder der virtuellen Server, die die TCP-Verbindungen verwalten, muss vom Typ TCP oder SSL_TCP sein. Der Begriff TCP-Rewrite bezieht sich auf das Rewrite von TCP-Nutzlasten, die keine HTTP-Daten sind. Im TCP-Datenverkehr können Sie einen beliebigen Teil der TCP-Nutzlast hinzufügen, ändern oder löschen.

Beispiele zur Verwendung der Rewrite-Funktion finden Sie unter Aktions- und Richtlinienbeispiele umschreiben.

Vergleich zwischen Rewrite und Responder Optionen

Der Hauptunterschied zwischen dem Rewrite-Feature und dem Responder-Feature ist wie folgt:

Responder kann nicht für Antwort- oder serverbasierte Ausdrücke verwendet werden. Responder kann nur für die folgenden Szenarien verwendet werden, abhängig von Client-Parametern:

- Umleiten einer HTTP-Anforderung an neue Websites oder Webseiten
- Reagieren mit einer benutzerdefinierten Antwort
- Löschen oder Zurücksetzen einer Verbindung auf Anforderungsebene

Im Falle einer Responderrichtlinie untersucht der Citrix ADC die Anforderung des Clients, führt Maßnahmen gemäß den geltenden Richtlinien aus, sendet die Antwort an den Client und schließt die Verbindung mit dem Client.

Im Falle einer Rewrite-Richtlinie überprüft der Citrix ADC die Anforderung des Clients oder die Antwort des Servers, führt Maßnahmen gemäß den geltenden Richtlinien aus und leitet den Datenverkehr an den Client oder den Server weiter.

Im Allgemeinen wird empfohlen, den Responder zu verwenden, wenn Citrix ADC eine Verbindung basierend auf einem Client- oder anforderungsbasierten Parameter zurücksetzen oder löschen soll. Verwenden Sie den Responder, um Datenverkehr umzuleiten oder mit benutzerdefinierten Nachrichten zu antworten. Verwenden Sie Rewrite zum Bearbeiten von Daten auf HTTP-Anforderungen und -Antworten.

Wie Rewrite funktioniert

October 5, 2021

Eine Rewrite-Richtlinie besteht aus einer Regel und einer Aktion. Die Regel bestimmt den Datenverkehr, auf den das Umschreiben angewendet wird, und die Aktion bestimmt die Aktion, die vom Citrix ADC ausgeführt werden soll. Sie können mehrere Umschreibungsrichtlinien definieren. Geben Sie für jede Richtlinie den Bindepunkt und die Priorität an.

Ein Bindepunkt bezieht sich auf einen Punkt im Datenfluss, an dem Citrix ADC den Datenverkehr prüft, um zu überprüfen, ob eine Umschreibungsrichtlinie darauf angewendet werden kann. Sie können eine Richtlinie an einen bestimmten virtuellen Lastausgleichs- oder Content Switching-Server binden oder die Richtlinie global festlegen, wenn die Richtlinie auf den gesamten Datenverkehr angewendet werden soll, der vom Citrix ADC verarbeitet wird. Diese Richtlinien werden als globale Richtlinien bezeichnet.

Zusätzlich zu den benutzerdefinierten Richtlinien verfügt der Citrix ADC über einige Standardrichtlinien. Eine Standardrichtlinie kann nicht geändert oder gelöscht werden.

Für die Bewertung der Richtlinien folgt Citrix ADC der folgenden Reihenfolge:

- Globale Richtlinien
- Richtlinien, die an bestimmte virtuelle Server gebunden sind
- Standardrichtlinien

Hinweis: Citrix ADC kann eine Rewrite-Richtlinie nur anwenden, wenn sie an einen Punkt gebunden ist.

Citrix ADC implementiert das Rewrite-Feature in den folgenden Schritten:

- Die Citrix ADC Appliance sucht nach globalen Richtlinien und sucht dann an einzelnen Bindungspunkten nach Richtlinien.
- Wenn mehrere Richtlinien an einen Bindepunkt gebunden sind, wertet der Citrix ADC die Richtlinien in der Reihenfolge ihrer Priorität aus. Die Richtlinie mit der höchsten Priorität wird zuerst bewertet. Wenn die Richtlinie nach der Auswertung der Richtlinie auf TRUE ausgewertet wird (der Datenverkehr entspricht der Regel), fügt sie die der Richtlinie zugeordnete Aktion einer Liste der auszuführenden Aktionen hinzu. Eine Übereinstimmung tritt auf, wenn die in der Richtlinienregel angegebenen Merkmale mit den Eigenschaften der auszuwertenden Anforderung oder Antwort übereinstimmen.
- Für jede Richtlinie können Sie zusätzlich zu der Aktion die Richtlinie angeben, die nach der Auswertung der aktuellen Richtlinie ausgewertet werden soll. Diese Richtlinie wird als Gehe zum Ausdruck bezeichnet. Wenn für jede Richtlinie ein Gehe zu Ausdruck (GoToPriorityExpr) angegeben ist, wertet Citrix ADC die Richtlinie Gehe zu Ausdrücken aus und ignoriert die Richtlinie mit der nächsthöheren Priorität.

  Sie können die Priorität der Richtlinie angeben, um die Richtlinie Gehe zu Ausdrücken anzugeben. Sie können den Namen der Richtlinie nicht verwenden. Wenn Sie möchten,

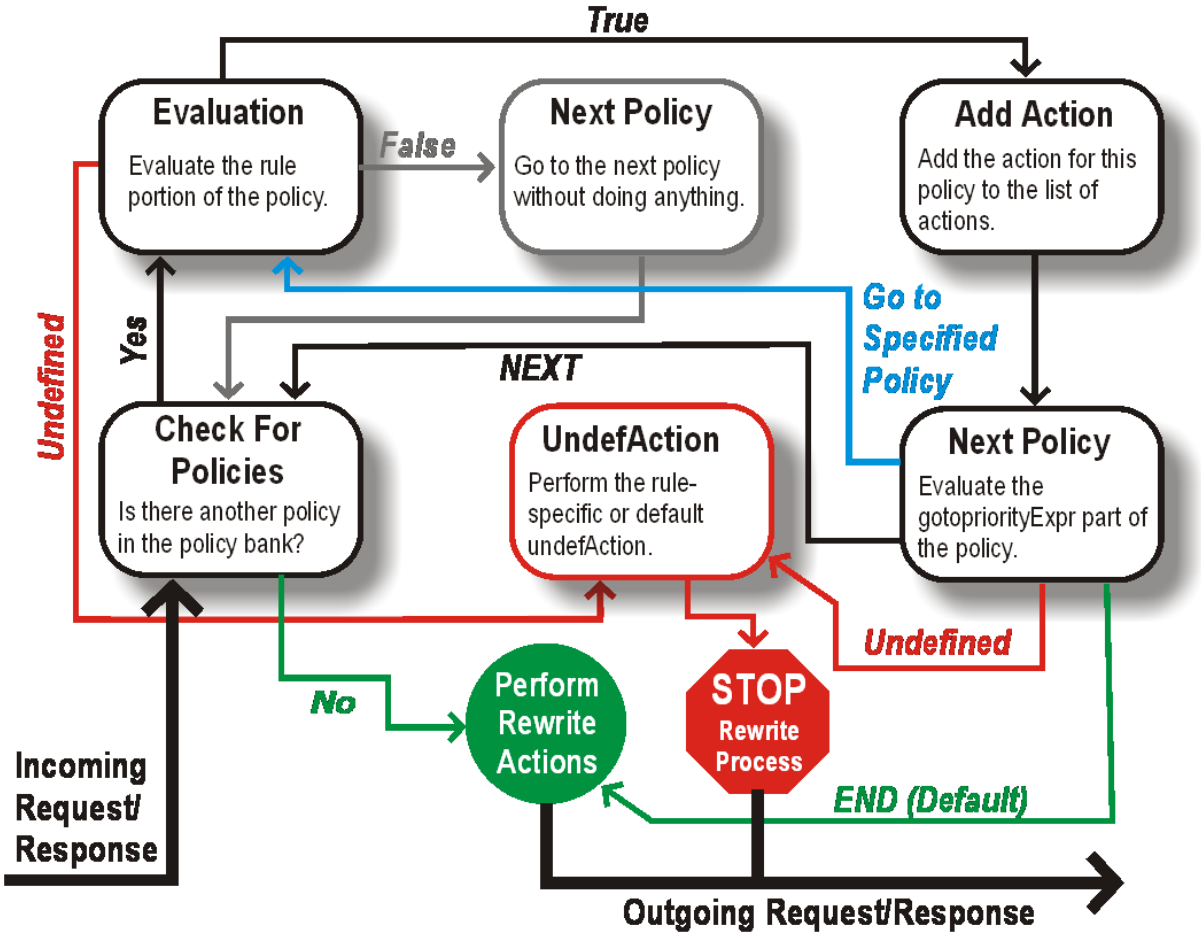
dass Citrix ADC die Auswertung anderer Richtlinien nach der Auswertung einer bestimmten Richtlinie nicht mehr auswertet, können Sie die Option Go to Expression auf END festlegen.

- Nachdem alle Richtlinien ausgewertet wurden oder wenn eine Richtlinie den Gehe zu Ausdruck als END festgelegt hat, beginnt Citrix ADC die Aktionen entsprechend der Liste der Aktionen auszuführen.

Weitere Informationen zum Konfigurieren von Rewrite-Richtlinien finden Sie unter Konfigurieren einer Rewrite-Richtlinie und zum Binden von Rewrite-Richtlinien finden Sie unter Binden einer Rewrite-Richtlinie.

Die folgende Abbildung zeigt, wie Citrix ADC eine Anforderung oder Antwort verarbeitet, wenn das Rewrite-Feature verwendet wird.

Abbildung 1. Der Rewrite-Prozess



Policy-Evaluierung

Die Richtlinie mit der höchsten Priorität wird zuerst bewertet. Citrix ADC stoppt die Auswertung von Umschreibrichtlinien nicht, wenn eine Übereinstimmung gefunden wird; es wertet alle auf dem Citrix

ADC konfigurierten Umschreibrichtlinien aus.

- Wenn eine Richtlinie auf TRUE ausgewertet wird, folgt der Citrix ADC wie folgt:
  - Wenn für die Richtlinie Gehe zu Ausdruck auf END festgelegt ist, stoppt Citrix ADC die Auswertung aller anderen Richtlinien und führt das Umschreiben durch.
  - Der gotoPriorityExpression kann auf 'NEXT', 'END', eine ganze Zahl oder INVOCATION_LIST gesetzt werden. Der Wert bestimmt die Richtlinie mit der nächsten Priorität. Die folgende Tabelle zeigt die Aktion, die Citrix ADC für jeden Wert des Ausdrucks ausgeführt hat.

Wert des Ausdrucks	Aktion
NEXT	Richtlinie mit der nächsten Priorität wird ausgewertet.
END	Die Evaluierung der Richtlinie stoppt.
<an integer>	Die Richtlinie mit der angegebenen Priorität wird ausgewertet.
INVOCATION_LIST	Gehe zu NEXT oder END wird basierend auf dem Ergebnis der Aufrufliste angewendet.

- Wenn eine Richtlinie auf FALSE ausgewertet wird, setzt Citrix ADC die Bewertung in der Reihenfolge der Priorität fort.
- Wenn eine Richtlinie als UNDEFINED ausgewertet wird (aufgrund eines Fehlers nicht ausgewertet werden kann), führt Citrix ADC die Aktion aus, die der UNDEFINED Bedingung zugewiesen ist (als undefAction bezeichnet) und stoppt die weitere Auswertung der Richtlinien.

Das Citrix ADC startet das eigentliche Umschreiben erst nach Abschluss der Auswertung. Es bezieht sich auf die Liste der Aktionen, die durch Richtlinien identifiziert werden, die als TRUE ausgewertet werden, und startet das Umschreiben. Nach der Implementierung aller Aktionen in der Liste leitet Citrix ADC den Datenverkehr nach Bedarf weiter.

> **Hinweis**:
>
> Stellen Sie sicher, dass die Richtlinien keine widersprüchlichen oder überlappenden Aktionen auf demselben Teil des HTTP-Headers oder -Hauptteils oder TCP-Nutzlast angeben. Wenn ein solcher Konflikt auftritt, tritt Citrix ADC auf eine undefinierte Situation und bricht das Rewrite ab.

Umschreiben von Aktionen

Geben Sie auf der Citrix ADC Appliance die Aktionen an, die ausgeführt werden sollen, z. B. das Hinzufügen, Ersetzen oder Löschen von Text innerhalb des Hauptteils oder Hinzufügen, Ändern

oder Löschen von Kopfzeilen oder Änderungen an der TCP-Nutzlast als Umschreibaktionen. Weitere Informationen zu Rewrite-Aktionen finden Sie unter Konfigurieren einer Rewrite-Aktion.

In der folgenden Tabelle werden die Schritte beschrieben, die Citrix ADC ausführen kann, wenn eine Richtlinie TRUE bewertet.

Aktion	Ergebnis
Einfg	Die für die Richtlinie angegebene Umschreibaktion wird ausgeführt.
NOREWRITE	Die Anfrage oder Antwort wird nicht neu geschrieben. Citrix ADC leitet den Datenverkehr weiter, ohne einen Teil der Nachricht neu zu schreiben.
RESET	Die Verbindung wird auf TCP-Ebene abgebrochen.
DROP	Die Nachricht wird gelöscht.

> **Hinweis**:
>
> Für jede Richtlinie können Sie die Undefaction (Aktion, die ausgeführt wird, wenn die Richtlinie als UNDEFINED ausgewertet wird) als NOREWRITE, RESET oder DROP konfigurieren.

Führen Sie die folgenden Schritte aus, um die Funktion Umschreiben zu verwenden:

- Aktivieren Sie die Funktion auf dem Citrix ADC.
- Definieren Sie Umschreibaktionen.
- Definieren Sie Umschreibrichtlinien.
- Binden Sie die Richtlinien an einen Bindepunkt, um eine Richtlinie in Kraft zu setzen.

Aktivieren des Rewrite-Features

October 5, 2021

Aktivieren Sie die Funktion Umschreiben auf der Citrix ADC Appliance, wenn Sie die HTTP- oder TCP-Anforderungen oder Antworten neu schreiben möchten. Wenn das Feature aktiviert ist, führt Citrix ADC Umschreibaktionen gemäß den angegebenen Richtlinien durch. Weitere Informationen finden Sie unter Funktionsweise von Rewrite.

So aktivieren Sie das Rewrite-Feature mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um das Rewrite-Feature zu aktivieren und die Konfiguration zu überprüfen:

- enable ns feature REWRITE
- show ns feature

Beispiel:

```
> enable ns feature REWRITE
 Done
> show ns feature

        Feature                         Acronym              Status
        -------                         -------              ------
 1)     Web Logging                     WL                   OFF
 2)     Surge Protection                SP                   ON
 .
 .
 .
 1)     Rewrite                         REWRITE              ON
 .
 .
 1)     Citrix ADC Push                  push                 OFF
 Done
<!--NeedCopy-->
```

So aktivieren Sie das Rewrite-Feature mit dem Konfigurationsdienstprogramm

1. Klicken Sie im Navigationsbereich auf **System**, und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie im Detailbereich unter Modi und Features auf **Grundfunktionen konfigurieren**.
3. Aktivieren **Sie im Dialogfeld Grundfunktionen konfigurieren** das Kontrollkästchen Umschreiben, und klicken Sie dann auf **OK**.
4. Klicken Sie im Dialogfeld **Feature (s) aktivieren/deaktivieren** auf **Ja**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das ausgewählte Feature aktiviert wurde.

Konfigurieren einer Rewrite-Aktion

October 8, 2021

> **Warnung**
>
> Die Pattern-Funktion in einer Rewrite-Aktion ist ab Citrix ADC 12.0 Build 56.20 veraltet, und Citrix empfiehlt Ihnen alternativ, den Aktionsparameter Rewrite Search zu verwenden.

Eine Rewrite-Aktion zeigt Änderungen an, die an einer Anfrage oder Antwort vorgenommen wurden, bevor sie an einen Server oder Client gesendet wurden.

Ausdrücke definieren Folgendes:

- Schreiben Sie den Aktionstyp neu.
- Ort der Rewrite-Aktion.
- Schreiben Sie den Aktionskonfiguration neu.

Beispielsweise verwendet eine DELETE-Aktion nur einen Zielausdruck. Eine REPLACE-Aktion verwendet einen Zielausdruck und einen Ausdruck, um den Ersetzungstext zu konfigurieren.

Nachdem Sie die Rewrite-Funktion aktiviert haben, müssen Sie eine oder mehrere Aktionen konfigurieren, es sei denn, eine integrierte Rewrite-Aktion reicht aus. Alle integrierten Aktionen haben Namen, die mit der Zeichenfolge ns_cvpn beginnen, gefolgt von einer Reihe von Buchstaben und Unterstrichen. Integrierte Aktionen führen nützliche und komplexe Aufgaben aus, z. B. das Dekodieren von Teilen einer clientlosen VPN-Anfrage oder Antwort oder das Ändern von JavaScript- oder XML-Daten. Die integrierten Aktionen können angezeigt, aktiviert und deaktiviert werden, können jedoch nicht geändert oder gelöscht werden.

> Hinweis:
>
> Aktionstypen, die nur für HTTP-Umschreibung verwendet werden können, werden in der Spalte **Aktionstyp umschreiben** identifiziert.

Weitere Informationen finden Sie unter **Typenparameter**.

Erstellen Sie eine Rewrite-Aktion mit der Befehlszeilenschnittstelle

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

- `add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-search <expression>] [refineSearch <expression>] [-comment<string>]`
- `show rewrite action <name>`

Weitere Informationen finden Sie in der Tabelle Aktionstypen umschreiben und deren Argumente .

Die Rewrite-Funktion verfügt über die folgenden integrierten Aktionen:

- NOREWRITE - Sendet die Anfrage oder Antwort an den Benutzer, ohne sie neu zu schreiben.

- RESET - Setzt die Verbindung zurück und benachrichtigt den Browser des Benutzers, damit der Benutzer die Anfrage erneut senden kann.
- DROP - Löscht die Verbindung, ohne eine Antwort an den Benutzer zu senden.

Einer der folgenden Flow-Typen ist implizit mit jeder Aktion verknüpft:

- Request - Aktion gilt für die Anfrage.
- Response - Aktion gilt für die Antwort.
- Neutral - Aktion gilt sowohl für Anfragen als auch für Antworten.

Name

Name für die benutzerdefinierte Rewrite-Aktion. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und darf nur Buchstaben, Zahlen und den Bindestrich (-), Punkt (.) Hash (#), Leerzeichen (), Leerzeichen (), bei (@), gleich (=), Doppelpunkt (:) und Unterstriche enthalten. Kann geändert werden, nachdem die Rewrite-Richtlinie hinzugefügt wurde.

Typ-Parameter

Der **Type-Parameter** zeigt den Typ der benutzerdefinierten Rewrite-Aktion an.

Im Folgenden sind die Werte des **Type-Parameters** aufgeführt:

- `REPLACE <target> <string_builder_expr>`. Ersetzt die Zeichenfolge durch den String-Builder-Ausdruck.

Beispiel:

```
> add rewrite action replace_http_act replace http.res.body(100) '"
   new_replaced_data"'
Done
> sh rewrite action replace_http_act
Name: replace_http_act
Operation: replace
Target:http.res.body(100)
Value:"new_replaced_data"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```


- REPLACE_ALL <target> <string_builder_expr1> -(pattern|search)<string_builder_expr>. Ersetzt in der von <target>angegebenen Anforderung oder Antwort alle Vorkommen der <string_builder_expr1> durch definierten Zeichenfolge durch <string_builder_expr2>. Sie können ein PCRE-Formatmuster oder die Suchfunktion verwenden, um die zu ersetzenden Strings zu ermitteln.

Beispiel:

```
> add policy patset pat_list_2
Done
> bind policy patset pat_list_2 ”www.abc.com”
Done
> bind policy patset pat_list_2 ”www.def.com”
Done
> add rewrite action refineSearch_act_31 replace_all ”HTTP.RES.BODY
   (100000)” ””https://””-search ”patset(”pat_list_2”)” -refineSearch ”
   EXTEND(7,0).REGEX_SELECT(re#http://#)”
Done

> sh rewrite action refineSearch_act_31
Name: refineSearch_act_31
Operation: replace_all
Target:HTTP.RES.BODY(100000)
Refine Search:EXTEND(7,0).REGEX_SELECT(re#http://#)
Value:”https://”
Search: patset(”pat_list_2”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- REPLACE_HTTP_RES <string_builder_expr>. Ersetzt die vollständige HTTP-Antwort durch die durch den String-Builder-Ausdruck definierte Zeichenfolge.

Beispiel:

```
> add rewrite action replace_http_res_act replace_http_res '”HTTP/1.1
   200 OK\r\n\r\nSending from ADC”'
 Done
> sh rewrite action replace_http_res_act
```



```
4  Name: replace_http_res_act
5  Operation: replace_http_res
6  Target:”HTTP/1.1 200 OK
7  Sending from ADC”
8  Hits: 0
9  Undef Hits: 0
10 Action Reference Count: 0
11 Done
12
13 <!--NeedCopy-->
```

- REPLACE_SIP_RES <target>. Ersetzt die vollständige SIP-Antwort durch die durch angegebene Zeichenfolge <target>.

Beispiel:

```
1  > add rewrite action replace_sip_res_act replace_sip_res '”HTTP/1.1 200
       OK\r\n\r\nSending from ADC”'
2  Done
3  > sh rewrite action replace_sip_res_act
4  Name: replace_sip_res_act
5  Operation: replace_sip_res
6  Target:”HTTP/1.1 200 OK
7  Sending from ADC”
8  Hits: 0
9  Undef Hits: 0
10 Action Reference Count: 0
11 Done
12
13 <!--NeedCopy-->
```

- INSERT_HTTP_HEADER <header_string_builder_expr> <contents_string_builder_expr>. Fügt den von <header_string_builder_expr> angegebenen HTTP-Header ein und Header-Inhalt angegeben durch <contents_string_builder_expr>.

Beispiel:

```
1  > add rewrite action ins_cip_header insert_http_header ”CIP” ”CLIENT.IP
       .SRC”
2  Done
3  > sh rewrite action ins_cip_header
4  Name: ins_cip_header
5  Operation: insert_http_header
```



```
Target:CIP
Value:CLIENT.IP.SRC
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- DELETE_HTTP_HEADER <target>. Löscht den HTTP-Header, der von angegeben wurde <target>

Beispiel:

```
> add rewrite action del_true_client_ip_header delete_http_header "True-Client-IP"
Done
> sh rewrite action del_true_client_ip_header
Name: del_true_client_ip_header
Operation: delete_http_header
Target:True-Client-IP
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- CORRUPT_HTTP_HEADER <target>. Ersetzt den Header-Namen aller Vorkommen des durch angegebenen HTTP-Headers <target> durch einen beschädigten Namen, so dass er vom Empfänger nicht erkannt wird Beispiel: MY_HEADER wird in MHEY_ADER geändert.

Beispiel:

```
> add rewrite action corrupt_content_length_hdr corrupt_http_header "Content-Length"
Done
> sh rewrite action corrupt_content_length_hdr
Name: corrupt_content_length_hdr
Operation: corrupt_http_header
Target:Content-Length
Hits: 0
Undef Hits: 0
```



```
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_BEFORE <string_builder_expr1> <string_builder_expr1>. Findet die in angegebene Zeichenfolge <string_builder_expr1> und fügt die Zeichenfolge <string_builder_expr2> davor ein.

```
> add rewrite action insert_before_ex_act insert_before http.res.body
   (100) '"Add this string in the starting"'
Done
> sh rewrite action insert_before_ex_act
Name: insert_before_ex_act
Operation: insert_before
Target:http.res.body(100)
Value:"Add this string in the starting"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_BEFORE_ALL <target> <string_builder_expr1> -(pattern|search)<string_builder_expr2>. Sucht in der von <target>angegebenen Anforderung oder Antwort alle Vorkommen der in angegebenen Zeichenfolge <string_builder_expr1> und fügt die <string_builder_expr2> zuvor angegebene Zeichenfolge ein. Sie können ein PCRE-Formatmuster oder die Suchfunktion verwenden, um die Strings zu finden.

Beispiel:

```
> add policy patset pat
 Done
> bind policy patset pat abcd
 Done
> add rewrite action refineSearch_act_1 insert_before_all http.res.body
   (10) 'target.prefix(10) + "refineSearch_testing"' -search patset("
   pat") -refineSearch extend(10,10)
 Done
> sh rewrite action refineSearch_act_1
Name: refineSearch_act_1
```



```
Operation: insert_before_all
Target:http.res.body(10)
Refine Search:extend(10,10)
Value:target.prefix(10) + ”refineSearch_testing”
Search: patset(”pat”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_AFTER <string_builder_expr1> <string_builder_expr2>. Findet die in <string_builder_expr1> angegebene Zeichenfolge und fügt die in <string_builder_expr2> angegebene Zeichenfolge danach ein.

Beispiel:

```
> add rewrite action insert_after_act insert_after http.req.body(100) '
   ”add this string after 100 bytes”'
Done
> sh rewrite action insert_after_act
Name: insert_after_act
Operation: insert_after
Target:http.req.body(100)
Value:”add this string after 100 bytes”
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_AFTER_ALL <target> <string_builder_expr1> -(pattern|search)< string_builder_expr>. Sucht in der von <target>angegebenen Anforderung oder Antwort alle Vorkommen der durch angegebenen Zeichenfolge <string_builder_expr1> und fügt die durch <string_builder_expr2> angegebene Zeichenfolge ein. Sie können ein PCRE-Formatmuster oder die Suchfunktion verwenden, um die Strings zu finden.

Beispiel:


```
> add rewrite action refineSearch_act_2 insert_after_all http.res.body
    (100) '"refineSearch_testing"' -search text("abc") -refineSearch
    extend(0, 10)
Done
> sh rewrite action refineSearch_act_2
Name: refineSearch_act_2
Operation: insert_after_all
Target:http.res.body(100)
Refine Search:extend(0, 10)
Value:"refineSearch_testing"
Search: text("abc")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- `DELETE <target>`. Findet und löscht das angegebene Ziel.

Beispiel:

```
> add rewrite action delete_ex_act delete http.req.header("HDR")
Done
> sh rewrite action delete_ex_act
Name: delete_ex_act
Operation: delete
Target:http.req.header("HDR")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- `DELETE_ALL <target> -(pattern|search)<string_builder_expr>`. In der von `<target>`angegebenen Anforderung oder Antwort sucht und löscht alle Vorkommen der durch angegebenen Zeichenfolge `<string_builder_expr>`. Sie können ein PCRE-Formatmuster oder die Suchfunktion verwenden, um die Strings zu finden.

Beispiel:


```
>add rewrite action refineSearch_act_4 delete_all "HTTP.RES.BODY(50000)
    " -search text("Windows Desktops") -refineSearch "EXTEND(40,40).
    REGEX_SELECT(re#\s`\*`<AppData>.`\*`\s`\*`<\\/AppData>#)"
Done
> show REWRITE action refineSearch_act_4
Name: refineSearch_act_4
Operation: delete_all
Target:HTTP.RES.BODY(50000)
Refine Search:EXTEND(40,40).REGEX_SELECT(re#\s`\*`<AppData>.`\*`\s
    `\*`</AppData>#)
Search: text("Windows Desktops")
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- `REPLACE_DIAMETER_HEADER_FIELD <target> <field value>`. Ändern Sie in der Anforderung oder den Antworten das durch angegebene Kopfzeilenfeld `<target>`. Verwenden Sie `Diameter.req.flags.SET(<flag>)` oder `Diameter.req.flags.UNSET<flag>` wie `stringbuilderexpression`, um Flags zu setzen oder aufzuheben.

Beispiel:

```
> add rewrite action replace_diameter_field_ex_act
    replace_diameter_header_field diameter.req.flags diameter.req.flags.
    set(PROXIABLE)
Done
> sh rewrite action replace_diameter_field_ex_act
Name: replace_diameter_field_ex_act
Operation: replace_diameter_header_field
Target:diameter.req.flags
Value:diameter.req.flags.set(PROXIABLE)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- `REPLACE_DNS_HEADER_FIELD <target>`. In der Anforderung oder Antwort ändert das durch angegebene Header-Feld `<target>`.

Beispiel:

```
> add rewrite action replace_dns_hdr_act replace_dns_header_field dns.
   req.header.flags.set(AA)
Done
> sh rewrite action replace_dns_hdr_act
Name: replace_dns_hdr_act
Operation: replace_dns_header_field
Target:dns.req.header.flags.set(AA)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- `REPLACE_DNS_ANSWER_SECTION <target>`. Ersetzen Sie den DNS-Antwortabschnitt in der Antwort. Dies gilt derzeit nur für A- und AAAA-Datensätze. Verwenden Sie `DNS.NEW_RRSET_A` und `NS.NEW_RRSET_AAAA` Ausdrücke, um den neuen Antwortabschnitt zu konfigurieren.

Beispiel:

```
> add rewrite action replace_dns_ans_act replace_dns_answer_section
   DNS.NEW_RRSET_A("1.1.1.1", 10)
Done
> sh rewrite action replace_dns_ans_act
Name: replace_dns_ans_act
Operation: replace_dns_answer_section
Target:DNS.NEW_RRSET_A("1.1.1.1", 10)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- `CLIENTLESS_VPN_DECODE<target>`. Dekodiert das vom Ziel angegebene Muster Im clientlosen VPN-Format.

Beispiel:


```
> add rewrite action cvpn_decode_act_1 clientless_vpn_decode http.req.
    body(100)
Done
> sh rewrite action cvpn_decode_act_1
Name: cvpn_decode_act_1
Operation: clientless_vpn_decode
Target:http.req.body(100)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- CLIENTLESS_VPN_DECODE_ALL<target>-search<expression>. Dekodiert ALLE durch den Suchparameter angegebenen Muster im clientlosen VPN-Format.

Beispiel:

```
> add rewrite action act1 clientless_vpn_decode_all http.req.body(100)
    -search text(”abcd”)
Done
> sh rewrite action act1
Name: act1
Operation: clientless_vpn_decode_all
Target:http.req.body(100)
Search: text(”abcd”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- CLIENTLESS_VPN_ENCODE<target>. Codiert das von target angegebene Muster im clientlosen VPN-Format.

Beispiel:

```
> add rewrite action cvpn_encode_act_1 clientless_vpn_encode http.req.
    body(100)
Done
> sh rewrite action cvpn_encode_act_1
```



```
Name: cvpn_encode_act_1
Operation: clientless_vpn_encode
Target:http.req.body(100)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- CLIENTLESS_VPN_ENCODE_ALL<target>-search<expression>. Kodiert ALLE Muster angegebenen Suchparameter im clientlosen VPN-Format.

Beispiel:

```
> add rewrite action act2 clientless_vpn_encode_all http.req.body(100)
   -search text(”abcd”)
Done
> sh rewrite action act2
Name: act1
Operation: clientless_vpn_encode_all
Target:http.req.body(100)
Search: text(”abcd”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- CORRUPT_SIP_HEADER<target>. Ersetzt den Header-Namen aller Vorkommen des durch angegebenen SIP-Headers <target> durch einen beschädigten Namen, damit der Empfänger ihn nicht erkennt.

Beispiel:

```
> add rewrite action corrupt_sip_hdr_act corrupt_sip_header SIP_HDR
Done
> sh rewrite action corrupt_sip_hdr_act
Name: corrupt_sip_hdr_act
Operation: corrupt_sip_header
Target:SIP_HDR
Hits: 0
```



```
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- INSERT_SIP_HEADER <header_string_builder_expr> <contents_string_builder_expr>. Fügt den durch angegebenen SIP-Header <header_string_builder_expr> und Header-Inhalt ein, der durch angegeben ist <contents_string_builder_expr>.

Beispiel:

```
> add rewrite action insert_sip_hdr_act insert_sip_header SIP_HDR '"
   inserting_sip_header"'
 Done
>sh rewrite action insert_sip_hdr_act
Name: insert_sip_hdr_act
Operation: insert_sip_header
Target:SIP_HDR
Value:"inserting_sip_header"
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

- DELETE_SIP_HEADER<target>. Löscht den SIP-Header, der von angegeben wurde <target>

Beispiel:

```
> add rewrite action delete_sip_hdr delete_sip_header  SIP_HDR
Done
> sh rewrite action delete_sip_hdr
Name: delete_sip_hdr
Operation: delete_sip_header
Target:SIP_HDR
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```


Target-Parameter

Der Target-Parameter Ist ein Ausdruck, der angibt, welcher Teil der Anforderung oder Antwort neu geschrieben werden soll.

StringBuilderExpr

Der StringBuilderExpr Ist ein Ausdruck, der den Inhalt angibt, der an der angegebenen Stelle in die Anforderung oder Antwort eingefügt werden soll. Dieser Ausdruck ersetzt eine angegebene Zeichenfolge.

Beispiel 1. Einfügen eines HTTP-Headers mit der Client-IP:

```
> add rewrite action insertact INSERT_HTTP_HEADER ”client-IP” CLIENT.IP
    .SRC
Done
> show rewrite action insertact
Name: insertact
Operation: insert_http_header
Target:Client-IP
Value:CLIENT.IP.SRC
BypassSafetyCheck : NO
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Beispiel 2. Strings in einer TCP-Nutzlast ersetzen (TCP Rewrite):

```
> add rewrite action client_tcp_payload_replace_all REPLACE_ALL
  'client.tcp.payload(1000)' '”new-string”' -search text(”old-string”)
Done
> show rewrite action client_tcp_payload_replace_all
Name: client_tcp_payload_replace_all
Operation: replace_all
Target:client.tcp.payload(1000)
Value:”new-string”
Search: text(”old-string”)
BypassSafetyCheck : NO
Hits: 0
```



```
Undef Hits: 0
Action Reference Count: 0
Done
>
<!--NeedCopy-->
```

Suchen Sie einen Teil der Anfrage oder Antwort zum Umschreiben

Die Suchfunktion hilft dabei, alle Instanzen des erforderlichen Musters in der Anfrage oder Antwort zu finden.

Die Suchfunktion muss in den folgenden Aktionstypen verwendet werden:

- INSERT_BEFORE_ALL
- INSERT_AFTER_ALL
- REPLACE_ALL
- DELETE_ALL
- CLIENTLESS_VPN_ENCODE_ALL
- CLIENTLESS_VPN_DECODE_ALL

Die Suchfunktion kann nicht mit den folgenden Aktionstypen verwendet werden:

- INSERT_HTTP_HEADER
- INSERT_BEFORE
- INSERT_AFTER
- REPLACE
- DELETE
- DELETE_HTTP_HEADER
- CORRUPT_HTTP_HEADER
- REPLACE_HTTP_RES
- CLIENTLESS_VPN_ENCODE
- CLIENTLESS_VPN_DECODE
- INSERT_SIP_HEADER
- DELETE_SIP_HEADER
- CORRUPT_SIP_HEADER
- REPLACE_DIAMETER_HEADER_FIELD
- REPLACE_DNS_ANSWER_SECTION
- REPLACE_DNS_HEADER_FIELD
- REPLACE_SIP_RES

Die folgenden Suchtypen werden unterstützt:

- Text - eine literale Zeichenfolge
  Beispiel: -search text (“hello”)

- Regulärer Ausdruck - Muster, das verwendet wird, um mehrere Strings in der Anfrage oder Antwort abzugleichen
  Beispiel: -search regex(re~^hello*~)
- XPATH - Ein XPATH-Ausdruck zur Suche nach XML.
  Beispiel: -search xpath(xp%/a/b%)
- JSON - Ein XPATH-Ausdruck zur Suche nach JSON.
  Beispiel: -search xpath_json(xp%/a/b%)
  HTML - Ein XPATH-Ausdruck zur Suche nach HTML
  Beispiel: -search xpath_html(xp%/html/body%)
  Patset - Dies durchsucht alle Muster, die an die Patset-Entität gebunden sind.
  Beispiel: -search patset(“patset1”)
- Datset - Dies durchsucht alle Muster, die an die Datset-Entität gebunden sind.
  Beispiel Suchdatensatz (“dataset1”)
- AVP - AVP-Nummer, die verwendet wird, um mehrere AVPs in einer Durchmesser-/Radius-Nachricht abzugleichen
  Beispiel: -search avp(999)

Verfeinern Sie die Suchergebnisse

Sie können die Funktion “Suche eingrenzen” verwenden, um die zusätzlichen Kriterien für die Verfeinerung der Suchergebnisse anzugeben. Die Funktion “Suche eingrenzen” kann nur verwendet werden, wenn die Suchfunktion verwendet wird.
Der Suchparameter “Verfeinern” beginnt immer mit der Operation “erweitern (m, n)”, wobei ‘m’ eine Anzahl von Bytes links vom Suchergebnis angibt und ‘n’ eine Anzahl von Bytes rechts vom Suchergebnis angibt, um den ausgewählten Bereich zu erweitern.

Wenn die konfigurierte Rewrite-Aktion lautet:

```
1 > add rewrite action test_refine_search replace_all http.res.body(10) '
    ” testing_refine_search” ' -search text(”abc”) -refineSearch extend
    (1,1)
2 And the HTTP response body is abcxxxx456.
3
4 <!--NeedCopy-->
```

Dann findet der Suchparameter das Muster “abc” und da der RefineSearch-Parameter auch so konfiguriert ist, dass er ein zusätzliches 1 Byte links und ein zusätzliches Byte rechts vom übereinstimmenden Muster überprüft. Der resultierende ersetzte Text ist: abcx. Die Ausgabe dieser Aktion ist also `testing_refine_searchxxx456`.

Beispiel 1: Verwenden der Suchfunktion Verfeinern im Aktionstyp INSERT_BEFORE_ALL.


```
> add policy patset pat
Done
> bind policy patset pat abcd
Done
> add rewrite action refineSearch_act_1 insert_before_all http.res.body
    (10) 'target.prefix(10) + ”refineSearch_testing”' -search patset(”
    pat”) -refineSearch extend(10,10)
Done
> sh rewrite action refineSearch_act_1
Name: refineSearch_act_1
Operation: insert_before_all
Target:http.res.body(10)
Refine Search:extend(10,10)
Value:target.prefix(10) + ”refineSearch_testing”
Search: patset(”pat”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Beispiel 2: Verwenden der Suchfunktion “Suche eingrenzen” im Aktionstyp INSERT_AFTER_ALL.

```
> add rewrite action refineSearch_act_2 insert_after_all http.res.body
    (100) '”refineSearch_testing”' -search text(”abc”) -refineSearch
    extend(0, 10)
Done
> sh rewrite action refineSearch_act_2
Name: refineSearch_act_2
Operation: insert_after_all
Target:http.res.body(100)
Refine Search:extend(0, 10)
Value:”refineSearch_testing”
Search: text(”abc”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```


Beispiel 3: Verwenden der Suchfunktion Verfeinern im Aktionstyp REPLACE_ALL.

```
> add policy patset pat_list_2
Done
> bind policy patset pat_list_2 ”www.abc.com”
Done
> bind policy patset pat_list_2 ”www.def.com”
Done
> add rewrite action refineSearch_act_31 replace_all ”HTTP.RES.BODY
    (100000)” ””https://”” -search ”patset(”pat_list_2”)” -refineSearch
    ”EXTEND(7,0).REGEX_SELECT(re#http://#)”
Done
> sh rewrite action refineSearch_act_31
Name: refineSearch_act_31
Operation: replace_all
Target:HTTP.RES.BODY(100000)
Refine Search:EXTEND(7,0).REGEX_SELECT(re#http://#)
Value:”https://”
Search: patset(”pat_list_2”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Beispiel 4: Verwenden der Suchfunktion “Suche eingrenzen” im Aktionstyp DELETE_ALL.

```
>add rewrite action refineSearch_act_4 delete_all ”HTTP.RES.BODY(50000)
    ” -search text(”Windows Desktops”) -refineSearch ”EXTEND(40,40).
    REGEX_SELECT(re#\s*<AppData>.\*\s\*<\\/AppData>#)”
> show REWRITE action refineSearch_act_4
Name: refineSearch_act_4
Operation: delete_all
Target:HTTP.RES.BODY(50000)
Refine Search:EXTEND(40,40).REGEX_SELECT(re#\s*<AppData>.\*\s\*</
    AppData>#)
Search: text(”Windows Desktops”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done
```



```
12 >
13 <!--NeedCopy-->
```

Beispiel 5: Verwenden der Funktion “Suche eingrenzen” im Aktionstyp CLIENTLESS_VPN_ENCODE_ALL.

”’

```
add rewrite action act2 clientless_vpn_encode_all http.req.body(100) -search text(“abcd”)
Done
sh rewrite action act2
Name: act1
Operation: clientless_vpn_encode_all
Target:http.req.body(100)
Search: text(“abcd”)
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done
”’
```

Beispiel 6: Verwenden der Funktion “Suche eingrenzen” im Aktionstyp CLIENTLESS_VPN_DECODE_ALL.

```
1  > add rewrite action act1 clientless_vpn_decode_all http.req.body(100)
       -search text(”abcd”)
2  Done
3  > sh rewrite action act1
4  Name: act1
5  Operation: clientless_vpn_decode_all
6  Target:http.req.body(100)
7  Search: text(”abcd”)
8  Hits: 0
9  Undef Hits: 0
10 Action Reference Count: 0
11 Done
12 >
13 <!--NeedCopy-->
```

Ändern Sie eine vorhandene Rewrite-Aktion mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine vorhandene Rewrite-Aktion zu ändern und die Konfiguration zu überprüfen:

- `set rewrite action <name> [-target<expression>] [-stringBuilderExpr<expression>] [-pattern<expression> | -search <expression>] [-refineSearch <expression>] [-comment<string>]`
- `show rewrite action <name>`

Beispiel:

```
> set rewrite action insertact -target ”Client-IP”
 Done
> show rewrite action insertact

Name: insertact
Operation: insert_http_header   Target:Client-IP
Value:CLIENT.IP.SRC
Hits: 0
Undef Hits: 0
Action Reference Count: 0
Done

<!--NeedCopy-->
```

Entfernen Sie eine Rewrite-Aktion mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Rewrite-Aktion zu entfernen:

```
rm rewrite action <name>
```

Beispiel:

```
> rm rewrite action insertact
Done

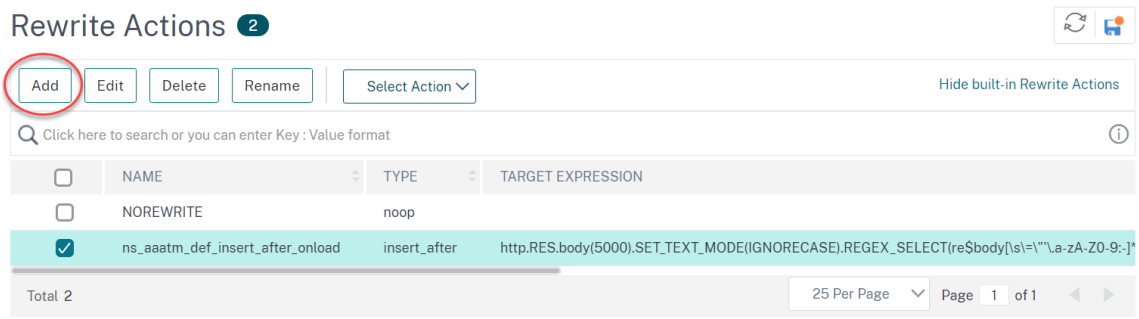
<!--NeedCopy-->
```

Konfigurieren Sie eine Rewrite-Aktion mit dem Konfigurationsdienstprogramm

1. Gehen Sie zu **AppExpert > Rewrite > Actions**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine Aktion zu erstellen, klicken Sie auf **Hinzufügen**.

- Um eine vorhandene Aktion zu ändern, wählen Sie die Aktion aus, und klicken Sie dann auf **Bearbeiten**.

3. Klicken Sie auf **Erstellen** oder **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Aktion erfolgreich konfiguriert wurde.
4. Wiederholen Sie die Schritte 2 bis 4, um beliebig viele Umschreibungsaktionen zu erstellen oder zu ändern.
5. Klicken Sie auf **Schließen**.



Fügen Sie mithilfe des Dialogfelds Ausdruck hinzufügen einen Ausdruck hinzu

1. Klicken Sie im Dialogfeld **Rewrite-Aktion erstellen** oder **Rewrite-Aktion konfigurieren** unter dem Textbereich für das einzugebende Typargument auf **Hinzufügen**.
2. Wählen **Sie im Dialogfeld Ausdruck hinzufügen** im ersten Listenfeld den ersten Begriff für Ihren Ausdruck aus.
   - HTTP. Das HTTP-Protokoll. Wählen Sie diese Option, wenn Sie einen Aspekt der Anforderung untersuchen möchten, der sich auf das HTTP-Protokoll bezieht.
   - SYS. Die geschützten Websites. Wählen Sie diese Option, wenn Sie einen Aspekt der Anfrage untersuchen möchten, der sich auf den Empfänger der Anfrage bezieht.
   - CLIENT. Der Computer, der die Anfrage gesendet hat. Wählen Sie diese Option aus, wenn Sie einen Aspekt des Absenders der Anfrage untersuchen möchten.

Wenn Sie Ihre Wahl treffen, werden im Listenfeld ganz rechts geeignete Begriffe für den nächsten Teil Ihres Ausdrucks aufgeführt.

1. Wählen Sie im zweiten Listenfeld den zweiten Begriff für Ihren Ausdruck aus. Die Auswahl hängt davon ab, welche Wahl Sie im vorherigen Schritt getroffen haben, und sind dem Kontext angemessen. Nachdem Sie Ihre zweite Wahl getroffen haben, wird im Hilfefenster unterhalb des Fensters “Ausdruck konstruieren” (das leer war) eine Hilfe zur Beschreibung des Zwecks

und der Verwendung des gerade gewählten Begriffs angezeigt.

2. Fahren Sie fort, Begriffe aus den Listenfeldern auszuwählen, die rechts neben dem vorherigen Listenfeld angezeigt werden, oder geben Sie Zeichenfolgen oder Zahlen in die Textfelder ein, die Sie zur Eingabe eines Werts auffordern, bis der Ausdruck beendet ist.
   Weitere Informationen zur Sprache der PI-Ausdrücke und zum Erstellen von Ausdrücken für Responder-Richtlinien finden Sie unter "Richtlinien und Ausdrücke. "

Wenn Sie die Wirkung einer Umschreibaktion testen möchten, wenn sie auf HTTP-Beispieldaten verwendet wird, können Sie den Ausdrucksauswertungsauswerter umschreiben verwenden.

TCP-Nutzlasten umschreiben

Zielausdrücke in Aktionen für TCP-Rewrite müssen mit einem der folgenden Ausdruckspräfixe beginnen:

- **CLIENT.TCP.PAYLOAD.** Zum Umschreiben von TCP-Nutzlasten in Clientanfragen. Zum Beispiel CLIENT.TCP.PAYLOAD(10000).AFTER_STR("string1").
- **SERVER.TCP.PAYLOAD.** Zum Umschreiben von TCP-Nutzlasten in Serverantworten. Zum Beispiel SERVER.TCP.PAYLOAD(1000).B64DECODE.BETWEEN("string1","string2").

Bewerten Sie eine Rewrite-Aktion mithilfe des Dialogfelds Aktions-Evaluator umschreiben

1. Wählen Sie im Detailbereich **Aktionen umschreiben** die Rewrite-Aktion aus, die Sie auswerten möchten, und klicken Sie dann auf **Auswerten**.
2. Geben Sie im Dialogfeld Expression Evaluator umschreiben Werte für die folgenden Parameter an. (Ein Sternchen gibt einen erforderlichen Parameter an.)

   Rewrite Action (Rewrite Action) — Wenn die neu zu bewertende Aktion noch nicht ausgewählt ist, wählen Sie sie aus der Dropdownliste aus. Nachdem Sie eine Aktion "Umschreiben" ausgewählt haben, werden im Abschnitt Details die Details der ausgewählten Aktion "Umschreiben" angezeigt.
   Neu — Wählen Sie Neu aus, um das Dialogfeld "Rewrite-Aktion erstellen" zu öffnen und eine Neuschreibaktion zu erstellen.
   Ändern — Wählen Sie Ändern aus, um das Dialogfeld "Rewrite-Aktion konfigurieren" zu öffnen und die ausgewählte Neuschreibaktion zu ändern.
   Flow-Typ — Gibt an, ob die ausgewählte Rewrite-Aktion mit HTTP-Anforderungsdaten oder HTTP-Antwortdaten getestet werden soll. Der Standardwert ist Request. Wenn Sie mit Antwortdaten testen möchten, wählen Sie Antwort aus.
   HTTP-Anforderung/Antwortdaten* — Dient zur Bereitstellung der HTTP-Daten, die der Rewrite Action Evaluator zum Testen verwendet wird. Sie können die Daten direkt in das Fenster

einfügen oder auf Sample klicken, um einige Beispiel-HTTP-Header einzufügen.
Zeilenende anzeigen — Gibt an, ob End-of-Line-Zeichen (\ n) im Unix-Stil am Ende jeder Zeile von HTTP-Beispieldaten angezeigt werden sollen.
Beispiel — Fügt Beispiel-HTTP-Daten in das Fenster “HTTP-Request/Response Data” ein. Sie können entweder GET- oder POST-Daten wählen.
Durchsuchen — Öffnet ein lokales Suchfenster, in dem Sie eine Datei mit Beispiel-HTTP-Daten von einem lokalen oder Netzwerkspeicherort auswählen können.
Clear—Löscht die aktuellen Beispiel-HTTP-Daten aus dem Fenster “HTTP-Request/Response Data”.

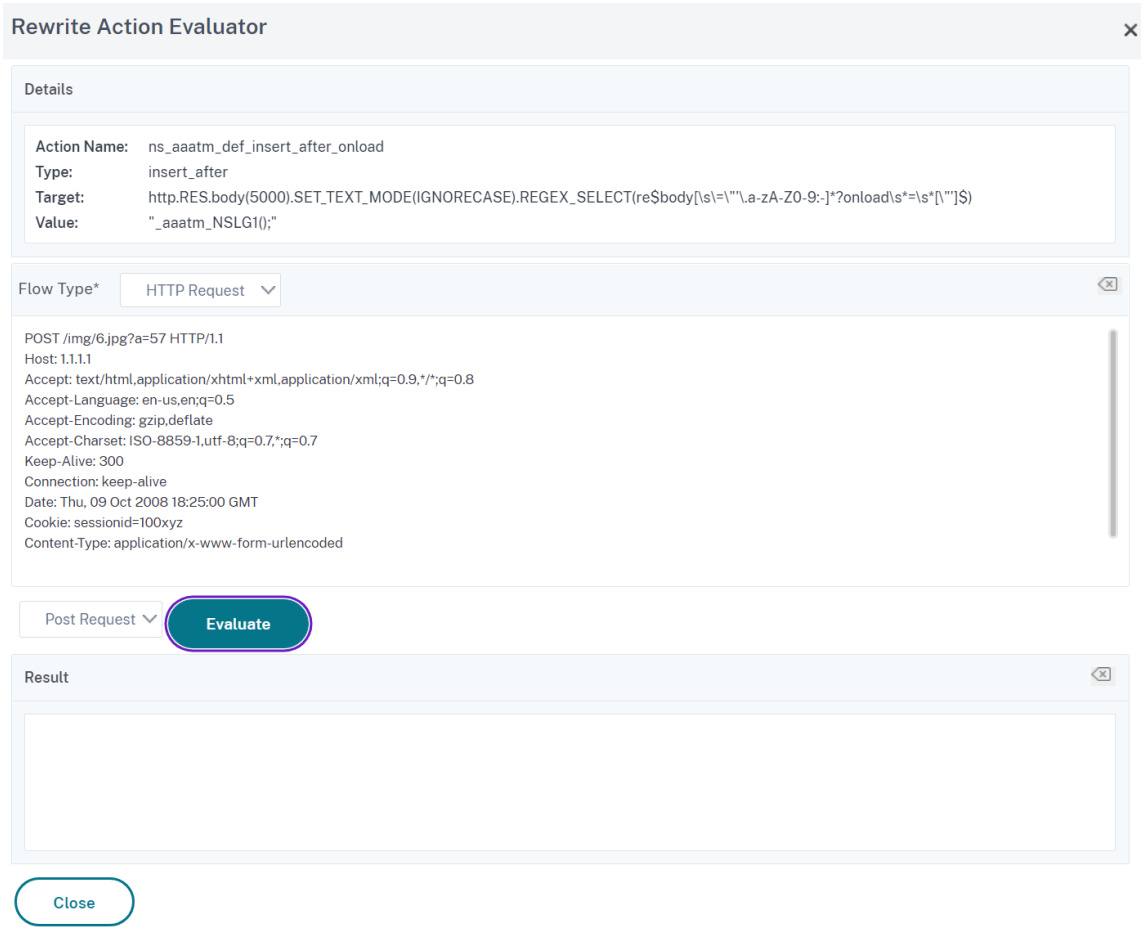
3. Klicken Sie auf Bewerten. Der **Auswertungsprogramm “Aktion umschreiben** “ wertet die Auswirkung der Aktion “Umschreiben” auf die ausgewählten Beispieldaten aus und zeigt die Ergebnisse an, die durch die ausgewählte Aktion “ **Umschreiben** “ im Fenster **Ergebnisse** geändert wurden. Hinzufügungen und Löschungen werden wie in der Legende in der unteren linken Ecke des Dialogfelds angegeben hervorgehoben.

4. Evaluieren Sie Rewrite-Aktionen weiter, bis Sie festgestellt haben, dass alle Ihre Aktionen die gewünschte Wirkung haben.

    - Sie können die ausgewählte Rewrite-Aktion ändern und die geänderte Version testen, indem Sie auf **Ändern** klicken, um das Dialogfeld **Rewrite-Aktion konfigurieren** zu öffnen, Ihre Änderungen vorzunehmen und zu speichern, und dann erneut auf Auswerten klicken.
    - Sie können eine andere Umschreibaktion mit denselben Anforderungs- oder Antwortdaten auswerten, indem Sie sie in der Dropdownliste **Aktion neu schreiben** auswählen und dann erneut auf **Auswerten** klicken.

5. Klicken Sie auf **Schließen**, um das Auswertungsprogramm **Expression umschreiben** zu schließen und zum Bereich **Aktionen umschreiben** zurückzukehren.

6. Um eine Rewrite-Aktion zu löschen, wählen Sie die Rewrite-Aktion aus, die Sie löschen möchten, klicken Sie dann auf **Entfernen** und bestätigen Sie bei Aufforderung Ihre Auswahl, indem Sie auf **OK** klicken.



Konfigurieren einer Rewrite-Richtlinie

October 5, 2021

Nachdem Sie eine erforderliche Rewrite-Aktion erstellt haben, müssen Sie mindestens eine Rewrite-Richtlinie erstellen, um die Anforderungen auszuwählen, die die Citrix ADC-Appliance neu schreiben soll.

Eine Rewrite-Richtlinie besteht aus einer Regel, die selbst aus einem oder mehreren Ausdrücken besteht. Und eine zugehörige Aktion, die ausgeführt wird, wenn eine Anfrage oder Antwort mit der Regel übereinstimmt. Richtlinienregeln für die Auswertung von HTTP-Anfragen und -Antworten können auf fast jedem Teil einer Anfrage oder Antwort basieren.

Sie können keine TCP-Rewrite-Aktionen verwenden, um andere Daten als die TCP-Nutzlast neu zu schreiben. Sie können die Richtlinienregeln für TCP-Rewrite-Richtlinien auf die Informationen in der Transportschicht stützen. Und die Schichten unter der Transportschicht.

Wenn eine konfigurierte Regel mit einer Anforderung oder Antwort übereinstimmt, wird die

entsprechende Richtlinie ausgelöst und die zugeordnete Aktion wird ausgeführt.

> **Hinweis:**
> Sie können entweder die Befehlszeilenschnittstelle oder das Konfigurationsdienstprogramm verwenden, um Rewrite-Richtlinien zu erstellen und zu konfigurieren. Benutzer, die mit der Befehlszeilenschnittstelle und der Ausdruckssprache der Citrix ADC Policy nicht genau vertraut sind, werden die Verwendung des Konfigurationsdienstprogramms normalerweise viel einfacher finden.

So fügen Sie eine neue Rewrite-Richtlinie mit der Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine neue Rewrite-Richtlinie hinzuzufügen und die Konfiguration zu überprüfen:

- <add rewrite policy <name> <expression> <action> [<undefaction>]
- <show rewrite policy <name>

Beispiel 1. Umschreiben von HTTP-Inhalten:

```
> add rewrite policy policyNew ”HTTP.RES.IS_VALID” insertact NOREWRITE
 Done
> show rewrite policy policyNew
        Name: policyNew
        Rule: HTTP.RES.IS_VALID
        RewriteAction: insertact
        UndefAction: NOREWRITE
        Hits: 0
        Undef Hits: 0

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

Beispiel 2. Umschreiben einer TCP-Nutzlast (TCP Rewrite):

```
> add rewrite policy client_tcp_payload_policy CLIENT.IP.SRC.EQ
    (172.168.12.232) client_tcp_payload_replace_all
 Done
> show rewrite policy client_tcp_payload_policy
        Name: client_tcp_payload_policy
        Rule: CLIENT.IP.SRC.EQ(172.168.12.232)
        RewriteAction: client_tcp_payload_replace_all
        UndefAction: Use Global
```



```
        LogAction: Use Global
        Hits: 0
        Undef Hits: 0

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

So ändern Sie eine vorhandene Rewrite-Richtlinie mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine vorhandene Rewrite-Richtlinie zu ändern und die Konfiguration zu überprüfen:

- <set rewrite policy <name>-rule <expression-action <action> [<undefaction>]
- <show rewrite policy <name>

Beispiel:

```
> set rewrite policy policyNew -rule ”HTTP.RES.IS_VALID” -action
   insertaction
 Done

> show rewrite policy policyNew
        Name: policyNew
        Rule: HTTP.RES.IS_VALID
        RewriteAction: insertaction
        UndefAction: NOREWRITE
        Hits: 0
        Undef Hits: 0

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

So entfernen Sie eine Rewrite-Richtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine Rewrite-Richtlinie zu entfernen:

rm rewrite policy <name>

Beispiel:


```
> rm rewrite policy policyNew
Done
<!--NeedCopy-->
```

So konfigurieren Sie eine Rewrite-Richtlinie mit dem Konfigurationsdienstprogramm

1. Gehen Sie zu **AppExpert > Rewrite > Policies**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine Richtlinie zu erstellen, klicken Sie auf Hinzufügen.
   - Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf Öffnen.
3. Klicken Sie auf **Erstellen** oder **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich konfiguriert wurde.
4. Wiederholen Sie die Schritte 2 bis 4, um beliebig viele Umschreibungsaktionen zu erstellen oder zu ändern.
5. Klicken Sie auf **Schließen**. Um eine Neuschreibrichtlinie zu löschen, wählen Sie die zu löschende Umschreibungsrichtlinie aus, klicken Sie auf **Entfernen**, und bestätigen Sie, wenn Sie dazu aufgefordert werden, Ihre Auswahl durch Klicken auf **OK**zu bestätigen.

Erstellen Sie Umschreibrichtlinien für Content-Sicherheits-Header, XSS-Schutz, HSTS, X-Content-Typ-Optionen und Content-Security-Policy

Geben Sie an der Eingabeaufforderung die folgenden Rewrite-Aktionsbefehle ein, um den Sicherheitskopf zu Webseiten hinzuzufügen, die über NetScaler mit Rewrites bereitgestellt werden.

```
add rewrite action insert_STS_header insert_http_header Strict-
    Transport-Security ””max-age=157680000””
add rewrite action rw_act_insert_XSS_header insert_http_header X-Xss-
    Protection ””1; mode=block””
add rewrite action rw_act_insert_Xcontent_header insert_http_header X-
    Content-Type-Options ””nosniff””
add rewrite action rw_act_insert_Content_security_policy
    insert_http_header Content-Security-Policy ””default-src 'self' ;
    script-src 'self' 'unsafe-inline' 'unsafe-eval' ; style-src 'self' '
    unsafe-inline' 'unsafe-eval'; img-src 'self' data:””
<!--NeedCopy-->
```

Geben Sie an der Eingabeaufforderung die folgenden Richtlinienbefehle zum Umschreiben ein,

um den Sicherheitskopf zu Webseiten hinzuzufügen, die über NetScaler mithilfe von Rewrites bereitgestellt werden

```
add rewrite policy enforce_STS true insert_STS_header
add rewrite policy rw_pol_insert_XSS_header "HTTP.RES.HEADER("X-Xss-Protection").EXISTS.NOT" rw_act_insert_XSS_header
add rewrite policy rw_pol_insert_XContent TRUE rw_act_insert_Xcontent_header
add rewrite policy rw_pol_insert_Content_security_policy TRUE rw_act_insert_Content_security_policy
<!--NeedCopy-->
```

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um Richtlinien mit Hilfe von Gehe zu Ausdruck NEXT an den virtuellen Server zu binden.

```
bind vpn vserver access -policy enforce_STS -priority 100 -gotoPriorityExpression NEXT -type RESPONSE
bind vpn vserver "VSERVERNAME" -policy rw_pol_insert_XSS_header -priority 110 -gotoPriorityExpression NEXT -type RESPONSE
bind vpn vserver access -policy rw_pol_insert_XContent -priority 120 -gotoPriorityExpression NEXT -type RESPONSE
bind vpn vserver access -policy rw_pol_insert_Content_security_policy -priority 130 -gotoPriorityExpression NEXT -type RESPONSE
<!--NeedCopy-->
```

Konfigurieren Sie die Umschreibungsrichtlinie für Content-Security-Header, XSS-Schutz, HSTS, X-Content-Typ-Optionen und Content-Security-Policy mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **AppExpert** > **Umschreiben** > **Aktionen**
2. Klicken Sie auf **Hinzufügen**, um Umschreibaktionen für jeden der Header zu erstellen.
3. Navigieren Sie zu **AppExpert** > **Umschreiben** > **Richtlinien**
4. Klicken Sie auf **Hinzufügen**, um Rewrite-Richtlinien zu erstellen und sie mit Aktionen zu verknüpfen.
5. Binden Sie Richtlinien an den virtuellen Server bei der Antwort mit dem Gehe zu Ausdruck **NEXT**.

> **Hinweis:**
> In SSLVPN müssen wir die folgende Content-Security-Aktion verwenden:


```
1 add rewrite action Rewrite_Insert_Content-Security-Policy
    insert_http_header Content-Security-Policy ""default-src 'self' ;
    script-src 'self' 'unsafe-inline' 'unsafe-eval' ; style-src 'self' '
    unsafe-inline' 'unsafe-eval'; img-src 'self' http://localhost:* data
    :;"
2 <!--NeedCopy-->
```

Die Localhost-Ausnahme ist erforderlich, da der Browser die Cookie/GW-Informationen mithilfe des HTTP-Aufrufs localhost an das Plug-In weitergibt. Da der CSP nur “selbst” hatte, wären nur Anrufe an den virtuellen Server zulässig.

Binden einer Umschreibungsrichtlinie

October 5, 2021

Nachdem Sie eine Richtlinie zum Umschreiben erstellt haben, müssen Sie sie binden, um sie in Kraft zu setzen. Sie können Ihre Richtlinie an Global binden, wenn Sie sie auf den gesamten Datenverkehr anwenden möchten, der Ihren Citrix ADC durchläuft, oder Sie können Ihre Richtlinie an einen bestimmten virtuellen Server oder einen Bindepunkt binden, um nur den eingehenden Datenverkehr des virtuellen Servers oder des Bindpunkts an diese Richtlinie weiterzuleiten. Wenn eine eingehende Anforderung mit einer Umschreibrichtlinie übereinstimmt, wird die dieser Richtlinie zugeordnete Aktion ausgeführt.

Rewrite-Richtlinien für die Auswertung von HTTP-Anforderungen und -Antworten können an virtuelle Server vom Typ HTTP oder SSL gebunden sein oder an die Bindpunkte REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE und RES_DEFAULT gebunden werden. Rewrite-Richtlinien für TCP-Neuschreiben können nur an virtuelle Server vom Typ TCP oder SSL_TCP oder an die Bindpunkte OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, OTHERTCP_RES_OVERRIDE und OTHERTCP_RES_DEFAULT gebunden werden.

Hinweis: Der Begriff OTHERTCP wird im Kontext der Citrix ADC Appliance verwendet, um auf alle TCP- oder SSL_TCP-Anforderungen und -Antworten zu verweisen, die Sie als Rohdatenstrom von Bytes behandeln möchten, unabhängig von den Protokollen, die die TCP-Pakete kapseln.

Wenn Sie eine Richtlinie binden, weisen Sie ihr eine Priorität zu. Die Priorität bestimmt die Reihenfolge, in der die von Ihnen definierten Richtlinien ausgewertet werden. Sie können die Priorität auf eine beliebige positive Ganzzahl festlegen.

Im Citrix ADC Betriebssystem funktionieren Richtlinienprioritäten in umgekehrter Reihenfolge - je höher die Zahl, desto niedriger die Priorität. Wenn Sie beispielsweise drei Richtlinien mit den Prioritäten 10, 100 und 1000 haben, wird zuerst die Richtlinie angewendet, die die Priorität 10 zugewiesen

hat, dann wird die Richtlinie mit der Priorität 100 und schließlich der Richtlinie eine Reihenfolge von 1000 zugewiesen.

Im Gegensatz zu den meisten anderen Features des Citrix ADC Betriebssystems werden Richtlinien durch das Rewrite-Feature weiter ausgewertet und implementiert, nachdem eine Anforderung mit einer Richtlinie übereinstimmt. Die Auswirkungen einer bestimmten Aktionsrichtlinie auf eine Anforderung oder Antwort sind jedoch oft unterschiedlich, je nachdem, ob sie vor oder nach einer anderen Aktion ausgeführt wird. Priorität ist wichtig, um die gewünschten Ergebnisse zu erhalten.

Sie können sich viel Platz lassen, um andere Richtlinien in beliebiger Reihenfolge hinzuzufügen und sie dennoch in der gewünschten Reihenfolge auszuwerten, indem Sie Prioritäten mit Intervallen von 50 oder 100 zwischen jeder Richtlinie festlegen, wenn Sie sie binden. In diesem Fall können Sie jederzeit zusätzliche Richtlinien hinzufügen, ohne die Priorität einer vorhandenen Richtlinie neu zuweisen zu müssen.

Wenn Sie eine Umschreibungsrichtlinie binden, haben Sie auch die Möglichkeit, der Richtlinie einen goto-Ausdruck (gotoPriorityExpression) zuzuweisen. Ein goto-Ausdruck kann eine beliebige positive Ganzzahl sein, die der Priorität entspricht, die einer anderen Richtlinie zugewiesen ist, die eine höhere Priorität hat als die Richtlinie, die den goto-Ausdruck enthält. Wenn Sie einer Richtlinie einen goto-Ausdruck zuweisen und eine Anforderung oder Antwort mit der Richtlinie übereinstimmt, wird der Citrix ADC sofort zu der Richtlinie geleitet, deren Priorität mit dem goto-Ausdruck übereinstimmt. Es überspringt alle Richtlinien mit Prioritätsnummern, die niedriger sind als die der aktuellen Richtlinie, aber höher als die Prioritätsnummer des goto-Ausdrucks und wertet diese Richtlinien nicht aus.

So binden Sie eine Umschreibungsrichtlinie global mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Umschreibungsrichtlinie global zu binden und die Konfiguration zu überprüfen:

- `bind rewrite global <policyName> <priority> [<gotoPriorityExpression>] [-type <type>] [-invoke (<labelType> <labelName>)]`
- `show rewrite global`

Beispiel:

```
>bind rewrite global policyNew 10
 Done

> show rewrite global
1)      Global bindpoint: RES_DEFAULT
        Number of bound policies: 1

2)      Global bindpoint: REQ_OVERRIDE
```



```
        Number of bound policies: 1

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

So binden Sie Rewrite-Richtlinie mit der Befehlszeilenschnittstelle an einen bestimmten virtuellen Server

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

- `bind lb vserver <name>@ (<serviceName>@ [-weight <positive_integer>])| <serviceGroupName>@ | (-policyName <string>@ [-priority <positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST | RESPONSE )] [-invoke (<labelType> <labelName>)] )`
- `show lb vserver <name>`

Beispiel:

```
> bind lb vserver lbvip -policyName ns_cmp_msapp -priority 50
 Done
>
> show lb vserver lbvip
        lbvip (8.7.6.6:80) - HTTP       Type: ADDRESS
        State: DOWN
        Last state change was at Wed Jul 15 05:54:24 2009 (+226 ms)
        Time since last state change: 28 days, 01:57:26.350
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

1)      Policy : ns_cmp_msapp Priority:50
2)      Policy : cf-pol Priority:1      Inherited
```



```
25   Done
26 <!--NeedCopy-->
```

So binden Sie eine Umschreibungsrichtlinie mit dem Konfigurationsdienstprogramm an einen Bindungspunkt

1. Navigieren Sie zu **AppExpert** >**Umschreiben** > **Richtlinien**.
2. Wählen Sie im Detailbereich die Umschreibungsrichtlinie aus, die global gebunden werden soll, und klicken Sie dann auf **Richtlinien-Manager**.
3. Führen Sie im Dialogfeld **Richtlinien-Manager neu schreiben** im Menü **Bindpunkte** eine der folgenden Aktionen aus:
   a) Wenn Sie Bindungen für HTTP-Umschreibrichtlinien konfigurieren möchten, klicken Sie auf **HTTP**, und klicken Sie dann entweder auf **Anforderung**oder **Antwort**, je nachdem, ob Sie anforderungsbasierte Umschreibrichtlinien oder Antwortrichtlinien konfigurieren möchten.
   b) Wenn Sie Bindungen für TCP-Rewrite-Richtlinien konfigurieren möchten, klicken Sie auf **TCP**, und klicken Sie dann entweder auf **Client**oder **Server**, je nachdem, ob Sie clientseitige TCP-Rewrite-Richtlinien oder serverseitige TCP-Rewrite-Richtlinien konfigurieren möchten.
4. Klicken Sie auf den Bindepunkt, an den Sie die Umschreibungsrichtlinie binden möchten. Im Dialogfeld **Richtlinien-Manager** umschreiben werden alle Umschreibrichtlinien angezeigt, die an den ausgewählten Bindepunkt gebunden sind.
5. Klicken Sie auf **Richtlinie einfügen**, um eine neue Zeile einzufügen und eine Dropdownliste mit allen verfügbaren, ungebundenen Umschreibrichtlinien anzuzeigen.
6. Klicken Sie auf die Richtlinie, die Sie an den Bindepunkt binden möchten. Die Richtlinie wird in die Liste der Umschreibrichtlinien eingefügt, die an den Bindepunkt gebunden sind.
7. In der Spalte **Priorität** können Sie die Priorität in eine beliebige positive Ganzzahl ändern. Weitere Informationen zu diesem Parameter finden Sie unter Priorität unter Parameter zum Binden einer Umschreibungsrichtlinie.
8. Wenn Sie Richtlinien überspringen und direkt zu einer bestimmten Richtlinie wechseln möchten, falls die aktuelle Richtlinie übereinstimmt, ändern Sie den Wert in der Spalte Gehe zu Ausdruck so, dass er der Priorität der nächsten anzuwendenden Richtlinie entspricht. Weitere Informationen zu diesem Parameter finden Sie unter gotoPriorityExpression unter Parameter zum Binden einer Rewrite-Richtlinie.
9. Um eine Richtlinie zu ändern, klicken Sie auf die Richtlinie und dann auf **Richtlinie ändern**.
10. Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf die Richtlinie, und klicken Sie dann auf **Richtlinie aufheben**.
11. Um eine Aktion zu ändern, klicken Sie in der Spalte Aktion auf die Aktion, die Sie ändern möchten, und klicken Sie dann auf **Aktion ändern**.

12. Um eine Aufrufbezeichnung zu ändern, klicken Sie in der Spalte **Invoke** auf die Aufrufbezeichnung, die Sie ändern möchten, und klicken Sie dann auf **Aufrufbezeichnung ändern**.
13. Um die Prioritäten aller Richtlinien neu zu generieren, die an den derzeit konfigurierten Bindungspunkt gebunden sind, klicken Sie auf **Prioritäten neu generieren**. Die Richtlinie behält ihre bestehenden Prioritäten im Verhältnis zu den anderen Richtlinienbereichen bei, aber die Prioritäten werden in Vielfaches von zehn umnummeriert.
14. Klicken Sie auf **Änderungen übernehmen**.
15. Klicken Sie auf **Schließen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich konfiguriert wurde.

So binden Sie eine Umschreibungsrichtlinie mit dem Konfigurationsdienstprogramm an einen bestimmten virtuellen Server

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Wählen Sie in der Detailliste der virtuellen Server den virtuellen Server aus, an den Sie die Richtlinie zum Umschreiben binden möchten, und klicken Sie dann auf **Öffnen**.
3. Wählen **Sie im Dialogfeld Virtuellen Server konfigurieren (Load Balancing)** die Registerkarte **Richtlinien** aus. Alle auf Ihrem Citrix ADC konfigurierten Richtlinien werden in der Liste angezeigt.
4. Aktivieren Sie das Kontrollkästchen neben dem Namen der Richtlinie, die Sie an diesen virtuellen Server binden möchten.
5. Klicken Sie auf **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich konfiguriert wurde.

Konfigurieren von Richtlinienbeschriftungen für Umschreiben

October 5, 2021

Wenn Sie eine komplexere Richtlinienstruktur erstellen möchten, als von einzelnen Richtlinien unterstützt wird, können Sie Richtlinienbeschriftungen erstellen und diese dann wie Richtlinien binden. Eine Richtlinienbezeichnung ist ein benutzerdefinierter Punkt, an den Richtlinien gebunden sind. Wenn eine Richtlinienbezeichnung aufgerufen wird, werden alle an sie gebundenen Richtlinien in der Reihenfolge der von Ihnen konfigurierten Priorität ausgewertet. Eine Richtlinienbezeichnung kann eine oder mehrere Richtlinien enthalten, von denen jeder ein eigenes Ergebnis zugewiesen werden kann. Eine Übereinstimmung einer Richtlinie in der Richtlinienbezeichnung kann dazu führen, dass mit der nächsten Richtlinie fortgefahren wird, eine andere Richtlinienbezeichnung oder eine geeignete Ressource aufgerufen wird, oder ein sofortiges Ende der Richtlinienauswertung und die Rückgabe der Kontrolle an die Richtlinie, die die Richtlinienbezeichnung aufgerufen hat.

Eine Richtlinienbezeichnung zum Umschreiben besteht aus einem Namen, einem Transformationsnamen, der den in der Richtlinienbezeichnung enthaltenen Richtlinientyp beschreibt, und einer Liste von Richtlinien, die an die Richtlinienbezeichnung gebunden sind. Jede Richtlinie, die an die Policy Label gebunden ist, enthält alle unter Neuschreibenrichtlinie konfigurierenbeschriebenen Elemente.

Hinweis: Sie können entweder die Befehlszeilenschnittstelle oder das Konfigurationsdienstprogramm zum Erstellen und Konfigurieren von Umschreibrichtlinienbeschriftungen verwenden. Benutzer, die mit der Befehlszeilenschnittstelle und der Citrix ADC Policy Infrastructure (PI) nicht vertraut sind, werden die Verwendung des Konfigurationsdienstprogramms in der Regel viel einfacher.

So konfigurieren Sie eine Richtlinienbezeichnung mit der Befehlszeilenschnittstelle

Um eine neue Richtlinienbezeichnung hinzuzufügen, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

add rewrite policylabel <labelName> <transform>

Wenn Sie beispielsweise eine Richtlinienbezeichnung mit dem Namen polLabelHTTPResponses hinzufügen möchten, um alle Richtlinien zu gruppieren, die mit HTTP-Antworten arbeiten, geben Sie Folgendes ein:

add rewrite policylabel polLabelHTTPResponses http_res

Um eine vorhandene Umschreibrichtlinienbezeichnung zu ändern, geben Sie an der Citrix ADC Eingabeaufforderung den folgenden Befehl ein:

set rewrite policy <name> <transform>

Hinweis: Der Befehl set rewrite policy verwendet dieselben Optionen wie der Befehl add rewrite policy.

Geben Sie zum Entfernen einer Richtlinienbezeichnung an der Citrix ADC Eingabeaufforderung den folgenden Befehl ein:

rm rewrite policy<name>

Um beispielsweise eine Richtlinienbezeichnung mit dem Namen polLabelHTTPResponses zu entfernen, geben Sie Folgendes ein:

rm rewrite policy polLabelHTTPResponses

So konfigurieren Sie eine Umschreibungsrichtlinienbezeichnung mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **AppExpert** > **Umschreiben** > **Richtlinienbeschriftungen**.

2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Klicken Sie auf **Hinzufügen**, um eine neue Richtlinienbezeichnung zu erstellen.
   - Um eine vorhandene Richtlinienbezeichnung zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Öffnen**.
3. Hinzufügen oder Entfernen von Richtlinien aus der Liste, die an die Richtlinienbezeichnung gebunden ist.
   - Um der Liste eine Richtlinie hinzuzufügen, klicken Sie auf **Richtlinie einfügen**, und wählen Sie eine Richtlinie aus der Dropdownliste aus. Sie können eine neue Richtlinie erstellen und zur Liste hinzufügen, indem Sie Neue Richtlinie in der Liste auswählen und den Anweisungen unter Konfigurieren einer Rewrite-Richtlinie folgen.
   - Um eine Richtlinie aus der Liste zu entfernen, wählen Sie diese Richtlinie aus, und klicken Sie dann auf Richtlinie aufheben.
4. Ändern Sie die Priorität jeder Richtlinie, indem Sie die Nummer in der Spalte Priorität bearbeiten.

   Sie können Richtlinien auch automatisch neu nummerieren, indem Sie auf Prioritäten neu erstellen klicken.
5. Klicken Sie auf **Erstellen** oder **OK** und dann auf **Schließen**.

   Um eine Richtlinienbezeichnung zu entfernen, wählen Sie sie aus, und klicken Sie dann auf **Entfernen**. Um eine Richtlinienbezeichnung umzubenennen, wählen Sie sie aus, und klicken Sie dann auf **Umbenennen**. Bearbeiten Sie den Namen der Richtlinie, und klicken Sie dann auf **OK**, um die Änderungen zu speichern.

Konfigurieren der Standardaktion Umschreiben

October 5, 2021

Ein undefiniertes Ereignis wird ausgelöst, wenn Citrix ADC eine Richtlinie nicht auswerten kann, normalerweise weil es einen logischen oder anderen Fehler in der Richtlinie oder eine Fehlerbedingung auf dem Citrix ADC erkennt. Wenn die Richtlinienauswertung zu einem Fehler führt, wird die angegebene undefinierte Aktion ausgeführt. Nicht definierte Aktionen, die auf der Richtlinienebene neu geschrieben werden, werden vor einer global konfigurierten nicht definierten Aktion ausgeführt.

Citrix ADC unterstützt die folgenden drei Arten von nicht definierten Aktionen:

- undefAction NOREWRITE

  Bricht die Rewrite-Verarbeitung ab, ändert aber nicht den Paketfluss. Dies bedeutet, dass Citrix ADC weiterhin Anforderungen und Antworten verarbeitet, die keiner Umschreibungsrichtlinie

entsprechen, und sie schließlich an die angeforderte URL weiterleitet, es sei denn, ein anderes Feature greift ein und blockiert oder umleitet die Anforderung weiter. Diese Aktion ist für normale Anforderungen an Ihre Webserver geeignet und ist die Standardeinstellung.

- undefAction RESET

  Setzt die Clientverbindung zurück. Dies bedeutet, dass der Citrix ADC dem Client mitteilt, dass er seine Sitzung mit dem Webserver wiederherstellen muss. Diese Aktion eignet sich für wiederholte Anforderungen für Webseiten, die nicht vorhanden sind, oder für Verbindungen, bei denen versucht werden kann, Ihre geschützten Websites zu hacken oder zu untersuchen.

- undefAction DROP

  Löscht die Anfrage im Hintergrund, ohne auf den Client in irgendeiner Weise zu antworten. Das bedeutet, dass Citrix ADC die Verbindung einfach verwirft, ohne auf den Client zu reagieren. Diese Aktion eignet sich für Anfragen, die anscheinend Teil eines DDoS-Angriffs oder eines anderen anhaltenden Angriffs auf Ihre Server zu sein scheinen.

Hinweis: Nicht definierte Ereignisse können sowohl für Anforderungs- als auch für Antwortfluss-spezifische Richtlinien ausgelöst werden.

So konfigurieren Sie die Standardaktion mit der Befehlszeilenschnittstelle

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

- <set rewrite param -undefAction (NOREWRITE | RESET | DROP)
- <show rewrite param

Beispiel:

```
> set rewrite param -undefAction NOREWRITE
 Done
> show rewrite param
        Action Name: NOREWRITE
 Done
<!--NeedCopy-->
```

So konfigurieren Sie die Standardaktion mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu AppExpert > Neu schreiben.
2. Klicken Sie im Detailbereich unter Rewrite Overview auf den Link Rewrite Settings ändern. Das Dialogfeld Rewrite Params festlegen wird angezeigt.

3. Wählen Sie unter Globale Aktion mit nicht definiertem Ergebnis eine Option wie folgt aus:
   - NoRewrite—NOREWRITE
   - Reset—RESET
   - Drop—DROP
4. Klicken Sie auf OK. Die globale nicht definierte Aktion wird auf den von Ihnen gewählten Wert festgelegt.

Umgehung der Sicherheitsprüfung

October 5, 2021

Wenn Sie eine Umschreibaktion erstellen, überprüft Citrix ADC, ob der Ausdruck, den Sie zum Erstellen der Aktion verwendet haben, sicher ist. Ausdrücke, die vom Citrix ADC aus Laufzeitdaten erstellt werden, z. B. URLs, die in HTTP-Anforderungen enthalten sind, können unerwartete Fehler verursachen. Citrix ADC meldet Ausdrücke, die Fehler wie unsichere Ausdrücke verursachen.

In einigen Fällen können die Ausdrücke sicher sein. Beispielsweise kann Citrix ADC keinen Ausdruck überprüfen, der eine URL enthält, die nicht aufgelöst wird, selbst wenn die URL nicht aufgelöst wird, weil der Webserver vorübergehend nicht verfügbar ist. Sie können die Sicherheitsprüfung manuell umgehen, um diese Ausdrücke zuzulassen.

So umgehen Sie die Sicherheitsprüfung über die Befehlszeilenschnittstelle

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

- <set rewrite action <name> -bypassSafetyCheck YES
- <show rewrite action <name>

Beispiel:

```
> set rewrite action insertact -bypassSafetyCheck YES
 Done
> show rewrite action insertact

        Name: insertact
        Operation: insert_http_header   Target:Client-IP
        Value:CLIENT.IP.SRC
        BypassSafetyCheck : YES
        Hits: 0
        Undef Hits: 0
```



```
        Action Reference Count: 2
 Done
<!--NeedCopy-->
```

So umgehen Sie die Sicherheitsprüfung mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **AppExpert** > **Umschreiben** > **Aktionen**.
2. Wählen Sie im Detailbereich die Neuschreibaktion aus, die von der Sicherheitsprüfung ausgenommen werden soll, und klicken Sie dann auf **Öffnen**.
3. Aktivieren **Sie im Dialogfeld Umschreibungsaktion konfigurieren** das **Kontrollkästchen Sicherheitsprüfung umgehen**.
4. Klicken Sie auf **OK**.

Beispiele für Umschreiben von Aktionen und Richtlinien

October 5, 2021

Die Beispiele in diesem Abschnitt zeigen, wie Sie Rewrite konfigurieren, um verschiedene nützliche Aufgaben auszuführen. Die Beispiele finden Sie im Serverraum von Example Manufacturing Inc. statt, einem mittelständischen Fertigungsunternehmen, das seine Website verwendet, um einen erheblichen Teil seiner Verkäufe, Lieferungen und Kundensupport zu verwalten.

Beispiel Manufacturing verfügt über zwei Domänen: example.com für seine Website und E-Mail an Kunden und example.net für sein Intranet. Kunden nutzen die Beispiel-Website, um Bestellungen aufzugeben, Angebote anzufordern, Produkte zu recherchieren und sich an den Kundenservice und den technischen Support zu wenden.

Als wichtiger Teil des Umsatzstroms von Example muss die Website schnell reagieren und Kundendaten vertraulich behandeln. Beispiel verfügt daher über mehrere Webserver und verwendet Citrix ADC Appliances, um die Auslastung der Website auszugleichen und den Datenverkehr zu und von ihren Webservern zu verwalten.

Die Beispielsystemadministratoren verwenden die Rewrite-Features, um die folgenden Aufgaben auszuführen:

Beispiel 1: Löschen alter X-Forwarded-For und Client-IP-Header

Example Inc. entfernt alte X-Forwarded-For und Client-IP-HTTP-Header aus eingehenden Anforderungen.

Beispiel 2: Hinzufügen eines lokalen Client-IP-Headers

Example Inc. fügt eingehenden Anforderungen einen neuen, lokalen Client-IP-Header hinzu.

Beispiel 3: Markieren sicherer und unsicherer Verbindungen

Example Inc. kennzeichnet eingehende Anforderungen mit einem Header, der angibt, ob die Verbindung eine sichere Verbindung ist.

Beispiel 4: Maskieren des HTTP-Servertyps

Example Inc. ändert den HTTP Server: Header so, dass nicht autorisierte Benutzer und bösartiger Code diesen Header nicht verwenden können, um die verwendete HTTP-Serversoftware zu ermitteln.

Beispiel 5: Umleiten einer externen URL zu einer internen URL

Example Inc. verbirgt Informationen über die tatsächlichen Namen der Webserver und die Konfiguration des Serverraums von Benutzern, um URLs auf der Website kürzer und leichter zu merken und die Sicherheit auf der Website zu verbessern.

Beispiel 6: Migrieren von Apache Rewrite-Modul-Regeln

Example Inc. hat die Apache-Rewrite-Regeln in eine Citrix ADC Appliance verschoben und die Apache Perl-basierte Skriptsyntax in die Citrix ADC-Rewrite-Regelsyntax übersetzt.

Beispiel 7: Umleitung von Marketingschlüsselwörtern

Die Marketingabteilung von Example Inc. richtet vereinfachte URLs für bestimmte vordefinierte Suchbegriffe auf der Website des Unternehmens ein.

Beispiel 8: Umleiten von Abfragen an den abgefragten Server.

Example Inc. leitet bestimmte Abfrageanforderungen an den entsprechenden Server weiter.

Beispiel 9: Startseitenumleitung

Example Inc. hat kürzlich einen kleineren Mitbewerber erworben, und es leitet nun Anfragen an die Homepage des erworbenen Unternehmens auf eine Seite auf seiner eigenen Website um.

Beispiel 10: Richtlinienbasierte RSA-Verschlüsselung

Beispiel Inc. verschlüsseln vordefinierte und benutzerdefinierte Header- oder Körperinhalte mithilfe des öffentlichen PEM RSA-Schlüssels.

Jede dieser Aufgaben erfordert, dass die Systemadministratoren Neuschreibaktionen und Richtlinien erstellen und sie an einen gültigen Bindepunkt auf dem Citrix ADC binden.

Beispiel 1: Löschen alter X-Forwarded-For und Client-IP-Header

October 5, 2021

Example Inc. möchte alte X-Forwarded-For und Client-IP-HTTP-Header aus eingehenden Anforderungen entfernen, sodass die einzigen X-Forwarded-For-Header angezeigt werden, die vom lokalen

Server hinzugefügt werden. Diese Konfiguration kann über die Citrix ADC Befehlszeile oder das Konfigurationsdienstprogramm erfolgen. Der Example Inc. Systemadministrator ist ein Old-School-Netzwerkingenieur und bevorzugt, wenn möglich eine CLI zu verwenden, möchte aber sicherstellen, dass er die Konfiguration Utility-Schnittstelle versteht, damit er neue Systemadministratoren im Team zeigen kann, wie sie verwendet werden.

Die folgenden Beispiele veranschaulichen, wie jede Konfiguration sowohl mit der CLI als auch mit dem Konfigurationsdienstprogramm durchgeführt wird. Die Prozeduren werden unter der Annahme abgekürzt, dass Benutzer bereits die Grundlagen zum Erstellen von Umschreibaktionen, Erstellen von Umschreibrichtlinien und Bindungsrichtlinien kennen.

- Ausführlichere Informationen zum Erstellen von Rewrite-Aktionen finden Sie unter Konfigurieren einer Rewrite-Aktion.
- Ausführlichere Informationen zum Erstellen von Rewrite-Richtlinien finden Sie unter Konfigurieren einer Rewrite-Richtlinie.
- Ausführlichere Informationen zum Binden von Rewrite-Richtlinien finden Sie unter Binden einer Rewrite-Richtlinie.

So löschen Sie alte X-Forwarded und Client-IP-Header aus einer Anforderung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

```
1 add rewrite action act_del_xfor delete_http_header x-forwarded-for
2 add rewrite action act_del_cip delete_http_header client-ip
3 add rewrite policy pol_check_xfor 'HTTP.REQ.HEADER(”x-forwarded-for”).
     EXISTS' act_del_xfor
4 add rewrite policy pol_check_cip 'HTTP.REQ.HEADER(”client-ip”).EXISTS'
     act_del_cip
5 bind rewrite global pol_check_xfor 100 200
6 bind rewrite global pol_check_cip 200 300
7 <!--NeedCopy-->
```

So löschen Sie alte X-Forwarded und Client-IP-Header aus einer Anforderung mit dem Konfigurationsdienstprogramm

Erstellen Sie im Dialogfeld Neuschreibaktion erstellen zwei Umschreibaktionen mit den folgenden Beschreibungen.

Name	Typ	Argument (e)
act_del_xfor	delete_http_header	x-weitergeleitet für
act_del_cip	delete_http_header	Client-IP

Erstellen Sie im Dialogfeld Rewrite-Richtlinie erstellen zwei Umschreibrichtlinien mit den folgenden Beschreibungen.

Name	Ausdruck	Aktion
pol_check_xfor	'HTTP.REQ.HEADER("x-forwarded-for").EXISTS'	act_del_xfor
pol_check_cip	'HTTP.REQ.HEADER("client-ip").EXISTS'	act_del_cip

Binden Sie beide Richtlinien an globale Richtlinien und weisen Sie die unten aufgeführten Prioritäten und Goto-Ausdruckswerte zu.

Name	Priorität	Gehe zu Ausdruck
pol_check_xfor	100	200
pol_check_cip	200	300

Alle alten X-Forwarded-For und Client-IP HTTP-Header werden nun aus eingehenden Anfragen gelöscht.

Beispiel 2: Hinzufügen eines lokalen Client-IP-Headers

October 5, 2021

Example Inc. möchte eingehenden Anforderungen einen lokalen Client-IP-HTTP-Header hinzufügen. Dieses Beispiel enthält zwei leicht unterschiedliche Versionen derselben Grundaufgabe.

So fügen Sie mit der Befehlszeilenschnittstelle einen lokalen Client-IP-Header hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:


```
add rewrite action act_ins_client insert_http_header NS-Client 'CLIENT.IP.SRC'
add rewrite policy pol_ins_client 'HTTP.REQ.HEADER(”x-forwarded-for”).EXISTS || HTTP.REQ.HEADER(”client-ip”).EXISTS' act_ins_client
bind rewrite global pol_ins_client 300 END
<!--NeedCopy-->
```

So fügen Sie mit dem Konfigurationsdienstprogramm einen lokalen Client-IP-Header hinzu

Erstellen Sie im Dialogfeld Rewrite Action erstellen eine Umschreiben Aktion mit der folgenden Beschreibung.

Name	Typ	Argument (e)
act_ins_client	insert_http_header	NS-Client ‘CLIENT.IP.SRC’

Erstellen Sie im Dialogfeld Rewrite-Richtlinie erstellen eine Richtlinie zum Umschreiben mit der folgenden Beschreibung.

Name	Ausdruck	Aktion
pol_ins_client	‘HTTP.REQ.HEADER (“x-forwarded-for”) .EXISTS || HTTP.REQ.HEADER (“client-ip”) .EXISTS’	act_ins_client

Binden Sie die Richtlinie an Global, Zuweisen der Prioritäten und Gehe zu Ausdruckswerten unten gezeigt.

Name	Priorität	Gehe zu Ausdruck
pol_ins_client	100	Neben

Beispiel 3: Markieren sicherer und unsicherer Verbindungen

October 5, 2021

Example Inc. möchte eingehende Anfragen mit einem Header versehen, der angibt, ob die Verbindung eine sichere Verbindung ist oder nicht. Dies hilft dem Server, sichere Verbindungen zu verfolgen, nachdem der Citrix ADC die Verbindungen entschlüsselt hat.

Um diese Konfiguration zu implementieren, erstellen Sie zunächst Rewrite-Aktionen mit den Werten in den folgenden Tabellen. Diese Aktionen beschriften Verbindungen zu Port 80 als unsichere Verbindungen und Verbindungen zu Port 443 als sichere Verbindungen.

Aktionsname	Art der Umschreibungsaktion	Kopfzeilenname	Wert
Action-Rewrite-SSL_YES	INSERT_HTTP_HEADER	SSL	JA

Aktionsname	Art der Umschreibungsaktion	Kopfzeilenname	Wert
Action-Rewrite-SSL_NO	INSERT_HTTP_HEADER	SSL	NEIN

Anschließend erstellen Sie eine Richtlinie zum Umschreiben mit den Werten in den folgenden Tabellen. Diese Richtlinien überprüfen eingehende Anforderungen, um zu bestimmen, welche Anforderungen an Port 80 weitergeleitet werden und welche an Port 443 weitergeleitet werden. Die Richtlinien fügen dann den richtigen SSL-Header hinzu.

Richtlinienname	Aktionsname	Nicht definierte Aktion	Ausdruck
Policy-Rewrite-SSL_YES	Action-Rewrite-SSL_YES	NOREWRITE	CLIENT.TCP.DSTPORT.EQ(443)
Policy-Rewrite-SSL_NO	Action-Rewrite-SSL_NO	NOREWRITE	CLIENT.TCP.DSTPORT.EQ (80)

Schließlich würden Sie die Umschreibungsrichtlinien an Citrix ADC binden, indem Sie der ersten Richtlinie eine Priorität von 200 und der zweiten eine Priorität von 300 zuweisen und den goto-Ausdruck beider Richtlinien auf END festlegen.

Jede eingehende Verbindung zu Port 80 hat nun einen SSL:NO HTTP-Header hinzugefügt und jede eingehende Verbindung zu Port 443 hat einen SSL:YES HTTP-Header hinzugefügt.

Beispiel 4: Maskieren des HTTP-Servertyps

October 5, 2021

Example Inc. möchte den HTTP Server: Header so ändern, dass nicht autorisierte Benutzer und bösartiger Code den Header nicht verwenden können, um die Software zu identifizieren, die der HTTP-Server verwendet.

Um den HTTP Server: Header zu ändern, erstellen Sie eine Rewrite-Aktion und eine Rewrite-Richtlinie mit den Werten in den folgenden Tabellen.

Aktionsname	Art der Umschreibungsaktion	Ausdruck zum Auswählen der Zielreferenz	Zeichenfolgenausdruck für Ersetzungstext
Action-Rewrite-Server_Mask	REPLACE	HTTP.RES.HEADER(“Se	“Web Server 1.0”

Richtlinienname	Aktionsname	Nicht definierte Aktion	Ausdruck
Policy-Rewrite-Server_Mask	Action-Rewrite-Server_Mask	NOREWRITE	HTTP.RES.IS_VALID

Beispielbefehle:

```
> add rewrite action Action-Rewrite-Server_Mask REPLACE HTTP.RES.HEADER(”Server”)”\”Web Server 1.0\””
```

```
> add rewrite policy Policy-Rewrite-Server_Mask HTTP.RES.IS_VALID Action-Rewrite-Server_Mask NOREWRITE
```

Anschließend würden Sie die Richtlinie zum Umschreiben global binden, indem Sie eine Priorität von 100 zuweisen und den Ausdruck Gehe zu Prioritätsausdruck der Richtlinie auf END festlegen.

Der HTTP Server: Header wurde nun so geändert, dass er Web Server 1.0 liest und die tatsächliche HTTP-Serversoftware maskiert, die von der Example Inc.-Website verwendet wird.

Beispiel 5: Umleiten einer externen URL auf eine interne URL

January 28, 2022

Example Inc. möchte seine tatsächliche Serverraumkonfiguration vor Benutzern verbergen, um die Sicherheit auf seinen Webservern zu verbessern.

Dazu würden Sie eine Rewriteaktion mit den Werten erstellen, wie in den folgenden Tabellen gezeigt. Bei Anforderungsheadern wird die Aktion in der Tabelle von `www.example.com` zu web.hq.example.net geändert. Bei Response-Headern macht die Aktion das Gegenteil und übersetzt `web.hq.example.net` in `www.example.com`.

Name der Aktion	Art der Rewrite-Aktion	Ausdruck zur Auswahl der Zielreferenz	Zeichenfolgenausdruck für Ersetzungstext
Action-Rewrite-Request_Server_Replac	REPLACE	HTTP.REQ.HOSTNAME.S	“Web.hq.example.net”
Action-Rewrite-Response_Server_Replace	REPLACE	HTTP.RES.HEADER(“Server”)	“www.example.com”

Die erste Richtlinie prüft eingehende Anfragen, um festzustellen, ob sie gültig sind, und wenn dies der Fall ist, führt sie die Aktion Action-Rewrite-Request_Server_Replace aus. Die zweite Richtlinie überprüft die Antworten, um festzustellen, ob sie vom Server stammen `web.hq.example.net`. Wenn dies der Fall ist, führt es die Aktion Action-Rewrite-Response_Server_Replace aus.

Beispiele für Rewrite-Aktionen und Richtlinien zum Umleiten einer externen URL.

```
add rewrite action Action-Rewrite-Request_Server_Replace REPLACE HTTP.REQ.
HOSTNAME.SERVER '”Web.hq.example.net”'
```

```
add rewrite action Action-Rewrite-Response_Server_Replace REPLACE HTTP.RES.
HEADER(”Server”)'”www.example.com”'
```

```
add rewrite policy Policy-Rewrite-Request_Server_Replace HTTP.REQ.HOSTNAME.
SERVER.EQ(”www.example.com”)Action-Rewrite-Request_Server_Replace NOREWRITE
```

```
add rewrite policy Policy-Rewrite-Response_Server_Replace HTTP.REQ.HEADER(”
Server”).EQ(”Web.hq.example.net”)Action-Rewrite-Response_Server_Replace
```

Schließlich würden Sie die Rewriterichtlinien binden und jedem eine Priorität von 500 zuweisen, da sie sich in verschiedenen Policenbanken befinden und daher keinen Konflikt verursachen. Sie sollten den goto Ausdruck für beide Bindungen auf NEXT setzen.


```
bind rewrite global Policy-Rewrite-Request_Server_Replace 500 END -type
REQ_DEFAULT

bind rewrite global Policy-Rewrite-Response_Server_Replace 500 END -type
RES_DEFAULT
```

Alle Instanzen von `www.example.com` in den Anforderungsheadern werden jetzt in geändert `web.hq.example.net`, und alle Instanzen von In-Response-Headern werden jetzt `web.hq.example.net` in geändert `www.example.com`.

Beispiel 6: Migrieren von Apache Rewrite-Modul-Regeln

October 5, 2021

Example Inc., verwendet derzeit das Apache-Rewrite-Modul, um Suchanfragen zu verarbeiten, die an die Webserver gesendet werden, und leitet diese Anfragen auf der Grundlage der Informationen in der Anforderungs-URL an den entsprechenden Server um. Example Inc. möchte die Einrichtung vereinfachen, indem diese Regeln auf die Citrix ADC Plattform migriert werden.

Mehrere Apache-Rewrite-Regeln, die Beispiel derzeit verwendet, werden unten gezeigt. Diese Regeln leiten Suchanfragen an eine spezielle Ergebnisseite um, wenn sie keine SiteID-Zeichenfolge haben oder eine SiteID-Zeichenfolge gleich Null (0) haben, oder an die Standardergebnisseite, wenn diese Bedingungen nicht zutreffen.

Im Folgenden sind die aktuellen Apache-Rewrite-Regeln aufgeführt:

- rewriteCond% {REQUEST_FILENAME} ^/search$ [NC]
- rewriteCond% {QUERY_STRING}! siteId= [ODER]
- RewriteCond %{QUERY_STRING} SiteId=0
- RewriteCond %{QUERY_STRING} CallName=DisplayResults [NC]
- RewriteRule ^.*$ results2.html [P, L]
- RewriteCond% {REQUEST_FILENAME} ^/search$ [NC]
- RewriteCond %{QUERY_STRING} CallName=DisplayResults [NC]
- RewriteRule ^.*$ /results.html [P, L]

Um diese Apache-Rewrite-Regeln auf dem Citrix ADC zu implementieren, würden Sie Rewrite-Aktionen mit den Werten in den folgenden Tabellen erstellen.

Aktionsname	Art der Umschreibungsaktion	Ausdruck zum Auswählen der Zielreferenz	Zeichenfolgenausdruck für Ersetzungstext
Action-Rewrite-Display_Results_NulSit	REPLACE	HTTP.REQ.URL	“/results2.html”

Aktionsname	Art der Umschreibungsaktion	Ausdruck zum Auswählen der Zielreferenz	Zeichenfolgenausdruck für Ersetzungstext
Action-Rewrite-Display_Results	REPLACE	HTTP.REQ.URL	“/results2.html”

Anschließend erstellen Sie Rewrite-Richtlinien mit den Werten, wie in den folgenden Tabellen dargestellt.

Richtlinienname	Aktionsname	Nicht definierte Aktion	Ausdruck
Policy-Rewrite-Display_Results_NulSit	Action-Rewrite-Display_Results_NulSit	NOREWRITE	HTTP.REQ.URL.PATH.SET_TEXT_MOD && (!HTTP.REQ.URL.QUERY.CONTAINS(“S || HTTP.REQ.URL.QUERY.CONTAINS(“Si || HTTP.REQ.URL.QUERY.SET_TEXT_MO
Policy-Rewrite-Display_Results	Action-Rewrite-Display_Results	NOREWRITE	HTTP.REQ.URL.PATH.SET_TEXT_MOD || HTTP.REQ.URL.QUERY.SET_TEXT_MO

Schließlich würden Sie die Umschreibungsrichtlinien binden, indem Sie der ersten eine Priorität von 600 und der zweiten eine Priorität von 700 zuweisen, und dann den goto-Ausdruck für beide Bindungen auf NEXT setzen.

Citrix ADC verarbeitet diese Suchanfragen nun genau so, wie es der Webserver getan hat, bevor die Regeln des Apache-Rewrite-Moduls migriert wurden.

Beispiel 7: Umleitung von Marketingschlüsselwörtern

October 5, 2021

Die Marketingabteilung von Example Inc. möchte vereinfachte URLs für bestimmte vordefinierte Suchbegriffe auf der Website des Unternehmens einrichten. Für diese Schlüsselwörter, es will die URL neu definieren, wie unten gezeigt.

- Externe URL:


```
http://www.example.com/\<marketingkeyword\>
```

- Interne URL:

```
http://www.example.com/go/kwsearch.asp?keyword=\<marketingkeyword\>
```

Um die Umleitung für Marketingschlüsselwörter einzurichten, erstellen Sie eine Umschreibaktion mit den Werten in der folgenden Tabelle.

Aktionsname	Art der Umschreibungsaktion	Ausdruck zum Auswählen des Zielorts	Zeichenfolgenausdruck für Ersetzungstext
Action-Rewrite-Modify_URL	INSERT_BEFORE	HTTP.REQ.URL.PATH.GE	””go/kwsearch.aspkeyword=”l”

Anschließend erstellen Sie eine Richtlinie zum Umschreiben mit den Werten in der folgenden Tabelle.

Richtlinienname	Aktionsname	Nicht definierte Aktion	Ausdruck
Policy-Rewrite-Modify_URL	Action-Rewrite-Modify_URL	NOREWRITE	HTTP.REQ.HOSTNAME.SERVER.EQ(“v

Schließlich würden Sie die Richtlinie zum Umschreiben binden und ihr eine Priorität von 800 zuweisen. Im Gegensatz zu den vorherigen Umschreibrichtlinien sollte diese Richtlinie die letzte sein, die auf eine Anforderung angewendet wird, die ihren Kriterien entspricht. Aus diesem Grund setzt Citrix ADC Administrator seinen Goto-Prioritätsausdruck auf END.

Jede Anfrage, die ein Marketing-Keyword verwendet, wird auf die CGI-Seite der Keywortsuche umgeleitet, woraufhin eine Suche durchgeführt wird und alle verbleibenden Richtlinien übersprungen werden.

Beispiel 8: Umleiten von Abfragen an den abgefragten Server

October 5, 2021

Beispiel Inc. möchte Abfrageanforderungen an den entsprechenden Server umleiten, wie hier gezeigt.

- <Request: GET /query.cgi?server=5HOST: www.example.com
- <Redirect URL: <http://web-5.example.com/>

Um diese Umleitung zu implementieren, erstellen Sie zunächst eine Umschreibungsaktion mit den Werten in der folgenden Tabelle.

Aktionsname	Art der Umschreibungsaktion	Ausdruck zum Auswählen der Zielreferenz	Zeichenfolgenausdruck für Ersetzungstext
Action-Rewrite-Replace_Hostheader	REPLACE	HTTP.REQ.HEADER(“Ho	“server-“ + HTTP.REQ.URL.QUERY.VALUE(“web”) ıple.com”)

Anschließend erstellen Sie eine Richtlinie zum Umschreiben mit den Werten in der folgenden Tabelle.

Richtlinienname	Aktionsname	Nicht definierte Aktion	Ausdruck
Policy-Rewrite-Replace_Hostheader	Action-Rewrite-Replace_Hostheader	NOREWRITE	HTTP.REQ.HEADER(”Host”).EQ(”www.example.com”)

Beispielbefehle:

```
> add rewrite action Action-Rewrite-Server_Mask REPLACE HTTP.RES.HEADER(”Server”)”\”Web Server 1.0\””
Done
```

```
> add rewrite policy Policy-Rewrite-Server_Mask HTTP.RES.IS_VALID Action-Rewrite-Server_Mask NOREWRITE
Done
```

Schließlich würden Sie die Richtlinie zum Umschreiben binden und ihr eine Priorität von 900 zuweisen. Da diese Richtlinie die letzte Richtlinie sein sollte, die auf eine Anforderung angewendet wird, die ihren Kriterien entspricht, legen Sie den goto-Ausdruck auf END fest.

Eingehende Anfragen an eine URL, die mit beginnt,<http://www.example.com/query.cgi?server>= werden an die Servernummer in der Abfrage umgeleitet.

Beispiel 9: Startseitenumleitung

October 5, 2021

New Company, Inc. hat kürzlich einen kleineren Konkurrenten erworben, gekaufte Firma, und möchte die Homepage für gekaufte Firma auf eine neue Seite auf der eigenen Website umleiten, wie hier

gezeigt.

- Alte URL:http://www.purchasedcompany.com/*
- Neue URL:http://www.newcompany.com/products/page.htm

Um Anforderungen an die Startseite Gekaufte Firma umzuleiten, würden Sie Umschreibaktionen mit den Werten in der folgenden Tabelle erstellen.

Aktionsname	Art der Umschreibungsaktion	Ausdruck zum Auswählen der Zielreferenz	Zeichenfolgenausdruck für Ersetzungstext
Action-Rewrite-Replace_URLr	REPLACE	HTTP.REQ.URL.PATH_A	“/products/page.htm”
Action-Rewrite-Replace_Host	REPLACE	HTTP.REQ.HOSTNAME	“www.newcompany.com”

Anschließend erstellen Sie Rewrite-Richtlinien mit den Werten in der folgenden Tabelle.

Richtlinienname	Aktionsname	Nicht definierte Aktion	Ausdruck
Policy-Rewrite-Replace-None	Action-Rewrite-Replace-None	NOREWRITE	!HTTP.REQ.HOSTNAME.SERVER.EQ(“
Policy-Rewrite-Replace-Host	Action-Rewrite-Replace_Host	NOREWRITE	HTTP.REQ.HOSTNAME.SERVER.EQ(“v
Policy-Rewrite-Replace-URL	Action-Rewrite-Replace_URL	NOREWRITE	HTTP.REQ.IS_VALID

Schließlich würden Sie die Umschreibungsrichtlinien global binden, indem Sie der ersten eine Priorität von 100, der zweiten eine Priorität von 200 und der dritten eine Priorität von 300 zuweisen. Diese Richtlinien sollten die letzten Richtlinien sein, die auf eine Anforderung angewendet werden, die den Kriterien entspricht. Aus diesem Grund legen Sie den goto-Ausdruck für die erste und dritte Richtlinie auf END und für die zweite Richtlinie auf 300 fest. Dadurch wird sichergestellt, dass alle verbleibenden Anforderungen korrekt verarbeitet werden.

Anfragen an die alte Website des erworbenen Unternehmens werden nun auf die richtige Seite auf der Homepage des neuen Unternehmens umgeleitet.

Beispiel 10: Richtlinienbasierte RSA-Verschlüsselung

October 5, 2021

Der RSA-Algorithmus verwendet die Funktion PKEY_ENCRYPT_PEM (), um HTTP-vordefinierte und benutzerdefinierte Header- oder Körperinhalte zu verschlüsseln. Die Funktion akzeptiert nur öffentliche RSA-Schlüssel (keine privaten Schlüssel) und die verschlüsselten Daten dürfen nicht länger als die Länge des öffentlichen Schlüssels sein. Wenn die zu verschlüsselnden Daten kürzer als die Schlüssellänge ist, verwendet der Algorithmus die RSA_PKCS1-Auffüllmethode.

In einem Beispielszenario kann die Funktion mit der Funktion B64ENCODE () in einer Umschreibaktion verwendet werden, um einen HTTP-Header-Wert durch einen durch einen öffentlichen RSA-Schlüssel verschlüsselten Wert zu ersetzen. Die verschlüsselten Daten werden dann vom Empfänger mit dem privaten RSA-Schlüssel entschlüsselt.

Sie können das Feature mithilfe einer Umschreibungsrichtlinie implementieren. Um dies zu tun, müssen Sie die folgenden Aufgaben ausführen:

1. Fügen Sie den öffentlichen RSA-Schlüssel als Richtlinienausdruck hinzu.
2. Rewrite-Aktion erstellen.
3. Erstellen Sie eine Umschreibungsrichtlinie.
4. Binden Sie die Richtlinie zum Umschreiben als global.
5. Überprüfen der RSA-Verschlüsselung

Richtlinienbasierte RSA-Verschlüsselung mit der Citrix ADC Befehlszeilenschnittstelle

Führen Sie die folgenden Aufgaben aus, um die richtlinienbasierte RSA-Verschlüsselung mit der Citrix ADC Befehlszeilenschnittstelle zu konfigurieren.

So fügen Sie mit der Citrix ADC Befehlszeilenschnittstelle einen öffentlichen RSA-Schlüssel als Richtlinienausdruckhinzu:

```
1 add policy expression pubkey '"-----BEGIN RSA PUBLIC KEY-----
     MIGJAoGBAKl5vgQEj73Kxp+9
     yn1v5gPR1pnc4oLM2a0kaWwBOsB6rzCIy6znwnvwCY1xRvQhRlJSAyJbloL7wZFIJ2FOR8Cz
     +8ZQWXU2syG+udi4EnWqLgFYowF9zK+o79az597eNPAjsHZ/C2oL/+6qY5a/
     f1z8bQPrHC4GpFfAEJhh/+NnAgMBAAE=-----END RSA PUBLIC KEY-----"'
2 <!--NeedCopy-->
```

So fügen Sie eine Aktion zum Verschlüsseln einer HTTP-Header-Anforderung mit der Citrix ADC Befehlszeilenschnittstellehinzu:

```
add rewrite action encrypt_act insert_http_header encrypted_data
```



```
HTTP.REQ.HEADER(”data_to_encrypt”).PKEY_ENCRYPT_PEM(pubkey).B64ENCODE
```

So fügen Sie Rewrite-Richtlinie mit der Citrix ADC Befehlszeilenschnittstellehinzu:

```
1 add rewrite policy encrypt_pol 'HTTP.REQ.HEADER(”data_to_encrypt”).
     EXISTS' encrypt_act
2 <!--NeedCopy-->
```

So binden Sie die Umschreibungsrichtlinie global mit der Citrix ADC Befehlszeilenschnittstelle:

```
bind rewrite global encrypt_pol 10 -type RES_DEFAULT
```

So überprüfen Sie die RSA-Verschlüsselung mit der Citrix ADC Befehlszeilenschnittstelle:

```
1  >curl -v -H ”data_to_encrypt: Now is the time that tries men's souls”
      http://10.217.24.7/`
2
3  * About to connect() to 10.217.24.7 port 80 (#0)
4
5  *  Trying 10.217.24.7...
6
7  *  connected
8
9  *  Connected to 10.217.24.7 (10.217.24.7) port 80 (#0)
10
11 > GET / HTTP/1.1
12 > User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4) libcurl/7.24.0
      OpenSSL/0.9.8y zlib/1.2.3
13 > Host: 10.217.24.7
14 > Accept: \*/\*
15 > data_to_encrypt: Now is the time that tries men's souls
16 >
17 < HTTP/1.1 200 OK
18 < Date: Mon, 09 Oct 2017 05:22:37 GMT
19 < Server: Apache/2.2.24 (FreeBSD) mod_ssl/2.2.24 OpenSSL/0.9.8y DAV/2
20 < Last-Modified: Thu, 20 Feb 2014 20:29:06 GMT
21 < ETag: ”6bd9f2-2c-4f2dc5b570880”
22 < Accept-Ranges: bytes
23 < Content-Length: 44
24 < Content-Type: text/html
25 < encrypted_data: UliegKBJqZd7JdaC49XMLEK1+eQN2rEfevypW91gKvBVlaKM9N9/
      C2BKuztS99SE0xQaisidzN5IgeIcpQMn+
      CiKYVlLzPG1RuhGaqHYzIt6C8A842da7xE4OlV5SHwScqkqZ5aVrXc3EwtUksna7jOLr40aLeXnnB
      /DB11pUAE=
```



```
<
* Connection #0 to host 10.217.24.7 left intact
<html><body><h1>It works!</h1></body></html>* Closing connection #0

<!--NeedCopy-->
```

Die nachfolgende Ausführung dieses curl-Befehls mit denselben zu verschlüsselnden Daten zeigt, dass sich die verschlüsselten Daten bei jeder Ausführung unterscheiden. Dies liegt daran, dass die Auffüllung zufällige Bytes am Anfang der zu verschlüsselnden Daten einfügt, wodurch die verschlüsselten Daten jedes Mal unterschiedlich sind.

```
>curl -v -H "data_to_encrypt: Now is the time that tries men's souls"
   http://10.217.24.7/`

< encrypted_data:
   DaOjtl1Pl4DlQKf58MMeL4cFwFvZwhjMqv5aUYM5Iyzk4UpwIYhpRvgTNu2lXEVc1H0tcR1EGC
   /ViQncLc4EbTurCWLbzjce3+fknnMmzF0lRT6ZZXWbMvsNFOxDA1SnuAgwxWXy/
   ooe9Wy6SYsL2oi1sr5wTG+RihDd9zP+P14=

>curl -v -H "data_to_encrypt: Now is the time that tries men's souls"
   http://10.217.24.7/

. . .

< encrypted_data: eej6YbGP68yHn48qFUvi+fkG+OiO8j3yYLScrRBU+
   TPQ8WeDVaWnDNAVLvL0ZYHHAU1W2YDRYb+8
   cdKHLpW36QbI6Q5FfBuWKZSI2hSyUvypTpCoAYcHXFv0ns+tRtg0EPNNj+
   lyGjKQWtFi6K8IXXISoDy42FblKIlaA7gEriY=
<!--NeedCopy-->
```

Richtlinienbasierte RSA-Verschlüsselung mit der GUI

Mit der grafischen Benutzeroberfläche können Sie die folgenden Aufgaben ausführen:

So fügen Sie mit der GUI einen öffentlichen RSA-Schlüssel als Richtlinienausdruckhinzu:

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zu **Konfigurationen** > **AppExpert** > **Erweiterte Ausdrücke** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**, um einen öffentlichen RSA-Schlüssel als erweiterten Richtlinienausdruck zu definieren.
3. Legen Sie auf der Seite Ausdruck erstellen die folgenden Parameter fest:
   a) Name des Ausdrucks. Name des erweiterten Ausdrucks.

b) Ausdruck. Definieren Sie den öffentlichen RSA-Schlüssel als erweiterten Ausdruck mit dem Ausdrucksеditor.
c) Kommentare. Eine kurze Beschreibung des Ausdrucks.

4. Klicken Sie auf **Erstellen**.

So fügen Sie eine Aktion zum Verschlüsseln einer HTTP-Header-Anforderung mit der GUIhinzu:

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zu **Konfigurationen** > **AppExpert** > **Umschreiben** > **Aktionen** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**, um eine Neuschreibaktion hinzuzufügen.
3. **Legen Sie im Bildschirm Rewrite-Aktion erstellen** die folgenden Parameter fest:
   a) Name. Name der Umschreibungsaktion.
   b) Geben Sie ein. Wählen Sie den Aktionstyp als INSERT_HTTP_HEADER aus.
   c) Verwenden Sie den Aktionstyp, um eine Kopfzeile einzufügen. Geben Sie den Namen des HTTP-Headers ein, der neu geschrieben werden muss.
   d) Ausdruck. Name des erweiterten Richtlinienausdrucks, der der Aktion zugeordnet ist.
   e) Kommentare. Eine kurze Beschreibung der Umschreibaktion.
4. Klicken Sie auf **Erstellen**.

So fügen Sie mit der GUI eine erweiterte Rewrite-Richtliniehinzu:

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zu **Konfigurationen** > **AppExpert** > **Umschreiben** > **Richtlinien** .
2. Klicken Sie auf der Seite **Richtlinien umschreiben** auf **Hinzufügen**, um eine Richtlinie zum Umschreiben hinzuzufügen.
3. **Legen Sie auf der Seite Rewrite-Richtlinie erstellen** die folgenden Parameter fest:
   a) Name. Name der Richtlinie zum Umschreiben.
   b) Aktion: Name der Umschreibaktion, die ausgeführt werden soll, wenn die Anforderung oder Antwort mit dieser Umschreibrichtlinie übereinstimmt.
   c) Aktion protokollieren. Name der Nachrichtenprotokollaktion, die verwendet werden soll, wenn eine Anforderung mit dieser Richtlinie übereinstimmt.
   d) Aktion Nicht definiertes Ergebnis. Aktion, die ausgeführt werden soll, wenn das Ergebnis der Richtlinienbewertung nicht definiert ist.
   e) Ausdruck. Name des erweiterten Richtlinienausdrucks, der die Aktion auslöst.
   f) Kommentare. Eine kurze Beschreibung der Umschreibaktion.
4. Klicken Sie auf **Erstellen**.

So binden Sie die Umschreibungsrichtlinie global mit der GUI:

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zu **Konfigurationen** > **AppExpert** > **Umschreiben** > **Richtlinien** .
2. Wählen Sie im Bildschirm **Richtlinien umschreiben** eine Richtlinie zum Umschreiben, die Sie binden möchten, und klicken Sie auf **Richtlinien-Manager** .

3. Legen Sie auf der Seite Richtlinien-Manager umschreiben im Abschnitt Bindpunkte die folgenden Parameter fest:
   a) Verbindungspunkt. Wählen Sie den Bindungspunkt als Standard Global aus.
   b) -Protokoll. Wählen Sie den Protokolltyp als HTTP aus.
   c) Verbindungstyp. Wählen Sie den Verbindungstyp als Anforderung aus.
   d) Klicken Sie auf **Weiter**, um den Abschnitt **Richtlinienbindung** anzuzeigen.
   e) Wählen Sie im Abschnitt **Richtlinienbindung** die Richtlinie zum Umschreiben aus, und legen Sie die Bindungsparameter fest.
4. Klicken Sie auf **Bind**.

Beispiel 11: Policy-basierte RSA-Verschlüsselung ohne Auffüllung

October 5, 2021

Die Richtlinienfunktion PKEY_ENCRYPT_PEM_NO_PADDING () verwendet den RSA-Algorithmus ohne Auffüllung, bevor die RSA-Verschlüsselung ausgeführt wird. Die Richtlinienfunktion funktioniert genau wie die Funktion PKEY_ENCRYPT_PEM (), außer sie verwendet die Methode RSA_NO_PADDING anstelle von RSA_PKCS1_PADDING. Der Parameter pkey ist eine Textzeichenfolge mit einem PEM-kodierten öffentlichen RSA-Schlüssel. Ähnlich wie PKEY_ENCRYPT_PEM () können Sie einen Richtlinienausdruck für den Schlüssel verwenden.

Sie können das Feature mithilfe einer Umschreibungsrichtlinie implementieren. Um dies zu tun, müssen Sie die folgenden Aufgaben ausführen:

1. Fügen Sie den öffentlichen RSA-Schlüssel als Richtlinienausdruck hinzu.
2. Rewrite-Aktion erstellen.

Richtlinienbasierte RSA-Verschlüsselung mit der Citrix ADC Befehlszeilenschnittstelle

Führen Sie die folgenden Aufgaben aus, um die richtlinienbasierte RSA-Verschlüsselung mit der Citrix ADC Befehlszeilenschnittstelle zu konfigurieren.

So fügen Sie mit der Citrix ADC Befehlszeilenschnittstelle einen öffentlichen RSA-Schlüssel ohne Auffüllunghinzu:

```
1 add expression rsa_pub_key_4096 '"-----BEGIN RSA PUBLIC KEY-----" + "
    MIICCgKCAgEArrwBldKd48xrpOSRPMrg+eNAO0ODU6t5b/WYQLdElqNv7WpefBrA" +
    "nwI2s619gEU1r4zoLqL7l5ALtt5Z+F0JBYfOzBzOky0GtEJ5iX5GP4QxT65J3nHH" +
     "4MTF3acmjvXxclmaKXEFlaVIzW7FTr3Luw/CnOjflAB403Q6F9VBVvQmOVYWnqoI"
    + "+0q1VIg6Q1pAcvdKBiOf85BBofE5EIbZ/1Jt0CdbsV568l+8ve7BnSUncFHoRR3O"
```



```
        + ”/VfSsDuNWZf7n3RNMzxEuIA72UGPzNYFQzvcPOdzd0aN7jAXw0mgC/NSvKzGKHlo
       ” + ”mUYYBzlVQdDMZWnd6jSzsBRXSXxsNEy/
       RuXwplrA5epo7JdCoMkfeI4vUXm6MNr8” + ”
       TQdFqIc1pdnOsbRf9ec62XbcfR7P8CDTsmLSaagx3rjenPdB+LTWKw2VUF+YONIg” +
       ”jM3fyFef9ovVhLhS5HvMqFGs8P75W+d7BOIbIu3EngACiEJOpYSsETD4WgPK6Iyv” +
        ”j6cxsLeYMtElTb0fBIIqysCHdmjF3M1lqdqp4dKs3+W798GJZYM5MxZKUzrBi0Xu”
       + ”e7GtSh2aimsfQureUD+0z0RN2umeDsYcA1ghXMclDP+jLS1lnrv0Yvo+TKcm9b8G”
        + ”uR/drbCrCsGyWFW+bsAu3AWz9S6TePurP5unRmNNvXpH5DRgsYl3d50CAwEAAQ
       ==” + ”-----END RSA PUBLIC KEY-----”
<!--NeedCopy-->
```

So fügen Sie mit der Citrix ADC Befehlszeilenschnittstelle Umschreibaktion für keinen Ausdruck der Auffüllrichtliniehinzu:

```
add rewrite action rsa_encrypt_act insertHttpHeader encrypted 'HTTP.REQ.
HEADER(”plaintext”).PKEY_ENCRYPT_PEM_NO_PADDING(rsa_pub_key_4096)
```

Richtlinienbasierte RSA-Verschlüsselung ohne Auffüllung mit der GUI

Mit der grafischen Benutzeroberfläche können Sie die folgenden Aufgaben ausführen:

So fügen Sie mit der GUI den öffentlichen RSA-Schlüssel für keinen Auffüllvorgang als Richtlinienausdruckhinzu:

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zu **Konfigurationen** > **AppExpert** > **Erweiterte Ausdrücke** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**, um einen öffentlichen RSA-Schlüssel als erweiterten Richtlinienausdruck zu definieren.
3. Legen Sie auf der Seite Ausdruck erstellen die folgenden Parameter fest:
   a) Name des Ausdrucks. Name des erweiterten Ausdrucks.
   b) Ausdruck. Definieren Sie den öffentlichen RSA-Schlüssel als erweiterten Ausdruck mit dem Ausdrucksеditor.
      Hinweis: Die maximale Zeichenfolgenlänge beträgt 255 Zeichen in einem Richtlinienausdruck. Für jeden Schlüssel, der länger als 1024-Bits ist, müssen Sie den Schlüssel in kleinere Chunks zerlegen und die Chunks als Chunk1” + Chunk2” + verketten…
   c) Kommentare. Eine kurze Beschreibung des Ausdrucks.
4. Klicken Sie auf **Erstellen**.

So fügen Sie eine Aktion mit der GUI neu schreiben:

1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zu **Konfigurationen** > **AppExpert** > **Umschreiben** > **Aktionen** .
2. Klicken Sie im Detailbereich auf **Hinzufügen**, um eine Neuschreibaktion hinzuzufügen.
3. **Legen Sie im Bildschirm Rewrite-Aktion erstellen** die folgenden Parameter fest:

a) Name. Name der Umschreibungsaktion.
b) Geben Sie ein. Wählen Sie den Aktionstyp als INSERT_HTTP_HEADER aus.
c) Verwenden Sie den Aktionstyp, um eine Kopfzeile einzufügen. Geben Sie den Namen des HTTP-Headers ein, der neu geschrieben werden muss.
d) Ausdruck. Name des erweiterten Richtlinienausdrucks, der der Aktion zugeordnet ist.
e) Kommentare. Eine kurze Beschreibung der Umschreibaktion.

4. Klicken Sie auf **Erstellen**.

Beispiel 12: Konfigurieren von Rewrite zum Ändern des Hostnamens und der URL in Clientanforderung auf der Citrix ADC Appliance

October 5, 2021

Das Rewrite-Feature auf einer Citrix ADC Appliance wird verwendet, um die in der Clientanforderung verfügbare URL in eine andere URL zu konvertieren, die der Back-End-Server verstehen kann. Sie können die folgenden Vorteile mit der Rewrite-Funktion erzielen:

- Erhöht die Sicherheit, indem die tatsächliche URL für die Ressource ausgeblendet wird, die vom Client angefordert wird.
- Verhindert, dass der unbefugte Benutzerzugriff auf die Netzwerkressourcen erhält.

Betrachten Sie ein Beispiel, in dem Ihre aktuelle Organisation von einer anderen Organisation übernommen wird. Es wird für Administratoren eine schwierige Aufgabe, jedem Benutzer der erworbenen Organisation über die neue Webadresse zu informieren. In diesem Szenario wird die Verwendung von Rewrite-Funktion bequem, um den Hostnamen und URL in den Clientanforderungen für die Website der erworbenen Organisation zu ändern. Sie können Rewrite verwenden, um die URLs in der Clientanforderung vorübergehend zu ändern, wenn die Website gewartet wird.

Im folgenden Abschnitt wird das Verfahren zum Ändern des Hostnamens und der URL in einer Clientanforderung mithilfe der Rewrite-Funktion beschrieben.

Betrachten Sie ein Beispiel, in dem der Benutzer eine `http://www.example.com` URL im Webbrowser eingibt. Der Websiteadministrator möchte, dass die Citrix ADC Appliance die vorhergehende URL in der Clientanforderung als konvertiert `http://myexample.example.net.in/resource/inventory/s?t=112`.

Im obigen Beispiel möchte der Websiteadministrator, dass die Citrix ADC Appliance den Domänennamen “example.com” durch “myexample.example.net.in” und die URL durch “resource/inventory/s?t=112”.

Führen Sie Folgendes mit der CLI aus

1. Melden Sie sich mit SSH bei der Citrix ADC Appliance an.
2. Hinzufügen von Umschreibungsaktionen.
   - `add rewrite action rewrite_host_hdr_act replace "HTTP.REQ.HEADER(\"Host\")""\"myexample.example.net.in\""`
   - `add rewrite action rewrite_url_act replace HTTP.REQ.URL.PATH_AND_QUERY "\"/resource/inventory/s?t=112\""`
3. Fügen Sie Rewrite-Richtlinien für die Umschreibungsaktionen hinzu.
   - `add rewrite policy rewrite_host_hdr_pol "HTTP.REQ.HEADER(\"Host\").CONTAINS(\"www.example.com\")"rewrite_host_hdr_act`
   - `add rewrite policy rewrite_url_pol "HTTP.REQ.HEADER(\"Host\").CONTAINS(\"www.example.com\")"rewrite_url_act`
4. Binden Sie die Umschreibungsrichtlinien an einen virtuellen Server.
   - `bind lb vserver rewrite_LB -policyName rewrite_host_hdr_pol -priority 10 -gotoPriorityExpression 20 -type REQUEST`
   - `bind lb vserver rewrite_LB -policyName rewrite_url_pol -priority 20 -gotoPriorityExpression END -type REQUEST`

URL-Transformation

October 5, 2021

Die URL-Transformationsfunktion bietet eine Methode zum Ändern aller URLs in bestimmten Anforderungen von einer externen Version, die von externen Benutzern angezeigt wird, zu einer internen URL, die nur von Ihren Webservern und IT-Mitarbeitern angezeigt wird. Sie können Benutzeranforderungen nahtlos umleiten, ohne dass die Netzwerkstruktur Benutzern zugänglich gemacht wird. Sie können auch komplexe interne URLs ändern, die Benutzer möglicherweise schwer merken können, in einfacheren, einfacheren externen URLs.

> **Hinweis:**
>
> Bevor Sie die URL-Transformationsfunktion verwenden können, müssen Sie die Funktion Umschreiben aktivieren. Informationen zum Aktivieren der Funktion "Umschreiben" finden Sie unter Aktivieren des Rewrite-Feature.
>
> URL-Transformationsfunktion schreibt URLs im HTML-Antworttext um und wird nicht auf

> JavaScript und andere Variablen angewendet.

Um mit der Konfiguration der URL-Transformation zu beginnen, erstellen Sie Profile, die jeweils eine bestimmte Transformation beschreiben. Innerhalb jedes Profils erstellen Sie eine oder mehrere Aktionen, die die Transformation detailliert beschreiben. Als Nächstes erstellen Sie Richtlinien, die jeweils einen Typ der zu transformierenden HTTP-Anforderung identifizieren, und Sie ordnen jede Richtlinie einem entsprechenden Profil zu. Schließlich binden Sie jede Richtlinie global an, um sie in Kraft zu setzen.

Konfigurieren von URL-Transformationsprofilen

October 5, 2021

Ein Profil beschreibt eine bestimmte URL-Transformation als eine Reihe von Aktionen. Das Profil dient primär als Container für die Aktionen und bestimmt die Reihenfolge, in der die Aktionen ausgeführt werden. Die meisten Transformationen transformieren einen externen Hostnamen und einen optionalen Pfad in einen anderen, internen Hostnamen und Pfad. Die meisten nützlichen Transformationen sind einfach und erfordern nur eine einzige Aktion. Sie können jedoch mehrere Aktionen verwenden, um komplexe Transformationen durchzuführen.

Sie können keine Aktionen erstellen und sie dann einem Profil hinzufügen. Sie müssen zuerst das Profil erstellen und dann Aktionen hinzufügen. In der CLI sind das Erstellen einer Aktion und das Konfigurieren der Aktion separate Schritte. Das Erstellen eines Profils und das Konfigurieren des Profils sind separate Schritte sowohl in der CLI als auch im Konfigurationsdienstprogramm.

So erstellen Sie ein URL-Transformationsprofil mit der Citrix ADC Befehlszeile

Geben Sie an der Citrix ADC Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein, um ein URL-Transformationsprofil zu erstellen und die Konfiguration zu überprüfen. Sie können dann den zweiten und dritten Befehl wiederholen, um zusätzliche Aktionen zu konfigurieren:

- `add transform profile <profileName> -type URL [-onlyTransformAbsURLinBody (ON|OFF)] \[-comment <comment>]`
- `add transform action <name> <profileName> <priority>`
- `set transform action <name> [-priority <priority>] [-reqUrlFrom <expression>] [-reqUrlInto <expression>] [-resUrlFrom <expression>] [-resUrlInto <expression>] [-cookieDomainFrom <expression>] [-cookieDomainInto <expression>] [-state (ENABLED|DISABLED)] [-comment "<string>"]`
- `show transform profile <name>`

Beispiel:


```
> add transform profile shoppingcart -type URL
 Done
> add transform action actshopping shoppingcart 1000
 Done
> set transform action actshopping -priority 1000 -reqUrlFrom 'shopping
   .example.com' -reqUrlInto 'www.example.net/shopping' -resUrlFrom '
   www.example.net/shopping' -resUrlInto 'shopping.example.com' -
   cookieDomainFrom 'example.com' -cookieDomainInto 'example.net' -
   state ENABLED -comment 'URL transformation for shopping cart.'
 Done
> show transform profile shoppingcart
        Name: shoppingcart
                Type: URL       onlyTransformAbsURLinBody: OFF
        Comment:
        Actions:

1)              Priority 1000   Name: actshopping       ENABLED
 Done
<!--NeedCopy-->
```

So ändern Sie ein vorhandenes URL-Transformationsprofil oder -aktion mit der Citrix ADC Befehlszeile

Geben Sie an der Citrix ADC Eingabeaufforderung die folgenden Befehle ein, um ein vorhandenes URL-Transformationsprofil oder eine vorhandene Aktion zu ändern und die Konfiguration zu überprüfen:

Hinweis: Verwenden Sie den Befehl set transform profile oder set transform action. Der Befehl set transform profile verwendet dieselben Argumente wie der Befehl add transform profile, und set transform action ist derselbe Befehl, der für die Erstkonfiguration verwendet wurde.

- `set transform action <name> [-priority <priority>] [-reqUrlFrom <expression>] [-reqUrlInto <expression>] [-resUrlFrom <expression>] [-resUrlInto <expression>] [-cookieDomainInto <expression>] [-state (ENABLED|DISABLED)] [-comment "<string>"]`
- `show transform profile <name>`

Beispiel:

```
> set transform action actshopping -priority 1000 -reqUrlFrom '
   searching.example.net' -reqUrlInto 'www.example.net/searching' -
   resUrlFrom 'www.example.net/searching' -resUrlInto 'searching.
```



```
      example.com' -cookieDomainInto 'example.net' -state ENABLED -comment
       'URL transformation for searching cart.'
 Done
> show transform profile shoppingcart
        Name: shoppingcart
                Type: URL       onlyTransformAbsURLinBody: OFF
        Comment:
        Actions:

1)              Priority 1000   Name: actshopping       ENABLED
 Done
<!--NeedCopy-->
```

So entfernen Sie ein URL-Transformationsprofil und Aktionen mit der Citrix ADC Befehlszeile

Entfernen Sie zunächst alle Aktionen, die diesem Profil zugeordnet sind, indem Sie den folgenden Befehl einmal für jede Aktion eingeben:

- rm transform action<name> Nachdem Sie alle Aktionen entfernt haben, die einem Profil zugeordnet sind, entfernen Sie das Profil wie unten dargestellt.
- rm Transformationsprofil<name>

So erstellen Sie ein URL-Transformationsprofil mit dem Konfigurationsdienstprogramm

1. Erweitern Sie im Navigationsbereich **Umschreiben**, erweitern Sie URL-Transformation, und klicken Sie dann auf **Profile**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld URL-Transformationsprofil erstellen** Werte für die Parameter ein oder wählen Sie sie aus. Der Inhalt des Dialogfelds entspricht den unter Parameter für die Konfiguration von URL-Transformationsprofilen beschriebenen Parametern (Sternchen gibt einen erforderlichen Parameter an):
   - Name*—Name
   - Kommentar—comment
   - Transformieren Sie nur absolute URLs im Antworttext — onlyTransformAbsURLinBody
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das Profil erfolgreich konfiguriert wurde.

So konfigurieren Sie ein URL-Transformationsprofil und -aktionen mit dem Konfigurationsdienstprogramm

1. Erweitern Sie im Navigationsbereich **Umschreiben**, erweitern Sie URL-Transformation, und klicken Sie dann auf **Profile**.
2. Wählen Sie im Detailbereich das Profil aus, das Sie konfigurieren möchten, und klicken Sie dann auf **Öffnen**.
3. **Führen Sie im Dialogfeld URL-Transformationsprofil konfigurieren** eine der folgenden Aktionen aus.
   - Um eine neue Aktion zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Aktion zu ändern, wählen Sie die Aktion aus, und klicken Sie dann auf **Öffnen**.
4. Füllen Sie das Dialogfeld **URL-Transformationsaktion erstellen** oder **URL-Transformationsaktion ändern** aus, indem Sie Werte für die Parameter eingeben oder auswählen. Der Inhalt des Dialogfelds entspricht den unter Parameter für die Konfiguration von URL-Transformationsprofilen beschriebenen Parametern (Sternchen gibt einen erforderlichen Parameter an):
   - Aktionsname* — name
   - Kommentare—comment
   - Priorität*— priority
   - URL anfordern von—reqUrlFrom
   - URL anfordern into—reqUrlInto
   - Antwort-URL von—resUrlFrom
   - Antwort-URL into—resUrlInto
   - Cookie-Domain von—cookieDomainFrom
   - Cookie-Domain into—cookieDomainInto
   - Aktiviert — state
5. Speichern Sie Ihre Änderungen.
   - Wenn Sie eine neue Aktion erstellen, klicken Sie auf **Erstellen**und dann auf **Schließen**.
   - Wenn Sie eine vorhandene Aktion ändern, klicken Sie auf **OK**.
     In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das Profil erfolgreich konfiguriert wurde.
6. Wiederholen Sie Schritt 3 bis Schritt 5, um zusätzliche Aktionen zu erstellen oder zu ändern.
7. Um eine Aktion zu löschen, wählen Sie die Aktion aus, und klicken Sie dann auf Entfernen. Wenn Sie dazu aufgefordert werden, klicken Sie auf OK, um den Löschvorgang zu bestätigen.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Dialogfeld URL-Transformationsprofil ändern zu schließen.
9. Um ein Profil zu löschen, wählen Sie im Detailbereich das Profil aus, und klicken Sie dann auf **Entfernen**. Wenn Sie dazu aufgefordert werden, klicken Sie auf **OK**, um den Löschvorgang zu bestätigen.

Konfigurieren von URL-Transformationsrichtlinien

October 5, 2021

Nachdem Sie ein URL-Transformationsprofil erstellt haben, erstellen Sie als nächstes eine URL-Transformationsrichtlinie, um die Anforderungen und Antworten auszuwählen, die der Citrix ADC mithilfe des Profils transformieren soll. URL-Transformation betrachtet jede Anforderung und die Antwort darauf als eine einzelne Einheit. Daher werden URL-Transformationsrichtlinien nur ausgewertet, wenn eine Anforderung empfangen wird. Wenn eine Richtlinie übereinstimmt, transformiert Citrix ADC sowohl die Anforderung als auch die Antwort.

Hinweis: Die URL-Transformations- und Rewrite-Funktionen können nicht beide auf demselben HTTP-Header während der Anforderungsverarbeitung ausgeführt werden. Wenn Sie eine URL-Transformation auf eine Anforderung anwenden möchten, müssen Sie sicherstellen, dass keiner der von ihm geänderten HTTP-Header durch eine Umschreibungsaktion manipuliert wird.

So konfigurieren Sie eine URL-Transformationsrichtlinie mit der Citrix ADC Befehlszeile

Sie müssen eine neue Richtlinie erstellen. In der Befehlszeile kann eine vorhandene Richtlinie nur entfernt werden. Geben Sie an der Citrix ADC Eingabeaufforderung die folgenden Befehle ein, um eine URL-Transformationsrichtlinie zu konfigurieren und die Konfiguration zu überprüfen:

- <add transform policy <name> <rule> <profileName>
- <show transform policy <name>

Beispiel:

```
1  > add transform policy polsearch  HTTP.REQ.URL.SUFFIX.EQ(”Searching”)
       prosearching
2   Done
3  > show transform policy polsearch
4  1)      Name: polsearch
5          Rule: HTTP.REQ.URL.SUFFIX.EQ(”Searching”)
6          Profile: prosearching
7          Priority: 0
8          Hits: 0
9   Done
10 <!--NeedCopy-->
```


So entfernen Sie eine URL-Transformationsrichtlinie mit der Citrix ADC Befehlszeile

Geben Sie an der Citrix ADC Eingabeaufforderung den folgenden Befehl ein, um eine URL-Transformationsrichtlinie zu entfernen:

```
rm transform policy <name>
```

Beispiel:

```
1 > rm transform policy polsearch
2 Done
3 <!--NeedCopy-->
```

So konfigurieren Sie eine URL-Transformationsrichtlinie mit dem Konfigurationsdienstprogramm

1. Erweitern Sie im Navigationsbereich **Umschreiben**, erweitern Sie URL-Transformation, und klicken Sie dann auf **Richtlinien**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine neue Richtlinie zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Öffnen**.
3. Geben **Sie im Dialogfeld URL-Transformationsrichtlinie erstellen** oder **URL-Transformationsrichtlinie konfigurieren** Werte für die Parameter ein oder wählen Sie sie aus. Der Inhalt des Dialogfelds entspricht den unter Parameter für die Konfiguration von URL-Transformationsrichtlinien beschriebenen Parametern wie folgt (Sternchen gibt einen erforderlichen Parameter an):
   - Name* — Name (Für eine zuvor konfigurierte Richtlinie kann nicht geändert werden.)
   - Profil* — Profilname
   - Ausdruck — Regel

   Wenn Sie Hilfe beim Erstellen eines Ausdrucks für eine neue Richtlinie benötigen, können Sie entweder die Steuerungstaste gedrückt halten und die Leertaste drücken, während sich der Cursor im Textfeld Ausdruck befindet. Um den Ausdruck zu erstellen, können Sie ihn direkt wie unten beschrieben eingeben, oder Sie können das Dialogfeld Ausdruck hinzufügen verwenden.
4. Klicken Sie auf **Präfix**, und wählen Sie das Präfix für Ihren Ausdruck aus.

   Ihre Auswahlmöglichkeiten:
   - HTTP — Das HTTP-Protokoll. Wählen Sie diese Option, wenn Sie einen Aspekt der Anforderung untersuchen möchten, die sich auf das HTTP-Protokoll bezieht.

- SYS: Die geschützte Website (en). Wählen Sie diese Option, wenn Sie einen Aspekt der Anforderung untersuchen möchten, der sich auf den Empfänger der Anforderung bezieht.
- CLIENT: Der Computer, der die Anforderung gesendet hat. Wählen Sie diese Option, wenn Sie einen Aspekt des Absenders der Anfrage untersuchen möchten.
- SERVER: Der Computer, an den die Anforderung gesendet wurde. Wählen Sie diese Option, wenn Sie einen Aspekt des Empfängers der Anfrage untersuchen möchten.
- URL: Die URL der Anforderung. Wählen Sie diese Option, wenn Sie einen Aspekt der URL untersuchen möchten, an die die Anforderung gesendet wurde.
- TEXT: Eine beliebige Textzeichenfolge in der Anforderung. Wählen Sie diese Option, wenn Sie eine Textzeichenfolge in der Anforderung untersuchen möchten.
- TARGET: Das Ziel der Anforderung. Wählen Sie diese Option, wenn Sie einen Aspekt des Anforderungsziels untersuchen möchten.

Nachdem Sie ein Präfix ausgewählt haben, zeigt das Citrix ADC ein zweiteiliges Eingabeaufforderungsfenster an, in dem die möglichen nächsten Auswahlmöglichkeiten oben angezeigt werden, und eine kurze Erläuterung darüber, was die ausgewählte Auswahl am unteren Rand bedeutet. Die Auswahl hängt davon ab, welches Präfix Sie gewählt haben.

5. Wählen Sie Ihren nächsten Begriff aus.

Wenn Sie HTTP als Präfix gewählt haben, wählen Sie REQ, das HTTP-Anforderungen angibt, und RES, das HTTP-Antworten angibt. Wenn Sie ein anderes Präfix gewählt haben, sind Ihre Auswahlmöglichkeiten vielfältiger. Um Hilfe zu einer bestimmten Auswahl zu erhalten, klicken Sie einmal auf diese Auswahl, um Informationen darüber im unteren Eingabeaufforderungsfenster anzuzeigen.

Wenn Sie sicher sind, welche Auswahl Sie möchten, doppelklicken Sie darauf, um sie in das Fenster Ausdruck einzufügen.

1. Geben Sie einen Zeitraum ein, und fahren Sie mit der Auswahl von Begriffen in den Listenfeldern fort, die rechts neben dem vorherigen Listenfeld angezeigt werden. Geben Sie die entsprechenden Textzeichenfolgen oder Zahlen in die Textfelder ein, die angezeigt werden, um Sie zur Eingabe eines Werts auffordern, bis der Ausdruck beendet ist.
2. Klicken Sie auf **Erstellen** oder **OK**, je nachdem, ob Sie eine neue Richtlinie erstellen oder eine vorhandene Richtlinie ändern.
3. Klicken Sie auf **Schließen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich konfiguriert wurde.

So fügen Sie einen Ausdruck mithilfe des Dialogfelds Ausdruck hinzufügen hinzu

1. Klicken Sie im Dialogfeld **Responderaktion erstellen** oder **Responderaktion konfigurieren** auf **Hinzufügen**.
2. Wählen **Sie im Dialogfeld Ausdruck hinzufügen** im ersten Listenfeld den ersten Begriff für Ihren Ausdruck aus.
   - HTTP Das HTTP-Protokoll. Wählen Sie diese Option, wenn Sie einen Aspekt der Anforderung untersuchen möchten, die sich auf das HTTP-Protokoll bezieht.
   - SYS. Die geschützte Website(s). Wählen Sie diese Option, wenn Sie einen Aspekt der Anforderung untersuchen möchten, der sich auf den Empfänger der Anforderung bezieht.
   - CLIENT. Der Computer, der die Anforderung gesendet hat. Wählen Sie diese Option, wenn Sie einen Aspekt des Absenders der Anfrage untersuchen möchten.
   - SERVER. Der Computer, an den die Anforderung gesendet wurde. Wählen Sie diese Option, wenn Sie einen Aspekt des Empfängers der Anfrage untersuchen möchten.
   - -URL. Die URL der Anforderung. Wählen Sie diese Option, wenn Sie einen Aspekt der URL untersuchen möchten, an die die Anforderung gesendet wurde.
   - TEXT. Jede Textzeichenfolge in der Anforderung. Wählen Sie diese Option, wenn Sie eine Textzeichenfolge in der Anforderung untersuchen möchten.
   - TARGET. Das Ziel der Anforderung. Wählen Sie diese Option, wenn Sie einen Aspekt des Anforderungsziels untersuchen möchten.

     Wenn Sie Ihre Wahl treffen, werden im Listenfeld ganz rechts die entsprechenden Begriffe für den nächsten Teil des Ausdrucks aufgeführt.
3. Wählen Sie im zweiten Listenfeld den zweiten Begriff für Ihren Ausdruck aus. Die Auswahlmöglichkeiten hängen davon ab, welche Auswahl Sie im vorherigen Schritt getroffen haben, und sind dem Kontext angemessen. Nachdem Sie Ihre zweite Wahl getroffen haben, zeigt das Hilfefenster unterhalb des Fensters Ausdruck erstellen (das leer war) Hilfe an, in dem der Zweck und die Verwendung des gerade ausgewählten Begriffs beschrieben wird.
4. Fahren Sie fort, Begriffe aus den Listenfeldern auszuwählen, die rechts neben dem vorherigen Listenfeld angezeigt werden, oder geben Sie Zeichenfolgen oder Zahlen in die Textfelder ein, die Sie zur Eingabe eines Werts auffordern, bis der Ausdruck beendet ist.

Globally Binding-URL-Transformationsrichtlinien

October 5, 2021

Nachdem Sie die URL-Transformationsrichtlinien konfiguriert haben, binden Sie sie an Global oder an einen Bindepunkt, um sie in Kraft zu setzen. Nach der Bindung wird jede Anforderung oder

Antwort, die einer URL-Transformationsrichtlinie entspricht, durch das Profil umgewandelt, das dieser Richtlinie zugeordnet ist.

Wenn Sie eine Richtlinie binden, weisen Sie ihr eine Priorität zu. Die Priorität bestimmt die Reihenfolge, in der die von Ihnen definierten Richtlinien ausgewertet werden. Sie können die Priorität auf eine beliebige positive Ganzzahl festlegen. Im Citrix ADC Betriebssystem funktionieren Richtlinienprioritäten in umgekehrter Reihenfolge - je höher die Zahl, desto niedriger die Priorität.

Da die URL-Transformationsfunktion nur die erste Richtlinie implementiert, mit der eine Anforderung übereinstimmt, und keine zusätzlichen Richtlinien, die ebenfalls übereinstimmen, ist die Richtlinienpriorität wichtig, um die gewünschten Ergebnisse zu erzielen. Wenn Sie Ihrer ersten Richtlinie eine niedrige Priorität einräumen (z. B. 1000), weisen Sie den Citrix ADC an, diese nur auszuführen, wenn andere Richtlinien mit höherer Priorität nicht mit einer Anforderung übereinstimmen. Wenn Sie Ihrer ersten Richtlinie eine hohe Priorität einräumen (z. B. 1), weisen Sie den Citrix ADC an, sie zuerst auszuführen, und überspringen alle anderen Richtlinien, die möglicherweise ebenfalls übereinstimmen. Sie können sich viel Raum lassen, andere Richtlinien in beliebiger Reihenfolge hinzuzufügen, ohne Prioritäten neu zuweisen zu müssen, indem Sie Prioritäten mit Intervallen von 50 oder 100 zwischen jeder Richtlinie festlegen, wenn Sie Ihre Richtlinien global binden.

Hinweis: URL-Transformationsrichtlinien können nicht an TCP-basierte virtuelle Server gebunden werden.

So binden Sie eine URL-Transformationsrichtlinie mit der Citrix ADC Befehlszeile

Geben Sie an der Citrix ADC Eingabeaufforderung die folgenden Befehle ein, um eine URL-Transformationsrichtlinie global zu binden und die Konfiguration zu überprüfen:

- `bind transform global <policyName> <priority>`
- `show transform global`

Beispiel:

```
> bind transform global polisearching 100
 Done
> show transform global
1)      Policy Name: polisearching
        Priority: 100

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


So binden Sie eine URL-Transformationsrichtlinie mit dem Konfigurationsdienstprogramm

1. Erweitern Sie im Navigationsbereich Umschreiben, dann URL-Transformation, und klicken Sie dann auf **Richtlinien.
2. Klicken Sie im Detailbereich auf **Richtlinien-Manager**.
3. Wählen Sie im Dialogfeld **Richtlinien-Manager transformieren** den Bindepunkt aus, an den Sie die Richtlinie binden möchten**. Folgende Möglichkeiten stehen zur Auswahl:
    - **Global überschreiben.** Richtlinien, die an diesen Bindungspunkt gebunden sind, verarbeiten den gesamten Datenverkehr von allen Schnittstellen der Citrix ADC Appliance und werden vor allen anderen Richtlinien angewendet.
    - **Virtueller LB Server.** Richtlinien, die an einen virtuellen Lastausgleichsserver gebunden sind, werden nur auf Datenverkehr angewendet, der von diesem virtuellen Lastausgleichsserver verarbeitet wird, und werden vor allen globalen Standardrichtlinien angewendet. Nachdem Sie LB Virtual Server ausgewählt haben, müssen Sie auch den spezifischen virtuellen Lastausgleichsserver auswählen, an den Sie diese Richtlinie binden möchten.
    - **CS Virtual Server.** Richtlinien, die an einen virtuellen Content Switching-Server gebunden sind, werden nur auf Datenverkehr angewendet, der von diesem virtuellen Content Switching-Server verarbeitet wird, und werden vor allen globalen Standardrichtlinien angewendet. Nachdem Sie CS Virtual Server ausgewählt haben, müssen Sie auch den spezifischen virtuellen Content Switching-Server auswählen, an den Sie diese Richtlinie binden möchten.
    - **Standard Global.** Richtlinien, die an diesen Bindungspunkt gebunden sind, verarbeiten den gesamten Datenverkehr von allen Schnittstellen der Citrix ADC Appliance.
    - **Richtlinienbezeichnung.** Richtlinien, die an eine Richtlinienbeschriftung gebunden sind, verarbeiten Datenverkehr, den die Richtlinienbeschriftung an sie weiterleitet. Die Richtlinienbezeichnung steuert die Reihenfolge, in der Richtlinien auf diesen Datenverkehr angewendet werden.
4. Wählen Sie Richtlinie einfügen aus, um eine neue Zeile einzufügen und eine Dropdownliste mit allen verfügbaren, ungebundenen URL-Transformationsrichtlinien anzuzeigen.
5. Wählen Sie die Richtlinie aus, die Sie binden möchten, oder wählen Sie Neue Richtlinie aus, um eine neue Richtlinie zu erstellen. Die ausgewählte oder erstellte Richtlinie wird in die Liste der global gebundenen URL-Transformationsrichtlinien eingefügt.
6. Nehmen Sie zusätzliche Anpassungen an der Bindung vor.
    - Um die Richtlinienpriorität zu ändern, klicken Sie auf das Feld, um es zu aktivieren, und geben Sie dann eine neue Priorität ein. Sie können auch Prioritäten neu generieren wählen, um die Prioritäten gleichmäßig neu zu nummerieren.
    - Um den Richtlinienausdruck zu ändern, doppelklicken Sie auf dieses Feld, um das Dialogfeld Transformationsrichtlinie konfigurieren zu öffnen, in dem Sie den Richtlinienausdruck bearbeiten können.

- Zum Festlegen des Gehen-Ausdrucks doppelklicken Sie auf das Feld in der Spaltenüberschrift Gehe zu Ausdruck, um die Dropdownliste anzuzeigen, in der Sie einen Ausdruck auswählen können.
- Um die Option Invoke festzulegen, doppelklicken Sie auf das Feld in der Spaltenüberschrift Invoke, um die Dropdownliste anzuzeigen, in der Sie einen Ausdruck auswählen können.

7. Wiederholen Sie die Schritte 3 bis 6, um zusätzliche URL-Transformationsrichtlinien hinzuzufügen, die Sie global binden möchten.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich konfiguriert wurde.

RADIUS-Unterstützung für das Rewrite-Feature

October 5, 2021

Die Citrix ADC Ausdruckssprache enthält Ausdrücke, die Informationen aus RADIUS-Nachrichten in Anforderungen und Antworten extrahieren und bearbeiten können. Mit diesen Ausdrücken können Sie die Funktion Umschreiben verwenden, um Teile einer RADIUS-Nachricht zu ändern, bevor sie an ihr Ziel gesendet wird. Ihre Umschreibungsrichtlinien und -aktionen können einen beliebigen Ausdruck verwenden, der für eine RADIUS-Nachricht geeignet oder relevant ist. Mit den verfügbaren Ausdrücken können Sie den RADIUS-Nachrichtentyp identifizieren, ein beliebiges Attributwertpaar (AVP) aus der Verbindung extrahieren und RADIUS-AVPs ändern. Sie können auch Richtlinienbeschriftungen für RADIUS-Verbindungen erstellen.

Sie können die neuen RADIUS-Ausdrücke in Rewrite-Regeln für eine Reihe von Zwecken verwenden. Zum Beispiel könnten Sie:

- Entfernen Sie den Domänenbereich des RADIUS-Benutzernamens AVP, um Single Sign-On (SSO) zu vereinfachen.
- Fügen Sie einen herstellerspezifischen AVP ein, z. B. das MSISDN-Feld, das im Telefonbetriebsbetrieb verwendet wird, um Teilnehmerinformationen zu enthalten.

Sie können auch Richtlinienbeschriftungen erstellen, um bestimmte Arten von RADIUS-Anforderungen durch eine Reihe von Richtlinien weiterzuleiten, die für diese Anforderungen geeignet sind.

> **Hinweis**:
>
> RADIUS for Rewrite hat folgende Einschränkungen:

- Das Citrix ADC signiert nicht neu geschriebene RADIUS-Anforderungen oder Antworten neu. Wenn der RADIUS-Authentifizierungsserver signierte RADIUS-Nachrichten erfordert, schlägt die Authentifizierung fehl.
- Die aktuell verfügbaren RADIUS-Ausdrücke funktionieren nicht mit RADIUS-IPv6-Attributen.

Die Citrix ADC Dokumentation für Ausdrücke, die RADIUS unterstützen, setzt voraus, dass sie mit der grundlegenden Struktur und dem Zweck der RADIUS-Kommunikation vertraut sind. Wenn Sie weitere Informationen zu RADIUS benötigen, lesen Sie Ihre RADIUS-Serverdokumentation oder suchen Sie online nach einer Einführung in das RADIUS-Protokoll.

Konfigurieren von Rewrite-Richtlinien für RADIUS

Das folgende Verfahren verwendet die Citrix ADC Befehlszeile, um eine Umschreibungsaktion und -richtlinie zu konfigurieren und die Richtlinie an einen neu schreibspezifischen globalen Bindungspunkt zu binden.

So konfigurieren Sie eine Umschreibungsaktion und -richtlinie und binden die Richtlinie:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add rewrite action <actName> <actType>`
- `add rewrite policy <polName> <rule> <actName>`
- bind rewrite policy <polName> <priority> <nextExpr> -type <bindPoint><bindPoint>““ wobei einen der Wiederbeschreibungsspezifischen globalen Bindungspunkte darstellt.

RADIUS-Ausdrücke für Umschreiben

In einer Rewrite-Konfiguration können Sie die folgenden Citrix ADC Ausdrücke verwenden, um auf verschiedene Teile einer RADIUS-Anforderung oder -Antwort zu verweisen.

Identifizieren der Art der Verbindung:

- `RADIUS.IS_CLIENT`

  Gibt TRUE zurück, wenn die Verbindung eine RADIUS-Client-Meldung (Anfrage) ist.

- `RADIUS.IS_SERVER`

  Gibt TRUE zurück, wenn die Verbindung eine RADIUS-Servermeldung (Antwort) ist.

Anforderungsausdrücke:

- `RADIUS.REQ.CODE`

  Gibt die Nummer zurück, die dem RADIUS-Anforderungstyp entspricht. Eine Ableitung der num_at-Klasse. Beispielsweise würde eine RADIUS-Zugriffsanforderung 1 (eins) zurückgeben. Eine RADIUS-Buchhaltungsanforderung würde 4 zurückgeben.

- `RADIUS.REQ.LENGTH`

  Gibt die Länge der RADIUS-Anforderung einschließlich des Headers zurück. Eine Ableitung der num_at-Klasse.

- `RADIUS.REQ.IDENTIFIER`

  Gibt die RADIUS-Anforderungskennung zurück, eine Nummer, die jeder Anforderung zugewiesen ist, die es ermöglicht, die Anforderung mit der entsprechenden Antwort abzugleichen. Eine Ableitung der
  num_at-Klasse.

- `RADIUS.REQ.AVP(<AVP Code No>).VALUE`

  Gibt den Wert des ersten Vorkommens dieses AVP als Zeichenfolge vom Typ
  text_t zurück.

- `RADIUS.REQ.AVP(<AVP code no>).INSTANCE(instance number)`

  Gibt die angegebene Instanz des AVP als Zeichenfolge vom Typ RAVP_t zurück. Ein bestimmter RADIUS-AVP kann mehrmals in einer RADIUS-Meldung auftreten. INSTANCE (0) gibt die erste Instanz zurück, INSTANCE (1) gibt die zweite Instanz zurück usw. bis zu sechzehn Instanzen.

- `RADIUS.REQ.AVP(<AVP code no>).VALUE(instance number)`

  Gibt den Wert der angegebenen Instanz des AVP als Zeichenfolge vom Typ
  text_t zurück.

- `RADIUS.REQ.AVP(<AVP code no>).COUNT`

  Gibt die Anzahl der Instanzen eines bestimmten AVP in einer RADIUS-Verbindung als Ganzzahl zurück.

- `RADIUS.REQ.AVP(<AVP code no>).EXISTS`

  Gibt TRUE zurück, wenn der angegebene Typ von AVP in der Nachricht vorhanden ist, oder FALSE, wenn dies nicht der Fall ist.

Response-Ausdrücke:

RADIUS-Antwortausdrücke sind identisch mit RADIUS-Anforderungsausdrücken, mit der Ausnahme, dass RES REQ ersetzt.

Typecasts von AVP-Werten:

Der ADC unterstützt Ausdrücke, um RADIUS-AVP-Werte für Text, Ganzzahl, Ganzzahl ohne Vorzeichen, lang, unsigned long, ipv4-Adresse, ipv6-Adresse, ipv6-Präfix und Zeitdatentypen zu typisieren. Die Syntax ist die gleiche wie bei anderen Citrix ADC -Typecast-Ausdrücken.

Beispiel:

Der ADC unterstützt Ausdrücke, um RADIUS-AVP-Werte für Text, Ganzzahl, Ganzzahl ohne Vorzeichen, lang, unsigned long, ipv4-Adresse, ipv6-Adresse, ipv6-Präfix und Zeitdatentypen zu typisieren. Die Syntax ist die gleiche wie bei anderen Citrix ADC -Typecast-Ausdrücken.


```
RADIUS.REQ.AVP(8).VALUE(0).typecast_ip_address_at
```

AVP-Typausdrücke:

Citrix ADC unterstützt Ausdrücke zum Extrahieren von RADIUS-AVP-Werten mit der zugewiesenen Ganzzahlcodes, die in RFC2865 und RFC2866 beschrieben sind. Sie können auch Textaliase verwenden, um dieselbe Aufgabe auszuführen. Einige Beispiele folgen.

- `RADIUS.REQ.AVP (1).VALUE or RADIUS.REQ.USERNAME.value`

  Extrahiert den RADIUS-Benutzernamenwert.

- `RADIUS.REQ.AVP (4). VALUE or RADIUS.REQ. ACCT\\_SESSION\\_ID.value`

  Extrahiert die Acct-Session-ID AVP (Code 44) aus der Nachricht.

- `RADIUS.REQ.AVP (26). VALUE or RADIUS.REQ.VENDOR\\_SPECIFIC.VALUE`

  Extrahiert den herstellerspezifischen Wert.

Die Werte der am häufigsten verwendeten RADIUS-AVPs können auf die gleiche Weise extrahiert werden.

RADIUS-Bindepunkte:

Für Richtlinien, die RADIUS-Ausdrücke enthalten, stehen vier globale Bindpunkte zur Verfügung.

- `RADIUS_REQ_OVERRIDE`

  Priorität/Überschreiben der Anforderungsrichtlinienwarteschlange.

- `RADIUS_REQ_DEFAULT`

  Standardanforderungsrichtlinienwarteschlange.

- `RADIUS_RES_OVERRIDE`

  Priorität/Überschreiben der Antwortrichtlinienwarteschlange.

- `RADIUS_RES_DEFAULT`

  Standardwarteschlange für Antwortrichtlinien.

RADIUS-Rewrite-spezifische Ausdrücke:

- `RADIUS.NEW_AVP`

  Gibt den angegebenen RADIUS AVP als String zurück.

- `RADIUS.NEW_AVP_INTEGER32`

  Gibt den angegebenen RADIUS AVP als Ganzzahl zurück.

- `RADIUS.NEW_AVP_UNSIGNED32`

  Gibt den angegebenen RADIUS AVP als Ganzzahl ohne Vorzeichen zurück.

- RADIUS.NEW_VENDOR_SPEC_AVP(<ID>, <definition>)

  Fügt der Verbindung die angegebenen erweiterten herstellerspezifischen AVPs hinzu. Für<ID>, ersetzen Sie eine lange Zahl. Ersetzen Sie für<definition>eine Zeichenfolge, die die Daten für den AVP enthält.

- RADIUS.REQ.AVP_START

  Gibt die Position zwischen dem Ende des RADIUS-Headers und dem Anfang der AVPs zurück. Wird in Umschreibaktionen verwendet.

  Beispiel:

```
1    add rewrite action insert1 insert_after radius.req.avp_start radius
        .new_avp(33, "NEW AVP")
```

- RADIUS.REQ.AVP_END

  Gibt die Position am Ende der Radiusnachricht (oder das Ende aller AVPs) in Radiusnachricht zurück. Wird beim Ausführen von Rewrite-Aktionen verwendet.

  Beispiel:

```
1    add rewrite action insert2 insert_before radius.req.avp_end "radius
        .new_avp(33, "NEW AVP")"
```

- RADIUS.REQ.AVP_LIST

  Gibt die Position am Anfang der AVPs in einer RADIUS-Nachricht und die Länge der RADIUS-Nachricht zurück, ohne den Header. Mit anderen Worten, gibt alle AVPs in einer RADIUS-Nachricht zurück. Wird verwendet, um Rewrite-Aktionen auszuführen.

  Beispiel:

```
1    add rewrite action insert3 insert_before_all radius.req.avp_list "
        radius.new_avp(33, "NEW AVP")" -search "avp(33)"
```

Gültige Rewrite-Aktionstypen für RADIUS:

Die Aktionstypen Umschreiben, die mit RADIUS-Ausdrücken verwendet werden können, sind:

- INSERT_AFTER
- INSERT_BEFORE
- INSERT_AFTER_ALL

- INSERT_BEFORE_ALL
- Löschen
- DELETE_ALL
- REPLACE
- REPLACE_ALL

Alle`INSERT_ actions` können verwendet werden, um einen RADIUS AVP in eine RADIUS-Verbindung einzufügen.

Anwendungsfälle

Im Folgenden sind Anwendungsfälle für RADIUS mit Rewrite.

Benutzername AVP neu schreiben

Um das Rewrite-Feature so zu konfigurieren, dass die Domain-Zeichenfolge aus dem RADIUS-Benutzernamen AVP entfernt wird, erstellen Sie zunächst eine Rewrite REPLACE -Aktion, wie im folgenden Beispiel dargestellt. Verwenden Sie die Aktion in einer Richtlinie Umschreiben, die alle RADIUS-Anforderungen auswählt. Binden Sie die Richtlinie an einen globalen Bindungspunkt. Legen Sie dabei die Priorität auf die entsprechende Ebene fest, damit alle Blockierungs- oder Ablehnungsrichtlinien zuerst wirksam werden. Stellen Sie jedoch sicher, dass alle Anforderungen, die nicht blockiert oder abgelehnt werden, neu geschrieben werden. Setzen Sie den Goto Expression (gotoPriorityExpr) auf NEXT, um die Richtlinienbewertung fortzusetzen, und fügen Sie die Richtlinie an die RADIUS_REQ_DEFAULT Warteschlange an.

Beispiel:

```
1 add rewrite action rwActRadiusDomainDel replace radius.req.user_name q/
     RADIUS.NEW_AVP(1,RADIUS.REQ.USER_NAME.VALUE.AFTER_STR(" "))/
2 add rewrite policy RadiusRemoveDomainPol true rwActRadiusDomainDel
```

> **Hinweis**:
>
> Die Richtlinie zum Umschreiben von RADIUS gilt nicht für einen virtuellen Gateway server. Wenn ein virtueller Gateway server ein Lastenausgleich verwendet wird, muss RADIUS konfiguriert werden, und die Rewrite-Richtlinie muss an einen virtuellen RADIUS-Lastausgleichsserver gebunden werden.

Einfügen eines herstellerspezifischen AVP

Um die Aktion Umschreiben so zu konfigurieren, dass ein herstellerspezifischer AVP eingefügt wird, der den Inhalt des MSISDN-Felds enthält, erstellen Sie zunächst eine neu schreibende INSERT-Aktion,

die das MSISDN-Feld in die Anforderung einfügt. Verwenden Sie die Aktion in einer Richtlinie Umschreiben, die alle RADIUS-Anforderungen auswählt. Binden Sie die Richtlinie an global, indem Sie die Priorität auf eine entsprechende Ebene und die anderen Parameter festlegen, wie im folgenden Beispiel gezeigt.

Beispiel:

```
1 add rewrite action rwActRadiusInsMSISDN insert_after radius.req.
     avp_start RADIUS.NEW_VENDOR_SPEC_AVP(<VENDOR ID>, "RADIUS.NEW_AVP(<
     Attribute Code>, <MSISDN>)")
2 add rewrite policy rwPolRadiusInsMSISDN true rwActRadiusInsMSISDN
3 bind rewrite global rwPolRadiusInsMSISDN 100 NEXT -type
     RADIUS_REQ_DEFAULT
```

‘‘‘

Diameter-Unterstützung für Umschreiben

October 5, 2021

Die Funktion Rewrite unterstützt jetzt das Diameter Protokoll. Sie können Rewrite so konfigurieren, dass Durchmesseranforderungen und -antwort wie HTTP- oder TCP-Anforderungen und -Antworten geändert werden, sodass Sie mithilfe von Rewrite den Ablauf von Durchmesseranforderungen verwalten und notwendige Änderungen vornehmen können. Wenn beispielsweise der Wert Ursprungs-Host in einer Durchmesseranforderung ungeeignet ist, können Sie ihn mit Rewrite durch einen Wert ersetzen, der für den Diameter Server akzeptabel ist.

So konfigurieren Sie Rewrite zum Ändern einer Durchmesseranforderung

Um die Funktion Umschreiben so zu konfigurieren, dass der Origin-Host in einer Durchmesseranforderung durch einen anderen Wert ersetzt wird, geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- <add rewrite action <actname> replace “DIAMETER.REQ.AVP (264,\“Citrix ADC.example.net\”)” Für <actname> ersetzen Sie einen Namen für Ihre neue Aktion. Der Name kann aus einem bis 127 Zeichen bestehen und kann Buchstaben, Zahlen sowie Bindestriche (-) und Unterstriche (_) enthalten. Ersetzen Sie für Citrix ADC.example.net den Host-Origin, den Sie anstelle des ursprünglichen Host-Namens verwenden möchten.
- add rewrite policy <polname> “diameter.req.avp(264).value.eq(\“host.example.com\”)” <actname>

Für <polname>, ersetzen Sie einen Namen für Ihre neue Richtlinie. Wie bei <actname> kann der Name aus einem bis 127 Zeichen bestehen und kann Buchstaben, Zahlen sowie Bindestriche (-) und Unterstriche (_) enthalten. Ersetzen Sie für host.example.com den Namen des Host-Origin, den Sie ändern möchten. Für <actname> ersetzen Sie den Namen der Aktion, die Sie gerade erstellt haben.

- bind lb vserver <vservername> -policyName <polname> -priority <priority> -type REQUEST
  For <vservername>, substitute the name of the load balancing virtual server to which you want to bind the policy. <polname>Ersetzen Sie den Namen der Richtlinie, die Sie gerade erstellt haben. Für <priority> ersetzen Sie eine Priorität für die Richtlinie.

Beispiel:

Um eine Umschreibung Aktion und Richtlinie zu erstellen, um alle Diameter Host-Origins von host.example.com in Citrix ADC.example.net zu ändern, können Sie die folgende Aktion und Richtlinie hinzufügen und die Richtlinie wie gezeigt binden.

```
1 > add rewrite action rw_act_replace_avp replace ”diameter.req.avp(264)”
      ”diameter.new.avp(264,”Citrix ADC.example.net”)”
2 > add rewrite policy rw_diam_pol ”diameter.req.avp(264).value.eq(”
     client.realm2.net”)” rw_act_replace_avp
3 > bind lb vserver vs1 -policyName rw_diam_pol -priority 10 -type
     REQUEST
4
5 Done
6 <!--NeedCopy-->
```

DNS-Unterstützung für das Rewrite-Feature

October 5, 2021

Sie können die Funktion zum Umschreiben konfigurieren, um DNS-Anforderungen und -Antworten zu ändern, wie für HTTP- oder TCP-Anforderungen und -Antworten. Sie können Rewrite verwenden, um den Fluss von DNS-Anforderungen zu verwalten und notwendige Änderungen im Header oder im Antwortbereich vorzunehmen. Wenn für die DNS-Antwort beispielsweise nicht das AA-Bit im Header-Flag festgelegt ist, können Sie mit Rewrite das AA-Bit in der DNS-Antwort festlegen und es an den Client senden.

DNS-Ausdrücke

In einer Rewrite-Konfiguration können Sie die folgenden Citrix ADC Ausdrücke verwenden, um auf verschiedene Teile einer DNS-Anforderung oder -Antwort zu verweisen:

Siehe Ausdrücke und Beschreibungen

DNS-Bindungspunkte

Die folgenden globalen Bindungspunkte sind für Richtlinien verfügbar, die DNS-Ausdrücke enthalten.

Punkte binden	Beschreibung
DNS_REQ_OVERRIDE	Überschreiben Sie die Anforderungsrichtlinienwarteschlange.
DNS_REQ_DEFAULT	Standardanforderungsrichtlinienwarteschlange.
DNS_RES_OVERRIDE	Überschreiben der Antwortrichtlinienwarteschlange.
DNS_RES_DEFAULT	Standardwarteschlange für Antwortrichtlinien.

Zusätzlich zu den Standardverbindungspunkten können Sie Richtlinienbeschriftungen vom Typ DNS_REQ oder DNS_RES erstellen und DNS-Richtlinien an diese binden.

Umschreiben von Aktionstypen für DNS

- **replace_dns_answer_section**—Diese Aktion ersetzt den DNS-Antwortabschnitt durch den definierten Ausdruck in der DNS-Richtlinie.
- **replace_dns_header_field**—Überprüft den Opcode-Typ in der DNS-Anforderung. Gibt True oder False zurück, der angibt, ob der Opcode-Typ in der DNS-Anforderung mit dem angegebenen Opcode-Typ übereinstimmt. Diese Aktion ersetzt den DNS-Header-Abschnitt durch den definierten Ausdruck in der DNS-Richtlinie.

Konfigurieren von Rewrite-Richtlinien für DNS

Das folgende Verfahren verwendet die Citrix ADC Befehlszeile, um eine Umschreibungsaktion und -richtlinie zu konfigurieren und die Richtlinie an einen neu schreibspezifischen globalen Bindungspunkt zu binden.

Aktion und Richtlinie neu schreiben konfigurieren und die Richtlinie für DNS binden

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

1. `add rewrite action <actName> <actType>`

   Ersetzen Sie `<actname>` durch einen Namen für Ihre neue Aktion. Der Name kann 1 bis 127 Zeichen lang sein und kann Buchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten. Geben Sie für `<actType>` die für DNS-Ausdrücke bereitgestellten Umschreibungsaktionstypen an.

2. `add rewrite policy <polName> <rule> <actName>`

   Ersetzen Sie `<polname>` durch einen Namen für Ihre neue Richtlinie. Für `<actname>` kann der Name 1 bis 127 Zeichen lang sein und kann Buchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten. Ersetzen Sie `<actname>` durch den Namen der Aktion, die Sie gerade erstellt haben.

3. `bind rewrite global <polName> <priority> <gotoPriorityExpression> -type <bindPoint>`

   Ersetzen Sie `<polName>` durch den Namen der Richtlinie, die Sie gerade erstellt haben. Geben Sie für `<priority>` die Priorität der Richtlinie an. Ersetzen Sie `<bindPoint>` durch einen der rewrite-spezifischen globalen Bindpunkte.

Beispiel:

Legen Sie das AA-Bit der DNS-Anforderung für den Lastenausgleich virtuellen Server fest.

Mit den folgenden Befehlen wird die Citrix ADC Appliance so konfiguriert, dass sie als autorisierender DNS-Server für alle von ihr bereiteten Abfragen fungiert.

```
1 add rewrite action set_aa replace_dns_header_field dns.req.header.flags
     .set(aa)
2 add rewrite policy pol !dns.req.header.flags.is_set(aa)  set_aa
3 bind rewrite global  pol  100  -type dns_res_override
4 <!--NeedCopy-->
```

Ändern Sie die Antwortantwort und den Kopfzeilenabschnitt.

Wenn der Server mit einer NX-Domäne antwortet, können Sie die Umschreibungsaktion so einstellen, dass die Antwort durch die angegebene IP-Adresse ersetzt wird. Ein NOPOLICY-REWRITE ermöglicht es Ihnen, eine externe Bank aufzurufen, ohne einen Ausdruck (eine Regel) zu verarbeiten. Dieser Eintrag ist eine Dummy-Richtlinie, die keine Regel enthält, sondern den Eintrag an eine Richtlinienbezeichnung oder virtuelle serverspezifische Richtlinienbanken weiterleitet.


```
add rewrite action set_aa_res replace_dns_header_field "dns.res.header.flags.set(aa)"
add rewrite action modify_nxdomain_res replace_dns_answer_section "dns.new_rrset_a("10.102.218.160",300)"
add rewrite policy set_res_aa true set_aa_res
add add rewrite policy modify_answer "dns.RES.HEADER.RCODE.EQ(nxdomain) && dns.RES.QUESTION.TYPE.EQ(A)"
modify_nxdomain_res
add rewrite policylabel MODIFY_NODATA dns_res
bind rewrite policylabel MODIFY_NODATA modify_answer 10 END
bind rewrite policylabel MODIFY_NODATA set_res_aa 11 END
bind lb vserver v1 -policyName NOPOLICY-REWRITE -priority 11 -gotoPriorityExpression END -type
RESPONSE -invoke policylabel MODIFY_NODATA
<!--NeedCopy-->
```

Einschränkungen:

- Rewrite-Richtlinien werden nur dann ausgewertet, wenn die Citrix ADC Appliance als DNS-Proxyserver konfiguriert ist und ein Cache-Fehler vorliegt.
- Wenn das Flag Recursion Available (RA) im Header auf YES gesetzt ist, wird das RA-Flag bei den Rewrites nicht geändert.
- Wenn das RA-Flag im Header auf YES gesetzt ist, wird das CD-Flag im Header unabhängig von einer Umschreibung geändert.

String-Maps

October 5, 2021

Sie können Zeichenfolgenzuordnungen verwenden, um Musterabgleich in allen Citrix ADC Features durchzuführen, die die Standardrichtliniensyntax verwenden. Eine Zeichenfolgenzuordnung ist eine Citrix ADC Entität, die aus Schlüssel-Wert-Paaren besteht. Die Schlüssel und Werte sind Zeichenfolgen im ASCII- oder UTF-8-Format. Der String-Vergleich verwendet zwei neue Funktionen `MAP_STRING(<string_map_name>)` und `IS_STRINGMAP_KEY(<string_map_name>)`.

Eine Richtlinienkonfiguration, die Zeichenfolgenzuordnungen verwendet, ist besser als eine, die Zeichenfolgenabgleich über Richtlinienausdrücke durchführt, und Sie benötigen weniger Richtlinien, um Zeichenfolgenabgleich mit einer großen Anzahl von Schlüssel-Wert-Paaren durchzuführen. String-Maps sind auch intuitiv, einfach zu konfigurieren und führen zu einer kleineren Konfiguration.

Funktionsweise von String-Maps

String-Maps sind in der Struktur ähnlich wie Mustersätze (ein Mustersatz definiert eine Zuordnung von Indexwerten zu Strings; eine String-Map definiert eine Zuordnung von Strings zu Strings) und die Konfigurationsbefehle für String-Maps (Befehle wie add, bind, unbind, remove und show) sind syntaktisch ähnlich der Konfiguration -Befehle für Mustersätze. Wie bei Indexwerten in einem Mustersatz muss jeder Schlüssel in einer Zeichenfolgenzuordnung auf der Karte eindeutig sein. Die folgende Tabelle zeigt eine String-Map namens url_string_map, die URLs als Schlüssel und Werte enthält.

Key	Wert
/url_1.html	http://www.redirect_url_1.com/url_1.html
/url_2.html	http://www.redirect_url_2.com/url_2.html
/url_3.html	http://www.redirect_url_1.com/url_1.html

Tabelle 1. String-Map url_string_map

In der folgenden Tabelle werden die beiden Funktionen beschrieben, die eingeführt wurden, um den Zeichenfolgenabgleich mit Schlüsseln in einer Zeichenfolgenzuordnung zu aktivieren. String-Matching wird immer mit den Tasten durchgeführt. Darüber hinaus führen die folgenden Funktionen einen Vergleich zwischen den Tasten in der Zeichenfolgenzuordnung und der vollständigen Zeichenfolge durch, die vom Ausdruckspräfix zurückgegeben wird. Die Beispiele in den Beschreibungen beziehen sich auf das vorangehende Beispiel.

Vollendete Informationen zu den beiden Funktionen, die zum Aktivieren des String-Abgleichs mit Schlüsseln in einer String-Map eingeführt wurden, finden Sie unter String Map Funktionstabelle pdf.

Konfigurieren einer Zeichenfolgenzuordnung

Sie erstellen zuerst eine String-Map und binden dann Schlüssel-Wert-Paare an sie. Sie können eine Zeichenfolgenzuordnung über die Befehlszeilenschnittstelle (CLI) oder das Konfigurationsdienstprogramm erstellen.

So konfigurieren Sie eine Zeichenfolgenzuordnung mit der Befehlszeilenschnittstelle

Führen Sie an der Eingabeaufforderung die folgenden Schritte aus:

1. Erstellen Sie eine Zeichenfolgenzuordnung.

```
add policy stringmap <name> -comment <string>
```


1. Binden Sie ein Schlüssel-Wert-Paar an die Zeichenfolgenzuordnung.

```
bind policy stringmap <name> <key> <value> [-comment <string>]
```

Beispiel:

```
1 bind policy stringmap url_string_map1 ”/url_1.html” ”http://www.
     redirect_url_1.com/url_1.html”
2 <!--NeedCopy-->
```

So konfigurieren Sie eine Zeichenfolgenzuordnung über die Citrix ADC GUI

Navigieren Sie zu **AppExpert** > **String-Maps**, klicken Sie auf **Hinzufügen** und geben Sie die relevanten Details an.

Beispiel: Responder-Richtlinie mit einer Umleitungsaktion

Der folgende Anwendungsfall umfasst eine Responder-Richtlinie mit einer Umleitungsaktion. Im folgenden Beispiel erstellen die ersten vier Befehle die Zeichenfolgenzuordnung url_string_map und binden die drei Schlüssel-Wert-Paare, die im vorherigen Beispiel verwendet wurden. Nachdem Sie die Zuordnung erstellt und die Schlüssel-Wert-Paare gebunden haben, erstellen Sie eine Responder-Aktion (act_url_redirects), die den Client auf die entsprechende URL in der String-Map oder auf www.default.com umleitet. Außerdem konfigurieren Sie eine Responderrichtlinie (pol_url_redirects), die prüft, ob angeforderte URLs mit einem der Schlüssel in url_string_map übereinstimmen und dann die konfigurierte Aktion ausführt. Schließlich binden Sie die Responder-Richtlinie an den virtuellen Content Switching-Server, der die Clientanforderungen empfängt, die ausgewertet werden sollen.

```
add stringmap url_string_map

bind stringmap url_string_map /url_1.html http://www.redirect_url_1.com/
url_1.html

bind stringmap url_string_map /url_2.html http://www.redirect_url_2.com/
url_2.html

bind stringmap url_string_map /url_3.html http://www.redirect_url_1.com/
url_1.html

add responder action act_url_redirects redirect 'HTTP.REQ.URL.MAP_STRING(”
url_string_map”)ALT ”www.default.com”'-bypassSafetyCheck yes

add responder policy pol_url_redirects TRUE act_url_redirects
```

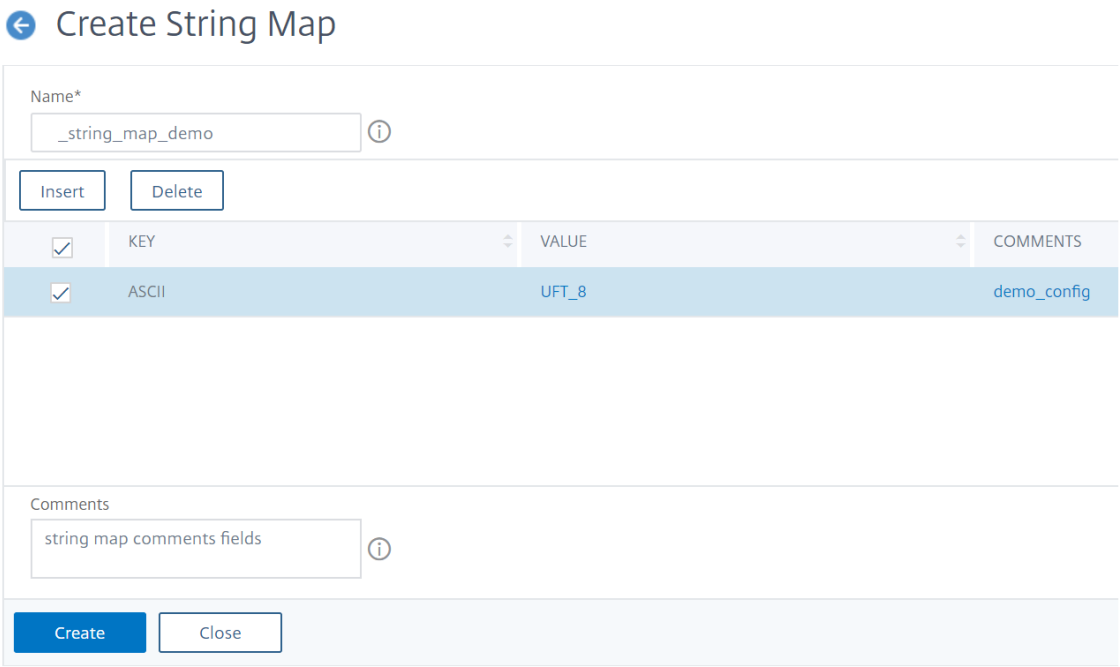


```
bind cs vserver csw_redirect -policyname pol_url_redirects -priority 1 -
type request
```

So konfigurieren Sie eine Zeichenfolgenzuordnung über die Citrix ADC GUI

Befolgen Sie das unten angegebene Verfahren, um eine Zeichenfolgenzuordnung zu konfigurieren.

1. Erweitern Sie im Navigationsbereich **AppExpert**, und klicken Sie auf **String-Maps**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **Zeichenfolgenzuordnung erstellen** die folgenden Parameter fest:
   - Name. Name der Zeichenfolgenzuordnung.
   - Schlüsselwert konfigurieren. ASCII-basierter Schlüsselwerteintrag, der an die Zeichenfolgenzuordnung gebunden ist
   - Kommentare. Eine kurze Beschreibung der Schlüsselwerte, die an die Zeichenfolgenzuordnung gebunden sind.
4. Klicken Sie auf **Erstellen** und **Schließen**.



URL-Sets

October 5, 2021

Mit dieser Funktion können Sie eine Million URLs in die Sperrliste eintragen. Der Abschnitt enthält die folgenden Themen:

Schnelleinstieg

October 5, 2021

Um den Zugriff auf eingeschränkte Websites zu verhindern, verwendet eine Citrix ADC Appliance einen speziellen URL-Übereinstimmungsalgorithmus. Der Algorithmus verwendet einen URL-Satz, der eine Liste von URLs bis zu 1 Million (1.000.000) Einträge auf der Sperrliste enthalten kann. Jeder Eintrag kann Metadaten enthalten, die URL-Kategorien und Kategoriegruppen als indizierte Muster definieren. Die Appliance kann auch regelmäßig URLs hochsensibler URLs herunterladen, die von Interneterzwingungsbehörden (mit Websites von Behörden) oder Internetorganisationen verwaltet werden. Sobald der URL-Satz von einer Website heruntergeladen und in die Appliance importiert wurde, verschlüsselt die Appliance die URL-Sets (wie von diesen Agenturen erforderlich) und sie werden vertraulich behandelt und die Einträge werden nicht manipuliert.

Die Citrix ADC Appliance verwendet erweiterte Richtlinien, um festzustellen, ob eine eingehende URL gesperrt, zugelassen oder umgeleitet werden muss. Diese Richtlinien verwenden erweiterte Ausdrücke, um eingehende URLs anhand von Einträgen aus der Sperrliste auszuwerten. Ein Eintrag kann Metadaten enthalten. Für Einträge, die keine Metadaten enthalten, sollten Sie möglicherweise einen Ausdruck verwenden, der die URL anhand einer exakten Zeichenfolgenübereinstimmung auswertet. Für andere URLs können Sie einen Ausdruck verwenden, der die Metadaten der URL auswertet, zusätzlich zu einem Ausdruck, der auf eine genaue Übereinstimmung mit der Zeichenfolge überprüft.

Anwendungsfall für sichere Internetzugriffsrichtlinien für ISPs/Telcos

Ein URL-Satz ermöglicht es einem ISP (ISP) oder einem Telco-Kunden, behördliche Richtlinien für den sicheren Internetzugang durchzusetzen, wie z. B.:

1. Sperrung des Zugriffs auf illegale Internetseiten (Kindesmissbrauch, Drogen usw.)
2. Sicheres Surfen für Kinder

Mit einer Citrix ADC Appliance können Sie regelmäßig URL-Sets herunterladen, die von Interneterzwingungsagenturen oder unabhängigen Internetorganisationen verwaltet werden. Die

Appliance lädt die Liste regelmäßig herunter und aktualisiert sie sicher. Die Liste wird als vertrauliche URL-Sätze gespeichert, sodass sie nicht manipuliert oder menschlich lesbar ist. Der regelmäßig heruntergeladene URL-Satz dient als Sperrliste für URL-Auswertungszwecke.

Wenn Sie eine private URL festgelegt haben und der Inhalt der Liste vertraulich behandelt werden und der Netzwerkadministrator keine Kenntnis von den in der Liste vorhandenen URLs auf der Sperrliste hat. Um sicherzustellen, dass die Richtlinie korrekt konfiguriert ist und auf die richtige Liste verwiesen wird, müssen Sie die Canary-URL konfigurieren und sie dem URL-Satz hinzufügen. Mithilfe der Canary-URL kann der Administrator über die Appliance die private URL anfordern, um sicherzustellen, dass sie für jede URL-Anforderung gesucht wird.

Erweiterte Richtlinienausdrücke für die URL-Auswertung

October 5, 2021

In der folgenden Tabelle werden die Ausdrücke beschrieben, mit denen Sie eingehende URLs mit Einträgen in einem URL-Set auswerten können.

Hinweis<URL expression>: HTTP.REQ.URL wird generalisiert, um als

Ausdruck	Vorgang
—	—
<URL expression>.URLSET_MATCHES_ANY	Wertet TRUE aus, wenn die URL genau mit einem Eintrag im URL-Set übereinstimmt.
<URL expression>.GET_URLSET_METADATA (<URLSET>)	Der Ausdruck GET_URLSET_METADATA () gibt die zugeordneten Metadaten zurück, wenn die URL genau einem Muster innerhalb des URL-Sets entspricht. Eine leere Zeichenfolge wird zurückgegeben, wenn keine Übereinstimmung vorhanden ist.
<URL expression>.GET_<URLSET>URLSET_METADATA () .EQ (<METADATA>	Wertet TRUE aus, wenn die übereinstimmenden Metadaten gleich sind <METADATA>.
<URL expression><URLSET>““.GET_URLSET_METADATA () .TYPECAST_LIST_T (‘,’) .GET (0) .EQ (<CATEGORY>) |Wertet TRUE aus, wenn sich die übereinstimmenden Metadaten am Anfang der Kategorie befindet. Dieses Muster kann verwendet werden, um separate Felder innerhalb von Metadaten zu kodieren, aber nur mit dem ersten Feld übereinstimmen.| |HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL) |Verbindet die Host- und URL-Parameter, die dann als`<URL expression>` Abgleich verwendet werden können.|<!--NeedCopy-->‘

Konfigurieren des URL-Sets

October 5, 2021

Sie können die folgenden Aufgaben ausführen, um einen URL-Satz zu konfigurieren und URLs auf einer Citrix ADC-Plattform einzuschränken:

1. Importieren Sie einen URL-Satz (laden Sie es herunter und verschlüsseln Sie es). Wenn Sie eine URL importieren, die in einer Citrix ADC-Appliance festgelegt ist, können Sie:

- Um die URL-Datei herunterzuladen.
- So fügen Sie die Datei der Appliance hinzu.
- Um die Datei zu verschlüsseln.
  Bis Sie die zum System festgelegte URL hinzufügen, ist sie für den Benutzer nicht sichtbar.

Sie können ein Set auf folgende Weise herunterladen:

- Laden Sie eine einmalig festgelegte URL von einem Remoteserver herunter und geben Sie sie als `http://myserver.com/file_with_urlset.csv`
- füge eine Datei unter dem `/var/tmp/` Pfad in ADC hinzu und verwende den Befehl wie im Beispiel:

```
> shell cat /var/tmp/test_urlset.csv
example.com
google.com
> import policy urlset top10
k -url local:test_urlset.csv -delimiter ”,” -rowSeparator ”n” -interval
    10 -privateSet -canaryUrl http://www.in.gr
Done

<!--NeedCopy-->
```

Der importierte URL-Satz wird weiter in verschiedene Kategorien und Kategoriegruppen in der Datenbank unterteilt. Dies ist nur gültig, wenn in den Metadaten der URL-Set-Datei Kategorien vorhanden sind.

Hinweis: Es besteht die Möglichkeit, dass Sie URL-Muster ohne Metadaten haben.

Nachdem Sie die Datei importiert haben, können Sie Dateieigenschaften aktualisieren, löschen oder anzeigen. Nachdem die Datei in die Appliance verschoben wurde, können Sie die Einträge ändern, indem Sie weitere Zeilen hinzufügen.

Der importierte Satz wird dann in einem verschlüsselten Dateiformat im Citrix ADC-Verzeichnis gespeichert. Die importierte Liste enthält Millionen von URL-Einträgen. Zu den folgenden “Die importierte

Liste kann bis zu 1 Million URL-Einträge enthalten. Andernfalls gibt die Appliance eine Fehlermeldung zurück, die besagt, dass der Wert den Grenzwert überschreitet. Wenn der importierte URL-Set Einträge auf der Sperrliste mit Metadaten enthält, werden die Metadaten von der Appliance beim Importieren erkannt.

Nachdem Sie einen URL-Satz importiert und zur Appliance hinzugefügt haben, steht der URL-Set für erweiterte Richtlinien zur Identifizierung der korrekten URL zur Verfügung, die während der eingehenden URL-Auswertung festgelegt wurde. `HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URLSET_MATCHES_ANY(<URL set name>)`

1. Aktualisieren einer auf der Citrix ADC-Appliance festgelegten URL. Nachdem Sie die Datei in die Appliance verschoben haben, können Sie in diesem Intervall eine URL-Datei mithilfe der Befehlszeilenschnittstelle manuell aktualisieren.
2. Exportieren eines URL-Sets. Wenn Sie eine Backup des URL-Sets bevorzugen, können Sie die Liste der URL-Muster exportieren und eine Kopie davon unter einer Ziel-URL speichern. Überprüfen Sie vor dem Exportieren, ob der URL-Satz als privat gekennzeichnet ist. Wenn als privat gekennzeichnet ist, kann der URL-Satz nicht exportiert werden. Die Exportfunktion funktioniert nicht mit Private Set. Ein neuer URL-Satz `myurl` würde also ohne definiertes privates Set importiert und dann in eine andere Datei in einem lokalen Pfad exportiert, wie folgt:

```
> shell touch /var/tmp/test_urlset_export.csv
Done
> shell cat /var/tmp/test_urlset_export.csv
Done
> shell cat /var/tmp/test_urlset.csv
example.com
google.com
Done
> export urlset myurl -url local:test_urlset_export.csv

> import urlset myurl -url local:test_urlset.csv
Done
(a non-private urlset is imported)

<!--NeedCopy-->
```

1. Ein URL-Satz wird entfernt. Wenn Sie einen URL-Satz von Einträgen auf der Sperrliste löschen möchten, können Sie den Befehl “remove” verwenden, um den URL-Satz von der Citrix ADC-Appliance zu löschen.
2. Zeigt einen URL-Satz an. Sie können die Eigenschaften einer URL anzeigen, die mit dem Befehl show festgelegt wurde.

> **Hinweis:** URLs mit Abfrageteil werden während des Imports entfernt.

Beispiel:

```
1 show urlset
2 Name: top100 PatternCount: 100 Delimiter:  RowSeparator: Interval: 0
3 Done
4 <!--NeedCopy-->
```

Importieren Sie eine mit Meta festgelegte URL mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Befehlszeile Folgendes ein:

```
1 import urlset <name> [-overwrite] [ - delimiter <character>] [-
     rowSeparator <character>] [-url] <url> [-interval <seconds>] [-
     privateSet] [-canaryUrl <URL>]
2 <!--NeedCopy-->
```

Hierbei gilt:

Delimiter ist ein CSV-Dateisatz mit dem Standardwert 44 festgelegt.

RowSeparator ist ein Zeilentrennzeichen für CSV-Dateien, bei dem der Standardwert auf 10 festgelegt ist.

Intervall ist das Zeitintervall in Sekunden, das auf die nächsten 15 Minuten gerundet wird, bei denen die Aktualisierung des URL-Sets erfolgt.

canaryUrl ist eine URL, die zum Testen verwendet wird, wenn der Inhalt des URL-Sets vertraulich behandelt wird.

Beispiel

```
import policy urlset -url local:test_urlset.csv -delimiter ”,”-rowSeparator
 ”n”-interval 10 -privateSet -canaryUrl http://www.in.gr
```

Führen Sie eine explizite Subdomain-Übereinstimmung für einen importierten URL-Set aus

Sie können jetzt eine explizite Subdomain-Übereinstimmung für einen importierten URL-Satz durchführen. Ein neuer Parameter, “SubDomainExactMatch”, wird dem Befehl “import policy urlSet” hinzugefügt. Wenn Sie den Parameter aktivieren, führt der URL-Filter-Algorithmus eine explizite Subdomain-Übereinstimmung durch. Wenn die eingehende URL beispielsweise

“news.example.com” lautet und der Eintrag im URL-Set “example.com” lautet, stimmt der Algorithmus nicht mit den URLs überein.

Geben Sie an der Eingabeaufforderung ein:

```
import policy urlset <name> [-overwrite] [-delimiter <character>][-rowSeparator
 <character>] -url [-interval <secs>] [-privateSet][-subdomainExactMatch]
[-canaryUrl <URL>]
```

Beispiel:

```
import policy urlset forth_urlset -url local:test_urlset.csv -interval 3600
 -subdomainExactMatch
```

So zeigen Sie die mit der Befehlszeilenschnittstelle festgelegte URL an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show urlset <name>
```

Beispiel:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1          URLset      Count
2          ------      -----
3  1)      top1k       100
4   Done
5
6  > show urlset top1k
7          Count       Delimiter   Interval    RowSeparator
8          -----       ---------   --------    ------------
9          100              ,         0          0x0a
10  Done
11 >
12
13 <!--NeedCopy-->
```

So zeigen Sie den URL-Satz an, der über die Befehlszeilenschnittstelle importiert wurde

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show urlset -imported
```

Beispiel:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1          URLset
2          ------
3  1)      top1k
4   Done
5  <!--NeedCopy-->
```

So zeigen Sie URL-Set an <urlset_name> mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show urlset <name>
```

So exportieren Sie eine URL, die über die Befehlszeilenschnittstelle festgelegt wurde

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
export urlset <name> <url>
```

So fügen Sie eine URL hinzu, die über die Befehlszeilenschnittstelle festgelegt wurde

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add urlset <urlset_name>
```

So aktualisieren Sie eine URL, die über die Befehlszeilenschnittstelle festgelegt wurde

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
update urlset <name>
```

So entfernen Sie einen URL-Set-Befehl mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
remove urlset <name>
```

Beispiel:

> Hinweis:
>
> Bevor Sie ein URLSet importieren oder exportieren, müssen Sie sicherstellen, dass die `test_urlset.csv` Dateien `test_urlset_export.csv` und unter dem `/var/tmp` Verzeich-

> nis erstellt und verfügbar sind.

```
import policy urlset -url local:test_urlset.csv -delimiter ”,” -
   rowSeparator ”n” -interval 10 -privateSet -overwrite  - canaryUrl
   http://www.in.gr

add policy urlset top10k

update policy urlset top10k

sh policy urlset

sh policy urlset top10k

export policy urlset urlset1 -url local:test_urlset_export.csv

import policy urlset top10k -url local:test_urlset.csv  - privateSet

add policy urlset top10k

update policy urlset top10k

show policy urlset top10k
<!--NeedCopy-->
```

Importierte URL-Sets anzeigen

Sie können jetzt zusätzlich zu hinzugefügten URL-Sets importierte URL-Sets anzeigen. Um dies zu tun, wird dem Befehl “show url set” ein neuer Parameter “importiert” hinzugefügt. Wenn Sie diese Option aktivieren, zeigt die Appliance alle importierten URL-Sets an und unterscheidet die importierten URL-Sets von den hinzugefügten URL-Sätzen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show policy urlset [<name>] [-imported]
```

Beispiel:

```
show policy urlset -imported
```

So importieren Sie eine URL, die mit der GUI festgelegt wurde

Navigieren Sie zu **AppExpert** > **URL-Sets**und klicken Sie auf **Importieren**, um den URL-Satz herunterzuladen.

So fügen Sie eine URL hinzu, die mit der GUI festgelegt wurde

Navigieren Sie zu **AppExpert** > **URL-Sets**und klicken Sie auf **Hinzufügen**, um eine URL-Set-Datei für den heruntergeladenen URL-Satz zu erstellen.

So bearbeiten Sie eine URL, die mit der GUI festgelegt wurde

Navigieren Sie zu **AppExpert** > **URL-Sets**, wählen Sie einen URL-Satz aus und klicken Sie zum Ändern auf **Bearbeiten** .

So aktualisieren Sie eine mit der GUI festgelegte URL

Navigieren Sie zu **AppExpert** > **URL-Sets,** wählen Sie einen URL-Satz aus und klicken Sie auf **URL-Set** aktualisieren, um den URL-Satz mit den neuesten Änderungen an der Datei zu aktualisieren.

So exportieren Sie eine mit der GUI festgelegte URL

Navigieren Sie zu **AppExpert > URL-Sets**, wählen Sie einen URL-Satz aus und klicken Sie auf **URL-Set** exportieren, um die URL-Muster in einem Set auf eine Ziel-URL zu exportieren und an diesem Speicherort zu speichern.

URL-Muster-Semantik

October 5, 2021

Die folgende Tabelle zeigt die URL-Muster, die zum Angeben der Liste der Seiten verwendet werden sollen, die gefiltert werden sollen. Zum Beispiel `http://www.example.com/bar` stimmt das URL-Muster mit einer einzelnen Seite überein `http://www.example.com/bar`. Um alle Seiten abzudecken, auf denen die URL mit www.example.com/bar beginnt, müssen Sie am Ende explizit ein '*' hinzufügen.

Weitere Informationen finden Sie unter Tabelle mit URL-Muster-Metadaten .

URL-Kategorien

October 5, 2021

Es folgt eine Liste der Kategorien auf der Sperrliste.

S.no	Kategorien auf der Sperrliste
1	Illegale Aktivitäten
2	Illegale Drogen
3	Medikamente
4	Marihuana
5	Terrorismus/Extremismus
6	Waffen
7	Hass/Verleumdung
8	Gewalt/Suizid
9	Rechtsfragen allgemein
10	Erotik/Pornografie
11	Nacktbilder
12	Sexuelle Dienste
13	Erwachseneninhalte (Suche/Links)
14	Computerkriminalität/Hacking
15	Malware
16	Remote-Proxyserver
17	Suchmaschinen-Caches
18	Übersetzungen
19	Dating/Singlebörsen
20	Hochzeit/Ehe
21	Börsenkurse
22	Onlinehandel
23	Versicherungen
24	Finanzprodukte
25	Glücksspiel allgemein
26	Lotterie
27	Onlinespiele
28	Spiele
29	Auktionen

S.no	Kategorien auf der Sperrliste
30	Shopping/Einzelhandel
31	Immobilien
32	IT-Online-Shopping
33	Webbasierte Chats
34	Instant Messaging/Sofortnachrichten
35	Web-basierte E-Mail
36	E-Mail-Abonnements
37	Bulletin Boards
38	IT-Foren
39	Persönliche Webseiten/Blogs
40	Downloads
41	Programmdownloads
42	Speicherdienste
43	Streamingmedien
44	Arbeitsmarkt
45	Karrieretipps
46	Nebengeschäft
47	Grotesk
48	Veranstaltungen
49	Beliebte Artikel
50	Erwachseneninhalte (Magazine/Nachrichten)
51	Tabakwaren
52	Trinken
53	Alkohol
54	Fetisch
55	Sexueller Ausdruck (Text)
56	Cosplay/Kostüme/Freizeit
57	Okkultes
58	Heim und Familie

S.no	Kategorien auf der Sperrliste
59	Profisport
60	Sport allgemein
61	Lebensereignisse
62	Reisen und Tourismus
63	Öffentliche Reiseagenturen
64	Öffentlicher Nahverkehr
65	Unterkünfte
66	Musik
67	Horoskop/Astrologie/Wahrsagerei
68	Entertainer/Prominente
69	Essen/Gourmetküche
70	Entertainment/Veranstaltungsorte/Aktivitäten
71	Traditionelle Religionen
72	Religionen
73	Politik
74	Reklame/Werbebanner
75	Gewinnspiele/Preise
76	SPAM
77	Nachrichten
78	Automobil
79	Handel und Business
80	Computer und Internet
81	Website zum Bereich Bildung
82	Behörden
83	Integrität
84	Internettelefonie
85	Militär
86	Peer to Peer /Torrent/Filesharing
87	Hobbys und Freizeit

S.no	Kategorien auf der Sperrliste
88	Referenz
89	Suchmaschinen und Portale
90	Sexuelle Aufklärung
91	SMS- und Mobilfunkdienste
92	Mobile Apps und Herausgeber
93	Spyware
94	Infrastruktur und Netzwerke für die Inhaltsübermittlung
95	Kinderwebsites
96	Bademode und Dessous
97	Kunst und Kultur
98	Hosting von Websites
99	Philanthropie und gemeinnützige Organisationen
100	Fotosuche und Fototauschbörsen
101	Klingeltöne
102	Mode und Schönheit
103	Mobile App-Stores
104	Domainparking
105	Emoticons
106	Mobilfunkbetreiber
107	Botnetze
108	Infizierte Websites
109	Phishing-Websites
110	Keylogger
111	Mobile Malware
112	Kein Inhalt
113	Landwirtschaft
114	Architektur

S.no	Kategorien auf der Sperrliste
115	Organisationen/Branchenverbände/Gewerkschaften
116	Bücher/eBooks
117	BOT Phone Home
118	DDNS
119	Nicht unterstützte URL
120	Rechtswesen
121	Lokales/Nachbarschaft
122	Sonstiges
123	Onlinemagazine
124	Haustiere/Tierarzt
125	Piraterie und Urheberrechtsverstöße
126	Private IP-Adressen
127	Recycling/Umweltschutz
128	Wissenschaft
129	Kultur und Gesellschaft
130	Transportdienstleistungen & Fracht
131	Film und Fotografie
132	Museen und Geschichte
133	eLearning
134	Soziale Netzwerke allgemein
135	Facebook
136	Facebook: Posts
137	Facebook: Kommentar
138	Facebook: Freunde
139	Facebook: Foto hochladen
140	Facebook: Veranstaltungen
141	Facebook: Apps
142	Facebook: Chat
143	Facebook: Fragen

S.no	Kategorien auf der Sperrliste
144	Facebook: Video hochladen
145	Facebook: Gruppen
146	Facebook: Spiele
147	LinkedIn
148	LinkedIn: Aktuelles
149	LinkedIn: E-Mail
150	LinkedIn: Verbindungen
151	LinkedIn: Jobs
152	Twitter
153	Twitter: Posts
154	Twitter: E-Mail
155	Twitter: Abonnieren
156	YouTube
157	YouTube: Kommentar
158	YouTube: Video hochladen
159	YouTube: Teilen
160	Instagram
161	Instagram: Hochladen
162	Instagram: Kommentar
163	Instagram: Private Nachricht
164	Tumblr
165	Tumblr: Posts
166	Tumblr: Kommentar
167	Tumblr: Foto oder Video hochladen
168	Google+
169	Google+: Posts
170	Google+: Kommentar
171	Google+: Foto hochladen
172	Google+: Video hochladen

S.no	Kategorien auf der Sperrliste
173	Google+: Videochat
174	Pinterest
175	Pinterest: Pin/Markierung
176	Vine: Hochladen
177	Vine: Kommentar
178	Vine: Nachricht
179	Ask.fm
180	Ask.fm: Frage
181	Ask.fm: Antwort
182	YikYak
183	YikYak: Posts
184	YikYak: Kommentar
185	Wordpress
186	Wordpress: Posts
187	Wordpress: Hochladen

AppFlow

October 5, 2021

Die Citrix ADC Appliance ist ein zentraler Kontrollpunkt für den gesamten Anwendungsverkehr im Rechenzentrum. Es sammelt Informationen auf Fluss- und Benutzersitzungsebene, die für die Überwachung der Anwendungsleistung, Analyse und Business Intelligence-Anwendungen nützlich sind. Es sammelt auch Leistungsdaten und Datenbankinformationen für Webseiten. AppFlow überträgt die Informationen mithilfe des IPFIX-Formats (Internet Protocol Flow Information Export), bei dem es sich um einen offenen IETF-Standard (Internet Engineering Task Force) handelt, der in RFC 5101 definiert ist. IPFIX (die standardisierte Version von NetFlow von Cisco) wird häufig zur Überwachung von Netzwerkflussinformationen verwendet. AppFlow definiert neue Informationselemente, um Informationen auf Anwendungsebene, Daten zur Webseitenleistung und Datenbankinformationen darzustellen.

Mit UDP als Transportprotokoll überträgt AppFlow die gesammelten Daten, sogenannte *Flow-*

Datensätze, an einen oder mehrere IPv4-Sammler. Die Kollektoren aggregieren die Flow-Datensätze und generieren Echtzeit- oder historische Berichte.

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

> **Hinweis**
>
> Weitere Informationen zu HDX Insight finden Sie unter HDX Insight.

AppFlow verwendet Aktionen und Richtlinien, um Datensätze für einen ausgewählten Flow an bestimmte Kollektoren zu senden. Eine AppFlow Aktion gibt an, welche Collectors die AppFlow Datensätze erhalten. Richtlinien, die auf erweiterten Ausdrücken basieren, können so konfiguriert werden, dass sie Flows auswählen, für die Flow-Datensätze an die durch die zugehörige AppFlow Aktion angegebenen Collectors gesendet werden.

Um die Arten von Flows zu begrenzen, können Sie AppFlow für einen virtuellen Server aktivieren. AppFlow kann auch Statistiken für den virtuellen Server bereitstellen.

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

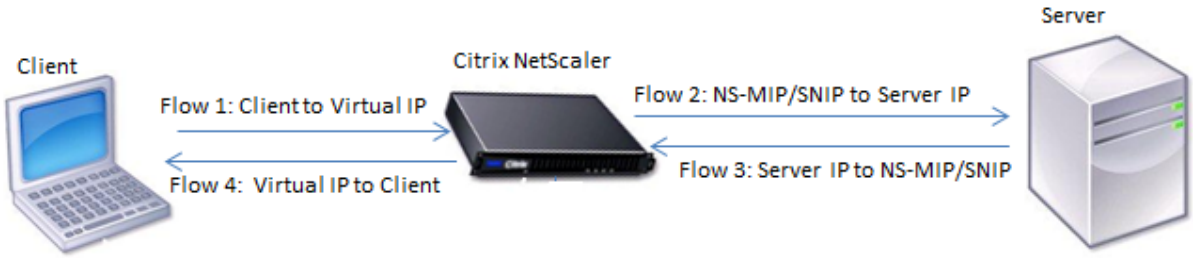
Hinweis: Diese Funktion wird nur bei Citrix ADC nCore Builds unterstützt.

Funktionsweise von AppFlow

Im häufigsten Bereitstellungsszenario fließt eingehender Datenverkehr zu einer virtuellen IP-Adresse (VIP) auf der Citrix ADC Appliance und wird auf einen Server ausgeglichen. Ausgehender Datenverkehr fließt vom Server zu einer zugeordneten oder Subnetz-IP-Adresse auf dem Citrix ADC und vom VIP zum Client. Ein Flow ist eine unidirektionale Sammlung von IP-Paketen, die durch die folgenden fünf Tupel identifiziert werden: SourceIP, SourcePort, DestIP, DestPort und Protokoll.

In der folgenden Abbildung wird die Funktionsweise des AppFlow Features beschrieben.

Abbildung 1. Citrix ADC Flusssequenz



Wie in der Abbildung gezeigt, hängen die Netzwerkflussbezeichner für jeden Abschnitt einer Transaktion von der Richtung des Datenverkehrs ab.

Die verschiedenen Flows, die einen Flow-Datensatz bilden, sind:

Flow1:<Client-IP, Client-Port, VIP-IP, VIP-port, Protocol>

Flow2:<NS-MIP/SNIP, NS-port, Server-IP, Server-Port, Protocol>

Flow3:<Server-IP, Server-Port, NS-MIP/SNIP, NS-Port, Protocol>

Flow4:<VIP-IP, VIP-port, Client-IP, Client-Port, Protocol>

Damit der Kollektor alle vier Flows in einer Transaktion verknüpfen kann, fügt AppFlow jedem Flow ein benutzerdefiniertes TransactionID-Element hinzu. Für Content Switching auf Anwendungsebene wie HTTP ist es möglich, dass eine einzelne Client-TCP-Verbindung für jede Anforderung auf verschiedene Backend-TCP-Verbindungen ausbalanciert wird. AppFlow stellt für jede Transaktion eine Gruppe von Datensätzen bereit.

Flowdatensätze

AppFlow Datensätze enthalten standardmäßige NetFlow- oder IPFIX-Informationen, z. B. Zeitstempel für Anfang und Ende eines Flows, Paketanzahl und Byteanzahl. AppFlow Datensätze enthalten auch Informationen auf Anwendungsebene (wie HTTP-URLs, HTTP-Anforderungsmethoden und Antwortstatuscodes, Server-Antwortzeit und Latenz). Daten zur Webseitenleistung (z. B. Seitenladezeit, Rendering-Zeit für Seiten und auf der Seite verbrachte Zeit). Und Datenbankinformationen (wie Datenbankprotokoll, Datenbankantwortstatus und Antwortgröße der Datenbank). IPFIX-Flow-Datensätze basieren auf Vorlagen, die vor dem Senden von Flow-Datensätzen gesendet werden müssen.

Vorlagen

AppFlow definiert einen Satz von Vorlagen, eine für jeden Flow. Jede Vorlage enthält eine Reihe von Standardinformationselementen (IEs) und unternehmensspezifische Informationselemente (EIEs). IPFIX-Vorlagen definieren die Reihenfolge und die Größe der Informationselemente (Internet Explorer) im Flow-Datensatz. Die Vorlagen werden in regelmäßigen Abständen an die Kollektoren gesendet, wie in RFC 5101 beschrieben.

Eine Vorlage kann die folgenden EIEs enthalten:

- transactionID

  Eine nicht signierte 32-Bit-Nummer, die eine Transaktion auf Anwendungsebene identifiziert. Für HTTP entspricht es einem Anforderungs- und Antwortpaar. Alle Flow-Datensätze, die diesem Anforderungs- und Antwortpaar entsprechen, haben dieselbe Transaktions-ID. Im häufigsten Fall gibt es vier `uniflow` Datensätze, die dieser Transaktion entsprechen. Wenn der Citrix ADC die Antwort selbst generiert (bereitgestellt aus dem integrierten Cache oder

durch eine Sicherheitsrichtlinie), gibt es möglicherweise nur zwei Flussdatensätze für diese Transaktion.

- connectionID

  Eine nicht signierte 32-Bit-Zahl, die eine Layer-4-Verbindung (TCP oder UDP) identifiziert. Die Citrix ADC Flows sind bidirektional, mit zwei separaten Flow-Datensätzen für jede Richtung des Flusses. Dieses Informationselement kann verwendet werden, um die beiden Flows zu verknüpfen.

  Für den Citrix ADC ist eine ConnectionID ein Bezeichner für die Verbindungsdatenstruktur, um den Fortschritt einer Verbindung zu verfolgen. In einer HTTP-Transaktion kann beispielsweise eine bestimmte ConnectionId mehrere transactionID-Elemente enthalten, die mehreren Anforderungen entsprechen, die für diese Verbindung gestellt wurden.

- tcpRTT

  Die Rundlaufzeit in Millisekunden, gemessen an der TCP-Verbindung. Es kann als Metrik verwendet werden, um die Client- oder Serverlatenz im Netzwerk zu bestimmen.

- httpRequestMethod

  Eine 8-Bit-Zahl, die die HTTP-Methode angibt, die in der Transaktion verwendet wird. Eine Optionsvorlage mit der Nummer-to-Method Zuordnung wird zusammen mit der Vorlage gesendet.

- httpRequestSize

  Eine nicht signierte 32-Bit-Nummer, die die Anforderungsnutzlastgröße angibt.

- httpRequestURL

  Die vom Client angeforderte HTTP-URL.

- httpUserAgent

  Die Quelle der eingehenden Anforderungen an den Webserver.

- httpResponseStatus

  Eine 32-Bit-Nummer ohne Vorzeichen, die den Antwortstatuscode angibt.

- httpResponseSize

  Eine 32-Bit-Nummer ohne Vorzeichen, die die Antwortgröße angibt.

- httpResponseTimeToFirstByte

  Eine 32-Bit-Nummer ohne Vorzeichen, die die Zeit angibt, die zum Empfangen des ersten Bytes der Antwort gebraucht wird.

- httpResponseTimeToLastByte

  Eine 32-Bit-Nummer ohne Vorzeichen, die die Zeit angibt, die zum Empfang des letzten Bytes der Antwort gebraucht wird.

- flowFlags

  Ein nicht signiertes 64-Bit-Flag, das verwendet wird, um unterschiedliche Flussbedingungen anzuzeigen.

EIEs für Leistungsdaten der Webseite

- clientInteractionStartTime

  Zeitpunkt, zu dem der Browser das erste Byte der Antwort erhält, um Objekte der Seite wie Bilder, Skripts und Stylesheets zu laden.

- clientInteractionEndTime

  Zeitpunkt, zu dem der Browser das letzte Byte an Antwort erhalten hat, um alle Objekte der Seite wie Bilder, Skripts und Stylesheets zu laden.

- clientRenderStartTime

  Zeitpunkt, zu dem der Browser beginnt, die Seite zu rendern.

- clientRenderEndTime

  Zeitpunkt, zu dem ein Browser die gesamte Seite einschließlich der eingebetteten Objekte beendet hat.

EIEs für Datenbankinformationen

- dbProtocolName

  Eine nicht signierte 8-Bit-Nummer, die das Datenbankprotokoll angibt. Gültige Werte sind 1 für MS SQL und 2 für MySQL.

- dbReqType

  Eine nicht signierte 8-Bit-Nummer, die die Datenbankanforderungsmethode angibt, die in der Transaktion verwendet wird. Für MS SQL sind gültige Werte 1 für QUERY, 2 für TRANSACTION und 3 für RPC. Gültige Werte für MySQL finden Sie in der MySQL-Dokumentation.

- dbReqString

  Gibt die Datenbankanforderungszeichenfolge ohne den Header an.

- dbRespStatus

  Eine nicht signierte 64-Bit-Nummer, die den Status der vom Webserver empfangenen Datenbank-Antwort angibt.

- dbRespLength

  Eine 64-Bit-Nummer ohne Vorzeichen, die die Antwortgröße angibt.

- dbRespStatString

  Die vom Webserver empfangene Antwortstatuszeichenfolge.

Konfigurieren der AppFlow Funktion

October 5, 2021

Sie konfigurieren AppFlow auf die gleiche Weise wie die meisten anderen richtlinienbasierten Features. Zuerst aktivieren Sie die AppFlow Funktion. Anschließend geben Sie die Kollektoren an, an die die Flow-Datensätze gesendet werden. Danach definieren Sie Aktionen, bei denen es sich um Sätze von konfigurierten Kollektoren handelt. Anschließend konfigurieren Sie eine oder mehrere Richtlinien und ordnen jeder Richtlinie eine Aktion zu. Die Richtlinie weist die Citrix ADC Appliance an, Anforderungen auszuwählen, deren Flow-Datensätze an die zugeordnete Aktion gesendet werden. Schließlich binden Sie jede Richtlinie entweder global oder an den spezifischen virtuellen Server, um sie in Kraft zu setzen.

Sie können AppFlow Parameter weiter festlegen, um das Vorlagenaktualisierungsintervall anzugeben und den Export von HttpURL, HttpCookie und httpReferer-Informationen zu aktivieren. Auf jedem Collector müssen Sie die Citrix ADC IP-Adresse als Adresse des Exporters angeben.

> **Hinweis:**
>
> Informationen zum Konfigurieren des Citrix ADC als Exporteur auf dem Collector finden Sie in der Dokumentation für den jeweiligen Collector.

Das Konfigurationsdienstprogramm bietet Tools, mit denen Benutzer die Richtlinien und Aktionen definieren können. Es bestimmt genau, wie die Citrix ADC Appliance Datensätze für einen bestimmten Flow in eine Reihe von Collectors exportiert (Aktion). Die Befehlszeilenschnittstelle bietet einen entsprechenden Satz von CLI-basierten Befehlen für erfahrene Benutzer, die eine Befehlszeile bevorzugen.

AppFlow aktivieren

Um die AppFlow Funktion verwenden zu können, müssen Sie sie zuerst aktivieren.

> **Hinweis:**
>
> AppFlow kann nur auf nCore Citrix ADC Appliances aktiviert werden.

So aktivieren Sie das AppFlow Feature mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:


```
enable ns feature AppFlow
<!--NeedCopy-->
```

So aktivieren Sie die AppFlow Funktion mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **System > Einstellungen**, klicken Sie auf **Erweiterte Funktionen konfigurieren**und wählen Sie die Option **AppFlow** aus.

Kollektor angeben

Ein Kollektor empfängt AppFlow Datensätze, die von der Citrix ADC Appliance generiert werden. Um die AppFlow Datensätze zu senden, müssen Sie mindestens einen Collector angeben. Standardmäßig überwacht der Collector IPFIX-Nachrichten am UDP-Port 4739. Sie können den Standardport ändern, wenn Sie den Collector konfigurieren. In ähnlicher Weise wird NSIP standardmäßig als Quell-IP für den AppFlow Verkehr verwendet. Sie können diese Standard-Quell-IP beim Konfigurieren eines Collectors in eine SNIP-Adresse ändern. Sie können auch nicht verwendete Kollektoren entfernen.

So legen Sie einen Kollektor mit der Befehlszeilenschnittstelle fest

> **Wichtig**
>
> Ab Citrix ADC Release 12.1 Build 55.13 können Sie den Typ des Collectors angeben, den Sie verwenden möchten. Ein neuer Parameter “Transport” wird im `add appflow collector` Befehl eingeführt. Standardmäßig lauscht der Collector IPFIX-Nachrichten. Sie können den Kollektortyp entweder `logstreamipfix` oder auf Ruhe ändern, indem Sie den Parameter “Transport” verwenden. Weitere Informationen zur Konfiguration finden Sie im Beispiel.

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

```
-  add appflow collector <name> -IPAddress <ipaddress> -port <
    port_number> -netprofile <netprofile_name> -Transport <Transport>

-  show appflow collector <name>
<!--NeedCopy-->
```

Beispiel


```
add appflow collector col1 -IPaddress 10.102.29.251 -port 8000 -
    netprofile n2 -Transport ipfix
<!--NeedCopy-->
```

So legen Sie mehrere Kollektoren mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um dieselben Daten hinzuzufügen und an mehrere Collectors zu senden:

```
add appflow collector <collector1> -IPAddress <IP>

add appflow collector <collector2> -IPAddress <IP>

add appflow action <action> -collectors <collector1> <collector2>

add appflow policy <policy> true <action>

bind lbvserver <lbvserver> -policy <policy> -priority <priority>
<!--NeedCopy-->
```

So geben Sie einen oder mehrere Kollektoren mit dem Konfigurationsdienstprogramm an

Navigieren Sie zu **System > AppFlow > Collectors**, und erstellen Sie den AppFlow-Collector.

Konfigurieren einer AppFlow Aktion

Eine AppFlow Aktion ist ein Set-Collector, an den die Flow-Datensätze gesendet werden, wenn die zugehörige AppFlow Richtlinie übereinstimmt.

So konfigurieren Sie eine AppFlow Aktion mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine AppFlow Aktion zu konfigurieren und die Konfiguration zu überprüfen:

```
add appflow action <name> --collectors <string> ... [-
    clientSideMeasurements (Enabled|Disabled) ] [-comment <string>]

show appflow action
```



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

Beispiel

```
1 add appflow action apfl-act-collector-1-and-3 -collectors collector-1
     collecter-3
2 <!--NeedCopy-->
```

So konfigurieren Sie eine AppFlow Aktion mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **System > AppFlow > Actions**und erstellen Sie die AppFlow-Aktion.

Konfigurieren einer AppFlow Richtlinie

Nachdem Sie eine AppFlow Aktion konfiguriert haben, müssen Sie als nächstes eine AppFlow-Richtlinie konfigurieren. Eine AppFlow Richtlinie basiert auf einer Regel, die aus einem oder mehreren Ausdrücken besteht.

> **Hinweis:**
>
> Für die Erstellung und Verwaltung von AppFlow Richtlinien bietet das Konfigurationsdienstprogramm Unterstützung, die an der Befehlszeilenschnittstelle nicht verfügbar ist.

So konfigurieren Sie eine AppFlow Richtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine AppFlow Richtlinie hinzuzufügen und die Konfiguration zu überprüfen:

```
1 add appflow policy <name> <rule> <action>
2
3 show appflow policy <name>
4 <!--NeedCopy-->
```

Beispiel


```
add appflow policy apfl-pol-tcp-dsprt client.TCP.DSTPORT.EQ(22) apfl-
    act-collector-1-and-3
<!--NeedCopy-->
```

So konfigurieren Sie eine AppFlow Richtlinie mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **System > AppFlow > Richtlinien**, und erstellen Sie die AppFlow-Richtlinie.

So fügen Sie einen Ausdruck mithilfe des Dialogfelds Ausdruck hinzufügen hinzu

1. Wählen Sie im Dialogfeld Ausdruck hinzufügen im ersten Listenfeld den ersten Begriff für Ihren Ausdruck aus.
   - HTTP
     Das HTTP-Protokoll. Wählen Sie die Option, wenn Sie einen Aspekt der Anfrage untersuchen möchten, der sich auf das HTTP-Protokoll bezieht.
   - SSL

     Die geschützten Websites. Wählen Sie die Option, wenn Sie einen Aspekt der Anfrage untersuchen möchten, der sich auf den Empfänger der Anfrage bezieht.
   - CLIENT

     Der Computer, der die Anforderung gesendet hat. Wählen Sie die Option, wenn Sie einen Aspekt des Absenders der Anfrage untersuchen möchten.
     Wenn Sie Ihre Wahl treffen, werden im Listenfeld ganz rechts die entsprechenden Begriffe für den nächsten Teil des Ausdrucks aufgeführt.
2. Wählen Sie im zweiten Listenfeld den zweiten Begriff für Ihren Ausdruck aus. Die Auswahlmöglichkeiten hängen davon ab, welche Auswahl Sie im vorherigen Schritt getroffen haben, und sind dem Kontext angemessen. Nachdem Sie Ihre zweite Wahl getroffen haben, zeigt das Hilfefenster unterhalb des Fensters Ausdruck erstellen (das leer war) Hilfe an, in dem der Zweck und die Verwendung des gerade ausgewählten Begriffs beschrieben wird.
3. Fahren Sie fort, Begriffe aus den Listenfeldern auszuwählen, die rechts neben dem vorherigen Listenfeld angezeigt werden, oder geben Sie Zeichenfolgen oder Zahlen in die Textfelder ein, die Sie zur Eingabe eines Werts auffordern, bis der Ausdruck beendet ist.

Binden einer AppFlow Richtlinie

Um eine Richtlinie in Kraft zu setzen, müssen Sie sie entweder global binden, sodass sie für den gesamten Datenverkehr gilt, der über das Citrix ADC fließt, oder für einen bestimmten virtuellen

Server, sodass die Richtlinie nur für den Datenverkehr gilt, der mit diesem virtuellen Server verknüpft ist.

Wenn Sie eine Richtlinie binden, weisen Sie ihr eine Priorität zu. Die Priorität bestimmt die Reihenfolge, in der die von Ihnen definierten Richtlinien ausgewertet werden. Sie können die Priorität auf eine beliebige positive Ganzzahl festlegen.

Im Citrix ADC Betriebssystem funktionieren Richtlinienprioritäten in umgekehrter Reihenfolge — je höher die Zahl, desto niedriger die Priorität. Wenn Sie beispielsweise drei Richtlinien mit Prioritäten von 10, 100 und 1000 haben, wird die Richtlinie, der eine Priorität von 10 zugewiesen hat, zuerst ausgeführt. Später wurde die Richtlinie mit einer Priorität von 100 zugewiesen, und schließlich hat die Richtlinie eine Reihenfolge von 1000 zugewiesen.

Sie können sich viel Raum lassen, um andere Richtlinien in beliebiger Reihenfolge hinzuzufügen, und sie dennoch so einstellen, dass sie in der gewünschten Reihenfolge bewertet werden. Sie können dies erreichen, indem Sie Prioritäten mit Intervallen von 50 oder 100 zwischen jeder Richtlinie festlegen, wenn Sie sie global binden. Sie können dann jederzeit weitere Richtlinien hinzufügen, ohne die Priorität einer bestehenden Richtlinie ändern zu müssen.

So binden Sie eine AppFlow Richtlinie global mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine AppFlow Richtlinie global zu binden und die Konfiguration zu überprüfen:

```
1 bind appflow global <policyName> <priority> [<gotoPriorityExpression [-
     type <type>] [-invoke (<labelType> <labelName>)]
2
3 show appflow global
4 <!--NeedCopy-->
```

Beispiel

```
1 bind appflow global af_policy_lb1_10.102.71.190 1 NEXT -type
     REQ_OVERRIDE -invoke vserver google
2 <!--NeedCopy-->
```


So binden Sie eine AppFlow Richtlinie mit der Befehlszeilenschnittstelle an einen bestimmten virtuellen Server

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine AppFlow Richtlinie an einen bestimmten virtuellen Server zu binden und die Konfiguration zu überprüfen:

```
bind lb vserver <name> -policyname <policy_name> -priority <priority>
<!--NeedCopy-->
```

Beispiel

```
bind lb vserver google -policyname af_policy_google_10.102.19.179 -
   priority 251
<!--NeedCopy-->
```

So binden Sie eine AppFlow Richtlinie global mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **System > AppFlow**, klicken Sie auf **AppFlow policy Manager**, wählen Sie den entsprechenden Bind-Point (Standard Global) und den Verbindungstyp aus, und binden Sie dann die AppFlow-Richtlinie.

So binden Sie eine AppFlow Richtlinie mit dem Konfigurationsdienstprogramm an einen bestimmten virtuellen Server

Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, wählen Sie den virtuellen Server aus, klicken Sie auf **Richtlinien**, und binden Sie die AppFlow Richtlinie.

Aktivieren von AppFlow für virtuelle Server

Wenn Sie nur den Datenverkehr über bestimmte virtuelle Server überwachen möchten, aktivieren Sie AppFlow speziell für diese virtuellen Server. Sie können AppFlow für Lastenausgleich, Content Switching, Cache-Umleitung, SSL-VPN-, GSLB- und Authentifizierungsserver aktivieren.

So aktivieren Sie AppFlow für einen virtuellen Server mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set cs vserver <name> <protocol> <IPAddress> <port> -appflowLog ENABLED
<!--NeedCopy-->
```

Beispiel

```
set cs vserver Vserver-CS-1 HTTP 10.102.29.161 80 -appflowLog ENABLED
<!--NeedCopy-->
```

So aktivieren Sie AppFlow für einen virtuellen Server mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, wählen Sie den virtuellen Server aus und aktivieren Sie die Option AppFlow Logging.

Aktivieren von AppFlow für einen Dienst

Sie können AppFlow für Dienste aktivieren, die an die virtuellen Server des Lastenausgleichs gebunden werden sollen.

So aktivieren Sie AppFlow für einen Dienst mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -appflowLog ENABLED
<!--NeedCopy-->
```

Beispiel

```
set service ser -appflowLog ENABLED
<!--NeedCopy-->
```

So aktivieren Sie AppFlow für einen Dienst mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management > Load Balancing > Services**, wählen Sie den Dienst aus und aktivieren Sie die Option AppFlow Logging.

Festlegen der AppFlow Parameter

Sie können AppFlow Parameter festlegen, um den Export von Daten in die Collectors anzupassen.

So legen Sie die AppFlow Parameter mit der Befehlszeilenschnittstelle fest

> **Wichtig**
>
> - Ab Citrix ADC Release 12.1 Build 55.13 können Sie mit dem NSIP `Logstream` Datensätze anstelle des SNIP senden. Ein neuer Parameter “LogStreamOurnSip” wird im `set appflow param` Befehl eingeführt. Standardmäßig ist der Parameter “logstreamOverNSIP” DISABLED, Sie müssen ihn auf ENABLE setzen. Weitere Informationen zur Konfiguration finden Sie im Beispiel.
> - Ausgehend von Citrix ADC Release 13.0 Build 58.x können Sie die Web-SaaS-Anwendungsoption in der AppFlow Funktion aktivieren. Es kann aktiviert werden, um die Datennutzung von Web- oder SaaS-Anwendungen vom Citrix Gateway Dienst zu empfangen. Weitere Informationen zur Konfiguration finden Sie im Beispiel.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die AppFlow Parameter festzulegen und die Einstellungen zu überprüfen:

```
1 -  set appflow param [-templateRefresh <secs>] [-appnameRefresh <secs>]
      [-flowRecordInterval <secs>] [-udpPmtu <positive_integer>] [-
     httpUrl ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-httpCookie ( \*\*
     ENABLED\*\* | \*\*DISABLED\*\* )] [-httpReferer ( \*\*ENABLED\*\* |
     \*\*DISABLED\*\* )] [-httpMethod ( \*\*ENABLED\*\* | \*\*DISABLED
     \*\* )] [-httpHost ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-
     httpUserAgent ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-
     httpXForwardedFor ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )][-
     clientTrafficOnly ( \*\*YES\*\* | \*\*NO\*\*)] [-
     webSaaSAppUsageReporting ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )] [-
     logstreamOverNSIP ( \*\*ENABLED\*\* | \*\*DISABLED\*\* )]
2
3 -  show appflow Param
4 <!--NeedCopy-->
```

Beispiel

```
1 set appflow Param -templateRefresh 240 -udpPmtu 128 -httpUrl enabled -
     webSaaSAppUsageReporting ENABLED -logstreamOverNSIP ENABLED
```



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

So legen Sie die AppFlow Parameter mit dem Konfigurationsdienstprogramm fest

Navigieren Sie zu **System > AppFlow**, klicken Sie auf **AppFlow-Einstellungen ändern**und geben Sie relevante AppFlow-Parameter an.

Unterstützung für die Verschleierung der Abonnenten-ID

Ab Citrix ADC Release 13.0 Build 35.xx wird die AppFlow Konfiguration erweitert, um den “SubscriberidOBFuscation” -Algorithmus zur Verschleierung von MSISDN in Schicht 4 oder Layer 7, AppFlow-Datensätzen, zu unterstützen. Bevor Sie den Algorithmus jedoch als MD5 oder SHA256 konfigurieren, müssen Sie ihn zuerst als AppFlow Parameter aktivieren. Der Parameter ist standardmäßig deaktiviert.

So konfigurieren Sie den Algorithmus zur Verschleierung der Abonnenten-ID mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set appflow param [-subscriberIdObfuscation ( ENABLED | DISABLED )  [-
     subscriberIdObfuscationAlgo ( MD5 | SHA256 )]]
2 <!--NeedCopy-->
```

Beispiel

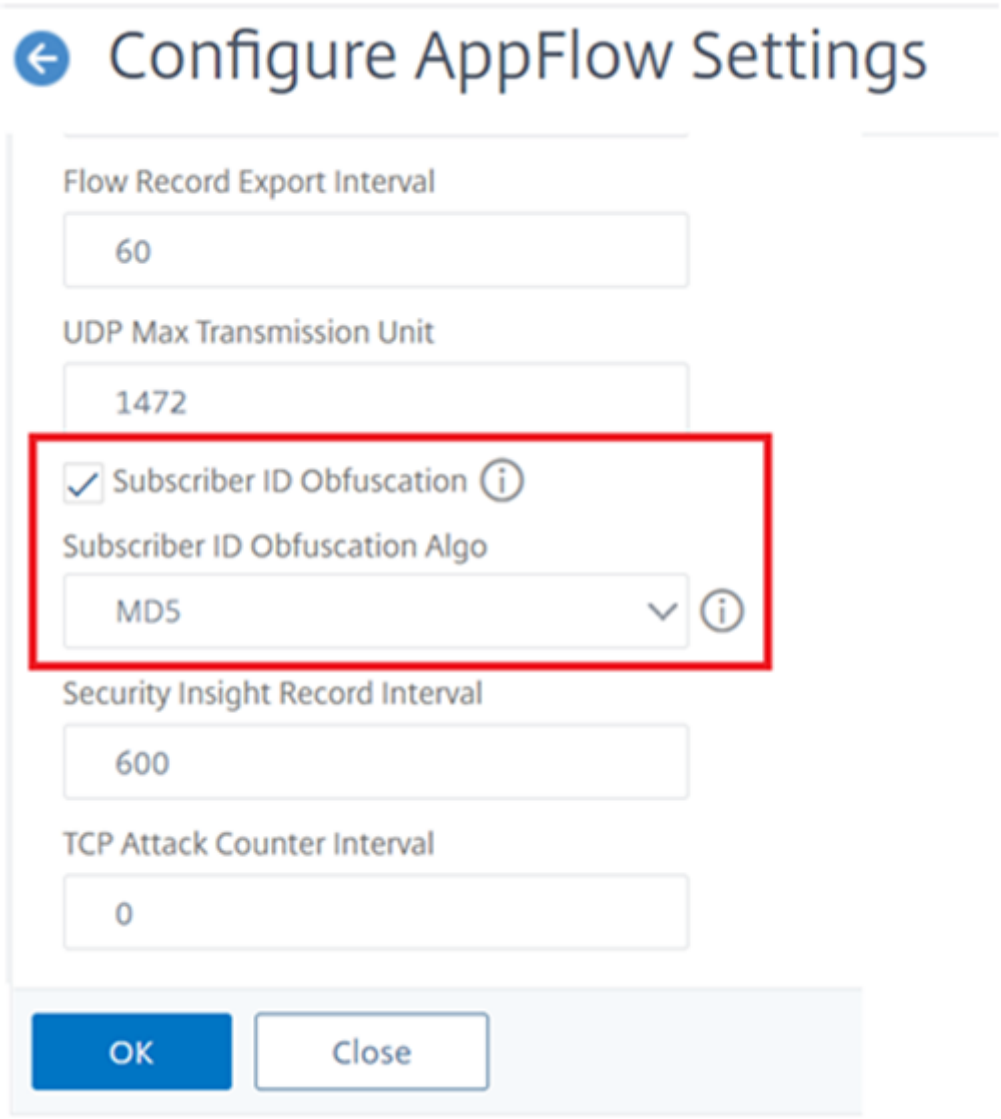
```
1 set appflow param  -subscriberIdObfuscation ENABLED  -
     subscriberIdObfuscationAlgo SHA256
2 <!--NeedCopy-->
```

So konfigurieren Sie den Algorithmus zur Verschleierung der Abonnenten-ID über die GUI

1. Navigieren Sie zu **System > AppFlow**.
2. Klicken Sie im Detailbereich von AppFlow unter **Settings** auf **AppFlow Einstellung ändern**.
3. Legen Sie auf der Seite AppFlow Einstellungen konfigurieren die folgenden Parameter fest:
   - **Verschleierung der Abonnenten-ID.** Aktivieren Sie die Option für die Verschleierung von MSISDN in L4/L7 AppFlow Einträgen.

- **Abonnenten-ID Obfuscation Algo.** Wählen Sie den Algorithmustyp als MD5 oder SHA256 aus.

4. Klicken Sie auf **OK** und **schließen**.



Beispiel: AppFlow für DataStream konfigurieren

Im folgenden Beispiel wird das Verfahren zum Konfigurieren von AppFlow für DataStream mit der Befehlszeilenschnittstelle veranschaulicht.

```
1 enable feature appflow
2
3 add db user sa password freebsd
```



```
4
5 add lbvserver lb0 MSSQL 10.102.147.97 1433 -appflowLog ENABLED
6
7 add service sv0 10.103.24.132 MSSQL 1433 -appflowLog ENABLED
8
9 bind lbvserver lb0 sv0
10
11 add appflow collector col0 -IPAddress 10.102.147.90
12
13 add appflow action act0 -collectors col0
14
15 add appflow policy pol0 "mssql.req.query.text.contains("select")" act0
16
17 bind lbvserver lb0 -policyName pol0 -priority 10
18 <!--NeedCopy-->
```

Wenn die Citrix ADC Appliance eine Datenbankanforderung empfängt, wertet die Appliance die Anforderung anhand einer konfigurierten Richtlinie aus. Wenn eine Übereinstimmung gefunden wird, werden die Details an den AppFlow -Kollektor gesendet, der in der Richtlinie konfiguriert ist.

Exportieren von Leistungsdaten von Webseiten in den AppFlow Collector

October 5, 2021

Die EdgeSight Monitoring-Anwendung bietet Webseiten-Überwachungsdaten, mit denen Sie die Leistung verschiedener Webanwendungen überwachen können, die in einer Citrix ADC-Umgebung bereitgestellt werden. Sie können diese Daten jetzt in AppFlow-Collectors exportieren, um eine eingehende Analyse der Webseitenanwendungen zu erhalten. AppFlow, der auf dem IPFIX-Standard basiert, liefert spezifischere Informationen über die Leistung von Webanwendungen als EdgeSight-Monitoring allein.

Sie können sowohl den Lastausgleich als auch den virtuellen Content Switching-Server konfigurieren, um EdgeSight Monitoring-Daten in AppFlow -Sammler zu exportieren. Bevor Sie einen virtuellen Server für den AppFlow-Export konfigurieren, ordnen Sie eine AppFlow-Aktion mit der EdgeSight Monitoring-Responder-Richtlinie zu.

Die folgenden Leistungsdaten der Webseite werden in AppFlow exportiert:

- **Seitenladezeit**. Verstrichene Zeit, in Millisekunden, ab dem der Browser beginnt, das erste Byte einer Antwort zu empfangen, bis der Benutzer beginnt, mit der Seite zu interagieren. In diesem Stadium werden möglicherweise nicht alle Seiteninhalte geladen.

- **Renderzeit der Seite**. Verstrichene Zeit in Millisekunden, ab dem der Browser das erste Antwortbyte erhält, bis entweder der gesamte Seiteninhalt gerendert wurde oder die Aktion zum Laden der Seite abgelaufen ist.
- **Verbrachte Zeit auf der Seite**. Zeit, die von Benutzern auf einer Seite verbracht wird. Stellt die Zeit von einer Seitenanforderung zur nächsten dar.

AppFlow überträgt die Performance-Daten mithilfe des IPFIX-Formats (Internet Protocol Flow Information Export), bei dem es sich um einen offenen IETF-Standard (Internet Engineering Task Force) handelt, der in RFC 5101 definiert ist. Die AppFlow Vorlagen verwenden die folgenden unternehmensspezifischen Informationselemente (EIEs), um die Informationen zu exportieren:

- **Endzeit des Clients**. Zeitpunkt, zu dem der Browser das letzte Byte einer Antwort erhalten hat, um alle Objekte der Seite wie Bilder, Skripts und Stylesheets zu laden.
- **Startzeit für das Laden des Clients**. Zeitpunkt, zu dem der Browser das erste Byte der Antwort erhält, um Objekte der Seite wie Bilder, Skripts und Stylesheets zu laden.
- **Endzeit des Client-Rendering-Clients**. Zeitpunkt, zu dem ein Browser die gesamte Seite einschließlich der eingebetteten Objekte beendet hat.
- **Client-Render-Startzeit**. Zeitpunkt, zu dem der Browser mit dem Rendern der Seite begonnen hat.

Voraussetzungen für den Export von Leistungsdaten von Webseiten in AppFlow Collectors

Bevor Sie die AppFlow -Aktion mit der AppFlow-Richtlinie verknüpfen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Die AppFlow Funktion wurde aktiviert und konfiguriert.
- Die Responder-Funktion wurde aktiviert.
- Die Funktion EdgeSight Monitoring wurde aktiviert.
- Die EdgeSight-Überwachung wurde auf den virtuellen Lastausgleichs- oder Content Switching-Servern aktiviert, die an die Dienste von Anwendungen gebunden sind, für die Sie die Performance-Daten erfassen möchten.

Verknüpfen einer AppFlow-Aktion mit der EdgeSight-Monitoring-Responder-Richtlinie

Um die Leistungsdaten der Webseite in den AppFlow-Collector zu exportieren, müssen Sie eine AppFlow-Aktion mit der EdgeSight Monitoring-Responder-Richtlinie verknüpfen. Eine AppFlow -Aktion gibt an, welche Kollektoren den Datenverkehr empfangen.

So verknüpfen Sie eine AppFlow-Aktion mit der EdgeSight Monitoring Responder-Richtlinie über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set responder policy <name> -appflowAction <action_Name>
<!--NeedCopy-->
```

Beispiel

```
set responder policy pol -appflowAction actn
<!--NeedCopy-->
```

So verknüpfen Sie eine AppFlow-Aktion mit der EdgeSight Monitoring-Responder-Richtlinie über die grafische Benutzeroberfläche

1. Navigieren Sie zu **AppExpert** > **Responder** > **Richtlinien**.
2. Wählen Sie im Detailbereich eine Responder-Richtlinie für die EdgeSight Monitoring aus, und klicken Sie dann auf **Öffnen**.
3. Wählen **Sie im Dialogfeld Responder-Richtlinie konfigurieren** in der Dropdownliste **AppFlow-Aktion** die AppFlow-Aktion aus, die mit den Collectors verknüpft ist, an die Sie die Leistungsdaten der Webseite senden möchten.
4. Klicken Sie auf **OK**.

Konfigurieren eines virtuellen Servers zum Exportieren von EdgeSight-Statistiken in AppFlow-Collectors

Um EdgeSight-Statistikinformationen von einem virtuellen Server in den AppFlow -Kollektor zu exportieren, müssen Sie dem virtuellen Server eine AppFlow-Aktion zuordnen.

So verknüpfen Sie eine AppFlow-Aktion mit einem virtuellen Load Balancing- oder Content Switching-Server über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**. Sie können auch zu **Traffic Management** > **Content Switching** > **Virtuelle Server** navigieren.
2. Wählen Sie im Detailbereich einen virtuellen Server oder mehrere virtuelle Server aus, und klicken Sie dann auf **EdgeSight-Überwachung aktivieren**.

3. Aktivieren Sie im Dialogfeld EdgeSight-Überwachung aktivieren das Kontrollkästchen **EdgeSight-Statistiken nach Appflow exportieren** .
4. Wählen Sie in der Dropdownliste AppFlow-Aktion die **AppFlow-Aktion** aus. Die AppFlow -Aktion definiert die Liste der AppFlow -Kollektoren, in die EdgeSight-Monitoring-Statistiken exportiert werden. Wenn Sie mehrere virtuelle Lastenausgleichsserver ausgewählt haben, ist dieselbe AppFlow-Aktion mit den an sie gebundenen Responder-Richtlinien verknüpft. Später können Sie die AppFlow-Aktion, die für jeden der ausgewählten virtuellen Load Balancing-Server konfiguriert wurde, gegebenenfalls einzeln ändern.
5. Klicken Sie auf **OK**.

Sitzungszuverlässigkeit bei Citrix ADC Hochverfügbarkeitspaar

July 27, 2022

Wenn während einer ICA-Sitzung eine Netzwerkunterbrechung oder ein Geräte-Failover auftritt, kann bei der Wiederverbindung einer Sitzung eine von zwei Mechanismen verwendet werden: Sitzungszuverlässigkeit oder Automatische Wiederverbindung des Clients.

Zuverlässigkeit der Sitzung. Der bevorzugte Modus ist eine reibungslose Erfahrung für den Benutzer. Die Störung ist bei kurzen Netzwerkunterbrechungen kaum wahrnehmbar.

Automatische Wiederverbindung von Clients: Die Fallback-Option beinhaltet einen Neustart des Clients. Dieser Mechanismus ist für den Benutzer störend und wird nicht immer unterstützt.

Empfänger können ihre ICA-Sitzungen mithilfe der Funktion zur Zuverlässigkeit von ICA-Sitzungen nahtlos wieder verbinden, wenn HDX Insight aktiviert ist.
Diese Funktion funktioniert sowohl in der eigenständigen Konfiguration als auch in einer Citrix ADC HA-Paarkonfiguration und sogar dann, wenn ein Citrix ADC-Failover auftritt.

> **Hinweis:**
>
> - Citrix ADC-Appliances müssen auf der Softwareversion 11.1 Build 49.16 oder höher ausgeführt werden.
> - Sie dürfen den Sitzungszuverlässigkeitsmodus nicht aktivieren oder deaktivieren, wenn die Citrix ADC-Appliances über aktive Verbindungen verfügen.
> - Das Aktivieren oder Deaktivieren der Funktion bei noch aktiven Verbindungen führt dazu, dass HDX Insight die Analyse dieser Sitzungen nach einem Failover beendet. Dies führt zum Verlust von Informationen über die Sitzungen.
> - Die Sitzungszuverlässigkeit bei einem Hochverfügbarkeitssetup ist für die Citrix ADC-Softwareversion 11.1 49.16 oder höher standardmäßig deaktiviert. Die Sitzungszuverlässigkeit wird bei einem Hochverfügbarkeitssetup nur unterstützt, wenn auf beiden Knoten

> des Setups derselbe Build ausgeführt wird (z. B. Version 11.1 Build 53). Mit anderen Worten, Sitzungszuverlässigkeit wird bei einem Hochverfügbarkeitssetup nicht unterstützt, wenn auf beiden Knoten unterschiedliche Builds ausgeführt werden (z. B. ein Knoten mit Version 11.1 Build 53 und der andere Version 11.1 Build 56). Die Sitzungszuverlässigkeit für SSL VDA wird unterstützt, wenn die folgenden Bedingungen erfüllt sind:
>
>   - The "EnableSRonHAFailover" parameter in the `set ica parameter` command must be YES.
>   - The HTTPS must be used instead of HTTP while configuring the virtual server.
>
> • Wenn HDX Insight aktiviert ist, verbinden sich grundlegende Verschlüsselungsanwendungen und -desktops nach einem Hochverfügbarkeitsfailover wieder, selbst wenn der Parameter EnableSronhaLover deaktiviert ist.

So konfigurieren Sie die Sitzungszuverlässigkeit mit CLI:

1. Verwenden Sie in der Befehlszeile die standardmäßigen Anmeldeinformationen des Systemadministrators, um sich am System anzumelden.
2. Um die Sitzungszuverlässigkeit bei HA-Failover zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein: `set ica parameter EnableSRonHAFailover YES`
3. Um die Sitzungszuverlässigkeit bei HA-Failover zu deaktivieren, geben Sie an der Eingabeaufforderung Folgendes ein: `set ica parameter EnableSRonHAFailover NO`

So aktivieren Sie die Sitzungszuverlässigkeit bei HA-Failover über die grafische Benutzeroberfläche:

1. Geben Sie in einem Webbrowser die IP-Adresse der primären Citrix ADC Instanz im HA-Paar ein (z. B.http://192.168.100.1).
2. Geben Sie **unter Benutzername** und **Kennwort** die Administratoranmeldeinformationen ein.
3. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System** > **Einstellungen**, und klicken Sie auf **ICA-Parameter ändern**.
4. Wählen Sie im Abschnitt **Ändern der ICA-Parameter** die Option **Sitzungszuverlässigkeit bei HA-Failover** aus.
5. Klicken Sie auf **OK**.

Einschränkungen

- Das Aktivieren dieser Funktion führt zu einem erhöhten Bandbreitenverbrauch, der darauf zurückzuführen ist, dass die ICA-Komprimierung durch die Funktion deaktiviert wurde. Und der zusätzliche Datenverkehr zwischen den primären und sekundären Knoten, um sie synchron zu halten.
- Diese Funktion wird nur im Aktiv-Passiv-Modus unterstützt. Der Aktiv-Aktiv-Modus wird derzeit nicht unterstützt.
- Wenn HDX Insight aktiviert ist und die Sitzungszuverlässigkeit auf dem HA-Regler auf NEIN gesetzt ist, wird im Citrix ADC High Availability Failover-Szenario nur der ACR-

Wiederverbindungsmodus unterstützt. Der HA-Regler deaktiviert die Sitzungszuverlässigkeit nicht, wenn HDX Insight deaktiviert ist.

Die **Session Reconnect Semantik-Tabelle** lautet wie folgt:

Session verbindet Semantik

Status	EnableSRonHAFailover Yes	EnableSRonHAFailover No (Standard)
HDX Insight aktiviert	Wiederverbinden der Sitzung für ICA-Sitzung funktioniert	Die Wiederverbindung von Sitzungen für ICA-Sitzungen funktioniert nicht
HDX Insight deaktiviert	Wiederverbinden der Sitzung für ICA-Sitzung funktioniert	Wiederverbinden von Sitzungen für ICA-Sitzungen funktioniert

Wichtige Hinweise

- Die Sitzungszuverlässigkeit für ICA-Sitzungen funktioniert standardmäßig mit Citrix Gateway.
- Die Sitzungszuverlässigkeit für ICA-Sitzungen funktioniert nicht, wenn die beiden folgenden Bedingungen erfüllt sind:
  - HDX Insight ist aktiviert
  - EnableSRonHAFailover ist auf NO gesetzt
- Das Festlegen des EnableSRonHAFailover-Reglers auf YES oder NO macht keinen Unterschied, wenn HDX Insight deaktiviert ist.

Citrix Web App Firewall

October 5, 2021

In den folgenden Themen werden die Installations- und Konfigurationsdetails der Citrix Web App Firewall -Funktion behandelt.

Einführung	Eine Übersicht über die Websicherheit und die Funktionsweise der Web App Firewall.
Konfiguration	So konfigurieren Sie die Web App Firewall zum Schutz einer Website, eines Webdienstes oder einer Web 2.0-Site.

Signaturen	Eine detaillierte Beschreibung der Signaturen und wie Sie sie von einem unterstützten Tool zum Scannen von Schwachstellen aus konfigurieren und mit Beispielen eigene Signaturen definieren.
Übersicht über Sicherheitsprüfungen	Eine detaillierte Beschreibung der Sicherheitsprüfungen von Web App Firewall mit Konfigurationsinformationen und Beispielen.
Profile	Eine Beschreibung der Konfiguration und Verwendung von Profilen in der Web App Firewall.
Richtlinien	Eine Beschreibung der Verwendung von Richtlinien bei der Konfiguration der Web App Firewall mit Beispielen nützlicher Richtlinien.
Einfuhren	Eine Beschreibung, wie die Web App Firewall verschiedene Arten von importierten Dateien verwendet und wie Dateien importiert und exportiert werden.
Globale Konfiguration	Eine Beschreibung der Web App Firewall Features, die für alle Profile gelten, und wie sie konfiguriert werden.
Anwendungsfälle	Erweiterte Beispiele, die zeigen, wie Sie die Web App Firewall einrichten, um bestimmte Arten komplexerer Websites und Webdienste am besten zu schützen.
Protokolle, Statistiken und Berichte	So greifen Sie auf die Web App Firewall -Protokolle, die Statistiken und die Berichte zu und verwenden sie, um bei der Konfiguration der Web App Firewall zu helfen.

Die Citrix Web App Firewall bietet einfach zu konfigurierende Optionen, um eine Vielzahl von Anwendungssicherheitsanforderungen zu erfüllen. Web App Firewall Profile, die aus Sicherheitsüberprüfungen bestehen, können zum Schutz sowohl der Anforderungen als auch der Antworten verwendet werden, indem umfassende Inspektionen auf Paketebene bereitgestellt werden. Jedes Profil enthält

eine Option zur Auswahl grundlegender Schutzmaßnahmen oder erweiterter Schutz. Einige Schutzmaßnahmen erfordern möglicherweise die Verwendung anderer Dateien. Beispielsweise erfordern XML-Validierungsprüfungen WSDL- oder Schemadateien. Die Profile können auch andere Dateien wie Signaturen oder Fehlerobjekte verwenden. Diese Dateien können lokal hinzugefügt oder im Vorfeld importiert und zur späteren Verwendung auf der Appliance gespeichert werden.

Jede Richtlinie identifiziert einen Typ von Datenverkehr, und dieser Datenverkehr wird auf die Sicherheitsüberprüfungsverletzungen überprüft, die in dem Profil angegeben sind, das der Richtlinie zugeordnet ist. Die Richtlinien können unterschiedliche Bindungspunkte haben, die den Umfang der Richtlinie bestimmen. Beispielsweise wird eine Richtlinie, die an einen bestimmten virtuellen Server gebunden ist, nur für den Datenverkehr aufgerufen und ausgewertet, der durch diesen virtuellen Server fließt. Die Richtlinien werden in der Reihenfolge ihrer festgelegten Prioritäten ausgewertet, und die erste, die der Anforderung oder Antwort entspricht, wird angewendet.

- Schnelle Bereitstellung des Web App Firewall Schutzes

  Sie können das folgende Verfahren für die schnelle Bereitstellung der Web App Firewall -Sicherheit verwenden:

  1. Fügen Sie ein Web App Firewall -Profil hinzu und wählen Sie den entsprechenden Typ (html, xml, JSON) für die Sicherheitsanforderungen der Anwendung aus.
  2. Wählen Sie die erforderliche Sicherheitsstufe (Basic oder Advanced) aus.
  3. Fügen Sie die erforderlichen Dateien hinzu, z. B. Signaturen oder WSDL.
  4. Konfigurieren Sie das Profil so, dass die Dateien verwendet werden, und nehmen Sie alle weiteren erforderlichen Änderungen an den Standardeinstellungen vor.
  5. Fügen Sie eine Web App Firewall Richtlinie für dieses Profil hinzu.
  6. Binden Sie die Richtlinie an den Ziel-Bindungspunkt und geben Sie die Priorität an.

- Web App Firewall Entitäten

  Profil— Ein Web App Firewall-Profil gibt an, worauf zu achten ist und was zu tun ist. Es prüft sowohl die Anfrage als auch die Antwort, um festzustellen, welche potenziellen Sicherheitsverstöße überprüft werden müssen und welche Maßnahmen bei der Verarbeitung einer Transaktion ergriffen werden müssen. Ein Profil kann eine HTML-, XML- oder HTML- und XML-Payload schützen. Abhängig von den Sicherheitsanforderungen der Anwendung können Sie entweder ein einfaches oder ein erweitertes Profil erstellen. Ein Basisprofil kann vor bekannten Angriffen schützen. Wenn höhere Sicherheit erforderlich ist, können Sie ein erweitertes Profil bereitstellen, um kontrollierten Zugriff auf die Anwendungsressourcen zu ermöglichen und Zero-Day-Angriffe zu blockieren. Ein Basisprofil kann jedoch geändert werden, um erweiterte Schutzmaßnahmen zu bieten. Es stehen mehrere Aktionsoptionen (z. B. Blockieren, Protokollieren, Lernen und Transformieren) zur Verfügung. Erweiterte Sicherheitsprüfungen können Sitzungscookies und versteckte Formular-Tags verwenden, um die Clientverbindungen zu steuern und zu überwachen. Web App Firewall Profile können die ausgelösten Verstöße lernen und die Relaxationsregeln vorschlagen.

Grundlegender Schutz—Ein Basisprofil enthält einen vorkonfigurierten Satz von Regeln für die Lockerung von Start-URL und URL verweigern. Diese Relaxationsregeln legen fest, welche Anfragen erlaubt und welche abgelehnt werden müssen. Eingehende Anforderungen werden mit diesen Listen abgeglichen, und die konfigurierten Aktionen werden angewendet. Dies ermöglicht es dem Benutzer, Anwendungen mit minimaler Konfiguration für Relaxationsregeln zu sichern. Die Start-URL-Regeln schützen vor erzwungenem Browsen. Bekannte Webserver-Schwachstellen, die von Hackern ausgenutzt werden, können erkannt und blockiert werden, indem eine Reihe von Standard-URL-Regeln verweigern aktiviert wird. Häufig gestartete Angriffe wie Pufferüberlauf, SQL oder siteübergreifende Skripterstellung können ebenfalls leicht erkannt werden.

Erweiterter Schutz— Wie der Name schon sagt, werden erweiterte Schutzmaßnahmen für Anwendungen verwendet, die höhere Sicherheitsanforderungen haben. Relaxationsregeln sind so konfiguriert, dass nur der Zugriff auf bestimmte Daten ermöglicht und der Rest blockiert wird. Dieses positive Sicherheitsmodell mildert unbekannte Angriffe, die möglicherweise nicht durch grundlegende Sicherheitsüberprüfungen erkannt werden. Zusätzlich zu allen grundlegenden Schutzmaßnahmen verfolgt ein erweitertes Profil eine Benutzersitzung, indem es das Browsen steuert, nach Cookies sucht, Eingabeanforderungen für verschiedene Formularfelder spezifiziert und vor Manipulationen von Formularen oder Cross-Site-Anforderungsfälschungen schützt. Das Lernen, das den Datenverkehr beobachtet und die entsprechenden Relaxationen bereitstellt, ist standardmäßig für viele Sicherheitsprüfungen aktiviert. Obwohl sie einfach zu bedienen sind, erfordern erweiterte Schutzmaßnahmen gebührende Berücksichtigung, da sie eine engere Sicherheit bieten, aber auch mehr Verarbeitung erfordern und keine Verwendung von Caching zulassen, was die Leistung beeinträchtigen kann.

Importieren— Die Importfunktion ist nützlich, wenn Web App Firewall-Profile externe Dateien verwenden müssen, dh Dateien, die auf einem externen oder internen Webserver gehostet werden, oder die von einem lokalen Computer kopiert werden müssen. Das Importieren einer Datei und das Speichern auf der Appliance ist nützlich, insbesondere in Situationen, in denen Sie den Zugriff auf externe Websites steuern müssen oder in denen die Kompilierung lange dauert, große Dateien über HA-Bereitstellungen synchronisiert werden müssen, oder Sie können eine Datei wiederverwenden, indem Sie sie auf mehrere Geräte kopieren. Beispiel:

- WSDLs, die auf externen Webservern gehostet werden, können lokal importiert werden, bevor der Zugriff auf externe Websites blockiert wird.
- Große Signaturdateien, die von einem externen Scan-Tool wie Cenzic generiert werden, können mithilfe eines Schemas auf der Citrix Appliance importiert und vorkompiliert werden.
- Eine benutzerdefinierte HTML- oder XML-Fehlerseite kann von einem externen Webserver importiert oder aus einer lokalen Datei kopiert werden.

Signaturen— Signaturen sind mächtig, da sie Musterabgleich verwenden, um bösartige An-

griffe zu erkennen und so konfiguriert werden können, dass sie sowohl die Anforderung als auch die Antwort einer Transaktion überprüfen. Sie sind eine bevorzugte Option, wenn eine anpassbare Sicherheitslösung benötigt wird. Mehrere Auswahlmöglichkeiten (z. B. Blockieren, Protokollieren, Lernen und Transformieren) stehen für die Aktion zur Verfügung, die ausgeführt werden soll, wenn eine Signaturübereinstimmung erkannt wird. Die Web App Firewall verfügt über ein integriertes Standardsignaturobjekt, das aus mehr als 1.300 Signaturregeln besteht, mit der Option, die neuesten Regeln mithilfe der automatischen Update-Funktion abzurufen. Regeln, die von anderen Scan-Tools erstellt wurden, können ebenfalls importiert werden. Das Signaturebjekt kann durch Hinzufügen neuer Regeln angepasst werden, die mit den anderen im Web App Firewall -Profil angegebenen Sicherheitsüberprüfungen arbeiten können. Eine Signaturregel kann mehrere Muster aufweisen und eine Verletzung nur dann kennzeichnen, wenn alle Muster übereinstimmen, wodurch falsche Positive vermieden werden. Die sorgfältige Auswahl eines wörtlichen `fastmatch` Musters für eine Regel kann die Bearbeitungszeit erheblich optimieren.

Richtlinien— Web App Firewall-Richtlinien werden verwendet, um den Datenverkehr in verschiedene Typen zu filtern und zu trennen. Dies bietet die Flexibilität, verschiedene Sicherheitsebenen für die Anwendungsdaten zu implementieren. Der Zugriff auf hochsensible Daten kann auf erweiterte Sicherheitsprüfungen geleitet werden, während weniger sensible Daten durch grundlegende Sicherheitsprüfungen geschützt werden. Richtlinien können auch so konfiguriert werden, dass die Überprüfung der Sicherheitsprüfung auf harmlosen Datenverkehr umgangen wird. Höhere Sicherheit erfordert mehr Verarbeitung, so dass eine sorgfältige Gestaltung der Richtlinien die gewünschte Sicherheit zusammen mit optimierter Leistung bieten kann. Die Priorität der Richtlinie bestimmt die Reihenfolge, in der sie ausgewertet wird, und ihr Bindepunkt bestimmt den Anwendungsbereich ihrer Anwendung.

Highlights

1. Möglichkeit, eine Vielzahl von Anwendungen zu sichern, indem verschiedene Datentypen geschützt werden, das richtige Maß an Sicherheit für verschiedene Ressourcen implementiert und immer noch maximale Leistung erreicht wird.
2. Flexibilität beim Hinzufügen oder Ändern einer Sicherheitskonfiguration. Sie können Sicherheitsprüfungen verschärfen oder entspannen, indem Sie grundlegende und erweiterte Schutzmaßnahmen aktivieren oder deaktivieren.
3. Option zum Konvertieren eines HTML-Profils in ein XML- oder Web2.0-Profil (HTML+XML) und umgekehrt die Flexibilität zur Erhöhung der Sicherheit für verschiedene Arten von Nutzlast.
4. Einfach implementierte Aktionen, um Angriffe zu blockieren, sie in Protokollen zu überwachen, Statistiken zu sammeln oder sogar einige Angriffszeichenfolgen zu transformieren, um sie harmlos zu machen.
5. Fähigkeit, Angriffe durch Inspektion eingehender Anforderungen zu erkennen und das Aus-

laufen vertraulicher Daten zu verhindern, indem die von den Servern gesendeten Antworten überprüft werden.

6. Möglichkeit, aus dem Datenverkehrsmuster zu lernen, um Empfehlungen für leicht bearbeitbare Relaxationsregeln zu erhalten, die bereitgestellt werden können, um Ausnahmen zu erlauben.
7. Hybrides Sicherheitsmodell, das die Leistungsfähigkeit anpassbarer Signaturen anwendet, um Angriffe zu blockieren, die bestimmten Mustern entsprechen, und bietet die Flexibilität, die Positive-Security-Modellüberprüfungen für grundlegende oder erweiterte Sicherheitsvorkehrungen zu verwenden.
8. Verfügbarkeit umfassender Konfigurationsberichte, einschließlich Informationen zur PCI-DSS-Konformität.

Häufig gestellte Fragen und Bereitstellungshandbuch

October 5, 2021

F: Warum ist Citrix Web App Firewall die bevorzugte Wahl für die Sicherung von Anwendungen?

Mit den folgenden Funktionen bietet die Citrix Web App Firewall eine umfassende Sicherheitslösung:

- **Hybrid-Sicherheitsmodell: Das** Hybridsicherheitsmodell von Citrix ADC ermöglicht es Ihnen, sowohl ein positives Sicherheitsmodell als auch ein negatives Sicherheitsmodell zu nutzen, um eine Konfiguration zu erstellen, die sich ideal für Ihre Anwendungen eignet.
  - **Positives Sicherheitsmodell** schützt vor Pufferüberlauf, CGI-BIN-Parameter-Manipulation, Manipulation von Formularen/versteckten Feldern, kraftvollem Browsen, Cookie- oder Sitzungsvergiftung, defekten ACLs, Cross-Site-Scripting (Cross-Site-Scripting), Command Injection, SQL Injection, Fehlerauslösung Informationsleck, unsichere Verwendung von Kryptographie, Server-Fehlkonfiguration, Hintertüren und Debug-Optionen, ratenbasierte Richtliniendurchsetzung, bekannte Plattform-Schwachstellen, Zero-Day-Exploits, Cross Site Request Forgery (CSRF) und das Auslaufen von Kreditkarten und anderen sensiblen Daten.
  - **Negatives Sicherheitsmodell** verwendet umfangreiche Signaturen zum Schutz vor L7- und HTTP-Anwendungsschwachstellen. Die Web App Firewall ist in verschiedene Scan-Tools von Drittanbietern integriert, wie sie von Cenzic, Qualys, Whitehat und IBM angeboten werden. Die integrierten XSLT-Dateien ermöglichen den einfachen Import von Regeln, die in Verbindung mit den native-Format Snort basierten Regeln verwendet werden können. Eine automatische Update-Funktion ruft die neuesten Updates für neue Schwachstellen ab.

Das positive Sicherheitsmodell könnte die bevorzugte Wahl für den Schutz von Anwendungen sein, die einen hohen Sicherheitsbedarf haben, da es Ihnen die Möglichkeit gibt, vollständig zu kontrollieren, wer auf welche Daten zugreifen kann. Sie erlauben nur, was Sie wollen und blockieren den Rest. Dieses Modell enthält eine integrierte Sicherheitskonfiguration, die mit wenigen Klicks bereitgestellt werden kann. Beachten Sie jedoch, dass je strenger die Sicherheit ist, desto größer der Verarbeitungsaufwand.

Das negative Sicherheitsmodell ist möglicherweise für benutzerdefinierte Anwendungen vorzuziehen. Mit den Signaturen können Sie mehrere Bedingungen kombinieren, und eine Übereinstimmung und die angegebene Aktion werden nur ausgelöst, wenn alle Bedingungen erfüllt sind. Sie blockieren nur das, was Sie nicht wollen, und erlauben den Rest. Ein bestimmtes Fast-Match-Muster an einem angegebenen Speicherort kann den Verarbeitungsaufwand erheblich reduzieren, um die Leistung zu optimieren. Die Möglichkeit, eigene Signaturregeln auf der Grundlage der spezifischen Sicherheitsanforderungen Ihrer Anwendungen hinzuzufügen, gibt Ihnen die Flexibilität, Ihre eigenen benutzerdefinierten Sicherheitslösungen zu entwerfen.

- **Request- und Reaktionsseitige Erkennung und Schutz:** Sie können die eingehenden Anfragen überprüfen, um verdächtiges Verhalten zu erkennen und geeignete Maßnahmen zu ergreifen, und Sie können die Antworten überprüfen, um vertrauliche Daten zu erkennen und zu schützen.
- **Umfassender integrierter Schutz für HTML-, XML- und JSON-Nutzlasten:** Die Web App Firewall bietet 19 verschiedene Sicherheitsprüfungen. Sechs davon (z. B. Start-URL und URL verweigern) gelten sowohl für HTML- als auch für XML-Daten. Fünf Prüfungen (z. B. Feldkonsistenz und Feldformat) sind spezifisch für HTML, und acht (z. B. XML-Format und Webdienst-Interoperabilität) sind spezifisch für XML-Nutzlasten. Diese Funktion enthält eine umfangreiche Reihe von Aktionen und Optionen. Mit der URL-Schließung können Sie beispielsweise die Navigation über Ihre Website steuern und optimieren, um sich vor einem erzwungenden Surfen zu schützen, ohne dass Sie Relaxationsregeln konfigurieren müssen, um jede gültige URL zuzulassen. Sie haben die Möglichkeit, die sensiblen Daten, wie Kreditkartennummern, in der Antwort zu entfernen oder zu x-out. Ob SOAP-Array-Angriffsschutz, XML-Denial-of-Service (XDoS), WSDL-Scan-Prävention, Anlagenprüfung oder eine beliebige Anzahl anderer XML-Angriffe — Sie haben den Komfort zu wissen, dass Sie über einen ironclad Shield verfügen, der Ihre Daten schützt, wenn Ihre Anwendungen durch die Web App Firewall geschützt sind. Mit den Signaturen können Sie Regeln mithilfe von XPath-Ausdrücken konfigurieren, um Verletzungen im Körper sowie den Header einer JSON-Nutzlast zu erkennen.
- **GWT:** Unterstützung für den Schutz von Google Web Toolkit-Anwendungen zum Schutz vor SQL, Cross-Site-Scripting und Verstößen gegen die Formularfeldkonsistenzprüfung.
- **Java-freie, benutzerfreundliche grafische Benutzeroberfläche (GUI):** Eine intuitive Benutzeroberfläche und vorkonfigurierte Sicherheitsprüfungen erleichtern die Bereitstellung von Sicherheit durch Klicken auf ein paar Schaltflächen. Ein Assistent fordert Sie auf und führt

Sie dazu, die erforderlichen Elemente wie Profile, Richtlinien, Signaturen und Bindungen zu erstellen. Die HTML5-basierte GUI ist frei von jeglicher Java-Abhängigkeit. Die Leistung ist deutlich besser als die der älteren, Java-basierten Versionen .

- **Benutzerfreundliche und automatisierbare CLI:** Die meisten Konfigurationsoptionen, die in GUI verfügbar sind, sind auch in der Befehlszeilenschnittstelle (CLI) verfügbar. Die CLI-Befehle können über eine Batchdatei ausgeführt werden und sind einfach zu automatisieren.
- **Unterstützung für REST-API:** Das Citrix ADC NITRO -Protokoll unterstützt eine Reihe von REST-APIs, um die Konfiguration der Web App Firewall zu automatisieren und relevante Statistiken für die laufende Überwachung von Sicherheitsverstößen zu sammeln.
- **Lernen:** Die Fähigkeit der Web App Firewall, durch Überwachung des Datenverkehrs zu lernen, um die Sicherheit zu optimieren, ist sehr benutzerfreundlich. Die Lern-Engine empfiehlt Regeln, die das Bereitstellen von Entspannungen ohne Kenntnisse in regulären Ausdrücken erleichtern.
- **RegEx Editorunterstützung:** Reguläre Ausdrücke bieten eine elegante Lösung für das Dilemma, Regeln zu konsolidieren und dennoch die Suche zu optimieren. Sie können die Möglichkeiten regulärer Ausdrücke nutzen, um URLs, Feldnamen, Signaturmuster usw. zu konfigurieren. Der umfangreiche integrierte GUI RegEx Editor bietet Ihnen eine schnelle Referenz für die Ausdrücke und bietet eine bequeme Möglichkeit, Ihre RegEx auf Genauigkeit zu überprüfen und zu testen.
- **Angepasste Fehlerseite:** Gesperrte Anforderungen können an eine Fehler-URL umgeleitet werden. Sie haben auch die Möglichkeit, ein benutzerdefiniertes Fehlerobjekt anzuzeigen, das unterstützte Variablen und Citrix Standardsyntax (erweiterte PI-Ausdrücke) verwendet, um Informationen zur Problembehandlung für den Client einzubetten.
- **PCI-DSS, Statistiken und andere Verstöße:** Mit dem umfangreichen Satz von Berichten ist es einfach, die PCI-DSS-Konformitätsanforderungen zu erfüllen, Statistiken über Verkehrszähler zu sammeln und Verstoßberichte für alle Profile oder nur ein Profil anzuzeigen.
- **Protokollierung und Klick-zu-Regel aus Protokoll:** Detaillierte Protokollierung wird sowohl für native als auch für CEF-Format unterstützt. Die Web App Firewall bietet Ihnen die Möglichkeit, gezielte Protokollmeldungen im Syslog-Viewer zu filtern. Sie können eine Protokollnachricht auswählen und eine entsprechende Relaxationsregel mit einem einfachen Klick auf eine Schaltfläche bereitstellen. Sie haben die Flexibilität, Protokollnachrichten anzupassen und unterstützen auch das Generieren von Webprotokollen. Weitere Informationen finden Sie unter Thema Web App Firewall-Protokolle.
- **Verletzungsprotokolle in Trace-Datensätze einschließen:** Die Möglichkeit, Protokollmeldungen in die Ablaufverfolgungsdatensätze einzuschließen, macht es sehr einfach, unerwartetes Verhalten wie Zurücksetzen und Blockieren zu debuggen.
- **Klonen:** Mit der nützlichen Profiloption Import/Export können Sie die Sicherheitskonfiguration von einer Citrix ADC Appliance auf andere klonen. Optionen zum Exportieren von erlernten

Daten erleichtern den Export der erlernten Regeln in eine Excel-Datei. Sie können sie dann vom Anwendungseigentümer überprüfen und genehmigen lassen, bevor Sie sie anwenden.

- **Eine AppExpert Vorlage** (eine Reihe von Konfigurationseinstellungen) kann so gestaltet werden, dass sie Ihren Websites einen angemessenen Schutz bieten. Sie können die Bereitstellung eines ähnlichen Schutzes auf anderen Appliances vereinfachen und beschleunigen, indem Sie diese Cookie-Cutter-Vorlagen in eine Vorlage exportieren.

Weitere Informationen finden Sie im Thema AppExpert-Vorlage.

- **Sitzungslose Sicherheitsprüfungen:** Durch die Bereitstellung sitzungsloser Sicherheitsprüfungen können Sie den Speicherbedarf reduzieren und die Verarbeitung beschleunigen.
- **Interoperabilität mit anderen Citrix ADC Funktionen:** Die Web App Firewall arbeitet nahtlos mit anderen Citrix ADC Funktionen wie Rewrite, URL-Transformation, integriertes Caching, CVPN und Ratenbegrenzung.
- **Unterstützung von PI-Ausdrücken in Richtlinien:** Sie können die Leistungsfähigkeit erweiterter PI-Ausdrücke nutzen, um Richtlinien zu entwerfen, um unterschiedliche Sicherheitsebenen für verschiedene Teile Ihrer Anwendung zu implementieren.
- **Unterstützung für IPv6:** Die Web App Firewall unterstützt sowohl IPv4- als auch IPv6-Protokolle.
- **Geolokalisierungsbasierter Sicherheitsschutz:** Sie haben die Flexibilität, die Citrix Standardsyntax (PI-Expressions) für die Konfiguration standortbasierter Richtlinien zu verwenden, die in Verbindung mit einer integrierten Standortdatenbank zum Anpassen des Firewallschutzes verwendet werden können. Sie können die Standorte identifizieren, von denen bösartige Anforderungen stammen, und die gewünschte Stufe der Sicherheitskontrollen für Anforderungen, die von einem bestimmten geografischen Standort stammen, durchsetzen.
- **Leistung:** Anforderungsseitiges **Streaming** verbessert die Leistung erheblich. Sobald ein Feld verarbeitet wird, werden die resultierenden Daten an das Backend weitergeleitet, während die Auswertung für die übrigen Felder fortgesetzt wird. Die Verbesserung der Bearbeitungszeit ist besonders bei der Bearbeitung großer Pfosten signifikant.
- **Weitere Sicherheitsfunktionen:** Die Web App Firewall verfügt über mehrere andere Sicherheitseinstellungen, die dazu beitragen können, die Sicherheit Ihrer Daten zu gewährleisten. Mit dem **vertraulichen Feld** können Sie beispielsweise das Versenden vertraulicher Informationen in den Protokollmeldungen blockieren, und **HTML-Kommentar streichen** können Sie die HTML-Kommentare aus der Antwort entfernen, bevor Sie sie an den Client weiterleiten. **Feldtypen** können verwendet werden, um anzugeben, welche Eingaben in den Formularen zulässig sind, die an Ihre Anwendung gesendet werden.

F: Was muss ich tun, um die Web App Firewall zu konfigurieren?

Führen Sie folgende Schritte aus:

- Fügen Sie ein Web App Firewall Profil hinzu, und wählen Sie den entsprechenden Typ (html, xml, web2.0) für die Sicherheitsanforderungen der Anwendung aus.
- Wählen Sie die erforderliche Sicherheitsstufe (Basic oder Advanced) aus.
- Fügen Sie die erforderlichen Dateien hinzu, z. B. Signaturen oder WSDL.
- Konfigurieren Sie das Profil so, dass die Dateien verwendet werden, und nehmen Sie alle weiteren erforderlichen Änderungen an den Standardeinstellungen vor.
- Fügen Sie eine Web App Firewall Richtlinie für dieses Profil hinzu.
- Binden Sie die Richtlinie an den Ziel-Bindungspunkt und geben Sie die Priorität an.

F: Woher weiß ich, welchen Profiltyp ich wählen soll?

Das Web App Firewall Profil bietet Schutz sowohl für HTML- als auch für XML-Nutzlasten. Je nach Bedarf Ihrer Anwendung können Sie entweder ein HTML-Profil oder ein XML-Profil auswählen. Wenn Ihre Anwendung sowohl HTML- als auch XML-Daten unterstützt, können Sie ein Web2.0-Profil auswählen.

F: Was ist der Unterschied zwischen grundlegenden und erweiterten Profilen? Wie entscheide ich, welche ich brauche?

Die Entscheidung, ein Basis- oder ein Advance-Profil zu verwenden, hängt von den Sicherheitsanforderungen Ihrer Anwendung ab. Ein Basisprofil enthält einen vorkonfigurierten Satz von Start-URL und URL-Relaxationsregeln verweigern. Diese Relaxationsregeln bestimmen, welche Anfragen zulässig sind und welche abgelehnt werden. Eingehende Anforderungen werden mit den vorkonfigurierten Regeln abgeglichen, und die konfigurierten Aktionen werden angewendet. Der Benutzer kann Anwendungen mit minimaler Konfiguration von Relaxationsregeln sichern. Die Start-URL-Regeln schützen vor erzwungenem Browsen. Bekannte Webserver-Schwachstellen, die von Hackern ausgenutzt werden, können erkannt und blockiert werden, indem eine Reihe von Standard-URL-Regeln verweigern aktiviert wird. Häufig gestartete Angriffe wie Pufferüberlauf, SQL oder Cross-Site Scripting können ebenfalls leicht erkannt werden.

Wie der Name schon sagt, gelten erweiterte Schutzmaßnahmen für Anwendungen mit höheren Sicherheitsanforderungen. Relaxationsregeln sind so konfiguriert, dass nur der Zugriff auf bestimmte Daten ermöglicht und der Rest blockiert wird. Dieses positive Sicherheitsmodell mildert unbekannte Angriffe, die möglicherweise nicht durch grundlegende Sicherheitsüberprüfungen erkannt werden. Zusätzlich zu allen grundlegenden Schutzmaßnahmen verfolgt ein erweitertes Profil eine Benutzersitzung, indem es das Browsen steuert, nach Cookies sucht, Eingabeanforderungen für verschiedene Formularfelder spezifiziert und vor Manipulation von Formularen oder Cross-Site Request Forgery Angriffe schützt. Das Lernen, das den Datenverkehr beobachtet und die entsprechenden Entspannungen empfiehlt, ist standardmäßig für viele Sicherheitsprüfungen aktiviert. Obwohl sie einfach zu bedienen sind, erfordern erweiterte Schutzmaßnahmen gebührende Beachtung, da sie eine engere Sicherheit bieten, aber auch mehr Verarbeitung erfordern. Einige vorangehende Sicher-

heitsprüfungen erlauben die Verwendung von Caching nicht, was sich auf die Leistung auswirken kann.

Beachten Sie bei der Entscheidung, ob grundlegende oder erweiterte Profile verwendet werden sollen, die folgenden Punkte:

- Grundlegende und erweiterte Profile sind nur Startvorlagen. Sie können das Basisprofil jederzeit ändern, um erweiterte Sicherheitsfunktionen bereitzustellen, und umgekehrt.
- Erweiterte Sicherheitsprüfungen erfordern mehr Verarbeitung und können sich auf die Leistung auswirken. Wenn Ihre Anwendung keine erweiterte Sicherheit benötigt, sollten Sie möglicherweise mit einem Basisprofil beginnen und die für Ihre Anwendung erforderliche Sicherheit erhöhen.
- Sie möchten nicht alle Sicherheitsprüfungen aktivieren, es sei denn, Ihre Anwendung benötigt sie.

F: Was ist eine Richtlinie? Wie wähle ich den Bindepunkt aus und setze die Priorität ein?

Mithilfe von Web App Firewall Richtlinien können Sie Ihren Datenverkehr in logische Gruppen sortieren, um verschiedene Ebenen der Sicherheitsimplementierung zu konfigurieren. Wählen Sie sorgfältig die Bindungspunkte für die Richtlinien aus, um zu bestimmen, welcher Datenverkehr mit welcher Richtlinie abgeglichen wird. Wenn Sie beispielsweise möchten, dass jede eingehende Anfrage auf SQL/Cross-Site Scripting-Angriffe überprüft wird, können Sie eine generische Richtlinie erstellen und sie global binden. Wenn Sie strengere Sicherheitsprüfungen auf den Datenverkehr eines virtuellen Servers anwenden möchten, der Anwendungen hostet, die vertrauliche Daten enthalten, können Sie eine Richtlinie an diesen virtuellen Server binden.

Eine sorgfältige Zuordnung von Prioritäten kann die Datenverarbeitung verbessern. Sie möchten spezifischeren Richtlinien höhere Prioritäten zuweisen und generischen Richtlinien niedrigere Prioritäten zuweisen. Beachten Sie, dass je höher die Zahl, desto niedriger die Priorität. Eine Richtlinie mit der Priorität 10 wird vor einer Richtlinie mit der Priorität 15 bewertet.

Sie können verschiedene Sicherheitsebenen für verschiedene Arten von Inhalten anwenden, z. B. Anfragen für statische Objekte wie Bilder und Text können mithilfe einer Richtlinie umgangen werden, und Anfragen für andere vertrauliche Inhalte können mit einer zweiten Richtlinie einer sehr strengen Prüfung unterzogen werden.

F: Wie kann ich die Regeln zum Sichern meiner Anwendung konfigurieren?

Die Web App Firewall macht es sehr einfach, das richtige Maß an Sicherheit für Ihre Website zu entwerfen. Sie können über mehrere Web App Firewall Richtlinien verfügen, die an unterschiedliche Web-App-Firewall-Profile gebunden sind, um verschiedene Ebenen von Sicherheitsprüfungen für Ihre Anwendungen zu implementieren. Sie können die Protokolle zunächst überwachen, um festzustellen,

welche Sicherheitsbedrohungen erkannt werden und welche Verletzungen ausgelöst werden. Sie können entweder manuell die Relaxationsregeln hinzufügen oder die empfohlenen Lernregeln der Web App Firewall nutzen, um die erforderlichen Relaxationen bereitzustellen, um Fehlalarme zu vermeiden.

Die Citrix Web App Firewall bietet **Visualizer-Unterstützung** in GUI, was die Regelverwaltung sehr einfach macht. Sie können auf einfache Weise alle Daten auf einem Bildschirm anzeigen und Aktionen für mehrere Regeln mit einem Klick durchführen. Der größte Vorteil des Visualizers besteht darin, dass reguläre Ausdrücke zur Konsolidierung mehrerer Regeln empfohlen werden. Sie können eine Teilmenge der Regeln auswählen, basierend auf dem Trennzeichen und der Aktions-URL. Visualizer-Unterstützung ist verfügbar, um 1) erlernte Regeln und 2) Relaxationsregeln anzuzeigen.

1. Der Visualizer für erlernte Regeln bietet die Möglichkeit, die Regeln zu bearbeiten und als Relaxation bereitzustellen. Sie können auch Regeln überspringen (ignorieren).
2. Der Visualizer für bereitgestellte Relaxationen bietet Ihnen die Möglichkeit, eine neue Regel hinzuzufügen oder eine vorhandene Regel zu bearbeiten. Sie können eine Gruppe von Regeln auch aktivieren oder deaktivieren, indem Sie einen Knoten auswählen und im Relaxationsvisualizer auf die Schaltfläche **Aktivieren** oder **Deaktivieren** klicken.

F: Was sind Unterschriften? Woher weiß ich, welche Signaturen ich verwenden soll?

Eine Signatur ist ein Objekt, das mehrere Regeln haben kann. Jede Regel besteht aus einem oder mehreren Mustern, die einem bestimmten Satz von Aktionen zugeordnet werden können. Die Web App Firewall verfügt über ein integriertes Standardsignaturobjekt, das aus mehr als 1.300 Signaturregeln besteht. Mit der Option können Sie die neuesten Regeln mit der **automatischen Update-Funktion** abrufen, um Schutz vor neuen Sicherheitsanfälligkeiten zu erhalten. Regeln, die von anderen Scan-Tools erstellt wurden, können ebenfalls importiert werden.

Signaturen sind sehr leistungsstark, da sie Pattern-Matching verwenden, um bösartige Angriffe zu erkennen, und können so konfiguriert werden, dass sowohl die Anforderung als auch die Antwort einer Transaktion überprüft werden. Sie sind eine bevorzugte Option, wenn eine anpassbare Sicherheitslösung benötigt wird. Mehrere Aktionsoptionen (z. B. Blockieren, Protokollieren, Lernen und Transformieren) stehen zur Verfügung, wenn eine Signaturübereinstimmung erkannt wird. Die Standardsignaturen umfassen Regeln zum Schutz verschiedener Arten von Anwendungen, wie web-cgi, web-coldfusion, web-frontpage, web-iis, web-php, web-client, web-activex, web-shell-shock und web-struts. Um den Anforderungen Ihrer Anwendung gerecht zu werden, können Sie die Regeln auswählen und bereitstellen, die zu einer bestimmten Kategorie gehören.

Tipps zur Signaturnutzung:

- Sie können einfach eine Kopie des Standardsignaturobjekts erstellen und es ändern, um die benötigten Regeln zu aktivieren und die gewünschten Aktionen zu konfigurieren.

- Das Signaturobjekt kann durch Hinzufügen neuer Regeln angepasst werden, die in Verbindung mit anderen Signaturregeln funktionieren können.
- Die Signaturregeln können auch so konfiguriert werden, dass sie in Verbindung mit den im Web App Firewall Profil angegebenen Sicherheitsprüfungen funktionieren. Wenn eine Übereinstimmung, die auf eine Verletzung hinweist, durch eine Signatur und eine Sicherheitsprüfung erkannt wird, wird die restriktivere Aktion durchgesetzt.
- Eine Signaturregel kann mehrere Muster aufweisen und so konfiguriert werden, dass sie nur dann eine Verletzung kennzeichnet, wenn alle Muster übereinstimmen, wodurch falsche Positive vermieden werden.
- Eine sorgfältige Auswahl eines literalen Fast-Match-Musters für eine Regel kann die Verarbeitungszeit erheblich optimieren.

F: Funktioniert die Web App Firewall mit anderen Citrix ADC Funktionen?

Die Web App Firewall ist vollständig in die Citrix ADC Appliance integriert und arbeitet nahtlos mit anderen Funktionen zusammen. Sie können maximale Sicherheit für Ihre Anwendung konfigurieren, indem Sie andere Citrix ADC -Sicherheitsfunktionen in Verbindung mit der Web App Firewall verwenden. **AAA-TM** kann beispielsweise verwendet werden, um den Benutzer zu authentifizieren, die Berechtigung des Benutzers für den Zugriff auf den Inhalt zu überprüfen und die Zugriffe zu protokollieren, einschließlich ungültiger Anmeldeversuche. **Rewrite** kann verwendet werden, um die URL zu ändern oder um Header hinzuzufügen, zu ändern oder zu löschen, und **Responder** kann verwendet werden, um benutzerdefinierte Inhalte an verschiedene Benutzer zu liefern. Sie können die maximale Belastung Ihrer Website definieren, indem Sie die **Rate Limiting** verwenden, um den Datenverkehr zu überwachen und die Rate zu drosseln, wenn sie zu hoch ist. **HTTP-Denial-of-Service (DoS)** -Schutz kann helfen, zwischen echten HTTP-Clients und bösartigen DoS-Clients zu unterscheiden. Sie können den Umfang der Sicherheitsprüfung einschränken, indem Sie die Web App Firewall Richtlinien an virtuelle Server binden und gleichzeitig die Benutzererfahrung optimieren, indem Sie die Funktion **Lastenausgleich** verwenden, um stark verwendete Anwendungen zu verwalten. Anforderungen für statische Objekte wie Bilder oder Text können die Sicherheitskontrolle umgehen und dabei die **integrierte Zwischenspeicherung** oder **Komprimierung** nutzen, um die Bandbreitenauslastung für solche Inhalte zu optimieren.

F: Wie wird die Nutzlast von der Web App Firewall und den anderen Citrix ADC Funktionen verarbeitet?

Ein Diagramm mit Details des L7-Paketflusses in einer Citrix ADC Appliance ist im Abschnitt Verarbeitungsreihenfolge der Features verfügbar.

F: Was ist der empfohlene Workflow für die Bereitstellung der Web App Firewall?

Da Sie nun die Vorteile der Verwendung des hochmodernen Sicherheitsschutzes der Citrix Web App Firewall kennen, können Sie zusätzliche Informationen sammeln, die Ihnen bei der Entwicklung der optimalen Lösung für Ihre Sicherheitsanforderungen helfen können. Citrix empfiehlt Folgendes:

- **Kennen Sie Ihre Umgebung:** Wenn Sie Ihre Umgebung kennen, können Sie die beste Sicherheitslösung (Signaturen, Sicherheitsprüfungen oder beides) für Ihre Anforderungen ermitteln. Bevor Sie mit der Konfiguration beginnen, müssen Sie die folgenden Informationen sammeln.
  - **OS:** Welche Art von Betriebssystem (MS Windows, Linux, BSD, Unix, andere) haben Sie?
  - **Web Server:** Welcher Webserver (IIS, Apache oder Citrix ADC Enterprise Server) wird ausgeführt?
  - **Anwendung:** Welche Art von Anwendungen werden auf Ihrem Anwendungsserver ausgeführt (z. B. ASP.NET, PHP, Cold Fusion, ActiveX, FrontPage, Struts, CGI, Apache Tomcat, Domino und WebLogic)?
  - Haben Sie benutzerdefinierte Anwendungen oder Standardanwendungen (z. B. Oracle, SAP)? Welche Version verwenden Sie?
  - **SSL:** Benötigen Sie SSL? Wenn ja, welche Schlüsselgröße (512, 1024, 2048, 4096) wird zum Signieren von Zertifikaten verwendet?
  - **Traffic Volume:** Wie hoch ist die durchschnittliche Traffic Rate durch Ihre Anwendungen? Haben Sie saisonale oder zeitspezifische Spitzen im Verkehr?
  - **Serverfarm:** Wie viele Server haben Sie? Müssen Sie den Lastausgleich verwenden?
  - **Datenbank:** Welche Art von Datenbank (MS-SQL, MySQL, Oracle, Postgres, SQLite, Nosql, Sybase, Informix usw.) verwenden Sie?
  - **DB-Konnektivität:** Welche Art von Datenbankkonnektivität haben Sie (DSN, Verbindungszeichenfolge pro Datei, Verbindungszeichenfolge für einzelne Dateien) und welche Treiber werden verwendet?
- **Identifizieren Sie Ihre Sicherheitsanforderungen:** Vielleicht möchten Sie bewerten, welche Anwendungen oder bestimmte Daten maximalen Sicherheitsschutz benötigen, welche weniger anfällig sind und welche für die Sicherheitsinspektion sicher umgangen werden kann. Dies hilft Ihnen bei der Erstellung einer optimalen Konfiguration und beim Entwerfen geeigneter Richtlinien und Bindungspunkte, um den Datenverkehr zu trennen. Sie können beispielsweise eine Richtlinie konfigurieren, um die Sicherheitsprüfung von Anforderungen für statische Webinhalte wie Bilder, MP3-Dateien und Filme zu umgehen, und eine andere Richtlinie so konfigurieren, dass erweiterte Sicherheitsprüfungen auf Anforderungen für dynamischen Inhalt angewendet werden. Sie können mehrere Richtlinien und Profile verwenden, um unterschiedliche Inhalte derselben Anwendung zu schützen.
- **Lizenzanforderung:** Citrix bietet eine einheitliche Lösung zur Optimierung der Leistung Ihrer Anwendung, indem Sie zahlreiche Funktionen wie Load Balancing, Content Switching, Caching, Komprimierung, Responder, Rewrite und Content-Filterung nutzen, um nur einige zu nennen. Wenn Sie die gewünschten Funktionen identifizieren, können Sie entscheiden, welche Lizenz

Sie benötigen.

- **Installieren und Basieren einer Citrix ADC Appliance:** Erstellen Sie einen virtuellen Server, und führen Sie Testdatenverkehr durch diesen aus, um sich einen Überblick über die Geschwindigkeit und den Umfang des Datenverkehrs zu verschaffen, der durch Ihr System fließt. Diese Informationen helfen Ihnen dabei, Ihre Kapazitätsanforderungen zu identifizieren und die richtige Appliance (VPX, MPX oder SDX) auszuwählen.
- **Bereitstellen der Web App Firewall:** Verwenden Sie den Web App Firewall Assistenten, um mit einer einfachen Sicherheitskonfiguration fortzufahren. Der Assistent führt Sie durch mehrere Bildschirme und fordert Sie auf, ein Profil, eine Richtlinie, eine Signatur und Sicherheitsprüfungen hinzuzufügen.
  - **Profil:** Wählen Sie einen aussagekräftigen Namen und den entsprechenden Typ (HTML, XML oder WEB 2.0) für Ihr Profil. Die Richtlinie und Signaturen werden automatisch mit demselben Namen generiert.
  - **Richtlinie:** Die automatisch generierte Richtlinie hat den Standardausdruck (true), der den gesamten Datenverkehr auswählt und global gebunden ist. Dies ist ein guter Ausgangspunkt, es sei denn, Sie haben eine bestimmte Richtlinie, die Sie verwenden möchten.
  - **Schutz:** Der Assistent unterstützt Sie dabei, das Hybridsicherheitsmodell zu nutzen, in dem Sie die Standardsignaturen verwenden können, die eine Reihe von Regeln bieten, um verschiedene Arten von Anwendungen zu schützen. Im**einfachen** Bearbeitungsmodus können Sie die verschiedenen Kategorien (CGI, Cold Fusion, PHP usw.) anzeigen. Sie können eine oder mehrere Kategorien auswählen, um einen bestimmten Satz von Regeln für Ihre Anwendung zu identifizieren. Verwenden Sie die Option **Aktion**, um alle Signaturregeln in den ausgewählten Kategorien zu aktivieren. Stellen Sie sicher, dass das Blockieren deaktiviert ist, damit Sie den Datenverkehr überwachen können, bevor Sie die Sicherheit verschärfen. Klicken Sie auf **Weiter**. Im Bereich **Deep Protection angeben** können Sie bei Bedarf Änderungen vornehmen, um den Schutz der Sicherheitsprüfung bereitzustellen. In den meisten Fällen reichen grundlegende Schutzmaßnahmen für die anfängliche Sicherheitskonfiguration aus. Führen Sie den Datenverkehr für eine Weile aus, um eine repräsentative Stichprobe der Sicherheitsinspektionsdaten zu sammeln.
  - **Verschärfung der Sicherheit:** Nach der Bereitstellung der Web App Firewall und der Überwachung des Datenverkehrs für eine Weile können Sie mit der Verschärfung der Sicherheit Ihrer Anwendungen beginnen, indem Sie Entspannungen bereitstellen und dann die Blockierung aktivieren. **Learning**, **Visualizer**und **Click to Deployment-Regeln**sind nützliche Funktionen, die es sehr einfach machen, Ihre Konfiguration zu optimieren, um genau das richtige Maß an Entspannung zu finden. An dieser Stelle können Sie auch den Richtlinienausdruck ändern und/oder zusätzliche Richtlinien und Profile konfigurieren, um die gewünschten Sicherheitsebenen für verschiedene Inhaltstypen zu implementieren.

- **Debugging:** Wenn Sie unerwartetes Verhalten Ihrer Anwendung sehen, bietet die Web App Firewall verschiedene Optionen zum einfachen Debuggen:
  * **Log**. Wenn legitime Anfragen blockiert werden, überprüfen Sie zunächst die Datei ns.log, um zu sehen, ob eine unerwartete Sicherheitsüberprüfungsverletzung ausgelöst wird.
  * **Funktion deaktivieren.** Wenn Sie keine Verletzungen sehen, aber immer noch unerwartetes Verhalten sehen, z. B. eine Anwendung zurücksetzen oder teilweise Antworten senden, können Sie die Web App Firewall Funktion zum Debuggen deaktivieren. Wenn das Problem weiterhin besteht, schließt es die Web App Firewall als Verdächtiger aus.
  * **Verfolgen Sie Datensätze mit Protokollmeldungen.** Wenn das Problem im Zusammenhang mit der Web App Firewall zu sein scheint und eine genauere Überprüfung erforderlich ist, haben Sie die Option, Sicherheitsverletzungsmeldungen in ein nstrace aufzunehmen. Sie können Follow TCP-Stream im Trace verwenden, um die Details der einzelnen Transaktion, einschließlich Header, Payload und die entsprechende Log-Nachricht, zusammen auf demselben Bildschirm anzuzeigen. Einzelheiten zur Verwendung dieser Funktionalität finden Sie in den Anhängen.

Einführung in die Citrix Web Application Firewall

October 8, 2021

Die Citrix Web App Firewall verhindert Sicherheitsverletzungen, Datenverlust und mögliche unbefugte Änderungen an Websites, die auf sensible Geschäfts- oder Kundeninformationen zugreifen. Dies geschieht, indem sowohl Anfragen als auch Antworten gefiltert, sie auf Beweise für böswillige Aktivitäten untersucht und Anfragen blockiert werden, die solche Aktivitäten aufweisen. Ihre Website ist nicht nur vor gängigen Arten von Angriffen geschützt, sondern auch vor neuen, noch unbekannten Angriffen. Neben dem Schutz von Webservern und Websites vor unbefugtem Zugriff schützt die Web App Firewall vor Schwachstellen in Legacy-CGI-Code oder -Skripten, Webframeworks, Webserver-Software und anderen zugrunde liegenden Betriebssystemen.

Die Citrix Web App Firewall ist als eigenständige Appliance oder als Funktion auf einer virtuellen Citrix ADC Appliance (VPX) verfügbar. In der Web App Firewall-Dokumentation bezieht sich der Begriff Citrix ADC auf die Plattform, auf der die Web App Firewall ausgeführt wird, unabhängig davon, ob es sich bei dieser Plattform um eine dedizierte Firewall-Appliance, ein Citrix ADC, auf dem auch andere Funktionen konfiguriert wurden, oder um ein Citrix ADC VPX handelt.

Um die Web App Firewall verwenden zu können, müssen Sie mindestens eine Sicherheitskonfiguration erstellen, um Verbindungen zu blockieren, die gegen die Regeln verstoßen, die Sie für Ihre geschützten Websites festgelegt haben. Die Anzahl der Sicherheitskonfigurationen, die Sie

möglicherweise erstellen möchten, hängt von der Komplexität Ihrer Website ab. Manchmal reicht eine einzige Konfiguration aus. In anderen Fällen, insbesondere in solchen, in denen interaktive Websites, Websites, die auf Datenbankserver zugreifen, Online-Shops mit Einkaufswagen, benötigen Sie möglicherweise mehrere verschiedene Konfigurationen, um sensible Daten am besten zu schützen, ohne großen Aufwand für Inhalte zu verschwenden, die für bestimmte Arten von -Angriffe. Sie können die Standardeinstellungen für die globalen Einstellungen, die sich auf alle Sicherheitskonfigurationen auswirken, oft unverändert lassen. Sie können jedoch die globalen Einstellungen ändern, wenn sie mit anderen Teilen Ihrer Konfiguration in Konflikt stehen oder Sie sie lieber anpassen möchten.

Sicherheit für Webanwendungen

Webanwendungssicherheit ist Netzwerksicherheit für Computer und Programme, die mit der HTTP- und HTTPS-Protokolle kommunizieren. Dies ist ein weites Gebiet, in dem es viele Sicherheitslücken und Schwächen gibt. Betriebssysteme auf Servern und Clients haben Sicherheitsprobleme und sind anfällig für Angriffe. Webserver-Software und Website-Endering-Technologien wie CGI, Java, JavaScript, PERL und PHP weisen zugrunde liegende Schwachstellen auf. Browser und andere Clientanwendungen, die mit webfähigen Anwendungen kommunizieren, weisen ebenfalls Schwachstellen auf. Websites, die eine beliebige Technologie verwenden, jedoch die einfachste HTML, einschließlich aller Websites, die die Interaktion mit Besuchern ermöglicht, weisen häufig eigene Schwachstellen auf.

In der Vergangenheit war eine Sicherheitsverletzung oft nur ein Ärger, aber heute ist das selten der Fall. Zum Beispiel waren Angriffe, bei denen ein Hacker Zugriff auf einen Webserver erhielt und unbefugte Änderungen an einer Website vorgenommen (unkennbar) machte, üblich. Sie wurden in der Regel von Hackern gestartet, die keine Motivation hatten, außer anderen Hackern ihre Fähigkeiten zu demonstrieren oder die zielgerichtete Person oder Firma in Verlegenheit zu bringen. Die meisten aktuellen Sicherheitsverletzungen sind jedoch durch den Wunsch nach Geld motiviert. Die Mehrheit versucht, eines oder beide der folgenden Ziele zu erreichen: sensible und potenziell wertvolle private Informationen zu erhalten oder unbefugten Zugriff auf und die Kontrolle über eine Website oder einen Webserver zu erhalten.

Bestimmte Formen von Web-Attacken konzentrieren sich auf die Beschaffung privater Informationen. Diese Angriffe sind oft sogar gegen Websites möglich, die sicher genug sind, um einen Angreifer daran zu hindern, die volle Kontrolle zu übernehmen. Zu den Informationen, die ein Angreifer von einer Website erhalten kann, können Kundennamen, Adressen, Telefonnummern, Sozialversicherungsnummern, Kreditkartennummern, Krankenakten und andere private Informationen umfassen. Der Angreifer kann diese Informationen dann verwenden oder an andere verkaufen. Ein Großteil der Informationen, die durch solche Angriffe erhalten werden, ist gesetzlich geschützt, und all dies durch Gewohnheit und Erwartung. Ein Verstoß dieser Art kann schwerwiegende Folgen für Kunden haben, deren private Informationen gefährdet sind. Im besten Fall müssen diese Kunden wachsam sein, um zu verhindern, dass andere ihre Kreditkarten missbrauchen, nicht autorisierte

Kreditkonten in ihrem Namen eröffnen oder ihre Identität direkt aneignen (Identitätsdiebstahl). Im schlimmsten Fall können die Kunden ruinierte Kreditratings oder sogar für kriminelle Aktivitäten verantwortlich gemacht werden, an denen sie keine Rolle hatten.

Andere Web-Angriffe zielen darauf ab, die Kontrolle über eine *Website oder*den Server, auf dem sie arbeitet, oder beides zu erlangen. Ein Hacker, der die Kontrolle über eine Website oder einen Server erlangt, kann damit nicht autorisierte Inhalte hosten, als Proxy für Inhalte fungieren, die auf einem anderen Webserver gehostet werden, SMTP-Dienste bereitstellen, um unerwünschte Massen-E-Mails zu senden, oder DNS-Dienste zur Unterstützung solcher Aktivitäten auf anderen kompromittierten Webservern bereitstellen. Die meisten Websites, die auf kompromittierten Webservern gehostet werden, fördern fragwürdige oder direkt betrügerische Unternehmen. Beispielsweise werden die meisten Phishing-Websites und Websites zur Ausbeutung von Kindern auf kompromittierten Webservern gehostet.

Der Schutz Ihrer Websites und Webdienste vor diesen Angriffen erfordert eine mehrschichtige Verteidigung, die sowohl bekannte Angriffe mit identifizierbaren Merkmalen blockieren als auch vor unbekannten Angriffen schützen kann, die häufig erkannt werden können, da sie sich vom normalen Datenverkehr zu Ihren Websites und Ihrem Web unterscheiden -Dienstleistungen.

Bekannte Webangriffe

Die erste Verteidigungslinie für Ihre Websites ist der Schutz vor der Vielzahl von Angriffen, von denen bekannt ist, dass sie existieren und von Web-Sicherheitsexperten beobachtet und analysiert wurden. Zu den häufigsten Arten von Angriffen auf HTML-basierte Websites gehören:

- **Pufferüberlaufangriffe.** Das Senden einer langen URL, eines langen Cookies oder langer Informationen an einen Webserver führt dazu, dass das System hängen bleibt, abstürzt oder unbefugten Zugriff auf das zugrunde liegende Betriebssystem bietet. Ein Pufferüberlaufangriff kann verwendet werden, um Zugriff auf nicht autorisierte Informationen zu erhalten, um einen Webserver oder beides zu gefährden.
- **Cookie-Sicherheitsangriffe.** Senden eines modifizierten Cookies an einen Webserver, in der Regel in der Hoffnung, Zugriff auf nicht autorisierte Inhalte durch gefälschte Anmeldeinformationen zu erhalten.
- **Zwangsvolles Surfen.** Direkter Zugriff auf URLs auf einer Website, ohne zu den URLs mit Hyperlinks auf der Startseite oder anderen allgemeinen Start-URLs auf der Website zu navigieren. Einzelne Fälle von kraftvollem Surfen können auf einen Benutzer hinweisen, der eine Seite auf Ihrer Website mit einem Lesezeichen versehen hat, aber wiederholte Versuche, auf nicht vorhandene Inhalte oder Inhalte zuzugreifen, auf die Benutzer niemals direkt zugreifen dürfen, stellen häufig einen Angriff auf die Website-Sicherheit dar. Erzwungenes Browsen wird normalerweise verwendet, um Zugriff auf nicht autorisierte Informationen zu erhalten, kann aber auch mit einem Pufferüberlaufangriff kombiniert werden, um Ihren Server zu gefährden.

- **Webformular-Sicherheitsangriffe.** Senden Sie unangemessene Inhalte in einem Webformular an Ihre Website. Unangemessene Inhalte können modifizierte ausgeblendete Felder, HTML oder Code in einem Feld enthalten, das nur für alphanumerische Daten bestimmt ist, eine zu lange Zeichenfolge in einem Feld, das nur eine kurze Zeichenfolge akzeptiert, eine alphanumerische Zeichenfolge in einem Feld, das nur eine ganze Zahl akzeptiert, und eine Vielzahl anderer Daten, die Ihre Website nicht akzeptiert erwarte, in diesem Webformular zu erhalten. Ein Sicherheitsangriff auf ein Web-Formular kann entweder verwendet werden, um nicht autorisierte Informationen von Ihrer Website zu erhalten oder um die Website direkt zu gefährden, normalerweise in Kombination mit einem Pufferüberlaufangriff.

Zwei spezielle Arten von Angriffen auf die Sicherheit von Webformularen verdienen besondere Erwähnung:

- **SQL-Injection-Angriffe.** Senden eines aktiven SQL-Befehls oder von Befehlen in einem Webformular oder als Teil einer URL, mit dem Ziel, dass eine SQL-Datenbank den Befehl oder die Befehle ausführt. SQL-Injection-Angriffe werden normalerweise verwendet, um nicht autorisierte Informationen zu erhalten.
- **Cross-Site-Skripting-Angriffe.** Verwenden einer URL oder eines Skripts auf einer Webseite, um gegen die Richtlinie für denselben Ursprung zu verstoßen, die es jedem Skript verbietet, Eigenschaften von einer anderen Website zu erhalten oder zu ändern. Da Skripts Informationen auf Ihrer Website abrufen und Dateien ändern können, kann der Zugriff eines Skripts auf Inhalte auf einer anderen Website einem Angreifer die Möglichkeit geben, nicht autorisierte Informationen zu erhalten, einen Webserver oder beides zu gefährden.

Angriffe auf XML-basierte Webdienste fallen normalerweise in mindestens eine der folgenden zwei Kategorien: Versuche, unangemessene Inhalte an einen Webdienst zu senden, oder Versuche, die Sicherheit eines Webdienstes zu verletzen. Häufige Arten von Angriffen gegen XML-basierte Webdienste sind:

- **Bösartiger Code oder Objekte.** XML-Anforderungen, die Code oder Objekte enthalten, die entweder direkt sensible Informationen abrufen oder einem Angreifer die Kontrolle über den Webdienst oder den zugrunde liegenden Server geben können.
- **Schlecht geformte XML-Anforderungen.** XML-Anforderungen, die nicht der W3C-XML-Spezifikation entsprechen und daher die Sicherheit eines unsicheren Webdienstes verletzen können
- **Denial-of-Service-Angriffe (DoS).** XML-Anforderungen, die wiederholt und in hohem Umfang gesendet werden, mit der Absicht, den zielgerichteten Webdienst zu überwältigen und legitimen Benutzern den Zugriff auf den Webdienst zu verweigern.

Neben standardmäßigen XML-basierten Angriffen sind XML-Webdienste und Web 2.0-Websites auch anfällig für SQL-Injection und Cross-Site-Skripting-Angriffe, wie unten beschrieben:

- **SQL-Injection-Angriffe.** Senden eines aktiven SQL-Befehls oder von Befehlen in einer XML-basierten Anforderung, mit dem Ziel, dass eine SQL-Datenbank diesen Befehl oder diese Befehle

ausführt. Wie bei HTML-SQL-Injectionsangriffen werden XML-SQL-Injectionsangriffe normalerweise verwendet, um nicht autorisierte Informationen zu erhalten.

- **Cross-Site-Skripting-Angriffe.** Verwenden eines Skripts, das in einer XML-basierten Anwendung enthalten ist, um gegen die Richtlinie des gleichen Ursprungs zu verstoßen, wodurch kein Skript Eigenschaften aus einer anderen Anwendung abrufen oder ändern kann. Da Skripts Informationen abrufen und Dateien mithilfe Ihrer XML-Anwendung ändern können, kann es einem Angreifer ermöglichen, nicht autorisierte Informationen zu erhalten, die Anwendung zu gefährden, oder beides zu gefährden.

Bekannte Webangriffe können normalerweise gestoppt werden, indem der Website-Verkehr nach bestimmten Merkmalen (Signaturen) gefiltert wird, die immer für einen bestimmten Angriff auftreten und niemals im legitimen Datenverkehr erscheinen dürfen. Dieser Ansatz hat die Vorteile, dass relativ wenige Ressourcen benötigt werden und ein relativ geringes Risiko von False-Positives darstellt. Daher ist es ein wertvolles Werkzeug zur Bekämpfung von Angriffen auf Websites und Webdienste und zur Konfiguration des grundlegenden Signaturschutzes.

Unbekannte Webangriffe

Die größte Bedrohung für Websites und Anwendungen ist nicht durch bekannte Angriffe, sondern durch unbekannte Angriffe. Die meisten unbekannten Angriffe fallen in eine von zwei Kategorien: neu eingeleitete Angriffe, für die Sicherheitsfirmen noch keine effektive Verteidigung entwickelt haben (Zero-Day-Angriffe), und sorgfältig gezielte Angriffe auf eine bestimmte Website oder einen Webdienst und nicht auf viele Websites oder Webdienste (Speerangriffe). Diese Angriffe, wie bekannte Angriffe, sollen sensible private Informationen erhalten, die Website oder den Webservice gefährden und die Verwendung für weitere Angriffe oder beide dieser Ziele ermöglichen.

Zero-Day-Angriffe stellen eine große Bedrohung für alle Benutzer dar. Diese Angriffe sind in der Regel von den gleichen Arten wie bekannte Angriffe; Zero-Day-Angriffe beinhalten oft injizierte SQL, ein siteübergreifendes Skript, eine siteübergreifende Anforderungsfälschung oder eine andere Art von Angriff ähnlich wie bekannte Angriffe. In der Regel zielen sie auf Schwachstellen ab, die den Entwicklern der Zielsoftware, der Website oder des Webdienstes entweder nicht bewusst sind oder von denen sie erfahren haben. Sicherheitsfirmen haben daher keine Abwehrmaßnahmen gegen diese Angriffe entwickelt, und selbst wenn dies der Fall ist, haben Benutzer die Patches nicht erhalten und installiert oder die zum Schutz vor diesen Angriffen erforderlichen Problemumgehungen durchgeführt. Die Zeit zwischen der Entdeckung eines Zero-Day-Angriffs und der Verfügbarkeit einer Verteidigung (dem Schwachstellenfenster) schrumpft, aber die Täter können immer noch auf Stunden oder sogar Tage zählen, in denen viele Websites und Webdienste keinen spezifischen Schutz vor dem Angriff haben.

Spear-Angriffe sind eine große Bedrohung, aber für eine ausgewählte Gruppe von Benutzern. Eine übliche Art von Speerangriff, ein Spear-Phishes, richtet sich an Kunden einer bestimmten Bank oder eines Finanzinstituts oder (seltener) an Mitarbeiter eines bestimmten Unternehmens oder einer bestimmten Organisation. Im Gegensatz zu anderen Phishes, bei denen es sich oft um grob geschriebene

Fälschungen handelt, die ein Benutzer, der mit der tatsächlichen Kommunikation dieser Bank oder dieses Finanzinstituts vertraut ist, erkennen kann, sind Speerphishes perfekt und überzeugend. Sie können spezifische Informationen enthalten, die für den Einzelnen spezifisch sind, die auf den ersten Blick kein Fremder wissen oder erhalten darf. Der Speer-Phisher ist daher in der Lage, das Ziel davon zu überzeugen, die angeforderten Informationen bereitzustellen, die der Phisher dann verwenden kann, um unrechtmäßig erhaltenes Geld aus anderen Quellen zu verarbeiten oder Zugang zu anderen, noch sensibleren Informationen zu erhalten.

Beide Arten von Angriffen haben bestimmte Merkmale, die normalerweise erkannt werden können, wenn auch nicht mit statischen Mustern, die nach bestimmten Merkmalen suchen, wie Standardsignaturen. Die Erkennung dieser Arten von Angriffen erfordert anspruchsvollere und ressourcenintensivere Ansätze, wie heuristische Filterung und positive Sicherheitsmodellsysteme. Heuristische Filterung sieht nicht für bestimmte Muster, sondern für Verhaltensmuster aus. Positive Sicherheitsmodellsysteme modellieren das normale Verhalten der Website oder des Webdienstes, den sie schützen, und blockieren dann Verbindungen, die nicht in dieses Modell der normalen Verwendung passen. URL-basierte und webformularbasierte Sicherheitsprüfungen erfassen die normale Nutzung Ihrer Websites und steuern dann, wie Benutzer mit Ihren Websites interagieren, wobei sowohl Heuristik als auch positive Sicherheit verwendet werden, um anomalen oder unerwarteten Datenverkehr zu blockieren. Sowohl heuristische als auch positive Sicherheit, die ordnungsgemäß entworfen und bereitgestellt werden, können die meisten Angriffe erfassen, die Signaturen verpassen. Sie benötigen jedoch wesentlich mehr Ressourcen als Signaturen, und Sie müssen einige Zeit damit verbringen, sie richtig zu konfigurieren, um Fehlalarme zu vermeiden. Sie werden daher nicht als primäre Verteidigungslinie verwendet, sondern als Backups von Signaturen oder anderen weniger ressourcenintensiven Ansätzen.

Durch die Konfiguration dieser erweiterten Schutzmaßnahmen zusätzlich zu Signaturen erstellen Sie ein hybrides Sicherheitsmodell, das es der Web App Firewall ermöglicht, umfassenden Schutz vor bekannten und unbekannten Angriffen zu bieten.

Funktionsweise der Citrix Web Application Firewall

Wenn Sie die Web App Firewall installieren, erstellen Sie eine erste Sicherheitskonfiguration, die aus einer Richtlinie, einem Profil und einem Signaturobjekt besteht. Die Richtlinie ist eine Regel, die den zu filternden Datenverkehr identifiziert, und das Profil identifiziert die Muster und Verhaltenstypen, die erlaubt oder blockiert werden sollen, wenn der Datenverkehr gefiltert wird. Die einfachsten Muster, die als Signaturen bezeichnet werden, werden nicht innerhalb des Profils angegeben, sondern in einem Signaturobjekt, das dem Profil zugeordnet ist.

Eine Signatur ist eine Zeichenfolge oder ein Muster, die einer bekannten Art von Angriff entspricht. Die Web App Firewall enthält über tausend Signaturen in sieben Kategorien, die jeweils auf Angriffe auf bestimmte Arten von Webservern und Webinhalten gerichtet sind. Citrix aktualisiert die Liste mit neuen Signaturen, wenn neue Bedrohungen erkannt werden. Während der Konfiguration geben Sie

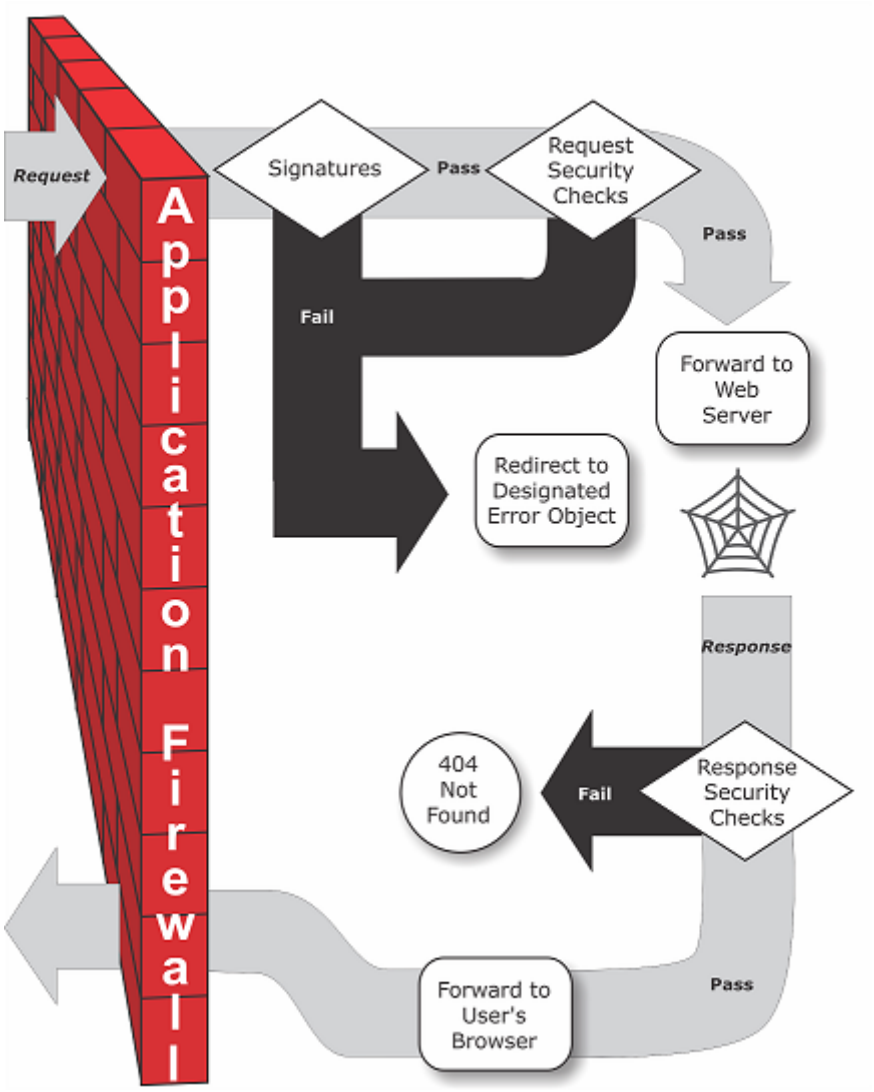
die Signaturkategorien an, die für die zu schützenden Webserver und Inhalte geeignet sind. Signaturen bieten einen guten Grundschutz bei geringem Verarbeitungsaufwand. Wenn Ihre Anwendungen spezielle Schwachstellen aufweisen oder Sie einen Angriff gegen sie erkennen, für den keine Signatur vorhanden ist, können Sie eigene Signaturen hinzufügen.

Die fortgeschrittenen Schutzmaßnahmen werden als Sicherheitsprüfungen bezeichnet. Eine Sicherheitsüberprüfung ist eine strengere, algorithmischere Prüfung einer Anfrage nach bestimmten Mustern oder Verhaltensweisen, die auf einen Angriff hinweisen oder eine Bedrohung für Ihre geschützten Websites und Webdienste darstellen könnten. Sie kann beispielsweise eine Anforderung identifizieren, die versucht, eine bestimmte Art von Vorgang auszuführen, die die Sicherheit verletzen könnte, oder eine Antwort, die vertrauliche private Informationen wie eine Sozialversicherungsnummer oder Kreditkartennummer enthält. Während der Konfiguration geben Sie die Sicherheitsprüfungen an, die für die zu schützenden Webserver und Inhalte geeignet sind. Die Sicherheitsprüfungen sind restriktiv. Viele von ihnen können legitime Anfragen und Antworten blockieren, wenn Sie bei der Konfiguration keine entsprechenden Ausnahmen (Relaxationen) hinzufügen. Die Identifizierung der erforderlichen Ausnahmen ist nicht schwierig, wenn Sie die Funktion zum adaptiven Lernen verwenden, die die normale Nutzung Ihrer Website beobachtet und empfohlene Ausnahmen schafft.

Die Web App Firewall kann entweder als Layer 3-Netzwerkgerät oder als Layer 2-Netzwerkbrücke zwischen Ihren Servern und Ihren Benutzern installiert werden, normalerweise hinter dem Router oder der Firewall Ihres Unternehmens. Er muss an einem Ort installiert sein, an dem er den Datenverkehr zwischen den zu schützenden Webservern und dem Hub abfangen kann oder über den Benutzer auf diese Webserver zugreifen kann. Anschließend konfigurieren Sie das Netzwerk so, dass Anforderungen an die Web App Firewall anstatt direkt an Ihre Webserver gesendet werden, und Antworten auf die Web App Firewall statt direkt an Ihre Benutzer. Die Web App Firewall filtert diesen Datenverkehr, bevor er an das endgültige Ziel weiterleitet. Dabei wird sowohl der interne Regelsatz als auch die Ergänzungen und Änderungen verwendet. Es blockiert oder macht harmlos alle Aktivitäten, die es als schädlich erkennt, und leitet dann den verbleibenden Datenverkehr an den Webserver weiter. Die folgende Abbildung gibt einen Überblick über den Filterprozess.

> **Hinweis:**
>
> Die Abbildung lässt die Anwendung einer Richtlinie auf eingehenden Datenverkehr auslassen. Es zeigt eine Sicherheitskonfiguration, in der die Richtlinie alle Anforderungen verarbeiten soll. Außerdem wurde in dieser Konfiguration ein Signaturobjekt konfiguriert und dem Profil zugeordnet, und Sicherheitsprüfungen wurden im Profil konfiguriert.

Abbildung 1. Ein Flussdiagramm der Web App Firewall Filterung



Wie die Abbildung zeigt, prüft die Web App Firewall, wenn ein Benutzer eine URL auf einer geschützten Website anfordert, zuerst die Anfrage, um sicherzustellen, dass sie nicht mit einer Signatur übereinstimmt. Wenn die Anforderung mit einer Signatur übereinstimmt, zeigt die Citrix Web Application Firewall entweder das Fehlerobjekt an (eine Webseite, die sich auf der Web App Firewall Appliance befindet und die Sie mithilfe der Importfunktion konfigurieren können) oder leitet die Anfrage an die angegebene Fehler-URL (die Fehlerseite) weiter. Signaturen benötigen nicht so viele Ressourcen wie Sicherheitsprüfungen. Das Erkennen und Beenden von Angriffen, die von einer Signatur erkannt werden, bevor eine der Sicherheitsprüfungen ausgeführt wird, verringert die Belastung des Servers.

Wenn eine Anforderung die Signaturprüfung bestanden hat, wendet die Web App Firewall die aktivierten Anforderungssicherheitsprüfungen an. Die Anforderungssicherheitsprüfungen stellen sicher, dass die Anfrage für Ihre Website oder Ihren Webdienst geeignet ist und kein Material enthält, das eine Bedrohung darstellen könnte. Beispielsweise untersuchen Sicherheitsprüfungen die Anforderung auf Zeichen, die darauf hindeuten, dass es sich um einen unerwarteten Typ handelt,

unerwarteten Inhalt anfordern oder unerwartete und möglicherweise bösartige Webformulardaten, SQL-Befehle oder Skripts enthalten. Wenn die Anforderung eine Sicherheitsprüfung fehlschlägt, bereinigt die Web App Firewall die Anforderung entweder und sendet sie dann an die Citrix ADC Appliance (oder die virtuelle Citrix ADC-Appliance) oder zeigt das Fehlerobjekt an. Wenn die Anforderung die Sicherheitsprüfungen bestanden hat, wird sie an die Citrix ADC Appliance zurückgesendet, die jede andere Verarbeitung abschließt und die Anforderung an den geschützten Webserver weiterleitet.

Wenn die Website oder der Webdienst eine Antwort an den Benutzer sendet, wendet die Web App Firewall die aktivierten Reaktionssicherheitsprüfungen an. Die Reaktionssicherheitsprüfungen untersuchen die Reaktion auf Lecks sensibler privater Informationen, Anzeichen für eine Website-Verunstaltung oder andere Inhalte, die nicht vorhanden sein dürfen. Wenn die Antwort eine Sicherheitsprüfung nicht besteht, entfernt die Web App Firewall entweder den Inhalt, der nicht vorhanden sein darf, oder blockiert die Antwort. Wenn die Antwort die Sicherheitsprüfungen bestanden hat, wird sie an die Citrix ADC Appliance zurückgesendet, die sie an den Benutzer weiterleitet.

Citrix Web Application Firewall-Funktionen

Die grundlegenden Funktionen der Web App Firewall sind Richtlinien, Profile und Signaturen, die ein hybrides Sicherheitsmodell bereitstellen, wie unter Bekannte Webangriffe, Unbekannte Webangriffeund Funktionsweise der Web App Firewallbeschrieben. Besonders hervorzuheben ist die Lernfunktion, die den Datenverkehr zu Ihren geschützten Anwendungen beobachtet und geeignete Konfigurationseinstellungen für bestimmte Sicherheitsprüfungen empfiehlt.

Die Importfunktion verwaltet Dateien, die Sie in die Web App Firewall hochladen. Diese Dateien werden dann von der Web App Firewall bei verschiedenen Sicherheitsprüfungen oder bei der Reaktion auf eine Verbindung verwendet, die einer Sicherheitsprüfung entspricht.

Sie können die Funktionen für Protokolle, Statistiken und Berichte verwenden, um die Leistung der Web App Firewall zu bewerten und mögliche Anforderungen an mehr Schutz zu ermitteln.

Ändern des Anwendungsdatenverkehrs durch Citrix Web Application Firewall

Die Citrix Web Application Firewall wirkt sich auf das Verhalten einer Webanwendung aus, die sie schützt, indem sie Folgendes ändert:

- Cookies
- HTTP-Header
- Formulare/Daten

Citrix Web Application Firewall-Sitzungscookie

Um den Status der Sitzung beizubehalten, generiert die Citrix ADC Web App Firewall ein eigenes Sitzungscookie. Dieses Cookie wird nur zwischen dem Webbrowser und der Citrix ADC Web Application Firewall und nicht an den Webserver übergeben. Wenn ein Hacker versucht, das Sitzungscookie zu ändern, löscht die Application Firewall das Cookie, bevor die Anforderung an den Server weitergeleitet wird und behandelt die Anforderung als eine neue Benutzersitzung. Das Session-Cookie ist vorhanden, solange der Webbrowser geöffnet ist. Wenn der Webbrowser geschlossen wird, wird das Sitzungscookie der Application Firewall länger gültig. Der Status der Sitzung verwaltet die Informationen der vom Kunden besuchten URLs und Formulare.

Das konfigurierbare Web App Firewall -Sitzungscookie lautet `citrix_ns_id`.

Ab Citrix ADC Build 12.1 54 und 13.0 ist die Cookie-Konsistenz sitzungslos und erzwingt nicht das Hinzufügen von Sitzungscookie, das von der Appliance `citrix_ns_id` generiert wird.

Citrix Web App Firewall Cookies

Viele Webanwendungen generieren Cookies, um benutzer- oder sitzungsspezifische Informationen zu verfolgen. Diese Informationen können Benutzerpräferenzen oder Warenkorbelemente sein. Ein Webanwendungs-Cookie kann einer der folgenden zwei Typen sein:

- **Permanente Cookies** - Diese Cookies werden lokal auf dem Computer gespeichert und beim nächsten Besuch der Website wieder verwendet. Diese Art von Cookie enthält in der Regel Informationen über den Benutzer, wie Anmeldung, Kennwort oder Einstellungen.
- **Sitzungs- oder transiente Cookies** - Diese Cookies werden nur während der Sitzung verwendet und nach Beendigung der Sitzung zerstört. Diese Art von Cookie enthält Informationen zum Anwendungsstatus, wie Einkaufswagenartikel oder Sitzungsdaten.

Hacker können versuchen, Anwendungscookies zu modifizieren oder zu stehlen, um eine Benutzersitzung zu entführen oder als Benutzer zu maskieren. Die Application Firewall verhindert solche Versuche, indem sie die Anwendungs-Cookies hasht und dann weitere Cookies mit den digitalen Signaturen hinzufügt. Durch die Verfolgung der Cookies stellt die Application Firewall sicher, dass die Cookies zwischen dem Client-Browser und der Application Firewall weder verändert noch gefährdet werden. Die Application Firewall ändert die Anwendungscookies nicht.

Die Citrix Web Application Firewall generiert die folgenden Standardcookies, um die Anwendungscookies zu verfolgen:

- **Permanente Cookies**: `citrix_ns_id_wlf`. Hinweis: wlf steht für wird ewig leben.
- **Sitzungs- oder vorübergehende Cookies**: `citrix_ns_id_wat`. Hinweis: wat steht für wird vorübergehend handeln.
  Um die Anwendungscookies zu verfolgen, gruppiert die Application Firewall die persistenten oder Session-Anwendungs-Cookies zusammen und hash und signiert dann alle Cookies zusam-

men. Daher generiert die Application Firewall ein `wlf` Cookie, um alle persistenten Anwendungscookies zu verfolgen, und ein `wat` Cookie, um alle Anwendungssitzungscookies zu verfolgen.

Die folgende Tabelle zeigt die Anzahl und Typen der Cookies, die von der Application Firewall basierend auf den von der Webanwendung generierten Cookies generiert werden:

Vor der Citrix ADC Web App Firewall	Vorgang
Ein persistentes Cookie	Persistentes Cookie: `citix_ns_id_wlf`
Ein vorübergehendes Cookie	Transientes Cookie: `citix_ns_id_wat`
Mehrere persistente Cookies, Mehrere transiente Cookies	Ein dauerhafter Cookie: `citrix_ns_id_wlf`Ein Transient-Cookie: `citix_ns_id_wat`

Citrix Web App Firewall ermöglicht die Verschlüsselung des Anwendungs-Cookie. Application Firewall bietet auch eine Option zum Proxy des Sitzungscookie, das von der Anwendung gesendet wird, indem es mit den restlichen Sitzungsdaten der Application Firewall gespeichert und nicht an den Client gesendet wird. Wenn ein Client eine Anforderung an die Anwendung sendet, die ein Anwendungsfirewall Sitzungscookie enthält, fügt Application Firewall das gesendete Cookie zurück in die Anforderung ein, bevor die Anforderung an die Ursprungsanwendung gesendet wird. Application Firewall ermöglicht auch das Hinzufügen der HttpOnly und/oder Secure Flags zu Cookies.

Wie sich die Anwendungsfirewall auf HTTP-Header auswirkt

Sowohl HTTPS-Anfragen als auch HTTPS-Antworten verwenden Header, um Informationen über eine oder mehrere Nachrichten von HPS zu senden. Ein Header ist eine Reihe von Zeilen, wobei jede Zeile einen Namen enthält, gefolgt von einem Doppelpunkt, einem Leerzeichen und einem Wert. Beispielsweise hat der Host-Header das folgende Format:

```
Host: www.citrix.com
```

Einige Header-Felder werden sowohl in Anforderungs- als auch in Antwort-Headern verwendet, während andere nur für eine Anforderung oder eine Antwort geeignet sind. Die Application Firewall kann einige Header in einer oder mehreren HTTPS-Anfragen oder -Antworten hinzufügen, ändern oder löschen, um die Sicherheit der Anwendung zu gewährleisten.

Anforderungsheader, die von der Citrix Web Application Firewall gelöscht wurden

Viele der Anforderungsheader, die sich auf das Caching beziehen, werden gelöscht, um jede Anfrage im Kontext einer Sitzung anzuzeigen. Wenn die Anforderung einen Codierungsheader enthält, der

es dem Webserver ermöglicht, komprimierte Antworten zu senden, löscht die Application Firewall diesen Header, sodass der Inhalt der Antwort auf dem unkomprimierten Server von der Web App Firewall überprüft wird, um ein Auslaufen vertraulicher Daten an den Client zu verhindern.

Die Anwendungsfirewall löscht die folgenden Anforderungsheader:

- Bereich — Wird zum Wiederherstellen von fehlgeschlagenen oder teilweisen Dateiübertragungen verwendet.
- If-Range — Ermöglicht es einem Client, ein partielles Objekt abzurufen, wenn es bereits einen Teil dieses Objekts in seinem Cache enthält (bedingtes GET).
- If-Modified-Since — Wenn das angeforderte Objekt seit der in diesem Feld angegebenen Zeit nicht geändert wird, wird keine Entität vom Server zurückgegeben. Sie erhalten einen HTTP 304 nicht modifizierten Fehler.
- If-None-Match — Ermöglicht effiziente Aktualisierungen zwischengespeicherter Informationen mit einem minimalen Overhead.
- Accept-Encoding — Welche Codierungsmethoden sind für ein bestimmtes Objekt erlaubt, wie gzip.

Anforderungsheader, geändert von der Citrix Web Application Firewall

Wenn ein Webbrowser HTTP/1.0 oder frühere Protokolle verwendet, öffnet und schließt der Browser kontinuierlich die TCP-Socket-Verbindung, nachdem jede Antwort empfangen wurde. Dies erhöht den Aufwand für den Webserver und verhindert die Aufrechterhaltung des Sitzungsstatus. Das HTTP/1.1-Protokoll ermöglicht es, dass die Verbindung während der Sitzung geöffnet bleibt. Die Application Firewall ändert den folgenden Anforderungsheader, um HTTP/1.1 zwischen der Application Firewall und dem Webserver zu verwenden, unabhängig von dem vom Webbrowser verwendeten Protokoll:
Verbindung: keep-alive

Anforderungskopfzeilen, die von der Citrix Web Application Firewall hinzugefügt wurden

Die Application Firewall fungiert als Reverse-Proxy und ersetzt die ursprüngliche Quell-IP-Adresse der Sitzung durch die IP-Adresse der Application Firewall. Daher zeigen alle Anfragen, die im Webserverprotokoll protokolliert wurden, an, dass die Anforderungen von der Application Firewall gesendet werden.

Antwort-Header, der von der Citrix Web Application Firewall gelöscht wurde

Die Anwendungsfirewall blockiert oder ändert möglicherweise Inhalte wie das Entfernen von Kreditkartennummern oder das Entfernen von Kommentaren. Dies kann zu einer Abweichung in der Größe führen. Um ein solches Szenario zu verhindern, löscht die Application Firewall den folgenden Header:

Content-Length — Gibt die Größe der an den Empfänger gesendeten Nachricht an.
Von der Anwendungsfirewall geänderte Antwort-Header

Viele der Antwort-Header, die von der Application Firewall geändert wurden, beziehen sich auf das Zwischenspeichern. Caching-Header in HTTP (S) -Antworten müssen geändert werden, um zu zwingen, dass der Webbrowser immer eine Anforderung an den Webserver für die neuesten Daten sendet und nicht den lokalen Cache verwendet. Einige ASP-Anwendungen verwenden jedoch separate Plug-Ins, um dynamische Inhalte anzuzeigen und erfordern möglicherweise die Möglichkeit, die Daten vorübergehend im Browser zwischenzuspeichern. Um temporäres Zwischenspeichern von Daten zu ermöglichen, wenn Advanced Security-Schutzmaßnahmen wie FFC, URL-Schließung oder CSRF-Prüfungen aktiviert sind, fügt Application Firewall die Cache-Control-Header in der Serverantwort hinzu oder ändert sie mithilfe der folgenden Logik:

- Wenn Server Pragma: no-cache sendet, führt die Application Firewall keine Änderung durch.
- Wenn die Clientanfrage HTTP 1.0 ist, fügt die Application Firewall Pragma: no-cache ein.
- Wenn Client Request HTTP 1.1 ist und Cache-Control: no-store hat, nimmt die Application Firewall keine Änderungen vor.
- Wenn Client Request HTTP 1.1 ist und Server Response Cache-Control-Header ohne Store oder keine Cache-Direktive hat, nimmt Application Firewall keine Änderungen vor.
- Wenn Client Request HTTP 1.1 ist und Server Response entweder No Cache-Control-Header oder Cache-Control-Header keine Store- oder No-Cache-Direktive hat, führt die Application Firewall die folgenden Aufgaben aus:

1. Fügt Cache-Control ein: max-age=3, must-revalidate, privat.
2. Fügt X-Cache-Control-orig = Ursprünglicher Wert von Cache-Control Header ein.
3. Löscht zuletzt geänderte Kopfzeile.
4. Ersetzt Etag.
5. Fügt X-Expires-Orig=Ursprünglicher Wert des vom Server gesendeten Expire-Headers ein.
6. Ändert den Expires-Header und legt das Ablaufdatum der Webseite auf die Vergangenheit fest, sodass sie immer wieder aufgenommen wird.
7. Ändert Akzept-Bereiche und setzt sie auf keine.

Um vorübergehend zwischengespeicherte Daten im Clientbrowser zu ersetzen, wenn Application Firewall die Antwort ändert, z. B. für StripComments, X-out/Remove SafeObject, xout oder Credit Card oder URL Transform, führt Application Firewall die folgenden Aktionen durch:

1. Löscht die letzte Änderung vom Server, bevor sie an den Client weitergeleitet wird.
2. Ersetzt Etag durch einen Wert, der von der Application Firewall bestimmt wird.

Von der Citrix Web App Firewall hinzugefügte Antwortkopfzeilen

- `Transfer-Encoding`: Chunked. Dieser Header streamt Informationen an einen Client zurück, ohne die Gesamtlänge der Antwort kennen zu müssen, bevor die Antwort gesendet wird. Dieser Header ist erforderlich, da der Content-length Header entfernt wird.
- `Set-Cookie`: Die von der Application Firewall hinzugefügten Cookies.
- `Xet-Cookie`: Wenn die Sitzung gültig ist und die Antwort nicht im Cache abgelaufen ist, können Sie aus dem Cache dienen und müssen kein neues Cookie senden, da die Sitzung noch gültig ist. In einem solchen Szenario wird das Set-Cookie in Xet-Cookie geändert. Für den Webbrowser.

Wie Formulardaten betroffen sind

Die Application Firewall schützt vor Angriffen, bei denen versucht wird, den Inhalt des ursprünglichen Formulars zu ändern, das vom Server gesendet wurde. Es kann auch vor Cross-Site-Request-Fälschungsangriffen schützen. Die Application Firewall erreicht durch das Einfügen des versteckten Formular-Tags al_fid in die Seite.

Beispiel:`<input type=”hidden”name=”as_fid”value=”VRgWq0I196Jmg/+LOY7C”/>`

Das ausgeblendete Feld as_fid wird für die Feldkonsistenz verwendet. Dieses Feld wird von Application Firewall verwendet, um alle Felder des Formulars einschließlich der verborgenen Feldname/Wert-Paare zu verfolgen und sicherzustellen, dass keines der Felder des Formulars, das vom Server gesendet wird, auf der Clientseite geändert wird. Die CSRF-Prüfung verwendet auch dieses eindeutige Formular-Tag as_fid, um sicherzustellen, dass die vom Benutzer übermittelten Formulare dem Benutzer in dieser Sitzung zugestellt wurden und kein Hacker versucht, die Benutzersitzung zu entführen.

Sitzungslose Formularprüfung

Application Firewall bietet außerdem eine Option zum Schutz von Formulardaten mit sitzungsloser Feldkonsistenz. Dies ist nützlich für Anwendungen, bei denen Formulare eine große Anzahl dynamischer ausgeblendeter Felder aufweisen können, die zu einer hohen Speicherzuweisung pro Sitzung durch die Anwendungsfirewall führen. Die Sitzungslose Feldkonsistenzprüfung wird durchgeführt, indem ein anderes ausgeblendetes Feld as_ffc_field nur für POST-Anfragen oder für GET- und POST-Anforderungen basierend auf der konfigurierten Einstellung eingefügt wird. Die Application Firewall ändert die Methode GET in POST, wenn sie das Formular an den Client weiterleitet. Die Appliance setzt die Methode dann auf GET zurück, wenn sie an den Server zurückgesendet wird. Der Wert as_ffc_field kann groß sein, da er den verschlüsselten Digest des gesendeten Formulars enthält. Im Folgenden finden Sie ein Beispiel für die sitzungslose Formularprüfung:

```
1 <input type=”hidden” name=”as_ffc_field” value=”CwAAAAVIGLD/
     luRRi1Wu1rbYrFYargEDcO5xVAxsEnMP1megXuQfiDTGbwk0fpgndMHqfMbzfAFdjwR+
     TOm1oT
```



```
+u+Svo9+NuloPhtnbkxGtNe7gB/o8GlxEcK9ZkIIVv3oIL/
    nIPSRWJljgpWgafzVx7wtugNwnn8/
    GdnhneLCJTaYU7ScnC6LexJDLisI1xsEeONWt8Zm
+vJTa3mTebDY6LVyhDpDQfBgI1XLgfLTexAUzSNWHYyloqPruGYfnRPw+
    DIGf6gGwn1BYLEsRHKNbjJBrKpOJo9JzhEqdtZ1g3bMzEF9PocPvM1Hpvi5T6VB
/YFunUFM4f+bD7EAVcugdhovzb71CsSQX5+qcC1B8WjQ==" />
<!--NeedCopy-->
```

HTML-Kommentarentfernung

Die Application Firewall bietet außerdem die Möglichkeit, alle HTML-Kommentare in den Antworten zu entfernen, bevor sie an den Client gesendet werden. Dies betrifft nicht nur Formulare, sondern alle Antwortseiten. Die Application Firewall sucht und entfernt jeden Text, der zwischen “<!-“ und “->” Kommentar-Tags. Die Tags zeigen weiterhin an, dass an diesem Speicherort des HTML-Quellcodes ein Kommentar vorhanden war. Jeder Text, der in andere HTML- oder JavaScript-Tags eingebettet ist, wird ignoriert.
Einige Anwendungen funktionieren möglicherweise nicht korrekt, wenn JavaScript falsch in Kommentar-Tags eingebettet ist. Ein Vergleich des Seitenquellcodes vor und nachdem die Kommentare von Application Firewall entfernt wurden, kann bei der Identifizierung helfen, ob in einem der gestrippten Kommentare das erforderliche JavaScript eingebettet wurde.

Kreditkartenschutz

Die Application Firewall bietet eine Option, um die Header und den Hauptteil der Antwort zu überprüfen und die Kreditkartennummern entweder zu entfernen oder zu entfernen, bevor die Antwort an den Client weitergeleitet wird. Derzeit bietet Application Firewall Schutz für die folgenden gängigen Kreditkarten: American Express, Diners Club, Discover, JCB, MasterCard und Visa. Die x-out-Aktion funktioniert unabhängig von der Block-Aktion.

Sicherer Objektschutz

Ähnlich wie bei Kreditkartennummern kann auch das Auslaufen anderer sensibler Daten verhindert werden, indem die Sicherheitsüberprüfung von Application Firewall für sicheres Objekt verwendet wird, um die sensiblen Inhalte in der Antwort zu entfernen oder zu löschen.

Siteübergreifendes Skripting transformiert Aktion

Wenn die Transformation für Cross-Site-Scripting aktiviert ist, ändert sich die Web App Firewall `”<”into ”%26lt;”and ”>”into ”%26gt;”` in den Anfragen. Wenn die Einstellung “CheckRequestHeaders” in der Web App Firewall aktiviert ist, überprüft die Web App Firewall die Request-Header und transformiert diese Zeichen auch in Header und Cookies. Die Transformationsaktion blockiert oder

transformiert keine Werte, die ursprünglich vom Server gesendet wurden. Es gibt eine Reihe von Standardattributen und Tags für Cross-Site-Scripting, die die Web App Firewall zulässt. Eine Standardliste der verweigerten Cross-Site-Scripting-Muster wird ebenfalls bereitgestellt. Diese können angepasst werden, indem Sie das Signaturobjekt auswählen und auf den **Dialog SQL/Cross-Site Scripting Patterns verwalten** in der GUI klicken.

Transformieren von SQL-Sonderzeichen

Application Firewall verfügt über die folgenden Standard-Transformationsregeln für SQL-Sonderzeichen:

Unter	Vorgang	Transformation
‘(einfaches Anführungszeichen, das heißt, %27)	”	Ein weiteres einfaches Zitat
\ (umgekehrter Schrägstrich, der ist%5C)	|Ein weiterer umgekehrter Schrägstrich hinzugefügt	
; (Semikolon, das ist%3B)		- Abgefallen

Wenn die Transformation von Sonderzeichen aktiviert ist und die checkRequestheAdern auf ON gesetzt ist, erfolgt die Transformation von Sonderzeichen auch in Headern und Cookies.
Hinweis: Einige Anforderungsheader wie User-Agent, Accept-Encoding enthalten normalerweise Semikolons und können von der SQL-Transformation beeinflusst werden.

Verhalten der Citrix Web Application Firewall, bei dem der Inspect Header beschädigt wird

1. Immer wenn NetScaler eine HTTP-Anfrage mit dem Expect-Header erhält, sendet NetScaler die Antwort expect: 100 -continue an den Client im Namen des Backend-Servers.
2. Dieses Verhalten liegt daran, dass der Schutz der Application Firewall für die gesamte Anfrage ausgeführt werden muss, bevor die Anfrage an den Server weitergeleitet wird. NetScaler muss die gesamte Anfrage vom Client abrufen.
3. Nach Erhalt einer `100 continue` Antwort sendet der Kunde den verbleibenden Teil der Anfrage, der die Anfrage abschließt.
4. NetScaler führt dann alle Schutzmaßnahmen aus und leitet die Anforderung dann an den Server weiter.
5. Jetzt, da NetScaler die vollständige Anfrage weiterleitet, wird der expect -Header, der in der ersten Anfrage enthalten ist, veraltet, da NetScaler diesen Header beschädigt und an den Server sendet.
6. Server beim Empfang der Anforderung ignoriert alle Header, die beschädigt sind.

Konfigurieren der Web App Firewall

October 8, 2021

Sie können die Citrix Web App Firewall (Web App Firewall) mit einer der folgenden Methoden konfigurieren:

- **Web App Firewall Assistent.** Ein Dialogfeld, das aus einer Reihe von Bildschirmen besteht, die Sie durch den Konfigurationsprozess führen.
- **Citrix Web Interface AppExpert Vorlage.** Eine AppExpert Vorlage (eine Reihe von Konfigurationseinstellungen), die einen angemessenen Schutz für Websites bieten soll. Diese AppExpert Vorlage enthält geeignete Konfigurationseinstellungen für die Web App Firewall zum Schutz vieler Websites.
- **Citrix ADC GUI.** Die webbasierte Konfigurationsschnittstelle.
- **Citrix ADC Befehlszeilenschnittstelle.** Die Befehlszeilenkonfigurationsschnittstelle.

Citrix empfiehlt die Verwendung des Web App Firewall Assistenten. Die meisten Benutzer finden es die einfachste Methode, die Web App Firewall zu konfigurieren, und sie wurde entwickelt, um Fehler zu vermeiden. Wenn Sie ein neues Citrix ADC oder VPX haben, das Sie hauptsächlich zum Schutz von Websites verwenden werden, finden Sie möglicherweise die Webinterface AppExpert Vorlage als eine bessere Option, da sie eine gute Standardkonfiguration bietet, nicht nur für die Web App Firewall, sondern für die gesamte Appliance. Sowohl die GUI als auch die Befehlszeilenschnittstelle sind für erfahrene Benutzer gedacht, in erster Linie um eine vorhandene Konfiguration zu ändern oder erweiterte Optionen zu verwenden.

Der Web App Firewall Assistent

Der Web App Firewall Assistent ist ein Dialogfeld, das aus mehreren Bildschirmen besteht, in denen Sie aufgefordert werden, jeden Teil einer einfachen Konfiguration zu konfigurieren. Die Web App Firewall erstellt dann die entsprechenden Konfigurationselemente aus den von Ihnen angegebenen Informationen. Dies ist der einfachste und für die meisten Zwecke der beste Weg, um die Web App Firewall zu konfigurieren.

Um den Assistenten zu verwenden, stellen Sie mit dem Browser Ihrer Wahl eine Verbindung zur GUI her. Wenn die Verbindung hergestellt wird, überprüfen Sie, ob die Web App Firewall aktiviert ist, und führen Sie dann den Web App Firewall-Assistenten aus, der Sie zur Eingabe von Konfigurationsinformationen auffordert. Sie müssen nicht alle angeforderten Informationen angeben, wenn Sie den Assistenten zum ersten Mal verwenden. Stattdessen können Sie Standardeinstellungen akzeptieren, einige relativ einfache Konfigurationsaufgaben ausführen, um wichtige Funktionen zu aktivieren, und dann zulassen, dass die Web App Firewall wichtige Informationen sammeln kann, um die Konfiguration abzuschließen.

Wenn der Assistent Sie beispielsweise auffordert, eine Regel für die Auswahl des zu verarbeitenden Datenverkehrs anzugeben, können Sie die Standardeinstellung übernehmen, die den gesamten Datenverkehr auswählt. Wenn eine Liste von Signaturen angezeigt wird, können Sie die entsprechenden Signaturkategorien aktivieren und die Sammlung von Statistiken für diese Signaturen aktivieren. Bei dieser Erstkonfiguration können Sie den erweiterten Schutz (Sicherheitsprüfungen) überspringen. Der Assistent erstellt automatisch die entsprechende Richtlinie, das Signaturobjekt und das entsprechende Profil (gemeinsam die Sicherheitskonfiguration) und bindet die Richtlinie an global. Die Web App Firewall beginnt dann mit dem Filtern von Verbindungen zu Ihren geschützten Websites, protokolliert alle Verbindungen, die mit einer oder mehreren der von Ihnen aktivierten Signaturen übereinstimmen, und sammelt Statistiken über die Verbindungen, denen jede Signatur entspricht. Nachdem die Web App Firewall einen bestimmten Datenverkehr verarbeitet hat, können Sie den Assistenten erneut ausführen und die Protokolle und Statistiken überprüfen, um festzustellen, ob eine der aktivierten Signaturen mit dem legitimen Datenverkehr übereinstimmt. Nachdem Sie ermittelt haben, welche Signaturen den Datenverkehr identifizieren, den Sie blockieren möchten, können Sie die Blockierung für diese Signaturen aktivieren. Wenn Ihre Website oder Webdienst nicht komplex ist, keine SQL verwendet und keinen Zugriff auf vertrauliche private Informationen hat, bietet diese grundlegende Sicherheitskonfiguration wahrscheinlich einen angemessenen Schutz.

Möglicherweise benötigen Sie zusätzlichen Schutz, wenn Ihre Website beispielsweise dynamisch ist. Inhalte, die Skripts verwenden, benötigen möglicherweise Schutz vor websiteübergreifenden Skriptangriffen. Webinhalte, die SQL verwenden, z. B. Einkaufswagen, viele Blogs und die meisten Content-Management-Systeme, benötigen möglicherweise Schutz vor SQL-Injection-Angriffen. Websites und Webdienste, die vertrauliche private Informationen wie Sozialversicherungsnummern oder Kreditkartennummern erfassen, können Schutz vor unbeabsichtigter Offenlegung dieser Informationen erfordern. Bestimmte Arten von Web-Server- oder XML-Server-Software erfordern möglicherweise Schutz vor Arten von Angriffen, die auf diese Software zugeschnitten sind. Eine andere Überlegung ist, dass bestimmte Elemente Ihrer Websites oder Webdienste einen anderen Schutz erfordern als andere Elemente. Wenn Sie die Protokolle und Statistiken der Web App Firewall überprüfen, können Sie die zusätzlichen Schutzmaßnahmen identifizieren, die Sie möglicherweise benötigen.

Nachdem Sie entschieden haben, welche erweiterten Schutzmaßnahmen für Ihre Websites und Webdienste erforderlich sind, können Sie den Assistenten erneut ausführen, um diese Schutzmaßnahmen zu konfigurieren. Bestimmte Sicherheitsprüfungen erfordern, dass Sie Ausnahmen (Relaxationen) eingeben, um zu verhindern, dass die Überprüfung den legitimen Datenverkehr blockiert. Sie können dies manuell tun, aber es ist in der Regel einfacher, die adaptive Lernfunktion zu aktivieren und ihm die notwendige Entspannung zu empfehlen. Sie können den Assistenten so oft wie nötig verwenden, um Ihre grundlegende Sicherheitskonfiguration zu verbessern und/oder zusätzliche Sicherheitskonfigurationen zu erstellen.

Der Assistent automatisiert einige Aufgaben, die Sie manuell ausführen müssen, wenn Sie den Assistenten nicht verwenden. Es erstellt automatisch eine Richtlinie, ein Signaturobjekt und ein Profil und

weist ihnen den Namen zu, den Sie angegeben haben, als Sie zur Eingabe des Namens Ihrer Konfiguration aufgefordert wurden. Der Assistent fügt auch Ihre Einstellungen für den verstärkten Schutz dem Profil hinzu, bindet das Signaturobjekt an das Profil, ordnet das Profil der Richtlinie zu und setzt die Richtlinie durch Bindung an Global in Kraft.

Einige Aufgaben können im Assistenten nicht ausgeführt werden. Sie können den Assistenten nicht verwenden, um eine Richtlinie an einen anderen Bindepunkt als Global zu binden. Wenn das Profil nur auf einen bestimmten Teil der Konfiguration angewendet werden soll, müssen Sie die Bindung manuell konfigurieren. Sie können die Moduleinstellungen oder bestimmte andere globale Konfigurationsoptionen im Assistenten nicht konfigurieren. Sie können zwar eine der erweiterten Schutzeinstellungen im Assistenten konfigurieren, aber wenn Sie eine bestimmte Einstellung in einer einzigen Sicherheitsprüfung ändern möchten, ist es möglicherweise einfacher, dies auf den manuellen Konfigurationsbildschirmen in der GUI zu tun.

Weitere Informationen zur Verwendung des Web App Firewall-Assistenten finden Sie unter Der Web App Firewall-Assistent.

Die Citrix Web Interface AppExpert Vorlage

AppExpert Templates sind ein anderer und einfacherer Ansatz zur Konfiguration und Verwaltung komplexer Unternehmensanwendungen. Die AppExpert Anzeige in der GUI besteht aus einer Tabelle. Anwendungen werden in der Spalte ganz links aufgeführt, wobei die Citrix ADC Funktionen, die für diese Anwendung gelten, jeweils in einer eigenen Spalte rechts angezeigt werden. (In der AppExpert Schnittstelle werden die Funktionen, die einer Anwendung zugeordnet sind, als *Anwendungseinheiten*bezeichnet.) In der AppExpert t-Benutzeroberfläche konfigurieren Sie den interessanten Datenverkehr für jede Anwendung und aktivieren Regeln für Komprimierung, Zwischenspeichern, Umschreiben, Filtern, Responder und die Web App Firewall, anstatt jedes Feature einzeln konfigurieren zu müssen.

Web Interface AppExpert Template enthält Regeln für die folgenden Web App Firewall -Signaturen und Sicherheitsprüfungen:

- **URL-Prüfung verweigern.** Erkennt Verbindungen zu Inhalten, die bekanntermaßen ein Sicherheitsrisiko darstellen, oder zu anderen URLs, die Sie festlegen.
- **Pufferüberlauf-Prüfung.** Erkennt Versuche, einen Pufferüberlauf auf einem geschützten Webserver zu verursachen.
- **Überprüfung der Cookie-Konsistenz.** Erkennt bösartige Änderungen an Cookies, die von einer geschützten Website gesetzt werden.
- **Konsistenzprüfung für Formularfelder.** Erkennt Änderungen an der Struktur eines Webformulars auf einer geschützten Website.
- **Überprüfung der CSRF-Formularkennzeichnung.** Erkennt Angriffe zur siteübergreifenden Anforderungsfälschung.

- **Überprüfung der Feldformate.** Erkennt unangemessene Informationen, die in Webformularen auf einer geschützten Website hochgeladen wurden.
- **Überprüfung der HTML SQL-Einschleusung.** Erkennt Versuche, nicht autorisierten SQL-Code zu injizieren.
- **HTML-Site-übergreifende Skript-Überprüfung** Erkennt Cross-Site-Scripting-Angriffe.

Informationen zum Installieren und Verwenden einer AppExpert-Vorlage finden Sie unter AppExpert AppExpert AppApplications and Templates.

Die Citrix GUI

Die GUI ist eine webbasierte Schnittstelle, die Zugriff auf alle Konfigurationsoptionen für die Web App Firewall Funktion bietet, einschließlich erweiterter Konfigurations- und Verwaltungsoptionen, die nicht über andere Konfigurationstools oder Schnittstellen verfügbar sind. Insbesondere können viele erweiterte Signaturoptionen nur in der GUI konfiguriert werden. Sie können Empfehlungen, die von der Lernfunktion generiert wurden, nur in der GUI überprüfen. Sie können Richtlinien nur in der GUI an einen anderen Bindepunkt als Global binden.

Eine Beschreibung der GUI finden Sie unter Die Web App Firewall-Konfigurationsschnittstellen. Weitere Informationen zur Verwendung der GUI zum Konfigurieren der Web App Firewall finden Sie unter Manuelle Konfiguration mit der GUI.

Anweisungen zum Konfigurieren der Web App Firewall über die grafische Benutzeroberfläche finden Sie unter Manuelle Konfiguration mit der GUI. Informationen zur Citrix-ADC-GUI finden Sie unter Die Web App Firewall-Konfigurationsschnittstellen.

Die Citrix ADC Befehlszeilenschnittstelle

Die Citrix ADC Befehlszeilenschnittstelle ist eine modifizierte UNIX-Shell, die auf der FreeBSD bash Shell basiert. Um die Web App Firewall über die Befehlszeilenschnittstelle zu konfigurieren, geben Sie Befehle an der Eingabeaufforderung ein und drücken die Eingabetaste, genau wie bei jeder anderen Unix-Shell. Sie können die meisten Parameter und Optionen für die Web App Firewall mit der NetScaler Befehlszeile konfigurieren. Ausnahmen sind die Signaturfunktion, von denen viele Optionen nur über die GUI oder den Web App Firewall Assistenten konfiguriert werden können, und die Lernfunktion, deren Empfehlungen nur in der GUI überprüft werden können.

Anweisungen zum Konfigurieren der Web App Firewall mithilfe der Citrix ADC-Befehlszeile finden Sie unter Manuelle Konfiguration mit der Befehlszeilenschnittstelle.

Citrix Web App Firewall aktivieren

October 5, 2021

Bevor Sie eine Sicherheitskonfiguration erstellen können, müssen Sie die Citrix Web App Firewall Funktion auf der Appliance aktivieren.

Wichtige Punkte

- Wenn Sie eine dedizierte Citrix Web App Firewall Appliance konfigurieren oder ein vorhandenes Gerät aktualisieren, ist das Feature bereits aktiviert. Sie müssen keines der hier beschriebenen Verfahren durchführen.
- Wenn Sie über einen neuen Citrix ADC oder VPX verfügen, müssen Sie die Citrix Web App Firewall Funktion aktivieren, bevor Sie sie konfigurieren.
- Wenn Sie ein Citrix ADC oder VPX von einer früheren Version aktualisieren, müssen Sie zuerst das Feature Citrix Web App Firewall aktivieren, bevor Sie es konfigurieren.

> **Hinweis:**
>
> Wenn Sie ein Citrix ADC oder VPX von einer früheren Version aktualisieren, müssen Sie möglicherweise die Lizenzen auf Ihrem Gerät aktualisieren, bevor Sie die Citrix Web App Firewall aktivieren. Wenden Sie sich an Ihren Citrix Vertreter oder Händler, um die richtige Lizenz zu erhalten.

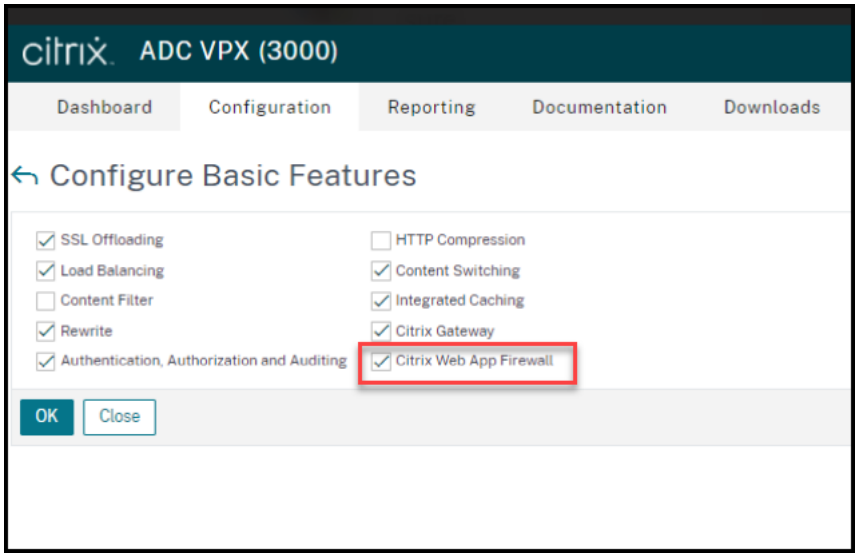
Aktivieren der Citrix Web App Firewall über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
enable ns feature AppFW
```

Aktivieren der Web App Firewall mit der GUI

1. Navigieren Sie zu **System** > **Einstellungen**.
2. Klicken Sie im Detailbereich auf **Erweiterte Funktionen konfigurieren**.
3. Wählen **Sie auf der Seite Erweiterte Funktionen konfigurieren** die Option **Citrix Web App Firewall**aus.
4. Klicken Sie auf **OK**.



Der Web App Firewall Assistent

October 8, 2021

Im Gegensatz zu den meisten Assistenten dient der Citrix Web App Firewall Wizard nicht nur dazu, den anfänglichen Konfigurationsprozess zu vereinfachen, sondern auch zuvor erstellte Konfigurationen zu ändern und Ihre Web App Firewall zu verwalten. Ein typischer Benutzer führt den Assistenten mehrmals aus und überspringt jedes Mal einige der Bildschirme.

Der Web App Firewall Assistent erstellt automatisch Profile, Richtlinien und Signaturen.

Öffnen des Assistenten

Um den Web App Firewall Assistenten auszuführen, öffnen Sie die GUI und gehen Sie folgendermaßen vor:

1. Navigieren Sie zu **Sicherheit** > **Application Firewall**.
2. Klicken Sie im Detailbereich unter **Erste Schritte** auf **Anwendungs-Firewall-Assistent**. Der Assistent wird geöffnet.

Weitere Informationen zur GUI finden Sie unter "Die Web App Firewall-Konfigurationsschnittstellen. "

Die Bildschirme des Assistenten

Der Web App Firewall Assistent zeigt die folgenden Bildschirme auf einer tabellarischen Seite an:

1. Name angeben: Geben Sie auf diesem Bildschirm beim Erstellen einer neuen Sicherheitskonfiguration einen aussagekräftigen Namen und den entsprechenden Typ (HTML, XML oder WEB 2.0) für

Ihr Profil an. Die Standardrichtlinie und die Signaturen werden automatisch unter Verwendung des gleichen Namens generiert.

Profilname

Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstreichungssymbol beginnen und kann aus 1 bis 31 Buchstaben, Zahlen und Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), at (@), Gleich (=), Doppelpunkt (:) und Unterstrich (_) bestehen. Wählen Sie einen Namen, der es anderen leicht macht, zu wissen, welche Inhalte Ihre neue Sicherheitskonfiguration schützt.

> **Hinweis:**
>
> Da der Assistent diesen Namen sowohl für die Richtlinie als auch für das Profil verwendet, ist er auf 31 Zeichen beschränkt. Manuell erstellte Richtlinien können bis zu 127 Zeichen lang sein.

Wenn Sie eine vorhandene Konfiguration ändern, wählen Sie Vorhandene Konfiguration ändern aus, und wählen Sie dann in der Dropdownliste Name den Namen der vorhandenen Konfiguration aus, die Sie ändern möchten.

> **Hinweis:**
>
> Nur Richtlinien, die an globale oder an einen Bindepunkt gebunden sind, werden in dieser Liste angezeigt. Sie können eine nicht gebundene Richtlinie nicht mithilfe des Assistenten für die Anwendungsfirewall ändern. Sie müssen es entweder manuell an Global oder an einen Bindepunkt binden oder manuell ändern. (Zur manuellen Änderung in der GUI) **Application Firewall** > **Richtlinien** > **Firewall** Bereich wählen Sie die Richtlinie aus und klicken Sie auf **Öffnen**.

Profiltyp

Auf diesem Bildschirm wählen Sie auch einen Profiltyp aus. Der Profiltyp bestimmt die Typen des erweiterten Schutzes (Sicherheitsprüfungen), die konfiguriert werden können. Da bestimmte Arten von Inhalten nicht anfällig für bestimmte Arten von Sicherheitsbedrohungen sind, spart die Einschränkung der Liste der verfügbaren Prüfungen während der Konfiguration Zeit. Die Typen von Web App Firewall Profilen sind:

- Webanwendung (HTML). Jede HTML-basierte Website, die keine XML- oder Web 2.0-Technologien verwendet.
- XML-Anwendung (XML, SOAP). Jeder XML-basierte Webdienst.
- Web 2.0-Anwendung (HTML, XML, REST). Jede Web 2.0-Website, die HTML- und XML-basierte Inhalte kombiniert, z. B. eine Atom-basierte Website, ein Blog, ein RSS-Feed oder ein Wiki.

Hinweis: Wenn Sie sich nicht sicher sind, welche Art von Inhalt auf Ihrer Website verwendet wird, können Sie Web 2.0-Anwendung wählen, um sicherzustellen, dass Sie alle Arten von Webanwendungsinhalten schützen.

2. Regel angeben: In diesem Fenster geben Sie die Richtlinienregel (Ausdruck) an, die den Datenverkehr definiert, den die aktuelle Konfiguration untersucht. Wenn Sie eine Erstkonfiguration zum

Schutz Ihrer Websites und Webdienste erstellen, können Sie den Standardwert **true**akzeptieren, der den gesamten Webverkehr auswählt.

Wenn diese Sicherheitskonfiguration nicht den gesamten HTTP-Datenverkehr, der über die Appliance geleitet wird, sondern den spezifischen Datenverkehr untersuchen soll, können Sie eine Richtlinienregel schreiben, die den Datenverkehr angibt, den er untersuchen soll. Regeln werden in Citrix ADC Ausdrücke geschrieben, die eine voll funktionsfähige objektorientierte Programmiersprache ist.

Hinweis: Zusätzlich zur Syntax der Standardausdrücke unterstützt das Citrix ADC-Betriebssystem aus Gründen der Abwärtskompatibilität die Syntax für klassische Ausdrücke von Citrix ADC auf Citrix ADC Classic- und NCore-Appliances und virtuellen Appliances. Klassische Ausdrücke werden von Citrix ADC Cluster-Appliances und virtuellen Appliances nicht unterstützt. Aktuelle Benutzer, die ihre vorhandenen Konfigurationen in den Citrix ADC Cluster migrieren möchten, müssen alle Richtlinien, die klassische Ausdrücke enthalten, in die Standardausdrucksyntax migrieren.

- Eine einfache Beschreibung zur Verwendung der Syntax für Citrix ADC-Ausdrücke zum Erstellen von Web App Firewall-Regeln und eine Liste nützlicher Regeln finden Sie unter Firewall-Richtlinien.
- Eine ausführliche Erklärung zum Erstellen von Richtlinienregeln in der Syntax von Citrix ADC Ausdrücken finden Sie unter Richtlinien und Ausdrücke.

4. Wählen Sie Signaturen aus: Auf diesem Bildschirm wählen Sie die Kategorien von Signaturen aus, die Sie zum Schutz Ihrer Websites und Webdienste verwenden möchten.

Dies ist kein obligatorischer Schritt, und Sie können ihn überspringen, wenn Sie möchten, und gehen Sie zum Bildschirm **Deep Protections angeben**. Wenn der Bildschirm Signaturen auswählen übersprungen wird, werden nur ein Profil und zugehörige Richtlinien erstellt, und die Signaturen werden nicht erstellt.

Sie können die Option **Neue Signatur erstellen** oder **Vorhandene Signatur auswählen** auswählen.

Wenn Sie eine neue Sicherheitskonfiguration erstellen, werden die ausgewählten Signaturkategorien aktiviert und standardmäßig in einem neuen Signaturobjekt aufgezeichnet. Dem neuen Signaturobjekt wird der gleiche Name zugewiesen, den Sie auf dem Bildschirm Name angeben eingegeben haben wie der Name der Sicherheitskonfiguration.

Wenn Sie zuvor Signaturobjekte konfiguriert haben und eines davon als Signaturobjekt verwenden möchten, das der zu erstellenden Sicherheitskonfiguration zugeordnet ist, klicken Sie auf **Vorhandene Signatur auswählen**, und wählen Sie ein Signaturobjekt aus der Liste Signaturen aus.

Wenn Sie eine vorhandene Sicherheitskonfiguration ändern, können Sie auf Vorhandene Signatur auswählen klicken und der Sicherheitskonfiguration ein anderes Signaturobjekt zuweisen.

Wenn Sie auf Neue Signatur erstellen klicken, können Sie den Bearbeitungsmodus als **Einfach** oder **Erweitert** wählen.

1. **Signaturschutz angeben (Einfacher Modus)**

Der einfache Modus ermöglicht eine einfache Konfiguration der Signatur mit einer voreingestellten Liste von Schutzdefinitionen für gängige Anwendungen wie IIS (Internet Information Server), PHP und ActiveX. Die Standardkategorien im einfachen Modus sind:

- CGI. Schutz vor Angriffen auf Websites, die CGI-Skripts in jeder Sprache verwenden, einschließlich PERL-Skripts, Unix-Shell-Skripts und Python-Skripts.
- Cold Fusion. Schutz vor Angriffen auf Websites, die die Adobe Systems® ColdFusion® Web-Entwicklungsplattform verwenden.
- FrontPage. Schutz vor Angriffen auf Websites, die die Microsoft® FrontPage® Web-Entwicklungsplattform nutzen.
- PHP. Schutz vor Angriffen auf Websites, die die Open-Source-Webentwicklungs-Scriptsprache von PHP verwenden.
- Client side. Schutz vor Angriffen auf clientseitige Tools, die für den Zugriff auf Ihre geschützten Websites wie Microsoft Internet Explorer, Mozilla Firefox, den Opera-Browser und den Adobe Acrobat Reader verwendet werden.
- Microsoft IIS. Schutz vor Angriffen auf Websites, auf denen der Microsoft Internet Information Server (IIS) betrieben wird
- Sonstiges. Schutz vor Angriffen auf andere serverseitige Tools wie Webserver und Datenbankserver.

Auf diesem Bildschirm wählen Sie die Aktionen aus, die den Signaturkategorien zugeordnet sind, die Sie auf dem Bildschirm Signaturen auswählen ausgewählt haben. Die Aktionen, die Sie konfigurieren können, sind:

- Blockieren
- Protokollierung
- Statistiken

Standardmäßig sind die Aktionen Protokoll und Statistik aktiviert, aber nicht die Aktion Blockieren. Klicken Sie zum Konfigurieren von Aktionen auf **Einstellungen**. Sie können die Aktionseinstellungen aller ausgewählten Kategorien mithilfe der Dropdownliste **Aktion** ändern.

1. **Signaturschutz angeben (erweiterter Modus)**

Der erweiterte Modus ermöglicht eine genauere Kontrolle über die Signaturdefinitionen und bietet deutlich mehr Informationen. Verwenden Sie den erweiterten Modus, wenn Sie vollständige Kontrolle über die Signaturdefinition wünschen.

Der Inhalt dieses Bildschirms entspricht dem Inhalt des Dialogfelds “Signatures-Objekt ändern”, wie unter Konfigurieren oder Ändern eines Signatures-Objektsbeschrieben. In diesem Bildschirm können Sie Aktionen konfigurieren, indem Sie entweder auf die Dropdownliste **Aktionen** oder auf das Aktionsmenü klicken, das als Kreis mit drei Punkten angezeigt wird.

7. Geben Sie Deep Protections an: Auf diesem Bildschirm wählen Sie die erweiterten Schutzmaßnahmen (auch Sicherheitsüberprüfungen oder einfach als Prüfungen bezeichnet), die Sie zum Schutz Ihrer Websites und Webdienste verwenden möchten. Welche Prüfungen verfügbar sind, hängt vom Profiltyp ab, den Sie im Fenster Name angeben ausgewählt haben. Alle Prüfungen sind für Web 2.0-Anwendungsprofile verfügbar.

Weitere Informationen finden Sie unter Überblick über Sicherheitsprüfungenund unter Erweiterte Formularschutzprüfungen.

Sie konfigurieren die Aktionen für den erweiterten Schutz, den Sie aktiviert haben.Die Aktionen, die Sie konfigurieren können, sind:

- Block: Blockiert Verbindungen, die mit der Signatur übereinstimmen. Diese Funktion ist standardmäßig deaktiviert.
- Protokoll: Protokolliert Verbindungen, die mit der Signatur übereinstimmen, für eine spätere Analyse. Standardmäßig aktiviert.
- Statistiken: verwaltet Statistiken für jede Signatur, die zeigen, wie viele Verbindungen sie übereinstimmten, und geben bestimmte andere Informationen über die Arten von Verbindungen, die blockiert wurden. Diese Funktion ist standardmäßig deaktiviert.
- Lernen. Beobachten Sie den Datenverkehr zu dieser Website oder Webdienst, und verwenden Sie Verbindungen, die wiederholt gegen diese Prüfung verstoßen, um empfohlene Ausnahmen für die Prüfung oder neue Regeln für die Prüfung zu generieren. Nur für einige Schecks verfügbar. Weitere Informationen zur Lernfunktion finden Sie unter Konfigurieren und Verwenden der Lernfunktionund wie Lernen funktioniert und wie Ausnahmen (Entspannungen) konfiguriert oder erlernte Regeln für eine Überprüfung bereitstellen, finden Sie unter Manuelle Konfiguration mit der GUI.

Um Aktionen zu konfigurieren, aktivieren Sie den Schutz, indem Sie auf das Kontrollkästchen klicken, und klicken Sie dann auf **Aktionseinstellungen**, um die erforderlichen Aktionen auszuwählen. Wählen Sie ggf. andere Parameter aus, und klicken Sie dann auf **OK**, um das Fenster Aktionseinstellungen zu schließen.

Um alle Protokolle für eine bestimmte Prüfung anzuzeigen, wählen Sie diese Prüfung aus, und klicken Sie dann auf **Protokolle**, um den Syslog Viewer anzuzeigen, wie in Web App Firewall Logsbeschrieben. Wenn eine Sicherheitsüberprüfung den legitimen Zugriff auf Ihre geschützte Website oder Ihren geschützten Webdienst blockiert, können Sie eine Entspannung für diese Sicherheitsprüfung erstellen und implementieren, indem Sie ein Protokoll auswählen, das die unerwünschte Blockierung anzeigt, und dann auf **Bereitstellen**klicken.

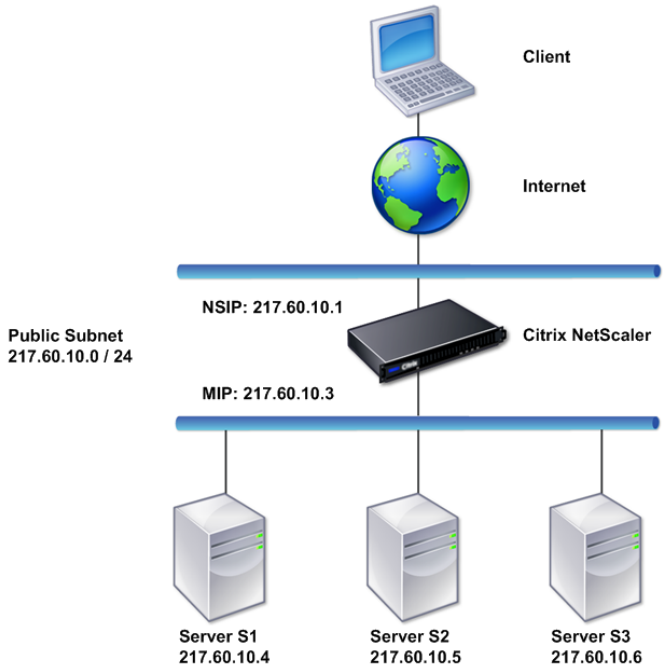
Nachdem Sie die Aktionseinstellungen festgelegt haben, klicken Sie auf **Fertig stellen**, um den Assistenten abzuschließen.

Im Folgenden finden Sie vier Verfahren, die zeigen, wie bestimmte Konfigurationstypen mithilfe des Web App Firewall Assistenten ausgeführt werden.

Erstellen einer neuen Konfiguration

Gehen Sie folgendermaßen vor, um mithilfe des Applicaiton Firewall-Assistenten eine neue Firewall-Konfiguration und Signaturobjekte zu erstellen.

1. Navigieren Sie zu **Sicherheit** > **Application Firewall**.
2. Klicken Sie im Detailbereich unter **Erste Schritte**auf **Anwendungsfirewall. Der Assistent wird geöffnet.



3. Wählen **Sie im Bildschirm Namen angeben** die Option Neue Konfiguration **erstellen aus.
4. Geben Sie im Feld **Name** einen Namen ein, und klicken Sie dann auf **Weiter**.
5. Klicken **Sie im Fenster Regel angeben** erneut auf **Weiter** .
6. Wählen Sie im Bildschirm **Signaturen auswählen** die Option **Neue Signatur erstellen** und **Einfach** als Bearbeitungsmodus aus, und klicken Sie dann auf **Weiter**.
7. Konfigurieren Sie im Bildschirm **Signaturschutz angeben** die erforderlichen Einstellungen. Weitere Informationen darüber, welche Signaturen zum Blockieren zu berücksichtigen sind und wie Sie feststellen können, wann Sie das Blockieren für eine Signatur sicher aktivieren können, finden Sie unter Signaturen.
8. Konfigurieren Sie im Bildschirm **Deep Protections angeben** die erforderlichen Aktionen und Parameter in den **Aktionseinstellungen**.

9. Wenn Sie den Vorgang abgeschlossen haben, klicken Sie auf **Fertig stellen**, um den Assistenten für die Anwendungsfirewall zu schließen.

Ändern einer vorhandenen Konfiguration

Gehen Sie folgendermaßen vor, um eine vorhandene Konfiguration und vorhandene Signaturkategorien zu ändern.

1. Navigieren Sie zu **Sicherheit** > **Application Firewall**.
2. Klicken Sie im Detailbereich unter **Erste Schritte** auf **Anwendungs-Firewall-Assistent**. Der Assistent wird geöffnet.
3. Wählen Sie im Fenster **Name angeben** die Option Vorhandene Konfiguration ändern aus, und wählen Sie in der Dropdownliste **Name** die Sicherheitskonfiguration aus, die Sie während der neuen Konfiguration erstellt haben, und klicken Sie dann auf **Weiter**.
4. Klicken Sie im Fenster **Regel angeben** auf "Weiter", um den Standardwert "true" beizubehalten. Wenn Sie die Regel ändern möchten, führen Sie die unter Konfigurieren eines benutzerdefinierten Richtlinienausdrucks beschriebenen Schritte aus.
5. Klicken Sie im Bildschirm **Signaturen auswählen** auf **Vorhandene Signatur auswählen**. Wählen Sie in der Dropdownliste **Vorhandene Unterschrift** die entsprechende Option aus, und klicken Sie dann auf **Weiter**. Der erweiterte Signaturschutz wird angezeigt.
   Hinweis: Wenn Sie eine vorhandene Signatur auswählen, wird der Standard-Bearbeitungsmodus für die geschützte Signatur erweitert.
6. Konfigurieren Sie im Bildschirm Signaturschutz angeben die erforderlichen Einstellungen, und klicken Sie auf **Weiter**. Weitere Informationen darüber, welche Signaturen zum Blockieren zu berücksichtigen sind und wie Sie feststellen können, wann Sie das Blockieren für eine Signatur sicher aktivieren können, finden Sie unter Signaturen.
7. Konfigurieren Sie im Fenster **Deep Protections angeben** die Einstellungen, und klicken Sie auf **Weiter**.
8. Klicken Sie nach dem Abschluss auf **Fertig stellen**, um den **Web App Firewall Assistenten** zu schließen.

Erstellen einer neuen Konfiguration ohne Signaturen

Gehen Sie folgendermaßen vor, um den Anwendungs-Firewall-Assistenten zu verwenden, um den Bildschirm Signaturen auswählen zu überspringen und eine neue Konfiguration mit nur dem Profil und den zugehörigen Richtlinien ohne Signaturen zu erstellen.

1. Navigieren Sie zu **Sicherheit** > **Application Firewall**.
2. Klicken Sie im Detailbereich unter **Erste Schritte** auf **Anwendungs-Firewall-Assistent**. Der Assistent wird geöffnet.
3. Wählen **Sie im Bildschirm Name angeben** die Option **Neue Konfiguration erstellen**aus.

4. Geben Sie im Feld **Name** einen Namen ein, und klicken Sie dann auf **Weiter**.
5. Klicken **Sie im Bildschirm "Regel angeben** " erneut auf **Nex**t.
6. Klicken **Sie im Bildschirm "Signaturen auswählen** " auf " **Überspringen".**
7. Konfigurieren Sie im Bildschirm **Deep Protections angeben** die erforderlichen Aktionen und Parameter in den **Aktionseinstellungen**.
8. Klicken Sie nach Abschluss auf **Fertig stellen**, um den Assistenten für die Anwendungsfirewall zu schließen.

Konfigurieren eines benutzerdefinierten Richtlinienausdrucks

Gehen Sie folgendermaßen vor, um mithilfe des Anwendungs-Firewall-Assistenten eine spezielle Sicherheitskonfiguration zu erstellen, um nur bestimmte Inhalte zu schützen. In diesem Fall erstellen Sie eine neue Sicherheitskonfiguration, anstatt die Erstkonfiguration zu ändern. Für diese Sicherheitskonfiguration ist eine benutzerdefinierte Regel erforderlich, damit die Richtlinie die Konfiguration nur auf den ausgewählten Webdatenverkehr anwendet.

1. Navigieren Sie zu **Sicherheit** > **Application Firewall**.
2. Klicken Sie im Detailbereich unter **Erste Schritte** auf **Anwendungs-Firewall-Assistent**.
3. Geben Sie im Fenster Name angeben einen Namen für die neue Sicherheitskonfiguration in das Textfeld Name ein, wählen Sie den Typ der Sicherheitskonfiguration aus der Dropdownliste Typ aus, und klicken Sie dann auf **Weiter**.
4. **Geben Sie im Fenster Regel angeben** eine Regel ein, die nur dem Inhalt entspricht, den diese Webanwendung schützen soll. Verwenden Sie die Dropdownliste **Häufig verwendete Ausdrücke** und den **Ausdrucksеditor**, um einen benutzerdefinierten Ausdruck zu erstellen. Wenn Sie den Vorgang abgeschlossen haben, klicken Sie auf **Weiter**.
5. **Wählen Sie im Bildschirm Signaturen** auswählen den Bearbeitungsmodus aus, und klicken Sie dann auf **Weiter** .
6. Konfigurieren Sie im Bildschirm **Signaturschutz angeben** die erforderlichen Einstellungen.
7. Konfigurieren Sie im Bildschirm **Deep Protections angeben** die erforderlichen Aktionen und Parameter in den **Aktionseinstellungen**.
8. Wenn Sie fertig sind, klicken Sie auf **Beenden**, um den **Assistenten für Anwendungsfirewall**zu schließen.

Manuelle Konfiguration

October 5, 2021

Wenn Sie ein Profil an einen anderen Bindepunkt als Global binden möchten, müssen Sie die Bindung manuell konfigurieren. Bestimmte Sicherheitsprüfungen erfordern außerdem, dass Sie entweder die

erforderlichen Ausnahmen manuell eingeben oder die Lernfunktion aktivieren, um die Ausnahmen zu generieren, die Ihre Websites und Webdienste benötigen. Einige dieser Aufgaben können nicht mithilfe des Web App Firewall Assistenten ausgeführt werden.

Wenn Sie mit der Funktionsweise der Web App Firewall vertraut sind und eine manuelle Konfiguration bevorzugen, können Sie ein Signaturobjekt und ein Profil manuell konfigurieren, das Signaturobjekt dem Profil zuordnen, eine Richtlinie mit einer Regel erstellen, die dem zu konfigurierenden Webdatenverkehr entspricht, und die Richtlinie zuordnen. mit dem Profil. Anschließend binden Sie die Richtlinie an Global oder an einen Bindepunkt, um sie in Kraft zu setzen, und Sie haben eine vollständige Sicherheitskonfiguration erstellt.

Für die manuelle Konfiguration können Sie die GUI (eine grafische Oberfläche) oder die Befehlszeile verwenden. Citrix empfiehlt die Verwendung der GUI. Nicht alle Konfigurationsaufgaben können über die Befehlszeile ausgeführt werden. Bestimmte Aufgaben, wie das Aktivieren von Signaturen und das Überprüfen von erlernten Daten, müssen in der GUI ausgeführt werden. Die meisten anderen Aufgaben sind in der GUI einfacher durchzuführen.

Konfiguration replizieren

Wenn Sie die Web App Firewall manuell mit der GUI (GUI) oder der Befehlszeilenschnittstelle (CLI) konfigurieren, wird die Konfiguration in der Datei /nsconfig/ns.conf gespeichert. Sie können die Befehle in dieser Datei verwenden, um die Konfiguration auf einer anderen Appliance zu replizieren. Sie können die Befehle einzeln ausschneiden und in die CLI einfügen, oder Sie können mehrere Befehle in einer Textdatei im Ordner /var/tmp speichern und als Batchdatei ausführen. Es folgt ein Beispiel für die Ausführung einer Batchdatei mit Befehlen, die aus der Datei /nsconfig/ns.conf einer anderen Appliance kopiert wurden:

```
> batch -f /var/tmp/appfw_add.txt
```

> **Warnung:**
>
> Importbefehle werden nicht in der Datei ns.conf gespeichert. Bevor Sie Befehle aus der Datei ns.conf ausführen, um die Konfiguration auf einer anderen Appliance zu replizieren, müssen Sie alle in der Konfiguration verwendeten Objekte (z. B. Signaturen, Fehlerseite, WSDL und Schema) in die Appliance importieren, auf der Sie die Konfiguration replizieren. Der Befehl add zum Hinzufügen eines in einer ns.conf-Datei gespeicherten Web App Firewall-Profils enthält möglicherweise den Namen eines importierten Objekts, aber ein solcher Befehl schlägt möglicherweise fehl, wenn er auf einer anderen Appliance ausgeführt wird, wenn das referenzierte Objekt auf dieser Appliance nicht vorhanden ist.

Weitere Informationen zu Import- oder Exportdetails für die Replikation der Konfiguration finden Sie unter Signaturexportund Themen über allgemeine Importexporte .

Manuelle Konfiguration mit der Citrix ADC GUI

December 7, 2021

Wenn Sie die Web App Firewall Funktion manuell konfigurieren müssen, empfiehlt Citrix, die Citrix ADC GUI-Prozedur zu verwenden.

So erstellen und konfigurieren Sie Signature-Objekt

Bevor Sie die Signaturen konfigurieren können, müssen Sie ein Signaturenobjektvorlage aus der entsprechenden Standardsignaturenobjektvorlage erstellen. Weisen Sie der Kopie einen neuen Namen zu, und konfigurieren Sie die Kopie. Sie können die Standardsignaturobjekte nicht direkt konfigurieren oder ändern. Das folgende Verfahren enthält grundlegende Anweisungen zum Konfigurieren eines Signaturobjekts. Ausführlichere Anweisungen finden Sie unter Manuelles Konfigurieren der Signature-Funktion.

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Signaturen**.
2. Wählen Sie im Detailbereich das Signaturobjekt aus, das Sie als Vorlage verwenden möchten, und klicken Sie dann auf **Hinzufügen**.

   Ihre Auswahlmöglichkeiten:

   - **Standardsignaturen.** Enthält die Signaturregeln, die SQL-Injectionsregeln und die siteübergreifenden Skriptregeln.
   - **XPath-Injection.** Enthält alle Elemente in den Standardsignaturen und enthält zusätzlich die XPath-Injectionsregeln.
3. Geben Sie im Dialogfeld **Signaturenobjekt hinzufügen** einen Namen für das neue Signaturenobjekt ein, klicken Sie auf OK, und klicken Sie dann auf **Schließen**. Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrich beginnen und kann aus einem bis 31 Buchstaben, Zahlen und Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), at (@), Gleich (=) und Unterstrich (_) bestehen.
4. Wählen Sie das von Ihnen erstellte Signaturobjekt aus, und klicken Sie dann auf **Öffnen**.
5. Legen Sie im Dialogfeld **Signaturobjekt ändern** die Optionen **Anzeigefilterkriterien** links fest, um die Filterelemente anzuzeigen, die Sie konfigurieren möchten.

   Wenn Sie diese Optionen ändern, werden die von Ihnen angegebenen Ergebnisse im Fenster Gefilterte Ergebnisse rechts angezeigt. Weitere Informationen zu den Kategorien von Signaturen finden Sie unter Signaturen.
6. Konfigurieren Sie im Bereich **Gefilterte Ergebnisse** die Einstellungen für eine Signatur, indem Sie die entsprechenden Kontrollkästchen aktivieren und deaktivieren.

7. Wenn Sie fertig sind, klicken Sie auf **Schließen**.

So erstellen Sie ein Web App Firewall Profil mit der GUI

Wenn Sie ein Web App Firewall Profil erstellen, müssen Sie nur einige Konfigurationsdetails angeben.

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profile**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben **Sie im Dialogfeld Web App Firewall Profil erstellen** einen Namen für Ihr Profil ein.

   Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstreichungssymbol beginnen und kann aus einem bis 31 Buchstaben, Zahlen und dem Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), at (@), Gleich (=), Doppelpunkt (:) und Unterstrich (_) bestehen.
4. Wählen Sie den Profiltyp aus der Dropdownliste aus.
5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So konfigurieren Sie ein Web App Firewall Profil mit der GUI

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich das Profil aus, das Sie konfigurieren möchten, und klicken Sie dann auf **Bearbeiten**.
3. Konfigurieren Sie im Dialogfeld **Web App Firewallprofil konfigurieren** auf der Registerkarte **Sicherheitsprüfungen** die Sicherheitsprüfungen.

   - Um eine Aktion für eine Prüfung zu aktivieren oder zu deaktivieren, aktivieren oder deaktivieren Sie in der Liste das Kontrollkästchen für diese Aktion.
   - Um andere Parameter für diese Prüfungen zu konfigurieren, klicken Sie in der Liste auf den blauen Chevron ganz rechts neben der Prüfung. Konfigurieren Sie im angezeigten Dialogfeld die Parameter. Diese variieren von Scheck zu Scheck.

     Sie können auch eine Prüfung auswählen und unten im Dialogfeld auf Öffnen klicken, um das Dialogfeld Entspannung konfigurieren oder das Dialogfeld Regel konfigurieren für diese Prüfung anzuzeigen. Diese Dialogfelder variieren auch von Häkchen zu Häkchen. Die meisten von ihnen umfassen eine Registerkarte Prüfungen und eine Registerkarte Allgemein . Wenn die Prüfung Entspannungen oder benutzerdefinierte Regeln unterstützt, enthält die Registerkarte Überprüfungen eine Schaltfläche Hinzufügen, die ein weiteres Dialogfeld öffnet, in dem Sie eine Entspannung oder Regel für die Prüfung angeben können. (Eine Entspannung ist eine Regel, um den angegebenen Datenverkehr von der Prüfung auszuschließen.) Wenn die Entspannungen bereits konfiguriert wurden, können Sie eine auswählen und auf Öffnen klicken, um sie zu ändern.

- Um gelernte Ausnahmen oder Regeln für eine Prüfung zu überprüfen, wählen Sie die Prüfung aus, und klicken Sie dann auf Gelernte Verletzungen. Wählen Sie im Dialogfeld Gelernte Regeln verwalten nacheinander jede erlernte Ausnahme oder Regel aus.
  - Klicken Sie auf **Bearbeiten und Bereitstellen**, um die Ausnahme oder Regel zu bearbeiten und dann zur Liste hinzuzufügen.
  - Klicken Sie auf **Bereitstellen**, um die Ausnahme oder Regel ohne Änderung zu akzeptieren.
  - Klicken Sie auf **Überspringen**, um die Ausnahme oder Regel aus der Liste zu entfernen.
- Klicken Sie auf **Aktualisieren**, um die Liste der zu überprüfenden Ausnahmen oder Regeln zu aktualisieren.
- Klicken Sie auf **Visualizer**, um den **Learning Visualizer** zu öffnen und ihn zum Überprüfen der erlernten Regeln zu verwenden.
- Um die Protokolleinträge für Verbindungen zu überprüfen, die einer Prüfung entsprechen, wählen Sie die Prüfung aus, und klicken Sie dann auf **Protokolle**. Mithilfe dieser Informationen können Sie ermitteln, welche Prüfungen mit Angriffen übereinstimmen, damit Sie die Blockierung für diese Prüfungen aktivieren können. Sie können diese Informationen auch verwenden, um zu bestimmen, welche Prüfungen mit dem legitimen Datenverkehr übereinstimmen, sodass Sie eine entsprechende Ausnahme konfigurieren können, um diese legitimen Verbindungen zuzulassen. Weitere Informationen zu den Protokollen finden Sie unter Protokolle, Statistiken und Berichte.
- Um eine Überprüfung vollständig zu deaktivieren, deaktivieren Sie in der Liste alle Kontrollkästchen rechts neben dieser Prüfung.

4. Konfigurieren Sie auf der Registerkarte **Einstellungen** die Profileinstellungen.
   - Um das Profil mit dem Satz von Signaturen zu verknüpfen, die Sie zuvor erstellt und konfiguriert haben, wählen Sie unter **Allgemeine Einstellungen**diesen Satz von Signaturen in der Dropdownliste Signaturen aus.

     > **Hinweis:**
     >
     > Möglicherweise müssen Sie die Bildlaufleiste auf der rechten Seite des Dialogfelds verwenden, um nach unten zu scrollen, um den Abschnitt Allgemeine Einstellungen anzuzeigen.

   - Um ein HTML- oder XML-Fehlerobjekt zu konfigurieren, wählen Sie das Objekt aus der entsprechenden Dropdownliste aus.

> **Hinweis:**
>
> Sie müssen zuerst das Fehlerobjekt hochladen, das Sie im Importbereich verwenden möchten.

- Um den Standard-XML-Inhaltstyp zu konfigurieren, geben Sie die Zeichenfolge des Inhaltstyps direkt in die Textfelder Standardanforderung und Standardantwort ein, oder klicken Sie auf Zulässige Inhaltstypen verwalten, um die Liste der zulässigen Inhaltstypen zu verwalten.

5. Wenn Sie die Lernfunktion verwenden möchten, klicken Sie auf Lernen, und konfigurieren Sie die Lerneinstellungen für das Profil. Weitere Informationen finden Sie unter Konfigurieren und Lernen Feature.
6. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Bereich Profile zurückzukehren.

Konfigurieren einer Web App Firewall Regel oder Relaxation

Sie konfigurieren in diesem Dialogfeld zwei verschiedene Informationstypen, je nachdem, welche Sicherheitsprüfung Sie konfigurieren. In den meisten Fällen konfigurieren Sie eine Ausnahme (oder Entspannung) für die Sicherheitsprüfung. Wenn Sie die Überprüfung URL verweigern oder die Feldformat-Prüfung konfigurieren, konfigurieren Sie einen Zusatz (oder eine Regel). Der Prozess für beide ist der gleiche.

So konfigurieren Sie eine Relaxationsregel über die Citrix ADC GUI

1. Navigieren Sie zu **Sicherheit** > **Citrix Web App Firewall** > **Profile**.
2. Wählen Sie im Bereich **Profile** das Profil aus, das Sie konfigurieren möchten, und klicken Sie dann auf **Bearbeiten** .
3. Klicken Sie auf der Seite **Web App Firewall Profil konfigurieren** im Abschnitt **Erweiterte Einstellungen** auf **Relaxationsregel**. Der Abschnitt **Relaxationsregel** enthält die vollständige Liste der Relaxationsregeln für Web App Firewall.
4. Klicken Sie auf eine Sicherheitsregel, die Sie konfigurieren möchten, und klicken Sie dann auf **Bearbeiten**.
5. Die Seite URL-Relaxationsregeln enthält eine Liste von Aktionen, die Sie für diese Regel konfigurieren können, sowie eine Liste vorhandener Relaxationen oder Regeln. Die Liste ist möglicherweise leer, wenn Sie entweder keine Entspannungen manuell hinzugefügt oder von der Lernmaschine empfohlenen Entspannungen genehmigt haben. Unter der Liste befindet sich eine Reihe von Schaltflächen, mit denen Sie die Relaxationen in der Liste hinzufügen, ändern, löschen, aktivieren oder deaktivieren können.

6. Führen Sie einen der folgenden Schritte aus, um eine Entspannung oder eine Regel hinzuzufügen oder zu ändern:

   - Um eine neue Entspannung hinzuzufügen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Entspannung zu ändern, wählen Sie die zu ändernde Entspannung aus, und klicken Sie dann auf **Öffnen**.

   Die Seite **URL-Relaxationsregel starten** wird angezeigt. Mit Ausnahme des Titels sind diese Dialogfelder identisch.

7. Füllen Sie das Dialogfenster wie unten beschrieben aus. Die Dialogfelder für jede Prüfung sind unterschiedlich. Die folgende Liste enthält alle Elemente, die in einem beliebigen Dialogfeld angezeigt werden können.

   - **Kontrollkästchen Aktiviert**— Aktivieren Sie diese Option, um diese Entspannung oder Regel aktiv zu verwenden. Deaktivieren Sie diese Option, um sie zu deaktivieren.
   - **Anlageninhaltstyp**— Das Content-Type-Attribut einer XML-Anlage. Geben Sie im Textbereich einen regulären Ausdruck ein, der dem Content-Type-Attribut der zuzulassenden XML-Anlagen entspricht.
   - **Aktions-URL**: Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der die URL definiert, an die in das Webformular eingegebene Daten übermittelt werden.
   - **Cookie**— Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der das Cookie definiert.
   - **Feldname**— Ein Webformularfeldnamenelement kann mit der Bezeichnung Feldname, Formularfeld oder einem anderen ähnlichen Namen versehen sein. Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der den Namen des Formularfelds definiert.
   - **Von Origin-URL**— Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der die URL definiert, die das Webformular hostet.
   - **Von Aktions-URL**— Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der die URL definiert, an die in das Webformular eingegebene Daten übermittelt werden.
   - **Name**— Ein XML-Element- oder Attributname. Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der den Namen des Elements oder Attributs definiert.
   - **URL**— Ein URL-Element kann mit der Bezeichnung Aktions-URL, URL verweigern, Formularaktions-URL, Formularorigin-URL, Start-URL oder einfach URL bezeichnet werden. Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der die URL definiert.

- **Format**— Der Formatabschnitt enthält mehrere Einstellungen, die Listenfelder und Textfelder enthalten. Es kann eine der folgenden Optionen angezeigt werden:
  - **Typ**— Wählen Sie einen Feldtyp in der Dropdownliste Typ aus. Um eine neue Feldtypdefinition hinzuzufügen, klicken Sie auf Verwalten—
  - **Minimale Länge**— Geben Sie eine positive Ganzzahl ein, die die Mindestlänge in Zeichen darstellt, wenn Sie Benutzer zum Ausfüllen dieses Felds zwingen möchten. Standard: 0 (Erlaubt, dass das Feld leer bleibt.)
  - **Maximale Länge**— Geben Sie eine positive Ganzzahl ein, die die maximale Länge in Zeichen darstellt, um die Länge der Daten in diesem Feld zu beschränken. Standard: 65535
- **Position**— Wählen Sie aus der Dropdownliste das Element der Anforderung aus, auf das Ihre Entspannung angewendet wird. Bei HTML-Sicherheitsprüfungen stehen folgende Optionen zur Auswahl:
  - FormField — Formularfelder in Webformularen.
  - Header — Header anfordern.
  - Cookie — Set-Cookie-Header.

  Bei XML-Sicherheitsprüfungen stehen folgende Optionen zur Auswahl:
  - ELEMENT — XML-Element.
  - ATTRIBUE — XML-Attribut.
- **Maximale Anlagengröße**— Die maximale Größe in Bytes, die für eine XML-Anlage zulässig ist.
- **Kommentare**— Geben Sie im Textbereich einen Kommentar ein. Optional.

Hinweis: Für jedes Element, das einen regulären Ausdruck erfordert, können Sie den regulären Ausdruck eingeben, das Menü “Regex-Tokens” verwenden, um Elemente und Symbole für reguläre Ausdrücke direkt in das Textfeld einzufügen, oder auf “ **Regex-Editor** “ klicken, um den Befehl “ **Regulären Ausdruck hinzufügen** “ zu öffnen. , und verwenden Sie es, um den Ausdruck zu erstellen.

8. Um eine Entspannung oder Regel zu entfernen, wählen Sie sie aus, und klicken Sie dann auf **Löschen**.
9. Um eine Entspannung oder Regel zu aktivieren, wählen Sie sie aus, und klicken Sie dann auf **Aktivieren**.
10. Um eine Entspannung oder Regel zu deaktivieren, wählen Sie sie aus, und klicken Sie dann auf **Deaktivieren**.
11. Um die Einstellungen und Beziehungen aller vorhandenen Relaxationen in einer integrierten interaktiven Grafikdarstellung zu konfigurieren, klicken Sie auf **Visualizer**, und verwenden Sie die Anzeigetools.

> **Hinweis:**
>
> Die Schaltfläche **Visualizer** wird nicht in allen Dialogfeldern für die Überprüfung der Entspannung angezeigt.

12. Um die erlernten Regeln für diese Prüfung zu überprüfen, klicken Sie auf Lernen und führen Sie die Schritte unter So konfigurieren und verwenden Sie die Lernfunktionaus
13. Klicken Sie auf **OK**.

So konfigurieren Sie die Learned Rules über die Citrix ADC GUI

1. Navigieren Sie zu **Sicherheit** > **Citrix Web App Firewall** > **Profile**.
2. Wählen Sie im Bereich **Profile** das Profil aus, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Citrix Web App Firewall Profil** auf **Gelernte Regeln** unter **Erweiterte Einstellungen**. Im Abschnitt **Gelernte Regeln** sehen Sie eine Liste der Sicherheitsprüfungen, die im aktuellen Profil verfügbar sind und die Lernfunktion unterstützen.
4. Um die Lernschwellenwerte zu konfigurieren, wählen Sie eine Sicherheitsüberprüfung aus und klicken Sie auf **Einstellungen**.
5. Auf der Seite **Einstellungen für dynamische Profilerstellung und Lernregeln** können Sie die Einstellungen festlegen. Weitere Informationen finden Sie unter Dynamische Profileinstellungen
   - **Mindestzahlschwelle.** Je nachdem, welche Lerneinstellungen für die Sicherheitsprüfung Sie konfigurieren, bezieht sich der Schwellenwert für die Mindestanzahl an Benutzersitzungen, die eingehalten werden müssen, auf die Mindestanzahl von Anforderungen, die eingehalten werden müssen, oder auf die Mindestanzahl der Beobachtungen eines bestimmten Formularfelds. bevor eine gelernte Entspannung erzeugt wird. Standard: 1
   - **Prozentsatz des Zeitgrenzwerts.** Je nachdem, welche Lerneinstellungen für die Sicherheitsprüfung Sie konfigurieren, bezieht sich der Prozentsatz der Zeiten des Schwellenwerts möglicherweise auf den Prozentsatz der gesamten beobachteten Benutzersitzungen, die die Sicherheitsprüfung verletzt haben, auf den Prozentsatz der Anforderungen oder auf den Prozentsatz, in dem ein Formularfeld mit einem bestimmten Feldtyp übereinstimmte, bevor ein gelernte Entspannung erzeugt wird. Standard: 0
6. Um alle erlernten Daten zu entfernen und die Lernfunktion zurückzusetzen, damit die Beobachtungen von Anfang an erneut beginnen müssen, wählen Sie die Aktion **Alle erlernten Daten entfernen** aus.

> **Hinweis:**
>
> Mit dieser Schaltfläche werden nur erlernte Empfehlungen entfernt, die nicht überprüft und entweder genehmigt oder übersprungen wurden. Es entfernt keine gelernten Entspannungen, die akzeptiert und eingesetzt wurden.

7. Klicken Sie auf **Vertrauenswürdige Lernclients**, und fügen Sie der Liste die IP-Adressen hinzu, die Sie verwenden möchten.
   a) Um der Liste Trusted Learning-Clients eine IP-Adresse oder einen IP-Adressbereich hinzuzufügen, klicken Sie auf **Hinzufügen**.
   b) Klicken Sie auf der Seite **AppFirewall Profil für vertrauenswürdige Clint-Bindung** auf **Hinzufügen**.
   c) Aktivieren Sie das Kontrollkästchen **Aktiviert**, um das Feature zu aktivieren.
   d) Geben Sie im** Feld Trusted Learning Client die IP-Adresse oder einen IP-Adressbereich im CIDR-Format ein.
   e) Geben Sie im Textbereich **Kommentare** einen Kommentar ein, der diese IP-Adresse oder diesen Bereich beschreibt.
   f) Klicken Sie auf **Erstellen** und **Schließen**.
8. Um eine vorhandene IP-Adresse oder einen vorhandenen Bereich zu ändern, klicken Sie auf die IP-Adresse oder den Bereich, und klicken Sie dann auf **Bearbeiten**. Mit Ausnahme des Namens ist das angezeigte Dialogfeld mit dem Dialogfeld Vertrauenswürdige Learning Clients hinzufügen identisch.
9. Um eine IP-Adresse oder einen Bereich zu deaktivieren oder zu aktivieren, sie jedoch in der Liste zu belassen, klicken Sie auf die IP-Adresse oder den Bereich und dann gegebenenfalls auf **Deaktivieren** oder **Aktivieren**.
10. Um eine IP-Adresse oder einen Bereich vollständig zu entfernen, klicken Sie auf die IP-Adresse oder den Bereich, und klicken Sie dann auf **Löschen**.
11. Klicken Sie auf **Schließen**, um zur Seite **Citrix Web App Firewall Profil** zurückzukehren.

So erstellen Sie eine Citrix Web App Firewall Richtlinie über die Citrix ADC GUI

1. Navigieren Sie zu **Sicherheit** > **Citrix Web App-Firewall** > **Richtlinien**.
2. Klicken Sie auf der Seite **Richtlinien** auf **Citrix Web App Firewall Richtlinie**.
3. Klicken Sie auf der Seite Citrix Web App Firewall Richtlinien auf **Hinzufügen**.
4. Legen Sie auf der Seite Citrix Web App Firewall Richtlinie erstellen die folgenden Parameter fest.
   a) Name. Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrichsymbol beginnen und kann aus einem bis 128 Buchstaben, Zahlen und dem Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), at (@), gleich (=), Doppelpunkt (:) und Unterstrich (_) bestehen.

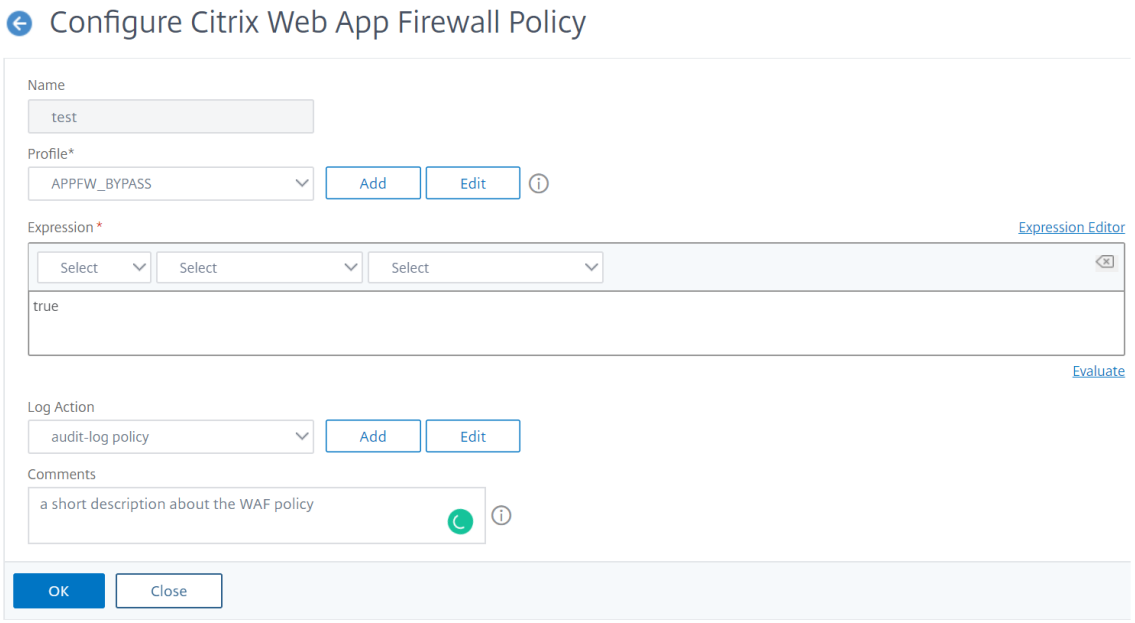
b) Profil. Wählen Sie in der Dropdownliste Profil das Profil aus, das Sie dieser Richtlinie zuordnen möchten. Sie können ein Profil erstellen, das der Richtlinie zugeordnet werden soll, indem Sie auf Neu klicken, und Sie können ein vorhandenes Profil ändern, indem Sie auf **Ändern**klicken.

c) Ausdruck. Erstellen Sie im Textbereich Ausdruck eine Regel für Ihre Richtlinie.

d) Aktion protokollieren. Fügen Sie eine Protokollaktion hinzu, oder Sie können eine vorhandene Protokollaktion ändern.

e) Kommentare. Eine kurze Beschreibung der Richtlinie.

5. Klicken Sie auf **Erstellen** oder **OK**und dann auf **Schließen**.



So erstellen oder konfigurieren Sie eine Web App Firewall Regel (Ausdruck)

Die Richtlinienregel, auch *Ausdruck* genannt, definiert den Webverkehr, den die Web App Firewall mithilfe des Profils filtert, das der Richtlinie zugeordnet ist. Wie andere Citrix ADC Richtlinienregeln (oder *Ausdrücke*) verwenden Web App Firewall Regeln die Syntax von Citrix ADC Ausdrücken. Diese Syntax ist leistungsstark, flexibel und erweiterbar. Es ist zu komplex, um in diesem Satz von Anweisungen vollständig zu beschreiben. Sie können das folgende Verfahren verwenden, um eine einfache Firewall-Richtlinienregel zu erstellen, oder Sie können sie als Überblick über den Richtlinienerstellungsprozess lesen.

1. Wenn Sie dies noch nicht getan haben, navigieren Sie zum entsprechenden Speicherort im Assistenten für Web App Firewall oder in der Citrix ADC GUI, um Ihre Richtlinienregel zu erstellen:

   - Wenn Sie eine Richtlinie im Web App Firewall -Assistenten konfigurieren, klicken Sie im Navigationsbereich auf **Citrix Web App Firewall -Assistent**, dann im Detailbereich auf **Citrix Web App Firewall-Assistent**, und navigieren Sie dann zur Registerkarte **Regel**

angeben .

- Wählen **Sie auf der Seite Regel angeben** das Präfix für Ihren Ausdruck aus der Dropdownliste aus. Ihre Auswahlmöglichkeiten:
- **HTTP.** Das HTTP-Protokoll. Wählen Sie diese Option, wenn Sie einen Aspekt der Anforderung untersuchen möchten, die sich auf das HTTP-Protokoll bezieht.
- **SYS.** Eine oder mehrere geschützte Websites. Wählen Sie diese Option, wenn Sie einen Aspekt der Anforderung untersuchen möchten, der sich auf den Empfänger der Anforderung bezieht.
- **CLIENT.** Der Computer, der die Anforderung gesendet hat. Wählen Sie diese Option, wenn Sie einen Aspekt des Absenders der Anfrage untersuchen möchten.
- **SERVER.** Der Computer, an den die Anforderung gesendet wurde. Wählen Sie diese Option, wenn Sie einen Aspekt des Empfängers der Anfrage untersuchen möchten.

Nachdem Sie ein Präfix ausgewählt haben, zeigt die Web App Firewall ein zweiteiliges Eingabeaufforderungsfenster an, in dem die möglichen nächsten Optionen oben angezeigt werden, und eine kurze Erläuterung darüber, was die ausgewählte Auswahl am unteren Rand bedeutet.

2. Wählen Sie Ihre nächste Amtszeit.

   Wenn Sie HTTP als Präfix gewählt haben, ist REQ die einzige Wahl, die das Request/Response-Paar angibt. (Die Web App Firewall arbeitet für die Anforderung und Antwort als Einheit statt für jede einzelne Einheit.) Wenn Sie ein anderes Präfix gewählt haben, sind Ihre Auswahlmöglichkeiten vielfältiger. Um Hilfe zu einer bestimmten Auswahl zu erhalten, klicken Sie einmal auf diese Auswahl, um Informationen darüber im unteren Eingabeaufforderungsfenster anzuzeigen.

   Wenn Sie sich entschieden haben, welchen Begriff Sie möchten, doppelklicken Sie darauf, um ihn in das Fenster Ausdruck einzufügen.

3. Geben Sie einen Zeitraum nach dem gerade ausgewählten Begriff ein. Sie werden dann aufgefordert, den nächsten Begriff auszuwählen, wie im vorherigen Schritt beschrieben. Wenn ein Begriff erfordert, dass Sie einen Wert eingeben, geben Sie den entsprechenden Wert ein. Wenn Sie beispielsweise HTTP.REQ.HEADER () wählen, geben Sie den Headernamen zwischen den Anführungszeichen ein.

4. Fahren Sie mit der Auswahl von Begriffen aus den Eingabeaufforderungen fort und füllen Sie alle erforderlichen Werte aus, bis der Ausdruck beendet ist.

   Im Folgenden finden Sie einige Beispiele für Ausdrücke für bestimmte Zwecke.

   - **Bestimmter Webhost.** So passen Sie den Datenverkehr von einem bestimmten Webhost an:


```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
```

Ersetzen Sie für shopping.example.com den Namen des Webhosts, dem Sie entsprechen möchten.

- **Bestimmter Webordner oder -verzeichnis.** So ordnen Sie den Datenverkehr aus einem bestimmten Ordner oder Verzeichnis auf einem Webhost zu:

```
HTTP.REQ.URL.STARTSWITH("https//www.example.com/folder")
```

Ersetzen Sie unter www.example.com den Namen des Webhosts. Ersetzen Sie für Ordner den Ordner oder Pfad zu dem Inhalt, den Sie abgleichen möchten. Wenn sich Ihr Warenkorb beispielsweise in einem Ordner namens /solutions/orders befindet, ersetzen Sie diese Zeichenfolge durch Ordner.

- **Bestimmte Art von Inhalt: GIF-Bilder.** So passen Sie Bilder im GIF-Format an:

```
HTTP.REQ.URL.ENDSWITH(".png")
```

Wenn Sie andere Formatbilder abgleichen möchten, ersetzen Sie anstelle von GIF eine andere Zeichenfolge.

- **Spezifischer Inhaltstyp: Skripts.** So passen Sie alle CGI-Skripts an, die sich im CGI-BIN-Verzeichnis befinden:

```
HTTP.REQ.URL.STARTSWITH("https//www.example.com/CGI-BIN")
```

So passen Sie alle JavaScripts mit .js-Erweiterungen an:

```
HTTP.REQ.URL.ENDSWITH(".js")
```

Weitere Informationen zum Erstellen von Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke.

> **Hinweis:**
>
> Wenn Sie die Befehlszeile verwenden, um eine Richtlinie zu konfigurieren, denken Sie daran, doppelte Anführungszeichen in Citrix ADC Ausdrücken zu entkommen. Beispielsweise ist der folgende Ausdruck korrekt, wenn er in der GUI eingegeben wird:

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
```

Wenn Sie jedoch in der Befehlszeile eingegeben werden, müssen Sie dies stattdessen eingeben:

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
```

```
1 ![Policy expression configuration](/en-us/citrix-adc/media/waf-rule.png
    )
```


So fügen Sie eine Firewallregel (Ausdruck) über das Dialogfeld Ausdruck hinzufügen hinzu

Das Dialogfeld **Ausdruck hinzufügen** (auch Ausdruckseditor genannt) hilft Benutzern, die nicht mit der Citrix ADC Ausdruckssprache vertraut sind, eine Richtlinie zu erstellen, die dem zu filternden Datenverkehr entspricht.

1. Wenn Sie dies noch nicht getan haben, navigieren Sie zum entsprechenden Speicherort im Web App Firewall Assistenten oder in der Citrix ADC GUI:
   - Wenn Sie eine Richtlinie im **Web App Firewall-Assistenten** konfigurieren, klicken Sie im Navigationsbereich auf **Web App Firewall**, klicken Sie dann im Detailbereich auf **Web App Firewall-Assistent**, und navigieren Sie dann zum Fenster **Regel angeben** .
   - Wenn Sie eine Richtlinie manuell konfigurieren, erweitern Sie im Navigationsbereich **Web App Firewall**, **Richtlinien** und **Firewall**. Klicken Sie im Detailbereich auf **Hinzufügen**, um eine Richtlinie zu erstellen. Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Öffnen**.
2. Klicken Sie auf dem Bildschirm **Regel angeben** im Dialogfeld **Web App Firewall-Profil erstellen** oder im Dialogfeld **Web App Firewallprofil konfigurieren** auf **Hinzufügen** .
3. Wählen **Sie im Dialogfeld Ausdruck hinzufügen** im Bereich Ausdruck konstruieren im ersten Listenfeld eines der folgenden Präfixe aus:
   - **HTTP.** Das HTTP-Protokoll. Wählen Sie diese Option, wenn Sie einen Aspekt der Anforderung untersuchen möchten, die sich auf das HTTP-Protokoll bezieht. Die Standardauswahl.
   - **SYS.** Eine oder mehrere geschützte Websites. Wählen Sie diese Option, wenn Sie einen Aspekt der Anforderung untersuchen möchten, der sich auf den Empfänger der Anforderung bezieht.
   - **CLIENT.** Der Computer, der die Anforderung gesendet hat. Wählen Sie diese Option, wenn Sie einen Aspekt des Absenders der Anfrage untersuchen möchten.
   - **SERVER.** Der Computer, an den die Anforderung gesendet wurde. Wählen Sie diese Option, wenn Sie einen Aspekt des Empfängers der Anfrage untersuchen möchten.
4. Wählen Sie im zweiten Listenfeld den nächsten Begriff aus. Die verfügbaren Begriffe unterscheiden sich je nach Auswahl, die Sie im vorherigen Schritt getroffen haben, da das Dialogfeld die Liste automatisch so anpasst, dass sie nur die für den Kontext gültigen Begriffe enthält. Wenn Sie beispielsweise HTTP im vorherigen Listenfeld ausgewählt haben, ist die einzige Option REQ für Anforderungen. Da die Web App Firewall Anforderungen und zugeordnete Antworten als eine Einheit behandelt und beide filtert, müssen Sie keine spezifischen Antworten separat durchführen. Nachdem Sie Ihren zweiten Begriff ausgewählt haben, wird rechts neben dem zweiten Begriff ein drittes Listenfeld angezeigt. Im Hilfefenster wird eine Beschreibung des zweiten Begriffs angezeigt, und im Fenster Vorschau Ausdruck wird der Ausdruck angezeigt.
5. Wählen Sie im dritten Listenfeld den nächsten Begriff aus. Rechts wird ein neues Listenfeld angezeigt, und das Hilfefenster ändert sich, um eine Beschreibung des neuen Begriffs

anzuzeigen. Das Fenster Vorschauausdruck wird aktualisiert, um den Ausdruck so anzuzeigen, wie er bis zu diesem Punkt angegeben wurde.

6. Fahren Sie mit der Auswahl von Begriffen fort, und wenn Sie dazu aufgefordert werden, Argumente auszufüllen, bis der Ausdruck abgeschlossen ist. Wenn Sie einen Fehler machen oder Ihren Ausdruck ändern möchten, nachdem Sie bereits einen Begriff ausgewählt haben, können Sie einfach einen anderen Begriff auswählen. Der Ausdruck wird geändert, und alle Argumente oder mehr Begriffe, die Sie nach dem geänderten Begriff hinzugefügt haben, werden gelöscht.
7. Wenn Sie mit der Erstellung Ihres Ausdrucks fertig sind, klicken Sie auf OK, um das Dialogfeld Ausdruck hinzufügen zu schließen. Ihr Ausdruck wird in den Textbereich Ausdruck eingefügt.

So binden Sie eine Web App Firewall Richtlinie über die Citrix ADC GUI

1. Führen Sie einen der folgenden Schritte aus:
   - Navigieren Sie zu **Sicherheit** > **Web App Firewall**, und klicken Sie im Detailbereich auf **Anwendungsfirewall Policy Manager** .
   - Navigieren Sie zu **Sicherheit** > **Citrix Web App Firewall** > **Richtlinien** > **Firewall**, und klicken Sie im Bereich “Citrix Web App Firewallrichtlinien” auf **Policy Manager**.
2. Wählen Sie im Dialogfeld **Anwendungsfirewall Policy Manager** aus der Dropdownliste den Bindpunkt aus, an den Sie die Richtlinie binden möchten. Folgende Möglichkeiten stehen zur Auswahl:
   - **Global überschreiben.** Richtlinien, die an diesen Bindungspunkt gebunden sind, verarbeiten den gesamten Datenverkehr von allen Schnittstellen der Citrix ADC Appliance und werden vor allen anderen Richtlinien angewendet.
   - **Virtueller LB Server.** Richtlinien, die an einen virtuellen Lastausgleichsserver gebunden sind, werden nur auf Datenverkehr angewendet, der von diesem virtuellen Lastausgleichsserver verarbeitet wird, und werden vor allen globalen Standardrichtlinien angewendet. Nachdem Sie LB Virtual Server ausgewählt haben, müssen Sie auch den spezifischen virtuellen Lastausgleichsserver auswählen, an den Sie diese Richtlinie binden möchten.
   - **CS Virtual Server.** Richtlinien, die an einen virtuellen Content Switching-Server gebunden sind, werden nur auf Datenverkehr angewendet, der von diesem virtuellen Content Switching-Server verarbeitet wird, und werden vor allen globalen Standardrichtlinien angewendet. Nachdem Sie CS Virtual Server ausgewählt haben, müssen Sie auch den spezifischen virtuellen Content Switching-Server auswählen, an den Sie diese Richtlinie binden möchten.
   - **Standard Global.** Richtlinien, die an diesen Bindungspunkt gebunden sind, verarbeiten den gesamten Datenverkehr von allen Schnittstellen der Citrix ADC Appliance.
   - **Richtlinienbezeichnung.** Richtlinien, die an eine Richtlinienbeschriftung gebunden sind, verarbeiten Datenverkehr, den die Richtlinienbeschriftung an sie weiterleitet. Die Richtlinienbezeichnung steuert die Reihenfolge, in der Richtlinien auf diesen Datenverkehr angewendet werden.

- **Keine.** Binden Sie die Richtlinie nicht an einen Bindepunkt.

3. Klicken Sie auf **Weiter**. Eine Liste der vorhandenen Web App Firewall Richtlinien wird angezeigt.
4. Wählen Sie die Richtlinie aus, die Sie binden möchten, indem Sie darauf klicken.
5. Nehmen Sie zusätzliche Anpassungen an der Bindung vor.
   - Um die Richtlinienpriorität zu ändern, klicken Sie auf das Feld, um es zu aktivieren, und geben Sie dann eine neue Priorität ein. Sie können auch Prioritäten **neu generieren wählen, um die Prioritäten** gleichmäßig neu zu nummerieren.
   - Um den Richtlinienausdruck zu ändern, doppelklicken Sie auf dieses Feld, um das Dialogfeld **Web App Firewall Richtlinie konfigurieren** zu öffnen, in dem Sie den Richtlinienausdruck bearbeiten können.
   - Um den Gehe zu Ausdruck festzulegen, doppelklicken Sie auf das Feld in der Spaltenüberschrift **Gehe zu Ausdruck**, um die Dropdownliste anzuzeigen, in der Sie einen Ausdruck auswählen können.
   - Um die Option “Aufrufen” festzulegen, doppelklicken Sie auf das Feld in der Spaltenüberschrift “Aufrufen”, um die Dropdownliste anzuzeigen, in der Sie einen Ausdruck auswählen können.
6. Wiederholen Sie die Schritte 3 bis 6, um zusätzliche Web App Firewall Richtlinien hinzuzufügen, die Sie global binden möchten.
7. Klicken Sie auf **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich gebunden wurde.

Manuelle Konfiguration Über die Befehlszeilenschnittstelle

October 5, 2021

> **Hinweis:**
>
> Wenn Sie die Web App Firewall Funktion manuell konfigurieren müssen, empfiehlt Citrix, die Citrix ADC GUI-Prozedur zu verwenden.

Sie können die Web App Firewall Funktionen über die **Citrix ADC** Befehlszeilenschnittstelle konfigurieren. Es gibt jedoch wichtige Ausnahmen. Sie können Signaturen nicht über die Befehlszeilenschnittstelle aktivieren. Es gibt rund 1.000 Standardsignaturen in sieben Kategorien, und die Aufgabe ist für die Befehlszeilenschnittstelle zu komplex. Sie können Features aktivieren oder deaktivieren und Parameter über die Befehlszeile konfigurieren, aber keine manuellen Relaxationen konfigurieren. Sie können die adaptive Lernfunktion konfigurieren und das Lernen über die Befehlszeile aktivieren, aber Sie können keine gelernten Entspannungen oder gelernten Regeln überprüfen und sie genehmigen oder überspringen. Die Befehlszeilenschnittstelle richtet sich an fortgeschrittene Benutzer, die mit der Citrix ADC Appliance und der Web App Firewall vertraut sind.

Um die Web App Firewall mit der Citrix ADC Befehlszeile manuell zu konfigurieren, verwenden Sie

einen Telnet- oder Secure Shell-Client Ihrer Wahl, um sich an der Citrix ADC-Befehlszeile anzumelden.

So erstellen Sie ein Profil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw profile <name> [-defaults ( basic | advanced )]`
- `set appfw profile <name> -type ( HTML | XML | HTML XML )`
- `save ns config`

Beispiel

Im folgenden Beispiel wird ein Profil mit dem Namen pr-basic mit grundlegenden Standardeinstellungen hinzugefügt und der Profiltyp HTML zugewiesen. Dies ist die geeignete Erstkonfiguration für ein Profil, um eine HTML-Website zu schützen.

```
1 add appfw profile pr-basic -defaults basic
2 set appfw profile pr-basic -type HTML
3 save ns config
4 <!--NeedCopy-->
```

So konfigurieren Sie ein Profil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw profile <name> <arg1> [<arg2> ...]` wobei `<arg1>` einen Parameter darstellt und `<arg2>` entweder einen anderen Parameter oder den Wert darstellt, der dem Parameter zugewiesen werden soll, der durch `<arg1>` gekennzeichnet ist. Eine Beschreibung der Parameter, die beim Konfigurieren bestimmter Sicherheitsprüfungen verwendet werden sollen, finden Sie unter Erweiterter Schutz und dessen Unterthemen. Beschreibungen der anderen Parameter finden Sie unter Parameter zum Erstellen eines Profils.
- `save ns config`

Beispiel

Das folgende Beispiel zeigt, wie Sie ein HTML-Profil konfigurieren, das mit grundlegenden Standardeinstellungen erstellt wurde, um mit dem Schutz einer einfachen HTML-basierten Website zu beginnen. In diesem Beispiel wird die Protokollierung und Verwaltung von Statistiken für die meisten Sicherheitsüberprüfungen aktiviert, das Blockieren jedoch nur für Prüfungen aktiviert, die niedrige Falsch-Positiv-Raten aufweisen und keine spezielle Konfiguration erfordern. Es aktiviert auch die Transformation von unsicherem HTML und unsicherem SQL, was Angriffe verhindert, aber keine Anfragen an Ihre

Websites blockiert. Wenn Protokollierung und Statistiken aktiviert sind, können Sie später die Protokolle überprüfen, um festzustellen, ob die Sperre für eine bestimmte Sicherheitsprüfung aktiviert werden soll.

```
set appfw profile -startURLAction log stats
set appfw profile -denyURLAction block log stats
set appfw profile -cookieConsistencyAction log stats
set appfw profile -crossSiteScriptingAction log stats
set appfw profile -crossSiteScriptingTransformUnsafeHTML ON
set appfw profile -fieldConsistencyAction log stats
set appfw profile -SQLInjectionAction log stats
set appfw profile -SQLInjectionTransformSpecialChars ON
set appfw profile -SQLInjectionOnlyCheckFieldsWithSQLChars ON
set appfw profile -SQLInjectionParseComments checkall
set appfw profile -fieldFormatAction log stats
set appfw profile -bufferOverflowAction block log stats
set appfw profile -CSRFtagAction log stats
save ns config
<!--NeedCopy-->
```

So erstellen und konfigurieren Sie eine Richtlinie

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw policy <name> <rule> <profile>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird eine Richtlinie mit dem Namen pl-blog mit einer Regel hinzugefügt, die den gesamten Datenverkehr zum oder vom Host blog.example.com abfängt und diese Richtlinie dem Profil pr-Blog zuordnet.

```
add appfw policy pl-blog "HTTP.REQ.HOSTNAME.DOMAIN.EQ("blog.example.com
    ")" pr-blog
<!--NeedCopy-->
```

So binden Sie eine Web App Firewall Richtlinie

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `bind appfw global <policyName> <priority>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird die Richtlinie pl-blog gebunden und die Priorität 10 zugewiesen.

```
bind appfw global pl-blog 10
save ns config
<!--NeedCopy-->
```

So konfigurieren Sie die Sitzungsgrenze pro PE

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw settings <session limit>`

Beispiel

Im folgenden Beispiel wird das Sitzungslimit pro PE konfiguriert.

```
> set appfw settings -sessionLimit 500000`

Done

Default value:100000   Max value:500000 per PE
<!--NeedCopy-->
```

Signaturen

October 5, 2021

Die Web App Firewall -Signaturen bieten spezifische, konfigurierbare Regeln, um den Schutz Ihrer Websites vor bekannten Angriffen zu vereinfachen. Eine Signatur stellt ein Muster dar, das eine Komponente eines bekannten Angriffs auf ein Betriebssystem, einen Webserver, eine Website, einen XML-basierten Webdienst oder eine andere Ressource ist. Eine umfangreiche Reihe von vorkonfigurierten integrierten oder systemeigenen Regeln der Web App Firewall bietet eine einfach zu

bedienende Sicherheitslösung, die die Leistung des Musterabgleichs nutzt, um Angriffe zu erkennen und vor Anwendungsschwachstellen zu schützen.

Sie können eigene Signaturen erstellen oder Signaturen in den integrierten Vorlagen verwenden. Die Web App Firewall verfügt über zwei integrierte Vorlagen:

- **Standardsignaturen**: Diese Vorlage enthält eine vorkonfigurierte Liste mit über 1.300 Signaturen, zusätzlich zu einer vollständigen Liste von SQL-Einschleusungsschlüsselwörtern, SQL-Sonderzeichenfolgen, SQL-Transformationsregeln und SQL-Platzhalterzeichen. Es enthält auch abgelehnte Muster für siteübergreifende Skripterstellung sowie zulässige Attribute und Tags für siteübergreifende Skripterstellung. Dies ist eine schreibgeschützte Vorlage. Sie können den Inhalt anzeigen, aber Sie können nichts in dieser Vorlage hinzufügen, bearbeiten oder löschen. Um es zu verwenden, müssen Sie eine Kopie erstellen. In Ihrer eigenen Kopie können Sie die Signaturregeln aktivieren, die Sie auf Ihren Datenverkehr anwenden möchten, und die Aktionen angeben, die ausgeführt werden sollen, wenn die Signaturregeln dem Datenverkehr entsprechen.

Die Web App Firewall-Signaturen stammen aus den von Snortveröffentlichten Regeln, einem Open-Source-Einbruchschutzsystem, das Echtzeit-Verkehrsanalysen durchführen kann, um verschiedene Angriffe und Prüfungen zu erkennen.

- ***Xpath Injection Patterns**: Diese Vorlage enthält einen vorkonfigurierten Satz von Literal und PCRE Schlüsselwörtern und speziellen Strings, die verwendet werden, um XPath (XML Path Language) Injectionsangriffe zu erkennen.

Leere Signaturen: Sie können nicht nur eine Kopie der integrierten Vorlage “Standardsignaturen” erstellen, sondern auch eine leere Signaturvorlage verwenden, um ein Signaturobjekt zu erstellen. Das Signaturobjekt, das Sie mit der Option für leere Signaturen erstellen, hat keine nativen Signaturregeln, verfügt jedoch genau wie die *Standardvorlage über alle integrierten SQL/Cross-Site-Skript-Entitäten.

Signaturen im externen Format: Die Web App Firewall unterstützt auch Signaturen im externen Format. Sie können den Scanbericht von Drittanbietern mit der XSLT-Dateien importieren, die von der Citrix Web App Firewall unterstützt werden. Für die folgenden Scanwerkzeuge stehen integrierte XSLT-Dateien zur Verfügung, um externe Formatdateien in ein natives Format zu übersetzen:

- Zenzic
- Tiefe Sicherheit für Web-Apps
- IBM AppScan Enterprise
- IBM AppScan Standard.
- Qualys
- Qualys Cloud
- Whitehat
- Hewlett Packard Enterprise WebInspect

- Rapid7 Appspider
- Acunetix

Sicherheitsschutz für Ihre Anwendung

Straffere Sicherheit erhöht den Verarbeitungsaufwand. Signaturen bieten die folgenden Bereitstellungsoptionen, mit denen Sie den Schutz Ihrer Anwendungen optimieren können:

- **Negatives Sicherheitsmodell**: Mit dem negativen Sicherheitsmodell verwenden Sie einen umfangreichen Satz vorkonfigurierter Signaturregeln, um die Leistung des Musterabgleichs anzuwenden, um Angriffe zu erkennen und vor Anwendungsschwachstellen zu schützen. Sie blockieren nur das, was Sie nicht wollen, und erlauben den Rest. Sie können Ihre eigenen Signaturregeln hinzufügen, die auf den spezifischen Sicherheitsanforderungen Ihrer Anwendungen basieren, um Ihre eigenen benutzerdefinierten Sicherheitslösungen zu entwerfen.
- **Hybrides Sicherheitsmodell**: Zusätzlich zur Verwendung von Signaturen können Sie positive Sicherheitsprüfungen verwenden, um eine Konfiguration zu erstellen, die sich ideal für Ihre Anwendungen eignet. Verwenden Sie Signaturen, um das zu blockieren, was Sie nicht möchten, und verwenden Sie positive Sicherheitsprüfungen, um die zulässigen Werte zu erzwingen.

Um Ihre Anwendung mithilfe von Signaturen zu schützen, müssen Sie ein oder mehrere Profile für die Verwendung des Signaturobjekts konfigurieren. In einer hybriden Sicherheitskonfiguration werden die SQL-Injections- und siteübergreifenden Skriptmuster sowie die SQL-Transformationsregeln in Ihrem Signaturenobjekt nicht nur von den Signaturregeln verwendet, sondern auch von den positiven Sicherheitsprüfungen, die im Web App Firewall Profil konfiguriert sind, das das Signature-Objekt verwendet.

Die Web App Firewall untersucht den Datenverkehr zu Ihren geschützten Websites und Webdiensten, um Datenverkehr zu erkennen, der einer Signatur entspricht. Eine Übereinstimmung wird nur ausgelöst, wenn jedes Muster in der Regel mit dem Datenverkehr übereinstimmt. Wenn eine Übereinstimmung auftritt, werden die angegebenen Aktionen für die Regel aufgerufen. Sie können eine Fehlerseite oder ein Fehlerobjekt anzeigen, wenn eine Anforderung blockiert wird. Protokollmeldungen können Ihnen helfen, Angriffe zu identifizieren, die gegen Ihre Anwendung gestartet werden. Wenn Sie Statistiken aktivieren, verwaltet die Web App Firewall Daten zu Anforderungen, die mit einer Web App Firewall-Signatur oder einer Sicherheitsprüfung übereinstimmen.

Wenn der Datenverkehr sowohl mit einer Signatur als auch mit einer positiven Sicherheitsprüfung übereinstimmt, werden die restriktiveren der beiden Aktionen durchgesetzt. Wenn beispielsweise eine Anforderung mit einer Signaturregel übereinstimmt, für die die Blockaktion deaktiviert ist, aber die Anforderung auch mit einer positiven SQL Injection Sicherheitsprüfung übereinstimmt, für die die Aktion blockiert ist, wird die Anforderung blockiert. In diesem Fall wird die Signaturverletzung möglicherweise als protokolliert<not blocked>, obwohl die Anforderung durch die SQL-Injectionsprüfung blockiert wird.

Anpassung: Bei Bedarf können Sie eigene Regeln zu einem Signaturobjekt hinzufügen. Sie können auch die SQL/Cross-Site Scripting Pattern anpassen. Die Möglichkeit, eigene Signaturregeln auf der Grundlage der spezifischen Sicherheitsanforderungen Ihrer Anwendungen hinzuzufügen, gibt Ihnen die Flexibilität, Ihre eigenen benutzerdefinierten Sicherheitslösungen zu entwerfen. Sie blockieren nur das, was Sie nicht wollen, und erlauben den Rest. Ein bestimmtes Fast-Match-Muster an einem angegebenen Speicherort kann den Verarbeitungsaufwand erheblich reduzieren, um die Leistung zu optimieren. Sie können SQL-Injections- und siteübergreifende Skriptmuster hinzufügen, ändern oder entfernen. Integrierte RegEx- und Expression-Editoren helfen Ihnen, Ihre Muster zu konfigurieren und deren Genauigkeit zu überprüfen.

Automatische Aktualisierung: Sie können das Signaturobjekt manuell aktualisieren, um die neuesten Signaturregeln abzurufen, oder Sie können das Feature für die automatische Aktualisierung anwenden, damit die Web App Firewall die Signaturen automatisch über den cloudbasierten Aktualisierungsdienst der Web App Firewall aktualisieren kann.

> **Hinweis:**
>
> Wenn während der automatischen Aktualisierung neue Signaturregeln hinzugefügt werden, sind sie standardmäßig deaktiviert. Sie müssen die aktualisierten Signaturen regelmäßig überprüfen und die neu hinzugefügten Regeln aktivieren, die für den Schutz Ihrer Anwendungen relevant sind.
>
> Sie müssen CORS so konfigurieren, dass Signaturen auf IIS-Servern gehostet werden.
>
> Die automatische Signaturaktualisierung funktioniert auf dem lokalen Webserver nicht, wenn Sie über die Citrix ADC GUI auf die URL zugreifen.

Erste Schritte

Die Verwendung von Citrix -Signaturen zum Schutz Ihrer Anwendung ist einfach und kann in wenigen einfachen Schritten ausgeführt werden:

1. Fügen Sie ein Signaturobjekt hinzu.

- Sie können den Assistenten verwenden, der Sie auffordert, die gesamte Web App Firewall Konfiguration zu erstellen, einschließlich Hinzufügen des Profils und der Richtlinie, Auswählen und Aktivieren von Signaturen und Angeben von Aktionen für Signaturen und positive Sicherheitsprüfungen. Das Signaturobjekt wird automatisch erstellt.
- Sie können eine Kopie des Signaturobjekts aus der Vorlage "*Standardsignaturen" erstellen, eine leere Vorlage verwenden, um eine Signatur mit Ihren eigenen benutzerdefinierten Regeln zu erstellen, oder eine externe Formatsignatur hinzufügen. Aktivieren Sie die Regeln und konfigurieren Sie die Aktionen, die Sie anwenden möchten.

1. Konfigurieren Sie das Zielprofil der Web App Firewall, um dieses Signaturobjekt zu verwenden.

2. Datenverkehr senden, um die Funktionalität zu validieren

Highlights

- Das Standardsignaturobjekt ist eine Vorlage. Sie kann nicht bearbeitet oder gelöscht werden. Um es zu verwenden, müssen Sie eine Kopie erstellen. In Ihrer eigenen Kopie können Sie die Regeln und die gewünschte Aktion für jede Regel aktivieren, wie für Ihre Anwendung erforderlich. Um die Anwendung zu schützen, müssen Sie das Zielprofil so konfigurieren, dass diese Signatur verwendet wird.
- Das Verarbeiten von Signaturmustern hat Overhead. Versuchen Sie, nur die Signaturen zu aktivieren, die für den Schutz Ihrer Anwendung gelten, anstatt alle Signaturregeln zu aktivieren.
- Jedes Muster in der Regel muss übereinstimmen, um eine Signaturübereinstimmung auszulösen.
- Sie können eigene benutzerdefinierte Regeln hinzufügen, um eingehende Anforderungen zu überprüfen, um verschiedene Arten von Angriffen zu erkennen, wie SQL-Injection oder Cross-Site-Skripting-Angriffe. Sie können auch Regeln hinzufügen, um die Antworten zu überprüfen, um das Auslaufen vertraulicher Informationen wie Kreditkartennummern zu erkennen und zu blockieren.
- Sie können eine Kopie eines vorhandenen Signaturobjekts erstellen und es anpassen, indem Sie Regeln und SQL/Cross-Site-Skriptmuster hinzufügen oder bearbeiten, um eine andere Anwendung zu schützen.
- Sie können die automatische Aktualisierung verwenden, um die neueste Version der Standardregeln der Web App Firewall herunterzuladen, ohne dass eine fortlaufende Überwachung erforderlich ist, um die Verfügbarkeit des neuen Updates zu überprüfen.
- Ein Signaturobjekt kann von mehr als einem Profil verwendet werden. Auch nachdem Sie ein oder mehrere Profile für die Verwendung eines Signaturobjekts konfiguriert haben, können Sie Signaturen weiterhin aktivieren oder deaktivieren oder die Aktionseinstellungen ändern. Sie können eigene benutzerdefinierte Signaturregeln manuell erstellen und ändern. Die Änderungen gelten für alle Profile, die derzeit für die Verwendung dieses Signaturobjekts konfiguriert sind.
- Sie können Signaturen konfigurieren, um Verletzungen in verschiedenen Arten von Nutzlasten zu erkennen, wie HTML, XML, JSON und GWT.
- Sie können ein konfiguriertes Signaturobjekt exportieren und es in eine andere Citrix ADC Appliance importieren, um Ihre benutzerdefinierten Signaturregeln einfach zu replizieren.

Signaturen sind Muster, die einer bekannten Sicherheitsanfälligkeit zugeordnet sind. Sie können den Signaturschutz verwenden, um den Datenverkehr zu identifizieren, der versucht, diese Sicherheitsanfälligkeiten auszunutzen, und bestimmte Maßnahmen ergreifen.

Signaturen sind in Kategorien unterteilt. Sie können die Leistung optimieren und den Verarbeitungsaufwand reduzieren, indem Sie nur die Regeln in den Kategorien aktivieren, die zum Schutz

Ihrer Anwendung geeignet sind.

Manuelles Konfigurieren des Signatur-Features

October 5, 2021

Um Signaturen zum Schutz Ihrer Websites zu verwenden, müssen Sie die Regeln überprüfen und diejenigen aktivieren und konfigurieren, die Sie anwenden möchten. Die Regeln sind standardmäßig deaktiviert. Citrix empfiehlt, dass Sie alle Regeln aktivieren, die für die Art des Inhalts gelten, den Ihre Website verwendet.

Um die Signaturfunktion manuell zu konfigurieren, verwenden Sie einen Browser, um eine Verbindung mit der GUI herzustellen. Erstellen Sie dann ein Signaturobjekt aus einer integrierten Vorlage, einem vorhandenen Signaturobjekt oder durch Importieren einer Datei. Konfigurieren Sie als Nächstes das neue Signatures-Objekt wie unter Konfigurieren oder Ändern eines Signatures-Objektsbeschrieben.

Hinzufügen oder Entfernen eines Signaturobjekts

April 25, 2022

Sie können der Web App Firewall ein neues Signaturobjekt hinzufügen, indem Sie:

- Eine eingebaute Vorlage kopieren.
- Kopieren eines vorhandenen Signaturobjekts.
- Importieren eines Signaturobjekts aus einer externen Datei.

Die Signaturdatei enthält die CPU-Auslastung, das letzte anwendbare Jahr und Details zum Schweregrad. Sie können die CPU-Auslastung, das letzte Jahr und den CVE-Schweregrad jedes Mal sehen, wenn eine Signaturdatei regelmäßig geändert und hochgeladen wird. Nachdem Sie diese Werte beobachtet haben, können Sie entscheiden, ob Sie die Signatur auf der Appliance aktivieren oder deaktivieren möchten.

Sie müssen die GUI verwenden, um eine Vorlage oder ein vorhandenes Signaturobjekt zu kopieren. Sie können entweder die GUI oder die Befehlszeile verwenden, um ein Signaturobjekt zu importieren. Sie können auch entweder die GUI oder die Befehlszeile verwenden, um ein Signaturobjekt zu entfernen.

So erstellen Sie ein Signaturobjekt aus einer Vorlage

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Signaturen**.

2. Wählen Sie im Detailbereich das Signaturobjekt aus, das Sie als Vorlage verwenden möchten.

   Ihre Auswahlmöglichkeiten:

   - **Standardsignaturen.** Enthält die Signaturregeln, die SQL-Einschleusungsregeln und die Cross-Site-Scripting-Regeln.
   - **XPath-Einschleusung.** Enthält die XPath-Einschleusungsmuster.
   - **Jedes vorhandene Signaturobjekt.**

   > **Achtung:**
   >
   > Wenn Sie keinen Signaturtyp wählen, der als Vorlage verwendet werden soll, werden Sie von der Web App Firewall aufgefordert, Signaturen von Grund auf neu zu erstellen.

3. Klicken Sie auf **Hinzufügen**.
4. Geben Sie im Dialogfeld Signaturobjekt hinzufügen einen Namen für das neue Signaturobjekt ein, und klicken Sie dann auf OK. Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrichsymbol beginnen und aus einem bis 31 Buchstaben, Zahlen und dem Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), bei (@), gleich (=) und Unterstrichen (_) bestehen.
5. Klicken Sie auf **Schließen**.

So erstellen Sie ein Signaturobjekt durch Importieren einer Datei

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Signaturen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Wählen **Sie im Dialogfeld Signaturen-Objekt hinzufügen** das Format der Signaturen aus, die Sie importieren möchten.
   - Um eine Signaturdatei im Citrix ADC-Format zu importieren, wählen Sie die Registerkarte **Natives Format** .
   - Um eine Datei im externen Signaturformat zu importieren, wählen Sie die Registerkarte **Externes Format** .
4. Wählen Sie die Datei aus, die Sie zum Erstellen Ihres Signaturobjekts verwenden möchten.
   - Um eine native Signaturdatei im Citrix ADC-Format zu importieren, wählen Sie im Abschnitt Importieren entweder Aus lokaler Datei importieren oder Aus URL importieren aus, und geben Sie dann den Pfad oder die URL der Datei ein oder navigieren Sie zu ihm.
   - Um eine Datei im Format Cenzic, IBM AppScan, Qualys oder Whitehat zu importieren, wählen Sie im Abschnitt XSLT die Option Integrierte XSLT-Datei verwenden, Lokale Datei verwenden oder Referenz von URL aus. Wenn Sie als Nächstes Integrierte XSLT-Datei verwenden gewählt haben, wählen Sie das entsprechende Dateiformat aus der Liste aus. Wenn Sie Lokale Datei oder Referenz von URL verwenden ausgewählt haben, geben Sie den Pfad oder die URL zur Datei ein oder navigieren Sie zu ihm.
5. Klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **Schließen**.

So erstellen Sie ein Signaturobjekt durch Importieren einer Datei mithilfe der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `import appfw signatures <src> <name> [-xslt <string>] [-comment <string>] [-overwrite] [-merge] [-sha1 <string>]`
- `save ns config`

Beispiel #1

Im folgenden Beispiel wird ein Signaturobjekt aus einer Datei mit dem Namen signatures.xml erstellt und ihm den Namen mySignatures zugewiesen.

```
1 import appfw signatures local:signatures.xml MySignatures
2 save ns config
3 <!--NeedCopy-->
```

So entfernen Sie ein Signaturobjekt mit der GUI

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Signaturen**.
2. Wählen Sie im Detailbereich das Signaturobjekt aus, das Sie entfernen möchten.
3. Klicken Sie auf **Entfernen**.

So entfernen Sie ein Signatures-Objekt mithilfe der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `rm appfw signatures <name>`
- `save ns config`

Konfigurieren oder Ändern eines Signaturobjekts

October 5, 2021

Sie konfigurieren ein Signaturobjekt nach dem Erstellen oder ändern ein vorhandenes Signaturobjekt, um Signaturkategorien oder bestimmte Signaturen zu aktivieren oder zu deaktivieren, und konfigurieren, wie die Web App Firewall reagiert, wenn eine Signatur mit einer Verbindung übereinstimmt.

So konfigurieren oder ändern Sie ein Signaturobjekt

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Signaturen**.
2. Wählen Sie im Detailbereich das Signaturobjekt aus, das Sie konfigurieren möchten, und klicken Sie dann auf **Öffnen**.
3. Legen Sie im Dialogfeld **Signaturobjekt ändern** die Optionen **Anzeigefilterkriterien** links fest, um die Filterelemente anzuzeigen, die Sie konfigurieren möchten.

   Wenn Sie diese Optionen ändern, werden die angeforderten Ergebnisse im Fenster Gefilterte Ergebnisse rechts angezeigt.

   - Um nur ausgewählte Signaturkategorien anzuzeigen, aktivieren oder deaktivieren Sie die entsprechenden Kontrollkästchen für Signaturkategorie. Die Unterschriftenkategorien sind:

Name	Art des Angriffs, vor dem diese Signatur schützt
cgi	CGI-Skripts. Enthält Perl- und UNIX-Shell-Skripts.
Client	Browser und andere Clients.
Coldfusion	Websites, die den Adobe Systems ColdFusion-Anwendungsserver verwenden.
Frontseite	Websites, die den FrontPage-Server von Microsoft verwenden.
Das ist es	Websites, die den Microsoft Internet Information Server (IIS) verwenden.
Sonstiges	Verschiedene Angriffe.
php	Websites, die PHP verwenden
web-activex	Websites, die ActiveX-Kontrollen enthalten.
Streben	Websites, die Apache Struts enthalten, bei denen es sich um Java-EE-basierte Applets handelt.

   - Um nur Signaturen anzuzeigen, für die bestimmte Prüfaktionen aktiviert sind, aktivieren Sie das Kontrollkästchen ON für jede dieser Aktionen, deaktivieren Sie die Kontrollkästchen ON für die anderen Aktionen und deaktivieren Sie alle Kontrollkästchen OFF. Um nur Signaturen anzuzeigen, für die eine bestimmte Checkaktion deaktiviert ist, aktivieren Sie die entsprechenden Kontrollkästchen OFF, und deaktivieren Sie alle Kontrollkästchen ON. Um Signaturen unabhängig davon anzuzeigen, ob eine Prüfaktion

aktiviert oder deaktiviert ist, aktivieren oder deaktivieren Sie die Kontrollkästchen ON und OFF für diese Aktion. Die Check-Aktionen sind:

Kriterium	Beschreibung
Aktiviert	Die Signatur ist aktiviert. Die Web App Firewall prüft nur auf Signaturen, die bei der Verarbeitung des Datenverkehrs aktiviert sind.
Blockieren	Verbindungen, die dieser Signatur entsprechen, werden blockiert.
Protokollierung	Für jede Verbindung, die dieser Signatur entspricht, wird ein Protokolleintrag erstellt.
Statistiken	Die Web App Firewall enthält jede Verbindung, die dieser Signatur entspricht, in den Statistiken, die sie für diese Prüfung generiert.

- Um nur Signaturen anzuzeigen, die eine bestimmte Zeichenfolge enthalten, geben Sie die Zeichenfolge in das Textfeld unter den Filterkriterien ein, und klicken Sie dann auf Suchen.
- Um alle Anzeigefilterkriterien auf die Standardeinstellungen zurückzusetzen und alle Signaturen anzuzeigen, klicken Sie auf Alle anzeigen.

4. Informationen zu einer bestimmten Signatur erhalten Sie, indem Sie die Signatur auswählen, und klicken Sie dann im Feld Weitere auf den blauen Doppelpfeil. Das Meldungsfeld Sicherheitsanfälligkeit in Signaturregel wird angezeigt. Sie enthält Informationen über den Zweck der Signatur und enthält Links zu externen webbasierten Informationen über die Sicherheitsanfälligkeit oder Sicherheitsanfälligkeiten, die diese Signatur behebt. Um auf einen externen Link zuzugreifen, klicken Sie auf den blauen Doppelpfeil links neben der Beschreibung dieses Links.
5. Konfigurieren Sie die Einstellungen für eine Signatur, indem Sie die entsprechenden Kontrollkästchen aktivieren.
6. Wenn Sie dem Signature-Objekt eine lokale Signaturregel hinzufügen oder eine vorhandene lokale Signaturregel ändern möchten, lesen Sie den Signatur-Editor.
7. Wenn Sie keine SQL-Injection, siteübergreifendes Skripting oder Xpath-Injectionsmuster benötigen, klicken Sie auf OK, und klicken Sie dann auf Schließen. Andernfalls klicken Sie in der unteren linken Ecke des Detailfensters auf SQL/Cross-Site Scripting Patterns verwalten.
8. Navigieren Sie im Dialogfeld SQL/Cross-Site-Skriptmuster verwalten im Fenster Gefilterte Ergebnisse zu der Musterkategorie und dem Muster, die Sie konfigurieren möchten. Informationen zu den SQL-Einschleusungsmustern finden Sie unter HTML SQL Injection Check. Informationen zu den Cross-Site-Skriptmustern finden Sie unter HTML Cross-Site Scripting Check.

9. So fügen Sie ein neues Muster hinzu:
    a) Wählen Sie den Zweig aus, dem Sie das neue Muster hinzufügen möchten.
    b) Klicken Sie direkt unter dem unteren Bereich des Fensters **Gefilterte Ergebnisse** auf die Schaltfläche **Hinzufügen**.
    c) Füllen Sie im Dialogfeld Signaturelement erstellen das Textfeld Element mit dem Muster aus, das Sie hinzufügen möchten. Wenn Sie dem Verzweig Transformationsregeln ein Transformationsmuster hinzufügen, füllen Sie unter Elemente das Textfeld Von mit dem Muster aus, das Sie ändern möchten, und das Textfeld Bis mit dem Muster aus, in das Sie das vorherige Muster ändern möchten.
    d) Klicken Sie auf **OK**.
10. So ändern Sie ein vorhandenes Muster:
    a) Wählen Sie im Fenster **Gefilterte Ergebnisse** den Zweig aus, der das zu ändernde Muster enthält.
    b) Wählen Sie im Detailfenster unterhalb des Fensters **Gefilterte Ergebnisse** das Muster aus, das Sie ändern möchten.
    c) Klicken Sie auf **Ändern**.
    d) **Ändern Sie im Dialogfeld Signaturelement** ändern (Modify Signature Item) im Textfeld **Element** das Muster. Wenn Sie ein Transformationsmuster ändern, können Sie entweder oder beide Muster unter Elemente in den Textfeldern Von und Bis ändern.
    e) Klicken Sie auf **OK**.
11. Um ein Muster zu entfernen, wählen Sie das Muster aus, das Sie entfernen möchten, und klicken Sie dann unter dem Detailbereich unterhalb des Fensters **Gefilterte Ergebnisse** auf die Schaltfläche **Entfernen**. Wenn Sie dazu aufgefordert werden, bestätigen Sie Ihre Auswahl, indem Sie auf **Schließen**klicken.
12. So fügen Sie dem Cross-Site-Scripting-Zweig die Kategorie “Pattern
    a) Wählen Sie den Zweig aus, dem Sie die Musterkategorie hinzufügen möchten.
    b) Klicken Sie direkt unter dem Fenster **Gefilterte Ergebnisse** auf die Schaltfläche **Hinzufügen**.

        > **Hinweis:** Derzeit können Sie dem Cross-Site-Scripting-Zweig nur eine Kategorie, benannte Muster, hinzufügen. Nachdem Sie auf **Hinzufügen**geklickt haben, müssen Sie die Standardauswahl akzeptieren, nämlich Muster.

    c) Klicken Sie auf **OK**.
13. Um einen Zweig zu entfernen, wählen Sie diesen Zweig aus, und klicken Sie dann direkt unter dem Fenster **Gefilterte Ergebnisse** auf die Schaltfläche Entfernen. Wenn Sie dazu aufgefordert werden, bestätigen Sie Ihre Auswahl, indem Sie auf **OK**klicken.

> **Hinweis:** Wenn Sie einen Standardzweig entfernen, entfernen Sie alle Muster in diesem Zweig. Auf diese Weise können die Sicherheitsprüfungen deaktiviert werden, die diese Informationen verwenden.

14. Wenn Sie die SQL-Injections-, siteübergreifende Skripterstellung und XPath-Injectionsmuster geändert haben, klicken Sie auf **OK**, und klicken Sie dann auf **Schließen**, um zum Dialogfeld **Signaturobjekt ändern**zurückzukehren.
15. Klicken Sie an einer beliebigen Stelle auf **OK**, um die Änderungen zu speichern. Wenn Sie die Konfiguration des Signaturobjekts abgeschlossen haben, klicken Sie auf **Schließen** .

Schützen von JSON-Anwendungen mit Signaturen

October 5, 2021

JavaScript Object Notation (JSON) ist ein textbasierter offener Standard, der von der JavaScript-Skriptsprache abgeleitet wird. JSON wird bevorzugt für die von Menschen lesbare Darstellung einfacher Datenstrukturen und assoziativer Arrays, sogenannte Objekte. Es dient als Alternative zu XML und wird hauptsächlich zur Übertragung serialisierter Datenstrukturen für die Kommunikation mit Webanwendungen verwendet. Die JSON-Dateien werden normalerweise mit der Erweiterung .json gespeichert.

Die JSON-Nutzlast wird normalerweise mit dem MIME-Typ gesendet, der als **application/json**angegeben ist. Die anderen Standard Inhaltstypen für JSON sind:

- **application/x-javascript**
- **text/javascript**
- **text/x-javascript**
- **text/x-json**

Verwenden der Citrix Web App Firewall -Signaturen zum Schutz von JSON-Anwendungen

Um JSON-Anforderungen zuzulassen, ist die Appliance mit dem JSON-Inhaltstyp vorkonfiguriert, wie in der folgenden Show-Command-Ausgabe dargestellt:

```
1 > sh appfw jsonContentType
2 1)      JSONContenttypevalue:  ”^application/json$” IsRegex:  REGEX
3 Done
4 <!--NeedCopy-->
```


Die Citrix Web App Firewall verarbeitet den Posttext nur für die folgenden Inhaltstypen:

- **application/x-www-form-urlencoded**
- **multipart/form-data**
- **text/x-gwt-rpc**

Die Anforderungen, die mit anderen Content-Type-Headern einschließlich application/json (oder einem anderen zulässigen Inhaltstyp) empfangen werden, werden nach der Header-Prüfung an das Backend weitergeleitet. Der Post-Text in solchen Anfragen wird nicht auf Verstöße gegen die Sicherheitsprüfung überprüft, selbst wenn die Sicherheitsprüfungen des Profils wie SQL oder Cross-Site-Scripting aktiviert sind.

Um JSON-Anwendungen zu schützen und Verletzungen zu erkennen, können Web App Firewall -Signaturen verwendet werden. Alle Anforderungen, die den zulässigen Content-Type-Header enthalten, werden von der Web App Firewall für die Signaturübereinstimmung verarbeitet. Sie können Ihre eigenen benutzerdefinierten Signaturregeln hinzufügen, um die JSON-Nutzlast zu verarbeiten und verschiedene Sicherheitsprüfungsinspektionen durchzuführen (z. B. standortübergreifendes Scripting, SQL und Feldkonsistenz), um Verstöße in den Headern sowie im Postbody zu erkennen und bestimmte Maßnahmen zu ergreifen.

> **Tipp**
>
> Im Gegensatz zu den anderen integrierten Standardeinstellungen kann der vorkonfigurierte JSON-Inhaltstyp mit der CLI oder der GUI (GUI) bearbeitet oder entfernt werden. Wenn legitime Anforderungen für JSON-Anwendungen blockiert werden und Inhaltstypverletzungen auslösen, überprüfen Sie, ob der Inhaltstypwert genau konfiguriert ist. Weitere Informationen darüber, wie Web App Firewall Content-Typ-Header verarbeitet, finden Sie unter Schutz von Inhaltstypen

So fügen Sie JSON-Inhaltstyp mit der Befehlszeilenschnittstelle hinzu oder entfernen Sie sie

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
add appfw jsonContentType ^application/json$ IsRegEx REGEX
```

```
rm appfw JSONContentType "^application/json$"
```

So verwalten Sie JSON-Inhaltstypen mit der GUI

Navigieren Sie zu **Sicherheit** > **Web App Firewall**, und wählen Sie im Abschnitt **Einstellungen** die Option **JSON-Inhaltstypen verwalten** aus.

Fügen Sie im Fenster **JSONWeb App Firewall Inhaltstyp konfigurieren** JSON-Inhaltstypen hinzu, bearbeiten oder löschen Sie JSON-Inhaltstypen entsprechend den Anforderungen Ihrer Anwendungen.

Konfigurieren des Signaturschutzes zur Erkennung von Angriffen in JSON-Nutzlast

Zusätzlich zu einem gültigen JSON-Inhaltstyp müssen Sie Signaturen konfigurieren, um die Muster anzugeben, die, wenn sie in einer JSON-Anforderung erkannt werden, auf eine Sicherheitsverletzung hinweisen. Die angegebenen Aktionen, wie Block und Protokoll, werden ausgeführt, wenn eine eingehende Anforderung eine Übereinstimmung für alle Zielmuster in der Signaturregel auslöst.

Um eine benutzerdefinierte Signaturregel hinzuzufügen, empfiehlt Citrix die Verwendung der GUI. Navigieren Sie zu **System** > **Sicherheit** > **Web App Firewall** > **Signaturen** . Doppelklicken Sie auf das Zielsignaturobjekt, um auf das Bedienfeld **Web App Firewall-Signaturen bearbeiten** zuzugreifen. Klicken Sie auf die Schaltfläche **Hinzufügen**, um Aktionen, Kategorie, Protokollzeichenfolge, Regelmuster usw. zu konfigurieren. Obwohl die Web App Firewall alle zulässigen Inhaltstype-Nutzlast auf Signaturübereinstimmung überprüft, können Sie die Verarbeitung optimieren, indem Sie den JSON-Ausdruck in der Regel angeben. Wenn Sie ein neues Regelmuster **hinzufügen**, wählen Sie in den Dropdown-Optionen für **Übereinstimmung** die Option **Ausdruck** aus, und geben Sie den Zielübereinstimmungsausdruck aus Ihrer JSON-Nutzlast an, um die spezifischen Anforderungen zu identifizieren, die überprüft werden müssen. Ein Ausdruck muss mit einem **TEXT** beginnen. Präfix. Sie können andere Regelmuster hinzufügen, um zusätzliche Übereinstimmungsmuster zur Identifizierung des Angriffs anzugeben.

Das folgende Beispiel zeigt eine Signaturregel. Wenn im POST-Text der JSON-Nutzlast ein siteübergreifendes Skript-Tag erkannt wird, das dem angegebenen XPATH_JSON-Ausdruck entspricht, wird eine Signaturübereinstimmung ausgelöst.

Beispiel einer Signatur zur Erkennung von Cross-Site-Scripting in JSON-Nutzlast

```
<SignatureRule actions="log,stats" category="JSON" enabled="ON" id="
    1000001" severity="" source="" type="" version="1">

  <PatternList>

    <RequestPatterns>

      <Pattern>

        <Location area="HTTP_POST_BODY"/>

        <Match type="Expression">TEXT.XPATH_JSON(xp%/glossary/title%).
            CONTAINS("example glossary")</Match>

      </Pattern>

      <Pattern>
```



```
16
17          <Location area="HTTP_METHOD"/>
18
19          <Match type="LITERAL">POST</Match>
20
21        </Pattern>
22
23        <Pattern>
24
25          <Location area="HTTP_POST_BODY"/>
26
27          <Match type="CrossSiteScripting"/>
28
29         </Pattern>
30
31      </RequestPatterns>
32
33    </PatternList>
34
35    <LogString>Cross-site scripting violation detected in json payload</
        LogString>
36
37    <Comment/>
38
39 </SignatureRule>
40 <!--NeedCopy-->
```

Beispiel für die Nutzlast

Die folgende Nutzlast löst die Signaturübereinstimmung aus, da sie das siteübergreifende Skript-Tag **<Gotcha!!>**.

```
1 {
2  "glossary": {
3  "title": "example glossary","GlossDiv": {
4  "title": "S","GlossList": {
5  "GlossEntry": {
6  "ID": "SGML","SortAs": "SGML","GlossTerm": "Standard Generalized
      Markup Language","Acronym": "SGML","Abbrev": "ISO 8879:1986","
      GlossDef": {
7  "para": "A meta-markup language, used to create markup languages \*\*<
      Gotcha!!>\*\* such as DocBook.","GlossSeeAlso": ["GML", "XML"] }
```



```
 ,"GlossSee": "markup" }
  }
  }
  }
  }

<!--NeedCopy-->
```

Beispiel für die Protokollnachricht

```
Aug 21 12:21:42 <local0.info> 10.217.31.239 08/21/2015:23:21:42 GMT ns
   0-PPE-1 : APPFW APPFW_SIGNATURE_MATCH 1471 0 :  10.217.253.62 990-
   PPE0 NtJnVMNnvPeQJnaUzXYW/GTvAQsA010 prof1 http://10.217.31.212/FFC/
   login_post.php Signature violation rule ID 1000001: cross-site
   scripting violation detected in json payload  <not blocked>
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn Sie dieselbe Nutzlast senden, nachdem Sie das Cross-Site-Script-Tag entfernt haben (**<Gotcha!!>**), wird die Signaturregelübereinstimmung nicht ausgelöst.

Highlights

- Um die JSON-Nutzlast zu schützen, verwenden Sie Web App Firewall -Signaturen, um Cross-Site-Scripting, SQL und andere Verstöße zu erkennen.
- Stellen Sie sicher, dass der JSON-Inhaltstyp auf der Appliance als zulässiger Inhaltstyp konfiguriert ist.
- Stellen Sie sicher, dass der Inhaltstyp in der Nutzlast mit dem konfigurierten JSON-Inhaltstyp übereinstimmt.
- Stellen Sie sicher, dass alle in der Signaturregel konfigurierten Muster mit der Signaturverletzung übereinstimmen, die ausgelöst werden soll.
- Wenn Sie eine Signaturregel hinzufügen, MUSS mindestens ein Regelmuster haben, das dem Ausdruck in der JSON-Nutzlast entspricht. Alle PI-Ausdrücke in Signaturregeln müssen mit dem Präfix TEXT beginnen und müssen boolean sein.

Schützen Sie den Anwendungs- oder JSON-Inhaltstyp mit SQL und Cross-Site-Scripting-codierter Nutzlast mithilfe von Richtlinien und Signaturen

Citrix Web App Firewall kann Anwendungs- oder JSON-Inhaltstyp mithilfe von Richtlinien und Signaturen schützen.

Überprüfen des Anwendungs- oder JSON-Inhaltstyps auf SQL-Injection mithilfe von Richtlinien

Sie müssen die folgenden Richtlinien hinzufügen und sie global an den virtuellen Server binden, um SQL-Injection zu unterstützen.

```
add appfw policy sqli_1 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A)
|(?<=[^a-zA-Z0-9_])))(select|insert|delete|update|drop|create|alter|grant
|revoke|commit|rollback|shutdown|union|intersect|minus|case|decode|where
|group|begin|join|exists|distinct|add|modify|constraint|null|like|exec|
execute|char|or|and|sp_sdidebug)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK
```

```
add appfw policy sqli_2 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A)
|(?<=[^a-zA-Z0-9_]))(xp_availablemedia|xp_cmdshell|xp_deletemail|xp_dirtree
|xp_dropwebtask|xp_dsninfo|xp_enumdsn|xp_enumerrorlogs|xp_enumgroups|
xp_enumqueuedtasks|xp_eventlog|xp_findnextmsg|xp_fixeddrives|xp_getfiledetails
|xp_getnetname|xp_grantlogin|xp_logevent|xp_loginconfig|xp_logininfo|
xp_makewebtask|xp_msver|xp_regread|xp_perfend|xp_perfmonitor|xp_perfsample
|xp_perfstart|xp_readerrorlog|xp_readmail|xp_revokelogin|xp_runwebtask|
xp_schedulersignal|xp_sendmail|xp_servicecontrol|xp_snmp_getstate|xp_snmp_raisetrap
|xp_sprintf|xp_sqlinventory|xp_sqlregister|xp_sqltrace|xp_sscanf|xp_startmail
|xp_stopmail|xp_subdirs|xp_unc_to_drive)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK
```

```
add appfw policy sqli_3 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A)
|(?<=[^a-zA-Z0-9_]))(sysobjects|syscolumns|MSysACEs|MSysObjects|MSysQueries
|MSysRelationships)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK
```

```
add appfw policy sqli_4 HTTP.REQ.BODY(10000).SET_TEXT_MODE(IGNORECASE).
SET_TEXT_MODE(URLENCODED).DECODE_USING_TEXT_MODE.REGEX_MATCH(re##((\\A
)|(?<=[^a-zA-Z0-9_]))(SYS\.USER_OBJECTS|SYS\.TAB|SYS\.USER_TABLES|SYS\.
USER_VIEWS|SYS\.ALL_TABLES|SYS\.USER_TAB_COLUMNS|SYS\.USER_CONSTRAINTS|SYS
\.USER_TRIGGERS|SYS\.USER_CATALOG|SYS\.ALL_CATALOG|SYS\.ALL_CONSTRAINTS|SYS
\.ALL_OBJECTS|SYS\.ALL_TAB_COLUMNS|SYS\.ALL_TAB_PRIVS|SYS\.ALL_TRIGGERS|SYS
\.ALL_USERS|SYS\.ALL_VIEWS|SYS\.USER_ROLE_PRIVS|SYS\.USER_SYS_PRIVS|SYS\.
USER_TAB_PRIVS)((Z)|(?=[^a-zA-Z0-9_]))##)APPFW_BLOCK
```

Überprüfen des Anwendungs- oder JSON-Inhaltstyps mit Signaturen

Sie können dem Signaturobjekt im Firewallprofil der Anwendung die folgenden Signaturregeln hinzufügen, um SQL-Injection für JSON-Inhaltstyp zu unterstützen.

> **Hinweis:**
>
> Post Body-Signaturen sind CPU-intensiv.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright 2013-2018 Citrix Systems, Inc. All rights reserved. -->
<SignaturesFile schema_version="6" version="0" minor_schema_version="0"
    >
     <Signatures>
         <SignatureRule id="4000000" enabled="ON" actions="log,block"
            category="sql" source="" severity="" type="" version="1"
            sourceid="" harmscore="">
             <PatternList>
                 <RequestPatterns>
                     <Pattern>
                         <Location area="HTTP_POST_BODY"/>
                         <Match type="Expression">TEXT.SET_TEXT_MODE(
                            IGNORECASE).SET_TEXT_MODE(URLENCODED).
                            DECODE_USING_TEXT_MODE.REGEX_MATCH(re#((((\A)
                            |(?<=[^a-zA-Z0-9_])))(select|insert|delete|
                            update|drop|create|alter|grant|revoke|commit
                            |rollback|shutdown|union|intersect|minus|
                            case|decode|where|group|begin|join|exists|
                            distinct|add|modify|constraint|null|like|
                            exec|execute|char|or|and|sp_sdidebug)((
Z)|(?=[^a-zA-Z0-9_]))#)</Match>
                     </Pattern>
                     <Pattern type="fastmatch">
                         <Location area="HTTP_METHOD"/>
                         <Match type="LITERAL">T</Match>
                     </Pattern>
                 </RequestPatterns>
             </PatternList>
             <LogString>sql Injection</LogString>
             <Comment/>
         </SignatureRule>
         <SignatureRule id="4000001" enabled="ON" actions="log,block"
            category="sql" source="" severity="" type="" version="1"
            sourceid="" harmscore="">
             <PatternList>
                 <RequestPatterns>
                     <Pattern>
                         <Location area="HTTP_POST_BODY"/>
```



```
                            <Match type="Expression">TEXT.SET_TEXT_MODE(
                                IGNORECASE).SET_TEXT_MODE(URLENCODED).
                                DECODE_USING_TEXT_MODE.REGEX_MATCH(re#((\A)
                                |(?<=[^a-zA-Z0-9_]))(xp_availablemedia|
                                xp_cmdshell|xp_deletemail|xp_dirtree|
                                xp_dropwebtask|xp_dsninfo|xp_enumdsn|
                                xp_enumerrorlogs|xp_enumgroups|
                                xp_enumqueuedtasks|xp_eventlog|
                                xp_findnextmsg|xp_fixeddrives|
                                xp_getfiledetails|xp_getnetname|
                                xp_grantlogin|xp_logevent|xp_loginconfig|
                                xp_logininfo|xp_makewebtask|xp_msver|
                                xp_regread|xp_perfend|xp_perfmonitor|
                                xp_perfsample|xp_perfstart|xp_readerrorlog|
                                xp_readmail|xp_revokelogin|xp_runwebtask|
                                xp_schedulersignal|xp_sendmail|
                                xp_servicecontrol|xp_snmp_getstate|
                                xp_snmp_raisetrap|xp_sprintf|xp_sqlinventory
                                |xp_sqlregister|xp_sqltrace|xp_sscanf|
                                xp_startmail|xp_stopmail|xp_subdirs|
                                xp_unc_to_drive)((
Z)|(?=[^a-zA-Z0-9_]))#)</Match>
                        </Pattern>
                        <Pattern type="fastmatch">
                            <Location area="HTTP_METHOD"/>
                            <Match type="LITERAL">T</Match>
                        </Pattern>
                    </RequestPatterns>
                </PatternList>
                <LogString>sql Injection</LogString>
                <Comment/>
            </SignatureRule>
            <SignatureRule id="4000002" enabled="ON" actions="log,block"
                category="sql" source="" severity="" type="" version="1"
                sourceid="" harmscore="">
                <PatternList>
                    <RequestPatterns>
                        <Pattern>
                            <Location area="HTTP_POST_BODY"/>
                            <Match type="Expression">TEXT.SET_TEXT_MODE(
                                IGNORECASE).SET_TEXT_MODE(URLENCODED).
                                DECODE_USING_TEXT_MODE.REGEX_MATCH(re#((\A)
                                |(?<=[^a-zA-Z0-9_]))(sysobjects|syscolumns|
                                MSysACEs|MSysObjects|MSysQueries|
                                MSysRelationships)((
```



```
Z)|(?=[^a-zA-Z0-9_]))#)</Match>
                    </Pattern>
                    <Pattern type="fastmatch">
                        <Location area="HTTP_METHOD"/>
                        <Match type="LITERAL">T</Match>
                    </Pattern>
                </RequestPatterns>
            </PatternList>
            <LogString>sql Injection</LogString>
            <Comment/>
        </SignatureRule>
        <SignatureRule id="4000003" enabled="ON" actions="log,block"
           category="sql" source="" severity="" type="" version="1"
           sourceid="" harmscore="">
            <PatternList>
                <RequestPatterns>
                    <Pattern>
                        <Location area="HTTP_POST_BODY"/>
                        <Match type="Expression">TEXT.SET_TEXT_MODE(
                           IGNORECASE).SET_TEXT_MODE(URLENCODED).
                           DECODE_USING_TEXT_MODE.REGEX_MATCH(re#((\A)
                           |(?<=[^a-zA-Z0-9_]))(SYS.USER_OBJECTS|SYS.
                           TAB|SYS.USER_TABLES|SYS.USER_VIEWS|SYS.
                           ALL_TABLES|SYS.USER_TAB_COLUMNS|SYS.
                           USER_CONSTRAINTS|SYS.USER_TRIGGERS|SYS.
                           USER_CATALOG|SYS.ALL_CATALOG|SYS.
                           ALL_CONSTRAINTS|SYS.ALL_OBJECTS|SYS.
                           ALL_TAB_COLUMNS|SYS.ALL_TAB_PRIVS|SYS.
                           ALL_TRIGGERS|SYS.ALL_USERS|SYS.ALL_VIEWS|SYS
                           .USER_ROLE_PRIVS|SYS.USER_SYS_PRIVS|SYS.
                           USER_TAB_PRIVS)((
Z)|(?=[^a-zA-Z0-9_]))#)</Match>
                    </Pattern>
                    <Pattern type="fastmatch">
                        <Location area="HTTP_METHOD"/>
                        <Match type="LITERAL">T</Match>
                    </Pattern>
                </RequestPatterns>
            </PatternList>
            <LogString>sql Injection</LogString>
            <Comment/>
        </SignatureRule>
    </Signatures>
</SignaturesFile>

```



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

Aktualisieren eines Signaturobjekts

October 5, 2021

Sie müssen Ihre Signaturobjekte regelmäßig aktualisieren, um sicherzustellen, dass Ihre Web App Firewall Schutz vor aktuellen Bedrohungen bietet. Sie müssen regelmäßig sowohl die standardmäßigen Web App Firewall -Signaturen als auch alle Signaturen aktualisieren, die Sie aus einem unterstützten Tool zum Scannen von Schwachstellen importieren.

Citrix aktualisiert regelmäßig die Standardsignaturen für die Web App Firewall. Sie können die Standardsignaturen manuell oder automatisch aktualisieren. Bitten Sie in beiden Fällen Ihren Citrix Vertreter oder Ihren Citrix Reseller nach der URL, um auf die Updates zuzugreifen. Sie können automatische Aktualisierungen der Signaturen des nativen Citrix Formats in den Dialogfeldern Moduleinstellungen und Einstellungen für automatische Signaturen aktivieren.

Die meisten Hersteller von Schwachstellen-Scan-Tools aktualisieren die Tools regelmäßig. Die meisten Websites ändern sich ebenfalls häufig. Sie müssen Ihr Tool aktualisieren und Ihre Websites regelmäßig erneut scannen, die resultierenden Signaturen in eine Datei exportieren und in Ihre Web App Firewall -Konfiguration importieren.

> **Tipp**
>
> Wenn Sie die Web App Firewall -Signaturen über die Citrix ADC Befehlszeile aktualisieren, müssen Sie zuerst die Standardsignaturen aktualisieren und dann weitere Update-Befehle ausführen, um jede benutzerdefinierte Signaturdatei zu aktualisieren, die auf den Standardsignaturen basiert. Wenn Sie die Standardsignaturen nicht zuerst aktualisieren, verhindert ein Versionsfehler die Aktualisierung der benutzerdefinierten Signaturdateien.
>
> **Hinweis:**
>
> Folgendes gilt für das Zusammenführen eines Signaturobjekts eines Drittanbieters mit einem benutzerdefinierten Signaturobjekt mit systemeigenen Regeln und benutzerdefinierten Regeln:
>
> Wenn Signaturen der Version 0 mit einer neuen importierten Datei zusammengeführt werden, bleiben die resultierenden Signaturen als Version 0 erhalten.
>
> Dies bedeutet, dass alle nativen (oder integrierten) Regeln in der importierten Datei nach dem Zusammenführen ignoriert werden. Dadurch wird sichergestellt, dass die Signaturen der Version 0 wie nach einer Zusammenführung beibehalten werden.
>
> Um die systemeigenen Regeln in die importierte Datei für die Zusammenführung aufzunehmen,

> müssen Sie die vorhandenen Signaturen erst vor dem Zusammenführen von Version 0 aktualisieren. Dies bedeutet, dass Sie die Art der Version 0 der vorhandenen Signaturen verlassen müssen.
>
> Wenn ein Citrix ADC Release-Upgrade durchgeführt wird, wird die Datei “default_signatures.xml” dem neuen Build hinzugefügt, und die Datei “updated_signature.xml” wird aus dem älteren Build entfernt. Wenn nach dem Upgrade die automatische Signaturaktualisierungsfunktion aktiviert ist, aktualisiert die Appliance die vorhandene Signatur auf die neueste Version des Builds und generiert die Datei “updated_signature.xml”.

So aktualisieren Sie die Web App Firewall -Signaturen aus der Quelle mit der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `update appfw signatures <name> [-mergedefault]`
- `save ns config`

Beispiel

Im folgenden Beispiel wird das Signatur-Objekt mit dem Namen MySignatures aus dem Standardsignaturobjekt aktualisiert, wobei neue Signaturen im Standardsignaturobjekt mit den vorhandenen Signaturen zusammengeführt werden. Dieser Befehl überschreibt keine vom Benutzer erstellten Signaturen oder Signaturen, die aus einer anderen Quelle importiert wurden, z. B. ein genehmigtes Tool zum Scannen von Schwachstellen.

```
update appfw signatures MySignatures -mergedefault
save ns config
<!--NeedCopy-->
```

Aktualisieren eines Signaturobjekts aus einer Citrix Formatdatei

Citrix aktualisiert regelmäßig die Signaturen für die Web App Firewall. Sie müssen die Signaturen in Ihrer Web App Firewall regelmäßig aktualisieren, um sicherzustellen, dass Ihre Web App Firewall die aktuellste Liste verwendet. Fragen Sie Ihren Citrix Vertreter oder Ihren Citrix Reseller nach der URL, um auf die Updates zuzugreifen.

So aktualisieren Sie ein Signaturobjekt aus einer Citrix Formatdatei mit der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `update appfw signatures <name> [-mergeDefault]`
- `save ns config`

So aktualisieren Sie ein Signaturobjekt aus einer Citrix Formatdatei mit der GUI

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Signaturen**.
2. Wählen Sie im Detailbereich das Signaturobjekt aus, das Sie aktualisieren möchten.
3. Wählen Sie in der Dropdownliste **Aktion** die Option **Zusammenführen** aus.
4. Wählen Sie im Dialogfeld **Signaturobjekt aktualisieren** eine der folgenden Optionen aus.
   - **Von URL importieren**— Wählen Sie diese Option, wenn Sie Signaturaktualisierungen von einer Web-URL herunterladen.
   - **Aus lokaler Datei importieren**— Wählen Sie diese Option, wenn Sie Signaturaktualisierungen aus einer Datei auf Ihrer lokalen Festplatte, Ihrer Netzwerkfestplatte oder einem anderen Speichergerät importieren.
5. Geben Sie im Textbereich den URL ein, oder geben Sie die lokale Datei ein, oder navigieren Sie zu der lokalen Datei.
6. Klicken Sie auf **Aktualisieren**. Die Aktualisierungsdatei wird importiert, und das Dialogfeld Signaturen aktualisieren ändert sich in ein Format, das fast identisch mit dem des Dialogfelds **Signaturobjekt ändern** ist. Im Dialogfeld **Signaturobjekt aktualisieren** werden alle Zweige mit neuen oder geänderten Signaturregeln, SQL-Injections- oder siteübergreifenden Skriptmustern und XPath-Injectionsmustern angezeigt, sofern vorhanden.
7. Überprüfen und konfigurieren Sie die neuen und geänderten Signaturen.
8. Wenn Sie fertig sind, klicken Sie auf **OK**, und klicken Sie dann auf **Schließen**.

Aktualisieren eines Signaturobjekts von einem unterstützten Tool zum Scannen von Schwachstellen

> **Hinweis:**
>
> Bevor Sie ein Signaturobjekt aus einer Datei aktualisieren, müssen Sie die Datei erstellen, indem Sie Signaturen aus dem Tool zum Scannen von Sicherheitslücken exportieren.

So importieren und aktualisieren Sie Signaturen von einem Tool zum Scannen von Schwachstellen

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Signaturen**.
2. Wählen Sie im Detailbereich das Signaturobjekt aus, das Sie aktualisieren möchten, und klicken Sie dann auf **Zusammenführen**.
3. Wählen **Sie im Dialogfeld Signaturobjekt aktualisieren** auf der Registerkarte **Externes Format** im Abschnitt Importieren eine der folgenden Optionen aus.

- **Von URL importieren**— Wählen Sie diese Option, wenn Sie Signaturaktualisierungen von einer Web-URL herunterladen.
- **Aus lokaler Datei importieren**— Wählen Sie diese Option, wenn Sie Signaturaktualisierungen aus einer Datei auf Ihrer lokalen oder einer Netzwerkfestplatte oder einem anderen Speichergerät importieren.

4. Geben Sie im Textbereich den URL ein, oder suchen Sie den Pfad zur lokalen Datei oder geben Sie ihn ein.
5. Wählen Sie im Abschnitt XSLT eine der folgenden Optionen aus.
   - **Integrierte XSLT-Datei verwenden**— Wählen Sie diese Option, wenn Sie eine integrierte XSLT-Datei verwenden möchten.
   - **Lokale XSLT-Datei verwenden**— Wählen Sie diese Option, um eine XSLT-Datei auf Ihrem lokalen Computer zu verwenden.
   - **XSLT von URL referenzieren**— Wählen Sie diese Option, um eine XSLT-Datei von einer Web-URL zu importieren.
6. Wenn Sie die Option Integrierte XSLT-Datei verwenden gewählt haben, wählen Sie in der Dropdownliste Integrierte XSLT die gewünschte Datei aus den folgenden Optionen aus:
   - **Cenzic.**
   - **Deep_Security_for_Web_Apps.**
   - **Hewlett_Packard_Enterprise_WebInspect.**
   - **IBM-AppScan-Enterprise.**
   - **IBM-AppScan-Standard.**
   - **Qualys.**
   - **Whitehat.**
7. Klicken Sie auf **Aktualisieren**. Die Update-Datei wird importiert, und das Dialogfeld Signaturen aktualisieren ändert sich in ein Format, das fast identisch mit dem des Dialogfelds Signatures-Objekt ändern ist, das unter Signatures-Objekt konfigurieren oder ändernbeschrieben wird. Im Dialogfeld **Signaturobjekt aktualisieren** werden alle Zweige mit neuen oder geänderten Signaturregeln, SQL-Injections- oder siteübergreifenden Skriptmustern und XPath-Injectionsmustern angezeigt, sofern vorhanden.
8. Überprüfen und konfigurieren Sie die neuen und geänderten Signaturen.
9. Wenn Sie fertig sind, klicken Sie auf **OK**, und klicken Sie dann auf **Schließen**.

Automatische Aktualisierung der Signatur

December 7, 2021

Die Funktion “Signature Auto Update” in der Web Application Firewall ermöglicht es dem Benutzer, die neuesten Signaturen zu erhalten, um die Webanwendung vor neuen Schwachstellen zu schützen. Die Funktion zur automatischen Aktualisierung bietet einen besseren Schutz, ohne dass ein fortlaufender

manueller Eingriff erforderlich ist, um die neuesten Updates zu erhalten.

Die Signaturen werden stündlich automatisch aktualisiert und müssen nicht regelmäßig auf die Verfügbarkeit des neuesten Updates überprüft werden. Sobald Sie das automatische Signatur-Update aktiviert haben, stellt die Citrix ADC-Appliance eine Verbindung mit dem Server her, der die Signaturen hostet, um zu prüfen, ob eine neuere Version verfügbar ist.

Anpassbarer Standort

Die neuesten Application Firewall-Signaturen werden auf Amazon gehostet, das als Standardsignatur-URL konfiguriert ist, um nach dem neuesten Update zu suchen.

Der Benutzer hat jedoch die Möglichkeit, diese Signaturzuordnungsdateien auf seinen internen Server herunterzuladen. Der Benutzer kann dann einen anderen Signatur-URL-Pfad konfigurieren, um die Signaturzuordnungsdateien von einem lokalen Server herunterzuladen. Damit die Funktion zur automatischen Aktualisierung funktioniert, müssen Sie möglicherweise den DNS-Server für den Zugriff auf die externe Site konfigurieren.

Signaturen aktualisieren

Alle benutzerdefinierten Signaturobjekte, die mit dem appfw-Standardsignaturobjekt erstellt werden, haben eine Version größer als Null. Wenn Sie das automatische Update der Signatur aktivieren, werden alle Signaturen automatisch aktualisiert.

Wenn der Benutzer Signaturen mit dem externen Format wie Cenzic oder Qualys importiert hat, werden die Signaturen mit der Version als Null importiert. Wenn der Benutzer ein Signaturobjekt mit der leeren Vorlage erstellt hat, wird es in ähnlicher Weise als Nullversionssignatur erstellt. Diese Signaturen werden nicht automatisch aktualisiert, da der Benutzer möglicherweise nicht an der Verwaltung der nicht verwendeten Standardsignaturen interessiert ist.

Die Web Application Firewall ermöglicht dem Benutzer jedoch auch die Flexibilität, diese Signaturen manuell auszuwählen und zu aktualisieren, um den vorhandenen Regeln die Standardsignaturregeln hinzuzufügen. Nachdem die Signaturen manuell aktualisiert wurden, ändert sich die Version und dann werden die Signaturen zusammen mit den anderen Signaturen automatisch aktualisiert.

Konfigurieren des automatischen Updates der Signatur

So konfigurieren Sie die Funktion zur automatischen Aktualisierung der Signatur mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

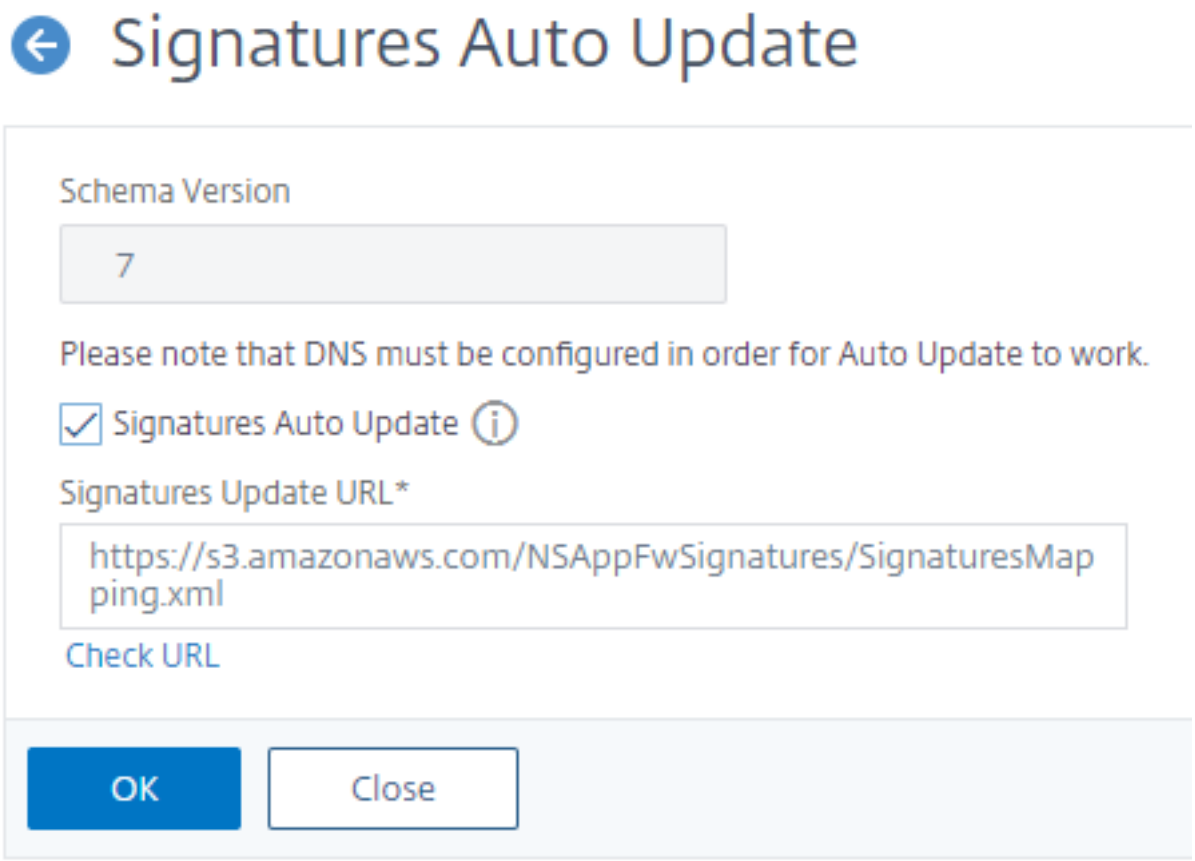
```
1 set appfw settings SignatureAutoUpdate on
```



```
2 set appfw settings SignatureUrl https://s3.amazonaws.com/
     NSAppFwSignatures/SignaturesMapping.xml
3 <!--NeedCopy-->
```

So konfigurieren Sie das automatische Update der Signatur mit der GUI:

1. Erweitern Sie den Sicherheitsknoten.
2. Erweitern Sie den Knoten Application Firewall.
3. Wählen Sie den Knoten Signaturen aus.
4. Wählen Sie unter **Aktion Einstellungen automatisch aktualisieren**aus.
5. Aktivieren Sie die Option " **Automatische Aktualisierung von Signaturen**".
6. Sie können bei Bedarf einen benutzerdefinierten Pfad für die Signaturaktualisierungs-URL angeben. Klicken Sie auf **Zurücksetzen**, um auf den Standard zurückzusetzen `s3.amazonaws.com server`.
7. Klicken Sie auf **OK**.



Signaturen manuell aktualisieren

Um eine Nullversionssignatur oder eine andere benutzerdefinierte Signatur manuell zu aktualisieren, müssen Sie zuerst das neueste Update für die Standardsignaturen erhalten und diese dann zum Aktu-

alisieren der benutzerdefinierten Zielsignatur verwenden.

Führen Sie die folgenden Befehle von der CLI aus, um eine Signaturdatei zu aktualisieren:

```
update appfw signatures "*Default Signatures"
update appfw signatures cenzic  - mergedefault
<!--NeedCopy-->
```

> **Hinweis:**
>
> `Default Signatures` Es wird Groß-/Kleinschreibung Cenzic im vorherigen Befehl ist der Name der Signaturdatei, die aktualisiert wird.

Importieren von Standardsignaturen ohne Internetzugang

Es wird empfohlen, einen Proxy-Server so zu konfigurieren, dass er auf den Amazon (AWS) -Server verweist, um das neueste Update zu erhalten. Wenn die NetScaler Appliance jedoch keine Internetverbindung zu den externen Sites hat, kann der Benutzer die aktualisierten Signaturdateien auf einem lokalen Server speichern. Die Appliance kann die Signaturen dann vom lokalen Server herunterladen. In diesem Szenario muss der Benutzer ständig die **Amazon-Website** überprüfen, um die neuesten Updates zu erhalten. Sie können die Signaturdatei mit der entsprechenden sha1-Datei herunterladen und überprüfen, die mit dem **öffentlichen Schlüssel von Citrix** zum Schutz vor Manipulationen erstellt wurde.

Führen Sie das folgende Verfahren aus, um die Signatures-Dateien auf einen lokalen Server zu kopieren:

1. Erstellen Sie ein lokales Verzeichnis wie <`MySignatures`> auf einem lokalen Server.
2. Öffnen Sie die AWS-Site.
3. Kopieren Sie die `SignaturesMapping.xml` Datei in den <`MySignatures`> Ordner.

Wenn Sie die `SignaturesMapping.xml` Datei öffnen, können Sie alle XML-Dateien für Signaturen und die entsprechenden sha1-Dateien für verschiedene unterstützte Versionen sehen. Ein solches Paar wird im folgenden Screenshot hervorgehoben:

1. Erstellen Sie ein Unterverzeichnis <`sigs`> im <`MySignatures`> Ordner.
2. Kopieren Sie alle Paare der `*.xml files listed in the` <`file`> Tags und die in den entsprechenden <`sha1`> Tags der `SignaturesMapping.xml` Datei aufgeführten `*.xml.sha1` Dateien in den <`sigs`> Ordner. Im Folgenden sind einige Beispieldateien aufgeführt, die in den <`sigs`> Ordner kopiert werden:

```
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b86v3s3.xml
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b86v3s3.xml.sha1
```


https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b0v3s2.xml
https://s3.amazonaws.com/NSAppFwSignatures/sigs/sig-r10.1b0v3s2.xml.sha1

> **Hinweis:**
>
> Sie können dem <MySignatures> Ordner einen beliebigen Namen geben und er kann sich an jedem Speicherort befinden, aber das Unterverzeichnis <sigs> muss ein Unterverzeichnis in dem <MySignatures> Ordner sein, in den die Zuordnungsdatei kopiert wird. Stellen Sie außerdem sicher, dass der Unterverzeichnisname, wie in der SignaturesMapping.xml gezeigt, den genauen Namen haben <sigs> muss und die Groß- und Kleinschreibung beachtet wird. Alle Signaturdateien und die entsprechenden sha1-Dateien sollten unter dieses <sigs> Verzeichnis kopiert werden.

Nachdem Sie den Inhalt vom gehosteten Amazon-Webserver auf den lokalen Server gespiegelt haben, ändern Sie den Pfad zum neuen lokalen Webserver, um ihn als signatureUrl für die automatische Aktualisierung festzulegen. Führen Sie beispielsweise den folgenden Befehl über die Befehlszeilenschnittstelle der Appliance aus:

```
1 set appfw settings SignatureUrl https://myserver.example.net/
     MySignatures/SignaturesMapping.xml
2 <!--NeedCopy-->
```

Der Update-Vorgang kann je nach Anzahl der zu aktualisierenden Signaturen mehrere Minuten dauern. Lassen Sie genügend Zeit, bis der Update-Vorgang abgeschlossen ist.

Wenn Sie auf einen Fehler stoßen “Fehler beim Zugriff auf URL! “Befolgen Sie während der Konfiguration die Schritte, um es zu beheben.

1. Fügen Sie die URL hinzu, https://myserver.example.net /netscaler/ns_gui/admin_ui/php/application/controllers/common/utils.php damit die Sicherheit der Inhaltssicherheitsrichtlinie (CSP) den URL-Zugriff nicht blockiert. Bitte beachten Sie, dass diese Einstellungen bei einem Upgrade nicht bestehen. Der Benutzer muss es nach dem Upgrade erneut hinzufügen.

```
1 $configuration_view_connect_src = ”connect-src 'self' https://app.pendo
     .io https://s3.amazonaws.comhttps://myserver.example.net;”;
2 <!--NeedCopy-->
```

1. Der Benutzer muss den Webserver https://myserver.example.net so konfigurieren, dass er auf die folgenden CORS-Header für reagiert https://myserver.example.net/MySignatures/SignaturesMapping.xml


```
Access-Control-Allow-Methods: GET
Access-Control-Allow-Origin: *
Access-Control-Max-Age: 3000
<!--NeedCopy-->
```

Richtlinien zum Aktualisieren von Signaturen

Beim Aktualisieren von Signaturen werden folgende Richtlinien verwendet:

- Die Signaturen werden aktualisiert, wenn die Signaturaktualisierungs-URL ein Signaturobjekt enthält, das dieselbe oder neuere Version hat.
- Jede Signaturregel ist mit einer Regel-ID und einer Versionsnummer verknüpft. Beispiel: <SignatureRule id=”803”version=”16”···>
- Die Signaturregel aus der eingehenden Signature-Datei mit derselben ID und Versionsnummer wie die vorhandene wird ignoriert, auch wenn sie unterschiedliche Muster oder Protokollzeichenfolgen hat.
- Eine Signaturregel mit einer neuen ID wird hinzugefügt. Alle Aktionen und aktiviertes Flag werden aus der neuen Datei verwendet.

  > **Hinweis:**
  >
  > Möglicherweise müssen Sie die aktualisierten Signaturen immer noch regelmäßig überprüfen, um diese neu hinzugefügten Regeln zu aktivieren und andere Aktionseinstellungen gemäß den Anforderungen der Anwendung zu ändern.

- Regeln mit derselben ID, aber mit einer neueren Versionsnummer ersetzen die vorhandene. Alle Aktionen und aktiviertes Flag aus der vorhandenen Regel bleiben erhalten.

> **Tipp:**
>
> Wenn Sie die Signaturen von der CLI aus aktualisieren, müssen Sie zuerst die Standardsignaturen aktualisieren. Sie müssen dann Aktualisierungsbefehle hinzufügen, um jede benutzerdefinierte Signaturdatei zu aktualisieren, die auf den Standardsignaturen basiert. Wenn Sie die Standardsignaturen nicht zuerst aktualisieren, verhindert ein Fehler bei der Nichtübereinstimmung der Version die Aktualisierung der Datei benutzerdefinierter Signaturen.

Integration von SNORT-Regeln

October 5, 2021

Bei bösartigen Angriffen auf Webanwendungen ist es wichtig, Ihr internes Netzwerk zu schützen. Bösartige Daten beeinflussen nicht nur Ihre Webanwendungen auf der Ebene der Benutzeroberfläche, sondern auch bösartige Pakete erreichen die Anwendungsschicht. Um solche Angriffe zu überwinden, ist es wichtig, ein Intrusion Detection and Prevention System zu konfigurieren, das Ihr internes Netzwerk untersucht.

Snort-Regeln sind in die Appliance integriert, um bösartige Angriffe in Datenpaketen in der Anwendungsschicht zu untersuchen. Sie können die Snort-Regeln herunterladen und in WAF-Signaturen-Regeln konvertieren. Die Signaturen verfügen über eine regelbasierte Konfiguration, die bösartige Aktivitäten wie DOS-Angriffe, Pufferüberläufe, Stealth-Port-Scans, CGI-Angriffe, SMB-Probes und Betriebssystem-Fingerprinting-Versuche erkennen kann. Durch die Integration von Snort-Regeln können Sie Ihre Sicherheitslösung auf der Schnittstelle und in der Anwendungsschicht stärken.

SNORT-Regeln konfigurieren

Die Konfiguration beginnt mit dem Herunterladen der Snort-Regeln und dem Import in WAF-Signaturregeln. Nachdem Sie die Regeln in WAF-Signaturen konvertiert haben, können die Regeln als WAF-Sicherheitsprüfungen verwendet werden. Die Snort-basierten Signaturregeln untersuchen das eingehende Datenpaket, um zu erkennen, ob es bösartige Angriffe in Ihrem Netzwerk gibt.

Ein neuer Parameter, “VendorType”, wird dem Importbefehl hinzugefügt, um Snort-Regeln in WAF-Signaturen zu konvertieren.

Der Parameter “VendorType” wird auf SNORT nur für Snort Regeln gesetzt.

Downloaden Sie snort-Regeln mithilfe der Befehlszeilenschnittstelle

Sie können die Snort Regeln als Textdatei von der folgenden URL herunterladen:

```
https://www.snort.org/downloads/community/snort3-community-rules.tar.gz
```

Importieren von Snort-Regeln mithilfe der Befehlszeilenschnittstelle

Nach dem Herunterladen können Sie die Snort-Regeln in Ihre Appliance importieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import appfw signatures <src> <name> [-xslt <string>] [-comment <string>]
[-overwrite] [-merge [-preservedefactions]] [-sha1 <string>] [-VendorType
Snort]
```

Beispiel:

```
import appfw signatures http://www.example.com/ns/signatures.xml sig-snort -
comment “signatures from snort rules” -VendorType snort
```


Argumente:

Src. URL (Protokoll, Host, Pfad und Dateiname) für den Speicherort, an dem das importierte Signaturenobjekt gespeichert werden soll.

> **Hinweis:**
>
> Der Import schlägt fehl, wenn sich das zu importierende Objekt auf einem HTTPS-Server befindet, der Clientzertifikatauthentifizierung für den Zugriff erfordert. Obligatorisches Argument der maximalen Länge: 2047

Name. Name, der dem Signaturenobjekt im Citrix ADC zugewiesen werden soll. Obligatorisches Argument der maximalen Länge: 31

Kommentieren. Beschreibung, wie Informationen über das Signaturen-Objekt beibehalten werden. Maximale Länge: 255
überschreiben. Überschreiben Sie alle vorhandenen Signaturen Objekte mit dem gleichen Namen.

Verschmelzen. Führt vorhandene Signatur mit neuen Signaturregeln zusammen.

Konservierungsfraktionen. Behält def Aktionen von Signaturregeln bei.

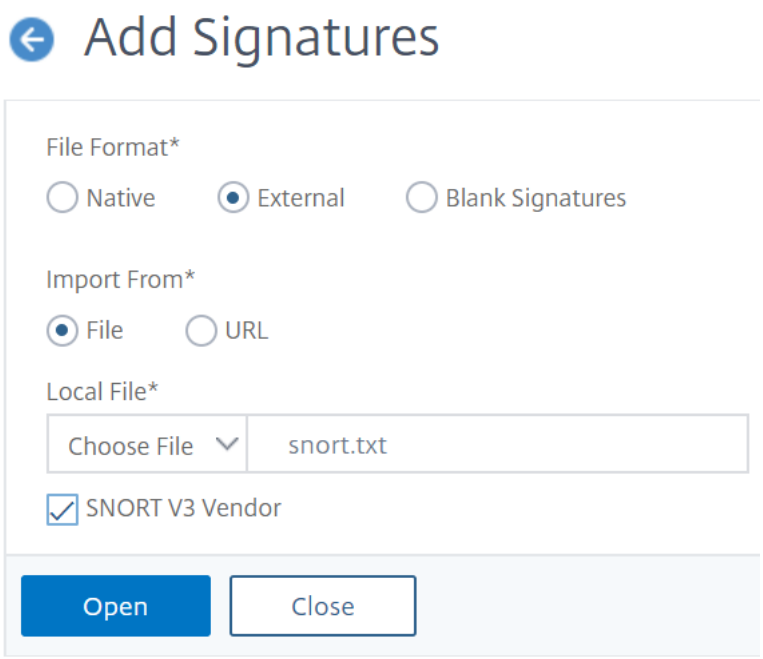
VendorType. Drittanbieter, um die WAF-Signaturen zu generieren. Mögliche Werte: Snort.

Konfigurieren von Snort-Regeln über die Citrix ADC GUI

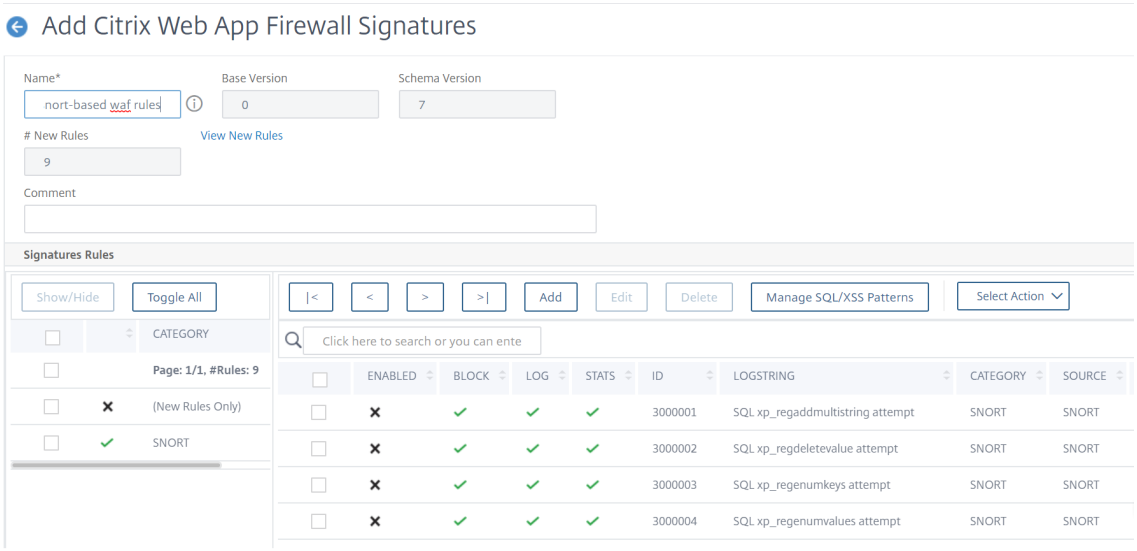
Die GUI-Konfiguration für Snort-Regeln ähnelt der Konfiguration anderer externer Webanwendungsscanner wie Cenzic, Qualys, Whitehat.

Führen Sie die folgenden Schritte aus, um Snort zu konfigurieren:

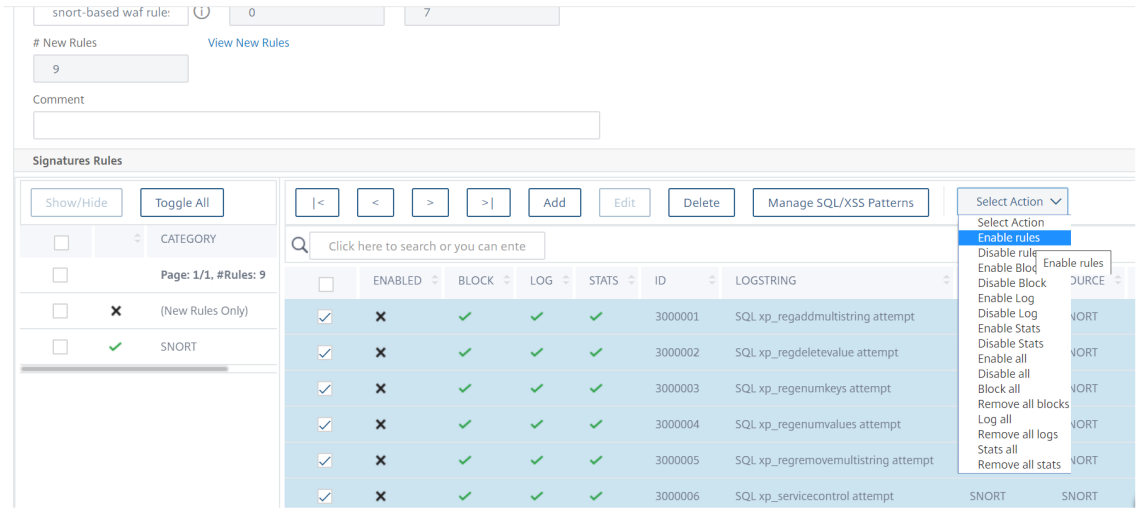
1. Navigieren Sie zu **Konfiguration > Sicherheit > Citrix Web App Firewall > Signaturen**.
2. Klicken Sie auf der Seite **Signaturen** auf **Hinzufügen**.
3. Legen **Sie auf der Seite Signaturen hinzufügen** die folgenden Parameter fest, um Snort-Regeln zu konfigurieren.
    a) Dateiformat. Wählen Sie das Dateiformat als extern aus.
    b) Importieren von. Wählen Sie die Importoption als snort Datei oder URL aus, um die URL einzugeben.
    c) Snort V3 Anbieter. Aktivieren Sie das Kontrollkästchen, um Snort-Regeln aus einer Datei oder aus einer URL zu importieren.
4. Klicken Sie auf **Öffnen**.



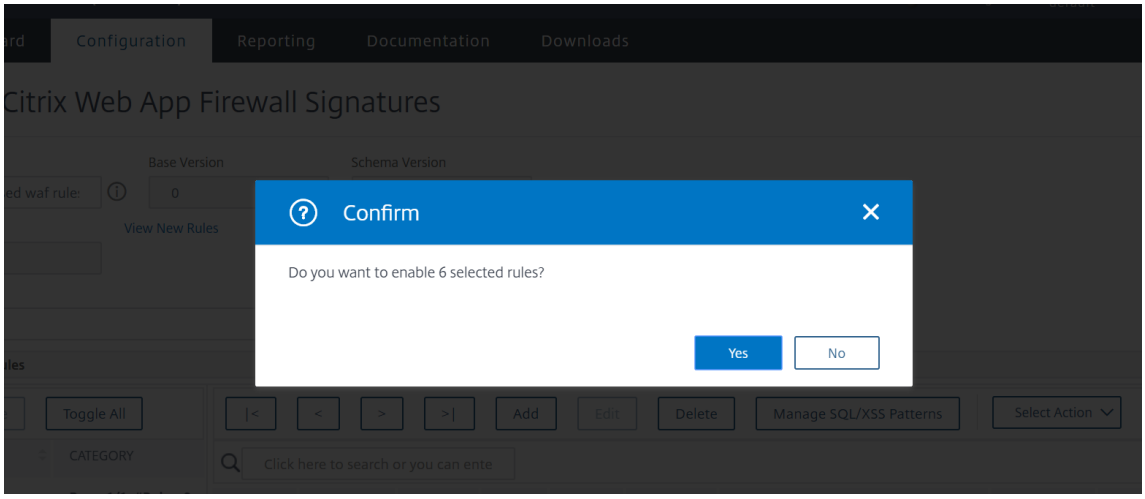
Die Appliance importiert die Snort-Regeln als Snort-basierte WAF-Signaturregeln.



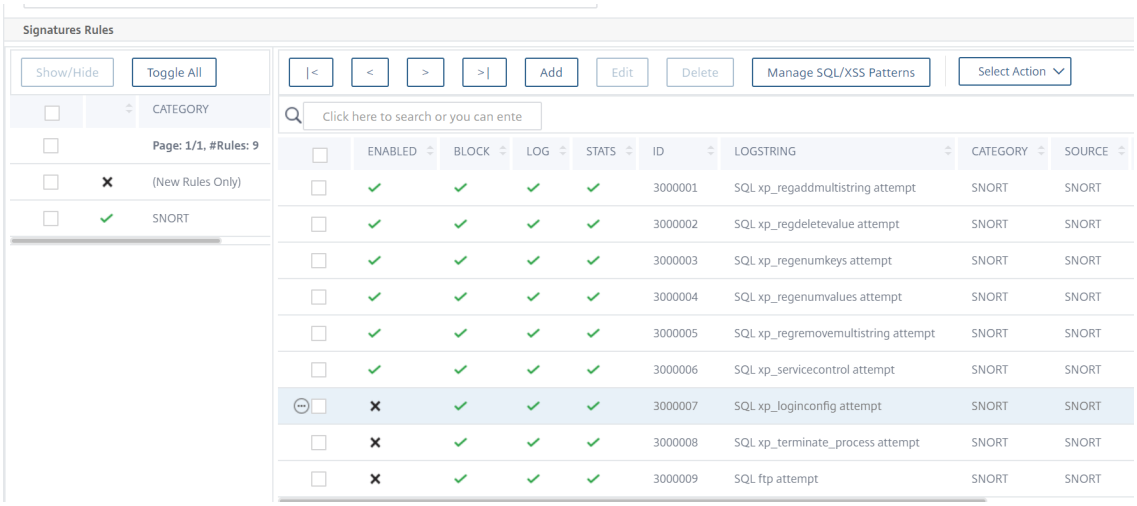
Als bewährte Methode müssen Sie Filteraktionen verwenden, um Snort-Regeln zu aktivieren, die Sie als WAF-Signaturregeln auf der Appliance importieren möchten.



5. Klicken Sie zur Bestätigung auf **Ja**.



6. Die ausgewählten Regeln sind auf der Appliance aktiviert.



7. Klicken Sie auf **OK**.

Exportieren eines Signaturobjekts in eine Datei

October 5, 2021

Sie exportieren ein Signaturobjekt in eine Datei, damit Sie es in einen anderen Citrix ADC importieren können.

So exportieren Sie ein Signaturobjekt in eine Datei

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Signaturen**.
2. Wählen Sie im Detailbereich das Signaturobjekt aus, das Sie konfigurieren möchten.
3. Wählen Sie in der Dropdownliste **Aktionen** die Option **Exportieren** aus.
4. Geben Sie im Dialogfeld **Signaturobjekt exportieren** im Textfeld **Lokale Datei** den Pfad und den Namen der Datei ein, in die Sie das Signaturobjekt exportieren möchten, oder verwenden **Sie das Dialogfeld Durchsuchen**, um einen Pfad und einen Namen festzulegen.
5. Klicken Sie auf **OK**.

Signaturen-Editor

October 5, 2021

Sie können den Signatur-Editor verwenden, um eine benutzerdefinierte (lokale) Signaturregel zu einem vorhandenen Signaturobjekt hinzuzufügen oder zu ändern. Eine lokale Signaturregel hat dieselben Attribute wie eine Standardsignaturregel von Citrix und funktioniert auf die gleiche Weise. Sie aktivieren oder deaktivieren es und konfigurieren die Signaturaktionen dafür, genau wie bei einer Standardsignatur.

Fügen Sie eine lokale Regel hinzu, wenn Sie Ihre Websites und Dienste vor einem bekannten Angriff schützen müssen, bei dem die vorhandenen Signaturen nicht übereinstimmen. Beispielsweise können Sie eine neue Art von Angriff entdecken und deren Eigenschaften bestimmen, indem Sie die Protokolle auf Ihrem Webserver überprüfen, oder Sie erhalten Informationen von Drittanbietern über eine neue Art von Angriff.

Im Mittelpunkt einer Signaturregel stehen die *Regelmuster*, die gemeinsam die Eigenschaften des Angriffs beschreiben, auf den die Regel abgestimmt ist. Jedes Muster kann aus einer einfachen Zeichenfolge, einem regulären PCRE-Ausdruck oder den integrierten SQL-Injections- oder siteübergreifenden Skriptmustern bestehen.

Sie können eine Signaturregel ändern, indem Sie ein neues Muster hinzufügen oder ein vorhandenes Muster entsprechend einem Angriff ändern. Beispielsweise können Sie sich über Änderungen an

einem Angriff informieren oder ein besseres Muster ermitteln, indem Sie die Protokolle auf Ihrem Webserver oder Informationen von Drittanbietern untersuchen.

So fügen Sie eine lokale Signaturregel mithilfe des Signatur-Editors hinzu oder ändern Sie sie

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Signaturen**.
2. Wählen Sie im Detailbereich das Signaturobjekt aus, das Sie bearbeiten möchten, und klicken Sie dann auf **Öffnen**.
3. Führen **Sie im Dialogfeld Signaturobjekt ändern** in der Mitte des Bildschirms unterhalb des Fensters **Gefilterte Ergebnisse** eine der folgenden Aktionen aus:
   - Klicken Sie auf Hinzufügen, um eine neue lokale Signaturregel hinzuzufügen.
   - Um eine vorhandene lokale Signaturregel zu ändern, wählen Sie diese Regel aus, und klicken Sie dann auf **Öffnen**.
4. Konfigurieren **Sie im Dialogfeld Lokale Signaturregel hinzufügen** oder im Dialogfeld **Lokale Signaturregel ändern** die Aktionen für eine Signatur, indem Sie die entsprechenden Kontrollkästchen aktivieren.
   - **Aktiviert.** Aktiviert die neue Signaturregel. Wenn Sie dies nicht auswählen, wird diese neue Signaturregel Ihrer Konfiguration hinzugefügt, ist jedoch inaktiv.
   - **Blockieren** Blockiert Verbindungen, die gegen diese Signaturregel verstoßen.
   - **Melden Sie sich** Protokolliert Verletzungen dieser Signaturregel im Citrix ADC Protokoll.
   - **Stat.** Schließt Verstöße gegen diese Signaturregel in die Statistiken ein.
   - **Remove.** Strikt Informationen, die mit der Signaturregel übereinstimmen, aus der Antwort. (Gilt nur für Antwortregeln.)
   - **X-Out.** Maskiert Informationen, die der Signaturregel entsprechen, mit dem Buchstaben X. (Gilt nur für Antwortregeln.)
   - **Duplikate zulassen.** Ermöglicht Duplikate dieser Signaturregel in diesem Signaturobjekt.
5. Wählen Sie in der Dropdownliste Kategorie eine **Kategorie** für die neue Signaturregel aus.

   Sie können eine Kategorie auch erstellen, indem Sie auf das Symbol rechts neben der Liste klicken und das Dialogfeld Signaturregelkategorie hinzufügen verwenden, um der Liste eine neue Kategorie hinzuzufügen. Die Regel, die Sie ändern, wird automatisch der neuen Kategorie hinzugefügt. Anweisungen finden Sie unter So fügen Sie eine Signaturregelkategoriehinzu.
6. Geben Sie im Textfeld **LogString** eine kurze Beschreibung der Signaturregel ein, die in den Protokollen verwendet werden soll.
7. Geben Sie im Textfeld **Kommentar** einen Kommentar ein. Optional:
8. Klicken Sie auf Mehr…, und ändern Sie die erweiterten Optionen.

a) Um HTML-Kommentare zu entfernen, bevor diese Signaturregel angewendet wird, wählen Sie in der Dropdownliste Kommentare entfernen die Option Alle oder Skript-Tag ausschließen.
b) Um die Überprüfung des CSRF-Referer-Headers festzulegen, wählen Sie im Optionsfeld Überprüfung des Optionsfeldes CSRF-Referrer-Header entweder das Optionsfeld Wenn vorhanden oder Immer aus.
c) Um die Regelkennung, die dieser lokalen Signaturregel zugewiesen ist, manuell zu ändern, ändern Sie die Nummer im Textfeld Regelkennung. Die ID muss eine positive Ganzzahl zwischen 1000000 und 1999999 sein, die noch keiner lokalen Signaturregel zugewiesen wurde.
d) Um der neuen Signaturregel eine Versionsnummer zuzuweisen, ändern Sie die Nummer im Textfeld Versionsnummer.
e) Um eine Quell-ID zuzuweisen, ändern Sie die Zeichenfolge im Textfeld Quell-ID.
f) Um die Quelle anzugeben, wählen Sie Lokal oder Snort aus der Dropdownliste Quelle, oder klicken Sie rechts neben der Liste auf das Symbol Hinzufügen, und fügen Sie eine neue Quelle hinzu.
g) Um Verstößen gegen diese lokale Signaturregel eine Schadensbewertung zuzuweisen, geben Sie eine Zahl zwischen 1 und 10 in das Textfeld Schadensbewertung ein.
h) Um dieser lokalen Signaturregel eine Bewertung des Schweregrads zuzuweisen, wählen Sie in der Dropdownliste Schweregrad die Option Hoch, Mittel oder Niedrig, oder klicken Sie auf das Symbol Hinzufügen rechts neben der Liste, und fügen Sie eine neue Schweregradbewertung hinzu.
i) Um dieser lokalen Signaturregel einen Verstoßtyp zuzuweisen, wählen Sie in der Dropdownliste Typ die Option Anfällig oder Warnung aus, oder klicken Sie rechts neben der Liste auf das Symbol Hinzufügen, und fügen Sie einen neuen Verletzungstyp hinzu.

9. Fügen Sie in der Liste **Muster** ein Muster hinzu oder bearbeiten Sie es.

   - Um ein Muster hinzuzufügen, klicken Sie auf **Hinzufügen**. Fügen **Sie im Dialogfeld Neues Signaturregelmuster erstellen** ein oder mehrere Muster für Ihre Signaturregel hinzu, und klicken Sie dann auf **OK** .
   - Um ein Muster zu bearbeiten, wählen Sie das Muster aus, und klicken Sie dann auf **Öffnen**. Ändern **Sie im Dialogfeld Signaturregelmuster bearbeiten** das Muster, und klicken Sie dann auf **OK** .

   Weitere Informationen zum Hinzufügen oder Bearbeiten von Mustern finden Sie unter Signaturregelmuster.

10. Klicken Sie auf **OK**.

So fügen Sie eine Signaturregelkategorie hinzu

October 5, 2021

Wenn Sie Signaturregeln in eine Kategorie einfügen, können Sie die Aktionen für eine Gruppe von Signaturen anstelle für jede einzelne Signatur konfigurieren. Möglicherweise möchten Sie dies aus folgenden Gründen tun:

- **Einfache Auswahl.** Angenommen, alle Signaturregeln in einer bestimmten Gruppe schützen vor Angriffen auf eine bestimmte Art von Webserver-Software oder -technologie. Wenn Ihre geschützten Websites diese Software oder Technologie verwenden, möchten Sie sie alle aktivieren. Wenn dies nicht der Fall ist, möchten Sie keine von ihnen aktivieren.
- **Einfache Erstkonfiguration.** Es ist am einfachsten, Standardwerte für eine Gruppe von Signaturen als Kategorie festzulegen, statt einzeln. Anschließend können Sie bei Bedarf Änderungen an einzelnen Signaturen vornehmen.
- **Einfache laufende Konfiguration.** Es ist einfacher, Signaturen zu konfigurieren, wenn Sie nur solche anzeigen können, die bestimmte Kriterien erfüllen, z. B. die Zugehörigkeit zu einer bestimmten Kategorie.

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Signaturen**.
2. Wählen Sie im Detailbereich das Signaturobjekt aus, das Sie konfigurieren möchten, und klicken Sie dann auf **Öffnen**.
3. Klicken **Sie im Dialogfeld Signaturobjekt ändern** in der Mitte des Bildschirms unterhalb des Fensters **Gefilterte Ergebnisse** auf **Hinzufügen** .
4. Klicken **Sie im Dialogfeld Lokale Signaturregel hinzufügen** auf das Symbol rechts neben der Dropdownliste Kategorie.
5. **Geben Sie im Dialogfeld Signaturregelkategorie hinzufügen** im Textfeld **Neue Kategorie** einen Namen für die neue Signaturkategorie ein. Der Name kann aus einem bis 64 Zeichen bestehen.
6. Klicken Sie auf **OK**.

Signaturregelmuster

October 5, 2021

Sie können ein Muster hinzufügen oder ein vorhandenes Muster ändern, um eine Zeichenfolge oder einen Ausdruck anzugeben, der einen Angriff kennzeichnet, wenn die Signatur übereinstimmt. Um die Muster eines Angriffs zu erkennen, können Sie die Protokolle auf Ihrem Webserver untersuchen. Sie können ein Tool verwenden, um Verbindungsdaten in Echtzeit zu beobachten oder die Zeichenfolge oder den Ausdruck aus einem Bericht eines Drittanbieters über den Angriff zu erhalten.

> **Achtung:**
>
> Jedes neue Muster, das Sie einer Signaturregel hinzufügen, befindet sich in einer UND- Beziehung zu den vorhandenen Mustern. Fügen Sie einer vorhandenen Signaturregel kein Muster hinzu, wenn Sie nicht möchten, dass ein potenzieller Angriff mit allen Mustern übereinstimmen muss, um der Signatur zu entsprechen.

Jedes Muster kann aus einer einfachen Zeichenfolge, einem regulären PCRE-Ausdruck oder dem integrierten SQL-Einschleusungs- oder siteübergreifenden Skriptmuster bestehen. Bevor Sie versuchen, ein Muster hinzuzufügen, das auf einem regulären Ausdruck basiert, müssen Sie sicherstellen, dass Sie reguläre Ausdrücke im PCRE-Format verstehen. PCRE-Ausdrücke sind komplex und leistungsstark. Wenn Sie nicht verstehen, wie sie funktionieren, können Sie versehentlich ein Muster erstellen, das zu etwas passt, das Sie nicht wollten (ein *falsches Positiv*) oder das nicht mit etwas übereinstimmt, das Sie wollten (ein *falsches Negativ*).

Benutzerdefiniertes Signaturmuster für nicht standardmäßige Inhaltstypen

Die Citrix ADC Web App Firewall (WAF) unterstützt jetzt neuen Speicherort zum Überprüfen kanonisierter Inhalte. Standardmäßig blockiert WAF kodierte Nutzlast nicht mit nicht standardmäßigen Inhaltstypen. Wenn diese Inhaltstypen auf der Positivliste sind und keine konfigurierte Aktion angewendet wird, filtern die SQL- und Cross-Site-Skriptschutzprüfung keine SQL- oder Cross-Site-Scripting-Angriffe in den codierten Nutzlasten. Um das Problem zu beheben, kann ein Benutzer eine benutzerdefinierte Signaturregel an diesem neuen Speicherort (HTTP_CANON_POST_BODY) erstellen, die die codierten Nutzlasten auf nicht standardmäßige Inhaltstypen untersucht. Wenn ein SQL- oder Cross-Site-Scripting-Angriff auftritt, blockiert er den Datenverkehr nach der Kanonisierung des Postkörpers.

> **Hinweis:**
>
> Diese Unterstützung gilt nur für HTTP-Anfragen.

Wenn Sie mit regulären Ausdrücken im PCRE-Format noch nicht vertraut sind, können Sie die folgenden Ressourcen verwenden, um die Grundlagen zu lernen, oder um Hilfe zu einem bestimmten Problem zu erhalten:

- “Reguläre Ausdrücke beherrschen”, Dritte Ausgabe. Copyright (c) 2006 von Jeffrey Friedl. O’Reilly Media, ISBN: 9780596528126.
- Reguläre Ausdrücke Kochbuch. Copyright (c) 2009 von Jan Goyvaerts und Steven Levithan. O’Reilly Media, ISBN: 9780596520687
- **PCRE Man Seite/Spezifikation** (text/offiziell):http://www.pcre.org/pcre.txt
- **PCRE Man Page/Spezifikation**

http://www.gammon.com.au/pcre/index.html

- **Wikipedia-PCRE-Eintrag**: http://en.wikipedia.org/wiki/PCRE
- **PCRE-Mailingliste**
  PCRE-Dev - PCRE-Entwicklung

Wenn Sie Nicht-ASCII-Zeichen in einem regulären Ausdruck des PCRE-Formats kodieren müssen, unterstützt die Citrix ADC Plattform die Kodierung von hexadezimalen UTF-8-Codes. Weitere Informationen finden Sie unter PCRE-Zeichenkodierungsformat.

So konfigurieren Sie ein Signaturregelmuster

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Signaturen**.
2. Wählen Sie im Detailbereich das Signaturobjekt aus, das Sie konfigurieren möchten, und klicken Sie dann auf **Öffnen**.
3. Klicken **Sie im Dialogfeld Signaturobjekt ändern** in der Mitte des Bildschirms unterhalb des Fensters **Gefilterte Ergebnisse** entweder auf **Hinzufügen**, um eine Signaturregel zu erstellen, oder wählen Sie eine vorhandene Signaturregel aus, und klicken Sie auf **Öffnen** .

   > **Hinweis:**
   >
   > Sie können nur Signaturregeln ändern, die Sie hinzugefügt haben. Sie können die Standardsignaturregeln nicht ändern.

   Je nach Aktion wird entweder das Dialogfeld Lokale Signaturregel hinzufügen oder das Dialogfeld Lokale Signaturregel ändern angezeigt. Beide Dialogfelder haben denselben Inhalt.
4. Klicken Sie im Dialogfeld im **Fenster Muster** auf **Hinzufügen**, um ein neues Muster hinzuzufügen, oder wählen Sie ein vorhandenes Muster aus der Liste unter der Schaltfläche **Hinzufügen** aus, und klicken Sie auf **Öffnen** . Abhängig von Ihrer Aktion wird entweder das Dialogfeld **Neues Signaturregelmuster erstellen** oder das Dialogfeld **Signaturregelmuster bearbeiten** angezeigt. Beide Dialogfelder haben denselben Inhalt.
5. Wählen Sie in der Dropdownliste **Mustertyp** den Verbindungstyp aus, mit dem das Muster übereinstimmen soll.
   - Wenn das Muster Anforderungselemente oder -features wie injiziertem SQL-Code, Angriffe auf Webformulare, siteübergreifende Skripts oder unangemessene URLs übereinstimmen soll, wählen Sie **Anforderung**.
   - Wenn das Muster darauf abzielt, Antwortelemente oder -funktionen wie Kreditkartennummern oder sichere Objekte abzugleichen, wählen Sie **Antwort**.
6. Definieren Sie im Bereich Position die Elemente, die mit diesem Muster untersucht werden sollen.
   Der Bereich Speicherort beschreibt, welche Elemente der HTTP-Anforderung oder -Antwort auf dieses Muster untersucht werden sollen. Welche Auswahlmöglichkeiten im Bereich Position

angezeigt werden, hängt vom gewählten Mustertyp ab. Wenn Sie “Anforderung” als Mustertyp gewählt haben, werden Elemente angezeigt, die für HTTP-Anforderungen relevant sind. Wenn Sie “Antwort” gewählt haben, werden Elemente angezeigt, die für HTTP-Antworten relevant sind.
Wenn Sie außerdem einen Wert aus der Dropdownliste Fläche auswählen, ändern sich die übrigen Teile des Standortbereichs interaktiv. Im Folgenden finden Sie alle Konfigurationselemente, die in diesem Abschnitt angezeigt werden können.

- Bereich. Dropdownliste mit Elementen, die einen bestimmten Teil der HTTP-Verbindung beschreiben. Folgende Möglichkeiten stehen zur Auswahl:
  - **HTTP_ANY**. Alle Teile der HTTP-Verbindung.
  - **HTTP_COOKIE**. Alle Cookies in den HTTP-Request-Headern nach irgendwelchen Cookie-Transformationen durchgeführt werden.
    Hinweis: Sucht keine HTTP-Antwort Set-Cookie: Header.
  - **HTTP_FORM_FIELD**. Formularfelder und deren Inhalt, nach URL-Dekodierung, Prozentdekodierung und Entfernung von überschüssigen Leerzeichen. Mit dem< `Location`> Tag können Sie die Liste der zu durchsuchenden Formularfeldnamen weiter einschränken.
  - **HTTP_HEADER**. Die Werteteile des HTTP-Headers nach allen Cross-Site-Skript- oder URL-Dekodierungs-Transformationen.
  - **HTTP_METHOD**. Die HTTP-Anforderungsmethode.
  - **HTTP_ORIGIN_URL**. Die Ursprungs-URL eines Webformulars.
  - **HTTP_POST_BODY**. Der HTTP-Posttext und die darin enthaltenen Webformulardaten.
  - **HTTP_RAW_COOKIE**. Alle HTTP-Anforderungscookie, einschließlich des Namensbereichs Cookie:.
    Hinweis: Sucht keine HTTP-Antwort Set-Cookie: Header.
  - **HTTP_RAW_HEADER**. Der gesamte HTTP-Header mit einzelnen Headern, die durch Zeilenvorschubzeichen (n) oder Wagenrücklauf-/Zeilenvorschubzeichenfolgen (rn) getrennt sind.
  - **HTTP_RAW_RESP_HEADER**. Der gesamte Antwortheader, einschließlich der Namens- und Werteteile des Antwortheaders nach Abschluss der URL-Transformation und des vollständigen Antwortstatus. Wie bei HTTP_RAW_HEADER werden einzelne Header durch Zeilenvorschubzeichen (n) oder Wagenrücklauf-/Zeilenvorschubzeichenfolgen (rn) getrennt.
  - **HTTP_RAW_SET_COOKIE**. Der gesamte Set-Cookie-Header, nachdem URL-Transformationen durchgeführt wurden
    Hinweis: URL-Transformation kann sowohl die Domäne als auch den Pfadbereich des Set-Cookie-Headers ändern.
  - **HTTP_RAW_URL**. Die gesamte Anforderungs-URL, bevor URL-Transformationen

durchgeführt werden, einschließlich aller Abfrage- oder Fragmentteile.
- **HTTP_RESP_HEADER**. Der Werteteil der vollständigen Antwort-Header, nachdem URL-Transformationen durchgeführt wurden.
- **HTTP_RESP_BODY**. Der HTTP-Antworttext
- **HTTP_SET_COOKIE**. Alle Set-Cookie -Header in den HTTP-Antwort-Headern.
- **HTTP_STATUS_CODE**. Der HTTP-Statuscode.
- **HTTP_STATUS_MESSAGE**. Die HTTP-Statusmeldung.
- **HTTP_URL**. Der Werteteil der URL in den HTTP-Headern, ausgenommen alle Abfrage- oder Fragmentports, nach der Konvertierung in den UTF-*-Zeichensatz, URL-Dekodierung, Strippen von Leerzeichen und Konvertierung relativer URLs in absolute. Enthält keine HTML-Entity-Dekodierung.
- -URL. Untersucht alle URLs, die in den durch die Einstellung
  Bereich angegebenen Elementen gefunden wurden. Wählen Sie eine der folgenden Einstellungen aus.
- **Any.** Überprüft alle URLs.
- Literal. Überprüft URLs, die eine Literalzeichenfolge enthalten. Nachdem Sie Literal ausgewählt haben, wird ein Textfeld angezeigt. Geben Sie die gewünschte Literalzeichenfolge in das Textfeld ein.
- PCRE. Überprüft URLs, die einem regulären Ausdruck im PCRE-Format entsprechen. Nachdem Sie diese Auswahl ausgewählt haben, wird das Fenster für reguläre Ausdrücke angezeigt. Geben Sie den regulären Ausdruck in das Fenster ein. Sie können die **Regex-Token** verwenden, um allgemeine reguläre Ausdruckselemente am Cursor einzufügen, oder Sie können auf Regex-Editor klicken, um das Dialogfeld Editor für Reguläre Ausdrücke anzuzeigen, das mehr Unterstützung beim Erstellen des gewünschten regulären Ausdrucks bietet.
- Ausdruck. Überprüft URLs, die mit einem Citrix ADC Standardausdruck übereinstimmen.
- Feldname. Untersucht alle Formularfeldnamen, die in den durch die Auswahl
  Bereich angegebenen Elementen gefunden werden. **Any.** Überprüft alle URLs.
- Literal. Überprüft URLs, die eine Literalzeichenfolge enthalten. Nachdem Sie Literal ausgewählt haben, wird ein Textfeld angezeigt. Geben Sie die gewünschte Literalzeichenfolge in das Textfeld ein.
- PCRE. Überprüft URLs, die einem regulären Ausdruck im PCRE-Format entsprechen. Nachdem Sie diese Auswahl ausgewählt haben, wird das Fenster für reguläre Ausdrücke angezeigt. Geben Sie den regulären Ausdruck in das Fenster ein. Sie können die **Regex-Token** verwenden, um gemeinsame Elemente für reguläre Ausdrücke einzufügen, oder Sie können den Regex-Editor für Unterstützung beim Erstellen eines regulären Ausdrucks verwenden, den Sie möchten.
- Ausdruck. Überprüft URLs, die mit einem Citrix ADC Standardausdruck übereinstim-

men.

7. Definieren Sie im Bereich Muster das Muster. Ein Muster ist eine literale Zeichenfolge oder ein regulärer Ausdruck im PCRE-Format, der das Muster definiert, das Sie übereinstimmen möchten. Der Bereich Muster enthält die folgenden Elemente:
- Übereinstimmung. Eine Dropdownliste mit Suchmethoden, die Sie für die Signatur verwenden können. Diese Liste unterscheidet sich je nachdem, ob der Mustertyp Request oder Response ist.

Anforderungsübereinstimmungstypen
PCRE. Ein regulärer Ausdruck im PCRE-Format.

> **Hinweis:**
>
> Wenn Sie PCRE wählen, sind die Werkzeuge für reguläre Ausdrücke unterhalb des Pattern-Fensters aktiviert. Diese Werkzeuge sind für die meisten anderen Arten von Mustern nicht nützlich.

- **Injection**. Weist die Web App Firewall an, nach injiziertem SQL am angegebenen Speicherort zu suchen. Das Pattern-Fenster verschwindet, da die Web App Firewall bereits über die Muster für die SQL-Injection verfügt.
- **CrossSiteScripting**. Weist die Web App Firewall an, am angegebenen Speicherort nach websiteübergreifenden Skripten zu suchen. Das Pattern-Fenster wird ausgeblendet, da die Web App Firewall bereits über die Muster für siteübergreifende Skripts verfügt.
- **Ausdruck**. Ein Ausdruck in der Citrix ADC Standardausdruckssprache ist dieselbe Ausdruckssprache für das Erstellen von Web App Firewall Richtlinien auf der Citrix ADC Appliance. Obwohl die Citrix ADC Ausdruckssprache ursprünglich für Richtlinienregeln entwickelt wurde, handelt es sich um eine hochflexible Allzwecksprache, die auch zum Definieren eines Signaturmusters verwendet werden kann.

Wenn Sie Expression auswählen, wird der Citrix ADC Ausdruckseditor unterhalb des Musterfensters angezeigt. Weitere Informationen zum Ausdrucks-Editor und Anweisungen zur Verwendung finden Sie unter So fügen Sie eine Firewallregel (Ausdruck) mithilfe des Dialogfelds Ausdruck hinzufügen hinzu

Antwort-Übereinstimmungstypen:

```
1 -  Literal. A literal string
2 -  PCRE. A PCRE-format regular expression.
```

> Hinweis:
>
> Wenn Sie PCRE wählen, sind die Werkzeuge für reguläre Ausdrücke unterhalb des Pattern-

> Fensters aktiviert. Diese Werkzeuge sind für die meisten anderen Arten von Mustern nicht nützlich.

- **Kreditkarte**. Ein integriertes Muster, das einer der sechs unterstützten Kreditkartennummern entspricht.

> Hinweis:
>
> Der Ausdruck-Übereinstimmungstyp ist für Antwort-Signaturen nicht verfügbar.

- Musterfenster (unbeschriftet)

Geben Sie in diesem Fenster das Muster ein, das Sie abgleichen möchten, und geben Sie zusätzliche Daten ein.

- Literal. Geben Sie im Textbereich die Zeichenfolge ein, nach der Sie suchen möchten.
- CRE. Geben Sie den regulären Ausdruck in den Textbereich ein. Verwenden Sie den Regex-Editor, um weitere Unterstützung beim Erstellen des gewünschten regulären Ausdrucks zu erhalten, oder die Regex-Token, um allgemeine reguläre Ausdruckselemente am Cursor einzufügen. Um UTF-8-Zeichen zu aktivieren, klicken Sie auf UTF-8.
- Ausdruck. Geben Sie den erweiterten Citrix ADC Ausdruck im Textbereich ein. Verwenden Sie Präfix, um den ersten Begriff in Ihrem Ausdruck auszuwählen, oder Operator, um gemeinsame Operatoren am Cursor einzufügen. Klicken Sie auf Hinzufügen, um das Dialogfeld Ausdruck hinzufügen zu öffnen, um weitere Unterstützung beim Erstellen des gewünschten regulären Ausdrucks zu erhalten. Klicken Sie auf Auswerten, um den erweiterten Ausdrucksauswerter zu öffnen, um festzustellen, welche Auswirkungen Ihr Ausdruck hat.
- Versatz. Die Anzahl der Zeichen, die übersprungen werden sollen, bevor sie mit diesem Muster übereinstimmen. Sie verwenden dieses Feld, um eine Zeichenfolge an einem anderen Punkt als dem ersten Zeichen zu untersuchen.
- Tiefe. Wie viele Zeichen vom Startpunkt auf Übereinstimmungen untersucht werden sollen. Verwenden Sie dieses Feld, um die Suche einer großen Zeichenfolge auf eine bestimmte Anzahl von Zeichen zu beschränken.
- Min-Länge. Die zu durchsuchende Zeichenfolge muss mindestens die angegebene Anzahl von Bytes in der Länge sein. Kürzere Zeichenfolgen werden nicht übereinstimmend.
- Max-Länge. Die zu durchsuchende Zeichenfolge darf nicht länger als die angegebene Anzahl von Bytes in der Länge sein. Längere Saiten werden nicht übereinstimmend.
- Suchmethode. Ein Kontrollkästchen mit der Bezeichnung Fastmatch. Sie können Fastmatch nur für ein Literalmuster aktivieren, um die Leistung zu verbessern.

8. Klicken Sie auf **OK**.
9. Wiederholen Sie die vorherigen vier Schritte, um weitere Muster hinzuzufügen oder zu ändern.
10. Wenn Sie mit dem Hinzufügen oder Ändern von Mustern fertig sind, klicken Sie auf **OK**, um die Änderungen zu speichern und zum Bereich Signaturen zurückzukehren.

> **Achtung:**
>
> Bis Sie im Dialogfeld **Lokale Signaturregel hinzufügen** oder **Lokale Signaturregel ändern** auf **OK** klicken, werden die Änderungen nicht gespeichert. Schließen Sie eines dieser Dialogfelder nicht, ohne auf **OK** zu klicken, es sei denn, Sie möchten die Änderungen verwerfen.

So importieren und zusammenführen Sie Regeln

October 5, 2021

Wenn Sie den Signatur-Editor zum Ausführen eines Import- und Zusammenführungsvorgangs über die GUI verwenden, können Sie nun die neuen, aktualisierten, duplizierten und ungültigen Regeln anzeigen.

Der Signatur-Editor zeigt die folgenden vier neuen Zeilen an:

1. Neue Regeln
2. Aktualisierte Regeln
3. Doppelte Regeln
4. Ungültige Regeln

Die Ausgabe der Filter Nur Neue Regeln und Nur aktualisierte Regeln wird auch im Kategoriefilterbereich des Bearbeitungsfensters im Signatureditor angezeigt.

Sie müssen die Dateien von der GUI importieren, um die entsprechenden Links für Neue, doppelte, ungültige und aktualisierte Regeln zu sehen.

Verfahren zum Importieren von Signaturregeln:

1. Wechseln Sie in der Citrix ADC Web-GUI zu **Konfiguration > Sicherheit > Citrix Web App Firewall Signatures**. Klicken Sie im Fenster Signaturen auf **Hinzufügen**. Wählen Sie dann **Dateiformat** > **Nativ**, **Importieren von** > **URL** und fügen Sie im Feld “URL” den obigen Link hinzu. Wenn Sie nicht auf die URL zugreifen können, können Sie die XML-Daten in einem Textdateiformat herunterladen.
2. Nachdem Sie auf **Öffnen**geklickt haben, wird die Signaturdatei geöffnet, und Sie können Links für neue Regel und ungültige Regeln sehen.
3. Wenn Sie eine3rd Partei-Signaturregel importieren, werden 90 neue Regeln und 9 doppelte Regeln in der importierten XML-Datei angezeigt. Wenn Sie nicht auf die URL zugreifen können, können Sie die XML-Daten in einem Textdateiformat herunterladen.

Signaturaktualisierungen bei Hochverfügbarkeitsbereitstellung und Build-Upgrades

October 5, 2021

Die Signaturaktualisierung erfolgt auf dem primären Knoten. Während die Signaturen auf dem primären Knoten aktualisiert werden, werden die aktualisierten Dateien gleichzeitig mit dem sekundären Knoten synchronisiert.

Die Standardsignatur wird immer zuerst aktualisiert, und dann werden die restlichen benutzerdefinierten Signaturen aktualisiert.

Herstellen einer Verbindung mit Amazon AWS

Der Standard-Routen-NSIP wird verwendet, um eine Verbindung mit Amazon AWS herzustellen. Wenn es ein bestimmtes Anwendungsfallszenario gibt, in dem SNIP verwendet wird, und wenn mehrere SNIPs vorhanden sind, wird der erste, der die ARP-Antwort von der Hosting-Site empfängt, die Route enthalten.

Signaturaktualisierungen bei Versions-Upgrades

Im Falle eines Upgrades, wenn der NS eine ältere Basisversion für die Signaturen hat, wird *Standardsignatur automatisch aktualisiert, wenn eine neuere Signaturversion verfügbar ist.

Wenn sich das Schema geändert hat, wird die Schemaversion aller Signaturobjekte aktualisiert, wenn die Version aktualisiert wird.

Bei der Basisversion der benutzerdefinierten Signaturen unterscheidet sich das Verhalten in Release 10.5 gegenüber Version 11.0.

In Release 10.5 wurde nur die Standardsignatur aktualisiert, und die Basisversion der restlichen Signaturen blieb nach dem Build-Upgrade unverändert.

In Release 11.0 hat sich dieses Verhalten geändert. Wenn die Appliance aktualisiert wird, um einen neuen Build zu installieren, werden nicht nur das Signaturobjekt *Default, sondern alle anderen benutzerdefinierten Signaturen, die derzeit in der Appliance vorhanden sind, ebenfalls aktualisiert und haben nach dem Build-Upgrade dieselbe Version.

Sowohl in 10.5 als auch 11.0 Release-Builds werden die *Default Signatures sowie alle Signaturen, die ungleich Null sind, automatisch auf die neueste veröffentlichte Signaturversion aktualisiert und haben dieselbe Basisversion.

Übersicht über Sicherheitsprüfungen

October 5, 2021

Die erweiterten Schutzmechanismen der Web App Firewall (Sicherheitsprüfungen) sind eine Reihe von Filtern, die komplexe oder unbekannte Angriffe auf Ihre geschützten Websites und Webdienste abfangen sollen. Die Sicherheitsprüfungen verwenden Heuristik, positive Sicherheit und andere Techniken, um Angriffe zu erkennen, die möglicherweise nicht allein von Signaturen erkannt werden. Sie konfigurieren die Sicherheitsprüfungen, indem Sie ein Web App Firewall Profil erstellen und konfigurieren. Dabei handelt es sich um eine Sammlung von benutzerdefinierten Einstellungen, die der Web App Firewall mitteilen, welche Sicherheitsprüfungen verwendet werden sollen und wie eine Anforderung oder Antwort verarbeitet werden soll, bei der eine Sicherheitsprüfung fehlgeschlagen ist. Ein Profil ist einem Signaturobjekt und einer Richtlinie zum Erstellen einer Sicherheitskonfiguration zugeordnet.

Die Web App Firewall bietet zwanzig Sicherheitsprüfungen, die sich in den angestrebten Angriffstypen und der Komplexität ihrer Konfiguration stark unterscheiden. Die Sicherheitsprüfungen sind in folgende Kategorien unterteilt:

- **Gemeinsame Sicherheitsprüfungen.** Überprüfungen, die für alle Aspekte der Websicherheit gelten, die entweder keinen Inhalt beinhalten oder für alle Arten von Inhalten gleichermaßen gelten.
- **HTML-Sicherheitsprüfungen.** Überprüfungen, die HTML-Anforderungen und Antworten untersuchen. Diese Prüfungen gelten für HTML-basierte Websites und die HTML-Teile von Web 2.0-Sites, die gemischte HTML- und XML-Inhalte enthalten.
- **XML-Sicherheitsprüfungen.** Überprüfungen, die XML-Anforderungen und Antworten untersuchen. Diese Prüfungen gelten für XML-basierte Webdienste und für die XML-Teile von Web 2.0-Websites.

Die Sicherheitsprüfungen schützen vor einer Vielzahl von Angriffen, darunter Angriffe auf Schwachstellen auf Sicherheitslücken in Betriebssystemen und Webserversoftware, Schwachstellen in der SQL-Datenbank, Fehler beim Design und Codieren von Websites und Webdiensten sowie Ausfälle beim Schutz von Websites, die auf sensible Informationen hosten oder darauf zugreifen können.

Alle Sicherheitsprüfungen verfügen über eine Reihe von Konfigurationsoptionen, die Prüfaktionen, mit denen gesteuert wird, wie die Web App Firewall eine Verbindung verarbeitet, die einer Prüfung entspricht. Für alle Sicherheitsprüfungen stehen drei Prüfaktionen zur Verfügung. Sie sind:

- **Blockieren** Verbindungen blockieren, die mit der Signatur übereinstimmen. Diese Funktion ist standardmäßig deaktiviert.
- **Melden Sie sich** Protokollieren Sie Verbindungen, die mit der Signatur übereinstimmen, für eine spätere Analyse. Standardmäßig aktiviert.

- **Statistiken.** Verwalten Sie Statistiken für jede Signatur, die zeigen, wie viele Verbindungen sie übereinstimmten, und geben Sie bestimmte andere Informationen über die Typen von Verbindungen, die blockiert wurden. Diese Funktion ist standardmäßig deaktiviert.

Für mehr als die Hälfte der Überprüfungsaktionen ist eine vierte Prüfaktion **Lernen** verfügbar. Es beobachtet den Datenverkehr zu einer geschützten Website oder einem geschützten Webdienst und verwendet Verbindungen, die wiederholt gegen die Sicherheitsprüfung verstoßen, um empfohlene Ausnahmen (Entspannungen) des Schecks oder neue Regeln für die Überprüfung zu generieren. Zusätzlich zu den Überprüfungsaktionen verfügen bestimmte Sicherheitsüberprüfungen über Parameter, die die Regeln steuern, mit denen die Prüfung ermittelt wird, welche Verbindungen gegen diese Prüfung verstoßen, oder die die Antwort der Web App Firewall auf Verbindungen konfigurieren, die gegen die Prüfung verstoßen. Diese Parameter unterscheiden sich für jede Prüfung und werden in der Dokumentation für jede Prüfung beschrieben.

Um Sicherheitsprüfungen zu konfigurieren, können Sie den Web App Firewall-Assistenten verwenden, wie im Web App Firewall-Assistentbeschrieben, oder Sie können die Sicherheitsprüfungen manuell konfigurieren, wie unter Manuelle Konfiguration mit der GUIbeschrieben. Einige Aufgaben, wie das manuelle Eingeben von Entspannungen oder Regeln oder das Überprüfen von erlernten Daten, können nur über die GUI und nicht über die Befehlszeile ausgeführt werden. Die Verwendung des Assistenten ist in der Regel die beste Konfigurationsmethode, aber in einigen Fällen kann die manuelle Konfiguration einfacher sein, wenn Sie mit ihm vertraut sind und einfach die Konfiguration für eine einzelne Sicherheitsprüfung anpassen möchten.

Unabhängig davon, welche Methode Sie zum Konfigurieren der Sicherheitsprüfungen verwenden, erfordert jede Sicherheitsprüfung, dass bestimmte Aufgaben ausgeführt werden. Viele Überprüfungen erfordern, dass Sie Ausnahmen (Relaxationen) angeben, um das Blockieren von legitimen Datenverkehr zu verhindern, bevor Sie die Sperre für diese Sicherheitsprüfung aktivieren. Sie können dies manuell tun, indem Sie die Protokolleinträge beobachten, nachdem ein bestimmter Datenverkehr gefiltert wurde und dann die erforderlichen Ausnahmen erstellen. In der Regel ist es jedoch viel einfacher, die Lernfunktion zu aktivieren und den Verkehr zu beobachten und die notwendigen Ausnahmen zu empfehlen.

Web App Firewall verwendet während der Verarbeitung der Transaktionen Packet Engines (PE). Jede Paketengine hat ein Limit von 100.000 Sitzungen, was für die meisten Bereitstellungsszenarien ausreichend ist. Wenn die Web App Firewall jedoch hohen Datenverkehr verarbeitet und das Sitzungstimeout mit einem höheren Wert konfiguriert ist, können die Sitzungen angesammelt werden. Wenn die Anzahl der Live Web App Firewall -Sitzungen die Grenze von 100.000 pro PE überschreitet, werden die Verletzungen der Web App Firewall Sicherheitsprüfung möglicherweise nicht an die Security Insight-Appliance gesendet. Das Senkung des Sitzungstimeouts auf einen kleineren Wert oder die Verwendung des Sitzungslos-Modus für die Sicherheitsprüfungen mit sitzungslosem URL-Schließen oder Sitzungslos-Feldkonsistenz kann dazu beitragen, dass die Sitzungen akkumuliert werden. Wenn dies in Szenarien, in denen Transaktionen möglicherweise längere Sitzungen

erfordern, keine praktikable Option ist, wird ein Upgrade auf eine übergeordnete Plattform mit mehr Paketmodul empfohlen.

Unterstützung für zwischengespeicherte AppFirewall wird hinzugefügt, und die maximale Sitzungseinstellung über die CLI pro Kern wird auf 50.000 Sitzungen festgelegt.

Top-Level-Schutz

October 5, 2021

Vier der Web App Firewall Schutzmaßnahmen sind besonders wirksam gegen gängige Arten von Web-Angriffen und werden daher häufiger als alle anderen verwendet. Sie sind:

- **HTML Cross-Site Scripting.** Untersucht Anfragen und Antworten auf Skripts, die versuchen, auf Inhalte auf einer anderen Website zuzugreifen oder diese zu ändern als der, auf der sich das Skript befindet. Wenn diese Überprüfung ein solches Skript findet, macht es entweder das Skript harmlos, bevor die Anforderung oder Antwort an das Ziel weitergeleitet wird, oder es blockiert die Verbindung.
- **HTML SQL Injection.** Prüft Anforderungen, die Formularfelddaten enthalten, auf Versuche, SQL-Befehle in eine SQL-Datenbank zu injizieren. Wenn diese Überprüfung injizierten SQL-Code erkennt, blockiert sie entweder die Anforderung oder macht den injizierten SQL-Code harmlos, bevor die Anforderung an den Webserver weitergeleitet wird.

  Hinweis: Wenn beide der folgenden Bedingungen für Ihre Konfiguration gelten, müssen Sie sicherstellen, dass Ihre Web App Firewall korrekt konfiguriert ist:

  - Wenn Sie die HTML Cross-Site Scripting Prüfung oder HTML SQL Injection Check (oder beide) aktivieren, und
  - Ihre geschützten Websites akzeptieren Datei-Uploads oder enthalten Webformulare, die große POST-Text-Daten enthalten können.

  Weitere Informationen zum Konfigurieren der Web App Firewall für diesen Fall finden Sie unter Konfigurieren der Application Firewall.
- **Pufferüberlauf.** Untersucht Anforderungen, um Versuche zu erkennen, einen Pufferüberlauf auf dem Webserver zu verursachen.
- **Cookie-Konsistenz.** Untersucht Cookies, die mit Benutzeranfragen zurückgegeben wurden, um sicherzustellen, dass sie mit den Cookies übereinstimmen, die Ihr Webserver für diesen Benutzer festgelegt hat. Wenn ein modifiziertes Cookie gefunden wird, wird es aus der Anforderung entfernt, bevor die Anforderung an den Webserver weitergeleitet wird.

Die Pufferüberlaufprüfung ist einfach. Sie können die Blockierung normalerweise sofort aktivieren. Die anderen drei übergeordneten Prüfungen sind wesentlich komplexer und erfordern eine Konfigu-

ration, bevor Sie sie sicher verwenden können, um Datenverkehr zu blockieren. Citrix empfiehlt dringend, die Lernfunktion zu aktivieren und die erforderlichen Ausnahmen zu generieren, anstatt diese Prüfungen manuell zu konfigurieren.

Websiteübergreifende HTML-Skripterstellung

December 7, 2021

Die Prüfung HTML Cross-Site Scripting (Cross-Site Scripting) untersucht sowohl die Header als auch die POST-Texte von Benutzeranfragen auf mögliche Cross-Site-Scripting-Angriffe. Wenn es ein siteübergreifendes Skript findet, ändert es entweder die Anforderung (*transformiert*), um den Angriff harmlos zu machen, oder blockiert die Anforderung.

> **Hinweis:**
>
> Die HTML Cross-Site Scripting (Cross-Site Scripting) -Prüfung funktioniert nur für Inhaltstyp, Inhaltslänge und so weiter. Es funktioniert nicht für das Cookie. Stellen Sie außerdem sicher, dass die Option 'CheckRequestHeaders' in Ihrem Web Application Firewall-Profil aktiviert ist.

Sie können den Missbrauch der Skripts auf Ihren geschützten Websites verhindern, indem Sie die HTML Cross-Site Scripting-Skripts verwenden, die gegen *dieselbe Ursprungsregel*verstoßen, die besagt, dass Skripts auf keinem Server, sondern auf dem Server, auf dem sie sich befinden, zugreifen oder diese ändern dürfen. Jedes Skript, das gegen dieselbe Ursprungsregel verstößt, wird als siteübergreifendes Skript bezeichnet, und die Praxis, Skripts zum Zugriff auf oder Ändern von Inhalten auf einem anderen Server zu verwenden, wird als siteübergreifende Skripts bezeichnet. Der Grund, warum Cross-Site Scripting ein Sicherheitsproblem ist, ist, dass ein Webserver, der Cross-Site Scripting ermöglicht, mit einem Skript angegriffen werden kann, das sich nicht auf diesem Webserver befindet, sondern auf einem anderen Webserver befindet, z. B. einem, der vom Angreifer gehört und kontrolliert wird.

Leider haben viele Unternehmen eine große installierte Basis von JavaScript-verbesserten Webinhalten, die gegen dieselbe Ursprungsregel verstößt. Wenn Sie die HTML Cross-Site Scripting Prüfung auf einer solchen Site aktivieren, müssen Sie die entsprechenden Ausnahmen generieren, damit die Prüfung legitime Aktivitäten nicht blockiert.

Die Web App Firewall bietet verschiedene Aktionsoptionen für die Implementierung von HTML Cross-Site Scripting Schutz. Zusätzlich zu den Aktionen **Blockieren**, **Protokollieren**, **Statistiken**und **Lernen**haben Sie auch die Möglichkeit, **siteübergreifende Skripts zu transformieren**, um einen Angriff durch Entitäten harmlos zu machen, die die Skript-Tags in der übermittelten Anforderung codiert. Sie können "Vollständige URLs für Cross-Site-Scripting-Parameter prüfen" konfigurieren, um anzugeben, ob Sie nicht nur die Abfrageparameter, sondern die gesamte URL überprüfen möchten, um Cross-Site-Scripting-Angriffe zu erkennen. Sie können den Parameter **InspectQueryContentTypes** so kon-

figurieren, dass der Anforderungsabfrageteil auf den Cross-Site-Scripting-Angriff auf die spezifischen Content-Typen untersucht wird.

Sie können Entspannungen bereitstellen, um Fehlalarme zu vermeiden. Die Lernengine der Web App Firewall kann Empfehlungen zum Konfigurieren von Relaxationsregeln enthalten.

Um einen optimierten HTML Cross-Site Scripting Schutz für Ihre Anwendung zu konfigurieren, konfigurieren Sie eine der folgenden Aktionen:

- **Block**— Wenn Sie Block aktivieren, wird die Blockaktion ausgelöst, wenn die siteübergreifenden Skript-Tags in der Anforderung erkannt werden.
- **Log**— Wenn Sie die Protokollfunktion aktivieren, werden bei der Prüfung Cross-Site Scripting Protokollmeldungen generiert, die die ausgeführten Aktionen angeben. Wenn der Block deaktiviert ist, wird für jedes Kopf- oder Formularfeld, in dem die Cross-Site-Scripting-Verletzung erkannt wurde, eine separate Protokollmeldung generiert. Allerdings wird nur eine Nachricht generiert, wenn die Anforderung blockiert wird. In ähnlicher Weise wird eine Protokollnachricht pro Anfrage für den Transformationsvorgang generiert, selbst wenn Cross-Site-Scripting-Tags in mehrere Felder umgewandelt werden. Sie können die Protokolle überwachen, um festzustellen, ob Antworten auf legitime Anfragen blockiert werden. Eine große Zunahme der Anzahl von Protokollmeldungen kann auf Versuche hinweisen, einen Angriff zu starten.
- **Statistiken**— Wenn diese Option aktiviert ist, sammelt die Statistikfunktion Statistiken über Verstöße und Protokolle. Ein unerwarteter Anstieg im Statistikzähler deutet möglicherweise darauf hin, dass Ihre Anwendung angegriffen wird. Wenn legitime Anfragen blockiert werden, müssen Sie möglicherweise die Konfiguration erneut aufrufen, um festzustellen, ob Sie neue Relaxationsregeln konfigurieren oder die vorhandenen ändern müssen.
- **Lernen**— Wenn Sie nicht sicher sind, welche Relaxationsregeln ideal für Ihre Anwendung geeignet sind, können Sie mit der Lernfunktion HTML Cross-Site-Skripting-Regelempfehlungen basierend auf den erlernten Daten generieren. Die Web App Firewall Learning Engine überwacht den Datenverkehr und bietet Lernempfehlungen basierend auf den beobachteten Werten. Um den optimalen Nutzen zu erzielen, ohne die Leistung zu beeinträchtigen, sollten Sie die Lernoption für kurze Zeit aktivieren, um ein repräsentatives Beispiel der Regeln zu erhalten, und dann die Regeln bereitstellen und das Lernen deaktivieren.
- **Siteübergreifende Skripts transformieren**— Wenn diese Option aktiviert ist, nimmt die Web App Firewall folgende Änderungen an Anforderungen vor, die mit der Prüfung für HTML Cross-Site Scripting übereinstimmen:
  - Linke eckige Klammer (<) zu HTML-Zeichenelement Äquivalent (<)
  - Rechtwinklige Klammer (>) zu HTML-Zeichenentität Äquivalent (>)

Dies stellt sicher, dass Browser keine unsicheren HTML-Tags interpretieren und dadurch bösartigen Code ausführen. `<script>` Wenn Sie sowohl die Überprüfung von Anforderungskopfdaten als auch die Transformation aktivieren, werden alle Sonderzeichen, die in Anforderungsheadern gefunden

werden, Wenn die Skripts auf Ihrer geschützten Website Cross-Site-Scripting-Funktionen enthalten, Ihre Website jedoch nicht darauf angewiesen ist, dass diese Skripts ordnungsgemäß funktionieren, können Sie das Blockieren sicher deaktivieren und die Transformation aktivieren. Diese Konfiguration stellt sicher, dass kein rechtmäßiger Webverkehr blockiert wird, während potenzielle Cross-Site Scripting Angriffe gestoppt werden.

- **Prüfen Sie vollständige URLs für Cross-Site-Scripting**. Wenn die Überprüfung vollständiger URLs aktiviert ist, untersucht die Web App Firewall gesamte URLs auf HTML-Cross-Site-Scripting-Angriffe, anstatt nur die Abfrageteile von URLs zu überprüfen.
- **Überprüfen Sie Anfrage-Header**. Wenn die Request-Header-Prüfung aktiviert ist, untersucht die Web App Firewall die Header von Anforderungen für HTML-Cross-Site-Scripting-Angriffe anstelle von nur URLs. Wenn Sie die GUI verwenden, können Sie diesen Parameter auf der Registerkarte Einstellungen des Web App Firewall Profils aktivieren.
- **InspectQueryContentTypes**. Wenn die Anforderungsabfrage-Inspektion konfiguriert ist, untersucht die App Firewall die Abfrage von Anforderungen für Cross-Site-Scripting-Angriffe für die spezifischen Content-Typen. Wenn Sie die GUI verwenden, können Sie diesen Parameter auf der Registerkarte Einstellungen des App-Firewall-Profils konfigurieren.

> **Wichtig:**
>
> Als Teil der Streaming-Änderungen hat sich die Web App Firewall Verarbeitung der Cross-Site-Skript-Tags geändert. Diese Änderung gilt für 11.0 Builds ab. Diese Änderung ist auch relevant für die Erweiterungsbuilds von 10.5.e, die das anforderungsseitige Streaming unterstützen. In früheren Versionen wurde entweder eine offene Klammer (<), or close bracket (>) oder beide offene und geschlossene Klammern (<>) als siteübergreifende Skriptverletzung gekennzeichnet. Das Verhalten hat sich in den Builds geändert, die Unterstützung für das anforderungsseitige Streaming enthalten. Nur das Close-Klammerzeichen (>) wird nicht mehr als Angriff betrachtet. Anfragen werden auch dann blockiert, wenn ein offenes Klammerzeichen (<) vorhanden ist, und werden als Angriff betrachtet. Der Cross-Site-Skripting-Angriff wird gekennzeichnet.

Siteübergreifende Skripterstellung Feinkörnige Relaxationen

Die Web App Firewall bietet Ihnen die Möglichkeit, ein bestimmtes Formularfeld, eine Kopfzeile oder ein Cookie von der websiteübergreifenden Skriptprüfung auszunehmen. Sie können die Inspektion für eines oder mehrere dieser Felder vollständig umgehen, indem Sie Relaxationsregeln konfigurieren.

Mit der Web App Firewall können Sie durch Feinabstimmung der Entspannungsregeln strengere Sicherheit implementieren. Eine Anwendung erfordert möglicherweise die Flexibilität, um bestimmte Muster zuzulassen, aber die Konfiguration einer Relaxationsregel, um die Sicherheitsprüfung zu umgehen, kann die Anwendung anfällig für Angriffe machen, da das Zielfeld von der Prüfung für standortübergreifende Skriptangriffsmuster ausgenommen ist. Die websiteübergreifende Scripting feinkörnige Entspannung bietet die Möglichkeit, bestimmte Attribute, Tags und Muster

zuzulassen. Der Rest der Attribute, Tags und Muster wird blockiert. Beispielsweise verfügt die Web App Firewall derzeit über einen Standardsatz von mehr als 125 abgelehnten Mustern. Da Hacker diese Muster bei standortübergreifenden Skriptangriffen verwenden können, kennzeichnet die Web App Firewall sie als potenzielle Bedrohungen. Sie können ein oder mehrere Muster entspannen, die für den bestimmten Standort als sicher angesehen werden. Der Rest der potenziell gefährlichen Cross-Site-Skriptmuster wird weiterhin auf den Zielort überprüft und löst weiterhin die Sicherheitsüberprüfungen aus. Sie haben jetzt viel strengere Kontrolle.

Die in Relaxationen verwendeten Befehle verfügen über optionale Parameter für **Werttyp** und **Wertausdruck**. Der Werttyp kann leer gelassen werden, oder Sie haben die Möglichkeit, **Tag** oder **Attribut** oder **Muster** auszuwählen. Wenn Sie den Werttyp leer lassen, wird das konfigurierte Feld der angegebenen URL von der Überprüfung Cross-Site Scripting ausgenommen. Wenn Sie einen Werttyp auswählen, müssen Sie einen Wertausdruck angeben. Sie können angeben, ob es sich bei dem Wertausdruck um einen regulären Ausdruck oder um eine Literalzeichenfolge handelt. Wenn die Eingabe mit der Liste Zulässige und Verweigerte abgeglichen wird, werden nur die angegebenen Ausdrücke, die in den Relaxationsregeln konfiguriert sind, ausgenommen.

Die Web App Firewall verfügt über die folgenden Siteübergreifenden Skripterstellungslisten:

1. **cross-site scripting Allowed Attributes**: There are 52 defaults allowed attributes, such as, **abbr**, **accesskey**, **align**, **alt**, **axis**, **bgcolor**, **border**, **cell padding**, **cell spacing**, **char**, **charoff**, **charset** and so forth
2. **cross-site scripting Allowed Tags**: There are 47 defaults allowed tags, such as, **address**, **basefont**, **bgsound**, **big**, **blockquote**, **bg**, **br**, **caption**, **center**, **cite**, **dd**, **del** and so forth
3. **cross-site scripting Denied Patterns**: There are 129 defaults denied patterns, such as, **FSCommand**, **javascript:**, **onAbort**, **onActivate** and so forth

> **Warnung**
>
> Web App Firewall Aktions-URLs sind reguläre Ausdrücke. Beim Konfigurieren von siteübergreifenden HTML-Relaxationsregeln für Skripts können Sie **Name**und **Value Expression** als Literal oder RegEx angeben. Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau die Regel definieren, die Sie als Ausnahme hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung von Platzhaltern und insbesondere der Punkt-Sternchen (.*) -Metazeichen/Platzhalterkombination kann zu Ergebnissen führen, die Sie nicht wünschen, z. B. das Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten, oder das Erlauben eines Angriffs, den die Cross-Site Scripting Prüfung sonst blockiert hätte.

Zu berücksichtigende Punkte:

- Value-Ausdruck ist ein optionales Argument. Ein Feldname hat möglicherweise keinen Werteausdruck.

- Ein Feldname kann an mehrere Wertausdrücke gebunden werden.
- Werteausdrücken muss ein Werttyp zugewiesen werden. Der siteübergreifende Scripting-Werttyp kann sein: 1) Tag, 2) Attribut oder 3) Pattern.
- Sie können mehrere Relaxationsregeln pro Feldname/URL-Kombination haben
- Bei den Formularfeldnamen und den Aktions-URLs wird die Groß- und Kleinschreibung nicht beachtet.

Verwenden der Befehlszeile zum Konfigurieren der HTML Cross-Site Scripting Prüfung

So konfigurieren Sie HTML Cross-Site Scripting Überprüfungsaktionen und andere Parameter mit der Befehlszeile

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie die folgenden Befehle eingeben, um die HTML Cross-Site Scripting Check zu konfigurieren:

- setze appfw profile “Parameterbeschreibungen unten auf der Seite. “)
- `<name> -crossSiteScriptingAction (([block] [learn] [log] [stats])| [** none**])`
- setze appfw profile “Parameterbeschreibungen unten auf der Seite. “)
- `<name> **-crossSiteScriptingTransformUnsafeHTML** (ON | OFF)`
- legen Sie appfw profile Parameterbeschreibungen fest, die unten auf der Seite angegeben sind.
- `<name> -crossSiteScriptingCheckCompleteURLs (ON | OFF)`
- legen Sie appfw profile Parameterbeschreibungen fest, die unten auf der Seite angegeben sind.
- `<name> - checkRequestHeaders (ON | OFF)` Parameterbeschreibungen unten auf der Seite.
- `<name> - CheckRequestQueryNonHtml (ON | OFF)` Parameterbeschreibungen unten auf der Seite.

So konfigurieren Sie eine HTML Cross-Site Scripting Check Relaxationsregel mit der Befehlszeile

Verwenden Sie den Befehl bind oder unbind, um die Bindung wie folgt hinzuzufügen oder zu löschen:

- `bind appfw profile <name> -crossSiteScripting <String> [isRegex (REGEX | NOTREGEX)] <formActionURL> [-location <location>] [-valueType (Tag| Attribute|Pattern)[<valueExpression>] [-isValueRegex (REGEX | NOTREGEX) ]]`
- `unbind appfw profile <name> -crossSiteScripting <String> <formActionURL > [-location <location>] [-valueType (Tag |Attribute|Pattern)[<valueExpression >]]`

Verwenden der GUI zum Konfigurieren der HTML-Cross-Site Scripting Check

In der grafischen Benutzeroberfläche können Sie das Kontrollkästchen HTML Cross-Site Scripting im Bereich für das Profil konfigurieren, das Ihrer Anwendung zugeordnet ist.

So konfigurieren oder ändern Sie die HTML Cross-Site Scripting Prüfung mit der GUI

1. Navigieren Sie zu **Application Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Sicherheitsprüfungen**.

In der Tabelle Sicherheitsprüfung werden die aktuell konfigurierten Aktionseinstellungen für alle Sicherheitsprüfungen angezeigt. Sie haben 2 Optionen für die Konfiguration:

a. Wenn Sie Aktionen zum **Blockieren**, **Protokollieren**, **Statistiken**und **Lernen** für HTML Cross-Site Scripting aktivieren oder deaktivieren möchten, können Sie die Kontrollkästchen in der Tabelle aktivieren oder deaktivieren, auf **OK**und dann auf **Speichern und Schließen** zu Schließen Sie den Bereich **Sicherheitsprüfung**.

b. Wenn Sie weitere Optionen für diese Sicherheitsprüfung konfigurieren möchten, doppelklicken Sie auf **HTML Cross-Site Scripting**, oder wählen Sie die Zeile aus und klicken Sie auf **Aktionseinstellungen**, um die folgenden Optionen anzuzeigen:

Websiteübergreifende Skripts transformieren — Transformieren Sie unsichere Skript-Tags.

Überprüfen Sie vollständige URLs für siteübergreifende Skripterstellung— Anstatt nur den Abfrageteil der URL zu überprüfen, überprüfen Sie die vollständige URL auf siteübergreifende Skriptverletzungen.

Nachdem Sie eine der oben genannten Einstellungen geändert haben, klicken Sie auf **OK**, um die Änderungen zu speichern und zur Tabelle Sicherheitsprüfungen zurückzukehren. Sie können bei Bedarf weitere Sicherheitsprüfungen konfigurieren. Klicken Sie auf **OK**, um alle Änderungen zu speichern, die Sie im Abschnitt Sicherheitsprüfungen vorgenommen haben, und klicken Sie dann auf **Speichern und schließen**, um den Bereich Sicherheitsüberprüfung zu schließen.

Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Profileinstellungen**, um die Einstellung **Überprüfungsanforderung** zu aktivieren oder zu deaktivieren. Aktivieren oder deaktivieren Sie unter **Allgemeine Einstellungen** das Kontrollkästchen **Anforderungskopfzeilen** überprüfen. Klicken Sie auf **OK**. Sie können entweder das X-Symbol oben rechts im Bereich Profileinstellungen verwenden, um diesen Abschnitt zu schließen, oder wenn Sie die Konfiguration dieses Profils abgeschlossen haben, können Sie auf **Fertig** klicken, um zur **Anwendungsfirewall** > **Profil**zurückzukehren.

Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Profileinstellungen**, um die Einstellung **Abfrage nicht HTML überprüfen** zu aktivieren oder zu deaktivieren. Aktivieren oder deaktivieren Sie unter **Allgemeine Einstellungen** das Kontrollkästchen **Abfrage Nicht-HTML überprüfen**. Klicken Sie auf **OK**. Sie können entweder das X-Symbol oben rechts im Bereich **Profileinstellungen** verwenden, um

diesen Abschnitt zu schließen oder, wenn Sie die Konfiguration dieses Profils abgeschlossen haben, klicken Sie auf **Fertig**, um zur **App-Firewall > Profil** zurückzukehren.

So konfigurieren Sie eine HTML Cross-Site-Scripting-Relaxationsregel mit der GUI

1. Navigieren Sie zu **Application Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Relaxationsregeln**.
3. Doppelklicken Sie in der Tabelle Relaxationsregeln auf den Eintrag **HTML Cross-Site Scripting**, oder wählen Sie ihn aus, und klicken Sie auf **Bearbeiten**.
4. Führen Sie im Dialogfeld **HTML Cross-Site Scripting Relaxationsregeln** die Vorgänge **Hinzufügen**, **Bearbeiten**, **Löschen**, **Aktivieren** oder **Deaktivieren** für Relaxationsregeln aus.

> **Hinweis:**
>
> Wenn Sie eine neue Regel hinzufügen, wird das Feld **Wertausdruck** nur angezeigt, wenn Sie im Feld **Werttyp** die Option **Tag** oder **Attribut** oder **Muster** auswählen.

So verwalten Sie HTML Cross-Site Scripting Relaxationsregeln mithilfe des Visualizers

Um eine konsolidierte Ansicht aller Relaxationsregeln zu erhalten, können Sie die Zeile **HTML Cross-Site Scripting** in der Tabelle Relaxationsregeln markieren und auf **Visualizer** klicken. Der Visualizer für bereitgestellte Relaxationen bietet Ihnen die Möglichkeit, eine neue Regel **hinzuzufügen** oder eine vorhandene zu **bearbeiten**. Sie können auch eine Gruppe von Regeln **aktivieren** oder **deaktivieren**, indem Sie einen Knoten auswählen und auf die entsprechenden Schaltflächen im Relaxationsvisualizer klicken.

So zeigen Sie die Cross-Site Scripting Patterns mit der GUI an oder passen Sie sie an

Sie können die GUI verwenden, um die Standardliste der Siteübergreifenden Skripting-Attribute oder zulässigen Tags anzuzeigen oder anzupassen. Sie können auch die Standardliste der Siteübergreifenden Skripterstellung verweigerter Muster anzeigen oder anpassen.

Die Standardlisten werden unter **Anwendungsfirewall** > **Signaturen** > **Standardsignaturen** angegeben. Wenn Sie kein Signaturobjekt an Ihr Profil binden, wird die standardmäßige siteübergreifende Skripterstellung erlaubt und verweigert, die im Objekt Standardsignaturen angegeben ist, vom Profil für die Verarbeitung der Cross-Site Scripting Sicherheitsüberprüfung verwendet. Die Tags, Attribute und Patterns, die im Standardsignaturobjekt angegeben sind, sind schreibgeschützt. Sie können sie nicht bearbeiten oder ändern. Wenn Sie diese ändern oder ändern möchten, erstellen Sie eine Kopie des Standardsignaturen-Objekts, um ein Benutzerdefiniertes Signaturobjekt zu erstellen. Nehmen Sie Änderungen an den zulässigen oder abgelehnten Listen im neuen Benutzerdefinierten Signaturobjekt vor, und verwenden Sie dieses Signaturobjekt in Ihrem Profil, das den Datenverkehr verarbeitet, für den Sie diese angepassten zulässigen und verweigerten Listen verwenden möchten.

1. So zeigen Sie standardmäßige Cross-Site-Skriptmuster an:

a. Navigieren Sie zu **Anwendungsfirewall** > **Signaturen**, wählen Sie **Standardsignaturen** aus, und klicken Sie auf **Bearbeiten** . Klicken Sie dann auf **SQL/Cross-Site Scripting Pattern verwalten**.

Die Tabelle **SQL/Cross-Site-Scripting-Pfade verwalten** zeigt die folgenden drei Zeilen, die sich auf Cross-Site-Skripts beziehen:

`xss/allowed/attribute`

`xss/allowed/tag`

`xss/denied/pattern`

b. Wählen Sie eine Zeile aus, und klicken Sie auf **Elemente verwalten**, um die entsprechenden siteübergreifenden Skriptelemente (Tag, Attribut, Muster) anzuzeigen, die von der Web App Firewall **Cross-Site Scripting** Prüfung verwendet werden.

1. **So passen Sie cross-Site-Scripting-Elemente**an: Sie können das benutzerdefinierte Signaturobjekt bearbeiten, um das zulässige Tag, die zugelassenen Attribute und die abgelehnten Sie können neue Einträge hinzufügen oder vorhandene entfernen.

a. Navigieren Sie zu **Application Firewall** > **Signaturen**, markieren Sie die benutzerdefinierte Zielsignatur und klicken Sie auf **Bearbeiten**. Klicken Sie auf **SQL/Cross-Site-Skriptmuster verwalten, um die Tabelle SQL/Cross-Site-Scripting-Pfade** verwalten anzuzeigen.

b. Wählen Sie die Cross-Site-Ziel-Skriptzeile aus.

i. Klicken Sie auf **Elemente verwalten**, um das entsprechende Cross-Site-Scripting-Element **hinzuzufügen**, zu **bearbeiten** oder zu **entfernen** .

ii. Klicken Sie auf **Entfernen**, um die ausgewählte Zeile zu entfernen.

> **Warnung:**
>
> Sie müssen vorsichtig sein, bevor Sie ein standardmäßiges Cross-Site-Scripting-Element entfernen oder ändern oder den Cross-Site-Scripting-Pfad löschen, um die gesamte Zeile zu entfernen. Die Signaturregeln und die Cross-Site Scripting Sicherheitsprüfung sind bei der Erkennung von Angriffen zum Schutz Ihrer Anwendungen auf diese Elemente angewiesen. Das Anpassen der Cross-Site-Scripting Elements kann Ihre Anwendung anfällig für Cross-Site Scripting-Angriffe machen, wenn das erforderliche Muster während der Bearbeitung entfernt wird.

Verwenden der Lernfunktion mit der HTML Cross-Site Scripting Check

Wenn die Aktion “Lernen” aktiviert ist, überwacht die Lernengine der Citrix Web App Firewall den Datenverkehr und lernt die Cross-Site-Scripting-URL-Verstöße. Sie können regelmäßig Cross-Site-Scripting-URL-Regeln überprüfen und sie für falsch positive Szenarien bereitstellen.

> **Hinweis:**
>
> In einer Clusterkonfiguration müssen alle Knoten dieselbe Version haben, um die Cross-Site-Scripting-URL-Regeln bereitstellen zu können.

Verbesserung des Cross-Site-Scripting-Lernens von HTML Eine Verbesserung des Web App Firewall wurde in Version 11.0 der Citrix ADC -Software eingeführt. Um feinkörniges HTML Cross-Site Scripting Relaxation bereitzustellen, bietet die Web App Firewall ein fein abgestimmtes HTML Cross-Site Scripting Lernen. Die Lern-Engine gibt Empfehlungen bezüglich des beobachteten Werttyps (Tag, Attribut, Muster) und des entsprechenden Werteausdrucks, der in den Eingabefeldern beobachtet wird. Zusätzlich zur Überprüfung der blockierten Anforderungen, um festzustellen, ob die aktuelle Regel zu restriktiv ist und gelockert werden muss, können Sie die von der Lern-Engine generierten Regeln überprüfen, um festzustellen, welcher Werttyp und welcher Werteausdruck Verstöße auslösen und in den Relaxationsregeln behandelt werden müssen.

> **Hinweis:**
>
> Die Lern-Engine der Web App Firewall kann nur die ersten 128 Byte des Namens unterscheiden. Wenn ein Formular mehrere Felder mit Namen enthält, die für die ersten 128 Bytes übereinstimmen, kann die Lern-Engine möglicherweise nicht zwischen ihnen unterscheiden. In ähnlicher Weise kann die bereitgestellte Relaxationsregel versehentlich alle Felder von der HTML Cross-Site Scripting Inspektion lockern.
>
> **Tipp**
>
> Siteübergreifende Skript-Tags, die länger als 12 Zeichen sind, werden nicht korrekt gelernt oder protokolliert.
>
> Wenn Sie eine größere Tag-Länge zum Lernen benötigen, können Sie ein großes, nicht erscheinendes Tag in **as_Cross-Site Scripting_Allowed_Tags_List** für die Länge “x” einfügen.

So zeigen Sie gelernte Daten mit der Befehlszeilenschnittstelle an oder verwenden

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- `show appfw learningdata <profilename> crossSiteScripting`
- `rm appfw learningdata <profilename> –crossSiteScripting <string> <formActionURL> [<location>] [<valueType> <valueExpression>]`
- `export appfw learningdata <profilename> **crossSiteScripting*`

So zeigen Sie gelernte Daten mit der GUI an oder verwenden

1. Navigieren Sie zu **Application Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Gelernte Regeln** . Sie können den Eintrag **HTML Cross-Site Scripting** in der Tabelle Gelernte Regeln auswählen und darauf doppelklicken, um auf die erlernten Regeln zuzugreifen. In der Tabelle werden die Spalten

Feldname, A**ction URL**, **Value Type**, **Value**und **Hits** angezeigt. Sie können die erlernten Regeln bereitstellen oder eine Regel bearbeiten, bevor Sie sie als Relaxationsregel bereitstellen. Um eine Regel zu verwerfen, können Sie sie auswählen und auf die Schaltfläche **Überspringen** klicken. Sie können jeweils nur eine Regel bearbeiten, aber Sie können mehrere Regeln zum Bereitstellen oder Überspringen auswählen.

Sie haben auch die Möglichkeit, eine zusammengefasste Ansicht der erlernten Relaxationen anzuzeigen, indem Sie den Eintrag **HTML Cross-Site Scripting** in der Tabelle "Gelernte Regeln" auswählen und auf **Visualizer** klicken, um eine konsolidierte Ansicht aller gelernten Verletzungen zu erhalten. Der Visualizer macht es einfach, die erlernten Regeln zu verwalten. Es bietet eine umfassende Ansicht der Daten auf einem Bildschirm und erleichtert das Handeln an einer Gruppe von Regeln mit einem Klick. Der größte Vorteil des Visualizers besteht darin, dass reguläre Ausdrücke zur Konsolidierung mehrerer Regeln empfohlen werden. Sie können eine Teilmenge dieser Regeln basierend auf dem Trennzeichen und der Aktions-URL auswählen. Sie können 25, 50 oder 75 Regeln im Visualizer anzeigen, indem Sie die Nummer aus einer Dropdownliste auswählen. Der Visualizer für erlernte Regeln bietet die Möglichkeit, die Regeln zu bearbeiten und als Relaxation bereitzustellen. Oder Sie können die Regeln überspringen, um sie zu ignorieren.

Verwenden der Protokollfunktion mit der HTML-Cross-Site Scripting-Überprüfung

Wenn die Protokollaktion aktiviert ist, werden die Verletzungen der HTML Cross-Site Scripting Sicherheitsprüfung im Audit-Log als Verstöße gegen **AppFW_Cross-Site Scripting** protokolliert. Die Web App Firewall unterstützt sowohl native als auch CEF-Protokollformate. Sie können die Protokolle auch an einen entfernten Syslog-Server senden.

So greifen Sie mit der Befehlszeile auf die Protokollmeldungen zu

Wechseln Sie zur Shell und halten Sie die ns.logs im /var/log/ Ordner, um auf die Protokollnachrichten im Zusammenhang mit den HTML Cross-Site Scripting Verstößen zuzugreifen:

```
Shell
tail -f /var/log/ns.log | grep APPFW_cross-site scripting
```

Beispiel für eine Meldung einer Cross-Site Scripting-Sicherheitsüberprüfung im CEF-Protokollformat:

```
1 Jul 11 00:45:51 <local0.info> 10.217.31.98 CEF:0|Citrix|Citrix ADC|NS11
    .0|APPFW|\*\*APPFW_cross-site scripting\*\*|6|src=10.217.253.62
    geolocation=Unknown spt=4840 method=GET request=http://aaron.
    stratum8.net/FFC/CreditCardMind.html?abc=%3Cdef%3E msg=\*\*Cross-
    site script check failed for field abc="Bad tag: def"\*\* cn1=133
    cn2=294 cs1=pr_ffc cs2=PPE1 cs3=eUljypvLa0BbabwfGVE52Sewg9U0001 cs4=
    ALERT cs5=2015 act=\*\*not blocked\*\*
```



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

Beispiel für eine Site-Cross-Site-Skripting-Sicherheitsüberprüfungsprotokollnachricht im systemeigenen Protokollformat mit Transformationsaktion

```
Jul 11 01:00:28 <local0.info> 10.217.31.98 07/11/2015:01:00:28 GMT ns
    0-PPE-0 : default APPFW \*\*APPFW_cross-site scripting\*\* 132 0 :
    10.217.253.62 392-PPE0 eUljypvLa0BbabwfGVE52Sewg9U0001 pr_ffc http:
    //aaron.stratum8.net/FFC/login.php?login_name=%3CBOB%3E&passwd=&
    drinking_pref=on &text_area=&loginButton=ClickToLogin&as_sfid=
    AAAAAAVFqmYL68IGvkrcn2pzehjfIkm5E6EZ9FL8YLvIW_41AvAATuKYe9N7uGThSpEAxbb0iBx55j
    -FC4llF \*\*Cross-site script special characters seen in fields <
    transformed>\*\*
<!--NeedCopy-->
```

Greifen Sie mit der GUI auf die Protokollnachrichten zu

Die Citrix GUI enthält ein nützliches Tool (Syslog Viewer) zum Analysieren der Protokollmeldungen. Sie haben mehrere Optionen für den Zugriff auf den Syslog Viewer:

- Navigieren Sie zu **Anwendungsfirewall** > **Profile**, wählen Sie das Zielprofil aus, und klicken Sie auf **Sicherheitsprüfungen**. Markieren Sie die Zeile **HTML Cross-Site Scripting,** und klicken Sie auf **Protokolle** . Wenn Sie direkt über die HTML Cross-Site Scripting Prüfung des Profils auf die Protokolle zugreifen, filtert die GUI die Protokollmeldungen aus und zeigt nur die Protokolle an, die diese Sicherheitsüberprüfungsverletzungen betreffen.
- Sie können auch auf den Syslog Viewer zugreifen, indem Sie zu **Citrix ADC** > **System** > **Auditing** navigieren. Klicken Sie im Abschnitt **Überwachungsmeldungen** auf den Link **Syslog-Nachrichten**, um den Syslog Viewer anzuzeigen, der alle Protokollmeldungen einschließlich anderer Protokolle gegen Sicherheitsüberprüfungen anzeigt. Dies ist nützlich für das Debuggen, wenn während der Anforderungsverarbeitung mehrere Sicherheitsüberprüfungsverletzungen ausgelöst werden können.
- Navigieren Sie zu **Anwendungsfirewall** > **Richtlinien** > **Überwachung**. Klicken Sie im Abschnitt Audit-Meldungen auf den Link **Syslog-Nachrichten**, um den Syslog-Viewer anzuzeigen, der alle Protokollmeldungen einschließlich anderer Protokolle für Sicherheitsüberprüfungen anzeigt.

Der HTML-basierte Syslog Viewer bietet verschiedene Filteroptionen, um nur die Protokollmeldungen auszuwählen, die für Sie von Interesse sind. Um Protokollmeldungen für die **HTML-Cross-Site Scripting-Überprüfung** auszuwählen, filtern Sie, indem Sie **APPFW** in der Dropdownliste Optionen für **Modul**auswählen. Die Liste **Ereignistyp** bietet eine Reihe von Optionen, um Ihre Auswahl weiter zu verfeinern. Wenn Sie beispielsweise das Kontrollkästchen **AppFW_Cross-Site Scripting** aktivieren

und auf die Schaltfläche **Übernehmen** klicken, werden im Syslog Viewer nur Protokollnachrichten im Zusammenhang mit der HTML Cross-Site Scripting-Sicherheitsprüfung angezeigt.

Wenn Sie den Cursor in der Zeile für eine bestimmte Protokollmeldung platzieren, werden unter der Protokollmeldung mehrere Optionen wie **Modul**, **Ereignistyp**, **Ereignis-ID**, **Client-IP** usw. angezeigt. Sie können eine dieser Optionen auswählen, um die entsprechenden Informationen in der Protokollmeldung hervorzuheben.

Klicken Sie zum Bereitstellen der Funktionalität ist nur in der grafischen Benutzeroberfläche verfügbar. Sie können den Syslog Viewer verwenden, um nicht nur die Protokolle anzuzeigen, sondern auch HTML Cross-Site Scripting Relaxationsregeln basierend auf den Protokollmeldungen für die Sicherheitsüberprüfungen der Web App Firewall bereitzustellen. Die Protokollmeldungen müssen für diesen Vorgang im CEF-Protokollformat vorliegen. Klicken Sie hier, um die Funktionalität bereitzustellen, ist nur für Protokollmeldungen verfügbar, die durch die Aktion Blockieren (oder nicht blockieren) generiert werden. Sie können keine Relaxationsregel für eine Protokollmeldung über den Transformationsvorgang bereitstellen.

Um eine Relaxationsregel aus dem Syslog-Viewer bereitzustellen, wählen Sie die Protokollmeldung aus. In der oberen rechten Ecke des Felds Syslog-Viewer der ausgewählten Zeile wird ein Kontrollkästchen angezeigt. Aktivieren Sie das Kontrollkästchen, und wählen Sie dann eine Option aus der Liste **Aktion** aus, um die Relaxationsregel bereitzustellen. **Bearbeiten und Bereitstellen**, **Bereitstellen** und **Alle bereitstellen** sind als **Aktionsoptionen** verfügbar.

Die HTML-Site-Cross-Site-Skripting-Regeln, die mit der Option **Zum Bereitstellen klicken** bereitgestellt werden, enthalten die Empfehlungen für die Feinkorn-Entspannung nicht.

Konfigurieren Sie die Funktion zum Bereitstellen über die GUI

1. Wählen Sie im Syslog Viewer in den Optionen des **Moduls** die Option **APPFW** aus.
2. Wählen Sie das **App_Cross-Site-Scripting** als **Ereignistyp** aus, um die entsprechenden Protokollnachrichten zu filtern.
3. Aktivieren Sie das Kontrollkästchen, um die Regel zu identifizieren, die bereitgestellt werden soll.
4. Verwenden Sie die Dropdownliste **Aktion** mit Optionen, um die Relaxationsregel bereitzustellen.
5. Stellen Sie sicher, dass die Regel im entsprechenden Abschnitt zur Relaxationsregel angezeigt wird.

Statistiken für die HTML Cross-Site Scripting Verstöße

Wenn die Aktion Statistik aktiviert ist, wird der Leistungsindikator für die HTML Cross-Site Scripting Prüfung erhöht, wenn die Web App Firewall eine Aktion für diese Sicherheitsprüfung durchführt. Die

Statistiken werden für Rate und Gesamtanzahl für Traffic, Verletzungen und Protokolle gesammelt. Die Größe eines Inkrements des Protokollzählers kann abhängig von den konfigurierten Einstellungen variieren. Wenn beispielsweise die Blockaktion aktiviert ist, erhöht die Anforderung für eine Seite, die 3 HTML Cross-Site Scripting Verletzungen enthält, den Statistikindikator um eins, da die Seite blockiert wird, sobald die erste Verletzung erkannt wird. Wenn der Block jedoch deaktiviert ist, erhöht die Verarbeitung derselben Anforderung den Statistikindikator für Verletzungen und Protokolle um drei, da jede Verletzung eine separate Protokollmeldung generiert.

So zeigen Sie HTML Cross-Site Scripting Statistiken mit der Befehlszeile an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
> sh appfw stats
```

Verwenden Sie den folgenden Befehl, um Statistiken für ein bestimmtes Profil anzuzeigen:

```
> **stat appfw profile** <profile name>
```

Anzeigen von HTML Cross-Site Scripting Statistiken über die GUI

1. Navigieren Sie zu **Sicherheit** > **Anwendungsfirewall > Profile > Statistik** .
2. Greifen Sie im rechten Bereich auf den **Statistik-Link** zu.
3. Verwenden Sie die Bildlaufleiste, um die Statistiken über HTML Cross-Site Scripting Verletzungen und Protokolle anzuzeigen. Die Statistiktabelle enthält Echtzeitdaten und wird alle 7 Sekunden aktualisiert.

Highlights

- **Integrierte Unterstützung für HTML-Site Scripting Angriffsschutz**— Die Citrix Web App Firewall schützt vor Cross-Site Scripting-Angriffen, indem sie eine Kombination aus zulässigen Attributen und Tags und verweigerten Mustern in der empfangenen Nutzlast überwacht. Alle integrierten standardmäßigen zulässigen Tags, zulässigen Attribute und verweigerten Muster, die von der Cross-Site-Scripting-Überprüfung verwendet werden, sind in der Datei /netscaler/default_custom_settings.xml angegeben.
- **Customizatio**n: Sie können die Standardliste mit Tags, Attributen und Mustern ändern, um die Sicherheitsprüfung Cross-Site Scripting an die spezifischen Anforderungen Ihrer Anwendung anzupassen. Erstellen Sie eine Kopie des Standardsignaturobjekts, ändern Sie vorhandene Einträge oder fügen Sie neue hinzu. Binden Sie dieses Signaturobjekt an Ihr Profil, um die benutzerdefinierte Konfiguration zu nutzen.
- **Hybrides Sicherheitsmodell**— Sowohl Signaturen als auch tiefer Sicherheitsschutz verwenden die SQL/Cross-Site-Skriptmuster, die im Signaturobjekt angegeben sind, das an das Profil gebunden ist. Wenn kein Signaturobjekt an das Profil gebunden ist, werden die SQL/Cross-Site-Skriptmuster verwendet, die im Standardsignaturobjekt vorhanden sind.

- **Transform**—Beachten Sie Folgendes zum Transformationsvorgang:

Der Transformationsvorgang funktioniert unabhängig von den anderen Einstellungen für Cross-Site Scripting Aktionen. Wenn Transformation aktiviert ist und Blockieren, Protokollieren, Statistiken und Lerndaten deaktiviert sind, werden Cross-Site-Script-Tags transformiert.

Wenn die Blockaktion aktiviert ist, hat sie Vorrang vor der Transformationsaktion.

- **Feinkörnige Entspannung und Lernen**. Optimieren Sie die Relaxationsregel, um eine Untergruppe von Cross-Site-Scripting-Elementen von der Sicherheitsprüfung zu entfernen, aber den Rest zu erkennen Die Lern-Engine empfiehlt einen bestimmten Werttyp und Wertausdrücke basierend auf den beobachteten Daten.
- **Klicken Sie auf Bereitstellen**— Wählen Sie im Syslog Viewer eine oder mehrere siteübergreifende Skripting-Verstöße aus, und stellen Sie sie als Relaxationsregeln bereit.
- **Charset**— Der Standard-Zeichensatz für das Profil muss basierend auf den Anforderungen der Anwendung festgelegt werden. Standardmäßig ist der Profil-Zeichensatz auf Englisch US (ISO-8859-1) eingestellt. Wenn eine Anforderung ohne den angegebenen Zeichensatz empfangen wird, verarbeitet die Web App Firewall die Anforderung so, als ob sie ISO-8859-1 ist. Das Zeichen der offenen Klammer (<) or the close bracket character (>) wird nicht als Cross-Site-Scripting-Tags interpretiert, wenn diese Zeichen in anderen Zeichensätzen codiert sind. Wenn eine Anforderung beispielsweise eine UTF-8-Zeichenkette “%uff1cscript%uff1e**“**enthält, der Zeichensatz jedoch nicht auf der Anforderungsseite angegeben ist, wird die Cross-Site-Skripterstellungsverletzung möglicherweise nur ausgelöst, wenn der Standardzeichensatz für das Profil als Unicode angegeben ist.

Prüfung auf HTML SQL-Einschleusung

April 25, 2022

Viele Webanwendungen haben Webformulare, die SQL für die Kommunikation mit relationalen Datenbankservern verwenden. Bösartiger Code oder ein Hacker können ein unsicheres Webformular verwenden, um SQL-Befehle an den Webserver zu senden. Die Web App Firewall HTML SQL Injection Check bietet spezielle Schutzmaßnahmen gegen das Einschleusen von nicht autorisiertem SQL-Code, der die Sicherheit verletzen Wenn die Web App Firewall in einer Benutzeranforderung nicht autorisierten SQL-Code erkennt, wandelt sie die Anforderung entweder um, um den SQL-Code inaktiv zu machen, oder blockiert die Anforderung. Die Web App Firewall untersucht die Anforderungsnutzlast für injizierten SQL-Code an drei Orten: 1) POST-Text, 2) Header und 3) Cookies. Um einen Abfrageteil in Anfragen für injizierten SQL-Code zu untersuchen, konfigurieren Sie bitte eine Einstellung des Anwendungs-Firewall-Profils “InspectQueryContentTypes” für die spezifischen Inhaltstypen.

Ein Standardsatz von Schlüsselwörtern und Sonderzeichen enthält bekannte Schlüsselwörter und Sonderzeichen, die häufig zum Starten von SQL-Angriffen verwendet werden. Sie können neue Muster hinzufügen und den Standardsatz bearbeiten, um die SQL-Prüfung anzupassen. Die Web App Firewall bietet verschiedene Aktionsoptionen für die Implementierung des SQL Injection-Schutzes. Neben den Aktionen **Blockieren**, **Protokollieren**, **Statistiken** und **Lernen** bietet das Web App Firewall Profil auch die Möglichkeit, **SQL-Sonderzeichen umzuwandeln**, um einen Angriff unschädlich zu machen.

Zusätzlich zu den Aktionen gibt es mehrere Parameter, die für die SQL-Einschleusung-Verarbeitung konfiguriert werden können. Sie können nach **SQL-Platzhalterzeichen**suchen. Sie können den SQL-Einschleusung-Typ ändern und eine der 4 Optionen auswählen (**SqlKeyword,**SqlSPLChar****, **SqlSPLCharandKeyword**, **SqlSPLCharorKeyword**), um anzugeben, wie die SQL-Schlüsselwörter und SQL-Sonderzeichen bei der Verarbeitung der Nutzlast ausgewertet werden sollen. Der **Parameter SQL Comments Handling** bietet Ihnen die Möglichkeit, den Typ der Kommentare anzugeben, die bei der Erkennung von SQL Injection überprüft oder ausgenommen werden müssen.

Sie können Entspannungen einsetzen, um Fehlalarme zu vermeiden. Die Lernengine der Web App Firewall kann Empfehlungen zum Konfigurieren von Relaxationsregeln enthalten.

Zum Konfigurieren eines optimierten SQL Injection-Schutzes für Ihre Anwendung stehen folgende Optionen zur Verfügung:

Block—Die Blockaktion wird nur ausgelöst, wenn die Eingabe mit der SQL-Einschleusungstypspezifikation übereinstimmt. Wenn beispielsweise **SQLSplCharAndKeyword** als SQL-Einschleusungstyp konfiguriert ist, wird eine Anforderung nicht blockiert, wenn sie keine Schlüsselwörter enthält, selbst wenn SQL-Sonderzeichen in der Eingabe erkannt werden. Eine solche Anforderung wird blockiert, wenn der SQL-Einschleusungstyp entweder auf **SqlSPLChar**oder **SqlSPLCharorKeyword**festgelegt ist.

Log— Wenn Sie die Protokollfunktion aktivieren, generiert die SQL Injection-Prüfung Protokollmeldungen, die die ausgeführten Aktionen angeben. Wenn die Blockaktion deaktiviert ist, wird für jedes Eingabefeld, in dem der SQL-Verstoß festgestellt wurde, eine separate Protokollmeldung generiert. Allerdings wird nur eine Nachricht generiert, wenn die Anforderung blockiert wird. In ähnlicher Weise wird eine Protokollnachricht pro Anforderung für den Transformationsvorgang generiert, auch wenn SQL-Sonderzeichen in mehrere Felder umgewandelt werden. Sie können die Protokolle überwachen, um festzustellen, ob Antworten auf legitime Anfragen blockiert werden. Ein starker Anstieg der Anzahl der Protokollmeldungen kann auf Versuche hinweisen, einen Angriff zu starten.

Statistiken— Wenn diese Option aktiviert ist, sammelt die Statistikfunktion Statistiken zu Verstößen und Protokollen. Ein unerwarteter Anstieg im Statistikzähler deutet möglicherweise darauf hin, dass Ihre Anwendung angegriffen wird. Wenn legitime Anfragen blockiert werden, müssen Sie möglicherweise die Konfiguration erneut aufrufen, um zu sehen, ob Sie neue Entspannungsregeln konfigurieren oder die vorhandenen ändern müssen.

Lernen— Wenn Sie nicht sicher sind, welche SQL-Entspannungsregeln für Ihre Anwendung ideal geeignet sind, können Sie die Lernfunktion verwenden, um basierend auf den erlernten Daten

Empfehlungen zu generieren. Die Web App Firewall Learning Engine überwacht den Datenverkehr und gibt auf der Grundlage der beobachteten Werte Empfehlungen zum SQL-Lernen ab. Um einen optimalen Nutzen zu erzielen, ohne die Leistung zu beeinträchtigen, sollten Sie die Lernoption möglicherweise für kurze Zeit aktivieren, um ein repräsentatives Beispiel der Regeln zu erhalten, und dann die Regeln bereitstellen und das Lernen deaktivieren.

SQL-Sonderzeichen transformieren— Die Web App Firewall berücksichtigt drei Zeichen, einfaches, gerades Anführungszeichen (') (\), Backslash und Semikolon (;) als Sonderzeichen für die Verarbeitung der SQL-Sicherheitsprüfung. Die Funktion "SQL Transformation" ändert den SQL-Einschleusung-Code in einer HTML-Anforderung, um sicherzustellen, dass die Anforderung unschädlich gemacht wird. Die geänderte HTML-Anforderung wird dann an den Server gesendet. Alle standardmäßigen Transformationsregeln sind in der Datei /netscaler/default_custom_settings.xml angegeben.

Durch die Transformationsoperation wird der SQL-Code inaktiv, indem die folgenden Änderungen an der Anforderung vorgenommen werden:

- Einfaches gerades Anführungszeichen (') bis zum doppelten geraden Anführungszeichen (").
- Backslash (\) zu doppeltem Backslash (\).
- Semikolon (;) wird vollständig verworfen.

Diese drei Zeichen (spezielle Zeichenfolgen) sind notwendig, um Befehle an einen SQL-Server auszugeben. Sofern einem SQL-Befehl keine spezielle Zeichenfolge vorangestellt wird, ignorieren die meisten SQL-Server diesen Befehl. Daher verhindern die Änderungen, die die Web App Firewall bei aktivierter Transformation durchführt, dass ein Angreifer Active SQL injiziert. Nachdem diese Änderungen vorgenommen wurden, kann die Anfrage sicher an Ihre geschützte Website weitergeleitet werden. Wenn Webformulare auf Ihrer geschützten Website legitim spezielle SQL-Zeichenfolgen enthalten können, die Webformulare jedoch nicht auf die speziellen Zeichenfolgen angewiesen sind, um ordnungsgemäß zu funktionieren, können Sie die Blockierung deaktivieren und die Transformation aktivieren, um das Blockieren legitimer Webformulardaten zu verhindern, ohne den Schutz zu verringern, den Web App Firewall Ihren geschützten Websites bietet.

Der Transformationsvorgang funktioniert unabhängig von der Einstellung **"SQL Injection Type**". Wenn die Transformation aktiviert ist und der SQL Injection-Typ als SQL-Schlüsselwort angegeben wird, werden SQL-Sonderzeichen auch dann transformiert, wenn die Anforderung keine Schlüsselwörter enthält.

> **Tipp**
>
> Normalerweise aktivieren Sie entweder die Transformation oder das Blockieren, aber nicht beide. Wenn die Blockaktion aktiviert ist, hat sie Vorrang vor der Transformationsaktion. Wenn Sie die Blockierung aktiviert haben, ist die Aktivierung der Transformation redundant.

Auf SQL-Platzhalterzeichen suchen — Wildcard-Zeichenkönnen verwendet werden, um die Auswahl einer SQL-Anweisung (SQL-SELECT) zu erweitern. Diese Wildcard-Operatoren können mit

den Operatoren **LIKE** und **NOT LIKE** verwendet werden, um einen Wert mit ähnlichen Werten zu vergleichen. Die Prozentzeichen (%) und Unterstriche (_) werden häufig als Platzhalter verwendet. Das Prozentzeichen entspricht dem Sternchen-Platzhalterzeichen (*), das mit MS-DOS verwendet wird, und entspricht null, einem oder mehreren Zeichen in einem Feld. Der Unterstrich ähnelt dem MS-DOS-Fragezeichen (?) Platzhalterzeichen. Es stimmt mit einer einzelnen Zahl oder einem Zeichen in einem Ausdruck überein.

Sie können beispielsweise die folgende Abfrage verwenden, um eine Zeichenfolgensuche durchzuführen, um alle Kunden zu finden, deren Namen das D-Zeichen enthalten.

WÄHLEN Sie* vom Kunden WHERE-Namen wie "%D%":

Im folgenden Beispiel werden die Operatoren kombiniert, um Gehaltswerte zu finden, die an zweiter und dritter Stelle 0 haben.

WÄHLEN Sie* vom Kunden WHERE Gehalt wie '_ 00% ':

Verschiedene DBMS-Anbieter haben die Platzhalterzeichen um zusätzliche Operatoren erweitert. Die Citrix Web App Firewall kann vor Angriffen schützen, die durch das Eingeben dieser Platzhalterzeichen gestartet werden. Die 5 standardmäßigen Platzhalterzeichen sind Prozent (%), Unterstrich (_), Caret (^), öffnende Klammer ([) und schließende Klammer (]). Dieser Schutz gilt sowohl für HTML- als auch für XML-Profile.

Die Standard-Platzhalterzeichen sind eine Liste von Literalen, die in der ***Standardsignaturen angegeben sind**:

- `<wildchar type="LITERAL">%</wildchar>`
- `<wildchar type="LITERAL">_</wildchar>`
- `<wildchar type="LITERAL">^</wildchar>`
- `<wildchar type="LITERAL">[</wildchar>`
- `<wildchar type="LITERAL">]</wildchar>`

Platzhalterzeichen in einem Angriff können PCRE sein, wie [^A-F]. Die Web App Firewall unterstützt auch PCRE-Platzhalter, aber die obigen Platzhalterzeichen reichen aus, um die meisten Angriffe zu blockieren.

> **Hinweis:**
>
> Die SQL-Platzhalterzeichenprüfung unterscheidet sich von der SQL-Sonderzeichenprüfung. Diese Option muss mit Vorsicht verwendet werden, um Fehlalarme zu vermeiden.

Check Request mit SQL-Einschleusung-Typ— Die Web App Firewall bietet 4 Optionen, um die gewünschte Strenge für die SQL Injection-Prüfung basierend auf den individuellen Anforderungen der Anwendung zu implementieren. Die Anforderung wird mit der Spezifikation des Injektionstyps zur Erkennung von SQL-Verletzungen abgeglichen. Die 4 Optionen für den SQL-Einschleusung-Typ sind:

- **SQL-Sonderzeichen und -Schlüsselwort**— Sowohl ein SQL-Schlüsselwort als auch ein SQL-Sonderzeichen müssen in der Eingabe vorhanden sein, um eine SQL-Verletzung auszulösen. Diese am wenigsten restriktive Einstellung ist auch die Standardeinstellung.
- **SQL-Sonderzeichen**—Mindestens eines der Sonderzeichen muss in der Eingabe vorhanden sein, um eine SQL-Verletzung auszulösen.
- **SQL-Schlüsselwort**— Mindestens eines der angegebenen SQL-Schlüsselwörter muss in der Eingabe vorhanden sein, um eine SQL-Verletzung auszulösen. Wählen Sie diese Option nicht ohne angemessene Berücksichtigung aus. Um Fehlalarme zu vermeiden, stellen Sie sicher, dass keines der Schlüsselwörter in den Eingaben erwartet wird.
- **SQL-Sonderzeichen oder Schlüsselwort**—Entweder das Schlüsselwort oder die Sonderzeichenfolge muss in der Eingabe vorhanden sein, um die Sicherheitsüberprüfungsverletzung auszulösen.

> **Tipp:**
>
> Wenn Sie die Web App Firewall so konfigurieren, dass sie nach Eingaben suchen, die ein SQL-Sonderzeichen enthalten, überspringt die Web App-Firewall Webformularfelder, die keine Sonderzeichen enthalten. Da die meisten SQL-Server keine SQL-Befehle verarbeiten, denen kein Sonderzeichen vorangestellt ist, kann die Aktivierung dieser Option die Web App Firewall erheblich entlasten und die Verarbeitung beschleunigen, ohne dass Ihre geschützten Websites gefährdet werden.

Verarbeitung von SQL-Kommentaren— Standardmäßig prüft die Web App Firewall alle SQL-Kommentare auf injizierte SQL-Befehle. Viele SQL-Server ignorieren jedoch alles in einem Kommentar, auch wenn ein SQL-Sonderzeichen vorangestellt ist. Für eine schnellere Verarbeitung, wenn Ihr SQL-Server Kommentare ignoriert, können Sie die Web App Firewall so konfigurieren, dass Kommentare übersprungen werden, wenn Sie Anforderungen für injiziertes SQL prüfen. Die Optionen für die Verarbeitung von SQL-Kommentaren sind:

- **ANSI**—Überspringt SQL-Kommentare im ANSI-Format, die normalerweise von UNIX-basierten SQL-Datenbanken verwendet werden. Beispiel:
  - — (Zwei Bindestriche) - Dies ist ein Kommentar, der mit zwei Bindestrichen beginnt und mit Zeilenende endet.
  - {} - Klammern (Klammern umschließen den Kommentar. Das {steht vor dem Kommentar und das} folgt ihm. Klammern können ein- oder mehrzeilige Kommentare abgrenzen, Kommentare können jedoch nicht verschachtelt werden)
  - `/**/: C style comments (Does not allow nested comments). Please note /*! <comment that begin with slash followed by asterisk and exclamation mark is not a comment > */`
  - MySQL Server unterstützt einige Varianten von Kommentaren im C-Stil. Diese ermöglichen es Ihnen, Code zu schreiben, der MySQL Erweiterungen enthält, aber immer noch portabel ist, indem Sie Kommentare der folgenden Form verwenden: `/*! MySQL-specific`


```
code */
```

  - . #: Mysql-Kommentare: Dies ist ein Kommentar, der mit dem Zeichen # beginnt.
- **Verschachtelt**— Verschachtelte SQL-Kommentare überspringen, die normalerweise von Microsoft SQL Server verwendet werden. Zum Beispiel; — (Zwei Bindestriche) und **/* */** (Erlaubt verschachtelte Kommentare)
- **ANSI/verschachtelt**—Überspringen Sie Kommentare, die sowohl den ANSI- als auch den verschachtelten SQL-Kommentarstandards entsprechen. Kommentare, die nur dem ANSI-Standard oder nur dem verschachtelten Standard entsprechen, werden weiterhin auf injizierte SQL überprüft.
- **Alle Kommentare überprüfen**— Überprüfen Sie die gesamte Anforderung für injiziertes SQL, ohne etwas zu überspringen. Dies ist die Standardeinstellung.

> **Tipp**
>
> Normalerweise dürfen Sie die Option Verschachtelt oder ANSI/Verschachtelt nicht wählen, es sei denn, Ihre Back-End-Datenbank wird auf Microsoft SQL Server ausgeführt. Die meisten anderen Typen von SQL Server-Software erkennen verschachtelte Kommentare nicht. Wenn verschachtelte Kommentare in einer Anfrage erscheinen, die an einen anderen SQL-Servertyp gerichtet ist, deuten sie möglicherweise auf einen Versuch hin, die Sicherheit auf diesem Server zu verletzen.

Request-Header prüfen— Aktivieren Sie diese Option, wenn Sie nicht nur die Eingabe in den Formularfeldern untersuchen, sondern auch die Anforderungsheader auf HTML-SQL-Einschleusung-Angriffe untersuchen möchten. Wenn Sie die GUI verwenden, können Sie diesen Parameter im Bereich **Erweiterte Einstellungen** -> **Profileinstellungen** des Web App Firewall Profils aktivieren.

> **Hinweis:**
>
> Wenn Sie das Header-Flag “Anforderung prüfen” aktivieren, müssen Sie möglicherweise eine Entspannungsregel für den **User-Agent-Header** konfigurieren. Das Vorhandensein des SQL-Schlüsselworts **like** und des SQL-Sonderzeichens Semikolon (**;**) kann falsch positive und Blockanforderungen auslösen, die diesen Header enthalten.
>
> **Warnung**
>
> Wenn Sie sowohl die Überprüfung des Anforderungsheaders als auch die Transformation aktivieren, werden alle SQL-Sonderzeichen in den Kopfzeilen ebenfalls transformiert. Die Header Accept, Accept-Charset, Accept-Encoding, Accept-Language, Expect und User-Agent enthalten normalerweise Semikolons (;). Die gleichzeitige Aktivierung von Request-Header-Überprüfung und Transformation kann zu Fehlern führen

inspectQueryContentTypes — Konfigurieren Sie diese Option, wenn Sie den Teil der Anforderungsabfrage auf SQL-Einschleusung-Angriffe auf bestimmte Inhaltstypen untersuchen möchten. Wenn Sie die GUI verwenden, können Sie diesen Parameter im Bereich **Erweiterte Einstellungen** -> **Profileinstellungen** des App Firewall-Profils konfigurieren.

SQL Feinkörnige Entspannungen

Die Web App Firewall bietet Ihnen die Möglichkeit, ein bestimmtes Formularfeld, einen Header oder ein Cookie von der SQL Injection-Prüfung auszunehmen. Sie können die Prüfung für eines oder mehrere dieser Felder vollständig Bypass, indem Sie die Entspannungsregeln für die SQL Injection-Prüfung konfigurieren.

Mit der Web App Firewall können Sie durch Feinabstimmung der Entspannungsregeln strengere Sicherheit implementieren. Eine Anwendung erfordert möglicherweise die Flexibilität, um bestimmte Muster zuzulassen, aber die Konfiguration einer Relaxationsregel zum Umgehen der Sicherheitsprüfung kann die Anwendung anfällig für Angriffe machen, da das Zielfeld von der Prüfung auf SQL-Angriffsmuster ausgenommen ist. Die feinkörnige SQL-Entspannung bietet die Möglichkeit, bestimmte Muster zuzulassen und den Rest zu blockieren. Beispielsweise verfügt die Web App Firewall derzeit über einen Standardsatz von mehr als 100 SQL-Schlüsselwörtern. Da Hacker diese Schlüsselwörter in SQL Injection-Angriffen verwenden können, kennzeichnet die Web App Firewall sie als potenzielle Bedrohungen. Sie können ein oder mehrere Keywords entspannen, die für den bestimmten Standort als sicher gelten. Die restlichen potenziell gefährlichen SQL-Schlüsselwörter werden weiterhin auf den Zielspeicherort überprüft und lösen weiterhin die Sicherheitsüberprüfungsverstöße aus. Sie haben jetzt eine viel strengere Kontrolle.

Die in Relaxationen verwendeten Befehle haben optionale Parameter für **Value Type** und **Value Expression**. Sie können angeben, ob der Wertausdruck ein regulärer Ausdruck oder eine literale Zeichenfolge ist. Der Werttyp kann leer gelassen werden oder Sie haben die Möglichkeit, **Keyword** oder **SpecialString** oder **WildChar** auszuwählen.

> **Warnung:**
>
> Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht genau vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau die URL definieren, die Sie als Ausnahme hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung von Platzhaltern und insbesondere der Punkt-Sternchen (.*) -Metazeichen- oder Platzhalterkombination kann zu Ergebnissen führen, die Sie nicht möchten, z. B. das Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten, oder einen Angriff zulassen, den die HTML SQL Injection-Prüfung sonst blockiert hätte.

Zu berücksichtigende Punkte:

- Der Wertausdruck ist ein optionales Argument. Ein Feldname hat möglicherweise keinen Wertausdruck.
- Ein Feldname kann an Ausdrücke mit mehreren Werten gebunden werden.
- Wertausdrücken muss ein Werttyp zugewiesen werden. Der SQL-Werttyp kann sein: 1) Schlüsselwort, 2) SpecialString oder 3) WildChar.
- Sie können mehrere Entspannungsregeln pro Feldname/URL-Kombination festlegen.

Verwenden der Befehlszeile zum Konfigurieren der SQL Injection Check

So konfigurieren Sie SQL Injection-Aktionen und andere Parameter mithilfe der Befehlszeile:

In der Befehlszeilenschnittstelle können Sie entweder den Befehl **set appfw profile** oder den Befehl **add appfw profile** verwenden, um den SQL Injection-Schutz zu konfigurieren. Sie können die Block-, Learn-, Log-Aktionen und Statistiken aktivieren und angeben, ob Sie die in SQL Injection-Angriffszeichenfolgen verwendeten Sonderzeichen transformieren möchten, um den Angriff zu deaktivieren. Wählen Sie den Typ des SQL-Angriffsmusters (Schlüsselwörter, Platzhalterzeichen, spezielle Zeichenfolgen) aus, den Sie in den Payloads erkennen möchten, und geben Sie an, ob die Web App Firewall auch die Anforderungskopfzeilen auf Verletzungen von SQL Injection überprüfen soll. Verwenden Sie den Befehl **unset appfw profile**, um die konfigurierten Einstellungen auf ihre Standardeinstellungen zurückzusetzen. Jeder der folgenden Befehle legt nur einen Parameter fest, aber Sie können mehrere Parameter in einen einzelnen Befehl aufnehmen:

- legen Sie das Anwendungs-Firewall-Profil fest “Parameterbeschreibungen unten auf der Seite. “
- <name> -SQLInjectionAction ([block] [learn] [log] [stats])| [none])
- legen Sie das Anwendungs-Firewall-Profil fest “Parameterbeschreibungen unten auf der Seite. “
- <name> -SQLInjectionTransformSpecialChars (**ON** | OFF)
- legen Sie das Anwendungs-Firewall-Profil fest “Parameterbeschreibungen unten auf der Seite. “
- <name> -**SQLInjectionCheckSQLWildChars** (**ON** |**OFF**)
- legen Sie das Anwendungs-Firewall-Profil fest “Parameterbeschreibungen unten auf der Seite. “
- **<name> -**SQLInjectionType** ([**SQLKeyword**] | [**SQLSplChar**] | [**SQLSplCharANDKeyword**] | [**SQLSplCharORKeyword**])
- **legen Sie das Anwendungs-Firewall-Profil** fest “Parameterbeschreibungen unten auf der Seite. “
- <name> -**SQLInjectionParseComments** ([**checkall**] | [**ansi|nested **] | [**ansinested**])
- **legen Sie das Anwendungs-Firewall-Profil fest “Parameterbeschreibungen unten auf der Seite. “
- <name> -CheckRequestHeaders (ON | OFF) Parameterbeschreibungen unten auf der Seite.
- <name> - CheckRequestQueryNonHtml (ON | OFF) Parameterbeschreibungen unten auf der Seite.

So konfigurieren Sie eine SQL Injection-Entspannungsregel mit der Befehlszeilenschnittstelle

Verwenden Sie den Befehl bind oder unbind, um die Bindung wie folgt hinzuzufügen oder zu löschen:

- `bind appfw profile <name> -SQLInjection <String> [isRegex(REGEX|NOTREGE)] <formActionURL> [-location <location>] [-valueType (Keywor|SpecialString|Wildchar)[<valueExpression>][-isValueRegex (REGEX | NOTREGEX)]]`
- `unbind appfw profile <name> -SQLInjection <String> <formActionURL> [-location <location>] [-valueTyp (Keyword|SpecialString|Wildchar)[<valueExpression>]]`

> **Hinweis:**
>
> Sie können die Liste der SQL-Schlüsselwörter aus dem Inhalt der Standardsignaturdatei finden, indem Sie das View-Signaturobjekt anzeigen, das eine Liste von SQL-Schlüsselwörtern und SQL-Sonderzeichen enthält.

Verwenden der GUI zum Konfigurieren der SQL Injection Security Check

In der GUI können Sie die Sicherheitsüberprüfung von SQL Injection im Bereich für das mit Ihrer Anwendung verknüpfte Profil konfigurieren.

So konfigurieren oder ändern Sie die SQL Injection-Prüfung mit der GUI

1. Navigieren Sie zu **Application Firewall > Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Sicherheitsprüfungen**.

In der Tabelle zur Sicherheitsüberprüfung werden die aktuell konfigurierten Aktionseinstellungen für alle Sicherheitsüberprüfungen angezeigt. Sie haben 2 Möglichkeiten für die Konfiguration:

a. Wenn Sie Block-, Log-, Statistiken- und Lernaktionen für HTML SQL Injection aktivieren oder deaktivieren möchten, können Sie die Kontrollkästchen in der Tabelle aktivieren oder deaktivieren, auf **OK**klicken und dann auf **Speichern und Schließen** klicken, um den Bereich **Sicherheitsprüfung** zu schließen.

b. Wenn Sie weitere Optionen für diese Sicherheitsprüfung konfigurieren möchten, doppelklicken Sie auf HTML SQL Injection oder wählen Sie die Zeile aus und klicken Sie auf **Aktionseinstellungen**, um die folgenden Optionen anzuzeigen:

SQL-Sonderzeichentransformieren —Transformieren Sie alle SQL-Sonderzeichen in der Anforderung.

Auf**SQL-Platzhalterzeichen prüfen**— Betrachten Sie SQL-Platzhalterzeichen in der Nutzlast als Angriffsmuster.

Überprüfen Sie die Anforderung mit—Type der SQL-Einschleusung (SqlKeyword, SqlSplChar, SqlSplcharandKeyword oder SqlSplcharorKeyword), die überprüft werden soll.

SQL Comments Handling— Art der zu prüfenden Kommentare (Alle Kommentare prüfen, ANSI, Verschachtelt oder ANSI/verschachtelt).

Nachdem Sie eine der obigen Einstellungen geändert haben, klicken Sie auf **OK**, um die Änderungen zu speichern und zur Tabelle Sicherheitsüberprüfungen zurückzukehren. Sie können bei Bedarf weitere Sicherheitsprüfungen konfigurieren. Klicken Sie auf **OK**, um alle Änderungen zu speichern, die Sie im Abschnitt Sicherheitsprüfungen vorgenommen haben, und klicken Sie dann auf **Speichern und schließen**, um den Bereich Sicherheitsüberprüfung zu schließen.

So konfigurieren Sie eine Regel zur Entspannung von SQL Injection über die GUI

- Navigieren Sie zu **Application Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
- Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Relaxationsregeln**.
- Doppelklicken Sie in der Tabelle Entspannungsregeln auf den Eintrag " **HTML SQL Injection** " oder wählen Sie ihn aus und klicken Sie auf **Bearbeiten**.
- Führen **Sie im Dialogfeld "Entspannungsregeln für HTML SQL Injection** " Vorgänge zum **Hinzufügen**, **Bearbeiten**, **Löschen**, **Aktivieren**oder **Deaktivieren** für Entspannungsregeln aus.

> **Hinweis**
>
> Wenn Sie eine neue Regel hinzufügen, wird das Feld **Wertausdruck** nur angezeigt, wenn Sie im Feld **Werttyp** die Option **Schlüsselwort** oder **SpecialString** oder **WildChar** auswählen.

So verwalten Sie Regeln zur Entspannung von SQL-Einschleusung mit dem Visualizer

Um eine konsolidierte Ansicht aller Relaxationsregeln zu erhalten, können Sie die Zeile **HTML SQL Injection** markieren und auf **Visualizer** klicken. Der Visualizer für bereitgestellte Relaxationen bietet Ihnen die Möglichkeit, eine neue Regel **hinzuzufügen** oder eine vorhandene zu **bearbeiten** . Sie können auch eine Gruppe von Regeln **aktivieren** oder **deaktivieren**, indem Sie einen Knoten auswählen und auf die entsprechenden Schaltflächen im Relaxationsvisualizer klicken.

Anzeigen oder Anpassen von Einschleusungsmustern über die grafische Benutzeroberfläche

Sie können die GUI verwenden, um die Einschleusungsmuster anzuzeigen oder anzupassen.

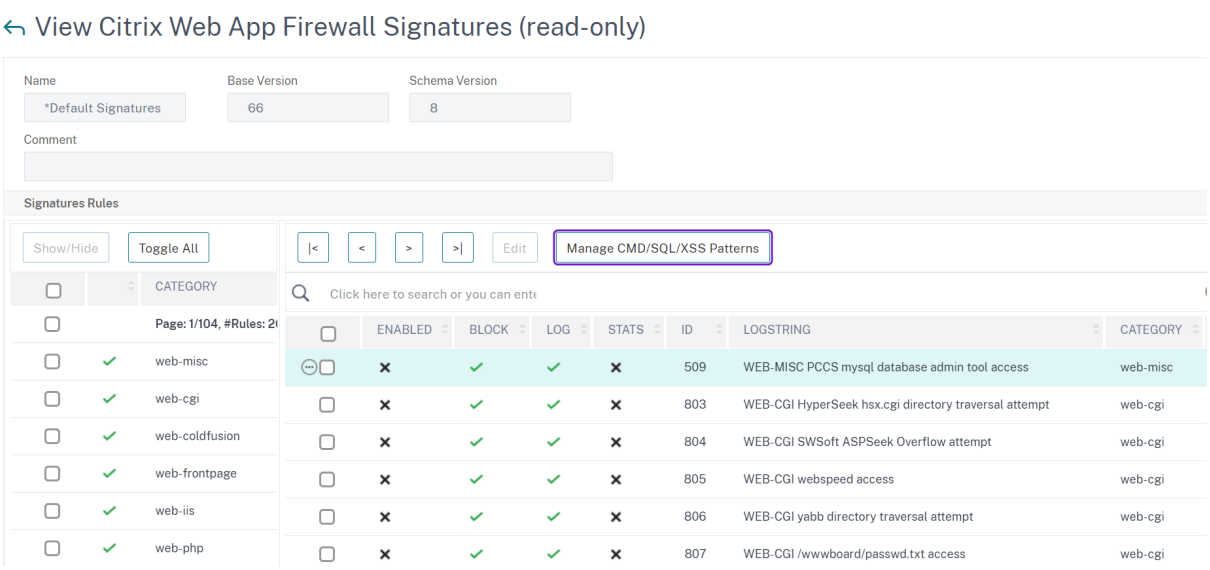
Die Standard-SQL-Muster sind in der Standardsignaturdatei angegeben. Wenn Sie kein Signaturobjekt an Ihr Profil binden, werden die im Standardsignaturobjekt angegebenen Standard-Injection-Pattern vom Profil für die Verarbeitung der Sicherheitsprüfung des Befehls verwendet. Die im Standardsignaturobjekt angegebenen Regeln und Muster sind schreibgeschützt. Sie können sie nicht bearbeiten oder ändern. Wenn Sie diese Muster ändern oder ändern möchten, erstellen Sie eine Kopie des Standardobjekts sSignatures, um ein benutzerdefiniertes Signaturobjekt zu erstellen. Nehmen Sie Änderungen an den Befehlseinschleusungsmustern im neuen benutzerdefinierten Signaturobjekt vor

und verwenden Sie dieses Signaturobjekt in Ihrem Profil, das den Datenverkehr verarbeitet, für den Sie diese benutzerdefinierten Muster verwenden möchten.

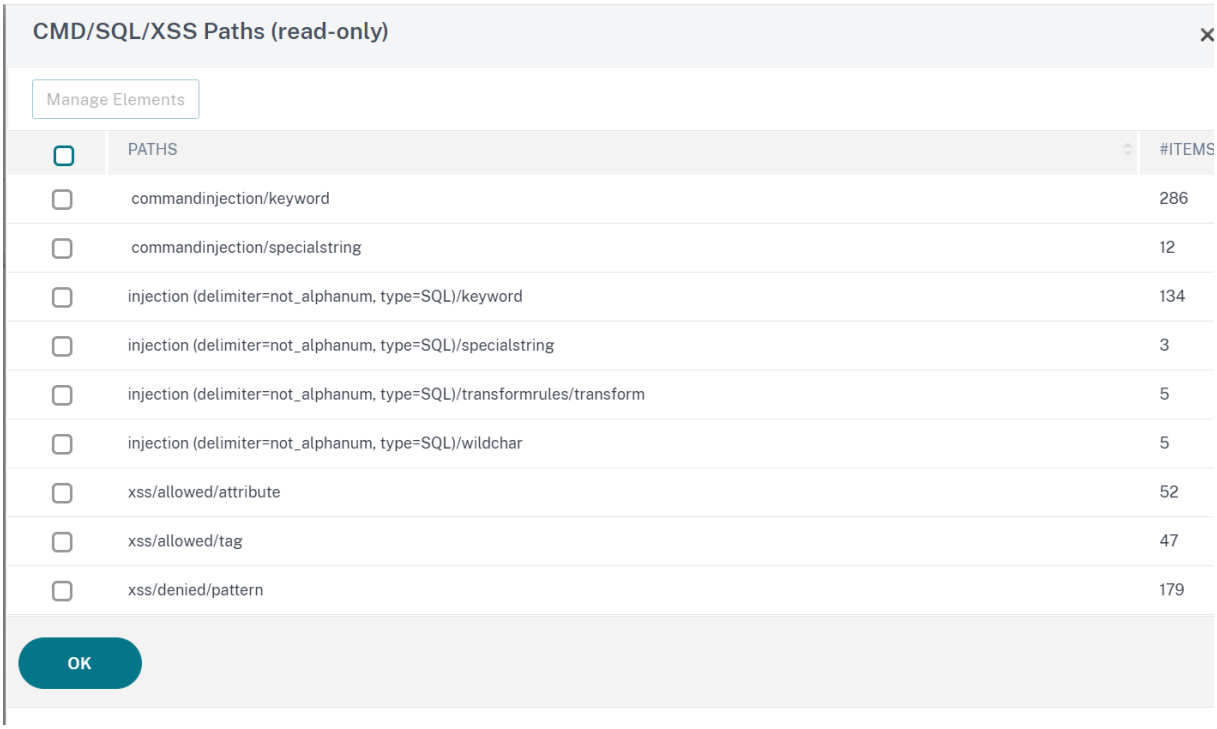
Weitere Informationen finden Sie unter Signaturen

So zeigen Sie die Standard-Einschleusungsmuster mit der GUI an:

1. Navigieren Sie zu **Application Firewall > Signaturen**, wählen Sie ***Standardsignaturen**aus und klicken Sie auf **Bearbeiten**.



1. Klicken Sie auf **CMD/SQL/XSS-Muster verwalten**. Die Tabelle **SQL/Cross-Site-Skriptpfade verwalten** zeigt Muster in Bezug auf CMD/SQL/XS-Einschleusung:



1. Wählen Sie eine Zeile aus und klicken Sie auf **Elemente verwalten**, um die entsprechenden Einschleusungsmuster (Schlüsselwörter, spezielle Zeichenfolgen, Transformationsregeln oder die Platzhalterzeichen) anzuzeigen, die von der Injection-Prüfung des Befehls Web App Firewall verwendet werden.

Verwenden der Lernfunktion mit der SQL Injection Check

Wenn die Lernaktion aktiviert ist, überwacht die Web App Firewall Learning Engine den Datenverkehr und lernt die ausgelösten Verstöße. Sie können diese gelernten Regeln regelmäßig überprüfen. Nach entsprechender Prüfung können Sie die gelernte Regel als eine Relaxierungsregel für SQL-Einschleusung bereitstellen.

SQL Injection Learning Enhancement— Eine Lernerweiterung für die Web App Firewall wurde in Version 11.0 der Citrix ADC Software eingeführt. Um eine feinkörnige SQL Injection-Entspannung bereitzustellen, bietet die Web App Firewall feinkörniges SQL Injection-Lernen. Die Lern-Engine gibt Empfehlungen bezüglich des beobachteten Werttyps (Schlüsselwort, SpecialString, Wildchar) und des entsprechenden Value-Ausdrucks, der in den Eingabefeldern beobachtet wird. Zusätzlich zur Überprüfung der blockierten Anforderungen, um festzustellen, ob die aktuelle Regel zu restriktiv ist und gelockert werden muss, können Sie die von der Lern-Engine generierten Regeln überprüfen, um festzustellen, welcher Werttyp und welcher Werteausdruck Verstöße auslösen und in den Relaxationsregeln behandelt werden müssen.

> **Wichtig**
>
> Die Lern-Engine der Web App Firewall kann nur die ersten 128 Byte des Namens unterscheiden. Wenn ein Formular mehrere Felder mit Namen enthält, die für die ersten 128 Bytes übereinstimmen, kann die Lern-Engine möglicherweise nicht zwischen ihnen unterscheiden. In ähnlicher Weise kann die bereitgestellte Relaxationsregel versehentlich alle Felder von der SQL Injection Inspektion entspannen.
>
> **Hinweis** Um das SQL zu Bypass, indem Sie den User-Agent-Header einchecken, verwenden Sie die folgende Entspannungsregel:
>
> ```
> bind appfw profile your_profile_name -SQLInjection User-Agent ".*"-
> location HEADER
> ```

So zeigen Sie gelernte Daten mit der Befehlszeilenschnittstelle an oder verwenden

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- `show appfw learningdata <profilename> SQLInjection`
- `rm appfw learningdata <profilename> -SQLInjection <string> <formActionURL > [<location>] [<valueType> <valueExpression>]`
- `export appfw learningdata <profilename> SQLInjection`

So zeigen Sie erlernte Daten mit der GUI an oder verwenden sie

1. Navigieren Sie zu **Application Firewall > Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **“Erweiterte Einstellungen** “ auf **Gelernte Regeln**. Sie können den Eintrag **HTML SQL Injection** in der Tabelle Gelernte Regeln auswählen und darauf doppelklicken, um auf die erlernten Regeln zuzugreifen. Sie können die erlernten Regeln bereitstellen oder eine Regel bearbeiten, bevor Sie sie als Entspannungsregel bereitstellen. Um eine Regel zu verwerfen, können Sie sie auswählen und auf die Schaltfläche **Überspringen** klicken. Sie können jeweils nur eine Regel bearbeiten, aber Sie können mehrere Regeln zum Bereitstellen oder Überspringen auswählen.

Sie haben auch die Möglichkeit, eine zusammengefasste Ansicht der gelernten Entspannungen anzuzeigen, indem Sie den Eintrag **HTML SQL Injection** in der Tabelle Learned Rules auswählen und auf **Visualizer** klicken, um eine konsolidierte Ansicht aller gelernten Verletzungen zu erhalten. Der Visualizer macht es einfach, die erlernten Regeln zu verwalten. Es bietet eine umfassende Ansicht der Daten auf einem Bildschirm und erleichtert das Ergreifen einer Gruppe von Regeln mit einem Klick. Der größte Vorteil des Visualizers besteht darin, dass reguläre Ausdrücke empfohlen werden, um mehrere Regeln zu konsolidieren. Sie können eine Teilmenge dieser Regeln basierend auf dem Trennzeichen und der Aktions-URL auswählen. Sie können 25, 50 oder 75 Regeln im Visualizer anzeigen, indem Sie die Zahl aus einer Dropdown-Liste auswählen. Der Visualizer für erlernte Regeln bietet die Möglichkeit, die Regeln zu bearbeiten und als Entspannungen einzusetzen. Oder Sie können die Regeln überspringen, um sie zu ignorieren.

Verwenden der Protokollfunktion mit der SQL Injection Check

Wenn die Protokollaktion aktiviert ist, werden die Verletzungen der Sicherheitsüberprüfung von HTML SQL Injection als **APPFW_SQL-Verletzungen** im Überwachungsprotokoll protokolliert. Die Web App Firewall unterstützt sowohl native als auch CEF-Protokollformate. Sie können die Protokolle auch an einen Remote-Syslog-Server senden.

So greifen Sie mit der Befehlszeile auf die Protokollmeldungen zu

Wechseln Sie zur Shell und schließen Sie die ns.logs im Ordner **/var/log/**, um auf die Protokollmeldungen zuzugreifen, die sich auf die SQL Injection-Verstöße beziehen:

```
> Shell

## tail -f /var/log/ns.log | grep APPFW_SQL
```

Beispiel für eine HTML SQL Injection-Protokollmeldung, wenn die Anforderung transformiert wird


```
1 Jun 26 21:08:41 <local0.info> 10.217.31.98 CEF:0|Citrix|Citrix ADC|NS11
    .0|APPFW|APPFW_SQL|6|src=10.217.253.62 geolocation=Unknown spt=54001
     method=GET request=http://aaron.stratum8.net/FFC/login.php?
    login_name=%27+or&passwd=and+%3B&drinking_pref=on&text_area=select
    +*+from+%5C+%3B&loginButton=ClickToLogin&as_sfid=AAAAAAXjnGN5gLH-
    hvhTOpIySEIqES7BjFRs5Mq0fwPp-3ZHDi5yWlRWByj0cVbMyy-
    Ens2vaaiULKOcUri4OD4kbXWwSY5s7I3QkDsrvIgCYMC9BMvBwY2wbNcSqCwk52lfE0k
    %3D&as_fid=feeec8758b41740eedeeb6b35b85dfd3d5def30c msg= Special
    characters seen in fields cn1=74 cn2=762 cs1=pr_ffc cs2=PPE1 cs3=9
    ztIlf9p1H7p6Xtzn6NMygTv/QM0002 cs4=ALERT cs5=2015 act=transformed
2 <!--NeedCopy-->
```

Beispiel für eine HTML SQL Injection-Protokollmeldung, wenn die Post-Anforderung blockiert ist

```
1 Jun 26 21:30:34 <local0.info> 10.217.31.98 CEF:0|Citrix|Citrix ADC|NS11
    .0|APPFW|APPFW_SQL|6|src=10.217.253.62 geolocation=Unknown spt=9459
    method=POST request=http://aaron.stratum8.net/FFC/login_post.php msg
    =SQL Keyword check failed for field text_area=”(')” cn1=78 cn2=834
    cs1=pr_ffc cs2=PPE1 cs3=eVJMMPtZ2XgylGrHjkx3rZLfBCI0002 cs4=ALERT
    cs5=2015 act=blocked
2 <!--NeedCopy-->
```

Hinweis

Im Rahmen der Streaming-Änderungen in 10.5.e Builds (Enhancement Builds) und 11.0 Build on wards verarbeiten wir die Eingabedaten jetzt in Blöcken. RegEx Pattern-Matching ist jetzt für zusammenhängende Zeichenfolgen auf 4K beschränkt. Mit dieser Änderung können die SQL-Verstoßprotokollmeldungen andere Informationen im Vergleich zu früheren Builds enthalten. Das Schlüsselwort und das Sonderzeichen in der Eingabe können durch viele Bytes getrennt werden. Wir behalten nun den Überblick über die SQL-Schlüsselwörter und spezielle Zeichenfolgen bei der Verarbeitung der Daten, anstatt den gesamten Eingabewert zu puffern. Zusätzlich zum Feldnamen enthält die Protokollnachricht jetzt das SQL-Schlüsselwort oder das SQL-Sonderzeichen oder sowohl das SQL-Schlüsselwort als auch das SQL-Sonderzeichen, wie in der konfigurierten Einstellung festgelegt. Der Rest der Eingabe ist nicht mehr in der Protokollnachricht enthalten, wie im folgenden Beispiel gezeigt:

Beispiel:

Wenn die Web App Firewall die SQL-Verletzung erkennt, wird in 10.5 möglicherweise die gesamte Eingabezeichenfolge in die Protokollmeldung aufgenommen, wie unten dargestellt:

```
SQL Keyword check failed for field text=\”select a name from testbed1
```



> ```
> ;(;)\".*<blocked>
> ```
>
> In den Erweiterungs-Builds von 10.5.e, die anforderungsseitiges Streaming und ab Build 11.0, protokollieren wir nur den Feldnamen, das Schlüsselwort und das Sonderzeichen (falls zutreffend) in der Protokollnachricht, wie unten gezeigt:
>
> ```
> SQL Keyword check failed for field **text="select(;)"<blocked>
> ```
>
> Diese Änderung gilt für Anforderungen, die Anwendung/x-www-form-urlencodedoder Multipart/Form-Daten oder Text-/x-gwt-rpc Inhaltstypen enthalten. Protokollmeldungen, die während der Verarbeitung von **JSON** - oder **XML-Nutzdaten** generiert werden, sind von dieser Änderung nicht betroffen.

So greifen Sie mit der GUI auf die Protokollmeldungen zu

Die Citrix GUI enthält ein nützliches Tool (**Syslog Viewer**) zum Analysieren der Protokollmeldungen. Sie haben mehrere Optionen für den Zugriff auf den Syslog Viewer:

- Navigieren Sie zu **Application Firewall** > **Profile**, wählen Sie das Zielprofil aus und klicken Sie auf **Sicherheitsüberprüfungen**. Markieren Sie die Zeile **HTML SQL Injection**, und klicken Sie auf **Protokolle** Wenn Sie direkt von der HTML-SQL-Einschleusung-Prüfung des Profils auf die Protokolle zugreifen, filtert die GUI die Protokollmeldungen heraus und zeigt nur die Protokolle an, die zu diesen Verstößen gegen die Sicherheitsüberprüfung gehören.
- Sie können auch auf den Syslog Viewer zugreifen, indem Sie zu **Citrix ADC** > **System** > **Auditing** navigieren. Klicken Sie im Abschnitt Überwachungsmeldungen auf den Link **Syslog-Meldungen**, um den Syslog-Viewer anzuzeigen, in dem alle Protokollmeldungen einschließlich anderer Protokolle über Sicherheitsüberprüfungen angezeigt werden. Dies ist nützlich für das Debuggen, wenn während der Anforderungsverarbeitung mehrere Sicherheitsüberprüfungen ausgelöst werden können.
- Navigieren Sie zu **Application Firewall** > **Richtlinien** > **Überwachung**. Klicken Sie im Abschnitt Überwachungsmeldungen auf den Link **Syslog-Meldungen**, um den Syslog-Viewer anzuzeigen, in dem alle Protokollmeldungen einschließlich anderer Protokolle über Sicherheitsüberprüfungen angezeigt werden.

Der HTML-basierte Syslog Viewer bietet verschiedene Filteroptionen, um nur die Protokollmeldungen auszuwählen, die für Sie von Interesse sind. Um Protokollmeldungen für die **HTML-SQL-Einschleusung-Prüfung** auszuwählen, filtern Sie, indem Sie **APPFW** in der Dropdownliste auswählen Optionen für **Module**. Die Liste **Ereignistyp** bietet eine Reihe von Optionen, um Ihre Auswahl weiter zu verfeinern. Wenn Sie beispielsweise das Kontrollkästchen **APPFW_SQL** aktivieren und auf die Schaltfläche **Übernehmen** klicken, werden im Syslog-Viewer nur Protokollmeldungen angezeigt, die zu den Verletzungen der **SQL Injection-Sicherheitsüberprüfung** gehören.

Wenn Sie den Cursor in die Zeile für eine bestimmte Protokollnachricht setzen, werden mehrere Optionen wie **Modul**, **Ereignistyp**, **Ereignis-ID**, **Client-IP** usw. unterhalb der Protokollmeldung angezeigt. Sie können eine dieser Optionen auswählen, um die entsprechenden Informationen in

der Protokollmeldung hervorzuheben.

Die Funktion**“Zum Bereitstellen klicken”** ist nur in der GUI verfügbar. Sie können den Syslog-Viewer nicht nur zum Anzeigen der Protokolle verwenden, sondern auch zum Bereitstellen von Entspannungsregeln für HTML SQL Injection basierend auf den Protokollmeldungen für Verstöße gegen die Sicherheitsüberprüfung der Web App Firewall. Die Protokollmeldungen müssen für diesen Vorgang im CEF-Protokollformat vorliegen. Die Funktion zum Bereitstellen klicken ist nur für Protokollmeldungen verfügbar, die durch die Blockierung (oder nicht Blockierung) generiert wurden. Sie können keine Entspannungsregel für eine Protokollmeldung über den Transformationsvorgang bereitstellen.

Um eine Entspannungsregel aus dem Syslog Viewer bereitzustellen, wählen Sie die Protokollmeldung aus. In der oberen rechten Ecke des Kästchens **Syslog Viewer** der ausgewählten Zeile wird ein Kontrollkästchen angezeigt. Aktivieren Sie das Kontrollkästchen, und wählen Sie dann eine Option aus der Liste Aktion aus, um die Entspannungsregel bereitzustellen. **“Bearbeiten und Bereitstellen**”, “ **Bereitstellen**” und “ **Alle bereitstellen** “ sind als **Aktionsoptionen** verfügbar.

Die SQL-Einschleusung-Regeln, die mithilfe der Option “Zum Bereitstellen klicken” bereitgestellt werden, sind die Empfehlungen zur Feinkornentspannung nicht enthalten.

So verwenden Sie die Click-to-Deploy-Funktion in der GUI:

1. Wählen Sie im Syslog Viewer in den **Moduloptionen** die Option **Application Firewall** aus.
2. Wählen Sie **APP_SQL** als **Ereignistyp** aus, um die entsprechenden Protokollmeldungen zu filtern.
3. Markieren Sie das Kontrollkästchen, um die auszubringende Regel zu identifizieren.
4. Verwenden Sie die Dropdownliste **Aktion** mit Optionen, um die Entspannungsregel bereitzustellen.
5. Stellen Sie sicher, dass die Regel im entsprechenden Abschnitt zur Entspannungsregel angezeigt wird.

Statistiken für die SQL Injection Verstöße

Wenn die Statistikaktion aktiviert ist, wird der Zähler für die SQL Injection-Prüfung inkrementiert, wenn die Web App Firewall Maßnahmen für diese Sicherheitsüberprüfung ergreift. Die Statistiken werden für Rate und Gesamtanzahl für Traffic, Verletzungen und Protokolle gesammelt. Die Größe eines Inkrements des Protokollzählers kann abhängig von den konfigurierten Einstellungen variieren. Wenn beispielsweise die Blockaktion aktiviert ist, erhöht die Anforderung für eine Seite, die 3 SQL-Einschleusung-Verletzungen enthält, den Statistikzähler um eins, da die Seite blockiert wird, sobald die erste Verletzung erkannt wird. Wenn der Block jedoch deaktiviert ist, erhöht die Verarbeitung derselben Anforderung den Statistikzähler für Verstöße und die Protokolle um drei, da jeder Verstoß eine separate Protokollnachricht generiert.

So zeigen Sie SQL Injection-Prüfstatistiken mit der Befehlszeile an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

> **sh appfw Statistiken**

Verwenden Sie den folgenden Befehl, um Statistiken für ein bestimmtes Profil anzuzeigen:

```
> stat appfw profile <profile name>
```

So zeigen Sie HTML SQL Injection-Statistiken mit der GUI an

1. Navigieren Sie zu **System** > **Sicherheit** > **Anwendungsfirewall**.
2. Greifen Sie im rechten Bereich auf den **Statistik-Link** zu.
3. Verwenden Sie die Bildlaufleiste, um die Statistiken über Verstöße und Protokolle von HTML SQL Injection anzuzeigen. Die Statistiktabelle enthält Echtzeitdaten und wird alle 7 Sekunden aktualisiert.

Highlights

Beachten Sie die folgenden Punkte zur Prüfung von SQL Injection:

- **Integrierte Unterstützung für den Schutz von SQL Injection**— Die Citrix Web App Firewall schützt vor SQL Injection, indem sie eine Kombination aus SQL-Schlüsselwörtern und Sonderzeichen in den Formularparametern überwacht Alle SQL-Schlüsselwörter, Sonderzeichen, Platzhalterzeichen und Standardtransformationsregeln werden in der Datei /netscaler/default_custom_settings.xml angegeben.
- **Anpassung**: Sie können die Standardschlüsselwörter, Sonderzeichen, Platzhalterzeichen und Transformationsregeln ändern, um die Überprüfung der SQL-Sicherheitsprüfung an die spezifischen Anforderungen Ihrer Anwendung anzupassen. Erstellen Sie eine Kopie des Standardsignaturobjekts, ändern Sie vorhandene Einträge oder fügen Sie neue hinzu. Binden Sie dieses Signaturobjekt an Ihr Profil, um die benutzerdefinierte Konfiguration zu nutzen.
- **Hybrides Sicherheitsmodell**— Sowohl Signaturen als auch umfassender Sicherheitsschutz verwenden die SQL/Cross-Site-Scripting-Muster, die in dem Signaturobjekt angegeben sind, das an das Profil gebunden ist. Wenn kein Signaturobjekt an das Profil gebunden ist, werden die im Standardsignaturobjekt vorhandenen SQL/Cross-Site-Scripting-Muster verwendet.
- **Transform**—Beachten Sie Folgendes über den Transformationsvorgang:
  - Der Transformationsvorgang funktioniert unabhängig von den anderen SQL Injection-Aktionseinstellungen. Wenn die Transformation aktiviert ist und Block, Log, Statistiken und Lernen alle deaktiviert sind, werden SQL-Sonderzeichen transformiert.
  - Wenn SQL Transformation aktiviert ist, werden Benutzeranfragen an die Back-End-Server gesendet, nachdem die SQL-Sonderzeichen im Nicht-Blockmodus transformiert wurden. Wenn die Blockaktion aktiviert ist, hat sie Vorrang vor der Transformationsaktion. Wenn der Einschleusungstyp als SQL-Sonderzeichen angegeben ist und der Block aktiviert ist, wird die Anforderung trotz der Transformationsaktion blockiert.

- **Fine Grained Relaxation and Learning**— Optimieren Sie die Entspannungsregel, um eine Teilmenge von SQL-Elementen aus der Sicherheitskontrolle zu entspannen, aber den Rest zu erkennen. Die Lern-Engine empfiehlt einen bestimmten Werttyp und Wertausdrücke basierend auf den beobachteten Daten.
- **Zum Bereitstellen klicken**— Wählen Sie eine oder mehrere SQL-Verletzungsprotokollmeldungen im Syslog-Viewer aus und stellen Sie sie als Entspannungsregeln bereit.

SQL-Grammatikschutz für HTML- und JSON-Nutzlast

October 5, 2021

Citrix Web App Firewall verwendet einen Pattern-Match-Ansatz zum Erkennen von SQL-Injection-Angriffen in `HTTP` und `JSON` Payloads. Der Ansatz verwendet eine Reihe von vordefinierten Schlüsselwörtern und (oder) Sonderzeichen, um einen Angriff zu erkennen und ihn als Verstoß zu kennzeichnen. Obwohl dieser Ansatz effektiv ist, kann dies zu vielen Fehlalarmen führen, was dazu führt, dass eine oder mehrere Entspannungsregeln hinzugefügt werden. Insbesondere wenn häufig verwendete Wörter wie “Select” und “From” in einer HTTP- oder JSON-Anfrage verwendet werden. Wir können Fehlalarme reduzieren, indem wir die Überprüfung des SQL-Grammatikschutzes `HTML` und die `JSON` Nutzlast implementieren.

Im bestehenden Pattern-Match-Ansatz wird ein SQL-Injection-Angriff identifiziert, wenn ein vordefiniertes Schlüsselwort und/oder ein Sonderzeichen in einer HTTP-Anforderung vorhanden ist. In diesem Fall muss die Anweisung keine gültige SQL-Anweisung sein. Im grammatikbasierten Ansatz wird jedoch ein SQL-Injection-Angriff nur erkannt, wenn ein Schlüsselwort oder ein Sonderzeichen in einer SQL-Anweisung vorhanden ist oder Teil einer SQL-Anweisung ist, wodurch falsch positive Szenarien reduziert werden.

Szenario zur Nutzung des SQL-Grammatikschutzes

Betrachten Sie eine Erklärung “Wählen Sie meine Tickets aus und treffen wir uns auf der Gewerkschaftsstation” in einer HTTP-Anfrage. Obwohl die Anweisung keine gültige SQL-Anweisung ist, erkennt der vorhandene Pattern-Match-Ansatz die Anforderung als SQL-Injection-Angriff, da die Anweisung Schlüsselwörter wie “Select”, “und” und “Union” verwendet. Im Falle des SQL-Grammatikansatzes wird die Anweisung jedoch nicht als Verstoßangriff erkannt, da die Schlüsselwörter nicht in einer gültigen SQL-Anweisung vorhanden sind oder nicht Teil einer gültigen SQL-Anweisung sind.

Der grammatikbasierte Ansatz kann auch für die Erkennung von SQL-Injection-Angriffen in `JSON` Payloads konfiguriert werden. Um eine Entspannungsregel hinzuzufügen, können Sie die bestehenden Entspannungsregeln wiederverwenden. Feinkörnige Entspannungsregeln gelten auch für die

SQL-Grammatik, für Regeln mit “ValueType” “Schlüsselwort”. In der JSON SQL-Grammatik kann die vorhandene URL-basierte Methode wiederverwendet werden.

Konfigurieren Sie den grammatikbasierten SQL-Schutz mit der CLI

Um die grammatikbasierte SQL-Erkennung zu implementieren, müssen Sie den Parameter “SqLinjectionGrammar” im Web App Firewall-Profil konfigurieren. Standardmäßig ist der Parameter deaktiviert. Alle vorhandenen SQL Injection-Aktionen werden mit Ausnahme des Lernens unterstützt. Jedes neue Profil, das nach einem Upgrade erstellt wurde, unterstützt die SQL-Injection-Grammatik und hat weiterhin den Standardtyp als “Sonderzeichen oder Schlüsselwort” und muss explizit aktiviert sein.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add appfw profile <profile-name>  - SQLInjectionAction <action-name> -
     SQLInjectionGrammar ON/OFF
2 <!--NeedCopy-->
```

Beispiel:

```
add appfw profile profile1 -SQLInjectionAction Block -SQLInjectionGrammar ON
```

Konfigurieren Sie den SQL-Pattern-Match-Schutz und den grammatikbasierten Schutz über die Befehlszeilenschnittstelle

Wenn Sie sowohl Grammatik-basierte als auch Pattern-Match-Ansätze aktiviert haben, führt die Appliance zuerst eine grammatikbasierte Erkennung durch, und wenn eine SQL-Einschleusungserkennung mit dem Aktionstyp auf blockiert festgelegt ist, wird die Anforderung blockiert (ohne die Erkennung mithilfe von Pattern-Match zu überprüfen).

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add appfw profile <profile-name>  - SQLInjectionAction <action-name> -
     SQLInjectionGrammar ON  - SQLInjectionType <Any action other than  '
     None' : SQLSplCharANDKeyword/ SQLSplCharORKeyword/ SQLSplChar/
     SQLKeyword>
2 <!--NeedCopy-->
```

Beispiel:

```
add appfw profile p1 -SQLInjectionAction block - SQLInjectionGrammar ON -
SQLInjectionType SQLSplChar
```


Konfigurieren Sie SQL Injection Check nur mit grammatikbasiertem Schutz über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add appfw profile <profile-name>  - SQLInjectionAction <action-name> -
     SQLInjectionGrammar ON  - SQLInjectionType None
2 <!--NeedCopy-->
```

Beispiel:

```
add appfw profile p1 -SQLInjectionAction block - SQLInjectionGrammar ON -
SQLInjectionType None
```

Binden Sie Entspannungsregeln für den grammatikbasierten SQL-Schutz über die Befehlszeilenschnittstelle

Wenn Ihre Anwendung erfordert, dass Sie die SQL Einschleusungsprüfung für ein bestimmtes “ELEMENT” oder “ATTRIBUT” in der Nutzlast Bypass müssen, müssen Sie eine Entspannungsregel konfigurieren.

> **Hinweis:**
>
> Entspannungsregeln mit ValueType “Schlüsselwort” werden nur ausgewertet, wenn die Appliance mithilfe der SQL Grammatik die Erkennung durchführt.

Der SQL Befehl Entspannungsregeln für die Einschleusungsinspektion haben die folgende Syntax. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind appfw profile <name> -SQLInjection <String> [isRegex(REGEX|
     NOTREGE)] <formActionURL> [-location <location>] [-valueType (Keywor
     |SpecialString|Wildchar) [<valueExpression>][-isValueRegex (REGEX |
     NOTREGEX) ]]
2 <!--NeedCopy-->
```

Beispiel:

```
bind appfw profile p1 -sqlinjection abc http://10.10.10.10/
bind appfw profile p1 -sqlinjection 'abc[0-9]+'http://10.10.10.10/ -isregex
regEX
bind appfw profile p1 -sqlinjection 'name'http://10.10.10.10/ -valueType
Keyword 'selec[a-z]+' -isvalueRegex regEX
```


Konfigurieren Sie den grammatikbasierten SQL-Schutz für JSON-Nutzlast über die Befehlszeilenschnittstelle

Um die grammatikbasierte SQL-Erkennung für die JSON-Nutzlast zu implementieren, müssen Sie den Parameter "JsonSqLinjectionGrammar" im Web App Firewall-Profil konfigurieren. Standardmäßig ist der Parameter deaktiviert. Alle vorhandenen SQL Injection-Aktionen werden mit Ausnahme des Lernens unterstützt. Jedes neue Profil, das nach einem Upgrade erstellt wurde, unterstützt die SQL-Injection-Grammatik und hat weiterhin den Standardtyp als "Sonderzeichen oder Schlüsselwort" und Sie müssen es explizit aktivieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add appfw profile <profile-name> -type JSON  - JSONSQLInjectionAction <
     action-name> -JSONSQLInjectionGrammar ON/OFF
2 <!--NeedCopy-->
```

Beispiel:

```
add appfw profile profile1 -type JSON -JSONSQLInjectionAction Block -JSONSQLInjectionG
 ON
```

Konfigurieren Sie den SQL-Muster-Match-Schutz und den grammatikbasierten Schutz über die Befehlszeilenschnittstelle

Wenn Sie sowohl Grammatik-basierte als auch Pattern-Match-Prüfungen aktiviert haben, führt die Appliance zuerst eine grammatikbasierte Erkennung durch, und wenn eine SQL-Einschleusungserkennung mit dem Aktionstyp auf blockiert festgelegt ist, wird die Anforderung blockiert (ohne die Erkennung mithilfe von Pattern-Match zu überprüfen).

> **Hinweis:**
>
> Entspannungsregeln mit ValueType "Schlüsselwort" werden nur ausgewertet, wenn die Appliance die Erkennung mithilfe der SQL-Grammatik durchführt.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add appfw profile <profile-name> -type JSON  - JSONSQLInjectionAction <
     action-name> -JSONSQLInjectionGrammar ON  - JSONSQLInjectionType <Any
      action other than  'None' : SQLSplCharANDKeyword/
     SQLSplCharORKeyword/ SQLSplChar/ SQLKeyword>
2 <!--NeedCopy-->
```


Beispiel:

```
add appfw profile p1 -type JSON -JSONSQLInjectionAction block - JSONSQLInjectionGramma
 ON -JSONSQLInjectionType SQLSplChar
```

Konfigurieren Sie den grammatikbasierten SQL-Schutz für JSON-Nutzlast über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add appfw profile <profile-name> -type JSON  - JSONSQLInjectionAction <
      action-name> -JSONSQLInjectionGrammar ON  - JSONSQLInjectionType None
      `\
2 <!--NeedCopy-->
```

Beispiel:

```
add appfw profile p1 -type JSON -JSONSQLInjectionAction block - JSONSQLInjectionGramma
 ON -JSONSQLInjectionType None
```

Binden Sie URL-basierte Entspannungsregeln für JSON SQL grammatikbasierten Schutz über die Befehlszeilenschnittstelle

Wenn Ihre Anwendung erfordert, dass Sie die JSON-Befehlseinschleusungsprüfung für ein bestimmtes “ELEMENT” oder “ATTRIBUT” in der Nutzlast umgehen müssen, können Sie eine Entspannungsregel konfigurieren.
Der JSON Befehl Entspannungsregeln für die Einschleusungsinspektion haben die folgende Syntax.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind appfw profile <profile name>  - JSONCMDURL <expression> -comment <
      string> -isAutoDeployed ( AUTODEPLOYED | NOTAUTODEPLOYED ) -state (
      ENABLED | DISABLED )
2 <!--NeedCopy-->
```

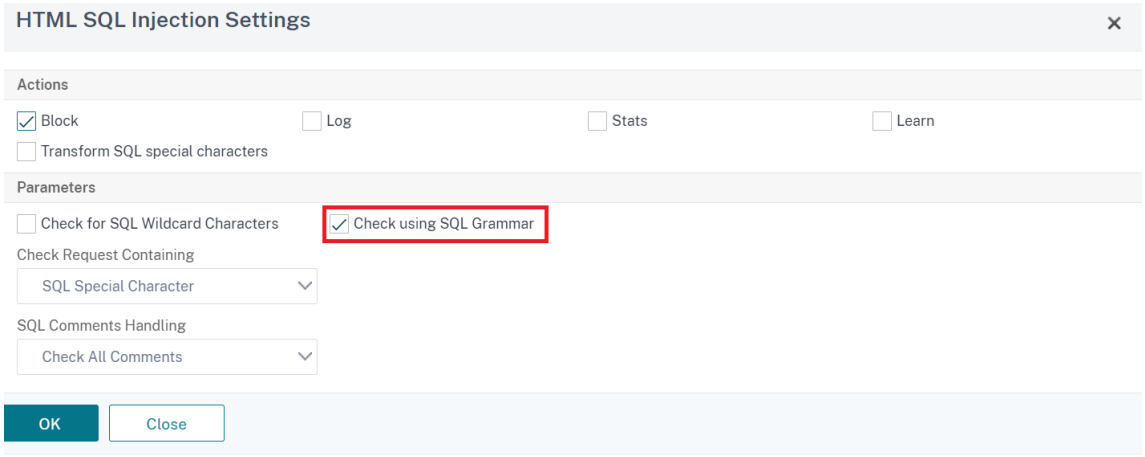
Beispiel:

```
bind appfw profile p1 -sqlinjection abc http://10.10.10.10/
bind appfw profile p1 -sqlinjection 'abc[0-9]+'http://10.10.10.10/ -isregex
regEX
bind appfw profile p1 -sqlinjection 'name'http://10.10.10.10/ -valueType
Keyword 'selec[a-z]+' -isvalueRegex regEX
```


Konfigurieren Sie den grammatikbasierten SQL-Schutz über die grafische Benutzeroberfläche

Führen Sie die GUI-Prozedur ab, um die grammatikbasierte HTML SQL Injection Erkennung zu konfigurieren

1. Navigieren Sie im Navigationsbereich zu **Sicherheit > Profile**.
2. Klicken Sie auf der Seite **Profile** auf **Hinzufügen**.
3. Klicken Sie auf der Seite **Citrix Web App Firewall Profile** unter **Erweiterte Einstellungen** auf **Sicherheitsprüfungen**.
4. Wechseln Sie im Abschnitt **Sicherheitsprüfungen** zu Einstellungen für **HTML SQL Injection** .
5. Klicken Sie auf das Symbol für die ausführbare Datei neben dem Kontrollkästchen.
6. Klicken Sie auf **Aktionseinstellungen**, um die Seite **Einstellungen für HMTL SQL Injection** aufzurufen.



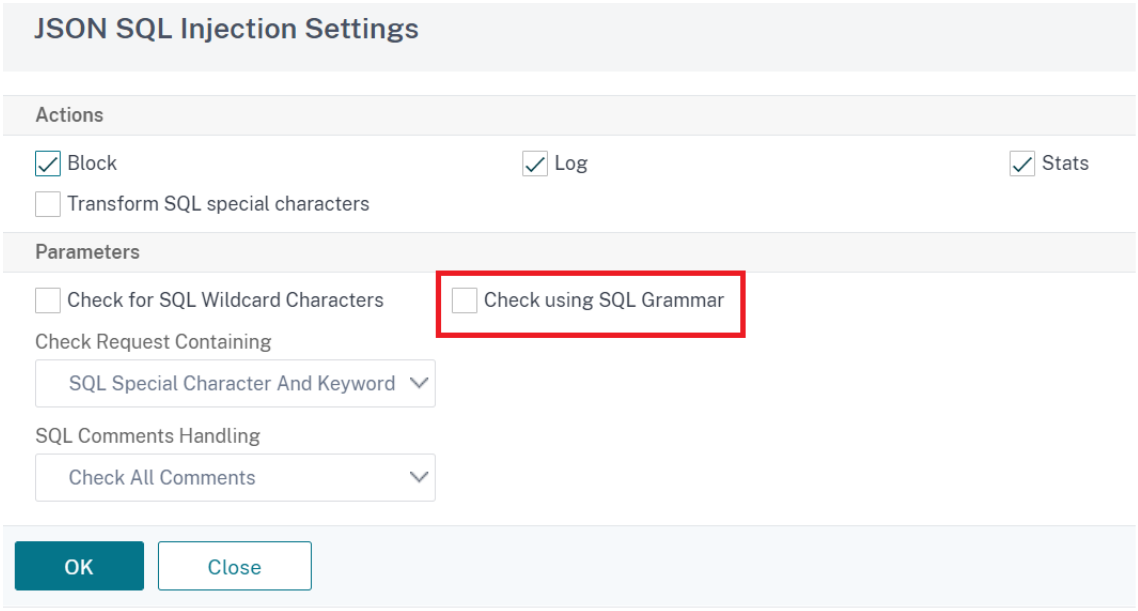
7. Aktivieren Sie das **Kontrollkästchen Mit SQL-Grammatik** prüfen.
8. Klicken Sie auf **OK**.

Konfigurieren Sie den grammatikbasierten SQL-Schutz für JSON-Nutzlast über die grafische Benutzeroberfläche

Führen Sie die GUI-Prozedur ab, um die grammatikbasierte JSON SQL Injection Erkennung zu konfigurieren.

1. Navigieren Sie im Navigationsbereich zu **Sicherheit > Profile**.
2. Klicken Sie auf der Seite **Profile** auf **Hinzufügen**.
3. Klicken Sie auf der Seite **Citrix Web App Firewall Profile** unter **Erweiterte Einstellungen** auf **Sicherheitsprüfungen**.

4. Wechseln Sie im Abschnitt **Sicherheitsprüfungen** zu **JSON SQL Injection-Einstellungen** .
5. Klicken Sie auf das Symbol für die ausführbare Datei neben dem Kontrollkästchen.
6. Klicken Sie auf **Aktionseinstellungen**, um die Seite **JSON SQL Injection Settings** aufzurufen.
7. Aktivieren Sie das **Kontrollkästchen Mit SQL-Grammatik** prüfen.
8. Klicken Sie auf **OK**.



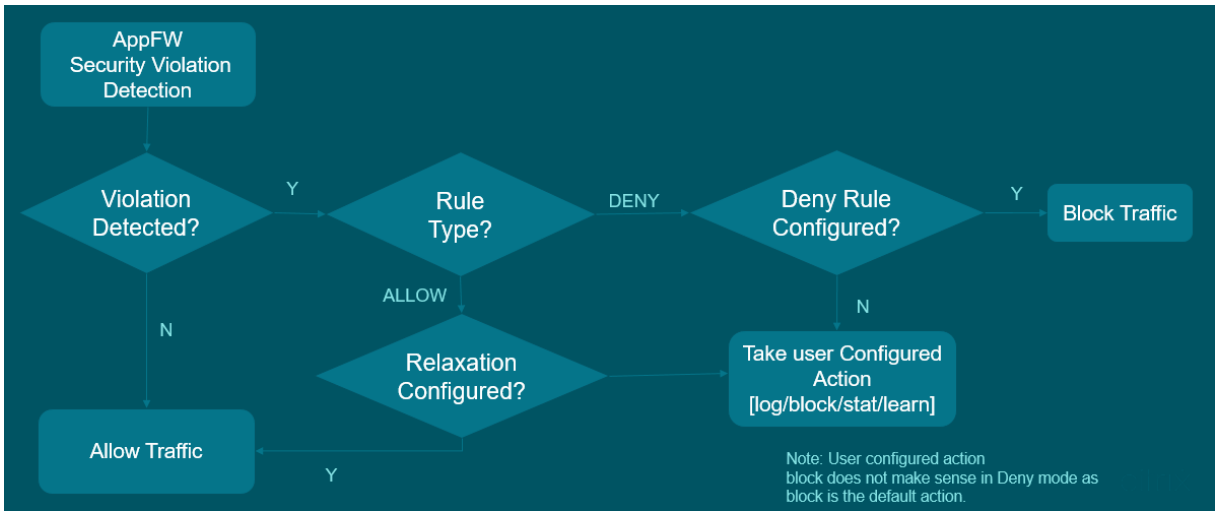
Regeln zur Entspannung und Ablehnung von HTML-SQL-Injection-Angriffen

October 5, 2021

Wenn ein eingehender Datenverkehr vorliegt, prüft die Logik zur Erkennung von Verstößen auf Verkehrsverstöße. Wenn keine HTML-SQL-Injection-Angriffe erkannt werden, darf der Datenverkehr bestehen. Wenn jedoch ein Verstoß festgestellt wird, definieren die Regeln für Entspannung (Zulassen) und Verweigern, wie mit den Verstößen umzugehen sind. Wenn die Sicherheitsprüfung im Zulassungsmodus (Standardmodus) konfiguriert ist, wird der erkannte Verstoß blockiert, es sei denn, der Benutzer hat explizit eine Entspannungs- oder Zulassungsregel konfiguriert.

Neben dem Zulassungsmodus kann die Sicherheitsprüfung auch im Ablehnmodus konfiguriert werden und Verweigerregeln für die Behandlung von Verstößen verwenden. Wenn die Sicherheitsprüfung in diesem Modus konfiguriert ist, werden die erkannten Verstöße blockiert, wenn ein Benutzer explizit eine Ablehnregel konfiguriert hat. Wenn keine Ablehnungsregeln konfiguriert sind, wird die vom Benutzer konfigurierte Aktion angewendet.

In der folgenden Abbildung wird erläutert, wie Betriebsmodi zugelassen und verweigert werden:



1. Wenn ein Verstoß festgestellt wird, definieren die Regeln für Entspannung (Zulassen) und Verweigern, wie mit den Verstößen umzugehen sind.
2. Wenn die Sicherheitsprüfung im Verweigerungsmodus konfiguriert ist (falls sie im Zulassungsmodus konfiguriert ist, springen Sie zu Schritt 5), wird der Verstoß blockiert, es sei denn, Sie haben explizit eine Ablehnungsregel konfiguriert.
3. Wenn der Verstoß mit einer Ablehnregel übereinstimmt, blockiert die Appliance den Datenverkehr.
4. Wenn der Verkehrsverstoß nicht mit einer Regel übereinstimmt, wendet die Appliance eine benutzerdefinierte Aktion an (blockieren, zurücksetzen oder löschen).
5. Wenn die Sicherheitsprüfung im Zulassungsmodus konfiguriert ist, prüft das Web App Firewall-Modul, ob eine Zulassungsregel konfiguriert ist.
6. Wenn der Verstoß mit einer Zulassungsregel übereinstimmt, lässt die Appliance den Datenverkehr andernfalls Bypass, er wird blockiert.

Konfigurieren des Entspannungs- und Durchsetzungsmodus

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set appfw profile <name>   - SQLInjectionAction [block stats learn]  -
    SQLInjectionRuleType [ALLOW DENY]
<!--NeedCopy-->
```

Beispiel:

```
set appfw profile prof1 sqlInjectionAction block -sqlInjectionRuleType
ALLOW DENY
```


Binden Sie Entspannungs- und Durchsetzungsregeln an das Web Application Firewall-

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind appfw profile <name> -SQLInjection <string> <formActionURL>
<!--NeedCopy-->
```

Beispiel:

```
bind appfw profile p1 -SQLInjection field_f1 ”/login.php”-RuleType ALLOW
bind appfw profile p2 -SQLInjection field_f1 ”/login.php”-RuleType ALLOW
```

HTML-Befehlseinschleusung Schutzüberprüfung

October 5, 2021

Die **HTML-Befehlseinschleusungsprüfung** untersucht, ob der eingehende Datenverkehr nicht autorisierte Befehle enthält, die die Systemsicherheit unterbrechen oder das System ändern. Wenn der Datenverkehr bei der Entdeckung schädliche Befehle enthält, blockiert die Appliance die Anforderung oder führt die konfigurierte Aktion aus.

Das Profil der Citrix Web App Firewall wurde jetzt um eine neue Sicherheitsprüfung für Befehlseinschleusungsangriffe erweitert. Wenn die Sicherheitsprüfung des Befehls Injection den Datenverkehr untersucht und schädliche Befehle erkennt, blockiert die Appliance die Anforderung oder führt die konfigurierte Aktion aus.

Bei einem Befehlseinschleusungsangriff zielt der Angreifer darauf ab, nicht autorisierte Befehle auf dem Citrix ADC Betriebssystem auszuführen. Um dies zu erreichen, injiziert der Angreifer Betriebssystembefehle mit einer anfälligen Anwendung. Eine Citrix ADC Appliance ist anfällig für Injection-Angriffe, wenn die Anwendung unsichere Daten (Formulare, Cookies oder Header) an die Systemshell weitergibt.

Funktionsweise des Befehlseinschleusungsschutzes

1. Bei einer eingehenden Anforderung untersucht WAF den Datenverkehr auf Schlüsselwörter oder Sonderzeichen. Wenn die eingehende Anforderung keine Muster aufweist, die mit einem der verweigerten Schlüsselwörter oder Sonderzeichen übereinstimmen, ist die Anforderung zulässig. Andernfalls wird die Anforderung basierend auf der konfigurierten Aktion blockiert, gelöscht oder umgeleitet.

2. Wenn Sie lieber ein Schlüsselwort oder ein Sonderzeichen von der Liste ausnehmen möchten, können Sie eine Relaxationsregel anwenden, um die Sicherheitsprüfung unter bestimmten Bedingungen zu umgehen.
3. Sie können die Protokollierung aktivieren, um Protokollmeldungen zu generieren. Sie können die Protokolle überwachen, um festzustellen, ob Antworten auf legitime Anfragen blockiert werden. Eine große Zunahme der Anzahl von Protokollmeldungen kann auf Versuche hinweisen, einen Angriff zu starten.
4. Sie können die Statistikfunktion auch aktivieren, um statistische Daten zu Verletzungen und Protokollen zu sammeln. Ein unerwarteter Anstieg im Statistikzähler deutet möglicherweise darauf hin, dass Ihre Anwendung angegriffen wird. Wenn legitime Anfragen blockiert werden, müssen Sie möglicherweise die Konfiguration erneut aufrufen, um zu sehen, ob Sie die neue Relaxationsregel konfigurieren oder die vorhandene ändern müssen.

Schlüsselwörter und Sonderzeichen, die für die Befehlseinschleusung verweigert werden

Um Befehlseinschleusungsangriffe zu erkennen und zu blockieren, verfügt die Appliance über eine Reihe von Mustern (Schlüsselwörter und Sonderzeichen), die in der Standardsignaturdatei definiert sind. Im Folgenden finden Sie eine Liste der Schlüsselwörter, die während der Erkennung der Befehlseinschleusung blockiert wurden.

```
    <commandinjection>
      <keyword type="LITERAL" builtin="ON">7z</keyword>
      <keyword type="LITERAL" builtin="ON">7za</keyword>
      <keyword type="LITERAL" builtin="ON">7zr</keyword>
…
</commandinjection>
<!--NeedCopy-->
```

In der Signaturdatei definierte Sonderzeichen sind:
`| ; & $ > < '\ ! >> ##`

Konfigurieren der Befehlseinschleusungsprüfung mit der CLI

In der Befehlszeilenschnittstelle können Sie entweder den Befehl set the profile oder den Befehl add the profile verwenden, um die Befehlseinschleusungseinstellungen zu konfigurieren. Sie können die Block-, Protokoll- und Statistikaktionen aktivieren. Sie müssen auch die Schlüsselwörter und Zeichenfolgenzeichen festlegen, die Sie in den Nutzlasten erkennen möchten.

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set appfw profile <profile-name> -cmdInjectionAction <action-name> -CMDInjectionType
 <CMDInjectionType>]
```

> **Hinweis:**
>
> Standardmäßig ist die Befehlseinschleusungsaktion auf “Keine” festgelegt. Außerdem wird der Standardeinschleusungsstyp des Befehls als festgelegt `CmdSplCharANDKeyWord`.

Beispiel:

```
set appfw profile profile1 -cmdInjectionAction block -CMDInjectionType
CmdSplChar
```

Wo sind die verfügbaren Befehlseinschleusungsaktionen:

- Keine - Deaktivieren Sie den Befehlseinschleusungsschutz.
- Log - Protokollieren Sie Verstöße gegen die Befehlseinschleusung für die Sicherheitsprüfung.
- Blockieren - blockiert Datenverkehr, der gegen die Sicherheitsprüfung des Befehls Einschleusung verstößt.
- Statistiken - Generiert Statistiken für die Befehlseinschleusung Sicherheitsverletzungen.

Dabei sind die verfügbaren Befehlseinschleusungstypen:

- Cmd SplChar. Überprüft Sonderzeichen
- CmdKeyWord. Überprüft Befehlseinschleusung Schlüsselwörter
- CmdSplCharANDKeyWord. Überprüft Sonderzeichen und Befehlseinschleusung. Schlüsselwörter und Blöcke nur, wenn beide vorhanden sind.
- CmdSplCharORKeyWord. Überprüft Sonderzeichen und Befehlseinschleusung Schlüsselwörter und Blöcke, wenn eines von ihnen gefunden wird.

Konfigurieren von Relaxationsregeln für die Überprüfung des Befehlseinschleusungsschutzes

Wenn Ihre Anwendung erfordert, dass Sie die Inspektion der Befehlseinschleusung für ein bestimmtes ELEMENT oder ATTRIBUTE in der Nutzlast umgehen müssen, können Sie eine Relaxationsregel konfigurieren.

Die Relaxationsregeln des Befehls “Injection Inspection” haben die folgende Syntax:

```
bind appfw profile <profile name> -cmdInjection <string> <URL> -isregex <
REGEX/NOTREGEX>
```

Beispiel für Relaxationsregel für Regex im Header

```
bind appfw profile sample -CMDInjection hdr ”http://10.10.10.10/”-location
heaDER -valueType Keyword '[a-z]+grep'-isvalueRegex REGEX
```


Infolgedessen befreit die Injektion den Befehl Injection Check ermöglicht Header, der Varianten von “grep” `hdr` enthält.

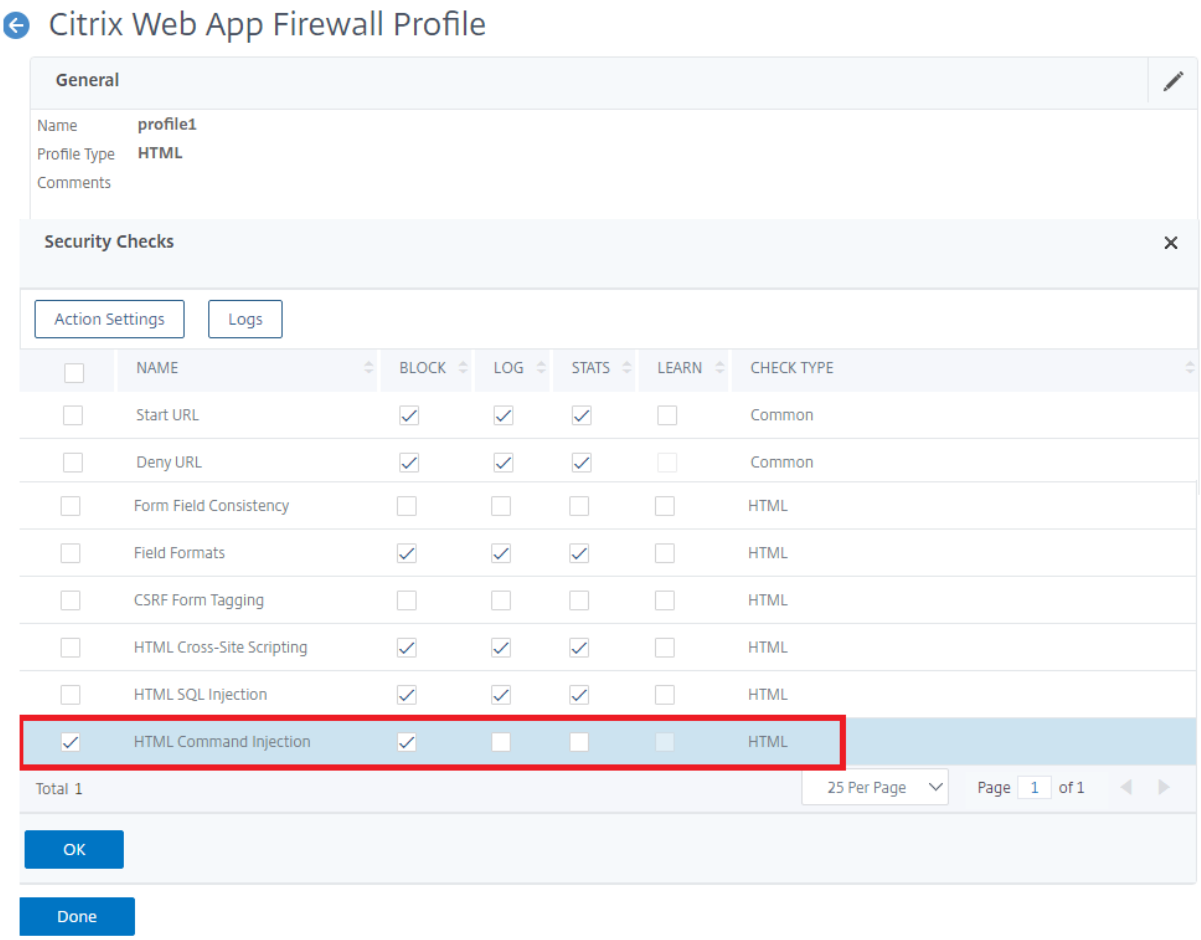
Beispiel für Relaxationsregel mit ValueType als Regex im Cookie

```
bind appfw profile sample -CMDInjection ck_login ”http://10.10.10.10/”-
location cookie -valueType Keyword 'pkg[a-z]+'-isvalueRegex REGEX
```

Konfigurieren der Befehlseinschleusungsprüfung über die Citrix ADC GUI

Führen Sie die folgenden Schritte aus, um die Befehlseinschleusungsprüfung zu konfigurieren.

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall und Profile**.
2. Wählen Sie auf der Seite **Profile** ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Wechseln Sie auf der Seite **Citrix Web App Firewall Profil** zum Abschnitt **Erweiterte Einstellungen** und klicken Sie auf **Sicherheitsprüfungen**.

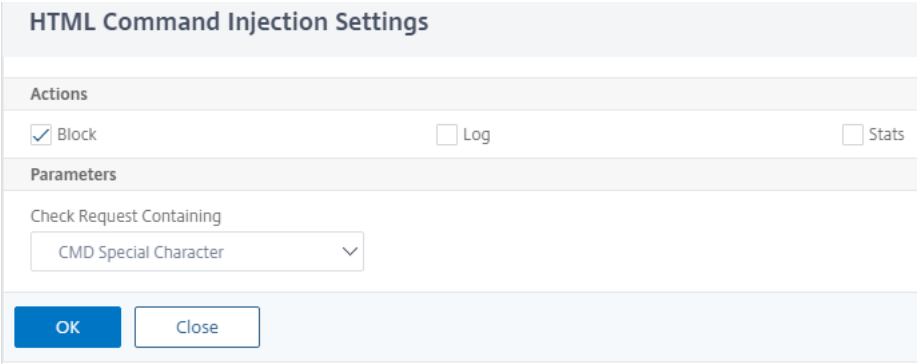


1. Wählen Sie im Abschnitt **Sicherheitsüberprüfungen** die Option **HTML Command Injection** aus **und** klicken Sie auf

2. Legen Sie auf der Seite **Einstellungen für HTML-Befehlseinschleusung** die folgenden Parameter fest:

   a) Aktionen. Wählen Sie eine oder mehrere Aktionen aus, die für die Sicherheitsprüfung der Befehlseinschleusung ausgeführt werden sollen.
   b) Prüfen Sie Anforderung enthält. Wählen Sie ein Befehlseinschleusungsmuster aus, um zu überprüfen, ob die eingehende Anforderung das Muster hat.

3. Klicken Sie auf **OK**.



Anzeigen oder Anpassen von Befehlseinschleusungsmustern über die grafische Benutzeroberfläche

Sie können die GUI verwenden, um die Injection-Pattern des **HTML-Befehls** anzuzeigen oder anzupassen.

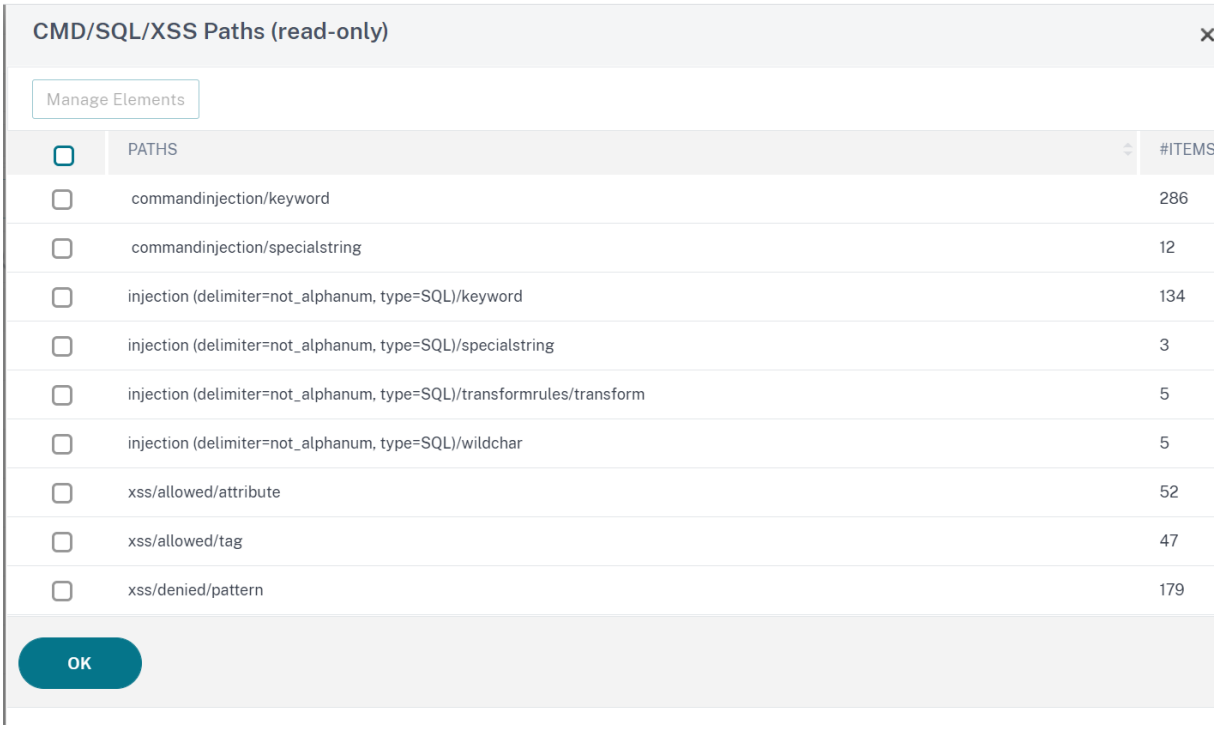
Die Standardbefehl-Einschleusungsmuster sind in der Standardsignaturdatei angegeben. Wenn Sie kein Signaturobjekt an Ihr Profil binden, werden die im Standardsignatur-Objekt angegebenen Standard-HTML-Befehlseinschleusungsmuster vom Profil für die Verarbeitung der Sicherheitsprüfung der Befehlseinschleusung verwendet. Die im Standardsignaturobjekt angegebenen Regeln und Muster sind schreibgeschützt. Sie können sie nicht bearbeiten oder ändern. Wenn Sie diese Muster ändern oder ändern möchten, erstellen Sie eine Kopie des Standardobjekts sSignatures, um ein benutzerdefiniertes Signaturobjekt zu erstellen. Nehmen Sie Änderungen an den Befehlseinschleusungsmustern im neuen benutzerdefinierten Signaturobjekt vor und verwenden Sie dieses Signaturobjekt in Ihrem Profil, das den Datenverkehr verarbeitet, für den Sie diese benutzerdefinierten Muster verwenden möchten.

Weitere Informationen finden Sie unter Signaturen

So zeigen Sie die Standardeinschleusungsmuster für Befehle über die GUI an:

1. Navigieren Sie zu **Application Firewall > Signaturen**, wählen Sie ***Standardsignaturen** aus und klicken Sie auf **Bearbeiten**.

1. Klicken Sie auf **CMD/SQL/XSS-Muster verwalten**. Die Tabelle **CMD/SQL/XSS Paths (schreibgeschützt)** zeigt Muster im Zusammenhang mit der `CMD`/`SQL`/`XSS`-Einschleusung:



1. Wählen Sie eine Zeile aus und klicken Sie auf **Elemente verwalten**, um die entsprechenden Befehlseinschleusungsmuster (Schlüsselwörter, spezielle Zeichenfolgen, Transformationsregeln oder Platzhalterzeichen) anzuzeigen, die von der Injection-Prüfung des Web App Firewall-Befehls verwendet werden.

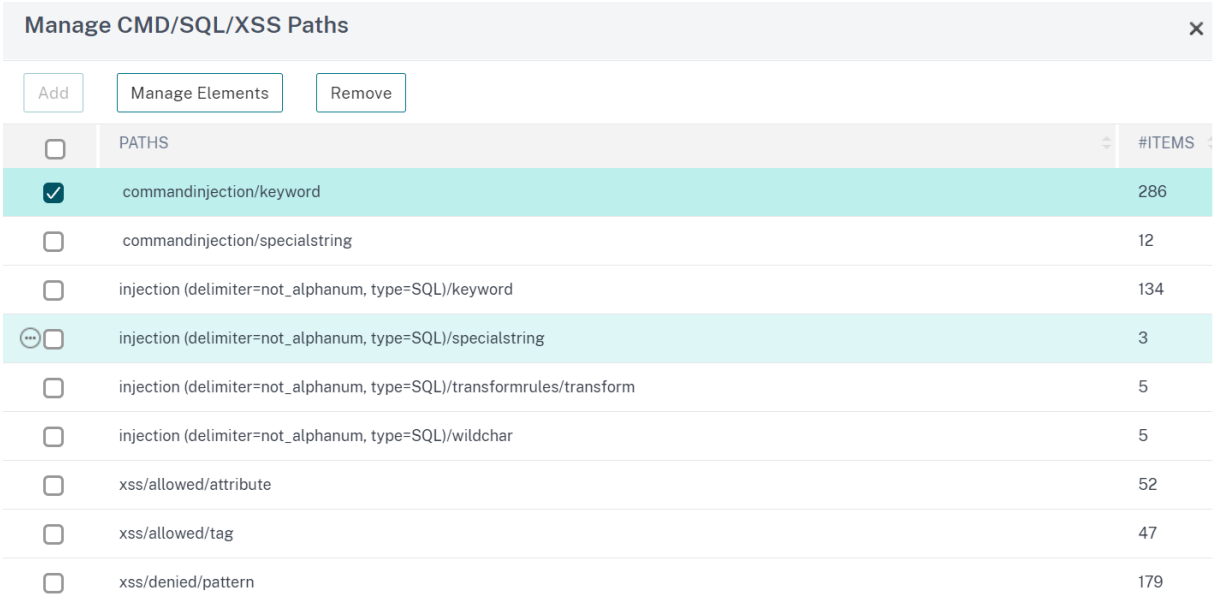
So passen Sie ein Befehlseinschleusungsmuster mit der GUI an

Sie können das benutzerdefinierte Signaturobjekt bearbeiten, um die **CMD-Schlüsselwörter**, Son-

derzeichenfolgen und Platzhalterzeichen anzupassen. Sie können neue Einträge hinzufügen oder vorhandene entfernen. Sie können die Transformationsregeln für die spezielle Zeichenfolgen für die Befehlseinschleusung ändern.

1. Navigieren Sie zu **Application Firewall > Signaturen**, markieren Sie die benutzerdefinierte Zielsignatur und klicken Sie auf **Hinzufügen**. Klicken Sie auf **CMD/SQL/XSS-Muster verwalten**.
2. Wählen Sie auf der Seite **CMD/SQL/XSS-Pfade verwalten** die Ziel-CMD-Einschleusungszeile aus.
3. Klicken Sie auf **Elemente verwalten**, **Hinzufügen** oder **Entfernen** eines Befehlseinschleusungselements.

> **Warnung:**
>
> Sie müssen vorsichtig sein, bevor Sie ein Standard-Befehlseinschleusungselement entfernen oder ändern, oder den CMD-Pfad löschen, um die gesamte Zeile zu entfernen. Die Signaturregeln und die Sicherheitsprüfung der Befehlseinschleusung beruhen auf diesen Elementen, um Angriffe auf Befehlseinschleusung zu erkennen, um Ihre Anwendungen zu schützen. Das Anpassen der SQL-Muster kann Ihre Anwendung anfällig für Befehlseinschleusungsangriffe machen, wenn das erforderliche Muster während der Bearbeitung entfernt wird.



Anzeigen von Statistiken zum Befehlseinschleusungsdatenverkehr und -verletzungen

Auf der Seite **Citrix Web App Firewall -Statistiken** werden Details zu Sicherheitsdatenverkehr und Sicherheitsverletzungen in einem tabellarischen oder grafischen Format angezeigt.

So zeigen Sie Sicherheitsstatistiken mithilfe der Befehlszeilenschnittstelle an.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat appfw profile profile1
```

Appfw-Profil Traffic Statistics	Rate (/s)	Gesamt
Anforderungen	0	0
Bytes anfordern	0	0
Antworten	0	0
Antwort-Bytes	0	0
Bricht ab	0	0
Weiterleitungen	0	0
Langzeit-Antwortzeit (ms)	–	0
Letzte Ave Reaktionszeit (ms)	–	0

HTML/XML/JSON Verstoßstatistiken	Rate (/s)	Gesamt
Start-URL	0	0
URL verweigern	0	0
Referer-Kopfzeile	0	0
Pufferüberlauf	0	0
Cookie-Konsistenz	0	0
Cookie-Hijacking	0	0
CSRF-Formular-Tag	0	0
HTML-Site-übergreifendes Skripting	0	0
HTML-SQL-Injection	0	0
Feld-Format	0	0
Feldkonsistenz	0	0
Kreditkarte	0	0
Sicheres Objekt	0	0
Verletzungen der Signatur	0	0

HTML/XML/JSON Verstoßstatistiken	Rate (/s)	Gesamt
Inhaltstyp	0	0
JSON Denial of Service	0	0
JSON SQL-Injection	0	0
JSON Cross-Site Scripting	0	0
Datei-Upload-Typen	0	0
XML-Payload des Inhaltstyps ableiten	0	0
HTML-CMD-Einschleusung	0	0
XML-Format	0	0
XML-Denial-of-Service (XDoS)	0	0
XML-Nachrichtenüberprüfung	0	0
Interoperabilität von Webdiensten	0	0
XML SQL Injection	0	0
XML-Site-übergreifendes Skripting	0	0
XML-Anhang	0	0
SOAP-Fehlerverletzungen	0	0
Allgemeine XML-Verstöße	0	0
Verstöße insgesamt	0	0

HTML/XML/JSON-Protokollstatistik	Rate (/s)	Gesamt
URL-Protokolle starten	0	0
URL-Protokolle verweigern	0	0
Referer-Header-Protokolle	0	0
Pufferüberlaufprotokolle	0	0
Cookie-Konsistenzprotokolle	0	0
Cookie-Hijacking Protokolle	0	0

HTML/XML/JSON-Protokollstatistik	Rate (/s)	Gesamt
CSRF aus Tag-Protokollen	0	0
HTML-Cross-Site Scripting Protokolle	0	0
HTML-Cross-Site Scripting Transformationsprotokolle	0	0
HTML SQL Injection-Protokolle	0	0
HTML-SQL-Transformationsprotokolle	0	0
Feldformatprotokolle	0	0
Konsistenzprotokolle für Felder	0	0
Kreditkarten	0	0
Transformationsprotokolle für Kreditkarten	0	0
Sichere Objektprotokolle	0	0
Signatur-Protokolle	0	0
Inhaltstyp-Protokolle	0	0
JSON Denial-of-Service-Protokolle	0	0
JSON-SQL-Injectionsprotokolle	0	0
JSON-Site-Cross-Site-Skripting-Protokolle	0	0
Datei-Upload-Typen Protokolle	0	0
Ableiten des Inhaltstyps XML Payload L	0	0
HTML Command Injection Protokolle	0	0
Protokolle im XML-Format	0	0

HTML/XML/JSON-Protokollstatistik	Rate (/s)	Gesamt
XML Denial-of-Service-Protokolle (XDoS)	0	0
XML-Nachrichtenüberprüfungsproto	0	0
WSI-Protokolle	0	0
XML SQL Injection-Protokolle	0	0
Site-übergreifendes XML-Scripting	0	0
XML-Anhangs-Protokolle	0	0
SOAP-Fehlerprotokolle	0	0
Generische XML-Protokolle	0	0
Log-Meldungen insgesamt	0	0

Statistikrate für Serverfehler (/s) > Gesamt		
HTTP Client Errors (4xx Resp)	0	0
HTTP Server Errors (5xx Resp)	0	0

Anzeigen von Statistiken zur Einschleusung von HTML-Befehlen mit der Citrix ADC GUI

Führen Sie die folgenden Schritte aus, um die Statistiken zur Einschleusung von Befehlen anzuzeigen:

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich ein Web App Firewall Profil aus und klicken Sie auf **Statistiken**.
3. Auf der Seite **Statistik der Citrix Web App Firewall** werden die HTML-Befehle zum Einschleusung von Datenverkehr und Verstößen angezeigt.
4. Sie können **Tabellarische Ansicht** auswählen oder zu **Graphische Ansicht** wechseln, um die Daten in einem tabellarischen oder grafischen Format anzuzeigen.

HTML-Befehl Injection Traffic-Statistiken

HTML SQL Injection logs	0	0
HTML SQL transform logs	0	0
Field format logs	0	0
Field consistency logs	0	0
Credit cards	0	0
Credit card transform logs	0	0
Safe object logs	0	0
Signature logs	0	0
Content Type logs	0	0
JSON Denial of Service logs	0	0
JSON SQL injection logs	0	0
JSON Cross-Site Scripting logs	0	0
File upload types logs	0	0
Infer Content Type XML Payload Logs	0	0
HTML Command Injection logs	0	0
XML Format logs	0	0
XML Denial of Service(XDoS) logs	0	0
XML Message Validation logs	0	0
WSI logs	0	0
XML SQL Injection logs	0	0
XML XSS logs	0	0
XML Attachment logs	0	0

HTML-Befehlsverletzungsstatistiken für die Einschleusung

HTML/XML/JSON Violation Statistics

	Rate (/s)	Total	
Start URL	0	0	0%
Deny URL	0	0	0%
Referer header	0	0	0%
Buffer overflow	0	0	0%
Cookie consistency	0	0	0%
Cookie hijacking	0	0	0%
CSRF form tag	0	0	0%
HTML Cross-site scripting	0	0	0%
HTML SQL injection	0	0	0%
Field format	0	0	0%
Field consistency	0	0	0%
Credit card	0	0	0%
Safe object	0	0	0%
Signature logs	0	0	0%
Content Type	0	0	0%
JSON Denial of Service	0	0	0%
JSON SQL injection	0	0	0%
JSON Cross-Site Scripting	0	0	0%
File Upload Types	0	0	0%
Infer Content Type XML Payload	0	0	0%
HTML CMD Injection	0	0	0%
XML Format	0	0	0%
XML Denial of Service (XDoS)	0	0	
XML Message Validation	0	0	
Web Services Interoperability	0	0	

XML Externe Entitäten (XXE) Angriffsschutz

October 5, 2021

Der XXE-Angriffsschutz (XML Externe Entitäten) prüft, ob eine eingehende Payload eine nicht autorisierte XML-Eingabe in Bezug auf Entitäten außerhalb der vertrauenswürdigen Domäne hat, in der sich die Webanwendung befindet. Der XXE-Angriff tritt auf, wenn Sie einen schwachen XML-Parser haben, der eine XML-Nutzlast mit Eingaben analysiert, die Verweise auf externe Entitäten enthalten.

Wenn der XML-Parser in einer Citrix ADC Appliance nicht ordnungsgemäß konfiguriert ist, kann die Ausnutzung der Sicherheitsanfälligkeit gefährlich sein. Es ermöglicht einem Angreifer, sensible Daten auf dem Webserver zu lesen. Führe den Denial-of-Service-Angriff aus und so weiter. Daher ist es wichtig, die Appliance vor XXE-Angriffen zu schützen. Web Application Firewall ist in der Lage, die Appliance vor XXE-Angriffen zu schützen, solange der Inhaltstyp als XML identifiziert wird. Um zu verhindern, dass ein böswilliger Benutzer diesen Schutzmechanismus umgeht, blockiert WAF eine eingehende Anforderung, wenn der "abgeleitete" Inhaltstyp in den HTTP-Headern nicht mit dem Inhaltstyp des Körpers übereinstimmt. Dieser Mechanismus verhindert die Umgehung des XXE-Angriffsschutzes, wenn ein standardmäßiger oder nicht standardmäßiger Inhaltstyp auf der Positivliste verwendet wird.

Einige der möglichen XXE-Bedrohungen, die eine Citrix ADC Appliance betreffen, sind:

- Lecks vertraulicher Daten
- Denial-of-Service (DOS) Angriffe
- Serverseitige Fälschungsanforderungen
- Port-Scannen

Konfigurieren des XXE-Einschleusungsschutzes für externe XML-Entitäten

So konfigurieren Sie die Prüfung von externen XML-Entitäten (XXE) mithilfe der Befehlszeilenschnittstelle:
In der Befehlszeilenschnittstelle können Sie den Befehl Application Firewall-Profil hinzufügen oder ändern, um die **XXE-Einstellungen** zu konfigurieren. Sie können die Block-, Protokoll- und Statistikaktionen aktivieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set appfw profile <name> [-inferContentTypeXmlPayloadAction <inferContentTypeXmlPayloa
 <block | log | stats | none>]
```

> Hinweis:
>
> Standardmäßig ist die XXE-Aktion auf "none" festgelegt.

Beispiel:


```
set appfw profile profile1 -inferContentTypeXmlPayloadAction Block
```

Wo sind Aktionstypen:

Blockieren: Die Anforderung wird ohne Ausnahme von den URLs in der Anforderung blockiert.

Log: Wenn eine Nichtübereinstimmung zwischen Inhaltstyp in einem HTTP-Anforderungsheader und Payload auftritt, müssen Informationen über die verletzende Anforderung in der Protokollmeldung enthalten sein.

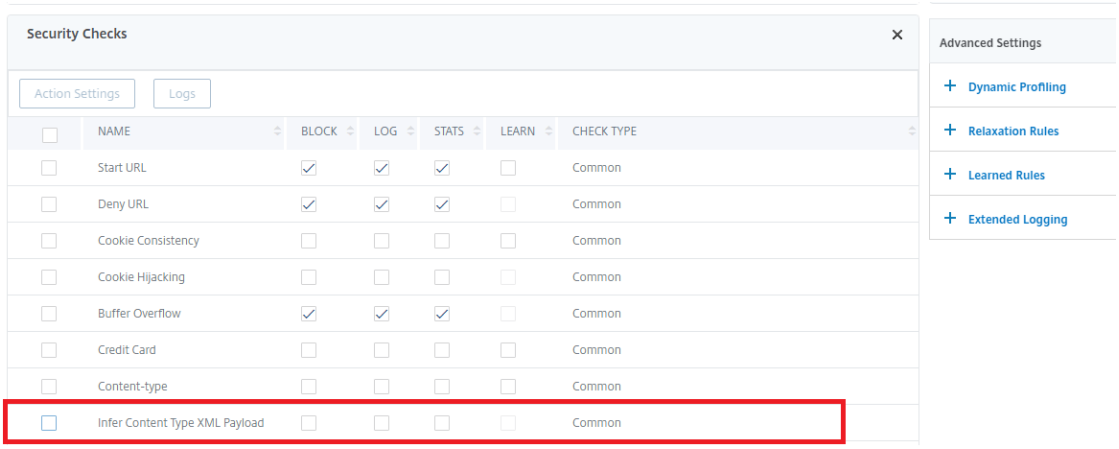
Statistiken: Wenn eine Nichtübereinstimmung in den Inhaltstypen festgestellt wird, wird die entsprechende Statistik für diesen Verstoßtyp erhöht.

Keine: Es wird keine Aktion ausgeführt, wenn eine Nichtübereinstimmung in Inhaltstypen festgestellt wird. Keine kann nicht mit einem anderen Aktionstyp kombiniert werden. Die Standardaktion ist auf Keine festgelegt.

Konfigurieren der XXE-Einschleusungsprüfung über die Citrix ADC GUI

Führen Sie die folgenden Schritte aus, um die XXE-Injectionsprüfung zu konfigurieren.

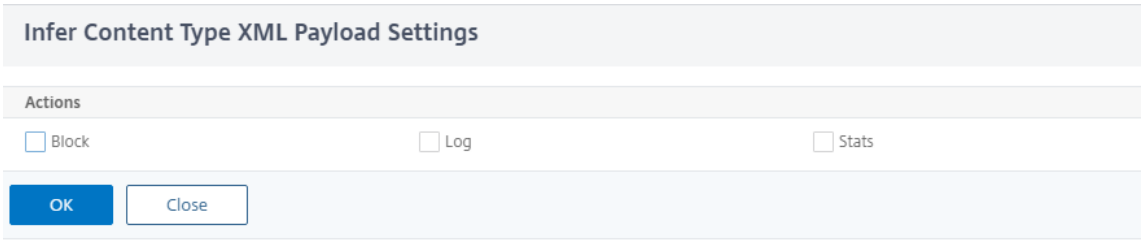
1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profile**.
2. Wählen Sie auf der Seite **Profile** ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Wechseln Sie auf der Seite **Citrix Web App Firewall Profil** zum Abschnitt **Erweiterte Einstellungen** und klicken Sie auf **Sicherheitsprüfungen**.



4. Wählen Sie im Abschnitt **Sicherheitsprüfungen** die Option **Content-Typ XML Payload ableiten**, und klicken Sie auf **Aktionseinstellungen**.
5. Legen Sie auf der Seite XML-Payload-Einstellungen für den Ableiten des Inhaltstyps die folgenden Parameter fest:

   a) Aktionen. Wählen Sie eine oder mehrere Aktionen aus, die für die XXE-Injectionssicherheitsprüfung ausgeführt werden sollen.

6. Klicken Sie auf **OK**.



Anzeigen von XXE-Einschleusungsdatenverkehrs und Verstößen

Auf der Seite Citrix Web App Firewall -Statistiken werden Details zu Sicherheitsdatenverkehr und Sicherheitsverletzungen in einem tabellarischen oder grafischen Format angezeigt.

So zeigen Sie Sicherheitsstatistiken mithilfe der Befehlszeilenschnittstelle an.

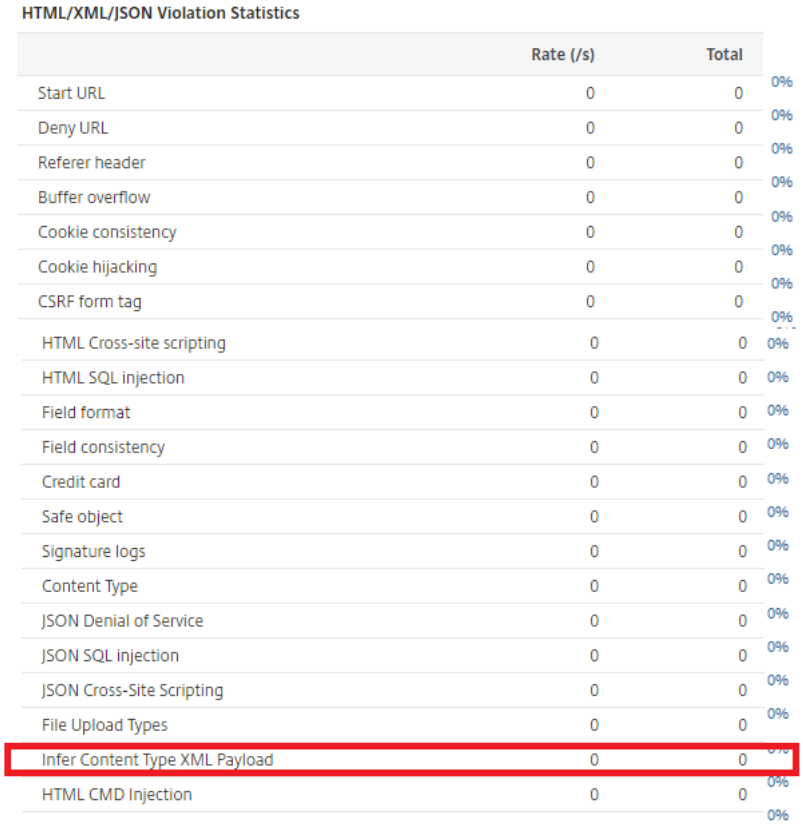
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat appfw profile profile1
```

Anzeigen von XXE-Injection-Statistiken über die Citrix ADC GUI

Führen Sie die folgenden Schritte aus, um die XXE-Injectionsstatistik anzuzeigen:

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich ein Web App Firewall Profil aus und klicken Sie auf **Statistiken**.
3. Auf der Seite **Statistiken der Citrix Web App Firewall** werden die Details zum XXE-Befehl Injection Traffic und Verletzungen angezeigt.
4. Sie können **Tabellarische Ansicht** auswählen oder zu **Graphische Ansicht** wechseln, um die Daten in einem tabellarischen oder grafischen Format anzuzeigen.



HTML/XML/JSON Violation Statistics

	Rate (/s)	Total	
Start URL	0	0	0%
Deny URL	0	0	0%
Referer header	0	0	0%
Buffer overflow	0	0	0%
Cookie consistency	0	0	0%
Cookie hijacking	0	0	0%
CSRF form tag	0	0	0%
HTML Cross-site scripting	0	0	0%
HTML SQL injection	0	0	0%
Field format	0	0	0%
Field consistency	0	0	0%
Credit card	0	0	0%
Safe object	0	0	0%
Signature logs	0	0	0%
Content Type	0	0	0%
JSON Denial of Service	0	0	0%
JSON SQL injection	0	0	0%
JSON Cross-Site Scripting	0	0	0%
File Upload Types	0	0	0%
Infer Content Type XML Payload	0	0	0%
HTML CMD Injection	0	0	0%

Pufferüberlaufprüfung

December 7, 2021

Die Pufferüberlaufprüfung erkennt Versuche, einen Pufferüberlauf auf dem Webserver zu verursachen. Wenn die Web App Firewall feststellt, dass die URL, Cookies oder Header länger als die konfigurierte Länge sind, blockiert sie die Anforderung, da sie zu einem Pufferüberlauf führen kann.

Die Pufferüberlaufprüfung verhindert Angriffe auf unsichere Betriebssystem- oder Webserver-Software, die abstürzen oder sich unvorhersehbar verhalten können, wenn sie eine Datenzeichenfolge empfängt, die größer ist als sie verarbeiten kann. Richtige Programmiertechniken verhindern Pufferüberläufe, indem eingehende Daten überprüft und überlange Zeichenfolgen zurückgewiesen oder abgeschnitten werden. Viele Programme überprüfen jedoch nicht alle eingehenden Daten und sind daher anfällig für Pufferüberläufe. Dieses Problem betrifft insbesondere ältere Versionen von Web-Server-Software und Betriebssystemen, von denen viele noch verwendet werden.

Mit der Sicherheitsprüfung Pufferüberlauf können Sie die Aktionen **Blockieren**, **Protokollieren** und **Statistiken** konfigurieren. Darüber hinaus können Sie auch die folgenden Parameter konfigurieren:

- **Maximale URL-Länge**. Die maximale Länge, die die Web App Firewall in einer angeforderten URL zulässt. Anfragen mit längeren URLs werden blockiert. **Mögliche Werte**: 0—65535. **Standard**: 1024
- **Maximale Cookie-Länge** Die maximale Länge, die die Web App Firewall für alle Cookies in einer Anfrage erlaubt. Anfragen mit längeren Cookies lösen die Verstöße aus. **Mögliche Werte**: 0—65535. **Standard**: 4096
- **Maximale Kopfzeilenlänge**. Die maximale Länge, die die Web App Firewall HTTP-Header zulässt. Anfragen mit längeren Kopfzeilen werden blockiert. **Mögliche Werte**: 0—65535. **Standard**: 4096
- **Länge der Abfragezeichenfolge**. Maximal zulässige Länge für Abfragezeichenfolge in einer eingehenden Anforderung. Anfragen mit längeren Abfragen werden blockiert. Mögliche Werte: 0—65535. Standard: 1024
- **Gesamtlänge der Anfrage**. Maximale Anforderungslänge für eine eingehende Anforderung. Anfragen mit längerer Länge werden blockiert. Mögliche Werte: 0—65535. Standard: 24820

Verwenden der Befehlszeile zum Konfigurieren der Sicherheitsprüfung Pufferüberlauf

So konfigurieren Sie Pufferüberlauf-Sicherheitsüberprüfungsaktionen und andere Parameter mit der Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add appfw profile <name> -bufferOverflowMaxURLLength <positive_integer> -
bufferOverflowMaxHeaderLength <positive_integer> - bufferOverflowMaxCookieLength
 <positive_integer> -bufferOverflowMaxQueryLength <positive_integer> -
bufferOverflowMaxTotalHeaderLength <positive_integer>
```

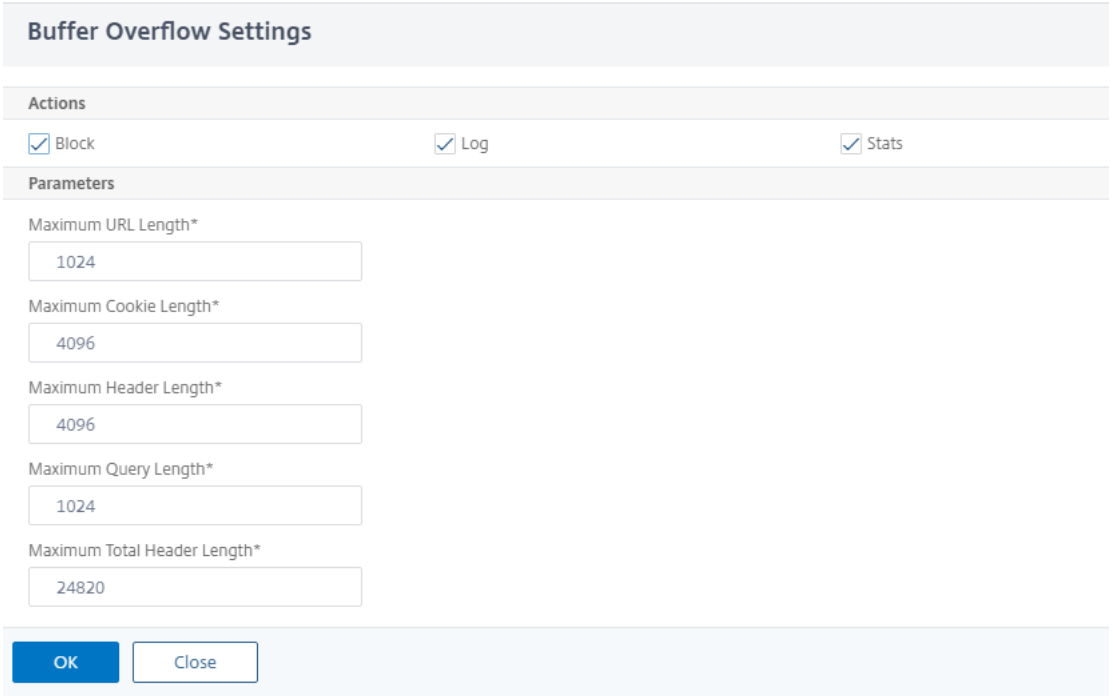
Beispiel:

```
add appfw profile profile1 -bufferOverflowMaxURLLength 7000 -bufferOverflowMaxHeaderLe
 7250 - bufferOverflowMaxCookieLength 7100 -bufferOverflowMaxQueryLength
7300 -bufferOverflowMaxTotalHeaderLength 7300
```

Konfigurieren der Pufferüberlauf-Sicherheitsprüfung über die Citrix ADC GUI

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** und **Profile**.
2. Wählen Sie auf der Seite **Profile** ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Wechseln Sie auf der Seite **Citrix Web App Firewall Profil** zum Abschnitt **Erweiterte Einstellungen** und klicken Sie auf **Sicherheitsprüfungen**.
4. Wählen Sie im Abschnitt **Sicherheitsüberprüfungen** die Option **Pufferüberlauf** aus, und klicken Sie auf **Aktionseinstellungen**.

5. Legen Sie auf der Seite **Pufferüberlauf-Einstellungen** die folgenden Parameter fest.
   a. Aktionen. Wählen Sie eine oder mehrere Aktionen aus, die für die Sicherheitsprüfung der Befehlseinschleusung ausgeführt werden sollen.
   b. Maximale URL-Länge. Maximale Länge (in Zeichen) für URLs auf Ihren geschützten Websites. Anfragen mit längeren URLs werden blockiert.
   c. Maximale Länge von Cookies. Maximale Länge (in Zeichen) für Cookies, die an Ihre geschützten Websites gesendet werden. Anfragen mit längeren Cookies werden blockiert.
   d. Maximale Kopfzeilenlänge. Maximale Länge (in Zeichen) für HTTP-Header in Anfragen, die an Ihre geschützten Websites gesendet werden. Anfragen mit längeren Kopfzeilen werden blockiert.
   e. Maximale Abfragelänge. Maximale Länge (in Byte) für Abfragezeichenfolgen, die an Ihre geschützten Websites gesendet werden. Anfragen mit längeren Abfragezeichenfolgen werden blockiert.
   f. Maximale Gesamtlänge der Kopfzeile. Maximale Länge (in Byte) für die gesamte HTTP-Headerlänge in Anfragen, die an Ihre geschützten Websites gesendet werden. Der Mindestwert dieser und MaxHeaderLen in HttpProfile wird verwendet. Anfragen mit längerer Länge werden blockiert.
6. Klicken Sie auf **OK** und **schließen**.



Verwenden der Protokollfunktion mit der Sicherheitsprüfung für Pufferüberlauf

Wenn die Protokollaktion aktiviert ist, werden die Verletzungen der Pufferüberlauf-Sicherheitsprüfung im Überwachungsprotokoll als Verletzungen **APPFW_BUFFEROVERFLOW_URL**, **APPFW_BUFFEROVERFLOW_CO** **APPFW_BUFFEROVERFLOW_HDR**protokolliert. Die Web App Firewall unterstützt sowohl native als auch CEF-Protokollformate. Sie können die Protokolle auch an einen entfernten Syslog-Server senden.

Wenn Sie die Protokolle mit der grafischen Benutzeroberfläche überprüfen, können Sie die Funktion Klick-zu-Deploy verwenden, um die in den Protokollen angegebenen Entspannungen anzuwenden.

So greifen Sie mit der Befehlszeile auf die Protokollmeldungen zu

Wechseln Sie zur Shell und fahren Sie die ns.logs im Ordner **/var/log/** ab, um auf die Protokollmeldungen zuzugreifen, die sich auf die Verletzungen des Pufferüberlaufs beziehen:

```
1 > \*\*Shell\*\*
2 > \*\*tail -f /var/log/ns.log | grep APPFW_BUFFEROVERFLOW\*\*
3 <!--NeedCopy-->
```

Beispiel für eine CEF-Protokollmeldung mit BufferOverflowMaxCookieLength-Verletzung im nicht-blockierten Modus

```
1 Oct 22 17:35:20 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
      .0|APPFW|\*\*APPFW_BUFFEROVERFLOW_COOKIE\*\*|6|src=10.217.253.62
      geolocation=Unknown spt=41198 method=GET request=http://aaron.
      stratum8.net/FFC/sc11.html \*\*msg=Cookie header length(43) is
      greater than maximum allowed(16).\*\* cn1=119 cn2=465 cs1=
      owa_profile cs2=PPE1 cs3=wvOOOb+cJ2ZRbstZpyeNXIqLj7Y0001 cs4=ALERT
      cs5=2015 \*\*act=not blocked\*\*
2 <!--NeedCopy-->
```

Beispiel für eine CEF-Protokollmeldung mit BufferOverflowMaxURLength Verletzung im Nicht-Blockmodus

```
1 Oct 22 18:39:56 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
      .0|APPFW|\*\*APPFW_BUFFEROVERFLOW_URL\*\*|6|src=10.217.253.62
      geolocation=Unknown spt=19171 method=GET request=http://aaron.
      stratum8.net/FFC/sc11.html \*\*msg=URL length(39) is greater than
      maximum allowed(20).\*\* cn1=707 cn2=402 cs1=owa_profile cs2=PPE0
      cs3=kW49GcKbnwKByByi3+jeNzfgWa80000 cs4=ALERT cs5=2015 \*\*act=not
      blocked\*\*
```



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

Beispiel für eine Meldung des Native Format-Protokolls mit BufferOverflowMaxHeaderLength-Verletzung im Blockmodus

```
Oct 22 18:44:00 <local0.info> 10.217.31.98 10/22/2015:18:44:00 GMT ns
    0-PPE-2 : default APPFW \*\*APPFW_BUFFEROVERFLOW_HDR\*\* 155 0 :
    10.217.253.62 374-PPE2 khhBEeY4DB8V2D3H2sMLkXmfWnA0002 owa_profile
    \*\*Header(User-Agent) length(82) is greater than maximum allowed
    (10)\*\* : http://aaron.stratum8.net/ \*\*<blocked>\*\*
<!--NeedCopy-->
```

So greifen Sie mit der GUI auf die Protokollmeldungen zu

Die Citrix GUI enthält ein nützliches Tool (**Syslog Viewer**) zum Analysieren der Protokollmeldungen. Sie haben mehrere Optionen für den Zugriff auf den Syslog Viewer:

- Navigieren Sie zu **Anwendungsfirewall** > **Profile**, wählen Sie das Zielprofil aus, und klicken Sie auf **Sicherheitsprüfungen**. Markieren Sie die Zeile **Pufferüberlauf**, und klicken Sie auf **Protokolle** . Wenn Sie direkt über die Sicherheitsprüfung des Buffer Overflow Security Check des Profils auf die Protokolle zugreifen, filtert die GUI die Protokollmeldungen aus und zeigt nur die Protokolle an, die diese Sicherheitsüberprüfungsverletzungen betreffen.
- Sie können auch auf den Syslog Viewer zugreifen, indem Sie zu **NetScaler** > **System** > **Auditing navigieren** . Klicken Sie im Abschnitt Überwachungsmeldungen auf den Link **Syslog-Nachrichten**, um den Syslog Viewer anzuzeigen, der alle Protokollmeldungen einschließlich anderer Protokolle gegen Sicherheitsüberprüfungen anzeigt. Dies ist nützlich für das Debuggen, wenn während der Anforderungsverarbeitung mehrere Sicherheitsüberprüfungsverletzungen ausgelöst werden können.
- Navigieren Sie zu **Anwendungsfirewall** > **Richtlinien** > **Überwachung**. Klicken Sie im Abschnitt **Überwachungsmeldungen** auf den Link **Syslog-Nachrichten**, um den Syslog Viewer anzuzeigen, der alle Protokollmeldungen einschließlich anderer Protokolle gegen Sicherheitsüberprüfungen anzeigt.

Der XML-basierte Syslog Viewer bietet verschiedene Filteroptionen, um nur die Protokollmeldungen auszuwählen, die für Sie von Interesse sind. Um Protokollmeldungen für die **Pufferüberlaufprüfung** auszuwählen, filtern Sie, indem Sie **APPFW** in der Dropdownliste Optionen für **Modul** auswählen. Die Liste **Ereignistyp** bietet drei Optionen, **APPFW_BUFFEROVERFLOW_URL**, **APPFW_BUFFEROVERFLOW_COOKIE** und A**PPFW_BUFFEROVERFLOW_HDR**, um alle Protokollmeldungen anzuzeigen, die sich auf die Sicherheitsprüfung des Pufferüberlaufs beziehen. Sie können eine oder mehrere Optionen auswählen, um Ihre Auswahl weiter zu verfeinern. Wenn Sie beispielsweise das Kontrollkästchen **APPFW_BUFFEROVERFLOW_COOKIE** aktivieren und auf die

Schaltfläche **Übernehmen** klicken, werden im Syslog Viewer nur Protokollmeldungen angezeigt, die sich auf die Verletzungen der **Pufferüberlauf-Sicherheitsprüfung** für den Cookie-Header beziehen. Wenn Sie den Cursor in der Zeile für eine bestimmte Protokollmeldung platzieren, werden unter der Protokollmeldung mehrere Optionen angezeigt, z. B. **Modul**, **Ereignistyp**, **Ereignis-ID** und **Client-IP**. Sie können eine dieser Optionen auswählen, um die entsprechenden Informationen in der Protokollmeldung hervorzuheben.

Click-to-Deploy: Die GUI bietet Klick-zu-Deploy-Funktionalität, die derzeit nur für die Pufferüberlaufprotokollmeldungen unterstützt wird, die sich auf die **URL-Length-Verletzungen**beziehen. Sie können den Syslog Viewer verwenden, um nicht nur die ausgelösten Verstöße anzuzeigen, sondern auch fundierte Entscheidungen basierend auf den beobachteten Längen der blockierten Nachrichten zu treffen. Wenn der aktuelle Wert zu restriktiv ist und False Positives auslöst, können Sie eine Nachricht auswählen und bereitstellen, um den aktuellen Wert durch den URL-Längenwert in der Nachricht zu ersetzen. Die Protokollmeldungen müssen für diesen Vorgang im CEF-Protokollformat vorliegen. Wenn die Entspannung für eine Protokollmeldung bereitgestellt werden kann, wird am rechten Rand des **Syslog Viewer-Felds** in der Zeile ein Kontrollkästchen angezeigt. Aktivieren Sie das Kontrollkästchen, und wählen Sie dann eine Option aus der Liste **Aktion** aus, um die Entspannung bereitzustellen. **Bearbeiten und Bereitstellen**, **Bereitstellen** und **Alle bereitstellen** sind als **Aktionsoptionen** verfügbar. Sie können den Filter **APPFW_BUFFEROVERFLOW_URL** verwenden, um alle Protokollmeldungen zu isolieren, die sich auf die konfigurierten URL-Längenverletzungen beziehen.

Wenn Sie eine einzelne Protokollmeldung auswählen, stehen alle drei Aktionsoptionen **Bearbeiten und Bereitstellen**, **Bereitstellen** und **Alle bereitstellen** zur Verfügung. Wenn Sie **Bearbeiten und Bereitstellen** auswählen, wird der Dialog **Pufferüberlaufeinstellungen** angezeigt. Die neue URL-Länge, die in der Anforderung beobachtet wurde, wird in das Eingabefeld **Maximale URL-Länge** eingefügt. Wenn Sie ohne Änderungen auf **Schließen** klicken, bleiben die aktuell konfigurierten Werte unverändert. Wenn Sie auf die Schaltfläche **OK** klicken, ersetzt der neue Wert der maximalen URL-Länge den vorherigen Wert.

> **Hinweis:**
>
> Die Aktion-Kontrollkästchen **Sperren**, **Protokolle** und **Statistiken** sind im angezeigten Dialogfeld **Pufferüberlaufeinstellungen** deaktiviert und müssen neu konfiguriert werden, wenn Sie die Option **Bearbeiten und Bereitstellen** auswählen. Stellen Sie sicher, dass Sie diese Kontrollkästchen aktivieren, bevor Sie auf **OK** klicken. Andernfalls wird die neue URL-Länge konfiguriert, die Aktionen sind jedoch auf **none** festgelegt.

Wenn Sie die Kontrollkästchen für mehrere Protokollmeldungen aktivieren, können Sie die Option **Bereitstellen** oder **Alle bereitstellen** verwenden. Wenn die bereitgestellten Protokollmeldungen unterschiedliche URL-Längen aufweisen, wird der konfigurierte Wert durch den höchsten Wert der URL-Länge ersetzt, der in den ausgewählten Nachrichten beobachtet wird. Das Bereitstellen der Regel führt nur dazu, dass der Wert **BufferOverflowMaxURLength** geändert wird. Konfigurierte Aktionen

bleiben erhalten und bleiben unverändert.

So verwenden Sie die Klick-und-Deploy-Funktionalität in der GUI

1. Wählen Sie im Syslog Viewer in den Optionen des **Moduls** die Option **APPFW** aus.
2. Aktivieren Sie das Kontrollkästchen **APPFW_BUFFEROVERFLOW_URL** als **Ereignistyp**, um entsprechende Protokollmeldungen zu filtern.
3. Aktivieren Sie das Kontrollkästchen, um die Regel auszuwählen.
4. Verwenden Sie die Dropdownliste **Aktion** mit Optionen, um die Entspannung bereitzustellen.
5. Navigieren Sie zu **Anwendungsfirewall** > **Profile**, wählen Sie das Zielprofil aus, und klicken Sie auf **Sicherheitsprüfungen**, um den Bereich **Pufferüberlaufeinstellungen** aufzurufen, um zu überprüfen, ob der Wert **Maximale URL-Länge** aktualisiert wird.

Statistiken für die Pufferüberlauf-Verstöße

Wenn die Aktion Statistik aktiviert ist, wird der Leistungsindikator für die Sicherheitsprüfung Pufferüberlauf erhöht, wenn die Web App Firewall eine Aktion für diese Sicherheitsprüfung durchführt. Die Statistiken werden für Rate und Gesamtanzahl für Traffic, Verletzungen und Protokolle gesammelt. Die Größe eines Inkrements des Protokollzählers kann abhängig von den konfigurierten Einstellungen variieren. Wenn beispielsweise die Blockaktion aktiviert ist, erhöht eine Anforderung für eine Seite, die drei Pufferüberlaufverletzungen enthält, den Statistikzähler um eins, da die Seite blockiert wird, wenn die erste Verletzung erkannt wird. Wenn der Block jedoch deaktiviert ist, erhöht die Verarbeitung derselben Anforderung den Statistikzähler für Verstöße, da jede Verletzung eine separate Protokollmeldung generiert.

So zeigen Sie Statistiken über die Pufferüberlauf-Sicherheitsprüfung mit der Befehlszeile an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
> sh appfw stats
```

Verwenden Sie den folgenden Befehl, um Statistiken für ein bestimmtes Profil anzuzeigen:

```
> stat appfw profile <profile name>
```

So zeigen Sie Pufferüberlaufstatistiken mit der GUI an

1. Navigieren Sie zu **System** > **Sicherheit** > **Anwendungsfirewall**.
2. Greifen Sie im rechten Bereich auf den **Statistik-Link** zu.
3. Verwenden Sie die Bildlaufleiste, um die Statistiken über Buffer Overflow Verletzungen und Protokolle anzuzeigen. Die Statistiktabelle enthält Echtzeitdaten und wird alle 7 Sekunden aktualisiert.

Highlights

- Die Pufferüberlauf-Sicherheitsprüfung ermöglicht es Ihnen, Limits zu konfigurieren, um die maximale Länge der zulässigen URLs, Cookies und Header zu erzwingen.
- **Sperren**, **Protokollieren**und **Statistiken**ermöglichen es Ihnen, den Datenverkehr zu überwachen und den optimalen Schutz für Ihre Anwendung zu konfigurieren.
- Mit Syslog Viewer können Sie alle Protokollmeldungen im Zusammenhang mit Pufferüberlaufverletzungen filtern und anzeigen.
- **Klick-und-Deploy-Funktionalität** wird für die **BufferOverflowMaxUrlLength-Verletzungen** unterstützt. Sie können eine einzelne Regel auswählen und bereitstellen, oder Sie können mehrere Protokollmeldungen auswählen, um den aktuellen konfigurierten Wert der maximal zulässigen Länge der URL zu optimieren und zu entspannen. Der höchste Wert der URL aus der ausgewählten Gruppe wird als neuer Wert festgelegt, um all diese Anforderungen zuzulassen, die derzeit als Verletzungen gekennzeichnet sind.
- Die Web App Firewall wertet nun einzelne Cookies aus, wenn die eingehende Anfrage überprüft wird. Wenn die Länge eines im Cookie-Header empfangenen Cookies die konfigurierte **BufferOverflowMaxCookieLength**überschreitet, wird die Verletzung des Pufferüberlaufs ausgelöst.

> **Wichtig**
>
> In Release 10.5.e (in einigen Zwischenverbesserungen vor dem Build 59.13xx.e) und in der Version 11.0 (in Builds vor 65.x) wurde die Verarbeitung des Cookie-Headers durch Web App Firewall geändert. In diesen Versionen wird jedes Cookie einzeln ausgewertet, und wenn die Länge eines im Cookie-Header empfangenen Cookies die konfigurierte BufferOverflowMaxCookieLength überschreitet, wird die Pufferüberlaufverletzung ausgelöst. Infolge dieser Änderung können Anfragen, die in 10.5 und früheren Versionen blockiert wurden, zulässig sein, da die Länge des gesamten Cookie-Headers nicht für die Bestimmung der Cookie-Länge berechnet wird . In einigen Situationen ist die gesamte Cookie-Größe, die an den Server weitergeleitet wird, möglicherweise größer als der akzeptierte Wert, und der Server reagiert möglicherweise mit “400 Bad Request”.
>
> Diese Änderung wurde rückgängig gemacht. Das Verhalten in der Version 10.5.e ->59.13xx.e und den nachfolgenden Erweiterungen 10.5.e zusätzlich zu Version 11.0 65.x und nachfolgenden Builds ähnelt nun dem der Builds ohne Erweiterung von Release 10.5. Der gesamte rohe Cookie-Header wird nun bei der Berechnung der Länge des Cookies berücksichtigt. Umgebende Leerzeichen und Semikolon (;) Zeichen, die die Name-Wert-Paare trennen, werden ebenfalls bei der Bestimmung der Cookie-Länge berücksichtigt.

Web App Firewall Unterstützung für Google Web Toolkit

October 5, 2021

Hinweis: Diese Funktion ist in Citrix ADC Version 10.5.e verfügbar.

Webserver, die Google Web Toolkit (GWT) Remote Procedure Call (RPC) -Mechanismen folgen, können durch die Citrix Web App Firewall gesichert werden, ohne dass eine bestimmte Konfiguration erforderlich ist, um die GWT-Unterstützung zu ermöglichen.

Was ist GWT?

Das GWT wird zum Erstellen und Optimieren komplexer Hochleistungs-Webanwendungen von Personen verwendet, die über keine Expertise in XMLHttpRequest und JavaScript verfügen. Dieses Open Source, kostenlose Entwicklungs-Toolkit wird ausgiebig für die Entwicklung von kleinen und großen Anwendungen verwendet und wird häufig verwendet, um Browser-basierte Daten wie Suchergebnisse für Flüge, Hotels usw. anzuzeigen. Das GWT bietet einen Kernsatz von Java-APIs und Widgets zum Schreiben optimierter JavaScript-Skripts, die auf den meisten Browsern und mobilen Geräten ausgeführt werden können. Das GWT RPC-Framework erleichtert es den Client- und Server-Komponenten der Webanwendung, Java-Objekte über HTTP auszutauschen. GWT RPC-Dienste sind nicht identisch mit Webdiensten, die auf SOAP oder REST basieren. Sie sind einfach eine einfache Methode, um Daten zwischen dem Server und der GWT-Anwendung auf dem Client zu übertragen. GWT verarbeitet die Serialisierung der Java-Objekte und tauscht die Argumente in den Methodenaufrufen und den Rückgabewert aus.

Beliebte Websites, die GWT verwenden, finden Sie unter

https://www.quora.com/What-web-applications-use-Google-Web-Toolkit-%28GWT%29

Funktionsweise einer GWT-Anfrage

Die GWT-RPC-Anforderung ist durch Pipe getrennt und hat eine variable Anzahl von Argumenten. Es wird als Payload von HTTP POST getragen und hat die folgenden Werte:

1. Content-type = text/x-gwt-rpc. Charset kann ein beliebiger Wert sein.
2. Method = POST.

Sowohl GET- als auch POST-HTTP-Anforderungen gelten als gültige GWT-Anforderungen, wenn der Inhaltstyp “text/x-gwt-rpc” ist. Abfragezeichenfolgen werden nun als Teil von GWT-Anforderungen unterstützt. Konfigurieren Sie den Parameter “InspectQueryContentTypes” des App-Firewall-Profils auf “OTHER”, um den Anforderungsabfrageteil für den Konent-Typ “text/x-gwt-rpc” zu untersuchen.

Das folgende Beispiel zeigt eine gültige Nutzlast für eine GWT-Anforderung:


```
5|0|8|http://localhost:8080/test/|16878339F02B83818D264AE430C20468| com
    .test.client.TestService|testMethod|java.lang.String|java.lang.
    Integer| myInput1|java.lang.Integer/3438268394|1|2|3|4|2|5|6|7|8|1|
<!--NeedCopy-->
```

Die Anfrage kann in drei Teile unterteilt werden:

a)Header: 5|0|8|

Die ersten 3 Ziffern `5|0|8|` in der obigen Anfrage stellen “Version, Subversion und Größe der Tabelle” dar. Dies müssen positive ganze Zahlen sein.

b) String-Tabelle:

`http://localhost:8080/test/|16878339F02B83818D264AE430C20468| com.test.client.TestService|testMethod|java.lang.String|java.lang.Integer|myInput1|java.lang.Integer/3438268394|`

Die Mitglieder der obigen Pipe getrennten String-Tabelle enthalten die vom Benutzer bereitgestellten Eingaben. Diese Eingaben werden für die Web App Firewall Prüfungen analysiert und wie folgt identifiziert:

- 1.: `http://localhost:8080/test/`

  Dies ist die Anforderungs-URL.

- 2.: `16878339F02B83818D264AE430C20468`

  Eindeutige HEX-ID. Eine Anforderung gilt als falsch formatiert, wenn diese Zeichenfolge Nicht-Hex-Zeichen enthält.

- 3.: `com.test.client.TestService`

  Name der Dienstklasse

- 4.: `testMethod`

  Name der Dienstmethode

- Ab 5.: `java.lang.String|java.lang.Integer|myInput1|java.lang.Integer/3438268394`

  Datentypen und Daten. Nicht-primitive Datentypen werden als

  `<container>.<sub-cntnr>.name/<integer><identifier>`

c)Payload: 1|2|3|4|2|5|6|7|8|1|

Die Nutzlast besteht aus Verweisen auf die Elemente in der String-Tabelle. Diese Ganzzahlwerte dürfen nicht größer sein als die Anzahl der Elemente in der String-Tabelle.

Web App Firewall Schutz für GWT-Anwendungen

Die Web App Firewall versteht und interpretiert GWT RPC-Anforderungen, überprüft die Nutzlast auf Sicherheitsüberprüfungsverletzungen und führt bestimmte Aktionen aus.

Die Header der Web App Firewall und Cookies überprüfen auf GWT-Anforderungen ähneln denen für andere Anforderungsformate. Nach entsprechender URL-Dekodierung und Zeichensatzkonvertierung werden alle Parameter in der String-Tabelle überprüft. Der GWT-Anforderungskörper enthält keine Feldnamen, sondern nur die Feldwerte. Die Eingabewerte können anhand des angegebenen Formats validiert werden, indem Sie die Web App Firewall Feldformatprüfung verwenden, die auch zur Steuerung der Länge der Eingabe verwendet werden kann. Die **Cross-Site Scripting** und **SQL Injection-Angriffe** in den Eingaben können leicht von der Web App Firewall erkannt und vereitelt werden.

Lern- und Relaxationsregeln: Das Lernen und die Bereitstellung von Relaxationsregeln werden für GWT-Anfragen unterstützt. Web App Firewall rules are in the form of <actionURL> <fieldName> mapping. Das GWT-Anforderungsformat hat nicht die Feldnamen und erfordert daher eine spezielle Behandlung. Die Web App Firewall fügt Dummy-Feldnamen in die erlernten Regeln ein, die als Relaxationsregeln bereitgestellt werden können. Das Flag -isRegex funktioniert wie bei Nicht-GWT-Regeln.

- Aktions-URL:

  Mehrere Dienste, die auf einen RPC reagieren, können auf demselben Webserver konfiguriert werden. Die HTTP-Anforderung hat die URL des Webservers, nicht des tatsächlichen Dienstes, der den RPC verarbeitet. Daher wird die Entspannung nicht auf der Grundlage der HTTP-Anforderungs-URL angewendet, da dies alle Dienste auf dieser URL für das Zielfeld lockern würde. Für GWT-Anforderungen verwendet die Web App Firewall die URL des tatsächlichen Dienstes, der in der GWT-Nutzlast gefunden wird, im vierten Feld in der String-Tabelle.

- Feldname:

  Da der GWT-Anforderungskörper nur Feldwerte enthält, fügt die Web App Firewall Dummy-Feldnamen wie 1, 2 usw. ein, wenn erlernte Regeln empfohlen werden.

  Beispiel für eine GWT-Learned Regel

```
POST /abcd/def/gh HTTP/1.1
Content-type: text/x-gwt-rpc
Host: 10.217.222.75
Content-length: 157

5|0|8|http://localhost:8080/acdtest/|16878339
   F02Baf83818D264AE430C20468|
com.test.client.TestService|testMethod|java.lang.String%3b|java.
   lang.Integer|onblur|
```



```
8
9     The learn data will be as follows:
10  > sh learningdata pr1 crossSiteScripting
11  Profile: pr1    SecurityCheck: crossSiteScripting
12  1)  Url:    http://localhost:8080/acdtest/  >> From GWT Payload.
13      Field:  10
14      Hits:   1
15   Done
16  <!--NeedCopy-->
```

Beispiel für eine GWT-Relaxationsregel

```
bind appfw profile pr1 -crossSiteScripting 1 abcd -isregex NOTREGEX
```

Protokollmeldungen: Die Web App Firewall generiert Protokollmeldungen für die Sicherheitsüberprüfungsverletzungen, die in den GWT-Anforderungen erkannt werden. Eine Protokollnachricht, die von einer fehlerhaften GWT-Anforderung generiert wird, enthält die Zeichenfolge GWT zur einfachen Identifizierung.

Beispiel für eine Protokollnachricht für fehlerhafte GWT-Anforderung:

```
Dec 5 21:48:02 <local0.notice> 10.217.31.247 12/05/2014:21:48:02 GMT ns
0-PPE-0 : APPFW Message 696 0 : "GWT RPC request with malformed payload. <
blocked>"
```

Unterschied in der Verarbeitung von GWT gegenüber Nicht-GWT-Anforderungen:

Dieselbe Nutzlast kann verschiedene Verletzungen der Web App Firewall Sicherheitsprüfung für verschiedene Inhaltstypen auslösen. Betrachten Sie das folgende Beispiel:

```
5|0|8|http://localhost:8080/acdtest/|16878339F02Baf83818D264AE430C20468|com
.test.client.TestService|testMethod|java.lang.String%3b|java.lang.Integer|
select|
```

Content-type: application/x-www-form-urlencoded:

Eine mit diesem Inhaltstyp gesendete Anforderung führt zu einer SQL-Verletzung, wenn der SQL-Injectionstyp so konfiguriert ist, dass eine der vier verfügbaren Optionen verwendet wird: SQLSplCharAndKeyword, SQLSplCharorKeyword, SQLKeyword oder SQLSplchar. Die Web App Firewall betrachtet '&' als Feldtrennzeichen und '=' als Name-Wert-Trennzeichen bei der Verarbeitung der obigen Nutzlast. Da keines dieser Zeichen irgendwo im Posttext angezeigt wird, wird der gesamte Inhalt als einzelner Feldname behandelt. Der Feldname in dieser Anforderung enthält sowohl ein SQL-Sonderzeichen (;) als auch ein SQL-Schlüsselwort (select). Daher werden Verstöße für alle vier SQL-Injection-Typoptionen abgefangen.

Content-type: text/x-gwt-rpc:

Eine Anforderung, die mit diesem Inhaltstyp gesendet wird, löst eine SQL-Verletzung nur aus, wenn der SQL-Injectionstyp auf eine der folgenden drei Optionen festgelegt ist: SQLSplCharORKeyword,SQLKeyword oder SQLSplChar. Es wird keine Verletzung ausgelöst, wenn der SQL-Injectionstyp auf SQLSplCharANDKeyword festgelegt ist, was die Standardoption ist. Die Web App Firewall betrachtet den vertikalen Balken | als Feldtrennzeichen für die oben genannte Nutzlast in der GWT-Anforderung. Daher wird der Postkörper in verschiedene Formularfeldwerte unterteilt, und Formularfeldnamen werden hinzugefügt (entsprechend der oben beschriebenen Konvention). Aufgrund dieser Aufteilung werden das SQL-Sonderzeichen und das SQL-Schlüsselwort zu Teilen separater Formularfelder.

Formularfeld 8: `java.lang.String%3b -\> %3b is the (;)char`

Formularfeld 10: `select`

Wenn SQL Injection Type auf **SQLSplchar**festgelegt ist, zeigt Feld 8 die SQL-Verletzung an. Für **SQLKeyword**gibt Feld 10 die Verletzung an. Beide Felder können auf eine Verletzung hinweisen, wenn der Typ SQL Inject mit der Option **SQLSplCharorKeyword** konfiguriert ist, die nach dem Vorhandensein eines Schlüsselworts oder eines Sonderzeichens sucht. Für die Standardoption **SQLSplCharAndKeyword** wird keine Verletzung abgefangen, da kein einzelnes Feld mit einem Wert vorhanden ist, der sowohl **SQLSplchar** als auch **SQLKeyword** zusammen enthält.

Tipps:

- Für die Aktivierung der GWT-Unterstützung ist keine spezielle Konfiguration der Web App Firewall erforderlich.
- Der Content-Typ muss text/x-gwt-rpc sein.
- Das Lernen und Bereitstellen der Relaxationsregeln für alle relevanten Web App Firewall -Sicherheitsprüfungen, die auf GWT-Nutzlast angewendet werden, funktioniert genauso wie für die anderen unterstützten Inhaltstypen.
- Nur POST-Anfragen gelten für GWT als gültig. Alle anderen Anforderungsmethoden werden blockiert, wenn der Inhaltstyp text/x-gwt-rpc ist.
- GWT-Anforderungen unterliegen dem konfigurierten POST-Body-Limit des Profils.
- Die Sitzungslose Einstellung für die Sicherheitsprüfungen ist nicht anwendbar und wird ignoriert.
- Das CEF-Protokollformat wird für die GWT-Protokollmeldungen unterstützt.

Cookie-Schutz

October 5, 2021

Cookie ist ein kleines Paket, das von einem Webserver an einen Clientbrowser gesendet wird. Cookies enthalten sensible Daten wie Kennwörter, Details zur Benutzerauthentifizierung und Anmeldein-

formationen über eine HTTP-Verbindung und werden in einem Webbrowser gespeichert. Daher ist es äußerst wichtig, Cookies vor Angreifern zu schützen, die Informationen stehlen.

Konsistenzprüfung von Cookies: Untersucht Cookies, die mit Benutzeranfragen zurückgegeben werden, um zu überprüfen, ob sie mit den Cookies übereinstimmen, die Ihr Webserver für diesen Benutzer Wenn ein modifiziertes Cookie gefunden wird, wird es aus der Anforderung entfernt, bevor die Anforderung an den Webserver weitergeleitet wird. Weitere Informationen finden Sie unter Thema Überprüfung der Cookie-Konsistenzprüfung .

Schutz vor Cookie-Hijacking: Hijacking bezieht sich auf eine Situation, in der ein Angreifer einen unbefugten Zugriff auf Cookies erhält. Um das Cookie vor autorisiertem Zugriff zu schützen, fordert die Citrix ADC Web App Firewall (WAF) die TLS-Verbindung des Clients zusammen mit der Validierung der WAF-Konsistenz heraus. Für jede neue Clientanforderung validiert die Appliance die TLS-Verbindung und überprüft auch die Konsistenz von Anwendungs- und Sitzungscookie in der Anforderung. Weitere Informationen finden Sie unter Thema Schutz bei Cookie-Hijacking .

`SameSite` SameSite-Cookie-Attribut: Das Attribut in der Set-Cookie-HTTP-Antwort ermöglicht es Ihnen zu erklären, ob Ihr Cookie auf einen Erstanbieter- oder gleichen Site-Kontext beschränkt sein muss. Die Cookie-Einstellung mindert Angriffe und bietet eine gesicherte Webkommunikation. Weitere Informationen finden Sie unter Thema SameSite-Cookie-Attribut .

Cookie-Konsistenzprüfung

October 5, 2021

Die Cookie-Konsistenzprüfung untersucht von Benutzern zurückgegebene Cookies, um sicherzustellen, dass sie mit den Cookies übereinstimmen, die Ihre Website für diesen Benutzer gesetzt hat. Wenn ein modifiziertes Cookie gefunden wird, wird es von der Anforderung entfernt, bevor die Anforderung an den Webserver weitergeleitet wird. Sie können die Cookie-Konsistenzprüfung auch so konfigurieren, dass alle von ihm verarbeiteten Server-Cookies transformiert werden, indem Sie die Cookies verschlüsseln, die Cookies über Proxy zu verarbeiten oder Flags zu den Cookies hinzufügen. Diese Prüfung gilt für Anfragen und Antworten.

Ein Angreifer würde normalerweise ein Cookie ändern, um Zugriff auf vertrauliche private Informationen zu erhalten, indem er sich als zuvor authentifizierter Benutzer posiert oder einen Pufferüberlauf verursacht. Die Pufferüberlaufprüfung schützt vor Versuchen, einen Pufferüberlauf durch Verwendung eines langen Cookies zu verursachen. Die Cookie-Konsistenzprüfung konzentriert sich auf das erste Szenario.

Wenn Sie den Assistenten oder die GUI verwenden, können
Sie im Dialogfeld Cookie-Konsistenzprüfung ändern auf der Registerkarte
Allgemein die folgenden Aktionen aktivieren oder deaktivieren:

- Blockieren
- Protokollierung
- Erfahren Sie mehr
- Statistik
- Transformieren. Wenn diese Option aktiviert ist, ändert die Aktion Transformieren alle Cookies wie in den folgenden Einstellungen angegeben:
  - **Verschlüsseln Sie Server-Cookies.** Verschlüsseln Sie Cookies, die von Ihrem Webserver festgelegt wurden, mit Ausnahme der in der Liste Cookie Consistency Check aufgeführten Cookies, bevor Sie die Antwort an den Client weiterleiten. Verschlüsselte Cookies werden entschlüsselt, wenn der Client eine nachfolgende Anfrage sendet, und die entschlüsselten Cookies werden wieder in die Anforderung eingefügt, bevor sie an den geschützten Webserver weitergeleitet werden. Geben Sie einen der folgenden Verschlüsselungstypen an:
    * **Keine.** Verschlüsseln oder entschlüsseln Sie Cookies nicht. Der Standardwert.
    * **Nur entschlüsseln.** Entschlüsseln Sie nur verschlüsselte Cookies. Verschlüsseln Sie keine Cookies.
    * **Nur Sitzung verschlüsseln.** Verschlüsseln Sie nur Session-Cookies. Verschlüsseln Sie keine persistenten Cookies. Verschlüsselte Cookies entschlüsseln.
    * **Verschlüsseln Sie alle.** Verschlüsseln Sie sowohl Sitzungs- als auch persistente Cookies. Verschlüsselte Cookies entschlüsseln.

      Hinweis: Beim Verschlüsseln von Cookies fügt die Web App Firewall dem Cookie das **HttpOnly-Flag**hinzu. Dieses Flag verhindert, dass Skripts auf den Cookie zugreifen und diese analysieren. Das Flag verhindert daher, dass ein skriptbasierter Virus oder Trojaner auf ein entschlüsseltes Cookie zugreifen und diese Informationen verwenden, um die Sicherheit zu verletzen. Dies geschieht unabhängig von den Parametereinstellungen für Flags zum Hinzufügen in Cookies, die unabhängig von den Parametereinstellungen für Encrypt Server Cookies behandelt werden.
- **Proxyserver-Cookies.** Proxy alle nicht persistenten (Sitzungs-) Cookies, die von Ihrem Webserver gesetzt werden, mit Ausnahme der in der Cookie-Konsistenzliste aufgeführten Cookies. Für Cookies wird mit das vorhandenen Sitzungscookies der Web App Firewall als Proxy verwender. Die Web App Firewall entfernt vom geschützten Webserver gesetzte Session-Cookies und speichert diese lokal, bevor die Antwort an den Client weitergeleitet wird. Wenn der Client eine nachfolgende Anforderung sendet, setzt die Web App Firewall die Session-Cookies wieder in die Anforderung ein, bevor sie an den geschützten Webserver weitergeleitet wird. Geben Sie eine der folgenden Einstellungen an:
  - **Keine.** Proxy Cookies nicht. Der Standardwert.
  - **Nur Sitzung.** Nur Proxy-Sitzungs-Cookies. Keine persistenten Proxy-Cookies
    Hinweis: Wenn Sie das Cookie-Proxying nach der Aktivierung deaktivieren (setzen Sie diesen Wert auf None, nachdem er nur auf Session festgelegt wurde), wird der Cookie-Proxying für Sitzungen beibehalten, die eingerichtet wurden, bevor Sie ihn deaktiviert

haben. Sie können diese Funktion daher sicher deaktivieren, während die Web App Firewall Benutzersitzungen verarbeitet.

- **Flags, die in Cookies hinzugefügt werden sollen**. Fügen Sie Flags zu Cookies während der Transformation hinzu. Geben Sie eine der folgenden Einstellungen an:
  - **Keine.** Fügen Sie keine Flags zu Cookies hinzu. Der Standardwert.
  - **Nur HTTP.** Fügen Sie das HttpOnly-Flag zu allen Cookies hinzu. Browser, die das HttpOnly-Flag unterstützen, erlauben Skripts nicht, auf Cookies zuzugreifen, für die dieses Flag festgelegt ist.
  - **Sichern**. Fügen Sie das Secure Flag zu Cookies hinzu, die nur über eine SSL-Verbindung gesendet werden sollen. Browser, die das Secure Flag unterstützen, senden die gekennzeichneten Cookies nicht über eine unsichere Verbindung.
  - **Alles.** Fügen Sie allen Cookies das HttpOnly-Flag hinzu und das Secure Flag zu Cookies, die nur über eine SSL-Verbindung gesendet werden sollen.

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie die folgenden Befehle eingeben, um die Cookie-Konsistenzprüfung zu konfigurieren:

- `set appfw profile <name> -cookieConsistencyAction [**block**] [**learn**] [**log**] [**stats**] [**none**]`
- `set appfw profile <name> -cookieTransforms ([**ON**] | [**OFF**])`
- `set appfw profile <name> -cookieEncryption ([**none**] | [**decryptOnly**] | [**encryptSession**] | [**encryptAll**])`
- `set appfw profile <name> -cookieProxying ([**none**] | [**sessionOnly**])`
- `set appfw profile <name> -addCookieFlags ([**none**] | [**httpOnly**] | [**secure**] | [**all**])`

Um Relaxationen für die Cookie-Konsistenzprüfung festzulegen, müssen Sie die GUI verwenden. Klicken Sie auf der Registerkarte Prüfungen des Dialogfelds Cookie-Konsistenzprüfung ändern auf Hinzufügen, um das Dialogfeld Cookie-Konsistenzprüfung hinzufügen zu öffnen, oder wählen Sie eine vorhandene Entspannung aus, und klicken Sie auf Öffnen, um das Dialogfeld Cookie-Konsistenzprüfung ändern zu öffnen. Beide Dialogfelder bieten die gleichen Optionen für die Konfiguration einer Entspannung.

Im Folgenden finden Sie Beispiele für die Cookie-Konsistenzprüfung:

- **Anmeldefelder.** Der folgende Ausdruck befreit alle Cookie-Namen, die mit der Zeichenfolge logon_ beginnen, gefolgt von einer Zeichenfolge aus Buchstaben oder Zahlen, die mindestens zwei Zeichen lang und höchstens fünfzehn Zeichen lang sind:

```
1 ^logon_[0-9A-Za-z]{
2 2,15 }
```



```
3  $
4  <!--NeedCopy-->
```

- **Anmeldefelder (Sonderzeichen).** Der folgende Ausdruck befreit alle Cookie-Namen, die mit der Zeichenfolge türkçe-logon_ beginnen, gefolgt von einer Zeichenfolge aus Buchstaben oder Zahlen, die mindestens zwei Zeichen lang und höchstens fünfzehn Zeichen lang sind:

```
1  ^txC3xBCrkxC3xA7e-logon_[0-9A-Za-z]{
2  2,15 }
3  $
4  <!--NeedCopy-->
```

- **Beliebige Zeichenfolgen.** Erlauben Sie Cookies, die die Zeichenfolge sc-item_enthalten, gefolgt von der ID eines Artikels, den der Benutzer seinem Warenkorb hinzugefügt hat ([0-9a-Za-Z]+), einem zweiten Unterstrich (_) und schließlich der Anzahl dieser Artikel, die er möchte ([1-9][0-9]?) , um vom Benutzer modifizierbar zu sein:

```
1  ^sc-item_[0-9A-Za-z]+_[1-9][0-9]?$
2  <!--NeedCopy-->
```

Achtung: Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau die URL definieren, die Sie als Ausnahme hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung von Wildcards und insbesondere der Punkt-Sternchen-Kombination (.*) kann zu Ergebnissen führen, die Sie nicht wollen oder erwarten, z. B. das Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten oder einen Angriff zulassen, den die Cookie-Konsistenzprüfung anderweitig hätte geblockt.

> **Wichtig**
>
> In Release 10.5.e (in einigen Interimbuilds mit Erweiterungen vor 59.13xx.e Build) sowie in 11.0 (in Builds vor 65.x) wurde die Verarbeitung des Cookie-Headers von Web App Firewall geändert. In diesen Versionen wird jedes Cookie einzeln ausgewertet, und wenn die Länge eines im Cookie-Header empfangenen Cookies die konfigurierte BufferOverflowMaxCookieLength überschreitet, wird die Pufferüberlaufverletzung ausgelöst. Infolge dieser Änderung können Anfragen, die in 10.5 und früheren Versionen blockiert wurden, zulässig sein, da die Länge des gesamten Cookie-Headers nicht für die Bestimmung der Cookie-Länge berechnet wird . In einigen Situationen ist die Gesamt-Cookie-Größe, die an den Server weitergeleitet wird, möglicherweise größer als der akzeptierte Wert, und der Server antwortet möglicherweise mit “400 Bad Request”.

> **Beachten** Sie, dass diese Änderung rückgängig gemacht wurde. Das Verhalten in den 10.5.e ->59.13xx.e und den nachfolgenden 10.5.e Erweiterungsbuilds sowie in 11.0 Release 65.x und nachfolgenden Builds ähnelt nun dem der Nicht-Erweiterungs-Builds von Release 10.5. Der gesamte rohe Cookie-Header wird nun bei der Berechnung der Länge des Cookies berücksichtigt. Umgebende Leerzeichen und Semikolon (;) Zeichen, die die Name-Wert-Paare trennen, werden ebenfalls bei der Bestimmung der Cookie-Länge berücksichtigt.**
>
> **Hinweis:**
>
> **Sitzungslose Cookie-Konsistenz:** Das Cookie-Konsistenzverhalten hat sich in Release 11.0 geändert. In früheren Versionen ruft die Cookie-Konsistenzprüfung Sitzungen auf. Die Cookies werden in der Sitzung gespeichert und signiert. Ein wlt_Suffix wird an transiente Cookies angehängt und ein wlf_ Suffix wird an die dauerhaften Cookies angehängt, bevor sie an den Client weitergeleitet werden. Selbst wenn der Client diese signierten wlf/wlt-Cookies nicht zurückgibt, verwendet die Web App Firewall die in der Sitzung gespeicherten Cookies, um die Cookie-Konsistenzprüfung durchzuführen.
>
> In Release 11.0 ist die Cookie-Konsistenzprüfung sitzungslos. Die Web App Firewall fügt nun ein Cookie hinzu, das ein Hash aller Cookies ist, die von der Web App Firewall verfolgt werden. Wenn dieses Hash-Cookie oder ein anderes verfolgtes Cookie fehlt oder manipuliert wird, entfernt die Web App Firewall die Cookies, bevor die Anforderung an den Back-End-Server weitergeleitet wird und löst eine Cookie-Konsistenzverletzung aus. Der Server behandelt die Anfrage als neue Anforderung und sendet neue Set-Cookie-Header. Die Cookie-Konsistenzprüfung in Citrix ADC Version 13.0, 12.1 und NetScaler 12.0 und 11.1 hat keine sitzungslose Option.

Cookie-Hijacking Schutz

October 8, 2021

Cookie-Hijacking Schutz mildert Cookie-Diebstahl-Angriffe von Hackern. Bei dem Sicherheitsangriff übernimmt ein Angreifer eine Benutzersitzung, um unbefugten Zugriff auf eine Webanwendung zu erhalten. Wenn ein Benutzer eine Website durchsucht, z. B. Banking-Anwendung, richtet die Website eine Sitzung mit dem Browser ein. Während der Sitzung speichert die Anwendung die Benutzerdaten wie Anmeldeinformationen, Seitenbesuche in einer Cookie-Datei. Die Cookie-Datei wird dann in der Antwort an den Client-Browser gesendet. Der Browser speichert die Cookies, um aktive Sitzungen aufrechtzuerhalten. Der Angreifer kann diese Cookies entweder manuell aus dem Cookie-Speicher des Browsers oder über eine Rouge Browser-Erweiterung stehlen. Der Angreifer verwendet diese Cookies, um Zugriff auf die Webanwendungssitzungen des Benutzers zu erhalten.

Zur Abwehr von Cookie-Angriffen stellt die Citrix ADC Web App Firewall (WAF) die TLS-Verbindung vom Client zusammen mit der Validierung der WAF-Cookie-Konsistenzvalidierung heraus. Für

jede neue Clientanforderung validiert die Appliance die TLS-Verbindung und überprüft auch die Konsistenz von Anwendungs- und Sitzungscookie in der Anforderung. Wenn ein Angreifer versucht, Anwendungscookies und Sitzungscookies, die vom Opfer gestohlen wurden, zu mischen und abzugleichen, schlägt die Validierung der Cookie-Konsistenz fehl, und die konfigurierte Cookie-Hijack-Aktion wird angewendet. Weitere Informationen zur Cookie-Konsistenz finden Sie im Thema Cookie-Konsistenzprüfung .

> **Hinweis:**
>
> Die Cookie-Hijacking Funktion unterstützt Protokollierung und SNMP-Traps. Weitere Informationen zur Protokollierung finden Sie unter ADM-Thema und weitere Informationen zur SNMP-Konfiguration unter SNMP-Thema.

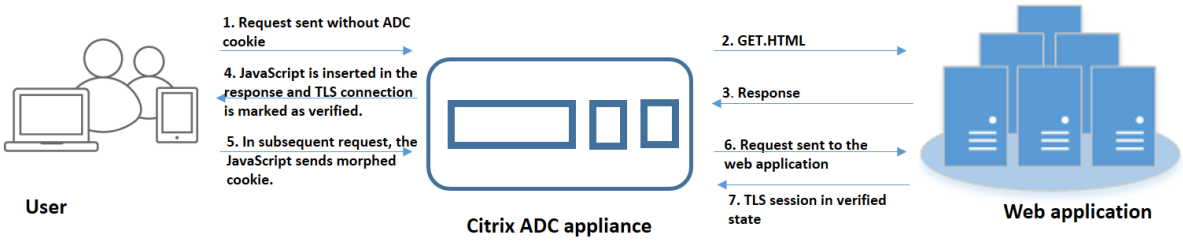
Einschränkungen

- JavaScript muss im Client-Browser aktiviert sein.
- Der Cookie-Hijacking Schutz wird auf TLS Version 1.3 nicht unterstützt.
- Begrenzte Unterstützung für den Internet Explorer (IE) -Browser, da der Browser die SSL-Verbindungen nicht wiederverwendet. Führt zu mehreren Weiterleitungen, die für eine Anfrage gesendet werden, die schließlich zu einem Fehler “MAX READCEED” im IE-Browser führen.

Funktionsweise des Cookie-Hijacking Schutzes

In den folgenden Szenarien wird erläutert, wie der Cookie-Hijacking-Schutz in einer Citrix ADC Appliance funktioniert.

Szenario 1: Benutzer, der ohne Session-Cookie auf die erste Webseite zugreift



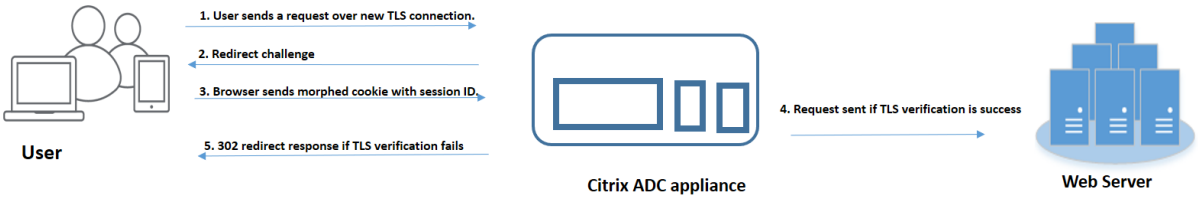
1. Der Benutzer versucht, sich bei einer Webanwendung zu authentifizieren und beginnt ohne ADC-Sitzungscookie in der Anfrage auf die erste Webseite zuzugreifen.
2. Wenn die Anforderung empfangen wird, erstellt die Appliance eine Application Firewall-Sitzung mit einer Sitzungs-Cookie-ID.

3. Dadurch wird eine TLS-Verbindung für die Sitzung initiiert. Da das JavaScript nicht im Client-browser gesendet und ausgeführt wird, markiert die Appliance die TLS-Verbindung als validiert, und es ist keine Herausforderung erforderlich.

   > **Hinweis:**
   >
   > Selbst wenn ein Angreifer versucht, alle App-Cookie-IDs von einem Opfer zu senden, ohne das Sitzungscookie zu senden, erkennt die Appliance das Problem und entfernt alle App-Cookies in der Anfrage, bevor sie die Anforderung an den Back-End-Server weiterleitet. Der Back-End-Server betrachtet diese Anfrage ohne App-Cookie und nimmt entsprechend seiner Konfiguration notwendig.

4. Wenn der Backend-Server eine Antwort sendet, empfängt die Appliance die Antwort und leitet sie mit einem JavaScript-Sitzungstoken und einem Seed-Cookie weiter. Die Appliance markiert dann die TLS-Verbindung als verifiziert.
5. Wenn der Client-Browser die Antwort empfängt, führt der Browser das JavaScript aus und generiert eine morphierte Cookie-ID mit dem Sitzungstoken und dem Seed-Cookie.
6. Wenn ein Benutzer eine nachfolgende Anforderung über die TLS-Verbindung sendet, umgeht die Appliance die morphierte Cookie-Validierung. Dies liegt daran, dass die TLS-Verbindung bereits validiert ist.

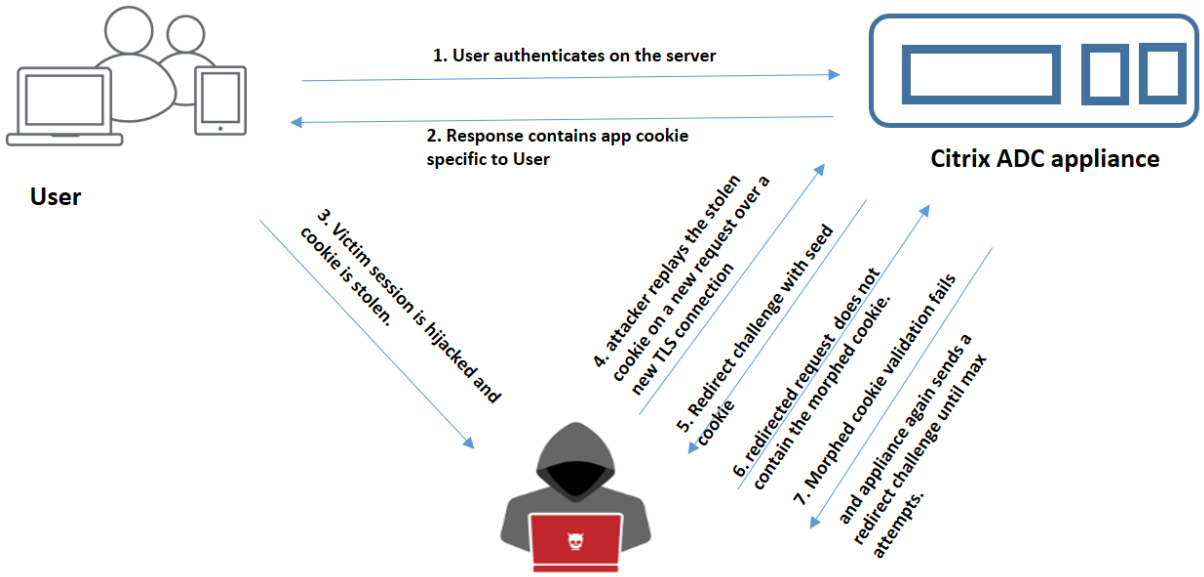
Szenario 2: Benutzer, der über neue TLS-Verbindung mit Session-Cookie auf aufeinanderfolgende Webseiten zugreift



1. Wenn ein Benutzer eine HTTP-Anforderung für aufeinanderfolgende Seiten über eine neue TLS-Verbindung sendet, sendet der Browser die Session-Cookie-ID und die morphierte Cookie-ID.
2. Da es sich um eine neue TLS-Verbindung handelt, erkennt die Appliance die TLS-Verbindung und fordert den Client mit einer Redirect-Antwort mit Seed-Cookie heraus.
3. Der Client berechnet nach Erhalt der Antwort vom ADC das morphierte Cookie mit dem Token der Sitzung und dem neuen Seed-Cookie.
4. Der Client sendet dann dieses neu berechnete morphed Cookie zusammen mit einer Session-ID.
5. Wenn das morphierte Cookie, das innerhalb der ADC-Appliance berechnet wird und das über die Anforderung gesendete Cookie übereinstimmt, wird die TLS-Verbindung als verifiziert markiert.

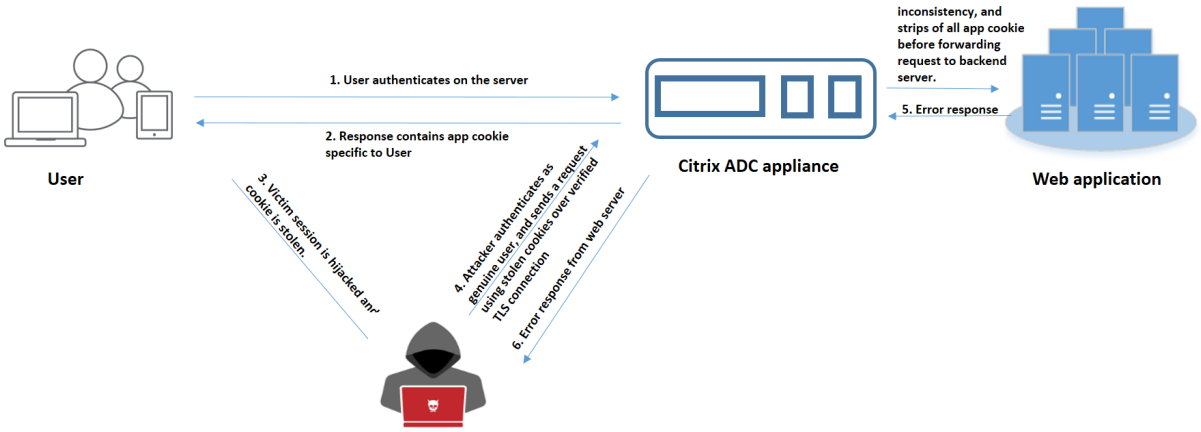
6. Wenn sich das berechnete morphierte Cookie von dem in der Clientanforderung vorhandenen Cookie unterscheidet, schlägt die Validierung fehl. Danach sendet die Appliance die Herausforderung an den Client zurück, um ein ordnungsgemäßes morphes Cookie zu senden.

Szenario 3: Angreifer, die sich als nicht authentifizierter Benutzer ausgeben



1. Wenn sich ein Benutzer bei der Webanwendung authentifiziert, verwendet der Angreifer verschiedene Techniken, um die Cookies zu stehlen und sie wiederzugeben.
2. Da es sich um eine neue TLS-Verbindung des Angreifers handelt, sendet der ADC eine Umleitungsherausforderung zusammen mit einem neuen Seed-Cookie.
3. Da der Angreifer kein JavaScript ausgeführt hat, enthält die Antwort des Angreifers für die umgeleitete Anfrage nicht das morphierte Cookie.
4. Dies führt zu einem morphierten Cookie-Validierungsfehler auf der ADC-Appliance-Seite. Die Appliance sendet erneut eine Umleitungsabfrage an den Client.
5. Wenn die Anzahl der morphierten Cookie-Validierungsversuche den Schwellenwert überschreitet, kennzeichnet die Appliance den Status als Cookie-Hijacking.
6. Wenn der Angreifer versucht, Anwendungscookies und Sitzungscookies zu mischen, die vom Opfer gestohlen wurden, schlägt die Cookie-Konsistenzprüfung fehl, und die Appliance wendet die konfigurierte Cookie-Hijack-Aktion an.

Szenario 4: Angreifer, die sich als authentifizierter Benutzer ausgeben



1. Angreifer können auch versuchen, sich bei einer Webanwendung als echter Benutzer zu authentifizieren und die Cookies des Opfers wiederzugeben, um Zugriff auf die Web-Sitzung zu erhalten.
2. Die ADC-Appliance erkennt auch solche verkörperten Angreifer. Obwohl eine verifizierte TLS-Verbindung vom Angreifer verwendet wird, um das Cookie eines Opfers wiederzugeben, überprüft die ADC-Appliance dennoch, ob das Sitzungscookie und das Anwendungscookie in der Anforderung konsistent sind. Die Appliance überprüft die Konsistenz eines Anwendungs-Cookie mithilfe des Sitzungscookie in der Anforderung. Da die Anforderung das Sitzungscookie eines Angreifers und das App-Cookie eines Opfers enthält, schlägt die Validierung der Cookie Konsistenz fehl.
3. Infolgedessen wendet die Appliance die konfigurierte Cookie-Hijack-Aktion an. Wenn die konfigurierte Aktion als “blockieren” festgelegt ist, entfernt die Appliance alle Anwendungscookies und sendet die Anfrage an den Back-End-Server.
4. Der Back-End-Server empfängt eine Anfrage ohne Anwendungscookie und reagiert daher auf eine Fehlerantwort an den Angreifer, z. B. “Benutzer nicht angemeldet”.

Konfigurieren von Cookie-Hijacking mit der CLI

Sie können ein bestimmtes Anwendungs-Firewall-Profil auswählen und eine oder mehrere Aktionen festlegen, die Cookie-Hijacking verhindern.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set appfw profile <name> [-cookieHijackingAction <action-name> <block | log
 | stats | none>]
```

> **Hinweis:**
>
> Standardmäßig ist die Aktion auf “none” gesetzt.

Beispiel:

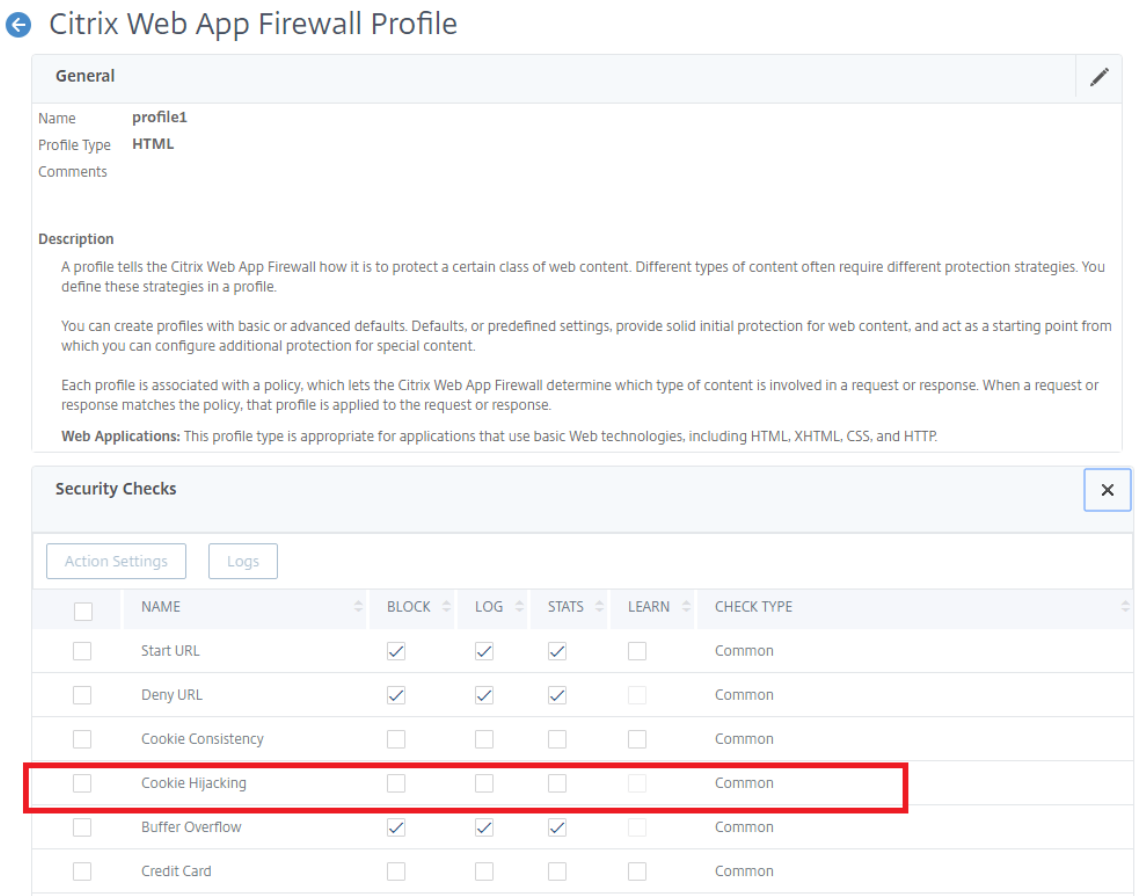

```
set appfw profile profile1 - cookieHijackingAction Block
```

Wo sind Aktionstypen:

Blockieren: Blockieren Sie Verbindungen, die gegen diese Sicherheitsprüfung verstoßen.
Log: Protokollieren Sie Verstöße gegen diese Sicherheitsprüfung.
Stats: Generieren Sie Statistiken für diese Sicherheitsprüfung.
Keine: Deaktivieren Sie alle Aktionen für diese Sicherheitsprüfung.

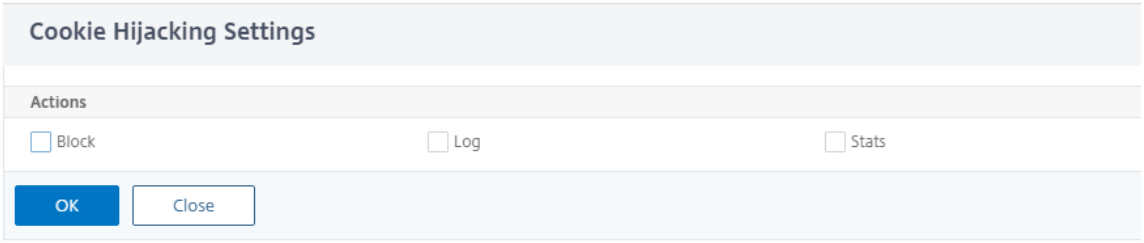
Konfigurieren von Cookie-Hijacking über die Citrix ADC GUI

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profile**.
2. Wählen Sie auf der Seite **Profile** ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Wechseln Sie auf der Seite **Citrix Web App Firewall Profil** zum Abschnitt **Erweiterte Einstellungen** und klicken Sie auf **Sicherheitsprüfungen**.



4. Wählen Sie im Abschnitt **Sicherheitsüberprüfungen** die Option **Cookie-Hijacking** aus, und klicken Sie dann auf **Aktionseinstellungen**.

5. Wählen Sie auf der Seite **Cookie-Hijacking Einstellungen** eine oder mehrere Aktionen aus, um Cookie-Hijacking zu verhindern.
6. Klicken Sie auf **OK**.



Hinzufügen einer Relaxationsregel für die Cookie-Konsistenzvalidierung über die Citrix ADC GUI

Um False Positives bei der Validierung der Cookie-Konsistenz zu behandeln, können Sie eine Relaxationsregel für Cookies hinzufügen, die von der Cookie-Validierung ausgenommen werden können.

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profile**.
2. Wählen Sie auf der Seite **Profile** ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Wechseln Sie auf der Seite **Citrix Web App Firewall Profil** zum Abschnitt **Erweiterte Einstellungen** und klicken Sie auf **Relaxationsregeln**.
4. Wählen Sie im Abschnitt **Relaxationsregeln** die Option **Cookie-Konsistenz** aus, und klicken Sie auf **Aktion**.
5. Legen Sie auf der Seite **Cookie Consistency Relax-Regel** die folgenden Parameter fest.
   a) Aktiviert. Wählen Sie diese Option aus, wenn Sie die Entspannungsregel aktivieren möchten.
   b) Ist Cookie-Name Regex. Wählen Sie aus, ob der Cookie-Name ein regulärer Ausdruck ist.
   c) Cookie-Name. Geben Sie den Namen des Cookies ein, das von der Cookie-Validierung ausgenommen werden kann.
   d) Regex-Editor. Klicken Sie auf diese Option, um die Details des regulären Ausdrucks anzugeben.
   e) Kommentare. Eine kurze Beschreibung über den Cookie.
6. Klicken Sie auf **Erstellen** und **Schließen**.

Anzeigen von Cookie-Hijacking Traffic und Verstöße Statistiken mit der CLI

Zeigen Sie Sicherheitsdatenverkehr und Sicherheitsverletzungen in einem tabellarischen oder grafischen Format an.

So zeigen Sie Sicherheitsstatistiken an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat appfw profile profile1
```

Appfw-Profil Traffic Statistics	Rate (/s)	Gesamt
Anforderungen	0	0
Bytes anfordern	0	0
Antworten	0	0
Antwort-Bytes	0	0
Bricht ab	0	0
Weiterleitungen	0	0
Langzeit-Antwortzeit (ms)	–	0
Letzte Ave Reaktionszeit (ms)	–	0

HTML/XML/JSON-Verstoßstatistik	Rate (/s)	Gesamt
Start-URL	0	0
URL verweigern	0	0
Referer-Kopfzeile	0	0
Pufferüberlauf	0	0
Cookie-Konsistenz	0	0
Cookie-Hijacking	0	0
CSRF-Formular-Tag	0	0
HTML-Site-übergreifendes Skripting	0	0
HTML-SQL-Injection	0	0
Feld-Format	0	0
Feldkonsistenz	0	0
Kreditkarte	0	0
Sicheres Objekt	0	0
Verletzungen der Signatur	0	0

HTML/XML/JSON-Verstoßstatistik	Rate (/s)	Gesamt
Inhaltstyp	0	0
JSON Denial of Service	0	0
JSON SQL-Injection	0	0
JSON Cross-Site Scripting	0	0
Datei-Upload-Typen	0	0
XML-Payload des Inhaltstyps ableiten	0	0
HTML-CMD-Einschleusung	0	0
XML-Format	0	0
XML-Denial-of-Service (XDoS)	0	0
XML-Nachrichtenüberprüfung	0	0
Interoperabilität von Webdiensten	0	0
XML SQL Injection	0	0
XML-Site-übergreifendes Skripting	0	0
XML-Anhang	0	0
SOAP-Fehlerverletzungen	0	0
Allgemeine XML-Verstöße	0	0
Verstöße insgesamt	0	0

HTML/XML/JSON-Protokollstatistik	Rate (/s)	Gesamt
URL-Protokolle starten	0	0
URL-Protokolle verweigern	0	0
Referer-Header-Protokolle	0	0
Pufferüberlaufprotokolle	0	0
Pufferüberlaufprotokolle	0	0
Cookie-Konsistenzprotokolle	0	0

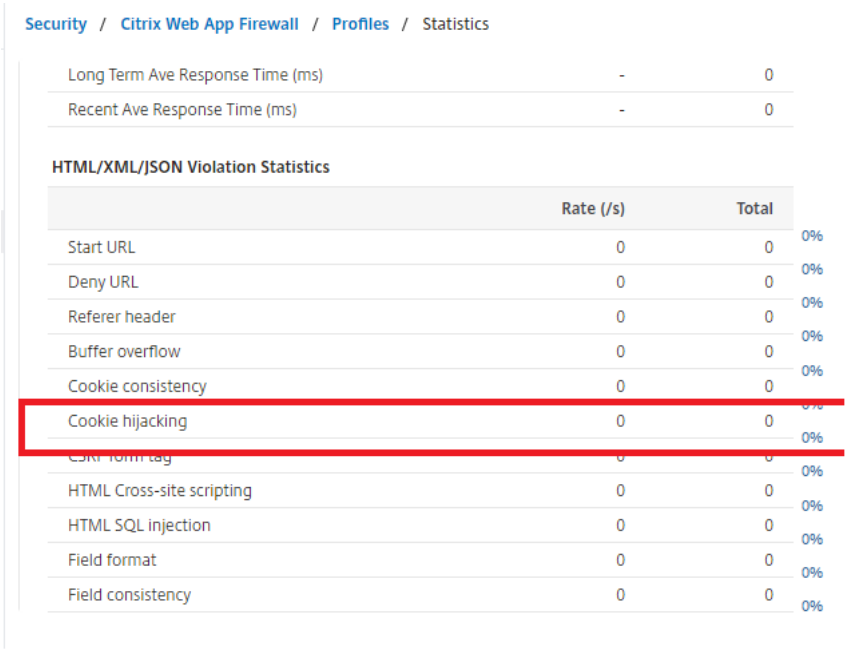
HTML/XML/JSON-Protokollstatistik	Rate (/s)	Gesamt
Cookie-Hijacking Protokolle	0	0
CSRF-Formular-Tag-Protokolle	0	0
HTML-Cross-Site Scripting Protokolle	0	0
HTML-Cross-Site Scripting Transformationsprotokolle	0	0
HTML SQL Injection-Protokolle	0	0
HTML-SQL-Transformationsprotokolle	0	0
Feldformatprotokolle	0	0
Konsistenzprotokolle für Felder	0	0
Kreditkarten	0	0
Transformationsprotokolle für Kreditkarten	0	0
Sichere Objektprotokolle	0	0
Signatur-Protokolle	0	0
Inhaltstyp-Protokolle	0	0
JSON Denial-of-Service-Protokolle	0	0
JSON-SQL-Injectionsprotokolle	0	0
JSON-Site-Cross-Site-Skripting-Protokolle	0	0
Datei-Upload-Typen Protokolle	0	0
Ableiten des Inhaltstyps XML Payload L	0	0
HTML Command Injection Protokolle	0	0

HTML/XML/JSON-Protokollstatistik	Rate (/s)	Gesamt
Protokolle im XML-Format	0	0
XML Denial-of-Service-Protokolle (XDoS)	0	0
XML-Nachrichtenüberprüfungsprotokolle	0	0
WSI-Protokolle	0	0
XML SQL Injection-Protokolle	0	0
Site-übergreifendes XML-Scripting	0	0
XML-Anhangs-Protokolle	0	0
SOAP-Fehlerprotokolle	0	0
Generische XML-Protokolle	0	0
Log-Meldungen insgesamt	0	0

Statistiken zur Serverfehlerantwort	Rate (/s)	Gesamt
HTTP-Client-Fehler (4xx Resp)	0	0
HTTP-Serverfehler (5xx)	0	0

Anzeigen von Cookie-Hijacking Traffic und Verstöße Statistiken mit der GUI

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich ein **Web App Firewall-Profil** aus und klicken Sie auf **Statistiken**.
3. Auf der Seite **Statistiken der Citrix Web App Firewall** werden die Details zum Cookie-Hijacking und zu Verstößen angezeigt.
4. Sie können **Tabellarische Ansicht** auswählen oder zu **Graphische Ansicht** wechseln, um die Daten in einem tabellarischen oder grafischen Format anzuzeigen.



SameSite-Cookie-At

October 5, 2021

Für eine sichere Webkommunikation hat Google die Verwendung des `SameSite` Cookie-Attributs vorgeschrieben. Durch die Einhaltung der neuen `SameSite` Richtlinie von Google Chrome kann die Citrix ADC Appliance Cookies von Drittanbietern mit dem im `set-cookie` Header festgelegten `SameSite` Attribut verwalten. Die Cookie-Einstellung mindert Angriffe und bietet eine gesicherte Webkommunikation.

Bis Februar 2020 wurde das `SameSite` Attribut nicht explizit im Cookie festgelegt. Der Browser hat den Standardwert als “Keine” verwendet. Bei bestimmten Browser-Upgrades wie Google Chrome 80 ändert sich jedoch das standardmäßige domänenübergreifende Verhalten von Cookies.

Festlegen des Cookie-At

Das `SameSite` Attribut ist auf einen der folgenden Werte festgelegt und für den Google Chrome-Browser ist der Standardwert auf “Lax” festgelegt.

Keine. Weist darauf hin, dass der Browser den Cookie nur bei sicheren Verbindungen für Anfragen im standortübergreifenden Kontext verwendet.

Lax. Gibt den Browser an, der das Cookie für Anfragen im Kontext derselben Site verwendet. Im Cross-Site-Kontext können nur sichere HTTP-Methoden wie GET-Request das Cookie verwenden.

Streng. Verwenden Sie das Cookie nur, wenn der Benutzer explizit nach der Domain fragt.

> **Hinweis:**
>
> Wenn Set-Cookies (einschließlich Firewall-Sitzungscookies) über das `SameSite` Attribut verfügen und das `addcookiesamesite` Attribut-Flag im Web Application Firewall-Profil aktiviert ist, wird das `SameSite` Attribut entsprechend dem im Profil konfigurierten Wert überschrieben.

Konfigurieren Sie das SameSite -Attribut im Web App Firewall -Profil mit der CLI

Um das `SameSite` Attribut zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Aktivieren Sie das `SameSite` Cookie Attribut.
2. Setzt das Cookie-Attribut für die appfw-Sitzungscookies.

Aktivieren Sie das Cookie-Attribut “Samesit”

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set appfw profile <profile-name> -insertCookieSameSiteAttribute ( ON | OFF)
```

Beispiel:

```
set appfw profile p1 -insertCookieSameSiteAttribute ON
```

Setzen Sie denselben Site-Cookie-Attributwert für Website-Firewall-S

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set appfw profile <profile-name> - cookieSameSiteAttribute ( LAX | NONE |
STRICT )
```

Beispiel:

```
set appfw profile p1 - cookieSameSiteAttribute LAX
```

Wo sind Attributtypen,

Keine. Das Cookie-Attribut SameSite ist auf “none” gesetzt und für alle WAF- und Anwendungs-Cookies als sicher gekennzeichnet.

Lax. Das Cookie-Attribut SameSite ist für alle WAF- und Anwendungs-Cookies auf “Lax” gesetzt.

Streng. Das Cookie-Attribut SameSite ist für alle WAF- und Anwendungs-Cookies auf “Lax” gesetzt.

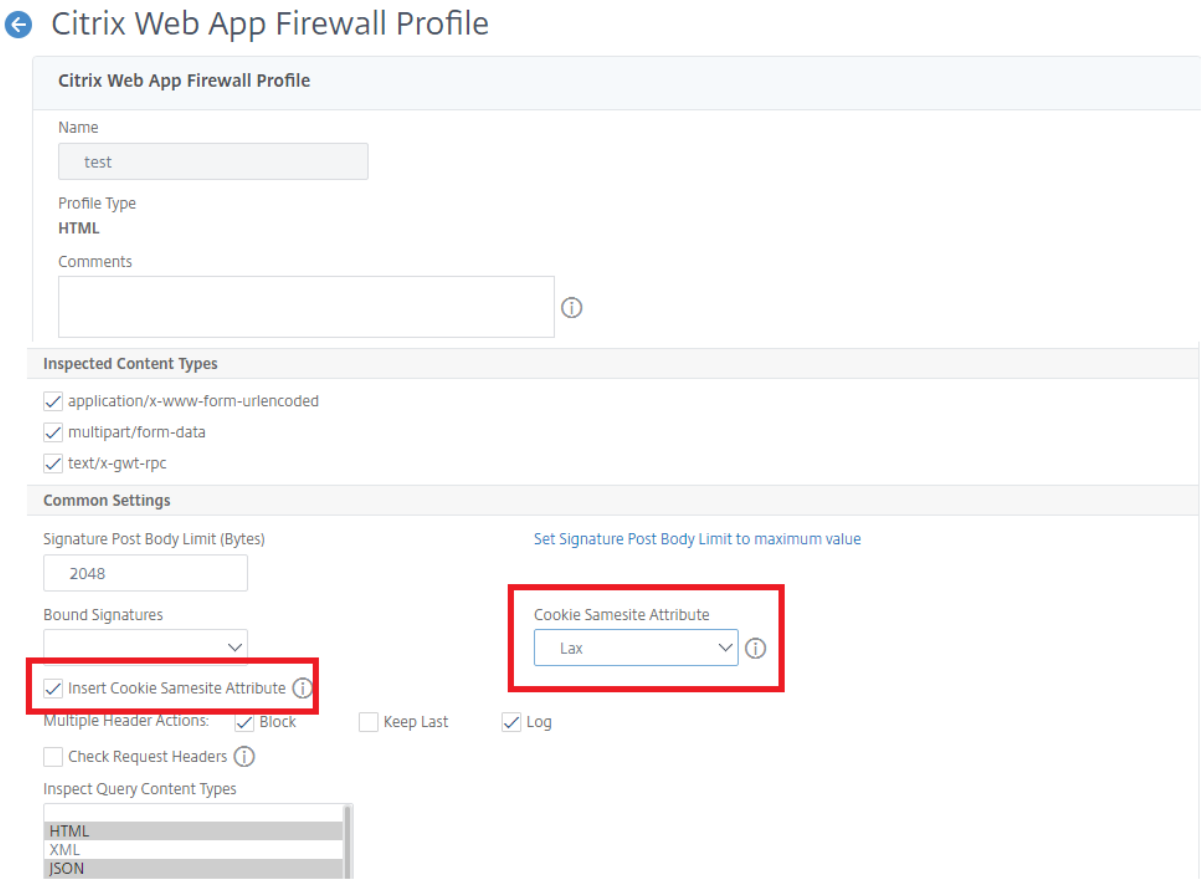
Konfigurieren Sie das SameSite-Cookie-Attribut im Web App Firewall -Profil mit der GUI

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Citrix Web App Firewall Profil**unter **Erweiterte Einstellungen**auf **Profileinstellungen**.
4. Legen Sie im Abschnitt **Profileinstellungen** die folgenden Parameter fest:

   a. Fügen Sie das `Samesite` Cookie-Attribut ein Aktivieren Sie das Kontrollkästchen, um das `Samesite` Cookie-Attribut zu aktivieren.

   b. Cookie Samesite-Attribut. Wählen Sie eine Option aus der Dropdownliste aus, um den `Samesite` Cookie-Wert festzulegen.

5. Klicken Sie auf **OK** und **Fertig**.



Überprüfungen zur Vermeidung von Datenlecks

October 5, 2021

Die Datenleak-Prevention prüft Filterantworten, um ein Versenden vertraulicher Informationen wie Kreditkartennummern und Sozialversicherungsnummern an nicht autorisierte Empfänger zu verhindern.

Kreditkarten-Scheck

October 5, 2021

Wenn Sie über eine Anwendung verfügen, die Kreditkarten akzeptiert oder Ihre Websites Zugriff auf Datenbankserver haben, auf denen Kreditkartennummern gespeichert sind, müssen Sie DLP-Maßnahmen (Data Leak Prevention) verwenden und den Schutz für jeden Kreditkartentyp konfigurieren, den Sie akzeptieren.

Die Citrix Web App Firewall Credit Card-Prüfung verhindert, dass Angreifer Datenleck Prevention-Fehler ausnutzen, um Kreditkartennummern Ihrer Kunden zu erhalten. Durch einfache Konfigurationsschritte können Sie den Schutz einer oder mehrerer der folgenden Kreditkarten erzwingen: 1) Visa, 2) Master Card, 3) Discover, 4) American Express (Amex), 5) JCB und 6) Diners Club.

Die Kreditkarten-Sicherheitsprüfung untersucht Serverantworten, um Instanzen der Zielkreditkartennummern zu identifizieren, und wendet eine bestimmte Aktion an, wenn eine solche Nummer gefunden wird. Die Aktion kann darin bestehen, die Antwort zu transformieren, indem alle Ziffern außer der letzten Gruppe in der Kreditkartennummer herausgenommen werden, oder die Antwort zu blockieren, wenn sie mehr als eine bestimmte Anzahl von Kreditkartennummern enthält. Wenn Sie beide angeben, hat die Blockaktion Vorrang. Die Einstellung Maximal zulässige Kreditkarten pro Seite legt fest, wann die Sperraktion aufgerufen wird. Die Standardeinstellung 0 (auf der Seite sind keine Kreditkartennummern zulässig) ist die sicherste, aber Sie können bis zu 255 zulassen. Je nachdem, wo die Verletzung in der Antwort erkannt wird und die Sperraktion ausgelöst wird, wird möglicherweise weniger als die maximal zulässige Anzahl an Kreditkarten in der Antwort angezeigt.

Um Fehlalarme zu vermeiden, können Sie Entspannungen anwenden, um bestimmte Nummern vom Kreditkartenscheck zu befreien. Beispielsweise könnte eine Sozialversicherungsnummer, eine Bestellnummer oder eine Google-Kontonummer mit einer Kreditkartennummer vergleichbar sein. Sie können einzelne Zahlen angeben oder einen regulären Ausdruck verwenden, um die Zeichenfolge anzugeben, die bei der Verarbeitung der Antwort-URL für die Kreditkartenprüfung umgangen werden soll.

Wenn Sie nicht sicher sind, welche Kreditkartennummern Sie befreien möchten, können Sie mit

der Lernfunktion Empfehlungen basierend auf den erlernten Daten generieren. Um den optimalen Nutzen zu erzielen, ohne die Leistung zu beeinträchtigen, sollten Sie diese Option für kurze Zeit aktivieren, um ein repräsentatives Beispiel der Regeln zu erhalten, und dann die Entspannungen bereitzustellen und das Lernen zu deaktivieren.

Wenn Sie die Protokollfunktion aktivieren, generiert die Kreditkartenprüfung Protokollmeldungen, die die durchgeführten Aktionen angeben. Sie können die Protokolle überwachen, um festzustellen, ob Antworten auf legitime Anfragen blockiert werden. Eine starke Zunahme der Anzahl von Protokollmeldungen kann auf vereitelte Zugriffsversuche hinweisen. Standardmäßig ist der Parameter doSecureCreditCardLogging auf ON, so dass die Kreditkartennummer nicht in der Protokollnachricht enthalten ist, die durch den Verstoß gegen den sicheren Handel (Kreditkarte) generiert wurde.

Die Statistikfunktion sammelt Statistiken über Verstöße und Protokolle. Ein unerwarteter Anstieg im Statistikzähler deutet möglicherweise darauf hin, dass Ihre Anwendung angegriffen wird.

Um die Kreditkarten-Sicherheitsprüfung für den Schutz Ihrer Anwendung zu konfigurieren, konfigurieren Sie das Profil, das die Überprüfung des Datenverkehrs zu und von dieser Anwendung regelt.

> **Hinweis**:
>
> Eine Website, die nicht auf eine SQL-Datenbank zugreift, hat in der Regel keinen Zugriff auf vertrauliche private Informationen wie Kreditkartennummern.

Verwenden der Befehlszeile zum Konfigurieren der Kreditkartenprüfung

In der Befehlszeilenschnittstelle können Sie entweder den Befehl set appfw profile oder den Befehl add appfw profile verwenden, um die Kreditkartenprüfung zu aktivieren und festzulegen, welche Aktionen ausgeführt werden sollen. Sie können den Befehl unset appfw profile verwenden, um auf die Standardeinstellungen zurückzusetzen. Verwenden Sie zum Festlegen von Relaxationen den Befehl bind appfw, um Kreditkartennummern an das Profil zu binden.

So konfigurieren Sie eine Kreditkartenprüfung mit der Befehlszeile

Verwenden Sie entweder den Befehl set appfw profile oder den Befehl add appfw profile wie folgt:

- `set appfw profile <name> -creditCardAction ( ([block][learn] [log][ stats])| [none])`
- `set appfw profile <name> -creditCard (VISA | MASTERCARD | DISCOVER | AMEX | JCB | DINERSCLUB)`
- `set appfw profile <name> -creditCardMaxAllowed <integer>`
- `set appfw profile <name> -creditCardXOut ([ON] | [OFF])<name> -doSecureCreditCard ([ON] | [OFF])`
- So konfigurieren Sie eine Kreditkartenentspannungsregel mit der Befehlszeile

Verwenden Sie den Befehl bind, um die Kreditkartennummer an das Profil zu binden. Um eine Kreditkartennummer aus einem Profil zu entfernen, verwenden Sie den Befehl unbind mit den gleichen Argumenten, die Sie für den Befehl bind verwendet haben. Mit dem Befehl show können Sie die Kreditkartennummern anzeigen, die an ein Profil gebunden sind.

- So binden Sie eine Kreditkartennummer ein Profil

  ```
  bind appfw profile <profile-name> -creditCardNumber <any number/regex>
  “<url>”
  ```

  Beispiel: bind appfw profile test_profile -creditCardNumber 378282246310005 http://www.example.com/credit_card_test.html

  - So heben Sie die Bindung einer Kreditkartennummer von einem Profil auf

    ```
    unbind appfw profile <profile-name> -creditCardNumber <credit card
    number / regex> <url>
    ```

  - Um die Liste der Kreditkartennummern anzuzeigen, die an ein Profil gebunden sind.

    ```
    show appfw profile <profile>
    ```

Verwenden der GUI zum Konfigurieren der Kreditkartenüberprüfung

In der GUI konfigurieren Sie die Kreditkartensicherheitsprüfung im Bereich für das Profil, das Ihrer Anwendung zugeordnet ist.

So fügen Sie die Kreditkarten-Sicherheitsprüfung mit der GUI hinzu oder ändern

1. Navigieren Sie zu **Web App Firewall** > **Profile, markieren** Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Sicherheitsprüfungen**.

   In der Tabelle Sicherheitsprüfung werden die aktuell konfigurierten Aktionseinstellungen für alle Sicherheitsprüfungen angezeigt. Sie haben 2 Optionen für die Konfiguration:

   a) Wenn Sie nur Sperren, Protokollieren, Statistiken und Lernaktionen für Kreditkarte aktivieren oder deaktivieren möchten, können Sie die Kontrollkästchen in der Tabelle aktivieren oder deaktivieren, klicken Sie auf **OK**, und klicken Sie dann auf **Speichern**und **Schließen**, um den Bereich **Sicherheitsprüfung**zu schließen.

   b) Wenn Sie zusätzliche Optionen für diese Sicherheitsprüfung konfigurieren möchten, doppelklicken Sie auf Kreditkarte, oder wählen Sie die Zeile aus und klicken Sie auf **Aktionseinstellungen**, um weitere Optionen wie folgt anzuzeigen:

      - Ausgang — Maskieren Sie jede in einer Antwort erkannte Kreditkartennummer, indem Sie jede Ziffer mit Ausnahme der Ziffern in der endgültigen Gruppe durch den Buchstaben X.

- Maximal zulässige Kreditkarten pro Seite — Geben Sie die Anzahl der Kreditkarten an, die an den Client weitergeleitet werden können, ohne eine Sperraktion auszulösen.
- Geschützte Kreditkarten. Aktivieren oder deaktivieren Sie ein Kontrollkästchen, um den Schutz für jeden Kreditkartentyp zu aktivieren oder zu deaktivieren.
- Sie können auch die Aktionen Sperren, Protokollieren, Statistiken und Lernen im Bereich Kreditkarteneinstellungen bearbeiten.
  Nachdem Sie eine der oben genannten Änderungen vorgenommen haben, klicken Sie auf OK, um die Änderungen zu speichern und zur Tabelle Sicherheitsprüfungen zurückzukehren. Sie können bei Bedarf weitere Sicherheitsprüfungen konfigurieren. Klicken Sie auf OK, um alle Änderungen zu speichern, die Sie im Abschnitt Sicherheitsprüfungen vorgenommen haben, und klicken Sie dann auf Speichern und Schließen, um den Bereich Sicherheitsprüfung zu schließen.

3. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Profileinstellungen** . Aktivieren oder deaktivieren Sie das Kontrollkästchen Sichere Kreditkartenprotokollierung, um die **sichere Protokollierung von Kreditkartennummern** zu aktivieren oder zu deaktivieren. (Standardmäßig ist es ausgewählt).

   Klicken Sie auf **OK**, um die Änderungen zu speichern.

- So konfigurieren Sie eine Kreditkartenentspannungsregel mit der GUI

  1. Navigieren Sie zu **Web App Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
  2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Relaxationsregeln**. Die Tabelle Relaxationsregeln enthält einen Kreditkarteneintrag. Sie können doppelklicken oder diese Zeile auswählen und auf **Bearbeiten** klicken, um den Dialog **Kreditkartenentspannungsregeln** aufzurufen. Sie können Vorgänge zum Hinzufügen, Bearbeiten, Löschen, Aktivierenoder Deaktivieren für Relaxationsregeln ausführen.

Verwenden der Learn-Funktion mit dem Kreditkartencheck

Wenn die Lernaktion aktiviert ist, überwacht die Web App Firewall Learning Engine den Datenverkehr und lernt die ausgelösten Verletzungen. Sie können diese gelernten Regeln regelmäßig überprüfen. Wenn Sie nach gebührender Überlegung eine bestimmte Zeichenfolge von der Kreditkarten-Sicherheitsprüfung ausnehmen möchten, können Sie die Gelernte Regel als Relaxationsregel bereitstellen.

- So zeigen Sie gelernte Daten mit der Befehlszeilenschnittstelle an oder verwenden

  ```
  show appfw learningdata <profilename> creditCardNumber
  ```

  ```
  rm appfw learningdata <profilename> -creditcardNumber <credit card
  number> "<url>"
  ```



```
export appfw learningdata <profilename> creditCardNumber
```

- So zeigen Sie gelernte Daten mit der GUI an oder verwenden

  1. Navigieren Sie zu **Web App Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
  2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Gelernte Regeln** . Sie können den Kreditkarteneintrag in der Tabelle Gelernte Regeln auswählen und darauf doppelklicken, um auf die gelernten Regeln zuzugreifen. Sie können die erlernten Regeln bereitstellen oder eine Regel bearbeiten, bevor Sie sie als Relaxationsregel bereitstellen. Um eine Regel zu verwerfen, können Sie sie auswählen und auf die Schaltfläche **Überspringen** klicken. Sie können jeweils nur eine Regel bearbeiten, aber Sie können mehrere Regeln zum Bereitstellen oder Überspringen auswählen.

  Sie haben auch die Möglichkeit, eine zusammengefasste Ansicht der gelernten Entspannungen anzuzeigen, indem Sie in der Tabelle Gelernte Regeln den Eintrag Kreditkarte auswählen und auf Visualizer klicken, um eine konsolidierte Ansicht aller gelernten Verletzungen zu erhalten. Der Visualizer macht es sehr einfach, die erlernten Regeln zu verwalten. Es bietet eine umfassende Ansicht der Daten auf einem Bildschirm und erleichtert das Handeln an einer Gruppe von Regeln mit einem Klick. Der größte Vorteil des Visualizers besteht darin, dass reguläre Ausdrücke zur Konsolidierung mehrerer Regeln empfohlen werden. Sie können eine Teilmenge dieser Regeln basierend auf dem Trennzeichen und der Aktions-URL auswählen. Sie können 25, 50 oder 75 Regeln im Visualizer anzeigen, indem Sie die Nummer aus einer Dropdownliste auswählen. Der Visualizer für erlernte Regeln bietet die Möglichkeit, die Regeln zu bearbeiten und als Relaxation bereitzustellen. Oder Sie können die Regeln überspringen, um sie zu ignorieren.

Verwenden der Log-Funktion mit dem Kreditkartencheck

Wenn die Protokollaktion aktiviert ist, werden die Verletzungen der Kreditkarten-Sicherheitsprüfung im Überwachungsprotokoll als Verstöße APPFW_SAFECOMMERCE oder APPFW_SAFECOMMERCE_XFORM protokolliert. Die Web App Firewall unterstützt sowohl native als auch CEF-Protokollformate. Sie können die Protokolle auch an einen entfernten Syslog-Server senden.

Die Standardeinstellung für doSecureCreditCardLogging ist ON. Wenn Sie es in OFF ändern, werden sowohl Kreditkartennummer als auch Typ in der Protokollnachricht enthalten.

Abhängig von den Einstellungen, die für die Kreditkartenüberprüfungen konfiguriert wurden, können die vom Anwendungs-Firewall generierten Protokollmeldungen folgende Informationen enthalten:

- Antwort wurde blockiert oder nicht blockiert.
- Kreditkartennummern wurden transformiert (X'd out). Für jede transformierte Kreditkartennummer wird eine separate Protokollnachricht generiert, so dass während der Verarbeitung einer einzelnen Antwort mehrere Protokollnachrichten generiert werden können.

- Die Antwort enthielt die maximale Anzahl potenzieller Kreditkartennummern.
- Kreditkartennummern und ihre entsprechenden Typen.
- So greifen Sie mit der Befehlszeile auf die Protokollmeldungen zu

  Wechseln Sie zur Shell und senden Sie die ns.logs im Ordner /var/log/, um auf die Protokollmeldungen zu den Kreditkartenverstößen zuzugreifen:

  - Shell
  - tail -f /var/log/ns.log | grep SAFECOMMERCE
- So greifen Sie mit der GUI auf die Protokollmeldungen zu

  1. Die Citrix GUI enthält ein sehr nützliches Tool (Syslog Viewer) zur Analyse der Protokollmeldungen. Sie haben einige Optionen für den Zugriff auf den Syslog Viewer: Navigieren Sie zum **Zielprofil** > **Sicherheitsprüfungen** . Markieren Sie die Zeile Kreditkarte, und klicken Sie auf Protokolle. Wenn Sie direkt über die Kreditkarten-Sicherheitsprüfung des Profils auf die Protokolle zugreifen, filtert es die Protokollmeldungen aus und zeigt nur die Protokolle an, die sich auf diese Sicherheitsüberprüfungsverstöße beziehen.
  2. Sie können auch auf den Syslog Viewer zugreifen, indem Sie zu **NetScaler** > **System** > **Auditing navigieren** . Klicken Sie im Abschnitt Audit-Meldungen auf den Link **Syslog-Nachrichten**, um den Syslog-Viewer anzuzeigen, der alle Protokollmeldungen einschließlich anderer Protokolle für Sicherheitsüberprüfungen anzeigt. Dies ist nützlich für das Debuggen, wenn während der Anforderungsverarbeitung mehrere Sicherheitsüberprüfungsverletzungen ausgelöst werden können.

     Der HTML-basierte Syslog Viewer bietet verschiedene Filteroptionen, um nur die Protokollmeldungen auszuwählen, die für Sie von Interesse sind. Um auf die Protokollmeldungen der Kreditkarten-Sicherheitsüberprüfung zuzugreifen, filtern Sie, indem Sie APPFW in den Dropdown-Optionen für Modul auswählen. Der Ereignistyp zeigt eine Reihe von Optionen an, um Ihre Auswahl weiter zu verfeinern. Wenn Sie beispielsweise die Kontrollkästchen APPFW_SAFECOMMERCE und APPFW_SAFECOMMERCE_XFORM aktivieren und auf die Schaltfläche Übernehmen klicken, werden im Syslog-Viewer nur Protokollmeldungen angezeigt, die sich auf die Verstöße der Kreditkarten-Sicherheitsprüfung beziehen.

     Wenn Sie den Cursor in der Zeile für eine bestimmte Protokollmeldung platzieren, werden unter der Protokollmeldung mehrere Optionen wie Module und EventType angezeigt. Sie können eine dieser Optionen auswählen, um die entsprechenden Informationen in den Protokollen hervorzuheben.

Beispiel für eine Protokollmeldung im nativen Format, wenn die Antwort nicht blockiert ist


```
May 29 01:26:31 <local0.info> 10.217.31.98 05/29/2015:01:26:31 GMT ns
    0-PPE-0 :
default APPFW APPFW_SAFECOMMERCE 2181 0 :  10.217.253.62 1098-PPE0
4erNfkaHy0IeGP+nv2S9Rsdu77I0000 pr_ffc http://aaron.stratum8.net/FFC/
    CreditCardMind.html
Maximum number of potential credit card numbers seen <not blocked>
<!--NeedCopy-->
```

Beispiel für eine Protokollmeldung im CEF-Format, wenn die Antwort transformiert wird

```
May 28 23:42:48 <local0.info> 10.217.31.98
CEF:0|Citrix|NetScaler|NS11.0|APPFW|APPFW_SAFECOMMERCE_XFORM|6|src
    =10.217.253.62
spt=25314 method=GET request=http://aaron.stratum8.net/FFC/
    CreditCardMind.html
msg=Transformed (xout) potential credit card numbers seen in server
    response
cn1=66 cn2=1095 cs1=pr_ffc cs2=PPE2 cs3=xzE7M0g9bovAtG/zLCrLd2zkVl80002
cs4=ALERT cs5=2015 act=transformed
<!--NeedCopy-->
```

Beispiel für eine Protokollmeldung im CEF-Format, wenn die Antwort blockiert wird. Die Kreditkartennummer und der Typ sind im Protokoll zu sehen, da der Parameter doSecureCreditCardLogging deaktiviert ist.

```
May 28 23:42:48 <local0.info> 10.217.31.98
CEF:0|Citrix|NetScaler|NS11.0|APPFW|APPFW_SAFECOMMERCE|6|src
    =10.217.253.62
spt=25314 method=GET request=http://aaron.stratum8.net/FFC/
    CreditCardMind.html
msg=Credit Card number 4505050504030302 of type Visa is seen in
    response cn1=68
cn2=1095 cs1=pr_ffc cs2=PPE2 cs3=xzE7M0g9bovAtG/zLCrLd2zkVl80002 cs4=
    ALERT cs5=2015
act=blocked
<!--NeedCopy-->
```


Statistiken für die Kreditkartenverstöße

Wenn die Aktion Statistik aktiviert ist, wird der entsprechende Zähler für die Kreditkartenprüfung erhöht, wenn die Web App Firewall eine Aktion für diese Sicherheitsprüfung ausführt. Die Statistiken werden für Rate und Gesamtanzahl für Traffic, Verletzungen und Protokolle gesammelt. Die Inkrement des Protokollzählers kann je nach konfigurierten Einstellungen variieren. Wenn beispielsweise die Aktion Sperren aktiviert ist und die Einstellung Maximal zulässige Kreditkarte 0 lautet, erhöht die Anforderung für eine Seite, die 20 Kreditkartennummern enthält, den Statistikzähler um eins, wenn die Seite blockiert wird, sobald die erste Kreditkartennummer erkannt wird. Wenn der Block jedoch deaktiviert ist und Transformation aktiviert ist, erhöht die Verarbeitung derselben Anforderung den Statistikindikator für Protokolle um 20, da jede Kreditkartentransformation eine separate Protokollnachricht generiert.

- So zeigen Sie Kreditkartenstatistiken mit der Befehlszeile an

  Geben Sie an der Eingabeaufforderung Folgendes ein:

  ```
  sh appfw stats
  ```

  Verwenden Sie den folgenden Befehl, um Statistiken für ein bestimmtes Profil anzuzeigen:

  ```
  stat appfw profile <profile name>
  ```

  So zeigen Sie Kreditkartenstatistiken mit der GUI an

  1. Navigieren Sie zu **System** > **Sicherheit** > **Web App Firewall** .
  2. Greifen Sie im rechten Bereich auf den **Statistik-Link** zu.
  3. Verwenden Sie die Bildlaufleiste, um Statistiken über Kreditkartenverstöße und -protokolle anzuzeigen. Die Statistiktabelle enthält Echtzeitdaten und wird alle 7 Sekunden aktualisiert.

Highlights

Beachten Sie die folgenden Punkte zur Kreditkarten-Sicherheitsprüfung:

- Mit der Web App Firewall können Sie Kreditkarteninformationen schützen und versuchen, auf diese sensiblen Daten zuzugreifen.
- Um die Kreditkartenschutzprüfung zu verwenden, müssen Sie mindestens einen Kreditkartentyp und eine Aktion angeben. Die Prüfung wird dann auf HTML-, XML- und Web 2.0-Profile angewendet.
- Sie können die Ausgabe von sh appfw profile Befehl und grep für CreditCard übergeben, um alle Kreditkarten-spezifische Konfiguration zu sehen. Beispielsweise zeigt sh appfw profile my_profile | grep CreditCard die konfigurierten Einstellungen verschiedener Parameter sowie die Relaxationsregeln für die Kreditkartenprüfung für das Web App Firewall Profil my_profile an.

- Sie können bestimmte Nummern von der Kreditkartenprüfung ausschließen, ohne die Sicherheitskontrolle für die restlichen Kreditkartennummern zu umgehen.
- Entspannung steht für alle mit Web App Firewall geschützten Kreditkartenmuster zur Verfügung. In der grafischen Benutzeroberfläche können Sie den Visualisierer verwenden, um Vorgänge zum Hinzufügen, Bearbeiten, Löschen, Aktivieren oder Deaktivieren für Relaxationsregeln anzugeben.
- Die Web App Firewall Lernmodul kann den ausgehenden Datenverkehr überwachen, um Regeln basierend auf beobachteten Verstößen zu empfehlen. Visualizer-Unterstützung ist auch für die Verwaltung der erlernten Kreditkartenregeln in der GUI verfügbar. Sie können die erlernten Regeln bearbeiten und bereitstellen oder sie nach sorgfältiger Prüfung überspringen.
- Die Einstellung für die Anzahl der zulässigen Kreditkarten gilt für jede Antwort. Sie bezieht sich nicht auf die kumulative Summe der Kreditkartennummern, die während der gesamten Benutzersitzung beobachtet wurden.
- Die Anzahl der X'd out Ziffern hängt von der Länge der Kreditkartennummern ab. Zehn Ziffern sind x'd out für Kreditkarten mit 13 bis 15 Ziffern. Zwölf Ziffern sind x'd out für Kreditkarten mit 16 Ziffern. Wenn für Ihre Anwendung nicht die gesamte Kreditkartennummer in der Antwort gesendet werden muss, empfiehlt Citrix, diese Aktion zu aktivieren, um die Ziffern in den Kreditkartennummern zu maskieren.
- Der X-Out-Vorgang transformiert alle Kreditkarten und arbeitet unabhängig von den konfigurierten Einstellungen für die maximale Anzahl zulässiger Kreditkarten. Wenn beispielsweise 4 Kreditkarten in der Antwort enthalten sind und der Parameter CreditCardMaxAllowed auf 10 gesetzt ist, sind alle 4 Kreditkarten X'd-out, aber sie werden nicht blockiert. Wenn die Kreditkartennummern im Dokument verteilt sind, kann eine Teilantwort mit X'd-Out-Nummern an den Kunden gesendet werden, bevor die Antwort blockiert wird.
- Deaktivieren Sie den Parameter doSecureCreditCardLogging nicht vor angemessener Berücksichtigung. Wenn dieser Parameter ausgeschaltet ist, werden die Kreditkartennummern angezeigt und sind in den Protokollmeldungen zugänglich. Diese Zahlen werden in den Protokollen nicht maskiert, selbst wenn die X-out-Aktion aktiviert ist. Wenn Sie Protokolle an einen entfernten Syslog-Server senden und die Protokolle kompromittiert werden, können die Kreditkartennummern offengelegt werden.
- Wenn die Antwortseite wegen einer Kreditkartenverletzung blockiert ist, leitet die Web App Firewall nicht zur Fehlerseite um.

Sichere Objektprüfung

October 5, 2021

Die Prüfung Safe Object bietet benutzerkonfigurierbaren Schutz für sensible Geschäftsinformationen wie Kundennummern, Bestellnummern und länderspezifische oder regionsspezifische Telefonnum-

mern oder Postleitzahlen. Ein benutzerdefinierter regulärer Ausdruck oder ein benutzerdefiniertes Plug-In teilt der Web App Firewall das Format dieser Informationen mit und definiert die Regeln, die zum Schutz verwendet werden sollen. Wenn eine Zeichenfolge in einer Benutzeranforderung mit einer Definition eines sicheren Objekts übereinstimmt, blockiert die Web App Firewall entweder die Antwort, maskiert die geschützten Informationen oder entfernt die geschützten Informationen aus der Antwort, bevor sie an den Benutzer gesendet wird, je nachdem, wie Sie diese bestimmte Regel für sichere Objekte konfiguriert haben.

Die Überprüfung des sicheren Objektes verhindert, dass Angreifer einen Sicherheitsfehler in Ihrer Webserversoftware oder auf Ihrer Website ausnutzen, um vertrauliche private Informationen wie Firmenkreditkartennummern oder Sozialversicherungsnummern zu erhalten. Wenn Ihre Websites keinen Zugriff auf diese Art von Informationen haben, müssen Sie diese Prüfung nicht konfigurieren. Wenn Sie einen Einkaufswagen oder eine andere Anwendung haben, die auf solche Informationen zugreifen kann, oder Ihre Websites Zugriff auf Datenbankserver haben, die solche Informationen enthalten, müssen Sie den Schutz für jede Art von sensiblen privaten Informationen konfigurieren, die Sie verarbeiten und speichern.

> **Hinweis:**
>
> Eine Website, die nicht auf eine SQL-Datenbank zugreift, hat normalerweise keinen Zugriff auf sensible private Informationen.

Das Dialogfeld Sichere Objektprüfung ist anders als bei jeder anderen Prüfung. Jeder von Ihnen erstellte sichere Objektausdruck entspricht einer separaten Sicherheitsprüfung, ähnlich der Kreditkartenprüfung, für diese Art von Informationen. Wenn Sie den Assistenten oder die GUI verwenden, fügen Sie einen neuen Ausdruck hinzu, indem Sie auf Hinzufügen klicken und den Ausdruck im Dialogfeld Sicheres Objekt hinzufügen konfigurieren. Sie ändern einen vorhandenen Ausdruck, indem Sie ihn auswählen, dann auf Öffnen klicken und dann den Ausdruck im Dialogfeld Sicheres Objekt ändern konfigurieren.

Im Dialogfeld Sicheres Objekt für jeden Ausdruck eines sicheren Objekts können Sie Folgendes konfigurieren:

- **Name des sicheren Objekts.** Ein Name für Ihr neues sicheres Objekt. Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrich beginnen und kann aus einem bis 255 Buchstaben, Zahlen und Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen ( ), At-Zeichen (@), Gleich (=), Doppelpunkt (:) und Unterstrich (_) bestehen.
- **Aktionen.** Aktivieren oder deaktivieren Sie die Aktionen Blockieren, Protokollieren und Statistiken sowie die folgenden Aktionen:
  - **X-Out.** Maskieren Sie alle Informationen, die dem sicheren Objektausdruck entsprechen, mit dem Buchstaben “X”.
  - **Remove.** Entfernen Sie alle Informationen, die dem sicheren Objektausdruck entsprechen.

- **Regulärer Ausdruck.** Geben Sie einen PCRE-kompatiblen regulären Ausdruck ein, der das sichere Objekt definiert. Sie können den regulären Ausdruck auf drei Arten erstellen: indem Sie den regulären Ausdruck direkt in das Textfeld eingeben, indem Sie das Menü **Regex-Token** verwenden, um Elemente und Symbole für reguläre Ausdrücke direkt in das Textfeld einzugeben, oder indem Sie den Editor für reguläre Ausdrücke öffnen und ihn für konstruieren den Ausdruck. Der reguläre Ausdruck darf nur aus ASCII-Zeichen bestehen. Ausschneiden und Einfügen von Zeichen, die nicht Teil des grundlegenden ASCII-Sets mit 128 Zeichen sind. Wenn Sie Nicht-ASCII-Zeichen einschließen möchten, müssen Sie diese Zeichen manuell im hexadezimalen PCRE-Zeichenkodierungsformat eingeben.
  Hinweis: Verwenden Sie keine Startanker (^) am Anfang von Ausdrücken des sicheren Objekts oder Endanker ($) am Ende von Ausdrücken des sicheren Objekts. Diese PCRE-Entitäten werden in Ausdrücken des sicheren Objekts nicht unterstützt, und wenn sie verwendet werden, wird der Ausdruck nicht mit dem übereinstimmen, was er beabsichtigt war.
- **Maximale Übereinstimmungslänge.** Geben Sie eine positive Ganzzahl ein, die die maximale Länge der Zeichenfolge darstellt, die Sie übereinstimmen möchten. Wenn Sie beispielsweise US-amerikanische Sozialversicherungsnummern abgleichen möchten, geben Sie in dieses Feld die Zahl elf (11) ein. Dadurch kann Ihr regulärer Ausdruck eine Zeichenfolge mit neun Ziffern und zwei Bindestrichen übereinstimmen. Wenn Sie die Nummern des kalifornischen Führerscheins übereinstimmen möchten, geben Sie die Nummer acht (8) ein.

  > **Achtung:**
  >
  > Wenn Sie in dieses Feld keine maximale Übereinstimmungslänge eingeben, verwendet die Web App Firewall beim Filtern nach Zeichenfolgen, die Ihren sicheren Objektausdrücken entsprechen, den Standardwert eins (1). Daher stimmen die meisten sicheren Objektausdrücke nicht mit ihren Zielzeichenfolgen überein.

Sie können die Befehlszeilenschnittstelle nicht zum Konfigurieren der Prüfung Safe Object verwenden. Sie müssen es mithilfe des Web App Firewall Assistenten oder der GUI konfigurieren.

Im Folgenden finden Sie Beispiele für reguläre Ausdrücke der sicheren Objektprüfung:

- Suchen Sie nach Zeichenfolgen, bei denen es sich um US-amerikanische Sozialversicherungsnummern handelt, die aus drei Ziffern bestehen (die erste darf nicht Null sein), gefolgt von einem Bindestrich, gefolgt von zwei weiteren Ziffern, gefolgt von einem zweiten Bindestrich und endet mit einer Zeichenfolge von vier weiteren Ziffern:

```
[1-9][0-9]{
3,3 }
-[0-9]{
2,2 }
-[0-9]{
```



```
4,4 }

<!--NeedCopy-->
```

- Suchen Sie nach Zeichenfolgen, die scheinbar kalifornische Führerschein-IDs zu sein scheinen, die mit einem Buchstaben beginnen und von einer Zeichenfolge mit genau sieben Ziffern gefolgt sind:

```
[A-Za-z][0-9]{
7,7 }

<!--NeedCopy-->
```

- Suchen Sie nach Zeichenfolgen, bei denen es sich um Kunden-IDs handelt, die aus einer Zeichenfolge von fünf hexadezimalen Zeichen (alle Ziffern und Buchstaben A bis F), gefolgt von einem Bindestrich, gefolgt von einem dreibuchstabigen Code, gefolgt von einem zweiten Bindestrich und endend mit einer Zeichenfolge von zehn Ziffern:

```
[0-9A-Fa-f]{
5,5 }
-[A-Za-z]{
3,3 }
-[0-9]{
10,10 }

<!--NeedCopy-->
```

> **Achtung:**
>
> Reguläre Ausdrücke sind leistungsstark. Insbesondere wenn Sie mit regulären Ausdrücken im PCRE-Format nicht vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben, um sicherzustellen, dass sie genau den Typ der Zeichenfolge definieren, den Sie als sichere Objektdefinition hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung von Platzhaltern und insbesondere der Punkt-Sternchen (.*) -Metazeichen/Platzhalterkombination kann zu Ergebnissen führen, die Sie nicht wollten oder erwarten, z. B. zum Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten.

Erweiterte Formularschutzprüfungen

October 5, 2021

Der erweiterte Formularschutz überprüft Webformulardaten, um zu verhindern, dass Angreifer Ihr System gefährden, indem sie die Webformulare auf Ihren Websites ändern oder unerwartete Arten und Mengen von Daten in einem Formular an Ihre Website senden.

> **Hinweis:**
>
> SQL-, Cross-Site-Scripting-, FFC- und FieldFormat-Schutzprüfungen werden angewendet, wenn die **Option Hochladen von Sicherheitsüberprüfungen ausschließen** nicht festgelegt ist.

Ein Datei-Upload ist auch ein Formularelement, das über das Feld für den **Namen des** Steuerelements verfügt, das als Teil des Formulars gesendet wird.

Weitere Informationen finden Sie auf dieser Seite: Formulare

Feldformat-Prüfung

October 5, 2021

Die Prüfung Feldformate überprüft die Daten, die Benutzer in Webformularen an Ihre Websites senden. Es untersucht sowohl die Länge als auch den Typ der Daten, um sicherzustellen, dass es für das Formularfeld geeignet ist, in dem es angezeigt wird. Wenn die Web App Firewall ungeeignete Webformulardaten in einer Benutzeranforderung erkennt, blockiert sie die Anforderung.

Indem verhindert wird, dass ein Angreifer unangemessene Webformulardaten an Ihre Website sendet, verhindert der Check Field Formats bestimmte Arten von Angriffen auf Ihre Website und Ihre Datenbankserver. Wenn beispielsweise ein bestimmtes Feld erwartet, dass der Benutzer eine Telefonnummer eingibt, untersucht die Prüfung Feldformate die vom Benutzer übermittelte Eingabe, um sicherzustellen, dass die Daten mit dem Format einer Telefonnummer übereinstimmen. Wenn ein bestimmtes Feld einen Vornamen erwartet, stellt die Feldformat-Prüfung sicher, dass die Daten in diesem Feld einen Typ und eine Länge aufweisen, die für einen Vornamen geeignet ist. Es tut dasselbe für jedes Formularfeld, das Sie für den Schutz konfigurieren.

Diese Prüfung gilt nur für HTML-Anfragen. Es gilt nicht für XML-Anforderungen. Sie können Feldformatprüfungen in HTML-Profilen oder Web 2.0-Profilen konfigurieren, um die HTML-Nutzlast zum Schutz Ihrer Anwendungen zu überprüfen. Die Web App Firewall unterstützt auch den Field Format Check Schutz für Google Web Toolkit (GWT) -Anwendungen.

Die Feldformat-Prüfung erfordert, dass Sie eine oder mehrere Aktionen aktivieren. Die Web App Firewall untersucht die übermittelten Eingaben und wendet die angegebenen Aktionen an.

> **Hinweis:**
>
> Feldformatregeln sind Verschärfungsregeln. Das Hinzufügen von ihnen zur Relaxationsliste aus erlernten Daten dient als Blockierungsregel.
>
> Um Feldformatregeln zu entspannen, entfernen Sie bitte bestimmte fieldname aus der Feldformat-Relaxationsliste.

Sie haben die Möglichkeit, die Standardfeldformate so festzulegen, dass Feldtyp und die minimale und maximale Länge der Daten angegeben werden, die in jedem Formularfeld auf jedem Webformular erwartet werden, das Sie schützen möchten. Sie können Relaxationsregeln bereitstellen, um ein Feldformat für ein einzelnes Feld eines bestimmten Formulars zu konfigurieren. Es können mehrere Regeln hinzugefügt werden, um den Feldnamen, die Aktions-URL und die Feldformate anzugeben. Geben Sie Feldformate an, um verschiedene Eingabetypen in verschiedenen Formularfeldern zu akzeptieren. Die Lernfunktion kann Empfehlungen für die Entspannungsregeln geben.

Feldformataktionen — Sie können Aktionen Blockieren, Protokollieren, Statistiken und Lernen aktivieren. Mindestens eine dieser Aktionen muss aktiviert sein, um den Feldformatprüfungsschutz zu aktivieren.

- **Blockieren**. Wenn Sie Block aktivieren, wird die Blockaktion ausgelöst, wenn die Eingabe nicht dem angegebenen Feldformat entspricht. Wenn für das Zielfeld eine Regel konfiguriert wurde, wird die Eingabe anhand der angegebenen Regel überprüft. Andernfalls wird es mit der Standardfeldformatspezifikation überprüft. Jede Nichtübereinstimmung in der Feldtyp- oder min/-max Längenspezifikation führt zu einer Blockierung der Anforderung.
- **Log**. Wenn Sie die Protokollfunktion aktivieren, generiert die Feldformatprüfung Protokollmeldungen, die die ausgeführten Aktionen angeben. Sie können die Protokolle überwachen, um festzustellen, ob Antworten auf legitime Anfragen blockiert werden. Eine große Zunahme der Anzahl von Protokollmeldungen kann auf bösartige Versuche hinweisen, einen Angriff zu starten.
- **Statistiken**. Wenn diese Option aktiviert ist, werden Statistiken über Verstöße und Protokolle gesammelt. Ein unerwarteter Anstieg des Statistikzählers weist möglicherweise darauf hin, dass Ihre Anwendung angegriffen wird, oder Sie müssen die Konfiguration erneut besuchen, um festzustellen, ob das angegebene Feldformat zu restriktiv ist.
- **Lernen**. Wenn Sie sich nicht sicher sind, welche Feldtypen oder Mindest- und Höchstlängenwerte für Ihre Anwendung ideal geeignet sind, können Sie mit der Lernfunktion Empfehlungen basierend auf den erlernten Daten generieren. Die Web App Firewall Learning Engine überwacht den Datenverkehr und bietet Empfehlungen für Feldformate basierend auf den beobachteten Werten. Um den optimalen Nutzen zu erzielen, ohne die Leistung zu beeinträchtigen, sollten Sie die Lernoption für kurze Zeit aktivieren, um ein repräsentatives Beispiel der Regeln zu erhalten, und dann die Regeln bereitstellen und das Lernen deaktivieren.
  Hinweis: Die Lern-Engine der Web App Firewall kann nur die ersten 128 Byte des Namens unterscheiden. Wenn ein Formular mehrere Felder mit Namen enthält, die für die ersten 128 Bytes

übereinstimmen, kann die Lern-Engine möglicherweise nicht zwischen ihnen unterscheiden. In ähnlicher Weise kann die implementierte Relaxationsregel versehentlich alle diese Felder entspannen.

Standardfeldformat— Zusätzlich zum Konfigurieren der Aktionen können Sie das Standardfeldformat so konfigurieren, dass der Typ der in allen Formularfeldern für Ihre Anwendung erwarteten Daten angegeben wird. Ein Feldtyp kann als Feldformattyp ausgewählt werden. Die Parameter Mindestlänge und Maximale Länge können verwendet werden, um die Länge der zulässigen Eingaben anzugeben. Alternativ zu Feldtypen können Sie Character Maps verwenden, um anzugeben, was in einem Feld zulässig ist (mit Ausnahme von Clusterbereitstellungen).

- **Feldtyp**—Feldtypen sind ein benannter Ausdruck, dem Sie zugewiesene Prioritätswerte zuweisen. Feldtyp-Ausdrücke geben die zulässigen Eingaben an und werden mit den übermittelten Daten abgeglichen, um festzustellen, ob die empfangenen Werte mit den zulässigen Werten übereinstimmen. Die Feldtypen werden in der Reihenfolge ihrer Prioritätsnummern überprüft. Eine niedrigere Zahl gibt eine höhere Priorität an. Die Web App Firewall bietet Ihnen die Möglichkeit, eigene Feldtypen hinzuzufügen und ihnen die gewünschten Prioritäten zuzuweisen. Der Prioritätswert kann zwischen 0 und 64000 liegen. Die folgenden integrierten Feldtypen werden bereitgestellt, um den Konfigurationsprozess zu vereinfachen:

```
> sh appfw fieldtype
1)      Name:  integer          Regex:  "^[+-]?[0-9]+$"
                Priority:  30           Comment:  Integer
                Builtin:  IMMUTABLE
2)      Name:  alpha            Regex:  "^[a-zA-Z]+$"
                Priority:  40           Comment:  "Alpha
                   characters"
             Builtin:  IMMUTABLE
3)      Name:  alphanum         Regex:  "^[a-zA-Z0-9]+$"
                Priority:  50           Comment:  "Alpha-numeric
                    characters"
                Builtin:  IMMUTABLE
4)      Name:  nohtml           Regex:  "^[^&<>]\*$"
                Priority:  60           Comment:  "Not HTML"
                Builtin:  IMMUTABLE
5)      Name:  any              Regex:  "^.\*$"
             Priority:  70           Comment:  Anything
                Builtin:  IMMUTABLE
    Done
>
<!--NeedCopy-->
```


> **Hinweis:** Die integrierten Feldtypen sind unveränderlich. Sie können nicht geändert oder entfernt werden. Alle Feldtypen, die Sie hinzufügen, sind MODIFIABLE. Sie können sie bearbeiten oder entfernen.

Das Konfigurieren eines Feldtyps als Standardfeldformat kann nützlich sein, wenn Sie über einen PCRE-Ausdruck verfügen, der die gültigen Eingaben in allen oder den meisten Formularfeldern für Ihre Anwendung identifizieren und die ungültigen Eingaben ausschließen kann. Wenn beispielsweise erwartet wird, dass alle Eingaben in Ihren Anwendungsformularen nur Zahlen und Buchstaben enthalten, sollten Sie das integrierte Feldtypalphanum als Standardfeldtyp verwenden. Jedes nicht-alphanumerische Zeichen wie ein umgekehrter Schrägstrich () oder Semikolon; in der Eingabe löst eine Verletzung aus. Sie können auch eigene benutzerdefinierte Feldtypen hinzufügen und diese verwenden, um Standardfeldformate zu konfigurieren. Wenn Sie beispielsweise die Kleinbuchstaben “x”, “y” und “z” zu den einzig zulässigen Alpha-Zeichen machen möchten, können Sie einen benutzerdefinierten Feldtyp mit dem regulären Ausdruck “^[x-z]+$” konfigurieren. Sie können ihm eine höhere Priorität (niedrigere Prioritätsnummer) als die integrierten Feldtypen zuweisen und sie als Standardfeldtyp verwenden.

- **Mindestlänge** — Die standardmäßige Mindestdatenlänge, die Formularfeldern in Webformularen zugewiesen ist, die keine explizite Einstellung aufweisen. Dieser Parameter ist standardmäßig auf 0 gesetzt, wodurch der Benutzer das Feld leer lassen kann. Eine höhere Einstellung zwingt Benutzer, das Feld auszufüllen.

  Achtung: Wenn der minimale Längenwert 0 ist, aber der Feldtyp Integer, Alpha oder Alphanum ist, wird eine Anforderung blockiert, wenn ein Eingabefeld trotz der Mindestlängeneinstellung leer bleibt. Das liegt daran, dass die RegEx für diese Feldtypen ein + -Zeichen enthält, was ein oder mehrere Zeichen bedeutet. Das Unterscheiden einer Ganzzahl von einem Alphazeichen erfordert mindestens ein Zeichen.

- **Maximale Länge**— Die standardmäßige maximale Datenlänge, die Formularfeldern in Webformularen zugewiesen wird, die keine explizite Einstellung aufweisen. Dieser Parameter ist standardmäßig auf 65535 eingestellt.

  > **Hinweis:** Zeichen im Vergleich zu Bytes. Die minimale und die maximale Länge für die Feldformate stellen die Anzahl der Bytes dar, nicht die Anzahl der Zeichen. Sprachen, die mehr als eine Byte-Zeichendarstellung haben, können dazu führen, dass der Grenzwert mit weniger Zeichen überschritten wird als die für den Maximalwert konfigurierte Zahl. Bei der Darstellung von Doppelbyte-Zeichen darf der maximale Wert von 9 beispielsweise nicht mehr als 4 Zeichen betragen.
  > **Tipp:** Mit der GUI können Sie UTF-8-Zeichen direkt in die GUI schneiden und einfügen, ohne sie in hex konvertieren zu müssen.

- **Zeichentabellen**: Neben der Empfehlung der Feldtypen bietet Ihnen die Lernmaschine Web

App Firewall die zusätzliche Option Zeichentabelle verwenden, um die Formatprüfungsregeln bereitzustellen. Eine Zeichenzuordnung ist ein Satz aller Zeichen, die in einem bestimmten Formularfeld zulässig sind. Mit Zeichentabellen können Sie die Feldformatspezifikation so einstellen, dass bestimmte Zeichen zugelassen oder nicht zugelassen werden. Für jedes Formularfeld wird eine separate Zeichentabelle generiert. Die Alpha- und numerischen Zeichen werden in Zeichentabelle unterschiedlich behandelt. Wenn ein Alpha-Zeichen in der Eingabe angezeigt wird, sind alle [Alpha-Zeichen A-Za-Z] durch den empfohlenen PCRE-Ausdruck in der Character Map zulässig. Wenn eine Ziffer enthalten ist, sind alle Ziffern [0-9] zulässig. Nicht druckbare Zeichen werden mit dem x-Konstrukt angegeben. Für Zeichenzuordnungsempfehlungen werden nur einzelne Byte-Zeichen mit Werten zwischen 0 und 255 berücksichtigt.

Eine Zeichenzuordnung kann spezifischer sein als die entsprechende Feldtypempfehlung. In einigen Situationen ist Zeichentabellen möglicherweise eine bessere Option, da sie Ihnen eine bessere Kontrolle über den Zeichensatz geben, der als Eingaben zulässig ist. Die bereitgestellten Zeichenzuordnungen werden als Zeichenfolgen angezeigt, die mit dem Präfix CM beginnen, gefolgt von Ziffern. Die Priorität für die Zeichentabelle beginnt bei 10000. Wie bei den vom Benutzer hinzugefügten Feldtypen können Sie eine Zeichentabelle hinzufügen, bearbeiten oder entfernen. Zeichenzuordnungen, die derzeit in bereitgestellten Regeln verwendet werden, können nicht geändert oder entfernt werden.

Hinweis: Zeichenzuordnungen werden in Clusterbereitstellungen nicht unterstützt.

> **Hinweis:**
>
> Wenn Sie eine Feldformat-Regel mit einem integrierten Feldtyp hinzufügen und anstelle von Feldtyp eine Zeichenzuordnung verwenden und diese speichern, werden die Änderungen nicht gespeichert, und die Regel wird weiterhin mit Feldtyp angezeigt.
>
> Wenn die Zeichenzuordnung mit einem der integrierten Typen übereinstimmt, wird der Feldtyp wiederverwendet, anstatt eine neue Zeichenzuordnung zu erstellen.

Verwenden der Befehlszeile zum Konfigurieren der Feldformatprüfung

In der Befehlszeilenschnittstelle können Sie den Befehl add appfw fieldtype verwenden, um einen neuen Feldtyp hinzuzufügen. Sie können entweder den Befehl set appfw profile oder den Befehl add appfw profile verwenden, um die Feldformatprüfung zu konfigurieren und anzugeben, welche Aktionen ausgeführt werden sollen. Sie können den Befehl unset appfw profile verwenden, um die konfigurierten Einstellungen wieder auf ihre Standardwerte zurückzusetzen. Zum Angeben einer Feldformatregel verwenden Sie den Befehl bind appfw, um einen Feldtyp an ein Formularfeld und die Aktions-URL zusammen mit den Mindest- und Höchstlängenspezifikationen zu binden.

Um einen Feldtyp mit der Befehlszeile hinzuzufügen, zu entfernen oder anzuzeigen:

Verwenden Sie den Befehl add, um einen Feldtyp hinzuzufügen. Beim Hinzufügen eines neuen Feld-

typs müssen Sie den Namen, den regulären Ausdruck und die Priorität angeben. Sie haben auch die Möglichkeit, einen Kommentar hinzuzufügen. Mit dem Befehl show können Sie die konfigurierten Feldtypen anzeigen. Sie können einen Feldtyp auch mit dem Befehl remove löschen, der nur den Namen des Feldtyps erfordert.

```
add [appfw] fieldType <name> <regex> <priority> [-comment <string>]
```

Wobei:

<regex> ist ein regulärer Ausdruck

<priority> ist eine positive_integer

Beispiel:

```
add fieldtype ”Cust_Zipcode” ”^[0-9]{
 5 }
 [-][0-9]{
 4 }
 $” 4

-  show [appfw] fieldType [<name>]

    Example: sh fieldtype

    sh appfw fieldtype

    sh appfw fieldtype cust_zipcode

-  `rm [appfw] fieldType <name>`

    Example: rm fieldtype cusT_ziPcode

    `rm appfw fieldtype cusT_ziPcode`
<!--NeedCopy-->
```

> **Hinweis:** Wie oben gezeigt, ist die Verwendung von “appfw” im Befehl optional. Beispielsweise sind Add FieldType oder Add appfw FieldType beide gültige Optionen. Bei den Namen der Feldtypen wird die Groß- und Kleinschreibung aufgrund der Normalisierung nicht berücksichtigt. Wie in den obigen Beispielen gezeigt, beziehen sich Cust_Zipcode, cust_Zipcode und cust_zipcode auf denselben Feldtyp.

So konfigurieren Sie eine Feldformatprüfung mit der Befehlszeile

Verwenden Sie entweder den Befehl set appfw profile oder den Befehl add appfw profile wie folgt:

- set appfw profile <name> -fieldFormatAction (([block] [learn] [log] [stats])| [none])
- set appfw profile <name>-defaultFieldFormatType <string>
- set appfw profile <name> -defaultFieldFormatMinLength <integer>
- set appfw profile <name> -defaultFieldFormatMaxLength <integer>

So konfigurieren Sie eine Feldformat-Relaxationsregel mit der Befehlszeile

```
1 bind appfw profile <name> (-fieldFormat <string> <formActionURL>  <
     fieldType>
2 [-fieldFormatMinLength <positive_integer>]  [-fieldFormatMaxLength <
     positive_integer>]
3 [-isRegex ( REGEX | NOTREGEX )])
4 <!--NeedCopy-->
```

Beispiel:

```
1 bind appfw profile pr_ffc -fieldFormat "login_name" ".*/login.php"
     integer -fieldformatMinLength 3 -FieldformatMaxlength 6
2 <!--NeedCopy-->
```

Verwenden der GUI zum Konfigurieren der Sicherheitsüberprüfung der Feldformate

In der GUI können Sie die Feldtypen verwalten. Sie können die Sicherheitsüberprüfung für Feldformate auch im Bereich für das Profil konfigurieren, das Ihrer Anwendung zugeordnet ist.

So fügen Sie einen Feldtyp mit der GUI hinzu, ändern oder entfernen Sie ihn

1. Navigieren Sie zum Knoten Anwendungsfirewall. Klicken Sie in den Einstellungen auf **Feldtypen verwalten**, um das Dialogfeld Feldtyp der Anwendungsfirewall konfigurieren anzuzeigen.
2. Klicken Sie auf **Hinzufügen**, um einen neuen Feldtyp hinzuzufügen. Folgen Sie den Anweisungen in diesem Bereich, und klicken Sie auf Erstellen. Sie können auch jeden vom Benutzer hinzugefügten Feldtyp bearbeiten oder löschen, wenn er derzeit nicht von einer bereitgestellten Regel verwendet wird.

So fügen Sie die Sicherheitsüberprüfung für Feldformate mit der GUI hinzu oder ändern

1. Navigieren Sie zu **Application Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Sicherheitsprüfungen**.

In der Tabelle Sicherheitsprüfung werden die aktuell konfigurierten Aktionseinstellungen für alle Sicherheitsprüfungen angezeigt. Sie haben 2 Optionen für die Konfiguration:

a) Wenn Sie nur **Sperren**, **Protokollieren**, **Statistiken**und **Lernaktionen**für Feldformate aktivieren oder deaktivieren möchten, können Sie Kontrollkästchen in der Tabelle aktivieren oder deaktivieren, klicken Sie auf **OK**, und klicken Sie dann auf **Speichern und Schließen**, um die Sicherheit zu schließen. Kontrollkästchen.

b) Wenn Sie zusätzliche Optionen für diese Sicherheitsprüfung konfigurieren möchten, doppelklicken Sie auf Feldformate, oder wählen Sie die Zeile aus und klicken Sie auf Aktionseinstellungen, um die folgenden Optionen für **Standardfeldformat**anzuzeigen:

- **Feldtyp**— Wählen Sie den Feldtyp aus, den Sie als Standardfeldtyp konfigurieren möchten. Sie können die integrierten und benutzerdefinierten Feldtypen auswählen. Die bereitgestellten Character Maps sind ebenfalls in der Liste enthalten und können ausgewählt werden.
- **Minimale Länge**— Geben Sie die Mindestanzahl von Zeichen an, die in jedem Feld enthalten sein müssen. Mögliche Werte: 0-65535
- **Maximale Länge**— Geben Sie die maximale Anzahl von Zeichen an, die in jedem Feld enthalten sein müssen. Mögliche Werte: 1-65535
  Sie können auch die Aktionen **Blockieren**, **Protokollieren**, **Statistiken**und **Lernen**im Bereich Einstellungen für Feldformate bearbeiten.

Nachdem Sie eine der oben genannten Änderungen vorgenommen haben, klicken Sie auf **OK**, um die Änderungen zu speichern und zur Tabelle Sicherheitsprüfungen zurückzukehren. Sie können bei Bedarf weitere Sicherheitsprüfungen konfigurieren. Klicken Sie auf **OK**, um alle Änderungen zu speichern, die Sie im Abschnitt Sicherheitsprüfungen vorgenommen haben, und klicken Sie dann auf **Speichern und schließen**, um den Bereich Sicherheitsüberprüfung zu schließen.

So konfigurieren Sie eine Relaxationsregel für Feldformate mit der GUI

1. Navigieren Sie zu **Application Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Relaxationsregeln**. Die Tabelle Relaxationsregeln enthält einen Eintrag Feldformate. Sie können doppelklicken oder diese Zeile auswählen und auf die Schaltfläche Bearbeiten klicken, um den Dialog Feldformat-Relaxationsregeln aufzurufen. Sie können Vorgänge zum **Hinzufügen**, **Bearbeiten**, **Löschen**, **Aktivieren**oder **Deaktivieren** für Relaxationsregeln ausführen.

Um eine konsolidierte Ansicht aller Relaxationsregeln zu erhalten, können Sie die Zeile Feldformate markieren und auf Visualizer klicken. Der Visualizer für bereitgestellte Relaxationen bietet Ihnen die Möglichkeit, eine neue Regel hinzuzufügen oder eine vorhandene zu bearbeiten. Sie können auch eine Gruppe von Regeln aktivieren oder deaktivieren, indem Sie einen Knoten auswählen und auf die entsprechenden Schaltflächen im Relaxationsvisualizer klicken.

Verwenden der Lernfunktion mit der Feldformat-Prüfung

Wenn die Lernaktion aktiviert ist, überwacht die Web App Firewall Learning Engine den Datenverkehr und lernt die ausgelösten Verletzungen. Sie können diese gelernten Regeln regelmäßig überprüfen. Nach gebührender Überlegung können Sie die gelernte Regel als Relaxationsregel für Feldformat bereitstellen.

Lernverbesserung für Feldformate— In Version 11.0 wurde eine Lernverbesserung der Web App Firewall eingeführt. In den vorherigen Versionen stoppt die Web App Firewall Lernmodul die Überwachung der gültigen Anforderungen, um neue Regeln auf der Grundlage der neuen Datenpunkte zu empfehlen. Dies schränkt den konfigurierten Sicherheitsschutz ein, da die Lerndatenbank keine Darstellungen der neuen Daten enthält, die in den gültigen Anforderungen angezeigt werden, die von der Sicherheitsprüfung verarbeitet werden.

Verstöße sind nicht mehr mit Lernen verbunden. Die Lern-Engine lernt und gibt Empfehlungen für die Feldformate unabhängig von den Verstößen. Zusätzlich zur Überprüfung der blockierten Anforderungen, um festzustellen, ob das aktuelle Feldformat zu restriktiv ist und entspannt werden muss, überwacht die Lern-Engine auch die zulässigen Anforderungen, um festzustellen, ob das aktuelle Feldformat zu permissiv ist, und ermöglicht die Erhöhung der Sicherheit durch Bereitstellung eines mehr restriktive Regel.

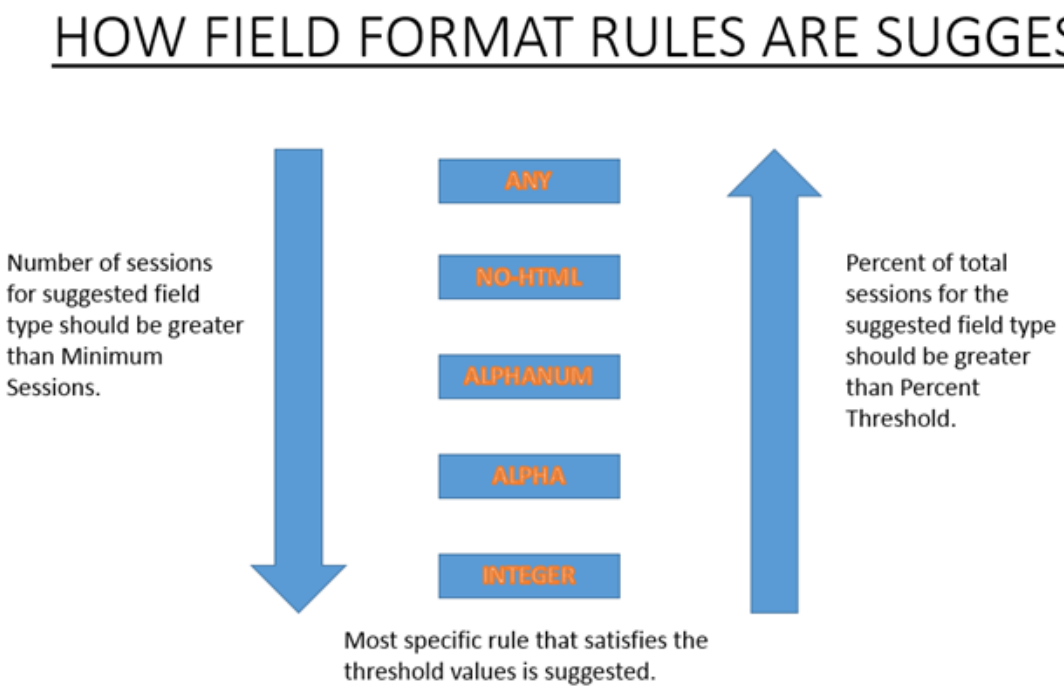
Im Folgenden finden Sie eine Zusammenfassung des Lernverhaltens von Feldformaten:

Kein Feldformat ist gebunden— Das Verhalten bleibt in diesem Szenario unverändert. Alle Lerndaten werden an die aslearn Engine gesendet. Die Lern-Engine schlägt eine Feldformatregel basierend auf dem Datensatz vor.

Feldformat ist gebunden: In den vorherigen Versionen werden beobachtete Daten nur im Falle einer Verletzung an die aslearn Engine gesendet. Die Lern-Engine schlägt eine Feldformatregel basierend auf dem Datensatz vor. In der Version 11.0 werden alle Daten an die aslearn Engine gesendet, auch wenn keine Verletzung ausgelöst wird. Die Lern-Engine schlägt eine Feldformatregel vor, die auf dem gesamten Datensatz aller empfangenen Eingaben basiert.

Anwendungsfall für Lernverbesserung:

Wenn die erlernten Regeln für das erste Feldformat auf einer kleinen Stichprobe von Daten basieren, können einige nicht typische Werte zu einer Empfehlung führen, die für das Zielfeld zu nachsichtig ist. Das laufende Lernen ermöglicht es der Web App Firewall, Datenpunkte aus jeder Anfrage zu beobachten, um eine repräsentative Probe für die erlernten Empfehlungen zu sammeln. Dies ist hilfreich, um die Sicherheit für die Bereitstellung des optimalen Eingabeformats mit einem angemessenen Bereichswert weiter zu verschärfen.



Das Feldformat-Lernen nutzt die Priorität der Feldtypen sowie die konfigurierten Einstellungen der folgenden Lernschwellenwerte:

- **FieldFormatMinThreshold**—Mindesthold, wie oft ein bestimmtes Formularfeld beobachtet werden muss, bevor eine gelernte Entspannung generiert wird. Standard: 1.
- **FieldFormatPercentThreshold**—Prozentsatz der Häufigkeit, in der ein Formularfeld mit einem bestimmten Feldtyp übereinstimmte, bevor eine gelernte Entspannung generiert wird. Standard: 0.

Die Empfehlungen für die Feldformatregel basieren auf den folgenden Kriterien:

- **Feldtypempfehlungen**— Die Feldtypempfehlungen werden durch die zugewiesenen Prioritäten der vorhandenen Feldtypen und der angegebenen Feldformatschwellenwerte bestimmt. Die Prioritäten bestimmen die Reihenfolge, in der die Feldtypen mit den Eingaben abgeglichen werden. Eine niedrigere Zahl gibt eine höhere Priorität an. Beispiel: Feldtyp-Ganzzahl hat die höhere Priorität (30) und wird daher vor dem Feldtypalphanum (50) ausgewertet. Die Schwellenwerte bestimmen die Anzahl der Eingaben, die ausgewertet werden, um eine repräsentative Stichprobe für den Datenpunkt zu sammeln. Das Zuweisen der richtigen Priorität zu den konfigurierten Feldtypen und das Konfigurieren eines geeigneten **Lerneinstellungswerts** für die Parameter **FieldFormatPercentThreshold** und **FieldFormatMinThreshold** ist unerlässlich, um die richtige Feldformatempfehlung abzuraten. Der Feldtyp mit der höchsten Priorität, basierend auf den konfigurierten Schwellenwerten, wird zuerst mit den Eingaben abgeglichen. Wenn es eine Übereinstimmung gibt, wird dieser Feldtyp vorgeschlagen, ohne die anderen Feldtypen zu berücksichtigen. Beispielsweise werden drei Standardfeldtypen, Integer, Alphanum und beliebige Feldtypen übereinstimmen, wenn alle Eingaben nur Zahlen

enthalten. Eine Ganzzahl wird jedoch empfohlen, da sie die höchste Priorität hat.

- **Empfehlungen für minimale und maximale Länge**— Berechnungen für die minimale und maximale Länge für das Feldformat werden unabhängig von der Bestimmung für den Feldtyp durchgeführt. Die Feldformatlängenberechnungen basieren auf der durchschnittlichen Länge aller beobachteten Eingaben. Die Hälfte dieses berechneten Durchschnitts wird als Mindestwert vorgeschlagen, und das Doppelte des Mittelwerts wird als Maximalwert vorgeschlagen. Der Bereich für die Mindestlänge beträgt 0-65535 und der Bereich für die maximale Länge 1-65535. Der konfigurierte Wert für die Mindestlänge darf die maximale Länge nicht überschreiten.
- **Umgang mit Leerzeichen**— Die Feldformatprüfung zählt jedes Leerzeichen, wenn die Länge der Feldformate überprüft wird. Führende oder nachfolgende Leerzeichen werden nicht entfernt, und mehrere aufeinanderfolgende Leerzeichen in der Mitte der Eingabezeichenfolge werden während der Eingabeverarbeitung nicht mehr zu einem einzigen Leerzeichen konsolidiert.

Beispiel zur Veranschaulichung der Feldformatempfehlungen:

```
Total requests: 100
Number of Req with Field Type:
Int : 22            (22 int values)  -  22%
Alpha : 44                  (44 alpha values)  -  44%
Alphanum: 14            (14 + 44 + 22 = 80 alphanum values) = 80%
noHTML: 10              (80 + 10 = 90 noHTML values) = 90%
any : 10                     (90 + 10 = 100 any values) = 100%

% threshold                              Suggested Field Type
0-22                int
23-44               alpha
45-80               alphanum
81-90               noHTML
91-100              any
<!--NeedCopy-->
```

So zeigen Sie gelernte Daten mit der Befehlszeilenschnittstelle an oder verwenden

```
show appfw learningdata <profilename> FieldFormat
rm appfw learningdata <profilename> -fieldFormat <string>  <
   formActionURL>
export appfw learningdata <profilename> FieldFormat
<!--NeedCopy-->
```

So zeigen Sie gelernte Daten mit der GUI an oder verwenden

1. Navigieren Sie zu **Application Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Gelernte Regeln** . Sie können den Eintrag Feldformate in der Tabelle Gelernte Regeln auswählen und darauf doppelklicken, um auf die erlernten Regeln zuzugreifen. Sie können die erlernten Regeln bereitstellen oder eine Regel bearbeiten, bevor Sie sie als Relaxationsregel bereitstellen. Um eine Regel zu verwerfen, können Sie sie auswählen und auf die Schaltfläche **Überspringen** klicken. Sie können jeweils nur eine Regel bearbeiten, aber Sie können mehrere Regeln zum Bereitstellen oder Überspringen auswählen.

   Sie haben auch die Möglichkeit, eine zusammengefasste Ansicht der gelernten Entspannungen anzuzeigen, indem Sie den Eintrag Feldformate in der Tabelle Gelernte Regeln auswählen und auf Visualizer klicken, um eine konsolidierte Ansicht aller gelernten Verletzungen zu erhalten. Der Visualizer macht es sehr einfach, die erlernten Regeln zu verwalten. Es bietet eine umfassende Ansicht der Daten auf einem Bildschirm und erleichtert das Handeln an einer Gruppe von Regeln mit einem Klick. Der größte Vorteil des Visualizers besteht darin, dass reguläre Ausdrücke zur Konsolidierung mehrerer Regeln empfohlen werden. Sie können eine Teilmenge dieser Regeln basierend auf dem Trennzeichen und der Aktions-URL auswählen. Sie können 25, 50 oder 75 Regeln im Visualizer anzeigen, indem Sie die Nummer aus einer Dropdownliste auswählen. Der Visualizer für erlernte Regeln bietet die Möglichkeit, die Regeln zu bearbeiten und als Relaxation bereitzustellen. Oder Sie können die Regeln überspringen, um sie zu ignorieren.

Verwenden der Protokollfunktion mit der Feldformat-Prüfung

Wenn die Protokollaktion aktiviert ist, werden die Sicherheitsüberprüfungsverletzungen für Feldformate im Überwachungsprotokoll als APPFW_FIELDFORMAT Verletzungen protokolliert. Die Web App Firewall unterstützt sowohl native als auch CEF-Protokollformate. Sie können die Protokolle auch an einen entfernten Syslog-Server senden.

So greifen Sie mit der Befehlszeile auf die Protokollmeldungen zu

Wechseln Sie zur Shell und senden Sie die ns.logs im Ordner /var/log/, um auf die Protokollmeldungen zu den Feldformat-Verletzungen zuzugreifen:

- `Shell`
- `tail -f /var/log/ns.log | grep APPFW_FIELDFORMAT`

So greifen Sie mit der GUI auf die Protokollmeldungen zu

Die Citrix GUI enthält ein sehr nützliches Tool (Syslog Viewer) zur Analyse der Protokollmeldungen. Sie haben mehrere Optionen für den Zugriff auf den Syslog Viewer:

- Navigieren Sie zu **Anwendungsfirewall** > **Profile**, wählen Sie das Zielprofil aus, und klicken Sie auf **Sicherheitsprüfungen**. Markieren Sie die Zeile Feldformate, und klicken Sie auf **Protokolle**. Wenn Sie direkt über die **Sicherheitsüberprüfung für Feldformate** des Profils auf die Protokolle zugreifen, werden die Protokollmeldungen herausgefiltert und nur die Protokolle angezeigt, die sich auf diese Sicherheitsüberprüfungsverletzungen beziehen.
- Sie können auch auf den Syslog Viewer zugreifen, indem Sie zu **Citrix ADC** > **System** > **Auditing** navigieren. Klicken Sie im Abschnitt **Überwachungsmeldungen** auf den Link **Syslog-Nachrichten**, um den **Syslog Viewer**anzuzeigen, der alle Protokollmeldungen einschließlich anderer Protokolle gegen Sicherheitsüberprüfungen anzeigt. Dies ist nützlich für das Debuggen, wenn während der Anforderungsverarbeitung mehrere Sicherheitsüberprüfungsverletzungen ausgelöst werden können.
- Navigieren Sie zu **Anwendungsfirewall** > **Richtlinien** > **Überwachung**. Klicken Sie im Abschnitt **Überwachungsmeldungen** auf den Link Syslog-Nachrichten, um den Syslog Viewer anzuzeigen, der alle Protokollmeldungen einschließlich anderer Protokolle gegen Sicherheitsüberprüfungen anzeigt.

  Der HTML-basierte Syslog Viewer bietet verschiedene Filteroptionen, um nur die Protokollmeldungen auszuwählen, die für Sie von Interesse sind. Um auf die Protokollmeldungen von Sicherheitsüberprüfungen für Feldformate zuzugreifen, filtern Sie, indem Sie APPFW in den Dropdown-Optionen für Modul auswählen. Der Ereignistyp zeigt eine Reihe von Optionen an, um Ihre Auswahl weiter zu verfeinern. Wenn Sie beispielsweise das Kontrollkästchen **APPFW_FIELDFORMAT** aktivieren und auf die Schaltfläche **Übernehmen** klicken, werden im Syslog Viewer nur Protokollmeldungen zu den Verstößen gegen die Sicherheitsüberprüfungen der Feldformate angezeigt.

Wenn Sie den Cursor in der Zeile für eine bestimmte Protokollmeldung platzieren, werden unter der Protokollmeldung mehrere Optionen wie Module und EventType angezeigt. Sie können eine dieser Optionen auswählen, um die entsprechenden Informationen in den Protokollen hervorzuheben.

Beispiel für eine Protokollmeldung im nativen Format, wenn die Anforderung nicht blockiert wird

```
1 Jun 10 22:32:26 <local0.info> 10.217.31.98 06/10/2015:22:32:26 GMT ns
     0-PPE-0 :
2 default APPFW APPFW_FIELDFORMAT 97 0 :  10.217.253.62 562-PPE0
3 x1MV+YnNGzQFM3Bsy2wti4bhXio0001 pr_ffc http://aaron.stratum8.net/FFC/
     login_post.php
4 Field format check failed for field passwd=”65568888sz-*_” <not blocked
     >
5 Example of a CEF format log message when the request is blocked
6 Jun 11 00:03:51 <local0.info> 10.217.31.98
7 CEF:0|Citrix|Citrix ADC|NS11.0|APPFW|APPFW_FIELDFORMAT|6|src
```



```
    =10.217.253.62 spt=27076
8 method=POST requet=http://aaron.stratum8.net/FFC/maxlen_post.php msg=
    Field format check
9 failed for field text_area="" cn1=108 cn2=644 cs1=pr_ffc cs2=PPE0
10 cs3=GaUROfl1Nx1jJTvja5twH5BBqI0000 cs4=ALERT cs5=2015 act=blocked
11 <!--NeedCopy-->
```

Statistiken für die Feldformat-Verstöße

Wenn die Aktion Statistik aktiviert ist, wird der entsprechende Zähler für die Feldformat-Prüfung erhöht, wenn die Web App Firewall eine Aktion für diese Sicherheitsprüfung ausführt. Die Statistiken werden für Rate und Gesamtanzahl für Traffic, Verletzungen und Protokolle gesammelt. Die Inkrement des Protokollzählers kann je nach konfigurierten Einstellungen variieren. Wenn beispielsweise die Blockaktion aktiviert ist, erhöht die Anforderung für eine Seite, die 3 Feldformatverletzungen enthält, den Statistikindikator um eins, da die Seite blockiert wird, sobald die erste Feldformat-Verletzung erkannt wird. Wenn der Block jedoch deaktiviert ist, erhöht die Verarbeitung derselben Anforderung den Statistikindikator für Verletzungen und Protokolle um 3, da jeder Feldformat-Verstoß eine separate Protokollmeldung generiert.

So zeigen Sie Feldformat-Statistiken mit der Befehlszeile an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
sh appfw stats
```

Verwenden Sie den folgenden Befehl, um Statistiken für ein bestimmtes Profil anzuzeigen:

```
stat appfw profile <profile name>
```

So zeigen Sie Feldformat-Statistiken mit der GUI an

1. Navigieren Sie zu **System** > **Sicherheit** > **Anwendungsfirewall**.
2. Greifen Sie im rechten Fensterausschnitt auf die Statistikverknüpfung zu.
3. Verwenden Sie die Bildlaufleiste, um die Statistiken zu Feldformat-Verletzungen und -Protokollen anzuzeigen. Die Statistiktabelle enthält Echtzeitdaten und wird alle 7 Sekunden aktualisiert.

Bereitstellungstipp

- Aktivieren Sie Feldformat-Aktionen protokollieren, lernen und Statistiken.
- Nachdem Sie ein repräsentatives Beispiel für den Datenverkehr zu Ihrer Anwendung ausgeführt haben, lesen Sie die erlernten Empfehlungen.
- Wenn ein Feldtyp von den meisten erlernten Regeln empfohlen wird, konfigurieren Sie diesen Feldtyp als Standardfeldtyp. Verwenden Sie für minimale und maximale Längen den breitesten von diesen Regeln vorgeschlagenen Bereich.

- Stellen Sie Regeln für andere Felder bereit, für die unterschiedliche Feldtypen oder unterschiedliche minimale/maximale Längen besser geeignet sind.
- Aktivieren Sie das Blockieren und deaktivieren Sie das Lernen.
- Überwachen Sie Statistiken und Protokolle. Wenn immer noch eine erhebliche Anzahl von Verstößen ausgelöst wird, sollten Sie die Protokollmeldungen überprüfen, um zu bestätigen, dass die Verstöße böswillige Anfragen darstellen, die blockiert worden sein müssen. Wenn gültige Anforderungen als Verstöße gekennzeichnet werden, können Sie entweder die konfigurierte Feldformatregel bearbeiten, um sie weiter zu entspannen, oder das Lernen erneut aktivieren, um Empfehlungen basierend auf den neuen Datenpunkten zu erhalten.

> **Hinweis:** Sie können Ihre Konfiguration anpassen, indem Sie neue Lernempfehlungen erhalten.

Highlights

Beachten Sie die folgenden Punkte zur Sicherheitsüberprüfung für Feldformat:

- **Schutz**— Durch die Konfiguration optimaler Feldformatregeln können Sie vor vielen Angriffen schützen. Wenn Sie beispielsweise angeben, dass ein Feld nur Ganzzahlen enthalten kann, können Hacker mit diesem Feld keine SQL-Injection- oder Cross-Site-Scripting-Angriffe starten, da die zum Starten solcher Angriffe erforderlichen Eingaben nicht den konfigurierten Feldformat-Anforderungen entsprechen.
- **Performance**— Sie können die minimale und maximal zulässige Länge für die Eingaben in den Feldformatregeln einschränken. Dies kann verhindern, dass ein böswilliger Benutzer übermäßig große Eingabezeichenfolgen eingeben, um dem Server Verarbeitungsaufwand hinzuzufügen, oder schlimmer noch, dass der Server Core wegen Stapelüberlauf ausgibt. Durch die Begrenzung der Eingabegröße können Sie die Zeit verkürzen, die für die Verarbeitung rechtmäßiger Anfragen erforderlich ist.
- **Konfigurieren von Feldformaten**— Sie müssen eine der Aktionen (block, log, stats, learn) aktivieren, um das Feld Formatschutz zu aktivieren. Sie können auch die Feldformatregeln angeben, um die zulässigen Eingaben in den Formularfeldern zu identifizieren.
- **Auswählen von Zeichenzuordnungen vs. Feldtypen**— Sowohl Zeichenzuordnungen als auch Feldtypen verwenden reguläre Ausdrücke. Eine Zeichenzuordnung stellt jedoch einen spezifischeren Ausdruck bereit, indem die Liste der zulässigen Zeichen eingeschränkt wird. Für eine Eingabe wie janedoe@citrix.com empfiehlt die Lern-Engine beispielsweise den Feldtyp nohtml, aber die Character Map [. @-za-z] könnte spezifischer sein, da es den zulässigen Satz von Nicht-Alpha-Zeichen einschränkt. Die Option Zeichenzuordnung erlaubt neben Alpha-Zeichen nur zwei Nicht-Alpha-Zeichen: Punkt (.) und at (@).
- **Laufendes Lernen**— Die Web App Firewall überwacht und berücksichtigt alle eingehenden Daten (Verletzungen sowie zulässige Eingaben), um eine Lerntabelle für die Empfehlung von Regeln zu erstellen. Die Regeln werden überarbeitet und aktualisiert, sobald neue eingehende Daten eintreffen. Neue Feldformatregeln werden für ein Feld vorgeschlagen, auch wenn es

bereits über eine gebundene Feldformatregel verfügt. Wenn die konfigurierten Feldformate zu restriktiv sind und die gültigen Anforderungen blockieren, können Sie ein entspannteres Feldformat bereitstellen. Wenn die aktuellen Feldformate zu generisch sind, können Sie die Sicherheit weiter verfeinern und verschärfen, indem Sie ein restriktiveres Feldformat bereitstellen.

- **Regeln überschreiben**— Wenn bereits eine Regel für eine Feld-/URL-Kombination bereitgestellt wurde, ermöglicht die grafische Benutzeroberfläche dem Benutzer, das Feldformat zu aktualisieren. In einem Dialogfeld werden Sie aufgefordert, die vorhandene Regel zu ersetzen. Wenn Sie die Befehlszeilenschnittstelle verwenden, müssen Sie die Bindung der vorherigen Bindung explizit aufheben und dann die neue Regel binden.
- **Mehrere Übereinstimmungen**— Wenn mehrere Feldformate mit einem bestimmten Feldnamen und seiner Aktions-URL übereinstimmen, wählt die Web App Firewall willkürlich eine dieser Formate aus, die angewendet werden soll.
- **Pufferbegrenzung**— Wenn sich ein Feldwert über mehrere Streaming-Puffer erstreckt und das Format für diese beiden Teile des Feldwerts unterschiedlich ist, wird ein Feldformat, das any entspricht, an die Lerndatenbank gesendet.
- **Feldformat vs. Feldkonsistenzprüfung**— Sowohl die Feldformatprüfung als auch die Feldkonsistenzprüfung sind formularbasierte Schutzprüfungen. Die Feldformat-Prüfung bietet einen anderen Schutz als die Formularfeldkonsistenzprüfung. Die Konsistenzprüfung für Formularfelder überprüft, ob die Struktur der von Benutzern zurückgegebenen Webformulare intakt ist, dass im HTML konfigurierte Datenformatbeschränkungen eingehalten werden und dass Daten in ausgeblendeten Feldern nicht geändert wurden. Es kann dies ohne spezifische Kenntnisse über Ihre Webformulare tun, außer dem, was es vom Webformular selbst ableitet. Die Feldformat-Prüfung überprüft, ob die Daten in den einzelnen Formularfeldern mit den spezifischen Formatierungseinschränkungen übereinstimmen, die Sie manuell konfiguriert haben oder ob das Lernfeature generiert und genehmigt wurde. Mit anderen Worten, die Konsistenzprüfung für Formularfelder erzwingt die allgemeine Webformularsicherheit, während die Feldformat-Prüfung die spezifischen Regeln für die zulässigen Eingaben für Ihre Webformulare durchsetzt.

Konsistenzprüfung des Formularfelds

October 5, 2021

Die Konsistenzprüfung für Formularfelder untersucht die von Benutzern Ihrer Website zurückgegebenen Webformulare und stellt sicher, dass Webformulare vom Kunden nicht unangemessen geändert wurden. Diese Prüfung gilt nur für HTML-Anfragen, die ein Webformular enthalten, mit oder ohne Daten. Es gilt nicht für XML-Anforderungen.

Die Konsistenzprüfung für Formularfelder verhindert, dass Kunden beim Ausfüllen und Absenden eines Formulars nicht autorisierte Änderungen an der Struktur der Webformulare auf Ihrer Website vornehmen. Es stellt außerdem sicher, dass die von einem Benutzer übermittelten Daten die HTML-Einschränkungen für Länge und Typ erfüllen und dass Daten in ausgeblendeten Feldern nicht geändert werden. Dies verhindert, dass ein Angreifer ein Webformular manipuliert und das geänderte Formular verwendet, um unbefugten Zugriff auf die Website zu erhalten, die Ausgabe eines Kontaktformulars umzuleiten, das ein unsicheres Skript verwendet und dadurch unerwünschte Massen-E-Mails sendet, oder eine Schwachstelle in Ihrer Webserversoftware auszunutzen, um die Kontrolle über das Internet zu erlangen -Server oder das zugrunde liegende Betriebssystem. Webformulare sind auf vielen Websites ein schwaches Bindeglied und ziehen eine Vielzahl von Angriffen an.

Die Konsistenzprüfung für Formularfelder überprüft alle folgenden Punkte:

- Wenn ein Feld an den Benutzer gesendet wird, stellt die Überprüfung sicher, dass es vom Benutzer zurückgegeben wird.
- Die Prüfung erzwingt HTML-Feldlängen und -typen.

  > **Hinweis:**
  >
  > – Die Konsistenzprüfung für Formularfelder erzwingt HTML-Beschränkungen für Datentyp und Länge, überprüft jedoch nicht anderweitig die Daten in Webformularen. Sie können das Kontrollkästchen Feldformate verwenden, um Regeln einzurichten, mit denen Daten überprüft werden, die in bestimmten Formularfeldern in Ihren Webformularen zurückgegeben werden.
  >
  > – Der Konsistenzschutz für Formularfelder fügt ein verstecktes Feld “as_fid” in die Antwortformulare ein, das an den Client gesendet wird. Das gleiche versteckte Feld wird von ADC entfernt, wenn der Kunde das Formular einreicht. Wenn clientseitiges JavaScript in den Formularfeldern eine Prüfsummenberechnung durchführt und dieselbe Prüfsumme im Backend überprüft wird, kann dies zu einem Bruch der Anwendung führen. In diesem Szenario wird empfohlen, das versteckte Feld für die Anwendungsfirewall-Formularfeldkonsistenz “as_fid” von der clientseitigen JavaScript-Prüfsummenberechnung zu lockern.

- Wenn Ihr Webserver kein Feld an den Benutzer sendet, erlaubt die Prüfung dem Benutzer nicht, dieses Feld hinzuzufügen und Daten darin zurückzugeben.
- Wenn es sich bei einem Feld um ein schreibgeschütztes oder ausgeblendetes Feld handelt, wird überprüft, ob sich die Daten nicht geändert haben.
- Wenn es sich bei einem Feld um ein Listenfeld oder ein Optionsfeld handelt, wird überprüft, ob die Daten in der Antwort einem der Werte in diesem Feld entsprechen.

Wenn ein von einem Benutzer zurückgegebenes Webformular gegen eine oder mehrere der Konsistenzprüfungen des Formularfelds verstößt und Sie die Web App Firewall nicht so konfiguriert haben,

dass dieses Webformular gegen die Konsistenzprüfungen von Formularfeldern verstößt, wird die Anforderung blockiert.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld Konsistenzprüfung für Formularfelder ändern auf der Registerkarte Allgemein die Aktionen Blockieren, Protokollieren, Lernen und Statistiken aktivieren oder deaktivieren.

Sie konfigurieren auch Sitzungslose Feldkonsistenz auf der Registerkarte Allgemein. Wenn Sessionless Field Consistency aktiviert ist, überprüft die Web App Firewall nur die Webformularstruktur und verzichtet auf die Teile der Formularfeldkonsistenzprüfung, die von der Pflege der Sitzungsinformationen abhängen. Dies kann die Konsistenzprüfung des Formularfelds mit geringer Sicherheitsstrafe für Websites beschleunigen, die viele Formulare verwenden. Um Sitzungslose Feldkonsistenz in allen Webformularen zu verwenden, wählen Sie On. Um es nur für Formulare zu verwenden, die mit der HTTP POST-Methode übermittelt wurden, wählen Sie PostOnly

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um die Konsistenzprüfung für Formularfelder zu konfigurieren:

- `set appfw profile <name> -fieldConsistencyAction [**block**] [**learn**] [**log**] [**stats**] [**none**]`

Um Relaxationen für die Konsistenzprüfung des Formularfelds festzulegen, müssen Sie die GUI verwenden. Klicken Sie auf der Registerkarte Prüfungen des Dialogfelds Konsistenzprüfung für Formularfelder ändern auf Hinzufügen, um das Dialogfeld Konsistenzprüfung hinzufügen zu öffnen, oder wählen Sie eine vorhandene Entspannung aus, und klicken Sie auf Öffnen, um das Dialogfeld Konsistenzprüfung für Formularfelder ändern zu öffnen. In beiden Dialogfeldern finden Sie die gleichen Optionen zum Konfigurieren einer Entspannung, wie unter Manuelle Konfiguration durch Verwendung der GUIbeschrieben.

Im Folgenden finden Sie Beispiele für die Konsistenzprüfung von Formularfeld-Konsistenzprüfungen:

Formularfeldnamen:

- Wählen Sie Formularfelder mit dem Namen UserType:

```
^UserType$
<!--NeedCopy-->
```

- Wählen Sie Formularfelder mit Namen aus, die mit UserType_ beginnen und eine Zeichenfolge folgen, die mit einem Buchstaben oder einer Zahl beginnt und aus einem bis einundzwanzig Buchstaben, Zahlen oder dem Apostroph oder Bindestrich besteht:

```
^UserType_[0-9A-Za-z][0-9A-Za-z'-]{
```



```
0,20 }
$
<!--NeedCopy-->
```

- Wählen Sie Formularfelder mit Namen aus, die mit Türkisch-UserType_ beginnen und andernfalls mit dem vorherigen Ausdruck identisch sind, außer dass sie türkische Sonderzeichen enthalten können:

```
^T\xC3\xBCrk\xC3\xA7e-UserType_([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa
   -f])+$
<!--NeedCopy-->
```

> **Hinweis:**
>
> Eine vollständige Beschreibung der unterstützten Sonderzeichen und deren ordnungsgemäße Kodierung finden Sie unter PCRE-Zeichenkodierungsformat .

- Wählen Sie Formularfeldnamen aus, die mit einem Buchstaben oder einer Zahl beginnen, nur aus einer Kombination aus Buchstaben und/oder Zahlen bestehen und die die Zeichenfolge Num an beliebiger Stelle in der Zeichenfolge enthalten:

```
^[0-9A-Za-z]\*Num[0-9A-Za-z]\*$
<!--NeedCopy-->
```

URLs für Formularfeldaktionen:

- Wählen Sie URLs, die mit einer beliebigen Zeichenfolge nach der Abfrage beginnen`http://www.example.com/search.pl?` und diese enthalten, außer für eine neue Abfrage:

```
^http://www[.]example[.]com/search[.]pl?[^?]*$
<!--NeedCopy-->
```

- Wählen Sie URLs aus, die mit `http://www.example-español.com` beginnen und Pfade und Dateinamen haben, die aus Groß- und Kleinbuchstaben, Zahlen, Nicht-ASCII-Sonderzeichen und ausgewählten Symbolen im Pfad bestehen. Das Zeichen ñ und alle anderen Sonderzeichen werden als codierte UTF-8-Zeichenfolgen dargestellt, die den Hexadezimalcode enthalten, der jedem Sonderzeichen im UTF-8-Zeichensatz zugewiesen ist:


```
^http://www[.]example-espa\xC3\xB1ol[.]com/(([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa-f])
([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa-f])
([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])*[.](asp|htp|php|s?html?)$
<!--NeedCopy-->
```

- Wählen Sie alle URLs aus, die die Zeichenfolge /search.cgi? enthalten:

```
^[^?<>]\*/search[.]cgi?[^?<>]\*$
<!--NeedCopy-->
```

> **Achtung:**
>
> Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau die URL definieren, die Sie als Ausnahme hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung von Wildcards und insbesondere der Punkt-Sternchen-Kombination (.*) kann zu Ergebnissen führen, die Sie nicht wollen oder erwarten, z. B. das Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten oder einen Angriff zulassen, den die Cookie-Konsistenzprüfung anderweitig hätte geblockt.

CSRF-Formular-Tagging-Prüfung

October 5, 2021

Die Cross-Site Request Forgery (CSRF) -Formular-Tagging markiert jedes Webformular, das von einer geschützten Website an Benutzer gesendet wird, mit einer eindeutigen und unvorhersehbaren FormID. Anschließend untersucht die von Benutzern zurückgegebenen Webformulare, um sicherzustellen, dass die bereitgestellte formID korrekt ist. Diese Überprüfung schützt vor standortübergreifenden Anforderungsfälschungen. Diese Prüfung gilt nur für HTML-Anfragen, die ein Webformular enthalten, mit oder ohne Daten. Es gilt nicht für XML-Anforderungen.

Die CSRF-Formkennzeichnungsprüfung verhindert, dass Angreifer ihre eigenen Webformulare verwenden, um hochvolumige Formularantworten mit Daten an Ihre geschützten Websites zu senden. Diese Prüfung erfordert relativ geringe CPU-Verarbeitungskapazität im Vergleich zu bestimmten anderen Sicherheitsprüfungen, die Webformulare eingehend analysieren. Es ist daher in der Lage, Angriffe mit hohem Volumen zu bewältigen, ohne die Leistung der geschützten Website oder der Web App Firewall selbst ernsthaft zu beeinträchtigen.

Bevor Sie die CSRF-Formkennzeichnungsprüfung aktivieren, müssen Sie Folgendes beachten:

- Sie müssen die Formularkennzeichnung aktivieren. Die CSRF-Prüfung hängt vom Formular-Tagging ab und funktioniert ohne sie nicht.
- Sie müssen die Citrix ADC Integrated Caching-Funktion für alle Webseiten deaktivieren, die Formulare enthalten, die durch dieses Profil geschützt sind. Das integrierte Caching-Feature und das CSRF-Formular-Tagging sind nicht kompatibel.
- Sie müssen erwägen, die Referer-Prüfung Die Überprüfung des Referers ist Teil der URL-Prüfung starten, verhindert jedoch standortübergreifende Anforderungsfälschungen, nicht Start-URL-Verstöße. Die Referenzprüfung belastet die CPU auch weniger als die CSRF-Formular-Tagging-Prüfung. Wenn eine Anforderung gegen die Verweisprüfung verstößt, wird sie sofort gesperrt, sodass die CSRF-Formular-Tagging-Prüfung nicht aufgerufen wird.
- Die Überprüfung CSRF-Formularkennzeichnung funktioniert nicht mit Webformularen, die unterschiedliche Domänen in der Formularursprung-URL und der Formularaktions-URL verwenden. Beispielsweise kann CSRF-Formular-Tagging ein Webformular nicht mit einer Formularursprungs-URL von `http://www.example.com` und einer Formularaktions-URL von `http://www.example.org/form`.pl schützen, da example.com und example.org unterschiedliche Domänen sind.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld CSRF-Formularkennzeichnung ändern auf der Registerkarte Allgemein die Aktionen Blockieren, Protokollieren, Lernen und Statistiken aktivieren oder deaktivieren.

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um die CSRF-Formularkennzeichnungsprüfung zu konfigurieren:

- `set appfw profile <name> -CSRFtagAction [**block**] [**log**] [**learn**] [**stats**] [**none**]`

Um die Relaxationen für die CSRF-Form-Tagging-Prüfung festzulegen, müssen Sie die GUI verwenden. Klicken Sie auf der Registerkarte Prüfungen des Dialogfelds CSRF-Formularkennzeichnung ändern auf Hinzufügen, um das Dialogfeld CSRF-Formularkennzeichnungsüberprüfung hinzufügen zu öffnen, oder wählen Sie eine vorhandene Entspannung aus, und klicken Sie auf Öffnen, um das Dialogfeld CSRF-Formularkennzeichnungsüberprüfung ändern zu öffnen. Beide Dialogfelder bieten die gleichen Optionen für die Konfiguration einer Entspannung.

Eine Warnung wird generiert, wenn Sie die Sitzungsbeschränkung der Citrix Web App Firewall auf einen Wert von 0 oder niedriger festlegen, da eine solche Einstellung die erweiterte Schutzüberprüfungsfunktion beeinflusst, die eine ordnungsgemäß funktionierende Web App Firewall-Sitzung erfordert.

Im Folgenden finden Sie Beispiele für CSRF-Formular-Tagging-Check-Relaxationen:

Hinweis: Die folgenden Ausdrücke sind URL-Ausdrücke, die sowohl in den Rollen Formularurigin-URL als auch Formularaktions-URL verwendet werden können.

- Wählen Sie URLs, die mit `http://www.example.com/search.pl?` beginnen und eine beliebigen Zeichenfolge nach der Abfrage enthalten, mit Ausnahme einer neuen Abfrage:

```
^http://www[.]example[.]com/search[.]pl?[^?]*$
<!--NeedCopy-->
```

- Wählen Sie URLs aus, die mit `http://www.example-español.com` beginnen und Pfade und Dateinamen haben, die aus Groß- und Kleinbuchstaben, Zahlen, Nicht-ASCII-Sonderzeichen und ausgewählten Symbolen im Pfad bestehen. Das Zeichen ñ und alle anderen Sonderzeichen werden als codierte UTF-8-Zeichenfolgen dargestellt, die den Hexadezimalcode enthalten, der jedem Sonderzeichen im UTF-8-Zeichensatz zugewiesen ist:

```
^http://www[.]example-espa\xC3\xB1ol[.]com/(([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa-f])
([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*([0-9A-Za-z]|\x[0-9A-Fa-f][0-9A-Fa-f])([0-9A-Za-z_-]|\x[0-9A-Fa-f][0-9A-Fa-f])*[.](asp|htp|php|s?html?)$
<!--NeedCopy-->
```

- Wählen Sie alle URLs aus, die die Zeichenfolge /search.cgi? enthalten:

```
^[^?<>]\*/search[.]cgi?[^?<>]\*$
<!--NeedCopy-->
```

Wichtig

Reguläre Ausdrücke sind leistungsstark. Wenn Sie mit regulären Ausdrücken im PCRE-Format nicht vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau die URL definieren, die Sie als Ausnahme hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung von Platzhaltern und insbesondere der Punkt-Sternchen (.*) -Metazeichen/Platzhalterkombination kann zu Ergebnissen führen, die Sie nicht wünschen, z. B. zum Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten, oder zum Erlauben eines Angriffs, den die Prüfung sonst blockiert hätte.

Tipp

Wenn der Referrer-Header EnableValidate unter der Start-URL-Aktion aktiviert ist, stellen Sie sicher, dass die Referrer-Header-URL ebenfalls zu startURL hinzugefügt wird.

Hinweis:

> Wenn Citrix ADC appfw_session_limit erreicht und CSRF-Prüfungen aktiviert sind, wird die Webanwendung eingefroren.
>
> Um das Einfrieren von Webanwendungen zu verhindern, verringern Sie das Sitzungstimeout und erhöhen Sie das Sitzungslimit mit der folgenden Befehle:
>
> Von CLI: > Appfw-Einstellungen festlegen —sessiontimeout 300
> Aus Shell: root @ns # nsapimgr_wr.sh -s appfw_session_limit=200000
> Das
> Protokollieren und Generieren von SNMP-Alarmen, wenn appfw_session_limit erreicht ist, hilft Ihnen bei der Fehlerbehebung und Fehlersuche.

Verwalten von CSRF-Formular-Tagging-Check-Relaxationen

December 7, 2021

Sie konfigurieren eine Ausnahme (oder Entspannung) für die Sicherheitsprüfung CSRF-Formularkennzeichnung im Dialogfeld Cross-Site-Request Forgery Tagging Check Relaxation hinzufügen oder im Dialogfeld Cross-Site-Request Forgery Tagging Check Relaxation ändern.

So konfigurieren Sie ein CSRF-Formular-Tagging, überprüfen Sie die Entspannung mit der GUI

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profile**.
2. Wählen Sie im Bereich **Profile** das Profil aus, das Sie konfigurieren möchten, und klicken Sie dann auf **Öffnen** .
3. Klicken **Sie im Dialogfeld Web App Firewall profil konfigurieren** auf die Registerkarte **Sicherheitsprüfungen** . Die Registerkarte **Sicherheitsprüfungen** enthält die Liste der Sicherheitsprüfungen der Web App Firewall.
4. Führen Sie einen der folgenden Schritte aus, um eine CSRF-Entspannung hinzuzufügen oder zu ändern:
   - Um eine neue Entspannung hinzuzufügen, klicken Sie auf Hinzufügen.
   - Um eine vorhandene Entspannung zu ändern, wählen Sie die zu ändernde Entspannung aus, und klicken Sie dann auf **Öffnen**.

   Das **Dialogfeld Cross-Site-Request Fälschung von Tagging Check Relaxation** oder **Cross-Site-Request Forgery Tagging Check Relaxation** wird angezeigt. Mit Ausnahme des Titels sind diese Dialogfelder identisch.
5. Füllen Sie das Dialogfenster wie unten beschrieben aus.

- **Kontrollkästchen Aktiviert**— Aktivieren Sie diese Option, um diese Entspannung oder Regel aktiv zu verwenden. Deaktivieren Sie diese Option, um sie zu deaktivieren.
- **Formularurigin-URL**— Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der die URL definiert, die das Formular hostet.
- **URL der Formularaktion**— Geben Sie im Textbereich einen regulären Ausdruck im PCRE-Format ein, der die URL definiert, an die in das Formular eingegebene Daten übermittelt werden.
- **Kommentare**— Geben Sie im Textbereich einen Kommentar ein. Optional.

> **Hinweis:**
>
> Für jedes Element, das einen regulären Ausdruck erfordert, können Sie den regulären Ausdruck eingeben. Verwenden Sie das Menü **Regex-Tokens**, um Elemente und Symbole für reguläre Ausdrücke direkt in das Textfeld einzufügen, oder klicken Sie auf **Regex-Editor**, um das Dialogfeld **Regulären Ausdruck hinzufügen** zu öffnen., und verwenden Sie es, um den Ausdruck zu konstruieren.

6. Klicken Sie auf **OK**. Das Dialogfeld **Cross-Site-Anforderungsfälschungsprüfung hinzufügen** oder **Cross-Site-Anforderungsfälschungsprüfung ändern** wird geschlossen, und Sie kehren zum Dialogfeld **Cross-Site-Anforderungsfälschungsprüfung ändern** zurück.
7. Um eine Entspannung oder Regel zu entfernen, wählen Sie sie aus, und klicken Sie dann auf **Entfernen**.
8. Um eine Entspannung oder Regel zu aktivieren, wählen Sie sie aus, und klicken Sie dann auf **Aktivieren**.
9. Um eine Entspannung oder Regel zu deaktivieren, wählen Sie sie aus, und klicken Sie dann auf **Deaktivieren**.
10. Um die Einstellungen und Beziehungen aller vorhandenen Relaxationen in einer integrierten interaktiven Grafikdarstellung zu konfigurieren, klicken Sie auf **Visualizer**, und verwenden Sie die Anzeigetools.
11. Um erlernte Regeln für die CSRF-Prüfung zu überprüfen und zu konfigurieren, klicken Sie auf **Lernen** und führen Sie die Schritte unter So konfigurieren und verwenden Sie die Lernfunktionaus.
12. Klicken Sie auf **OK**.

URL-Schutzüberprüfungen

October 5, 2021

Der URL-Schutz prüft Anforderungs-URLs, um zu verhindern, dass Angreifer aggressiv versuchen, auf mehrere URLs zuzugreifen (kraftvolles Surfen) oder mithilfe einer URL eine bekannte Sicherheitslücke in Webserversoftware oder Website-Skripten auszulösen.

URL-Prüfung starten

October 5, 2021

Die Start-URL-Prüfung untersucht die URLs in eingehenden Anforderungen und blockiert den Verbindungsversuch, wenn die URL die angegebenen Kriterien nicht erfüllt. Um die Kriterien zu erfüllen, muss die URL mit einem Eintrag in der Liste Start-URL übereinstimmen, es sei denn, der Parameter URL-Schließung erzwingen ist aktiviert. Wenn Sie diesen Parameter aktivieren, ist ein Benutzer, der auf einen Link auf Ihrer Website klickt, mit dem Ziel dieses Links verbunden.

Der Hauptzweck der Start-URL-Prüfung besteht darin, wiederholte Versuche zu verhindern, auf zufällige URLs auf einer Website zuzugreifen (kraftvolles Surfen) durch Lesezeichen, externe Links oder das Springen zu Seiten, indem die URLs manuell eingegeben werden, um diesen Teil der Website zu erreichen. Erzwungenes Browsen kann verwendet werden, um einen Pufferüberlauf auszulösen, Inhalte zu finden, auf die Benutzer nicht direkt zugreifen sollen, oder eine Hintertür in sicheren Bereichen Ihres Webservers zu finden. Die Web App Firewall erzwingt den angegebenen Traversal- oder Logikpfad einer Website, indem nur Zugriff auf die URLs gewährt wird, die als Start-URLs konfiguriert sind.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld Start URL Check ändern auf der Registerkarte Allgemein Sperren, Protokollieren, Statistiken, Lernaktionen und die folgenden Parameter aktivieren oder deaktivieren:

- **URL-Schließung erzwingen.** Ermöglichen Sie Benutzern den Zugriff auf jede Webseite Ihrer Website, indem Sie auf einen Hyperlink auf einer anderen Seite Ihrer Website klicken. Benutzer können zu jeder Seite Ihrer Website navigieren, die von der Startseite oder einer bestimmten Startseite aus erreicht werden kann, indem sie auf Hyperlinks klicken.
  Hinweis: Die URL-Schließfunktion ermöglicht es, jede Abfragezeichenfolge anzuhängen und mit der Aktion-URL eines Webformulars zu senden, das mit der HTTP-GET-Methode gesendet wird. Wenn Ihre geschützten Websites Formulare für den Zugriff auf eine SQL-Datenbank verwenden, stellen Sie sicher, dass Sie die SQL-Injection-Prüfung aktiviert und ordnungsgemäß konfiguriert haben.
- **Sitzungsloser URL-Abschluss.** Aus Sicht des Kunden funktioniert diese Art von URL-Schließung genauso wie die standardmäßige, sitzungsbewusste URL-Schließung, verwendet aber ein in die URL eingebettetes Token anstelle eines Cookies, um die Aktivität des Benutzers zu verfolgen, was deutlich weniger Ressourcen verbraucht. Wenn sitzungslose URL-Schließung aktiviert ist, hängt die Web App Firewall ein as_url_id -Tag an alle URLs, die sich im URL-Abschluss befinden.

Hinweis: Wenn Sie sessionless (Sessionless URL Closure) aktivieren, müssen Sie auch den regulären URL-Closure aktivieren (URL-Closure
erzwingen), oder der sitzungslose URL-Closure funktioniert nicht.

- **Referer-Header validieren.** Stellen Sie sicher, dass der Referer-Header in einer Anfrage, die Webformulardaten von Ihrer geschützten Website anstelle einer anderen Website enthält. Diese Aktion überprüft, ob Ihre Website, kein externer Angreifer, die Quelle des Webformulars ist. Dadurch wird vor Cross-Site Request Forgeries (CSRF) geschützt, ohne dass Formular-Tagging erforderlich ist, was CPU-intensiver ist als Header-Prüfungen. Die Web App Firewall kann den HTTP-Referer-Header auf eine der folgenden vier Arten verarbeiten, je nachdem, welche Option Sie in der Dropdownliste auswählen:
  - **Off**— Validieren Sie den Referer-Header nicht.
  - **If-Present**—Validieren Sie den Referer-Header, wenn ein Referer-Header vorhanden ist. Wenn ein ungültiger Referer-Header gefunden wird, generiert die Anforderung eine Referer-Header-Verletzung. Wenn kein Referer-Header vorhanden ist, generiert die Anforderung keine Verweis-Header-Verletzung. Mit dieser Option kann die Web App Firewall Referer-Header-Validierung für Anforderungen durchführen, die einen Referer-Header enthalten, aber keine Anforderungen von Benutzern blockieren, deren Browser den Referer-Header nicht festlegen oder Webproxys oder Filter verwenden, die diesen Header entfernen.
  - **Always außer Start-URLs**—Validieren Sie den Referer-Header immer. Wenn kein Referer-Header vorhanden ist und die angeforderte URL nicht von der StartURL-Relaxationsregel ausgenommen wird, generiert die Anforderung eine Referer-Header-Verletzung. Wenn der Referer-Header vorhanden ist, aber ungültig ist, generiert die Anforderung eine Referer-Header-Verletzung.
  - **Always Except First Request**— Validieren Sie immer den Referer-Header. Wenn kein Referer-Header vorhanden ist, ist nur die URL zulässig, auf die zuerst zugegriffen wird. Alle anderen URLs sind ohne gültige Referer-Header gesperrt. Wenn der Referer-Header vorhanden ist, aber ungültig ist, generiert die Anforderung eine Referer-Header-Verletzung.

Eine Start-URL-Einstellung, **Closure URLs von Sicherheitsprüfungen**ausschließen, wird nicht im Dialogfeld Start URL Check ändern konfiguriert, sondern auf der Registerkarte Einstellungen des Profils konfiguriert. Wenn diese Einstellung aktiviert ist, weist die Web App Firewall darauf hin, keine weiteren formularbasierten Prüfungen (wie Cross-Site Scripting und SQL Injection-Prüfung) für URLs durchzuführen, die die URL-Schließungskriterien erfüllen.

> **Hinweis:**
>
> Obwohl die Referer-Header-Prüfung und die Start-URL-Sicherheitsprüfung dieselben Aktionseinstellungen verwenden, ist es möglich, die Referer-Header-Prüfung zu verletzen, ohne die Start-URL-Prüfung zu verletzen. Der Unterschied ist in den Protokollen sichtbar, die Verweiskopfver-

> letzungen getrennt von Start-URL-Überprüfungsverletzungen protokollieren.

Die Referer-Header-Einstellungen (OFF, IF-Present, AlwaysExceptStartUrls und AlwaysExceptFirstRequest) sind in der Reihenfolge der am wenigsten restriktiven angeordnet und funktionieren wie folgt:

OFF:

- Referer Header wird nicht geprüft.

Wenn vorhanden:

- Anfrage hat keinen Referer-Header -> Anfrage ist erlaubt.
- Anfrage hat Referer-Header und die Referer-URL ist in URL-Schließung -> Anfrage ist erlaubt.
- Anfrage hat Referer-Header und die Referer-URL ist **nicht** in URL-Schließung -> Anfrage ist blockiert.

AlwaysExceptStartURLs:

- Anfrage hat keinen Referer-Header und die Anforderungs-URL ist eine Start-URL -> Anfrage ist erlaubt.
- Anfrage hat keinen Referer-Header und die Anforderungs-URL ist keine Start-URL ->Anforderung ist blockiert.
- Anfrage hat Referer-Header und die Referer-URL ist in URL-Schließung -> Anfrage ist erlaubt.
- Anfrage hat Referer-Header und die Referer-URL ist **nicht** in URL-Schließung -> Anfrage ist blockiert.

AlwaysExceptFirstRequest:

- Anfrage hat keinen Referer-Header und ist die erste Anforderungs-URL der Sitzung -> Anfrage ist erlaubt.
- Anfrage hat keinen Referer-Header und ist **nicht** die erste Anforderungs-URL der Sitzung -> Anfrage ist blockiert.
- Anfrage hat Referer-Header und ist entweder die erste Anforderungs-URL der Sitzung oder ist in URL-Schließung -> Anfrage ist erlaubt.
- Request hat Referer-Header und ist weder die erste Anforderungs-URL der Sitzung noch befindet sich in URL-Schließung -> Anfrage ist blockiert.

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie die folgenden Befehle eingeben, um die Start-URL-Prüfung zu konfigurieren:

- `set appfw profile <name> -startURLAction [block] [learn] [log] [stats] [none]`
- `set appfw profile <name> -startURLClosure ([ON] | [OFF])`
- `set appfw profile <name> -sessionlessURLClosure ([ON] | [OFF])`
- `set appfw profile <name> -exemptClosureURLsFromSecurityChecks ([ON] | [OFF)`

- `set appfw profile <name> -RefererHeaderCheck ([OFF] | [if-present] | [AlwaysExceptStartURLs] | [AlwaysExceptFirstRequest])`

Um Relaxationen für die Start-URL-Prüfung festzulegen, müssen Sie die GUI verwenden. Klicken Sie auf der Registerkarte Prüfungen des Dialogfelds Start URL Check ändern auf Hinzufügen, um das Dialogfeld Start URL Check Relaxation hinzufügen zu öffnen, oder wählen Sie eine vorhandene Entspannung aus, und klicken Sie auf Öffnen, um das Dialogfeld URL Check Relaxation ändern zu öffnen. Beide Dialogfelder bieten die gleichen Optionen für die Konfiguration einer Entspannung.

Im Folgenden finden Sie Beispiele für Start-URL-Check-Relaxationen:

- Erlauben Sie den Zugriff auf die Homepage unter www.example.com:

```
1 ^http://www[.]example[.]com$
2 <!--NeedCopy-->
```

- Benutzer können auf alle Webseiten im statischen HTML (.htm und .html), serveranalysierten HTML (.htp und .shtml), PHP (.php) und Microsoft ASP (.asp) unter www.example.com zugreifen:

```
1 ^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]\*/)\*
2 [0-9A-Za-z][0-9A-Za-z_.-]*[.](asp|htp|php|s?html?)$
3 <!--NeedCopy-->
```

- Benutzer können auf Webseiten mit Pfadnamen oder Dateinamen zugreifen, die Nicht-ASCII-Zeichen enthalten, unter www.example-español.com:

```
1 ^http://www[.]example-espaxC3xB1ol[.]com/(([0-9A-Za-z]|x[0-9A-Fa-
     f][0-9A-Fa-f])([0-9A-Za-z_-]|x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*
2 ([0-9A-Za-z]|x[0-9A-Fa-f][0-9A-Fa-f])([0-9A-Za-z_-]|x[0-9A-Fa-f
     ][0-9A-Fa-f])*[.](asp|htp|php|s?html?)$
3 <!--NeedCopy-->
```

Hinweis: Im obigen Ausdruck wurde jede Zeichenklasse mit der Zeichenfolge x[0-9a-Fa-F][0-9A-Fa-f]gruppiert, die allen ordnungsgemäß konstruierten Zeichencodierungszeichenfolgen entspricht, aber keine streunenden Backslash-Zeichen zulässt, die nicht mit einer UTF-8-Zeichencodierungszeichenfolge verknüpft sind. Der doppelte umgekehrte Schrägstrich () ist ein maskierter umgekehrter Schrägstrich, der die Web App Firewall anweist, ihn als wörtlichen umgekehrten Schrägstrich zu interpretieren. Wenn Sie nur einen umgekehrten Schrägstrich enthalten, interpretiert die Web App Firewall stattdessen die folgende linke eckige Klammer ([) als Literalzeichen anstelle des Öffnens einer Zeichenklasse, wodurch der Ausdruck unterbrochen wird.

- Ermöglichen Sie Benutzern den Zugriff auf alle Grafiken im Format GIF (.png), JPEG (.jpg und .jpeg) und PNG (.png) unter www.example.com:

```
^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]\*/)\*
[0-9A-Za-z][0-9A-Za-z_.-]*[.](gif|jpe?g|png)$
<!--NeedCopy-->
```

- Erlauben Sie Benutzern den Zugriff auf CGI- (.cgi) und PERL-Skripts (.pl), jedoch nur im CGI-BIN-Verzeichnis:

```
^http://www[.]example[.]com/CGI-BIN/[0-9A-Za-z][0-9A-Za-z_
   .-]*[.](cgi|pl)$
<!--NeedCopy-->
```

- Erlauben Sie Benutzern den Zugriff auf Microsoft Office und andere Dokumentdateien im Verzeichnis docsarchive:

```
^http://www[.]example[.]com/docsarchive/[0-9A-Za-z][0-9A-Za-z_
   -.]*[.](doc|xls|pdf|ppt)$
<!--NeedCopy-->
```

> **Hinweis:**
>
> Standardmäßig gelten alle Web App Firewall URLs als reguläre Ausdrücke.

Achtung: Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau die URL definieren, die Sie als Ausnahme hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung von Platzhaltern und insbesondere der Punkt-Sternchen (.*) -Metazeichen/Platzhalterkombination kann zu Ergebnissen führen, die Sie nicht wünschen, z. B. zum Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten, oder zum Erlauben eines Angriffs, den die Start-URL-Prüfung sonst blockiert hätte.

> **Tipp**
>
> Sie können das *-und-* zur zulässigen Liste von SQL-Schlüsselwörtern für das URL-Benennungsschema hinzufügen. Zum Beispiel https://FQDN/bread-and-butter.

URL-Prüfung verweigern

October 5, 2021

Die Überprüfung URL verweigern untersucht und blockiert Verbindungen zu URLs, auf die Hacker und bösartigen Code häufig zugegriffen werden. Diese Prüfung enthält eine Liste von URLs, die gemeinsame Ziele von Hackern oder bösartigem Code sind und die selten, wenn überhaupt in legitimen Anfragen angezeigt werden. Sie können der Liste auch URLs oder URL-Muster hinzufügen. Die Überprüfung URL ablehnen verhindert Angriffe auf verschiedene Sicherheitsschwachstellen, von denen bekannt ist, dass sie in der Webserver-Software oder auf vielen Websites existieren.

Die URL-Prüfung verweigert hat Vorrang vor der Start-URL-Prüfung und verweigert somit bösartige Verbindungsversuche, selbst wenn eine Start-URL-Lockerung normalerweise eine Anforderung fortfahren würde.

Im Dialogfeld URL-Überprüfung ändern können Sie auf der Registerkarte Allgemein die Aktionen Blockieren, Protokollieren und Statistiken aktivieren oder deaktivieren.

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um die URL-Prüfung zu verweigern:

- `set appfw profile <name> -denyURLAction [**block**] [**log**] [**stats**] [**none**]`

Um eigene Deny-URLs zu erstellen und zu konfigurieren, müssen Sie die GUI verwenden. Klicken Sie auf der Registerkarte Überprüfungen des Dialogfelds URL-Überprüfung ändern auf Hinzufügen, um das Dialogfeld Ablehnen-URL hinzufügen zu öffnen, oder wählen Sie eine vorhandene benutzerdefinierte Ablehnungs-URL aus, und klicken Sie auf Öffnen, um das Dialogfeld URL ändern zu öffnen. Beide Dialogfelder bieten dieselben Optionen zum Erstellen und Konfigurieren einer Deny-URL.

Im Folgenden finden Sie Beispiele für URL-Ausdrücke ablehnen:

- Erlauben Sie Benutzern nicht, direkt auf den Image-Server unter images.example.com zuzugreifen:

```
1  ^http://images[.]example[.]com$
2  <!--NeedCopy-->
```

- Benutzer dürfen nicht direkt auf CGI- (.cgi) - oder PERL- (.pl) -Skripts zugreifen:

```
1  ^http://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-]\*/)\*
2  [0-9A-Za-z][0-9A-Za-z_.-]*[.](cgi|pl)$
```



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

- Hier ist die gleiche Deny-URL, die geändert wurde, um Nicht-ASCII-Zeichen zu unterstützen:

```
1  ^http://www[.]example[.]com/(([0-9A-Za-z]|x[0-9A-Fa-f][0-9A-Fa-f
      ])
2  ([0-9A-Za-z_-]|x[0-9A-Fa-f][0-9A-Fa-f])\*/)\*([0-9A-Za-z]|x[0-9A-
      Fa-f][0-9A-Fa-f])
3  ([0-9A-Za-z_-]|x[0-9A-Fa-f][0-9A-Fa-f])*[.](cgi|pl)$
4  <!--NeedCopy-->
```

> **Achtung:**
>
> Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau die URL oder das Muster definieren, die Sie blockieren möchten, und nichts anderes. Die unvorsichtige Verwendung von Platzhaltern und insbesondere der Punkt-Sternchen (.*) -Metazeichen/Platzhalterkombination kann zu Ergebnissen führen, die Sie nicht möchten, z. B. zum Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten.

XML-Schutzüberprüfungen

October 5, 2021

Die XML-Schutzüberprüfungen untersuchen Anfragen für XML-basierte Angriffe aller Art.

> **Achtung:**
>
> Die XML-Sicherheitsprüfungen gelten nur für Inhalte, die mit einem HTTP-Content-Type-Header von text/xml gesendet werden. Wenn der Content-Type-Header fehlt oder auf einen anderen Wert eingestellt ist, werden alle XML-Sicherheitsprüfungen umgangen. Wenn Sie vorhaben, XML- oder Web 2.0-Webanwendungen zu schützen, müssen die Webmaster jedes Webservers, der diese Anwendungen hostet, sicherstellen, dass der richtige HTTP-Inhaltstyp-Header gesendet wird.

XML-Formatprüfung

October 5, 2021

Die XML-Formatprüfung untersucht das XML-Format eingehender Anforderungen und blockiert die Anforderungen, die nicht gut geformt sind oder die die Kriterien in der XML-Spezifikation für korrekt geformte XML-Dokumente nicht erfüllen. Einige dieser Kriterien sind:

- Ein XML-Dokument darf nur richtig codierte Unicode-Zeichen enthalten, die der Unicode-Spezifikation entsprechen.
- Es können keine speziellen XML-Syntaxzeichen wie <, > und &in das Dokument aufgenommen werden, außer wenn sie in XML-Markup verwendet werden.
- Alle Beginn-, End- und Leerelement-Tags müssen korrekt verschachtelt sein und keine fehlen oder überlappen.
- Bei XML-Element-Tags wird zwischen Groß- und Kleinschreibung unterschieden. Alle Anfangs- und End-Tags müssen genau übereinstimmen.
- Ein einzelnes Stammelement muss alle anderen Elemente im XML-Dokument enthalten.

Ein Dokument, das die Kriterien für wohlgeformte XML nicht erfüllt, erfüllt nicht die Definition eines XML-Dokuments. Streng genommen ist es kein XML. Allerdings erzwingen nicht alle XML-Anwendungen und Webdienste den XML-Standard, und nicht alle behandeln schlecht geformte oder ungültige XML korrekt. Unsachgemäße Verarbeitung eines schlecht geformten XML-Dokuments kann zu Sicherheitsverstößen führen. Der Zweck der XML-Formatprüfung besteht darin, einen böswilligen Benutzer daran zu hindern, eine schlecht geformte XML-Anforderung zu verwenden, um die Sicherheit Ihrer XML-Anwendung oder Web-Service zu verletzen.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld XML-Format ändern auf der Registerkarte Allgemein die Aktionen Blockieren, Protokollieren und Statistiken aktivieren oder deaktivieren.

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um die XML-Formatprüfung zu konfigurieren:

- `set appfw profile <name> -xmlFormatAction [**block**] [**log**] [**stats**] [**none**]`

Sie können keine Ausnahmen für die XML-Formatprüfung konfigurieren. Sie können es nur aktivieren oder deaktivieren.

XML-Denial-of-Service-Prüfung

October 5, 2021

Die XML Denial-of-Service-Prüfung (XML DoS oder XDOs) untersucht eingehende XML-Anfragen, um festzustellen, ob sie mit den Merkmalen eines Denial-of-Service (DoS) -Angriffs übereinstimmen. Wenn es eine Übereinstimmung gibt, blockiert diese Anfragen. Der Zweck der XML-DoS-Prüfung

besteht darin, zu verhindern, dass ein Angreifer XML-Anfragen verwendet, um einen Denial-of-Service-Angriff auf Ihren Webserver oder Ihre Website zu starten.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld Denial-of-Service-Prüfung ändern auf der Registerkarte **Allgemein** die Aktionen Blockieren, Protokollieren, Statistiken und Lernen aktivieren oder deaktivieren:

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um die XML-Denial-of-Service-Prüfung zu konfigurieren:

- `set appfw profile <name> -xmlDoSAction [**block**] [**log**] [**learn**] [**stats**] [**none**]`

Um einzelne XML-Denial-of-Service-Regeln zu konfigurieren, müssen Sie die GUI verwenden. Wählen Sie auf der Registerkarte **Prüfungen** des Dialogfelds **Denial-of-Service-Überprüfung** ändern eine Regel aus, und klicken Sie auf **Öffnen**, um das Dialogfeld **Denial-of-Service ändern** für diese Regel zu öffnen. Die einzelnen Dialogfelder unterscheiden sich für die verschiedenen Regeln, sind aber einfach. Einige erlauben es Ihnen nur, die Regel zu aktivieren oder zu deaktivieren, andere ermöglichen es Ihnen, eine Zahl zu ändern, indem Sie einen neuen Wert in ein Textfeld eingeben.

> **Hinweis:**
>
> Das erwartete Verhalten der Learning Engine für Denial-of-Service-Angriffe basiert auf der konfigurierten Aktion. Wenn die Aktion als “Blockieren” festgelegt ist, lernt die Engine den konfigurierten Bind-Wert +1 und die XML-Analyse stoppt bei einer Verletzung. Wenn die konfigurierte Aktion nicht als “Block” festgelegt ist, lernt die Engine den tatsächlichen Wert für die Länge des eingehenden Verstoßes.

Die einzelnen XML-Denial-of-Service-Regeln lauten:

- Maximale Elementtiefe. Beschränken Sie die maximale Anzahl verschachtelter Ebenen in jedem einzelnen Element auf 256. Wenn diese Regel aktiviert ist und die Web App Firewall eine XML-Anforderung mit einem Element erkennt, das mehr als die maximale Anzahl zulässiger Ebenen aufweist, blockiert sie die Anforderung. Sie können die maximale Anzahl von Ebenen auf einen beliebigen Wert von 1 bis 65.535 ändern.
- Maximale Länge des Elementnamens. Beschränken Sie die maximale Länge jedes Elementnamens auf 128 Zeichen. Dies schließt den Namen innerhalb des erweiterten Namespace ein, der den XML-Pfad und den Elementnamen im folgenden Format enthält:

```
{
http://prefix.example.com/path/ }
target_page.xml
<!--NeedCopy-->
```


Der Benutzer kann die maximale Namenslänge auf einen beliebigen Wert zwischen einem (1) Zeichen und 65.535 ändern.

- Maximal # Elemente. Beschränken Sie die maximale Anzahl eines beliebigen Elementtyps pro XML-Dokument auf 65.535. Sie können die maximale Anzahl von Elementen auf einen beliebigen Wert zwischen 1 und 65.535 ändern.
- Maximal # Element Kinder. Beschränken Sie die maximale Anzahl von untergeordneten Elementen (einschließlich anderer Elemente, Zeicheninformationen und Kommentare), die jedes einzelne Element auf 65.535 haben darf. Sie können die maximale Anzahl von untergeordneten Elementen auf einen beliebigen Wert zwischen 1 und 65.535 ändern.
- Maximale Anzahl von Attributen Beschränken Sie die maximale Anzahl von Attributen, die jedes einzelne Element haben darf, auf 256. Sie können die maximale Anzahl von Attributen in einen beliebigen Wert zwischen 1 und 256 ändern.
- Maximale Länge von Attributnamen. Beschränken Sie die maximale Länge jedes Attributnamens auf 128 Zeichen. Sie können die maximale Länge des Attributnamens auf einen beliebigen Wert zwischen 1 und 2.048 ändern.
- Maximale Attributwert-Länge. Beschränken Sie die maximale Länge jedes Attributwerts auf 2048 Zeichen. Sie können die maximale Länge des Attributnamens auf einen beliebigen Wert zwischen 1 und 2.048 ändern.
- Maximale Länge der Zeichendaten Beschränken Sie die maximale Zeichendatenlänge für jedes Element auf 65.535. Sie können die Länge auf einen beliebigen Wert zwischen 1 und 65.535 ändern.
- Maximale Dateigröße Beschränken Sie die Größe jeder Datei auf 20 MB. Sie können die maximale Dateigröße auf einen beliebigen Wert ändern.
- Minimale Dateigröße. Erfordert, dass jede Datei mindestens 9 Byte lang ist. Sie können die minimale Dateigröße auf jede positive Ganzzahl ändern, die verschiedene Bytes repräsentiert.
- Maximale # Entity Expansions. Beschränken Sie die Anzahl der erlaubten Entitätenerweiterungen auf die angegebene Zahl. Standard: 1024.
- Maximale Entity-Erweiterungstiefe Beschränken Sie die maximale Anzahl verschachtelter Entitätenerweiterungen auf höchstens die angegebene Zahl. Standard: 32.
- Maximal # Namespaces. Beschränken Sie die Anzahl der Namespace-Deklarationen in einem XML-Dokument auf nicht mehr als die angegebene Zahl. Standard: 16.
- Maximale Namespace-URI-Länge. Begrenzen Sie die URL-Länge jeder Namespace-Deklaration auf nicht mehr als die angegebene Anzahl von Zeichen. Standard: 256.
- Anweisungen zur Blockverarbeitung. Sperren Sie alle speziellen Verarbeitungsanweisungen, die in der Anfrage enthalten sind. Diese Regel weist keine vom Benutzer veränderbaren Werte

auf.

- Blockieren Sie DTD. Blockieren Sie alle Dokumenttypdefinitionen (DTD), die in der Anforderung enthalten sind. Diese Regel weist keine vom Benutzer veränderbaren Werte auf.
- Blockieren Sie externe Entitäten Blockieren Sie alle Verweise auf externe Entitäten in der Anforderung. Diese Regel weist keine vom Benutzer veränderbaren Werte auf.
- SOAP-Array-Prüfung Aktivieren oder deaktivieren Sie die folgenden SOAP-Array-Prüfungen:
  - **Maximale SOAP-Array-Größe.** Die maximale Gesamtgröße aller SOAP-Arrays in einer XML-Anforderung, bevor die Verbindung blockiert wird. Sie können diesen Wert ändern. Standard: 20000000.
  - **Maximaler SOAP-Array-Rang.** Der maximale Rang oder die Dimensionen eines einzelnen SOAP-Arrays in einer XML-Anforderung, bevor die Verbindung blockiert wird. Sie können diesen Wert ändern. Standard: 16.

Site-übergreifende XML-Skripterstellung

December 7, 2021

Die XML Cross-Site Scripting Prüfung prüft die Benutzeranforderungen auf mögliche Cross-Site Scripting Angriffe in der XML-Payload. Wenn es einen möglichen siteübergreifenden Skriptangriff findet, blockiert es die Anforderung.

Um den Missbrauch der Skripts in Ihren geschützten Webdiensten zu verhindern, um die Sicherheit Ihrer Webdienste zu verletzen, blockiert die XML Cross-Site Scripting-Prüfung Skripts, die gegen dieselbe Ursprungsregel verstoßen, und besagt, dass Skripts auf keinem Server, sondern auf dem Server, auf dem sie sich befinden, zugreifen oder diese ändern dürfen. Jedes Skript, das gegen dieselbe Ursprungsregel verstößt, wird als siteübergreifendes Skript bezeichnet, und die Praxis, Skripts zum Zugriff auf oder Ändern von Inhalten auf einem anderen Server zu verwenden, wird als siteübergreifende Skripts bezeichnet. Der Grund, warum Cross-Site Scripting ein Sicherheitsproblem ist, ist, dass ein Webserver, der Cross-Site Scripting ermöglicht, mit einem Skript angegriffen werden kann, das sich nicht auf diesem Webserver befindet, sondern auf einem anderen Webserver befindet, z. B. einem, der vom Angreifer gehört und kontrolliert wird.

Die Web App Firewall bietet verschiedene Aktionsoptionen für die Implementierung von XML Cross-Site Scripting Protection. Sie haben die Möglichkeit, **Block-**, **Protokoll-**und **Statistikaktionen**zu konfigurieren.

Die Site-Cross-Scripting-Überprüfung der Web App Firewall XML wird für die Nutzlast der eingehenden Anforderungen durchgeführt und Angriffszeichenfolgen werden auch dann identifiziert, wenn sie über

mehrere Zeilen verteilt sind. Die Prüfung sucht nach Cross-Site-Scripting-Angriffszeichenfolgen im **Element** und den **Attributwerten**. Sie können Entspannungen anwenden, um die Sicherheitskontrolle unter bestimmten Bedingungen zu umgehen. Die Protokolle und Statistiken können Ihnen helfen, benötigte Entspannungen zu identifizieren.

Der CDATA Abschnitt der XML-Nutzlast könnte ein attraktiver Schwerpunkt für die Hacker sein, da die Skripts außerhalb des CDATA Abschnitts nicht ausführbar sind. Ein CDATA Abschnitt wird für Inhalte verwendet, die vollständig als Zeichendaten behandelt werden sollen. HTML-Markierungs-Tagtrennzeichen **<**, **>**und **/>**führen nicht dazu, dass der Parser den Code als HTML-Elemente interpretiert. Das folgende Beispiel zeigt einen CDATA-Section mit Cross-Site-Scripting-Angriffsstring:

```
1     <![CDATA[rn
2     <script language=”Javascript” type=”text/javascript”>alert (”Got
         you”)</script>rn
3     ]]>
4 <!--NeedCopy-->
```

Aktionsoptionen

Eine Aktion wird angewendet, wenn die Prüfung auf XML Cross-Site Scripting einen Cross-Site-Scripting-Angriff in der Anfrage erkennt. Die folgenden Optionen stehen zur Optimierung des XML Cross-Site Scripting Protects für Ihre Anwendung zur Verfügung:

- **Block**: Die Blockierungsaktion wird ausgelöst, wenn die Cross-Site-Scripting-Tags in der Anforderung erkannt werden.
- **Log**— Generieren Sie Protokollmeldungen, die die Aktionen angeben, die von der XML Cross-Site Scripting Prüfung ausgeführt werden. Wenn der Block deaktiviert ist, wird für jeden Standort (ELEMENT, ATTRIBUTE) eine separate Protokollnachricht generiert, in der die Cross-Site-Scripting-Verletzung erkannt wird. Allerdings wird nur eine Nachricht generiert, wenn die Anforderung blockiert wird. Sie können die Protokolle überwachen, um festzustellen, ob Antworten auf legitime Anfragen blockiert werden. Eine große Zunahme der Anzahl von Protokollmeldungen kann auf Versuche hinweisen, einen Angriff zu starten.
- **Statistiken**— Sammeln Sie Statistiken über Verstöße und Protokolle. Ein unerwarteter Anstieg im Statistikzähler deutet möglicherweise darauf hin, dass Ihre Anwendung angegriffen wird. Wenn legitime Anfragen blockiert werden, müssen Sie möglicherweise die Konfiguration erneut besuchen, um zu sehen, ob Sie neue Relaxationsregeln konfigurieren oder die vorhandenen ändern müssen.

Relaxationsregeln

Wenn Ihre Anwendung erfordert, dass Sie die Cross-Site Scripting Prüfung für ein bestimmtes ELEMENT oder ATTRIBUTE in der XML-Nutzlast umgehen müssen, können Sie eine Relaxationsregel konfigurieren. Die Relaxationsregeln für die XML-Cross-Site Scripting haben die folgenden Parameter:

- **Name**—Sie können Literalzeichenfolgen oder reguläre Ausdrücke verwenden, um den Namen des ELEMENT oder des Attributs zu konfigurieren. Der folgende Ausdruck befreit alle ELEMENTS, die mit dem Zeichenfolgenname_ beginnen, gefolgt von einer Zeichenfolge aus Groß- oder Kleinbuchstaben oder Zahlen, die mindestens zwei und höchstens fünfzehn Zeichen lang sind:

  ```
  ^name_[0-9A-Za-z]{ 2,15 } $
  ```

> **Hinweis:**
>
> Bei den Namen wird Groß- und Kleinschreibung erkannt. Doppelte Einträge sind nicht zulässig, aber Sie können die Großschreibung der Namen und Unterschiede in der Position verwenden, um ähnliche Einträge zu erstellen. Zum Beispiel ist jede der folgenden Entspannungsregeln einzigartig:
>
> 1. `XMLcross-site scripting: ABC IsRegex: NOTREGEX Location: ATTRIBUTE State: ENABLED`
> 2. `XMLcross-site scripting: ABC IsRegex: NOTREGEX Location: ELEMENT State: ENABLED`
> 3. `XMLcross-site scripting: abc IsRegex: NOTREGEX Location: ELEMENT State: ENABLED`
> 4. `XMLcross-site scripting: abc IsRegex: NOTREGEX Location: ATTRIBUTE State: ENABLED`

- **Speicherort**— Sie können den Speicherort der Ausnahme für die standortübergreifende Skriptüberprüfung in Ihrer XML-Nutzlast angeben. Die Option ELEMENT ist standardmäßig ausgewählt. Sie können es in ATTRIBUTEändern.
- **Kommentar**—Dies ist ein optionales Feld. Sie können bis zu 255 Zeichen verwenden, um den Zweck dieser Relaxationsregel zu beschreiben.

> **Warnung**
>
> Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau den Namen definieren, den Sie als Ausnahme hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung von regulären Ausdrücken kann Ergebnisse haben, die Sie nicht wünschen, z. B. das Blockieren des Zugriffs auf Webinhalte, die Sie nicht

> blockieren wollten, oder das Zulassen eines Angriffs, den die XML Cross-Site Scripting Prüfung ansonsten blockiert hätte.

Verwenden der Befehlszeile zum Konfigurieren der XML-Site-Cross-Site-Skripting-Prüfung

So konfigurieren Sie XML Cross-Site Scripting Überprüfungsaktionen und andere Parameter mit der Befehlszeile

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie die folgenden Befehle eingeben, um die XML Cross-Site Scripting Check zu konfigurieren:

```
> set appfw profile <name> -XMLcross-site scriptingAction (([block] [log] [
stats])| [none])
```

So konfigurieren Sie eine XML-Cross-Site Scripting Check-Relaxationsregel mit der Befehlszeile

Sie können Relaxationsregeln hinzufügen, um die Inspektion der Cross-Site Scripting Script-Angriffsprüfung an einem bestimmten Ort zu umgehen. Verwenden Sie den Befehl bind oder unbind, um die Relaxationsregelbindung wie folgt hinzuzufügen oder zu löschen:

```
> bind appfw profile <name> -XMLcross-site scripting <string> [isRegex (
REGEX | NOTREGEX)] [-location ( ELEMENT | ATTRIBUTE )] -comment <string> [-
state ( ENABLED | DISABLED )]
```

```
> unbind appfw profile <name> -XMLcross-site scripting <String>
```

Beispiel:

```
> bind appfw profile test_pr -XMLcross-site scripting ABC
```

Nach dem Ausführen des obigen Befehls wird die folgende Relaxationsregel konfiguriert. Die Regel ist aktiviert, der Name wird als Literal (NOTREGEX) behandelt, und ELEMENT wird als Standardspeicherort ausgewählt:

```
1)      XMLcross-site scripting:  ABC            IsRegex:  NOTREGEX

        Location:  ELEMENT       State:  ENABLED

`> unbind appfw profile test_pr -XMLcross-site scripting abc`

ERROR: No such XMLcross-site scripting check

`> unbind appfw profile test_pr -XMLcross-site scripting ABC`

 Done
```



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

Verwenden der GUI zum Konfigurieren der XML-Site-Cross-Site-Skriptprüfung

In der grafischen Benutzeroberfläche können Sie die XML-Cross-Site-Skripterstellung im Bereich für das Profil konfigurieren, das Ihrer Anwendung zugeordnet ist.

So konfigurieren oder ändern Sie die XML Cross-Site Scripting Prüfung mit der GUI

1. Navigieren Sie zu **Web App Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich Erweiterte Einstellungen auf **Sicherheitsprüfungen**.

In der Tabelle Sicherheitsprüfung werden die aktuell konfigurierten Aktionseinstellungen für alle Sicherheitsprüfungen angezeigt. Sie haben 2 Optionen für die Konfiguration:

a) Wenn Sie nur Aktionen **Blockieren**, **Protokollieren**und **Statistiken**für die **XML Cross-Site Scripting aktivieren oder deaktivieren möchten, können Sie Kontrollkästchen**in der Tabelle aktivieren oder deaktivieren, klicken Sie auf **OK**, und klicken Sie dann auf Speichern und Schließen, um die Sicherheit zu schließen. Kontrollkästchen.

b) Sie können auf **XML Cross-Site Scripting**doppelklicken oder die Zeile auswählen und auf **Aktionseinstellungen**klicken, um die Aktionsoptionen anzuzeigen. Nachdem Sie eine der Aktionseinstellungen geändert haben, klicken Sie auf **OK**, um die Änderungen zu speichern und zur Tabelle Sicherheitsprüfungen zurückzukehren.

Sie können bei Bedarf weitere Sicherheitsprüfungen konfigurieren. Klicken Sie auf **OK**, um alle Änderungen zu speichern, die Sie im Abschnitt Sicherheitsprüfungen vorgenommen haben, und klicken Sie dann auf **Speichern und schließen**, um den Bereich Sicherheitsüberprüfung zu schließen.

So konfigurieren Sie eine XML-Cross-Site Scripting Relaxationsregel mit der GUI

1. Navigieren Sie zu **Web App Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Relaxationsregeln**.
3. Doppelklicken Sie in der Tabelle Relaxationsregeln auf den Eintrag **XML Cross-Site Scripting**, oder wählen Sie ihn aus, und klicken Sie auf **Bearbeiten** .
4. Führen Sie im Dialogfeld **XML-Cross-Site Scripting Relaxationsregeln** die Vorgänge **Hinzufügen**, **Bearbeiten**, **Löschen**, **Aktivieren** oder **Deaktivieren** für Relaxationsregeln aus.

So verwalten Sie XML Cross-Site Scripting Relaxationsregeln mithilfe des Visualizers

Um eine konsolidierte Ansicht aller Relaxationsregeln zu erhalten, können Sie die Zeile **XML Cross-Site Scripting** in der Tabelle Relaxationsregeln markieren und auf **Visualizer** klicken. Der Visualizer für bereitgestellte Relaxationen bietet Ihnen die Möglichkeit, eine neue Regel **hinzuzufügen** oder eine

vorhandene zu **bearbeiten**. Sie können auch eine Gruppe von Regeln **aktivieren** oder **deaktivieren**, indem Sie einen Knoten auswählen und auf die entsprechenden Schaltflächen im Relaxationsvisualizer klicken.

So zeigen Sie die Cross-Site Scripting Patterns mit der GUI an oder passen Sie sie an

Sie können die GUI verwenden, um die Standardliste der Siteübergreifenden Skripting-Attribute oder zulässigen Tags anzuzeigen oder anzupassen. Sie können auch die Standardliste der Siteübergreifenden Skripterstellung verweigerter Muster anzeigen oder anpassen.

Die Standardlisten werden unter **Web App Firewall** > **Signaturen** > **Standardsignaturen** angegeben. Wenn Sie kein Signaturobjekt an Ihr Profil binden, wird die im Standardobjekt "Standardsignaturen" angegebene Standardliste für Cross-Site Scripting Allowed und "Verweigert" vom Profil für die Verarbeitung der Cross-Site Scripting Sicherheitsprüfung verwendet. Die Tags, Attribute und Patterns, die im Standardsignaturobjekt angegeben sind, sind schreibgeschützt. Sie können sie nicht bearbeiten oder ändern. Wenn Sie diese ändern oder ändern möchten, erstellen Sie eine Kopie des Standardsignaturen-Objekts, um ein Benutzerdefiniertes Signaturobjekt zu erstellen. Nehmen Sie Änderungen in den Listen Zulässig oder Verweigert im neuen benutzerdefinierten Signaturobjekt vor, und verwenden Sie dieses Signaturobjekt in dem Profil, das den Datenverkehr verarbeitet, für den Sie diese angepassten zulässigen und verweigerten Listen verwenden möchten.

Weitere Hinweise zu Signaturen finden Sie unterhttp://support.citrix.com/proddocs/topic/ns-security-10-map/appfw-signatures-con.html.

So zeigen Sie standardmäßige Cross-Site-Skriptmuster an:

1. Navigieren Sie zu **Web App Firewall** > **Signaturen**, wählen Sie ***Standardsignaturen aus**, und klicken Sie auf **Bearbeiten** . Klicken Sie dann auf **SQL/Cross-Site Scripting Pattern verwalten**.

Die Tabelle **SQL/Cross-Site-Scripting-Pfade verwalten** zeigt die folgenden drei Zeilen, die sich auf Cross-Site-Skripts beziehen:

```
1             xss/allowed/attribute
2
3             xss/allowed/tag
4
5             xss/denied/pattern
6 <!--NeedCopy-->
```

Wählen Sie eine Zeile aus und klicken Sie auf **Elemente verwalten**, um die entsprechenden Cross-Site-Scripting-Elemente (Tag, Attribut, Pattern) anzuzeigen, die von der **Cross-Site Scripting-Überprüfung** der Web App Firewall verwendet werden.

So passen Sie Cross-Site-Scripting-Elementean: Sie können das benutzerdefinierte Signaturobjekt

bearbeiten, um das zulässige Tag, die zulässigen Attribute und die verweigerten Sie können neue Einträge hinzufügen oder vorhandene entfernen.

1. **Navigieren Sie zu Web App Firewall** > **Signaturen**, markieren Sie die benutzerdefinierte Zielsignatur und klicken Sie auf **Bearbeiten**. Klicken Sie auf **SQL/Cross-Site-Skriptmuster verwalten, um die Tabelle SQL/Cross-Site-Scripting-Pfade** verwalten anzuzeigen.
2. Wählen Sie die Ziel-Cross-Site-Skript-Zeile aus

a) Klicken Sie auf **Elemente verwalten**, um das entsprechende Cross-Site-Scripting-Element **hinzuzufügen**, zu **bearbeiten** oder zu **entfernen** .

b) Klicken Sie auf **Entfernen**, um die ausgewählte Zeile zu entfernen.

> **Warnung**
>
> Seien Sie sehr vorsichtig, wenn Sie ein standardmäßiges Cross-Site-Scripting-Element entfernen oder ändern oder den Cross-Site-Skriptpfad löschen, um die gesamte Zeile zu entfernen. Die Signaturen, die Sicherheitsprüfung für HTML Cross-Site Scripting und die Sicherheitsprüfung für XML Cross-Site Scripting basieren auf diesen Elementen, um Angriffe zum Schutz Ihrer Anwendungen zu erkennen. Das Anpassen der Cross-Site-Scripting Elements kann Ihre Anwendung anfällig für Cross-Site Scripting-Angriffe machen, wenn das erforderliche Muster während der Bearbeitung entfernt wird.

Verwenden der Protokollfunktion mit der websiteübergreifenden XML-Skriptprüfung

Wenn die Protokollaktion aktiviert ist, werden die Verletzungen der XML Cross-Site Scripting-Sicherheitsprüfung im Audit-Log als Verstöße gegen **AppFW_XML_Cross-Site Scripting** protokolliert. Die Web App Firewall unterstützt sowohl native als auch CEF-Protokollformate. Sie können die Protokolle auch an einen entfernten Syslog-Server senden.

So greifen Sie mit der Befehlszeile auf die Protokollmeldungen zu

Wechseln Sie zur Shell und ziehen Sie die ns.logs im Ordner /var/log/, um auf die Protokollmeldungen zu den XML-Cross-Site Scripting Verletzungen zuzugreifen:

```
> \*\*Shell\*\*

> \*\*tail -f /var/log/ns.log | grep APPFW_XML_cross-site scripting\*\*
<!--NeedCopy-->
```

Beispiel für eine XML-Cross-Site Scripting Sicherheitsüberprüfungsprotokollnachricht im systemeigenen Protokollformat mit<blocked> Aktion


```
Oct  7 01:44:34 <local0.warn> 10.217.31.98 10/07/2015:01:44:34 GMT ns
    0-PPE-1 : default APPFW APPFW_XML_cross-site scripting 1154 0 :
    10.217.253.69 3466-PPE1 - owa_profile http://10.217.31.101/FFC/login
    .html Cross-site script check failed for field script=”Bad tag:
    script” <\*\*blocked\*\*>
<!--NeedCopy-->
```

Beispiel für eine XML-Cross-Site Scripting Sicherheitsüberprüfungsprotokollnachricht im CEF-Protokollformat mit<not blocked> Aktion

```
Oct  7 01:46:52 <local0.warn> 10.217.31.98 CEF:0|Citrix|Citrix ADC|NS11
    .0|APPFW|APPFW_XML_cross-site scripting|4|src=10.217.30.17
    geolocation=Unknown spt=33141 method=GET request=http://
    10.217.31.101/FFC/login.html msg=Cross-site script check failed for
    field script=”Bad tag: script” cn1=1607 cn2=3538 cs1=owa_profile cs2
    =PPE0 cs4=ERROR cs5=2015 act=\*\*not blocked\*\*
<!--NeedCopy-->
```

So greifen Sie mit der GUI auf die Protokollmeldungen zu

Die Citrix GUI enthält ein nützliches Tool (**Syslog Viewer**) zum Analysieren der Protokollmeldungen. Sie haben mehrere Optionen für den Zugriff auf den Syslog Viewer:

- Navigieren Sie zu **Web App Firewall** > **Profile**, wählen Sie das Zielprofil aus, und klicken Sie auf **Sicherheitsprüfungen** . Markieren Sie die Zeile **XML Cross-Site Scripting,** und klicken Sie auf **Protokolle** . Wenn Sie direkt über die XML Cross-Site Scripting Prüfung des Profils auf die Protokolle zugreifen, filtert die GUI die Protokollmeldungen aus und zeigt nur die Protokolle an, die diese Sicherheitsüberprüfungsverletzungen betreffen.
- Sie können auch auf den Syslog Viewer zugreifen, indem Sie zu **Citrix ADC** > **System** > **Auditing** navigieren. Klicken Sie im Abschnitt Audit-Meldungen auf den Link Syslog-Nachrichten, um den Syslog-Viewer anzuzeigen, der alle Protokollmeldungen einschließlich anderer Protokolle für Sicherheitsüberprüfungen anzeigt. Dies ist nützlich für das Debuggen, wenn während der Anforderungsverarbeitung mehrere Sicherheitsüberprüfungsverletzungen ausgelöst werden können.
- Navigieren Sie zu **Web App Firewall** > **Richtlinien** > **Überwachung** . Klicken Sie im Abschnitt **Überwachungsmeldungen** auf den Link **Syslog-Nachrichten**, um den Syslog Viewer anzuzeigen, der alle Protokollmeldungen einschließlich anderer Protokolle gegen Sicherheitsüberprüfungen anzeigt.

Der XML-basierte Syslog Viewer bietet verschiedene Filteroptionen, um nur die Protokollmeldungen auszuwählen, die für Sie von Interesse sind. Um Protokollmeldungen für die **XML Cross-Site**

Scripting Prüfung auszuwählen, filtern Sie, indem Sie **APPFW** in den Dropdown-Optionen für **Modul** auswählen. Die Liste **Ereignistyp** bietet eine Reihe von Optionen, um Ihre Auswahl weiter zu verfeinern. Wenn Sie beispielsweise das Kontrollkästchen **AppFW_XML_Cross-Site Scripting** aktivieren und auf die Schaltfläche **Übernehmen** klicken, werden im Syslog Viewer nur Protokollnachrichten zu den Verletzungen der XML Cross-Site Scripting-Sicherheitsprüfung angezeigt.

Wenn Sie den Cursor in die Zeile für eine bestimmte Protokollnachricht stellen, werden unter der Protokollmeldung mehrere Optionen wie **Modul**, **Ereignistyp**, **Ereignis-ID**, **Client-IP** usw. angezeigt. Sie können eine dieser Optionen auswählen, um die entsprechenden Informationen in der Protokollmeldung hervorzuheben.

Statistiken für die siteübergreifenden XML-Skriptverstöße

Wenn die Aktion Statistik aktiviert ist, wird der Zähler für die XML Cross-Site Scripting Prüfung erhöht, wenn die Web App Firewall eine Aktion für diese Sicherheitsprüfung durchführt. Die Statistiken werden für Rate und Gesamtanzahl für Traffic, Verletzungen und Protokolle gesammelt. Die Größe eines Inkrements des Protokollzählers kann abhängig von den konfigurierten Einstellungen variieren. Wenn beispielsweise die Blockaktion aktiviert ist, erhöht eine Anforderung für eine Seite, die drei XML Cross-Site Scripting Verletzungen enthält, den Statistikindikator um eins, da die Seite blockiert wird, sobald die erste Verletzung erkannt wird. Wenn der Block jedoch deaktiviert ist, erhöht die Verarbeitung derselben Anforderung den Statistikindikator für Verletzungen und Protokolle um drei, da jede Verletzung eine separate Protokollmeldung generiert.

So zeigen Sie XML Cross-Site Scripting Prüfstatistiken mit der Befehlszeile an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
> **sh appfw stats**
```

Verwenden Sie den folgenden Befehl, um Statistiken für ein bestimmtes Profil anzuzeigen:

```
> **stat appfw profile** <profile name>
```

So zeigen Sie XML Cross-Site Scripting Statistiken mit der GUI an

1. Navigieren Sie zu **System** > **Sicherheit** > **Web App Firewall** .
2. Greifen Sie im rechten Bereich auf den **Statistik-Link** zu.
3. Verwenden Sie die Bildlaufleiste, um die Statistiken über XML Cross-Site Scripting Verletzungen und Protokolle anzuzeigen. Die Statistiktabelle enthält Echtzeitdaten und wird alle 7 Sekunden aktualisiert.

XML-SQL-Injectionsprüfung

December 7, 2021

Die XML-SQL-Injectionsprüfung untersucht die Benutzeranforderungen auf mögliche XML-SQL-Injection-Angriffe. Wenn es injizierte SQL in XML-Payloads findet, blockiert es die Anforderungen.

Ein XML-SQL-Angriff kann Quellcode in eine Webanwendung einspeisen, sodass er interpretiert und als gültige SQL-Abfrage ausgeführt werden kann, um einen Datenbankvorgang mit böswilliger Absicht durchzuführen. Beispielsweise können XML-SQL-Angriffe gestartet werden, um unbefugten Zugriff auf den Inhalt einer Datenbank zu erhalten oder die gespeicherten Daten zu manipulieren. XML SQL Injection-Angriffe sind nicht nur häufig, sondern können auch sehr schädlich und teuer sein.

Das Eingrenzen der Berechtigungen der Datenbankbenutzer kann dazu beitragen, die Datenbank zu einem gewissen Grad zu schützen. Alle Datenbankbenutzer müssen nur die erforderlichen Berechtigungen erhalten, um ihre beabsichtigten Aufgaben abzuschließen, damit sie keine SQL-Abfragen ausführen können, um andere Aufgaben auszuführen. Beispielsweise darf ein schreibgeschützter Benutzer keine Datentabellen schreiben oder manipulieren dürfen. Die Web App Firewall XML SQL Injection Prüfung überprüft alle XML-Anforderungen, um spezielle Abwehrmaßnahmen gegen die Einschleusung von nicht autorisiertem SQL-Code zu bieten, der die Sicherheit unterbrechen könnte. Wenn die Web App Firewall nicht autorisierten SQL-Code in einer XML-Anforderung eines Benutzers erkennt, kann sie die Anforderung blockieren.

Die Citrix Web App Firewall überprüft das Vorhandensein von SQL-Schlüsselwörtern und Sonderzeichen, um den XML SQL Injection-Angriff zu identifizieren. Ein Standardsatz von Schlüsselwörtern und Sonderzeichen enthält bekannte Schlüsselwörter und Sonderzeichen, die häufig zum Starten von XML-SQL-Angriffen verwendet werden. Die Web App Firewall betrachtet drei Zeichen, einfaches gerades Anführungszeichen (‘), umgekehrter Schrägstrich () und Semikolon (;) als Sonderzeichen für die SQL-Sicherheitsprüfung. Sie können neue Muster hinzufügen und den Standardsatz bearbeiten, um die XML-SQL-Prüfung anzupassen.

Die Web App Firewall bietet verschiedene Aktionsoptionen für die Implementierung von XML SQL Injection-Schutz. Sie können die Anfrage **blockieren**, eine Nachricht in der Datei ns.log mit Details zu den beobachteten Verstößen **protokollieren** und **Statistiken** sammeln, um die Anzahl der beobachteten Angriffe zu verfolgen.

Zusätzlich zu Aktionen gibt es mehrere Parameter, die für die XML-SQL-Injectionsverarbeitung konfiguriert werden können. Sie können nach **SQL-Platzhalterzeichen**suchen. Sie können den XML SQL Injection-Typ ändern und eine der 4 Optionen auswählen (**SQLKeyword**, **SQLSplchar**, **SQLSplCharandKeyword**, **SQLSplCharorKeyword**), um anzugeben, wie die SQL-Schlüsselwörter und SQL-Sonderzeichen bei der Verarbeitung der XML Nutzlast. Mit dem Parameter XML **SQL Comments Handling** können Sie den Typ der Kommentare angeben, die während der XML SQL Injection-Erkennung überprüft oder ausgenommen werden müssen.

Sie können Entspannungen bereitstellen, um Fehlalarme zu vermeiden. Die XML-SQL-Prüfung der Web App Firewall wird für die Nutzlast der eingehenden Anforderungen durchgeführt, und Angriffszeichenfolgen werden identifiziert, selbst wenn sie über mehrere Zeilen verteilt sind. Die Prüfung sucht

nach SQL-Injection-Strings im **Element** und den **Attributwerten**. Sie können Entspannungen anwenden, um die Sicherheitskontrolle unter bestimmten Bedingungen zu umgehen. Die Protokolle und Statistiken können Ihnen helfen, benötigte Entspannungen zu identifizieren.

Aktionsoptionen

Eine Aktion wird angewendet, wenn die XML-SQL-Injection-Prüfung eine SQL-Injection-Angriffszeichenfolge in der Anforderung erkennt. Die folgenden Aktionen sind verfügbar, um einen optimierten XML SQL Injection-Schutz für Ihre Anwendung zu konfigurieren:

Block— Wenn Sie Block aktivieren, wird die Blockaktion nur ausgelöst, wenn die Eingabe mit der XML-SQL-Injectionstypspezifikation übereinstimmt. Wenn beispielsweise **SQLSplCharAndKeyword** als XML-SQL-Injectionstyp konfiguriert ist, wird eine Anforderung nicht blockiert, wenn sie keine Schlüsselwörter enthält, selbst wenn SQL-Sonderzeichen in der Nutzlast erkannt werden. Eine solche Anforderung wird blockiert, wenn der XML-SQL-Injectionstyp auf **SQLSplchar**oder **SQLSplCharorKeyword**festgelegt ist.

Log— Wenn Sie die Protokollfunktion aktivieren, generiert die XML-SQL-Injection-Prüfung Protokollmeldungen, die die ausgeführten Aktionen angeben. Wenn der Block deaktiviert ist, wird für jeden Speicherort (**ELEMENT**, **ATTRIBUTE**), an dem die XML-SQL-Verletzung erkannt wurde, eine separate Protokollmeldung generiert. Allerdings wird nur eine Nachricht generiert, wenn die Anforderung blockiert wird. Sie können die Protokolle überwachen, um festzustellen, ob Antworten auf legitime Anfragen blockiert werden. Eine große Zunahme der Anzahl von Protokollmeldungen kann auf Versuche hinweisen, einen Angriff zu starten.

Statistiken— Wenn diese Option aktiviert ist, sammelt die Statistikfunktion Statistiken über Verstöße und Protokolle. Ein unerwarteter Anstieg im Statistikzähler deutet möglicherweise darauf hin, dass Ihre Anwendung angegriffen wird. Wenn legitime Anfragen blockiert werden, müssen Sie möglicherweise die Konfiguration erneut besuchen, um zu sehen, ob Sie neue Relaxationsregeln konfigurieren oder die vorhandenen ändern müssen.

XML-SQL-Parameter

Zusätzlich zu den Block-, Protokoll- und Statistikaktionen können Sie die folgenden Parameter für die XML SQL Injection-Prüfung konfigurieren:

Suche nach XML SQL-Platzhalterzeichen — Wildcard-Zeichenkönnen verwendet werden, um die Auswahl einer SQL-SELECT-Anweisung (Structured Query Language) zu erweitern. Diese Wildcard-Operatoren können in Verbindung mit den Operatoren **LIKE** und **NOT LIKE** verwendet werden, um einen Wert mit ähnlichen Werten zu vergleichen. Die Prozentzeichen (%) und Unterstriche (_) werden häufig als Platzhalter verwendet. Das Prozentzeichen entspricht dem Sternchen (*) -Platzhalterzeichen, das mit MS-DOS verwendet wird, und um Null, ein oder mehrere Zeichen in

einem Feld abzugleichen. Der Unterstrich ähnelt dem MS-DOS-Fragezeichen (?) Platzhalterzeichen. Es entspricht einer einzelnen Zahl oder einem Zeichen in einem Ausdruck.

Sie können beispielsweise die folgende Abfrage verwenden, um eine Zeichenfolgensuche durchzuführen, um alle Kunden zu suchen, deren Namen das D-Zeichen enthalten.

```
SELECT * from customer WHERE name like "%D%"
```

Im folgenden Beispiel werden die Operatoren kombiniert, um Gehaltswerte zu finden, die 0 als zweites und drittes Zeichen haben.

```
SELECT * from customer WHERE salary like '_00%
```

Verschiedene DBMS-Anbieter haben die Platzhalterzeichen durch Hinzufügen zusätzlicher Operatoren erweitert. Die Citrix Web App Firewall kann vor Angriffen schützen, die durch das Eingeben dieser Platzhalterzeichen gestartet werden. Die 5 Standardplatzhalterzeichen sind Prozent (%), Unterstrich (_), Caret (^), öffnende eckige Klammer ([) und schließende eckige Klammer (]). Dieser Schutz gilt sowohl für HTML- als auch für XML-Profile.

Die Standard-Platzhalterzeichen sind eine Liste von Literalen, die in der ***Standardsignaturen angegeben sind**:

```
1 -  <wildchar type=" LITERAL" >%</wildchar>
2 -  <wildchar type=" LITERAL" >_</wildchar>
3 -  <wildchar type=" LITERAL" >^</wildchar>
4 -  <wildchar type=" LITERAL" >[</wildchar>
5 -  <wildchar type=" LITERAL" >]</wildchar>
6 <!--NeedCopy-->
```

Platzhalterzeichen in einem Angriff können PCRE sein, wie [^A-F]. Die Web App Firewall unterstützt auch PCRE-Platzhalter, aber die obigen Platzhalterzeichen reichen aus, um die meisten Angriffe zu blockieren.

> **Hinweis:**
>
> Die **XML-SQL-Platzhalterzeichenprüfung** unterscheidet sich von der **XML-SQL-Sonderzeichenprüfung**. Diese Option muss mit Vorsicht verwendet werden, um Falschmeldungen zu vermeiden.

Prüfanforderung mit SQL Injection Type— Die Web App Firewall bietet 4 Optionen, um die gewünschte Strenge für die SQL Injection-Inspektion zu implementieren, basierend auf den individuellen Anforderungen der Anwendung. Die Anforderung wird anhand der Einschleusungstypspezifikation zum Erkennen von SQL-Verletzungen überprüft. Die 4 SQL-Injection-Typ-Optionen sind:

- **SQL-Sonderzeichen und Schlüsselwort**—Sowohl ein SQL-Schlüsselwort als auch ein SQL-Sonderzeichen müssen am geprüften Speicherort vorhanden sein, um eine SQL-Verletzung auszulösen. Diese am wenigsten einschränkende Einstellung ist auch die Standardeinstellung.

- **SQL-Sonderzeichen**—Mindestens eines der Sonderzeichen muss in der verarbeiteten Nutzlastzeichenfolge vorhanden sein, um eine SQL-Verletzung auszulösen.
- **SQL-Schlüsselwort**—Mindestens eines der angegebenen SQL-Schlüsselwörter muss in der verarbeiteten Nutzlastzeichenfolge vorhanden sein, um eine SQL-Verletzung auszulösen. Wählen Sie diese Option nicht ohne Berücksichtigung. Um Fehlalarme zu vermeiden, stellen Sie sicher, dass keines der Schlüsselwörter in den Eingaben erwartet wird.
- **SQL-Sonderzeichen oder Schlüsselwort**—Entweder das Schlüsselwort oder die Sonderzeichenfolge muss in der Nutzlast vorhanden sein, um die Sicherheitsüberprüfungsverletzung auszulösen.

> **Tipp**
>
> Wenn Sie die Option SQL-Sonderzeichen auswählen, überspringt die Web App Firewall Zeichenfolgen, die keine Sonderzeichen enthalten. Da die meisten SQL-Server keine SQL-Befehle verarbeiten, denen kein Sonderzeichen vorausgeht, kann die Aktivierung dieser Option die Belastung der Web App Firewall erheblich reduzieren und die Verarbeitung beschleunigen, ohne Ihre geschützten Websites zu gefährden.

SQL-Kommentarbehandlung— Standardmäßig analysiert und überprüft die Web App Firewall alle Kommentare in XML-Daten auf injizierte SQL-Befehle. Viele SQL-Server ignorieren alles in einem Kommentar, selbst wenn ein SQL-Sonderzeichen vorangestellt ist. Wenn Ihr XML-SQL-Server Kommentare ignoriert, können Sie die Web App Firewall so konfigurieren, dass Kommentare beim Überprüfen von Anforderungen für injizierte SQL übersprungen werden. Die Optionen zur Verarbeitung von XML SQL-Kommentaren sind:

- **ANSI**—Überspringen Sie SQL-Kommentare im ANSI-Format, die normalerweise von UNIX-basierten SQL-Datenbanken verwendet werden.
- **Verschachtelt**— Verschachtelte SQL-Kommentare überspringen, die normalerweise von Microsoft SQL Server verwendet werden.
- **ANSI/verschachtelt**—Überspringen Sie Kommentare, die sowohl den ANSI- als auch den verschachtelten SQL-Kommentarstandards entsprechen. Kommentare, die nur dem ANSI-Standard oder nur dem verschachtelten Standard entsprechen, werden weiterhin auf injizierte SQL überprüft.
- **Alle Kommentare prüfen**— Überprüfen Sie die gesamte Anforderung für injizierte SQL, ohne etwas zu überspringen. Dies ist die Standardeinstellung.

> **Tipp**
>
> In den meisten Fällen dürfen Sie die Option “Verschachtelt” oder “Ansi/verschachtelt” nicht wählen, es sei denn, Ihre Backend-Datenbank läuft auf Microsoft SQL Server. Die meisten anderen Typen von SQL Server-Software erkennen verschachtelte Kommentare nicht. Wenn verschachtelte Kommentare in einer Anforderung angezeigt werden, die an einen anderen SQL-Servertyp weitergeleitet wird, deutet dies möglicherweise auf einen Versuch hin, die

> Sicherheit auf diesem Server zu verletzen.

Entspannungsregeln

Wenn Ihre Anwendung erfordert, dass Sie die XML-SQL-Injection-Inspektion für ein bestimmtes ELEMENT oder ATTRIBUTE in der XML-Payload umgehen müssen, können Sie eine Relaxationsregel konfigurieren. Die Relaxationsregeln für XML SQL Injection Überprüfung weisen die folgenden Parameter auf:

- **Name:** Sie können Literalzeichenfolgen oder reguläre Ausdrücke verwenden, um den Namen des **ELEMENT** oder des **ATTRIBUTE** zu konfigurieren. Der folgende Ausdruck befreit alle **ELEMENTS**, die mit der Zeichenfolge **PurchaseOrder_** beginnen, gefolgt von einer Zeichenfolge mit mindestens zwei und höchstens zehn Zeichen lang sind:

  Kommentar: “Ausgenommen XML-SQL-Prüfung für Bestellelemente”

```
    XMLSQLInjection:  ”PurchaseOrder_[0-9A-Za-z]{
 2,10 }
 ”

    IsRegex:  REGEX          Location:  ELEMENT

    State:  ENABLED
<!--NeedCopy-->
```

Hinweis: Bei den Namen wird die Groß- und Kleinschreibung unterschieden. Doppelte Einträge sind nicht zulässig, aber Sie können die Großschreibung der Namen und Unterschiede in der Position verwenden, um ähnliche Einträge zu erstellen. Zum Beispiel ist jede der folgenden Entspannungsregeln einzigartig:

```
1)      XMLSQLInjection:  XYZ    IsRegex:  NOTREGEX

        Location:  ELEMENT       State:  ENABLED

2)      XMLSQLInjection:  xyz    IsRegex:  NOTREGEX

        Location:  ELEMENT       State:  ENABLED

3)      XMLSQLInjection:  xyz    IsRegex:  NOTREGEX

        Location:  ATTRIBUTE     State:  ENABLED

```



```
4)      XMLSQLInjection:  XYZ    IsRegex:  NOTREGEX

        Location:  ATTRIBUTE     State:  ENABLED
<!--NeedCopy-->
```

- **Speicherort**: Sie können den Speicherort der XML-SQL-Inspektionsausnahme in Ihrer XML-Nutzlast angeben. Die Option **ELEMENT** ist standardmäßig ausgewählt. Sie können es in **ATTRIBUTE**ändern.
- **Kommentar**: Dies ist ein optionales Feld. Sie können bis zu 255 Zeichen verwenden, um den Zweck dieser Relaxationsregel zu beschreiben.

> **Warnung**
>
> Reguläre Ausdrücke sind leistungsstark. Vor allem, wenn Sie mit regulären Ausdrücken im PCRE-Format nicht vertraut sind, überprüfen Sie alle regulären Ausdrücke, die Sie schreiben. Stellen Sie sicher, dass sie genau den Namen definieren, den Sie als Ausnahme hinzufügen möchten, und nichts anderes. Die unvorsichtige Verwendung von regulären Ausdrücken kann Ergebnisse haben, die Sie nicht möchten, z. B. das Blockieren des Zugriffs auf Webinhalte, die Sie nicht blockieren wollten, oder das Zulassen eines Angriffs, den die XML-SQL-Injection-Inspektion sonst blockiert hätte.

Verwenden der Befehlszeile zum Konfigurieren der XML SQL Injection Check

So konfigurieren Sie XML SQL Injection-Aktionen und andere Parameter mit der Befehlszeile:

In der Befehlszeilenschnittstelle können Sie entweder den Befehl **set appfw profile** oder den Befehl **add appfw profile** verwenden, um den XML SQL Injection-Schutz zu konfigurieren. Sie können die Block-, Protokoll- und Statistikaktionen aktivieren. Wählen Sie den Typ des SQL-Angriffsmusters (Schlüsselwörter, Platzhalterzeichen, Sonderzeichenfolgen) aus, den Sie in den Nutzlasten erkennen möchten. Verwenden Sie den Befehl **unset appfw profile**, um die konfigurierten Einstellungen wieder auf ihre Standardwerte zurückzusetzen. Jeder der folgenden Befehle legt nur einen Parameter fest, aber Sie können mehrere Parameter in einen einzelnen Befehl aufnehmen:

- `set appfw profile <name> **-XMLSQLInjectionAction** ([block] [log] [stats])| [none])`
- `set appfw profile <name> -XMLSQLInjectionCheckSQLWildChars (ON |OFF)`
- `set appfw profile <name> -XMLSQLInjectionType ([SQLKeyword] | [SQLSplChar] | [SQLSplCharANDKeyword] | [SQLSplCharORKeyword])`
- `set appfw profile <name> -XMLSQLInjectionParseComments ([checkall] | [ansi|nested] | [ansinested])`

So konfigurieren Sie eine SQL Injection-Relaxationsregel mit der Befehlszeile

Verwenden Sie den Befehl bind oder unbind, um Relaxationsregeln wie folgt hinzuzufügen oder zu löschen:

```
- bind appfw profile <name> -XMLSQLInjection <string> [isRegex (REGEX | NOTREGEX)] [-location ( ELEMENT | ATTRIBUTE )] -comment <string> [-state ( ENABLED | DISABLED )]
- unbind appfw profile <name> -XMLSQLInjection <String>
<!--NeedCopy-->
```

Beispiel:

```
> bind appfw profile test_profile -XMLSQLInjection "PurchaseOrder_[0-9A-Za-z]{
 2,15 }
 " -isregex REGEX -location ATTRIBUTE

> unbind appfw profile test_profile -XMLSQLInjection "PurchaseOrder_[0-9A-Za-z]{
 2,15 }
 " -location ATTRIBUTE
<!--NeedCopy-->
```

Verwenden der GUI zum Konfigurieren der XMLSQL-Injectionssicherheitsprüfung

In der GUI können Sie die Sicherheitsprüfung für XML SQL Injection im Bereich für das Profil konfigurieren, das Ihrer Anwendung zugeordnet ist.

So konfigurieren oder ändern Sie die XML-SQL-Injection-Prüfung mit der GUI

1. Navigieren Sie zu **Web App Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich Erweiterte Einstellungen auf **Sicherheitsprüfungen**.

In der Tabelle Sicherheitsprüfung werden die aktuell konfigurierten Aktionseinstellungen für alle Sicherheitsprüfungen angezeigt. Sie haben 2 Optionen für die Konfiguration:

a. Wenn Sie nur Block-, Protokoll- und Statistikaktionen für XML-SQL-Injection aktivieren oder deaktivieren möchten, können Sie die Kontrollkästchen in der Tabelle aktivieren oder deaktivieren, klicken Sie auf OK, und klicken Sie dann auf Speichern und Schließen, um den Sicherheitsüberprüfungsbereich zu schließen.

b. Wenn Sie zusätzliche Optionen für diese Sicherheitsprüfung konfigurieren möchten, doppelklicken Sie auf XML SQL Injection, oder wählen Sie die Zeile aus und klicken Sie auf **Aktionseinstellungen**, um die folgenden Optionen anzuzeigen:

Nach SQL-Platzhalterzeichen suchen— Betrachten Sie SQL-Platzhalterzeichen in der Nutzlast als Angriffsmuster.

Überprüfen Sie die Anforderung mit—Type der SQL-Einschleusung (SqlKeyword, SqlSplChar, SqlSplcharandKeyword oder SqlSplcharorKeyword), die überprüft werden soll.

SQL Comments Handling— Art der zu prüfenden Kommentare (Alle Kommentare überprüfen, ANSI, verschachtelte oder ANSI/verschachtelte Kommentare).

Nachdem Sie eine der oben genannten Einstellungen geändert haben, klicken Sie auf **OK**, um die Änderungen zu speichern und zur Tabelle Sicherheitsprüfungen zurückzukehren. Sie können bei Bedarf weitere Sicherheitsprüfungen konfigurieren. Klicken Sie auf **OK**, um alle Änderungen zu speichern, die Sie im Abschnitt Sicherheitsüberprüfungen vorgenommen haben, und klicken Sie dann auf **Speichern** und **schließen**, um den Bereich Sicherheitsprüfung zu schließen.

So konfigurieren Sie eine XML SQL Injection-Relaxationsregel mit der GUI

1. Navigieren Sie zu **Web App Firewall** > **Profile**, markieren Sie das Zielprofil und klicken Sie auf **Bearbeiten**.
2. Klicken Sie im Bereich **Erweiterte Einstellungen** auf **Relaxationsregeln**.
3. Doppelklicken Sie in der Tabelle Relaxationsregeln auf den Eintrag **XML SQL Injection**, oder wählen Sie ihn aus, und klicken Sie auf **Bearbeiten** .
4. Führen Sie im Dialogfeld **XML-SQL-Injection-Relaxationsregeln** die Vorgänge **Hinzufügen**, **Bearbeiten**, **Löschen**, **Aktivieren** oder **Deaktivieren** für Relaxationsregeln aus.

So verwalten Sie XML SQL Injection-Relaxationsregeln mithilfe des Visualizers

Um eine konsolidierte Ansicht aller Relaxationsregeln zu erhalten, können Sie die Zeile **XML SQL Injection** in der Tabelle Relaxationsregeln markieren und auf **Visualizer** klicken. Der Visualizer für bereitgestellte Relaxationen bietet Ihnen die Möglichkeit, eine neue Regel **hinzuzufügen** oder eine vorhandene zu **bearbeiten**. Sie können auch eine Gruppe von Regeln **aktivieren** oder **deaktivieren**, indem Sie einen Knoten auswählen und auf die entsprechenden Schaltflächen im Relaxationsvisualizer klicken.

So zeigen Sie die SQL Injection-Muster mit der GUI an oder passen Sie sie an:

Sie können die GUI verwenden, um die SQL-Muster anzuzeigen oder anzupassen.

Die Standard-SQL-Muster werden unter **Web App Firewall** > **Signaturen** > ***Standardsignaturen angegeben**. Wenn Sie kein Signaturobjekt an Ihr Profil binden, werden die im Default Signatures -Objekt angegebenen Standard-SQL-Muster vom Profil für die Verarbeitung von XML SQL Injection Sicherheitsprüfung verwendet. Die Regeln und Muster im Default Signatures -Objekt

sind schreibgeschützt. Sie können sie nicht bearbeiten oder ändern. Wenn Sie diese Muster ändern oder ändern möchten, erstellen Sie ein benutzerdefiniertes Signaturobjekt, indem Sie eine Kopie des Standardsignatur-Objekts erstellen und die SQL-Muster ändern. Verwenden Sie das benutzerdefinierte Signaturobjekt in dem Profil, das den Datenverkehr verarbeitet, für den Sie diese benutzerdefinierten SQL-Muster verwenden möchten.

Weitere Informationen finden Sie unter Signaturen.

So zeigen Sie SQL-Standardmuster an:

a. Navigieren Sie zu **Web App Firewall** > **Signaturen**, wählen Sie ***Standardsignaturen aus**, und klicken Sie auf **Bearbeiten** . Klicken Sie dann auf **SQL/Cross-Site Scripting Pattern verwalten**.

Die Tabelle SQL/Cross-Site Scripting Paths verwalten zeigt die folgenden vier Zeilen in Bezug auf SQL Injection:

```
Injection (not_alphanum, SQL)/ Keyword

Injection (not_alphanum, SQL)/ specialstring

Injection (not_alphanum, SQL)/ transformrules/transform

Injection (not_alphanum, SQL)/ wildchar
<!--NeedCopy-->
```

b. Wählen Sie eine Zeile aus, und klicken Sie auf **Elemente verwalten**, um die entsprechenden SQL-Muster (Schlüsselwörter, spezielle Zeichenfolgen, Transformationsregeln oder Platzhalterzeichen) anzuzeigen, die von der SQL Injection Check der Web App Firewall verwendet werden.

So passen Sie SQL-Muster an: Sie können ein benutzerdefiniertes Signaturobjekt bearbeiten, um die SQL-Schlüsselwörter, Sonderzeichenfolgen und Platzhalterzeichen anzupassen. Sie können neue Einträge hinzufügen oder vorhandene entfernen. Sie können die Transformationsregeln für die SQL-Spezialzeichenfolgen ändern.

a. Navigieren Sie zu **Web App Firewall** > **Signaturen**, markieren Sie die benutzerdefinierte Zielsignatur und klicken Sie auf **Bearbeiten**. Klicken Sie auf **SQL/Cross-Site-Skriptmuster verwalten, um die Tabelle SQL/Cross-Site-Scripting-Pfade** verwalten anzuzeigen.

b. Wählen Sie die SQL-Zielzeile aus.

i. Klicken Sie auf **Elemente verwalten**, um das entsprechende SQL-Element **hinzuzufügen**, zu **bearbeiten**oder **zu entfernen**.

ii. Klicken Sie auf **Entfernen**, um die ausgewählte Zeile zu entfernen.

> **Warnung**
>
> Sie müssen sehr vorsichtig sein, wenn Sie ein Standard-SQL-Element entfernen oder ändern oder den SQL-Pfad löschen, um die gesamte Zeile zu entfernen. Die Signaturregeln sowie die Sicherheitsprüfung von XML SQL Injection basieren auf diesen Elementen, um SQL Injection-Angriffe zu erkennen, um Ihre Anwendungen zu schützen. Das Anpassen der SQL-Muster kann Ihre Anwendung anfällig für XML-SQL-Angriffe machen, wenn das erforderliche Muster während der Bearbeitung entfernt wird.

Verwenden der Protokollfunktion mit der XML-SQL-Injectionsprüfung

Wenn die Protokollaktion aktiviert ist, werden die **XML SQL Injection** Sicherheitsüberprüfungsverletzungen im Überwachungsprotokoll als **APPFW_XML_SQL-Verletzungen** protokolliert. Die Web App Firewall unterstützt sowohl native als auch CEF-Protokollformate. Sie können die Protokolle auch an einen entfernten Syslog-Server senden.

So greifen Sie über die Befehlszeile auf die Protokollmeldungenzu:

Wechseln Sie zur Shell und ziehen Sie die ns.logs im Ordner /var/log/, um auf die Protokollmeldungen zu den XML-Cross-Site Scripting Verletzungen zuzugreifen:

```
1 > Shell
2
3 > tail -f /var/log/ns.log | grep APPFW_XML_SQL
4 <!--NeedCopy-->
```

So greifen Sie mit der GUI auf die Protokollmeldungen zu

Die Citrix GUI enthält ein nützliches Tool (Syslog Viewer) zum Analysieren der Protokollmeldungen. Sie haben mehrere Optionen für den Zugriff auf den Syslog Viewer:

- Navigieren Sie zu **Web App Firewall** > **Profile**, wählen Sie das Zielprofil aus, und klicken Sie auf **Sicherheitsprüfungen** . Markieren Sie die Zeile **XML SQL Injection**, und klicken Sie auf **Protokolle** . Wenn Sie direkt über die XML SQL Injection-Prüfung des Profils auf die Protokolle zugreifen, filtert die GUI die Protokollmeldungen aus und zeigt nur die Protokolle an, die diese Sicherheitsüberprüfungsverletzungen betreffen.
- Sie können auch auf den Syslog Viewer zugreifen, indem Sie zu **System** > **Auditing navigieren** . Klicken Sie im Abschnitt Audit-Meldungen auf den Link **Syslog-Nachrichten**, um den Syslog-Viewer anzuzeigen, der alle Protokollmeldungen einschließlich anderer Protokolle für Sicherheitsüberprüfungen anzeigt. Dies ist nützlich für das Debuggen, wenn während der Anforderungsverarbeitung mehrere Sicherheitsüberprüfungsverletzungen ausgelöst werden können.

- Navigieren Sie zu **Web App Firewall** > **Richtlinien** > **Überwachung** . Klicken Sie im Abschnitt Überwachungsmeldungen auf den Link **Syslog-Nachrichten**, um den **Syslog Viewer**anzuzeigen, der alle Protokollmeldungen einschließlich anderer Protokolle gegen Sicherheitsüberprüfungen anzeigt.

Der XML-basierte Syslog Viewer bietet verschiedene Filteroptionen, um nur die Protokollmeldungen auszuwählen, die für Sie von Interesse sind. Um Protokollmeldungen für die **XML-SQL-Injection-Prüfung** auszuwählen, filtern Sie, indem Sie **APPFW** in den Dropdown-Optionen für **Modul** auswählen. Die Liste **Ereignistyp** bietet eine Reihe von Optionen, um Ihre Auswahl weiter zu verfeinern. Wenn Sie beispielsweise das Kontrollkästchen **APPFW_XML_SQL** aktivieren und auf die Schaltfläche **Übernehmen** klicken, werden im Syslog-Viewer nur Protokollmeldungen angezeigt, die sich auf die Sicherheitsüberprüfungsverletzungen von **XML SQL Injection** beziehen.

Wenn Sie den Cursor in der Zeile für eine bestimmte Protokollmeldung platzieren, werden unter der Protokollmeldung mehrere Optionen angezeigt, z. B. **Modul**, **Ereignistyp**, **Ereignis-ID**und **Client-IP**. Sie können eine dieser Optionen auswählen, um die entsprechenden Informationen in der Protokollmeldung hervorzuheben.

Statistiken für die XML-SQL-Injectionsverletzungen

Wenn die Aktion Statistik aktiviert ist, wird der Zähler für die **XML-SQL-Injection-Prüfung** erhöht, wenn die Web App Firewall eine Aktion für diese Sicherheitsprüfung ausführt. Die Statistiken werden für Rate und Gesamtanzahl für Traffic, Verletzungen und Protokolle gesammelt. Die Größe eines Inkrements des Protokollzählers kann abhängig von den konfigurierten Einstellungen variieren. Wenn beispielsweise die Blockaktion aktiviert ist, erhöht eine Anforderung für eine Seite, die drei **XML-SQL-Injection-Verletzungen** enthält, den Statistikindikator um eins, da die Seite blockiert wird, sobald die erste Verletzung erkannt wird. Wenn der Block jedoch deaktiviert ist, erhöht die Verarbeitung derselben Anforderung den Statistikindikator für Verletzungen und Protokolle um drei, da jede Verletzung eine separate Protokollmeldung generiert.

So zeigen Sie XML-SQL-Injection-Prüfstatistiken mit der Befehlszeile an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
> sh appfw stats
```

Verwenden Sie den folgenden Befehl, um Statistiken für ein bestimmtes Profil anzuzeigen:

```
> stat appfw profile <profile name>
```

So zeigen Sie XML-SQL-Injection-Statistiken mit der GUI an

1. Navigieren Sie zu **System** > **Sicherheit** > **Web App Firewall** .
2. Greifen Sie im rechten Bereich auf den **Statistik-Link** zu.

3. Verwenden Sie die Bildlaufleiste, um die Statistiken über **XML-SQL-Injection-Verletzungen** und -Protokolle anzuzeigen. Die Statistiktabelle enthält Echtzeitdaten und wird alle 7 Sekunden aktualisiert.

XML-Anlagenprüfung

October 5, 2021

Die XML-Anlagenprüfung prüft eingehende Anforderungen auf schädliche Anlagen und blockiert die Anforderungen, die Anlagen enthalten, die die Anwendungssicherheit verletzen könnten. Der Zweck der Überprüfung von XML-Anlagen besteht darin, zu verhindern, dass Angreifer eine XML-Anlage verwenden, um die Sicherheit auf Ihrem Server zu verletzen.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld XML-Anhang ändern auf der Registerkarte Allgemein die Aktionen Blockieren, Lernen, Protokollieren, Statistiken und Lernen aktivieren oder deaktivieren:

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um die XML-Anlagenprüfung zu konfigurieren:

- `set appfw profile <name> -xmlAttachmentAction [block] [learn] [log] [stats] [none]`

Sie müssen die anderen Einstellungen für die Überprüfung der XML-Anlagen in der Benutzeroberfläche konfigurieren. Im Dialogfeld `Modify XML Attachment` Prüfen können Sie auf der Registerkarte Prüfen die folgenden Einstellungen konfigurieren:

- **Maximale Anlagengröße.** Zulassen von Anlagen, die nicht größer als die von Ihnen angegebene maximale Anlagengröße sind. Um diese Option zu aktivieren, aktivieren Sie zuerst das Kontrollkästchen Aktiviert, und geben Sie dann die maximale Anlagengröße in Byte in das`Size` Textfeld ein.
- **Anlageninhaltstyp.** Anhänge des angegebenen Inhaltstyps zulassen. Aktivieren Sie zum Aktivieren dieser Option zuerst das Kontrollkästchen Aktiviert, und geben Sie dann einen regulären Ausdruck ein, der dem Content-Type-Attribut der Anlagen entspricht, die Sie zulassen möchten.
  - Sie können den URL-Ausdruck direkt in das Textfenster eingeben. In diesem Fall können Sie über das`Regex Tokens` Menü eine Reihe nützlicher regulärer Ausdrücke am Cursor eingeben, anstatt sie manuell einzugeben.
  - Sie können auf Regex-Editor klicken, um das`Add Regular Expression` Dialogfeld zu öffnen und es zum Erstellen des URL-Ausdrucks zu verwenden.

Interoperabilitätsprüfung von Webdiensten

October 5, 2021

Bei der WS-I-Prüfung (Web Services Interoperability) werden sowohl Anforderungen als auch Antworten auf die Einhaltung des WS-I-Standards untersucht und die Anforderungen und Antworten blockiert, die diesen Standard nicht erfüllen. Der Zweck der WS-I-Prüfung besteht darin, Anforderungen zu blockieren, die möglicherweise nicht mit anderen XML interagieren. Ein Angreifer kann Inkonsistenzen in der Interoperabilität verwenden, um einen Angriff auf Ihre XML-Anwendung zu starten.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld Interoperabilitätsprüfung für Webdienste ändern auf der Registerkarte Allgemein die Aktionen Blockieren, Protokollieren, Statistiken und Lernen aktivieren oder deaktivieren.

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um die Interoperabilitätsprüfung für Webdienste zu konfigurieren:

- `set appfw profile <name> -xmlWSIAction [block] ][log] [learn] [stats] [ none]`

Um einzelne Web Services Interoperabilitätsregeln zu konfigurieren, müssen Sie die GUI verwenden. Wählen Sie im Dialogfeld Interoperabilitätsprüfung für Webdienste auf der Registerkarte Prüfungen eine Regel aus, und klicken Sie auf Aktivieren oder Deaktivieren, um die Regel zu aktivieren oder zu deaktivieren. Sie können auch auf Öffnen klicken, um das Meldungsfeld Webdienst-Interoperabilitätsdetails für diese Regel zu öffnen. Im Meldungsfeld werden schreibgeschützte Informationen zur Regel angezeigt. Sie können keine dieser Regeln ändern oder andere Konfigurationsänderungen vornehmen.

Bei der WS-I-Prüfung werden die in WS-I Basic Profile 1.0 aufgeführten Regeln verwendet. WS-I bietet Best Practices für die Entwicklung interoperabler Web Services-Lösungen. WS-I-Prüfungen werden nur für SOAP-Nachrichten durchgeführt.

Eine Beschreibung der einzelnen WSI-Standardregeln finden Sie im Folgenden:

Regel	Beschreibung
BP1201	Der Nachrichtentext sollte ein soap:envelope mit Namespace sein.
R1000	Wenn ein ENVELOPE ein Fehler ist, darf das soap:Fault-Element NUR die untergeordneten Elemente faultcode, faultstring, faultactor und detail haben.

Regel	Beschreibung
R1001	Wenn ein ENVELOPE ein Fehler ist, müssen die untergeordneten Elemente des Elements SOAP:Fault nicht qualifiziert sein.
R1003	Ein RECEIVER MUSS Fehlermeldungen akzeptieren, die eine beliebige Anzahl qualifizierter oder nicht qualifizierter Attribute aufweisen, einschließlich Null, die auf dem Detailelement angezeigt werden. Der Namespace von qualifizierten Attributen kann alles andere als der Namespace des qualifizierten Dokumentelements Envelope sein.
R1004	Wenn ein ENVELOPE ein faultcode-Element enthält, muss der Inhalt dieses Elements entweder einer der in SOAP 1.1 definierten Fehlercodes sein (ggf. zusätzliche Informationen im Detailelement liefern) oder ein Qname, dessen Namespace durch die spezifizierende Autorität des Fehlers gesteuert wird (in dieser Reihenfolge der Präferenz).
R1005	Ein ENVEL MUSS NICHT SOAP:EncodingStyle-Attribut für eines der Elemente enthalten, deren Namespace dem Namespace des qualifizierten Dokumentelements Envelope entspricht.
R1006	Ein ENVELOPE darf NICHT soap:encodingStyle-Attribute für ein Element enthalten, das ein untergeordnetes Element von soap:Body ist.
R1007	Ein in einer rpc-literal-Bindung beschriebener ENVELOPE darf NICHT das soap:encodingStyle-Attribut für ein Element enthalten, das ein Enkelkind von soap:Body ist.
R1011	Ein ENVELOPE darf NICHT untergeordnete Elemente von soap:Envelope nach dem Element soap:Body haben.

Regel	Beschreibung
R1012	Eine MESSAGE MUSS als UTF-8 oder UTF-16 serialisiert werden.
R1013	Ein ENVELOPE, der ein soap:mustUnderstand-Attribut enthält, DARF nur die lexikalischen Formulare 0 und 1 verwenden.
R1014	Die untergeordneten Elemente des soap:Body-Elements in einem ENVELOPE müssen namespace-qualifiziert sein.
R1015	Ein RECEIVER MUSS einen Fehler erzeugen, wenn ein Envelope auftritt, dessen Dokumentelement nicht SOAP:Envelope ist.
R1031	Wenn ein ENVELOPE ein faultcode-Element enthält, darf der Inhalt dieses Elements NICHT die SOAP 1.1-Punktnotation verwenden, um die Bedeutung des Fehlers zu verfeinern.
R1032	Die Elemente soap:Envelope, soap:Header und soap:Body in einem ENVELOPE dürfen NICHT Attribute im gleichen Namespace wie das des qualifizierten Dokumentelements Envelope haben
R1033	Ein ENVELOPE sollte NICHT die Namespace-Deklaration enthalten: `xmlns:xml=http://www.w3.org/XML/1998/namespace.`
R1109	Der Wert des SOAPAction HTTP-Header-Feldes in einer HTTP-Anforderung MESSAGE MUSS eine Zeichenfolge in Anführungszeichen sein.
R1111	Eine INSTANCE SOLL einen 200-OK-HTTP-Statuscode für eine Antwortnachricht verwenden, die einen Envelope enthält, der kein Fehler ist.
R1126	Eine INSTANCE MUSS einen HTTP-Statuscode 500 Internal Server Error zurückgeben, wenn der Antwort-Envelope ein Fehler ist.

Regel	Beschreibung
R1132	Eine HTTP-Anforderung MESSAGE MUSS die HTTP POST-Methode verwenden.
R1140	Eine Nachricht sollte mit HTTP/1.1 gesendet werden.
R1141	Eine MESSAGE MUSS mit HTTP/1.1 oder HTTP/1.0 gesendet werden.
R2113	Ein Envelope MUSS NICHT das soapenc:arrayType -Attribut enthalten.
R2211	Ein Envelope, der mit einer rpc-Literal Bindung beschrieben wurde, MUSS NICHT das xsi:nil -Attribut mit dem Wert 1 oder true für die Teile-Accessoren haben.
R2714	Bei unidirektionalen Operationen darf eine INSTANCE NICHT eine HTTP-Antwort zurückgeben, die einen Envelope enthält. Insbesondere muss der HTTP-Antwort-Entity-Body leer sein.
R2729	Ein Envelope, der mit einer rpc-Literal Bindung beschrieben wird, die eine Antwort ist, MUSS ein Wrapper-Element haben, dessen Name der entsprechende wsdl:Operationsname ist, der mit dem StringResponse versehen ist.
R2735	Ein Envelope, der mit einer rpc-Literal Bindung beschrieben wird, MUSS die Teilzugriffselemente für Parameter und Rückgabewerte in keinem Namespace platzieren.
R2738	Ein Envelope MUSS alle soapbind:Header enthalten, die auf einer wsdl:input oder wsdl:output einer wsdl:operation einer wsdl:binding angegeben sind, die sie beschreibt.
R2740	Eine wsdl:Bindung in einer DESCRIPTION sollte ein soapbind:fault enthalten, der jeden bekannten Fehler beschreibt.

Regel	Beschreibung
R2744	Eine HTTP-Anforderung MESSAGE MUSS ein SOAPAction-HTTP-Header-Feld mit einem in Anführungszeichen angegebenen Wert enthalten, der dem Wert des soapAction-Attributs von soapbind:operation entspricht, falls in der entsprechenden WSDL-Beschreibung vorhanden ist.

Überprüfung der XML-Nachrichtenüberprüfung

October 5, 2021

Die Überprüfung der XML-Nachrichtenüberprüfung prüft Anforderungen, die XML-Nachrichten enthalten, um sicherzustellen, dass sie gültig sind. Wenn eine Anforderung eine ungültige XML-Nachricht enthält, blockiert die Web App Firewall die Anforderung. Der Zweck der XML-Validierungsprüfung besteht darin, einen Angreifer daran zu hindern, speziell konstruierte ungültige XML-Nachrichten zu verwenden, um die Sicherheit Ihrer Anwendung zu verletzen.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld XML-Nachrichtenüberprüfung ändern auf der Registerkarte Allgemein die Aktionen Blockieren, Protokollieren und Statistiken aktivieren oder deaktivieren.

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um die XML-Nachrichtenüberprüfungsprüfung zu konfigurieren:

- `set appfw profile <name> -xmlValidationAction [**block**] [**log**] [**stats**] [**none**]`

Sie müssen die GUI verwenden, um die anderen Einstellungen für die Überprüfung der XML-Gültigkeitsprüfung zu konfigurieren. Im Dialogfeld Überprüfung der XML-Nachrichtenüberprüfung ändern können Sie auf der Registerkarte
Prüfungen die folgenden Einstellungen konfigurieren:

- **XML-Nachrichtenüberprüfung.** Verwenden Sie eine der folgenden Optionen, um die XML-Nachricht zu validieren:
  - **SOAP-Umschlag.** Überprüfen Sie nur den SOAP-Umschlag von XML-Nachrichten.
  - **WSDL.** Validieren von XML-Nachrichten mithilfe einer XML-SAAP-WSDL. Wenn Sie WSDL-Validierung wählen, müssen Sie in der Dropdownliste WSDL-Objekt eine WSDL auswählen. Wenn Sie mit einer WSDL überprüfen möchten, die noch nicht in die Web App Firewall

importiert wurde, können Sie auf die Schaltfläche Importieren klicken, um das Dialogfeld WSDL-Importe verwalten zu öffnen und Ihre WSDL zu importieren. Weitere Informationen finden Sie unter WSDL .

* Wenn Sie die gesamte URL validieren möchten, lassen Sie das Optionsfeld Absolut im Schaltflächenfeld Endpunktprüfung aktiviert. Wenn Sie nur den Teil der URL nach dem Host überprüfen möchten, aktivieren Sie das Optionsfeld Relativ.
* Wenn Sie möchten, dass die Web App Firewall die WSDL strikt durchsetzen und keine zusätzlichen XML-Header zulassen, die nicht in der WSDL definiert sind, müssen Sie das Kontrollkästchen Zusätzliche Header zulassen, die nicht in der WSDL definiert sind.

  Achtung: Wenn Sie das Kontrollkästchen Zusätzliche Kopfzeilen
  zulassen, die nicht in der WSDL definiert sind, deaktivieren und Ihre WSDL nicht alle XML-Header definiert, die Ihre geschützte XML-Anwendung oder Web 2.0-Anwendung erwartet oder die ein Client sendet, können Sie den legitimen Zugriff auf Ihren geschützten Dienst sperren.

– **XML-Schema.** Validieren von XML-Nachrichten mithilfe eines XML-Schemas. Wenn Sie die XML-Schemaüberprüfung wählen, müssen Sie in der Dropdownliste XML-Schemaobjekt ein XML-Schema auswählen. Wenn Sie ein XML-Schema überprüfen möchten, das noch nicht in die Web App Firewall importiert wurde, können Sie auf die Schaltfläche Importieren klicken, um das Dialogfeld XML-Schemaimporte verwalten zu öffnen und Ihre WSDL zu importieren. Weitere Informationen finden Sie unter WSDL .

- **Antwortvalidierung.** Standardmäßig versucht die Web App Firewall nicht, Antworten zu validieren. Wenn Sie Antworten von Ihrer geschützten Anwendung oder Website 2.0-Website validieren möchten, aktivieren Sie das Kontrollkästchen Antwort überprüfen. Wenn Sie dies tun, werden das Kontrollkästchen XML-Schema wiederverwenden, das in der Anforderungsüberprüfung angegeben wurde, und die Dropdownliste XML-Schemaobjekt aktiviert.
  – Aktivieren Sie das Kontrollkästchen XML-Schema wiederverwenden, um das für die Anforderungsvalidierung angegebene Schema auch zur Antwortvalidierung zu verwenden.
  Hinweis: Wenn Sie dieses Kontrollkästchen aktivieren, ist die Dropdownliste
  XML-Schemaobjekt ausgegraut.
  – Wenn Sie ein anderes XML-Schema für die Antwortüberprüfung verwenden möchten, verwenden Sie die Dropdownliste XML-Schemaobjekt, um dieses XML-Schema auszuwählen oder hochzuladen.

XML-SOAP-Fehlerfilterprüfung

October 5, 2021

Die XML-SOAP-Fehlerfilterungsprüfung untersucht Antworten Ihrer geschützten Webdienste und fil-

tert XML-SOAP-Fehler heraus. Dadurch wird verhindert, dass vertrauliche Informationen an Angreifer auslaufen.

Wenn Sie den Assistenten oder die GUI verwenden, können Sie im Dialogfeld XML-SOAP-Fehlerfilterungsprüfung ändern auf der Registerkarte **Allgemein die** Aktionen Blockieren, Protokollieren und Statistiken sowie die Aktion Entfernen aktivieren oder deaktivieren, mit der SOAP-Fehler entfernt werden, bevor die Antwort an den Benutzer weitergeleitet wird.

Wenn Sie die Befehlszeilenschnittstelle verwenden, können Sie den folgenden Befehl eingeben, um die XML-SOAP-Fehlerfilterungsprüfung zu konfigurieren:

```
set appfw profile <name> -XMLSOAPFaultAction [block] [log] [stats] [none]
```

Sie können keine Ausnahmen für die XML-SOAP-Fehlerfilterprüfung konfigurieren. Sie können es nur aktivieren oder deaktivieren.

JSON-Schutzüberprüfungen

October 5, 2021

Die Citrix Web App Firewall schützt Ihre JSON-Anwendungen vor DoS-, SQL- oder Cross-Site-Scripting-Angriffen auf Content-Ebene. Wenn eine JSON-Anforderung einen DoS-, SQL- oder Cross-Site-Scripting-Angriff aufweist, müssen Sie Ihre Anwendung schützen, indem Sie Grenzwerte für JSON-Strukturen wie Arrays und Zeichenfolgen konfigurieren.

> **Hinweis:**
>
> Die JSON-Sicherheitsprüfungen gelten nur für Inhalte, die mit einem JSON-Inhaltstyp-Header gesendet werden. Wenn der Content-Type-Header fehlt oder auf einen anderen Wert festgelegt ist, werden alle JSON-Sicherheitsprüfungen umgangen. Wenn Sie Ihre JSON-Anwendungen schützen möchten, müssen die Webmaster jedes Webservers, der diese Anwendungen hostet, sicherstellen, dass ein richtiger JSON-Inhaltstyp Header gesendet wird.
>
> Die Lernfunktion unterstützt JSON-SQL, Cross-Site-Scripting und DOS-Inhaltstypen nicht.

JSON-Denial-of-Service-Schutzüberprüfung

December 7, 2021

Die JSON-Denial-of-Service-Prüfung (DoS) prüft eine eingehende JSON-Anforderung und überprüft, ob Daten vorhanden sind, die den Eigenschaften eines DoS-Angriffs entsprechen. Wenn die Anforderung JSON-Verstöße aufwies, blockiert die Appliance die Anforderung, protokolliert die Daten,

sendet eine SNMP-Warnung und zeigt auch eine JSON-Fehlerseite an. Der Zweck der JSON-DoS-Prüfung besteht darin, einen Angreifer daran zu hindern, JSON-Anfrage zu senden, um DoS-Angriffe auf Ihre JSON-Anwendungen oder -Website zu starten.

Wenn ein Client eine Anforderung an eine Citrix ADC Appliance sendet, analysiert der JSON-Parser die Anforderungsnutzlast, und wenn eine Verletzung beobachtet wird, erzwingt die Appliance Einschränkungen für die JSON-Struktur. Die Einschränkung erzwingt eine Größenbeschränkung für die JSON-Anforderung. Wenn eine JSON-Verletzung beobachtet wurde, wendet die Appliance eine Aktion an und antwortet mit der JSON-Fehlerseite.

JSON DoS-Regeln

Wenn die Appliance eine JSON-Anforderung empfängt, erzwingt der JSON-DOS-Schutz die Größenbeschränkung für die folgenden DoS-Parameter in der Anforderungs-Nutzlast.

1. maximale Tiefe: Maximale Verschachtelung (Tiefe) des JSON-Dokuments. Diese Prüfung schützt vor Dokumenten mit übermäßiger Hierarchietiefe.
2. Maximale Dokumentlänge: Maximale Dokumentlänge des JSON-Dokuments.
3. maximale Array-Länge: Maximale Array-Länge in einem beliebigen JSON-Objekt. Diese Prüfung schützt vor Arrays mit großen Längen.
4. maximale Zeichenfolgenlänge: Maximale Zeichenfolgenlänge im JSON. Diese Prüfung schützt vor Saiten mit großer Länge.
5. Maximale Objektschlüsselanzahl: Maximale Anzahl der Schlüssel in einem beliebigen JSON-Objekt. Diese Prüfung schützt vor Objekten, die eine große Anzahl von Schlüsseln haben.
6. Maximale Objektschlüssellänge: Maximale Schlüssellänge in einem beliebigen JSON-Objekt. Diese Prüfung schützt vor Objekten mit großen Schlüsseln.

Im Folgenden finden Sie eine Liste der JSON-DoS-Regeln, die während des JSON-Parsens validiert wurden.

1. JSONMaxContainerDepth. Diese Prüfung kann durch Konfigurieren der JSONMaxContainerDepth Check aktiviert werden und standardmäßig ist die Option OFF.
2. JSONMaxContainerDepth. Diese Prüfung kann durch die konfigurierbare Option aktiviert/deaktiviert werden jsonmaxContainerDepthCheck und der Standardwert kann mit der Option jsonMaxContainerDepth geändert werden. Sie können jedoch die Maximalstufen auf einen Wert zwischen 1 und 127 variieren. Standardwert: 5, Minimalwert: 1, Maximalwert: 127
3. JSONMaxDocumentLength. Diese Prüfung kann durch Konfigurieren der JSONMaxDocumentLength-Prüfung aktiviert werden und die Standardoption ist OFF.
4. JSONMaxDocumentLength. Diese Prüfung kann durch Konfigurieren der JSONMaxDocumentLength-Prüfung aktiviert werden und die Standardlänge ist auf 20000000 Bytes festgelegt. Minimaler Wert: 1, Maximaler Wert: 2147483647

5. JSONMaxObjectKeyCount. Die Regel überprüft, ob die JSON-Prüfung für maximale Objektschlüsselanzahl aktiviert oder deaktiviert ist. Mögliche Werte: ON, OFF, Standardwert: OFF
6. JSONMaxObjectKeyCount. Diese Prüfung kann durch Konfigurieren der JSONMaxObjectKeyCount-Prüfung aktiviert werden. Die Prüfung schützt vor Objekten, die eine große Anzahl von Schlüsseln haben, und der Standardwert ist auf 1000 Byte festgelegt. Minimalwert: 0, Maximalwert: 2147483647
7. JSONMaxObjectKeyLength. Diese Prüfung kann durch Konfigurieren der JSONMaxObjectKeyLength-Prüfung aktiviert werden. Die Regel überprüft, ob die Prüfung der maximalen JSON-Objekt-Schlüssellänge aktiviert oder deaktiviert ist. Standardmäßig ist es ausgeschaltet.
8. JSONMaxObjectKeyLength. Der Check schützt vor Objekten mit großer Schlüssellänge. Standardwert: 128. Minimaler Wert: 1, Maximaler Wert: 2147483647
9. JSONMaxArrayLength. Die Regel überprüft, ob die maximale JSON-Array-Längenüberprüfung ON oder OFF ist. Standardmäßig ist es deaktiviert.
10. JSONMaxArrayLength. Der Check schützt vor Arrays mit großen Längen. Standardmäßig ist der Wert auf 10000 festgelegt. Minimaler Wert: 1, Maximaler Wert: 2147483647
11. JSONMaxStringLength. Diese Prüfung kann durch Konfigurieren der JSONMaxStringLength Prüfung aktiviert werden. Die Prüfung überprüft, ob die maximale JSON-Stringlänge ON oder OFF ist. Standardmäßig ist es deaktiviert.
12. JSONMaxStringLength. Der Check schützt vor großen Saiten. Standardmäßig ist es auf 1000000 eingestellt. Minimaler Wert: 1, Maximaler Wert: 2147483647

Konfigurieren der JSON-DoS-Schutzprüfung

Zum Konfigurieren des JSON-DoS-Schutzes müssen Sie die folgenden Schritte ausführen:

1. Fügen Sie ein Anwendungs-Firewall-Profil für JSON hinzu.
2. Legen Sie das Anwendungs-Firewall-Profil für JSON DoS-Einstellungen fest.
3. Konfigurieren Sie JSON DoS-Variablen, indem Sie das Firewallprofil der Anwendung binden.

Hinzufügen eines Anwendungs-Firewall-Profils für JSON DoS-Schutz

Sie müssen zunächst ein Profil erstellen, das angibt, wie die Anwendungsfirewall Ihre JSON-Webinhalte vor JSON-DoS-Angriff schützen muss.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add appfw profile <name> -type (HTML | XML | JSON)
```


> *Hinweis*:
>
> Wenn Sie den Profiltyp als JSON festlegen, sind andere Prüfungen wie HTML oder XML nicht anwendbar.

Beispiel

```
add appfw profile profile1 -type JSON
```

Festlegen des Anwendungsfirewall Profils für den JSON DoS-Schutz

Sie müssen das Profil für eine oder mehrere JSON DoS-Aktionen und das JSON DoS-Fehlerobjekt konfigurieren, die im Firewallprofil der Anwendung festgelegt werden sollen.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set appfw profile <name> -JSONDoSAction [block] | [log] | [stats] | [none]
```

Block - Blockieren von Verbindungen, die gegen diese Sicherheitsprüfung verstoßen.
Log - Protokollieren Sie Verstöße gegen diese Sicherheitsprüfung.
Stats- Generieren Sie Statistiken für diese Sicherheitsprüfung.
None - Deaktivieren Sie alle Aktionen für diese Sicherheitsprüfung.

> *Hinweis*:
>
> Um eine oder mehrere Aktionen zu aktivieren, geben Sie set appfw profile -jsondosAction gefolgt von den zu aktivierenden Aktionen ein.

Beispiel

```
set appfw profile profile1 -JSONDoSAction block log stat
```

Konfigurieren von DoS-Variablen durch Binden des Anwendungs-Firewall-Profils

Um JSON DoS-Schutz zu bieten, müssen Sie das Firewallprofil der Anwendung mit JSON DoS-Einstellungen verbinden.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind appfw profile <name> -JSONDoSURL <expression> [-JSONMaxContainerDepthCheck
 ( ON | OFF )[-JSONMaxContainerDepth <positive_integer>]] [-JSONMaxDocumentLengthCheck
 ( ON | OFF )[-JSONMaxDocumentLength <positive_integer>]] [-JSONMaxObjectKeyCountCheck
 ( ON | OFF )[-SONMaxObjectKeyCount <positive_integer>]] [-JSONMaxObjectKeyLengthCheck
 ( ON | OFF )[-JSONMaxObjectKeyLength <positive_integer>]] [-JSONMaxArrayLengthCheck
 ( ON | OFF )[-JSONMaxArrayLength <positive_integer>]] [-JSONMaxStringLengthCheck
 ( ON | OFF )[-JSONMaxStringLength <positive_integer>]]
```


Beispiel

```
bind appfw profile profile1 -JSONDoSURL ".*" -JSONMaxContainerDepthCheck ON
```

> *Hinweis*:
>
> Die JSON-DoS-Prüfungen sind nur anwendbar, wenn der Profiltyp als JSON ausgewählt ist. Außerdem werden die SQL-, Cross-Site-Scripting-, Feldformat- und Formularfeldsignaturen bei JSON-Profilen auf Abfrageparameter angewendet.

JSON-Fehlerseite importieren

Wenn eine eingehende Anforderung einen DoS-Angriff hatte und Sie die Anforderung blockieren, zeigt die Appliance eine Fehlermeldung an. Dazu müssen Sie die JSON-Fehlerseite importieren.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import appfw jsonerrorpage <src> <name> [-comment <string>] [-overwrite]
```

Hierbei gilt:

src. URL (Protokoll, Host, Pfad und Name) für den Speicherort, an dem das importierte JSON-Fehlerobjekt gespeichert werden soll.

> *Hinweis*:
>
> Der Import schlägt fehl, wenn sich das zu importierende Objekt auf einem HTTPS-Server befindet, der Clientzertifikatauthentifizierung für den Zugriff erfordert. Dies ist ein obligatorisches Argument. Maximale Länge: 2047.

Name. Name, der dem JSON-Fehlerobjekt auf dem Citrix ADC zugewiesen werden soll. Dies ist ein obligatorisches Argument. Maximale Länge: 31
Kommentar. Alle Kommentare, um Informationen über das JSON-Fehlerobjekt beizubehalten. Maximale Länge: 255
Überschreiben. Überschreiben Sie jedes vorhandene JSON-Fehlerobjekt mit demselben Namen.

Beispielkonfiguration

```
1 Add appfw prof profjson - type JSON
2 Bind appfw prof profjson - JSONDoSURL ".*" -
    JSONMaxDocumentLengthCheck ON -JSONMaxDocumentLength 30 -
    JSONMaxContainerDepthCheck ON -JSONMaxContainerDepth 3
    JSONMaxObjectKeyCountCheck ON -JSONMaxObjectKeyCount 4 -
    JSONMaxObjectKeyLengthCheck ON -JSONMaxObjectKeyLength 10 -
    JSONMaxArrayLengthCheck ON -JSONMaxArrayLength 5 -
    JSONMaxStringLengthCheck ON -JSONMaxStringLength 30
```



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

Beispielnutzlasten, Protokollnachrichten und Leistungsindikatoren:

JSONMaxDocumentLength Violation

JSONMaxDocumentLength: 30
Payload: {“a”:”A”,”b”:”B”,”c”:”C”,”d”:”D”,”e”:”E”}

Protokollmeldung:

```
Document Length exceeds 20000000 May 29 20:23:32 <local0.info>
    10.217.31.243 05/29/2019:20:23:32 GMT 0-PPE-0 : default APPFW
    APPFW_JSON_DOS_MAX_DOCUMENT_LENGTH 136 0 : 10.217.32.134 114-PPE0 -
    profjson http://10.217.30.120/forms/login.html Document exceeds
    maximum document length (30). cn1=30467 cn2=115 cs1=profjson cs2=
    PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Zähler:

```
1 0 6 as_viol_json_dos
2 0 3 as_viol_json_dos_max_document_length
3 0 6 as_log_json_dos
4 0 3 as_log_json_dos_max_document_length
5 0 6 as_viol_json_dos_profile appfw__(profile1)
6 0 3 as_viol_json_dos_max_document_length_profile appfw__(profile1)
7 0 6 as_log_json_dos_profile appfw__(profile1)
8 0 3 as_log_json_dos_max_document_length_profile appfw__(profile1)
<!--NeedCopy-->
```

JSONMaxContainerDepth Violation

JSONMaxContainerDepth: 3
Payload: {“a”: {“b”: {“c”: {“d”: { “e” : “f” }}}}}

Protokollmeldung:


```
May 29 19:33:59 <local0.info> 10.217.31.243 05/29/2019:19:33:59 GMT 0-PPE-1 : default APPFW APPFW_JSON_DOS_MAX_CONTAINER_DEPTH 4626 0 : 10.217.31.247 22-PPE1 - profjson http://10.217.30.120/forms/login.html Document at offset (15) exceeds maximum container depth (3). cn1=30466 cn2=113 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Zähler:

```
36 20999 7 1 0 as_viol_json_dos
37 0 6 1 0 as_viol_json_dos_max_container_depth
38 0 7 1 0 as_log_json_dos
39 0 6 1 0 as_log_json_dos_max_container_depth
40 0 7 1 0 as_viol_json_dos_profile appfw__(profile1)
41 0 6 1 0 as_viol_json_dos_max_container_depth_profile appfw__(profile1)
42 0 7 1 0 as_log_json_dos_profile appfw__(profile1)
43 0 6 1 0 as_log_json_dos_max_container_depth_profile appfw__(profile1)
<!--NeedCopy-->
```

JSONMaxObjectKeyCount Violation

JSONMaxObjectKeyCount: 4

Payload: {“a”: “A”, “b”: “B”, “c”:”C”, “d” :”D”, “e” : “E” }

Protokollmeldung:

```
May 30 19:42:41 <local0.info> 10.217.31.243 05/30/2019:19:42:41 GMT 0-PPE-1 : default APPFW APPFW_JSON_DOS_MAX_OBJECT_KEY_COUNT 457 0 : 10.217.32.134 219-PPE1 - profjson http://10.217.30.120/forms/login.html Object at offset (41) that exceeds maximum key count (4). cn1=30468 cn2=118 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Zähler:

```
94 119105 15 1 0 as_viol_json_dos
95 0 4 1 0 as_viol_json_dos_max_object_key_count
```



```
96 0 15 1 0 as_log_json_dos
97 0 4 1 0 as_log_json_dos_max_object_key_count
98 0 15 1 0 as_viol_json_dos_profile appfw__(profile1)
99 0 4 1 0 as_viol_json_dos_max_object_key_count_profile appfw__(
   profile1)
100 0 15 1 0 as_log_json_dos_profile appfw__(profile1)
101 0 4 1 0 as_log_json_dos_max_object_key_count_profile appfw__(
   profile1)
<!--NeedCopy-->
```

JSONMaxObjectKeyLength Violation

JSONMaxObjectKeyLength: 10
Payload: {“a”: “A”, “b1234567890”: “B”, “c”:”C”, “d” :”D”, “e” : “E” }

Protokollmeldung:

```
May 31 20:26:10 <local0.info> 10.217.31.243 05/31/2019:20:26:10 GMT 0-
   PPE-1 : default APPFW APPFW_JSON_DOS_MAX_OBJECT_KEY_LENGTH 102 0 :
   10.217.32.134 89-PPE1 - profjson http://10.217.30.120/forms/login.
   html Object key(b1234567890) at offset (12) exceeds maximum key
   length (10). cn1=30469 cn2=118 cs1=profjson cs2=PPE0 cs4=ALERT cs5
   =2019 act=blocked
<!--NeedCopy-->
```

Zähler:

```
242172 6 1 0 as_viol_json_dos
0 1 1 0 as_viol_json_dos_max_object_key_length
10 0 5 1 0 as_log_json_dos
11 0 1 1 0 as_log_json_dos_max_object_key_length
12 0 6 1 0 as_viol_json_dos_profile appfw__(profile1)
13 0 1 1 0 as_viol_json_dos_max_object_key_length_profile appfw__(
   profile1)
14 0 5 1 0 as_log_json_dos_profile appfw__(profile1)
15 0 1 1 0 as_log_json_dos_max_object_key_length_profile appfw__(
   profile1)
<!--NeedCopy-->
```

JSONMaxArrayLength Violation

jsonMaxArrayLength: 5
Nutzlast: {“a”:” A”, “c”:[” d”,” e”,” f”,” g”,” h”,” i”],” e”:[“E”,” e”]}

Protokollmeldung:

```
May 29 20:58:39 <local0.info> 10.217.31.243 05/29/2019:20:58:39 GMT 0-PPE-1 : default APPFW APPFW_JSON_DOS_MAX_ARRAY_LENGTH 4650 0 : 10.217.32.134 153-PPE1 -profjson http://10.217.30.120/forms/login.html Array at offset (37) that exceeds maximum array length (5). cn1=30469 cn2=120 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

Zähler:

```
36 182293 10 1 0 as_viol_json_dos
37 0 1 1 0 as_viol_json_dos_max_array_length
38 0 10 1 0 as_log_json_dos 39 0 1 1 0 as_log_json_dos_max_array_length
40 0 10 1 0 as_viol_json_dos_profile appfw__(profile1)
41 0 1 1 0 as_viol_json_dos_max_array_length_profile appfw__(profile1)
42 0 10 1 0 as_log_json_dos_profile appfw__(profile1)
43 0 1 1 0 as_log_json_dos_max_array_length_profile appfw__(profile1))
<!--NeedCopy-->
```

JSONMaxStringLength Violation

JSONMaxStringLength: 10

Payload: {“a”: “A”, “c”:”CcCcCcCcCcCcCcCcCc”,”e”:[“E”,” e”]}

Protokollmeldung:

```
May 29 20:05:02 <local0.info> 10.217.31.243 05/29/2019:20:05:02 GMT 0-PPE-0 : default APPFW APPFW_JSON_DOS_MAX_STRING_LENGTH 134 0 : 10.217.32.134 80-PPE0 - profjson http://10.217.30.120/forms/login.html String(CcCcCcCcCcCcCc) at offset (27) that exceeds maximum string length (10). n1=30470 cn2=122 cs1=profjson cs2=PPE0 cs4=ALERT cs5=2019 act=blocked
<!--NeedCopy-->
```

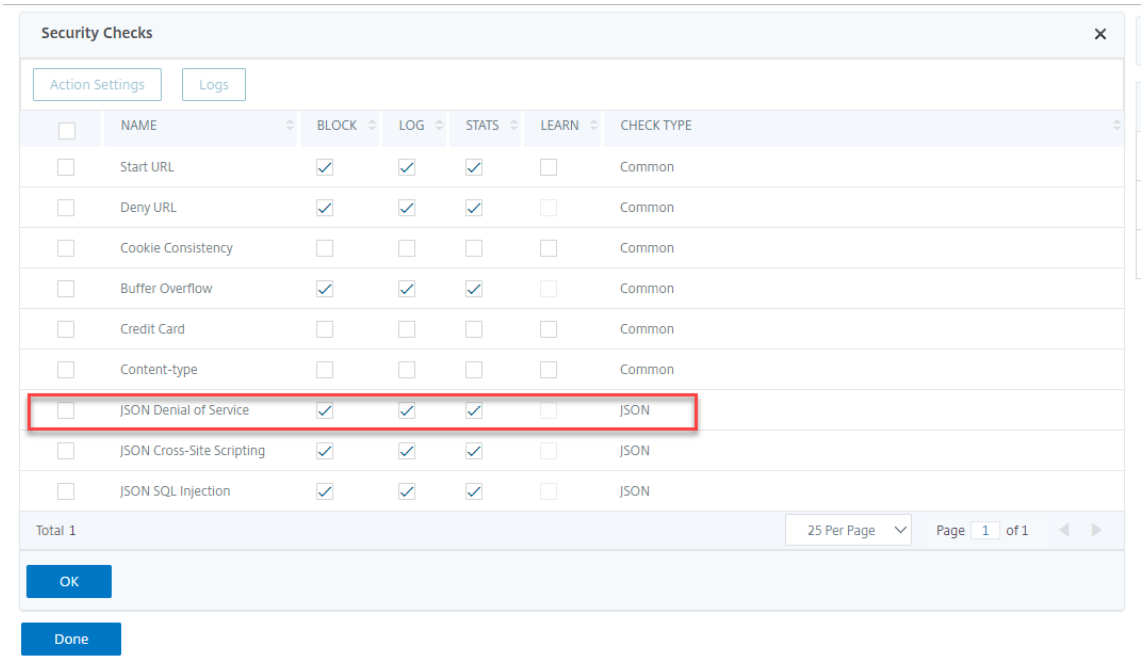
Zähler:


```
44 91079 3 1 0 as_viol_json_dos
45 0 1 1 0 as_viol_json_dos_max_string_length
46 0 3 1 0 as_log_json_dos
47 0 1 1 0 as_log_json_dos_max_string_length
48 0 3 1 0 as_viol_json_dos_profile appfw__(profile1)
49 0 1 1 0 as_viol_json_dos_max_string_length_profile appfw__(profile1)
50 0 3 1 0 as_log_json_dos_profile appfw__(profile1)
51 0 1 1 0 as_log_json_dos_max_string_length_profile appfw__(profile1
<!--NeedCopy-->
```

Konfigurieren des JSON-DoS-Schutzes mit der Citrix GUI

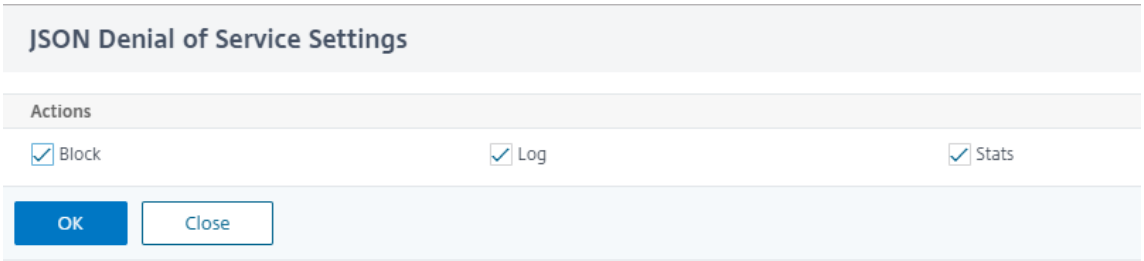
Gehen Sie folgendermaßen vor, um die JSON DoS-Schutzeinstellungen festzulegen.

1. Navigieren Sie im Navigationsbereich zu **Sicherheit** > **Profile**.
2. Klicken Sie auf der Seite **Profile** auf **Hinzufügen**.
3. Klicken Sie auf der Seite **Citrix Web App Firewall-Profil** unter **Erweiterte Einstellungen auf Sicherheitsprüfungen**.
4. Wechseln Sie im Abschnitt **Sicherheitsprüfungen** zu **JSON Denial of Service-Einstellungen** .
5. Klicken Sie auf das Symbol für die ausführbare Datei neben dem Kontrollkästchen.

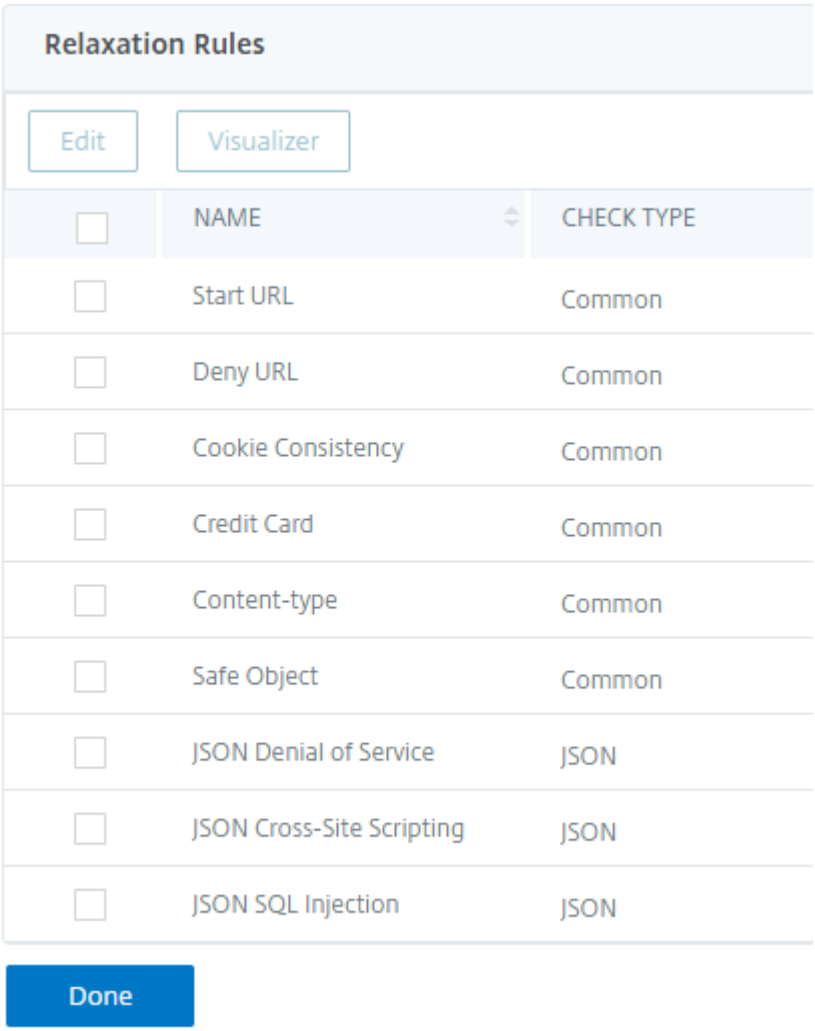


6. Klicken Sie auf **Aktionseinstellungen**, um die Seite **JSON-Denial-of-Service-Einstellungen** aufzurufen.

7. Wählen Sie die JSON DoS-Aktion aus.
8. Klicken Sie auf **OK**.



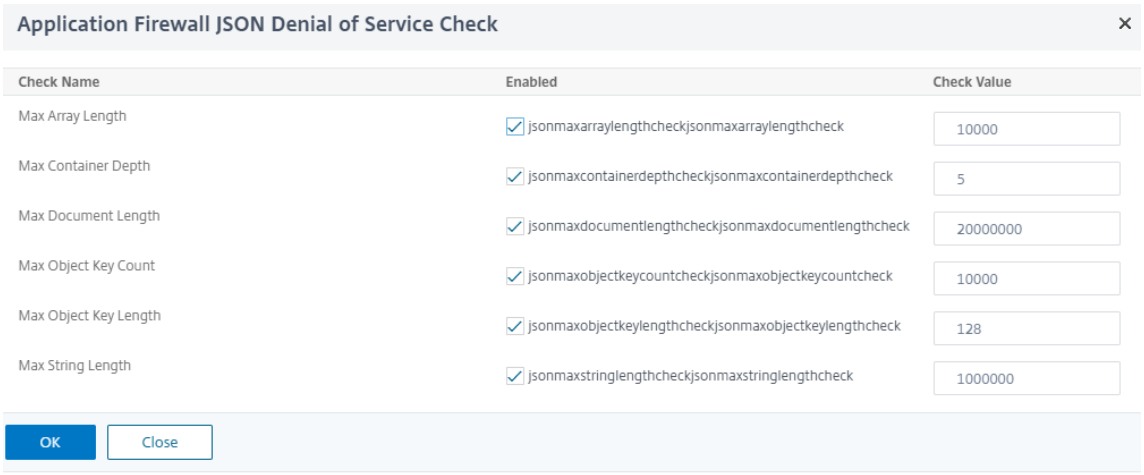
9. Klicken Sie auf der Seite **Citrix Web App Firewall Profil** unter **Erweiterte Einstellungen** auf **Relaxationsregeln**.
10. Wählen Sie im Abschnitt **Relaxationsregeln** die Option **JSON-Denial-of-Service-Einstellungen aus**, und klicken Sie auf **Bearbeiten** .



11. Legen Sie in der **Application Firewall JSON Denial of Service Check** die JSON DoS-

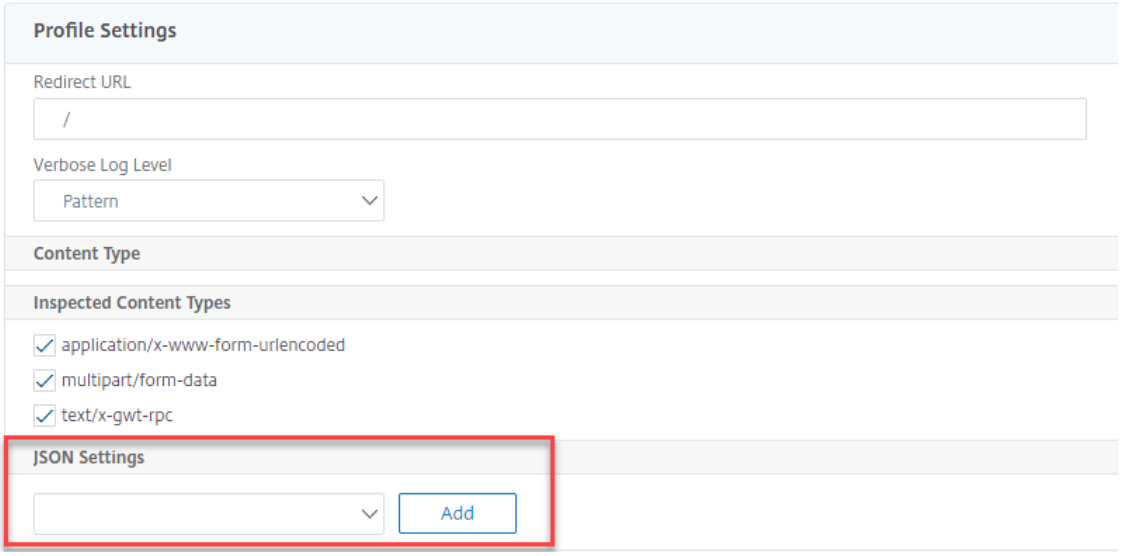
Validierungswerte fest.

12. Klicken Sie auf **OK**.



13. Klicken Sie auf der Seite **Citrix Web App Firewall Profil**unter **Erweiterte Einstellungen**auf **Profileinstellungen**.

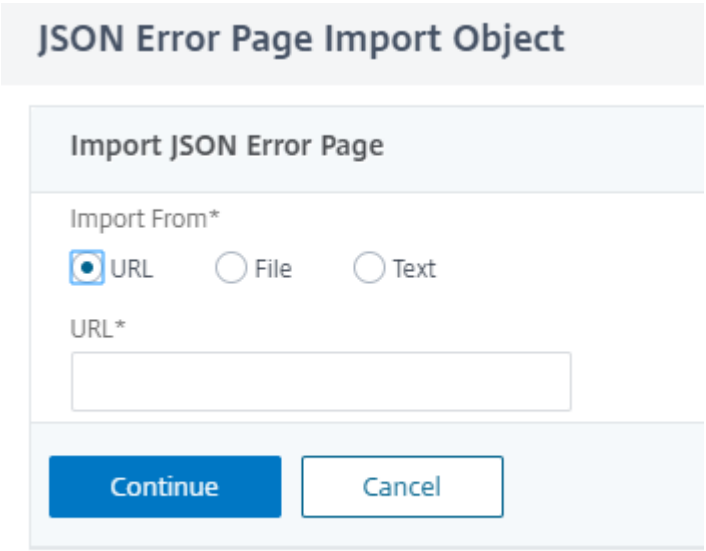
14. Gehen Sie im Abschnitt **Profileinstellungen** zum Abschnitt **JSON-Fehlereinstellungen**, um die **JSON-DoS-Fehlerseite** festzulegen.



15. Legen Sie auf der **Seite JSON-Fehlerseite Importobjekt** die folgenden Parameter fest:

    a) Importieren von. Importieren Sie die Fehlerseite als Text, Datei oder URL.
    b) -URL. URL, um den Benutzer auf die Fehlerseite umzuleiten.
    1 Datei. Wählen Sie eine Datei aus, die als JSON DoS-Fehlerdatei importiert werden soll.
    c) Text. Geben Sie den Inhalt der JSON-Datei ein.
    d) Klicken Sie auf Weiter.
    e) Akte. Geben Sie den Dateinamen ein.

f) Dateiinhalt. Fügen Sie den Inhalt der Fehlerdatei hinzu.
g) Klicken Sie auf **OK**.



16. Klicken Sie auf **OK**.
17. Klicken Sie auf **Fertig**.

JSON SQL-Injection-Schutzprüfung

October 5, 2021

Eine eingehende JSON-Anforderung kann SQL-Injection in Form von partiellen SQL-Abfragezeichenfolgen oder nicht autorisierten Befehlen im Code haben. Dies führt zum Diebstahl von Daten aus der JSON-Datenbank Ihrer Webserver. Nach Erhalt einer solchen Anfrage blockiert die Appliance diese Anfrage zum Schutz Ihrer Daten.

Betrachten Sie ein Szenario, in dem ein Client eine JSON-SQL-Anforderung an eine Citrix ADC Appliance sendet, der JSON-Parser die Anforderungsnutzlast analysiert und wenn eine SQL-Injection beobachtet wird, erzwingt die Appliance Einschränkungen für den JSON-SQL-Inhalt. Die Einschränkung erzwingt eine Größenbeschränkung für die JSON-SQL-Anforderung. Wenn eine JSON-SQL-Injection beobachtet wird, wendet die Appliance eine Aktion an und antwortet mit der JSON-SQL-Fehlerseite.

Konfigurieren des JSON SQL-Injection-Schutzes

Zum Konfigurieren des JSON-SQL-Schutzes müssen Sie die folgenden Schritte ausführen:

1. Fügen Sie das Anwendungs-Firewall-Profil als JSON hinzu.
2. Festlegen des Anwendungs-Firewallprofils für JSON SQL Injection-Einstellungen
3. Konfigurieren Sie die JSON-SQL-Aktion, indem Sie das Firewallprofil der Anwendung binden.

Anwendungs-Firewall-Profil vom Typ JSON hinzufügen

Sie müssen zunächst ein Profil erstellen, das angibt, wie die Anwendungsfirewall Ihren JSON-Webinhalt vor JSON SQL Injection-Angriff schützen muss.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add appfw profile <name> -type (HTML | XML | JSON)
```

> *Hinweis*:
>
> Wenn Sie den Profiltyp als JSON festlegen, sind andere Prüfungen wie HTML oder XML nicht anwendbar.

Beispiel

```
add appfw profile profile1 -type JSON
```

Konfigurieren der JSON-SQL-Injection-Aktion

Sie müssen eine oder mehrere JSON SQL Injection-Aktionen konfigurieren, um Ihre Anwendung vor JSON SQL-Injection-Angriffen zu schützen.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set appfw profile <name> - JSONSQLInjectionAction [block] [log] [stats] [
none]
```

SQL Injection-Aktionen sind:
Blockieren - Blockieren von Verbindungen, die diese Sicherheitsprüfung verletzen.
Log - Protokollieren Sie Verstöße gegen diese Sicherheitsprüfung.
Stats- Generieren Sie Statistiken für diese Sicherheitsprüfung.
None - Deaktivieren Sie alle Aktionen für diese Sicherheitsprüfung.

JSON SQL Injection-Typ konfigurieren

Geben Sie an der Eingabeaufforderung Folgendes ein, um den JSON SQL Injection-Typ in einem Anwendungsfirewallprofil zu konfigurieren:

```
set appfw profile <name> - JSONSQLInjectionType <JSONSQLInjectionType>
```


Beispiel

```
set appfw profile profile1 -JSONSQLInjectionType SQLKeyword
```

Wo die verfügbaren SQL Injection-Typen sind:
Verfügbare SQL-Injectionstypen.
SQLsPlchar. Prüft auf SQL-Sonderzeichen,
SQLKeyword. Überprüft nach SQL-Schlüsselwörtern.
SQLSplCharAndKeyword. Prüft auf beide und Blöcke, wenn gefunden.
SQLSplCharorKeyword. Blockiert, wenn SQL-Sonderzeichen oder SPL-Schlüsselwort gefunden wird.
Mögliche Werte: SQLSplchar, SQLKeyword, SQLSplCharorKeyword, SQLSplCharAndKeyword.

> *Hinweis*:
> Um eine oder mehrere Aktionen zu aktivieren, geben Sie set appfw profile - jsonSQLInjectionAction gefolgt von den zu aktivierenden Aktionen ein.

Beispiel

```
set appfw profile profile1 -JSONSQLInjectionAction block log stat
```

Das folgende Beispiel zeigt eine Beispielnutzlast, die entsprechende Protokollnachricht und die Statistikzähler:

```
Payload:
=======
{

  ”test”: ”data”,
  ”username”: ”waf”,
  ”password”: ”select * from t1;”,
  ”details”: {

    ”surname”: ”test”,
    ”age”: ”23”
   }

 }


Log Message:
===========
08/19/2019:08:49:46 GMT pegasus121 Informational 0-PPE-0 : default
   APPFW APPFW_JSON_SQL 6656 0 :  10.217.32.165 18402-PPE0 - profjson
```

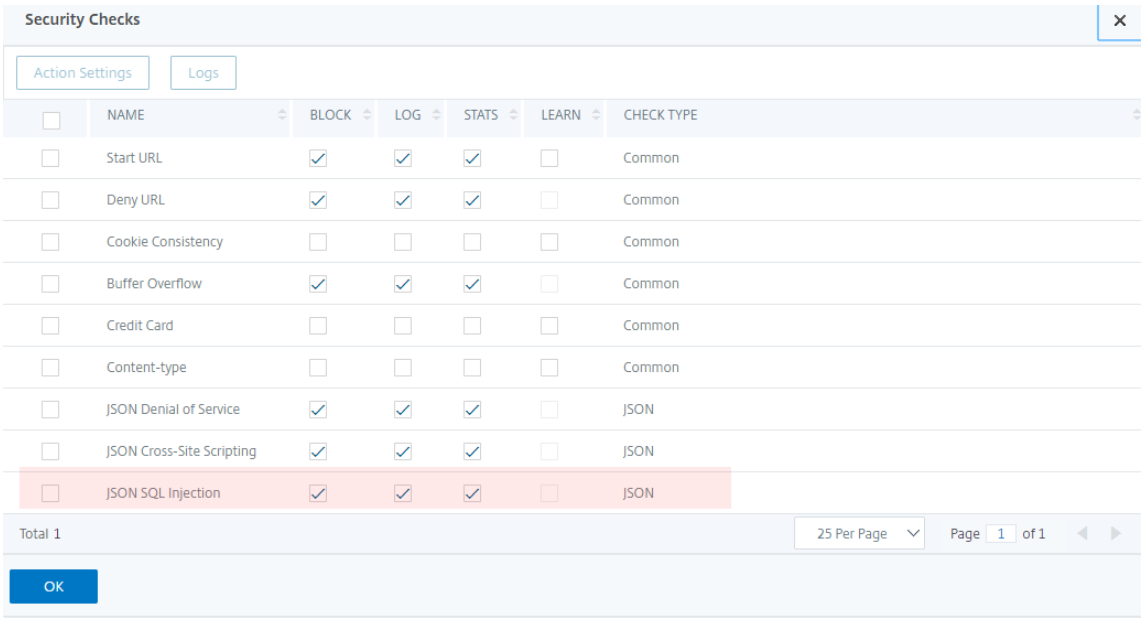


```
      http://10.217.32.147/test.html SQL Keyword check failed for object
      value(with violation="select(;)") starting at offset(52) <blocked>
20 Counters:
21 ========
22    1  441083              1 as_viol_json_sql
23    3       0              1 as_log_json_sql
24    5       0              1 as_viol_json_sql_profile appfw__(profjson)
25    7       0              1 as_log_json_sql_profile appfw__(profjson)
26 <!--NeedCopy-->
```

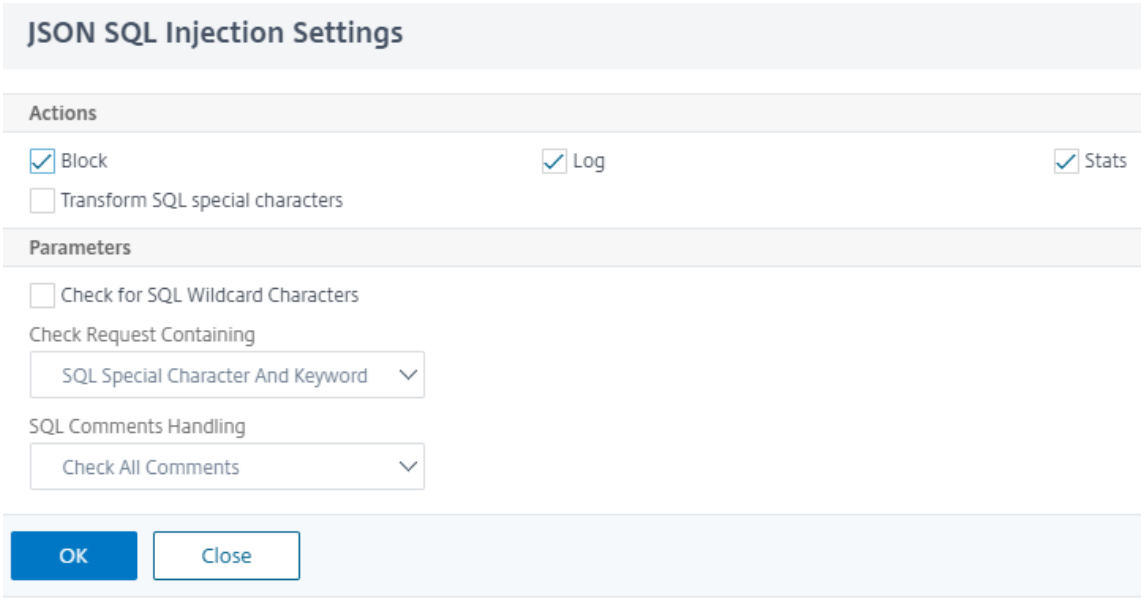
Konfigurieren des JSON SQL Injection-Schutzes mit der Citrix GUI

Gehen Sie folgendermaßen vor, um die JSON SQL Injection-Schutzeinstellungen festzulegen.

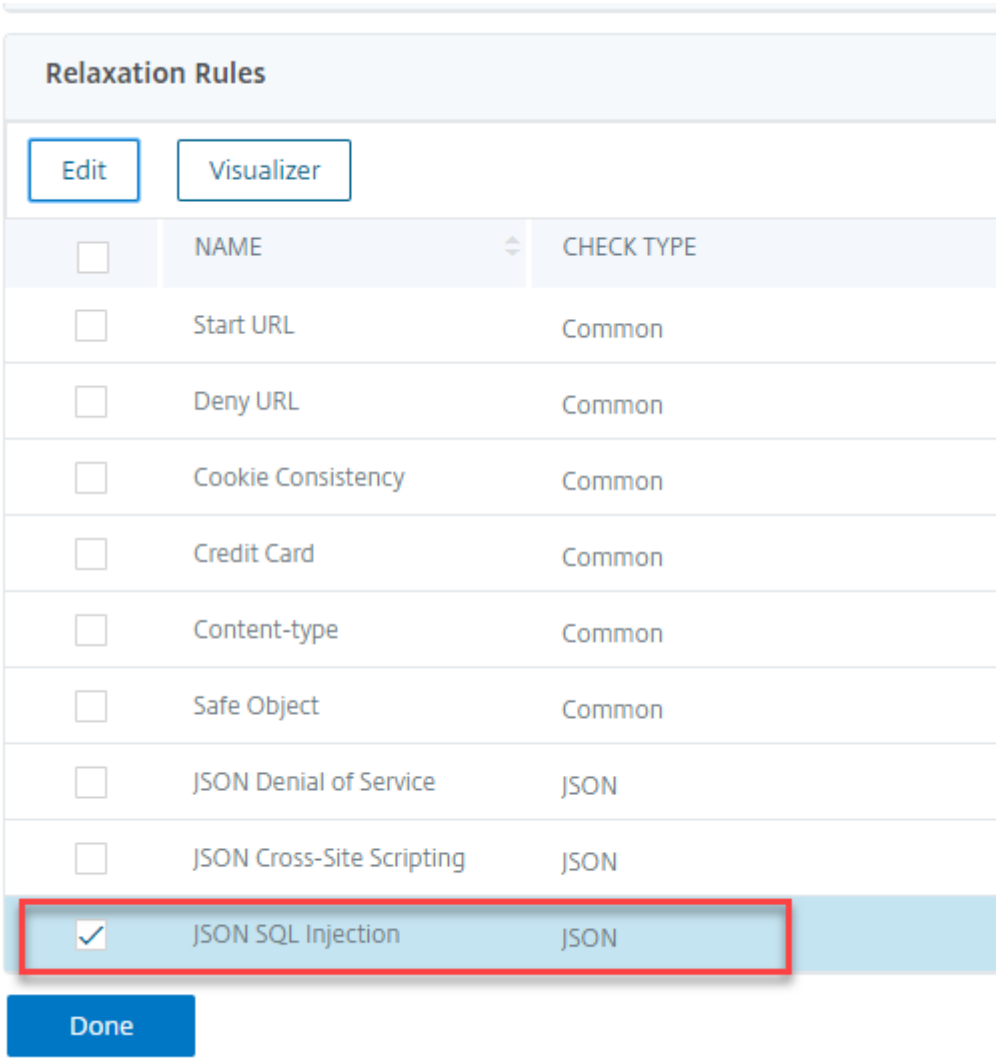
1. Navigieren Sie im Navigationsbereich zu **Sicherheit** > **Profile**.
2. Klicken Sie auf der Seite **Profile** auf **Hinzufügen**.
3. Klicken Sie auf der Seite **Citrix Web App Firewall Profile** unter **Erweiterte Einstellungen** auf **Sicherheitsprüfungen**.
4. Wechseln Sie im Abschnitt **Sicherheitsprüfungen** zu **JSON SQL Injection-Einstellungen** .
5. Klicken Sie auf das Symbol für die ausführbare Datei neben dem Kontrollkästchen.



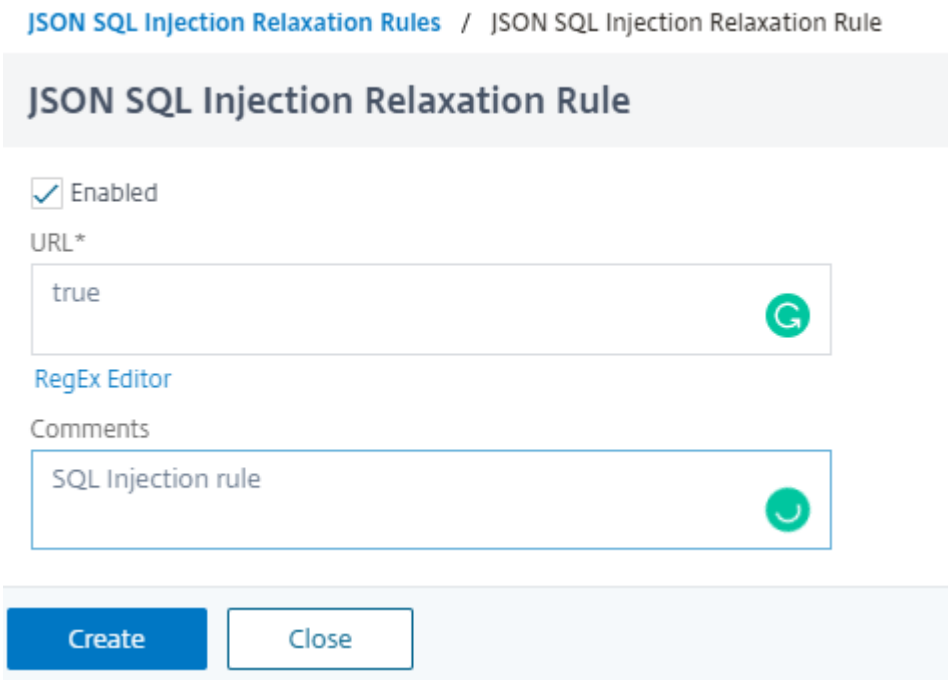
6. Klicken Sie auf **Aktionseinstellungen**, um die Seite **JSON SQL Injection Settings** aufzurufen.
7. Wählen Sie die **JSON SQL Injection-Aktionen** aus.
8. Klicken Sie auf **OK**.



9. Klicken Sie auf der Seite **Citrix Web App Firewall Profil** unter **Erweiterte Einstellungen** auf **Relaxationsregeln**.
10. Wählen Sie im Abschnitt **Relaxationsregeln** die Option **JSON SQL Injection-Einstellungen** aus, und klicken Sie auf **Bearbeiten**.



11. Geben Sie auf der Seite JSON SQL Injection Relaxation Rule die URL ein, an die die Anforderung gesendet werden muss. Alle Anfragen, die an diese URL gesendet werden, werden nicht gesperrt.
12. Klicken Sie auf **Erstellen**.



JSON Cross-Site Scripting Schutzprüfung

October 5, 2021

Wenn eine eingehende JSON-Nutzlast über bösartige websiteübergreifende Skriptdaten verfügt, blockiert WAF die Anforderung. In den folgenden Verfahren wird erläutert, wie Sie dies über CLI- und GUI-Schnittstellen konfigurieren können.

Konfigurieren des JSON Cross-Site Scripting Schutzes

Um den JSON-Cross-Site-Scripting-Schutz zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Fügen Sie das Anwendungs-Firewall-Profil als JSON hinzu.
2. Konfigurieren der JSON-Cross-Site-Scripting-Aktion zum Blockieren der böswilligen Nutzlast für Cross-S

Anwendungs-Firewall-Profil vom Typ JSON hinzufügen

Sie müssen zuerst ein Profil erstellen, das angibt, wie die Anwendungsfirewall Ihre JSON-Webinhalte vor Cross-Site-Scripting-Angriffen von JSON schützen muss.

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add appfw profile <name> -type (HTML | XML | JSON)
```

> **Hinweis**:
>
> Wenn Sie den Profiltyp als JSON festlegen, sind andere Prüfungen wie HTML oder XML nicht anwendbar.

Beispiel

```
add appfw profile profile1 -type JSON
```

Beispielausgabe für JSON Cross-Site Scripting Verletzung

```
JSONcross-site scriptingAction: block log stats
Payload: {
 ”username”:”<a href=”jAvAsCrIpT:alert(1)”>X</a>”,”password”:”xyz” }


Log message: Aug 19 06:57:33 <local0.info> 10.106.102.21
   08/19/2019:06:57:33 GMT  0-PPE-0 : default APPFW APPFW_JSON_cross-
   site scripting 58 0 :  10.102.1.98 12-PPE0 - profjson http://
   10.106.102.24/ Cross-site script check failed for object value(with
   violation=”Bad URL: jAvAsCrIpT:alert(1)”) starting at offset(12). <
   blocked>

Counters
   1  357000                  1 as_viol_json_xss
   3  0                       1 as_log_json_xss
   5  0                       1 as_viol_json_xss_profile appfw__(
      profjson)
   7  0                       1 as_log_json_xss_profile appfw__(
      profjson)

<!--NeedCopy-->
```

Konfigurieren von JSON Cross-Site Scripting Aktion

Sie müssen eine oder mehrere Cross-Site-Scripting-Aktionen von JSON konfigurieren, um Ihre Anwendung vor JSON Cross-Site Scripting-Angriffen zu schützen.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set appfw profile <name> - JSONcross-site scriptingAction [block] [log] [
stats] [none]
```


Beispiel

```
set appfw profile profile1 -JSONcross-site scriptingAction block
```

Die verfügbaren Cross-Site-Skripting-Aktionen sind:
Blockieren - Blockieren von Verbindungen, die gegen diese Sicherheitsprüfung verstoßen.
Log - Protokollieren Sie Verstöße gegen diese Sicherheitsprüfung.
Stats- Generieren Sie Statistiken für diese Sicherheitsprüfung.
None - Deaktivieren Sie alle Aktionen für diese Sicherheitsprüfung.

> **Hinweis**:
> Um eine oder mehrere Aktionen zu aktivieren, geben Sie “set appfw profile - JSONCROSS-Site ScriptingAction” ein, gefolgt von den zu aktivierenden Aktionen.

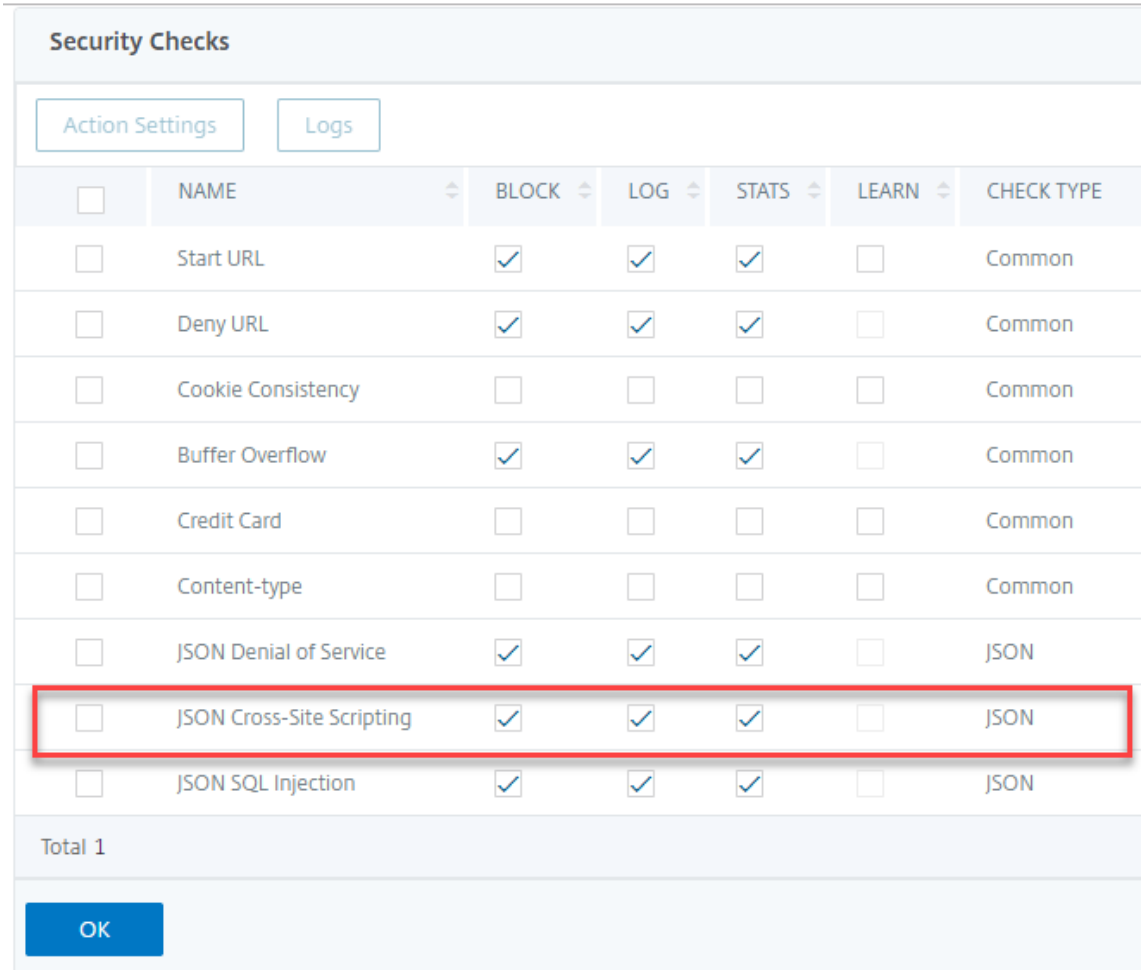
Beispiel

```
set appfw profile profile1 -JSONSQLInjectionAction block log stat
```

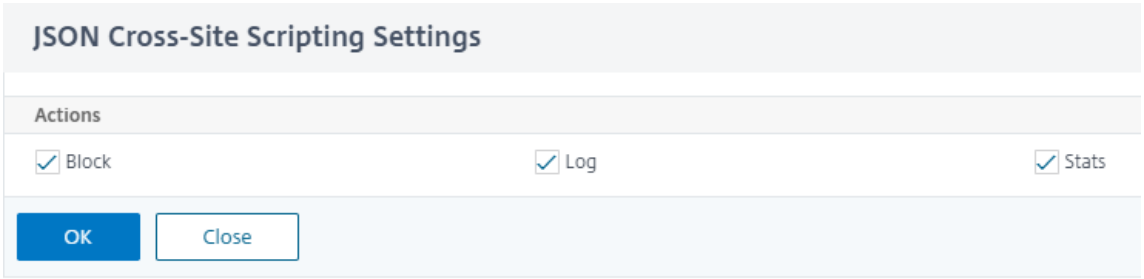
Konfigurieren des JSON Cross Site Scripting (Cross-Site-Scripting) -Schutzes mit Citrix GUI

Befolgen Sie die nachstehenden Schritte, um die Cross Site Scripting (Cross-Site Scripting) -Schutzeinstellungen festzulegen.

1. Navigieren Sie im Navigationsbereich zu **Sicherheit** > **Profile**.
2. Klicken Sie auf der Seite **Profile** auf **Hinzufügen**.
3. Klicken Sie auf der Seite **Citrix Web App Firewall Profile** unter **Erweiterte Einstellungen** auf **Sicherheitsprüfungen**.
4. Gehen Sie im Abschnitt **Sicherheitsüberprüfungen** zu **JSON Cross-Site Scripting (Cross-Site-Scripting)** -Einstellungen.
5. Klicken Sie auf das Symbol für die ausführbare Datei neben dem Kontrollkästchen.

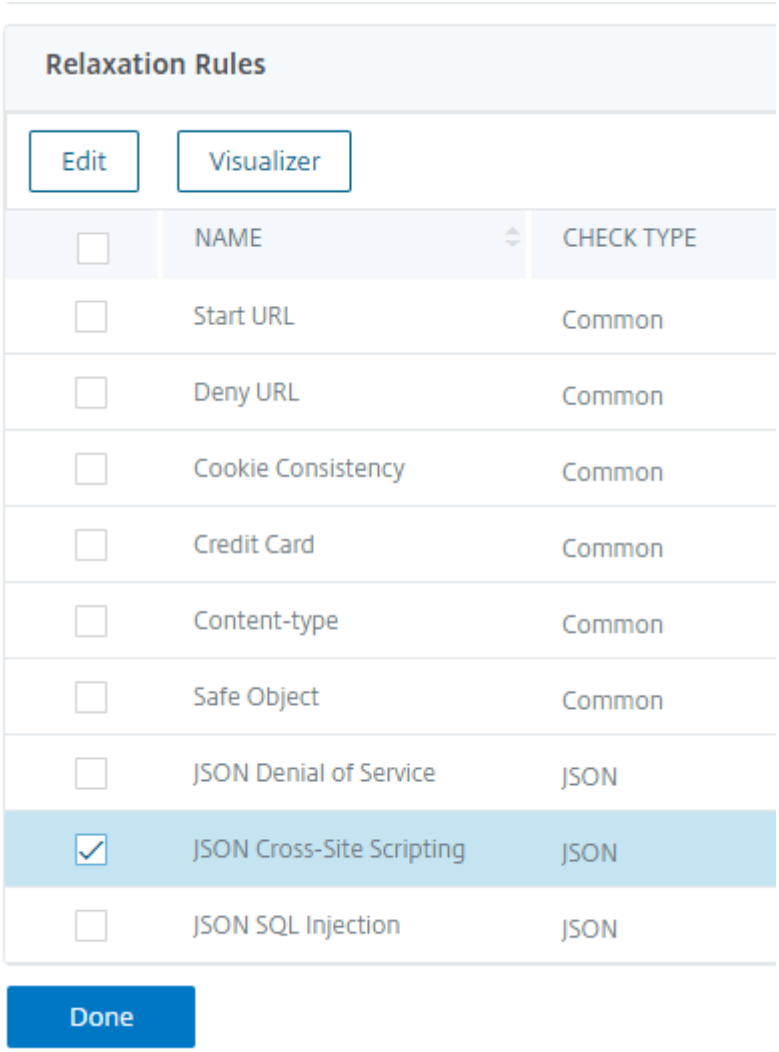


6. Klicken Sie auf **Aktionseinstellungen**, um die Seite **JSON Cross-Site Scripting Settings** aufzurufen.
7. Wählen Sie die JSON Cross-Site Scripting Aktionen aus.
8. Klicken Sie auf **OK**.

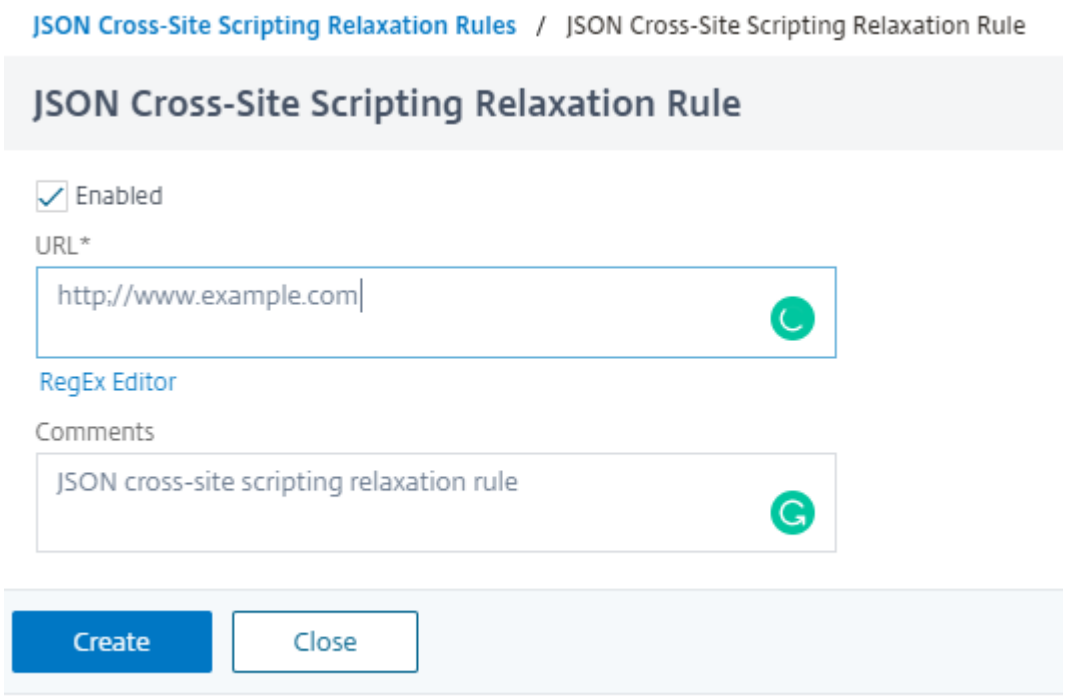


9. Klicken Sie auf der Seite **Citrix Web App Firewall Profil** unter **Erweiterte Einstellungen** auf **Relaxationsregeln**.
10. Wählen Sie im Abschnitt **Relaxationsregeln** JSON Cross-Site Scripting Settings aus, und klicken

Sie auf **Bearbeiten** .



11. Klicken Sie auf der Seite **JSON Cross-Site Scripting Relaxation Rule** auf **Hinzufügen**, um eine JSON Cross-Site Scripting Relaxationsregel hinzuzufügen.
12. Geben Sie die URL ein, an die die Anforderung gesendet werden soll. Alle Anfragen, die an diese URL gesendet werden, werden nicht gesperrt.
13. Klicken Sie auf **Erstellen**.



JSON-Befehlseinschleusungsprüfung

January 25, 2022

Die JSON-Befehlseinschleusungsprüfung untersucht den eingehenden JSON-Datenverkehr auf nicht autorisierte Befehle, die die Systemsicherheit beeinträchtigen oder das System modifizieren. Wenn bei der Untersuchung des Datenverkehrs schädliche Befehle erkannt werden, blockiert die Appliance die Anforderung oder führt die konfigurierte Aktion aus.

Bei einem Befehlseinschleusungsangriff zielt der Angreifer darauf ab, nicht autorisierte Befehle auf dem Citrix ADC-Betriebssystem oder dem Backend-Server auszuführen. Um dies zu erreichen, schleust der Angreifer Betriebssystembefehle über eine anfällige Anwendung ein. Die Back-End-Anwendung ist anfällig für Einschleusungsangriffe, wenn die Appliance eine Anfrage einfach ohne Sicherheitsüberprüfung weiterleitet. Daher ist es sehr wichtig, eine Sicherheitsüberprüfung zu konfigurieren, damit die Citrix ADC-Appliance Ihre Webanwendung schützen kann, indem sie unsichere Daten blockiert.

So funktioniert der Befehlseinschleusungsschutz

1. Bei einer eingehenden JSON-Anforderung untersucht WAF den Datenverkehr auf Schlüsselwörter oder Sonderzeichen. Wenn die JSON-Anforderung keine Muster enthält, die mit einem

der verweigerten Schlüsselwörter oder Sonderzeichen übereinstimmen, ist die Anforderung zulässig. Andernfalls wird die Anforderung basierend auf der konfigurierten Aktion blockiert, verworfen oder umgeleitet.

2. Wenn Sie es vorziehen, ein Schlüsselwort oder ein Sonderzeichen von der Liste auszunehmen, können Sie eine Entspannungsregel erstellen, um die Sicherheitsüberprüfung unter bestimmten Bedingungen zu Bypass.
3. Sie können die Protokollierung aktivieren, um Protokollmeldungen zu generieren Sie können die Protokolle überwachen, um festzustellen, ob Antworten auf legitime Anfragen blockiert werden. Ein starker Anstieg der Anzahl der Protokollmeldungen kann auf Versuche hinweisen, einen Angriff zu starten.
4. Sie können die Statistikfunktion auch aktivieren, um statistische Daten zu Verstößen und Protokollen zu sammeln. Ein unerwarteter Anstieg im Statistikzähler deutet möglicherweise darauf hin, dass Ihre Anwendung angegriffen wird. Wenn legitime Anforderungen blockiert werden, müssen Sie möglicherweise die Konfiguration erneut aufrufen, um festzustellen, ob Sie die neue Entspannungsregel konfigurieren oder die vorhandene ändern müssen.

Schlüsselwörter und Sonderzeichen, die für die Befehlseinschleusung verweigert werden

Zum Erkennen und Blockieren von JSON-Befehlseinschleusungsangriffen hat die Appliance über eine Reihe von Mustern (Schlüsselwörter und Sonderzeichen), die in der Standardsignaturdatei definiert sind. Es folgt eine Liste der blockierten Schlüsselwörter beim Erkennen von Befehlseinschleusungsverstößen

```
<commandinjection>
      <keyword type="LITERAL" builtin="ON">7z</keyword>
      <keyword type="LITERAL" builtin="ON">7za</keyword>
      <keyword type="LITERAL" builtin="ON">7zr</keyword>
...
</commandinjection>

<!--NeedCopy-->
```

In der Signaturdatei definierte Sonderzeichen sind:
`| ; & $ > < '\ ! >> ##`

Konfigurieren der JSON-Befehlseinschleusungsprüfung über die CLI

In der Befehlszeilenschnittstelle können Sie entweder den Befehl set appfw profile verwenden oder einen appfw-Profilbefehl hinzufügen, um die JSON-Befehlseinschleusungseinstellungen zu konfiguri-

eren. Sie können die Block-, Protokoll- und Statistikaktionen aktivieren. Sie müssen auch den Befehlseinschleusungstyp wie Schlüsselwörter und Zeichenfolgenzeichen festlegen, die Sie in den Nutzdaten erkennen möchten.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set appfw profile <profile-name> -cmdInjectionAction <action-name> -CMDInjectionType
 <CMDInjectionType>]
```

> **Hinweis:**
>
> Standardmäßig ist die Befehlseinschleusungsaktion auf “Protokollstatistiken blockieren” festgelegt. Außerdem wird der Standardeinschleusungsstyp des Befehls als festgelegt `CmdSplCharANDKeyWord`. Nach einem Upgrade ist für die vorhandenen Web-App-Firewall-Profile die Aktion auf “Keine” festgelegt.

Beispiel:

```
set appfw profile profile1 -JSONCMDInjectionAction block -JSONCMDInjectionType
 CmdSplChar
```

Dabei sind die verfügbaren JSON-Befehlseinschleusungsaktionen:

Keine — Deaktiviert den Befehlseinschleusungsschutz.
Log — Protokollieren von Befehlseinschleusungsverstößen für die Sicherheitsprüfung
Blockieren - blockiert Datenverkehr, der gegen die Befehlseinschleusungsüberprüfung verstößt.
Statistik - Generiert Statistiken für Sicherheitsverletzungen durch Befehlseinschleusung.

Dabei sind die verfügbaren JSON-Befehlseinschleusungstypen:

`Cmd SplChar` - Prüft Sonderzeichen
`CmdKeyWord` - Prüft Schlüsselwörter zur Befehlseinschleusung
`CmdSplCharANDKeyWord` - Dies ist die Standardaktion. Die Aktion prüft Sonderzeichen und Befehlseinschleusung. Schlüsselwörter und Blöcke nur, wenn beide vorhanden sind.
`CmdSplCharORKeyWord` - Überprüft Sonderzeichen und Befehlseinschleusungsschlüsselwörter und blockiert, wenn gefunden.

Konfigurieren der Entspannungsregeln für die JSON-Befehlseinschleusungsprüfung

Wenn Ihre Anwendung erfordert, dass Sie die JSON-Befehlseinschleusungsprüfung für ein bestimmtes ELEMENT oder ATTRIBUTE in der Nutzlast umgehen müssen, können Sie eine Entspannungsregel konfigurieren.

Die Entspannungsregeln für die JSON-Befehlseinschleusungsprüfung haben folgende Syntax.

```
bind appfw profile <profile name> -JSONCMDURL <expression> -comment <string
> -isAutoDeployed ( AUTODEPLOYED | NOTAUTODEPLOYED )-state ( ENABLED |
DISABLED )
```


Beispiel für Relaxationsregel für Regex im Header

```
bind appfw profile abc_json -jsoncmDURL http://1.1.1.1/hello.html
```

Im Folgenden werden Anfragen von allen auf 1.1.1.1 gehosteten URLs gelockert:

```
bind appfw profile abc_json -jsoncmDURL http://1.1.1.1/*"
```

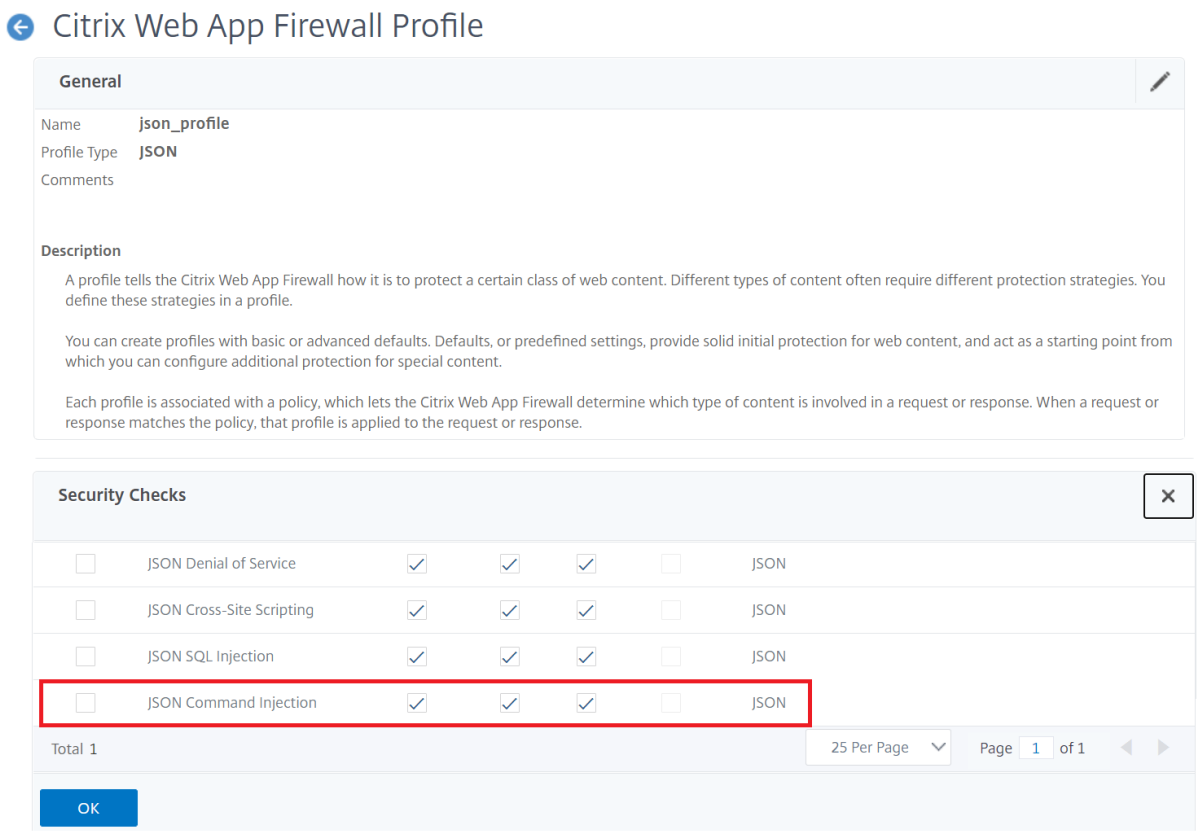
Um die Entspannung zu entfernen, verwenden Sie "unbind".

```
unbind appfw profile abc_json -jsoncmDURL  " http://1.1.1.1/*"
```

Konfigurieren der JSON-Befehlseinschleusungsprüfung über die GUI

Führen Sie die folgenden Schritte aus, um die JSON-Befehlseinschleusungsprüfung zu konfigurieren.

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall und Profile**.
2. Wählen Sie auf der Seite **Profile** ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Wechseln Sie auf der **Citrix Web App Firewall Profilseite** zum Abschnitt **Erweiterte Einstellungen** und klicken Sie auf **Sicherheitsprüfungen**.

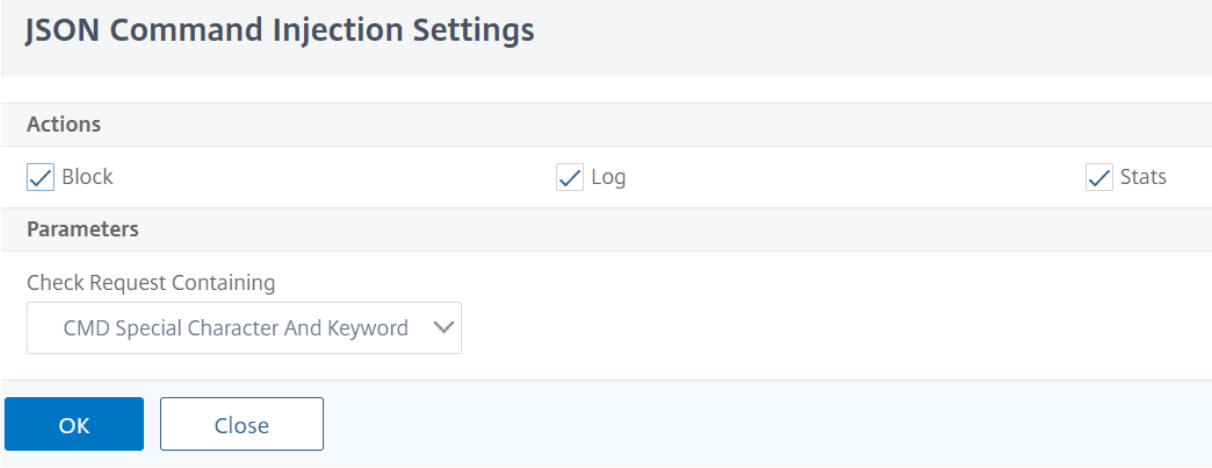


1. Wählen Sie im Abschnitt **Sicherheitsüberprüfungen** die Option **JSON-Befehlseinschleusung** aus und klicken Sie auf**Aktion**.

2. Stellen Sie auf der Seite **JSON-Befehlseinschleusungseinstellungen** die folgenden Parameter ein

   a) Aktionen. Wählen Sie eine oder mehrere Aktionen für die Sicherheitsüberprüfung der JSON-Befehlseinschleusung aus.
   b) Überprüfen Sie die Anfrage enthält. Wählen Sie ein Befehlseinschleusungsmuster, um zu überprüfen, ob die eingehende Anforderung das Muster enthält.

3. Klicken Sie auf **OK**.



Anzeigen von Statistiken zum Befehlseinschleusungsdatenverkehr und -verletzungen

Auf der Seite " **Citrix Web App Firewall Statistics** " werden Details zu Sicherheitsdatenverkehr und Sicherheitsverletzungen in einem tabellarischen oder grafischen Format angezeigt.

So zeigen Sie Sicherheitsstatistiken mithilfe der Befehlszeilenschnittstelle an.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat appfw profile profile1
```

Appfw-Profil Verkehrsstatistiken	Geschwindigkeit (/s)	Gesamt
Anfragen	0	0
Byte anfragen	0	0
Antworten	0	0
Antwort Byte	0	0
Bricht ab	0	0
Leitet	0	0

Appfw-Profil Verkehrsstatistiken	Geschwindigkeit (/s)	Gesamt
Langfristige Reaktionszeit (ms)	–	0
Letzte Reaktionszeit von Ave (ms)	–	0

Statistiken zu HTML/XML/JSON-Verstößen	Geschwindigkeit (/s)	Gesamt
Start-URL	0	0
URL verweigern	0	0
Referer-Header	0	0
Pufferüberlauf	0	0
Cookie-Konsistenz	0	0
Cookie-Entführung	0	0
CSRF-Formular-Tag	0	0
Site-übergreifendes HTML	0	0
HTML SQL injection	0	0
Feld-Format	0	0
Field consistency	0	0
Kreditkarte	0	0
Sicheres Objekt	0	0
Verstöße gegen die Signatur	0	0
Inhaltstyp	0	0
JSON-Denial-of-Service-Angriff	0	0
JSON-SQL-Einschleusung	0	0
JSON-Cross-Site Scripting	0	0
Dateiuploadtyp	0	0
Ableiten der XML-Nutzlast für Inhaltstypen	0	0
HTML-Befehlseinschleusung	0	0

Statistiken zu HTML/XML/JSON-Verstößen	Geschwindigkeit (/s)	Gesamt
XML-Format	0	0
XML-Denial-of-Service-Angriff (XDoS)	0	0
XML-Nachrichtenüberprüfung	0	0
Interoperabilität der Webdienste	0	0
XML SQL Injection	0	0
Site-übergreifende XML-Skrip	0	0
XML-Anhang	0	0
SOAP-Fehlerverletzungen	0	0
Generische XML-Verstöße	0	0
Verstöße insgesamt	0	0

HTML/XML/JSON-Protokollstatistiken	Geschwindigkeit (/s)	Gesamt
Starten der URL-Protokolle	0	0
URL-Protokolle verweigern	0	0
Referer-Header-Protokolle	0	0
Pufferüberlauf-Protokolle	0	0
Protokolle zur Cookie-Konsistenz	0	0
Protokolle zur Cookie-Entführung	0	0
CSRF aus Tag-Protokollen	0	0
HTML-Cross-Site Scripting-Protokolle	0	0
HTML Cross-Site Scripting-Transformationsprotokolle	0	0
HTML SQL-Einschleusungsprotokolle	0	0

HTML/XML/JSON-Protokollstatistiken	Geschwindigkeit (/s)	Gesamt
HTML SQL Transformationsprotokolle	0	0
Protokolle im Feldformat	0	0
Protokolle zur Feldkonsistenz	0	0
Kreditkarten	0	0
Protokolle zur Kreditkarten-Transformation	0	0
Sichere Objektprotokolle	0	0
Signatur-Protokolle	0	0
Inhalts-Typ-Protokolle	0	0
JSON-Denial-of-Service-Protokolle	0	0
JSON SQL-Einschleusungsprotokolle	0	0
JSON-Site-Scripting-Protokolle	0	0
Protokolle zum Hochladen von Dateien	0	0
Ableiten der XML-Nutzlast des Inhaltstyps L	0	0
JSON-CMD-Einschleusung	0	0
HTML-Befehlseinschleusungsprotokol	0	0
Protokolle im XML-Format	0	0
XML Denial of Service (XDoS) -Protokolle	0	0
Protokolle zur XML-Nachrichtenüberprüfung	0	0
WSI-Protokolle	0	0
XML SQL Injection-Protokolle	0	0
XML-Cross-Site Scripting-Protokolle	0	0

HTML/XML/JSON-Protokollstatistiken	Geschwindigkeit (/s)	Gesamt
Protokolle für XML-Anhänge	0	0
SOAP-Fehlerlogs	0	0
Generische XML-Protokolle	0	0
Gesamtzahl der Protokollmeldungen	0	0

Statistikrate der Serverfehlerantwort (/s) | Gesamt |
|—|–|–|
HTTP Client Errors (4xx Resp) | 0 | 0|
HTTP Server Errors (5xx Resp) | 0 | 0 |

HTML/XML/JSON-Protokollstatistiken	Geschwindigkeit (/s)	Gesamt
JSON-Command Injection-	0	0
Protokolle im XML-Format	0	0

Anzeigen von JSON-Befehlseinschleusungsstatistiken über die Citrix ADC GUI

Führen Sie die folgenden Schritte aus, um Befehlseinschleusungsstatistiken anzuzeigen:

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich ein Web App Firewall-Profil aus und klicken Sie auf **Statistiken**.
3. Auf der Seite **Citrix Web App Firewall Statistics** werden die Details zum JSON-Befehlseinschleusungsverkeh
   und Verstößen angezeigt.
4. Sie können **Tabellarische Ansicht** wählen oder zur **grafischen Ansicht** wechseln, um die Daten
   in einem tabellarischen oder grafischen Format anzuzeigen.

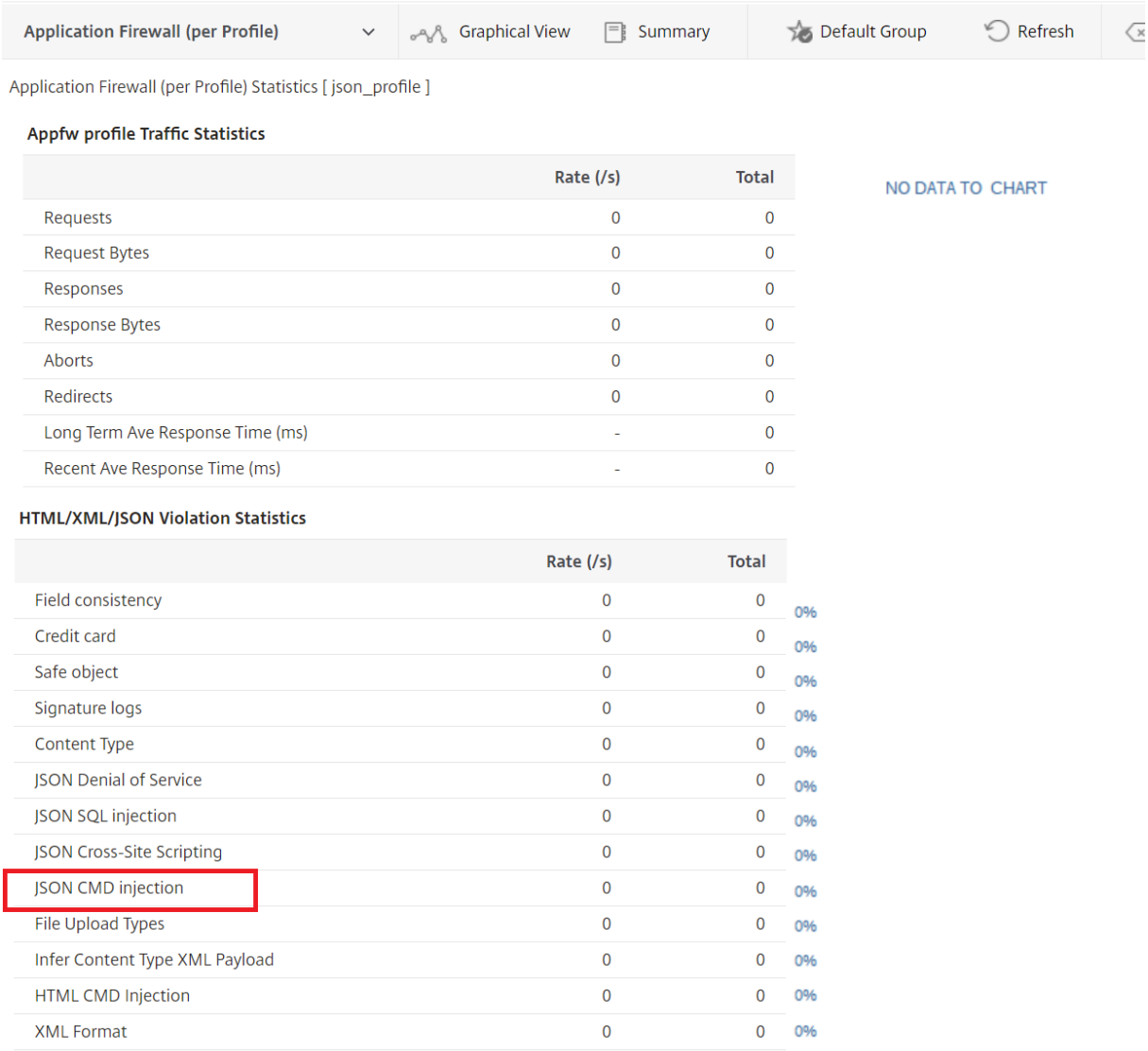
JSON-Befehlseinschleusungverkehrsstatistiken

HTML/XML/JSON Log Statistics

	Rate (/s)	Total
Start URL logs	0	0
Deny URL logs	0	0
Field consistency logs	0	0
Credit cards	0	0
Credit card transform logs	0	0
Safe object logs	0	0
Signature logs	0	0
Content Type logs	0	0
JSON Denial of Service logs	0	0
JSON SQL injection logs	0	0
JSON Cross-Site Scripting logs	0	0
JSON CMD injection logs	0	0
File upload types logs	0	0
Infer Content Type XML Payload Logs	0	0

JSON CMD injection logs: X
Number of JSON Command Injection security check log messages generated by the Application Firewall.

Statistiken zu JSON-Befehlseinschleusungsverstößen



Verwalten von Inhaltstypen

October 5, 2021

Webserver fügen für jeden Inhaltstyp einen Content-Type-Header mit einer MIME/Typ-Definition hinzu. Webserver bedienen viele verschiedene Arten von Inhalten. Zum Beispiel wird Standard-HTML der MIME-Typ text/html zugewiesen. JPG-Bildern werden dem Inhaltstyp image/jpeg oder image/jpg zugewiesen. Ein normaler Webserver kann verschiedene Inhaltstypen bereitstellen, die alle im Content Type Header durch den zugewiesenen MIME/Type definiert sind.

Viele Web App Firewall Filterregeln dienen dem Filtern eines bestimmten Inhaltstyps. Die Filterregeln gelten für einen Inhaltstyp wie HTML und sind oft ungeeignet, wenn ein anderer Inhaltstyp (z. B.

Bilder) gefiltert wird. Daher versucht die Web App Firewall, den Inhaltstyp von Anforderungen und Antworten zu bestimmen, bevor sie gefiltert werden. Wenn ein Webserver oder Browser einer Anforderung oder Antwort keinen Content-Type-Header hinzufügt, wendet die Web App Firewall einen Standard-Inhaltstyp an und filtert den Inhalt entsprechend.

Der Standard-Inhaltstyp ist normalerweise "application/octet-stream" mit der generischsten MIME/Typ-Definition. Der MIME/Typ ist für jeden Inhaltstyp geeignet, den ein Webserver wahrscheinlich bereitstellen wird. Der Web App Firewall stellt jedoch nicht viele Informationen zur Verfügung, damit die entsprechende Filterung ausgewählt werden kann. Wenn ein geschützter Webserver so konfiguriert ist, dass genaue Inhaltstypheader hinzugefügt werden, können Sie dann ein Profil für den Webserver erstellen und ihm einen Standard-Inhaltstyp zuweisen. Dies geschieht, um sowohl die Geschwindigkeit als auch die Genauigkeit der Filterung zu verbessern.

Sie können auch eine Liste der zulässigen Anforderungsinhaltstypen für ein bestimmtes Profil konfigurieren. Wenn diese Funktion konfiguriert ist und die Web App Firewall eine Anforderung filtert, die nicht mit einem der zulässigen Inhaltstypen übereinstimmt, blockiert sie die Anforderung. Nach dem Upgrade von Version 10.5 auf 11.0 werden unbekannte Inhaltstypen, die nicht in der Standardliste für zulässige Inhaltstypen enthalten sind, nicht gebunden. Sie können andere Inhaltstypen hinzufügen, die Sie den entspannten Regeln erlauben möchten.

Anfragen müssen immer entweder vom Typ "application/x-www-form-urlencoded", "multipart/form-data" oder "text/x-gwt-rpc" sein. Die Web App Firewall blockiert alle Anforderungen, die einen anderen Inhaltstyp festgelegt haben.

> **Hinweis:**
>
> Sie können die Inhaltstypen application/x-www-form-urlencoded oder multipart/form-data nicht in die Liste der zulässigen Antwort-Inhaltstypen aufnehmen.

So legen Sie den Standardanforderungsinhaltstyp mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw profile <name> -requestContentType <type>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Inhaltstyp text/html als Standard für das angegebene Profil festgelegt:

```
1 set appfw profile profile1 -requestContentType "text/html"
2 save ns config
```



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

So entfernen Sie den benutzerdefinierten Standardanforderungstyp mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `unset appfw profile <name> -requestContentType <type>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Standardinhaltstyp text/html für das angegebene Profil aufgehoben, wodurch der Typ auf application/octet-stream zurückgesetzt wird:

```
unset appfw profile profile1 -requestContentType "text/html"
save ns config
<!--NeedCopy-->
```

> **Hinweis:**
>
> Verwenden Sie immer den letzten Content-Type-Header für die Verarbeitung und entfernen Sie verbleibende Content-Type-Header, falls vorhanden, die sicherstellt, dass der Back-End-Server eine Anforderung mit nur einem Inhaltstyp empfängt.
>
> Um Anforderungen zu blockieren, die umgangen werden können, fügen Sie eine Web App Firewall Richtlinie mit der Regel HTTP.REQ.HEADER ("content-type") .COUNT.GT (1) 'und Profil als *appfw_block*hinzu.
>
> Wenn eine Anforderung ohne Content-Type-Header empfangen wird oder wenn die Anforderung Content-Type-Header ohne Wert hat, wendet Web App Firewall den konfigurierten **RequestContentType-Wert** an und verarbeitet die Anforderung entsprechend.

So legen Sie den Standard-Antwort-Inhaltstyp mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw profile <name> -responseContentType <type>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Inhaltstyp text/html als Standard für das angegebene Profil festgelegt:

```
set appfw profile profile1 -responseContentType ”text/html”
save ns config
<!--NeedCopy-->
```

So entfernen Sie den benutzerdefinierten Standardantwortinhaltstyp mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `unset appfw profile <name> -responseContentType <type>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Standardinhaltstyp text/html für das angegebene Profil aufgehoben, wodurch der Typ auf application/octet-stream zurückgesetzt wird:

```
unset appfw profile profile1 -responseContentType ”text/html”
save ns config
<!--NeedCopy-->
```

So fügen Sie mit der Befehlszeilenschnittstelle einen Inhaltstyp zur Liste zulässiger Inhaltstypen hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `bind appfw profile <name> -ContentType <contentTypeName>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Inhaltstyp text/shtml zur Liste zulässiger Inhaltstypen für das angegebene Profil hinzugefügt:


```
bind appfw profile profile1 -contentType ”text/shtml”
save ns config
<!--NeedCopy-->
```

So entfernen Sie einen Inhaltstyp aus der Liste zulässiger Inhaltstypen mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `unbind appfw profile <name> -ContentType <contentTypeName>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Inhaltstyp text/shtml aus der Liste zulässiger Inhaltstypen für das angegebene Profil entfernt:

```
unbind appfw profile profile1 -contentType ”text/shtml”
save ns config
<!--NeedCopy-->
```

Verwalten von URL-kodierten und mehrteiligen Inhaltstypen

Mit der Citrix ADC Web App Firewall können Sie nun URLencoded und Multipart-Formular-Inhaltstypen für Formulare konfigurieren. Die Inhaltstypkonfiguration ähnelt XML- und JSON-Liste. Basierend auf der Konfiguration klassifiziert Web App Firewall die Anforderungen und prüft auf Inhaltstyp urlencoded oder multipart-form.

So konfigurieren Sie Web App Firewall-Profil mit Inhaltstypen urlencoded oder multipart-form
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind appfw profile p2 -contentType <string>
```

Beispiel:

```
bind appfw profile p2 -contentType UrlencodedFormContentType

bind appfw profile p2 -ContentType appfwmultipartform
```

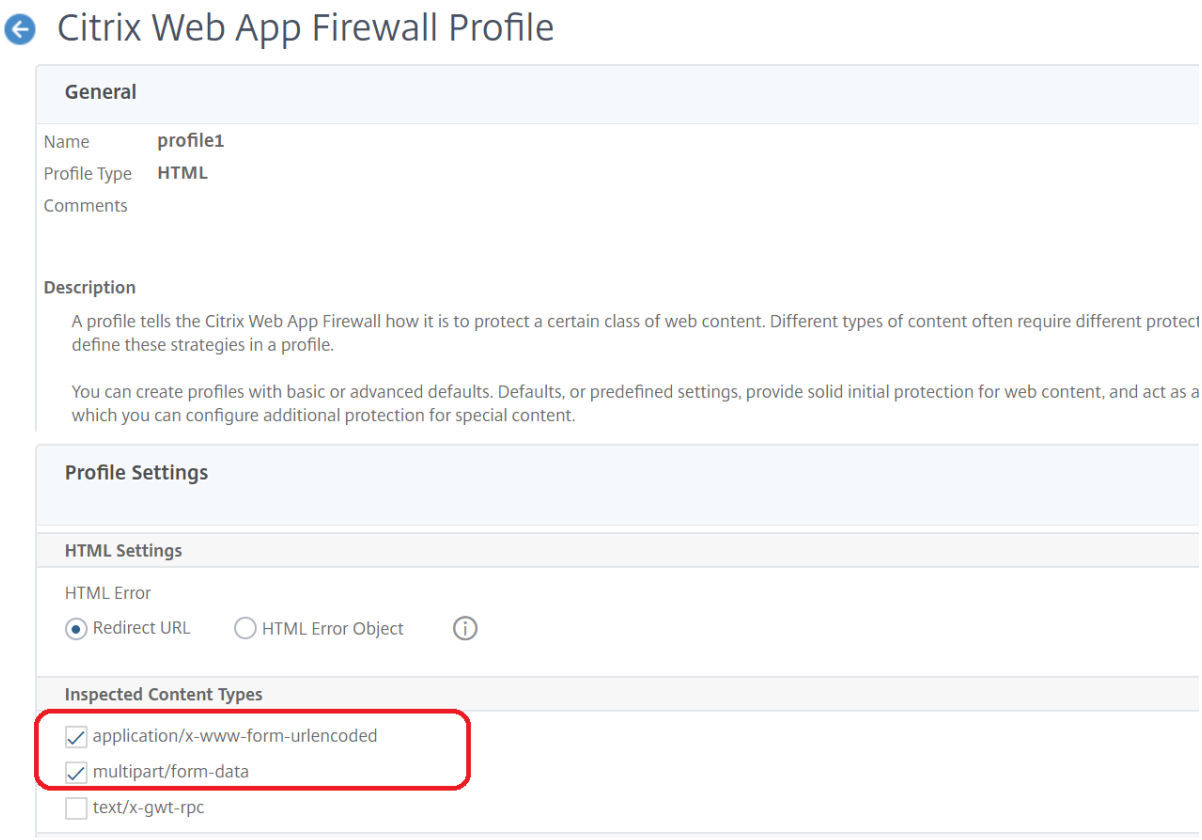
So verwalten Sie die standardmäßigen und zulässigen Inhaltstypen mit der GUI

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Profile** .

2. Wählen Sie im Detailbereich das Profil aus, das Sie konfigurieren möchten, und klicken Sie dann auf **Bearbeiten**. Das Dialogfeld **Web App Firewall Profil konfigurieren** wird angezeigt.
3. Klicken Sie im Dialogfeld **Web App Firewall Profil konfigurieren** auf die Registerkarte **Einstellungen**.
4. Führen Sie auf der Registerkarte **Einstellungen** einen Bildlauf nach unten in den Bereich Inhaltstyp durch.
5. Konfigurieren Sie im Bereich Inhaltstyp den Standardinhaltstyp für Anforderung oder Antwort:
   - Um den Standardanforderungsinhaltstyp zu konfigurieren, geben Sie die MIME/Typ-Definition des Inhaltstyps, den Sie verwenden möchten, in das Textfeld Standardanforderung ein.
   - Um den Standardantwortinhaltstyp zu konfigurieren, geben Sie die MIME/Typ-Definition des Inhaltstyps, den Sie verwenden möchten, in das Textfeld Standardantwort ein.
   - Klicken Sie auf **Hinzufügen**, um einen neuen zulässigen Inhaltstyp zu erstellen. Das Dialogfeld **Zulässigen Inhaltstyp hinzufügen** wird angezeigt.
   - Um einen vorhandenen zulässigen Inhaltstyp zu bearbeiten, wählen Sie diesen Inhaltstyp aus, und klicken Sie dann auf **Öffnen**. Das Dialogfeld **Zulässiger Inhaltstyp ändern** wird angezeigt.
6. Um die zulässigen Inhaltstypen zu verwalten, klicken Sie auf Zulässige Inhaltstypen verwalten.
7. Um einen neuen Inhaltstyp hinzuzufügen oder einen vorhandenen Inhaltstyp zu ändern, klicken Sie auf Hinzufügen oder Öffnen, und führen **Sie im Dialogfeld Zulässigen Inhaltstyp hinzufügen** oder **Zulässigen Inhaltstyp ändern** die folgenden Schritte aus.
   a) Aktivieren bzw. deaktivieren Sie das Kontrollkästchen Aktiviert, um den Inhaltstyp in die Liste der zulässigen Inhaltstypen aufzunehmen oder ihn auszuschließen.
   b) Geben Sie im Textfeld Inhaltstyp einen regulären Ausdruck ein, der den Inhaltstyp beschreibt, den Sie hinzufügen möchten, oder ändern Sie den vorhandenen regulären Ausdruck des Inhaltstyps.
   Inhaltstypen werden genau wie MIME-Typbeschreibungen formatiert.
   > **Hinweis:**
   > Sie können jeden gültigen MIME-Typ in die Liste zulässiger Inhaltstypen aufnehmen. Da viele Arten von Dokumenten aktiven Inhalt enthalten können und daher möglicherweise schädliche Inhalte enthalten können, müssen Sie beim Hinzufügen von MIME-Typen zu dieser Liste Vorsicht walten lassen.
   c) Geben Sie eine kurze Beschreibung an, in der der Grund für das Hinzufügen dieses bestimmten MIME-Typs zur Liste zulässiger Inhaltstypen erläutert wird.
   d) Klicken Sie auf **Erstellen** oder **OK**, um die Änderungen zu speichern.
8. Klicken Sie auf **Schließen**, um das Dialogfeld Zulässige Inhaltstypen verwalten zu schließen und zur Registerkarte **Einstellungen** zurückzukehren.
9. Klicken Sie auf **OK**, um die Änderungen zu speichern.

So verwalten Sie URLencoded und Multipart-Formular-Inhaltstypen mit der Citrix ADC GUI

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Profile** .
2. Wählen Sie im Detailbereich das Profil aus, das Sie konfigurieren möchten, und klicken Sie dann auf **Bearbeiten**.
3. Wählen **Sie auf der Seite Web App Firewall Profil konfigurieren** die **Profileinstellungen** im Abschnitt **Erweiterte Einstellungen** aus.
4. Legen Sie im Abschnitt **Geprüfte Inhaltstyp** die folgenden Parameter fest:
   a) application/x-www-form-urlencoded. Aktivieren Sie das Kontrollkästchen, um den Inhaltstyp Urlencoded zu überprüfen.
   b) multipart/form-data. Aktivieren Sie die Prüfung, um den Inhaltstyp Multipart-Form zu überprüfen.
5. Klicken Sie auf **OK**.



Profile

October 5, 2021

Ein Profil ist eine Sammlung von Sicherheitseinstellungen, die zum Schutz bestimmter Arten von Webinhalten oder bestimmten Teilen Ihrer Website verwendet werden. In einem Profil bestimmen Sie, wie die Web App Firewall jeden ihrer Filter (oder Prüfungen) auf Anfragen an Ihre Websites und Antworten von ihnen anwendet. Die Web App Firewall unterstützt zwei Arten von Profilen: vier integrierte (Standard-) Profile, für die keine weitere Konfiguration erforderlich ist, und benutzerdefinierte Profile, die eine weitere Konfiguration erfordern.

Eingebaute Profile

Die vier integrierten Web App Firewall -Profile bieten einfachen Schutz für Anwendungen und Websites, die entweder keinen Schutz benötigen oder auf die Benutzer überhaupt nicht direkt zugreifen dürfen. Folgende Profiltypen sind:

- **APPFW_BYPASS.** Überspringt die gesamte Filterung der Web App Firewall und sendet den unveränderten Datenverkehr an die geschützte Anwendung oder Website oder an den Client.
- **APPFW_RESET.** Setzt die Verbindung zurück und erfordert, dass der Client seine Sitzung wiederherstellt, indem er eine bestimmte Startseite besucht.
- **APPFW_DROP.** Lässt den gesamten Datenverkehr zur oder von der geschützten Anwendung oder Website fallen und sendet keinerlei Antwort an den Kunden.
- **APPFW_BLOCK.** Blockiert den Datenverkehr zu oder von der geschützten Anwendung oder Website.

Sie verwenden die integrierten Profile genau wie benutzerdefinierte Profile, indem Sie eine Richtlinie konfigurieren, die den Datenverkehr auswählt, auf den Sie das Profil anwenden möchten, und dann das Profil Ihrer Richtlinie zuordnen. Da Sie keine integrierte Richtlinie konfigurieren müssen, bietet sie eine schnelle Möglichkeit, bestimmte Arten von Datenverkehr oder Datenverkehr zuzulassen oder zu blockieren, die an bestimmte Anwendungen oder Websites gesendet werden.

Benutzerdefinierte Profile

Benutzerdefinierte Profile sind Profile, die von Benutzern erstellt und konfiguriert werden. Im Gegensatz zu den Standardprofilen müssen Sie ein benutzerdefiniertes Profil konfigurieren, bevor es den Datenverkehr zu und von Ihren geschützten Anwendungen filtert.

Es gibt drei Arten von benutzerdefinierten Profilen:

- **HTML.** Schützt HTML-basierte Webseiten.
- **XML.** Schützt XML-basierte Webservices und Websites.

- **Web 2.0.** Schützt Web 2.0-Inhalte, die HTML- und XML-Inhalte wie ATOM-Feeds, Blogs und RSS-Feeds kombinieren.

Die Web App Firewall verfügt über eine Reihe von Sicherheitsprüfungen, die alle aktiviert oder deaktiviert werden können und in jedem Profil auf verschiedene Arten konfiguriert werden können. Jedes Profil verfügt außerdem über eine Reihe von Einstellungen, mit denen gesteuert wird, wie verschiedene Inhaltstypen verarbeitet werden. Statt alle Sicherheitsprüfungen manuell zu konfigurieren, können Sie die Lernfunktion aktivieren und konfigurieren. Diese Funktion beobachtet den normalen Datenverkehr zu Ihren geschützten Websites für einen bestimmten Zeitraum und verwendet diese Beobachtungen, um Ihnen eine maßgeschneiderte Liste empfohlener Ausnahmen (*Entspannungen*) für einige Sicherheitskontrollen und zusätzliche Regeln für andere Sicherheitsprüfungen zu liefern.

Bei der Erstkonfiguration, sei es, ob Sie den Web App Firewall Wizard oder manuell verwenden, erstellen Sie normalerweise ein Allzweckprofil, um alle Inhalte auf Ihren Websites zu schützen, die nicht von einem spezifischeren Profil abgedeckt werden. Danach können Sie so viele spezifische Profile erstellen, wie Sie spezialisierte Inhalte schützen möchten.

Der Bereich Profile besteht aus einer Tabelle, die die folgenden Elemente enthält:

Name. Zeigt alle Web App Firewall Profile an, die in der Appliance konfiguriert sind.

Gebundene Signatur. Zeigt das Signaturobjekt an, das an das Profil in der vorherigen Spalte gebunden ist, sofern vorhanden.

Richtlinien. Zeigt die Web App Firewall Richtlinie an, die das Profil in der Spalte ganz links dieser Zeile aufruft, sofern vorhanden.

Kommentare. Zeigt den dem Profil zugeordneten Kommentar in der Spalte ganz links dieser Zeile an.

Profiltyp. Zeigt den Profiltyp an. Typen sind Built-in, HTML, XML und Web 2.0.

Über der Tabelle befindet sich eine Reihe von Schaltflächen und eine Dropdownliste, mit der Sie Informationen zu Ihren Profilen erstellen, konfigurieren, löschen und anzeigen können:

- **Add.** Fügen Sie der Liste ein neues Profil hinzu.
- **Bearbeiten.** Bearbeiten Sie das ausgewählte Profil.
- **Löschen.** Löschen Sie das ausgewählte Profil aus der Liste.
- **Statistik.** Zeigen Sie die Statistiken für das ausgewählte Profil an.
- **Aktion.** Dropdownliste, die zusätzliche Befehle enthält. Derzeit können Sie ein Profil importieren, das aus einer anderen Web App Firewall Konfiguration exportiert wurde.

Erstellen von Web App Firewall-Profilen

October 5, 2021

Sie können ein Web App Firewall-Profil auf zwei Arten erstellen: über die Befehlszeile und mithilfe der GUI. Das Erstellen eines Profils mit der Befehlszeile erfordert, dass Sie Optionen in der Befehlszeile angeben. Der Prozess ähnelt dem Konfigurieren eines Profils, und mit wenigen Ausnahmen nehmen die beiden Befehle dieselben Parameter an.

Das Erstellen eines Profils mit der GUI erfordert, dass Sie nur zwei Optionen angeben. Sie geben grundlegende oder erweiterte *Standardeinstellungen*an, die Standardkonfiguration für die verschiedenen Sicherheitsprüfungen und Einstellungen, die Teil eines Profils sind, und wählen den *Profiltyp* aus, der dem Inhaltstyp entspricht, den das Profil schützen soll. Sie können optional auch einen Kommentar hinzufügen. Nachdem Sie das Profil erstellt haben, müssen Sie es dann konfigurieren, indem Sie es im Datenbereich auswählen und dann auf **Bearbeiten**klicken.

Wenn Sie vorhaben, die Lernfunktion zu verwenden oder viele erweiterte Schutzmaßnahmen zu aktivieren und zu konfigurieren, müssen Sie erweiterte Standardeinstellungen wählen. Insbesondere wenn Sie planen, eine der SQL-Injection-Prüfungen, eine der Cross-Site-Scriptingprüfungen, jede Überprüfung, die Schutz vor Webformular-Angriffen bietet, oder die Cookie-Konsistenzprüfung zu konfigurieren, müssen Sie planen, die Lernfunktion zu verwenden. Sofern Sie bei der Konfiguration dieser Prüfungen nicht die richtigen Ausnahmen für Ihre geschützten Websites angeben, können diese den legitimen Datenverkehr blockieren. Es ist schwierig, alle Ausnahmen zu antizipieren, ohne zu breit gefächerte Ausnahmen zu schaffen. Die Lernfunktion erleichtert diese Aufgabe erheblich. Andernfalls sind die grundlegenden Standardeinstellungen schnell und müssen den Schutz bieten, den Ihre Webanwendungen benötigen.

Es gibt drei Profiltypen:

- **HTML.** Schützt Standard-HTML-basierte Websites.
- **XML.** Schützt XML-basierte Webdienste und Websites.
- **Web 2.0 (HTML-XML).** Schützt Websites, die sowohl HTML- als auch XML-Elemente enthalten, wie ATOM-Feeds, Blogs und RSS-Feeds.

Es gibt auch ein paar Einschränkungen für den Namen, den Sie einem Profil geben können. Ein Profilname darf nicht mit dem Namen übereinstimmen, der einem anderen Profil oder einer anderen Aktion in einer Funktion der NetScaler Appliance zugewiesen wurde. Bestimmte Aktions- oder Profilnamen werden integrierten Aktionen oder Profilen zugewiesen und können niemals für Benutzerprofile verwendet werden. Eine vollständige Liste der nicht zulässigen Namen finden Sie in den zusätzlichen Informationen zumWeb App Firewall-Profil. Wenn Sie versuchen, ein Profil mit einem Namen zu erstellen, der bereits für eine Aktion oder ein Profil verwendet wurde, wird eine Fehlermeldung angezeigt, und das Profil wird nicht erstellt.

So erstellen Sie ein Web App Firewall-Profil mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw profile <name> [-defaults ( **basic** | **advanced** )]`
- `set appfw profile <name> -type ( **HTML** | **XML** | **HTML XML** )`
- `set appfw profile <name> -comment "<comment>"`
- `save ns config`

Beispiel

Im folgenden Beispiel wird ein Profil mit dem Namen pr-basic mit grundlegenden Standardeinstellungen hinzugefügt und einen Profiltyp von HTML zugewiesen. Dies ist die geeignete Erstkonfiguration für ein Profil zum Schutz einer HTML-Website.

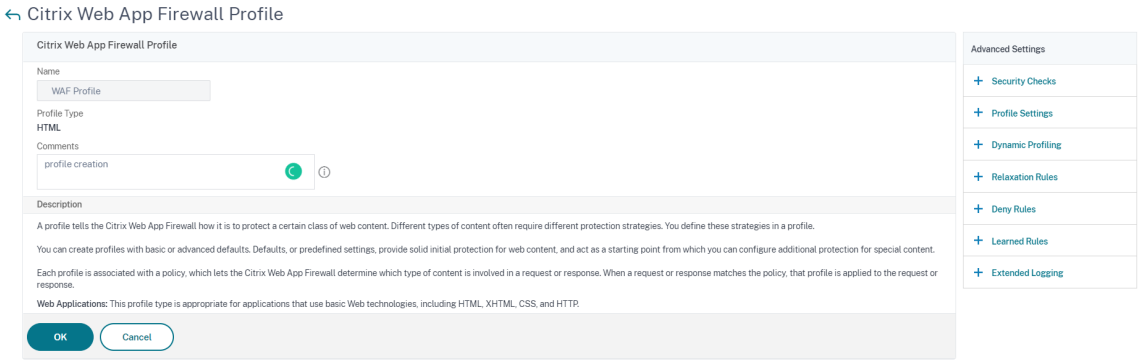
```
1 add appfw profile pr-basic -defaults basic -comment "Simple profile for
      websites."
2 set appfw profile pr-basic -type HTML
3 save ns config
4 <!--NeedCopy-->
```

So erstellen Sie ein Web App Firewall-Profil mit der GUI

Führen Sie das folgende Verfahren aus, um ein Web App Firewall-Profil zu erstellen:

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profile**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **“Web App Firewall-Profil erstellen** “ die folgenden grundlegenden Parameter fest:
    a) Name
    b) Profiltyp
    c) Anmerkungen
    d) Standardwerte
    e) Beschreibung
4. Klicken Sie auf **OK**.
5. Führen Sie im Abschnitt **Erweiterte Einstellungen** die folgenden Konfigurationen aus:
    a) Sicherheitschecks
    b) Profil-Einstellungen

c) Dynamische Profilerstellung
d) Regeln für Entspannung
e) Regeln verweigern
f) Gelernte Regel
g) Erweiterte Protokollierung

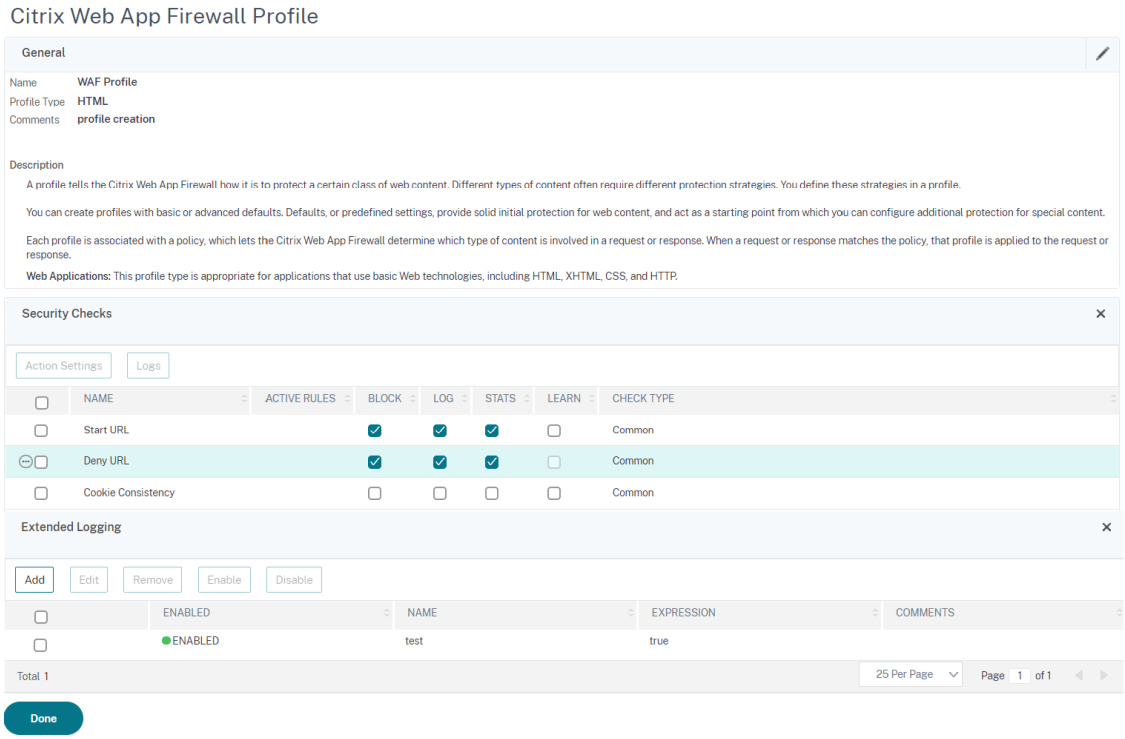


6. Wählen Sie im Abschnitt **Sicherheitsprüfungen** einen Sicherheitsschutz aus und klicken Sie auf Aktionseinstellungen.
7. Legen Sie auf der Seite “Sicherheitsprüfung” die Parameter fest.

   > **Hinweis:**
   > Die Einstellung “ **Aktive Regel** “ ist nur für die **HTML-SQL-Injection-Prüfung** verfügbar, um > oder Verweigern Signaturregeln zuzulassen

8. Klicken Sie auf **OK** und **Schließen**.
9. Legen Sie im Abschnitt **Profileinstellungen** die Profilparameter fest. Weitere Informationen finden Sie unter Konfigurieren der Einstellungen des Web App Firewall-Profils .
10. Wählen Sie im Abschnitt **Dynamische Profilerstellung** eine Sicherheitsprüfung aus, um dynamische Profileinstellungen hinzuzufügen. Weitere Informationen finden Sie unter Thema Dynamisches Profil .
11. Klicken Sie im Abschnitt **Entspannungsregeln** auf **Bearbeiten**, um eine Entspannungsregel für eine Sicherheitsprüfung hinzuzufügen. Weitere Informationen finden Sie unter Entspannungsregel für Einzelheiten.
12. Fügen Sie im Abschnitt **Regeln ablehnen** eine Ablehnungsregel für die HTML-SQL-Injection-Prüfung hinzu. Weitere Informationen finden Sie unter Regeln für HTML-Ablehnung .
13. Legen Sie im Abschnitt **Gelernte Regel** die Lerneinstellungen fest. Weitere Informationen finden Sie unter Learning von Web App Firewall .
14. Klicken Sie im Abschnitt **Erweiterte Protokollierung** auf **Hinzufügen**, um sensible Daten zu maskieren. Weitere Informationen finden Sie unter Thema Erweiterte Protokollierung .

15. Klicken Sie auf **Fertig**und dann auf **Schließen**.



Erzwingen der HTTP-RFC-Konformität

June 21, 2022

Citrix Web App Firewall prüft den eingehenden Datenverkehr auf HTTP-RFC-Konformität und legt jede Anforderung ab, die standardmäßig RFC-Verstöße aufweist. Es gibt jedoch bestimmte Szenarien, in denen die Appliance möglicherweise eine nicht RFC-Konformitätsanforderung Bypass oder blockieren muss. In solchen Fällen können Sie die Appliance so konfigurieren, dass solche Anfragen auf globaler oder Profilebene Bypass oder blockiert werden.

Blockieren oder Bypass Sie nicht RFC-konforme Anfragen auf globaler Ebene

Das HTTP-Modul identifiziert eine Anfrage als ungültig, wenn sie unvollständig ist und solche Anfragen nicht von der WAF bearbeitet werden können. Zum Beispiel fehlt eine eingehende HTTP-Anforderung, bei der ein Host-Header fehlt. Um solche ungültigen Anfragen zu blockieren oder zu Bypass, müssen Sie die Option `malformedReqAction` in den globalen Einstellungen der Anwendungs-Firewall konfigurieren.

Der Parameter ‘malformedReqAction’ überprüft die eingehende Anforderung auf ungültige Inhaltslänge, ungültige Chunked-Anforderung, keine HTTP-Version und unvollständigen Header.

> **Hinweis:**
>
> Wenn Sie die Blockoption im Parameter `malformedReqAction` deaktivieren, umgeht die Appliance die gesamte App-Firewall-Verarbeitung für alle Nicht-RFC-Konformitätsanforderungen und leitet die Anforderungen an das nächste Modul weiter.

So blockieren oder Bypass Sie ungültige HTTP-Anfragen ohne RFC-Beschwerde mithilfe der Befehlszeilenschnittstelle

Um ungültige Anfragen zu blockieren oder zu Bypass, geben Sie den folgenden Befehl ein:

```
set appfw settings -malformedreqaction <action>
```

Beispiel:

```
set appfw settings -malformedReqAction block
```

So zeigen Sie fehlerhafte Anforderungsaktionseinstellungen an

Um die Einstellungen für fehlerhafte Anforderungsaktionen anzuzeigen, geben Sie den folgenden Befehl ein:

```
show appfw settings
```

Ausgang:

```
1 DefaultProfile: APPFW_BYPASS UndefAction: APPFW_BLOCK SessionTimeout:
      900    LearnRateLimit: 400    SessionLifetime: 0
    SessionCookieName: citrix_ns_id ImportSizeLimit: 134217728
    SignatureAutoUpdate: OFF SignatureUrl:"https://s3.amazonaws.com/
    NSAppFwSignatures/SignaturesMapping.xml" CookiePostEncryptPrefix:
    ENC GeoLocationLogging: OFF CEFLogging: OFF      EntityDecoding:
     OFF    UseConfigurableSecretKey: OFF SessionLimit: 100000
    MalformedReqAction: block log stats
2  Done
3 <!--NeedCopy-->
```

So blockieren oder Bypass Sie ungültige HTTP-Anfragen ohne RFC-Beschwerde mithilfe der Citrix ADC GUI

1. Navigieren Sie zu **Sicherheit** > **Citrix Web App Firewall**.
2. Klicken Sie auf der Seite **Citrix Web App Firewall** unter **Einstellungen** auf **Engine-Einstellungen** ändern.

3. Wählen Sie auf der Seite **Citrix Web App Firewall-Einstellungen konfigurieren** die Option **Fehlerhafte Anforderung protokollieren** als Blockieren, Log oder Statistik aus.
4. Klicken Sie auf **OK** und **Schließen**.

> **Hinweis:**
>
> Wenn Sie die Auswahl der Blockaktion aufheben oder keine fehlerhafte Anforderungsaktion auswählen, umgeht die Appliance die Anforderung, ohne den Benutzer zu verweilen.

Blockieren oder Umgehen von nicht RFC-konformen Anforderungen auf Profilebene

Andere nicht RFC-konforme Anforderungen können so konfiguriert werden, dass sie auf Profilebene blockiert oder umgangen werden. Sie müssen das RFC-Profil entweder im Block- oder Bypass-Modus konfigurieren. Durch diese Konfiguration wird jeder ungültige Datenverkehr, der mit dem Web App Firewall-Profil übereinstimmt, entweder umgangen oder entsprechend blockiert. Das RFC-Profil überprüft die folgenden Sicherheitsüberprüfungen:

- Ungültige GWT-RPC-Anfragen
- Ungültige Kopfzeilen für Inhaltstypen
- Ungültige Multipart-Anfragen
- Ungültige JSON-Anfragen
- Doppelte Cookie-Namen-Wert-Paarprüf

> **Hinweis:**
>
> Wenn Sie das Profil `RFC` in den Modus “Bypass” setzen, müssen Sie sicherstellen, dass Sie die Transformationsoption in den **HTML Cross-Site-Scripting-Einstellungen** und in den Abschnitten **HTML SQL Injection Settings** deaktivieren. Wenn Sie das `RFC`-Profil im Bypass-Modus aktivieren und festlegen, zeigt die Appliance eine Warnmeldung an: “Site-übergreifende Skripte umwandeln” und “SQL-Sonderzeichen transformieren” sind beide derzeit eingeschaltet. Empfehlen Sie es auszuschalten, wenn es mit verwendet wird `APPFW_RFC_BYPASS`.
>
> **Wichtig:**
>
> Außerdem zeigt die Appliance einen Warnhinweis an: “Appfw-Sicherheitsprüfungen sind möglicherweise nicht auf Anfragen anwendbar, die gegen RFC-Prüfungen verstoßen, wenn dieses Profil festgelegt wird. Das Aktivieren einer Transformationseinstellung wird nicht empfohlen, da Anfragen möglicherweise teilweise transformiert werden, die RFC-Verstöße enthalten.

So konfigurieren Sie ein RFC-Profil im Web App Firewall-Profil mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:


```
set appfw profile <profile_name> -rfcprofile <rfcprofile_name
```

Beispiel

```
set appfw profile P1 -rfcprofile APPFW_RFC_BLOCK
```

> **Hinweis:**
>
> Standardmäßig ist das RFC-Profil im Blockmodus an das Web App Firewall-Profil gebunden.

So konfigurieren Sie ein RFC-Profil im Web App Firewall-Profil über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profile**.
2. Wählen Sie auf der Seite **Profile** ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Web App Firewall-Profil** im Abschnitt **Erweiterte Einstellungen** auf **Profileinstellungen**.
4. Stellen Sie im Abschnitt **HTML-Einstellungen** das RFC-Profil auf den Modus APPFW_RFC_BYPASS ein.
   Das System zeigt eine Warnmeldung an: Appfw Security checks enabled ist möglicherweise nicht für Anforderungen anwendbar, die gegen RFC-Prüfungen verstößt, wenn dieses Profil eingestellt ist. Das Aktivieren einer Transformationseinstellung wird nicht empfohlen, da Anfragen teilweise transformiert werden können, die RFC-Verletzungen enthalten.

Konfigurieren von Web App Firewall-Profilen

February 24, 2022

Um ein benutzerdefiniertes Web App Firewall-Profil zu konfigurieren, konfigurieren Sie zunächst die Sicherheitsüberprüfungen, die im Web App Firewall-Assistenten als *tiefer Schutz**oder erweiterter Schutz* bezeichnet werden. Bestimmte Prüfungen erfordern eine Konfiguration, wenn Sie sie überhaupt verwenden möchten. Andere haben Standardkonfigurationen, die sicher, aber begrenzt sind. Ihre Websites benötigen oder profitieren möglicherweise von einer anderen Konfiguration, die mehr Funktionen bestimmter Sicherheitsüberprüfungen nutzt.

Nachdem Sie die Sicherheitsüberprüfungen konfiguriert haben, können Sie auch einige andere Einstellungen konfigurieren, die das Verhalten steuern, nicht einer einzigen Sicherheitsüberprüfung, sondern der Web App Firewall-Funktion. Die Standardkonfiguration reicht aus, um die meisten Websites zu schützen, aber Sie müssen sie überprüfen, um sicherzustellen, dass sie für Ihre geschützten Websites geeignet sind.

> **Hinweis:**
>
> Die Länge des Profilnamens und die gesamte Länge des Importobjektnamens können bis zu 127 Zeichen festgelegt werden.

Weitere Informationen zu den Sicherheitsprüfungen der Web App Firewall finden Sie unter Erweiterter Schutz.

So konfigurieren Sie ein Web App Firewall Profil mit der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw profile <name> <arg1> [<arg2> ...]`

  Wobei:

  - `<arg1>` = ein Parameter und alle zugehörigen Optionen.
  - `<arg2>` = ein zweiter Parameter und alle zugehörigen Optionen.
  - … = zusätzliche Parameter und Optionen.

  Eine Beschreibung der Parameter, die beim Konfigurieren bestimmter Sicherheitsprüfungen verwendet werden sollen, finden Sie unter Erweiterter Schutz.

- `save ns config`

Beispiel

Das folgende Beispiel zeigt, wie das Blockieren von HTML SQL Injection und HTML Cross-Site Scripting in einem Profil namens pr-basic aktiviert wird. Dieser Befehl ermöglicht das Blockieren dieser Aktionen, ohne weitere Änderungen am Profil vorzunehmen.

```
1 set appfw profile pr-basic -crossSiteScriptingAction block -
     SQLInjectionAction block
2 <!--NeedCopy-->
```

Binden einer Entspannungsregel an ein Web App Firewall-Profil

Wenn die Web App Firewall einen Verstoß feststellt, kann der Benutzer die durch Entspannungsregeln ausgeführte Aktion Bypass. Die Entspannungsregel ist eine Ausnahme, die auf die erkannte Sicherheitsverletzung angewendet wird. Zum Beispiel schützen die Regeln zur Entspannung der Start-URL vor gewaltsantem Surfen. Bekannte Webserver-Schwachstellen, die von Hackern ausgenutzt werden,

können erkannt und blockiert werden, indem eine Reihe von standardmäßigen Deny-URL-Regeln aktiviert wird. Häufig gestartete Angriffe wie Pufferüberlauf, SQL oder siteübergreifende Skripterstellung können ebenfalls leicht erkannt werden.

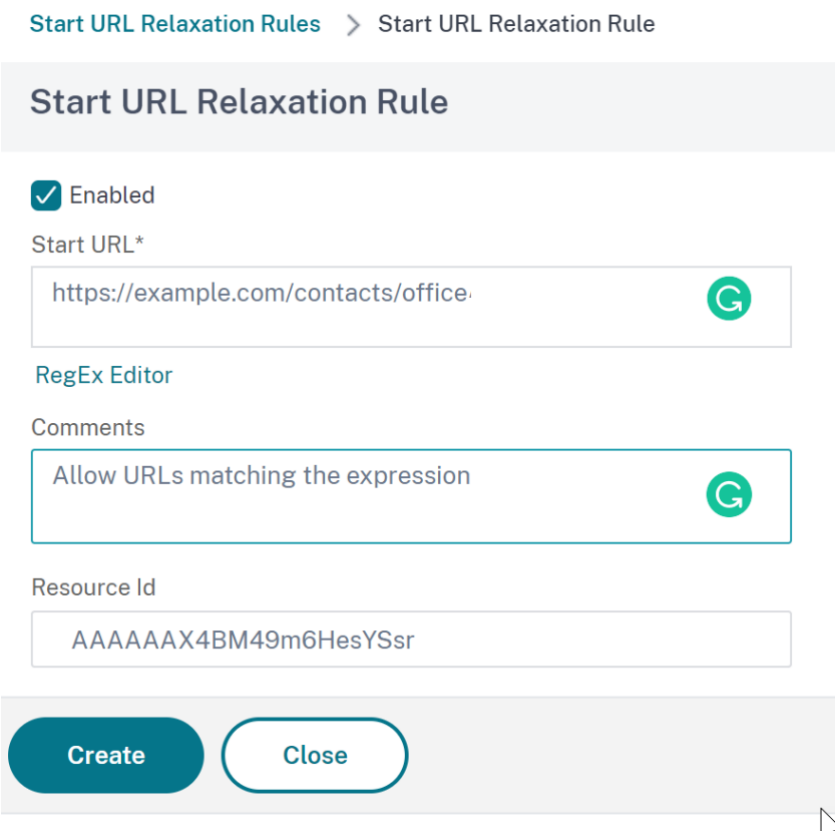
Bindung von Sicherheitsbefreiungs- oder Entspannungsregeln über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind appfw profile <name> ((-startURL <expression> [-resourceId  <
    string>]) | -denyURL <expression> | (-fieldConsistency <string>   <
    formActionURL> [-isRegex ( REGEX | NOTREGEX )]) | (-
    cookieConsistency <string> [-isRegex ( REGEX | NOTREGEX )]) | (-
    SQLInjection <string> <formActionURL> [-isRegex ( REGEX | NOTREGEX )
    ] [-location <location>] [-valueType <valueType> <valueExpression
    >....
<!--NeedCopy-->
```

So binden Sie Sicherheitsbefreiungs- oder Lockerungsregeln mithilfe der GUI

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich ein Profil aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der **Profilseite der Citrix Web App Firewall** im Abschnitt **Erweiterte Einstellungen** auf **Entspannungsregeln** .
4. Klicken Sie im Abschnitt **Entspannungsregeln** auf **startURL** und dann auf **Bearbeiten**.
5. Klicken Sie auf der Seite **Regeln zur Entspannung der Start-URL** auf **Hinzufügen**.
6. Legen **Sie auf der Seite Regel zur Entspannung der Start-URL** die folgenden Parameter fest:
    a) Aktiviert. Wählen Sie das Kontrollkästchen, um die Entspannungsregel
    b) Startet die URL. Geben Sie den Wert für regulären Ausdruck
    c) Kommentare. Geben Sie eine kurze Beschreibung der Entspannungsregel an.
7. Klicken Sie auf **Erstellen** und **Schließen**.



So konfigurieren Sie ein Web App Firewall-Profil mithilfe der GUI

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich das zu konfigurierende Profil aus, und klicken Sie dann auf **Bearbeiten**.
3. Konfigurieren Sie im Dialogfeld **Web App Firewall-Profil konfigurieren** auf der Registerkarte **Sicherheitsüberprüfungen** die Sicherheitsüberprüfungen.
   - Um eine Aktion für eine Prüfung zu aktivieren oder zu deaktivieren, aktivieren oder deaktivieren Sie in der Liste das Kontrollkästchen für diese Aktion.
   - Um weitere Parameter für die Prüfungen zu konfigurieren, die sie haben, klicken Sie in der Liste auf den blauen Chevron ganz rechts neben dieser Prüfung. Konfigurieren Sie im daraufhin angezeigten Dialogfeld die Parameter. Diese variieren von Scheck zu Scheck.

     Sie können auch eine Prüfung auswählen und unten im Dialogfeld auf Öffnen klicken, um das Dialogfeld **Entspannung konfigurieren** oder **Regel konfigurieren** für diese Überprüfung anzuzeigen. Diese Dialogfelder variieren auch von Prüfung zu Prüfung. Die meisten von ihnen enthalten eine Registerkarte **Schecks** und eine Registerkarte **Allgemein** . Wenn die Prüfung Entspannungen oder benutzerdefinierte Regeln unterstützt, enthält die Registerkarte **Prüfungen** eine Schaltfläche **Hinzufügen**, wodurch ein weiteres Dialogfeld

geöffnet wird, in dem Sie eine Entspannung oder Regel für die Prüfung angeben können. (Eine Entspannung ist eine Regel, um bestimmten Verkehr vom Scheck auszunehmen.) Wenn Entspannungen bereits konfiguriert wurden, können Sie eine auswählen und auf **Öffnen** klicken, um sie zu ändern.

- Um gelernte Ausnahmen oder Regeln für eine Prüfung zu überprüfen, wählen Sie die Prüfung aus, und klicken Sie dann auf **Erlernte Verletzungen**. Wählen **Sie im Dialogfeld Gelernte Regeln verwalten** nacheinander jede gelernte Ausnahme oder Regel aus.
  - Um die Ausnahme oder Regel zu bearbeiten und sie dann zur Liste hinzuzufügen, klicken Sie auf **Bearbeiten und bereitstellen**.
  - Um die Ausnahme oder Regel ohne Änderung zu akzeptieren, klicken Sie auf **Bereitstellen**.
  - Um die Ausnahme oder Regel aus der Liste zu entfernen, klicken Sie auf **Überspringen**.
- Um die Liste der zu überprüfenden Ausnahmen oder Regeln zu aktualisieren, klicken Sie auf **Aktualisieren**.
- Öffnen Sie den Learning Visualizer und verwenden Sie ihn, um erlernte Regeln zu überprüfen, klicken Sie auf **Visualizer**.
- überprüfen Sie die Protokolleinträge für Verbindungen, die mit einer Prüfung übereinstimmen, wählen Sie die Prüfung aus, und klicken Sie dann auf Protokolle. Sie können diese Informationen verwenden, um festzustellen, welche Checks mit Angriffen übereinstimmen, sodass Sie die Blockierung für diese Prüfungen aktivieren können. Sie können diese Informationen auch verwenden, um zu bestimmen, welche Prüfungen mit dem legitimen Datenverkehr übereinstimmen, sodass Sie eine entsprechende Ausnahme konfigurieren können, um diese legitimen Verbindungen zuzulassen. Weitere Informationen zu den Protokollen finden Sie unter Protokolle, Statistiken und Berichte.
- Um eine Überprüfung vollständig zu deaktivieren, deaktivieren Sie in der Liste alle Kontrollkästchen rechts neben dieser Prüfung.

4. Konfigurieren Sie auf der Registerkarte **Einstellungen** die Profileinstellungen.
   - Um das Profil mit dem Satz von Signaturen zu verknüpfen, die Sie zuvor erstellt und konfiguriert haben, wählen Sie unter Allgemeine Einstellungen diesen Signatursatz in der Dropdownliste **Signaturen** aus.

     > **Hinweis:**
     >
     > Sie können die Bildlaufleiste auf der rechten Seite des Dialogfelds verwenden, um nach unten zu scrollen und den Abschnitt Allgemeine Einstellungen anzuzeigen.

   - Um ein HTML- oder XML-Fehlerobjekt zu konfigurieren, wählen Sie das Objekt aus der entsprechenden Dropdownliste aus.

> **Hinweis:**
>
> Sie müssen zuerst das Fehlerobjekt hochladen, das Sie im Bereich Importe verwenden möchten. Weitere Informationen zum Importieren von Fehlerobjekten finden Sie unter Importe.

- Um den Standard-XML-Inhaltstyp zu konfigurieren, geben Sie die Inhaltstypzeichenfolge direkt in die Textfelder Standardanforderung und Standardantwort ein oder klicken Sie auf Zulässige Inhaltstypen verwalten, um die Liste der zulässigen Inhaltstypen zu verwalten »Mehr…..

5. Wenn Sie die Lernfunktion verwenden möchten, klicken Sie auf Lernen und konfigurieren Sie die Lerneinstellungen für das Profil, wie unter Konfigurieren und Verwenden der Lernfunktionbeschrieben.
6. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Bereich **Profile** zurückzukehren.

Webanwendungs-Firewall-Profileinstellungen

October 5, 2021

Im Folgenden sind die Profileinstellungen aufgeführt, die Sie auf der Appliance konfigurieren müssen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add appfw profile <name> [-invalidPercentHandling <invalidPercentHandling>]
 [-checkRequestHeaders ( ON | OFF )] [-URLDecodeRequestCookies ( ON | OFF )
] [-optimizePartialReqs ( ON | OFF )] [-errorURL <expression>]
```

Beispiel:

```
add appfw profile profile1 [-invalidPercentHandling secure_mode] [-checkRequestHeaders
 ON] [-URLDecodeRequestCookies OFF] [-optimizePartialReqs OFF]
```

Hierbei gilt:

invalidPercentHandling. Konfigurieren Sie die Methode für die Verarbeitung von prozentkodierten Namen und Werten.

Verfügbare Einstellungen funktionieren wie folgt:

asp_mode - Strips and Parses Ungültiger Prozentsatz für das Parsen. Beispiel curl -v "http://<vip>/forms/login.html?field=sel%zzect -> Invalid percent encoded char(%zz) wird entfernt und der Rest des Inhalts wird überprüft und die Aktion für die SQLInjection-Überprüfung durchgeführt.
secure_mode - Wir erkennen den codierten Wert ungültig Prozent und ignorieren ihn. Beispiel: -

`curl -v "http://<vip>/forms/login.html?field=sel%zzect -> Invalid percent encoded char(%zz)` wird erkannt, Leistungsindikatoren werden inkrementiert und Inhalt wird wie an den Server übergeben.
apache_mode - Dieser Modus funktioniert ähnlich wie der sichere Modus.
Mögliche Werte: apache_mode, asp_mode, secure_mode
Standardwert: secure_mode

optimizePartialReqs. Bei OFF/ON (ohne sicheres Objekt) sendet eine Citrix ADC Appliance die Teilanforderung an den Back-End-Server. Diese teilweise Antwort wurde an den Client zurückgesendet. OptimizePartialReqs ist sinnvoll, wenn das Safe-Objekt konfiguriert ist. Die Appliance sendet Anfragen für vollständige Antwort vom Server, wenn AUS, und fordert nur teilweise Antwort an, wenn EIN.

Folgende Einstellungen sind verfügbar:

ON - Teilanforderungen des Clients führen zu Teilanforderungen an den Back-End-Server.
OFF - Teilanforderungen durch den Client werden in vollständige Anforderungen an den Back-End-Server geändert
Mögliche Werte: ON, OFF
Standardwert: ON

URLDecodeRequestCookies. URL-Dekodierung von Anforderungscookies, bevor sie SQL- und siteübergreifenden Skripterstellungsüberprüfungen unterzogen werden.

Mögliche Werte: ON, OFF
Standardwert: OFF

Unterschriften-Post-Body-Limit (Bytes). Begrenzt die Anforderungsnutzlast (in Bytes), die für Signaturen mit dem als 'HTTP_POST_BODY' angegebenen Speicherort überprüft wurde.

Standardwert: 8096
Mindestwert: 0
Maximaler Wert: 4294967295

Post-Body-Limit (Bytes). Begrenzt die Anforderungsnutzlast (in Bytes), die von der Web Application Firewall überprüft wird.

Standardwert: 20000000
Minimalwert: 0
Maximalwert: 10 GB

Weitere Informationen zur Sicherheitseinstellung und ihrer GUI-Prozedur finden Sie unter Konfigurieren des Web App Firewall App-Firewall-Profils .

PostBodyLimitAction. PostBodyLimit berücksichtigt Fehlereinstellungen, wenn Sie die maximale Größe des zulässigen HTTP-Body angeben. Um Fehlereinstellungen zu berücksichtigen, müssen Sie eine oder mehrere Post-Body-Limit-Aktionen konfigurieren. Die Konfiguration ist auch für Anforderungen anwendbar, bei denen der Transfercodierungskopf in Chunked ist.


```
set appfw profile <profile_name> -PostBodyLimitAction block log stats
```

Wo,
Block - Diese Aktion blockiert eine Verbindung, die gegen die Sicherheitsprüfung verstößt und basiert auf der maximalen Größe des konfigurierten HTTP-Body (Post-Body-Limit). Sie müssen die Option immer aktivieren.

Log - Protokollieren Sie Verstöße gegen diese Sicherheitsprüfung.

Stats- Generieren Sie Statistiken für diese Sicherheitsprüfung.

> **Hinweis:**
>
> Das Protokollformat für die Post-Body-Limit-Aktion wird jetzt so geändert, dass es dem Standardformat für die Audit-Protokollierung entspricht, z.
> `ns.log.4.gz:Jun 25 1.1.1.1. <local0.info> 10.101.10.100 06/25/2020:10:10:28 GMT 0-PPE-0 : default APPFW APPFW_POSTBODYLIMIT 1506 0 : <Netscaler IP> 4234-PPE0 - testprof ><URL> Request post body length(<Post Body Length >)exceeds post body limit.`

InspectQueryContentTypes Prüfen Sie Anforderungs- und Webformulare für injizierte SQL- und Cross-Site-Skripts für die folgenden Inhaltstypen.

```
set appfw profile p1 -inspectQueryContentTypes HTML XML JSON OTHER
```

Mögliche Werte: HTML, XML, JSON, OTHER

Standardmäßig ist dieser Parameter sowohl für grundlegende als auch für erweiterte appfw-Profile als “inspectQueryContentTypes: HTML JSON OTHER” festgelegt.

Beispiel für Inspect-Abfrage-Inhaltstyp als XML:

```
1 > set appfw profile p1 -type XML
2 Warning: HTML, JSON checks except “InspectQueryContentTypes” & “
     Infer Content-Type XML Payload Action” will not be applicable when
     profile type is not HTML or JSON respectively.
3 <!--NeedCopy-->
```

Beispiel für Inspect-Abfrage-Inhaltstyp als HTML:

```
1 > set appfw profile p1 -type HTML
2 Warning: XML, JSON checks except “InspectQueryContentTypes” & “Infer
      Content-Type XML Payload Action” will not be applicable when
     profile type is not XML or JSON respectively
3 Done
```



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

Beispiel für den Inhaltstyp “Abfrage prüfen” als JSON:

```
> set appfw profile p1 -type JSON
Warning: HTML, XML checks except “InspectQueryContentTypes” & “Infer
    Content-Type XML Payload Action will not be applicable when profile
    type is not HTML or XML respectively
Done
<!--NeedCopy-->
```

errorURL expression. Die URL, die die Citrix Web App Firewall als Fehler-URL verwendet. Maximale Länge: 2047.

> **Hinweis:**
>
> Wenn die Fehler-URL mit der Signatur-URL vergleichbar ist, setzt die Appliance die Verbindung zurück, um Verletzungen in einer angeforderten URL zu blockieren.

Ändern eines Web App Firewall Profiltyps

October 5, 2021

Wenn Sie den falschen Profiltyp für ein Web App Firewall -Profil gewählt haben oder sich die Art des Inhalts auf der geschützten Website geändert hat, können Sie den Profiltyp ändern.

> **Hinweis:** Wenn Sie den Profiltyp ändern, verlieren Sie alle Konfigurationseinstellungen und gelernte Entspannungen oder Regeln für die Features, die der neue Profiltyp nicht unterstützt. Wenn Sie beispielsweise den Profiltyp von Web 2.0 in XML ändern, gehen alle Konfigurationsoptionen für Start-URL, Formularfeldkonsistenzprüfung und die anderen HTML-spezifischen Sicherheitsprüfungen verloren. Die Konfiguration aller Optionen, die sowohl vom alten als auch vom neuen Profiltyp unterstützt werden, bleibt unverändert.

So ändern Sie einen Web App Firewall Profiltyp mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw profile <name> -type ( **HTML** | **XML** | **HTML XML** )`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Typ eines Profils mit dem Namen pr-basic von HTML in HTML XML geändert, was dem Typ Web 2.0 in der GUI entspricht.

```
set appfw profile pr-basic -type HTML XML
save ns config
<!--NeedCopy-->
```

So ändern Sie einen Web App Firewall Profiltyp mit der GUI

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Richtlinien**.
2. Klicken Sie im Detailbereich auf **Aktion** und dann auf **Profiltyp ändern**.
3. Wählen Sie im Dialogfeld Web App Firewall **Profiltyp ändern** in der Dropdownliste **Profiltyp** einen neuen Profiltyp aus.
4. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Bereich **Profile** zurückzukehren.

Exportieren und Importieren eines Web App Firewall Profils

December 7, 2021

Sie können die gesamte Konfiguration eines Web App Firewall Profils (einschließlich aller gebundenen Objekte, wie HTML-Fehlerobjekt, XML-Fehlerobjekt, WSDL- oder XML-Schema, Signaturen usw.) über mehrere Appliances replizieren. Sie können ein Zielprofil auswählen und die Konfiguration exportieren, um sie im lokalen Dateisystem Ihres Computers zu speichern, oder Sie können die archivierte Konfiguration übertragen, um sie auf einem Server zu speichern. Ebenso können Sie das lokale Dateisystem Ihres Computers durchsuchen oder das Archiv vom Server importieren, um ein zuvor exportiertes Profil auszuwählen und in Ihre NetScaler Appliance zu importieren.

Die Option, die gesamte Profilkonfiguration zu exportieren und dann in eine andere Appliance zu importieren, kann in verschiedenen Anwendungsfällen nützlich sein. Sie können beispielsweise ein Web App Firewall Profil in einer Testbetteinrichtung konfigurieren, um zu testen und zu überprüfen, ob es wie erwartet funktioniert. Sobald Sie zufrieden sind, können Sie das Profil exportieren und die Profilkonfiguration in Ihre NetScaler Produktionen importieren. Diese Funktionalität ist auch nützlich, um Ihre Konfiguration zu sichern. Sie können das Profil exportieren, bevor Sie Änderungen vornehmen, sodass Sie die Konfiguration bei Bedarf problemlos in einen bekannten Zustand zurücksetzen können.

> **Hinweis:**
>
> Web App Firewall Profile, die aus einem Build exportiert und archiviert werden, können nicht auf einem System wiederhergestellt werden, auf dem ein anderer Build ausgeführt wird, da Änderungen in neueren Versionen zu Kompatibilitätsproblemen führen können. Wenn Sie versuchen, ein archiviertes Profil in einem anderen Build als dem, aus dem es exportiert wurde, wiederherzustellen, wird eine Fehlermeldung in ns.log protokolliert.

Die Export- und Importprofilfunktionalität ist sowohl in der GUI (GUI) als auch in der Befehlszeilenschnittstelle (CLI) verfügbar. Die GUI wird empfohlen, da sie einfach zu bedienende **Aktionsoptionen** bietet. Mit einem Klick auf eine Schaltfläche können Sie die gesamte Konfiguration eines Profils **exportieren oder importieren** .

Exportieren Web App Firewall Profilen mit der CLI

Wenn Sie ein Profil mit CLI **exportieren**, müssen Sie die Konfiguration **archivieren** und dann **exportieren** . Um ein Profil zu **importieren**, müssen Sie das Archiv in die NetScaler Appliance **importieren** und dann den **Restore-Befehl** ausführen, um die Konfiguration zu extrahieren. Die folgenden CLI-Befehle können zum Exportieren, Importieren und Verwalten der Profilkonfigurationen verwendet werden.

CLI-Befehle zum Exportieren von Archiven:

- `archive appfw profile <name> <archivename> [-comment <string>]`
- `export appfw archive <name> <target>`

CLI-Befehle zum Importieren von Archiven:

- **`import`** `appfw archive <src> <name> [-comment <string>]`
- `restore appfw profile <archivename>`

CLI-Befehle zum Verwalten von Archiven:

- `show appfw archive`
- `rm appfw archive <name>`

Das Exportieren eines Profils von einer Appliance und das Importieren in eine andere erfordert fünf Schritte in CLI. Die ersten drei Schritte werden auf der Quell-Appliance ausgeführt, auf der die Profilkonfiguration ursprünglich erstellt wurde, und die nächsten 2 Schritte werden auf der Ziel-Appliance ausgeführt, auf der die Profilkonfiguration repliziert werden soll.

Profil aus der Quell-NetScaler Appliance exportieren:

Schritt 1: Erstellen Sie ein Archiv des konfigurierten Profils.

Schritt 2: Exportieren Sie das Archiv in das NetScaler Dateisystem.

Schritt 3: Verwenden Sie ein Dateiübertragungsprogramm wie scp, um die exportierte Archivdatei von der NetScaler Appliance A auf die NetScaler-Ziel-Appliance zu übertragen.

Profil in die NetScaler Ziel-Appliance importieren:

Schritt 4: Führen Sie den Importbefehl aus, um die archivierte Datei zu importieren. Sie können das Archiv aus dem lokalen Dateisystem Ihres NetScaler importieren oder das HTTP- oder HTTPS-Protokoll verwenden, um das Archiv von einem Server mit der URL zu importieren.

Schritt 5: Führen Sie den Restore-Befehl aus, um die Profilkonfiguration aus dem importierten Archiv wiederherzustellen

So exportieren Sie ein Web App Firewall Profil mit der Befehlszeilenschnittstelle:

Archivieren Sie zunächst die Konfiguration des Profils, und **exportieren** Sie das Archiv an einen Zielspeicherort. Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
archive appfw profile <profileName> <archiveName>
```

Wobei:

- <profileName> ist der Name des Profils, das archiviert werden soll.
- <archiveName> ist der Name der zu erstellenden Archivdatei.

Ausführung des obigen Befehls erstellt 2 Instanzen der Archivdatei. Einer im Ordner /var/tmp und der andere im Ordner /var/archive/appfw.

```
export appfw archive <archiveName> <target>
```

Wobei:

- <archiveName> ist der Name des zu exportierenden Archivs. (Der gleiche Name wie im vorherigen Befehl.
- <target> ist ein Dateipfad, der mit local: als Präfix beginnt, gefolgt von<archiveName> .

Die Ausführung des Export-Befehls speichert die exportierte Archivdatei im Dateisystem Ihrer NetScaler Appliance im Ordner /var/tmp.

Beispiele:

```
> archive appfw profile test_pr archived_test_pr
```

```
> export appfw archive archived_test_pr local:dutA_test_pr
```

Nachdem die beiden oben genannten Befehle ausgeführt wurden, enthält der Ordner /var/tmp die archived_test_pr-Datei und die exportierte Kopie Duta_test_PR, die in ihrer Größe identisch sind. Über die Befehlszeilenschnittstelle können Sie in die Shell ablegen, um zu dem Ordner zu navigieren, um zu überprüfen, ob diese Dateien vorhanden sind.

Nach dem Exportieren der Archivdatei können Sie **scp** oder ein anderes solches Dateiübertragungsprogramm verwenden, um eine Kopie der Archivdatei von der NetScaler Appliance, auf der sie erstellt wurden, auf Ihre NetScaler-Ziel-Appliance zu übertragen.

Importieren von Web App Firewall Profilen mit der CLI

Nachdem Sie die archivierte Datei erfolgreich von der Quell-Appliance auf die Ziel-Appliance verschoben haben, können Sie das Archiv des Profils **importieren** und dann den **Wiederherstellungsbefehl** ausführen, um die Konfiguration des Profils auf der Ziel-Appliance zu replizieren.

Melden Sie sich bei der Ziel-Appliance an. Gehen Sie in die Shell und cd in den Ordner /var/tmp, um zu überprüfen, ob die Größe der scp'd Datei auf dieser Appliance mit der Größe der ursprünglichen archivierten Datei auf der Quell-Appliance übereinstimmt. Beenden Sie die Shell, um zur Befehlszeile zurückzukehren.

So importieren Sie ein Profil mit der CLI:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
import appfw archive <src> <name> [-comment <string>]
```

wobei

- <src> ist der Speicherort der Archivdatei, nachdem sie von der Quell-Appliance übertragen wurde, auf der sie erstellt wurde. Sie können ein lokales Dateisystem und einen Dateinamen verwenden. Wenn Sie das Archiv auf einem Server abgelegt haben, können Sie eine URL zum Importieren der archivierten Datei verwenden. Wenn der Pfad oder Dateiname Leerzeichen enthält, schließen Sie die URL in doppelte Anführungszeichen ein.
- <name> ist der Name der zu importierenden Archivdatei.
- <string> ist eine optionale Beschreibung des Zwecks des Archivs.

```
restore appfw profile <archiveName>
```

Beispiele:

A. Import aus lokaler Datei gefolgt von Wiederherstellung:

```
> import appfw archive local:dutA_test_pr dut2_test_pr
```

```
> restore appfw profile dut2_test_pr
```

B. Importieren von URL gefolgt von Wiederherstellung:

```
import appfw archive http://10.217.30.16/FFC/Profile_ImportExport/
dutA_test_pr.tgz my_archive
restore appfw profile my_archive
```

In diesem Beispiel wird das test_pr-Profil zusammen mit allen gebundenen Objekten (wie Signaturen, HTML-Fehlerseite, Relaxationsregeln usw.) auf der NetScaler Ziel-Appliance wiederhergestellt.

Sie können die folgenden CLI-Befehle verwenden, um auf Manpages für weitere Details zuzugreifen.

- manarchiv appfw Profil
- man export appfw archiv

- man import appfw archiv
- man wiederherstellen appfw Profil
- man show appfw archiv
- man rm appfw Archiv

Exportieren und Importieren von Web App Firewall Profilen mit der GUI

Die GUI ist einfacher zu verwenden als die CLI. Das Dienstprogramm führt sowohl Archivierungs- als auch Exportvorgänge durch, wenn Sie auf **Exportieren**klicken. Ebenso wird sowohl der Import als auch der Wiederherstellung ausgeführt, wenn Sie auf **Importieren**klicken. Die GUI kann auf das lokale Dateisystem des Computers zugreifen, von dem aus Sie auf das Dienstprogramm zugreifen. Sie können eine Kopie des Archivs exportieren und auf Ihrem lokalen Computer speichern. Sie können diese Kopie dann direkt in die Ziel-Appliance importieren, ohne die Archivdatei manuell von einer Appliance auf die andere übertragen zu müssen.

So exportieren Sie ein Web App Firewall Profil mit der GUI:

1. Navigieren Sie zu **Konfiguration** > **Sicherheit** > **Web App Firewall** > **Profile** .
2. Wählen Sie im Detailbereich ein zu exportierendes Profil aus. Klicken Sie auf **Aktionen** und wählen Sie **Exportieren** aus, um eine Kopie im lokalen Dateisystem Ihres Computers herunterzuladen und zu speichern.

So importieren Sie ein Web App Firewall Profil mit der GUI:

1. Navigieren Sie zu **Konfiguration** > **Sicherheit** > **Web App Firewall** > **Profile** .
2. Klicken Sie im Detailbereich auf **Aktionen**, und wählen Sie **Importieren** aus. Im Bereich Web App Firewall Profil importieren stehen Ihnen das Auswahlfeld Aus importieren 2 Optionen zur Verfügung:

URL: Sie können ein Archiv importieren, indem Sie eine **URL** angeben. Wenn diese Option ausgewählt ist, müssen Sie im **URL-Eingabefeld** einen absoluten Pfad für die archivierte Datei angeben.

Datei: Sie können ein Archiv aus der lokalen **Datei** importieren. Wenn diese Option ausgewählt ist, wird ein Auswahlfeld **Lokale Datei** angezeigt. Sie können die lokalen Dateien Ihres Computers durchsuchen, um die Zielarchivdatei auszuwählen.

Klicken Sie auf **Erstellen**, um das angegebene Archiv zu importieren. Beim erfolgreichen Abschluss des Importvorgangs wird die Profilkonfiguration auf der Ziel-Appliance erstellt.

Highlights

- Sie können die gesamte Konfiguration (einschließlich aller Importobjekte sowie konfigurierten Relaxationsregeln für das Profil) auf mehreren Appliances replizieren, ohne dass Sie Konfigurationsschritte wiederholen müssen, indem Sie die Export- und Importprofilfunktionalität verwenden.

- Die importierten Objekte, wie Signaturen, WSDL, Schema, Fehlerseite usw., sind in der archivierten TAR-Datei enthalten und auf der Ziel-Appliance repliziert.
- Angepasste Feldtypen sind in der archivierten TAR-Datei enthalten und auf der Ziel-Appliance repliziert.
- Die Richtlinienbindungen des archivierten Profils werden nicht repliziert, wenn die Konfiguration wiederhergestellt wird. Sie müssen die Richtlinie konfigurieren und sie an das Profil binden, nachdem Sie das Profil in die Appliance importiert haben.
- Der Name der Archivdatei kann bis zu 31 Zeichen lang sein. Wie bei Profilnamen muss ein Archivname mit einem alphanumerischen Zeichen oder Unterstrich beginnen und nur alphanumerische Zeichen und Unterstriche (_), Zahl (#), Punkt (.), Leerzeichen (), Doppelpunkt (:), at (@), Gleich (=) oder Bindestrich (-) enthalten.
- Kommentare, die mit dem Archiv verknüpft sind, müssen beschreibend genug sein, um den Zweck der archivierten Konfiguration zu vermitteln. Die maximal zulässige Länge für einen Kommentar beträgt 255 Zeichen.
- `clear config -force basic` Mit dem Befehl werden die archivierten Profile nicht entfernt.
- Die Import- und Exportprofilfunktionalität wird in Hochverfügbarkeitsbereitstellungen (HA) unterstützt.

Tipps zum Debuggen

- Überwachen Sie die Datei /var/log/ns.log während der Befehlsausführung, um festzustellen, ob Fehlermeldungen vorhanden sind.
- Zusätzliche Protokolle (_restore.log, remove.log, import.log) werden im Ordner /var/tmp/- generiert. Sie können beim Debuggen von Problemen während der entsprechenden Operationen helfen. Wenn diese Protokolle eine MB Größe erreichen, werden die Protokollmeldungen gelöscht, um die Protokolldatei auf ein Viertel der ursprünglichen Größe zu verkleinern.
- Wenn der Importbefehl fehlschlägt, wenn Sie die URL-Option anstelle des lokalen Dateisystems verwenden, stellen Sie sicher, dass DNS-Namensserver und Routeneinstellungen korrekt konfiguriert sind.
- Wenn Sie das HTTPS-Protokoll zum Importieren des Archivs verwenden, schlägt der Befehl möglicherweise fehl, wenn der HTTPS-Server Clientzertifikatauthentifizierung erfordert.

Einfache Fehlerbehebung mit Web Application Firewall-Protokollen

October 5, 2021

Bei einem Sicherheitsangriff ist es wichtig, eine detaillierte WAF-Protokollierung auf der Appliance zu erfassen. Dazu können Sie den Parameter VerboseLogLevel in einem Anwendungsfirewall Profil konfigurieren.

Betrachten Sie einen Web-Traffic, der einen Sicherheitsangriff hat. Wenn die Appliance den Datenverkehr empfängt, werden Verletzungsdetails wie HTTP-Header-Details, Protokollmuster und Mustern utzlastinformationen protokolliert und an den ADM-Server gesendet. Der ADM-Server überwacht die detaillierten Protokolle und zeigt sie zur Überwachung und Nachverfolgung auf der Seite Security Insight an.

Ausführliche Protokollierungsstufe mit der Befehlszeilenschnittstelle konfigurieren

Um detaillierte WAF-Protokolle zu erfassen, konfigurieren Sie den folgenden Befehl.
Geben Sie an der Befehlszeilenschnittstelle Folgendes ein:

```
set appfw profile <profile_name> -VerboseLogLevel (pattern|patternPayload|
patternPayloadHeader)
```

Beispiel

```
set appfw profile profile1 -VerboseLogLevel patternPayloadHeader
```

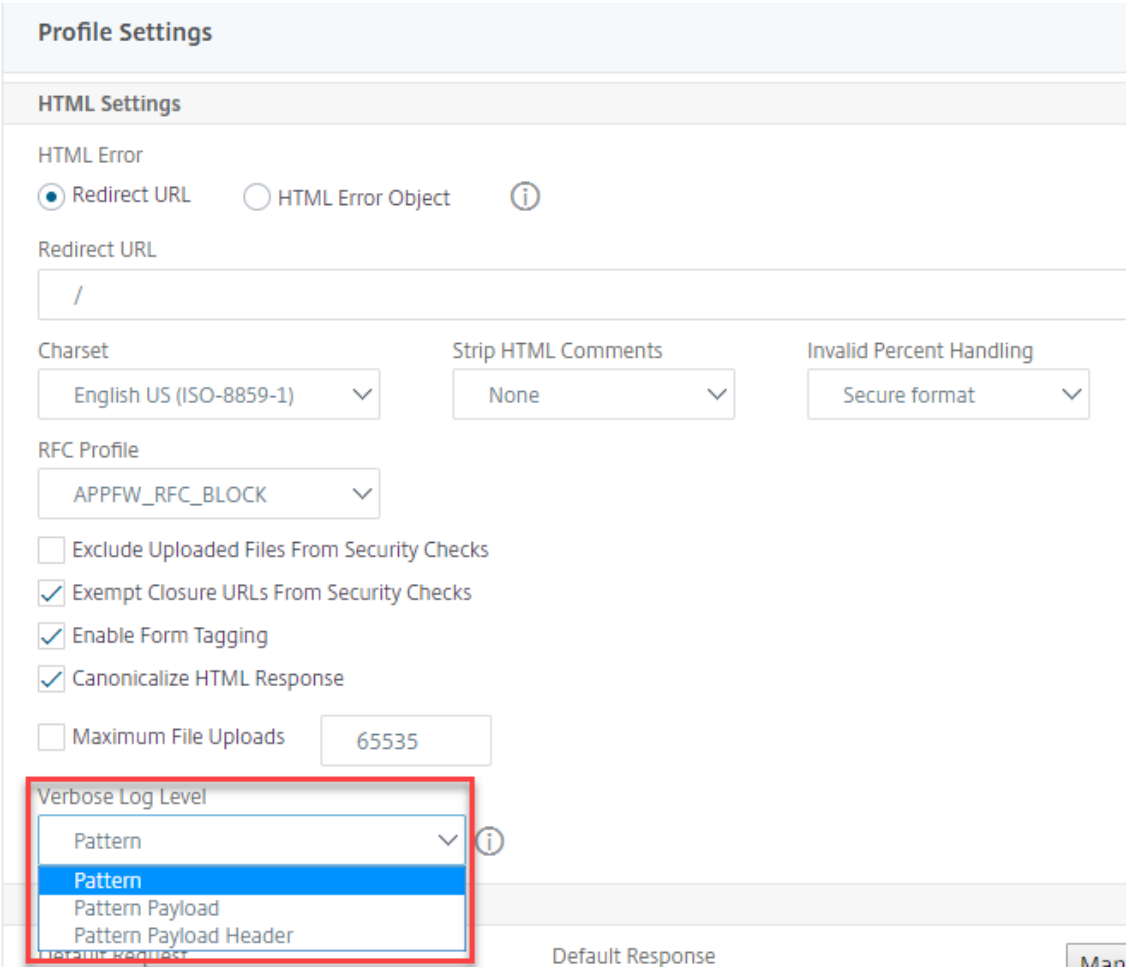
Die verfügbaren Protokollebenen sind:

1. Muster. Protokolliert nur das Verstoßmuster.
2. Muster Nutzlast. Protokolliert das Verstoßmuster und 150 Bytes zusätzlicher Feldelementnutzlast.
3. Muster-Nutzlast-Header. Protokolliert Verletzungen Patter, 150 Bytes zusätzlicher Feldelementnutzlast und HTTP-Header-Informationen.

Konfigurieren ausführlicher Log-Level mit der Citrix ADC GUI

Gehen Sie folgendermaßen vor, um die ausführliche Protokollstufe im WAF-Profil zu konfigurieren.

1. Navigieren Sie im Navigationsbereich zu **Sicherheit** > **Profile**.
2. Klicken Sie auf der Seite **Profile** auf **Hinzufügen**.
3. Klicken Sie auf der Seite **Citrix Web App Firewall Profil**unter **Erweiterte Einstellungen**auf **Profileinstellungen**.
4. Wählen Sie im Abschnitt **Profileinstellungen** die detaillierte WAF-Protokollebene im Feld Ausführliche Protokollebene aus.
5. Klicken Sie auf **OK** und **Fertig**.



Datei-Upload-Schutz

October 5, 2021

Viele Angreifer versuchen, bösartigen Code, Viren oder Malware als Dateianhänge während der Übermittlung mehrerer Formulare hochzuladen. Es ist wichtig, unser Netzwerk zu schützen und solche Bedrohungen zu überwinden. Um ein solches Hochladen bösartiger Dateien zu verhindern, kann ein Citrix ADC Administrator nun eine Reihe zulässiger Dateiupload-Formate im WAF-Profil konfigurieren. Auf diese Weise beschränken Sie Dateiuploads auf bestimmte Formate und schützen die Appliance vor bösartigen Dateiuploads. Der Schutz funktioniert jedoch nur, wenn Sie die Option ExcludeFileUploadFormChecks im WAF-Profil deaktivieren.

Funktionsweise des Dateiupload

Wenn Sie zulässige Dateiupload-Formate konfigurieren, ist die Komponenteninteraktion wie folgt:

- Kundenanfrage hat eine Formularübergabe mit einem Datei-Upload-Typ, zum Beispiel PDF.
- Im Rahmen der Sicherheitsprüfung überprüft WAF die Anforderungsnutzlast und validiert den Dateityp (basierend auf magischen Signaturnummern).
- Wenn der Dateityp ein zulässiges Dateiformat ist, wird die entsprechende Aktion basierend auf der Dateitypbindung angewendet.
- Zur Validierung des Dateityps überprüft die Appliance die Nutzlast und prüft bei bekannten Offsets auf die bekannten magischen Nummern. Jeder Dateityp hat eine Folge von magischen Zahlen, die den Dateityp validieren.
- Nur wenn die Validierung erfolgreich ist, identifiziert WAF die Datei als zulässiges Format und die zugehörige Aktion wird angewendet.

Konfigurieren des Uploads von Dateityps mit der Citrix ADC CLI

Um zulässige Dateiformate zu konfigurieren, verwendet die Appliance ein WAF-Profil, das an Dateiupload-Parameter gebunden ist.

1. Webanwendungs-Firewall-Profil konfigurieren

Geben Sie Folgendes ein, um ein Firewallprofil für Webanwendungen zu konfigurieren:

```
set appfw profile <profile_name> [-fileUploadTypesAction <fileUploadTypesAction
>]<fileUploadTypesAction> = ( none | block | log | stats )
```

Beispiel

```
set appfw profile profile1 -fileUploadTypesAction block
```

1. Binden Sie das Web Application Firewall-Profil mit Datei-Upload-Parametern.

Um ein Profil mit Datei-Upload-Parametern zu binden, geben Sie Folgendes ein:

```
bind appfw profile <profile_name> - fileUploadType <form_field > <form_action_url
> -fileType <fileType> ( pdf | msdoc | text | image | any)
```

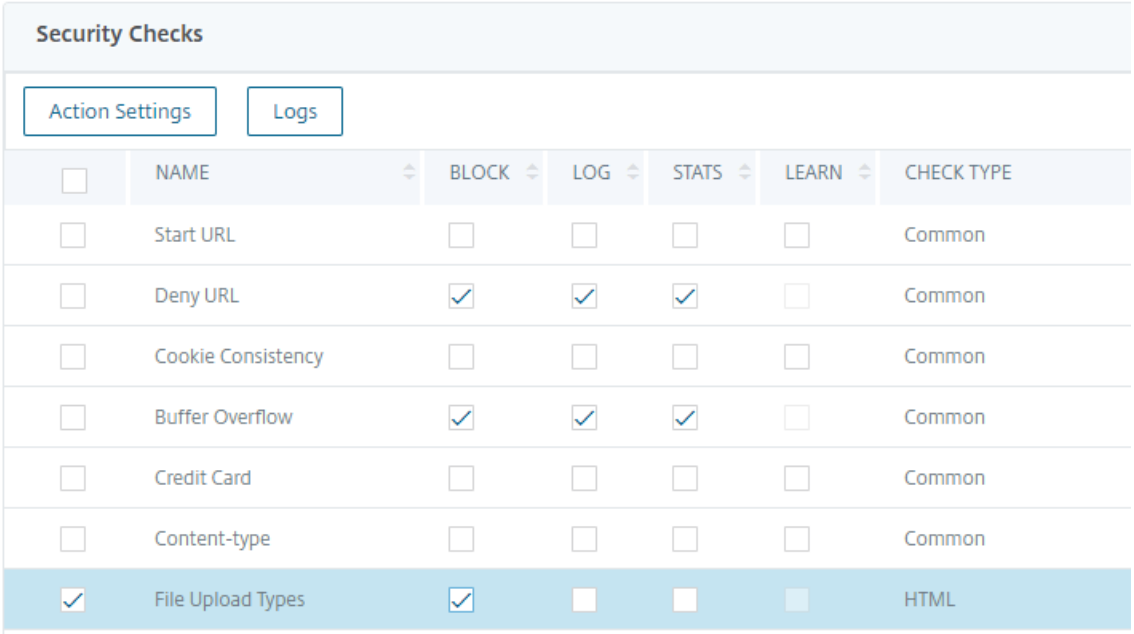
Beispiel

```
bind appfw profile profile1 -fileuploadType image action_url -fileType
image
```

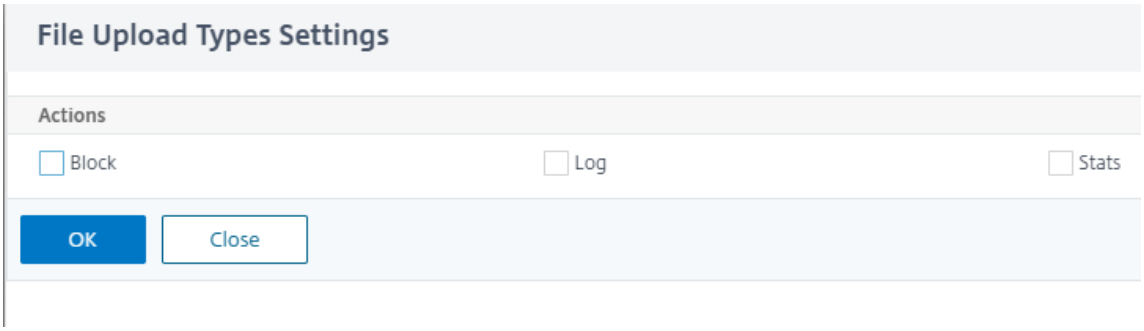
Konfigurieren des Sicherheitsschutzes zum Hochladen von Dateien über die Citrix ADC GUI

Gehen Sie folgendermaßen vor, um die Einstellungen für den Dateiupload festzulegen.

1. Navigieren Sie im Navigationsbereich zu **Sicherheit** > **Profile** .
2. Klicken Sie auf der Seite “Profile” auf **Add**.
3. Klicken Sie auf der Seite **Citrix Web App Firewall Profile** unter **Erweiterte Einstellungen** auf **Sicherheitsprüfungen**.
4. Wechseln Sie im Abschnitt **Sicherheitsprüfungen** zu Einstellungen für **Datei-Upload-Typen** .



5. Aktivieren Sie das Kontrollkästchen, und klicken Sie auf **Aktionseinstellungen**.
6. Legen Sie auf der Seite **Einstellungen für Datei-Upload-Typen** die Datei-Upload-Aktion fest.
7. Klicken Sie auf **OK**.
8. Klicken Sie auf der Seite **Citrix Web App Firewall profil** auf **OK** und **Fertig** .



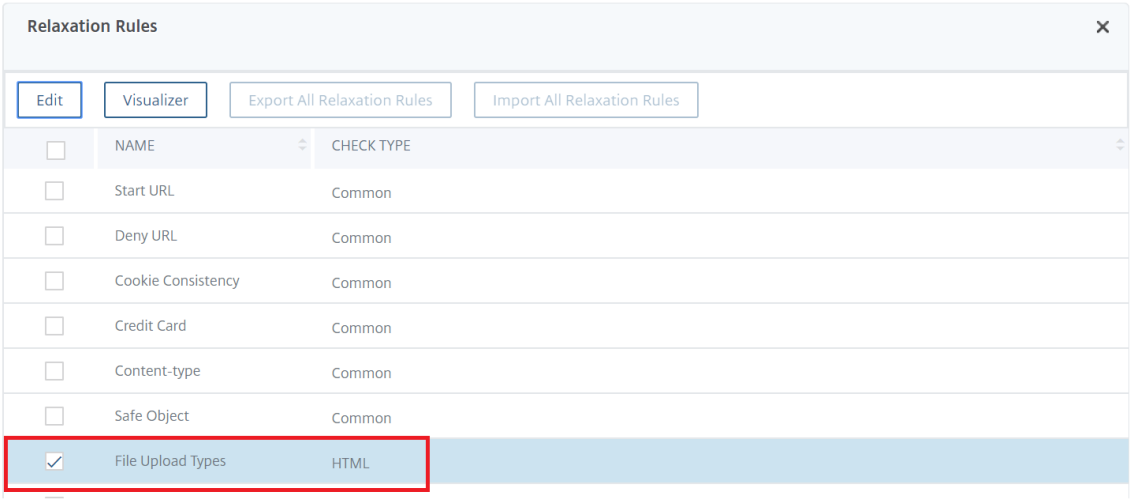
Konfigurieren der Relaxationsregel zum Hochladen von Dateien über die Citrix ADC GUI

Sie können einen Datei-Upload-Sicherheitsschutz entspannen, um Fehlalarme zu vermeiden. Beispielsweise kann die Appliance Dateiuploads blockieren, Sie können jedoch eine Relaxationsregel

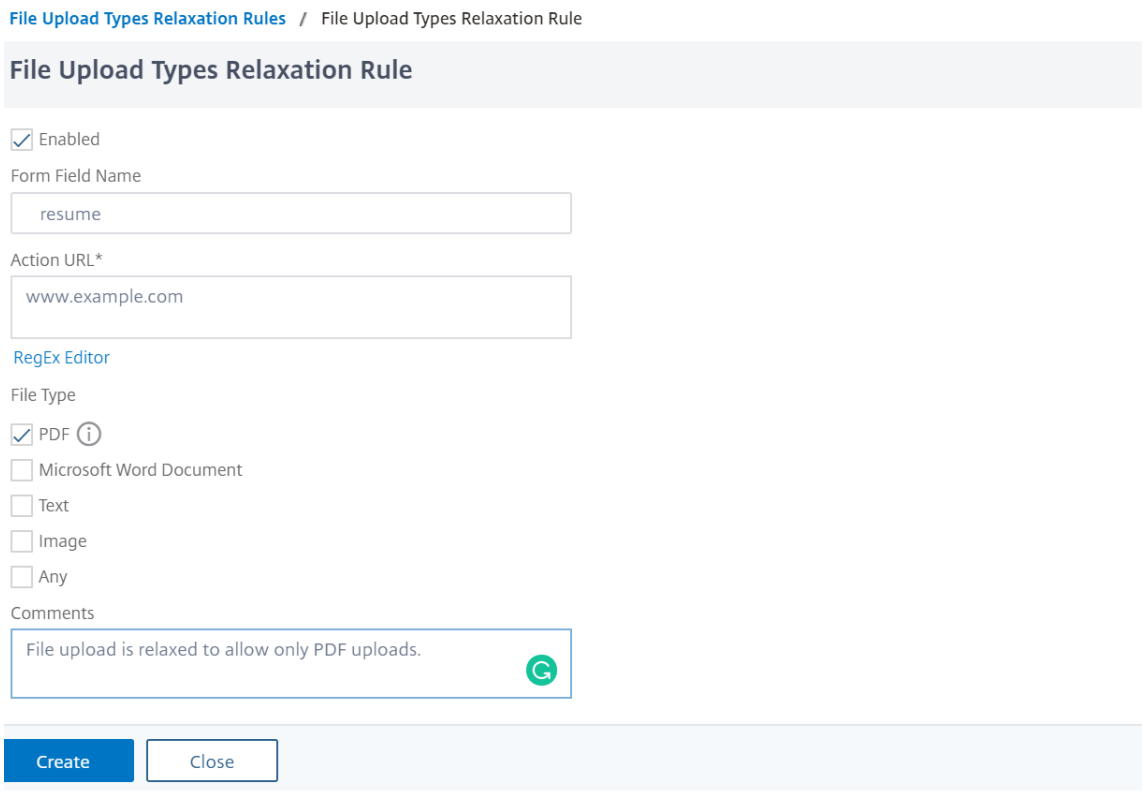
hinzufügen, um Dateiuploads von bestimmten Websites zuzulassen. Auf diese Weise umgeht die Appliance die Sicherheitsprüfung für das angegebene Formularfeld und ermöglicht es Benutzern, Dateien von der Website hochzuladen, die in der Aktions-URL angegeben ist.

Gehen Sie wie folgt vor, um eine Entspannungsregel zu erstellen.

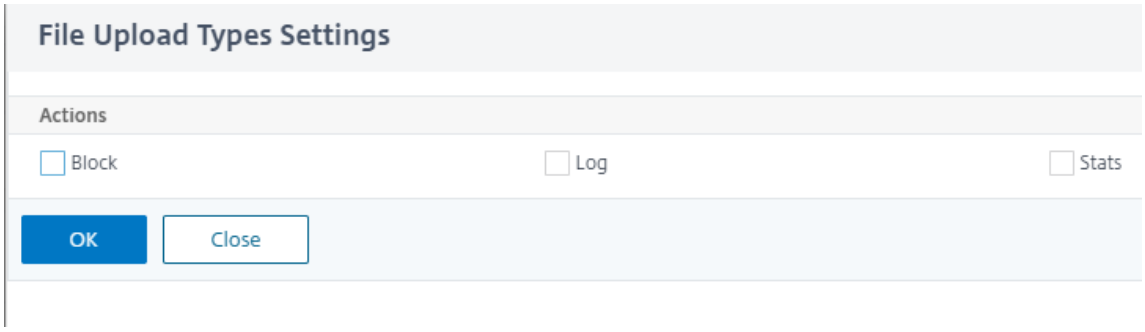
1. Navigieren Sie im Navigationsbereich zu **Sicherheit** > **Citrix Web App Firewall** < **Profile**.
2. Klicken Sie auf der Seite "Profile" auf **Add**.
3. Klicken Sie auf der Seite **Citrix Web App Firewall Profil** unter **Erweiterte Einstellungen** auf **Relaxationsregeln**.
4. Wählen Sie im Abschnitt **Relaxationsregeln** die Option **Datei-Upload-Typen** aus, und klicken Sie auf **Bearbeiten**.



5. Klicken Sie auf der Seite **Rexalationsregeln für Datei-Upload-Typen** auf **Hinzufügen**.
6. Legen Sie auf der Seite **Relaxationsregel für Datei-Upload-Typen** die folgenden Parameter fest:
   a) Aktiviert. Aktivieren Sie dieses Kontrollkästchen, um die Entspannungsregel zu aktivieren.
   b) Name des Formularfelds. Geben Sie den Feldnamen ein, für den keine Sicherheitsüberprüfung erforderlich ist.
   c) Aktions-URL. Die Formularübermittlungs-URL, die von der Sicherheitsprüfung ausgenommen werden muss.
   d) Dateityp. Dateityp, der für den Benutzer zum Hochladen zugelassen sein muss.
   e) Kommentare. Eine kurze Beschreibung des Datei-Uploads.
7. Klicken Sie auf **Erstellen**.



8. Klicken Sie auf der Seite **Citrix Web App Firewall profil** auf **OK** und **Fertig** .



Konfiguration und Verwendung der Lernfunktion

December 3, 2021

Die Lernfunktion ist ein Filter für sich wiederholende Muster, der Aktivitäten auf einer Website oder Anwendung beobachtet, die durch die Web App Firewall geschützt ist, um festzustellen, was normale Aktivitäten auf dieser Website oder Anwendung ausmacht. Anschließend wird für jede Sicherheitsüberprüfung, die die Unterstützung der Lernfunktion beinhaltet, eine Liste mit bis zu 2.000 vorgeschlagenen Regeln oder Ausnahmen (Lockerungen) generiert. Benutzer finden

es normalerweise einfacher, Entspannungen mithilfe der Lernfunktion zu konfigurieren, als die erforderlichen Entspannungen manuell einzugeben.

Die Sicherheitsüberprüfungen, die die Lernfunktion unterstützen, sind:

- URL-Prüfung starten
- Cookie-Konsistenzprüfung
- Form Field Consistency Check
- Field Formats Check
- CSRF Form Tagging Check
- HTML SQL Injection Check
- HTML Cross-Site Scripting Check
- XML-Denial-of-Service-Prüfung
- XML Attachment Check
- Interoperabilitätsprüfung der Webdienste

Sie führen zwei verschiedene Arten von Aktivitäten aus, wenn Sie die Lernfunktion verwenden. Zunächst aktivieren und konfigurieren Sie die Funktion für die Verwendung. Sie können das Lernen für den gesamten Datenverkehr zu Ihren geschützten Webanwendungen verwenden, oder Sie können eine Liste von IPs (Liste *Trusted Learning Clients hinzufügen*) konfigurieren, aus der die Lernfunktion Empfehlungen generieren muss. Zweitens, nachdem die Funktion aktiviert wurde und eine bestimmte Menge an Traffic auf Ihre geschützten Websites verarbeitet hat, überprüfen Sie die Liste der vorgeschlagenen Regeln und Lockerungen (gelernte Regeln) und markieren jede mit einer der folgenden Bezeichnungen:

- **Bearbeiten und bereitstellen.** Die Regel wird in das Dialogfeld Bearbeiten gezogen, sodass Sie sie ändern können, und das geänderte Formular wird bereitgestellt.
- **Bereitstellen.** Die unveränderte gelernte Regel wird auf die Liste der Regeln oder Lockerungen für diese Sicherheitsüberprüfung gesetzt.
- **Überspringen.** Die gelernte Regel steht auf einer Liste von Regeln oder Lockerungen, die nicht eingesetzt werden. Die gelernte Regel wird beim Überspringen entfernt. Da sie jedoch nicht zu Entspannungen hinzugefügt werden, werden sie möglicherweise wieder gelernt.

Lernen wird nicht nur durchgeführt, wenn Entspannungen vorhanden sind, außer bei Feldformat-Regeln. Wenn Regeln übersprungen werden, werden sie nur aus der erlernten Datenbank entfernt. Da keine Entspannungen hinzugefügt werden, werden sie möglicherweise wieder gelernt. Wenn die Regeln bereitgestellt werden, werden sie aus der erlernten Datenbank entfernt und es werden auch Lockerungen für die Regeln hinzugefügt. Da Entspannungen hinzukommen, würden sie nicht wieder gelernt werden. Zum Schutz des Feldformats wird das Lernen unabhängig von Entspannungen durchgeführt.

Sie können zwar die Befehlszeilenschnittstelle für die Grundkonfiguration der Lernfunktion verwenden, die Funktion ist jedoch hauptsächlich für die Konfiguration über den Web App Firewall-

Assistenten oder die GUI konzipiert. Sie können die Lernfunktion nur eingeschränkt konfigurieren, indem Sie die Befehlszeile verwenden.

Der Assistent integriert die Konfiguration von Lernfunktionen in die Konfiguration der Web App Firewall als Ganzes und ist daher die einfachste Methode zur Konfiguration dieser Funktion auf einer neuen Citrix ADC Appliance oder bei der Verwaltung einer einfachen Web App Firewall-Konfiguration. Der GUI-Visualisierer und die manuelle Oberfläche bieten beide direkten Zugriff auf alle erlernten Regeln für alle Sicherheitsüberprüfungen und sind daher häufig vorzuziehen, wenn Sie erlernte Regeln für viele Sicherheitsüberprüfungen überprüfen müssen.

Die Lerndatenbank ist auf 20 MB begrenzt, was erreicht wird, nachdem pro Sicherheitsüberprüfung, für die Lernen aktiviert ist, etwa 2.000 gelernte Regeln oder Entspannungen generiert wurden. Wenn Sie gelernte Regeln nicht regelmäßig überprüfen und entweder genehmigen oder ignorieren und dieses Limit erreicht ist, wird ein Fehler im NetScaler-Protokoll protokolliert und es werden keine gelernten Regeln mehr generiert, bis Sie die bestehenden gelernten Regeln und Lockerungen überprüft haben.

Wenn das Lernen aufhört, weil die Datenbank ihre Größenbeschränkung erreicht hat, können Sie das Lernen neu starten, indem Sie entweder die vorhandenen gelernten Regeln und Lockerungen überprüfen oder die Lerndaten zurücksetzen. Nachdem erlernte Regeln oder Lockerungen genehmigt oder ignoriert wurden, werden sie aus der Datenbank entfernt. Nachdem Sie die Lerndaten zurückgesetzt haben, werden alle vorhandenen Lerndaten aus der Datenbank entfernt und auf ihre Mindestgröße zurückgesetzt. Wenn die Datenbank unter 20 MB fällt, wird das Lernen automatisch neu gestartet.

So konfigurieren Sie die Lerneinstellungen mit der Befehlszeilenschnittstelle

Geben Sie das zu konfigurierende Web App Firewall-Profil an, und geben Sie für jede Sicherheitsüberprüfung, die Sie in dieses Profil aufnehmen möchten, den Mindestschwellenwert oder den prozentualen Schwellenwert an. Der Mindestschwellenwert ist eine Ganzzahl, die die Mindestanzahl von Benutzersitzungen darstellt, die die Web App Firewall verarbeiten muss, bevor sie eine Regel oder Entspannung erlernt (Standard: 1). Der prozentuale Schwellenwert ist eine Ganzzahl, die den Prozentsatz der Benutzersitzungen darstellt, in denen die Web App Firewall ein bestimmtes Muster (URL, Cookie, Feld, Anlage oder Regelverletzung) beachten muss, bevor sie eine Regel oder Entspannung erfährt (Standard: 0). Verwenden Sie die folgenden Befehle:

- `set appfw learningsettings <profileName> [-startURLMinThreshold <positive_integer>] [-startURLPercentThreshold <positive_integer>] [-cookieConsistencyMinThreshold <positive_integer>] [-cookieConsistencyPercentThres <positive_integer>] [-CSRFtagMinThreshold <positive_integer>] [-CSRFtagPercentThreshold <positive_integer>] [-fieldConsistencyMinThreshold <positive_integer>] [-fieldConsistencyPercentThreshold <positive_integer>] [-crossSiteScriptingMinThreshold <positive_integer>] [-crossSiteScriptingPerce`

<positive_integer>] [-SQLInjectionMinThreshold <positive_integer>] [-SQLInjectionPercentThreshold <positive_integer>] [-fieldFormatMinThreshold <positive_integer>] [-fieldFormatPercentThreshold <positive_integer>] [-XMLWSIMinThreshold <positive_integer>] [-XMLWSIPercentThreshold <positive_integer>] [-XMLAttachmentMinThreshold <positive_integer>] [-XMLAttachmentPercentThreshold <positive_integer>]

- save ns config

Beispiel

Im folgenden Beispiel werden die Lerneinstellungen im Profil oder der HTML SQL Injection-Sicherheitsüberprüfung aktiviert und konfiguriert. Dies ist eine geeignete Erstkonfiguration des Testbett-Lernens, bei der Sie die vollständige Kontrolle über den Datenverkehr haben, der an die Web App Firewall gesendet wird.

```
set appfw learningsettings pr-basic -SQLInjectionMinThreshold 10
set appfw learningsettings pr-basic -SQLInjectionPercentThreshold 70
save ns config
<!--NeedCopy-->
```

So setzen Sie die Lerneinstellungen mithilfe der Befehlszeilenschnittstelle auf die Standardeinstellungen zurück

Um jede benutzerdefinierte Konfiguration der Lerneinstellungen für das angegebene Profil und die Sicherheitsüberprüfung zu entfernen und die Lerneinstellungen auf ihre Standardeinstellungen zurückzusetzen, geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- unset appfw learningsettings <profileName> [-startURLMinThreshold] [-startURLPercentThreshold] [-cookieConsistencyMinThreshold] [-cookieConsistencyPercentThreshold] [-CSRFtagMinThreshold] [-CSRFtagPercentThresh] [-fieldConsistencyMinThreshold] [-fieldConsistencyPercentThreshold] [-crossSiteScriptingMinThreshold] [-crossSiteScriptingPercentThreshold] [-SQLInjectionMinThreshold] [-SQLInjectionPercentThreshold] [-fieldFormatMinThreshold] [-fieldFormatPercentThreshold] [-XMLWSIMinThreshold] [-XMLWSIPercentThreshold] [-XMLAttachmentMinThreshold] [-XMLAttachmentPercen]
- save ns config

So zeigen Sie die Lerneinstellungen für ein Profil mithilfe der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
show appfw learningsettings <profileName>
```

So zeigen Sie nicht geprüfte gelernte Regeln oder Entspannungen für ein Profil mithilfe der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
show appfw learningdata <profileName> <securityCheck>
```

So entfernen Sie bestimmte nicht geprüfte gelernte Regeln oder Entspannungen mithilfe der Befehlszeilenschnittstelle aus der Lerndatenbank

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
rm appfw learningdata <profileName> (-startURL <expression> | -cookieConsistency
 <string> | (-fieldConsistency <string> <formActionURL>)| (-crossSiteScripting
 <string> <formActionURL>)| (-SQLInjection <string> <formActionURL>)| (-
fieldFormat <string><formActionURL>)| (-CSRFTag <expression> <CSRFFormOriginURL
>)| -XMLDoSCheck <expression> | -XMLWSICheck <expression> | -XMLAttachmentCheck
 <expression>)[-TotalXMLRequests]
```

Beispiel

Im folgenden Beispiel werden alle nicht überprüften gelernten Lockerungen für das Profil, die Sicherheitsüberprüfung HTML SQL Injection, entfernt, die für das Nachnamen-Formularfeld gelten.

```
1 rm appfw learningdata pr-basic -SQLInjection LastName
2 <!--NeedCopy-->
```

So entfernen Sie alle nicht überprüften gelernten Daten mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
reset appfw learningdata
```


So exportieren Sie Lerndaten mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
export appfw learningdata <profileName> <securitycheck>[-target <string>]
```

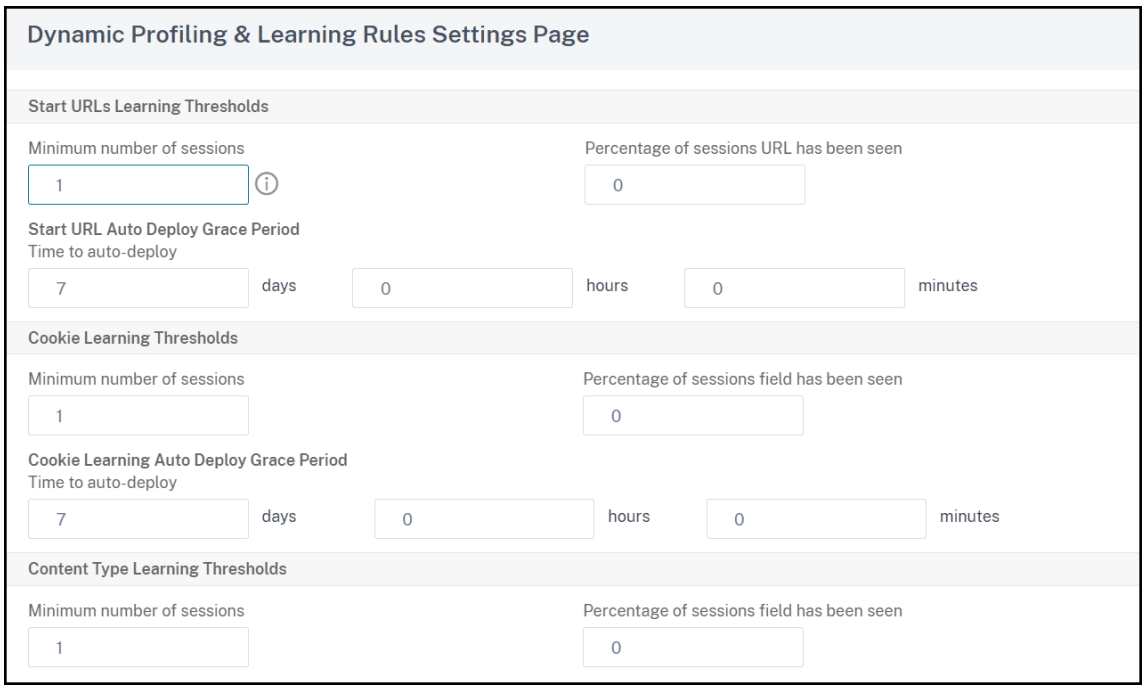
Beispiel

Im folgenden Beispiel werden gelernte Entspannungen für das Profil und die Sicherheitsüberprüfung der HTML SQL Injection in eine Datei im Format mit kommagetrennten Werten (CSV) im Verzeichnis /var/learnt_data/ unter dem im Parameter -target angegebenen Dateinamen exportiert.

```
1 export appfw learningdata pr-basic SQLInjection -target sqli_ld
2 <!--NeedCopy-->
```

So konfigurieren Sie die Lernfunktion mithilfe der GUI

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Profile**.
2. Wählen Sie im Bereich **Profile** das Profil aus, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Gelernte Regeln** .
4. Wählen Sie im Abschnitt “ **Gelernte Regeln** “ eine Sicherheitsüberprüfung aus und klicken Sie auf **Einstellungen**.
5. Legen Sie auf der Seite **Einstellungen für die Sicherheitsprüfung** die folgenden Parameter fest:
   a) **Mindestzahlschwelle.** Je nachdem, welche Lerneinstellungen der Sicherheitsüberprüfung Sie konfigurieren, bezieht sich der Schwellenwert für die Mindestanzahl an Benutzersitzungen, die eingehalten werden müssen, auf die Mindestanzahl von zu beachtenden Anfragen oder auf die Mindestanzahl, wie oft ein bestimmtes Formularfeld eingehalten werden muss. bevor eine erlernte Entspannung erzeugt wird. Standard: 1
   b) **Prozentsatz des Schwellenwerts.** Je nachdem, welche Lerneinstellungen der Sicherheitsüberprüfung Sie konfigurieren, bezieht sich der Schwellenwert in Prozent auf den Prozentsatz der gesamten beobachteten Benutzersitzungen, die gegen die Sicherheitsüberprüfung verstoßen haben, auf den Prozentsatz der Anfragen oder auf den Prozentsatz, mit dem ein Formularfeld mit einem bestimmten Feldtyp übereinstimmte, vor erlernte Entspannung wird erzeugt. Standard: 0
6. Klicken Sie auf **OK** und **Schließen**.



7. Klicken Sie auf **Alle gelernten Daten** entfernen, um alle gelernten Daten zu entfernen und die Lernfunktion zurückzusetzen, sodass sie ihre Beobachtungen von Anfang an erneut starten muss.

   > **Hinweis:**
   >
   > Mit dieser Schaltfläche werden nur gelernte Empfehlungen entfernt, die nicht geprüft und entweder genehmigt oder übersprungen wurden. Erlernte Entspannungen, die akzeptiert und eingesetzt wurden, werden nicht beseitigt.

8. Um die Lernmaschine auf den Datenverkehr von einer bestimmten Gruppe von IPs zu beschränken, klicken Sie auf **Trusted Learning Clients**und fügen Sie die zu verwendenden IP-Adressen zur Liste hinzu.

   a) Um der Liste der vertrauenswürdigen Lernclients eine IP-Adresse oder einen IP-Adressbereich hinzuzufügen, klicken Sie auf **Hinzufügen**.
   b) Geben Sie im Dialogfeld **Trusted Learning Clients hinzufügen** im Listenfeld “Vertrauenswürdige Clients” die IP-Adresse oder einen IP-Adressbereich im CIDR-Format ein.
   c) Geben Sie im Textbereich Kommentare einen Kommentar ein, der diese IP-Adresse oder diesen Bereich beschreibt.
   d) Klicken Sie auf **Erstellen**, um Ihre neue IP-Adresse oder Ihren neuen Bereich zur Liste hinzuzufügen.
   e) Um eine vorhandene IP-Adresse oder einen Bereich zu ändern, klicken Sie auf die IP-Adresse oder den Bereich, und klicken Sie dann auf **Öffnen**. Mit Ausnahme des Namens ist das angezeigte Dialogfeld identisch mit dem Dialogfeld **Trusted Learning Clients**

hinzufügen.

f) Um eine IP-Adresse oder einen Bereich zu deaktivieren oder zu aktivieren, diese jedoch in der Liste zu belassen, klicken Sie auf die IP-Adresse oder den Bereich, und klicken Sie dann entsprechend auf **Deaktivieren oder Aktivieren**.

g) Um eine IP-Adresse oder einen Bereich vollständig zu entfernen, klicken Sie auf die IP-Adresse oder den Bereich, und klicken Sie dann auf **Entfernen**.

9. Klicken Sie auf **Schließen**, um zur Seite Web App Firewall-Profil konfigurieren zurückzukehren.
10. Klicken Sie auf **Fertig**.

So überprüfen Sie gelernte Regeln oder Entspannungen mithilfe der GUI

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Profile**.
2. Wählen Sie im Bereich **Profile** das Profil aus, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Gelernte Regeln** .
4. Wählen Sie im Abschnitt " **Gelernte Regeln** " eine Sicherheitsüberprüfung aus und klicken Sie auf **Einstellungen**.
5. Um die erlernten Daten hierarchisch als verzweigten Baum zu überprüfen, sodass Sie allgemeine Muster auswählen können, die vielen der erlernten Muster entsprechen, klicken Sie auf **Visualizer**.
6. Wenn Sie sich entschieden haben, tatsächlich erlernte Muster zu überprüfen, führen Sie die folgenden Schritte aus.
7. Wählen Sie die erste erlernte Entspannung aus und entscheiden Sie, wie Sie damit umgehen

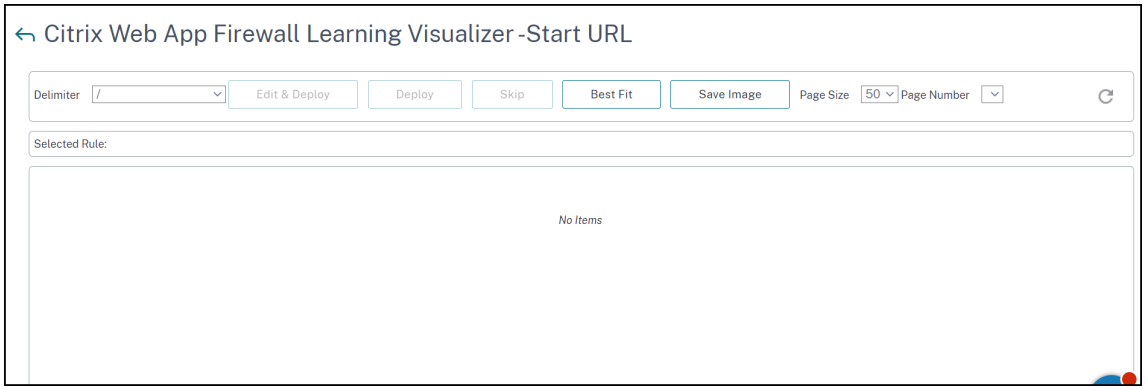
   a) Um die Entspannung zu ändern und dann zu akzeptieren, klicken Sie auf **Bearbeiten und bereitstellen**, bearbeiten Sie den regulären Entspannungsausdruck, und klicken Sie dann auf **OK**.

   b) Um die Entspannung ohne Änderungen zu akzeptieren, klicken Sie auf **Bereitstellen**.

   c) Um die Entspannung aus der Liste zu entfernen, ohne sie bereitzustellen, klicken Sie auf **Überspringen**.

   d) Wiederholen Sie den vorherigen Schritt, um jede weitere gelernte Entspannung zu überprüfen.

8. Klicken Sie auf **Schließen**, um zum Dialogfeld **Gelernte Regeln verwalten** zurückzukehren.
9. Klicken Sie auf **Fertig**.



Dynamische Profilerstellung

October 5, 2021

Die Lernfunktion ist ein Musterfilter, der Aktivitäten auf dem Back-End-Server beobachtet und lernt. Basierend auf der Beobachtung generiert die Lern-Engine bis zu 2000 Regeln oder Ausnahmen (Entspannungen) für jede Sicherheitsprüfung. Um den Prozess zu automatisieren und die Relaxationsregeln automatisch bereitzustellen, verwendet die Citrix ADC Appliance eine dynamische Profilerstellung.

Bei der dynamischen Profilerstellung zeichnet die Appliance die erlernten Daten für einen vordefinierten Schwellenwert auf und sendet eine SNMP-Warnung an den Benutzer. Wenn der Benutzer die Daten nicht innerhalb einer Nachfrist überspringt, stellt die Appliance sie automatisch als Entspannungsregel bereit. Früher musste der Benutzer die Relaxationsregeln manuell bereitstellen. Derzeit ist die dynamische Profilerstellung nur für die folgenden Sicherheitsprüfungen verfügbar:

1. HTML-SQL-Injection
2. HTML Cross-Site-Skripterstellung
3. Feld-Format
4. Start-URL
5. Inhaltstyp
6. Feld-Formate
7. CSRF-Formular-Tagging
8. Cookie-Konsistenz
9. URL verweigern
10. Pufferüberlauf
11. Kreditkarte

Betrachten Sie beispielsweise die Sicherheitsprüfung für HTML SQL Injection, die mit dynamischer Profilerstellung aktiviert ist. Sie können das Lernen für eine Liste von IPs (die sogenannte Liste der

vertrauenswürdigen Lernclients) verwenden, aus der die Lernfunktion Empfehlungen generieren muss. Informationen zum Konfigurieren einer Liste vertrauenswürdiger Clients finden Sie unter Learning Trusted Clients. Wenn der eingehende Datenverkehr Verletzungen hat, wird er als erlernte Daten aufgezeichnet. Wenn die erlernten Daten in der Lern-Engine aufgezeichnet werden, sendet die Appliance eine SNMP-Warnung an den Benutzer. Wenn der Benutzer ein falsches Positiv nicht erkennt und die erlernten Daten nicht innerhalb eines Kulanzzeitraums überspringt, stellt die Appliance diese automatisch als Relaxationsregel bereit.

> **Hinweis:**
> Nachdem Sie das dynamische Profil konfiguriert haben, müssen Sie die Appliance-Konfiguration regelmäßig auf die automatische Bereitstellung der Entspannungsregeln überprüfen und auf der Appliance speichern.

Konfigurieren der dynamischen Profilerstellung mit der Citrix ADC Befehlszeilenschnittstelle

Dynamische Profilerstellung ist für die Sicherheitsprüfung Start URL, HTML Cross-Site Scripting, Field Format oder HTML SQL Injection verfügbar. Um die dynamische Profilerstellung zu konfigurieren, müssen Sie die folgenden Schritte ausführen.

1. Dynamisches Lernen konfigurieren
2. Konfigurieren des Kulanzzeitraums für die automatische Bereitstellung

Dynamisches Lernen konfigurieren

Als ersten Schritt müssen Sie dynamisches Lernen auf Ihrer Appliance konfigurieren. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set appfw profile <profile_name> dynamicLearning <security_checks>
```

Beispiel

```
set appfw profile test1 dynamicLearning SQLInjection CrossSiteScripting
fieldFormat startURL
```

Konfigurieren des Kulanzzeitraums für die automatische Bereitstellung

Sobald Sie das Feature für bestimmte Sicherheitsprüfungen aktiviert haben, müssen Sie den Kulanzzeitraum für die automatische Bereitstellung konfigurieren.

```
set appfw learningsettings <profile name> -crossSiteScriptingAutoDeployGracePeriod
 <seconds>
```



```
set appfw learningsettings <profile name> fieldFormatAutoDeploymentGracePeriod
 <seconds>

set appfw learningsettings <profile name> SQLInjectionAutoDeploymentGracePeriod
 <seconds>

set appfw learningsettings <profile name> -startURLAutoDeployGracePeriod <
seconds>
```

Beispiel

```
set appfw learningsettings test1 -crossSiteScriptingAutoDeployGracePeriod 30

set appfw learningsettings test1 -startURLAutoDeployGracePeriod 7

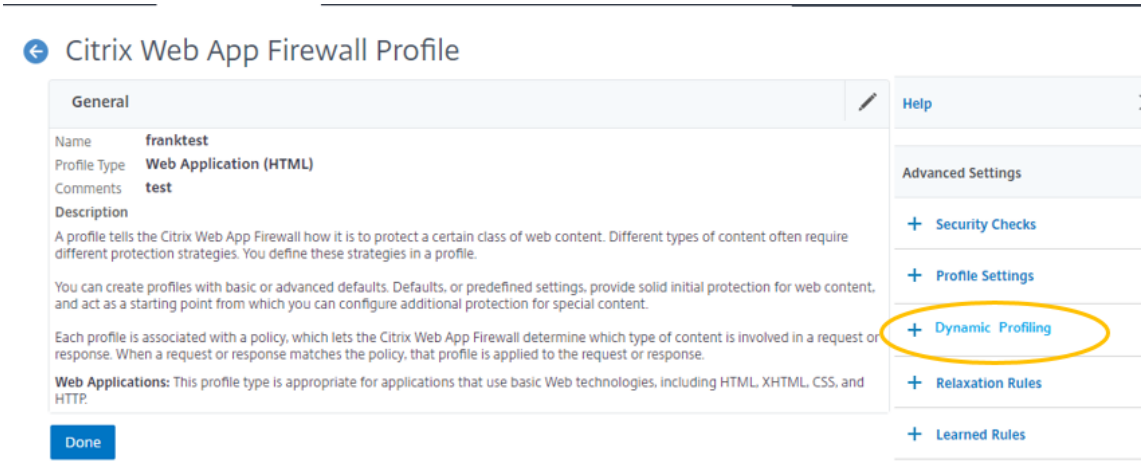
set appfw learningsettings test1 -fieldFormatAutoDeploymentGracePeriod 10

set appfw learning settings test1 -SQLInjectionAutoDeploymentGracePeriod 12
```

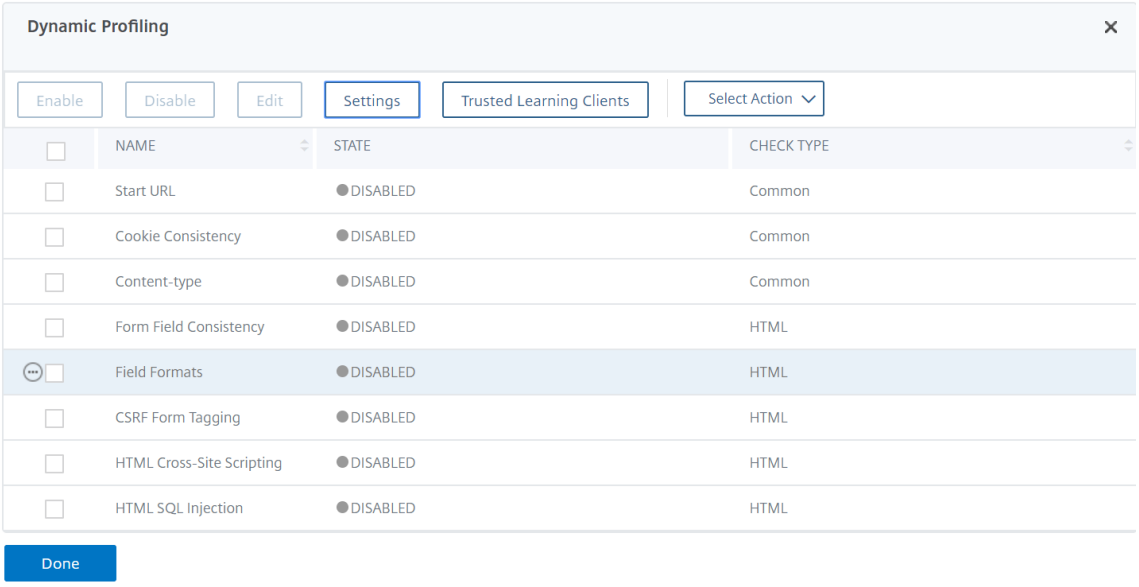
> **Hinweis:**
>
> Hier liegt der Kulanzzeitraum für die automatische Bereitstellung in Minuten.

Konfigurieren der dynamischen Profilerstellung mit der Citrix ADC GUI

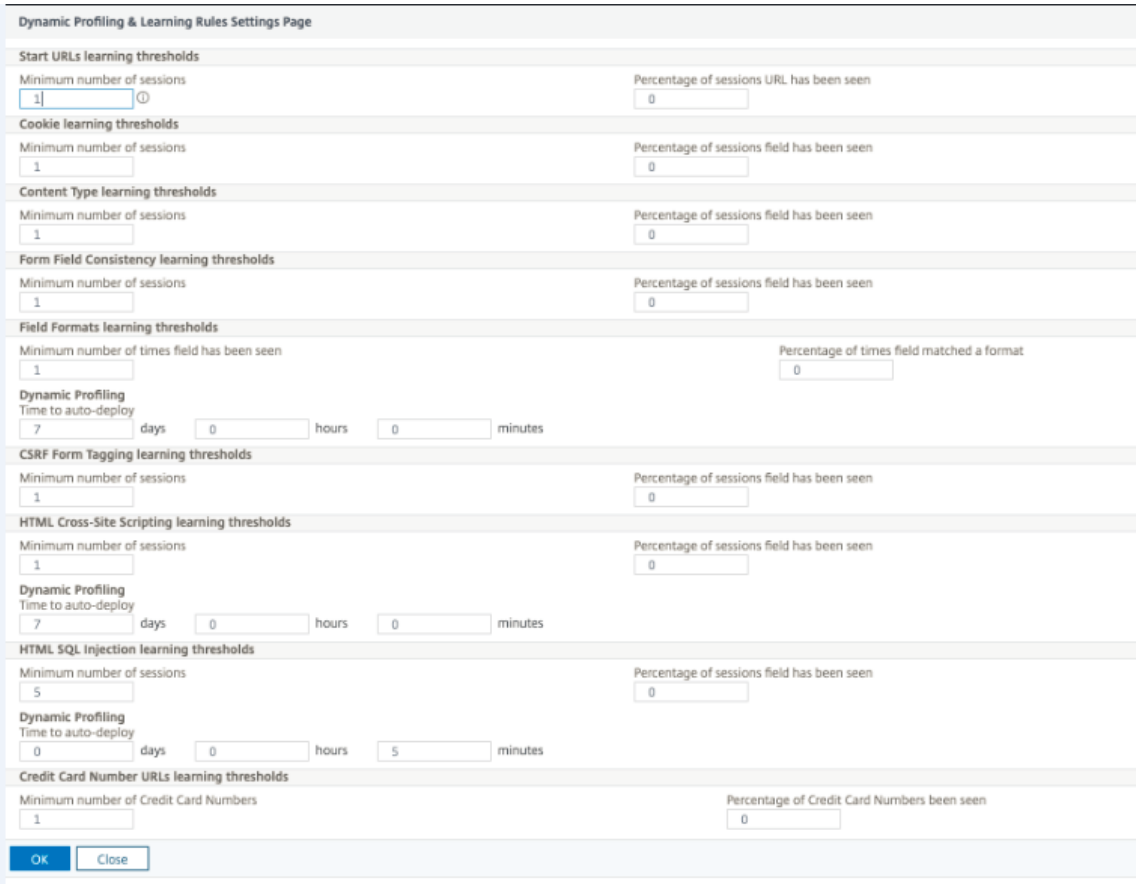
1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profil**.
2. Wählen Sie im Detailbereich ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Citrix Web App-Profil** unter **Erweiterte Einstellungen** auf **Dynamische Profilerstellung** .



4. Wählen Sie im Abschnitt **Dynamische Profilerstellung** eine Sicherheitsprüfung aus, und klicken Sie auf **Bearbeiten** .



5. Legen Sie auf der Seite **Dynamische Profilerstellungs- und Lerneinstellungen** den Kulanzzeitraum für die Sicherheitsprüfung fest.



6. Klicken Sie auf **OK** und **Fertig**.

Export und Import von Entspannungsregeln

Wenn Sie die dynamische Profilerstellung aktivieren, werden die erlernten Daten automatisch als Relaxationsregeln bereitgestellt. Darüber hinaus können Sie mit der Appliance auch die dynamischen Profilerstellungsregeln und regulären Entspannungsregeln exportieren. Sie können die Regeln aus der Staging-Umgebung exportieren und in die Produktionsumgebung importieren.

> **Hinweis:**
>
> Wenn Sie Regeln in die Produktionsumgebung importieren, müssen Sie sicherstellen, dass der Prozess additiv ist und die vorhandene Konfiguration nicht außer Kraft setzt.

Wie man Relaxationsregeln exportiert und importiert

Um die Relaxationsregeln zu exportieren und zu importieren, müssen Sie die folgenden Schritte ausführen:

1. Sie müssen zuerst die dynamischen profilbasierten Daten exportieren. Dazu steht für die Relaxationsregeln im WAF-Profil die Exportoption zur Verfügung. Wenn Sie diese Option auswählen, exportieren Sie die Relaxationsregeln für dynamische Profilerstellung und reguläre Relaxationsregeln. Sie können die Exportoption verwenden, um die Konfiguration als komprimiertes Paket auf der Appliance herunterzuladen.
2. Nachdem Sie die Daten aus der Stagingumgebung exportiert haben, müssen Sie sie in eine andere Citrix ADC Appliance importieren. Dazu müssen Sie die Importoption verwenden, die in den Relaxationsregeln des WAF-Profils verfügbar ist. Wenn Sie diese Option auswählen, importiert die Appliance die angegebenen Relaxationsregeln im Paket und stellt sie im WAF-Profil der ausgewählten Appliance wieder her.

> **Hinweis:**
>
> Wenn Sie Relaxationsregeln in ein WAF-Profil importieren möchten, gibt es zwei Arten von Aktionen:
> Erweitern — Diese Aktion stellt sicher, dass der Import additiv ist, sodass keine vorhandene Konfiguration außer Kraft gesetzt wird.
> Überschreiben — Diese Aktion überschreibt die vorhandene Konfiguration mit der Konfiguration, die im komprimierten Exportpaket vorhanden ist."

Importieren Sie archivierte Relaxationsregeldatei mithilfe von CLI

Um die Entspannungsregeln zu importieren, müssen Sie das Archiv in die Citrix ADC Appliance importieren und dann den Restore-Befehl ausführen, um die Konfiguration zu extrahieren. Der folgende Satz von CLI-Befehlen kann zum Exportieren, Importieren und Verwalten der Konfigurationen verwendet werden.

Um die archivierte Datei vom bestimmten Speicherort zu importieren und wiederherzustellen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
import appfw archive <src> <name> [-comment <string>]
```

Wo,
“src”: Gibt die Quelle der tar-Archivdatei im Formular an, <protocol>://<host>[:<port>][/<path>]
“name”: Gibt den Namen des Archivs an.
“ comment”: Kommentare, die mit diesem Archiv verknüpft sind.

```
restore appfw profile <archivename> [-relaxationRules] [-importProfileName <string>] [-matchUrlString <string>] [-replaceUrlString <string>] [-overwrite] [-augment]
```

Wo,
archivename: Zeigt die Quelle für das TAR-Archiv an. Dies ist ein obligatorisches Argument.
“RelaxationRules”: Option zum Importieren aller appfw-Entspannungsregeln.

importProfileName: Gibt den Profilnamen an, der erstellt oder aktualisiert wurde, um die Entspannungsregeln während des Wiederherstellungsvorgangs zuzuord
“ MatchUrlString”: Gibt die Action-URL-Zeichenfolge an, die in archivierten Relaxationsregeln übereinstimmt.

replaceUrlString: Zeigt die Zeichenfolge an, die in Aktion ersetzt werden soll, während Entspannungsregeln wiederhergestellt werden soll.

overwrite: Bestehende Regelaktion, um bestehende Entspannungsregeln zu bereinigen und während des Imports zu ersetzen.

augment: Bestehende Regelaktion zur VersteiGERUNG von Relaxationsregeln während des Imports.

Beispiel:

```
import appfw archive local: dutA_test_pr.tgz demo
restore appfw profile dutA_test_pr
```

Exportieren Sie die archivierte Datei über die Befehlszeilenschnittstelle in die ausgewählte Appliance

Wenn Sie die Appfw-Entspannungsregeln mit CLI exportieren, müssen Sie die Konfiguration archivieren und dann exportieren.
Um die archivierte Datei zu archivieren und zu exportieren, geben Sie an der Eingabeaufforderung Folgendes ein:

```
archive appfw profile <name> <archivename> [-comment <string>]
```


Wo,
`archive name`: Zeigt die Quelle für das TAR-Archiv an. Dies ist ein obligatorisches Argument.
`name`: Gibt den appfw-Profilnamen an, der die zu exportierenden Entspannungsregeln enthält

```
export appfw archive <name> <target>
```

Wo,
Name. Name des tar-Archivs. Dies ist ein obligatorisches Argument. Maximale Länge: 31
Ziel. Pfad zu der Datei, die exportiert werden soll. Dies ist ein obligatorisches Argument. Maximale Länge: 2047

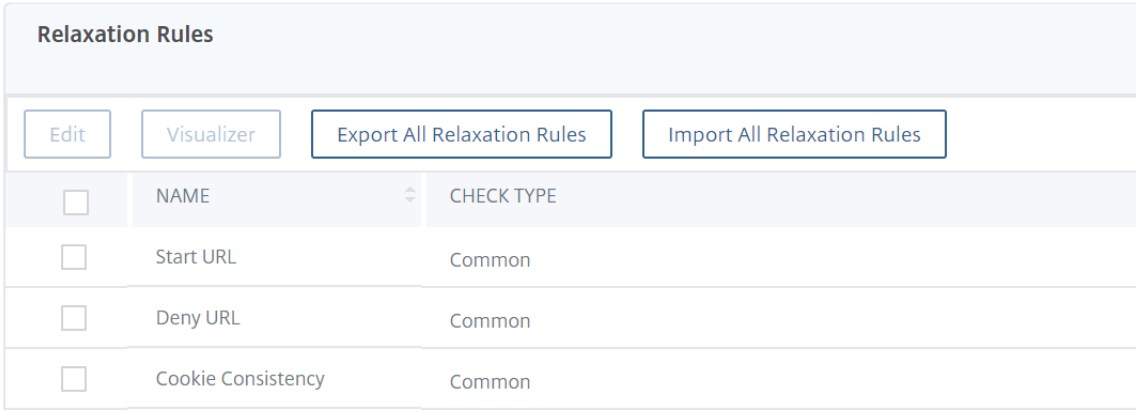
Beispiel:

```
> archive appfw profile test_pr archived_test_pr
> export appfw archive archived_test_pr local:dutA_test_pr
```

So exportieren Sie Relaxationsregeln über die Citrix ADC GUI

Befolgen Sie die unten angegebenen Schritte, um Relax-Regeln zu exportieren:

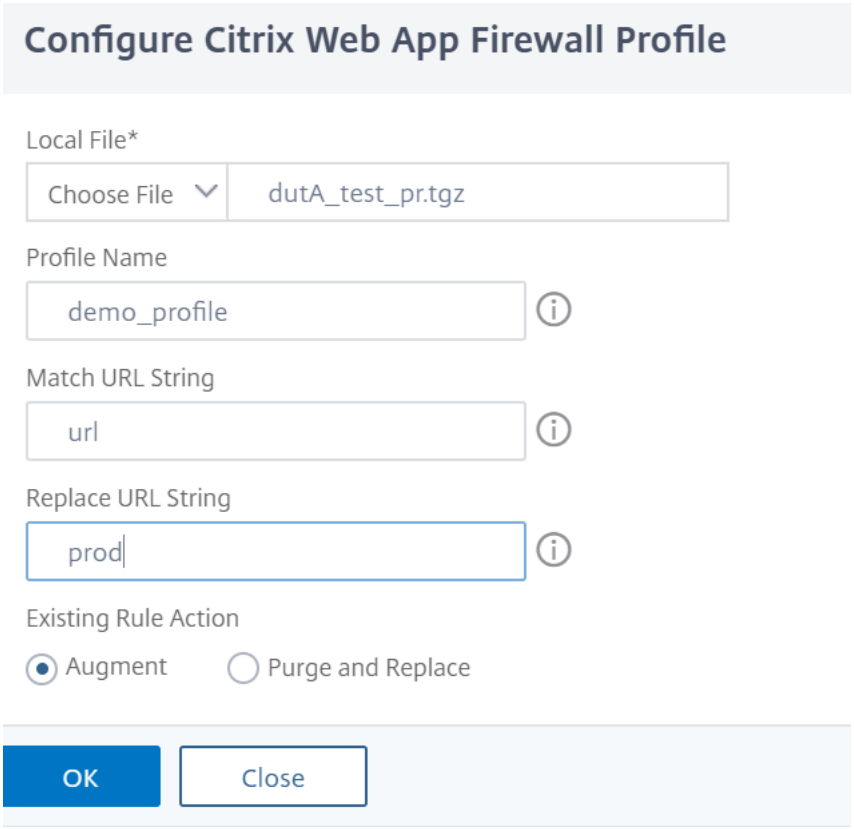
1. Navigieren Sie zu **Sicherheit** > **Citrix Web App Firewall**.
2. Klicken Sie auf der Detailseite unter **Konfigurationsübersicht** auf den Link **Citrix Web App Firewall Profile**.
3. Klicken Sie auf der Seite **Citrix Web App Firewall Profil** im Abschnitt **Erweiterte Einstellungen** auf den Link **Relax-Regeln**.
4. Klicken Sie im Abschnitt **Entspannungsregeln** auf **Alle Entspannungsregeln exportieren**. Die Aktion gilt für alle Sicherheitsprüfungen und für diejenigen, die dynamisches Lernen in diesem Profil aktiviert ist.



So importieren Sie Relaxationsregeln über die Citrix ADC GUI

Führen Sie die Schritte aus, um Entspannungsregeln zu importieren:

1. Navigieren Sie zu **Sicherheit** > **Citrix Web App Firewall**.
2. Klicken Sie auf der Detailseite unter **Konfigurationsübersicht** auf den Link **Citrix Web App Firewall Profile**.
3. Klicken Sie auf der Seite **Citrix Web App Firewall Profil** im Abschnitt **Erweiterte Einstellungen** auf den Link **Relax-Regeln**.
4. Klicken Sie im Abschnitt **Entspannungsregeln** auf **Alle Entspannungsregeln importieren**.
5. Legen Sie auf der Seite **Citrix Web App Firewall profil konfigurieren** die folgenden Parameter fest:
   a) Lokale Datei. Name der komprimierten archivierten Datei, die die Entspannungsregeln enthält.
   b) Profilname Name des Profils, an das die Entspannungsregeln gebunden sind.
   c) Passende URL-Zeichenfolge. Teil der URL, der übereinstimmt.
   d) URL-Zeichenfolge ersetzen. Teil der URL, der die URL-Zeichenfolge ersetzt.
   e) Vorhandene Regelaktion. Wählen Sie diese Option aus, ob die Regel vorhandene Regeln überschreiben oder die vorhandenen Regeln erweitern muss.
6. Klicken Sie auf **OK**.



Ergänzende Informationen zu Profilen

April 7, 2022

Im Folgenden finden Sie zusätzliche Informationen zu bestimmten Aspekten von Web App Firewall-Profilen. In diesen Informationen wird erläutert, wie Sonderzeichen in eine Sicherheitsüberprüfungsregel oder Entspannung aufgenommen werden und wie Variablen beim Konfigurieren von Profilen verwendet werden.

Unterstützung von Konfigurationsvariablen

Anstatt statische Werte zu verwenden, können Sie zum Konfigurieren der Sicherheitsüberprüfungen und -einstellungen der Web App Firewall jetzt benannte Citrix ADC-Standardvariablen verwenden. Durch das Erstellen von Variablen können Sie Konfigurationen einfacher exportieren und dann in neue Citrix ADC Appliances importieren oder vorhandene Citrix ADC Appliances aus einem einzigen Satz von Konfigurationsdateien aktualisieren. Dies vereinfacht Updates, wenn Sie ein Testbett-Setup verwenden, um eine komplexe Web App Firewall-Konfiguration zu entwickeln, die auf Ihr lokales Netzwerk und Ihre Server abgestimmt ist, und diese Konfiguration dann auf Ihre Citrix ADC-Produktionsanlagen übertragen.

Sie erstellen Web App Firewall Konfigurationsvariablen auf die gleiche Weise wie alle anderen Citrix ADC Variablen, die nach den standardmäßigen Citrix ADC-Konventionen ausgeführt werden. Sie können eine benannte Ausdrucksvariable erstellen, indem Sie die GUI und die Citrix ADC-Befehlszeilenschnittstelle verwenden.

Die folgenden URLs und Ausdrücke können mit Variablen anstelle von statischen Werten konfiguriert werden:

- **URL starten** (-starturl)
- **URL verweigern** (-denyurl)
- **Formularaktions-URL** für *Konsistenzprüfung von Formularfeldern* (-fieldconsistency)
- **Aktions-URL** für *XML SQL Injection Check* (-xmlSQLInjection)
- **Aktions-URL** für *XML-Cross-Site-Scripting Check* (-xmlcross-site scripting)
- **Formularaktions-URL** für *HTML SQL Injection Check* (-sqlInjection)
- **Formularaktions-URL** für *Field Format Check* (-fieldFormat)
- **Formularursprung-URL** und **Formularaktions-URL** für die *Prüfung auf websiteübergreifende Anforderungsfälschung (CSRF)* (-csrfTag)
- **Formularaktions-URL** für die *HTML Cross-Site Scripting Check* (-crossSiteScripting)
- **Safe Object** (-safeObject)
- **Aktions-URL** für *XML Denial-of-Service (XDoS)-Prüfung* (-XMLDoS)
- **URL** für die *Interoperabilitätsprüfung von Webdiensten* (-XMLWSIURL)
- <**URL** für die *XML-Validierungsprüfung* (-XMLValidationURL)

- **URL** für die *Überprüfung von XML-Anhängen* (-XMLAttachmentURL)

Weitere Informationen finden Sie unter Richtlinien und Ausdrücke.

Um eine Variable in der Konfiguration zu verwenden, schließen Sie den Variablennamen zwischen zwei bei (@) -Symbolen ein und verwenden sie dann genau so, wie Sie den statischen Wert, den sie ersetzt. Wenn Sie beispielsweise die Deny-URL-Prüfung über die grafische Benutzeroberfläche konfigurieren und die benannte Ausdrucksvariable myDenyURL zur Konfiguration hinzufügen möchten, geben Sie @myDenyURL@ in das Dialogfeld Verweigern-URL hinzufügen im Textbereich URL verweigern ein. Um dieselbe Aufgabe mithilfe der Citrix ADC-Befehlszeile auszuführen, geben Sie appfw profile <name> -denyURLAction @myDenyURL@ ein.

PCRE-Zeichencodierungsformat

Das Citrix ADC-Betriebssystem unterstützt nur die direkte Eingabe von Zeichen in den druckbaren ASCII-Zeichensatz — Zeichen mit Hexadezimalcodes zwischen HEX 20 (ASCII 32) und HEX 7E (ASCII 127). Um ein Zeichen mit einem Code außerhalb dieses Bereichs in Ihre Web App Firewall-Konfiguration aufzunehmen, müssen Sie seinen UTF-8-Hexadezimalcode als regulären PCRE-Ausdruck eingeben.

Für eine Reihe von Zeichentypen ist die Codierung mit einem regulären PCRE-Ausdruck erforderlich, wenn Sie sie als URL, Formularfeldname oder Safe-Object-Ausdruck in Ihre Web App Firewall-Konfiguration aufnehmen. Sie beinhalten:

- **Obere-ASCII-Zeichen.** Zeichen mit Kodierungen von HEX 7F (ASCII 128) bis HEX FF (ASCII 255). Abhängig von der verwendeten Zeichenzuordnung können sich diese Kodierungen auf Steuercodes, ASCII-Zeichen mit Akzenten oder anderen Modifikationen, nicht-lateinische Alphabet-Zeichen und Symbole beziehen, die nicht im ASCII-Basissatz enthalten sind. Diese Zeichen können in URLs, Formularfeldnamen und sicheren Objektausdrücken vorkommen.
- **Doppelbyte-Zeichen.** Zeichen mit Kodierungen, die zwei 8-Byte-Wörter verwenden. Doppelbyte-Zeichen werden hauptsächlich für die Darstellung von chinesischem, japanischem und koreanischem Text in elektronischer Form verwendet. Diese Zeichen können in URLs, Formularfeldnamen und sicheren Objektausdrücken vorkommen.
- **ASCII-Steuerzeichen.** Nicht druckbare Zeichen, die zum Senden von Befehlen an einen Drucker verwendet werden. Alle ASCII-Zeichen mit Hexadezimalcodes kleiner als HEX 20 (ASCII 32) fallen in diese Kategorie. Diese Zeichen dürfen jedoch niemals in einem URL- oder Formularfeldnamen vorkommen und würden selten, wenn überhaupt, in einem sicheren Objektausdruck vorkommen.

Die Citrix ADC Appliance unterstützt nicht den gesamten UTF-8-Zeichensatz, sondern nur die Zeichen in den folgenden acht Zeichensätzen:

- **Englisch US (ISO-8859-1).** Obwohl die Bezeichnung “English US” lautet, unterstützt die Web App Firewall alle Zeichen im ISO-8859-1-Zeichensatz, auch Latin-1-Zeichensatz genannt. Dieser Zeichensatz repräsentiert vollständig die meisten modernen westeuropäischen Sprachen und repräsentiert alle bis auf einige ungewöhnliche Zeichen im Rest.
- **Traditionelles Chinesisch (Big5).** Die Web App Firewall unterstützt alle Zeichen im BIG5-Zeichensatz, der alle traditionellen chinesischen Schriftzeichen (Ideogramme) enthält, die im modernen Chinesisch häufig verwendet werden, wie sie in Hongkong, Macau, Taiwan und von vielen Menschen chinesischer ethnischer Herkunft, die außerhalb des chinesischen Festlandes leben, gesprochen und geschrieben werden.
- **Chinesisch vereinfacht (GB2312).** Die Web App Firewall unterstützt alle Zeichen im GB2312-Zeichensatz, der alle im modernen Chinesisch gebräuchlichen vereinfachten chinesischen Schriftzeichen (Ideogramme) enthält, wie sie auf dem chinesischen Festland gesprochen und geschrieben werden.
- **Japanisch (SJIS).** Die Web App Firewall unterstützt alle Zeichen im Shift-JIS (SJIS) -Zeichensatz, der die meisten Zeichen (Ideogramme) enthält, die üblicherweise im modernen Japanisch verwendet werden.
- **Japanisch (EUC-JP).** Die Web App Firewall unterstützt alle Zeichen im EUC-JP-Zeichensatz, einschließlich aller Zeichen (Ideogramme), die üblicherweise im modernen Japanisch verwendet werden.
- **Koreanisch (EUC-KR).** Die Web App Firewall unterstützt alle Zeichen im EUC-KR-Zeichensatz, einschließlich aller Zeichen (Ideogramme), die üblicherweise im modernen Koreanisch verwendet werden.
- **türkisch (ISO-8859-9).** Die Web App Firewall unterstützt alle Zeichen im ISO-8859-9-Zeichensatz, der alle im modernen Türkisch verwendeten Buchstaben umfasst.
- **Unicode (UTF-8).** Die Web App Firewall unterstützt bestimmte zusätzliche Zeichen im UTF-8-Zeichensatz, einschließlich solcher, die im modernen Russisch verwendet werden.

Bei der Konfiguration der Web App Firewall geben Sie alle Nicht-ASCII-Zeichen als reguläre Ausdrücke im PCRE-Format ein, indem Sie den Hexadezimalcode verwenden, der diesem Zeichen in der UTF-8-Spezifikation zugewiesen ist. Symbolen und Zeichen innerhalb des normalen ASCII-Zeichensatzes, denen in diesem Zeichensatz einzelne, zweistellige Codes zugewiesen sind, werden im UTF-8-Zeichensatz dieselben Codes zugewiesen. Zum Beispiel das Ausrufezeichen (!) , dem der Hexadezimalcode 21 im ASCII-Zeichensatz zugewiesen ist, ist auch Hex 21 im UTF-8-Zeichensatz. Symbolen und Zeichen aus einem anderen unterstützten Zeichensatz sind paarweise Hexadezimalcodes im UTF-8-Zeichensatz zugewiesen. Zum Beispiel wird dem Buchstaben a mit einem akuten Akzent (á) der UTF-8-Code C3 A1 zugewiesen.

Die Syntax, die Sie verwenden, um diese UTF-8-Codes in der Konfiguration der Web App Firewall darzustellen, ist “xNN” für ASCII-Zeichen, “\ xNN\ xNN” für Nicht-ASCII-Zeichen, die in Englisch,

Russisch und Türkisch verwendet werden, und "\ xNN\ xNN\ xNN" für Zeichen, die in Chinesisch, Japanisch und Koreanisch verwendet werden. Zum Beispiel, wenn Sie eine! in einem regulären Ausdruck der Web App Firewall als UTF-8-Zeichen würden Sie\ x21 eingeben. Wenn Sie ein á einschließen möchten, geben Sie\ xC3\ xA1 ein.

> **Hinweis:**
>
> Normalerweise müssen Sie keine ASCII-Zeichen im UTF-8-Format darstellen, aber wenn diese Zeichen einen Webbrowser oder ein zugrunde liegendes Betriebssystem verwirren könnten, können Sie die UTF-8-Darstellung des Charakters verwenden, um diese Verwirrung zu vermeiden. Wenn eine URL beispielsweise ein Leerzeichen enthält, möchten Sie den Space möglicherweise als x20 codieren, um bestimmte Browser und Webserver-Software nicht zu verwechseln.

Im Folgenden finden Sie Beispiele für URLs, Formularfeldnamen und sichere Objektausdrücke, die Nicht-ASCII-Zeichen enthalten, die als reguläre Ausdrücke im PCRE-Format eingegeben werden müssen, um in die Konfiguration der Web App Firewall aufgenommen zu werden. Jedes Beispiel zeigt zuerst die tatsächliche URL, den Feldnamen oder die Ausdruckszeichenfolge, gefolgt von einem regulären Ausdruck im PCRE-Format.

- Eine URL mit erweiterten ASCII-Zeichen.

  Aktuelle URL: `http://www.josénuñez.com`

  Codierte URL: `^http://www\[.\]jos\xC3\xA9nu\xC3\xB1ez\[.\]com$`

- Eine weitere URL mit erweiterten ASCII-Zeichen.

  Aktuelle URL: `http://www.example.de/trömso.html`

  Codierte URL: `^http://www[.]example\[.]de/tr\xC3\xB6mso[.]html$`

- Ein Formularfeldname mit erweiterten ASCII-Zeichen.

  `Actual Name: nome_do_usuário`

  Codierter Name: `^nome_do_usu\xC3\xA1rio$`

- Ein sicherer Objektausdruck, der erweiterte ASCII-Zeichen enthält.

  Uncodierter Ausdruck [A-Z] {3,6} ¥[1-9][0-9]{6,6}

  Codierter Ausdruck: [A-Z] {3,6}\ xC2\ xA5[1-9][0-9]{6,6}

Sie können eine Reihe von Tabellen finden, die den gesamten Unicode-Zeichensatz und die passenden UTF-8-Kodierungen im Internet enthalten. Eine nützliche Website, die diese Informationen enthält, befindet sich unter der folgenden URL:

`http://www.utf8-chartable.de/unicode-utf8-table.pl`

Damit die Zeichen in der Tabelle auf dieser Website korrekt angezeigt werden, muss auf Ihrem Computer eine entsprechende Unicode-Schriftart installiert sein. Wenn Sie dies nicht tun, ist die visuelle

Anzeige des Charakters möglicherweise fehlerhaft. Selbst wenn Sie keine geeignete Schriftart zur Anzeige eines Zeichens installiert haben, sind die Beschreibung und die UTF-8- und UTF-16-Codes auf diesen Webseiten korrekt.

Invertierte PCRE-Ausdrücke

Zusätzlich zum übereinstimmenden Inhalt, der ein Muster enthält, können Sie auch Inhalt zuordnen, der kein Muster enthält, indem Sie einen invertierten PCRE-Ausdruck verwenden. Um einen Ausdruck umzukehren, fügen Sie einfach ein Ausrufezeichen (!) gefolgt von Leerraum als erstes Zeichen im Ausdruck.

> **Hinweis:** Wenn ein Ausdruck nur aus einem Ausrufezeichen besteht und nichts folgt, wird das Ausrufezeichen als Literalzeichen behandelt und nicht als Syntax, die einen invertierten Ausdruck angibt.

Die folgenden Web App Firewall Befehle unterstützen invertierte PCRE-Ausdrücke:

- Start-URL (URL)
- URL verweigern (URL)
- Konsistenz des Formularfeldes (Formularaktions-URL)
- Cookie-Konsistenz (Formularaktions-URL)
- Websiteübergreifende Anforderungsfälschung (CSRF) (Formularaktions-URL)
- HTML Cross-site Scripting (Formularaktions-URL)
- Feldformat (Formularaktions-URL)
- Feldtyp (Typ)
- Vertrauliches Feld (URL)

Hinweis: Wenn die Sicherheitsüberprüfung ein IsRegex-Flag oder -Kontrollkästchen enthält, muss sie auf YES gesetzt oder aktiviert sein, um reguläre Ausdrücke im Feld zu aktivieren. Andernfalls wird der Inhalt dieses Feldes als Literal behandelt und es werden keine regulären Ausdrücke (invertiert oder nicht) analysiert.

Unzulässige Namen für Web App Firewall-Profile

Die folgenden Namen werden integrierten Aktionen und Profilen auf der Citrix ADC Appliance zugewiesen und können nicht als Namen für ein vom Benutzer erstelltes Web App Firewall-Profil verwendet werden.

- AGRESSIVE
- ALLOW
- BASIC
- CLIENTAUTH
- COMPRESS

- CSSMINIFY
- DEFLATE
- DENY
- DNS-NOP
- DROP
- GZIP
- HTMLMINIFY
- IMGOPTIMIZE
- JSMINIFY
- MODERATE
- NOCLIENTAUTH
- NOCOMPRESS
- NONE
- NOOP
- NOREWRITE
- RESET
- SETASLEARNNSLOG_ACT
- SETNSLOGPARAMS_ACT
- SETSYSLOGPARAMS_ACT
- SETTMSESSPARAMS_ACT
- SETVPNPARAMS_ACT
- SET_PREAUTHPARAMS_ACT
- default_DNS64_action
- dns_default_act_Cachebypass
- dns_default_act_Drop
- nshttp_default_profile
- nshttp_default_strict_validation
- nstcp_default_Mobile_profile
- nstcp_default_XA_XD_profile
- nstcp_default_profile
- nstcp_default_tcp_interactive_stream
- nstcp_default_tcp_lan
- nstcp_default_tcp_lan_thin_stream
- nstcp_default_tcp_lfp
- nstcp_default_tcp_lfp_thin_stream
- nstcp_default_tcp_lnp
- nstcp_default_tcp_lnp_thin_stream
- nstcp_internal_apps

Benutzerdefinierter Fehlerstatus und Meldung für HTML-, XML- und JSON-Fehlerobjekt

October 5, 2021

Wenn die Citrix Web App Firewall einen Verstoß erkennt, verarbeitet die Appliance das Fehlerszenario entweder mit einer Umleitungs-URL oder dem Fehlerobjekt (in das Profil importiert und aktiviert). Wenn das Szenario mit einer Fehlerobjektkonfiguration behandelt wird, liefert das WAF-Profil einen benutzerdefinierten Antwortstatuscode und eine benutzerdefinierte Meldung. Sie können die Antwortfehlerdetails für ein HTML-, XML- oder JSON-Fehlerobjekt im WAF-Profil anpassen.

> **Hinweis:**
>
> Standardmäßig werden der Fehlercode und die Fehlermeldung auf “200” und “OK” festgelegt, wenn die Einstellungen für Fehlerobjekte konfiguriert sind.

Beim Umgang mit Fehlerszenarien ist es wichtig, dass die Appliance mit dem entsprechenden HTTP-Antwortstatuscode und einer entsprechenden Meldung für die Behebung von Problemen antwortet. Durch die Bereitstellung einer benutzerdefinierten Fehlerstatusmeldung und eines benutzerdefinierten Fehlerstatuscodes kann die Appliance einen besseren Benutzereingriff ermöglichen, um ein Problem bei Auftreten eines Verstoßes zu beheben. Wenn Sie beispielsweise den Antwortfehlercode auf “404” und die Statusmeldung auf “Nicht gefunden” setzen, kann der Benutzer den Antwortstatuscode und die Nachricht überprüfen, um zu überprüfen, ob ein Verstoß aufgetreten ist. Dies kann dem Benutzer helfen, Antworten zu filtern, die das Fehlerobjekt enthalten

Konfigurieren Sie den benutzerdefinierten Statuscode und die Meldung für ein HTML-Fehlerobjekt in einem WAF-Profil über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set appfw profile <profile-name> -HTMLErrorStatusCode <value> -
    HTMLErrorStatusMessage <value> -useHTMLErrorObject ON
<!--NeedCopy-->
```

Beispiel:

```
set appfw profile profile_1 -HTMLErrorStatusCode 404 -HTMLErrorStatusMessage
  “Not Found”  -useHTMLErrorObject ON
```


Konfigurieren Sie den benutzerdefinierten Statuscode und die Meldung für das XML-Fehlerobjekt in einem WAF-Profil über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set appfw profile <profile-name> -XMLErrorStatusCode <value> -
     XMLErrorStatusMessage <value>
2 <!--NeedCopy-->
```

Beispiel:

```
set appfw profile profile_1 -XMLErrorStatusCode 406 - XMLErrorStatusMessage
  “Not Acceptable”
```

Konfigurieren Sie den benutzerdefinierten Statuscode und die Meldung für das JSON-Fehlerobjekt in einem WAF-Profil über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set appfw profile <profile-name> -JSONErrorStatusCode <value> -
     JSONErrorStatusMessage <value>
2 <!--NeedCopy-->
```

Beispiel:

```
set appfw profile profile_1 -JSONErrorStatusCode 500 - JSONErrorStatusMessage
  “Internal Server Error”
```

Konfigurieren Sie den benutzerdefinierten Statuscode und die Nachricht für HTML-, JSON- oder XML-Fehlerobjekt in einem WAF-Profil über die grafische Benutzeroberfläche

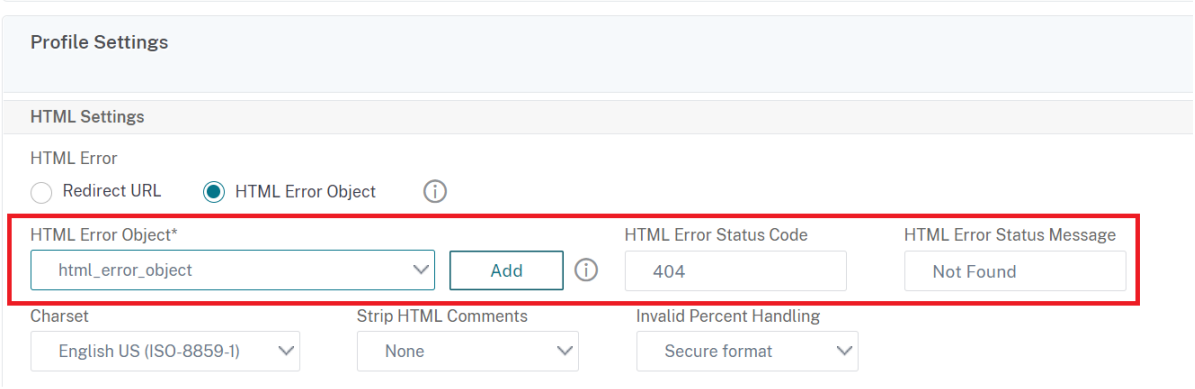
1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profile**.
2. Klicken Sie im Detailbereich auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Web App Firewall-Profil erstellen** im Abschnitt **Erweiterte Einstellungen** auf **Profileinstellungen**.
4. Legen Sie im Abschnitt **Profileinstellungen** die folgenden Parameter fest.

   a. HTML-Fehlerobjekt. Wählen Sie die Option zur Übergabe von Fehlerszenarien mit einem HTML-Fehlerobjekt aus. Importieren Sie das Fehlerobjekt aus einer URL, Datei oder einem Text.

b. HTML-Fehlerstatuscode. Geben Sie einen benutzerdefinierten Fehlerstatuscode an.
c. HTML-Fehlerstatusmeldung Geben Sie eine Kundenfehlermeldung ein.

5. Klicken Sie auf **OK** und **Fertig**.

> **Hinweis:**
>
> Das gleiche Verfahren gilt für benutzerdefinierte Fehlerobjekteinstellungen von JSON und XML.



Richtlinienbezeichnungen

October 5, 2021

Eine Richtlinienbezeichnung besteht aus einer Reihe von Richtlinien, anderen Richtlinienbezeichnungen und virtuellen serverspezifischen Richtlinienbanken. Die Web App Firewall wertet jede an die Richtlinienbezeichnung gebundene Richtlinie in der Reihenfolge ihrer Priorität aus. Wenn die Richtlinie übereinstimmt, filtert sie die Verbindung wie im zugeordneten Profil angegeben. Dann wird ausgeführt, was auch immer der Goto-Parameter angegeben hat. Dies kann sein, um die Richtlinienbewertung zu beenden, zur nächsten Richtlinie zu wechseln oder zu der Richtlinie mit der angegebenen Priorität zu wechseln. Wenn der Parameter Invoke festgelegt ist, beendet er die Verarbeitung der aktuellen Richtlinienbezeichnung und beginnt mit der Verarbeitung der angegebenen Richtlinienbezeichnung oder des virtuellen Servers.

So erstellen Sie eine Web App Firewall Richtlinienbezeichnung mit der Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw policylabel <labelName> http_req`
- `save ns config`

Beispiel

Im folgenden Beispiel wird eine Richtlinienbezeichnung namens policylbl1 erstellt.

```
add appfw policylabel policylbl1 http_req
save ns config
<!--NeedCopy-->
```

So binden Sie eine Richtlinie mit der Befehlszeile an eine Richtlinienbezeichnung

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `bind appfw policylabel <labelName> <policyName> <priority> [<gotoPriorityExpressi >] [-invoke (<labelType> <labelName>)]`
- `save ns config`

Beispiel

Im folgenden Beispiel wird die Richtlinien policy1 an das Richtlinienlabel policylbl1 mit der Priorität 1 gebunden.

```
bind appfw policylabel policylbl1 policy1 1
save ns config
<!--NeedCopy-->
```

So konfigurieren Sie eine Web App Firewall Richtlinienbezeichnung mit der GUI

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Richtlinienbeschriftungen**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Klicken Sie auf **Hinzufügen**, um eine neue Richtlinienbezeichnung hinzuzufügen.
   - Um eine vorhandene Richtlinienbezeichnung zu konfigurieren, wählen Sie die Richtlinienbezeichnung aus und klicken Sie auf **Öffnen**.

   Das Dialogfeld **Web App Firewall Richtlinienlabel erstellen** oder das Dialogfeld **Web App Firewall Richtlinienlabel konfigurieren** wird geöffnet. Die Dialogfelder sind nahezu identisch.
3. Wenn Sie eine neue Richtlinienbezeichnung erstellen, geben Sie im Dialogfeld Web App Firewall Richtlinienlabel erstellen einen Namen für die neue Richtlinienbezeichnung ein.

Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrich beginnen und kann aus einem bis 127 Buchstaben, Zahlen und dem Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), at (@), Gleich (=), Doppelpunkt (:) und Unterstrich (_) bestehen.

4. Wählen Sie **Richtlinie einfügen** aus, um eine neue Zeile einzufügen und eine Dropdownliste mit allen vorhandenen Web App Firewall -Richtlinien anzuzeigen.
5. Wählen Sie die Richtlinie aus, die Sie an das Policy Label binden möchten, oder wählen Sie Neue Richtlinie aus, um eine neue Richtlinie zu erstellen, und befolgen Sie die Anweisungen unter So erstellen und konfigurieren Sie eine Richtlinie über die grafische Benutzeroberfläche. Die ausgewählte oder erstellte Richtlinie wird in die Liste der global gebundenen Web App Firewall Richtlinien eingefügt.
6. Nehmen Sie zusätzliche Anpassungen vor.
   - Um die Richtlinienpriorität zu ändern, klicken Sie auf das Feld, um es zu aktivieren, und geben Sie dann eine neue Priorität ein. Sie können auch Prioritäten neu generieren wählen, um die Prioritäten gleichmäßig neu zu nummerieren.
   - Um den Richtlinienausdruck zu ändern, doppelklicken Sie auf dieses Feld, um das Dialogfeld Web App Firewall richtlinie konfigurieren zu öffnen, in dem Sie den Richtlinienausdruck bearbeiten können.
   - Zum Festlegen des Gehen-Ausdrucks doppelklicken Sie auf das Feld in der Spaltenüberschrift Gehe zu Ausdruck, um die Dropdownliste anzuzeigen, in der Sie einen Ausdruck auswählen können.
   - Um die Option Invoke festzulegen, doppelklicken Sie in der Spaltenüberschrift Invoke, um die Dropdownliste anzuzeigen, in der Sie einen Ausdruck auswählen können.
7. Wiederholen Sie die Schritte 5 bis 7, um zusätzliche Web App Firewall Richtlinien an die Richtlinienbezeichnung zu binden.
8. Klicken Sie auf **Erstellen** oder **OK**und dann auf **Schließen**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass Sie die Richtlinienbezeichnung erfolgreich erstellt oder geändert haben.

Richtlinien

October 5, 2021

Die Web App Firewall verwendet zwei Arten von Richtlinien: Firewall-Richtlinien und Überwachungsrichtlinien. Firewall-Richtlinien steuern, welcher Datenverkehr an die Web App Firewall gesendet wird. Überwachungsrichtlinien steuern den Protokollserver, an den Web App Firewall Protokolle gesendet werden.

Firewall-Richtlinien können komplex sein, da die Richtlinienregel aus mehreren Ausdrücken in der Citrix ADC Ausdruckssprache bestehen kann. Dabei handelt es sich um eine vollwertige objektorientierte Programmiersprache, die mit äußerster Präzision genau definieren kann, welche Verbindungen gefiltert werden sollen. Da Firewall-Richtlinien im Kontext der Web App Firewall funktionieren, müssen sie bestimmte Kriterien erfüllen, die mit der Funktionsweise der Web App Firewall verbunden sind und welcher Datenverkehr entsprechend gefiltert wird. Solange Sie diese Kriterien beachten, ähneln Firewallrichtlinien jedoch Richtlinien für andere Citrix ADC Funktionen. Die Anweisungen hier versuchen nicht, alle Aspekte des Schreibens von Firewall-Richtlinien abzudecken, sondern bieten nur eine Einführung in Richtlinien und decken die Kriterien ab, die für die Web App Firewall eindeutig sind.

Überwachungsrichtlinien sind einfach, da die Richtlinienregel immer ns_true lautet. Sie müssen nur den Protokollserver angeben, an den Sie Protokolle senden möchten, die Protokollierungsstufen, die Sie verwenden möchten, und einige weitere Kriterien, die detailliert erläutert werden.

Web App Firewall Richtlinien

October 5, 2021

Eine Firewall-Richtlinie ist eine Regel, die einem Profil zugeordnet ist. Die Regel ist ein Ausdruck oder eine Gruppe von Ausdrücken, die die Arten von Anforderungs-/Antwortpaaren definieren, die die Web App Firewall durch Anwenden des Profils filtern soll. Firewall-Richtlinienausdrücke werden in der Citrix ADC Ausdruckssprache geschrieben, einer objektorientierten Programmiersprache mit speziellen Funktionen zur Unterstützung bestimmter Citrix ADC-Funktionen. Das Profil ist die Gruppe von Aktionen, die die Web App Firewall zum Filtern von Anforderungen/Antwortpaaren verwenden soll, die der Regel entsprechen.

Mit Firewall-Richtlinien können Sie verschiedenen Arten von Webinhalten unterschiedliche Filterregeln zuweisen. Nicht alle Webinhalte sind gleich. Eine einfache Website, die kein komplexes Scripting verwendet und auf keine privaten Daten zugreift und verarbeitet, erfordert möglicherweise nur das Schutzniveau, das durch ein mit grundlegenden Standardeinstellungen erstelltes Profil bereitgestellt wird. Webinhalte, die JavaScript-erweiterte Webformulare enthalten oder auf eine SQL-Datenbank zugreift, erfordern wahrscheinlich einen maßgeschneiderten Schutz. Sie können ein anderes Profil erstellen, um diesen Inhalt zu filtern und eine separate Firewallrichtlinie zu erstellen, die bestimmen kann, welche Anforderungen versuchen, auf diesen Inhalt zuzugreifen. Anschließend ordnen Sie den Richtlinienausdruck einem von Ihnen erstellten Profil zu und binden die Richtlinie global, um sie in Kraft zu setzen.

Die Web App Firewall verarbeitet nur HTTP-Verbindungen und verwendet daher eine Teilmenge der allgemeinen Citrix ADC Ausdrücke. Die Informationen hier sind auf Themen und Beispiele beschränkt,

die bei der Konfiguration der Web App Firewall nützlich sein können. Im Folgenden finden Sie Links zu weiteren Informationen und Verfahren für Firewall-Richtlinien:

- Anweisungen, die erklären, wie Sie eine Richtlinie erstellen und konfigurieren, finden Sie unter Erstellen und Konfigurieren von Web App Firewall-Richtlinien.
- Eine Prozedur, die ausführlich erklärt, wie eine Richtlinienregel (Ausdruck) erstellt wird, finden Sie unter So erstellen oder konfigurieren Sie eine Web App Firewall-Regel (Ausdruck).
- Eine Prozedur, die erklärt, wie Sie das Dialogfeld Ausdruck hinzufügen zum Erstellen einer Richtlinienregel verwenden, finden Sie unter So fügen Sie eine Firewallregel (Ausdruck) mithilfe des Dialogfelds Ausdruck hinzufügen hinzu.
- Eine Prozedur, die erklärt, wie Sie die aktuellen Bindungen für eine Richtlinie anzeigen, finden Sie unter Anzeigen der Bindungen einer Firewall-Richtlinie.
- Anweisungen, die erklären, wie Sie eine Web App Firewall-Richtlinie binden, finden Sie unter Binden von Web App Firewall-Richtlinien.
- Ausführliche Informationen zur Sprache der Citrix ADC-Ausdrücke finden Sie unter Richtlinien und Ausdrücke.

> **Hinweis:**
>
> Die Web App Firewall wertet die Richtlinien basierend auf der konfigurierten Priorität und den Goto-Ausdrücken aus. Am Ende der Richtlinienbewertung wird die letzte Richtlinie verwendet, die als true ausgewertet wird, und die Sicherheitskonfiguration des entsprechenden Profils wird für die Verarbeitung der Anforderung aufgerufen.
>
> Betrachten Sie beispielsweise ein Szenario, in dem es zwei Richtlinien gibt.
>
> - Policy_1 ist eine generische Richtlinie mit Expression=ns_true und hat ein entsprechendes profile_1, das ein Basisprofil ist. Die Priorität ist auf 100 festgelegt.
> - Policy_2 ist spezifischer mit Expression=HTTP.REQ.URL.CONTAINS(“XYZ”) und hat ein entsprechendes profile_2, das ein Advance-Profil ist. Der GoTo-Ausdruck ist auf NEXT und die Priorität auf 95 gesetzt, was eine höhere Priorität im Vergleich zu Policy_1 hat.
>
> Wenn in diesem Szenario die Zielzeichenfolge XYZ in der URL der verarbeiteten Anforderung erkannt wird, wird Policy_2 Übereinstimmung ausgelöst, da sie eine höhere Priorität hat, obwohl Policy_1 auch eine Übereinstimmung ist. Gemäß der GoTo-Ausdruckskonfiguration von Policy_2 wird die Richtlinienbewertung fortgesetzt und die nächste Richtlinie Policy_1 wird ebenfalls verarbeitet. Am Ende der Richtlinienbewertung wird Policy_1 als wahr ausgewertet, und die grundlegenden Sicherheitsprüfungen, die in Profile_1 konfiguriert sind, werden aufgerufen.
>
> Wenn die Policy_2 geändert wird und der GoTo-Ausdruck von **NEXT** in **END** geändert wird, löst die verarbeitete Anforderung mit der Zielzeichenfolge “XYZ” die Policy_2-Übereinstimmung aufgrund der Prioritätsbetrachtung aus und gemäß der GoTo-Ausdruckskonfiguration endet die Richtlinienbewertung an dieser Stelle. Policy_2 wird als true ausgewertet, und die in Profile_2

> konfigurierten erweiterten Sicherheitsprüfungen werden aufgerufen.
>
> **NEXT**
> **END**
>
> Die Richtlinienbewertung wird in einem Durchgang abgeschlossen. Sobald die Richtlinienbewertung für die Anforderung abgeschlossen ist und die entsprechenden Profilaktionen aufgerufen werden, durchläuft die Anforderung keine weitere Runde der Richtlinienbewertung.

Erstellen und Konfigurieren von Web App Firewall-Richtlinien

October 5, 2021

Eine Firewall-Richtlinie besteht aus zwei Elementen: einer *Regel*und einem zugeordneten *Profil*. Die Regel wählt den HTTP-Datenverkehr aus, der den von Ihnen festgelegten Kriterien entspricht, und sendet diesen Datenverkehr zur Filterung an die Web App Firewall. Das Profil enthält die Filterkriterien, die die Web App Firewall verwendet.

Die Richtlinienregel besteht aus einem oder mehreren Ausdrücken in der Sprache für Citrix ADC Ausdrücke. Die Syntax von Citrix ADC Expressions ist eine leistungsstarke, objektorientierte Programmiersprache, mit der Sie den Datenverkehr, den Sie mit einem bestimmten Profil verarbeiten möchten, genau bestimmen können. Für Benutzer, die mit der Sprachsyntax für Citrix ADC-Ausdrücke nicht vertraut sind oder ihre Citrix ADC-Appliance über eine webbasierte Oberfläche konfigurieren möchten, bietet die GUI zwei Tools: das **Präfix-Menü** und das Dialogfeld **Ausdruck hinzufügen** . Beide helfen Ihnen beim Schreiben von Ausdrücken, die genau den Datenverkehr auswählen, den Sie verarbeiten möchten. Erfahrene Benutzer, die mit der Syntax vertraut sind, bevorzugen möglicherweise die Citrix ADC-Befehlszeile, um ihre Citrix ADC-Appliances zu konfigurieren.

> **Hinweis:**
>
> Zusätzlich zur Syntax der Standardausdrücke unterstützt das Citrix ADC-Betriebssystem aus Gründen der Abwärtskompatibilität die Syntax für klassische Ausdrücke von Citrix ADC auf Citrix ADC Classic- und NCore-Appliances und virtuellen Appliances. Klassische Ausdrücke werden auf Citrix ADC Cluster-Appliances und virtuellen Appliances nicht unterstützt. Aktuelle Citrix ADC Benutzer, die vorhandene Konfigurationen in den Citrix ADC Cluster migrieren möchten, müssen alle Richtlinien, die klassische Ausdrücke enthalten, in die Standardausdrucksyntax migrieren.

Ausführliche Informationen zu den Sprachen der Citrix ADC-Ausdrücke finden Sie unter Richtlinien und Ausdrücke.

Sie können eine Firewallrichtlinie mit der GUI oder der Citrix ADC Befehlszeile erstellen.

So erstellen und konfigurieren Sie eine Richtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw policy <name><rule> <profileName>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird eine Richtlinie mit dem Namen pl-blog mit einer Regel hinzugefügt, die den gesamten Datenverkehr zum oder vom Host blog.example.com abfängt und diese Richtlinie dem Profil pr-Blog zuordnet. Dies ist eine geeignete Richtlinie zum Schutz eines Blogs, das auf einem bestimmten Hostnamen gehostet wird.

```
1 add appfw policy pl-blog "HTTP.REQ.HOSTNAME.DOMAIN.EQ("blog.example.com
    ")" pr-blog
2 <!--NeedCopy-->
```

So erstellen und konfigurieren Sie eine Richtlinie mit der GUI

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Richtlinien**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine Firewall-Richtlinie zu erstellen, klicken Sie auf **Hinzufügen**. Die **Richtlinie "Web App Firewall erstellen** " wird angezeigt.
   - Um eine vorhandene Firewall-Richtlinie zu bearbeiten, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Bearbeiten**.

   Die **Richtlinie "Web App Firewall erstellen** " oder **"Web App Firewall konfigurieren** " wird angezeigt.
3. Wenn Sie eine Firewall-Richtlinie **erstellen, geben Sie im Dialogfeld Web App Firewall App-Firewall-Richtlinie** erstellen im Textfeld Richtlinienname einen Namen für Ihre neue Richtlinie ein.

   Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrich beginnen und kann aus einem bis 128 Buchstaben, Zahlen und dem Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), Leerzeichen (), bei (@), gleich (=), Doppelpunkt (:) und Unterstrich (_) Symbolen bestehen.

   Wenn Sie eine vorhandene Firewall-Richtlinie konfigurieren, ist dieses Feld schreibgeschützt. Sie können es nicht ändern.

4. Wählen Sie in der Dropdown-Liste Profil das Profil aus, das Sie dieser Richtlinie zuordnen möchten. Sie können ein Profil erstellen, das mit Ihrer Richtlinie verknüpft werden soll, indem Sie auf Neu klicken, und Sie können ein vorhandenes Profil ändern, indem Sie auf Ändern klicken.
5. Erstellen Sie im Textbereich Ausdruck eine Regel für Ihre Richtlinie.
    - Sie können eine Regel direkt in den Textbereich eingeben.
    - Sie können auf Präfix klicken, um den ersten Begriff für Ihre Regel auszuwählen, und den Anweisungen folgen.
    - Sie können auf Hinzufügen klicken, um das Dialogfeld Ausdruck hinzufügen zu öffnen und damit die Regel zu erstellen.
6. Klicken Sie auf **Erstellen** oder **OK**und dann auf **Schließen**.

So erstellen oder konfigurieren Sie eine Web App Firewall-Regel (Ausdruck)

Die Richtlinienregel, auch *Ausdruck*genannt, definiert den Webverkehr, den die Web App Firewall mithilfe des mit der Richtlinie verknüpften Profils filtert. Wie andere Citrix ADC-Richtlinienregeln (oder *Ausdrücke*) verwenden die Web App Firewall-Regeln die Syntax von Citrix ADC-Ausdrücken. Diese Syntax ist leistungsstark, flexibel und erweiterbar. Es ist zu komplex, um es in diesen Anweisungen vollständig zu beschreiben. Sie können das folgende Verfahren verwenden, um eine einfache Firewall-Richtlinienregel zu erstellen, oder Sie können sie als Überblick über den Richtlinienerstellungsprozess lesen.

1. Wenn Sie dies noch nicht getan haben, navigieren Sie zum entsprechenden Speicherort im **Web App Firewall-Assistenten** oder zur Citrix ADC GUI, um Ihre Richtlinienregel zu erstellen:
    - Wenn Sie eine Richtlinie im **Web App Firewall-Assistenten** konfigurieren, klicken Sie im Navigationsbereich auf **Web App Firewall**, klicken Sie dann im Detailbereich auf **Web App Firewall-Assistent**, und navigieren Sie dann zum Fenster **Regel angeben** .
    - Wenn Sie eine Richtlinie manuell konfigurieren, erweitern Sie im Navigationsbereich **Web App Firewall**, **Richtlinien**und dann **Firewall**. Klicken Sie im Detailbereich auf **Hinzufügen**, um eine Richtlinie zu erstellen. Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Öffnen**.
2. Klicken Sie auf dem Bildschirm **Regel angeben** im Dialogfeld **Web App Firewall App-Firewall-Profil erstellen** oder im Dialogfeld **Web App Firewall App-Firewall-Profil konfigurieren** auf **Präfix**, und wählen Sie dann das Präfix für Ihren Ausdruck aus der Dropdown-Liste aus. Ihre Auswahlmöglichkeiten:
    - **HTTP.** Wählen Sie ein HTTP-Protokoll aus, wenn Sie einen Aspekt der Anforderung untersuchen möchten, der sich auf das Protokoll bezieht.

- **SYS.** Wählen Sie geschützte Websites aus, wenn Sie einen Aspekt der Anfrage untersuchen möchten, der sich auf den Empfänger der Anfrage bezieht.
- **CLIENT.** Wählen Sie einen Kunden aus, der die Anfrage gesendet hat. Wählen Sie diese Option aus, wenn Sie einen Aspekt des Absenders der Anfrage untersuchen möchten.
- **-SERVER.** Wählen Sie einen Kunden aus, an den die Anfrage gesendet wurde und ob Sie einen Aspekt des Empfängers der Anfrage untersuchen möchten.

Nachdem Sie ein Präfix ausgewählt haben, zeigt die Web App Firewall ein zweiteiliges Eingabeaufforderungsfenster an, in dem oben die möglichen nächsten Optionen angezeigt werden, und eine kurze Erklärung, was die ausgewählte Auswahl unten bedeutet.

3. Wähle dein nächstes Semester.

   Wenn Sie das HTTP-Protokoll als Präfix gewählt haben, wählen Sie nur REQ, das das Request/Response-Paar angibt. (Die Web App Firewall arbeitet bei der Anfrage und Antwort als Einheit statt auf jeder separat.) Wenn Sie ein anderes Präfix gewählt haben, sind Ihre Auswahl vielfältiger. Um Hilfe zu einer bestimmten Auswahl zu erhalten, klicken Sie einmal auf diese Auswahl, um Informationen darüber im unteren Eingabeaufforderungsfenster anzuzeigen.

   Wenn Sie entschieden haben, welchen Begriff Sie möchten, doppelklicken Sie darauf, um ihn in das **Ausdrucksfenster** einzufügen.

4. Geben Sie einen Zeitraum nach dem gerade gewählten Term ein. Sie werden dann aufgefordert, Ihren nächsten Begriff zu wählen, wie im vorherigen Schritt beschrieben. Wenn für einen Begriff die Eingabe eines Wertes erforderlich ist, geben Sie den entsprechenden Wert ein. Wenn Sie beispielsweise HTTP.REQ.HEADER (“”) wählen, geben Sie den Kopfzeilennamen zwischen den Anführungszeichen ein.

5. Wählen Sie weiterhin Begriffe aus den Eingabeaufforderungen aus und geben Sie alle benötigten Werte ein, bis Ihr Ausdruck beendet ist.

   Im Folgenden finden Sie einige Beispiele für Ausdrücke für bestimmte Zwecke.

   - **Spezifischer Webhost.** So stimmen Sie den Datenverkehr von einem bestimmten Webhost ab:

     ```
     1 HTTP.REQ.HEADER(”Host”).EQ(”shopping.example.com”)
     2 <!--NeedCopy-->
     ```

     Ersetzen Sie für `shopping.example.com`den Namen des Webhosts, den Sie abgleichen möchten.

   - **Bestimmter Webordner oder -verzeichnis.** So stimmen Sie den Datenverkehr aus einem bestimmten Ordner oder Verzeichnis auf einem Webhost ab:


```
1 HTTP.REQ.URL.STARTSWITH("https//www.example.com/folder")
2 <!--NeedCopy-->
```

Ersetzen Sie für www.example.com den Namen des Webhosts. Ersetzen Sie für den Ordner den Ordner oder Pfad zu dem Inhalt, den Sie abgleichen möchten. Wenn sich Ihr Warenkorb beispielsweise in einem Ordner namens /solutions/orders befindet, ersetzen Sie diese Zeichenfolge durch Ordner.

- **Bestimmte Art von Inhalt: GIF-Bilder.** So passen Sie Bilder im GIF-Format an:

```
1 HTTP.REQ.URL.ENDSWITH(".png")
2 <!--NeedCopy-->
```

Um Bilder in anderen Formaten zu entsprechen, ersetzen Sie anstelle von .png eine andere Zeichenfolge.

- **Spezifischer Inhaltstyp: Skripts.** So passen Sie alle CGI-Skripts an, die sich im CGI-BIN-Verzeichnis befinden:

```
1 HTTP.REQ.URL.STARTSWITH("https//www.example.com/CGI-BIN")
2 <!--NeedCopy-->
```

Um alle JavaScript mit .js-Erweiterungen abzugleichen:

```
1 HTTP.REQ.URL.ENDSWITH(".js")
2 <!--NeedCopy-->
```

Weitere Informationen zum Erstellen von Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke.

> **Hinweis:**
>
> Wenn Sie die Befehlszeile zum Konfigurieren einer Richtlinie verwenden, denken Sie daran, doppelte Anführungszeichen in Citrix ADC-Ausdrücken zu umgehen. Der folgende Ausdruck ist beispielsweise korrekt, wenn er in die GUI eingegeben wird:

```
1 HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
2 <!--NeedCopy-->
```


Wenn Sie jedoch in der Befehlszeile eingegeben werden, müssen Sie stattdessen den folgenden Befehl eingeben:

```
HTTP.REQ.HEADER("Host").EQ("shopping.example.com")
<!--NeedCopy-->
```

So fügen Sie eine Firewallregel (Ausdruck) mithilfe des Dialogfelds Ausdruck hinzufügen hinzu

Das Dialogfeld **Ausdruck hinzufügen** (auch als Ausdrucksеditor bezeichnet) hilft Benutzern, die mit der Sprache der Citrix ADC-Ausdrücke nicht vertraut sind, eine Richtlinie zu erstellen, die dem Datenverkehr entspricht, den sie filtern möchten.

1. Wenn Sie dies noch nicht getan haben, navigieren Sie im **Web App Firewall-Assistenten** oder in der Citrix ADC GUI zum entsprechenden Speicherort:
   - Wenn Sie eine Richtlinie im **Web App Firewall-Assistenten** konfigurieren, klicken Sie im Navigationsbereich auf **Web App Firewall**, klicken Sie dann im Detailbereich auf **Web App Firewall-Assistent**, und navigieren Sie dann zum Fenster **Regel angeben** .
   - Wenn Sie eine Richtlinie manuell konfigurieren, erweitern Sie im Navigationsbereich **Web App Firewall**, **Richtlinien**und dann **Firewall**. Klicken Sie im Detailbereich auf **Hinzufügen**, um eine Richtlinie zu erstellen. Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Öffnen**.
2. Klicken Sie auf dem Bildschirm **Regel angeben** im Dialogfeld **Web App-Firewall-Profil erstellen** oder im Dialogfeld **Web App Firewall-Profil konfigurieren** auf **Hinzufügen**.
3. Wählen **Sie im Dialogfeld Ausdruck hinzufügen** im Bereich Ausdruck konstruieren im ersten Listenfeld eines der folgenden Präfixe aus:
   - **HTTP.** Wählen Sie das HTTP-Protokoll, wenn Sie einen Aspekt der Anforderung untersuchen möchten, der sich auf das HTTP-Protokoll bezieht. Die Standardauswahl.
   - **SYS.** Wählen Sie geschützte Websites aus, wenn Sie einen Aspekt der Anfrage untersuchen möchten, der sich auf den Empfänger der Anfrage bezieht.
   - **CLIENT.** Wählen Sie den Computer aus, der die Anfrage gesendet hat, wenn Sie einen Aspekt des Absenders der Anfrage untersuchen möchten.
   - **-SERVER.** Wählen Sie den Computer aus, an den die Anfrage gesendet wurde, und prüfen Sie einen Aspekt des Empfängers der Anfrage.
4. Wählen Sie im zweiten Listenfeld Ihren nächsten Begriff aus. Die verfügbaren Begriffe unterscheiden sich je nach Auswahl, die Sie im vorherigen Schritt getroffen haben, da das Dialogfeld die Liste automatisch so anpasst, dass sie nur die Begriffe enthält, die für den Kontext gültig sind. Wenn Sie beispielsweise im vorherigen Listenfeld HTTP ausgewählt haben, ist REQ für Anfragen die einzige Wahl. Da die Web App Firewall Anfragen und zugehörige Antworten als

eine einzige Einheit behandelt und beide filtert, müssen Sie keine spezifischen Antworten separat eingehen. Nachdem Sie Ihren zweiten Begriff gewählt haben, erscheint rechts neben dem zweiten ein drittes Listenfeld. Im Hilfefenster wird eine Beschreibung des zweiten Begriffs angezeigt, und im Fenster **Vorschauausdruck** wird Ihr Ausdruck angezeigt.

5. Wählen Sie im dritten Listenfeld den nächsten Begriff aus. Rechts erscheint ein neues Listenfeld, und das Hilfefenster ändert sich, um eine Beschreibung des neuen Begriffs anzuzeigen. Das Fenster **Vorschauausdruck** wird aktualisiert, um den Ausdruck so anzuzeigen, wie Sie ihn bis zu diesem Zeitpunkt angegeben haben.
6. Wählen Sie weiterhin Begriffe aus und wenn Sie dazu aufgefordert werden, Argumente auszufüllen, bis Ihr Ausdruck vollständig ist. Wenn Sie einen Fehler machen oder Ihren Ausdruck ändern möchten, nachdem Sie bereits einen Begriff ausgewählt haben, können Sie einfach einen anderen Begriff wählen. Der Ausdruck wird geändert, und alle Argumente oder mehr Begriffe, die Sie nach dem von Ihnen geänderten Begriff hinzugefügt haben, werden gelöscht.
7. Wenn Sie mit der Erstellung Ihres Ausdrucks fertig sind, klicken Sie auf **OK**, um das Dialogfeld **Ausdruck hinzufügen** zu schließen. Ihr Ausdruck wird in den Textbereich **Ausdruck** eingefügt.

Binden Web App Firewall Richtlinien

October 5, 2021

Nachdem Sie Ihre Web App Firewall Richtlinien konfiguriert haben, binden Sie sie an Global oder an einen Bindepunkt, um sie in Kraft zu setzen. Nach der Bindung wird jede Anforderung oder Antwort, die einer Web App Firewall Richtlinie entspricht, durch das Profil umgewandelt, das dieser Richtlinie zugeordnet ist.

Wenn Sie eine Richtlinie binden, weisen Sie ihr eine Priorität zu. Die Priorität bestimmt die Reihenfolge, in der die von Ihnen definierten Richtlinien ausgewertet werden. Sie können die Priorität auf eine beliebige positive Ganzzahl festlegen. Im Citrix ADC Betriebssystem funktionieren Richtlinienprioritäten in umgekehrter Reihenfolge - je höher die Zahl, desto niedriger die Priorität.

Da die Web App Firewall Funktion nur die erste Richtlinie implementiert, mit der eine Anforderung übereinstimmt, und keine zusätzlichen Richtlinien, die ebenfalls übereinstimmen, ist die Richtlinienpriorität wichtig, um die gewünschten Ergebnisse zu erzielen. Wenn Sie Ihrer ersten Richtlinie eine niedrige Priorität einräumen (z. B. 1000), konfigurieren Sie die Web App Firewall nur dann, wenn andere Richtlinien mit höherer Priorität nicht mit einer Anforderung übereinstimmen. Wenn Sie Ihrer ersten Richtlinie eine hohe Priorität einräumen (z. B. 1), konfigurieren Sie die Web App Firewall so, dass sie zuerst ausgeführt wird, und überspringen alle anderen Richtlinien, die möglicherweise ebenfalls übereinstimmen. Sie können sich viel Raum lassen, um andere Richtlinien in beliebiger Reihenfolge hinzuzufügen, ohne Prioritäten neu zuweisen zu müssen, indem Sie Prioritäten mit Intervallen von 50

oder 100 zwischen jeder Richtlinie festlegen, wenn Sie Ihre Richtlinien binden.

Weitere Informationen zum Binden von Richtlinien auf der Citrix ADC Appliance finden Sie unter “Richtlinien und Ausdrücke. “

So binden Sie eine Web App Firewall Richtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `bind appfw global <policyName>`
- `bind appfw profile <profile_name> -crossSiteScripting data`

Beispiel

Im folgenden Beispiel wird die Richtlinie pl-blog gebunden und die Priorität 10 zugewiesen.

```
1 bind appfw global pl-blog 10
2 save ns config
3 <!--NeedCopy-->
```

Konfigurieren von Protokollausdrücken

Die Protokollausdruck-Unterstützung für die Bindung der Web App Firewall wird hinzugefügt, um HTTP-Header-Informationen zu protokollieren, wenn eine Verletzung auftritt.

Der Protokollausdruck wird im Anwendungsprofil gebunden, und die Bindung enthält den Ausdruck, der ausgewertet und an Protokollierungsframeworks gesendet werden muss, wenn eine Verletzung auftritt.

Der Web App Firewall -Verletzungsprotokolleintrag mit HTTP-Header-Informationen wird aufgezeichnet. Sie können einen benutzerdefinierten Protokollausdruck angeben und hilft bei der Analyse und Diagnose, wenn Verletzungen für den aktuellen Fluss generiert werden (Anforderung/Antwort).

Beispielkonfiguration

```
1 bind appfw profile <profile> -logexpression <string> <expression>
2 add policy expression headers "" HEADERS(100):"+HTTP.REQ.FULL_HEADER"
3 add policy expression body_100 ""BODY:"+HTTP.REQ.BODY(100)"
4 bind appfw profile test -logExpression log_body body_100
5 bind appfw profile test -logExpression log_headers  headers
6 bind appfw profile test -logExpression ""URL:"+HTTP.REQ.URL+" IP:"+
     CLIENT.IP.SRC"
```



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

Beispielprotokolle

```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_LOGEXPRESSION|6|src=10.217.222.128 spt=26409 method=
    POST request=http://10.217.222.44/test/credit.html msg= HEADERS(100)
    :POST /test/credit.html HTTP/1.1^M User-Agent: curl/7.24.0 (amd64-
    portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3^M Host:
     10.217.222.44^M Accept: /^M Content-Length: 33^M Content-Type:
    application/x-www-form-urlencoded^M ^M  cn1=58 cn2=174 cs1=test cs2=
    PPE1 cs4=ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_LOGEXPRESSION|6|src=10.217.222.128 spt=26409 method=
    POST request=http://10.217.222.44/test/credit.html msg=BODY:ata=
    asdadasdasdasddddddddddddddd cn1=59 cn2=174 cs1=test cs2=PPE1 cs4=
    ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_LOGEXPRESSION|6|src=10.217.222.128 spt=26409 method=
    POST request=http://10.217.222.44/test/credit.html msg=URL:/test/
    credit.html IP:10.217.222.128 cn1=60 cn2=174 cs1=test cs2=PPE1 cs4=
    ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

```
Other violation logs
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_STARTURL|6|src=10.217.222.128 spt=26409 method=POST
    request=http://10.217.222.44/test/credit.html msg=Disallow Illegal
    URL. cn1=61 cn2=174 cs1=test cs2=PPE1 cs4=ALERT cs5=2017 act=not
    blocked
<!--NeedCopy-->
```



```
Dec 8 16:55:33 <local0.info> 10.87.222.145 CEF:0|Citrix|NetScaler|NS12
    .1|APPFW|APPFW_SAFECOMMERCE|6|src=10.217.222.128 spt=26409 method=
    POST request=http://10.217.222.44/test/credit.html msg=Maximum
    number of potential credit card numbers seen cn1=62 cn2=174 cs1=test
     cs2=PPE1 cs4=ALERT cs5=2017 act=not blocked
<!--NeedCopy-->
```

Hinweis:

1. Nur Auditlog-Unterstützung ist verfügbar. Unterstützung für Logstream und Sichtbarkeit in Sicherheitsinformationen würde in zukünftigen Versionen hinzugefügt werden.
2. Wenn Auditlogs generiert werden, können pro Protokollnachricht nur 1024 Byte Daten generiert werden.
3. Wenn Protokollstreaming verwendet wird, basieren die Grenzwerte auf der maximal unterstützten Größe von Protokollstream/IPFIX-Protokollgrößenbeschränkungen. Die maximale Unterstützungsgröße für Protokolldatenstrom ist größer als 1024 Bytes.

So binden Sie eine Web App Firewall Richtlinie mit der GUI

1. Führen Sie einen der folgenden Schritte aus:
   - Navigieren Sie zu **Sicherheit** > **Web App Firewall**, und klicken Sie im Detailbereich auf Web App Firewall Policy Manager.
   - Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Richtlinien** > **Firewall-Richtlinien**, und klicken Sie im Detailbereich auf **Richtlinien-Manager** .
2. Wählen Sie im Dialogfeld **Web App Firewall-Richtlinien-Manager** den Bindepunkt aus der Dropdownliste aus, an den Sie die Richtlinie binden möchten. Folgende Möglichkeiten stehen zur Auswahl:
   - **Global überschreiben.** Richtlinien, die an diesen Bindungspunkt gebunden sind, verarbeiten den gesamten Datenverkehr von allen Schnittstellen der Citrix ADC Appliance und werden vor allen anderen Richtlinien angewendet.
   - **Virtueller LB Server.** Richtlinien, die an einen virtuellen Lastausgleichsserver gebunden sind, werden nur auf Datenverkehr angewendet, der von diesem virtuellen Lastausgleichsserver verarbeitet wird, und werden vor allen globalen Standardrichtlinien angewendet. Nachdem Sie LB Virtual Server ausgewählt haben, müssen Sie auch den spezifischen virtuellen Lastausgleichsserver auswählen, an den Sie diese Richtlinie binden möchten.
   - **CS Virtual Server.** Richtlinien, die an einen virtuellen Content Switching-Server gebunden sind, werden nur auf Datenverkehr angewendet, der von diesem virtuellen Content Switching-Server verarbeitet wird, und werden vor allen globalen Standardrichtlinien angewendet. Nachdem Sie CS Virtual Server ausgewählt haben, müssen Sie auch den

spezifischen virtuellen Content Switching-Server auswählen, an den Sie diese Richtlinie binden möchten.

- **Standard Global.** Richtlinien, die an diesen Bindungspunkt gebunden sind, verarbeiten den gesamten Datenverkehr von allen Schnittstellen der Citrix ADC Appliance.
- **Richtlinienbezeichnung.** Richtlinien, die an eine Richtlinienbeschriftung gebunden sind, verarbeiten Datenverkehr, den die Richtlinienbeschriftung an sie weiterleitet. Die Richtlinienbezeichnung steuert die Reihenfolge, in der Richtlinien auf diesen Datenverkehr angewendet werden.
- **Keine.** Binden Sie die Richtlinie nicht an einen Bindepunkt.

3. Klicken Sie auf **Weiter**. Eine Liste der vorhandenen Web App Firewall Richtlinien wird angezeigt.
4. Wählen Sie die Richtlinie aus, die Sie binden möchten, indem Sie darauf klicken.
5. Nehmen Sie zusätzliche Anpassungen an der Bindung vor.
   - Um die Richtlinienpriorität zu ändern, klicken Sie auf das Feld, um es zu aktivieren, und geben Sie dann eine neue Priorität ein. Sie können auch Prioritäten neu generieren wählen, um die Prioritäten gleichmäßig neu zu nummerieren.
   - Um den Richtlinienausdruck zu ändern, doppelklicken Sie auf dieses Feld, um das Dialogfeld **Web App Firewall richtlinie konfigurieren** zu öffnen, in dem Sie den Richtlinienausdruck bearbeiten können.
   - Zum Festlegen des Gehen-Ausdrucks doppelklicken Sie auf das **Feld** in der Spaltenüberschrift Gehe zu Ausdruck, um die Dropdownliste anzuzeigen, in der Sie einen Ausdruck auswählen können.
   - Um die Option Invoke festzulegen, doppelklicken Sie in der Spaltenüberschrift Invoke, um die Dropdownliste anzuzeigen, in der Sie einen Ausdruck auswählen können.
6. Wiederholen Sie die Schritte 3 bis 6, um zusätzliche Web App Firewall Richtlinien hinzuzufügen, die Sie global binden möchten.
7. Klicken Sie auf **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich gebunden wurde.

Anzeigen von Richtlinienbindungen

October 5, 2021

Sie können schnell überprüfen, welche Bindungen für eine Firewall-Richtlinie vorhanden sind, indem Sie die Bindungen in der GUI anzeigen.

So zeigen Sie Bindungen für eine Web App Firewall Richtlinie an

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Richtlinien > Firewall-Richtlinien**

2. Wählen Sie im Detailbereich die Richtlinie aus, die Sie überprüfen möchten, und klicken Sie dann auf Bindungen anzeigen. Das Meldungsfeld Bindungsdetails für Richtlinie: Richtlinie wird mit einer Liste der Bindungen für die ausgewählte Richtlinie angezeigt.
3. Klicken Sie auf **Schließen**.

Zusätzliche Informationen zu Web App Firewall Richtlinien

October 5, 2021

Im Folgenden finden Sie zusätzliche Informationen zu bestimmten Aspekten der Web App Firewall Richtlinien, die Systemadministratoren, die die Web App Firewall verwalten, möglicherweise wissen müssen.

Korrektes, aber unerwartetes Verhalten

Die Sicherheit von Webanwendungen und moderne Websites sind komplex. In einer Reihe von Szenarien kann eine Citrix ADC Richtlinie dazu führen, dass sich die Web App Firewall in bestimmten Situationen anders verhält, als ein Benutzer, der mit Richtlinien vertraut ist, normalerweise erwarten würde. Im Folgenden finden Sie eine Reihe von Fällen, in denen die Web App Firewall in einer unerwarteten Art und Weise verhalten kann.

- **Anforderung mit einem fehlenden HTTP-Host-Header und einer absoluten URL.** Wenn ein Benutzer eine Anforderung sendet, ist die Anforderungs-URL in den meisten Fällen relativ. Das heißt, es nimmt als Ausgangspunkt die Referer-URL, die URL, in der sich der Browser des Benutzers befindet, wenn er die Anfrage sendet. Wenn eine Anfrage ohne einen Host-Header und mit einer relativen URL gesendet wird, wird die Anfrage normalerweise blockiert, da sie gegen die HTTP-Spezifikation verstößt und weil eine Anfrage, die den Host nicht angibt, unter bestimmten Umständen einen Angriff darstellen kann. Wenn eine Anforderung jedoch mit einer absoluten URL gesendet wird, selbst wenn der Host-Header fehlt, umgeht die Anforderung die Web App Firewall und wird an den Webserver weitergeleitet. Obwohl eine solche Anforderung gegen die HTTP-Spezifikation verstößt, stellt sie keine mögliche Bedrohung dar, da eine absolute URL den Host enthält.

Überwachungsrichtlinien

October 5, 2021

Überwachungsrichtlinien bestimmen die Nachrichten, die während einer Web App Firewall -Sitzung generiert und protokolliert werden. Die Meldungen werden im SYSLOG-Format am lokalen NSLOG-

Server oder an einem externen Logg-Server protokolliert. Verschiedene Arten von Nachrichten werden basierend auf der ausgewählten Protokollierungsstufe protokolliert.

Um eine Überwachungsrichtlinie zu erstellen, müssen Sie zunächst einen NSLOG-Server oder einen SYSLOG-Server erstellen. Und dann erstellen Sie die Richtlinie und geben den Protokolltyp und den Server an, an den Protokolle gesendet werden.

So erstellen Sie einen Überwachungsserver mit der Befehlszeilenschnittstelle

Sie können zwei verschiedene Arten von Auditing-Servern erstellen: einen NSLOG-Server oder einen SYSLOG-Server. Die Befehlsnamen sind unterschiedlich, aber die Parameter für die Befehle sind identisch.

Um einen Überwachungsserver zu erstellen, geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add audit syslogAction <name> <serverIP> [-serverPort <port>] -logLevel <logLevel> ... [-dateFormat (MMDDYYYY | DDMMYYYY)] [-logFacility <logFacility>] [-tcp (NONE | ALL)] [-acl (ENABLED | DISABLED)] [-timeZone (GMT_TIME | LOCAL_TIME)] [-userDefinedAuditlog (YES | NO)] [-appflowExport (ENABLED | DISABLED)]`
- `save ns config`

Beispiel

Im folgenden Beispiel wird ein Syslog-Server mit dem Namen syslog1 in IP 10.124.67.91 erstellt, wobei die Protokollfunktion für Notfälle, Kritische und Warnung auf LOCAL1 festgelegt ist und alle TCP-Verbindungen protokolliert:

```
1 add audit syslogAction syslog1 10.124.67.91 -logLevel emergency
     critical warning -logFacility
2 LOCAL1 -tcp ALL
3 save ns config
4 <!--NeedCopy-->
```

So ändern oder entfernen Sie einen Überwachungsserver mit der Befehlszeilenschnittstelle

- Um einen Überwachungsserver zu ändern, geben Sie den`<type>` Befehl set audit, den Namen des Überwachungsservers und die zu ändernden Parameter mit den neuen Werten ein.

- Um einen Überwachungsserver zu entfernen, geben Sie den<type> Befehl rm audit und den Namen des Überwachungsservers ein.

Beispiel

Im folgenden Beispiel wird der Syslog-Server mit dem Namen syslog1 so geändert, dass der Protokollebene Fehler und Warnungen hinzugefügt werden:

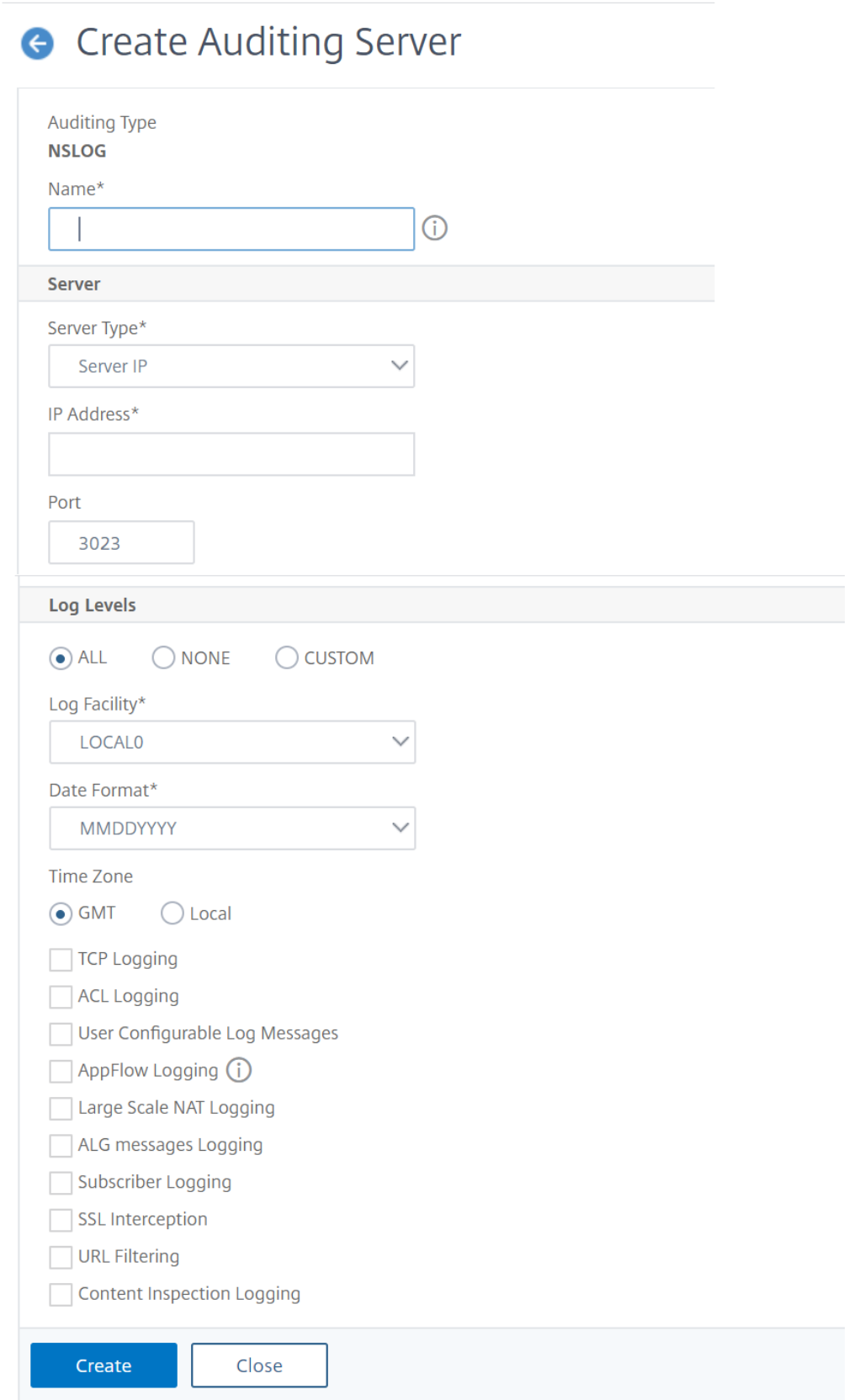
```
set audit syslogAction syslog1 10.124.67.91 -logLevel emergency
   critical warning alert error
-logFacility LOCAL1 -tcp ALL
save ns config
<!--NeedCopy-->
```

So erstellen oder konfigurieren Sie einen Überwachungsserver mit der GUI

1. Navigieren Sie zu **Sicherheit** > **Citrix Web App Firewall** > **Richtlinien** > **Überwachung** > **Nslog** .
2. Klicken Sie auf der Seite Nslog-Überwachung auf die Registerkarte **Server** .
3. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf Hinzufügen, um einen neuen Überwachungsserver **hinzuzufügen**.
   - Um einen vorhandenen Überwachungsserver zu ändern, wählen Sie den Server aus, und klicken Sie dann auf **Bearbeiten**.
4. **Legen Sie auf der Seite Überwachungsserver erstellen** die folgenden Parameter fest:
   - Name
   - Servertyp
   - IP-Adresse
   - Port
   - Protokollierungsebenen
   - Log-Einrichtung
   - Datumsformat
   - Zeitzone
   - TCP-Protokollierung
   - ACL-Protokollierung
   - Benutzerkonfigurierbare Protokollmeldungen
   - AppFlow-Protokollierung
   - NAT-Protokollierung in großem Maßstab

- Protokollierung von ALG-Meldungen
- Abonnentenprotokollierung
- SSL-Interception
- URL-Filterung
- Content-Inspection-Protokollierung

5. Klicken Sie auf **Erstellen** und **Schließen**.



So erstellen Sie eine Überwachungsrichtlinie mit der Befehlszeilenschnittstelle

Sie können eine NSLOG-Richtlinie oder eine SYSLOG-Richtlinie erstellen. Der Richtlinientyp muss mit dem Servertyp übereinstimmen. Die Befehlsnamen für die beiden Richtlinientypen sind unterschiedlich, aber die Parameter für die Befehle sind identisch.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add audit syslogPolicy <name> <-rule > <action>`
- `save ns config`

Beispiel

Im folgenden Beispiel wird eine Richtlinie namens SysLogP1 erstellt, die den Web App Firewall Datenverkehr auf einem Syslog-Server namens syslog1 protokolliert.

```
add audit syslogPolicy syslogP1 rule ”ns_true”action syslog1
save ns config
```

So konfigurieren Sie eine Überwachungsrichtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set audit syslogPolicy <name> [-rule <expression>] [-action <string>]`
- `save ns config`

Beispiel

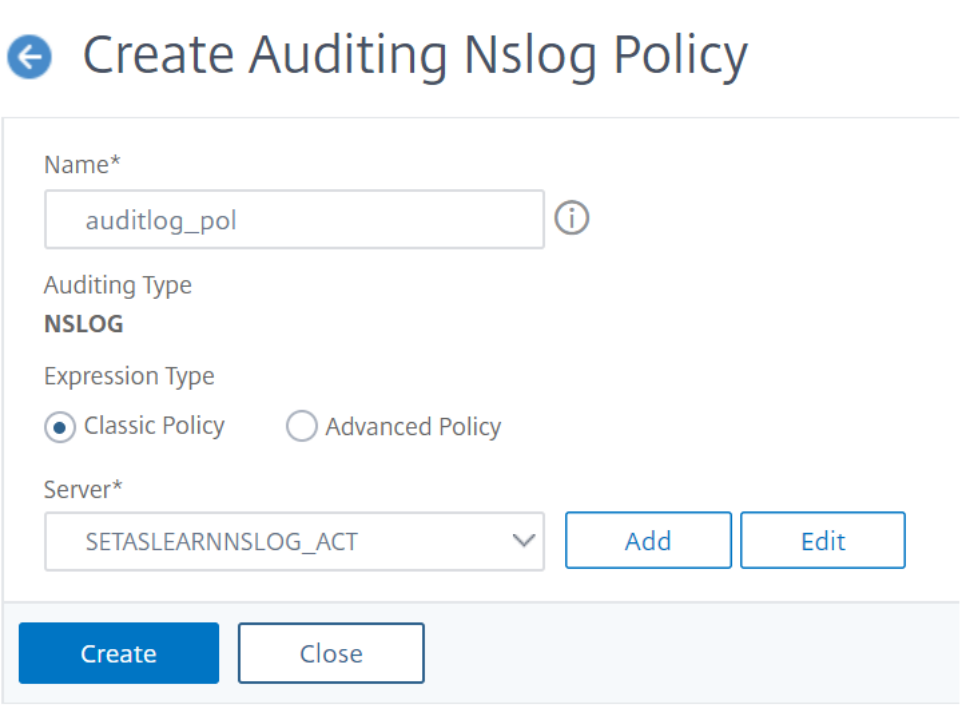
Im folgenden Beispiel wird die Richtlinie SysLogP1 so geändert, dass der Web App Firewall Datenverkehr auf einem Syslog-Server namens syslog2 protokolliert wird.

```
set audit syslogPolicy syslogP1 rule ”ns_true”action syslog2
save ns config
```

So konfigurieren Sie eine Überwachungsrichtlinie mit der GUI

1. Navigieren Sie zu **Sicherheit** > **Citrix Web App Firewall** > **Richtlinien**.
2. Klicken Sie im Detailbereich auf **Überwachungs-Nslog-Richtlinie**.
3. Klicken Sie auf der Seite Nslog-Überwachung auf **die Registerkarte Richtlinien**, und führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf Hinzufügen, um eine neue Richtlinie **hinzuzufügen**.
   - Um eine vorhandene Richtlinie zu ändern, wählen Sie die Richtlinie aus, und klicken Sie dann auf **Bearbeiten**.

4. **Legen Sie auf der Seite Überwachungs-Nslog-Richtlinie** erstellen die folgenden Parameter fest:
   - Name
   - Auditing-Typ
   - Ausdruckstyp
   - Server
5. Klicken Sie auf **Erstellen**.



Einfuhren

October 5, 2021

Mehrere Funktionen der Web App Firewall verwenden externe Dateien, die Sie bei der Konfiguration in die Web App Firewall hochladen. mit der GUI verwalten Sie diese Dateien im Bereich Importieren, der vier Registerkarten enthält, die den vier zu importierenden Dateitypen entsprechen: HTML-Fehlerobjekte, XML-Fehlerobjekte, XML-Schemas und WSDL-Dateien (Web Services Description Language). Mit der Citrix ADC Befehlszeile können Sie diese Dateitypen importieren, diese jedoch nicht exportieren.

HTML-Fehlerobjekt

Wenn die Verbindung eines Benutzers zu einer HTML- oder Web-2.0-Seite blockiert wird oder ein Benutzer nach einer nicht vorhandenen HTML- oder Web-2.0-Seite fragt, sendet die Web App Firewall eine HTML-basierte Fehlerantwort an den Browser des Benutzers. Wenn Sie konfigurieren, welche Fehlerantwort die Web App Firewall verwenden muss, haben Sie zwei Möglichkeiten:

- Sie können eine Umleitungs-URL konfigurieren, die auf jedem Webserver gehostet werden kann, auf den Benutzer auch Zugriff haben. Wenn auf Ihrem Webserver beispielsweise eine benutzerdefinierte Fehlerseite 404.html vorhanden ist, können Sie die Web App Firewall so konfigurieren, dass Benutzer zu dieser Seite umgeleitet werden, wenn eine Verbindung blockiert wird.
- Sie können ein HTML-Fehlerobjekt konfigurieren, bei dem es sich um eine HTML-basierte Webseite handelt, die auf der Web App Firewall selbst gehostet wird. Wenn Sie diese Option auswählen, müssen Sie das HTML-Fehlerobjekt in die Web App Firewall hochladen. Dies tun Sie im Bereich Importe auf der Registerkarte HTML-Fehlerobjekt.

Das Fehlerobjekt muss eine Standard-HTML-Datei sein, die keine Nicht-HTML-Syntax enthält, außer für die Anpassungsvariablen für die Web App Firewall Fehlerobjekte. Es kann keine CGI-Skripts, serveranalysierten Code oder PHP-Code enthalten. Mit den Anpassungsvariablen können Sie Informationen zur Problembehandlung in das Fehlerobjekt einbetten, das der Benutzer erhält, wenn eine Anforderung blockiert wird. Während die meisten Anfragen, dass die Web App Firewall -Blöcke illegitim sind, kann selbst eine ordnungsgemäß konfigurierte Web App Firewall gelegentlich legitime Anfragen blockieren, insbesondere wenn Sie sie zum ersten Mal bereitstellen oder nachdem Sie wichtige Änderungen an Ihren geschützten Websites vorgenommen haben. Indem Sie Informationen in die Fehlerseite einbetten, geben Sie dem Benutzer die Informationen an, die er dem technischen Support-Mitarbeiter mitteilen muss, damit etwaige Probleme behoben werden können.

Die Anpassungsvariablen der Web App Firewall auf der Fehlerseite lauten:

- $ {NS_TRANSACTION_ID}. Die Transaktions-ID, die die Web App Firewall dieser Transaktion zugewiesen hat.
- $ {NS_APPFW_SESSION_ID}. Die Sitzungs-ID der Web App Firewall.
- $ {NS_APPFW_VIOLATION_CATEGORY}. Die bestimmte Sicherheitsüberprüfung oder Regel der Web App Firewall, die verletzt wurde.
- $ {NS_APPFW_VIOLATION_LOG}. Die ausführliche Fehlermeldung im Zusammenhang mit der Verletzung.
- ${COOKIE Der Inhalt des angegebenen Cookies. Ersetzen Sie für<CookieName>den Namen des spezifischen Cookies, das Sie auf der Fehlerseite anzeigen möchten. Wenn Sie mehrere Cookies haben, deren Inhalt Sie zur Fehlerbehebung anzeigen möchten, können Sie mehrere Instanzen dieser Anpassungsvariablen verwenden, die jeweils mit dem entsprechenden Cookie-Namen

versehen sind.

Hinweis: Wenn Sie die Blockierung für die Cookie-Konsistenzprüfung aktiviert haben, werden blockierte Cookies nicht auf der Fehlerseite angezeigt, da die Web App Firewall sie blockiert.

Um diese Variablen zu verwenden, betten Sie sie in den HTML oder XML des Fehlerseitenobjekts ein, als wären sie eine gewöhnliche Textzeichenfolge. Wenn dem Benutzer das Fehlerobjekt angezeigt wird, ersetzt die Web App Firewall für jede Anpassungsvariable die Informationen, auf die sich die Variable bezieht. Eine Beispiel-HTML-Fehlerseite, die benutzerdefinierte Variablen verwendet, ist unten dargestellt.

```
<!doctype html public "-//w3c//dtd html 4.0//en"> <html> <head> <
   title>Page Not Accessible</title> </head> <body> <h1>Page Not
   Accessible</h1> <p>The page that you accessed is not available. You
    can:</p> <ul> <li>return to the <b><a href="[homePage]">home page
   </a></b>, re-establish your session, and try again, or,</li> <li>
   report this incident to the help desk via <b><a href="mailto:[
   helpDeskEmailAddress]">email</a></b> or by calling [
   helpDeskPhoneNumber].</li> </ul> <p>If you contact the help desk,
   please provide the following information:</p> <table cellpadding=8
   width=80%> <tr><th align="right" width=30%>Transaction ID:</th><td
   align="left" valign="top" width=70%>${
 NS_TRANSACTION_ID }
 </td></tr> <tr><th align="right" width=30%>Session ID:</th><td align=
    "left" valign="top" width=70%>${
 NS_APPFW_SESSION_ID }
 </td></tr> <tr><th align="right" width=30%>Violation Category:</th><
    td align="left" valign="top" width=70%>${
 NS_APPFW_VIOLATION_CATEGORY }
 </td></tr> <tr><th align="right" width=30%>Violation Log:</th><td
    align="left" valign="top" width=70%>${
 NS_APPFW_VIOLATION_LOG }
 </td></tr> <tr><th align="right" width=30%>Cookie Name:</th><td align
    ="left" valign="top" width=70%>${
 COOKIE("[cookieName]") }
 </td></tr> </table> <body> <html>
<!--NeedCopy-->
```

Um diese Fehlerseite zu verwenden, kopieren Sie sie in einen Text- oder HTML-Editor. Ersetzen Sie die entsprechenden lokalen Informationen für die folgenden Variablen, die in eckigen Klammern eingeschlossen sind, um sie von den Citrix ADC Variablen zu unterscheiden. (Lassen Sie diese unverändert.):

- `[homePage]`. Die URL für die Homepage Ihrer Website.

- [helpDeskEmailAddress]. Die E-Mail-Adresse, die Benutzer verwenden sollen, um blockierende Vorfälle zu melden.
- [helpDeskPhoneNumber]. Die Telefonnummer, die Benutzer anrufen sollen, um blockierende Vorfälle zu melden.
- [cookieName]. Der Name des Cookies, dessen Inhalt Sie auf der Fehlerseite anzeigen möchten.

XML-Fehlerobjekt

Wenn die Verbindung eines Benutzers zu einer XML-Seite blockiert wird oder ein Benutzer nach einer nicht vorhandenen XML-Anwendung fragt, sendet die Web App Firewall eine XML-basierte Fehlerantwort an den Browser des Benutzers. Sie konfigurieren die Fehlerantwort, indem Sie eine XML-basierte Fehlerseite in die Web App Firewall im Bereich Importe auf der Registerkarte XML-Fehlerobjekt hochladen. Alle XML-Fehlerantworten werden auf der Web App Firewall gehostet. Sie können keine Umleitungs-URL für XML-Anwendungen konfigurieren.

> **Hinweis**:
> Sie können dieselben Anpassungsvariablen in einem XML-Fehlerobjekt verwenden wie in einem HTML-Fehlerobjekt.

XML-Schema

Wenn die Web App Firewall eine Validierungsprüfung für die Anforderung eines Benutzers für eine XML- oder Web 2.0-Anwendung durchführt, kann sie die Anforderung anhand des XML-Schemas oder des Entwurfsdokuments (DTD) für diese Anwendung validieren und jede Anforderung ablehnen, die dem Schema oder der DTD nicht entspricht. Sowohl ein XML-Schema als auch eine DTD sind Standard-XML-Konfigurationsdateien, die die Struktur eines bestimmten XML-Dokumenttyps beschreiben.

WSDL

Wenn die Web App Firewall eine Validierungsprüfung für die Anforderung eines Benutzers für einen XML-SOAP-basierten Webdienst durchführt, kann sie die Anforderung anhand der WSDL-Datei (Web Services Type Definition) für diesen Webdienst validieren. Eine WSDL-Datei ist eine standardmäßige XML-SOAP-Konfigurationsdatei, die die Elemente eines bestimmten XML-SOAP-Webdienstes definiert.

Importieren und Exportieren von Dateien

October 5, 2021

Sie können HTML- oder XML-Fehlerobjekte, XML-Schemas, DTDs und WSDLs mit der GUI oder der Befehlszeile in die Web App Firewall importieren. Sie können diese Dateien nach dem Importieren in einem webbasierten Textbereich bearbeiten, um kleine Änderungen direkt auf dem Citrix ADC vornehmen zu müssen, anstatt sie auf Ihrem Computer vornehmen und dann erneut importieren zu müssen. Schließlich können Sie diese Dateien mit der GUI auf Ihren Computer exportieren oder diese Dateien löschen.

> **Hinweis:**
>
> Sie können eine importierte Datei nicht mit der Befehlszeile löschen oder exportieren.

So importieren Sie eine Datei mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `import appfw htmlerrorpage <src> <name>`
- `<save> ns config`

Beispiel

Im folgenden Beispiel wird ein HTML-Fehlerobjekt aus einer Datei namens error.html importiert und ihm den Namen htmlError zugewiesen.

```
1 import htmlerrorpage error.html HTMLError
2 save ns config
3 <!--NeedCopy-->
```

So importieren Sie eine Datei mit der GUI

Bevor Sie versuchen, ein XML-Schema, eine DTD- oder WSDL-Datei oder ein HTML- oder XML-Fehlerobjekt von einem Netzwerkspeicherort zu importieren, stellen Sie sicher, dass Citrix ADC eine Verbindung mit dem Internet- oder LAN-Computer herstellen kann, auf dem sich die Datei befindet. Andernfalls können Sie die Datei oder das Objekt nicht importieren.

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Importe**.
2. Navigieren Sie zu **Anwendungsfirewall** > **Importe**.
3. Wählen Sie im Bereich **Anwendungsfirewall Importe** die Registerkarte für den Dateityp aus, den Sie importieren möchten, und klicken Sie dann auf **Hinzufügen**.

   Die Registerkarten sind HTML-Fehlerseite, XML-Fehlerseite, XML-Schema oder WSDL. Der Upload-Prozess ist aus Benutzersicht auf allen vier Registerkarten identisch.

4. Füllen Sie die Dialogfelder aus.

   - **Name**— Ein Name für das importierte Objekt.
   - **Importieren von**— Wählen Sie den Speicherort der HTML-Datei, der XML-Datei, des XML-Schemas oder der WSDL, die Sie importieren möchten, in der Dropdownliste:
     - **URL:** Eine Web-URL auf einer Website, auf die die Appliance zugreifen kann.
     - **Datei:** Eine Datei auf einer lokalen oder vernetzten Festplatte oder einem anderen Speichergerät.
     - **Text:** Geben Sie den Text der benutzerdefinierten Antwort direkt in ein Textfeld in der GUI ein oder fügen Sie ihn ein.

     Das dritte Textfeld ändert sich in den entsprechenden Wert. Die drei möglichen Werte sind unten angegeben.
   - **URL**—Geben Sie die URL in das Textfeld ein.
   - **Datei**— Geben Sie den Pfad und den Dateinamen der HTML-Datei direkt ein, oder klicken Sie auf Durchsuchen, und navigieren Sie zur HTML-Datei.
   - **Text**—Das dritte Feld wird entfernt, wobei ein Leerzeichen bleibt.
5. Klicken Sie auf **Weiter**. Das Dialogfeld Dateiinhalt wird angezeigt. Wenn Sie URL oder Datei ausgewählt haben, enthält das Textfeld Dateiinhalt die von Ihnen angegebene HTML-Datei. Wenn Sie Text ausgewählt haben, ist das Textfeld Dateiinhalt leer.
6. Wenn Sie Text ausgewählt haben, geben oder kopieren Sie den HTML-HTML-Code, den Sie importieren möchten, und fügen Sie ihn ein.
7. Klicken Sie auf **Fertig**.
8. Um ein Objekt zu löschen, wählen Sie das Objekt aus, und klicken Sie dann auf **Löschen**.

So exportieren Sie eine Datei mit der GUI

Bevor Sie versuchen, ein XML-Schema, eine DTD- oder WSDL-Datei oder ein HTML- oder XML-Fehlerobjekt zu exportieren, überprüfen Sie, ob die Web App Firewall Appliance auf den Computer zugreifen kann, auf dem die Datei gespeichert werden soll. Andernfalls können Sie die Datei nicht exportieren.

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** > **Importe** .
2. Wählen Sie im Bereich **Web App Firewall Importe** die Registerkarte für den Dateityp aus, den Sie exportieren möchten.

   Der Exportvorgang ist aus Benutzersicht auf allen vier Registerkarten identisch.
3. Wählen Sie die Datei aus, die Sie exportieren möchten.

4. Erweitern Sie die Dropdownliste Aktion, und wählen Sie **Exportieren**aus.
5. Wählen Sie im Dialogfeld **Datei speichern** und klicken Sie auf **OK** .
6. Navigieren **Sie im Dialogfeld Durchsuchen** zu dem lokalen Dateisystem und dem Verzeichnis, in dem Sie die exportierte Datei speichern möchten, und klicken Sie auf **Speichern** .

So bearbeiten Sie ein HTML- oder XML-Fehlerobjekt in der GUI

Sie bearbeiten den Text von HTML- und XML-Fehlerobjekten in der GUI, ohne sie zu exportieren und dann erneut zu importieren.

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Importe**, und wählen Sie dann die Registerkarte für den Dateityp aus, den Sie ändern möchten.
2. Navigieren Sie zu **Anwendungsfirewall** > **Importiert**, und wählen Sie dann die Registerkarte für den Dateityp aus, den Sie ändern möchten.
3. Wählen Sie die Datei aus, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.

   Der Text des HTML- oder XML-Fehlerobjekts wird in einem Browser-Textbereich angezeigt. Sie können den Text mit der standardmäßigen browserbasierten Bearbeitungswerkzeuge und -methoden für Ihren Browser ändern.

   Hinweis: Im Bearbeitungsfenster können Sie kleinere Änderungen an Ihrem HTML- oder XML-Fehlerobjekt vornehmen. Um umfangreiche Änderungen vorzunehmen, können Sie das Fehlerobjekt auf Ihren lokalen Computer exportieren und Standard-HTML- oder XML-Webseitenbearbeitungstools verwenden.
4. Klicken Sie auf **OK**und dann auf **Schließen**.

Globale Konfiguration

October 5, 2021

Die globale Konfiguration der Web App Firewall wirkt sich auf alle Profile und Richtlinien aus. Die globalen Konfigurationselemente sind:

- **Motoreinstellungen.** Eine Sammlung globaler Einstellungen — Name des Sitzungscookies, Sitzungszeitüberschreitung, maximale Sitzungslebensdauer, Protokollkopfname, undefiniertes Profil, Standardprofil und Importgrößenbeschränkung —, die sich auf alle Verbindungen beziehen, die die Web App Firewall verarbeitet, anstatt auf eine bestimmte Teilmenge von Verbindungen.

- **Vertrauliche Felder.** Eine Reihe von Formularfeldern in Webformularen, die vertrauliche Informationen enthalten, die nicht in den Web App Firewall -Protokollen protokolliert werden dürfen. Formularfelder wie Kennwortfelder auf einer Anmeldeseite oder Kreditkartendaten in einem Warenkorb-Bestellformular werden normalerweise als vertrauliche Felder bezeichnet.
- **Feldtypen.** Die Liste der Webformularfeldtypen, die von der Sicherheitsprüfung Feldformate verwendet werden. Jeder dieser Feldtypen wird durch einen PCRE-konformen regulären Ausdruck definiert, der den Datentyp und die minimale/maximale Länge der Daten definiert, die in diesem Formularfeldtyp zulässig sein müssen.
- **XML-Inhaltstypen.** Die Liste der Inhaltstypen, die als XML erkannt und XML-spezifischen Sicherheitsprüfungen unterzogen wurden. Jeder dieser Inhaltstypen wird durch einen PCRE-kompatiblen regulären Ausdruck definiert, der den exakten MIME-Typ definiert, der diesem Inhalt zugewiesen ist.
- **JSON-Inhaltstypen.** Die Liste der Inhaltstypen, die als JSON erkannt und JSON-spezifischen Sicherheitsprüfungen unterzogen wurden. Jeder dieser Inhaltstypen wird durch einen PCRE-kompatiblen regulären Ausdruck definiert, der den exakten MIME-Typ definiert, der diesem Inhalt zugewiesen ist.

Engine-Einstellungen

October 5, 2021

Die Engine-Einstellungen wirken sich auf alle Anforderungen und Antworten aus, die von der Citrix Web App Firewall verarbeitet werden. Im Folgenden sind die Einstellungen:

- **Cookie-Name**— Der Name des Cookies, in dem die Citrix ADC -Sitzungs-ID gespeichert ist.
- **Sitzungszeitüberschreitung**— Der maximal zulässige inaktive Zeitraum. Wenn eine Benutzersitzung für diese Dauer keine Aktivität anzeigt, wird die Sitzung beendet und der Benutzer muss sie durch den Besuch einer bestimmten Startseite wiederherstellen.
- **Cookie post-encrypts Präfix**: Die Zeichenfolge, die dem verschlüsselten Teil aller verschlüsselten Cookies vorangeht.
- **Maximale Sitzungslebensdauer**: Die maximale Zeitdauer (in Sekunden), in der eine Sitzung live bleiben darf. Nachdem dieser Zeitraum erreicht ist, wird die Sitzung beendet und der Benutzer muss sie durch den Besuch einer bestimmten Startseite wiederherstellen. Diese Einstellung darf nicht kleiner sein als das Sitzungstimeout. Um diese Einstellung zu deaktivieren, so dass keine maximale Sitzungslebensdauer vorhanden ist, setzen Sie den Wert auf Null (0).
- **Logging Headername**— Der Name des HTTP-Headers, der die Client-IP enthält, für die Protokollierung.
- **Undefiniertes Profil**— Das Profil, das angewendet wird, wenn die entsprechende Richtlinienaktion als nicht definiert ausgewertet wird.

- **Standardprofil**— Das Profil, das auf Verbindungen angewendet wird, die nicht mit einer Richtlinie übereinstimmen.
- **Importgrößenlimit**: Die maximale Byteanzahl aller in die Appliance importierten Dateien, einschließlich Signaturen, WSDLs, Schemas, HTML- und XML-Fehlerseiten. Wenn während eines Imports die Größe des importierten Objekts bewirkt, dass die kumulative Anzahl aller importierten Dateien den konfigurierten Grenzwert überschreitet, schlägt der Importvorgang fehl. Und die Appliance zeigt die folgende Fehlermeldung an: "*FEHLER: Import fehlgeschlagen - Überschreiten der konfigurierten Gesamtgrößengrenze für die importierten Objekte*".
- **Grenzwert für Lernnachrichten**: Die maximale Anzahl von Anfragen und Antworten pro Sekunde, die die Lern-Engine verarbeiten soll. Zusätzliche Anfragen oder Antworten über dieses Limit werden nicht an die Lern-Engine gesendet.
- **Entitätsdekodierung**— Dekodieren von HTML-Entitäten bei der Ausführung von Web App Firewall Prüfungen.
- **Fehlerhafte Anforderung protokollieren**— Aktivieren Sie die Protokollierung von fehlerhaften HTTP-Anforderungen.
- **Konfigurierbarer geheimer Schlüssel**verwenden — Verwenden Sie einen konfigurierbaren geheimen Schlüssel für Web App Firewall Vorgänge. Dieser geheime Schlüssel wird zum Signieren und Verifizieren von Daten verwendet. Wenn "UseConfigurableSecretKey" eingeschaltet ist, müssen Sie den Schlüssel verwenden, der im Parameter "set ns EncryptionParams" aktiviert ist.
- **Gelernte Daten zurücksetzen**— Entfernen Sie alle gelernten Daten aus der Web App Firewall. Startet den Lernprozess neu, indem neue Daten gesammelt werden.

Zwei Einstellungen, *Gelernte Daten zurücksetzen* und *Automatische Signaturen*, sind an verschiedenen Stellen, je nachdem, ob Sie die Citrix Web App Firewall über die Befehlszeilenschnittstelle oder die Citrix ADC GUI konfigurieren. Wenn Sie die Befehlszeilenschnittstelle verwenden, konfigurieren Sie "Gelernte Daten zurücksetzen" mithilfe des Befehls "appfw learning data". Dies nimmt keine Parameter und hat keine anderen Funktionen. Sie können die automatische Aktualisierung der Signatur im Befehl set appfw settings konfigurieren. Der Parameter -SignatureAutoUpdate aktiviert oder deaktiviert die automatische Aktualisierung der Signaturen, und -signatureURL konfiguriert die URL, die die aktualisierte Signaturdatei hostet.

Wenn Sie die Citrix ADC GUI verwenden, konfigurieren Sie **Gelernte Daten zurücksetzen** unter **Sicherheit > Citrix Web App Firewall > Engine-Einstellungen**. Die Option **Gelernte Daten zurücksetzen** befindet sich am unteren Rand des Dialogfelds. Sie konfigurieren Signaturen Auto-Update für jeden Satz von Signaturen unter **Sicherheit** > **Citrix Web App Firewall** > **Signaturen**, indem Sie die Signaturdatei auswählen, mit der rechten Maustaste klicken und **Einstellungen für automatische Updates** auswählen.

Normalerweise sind die Standardwerte für die **Web App Firewall** Einstellungen korrekt. Wenn die Standardeinstellungen jedoch zu einem Konflikt mit anderen Servern führen oder eine vorzeitige Trennung Ihrer Benutzer führen, müssen Sie diese ändern.

Das Sitzungslimit der **Web App Firewall** kann mit dem folgenden Befehl konfiguriert werden:

```
> set appfw settings -sessionLimit 500000

Done

Default value:100000   Max value:500000 per PE
<!--NeedCopy-->
```

So konfigurieren Sie Engine-Einstellungen mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw settings [-sessionCookieName <name>] [-sessionTimeout <positiveInteger>] [-sessionLifetime <positiveInteger>][-clientIPLoggingHeader <headerName>] [-undefaction <profileName>] [-defaultProfile <profileName>] [-importSizeLimit <positiveInteger>] [-logMalformedReq (ON | OFF)] [-signatureAutoUpdate (ON | OFF)] [-signatureUrl <expression>] [-cookiePostEncryptPrefix <string>] [-entityDecoding (ON | OFF)] [-useConfigurableSecretKey (ON | OFF)][-learnRateLimit <positiveInteger>]`
- `save ns config`

Beispiel

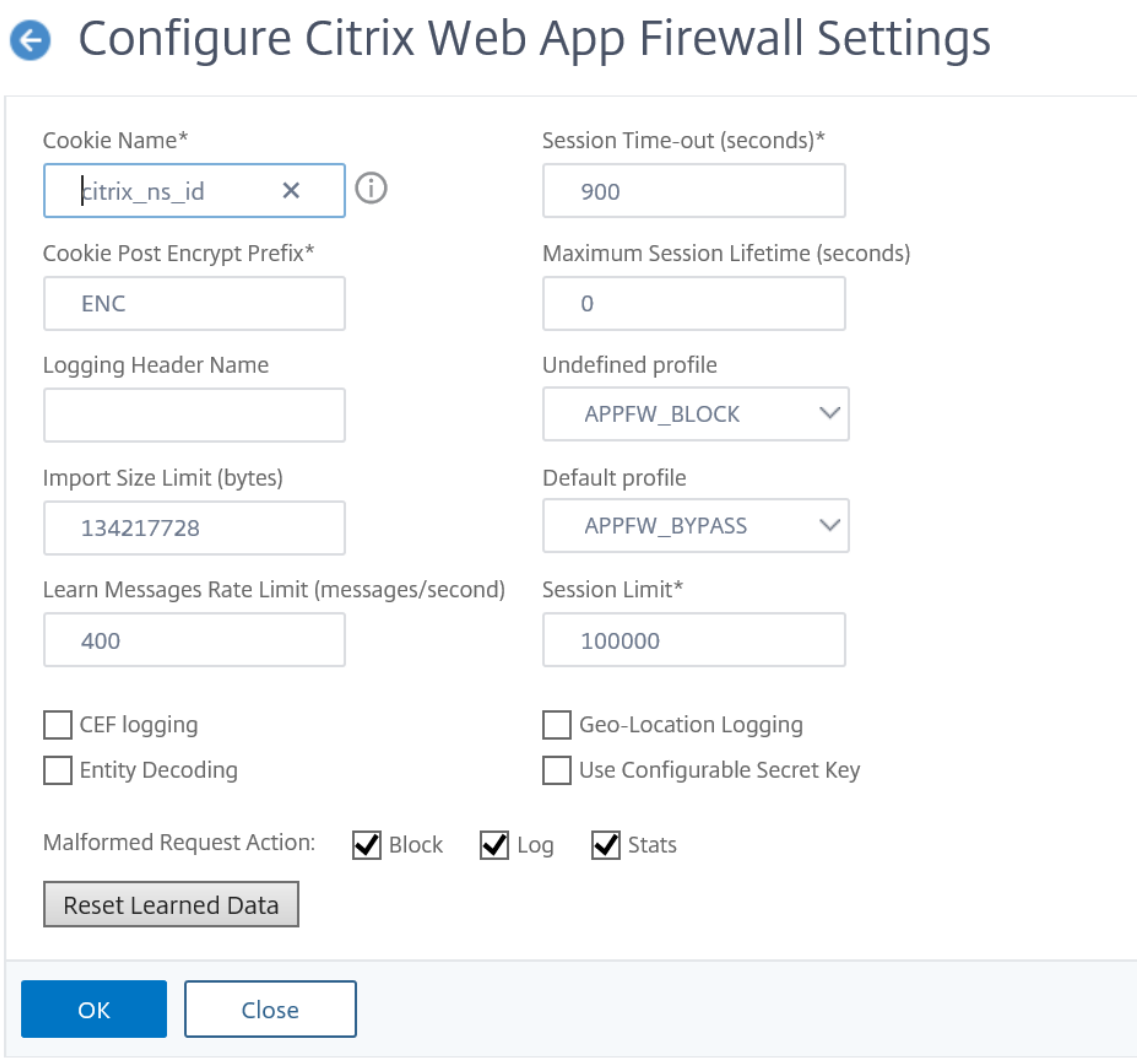
```
set appfw settings -sessionCookieName citrix-appfw-id -sessionTimeout
    3600
-sessionLifetime 14400 -clientIPLoggingHeader NS-AppFW-Client-IP -
    undefaction APPFW_RESET
-defaultProfile APPFW_RESET -importSizeLimit 4096
save ns config
<!--NeedCopy-->
```

So konfigurieren Sie Engine-Einstellungen über die Citrix ADC GUI

1. Navigieren Sie zu **Sicherheit** > **Citrix Web App Firewall**
2. Klicken Sie im Detailbereich unter **Einstellungen** auf **Engine-Einstellungen ändern**.
3. Legen Sie im Dialogfeld **Einstellungen für Web App Firewall** die folgenden Parameter fest:

- Cookie-Name
- Sitzungstimeout
- Präfix für Cookie-Post verschlüsseln
- Maximale Sitzungslebensdauer
- Protokollierungskopfname
- Nicht definiertes Profil
- Standardprofil
- Import-Größenbeschränkung
- Lerne Nachrichten Rate Limit
- Entitätsdekodierung
- Fehlformatierte Anforderung protokollieren
- Geheimer Schlüssel verwenden
- Lernen Grenzwert für Nachrichtenrate
- Signaturen automatisch aktualisieren

4. Klicken Sie auf **OK**.



Vertrauliche Felder

October 5, 2021

Sie können Webformularfelder als vertraulich festlegen, um die Informationen zu schützen, die Benutzer in sie eingeben. Normalerweise werden alle Informationen, die ein Benutzer in ein Webformular auf einem Ihrer geschützten Webserver eingibt, in den Citrix ADC Protokollen protokolliert. Die Informationen, die in ein als vertraulich eingestuft werden, werden jedoch nicht protokolliert. Diese Informationen werden nur dort gespeichert, wo die Website so konfiguriert ist, dass sie solche Daten speichert, normalerweise in einer sicheren Datenbank.

Häufige Arten von Informationen, die Sie mit einer vertraulichen Feldbezeichnung schützen möchten, sind:

- Kennwörter
- Kreditkartennummern, Validierungscodes und Ablaufdatum
- Sozialversicherungsnummern
- Steuer-ID-Nummern
- Privatadressen
- Private Telefonnummern

Neben der bewährten Praxis kann die ordnungsgemäße Verwendung vertraulicher Feldbezeichnungen für die PCI-DSS-Konformität auf E-Commerce-Servern, die HIPAA-Konformität auf Servern, die medizinische Informationen in den USA verwalten, und die Einhaltung anderer Datenschutzstandards erforderlich sein.

> **Wichtig**:
>
> In den folgenden beiden Fällen funktioniert die Bezeichnung Vertrauliches Feld nicht wie erwartet:

- Wenn ein Webformular über ein vertrauliches Feld oder eine Aktions-URL mit mehr als 256 Zeichen verfügt, wird die Feld- oder Aktions-URL in den Citrix ADC Protokollen abgeschnitten.
- Bei bestimmten SSL-Transaktionen werden die Protokolle abgeschnitten, wenn entweder das vertrauliche Feld oder die Aktions-URL länger als 127 Zeichen ist.

In jedem dieser Fälle maskiert die Web App Firewall eine fünfzehnstellige Zeichenfolge mit dem Buchstaben x anstelle der normalen 8-stelligen Zeichenfolge. Um sicherzustellen, dass vertrauliche Informationen entfernt werden, muss der Benutzer Formularfeldnamen und Aktions-URL-Ausdrücke verwenden, die mit den ersten 256 übereinstimmen, oder (in Fällen, in denen SSL verwendet wird) die ersten 127 Zeichen.

Um Ihre Web App Firewall so zu konfigurieren, dass ein Webformularfeld auf einer geschützten Website als vertraulich behandelt wird, fügen Sie dieses Feld der Liste Vertrauliche Felder hinzu. Sie können den Feldnamen als Zeichenfolge eingeben oder einen PCRE-kompatiblen regulären Ausdruck eingeben, der mindestens ein Feld angibt. Sie können die Bezeichnung vertraulicher Felder aktivieren, wenn Sie das Feld hinzufügen, oder Sie können die Bezeichnung später ändern.

So fügen Sie mit der Befehlszeilenschnittstelle ein vertrauliches Feld hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw confidField <fieldName> <url> [-isRegex ( REGEX | NOTREGEX )] [-comment "<string>"] [-state ( ENABLED | DISABLED )]`
- `save ns config`

Beispiel

Im folgenden Beispiel werden alle Webformularfelder, deren Namen mit “Password” beginnen, zur Liste vertraulicher Felder hinzugefügt.

```
1 add appfw confidField Password ”https?://www[.]example[.]com/[^<>]\*[^a
    -z]password[0-9a-z._-]\*[.](asp|cgi|htm|html|htp|js|php)” -isRegex
    REGEX -state ENABLED
2 save ns config
3 <!--NeedCopy-->
```

So ändern Sie ein vertrauliches Feld mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw confidField <fieldName> <url> [-isRegex ( REGEX | NOTREGEX ) ][-comment ”<string>”] [-state ( ENABLED | DISABLED )]`
- `save ns config`

Beispiel

Im folgenden Beispiel wird die Bezeichnung vertraulicher Felder geändert, um einen Kommentar hinzuzufügen.

```
1 set appfw confidField Password ”https?://www[.]example[.]com/[^<>]\*[^a
    -z]password[0-9a-z._-]\*[.](asp|cgi|htm|html|htp|js|php)” -comment ”
    Protect password fields.” -isRegex REGEX -state ENABLED
2 save ns config
3 <!--NeedCopy-->
```

So entfernen Sie ein vertrauliches Feld mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `rm appfw confidField <fieldName> <url>`
- `save ns config`

So konfigurieren Sie ein vertrauliches Feld mit der GUI

1. Navigieren Sie zu **Sicherheit** > **Application Firewall**.

2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Vertrauliche Felder verwalten**.
3. Führen Sie im Dialogfeld Vertrauliche Felder verwalten eine der folgenden Aktionen aus:
   - Um der Liste ein neues Formularfeld hinzuzufügen, klicken Sie auf Hinzufügen.
   - Um eine vorhandene vertrauliche Feldbezeichnung zu ändern, wählen Sie das Feld aus, und klicken Sie dann auf **Bearbeiten**.
     Das Dialogfeld **Vertrauliche Felder der Web App Firewall** wird angezeigt.

     > **Hinweis**:
     > Wenn Sie eine vorhandene vertrauliche Feldbezeichnung auswählen und dann auf **Hinzufügen**klicken, werden im Dialogfeld **Vertrauliches Formularfeld erstellen**die Informationen für dieses vertrauliche Feld angezeigt. Sie können diese Informationen ändern, um Ihr neues vertrauliches Feld zu erstellen.
4. Füllen Sie im Dialogfeld die Elemente aus. Sie sind:
   - **Aktiviert.** Aktivieren oder deaktivieren Sie diese vertrauliche Feldbezeichnung.
   - **Ist Formularfeldname ein regulärer Ausdruck Kontrollkästchen.** Aktivieren oder deaktivieren Sie diese Option, um reguläre Ausdrücke im Formularfeldnamen im PCRE-Format zu aktivieren.
   - **Feldname.** Geben Sie eine literale Zeichenfolge oder einen regulären Ausdruck im PCRE-Format ein, der entweder einen bestimmten Feldnamen darstellt oder mehrere Felder mit Namen übereinstimmt, die einem Muster folgen.
   - **Aktions-URL.** Geben Sie eine literale URL oder einen regulären Ausdruck ein, der eine oder mehrere URLs der Webseite (n) definiert, auf der sich die Webformulare befinden, die das vertrauliche Feld enthält.
   - **Kommentare.** Geben Sie einen Kommentar ein. Optional.
5. Klicken Sie auf **Erstellen** oder **OK**.
6. Um eine vertrauliche Feldbezeichnung aus der Liste vertraulicher Felder zu entfernen, wählen Sie die Liste vertraulicher Felder aus, die Sie entfernen möchten, klicken Sie dann auf Entfernen, um sie zu entfernen, und klicken Sie dann auf **OK**, um Ihre Auswahl zu bestätigen.
7. Wenn Sie mit dem Hinzufügen, Ändern und Entfernen vertraulicher Feldbezeichnungen fertig sind, klicken Sie auf **Schließen**.

Beispiele

Im Folgenden finden Sie einige reguläre Ausdrücke, die Formularfeldnamen definieren, die Sie möglicherweise nützlich finden:

- `^passwd_ (Applies confidential-field status to all field names that begin with the “passwd_” string.)`
- `^((\[0-9a-zA-Z._-]*||\\x\[0-9A-Fa-f][0-9A-Fa-f])+-)?passwd_ (Applies confidential-field status to all field names that begin with the string passwd_, or that contain the string -passwd_ after another string that`


```
might contain non-ASCII special characters.)
```

Im Folgenden finden Sie einige reguläre Ausdrücke, die bestimmte URL-Typen definieren, die Sie möglicherweise nützlich finden. Ersetzen Sie Ihre eigenen Web-Hosts und Domain (s) für diejenigen in den Beispielen.

- Wenn das Webformular auf mehreren Webseiten auf dem Webhost www.example.com erscheint, aber alle diese Webseiten den Namen logon.pl?verwenden, können Sie den folgenden regulären Ausdruck verwenden:

```
https?://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_.-]*/)*logon
   [.]pl?
<!--NeedCopy-->
```

- Wenn das Webformular auf mehreren Webseiten auf dem Webhost www.example-español.com angezeigt wird, das das Sonderzeichen n-Tilde (ñ) enthält, können Sie den folgenden regulären Ausdruck verwenden, der das Sonderzeichen n-Tilde als codierte UTF-8-String darstellt, die C3 B1, den diesem zugewiesenen Hexadezimalcode Zeichen im UTF-8 Zeichensatz:

```
https?://www[.]example-espa\xC3\xB1ol[.]com/([0-9A-Za-z][0-9A-Za-
   z_.-]\*/)\* logon[.]pl?
<!--NeedCopy-->
```

- Wenn das Webformular mit query.pl auf mehreren Webseiten auf verschiedenen Hosts innerhalb der Domäne example.com angezeigt wird, können Sie den folgenden regulären Ausdruck verwenden:

```
https?://([0-9A-Za-z][0-9A-Za-z_-.]*[.])\*example[.]com/([0-9A-Za
   -z][0-9A-Za-z_-.]\*/)*logon[.]pl?
<!--NeedCopy-->
```

- Wenn das Webformular mit query.pl auf mehreren Webseiten auf verschiedenen Hosts in verschiedenen Domänen angezeigt wird, können Sie den folgenden regulären Ausdruck verwenden:

```
https?://([0-9A-Za-z][0-9A-Za-z_-.]\*[.])\*[0-9A-Za-z][0-9A-Za-z_
   -.]+[.][a-z]{
2,6 }
/([0-9A-Za-z][0-9A-Za-z_-.]*/)*logon[.]pl?
```



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

- Wenn das Webformular auf mehreren Webseiten auf dem Webhost www.example.com erscheint, aber alle diese Webseiten den Namen logon.pl?verwenden, können Sie den folgenden regulären Ausdruck verwenden:

```
https?://www[.]example[.]com/([0-9A-Za-z][0-9A-Za-z_-.]*/)*logon
   [.]pl?
<!--NeedCopy-->
```

Feldtypen

October 5, 2021

Ein Feldtyp ist ein regulärer Ausdruck im PCRE-Format, der ein bestimmtes Datenformat und minimale/maximale Datenlängen für ein Formularfeld in einem Webformular definiert. Feldtypen werden in der Feldformat-Prüfung verwendet.

Die Web App Firewall enthält mehrere Standardfeldtypen, die sind:

- integer. Eine Zeichenfolge beliebiger Länge, die nur aus Zahlen besteht, ohne Dezimalzeichen und mit einem optionalen vorangegangenen Minuszeichen (-).
- alpha. Eine Zeichenfolge beliebiger Länge, die nur aus Buchstaben besteht.
- alphanum. Eine Zeichenfolge beliebiger Länge, bestehend aus Buchstaben und/oder Zahlen.
- nohtml. Eine Zeichenfolge beliebiger Länge, die aus Zeichen besteht, einschließlich Satzzeichen und Leerzeichen, die keine HTML-Symbole oder Abfragen enthält.
- any. Irgendwas.

> **Wichtig:**
>
> Wenn Sie den beliebigen Feldtyp als Standardfeldtyp oder einem Feld zuweisen, können aktive Skripts, SQL-Befehle und andere möglicherweise gefährliche Inhalte an Ihre geschützten Websites und Anwendungen in diesem Formularfeld gesendet werden. Sie müssen den Typ jeden Typ sparsam verwenden, wenn Sie ihn überhaupt benutzen.

Sie können auch eigene Feldtypen zur Liste Feldtypen hinzufügen. Sie können beispielsweise einen Feldtyp für eine Sozialversicherungsnummer, eine Postleitzahl oder eine Telefonnummer in Ihrem Land hinzufügen. Sie können auch einen Feldtyp für eine Kundenidentifikationsnummer oder eine Kreditkartennummer hinzufügen.

Um der Liste Feldtypen einen Feldtyp hinzuzufügen, geben Sie den Feldnamen als Literalzeichenfolge oder regulären Ausdruck im PCRE-Format ein.

So fügen Sie einen Feldtyp mit der Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw fieldType <name> <regex> <priority> [-comment "<string>"]`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Liste Feldtypen ein Feldtyp namens SSN hinzugefügt, der US-Sozialversicherungsnummern entspricht, und die Priorität auf 1 festgelegt.

```
add appfw fieldType SSN "^[1-9][0-9]{
 2,2 }
 -[0-9 }
 {
 2,2 }
 -[0-9]{
 4,4 }
 $" 1
save ns config
<!--NeedCopy-->
```

So ändern Sie einen Feldtyp mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `set appfw fieldType <name> <regex> <priority> [-comment "<string>"]`
- `save ns config`

Beispiel

Im folgenden Beispiel wird der Feldtyp so geändert, dass ein Kommentar hinzugefügt wird.

```
set appfw fieldType SSN "^[1-9][0-9]{
 2,2 }
 -[0-9 }
```



```
 {
 2,2 }
 -[0-9]{
 4,4 }
 $" 1 -comment "US Social Security Number"
save ns config
<!--NeedCopy-->
```

So entfernen Sie einen Feldtyp mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- >rm appfw fieldType <name>
- save ns config

So konfigurieren Sie einen Feldtyp mit der GUI

1. Navigieren Sie zu Sicherheit > Application Firewall.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Feldtypen verwalten**.
3. **Führen Sie im Dialogfeld Feldtypen verwalten** eine der folgenden Aktionen aus:
   - Um der Liste einen neuen Feldtyp hinzuzufügen, klicken Sie auf **Hinzufügen**.
   - Um einen vorhandenen Feldtyp zu ändern, wählen Sie den Feldtyp aus, und klicken Sie dann auf **Bearbeiten**.
     Das Dialogfeld **Feldtyp konfigurieren** wird angezeigt.

   > **Hinweis:**
   >
   > Wenn Sie eine vorhandene Feldtypbezeichnung auswählen und dann auf **Hinzufügen**klicken, werden im Dialogfeld die Informationen für diesen Feldtyp angezeigt. Sie können diese Informationen ändern, um den neuen Feldtyp zu erstellen.

4. Füllen Sie im Dialogfeld die Elemente aus. Sie sind:
   - Name
   - Regulärer Ausdruck
   - Priorität
   - Kommentar
5. Klicken Sie auf Erstellen oder OK.
6. Um einen Feldtyp aus der Liste Feldtypen zu entfernen, wählen Sie die zu entfernende Feldtypliste aus, klicken Sie dann auf **Entfernen**, um ihn zu entfernen, und klicken Sie dann auf **OK**, um Ihre Auswahl zu bestätigen.

7. Wenn Sie mit dem Hinzufügen, Ändern und Entfernen von Feldtypen fertig sind, klicken Sie auf **Schließen**.

Beispiele

Im Folgenden finden Sie einige reguläre Ausdrücke für Feldtypen, die Sie möglicherweise nützlich finden:

`^[1-9][0-9]{ 2,2 } -[0-9 } { 2,2 } -[0-9]{ 4,4 } $` US-Sozialversicherungsnummern

`^\[A-C\]\[0-9\]{ 7,7 } $` Kalifornien Führerscheinnummern

`^+[0-9]{ 1,3 } [0-9()-]{ 1,40 } $` Internationale Telefonnummern mit Ländervorwahl

`^[0-9]{ 5,5 } -[0-9]{ 4,4 } $` US-Postleitzahlennummern

`^[0-9A-Za-z][0-9A-Za-z.+_-]{ 0,25 } @([0-9A-Za-z][0-9A-Za-z_-]*[.]){ 1,4 } [A-Za-z]{ 2,6 } $` E-Mail-Adressen

XML-Inhaltstypen

October 5, 2021

Standardmäßig behandelt die Web App Firewall Dateien, die bestimmten Namenskonventionen folgen, als XML. Sie können die Web App Firewall so konfigurieren, dass Webinhalte auf zusätzliche Zeichenfolgen oder Muster untersucht werden, die darauf hindeuten, dass es sich bei diesen Dateien um XML-Dateien handelt. Dadurch kann sichergestellt werden, dass die Web App Firewall alle XML-Inhalte auf Ihrer Site erkennt, selbst wenn bestimmte XML-Inhalte nicht den normalen XML-Namenskonventionen entsprechen. Dadurch wird sichergestellt, dass XML-Inhalte XML-Sicherheitsprüfungen unterzogen werden.

Um die XML-Inhaltstypen zu konfigurieren, fügen Sie der Liste XML-Inhaltstypen die entsprechenden Muster hinzu. Sie können einen Inhaltstyp als Zeichenfolge eingeben oder einen PCRE-kompatiblen regulären Ausdruck eingeben, der eine oder mehrere Zeichenfolgen angibt. Sie können auch die vorhandenen XML-Inhaltstypen Muster ändern.

So fügen Sie mit der Befehlszeilenschnittstelle ein XML-Inhaltstypmuster hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw XMLContentType <XMLContenttypevalue> [-isRegex ( REGEX | NOTREGEX )]`
- `save ns config`

Beispiel

Im folgenden Beispiel wird das Muster hinzugefügt. */xml in die Liste XML-Inhaltstypen und bezeichnet sie als regulären Ausdruck.

```
1 add appfw XMLContentType ".*/xml" -isRegex REGEX
2 <!--NeedCopy-->
```

So entfernen Sie ein XML-Inhaltstypmuster mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `rm appfw XMLContentType <XMLContenttypevalue>`
- `save ns config`

So konfigurieren Sie die XML-Inhaltstypliste mit der GUI

1. Navigieren Sie zu **Sicherheit** > **Web App Firewall** .
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **XML-Inhaltstypen verwalten**.
3. **Führen Sie im Dialogfeld XML-Inhaltstypen verwalten** eine der folgenden Aktionen aus:
   - Um einen neuen XML-Inhaltstyp hinzuzufügen, klicken Sie auf Hinzufügen.
   - Um einen vorhandenen XML-Inhaltstyp zu ändern, wählen Sie diesen Typ aus, und klicken Sie dann auf Bearbeiten.
     Das Dialogfeld XML-Inhaltstyp der Web App Firewall konfigurieren wird angezeigt. Hinweis: Wenn Sie ein vorhandenes XML-Inhaltstypmuster auswählen und dann auf Hinzufügen klicken, werden im Dialogfeld die Informationen für dieses Muster für den XML-Inhaltstyp angezeigt. Sie können diese Informationen ändern, um Ihr neues XML-Inhaltstypmuster zu erstellen.
4. Füllen Sie im Dialogfeld die Elemente aus. Sie sind:
   - **IsRegex.** Aktivieren oder deaktivieren Sie diese Option, um reguläre Ausdrücke im Formularfeldnamen im PCRE-Format zu aktivieren.
   - **XML-Inhaltstyp** Geben Sie eine Literalzeichenfolge oder einen regulären Ausdruck im PCRE-Format ein, der dem XML-Inhaltstypmuster entspricht, das Sie hinzufügen möchten.
5. Klicken Sie auf **Erstellen**.
6. Um ein XML-Inhaltstypmuster aus der Liste zu entfernen, wählen Sie es aus, klicken Sie dann auf **Entfernen**, um es zu entfernen, und klicken Sie dann auf **OK**, um Ihre Auswahl zu bestätigen.
7. Wenn Sie mit dem Hinzufügen und Entfernen von XML-Inhaltstypmustern fertig sind, klicken Sie auf **Schließen**.

JSON-Inhaltstypen

October 5, 2021

Standardmäßig behandelt die Web App Firewall Dateien mit dem Inhaltstyp application/json als JSON-Dateien. Die Standardeinstellung ermöglicht es der Web App Firewall, JSON-Inhalte in Anfragen und Antworten zu erkennen und diesen Inhalt entsprechend zu handhaben.

Sie können die Web App Firewall so konfigurieren, dass Webinhalte auf zusätzliche Zeichenfolgen oder Muster untersucht werden, die darauf hindeuten, dass es sich bei diesen Dateien um JSON-Dateien handelt. Dadurch kann sichergestellt werden, dass die Web App Firewall alle JSON-Inhalte auf Ihrer Site erkennt, selbst wenn bestimmte JSON-Inhalte nicht den normalen JSON-Namenskonventionen entsprechen, wodurch sichergestellt wird, dass JSON-Inhalte JSON-Sicherheitsprüfungen unterzogen werden.

Um die JSON-Inhaltstypen zu konfigurieren, fügen Sie der Liste JSON-Inhaltstypen die entsprechenden Muster hinzu. Sie können einen Inhaltstyp als Zeichenfolge eingeben oder einen PCRE-kompatiblen regulären Ausdruck eingeben, der eine oder mehrere Zeichenfolgen angibt. Sie können auch die vorhandenen JSON-Inhaltstypenmuster ändern.

So fügen Sie ein JSON-Inhaltstypmuster mit der Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add appfw JSONContentType <JSONContenttypevalue> [-isRegex ( REGEX | NOTREGEX )]`
- `save ns config`

Beispiel

Im folgenden Beispiel wird das Muster hinzugefügt. */json in die Liste JSON-Inhaltstypen und bezeichnet sie als regulären Ausdruck.

```
1 add appfw JSONContentType ".*/json" -isRegex REGEX
2 <!--NeedCopy-->
```

So konfigurieren Sie die JSON-Inhaltstypliste mit der GUI

1. Navigieren Sie zu **Sicherheit** > **Application Firewall**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **JSON-Inhaltstypen verwalten**.

3. Führen Sie im Dialogfeld JSON-Inhaltstypen verwalten eine der folgenden Aktionen aus:
   - Um einen neuen JSON-Inhaltstyp hinzuzufügen, klicken Sie auf Hinzufügen.
   - Um einen vorhandenen JSON-Inhaltstyp zu ändern, wählen Sie diesen Typ aus, und klicken Sie dann auf Bearbeiten.
     Das Dialogfeld Web App Firewall JSON-Inhaltstyp konfigurieren wird angezeigt.
     Hinweis: Wenn Sie ein vorhandenes JSON-Inhaltstypmuster auswählen und dann auf Hinzufügen klicken, werden im Dialogfeld die Informationen für dieses JSON-Inhaltstypmuster angezeigt. Sie können diese Informationen ändern, um Ihr neues JSON-Inhaltstypmuster zu erstellen.
4. Füllen Sie im Dialogfeld die Elemente aus. Sie sind:
   - **IsRegex.** Aktivieren oder deaktivieren Sie diese Option, um reguläre Ausdrücke im Formularfeldnamen im PCRE-Format zu aktivieren.
   - **JSON-Inhaltstyp** Geben Sie eine Literalzeichenfolge oder einen regulären Ausdruck im PCRE-Format ein, der dem JSON-Inhaltstypmuster entspricht, das Sie hinzufügen möchten.
5. Klicken Sie auf **Erstellen** oder **OK**.
6. Um ein JSON-Inhaltstypmuster aus der Liste zu entfernen, wählen Sie es aus, klicken Sie dann auf **Entfernen**, um es zu entfernen, und klicken Sie dann auf **OK**, um Ihre Auswahl zu bestätigen.
7. Wenn Sie mit dem Hinzufügen und Entfernen von XML-Inhaltstypmustern fertig sind, klicken Sie auf **Schließen**.

Statistiken und Berichte

October 5, 2021

Die in den Protokollen und Statistiken gepflegten und in den Berichten angezeigten Informationen enthalten wichtige Hinweise zum Konfigurieren und Verwalten der Web App Firewall.

Die Statistiken der Web App Firewall

Wenn Sie die Statistikaktion für Web App Firewall-Signaturen oder Sicherheitsprüfungen aktivieren, speichert die Web App Firewall Informationen über Verbindungen, die dieser Signatur oder Sicherheitsprüfung entsprechen. Sie können die gesammelten Statistikinformationen auf der Registerkarte **Überwachung** anzeigen, indem Sie im Listenfeld “Gruppe auswählen” eine der folgenden Optionen auswählen:

- **Web App Firewall.** Eine Zusammenfassung aller Statistikinformationen, die von Ihrer Web App Firewall-Appliance für alle Profile gesammelt wurden.
- **Web App Firewall (pro Profil).** Die gleichen Informationen, aber pro Profil angezeigt und nicht zusammengefasst.

Sie können diese Informationen verwenden, um zu überwachen, wie Ihre Web App Firewall funktioniert, und um festzustellen, ob bei einer Signatur oder Sicherheitsprüfung abnormale Aktivitäten oder ungewöhnliche Treffermengen vorliegen. Wenn Sie ein solches Muster abnormaler Aktivitäten sehen, können Sie die Protokolle auf diese Signatur oder Sicherheitsprüfung überprüfen, um Korrekturmaßnahmen zu diagnostizieren und zu ergreifen.

Entspannung traf den statistischen Zähler

Basierend auf der Lockerung, die auf den verletzten Verkehr angewendet wird, können Sie auch statistische Details anzeigen, z. B. die Anzahl der Fälle eines Verstoßes auf dem Gerät, die Anzahl der zum Zeitpunkt des Verstoßes geltenden Entspannungsregeln und den zuletzt angewendeten Zeitstempel. Dadurch kann die zentralisierte Lern-Engine automatisch ungenutzte oder redundante Entspannungsbindungen löschen. Weitere Informationen finden Sie unter Thema WAF Learn Engine
.

Der statistische Zähler für die Entspannungstreffer ist nur für die folgenden Sicherheitsprüfungen verfügbar.

- Starturl
- Denyurl
- Cross-Site Scripting
- SQL Injection

So zeigen Sie Statistiken für Trefferindikatoren für Relationsregel über die Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat appfw profile p1
```

Beispiel:

```
stat appfw profile p1 -fullvalues
```

Starturl-Regel-Statistik

Regel	Hits	Bewerten	letzte Treffer-Zeit
87a4…51177	0	0	Do… 1970
5b83…dc12a	0	0	Do… 1970
12345	0	0	Do… 1970

So zeigen Sie Statistiken für Relaxationsregel an, indem Sie die GUI verwenden

Führen Sie die folgenden Schritte aus, um die Trefferzählerstatistiken der Entspannungsregel anzuzeigen

1. Navigieren Sie zu **Sicherheit > Citrix Web App Firewall > Profile**.
2. Wählen Sie im Detailbereich ein **Web App Firewall-Profil** aus und klicken Sie auf **Statistiken**.
3. Auf der Seite **Citrix Web App Firewall-Statistiken** werden die Statistikdetails angezeigt.
4. Sie können Tabellenansicht auswählen oder zur Graphischen Ansicht wechseln, um die Daten in einem tabellarischen oder grafischen Format anzuzeigen.

Die Web App Firewall-Berichte

Die Web App Firewall-Berichte enthalten Informationen über Ihre Web App Firewall-Konfiguration und zum Umgang mit dem Datenverkehr für Ihre geschützten Websites.

Der PCI-DSS-Bericht

Der Data Security Standard (DSS) der Payment Card Industry (PCI), Version 1.2, besteht aus 12 Sicherheitskriterien, die von den meisten Kreditkartenunternehmen Unternehmen verlangen, die Online-Zahlungen per Kredit- und Debitkarten akzeptieren, zu erfüllen. Diese Kriterien sollen Identitätsdiebstahl, Hacking und andere Arten von Betrug verhindern. Wenn ein Internetdienstanbieter die PCI-DSS-Kriterien nicht erfüllt, verliert dieser ISP oder Händler möglicherweise die Autorisierung, Kreditkartenzahlungen über die Website zu akzeptieren.

ISPs und Online-Händler beweisen, dass sie PCI DSS einhalten, indem sie ein Audit von einem PCI DSS Qualified Security Assessor (QSA) -Unternehmen durchführen lassen. Der PCI-DSS-Bericht soll sie sowohl vor als auch während des Audits unterstützen. Vor dem Audit wird angezeigt, welche Web App Firewall-Einstellungen für PCI DSS relevant sind, wie sie konfiguriert werden müssen und (am wichtigsten), ob Ihre aktuelle Web App Firewall-Konfiguration dem Standard entspricht. Während des Audits kann der Bericht verwendet werden, um die Einhaltung der relevanten PCI-DSS-Kriterien nachzuweisen.

Der PCI-DSS-Bericht besteht aus einer Liste der Kriterien, die für Ihre Web App Firewall-Konfiguration relevant sind. Unter jedem Kriterium listet es Ihre aktuellen Konfigurationsoptionen auf, gibt an, ob Ihre aktuelle Konfiguration dem PCI-DSS-Kriterium entspricht, und erklärt, wie Sie die Web App Firewall so konfigurieren, dass Ihre geschützten Websites das Kriterium erfüllen.

Der PCI-DSS-Bericht befindet sich unter **System > Berichte**. Um den Bericht als Adobe PDF-Datei zu generieren, klicken Sie auf PCI-DSS-Bericht erstellen. Abhängig von Ihren Browsereinstellungen wird der Bericht im Popup-Fenster angezeigt oder Sie werden aufgefordert, ihn auf Ihrer Festplatte zu speichern.

> **Hinweis:**
>
> Um diese und andere Berichte anzuzeigen, muss das Adobe Reader-Programm auf Ihrem Computer installiert sein.

Der PCI-DSS-Bericht besteht aus den folgenden Abschnitten:

- **Beschreibung.** Eine Beschreibung des PCI-DSS-Compliance-Zusammenfassungsberichts.
- **Firewall-Lizenz und Featurestatus** Zeigt an, ob die Web App Firewall auf Ihrer Citrix ADC-Appliance lizenziert und aktiviert ist.
- **Zusammenfassung der Geschäftsführung.** Eine Tabelle, die die PCI-DSS-Kriterien auflistet und Ihnen mitteilt, welche dieser Kriterien für die Web App Firewall relevant sind.
- **Detaillierte PCI-DSS-Kriterieninformationen.** Für jedes PCI-DSS-Kriterium, das für Ihre Web App Firewall-Konfiguration relevant ist, enthält der PCI-DSS-Bericht einen Abschnitt, der Informationen darüber enthält, ob Ihre Konfiguration konform ist, und wenn dies nicht der Fall ist, wie Sie sie einhalten können.
- **Konfiguration.** Daten für einzelne Profile, auf die Sie entweder zugreifen, indem Sie oben im Bericht auf Web App Firewall-Konfiguration oder direkt im Bereich Berichte klicken. Der Bericht zur Konfiguration der Web App Firewall entspricht dem PCI-DSS-Bericht, wobei die PCI-DSS-spezifische Zusammenfassung weggelassen wird.

Der Konfigurationsbericht der Web App Firewall

Der Bericht zur Konfiguration der Web App Firewall befindet sich unter **System > Berichte**. Um es anzuzeigen, klicken Sie auf **Web App Firewall-Konfigurationsbericht generieren**. Abhängig von Ihren Browsereinstellungen wird der Bericht im Popup-Fenster angezeigt oder Sie werden aufgefordert, ihn auf Ihrer Festplatte zu speichern.

Der Bericht zur Web App Firewall-Konfiguration beginnt mit einer Zusammenfassungsseite, die aus den folgenden Abschnitten besteht:

- **Web App Firewall-Richtlinien.** Eine Tabelle, in der Ihre aktuellen Web App Firewall-Richtlinien aufgeführt sind und den Richtliniennamen, den Inhalt der Richtlinie, die Aktion (oder das Profil), mit der sie verknüpft ist, und globale Bindungsinformationen anzeigen.
- **Web App Firewall App-Firewall-Profile.** Eine Tabelle, die Ihre aktuellen Web App Firewall-Profile auflistet und angibt, mit welcher Richtlinie jedes Profil verknüpft ist. Wenn ein Profil keiner Richtlinie zugeordnet ist, wird in der Tabelle an diesem Speicherort INAKTIV angezeigt.

Um alle Berichtsseiten für alle Richtlinien herunterzuladen, klicken Sie oben auf der Seite Profilübersicht auf **Alle Profile herunterladen**. Sie zeigen die Berichtsseite für jedes einzelne Profil an, indem Sie dieses Profil in der Tabelle unten auf dem Bildschirm auswählen. Die Profilseite für ein einzelnes

Profil zeigt an, ob jede Prüfaktion für jede Prüfung aktiviert oder deaktiviert ist, und die anderen Konfigurationseinstellungen für die Prüfung.

Um eine PDF-Datei mit der PCI-DSS-Berichtsseite für das aktuelle Profil **herunterzuladen, klicken Sie oben auf der Seite auf Aktuelles Profil** herunterladen. Um zur Seite Profilübersicht zurückzukehren, klicken Sie auf **Web App Firewall-Profile**. Um zur Hauptseite zurückzukehren, klicken Sie auf **Home**. Sie können den PCI-DSS-Bericht jederzeit **aktualisieren**, indem Sie in der oberen rechten Ecke des Browsers auf Aktualisieren klicken.

Web App Firewall Protokolle

June 21, 2022

Die Web App Firewall generiert Protokollmeldungen für die Nachverfolgung der Konfiguration, den Richtlinienaufruf und Details zu Verstößen gegen Sicherheitsüberprüfungen.

Wenn Sie die Protokollaktion für Sicherheitsprüfungen oder Signaturen aktivieren, enthalten die daraus resultierenden Protokollmeldungen Informationen über die Anforderungen und Antworten, die die Web App Firewall beim Schutz Ihrer Sites und Anwendungen beobachtet hat. Die wichtigsten Informationen sind die Maßnahmen, die die Web App Firewall ergriffen hat, wenn eine Signatur oder eine Verletzung der Sicherheitsüberprüfung festgestellt wurde. Für einige Sicherheitsüberprüfungen kann die Protokollnachricht nützliche Informationen liefern, z. B. den Standort des Benutzers oder ein erkanntes Muster, das eine Verletzung ausgelöst hat. Ein übermäßiger Anstieg der Anzahl von Nachrichten über Verstöße in den Protokollen kann auf einen Anstieg böswilliger Anfragen hinweisen. In der Meldung werden Sie darauf hingewiesen, dass Ihre Anwendung möglicherweise angegriffen wird, um eine bestimmte Sicherheitsanfälligkeit auszunutzen, die durch den Schutz der Web App Firewall erkannt und vereitelt wird.

> **Hinweis:**
>
> Die Citrix Web App Firewall-Protokollierung darf nur mit externen SYSLOG-Servern verwendet werden.

Citrix ADC (Native) Formatprotokolle

Die Web App Firewall verwendet standardmäßig die Citrix ADC-Formatprotokolle (auch als native Formatprotokolle bezeichnet). Diese Protokolle haben dasselbe Format wie die von anderen Citrix ADC-Funktionen generierten. Jedes Protokoll enthält die folgenden Felder:

- Zeitstempel. Datum und Uhrzeit, an dem die Verbindung hergestellt wurde.
- Schweregrad. Schweregrad des Protokolls.
- Modul. Citrix ADC-Modul, das den Protokolleintrag generiert hat.

- Event-Typ. Art des Ereignisses, wie Unterschriftenverletzung oder Verletzung der Sicherheitsüberprüfung.
- Ereignis-ID. Dem Ereignis zugewiesene ID.
- Client-IP. IP-Adresse des Benutzers, dessen Verbindung protokolliert wurde.
- Transaktions-ID. ID, die der Transaktion zugewiesen wurde, die das Protokoll verursacht hat.
- Sitzungs-ID. ID, die der Benutzersitzung zugewiesen wurde, die das Protokoll verursacht hat.
- Botschaft. Die Protokollnachricht. Enthält Informationen zur Identifizierung der Signatur oder Sicherheitsüberprüfung, die den Protokolleintrag ausgelöst hat.

Sie können nach jedem dieser Felder oder einer beliebigen Kombination von Informationen aus verschiedenen Feldern suchen. Ihre Auswahl ist nur durch die Funktionen der Tools begrenzt, die Sie zum Anzeigen der Protokolle verwenden. Sie können die Web App Firewall-Protokollmeldungen in der GUI beobachten, indem Sie auf den Citrix ADC Syslog-Viewer zugreifen, oder Sie können manuell eine Verbindung zur Citrix ADC-Appliance herstellen und über die Befehlszeilenschnittstelle auf Protokolle zugreifen, oder Sie können in die Shell wechseln und die Protokolle direkt aus `/var/log/folder` verfolgen.

Beispiel einer Protokollmeldung im nativen Format

```
1 Jun 22 19:14:37 <local0.info> 10.217.31.98 06/22/2015:19:14:37 GMT ns
     0-PPE-1 :
2 default APPFW APPFW_cross-site scripting 60 0 :  10.217.253.62 616-PPE1
      y/3upt2K8ySWWId3Kavbxyni7Rw0000
3 pr_ffc http://aaron.stratum8.net/FFC/login.php?login_name=abc&passwd=
4 12345&drinking_pref=on&text_area=%3Cscript%3E%0D%0A&loginButton=
     ClickToLogin&as_sfid=
5 AAAAAAWEXcNQLlSokNmqaYF6dvfqlChNzSMsdyO9JXOJomm2v
6 BwAMOqZIChv21EcgBc3rexIUcfm0vckKlsgoOeC_BArx1Ic4NLxxkWMtrJe4H7SOfkiv9NL7AG4juPIan

7 %3D&as_fid=feeec8758b41740eedeeb6b35b85dfd3d5def30c Cross-site script
     check failed for
8 field text_area=”Bad tag: script” <blocked>
9 <!--NeedCopy-->
```

Common Event Format (CEF) -Protokolle

Die Web App Firewall unterstützt auch CEF-Protokolle. CEF ist ein offener Protokollverwaltungsstandard, der die Interoperabilität sicherheitsrelevanter Informationen von verschiedenen Sicherheits- und Netzwerkgeräten und -anwendungen verbessert. Mit CEF können Kunden ein allgemeines Ereignisprotokollformat verwenden, sodass Daten einfach erfasst und für die Analyse durch ein Unternehmensverwaltungssystem aggregiert werden können. Die Protokollnachricht ist in ver-

schiedene Felder unterteilt, sodass Sie die Nachricht einfach analysieren und Skripte schreiben können, um wichtige Informationen zu identifizieren.

Analysieren der CEF-Protokollnachricht

Neben Datum, Zeitstempel, Client-IP, Protokollformat, Appliance, Unternehmen, Build-Version, Modul- und Sicherheitsüberprüfungsinformationen enthalten die CEF-Protokollmeldungen der Web App Firewall die folgenden Details:

- src — Quell-IP-Adresse
- spt — Quell-Portnummer
- Anfrage — URL anfragen
- act — action (zum Beispiel blockiert, transformiert)
- msg — Meldung bezüglich des beobachteten Verstoßes der Sicherheitsüberprüfung
- cn1 — Ereignis-ID
- cn2 — HTTP-Transaktion-ID
- cs1 — Profilname
- cs2 — PPE ID (zum Beispiel PPE1)
- cs3 — Sitzungs-ID
- cs4 — Schweregrad (zum Beispiel INFO, ALERT)
- cs5 — Ereignisjahr
- cs6 - Kategorie “Signatur-Verstoß”
- method — Methode (zum Beispiel GET/POST)

Betrachten Sie beispielsweise die folgende Protokollnachricht im CEF-Format, die generiert wurde, als ein Verstoß gegen die Start-URL ausgelöst wurde:

```
Jun 12 23:37:17 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11.0
|APPFW|APPFW_STARTURL|6|src=10.217.253.62 spt=47606 method=GET
request=http://aaron.stratum8.net/FFC/login.html msg=Disallow Illegal URL. cn1=1340
cn2=653 cs1=pr_ffc cs2=PPE1 cs3=EsdGd3VD0OaaURLcZnj05Y6DOmE0002 cs4=ALERT cs5=2015
act=blocked
<!--NeedCopy-->
```

Die obige Nachricht kann in verschiedene Komponenten unterteilt werden. Weitere Informationen finden Sie in der Tabelle mit den CEP-Protokollkomponenten .

Beispiel für eine Anforderungsprüfung Verletzung im CEF-Protokollformat: Anforderung ist nicht blockiert


```
Jun 13 00:21:28 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|
APPFW_FIELDCONSISTENCY|6|src=10.217.253.62 spt=761 method=GET request=
http://aaron.stratum8.net/FFC/login.php?login_name=abc&passwd=
123456789234&drinking_pref=on&text_area=&loginButton=ClickToLogin&
    as_sfid
=
    AAAAAAWIahZuYoIFbjBhYMP05mJLTwEfIY0a7AKGMg3jIBaKmwtK4t7M7lNxOgj7Gmd3SZc8KUj6CP

7W5kIWDRHN8PtK1Zc-txHkHNx1WknuG9DzTuM7t1THhluevXu9I4kp8%3D&as_fid=
    feeec8758b4174
0eedeeb6b35b85dfd3d5def30c msg=Field consistency check failed for field
     passwd cn1=1401
cn2=707 cs1=pr_ffc cs2=PPE1 cs3=Ycby5IvjL6FoVa6Ah94QFTIUpC80001 cs4=
    ALERT cs5=2015 act=
not blocked
<!--NeedCopy-->
```

Beispiel für eine Verletzung der Antwortprüfung im CEF-Format: Antwort wird transformiert

```
Jun 13 00:25:31 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|
APPFW_SAFECOMMERCE|6|src=10.217.253.62 spt=34041 method=GET request=
http://aaron.stratum8.net/FFC/CreditCardMind.html msg=Maximum number of
     potential credit
card numbers seen cn1=1470 cn2=708 cs1=pr_ffc cs2=PPE1
cs3=Ycby5IvjL6FoVa6Ah94QFTIUpC80001 cs4=ALERT cs5=2015 act=transformed
<!--NeedCopy-->
```

Beispiel für eine Verletzung der anforderungsseitigen Signatur im CEF-Format: Anfrage ist blockiert

```
Jun 13 01:11:09 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|APPFW|
APPFW_SIGNATURE_MATCH|6|src=10.217.253.62 spt=61141 method=GET request=
http://aaron.stratum8.net/FFC/wwwboard/passwd.txt msg=Signature
    violation rule ID 807:
web-cgi /wwwboard/passwd.txt access  cn1=140 cn2=841 cs1=pr_ffc cs2=
    PPE0
cs3=OyTgjbXBqcpBFeENKDlde3OkMQ00001 cs4=ALERT cs5=2015 cs6=web-cgi act=
    blocked
<!--NeedCopy-->
```


Protokollieren der Geolocation in den Verstoßmeldungen der Web App Firewall

Die Protokolldetails identifizieren den Ort, von dem Anforderungen stammen, und helfen Ihnen, die Web App Firewall für die optimale Sicherheitsstufe zu konfigurieren. Um Sicherheitsimplementierungen wie Ratenbegrenzungen zu Bypass, die auf den IP-Adressen der Clients beruhen, können Malware oder nicht autorisierte Computer die Quell-IP-Adresse in Anfragen ständig ändern. Durch die Identifizierung der spezifischen Region, aus der Anfragen kommen, kann festgestellt werden, ob die Anfragen von einem gültigen Benutzer oder einem Gerät stammen, das versucht, Cyberangriffe zu starten. Wenn beispielsweise eine übermäßig große Anzahl von Anfragen aus einem bestimmten Bereich eingeht, kann leicht festgestellt werden, ob sie von Benutzern oder einem Schurkencomputer gesendet werden. Die Geolokalisierungsanalyse des empfangenen Datenverkehrs kann nützlich sein, um Angriffe wie Denial-of-Service-Angriffe (DoS) abzuwehren.

Die Web App Firewall bietet Ihnen die Möglichkeit, die integrierte Citrix ADC-Datenbank zu verwenden, um die Speicherorte zu identifizieren, die den IP-Adressen entsprechen, von denen böswillige Anfragen stammen. Sie können dann ein höheres Sicherheitsniveau für Anfragen von diesen Sites erzwingen. Citrix Standardsyntax (PI) -Ausdrücke bieten Ihnen die Flexibilität, standortbasierte Richtlinien zu konfigurieren, die mit der integrierten Standortdatenbank verwendet werden können, um den Firewall-Schutz anzupassen und so Ihren Schutz vor koordinierten Angriffen zu stärken, die von Rogue-Clients in einer bestimmten Region gestartet werden.

Sie können die integrierte Citrix ADC-Datenbank oder eine andere Datenbank verwenden. Wenn die Datenbank keine Standortinformationen für die bestimmte Client-IP-Adresse enthält, zeigt das CEF-Protokoll die Geolocation als unbekannte Geolocation an.

> **Hinweis:**
>
> Die Geolocation-Protokollierung verwendet das Common Event Format (CEF). Standardmäßig sind `CEF logging` und `GeoLocationLogging` AUS. Sie müssen beide Parameter explizit aktivieren.

Beispiel für eine CEF-Protokollnachricht mit Geolokationsinformationen

```
June 8 00:21:09 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
   .0|APPFW|
APPFW_STARTURL|6|src=10.217.253.62 geolocation=NorthAmerica.US.Arizona.
   Tucson.\*.\*
spt=18655 method=GET request=http://aaron.stratum8.net/FFC/login.html
msg=Disallow Illegal URL. cn1=77 cn2=1547 cs1=test_pr_adv cs2=PPE1
cs3=KDynjg1pbFtfhC/nt0rBU1o/Tyg0001 cs4=ALERT cs5=2015 act=not blocked
<!--NeedCopy-->
```

Beispiel einer Protokollnachricht mit Geolocation= Unknown


```
June 9 23:50:53 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11
    .0|
APPFW|APPFW_STARTURL|6|src=10.217.30.251 geolocation=Unknown spt=5086
method=GET request=http://aaron.stratum8.net/FFC/login.html msg=
    Disallow Illegal URL.
cn1=74 cn2=1576 cs1=test_pr_adv cs2=PPE2 cs3=
    PyR0eOEM4gf6GJiTyauiHByL88E0002
cs4=ALERT cs5=2015 act=not blocked
<!--NeedCopy-->
```

Konfigurieren der Protokollaktion und anderer Protokollparameter mithilfe der Befehlsschnittstelle

So konfigurieren Sie die Protokollaktion für eine Sicherheitsüberprüfung eines Profils mithilfe der Befehlszeile

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- `set appfw profile <name> SecurityCheckAction ([log] | [none])`
- `unset appfw profile <name> SecurityCheckAction`

Beispiele

```
set appfw profile pr_ffc StartURLAction log
```

```
unset appfw profile pr_ffc StartURLAction
```

So konfigurieren Sie die CEF-Protokollierung mithilfe der Befehlszeile

Die CEF-Protokollierung ist standardmäßig deaktiviert. Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um die aktuelle Einstellung zu ändern oder anzuzeigen:

- `set appfw settings CEFLogging on`
- `unset appfw settings CEFLogging`
- `sh appfw settings | grep CEFLogging`

So konfigurieren Sie die Protokollierung der Kreditkartennummern mithilfe der Befehlszeile

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- `set appfw profile <name> -doSecureCreditCardLogging ([ON] | [OFF])`
- `unset appfw profile <name> -doSecureCreditCardLogging`

So konfigurieren Sie die Geolocation-Protokollierung mithilfe der Befehlszeile

1. Verwenden Sie den Befehl set, um GeolocationLogging zu aktivieren. Sie können die CEF-Protokollierung gleichzeitig aktivieren. Verwenden Sie den Befehl unset, um die Geolocation-Protokollierung zu deaktivieren. Der Befehl show zeigt die aktuellen Einstellungen aller Web

App Firewall-Parameter an, es sei denn, Sie schließen den Befehl grep ein, um die Einstellung für einen bestimmten Parameter anzuzeigen.

- `set appfw settings GeoLocationLogging ON [CEFLogging ON]`
- `unset appfw settings GeoLocationLogging`
- `sh appfw settings | grep GeoLocationLogging`

2. Geben Sie die Datenbank an

   ```
   add locationfile /var/netscaler/inbuilt_db/Citrix_netscaler_InBuilt_GeoIP_DB
   .csv
   ```

   oder

   ```
   add locationfile <path to database file>
   ```

Anpassen der Web App Firewall-Protokolle

Standardformat-Ausdrücke (PI) geben Ihnen die Flexibilität, die in den Protokollen enthaltenen Informationen anzupassen. Sie haben die Möglichkeit, die spezifischen Daten, die Sie erfassen möchten, in die von der Web App Firewall generierten Protokollmeldungen aufzunehmen. Wenn Sie beispielsweise die AAA-TM-Authentifizierung zusammen mit den Sicherheitsüberprüfungen der Web App Firewall verwenden und die URL, auf die zugegriffen wird, die den Verstoß gegen die Sicherheitsüberprüfung ausgelöst hat, den Namen des Benutzers, der die URL angefordert hat, die Quell-IP-Adresse und den Quellport, von dem aus der Benutzer die Anfrage gesendet hat, wissen möchten, können Sie kann die folgenden Befehle verwenden, um benutzerdefinierte Protokollmeldungen anzugeben, die alle Daten enthalten:

```
1 > sh version
2 NetScaler NS12.1: Build 50.0013.nc, Date: Aug 28 2018, 10:51:08   (64-
     bit)
3  Done
4 <!--NeedCopy-->
```

```
1 > add audit messageaction custom1 ALERT 'HTTP.REQ.URL + " " + HTTP.REQ.
     USER.NAME + " " + CLIENT.IP.SRC + ":" + CLIENT.TCP.SRCPORT'
2 Warning: HTTP.REQ.USER has been deprecated. Use AAA.USER instead.
3  Done
4 <!--NeedCopy-->
```



```
> add appfw profile test_profile
 Done
<!--NeedCopy-->
```

```
> add appfw policy appfw_pol true test_profile -logAction custom1
 Done
<!--NeedCopy-->
```

Konfigurieren der Syslog-Richtlinie, um Web App Firewall-Protokolle zu trennen

Die Web App Firewall bietet Ihnen die Möglichkeit, die Sicherheitsprotokollmeldungen der Web App Firewall zu isolieren und in eine andere Protokolldatei umzuleiten. Dies kann wünschenswert sein, wenn die Web App Firewall viele Protokolle generiert, wodurch es schwierig wird, andere Citrix ADC-Protokollmeldungen anzuzeigen. Sie können diese Option auch verwenden, wenn Sie nur die Web App Firewall-Protokollmeldungen anzeigen möchten und die anderen Protokollmeldungen nicht sehen möchten.

Um die Web App Firewall-Protokolle in eine andere Protokolldatei umzuleiten, konfigurieren Sie eine Syslog-Aktion, um die Web App Firewall-Protokolle an eine andere Protokolleinrichtung zu senden. Sie können diese Aktion verwenden, wenn Sie die Syslog-Richtlinie konfigurieren und global für die Verwendung durch Web App Firewall binden.

Beispiel:

1. Wechseln Sie zur Shell und bearbeiten Sie mit einem Editor wie vi die Datei /etc/syslog.conf. Fügen Sie einen neuen Eintrag hinzu, um local2.* zu verwenden, um Protokolle an eine separate Datei zu senden, wie im folgenden Beispiel gezeigt:

   ```
   local2.\* /var/log/ns.log.appfw
   ```

2. Starten Sie den Syslog-Prozess neu. Sie können den Befehl grep verwenden, um die Syslog-Prozess-ID (PID) zu identifizieren, wie im folgenden Beispiel gezeigt:

   ```
   root@ns\## **ps -A | grep syslog**

   1063 ?? Ss 0:03.00 /usr/sbin/syslogd -b 127.0.0.1 -n -v -v -8 -C

   root@ns## **kill -HUP** 1063
   ```

3. Konfigurieren Sie über die Befehlszeilenschnittstelle entweder erweiterte oder klassische SYSLOG-Richtlinien mit Aktion und binden Sie sie als globale Web App Firewall-Richtlinie. Citrix empfiehlt Ihnen, die erweiterte SYSLOG-Richtlinie zu konfigurieren.

   Erweiterte SYSLOG-Richtlinienkonfiguration


```
add audit syslogAction sysact1 1.1.1.1 -logLevel ALL -logFacility
LOCAL2

add audit syslogPolicy syspol1 true sysact1

bind audit syslogGlobal -policyName syspol1 -priority 100 -globalBindType
 APPFW_GLOBAL
```

Klassische SYSLOG-Richtlinienkonfiguration

```
add audit syslogAction sysact1 1.1.1.1 -logLevel ALL -logFacility
LOCAL2

add audit syslogPolicy syspol1 true sysact1

bind audit syslogGlobal -policyName syspol1 -priority 100 -globalBindType
 APPFW_GLOBAL
```

4. Alle Verstöße gegen die Sicherheitsüberprüfung der Web App Firewall werden jetzt in die Datei `/var/log/ns.log.appfw` umgeleitet. Sie können diese Datei verkürzen, um die Verstöße gegen die Web App Firewall anzuzeigen, die während der Verarbeitung des laufenden Datenverkehrs ausgelöst werden.

   ```
   root@ns## tail -f ns.log.appfw
   ```

Warnung: Wenn Sie die Syslog-Richtlinie so konfiguriert haben, dass die Protokolle an eine andere Protokollfunktion umgeleitet werden, werden die Web App Firewall-Protokollmeldungen nicht mehr in der Datei `/var/log/ns.log` angezeigt.

> **Hinweis:**
>
> Wenn Sie Protokolle an eine andere Protokolldatei auf der lokalen Citrix ADC-Appliance senden möchten, können Sie einen Syslog-Server auf dieser lokalen Citrix ADC-Appliance erstellen. Fügen Sie `syslogaction` zu der eigenen IP hinzu und konfigurieren Sie den ADC so, als würden Sie einen externen Server konfigurieren. Der ADC fungiert als Server zum Speichern Ihrer Logs. Zwei Aktionen können nicht mit derselben IP und demselben Port hinzugefügt werden. In `syslogaction` ist der Wert von IP standardmäßig auf `127.0.0.1` und der Wert von Port auf `514` festgelegt.

Web App Firewall-Protokolle anzeigen

Sie können die Protokolle anzeigen, indem Sie den Syslog-Viewer verwenden oder sich bei der Citrix ADC-Appliance anmelden, eine UNIX-Shell öffnen und den UNIX-Texteditor Ihrer Wahl verwenden.

So greifen Sie mit der Befehlszeile auf die Protokollmeldungen zu

Wechseln Sie zur Shell und schließen Sie die ns.logs im Ordner **/var/log/** an, um auf die Protokollmeldungen zuzugreifen, die sich auf Verstöße gegen die **Sicherheitsüberprüfung der Web App Firewall**

beziehen:

- `Shell`
- `tail -f /var/log/ns.log`

Sie können den vi-Editor oder einen beliebigen Unix-Texteditor oder ein Textsuchwerkzeug verwenden, um die Protokolle nach bestimmten Einträgen anzuzeigen und zu filtern. Sie können den Befehl `grep` beispielsweise verwenden, um auf die Protokollmeldungen zuzugreifen, die sich auf die Kreditkartenverletzungen beziehen:

- `tail -f /var/log/ns.log | grep SAFECOMMERCE`

So greifen Sie mit der GUI auf die Protokollmeldungen zu

Die Citrix GUI enthält ein nützliches Tool (Syslog Viewer) zum Analysieren der Protokollmeldungen. Sie haben mehrere Optionen für den Zugriff auf den Syslog Viewer:

- Um Protokollmeldungen für eine bestimmte Sicherheitsüberprüfung eines Profils anzuzeigen, navigieren Sie zu **Web App Firewall** > **Profile**, wählen Sie das Zielprofil aus und klicken Sie auf Sicherheitsprüfungen. Markieren Sie die Zeile für die Zielsicherheitsprüfung und klicken Sie auf Protokolle. Wenn Sie direkt von der ausgewählten Sicherheitsüberprüfung des Profils auf die Protokolle zugreifen, filtert es die Protokollmeldungen heraus und zeigt nur die Protokolle an, die sich auf die Verletzungen für die ausgewählte Sicherheitsüberprüfung beziehen. Der Syslog-Viewer kann Web App Firewall-Protokolle im nativen Format und im CEF-Format anzeigen. Damit der Syslog-Viewer jedoch die zielprofilspezifischen Protokollmeldungen herausfiltern kann, müssen die Protokolle beim Zugriff über das Profil im CEF-Protokollformat vorliegen.
- Sie können auch auf den Syslog Viewer zugreifen, indem Sie zu **Citrix ADC** > **System** > **Auditing** navigieren. Klicken Sie im Abschnitt Überwachungsmeldungen auf den Link Syslog-Meldungen, um den Syslog-Viewer anzuzeigen, in dem alle Protokollmeldungen angezeigt werden, einschließlich aller Protokolle von Verstößen gegen die Sicherheitsüberprüfung der Web App Firewall für alle Profile. Die Protokollmeldungen sind nützlich für das Debuggen, wenn während der Anforderungsverarbeitung mehrere Verstöße gegen die Sicherheitsüberprüfung ausgelöst werden können.
- Navigieren Sie zu **Web App Firewall** > **Richtlinien** > **Auditing**. Klicken Sie im Abschnitt Überwachungsmeldungen auf den Link Syslog-Meldungen, um den Syslog-Viewer anzuzeigen, in dem alle Protokollmeldungen einschließlich aller Protokolle von Sicherheitsüberprüfungen für alle Profile angezeigt werden.

Der HTML-basierte Syslog Viewer bietet die folgenden Filteroptionen, um nur die Protokollmeldungen auszuwählen, die für Sie von Interesse sind:

- **Datei**— Die aktuelle Datei `/var/log/ns.log` ist standardmäßig ausgewählt, und die entsprechenden Meldungen werden im Syslog Viewer angezeigt. Eine Liste anderer Protokolldateien im /var/log-Verzeichnis ist in einem komprimierten.gz-Format verfügbar. Um eine

archivierte Protokolldatei herunterzuladen und zu dekomprimieren, wählen Sie die Protokolldatei aus der Dropdown-Liste aus. Die Protokollmeldungen, die sich auf die ausgewählte Datei beziehen, werden dann im Syslog-Viewer angezeigt. Um die Anzeige zu aktualisieren, klicken Sie auf das Aktualisierungssymbol (ein Kreis aus zwei Pfeilen).

- **Modullistenfeld**—Sie können das Citrix ADC-Modul auswählen, dessen Protokolle Sie anzeigen möchten. Sie können es auf APPFW für Web App Firewall-Protokolle setzen.
- **Listenfeld Ereignisart**—Dieses Feld enthält eine Reihe von Kontrollkästchen zur Auswahl des Ereignistyps, an dem Sie interessiert sind. Um beispielsweise die Protokollmeldungen zu den Signaturverletzungen anzuzeigen, können Sie das Kontrollkästchen **APPFW_SIGNATURE_MATCH** aktivieren. In ähnlicher Weise können Sie ein Kontrollkästchen aktivieren, um die für Sie interessante Sicherheitsüberprüfung zu aktivieren. Sie können mehrere Optionen auswählen.
- **Schweregrad**—Sie können einen bestimmten Schweregrad auswählen, um nur die Protokolle für diesen Schweregrad anzuzeigen. Lassen Sie alle Kontrollkästchen leer, wenn Sie alle Protokolle sehen möchten.

  Um auf die Protokollmeldungen der Sicherheitsüberprüfung der Web App Firewall für eine bestimmte Sicherheitsüberprüfung zuzugreifen, filtern Sie, indem Sie in der Dropdown-Liste für Modul **APPFW** auswählen. Der Event-Typ zeigt eine Vielzahl von Optionen an, um Ihre Auswahl weiter zu verfeinern. Wenn Sie beispielsweise das Kontrollkästchen **APPFW_FIELDFORMAT** aktivieren und auf die Schaltfläche Übernehmen klicken, werden im Syslog Viewer nur Protokollmeldungen zu den Sicherheitsüberprüfungen von Feldformaten angezeigt. Wenn Sie die Kontrollkästchen **APPFW_SQL** und **APPFW_STARTURL** aktivieren und auf die Schaltfläche **Übernehmen** klicken, werden im Syslog-Viewer nur Protokollmeldungen zu diesen beiden Verstößen gegen die Sicherheitsüberprüfung angezeigt.

Wenn Sie den Cursor in die Zeile für eine bestimmte Protokollnachricht setzen, werden mehrere Optionen wie **Module**, **EventType, EventID**oder**Message** unter der Protokollnachricht angezeigt. Sie können eine dieser Optionen auswählen, um die entsprechenden Informationen in den Protokollen hervorzuheben.

Highlights

- **Unterstützung des CEF-Protokollformats**— Die CEF-Protokollformat-Option bietet eine praktische Option zum Überwachen, Analysieren und Analysieren der Web App Firewall Protokollmeldungen, um Angriffe zu erkennen, konfigurierte Einstellungen zu optimieren, um Fehlalarme zu verringern und Statistiken zu sammeln.
- **Option zum Anpassen der Protokollnachricht**— Sie können erweiterte PI-Ausdrücke verwenden, um Protokollmeldungen anzupassen und die Daten, die Sie sehen möchten, in die Protokolle aufzunehmen.

- **Segregieren Sie Web App Firewall-spezifische Protokolle**— Sie haben die Möglichkeit, anwendungsfirewall-spezifische Protokolle zu filtern und in eine separate Protokolldatei umzuleiten.
- **Remote-Protokollierung**— Sie können die Protokollmeldungen an einen Remote-Syslog-Server umleiten.
- **Geolocation-Protokollierung**— Sie können die Web App Firewall so konfigurieren, dass sie die Geolocation des Bereichs einschließt, von dem aus die Anforderung empfangen wird. Eine eingebaute Geolokationsdatenbank ist verfügbar, aber Sie haben die Möglichkeit, eine externe Geolokationsdatenbank zu verwenden. Die Citrix ADC-Appliance unterstützt statische IPv4- und IPv6-Geolokationsdatenbanken.
- **Informationsreiche Protokollnachricht**— Im Folgenden finden Sie einige Beispiele für die Art der Informationen, die je nach Konfiguration in die Protokolle aufgenommen werden können:
  - Eine Web App Firewall-Richtlinie wurde ausgelöst.
  - Ein Verstoß gegen die Sicherheitsüberprüfung wurde ausgelöst.
  - Eine Anfrage wurde als missgebildet angesehen.
  - Eine Anfrage oder die Antwort wurde blockiert oder nicht blockiert.
  - Anforderungsdaten (wie SQL- oder Cross-Site-Scripting-Sonderzeichen) oder Antwortdaten (wie Kreditkartennummern oder sichere Objektzeichenfolgen) wurden transformiert.
  - Die Anzahl der Kreditkarten in der Antwort überschritt das konfigurierte Limit.
  - Die Kreditkartennummer und der Kreditkartentyp.
  - Die in den Signaturregeln konfigurierten Protokollzeichenfolgen und die Signatur-ID.
  - Geolokationsinformationen über die Quelle der Anfrage.
  - Maskierte (X) Benutzereingaben für geschützte vertrauliche Felder.

Maskieren Sie sensible Daten mit einem Regex-M

Die erweiterte Richtlinienfunktion (PI) `REGEX_REPLACE` in einem Protokollausdruck (gebunden an ein Web Application Firewall (WAF) -Profil) ermöglicht es Ihnen, sensible Daten in WAF-Protokollen zu maskieren. Sie können die Option verwenden, um Daten mithilfe eines Regex-Musters zu maskieren und ein Zeichen oder ein Zeichenfolgenmuster bereitzustellen, um die Daten zu maskieren. Sie können die PI-Funktion auch so konfigurieren, dass sie das erste Vorkommen oder alle Vorkommen des Regex-Musters ersetzt.

Standardmäßig bietet die Citrix GUI-Schnittstelle die folgende Maske:

- SSN
- Kreditkarte
- Kennwort
- Benutzername

Maskieren Sie sensible Daten in Web Application Firewall-

Sie können sensible Daten in WAF-Protokollen maskieren, indem Sie den erweiterten Richtlinienausdruck `REGEX_REPLACE` in dem an ein WAF-Profil gebundenen Protokollausdruck konfigurieren.
Um sensible Daten zu maskieren, müssen Sie die folgenden Schritte ausführen:

1. Hinzufügen eines Web Application Firewall-Profils
2. Binden Sie einen Protokollausdruck an das WAF-Profil

Hinzufügen eines Web Application Firewall-Profils

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add appfw profile <name>
```

Beispiel:

```
Add appfw profile testprofile1
```

Binden eines Protokollausdrucks mit dem Web Application Firewall-Profil

Geben Sie an der Eingabeaufforderung Folgendes ein:

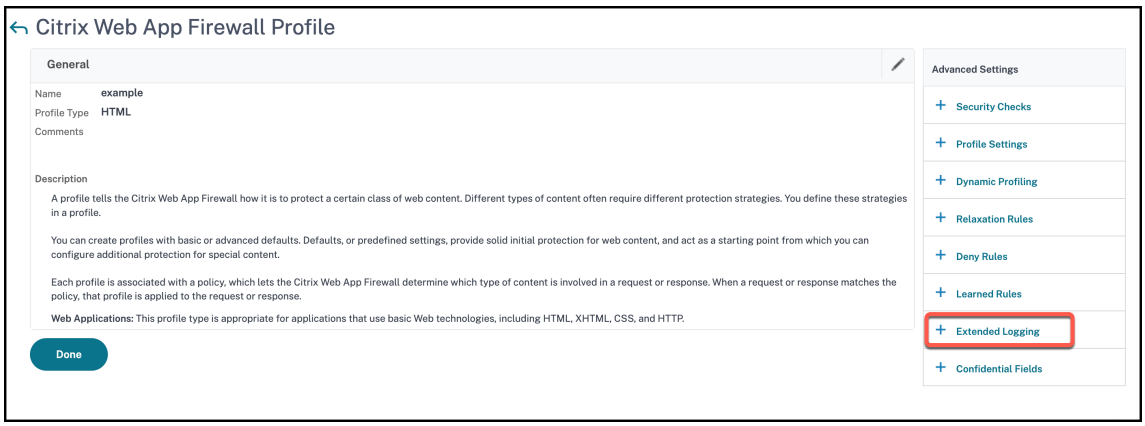
```
bind appfw profile <name> -logExpression <string> <expression> -comment <
string>
```

Beispiel:

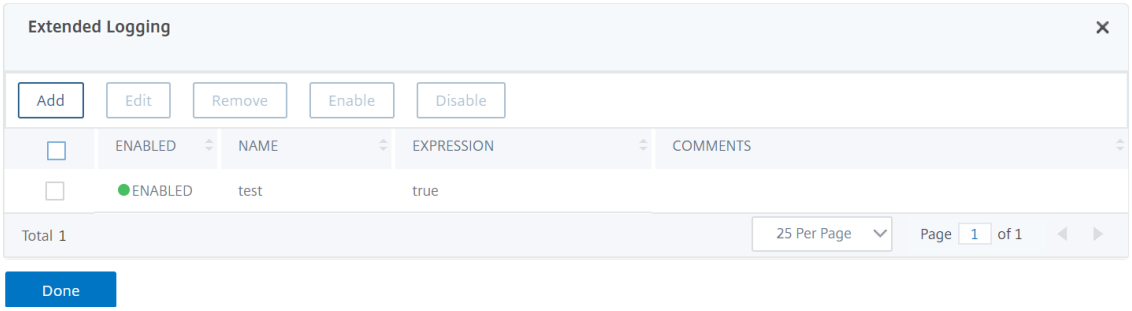
```
bind appfw profile testProfile -logExpression "MaskSSN""HTTP.REQ.BODY
(10000).REGEX_REPLACE(re!\b\d{ 3 } -\d{ 2 } -\d{ 4 } \b!, "xxx" , ALL)"-
comment "SSN Masked"
```

Maskieren Sie sensible Daten in Web Application Firewall-Protokollen über die Citrix ADC-GUI

1. Erweitern Sie im Navigationsbereich **Sicherheit** > **Citrix Web App Firewall** > **Profile**.
2. Klicken Sie auf der Seite **Profile** auf **Bearbeiten**.
3. Navigieren Sie auf der Seite **Citrix Web App Firewall Profile** zum Abschnitt **Erweiterte Einstellungen** und klicken Sie auf **Erweiterte Protokollierung**.



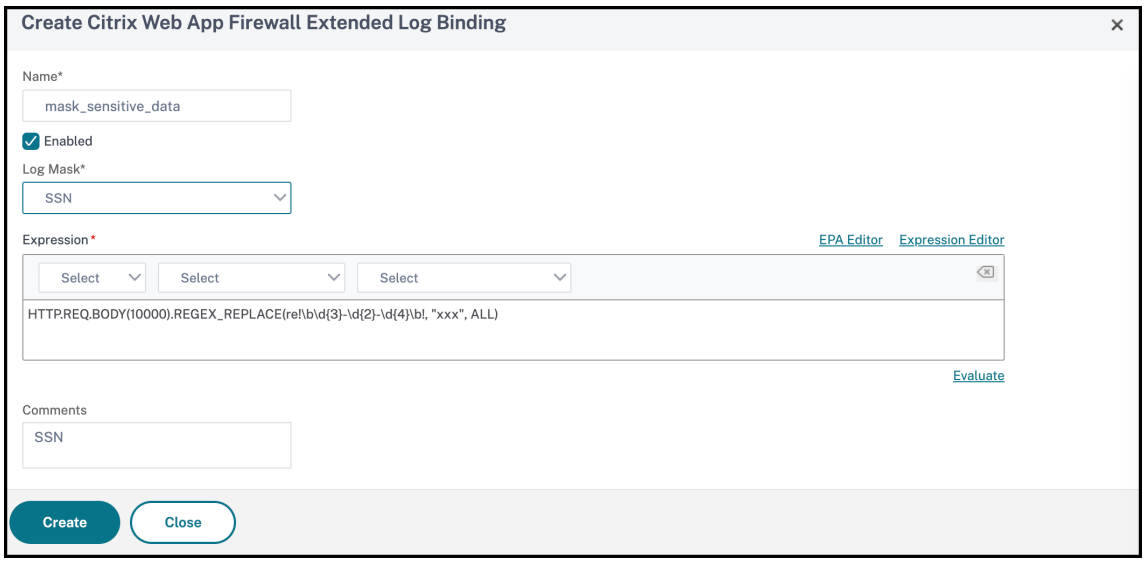
4. Klicken Sie im Abschnitt **Erweitertes Logging** auf **Hinzufügen**.



5. Legen Sie auf der Seite **Create Citrix Web App Firewall Extended Log Binding** die folgenden Parameter fest:

   a) Name. Name des Protokollausdrucks.
   b) Aktiviert. Wählen Sie diese Option um sensible Daten zu maskieren.
   c) Log-Maske. Wählen Sie die zu maskierten Daten aus.
   d) Ausdruck. Geben Sie den erweiterten Richtlinienausdruck ein, mit dem Sie sensible Daten in WAF-Protokollen maskieren
   e) Kommentare. Kurze Beschreibung der Maskierung sensibler Daten.

6. Klicken Sie auf **Erstellen** und **Schließen**.



Anhänge

October 5, 2021

Das folgende ergänzende Material enthält zusätzliche Details zu komplexen oder peripheren Aufgaben der Web App Firewall.

PCRE-Zeichenkodierungsformat

October 5, 2021

Das **Citrix ADC Betriebssystem unterstützt die direkte** Eingabe von Zeichen in den druckbaren ASCII-Zeichensatz — Zeichen mit hexadezimalen Codes zwischen HEX 20 (ASCII 32) und HEX 7E (ASCII 127). Um ein Zeichen mit einem Code außerhalb dieses Bereichs in die Web App Firewall Konfiguration aufzunehmen, müssen Sie den Hexadezimalcode UTF-8 als regulären PCRE-Ausdruck eingeben.

Viele Zeichentypen erfordern die Codierung mit einem regulären PCRE-Ausdruck, wenn Sie diese als URL, Formularfeldname oder Safe Object-Ausdruck in Ihre Web App Firewall -Konfiguration aufnehmen. Dazu gehören:

- **Oberere ASCII-Zeichen.** Zeichen mit Codierungen von HEX 7F (ASCII 128) bis HEX FF (ASCII 255). Abhängig von der verwendeten Zeichenzuordnung können sich diese Kodierungen auf Steuercodes, ASCII-Zeichen mit Akzenten oder anderen Modifikationen, nicht-lateinische Alphabetze-

ichen und Symbole beziehen, die nicht im Basis-ASCII-Satz enthalten sind. Diese Zeichen können in URLs, Formularfeldnamen und sicheren Objektausdrücken angezeigt werden.

- **Doppelbyte-Zeichen.** Zeichen mit Kodierungen, die zwei 8-Byte-Wörter verwenden. Doppelbyte-Zeichen werden hauptsächlich für die Darstellung von chinesischem, japanischem und koreanischem Text in elektronischem Format verwendet. Diese Zeichen können in URLs, Formularfeldnamen und sicheren Objektausdrücken angezeigt werden.

  ASCII-Steuerzeichen. Nicht druckbare Zeichen, die zum Senden von Befehlen an einen Drucker verwendet werden. Alle ASCII-Zeichen mit Hexadezimalcodes kleiner als HEX 20 (ASCII 32) fallen in diese Kategorie. Diese Zeichen dürfen jedoch niemals in einem URL- oder Formularfeldnamen erscheinen und würden selten, wenn überhaupt, in einem sicheren Objektausdruck erscheinen.

Die Citrix ADC Appliance unterstützt nicht den gesamten UTF-8-Zeichensatz, sondern nur die Zeichen in den folgenden acht Zeichensätzen:

- **Englisch US (ISO-8859-1).** Obwohl die Bezeichnung “English US” lautet, unterstützt die Web App Firewall alle Zeichen im Zeichensatz ISO-8859-1, auch Latin-1-Zeichensatz genannt. Dieser Zeichensatz stellt die meisten modernen westeuropäischen Sprachen vollständig dar und stellt alle außer einigen wenigen ungewöhnlichen Zeichen im Rest dar.
- **Traditionelles Chinesisch (Big5).** Die Web App Firewall unterstützt alle Zeichen im BIG5-Zeichensatz, der alle traditionellen chinesischen Schriftzeichen (Ideogramme) enthält, die häufig im modernen Chinesisch verwendet werden, wie sie in Hongkong, Macau, Taiwan gesprochen und geschrieben werden, und von vielen Menschen chinesischen ethnischen Erbes, die außerhalb des chinesischen Festlandes leben.
- **Chinesisch vereinfacht (GB2312).** Die Web App Firewall unterstützt alle Zeichen des GB2312-Zeichensatzes, der alle vereinfachten chinesischen Schriftzeichen (Ideogramme) enthält, die häufig im modernen Chinesisch verwendet werden, wie sie auf dem chinesischen Festland gesprochen und geschrieben werden.
- **Japanisch (SJIS).** Die Web App Firewall unterstützt alle Zeichen im Shift-JIS (SJIS) Zeichensatz, der die meisten Zeichen (Ideogramme) enthält, die häufig im modernen Japanisch verwendet werden.
- **Japanisch (EUC-JP).** Die Web App Firewall unterstützt alle Zeichen im EUC-JP-Zeichensatz, der alle Zeichen (Ideogramme) enthält, die häufig im modernen Japanisch verwendet werden.
- **Koreanisch (EUC-KR).** Die Web App Firewall unterstützt alle Zeichen im EUC-KR-Zeichensatz, der alle Zeichen (Ideogramme) enthält, die häufig im modernen Koreanisch verwendet werden.
- **Türkisch (ISO-8859-9).** Die Web App Firewall unterstützt alle Zeichen im Zeichensatz ISO-8859-9, der alle Buchstaben enthält, die im modernen Türkisch verwendet werden.

- **Unicode (UTF-8).** Die Web App Firewall unterstützt bestimmte weitere Zeichen im UTF-8-Zeichensatz, auch solche, die im modernen Russisch verwendet werden.

Wenn Sie die Web App Firewall konfigurieren, geben Sie alle Nicht-ASCII-Zeichen als reguläre Ausdrücke im PCRE-Format mit dem Hexadezimalcode ein, der diesem Zeichen in der UTF-8-Spezifikation zugewiesen ist. Symbole und Zeichen innerhalb des normalen ASCII-Zeichensatzes, dem einzelne, zweistellige Codes in diesem Zeichensatz zugewiesen sind, werden im UTF-8-Zeichensatz dieselben Codes zugewiesen. Zum Beispiel das Ausrufezeichen (!), dem Hex-Code 21 im ASCII-Zeichensatz zugewiesen wird, ist auch hex 21 im UTF-8-Zeichensatz. Symbolen und Zeichen aus einem anderen unterstützten Zeichensatz sind ihnen im UTF-8-Zeichensatz ein paarweise Hexadezimalcode zugewiesen. Zum Beispiel wird dem Buchstaben a mit einem akuten Akzent (á) UTF-8-Code C3 A1 zugewiesen.

Die Syntax, die Sie verwenden, um diese UTF-8-Codes in der Web App Firewall Konfiguration darzustellen, ist \xNN für ASCII-Zeichen, \xNN\xNN für Nicht-ASCII-Zeichen, die in Englisch, Russisch und Türkisch verwendet werden, und \xNN\xNN\xNN für Zeichen, die in Chinesisch, Japanisch und Koreanisch verwendet werden. Zum Beispiel, wenn Sie ein! in einem regulären Ausdruck der Web App Firewall als UTF-8-Zeichen eingeben, geben Sie\x21 ein. Wenn Sie ein á einschließen möchten, geben Sie \xC3\xA1 ein.

> **Hinweis:**
>
> Normalerweise müssen Sie keine ASCII-Zeichen im UTF-8-Format darstellen. Wenn diese Zeichen jedoch einen Webbrowser oder ein zugrunde liegendes Betriebssystem verwirren, können Sie die UTF-8-Darstellung des Zeichens verwenden, um diese Verwirrung zu vermeiden. Wenn eine URL beispielsweise ein Leerzeichen enthält, sollten Sie den Speicherplatz als \x20 codieren, um bestimmte Browser und Webserver-Software zu vermeiden.

Im Folgenden finden Sie Beispiele für URLs, Formularfeldnamen und sichere Objektausdrücke, die Nicht-ASCII-Zeichen enthalten, die als reguläre Ausdrücke im PCRE-Format eingegeben werden müssen, um in die Web App Firewall -Konfiguration aufgenommen zu werden. Jedes Beispiel zeigt zuerst die tatsächliche URL, den Feldnamen oder die Ausdruckszeichenfolge, gefolgt von einem regulären PCRE-Ausdruck.

- Eine URL mit erweiterten ASCII-Zeichen.

  Tatsächliche URL: `http://www.josénuñez.com`
  Codierte URL: `^http://www\[.\]jos\\xC3\\xA9nu\\xC3\\xB1ez\[.\]com$`

- Eine andere URL mit erweiterten ASCII-Zeichen.

  Tatsächliche URL: `http://www.example.de/trömso.html`
  Codierte URL: `^http://www[.]example[.\]de/tr\xC3\xB6mso[.]html$`

  Ein Formularfeldname, der erweiterte ASCII-Zeichen enthält.

Tatsächlicher Name: nome_do_usuário
Codierter Name: ^nome_do_usu\ xC3\ xA1rio$

- Ein sicherer Objektausdruck, der erweiterte ASCII-Zeichen enthält.

  Uncodierter Ausdruck [A-Z]{3,6} ¥[1-9\][0-9]{6,6}
  Codierter Ausdruck: [A-Z]{3,6}\ xC2\ xA5 [1-9] [0-9] {6,6}

Sie können mehrere Tabellen finden, die den gesamten Unicode-Zeichensatz und passende UTF-8-Kodierungen im Internet enthalten. Eine nützliche Website, die diese Informationen enthält, ist in der folgenden Tabelle verfügbar.

http://www.utf8-chartable.de/unicode-utf8-table.pl

Damit die Zeichen in der Tabelle auf dieser Website korrekt angezeigt werden, muss auf Ihrem Computer eine entsprechende Unicode-Schriftart installiert sein. Wenn Sie dies nicht tun, kann die visuelle Darstellung des Zeichens fehlerhaft sein. Auch wenn Sie keine entsprechende Schriftart installiert haben, um ein Zeichen anzuzeigen, sind die Beschreibung und die UTF-8- und UTF-16-Codes auf diesem Satz von Webseiten korrekt.

Whitehat WASC-Signaturtypen für WAF-Verwendung

October 5, 2021

Die Citrix Web App Firewall akzeptiert und generiert Blockierungsregeln für alle Schwachstellentypen, die die Whitehat-Scanner generieren. Bestimmte Schwachstellen gelten jedoch am besten für eine Web-App-Firewall. Im Folgenden finden Sie eine Liste dieser Sicherheitsanfälligkeiten, die nach ihrer Behebung durch die Signaturtypen WASC 1.0, WASC 2.0 oder Best Practices kategorisiert sind.

WASC 1.0-Signaturtypen

- HTTP-Anforderungsschmuggel
- HTTP-Antwortaufteilung
- HTTP-Antwortschmuggel
- Null-Byte-Injection
- Remote-Dateieinbindung
- URL-Umleitungsmissbrauch

WASC 2.0-Signaturtypen

- Missbrauch der Funktionalität
- Brute Force

- Content-Spoofing
- Diensteverweigerung
- Verzeichnisindizierung
- Informationsverlust
- Unzureichende Anti-Automatisierung
- Unzureichende Authentifizierung
- Unzureichende Autorisierung
- Unzureichender Sitzungsablauf
- LDAP-Injection
- Sitzungsfixierung

Bewährte Methoden

- Attribut Automatische Vervollständigung
- Unzureichende Cookie-Zugriffskontrolle
- Unzureichende Kennwortstärke
- Ungültige HTTP-Methodenverwendung
- Nicht-HTTP-Only Session-Cookie
- Persistentes Session-Cookie
- Persönlich identifizierbare Informationen
- Gesicherte Cachable HTTP-Nachrichten
- Unsicheres Session-Cookie

Streaming-Unterstützung für die Anforderungsverarbeitung

October 5, 2021

Die Citrix Web App Firewall unterstützt das anforderungsseitige Streaming, um eine signifikante Leistungssteigerung zu erzielen. Anstatt eine Anforderung zu puffern, untersucht die Appliance den eingehenden Datenverkehr auf Sicherheitsverletzungen wie SQL, Cross-Site-Scripting, Feldkonsistenz und Feldformate. Wenn die Appliance die Verarbeitung von Daten für ein Feld abgeschlossen hat, wird die Anforderung an den Back-End-Server weitergeleitet, während die Appliance weitere Felder auswertet. Diese Datenverarbeitung erheblich verbessert die Verarbeitungszeit bei der Bearbeitung von Formularen haben viele Felder.

> **Hinweis:**
>
> Citrix Web App Firewall unterstützt eine maximale Postgröße von 20 MB ohne Streaming. Zur besseren Ressourcennutzung empfiehlt Citrix, das Streaming nur für Nutzlasten mit mehr als

> 20 MB zu aktivieren. Außerdem muss der Back-End-Server die Chunked Requests akzeptieren, wenn Streaming aktiviert ist.

Obwohl der Streaming-Prozess für die Benutzer transparent ist, sind aufgrund der folgenden Änderungen kleinere Konfigurationsanpassungen erforderlich:

RegEx Pattern Match: RegEx Pattern-Übereinstimmung ist jetzt auf 4K für zusammenhängende Zeichenfolgen-Übereinstimmung beschränkt.

Field Name Match: Die Web App Firewall Lernengine kann nur die ersten 128 Bytes des Namens unterscheiden. Wenn ein Formular mehrere Felder mit Namen hat, die eine identische String-Übereinstimmung für die ersten 128 Bytes haben, unterscheidet sie von der Lernengine nicht. In ähnlicher Weise kann die implementierte Relaxationsregel versehentlich alle diese Felder entspannen.

Die Entfernung von Leerräumen, die prozentuale Dekodierung, die Unicode-Dekodierung und die Zeichensatzkonvertierung werden während der Kanonisierung durchgeführt, um eine Sicherheitsprüfung zu ermöglichen. Die 128-Byte-Grenze gilt für die kanonisierte Darstellung des Feldnamens im UTF-8-Zeichenformat. Die ASCII-Zeichen sind 1 Byte lang, aber die UTF-8-Darstellung der Zeichen in einigen internationalen Sprachen kann zwischen 1 Byte und 4 Byte liegen. Wenn jedes Zeichen in einem Namen 4 Bytes für die Konvertierung in das UTF-8-Format benötigt, können nur die ersten 32 Zeichen im Namen durch die erlernte Regel unterschieden werden.

Überprüfung der Feldkonsistenz: Wenn Sie die Feldkonsistenz aktivieren, werden alle Formulare in der Sitzung basierend auf dem Tag “as_fid” gespeichert, das von der Web App Firewall eingefügt wurde, ohne die “action_url” zu berücksichtigen.

- **Obligatorisches Formular-Tagging für die Konsistenz von Formularfeldern:** Wenn die Feldkonsistenzprüfung aktiviert ist, muss auch das Formular-Tag aktiviert sein. Der Feldkonsistenzschutz funktioniert möglicherweise nicht, wenn die Formularkennzeichnung deaktiviert ist.
- **Konsistenz von sitzungslosen Formularfeldern:** Die Web App Firewall führt die Konvertierung von Formularen in “GET” in “POST” nicht mehr durch, wenn der Parameter für die sitzungslose Feldkonsistenz aktiviert ist. Das Formular-Tag ist auch für sitzungslose Feldkonsistenz erforderlich.
- **Manipulation von as_fid:** Wenn ein Formular gesendet wird, nachdem as_fid manipuliert wurde, löst es eine Feldkonsistenzverletzung aus, auch wenn kein Feld manipuliert wurde. Bei Nicht-Streaming-Anforderungen war dies zulässig, da die Formulare mithilfe der in der Sitzung gespeicherten “action_url” validiert werden können.

Signaturen: Die Signaturen haben nun die folgenden Spezifikationen:

- **Ort:** Es ist jetzt zwingend erforderlich, dass für jedes Muster eine Position angegeben werden muss. Alle Muster in der Regel **MÜSSEN** ein Tag <Location> haben.
- **Schnelle Übereinstimmung:** Alle Signaturregeln müssen ein schnelles Übereinstimmungsmuster aufweisen. Wenn es kein schnelles Übereinstimmungsmuster gibt, wird

versucht, ein möglichst ausgewähltes Muster auszuwählen. Fast Match ist eine wörtliche Zeichenfolge, PCRE kann jedoch für eine schnelle Übereinstimmung verwendet werden, wenn sie eine verwendbare Literalzeichenfolge enthalten.

- **Veraltete Speicherorte:** Folgende Speicherorte werden in Signaturregeln nicht mehr unterstützt.
  - HTTP_ANY
  - HTTP_RAW_COOKIE
  - HTTP_RAW_HEADER
  - HTTP_RAW_RESP_HEADER
  - HTTP_RAW_SET_COOKIE

Cross-Site-Scripting/SQL-Transformation: Rohdaten werden für die Transformation verwendet, da die SQL-Sonderzeichen wie Single Quote (‘), Backslash () und Semikolon (;) und Cross-Site-Scripting-Tags gleich sind und keine Kanonisierung von Daten erfordern. Die Darstellung von Sonderzeichen wie HTML-Entitätskodierung, Prozentkodierung oder ASCII wird für den Transformationsvorgang ausgewertet.

Die Web App Firewall überprüft nicht mehr den Attributnamen und den Wert für den Cross-Site-Skript-Transformationsvorgang. Jetzt werden nur Cross-Site-Scripting-Attributnamen transformiert, wenn das Streaming aktiviert ist.

Verarbeitung von Cross-Site-Scripting-Tags: Im Rahmen der Streaming-Änderungen im NetScaler 10.5.e-Build und höher hat sich die Verarbeitung der Cross-Site-Scripting-Tags geändert. In früheren Versionen wurde das Vorhandensein einer öffnenden (<) oder schließenden (>) Klammer, oder beides (<>) als Cross-Site-Scripting-Verstoß betrachtet. Das Verhalten hat sich ab 10.5.e Build geändert. Wenn nur eine öffnende (<) oder nur eine schließende (>) Klammer vorhanden ist, wird es nicht mehr als Angriff betrachtet. Wenn ein auf eine öffnende (<) eine schließende (>) Klammer folgt, wird ein Cross-Site-Scripting-Angriff gemeldet. Beide Zeichen müssen in der richtigen Reihenfolge vorhanden sein (< gefolgt von >), um als Cross-Site-Scripting-Verletzung erkannt zu werden.

> **Hinweis:**
>
> **Änderung im SQL-Verstoßprotokoll Meldung:** Als Teil der Streaming-Änderungen in 10.5.e ab, verarbeiten wir nun die Eingabedaten in Blöcken. RegEx Pattern-Matching ist jetzt für zusammenhängende Zeichenfolgen auf 4K beschränkt. Mit dieser Änderung können die SQL-Verstoßprotokollmeldungen andere Informationen im Vergleich zu früheren Builds enthalten. Das Schlüsselwort und das Sonderzeichen in der Eingabe sind durch viele Bytes getrennt. Die Appliance weist bei der Verarbeitung der Daten eine Spur der SQL-Schlüsselwörter und speziellen Zeichenfolgen auf, anstatt den gesamten Eingabewert zu puffern. Zusätzlich zum Feldnamen enthält die Protokollmeldung SQL-Schlüsselwort, SQL-Sonderzeichen oder sowohl das SQL-Schlüsselwort als auch das SQL-Sonderzeichen. Der Rest der Eingabe ist nicht mehr in

> der Protokollmeldung enthalten, wie im folgenden Beispiel gezeigt:
>
> **Beispiel:**
>
> Wenn in 10.5 die Web App Firewall die SQL-Verletzung erkennt, kann die gesamte Eingabezeichenfolge in der folgenden Protokollmeldung enthalten sein:
>
> SQL-Schlüsselwortüberprüfung für Feld **text=”Wählen Sie einen Namen aus testbed1;\(;\)”.*<blocked>**
>
> In 11.0 protokollieren wir nur den Feldnamen, das Schlüsselwort und das Sonderzeichen (falls zutreffend) in der folgenden Protokollmeldung.
>
> SQL-Schlüsselwortüberprüfung für Feld`text=”select(;)”<blocked>`
> fehlgeschlagen
> Diese Änderung gilt für Anforderungen, die **application/x-www-form-urlencoded**oder **multipart/form-data**oder **text/x-gwt-rpc** Inhaltstypen enthalten. Protokollmeldungen, die während der Verarbeitung von **JSON-** oder **XML-Nutzlasten** generiert werden, sind von dieser Änderung nicht betroffen.

RAW POST Body: Die Sicherheitsprüfungen werden immer auf RAW POST Body durchgeführt.

Formular-ID: Die Web App Firewall hat das Tag “as_fid” eingefügt, bei dem es sich um einen berechneten Hash des Formulars handelt, der für die Benutzersitzung länger eindeutig ist. Es handelt sich um einen identischen Wert für ein bestimmtes Formular, unabhängig vom Benutzer oder der Sitzung.

Zeichensatz: Wenn eine Anforderung keinen Zeichensatz hat, wird bei der Verarbeitung der Anforderung der Standard-Zeichensatz verwendet, der im Anwendungsprofil angegeben ist.

Zähler:

Leistungsindikatoren mit Präfix “se” und “appfwreq” werden hinzugefügt, um die Streaming-Engine und die Anforderungszähler der Streaming-Engine zu verfolgen.

```
nsconsmg -d statswt0 -g se_err_
```

```
nsconsmg -d statswt0 -g se_tot_
```

```
nsconsmg -d statswt0 -g se_cur_
```

```
nsconsmg -d statswt0 -g appfwreq_err_
```

```
nsconsmg -d statswt0 -g appfwreq_tot_
```

```
nsconsmg -d statswt0 -g appfwreq_cur_
```

`_err counters`: gibt das seltene Ereignis an, das erfolgreich gewesen sein muss, aber aufgrund eines Speicherzuweisungsproblems oder einer anderen Ressourcenauflösung fehlgeschlagen ist.

`_tot counters`: Steigende Zähler.

`_cur counters`: Zähler, die aktuelle Werte angeben, die sich basierend auf der Nutzung aktueller Transaktionen ändern.

Tipps:

- Die Sicherheitsprüfungen der Web App Firewall müssen wie zuvor funktionieren.
- Für die Abwicklung der Sicherheitskontrollen gibt es keine festgelegte Reihenfolge.
- Die Verarbeitung der Antwortseite wird nicht beeinträchtigt und bleibt unverändert.
- Streaming ist nicht aktiv, wenn clientloses VPN verwendet wird.

> **Wichtig:**
>
> **Berechnung der Cookie-Länge:** In Release 10.5.e wurde zusätzlich zur Version 11.0 (in Builds vor 65.x) die Web App Firewall die Art der Verarbeitung des Cookie-Headers geändert. Die Appliance hat das Cookie einzeln ausgewertet, und wenn die Länge eines Cookies im Cookie-Header die konfigurierte Länge überschritten hat, wurde die Pufferüberlaufverletzung ausgelöst. Daher können Anforderungen, die in NetScaler 10.5 oder früheren Versionen blockiert wurden, zulässig sein. Die Länge des gesamten Cookie-Headers wird nicht zur Bestimmung der Cookie-Länge berechnet. In einigen Situationen kann die gesamte Cookie-Größe größer als der akzeptierte Wert sein, und der Server reagiert möglicherweise mit "400 Bad Request".
>
> **Hinweis:**
> Die Änderung wurde rückgängig gemacht. Das Verhalten in NetScaler Version 10.5.e auf Version 59.13xx.e und den nachfolgenden Builds ähnelt den Builds ohne Erweiterung von Release 10.5. Der gesamte rohe Cookie-Header wird nun bei der Berechnung der Länge des Cookies berücksichtigt. Umgebende Leerzeichen und Semikolon (;) Zeichen, die die Name-Wert-Paare trennen, werden ebenfalls bei der Bestimmung der Cookie-Länge berücksichtigt.

Verfolgen von HTML-Anforderungen mit Sicherheitsprotokollen

October 5, 2021

> **Hinweis:**
>
> Diese Funktion ist in Citrix ADC Version 10.5.e verfügbar.

Die Fehlerbehebung erfordert eine Analyse der Daten, die in der Clientanforderung empfangen wurden, und kann eine Herausforderung darstellen. Vor allem, wenn starker Verkehr durch die Appliance fließt. Die Diagnose von Problemen kann sich auf die Funktionalität auswirken, oder die Anwendungssicherheit kann eine schnelle Reaktion erfordern.

Der Citrix ADC isoliert den Datenverkehr für ein Web App Firewall -Profil und sammelt `nstrace` für die HTML-Anfragen. Der im Appfw-Modus `nstrace` gesammelte Modus enthält Details zur Anfrage mit Protokollnachrichten. Sie können "TCP-Stream folgen" im Trace verwenden, um die Details der einzelnen Transaktion einschließlich Header, Payload und der entsprechenden Protokollnachricht auf demselben Bildschirm anzuzeigen.

So erhalten Sie einen umfassenden Überblick über Ihren Traffic. Eine detaillierte Ansicht der Anfrage, der Payload und der zugehörigen Protokolldatensätze kann nützlich sein, um die Verstöße gegen die Sicherheitsprüfung zu analysieren. Sie können leicht das Muster identifizieren, das die Verletzung auslöst. Wenn das Muster zulässig sein muss, können Sie eine Entscheidung treffen, die Konfiguration zu ändern oder eine Relaxationsregel hinzuzufügen.

Vorteile

1. **Datenverkehr für ein bestimmtes Profil isolieren**: Diese Erweiterung ist nützlich, wenn Sie Datenverkehr für nur ein Profil oder bestimmte Transaktionen eines Profils zur Fehlerbehebung isolieren. Sie müssen nicht mehr die gesamten Daten durchlaufen, die in der Trace gesammelt werden, oder benötigen spezielle Filter, um Anfragen zu isolieren, die Sie interessieren, was mit starkem Datenverkehr mühsam sein kann. Sie können die von Ihnen bevorzugten Daten anzeigen.
2. **Sammeln von Daten für bestimmte Anforderungen**: Der Trace kann für eine bestimmte Dauer gesammelt werden. Sie können Trace für nur einige Anforderungen sammeln, um bestimmte Transaktionen zu isolieren, zu analysieren und zu debuggen.
3. **Identifizieren Sie Resets oder Abbrüche**: Unerwartetes Schließen von Verbindungen ist nicht leicht sichtbar. Die im —appfw-Modus gesammelte Ablaufverfolgung erfasst einen Reset oder einen Abbruch, der von der Web App Firewall ausgelöst wird. Dies ermöglicht eine schnellere Isolierung eines Problems, wenn Sie keine Meldung über eine Sicherheitsüberprüfung sehen. Fehlgebildete Anforderungen oder andere nicht RFC-konforme Anforderungen, die von der Web App Firewall beendet werden, sind jetzt leichter zu identifizieren.
4. **Entschlüsselten SSL-Datenverkehr anzeigen**: HTTPS-Datenverkehr wird im Klartext erfasst, um die Fehlerbehebung zu erleichtern.
5. **Bietet umfassende Ansicht**: Ermöglicht es Ihnen, die gesamte Anforderung auf Paketebene zu betrachten, die Nutzlast zu überprüfen, die Protokolle zu überprüfen, welche Sicherheitsüberprüfungsverletzung ausgelöst wird, und das Übereinstimmungsmuster in der Nutzlast zu identifizieren. Wenn die Nutzlast aus unerwarteten Daten, Junk-Strings oder nicht druckbaren Zeichen (Nullzeichen,\ r oder\ n usw.) besteht, sind sie im Trace leicht zu erkennen.
6. **Konfiguration ändern**: Das Debugging kann nützliche Informationen liefern, um zu entscheiden, ob das beobachtete Verhalten das richtige Verhalten ist oder die Konfiguration geändert werden muss.
7. Schnellere**Reaktionszeit**: Schnelleres Debuggen im Zieldatenverkehr kann die Reaktionszeit verbessern, um Erklärungen oder Ursachenanalysen durch das Citrix Engineering- und Support-Team zu liefern.

Weitere Informationen finden Sie unter Manuelle Konfiguration mithilfe des Themas der Befehlszeilenschnittstelle .

So konfigurieren Sie die Debug-Ablaufverfolgung für ein Profil mit der Befehlszeilenschnittstelle

Schritt 1. NS-Ablaufverfolgung aktivieren.

Sie können den Befehl show verwenden, um die konfigurierte Einstellung zu überprüfen.

- `set appfw profile <profile> -trace ON`

Schritt 2. Sammeln Sie Spuren. Sie können weiterhin alle Optionen verwenden, die für den `nstrace` Befehl gelten.

- `start nstrace -mode APPFW`

Schritt 3. Stoppen Sie die Spur.

- `stop nstrace`

Speicherort des Trace: Der `nstrace` wird in einem Zeitstempelordner gespeichert, der im Verzeichnis /var/nstrace erstellt und mit angezeigt werden kann `wireshark`. Sie können den in der `/var/log/ns.log` Datei anzeigen, um die Protokollmeldungen anzuzeigen, die Details zum Speicherort der neuen Ablaufverfolgung enthalten.

Tipps:

- Wenn die Option appfw mode verwendet `nstrace` wird, sammelt der nur die Daten für ein oder mehrere Profile, für die der “nstrace” aktiviert wurde.
- Wenn Sie den Trace im Profil aktivieren, werden die Traces nicht automatisch gesammelt, bis Sie explizit den Befehl “start ns trace” ausführen, um den Trace zu sammeln.
- Obwohl das Aktivieren von Trace für ein Profil möglicherweise keine negativen Auswirkungen auf die Leistung der Web App Firewall hat, möchten Sie diese Funktion möglicherweise nur für die Dauer aktivieren, für die Sie die Daten erfassen möchten. Es wird empfohlen, dass Sie das —trace Flag deaktivieren, nachdem Sie die Ablaufverfolgung erfasst haben. Die Option verhindert das Risiko, versehentlich Daten aus Profilen zu erhalten, für die Sie dieses Flag in der Vergangenheit aktiviert haben.
- Die Block- oder Protokollaktion muss für die Sicherheitsüberprüfung aktiviert sein, damit der Transaktionsdatensatz in den enthalten ist `nstrace`.
- Rückgänge und Abbrüche werden unabhängig von Sicherheitsüberprüfungsaktionen protokolliert, wenn der Trace für die Profile “On” ist.
- Die Funktion gilt nur für die Fehlerbehebung der vom Kunden eingegangenen Anfragen. Die Traces im —appfw-Modus enthalten nicht die vom Server empfangenen Antworten.
- Sie können weiterhin alle Optionen verwenden, die für den `nstrace` Befehl gelten. Zum Beispiel:

  ```
  start nstrace -tcpdump enabled -size 0 -mode appFW
  ```

- Wenn eine Anfrage mehrere Verstöße auslöst, enthält der `nstrace` für diesen Datensatz alle entsprechenden Protokollnachrichten.

- CEF-Protokollnachrichtenformat wird für diese Funktionalität unterstützt.
- Signaturverletzungen, die Block- oder Protokollaktionen für Prüfungen auf der Anforderungsseite auslösen, werden ebenfalls in den Trace aufgenommen.
- Im Ablaufverfolgungsprotokoll werden nur HTML-Anforderungen (Nicht-XML) erfasst.

Unterstützung der Web App Firewall für Clusterkonfigurationen

October 5, 2021

> **Hinweis:**
>
> Citrix Web App Firewall für Stripeset- und teilweise Stripesetkonfigurationen wurde in der Citrix ADC 11.0 Version eingeführt.

Ein Cluster ist eine Gruppe von Citrix ADC Appliances, die als ein einzelnes System konfiguriert und verwaltet werden. Jede Appliance im Cluster wird als Knoten bezeichnet. Abhängig von der Anzahl der Knoten, auf denen die Konfigurationen aktiv sind, werden Clusterkonfigurationen als gestreifte, teilweise gestreifte oder gepunktete Konfigurationen bezeichnet. Die Web App Firewall wird in allen Konfigurationen vollständig unterstützt.

Die beiden Hauptvorteile der Unterstützung virtueller Server mit Stripeset- und teilweise Stripeset-Servern in Clusterkonfigurationen sind die folgenden:

1. Session-Failover-Unterstützung — Konfigurationen virtueller Server mit Stripeset- und teilweise Stripeset-Servern unterstützen das Session-Failover. Die erweiterten Sicherheitsfunktionen der Web App Firewall, wie URL-Schließung starten und Formularfeldkonsistenz überprüfen, verwalten und verwenden Sitzungen während der Transaktionsverarbeitung. Wenn in einer Hochverfügbarkeitskonfiguration oder in einer ermittelten Clusterkonfiguration der Knoten, der den Web App Firewall Datenverkehr verarbeitet, fehlschlägt, gehen alle Sitzungsinformationen verloren, und der Benutzer muss die Sitzung wiederherstellen. In Stripeset-Server-Konfigurationen werden Benutzersitzungen über mehrere Knoten repliziert. Wenn ein Knoten ausfällt, wird ein Knoten, auf dem das Replikat ausgeführt wird, zum Besitzer. Sitzungsinformationen werden ohne sichtbare Auswirkungen auf den Benutzer gepflegt.
2. Skalierbarkeit: Jeder Knoten im Cluster kann den Datenverkehr verarbeiten. Mehrere Knoten des Clusters können die eingehenden Anforderungen verarbeiten, die vom virtuellen Stripeset-Server bereitgestellt werden. Dies verbessert die Fähigkeit der Web App Firewall, mehrere gleichzeitige Anforderungen zu verarbeiten, wodurch die Gesamtleistung verbessert wird.

Sicherheitsprüfungen und Signaturschutz können ohne zusätzliche clusterspezifische Web App Firewall -Konfiguration bereitgestellt werden. Sie können die übliche Web App Firewall Konfiguration auf dem CCO-Knoten (Configuration Coordinator) zur Weitergabe an alle Knoten vornehmen.

> **Hinweis:**
>
> Die Sitzungsinformationen werden über mehrere Knoten repliziert, jedoch nicht über alle Knoten in der Stripesetkonfiguration. Daher unterstützt die Failover-Unterstützung eine begrenzte Anzahl gleichzeitiger Fehler. Wenn mehrere Knoten gleichzeitig fehlschlagen, verliert die Web App Firewall möglicherweise die Sitzungsinformationen, wenn ein Fehler auftritt, bevor die Sitzung auf einem anderen Knoten repliziert wird.

Highlights

- Die Web App Firewall bietet Skalierbarkeit, hohen Durchsatz und Unterstützung für Session-Failover in Clusterbereitstellungen.
- Alle Sicherheitsprüfungen der Web App Firewall und Signaturschutz werden in allen Clusterkonfigurationen unterstützt.
- Character-Maps werden für einen Cluster noch nicht unterstützt. Die Lern-Engine empfiehlt Feldtypen in erlernten Regeln für die Sicherheitsüberprüfung im Feldformat.
- Statistiken und Lernregeln werden von allen Knoten in einem Cluster aggregiert.
- Distributed Hash Table (DHT) bietet das Caching der Sitzung und bietet die Möglichkeit, Sitzungsinformationen über mehrere Knoten hinweg zu replizieren. Wenn eine Anforderung an den virtuellen Server gesendet wird, erstellt die Citrix ADC Appliance Web App Firewall -Sitzungen im DHT und kann die Sitzungsinformationen auch aus dem DHT abrufen.
- Clustering ist mit den Advanced- und Premium-Lizenzen lizenziert. Diese Funktion ist mit der Standardlizenz nicht verfügbar.

Debuggen und Fehlerbehebung

October 5, 2021

Lesen Sie die folgenden Informationen zur Fehlerbehebung und zum Debuggen in Bezug auf die einzelnen Funktionen der Web App Firewall:

- Anwendungs-Firewall - Hohe CPU
- Speicher
- Fehler beim Hochladen großer Dateien
- Lernen
- Signaturen
- Ablaufverfolgungsprotokoll
- Sonstiges

Hohe CPU

October 5, 2021

Im Folgenden finden Sie einige der Funktionen und Probleme mit hoher CPU im Zusammenhang mit dem Debuggen und die bewährten Methoden, die bei der Arbeit mit der Web App Firewall befolgt werden:

Überprüfen Sie Richtlinientreffer, Bindungen, Netzwerkkonfiguration, Konfiguration der Web App Firewall:

- Fehlkonfiguration identifizieren
- Identifizieren *des vservers*, der den betroffenen Datenverkehr bedient

Überprüfen Sie Protokolle in den folgenden Protokolldateien auf Sicherheitsverstöße und aktuelle Konfigurationsänderungen:

- `/var/log/ns.log`
- `/var/nslog/import.log`
- `/var/nslog/aslearn.log`
- `tail -f /var/log/ns.log | grep APPFW_SIGNATURE_MATCH`

Beispiel:

```
Jun 13 01:11:09 <local0.info> 10.217.31.98 CEF:0|Citrix|NetScaler|NS11.0|APPFW| APPFW_SIGNATURE_MATCH|6|src=10.217.253.62 spt=61141 method=GET request= http://aaron.stratum8.net/FFC/wwwboard/passwd.txt msg=Signature violation rule ID 807: web-cgi /wwwboard/passwd.txt access  cn1=140 cn2=841 cs1=pr_ffc cs2=PPE0 cs3=OyTgjbXBqcpBFeENKDlde3OkMQ00001 cs4=ALERT cs5=2015 cs6=web-cgi act=not blocked
<!--NeedCopy-->
```

Isolieren Sie den Datenverkehr, der ausgeführt wird:

- Isolieren des Profils
- Sicherheitsüberprüfung isolieren
- Isolieren der URL-, virtuellen Server- und Verkehrsparameter

Die Ablaufverfolgung der bedingten Profilebene hilft bei der Identifizierung der Datenverkehrs- und Verletzungsdatensätze:

- `set appfw profile <profile> -trace ON`
- `start nstrace -mode APPFW -size 0`
- `stop nstrace`

Hinweis: Stellen Sie sicher, dass die Ablaufverfolgung mit der Option -size 0 erfasst wird.

Überprüfen Sie Aktivitätszähler für appfw, dht, IP-Reputation:

- `nsconmsg -g as_ -g appfwreq_ -g iprep -d current`

Monitorfenstergröße für Resets in Verbindung:

Appfw legt die Fenstergröße auf 9845 fest, wenn Citrix ADC die Verbindung aufgrund einer ungültigen HTTP-Nachricht zurücksetzt.

Beispiele:

- Fehlgebildete Anfrage empfangen - Verbindung zurückgesetzt
- Probleme mit hoher CPU
- Datenblätter auf Systemgrenzen prüfen
- Überprüfen Sie auf CPU-Auslastung, appfw, DHT und speicherbezogene Aktivität. Überwachen von AppFW-Sitzungen
- nsconmsg -g cc_cpu_use -g appfwreq -g as -g dht -g mem_AS_OBJ -g mem_AS_COMPONENT -d current

Überwachen Sie den Speicher, der während des Zielzeitraums von Komponenten und Objekten der Web App Firewall zugewiesen und freigegeben wurde. Es hilft, den Schutz zu isolieren, was zu einer hohen CPU-Auslastung führt.

- Profiler-Ausgabe
- Protokolle beobachten

Appfw-Prüfung isolieren, die zu einer hohen CPU führt:

- startURLClosure
- Formfiledconsistency
- CSRF
- Cookie-Schutz
- Überweisungskopfprüfung

Stellen Sie sicher, dass das automatische Update von Signaturen nicht zu einer hohen CPU führt (Deaktivieren, um zu bestätigen).

Speicher

October 5, 2021

Im Folgenden finden Sie einige der bewährten Methoden, die Sie bei Problemen mit der Verwendung des Speichers der Web App Firewall beachten sollten:

Verwendung des Befehls nsconmsg:

- Suchen Sie nach globalen Speicherstatistiken, um festzustellen, dass genügend Speicher im System vorhanden ist und keine Speicherzuordnungsfehler auftreten, indem Sie den folgenden Befehl ausführen:

  ```
  * *- nsconmsg -d memstats
  ```

- Beachten Sie die aktuell zugewiesenen und maximalen Speichergrenzen für Appsecure, IP-Reputation, Cache und Komprimierung, indem Sie den folgenden Befehl ausführen:

  ```
  nsconmsg -d memstats | egrep -i APPSECURE|IPREP|CACHE|CMP
  ```

- Überprüfen Sie appfw, DHT, IP-Reputation Aktivitätszähler, indem Sie den folgenden Befehl ausführen:

  ```
  nsconmsg -g as -g appfwreq_ -g iprep -d current
  ```

- Überprüfen Sie alle Fehlerindikatoren der Web App Firewall, indem Sie den folgenden Befehl ausführen:

  ```
  nsconmsg -g as_ -g appfwreq_ -g iprep_ -d stats | grep err
  ```

- Überprüfen Sie alle Systemfehlerindikatoren, indem Sie den folgenden Befehl ausführen:

  ```
  nsconmsg -g err -d current
  ```

- Prüfen Sie nach CPU-, APPFWREQ-, AS-und DHT-Leistungsindikatoren, indem Sie den folgenden Befehl ausführen:

  ```
  nsconmsg -g cc_cpu_use -g appfwreq -g as -g dht -d current
  ```

- Überprüfen Sie den konfigurierten Cache-Speicher, indem Sie den folgenden Befehl ausführen:
- `show cacheparameter`
- Überprüfen Sie den konfigurierten Speicher, indem Sie den folgenden Befehl ausführen:

  ```
  nsconmsg -d memstats | egrep -i CACHE
  ```

- Identifizieren der Speicherverteilung in Komponenten und Objekten der Web App Firewall:

AS_OBJ_-Speicher anzeigen:

```
nsconmsg -K newnslog -d stats | grep AS_OBJ | egrep -v AppFW_cpu0|total |
sort -k3
```

AS_COMPONENT_Speicher anzeigen:

```
nsconmsg -K newnslog -d stats | grep AS_COMPONENT | egrep -v AppFW_cpu0|
total | sort -k3
```

Überprüfen Sie die Anzahl der lebenden Sitzungen, indem Sie den folgenden Befehl ausführen:

Monitor/Plotten der aktiven Sitzung:


```
nsconmsg -g as_alive_sessions -d current
```

Monitor/Plot insgesamt zugewiesene, kostenlose, aktualisierte Sitzungen:

- `nsconmsg -g as_tot_alloc_sessions -g as_tot_free_sessions -d current`
- `nsconmsg -g as_tot_update_sessions -d current`

Reduzieren Sie bei Bedarf das Sitzungszeitlimit, um sicherzustellen, dass Sitzungslimits nicht verwendet werden, indem Sie den folgenden Befehl ausführen:

```
set appfwsettings -sessionTimeout <300>
```

Legen Sie bei Bedarf die maximale Lebensdauer der Sitzung fest, indem Sie den folgenden Befehl ausführen:

```
set appfwsettings -sessionLifetime <7200>
```

Überprüfen des zugewiesenen und genutzten Speichers

So überprüfen Sie den gesamten zugewiesenen Speicher und den verwendeten Speicher:

- Verwenden Sie den Befehl **nsconmsg —d memstats** . Beachten Sie das Feld **MEM_APPSECURE** .
- Verwenden Sie den Befehl **stat appfw**, um Informationen über den Verbrauch zu erhalten.

Die Web App Firewall löscht die Protokolle nach einer bestimmten Zeit oder Größe nicht automatisch.

- `All AppFw logs are archived in the */var/log/ns.log*` -Datei. Die Datei *ns.log* führt den Rollover-Task aus.

Weitere Informationen finden Sie unter folgendem Link:<`http://support.citrix.com/article/CTX121898`>

Erhöhen des Speichers der Web App Firewall:

- Es gibt keine CLI-Option, um den Speicher der Web App Firewall zu erhöhen. Der Web App Firewall -Speicher ist plattformspezifisch.
- Sie können die Option *nsapimgr* verwenden, um den Speicher zu erhöhen, dies wird jedoch nicht empfohlen.

Der maximal zulässige Speicher für die Web App Firewall wird von der Plattform bestimmt, und das Deaktivieren des IC wirkt sich nicht auf die Speicherzuweisung aus.

Fehler beim Hochladen großer Dateien

October 5, 2021

Wenn große Fehler beim Hochladen von Dateien auftreten, stellen Sie sicher, dass Sie Folgendes überprüfen:

— Falsch konfigurierte Anwendungsfirewall Postbody-Grenze
— Aktiviert das Scannen von Dateien, was zu einer erhöhten Verarbeitungszeit führt.
— Erledigen von Systemgrenzen.

Für Nutzlasten mit mehr als 20 MB empfiehlt Citrix, das Streaming auf dem Firewallprofil der Anwendung zu aktivieren. Außerdem müssen Sie sicherstellen, dass der Backend-Server Chunked Requests unterstützt, bevor Sie das Streaming aktivieren.

Seit Release 11.0 kann das Streaming-Flag auf Profilbasis aktiviert werden, um Puffern zu vermeiden, indem Sie den folgenden Befehl ausführen:

```
set appfw profile <profile name> -streaming on
```

Lernen

October 5, 2021

Im Folgenden finden Sie einige der empfohlenen Best Practices, wenn Probleme mit der Lernfunktionalität auftreten:

Aslearn Prozess:

- Stellen Sie sicher, dass der Prozess *aslearn* ausgeführt wird.
- Top-Befehlsausgabe prüfen
- Überprüfen Sie die Ausgabe von ps Befehl, indem Sie den folgenden Befehl ausführen:

  ```
  ps -ax | grep aslearn | grep -v "grep"
  ```

  Beispiel:

  ```
  root@ns# ps -ax | grep aslearn | grep -v "grep"
  1439  ??  Ss     0:03.86 /netscaler/aslearn -start -f /netscaler/
     aslearn.conf
  <!--NeedCopy-->
  ```

- Identifizieren Sie die letzten Konfigurationsbefehle, die vor dem beobachteten Problem ausgeführt wurden, indem Sie die Datei *ns.log* überprüfen:

  ```
  /var/log/ns.log
  ```


- Prüfen Sie aslearn Protokolle, um nach aslearn Nachrichten zu suchen:

  ```
  /var/log/aslearn.log
  ```

- Isolieren des Profils und der Sicherheitsüberprüfung, die durchgeführt wird
- Identifizieren Sie den GUI- und CLI-Befehl, der fehlschlägt, indem Sie den folgenden Befehl ausführen:

  ```
  show appfw learningdata <profileName> <securityCheck>
  ```

  Beispiele:

  - `show learningdata test_profile starturl`
  - `show learningdata test_profile crosssiteScripting`
  - `show learningdata test_profile sqLInjection`
  - `show learningdata test_profile csRFtag`
  - `show learningdata test_profile fieldformat`
  - `show learningdata test_profile fieldconsistency`

- Führen Sie die Integritätsprüfung von sqlite von der bsd Shell-Eingabeaufforderung durch:

  ```
  nsshell ## sqlite3 /var/nslog/asl/<profile_name_in_lowercase>.db '
  pragma integrity_check;
  ```

  Beispiele:

  ```
  root@ns# sqlite3 /var/nslog/asl/tsk0247284.db 'pragma
     integrity_check;'
  ok
  <!--NeedCopy-->
  ```

- Bereitstellen oder Entfernen von Regeln, um wieder mit dem Lernen zu beginnen:
  - Wenn 2000 Lernelemente (pro Schutz) erreicht sind, können Sie für diesen Schutz nicht mehr lernen.
  - Wenn eine Größe von 20 MB für die Datenbank erreicht wird, beenden Sie das Lernen für alle Schutzmaßnahmen
  - Neustart des aslearn-Prozesses

  ```
  */netscaler/aslearn -start -f/netscaler/aslearn.conf*
  ```

- Überprüfen Sie den Speicherplatz im Ordner /var, indem Sie Folgendes ausführen:

  ```
  du -h /var
  ```

- Überprüfen Sie die Grenzwerte für Lernschwellenwerte, indem Sie den folgenden Befehl ausführen:


```
show appfwlearningsettings <profile_name> <securityCheck>
```

- Sammeln Sie gelernte Daten, indem Sie den folgenden Befehl ausführen:

  ```
  export appfwlearningdata <profile_name> <securityCheck>
  ```

- Stellen Sie sicher, dass erlernte Daten in den Collector hochgeladen werden.

Signaturen

October 5, 2021

Erste Schritte mit Signaturen

So fügen Sie Signatur hinzu:

1. Wählen Sie die **Standardsignatur**aus, und klicken Sie auf **Hinzufügen**, um eine Kopie zu erstellen.
2. Geben Sie einen aussagekräftigen Namen. Das neue SIG-Objekt wird als Benutzerdefiniertes Objekt hinzugefügt.
3. Aktivieren Sie die Zielregeln, die Ihren spezifischen Anforderungen entsprechen.
   - Die Regeln sind standardmäßig deaktiviert.
   - mehr Regeln erfordern mehr Verarbeitung
4. Konfigurieren Sie die Aktionen:

   Block- und Protokollaktionen sind standardmäßig aktiviert. Statistik ist eine weitere Option
5. Legen Sie die Signatur fest, die von Ihrem Profil verwendet werden soll.

Tipps zur Verwendung von Signaturen

- Optimieren Sie den Verarbeitungsaufwand, indem Sie nur die Signaturen aktivieren, die zum Schutz Ihrer Anwendung anwendbar sind.
- Jedes Muster in der Regel muss übereinstimmen, um eine Signaturübereinstimmung auszulösen.
- Sie können eigene benutzerdefinierte Regeln hinzufügen, um eingehende Anforderungen zu überprüfen, um verschiedene Arten von Angriffen zu erkennen, wie SQL-Injection oder Cross-Site-Skripting-Angriffe.
- Sie können auch Regeln hinzufügen, um die Antworten zu überprüfen, um das Auslaufen vertraulicher Informationen wie Kreditkartennummern zu erkennen und zu blockieren.

- Fügen Sie mehrere Sicherheitsüberprüfungsbedingungen hinzu, um Ihre eigene benutzerdefinierte Prüfung zu erstellen.

Best Practices für die Verwendung von Signaturen

Im Folgenden finden Sie einige der bewährten Methoden, die Sie bei Problemen im Zusammenhang mit Signaturen befolgen können:

- Stellen Sie sicher, dass der Importbefehl sowohl für primäre als auch für sekundäre erfolgreich war.
- Überprüfen Sie, ob CLI- und GUI-Ausgaben konsistent sind.
- Überprüfen Sie ns.log, um Fehler beim Signaturimport und beim automatischen Update zu identifizieren.
- Überprüfen Sie, ob der DNS-Nameserver ordnungsgemäß konfiguriert ist.
- Überprüfen Sie die Inkompatibilität der Schemaversion.
- Überprüfen Sie, ob das Gerät nicht auf die Signaturaktualisierungs-URL zugreifen kann, die in AWS zur automatischen Aktualisierung gehostet wird.
- Überprüfen Sie, ob die Version nicht übereinstimmt zwischen der Standardsignatur und den vom Benutzer hinzugefügten Signaturen.
- Überprüfen Sie, ob die Versionsfehlung zwischen Signaturobjekten auf dem primären und sekundären Knoten übereinstimmt.
- Überwachen Sie die hohe CPU-Auslastung (deaktivieren Sie die automatische Aktualisierung, um ein Problem mit der Signaturaktualisierung auszuschließen).

Ablaufverfolgungsprotokoll

October 5, 2021

So zeichnen Sie Ablaufverfolgungsprotokolle auf:

1. Aktivieren Sie die Ablaufverfolgung für das Profil. Sie können den Befehl show verwenden, um die konfigurierte Einstellung zu überprüfen.

```
set appfw profile <profile> -trace ON
```

1. Beginnen Sie mit dem Sammeln von Trace. Sie können weiterhin alle Optionen verwenden, die für den Befehl nstrace gelten.

```
start nstrace -mode APPFW
```


1. Stoppen Sie das Sammeln der Trace

```
stop nstrace
```

Speicherort des Trace: Der nstrace wird in einem Zeitstempelordner gespeichert, der im Verzeichnis */var/nstrace* erstellt und mit Wireshark angezeigt werden kann. Sie können die Datei */var/log/ns.log* senden, um die Protokollmeldungen anzuzeigen, die Details zum Speicherort der neuen Ablaufverfolgung enthalten.

Vorteile von Trace-Protokollen:

- Datenverkehr für ein bestimmtes Profil isolieren
- Sammeln von Daten für bestimmte Anfragen
- Identifizieren von Zurücksetzungen oder Abbrüchen
- Entschlüsselten SSL-Datenverkehr anzeigen: HTTPS-Datenverkehr wird im Klartext erfasst, um die Fehlerbehebung zu erleichtern.
- Bietet umfassende Ansicht: Ermöglicht Ihnen, die gesamte Anforderung auf Paketebene zu betrachten, die Nutzlast zu überprüfen, Protokolle anzuzeigen, um zu überprüfen, welche Sicherheitsüberprüfungsverletzung ausgelöst wird, und das Übereinstimmungsmuster in der Nutzlast zu identifizieren. Wenn die Nutzlast aus unerwarteten Daten, Junk-Strings oder nicht druckbaren Zeichen (Nullzeichen, r oder n usw.) besteht, sind sie im Trace leicht zu erkennen.
- Beschleunigte Reaktionszeit: Schnelleres Debuggen im Zieldatenverkehr, um die Ursachenanalyse durchzuführen.

Sonstiges

October 5, 2021

Im Folgenden finden Sie die Lösungen für einige der Probleme, die bei der Verwendung der Web App Firewall auftreten können.

- Web App Firewall legt die Fenstergröße auf 9845 fest, wenn die Verbindung für ungültige HTTP-Nachrichten zurückgesetzt wird.

  — Fehlerhafte Anfrage empfangen - Verbindungszurücksetzung [Client/Server sendet ungültigen Header für Inhaltslänge]
  — Unbekannter Inhaltstyp in Anforderungsheadern

- Systemlimit: Die Anwendung erscheint eingefroren

  — Tritt auf, wenn die maximale Sitzungsgrenze erreicht ist. (100K)
  — Weniger Systemspeicher für den Betrieb.

    - IP-Reputation-Funktion funktioniert nicht
      — Der iprep-Prozess dauert etwa fünf Minuten, nachdem Sie die Reputation-Funktion

aktiviert haben. Die IP-Reputationsfunktion funktioniert möglicherweise für diese Dauer nicht.

- Unerwartete Verletzungen der Web App Firewall, die ausgelöst werden

  — Sitzungszeitüberschreitung hat einen Standardwert von 900 Sekunden. Wenn Sitzungstimeout auf einen niedrigen Wert eingestellt ist, kann der Browser falsche Positive für Prüfungen auslösen, die auf Sitzungssitzung beruhen (z. B. CSRF, FFC). Überprüfen Sie die Sitzungszeitüberschreitung, und schauen Sie sich die Sitzungs-ID an (cs3 in CEF-Protokollen). Wenn die SessionID unterschiedlich ist, könnte das Sitzungstimeout der Grund sein.
  — Wenn Formular dynamisch durch Javascript generiert wird, kann es falsche FFC-Verletzungen auslösen.

- Leerer Feldname in FFC Verletzungsprotokollen (vor Version 11.0)

  Dies kann in Szenarien gesehen werden, in denen wir auf ein Formularfeld stoßen, das nicht in den Formularen in unserer Sitzung enthalten ist.

  Szenarien, in denen dies auftreten kann:

  — Die Sitzung hat das Timeout ab dem Zeitpunkt, an dem das Formular an den Client gesendet wurde und wann es empfangen wurde.
  — Das Formular wurde auf der Client-Seite mit einem Java-Skript generiert.

Referenzen

January 25, 2022

Weitere Informationen zu den Funktionen der Web App Firewall finden Sie in den folgenden Ressourcen.

- So ändert die Citrix Web App Firewall den Datenverkehr von Anwendungen.
- Ablaufverfolgung und wie HTML-Anfragen über Web App Firewall Sicherheitsverletzung auf der Citrix ADC-Appliance protokolliert
- Schutz auf höchstem Niveau
- Entspannung der Sicherheit
- Informationen zum Konfigurieren und Bereitstellen einer Anwendung:
  - Anwendung
  - Firewall
  - Protokolle
- Artikel zur Signaturaktualisierung

- Bot-Verwaltung

Signaturwarnung Artikel

October 5, 2021

Citrix Web Application Firewall (WAF) kündigt Signaturaktualisierungen an, die Sie herunterladen und auf Ihre Appliance anwenden können. Wenn Sie einen Sicherheitsangriff entdecken, erhalten Sie eine E-Mail-Benachrichtigung über das neue Signaturupdate. Sie können die Signatur herunterladen und auf Ihre Appliance anwenden.

So erhalten Sie Signaturwarnbenachrichtigung

October 5, 2021

In diesem Artikel wird erläutert, wie Sie Signaturwarneinstellungen konfigurieren, um E-Mail-Benachrichtigungen für neue Signaturaktualisierungen zu erhalten.

Zusammenfassung

Netzwerkadministratoren möchten eine E-Mail-Benachrichtigung für neue Signaturaktualisierungen und -benachrichtigungen der Web Application Firewall erhalten.

Problem

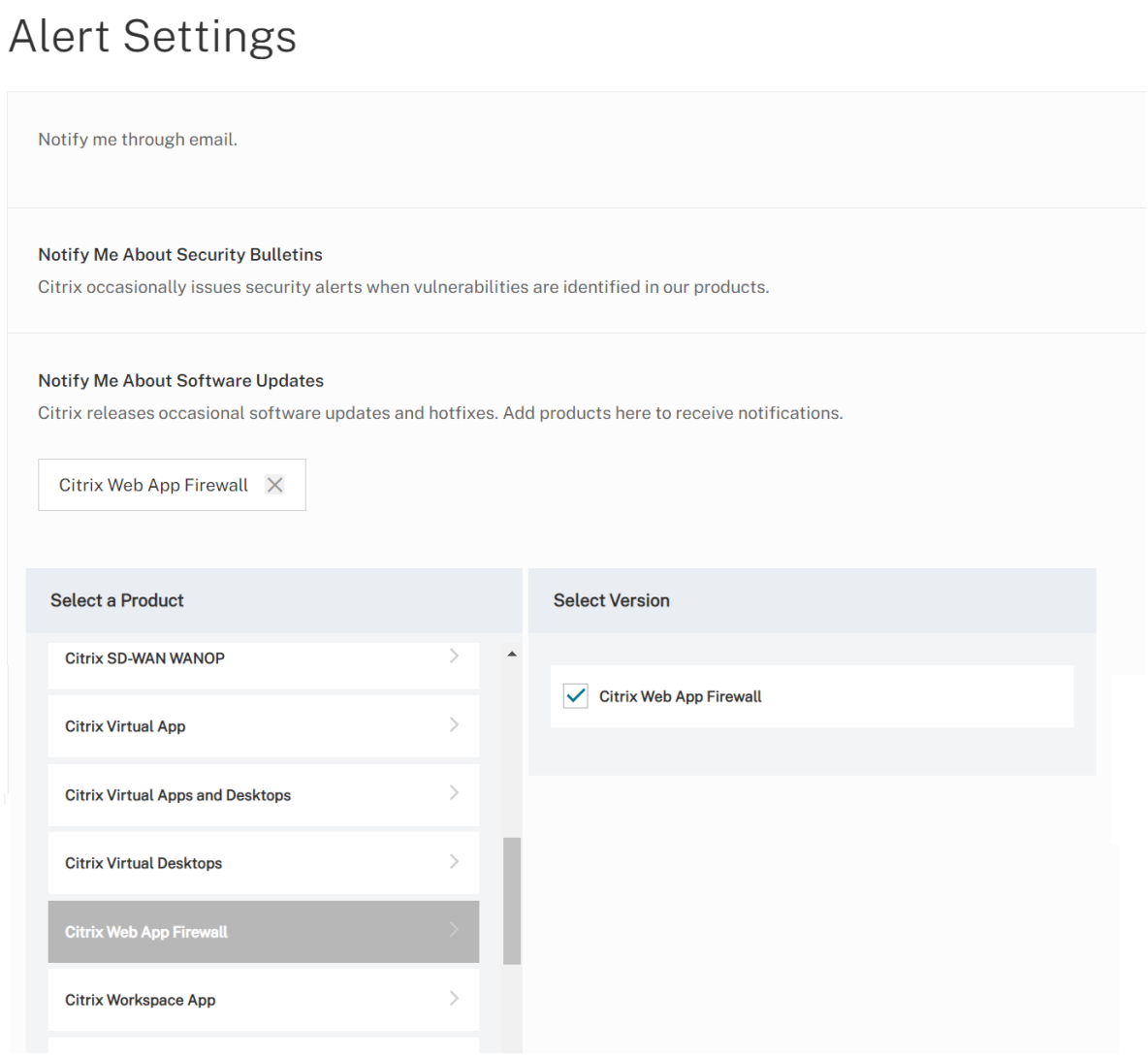
Ein Netzwerkadministrator, der benachrichtigt werden möchte, wenn eine neue Signatur für die Web Application Firewall verfügbar ist, kann sich dafür entscheiden, per E-Mail benachrichtigt zu werden. Der Administrator erhält eine E-Mail-Benachrichtigung, wenn neue Signaturen zum Herunterladen verfügbar sind.
Netzwerkadministratoren, um E-Mail-Benachrichtigungen für neue Signaturaktualisierungen zu erhalten.

Lösung

Gehen Sie folgendermaßen vor, um E-Mail-Benachrichtigungen für neue Signaturaktualisierungen zu erhalten:

1. Melden Sie sich bei der Citrix Support-Website an`https://support.citrix.com/user/alerts`.

2. Aktivieren Sie im Abschnitt **Warnungseinstellungen** die Option Über E-Mail benachrichtigen.
3. Wählen Sie **Produkte hinzufügen** aus, um den Produktkatalog anzuzeigen.
4. Klicken Sie auf **Citrix Web App Firewall** und aktivieren Sie dann das Kontrollkästchen **Citrix Web App Firewall**.
5. Klicken Sie auf **Einstellungen speichern**.



1. Aktivieren Sie im Abschnitt **Warnungseinstellungen** die Option Über E-Mail benachrichtigen.
2. Wählen Sie **Produkte hinzufügen** aus, um den Produktkatalog anzuzeigen.
3. Klicken Sie auf **Anwendungsfirewall**, und klicken Sie dann auf das Kontrollkästchen **Signaturen** .
4. Klicken Sie auf **Einstellungen speichern**.

Signaturupdate Version 27

January 25, 2022

Für die in Version 27 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen. Das Signatur-Update umfasst die Signatur-ID, die Signaturversion und eine Liste der adressierten CVEs.

Signaturversion

Signaturen sind mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999921	cve-2018-1002000	Web-miscWordPress Arigato Autoresponder und Newsletter SQL Injection Sicherheitslücke.
999920		Web-MiscWordPress-Plug-In Corner Ad 1.0.7 - Gespeichertes Cross-Site Scripting
999919	cve-2018-1002009	Web-MiscWordPress Arigato Autoresponder und Newsletter bft_unsubscribe Cross-Site-Scripting-Schwachstelle.
999918	cve-2018-1002002	Web-MiscWordPress Arigato Autoresponder und Newsletter mehrere Cross-Site-Scripting-Schwachstelle.

Regel zur Unterschrift	CVE-ID	Beschreibung
999918	cve-2018-1002003	Web-MiscWordPress Arigato Autoresponder und Newsletter mehrere Cross-Site-Scripting-Schwachstelle.
999918	cve-2018-1002004	Web-MiscWordPress Arigato Autoresponder und Newsletter mehrere Cross-Site-Scripting-Schwachstelle.
999918	cve-2018-1002005	Web-MiscWordPress Arigato Autoresponder und Newsletter mehrere Cross-Site-Scripting-Schwachstelle.
999918	cve-2018-1002006	Web-MiscWordPress Arigato Autoresponder und Newsletter mehrere Cross-Site-Scripting-Schwachstelle.
999918	cve-2018-1002007	Web-MiscWordPress Arigato Autoresponder und Newsletter mehrere Cross-Site-Scripting-Schwachstelle.
999917	cve-2018-1002001	Web-MiscWordPress Arigato Autoresponder und Newsletter mehrere Cross-Site-Scripting-Schwachstelle.
999917	cve-2018-1002008	Web-MiscWordPress Arigato Autoresponder und Newsletter mehrere Cross-Site-Scripting-Schwachstelle.
999916	cve-2018-8719	Web-MiscWordPress-Plug-in WP-Sicherheitsprüfprotokoll - wp-content/uploads/wp-security-audit-log/* uneingeschränkter Zugriff

Regel zur Unterschrift	CVE-ID	Beschreibung
999915	cve-2019-7743	WEB-MISC- Joomla phar:// Stream-Wrapper-Objekteinschleusungsrisiko durch Ausführen von hochgeladenen Nicht-Phar-Dateien
999914		Web-MiscWordPress Plug-in E-Mail-Abonnenten und Newsletter 3.4.7 Schwachstelle bei der Offenlegung von Informationen
999913		Web-MiscWordPress-Plug-In AD Manager WD v1.0.11 - wd_ads_admin_class.php Download beliebiger Dateien
999912		Web-IISMicrosoft IIS - Offenlegung von Kurzdatei/Ordnernamen

Signaturupdate Version 28

January 25, 2022

Für die in Version 28 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen. Das Signatur-Update umfasst die Signatur-ID, die Signaturversion und eine Liste der adressierten CVEs.

Signaturversion

Die Signaturversion 28 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999898	CVE-2018-12895	WEB-MISC WordPress vor 4.9.7 Sicherheitsanfälligkeit beim Durchlaufen von Verzeichnissen.
999899	CVE-2019-9618	Web-misc-GraceMedia Player WordPress Plug-in 1.0 Schwachstelle für willkürliche lokale Dateieinbindung
999900	CVE-2018-20714	WEB-MISC WordPress-Plug-In WooCommerce vor 3.4.6 - Sicherheitslücke beim Löschen von Dateien.
999901	CVE-2018-11868	WEB-MISC FlowPaper FlexPaper vor 2.3.7 kann das Zurücksetzen von Konfigurationsdateien durch Remotecodeausführung und -rücksetzung ermöglichen.
999902	CVE-2018-11868	WEB-MISC FlowPaper FlexPaper vor 2.3.7 kann Remotecodeausführung ermöglichen.
999903	CVE-2019-9184	Web-misc-joomla! J2Store-Plug-in 3.x vor 3.3.7 Ermöglicht SQL-Injection.
999904	CVE-2019-9168	WEB-MISC WordPress-Plug-In WooCommerce vor 3.5.5-Cross-Site-Scripting über Photoswipe-Beschriftung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999905		WEB-MISC WordPress-Plug-In Abandoned Cart vor 5.1.3 für WooCommerce-gespeichertes Cross-Site-Scripting.
999906	CVE-2019-8942	WEB-MISC WordPress vor 4.9.9 und 5.x vor 5.0.1-Remotecodeausführung.
999907	CVE-2019-8942	WEB-MISC WordPress vor 4.9.9 und 5.x vor 5.0.1-Remotecodeausführung.
999908	CVE-2019-8942	WEB-MISC WordPress vor 4.9.9 und 5.x vor 5.0.1-Remotecodeausführung
999909	CVE-2017-16562	Web-Misc-deluxe Theme UserPro WordPress Plug-in-Sicherheit Umgehung der Sicherheitslücke über up_auto_log=true Parameter
999910	CVE-2018-20782	WEB-MISC WordPress-Plugin GloBee vor 1.1.2 für WooCommerce-IPN Nachrichten Spoofing
999911	CVE-2019-6340	Drupal-willkürliche Remotecodeausführung in Drupal Core 8 RESTful WebServices

Signaturupdate Version 29

January 25, 2022

Für die in Version 29 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 29 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis**:
>
> Das Aktivieren der Regeln für Postbody und Response Body kann sich auf die Citrix ADC CPU auswirken

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999896	CVE-2019-2725	Weblogic 10.3.6 Remotecodeausführung
999897	CVE-2019-2725	Weblogic 10.3.6 Remotecodeausführung

Signaturupdate Version 30

January 25, 2022

Für die in Version 30 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 30 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren der Regeln für Postbody und Response Body kann sich auf die Citrix ADC CPU auswirken

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999879	<>	WEB-MISC WordPress-Plug-In WooCommerce Checkout Manager - Schwachstelle beim Hochladen beliebiger Dateien
999880	<>	Web-MISC WordPress Plug-in-Erweitertes Kontaktformular 7 DB vor 1.6.1 - Sicherheitsanfälligkeit in SQL Injection
999881	<>	WEB-MISC WordPress-Plug-In-Kontaktformulargenerator vor 1.0.67 — Sicherheitsanfälligkeit bei der Einbindung lokaler Dateien
999882	<>	SQL HTTP URI-Blindeinschleusungsversuch
999883	<>	WEB-MISC Loco Translate WordPress-Plug-In 2.1.1 und früher — Sicherheitsanfälligkeit für lokale Dateiein
999884	<>	WEB-MISC WordPress Plug-In Duplikate-Seite vor 3.4 - Sicherheitsanfälligkeit bei SQL-Injection

Regel zur Unterschrift	CVE-ID	Beschreibung
999885	CVE-2019-0232	WEB-MISC Apache Tomcat RCE über .CMD CGI-Skripts bei EnableCmdLineArgu-ments=true in MS Windows
999886	CVE-2019-0232	WEB-MISC Apache Tomcat RCE über .BAT CGI-Skripts bei EnableCmdLineArgu-ments=true in MS Windows
999887	CVE-2019-10692	WWEB-MISC WordPress-Plug-In wp-Google-Maps Vor 7.11.18 - Sicherheitsanfälligkeit in SQL Injection.
999888	CVE-2019-10946	WEB-MISC Joomla! Vor 3.9.5 — Sicherheitslücke beim Umgehen der Sicherheit
999889	CVE-2019-10945	WEB-MISC Joomla! Vor 3.9.5 — Sicherheitsanfälligkeit durch Verzeichnisdurchlauf
999890	CVE-2019-9912	WEB-MISC WPGoogleMaps WordPress-Plug-In vor 7.10.41 Reflektierte Sicherheitsanfälligkeit Cross-Site Scripting
999890	CVE-2019-9912	WEB-MISC WPGoogleMaps WordPress-Plug-In vor 7.10.41 Reflektierte Sicherheitsanfälligkeit Cross-Site Scripting
999891	CVE-2019-9911	WEB-MISC WordPress-Plug-In Auto-Poster für soziale Netzwerke vor 4.2.8 - Reflektierte Sicherheitslücke Cross-Site Scripting

Regel zur Unterschrift	CVE-ID	Beschreibung
999892	CVE-2019-9908	WEB-MISC WordPress-Plug-In Font_Organizer 2.1.1 - Reflektierte Cross-Site Scripting
999893	CVE-2019-9787	WEB-MISC WordPress vor 4.9.7 — Sicherheitsanfälligkeit bei Remotecodeausführung
999894	CVE-2019-9568	WEB-MISC Forminator Kontaktformular, Umfrage & Quiz Builder WordPress-Plug-In vor 1.6 Blind SQLi Sicherheitsanfälligkeit
999895	CVE-2019-9567	WEB-MISC Forminator Kontaktformular, Umfrage & Quiz Builder-WP-Plug-in vor 1.6 Persistente Cross-Site Scripting Sicherheitsanfälligkeit
999877	CVE-2018-20062	WEB-MISC nonECM V1.3 - ThinkPHP filtert willkürliche Schwachstelle bei der Ausführung von PHP-Code
999878	CVE-2019-9082	Sicherheitsanfälligkeit in WEB-MISC bei Remotecodeausführung in ThinkPHP 5.x vor 5.1.32

Signaturupdate Version 32

January 25, 2022

Für die in Version 32 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 32 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis**
>
> Das Aktivieren der Regeln für Postbody und Response Body kann sich auf die Citrix ADC CPU auswirken

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999875	CVE-2016-4438, CVE-2016-3087	WEB-STRUTS Apache Struts 2.3.20 bis 2.3.28.1 Sicherheitsanfälligkeit bei Remote-Ausführung über URL
999876	CVE-2019-10867	WEB-MISC Pimcore vor 5.7.1 — Sicherheitsanfälligkeit durch Deserialisierung (CVE-2019-10867)

Signaturupdate Version 33

January 25, 2022

Für die in Version 33 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 33 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis**
>
> Das Aktivieren der Regeln für Postbody und Response Body kann sich auf die Citrix ADC CPU auswirken

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel	CVE	Beschreibung	Schwachstellen-Referenz
999860		WordPress-Plug-in Yuzo Verwandte Beiträge Site-übergreifende Sicherheitsanfälligkeit	https://www.wordfence.com/blog/2019/04/yuzo-related-posts-zero-day-vulnerability-exploited-in-the-wild
999861	CVE-2019-12099		cve,2019-12099
999862		WordPress-Plug-in-Datenbankbackup <= 5.2 — Remote-codeausführung	https://www.wordfence.com/blog/2019/05/os-command-injection-vulnerability-patched-in-wp-database-backup-plug-in
999863		WordPress-Plugin Slick Popup - Berechtigungseskalation	https://www.wordfence.com/blog/2019/05/privilege-escalation-flaw-present-in-slick-popup-plug-in

Regel	CVE	Beschreibung	Schwachstellen-Referenz
999864	CVE-2019-10866	WordPress-Plug-In Form Maker 1.13.3 - SQL-Einschleusung	cve,2019-10866
999865		WordPress Plug-in Give— Cross-Site Scripting für Spender	https://blog.sucuri.net/2019/05/wordpress-plug-in-give-stored-xss-for-donors.html
999866		WordPress-Plug-In Mein Kalender <= 3.1.9 — Sicherheitslücke beim Cross-Site Scripting nicht authentifiziert	https://wpvulndb.com/vulnerabilities/9267
999867		WordPress-Plugin Slimstat <= 4.8 - Nicht authentifiziert Gespeichertes Cross-Site Scripting	https://blog.sucuri.net/2019/05/slimstat-stored-xss-from-visitors.html
999868	CVE-2019-2618	WebLogic Schwachstelle beim willkürlichen Hochladen	cve,2019-2618
999869	CVE-2019-11871	WEB-WORDPRESS WordPress Plug-in Benutzerdefinierte Field Suite vor 2.5.15 — Site-übergreifende Sicherheitsanfäl-ligkeit beim Scripting	cve,2019-11871

Regel	CVE	Beschreibung	Schwachstellen-Referenz
999870		WEB-WORDPRESS WordPress Live-Chat-Unterstützung Plug-in Persistentes Cross-Site Scripting Sicherheitslücke vor 8.0.27 über den wplc_custom_js-Parameter	https://blog.sucuri.net/2019/05/persistent-cross-site-scripting-in-wp-live-chat-support-plug-in.html
999871		WEB-WORDPRESS WordPress-Plug-In W3 Gesamt-Cache vor 0.9.7.4 — Schwachstelle bei der Ausführung von PHAR-Remotecode	https://wpvulndb.com/vulnerabilities/9270
999872		WEB-WORDPRESS WordPress-Plug-In W3 Gesamt-Cache vor 0.9.7.4 — Schwachstelle bei der Ausführung von PHAR-Remotecode	https://wpvulndb.com/vulnerabilities/9269
999873	CVE-2019-0604	WEB-MISC Microsoft Windows Sharepoint Server — Sicherheitsrisiko durch Remote-codeausführung	cve,2019-0604

Regel	CVE	Beschreibung	Schwachstellen-Referenz
999874		WEB-WORDPRESS Yuzo Related Posts Sicherheitsrisiko durch Cross-Site Scripting in 5.12.91	https://www.wordfence.com/blog/2019/04/yuzo-related-posts-zero-day-vulnerability-exploited-in-the-wild

Signaturupdate Version 34

January 25, 2022

Für die in Version 34 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 34 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999843		WEB-WORDPRESS WordPress Plug-in Ultimate Member vor Version 2.0.46 - Festlegen beliebiger Datei zum Lesen
999844		WEB-WORDPRESS WordPress Plug-in Ultimate Member vor Version 2.0.46 - Beliebige Datei gelesen
999845		WEB-WORDPRESS WordPress Plug-in Ultimatives Mitglied vor Version 2.0.46 - Dateientfernung durch Dateiersetzung
999846		WEB-WORDPRESS WordPress Plug-in Ultimatives Mitglied vor Version 2.0.46 - Datei entfernen
999847		WEB-WORDPRESS WordPress-Plug-in-Shortlinks vor 2.1.10 - CSV-Injection
999848		WEB-WORDPRESS WordPress-Plug-in-Shortlinks vor 2.1.10 — Sicherheitsanfälligkeit für nicht authentifizierte, Cross-Site Scripting
999849		WEB-WORDPRESS WordPress-Plug-in FV Flowplayer Video Player vor 7.3.13.727 — Sicherheitsrisiko durch gespeichertes Cross-Site Scripting

Regel zur Unterschrift	CVE-ID	Beschreibung
999850		WEB-WORDPRESS WordPress-Plug-In Einfache digitale Downloads vor 2.9.16 — Sicherheitsrisiko durch nicht authentifiziertes gespeichertes Cross-Site Scripting
999851		WEB-WORDPRESS WordPress Plug-in Crelly Slider Vor Version 1.3.5 — Schwachstelle durch Hochladen beliebiger Dateien
999853	CVE-2019-2615	WEB-MISC Sicherheitslücke bei der Offenlegung von Oracle WebLogic Serverinformationen
999854	CVE-2019-11872	WordPress-Plug-in-Hustle vor 6.0.8.1 - CSV-Injection-Schwachstelle
999855	CVE-2019-11231	WEB-MISC GetSimple CMS Version 3.3.15 und früher — Sicherheitsanfälligkeit beim Hochladen beliebiger Dateien
999856	CVE-2019-11231	WEB-MISC GetSimple CMS Version 3.3.15 und früher — Offenlegung von API-Schlüsselinformationen
999857		WEB-WORDPRESS WordPress-Plug-In WP-Datenbankbackup vor 5.2 - Befehlseinschleusungsanfälligkeit
999858		WEB-WORDPRESS WordPress Plug-in Slick Popup bis zu 1.7.1 — Sicherheitslücke bei Berechtigungseskalation

Regel zur Unterschrift	CVE-ID	Beschreibung
999859	CVE-2019-12099	WEB-MISC PHP Fusion CMS Sicherheitsanfälligkeit bezüglich Remotecodeausführung in Version 9.03.00 und früher

Signaturupdate Version 35

January 25, 2022

Für die in Version 35 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 35 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999834	CVE-2019-13024	WEB-MISC Centreon Version 19.04 und früher — Sicherheitsanfälligkeit durch Befehlseinschleusung

Regel zur Unterschrift	CVE-ID	Beschreibung
999835	CVE-2019-5420	WEB-MISC Rails-Entwicklungsmodus — Sicherheitslücke bei der Offenlegung geheimer
999836	CVE-2019-5418	WEB-MISC Rails-Aktionsansicht — Schwachstelle bei Offenlegung von Dateiinhalten
999837	CVE-2018-12426, CVE-2019-11185	WEB-WORDPRESS WP Live-Chat-Unterstützung Pro-Plug-In Vor 8.0.26 - Hochladen beliebiger Dateien
999838	CVE-2019-10270	WEB-WORDPRESS WordPress Plug-in Ultimate Member vor Version 2.0.40 - Zurücksetzen beliebiger Kennwörter
999839	CVE-2019-12826	WEB-WORDPRESS WordPress Plug-in-Widget-Logik vor 5.10.2 — CSRF-Sicherheitslücke
999840		WEB-WORDPRESS WordPress Plug-in All-in-One-Veranstaltungskalender vor 2.5.39 — Cross-Site Scripting-Sicherheitsanfälligkeit
999841	CVE-2019-11565	WEB-WORDPRESS WordPress-Plug-In Meinen Blog vor 1.6.7 drucken - Nicht authentifizierte SSRF-Sicherheitslücke

Regel zur Unterschrift	CVE-ID	Beschreibung
999842		WEB-WORDPRESS WordPress Plug-in Ultimatives Mitglied vor Version 2.0.46 - mehrere `cross-site scripting</LogString`

Signaturupdate Version 36

January 25, 2022

Für die in Version 36 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können die Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor sicherheitsgefährdeten Angriffen zu schützen.

Signaturversion

Die Signaturversion 36 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis**:
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999817		WEB-WORDPRESS WordPress Ad Inserter-Plug-In vor Version 2.4.22 — Remotecodeausführung

Regel zur Unterschrift	CVE-ID	Beschreibung
999818	CVE-2019-7839	WEB-MISC Adobe ColdFusion mehrere Versionen — Sicherheitsanfälligkeit bei Remotecodeausführung über HTTP/SOAP DotNet-to-Java (CVE-2019-7839)
999819	CVE-2019-7839	WEB-MISC Adobe ColdFusion mehrere Versionen — Sicherheitsanfälligkeit bei Remotecodeausführung über HTTP/SOAP Java-zu-DotNet (CVE-2019-7839)
999820	CVE-2019-11469	WEB-MISC Zoho ManageEngine Applications Manager vor 14 Build 14150 Erlaubt SQLi über resourceid-Parameter (CVE-2019-11469)
999821	CVE-2019-11448	WEB-MISC Zoho ManageEngine Application Manager 11.0 bis 14.0 — Nicht authentifizierte SQL-Injection (CVE-2019-11448)
999822	CVE-2019-1003000	WEB-MISC Jenkins Script Security Plug-in bis zu 1.49 — Sandbox-Bypass-Sicherheitsanfälligkeit (CVE-2019-1003000)
999823		WEB-WORDPRESS WordPress Cforms2 Plug-in bis zu 15.0.1 — Sicherheitsrisiko durch Einschleusen von nicht authentifiziertem HTML

Regel zur Unterschrift	CVE-ID	Beschreibung
999824	CVE-2019-0193	WEB-MISC Apache Solr vor 8.2 - Sicherheitsanfälligkeit bei DIH-Remote-Codeausführung über DataConfig-Parameter (CVE-2019-0193)
999825	CVE-2019-11580	WEB-MISC Atlassian Crowd Pdkinstall Entwicklungs-Plug-In aktiviert — nicht authentifiziertes RCE (CVE-2019-11580)
999826	CVE-2019-0192	WEB-MISC Apache Solr bis zu 5.5.5/6.6.5 — Sicherheitsanfälligkeit bei Remotecodeausführung in der Konfigurations-API (CVE-2019-0192)
999827		WEB-WORDPRESS WooCommerce-Variationsmuster-Plug-In Bis zu 1.0.61 - Reflektierte Site-übergreifende Sicherheitsanfälligkeit
999828	CVE-2019-1003001	WEB-MISC Jenkins Pipeline Groovy-Plug-in bis zu 2.61 - Sandbox-Bypass-Sicherheitsanfälligkeit durch Auftragserstellung (CVE-2019-1003001)
999829	CVE-2019-1003001	WEB-MISC Jenkins Pipeline Groovy-Plug-in bis zu 2.61 — Sandbox-Bypass-Sicherheitsanfälligkeit (CVE-2019-1003001)

Regel zur Unterschrift	CVE-ID	Beschreibung
999830		WEB-WORDPRESS WordPress Bold Page Builder-Plug-In vor 2.3.2 — Sicherheitslücke umgehen
999831	CVE-2019-15107	WEB-MISC Webmin vor 1.930 — Sicherheitsanfälligkeit bei Ausführung von nicht authentifiziertem Remotecode (CVE-2019-15107)
999832	CVE-2019-2767	WEB-MISC Oracle BI Publisher 11.1.1.9.0 und 12.2.1.4 — XXE-Schwachstelle (CVE-2019-2767)
999833	CVE-2019-15106	WEB-MISC Zoho ManageEngine OpManager bis 12.4x — Sicherheitslücke bei Umgehung der Authentifizierung (CVE-2019-15106)
999948	CVE-2014-0114	Apache Struts 1 bis 1.3.10 ermöglicht die Manipulation von ClassLoader und ermöglicht die Ausführung beliebigen Codes über HTTP_FORM_FIELD
999949	CVE-2013-4316	Apache Struts 2 vor 2.3.15.2 ermöglicht den Aufruf dynamischer Methoden durch Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit

Regel zur Unterschrift	CVE-ID	Beschreibung
999950	CVE-2013-4316	Apache Struts 2 vor 2.3.15.2 ermöglicht den Aufruf dynamischer Methoden durch Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit

> **Hinweis:**
>
> Die Signaturregel 999947 wurde aufgrund eines Leistungsproblems gelöscht.

Signaturupdate Version 37

January 25, 2022

Für die in Version 37 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 37 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999806	CVE-2019-3394	WEB-MISC Atlassian Confluence oder Rechenzentrum — Sicherheitsanfälligkeit bei der Offenlegung lokaler Dateien (CVE-2019-3394)
999807	CVE-2019-13569	WEB-WORDPRESS Icegram Plug-in für E-Mail-Abonnenten und Newsletter vor 4.1.8 - SQLi über ESFPX_Lists Param (CVE-2019-13569)
999808	CVE-2019-13569	WEB-WORDPRESS Icegram Plug-in für E-Mail-Abonnenten und Newsletter vor 4.1.8 - SQLi über Order Param (CVE-2019-13569)
999809	CVE-2019-2768	WEB-MISC Oracle BI Publisher — Vorhersehbare Sicherheitslücke in Sitzungstoken (CVE-2019-2768)
999810	CVE-2019-1003001	WEB-MISC Jenkins Pipeline Groovy-Plug-in bis zu 2.61 — Sandbox-Bypass-Sicherheitsanfälligkeit über Job-Update (CVE-2019-1003001)
999811	CVE-2019-13575	WEB-WORDPRESS WPEverest Everest Forms Plug-in vor 1.5.0 - SQL Injection (CVE-2019-13575)

Regel zur Unterschrift	CVE-ID	Beschreibung
999812	CVE-2019-15896	WEB-WORDPRESS LifterLMS-Plug-in bis zu 3.34.5 — Sicherheitslücke bei Umgehung der Sicherheit (CVE-2019-15896)
999813	CVE-2019-3396	WEB-MISC Atlassian Confluence oder Rechenzentrum — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2019-3396)
999814	CVE-2019-5475	WEB-MISC Sonatype Nexus Repository Manager vor 2.14.14 — Remotecodeausführung über den Createrepo-Pfad (CVE-2019-5475)
999815	CVE-2019-5475	WEB-MISC Sonatype Nexus Repository Manager vor 2.14.14 — Remotecodeausführung über Mergerepo-Pfad (CVE-2019-5475)
999816	CVE-2019-15104	WEB-MISC Zoho ManageEngine OpManager Version vor 12.4 — Sicherheitsanfälligkeit durch SQL Injection (CVE-2019-15104)

Signaturupdate Version 38

January 25, 2022

Für die in Version 38 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie kön-

nen diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 38 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999800	CVE-2019-12517	WEB-WORDPRESS SlickQuiz-Plug-In Version 1.3.7.1 und früher — Site-übergreifende Sicherheitsanfälligkeit beim Scripting (CVE-2019-12517)
999801	CVE-2019-10392	WEB-MISC Jenkins Git Client-Plug-In 2.8.4 und früher - Sicherheitsrisiko durch Einschleusen von Betriebssystembefehlen (CVE-2019-10392)
999802	CVE-2019-8371	WEB-MISC OpenEMR vor 5.0.2 - Sicherheitsanfälligkeit bei Remotecodeausführung über das Feld Form_Filedata (CVE-2019-8371)

Regel zur Unterschrift	CVE-ID	Beschreibung
999803	CVE-2019-8371	WEB-MISC OpenEMR vor 5.0.2 - Sicherheitsanfälligkeit bei Remotecodeausführung über das Feld Form_Image (CVE-2019-8371)
999804	CVE-2019-12516	WEB-WORDPRESS SlickQuiz-Plug-In Version 1.3.7.1 und früher — Sicherheitsrisiko durch SQL-Einschleusung (CVE-2019-12516)
999805	CVE-2019-1262	WEB-MISC Sicherheitsanfälligkeit in Microsoft SharePoint Server — Standortübergreifende Skripterstellung (CVE-2019-1262)

Signatur-Update für Dezember 2019

January 25, 2022

Für die in der Woche 2019-12-19 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 39 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die

> Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999760		WEB-MISC FusionPBX-Versionen vor 4.4.7 und 4.5.5 — Sicherheitslücke bei Remotecodeausführung über /app/exec/exec.php
999761	CVE-2019-12747	WEB-MISC Typo3 vor 8.7.27 und 9.5.8 — Deserialisierung nicht vertrauenswürdiger Daten (CVE-2019-12747)
999762	CVE-2019-13608	WEB-MISC Citrix StoreFront Server — Sicherheitsrisiko durch Einschleusung externer XML-Entitäten (CVE-2019-13608)
999763		WEB-WORDPRESS WordPress vor 5.2.4 - Nicht authentifizierte Ansicht von privaten oder entworfenen Beiträgen/Seiten Sicherheitslücke über FORM
999764		WEB-WORDPRESS WordPress vor 5.2.4 - Nicht authentifizierte Ansicht von privaten oder entworfenen Beiträgen/Seiten Sicherheitslücke über URL

Regel zur Unterschrift	CVE-ID	Beschreibung
999765	CVE-2019-15954	WEB-MISC Total.js CMS 12.0.0 — Sicherheitsanfälligkeit durch Widget-JavaScript-Codeeinschleusung über JSON (CVE-2019-15954)
999766	CVE-2019-15954	WEB-MISC Total.js CMS 12.0.0 — Sicherheitsanfälligkeit in Widget-JavaScript-Codeeinschleusung über FORM (CVE-2019-15954)
999767		Web-Wordpress SyntaxHighlighter Evolved Plug-in vor 5.3.1 — Cross-Site-Scripting Sicherheitsrisiko über Kommentare
999768		Web-WORDPRESS SyntaxHighlighter Evolved Plug-in vor 5.3.1 — Cross-Site-Scripting-Sicherheitsrisiko über POST
999769		WEB-WORDPRESS SyntaxHighlighter Evolved plug-in Prior To 5.3.1 - Cross-Site Scripting-Sicherheitsrisiko über JSON
999770	CVE-2019-16120	WEB-WORDPRESS Event Tickets plug-in Before 4.10.7.2 - CSV-Einschleusungssicherheitsrisiko (CVE-2019-16120)

Regel zur Unterschrift	CVE-ID	Beschreibung
999771	CVE-2019-15029	WEB-MISC FusionPBX vor 4.4.8 — Sicherheitsrisiko durch Remotecodeausführung (CVE-2019-15029)
999772		WEB-WORDPRESS Sassy Social Share-Plug-in vor 3.3.4 — Nicht authentifizierte Cross-Site-Scripting-Sicherheitsrisiko
999773		WEB-WORDPRESS Plug-in für E-Mail-Abonnenten und Newsletter Version 4.3.1 und früher — nicht authentifiziertes blindes SQLi-Sicherheitsrisiko
999774	CVE-2019-3398	WEB-MISC Atlassian Confluence oder Data Center - downloadallattachments Path Traversal Vulnerability (CVE-2019-3398)
999775	CVE-2019-15952	WEB-MISC Total.js CMS 12.0.0 — Sicherheitsrisiko durch Pfaddurchquerung in Seitenvorlagen (CVE-2019-15952)
999776	CVE-2019-17236	WEB-WORDPRESS IgniteUp Coming Soon und Maintenance Mode-Plug-in bis zu 3.4.0 - Gespeichertes Cross-Site Scripting (CVE-2019-17236)

Regel zur Unterschrift	CVE-ID	Beschreibung
999777	CVE-2019-10475	WEB-MISC Jenkins Build-Metrics Plug-in 1.3 — Reflektierte Cross-Site Scripting-Schwachstelle (CVE-2019-10475)
999778	CVE-2019-17132	WEB-MISC vBulletin vor 5.5.4 Patch-Ebene 2 — UpdateAvatar-API-Endpunkt-Schwachstelle bei Remotecodeausführung (CVE-2019-17132)
999779	CVE-2019-14994	WEB-MISC Atlassian Jira Service Desk — Schwachstelle durch Pfaddurchquerung (CVE-2019-14994)
999780	CVE-2019-19367	WEB-MISC FusionPBX 4.4.1 und früher — Standortübergreifende Scripting-Schwachstelle (CVE-2019-19367)
999781	CVE-2019-18668	WEB-WORDPRESS Currency Switcher-Plug-In vor 2.11.2 - Sicherheitsanfälligkeit durch Währungseinstellung umgehen über POST (CVE-2019-18668)
999782	CVE-2019-18668	WEB-WORDPRESS Currency Switcher-Plug-In vor 2.11.2 - Sicherheitslücke durch Währungseinstellung umgehen über GET (CVE-2019-18668)

Regel zur Unterschrift	CVE-ID	Beschreibung
999783	CVE-2019-16663	WEB-MISC RConfig 3.9.2 und früher - Sicherheitsanfälligkeit bei Remotecodeausführung über Search.crud.php (CVE-2019-16663)
999784		WEB-MISC Apache Solr Bis zu 8.3.0 - Nicht authentifizierte Remotecodeausführung über benutzerdefinierte VelocityResponseWriter-Vorlage
999785	CVE-2019-17235	WEB-WORDPRESS IgniteUp kommt bald und Wartungsmodus-Plug-in bis zu 3.4.0 - Offenlegung von Informationen über CSV (CVE-2019-17235)
999786	CVE-2019-17235	WEB-WORDPRESS IgniteUp kommt bald und Wartungsmodus-Plug-in bis zu 3.4.0 - Offenlegung von Informationen über Bcc (CVE-2019-17235)
999787	CVE-2019-12276	WEB-MISC GrandNode 4.40 - LetsEncryptController-Pfad-Traversal-Verwundbarkeit (CVE-2019-12276)
999788		WEB-WORDPRESS Plug-in für E-Mail-Abonnenten und Newsletter vor Version 4.2.3 — Offenlegung nicht authentifizierter Informationen

Regel zur Unterschrift	CVE-ID	Beschreibung
999789	CVE-2019-4013	WEB-MISC IBM BigFix Platform 9.5 — Authenticated Arbitry-Datei-Upload mit Root-Rechten (CVE-2019-4013)
999790	CVE-2019-11409	WEB-MISC FusionPBX Version 4.4.3 und früher — Remotecodeausführung über /app/basic_operator_panel/exec.php (CVE-2019-11409)
999791	CVE-2019-11409	WEB-MISC FusionPBX Version 4.4.3 und früher — Remotecodeausführung über /app/operator_panel/exec.php (CVE-2019-11409)
999792	CVE-2019-16662	WEB-MISC RConfig 3.9.2 und früher - Nicht authentifizierte Remotecodeausführung über AjaxServerSettingsChk.php (CVE-2019-16662)
999793	CVE-2019-7609	WEB-MISC Elastic Kibana vor 5.6.15 und 6.6.1 — Sicherheitsanfälligkeit durch Prototyp-Verschmutzung ermöglicht nicht authentifizierten RCE (CVE-2019-7609)
999794	CVE-2019-10092	WEB-MISC Apache-HTTP-Server bis zu 2.4.39 - mod_proxy Begrenztes Cross-Site-Scripting (CVE-2019-10092)

Regel zur Unterschrift	CVE-ID	Beschreibung
999795	CVE-2019-16520	WEB-WORDPRESS All-in-One-SEO-Pack-Plug-In vor 3.2.7 — Gespeicherte Cross-Site-Scripting-Schwachstelle (CVE-2019-16520
999796	CVE-2019-17234	WEB-WORDPRESS IgniteUp kommt bald und Wartungsmodus-Plug-in bis 3.4.0 - Beliebiges Löschen von Dateien (CVE-2019-17234)
999797	CVE-2019-16525	WEB-WORDPRESS-Checklisten-Plug-in vor Version 1.1.9 — Sicherheitsanfälligkeit für Cross-Site Scripting (CVE-2019-16525)
999798		Sicheres SVG-Plug-In für WEB-WORDPRESS vor 1.9.6 - Sicherheitslücke Cross-Site Scripting
999799		WEB-WORDPRESS Plug-in für E-Mail-Abonnenten und Newsletter vor Version 4.2.3 - Erstellung willkürlicher Optionen ohne Authentifizierung

Signaturupdate Version 40

January 25, 2022

Für die identifizierten Schwachstellen für die Woche 2020-01-14 werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen. Das Signatur-Update umfasst die Signatur-ID, die Signaturversion und

eine Liste der adressierten CVEs.

Signaturversion

Die Signaturversion 40 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Die Signaturaktualisierung Version 40 enthält einen Fix für die falsche Signaturregel 1861. Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999732	CVE-2019-1620	WEB-MISC Cisco Data Center Network Manager vor 11.2 (1) — Schwachstelle beim Hochladen beliebiger Dateien (CVE-2019-1620)
999733	CVE-2019-16702	WEB-MISC Integard Pro 2.2.0.9026 — NOJs-Pufferüberlauf-Sicherheitslücke (CVE-2019-16702)
999734	CVE-2019-1621	WEB-MISC Cisco Data Center Network Manager vor 11.2 (1) — Sicherheitsanfälligkeit beim Herunterladen beliebiger Dateien (CVE-2019-1621)

Regel zur Unterschrift	CVE-ID	Beschreibung
999735	CVE-2019-8451	WEB-MISC Atlassian Jira Server vor 8.4.0 — Sicherheitslücke bei serverseitigen Anforderungsfälschungen (CVE-2019-8451)
999736		WEB-WORDPRESS DSGVO-Plug-in zur Einhaltung von Cookies vor 4.0.3 - Sicherheitslücke beim Löschen authentifizierter
999737	CVE-2019-11287	WEB-MISC Pivotal RabbitMQ 3.7.x vor 3.7.21 und 3.8.x vor 3.8.1 — Denial-of-Service-Schwachstelle (CVE-2019-11287)
999738		WEB-WORDPRESS Ultimate Addons für Elementor vor 1.20.1 - Umgehung der Authentifizierung über Facebook-Anmeldeschwachstelle
999739		WEB-WORDPRESS Ultimate Addons für Elementor vor 1.20.1 - Umgehung der Authentifizierung über Google-Anmeldungsschwachstelle
999740	CVE-2019-19366	WEB-MISC FusionPBX vor 4.4.10 — Cross-Site Scripting-Schwachstelle in xml_cdr_search.php über Redirect-Parameter (CVE-2019-19366)

Regel zur Unterschrift	CVE-ID	Beschreibung
999741	CVE-2019-16931	WEB-WORDPRESS Visualizer-Plug-in vor Version 3.3.1 — Sicherheitsanfälligkeit durch nicht authentifizierte Cross-Site Scripting (CVE-2019-16931)
999742	CVE-2019-16932	WEB-WORDPRESS Visualizer-Plug-In vor Version 3.3.1 — nicht authentifizierte SSRF (CVE-2019-16932)
999743	CVE-2019-1619	WEB-MISC Cisco Data Center Network Manager vor 11.1 (1) — Sicherheitsanfälligkeit bei Umgehung der Authentifizierung (CVE-2019-1619)
999744	CVE-2019-12562	WEB-MISC DotNetNuke vor 9.4.0 — Sicherheitsrisiko durch Cross-Site Scripting (CVE-2019-12562)
999745	CVE-2019-8371	WEB-MISC OpenEMR vor 5.0.2 - Sicherheitsanfälligkeit bei Remotecodeausführung über das Feld Form_Filedata (CVE-2019-8371)
999746	CVE-2019-8371	WEB-MISC OpenEMR vor 5.0.2 - Sicherheitsanfälligkeit bei Remotecodeausführung über das Feld Form_Image (CVE-2019-8371)
999747		WEB-WORDPRESS Beaver Builder Ultimate Addons vor 1.24.1 — Umgehung der Authentifizierung über Facebook-Anmeldungsschwachstelle

Regel zur Unterschrift	CVE-ID	Beschreibung
999748		WEB-WORDPRESS Beaver Builder Ultimate Addons vor 1.24.1 — Umgehung der Authentifizierung über Google-Anmeldungsschwachstelle
999749	CVE-2019-19650	WEB-MISC Zoho ManageEngine AM vor dem Erstellen 13640 — SQLi über Agent-Servlet (CVE-2019-19650)
999750		WEB-MISC Zoho ManageEngine AM vor Build 13620 — Offenlegung von API-Schlüsseln über OPMRequestHandlerServlet Servlet
999751	CVE-2019-1622	WEB-MISC Cisco Data Center Network Manager 11.0 (1) — Schwachstelle bei der Offenlegung von Informationen (CVE-2019-1622)
999752	CVE-2019-16759	WEB-MISC vBulletin vor 5.5.4 Patch Level 1 — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2019-16759)
999753		Web-WORDPRESS vorgestelltes Bild vom URL-Plug-In vor 2.7.8 - Fehlende Zugriffskontrollen für die REST-API

Regel zur Unterschrift	CVE-ID	Beschreibung
999754	CVE-2019-10098	WEB-MISC Apache HTTP-Server bis zu 2.4.39 — mod_rewrite Sicherheitsanfälligkeit für selbstreferentielle Umleitung (CVE-2019-10098)
999755	CVE-2019-1936	WEB-MISC Cisco UCS Director 6.0 bis 6.6.1.0 und 6.7.0.0 bis 6.7.1.0 — Sicherheitsanfälligkeit bei der Befehlseinschleusung (CVE-2019-1936)
999756	CVE-2019-19649	WEB-MISC Zoho ManageEngine AM vor Build 13620 — nicht authentifiziertes SQLI über EventID-Parameter (CVE-2019-19649)
999757	CVE-2019-19649	WEB-MISC Zoho ManageEngine AM vor Build 13620 — nicht authentifiziertes SQLi über Entitätsparameter (CVE-2019-19649)
999758	CVE-2019-15036	WEB-MISC JetBrains TeamCity vor 2019.1 — Sicherheitsrisiko durch OS-Befehlseinschleusung (CVE-2019-15036)
999759	CVE-2019-17239	WEB-WORDPRESS Laden Sie Plug-Ins und Themes vom Dashboard-Plug-in bis zu 1.5 herunter - Sicherheitsrisiko durch Cross-Site Scripting (CVE-2019-17239)

Signaturupdate Version 41

January 25, 2022

Für die identifizierten Sicherheitsrisikos für die Woche 2020-02-04 werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen. Das Signatur-Update umfasst die Signatur-ID, die Signaturversion und eine Liste der adressierten CVEs.

Signaturversion

Die Signaturversion 41 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Die Signaturaktualisierung Version 41 enthält einen Fix für die falsche Signaturregel 1861.
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999717		WEB-WORDPRESS WordPress Version 5.3.x und früher — Denial-of-Service-Sicherheitsanfälligkeit über xmlrpc.php pingback.ping-Methode
999718		WEB-WORDPRESS-Backup und Staging durch das WP Time Capsule-Plug-In vor 1.21.16 — Authentifizierung-sumgehungsanfälligkeit

Regel zur Unterschrift	CVE-ID	Beschreibung
999719	CVE-2019-19731	WEB-MISC Roxy Fileman für .NET 1.4.5 - Verwundbarkeit durch Pfaddurchquerung über RENAMEFILE (CVE-2019-19731)
999720	CVE-2019-19915	WEB-WORDPRESS 301-Weiterleitungen - Einfaches Redirect Manager-Plug-in bis zu 2.4.0 - Mehrere Sicherheitslücken (CVE-2019-19915)
999721	CVE-2019-17662	WEB-MISC Cybele Software ThinVNC vor Version 1.0b1 — Sicherheitsanfälligkeit durch Verzeichnisdurchquerung (CVE-2019-17662)
999722	CVE-2020-6168	WEB-WORDPRESS Minimal kommt bald und Wartungsmodus-Plug-in vor 2.17 - Sicherheitsanfälligkeit durch Wartungseinstellungen (CVE-2020-6168)
999723	CVE-2020-6166	WEB-WORDPRESS Minimal kommt bald und Plug-in im Wartungsmodus vor 2.17 - Sicherheitsanfälligkeit für Themenänderungen (CVE-2020-6166)
999724	CVE-2020-6166	WEB-WORDPRESS Minimal kommt bald und Plug-in im Wartungsmodus vor 2.17 - Sicherheitsanfälligkeit für Exporteinstellungen (CVE-2020-6166)

Regel zur Unterschrift	CVE-ID	Beschreibung
999725		WEB-WORDPRESS IniFiniteWP Client-Plug-in vor 1.9.4.5 — Sicherheitsanfälligkeit durch Authentifizierung umgehen
999726	CVE-2019-16773	WEB-WORDPRESS WordPress-Versionen vor 5.3.1 — Cross-Site Scripting-Schwachstelle über REST-API mit JSON-Objekt (CVE-2019-16773)
999727	CVE-2019-16773	WEB-WORDPRESS WordPress-Versionen vor 5.3.1 — Cross-Site Scripting-Schwachstelle über REST-API mit FORMULARFELD (CVE-2019-16773)
999728	CVE-2019-16773	WEB-WORDPRESS WordPress-Versionen vor 5.3.1 — Cross-Site Scripting-Sicherheitsrisiko über user-edit.php (CVE-2019-16773)
999729	CVE-2019-16773	WEB-WORDPRESS WordPress-Versionen vor 5.3.1 — Cross-Site Scripting-Sicherheitsrisiko über profile.php (CVE-2019-16773)
999730	CVE-2019-16113	WEB-MISC Bludit 3.9.2 — Sicherheitsanfälligkeit für Remotecodeausführung beim Hochladen von Images über uuid (CVE-2019-16113)

Regel zur Unterschrift	CVE-ID	Beschreibung
999731	CVE-2019-16113	WEB-MISC Bludit 3.9.2 — Sicherheitsanfälligkeit für Remotecodeausführung beim Hochladen von Images über Dateinamen (CVE-2019-16113)

Aktualisierung der Unterschrift für Februar 2020

January 25, 2022

Für die in der Woche 2020-02-11 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 42 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999707		WEB-WORDPRESS wpCentral Plug-in vor Version 1.4.8 — Sicherheitslücke durch Privilege-Eskal

Regel zur Unterschrift	CVE-ID	Beschreibung
999708	CVE-2019-15979	WEB-MISC Cisco Data Center Network Manager vor 11.3 (1) — Sicherheitsanfälligkeit durch Befehlseinschleusung (CVE-2019-15979)
999709	CVE-2019-15978	WEB-MISC Cisco Data Center Network Manager vor 11.3 (1) — Sicherheitsanfälligkeit durch Befehlseinschleusung (CVE-2019-15978)
999710	CVE-2019-15975	WEB-MISC Cisco Data Center Network Manager vor 11.3 (1) — Sicherheitsanfälligkeit durch Umgehung der Authentifizierung (CVE-2019-15975)
999711	CVE-2019-15976	WEB-MISC Cisco Data Center Network Manager vor 11.3 (1) — Sicherheitsanfälligkeit bei Umgehung der Authentifizierung (CVE-2019-15976)
999712	CVE-2019-16405	WEB-MISC Centreon vor Version 19.10.2 — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2019-16405)
999713	CVE-2020-7048	WEB-WORDPRESS Plug-in zum Zurücksetzen der WP-Datenbank bis zu 3.1 - Sicherheitsanfälligkeit beim Zurücksetzen nicht authentifizierter Datenbanktabellen (CVE-2020-7048)

Regel zur Unterschrift	CVE-ID	Beschreibung
999714	CVE-2020-7108	WEB-WORDPRESS LearnDash-Plug-In vor Version 3.1.2 — Reflektierte Cross-Site Scripting-Schwachstelle (CVE-2020-7108)
999715	CVE-2019-15977	WEB-MISC Cisco Data Center Network Manager vor 11.3 (1) — Sicherheitsanfälligkeit bei Umgehung der Authentifizierung (CVE-2019-15977)
999716	CVE-2020-2096	WEB-MISC Jenkins Gitlab Hook Plug-In Version 1.4.2 und früher - Cross-Site Scripting-Schwachstelle (CVE-2020-2096)

Aktualisierung der Unterschrift für Februar 2020

January 25, 2022

Für die in der Woche 2020-02-27 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 43 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU

> auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999696	CVE-2019-15983	WEB-MISC Cisco Data Center Network Manager vor 11.3 (1) — XML-Sicherheitsanfälligkeit für externe Entitäten (CVE-2019-15983) über CablePlans
999697	CVE-2019-20197	WEB-MISC Nagios XI 5.6.9 — Authentifizierte Schwachstelle bei der Ausführung beliebiger Befehle (CVE-2019-20197)
999698	CVE-2020-8417	WEB-WORDPRESS-Codeausschnitte Plug-in vor 2.14.0 — CSRF-Sicherheitslücke (CVE-2020-8417)
999699		WEB-WORDPRESS wpCentral Plug-in vor Version 1.4.8 — Sicherheitslücke durch Privilege-Eskal
999700	CVE-2020-8596	WEB-WORDPRESS Participants Database-Plug-in vor 1.9.5.6 — Sicherheitsrisiko durch authentifizierte SQL-Einschleusung (CVE-2020-8596)

Regel zur Unterschrift	CVE-ID	Beschreibung
999701	CVE-2020-8426	WEB-WORDPRESS Elementor Page Builder-Plug-In vor 2.8.5 — Authentifizierte reflektierte Cross-Site-Scripting-Schwachstelle (CVE-2020-8426)
999702	CVE-2019-19509	WEB-MISC RConfig 3.9.3 - Sicherheitsanfälligkeit bei Remotecodeausführung über ajaxArchiveFiles.php (CVE-2019-19509)
999703	CVE-2019-8449	WEB-MISC Atlassian Jira Server vor 8.4.0 — Schwachstelle bei der Offenlegung von Informationen (CVE-2019-8449)
999704	CVE-2019-9194	WEB-MISC ElFinder vor 2.1.48 - Schwachstelle bei der Befehlseinschleusung durch PHP-Konnektoren (CVE-2019-9194)
999705	CVE-2019-15985	WEB-MISC Cisco Data Center Network Manager vor 11.3 (1) — SQL-Einschleusungssicherheitsrisiko (CVE-2019-15985) über GetVMHostData
999706	CVE-2020-8549	WEB-WORDPRESS Plug-in Strong Testimonials vor 2.40.1 - Sicherheitsrisiko durch Cross-Site Scripting (CVE-2020-8549)

Signaturaktualisierung für April 2020

January 25, 2022

Für die in der Woche 2020-04-27 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 44 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999683	CVE-2020-9043	WEB-WORDPRESS WPCentral Plug-in vor 1.5.1 — Sicherheitsanfälligkeit bei der Offenlegung von Verbindungsschlüsseln (CVE-2020-9043)
999684		WEB-WORDPRESS Plug-in “Doppelte Post” Version 3.2.3 und früher - Persistentes Site-übergreifendes
999685		WEB-WORDPRESS Plug-in “Doppelte Post” Version 3.2.3 und früher - Persistentes Site-übergreifendes

Regel zur Unterschrift	CVE-ID	Beschreibung
999686	CVE-2020-0618	WEB-MISC Microsoft SQL Server Reporting Services — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2020-0618)
999687	CVE-2019-16278	WEB-MISC Nostromo Nhttpd vor 1.3.7 - Strcutl-Funktion ermöglicht nicht authentifizierte Remotecodeausführung (CVE-2019-16278)
999688	CVE-2019-1937	WEB-MISC Cisco UCS Director 6.6.0.0 bis 6.6.1.0 und 6.7.0.0 bis 6.7.1.0 — Sicherheitsanfälligkeit durch Authentifizierung umgehen (CVE-2019-1937)
999689		WEB-WORDPRESS Plug-in “Doppelte Post” Version 3.2.3 und früher - Persistentes Site-übergreifendes
999690	CVE-2020-9006	WEB-WORDPRESS Popup Builder-Plug-In vor 3.0 - SQL-Injection über PHP-Deserialisierungsschwachstelle (CVE-2020-9006)
999691		WEB-WORDPRESS Plug-in “Doppelte Post” Version 3.2.3 und früher - Persistentes Site-übergreifendes
999692		WEB-MISC verhindert das Schmuggeln von Anfragen über Inhaltslänge und Transfer-Codierungs-Header

Regel zur Unterschrift	CVE-ID	Beschreibung
999693		WEB-WORDPRESS ThemeGrill-Demo-Importer-Plug-In vor 1.6.3 — Umgehung der Authentifizierung und Sicherheitsanfälligkeit
999694	CVE-2019-17237	WEB-WORDPRESS IgniteUp kommt bald und Wartungsmodus-Plug-in vor 3.4.1 - CSRF-Sicherheitslücke per Nachricht (CVE-2019-17237)
999695	CVE-2019-17237	WEB-WORDPRESS IgniteUp kommt bald und Wartungsmodus-Plug-in vor 3.4.1 - CSRF-Sicherheitslücke über Betreff (CVE-2019-17237)

Signatur-Update für Mai 2020

January 25, 2022

Für die in der Woche 2020-05-26 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 45 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC Laut der neuesten Snort-Version wurden die Signaturregeln mit der ID 1258, 1306, 2520,

> 2661, 5695, 10996, 11817, 12056, 15471, 17049 und 21634 entfernt.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999666		WEB-WORDPRESS Duplicator-Plug-In vor 1.3.28 — Sicherheitsanfälligkeit beim Herunterladen willkürlicher Dateien ohne Authentifizierung
999667	CVE-2020-10220	WEB-MISC RConfig bis 3.94 — Sicherheitsanfälligkeit durch SQL-Injection (CVE-2020-10220)
999668	CVE-2020-5844	WEB-MISC Artica Pandora FMS 7.0 - Ausführung beliebiger Dateien gefährlichen Typs über /attachment/files_repo/ (CVE-2020-5844)
999669	CVE-2020-8813	WEB-MISC-Kakteen vor 1.2.10 — Sicherheitsanfälligkeit bei Remotecodeausführung über graph_realtime.php (CVE-2020-8813)
999670	CVE-2020-8654	WEB-MISC EyesOfNetwork 5.3 — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2020-8654)

Regel zur Unterschrift	CVE-ID	Beschreibung
999671	CVE-2020-10196	WEB-WORDPRESS Sygnoos Popup Builder-Plug-in vor 3.64.1 — Sicherheitsanfälligkeit für nicht authentifiziertes Cross-Site Scripting (CVE-2020-10196)
999672	CVE-2019-15949	WEB-MISC Nagios XI vor 5.6.6 — Remotecodeausführung als Root-Schwachstelle (CVE-2019-15949)
999673	CVE-2020-10879	WEB-MISC RConfig 3.9.5 und früher — Sicherheitsanfälligkeit bei Remotecodeausführung über search.crud.php (CVE-2020-10879)
999674	CVE-2020-8656	WEB-MISC EyesOfNetwork 5.3 - EyesOfNetwork API 2.4.2 Sicherheitsrisiko durch SQL-Einschleusung (CVE-2020-8656)
999675	CVE-2020-10195	WEB-WORDPRESS Sygnoos Popup Builder-Plug-In vor 3.64.1 — Offenlegung authentifizierter Systeminformationen (CVE-2020-10195)
999676	CVE-2020-10195	WEB-WORDPRESS Sygnoos Popup Builder-Plug-In vor 3.64.1 — Offenlegung authentifizierter Abonnenteninformationen (CVE-2020-10195)

Regel zur Unterschrift	CVE-ID	Beschreibung
999677	CVE-2020-10195	WEB-WORDPRESS Sygnoos Popup Builder-Plug-In vor 3.64.1 - Änderung authentifizierter Einstellungen (CVE-2020-10195)
999678	CVE-2020-0646	Microsoft SharePoint Server — .NET-Framework-Workflow-Schwachstelle Remotecodeausführung über SOAP 1.2 (CVE-2020-0646
999679	CVE-2020-0646	Microsoft SharePoint Server — .NET-Framework-Workflow-Schwachstelle Remotecodeausführung über SOAP 1.1 (CVE-2020-0646
999680	CVE-2020-10221	WEB-MISC RConfig bis 3.94 — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2020-10221)
999681	CVE-2019-19134	WEB-WORDPRESS Hero Maps Premium vor 2.2.3 — Nicht authentifizierte reflektierte Sicherheitsanfälligkeit für Cross-Site Scripting (CVE-2019-19134)
999682	CVE-2020-10385	WEB-WORDPRESS WPForms-Plug-In vor 1.5.9 - Sicherheitsrisiko durch Cross-Site Scripting (CVE-2020-10385)

Signaturaktualisierung für Juni 2020

January 25, 2022

Für die in der Woche 2020-06-03 identifizierten Sicherheitsrisikos werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 46 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999643		WEB-WORDPRESS 10Web Map Builder für Google Maps Plug-in vor 10.0.64 — Nicht authentifizierte Cross-Site-Scripting-Schwachstelle über die Seite gmwd_setup
999644		WEB-WORDPRESS 10Web Map Builder für Google Maps Plug-in 10.0.64 und früher — Cross-Site Scripting-Sicherheitsrisiko über options_gmwd Seite

Regel zur Unterschrift	CVE-ID	Beschreibung
999645	CVE-2020-5187	WEB-MISC DNN bis zu 9.4.4 — Sicherheitsanfälligkeit durch Pfaddurchquerung über URL (CVE-2020-5187)
999646	CVE-2020-5187	WEB-MISC DNN bis zu 9.4.4 — Sicherheitsanfälligkeit durch Pfaddurchquerung über Lokal (CVE-2020-5187)
999647	CVE-2020-9335	WEB-WORDPRESS-Fotogalerie-Plug-In vor 1.5.46 - Cross-Site Scripting-Sicherheitsrisiko durch das Feld image_alt_text_ (CVE-2020-9335)
999648	CVE-2020-9335	WEB-WORDPRESS-Fotogalerie-Plug-In vor 1.5.46 — Cross-Site Scripting-Sicherheitsrisiko über Namensfeld (CVE-2020-9335)
999649	CVE-2020-9335	WEB-WORDPRESS-Fotogalerie-Plug-In vor 1.5.46 — Cross-Site Scripting-Sicherheitsrisiko über Beschreibungsfelder (CVE-2020-9335)
999650	CVE-2020-10189	WEB-MISC Zoho ManageEngine Desktop Central vor 10.0.479 — Fehler zur Ausführung von nicht authentifiziertem Remotecode (CVE-2020-10189)

Regel zur Unterschrift	CVE-ID	Beschreibung
999651	CVE-2020-10189	WEB-MISC Zoho ManageEngine Desktop Central vor 10.0.479 — Fehler zum Hochladen beliebiger Dateien ohne Authentifizierung (CVE-2020-10189)
999652		WEB-WORDPRESS Flexible Checkout-Felder für das WooCommerce-Plug-in vor 2.3.2 - Änderung nicht authentifizierter Einstellungen
999653	CVE-2020-0688	WEB-MISC Microsoft Exchange Server — Schlüsselanfälligkeit bei der Ausführung von Remotecode bei der Validierung (CVE-2020-0688)
999654	CVE-2020-8947, CVE-2019-20224	WEB-MISC Artica Pandora FMS 7.0 - Sicherheitsanfälligkeit bei Remotecodeausführung über den ip_src-Parameter (CVE-2020-8947, CVE-2019-20224)
999655	CVE-2020-8947, CVE-2019-20224	WEB-MISC Artica Pandora FMS 7.0 - Sicherheitsanfälligkeit bei Remotecodeausführung über den dst_port-Parameter (CVE-2020-8947, CVE-2019-20224)

Regel zur Unterschrift	CVE-ID	Beschreibung
999656	CVE-2020-8947, CVE-2019-20224	WEB-MISC Artica Pandora FMS 7.0 - Sicherheitsanfälligkeit bei Remotecodeausführung über den src_port-Parameter (CVE-2020-8947, CVE-2019-20224)
999657	CVE-2020-8947, CVE-2019-20224	WEB-MISC Artica Pandora FMS 7.0 - Sicherheitsanfälligkeit bei Remotecodeausführung über den ip_dst-Parameter (CVE-2020-8947, CVE-2019-20224)
999658	CVE-2020-5186	WEB-MISC DNN bis zu 9.5.0 — Standortübergreifende Scripting-Schwachstelle durch Journal XML-Upload (CVE-2020-5186)
999659		WEB-WORDPRESS WP Sitemap-Seiten-Plug-in 1.6.2 und früher — Cross-Site Scripting-Schwachstelle über wsp_exclude_pages
999660	CVE-2020-5188	WEB-MISC DNN bis zu 9.5.0 — Sicherheitslücke bei unsicheren Berechtigungen über UploadFromUrl (CVE-2020-5188)
999661	CVE-2020-5188	WEB-MISC DNN bis zu 9.5.0 — Sicherheitslücke bei unsicheren Berechtigungen über UploadFromLocal (CVE-2020-5188)

Regel zur Unterschrift	CVE-ID	Beschreibung
999662	CVE-2020-7799	WEB-MISC FusionAuth vor 1.11.0 — Sicherheitsanfälligkeit bei Remotecodeausführung über API-Thema (CVE-2020-7799)
999663	CVE-2020-7799	WEB-MISC FusionAuth vor 1.11.0 — Sicherheitsanfälligkeit bei Remotecodeausführung über API-E-Mail-Vorlage (CVE-2020-7799)
999664	CVE-2020-7799	WEB-MISC FusionAuth vor 1.11.0 — Sicherheitsanfälligkeit bei Remotecodeausführung über GUI-Thema (CVE-2020-7799)
999665	CVE-2020-7799	WEB-MISC FusionAuth vor 1.11.0 — Sicherheitsanfälligkeit bei Remotecodeausführung über GUI-E-Mail-Vorlage (CVE-2020-7799)

Signaturaktualisierung für Juni 2020

January 25, 2022

Für die in der Woche 2020-06-12 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 47 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999580	CVE-2020-6010	WEB-WORDPRESS LearnPress LMS-Plug-In vor 3.2.6.9 — Sicherheitsanfälligkeit durch SQL-Injection (CVE-2020-6010)
999581		WEB-MISC Nagios XI bis 5.6.13 — Sicherheitsanfälligkeit bei Ausführung beliebiger Befehle im Dienst Command_Test
999582	CVE-2020-0932	Microsoft SharePoint Server - WebPart-Quellmarkup Remotecodeausführung Sicherheitsanfälligkeit über SOAP 1.2 (CVE-2020-0932)
999583	CVE-2020-0932	Microsoft SharePoint Server - WebPart-Quellmarkup Remotecodeausführung Sicherheitsanfälligkeit über SOAP 1.1 (CVE-2020-0932)
999584	CVE-2020-12642	WEB-WORDPRESS Ninja Forms Plug-in vor 3.4.24.2 - Standortübergreifende Anforderungsfälschung durch Importfelder (CVE-2020-12642)

Regel zur Unterschrift	CVE-ID	Beschreibung
999585	CVE-2020-12642	WEB-WORDPRESS Ninja Forms Plug-in vor 3.4.24.2 — Standortübergreifende Anforderungsfälschung durch Importformular (CVE-2020-12642)
999586	CVE-2020-11450	WEB-MISC Microstrategy Web 10.4 — Schwachstelle bei der Offenlegung von Informationen (CVE-2020-11450)
999587	CVE-2020-7935	WEB-MISC Artica Pandora FMS 7.0 - Uneingeschränktes Hochladen von Dateien mit gefährlicher Sicherheitsanfälligkeit ermöglicht RCE (CVE-2020-7935)
999588	CVE-2020-12116	WEB-MISC Zoho ManageEngine OpManager vor Build 125125 — Sicherheitsanfälligkeit bei der Offenlegung von Informationen (CVE-2020-12116)
999589		WEB-WORDPRESS Elementor Page Builder vor 2.9.6 — Sicherheitslücke durch Privilegieneskal
999590	CVE-2020-11738	WEB-WORDPRESS — Snap Creek Duplicator Plug-in vor 1.3.28 — Sicherheitsanfälligkeit durch Pfaddurchquerung (CVE-2020-11738)

Regel zur Unterschrift	CVE-ID	Beschreibung
999591	CVE-2020-10389	WEB-MISC Chadha PHPKB Standard Mehrsprachig 9 - Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2020-10389)
999592	CVE-2020-11516	WEB-WORDPRESS-Kontaktformular 7 Datepicker-Plug-in bis zu 2.6.0 - Sicherheitsanfälligkeit für Cross-Site Scripting (CVE-2020-11516)
999593		WEB-MISC Nagios XI bis 5.6.13 — Export-RRD-Anfälligkeit bei der Ausführung beliebiger Befehle über Schritt
999594		WEB-MISC Nagios XI bis 5.6.13 — Export-RRD-Schwachstelle bei der Ausführung beliebiger Befehle über End
999595		WEB-MISC Nagios XI bis 5.6.13 — Export-RRD-Schwachstelle bei der Ausführung beliebiger Befehle über Start
999596	CVE-2019-19799	Zoho ManageEngine Applications Manager Vor 14600 — Sicherheitsrisiko durch Offenlegung von Informationen (CVE-2019-19799)
999597	CVE-2020-10458	WEB-MISC Chadha PHPKB Standard Mehrsprachig 9 - Sicherheitsrisiko durch Löschen beliebiger Ordner (CVE-2020-10458)

Regel zur Unterschrift	CVE-ID	Beschreibung
999598	CVE-2017-9822	WEB-MISC DNN vor 9.1.1 — Sicherheitsrisiko durch Remotecodeausführung über DNNPersonalization-Cookie (CVE-2017-9822)
999599	CVE-2020-7953	WEB-MISC OpServices OpMon 9.3.2 — Sicherheitsanfälligkeit durch Offenlegung nicht authentifizierter Informationen über nmap_options Param (CVE-2020-7953)
999600	CVE-2020-7953	WEB-MISC OpServices OpMon 9.3.2 — Sicherheitsanfälligkeit bei der Offenlegung nicht authentifizierter Informationen über Host Param (CVE-2020-7953)
999601		WEB-MISC Bolt CMS 3.7.0 - Datei umbenennen in eine Sicherheitslücke des gefährlichen Typs über newname Parameter
999602		WEB-MISC Bolt CMS 3.7.0 — Schwachstelle durch Pfaddurchquerung über newname Parameter
999603		WEB-MISC Bolt CMS 3.7.0 — Sicherheitsanfälligkeit durch Pfaddurchquerung über Oldname-Parameter

Regel zur Unterschrift	CVE-ID	Beschreibung
999604		WEB-MISC Bolt CMS 3.7.0 — Schwachstelle durch Pfaddurchquerung über übergeordneten Parameter
999605		WEB-MISC Bolt CMS 3.7.0 - Unsachgemäße Sicherheitslücke bei der Feldvalidierung im displayname
999606	CVE-2020-9004	WEB-MISC — Wowza Streaming Engine 4.7.8 — Inkorrekte Autorisierungsschwachstelle in View-Protokollen (CVE-2020-9004)
999607	CVE-2020-9004	WEB-MISC — Wowza Streaming Engine 4.7.8 — Inkorrekte Autorisierungsschwachstelle in Medien-Cache-Einstellungen (CVE-2020-9004)
999608	CVE-2020-9004	WEB-MISC — Wowza Streaming Engine 4.7.8 — Falsche Autorisierungsschwachstelle in Anwendungseinstellungen (CVE-2020-9004)
999609	CVE-2020-9004	WEB-MISC — Wowza Streaming Engine 4.7.8 — Falsche Autorisierungsschwachstelle in Servereinstellungen (CVE-2020-9004)

Regel zur Unterschrift	CVE-ID	Beschreibung
999610		WEB-MISC PrestaShop 1.7.6.5 - CSRF-Sicherheitslücke über Filemanager
999611	CVE-2020-10238	WEB-MISC Joomla! Zurück zu 3.9.16 — Sicherheitslücke durch Umgehung der Sicherheit via com_templates (CVE-2020-10238)
999612	CVE-2020-11510	WEB-WORDPRESS LearnPress LMS-Plug-In vor 3.2.6.9 - Berechtigungseskalation über learnpress_create_page (CVE-2020-11510)
999613	CVE-2020-11510	WEB-WORDPRESS LearnPress LMS-Plug-In vor 3.2.6.9 - Berechtigungseskalation über learn-press_update_order_status (CVE-2020-11510)
999614	CVE-2020-8636	WEB-MISC OpServices OpMon 9.3.2 — Sicherheitsanfälligkeit bei nicht authentifizierter Remotecodeausführung über den Parameter nmap_options (CVE-2020-8636)
999615	CVE-2020-8636	WEB-MISC OpServices OpMon 9.3.2 — Sicherheitsanfälligkeit bei der Remotecodeausführung über Host-Parameter (CVE-2020-8636)

Regel zur Unterschrift	CVE-ID	Beschreibung
999616	CVE-2020-11511	WEB-WORDPRESS LearnPress LMS-Plug-In vor 3.2.6.9 - Berechtigungseskalation über Akzeptieren zum Lehrer (CVE-2020-11511)
999617	CVE-2020-11451	WEB-MISC Microstrategy Web — Sicherheitsanfälligkeit beim Hochladen von Dateitypen über JSP (CVE-2020-11451)
999618	CVE-2020-11451	WEB-MISC Microstrategy Web — Sicherheitslücke beim Hochladen von Dateitypen über ASP (CVE-2020-11451)
999619	CVE-2020-11515	WEB-WORDPRESS WP SEO-Plug-In Rang Mathematik vor 1.0.41 - Sicherheitsanfälligkeit bei Umleitung über REST-API über URL (CVE-2020-11515)
999620	CVE-2020-11515	WEB-WORDPRESS WP SEO-Plug-In Rang Mathematik vor 1.0.41 - Sicherheitsanfälligkeit bei Umleitung über REST-API rest_route Param (CVE-2020-11515)
999621	CVE-2020-10457	WEB-MISC Chadha PHPKB Standard mehrsprachig 9 - Schwachstelle beim Umbenennen beliebiger Dateien über ImgName (CVE-2020-10457)

Regel zur Unterschrift	CVE-ID	Beschreibung
999622	CVE-2020-10457	WEB-MISC Chadha PHPKB Standard mehrsprachig 9 - Schwachstelle beim Umbenennen beliebiger Dateien über imgURL (CVE-2020-10457)
999623	CVE-2019-1821	WEB-MISC Cisco Prime Infrastructure — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2019-1821)
999624		WEB-WORDPRESS Page Builder-Plug-In vor 2.10.16 — CSRF-Sicherheitslücke über Ajax action_builder_content
999625		WEB-WORDPRESS Page Builder-Plug-In vor 2.10.16 — CSRF-Sicherheitslücke über Live-Editor
999626	CVE-2020-11514	WEB-WORDPRESS WP SEO-Plug-In Rang Mathematik vor 1.0.41 - Berechtigungseskalation über REST-API über URL (CVE-2020-11514)
999627	CVE-2020-11514	WEB-WORDPRESS WP SEO-Plug-In Rang Mathematik vor 1.0.41 - Privilegien-Eskalation über REST-API rest_route Param (CVE-2020-11514)
999628	CVE-2019-6713	WEB-MISC ThinkCMF vor 5.0.190312 - Sicherheitsrisiko durch Code-Einschleusung über /route/editpost.html (CVE-2019-6713)

Regel zur Unterschrift	CVE-ID	Beschreibung
999629	CVE-2019-6713	WEB-MISC ThinkCMF vor 5.0.190312 - Sicherheitsrisiko durch Code-Einschleusung über /route/addpost.html (CVE-2019-6713)
999630		WEB-WORDPRESS Google Site Kit-Plug-In vor 1.8.0 — Sicherheitslücke bei ungeschützter Überprüfung
999631	CVE-2020-9315	WEB-MISC Oracle iPlanet Web Server 7.0.x — Inkorrekte Sicherheitsanfälligkeit bei der Zugriffskontrolle (CVE-2020-9315)
999632	CVE-2020-1947	WEB-MISC Apache ShardingSphere 4.0.0-RC3 und 4.0.0 — SnakeYAML Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2020-1947)
999633	CVE-2020-7961	Liferay Portal vor 7.2.1 CE GA2 - RCE-Schwachstelle durch JSONWS-Deserialisierung über JSON-RPC (CVE-2020-7961)
999634	CVE-2020-7961	Liferay Portal vor 7.2.1 CE GA2 - JSONWS Deserialisierung RCE-Schwachstelle über URL-Pfad (CVE-2020-7961)
999635	CVE-2020-7961	Liferay Portal vor 7.2.1 CE GA2 - RCE-Schwachstelle bei JSONWS-Deserialisierung über Formular- und URI-Abfrage (CVE-2020-7961)

Regel zur Unterschrift	CVE-ID	Beschreibung
999636	CVE-2020-8518	WEB-MISC Horde Groupware Webmail Edition 5.2.22 — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2020-8518)
999637	CVE-2020-7351	WEB-MISC Fonality Trixbox CE 2.8.0.4 und früher — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2020-7351)
999638	CVE-2020-12720	WEB-MISC vBulletin vor 5.6.1 Patch Level 1 — Sicherheitsrisiko durch nicht authentifizierte SQL-Einschleusung (CVE-2020-12720)
999639	CVE-2019-19800	Zoho ManageEngine Applications Manager Vor 14520 — Path Traversal Vulnerability (CVE-2019-19800)
999640	CVE-2020-10386	WEB-MISC Chadha PHPKB Standard mehrsprachig 9 - Remotecodeausführung (CVE-2020-10386)
999641	CVE-2020-8497	WEB-MISC Artica Pandora FMS 7.0 — Sicherheitsanfälligkeit bei der Offenlegung nicht authentifizierter Informationen (CVE-2020-8497)

Regel zur Unterschrift	CVE-ID	Beschreibung
999642	CVE-2020-6009	WEB-WORDPRESS LearnDash LMS-Plug-In vor 3.1.6 — Sicherheitsrisiko durch nicht authentifizierte SQL-Einschleusung (CVE-2020-6009)

Signaturaktualisierung für Juli 2020

January 25, 2022

Für die in der Woche 2020-07-01 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 48 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999563		WEB-WORDPRESS Page Builder PageLayer-Plug-in vor 1.1.2 — Cross-Site Scripting-Sicherheitsrisiko über pagelayer_cf_to_email

Regel zur Unterschrift	CVE-ID	Beschreibung
999564		WEB-WORDPRESS Page Builder PageLayer-Plug-In Vor 1.1.2 - Cross-Site Scripting-Sicherheitsrisiko über pagelay
999565		WEB-WORDPRESS Page Builder PageLayer-Plug-In Vor 1.1.2 — Cross-Site Scripting-Sicherheitsrisiko über Seitenlayer
999566	CVE-2020-1961	WEB-MISC Apache-Synkope — Sicherheitsrisiko durch serverseitiger Template-Einschleusung (CVE-2020-1961)
999567	CVE-2019-18935	WEB-MISC Fortschritt Telerik UI für ASP.NET AJAX - RadAsyncUpload.NET-Deserialisierungsschwachstelle (CVE-2019-18935)
999568	CVE-2020-9463	WEB-MISC Centreon 19.10 — Sicherheitsrisiko durch OS-Befehlseinschleusung (CVE-2020-9463)
999569		Plug-In zur Überprüfung der WEB-WORDPRESS-Support vor 3.7.6 — Sicherheitsanfälligkeit für gespeichertes Cross-Site-Scripting
999570		WEB-WORDPRESS Page Builder PageLayer-Plug-In vor 1.1.2 - Unsachgemäße Zugriffskontrolle Vuln Über pagelayer_save_template

Regel zur Unterschrift	CVE-ID	Beschreibung
999571		WEB-WORDPRESS Page Builder PageLayer-Plug-In vor 1.1.2 - Unsachgemäße Zugriffskontrolle Vuln Über pagelayer_update_site_title
999572		WEB-WORDPRESS Page Builder PageLayer-Plug-In vor 1.1.2 - Unsachgemäße Zugriffskontrolle Vuln Über pagelayer_save_content
999573		WEB-WORDPRESS Drag & Drop-Upload für Kontaktformular 7 vor 1.3.3.3 — Sicherheitsanfälligkeit beim Hochladen beliebiger Dateierweiterungen
999574	CVE-2020-9314	WEB-MISC Oracle iPlanet Web Server 7.0.x — Sicherheitsrisiko durch Image-Einschleusung (CVE-2020-9314)
999575	CVE-2020-9484	WEB-MISC Apache Tomcat mehrere Versionen - Deserialisierung nicht vertrauenswürdiger Daten (CVE-2020-9484)
999576	CVE-2020-13252	WEB-MISC Centreon Vor 19.04.15 — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2020-13252)
999577	CVE-2020-11453	WEB-MISC Microstrategy Web - CSRF-Sicherheitslücke über SOAP (CVE-2020-11453)

Regel zur Unterschrift	CVE-ID	Beschreibung
999578	CVE-2020-11453	WEB-MISC Microstrategy Web — CSRF-Sicherheitslücke (CVE-2020-11453)
999579	CVE-2020-7237	WEB-MISC Cacti vor 1.2.8 — Sicherheitsanfälligkeit bezüglich Remotecodeausführung (CVE-2020-7237)

Signatur-Update für August 2020

January 25, 2022

Für die in der Woche 2020-08-26 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 49 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999556	CVE-2020-13241	WEB-MISC Microweber 1.1.18 — Uneingeschränktes Hochladen von Dateien mit Sicherheitslücke durch gefährliche Typen (CVE-2020-13241)
999557	CVE-2020-3250	WEB-MISC Cisco UCS Director - REST-API-Pfad-Traversal-Verwundbarkeit über UserAPIDownloadFile (CVE-2020-3250)
999558		WEB-WORDPRESS PageBuilder KingComposer Plug-in vor 2.9.4 - Beliebiges Löschen von Verzeichnissen per action=bulk-delete
999559		WEB-WORDPRESS PageBuilder KingComposer Plug-in vor 2.9.4 - Sicherheitsanfälligkeit bei Remotecodeausführung über
999560	CVE-2018-1999024	WEB-MISC Moodle - MathJax Unicode-Schwachstelle für Cross-Site Scripting (CVE-2018-1999024)
999561	CVE-2020-13693	WEB-WORDPRESS bbPress-Plug-In vor 2.6.5 — Sicherheitsanfälligkeit für nicht authentifizierte Berechtigungseskalation (CVE-2020-13693)

Regel zur Unterschrift	CVE-ID	Beschreibung
999562	CVE-2020-12847	WEB-MISC Pydio-Zellen vor 2.0.7 - Sicherheitsanfälligkeit bei der Remotecodeausführung (CVE-2020-12847)

Signatur-Update für September 2020

January 25, 2022

Für die in der Woche 2020-09-26 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 50 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999532	CVE-2020-1956	WEB-MISC Apache Kylin - Würfel migrieren Remote-Code-Ausführung über dest-config (CVE-2020-1956)

Regel zur Unterschrift	CVE-ID	Beschreibung
999533	CVE-2020-1956	WEB-MISC Apache Kylin - Cube migrieren Remote-Code-Ausführung über src-config (CVE-2020-1956)
999534	CVE-2020-1956	WEB-MISC Apache Kylin - Cube migrieren Remote-Code-Ausführung über ProjectName (CVE-2020-1956)
999535	CVE-2020-3247	WEB-MISC Cisco UCS Director - CopyFileRunnable willkürliche Symlink-Erstellungsschwachstelle (CVE-2020-3247)
999536	CVE-2019-16872	WEB-MISC-Portainer vor 1.22.1 — Inkorrekte Sicherheitslücke bei der Zugriffskontrolle über Update-Stacks (CVE-2019-16872)
999537	CVE-2019-16872	WEB-MISC-Portainer vor 1.22.1 — Inkorrekte Sicherheitslücke bei der Zugriffskontrolle durch Erstellen von Stacks (CVE-2019-16872)
999538	CVE-2020-13855	WEB-MISC Artica Pandora FMS 7.44 - Schwachstelle beim Hochladen beliebiger Dateien über den Datei-Repository-Manager (CVE-2020-13855)
999539	CVE-2020-5902	WEB-MISC F5 BIG-IP - Verkehrsmanagement-Benutzerschnittstelle RCE-Schwachstelle über /hsqldb (CVE-2020-5902)

Regel zur Unterschrift	CVE-ID	Beschreibung
999540	CVE-2020-5902	WEB-MISC F5 BIG-IP - Verkehrsmanagement-Benutzerschnittstelle RCE-Schwachstelle über /tmui (CVE-2020-5902)
999541		WEB-MISC WebERP 4.15.1 und früher — Sicherheitsanfälligkeit bei der Offenlegung nicht authentifizierter Informationen
999542	CVE-2020-7209	WEB-MISC HP LinuxKI vor 6.0-2 - Nicht authentifizierte RCE-Schwachstelle über timeline.php und Zeitstempel Param (CVE-2020-7209)
999543	CVE-2020-7209	WEB-MISC HP LinuxKI vor 6.0-2 - Nicht authentifizierte RCE-Schwachstelle über kivis.php und seinen Parameter (CVE-2020-7209)
999544	CVE-2020-7209	WEB-MISC HP LinuxKI vor 6.0-2 - Nicht authentifizierte RCE-Schwachstelle über kivis.php und Ende Param (CVE-2020-7209)
999545	CVE-2020-7209	WEB-MISC HP LinuxKI vor 6.0-2 - Nicht authentifizierte RCE-Schwachstelle über kivis.php und starten Param (CVE-2020-7209)
999546	CVE-2020-7209	WEB-MISC HP LinuxKI vor 6.0-2 - Nicht authentifizierte RCE-Schwachstelle über kivis.php und PID Param (CVE-2020-7209)

Regel zur Unterschrift	CVE-ID	Beschreibung
999547	CVE-2020-7209	WEB-MISC HP LinuxKI vor 6.0-2 - Nicht authentifizierte RCE-Schwachstelle über kidsk_trace_view.php und Ende Param (CVE-2020-7209)
999548	CVE-2020-7209	WEB-MISC HP LinuxKI vor 6.0-2 - Nicht authentifizierte RCE-Schwachstelle über kidsk_trace_view.php und starten Param (CVE-2020-7209)
999549		WEB-MISC PHP-Fusion vor 9.03.70 - Sicherheitsrisiko durch PHP-Objekteinschleusung
999550	CVE-2020-1181	WEB-MISC Microsoft SharePoint Server — Remotecodeausführung über Webparts (CVE-2020-1181)
999551	CVE-2020-10547	WEB-MISC RConfig vor 3.9.5 — Nicht authentifizierte SQLi-Schwachstelle in Richtlinienelementen über SearchColumn (CVE-2020-10547)
999552	CVE-2020-10547	WEB-MISC RConfig vor 3.9.5 — Nicht authentifizierte SQLi-Schwachstelle in Richtlinienelementen über SearchField (CVE-2020-10547)
999553	CVE-2020-8605	WEB-MISC Trend Micro InterScan Web Security Virtual Appliance vor 6.5 SP2 Patch 4 — RCE-Schwachstelle (CVE-2020-8605)

Regel zur Unterschrift	CVE-ID	Beschreibung
999554	CVE-2019-10068	WEB-MISC Kentico CMS mehrere Versionen — Sicherheitsanfälligkeit bei der Ausführung von nicht authentifiziertem Remotecode (CVE-2019-10068)
999555	CVE-2020-11108	WEB-MISC Pi-hole bis zu 4.4 - Authentifizierte RCE-Sicherheitslücke (CVE-2020-11108)

Signatur-Update für Okt. 2020

January 25, 2022

Für die in der Woche 2020-10-13 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 51 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999505		WEB-WORDPRESS WordPress Plug-in wpDiscuz 7.0.0 bis zu 7.0.4 - Sicherheitslücke beim Hochladen willkürlicher Dateien nicht authentifiziert
999506		WEB-WORDPRESS Quiz & Survey Master — Cross-Site Scripting — Funktion
999507	CVE-2020-8604	WEB-MISC Trend Micro IWS VA vor 6.5 SP2 Patch 4 — Pfaddurchquerung über /log_search und vgl. Param (CVE-2020-8604)
999508	CVE-2020-8604	WEB-MISC Trend Micro IWS VA vor 6.5 SP2 Patch 4 — Pfad Traversal Vuln Va/collection und vgl. Param (CVE-2020-8604)
999509	CVE-2020-8604	WEB-MISC Trend Micro IWS VA vor 6.5 SP2 Patch 4 — Pfaddurchquerung der Vuln über /log_search und Dateiparam (CVE-2020-8604)
999510	CVE-2020-8604	WEB-MISC Trend Micro IWS VA vor 6.5 SP2 Patch 4 — Pfaddurchquerung über /collection und Dateiparam (CVE-2020-8604)
999511	CVE-2020-7361	WEB-MISC ZenTAO Enterprise 8.8.3 und früher — Sicherheitsanfälligkeit bei Remotecodeausführung über Repo-Edit (CVE-2020-7361)

Regel zur Unterschrift	CVE-ID	Beschreibung
999512	CVE-2020-7361	WEB-MISC ZenTAO Pro 8.8.3 und früher — Sicherheitsanfälligkeit bei Remotecodeausführung über Repo-Edit (CVE-2020-7361)
999513	CVE-2020-7361	WEB-MISC ZenTAO Enterprise 8.8.3 und früher — Sicherheitsanfälligkeit bei Remotecodeausführung über Repo-Create (CVE-2020-7361)
999514	CVE-2020-7361	WEB-MISC ZenTAO Pro 8.8.3 und früher — Sicherheitsanfälligkeit bei Remotecodeausführung über Repo-Create (CVE-2020-7361)
999515	CVE-2020-5768	WEB-WORDPRESS Plug-in für Icegram E-Mail-Abonnenten und Newsletter vor 4.5.1 - Sicherheitsanfälligkeit durch SQL Injection (CVE-2020-5768)
999516	CVE-2020-5767	WEB-WORDPRESS Plug-in für Icegram E-Mail-Abonnenten und Newsletter vor 4.5.1 - CSRF-Sicherheitslücke (CVE-2020-5767)
999517	CVE-2020-15299	WEB-WORDPRESS KingComposer Plug-in vor 2.9.5 — Site-übergreifende Sicherheitslücke beim Scripting (CVE-2020-15299)
999518	CVE-2020-13854	WEB-MISC Artica Pandora FMS — Sicherheitsanfälligkeit bei Berechtigungseskalation (CVE-2020-13854)

Regel zur Unterschrift	CVE-ID	Beschreibung
999519	CVE-2020-13852	WEB-MISC Artica Pandora FMS - Schwachstelle beim Hochladen beliebiger Dateien über Dateimanager (CVE-2020-13852)
999520	CVE-2020-13700	WEB-WORDPRESS WordPress Plug-in acf-zu-rest-api vor 3.3.0 - Sicherheitslücke bei der Offenlegung von Informationen über URI (CVE-2020-13700)
999521	CVE-2020-13700	WEB-WORDPRESS WordPress Plug-in acf-zu-rest-api vor 3.3.0 — Sicherheitslücke bei der Offenlegung von Informationen über URL (CVE-2020-13700)
999522	CVE-2020-13379	WEB-MISC Grafana 3.0.1 bis 7.0.1 - CSRF-Bypass führt zu DOS-Schwachstelle (CVE-2020-13379)
999523	CVE-2020-12851	WEB-MISC Pydio-Zellen vor 2.0.7 - Schwachstelle beim Schreiben beliebiger Dateien (CVE-2020-12851)
999524	CVE-2020-12848	WEB-MISC Pydio-Zellen vor 2.0.7 - Anmeldung als temporäre Sicherheitsanfälligkeit für gemeinsam genutzte Benutzer (CVE-2020-12848)
999525	CVE-2020-11749	WEB-MISC Artica Pandora FMS vor 7.47 - Cross-Site Scripting-Schwachstelle über SNMP-Browser (CVE-2020-11749)

Regel zur Unterschrift	CVE-ID	Beschreibung
999526	CVE-2020-11579	WEB-MISC PHPKBV9 - Schwachstelle bei der Dateiexfiltration (CVE-2020-11579)
999527	CVE-2020-10546	WEB-MISC RConfig vor 3.9.5 — Nicht authentifizierte SQLi-Schwachstelle in Compliance-Richtlinien über SearchColumn (CVE-2020-10546)
999528	CVE-2020-10546	WEB-MISC RConfig vor 3.9.5 — Nicht authentifizierte SQLi-Schwachstelle in Compliance-Richtlinien über SearchField (CVE-2020-10546)
999529	CVE-2019-16876	WEB-MISC-Portainer vor 1.22.1 — Sicherheitsanfälligkeit durch Verzeichnisdurchlauf (CVE-2019-16876)
999530		WEB-WORDPRESS — ADNing-Plug-In vor 1.5.6 — Sicherheitsanfälligkeit beim Löschen willkürlicher Dateien ohne Authentifizierung
999531		WEB-WORDPRESS - Adning-Plug-in vor 1.5.6 - Nicht authentifizierte Schwachstelle beim Hochladen willkürlicher Dateien

Signatur-Update für Oktober 2020

January 25, 2022

Für die in der Woche 2020-10-29 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 52 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken. Anfällige Versionen werden auch in einigen Protokollzeichenfolgen der Signaturregel erwähnt. Sie müssen es entsprechend aktivieren.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999500	CVE-2018-14667	WEB-MISC RichFaces Framework 3.X bis 3.3.4 - EL-Einschleusung über UserResource (CVE-2018-14667)
999501	CVE-2018-12533	WEB-MISC RichFaces Framework 3.1.0 bis 3.3.4 - EL-Einschleusung über Paint2dResource (CVE-2018-12533)
999502	CVE-2015-0279, CVE-2018-12532	WEB-MISC RichFaces Framework 4.X bis 4.5.17 - EL-Einschleusung über Medienausgaberessource (CVE-2015-0279, CVE-2018-12532)

Regel zur Unterschrift	CVE-ID	Beschreibung
999503	CVE-2013-2165	WEB-MISC RichFaces v4 vor 4.3.3 — Schwachstelle bei der Deserialisierung von Java-Objekten (CVE-2013-2165)
999504	CVE-2013-2165	WEB-MISC RichFaces v3 Vor 3.3.4 - Schwachstelle zur Deserialisierung von Java-Objekten (CVE-2013-2165)

Signatur-Update für November 2020

January 25, 2022

Für die in der Woche 2020-11-10 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 53 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999411		WEB-WORDPRESS WordPress Plug-in wpDiscuz 7.0.0 bis zu 7.0.4 - Sicherheitslücke beim Hochladen willkürlicher Dateien nicht authentifiziert
999412		WEB-WORDPRESS Quiz & Survey Master — Cross-Site Scripting — Funktion
999413		WEB-WORDPRESS WordPress Plug-in-Dateimanager vor 6.9 - Sicherheitsanfälligkeit bei der Ausführung nicht authentifizierter ElFinder-Befehle
999414	CVE-2020-11700	WEB-MISC Titan SpamTitan vor 7.08 — Schwachstelle bei der Offenlegung von Informationen (CVE-2020-11700)
999415	CVE-2020-9446	WEB-MISC Apache ofBiz 17.12.03 - Sicherheitslücke bei unsicherer Deserialisierung durch XML-RPC (CVE-2020-9446)
999416	CVE-2020-9446	WEB-MISC Apache ofBiz 17.12.03 - XML-RPC-Cross-Site Scripting-Sicherheitsrisiko (CVE-2020-9446)
999417	CVE-2020-9047	WEB-MISC exacqVision-Webdienst bis zu 20.06.3.0 — Sicherheitsrisiko durch OS-Befehlseinschleusung (CVE-2020-9047)

Regel zur Unterschrift	CVE-ID	Beschreibung
999418	CVE-2020-8866	WEB-MISC Horde Groupware Webmail Edition 5.2.22 - Uneingeschränktes Hochladen von Dateischwachstellen über edit.php (CVE-2020-8866)
999419	CVE-2020-8866	WEB-MISC Horde Groupware Webmail Edition 5.2.22 - Uneingeschränktes Hochladen von Dateischwachstellen über add.php (CVE-2020-8866)
999420	CVE-2020-8865	WEB-MISC Horde Groupware Webmail Edition 5.2.22 - Schwachstelle bei der Einbeziehung beliebiger Dateien über edit.php (CVE-2020-8865)
999421	CVE-2020-8816	WEB-MISC Pi-hole vor 4.3.2 — Sicherheitsanfälligkeit bei Remotecodeausführung über removestatic (CVE-2020-8816)
999422	CVE-2020-8816	WEB-MISC Pi-Hole vor 4.3.2 — Sicherheitsanfälligkeit bei Remotecodeausführung über AddMac (CVE-2020-8816)
999423	CVE-2020-8243	WEB-MISC Pulse Connect Secure vor 9.1R8.2 — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2020-8243)
999424	CVE-2020-8218	WEB-MISC Pulse Connect Secure vor 9.1R8 — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2020-8218)

Regel zur Unterschrift	CVE-ID	Beschreibung
999425	CVE-2020-6143, CVE-2020-6144	WEB-MISC OS4ed OpenSIS — Sicherheitsrisiko durch CodeEinschleusung über /install/Ins1.php (CVE-2020-6143, CVE-2020-6144)
999426	CVE-2020-6142	WEB-MISC OS4ed OpenSIS - Schwachstelle durch Pfaddurchquerung über Modname (CVE-2020-6142)
999427	CVE-2020-6141	WEB-MISC OS4ed OpenSIS vor 7.4 — Nicht authentifizierte SQLi-Schwachstelle über USERNAME (CVE-2020-6141)
999428	CVE-2020-6140	WEB-MISC OS4ed OpenSIS vor 7.5 — Nicht authentifizierte SQLi-Schwachstelle über username_stn_id (CVE-2020-6140)
999429	CVE-2020-6139	WEB-MISC OS4ed OpenSIS vor 7.5 — Nicht authentifizierte SQLi-Sicherheitslücke über username_stf_email (CVE-2020-6139)
999430	CVE-2020-6138	WEB-MISC OS4ed OpenSIS vor 7.5 — Nicht authentifizierte SQLi-Schwachstelle über uname (CVE-2020-6138)

Regel zur Unterschrift	CVE-ID	Beschreibung
999431	CVE-2020-6137	WEB-MISC OS4ed OpenSIS vor 7.5 — Nicht authentifizierte SQLi-Schwachstelle über password_stf_email (CVE-2020-6137)
999432	CVE-2020-6125	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über GetSchool.php und u Parameter (CVE-2020-6125)
999433	CVE-2020-6124	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über EmailCheckOthers.php (CVE-2020-6124)
999434	CVE-2020-6123	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über EmailCheck.php und p_id-Parameter (CVE-2020-6123)
999435	CVE-2020-6123	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über EmailCheck.php und E-Mail-Parameter (CVE-2020-6123)
999436	CVE-2020-6122	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über CheckDuplicateStudent.php und mn-Parameter (CVE-2020-6122)
999437	CVE-2020-6121	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über CheckDuplicateStudent.php und ln Parameter (CVE-2020-6121)

Regel zur Unterschrift	CVE-ID	Beschreibung
999438	CVE-2020-6120	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über CheckDuplicateStudent.php und fn-Parameter (CVE-2020-6120)
999439	CVE-2020-6119	WEB-MISC OS4ed OpenSIS vor 7.5 - SQLi-Schwachstelle über CheckDuplicateStudent.php und byear Parameter (CVE-2020-6119)
999440	CVE-2020-6118	WEB-MISC OS4ed OpenSIS vor 7.5 - SQLi-Schwachstelle über CheckDuplicateStudent.php und bmonth Parameter (CVE-2020-6118)
999441	CVE-2020-6117	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über CheckDuplicateStudent.php und bday-Parameter (CVE-2020-6117)
999442	CVE-2020-5780	WEB-WORDPRESS WordPress-Plug-In E-Mail-Abonnenten und Newsletter vor 4.5.6 — Sicherheitslücke bei E-Mail-Fälschungen (CVE-2020-5780)
999443	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 und 7.4 — Unsichere Sicherheitsanfälligkeit durch Java-Deserialisierung über JSON-RPC (CVE-2020-4280)

Regel zur Unterschrift	CVE-ID	Beschreibung
999444	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 und 7.4 — Unsichere Sicherheitsanfälligkeit durch Java-Deserialisierung über RemoteMethod (CVE-2020-4280)
999445	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 und 7.4 — Unsichere Sicherheitsanfälligkeit durch Java-Deserialisierung über RemoteJavaScript (CVE-2020-4280)
999446	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 und 7.4 — Unsichere Sicherheitsanfälligkeit durch Java-Deserialisierung über JSON-RPC (CVE-2020-4280)
999447	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 und 7.4 — Unsichere Sicherheitsanfälligkeit durch Java-Deserialisierung über RemoteMethod (CVE-2020-4280)
999448	CVE-2020-4280	WEB-MISC IBM QRadar SIEM 7.3 und 7.4 — Unsichere Sicherheitsanfälligkeit durch Java-Deserialisierung über RemoteJavaScript (CVE-2020-4280)
999449	CVE-2020-24786	WEB-MISC Zoho ManageEngine AdManager Plus 7.0 vor Build 55 — Sicherheitslücke bei unsachgemäßer Authentifizierung (CVE-2020-24786)

Regel zur Unterschrift	CVE-ID	Beschreibung
999450	CVE-2020-24389	WEB-WORDPRESS Plug-In zum Hochladen mehrerer Dateien per Drag & Drop vor 1.3.5.5 — Sicherheitsschwachstelle umgehen (CVE-2020-24389)
999451	CVE-2020-24046	WEB-MISC TitanHQ SpamTitan Gateway 7.08 — Sicherheitslücke bei Berechtigungseskalation (CVE-2020-24046)
999452	CVE-2020-17506	WEB-MISC Artica Web Proxy 4.30.000000 - Sicherheitsanfälligkeit durch PreAuth SQL-Injection über Apikey-Parameter (CVE-2020-17506)
999453	CVE-2020-17505	WEB-MISC Artica Web Proxy 4.30.000000 — Sicherheitsrisiko durch OS-Befehlseinschleusung über Service-cmds-Perform-Parameter (CVE-2020-17505)
999454	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 - SQLi-Schwachstelle über /fuel/users/items (CVE-2020-17463)
999455	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 — SQLi-Schwachstelle über /fuel/sitevariables/items (CVE-2020-17463)
999456	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 — SQLi-Schwachstelle über /fuel/permissions/items (CVE-2020-17463)

Regel zur Unterschrift	CVE-ID	Beschreibung
999457	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 — SQLi-Schwachstelle über /fuel/pages/items (CVE-2020-17463)
999458	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 - SQLi-Schwachstelle über /fuel/navigation/items (CVE-2020-17463)
999459	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 — SQLi-Schwachstelle über /fuel/logs/items (CVE-2020-17463)
999460	CVE-2020-17463	WEB-MISC Fuel CMS 1.4.8 - SQLi-Schwachstelle über /fuel/blocks/items (CVE-2020-17463)
999461	CVE-2020-16875	WEB-MISC Microsoft Exchange Server — Sicherheitsanfälligkeit bei der Ausführung von Remote-Code durch DLP-Richtlinien (CVE-2020-16875)
999462	CVE-2020-16171	WEB-MISC Acronis Cyber Backup vor 12.5 Build 16342 — SSRF über Shard-Header-Schwachstelle (CVE-2020-16171)
999463	CVE-2020-14947	WEB-MISC OCS Inventar vor 2.8 — Sicherheitsrisiko durch OS-Befehlseinschleusung über SNMP_MIB_DIRECTORY (CVE-2020-14947)

Regel zur Unterschrift	CVE-ID	Beschreibung
999464	CVE-2020-14947	WEB-MISC OCS Inventar vor 2.8 — Sicherheitsrisiko durch OS-Befehlseinschleusung über mib_file (CVE-2020-14947)
999465	CVE-2020-14008	WEB-MISC Zoho ManageEngine Applications Manager bis zu 14710 — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2020-14008)
999466	CVE-2020-13925	WEB-MISC Apache Kylin vor 3.1.0 — Sicherheitsanfälligkeit bei Remotecodeausführung über Job (CVE-2020-13925)
999467	CVE-2020-13925	WEB-MISC Apache Kylin vor 3.1.0 — Sicherheitsanfälligkeit bei Remotecodeausführung über Projekt (CVE-2020-13925)
999468	CVE-2020-13854	WEB-MISC Artica Pandora FMS — Sicherheitsanfälligkeit bei Berechtigungseskalation (CVE-2020-13854)
999469	CVE-2020-13405	WEB-MISC Microweber vor 1.1.20 — Sicherheitsanfälligkeit bei der Offenlegung nicht authentifizierter Informationen (CVE-2020-13405)

Regel zur Unterschrift	CVE-ID	Beschreibung
999470	CVE-2020-13376	WEB-MISC SecurEnvoy SecurMail 9.3.503 — SecurEnvoyReply Sicherheitsanfälligkeit beim Durchlaufen des Cookie-Pfads (CVE-2020-13376)
999471	CVE-2020-13159	WEB-MISC Artica Webproxy vor 4.30.000000 — Sicherheitsrisiko durch OS-Befehlseinschleusung über Domäne (CVE-2020-13159)
999472	CVE-2020-13159	WEB-MISC Artica Web Proxy vor 4.30.000000 - Sicherheitsrisiko durch OS-Befehlseinschleusung über netbiosname (CVE-2020-13159)
999473	CVE-2020-13159	WEB-MISC Artica Webproxy vor 4.30.000000 — Sicherheitsrisiko durch OS-Befehlseinschleusung über Alias (CVE-2020-13159)
999474	CVE-2020-13159	WEB-MISC Artica Webproxy vor 4.30.000000 - Sicherheitsrisiko durch OS-Befehlseinschleusung über Hostnamen (CVE-2020-13159)
999475	CVE-2020-13159	WEB-MISC Artica Webproxy vor 4.30.000000 — Sicherheitsrisiko durch OS-Befehlseinschleusung über dhclient_server (CVE-2020-13159)

Regel zur Unterschrift	CVE-ID	Beschreibung
999476	CVE-2020-13159	WEB-MISC Artica Webproxy vor 4.30.000000 — Sicherheitsrisiko durch OS-Befehlseinschleusung über dhclient_interface (CVE-2020-13159)
999477	CVE-2020-13159	WEB-MISC Artica Webproxy vor 4.30.000000 — Sicherheitsrisiko durch OS-Befehlseinschleusung über dhclient_mac (CVE-2020-13159)
999478	CVE-2020-13158	WEB-MISC Artica Web Proxy vor 4.30.000000 - Schwachstelle durch Pfaddurchquerung über Popup (CVE-2020-13158)
999479	CVE-2020-12851	WEB-MISC Pydio-Zellen vor 2.0.7 - Schwachstelle beim Schreiben beliebiger Dateien (CVE-2020-12851)
999480	CVE-2020-12848	WEB-MISC Pydio-Zellen vor 2.0.7 - Anmeldung als temporäre Sicherheitsanfälligkeit für gemeinsam genutzte Benutzer (CVE-2020-12848)
999481	CVE-2020-11699	WEB-MISC Titan SpamTitan vor 7.08 — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2020-11699)
999482	CVE-2020-11579	WEB-MISC PHPKBV9 - Schwachstelle bei der Dateiexfiltration (CVE-2020-11579)

Regel zur Unterschrift	CVE-ID	Beschreibung
999483	CVE-2020-10818	WEB-MISC Artica Web Proxy 4.26 - Sicherheitsrisiko durch OS-Befehlseinschleusung über fw.system.info.php (CVE-2020-10818)
999484	CVE-2020-10228	WEB-MISC Vtenext CE vor Version 20 — Uneingeschränktes Hochladen von Dateien mit Sicherheitsanfälligkeit durch gefährliche Typen (CVE-2020-10228)
999485	CVE-2020-10204	WEB-MISC Sonatype Nexus Repository Manager vor 3.21.2 — RCE-Schwachstelle über CoreUI_User-Rollen (CVE-2020-10204)
999486	CVE-2020-10204	WEB-MISC Sonatype Nexus Repository Manager vor 3.21.2 — RCE-Schwachstelle über CoreUI_Role-Berechtigungen (CVE-2020-10204)
999487	CVE-2020-10204	WEB-MISC Sonatype Nexus Repository Manager vor 3.21.2 — RCE-Schwachstelle über CoreUI_Role-Rollen (CVE-2020-10204)
999488	CVE-2020-10199	WEB-MISC Sonatype Nexus Repository Manager vor 3.21.2 — RCE-Schwachstelle über REST-Endpunkt /bower/group (CVE-2020-10199)

Regel zur Unterschrift	CVE-ID	Beschreibung
999489	CVE-2020-10199	WEB-MISC Sonatype Nexus Repository Manager vor 3.21.2 — RCE-Schwachstelle über REST-Endpunkt /go/group (CVE-2020-10199)
999490	CVE-2020-10199	WEB-MISC Sonatype Nexus Repository Manager vor 3.21.2 — RCE-Schwachstelle über REST-Endpunkt /docker/group (CVE-2020-10199)
999491	CVE-2019-19699	WEB-MISC Centreon bis zu 19,10 — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2019-19699)
999492	CVE-2019-19499	WEB-MISC Apache Grafana bis zu 6.4.3 — Sicherheitsanfälligkeit beim Lesen beliebiger Dateien (CVE-2019-19499)
999493	CVE-2019-18394	WEB-MISC Ignite Realtime Openfire bis zu 4.4.2 - FaviconServlet Serverseitige Anforderungsfälschung (CVE-2019-18394)
999494	CVE-2019-18393	WEB-MISC Ignite Realtime Openfire bis zu 4.4.2 — Plug-in-Servlet-Verzeichnisdurchlauf-Sicherheitsanfälligkeit (CVE-2019-18393)
999495	CVE-2019-16759	WEB-MISC vBulletin vor 5.6.2 — Sicherheitsanfälligkeit bei Remotecodeausführung über verschachtelte Vorlage (CVE-2019-16759)

Regel zur Unterschrift	CVE-ID	Beschreibung
999496	CVE-2019-15715	WEB-MISC MantisBT vor 1.3.20 und 2.22.1 — Sicherheitsanfälligkeit bei Remotecodeausführung über neato_tool (CVE-2019-15715)
999497	CVE-2019-15715	WEB-MISC MantisBT vor 1.3.20 und 2.22.1 — Sicherheitsanfälligkeit bei Remotecodeausführung über dot_tool (CVE-2019-15715)
999498	CVE-2019-11043	WEB-MISC PHP-FPM mehrere Versionen - Sicherheitsanfälligkeit beim Schreiben außerhalb der Grenzen ermöglicht die Ausführung beliebigen Codes (CVE-2019-11043)
999499		WEB-WORDPRESS-Plug-in Autoptimize bis zu 2.7.6 - Authentifizierte Schwachstelle beim Hochladen beliebiger Dateien

Signatur-Update für Dezember 2020

January 25, 2022

Für die in der Woche 2020-12-02 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 54 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken. Im Rahmen der Signaturaktualisierung Version 54 wird die Protokollzeichenfolge für Signatur 999720 geändert, um sicherzustellen, dass sie nur ASCI-Zeichen enthält.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999394	CVE-2020-8255	WEB-MISC Pulse Connect Secure vor 9.1R9 — Sicherheitsanfälligkeit bei der Offenlegung von Informationen (CVE-2020-8255)
999395	CVE-2020-6128	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über CoursePeriodModal.php (CVE-2020-6128)
999396	CVE-2020-6126, CVE-2020-6127	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über CoursePeriodModal.php (CVE-2020-6126, CVE-2020-6127)
999397	CVE-2020-28328	WEB-MISC SuiteCRM vor 7.11.16 — Sicherheitsanfälligkeit bei Remotecodeausführung (CVE-2020-28328)

Regel zur Unterschrift	CVE-ID	Beschreibung
999398	CVE-2020-27995	WEB-MISC Zoho ManageEngine Applications Manager 14 vor Build 14560 — Sicherheitsanfälligkeit durch SQL Injection (CVE-2020-27995)
999399	CVE-2020-26879	WEB-MISC Ruckus vRiot Server vor 1.6.0 — Sicherheitsanfälligkeit durch Autorisierung umgehen über /service/ (CVE-2020-26879)
999400	CVE-2020-26879	WEB-MISC Ruckus vRiot Server vor 1.6.0 — Sicherheitsanfälligkeit durch Autorisierung umgehen über /reboot (CVE-2020-26879)
999401	CVE-2020-26879	WEB-MISC Ruckus vRiot Server vor 1.6.0 — Sicherheitsanfälligkeit durch Autorisierung umgehen über /patch/ (CVE-2020-26879)
999402	CVE-2020-26879	WEB-MISC Ruckus vRiot Server vor 1.6.0 — Sicherheitsanfälligkeit durch Autorisierung umgehen über /upgrade/ (CVE-2020-26879)
999403	CVE-2020-26879	WEB-MISC Ruckus vRiot Server vor 1.6.0 — Sicherheitsanfälligkeit durch Autorisierung umgehen über /module/ (CVE-2020-26879)

Regel zur Unterschrift	CVE-ID	Beschreibung
999404	CVE-2020-26878	WEB-MISC Ruckus vRiot Server vor 1.6.0 — Sicherheitsrisiko durch Einschleusung beliebiger Betriebssystembefehle (CVE-2020-26878)
999405	CVE-2020-25790	WEB-MISC Typesetter CMS 5.x bis 5.1 — Sicherheitsanfälligkeit beim Hochladen unsicherer Dateien (CVE-2020-25790)
999406	CVE-2020-25540	WEB-MISC ThinkAdmin v6 — Sicherheitsrisiko durch Verzeichnisdurchquerung (CVE-2020-25540)
999407	CVE-2020-14883	WEB-MISC Oracle WebLogic Server — Authentifizierte Remotecodeausführung Schwachstelle (CVE-2020-14883)
999408	CVE-2020-14882, CVE-2020-14750	WEB-MISC Oracle WebLogic Server — Sicherheitsrisiko durch Umgehung der Authentifizierung (CVE-2020-14882, CVE-2020-14750)
999409	CVE-2020-11975, CVE-2020-13942	WEB-MISC Apache Unomi vor 1.5.2 — Sicherheitsrisiko durch Remotecodeausführung (CVE-2020-11975, CVE-2020-13942)

Regel zur Unterschrift	CVE-ID	Beschreibung
999410	CVE-2020-11803	WEB-MISC Titan SpamTitan vor 7.08 — Sicherheitsrisiko durch Remotecodeausführung (CVE-2020-11803)

Signatur-Update für Dezember 2020

January 25, 2022

Für die in der Woche 2020-12-17 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 55 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999377		WEB-WORDPRESS TI WooCommerce Wishlist Plugin vor 1.21.11 - Sicherheitslücke bei der Offenlegung von Informationen über tinvwl_export_settings
999378		WEB-WORDPRESS TI WooCommerce Wishlist Plugin vor 1.21.11 - WP-Optionen ändern Sicherheitslücke über tinvwl_import_settings
999379	CVE-2020-6134	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über MassDropModal.php (CVE-2020-6134)
999380	CVE-2020-6133	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über CourseMoreInfo.php (CVE-2020-6133)
999381	CVE-2020-6132	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über ChooseCP.php (CVE-2020-6132)
999382	CVE-2020-6131	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über MassScheduleSessionSet.php (CVE-2020-6131)
999383	CVE-2020-6130	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über MassDropSessionSet.php (CVE-2020-6130)

Regel zur Unterschrift	CVE-ID	Beschreibung
999384	CVE-2020-6129	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über CpSessionSet.php (CVE-2020-6129)
999385	CVE-2020-35234	WEB-WORDPRES Easy WP SMTP-Plugin vor 1.4.4 - Sicherheitsrisiko durch Offenlegung von Informationen (CVE-2020-35234)
999386	CVE-2020-25042	WEB-MISC Mara CMS 7.5 — Schwachstelle beim Hochladen beliebiger Dateien (CVE-2020-25042)
999387	CVE-2020-13526	WEB-MISC ProcessMaker — Sicherheitsrisiko durch SQL-Injection über ClientSetupAJAX (CVE-2020-13526)
999388	CVE-2020-13525	WEB-MISC ProcessMaker — Sicherheitsrisiko durch SQL-Injection über ReportTables_AJAX (CVE-2020-13525)
999389	CVE-2020-12147	WEB-MISC Silver Peak Unity Orchestrator — Schwachstelle bei beliebigen MySQL-Abfragen über SQLExecution REST API (CVE-2020-12147)
999390	CVE-2020-12146	WEB-MISC Silver Peak Unity Orchestrator — Sicherheitsrisiko durch Pfaddurchquerung über DebugFiles-REST-API (CVE-2020-12146)

Regel zur Unterschrift	CVE-ID	Beschreibung
999391	CVE-2020-12145	WEB-MISC Silver Peak Unity Orchestrator — Sicherheitsrisiko durch Umgehung der Authentifizierung (CVE-2020-12145)
999392	CVE-2019-8394	WEB-MISC Zoho ManageEngine ServiceDesk Plus vor 10.0 Build 10012 — Schwachstelle beim Hochladen beliebiger Dateien (CVE-2019-8394)
999393	CVE-2019-11447	WEB-MISC CutePHP CuteNews 2.1.2 - Sicherheitsrisiko durch Remotecodeausführung (CVE-2019-11447)

Signatur-Update für Januar 2021

January 25, 2022

Für die in der Woche 2021-01-18 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 56 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU

> auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999366	CVE-2020-8466	WEB-MISC Trend Micro IWSSVA 6.5 SP2 vor Build 1919 — Sicherheitsrisiko durch nicht authentifizierte BS-Befehlseinschleusung (CVE-2020-8466)
999367	CVE-2020-6135	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über Validator.php (CVE-2020-6135)
999368	CVE-2020-4001	WEB-MISC VMware SD-WAN Orchestrator — Hash-Schwachstelle (CVE-2020-4001)
999369	CVE-2020-4000	WEB-MISC VMware SD-WAN Orchestrator — Schwachstelle durch Pfaddurchquerung (CVE-2020-4000)
999370	CVE-2020-3984	WEB-MISC VMware SD-WAN Orchestrator — Sicherheitsrisiko durch SQL-Einschleusung über Modul (CVE-2020-3984)
999371	CVE-2020-35606	WEB-MISC Webmin Bis zu 1.962 — Sicherheitsrisiko durch Remotecodeausführung (CVE-2020-35606)

Regel zur Unterschrift	CVE-ID	Beschreibung
999372	CVE-2020-17143	WEB-MISC Microsoft Exchange Server — Schwachstelle bei der Offenlegung von Informationen (CVE-2020-17143)
999373	CVE-2020-17141	WEB-MISC Microsoft Exchange Server — Sicherheitsrisiko durch Remotecodeausführung über RouteComplaint (CVE-2020-17141)
999374	CVE-2020-10816	WEB-MISC Zoho ManageEngine Applications Manager 14 vor Build 14790 — Sicherheitslücke bei unsachgemäßer Authentifizierung (CVE-2020-10816)
999375	CVE-2019-5533	WEB-MISC VMware SD-WAN Orchestrator — Schwachstelle bei der Offenlegung von Informationen (CVE-2019-5533)
999376	CVE-2018-15961	WEB-MISC Adobe ColdFusion 12 vor Update 6 oder 14 - Willkürliche Schwachstelle beim Hochladen von Dateien (CVE-2018-15961)

Aktualisierung der Unterschrift für Februar 2021

January 25, 2022

Für die in der Woche 2021-02-03 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheit-

sangriffen zu schützen.

Signaturversion

Die Signaturversion 57 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999339		WEB-MISC Zoom Meeting Connector 4.6.348.20201217 — Sicherheitsrisiko durch Remotecodeausführung über ProxyPasswd
999340		WEB-MISC Zoom Meeting Connector 4.6.348.20201217 — Sicherheitsrisiko durch Remotecodeausführung über ProxyName
999341	CVE-2021-3129	WEB-MISC-Zündung vor 2.5.2 — Sicherheitsanfälligkeit bei Ausführung von nicht authentifiziertem Remotecode (CVE-2021-3129)
999342	CVE-2021-3025	WEB-MISC Invision Community IPS-Community-Suite vor 4.5.4.2 — Sicherheitsrisiko durch SQL-Injection über SortDir (CVE-2021-3025)

Regel zur Unterschrift	CVE-ID	Beschreibung
999343	CVE-2021-2109	WEB-MISC Oracle WebLogic Server — Sicherheitsrisiko durch Remotecodeausführung über JNDI-Einschleusung (CVE-2021-2109)
999344	CVE-2020-7200	WEB-MISC HPE Systems Insight Manager 7.6.x — Sicherheitslücke bei unsicherer AMF-Deserialisierung (CVE-2020-7200)
999345	CVE-2020-7199	WEB-MISC HPE EIM vor Version 1.21 — Sicherheitslücke bei unsachgemäßer Authentifizierung in /private/eimApplianceIP (CVE-2020-7199)
999346	CVE-2020-7199	WEB-MISC HPE EIM vor Version 1.21 — Sicherheitslücke bei unsachgemäßer Authentifizierung in /private/adminPassReset (CVE-2020-7199)
999347	CVE-2020-7199	WEB-MISC HPE EIM vor Version 1.21 — Sicherheitslücke bei unsachgemäßer Authentifizierung in /private/resetAppliance (CVE-2020-7199)

Regel zur Unterschrift	CVE-ID	Beschreibung
999348	CVE-2020-6136	WEB-MISC OS4ed OpenSIS vor 7.5 — SQLi-Schwachstelle über DownloadWindow.php (CVE-2020-6136)
999349	CVE-2020-35729	WEB-MISC KLog Server 2.4.1 und früher — Sicherheitsrisiko durch OS-Befehlseinschleusung (CVE-2020-35729)
999350	CVE-2020-35701	WEB-MISC Cacti 1.2.16 und früher — Sicherheitsrisiko durch SQL-Injection über site_id (CVE-2020-35701)
999351	CVE-2020-35489	WEB-WORDPRESS-Kontaktformular 7 vor 5.3.2 — Sicherheitslücke beim uneingeschränkten Hochladen von Dateien (CVE-2020-35489)
999352	CVE-2020-27615	WEB-WORDPRESS Loginizer-Plugin vor 1.6.4 — Sicherheitsrisiko durch SQL-Einschleusung (CVE-2020-27615)
999353	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 und früher — XSS-Schwachstelle über /fuel/sitevariables/create (CVE-2020-26046)
999354	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 und früher — XSS-Sicherheitslücke über /fuel/sitevariables/edit (CVE-2020-26046)

Regel zur Unterschrift	CVE-ID	Beschreibung
999355	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 und früher — XSS-Schwachstelle über /fuel/navigation/create (CVE-2020-26046)
999356	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 und früher — XSS-Sicherheitslücke über /fuel/navigation/edit (CVE-2020-26046)
999357	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 und früher — XSS-Schwachstelle über /fuel/blocks/create (CVE-2020-26046)
999358	CVE-2020-26046	WEB-MISC Fuel CMS 1.4.11 und früher — XSS-Schwachstelle über /fuel/blocks/edit (CVE-2020-26046)
999359	CVE-2020-26045	WEB-MISC Fuel CMS 1.4.11 — SQLi-Schwachstelle über /fuel/permissions/create (CVE-2020-26045)
999360	CVE-2020-17519	WEB-MISC Apache Flink vor 1.11.3 — Schwachstelle bei der Offenlegung willkürlicher Dateien (CVE-2020-17519)
999361	CVE-2020-17518	WEB-MISC Apache Flink 1.5.1 bis 1.11.2 — Sicherheitsrisiko durch Hochladen von Dateien an beliebigen Orten (CVE-2020-17518)
999362	CVE-2019-16010	WEB-MISC Cisco SD-WAN vManage vor 19.2.2 — Gespeicherte XSS-Sicherheitsrisiko (CVE-2019-16010)

Regel zur Unterschrift	CVE-ID	Beschreibung
999363	CVE-2019-15000	WEB-MISC VMware Bitbucket Server und Rechenzentrum — Git Command Injection Sicherheitslücke über at (CVE-2019-15000)
999364	CVE-2019-15000	WEB-MISC VMware Bitbucket Server und Rechenzentrum - Git Command Injection Sicherheitsrisiko über until/untiliD (CVE-2019-15000)
999365	CVE-2019-15000	WEB-MISC VMware Bitbucket Server und Rechenzentrum - Sicherheitsrisiko durch Git-Befehlseinschleusung über Since/sinceID (CVE-2019-15000)

Aktualisierung der Unterschrift für Februar 2021

January 25, 2022

Für die in der Woche 2021-02-17 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 58 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999328	CVE-2021-3317	WEB-MISC KLog Server 2.4.1 und früher - Schwachstelle für Betriebssystem-Command Injection (CVE-2021-3317)
999329	CVE-2021-3110	WEB-MISC PrestaShop Vor 1.7.7.1 - Sicherheitslücke in SQL Injection über id_products (CVE-2021-3110)
999330	CVE-2021-3110	WEB-MISC PrestaShop Vor 1.7.7.1 - Sicherheitslücke in SQL Injection über /module/ProductComments/-CommentGrade (CVE-2021-3110)
999331	CVE-2021-25646	WEB-MISC Apache Druid vor 0.20.1 - Sicherheitslücke bei der Remote-Code-Ausführung (CVE-2021-25646)
999332	CVE-2020-36171	WEB-WORDPRESS Elementor Page Builder-Plugin vor 3.0.14 - XSS Sicherheitslücke (CVE-2020-36171)
999333	CVE-2020-35765	WEB-MISC Zoho ManageEngine Applications Manager vor Build 15000 - SQL Injection Sicherheitslücke (CVE-2020-35765)

Regel zur Unterschrift	CVE-ID	Beschreibung
999334	CVE-2020-35589	WEB-WORDPRESS Limit Anmeldeversuche vor 2.15.2 neu geladen - Spiegelte Sicherheitslücke für Cross-Site-Scripting (CVE-2020-35589)
999335	CVE-2020-26282	WEB-MISC BrowserUp Proxy vor 2.1.2 - Template-Injection führt zu RCE-Sicherheitslücke über MostRecentEntry (CVE-2020-26282)
999336	CVE-2020-26282	WEB-MISC BrowserUp Proxy vor 2.1.2 - Template-Injection führt zu RCE-Schwachstelle durch Einträge (CVE-2020-26282)
999337	CVE-2020-14815	WEB-MISC Oracle Business Intelligence Enterprise Edition - Spiegelte Site-Cross-Site-Scripting-Schwachstelle (CVE-2020-14815)
999338		WEB-WORDPRESS Kontaktformular 7 Database Addon vor 1.2.5.4 - SQLi-Schwachstelle durch Massenaktion löschen

Signatur-Update für März 2021

January 25, 2022

Für die in der Woche 2021-03-08 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 59 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999313	CVE-2021-25299	WEB-MISC NagiosXi Bis zu 5.7.5 - XSS Sicherheitslücke über URL (CVE-2021-25299)
999314	CVE-2021-25298	WEB-MISC NagiosXi Bis zu 5.7.5 - Sicherheitslücke bei der Remote-Codeausführung über DigitalOcean Wizard (CVE-2021-25298)
999315	CVE-2021-25297	WEB-MISC NagiOSXi Bis zu 5.7.5 - Sicherheitslücke bei Remote-Codeausführung über Switch-Assistent (CVE-2021-25297)
999316	CVE-2021-25296	WEB-MISC NagiosXi Bis zu 5.7.5 - Sicherheitslücke bei Remote-Codeausführung über WindowsWMI Wizard (CVE-2021-25296)

Regel zur Unterschrift	CVE-ID	Beschreibung
999317	CVE-2021-24164	WEB-WORDPRESS Ninja Forms Plugin vor 3.4.34.1 - Sicherheitslücke bei der Offenlegung von Informationen (CVE-2021-24164)
999318	CVE-2021-24163	WEB-WORDPRESS Ninja Forms Plugin vor 3.4.34 - Sicherheitslücke durch Autorisierung umgehen (CVE-2021-24163)
999319	CVE-2021-21972	WEB-MISC VMware vCenter Server Plugin - Sicherheitslücke bei der Remote-Codeausführung (CVE-2021-21972)
999320	CVE-2020-35129	WEB-MISC Mautic Vor 3.2.4 - XSS-Schwachstelle über neues Social-Monitoring-Formular (CVE-2020-35129)
999321	CVE-2020-35129	WEB-MISC Mautic Vor 3.2.4 - XSS Sicherheitslücke über Social Monitoring Formular bearbeiten (CVE-2020-35129)
999322	CVE-2020-35128	WEB-MISC Mautic Vor 3.2.4 - XSS Sicherheitslücke über neue Unternehmen (CVE-2020-35128)
999323	CVE-2020-35128	WEB-MISC Mautic Vor 3.2.4 - XSS Sicherheitslücke über das Formular “Unternehmen bearbeiten” (CVE-2020-35128)

Regel zur Unterschrift	CVE-ID	Beschreibung
999324	CVE-2020-35125	WEB-MISC Mautic Vor 3.2.4 - XSS Sicherheitslücke über Referer-Header (CVE-2020-35125)
999325	CVE-2020-35125	WEB-MISC Mautic Vor 3.2.4 - XSS Sicherheitslücke durch mauticforme[Rückkehr] (CVE-2020-35125)
999326	CVE-2020-13933	WEB-MISC Apache Shiro Vor 1.6.0 - Authentifizierung umgehen Sicherheitslücke über Semikolon (CVE-2020-13933)
999327	CVE-2020-13921, CVE-2020-9483	WEB-MISC Apache SkyWalking vor 8.4.0 - Sicherheitslücke bei SQL-Injection über QueryLogs-Funktion (CVE-2020-13921, CVE-2020-9483)

Signatur-Update für März 2021

January 25, 2022

Für die in der Woche 2021-03-09 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 60 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999311	CVE-2021-26855	WEB-MISC Microsoft Exchange Server - Sicherheitslücke bei der Remote-Codeausführung über X-AnonResource-Backend (CVE-2021-26855)
999312	CVE-2021-26855	WEB-MISC Microsoft Exchange Server - Sicherheitslücke bei der Remote-Codeausführung über X-BEResource (CVE-2021-26855)

Signatur-Update für März 2021

January 25, 2022

Für die in der Woche 2021-03-11 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 61 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999308	CVE-2021-21302	WEB-MISC PrestaShop Vor 1.7.7.2 - Sicherheitslücke in CSV Injection (CVE-2021-21302)
999309	CVE-2020-35749	WEB-WORDPRESS Einfache Jobbörse vor 2.9.4 - Schwachstelle für willkürliche Offenlegung von Dateien (CVE-2020-35749)
999310	CVE-2019-16012	WEB-MISC Cisco SD-WAN vManage Vor 19.2.2 - Sicherheitslücke in SQL Injection (CVE-2019-16012)

Signatur-Update für März 2021

January 25, 2022

Für die in der Woche 2021-03-11 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 62 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden

Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999307	CVE-2021-27065	WEB-MISC Microsoft Exchange Server - Sicherheitslücke bei der Remote-Codeausführung (CVE-2021-27065)

Signaturaktualisierung für April 2021

January 25, 2022

Für die in der Woche 2021-04-08 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 63 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999294	CVE-2021-3273	WEB-MISC NagiOSXi Vor 5.7 - Sicherheitslücke in Code Injection (CVE-2021-3273)
999295	CVE-2021-3197	WEB-MISC SaltStack Vor 3002.3 - Sicherheitslücke bei der Remote-Code-Ausführung über ssh_priv (CVE-2021-3197)
999296	CVE-2021-3197	WEB-MISC SaltStack Vor 3002.3 - Sicherheitslücke bei der Remote-Codeausführung über ssh_port (CVE-2021-3197)
999297	CVE-2021-3197	WEB-MISC SaltStack Vor 3002.3 - Sicherheitslücke bei der Remote-Code-Ausführung über ssh_options (CVE-2021-3197)
999298	CVE-2021-3197	WEB-MISC SaltStack Vor 3002.3 - Sicherheitslücke bei der Remote-Codeausführung über ProxyCommand im JSON-Objekt (CVE-2021-3197)
999299	CVE-2021-25282	WEB-MISC SaltStack Vor 3002.3 - Sicherheitslücke durch Pfaddurchqueren über pillar_roots.write (CVE-2021-25282)
999300	CVE-2021-24166	WEB-WORDPRESS Ninja Forms Plugin vor 3.4.34 - CSRF-Schwachstelle (CVE-2021-24166)
999301	CVE-2021-24085	WEB-MISC Microsoft Exchange Server - Schwachstelle im Spoofing (CVE-2021-24085)

Regel zur Unterschrift	CVE-ID	Beschreibung
999302	CVE-2021-22986	WEB-MISC F5 iControl REST API - Sicherheitslücke bei der Remote-Codeausführung (CVE-2021-22986)
999303	CVE-2021-21978	WEB-MISC VMware View Planner Harness 4.x vor 4.6 Security Patch 1 - Sicherheitslücke bei der Remote-Code-Ausführung (CVE-2021-21978)
999304	CVE-2020-23132	WEB-MISC Joomla! Vor 3.9.25 - Unsicher com_media Pfadanfälligkeit hochladen über file_path (CVE-2020-23132)
999305	CVE-2020-23132	WEB-MISC Joomla! Vor 3.9.25 - Unsicher com_media Pfadanfälligkeit hochladen über image_path (CVE-2020-23132)
999306	CVE-2020-22425	WEB-MISC Centreon vor 20.10.4 - Sicherheitslücke in SQL Injection (CVE-2020-22425)

Signaturaktualisierung für April 2021

January 25, 2022

Für die in der Woche 2021-04-22 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 64 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999275	CVE-2021-3378	WEB-MISC FortiLogger 4.4.2.2 - Sicherheitslücke beim Hochladen beliebiger Dateien (CVE-2021-3378)
999276	CVE-2021-28925	WEB-MISC Nagios Network Analyzer vor 2.4.3 - Sicherheitslücke bei SQL-Injection (CVE-2021-28925)
999277	CVE-2021-28924	WEB-MISC Nagios Network Analyzer vor 2.4.3 - XSS Sicherheitslücke (CVE-2021-28924)
999278	CVE-2021-27927	WEB-MISC Zabbix - CSRF-Schwachstelle über action=authentication.update (CVE-2021-27927)
999279	CVE-2021-26295	WEB-MISC Apache OfBiz 17.12.06 - Nicht authentifizierte Schwachstelle für willkürliche Deserialisierung (CVE-2021-26295)

Regel zur Unterschrift	CVE-ID	Beschreibung
999280	CVE-2021-25770	WEB-MISC JetBrains YouTrack Vor 2020.5.3123 - Schwachstelle für serverseitige Template-Injection (CVE-2021-25770)
999281	CVE-2021-25283	WEB-MISC SaltStack Vor 3002.5 - Sicherheitslücke bei der Remote-Code-Ausführung (CVE-2021-25283)
999282	CVE-2021-25283	WEB-MISC SaltStack vor 3002.5 - Sicherheitslücke bei der Remote-Codeausführung über JSON-Objekt (CVE-2021-25283)
999283	CVE-2021-24218	WEB-WORDPRESS Facebook für WordPress Plugin vor 3.0.4 - Gespeicherte Sicherheitslücke für Cross-Site-Scripting (CVE-2021-24218)
999284	CVE-2021-24217	WEB-WORDPRESS Facebook für WordPress Plugin vor 3.0.2 - Schwachstelle für PHP Object Injection (CVE-2021-24217)
999285	CVE-2021-24209	WEB-WORDPRESS WP Super Cache Plugin vor 1.7.2 - Sicherheitslücke bei der Remote-Codeausführung in wp-cache-config.php (CVE-2021-24209)

Regel zur Unterschrift	CVE-ID	Beschreibung
999286	CVE-2021-24209	WEB-WORDPRESS WP Super Cache Plugin vor 1.7.2 - Schwachstelle für willkürliche Code-Injection (CVE-2021-24209)
999287	CVE-2021-24165	WEB-WORDPRESS Ninja Forms Plugin vor 3.4.34 - Open Redirect Schwachstelle (CVE-2021-24165)
999288	CVE-2021-21975	WEB-MISC vRealize Operations Manager - Sicherheitslücke bei nicht authentifizierter serverseitiger Anforderungsfälschung (CVE-2021-21975)
999289	CVE-2020-35578	WEB-MISC Nagios XI Vor 5.8.0 - Sicherheitslücke bei der Remote-Code-Ausführung (CVE-2020-35578)
999290	CVE-2020-2766	WEB-MISC Oracle WebLogic Server - Nicht authentifizierte SSRF-Schwachstelle (CVE-2020-2766)
999291	CVE-2020-17523	WEB-MISC Apache Shiro Vor 1.7.1 - Authentifizierung umgehen Sicherheitslücke über den Speicherplatz (CVE-2020-17523)
999292	CVE-2020-17523	WEB-MISC Apache Shiro Vor 1.7.1 - Authentifizierung umgehen Sicherheitslücke über Dot (CVE-2020-17523)

Regel zur Unterschrift	CVE-ID	Beschreibung
999293	CVE-2020-15160	WEB-MISC PrestaShop Vor 1.7.6.8 - Sicherheitslücke in SQL Injection (CVE-2020-15160)

Signaturaktualisierung für Juni 2021

January 25, 2022

Für die in der Woche 2021-06-02 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 65 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999243	CVE-2021-31761	WEB-MISC Webmin Vor 1.974 - XSS Sicherheitslücke über /servers/link.cgi/ (CVE-2021-31761)

Regel zur Unterschrift	CVE-ID	Beschreibung
999244	CVE-2021-31761	WEB-MISC Webmin Vor 1.974 - XSS Sicherheitslücke Über /tunnel/link.cgi/ (CVE-2021-31761)
999245	CVE-2021-31166	WEB-IIS Microsoft HTTP-Protokoll-Stack - Sicherheitslücke bei der Remote-Codeausführung (CVE-2021-31166)
999246	CVE-2021-29447	WEB-WORDPRESS WordPress Vor 5.7.1 - Sicherheitslücke der Medienbibliothek XXE (CVE-2021-29447)
999247	CVE-2021-28157	WEB-MISC Devolutions Server vor 2021.1 und 2020.3.18 - Sicherheitslücke bei SQL Injection via Benutzerlöschung (CVE-2021-28157)
999248	CVE-2021-27905	WEB-MISC Apache Solr Vor 8.2.2 - ReplicationHandler SSRF-Sicherheitslücke über LeaderUrl (CVE-2021-27905)
999249	CVE-2021-27905	WEB-MISC Apache Solr Vor 8.2.2 - ReplicationHandler SSRF-Sicherheitslücke über MasterUrl (CVE-2021-27905)
999250	CVE-2021-27890	WEB-MISC myBB Vor 1.8.26 - Theme Eigenschaften SQL-Injection Sicherheitslücke (CVE-2021-27890)

Regel zur Unterschrift	CVE-ID	Beschreibung
999251	CVE-2021-27850, CVE-2019-0195	WEB-MISC Apache Tapestry - Sicherheitslücke bei nicht authentifizierter Offenlegung von Informationen (CVE-2021-27850 und CVE-2019-0195)
999252	CVE-2021-27183	WEB-MISC MDaemon vor 20.0.4 - Schwachstelle für willkürliche Dateischreiben (CVE-2021-27183)
999253	CVE-2021-27181	WEB-MISC MDaemon vor 20.0.4 - Sicherheitslücke zur Fixierung von Anti-CSRF-Token (CVE-2021-27181)
999254	CVE-2021-27180	WEB-MISC MDaemon vor 20.0.4 - Spiegelte XSS-Schwachstelle (CVE-2021-27180)
999255	CVE-2021-24340	WEB-WORDPRESS WP Statistics Vor 13.0.8 - Sicherheitslücke bei nicht authentifizierter SQL-Injection (CVE-2021-24340)
999256	CVE-2021-24171	WEB-WORDPRESS WooCommerce Dateien hochladen Plugin vor 59.4 - Sicherheitslücke bei Pfaddurchqueren (CVE-2021-24171)

Regel zur Unterschrift	CVE-ID	Beschreibung
999257	CVE-2021-24171	WEB-WORDPRESS WooCommerce Upload-Datei-Plugin vor 59.4 - Schwachstelle für willkürliche Datei-Upload (CVE-2021-24171)
999258	CVE-2021-22658	WEB-MISC Advantech iView Vor 5.7.03.6112 - Sicherheitslücke in SQLi über UserServlet und user_password (CVE-2021-22658)
999259	CVE-2021-22658	WEB-MISC Advantech iView Vor 5.7.03.6112 - Sicherheitslücke in SQLi über UserServlet und user_name (CVE-2021-22658)
999260	CVE-2021-22658	WEB-MISC Advantech iView Vor 5.7.03.6112 - Sicherheitslücke in SQLi über CommandServlet und user_password (CVE-2021-22658)
999261	CVE-2021-22658	WEB-MISC Advantech iView Vor 5.7.03.6112 - Sicherheitslücke in SQLi über CommandServlet und user_name (CVE-2021-22658)
999262	CVE-2021-21983	WEB-MISC VMware vRealize Operations Manager vor 8.4 - Schwachstelle für willkürliche Dateischreiben (CVE-2021-21983)
999263	CVE-2020-6754	WEB-MISC dotCMS Vor 5.2.4 - Verzeichnisdurchquerung über Assets (CVE-2020-6754)

Regel zur Unterschrift	CVE-ID	Beschreibung
999264	CVE-2020-27128	WEB-MISC Cisco SD-WAN vManage Vor 20.3.1 - Schwachstelle für beliebige Datei-Schreibzugriff über Remoteprocessing (CVE-2020-27128)
999265	CVE-2020-27128	WEB-MISC Cisco SD-WAN vManage Vor 20.3.1 - Schwachstelle für beliebige Datei-Schreibzugriff über dr (CVE-2020-27128)
999266	CVE-2020-15714	WEB-MISC RConfig 3.9.5 und früher - SQL Injection Sicherheitslücke (CVE-2020-15714)
999267	CVE-2020-15713	WEB-MISC RConfig Vor 3.9.6 - Sicherheitslücke in SQL Injection (CVE-2020-15713)
999268	CVE-2020-14295	WEB-MISC Cacti vor 1.2.13 - Sicherheitslücke bei SQL-Injection (CVE-2020-14295)
999269	CVE-2020-13778	WEB-MISC RConfig Vor 3.9.5 - Sicherheitslücke bei der Remote-Code-Ausführung über ajaxEditTemplate.php (CVE-2020-13778)
999270	CVE-2020-13778	WEB-MISC RConfig Vor 3.9.5 - Sicherheitslücke bei der Remote-Code-Ausführung über ajaxAddTemplate.php (CVE-2020-13778)

Regel zur Unterschrift	CVE-ID	Beschreibung
999271	CVE-2020-13592	WEB-MISC Rukovoditel Project Management App - Sicherheitslücke bei SQL-Injection über selected_fields (CVE-2020-13592)
999272	CVE-2020-13592	WEB-MISC Rukovoditel Project Management App - Sicherheitslücke bei SQL-Injection über lists_id (CVE-2020-13592)
999273	CVE-2020-13591	WEB-MISC Rukovoditel Projektmanagement-App - Sicherheitslücke bei SQL-Injection (CVE-2020-13591)
999274	CVE-2020-13550	WEB-MISC Advantech WebAccess/SCADA - Sicherheitslücke durch Pfaddurchquerung über FileName (CVE-2020-13550)

Signaturaktualisierung für Juli 2021

January 25, 2022

Für die in der Woche 2021-07-08 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 66 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden

Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999231	CVE-2021-34074	WEB-MISC Artica Pandora FMS Bis zu 7,54 - Schwachstelle für willkürliche Dateien über relativen Pfad (CVE-2021-34074)
999232	CVE-2021-32633	WEB-MISC Plone CMS - Zope-Seitenvorlagen Sicherheitslücke bei Remote-Codeausführung per Upload (CVE-2021-32633)
999233	CVE-2021-32633	WEB-MISC Plone CMS - Zope Page Templates Sicherheitslücke bei Remote-Codeausführung über Neu (CVE-2021-32633)
999234	CVE-2021-31181	WEB-MISC Microsoft SharePoint Server - Sicherheitslücke bei der Remote-Codeausführung (CVE-2021-31181)
999235	CVE-2021-24370	WEB-WORDPRESS Fancy Product Designer-Plugin vor 5.6.9 - RCE-Sicherheitslücke über fpd_custom_uplod_file (CVE-2021-24370)

Regel zur Unterschrift	CVE-ID	Beschreibung
999236	CVE-2021-24370	WEB-WORDPRESS Fancy Product Designer-Plugin vor 5.6.9 - RCE-Schwachstelle über custom-image-handler.php (CVE-2021-24370)
999237	CVE-2021-24354	WEB-WORDPRESS Simple 301 leitet Plugin vor 2.0.4 um - Schwachstelle für beliebige Plugin-Installation (CVE-2021-24354)
999238	CVE-2021-24352	WEB-WORDPRESS Simple 301 leitet Plugin vor 2.0.4 um - Exportschwachstelle umleiten (CVE-2021-24352)
999239	CVE-2021-1497, CVE-2021-1498	WEB-MISC Cisco HyperFlex HX Vor 4.0 (2e) - Sicherheitslücke bei der Remote-Code-Ausführung (CVE-2021-1497, CVE-2021-1498)
999240	CVE-2020-21057	WEB-MISC FusionPBx 4.5.7 - Sicherheitslücke durch Pfaddurchqueren über folderdelete (CVE-2020-21057)
999241	CVE-2020-16245	WEB-MISC Advantech iView Vor 5.7.03.6112 - Sicherheitslücke durch Pfaddurchquerungen über BackupDatabase (CVE-2020-16245)

Regel zur Unterschrift	CVE-ID	Beschreibung
999242	CVE-2020-10148	WEB-MISC SolarWinds Orion Mehrere Versionen - Authentifizierung umgehen Sicherheitslücke (CVE-2020-10148)

Signatur-Update für August 2021

January 25, 2022

Für die in der Woche 2021-08-29 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 67 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999183	CVE-2021-37557	WEB-MISC Centreon Mehrere Versionen - Sicherheitslücke in SQL Injection (CVE-2021-37557)

Regel zur Unterschrift	CVE-ID	Beschreibung
999184	CVE-2021-35501	WEB-MISC Artica Pandora FMS Bis zu 7,54 - Gespeicherte XSS-Schwachstelle in Visual Console (CVE-2021-35501)
999185	CVE-2021-35464	WEB-MISC ForgeRock Access Management und OpenAM - Sicherheitslücke bei der Remote-Code-Ausführung (CVE-2021-35464)
999186	CVE-2021-34523	WEB-MISC Microsoft Exchange Server - Erhöhung der Berechtigungsschwachstelle (CVE-2021-34523)
999187	CVE-2021-34473	WEB-MISC Microsoft Exchange Server - Serverseitige Authentifizierung bei Fälschungsauthentifizierung umgehen Schwachstelle per Abfrage (CVE-2021-34473)
999188	CVE-2021-34473	WEB-MISC Microsoft Exchange Server - serverseitige Authentifizierung bei Fälschungsanforderung umgehen Sicherheitslücke per Cookie (CVE-2021-34473)
999189	CVE-2021-33203	WEB-MISC Django - Schwachstelle für die Offenlegung von Dateien über den absoluten Pfad (CVE-2021-33203)
999190	CVE-2021-33203	WEB-MISC Django - Sicherheitslücke bei der Offenlegung von Dateien durch Pfad-Traversal (CVE-2021-33203)

Regel zur Unterschrift	CVE-ID	Beschreibung
999191	CVE-2021-33203	WEB-MISC Django - Schwachstelle für die Offenlegung von Dateien durch Backslash (CVE-2021-33203)
999192	CVE-2021-33203	WEB-MISC Django - Sicherheitslücke bei der Offenlegung von Dateien über Slash (CVE-2021-33203)
999193	CVE-2021-3287, CVE-2020-28653	WEB-MISC Zoho ManageEngine OpManager vor 12.5.329 - Nicht authentifizierte RCE-Schwachstelle (CVE-2021-3287, CVE-2020-28653)
999194	CVE-2021-32789	WEB-WORDPRESS WooCommerce-Plugin Bis zu 5.5.0 - SQL Injection Schwachstelle über Taxonomie und rest_route (CVE-2021-32789)
999195	CVE-2021-32789	WEB-WORDPRESS WooCommerce-Plugin Bis zu 5.5.0 - SQL Injection Schwachstelle über Taxonomie (CVE-2021-32789)
999196	CVE-2021-32604	WEB-MISC SolarWinds Serv-U Vor 15.2.3 - Sicherheitsrisiko durch Cross-Site Scripting über SenderEmail-Parameter (CVE-2021-32604)

Regel zur Unterschrift	CVE-ID	Beschreibung
999197	CVE-2021-32093	WEB-MISC National Security Agency Abgesandter 5.9.0 - Schwachstelle für willkürliche Dateien zum Lesen von Dateien (CVE-2021-32093)
999198	CVE-2021-31760	WEB-MISC Webmin Vor 1.974 - CSRF-Schwachstelle führt über run.cgi zu RCE (CVE-2021-31760)
999199	CVE-2021-31207	WEB-MISC Microsoft Exchange Server - Sicherheitsfunktion umgehen Schwachstelle (CVE-2021-31207)
999200	CVE-2021-31195	WEB-MISC Microsoft Exchange Server - Vunerability für Remote-Codeausführung (CVE-2021-31195)
999201	CVE-2021-28474	WEB-MISC Microsoft SharePoint Server - Sicherheitslücke bei der Remote-Codeausführung (CVE-2021-28474)
999202	CVE-2021-24385	WEB-WORDPRESS FileBird Plugin 4.7.3 - Sicherheitslücke in SQL Injection über SelectedFolder-Parameter und rest_route (CVE-2021-24385)
999203	CVE-2021-24385	WEB-WORDPRESS FileBird Plugin 4.7.3 - Sicherheitslücke in SQL Injection über SelectedFolder-Parameter (CVE-2021-24385)

Regel zur Unterschrift	CVE-ID	Beschreibung
999204	CVE-2021-24385	WEB-WORDPRESS FileBird Plugin 4.7.3 - Sicherheitslücke bei SQL-Injection über JSON-kodierten Körper (CVE-2021-24385)
999205	CVE-2021-24356	WEB-WORDPRESS Simple 301 leitet Plugin vor 2.0.4 um - Schwachstelle für willkürliche Plugin-Aktivierung (CVE-2021-24356)
999206	CVE-2021-23024	WEB-MISC F5 BIG-IQ Mehrere Versionen - Sicherheitslücke bei der Remote-Codeausführung (CVE-2021-23024)
999207	CVE-2021-22911	WEB-MISC Rocket.Chat Server 3.11, 3.12 und 3.13 - Blinde NOSQL-Injection Sicherheitslücke (CVE-2021-22911)
999208	CVE-2021-22900	WEB-MISC Pulse Connect Secure vor 9.1R11.4 - Sicherheitslücke bei Remote-Code-Ausführung über smimeCert.cgi (CVE-2021-22900)
999209	CVE-2021-22900	WEB-MISC Pulse Connect Secure vor 9.1R11.4 - Sicherheitslücke bei Remote-Code-Ausführung über admincert.cgi (CVE-2021-22900)

Regel zur Unterschrift	CVE-ID	Beschreibung
999210	CVE-2021-22900	WEB-MISC Pulse Connect Secure vor 9.1R11.4 - Sicherheitslücke bei Remote-Code-Ausführung über clientauthcert.cgi (CVE-2021-22900)
999211	CVE-2021-22160	WEB-MISC Apache Pulsar - JSON-Web-Token-Authentifizierung umgehen Sicherheitslücke (CVE-2021-22160)
999212	CVE-2021-21809	WEB-MISC Moodle - Sicherheitslücke bei der Remote-Codeausführung über das Spellchecker-Plugin und die GetSuggestions Methode (CVE-2021-21809)
999213	CVE-2021-21809	WEB-MISC Moodle - Sicherheitslücke bei der Remote-Codeausführung über das Rechtschreibprüfung Plugin und CheckWords Methode (CVE-2021-21809)
999214	CVE-2021-21809	WEB-MISC Moodle - Sicherheitslücke bei der Remote-Codeausführung über s__aspellpath (CVE-2021-21809)
999215	CVE-2021-21805	WEB-MISC Advantech R-SeeNet - Sicherheitslücke bei nicht authentifizierter Remote-Code-Ausführung (CVE-2021-21805)

Regel zur Unterschrift	CVE-ID	Beschreibung
999216	CVE-2021-21804	WEB-MISC Advantech R-SeeNet - Sicherheitslücke bei lokaler Dateieinbeziehung über sub_opt (CVE-2021-21804)
999217	CVE-2021-21587	WEB-MISC Dell Wyse Management Suite vor 3.3 - Sicherheitslücke im Pfaddurchgang über /image/os/listfiles (CVE-2021-21587)
999218	CVE-2021-21587	WEB-MISC Dell Wyse Management Suite vor 3.3 - Sicherheitslücke im Pfaddurchgang über /image/app/rsp/listfiles (CVE-2021-21587)
999219	CVE-2021-21586	WEB-MISC Dell Wyse Management Suite vor 3.3 - Sicherheitslücke durch Pfaddurchquerung via /image/app und FileName (CVE-2021-21586)
999220	CVE-2021-21586	WEB-MISC Dell Wyse Management Suite vor 3.3 - Sicherheitslücke durch Pfaddurchquerung über /image/os und FileName (CVE-2021-21586)
999221	CVE-2021-21586	WEB-MISC Dell Wyse Management Suite vor 3.3 - Sicherheitslücke durch Pfaddurchquerung über /image/os und FilePath (CVE-2021-21586)

Regel zur Unterschrift	CVE-ID	Beschreibung
999222	CVE-2020-25223	WEB-MISC Sophos SG UTM - Remote-Codeausführung über SID und /var (CVE-2020-25223)
999223	CVE-2020-25223	WEB-MISC Sophos SG UTM - Remote-Codeausführung über SID und/webadmin.plx (CVE-2020-25223)
999224	CVE-2020-21056	WEB-MISC FusionPBx 4.5.7 - Sicherheitslücke durch Pfaddurchqueren über foldernew (CVE-2020-21056)
999225	CVE-2020-21055	WEB-MISC FusionPBx 4.5.7 - Sicherheitslücke durch Pfaddurchquerung per Funktion zum Umbenennen von Dateien (CVE-2020-21055)
999226	CVE-2020-16245	WEB-MISC Advantech iView Vor 5.7.03.6112 - Sicherheitslücke in FindSummaryUpdateDeviceListExpo (CVE-2020-16245)
999227	CVE-2020-16245	WEB-MISC Advantech iView Vor 5.7.03.6112 - Sicherheitslücke durch Pfaddurchqueren über findCfgDeviceListExport (CVE-2020-16245)
999228	CVE-2020-14181	WEB-MISC Atlassian Jira Server - Sicherheitslücke bei der Offenlegung von Informationen über ViewUserHover.jspa (CVE-2020-14181)

Regel zur Unterschrift	CVE-ID	Beschreibung
999229	CVE-2020-14005	WEB-MISC SolarWinds Orion Vor 2020.2.1 HF 2 - Remote-Code-Ausführung über ExecuteVBScript-Aktionstyp (CVE-2020-14005)
999230	CVE-2020-14005	WEB-MISC SolarWinds Orion Vor 2020.2.1 HF 2 - Remote-Code-Ausführung über ExecuteExternalProgram Aktionstyp (CVE-2020-14005)

Signatur-Update für September 2021

January 25, 2022

Für die in der Woche 2021-09-11 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 68 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999163	CVE-2021-37556	WEB-MISC Centreon Mehrere Versionen - Sicherheitslücke bei SQL-Injection über Endparameter (CVE-2021-37556)
999164	CVE-2021-37556	WEB-MISC Centreon Mehrere Versionen - Sicherheitslücke bei SQL-Injection über Startparameter (CVE-2021-37556)
999165	CVE-2021-37353	WEB-MISC Nagios XI Docker-Assistent vor 1.1.3 - SSRF-Schwachstelle über Host-Parameter ohne URI-Schema (CVE-2021-37353)
999166	CVE-2021-37353	WEB-MISC Nagios XI Docker-Assistent vor 1.1.3 - SSRF-Schwachstelle über Host-Parameter mit URI-Schema (CVE-2021-37353)
999167	CVE-2021-34638	WEB-WORDPRESS Download-Manager-Plugin vor 3.1.25 — Sicherheitslücke durch Directory-Traversal (CVE-2021-34638)
999168	CVE-2021-33766	WEB-MISC Microsoft Exchange Server - Sicherheitslücke bei der Offenlegung von Informationen (CVE-2021-33766)
999169	CVE-2021-32682	WEB-MISC ElFinder vor 2.1.59 - Sicherheitslücke durch Command Injection über Archiv (CVE-2021-32682)

Regel zur Unterschrift	CVE-ID	Beschreibung
999170	CVE-2021-26084	WEB-MISC Confluence Server und Rechenzentrum - OGNL Injection Sicherheitslücke über doenterpagevariablen (CVE-2021-26084)
999171	CVE-2021-26084	WEB-MISC Confluence Server und Rechenzentrum - OGNL Injection Sicherheitslücke Über createpage-entervariable (CVE-2021-26084)
999172	CVE-2021-23394	WEB-MISC ElFinder vor 2.1.59 - Sicherheitslücke bei der Remotecodeausführung über Phar Makefile (CVE-2021-23394)
999173	CVE-2021-23394	WEB-MISC ElFinder vor 2.1.59 - Sicherheitslücke bei der Remotecodeausführung über Phar Rename (CVE-2021-23394)
999174	CVE-2021-23394	WEB-MISC ElFinder vor 2.1.59 - Sicherheitslücke bei der Remotecodeausführung über Phar-Upload (CVE-2021-23394)
999175	CVE-2020-36289	WEB-MISC Atlassian Jira Server - Sicherheitslücke bei der Offenlegung von Informationen über QueryComponentRender-erValue (CVE-2020-36289)

Regel zur Unterschrift	CVE-ID	Beschreibung
999176	CVE-2020-16245	WEB-MISC Advantech iView vor 5.7.03.6112 - Sicherheitslücke durch Pfad-Traversal über FindSummaryCFGDeviceListExport (CVE-2020-16245)
999177	CVE-2020-16245	WEB-MISC Advantech iView vor 5.7.03.6112 - Sicherheitslücke durch Pfaddurchlauf über FindUpdateDeviceListExport (CVE-2020-16245)
999178	CVE-2020-13774	WEB-MISC Ivanti Endpoint Manager Mehrere Versionen — RCE-Schwachstelle über EditLaunchPadDialog.aspx (CVE-2020-13774)
999179	CVE-2020-1147	WEB-MISC Microsoft SharePoint Server - Sicherheitslücke bei Remotecodeausführung über benutzerdefinierte Seite (CVE-2020-1147)
999180	CVE-2020-1147	WEB-MISC Microsoft SharePoint Server — Sicherheitslücke bei der Remotecodeausführung über quicklinksdialogform.aspx (CVE-2020-1147)
999181	CVE-2020-1147	WEB-MISC Microsoft SharePoint Server — Sicherheitslücke bei der Remotecodeausführung über quicklinks.aspx (CVE-2020-1147)

Regel zur Unterschrift	CVE-ID	Beschreibung
999182	CVE-2020-11110	WEB-MISC Apache Grafana Bis zu 6.7.1 - XSS Sicherheitslücke (CVE-2020-11110)
999522	CVE-2020-13379	WEB-MISC Grafana 3.0.1 bis 7.0.1 - CSRF-Bypass führt zu DOS-Schwachstelle (CVE-2020-13379)

Signatur-Update für Oktober 2021

January 25, 2022

Für die in der Woche 2021-10-09 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 69 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999149	CVE-2021-38312	WEB-WORDPRESS Gutenberg-Vorlagenbibliothek und Redux Framework-Plugin vor 4.2.12 - Sicherheitslücke REST_ROUTE (CVE-2021-38312)
999150	CVE-2021-38312	WEB-WORDPRESS Gutenberg-Vorlagenbibliothek und Redux Framework-Plugin vor 4.2.12 - REST-API-Schwachstelle (CVE-2021-38312)
999151	CVE-2021-34639	WEB-WORDPRESS Download-Manager-Plugin vor 3.1.25 — Sicherheitslücke beim Hochladen doppelter Erweiterungen (CVE-2021-34639)
999152	CVE-2021-34621	WEB-WORDPRESS ProfilePress Plugin vor 3.1.3 — Erhöhung der Sicherheitslücke durch wp_abilities (CVE-2021-34621)
999153	CVE-2021-32682	WEB-MISC ElFinder vor 2.1.59 — Schwachstelle bei Pfaddurchquerung per Umbenennungsbefehl (CVE-2021-32682)
999154	CVE-2021-32682	WEB-MISC ElFinder vor 2.1.59 — Schwachstelle bei Pfaddurchquierung per Abbruchbefehl (CVE-2021-32682)

Regel zur Unterschrift	CVE-ID	Beschreibung
999155	CVE-2021-26086	WEB-MISC Atlassian Jira Server und Rechenzentrum — Sicherheitslücke bei Offenlegung von Informationen über WEB-INF (CVE-2021-26086)
999156	CVE-2021-26086	WEB-MISC Atlassian Jira Server und Rechenzentrum — Sicherheitslücke bei Offenlegung von Informationen über META-INF (CVE-2021-26086)
999157	CVE-2021-22005	WEB-MISC VMware vCenter — Sicherheitslücke beim Hochladen von Dateien via Daten-App (CVE-2021-22005)
999158	CVE-2021-22005	WEB-MISC VMware vCenter — Sicherheitslücke beim Hochladen von Dateien über Telemetrie-Phase Log (CVE-2021-22005)
999159	CVE-2021-22005	WEB-MISC VMware vCenter — Sicherheitslücke beim Hochladen von Dateien über Telemetrie Prod Log (CVE-2021-22005)
999160	CVE-2021-20081	WEB-MISC Zoho ManageEngine Service Desk vor 11.2.0.5 — Sicherheitslücke bei der Remote-Codeausführung (CVE-2021-20081)

Regel zur Unterschrift	CVE-ID	Beschreibung
999161	CVE-2020-29453	WEB-MISC Atlassian Jira Server und Rechenzentrum — Sicherheitslücke bei Offenlegung von Informationen über WEB-INF (CVE-2020-29453)
999162	CVE-2020-29453	WEB-MISC Atlassian Jira Server und Rechenzentrum — Sicherheitslücke bei Offenlegung von Informationen über META-INF (CVE-2020-29453)

Signatur-Update für Oktober 2021

January 25, 2022

Für die in der Woche 2021-10-26 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 70 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999127	CVE-2021-42013	WEB-MISC Apache HTTP Server 2.4.49 and 2.4.50 - Path Traversal Vulnerability Via %%32 (CVE-2021-42013)
999128	CVE-2021-42013	WEB-MISC Apache HTTP Server 2.4.49 and 2.4.50 - Path Traversal Vulnerability Via %2% (CVE-2021-42013)
999129	CVE-2021-41773	WEB-MISC Apache HTTP Server 2.4.49 - Path Traversal Vulnerability Via %2e%2e (CVE-2021-41773)
999130	CVE-2021-41773	WEB-MISC Apache HTTP Server 2.4.49 - Path Traversal Vulnerability Via .%2e (CVE-2021-41773)
999131	CVE-2021-40539	WEB-MISC Zoho ManageEngine AdSelfService Plus 6.1 vor dem Bau 6114 — Sicherheitslücke durch Umgehung der Authentifizierung (CVE-2021-40539)
999132	CVE-2021-34648	WEB-WORDPRESS Ninja Forms Plugin Bis zu 3.5.7 - REST_ROUTE Sicherheitslücke über E-Mail-Aktion für Einsendungen (CVE-2021-34648)
999133	CVE-2021-34648	WEB-WORDPRESS Ninja Forms Plugin Bis zu 3.5.7 - REST-API-Schwachstelle über E-Mail-Aktion für Einsendungen (CVE-2021-34648)

Regel zur Unterschrift	CVE-ID	Beschreibung
999134	CVE-2021-34647	WEB-WORDPRESS Ninja Forms Plugin Bis zu 3.5.7 - REST_ROUTE Sicherheitslücke über Einreichungen Export (CVE-2021-34647)
999135	CVE-2021-34647	WEB-WORDPRESS Ninja Forms Plugin Bis zu 3.5.7 - REST-API-Schwachstelle über Einreichungen Export (CVE-2021-34647)
999136	CVE-2021-34623	WEB-WORDPRESS ProfilePress Plugin vor 3.1.4 — Sicherheitslücke beim Hochladen beliebiger Dateien über eup_cover_image (CVE-2021-34623)
999137	CVE-2021-34623	WEB-WORDPRESS ProfilePress Plugin vor 3.1.4 — Sicherheitslücke beim Hochladen beliebiger Dateien über eup_avatar (CVE-2021-34623)
999138	CVE-2021-2400	WEB-MISC Oracle BI Publisher - SaxParser XXE-Schwachstelle über Mobilgerät X ReportTemplateService (CVE-2021-2400)
999139	CVE-2021-2400	WEB-MISC Oracle BI Publisher - SaxParser XXE-Schwachstelle über mobilen ReportTemplateService (CVE-2021-2400)

Regel zur Unterschrift	CVE-ID	Beschreibung
999140	CVE-2021-2400	WEB-MISC Oracle BI Publisher - SaxParser XXE-Schwachstelle über xmlpservice X ReportTemplateService (CVE-2021-2400)
999141	CVE-2021-2400	WEB-MISC Oracle BI Publisher - SaxParser XXE-Schwachstelle über xmlpservice ReportTemplateService (CVE-2021-2400)
999142	CVE-2021-21985	WEB-MISC VMware vCenter — Sicherheitsrisiko für Virtual SAN Health Check Plugin zur Remote-Codeausführung (CVE-2021-21985)
999143	CVE-2021-20078	WEB-MISC Zoho ManageEngine OpManager 12.5 Vor dem Bau 125362 — Schwachstelle durch Pfaddurchquerung (CVE-2021-20078)
999144	CVE-2020-29448	WEB-MISC Atlassian Confluence Server und Rechenzentrum — Sicherheitsrisiko durch Offenlegung von Informationen über WEB-INF (CVE-2020-29448)
999145	CVE-2020-29448	WEB-MISC Atlassian Confluence Server und Rechenzentrum — Sicherheitsrisiko durch Offenlegung von Informationen über META-INF (CVE-2020-29448)

Regel zur Unterschrift	CVE-ID	Beschreibung
999146	CVE-2020-12442	WEB-MISC Ivanti Avalanche 6.3 — Sicherheitsrisiko durch Einschleusung von nicht authentifizierte, SQL über osupdate-Endpunkt (CVE-2020-12442)
999147	CVE-2020-12442	WEB-MISC Ivanti Avalanche 6.3 — Sicherheitslücke bei nicht authentifizierter SQL-Injection über einen Wapl-Endpunkt (CVE-2020-12442)
999148		WEB-WORDPRESS BuddyPress-Plugin Vor 9.1.1 - Sicherheitslücke bei SQL-Injection über bp-Members-Einladungsfunktion

Signatur-Update für November 2021

January 25, 2022

Für die in der Woche 2021-11-18 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 71 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU

> auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999098	CVE-2021-41765	WEB-MISC ResourceSpace 9.5 und 9.6 vor Rev. 18274 — Sicherheitslücke in SQL Injection (CVE-2021-41765)
999099	CVE-2021-41288	WEB-MISC Zoho ManageEngine OpManager Vor Build 125467 — Sicherheitslücke bei SQL-Injection über die GetReportData-API (CVE-2021-41288)
999100	CVE-2021-40493	WEB-MISC Zoho ManageEngine OpManager vor Build 125437 — Sicherheitslücke bei SQL-Injection über DeviceName (CVE-2021-40493)
999101	CVE-2021-40493	WEB-MISC Zoho ManageEngine OpManager vor Build 125437 — Sicherheitslücke bei SQL-Injection über PollingObject (CVE-2021-40493)
999102	CVE-2021-40438	WEB-MISC Apache HTTP-Server — mod_proxy Sicherheitslücke zur Weiterleitung von Anfragen (CVE-2021-40438)

Regel zur Unterschrift	CVE-ID	Beschreibung
999103	CVE-2021-39341	WEB-WORDPRESS OptinMonster Plugin Bis zu 2.6.4 — Sicherheitslücke durch Umgehung von REST_ROUTE-Berechtigungen (CVE-2021-39341)
999104	CVE-2021-39341	WEB-WORDPRESS OptinMonster Plugin Bis zu 2.6.4 — Sicherheitslücke durch Umgehung von REST-API-Berechtigungen (CVE-2021-39341)
999105	CVE-2021-37344	WEB-MISC Nagios XI Switch Wizard vor 2.5.7 — Sicherheitslücke bei der Remote-Codeausführung über den Parameter ip_address (CVE-2021-37344)
999106	CVE-2021-35218	WEB-MISC SolarWinds Orion Vor 2020.2.6 — Sicherheitslücke bei Deserialisierung über Chart.ashx (CVE-2021-35218)
999107	CVE-2021-35215	WEB-MISC SolarWinds Orion Platform vor 2020.2.6 — Sicherheitsrisiko durch Remote-Codeausführung über Reporting (CVE-2021-35215)
999108	CVE-2021-35215	WEB-MISC SolarWinds Orion Platform vor 2020.2.6 — Sicherheitslücke bei der Remote-Codeausführung durch Alerting (CVE-2021-35215)

Regel zur Unterschrift	CVE-ID	Beschreibung
999109	CVE-2021-24889	WEB-WORDPRESS Ninja Forms Plugin vor 3.6.4 — Sicherheitslücke durch SQL-Injection (CVE-2021-24889)
999110	CVE-2021-24381	WEB-WORDPRESS Ninja Forms Plugin vor 3.5.8.2 — Benutzerdefinierter Klassenname gespeicherte Cross-Site-Scripting-Schwachstelle (CVE-2021-24381)
999111	CVE-2021-2401	WEB-MISC Oracle BI Publisher - DomParser XXE-Schwachstelle über Mobilgerät X ReportTemplateService (CVE-2021-2401)
999112	CVE-2021-2401	WEB-MISC Oracle BI Publisher - domParser XXE-Schwachstelle über mobilen ReportTemplateService (CVE-2021-2401)
999113	CVE-2021-2401	WEB-MISC Oracle BI Publisher - domParser XXE-Schwachstelle über xmlpservice X ReportTemplateService (CVE-2021-2401)
999114	CVE-2021-2401	WEB-MISC Oracle BI Publisher - domParser XXE-Schwachstelle über xmlpservice ReportTemplateService (CVE-2021-2401)

Regel zur Unterschrift	CVE-ID	Beschreibung
999115	CVE-2021-2392	WEB-MISC Oracle BI Publisher — Sicherheitslücke beim Hochladen beliebiger Dateien (CVE-2021-2392)
999116	CVE-2021-2244	WEB-MISC Oracle Hyperion-Essbase Analytic Provider Services — Sicherheitslücke bei der Remote-Codeausführung über Essbase (CVE-2021-2244)
999117	CVE-2021-2244	WEB-MISC Oracle Hyperion-Essbase Analytic Provider Services — Sicherheitslücke bei Remote-Codeausführung über Administrator (CVE-2021-2244)
999118	CVE-2021-2244	WEB-MISC Oracle Hyperion-Essbase Analytic Provider Services — Sicherheitsrisiko durch Remote-Codeausführung über JAPI (CVE-2021-2244)
999119	CVE-2021-22205	WEB-MISC GitLab CE/EE - Sicherheitslücke bei der Remote-Codeausführung durch böswillig gestaltete JPEG/TIFF-Dateien (CVE-2021-22205)
999120	CVE-2021-22017	WEB-MISC VMWare vCenter - Path Traversal Vulnerability Via rhhtproxy (CVE-2021-22017)

Regel zur Unterschrift	CVE-ID	Beschreibung
999121	CVE-2021-20837	WEB-MISC beweglicher Typ vor r.5003 - Remote-Codeausführung über mt.handler_to_coderef (CVE-2021-20837)
999122	CVE-2021-20131	WEB-MISC Zoho ManageEngine AdManager vor Build 7115 — Sicherheitslücke bei Remote-Codeausführung durch Dateiupload (CVE-2021-20131)
999123	CVE-2021-20130	WEB-MISC Zoho ManageEngine AdManager vor Build 7115 — Sicherheitslücke bei Remote-Codeausführung durch Dateiupload (CVE-2021-20130)
999124	CVE-2021-20034	WEB-MISC SonicWall Secure Mobile Access — Schwachstelle durch Pfaddurchqueren (CVE-2021-20034)
999125		WEB-WORDPRESS BuddyPress-Plugin Vor 9.1.1 — Sicherheitslücke bei Offenlegung von Informationen über die Anmeldung REST API und rest_route

Regel zur Unterschrift	CVE-ID	Beschreibung
999126		WEB-WORDPRESS BuddyPress Plugin vor 9.1.1 - Sicherheitslücke bei Offenlegung von Informationen über die Anmeldung REST-API

Signatur-Update für Dezember 2021

January 25, 2022

Für die in der Woche 2021-12-11 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 72 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999077	CVE-2021-44228	WEB-MISC Apache Log4j — Sicherheitsrisiko durch Remotecodeausführung via FORM (CVE-2021-44228)

Regel zur Unterschrift	CVE-ID	Beschreibung
999078	CVE-2021-44228	WEB-MISC Apache LOG4j - Sicherheitsrisiko durch Remotecodeausführung über BODY (CVE-2021-44228)
999079	CVE-2021-44228	WEB-MISC Apache Log4j — Sicherheitsrisiko durch Remotecodeausführung über HEADER (CVE-2021-44228)
999080	CVE-2021-44228	WEB-MISC Apache Log4j — Sicherheitsrisiko durch Remotecodeausführung über URL (CVE-2021-44228)
999081	CVE-2021-42847	WEB-MISC Zoho ManageEngine AdAudit Plus vor 7006 — Sicherheitsrisiko durch Schreiben willkürlicher Dateien ohne Authentifizierung (CVE-2021-42847)
999082	CVE-2021-42321	WEB-MISC Microsoft Exchange Server — Sicherheitsrisiko durch Remotecodeausführung (CVE-2021-42321)
999083	CVE-2021-42258	WEB-MISC BQE BillQuick Web Suite 2021 — Sicherheitsrisiko durch nicht authentifizierter SQL-Einschleusung über txtID (CVE-2021-42258)
999084	CVE-2021-42258	WEB-MISC BQE BillQuick Web Suite 2020 — Sicherheitsrisiko durch nicht authentifizierter SQL-Einschleusung über txtID (CVE-2021-42258)

Regel zur Unterschrift	CVE-ID	Beschreibung
999085	CVE-2021-42258	WEB-MISC BQE BillQuick Web Suite 2019 — Sicherheitsrisiko durch nicht authentifizierter SQL-Einschleusung über txtID (CVE-2021-42258)
999086	CVE-2021-42258	WEB-MISC BQE BillQuick Web Suite 2018 — Sicherheitsrisiko durch nicht authentifizierter SQL-Einschleusung über txtID (CVE-2021-42258)
999087	CVE-2021-42237	WEB-MISC Sitecore von 7.5.0 bis 8.2.7 — Sicherheitsrisiko durch Remotecodeausführung (CVE-2021-42237)
999088	CVE-2021-41950	WEB-MISC ResourceSpace 9.6 vor Rev. 18277 — Sicherheitsrisiko durch nicht authentifizierte Pfaddurchquerung über Variante (CVE-2021-41950)
999089	CVE-2021-41950	WEB-MISC ResourceSpace 9.6 vor Rev. 18277 — Sicherheitsrisiko durch nicht authentifizierte Pfaddurchquerung via Provider (CVE-2021-41950)
999090	CVE-2021-41349	WEB-MISC Microsoft Exchange Server — Sicherheitsrisiko durch Cross-Site Scripting (CVE-2021-41349)
999091	CVE-2021-35217	WEB-MISC SolarWinds Orion vor 2020.2.6 HF1 — Deserial-isierungsschwachstelle über WSAsyncExecuteTasks.aspx (CVE-2021-35217)

Regel zur Unterschrift	CVE-ID	Beschreibung
999092	CVE-2021-34416	WEB-MISC Zoom Meeting Connector 4.6.360.20210325 — Sicherheitsrisiko durch Remotecodeausführung (CVE-2021-34416)
999093	CVE-2021-22941	WEB-MISC Citrix ShareFile-Speicher vor 5.11.20 — Sicherheitsrisiko durch unsachgemäßer Zugriffssteuerung (CVE-2021-22941)
999094	CVE-2020-35136	WEB-MISC Dolibarr vor 12.0.4 - Sicherheitsrisiko durch Remotecodeausführung über zipfilename_template und bz (CVE-2020-35136)
999095	CVE-2020-35136	WEB-MISC Dolibarr vor 12.0.4 - Sicherheitsrisiko durch Remotecodeausführung über zipfilename_template und gz (CVE-2020-35136)
999096	CVE-2020-2950, CVE-2021-2456	WEB-MISC Oracle BI Publisher — Schwachstelle beim Hochladen beliebiger Dateien (CVE-2020-2950, CVE-2021-2456)
999097	CVE-2020-2950, CVE-2021-2456	WEB-MISC Oracle BI Publisher — Sicherheitsrisiko durch Remotecodeausführung (CVE-2020-2950, CVE-2021-2456)

Signatur-Update für Dezember 2021

January 25, 2022

Für die in der Woche 2021-12-13 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Die Signaturversion 73 ist mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung, die aktualisiert werden.

> **Hinweis:**
>
> Die folgenden Signaturregeln (999077, 999078, 999079, 999080) richten sich an beide CVEs (CVE-2021-44228 und CVE-2021-45046).

Regel zur Unterschrift	CVE-ID	Beschreibung
999077	CVE-2021-44228, CVE-2021-45046	WEB-MISC Apache Log4j — Sicherheitsrisiko durch Remotecodeausführung über FORM (CVE-2021-44228, CVE-2021-45046)
999078	CVE-2021-44228, CVE-2021-45046	WEB-MISC Apache Log4j - Sicherheitsrisiko durch Remotecodeausführung über BODY (CVE-2021-44228, CVE-2021-45046)

Regel zur Unterschrift	CVE-ID	Beschreibung
999079	CVE-2021-44228, CVE-2021-45046	WEB-MISC Apache Log4j — Sicherheitsrisiko durch Remotecodeausführung über HEADER (CVE-2021-44228, CVE-2021-45046)
999080	CVE-2021-44228, CVE-2021-45046	WEB-MISC Apache Log4j — Sicherheitsrisiko durch Remotecodeausführung über URL (CVE-2021-44228, CVE-2021-45046)

Signatur-Update für Dezember 2021

January 25, 2022

Für die in der Woche 2021-12-21 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturen sind mit den folgenden Softwareversionen von Citrix Application Delivery Controller (ADC) 11.1, 12.0, 12.1, 13.0 und 13.1 kompatibel.

Citrix ADC Version 12.0 hat das Ende der Lebensdauer (EOL) erreicht. Weitere Informationen finden Sie auf der Seite Lebenszyklus von Versionen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999073	CVE-2021-44077	WEB-MISC Zoho ManageEngine ServiceDesk Plus vor 11306 — PreAuth RCE-Schwachstelle über ImportTechnicians (CVE-2021-44077)
999074	CVE-2021-43798	WEB-MISC Apache Grafana 8.0.0 Bis zu 8.3.0 — Path Traversal Verwundbarkeit (CVE-2021-43798)
999075	CVE-2021-35216	WEB-MISC SolarWinds Orion vor 2020.2.6 — Deserial-isierungsschwachstelle über EditTopXX.aspx (CVE-2021-35216)
999076	CVE-2021-34993	WEB-MISC CommVault CommCell - CVSearchService Sicherheitsrisiko für Authentifizierung umgehen (CVE-2021-34993)

Signatur-Update für Januar 2022

January 28, 2022

Für die in der Woche 2022-01-20 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheit-sangriffen zu schützen.

Signaturversion

Signaturversion 75 gilt für NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 und Citrix ADC 13.0-Plattformen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999055	CVE-2021-44224	WEB-MISC Apache-HTTP-Server — Fehlgeformte UDS-Schwachstelle über Forward- und Reverse-Proxy (CVE-2021-44224)
999056	CVE-2021-43815	WEB-MISC Apache Grafana - TestData DB-Datenquell-Pfad-Durchlauf-Sicherheitsanfälligkeit (CVE-2021-43815)
999057	CVE-2021-43813	WEB-MISC Apache Grafana - Verwundbarkeit durch Pfaddurchquerung über Markdown (CVE-2021-43813)
999058	CVE-2021-43405	WEB-MISC FusionPBX vor 4.5.30 - OS-Befehlseinschleusung über fax_extension (CVE-2021-43405)
999059	CVE-2021-42392	WEB-MISC H2-Konsole vor 2.0.206 — Sicherheitsrisiko durch Remotecodeausführung (CVE-2021-42392)

Regel zur Unterschrift	CVE-ID	Beschreibung
999060	CVE-2021-42362	WEB-WORDPRESS Popular Post Plugin vor 5.3.3 - Sicherheitsrisiko durch Hochladen beliebiger Dateien (CVE-2021-42362)
999061	CVE-2021-42129	WEB-MISC Ivanti Avalanche vor 6.3.3 - Sicherheitsrisiko durch OS-Befehlseinschleusung über txtUpass (CVE-2021-42129)
999062	CVE-2021-42129	WEB-MISC Ivanti Avalanche vor 6.3.3 - Sicherheitsrisiko durch OS-Befehlseinschleusung über txtUname (CVE-2021-42129)
999063	CVE-2021-42129	WEB-MISC Ivanti Avalanche vor 6.3.3 - Sicherheitsrisiko durch OS-Befehlseinschleusung über txtUncPath (CVE-2021-42129)
999064	CVE-2021-40345	WEB-MISC Nagios XI vor 5.8.6 - Sicherheitsrisiko durch OS-Befehlseinschleusung über in böser Absicht erstellte ZIP-Datei (CVE-2021-40345)
999065	CVE-2021-37928	WEB-MISC Zoho ManageEngine AdManager Plus vor 7110 — Sicherheitslücke beim uneingeschränkten Hochladen von Dateien (CVE-2021-37928)

Regel zur Unterschrift	CVE-ID	Beschreibung
999066	CVE-2021-25037	WEB-WORDPRESS All-in-One-SEO-Plugin vor 4.1.5.3 - Sicherheitsanfälligkeit durch SQL-Injection über Objekte REST-API und rest_route
999067	CVE-2021-25037	WEB-WORDPRESS Alles in einem SEO-Plugin vor 4.1.5.3 - Sicherheitsrisiko durch SQL-Einschleusung über Objekte REST-API
999068	CVE-2021-25036	WEB-WORDPRESS All-in-One-SEO-Plugin vor 4.1.5.3 - Sicherheitsrisiko durch Berechtigungseskalation über REST-API und rest_route
999069	CVE-2021-25036	WEB-WORDPRESS All-in-One-SEO-Plugin vor 4.1.5.3 — Sicherheitsrisiko durch Berechtigungseskalation über REST-API
999070	CVE-2021-21917	WEB-MISC Advantech R-SeeNet vor 2.4.17 - Sicherheitsanfälligkeit durch SQL-Injection über ord (CVE-2021-21917)
999071	CVE-2021-20040	WEB-MISC SonicWall Secure Mobile Access — Sicherheitsrisiko durch Schreiben beliebiger Dateien (CVE-2021-20040)

Regel zur Unterschrift	CVE-ID	Beschreibung
999072	CVE-2021-20039	WEB-MISC SonicWall Secure Mobile Access — Sicherheitsrisiko durch Befehlseinschleusung (CVE-2021-20039)

Signatur-Update für Februar 2022

February 24, 2022

Für die in der Woche 2022-02-20 identifizierten Sicherheitsrisikos werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 76 gilt für NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1 und Citrix ADC 13.0-Plattformen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999047	CVE-2022-23863	WEB-MISC FusionPBX vor 4.5.30 — OS-Befehlseinschleusung über fax_page_size (CVE-2021-43406)

Regel zur Unterschrift	CVE-ID	Beschreibung
999048	CVE-2021-44515	WEB-MISC JetBrains TeamCity — Sicherheitsrisiko durch Remotecodeausführung über Agent Push (CVE-2021-43193)
999049	CVE-2021-43406	WEB-MISC GoAhead vor 5.1.5 — Sicherheitsrisiko durch Einschleusung von CGI-Umgebungsvariablen (CVE-2021-42342)
999050	CVE-2021-43193	WEB-MISC SonicWall Secure Mobile Access — Sicherheitsrisiko durch Remotecodeausführen (CVE-2021-20045)
999051	CVE-2021-42342	WEB-MISC GoAhead vor 5.1.5 — Sicherheitsrisiko durch Einschleusung von CGI-Umgebungsvariablen (CVE-2021-42342)
999052	CVE-2021-20045	WEB-MISC SonicWall Secure Mobile Access — Sicherheitsrisiko durch Remotecodeausführen (CVE-2021-20045)
999053	CVE-2021-20044	WEB-MISC SonicWall Secure Mobile Access — Sicherheitsrisiko durch Befehlseinschleusung (CVE-2021-20044)
999054		WEB-WORDPRESS AdSanity-Plugin — Sicherheitsrisiko durch Remotecodeausführung über HTML5-Dateiupload

Signatur-Update für Februar 2022

March 8, 2022

Für die in der Woche 2022-02-25 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 77 gilt für NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 und Citrix ADC 13.1 Plattformen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Regel zur Unterschrift	CVE-ID	Beschreibung
999034		WEB-WORDPRESS WordPress 5.9 — Gespeicherte XSS-Sicherheitslücke über Seitenauszug im Json-Objekt
999035		WEB-WORDPRESS WordPress 5.9 — Gespeicherte XSS-Sicherheitslücke über Seitenauszug im Formular
999036		WEB-WORDPRESS WordPress 5.9 — Gespeicherte XSS-Schwachstelle über post.php
999037		WEB-WORDPRESS WordPress 5.9 — Gespeicherte XSS-Sicherheitslücke über Post-Auszug im Json-Objekt

Regel zur Unterschrift	CVE-ID	Beschreibung
999038		WEB-WORDPRESS WordPress 5.9 — Gespeicherte XSS-Sicherheitslücke über Post-Auszug im Formular
999039		WEB-MISC Anfälligkeit durch Pfaddurchgang über Formularfeld-Werte
999040		WEB-MISC-Pfad-Durchlauf-Schwachstelle über URI
999041	CVE-2022-23221	WEB-MISC H2-Konsole vor 2.1.210 — Sicherheitsanfälligkeit bei Remotecodeausführung über test.do (CVE-2022-23221)
999042	CVE-2022-23221	WEB-MISC H2-Konsole vor 2.1.210 — Sicherheitsanfälligkeit bei Remotecodeausführung über login.do (CVE-2022-23221)
999043	CVE-2022-21662	WEB-WORDPRESS WordPress vor 5.8.3 — Sicherheitsanfälligkeit für siteübergreifendes Skripting (CVE-2022-21662)
999044	CVE-2022-0320	WEB-WORDPRESS Die wesentlichen Addons für das Elementor-Plugin vor 5.0.5 - LFI über eael_product_gallery (CVE-2022-0320)
999045	CVE-2022-0320	WEB-WORDPRESS Die wesentlichen Addons für das Elementor-Plugin vor 5.0.5 - LFI über woo_product_pagination_product (CVE-2022-0320)

Regel zur Unterschrift	CVE-ID	Beschreibung
999046	CVE-2022-0320	WEB-WORDPRESS Die wesentlichen Addons für das Elementor-Plugin vor 5.0.5 - LFI über load_more (CVE-2022-0320)

Signatur-Update für März 2022

April 7, 2022

Für die in der Woche 2022-03-29 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor sicherheitsgefährdeten Angriffen zu schützen.

Signaturversion

Signaturversion 78 gilt für NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 und Citrix ADC 13.1 Plattformen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
999006		WEB-MISC Zabbix mehrere Versionen - Sicherheitsrisiko durch Remotecodeausführung über items.php

Signaturregel	CVE-ID	Beschreibung
999007	CVE-2022-24266	WEB-MISC Cuppa CMS v1.0 — Sicherheitsrisiko durch SQL-Einschleusung über order_orientation (CVE-2022-24266)
999008	CVE-2022-24266	WEB-MISC Cuppa CMS v1.0 — Sicherheitsrisiko durch SQL-Einschleusung über order_by (CVE-2022-24266)
999009	CVE-2022-22005	WEB-MISC Microsoft SharePoint — RCE-Sicherheitsrisiko durch Deserialisierung für nicht vertrauenswürdige Daten (CVE-2022-22005)
999010	CVE-2022-21705	WEB-MISC OctoberCMS vor Build 474 und v1.1.10 — Sicherheitsrisiko durch Remotecodeausführung (CVE-2022-21705)
999011	CVE-2022-0557	WEB-MISC Microweber vor 1.2.11 — Sicherheitsrisiko durch Remotecodeausführung (CVE-2022-0557)
999012	CVE-2022-0513	WEB-WORDPRESS WP-Statistik-Plugin vor 13.1.5 — Sicherheitsrisiko durch blinde SQL-Einschleusung (CVE-2022-0513)
999013	CVE-2022-0332	WEB-MISC Moodle 3.11.0 bis 3.11.4 — Sicherheitsrisiko durch SQL-Einschleusung über H5P-Aktivität (CVE-2022-0332)

Signaturregel	CVE-ID	Beschreibung
999014	CVE-2021-46088	WEB-MISC Zabbix Multiple Versions — Sicherheitsrisiko durch Remotecodeausführung (CVE-2021-46088)
999015	CVE-2021-43789	WEB-MISC PrestaShop vor 1.7.8.2 - Sicherheitsrisiko durch SQL-Einschleusung über sortOrder (CVE-2021-43789)
999016	CVE-2021-43789	WEB-MISC PrestaShop vor 1.7.8.2 - Sicherheitsrisiko durch SQL-Einschleusung über orderBy (CVE-2021-43789)
999017	CVE-2021-43408	WEB-WORDPRESS Post-Plugin Duplizieren vor 1.1.9 - Sicherheitsrisiko durch SQL-Einschleusung (CVE-2021-43408)
999018	CVE-2021-43319	WEB-MISC Zoho ManageEngine NCM vor 125488 — Sicherheitsrisiko durch Einschleusung von Betriebssystembefehlen (CVE-2021-43319)
999019	CVE-2021-41282	WEB-MISC pfSense 2.5.2 — Sicherheitsrisiko durch Remotecodeausführung (CVE-2021-41282)

Signaturregel	CVE-ID	Beschreibung
999020	CVE-2021-39115, CVE-2021-43947	WEB-MISC Atlassian Jira Server und Rechenzentrum — Sicherheitsrisiko durch Einschleusung von serverseitigen Vorlagen (CVE-2021-39115, CVE-2021-43947)
999021	CVE-2021-38452	WEB-MISC Moxa MXview Network Management vor 3.2.2 - Path Traversal Vulnerability (CVE-2021-38452)
999022	CVE-2021-37918	WEB-MISC Zoho ManageEngine AdManager Plus vor 7111 — Path Traversal Vulnerability über domainName (CVE-2021-37918)
999023	CVE-2021-37918	WEB-MISC Zoho ManageEngine AdManager Plus vor 7111 — Path Traversal Vulnerability über BM_OperationID (CVE-2021-37918)
999024	CVE-2021-37918	WEB-MISC Zoho ManageEngine AdManager Plus vor 7111 — RCE-Sicherheitsrisiko durch Hochladen beliebiger Dateien (CVE-2021-37918)
999025	CVE-2021-32649	WEB-MISC OctoberCMS vor Build 473 und v1.1.6 — Sicherheitsrisiko durch Remotecodeausführung über Twig (CVE-2021-32649)

Signaturregel	CVE-ID	Beschreibung
999026	CVE-2021-32648	WEB-MISC OctoberCMS vor Build 472 und v1.1.5 — Sicherheitsrisiko durch Zurücksetzen des Kennworts (CVE-2021-32648)
999027	CVE-2021-32099, CVE-2020-26518	WEB-MISC Artica Pandora vor 743 - Sicherheitsrisiko durch SQL-Einschleusung über chart_generator (CVE-2021-32099, CVE-2020-26518)
999028	CVE-2021-32098	WEB-MISC Artica Pandora vor 743 - Sicherheitsrisiko durch Phar-Deserialisierung über progressbubble (CVE-2021-32098)
999029	CVE-2021-32098	WEB-MISC Artica Pandora vor 743 - Sicherheitsrisiko durch Phar-Deserialisierung über Progressbar (CVE-2021-32098)
999030	CVE-2021-30149	WEB-MISC Composr 10.0.36 — Sicherheitsrisiko durch Remotecodeausführung (CVE-2021-30149)
999031	CVE-2021-25114	WEB-WORDPRESS Paid Memberships Pro Plugin vor 2.6.7 - Sicherheitsrisiko für SQLi über rest_route und discount_code (CVE-2021-25114)
999032	CVE-2021-25114	WEB-WORDPRESS Paid Memberships Pro Plugin vor 2.6.7 - Sicherheitsrisiko für SQLi über wp-json und discount_code (CVE-2021-25114)

Signaturregel	CVE-ID	Beschreibung
999033	CVE-2021-21984	WEB-MISC VMware vRealize Business for Cloud 7.x vor 7.6.0 — Sicherheitsrisiko durch Remotecodeausführung (CVE-2021-21984)

Signatur-Update für März 2022

April 7, 2022

Für die in der Woche 2022-03-29 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor sicherheitsgefährdeten Angriffen zu schützen.

Signaturversion

Signaturversion 79 gilt für NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 und Citrix ADC 13.1 Plattformen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
18959 (aktualisierte Regel)	CVE-2022-22965	WEB-MISC VMware Spring4Shell, SpringSource Spring Framework class.classloader RCE-Versuch

Signaturregel	CVE-ID	Beschreibung
999005	CVE-2022-22963	WEB-MISC Spring Cloud-Funktion — Sicherheitsrisiko durch Codeeinschleusung (CVE-2022-22963)

Signaturaktualisierung für April 2022

April 25, 2022

Für die in der Woche 2022-04-04 identifizierten Schwachstellen werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 80 gilt für NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 und Citrix ADC 13.1 Plattformen.

> **Hinweis:**
>
> Das Aktivieren von Postbody und Antworttextsignaturregeln kann sich auf die Citrix ADC CPU auswirken.

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
999004	CVE-2022-22965	WEB-MISC Spring4Shell Spring Core Framework — RCE-Schwachstelle (CVE-2022-22965)

Signaturaktualisierung für April 2022

April 25, 2022

Für die in der Woche 2022-04-08 identifizierten Sicherheitsrisiken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 81 gilt für NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0 und Citrix ADC 13.1 Plattformen.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
999001	CVE-2022-0479	WEB-WORDPRESS Popup Builder Plugin vor 4.1.1 — Sicherheitsrisiko durch SQL-Einschleusung (CVE-2022-0479)
999002	CVE-2021-36393	WEB-MISC Moodle vor 3.11.1 — Sicherheitsrisiko durch SQL-Einschleusung (CVE-2021-36393)
999003	CVE-2021-26599	WEB-MISC ImpressCMS vor 1.4.3 — Sicherheitsrisiko durch SQL-Einschleusung (CVE-2021-26599)

Signaturaktualisierung für April 2022

May 10, 2022

Neue Signaturregeln werden für die in der Woche 2022-04-23 identifizierten Sicherheitslücken generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 82 gilt für NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0, Citrix ADC 13.1 Plattformen.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann die Citrix ADC CPU beeinflussen

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998997	CVE-2022-27924	WEB-MISC Zimbra Collaboration Joule - Sicherheitsrisiko durch Cachevergiftung (CVE-2022-27924)
998998	CVE-2022-21907	WEB-MISC Microsoft HTTP-Protokollstapel — Sicherheitsrisiko durch Remotecodeausführung (CVE-2022-21907)
998999	CVE-2021-37930	WEB-MISC ManageEngine AdManager Plus vor 7111 — Sicherheitsrisiko durch Hochladen beliebiger Dateien über sm_domainName (CVE-2021-37930)

Signaturregel	CVE-ID	Beschreibung
999000	CVE-2021-37930	WEB-MISC ManageEngine AdManager Plus vor 7111 — Sicherheitsrisiko durch Hochladen beliebiger Dateien über sm_operationId (CVE-2021-37930)

Signatur-Update für Mai 2022

June 1, 2022

Neue Signaturregeln werden für die in der Woche 2022-05-04 identifizierten Sicherheitslücken generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 83 gilt für NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0, Citrix ADC 13.1 Plattformen.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998993	CVE-2022-29464	WEB-MISC WSO2 Mehrere Produkte — Sicherheitsrisiko durch uneingeschränkten Dateiupload (CVE-2022-29464)

Signaturregel	CVE-ID	Beschreibung
998994	CVE-2022-22954	WEB-MISC VMware Workspace ONE Access and Identity Manager — Sicherheitsrisiko durch Remotecodeausführung über deviceType (CVE-2022-22954)
998995	CVE-2022-22954	WEB-MISC VMware Workspace ONE Access and Identity Manager —Sicherheitsrisiko durch Remotecodeausführung über deviceUdid (CVE-2022-22954)
998996	CVE-2022-1329	WEB-WORDPRESS WordPress Elementor Website Builder Vor 3.6.3 - Sicherheitsrisiko durch unbefugte AJAX-Aktionen (CVE-2022-1329)

Signatur-Update für Mai 2022

June 1, 2022

Neue Signaturregeln werden für die in der Woche 2022-05-08 identifizierten Sicherheitsrisiken generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 84 gilt für die Plattformen NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0, Citrix ADC 13.1.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998988	CVE-2022-26986	WEB-MISC ImpressCMS vor 1.4.3 — Sicherheitsrisiko durch SQL-Einschleusung über mimetypeid (CVE-2022-26986)
998989	CVE-2022-24112	WEB-MISC Apache APISIX Batch-Request-Plugin — Sicherheitsrisiko durch Umgehen der IP-Einschränkung (CVE-2022-24112)
998990	CVE-2021-37558	WEB-MISC Centreon vor 20.04.14, 20.10.8 und 21.04.2 — Sicherheitsrisiko durch SQL-Einschleusung über service_description (CVE-2021-37558)
998991	CVE-2021-37558	WEB-MISC Centreon vor 20.04.14, 20.10.8 und 21.04.2 — Sicherheitsrisiko durch SQL-Einschleusung über host_name (CVE-2021-37558)
998992	CVE-2021-22056	WEB-MISC VMware Workspace ONE Access and Identity Manager — Sicherheitsrisiko für serverseitige Anforderungsfälschung (CVE-2021-22056)

Signatur-Update für Mai 2022

June 1, 2022

Neue Signaturregeln werden für die in der Woche 2022-05-13 identifizierten Sicherheitsrisiken generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 85 gilt für die Plattformen NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0, Citrix ADC 13.1.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998982	CVE-2022-26352	WEB-MISC dotCMS - Sicherheitsrisiko durch Hochladen beliebiger Dateien über PUT (CVE-2022-26352)
998983	CVE-2022-26352	WEB-MISC dotCMS - Sicherheitsrisiko durch Hochladen beliebiger Dateien über POST (CVE-2022-26352)
998984	CVE-2022-1388	WEB-MISC F5 BIG-IP - Sicherheitsrisiko durch Umgehen der iControl-REST-Authentifizierung (CVE-2022-1388)

Signaturregel	CVE-ID	Beschreibung
998985	CVE-2022-1162	WEB-MISC Gitlab CE/EE mehrere Versionen - Sicherheitsrisiko durch hartcodierte Anmeldeinformationen (CVE-2022-1162)
998986	CVE-2022-0888	WEB-WORDPRESS-Plugin Ninja Forms-Datei-Uploads vor 3.3.1 - Sicherheitsrisiko durch Hochladen beliebiger Dateien (CVE-2022-0888)
998987	CVE-2021-35244	WEB-MISC SolarWinds Orion vor 2020.2.6 HF3 — Sicherheitsanfälligkeit durch Hochladen beliebiger Dateien durch WriteToFile-Aktion (CVE-2021-35244)

Signatur-Update für Mai 2022

June 1, 2022

Neue Signaturregeln werden für die in der Woche 2022-05-20 identifizierten Sicherheitsrisiken generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 86 gilt für die Plattformen NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0, Citrix ADC 13.1.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998980	CVE-2022-30525	WEB-MISC Zyxel Firewalls mehrere Versionen - Sicherheitsrisiko durch nicht authentifizierte Betriebssystembefehlseinschleusung in setWanPortSt (CVE-2022-30525)
998981	CVE-2021-25094	WEB-WORDPRESS-Plugin Tatsu Builder vor 3.3.12 - Sicherheitsrisiko durch Remotecodeausführung (CVE-2021-25094)

Signaturaktualisierung für Juni 2022

June 21, 2022

Neue Signaturregeln werden für die in der Woche 2022-06-07 identifizierten Sicherheitslücken generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 87 gilt für NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0, Citrix ADC 13.1 Plattformen.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in den allgemeinen Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998964	CVE-2022-30525	WEB-MISC Zyxel Firewalls mehrere Versionen - Sicherheitsrisiko durch nicht authentifizierte Betriebssystembefehlseinschleusung in setWanPortSt (CVE-2022-30525)
998965	CVE-2022-29108	WEB-MISC Microsoft SharePoint — Sicherheitsrisiko durch RCE über Deserialisierung von nicht vertrauenswürdigen Daten (CVE-2022-29108)
998966	CVE-2022-26134	WEB-MISC Atlassian Confluence mehrere Versionen - Sicherheitsrisiko durch Einschleusung von nicht authentifiziertem OGNL (CVE-2022-26134)
998967	CVE-2022-26019	WEB-MISC pfSense CE < 2.6.0 — Sicherheitsrisiko durch Remotecodeausführung über services_ntpd_gps.php und gpsport (CVE-2022-26019)
998968	CVE-2022-26019	WEB-MISC pfSense CE < 2.6.0 — Sicherheitsrisiko durch Remotecodeausführung über services_ntpd.php und gpsport (CVE-2022-26019)
998969	CVE-2022-24288	WEB-MISC Apache Airflow bis 2.2.3 — DAG-Beispiel Sicherheitsrisiko durch Remotecodeausführung über my_param (CVE-2022-24288)

Signaturregel	CVE-ID	Beschreibung
998970	CVE-2022-24288	WEB-MISC Apache Airflow Bis zu 2.2.3 — DAG-Beispiel Sicherheitsrisiko durch Remotecodeausführung über foo oder miff (CVE-2022-24288)
998971	CVE-2022-22978	WEB-MISC Spring Security Bis zu 5.5.6 und 5.6.3 — Sicherheitsrisiko durch Umgehen von RegexRequestMatcher über Zeilenvorschub (CVE-2022-22978)
998972	CVE-2022-22978	WEB-MISC Spring Security Bis zu 5.5.6 und 5.6.3 — Sicherheitsrisiko durch Umgehen von RegexRequestMatcher über Wagenrücklauf (CVE-2022-22978)
998973	CVE-2022-22957	WEB-MISC VMware mehrere Produkte — Sicherheitsrisiko durch Remotecodeausführung (CVE-2022-22957)
998974	CVE-2021-45232	WEB-MISC Apache APISIX Dashboard vor 2.10.1 — Sicherheitsrisiko durch Umgehen der Authentifizierung über Export (CVE-2021-45232)

Signaturregel	CVE-ID	Beschreibung
998975	CVE-2021-45232	WEB-MISC Apache APISIX Dashboard vor 2.10.1 — Sicherheitsrisiko durch Umgehen der Authentifizierung über Import (CVE-2021-45232)
998976	CVE-2021-41739	WEB-MISC Artica Proxy - Sicherheitsrisiko durch Einschleusen von Betriebssystembefehlen über cyrus.events.php (CVE-2021-41739)
998977	CVE-2021-37927	WEB-MISC ManageEngine ADManager Plus vor 7111 — Sicherheitsrisiko durch Umgehen der Authentifizierung (CVE-2021-37927)
998978	CVE-2021-36356	WEB-MISC Kramer VIA VSM-Server - Sicherheitsrisiko durch nicht authentifizierte Remotecodeausführung in writeBrowseFilePathAjax (CVE-2021-36356)
998979	CVE-2021-25094	WEB-WORDPRESS-Plugin Tatsu Builder vor 3.3.12 - Sicherheitsrisiko durch Remotecodeausführung (CVE-2021-25094)

Signaturaktualisierung für Juni 2022

July 8, 2022

Für die in der Woche 2022-06-16 identifizierten Sicherheitslücken werden neue Signaturregeln gener-

iert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 88 gilt für die Plattformen NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0, Citrix ADC 13.1.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in Common Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998958	CVE-2022-28810	WEB-MISC Zoho ManageEngine ADSelfService vor 6122 — Sicherheitsrisiko durch Einschleusung von Betriebssystembefehlen über UNLOCK-Skript (CVE-2022-28810)
998959	CVE-2022-28810	WEB-MISC Zoho ManageEngine ADSelfService vor 6122 — Sicherheitsrisiko durch Einschleusen von Betriebssystembefehlen über RESET-Skript (CVE-2022-28810)
998960	CVE-2022-25237	WEB-MISC Bonita Web vor 7.14.0 - Sicherheitsrisiko durch Umgehen der Autorisierung über i18ntranslation/../(CVE-2022-25237)

Signaturregel	CVE-ID	Beschreibung
998961	CVE-2022-25237	WEB-MISC Bonita Web vor 7.14.0 - Sicherheitsrisiko durch Umgehen der Autorisierung via; i18ntranslation (CVE-2022-25237)
998962	CVE-2022-0540	WEB-MISC Atlassian Jira Server und Data Center — Sicherheitsrisiko durch Umgehen der Jira Seraph-Authentifizierung (CVE-2022-0540)
998963	CVE-2021-44548	WEB-MISC Apache Solr vor 8.11.1 — Sicherheitsrisiko durch DataImportHandler SMB-Angriffe (CVE-2021-44548)

Signaturaktualisierung für Juli 2022

July 15, 2022

Für die in der Woche 2022-07-08 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 89 gilt für die Plattformen NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0, Citrix ADC 13.1.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Einblick in Common Vulnerability Entry (CVE)

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998942	CVE-2022-32532	WEB-MISC Apache Shiro vor 1.9.1 - Sicherheitsrisiko durch Umgehen von RegexRequestMatcher über Zeilenvorschub (CVE-2022-32532)
998943	CVE-2022-32532	WEB-MISC Apache Shiro vor 1.9.1 - Sicherheitsrisiko durch Umgehen von RegexRequestMatcher über Wagenrücklauf (CVE-2022-32532)
998944	CVE-2022-30157	WEB-MISC Microsoft SharePoint - Sicherheitsrisiko durch RCE über Deserialisierung von nicht vertrauenswürdigen Daten (CVE-2022-30157)
998945	CVE-2022-29847	WEB-MISC In Progress Ipswitch WhatsUp Gold - Sicherheitsrisiko durch nicht authentifizierten serverseitige Anforderungsfälschungen (CVE-2022-29847)
998946	CVE-2022-29535	WEB-MISC Zoho ManageEngine OpManager Mehrere Versionen - Sicherheitsrisiko durch SQL-Einschleusung über bview (CVE-2022-29535)

Signaturregel	CVE-ID	Beschreibung
998947	CVE-2022-29535	WEB-MISC Zoho ManageEngine OpManager Mehrere Versionen - Sicherheitsrisiko durch SQL-Einschleusung über category (CVE-2022-29535)
998948	CVE-2022-28219	WEB-MISC Zoho ManageEngine ADAudit Plus vor 7060 — Sicherheitsrisiko durch Remotecodeausführung (CVE-2022-28219)
998949	CVE-2022-28219	WEB-MISC Zoho ManageEngine ADAudit Plus vor 7060 - Sicherheitsrisiko durch XXE-Einschleusung über Task New Content (CVE-2022-28219)
998950	CVE-2022-28219	WEB-MISC Zoho ManageEngine ADAudit Plus vor 7060 — Sicherheitsrisiko durch XXE-Einschleusung über Task Content (CVE-2022-28219)
998951	CVE-2022-23642	WEB-MISC SourceGraph Vor 3.37 - Sicherheitsrisiko durch Remotecodeausführung im Gitserver-Dienst (CVE-2022-23642)
998952	CVE-2022-23206	WEB-MISC Apache Traffic Control Traffic Ops vor 5.1.6 und 6.1.0 — SSRF-Schwachstelle (CVE-2022-23206)

Signaturregel	CVE-ID	Beschreibung
998953	CVE-2022-1609	WEB-WORDPRESS Weblizar School Management Pro-Plugin vor 9.9.7 - Sicherheitsrisiko durch Remotecodeausführung (CVE-2022-1609)
998954	CVE-2022-1209	WEB-WORDPRESS WordPress Plugin Ultimate Member vor 2.3.2 - Sicherheitsrisiko durch offene Weiterleitung (CVE-2022-1209)
998955	CVE-2021-46360	WEB-MISC Composr-CMS - Sicherheitsrisiko durch Remotecodeausführung (CVE-2021-46360)
998956	CVE-2021-43350	WEB-MISC Apache Traffic Control Traffic Ops vor 5.1.4 und 6.0.1 — Sicherheitsrisiko durch LDAP-Einschleusung (CVE-2021-43350)
998957	CVE-2017-9248	WEB-MISC Telerik UI für ASP.NET AJAX vor R2 2017 SP1 — Sicherheitsrisiko durch Offenlegung von Verschlüsselungsschlüsseln (CVE-2017-9248)

Signaturaktualisierung für Juli 2022

August 11, 2022

Für die in der Woche 2022-07-30 identifizierten Sicherheitsrisiken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 90 gilt für die Plattformen NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0, Citrix ADC 13.1.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Common Vulnerability Entry (CVE) Insight

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998929	CVE-2022-34871	WEB-MISC Centreon vor 21.10.6 — Sicherheitsrisiko durch SQL-Einschleusung (CVE-2022-34871)
998930	CVE-2022-29846	WEB-MISC In Progress Ipswitch WhatsUp Gold - Sicherheitsrisiko durch Offenlegung von Informationen (CVE-2022-29846)
998931	CVE-2022-29845	WEB-MISC In Progress Ipswitch WhatsUp Gold - Sicherheitsrisiko durch Pfaddurchquerung (CVE-2022-29845)
998932	CVE-2022-28055	WEB-MISC FusionPBX vor 5.0.1 — Sicherheitsrisiko durch Remotecodeausführung (CVE-2022-28055)
998933	CVE-2022-26138	WEB-MISC Atlassian Questions For Confluence App — Sicherheitsrisiko durch hartcodierte Anmeldeinformationen über REST-API (CVE-2022-26138)

Signaturregel	CVE-ID	Beschreibung
998934	CVE-2022-26138	WEB-MISC Atlassian Questions for Confluence App — Sicherheitsrisiko durch hartcodierte Anmeldeinformationen über Anmeldeformular (CVE-2022-26138)
998935	CVE-2022-26135	WEB-MISC Jira Server and Data Center — Sicherheitsrisiko durch serverseitige Anforderungsfälschungen im mobilen Plug-In (CVE-2022-26135)
998936	CVE-2022-21445	WEB-MISC Oracle OBIEE ADF Faces - Sicherheitsrisiko durch Deserialisierung von nicht vertrauenswürdigen Daten (CVE-2022-21445)
998937	CVE-2022-2143	WEB-MISC Advantech iView vor 5.7.04.6469 - Sicherheitsrisiko durch Remotecodeausführung über NetworkServlet-URI und fwfilename (CVE-2022-2143)
998938	CVE-2022-2143	WEB-MISC Advantech iView vor 5.7.04.6469 - Sicherheitsrisiko durch Remotecodeausführung über CommandServlet-URI und fwfilename (CVE-2022-2143)

Signaturregel	CVE-ID	Beschreibung
998939	CVE-2022-2143	WEB-MISC Advantech iView vor 5.7.04.6469 - Sicherheitsrisiko durch Remotecodeausführung über NetworkServlet-URI und backup_filename (CVE-2022-2143)
998940	CVE-2022-2143	WEB-MISC Advantech iView vor 5.7.04.6469 - Sicherheitsrisiko durch Remotecodeausführung über CommandServlet-URI und backup_filename (CVE-2022-2143)
998941	CVE-2022-2099	WEB-WORDPRESS WooCommerce-Plugin vor 6.6.0 - Sicherheitsrisiko durch HTML-Einschleusung bei Zahlungsgateway (CVE-2022-2099)

Signatur-Update für August 2022

September 1, 2022

Für die in der Woche 2022-08-23 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 91 gilt für die Plattformen NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0, Citrix ADC 13.1.

> **Hinweis:**
>
> Das Aktivieren der Signaturregeln für Postbody und Antworttext kann sich auf die Citrix ADC CPU

Common Vulnerability Entry (CVE) Insight

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998909	CVE-2022-38129	WEB-MISC Keysight SMS vor 2.4.1 — Sicherheitsrisiko durch Pfaddurchquerung ermöglicht RCE (CVE-2022-38129)
998910	CVE-2022-37042, CVE-2022-27925	WEB-MISC Zimbra Collaboration Suite - MailboxImportServlet - Mehrere Sicherheitsrisiken (CVE-2022-37042, CVE-2022-27925)
998911	CVE-2022-36446	WEB-MISC Webmin Multiple Versions - Sicherheitsrisiko durch HTML-Einschleusung und Remotecodeausführung (CVE-2022-36446)
998912	CVE-2022-35405	WEB-MISC Zoho ManageEngine Password Manager Pro vor 12101 — Sicherheitsrisiko durch Java-Deserialisierung (CVE-2022-35405)
998913	CVE-2022-34872	WEB-MISC Centreon vor 21.10.7 — Sicherheitsrisiko durch SQL-Einschleusung über vhidden (CVE-2022-34872)

Signaturregel	CVE-ID	Beschreibung
998914	CVE-2022-34872	WEB-MISC Centreon vor 21.10.7 — Sicherheitsrisiko durch SQL-Einschleusung über rpn_function (CVE-2022-34872)
998915	CVE-2022-34872	WEB-MISC Centreon vor 21.10.7 — Sicherheitsrisiko durch SQL-Einschleusung über unit_name (CVE-2022-34872)
998916	CVE-2022-34872	WEB-MISC Centreon vor 21.10.7 — Sicherheitsrisiko durch SQL-Einschleusung via warn (CVE-2022-34872)
998917	CVE-2022-34872	WEB-MISC Centreon vor 21.10.7 — Sicherheitsrisiko durch SQL-Einschleusung über crit (CVE-2022-34872)
998918	CVE-2022-34872	WEB-MISC Centreon vor 21.10.7 — Sicherheitsrisiko durch SQL-Einschleusung über def_type (CVE-2022-34872)
998919	CVE-2022-31813	WEB-MISC Apache HTTP-Server Bis zu 2.4.53 — Sicherheitsrisiko durch Enfernen von mod_proxy X-Forwarded-*Headern (CVE-2022-31813)
998920	CVE-2022-31125	WEB-MISC Roxy-wi vor 6.1.1.0 - Sicherheitsrisiko durch Umgehen der Authentifizierung über alert_consumer (CVE-2022-31125)

Signaturregel	CVE-ID	Beschreibung
998921	CVE-2022-31101	WEB-MISC Prestashop Blockwishlist vor 2.1.1 — Sicherheitsrisiko durch SQL-Einschleusung (CVE-2022-31101)
998922	CVE-2022-26137	WEB-MISC Atlassian-Produkte — Mehrere Versionen — Sicherheitsrisiko durch Cross-Origin Resource Sharing Bypass (CVE-2022-26137)
998923	CVE-2022-24299	WEB-MISC pfSense CE vor 2.6.0 - Sicherheitsrisiko durch Remotecodeausführung über vpn_openvpn_client.php (CVE-2022-24299)
998924	CVE-2022-24299	WEB-MISC pfSense CE vor 2.6.0 - Sicherheitsrisiko druch Remotecodeausführung über vpn_openvpn_server.php (CVE-2022-24299)
998925	CVE-2022-0817	WEB-WORDPRESS BadgeOS-Plugin vor 3.7.1 - Sicherheitsrisiko durch SQL-Einschleusung über get-achievements und user_id (CVE-2022-0817)
998926	CVE-2021-36749	WEB-MISC Apache Druid - Sicherheitsrisiko durch Offenlegung beliebiger lokaler Dateien (CVE-2021-36749)

Signaturregel	CVE-ID	Beschreibung
998927	CVE-2021-26919	WEB-MISC Apache Druid vor 0.20.2 - Sicherheitsrisiko durch nicht vertrauenswürdige Deserialisierung über autoDeserialize=true (CVE-2021-26919)
998928	CVE-2021-26919	WEB-MISC Apache Druid vor 0.20.2 - Sicherheitsrisiko durch nicht vertrauenswürdige Deserialisierung über detectCustomCollations=true (CVE-2021-26919)

Signatur-Update für September 2022

September 28, 2022

Für die in der Woche 2022-09-22 identifizierten Sicherheitsrisiken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 92 gilt für die Plattformen NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0, Citrix ADC 13.1.

> **Hinweis**
>
> Das Aktivieren der Regeln für die Signatur von Post Body und Response Body kann sich auf die Citrix ADC

Common Vulnerability Entry (CVE) Insight

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998884	CVE-2022-38130	WEB-MISC Keysight SMS vor 2.4.1 - Sicherheitsrisiko - Hochladen willkürlicher Dateien ermöglicht SQL-Einschleusung(CVE-2022-38130)
998885	CVE-2022-35741	WEB-MISC Apache Cloudstack vor 4.16.1.1 - Sicherheitsrisiko durch Einschleusung externer XML-Entität über SAMLResponse (CVE-2022-35741)
998886	CVE-2022-35650	WEB-MISC Moodle Mehrere Versionen - Sicherheitsrisiko durch Pfaddurchlauf über Blackboard-Fragen (CVE-2022-35650)
998887	CVE-2022-32551	WEB-MISC Zoho ManageEngine ServiceDesk MSP vor 10604 — Nicht authentifizierte Offenlegung von Informationen über /WEB-INF (CVE-2022-32551)
998888	CVE-2022-31675	WEB-MISC VMware vRealize Operations Manager — Sicherheitsrisiko durch Umgehen der Authentifizierung (CVE-2022-31675)
998889	CVE-2022-31674	WEB-MISC VMware vRealize Operations Manager — Sicherheitsrisiko durch Offenlegung von Informationen (CVE-2022-31674)

Signaturregel	CVE-ID	Beschreibung
998890	CVE-2022-31656	WEB-MISC VMware Workspace ONE Access — Sicherheitsrisiko durch Umgehen der Authentifizierung (CVE-2022-31656)
998891	CVE-2022-31474	WEB-WORDPRESS BackupBuddy-Plugin Vor 8.7.5 - Offenlegung von Informationen über backup-buddy_local_download (CVE-2022-31474)
998892	CVE-2022-31137, CVE-2022-31126	WEB-MISC Roxy-wi vor 6.1.1.0 - Mehrere Sicherheitsrisiken durch Befehlseinschleusung (CVE-2022-31137, CVE-2022-31126)
998893	CVE-2022-28731	WEB-MISC Apache JSPWiki vor 2.11.3 - Sicherheitsrisiko durch serverseitige Anforderungsfälschung (CVE-2022-28731)
998894	CVE-2022-2551	WEB-WORDPRESS Duplicator Plugin vor 1.4.7.1 - Sicherheitsrisiko durch nicht authentifizierte Backupdownloads (CVE-2022-2551)
998895	CVE-2022-2546	WEB-WORDPRESS All-in-One-WP-Migrations-Plugin vor 7.63 - Sicherheitsrisiko durch reflektiertes XSS über ai1wm_export (CVE-2022-2546)

Signaturregel	CVE-ID	Beschreibung
998896	CVE-2022-2546	WEB-WORDPRESS All-in-One-WP-Migrations-Plugin vor 7.63 - Sicherheitsrisiko durch reflektiertes XSS über ai1wm_import (CVE-2022-2546)
998897	CVE-2022-24948	WEB-MISC Apache JSPWiki Vor 2.11.2 - XSS-Sicherheitsrisiko (CVE-2022-24948)
998898	CVE-2022-2139	WEB-MISC Advantech iView Vor 5.7.04.6469 - Sicherheitsrisiko durch Pfaddurchlauf über MenuServlet-URI und -Seite (CVE-2022-2139)
998899	CVE-2022-2139	WEB-MISC Advantech iView Vor 5.7.04.6469 - Sicherheitsrisiko durch Pfaddurchlauf über CommandServlet-URI und -Seite (CVE-2022-2139)
998900	CVE-2022-2139	WEB-MISC Advantech iView Vor 5.7.04.6469 - Sicherheitsrisiko durch Pfaddurchlauf über CommandServlet-URI und -Dateiname (CVE-2022-2139)
998901	CVE-2022-2139	WEB-MISC Advantech iView Vor 5.7.04.6469 - Sicherheitsrisiko durch Pfaddurchlauf über NetworkServlet-URI und -Dateiname (CVE-2022-2139)

Signaturregel	CVE-ID	Beschreibung
998902	CVE-2022-0817	WEB-WORDPRESS BadgeOS Plugin Vor 3.7.1 - SQLi-Sicherheitsrisiko über get-earned-achievements und exclude (CVE-2022-0817)
998903	CVE-2022-0817	WEB-WORDPRESS BadgeOS Plugin Vor 3.7.1 - SQLi-Sicherheitsrisiko über get-earned-achievements und include (CVE-2022-0817)
998904	CVE-2022-0817	WEB-WORDPRESS BadgeOS Plugin Vor 3.7.1 - SQLi-Sicherheitsrisiko über get-earned-achievements und order (CVE-2022-0817)
998905	CVE-2022-0817	WEB-WORDPRESS BadgeOS Plugin Vor 3.7.1 - SQLi-Sicherheitsrisiko über get-earned-achievements und orderby (CVE-2022-0817)
998906	CVE-2022-0817	WEB-WORDPRESS BadgeOS Plugin Vor 3.7.1 - SQLi-Sicherheitsrisiko über get-earned-achievements und offset (CVE-2022-0817)
998907	CVE-2022-0817	WEB-WORDPRESS BadgeOS Plugin Vor 3.7.1 - SQLi-Sicherheitsrisiko über get-earned-achievements und limit (CVE-2022-0817)

Signaturregel	CVE-ID	Beschreibung
998908	CVE-2018-20062, CVE-2019-9082	WEB-MISC ThinkPHP 5.x vor 5.1.32 — Sicherheitsrisiko durch nicht authentifizierte Remotecodeausführung (CVE-2018-20062, CVE-2019-9082)

Signatur-Update für Oktober 2022

October 4, 2022

Für die in der Woche 2022-10-02 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 93 gilt für die Plattformen NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0, Citrix ADC 13.1.

> **Hinweis:**
>
> Das Aktivieren der Signaturregeln für Postbody und Antworttext kann sich auf die Citrix ADC CPU

Common Vulnerability Entry (CVE) Insight

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998871	CVE-2022-41082, CVE-2022-41040	WEB-MISC Microsoft Exchange Server - RCE-Sicherheitsrisiko (CVE-2022-41082, CVE-2022-41040)

Signaturregel	CVE-ID	Beschreibung
998872	CVE-2022-37299	WEB-MISC Shirne CMS 1.2.0 - Sicherheitsrisiko durch Pfaddurchlauf über /static/ueditor/php/controller.php (CVE-2022-37299)
998873	CVE-2022-36923	WEB-MISC Zoho ManageEngine Mehrere Produkte Mehrere Versionen — Sicherheitsrisiko durch Umgehen der Authentifizierung (CVE-2022-36923)
998874	CVE-2022-33891	WEB-MISC Apache Spark UI Mehrere Versionen - Sicherheitsrisiko durch Remotecodeausführung über doAs-Parameter (CVE-2022-33891)
998875	CVE-2022-3184, CVE-2022-3183	WEB-MISC DataProbe iBoot-PDU vor 1.42.06162022 — Sicherheitsrisiko durch Remotecodeausführung (CVE-2022-3184, CVE-2022-3183)
998876	CVE-2022-31814	WEB-MISC pfSense pfBlockerNG vor 2.1.4_26 - Sicherheitsrisiko durch Remotecodeausführung (CVE-2022-31814)
998877	CVE-2022-31097	WEB-MISC Apache Grafana - Sicherheitsrisiko durch Unified Alerting Stored XSS (CVE-2022-31097)

Signaturregel	CVE-ID	Beschreibung
998878	CVE-2022-2903	WEB-WORDPRESS NinjaForms-Plugin vor 3.6.13 - Sicherheitsrisiko durch PHP-Objekteinschleusung (CVE-2022-2903)
998879	CVE-2022-2552	WEB-WORDPRESS Duplicator Plugin vor 1.4.7.1 - Sicherheitsrisiko durch nicht authentifizierte Offenlegung von Informationen (CVE-2022-2552)
998880	CVE-2022-23854	WEB-MISC AVEVA InTouch Access Anywhere Secure Gateway - Sicherheitsrisiko durch Pfaddurchlauf über SG-URI (CVE-2022-23854)
998881	CVE-2022-23854	WEB-MISC AVEVA InTouch Access Anywhere Secure Gateway - Sicherheitsrisiko durch Pfaddurchlauf über Blaze URI (CVE-2022-23854)
998882	CVE-2022-23854	WEB-MISC AVEVA InTouch Access Anywhere Secure Gateway - Sicherheitsrisiko durch Pfaddurchlauf über AccessAnywhere URI (CVE-2022-23854)
998883	CVE-2017-9841	WEB-MISC PHPUnit Vor 4.8.28 und 5.x vor 5.6.3 - Sicherheitsrisiko durch Remotecodeausführung über eval-stdin.php (CVE-2017-9841)

Signatur-Update für Oktober 2022

October 11, 2022

Für die in der Woche 2022-10-06 identifizierten Sicherheitslücken werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Sicherheitsangriffen zu schützen.

Signaturversion

Signaturversion 94 gilt für die Plattformen NetScaler VPX 11.1, NetScaler 12.0, Citrix ADC 12.1, Citrix ADC 13.0, Citrix ADC 13.1.

> **Hinweis:**
>
> Das Aktivieren der Signaturregeln für Postbody und Antworttext kann sich auf die Citrix ADC CPU

Common Vulnerability Entry (CVE) Insight

Im Folgenden finden Sie eine Liste von Signaturregeln, CVE-IDs und deren Beschreibung.

Signaturregel	CVE-ID	Beschreibung
998870	CVE-2022-41082, CVE-2022-41040	WEB-MISC Microsoft Exchange Server - RCE-Sicherheitsrisiko (CVE-2022-41082, CVE-2022-41040)

Bot Management

October 5, 2021

Manchmal besteht der eingehende Web-Traffic aus Bots und die meisten Organisationen leiden unter Bot-Attacken. Web- und mobile Anwendungen sind große Umsatztreiber für Unternehmen und die meisten Unternehmen sind unter der Bedrohung von fortgeschrittenen Cyberangriffen wie Bots.
Ein Bot ist ein Softwareprogramm, das automatisch bestimmte Aktionen wiederholt mit einer viel schnelleren Geschwindigkeit ausführt als ein Mensch. Bots können mit Webseiten interagieren, Formulare einreichen, Aktionen ausführen, Texte scannen oder Inhalte herunterladen. Sie können auf Social-Media-Plattformen auf Videos zugreifen, Kommentare posten und twittern. Einige Bots, bekannt als Chatbots, können grundlegende Gespräche mit menschlichen Benutzern führen.

Ein Bot, der einen hilfreichen Service wie Kundenservice, automatisierter Chat und Suchmaschinen-Crawler ausführt, sind gute Bots. Gleichzeitig sind ein Bot, der Inhalte von einer Website kratzen oder herunterladen kann, Benutzeranmeldeinformationen, Spam-Inhalte stehlen und andere Arten von Cyberangriffen ausführen kann, schlechte Bots.
Da viele schlechte Bots bösartige Aufgaben ausführen, ist es wichtig, den Bot-Verkehr zu verwalten und Ihre Web-Anwendungen vor Bot-Angriffen zu schützen. Mithilfe der Citrix Bot-Verwaltung können Sie den eingehenden Bot-Datenverkehr erkennen und Bot-Angriffe abschwächen, um Ihre Webanwendungen zu schützen.
Citrix Bot Management hilft, schlechte Bots zu identifizieren und Ihre Appliance vor erweiterten Sicherheitsangriffen zu schützen. Es erkennt gute und schlechte Bots und identifiziert, ob eingehender Traffic ein Bot-Angriff ist. Mit der Bot-Verwaltung können Sie Angriffe abschwächen und Ihre Webanwendungen schützen.

Die Citrix ADC Bot-Verwaltung bietet folgende Vorteile:

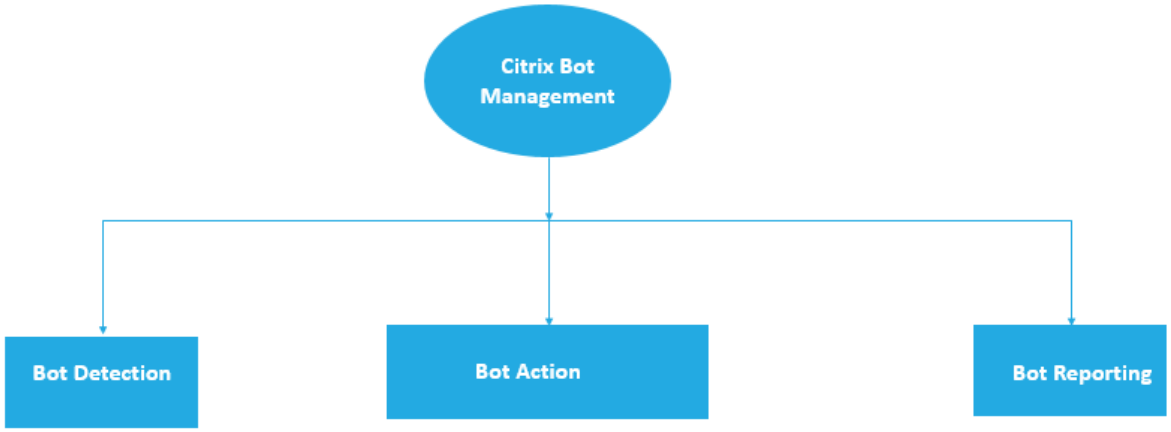
- **Verteidigen Sie sich gegen Bots, Skripts und Toolkits**. Bietet Echtzeit-Bedrohungsschutz durch statische Signaturen basierende Abwehr und Fingerabdrücke von Geräten.
- **Neutralisieren Sie automatisierte grundlegende und fortgeschrittene Angriffe**. Verhindert Angriffe, wie App-Layer-DDoS, Kennwort-Spraying, Kennwort-Stuffing, Preis-Scraper und Inhalts-Scraper.
- **Schützen Sie Ihre APIs und Investitionen**. Schützt Ihre APIs vor ungerechtfertigten Missbrauch und schützt Infrastrukturinvestitionen vor automatisierten Datenverkehr.

Einige Anwendungsfälle, in denen Sie von der Verwendung des Citrix Bot-Managementsystems profitieren können, sind:

- Brute-Force-Login. Ein Regierungs-Webportal wird ständig von Bots angegriffen, die versuchen, Benutzeranmeldungen zu erzwingen. Die Organisation entdeckte den Angriff, indem sie Weblogs durchsah und sah, wie bestimmte Benutzer immer wieder ausgewählt wurden, wobei schnelle Anmeldeversuche und Kennwörter über einen Wörterbuchangriff zunahmen. Nach dem Gesetz müssen sie sich und ihre Nutzer schützen. Durch die Bereitstellung der Citrix Bot-Verwaltung können sie die Brute-Force-Anmeldung mit Geräte-Fingerprinting und Ratenbegrenzungstechniken stoppen.
- Blockieren Sie schlechte Bots und Geräte-Fingerabdruck unbekannte Bots. Eine Web-Entität erhält jeden Tag 100.000 Besucher. Sie müssen den zugrundeliegenden Fußabdruck verbessern und sie geben ein Vermögen aus. In einem kürzlich durchgeführten Audit entdeckte das Team, dass 40 Prozent des Traffics von Bots, Scraping von Inhalten, Auswahl von Nachrichten, Überprüfung von Benutzerprofilen und mehr kamen. Sie möchten diesen Datenverkehr blockieren, um ihre Benutzer zu schützen und ihre Hosting-Kosten zu senken. Mit der Bot-Verwaltung können sie bekannte schlechte Bots und Fingerabdrücke unbekannte Bots blockieren, die ihre Website hämmern. Indem sie diese Bots blockieren, können sie den Bot-Verkehr um 90 Prozent reduzieren.

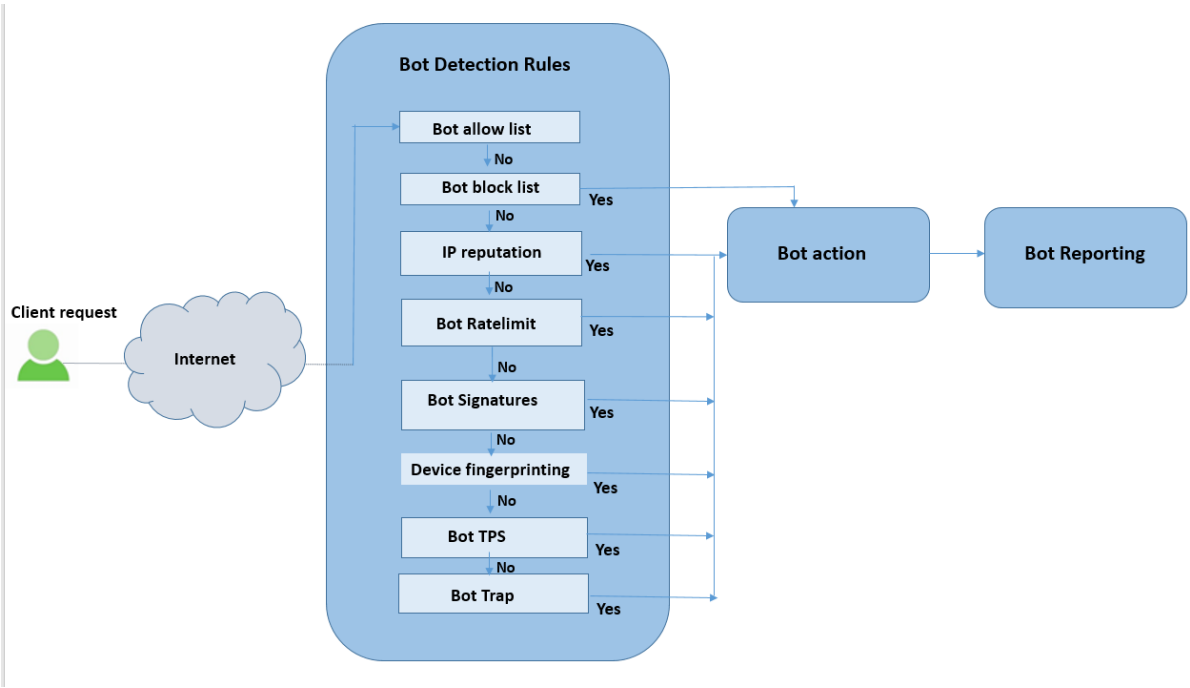
Was macht Citrix Bot Management?

Die Citrix Bot-Verwaltung hilft Unternehmen, ihre Webanwendungen und öffentlichen Ressourcen vor erweiterten Sicherheitsangriffen zu schützen. Wenn ein eingehender Datenverkehr ein Bot ist, erkennt das Bot-Managementsystem den Bot-Typ, weist eine Aktion zu und generiert Bot-Insights, wie im folgenden Diagramm gezeigt.



Wie funktioniert das Citrix ADC Bot-Management?

Das folgende Diagramm zeigt, wie die Citrix ADC Bot-Verwaltung funktioniert. Der Prozess umfasst acht Erkennungstechniken, die helfen, den eingehenden Datenverkehr als guten oder schlechten Bot zu erkennen. Standardmäßig sind gute Bots, die von Signaturen erkannt wurden, zulässig und schlechte Bots, die von Signaturen erkannt wurden, werden gelöscht.



1. Der Prozess beginnt mit der Aktivierung der Bot-Verwaltungsfunktion auf der Appliance.
2. Wenn ein Client eine Anforderung sendet, wertet die Appliance den Datenverkehr mithilfe von Bot-Richtlinienregeln aus. Wenn die eingehende Anforderung als Bot identifiziert wird, wendet die Appliance ein Bot-Erkennungsprofil an.
3. Sie müssen die Standard- oder benutzerdefinierte Bot-Signaturdatei an das Bot-Erkennungsprofil binden. Die Bot-Signaturdatei enthält eine Liste von Bot-Signaturregeln zur Identifizierung des eingehenden Bot-Typs.
4. Die Bot-Erkennungsregeln sind unter acht Erkennungskategorien in der Signaturdatei verfügbar. Die Kategorien sind Zulassungsliste, Sperrliste, statische Signatur, IP-Reputation, Geräte-Fingerabdruck und Ratenbegrenzung. Basierend auf dem Bot-Datenverkehr wendet das System eine Erkennungsregel auf den Datenverkehr an.
5. Wenn der eingehende Bot-Traffic mit einem Eintrag in der Bot-Zulassungsliste übereinstimmt, umgeht das System andere Erkennungstechniken und die zugehörige Aktion protokolliert die Daten.
6. Bei anderen Erkennungstechniken als der Bot-Zulassungsliste wird die entsprechende Aktion angewendet, wenn eine eingehende Anforderung mit einer konfigurierten Regel übereinstimmt. Die möglichen Aktionen sind Drop, Redirect, Reset, Minderung und Log. CAPTCHA ist eine Minderungsaktion, die für IP-Reputation, Gerätefingerabdruck und TPS-Erkennungstechniken unterstützt wird.

Bot-Erkennung

April 25, 2022

Das Citrix ADC Bot-Managementsystem verwendet sechs verschiedene Techniken, um den eingehenden Bot-Verkehr zu erkennen. Die Techniken werden als Erkennungsregeln verwendet, um den Bot-Typ zu erkennen. Die Techniken sind Bot-Positivliste, Bot-Sperrliste, IP-Reputation, Gerätefingerprint, Ratenbegrenzung, Bot-Trap, TPS und CAPTCHA.

> **Hinweis:**
>
> Die Bot-Verwaltung unterstützt maximal 32 Konfigurations-Entitäten für Sperrlisten-, Positivlisten- und Ratenbegrenzungstechniken.

Bot-Positivliste. Eine angepasste Liste von IP-Adressen, Subnetzen und Richtlinienausdrücken, die als Positivliste umgangen werden können.

Bot-Sperrliste. Eine angepasste Liste von IP-Adressen, Subnetzen und Richtlinienausdrücken, die für den Zugriff auf Ihre Webanwendungen blockiert werden müssen.

Ruf von geistigem Eigentum. Diese Regel erkennt, ob der eingehende Bot-Verkehr von einer böswilligen IP-Adresse stammt.

Geräte-Fingerabdruck. Diese Regel erkennt, ob der eingehende Bot-Verkehr die Geräte-Fingerabdruck-ID im Header für eingehende Anfragen und Browserattribute eines eingehenden Client-Bot-Traffics enthält.

> **Einschränkung:**
>
> 1. JavaScript muss im Client-Browser aktiviert sein.
> 2. Funktioniert nicht für XML-Antworten.

Bot-Log-Ausdruck. Die Erkennungstechnik ermöglicht es Ihnen, zusätzliche Informationen als Protokollmeldungen zu erfassen. Die Daten können der Name des Benutzers sein, der die URL angefordert hat, die Quell-IP-Adresse und der Quellport, von dem der Benutzer die Anforderung oder Daten gesendet hat, die aus einem Ausdruck generiert wurden.

Rate Limit. Diese Regelrate begrenzt mehrere Anfragen desselben Kunden.

Bot-Trap. Erkennt und blockiert automatisierte Bots, indem eine Trap-URL in der Kundenantwort angezeigt wird. Die URL erscheint unsichtbar und nicht zugänglich, wenn der Client ein menschlicher Benutzer ist. Die Erkennungstechnik blockiert effektiv Angriffe von automatisierten Bots.

TPS. Erkennt eingehenden Datenverkehr als Bots, wenn die maximale Anzahl von Anfragen und der prozentuale Anstieg der Anfragen das konfigurierte Zeitintervall überschreiten.

CAPTCHA. Diese Regel verwendet ein CAPTCHA zur Abwehr von Bot-Angriffen. Ein CAPTCHA ist eine Challenge-Response-Validierung, um festzustellen, ob der eingehende Verkehr von einem menschlichen Benutzer oder einem automatisierten Bot stammt. Die Validierung hilft dabei, automatisierte Bots zu blockieren, die Sicherheitsverletzungen für Webanwendungen verursachen. Sie können CAPTCHA als Bot-Aktion für IP-Reputation und Geräte-Fingerabdruck-Erkennungstechniken konfigurieren.

Lassen Sie uns nun sehen, wie Sie jede Technik konfigurieren können, um Ihren Bot-Traffic zu erkennen und zu verwalten.

So aktualisieren Sie Ihre Appliance auf Citrix ADC CLI-basierte Bot-Management-Konfiguration

Wenn Sie Ihre Appliance von einer älteren Version aktualisieren (Citrix ADC Version 13.0 Build 58.32 oder früher), müssen Sie die vorhandene Bot-Verwaltungskonfiguration zuerst nur einmal manuell in die Citrix ADC CLI-basierte Bot-Management-Konfiguration konvertieren. Führen Sie die folgenden Schritte aus, um Ihre Bot-Management-Konfiguration manuell zu konvertieren.

1. Stellen Sie nach dem Upgrade auf die neueste Version mithilfe des folgenden Befehls eine Verbindung zum Upgrade-Tool “upgrade_bot_config.py” her

   Geben Sie an der Eingabeaufforderung Folgendes ein:


```
shell "/var/python/bin/python /netscaler/upgrade_bot_config.py > /var/
bot_upgrade_commands.txt"
```

2. Führen Sie die Konfiguration mit dem folgenden Befehl aus.

   Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   batch -f /var/bot_upgrade_commands.txt
   ```

3. Speichern Sie die aktualisierte Konfiguration.

```
save ns config
```

Konfigurieren der Citrix ADC CLI-basierten Bot-Verwaltung

Mit der Bot-Management-Konfiguration können Sie eine oder mehrere Bot-Erkennungstechniken an ein bestimmtes Bot-Profil binden. Sie beginnen den Prozess, indem Sie die Bot-Verwaltungsfunktion auf Ihrer Appliance aktivieren. Sobald Sie aktiviert haben, importieren Sie die Bot-Signaturdatei in die Appliance. Nach dem Import müssen Sie ein Bot-Profil erstellen. Anschließend erstellen Sie eine Bot-Richtlinie mit dem daran gebundenen Bot-Profil, um den eingehenden Datenverkehr als Bot auszuwerten und die Richtlinie global oder an einen virtuellen Server zu binden.

> **Hinweis:**
>
> Wenn Sie Ihre Appliance von einer älteren Version upgraden, müssen Sie zuerst die vorhandene Bot-Management-Konfiguration manuell konvertieren. Weitere Informationen finden Sie unter Abschnitt Upgrade auf Citrix ADC Cli-basierte Bot-Management-Konfiguration .

Sie müssen die folgenden Schritte ausführen, um die Citrix ADC-basierte Bot-Verwaltung zu konfigurieren:

1. Bot-Management aktivieren
2. Botsignatur importieren
3. Bot-Profil hinzufügen
4. Bot-Profil binden
5. Bot-Richtlinie hinzufügen
6. Bind-Bot-Richtlinie
7. Konfigurieren Sie Bot-Einstellungen

Bot-Management aktivieren

Bevor Sie beginnen können, stellen Sie sicher, dass die Bot-Verwaltungsfunktion auf der Appliance aktiviert ist. Wenn Sie über einen neuen Citrix ADC oder VPX verfügen, müssen Sie die Funktion aktivieren, bevor Sie sie konfigurieren. Wenn Sie eine Citrix ADC- oder VPX-Appliance von einer früheren Version der Citrix ADC-Softwareversion auf die aktuelle Version aktualisieren, müssen Sie die Funktion aktivieren, bevor Sie sie konfigurieren. Geben Sie an der Eingabeaufforderung Folgendes ein:


```
enable ns feature Bot
```

Botsignatur importieren

Sie können die Standardsignatur-Bot-Datei importieren und an das Bot-Profil binden. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import bot signature [<src>] <name> [-comment <string>] [-overwrite]
```

Wo,
src. Lokaler Pfad und Name oder URL (Protokoll, Host, Pfad und Dateiname) für die Datei, in der die importierte Signaturdatei gespeichert werden soll. Hinweis: Der Import schlägt fehl, wenn sich das zu importierende Objekt auf einem HTTPS-Server befindet, für den Zugriff eine Clientzertifikatauthentifizierung erforderlich ist. Maximale Länge: 2047
Name. Name, der dem Bot-Signaturdateiobjekt auf dem Citrix ADC zugewiesen werden soll. Dies ist ein zwingendes Argument. Maximale Länge: 31
Kommentar. Irgendwelche Kommentare, um Informationen über das Signaturdateiobjekt beizubehalten. Maximale Länge: 255
überschreiben. Überschreibt die bestehende Datei.
Hinweis: Verwenden Sie die Option `overwrite`, um den Inhalt der Signaturdatei zu aktualisieren. Verwenden Sie alternativ den Befehl `update bot signature <name>`, um die Signaturdatei auf der Citrix ADC-Appliance zu aktualisieren

Beispiel

```
import bot signature http://www.example.com/signature.json signaturefile -
comment commentsforbot -overwrite
```

> **Hinweis:**
>
> Sie können die Option zum Überschreiben verwenden, um den Inhalt in der Signaturdatei zu aktualisieren. Sie können den Befehl `update bot signature <name>` auch verwenden, um die Signaturdatei in der Citrix ADC-Appliance zu aktualisieren.

Bot-Profil hinzufügen

Ein Bot-Profil ist eine Sammlung von Profileinstellungen zur Konfiguration der Bot-Verwaltung auf der Appliance. Sie können die Einstellungen für die Durchführung der Bot-Erkennung konfigurieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add bot profile <name> [-signature <string>] [-errorURL <string>] [-trapURL
 <string>] [-comment <string>] [-whiteList ( ON | OFF )] [-blackList ( ON
 | OFF )] [-rateLimit ( ON | OFF )] [-deviceFingerprint ( ON | OFF )] [-
```



```
deviceFingerprintAction ( none | log | drop | redirect | reset | mitigation
 )] [-ipReputation ( ON | OFF )] [-trap ( ON | OFF )] [-trapAction ( none |
 log | drop | redirect | reset )] [-tps ( ON | OFF )]
```

Beispiel:

```
add bot profile profile1 -signature signature -errorURL http://www.example
.com/error.html -trapURL /trap.html -whitelist ON -blacklist ON -ratelimit
 ON -deviceFingerprint ON -deviceFingerprintAction drop -ipReputation ON -
trap ON
```

Bot-Profil binden

Nachdem Sie ein Bot-Profil erstellt haben, müssen Sie den Bot-Erkennungsmechanismus an das Profil binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind bot profile <name> ((-blackList [-type ( IPv4 | Subnet | Expression
 )] [-enabled ( ON | OFF )] [-value <string>] [-action ( log | drop |
reset )] [-logMessage <string>] [-comment <string>])| (-whiteList [-type
 ( IPv4 | Subnet | Expression )] [-enabled ( ON | OFF )] [-value <string
>] [-log ( ON | OFF )] [-logMessage <string>] [-comment <string>]))|
(-rateLimit [-type ( session |SOURCE_IP | url )] [-enabled ( ON | OFF
)] [-url <string>] [-cookieName <string>] [-rate <positive_integer>] [-
timeslice <positive_integer>] [-action ( none | log | drop | redirect |
reset )] [-logMessage <string>] [-comment <string>])| (-ipReputation [-
category <ipReputationCategory>] [-enabled ( ON | OFF )] [-action ( none
 | log | drop | redirect | reset | mitigation )] [-logMessage <string>]
[-comment <string>])| (-captchaResource [-url <string>] [-enabled ( ON |
 OFF )] [-waitTime <positive_integer>] [-gracePeriod <positive_integer>]
 [-mutePeriod <positive_integer>] [-requestLengthLimit <positive_integer
>] [-retryAttempts <positive_integer>] [-action ( none | log | drop |
redirect | reset )] [-logMessage <string>] [-comment <string>])| (-tps
 [-type ( SOURCE_IP | GeoLocation | REQUEST_URL | Host )] [-threshold <
positive_integer>] [-percentage <positive_integer>] [-action ( none | log |
 drop | redirect | reset | mitigation )] [-logMessage <string>] [-comment <
string>])
```

Beispiel:

Das folgende Beispiel dient zur Bindung der IP-Reputationserkennungstechnik an ein bestimmtes Bot-Profil.


```
bind bot profile profile5 -ipReputation -category BOTNET -enabled ON -
action drop -logMessage message
```

Bot-Richtlinie hinzufügen

Sie müssen die Bot-Richtlinie zur Bewertung des Bot-Traffics hinzufügen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add bot policy <name> -rule <expression> -profileName <string> [-undefAction
 <string>] [-comment <string>] [-logAction <string>]
```

Hierbei gilt:

Name. Name für die Bot-Richtlinie. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und darf nur Buchstaben, Zahlen und den Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), Leerzeichen (), bei (@), gleich (=), Doppelpunkt (:) und Unterstriche enthalten. Kann geändert werden, nachdem die Bot-Richtlinie hinzugefügt wurde.

Regel. Ausdruck, den die Richtlinie verwendet, um zu bestimmen, ob das Bot-Profil auf die angegebene Anforderung angewendet werden soll. Dies ist ein zwingendes Argument. Maximale Länge: 1499

profileName. Name des anzuwendenden Bot-Profils, wenn die Anforderung dieser Bot-Richtlinie entspricht. Dies ist ein zwingendes Argument. Maximale Länge: 127

undefAction. Durchzuführende Maßnahme, wenn das Ergebnis der Richtlinienbewertung nicht definiert ist (UNDEF). Ein UNDEF-Ereignis weist auf einen internen Fehlerzustand hin. Maximale Länge: 127

Kommentar. Jede Art von Informationen zu dieser Bot-Richtlinie. Maximale Länge: 255

logAction. Name der Protokollaktion, die für Anfragen verwendet werden soll, die dieser Richtlinie entsprechen. Maximale Länge: 127

Beispiel:

```
add bot policy pol1 -rule "HTTP.REQ.HEADER(\"header\").CONTAINS(\"custom
\")"- profileName profile1 -undefAction drop -comment commentforbotpolicy -
logAction log1
```

Binden Sie die Bot-Richtlinie global

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind bot global -policyName <string> -priority <positive_integer> [-gotoPriorityExpres
 <expression>][-type ( REQ_OVERRIDE | REQ_DEFAULT )] [-invoke (-labelType (
 vserver | policylabel )-labelName <string>)]
```


Beispiel:

```
bind bot global -policyName pol1 -priority 100 -gotoPriorityExpression NEXT
-type REQ_OVERRIDE
```

Binden Sie die Bot-Richtlinie an einen virtuellen Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name>@ ((<serviceName>@ [-weight <positive_integer>] )| <
serviceGroupName>@ | (-policyName <string>@ [-priority <positive_integer>]
 [-gotoPriorityExpression <expression>] [-type ( REQUEST | RESPONSE )] [-
invoke (<labelType> <labelName>)] )| -analyticsProfile <string>@)
```

Beispiel:

```
bind lb vserver lb-server1 -policyName pol1 -priority 100 -gotoPriorityExpression
 NEXT -type REQ_OVERRIDE
```

Konfigurieren Sie Bot-Einstellungen

Sie können die Standardeinstellungen bei Bedarf anpassen.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set bot settings [-defaultProfile <string>] [-javaScriptName <string>]
 [-sessionTimeout <positive_integer>] [-sessionCookieName <string>] [-
dfpRequestLimit <positive_integer>] [-signatureAutoUpdate ( ON | OFF )]
[-signatureUrl <URL>] [-proxyServer <ip_addr|ipv6_addr|*>] [-proxyPort <
port|*>]
```

Hierbei gilt:

defaultProfile. Profil, das verwendet werden soll, wenn eine Verbindung keiner Richtlinie entspricht. Die Standardeinstellung ist “, die nicht übereinstimmende Verbindungen zurück an den Citrix ADC sendet, ohne zu versuchen, sie weiter zu filtern. Maximale Länge: 31

javaScriptName. Name des JavaScripts, das die BotNet-Funktion als Antwort verwendet. Muss mit einem Buchstaben oder einer Zahl beginnen und kann aus 1 bis 31 Buchstaben, Zahlen und den Bindestrichen (-) und Unterstrichen (_) bestehen. Die folgende Anforderung gilt nur für die Citrix ADC CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “mein Cookie-Name” oder “mein Cookie-Name”). Maximale Länge: 31

sessionTimeout. Sitzungstimablauf in Sekunden, wonach eine Benutzersitzung beendet wird.

Mindestwert: 1, Maximalwert: 65535

sessionCookieName. Name des SessionCookie, das von der BotNet-Funktion zur Nachverfolgung verwendet wird. Muss mit einem Buchstaben oder einer Zahl beginnen und kann aus 1 bis 31 Buchstaben, Zahlen und den Bindestrichen (-) und Unterstrichen (_) bestehen. Die folgende Anforderung gilt nur für die Citrix ADC CLI: Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “mein Cookie-Name” oder “mein Cookie-Name”). Maximale Länge: 31

dfpRequestLimit. Anzahl der Anfragen, die ohne Bot-Sitzungscookie zugelassen werden sollen, wenn der Geräte-Fingerabdruck aktiviert ist.

Mindestwert: 1, Maximalwert: 4294967295

signatureAutoUpdate. Flag zum Aktivieren/Deaktivieren von Bot-Auto-Update-Signaturen.

Mögliche Werte: ON, OFF

Standardwert: OFF

signatureUrl. URL zum Herunterladen der Bot-Signaturzuordnungsdatei vom Server.

Standardwert: `https://nsbotsignatures.s3.amazonaws.com/BotSignatureMapping.json`.

Maximale Länge: 2047

ProxyServer. Proxy-Server-IP, um aktualisierte Signaturen von AWS zu erhalten.

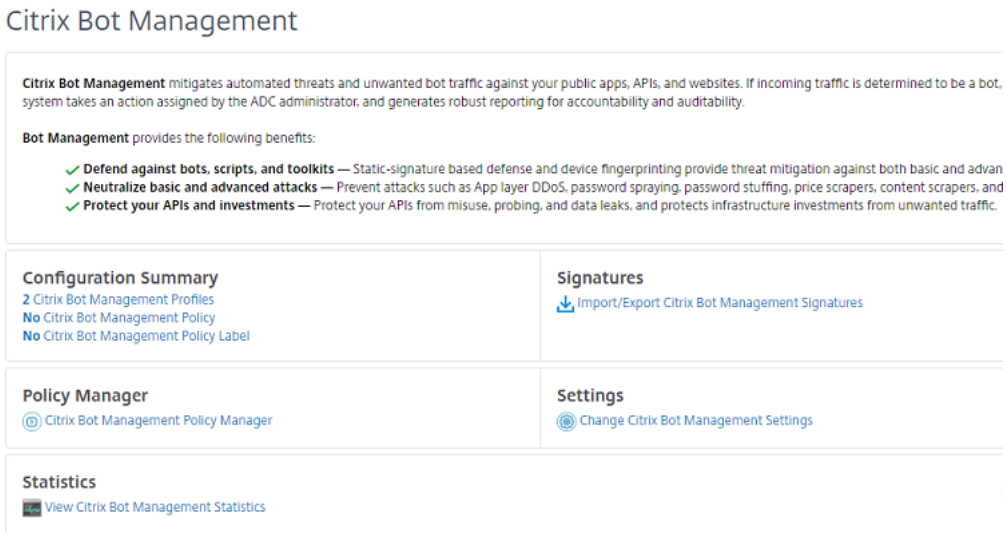
proxyPort. Proxy-Server-Port zum Abrufen aktualisierter Signaturen von AWS. Standardwert: 8080

Beispiel:

```
set bot settings -defaultProfile profile1 -javaScriptName json.js -sessionTimeout
 1000 -sessionCookieName session
```

Konfigurieren der Bot-Verwaltung über die Citrix ADC-GUI

Sie können die Citrix ADC-Bot-Verwaltung konfigurieren, indem Sie zuerst die Funktion auf der Appliance aktivieren. Sobald Sie aktiviert haben, können Sie eine Bot-Richtlinie erstellen, um den eingehenden Traffic als Bot auszuwerten und den Traffic an das Bot-Profil zu senden. Dann erstellen Sie ein Bot-Profil und binden das Profil dann an eine Bot-Signatur. Alternativ können Sie auch die Standard-Bot-Signaturdatei klonen und die Signaturdatei verwenden, um die Erkennungstechniken zu konfigurieren. Nachdem Sie die Signaturdatei erstellt haben, können Sie sie in das Bot-Profil importieren.

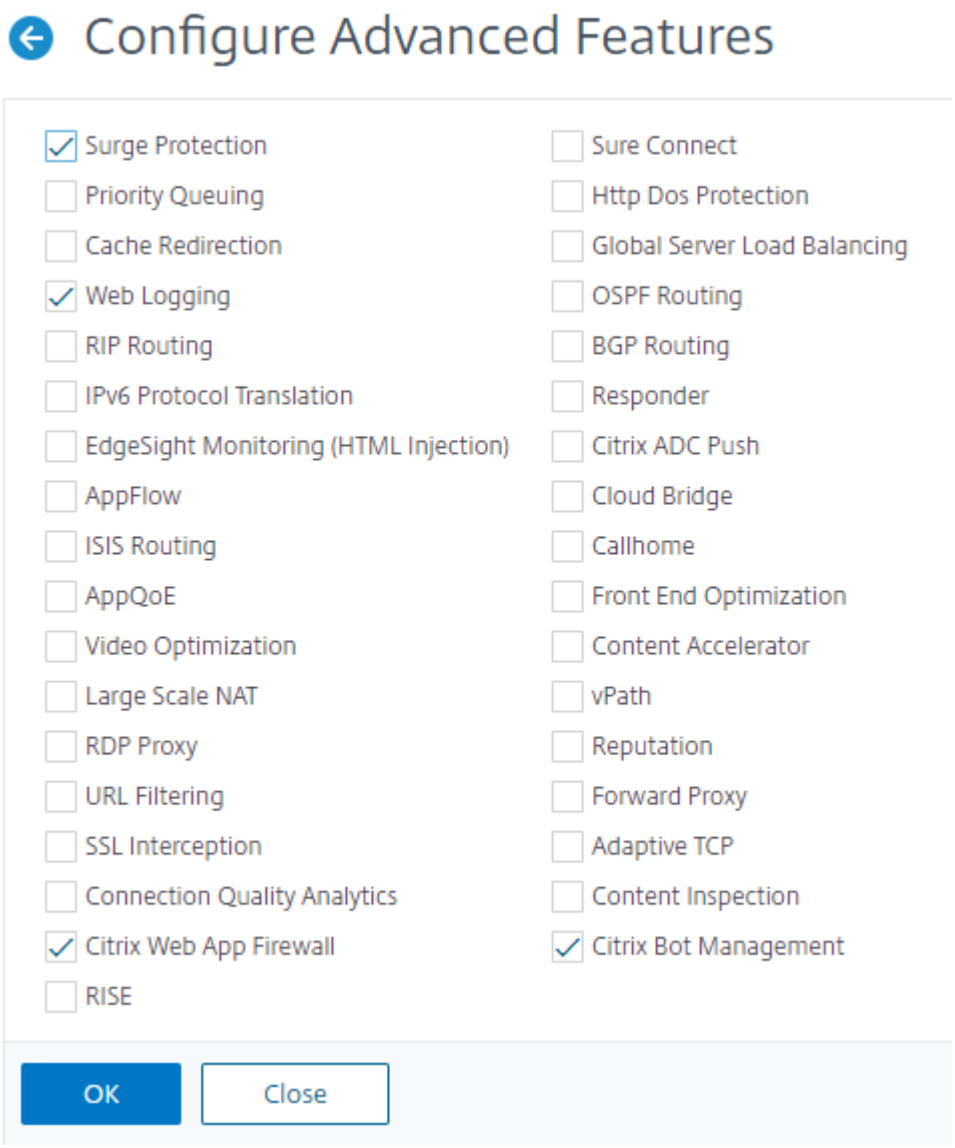


1. Bot-Management-Funktion aktivieren
2. Konfigurieren von Bot-Verwaltungseinstellungen
3. Klonen der Citrix Bot-Standardsignatur
4. Importieren der Citrix Bot-Signatur
5. Konfigurieren Sie Bot Einstellungen für die
6. Erstellen Sie ein Bot-Profil
7. Erstellen Sie Bot-Richtlinie

Bot-Management-Funktion aktivieren

Führen Sie die folgenden Schritte aus, um das Bot-Management zu aktivieren

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**.
2. Aktivieren Sie auf der Seite **Erweiterte Funktionen konfigurieren** das Kontrollkästchen **Bot Management** .
3. Klicken Sie auf **OK**, und klicken Sie dann auf **Schließen**.



Konfigurieren der Bot-Verwaltungseinstellungen für die Geräte-Fingerabdruck-

Führen Sie den folgenden Schritt aus, um die Fingerabdrucktechnik des Geräts zu konfigurieren:

1. Navigieren Sie zu **Sicherheit** > **Citrix Bot Management**.
2. Klicken Sie im Detailbereich unter **Einstellungen** auf **Citrix Bot Management-Einstellungen ändern**.
3. Legen Sie in den **Citrix Bot-Verwaltungseinstellungen konfigurieren** die folgenden Parameter fest.

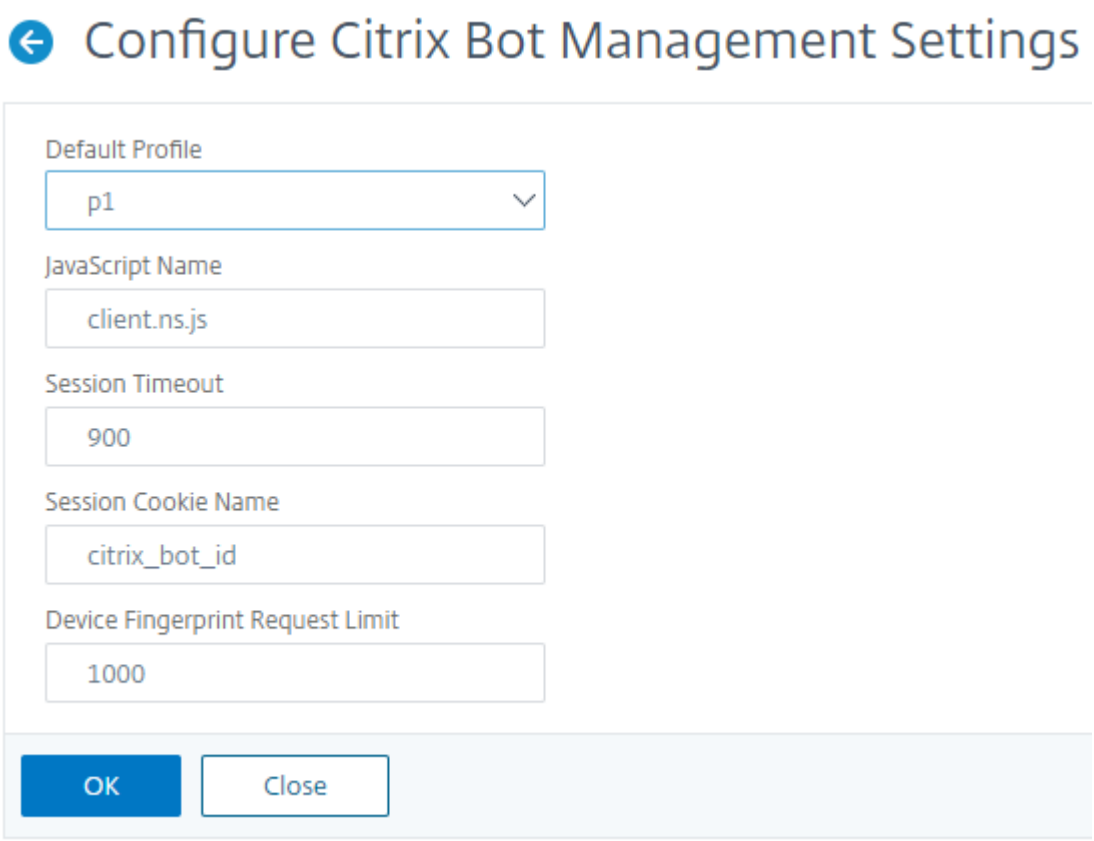
   a) Standardprofil. Wähle ein Bot-Profil aus.
   b) JavaScript-Name Name der JavaScript-Datei, die das Bot-Management in seiner Antwort

an den Client verwendet.

c) Sitzungs-Timeout. Timeout in Sekunden, nach dem die Benutzersitzung beendet wird.

d) Sitzungs-Cookie. Name des Sitzungscookies, das das Bot-Managementsystem zur Verfolgung verwendet.

e) Limit für Geräte-Fingerabdruck-Anfragen Anzahl der Anfragen, die ohne ein Bot-Sitzungscookie zugelassen werden sollen, wenn der Geräte-Fingerabdruck aktiviert ist



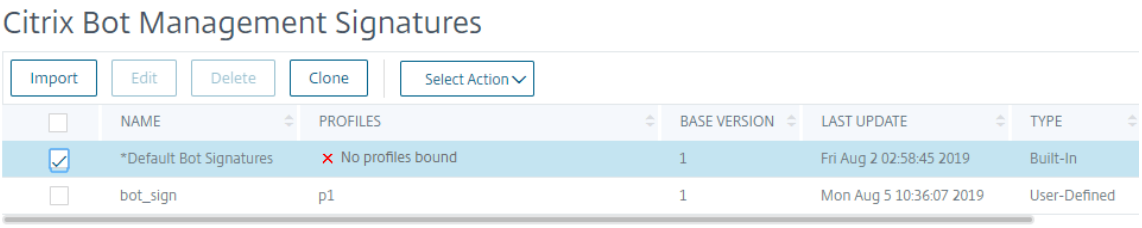
4. Klicken Sie auf **OK**.

Klonen der Bot-Signaturdatei

Führen Sie den folgenden Schritt aus, um die Bot-Signaturdatei zu klonen:

1. Navigieren Sie zu **Sicherheit** > **Citrix Bot Management** and **Signaturen**.
2. Wählen Sie auf der Seite **Citrix Bot Management Signaturen** den Standard-Bot-Signaturendatensatz aus und klicken Sie auf **Klonen**.
3. Geben Sie auf der Seite " **Bot-Signatur klonen** " einen Namen ein und bearbeiten Sie die Signaturdaten.

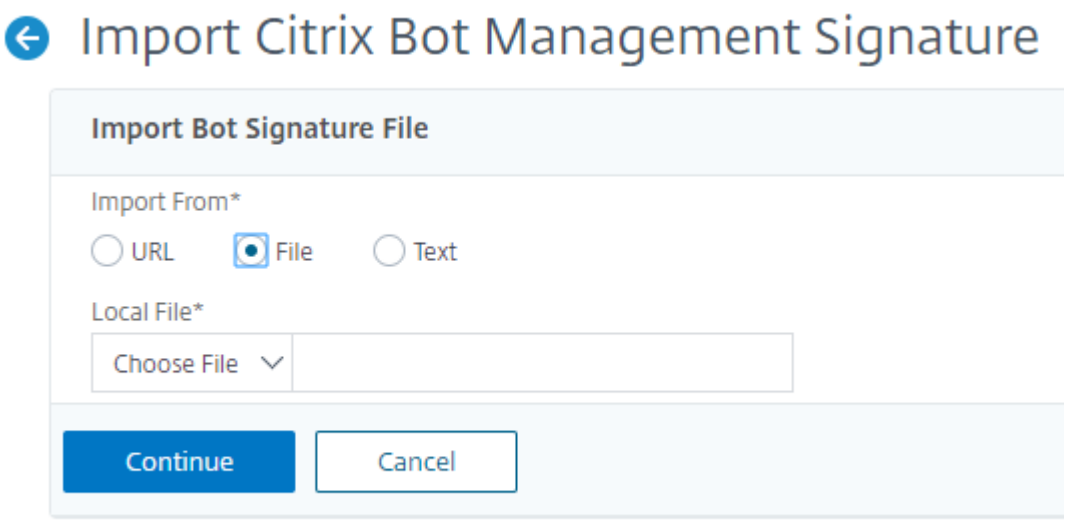
4. Klicken Sie auf **Erstellen**.



Importieren von Bot-Signatur

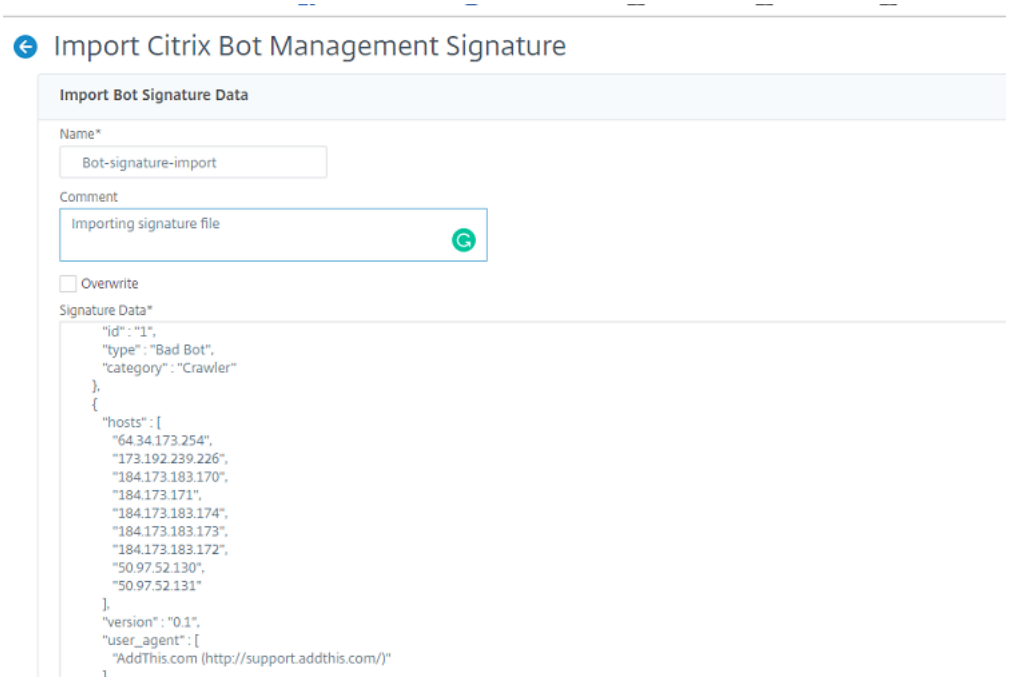
Wenn Sie eine eigene Signaturdatei haben, können Sie diese als Datei, Text oder URL importieren. Führen Sie die folgenden Schritte aus, um die Bot-Signaturdatei zu importieren:

1. Navigieren Sie zu **Sicherheit** > **Citrix Bot Management** and **Signaturen**.
2. Importieren Sie die Datei auf der Seite **Citrix Bot Management Signaturen** als URL, Datei oder Text.
3. Klicken Sie auf **Weiter**.



4. Legen Sie auf der Seite Citrix Bot Management-Signatur importieren die folgenden Parameter fest.
   a) Name. Name der Bot-Signaturdatei.
   b) Kommentar. Kurzbeschreibung der importierten Datei.
   c) überschreiben. Aktivieren Sie das Kontrollkästchen, um das Überschreiben von Daten während der Dateiaktualisierung zu ermöglichen.
   d) Signatur-Daten. Ändern von Signaturparametern

5. Klicken Sie auf **Fertig**.

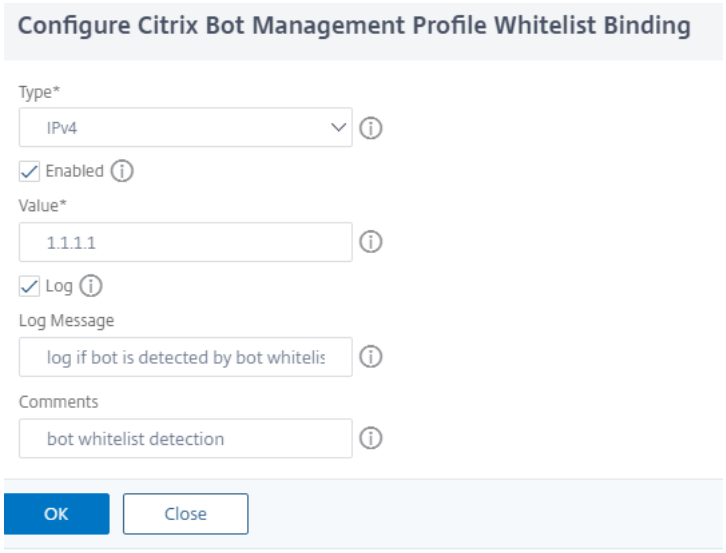


Konfigurieren der Bot-Positivliste über die Citrix ADC-GUI

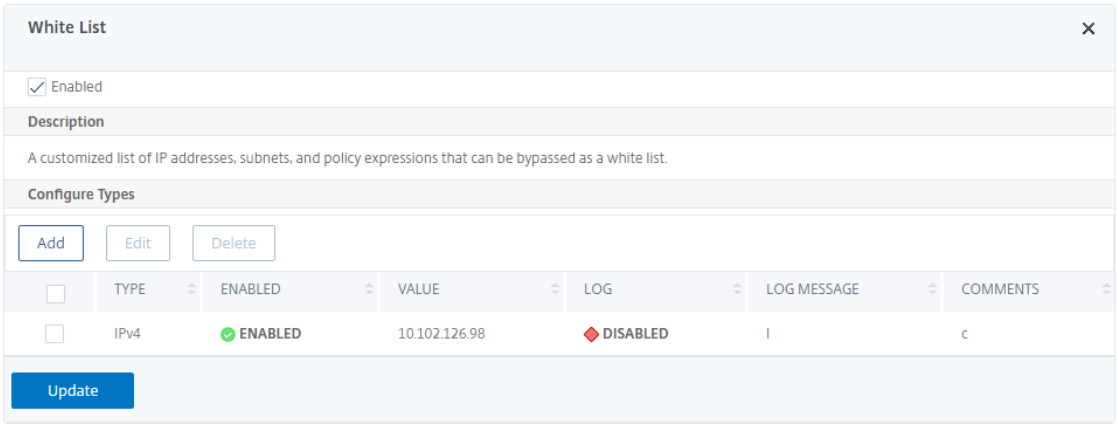
Mit dieser Erkennungstechnik können Sie URLs Bypass, die Sie als zulässige aufgelistete konfigurieren. Führen Sie den folgenden Schritt aus, um eine Positivliste zu konfigurieren:

1. Navigieren Sie zu **Sicherheit** > **Citrix Bot Management** and **Profiles**.
2. Wählen Sie auf der Seite **Citrix Bot Management-Profile** eine Datei aus und klicken Sie auf **Bearbeiten**.
3. Wechseln Sie auf der Seite **Citrix Bot-Verwaltungsprofil** zum Abschnitt **Signatureinstellungen** und klicken Sie auf **White List**.
4. Stellen Sie im Abschnitt **Positivliste** die folgenden Parameter ein:
   a) Aktiviert. Aktivieren Sie das Kontrollkästchen, um die URLs der Positivliste im Rahmen des Erkennungsprozesses zu validieren.
   b) Konfigurieren Sie Typen. Konfigurieren Sie eine URL für Positivlisten Die URL wird während der Bot-Erkennung umgangen. Klicken Sie auf Hinzufügen, um der Bot-Positivliste eine URL hinzuzufügen.
   c) Legen Sie auf der Seite **Configure Citrix Bot Management Profile Whitelist Binding** die folgenden Parameter fest:
      i. Typ. Der URL-Typ kann eine IPv4-Adresse, eine Subnetz-IP-Adresse oder eine IP-Adresse sein, die einem Richtlinienausdruck entspricht.
      ii. Aktiviert. Aktivieren Sie das Kontrollkästchen, um die URL zu validieren.

iii. Wert. URL-Adresse.
iv. Log. Aktivieren Sie das Kontrollkästchen, um Logeinträge zu speichern.
v. Meldung protokollieren. Kurzbeschreibung des Protokolls.
vi. Kommentare. Kurze Beschreibung der URL der Positivliste.
vii. Klicken Sie auf **OK**.



5. Klicken Sie auf **Aktualisieren**.
6. Klicken Sie auf **Fertig**.



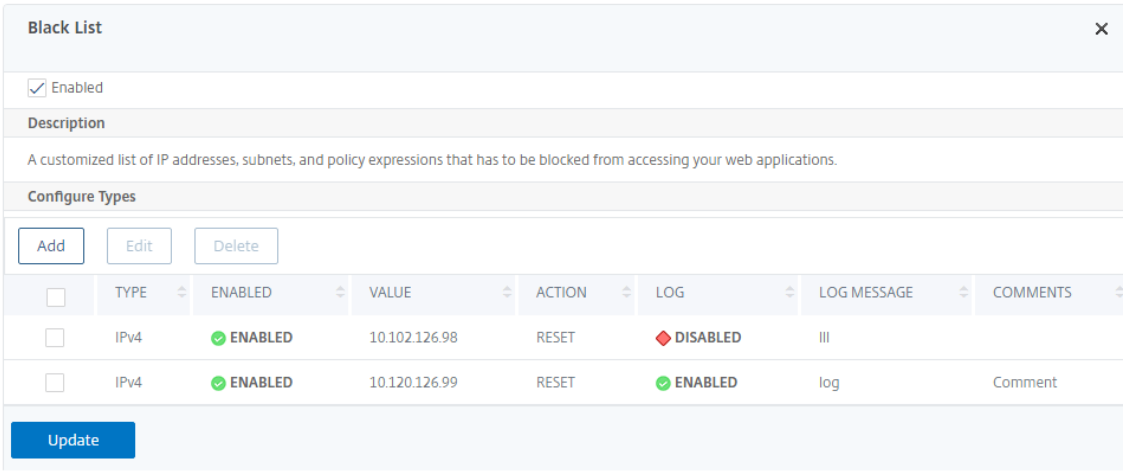
Konfigurieren Sie die Bot-Sperrliste über die Citrix ADC-GUI

Mit dieser Erkennungstechnik können Sie die URLs löschen, die Sie als Sperrlisten-URLs konfigurieren. Führen Sie den folgenden Schritt aus, um eine Sperrlisten-URL zu konfigurieren.

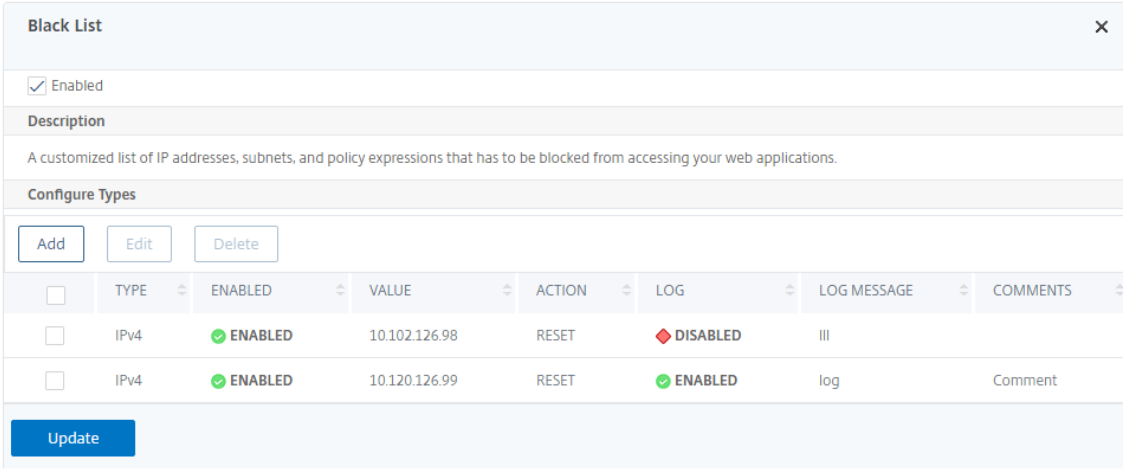
1. Navigieren Sie zu **Sicherheit** > **Citrix Bot Management** and **Profiles**.
2. Wählen Sie auf der Seite **Citrix Bot Management-Profile** eine Signaturdatei aus und klicken Sie

auf **Bearbeiten**.

3. Wechseln Sie auf der Seite **Citrix Bot-Verwaltungsprofil** zum Abschnitt **Signatureinstellungen** und klicken Sie auf **Black List**.
4. Stellen Sie im Abschnitt **Black List** die folgenden Parameter ein:
   a) Aktiviert. Aktivieren Sie das Kontrollkästchen, um Sperrlisten-URLs als Teil des Erkennungsprozesses zu validieren.
   b) Konfigurieren Sie Typen. Konfigurieren Sie eine URL, um Teil des Erkennungsprozesses für Bot-Sperrlisten zu sein. Diese URLs werden während der Bot-Erkennung gelöscht. Klicken Sie auf Hinzufügen, um eine URL zur Bot-Sperrliste hinzuzufügen.
   c) Legen Sie auf der Seite **Configure Citrix Bot Management Profile Blacklist Binding** die folgenden Parameter fest.
      i. Typ. Der URL-Typ kann eine IPv4-Adresse, eine Subnetz-IP-Adresse oder eine IP-Adresse sein.
      ii. Aktiviert. Aktivieren Sie das Kontrollkästchen, um die URL zu validieren.
      iii. Wert. URL-Adresse.
      iv. Log. Aktivieren Sie das Kontrollkästchen, um Logeinträge zu speichern.
      v. Meldung protokollieren. Kurzbeschreibung des Logins.
      vi. Kommentare. Kurze Beschreibung über die Sperrlisten-URL.
      vii. Klicken Sie auf **OK**.



5. Klicken Sie auf **Aktualisieren**.
6. Klicken Sie auf **Fertig**.



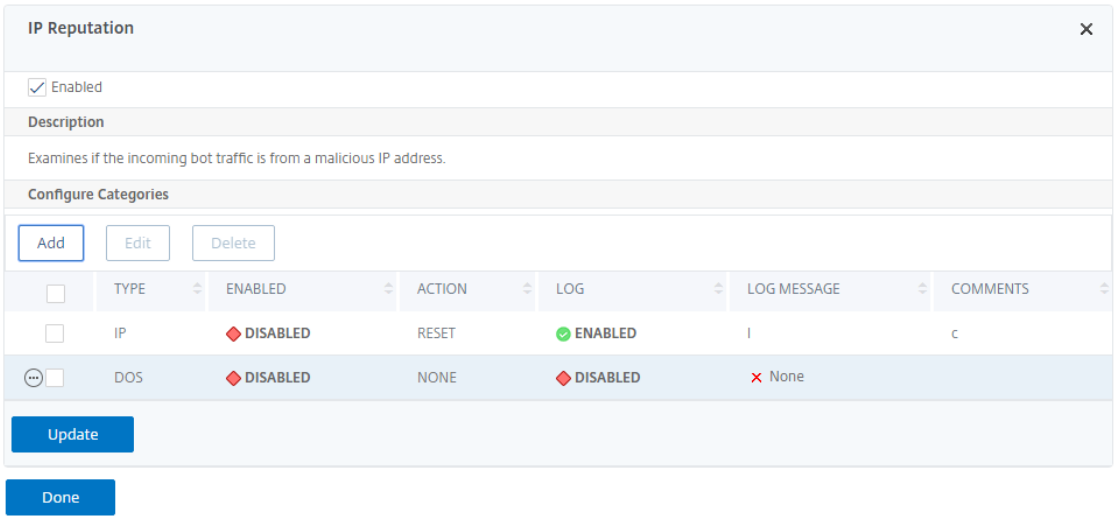
Konfigurieren Sie die IP-Reputation über die Citrix ADC-GUI

Diese Konfiguration ist eine Voraussetzung für die Bot-IP-Reputationsfunktion. Mit der Erkennungstechnik können Sie feststellen, ob von einer eingehenden IP-Adresse böswillige Aktivitäten vorliegen. Im Rahmen der Konfiguration legen wir verschiedene schädliche Bot-Kategorien fest und ordnen jeder Bot-Aktion eine Bot-Aktion zu. Führen Sie den folgenden Schritt aus, um die IP-Reputation-Technik zu konfigurieren.

1. Navigieren Sie zu **Sicherheit** > **Citrix Bot-Verwaltung** und **Profile**.
2. Wählen Sie auf der Seite **Citrix Bot Management-Profile** eine Signaturdatei aus und klicken Sie auf **Bearbeiten**.
3. Wechseln Sie auf der Seite **Citrix Bot-Verwaltungsprofil** zum Abschnitt **Signatureinstellungen** und klicken Sie auf **IP-Reputation**.
4. Stellen Sie im Abschnitt **IP-Reputation** die folgenden Parameter ein:
   a) Aktiviert. Aktivieren Sie das Kontrollkästchen, um eingehenden Bot-Verkehr als Teil des Erkennungsprozesses zu validieren.
   b) Konfigurieren Sie Kategorien. Sie können die IP-Reputationstechnik für eingehenden Bot-Verkehr in verschiedenen Kategorien verwenden. Basierend auf der konfigurierten Kategorie können Sie den Bot-Traffic löschen oder umleiten. Klicken Sie auf **Hinzufügen**, um eine schädliche Bot-Kategorie zu konfigurieren.
   c) Legen Sie auf der Seite **IP-Reputationsbindung des Citrix Bot-Verwaltungsprofils konfigurieren** die folgenden Parameter fest:
      i. Kategorie. Wählen Sie eine böswillige Bot-Kategorie aus der Liste aus. Ordnen Sie eine Bot-Aktion basierend auf der Kategorie zu.
      ii. Aktiviert. Aktivieren Sie das Kontrollkästchen, um die Erkennung von IP-Reputations-Signaturen

iii. Bot-Aktion. Basierend auf der konfigurierten Kategorie können Sie keine Aktion, Drop, Umleitung, Minderung oder CAPTCHA-Aktion zuweisen.
iv. Log. Aktivieren Sie das Kontrollkästchen, um Logeinträge zu speichern.
v. Meldung protokollieren. Kurzbeschreibung des Protokolls.
vi. Kommentare. Kurze Beschreibung der Bot-Kategorie.

5. Klicken Sie auf **OK**.
6. Klicken Sie auf **Aktualisieren**.
7. Klicken Sie auf **Fertig**.



Konfigurieren Sie das Bot-Ratenlimit über die Citrix ADC-GUI

Mit dieser Erkennungstechnik können Sie Bots basierend auf der Anzahl der Anfragen blockieren, die innerhalb einer vordefinierten Zeit von einer Client-IP-Adresse, einer Sitzung oder einer konfigurierten Ressource (z. B. von einer URL) empfangen wurden. Führen Sie den folgenden Schritt aus, um die Ratenbegrenzungstechnik zu konfigurieren.

1. Navigieren Sie zu **Sicherheit** > **Citrix Bot Management** and **Profiles**.
2. Wählen Sie auf der Seite **Citrix Bot Management-Profile** eine Signaturdatei aus und klicken Sie auf **Bearbeiten**.
3. Wechseln Sie auf der Seite **Citrix Bot-Verwaltungsprofil** zum Abschnitt **Signatureinstellungen** und klicken Sie auf **Ratenbegrenzung**.
4. Stellen Sie im Abschnitt **Ratenbegrenzung** die folgenden Parameter ein:

   a) Aktiviert. Aktivieren Sie das Kontrollkästchen, um den eingehenden Bot-Verkehr im Rahmen des Erkennungsprozesses zu validieren.

b) Sitzung. Ratenbegrenzungsanfragen basierend auf einer Sitzung. Klicken Sie auf Hinzufügen, um Tarifbegrenzungsanfragen basierend auf einer Sitzung zu konfigurieren.

c) Legen **Sie auf der Seite Citrix Bot Management Signaturratenlimit konfigurieren** die folgenden Parameter fest.

i. Kategorie. Wählen Sie eine böswillige Bot-Kategorie aus der Liste aus. Ordnen Sie eine Aktion basierend auf der Kategorie zu.

ii. Aktiviert. Aktivieren Sie das Kontrollkästchen, um den eingehenden Bot-Verkehr zu validieren.

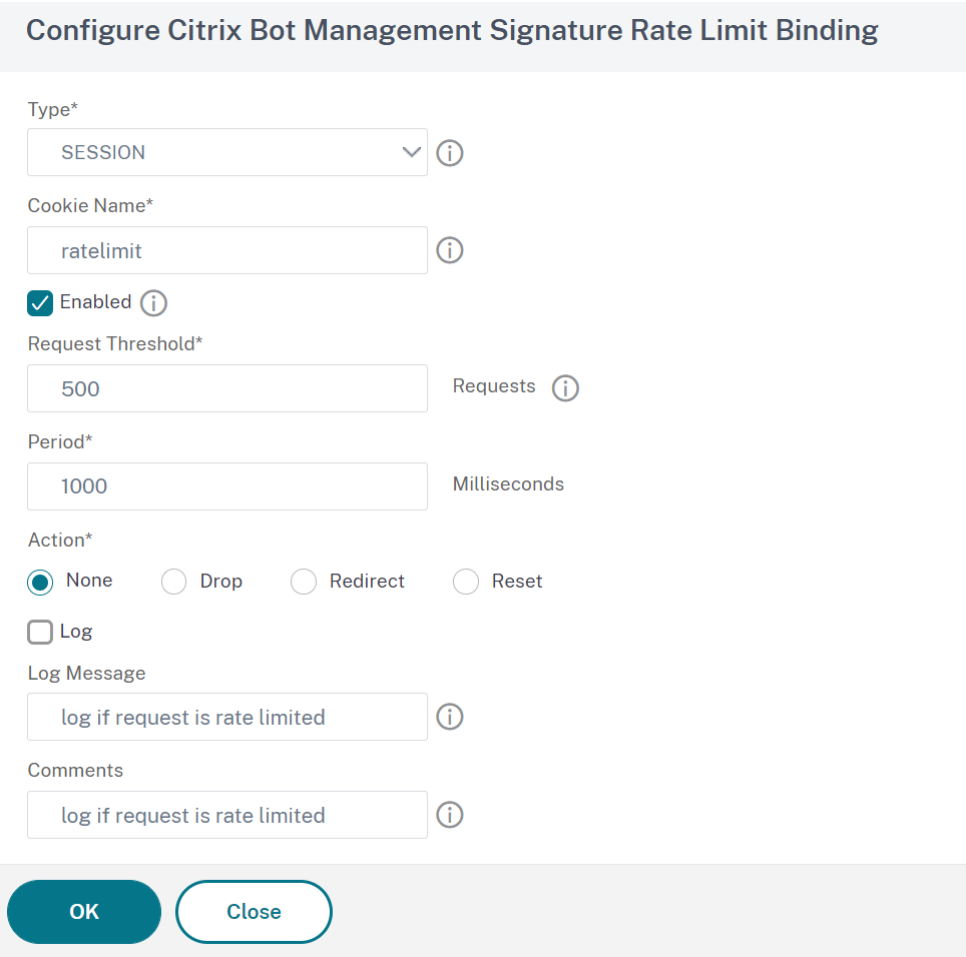
iii. Bot-Aktion. Wählen Sie eine Bot-Aktion für die ausgewählte Kategorie.

iv. Log. Aktivieren Sie das Kontrollkästchen, um Logeinträge zu speichern.

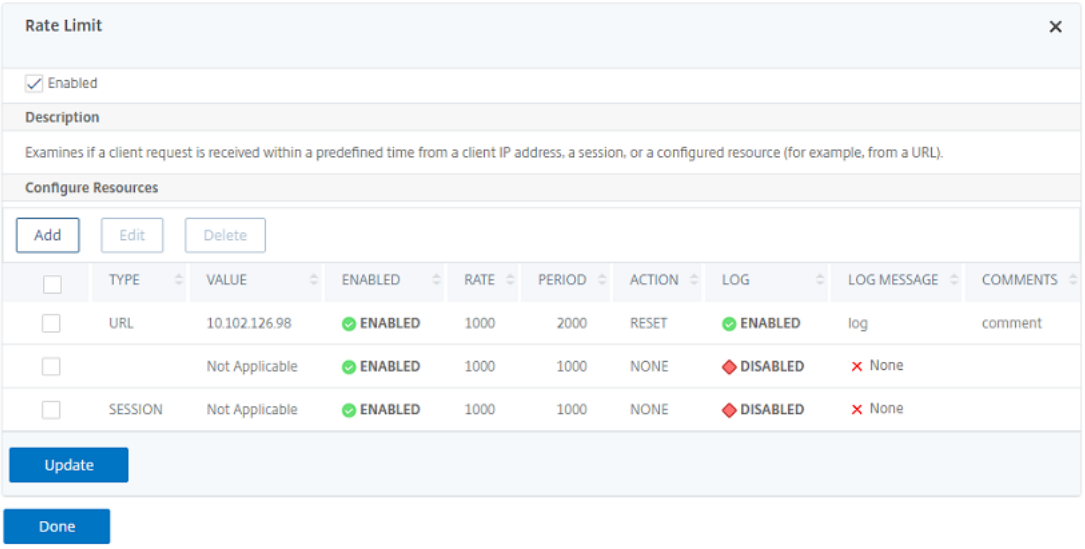
v. Meldung protokollieren. Kurzbeschreibung des Protokolls.

vi. Kommentare. Kurze Beschreibung der Bot-Kategorie.

vii. Klicken Sie auf **OK**.



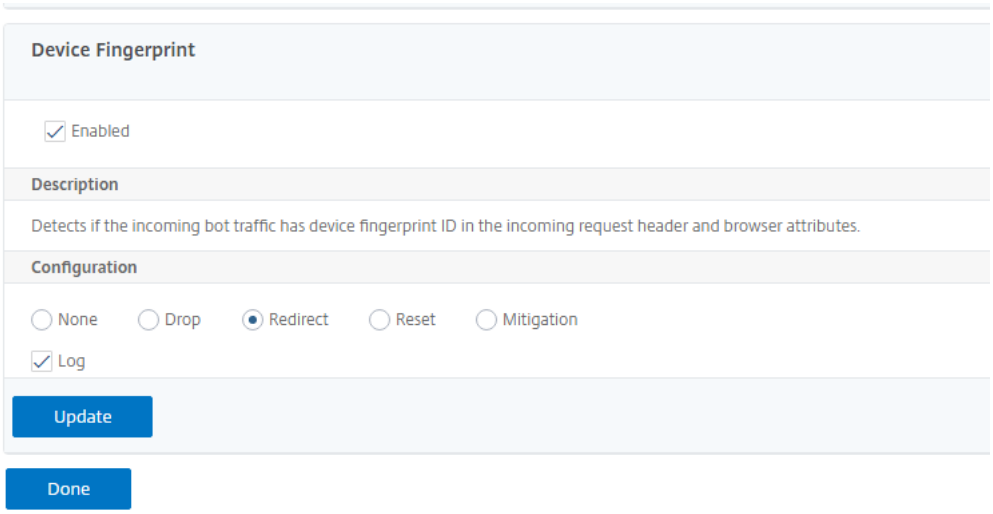
5. Klicken Sie auf **Aktualisieren**.
6. Klicken Sie auf **Fertig**.



Konfigurieren Sie die Geräte-Fingerabdrucktechnik über die Citrix ADC-GUI

Diese Erkennungstechnik sendet eine Java-Skript-Herausforderung an den Client und extrahiert die Geräteinformationen. Basierend auf Geräteinformationen lässt die Technik den Bot-Verkehr fallen oder umgeht. Folgen Sie den Schritten, um die Erkennungstechnik zu konfigurieren.

1. Navigieren Sie zu **Sicherheit** > **Citrix Bot Management** and **Profiles**.
2. Wählen Sie auf der Seite **Citrix Bot Management-Profile** eine Signaturdatei aus und klicken Sie auf **Bearbeiten**.
3. Gehen Sie auf der Seite **Citrix Bot-Verwaltungsprofil** zum Abschnitt **Signatureinstellungen** und klicken Sie auf **Geräte-Fingerabdruck**.
4. Stellen Sie im Abschnitt **Geräte-Fingerabdruck** die folgenden Parameter ein:
   a) Aktiviert. Stellen Sie diese Option ein, um die Regel zu aktivieren.
   b) Konfiguration. Weisen Sie für den angegebenen Geräte-Fingerabdruck keine Aktion, Drop oder Umleitung, Abschwächung oder CAPTCHA-Aktion zu.
   c) Log. Aktivieren Sie das Kontrollkästchen, um Logeinträge zu speichern.
5. Klicken Sie auf **Aktualisieren**.
6. Klicken Sie auf **Fertig**.



Konfigurieren der Geräte-Fingerabdruck-Technik für mobile (Android) -Anwendungen

Die Geräte-Fingerabdruck-Technik erkennt einen eingehenden Datenverkehr als Bot, indem ein JavaScript-Skript in die HTML-Antwort an den Client eingefügt wird. Wenn das JavaScript-Skript vom Browser aufgerufen wird, sammelt es Browser- und Client-Attribute und sendet eine Anfrage an die Appliance. Die Attribute werden untersucht, um festzustellen, ob es sich bei dem Traffic um einen Bot oder einen Menschen handelt.

Die Erkennungstechnik wird weiter erweitert, um Bots auf einer mobilen (Android) Plattform zu erkennen. Im Gegensatz zu Webanwendungen gilt im mobilen (Android) -Verkehr die Bot-Erkennung basierend auf dem JavaScript-Skript nicht. Um Bots in einem Mobilfunknetz zu erkennen, verwendet die Technik ein Bot Mobile SDK, das clientseitig in mobile Anwendungen integriert ist. Das SDK fängt den mobilen Verkehr ab, sammelt Gerätedetails und sendet die Daten an die Appliance. Auf der Appliance-Seite untersucht die Erkennungstechnik die Daten und bestimmt, ob die Verbindung von einem Bot oder einem Menschen stammt.

So funktioniert die Geräte-Fingerabdruck-Technik für mobile Anwendungen

In den folgenden Schritten wird der Workflow zur Bot-Erkennung erläutert, um festzustellen, ob eine Anfrage von einem mobilen Gerät von einem Menschen oder einem Bot stammt.

1. Wenn ein Benutzer mit einer mobilen Anwendung interagiert, wird das Geräteverhalten vom Bot Mobile SDK aufgezeichnet.
2. Der Client sendet eine Anfrage an die Citrix ADC-Appliance.
3. Beim Senden der Antwort fügt die Appliance ein Bot-Sitzungscookie mit Sitzungsdetails und Parametern ein, um Clientparameter zu erfassen.
4. Wenn die mobile Anwendung die Antwort erhält, validiert das Citrix Bot SDK, das in die mobile Anwendung integriert ist, die Antwort, ruft die aufgezeichneten Geräte-Fingerabdruckparameter

ab und sendet sie an die Appliance.
5. Die Technik zur Erkennung von Fingerabdrücken des Geräts auf der Appliance-Seite validiert die Gerätedetails und aktualisiert das Bot-Sitzungscookie, ob es sich um einen vermuteten Bot handelt oder nicht.
6. Wenn das Cookie abgelaufen ist oder der Fingerabdruckschutz des Geräts es vorzieht, Geräteparameter regelmäßig zu validieren und zu sammeln, wird der gesamte Vorgang oder die Herausforderung wiederholt.

Voraussetzung

Um mit der Citrix ADC-Technik zur Erkennung von Fingerabdrücken für mobile Anwendungen zu beginnen, müssen Sie das Bot Mobile SDK in Ihrer mobilen Anwendung herunterladen und installieren.

Konfigurieren Sie die Technik der Fingerabdruckerkennung für mobile (Android) -Anwendungen über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

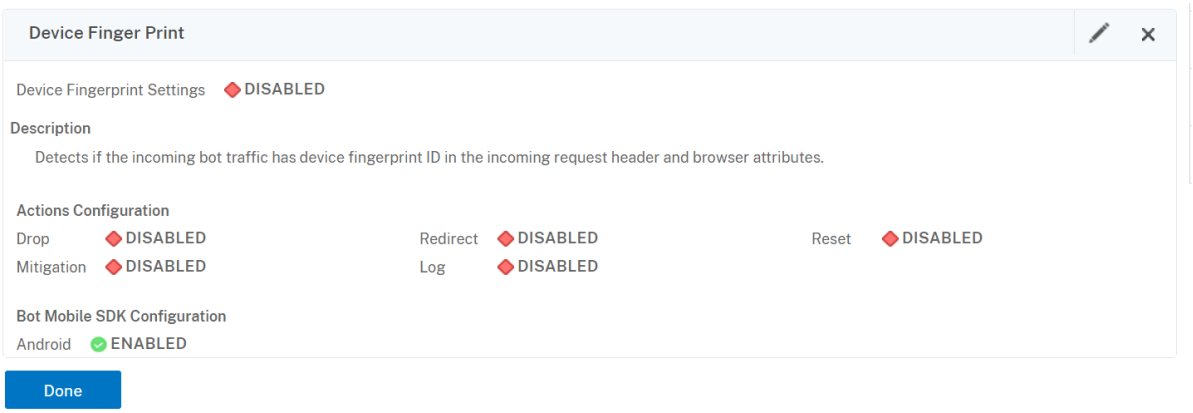
```
set bot profile <profile name> -deviceFingerprintMobile ( NONE | Android )
```

Beispiel:

```
set bot profile profile 1 -deviceFingerprintMobile Android
```

Konfigurieren Sie die Technik zur Erkennung von Geräte-Fingerabdrücken für mobile (Android) -Anwendungen über die GUI

1. Navigieren Sie zu **Sicherheit** > **Citrix Bot Management** and **Profiles**.
2. Wählen Sie auf der Seite **Citrix Bot Management-Profile** eine Datei aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Citrix Bot-Verwaltungsprofil** unter **Profileinstellungen** auf **Geräte-Fingerabdruck**.
4. Wählen **Sie im Abschnitt Configure Bot Mobile SDK** den Typ des mobilen Clients aus.
5. Klicken Sie auf **Aktualisieren** und **Fertig**.



Bot-Log-Ausdruck konfigurieren

Wenn der Client als Bot identifiziert wird, können Sie mit der Citrix Bot-Verwaltung zusätzliche Informationen als Protokollnachrichten erfassen. Die Daten können der Name des Benutzers sein, der die URL angefordert hat, die Quell-IP-Adresse und der Quellport, von dem der Benutzer die Anforderung oder Daten gesendet hat, die aus einem Ausdruck generiert wurden. Um eine benutzerdefinierte Protokollierung durchzuführen, müssen Sie einen Protokollausdruck im Bot-Verwaltungsprofil konfigurieren.

Binden Sie den Log-Ausdruck im Bot-Profil über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind bot profile <name> (-logExpression -name <string> -expression <
    expression> [-enabled ( ON | OFF )]) -comment <string>
2 <!--NeedCopy-->
```

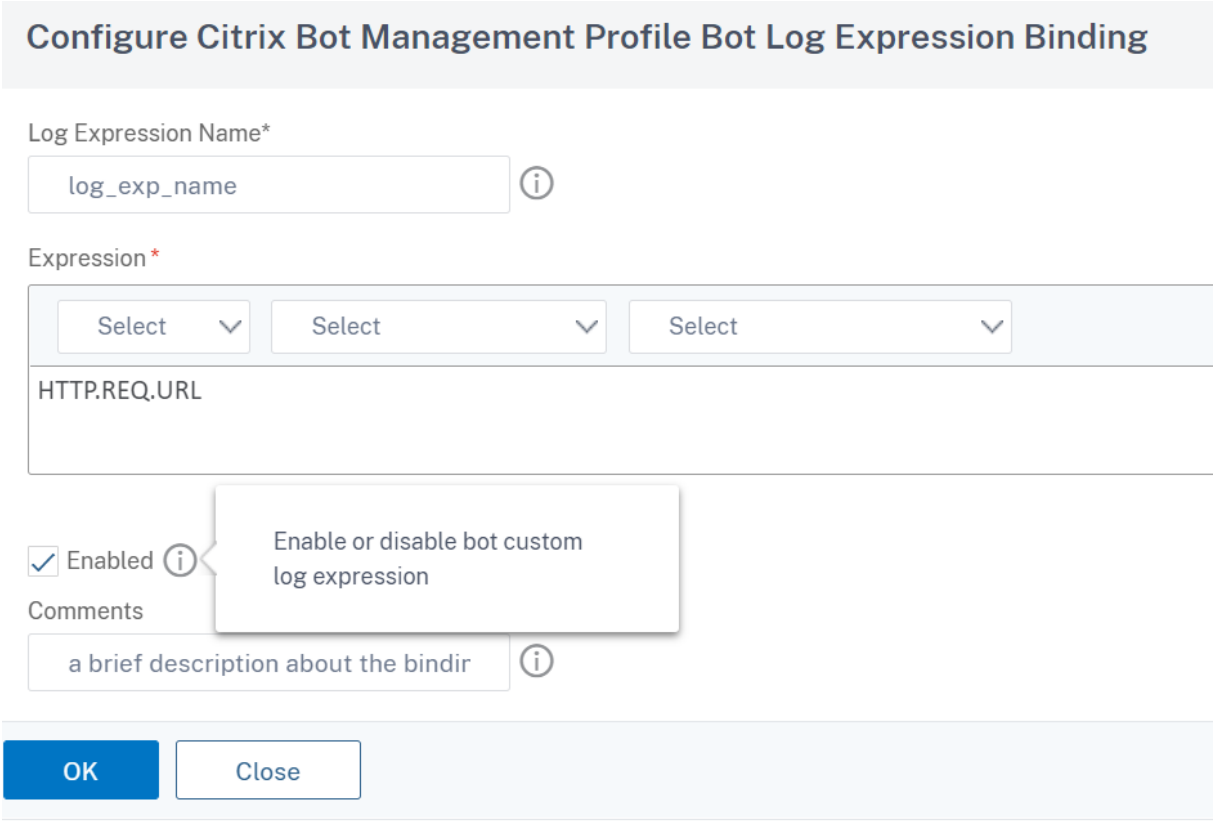
Beispiel:

```
bind bot profile profile1 -logExpression exp1 -expression HTTP.REQ.URL -
enabled ON -comment ”testing log expression”
```

Binden Sie den Log-Ausdruck über die GUI an das Bot-Profil

1. Navigieren Sie zu **Sicherheit > Citrix Bot Management > Profiles**.
2. Wählen Sie auf der Seite **Citrix Bot Managementprofile** im Abschnitt **Profileinstellungen** die Option **Bot-Protokollausdrücke** aus.
3. Klicken Sie im Abschnitt Einstellungen für **Bot Log Expression Settings* auf **Hinzufügen**.

4. Legen Sie auf der Seite **Configure Citrix Bot Management Profile Bot Log Expression Binding** die folgenden Parameter fest.
   a) Name des Protokollausdrucks Name des Protokollausdrucks.
   b) Ausdruck. Geben Sie den Log-Ausdruck ein.
   c) Aktiviert. Aktivieren oder deaktivieren Sie die Bindung des Logausdrucks.
   d) Kommentare. Eine kurze Beschreibung zur Bindung des Bot-Log-Ausdrucks.
5. Klicken Sie auf**OK** und **Fertig**.



Konfigurieren der Bot-Trap-Technik

Die Citrix Bot-Trap-Technik fügt zufällig oder regelmäßig eine Trap-URL in die Clientantwort ein. Sie können auch eine Trap-URL-Liste erstellen und URLs dafür hinzufügen. Die URL erscheint unsichtbar und nicht zugänglich, wenn der Client ein menschlicher Benutzer ist. Wenn der Client jedoch ein automatisierter Bot ist, ist die URL zugänglich, und wenn darauf zugegriffen wird, wird der Angreifer als Bot kategorisiert und jede nachfolgende Anfrage des Bot wird blockiert. Die Trap-Technik blockiert effektiv Angriffe von Bots.

Die Trap-URL ist eine alphanumerische URL mit konfigurierbarer Länge und wird im konfigurierbaren

Intervall automatisch generiert. Mit dieser Technik können Sie auch eine URL zum Einfügen von Traps für am häufigsten besuchte Sites oder häufig besuchte Sites konfigurieren. Auf diese Weise können Sie den Zweck festlegen, die Bot-Trap-URL für Anforderungen einzufügen, die der URL zum Einfügen von Traps entsprechen.

> **Hinweis:**
>
> Obwohl die Bot-Trap-URL automatisch generiert wird, ermöglicht Ihnen das Citrix ADC-Bot-Management weiterhin die Konfiguration einer benutzerdefinierten Trap-URL im Bot-Profil. Dies geschieht, um
> die Bot-Erkennungstechnik zu stärken und Angreifern den Zugriff auf die Trap-URL zu erschweren.

Um die Konfiguration der Bot-Trap abzuschließen, müssen Sie die folgenden Schritte ausführen.

1. Bot-Trap-URL aktivieren
2. Konfigurieren der Bot-Trap-URL im Bot-Profil
3. Binden Sie die URL zum Einfügen von Bot-Traps an
4. Konfigurieren Sie die Länge und das Intervall der Bot-Trap-URL in den Bot

Den URL-Schutz für Bot-Trap aktivieren

Bevor Sie beginnen können, müssen Sie sicherstellen, dass der Bot-Trap-URL-Schutz auf der Appliance aktiviert ist. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns feature Bot
```

Konfigurieren der Bot-Trap-URL im Bot-Profil

Sie können die Bot-Trap-URL konfigurieren und eine Trap-Aktion im Bot-Profil angeben.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add bot profile <name> -trapURL <string> -trap ( ON | OFF )-trapAction <
trapAction>
```

Hierbei gilt:

`trapURL`. URL, die der Bot-Schutz als Trap-URL verwendet. Maximale Länge: 127

`trap`. Erkennung von Bot-Trapn aktivieren. Mögliche Werte: ON, OFF, Standardwert: OFF

`trapAction`. Zu ergreifende Maßnahmen basierend auf Bot-Erkennung. Mögliche Werte: NONE, LOG, DROP, REDIRECT, RESET, MITIGATION. Standardwert: NONE

Beispiel:

```
add bot profile profile1 -trapURL www.bottrap1.com trap ON -trapAction
RESET
```


Binden Sie die URL zum Einfügen von Bot-Traps an

Sie können die URL zum Einfügen von Bot-Traps konfigurieren und an das Bot-Profil binden.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind bot profile <profile_name> trapInsertionURL -url <url> -enabled ON|OFF
-comment <comment>
```

Hierbei gilt:

`URL`. Fordern Sie ein URL-Regex-Muster an, für das die Bot-Trap-URL eingefügt wird. Maximale Länge: 127

Beispiel:

```
bind bot profile profile1 trapInsertionURL -url www.example.com -enabled ON
-comment insert a trap URL randomly
```

Konfigurieren Sie die Länge und das Intervall der Bot-Trap-URL in den Bot

Sie können die Länge der Bot-Trap-URL konfigurieren und das Intervall festlegen, um die Bot-Trap-URL automatisch zu generieren.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set bot settings -trapURLAutoGenerate ( ON | OFF )-trapURLInterval <positive_integer
> -trapURLLength <positive_integer>
```

Hierbei gilt:

`trapURLInterval`. Zeit in Sekunden, nach der die URL der Bot-Trap aktualisiert wird. Standardwert: 3600, Mindestwert: 300, Maximalwert: 86400

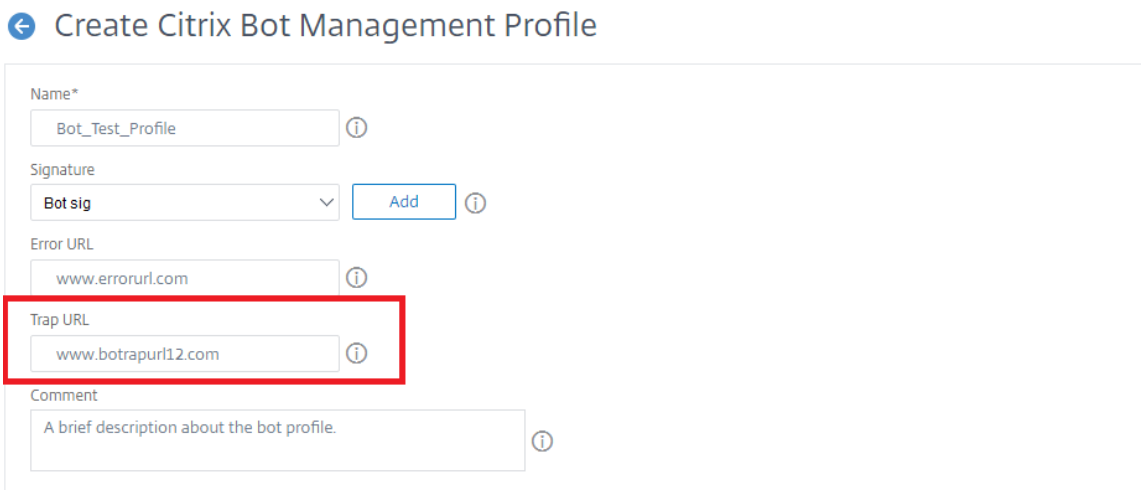
`trapURLLength`. Länge der automatisch generierten Bot-Trap-URL. Standardwert: 32, Mindestwert: 10, Maximalwert: 255

Beispiel:

```
set bot settings -trapURLAutoGenerate ON -trapURLInterval 300 -trapURLLength
 60
```

Konfigurieren Sie die Bot-Trap-URL über die GUI

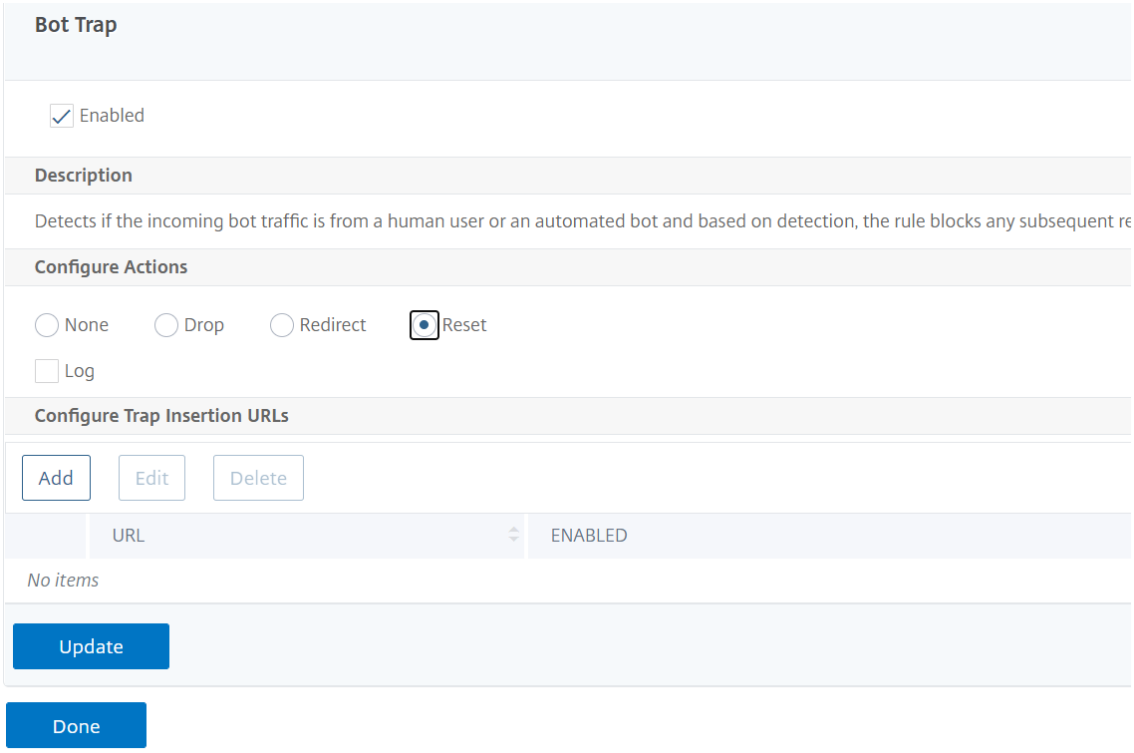
1. Navigieren Sie zu **Sicherheit > Citrix Bot Management > Profiles**.
2. Klicken Sie auf der Seite **Citrix Bot-Verwaltungsprofile** auf **Bearbeiten**, um die Bot-Trap-URL-Technik zu konfigurieren.
3. Geben Sie auf der Seite **Citrix Bot-Verwaltungsprofil erstellen** die Bot-Trap-URL im Abschnitt “Allgemein” ein.



4. Klicken Sie auf der Seite **Citrix Bot-Verwaltungsprofil erstellen** in den **Profileinstellungen** auf **Bot-Trap**.

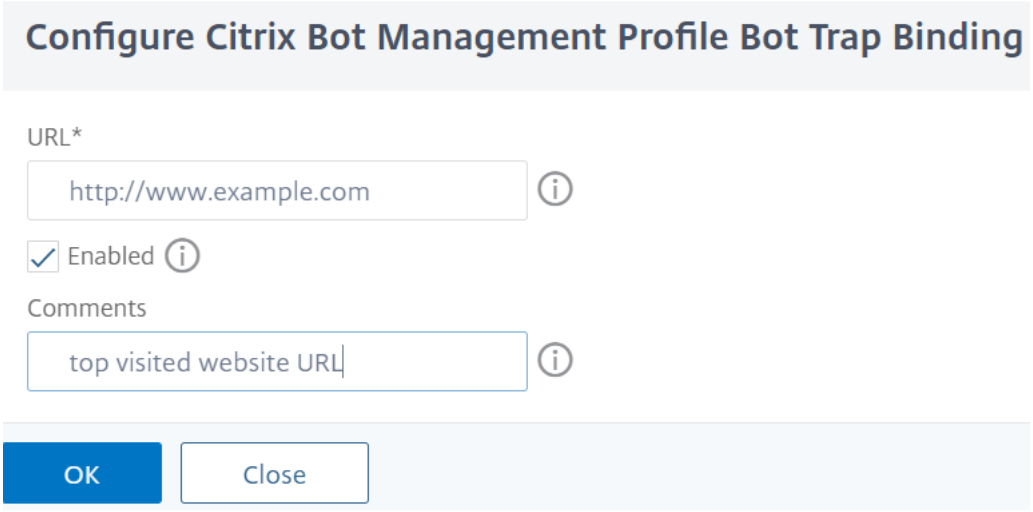
5. Stellen Sie im Abschnitt **Bot-Trap** die folgenden Parameter ein.

   a. Aktiviert. Aktivieren Sie das Kontrollkästchen, um die Erkennung
   von Bot-Traps zu aktivieren. Kurze Beschreibung der URL.
   c. Konfigurieren Sie Aktionen. Zu ergreifende Maßnahmen für Bot, die durch den Zugriff auf die Bot-Trap erkannt werden.



6. Klicken Sie im Abschnitt **Trap-Einfügungs-URLs konfigurieren** auf **Hinzufügen**.

7. Legen Sie auf der Seite **Bot-Trap-Bindung des Citrix Bot-Verwaltungsprofils konfigurieren** die folgenden Parameter fest.
   a) Trap-URL. Geben Sie die zu bestätigende URL als URL zum Einfügen von Bot-Traps ein.
   b) Aktiviert. Aktiviert oder deaktiviert Bot-Trap-Einfüge-URL.
   c) Kommentar. Eine kurze Beschreibung der URL zum Einfügen von Traps.



8. Klicken Sie im Abschnitt **Signatureinstellungen** auf **Bot Trap**.
9. Stellen Sie im Abschnitt **Bot Trap** die folgenden Parameter ein:
   a) Aktiviert. Aktivieren Sie das Kontrollkästchen, um die Erkennung von Bot-Traps zu aktivieren.
   b) Stellen Sie im Abschnitt Konfigurieren die folgenden Parameter ein.
      i. Aktion. Zu ergreifende Maßnahmen für Bot, die durch den Zugriff auf die Bot-Trap erkannt werden.
      ii. Log. Aktiviert oder deaktiviert die Protokollierung für die Bindung von Bot-Traps.
10. Klicken Sie auf **Aktualisieren** und **Fertig**.

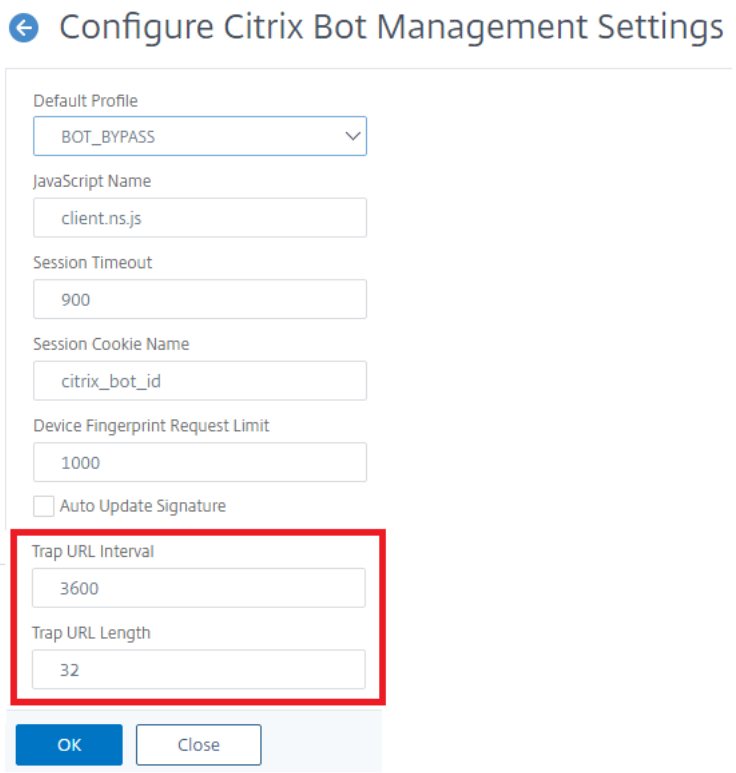
Konfigurieren von Bot-Trap-URL-Einstellungen

Führen Sie die folgenden Schritte aus, um die URL-Einstellungen für Bot-Trap zu konfigurieren

1. Navigieren Sie zu **Sicherheit > Citrix Bot Management**.
2. Klicken Sie im Detailbereich unter **Einstellungen** auf **Citrix Bot Management-Einstellungen ändern**.
3. Legen Sie in den **Citrix Bot-Verwaltungseinstellungen konfigurieren** die folgenden Parameter fest.
   a) Trap-URL-Intervall. Zeit in Sekunden, nach der die URL der Bot-Trap aktualisiert wird.

b) Länge der Trap-URL. Länge der automatisch generierten Bot-Trap-URL.

4. Klicken Sie auf **OK** und **Fertig**.



Ausdruck der Client-IP-Richtlinie zur Bot-Erkennung

Mit der Citrix Bot-Verwaltung können Sie jetzt einen erweiterten Richtlinienausdruck konfigurieren, um die Client-IP-Adresse aus einem HTTP-Anforderungsheader, einem HTTP-Anforderungstext, einer HTTP-Anforderungs-URL oder einem erweiterten Richtlinienausdruck zu extrahieren. Der extrahierte Wert kann von einem Bot-Erkennungsmechanismus (wie TPS, Bot-Trap oder Ratenlimit) verwendet werden, um festzustellen, ob es sich bei der eingehenden Anforderung um einen Bot handelt.

> **Hinweis:**
>
> Wenn Sie keinen Client-IP-Ausdruck konfiguriert haben, wird die Standard- oder vorhandene Quellclient-IP-Adresse für die Bot-Erkennung verwendet. Wenn ein Ausdruck konfiguriert ist, liefert das Auswertergebnis die Client-IP-Adresse, die für die Bot-Erkennung verwendet werden kann.

Sie können den Client-IP-Ausdruck konfigurieren und verwenden, um die tatsächliche Client-IP-Adresse zu extrahieren, wenn die eingehende Anforderung über einen Proxy-Server erfolgt und wenn die Client-IP-Adresse im Header vorhanden ist. Durch das Hinzufügen dieser Konfiguration kann die Appliance den Bot-Erkennungsmechanismus verwenden, um Software-Clients und Servern mehr

Sicherheit zu bieten.

Konfigurieren Sie den IP-Richtlinienausdruck des Clients im Bot-Profil über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

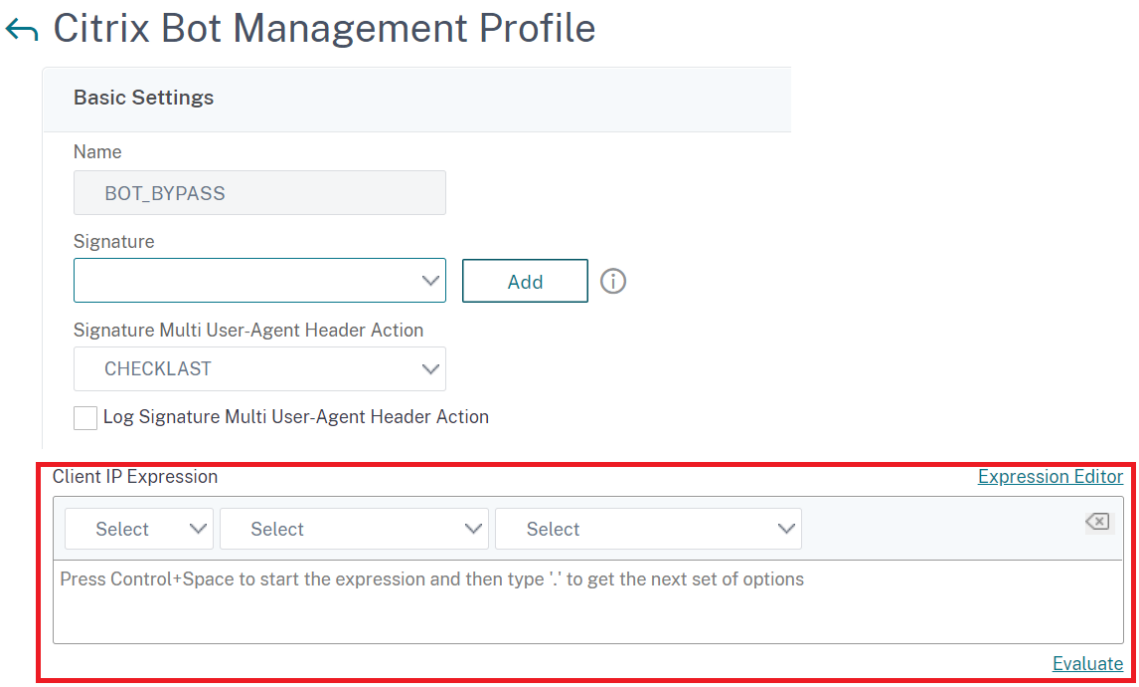
```
1 add bot profile <name> [-clientIPExpression <expression>]
2 <!--NeedCopy-->
```

Beispiel:

```
add bot profile profile1 -clientIPExpression 'HTTP.REQ.HEADER(”X-Forwarded-For”)ALT CLIENT.IP.SRC.TYPECAST_TEXT_T'
```

Konfigurieren Sie den Ausdruck der Client-IP-Richtlinie im Bot-Profil über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Sicherheit > Citrix Bot Management > Profiles**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **Citrix Bot-Verwaltungsprofil erstellen** den Client-IP-Ausdruck fest.
4. Klicken Sie auf **Erstellen** und **Schließen**.



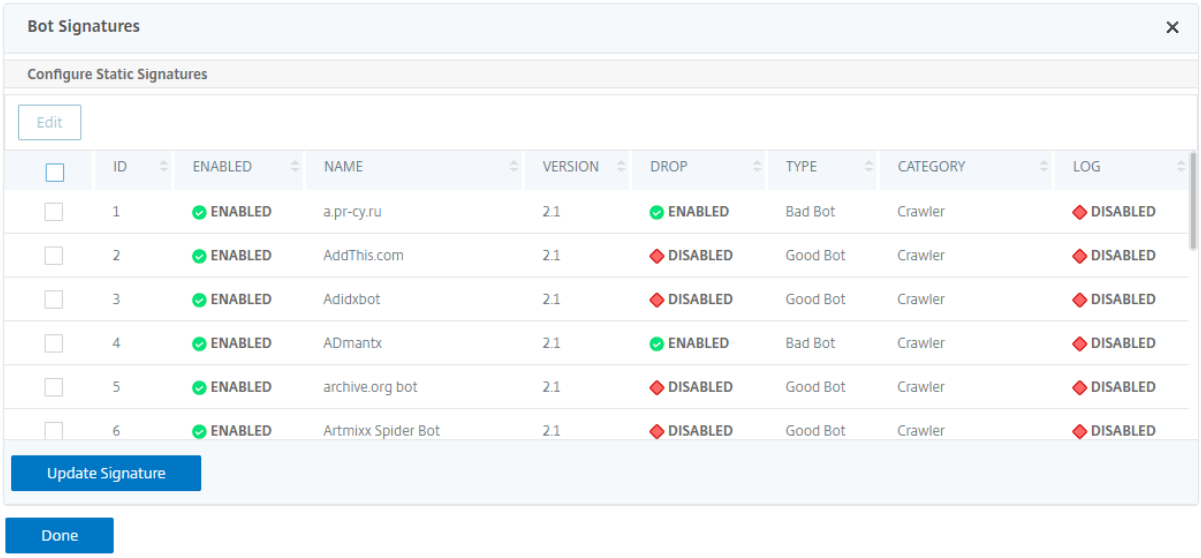
Konfigurieren von CAPTCHA für IP-Reputation und Gerätefingerabdruckerkennung

CAPTCHA ist ein Akronym, das für "Vollständig automatisierter öffentlicher Turing-Test, um Computer und Menschen voneinander zu unterscheiden" steht. CAPTCHA wurde entwickelt, um zu testen, ob ein eingehender Verkehr von einem menschlichen Benutzer oder einem automatisierten Bot stammt. CAPTCHA hilft dabei, automatisierte Bots zu blockieren, die Sicherheitsverletzungen für Webanwendungen verursachen. In der ADC-Appliance verwendet CAPTCHA das Challenge-Response-Modul, um festzustellen, ob der eingehende Datenverkehr von einem menschlichen Benutzer und nicht von einem automatisierten Bot stammt.

Konfigurieren statischer Bot-Signaturen

Diese Erkennungstechnik ermöglicht es Ihnen, die Benutzeragent-Informationen aus den Browserdetails zu identifizieren. Basierend auf Benutzeragent-Informationen wird der Bot als schlechter oder guter Bot identifiziert und dann weisen Sie ihm eine Bot-Aktion zu. Befolgen Sie die nachstehenden Schritte zur Konfiguration der statischen Signaturtechnik:

1. Erweitern Sie im Navigationsbereich **Sicherheit > Citrix Bot Management > Signaturen**.
2. Wählen Sie auf der Seite **Citrix Bot Management-Signaturen** eine Signaturdatei aus, und klicken Sie auf **Bearbeiten**.
3. Gehen Sie auf der Seite **Citrix Bot Management Signaturezum Abschnitt Signatureinstellungen**und klicken Sie auf**Bot-Signaturen**.
4. Stellen Sie im Abschnitt **Bot-Signaturen** die folgenden Parameter ein:
    a) Konfigurieren Sie statische Signaturen. Dieser Abschnitt enthält eine Liste der statischen Signaturdatensätze des Bot. Sie können einen Datensatz auswählen und auf **Bearbeiten** klicken, um ihm eine Bot-Aktion zuzuweisen.
    b) Klicken Sie auf **OK**.
5. Klicken Sie auf **Signatur aktualisieren**.
6. Klicken Sie auf **Fertig**.



Abgrenzung der statischen Unterschrift Bot

Citrix ADC Bot Management schützt Ihre Webanwendung vor Bots. Statische Bot-Signaturen helfen dabei, gute und schlechte Bots basierend auf Anforderungsparametern wie User-Agent in der eingehenden Anforderung zu identifizieren.
Die Liste der Signaturen in der Datei ist riesig und es werden auch neue Regeln hinzugefügt und abgestandene werden regelmäßig entfernt. Als Administrator möchten Sie möglicherweise nach einer bestimmten Signatur oder einer Liste von Signaturen unter einer Kategorie suchen. Um Signaturen einfach zu filtern, bietet die Bot-Signaturseite eine verbesserte Suchfunktion. Mit der Suchfunktion können Sie Signaturregeln finden und ihre Eigenschaft basierend auf einem oder mehreren Signaturparametern wie Aktion, Signatur-ID, Entwickler und Signaturnamen konfigurieren.

Aktion. Wählen Sie eine Bot-Aktion aus, die Sie lieber für eine bestimmte Kategorie von Signaturregeln konfigurieren möchten. Im Folgenden sind die verfügbaren Aktionstypen aufgeführt:

- Aktivieren Sie Ausgewählt. Aktivieren Sie alle ausgewählten Signaturregeln.
- Deaktivieren Sie Ausgewählt. Deaktivieren Sie alle Regeln für ausgewählte Signaturen.
- Auswahl löschen. Wenden Sie die Aktion als “Drop” auf alle ausgewählten Signaturregeln an.
- Weiterleitung Ausgewählt. Wenden Sie die Aktion als “Umleitung” auf alle ausgewählten Signaturregeln an.
- Ausgewählt zurücksetzen. Wenden Sie die Aktion als “Zurücksetzen” auf alle ausgewählten Signaturregeln an.
- Log Ausgewählt. Wenden Sie die Aktion als “Log” auf alle ausgewählten Signaturregeln an.
- Entfernen Sie “Auswahl löschen”. Heben Sie die Drop-Aktion auf alle ausgewählten Signaturregeln auf.
- Entfernen Sie Redirect Selected. Heben Sie die Umleitungsaktion auf alle ausgewählten Signaturregeln auf.

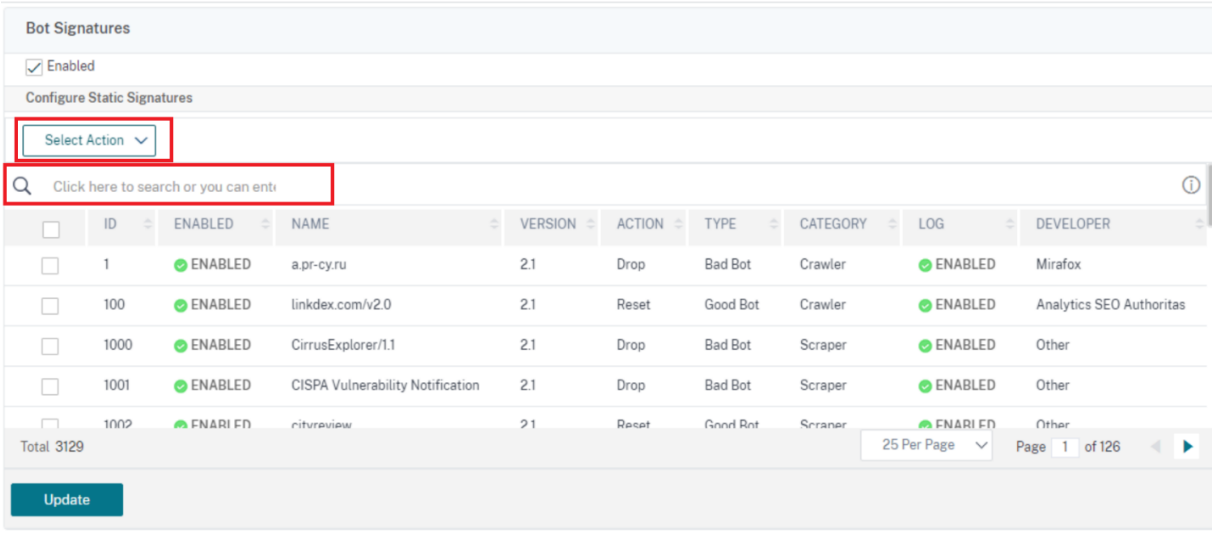
- Entfernen Sie Ausgewählte zurücksetzen. Heben Sie die Reset-Aktion auf alle ausgewählten Signaturregeln auf.
- Entfernen Sie Log Selected. Heben Sie die Protokollaktion auf alle ausgewählten Signaturregeln auf.

Kategorie. Wählen Sie eine Kategorie aus, um Signaturregeln entsprechend zu filtern. Im Folgenden finden Sie eine Liste der Kategorien, die zum Sortieren von Signaturregeln verfügbar sind.

- Aktion. Sortieren basierend auf Bot-Action.
- Kategorie. Sortieren Sie basierend auf der Bot-Kategorie.
- Entwickler. Sortieren basierend auf dem Herausgeber des Hostunternehmens.
- Aktiviert. Sortieren Sie basierend auf aktivierten Signaturregeln.
- Id. Sortieren Sie basierend auf der Signaturregel-ID.
- Log. Sortieren Sie basierend auf Signaturregeln, bei denen die Protokollierung aktiviert ist.
- Name. Sortieren basierend auf dem Namen der Signaturregel.
- Typ. Sortieren Sie basierend auf dem Signaturtyp.
- Version. Sortieren Sie basierend auf der Version der Signaturregeln.

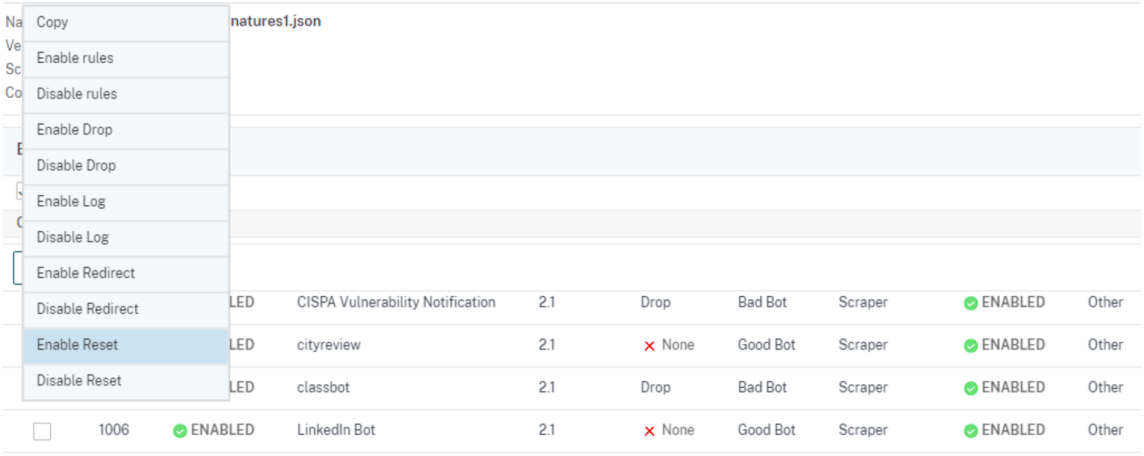
Suche nach Regeln für statische Unterschriften des Bot basierend auf Aktions- und Kategorietypen über die Citrix ADC-GUI

1. Navigieren Sie zu **Sicherheit > Citrix Bot Management > Signatur**.
2. Klicken Sie auf der Detailseite auf **Hinzufügen**.
3. Klicken Sie auf der Seite **Citrix Bot Management Signaturen** im Abschnitt **Statische Signaturen** auf Bearbeiten.
4. Wählen **Sie im Abschnitt Statische Signatur konfigurieren** eine Signaturaktion aus der Dropdownliste aus.
5. Verwenden Sie die Suchfunktion, um eine Kategorie auszuwählen und die Regeln entsprechend zu filtern.
6. Klicken Sie auf **Aktualisieren**.



Bearbeiten Sie die Eigenschaft der statischen Signaturregel des Bot mithilfe der Citrix ADC GUI

1. Navigieren Sie zu **Sicherheit > Citrix Bot Management > Signatur**.
2. Klicken Sie auf der Detailseite auf **Hinzufügen**.
3. Klicken Sie auf der Seite **Citrix Bot Management Signaturen** im Abschnitt **Statische Signaturen** auf Bearbeiten.
4. Wählen **Sie im Abschnitt Statische Signatur konfigurieren** eine Aktion aus der Dropdownliste aus.
5. Verwenden Sie die Suchfunktion, um eine Kategorie auszuwählen und Regeln entsprechend zu filtern.
6. Wählen Sie aus der Liste der statischen Signaturen eine Signatur aus, um ihre Eigenschaft zu ändern.



7. Klicken Sie zum Bestätigen auf **OK**.

Funktionsweise von CAPTCHA in der Citrix ADC Bot-Verwaltung

In der Citrix ADC-Bot-Verwaltung wird die CAPTCHA-Validierung als Richtlinienaktion konfiguriert, die ausgeführt wird, nachdem die Bot-Richtlinie ausgewertet wurde. Die CAPTCHA-Aktion ist nur für IP-Reputation und Techniken zur Erkennung von Geräte-Fingerabdrücken verfügbar. Im Folgenden sind die Schritte aufgeführt, um zu verstehen, wie CAPTCHA funktioniert:

1. Wenn während der IP-Reputation oder der Erkennung von Geräte-Fingerabdruck-Bots eine Sicherheitsverletzung festgestellt wird, sendet die ADC-Appliance eine CAPTCHA-Herausforderung.
2. Der Client sendet die CAPTCHA-Antwort.
3. Die Appliance validiert die CAPTCHA-Antwort und wenn das CAPTCHA gültig ist, ist die Anforderung zulässig und wird an den Back-End-Server weitergeleitet.
4. Wenn die CATCHA-Antwort ungültig ist, sendet die Appliance eine neue CAPTCHA-Herausforderung, bis die maximale Anzahl von Versuchen erreicht ist.
5. Wenn die CAPTCHA-Antwort auch nach der maximalen Anzahl von Versuchen ungültig ist, löscht die Appliance die Anforderung oder leitet sie an die konfigurierte Fehler-URL um.
6. Wenn Sie die Protokollaktion konfiguriert haben, speichert die Appliance die Anforderungsdetails in der Datei ns.log.

Konfigurieren Sie die CAPTCHA-Einstellungen über die Citrix ADC-GUI

Die CAPTCHA-Aktion für das Bot-Management wird nur für IP-Reputation und Techniken zur Erkennung von Geräte-Fingerabdrücken unterstützt. Führen Sie die folgenden Schritte aus, um die **CAPTCHA-Einstellungen** zu konfigurieren.

1. Navigieren Sie zu **Sicherheit > Citrix Bot Management and Profiles**.
2. Wählen Sie auf der Seite **Citrix Bot Management-Profile** ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Wechseln Sie auf der Seite **Citrix Bot-Verwaltungsprofil** zum Abschnitt **Signatureinstellungen** und klicken Sie auf **CAPTCHA**.
4. Klicken Sie im Abschnitt **CAPTCHA-Einstellungen** auf **Hinzufügen, um CAPTCHA-Einstellungen für das Profil zu konfigurieren** :
5. Legen **Sie auf der Seite Citrix Bot Management CAPTCHA konfigurieren** die folgenden Parameter fest.
    a) URL. Bot-URL, für die die CAPTCHA-Aktion während der IP-Reputation und der Erkennung von Geräte-Fingerabdrücken angewendet wird.

b) Aktiviert. Stellen Sie diese Option ein, um die CAPTCHA-Unterstützung zu aktivieren.

c) Gnade Zeit. Dauer bis zu dem keine neue CAPTCHA-Herausforderung gesendet wird, nachdem die aktuell gültige CAPTCHA-Antwort empfangen wurde.

d) Warte mal. Dauer, die die ADC Appliance braucht, um zu warten, bis der Client die CAPTCHA-Antwort sendet.

e) Stummschaltung. Dauer, für die der Client, der eine falsche CAPTCHA-Antwort gesendet hat, warten muss, bis er es als nächstes versuchen darf. Während dieser Stummschaltung lässt die ADC-Appliance keine Anfragen zu. Reichweite: 60-900 Sekunden, Empfohlen: 300 Sekunden

f) Längenbegrenzung anfordern. Länge der Anfrage, für die die CAPTCHA-Herausforderung an den Kunden gesendet wird. Wenn die Länge größer als der Schwellenwert ist, wird die Anforderung gelöscht. Der Standardwert beträgt 10—3000 Byte.

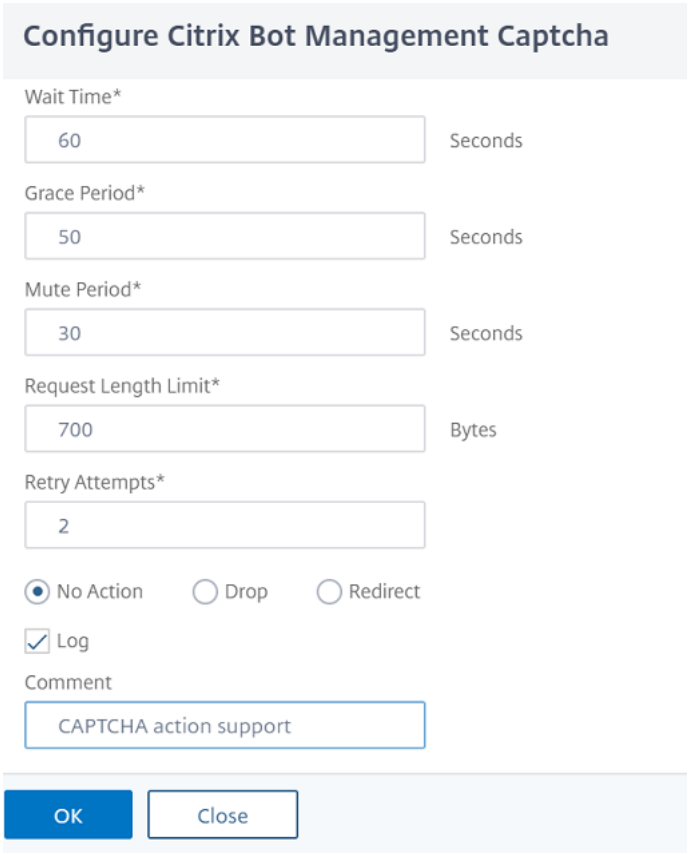
g) Versuche erneut versuchen. Anzahl der Versuche, die der Client erneut versuchen darf, die CAPTCHA-Herausforderung zu lösen. Reichweite: 1—10, Empfohlen: 5.

h) Es müssen keine Aktions-/Drop-/Umleitungsmaßnahmen ergriffen werden, wenn der Client die CAPTCHA-Validierung nicht besteht.

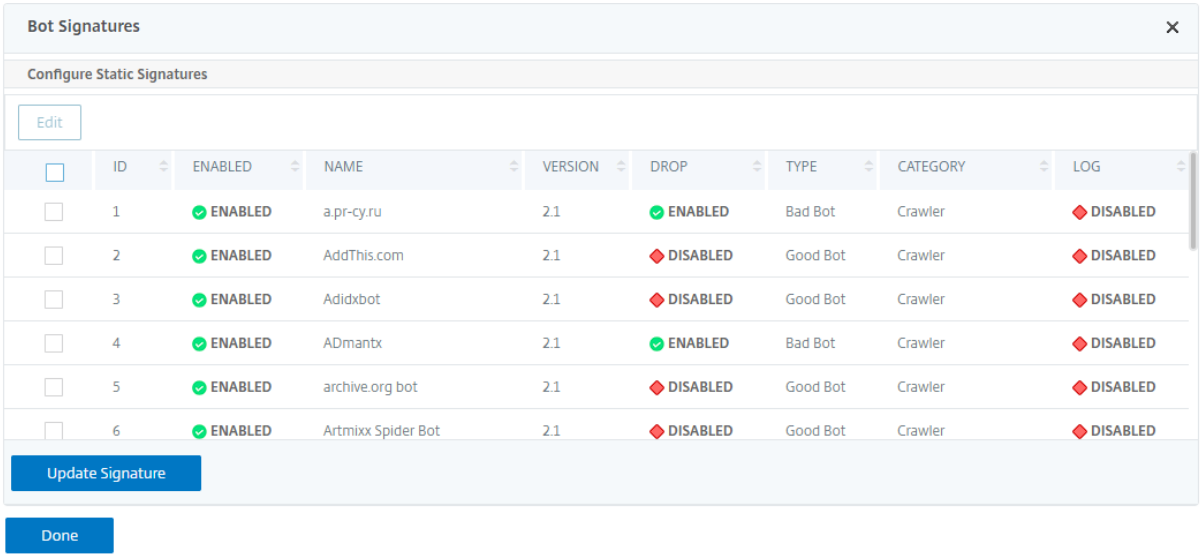
i) Log. Stellen Sie diese Option ein, um Anforderungsinformationen vom Client zu speichern, wenn die Antwort CAPTCHA fehlschlägt. Die Daten werden in einer Datei `ns.log` gespeichert.

j) Kommentar. Eine kurze Beschreibung der CAPTCHA-Konfiguration.

6. Klicken Sie auf **OK** und **Fertig**.



7. Navigieren Sie zu **Sicherheit > Citrix Bot Management > Signaturen**.
8. Wählen Sie auf der Seite **Citrix Bot Management-Signaturen** eine Signaturdatei aus, und klicken Sie auf **Bearbeiten**.
9. Wechseln Sie auf der Seite **Citrix Bot Management Signaturezum Abschnitt Signatureinstellungen**und klicken Sie auf**Bot-Signaturen**.
10. Stellen Sie im Abschnitt **Bot-Signaturen** die folgenden Parameter ein:
11. Konfigurieren Sie **statische Signaturen**. Wählen Sie einen statischen Bot-Signatureintrag aus und klicken Sie auf Bearbeiten, um ihm eine Bot-Aktion zuzuweisen.
12. Klicken Sie auf **OK**.
13. Klicken Sie auf **Signatur aktualisieren**.
14. Klicken Sie auf **Fertig**.



Automatisches Update für Bot-Signaturen

Die statische Bot-Signaturtechnik verwendet eine Signatur-Lookup-Tabelle mit einer Liste guter Bots und schlechter Bots. Die Bots werden basierend auf Benutzer-Agent-Zeichenfolgen und Domain-Namen kategorisiert. Wenn die Benutzer-Agent-Zeichenfolge und der Domänenname im eingehenden Bot-Verkehr mit einem Wert in der Nachschlagetabelle übereinstimmen, wird eine konfigurierte Bot-Aktion angewendet.
Die Bot-Signatur-Updates werden in der AWS-Cloud gehostet, und die Signatur-Lookup-Tabelle kommuniziert mit der AWS-Datenbank für Signaturaktualisierungen. Der Update-Scheduler für automatische Signaturen wird alle 1 Stunde ausgeführt, um die **AWS-Datenbank** zu überprüfen und die Signaturtabelle in der Citrix ADC-Appliance zu aktualisieren.

Die zu konfigurierende Signatur-Auto-Update-URL lautet: `https://nsbotsignatures.s3.amazonaws.com/BotSignatureMapping.json`

> **Hinweis:**
>
> Sie können auch einen Proxyserver konfigurieren und Signaturen regelmäßig von der AWS-Cloud über den Proxy auf die Appliance aktualisieren. Für die Proxy-Konfiguration müssen Sie die Proxy-IP-Adresse und die Portadresse in den Bot-Einstellungen festlegen.

Wie das automatische Update der Bot-Signatur funktioniert

Das folgende Diagramm zeigt, wie die Bot-Signaturen aus der AWS-Cloud abgerufen, auf Citrix ADC aktualisiert und auf Citrix ADM für eine Zusammenfassung der Signaturaktualisierung angezeigt werden.

Der Bot-Signatur-Auto-Update-Scheduler tut Folgendes:

1. Ruft die Zuordnungsdatei von der AWS-URI ab.
2. Überprüft die neuesten Signaturen in der Mapping-Datei mit den vorhandenen Signaturen in der ADC-Appliance.
3. Lädt die neuen Signaturen von AWS herunter und überprüft die Signaturintegrität.
4. Aktualisiert die vorhandenen Bot-Signaturen mit den neuen Signaturen in der Bot-Signaturdatei.
5. Generiert eine SNMP-Warnung und sendet die Signaturaktualisierungszusammenfassung an Citrix ADM.

Konfigurieren Sie das automatische Update der Bot

Führen Sie die folgenden Schritte aus, um das automatische Update der Bot-Signatur zu konfigurieren:

Automatisches Update der Bot-Signatur aktivieren

Sie müssen die Option für die automatische Aktualisierung in den Bot-Einstellungen der ADC-Appliance aktivieren.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set bot settings -signatureAutoUpdate ON
```

Konfigurieren von Proxyservereinstellungen (optional)

Wenn Sie über einen Proxyserver auf die AWS-Signaturdatenbank zugreifen, müssen Sie den Proxyserver und den Port konfigurieren.

```
set bot settings -proxyserver -proxyport
```

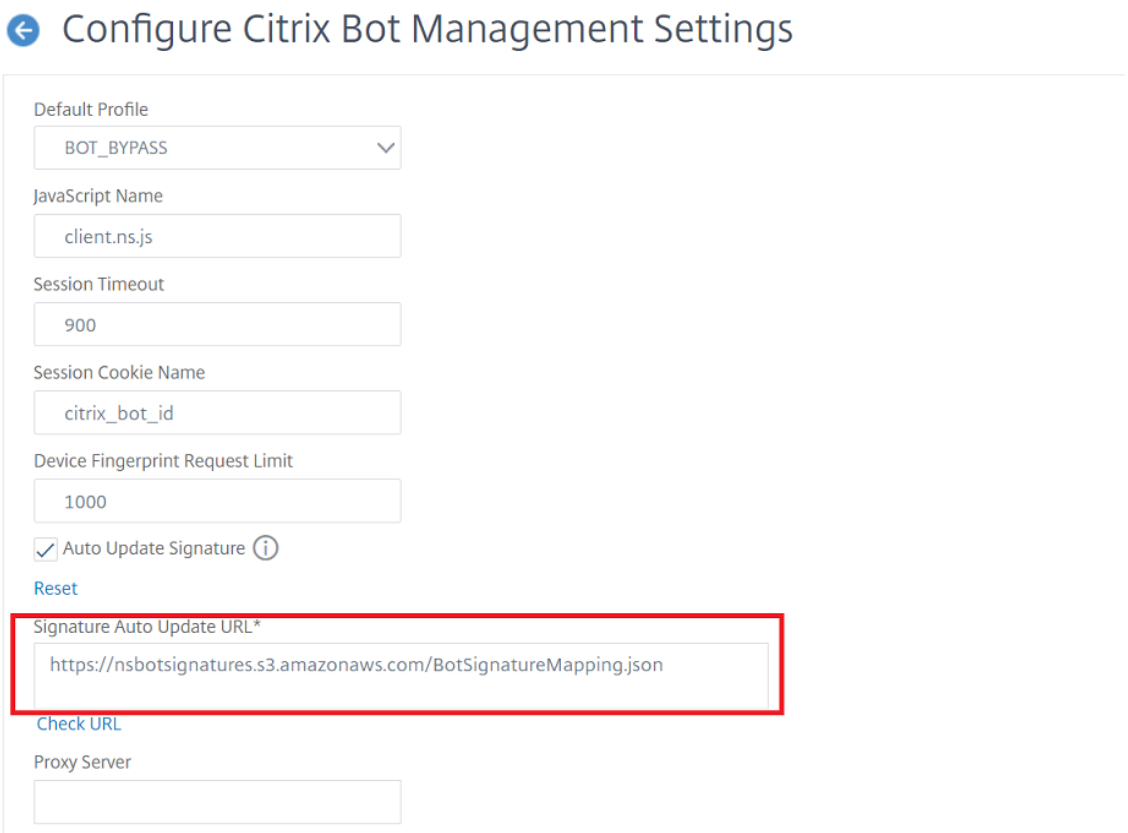
Beispiel:

```
set bot settings -proxy server 1.1.1.1 -proxyport 1356
```


Konfigurieren Sie das automatische Update der Bot-Signatur über die Citrix ADC-GUI

Führen Sie die folgenden Schritte aus, um das automatische Update für die Bot-Signatur

1. Navigieren Sie zu **Sicherheit > Citrix Bot Management**.
2. Klicken Sie im Detailbereich unter **Einstellungen** auf **Citrix Bot Management-Einstellungen ändern**.
3. Aktivieren Sie in den **Citrix Bot-Verwaltungseinstellungen konfigurieren**das Kontrollkästchen **Signatur automatisch aktualisieren** .



4. Klicken Sie auf **OK** und **Schließen**.

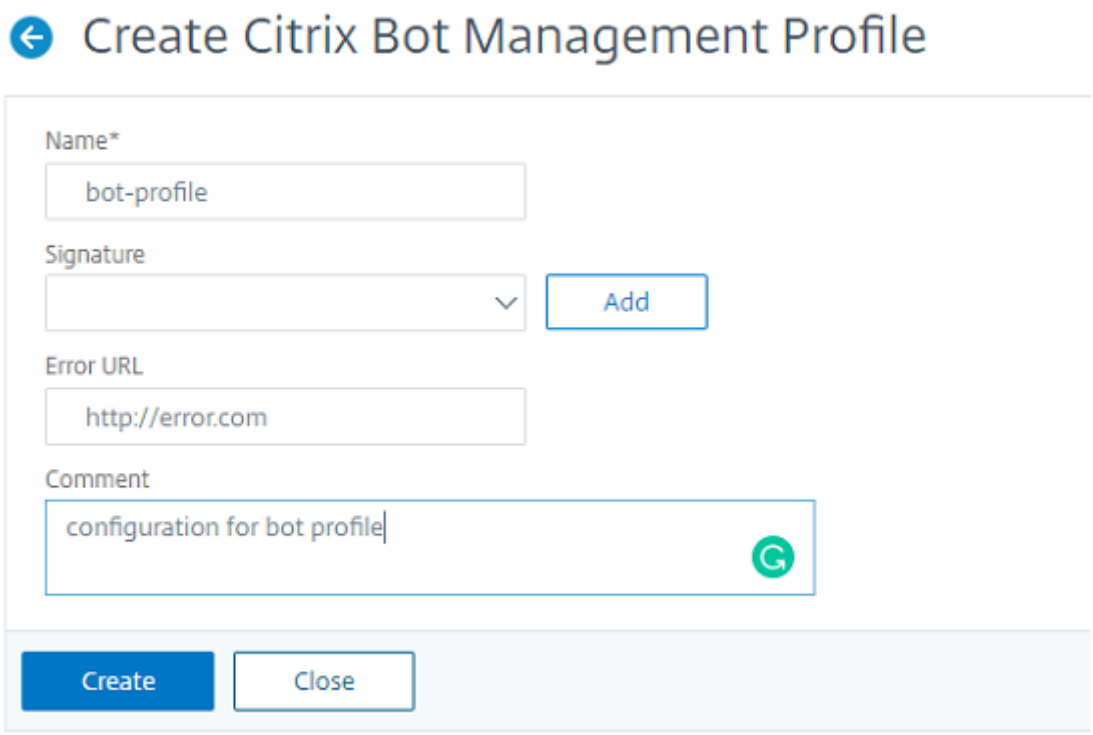
Erstellen Sie Bot-Management-Profil

Ein Bot-Profil ist eine Sammlung von Bot-Management-Einstellungen, die zur Erkennung des Bot-Typs verwendet werden. In einem Profil legen Sie fest, wie die Web App Firewall jeden ihrer Filter (oder Schecks) auf den Bot-Traffic auf Ihre Sites und Antworten von diesen anwendet.

Führen Sie die folgenden Schritte aus, um das Bot-Profil zu konfigurieren:

1. Navigieren Sie zu **Sicherheit** > **Citrix Bot Management** > **Profiles**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.

3. Legen **Sie auf der Seite Citrix Bot-Verwaltungsprofil erstellen** die folgenden Parameter fest.
   a) Name. Name des Bot-Profils.
   b) Unterschrift. Name der Bot-Signaturdatei.
   c) Fehler-URL. URL für Weiterleitungen.
   d) Kommentar. Kurzbeschreibung des Profils.
4. Klicken Sie auf **Erstellen** und **Schließen**.



Erstellen Sie Bot-Richtlinie

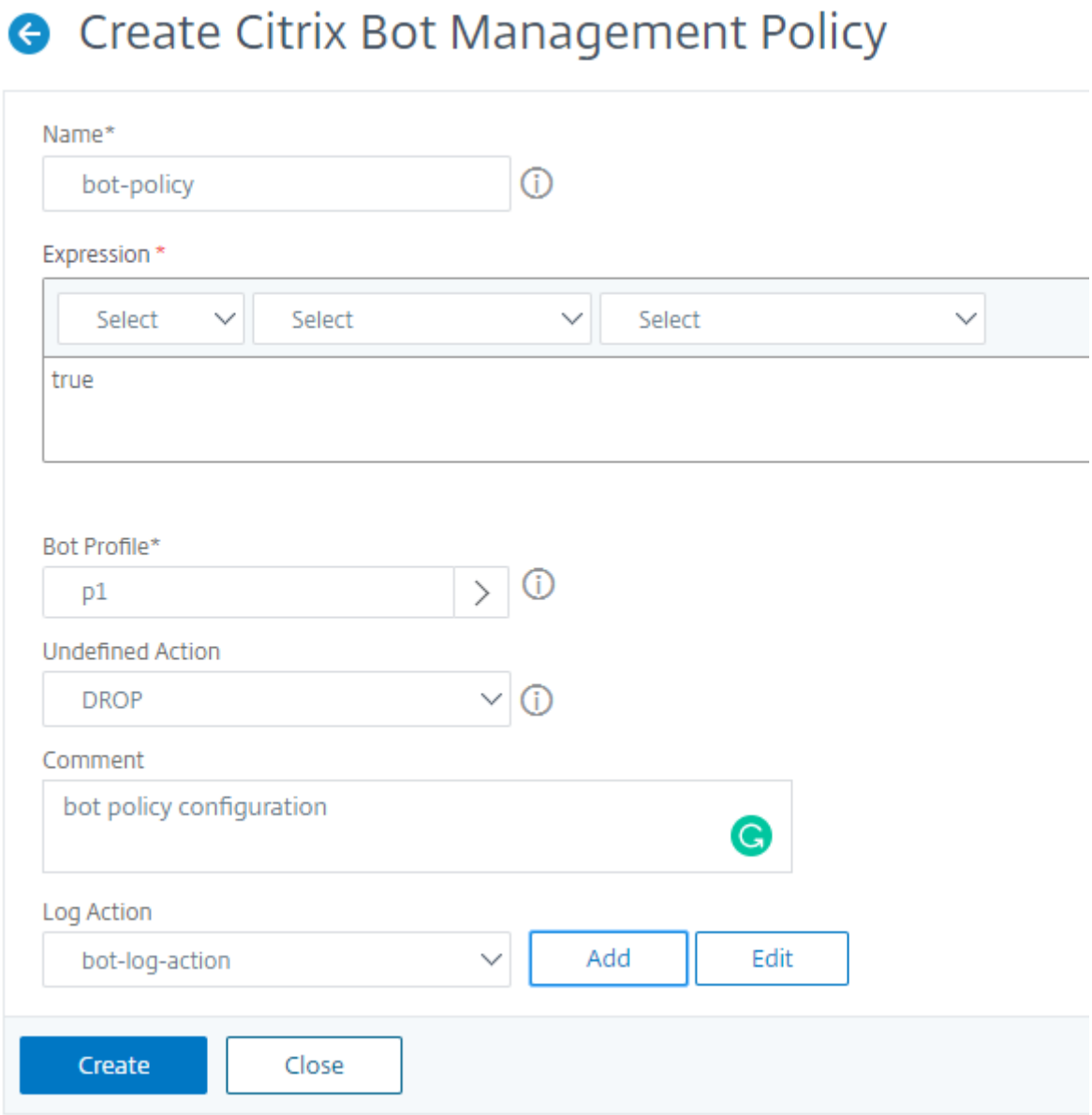
Die Bot-Richtlinie steuert den Datenverkehr, der zum Bot-Verwaltungssystem fließt, und steuert auch die Bot-Protokolle, die an den Auditlog-Server gesendet werden. Folgen Sie dem Verfahren, um die Bot-Richtlinie zu konfigurieren.

1. Navigieren Sie zu **Sicherheit** > **Citrix Bot Management** > **Bot-Richtlinien**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen **Sie auf der Seite Citrix Bot-Verwaltungsrichtlinie erstellen** die folgenden Parameter fest.
   a) Name. Name der Bot-Richtlinie.
   b) Ausdruck. Geben Sie den Richtlinienausdruck oder die Regel direkt in den Textbereich ein.
   c) Bot-Profil. Bot-Profil zur Anwendung der Bot-Richtlinie.
   d) Undefinierte Aktion. Wählen Sie eine Aktion aus, die Sie lieber zuweisen möchten.

e) Kommentar. Kurze Beschreibung der Richtlinie.

f) Aktion protokollieren. Aktion der Überwachungsprotokollnachricht zum Protokollieren des Bot-Traffics. Weitere Informationen zur Aktion des Überwachungsprotokolls finden Sie unter Thema Audit-Protokollierung.

4. Klicken Sie auf **Erstellen** und **Schließen**.



Bot-Transaktionen pro Sekunde (TPS)

Die Bot-Technik “Transaktionen pro Sekunde” (TPS) erkennt eingehenden Traffic als Bot, wenn die Anzahl der Anfragen pro Sekunde (RPS) und der prozentuale Anstieg des RPS den konfigurierten Schwellenwert überschreiten. Die Erkennungstechnik schützt Ihre Webanwendungen vor automatisierten Bots, die Web-Scraping-Aktivitäten, Brute-Forcing-Login und andere böswillige Angriffe

verursachen können.

> **Hinweis:**
>
> Die Bot-Technik erkennt einen eingehenden Traffic nur als Bot, wenn beide Parameter konfiguriert sind und wenn beide Werte über das Schwellenwertlimit hinaus steigen.
> Betrachten wir ein Szenario, in dem die Appliance viele Anfragen von einer bestimmten URL erhält und Sie möchten, dass das Citrix ADC-Bot-Management erkennt, ob es einen Bot-Angriff gibt. Die TPS-Erkennungstechnik untersucht die Anzahl der Anfragen (konfigurierter Wert), die innerhalb von 1 Sekunde von der URL kommen, und den prozentualen Anstieg (konfigurierter Wert) der Anzahl der Anfragen, die innerhalb von 30 Minuten empfangen wurden. Wenn die Werte das Schwellenwertlimit überschreiten, wird der Verkehr als Bot betrachtet und die Appliance führt die konfigurierte Aktion aus.

Konfigurieren von Bot-Transaktionen pro Sekunde (TPS) -Technik

Um TPS zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Aktivieren Sie Bot TPS
2. Binden Sie TPS-Einstellungen an das Bot-Verwaltungsprofil

Binden Sie TPS-Einstellungen an das Bot-Verwaltungsprofil

Sobald Sie die Bot-TPS-Funktion aktiviert haben, müssen Sie die TPS-Einstellungen an das Bot-Verwaltungsprofil binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind bot profile <name>… (-tps [-type ( SourceIP | GeoLocation | RequestURL
 | Host )] [-threshold <positive_integer>] [-percentage <positive_integer
>] [-action ( none | log | drop | redirect | reset | mitigation )] [-
logMessage <string>])
```

Beispiel:

```
bind bot profile profile1 -tps -type RequestURL -threshold 1 -percentage
100000 -action drop -logMessage log
```

Aktivieren Sie die Bot-Transaktion pro Sekunde (TPS)

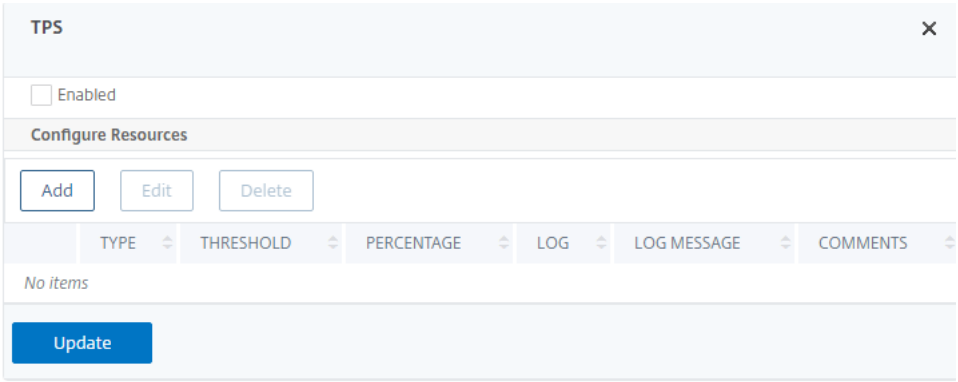
Bevor Sie beginnen können, müssen Sie sicherstellen, dass die Bot TPS-Funktion auf der Appliance aktiviert ist. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set bot profile profile1 -enableTPS ON
```


Konfigurieren Sie Bot-Transaktionen pro Sekunde (TPS) über die Citrix ADC-GUI

Führen Sie die folgenden Schritte aus, um Bot-Transaktionen pro Sekunde zu konfigurieren:

1. Navigieren Sie zu **Sicherheit > Citrix Bot Management > Profiles**.
2. Wählen Sie auf der Seite **Citrix Bot Management-Profile** ein Profil aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Citrix Bot-Verwaltungsprofil erstellenim Abschnitt **Signatureinstellungen** auf TPS** .
4. Aktivieren Sie im Abschnitt **TPS** die Funktion und klicken Sie auf **Hinzufügen**.



5. Legen Sie auf der Seite **TPS-Bindung des Citrix Bot-Verwaltungsprofils konfigurieren** die folgenden Parameter fest.

   a) Typ. Durch die Erkennungstechnik erlaubte Eingabetypen. Mögliche Werte: SOURCE IP, GEOLOCATION, HOST, URL.

   SOURCE_IP — TPS basierend auf der IP-Adresse des Clients.

   GEOLOCATION — TPS basierend auf dem geografischen Standort des Kunden.

   HOST - TPS basierend auf Clientanforderungen, die an eine bestimmte Back-End-Server-IP-Adresse weitergeleitet werden.

   URL — TPS basierend auf Clientanforderungen, die von einer bestimmten URL stammen.

   b) Fester Schwellenwert. Maximale Anzahl von Anfragen, die von einem TPS-Eingabetyp innerhalb eines Zeitintervalls von 1 Sekunde zulässig sind.

   c) Prozentualer Schwellenwert. Maximaler prozentualer Anstieg der Anfragen von einem TPS-Eingabetyp innerhalb eines 30-Minuten-Zeitintervalls

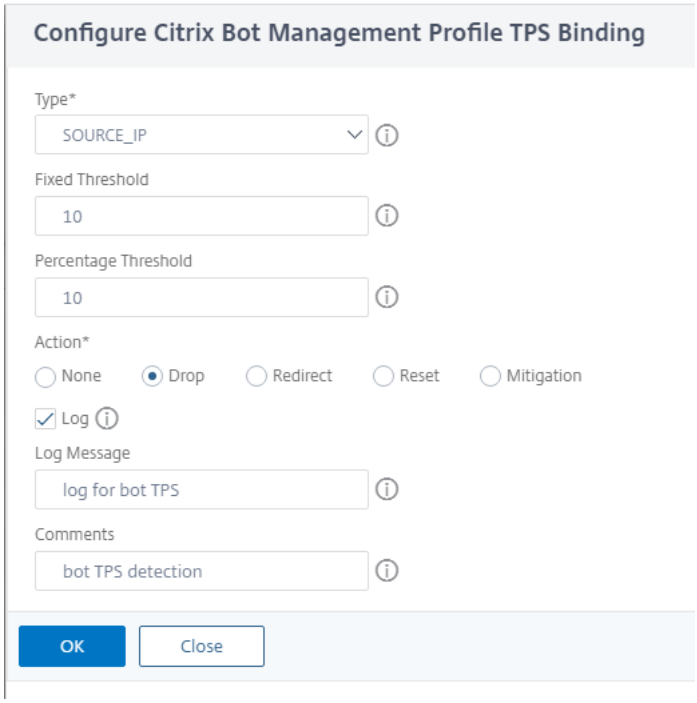
   d) Aktion. Zu ergreifende Maßnahmen für Bot, der durch TPS-Bindung erkannt wird.

   e) Log. Aktivieren oder deaktivieren Sie die Protokollierung für TPS-Bindung.

   f) Meldung protokollieren. Meldung zum Log für Bot, die durch TPS-Bindung erkannt wurde. Maximale Länge: 255

g) Kommentare. Eine kurze Beschreibung der TPS-Konfiguration. Maximale Länge: 255

6. Klicken Sie auf **OK** und dann auf **Schließen**.



Bot-Erkennung basierend auf Maus- und Tastaturdynamik

Um Bots zu erkennen und Anomalien des Web-Scrapings zu mildern, verwendet das Citrix ADC Bot Management eine erweiterte Bot-Erkennungstechnik, die auf dem Verhalten von Maus und Tastatur basiert. Im Gegensatz zu herkömmlichen Bot-Techniken, die eine direkte menschliche Interaktion erfordern (z. B. die CAPTCHA-Validierung), überwacht die erweiterte Technik passiv die Maus und die Tastaturdynamik. Die Citrix ADC-Appliance sammelt dann die Benutzerdaten in Echtzeit und analysiert das Verhalten zwischen einem Menschen und einem Bot.

Die passive Bot-Erkennung mit Maus- und Tastaturdynamik hat gegenüber bestehenden Bot-Erkennungsmechanismen folgende Vorteile:

- Bietet eine kontinuierliche Überwachung während der gesamten Benutzersitzung und eliminiert einen einzelnen Checkpoint.
- Erfordert keine menschliche Interaktion und ist für Benutzer völlig transparent.

So funktioniert die Bot-Erkennung mit Maus- und Tastaturdynamik

Die Bot-Erkennungstechnik mit Tastatur- und Mausdynamik besteht aus zwei Komponenten, einem Webseitenlogger und einem Bot-Detektor. Der Webseitenlogger ist ein JavaScript, das Tastatur- und Mausbewegungen aufzeichnet, wenn ein Benutzer eine Aufgabe auf der Webseite ausführt (z. B.

ein Registrierungsformular ausfüllt). Der Logger sendet die Daten dann stapelweise an die Citrix ADC-Appliance. Die Appliance speichert die Daten dann als KM-Datensatz und sendet sie an den Bot-Detektor auf dem Citrix ADM-Server, der analysiert, ob der Benutzer ein Mensch oder Bot ist.

Die folgenden Schritte erklären, wie die Komponenten miteinander interagieren:

1. Der Citrix ADC-Administrator konfiguriert den Richtlinienausdruck über das ADM StyleBook, CLI oder NITRO oder eine andere Methode.
2. Die URL wird im Bot-Profil festgelegt, wenn der Administrator die Funktion auf der Appliance aktiviert.
3. Wenn ein Client eine Anforderung sendet, verfolgt die Citrix ADC-Appliance die Sitzung und alle Anforderungen in der Sitzung.
4. Die Appliance fügt ein JavaScript (Webseitenlogger) in die Antwort ein, wenn die Anforderung mit dem konfigurierten Ausdruck im Bot-Profil übereinstimmt.
5. Das JavaScript sammelt dann die gesamte Tastatur- und Mausaktivität und sendet die KM-Daten in einer POST-URL (transient).
6. Die Citrix ADC-Appliance speichert die Daten und sendet sie am Ende der Sitzung an den Citrix ADM-Server. Sobald die Appliance die vollständigen Daten einer POST-Anforderung erhalten hat, werden die Daten an den ADM-Server gesendet.
7. Der Citrix ADM-Dienst analysiert die Daten und basierend auf der Analyse ist das Ergebnis auf der GUI des Citrix ADM Service ADM-Dienstes verfügbar.

Der JavaScript-Logger zeichnet die folgenden Maus- und Tastaturbewegungen auf:

- Tastaturereignisse — alle Ereignisse
- Mausereignisse - Maus bewegen, Maus hoch, Maus runter
- Ereignisse in der Zwischenablage - einfügen
- Benutzerdefinierte Ereignisse - autofill, autofillcancel
- Zeitstempel jedes Ereignisses

Konfigurieren der Bot-Erkennung mit Maus- und Tastatur

Die Citrix ADC Bot-Management-Konfiguration umfasst das Aktivieren oder Deaktivieren der Tastatur- und mausbasierter Erkennungsfunktion und konfiguriert die JavaScript-URL im Bot-Profil.
Führen Sie die folgenden Schritte aus, um die Bot-Erkennung mit Maus- und Tastaturdynamik zu konfigurieren

1. Tastatur- und mausbasierte Erkennung aktivieren
2. Konfigurieren Sie den Ausdruck, um zu entscheiden, wann das JavaScript in die HTTP-Antwort eingefügt werden kann.

Tastaturmausbasierte Bot-Erkennung aktivieren

Bevor Sie mit der Konfiguration beginnen, stellen Sie sicher, dass Sie die Tastatur- und mausbasierte Bot-Erkennungsfunktion auf der Appliance aktiviert haben.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add bot profile <name> -KMDetection ( ON | OFF )
2 <!--NeedCopy-->
```

Beispiel:

```
add bot profile profile1 -KMDetection ON
```

Bot-Ausdruck für das Einfügen von JavaScript konfigurieren

Konfigurieren Sie Bot-Ausdruck, um den Datenverkehr auszuwerten und JavaScript einzufügen. Das JavaScript wird nur eingefügt, wenn der Ausdruck als wahr ausgewertet wird.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind bot profile <name> -KMDetectionExpr -name <string> -expression <
     expression> -enabled ( ON | OFF ) - comment <string>
2 <!--NeedCopy-->
```

Beispiel:

```
bind bot profile profile1 -KMDetectionExpr -name test -expression http.req.
url.startswith(”/testsite”)-enabled ON
```

Konfigurieren Sie den in der HTTP-Antwort eingefügten JavaScript-Dateinamen für die tastatur-mausbasierte

Um die Benutzeraktionsdetails zu erfassen, sendet die Appliance einen JavaScript-Dateinamen in der HTTP-Antwort. Die JavaScript-Datei sammelt alle Daten in einem KM-Datensatz und sendet sie an die Appliance.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set bot profile profile1 - KMJavaScriptName <string>
2 <!--NeedCopy-->
```

Beispiel:

```
set bot profile profile1 -KMJavaScriptName script1
```


Verhaltensgröße der Biometrie konfigurieren

Sie können die maximale Größe von Maus- und Tastaturverhaltensdaten konfigurieren, die als KM-Datensatz an die Appliance gesendet und vom ADM-Server verarbeitet werden können.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set bot profile profile1 -KMEventsPostBodyLimit <positive_integer>
2 <!--NeedCopy-->
```

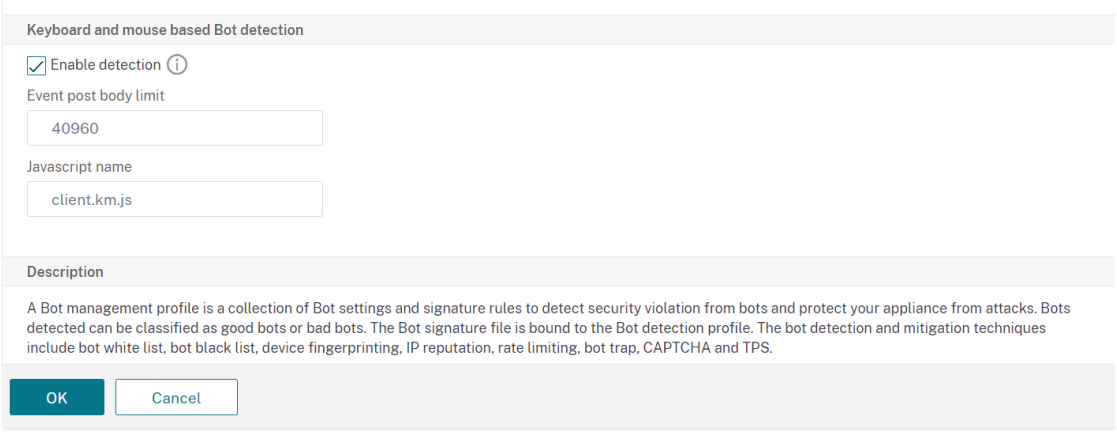
Beispiel:

```
set bot profile profile1 - KMEventsPostBodyLimit 25
```

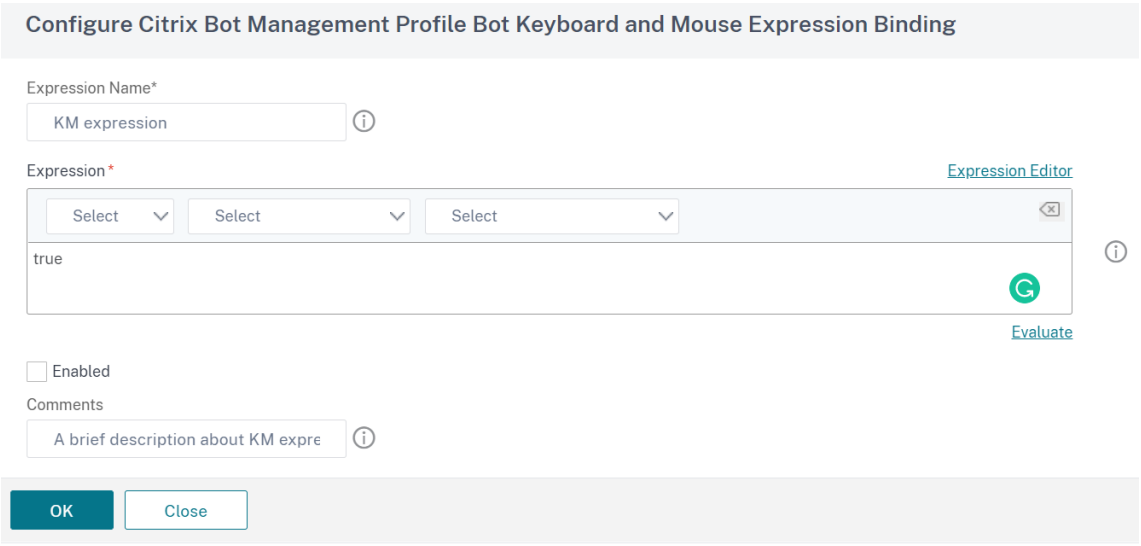
Nachdem Sie die Citrix ADC-Appliance so konfiguriert haben, dass JavaScript konfiguriert und Biometrie für das Verhalten von Tastatur und Maus erfasst werden, sendet die Appliance die Daten an den Citrix ADM-Server. Weitere Informationen darüber, wie der Citrix ADM-Server Bots aus der Verhaltensbiometrie erkennt, finden Sie unter Bot-Verstöße.

Konfigurieren von Tastatur- und Maus-Bot-Ausdruckseinstellungen über die GUI

1. Navigieren Sie zu **Sicherheit > Citrix Bot Management and Profiles**.
2. Wählen Sie auf der Seite **Citrix Bot Management-Profile** ein Profil aus, und klicken Sie auf **Bearbeiten**.
3. Stellen Sie im Abschnitt **Tastatur- und mausbasierte Bot-Erkennung** die folgenden Parameter ein:
   a) Aktivieren Sie die Erkennung. Aktivieren Sie das Kontrollkästchen, um das Bot-basierte Verhalten der Tastatur- und Mausdynamik zu erkennen.
   b) Grenzwert für das Ereignis nach dem Hauptteil Größe der Tastatur- und Mausdynamikdaten, die vom Browser gesendet werden, um von der Citrix ADC-Appliance verarbeitet zu werden.
4. Klicken Sie auf **OK**.



5. Gehen Sie auf der Seite **Citrix Bot Management Profile** zum Abschnitt **Profileinstellungen** und klicken Sie auf **Tastatur- und mausbasierte Bot-Ausdruckseinstellungen**.
6. Klicken Sie im Abschnitt **Einstellungen für Tastatur und Maus auf Bot Expression** Settings auf **Hinzufügen**.
7. Legen Sie auf der Seite **Configure Citrix Bot Management Profile Bot Keyboard and Mouse Expression Binding** die folgenden Parameter fest:
   a) Name des Ausdrucks. Name des Bot-Richtlinienausdrucks zur Erkennung von Tastatur- und Mausdynamik.
   b) Ausdruck. Ausdruck der Bot-Richtlinie.
   c) Aktiviert. Aktivieren Sie das Kontrollkästchen, um die Tastatur- und Bot-Tastatur- und Mausdruck-Bindung zu aktivieren.
   d) Kommentare. Eine kurze Beschreibung des Bot-Richtlinienausdrucks und seiner Bindung an das Bot-Profil.
   e) Klicken Sie auf **OK** und **Schließen**.
8. Klicken Sie im Abschnitt **Einstellungen für Tastatur- und mausbasierte Bot-Ausdrücke** auf **Aktualisieren**.



Vom Citrix Bot Management gelöschte Header anfordern

Viele der Anforderungsheader im Zusammenhang mit dem Caching werden gelöscht, um jede Anforderung im Kontext einer Sitzung anzuzeigen. Wenn die Anforderung einen Codierungs-Header enthält, der es dem Webserver ermöglicht, komprimierte Antworten zu senden, löscht das Bot-Management diesen Header, sodass der Inhalt der unkomprimierten Serverantwort von der Bot-Verwaltung überprüft wird, um die JavaScripts einzufügen.

Die Bot-Verwaltung löscht die folgenden Request-Header:

Reichweite. Wird zur Wiederherstellung nach einer fehlgeschlagenen oder teilweisen Dateiübertragung verwendet.

Wenn-Bereich. Ermöglicht einem Client, ein Teilobjekt abzurufen, wenn es bereits einen Teil dieses Objekts in seinem Cache enthält (bedingtes GET).

Wenn-Modifiziert-seit. Wenn das angeforderte Objekt seit der in diesem Feld angegebenen Zeit nicht geändert wurde, wird keine Entität vom Server zurückgegeben. Sie erhalten einen nicht modifizierten HTTP-304-Fehler.

Wenn-keines Spiel. Ermöglicht effiziente Aktualisierungen von zwischengespeicherten Informationen mit minimalem Overhead.

Kodierung akzeptieren. Welche Kodierungsmethoden sind für ein bestimmtes Objekt zulässig, z. B. gzip.

Bot Management

October 5, 2021

Im Folgenden finden Sie einige der Problembehandlungsszenarien, die in der Citrix ADC Bot-Verwaltung behandelt werden.

1. Wie behandelt man falsch positive Fälle?

   Sie können die Bot-Zulassungslistenfunktionalität verwenden, um falsch positive Fälle zu verwalten, und diese Transaktionen können umgangen werden.

2. Wie finde ich weitere Details über schlechten Bot Traffic?

   Sie können die Audit-Protokollierungsfunktion verwenden, um Details zum Datenverkehr zu erhalten, der als schlechte Bots klassifiziert ist

3. Warum sollten Sie den Standardsignaturnamen ändern?

   Sie können den Standardsignaturnamen ändern, wenn Konflikte an den Endpunkt-Ressourcen festgestellt werden, die von der Citrix ADC Appliance bereitgestellt werden.

Bot Management

October 5, 2021

1. Was ist Citrix ADC Bot-Management?

   Citrix ADC Bot-Management erkennt und unterscheidet Traffic von guten Bots, schlechten Bots und menschlichen Clients. Die Bot-Management-Funktionalität schützt Ihre Webanwendungen, indem Verbindungen von schlechten Bots entfernt werden.

2. Warum muss Citrix ADC Bots für Ihre Webanwendung verwalten?

   Bösartige Bots machen 30% Ihres Internetverkehrs aus. Schädliche Bots wirken sich auf verschiedene Arten auf Webanwendungen aus, z. B. das Einleiten eines DoS-Angriffs, das Spammen von E-Mail-Adressen, die Verlangsamung von Anwendungen mit Downloader-Programmen, das Herunterladen der Inhalte von Websites usw. Darüber hinaus können Bots einige der bekannten Erkennungsmechanismen leicht umgehen, die zu Verlust von Daten, Einnahmen und Reputation für Ihr Unternehmen führen.

3. Welche Techniken werden verwendet, um einen eingehenden Bot zu erkennen?

   Die Appliance verwendet Erkennungstechniken wie IP-Reputation, Ratenbegrenzung und Techniken zur Erkennung von Geräte-Fingerprinting-Techniken. Darüber hinaus können Sie eine angepasste Sperrliste auf der Citrix ADC GUI konfigurieren, um organisationsspezifische Bad Bots zu kategorisieren.

4. Was ist eine Bot-Signaturdatei und ihr Zweck?

Die Bot-Signaturdatei enthält den Footprint bekannter guter und schlechter Bots. Die Signaturdatei kann regelmäßig aktualisiert werden, um die neuesten Botsignaturen für einen besseren Bot-Schutz zu enthalten.

5. Welche Art von Citrix ADC -Lizenz muss ich kaufen?

   Die Bot-Verwaltung ist mit der ADC Premium-Lizenz verfügbar.

6. Wo finde ich Bot-Protokolle zur Fehlerbehebung?

   Citrix ADC Überwachungsprotokolle bieten erkannte Bot-Details. Weitere Informationen finden Sie unter Thema Überwachungsprotokollierung .

7. Gibt es eine automatische Update-Funktion für die Bot-Signaturdateien?

   Derzeit unterstützt Citrix ADC keine automatische Update-Funktionalität.

8. Gibt es eine Voraussetzung für die Verwendung der Bot-IP-Reputationstechnik?

   Aktivieren Sie die IP-Reputation-Funktion, bevor Sie die IP-Reputation im Bot-Profil aktivieren und konfigurieren.

Bot Signatur Auto Update

April 7, 2022

Mit der automatischen Aktualisierungsfunktion für Bot-Signaturen erhalten Sie die neuesten Signaturen, die einen besseren Schutz und ein besseres Verkehrsmanagement vor guten und schlechten Bots bieten.

Die Signaturen werden stündlich automatisch aktualisiert, sodass nicht ständig nach der Verfügbarkeit des neuesten Updates gesucht werden muss. Wenn Sie die automatische Signaturaktualisierung aktiviert haben, stellt die Citrix ADC Appliance eine Verbindung zu dem Server her, auf dem die Signaturen gehostet werden, um zu überprüfen, ob eine neuere Version verfügbar ist.

Die neuesten in der Amazon-Cloud gehosteten Bot-Signaturen sind als Standard-Signatur-URL konfiguriert, um nach dem neuesten Update zu suchen. Damit die automatische Aktualisierungsfunktion funktioniert, müssen Sie auch den DNS-Server für den Zugriff auf die externe Site konfigurieren.

Signaturen aktualisieren

Alle benutzerdefinierten Signaturobjekte, die mit dem Standard-Signaturobjekt des Bot erstellt wurden, haben eine Version größer als Null. Wenn Sie die automatische Signaturaktualisierung aktivieren, werden alle Signaturen automatisch aktualisiert. Sie können die Standardaktion für

Bot-Signaturen aktualisieren, indem Sie entweder eine Signatur oder eine Gruppe von Signaturen mithilfe der Suchfunktion in der Citrix ADC Bot-Management-GUI auswählen.

URL zur Aktualisierung der Bot-Signatur `https://nsbotsignatures.s3.amazonaws.com/BotSignatureMapping.json`

Konfigurieren des automatischen Updates der Signatur

Um die automatische Signaturaktualisierung zu aktivieren, müssen Sie den folgenden Befehl ausführen:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set bot settings SignatureAutoUpdate ON
<!--NeedCopy-->
```

Artikel zur Bot-Signaturwar

October 5, 2021

Citrix Bot Management kündigt Signatur-Updates an, die Sie herunterladen und auf Ihre Appliance anwenden können. Wenn Sie einen Bot-Angriff feststellen, erhalten Sie eine E-Mail-Benachrichtigung über das neue Signatur-Update. Sie können die Signatur herunterladen und auf Ihre Appliance anwenden.

Aktualisierung der Botunterschrift für November 2020

October 5, 2021

Für die in der Woche 2020-11-11 identifizierten Bots werden neue Signaturregeln generiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Bot-Angriffen zu schützen.

Version der Bots

Signaturversion 5 gilt für Citrix ADC 13.0 Plattform.

Neue Bots Insight

Es folgt eine Liste der Bot-Signaturregeln, der Kategorie und ihres Typs.

Kategorie	Bot-Typ	Anzahl der Unterschriften
Scraper	Guter Bot	3
Marketing	Guter Bot	23
Feed Fetcher	Guter Bot	2
Tool	Schlechter Bot	3
Suchmaschine	Guter Bot	34
Crawler	Guter Bot	6
Nicht kategorisiert	Schlechter Bot	6
Viren-Scanner	Guter Bot	1
Screenshot Creator	Guter Bot	7
Scraper	Schlechter Bot	1
Tool	Guter Bot	7

Bot signature update for January 2021

December 7, 2021

Some of existing bot signatures are updated. You can download and configure these signature rules to protect your appliance from bot attacks.

Bot signature version

Signature version 6 is applicable for Citrix ADC platforms with 13.0 61.x builds or later.

Updated bot signatures in this version

Following is a list of bot signature rule IDs, category and its type.

Bot signature rule	ID	Description
143	Crawler	Good Bot

Bot signature rule	ID	Description
561	Scraper	Good Bot
857	Site Monitor	Good Bot
892	Site Monitor	Bad Bot
894	Site Monitor	Bad Bot
980	Scraper	Bad Bot
1025	Site Monitor	Bad Bot
1029	Feed Fetcher	Bad Bot
1030	Screenshot Creator	Bad Bot
1034	Tool	Bad Bot
1039	Marketing	Bad Bot
1042	Site Monitor	Bad Bot
1047	Site Monitor	Bad Bot
1053	Site Monitor	Bad Bot
1072	Search Engine	Bad Bot
1073	Feed Fetcher	Bad Bot
1074	Uncategorized	Bad Bot
1078	Screenshot Creator	Bad Bot
1109	Marketing	Bad Bot
1132	Feed Fetcher	Bad Bot
1138	Marketing	Bad Bot
1150	Search Engine	Bad Bot
1164	Search Engine	Bad Bot
1167	Marketing	Bad Bot
1173	Tool	Bad Bot
1174	Marketing	Bad Bot
1176	Search Engine	Bad Bot
1178	Speed Tester	Bad Bot
1185	Screenshot Creator	Bad Bot
1209	Uncategorized	Bad Bot

Bot signature rule	ID	Description
1244	Site Monitor	Bad Bot
1251	Search Engine	Bad Bot
1254	Site Monitor	Bad Bot
1256	Uncategorized	Bad Bot
1259	Tool	Bad Bot
1287	Search Engine	Bad Bot
1296	Search Engine	Bad Bot
1312	Uncategorized	Bad Bot
1316	Marketing	Bad Bot
1322	Site Monitor	Bad Bot
1325	Screenshot Creator	Bad Bot
1328	Search Engine	Bad Bot
1330	Marketing	Bad Bot
1337	Tool	Bad Bot
1360	Search Engine	Bad Bot
1367	Search Engine	Bad Bot
1374	Tool	Bad Bot
1380	Uncategorized	Bad Bot
1388	Search Engine	Bad Bot
1400	Feed Fetcher	Bad Bot
1413	Uncategorized	Bad Bot
1420	Feed Fetcher	Bad Bot
1422	Site Monitor	Bad Bot
1442	Uncategorized	Bad Bot
1447	Search Engine	Bad Bot
1460	Marketing	Bad Bot
1467	Tool	Bad Bot
1469	Tool	Bad Bot
1471	Search Engine	Bad Bot

Bot signature rule	ID	Description
1484	Uncategorized	Bad Bot
1493	Marketing	Bad Bot
1502	Site Monitor	Bad Bot
1504	Uncategorized	Bad Bot
1506	Uncategorized	Bad Bot
1518	Uncategorized	Bad Bot
1520	Search Engine	Bad Bot
1531	Feed Fetcher	Bad Bot
1533	Uncategorized	Bad Bot
1540	Search Engine	Bad Bot
1556	Marketing	Bad Bot
1560	Uncategorized	Bad Bot
1564	Tool	Bad Bot
1570	Site Monitor	Bad Bot
1575	Search Engine	Bad Bot
1586	Virus Scanner	Bad Bot
1588	Uncategorized	Bad Bot
1594	Tool	Bad Bot
1619	Marketing	Bad Bot
1623	Tool	Bad Bot
1626	Search Engine	Bad Bot
1632	Feed Fetcher	Bad Bot
1648	Search Engine	Bad Bot
1652	Marketing	Bad Bot
1660	Marketing	Bad Bot
1713	Tool	Bad Bot
1719	Search Engine	Bad Bot
1722	Uncategorized	Bad Bot
1744	Uncategorized	Bad Bot

Bot signature rule	ID	Description
1754	Uncategorized	Bad Bot
1757	Uncategorized	Bad Bot
1762	Uncategorized	Bad Bot
1769	Uncategorized	Bad Bot
1771	Marketing	Bad Bot
1779	Tool	Bad Bot
1782	Tool	Bad Bot
1785	Speed Tester	Bad Bot
1786	Tool	Bad Bot
1792	Site Monitor	Bad Bot
1869	Tool	Bad Bot
1928	Marketing	Bad Bot
1942	Site Monitor	Bad Bot
1949	Marketing	Bad Bot
1954	Marketing	Bad Bot
1964	Uncategorized	Bad Bot
1969	Search Engine	Bad Bot
2294	Search Engine	Bad Bot
2303	Uncategorized	Bad Bot
2308	Scraper	Bad Bot
2335	Marketing	Bad Bot
2374	Uncategorized	Bad Bot
2377	Uncategorized	Bad Bot
2385	Tool	Bad Bot
2389	Uncategorized	Bad Bot
2414	Uncategorized	Bad Bot
2421	Uncategorized	Bad Bot
2424	Uncategorized	Bad Bot
2427	Uncategorized	Bad Bot

Bot signature rule	ID	Description
2429	Search Engine	Bad Bot
2437	Uncategorized	Bad Bot
2440	Search Engine	Bad Bot
2443	Uncategorized	Bad Bot
2453	Marketing	Bad Bot
2472	Marketing	Bad Bot
2474	Feed Fetcher	Bad Bot
2482	Uncategorized	Bad Bot
2500	Screenshot Creator	Bad Bot
2503	Uncategorized	Bad Bot
2507	Uncategorized	Bad Bot
2516	Tool	Bad Bot
2536	Marketing	Bad Bot
2543	Tool	Bad Bot
2548	Tool	Bad Bot
2557	Marketing	Bad Bot
2561	Uncategorized	Bad Bot
2572	Uncategorized	Bad Bot
2578	Uncategorized	Bad Bot
2584	Uncategorized	Bad Bot
2588	Uncategorized	Bad Bot
2592	Search Engine	Bad Bot
2600	Tool	Bad Bot
2606	Uncategorized	Bad Bot
2611	Uncategorized	Bad Bot
2622	Tool	Bad Bot
2625	Tool	Bad Bot
2631	Tool	Bad Bot
2635	Tool	Bad Bot

Bot signature rule	ID	Description
2637	Screenshot Creator	Bad Bot
2641	Search Engine	Bad Bot
2655	Uncategorized	Bad Bot
2657	Marketing	Bad Bot
2663	Uncategorized	Bad Bot
2666	Tool	Bad Bot
2672	Feed Fetcher	Bad Bot
2674	Tool	Bad Bot
2681	Search Engine	Bad Bot
2684	Marketing	Bad Bot
2690	Uncategorized	Bad Bot
2704	Uncategorized	Bad Bot
2707	Uncategorized	Bad Bot
2714	Feed Fetcher	Bad Bot
2722	Uncategorized	Bad Bot
2726	Feed Fetcher	Bad Bot
2730	Screenshot Creator	Bad Bot
2736	Uncategorized	Bad Bot
2749	Uncategorized	Bad Bot
2753	Tool	Bad Bot
2756	Tool	Bad Bot
2760	Speed Tester	Bad Bot
2780	Tool	Bad Bot
2785	Site Monitor	Bad Bot
2789	Uncategorized	Bad Bot
2797	Tool	Bad Bot
2801	Tool	Bad Bot
2808	Tool	Bad Bot
2810	Uncategorized	Bad Bot

Bot signature rule	ID	Description
2813	Uncategorized	Bad Bot
2816	Uncategorized	Bad Bot
2820	Link Checker	Bad Bot
2824	Link Checker	Bad Bot
2831	Screenshot Creator	Bad Bot
2843	Tool	Bad Bot
2846	Tool	Bad Bot
2849	Marketing	Bad Bot
2851	Uncategorized	Bad Bot
2855	Uncategorized	Bad Bot
2859	Tool	Bad Bot
2873	Uncategorized	Bad Bot
2875	Screenshot Creator	Bad Bot
2879	Uncategorized	Bad Bot
2881	Uncategorized	Bad Bot
2886	Site Monitor	Bad Bot
2899	Uncategorized	Bad Bot
2916	Uncategorized	Bad Bot
2924	Tool	Bad Bot
2932	Marketing	Bad Bot
2935	Link Checker	Bad Bot
2939	Marketing	Bad Bot
2942	Uncategorized	Bad Bot
2955	Search Engine	Bad Bot
2960	Tool	Bad Bot
2964	Uncategorized	Bad Bot
2972	Marketing	Bad Bot
2978	Vulnerability Scanner	Bad Bot
2980	Tool	Bad Bot

Bot signature rule	ID	Description
2985	Marketing	Bad Bot
2993	Uncategorized	Bad Bot
2999	Screenshot Creator	Bad Bot
3003	Feed Fetcher	Bad Bot
3005	Uncategorized	Bad Bot
3013	Uncategorized	Bad Bot
3016	Uncategorized	Bad Bot
3021	Search Engine	Bad Bot
3026	Uncategorized	Bad Bot
3030	Marketing	Bad Bot
3065	Marketing	Bad Bot
3068	Uncategorized	Bad Bot
3072	Marketing	Bad Bot
3077	Marketing	Bad Bot
3080	Uncategorized	Bad Bot
3086	Scraper	Bad Bot
3092	Search Engine	Bad Bot
3100	Uncategorized	Bad Bot
3104	Tool	Bad Bot
3111	Uncategorized	Bad Bot
3116	Site Monitor	Bad Bot
3118	Tool	Bad Bot
3120	Marketing	Bad Bot
3122	Search Engine	Bad Bot
3126	Marketing	Bad Bot
3141	Tool	Bad Bot
3143	Uncategorized	Bad Bot
3145	Scraper	Bad Bot
3150	Uncategorized	Bad Bot

Bot signature rule	ID	Description
3173	Link Checker	Bad Bot
3176	Uncategorized	Bad Bot
3186	Speed Tester	Bad Bot
3190	Scraper	Bad Bot
3203	Search Engine	Bad Bot
3216	Uncategorized	Bad Bot
3220	Tool	Bad Bot
3223	Link Checker	Bad Bot
3241	Uncategorized	Bad Bot
3245	Site Monitor	Bad Bot
3285	Uncategorized	Bad Bot
3304	Marketing	Bad Bot
3307	Link Checker	Bad Bot
3316	Tool	Bad Bot
3326	Marketing	Bad Bot
3333	Search Engine	Bad Bot
3340	Search Engine	Bad Bot
3344	Marketing	Bad Bot
3350	Uncategorized	Bad Bot
3355	Marketing	Bad Bot
3365	Uncategorized	Bad Bot
3378	Uncategorized	Bad Bot
3388	Tool	Bad Bot
3396	Uncategorized	Bad Bot
3400	Uncategorized	Bad Bot
3421	Uncategorized	Bad Bot
3439	Uncategorized	Bad Bot
3447	Feed Fetcher	Bad Bot
3451	Tool	Bad Bot

Bot signature rule	ID	Description
3459	Screenshot Creator	Bad Bot
3469	Vulnerability Scanner	Bad Bot
3475	Uncategorized	Bad Bot
3485	Search Engine	Bad Bot
3493	Tool	Bad Bot
3502	Marketing	Bad Bot
3507	Search Engine	Bad Bot
3523	Uncategorized	Bad Bot
3535	Speed Tester	Bad Bot
3549	Uncategorized	Bad Bot
3556	Uncategorized	Bad Bot
3561	Uncategorized	Bad Bot
3565	Uncategorized	Bad Bot
3572	Search Engine	Bad Bot
3578	Uncategorized	Bad Bot
3610	Search Engine	Bad Bot
3617	Uncategorized	Bad Bot
3621	Marketing	Bad Bot
3632	Tool	Bad Bot
3635	Marketing	Bad Bot
3653	Uncategorized	Bad Bot
3661	Search Engine	Bad Bot
3704	Uncategorized	Bad Bot
3707	Uncategorized	Bad Bot
3711	Uncategorized	Bad Bot
3730	Search Engine	Bad Bot
3740	Site Monitor	Bad Bot
3759	Search Engine	Bad Bot
3764	Uncategorized	Bad Bot

Bot signature rule	ID	Description
3770	Uncategorized	Bad Bot

Bot signature update for March 2021

December 7, 2021

Some of existing bot signatures are updated. You can download and configure these signature rules to protect your appliance from bot attacks.

Bot signature version

Signature version 7 is applicable for Citrix ADC platforms with 13.0 61.x builds or later.

Updated bot signatures in this version

Following is a list of bot signature rule IDs, category, and its type.

Bot signature rule	ID	Description
278	Scraper	Good Bot
378	Scraper	Good Bot
379	Scraper	Good Bot
380	Scraper	Good Bot
381	Scraper	Good Bot
382	Scraper	Good Bot
383	Scraper	Good Bot
384	Scraper	Good Bot
385	Scraper	Good Bot
386	Scraper	Good Bot
387	Scraper	Good Bot
389	Scraper	Good Bot
390	Scraper	Good Bot

Bot signature rule	ID	Description
391	Scraper	Good Bot
494	Scraper	Good Bot
627	Search Engine	Good Bot
660	Search Engine	Good Bot
3840	Crawler	Good Bot

Bot signature update for August 2021

December 7, 2021

New signatures are added and some of existing bot signatures are updated. You can download and configure these signature rules to protect your appliance from bot attacks.

Bot signature version

Signature version 8 is applicable for Citrix ADC platforms with 13.0 61.x builds or later.

Updated bot signatures in this version

Following is a list of bot signature rule IDs, category, and its type.

Bot signature rule	ID	Description
236	Scraper	Good Bot
378	Scraper	Good Bot
381	Scraper	Good Bot
382	Scraper	Good Bot
390	Scraper	Good Bot
544	Scraper	Good Bot
702	Search Engine	Good Bot
979	Scraper	Bad Bot
3791	Speed Tester	Good Bot

Bot signature rule	ID	Description
3797	Marketing	Good Bot
3800	Marketing	Good Bot
3824	Crawler	Bad Bot
3833	Search Engine	Good Bot
3849	Crawler	Good Bot
3871	Marketing	Good Bot
3963	Marketing	Good Bot
4027	Search Engine	Good Bot

New bot signatures in this version

Bot signature rule	ID	Description
4028	Marketing	Good Bot
4029	Tool	Good Bot
4030	Scraper	Good Bot
4031	Scraper	Good Bot
4032	Uncategorized	Bad Bot
4033	Crawler	Good Bot
4034	Crawler	Good Bot
4035	Marketing	Good Bot
4036	Vulnerability Scanner	Good Bot
4037	Vulnerability Scanner	Good Bot
4038	Uncategorized	Bad Bot
4039	Tool	Good Bot
4040	Crawler	Good Bot
4041	Tool	Good Bot
4042	Crawler	Good Bot
4043	Screenshot Creator	Good Bot
4044	Scraper	Bad Bot

Bot signature rule	ID	Description
4045	Scraper	Bad Bot
4046	Scraper	Bad Bot
4047	Uncategorized	Bad Bot
4048	Feed Fetcher	Good Bot
4049	Uncategorized	Bad Bot
4050	Crawler	Good Bot
4051	Crawler	Good Bot
4052	Tool	Good Bot
4053	Tool	Good Bot
4054	Scraper	Bad Bot
4055	Uncategorized	Good Bot
4056	Marketing	Good Bot
4057	Screenshot Creator	Good Bot
4058	Crawler	Good Bot
4059	Uncategorized	Bad Bot
4060	Search Engine	Good Bot
4061	Search Engine	Good Bot
4062	Search Engine	Good Bot
4063	Search Engine	Good Bot
4064	Tool	Good Bot
4065	Scraper	Good Bot
4066	Marketing	Good Bot
4067	Marketing	Good Bot
4068	Uncategorized	Bad Bot
4069	Uncategorized	Bad Bot
4070	Uncategorized	Bad Bot
4071	Tool	Good Bot
4072	Tool	Bad Bot
4073	Uncategorized	Bad Bot

Bot signature rule	ID	Description
4074	Uncategorized	Bad Bot
4075	Tool	Bad Bot
4076	Marketing	Good Bot
4077	Scraper	Good Bot
4078	Crawler	Good Bot
4079	Crawler	Good Bot
4080	Tool	Bad Bot
4081	Search Engine	Good Bot
4082	Tool	Good Bot
4083	Uncategorized	Bad Bot
4084	Uncategorized	Bad Bot
4085	Tool	Good Bot
4086	Tool	Good Bot
4087	Tool	Bad Bot
4088	Search Engine	Good Bot
4089	Marketing	Good Bot
4090	Tool	Good Bot
4091	Tool	Good Bot
4092	Tool	Good Bot
4093	Tool	Good Bot
4094	Uncategorized	Good Bot
4095	Site Monitor	Good Bot
4096	Site Monitor	Good Bot
4097	Site Monitor	Good Bot
4098	Crawler	Good Bot
4099	Search Engine	Good Bot
4100	Search Engine	Good Bot
4101	Search Engine	Good Bot
4102	Search Engine	Good Bot

Bot signature rule	ID	Description
4103	Marketing	Good Bot
4104	Marketing	Good Bot
4105	Marketing	Good Bot
4106	Marketing	Good Bot
4107	Marketing	Good Bot
4108	Marketing	Good Bot
4109	Search Engine	Good Bot
4110	Crawler	Good Bot
4111	Crawler	Good Bot
4112	Crawler	Good Bot
4113	Vulnerability Scanner	Good Bot
4114	Crawler	Good Bot
4115	Tool	Good Bot
4116	Uncategorized	Bad Bot
4117	Uncategorized	Bad Bot
4118	Uncategorized	Bad Bot
4119	Uncategorized	Bad Bot
4120	Marketing	Good Bot
4121	Marketing	Good Bot
4122	Marketing	Good Bot
4123	Marketing	Good Bot
4124	Marketing	Good Bot
4125	Marketing	Good Bot
4126	Marketing	Good Bot
4127	Marketing	Good Bot
4128	Marketing	Good Bot
4129	Marketing	Good Bot
4130	Marketing	Good Bot
4131	Tool	Good Bot

Bot signature rule	ID	Description
4132	Marketing	Good Bot
4133	Marketing	Good Bot
4134	Tool	Good Bot
4135	Marketing	Good Bot
4136	Marketing	Good Bot
4137	Marketing	Good Bot
4138	Marketing	Good Bot
4139	Marketing	Good Bot
4140	Marketing	Good Bot
4141	Marketing	Good Bot
4142	Marketing	Good Bot
4143	Marketing	Good Bot
4144	Marketing	Good Bot
4145	Search Engine	Good Bot
4146	Search Engine	Good Bot
4147	Search Engine	Good Bot
4148	Search Engine	Good Bot
4149	Search Engine	Good Bot
4150	Search Engine	Good Bot
4151	Search Engine	Good Bot
4152	Search Engine	Good Bot
4153	Search Engine	Good Bot
4154	Search Engine	Good Bot
4155	Search Engine	Good Bot
4156	Screenshot Creator	Good Bot
4157	Search Engine	Good Bot
4158	Search Engine	Good Bot
4159	Search Engine	Good Bot
4160	Screenshot Creator	Good Bot

Bot signature rule	ID	Description
4161	Search Engine	Good Bot
4162	Search Engine	Good Bot
4163	Tool	Good Bot
4164	Search Engine	Good Bot
4165	Marketing	Good Bot
4166	Uncategorized	Bad Bot
4167	Tool	Bad Bot
4168	Speed Tester	Good Bot
4169	Scraper	Bad Bot
4170	Tool	Good Bot
4171	Scraper	Bad Bot
4172	Web Crawler	Good Bot
4173	Tool	Good Bot
4174	Crawler	Good Bot
4175	Crawler	Good Bot
4176	Tool	Good Bot
4177	Search Engine	Good Bot
4178	Tool	Good Bot
4179	Web Crawler	Good Bot
4180	Tool	Good Bot
4181	Site Monitor	Good Bot
4182	Site Monitor	Good Bot
4183	Site Monitor	Good Bot
4184	Site Monitor	Good Bot
4185	Search Engine	Good Bot
4186	Tool	Good Bot
4187	Tool	Good Bot
4188	Screenshot Creator	Good Bot
4189	Marketing	Good Bot

Bot signature rule	ID	Description
4190	Search Engine	Good Bot
4191	Search Engine	Good Bot
4192	Search Engine	Good Bot
4193	Search Engine	Good Bot
4194	Tool	Good Bot
4195	Search Engine	Bad Bot
4196	Tool	Good Bot
4197	Tool	Good Bot
4198	Marketing	Good Bot
4199	Marketing	Good Bot
4200	Vulnerability Scanner	Good Bot
4201	Tool	Good Bot
4202	Tool	Good Bot
4203	Uncategorized	Bad Bot
4204	Uncategorized	Bad Bot
4205	Search Engine	Good Bot
4206	Marketing	Good Bot
4207	Marketing	Good Bot
4208	Search Engine	Good Bot
4209	Search Engine	Good Bot
4210	Speed Tester	Good Bot
4211	Tool	Good Bot
4212	Feed Fetcher	Good Bot
4213	Feed Fetcher	Good Bot
4214	Scraper	Bad Bot
4215	Tool	Good Bot
4216	Tool	Good Bot
4217	Tool	Bad Bot
4218	Scraper	Bad Bot

Bot signature rule	ID	Description
4219	Marketing	Good Bot
4220	Tool	Good Bot
4221	Tool	Bad Bot
4222	Site Monitor	Good Bot
4223	Marketing	Good Bot
4224	Search Engine	Good Bot
4225	Search Engine	Good Bot
4226	Search Engine	Good Bot
4227	Marketing	Good Bot
4228	Marketing	Good Bot
4229	Tool	Good Bot
4230	Uncategorized	Bad Bot
4231	Screenshot Creator	Good Bot
4232	Tool	Good Bot
4233	Site Monitor	Good Bot
4234	Site Monitor	Good Bot
4235	Site Monitor	Good Bot
4236	Site Monitor	Good Bot
4237	Site Monitor	Good Bot
4238	Site Monitor	Good Bot
4239	Uncategorized	Bad Bot
4240	Marketing	Good Bot
4241	Marketing	Good Bot
4242	Marketing	Good Bot
4243	Marketing	Good Bot
4244	Marketing	Good Bot
4245	Marketing	Good Bot
4246	Marketing	Good Bot
4247	Search Engine	Good Bot

Bot signature rule	ID	Description
4248	Search Engine	Good Bot
4249	Screenshot Creator	Good Bot
4250	Search Engine	Good Bot
4251	Search Engine	Good Bot
4252	Crawler	Good Bot
4253	Crawler	Good Bot
4254	Crawler	Good Bot
4255	Tool	Good Bot
4256	Uncategorized	Good Bot
4257	Tool	Good Bot
4258	Crawler	Good Bot
4259	Crawler	Good Bot
4260	Tool	Good Bot
4261	Tool	Good Bot
4262	Tool	Good Bot
4263	Marketing	Good Bot
4264	Crawler	Bad Bot
4265	Search Engine	Good Bot
4266	Uncategorized	Good Bot
4267	Tool	Good Bot
4268	Tool	Good Bot
4269	Search Engine	Good Bot
4270	Search Engine	Good Bot
4271	Search Engine	Good Bot
4272	Search Engine	Good Bot
4273	Search Engine	Good Bot
4274	Search Engine	Good Bot
4275	Search Engine	Good Bot
4276	Uncategorized	Bad Bot

Bot signature rule	ID	Description
4277	Uncategorized	Bad Bot
4278	Uncategorized	Bad Bot
4279	Marketing	Good Bot
4280	Crawler	Good Bot
4281	Uncategorized	Bad Bot
4282	Marketing	Good Bot
4283	Marketing	Good Bot
4284	Marketing	Good Bot
4285	Marketing	Good Bot
4286	Marketing	Good Bot
4287	Marketing	Good Bot
4288	Marketing	Good Bot
4289	Marketing	Good Bot
4290	Marketing	Good Bot
4291	Marketing	Good Bot
4292	Marketing	Good Bot
4293	Marketing	Good Bot
4294	Marketing	Good Bot
4295	Search Engine	Good Bot
4296	Search Engine	Good Bot
4297	Search Engine	Good Bot
4298	Search Engine	Good Bot
4299	Search Engine	Good Bot
4300	Search Engine	Good Bot
4301	Search Engine	Good Bot
4302	Search Engine	Good Bot
4303	Search Engine	Good Bot
4304	Search Engine	Good Bot
4305	Search Engine	Good Bot

Bot signature rule	ID	Description
4306	Screenshot Creator	Good Bot
4307	Search Engine	Good Bot
4308	Search Engine	Good Bot
4309	Search Engine	Good Bot
4310	Search Engine	Good Bot
4311	Screenshot Creator	Good Bot
4312	Search Engine	Good Bot
4313	Search Engine	Good Bot
4314	Search Engine	Good Bot
4315	Search Engine	Good Bot
4316	Search Engine	Good Bot
4317	Search Engine	Good Bot
4318	Screenshot Creator	Good Bot
4319	Screenshot Creator	Good Bot
4320	Uncategorized	Bad Bot
4321	Uncategorized	Good Bot
4322	Crawler	Good Bot
4323	Tool	Good Bot
4324	Tool	Good Bot
4325	Tool	Good Bot
4326	Scraper	Bad Bot
4327	Search Engine	Good Bot
4328	Marketing	Good Bot
4329	Uncategorized	Bad Bot
4330	Site Monitor	Good Bot
4331	Search Engine	Good Bot
4332	Search Engine	Good Bot
4333	Uncategorized	Bad Bot
4334	Scraper	Good Bot

Bot signature rule	ID	Description
4335	Marketing	Good Bot
4336	Marketing	Good Bot
4337	Tool	Good Bot
4338	Tool	Good Bot
4339	Tool	Good Bot
4340	Crawler	Good Bot
4341	Crawler	Good Bot
4342	Vulnerability Scanner	Good Bot
4343	Vulnerability Scanner	Good Bot
4344	Scraper	Good Bot
4345	Marketing	Good Bot
4346	Marketing	Good Bot
4347	Marketing	Good Bot
4348	Marketing	Good Bot
4349	Marketing	Good Bot
4350	Marketing	Good Bot
4351	Marketing	Good Bot
4352	Marketing	Good Bot
4353	Marketing	Good Bot
4354	Marketing	Good Bot
4355	Search Engine	Good Bot
4356	Search Engine	Good Bot
4357	Search Engine	Good Bot
4358	Search Engine	Good Bot
4359	Search Engine	Good Bot
4360	Search Engine	Good Bot
4361	Search Engine	Good Bot
4362	Search Engine	Good Bot
4363	Search Engine	Good Bot

Bot signature rule	ID	Description
4364	Search Engine	Good Bot
4365	Screenshot Creator	Good Bot
4366	Search Engine	Good Bot
4367	Search Engine	Good Bot
4368	Search Engine	Good Bot
4369	Search Engine	Good Bot
4370	Screenshot Creator	Good Bot
4371	Search Engine	Good Bot
4372	Search Engine	Good Bot
4373	Search Engine	Good Bot
4374	Search Engine	Good Bot
4375	Search Engine	Good Bot
4376	Screenshot Creator	Good Bot
4377	Crawler	Good Bot
4378	Crawler	Good Bot
4379	Search Engine	Good Bot
4380	Search Engine	Good Bot
4381	Search Engine	Good Bot
4382	Search Engine	Good Bot
4383	Crawler	Good Bot
4384	Search Engine	Good Bot
4385	Tool	Good Bot
4386	Uncategorized	Good Bot
4387	Crawler	Good Bot
4388	Crawler	Good Bot
4389	Tool	Good Bot
4390	Tool	Good Bot
4391	Tool	Good Bot
4392	Tool	Good Bot

Bot signature rule	ID	Description
4393	Tool	Good Bot
4394	Uncategorized	Good Bot
4395	Tool	Good Bot
4396	Site Monitor	Good Bot
4397	Site Monitor	Good Bot
4398	Tool	Bad Bot
4399	Tool	Bad Bot
4400	Tool	Bad Bot
4401	Tool	Bad Bot
4402	Tool	Bad Bot
4403	Tool	Bad Bot
4404	Search Engine	Good Bot
4405	Search Engine	Good Bot
4406	Search Engine	Good Bot
4407	Uncategorized	Good Bot

Aktualisierung der Bot-Signatur für September 2021

January 28, 2022

Neue Signaturen wurden hinzugefügt und einige der vorhandenen Bot-Signaturen wurden aktualisiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Bot-Angriffen zu schützen.

Bot-Signaturversion

Signaturversion 9 gilt für Citrix ADC-Plattformen mit 13.0 Builds 61.48 oder höher.

Aktualisierte Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signaturregel	ID	Beschreibung
2	Crawler	Good Bot
5	Crawler	Good Bot
9	Crawler	Good Bot
45	Crawler	Good Bot
46	Crawler	Good Bot
48	Crawler	Good Bot
52	Crawler	Good Bot
60	Crawler	Good Bot
61	Crawler	Good Bot
63	Crawler	Good Bot
67	Crawler	Good Bot
71	Crawler	Good Bot
74	Crawler	Good Bot
75	Crawler	Good Bot
76	Crawler	Good Bot
78	Crawler	Good Bot
79	Crawler	Good Bot
80	Crawler	Good Bot
81	Crawler	Good Bot
82	Crawler	Good Bot
83	Crawler	Good Bot
84	Crawler	Good Bot
87	Crawler	Good Bot
90	Crawler	Good Bot
95	Crawler	Good Bot
96	Crawler	Good Bot
97	Crawler	Good Bot
100	Crawler	Good Bot
101	Crawler	Good Bot

Bot-Signaturregel	ID	Beschreibung
102	Crawler	Good Bot
103	Crawler	Good Bot
104	Crawler	Good Bot
107	Crawler	Good Bot
108	Crawler	Good Bot
110	Crawler	Good Bot
111	Crawler	Good Bot
114	Crawler	Good Bot
115	Crawler	Good Bot
123	Crawler	Good Bot
135	Crawler	Good Bot
136	Crawler	Good Bot
137	Crawler	Good Bot
140	Crawler	Good Bot
141	Crawler	Good Bot
143	Crawler	Good Bot
144	Crawler	Good Bot
145	Crawler	Good Bot
146	Crawler	Good Bot
147	Crawler	Good Bot
149	Crawler	Good Bot
152	Crawler	Good Bot
155	Crawler	Good Bot
156	Crawler	Good Bot
157	Crawler	Good Bot
158	Crawler	Good Bot
159	Crawler	Good Bot
160	Crawler	Good Bot
161	Crawler	Good Bot

Bot-Signaturregel	ID	Beschreibung
162	Crawler	Good Bot
163	Crawler	Good Bot
164	Crawler	Good Bot
165	Crawler	Good Bot
166	Crawler	Good Bot
167	Crawler	Good Bot
172	Crawler	Good Bot
173	Crawler	Good Bot
174	Crawler	Good Bot
176	Crawler	Good Bot
177	Crawler	Good Bot
180	Crawler	Good Bot
187	Crawler	Good Bot
197	Crawler	Good Bot
201	Crawler	Good Bot
202	Crawler	Good Bot
203	Crawler	Good Bot
206	Crawler	Good Bot
211	Feed Fetcher	Schlechter Bot
217	Feed Fetcher	Good Bot
219	Feed Fetcher	Good Bot
229	Scraper	Good Bot
235	Scraper	Good Bot
236	Scraper	Good Bot
237	Scraper	Good Bot
248	Scraper	Good Bot
250	Scraper	Good Bot
260	Scraper	Good Bot
263	Scraper	Good Bot

Bot-Signaturregel	ID	Beschreibung
265	Scraper	Good Bot
267	Scraper	Good Bot
268	Scraper	Good Bot
271	Scraper	Good Bot
272	Scraper	Good Bot
276	Scraper	Good Bot
277	Scraper	Good Bot
278	Scraper	Good Bot
279	Scraper	Good Bot
280	Scraper	Good Bot
281	Scraper	Good Bot
283	Scraper	Good Bot
285	Scraper	Good Bot
286	Scraper	Good Bot
287	Scraper	Good Bot
290	Scraper	Good Bot
292	Scraper	Good Bot
293	Scraper	Good Bot
342	Scraper	Good Bot
343	Scraper	Good Bot
344	Scraper	Good Bot
355	Scraper	Good Bot
357	Scraper	Good Bot
360	Scraper	Good Bot
362	Scraper	Good Bot
366	Scraper	Good Bot
370	Scraper	Good Bot
371	Scraper	Good Bot
372	Scraper	Good Bot

Bot-Signaturregel	ID	Beschreibung
373	Scraper	Good Bot
374	Scraper	Good Bot
376	Scraper	Good Bot
377	Scraper	Good Bot
380	Scraper	Good Bot
392	Scraper	Good Bot
393	Scraper	Good Bot
394	Scraper	Good Bot
396	Scraper	Good Bot
397	Scraper	Good Bot
414	Scraper	Good Bot
418	Scraper	Good Bot
419	Scraper	Good Bot
421	Scraper	Good Bot
422	Scraper	Good Bot
423	Scraper	Good Bot
424	Scraper	Good Bot
425	Scraper	Good Bot
426	Scraper	Good Bot
427	Scraper	Good Bot
428	Scraper	Good Bot
430	Scraper	Good Bot
432	Scraper	Good Bot
433	Scraper	Good Bot
434	Scraper	Good Bot
435	Scraper	Good Bot
441	Scraper	Good Bot
445	Scraper	Good Bot
446	Scraper	Good Bot

Bot-Signaturregel	ID	Beschreibung
451	Scraper	Good Bot
452	Scraper	Good Bot
454	Scraper	Good Bot
455	Scraper	Good Bot
456	Scraper	Good Bot
457	Scraper	Good Bot
458	Scraper	Good Bot
461	Scraper	Good Bot
465	Scraper	Good Bot
466	Scraper	Good Bot
469	Scraper	Good Bot
473	Scraper	Good Bot
474	Scraper	Good Bot
476	Scraper	Good Bot
477	Scraper	Good Bot
484	Scraper	Good Bot
485	Scraper	Good Bot
487	Scraper	Good Bot
488	Scraper	Good Bot
489	Scraper	Good Bot
490	Scraper	Good Bot
493	Scraper	Good Bot
494	Scraper	Good Bot
495	Scraper	Good Bot
497	Scraper	Good Bot
498	Scraper	Good Bot
499	Scraper	Good Bot
500	Scraper	Good Bot
505	Scraper	Good Bot

Bot-Signaturregel	ID	Beschreibung
506	Scraper	Good Bot
507	Scraper	Good Bot
512	Scraper	Good Bot
513	Scraper	Good Bot
514	Scraper	Good Bot
527	Scraper	Good Bot
533	Scraper	Good Bot
539	Scraper	Good Bot
540	Scraper	Good Bot
542	Scraper	Good Bot
544	Scraper	Good Bot
545	Scraper	Good Bot
546	Scraper	Good Bot
547	Scraper	Good Bot
548	Scraper	Good Bot
551	Scraper	Good Bot
552	Scraper	Good Bot
554	Scraper	Good Bot
556	Scraper	Good Bot
558	Scraper	Good Bot
560	Scraper	Good Bot
561	Scraper	Good Bot
566	Scraper	Good Bot
575	Scraper	Good Bot
578	Scraper	Good Bot
581	Scraper	Good Bot
591	Scraper	Good Bot
593	Scraper	Good Bot
595	Scraper	Good Bot

Bot-Signaturregel	ID	Beschreibung
600	Scraper	Good Bot
601	Scraper	Good Bot
602	Scraper	Good Bot
604	Scraper	Good Bot
605	Scraper	Good Bot
609	Scraper	Good Bot
610	Scraper	Good Bot
611	Scraper	Good Bot
612	Scraper	Good Bot
613	Scraper	Good Bot
615	Scraper	Good Bot
620	Suchmaschine	Good Bot
622	Suchmaschine	Good Bot
623	Suchmaschine	Good Bot
624	Suchmaschine	Good Bot
626	Suchmaschine	Good Bot
627	Suchmaschine	Good Bot
628	Suchmaschine	Good Bot
629	Suchmaschine	Good Bot
633	Suchmaschine	Good Bot
634	Suchmaschine	Good Bot
636	Suchmaschine	Good Bot
637	Suchmaschine	Good Bot
639	Suchmaschine	Good Bot
640	Suchmaschine	Good Bot
641	Suchmaschine	Good Bot
642	Suchmaschine	Good Bot
643	Suchmaschine	Good Bot
647	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
649	Suchmaschine	Good Bot
650	Suchmaschine	Good Bot
651	Suchmaschine	Good Bot
654	Suchmaschine	Good Bot
656	Suchmaschine	Good Bot
657	Suchmaschine	Good Bot
658	Suchmaschine	Good Bot
659	Suchmaschine	Good Bot
660	Suchmaschine	Good Bot
663	Suchmaschine	Good Bot
664	Suchmaschine	Good Bot
665	Suchmaschine	Good Bot
666	Suchmaschine	Good Bot
667	Suchmaschine	Good Bot
669	Suchmaschine	Good Bot
670	Suchmaschine	Good Bot
671	Suchmaschine	Good Bot
672	Suchmaschine	Good Bot
673	Suchmaschine	Good Bot
674	Suchmaschine	Good Bot
675	Suchmaschine	Good Bot
676	Suchmaschine	Good Bot
677	Suchmaschine	Good Bot
679	Suchmaschine	Good Bot
680	Suchmaschine	Good Bot
690	Suchmaschine	Good Bot
693	Suchmaschine	Good Bot
694	Suchmaschine	Good Bot
697	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
698	Suchmaschine	Good Bot
703	Suchmaschine	Good Bot
706	Suchmaschine	Good Bot
712	Suchmaschine	Good Bot
714	Suchmaschine	Good Bot
715	Suchmaschine	Good Bot
716	Suchmaschine	Good Bot
721	Suchmaschine	Good Bot
723	Suchmaschine	Good Bot
725	Suchmaschine	Good Bot
727	Suchmaschine	Good Bot
728	Suchmaschine	Good Bot
729	Suchmaschine	Good Bot
730	Suchmaschine	Good Bot
731	Suchmaschine	Good Bot
732	Suchmaschine	Good Bot
735	Suchmaschine	Good Bot
736	Suchmaschine	Good Bot
740	Suchmaschine	Good Bot
748	Suchmaschine	Good Bot
749	Suchmaschine	Good Bot
750	Suchmaschine	Good Bot
751	Suchmaschine	Good Bot
756	Suchmaschine	Good Bot
757	Suchmaschine	Good Bot
758	Suchmaschine	Good Bot
759	Suchmaschine	Good Bot
760	Suchmaschine	Good Bot
761	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
762	Suchmaschine	Good Bot
763	Suchmaschine	Good Bot
764	Suchmaschine	Good Bot
765	Suchmaschine	Good Bot
766	Suchmaschine	Good Bot
767	Suchmaschine	Good Bot
768	Suchmaschine	Good Bot
769	Suchmaschine	Good Bot
770	Suchmaschine	Good Bot
771	Suchmaschine	Good Bot
772	Suchmaschine	Good Bot
773	Suchmaschine	Good Bot
776	Suchmaschine	Good Bot
777	Suchmaschine	Good Bot
780	Suchmaschine	Good Bot
781	Suchmaschine	Good Bot
784	Suchmaschine	Good Bot
786	Suchmaschine	Good Bot
787	Suchmaschine	Good Bot
788	Suchmaschine	Good Bot
789	Suchmaschine	Good Bot
790	Suchmaschine	Good Bot
791	Suchmaschine	Good Bot
792	Suchmaschine	Good Bot
795	Suchmaschine	Good Bot
796	Suchmaschine	Good Bot
798	Suchmaschine	Good Bot
800	Suchmaschine	Good Bot
801	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
802	Suchmaschine	Good Bot
803	Suchmaschine	Good Bot
805	Suchmaschine	Good Bot
806	Suchmaschine	Good Bot
807	Suchmaschine	Good Bot
809	Suchmaschine	Good Bot
810	Suchmaschine	Good Bot
811	Suchmaschine	Good Bot
812	Suchmaschine	Good Bot
814	Suchmaschine	Good Bot
815	Suchmaschine	Good Bot
816	Suchmaschine	Good Bot
817	Suchmaschine	Good Bot
818	Suchmaschine	Good Bot
819	Suchmaschine	Good Bot
820	Suchmaschine	Good Bot
821	Suchmaschine	Good Bot
822	Suchmaschine	Good Bot
823	Suchmaschine	Good Bot
825	Suchmaschine	Good Bot
827	Suchmaschine	Good Bot
830	Suchmaschine	Good Bot
831	Suchmaschine	Good Bot
834	Suchmaschine	Good Bot
837	Suchmaschine	Good Bot
838	Suchmaschine	Good Bot
849	Sitemonitor	Good Bot
850	Sitemonitor	Good Bot
851	Sitemonitor	Good Bot

Bot-Signaturregel	ID	Beschreibung
853	Sitemonitor	Good Bot
857	Sitemonitor	Good Bot
858	Sitemonitor	Good Bot
859	Sitemonitor	Good Bot
860	Sitemonitor	Good Bot
861	Sitemonitor	Good Bot
862	Sitemonitor	Good Bot
863	Sitemonitor	Good Bot
864	Sitemonitor	Good Bot
865	Sitemonitor	Good Bot
866	Sitemonitor	Good Bot
867	Sitemonitor	Good Bot
868	Sitemonitor	Good Bot
869	Sitemonitor	Good Bot
870	Sitemonitor	Good Bot
871	Sitemonitor	Good Bot
872	Sitemonitor	Good Bot
873	Sitemonitor	Good Bot
874	Sitemonitor	Good Bot
875	Sitemonitor	Good Bot
876	Sitemonitor	Good Bot
877	Sitemonitor	Good Bot
880	Sitemonitor	Good Bot
883	Sitemonitor	Good Bot
885	Sitemonitor	Good Bot
886	Sitemonitor	Good Bot
888	Sitemonitor	Good Bot
889	Sitemonitor	Good Bot
895	Sitemonitor	Good Bot

Bot-Signaturregel	ID	Beschreibung
896	Sitemonitor	Good Bot
897	Sitemonitor	Good Bot
898	Sitemonitor	Good Bot
900	Sitemonitor	Good Bot
901	Sitemonitor	Good Bot
904	Sitemonitor	Good Bot
906	Sitemonitor	Good Bot
908	Sitemonitor	Good Bot
909	Sitemonitor	Good Bot
910	Sitemonitor	Good Bot
911	Sitemonitor	Good Bot
912	Sitemonitor	Good Bot
913	Sitemonitor	Good Bot
917	Sitemonitor	Good Bot
918	Sitemonitor	Good Bot
919	Sitemonitor	Good Bot
920	Sitemonitor	Good Bot
921	Sitemonitor	Good Bot
924	Sitemonitor	Good Bot
926	Sitemonitor	Good Bot
927	Sitemonitor	Good Bot
928	Sitemonitor	Good Bot
929	Sitemonitor	Good Bot
930	Sitemonitor	Good Bot
931	Sitemonitor	Good Bot
938	Sitemonitor	Good Bot
939	Sitemonitor	Good Bot
943	Sitemonitor	Schlechter Bot
958	Sitemonitor	Good Bot

Bot-Signaturregel	ID	Beschreibung
959	Sitemonitor	Good Bot
960	Sitemonitor	Good Bot
963	Sitemonitor	Good Bot
984	Scraper	Good Bot
996	Scraper	Good Bot
997	Scraper	Good Bot
998	Scraper	Good Bot
1002	Scraper	Good Bot
1006	Scraper	Good Bot
1588	Nicht kategorisiert	Schlechter Bot
2561	Scraper	Schlechter Bot
2810	Crawler	Good Bot
3782	Marketing	Good Bot
3783	Suchmaschine	Good Bot
3788	Tool	Good Bot
3789	Tool	Good Bot
3790	Crawler	Good Bot
3792	Tool	Good Bot
3793	Tool	Good Bot
3794	Crawler	Good Bot
3796	Scraper	Good Bot
3798	Marketing	Good Bot
3799	Marketing	Good Bot
3801	Marketing	Good Bot
3802	Screenshot Creator	Good Bot
3803	Suchmaschine	Good Bot
3804	Screenshot Creator	Good Bot
3805	Suchmaschine	Good Bot
3806	Tool	Good Bot

Bot-Signaturregel	ID	Beschreibung
3807	Crawler	Good Bot
3808	Crawler	Good Bot
3809	Tool	Good Bot
3810	Scraper	Good Bot
3811	Tool	Good Bot
3813	Tool	Good Bot
3814	Crawler	Good Bot
3815	Nicht kategorisiert	Good Bot
3817	Tool	Good Bot
3818	Tool	Good Bot
3819	Tool	Good Bot
3820	Crawler	Good Bot
3821	Suchmaschine	Good Bot
3822	Marketing	Good Bot
3823	Nicht kategorisiert	Good Bot
3831	Scraper	Good Bot
3834	Suchmaschine	Good Bot
3835	Suchmaschine	Good Bot
3836	Nicht kategorisiert	Good Bot
3837	Nicht kategorisiert	Good Bot
3838	Nicht kategorisiert	Good Bot
3839	Marketing	Good Bot
3840	Crawler	Good Bot
3842	Crawler	Good Bot
3843	Crawler	Good Bot
3844	Marketing	Good Bot
3845	Marketing	Good Bot
3846	Marketing	Good Bot
3847	Marketing	Good Bot

Bot-Signaturregel	ID	Beschreibung
3848	Nicht kategorisiert	Good Bot
3850	Tool	Good Bot
3851	Nicht kategorisiert	Good Bot
3852	Tool	Good Bot
3853	Vulnerability Scanner	Good Bot
3854	Crawler	Good Bot
3855	Crawler	Good Bot
3856	Tool	Good Bot
3861	Marketing	Good Bot
3862	Marketing	Good Bot
3863	Marketing	Good Bot
3864	Marketing	Good Bot
3865	Marketing	Good Bot
3866	Marketing	Good Bot
3867	Marketing	Good Bot
3868	Marketing	Good Bot
3869	Tool	Good Bot
3870	Marketing	Good Bot
3872	Marketing	Good Bot
3873	Suchmaschine	Good Bot
3874	Suchmaschine	Good Bot
3875	Suchmaschine	Good Bot
3876	Suchmaschine	Good Bot
3877	Screenshot Creator	Good Bot
3878	Suchmaschine	Good Bot
3879	Suchmaschine	Good Bot
3880	Screenshot Creator	Good Bot
3881	Screenshot Creator	Good Bot
3882	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
3883	Suchmaschine	Good Bot
3884	Suchmaschine	Good Bot
3885	Suchmaschine	Good Bot
3886	Tool	Good Bot
3887	Crawler	Good Bot
3888	Crawler	Good Bot
3889	Nicht kategorisiert	Good Bot
3890	Marketing	Good Bot
3893	Crawler	Good Bot
3894	Tool	Good Bot
3895	Tool	Good Bot
3896	Suchmaschine	Good Bot
3897	Tool	Good Bot
3898	Tool	Good Bot
3899	Nicht kategorisiert	Good Bot
3901	Crawler	Good Bot
3903	Tool	Good Bot
3904	Suchmaschine	Good Bot
3905	Suchmaschine	Good Bot
3906	Suchmaschine	Good Bot
3912	Crawler	Good Bot
3918	Crawler	Good Bot
3919	Nicht kategorisiert	Good Bot
3920	Nicht kategorisiert	Good Bot
3921	Nicht kategorisiert	Good Bot
3922	Nicht kategorisiert	Good Bot
3923	Nicht kategorisiert	Good Bot
3924	Nicht kategorisiert	Good Bot
3925	Nicht kategorisiert	Good Bot

Bot-Signaturregel	ID	Beschreibung
3926	Marketing	Good Bot
3927	Marketing	Good Bot
3928	Marketing	Good Bot
3929	Tool	Good Bot
3930	Marketing	Good Bot
3931	Nicht kategorisiert	Good Bot
3932	Crawler	Good Bot
3933	Marketing	Good Bot
3934	Marketing	Good Bot
3935	Scraper	Good Bot
3936	Marketing	Good Bot
3937	Scraper	Good Bot
3938	Feed Fetcher	Good Bot
3940	Suchmaschine	Good Bot
3941	Crawler	Good Bot
3942	Scraper	Good Bot
3946	Feed Fetcher	Good Bot
3947	Crawler	Good Bot
3950	Viren-Scanner	Good Bot
3951	Marketing	Good Bot
3952	Marketing	Good Bot
3953	Marketing	Good Bot
3954	Marketing	Good Bot
3955	Marketing	Good Bot
3956	Marketing	Good Bot
3957	Marketing	Good Bot
3958	Marketing	Good Bot
3959	Marketing	Good Bot
3960	Marketing	Good Bot

Bot-Signaturregel	ID	Beschreibung
3961	Marketing	Good Bot
3962	Marketing	Good Bot
3964	Marketing	Good Bot
3965	Marketing	Good Bot
3966	Marketing	Good Bot
3967	Marketing	Good Bot
3968	Marketing	Good Bot
3969	Marketing	Good Bot
3970	Suchmaschine	Good Bot
3971	Screenshot Creator	Good Bot
3972	Screenshot Creator	Good Bot
3973	Suchmaschine	Good Bot
3974	Suchmaschine	Good Bot
3975	Suchmaschine	Good Bot
3976	Suchmaschine	Good Bot
3977	Suchmaschine	Good Bot
3978	Screenshot Creator	Good Bot
3979	Suchmaschine	Good Bot
3980	Screenshot Creator	Good Bot
3981	Suchmaschine	Good Bot
3982	Suchmaschine	Good Bot
3983	Suchmaschine	Good Bot
3984	Suchmaschine	Good Bot
3985	Suchmaschine	Good Bot
3986	Suchmaschine	Good Bot
3987	Screenshot Creator	Good Bot
3988	Suchmaschine	Good Bot
3989	Suchmaschine	Good Bot
3990	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
3991	Suchmaschine	Good Bot
3992	Suchmaschine	Good Bot
3993	Suchmaschine	Good Bot
3994	Suchmaschine	Good Bot
3995	Suchmaschine	Good Bot
3996	Suchmaschine	Good Bot
3997	Suchmaschine	Good Bot
3998	Suchmaschine	Good Bot
3999	Suchmaschine	Good Bot
4000	Screenshot Creator	Good Bot
4001	Suchmaschine	Good Bot
4002	Suchmaschine	Good Bot
4003	Suchmaschine	Good Bot
4004	Suchmaschine	Good Bot
4005	Screenshot Creator	Good Bot
4006	Crawler	Good Bot
4007	Marketing	Good Bot
4008	Marketing	Good Bot
4011	Tool	Good Bot
4012	Crawler	Good Bot
4013	Suchmaschine	Good Bot
4014	Tool	Good Bot
4015	Crawler	Good Bot
4016	Crawler	Good Bot
4017	Tool	Good Bot
4018	Tool	Good Bot
4019	Tool	Good Bot
4020	Tool	Good Bot
4021	Marketing	Good Bot

Bot-Signaturregel	ID	Beschreibung
4024	Tool	Good Bot
4025	Suchmaschine	Good Bot
4026	Suchmaschine	Good Bot
4028	Marketing	Good Bot
4029	Tool	Good Bot
4030	Scraper	Good Bot
4031	Scraper	Good Bot
4035	Marketing	Good Bot
4037	Vulnerability Scanner	Good Bot
4042	Crawler	Good Bot
4043	Screenshot Creator	Good Bot
4048	Feed Fetcher	Good Bot
4052	Tool	Good Bot
4055	Nicht kategorisiert	Good Bot
4056	Marketing	Good Bot
4057	Screenshot Creator	Good Bot
4058	Crawler	Good Bot
4060	Suchmaschine	Good Bot
4061	Suchmaschine	Good Bot
4062	Suchmaschine	Good Bot
4063	Suchmaschine	Good Bot
4065	Scraper	Good Bot
4066	Marketing	Good Bot
4067	Marketing	Good Bot
4071	Tool	Good Bot
4076	Marketing	Good Bot
4078	Crawler	Good Bot
4079	Crawler	Good Bot
4081	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
4082	Tool	Good Bot
4085	Tool	Good Bot
4086	Tool	Good Bot
4090	Tool	Good Bot
4091	Tool	Good Bot
4092	Tool	Good Bot
4093	Tool	Good Bot
4094	Nicht kategorisiert	Good Bot
4095	Sitemonitor	Good Bot
4096	Sitemonitor	Good Bot
4097	Sitemonitor	Good Bot
4098	Crawler	Good Bot
4099	Suchmaschine	Good Bot
4100	Suchmaschine	Good Bot
4101	Suchmaschine	Good Bot
4102	Suchmaschine	Good Bot
4103	Marketing	Good Bot
4104	Marketing	Good Bot
4105	Marketing	Good Bot
4106	Marketing	Good Bot
4107	Marketing	Good Bot
4108	Marketing	Good Bot
4109	Suchmaschine	Good Bot
4110	Crawler	Good Bot
4111	Crawler	Good Bot
4112	Crawler	Good Bot
4113	Vulnerability Scanner	Good Bot
4114	Crawler	Good Bot
4115	Tool	Good Bot

Bot-Signaturregel	ID	Beschreibung
4120	Marketing	Good Bot
4121	Marketing	Good Bot
4122	Marketing	Good Bot
4123	Marketing	Good Bot
4124	Marketing	Good Bot
4125	Marketing	Good Bot
4126	Marketing	Good Bot
4127	Marketing	Good Bot
4128	Marketing	Good Bot
4129	Marketing	Good Bot
4130	Marketing	Good Bot
4131	Tool	Good Bot
4132	Marketing	Good Bot
4133	Marketing	Good Bot
4134	Tool	Good Bot
4135	Marketing	Good Bot
4136	Marketing	Good Bot
4137	Marketing	Good Bot
4138	Marketing	Good Bot
4139	Marketing	Good Bot
4140	Marketing	Good Bot
4141	Marketing	Good Bot
4142	Marketing	Good Bot
4143	Marketing	Good Bot
4144	Marketing	Good Bot
4147	Suchmaschine	Good Bot
4148	Suchmaschine	Good Bot
4149	Suchmaschine	Good Bot
4150	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
4151	Suchmaschine	Good Bot
4152	Suchmaschine	Good Bot
4153	Suchmaschine	Good Bot
4154	Suchmaschine	Good Bot
4155	Suchmaschine	Good Bot
4156	Screenshot Creator	Good Bot
4157	Suchmaschine	Good Bot
4158	Suchmaschine	Good Bot
4159	Suchmaschine	Good Bot
4160	Screenshot Creator	Good Bot
4161	Suchmaschine	Good Bot
4162	Suchmaschine	Good Bot
4163	Tool	Good Bot
4164	Suchmaschine	Good Bot
4168	Geschwindigkeitstester	Good Bot
4170	Tool	Good Bot
4172	Crawler	Good Bot
4173	Tool	Good Bot
4174	Crawler	Good Bot
4175	Crawler	Good Bot
4176	Tool	Good Bot
4177	Suchmaschine	Good Bot
4178	Tool	Good Bot
4179	Crawler	Good Bot
4180	Tool	Good Bot
4181	Sitemonitor	Good Bot
4182	Sitemonitor	Good Bot
4183	Sitemonitor	Good Bot
4184	Sitemonitor	Good Bot

Bot-Signaturregel	ID	Beschreibung
4185	Suchmaschine	Good Bot
4186	Tool	Good Bot
4187	Tool	Good Bot
4190	Suchmaschine	Good Bot
4191	Suchmaschine	Good Bot
4192	Suchmaschine	Good Bot
4193	Suchmaschine	Good Bot
4194	Tool	Good Bot
4196	Tool	Good Bot
4197	Tool	Good Bot
4198	Marketing	Good Bot
4199	Marketing	Good Bot
4200	Vulnerability Scanner	Good Bot
4201	Tool	Good Bot
4202	Tool	Good Bot
4205	Suchmaschine	Good Bot
4206	Marketing	Good Bot
4207	Marketing	Good Bot
4208	Suchmaschine	Good Bot
4209	Suchmaschine	Good Bot
4210	Geschwindigkeitstester	Good Bot
4211	Tool	Good Bot
4212	Feed Fetcher	Good Bot
4213	Feed Fetcher	Good Bot
4215	Tool	Good Bot
4216	Tool	Good Bot
4219	Marketing	Good Bot
4220	Tool	Good Bot
4222	Sitemonitor	Good Bot

Bot-Signaturregel	ID	Beschreibung
4223	Marketing	Good Bot
4224	Suchmaschine	Good Bot
4225	Suchmaschine	Good Bot
4226	Suchmaschine	Good Bot
4227	Marketing	Good Bot
4228	Marketing	Good Bot
4229	Tool	Good Bot
4231	Screenshot Creator	Good Bot
4232	Tool	Good Bot
4233	Sitemonitor	Good Bot
4234	Sitemonitor	Good Bot
4235	Sitemonitor	Good Bot
4236	Sitemonitor	Good Bot
4237	Sitemonitor	Good Bot
4238	Sitemonitor	Good Bot
4240	Marketing	Good Bot
4241	Marketing	Good Bot
4242	Marketing	Good Bot
4243	Marketing	Good Bot
4244	Marketing	Good Bot
4245	Marketing	Good Bot
4246	Marketing	Good Bot
4247	Suchmaschine	Good Bot
4248	Suchmaschine	Good Bot
4249	Screenshot Creator	Good Bot
4250	Suchmaschine	Good Bot
4251	Suchmaschine	Good Bot
4252	Crawler	Good Bot
4253	Crawler	Good Bot

Bot-Signaturregel	ID	Beschreibung
4254	Crawler	Good Bot
4255	Tool	Good Bot
4256	Nicht kategorisiert	Good Bot
4257	Tool	Good Bot
4258	Crawler	Good Bot
4259	Crawler	Good Bot
4260	Tool	Good Bot
4261	Tool	Good Bot
4262	Tool	Good Bot
4265	Suchmaschine	Good Bot
4266	Nicht kategorisiert	Good Bot
4267	Tool	Good Bot
4268	Tool	Good Bot
4269	Suchmaschine	Good Bot
4270	Suchmaschine	Good Bot
4271	Suchmaschine	Good Bot
4272	Suchmaschine	Good Bot
4273	Suchmaschine	Good Bot
4274	Suchmaschine	Good Bot
4275	Suchmaschine	Good Bot
4279	Marketing	Good Bot
4280	Crawler	Good Bot
4282	Marketing	Good Bot
4283	Marketing	Good Bot
4284	Marketing	Good Bot
4285	Marketing	Good Bot
4286	Marketing	Good Bot
4287	Marketing	Good Bot
4288	Marketing	Good Bot

Bot-Signaturregel	ID	Beschreibung
4289	Marketing	Good Bot
4290	Marketing	Good Bot
4291	Marketing	Good Bot
4292	Marketing	Good Bot
4293	Marketing	Good Bot
4294	Marketing	Good Bot
4295	Suchmaschine	Good Bot
4296	Suchmaschine	Good Bot
4297	Suchmaschine	Good Bot
4298	Suchmaschine	Good Bot
4299	Suchmaschine	Good Bot
4300	Suchmaschine	Good Bot
4301	Suchmaschine	Good Bot
4302	Suchmaschine	Good Bot
4303	Suchmaschine	Good Bot
4304	Suchmaschine	Good Bot
4305	Suchmaschine	Good Bot
4306	Screenshot Creator	Good Bot
4307	Suchmaschine	Good Bot
4308	Suchmaschine	Good Bot
4309	Suchmaschine	Good Bot
4310	Suchmaschine	Good Bot
4311	Screenshot Creator	Good Bot
4312	Suchmaschine	Good Bot
4313	Suchmaschine	Good Bot
4314	Suchmaschine	Good Bot
4315	Suchmaschine	Good Bot
4316	Suchmaschine	Good Bot
4317	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
4318	Screenshot Creator	Good Bot
4319	Screenshot Creator	Good Bot
4321	Nicht kategorisiert	Good Bot
4322	Crawler	Good Bot
4323	Tool	Good Bot
4324	Tool	Good Bot
4325	Tool	Good Bot
4328	Marketing	Good Bot
4330	Sitemonitor	Good Bot
4331	Suchmaschine	Good Bot
4332	Suchmaschine	Good Bot
4335	Marketing	Good Bot
4336	Marketing	Good Bot
4337	Tool	Good Bot
4338	Tool	Good Bot
4339	Tool	Good Bot
4340	Crawler	Good Bot
4341	Crawler	Good Bot
4342	Vulnerability Scanner	Good Bot
4343	Vulnerability Scanner	Good Bot
4344	Scraper	Good Bot
4345	Marketing	Good Bot
4346	Marketing	Good Bot
4347	Marketing	Good Bot
4348	Marketing	Good Bot
4349	Marketing	Good Bot
4350	Marketing	Good Bot
4351	Marketing	Good Bot
4352	Marketing	Good Bot

Bot-Signaturregel	ID	Beschreibung
4353	Marketing	Good Bot
4354	Marketing	Good Bot
4355	Suchmaschine	Good Bot
4356	Suchmaschine	Good Bot
4357	Suchmaschine	Good Bot
4358	Suchmaschine	Good Bot
4359	Suchmaschine	Good Bot
4360	Suchmaschine	Good Bot
4361	Suchmaschine	Good Bot
4362	Suchmaschine	Good Bot
4363	Suchmaschine	Good Bot
4364	Suchmaschine	Good Bot
4365	Screenshot Creator	Good Bot
4366	Suchmaschine	Good Bot
4367	Suchmaschine	Good Bot
4368	Suchmaschine	Good Bot
4369	Suchmaschine	Good Bot
4370	Screenshot Creator	Good Bot
4371	Suchmaschine	Good Bot
4372	Suchmaschine	Good Bot
4373	Suchmaschine	Good Bot
4374	Suchmaschine	Good Bot
4375	Suchmaschine	Good Bot
4376	Screenshot Creator	Good Bot
4377	Crawler	Good Bot
4378	Crawler	Good Bot
4379	Suchmaschine	Good Bot
4380	Suchmaschine	Good Bot
4381	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
4382	Suchmaschine	Good Bot
4383	Crawler	Good Bot
4384	Suchmaschine	Good Bot
4385	Tool	Good Bot
4386	Nicht kategorisiert	Good Bot
4387	Crawler	Good Bot
4388	Crawler	Good Bot
4389	Tool	Good Bot
4390	Tool	Good Bot
4391	Tool	Good Bot
4392	Tool	Good Bot
4393	Tool	Good Bot
4394	Nicht kategorisiert	Good Bot
4395	Tool	Good Bot
4396	Sitemonitor	Good Bot
4397	Sitemonitor	Good Bot
4404	Suchmaschine	Good Bot
4405	Suchmaschine	Good Bot
4406	Suchmaschine	Good Bot
4407	Nicht kategorisiert	Good Bot

Bot-Signatur-Update für Oktober 2021

January 28, 2022

Neue Signaturen wurden hinzugefügt und einige der vorhandenen Bot-Signaturen wurden aktualisiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Bot-Angriffen zu schützen.

Bot-Signaturversion

Signaturversion 10 gilt für NetScaler Citrix ADC-Plattformen mit 13.0 Builds von 76.31 oder höher.

Aktualisierte Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signaturregel	ID	Beschreibung
71	Crawler	Good Bot
74	Crawler	Good Bot
75	Crawler	Good Bot
372	Scraper	Good Bot
373	Scraper	Good Bot
374	Scraper	Good Bot
375	Scraper	Good Bot
376	Scraper	Good Bot
377	Scraper	Good Bot
378	Scraper	Good Bot
379	Scraper	Good Bot
380	Scraper	Good Bot
381	Scraper	Good Bot
382	Scraper	Good Bot
383	Scraper	Good Bot
384	Scraper	Good Bot
385	Scraper	Good Bot
386	Scraper	Good Bot
387	Scraper	Good Bot
389	Scraper	Good Bot
390	Scraper	Good Bot
391	Scraper	Good Bot
639	Suchmaschine	Good Bot
702	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
703	Suchmaschine	Good Bot
1173	Tool	Good Bot
1174	Marketing	Good Bot
1176	Suchmaschine	Good Bot
1178	Geschwindigkeitstester	Good Bot
1185	Screenshot Creator	Good Bot
1209	Nicht kategorisiert	Good Bot
1531	Feed Fetcher	Good Bot
2586	Nicht kategorisiert	Good Bot
2674	Tool	Good Bot
2756	Tool	Good Bot
2758	Nicht kategorisiert	Good Bot
2759	Tool	Good Bot
2784	Tool	Good Bot
2952	Tool	Good Bot
3163	Tool	Good Bot
3554	Tool	Good Bot
3782	Marketing	Good Bot
3788	Tool	Good Bot
3789	Tool	Good Bot
3797	Marketing	Good Bot
3798	Marketing	Good Bot
3799	Marketing	Good Bot
3800	Marketing	Good Bot
3801	Marketing	Good Bot
3802	Screenshot Creator	Good Bot
3803	Suchmaschine	Good Bot
3804	Screenshot Creator	Good Bot
3805	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
3861	Marketing	Good Bot
3862	Marketing	Good Bot
3863	Marketing	Good Bot
3864	Marketing	Good Bot
3865	Marketing	Good Bot
3866	Marketing	Good Bot
3867	Marketing	Good Bot
3868	Marketing	Good Bot
3869	Tool	Good Bot
3871	Marketing	Good Bot
3872	Marketing	Good Bot
3873	Suchmaschine	Good Bot
3874	Suchmaschine	Good Bot
3875	Suchmaschine	Good Bot
3876	Suchmaschine	Good Bot
3877	Screenshot Creator	Good Bot
3878	Suchmaschine	Good Bot
3879	Suchmaschine	Good Bot
3880	Screenshot Creator	Good Bot
3881	Screenshot Creator	Good Bot
3882	Suchmaschine	Good Bot
3883	Suchmaschine	Good Bot
3884	Suchmaschine	Good Bot
3885	Suchmaschine	Good Bot
3963	Marketing	Good Bot
4040	Crawler	Good Bot
4041	Tool	Good Bot
4120	Marketing	Good Bot
4122	Marketing	Good Bot

Bot-Signaturregel	ID	Beschreibung
4123	Marketing	Good Bot
4124	Marketing	Good Bot
4125	Marketing	Good Bot
4133	Marketing	Good Bot
4134	Tool	Good Bot
4135	Marketing	Good Bot
4136	Marketing	Good Bot
4137	Marketing	Good Bot
4138	Marketing	Good Bot
4139	Marketing	Good Bot
4140	Marketing	Good Bot
4141	Marketing	Good Bot
4142	Marketing	Good Bot
4143	Marketing	Good Bot
4144	Marketing	Good Bot
4145	Suchmaschine	Good Bot
4146	Suchmaschine	Good Bot
4147	Suchmaschine	Good Bot
4148	Suchmaschine	Good Bot
4149	Suchmaschine	Good Bot
4150	Suchmaschine	Good Bot
4151	Suchmaschine	Good Bot
4152	Suchmaschine	Good Bot
4153	Suchmaschine	Good Bot
4154	Suchmaschine	Good Bot
4155	Suchmaschine	Good Bot
4156	Screenshot Creator	Good Bot
4157	Suchmaschine	Good Bot
4158	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
4159	Suchmaschine	Good Bot
4160	Screenshot Creator	Good Bot
4161	Suchmaschine	Good Bot
4162	Suchmaschine	Good Bot
4163	Tool	Good Bot
4164	Suchmaschine	Good Bot
4209	Suchmaschine	Good Bot
4240	Marketing	Good Bot
4241	Marketing	Good Bot
4248	Suchmaschine	Good Bot
4249	Screenshot Creator	Good Bot
4250	Suchmaschine	Good Bot
4251	Suchmaschine	Good Bot
4282	Marketing	Good Bot
4283	Marketing	Good Bot
4284	Marketing	Good Bot
4285	Marketing	Good Bot
4286	Marketing	Good Bot
4287	Marketing	Good Bot
4288	Marketing	Good Bot
4289	Marketing	Good Bot
4290	Marketing	Good Bot
4291	Marketing	Good Bot
4292	Marketing	Good Bot
4293	Marketing	Good Bot
4294	Marketing	Good Bot
4295	Suchmaschine	Good Bot
4296	Suchmaschine	Good Bot
4297	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
4298	Suchmaschine	Good Bot
4299	Suchmaschine	Good Bot
4300	Suchmaschine	Good Bot
4301	Suchmaschine	Good Bot
4302	Suchmaschine	Good Bot
4303	Suchmaschine	Good Bot
4304	Suchmaschine	Good Bot
4305	Suchmaschine	Good Bot
4306	Screenshot Creator	Good Bot
4307	Suchmaschine	Good Bot
4308	Suchmaschine	Good Bot
4309	Suchmaschine	Good Bot
4310	Suchmaschine	Good Bot
4311	Screenshot Creator	Good Bot
4312	Suchmaschine	Good Bot
4313	Suchmaschine	Good Bot
4314	Suchmaschine	Good Bot
4315	Suchmaschine	Good Bot
4316	Suchmaschine	Good Bot
4317	Suchmaschine	Good Bot
4318	Screenshot Creator	Good Bot
4319	Screenshot Creator	Good Bot
4337	Tool	Good Bot
4338	Tool	Good Bot
4345	Marketing	Good Bot
4346	Marketing	Good Bot
4347	Marketing	Good Bot
4348	Marketing	Good Bot
4349	Marketing	Good Bot

Bot-Signaturregel	ID	Beschreibung
4350	Marketing	Good Bot
4351	Marketing	Good Bot
4352	Marketing	Good Bot
4353	Marketing	Good Bot
4354	Marketing	Good Bot
4355	Suchmaschine	Good Bot
4356	Suchmaschine	Good Bot
4357	Suchmaschine	Good Bot
4358	Suchmaschine	Good Bot
4359	Suchmaschine	Good Bot
4360	Suchmaschine	Good Bot
4361	Suchmaschine	Good Bot
4362	Suchmaschine	Good Bot
4363	Suchmaschine	Good Bot
4364	Suchmaschine	Good Bot
4365	Screenshot Creator	Good Bot
4366	Suchmaschine	Good Bot
4367	Suchmaschine	Good Bot
4368	Suchmaschine	Good Bot
4369	Suchmaschine	Good Bot
4370	Screenshot Creator	Good Bot
4371	Suchmaschine	Good Bot
4372	Suchmaschine	Good Bot
4373	Suchmaschine	Good Bot
4374	Suchmaschine	Good Bot
4375	Suchmaschine	Good Bot
4376	Screenshot Creator	Good Bot

Bot-Signatur-Update für November 2021

July 8, 2022

Neue Signaturen wurden hinzugefügt und einige der vorhandenen Bot-Signaturen wurden aktualisiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Bot-Angriffen zu schützen.

Bot-Signaturversion

Signaturversion 11 gilt für NetScaler Citrix ADC-Plattformen mit 13.0 Builds von 76.31 oder höher.

Neue Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signaturregel	ID	Beschreibung
4408	Scraper	Good Bot
4409	Crawler	Bad Bot
4411	Marketing	Good Bot
4412	Marketing	Good Bot
4413	Marketing	Good Bot
4421	Screenshot Creator	Good Bot
4422	Crawler	Good Bot
4423	Tool	Bad Bot
4424	Sitemonitor	Good Bot
4425	Marketing	Good Bot
4426	Crawler	Bad Bot
4427	Scraper	Good Bot
4428	Scraper	Good Bot
4429	Screenshot Creator	Good Bot
4430	Viren-Scanner	Good Bot
4431	Sitemonitor	Good Bot
4432	Tool	Good Bot

Bot-Signaturregel	ID	Beschreibung
4433	Suchmaschine	Good Bot
4434	Suchmaschine	Good Bot
4435	Suchmaschine	Good Bot
4436	Marketing	Good Bot
4437	Marketing	Good Bot
4438	Scraper	Good Bot
4439	Scraper	Good Bot
4440	Scraper	Good Bot
4441	Feed Fetcher	Good Bot
4442	Marketing	Good Bot
4443	Scraper	Good Bot
4445	Nicht kategorisiert	Bad Bot
4446	Scraper	Good Bot
4450	Screenshot Creator	Good Bot
4451	Geschwindigkeitstester	Good Bot
4452	Suchmaschine	Good Bot
4466	Nicht kategorisiert	Good Bot
4467	Screenshot Creator	Good Bot
4468	Tool	Good Bot
4469	Nicht kategorisiert	Good Bot
4470	Tool	Good Bot
4472	Scraper	Good Bot
4473	Nicht kategorisiert	Good Bot
4474	Marketing	Good Bot
4476	Crawler	Good Bot
4477	Crawler	Good Bot
4478	Crawler	Good Bot
4479	Crawler	Good Bot
4480	Crawler	Good Bot

Bot-Signaturregel	ID	Beschreibung
4481	Crawler	Good Bot
4482	Crawler	Good Bot
4483	Crawler	Good Bot
4484	Crawler	Good Bot
4485	Crawler	Good Bot
4486	Scraper	Good Bot
4487	Scraper	Good Bot
4488	Scraper	Good Bot
4489	Suchmaschine	Good Bot
4491	Tool	Good Bot
4492	Nicht kategorisiert	Bad Bot
4493	Crawler	Good Bot
4494	Tool	Good Bot
4496	Tool	Good Bot
4497	Crawler	Good Bot
4498	Nicht kategorisiert	Bad Bot
4499	Nicht kategorisiert	Bad Bot
4501	Marketing	Good Bot
4502	Marketing	Good Bot
4503	Marketing	Good Bot
4508	Nicht kategorisiert	Good Bot
4509	Nicht kategorisiert	Good Bot
4510	Nicht kategorisiert	Good Bot
4511	Nicht kategorisiert	Good Bot
4512	Tool	Good Bot
4513	Tool	Good Bot
4514	Tool	Good Bot
4515	Tool	Good Bot
4516	Nicht kategorisiert	Good Bot

Bot-Signaturregel	ID	Beschreibung
4518	Scraper	Bad Bot
4519	Screenshot Creator	Good Bot
4520	Marketing	Good Bot
4521	Nicht kategorisiert	Good Bot
4522	Tool	Good Bot
4523	Nicht kategorisiert	Bad Bot
4524	Nicht kategorisiert	Bad Bot
4525	Crawler	Good Bot
4526	Crawler	Good Bot
4527	Crawler	Good Bot
4528	Crawler	Good Bot
4529	Crawler	Good Bot
4530	Nicht kategorisiert	Bad Bot
4531	Marketing	Good Bot
4532	Marketing	Good Bot
4533	Marketing	Good Bot
4534	Marketing	Good Bot
4535	Marketing	Good Bot
4541	Marketing	Good Bot
4552	Nicht kategorisiert	Good Bot
4553	Tool	Bad Bot
4554	Tool	Bad Bot
4555	Tool	Good Bot
4556	Tool	Good Bot
4558	Scraper	Good Bot
4559	Crawler	Good Bot
4560	Crawler	Good Bot
4561	Sitemonitor	Good Bot
4562	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
4563	Suchmaschine	Good Bot
1000000	Browser	Good Bot
1000001	Scraper	Bad Bot
1000002	Anwendung	Bad Bot
1000003	Browser	Good Bot
1000004	Scraper	Good Bot
1000005	Scraper	Good Bot
1000006	Crawler	Bad Bot
1000007	Browser	Bad Bot
1000008	Nicht kategorisiert	Bad Bot
1000009	Browser	Good Bot
1000010	Scraper	Bad Bot
1000011	Browser	Bad Bot
1000012	Browser	Good Bot
1000013	Browser	Bad Bot
1000014	Scraper	Good Bot
1000015	Scraper	Bad Bot
1000016	Scraper	Bad Bot
1000017	Browser	Good Bot
1000018	Browser	Bad Bot
1000019	Nicht kategorisiert	Bad Bot
1000020	Scraper	Good Bot
1000021	Browser	Bad Bot
1000022	Scraper	Good Bot
1000023	Scraper	Good Bot
1000024	Crawler	Good Bot
1000025	Browser	Bad Bot
1000026	Analysator	Good Bot
1000027	Analysator	Good Bot

Bot-Signaturregel	ID	Beschreibung
1000028	Analysator	Good Bot
1000029	Analysator	Good Bot
1000030	Analysator	Good Bot
1000031	Browser	Good Bot
1000032	Analysator	Good Bot
1000033	Analysator	Good Bot
1000034	Browser	Bad Bot
1000035	Scraper	Good Bot
1000036	Scraper	Good Bot
1000037	Analysator	Good Bot
1000038	Analysator	Good Bot
1000039	Analysator	Good Bot
1000040	Analysator	Good Bot
1000041	Scraper	Good Bot
1000042	Analysator	Good Bot
1000043	Analysator	Good Bot
1000044	Crawler	Good Bot
1000045	Browser	Bad Bot
1000046	Browser	Bad Bot
1000047	Scraper	Good Bot
1000048	Browser	Bad Bot
1000049	Analysator	Good Bot
1000050	Browser	Bad Bot
1000051	Browser	Good Bot
1000052	Browser	Bad Bot
1000053	Scraper	Good Bot
1000054	Browser	Good Bot
1000055	Browser	Good Bot
1000056	Scraper	Bad Bot

Bot-Signaturregel	ID	Beschreibung
1000057	Crawler	Bad Bot
1000058	Scraper	Bad Bot
1000059	Analysator	Good Bot
1000060	Browser	Bad Bot
1000061	Browser	Bad Bot
1000062	Browser	Bad Bot
1000063	Scraper	Bad Bot
1000064	Scraper	Bad Bot
1000065	Scraper	Bad Bot
1000066	Anwendung	Bad Bot
1000067	Scraper	Bad Bot
1000068	Browser	Bad Bot
1000069	Scraper	Bad Bot
1000070	Scraper	Good Bot
1000071	Browser	Good Bot
1000072	Browser	Good Bot
1000073	Browser	Bad Bot
1000074	Browser	Bad Bot
1000075	Anwendung	Bad Bot
1000076	Scraper	Bad Bot

Aktualisierte Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signaturregel	ID	Beschreibung
2	Crawler	Good Bot
5	Crawler	Good Bot
9	Crawler	Good Bot
30	Crawler	Bad Bot

Bot-Signaturregel	ID	Beschreibung
45	Crawler	Good Bot
46	Crawler	Good Bot
48	Crawler	Good Bot
52	Crawler	Good Bot
60	Crawler	Good Bot
61	Crawler	Good Bot
63	Crawler	Good Bot
67	Crawler	Good Bot
76	Crawler	Good Bot
78	Crawler	Good Bot
79	Crawler	Good Bot
80	Crawler	Good Bot
81	Crawler	Good Bot
82	Crawler	Good Bot
83	Crawler	Good Bot
84	Crawler	Good Bot
87	Crawler	Good Bot
90	Crawler	Good Bot
95	Crawler	Good Bot
96	Crawler	Good Bot
97	Crawler	Good Bot
100	Crawler	Good Bot
101	Crawler	Good Bot
102	Crawler	Good Bot
103	Crawler	Good Bot
104	Crawler	Good Bot
107	Crawler	Good Bot
108	Crawler	Good Bot
110	Crawler	Good Bot

Bot-Signaturregel	ID	Beschreibung
111	Crawler	Good Bot
114	Crawler	Good Bot
115	Crawler	Good Bot
123	Crawler	Good Bot
135	Crawler	Good Bot
136	Crawler	Good Bot
137	Crawler	Good Bot
140	Crawler	Good Bot
141	Crawler	Good Bot
143	Crawler	Good Bot
144	Crawler	Good Bot
145	Crawler	Good Bot
146	Crawler	Good Bot
147	Crawler	Good Bot
149	Crawler	Good Bot
152	Crawler	Good Bot
155	Crawler	Good Bot
156	Crawler	Good Bot
157	Crawler	Good Bot
158	Crawler	Good Bot
159	Crawler	Good Bot
160	Crawler	Good Bot
161	Crawler	Good Bot
162	Crawler	Good Bot
163	Crawler	Good Bot
164	Crawler	Good Bot
165	Crawler	Good Bot
166	Crawler	Good Bot
167	Crawler	Good Bot

Bot-Signaturregel	ID	Beschreibung
172	Crawler	Good Bot
173	Crawler	Good Bot
174	Crawler	Good Bot
176	Crawler	Good Bot
177	Crawler	Good Bot
180	Crawler	Good Bot
182	Crawler	Good Bot
187	Crawler	Good Bot
197	Crawler	Good Bot
201	Crawler	Good Bot
202	Crawler	Good Bot
203	Crawler	Good Bot
206	Crawler	Good Bot
217	Feed Fetcher	Good Bot
219	Feed Fetcher	Good Bot
229	Scraper	Good Bot
235	Scraper	Good Bot
236	Scraper	Good Bot
237	Scraper	Good Bot
248	Scraper	Good Bot
250	Scraper	Good Bot
252	Scraper	Good Bot
260	Scraper	Good Bot
263	Scraper	Good Bot
265	Scraper	Good Bot
267	Scraper	Good Bot
268	Scraper	Good Bot
271	Scraper	Good Bot
272	Scraper	Good Bot

Bot-Signaturregel	ID	Beschreibung
276	Scraper	Good Bot
277	Scraper	Good Bot
278	Scraper	Good Bot
279	Scraper	Good Bot
280	Scraper	Good Bot
281	Scraper	Good Bot
283	Scraper	Good Bot
285	Scraper	Good Bot
286	Scraper	Good Bot
287	Scraper	Good Bot
290	Scraper	Good Bot
292	Scraper	Good Bot
293	Scraper	Good Bot
338	Scraper	Good Bot
342	Scraper	Good Bot
343	Scraper	Good Bot
344	Scraper	Good Bot
351	Scraper	Good Bot
352	Scraper	Good Bot
353	Scraper	Good Bot
355	Scraper	Good Bot
357	Scraper	Good Bot
360	Scraper	Good Bot
362	Scraper	Good Bot
366	Scraper	Good Bot
370	Scraper	Good Bot
371	Scraper	Good Bot
392	Scraper	Good Bot
393	Scraper	Good Bot

Bot-Signaturregel	ID	Beschreibung
394	Scraper	Good Bot
396	Scraper	Good Bot
397	Scraper	Good Bot
414	Scraper	Good Bot
418	Scraper	Good Bot
419	Scraper	Good Bot
421	Scraper	Good Bot
422	Scraper	Good Bot
423	Scraper	Good Bot
424	Scraper	Good Bot
425	Scraper	Good Bot
426	Scraper	Good Bot
427	Scraper	Good Bot
428	Scraper	Good Bot
430	Scraper	Good Bot
432	Scraper	Good Bot
433	Scraper	Good Bot
434	Scraper	Good Bot
435	Scraper	Good Bot
441	Scraper	Good Bot
445	Scraper	Good Bot
446	Scraper	Good Bot
451	Scraper	Good Bot
452	Scraper	Good Bot
454	Scraper	Good Bot
455	Scraper	Good Bot
456	Scraper	Good Bot
457	Scraper	Good Bot
458	Scraper	Good Bot

Bot-Signaturregel	ID	Beschreibung
461	Scraper	Good Bot
465	Scraper	Good Bot
466	Scraper	Good Bot
469	Scraper	Good Bot
473	Scraper	Good Bot
474	Scraper	Good Bot
476	Scraper	Good Bot
477	Scraper	Good Bot
484	Scraper	Good Bot
485	Scraper	Good Bot
487	Scraper	Good Bot
488	Scraper	Good Bot
489	Scraper	Good Bot
490	Scraper	Good Bot
493	Scraper	Good Bot
494	Scraper	Good Bot
495	Scraper	Good Bot
497	Scraper	Good Bot
498	Scraper	Good Bot
499	Scraper	Good Bot
500	Scraper	Good Bot
505	Scraper	Good Bot
506	Scraper	Good Bot
507	Scraper	Good Bot
512	Scraper	Good Bot
513	Scraper	Good Bot
514	Scraper	Good Bot
527	Scraper	Good Bot
533	Scraper	Good Bot

Bot-Signaturregel	ID	Beschreibung
539	Scraper	Good Bot
540	Scraper	Good Bot
542	Scraper	Good Bot
544	Scraper	Good Bot
545	Scraper	Good Bot
546	Scraper	Good Bot
547	Scraper	Good Bot
548	Scraper	Good Bot
551	Scraper	Good Bot
552	Scraper	Good Bot
554	Scraper	Good Bot
556	Scraper	Good Bot
558	Scraper	Good Bot
560	Scraper	Good Bot
561	Scraper	Good Bot
566	Scraper	Good Bot
575	Scraper	Good Bot
578	Scraper	Good Bot
581	Scraper	Good Bot
582	Scraper	Good Bot
591	Scraper	Good Bot
593	Scraper	Good Bot
595	Scraper	Good Bot
600	Scraper	Good Bot
601	Scraper	Good Bot
602	Scraper	Good Bot
604	Scraper	Good Bot
605	Scraper	Good Bot
609	Scraper	Good Bot

Bot-Signaturregel	ID	Beschreibung
610	Scraper	Good Bot
611	Scraper	Good Bot
612	Scraper	Good Bot
613	Scraper	Good Bot
615	Scraper	Good Bot
620	Suchmaschine	Good Bot
622	Suchmaschine	Good Bot
623	Suchmaschine	Good Bot
624	Suchmaschine	Good Bot
626	Suchmaschine	Good Bot
627	Suchmaschine	Good Bot
628	Suchmaschine	Good Bot
629	Suchmaschine	Good Bot
633	Suchmaschine	Good Bot
634	Suchmaschine	Good Bot
636	Suchmaschine	Good Bot
637	Suchmaschine	Good Bot
640	Suchmaschine	Good Bot
641	Suchmaschine	Good Bot
642	Suchmaschine	Good Bot
643	Suchmaschine	Good Bot
647	Suchmaschine	Good Bot
649	Suchmaschine	Good Bot
650	Suchmaschine	Good Bot
651	Suchmaschine	Good Bot
654	Suchmaschine	Good Bot
656	Suchmaschine	Good Bot
657	Suchmaschine	Good Bot
658	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
659	Suchmaschine	Good Bot
660	Suchmaschine	Good Bot
663	Suchmaschine	Good Bot
664	Suchmaschine	Good Bot
665	Suchmaschine	Good Bot
666	Suchmaschine	Good Bot
667	Suchmaschine	Good Bot
669	Suchmaschine	Good Bot
670	Suchmaschine	Good Bot
671	Suchmaschine	Good Bot
672	Suchmaschine	Good Bot
673	Suchmaschine	Good Bot
674	Suchmaschine	Good Bot
675	Suchmaschine	Good Bot
676	Suchmaschine	Good Bot
677	Suchmaschine	Good Bot
679	Suchmaschine	Good Bot
680	Suchmaschine	Good Bot
690	Suchmaschine	Good Bot
693	Suchmaschine	Good Bot
694	Suchmaschine	Good Bot
697	Suchmaschine	Good Bot
698	Suchmaschine	Good Bot
702	Suchmaschine	Good Bot
706	Suchmaschine	Good Bot
712	Suchmaschine	Good Bot
713	Suchmaschine	Good Bot
714	Suchmaschine	Good Bot
715	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
716	Suchmaschine	Good Bot
721	Suchmaschine	Good Bot
723	Suchmaschine	Good Bot
725	Suchmaschine	Good Bot
727	Suchmaschine	Good Bot
728	Suchmaschine	Good Bot
729	Suchmaschine	Good Bot
730	Suchmaschine	Good Bot
731	Suchmaschine	Good Bot
732	Suchmaschine	Good Bot
735	Suchmaschine	Good Bot
736	Suchmaschine	Good Bot
740	Suchmaschine	Good Bot
748	Suchmaschine	Good Bot
749	Suchmaschine	Good Bot
750	Suchmaschine	Good Bot
751	Suchmaschine	Good Bot
756	Suchmaschine	Good Bot
757	Suchmaschine	Good Bot
758	Suchmaschine	Good Bot
759	Suchmaschine	Good Bot
760	Suchmaschine	Good Bot
761	Suchmaschine	Good Bot
762	Suchmaschine	Good Bot
763	Suchmaschine	Good Bot
764	Suchmaschine	Good Bot
765	Suchmaschine	Good Bot
766	Suchmaschine	Good Bot
767	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
768	Suchmaschine	Good Bot
769	Suchmaschine	Good Bot
770	Suchmaschine	Good Bot
771	Suchmaschine	Good Bot
772	Suchmaschine	Good Bot
773	Suchmaschine	Good Bot
776	Suchmaschine	Good Bot
777	Suchmaschine	Good Bot
780	Suchmaschine	Good Bot
781	Suchmaschine	Good Bot
784	Suchmaschine	Good Bot
786	Suchmaschine	Good Bot
787	Suchmaschine	Good Bot
788	Suchmaschine	Good Bot
789	Suchmaschine	Good Bot
790	Suchmaschine	Good Bot
791	Suchmaschine	Good Bot
792	Suchmaschine	Good Bot
795	Suchmaschine	Good Bot
796	Suchmaschine	Good Bot
798	Suchmaschine	Good Bot
800	Suchmaschine	Good Bot
801	Suchmaschine	Good Bot
802	Suchmaschine	Good Bot
803	Suchmaschine	Good Bot
805	Suchmaschine	Good Bot
806	Suchmaschine	Good Bot
807	Suchmaschine	Good Bot
809	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
810	Suchmaschine	Good Bot
811	Suchmaschine	Good Bot
812	Suchmaschine	Good Bot
814	Suchmaschine	Good Bot
815	Suchmaschine	Good Bot
816	Suchmaschine	Good Bot
817	Suchmaschine	Good Bot
818	Suchmaschine	Good Bot
819	Suchmaschine	Good Bot
820	Suchmaschine	Good Bot
821	Suchmaschine	Good Bot
822	Suchmaschine	Good Bot
823	Suchmaschine	Good Bot
825	Suchmaschine	Good Bot
827	Suchmaschine	Good Bot
830	Suchmaschine	Good Bot
831	Suchmaschine	Good Bot
834	Suchmaschine	Good Bot
837	Suchmaschine	Good Bot
838	Suchmaschine	Good Bot
849	Sitemonitor	Good Bot
850	Sitemonitor	Good Bot
851	Sitemonitor	Good Bot
853	Sitemonitor	Good Bot
857	Sitemonitor	Good Bot
858	Sitemonitor	Good Bot
859	Sitemonitor	Good Bot
860	Sitemonitor	Good Bot
861	Sitemonitor	Good Bot

Bot-Signaturregel	ID	Beschreibung
862	Sitemonitor	Good Bot
863	Sitemonitor	Good Bot
864	Sitemonitor	Good Bot
865	Sitemonitor	Good Bot
866	Sitemonitor	Good Bot
867	Sitemonitor	Good Bot
868	Sitemonitor	Good Bot
869	Sitemonitor	Good Bot
870	Sitemonitor	Good Bot
871	Sitemonitor	Good Bot
872	Sitemonitor	Good Bot
873	Sitemonitor	Good Bot
874	Sitemonitor	Good Bot
875	Sitemonitor	Good Bot
876	Sitemonitor	Good Bot
877	Sitemonitor	Good Bot
880	Sitemonitor	Good Bot
881	Sitemonitor	Good Bot
883	Sitemonitor	Good Bot
885	Sitemonitor	Good Bot
886	Sitemonitor	Good Bot
888	Sitemonitor	Good Bot
889	Sitemonitor	Good Bot
895	Sitemonitor	Good Bot
896	Sitemonitor	Good Bot
897	Sitemonitor	Good Bot
898	Sitemonitor	Good Bot
900	Sitemonitor	Good Bot
901	Sitemonitor	Good Bot

Bot-Signaturregel	ID	Beschreibung
904	Sitemonitor	Good Bot
906	Sitemonitor	Good Bot
908	Sitemonitor	Good Bot
909	Sitemonitor	Good Bot
910	Sitemonitor	Good Bot
911	Sitemonitor	Good Bot
912	Sitemonitor	Good Bot
913	Sitemonitor	Good Bot
917	Sitemonitor	Good Bot
918	Sitemonitor	Good Bot
919	Sitemonitor	Good Bot
920	Sitemonitor	Good Bot
921	Sitemonitor	Good Bot
924	Sitemonitor	Good Bot
926	Sitemonitor	Good Bot
927	Sitemonitor	Good Bot
928	Sitemonitor	Good Bot
929	Sitemonitor	Good Bot
930	Sitemonitor	Good Bot
931	Sitemonitor	Good Bot
934	Sitemonitor	Good Bot
938	Sitemonitor	Good Bot
939	Sitemonitor	Good Bot
958	Sitemonitor	Good Bot
959	Sitemonitor	Good Bot
960	Sitemonitor	Good Bot
963	Sitemonitor	Good Bot
984	Scraper	Good Bot
991	Scraper	Bad Bot

Bot-Signaturregel	ID	Beschreibung
996	Scraper	Good Bot
997	Scraper	Good Bot
998	Scraper	Good Bot
1002	Scraper	Good Bot
1006	Scraper	Good Bot
1622	Screenshot Creator	Good Bot
2810	Crawler	Good Bot
3432	Nicht kategorisiert	Bad Bot
3783	Suchmaschine	Good Bot
3784	Scraper	Bad Bot
3788	Tool	Good Bot
3790	Crawler	Good Bot
3791	Geschwindigkeitstester	Good Bot
3792	Tool	Good Bot
3793	Tool	Good Bot
3794	Crawler	Good Bot
3796	Scraper	Good Bot
3797	Marketing	Good Bot
3799	Marketing	Good Bot
3800	Marketing	Good Bot
3806	Tool	Good Bot
3807	Crawler	Good Bot
3808	Crawler	Good Bot
3809	Tool	Good Bot
3810	Scraper	Good Bot
3811	Tool	Good Bot
3812	Crawler	Good Bot
3813	Tool	Good Bot
3814	Crawler	Good Bot

Bot-Signaturregel	ID	Beschreibung
3815	Nicht kategorisiert	Good Bot
3817	Tool	Good Bot
3818	Tool	Good Bot
3819	Tool	Good Bot
3820	Crawler	Good Bot
3821	Suchmaschine	Good Bot
3822	Marketing	Good Bot
3823	Nicht kategorisiert	Good Bot
3831	Scraper	Good Bot
3833	Suchmaschine	Good Bot
3834	Suchmaschine	Good Bot
3835	Suchmaschine	Good Bot
3836	Nicht kategorisiert	Good Bot
3838	Nicht kategorisiert	Good Bot
3839	Marketing	Good Bot
3840	Crawler	Good Bot
3842	Crawler	Good Bot
3843	Crawler	Good Bot
3844	Marketing	Good Bot
3845	Marketing	Good Bot
3846	Marketing	Good Bot
3847	Marketing	Good Bot
3848	Nicht kategorisiert	Good Bot
3849	Crawler	Good Bot
3850	Tool	Good Bot
3851	Nicht kategorisiert	Good Bot
3852	Tool	Good Bot
3853	Vulnerability Scanner	Good Bot
3854	Crawler	Good Bot

Bot-Signaturregel	ID	Beschreibung
3855	Crawler	Good Bot
3856	Tool	Good Bot
3871	Marketing	Good Bot
3886	Tool	Good Bot
3887	Crawler	Good Bot
3888	Crawler	Good Bot
3889	Nicht kategorisiert	Good Bot
3890	Marketing	Good Bot
3893	Crawler	Good Bot
3894	Tool	Good Bot
3895	Tool	Good Bot
3896	Suchmaschine	Good Bot
3897	Tool	Good Bot
3898	Tool	Good Bot
3899	Nicht kategorisiert	Good Bot
3901	Crawler	Good Bot
3902	Tool	Good Bot
3903	Tool	Good Bot
3904	Suchmaschine	Good Bot
3905	Suchmaschine	Good Bot
3906	Suchmaschine	Good Bot
3907	Suchmaschine	Good Bot
3912	Crawler	Good Bot
3917	Nicht kategorisiert	Good Bot
3918	Crawler	Good Bot
3919	Nicht kategorisiert	Good Bot
3920	Nicht kategorisiert	Good Bot
3921	Nicht kategorisiert	Good Bot
3922	Nicht kategorisiert	Good Bot

Bot-Signaturregel	ID	Beschreibung
3923	Nicht kategorisiert	Good Bot
3924	Nicht kategorisiert	Good Bot
3925	Nicht kategorisiert	Good Bot
3926	Marketing	Good Bot
3927	Marketing	Good Bot
3928	Marketing	Good Bot
3929	Tool	Good Bot
3930	Marketing	Good Bot
3931	Nicht kategorisiert	Good Bot
3932	Crawler	Good Bot
3933	Marketing	Good Bot
3934	Marketing	Good Bot
3935	Scraper	Good Bot
3936	Marketing	Good Bot
3937	Scraper	Good Bot
3938	Feed Fetcher	Good Bot
3940	Suchmaschine	Good Bot
3941	Crawler	Good Bot
3942	Scraper	Good Bot
3946	Feed Fetcher	Good Bot
3947	Crawler	Good Bot
3950	Viren-Scanner	Good Bot
3951	Marketing	Good Bot
3952	Marketing	Good Bot
3953	Marketing	Good Bot
3954	Marketing	Good Bot
3955	Marketing	Good Bot
3956	Marketing	Good Bot
3957	Marketing	Good Bot

Bot-Signaturregel	ID	Beschreibung
3958	Marketing	Good Bot
3959	Marketing	Good Bot
3960	Marketing	Good Bot
3961	Marketing	Good Bot
3962	Marketing	Good Bot
3963	Marketing	Good Bot
3964	Marketing	Good Bot
3965	Marketing	Good Bot
3966	Marketing	Good Bot
3967	Marketing	Good Bot
3968	Marketing	Good Bot
3969	Marketing	Good Bot
3970	Suchmaschine	Good Bot
3971	Screenshot Creator	Good Bot
3972	Screenshot Creator	Good Bot
3973	Suchmaschine	Good Bot
3974	Suchmaschine	Good Bot
3975	Suchmaschine	Good Bot
3976	Suchmaschine	Good Bot
3977	Suchmaschine	Good Bot
3978	Screenshot Creator	Good Bot
3979	Suchmaschine	Good Bot
3980	Screenshot Creator	Good Bot
3981	Suchmaschine	Good Bot
3982	Suchmaschine	Good Bot
3983	Suchmaschine	Good Bot
3984	Suchmaschine	Good Bot
3985	Suchmaschine	Good Bot
3986	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
3987	Screenshot Creator	Good Bot
3988	Suchmaschine	Good Bot
3989	Suchmaschine	Good Bot
3990	Suchmaschine	Good Bot
3991	Suchmaschine	Good Bot
3992	Suchmaschine	Good Bot
3993	Suchmaschine	Good Bot
3994	Suchmaschine	Good Bot
3995	Suchmaschine	Good Bot
3996	Suchmaschine	Good Bot
3997	Suchmaschine	Good Bot
3998	Suchmaschine	Good Bot
3999	Suchmaschine	Good Bot
4000	Screenshot Creator	Good Bot
4001	Suchmaschine	Good Bot
4002	Suchmaschine	Good Bot
4003	Suchmaschine	Good Bot
4004	Suchmaschine	Good Bot
4005	Screenshot Creator	Good Bot
4006	Crawler	Good Bot
4007	Marketing	Good Bot
4008	Marketing	Good Bot
4011	Tool	Good Bot
4012	Crawler	Good Bot
4013	Suchmaschine	Good Bot
4014	Tool	Good Bot
4015	Crawler	Good Bot
4016	Crawler	Good Bot
4017	Tool	Good Bot

Bot-Signaturregel	ID	Beschreibung
4018	Tool	Good Bot
4019	Tool	Good Bot
4020	Tool	Good Bot
4021	Marketing	Good Bot
4024	Tool	Good Bot
4025	Suchmaschine	Good Bot
4026	Suchmaschine	Good Bot
4027	Suchmaschine	Good Bot
4028	Marketing	Good Bot
4029	Tool	Good Bot
4030	Scraper	Good Bot
4031	Scraper	Good Bot
4033	Crawler	Good Bot
4034	Crawler	Good Bot
4035	Marketing	Good Bot
4036	Vulnerability Scanner	Good Bot
4037	Vulnerability Scanner	Good Bot
4038	Nicht kategorisiert	Bad Bot
4039	Tool	Good Bot
4042	Crawler	Good Bot
4043	Screenshot Creator	Good Bot
4048	Feed Fetcher	Good Bot
4050	Crawler	Good Bot
4051	Crawler	Good Bot
4052	Tool	Good Bot
4053	Tool	Good Bot
4055	Nicht kategorisiert	Good Bot
4056	Marketing	Good Bot
4057	Screenshot Creator	Good Bot

Bot-Signaturregel	ID	Beschreibung
4058	Crawler	Good Bot
4060	Suchmaschine	Good Bot
4061	Suchmaschine	Good Bot
4062	Suchmaschine	Good Bot
4063	Suchmaschine	Good Bot
4064	Tool	Good Bot
4065	Scraper	Good Bot
4066	Marketing	Good Bot
4067	Marketing	Good Bot
4071	Tool	Good Bot
4076	Marketing	Good Bot
4077	Scraper	Good Bot
4078	Crawler	Good Bot
4079	Crawler	Good Bot
4081	Suchmaschine	Good Bot
4082	Tool	Good Bot
4085	Tool	Good Bot
4086	Tool	Good Bot
4087	Tool	Bad Bot
4088	Suchmaschine	Good Bot
4089	Marketing	Good Bot
4090	Tool	Good Bot
4091	Tool	Good Bot
4092	Tool	Good Bot
4093	Tool	Good Bot
4094	Nicht kategorisiert	Good Bot
4095	Sitemonitor	Good Bot
4096	Sitemonitor	Good Bot
4097	Sitemonitor	Good Bot

Bot-Signaturregel	ID	Beschreibung
4098	Crawler	Good Bot
4099	Suchmaschine	Good Bot
4100	Suchmaschine	Good Bot
4101	Suchmaschine	Good Bot
4102	Suchmaschine	Good Bot
4103	Marketing	Good Bot
4104	Marketing	Good Bot
4105	Marketing	Good Bot
4106	Marketing	Good Bot
4109	Suchmaschine	Good Bot
4110	Crawler	Good Bot
4111	Crawler	Good Bot
4112	Crawler	Good Bot
4113	Vulnerability Scanner	Good Bot
4114	Crawler	Good Bot
4115	Tool	Good Bot
4121	Marketing	Good Bot
4126	Marketing	Good Bot
4127	Marketing	Good Bot
4128	Marketing	Good Bot
4129	Marketing	Good Bot
4130	Marketing	Good Bot
4131	Tool	Good Bot
4132	Marketing	Good Bot
4165	Marketing	Good Bot
4168	Geschwindigkeitstester	Good Bot
4170	Tool	Good Bot
4172	Crawler	Good Bot
4173	Tool	Good Bot

Bot-Signaturregel	ID	Beschreibung
4174	Crawler	Good Bot
4175	Crawler	Good Bot
4176	Tool	Good Bot
4177	Suchmaschine	Good Bot
4178	Tool	Good Bot
4179	Crawler	Good Bot
4180	Tool	Good Bot
4181	Sitemonitor	Good Bot
4182	Sitemonitor	Good Bot
4183	Sitemonitor	Good Bot
4184	Sitemonitor	Good Bot
4185	Suchmaschine	Good Bot
4186	Tool	Good Bot
4187	Tool	Good Bot
4188	Screenshot Creator	Good Bot
4189	Marketing	Good Bot
4190	Suchmaschine	Good Bot
4191	Suchmaschine	Good Bot
4192	Suchmaschine	Good Bot
4193	Suchmaschine	Good Bot
4194	Tool	Good Bot
4196	Tool	Good Bot
4197	Tool	Good Bot
4198	Marketing	Good Bot
4199	Marketing	Good Bot
4200	Vulnerability Scanner	Good Bot
4201	Tool	Good Bot
4202	Tool	Good Bot
4205	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
4209	Suchmaschine	Good Bot
4210	Geschwindigkeitstester	Good Bot
4211	Tool	Good Bot
4212	Feed Fetcher	Good Bot
4213	Feed Fetcher	Good Bot
4215	Tool	Good Bot
4216	Tool	Good Bot
4219	Marketing	Good Bot
4220	Tool	Good Bot
4222	Sitemonitor	Good Bot
4223	Marketing	Good Bot
4224	Suchmaschine	Good Bot
4225	Suchmaschine	Good Bot
4226	Suchmaschine	Good Bot
4227	Marketing	Good Bot
4228	Marketing	Good Bot
4229	Tool	Good Bot
4231	Screenshot Creator	Good Bot
4232	Tool	Good Bot
4233	Sitemonitor	Good Bot
4236	Sitemonitor	Good Bot
4242	Marketing	Good Bot
4243	Marketing	Good Bot
4244	Marketing	Good Bot
4245	Marketing	Good Bot
4246	Marketing	Good Bot
4247	Suchmaschine	Good Bot
4252	Crawler	Good Bot
4253	Crawler	Good Bot

Bot-Signaturregel	ID	Beschreibung
4254	Crawler	Good Bot
4255	Tool	Good Bot
4256	Nicht kategorisiert	Good Bot
4257	Tool	Good Bot
4258	Crawler	Good Bot
4259	Crawler	Good Bot
4260	Tool	Good Bot
4261	Tool	Good Bot
4262	Tool	Good Bot
4263	Marketing	Good Bot
4265	Suchmaschine	Good Bot
4266	Nicht kategorisiert	Good Bot
4267	Tool	Good Bot
4268	Tool	Good Bot
4269	Suchmaschine	Good Bot
4270	Suchmaschine	Good Bot
4271	Suchmaschine	Good Bot
4272	Suchmaschine	Good Bot
4273	Suchmaschine	Good Bot
4274	Suchmaschine	Good Bot
4275	Suchmaschine	Good Bot
4279	Marketing	Good Bot
4280	Crawler	Good Bot
4321	Nicht kategorisiert	Good Bot
4322	Crawler	Good Bot
4323	Tool	Good Bot
4324	Tool	Good Bot
4325	Tool	Good Bot
4327	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
4328	Marketing	Good Bot
4330	Sitemonitor	Good Bot
4331	Suchmaschine	Good Bot
4334	Scraper	Good Bot
4335	Marketing	Good Bot
4336	Marketing	Good Bot
4339	Tool	Good Bot
4340	Crawler	Good Bot
4341	Crawler	Good Bot
4342	Vulnerability Scanner	Good Bot
4343	Vulnerability Scanner	Good Bot
4344	Scraper	Good Bot
4377	Crawler	Good Bot
4378	Crawler	Good Bot
4379	Suchmaschine	Good Bot
4380	Suchmaschine	Good Bot
4381	Suchmaschine	Good Bot
4382	Suchmaschine	Good Bot
4383	Crawler	Good Bot
4384	Suchmaschine	Good Bot
4385	Tool	Good Bot
4386	Nicht kategorisiert	Good Bot
4387	Crawler	Good Bot
4388	Crawler	Good Bot
4389	Tool	Good Bot
4390	Tool	Good Bot
4391	Tool	Good Bot
4392	Tool	Good Bot
4393	Tool	Good Bot

Bot-Signaturregel	ID	Beschreibung
4394	Nicht kategorisiert	Good Bot
4395	Tool	Good Bot
4396	Sitemonitor	Good Bot
4397	Sitemonitor	Good Bot
4404	Suchmaschine	Good Bot
4405	Suchmaschine	Good Bot
4406	Suchmaschine	Good Bot
4407	Nicht kategorisiert	Good Bot

Bot-Signatur-Update für März 2022

July 27, 2022

Neue Signaturen wurden hinzugefügt und einige der vorhandenen Bot-Signaturen wurden aktualisiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Bot-Angriffen zu schützen.

Bot-Signaturversion

Signaturversion 12 gilt für Citrix ADC-Plattformen mit 13.0 76.31 oder höheren Builds.

Neue Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signaturregel	ID	Beschreibung
4564	Marketing	Good Bot
4565	Marketing	Good Bot
4566	Marketing	Good Bot
4567	Marketing	Good Bot
4568	Marketing	Good Bot
4569	Nicht kategorisiert	Bad Bot

Bot-Signaturregel	ID	Beschreibung
4570	Nicht kategorisiert	Bad Bot
4571	Crawler	Good Bot
4572	Crawler	Good Bot
4573	Nicht kategorisiert	Bad Bot
4574	Nicht kategorisiert	Bad Bot
4575	Marketing	Good Bot
4576	Marketing	Good Bot
4577	Marketing	Good Bot
4578	Marketing	Good Bot
4579	Marketing	Good Bot
4580	Marketing	Good Bot
4581	Marketing	Good Bot
4582	Marketing	Good Bot
4583	Screenshot Creator	Good Bot
4584	Suchmaschine	Good Bot
4585	Suchmaschine	Good Bot
4586	Screenshot Creator	Good Bot
4587	Nicht kategorisiert	Good Bot
4588	Geschwindigkeitstester	Good Bot
4589	Crawler	Good Bot
4590	Tool	Good Bot
4591	Tool	Good Bot
4592	Crawler	Bad Bot
4593	Suchmaschine	Good Bot
4594	Suchmaschine	Good Bot
4595	Suchmaschine	Good Bot
4596	Marketing	Good Bot
4597	Tool	Good Bot
4598	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
4599	Marketing	Good Bot
4600	Marketing	Good Bot
4601	Marketing	Good Bot
4602	Suchmaschine	Good Bot
4603	Nicht kategorisiert	Good Bot
4604	Marketing	Good Bot
4605	Marketing	Good Bot
4606	Nicht kategorisiert	Bad Bot
4607	Nicht kategorisiert	Bad Bot
4608	Tool	Good Bot
4609	Nicht kategorisiert	Bad Bot
4610	Tool	Good Bot
4611	Tool	Good Bot
4612	Scraper	Good Bot
4613	Nicht kategorisiert	Good Bot
4614	Nicht kategorisiert	Good Bot
4615	Sitemonitor	Good Bot
4616	Crawler	Good Bot
4617	Sitemonitor	Good Bot
4618	Suchmaschine	Good Bot
4619	Marketing	Good Bot
4620	Marketing	Good Bot
4621	Suchmaschine	Good Bot
4622	Crawler	Good Bot
4623	Crawler	Good Bot
4624	Crawler	Good Bot
4625	Scraper	Good Bot
4626	Crawler	Good Bot
4627	Vulnerability Scanner	Good Bot

Bot-Signaturregel	ID	Beschreibung
4628	Tool	Good Bot
4629	Nicht kategorisiert	Bad Bot
4630	Nicht kategorisiert	Bad Bot
4631	Tool	Good Bot
4632	Feed Fetcher	Good Bot
4633	Crawler	Bad Bot
4634	Nicht kategorisiert	Good Bot
4635	Feed Fetcher	Good Bot
4636	Nicht kategorisiert	Good Bot
4637	Tool	Good Bot
4638	Tool	Good Bot
4639	Scraper	Bad Bot
4640	Nicht kategorisiert	Bad Bot
4641	Tool	Good Bot
4642	Crawler	Bad Bot
4643	Sitemonitor	Good Bot
4644	Sitemonitor	Good Bot
4645	Suchmaschine	Good Bot
4646	Suchmaschine	Good Bot
4647	Suchmaschine	Good Bot
4648	Suchmaschine	Good Bot
4649	Suchmaschine	Bad Bot
4650	Nicht kategorisiert	Good Bot

Aktualisierte Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signaturregel	ID	Beschreibung
2554	Nicht kategorisiert	Bad Bot

Bot-Signaturregel	ID	Beschreibung
3835	Suchmaschine	Good Bot
4027	Suchmaschine	Good Bot
4038	Nicht kategorisiert	Bad Bot
4085	Tool	Good Bot
4098	Crawler	Good Bot
4100	Suchmaschine	Good Bot
4220	Tool	Good Bot
4224	Suchmaschine	Good Bot
4281	Nicht kategorisiert	Bad Bot
4412	Marketing	Good Bot
4425	Marketing	Good Bot
4429	Screenshot Creator	Good Bot
4430	Viren-Scanner	Good Bot
4483	Crawler	Good Bot
4552	Nicht kategorisiert	Good Bot
4562	Suchmaschine	Good Bot
1000000	Browser	Good Bot
1000003	Browser	Good Bot
1000004	Scraper	Good Bot
1000005	Google_Crawler	Bad Bot
1000006	Browser	Bad Bot
1000007	Bot	Bad Bot
1000008	Browser	Bad Bot
1000009	Browser	Good Bot
1000010	Bot	Bad Bot
1000011	Browser	Bad Bot
1000012	Scraper	Good Bot
1000013	Scraper	Bad Bot
1000014	Scraper	Bad Bot

Bot-Signaturregel	ID	Beschreibung
1000015	Browser	Good Bot
1000016	Bot	Bad Bot
1000017	Browser	Bad Bot
1000018	Browser	Good Bot
1000019	Scraper	Good Bot
1000020	Scraper	Good Bot
1000021	Scraper	Good Bot
1000022	Google_Crawler	Good Bot
1000023	Browser	Bad Bot
1000024	Analysator	Good Bot
1000025	Analysator	Good Bot
1000026	Analysator	Good Bot
1000027	Analysator	Good Bot
1000028	Analysator	Good Bot
1000029	Browser	Good Bot
1000030	Analysator	Good Bot
1000031	Analysator	Good Bot
1000032	Browser	Bad Bot
1000033	Analysator	Good Bot
1000034	Browser	Bad Bot
1000035	Scraper	Good Bot
1000036	Scraper	Good Bot
1000037	Browser	Good Bot
1000038	Analysator	Good Bot
1000039	Analysator	Good Bot
1000040	Analysator	Good Bot
1000041	Analysator	Good Bot
1000042	Analysator	Good Bot
1000043	Analysator	Good Bot

Bot-Signaturregel	ID	Beschreibung
1000044	Analysator	Good Bot
1000045	Google_App_Engine_Software	Good Bot
1000046	Google_Crawler	Good Bot
1000047	Browser	Bad Bot
1000048	Browser	Bad Bot
1000049	Analysator	Good Bot
1000050	Browser	Bad Bot
1000051	Browser	Good Bot
1000052	Browser	Bad Bot
1000053	Scraper	Good Bot
1000054	Google_Crawler	Bad Bot
1000055	Scraper	Bad Bot
1000056	Analysator	Good Bot
1000057	Browser	Bad Bot
1000058	Browser	Bad Bot
1000059	Browser	Bad Bot
1000060	Scraper	Bad Bot
1000061	Anwendung	Bad Bot
1000062	Scraper	Bad Bot
1000063	Scraper	Bad Bot
1000064	Scraper	Good Bot
1000065	Scraper	Bad Bot
1000066	Scraper	Bad Bot
1000067	Browser	Bad Bot
1000068	Scraper	Bad Bot
1000069	Browser	Bad Bot
1000070	Scraper	Bad Bot
1000071	Anwendung	Bad Bot

Bot-Signatur-Update für August 2022

September 28, 2022

Neue Signaturen wurden hinzugefügt und einige der vorhandenen Bot-Signaturen wurden aktualisiert. Sie können diese Signaturregeln herunterladen und konfigurieren, um Ihre Appliance vor Bot-Angriffen zu schützen.

Bot-Signaturversion

Signaturversion 13 gilt für Citrix ADC-Plattformen mit 13.0 76.31 oder höheren Builds.

Neue Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signaturregel	ID	Beschreibung
4651	Marketing	Good Bot
4652	Nicht kategorisiert	Bad Bot
4653	Suchmaschine	Good Bot
4654	Tool	Good Bot
4655	Crawler	Good Bot
4656	Marketing	Good Bot
4657	Scraper	Good Bot
4658	Feed Fetcher	Good Bot
4659	Nicht kategorisiert	Bad Bot
4660	Tool	Good Bot
4661	Tool	Good Bot
4662	Nicht kategorisiert	Bad Bot
4663	Nicht kategorisiert	Bad Bot
4664	Marketing	Good Bot
4665	Nicht kategorisiert	Good Bot
4666	Nicht kategorisiert	Good Bot
4667	Feed Fetcher	Good Bot

Bot-Signaturregel	ID	Beschreibung
4668	Nicht kategorisiert	Good Bot
4669	Tool	Good Bot
4670	Tool	Good Bot
4671	Suchmaschine	Good Bot
4672	Tool	Good Bot
4673	Nicht kategorisiert	Good Bot
4674	Nicht kategorisiert	Good Bot
4675	Nicht kategorisiert	Good Bot
4676	Marketing	Good Bot
4677	Scraper	Good Bot
4678	Marketing	Good Bot
4679	Crawler	Bad Bot
4680	Nicht kategorisiert	Good Bot
4681	Nicht kategorisiert	Good Bot
4682	Sitemonitor	Good Bot
4683	Sitemonitor	Good Bot
4684	Suchmaschine	Good Bot
4685	Suchmaschine	Good Bot
4686	Suchmaschine	Good Bot
4687	Suchmaschine	Good Bot
4688	Suchmaschine	Good Bot
4689	Suchmaschine	Good Bot
4690	Suchmaschine	Good Bot
4691	Suchmaschine	Good Bot
4692	Suchmaschine	Good Bot
4693	Nicht kategorisiert	Good Bot
4694	Nicht kategorisiert	Bad Bot
4695	Crawler	Good Bot
4696	Crawler	Good Bot

Bot-Signaturregel	ID	Beschreibung
4697	Crawler	Good Bot
4698	Suchmaschine	Good Bot
4699	Suchmaschine	Good Bot
4700	Suchmaschine	Good Bot
4701	Tool	Bad Bot
4702	Nicht kategorisiert	Good Bot
4703	Tool	Good Bot
4704	Tool	Good Bot
4705	Crawler	Good Bot
4706	Sitemonitor	Good Bot
4707	Suchmaschine	Good Bot
4708	Tool	Good Bot
4709	Vulnerability Scanner	Good Bot
4710	Vulnerability Scanner	Good Bot
4711	Crawler	Good Bot
4712	Crawler	Good Bot
4713	Crawler	Good Bot
4714	Scraper	Good Bot
4715	Tool	Good Bot
4716	Tool	Good Bot
4717	Suchmaschine	Bad Bot
4718	Nicht kategorisiert	Good Bot
4719	Tool	Good Bot
4720	Marketing	Good Bot
4721	Marketing	Good Bot
4722	Suchmaschine	Good Bot
4723	Nicht kategorisiert	Bad Bot
4724	Tool	Good Bot
4725	Suchmaschine	Good Bot

Bot-Signaturregel	ID	Beschreibung
4726	Suchmaschine	Good Bot
4727	Tool	Good Bot
4728	Nicht kategorisiert	Bad Bot
4729	Sitemonitor	Good Bot
4730	Suchmaschine	Good Bot
4731	Suchmaschine	Good Bot
4732	Suchmaschine	Good Bot
4733	Suchmaschine	Good Bot
4734	Tool	Bad Bot
4735	Tool	Bad Bot
4736	Tool	Good Bot
4737	Marketing	Good Bot
4738	Tool	Good Bot
4739	Feed Fetcher	Good Bot
4740	Suchmaschine	Good Bot
4741	Nicht kategorisiert	Bad Bot
4742	Suchmaschine	Good Bot
4743	Crawler	Good Bot
4744	Tool	Good Bot
4745	Tool	Good Bot
4746	Marketing	Good Bot
4747	Nicht kategorisiert	Bad Bot
4748	Suchmaschine	Good Bot
4749	Suchmaschine	Good Bot
4750	Suchmaschine	Good Bot
4751	Suchmaschine	Good Bot
4752	Suchmaschine	Good Bot

Aktualisierte Bot-Signaturen

Es folgt eine Liste der Regel-IDs, der Kategorie und ihres Typs für Bot-Signaturregeln.

Bot-Signaturregel	ID	Beschreibung
3796	Scraper	Good Bot
3835	Suchmaschine	Good Bot
3935	Scraper	Good Bot
4027	Suchmaschine	Good Bot
4061	Suchmaschine	Good Bot
4100	Suchmaschine	Good Bot
4451	Geschwindigkeitstester	Good Bot
4562	Suchmaschine	Good Bot
4575	Marketing	Good Bot
4577	Marketing	Good Bot
4578	Marketing	Good Bot
4579	Marketing	Good Bot
4580	Marketing	Good Bot
4583	Screenshot Creator	Good Bot
4584	Suchmaschine	Good Bot
4585	Suchmaschine	Good Bot
4597	Tool	Good Bot
4599	Marketing	Good Bot
4601	Marketing	Good Bot
4623	Crawler	Good Bot
4630	Nicht kategorisiert	Bad Bot
4647	Suchmaschine	Good Bot
1000000	Browser	Good Bot
1000001	Anwendung	Bad Bot
1000002	Browser	Good Bot
1000003	Scraper	Good Bot
1000004	Browser	Good Bot

Bot-Signaturregel	ID	Beschreibung
1000005	Browser	Bad Bot
1000006	Google Crawler	Bad Bot
1000007	Scraper	Bad Bot
1000008	Scraper	Good Bot
1000009	Browser	Bad Bot
1000010	Bot	Bad Bot
1000011	Bot	Bad Bot
1000012	Scraper	Bad Bot
1000013	Scraper	Bad Bot
1000014	Browser	Bad Bot
1000015	Browser	Good Bot
1000016	Browser	Bad Bot
1000017	Scraper	Good Bot
1000018	Scraper	Bad Bot
1000019	Scraper	Bad Bot
1000020	Scraper	Bad Bot
1000021	Browser	Good Bot
1000022	Scraper	Good Bot
1000023	Browser	Bad Bot
1000024	Bot	Bad Bot
1000025	Analysator	Good Bot
1000026	Scraper	Good Bot
1000027	Browser	Bad Bot
1000028	Browser	Bad Bot
1000029	Scraper	Good Bot
1000030	Google Crawler	Good Bot
1000031	Browser	Bad Bot
1000032	Analysator	Good Bot
1000033	Bot	Bad Bot

Bot-Signaturregel	ID	Beschreibung
1000034	Analysator	Good Bot
1000035	Analysator	Good Bot
1000036	Analysator	Good Bot
1000037	Analysator	Good Bot
1000038	Scraper	Good Bot
1000039	Analysator	Good Bot
1000040	Browser	Bad Bot
1000041	Browser	Bad Bot
1000042	Scraper	Good Bot
1000043	Browser	Good Bot
1000044	Analysator	Good Bot
1000045	Analysator	Good Bot
1000046	Analysator	Good Bot
1000047	Analysator	Good Bot
1000048	Analysator	Good Bot
1000049	Browser	Bad Bot
1000050	Google Crawler	Good Bot
1000051	Browser	Bad Bot
1000052	Browser	Bad Bot
1000053	Analysator	Good Bot
1000054	Browser	Good Bot
1000055	Scraper	Good Bot
1000056	Browser	Good Bot
1000057	Analysator	Good Bot
1000058	Google Crawler	Bad Bot
1000059	Scraper	Bad Bot
1000060	Browser	Bad Bot
1000061	Browser	Good Bot
1000062	Browser	Bad Bot

Bot-Signaturregel	ID	Beschreibung
1000063	Browser	Bad Bot
1000064	Browser	Bad Bot
1000065	Scraper	Bad Bot
1000066	Anwendung	Bad Bot
1000067	Scraper	Bad Bot
1000068	Scraper	Bad Bot
1000069	Browser	Good Bot
1000070	Anwendung	Bad Bot

Cacheumleitung

October 5, 2021

Bei einer typischen Bereitstellung fragen verschiedene Clients immer wieder Webserver nach demselben Inhalt. Um den Ursprungswebserver bei der Verarbeitung jeder Anforderung zu entlasten, kann eine Citrix ADC Appliance mit aktivierter Cache-Umleitung diesen Inhalt von einem Cacheserver anstelle vom Ursprungsserver bereitstellen.

Die Citrix ADC Appliance analysiert eingehende Anforderungen, sendet Anforderungen für zwischenspeicherbare Daten an Cacheserver und sendet nicht zwischenspeicherbare Anforderungen und dynamische HTTP-Anforderungen an Ursprungsserver.

Die Cache-Umleitung ist ein richtlinienbasiertes Feature. Standardmäßig werden Anforderungen, die einer Richtlinie entsprechen, an den Ursprungsserver gesendet, und alle anderen Anforderungen werden an einen Cacheserver gesendet. Zum Testen oder Wartungsarbeiten möchten Sie möglicherweise die Richtlinienbewertung überspringen und alle Anforderungen an den Cache oder an den Ursprungsserver weiterleiten.

Sie können Content Switching mit Cache-Umleitung kombinieren, um selektive Inhalte zwischenzuspeichern und Inhalte von bestimmten Cacheservern für bestimmte Arten von angeforderten Inhalten bereitzustellen.

Eine Citrix ADC Appliance, die für die Cacheumleitung konfiguriert ist, kann am Rand eines Netzwerks, vor dem Ursprungsserver oder an einem beliebigen Ort entlang des Netzwerkbackbones bereitgestellt werden. In einer Edge-Bereitstellung, die häufig von Internetdienstanbietern (ISPs), Kabelunternehmen, Content-Delivery Distributionsnetzwerken und Unternehmensnetzwerken

verwendet wird, befindet sich die Citrix ADC Appliance direkt vor den Clients. In einer serverseitigen Bereitstellung ist die Citrix ADC Appliance näher an den Ursprungsservern.

Die Cache-Umleitung wird am häufigsten mit dem HTTP-Diensttyp verwendet, unterstützt aber auch das sichere HTTPS-Protokoll.

Cache-Umleitungsrichtlinien

October 5, 2021

Ein virtueller Server zur Cache-Umleitung wendet Cache-Umleitungsrichtlinien auf jede eingehende Anforderung an. Wenn eine Anforderung mit einer der konfigurierten Richtlinien übereinstimmt, gilt sie standardmäßig als nicht zwischenspeicherbar, und die Citrix ADC Appliance sendet sie an den Ursprungsserver. Andere Anforderungen werden an einen Cacheserver gesendet. Dieses Verhalten kann umgekehrt werden, so dass Anforderungen, die mit konfigurierten Cache-Umleitungsrichtlinien übereinstimmen, an Cacheserver gesendet werden.

Die Appliance stellt eine Reihe von Richtlinien für die Cache-Umleitung bereit. Wenn diese integrierten Richtlinien für die Bereitstellung nicht ausreichend sind, können Sie benutzerdefinierte Cache-Umleitungsrichtlinien konfigurieren.

Hinweis: Wenn Sie ermittelt haben, welche integrierten Cache-Umleitungsrichtlinien verwendet werden sollen, oder benutzerdefinierte Richtlinien erstellt haben, fahren Sie mit der Konfiguration der Cache-Umleitung fort. Um dieses Feature verwenden zu können, müssen Sie mindestens einen virtuellen Cache-Umleitungsserver konfigurieren, und für den normalen Betrieb müssen Sie mindestens eine Cache-Umleitungsrichtlinie an diesen virtuellen Server binden.

Integrierte Cache-Umleitungsrichtlinien

October 5, 2021

Die Citrix ADC Appliance bietet integrierte Cache-Umleitungsrichtlinien, die typische Cache-Anforderungen verarbeiten. Diese Richtlinien basieren auf HTTP-Methoden, den URL- oder URL-Tokens der eingehenden Anforderung, der HTTP-Version oder den HTTP-Headern und ihren Werten in der Anforderung.

Integrierte Cache-Umleitungsrichtlinien können direkt an einen virtuellen Server gebunden werden und benötigen keine weitere Konfiguration.

Cache-Umleitungsrichtlinien verwenden zwei Arten von Appliance-Ausdruckssprachen, die klassische und die Standardsyntax. Weitere Informationen zu diesen Sprachen finden Sie unter Richtlinien

und Ausdrücke.

Integrierte Richtlinien zur klassischen Cache-Umleitung

Integrierte Cacheumleitungsrichtlinien, die auf klassischen Ausdrücken basieren, werden *klassische Cacheumleitungsrichtlinien*genannt. Eine vollständige Beschreibung klassischer Ausdrücke und deren Konfiguration finden Sie unter Richtlinien und Ausdrücke.

Die klassischen Cache-Umleitungsrichtlinien bewerten grundlegende Merkmale des Datenverkehrs und anderer Daten. Klassische Cache-Umleitungsrichtlinien können beispielsweise bestimmen, ob eine HTTP-Anforderung oder -Antwort einen bestimmten Header- oder URL-Typ enthält.

Die Citrix ADC Appliance bietet die folgenden integrierten Richtlinien für die klassische Cache-Umleitung:

Integrierter Richtlinienname	Beschreibung
Bypass-non-get	Umgehen Sie den Cache, wenn die Anforderung eine andere HTTP-Methode als GET verwendet.
Bypass-Cache-Kontrolle	Umgehen Sie den Cache, wenn der Request-Header einen Cache-Control: no-cache oder Cache-Control: no-store Header enthält oder wenn die HTTP-Anforderung einen Pragma-Header enthält.
Bypass-dynamic-url	Umgehen Sie den Cache, wenn die URL vorschlägt, dass der Inhalt dynamisch ist, wie durch das Vorhandensein einer der folgenden Erweiterungen angegeben: cgi, asp, exe, cfm, ex, shtml oder htx. Umgehen Sie auch den Cache, wenn die URL mit einer der folgenden Optionen beginnt: /cgi-bin/, /bin/ oder /exec/.
bypass-urltoken	Umgehen Sie den Cache, da die Anforderung dynamisch ist, wie durch eines der folgenden Token in der URL angegeben:? ,! oder =.
Bypass-Cookie	Umgehen Sie den Cache für jede URL mit einem Cookie-Header und einer anderen Erweiterung als GIF oder JPG.

Integrierte Standardsyntaxrichtlinien für die Cacheumleitung

Integrierte Cacheumleitungsrichtlinien, die auf Standard-Syntaxausdrücken basieren, werden als *Standardrichtlinien für die Syntaxcacheumleitung*bezeichnet. Eine vollständige Beschreibung der Standardsyntaxausdrücke und deren Konfiguration finden Sie unter Richtlinien und Ausdrücke.

Zusätzlich zu den gleichen Arten von Auswertungen, die von klassischen Cache-Umleitungsrichtlinien durchgeführt werden, ermöglichen Standardrichtlinien für die Syntaxcacheumleitung, weitere Daten zu analysieren (z. B. den Hauptteil einer HTTP-Anforderung) und weitere Vorgänge in der Richtlinienregel zu konfigurieren (z. B. Ursprungsserver).

Citrix ADC Appliances bieten die folgenden zwei integrierten Aktionen für die standardmäßigen Syntaxcache-Umleitungsrichtlinien:

- CACHE
- ORIGIN

Wie durch ihre Namen impliziert, leiten sie die Anforderung an den Cacheserver bzw. den Ursprungsserver.

Hinweis: Wenn Sie die integrierte Standard-Cache-Umleitungsrichtlinie für Syntax verwenden, können Sie die Aktion nicht ändern.

Die Citrix ADC Appliance bietet die folgenden integrierten Standardrichtlinien zur Syntaxcacheumleitung:

Integrierter Richtlinienname	Beschreibung
Bypass-non-get_adv	Umgehen Sie den Cache, wenn die Anforderung eine andere HTTP-Methode als GET verwendet.
Bypass-cache-control_adv	Umgehen Sie den Cache, wenn der Request-Header einen Cache-Control: no-cache oder Cache-Control: no-store Header enthält oder wenn die HTTP-Anforderung einen Pragma-Header enthält.
bypass-dynamic-url_adv	Umgehen Sie den Cache, wenn die URL vorschlägt, dass der Inhalt dynamisch ist, wie durch das Vorhandensein einer der folgenden Erweiterungen angegeben: cgi, asp, exe, cfm, ex, shtml oder htx. Umgehen Sie auch den Cache, wenn die URL mit einer der folgenden Optionen beginnt: /cgi-bin/, /bin/ oder /exec/.

Integrierter Richtlinienname	Beschreibung
bypass-urltokens_adv	Umgehen Sie den Cache, da die Anforderung dynamisch ist, wie durch eines der folgenden Token in der URL angegeben:? ,! oder =.
bypass-cookie_adv	Umgehen Sie den Cache für jede URL mit einem Cookie-Header und einer anderen Erweiterung als GIF oder JPG.

Anzeigen der integrierten Cache-Umleitungsrichtlinien

Sie können die verfügbaren Cache-Umleitungsrichtlinien über die Befehlszeilenschnittstelle oder das Konfigurationsdienstprogramm anzeigen.

Anzeigen der integrierten Cache-Umleitungsrichtlinien mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show cr policy [<policyName>]
```

Beispiel:

```
> show cr policy
1)       Cache-By-Pass RULE: NS_NON_GET          Policy:bypass-non-get
2)       Cache-By-Pass RULE: (NS_CACHECONTROL_NOSTORE ||
   NS_CACHECONTROL_NOCACHE || NS_HEADER_PRAGMA)    Policy:bypass-cache-
   control
3)       Cache-By-Pass RULE: (NS_EXT_CGI || NS_EXT_ASP || NS_EXT_EXE ||
    NS_EXT_CFM || NS_EXT_EX || NS_EXT_SHTML || NS_EXT_HTX) || (
   NS_URL_PATH_CGIBIN || NS_URL_PATH_EXEC || NS_URL_PATH_BIN)
   Policy:bypass-dynamic-url
4)       Cache-By-Pass RULE: NS_URL_TOKENS       Policy:bypass-
   urltokens
5)       Cache-By-Pass RULE: (NS_HEADER_COOKIE && NS_EXT_NOT_GIF &&
   NS_EXT_NOT_JPEG)     Policy:bypass-cookie
 Done
<!--NeedCopy-->
```


Anzeigen der integrierten Cache-Umleitungsrichtlinien mit der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Richtlinien. Die konfigurierten Cache-Umleitungsrichtlinien werden im Detailbereich angezeigt.
2. Wählen Sie eine der konfigurierten Richtlinien aus, um Details anzuzeigen.

Konfigurieren einer Cache-Umleitungsrichtlinie

October 5, 2021

Eine Cache-Umleitungsrichtlinie enthält einen oder mehrere Ausdrücke (auch als *Regeln* bezeichnet). Jeder Ausdruck stellt eine Bedingung dar, die ausgewertet wird, wenn die Clientanforderung mit der Richtlinie verglichen wird.

Aktionen für Cache-Umleitungsrichtlinien werden nicht explizit konfiguriert. Standardmäßig betrachtet die Citrix ADC Appliance alle Anforderungen, die einer Richtlinie entsprechen, als nicht zwischenspeicherbar und leitet die Anforderung an den Ursprungsserver anstelle des Cache weiter.

Cache-Umleitungsrichtlinien, die auf dem klassischen Richtlinienformat basieren, werden als *klassische Cache-Umleitungsrichtlinien*bezeichnet. Jede dieser Richtlinien hat einen Namen und enthält einen klassischen Ausdruck oder einen Satz klassischer Ausdrücke, die mithilfe von logischen Operatoren kombiniert werden.

Bei klassischen Cache-Umleitungsrichtlinien konfigurieren Sie nicht explizit Aktionen für die Richtlinien. Standardmäßig betrachtet die Citrix ADC Appliance alle Anforderungen, die einer Richtlinie entsprechen, als nicht zwischenspeicherbar und leitet die Anforderung an den Ursprungsserver anstelle des Cache weiter.

Cacheumleitungsrichtlinien, die auf dem neueren Richtlinienformat basieren, werden als *Erweiterte Umleitungsrichtlinien*bezeichnet. Diese Richtlinie hat einen Namen und enthält einen Standard-Syntaxausdruck oder einen Satz von Standard-Syntaxausdrücken, die mithilfe von logischen Operatoren kombiniert werden, und die folgenden integrierten Aktionen:

- CACHE
- ORIGIN

Weitere Informationen zu klassischen Ausdrücken und Standardsyntaxausdrücken finden Sie unter Richtlinien und Ausdrücke.

Hinzufügen einer Cache-Umleitungsrichtlinie mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Cache-Umleitungsrichtlinie hinzuzufügen und die Konfiguration zu überprüfen:


```
-  add cr policy <policyName> \*\*-rule\*\* <expression>
-  show cr policy [<policyName>]
<!--NeedCopy-->
```

Beispiele:

Richtlinie mit einem einfachen Ausdruck:

```
> add cr policy Policy-CRD-1 -rule ”REQ.HTTP.URL != /\*.jpeg”
 Done
> show cr policy Policy-CRD-1
         Cache-By-Pass RULE: REQ.HTTP.URL != '/\*.jpeg'   Policy:Policy
            -CRD-1
 Done
<!--NeedCopy-->
```

Richtlinie mit einem zusammengesetzten Ausdruck:

```
> add cr policy Policy-CRD-2 -rule ”REQ.HTTP.METHOD == POST && (REQ.
   HTTP.URL == /\*.cgi || REQ.HTTP.URL != /\*.png)”
 Done
> show cr policy Policy-CRD-2
         Cache-By-Pass RULE: REQ.HTTP.METHOD == POST && (REQ.HTTP.URL
            == '/\*.cgi' || REQ.HTTP.URL != '/\*.png')   Policy:Policy-
            CRD-2
 Done
<!--NeedCopy-->
```

Richtlinie, die einen Header auswertet:

```
> add cr policy Policy-CRD-3 -rule ”REQ.HTTP.HEADER If-Modified-Since
   EXISTS”
 Done
> show cr policy Policy-CRD-3
         Cache-By-Pass RULE: REQ.HTTP.HEADER If-Modified-Since EXISTS
               Policy:Policy-CRD-3
 Done
<!--NeedCopy-->
```


Hinzufügen einer standardmäßigen Syntaxcacheumleitungsrichtlinie mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Cache-Umleitungsrichtlinie hinzuzufügen und die Konfiguration zu überprüfen:

```
1 -  add cr policy <policyName> \*\*-rule\*\* <expression> [-action<
     string>] [-logAction<string>]
2 -  show cr policy [<policyName>]
3 <!--NeedCopy-->
```

Beispiele:

Richtlinie mit einem einfachen Ausdruck:

```
1 > add cr policy crpol1 -rule !(HTTP.REQ.URL.ENDSWITH(".jpeg" )) -action
      origin
2  Done
3 > show cr policy crpoll
4          Policy: crpol1 Rule: !(HTTP.REQ.URL.ENDSWITH(".jpeg")) Action:
               ORIGIN
5  Done
6 <!--NeedCopy-->
```

Richtlinie mit einem zusammengesetzten Ausdruck:

```
1 > add cr policy crpol11 -rule "http.req.method.eq(post) && (HTTP.REQ.
     URL.ENDSWITH(".png") || HTTP.REQ.URL.ENDSWITH(".cgi"))"  -action
     cache
2  Done
3 > show cr policy crpol11
4          Policy: crpol11    Rule: http.req.method.eq(post) && (HTTP.REQ
              .URL.ENDSWITH(".png") || HTTP.REQ.URL.ENDSWITH(".cgi"))
              Action: CACHE
5  Done
6 <!--NeedCopy-->
```

Richtlinie, die einen Header auswertet:

```
1 > add cr policy crpol12 -rule http.req.header("If-Modified-Since").
     exists -action origin
```



```
 Done
> show cr policy crpol12
         Policy: crpol12    Rule: http.req.header("If-Modified-Since").
            exists   Action: ORIGIN
 Done
<!--NeedCopy-->
```

Ändern oder Entfernen einer Cache-Umleitungsrichtlinie mit der CLI

- Um eine Cache-Umleitungsrichtlinie zu ändern, verwenden Sie den Befehl set cr policy, der genau wie der Befehl add cr policy entspricht, mit der Ausnahme, dass Sie den Namen einer vorhandenen Richtlinie eingeben.
- Um eine Richtlinie zu entfernen, verwenden Sie den`rm cr policy` Befehl, der nur das <name> Argument akzeptiert. Wenn die Richtlinie an einen virtuellen Server gebunden ist, müssen Sie die Bindung aufheben, bevor Sie sie entfernen können.

Weitere Informationen zum Aufheben der Bindung einer Cache-Umleitungsrichtlinie finden Sie unter Aufheben der Bindung einer Richtlinie von einem virtuellen Cache-Umleitungsserver.

Konfigurieren einer Cache-Umleitungsrichtlinie mit einem einfachen Ausdruck mit der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Richtlinien.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Cache-Umleitungsrichtlinie erstellen im Textfeld Name* den Namen der Richtlinie ein, und klicken Sie dann im Bereich Ausdruck auf Hinzufügen.
4. Um einen einfachen Ausdruck zu konfigurieren, geben Sie den Ausdruck ein. Es folgt ein Beispiel für einen Ausdruck, der nach einer JPEG-Erweiterung in einer URL sucht:

   - Ausdruckstype-Allgemein
   - Durchflussart -REQ
   - Protokoll -HTTP
   - Kennzeichner -URL
   - Betreiber -! =
   - Wert- /.jpeg

   Der einfache Ausdruck im folgenden Beispiel prüft auf einen If-Modified-Since Header in einer Anforderung:

   - Ausdruckstype-Allgemein
   - Durchflussart -REQ

- Protokoll -HTTP
- Qualifizierer -HEADER
- Operator -EXISTS
- Headername -If-Modified-Since

5. Wenn Sie die Eingabe des Ausdrucks abgeschlossen haben, klicken Sie auf OK oder Erstellen, und klicken Sie dann auf Schließen.

Konfigurieren einer Cache-Umleitungsrichtlinie mit einem zusammengesetzten Ausdruck mit der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Richtlinien.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Textfeld Name einen Namen für die Richtlinie ein.

   Der Name kann mit einem Buchstaben, einer Zahl oder dem Unterstrich beginnen und kann aus einem bis 127 Buchstaben, Zahlen und dem Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), at (@), Gleich (=) und Unterstrich (_) bestehen. Sie sollten einen Namen auswählen, der es anderen erleichtert, zu erkennen, welche Art von Inhalt diese Richtlinie erstellt hat.
4. Wählen Sie den Typ des zusammengesetzten Ausdrucks aus, den Sie erstellen möchten. Ihre Auswahlmöglichkeiten:

   - **Entsprechen Sie mit jedem Ausdruck**. Die Richtlinie entspricht dem Datenverkehr, wenn ein oder mehrere einzelne Ausdrücke mit dem Datenverkehr übereinstimmen.
   - **Entspricht allen Ausdrücken**. Die Richtlinie stimmt nur dann mit dem Datenverkehr überein, wenn jeder einzelne Ausdruck dem Datenverkehr entspricht.
   - **Tabellarische Ausdrücke**. Schaltet die Liste Ausdrücke in ein tabellarisches Format mit drei Spalten um. In der Spalte ganz rechts platzieren Sie einen der folgenden Operatoren:

     – Der Operator AND [&&], um dies zu verlangen, muss eine Anforderung zur Übereinstimmung mit der Richtlinie sowohl dem aktuellen Ausdruck als auch dem folgenden Ausdruck entsprechen.

Der Operator ODER [	], um zu verlangen, dass eine Anforderung, um der Richtlinie entsprechen zu können, entweder mit dem aktuellen Ausdruck oder dem folgenden Ausdruck oder beidem übereinstimmen muss. Nur wenn die Anforderung nicht mit einem Ausdruck übereinstimmt, stimmt sie nicht mit der Richtlinie überein.

–

Sie können Ausdrücke auch in verschachtelten Untergruppen gruppieren, indem Sie einen vorhandenen Ausdruck auswählen und auf einen der folgenden Operatoren klicken:

- Der Operator BEGIN SUBGROUP [+ ( ] der die Citrix ADC Appliance anweist, eine verschachtelte Untergruppe mit dem ausgewählten Ausdruck zu beginnen. (Um diesen Operator aus dem Ausdruck zu entfernen, klicken Sie auf - (.)
- Der Operator END SUBGROUP [+)], der die Citrix ADC Appliance anweist, die aktuell verschachtelte Untergruppe mit dem ausgewählten Ausdruck zu beenden. (Um diesen Operator aus dem Ausdruck zu entfernen, klicken Sie auf -).)

- **Fortgeschrittene Freiform**. Schaltet den Ausdruckseditor vollständig aus und verwandelt die Ausdrucksliste in einen Textbereich, in den Sie einen zusammengesetzten Ausdruck eingeben können. Dies ist sowohl die leistungsstärkste als auch die schwierigste Methode zum Erstellen eines Richtlinienausdrucks und wird nur für diejenigen empfohlen, die mit der klassischen Citrix ADC Ausdruckssprache vertraut sind.

  Weitere Informationen zum Erstellen klassischer Ausdrücke im Textbereich Erweiterte Freiform finden Sie unter Konfigurieren klassischer Richtlinien und Ausdrücke.

  Achtung: Wenn Sie in den Bearbeitungsmodus für erweiterte Freiformausdrücke wechseln, können Sie nicht zu einem der anderen Modi zurückkehren. Wählen Sie diesen Ausdruckbearbeitungsmodus nur aus, wenn Sie sicher sind, dass Sie ihn verwenden möchten.

5. Wenn Sie Beliebigen Ausdruck, Alle Ausdrücke abgleichen oder Tabellarische Ausdrücke gewählt haben, klicken Sie auf **Hinzufügen**, um das Dialogfeld Ausdruck hinzufügen anzuzeigen.

   Sie sollten den Ausdruckstyp für Cache-Umleitungsrichtlinien auf Allgemein festlegen.

6. Wählen Sie in der Dropdownliste Flow Type einen Flow Type für Ihren Ausdruck aus.

   Der Flow-Typ bestimmt, ob die Richtlinie eingehende oder ausgehende Verbindungen prüft. Sie haben zwei Möglichkeiten:

   - **REQ**. Konfiguriert die Citrix ADC Appliance, um eingehende Verbindungen oder Anforderungen zu untersuchen.
   - **RES**. Konfiguriert die Appliance so, dass ausgehende Verbindungen oder Antworten untersucht werden.

7. Wählen Sie in der Dropdownliste Protokoll ein Protokoll für Ihren Ausdruck aus.

   Das Protokoll bestimmt die Art von Informationen, die die Richtlinie in der Anforderung oder Antwort prüft. Je nachdem, ob Sie REQ oder RES in der vorherigen Dropdownliste ausgewählt haben, stehen entweder alle vier oder nur drei der folgenden Optionen zur Verfügung:

   - **HTTP** Konfiguriert die Appliance, um den HTTP-Header zu untersuchen.
   - **SSL**. Konfiguriert die Appliance für die Prüfung des SSL-Clientzertifikats. Nur verfügbar, wenn Sie REQ (Requests) in der vorherigen Dropdownliste ausgewählt haben.
   - **TCP**. Konfiguriert die Appliance, um den TCP-Header zu untersuchen.
   - **IP**. Konfiguriert die Appliance, um die Quell- oder Ziel-IP-Adresse zu untersuchen.

8. Wählen Sie in der Dropdownliste Qualifier einen Qualifier für Ihren Ausdruck aus.

   Der Inhalt der Dropdownliste Qualifier hängt davon ab, welches Protokoll Sie gewählt haben. In der folgenden Tabelle werden die verfügbaren Optionen für jedes Protokoll beschrieben.

   Tabelle 1. Cache-Umleitungsrichtlinien für jedes Protokoll verfügbar

Protokoll	Kennzeichner	Definition
HTTP	METHOD	HTTP-Methode, die in der Anforderung verwendet wird.
-	URL	Inhalt des URL-Headers.
-	URLTOKENS	URL-Token im HTTP-Header.
-	VERSION	HTTP-Version der Verbindung.
-	HEADER	Header-Teil der HTTP-Anforderung.
-	URLLEN	Länge des Inhalts des URL-Headers.
-	URLQUERY	Abfragen Teil des Inhalts des URL-Headers.

Protokoll	Kennzeichner	Definition
-	URLQUERYLEN	Länge des Abfrageabschnitts des URL-Headers.
SSL	CLIENT.CERT	SSL-Client-Zertifikat als Ganzes.
-	CLIENT.CERT.SUBJECT	Inhalt des Felds für das Clientzertifikat.
-	CLIENT.CERT.ISSUER	Client-Zertifikataussteller.
-	CLIENT.CERT.SIGALGO	Signaturalgorithmus, der im Clientzertifikat verwendet wird.
-	CLIENT.CERT.VERSION	Clientzertifikatversion.
-	CLIENT.CERT.VALIDFROM	Datum, ab dem das Clientzertifikat gültig ist. (Das Startdatum.)
-	CLIENT.CERT.VALIDTO	Datum, nach dem das Clientzertifikat nicht mehr gültig ist. (Das Enddatum.)
-	CLIENT.CERT.SERIALNUMBER	Seriennummer des Clientzertifikats.
-	CLIENT.CIPHER.TYPE	Verschlüsselungsmethode, die im Clientzertifikat verwendet wird.
-	CLIENT.CIPHER.BITS	Anzahl der signifikanten Bits im Verschlüsselungsschlüssel.
-	CLIENT.SSL.VERSION	SSL-Version des Clientzertifikats.
TCP	SOURCEPORT	Quellport der TCP-Verbindung.
-	DESTPORT	Zielport der TCP-Verbindung.
-	MSS	Maximale Segmentgröße (MSS) der TCP-Verbindung.
IP	SOURCEIP	Quell-IP-Adresse der Verbindung.

Protokoll	Kennzeichner	Definition
-	DESTIP	Ziel-IP-Adresse der Verbindung.

9. Wählen Sie den Operator für Ihren Ausdruck aus der Dropdownliste Operator aus.

   Ihre Auswahl hängt vom Qualifier ab, das Sie im vorherigen Schritt ausgewählt haben. Die vollständige Liste der Operatoren, die in dieser Dropdownliste angezeigt werden können, lautet:

   - == . Entspricht exakt der folgenden Textzeichenfolge.
   - != . Entspricht nicht der folgenden Textzeichenfolge.
     - . Ist größer als die folgende ganze Zahl.
   - CONTAINS. Enthält die folgende Textzeichenfolge.
   - CONTENTS. Der Inhalt der angegebenen Header-, URL- oder URL-Abfrage.
   - EXISTS. Der angegebene Header oder die angegebene Abfrage ist vorhanden.
   - NOTCONTAINS. Enthält nicht die folgende Textzeichenfolge.
   - NOTEXISTS. Der angegebene Header oder die angegebene Abfrage ist nicht vorhanden.

   Wenn diese Richtlinie für Anforderungen verwendet werden soll, die an einen bestimmten Host gesendet werden, können Sie das Standardzeichen, das Gleichheitszeichen (==), belassen.

10. Wenn das Textfeld Wert sichtbar ist, geben Sie die entsprechende Zeichenfolge oder Zahl in das Textfeld ein.

    Wenn diese Richtlinie beispielsweise Anforderungen auswählen soll, die an den Host shopping.example.com gesendet werden, geben Sie diese Zeichenfolge in das Textfeld Wert ein.

11. Wenn Sie HEADER als Kriterium gewählt haben, geben Sie die gewünschte Kopfzeile in das Textfeld Kopfzeilenname ein.
12. Klicken Sie auf OK, um den Ausdruck der Liste Ausdruck hinzuzufügen.
13. Wiederholen Sie die Schritte 4 bis 11, um zusätzliche Ausdrücke zu erstellen.
14. Klicken Sie auf Schließen, um das Dialogfeld Ausdruck hinzufügen zu schließen und zum Dialogfeld Cache-Umleitungsrichtlinie erstellen zurückzukehren.

Cache-Umleitungskonfigurationen

October 5, 2021

Je nach Bereitstellung und Netzwerktopologie können Sie einen der folgenden Cache-Umleitungstypen konfigurieren:

- **Transparent**. Ein transparenter Cache kann an verschiedenen Punkten entlang eines Netzwerkbackbones sein, um den Datenverkehr entlang der Zustellungsroute zu verringern. Im transparenten Modus fängt der virtuelle Cache-Umleitungsserver den gesamten Datenverkehr ab, der zur Citrix ADC Appliance fließt, und wendet Cache-Umleitungsrichtlinien an, um festzustellen, ob Inhalte aus dem Cache oder vom Ursprungsserver bereitgestellt werden sollen.
- **Proxy weiterleiten**. Ein Forward-Proxycacheserver befindet sich am Rand eines Unternehmens-LAN und steht mit Blick auf das WAN. Im Forward-Proxymodus löst der virtuelle Cache-Umleitungsserver den Hostnamen der eingehenden Anforderung mithilfe eines DNS-Servers auf und leitet Anforderungen für nicht zwischenspeicherbare Inhalte an die aufgelösten Ursprungsserver weiter. Cache-Anforderungen werden an die konfigurierten Cacheserver gesendet.
- **Reverse Proxy**. Reverse-Proxy-Caches werden für bestimmte Ursprungsserver konfiguriert. Eingehender Datenverkehr, der an den Reverse-Proxy geleitet wird, kann entweder von einem Cacheserver bedient werden oder mit oder ohne Änderung der URL an den Ursprungsserver gesendet werden.

Transparente Umleitung konfigurieren

October 5, 2021

Wenn Sie die transparente Cache-Umleitung konfigurieren, wertet die Citrix ADC Appliance den gesamten empfangenen Datenverkehr aus, um festzustellen, ob sie zwischengespeichert werden kann. Dieser Modus verringert den Datenverkehr entlang der Zustellungsroute und wird häufig verwendet, wenn der Cacheserver auf dem Backbone eines ISP oder Netzbetreibers ist.

Standardmäßig werden zwischenspeicherbare Anforderungen an einen Cacheserver und nicht zwischenspeicherbare Anforderungen an den Ursprungsserver gesendet. Wenn beispielsweise die Citrix ADC Appliance eine Anforderung empfängt, die an einen Webserver weitergeleitet wird, vergleicht sie die HTTP-Header in der Anforderung mit einer Reihe von Richtlinienausdrücken. Wenn die Anforderung nicht mit der Richtlinie übereinstimmt, leitet die Appliance die Anforderung an einen Cacheserver weiter. Wenn die Anforderung einer Richtlinie entspricht, leitet die Appliance die Anforderung unverändert an den Webserver weiter.

Weitere Informationen zum Ändern dieses Standardverhaltens finden Sie unter Direkte Richtlinientreffer auf den Cache anstelle des Ursprungs.

Um die transparente Umleitung zu konfigurieren, aktivieren Sie zunächst die Cache-Umleitung und den Lastausgleich und konfigurieren Sie den Edge-Modus. Erstellen Sie dann einen virtuellen

Cache-Umleitungsserver mit einer Platzhalter-IP-Adresse (*), damit dieser virtuelle Server Datenverkehr empfangen kann, der an die Appliance mit einer beliebigen IP-Adresse der Appliance gesendet wird. Binden Sie an diesen virtuellen Server Cache-Umleitungsrichtlinien, die die Arten von Anforderungen beschreiben, die nicht zwischengespeichert werden sollen. Erstellen Sie dann einen virtuellen Lastausgleichsserver, der Datenverkehr vom virtuellen Cache-Umleitungsserver für zwischenspeicherbare Anforderungen empfängt. Erstellen Sie schließlich einen Dienst, der einen physischen Cacheserver darstellt, und binden Sie ihn an den virtuellen Lastausgleichsserver.

Cache-Umleitung und Lastausgleich aktivieren

October 5, 2021

Die Funktionen für die Cache-Umleitung und den Lastausgleich der Appliance sind standardmäßig nicht aktiviert. Sie müssen aktiviert sein, bevor eine Cache-Umleitungskonfiguration wirksam werden kann.

Aktivieren der Cache-Umleitung und des Lastenausgleichs mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die Cache-Umleitung und den Lastausgleich zu aktivieren, und überprüfen Sie die Einstellungen:

```
-  enable ns feature cr lb
-  show ns feature
<!--NeedCopy-->
```

Beispiel:

```
> enable ns feature cr lb
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  ON
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 4)     Content Switching               CS                  ON
 5)     Cache Redirection               CR                  ON
 6)     Sure Connect
```



```
13
14              ...
15              ...
16              ...
17
18   23)    HTML Injection                HTMLInjection        ON
19   24)    appliance Push                push                 OF
20   Done
21 <!--NeedCopy-->
```

Aktivieren der Cache-Umleitung und des Lastenausgleichs mit der GUI

1. Erweitern Sie im Navigationsbereich System, und klicken Sie dann auf Einstellungen.
2. Um die Cache-Umleitung zu aktivieren, klicken Sie im Detailbereich unter Modi und Features auf Erweiterte Features konfigurieren.
   a) Aktivieren Sie im Dialogfeld Erweiterte Funktionen konfigurieren das Kontrollkästchen neben der Cache-Umleitung, und klicken Sie dann auf OK.
   b) In Funktion (en) aktivieren/deaktivieren? auf Ja.
3. Um den Lastenausgleich zu aktivieren, klicken Sie im Detailbereich unter Modi und Features auf Grundfunktionen konfigurieren.
   a) Aktivieren Sie im Dialogfeld Grundfunktionen konfigurieren das Kontrollkästchen neben Lastenausgleich, und klicken Sie dann auf OK.
   b) In Funktion (en) aktivieren/deaktivieren? auf Ja.

Edgemodus konfigurieren

October 5, 2021

Bei der Bereitstellung am Rand eines Netzwerks informiert die Citrix ADC Appliance dynamisch über die Server in diesem Netzwerk. Mit dem Edge-Modus kann die Appliance dynamisch über bis zu 40.000 HTTP-Server und Proxy-TCP-Verbindungen für diese Server erfahren.

Dieser Modus aktiviert die Erfassung von Statistiken für die dynamisch erlernten Dienste und wird normalerweise in transparenten Bereitstellungen für die Cache-Umleitung verwendet.

Aktivieren des Edge-Modus mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den Kantenmodus zu aktivieren und die Einstellung zu überprüfen:


```
-  enable ns mode Edge
-  show ns mode
<!--NeedCopy-->
```

Beispiel:

```
> enable ns mode edge
 Done

> show ns mode

        Mode                          Acronym             Status
        -------                       -------             ------
          ...
          ...
          ...
 6)     MAC-based forwarding          MBF                 ON
 7)     Edge configuration            Edge                ON
 8)     Use Subnet IP                 USNIP               OFF
          ...
          ...
          ...
 16)    Bridge BPDUs                  BridgeBPDUs         OFF
 Done
<!--NeedCopy-->
```

Aktivieren des Edge-Modus mit der GUI

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

Konfigurieren eines virtuellen Cache-Umleitungsservers

October 5, 2021

Standardmäßig leitet ein virtueller Cache-Umleitungsserver zwischenspeicherbare Anforderungen an den virtuellen Lastausgleichsserver für den Cache weiter und leitet nicht zwischenspeicherbare Anforderungen an den Ursprungsserver weiter (außer in einer Reverseproxy-Konfiguration, bei der nicht zwischenspeicherbare Anforderungen an einen virtuellen Lastenausgleichsserver gesendet werden). Es gibt drei Arten von virtuellen Cache-Umleitungsservern: transparent, Forward-Proxy und Reverse-Proxy.

Ein virtueller Server zur Cache-Umleitung verwendet eine IP-Adresse von * und eine Portnummer (in der Regel 80), die HTTP-Datenverkehr akzeptieren kann, der an jede IP-Adresse gesendet wird, die die Appliance repräsentiert. Daher können Sie nur einen virtuellen Server für die transparente Cache-Umleitung konfigurieren. Alle zusätzlichen virtuellen Cache-Umleitungsserver, die Sie konfigurieren, müssen Forward-Proxy- oder Reverse-Proxyumleitungsserver sein.

Hinzufügen eines virtuellen Cache-Umleitungsservers im transparenten Modus mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen virtuellen Cache-Umleitungsserver hinzuzufügen und die Konfiguration zu überprüfen:

```
1 -  add cr vserver <name> <serviceType> [<IPAddress> <port> ] [-
     cacheType <cacheType>] [-redirect <redirect>]
2 -  show cr vserver [<name>]
3 <!--NeedCopy-->
```

Beispiel:

```
1 add cr vserver Vserver-CRD-1 HTTP * 80 -cacheType TRANSPARENT -redirect
      POLICY
2 > show cr vserver Vserver-CRD-1
3         Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
4         State: UP  ARP:DISABLED
5         Client Idle Timeout: 180 sec
6         Down state flush: ENABLED
7         Disable Primary Vserver On Down : DISABLED
8         Default:        Content Precedence: RULE        Cache:
             TRANSPARENT
9         On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
10        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
11  Done
12 <!--NeedCopy-->
```


Ändern oder Entfernen eines virtuellen Cache-Umleitungsservers mit der CLI

- Um einen virtuellen Server zu ändern, verwenden Sie den Befehl set cr vserver, der genauso aussieht wie mit dem Befehl add cr vserver, außer dass Sie den Namen eines vorhandenen virtuellen Servers eingeben.
- Um einen virtuellen Server zu entfernen, verwenden Sie den Befehl `rm cr vserver`, der nur das <name> Argument akzeptiert.

Hinzufügen eines virtuellen Cache-Umleitungsservers im transparenten Modus mit der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Virtuellen Server erstellen (Cache-Umleitung) Werte für die folgenden Parameter an:

   - Name*—Name
   - Anschluss* — Anschluss

   * Ein erforderlicher Parameter
4. Wählen Sie in der Dropdownliste Protokoll ein unterstütztes Protokoll aus (z. B. **HTTP**). Wenn der virtuelle Server Datenverkehr an einem anderen Port als dem Standardport für das ausgewählte Protokoll empfangen soll, geben Sie einen neuen Wert in das Feld Port ein.
5. Klicken Sie auf die Registerkarte Erweitert.
6. Stellen Sie sicher, dass Cachetyp auf TRANSPARENT und Redirect auf POLICY festgelegt ist.
7. Klicken Sie auf Erstellenund dann auf Schließen. Im Bereich Cache-Umleitung Virtuelle Server wird der neue virtuelle Server angezeigt.
8. Wählen Sie den neuen virtuellen Cache-Umleitungsserver aus, um die Details seiner Konfiguration anzuzeigen.

Binden von Richtlinien an den virtuellen Cache-Umleitungsserver

October 5, 2021

Cache-Umleitungsrichtlinien werden nicht automatisch an den virtuellen Cache-Umleitungsserver gebunden. Ein richtlinienbasierter virtueller Cache-Umleitungsserver kann nur funktionieren, wenn Sie mindestens eine Richtlinie an ihn binden.

Binden von Richtlinien an einen virtuellen Cache-Umleitungsserver mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
-  bind cr vserver <name> -policyName <string>
-  show cr vserver [<name>]
<!--NeedCopy-->
```

Beispiel:

```
> bind cr vserver Vserver-CRD-1 -policyName bypass-cache-control
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-dynamic-url
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-urltokens
 Done
> bind cr vserver Vserver-CRD-1 -policyName bypass-cookie
 Done

> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: RULE        Cache:
           TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: bypass-dynamic-url
3)      Cache bypass  Policy: bypass-urltokens
4)      Cache bypass  Policy: bypass-cookie
 Done
<!--NeedCopy-->
```

Binden einer benutzerdefinierten Richtlinie an einen virtuellen Cache-Umleitungsserver mit der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server.

2. Klicken Sie auf den virtuellen Server, den Sie konfigurieren möchten, und klicken Sie auf Öffnen.
3. Wählen Sie auf der Registerkarte Richtlinien den Typ der Richtlinie aus, und klicken Sie dann auf Richtlinie einfügen.
4. Wählen Sie unter der Spalte Richtlinienname die Richtlinie aus, die Sie binden möchten.
5. Klicken Sie auf OK.

Aufheben der Bindung einer Richtlinie von einem virtuellen Cache-Umleitungsserver

October 5, 2021

Wenn Sie eine Richtlinie vom virtuellen Server für die Cache-Umleitung aufheben, wendet die Citrix ADC Appliance die Richtlinie nicht mehr an, wenn Clientanforderungen ausgewertet werden.

Entbinden einer Richtlinie von einem virtuellen Cache-Umleitungsserver mithilfe des Befehls CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
-  unbind cr vserver <name> -policyName <string>
-  show cr vserver [<name>]
<!--NeedCopy-->
```

Beispiel:

```
unbind cr vserver Vserver-CR-1 -policyName bypass-non-get
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: RULE        Cache:
           TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
```



```
13   Done
14 <!--NeedCopy-->
```

Aufheben der Bindung einer benutzerdefinierten Richtlinie von einem virtuellen Cache-Umleitungsserver mit der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server.
2. Klicken Sie auf den virtuellen Server, den Sie konfigurieren möchten, und klicken Sie dann auf Öffnen.
3. Wählen Sie auf der Registerkarte Richtlinien unter Richtlinienname die Richtlinie aus, die Sie aufheben möchten.
4. Klicken Sie auf Richtlinie aufheben, und klicken Sie dann auf OK.

Erstellen eines virtuellen Lastausgleichsservers

October 5, 2021

Der virtuelle Cache-Umleitungsserver auf der Citrix ADC Appliance kann Anforderungen entweder an eine Cacheserverfarm senden, wenn die Anforderung zwischengespeichert werden kann, oder an die Ursprungsserverfarm, wenn die Anforderung nicht zwischengespeichert werden kann.

Jeder Cacheserver wird auf der Appliance durch einen Dienst dargestellt, der an einen virtuellen Lastausgleichsserver gebunden ist, der Anforderungen vom virtuellen Cache-Umleitungsserver empfängt und diese Anforderungen an die Server weiterleitet.

Weitere Informationen zum Konfigurieren von virtuellen Lastenausgleichs-Servern und anderen Konfigurationsoptionen finden Sie unter Load Balancing.

Erstellen eines virtuellen Lastausgleichsservers mit der CLI

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

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

Beispiel:


```
> add lb vserver Vserver-LB-CR HTTP 10.102.20.30 80
 Done
> show lb vserver Vserver-LB-CR
        Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 08:47:52 2010
        Time since last state change: 0 days, 00:00:08.470
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none
 Done
<!--NeedCopy-->
```

Erstellen eines virtuellen Lastausgleichsservers mit der GUI

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Virtuellen Server erstellen (Load Balancing) Werte für die folgenden Parameter an:

   - Name*-name
   - IP-Adresse*- IP-Adresse
   - Anschluss*-Anschluss

   * Ein erforderlicher Parameter

4. Wählen Sie in der Liste Protokoll ein unterstütztes Protokoll aus (z. B. **HTTP**). Wenn der virtuelle Server Datenverkehr an einem anderen Port als dem bekannten Port für das ausgewählte Protokoll empfangen soll, geben Sie einen neuen Wert in das Feld Port ein.
5. Klicken Sie auf Erstellenund dann auf Schließen. Im Bereich Load Balancing Virtuelle Server wird der neue virtuelle Server angezeigt.

Konfigurieren eines HTTP-Dienstes

October 5, 2021

Auf der Citrix ADC Appliance stellt ein Dienst einen physischen Server im Netzwerk dar. In der Konfiguration der transparenten Cache-Umleitung stellt der Dienst den Cacheserver dar. Cache-Requests werden vom virtuellen Cache-Umleitungsserver an den virtuellen Load Balancing Server gesendet, der wiederum jede Anforderung an den richtigen Dienst weiterleitet, der sie an den Cacheserver weiterleitet.

Konfigurieren eines HTTP-Dienstes mit der CLI

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

```
1 -  add service <name> <IP> <serviceType> <port> -cacheType <cacheType>
2 -  show service [<name>]
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add service Service-HTTP-1 10.102.29.40 HTTP 80 -cacheType
     TRANSPARENT
2  Done
3 > show service Service-HTTP-1
4         Service-HTTP-1 (10.102.29.40:80) - HTTP
5         State: DOWN
6         Last state change was at Fri Jul  2 09:14:17 2010
7         Time since last state change: 0 days, 00:00:13.820
8         Server Name: 10.102.29.40
9         Server ID : 0   Monitor Threshold : 0
10        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
11        Use Source IP: NO
12        Client Keepalive(CKA): NO
13        Access Down Service: NO
14        TCP Buffering(TCPB): NO
15        HTTP Compression(CMP): YES
16        Idle timeout: Client: 180 sec   Server: 360 sec
17        Client IP: DISABLED
18        Cache Type: TRANSPARENT Redirect Mode:
```



```
19          Cacheable: NO
20          SC: OFF
21          SP: ON
22          Down state flush: ENABLED
23
24  1)      Monitor Name: tcp-default
25                  State: DOWN     Weight: 1
26                  Probes: 3       Failed [Total: 3 Current: 3]
27                  Last response: Failure - Time out during TCP connection
                        establishment stage
28                  Response Time: N/A
29   Done
30  <!--NeedCopy-->
```

Ändern oder Entfernen eines Dienstes mit der CLI

- Um einen Dienst zu ändern, verwenden Sie den Befehl set service, der genauso wie mit dem Befehl add service entspricht, mit der Ausnahme, dass Sie den Namen eines vorhandenen Dienstes eingeben.
- Um einen Dienst zu entfernen, verwenden Sie den`rm service` Befehl, der nur das <name> Argument akzeptiert.

Hinzufügen eines HTTP-Dienstes mit der GUI

1. Navigieren Sie zu Traffic Management > Load Balancing > Services
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Dienst erstellen Werte für die folgenden Parameter an, wie gezeigt:
   - Dienstname* — Name
   - Server*—IP
   - Anschluss* — Anschluss

   * Ein erforderlicher Parameter
4. Wählen Sie in der Dropdownliste Protokoll* ein unterstütztes Protokoll aus (z. B. **HTTP**).
5. Klicken Sie auf Erstellenund dann auf Schließen.

Binden/Entbinden eines Dienstes/eines virtuellen Lastenausgleichsservers

October 5, 2021

Sie müssen einen Dienst an den virtuellen Lastausgleichsserver binden. Dadurch kann der Load Balancer die Anforderung an den Server weiterleiten, den der Dienst darstellt. Wenn sich Ihre Konfiguration ändert, können Sie die Bindung eines Diensts vom virtuellen Lastausgleichsserver aufheben.

Binden eines Dienstes an einen virtuellen Lastausgleichsserver mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel:

```
> bind lb vserver vserver-LB-CR service-HTTP-1
 Done
> show lb vserver Vserver-LB-CR
        Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 08:47:52 2010
        Time since last state change: 0 days, 00:42:25.610
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

```



```
1) Service-HTTP-1 (10.102.29.40: 80) - HTTP State: DOWN Weight: 1
 Done
<!--NeedCopy-->
```

Aufheben der Bindung eines Dienstes von einem virtuellen Lastausgleichsserver mit der CLI

Um die Bindung eines Dienstes aufzuheben, verwenden Sie den Befehl `unbind lb vserver` anstelle von `bind lb vserver`.

Binden/Entbinden eines Dienstes von einem virtuellen Lastausgleichsserver mit der GUI

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server
2. Wählen Sie im Detailbereich den virtuellen Server aus, von dem Sie den Dienst binden/aufheben möchten, und klicken Sie dann auf Öffnen.
3. Aktivieren bzw. deaktivieren Sie auf der Registerkarte Dienste in der Spalte Aktiv das Kontrollkästchen neben dem Dienstnamen.
4. Klicken Sie auf OK.

Deaktivieren der Proxy-Port-Einstellung für transparentes Caching

October 5, 2021

Wenn die Option Quell-IP (USIP) verwenden für einen Cache-Dienst deaktiviert ist, der auf der Citrix ADC Appliance konfiguriert ist, leitet die Appliance Clientanforderungen an den Cache-Dienst weiter, indem sie eine SNIP-Adresse (Subnetz-IP) oder eine zugeordnete IP-Adresse (MIP) als Quell-IP-Adresse und einen zufälligen Port als Quellport verwendet. Der zufällig ausgewählte Port wird als Proxy-Port bezeichnet.

Wenn Sie jedoch einen vollständig transparenten Cache konfigurieren möchten (eine Cachekonfiguration, in der der Cache-Dienst die IP-Adresse und die Portnummer des Clients empfängt), müssen Sie nicht nur die USIP-Option global oder im Cache-Dienst aktivieren, sondern auch die Einstellung Proxy-Port verwenden entweder global oder auf der Cache-Dienst. Wenn Sie die Einstellung Proxy-Port verwenden deaktivieren, kann die Appliance den Quellport des Clients als Quellport verwenden, wenn sie eine Verbindung mit dem Cache-Dienst herstellt, und stellt eine vollständig transparente Cachekonfiguration sicher.

Weitere Informationen zum Konfigurieren der Option Proxyport verwenden global oder für einen Dienst finden Sie unter Konfigurieren des Quellports für serverseitige Verbindungen.

Zuweisen eines Portbereichs zur Citrix ADC Appliance

October 5, 2021

Die Freigabe der Client-IP-Adresse kann zu einem Konflikt führen, der dazu führt, dass Netzwerkgeräte wie Router, Cacheserver, Ursprungsserver und andere Citrix ADC Appliances die Appliance und damit den Client, an den die Antwort gesendet werden soll, nicht ermitteln können.

Eine Methode zur Lösung dieses Problems besteht darin, der Citrix ADC Appliance einen Quellportbereich zuzuweisen. Diese Zuteilung ermöglicht es Netzwerkgeräten, die Citrix ADC Appliance, die die Anforderung gesendet hat, eindeutig zu identifizieren.

Zuweisen eines Quellportbereichs zu einer Citrix ADC Appliance mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns param -crPortRange <startPortNumber-endPortNumber>
```

Zuweisen eines Quellportbereichs zu einer Citrix ADC Appliance mit der Benutzeroberfläche der Appliance

1. Klicken Sie im Navigationsbereich auf System, und klicken Sie dann auf Einstellungen.
2. Klicken Sie in der Gruppe Einstellungen auf den Link Globale Systemeinstellungen ändern.
3. Geben Sie in der Gruppe Cache-Umleitungs-Portbereich den Portbereich für die Appliance an, indem Sie eine Portnummer für Startport und eine Portnummer für Endport eingeben.
4. Klicken Sie auf OK.

Aktivieren des Lastenausgleichs von virtuellen Servern zum Umleiten von Anforderungen in den Cache

October 5, 2021

Wenn ein virtueller Lastausgleichsserver so konfiguriert ist, dass er eine bestimmte IP-Adresse und eine bestimmte Portkombination überwacht, hat er Vorrang vor dem virtuellen Cache-Umleitungsserver für alle Anforderungen, die für diese Adress-Port-Kombination bestimmt sind. Daher verarbeitet der virtuelle Cache-Umleitung Server diese Anforderungen nicht.

Wenn Sie diese Funktionalität außer Kraft setzen und den virtuellen Server für die Cache-Umleitung entscheiden lassen möchten, ob die Anforderung aus dem Cache bedient werden soll oder nicht, konfigurieren Sie den jeweiligen virtuellen Lastausgleichsserver so, dass er zwischengespeichert werden kann.

Eine solche Konfiguration wird normalerweise verwendet, wenn ein ISP eine Citrix ADC Appliance am Rand seines Netzwerks verwendet und der gesamte Datenverkehr durch die Appliance fließt.

Aktivieren Sie die Lastenausgleichsserver, um Anforderungen an den Cache mit der CLI umzuleiten

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
-  set lb vserver <name> [-cacheable ( YES | NO)]
-  show lb vserver [<name>]
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-CR  - cacheable YES
> show lb vserver vserver-LB-CR
        Vserver-LB-CR (10.102.20.30:80) - HTTP  Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 08:47:52 2010
        Time since last state change: 0 days, 01:05:51.510
        Effective State: DOWN
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
        Cacheable: YES  PQ: OFF SC: OFF
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none

1) Service-HTTP-1 (10.102.29.40: 80) - HTTP State: DOWN Weight: 1
 Done
<!--NeedCopy-->
```

Für eine transparente Cache-Umleitung fängt die Appliance den gesamten Datenverkehr ab und wertet jede Anforderung aus, um festzustellen, ob sie zwischengespeichert werden kann. Nicht

zwischenspeicherbare Anforderungen werden unverändert an den Ursprungsserver gesendet.

Wenn Sie die transparente Cache-Umleitung verwenden, können Sie die Cache-Umleitung für virtuelle Server deaktivieren, die den Datenverkehr immer an Ursprungsserver weiterleiten.

Deaktivieren der Zwischenspeicherung für einen virtuellen Lastausgleichsserver mit der CLI

Um die Zwischenspeicherung für einen virtuellen Lastenausgleich zu deaktivieren, verwenden Sie den Befehl unset lb vserver anstelle von set lb vserver. Geben Sie den Wert NO für den **cacheable** Parameter an.

Aktivieren oder Deaktivieren des Lastenausgleichs von virtuellen Servern zum Umleiten von Anforderungen an den Cache mit der GUI

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, von dem Sie das Caching aktivieren/deaktivieren möchten, und klicken Sie dann auf Öffnen.
3. Aktivieren Sie auf der Registerkarte Erweitert das Kontrollkästchen Cache-Umleitung.
4. Klicken Sie auf OK.

Konfigurieren der Weiterleitungsproxy-Umleitung

October 5, 2021

Ein Forward-Proxy ist ein zentraler Ansprechpartner für einen Client oder eine Gruppe von Clients. In dieser Konfiguration leitet die Citrix ADC Appliance nicht zwischenspeicherbare Anforderungen an einen Ursprungsserver um und leitet zwischenspeicherbare Anforderungen entweder an einen Forward-Proxycache oder einen transparenten Cache um.

Wenn die Appliance als Forward-Proxy konfiguriert ist, müssen Benutzer ihre Browser so ändern, dass der Browser Anforderungen an den Forward-Proxy anstelle der Zielserver sendet.

Ein virtueller Forward-Proxy-Cache-Umleitungsserver auf der Appliance vergleicht die Anforderung mit einer Cache-Richtlinie. Wenn die Anforderung nicht zwischengespeichert werden kann, fragt die Appliance einen virtuellen DNS-Lastausgleichsserver für die Auflösung des Ziels ab und sendet die Anforderung dann an den Ursprungsserver. Wenn die Anforderung zwischengespeichert werden kann, leitet die Appliance die Anforderung an einen virtuellen Lastausgleichsserver für den Cache weiter.

Die Appliance verwendet einen Hostdomänennamen oder eine IP-Adresse im HOST-Header der Anforderung, um das angeforderte Ziel zu bestimmen. Wenn in der Anforderung kein HOST-Header

vorhanden ist, fügt die Appliance einen HOST-Header basierend auf der Ziel-IP-Adresse in die Anforderung ein.

In der Regel fungiert die Citrix ADC Appliance als Forward-Proxy in einem Unternehmens-LAN. In einer solchen Konfiguration befindet sich die Appliance am Rand eines Unternehmens-LAN und fängt Clientanforderungen ab, bevor sie an das WAN gesendet werden. Durch die Konfiguration der Appliance im Forward-Proxy-Modus wird der Datenverkehr auf dem WAN reduziert.

Um die Weiterleitungsproxy-Cache-Umleitung zu konfigurieren, aktivieren Sie zuerst den Lastausgleich und die Cache-Umleitung auf der Appliance. Konfigurieren Sie dann einen virtuellen DNS-Lastenausgleichsserver und die zugehörigen Dienste. Konfigurieren Sie außerdem einen virtuellen Lastausgleichsserver und binden Sie entsprechende Dienste für den Cache an ihn. Konfigurieren Sie einen virtuellen Forward-Proxy-Cache-Umleitungsserver und binden Sie die DNS- und Lastausgleichsserver an diesen. Sie müssen auch Caching-Richtlinien konfigurieren und sie an den virtuellen Cache-Umleitungsserver binden. Um das Setup abzuschließen, konfigurieren Sie die Client-Browser so, dass der Forward-Proxy verwendet wird.

Weitere Informationen zum Aktivieren der Cache-Umleitung und des Lastausgleichs auf der Appliance finden Sie unter Aktivieren der Cache-Umleitung und des Lastausgleichs.

Weitere Informationen zum Erstellen eines virtuellen Lastausgleichsservers finden Sie unter Erstellen eines virtuellen Lastausgleichsservers.

Weitere Informationen zur Konfiguration von Diensten, die den Cache-Server darstellen, finden Sie unter Konfigurieren eines HTTP-Dienstes.

Weitere Informationen zum Binden des Dienstes an einen virtuellen Server finden Sie unter Binden/Aufheben eines Dienstes an/von einem virtuellen Lastausgleichsserver.

Weitere Informationen zum Erstellen eines Forward-Proxy-Cache-Umleitungsservers finden Sie unter Konfigurieren eines virtuellen Cache-Umleitungsserversund Erstellen eines virtuellen Servers vom Typ TRANSPARENT oder FORWARD.

Weitere Informationen zum Binden von Cache-Umleitungsrichtlinien an den virtuellen Cache-Umleitungsserver finden Sie unter Konfigurieren einer Cache-Umleitungsrichtlinie.

Erstellen eines DNS-Dienstes

October 5, 2021

Ein DNS-Dienst ist eine Darstellung eines physischen DNS-Servers im Netzwerk auf der Citrix ADC Appliance. Ein virtueller DNS-Lastenausgleichsserver sendet DNS-Anforderungen an den DNS-Server im Netzwerk über einen solchen Dienst.

Erstellen eines DNS-Dienstes mit der CLI

Geben Sie in der Befehlszeile die folgenden Befehle ein, um einen DNS-Dienst zu erstellen und die Konfiguration zu überprüfen:

```
-  add service <name> <IP> <serviceType> <port>
-  show service [<name>]
<!--NeedCopy-->
```

Beispiel:

```
add service Service-DNS-1 10.102.29.41 DNS 53
show service Service-DNS-1
        Service-DNS-1 (10.102.29.41:53) - DNS
        State: DOWN
        Last state change was at Fri Jul  2 10:14:32 2010
        Time since last state change: 0 days, 00:00:13.550
        Server Name: 10.102.29.41
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: ping-default
                State: DOWN     Weight: 1
                Probes: 3       Failed [Total: 3 Current: 3]
                Last response: Failure - Probe timed out.
                Response Time: 2000.0 millisec
 Done
<!--NeedCopy-->
```


Hinzufügen eines DNS-Dienstes mit der GUI

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Dienst erstellen Werte für die folgenden Parameter an, wie gezeigt:
    - Dienstname* — Name
    - Server*— IP
    - Anschluss* — Anschluss

* Ein erforderlicher Parameter

1. Wählen Sie in der Dropdownliste Protokoll* ein unterstütztes Protokoll (z. B. **DNS**) aus.
2. Klicken Sie auf Erstellenund dann auf Schließen.

Erstellen eines virtuellen DNS-Lastausgleichsservers

October 5, 2021

Der virtuelle DNS-Server ermöglicht es dem Forward-Proxy, die DNS-Auflösung durchzuführen, bevor eine Clientanforderung an einen Ursprungsserver weitergeleitet wird. Der virtuelle DNS-Lastausgleichsserver ist dem DNS-Dienst zugeordnet, der den physischen DNS-Server im Netzwerk darstellt.

Erstellen eines virtuellen DNS-Lastausgleichsservers mit der CLI

Geben Sie in der Befehlszeile die folgenden Befehle ein, um einen virtuellen DNS-Lastausgleichsserver zu erstellen und die Konfiguration zu überprüfen:

```
1 -  add lb vserver <name> <serviceType>
2 -  show lb vserver [<name>]
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add lb vserver Vserver-DNS-1 DNS
2  Done
3 > show lb vserver Vserver-DNS-1
4         Vserver-DNS-1 (0.0.0.0:0) - DNS Type: ADDRESS
```



```
        State: DOWN
        Last state change was at Fri Jul  2 10:32:28 2010
        Time since last state change: 0 days, 00:00:08.10
        Effective State: DOWN  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE
 Done
<!--NeedCopy-->
```

Erstellen eines virtuellen DNS-Lastausgleichsservers mit der GUI

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Virtuellen Server erstellen (Load Balancing) im Feld Name einen Namen für den virtuellen Server ein.
4. Wählen Sie in der Dropdownliste Protokoll* ein unterstütztes Protokoll (z. B. **DNS**) aus.
5. Klicken Sie auf Erstellenund dann auf Schließen. Im Bereich Virtuelle DNS-Server wird der neue virtuelle Server angezeigt.

Binden des DNS-Diensts an den virtuellen Server

October 5, 2021

Damit der DNS-Server auf DNS-Anforderungen antwortet, muss der Dienst, der den DNS-Server darstellt, an den virtuellen DNS-Server gebunden sein.

Binden Sie den DNS-Dienst an den virtuellen Lastausgleichsserver mit der CLI

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

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


Beispiel:

```
> bind lb vserver Vserver-DNS-1 Service-DNS-1
 Done
> show lb vserver Vserver-DNS-1
        Vserver-DNS-1 (0.0.0.0:0) - DNS Type: ADDRESS
        State: DOWN
        Last state change was at Fri Jul  2 10:32:28 2010
        Time since last state change: 0 days, 00:12:16.80
        Effective State: DOWN  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: LEASTCONNECTION
        Mode: IP
        Persistence: NONE

1) Service-DNS-1 (10.102.29.41: 53) - DNS State: DOWN   Weight: 1
 Done
>
<!--NeedCopy-->
```

Entbinden eines DNS-Dienstes vom virtuellen Lastausgleichsserver mit der CLI

Verwenden Sie den`unbind lb vserver` Befehl anstelle von`bind lb vserver` .

Binden/Entbinden eines DNS-Dienstes eines virtuellen Lastausgleichsservers mit der GUI

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server
2. Wählen Sie im Detailbereich den virtuellen Server aus, an den Sie den DNS-Dienst binden/aufheben möchten, und klicken Sie dann auf Öffnen.
3. Aktivieren bzw. deaktivieren Sie auf der Registerkarte Dienste in der Spalte Aktiv das Kontrollkästchen neben dem Dienstnamen.
4. Klicken Sie auf OK.

Konfigurieren eines Client-Webbrowsers für die Verwendung eines Forward-Proxy

October 5, 2021

Wenn Sie die Citrix ADC Appliance als virtueller Forward-Proxy-Cache-Umleitungsserver im Netzwerk konfigurieren, müssen Sie den Client-Webbrowser so konfigurieren, dass Anforderungen an den Forward-Proxy gesendet werden. Wenn Sie einen Forward-Proxy verwenden, ist die einzige Route zu den Servern im Netzwerk über den Forward-Proxy.

Lesen Sie die Dokumentation Ihres Browsers, um den Browser so zu konfigurieren, dass er einen Forward-Proxy verwendet. Geben Sie die IP-Adresse und die Portnummer des virtuellen Forward-Proxy-Cache-Umleitungsservers für diese Konfiguration an.

Konfigurieren der Reverse-Proxy-Umleitung

October 5, 2021

Ein Reverse-Proxy befindet sich vor einem oder mehreren Webservern und schützt den Ursprungsserver vor Clientanforderungen. Häufig ist ein Reverse-Proxy-Cache ein Front-End für alle Clientanforderungen an einen Server. Ein Administrator weist einem bestimmten Ursprungsserver einen Reverse-Proxy-Cache zu. Der Reverse-Proxy-Cache ist anders als transparente Proxy-Caches und Forward-Proxy-Caches, die häufig angeforderten Inhalte für alle Anfragen an einen Ursprungsserver zwischenspeichern, und die Wahl eines Servers basiert auf der Anforderung.

Im Gegensatz zu einem transparenten Proxy-Cache verfügt der Reverse-Proxy-Cache über eine eigene IP-Adresse und kann Zieldomänen und URLs in einer nicht zwischenspeicherbaren Anforderung durch neue Zieldomänen und URLs ersetzen.

Sie können die Reverse-Proxy-Cache-Umleitung auf der Ursprungsserverseite oder am Rand eines Netzwerks bereitstellen. Bei der Bereitstellung auf dem Ursprungsserver ist der virtuelle Reverse-Proxy-Cache-Umleitungsserver ein Front-End für alle Anforderungen an den Ursprungsserver.

Wenn die Appliance im Reverse-Proxymodus eine Anforderung erhält, wertet ein virtueller Cache-Umleitungsserver die Anforderung aus und leitet sie entweder an einen virtuellen Lastausgleichsserver für den Cache oder an einen virtuellen Lastausgleichsserver für den Ursprung weiter. Die eingehende Anforderung kann transformiert werden, indem der Host-Header oder die Host-URL geändert wird, bevor sie an den Back-End-Server gesendet werden.

Um die Reverse-Proxy-Cache-Umleitung zu konfigurieren, aktivieren Sie zunächst die Cache-Umleitung und den Lastausgleich. Konfigurieren Sie dann einen virtuellen Lastausgleichsserver

und -dienste, um zwischenspeicherbare Anforderungen an die Cacheserver zu senden. Konfigurieren Sie außerdem einen virtuellen Lastausgleichsserver und die zugehörigen Dienste für die Ursprungsserver. Konfigurieren Sie dann einen virtuellen Reverse-Proxy-Cache-Umleitungsserver, und binden Sie relevante Cache-Umleitungsrichtlinien an ihn. Konfigurieren Sie schließlich Zuordnungsrichtlinien und binden Sie sie an den virtuellen Reverse-Proxy-Cache-Umleitungsserver.

Den Zuordnungsrichtlinien ist eine zugeordnete Aktion zugeordnet, mit der der virtuelle Cache-Umleitungsserver alle nicht zwischenspeicherbaren Anforderungen an den virtuellen Lastausgleichsserver für den Ursprung weiterleiten kann.

Stellen Sie sicher, dass Sie das Standard-Cacheserver-Ziel erstellen.

Weitere Informationen zum Aktivieren der Cache-Umleitung und des Lastausgleichs auf der Appliance finden Sie unter Aktivieren der Cache-Umleitung und des Lastausgleichs.

Weitere Informationen zum Erstellen eines virtuellen Lastausgleichsservers finden Sie unter Erstellen eines virtuellen Lastausgleichsservers.

Weitere Informationen zur Konfiguration von Diensten, die den Cache-Server darstellen, finden Sie unter Konfigurieren eines HTTP-Dienstes.

Weitere Informationen zum Binden des Dienstes an einen virtuellen Server finden Sie unter Binden/Aufheben eines Dienstes an/von einem virtuellen Lastausgleichsserver.

Weitere Informationen zum Erstellen eines Reverse-Proxy-Cache-Umleitungsservers finden Sie unter Konfigurieren eines virtuellen Cache-Umleitungsserversund Erstellen eines virtuellen Servers vom Typ REVERSE.

Weitere Informationen zum Binden integrierter Cache-Umleitungsrichtlinien an den virtuellen Cache-Umleitungsserver finden Sie unter Binden von Richtlinien an den virtuellen Cache-Umleitungsserver.

Konfigurieren von Zuordnungsrichtlinien

Wenn eine eingehende Anforderung nicht zwischengespeichert werden kann, ersetzt der virtuelle Reverse-Proxy-Cache-Umleitungsserver die Domäne und URL in der Anforderung durch die Domäne und URL eines Ziel-Ursprungsservers und leitet die Anforderung an den virtuellen Lastausgleichsserver für den Ursprung weiter.

Eine Zuordnungsrichtlinie ermöglicht es dem virtuellen Reverse-Proxy-Cache-Umleitungsserver, die Zieldomäne und den URL zu ersetzen und die Anforderung an den virtuellen Lastausgleichsserver für den Ursprung weiterzuleiten.

Eine Zuordnungsrichtlinie muss zuerst die Domäne und die URL übersetzen und dann die Anforderung an den virtuellen Server des Ursprungslastenausgleichs weitergeben.

Eine Zuordnungsrichtlinie kann eine Domäne, ein URL-Präfix und ein URL-Suffix wie folgt zuordnen:

- Domänenzuordnung: Sie können eine Domäne ohne Präfix oder Suffix zuordnen. Die Domänenzuordnung ist die Standardzuordnung für den virtuellen Server (z. B. die Zuordnung von www.mycompany.com zu www.myrealcompany.com).
- Präfixzuordnung: Sie können ein bestimmtes Muster ersetzen, das als Teil der URL vorangestellt ist (z. B. die Zuordnung von www.mycompany.com/sports/index.html zu www.mycompany.com/news/index.html).
- Suffixzuordnung: Sie können das Dateisuffix in der URL ersetzen (z. B. die Zuordnung von www.mycompany.com/sports/index.html zu www.mycompany.com/sports/index.asp).

Die Quell- und Zielzeichenfolgen, die zugeordnet werden, müssen ähnlich sein. Wenn Sie eine Quelldomäne angeben, müssen Sie eine Zieldomäne angeben. Wenn Sie ein Quellsuffix angeben, müssen Sie ein Zielsuffix angeben. Wenn Sie eine genaue URL aus der Quelle angeben, muss die Ziel-URL auch eine genaue URL sein.

Nachdem Sie Zuordnungsrichtlinien für den Reverse-Proxymodus konfiguriert haben, müssen Sie sie an den virtuellen Cache-Umleitungsserver binden.

Sie können Kombinationen aus Quell-URL, Ziel-URL sowie Quell- und Zieldomänen verwenden, um alle drei Arten der Domänenzuordnung zu konfigurieren.

Konfigurieren einer Zuordnungsrichtlinie für den Reverse-Proxymodus mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine Richtlinienzuordnung hinzuzufügen und die Konfiguration zu überprüfen:

```
1 -  add policy map <mapPolicyName> -sd <string> [-su <string>] [-td <
     string>] [-tu <string>]
2 -  show policy map [<mapPolicyName>]
3 <!--NeedCopy-->
```

Beispiel:

Der folgende Befehl ordnet eine Domäne in einer Clientanforderung einer Zieldomäne zu:

```
1 > add policy map myMappingPolicy -sd www.mycompany.com -td www.
     myrealcompany.com
2  Done
3 > show policy map myMappingPolicy
4 1)      Name: myMappingPolicy
5         Source Domain: www.mycompany.com        Source Url:
6         Target Domain: www.myrealcompany.com    Target Url:
7  Done
```



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

Es folgt ein Beispiel für die Zuordnung eines URL-Suffixes zu einem anderen URL-Suffix:

```
> add policy map myOtherMappingPolicy -sd www.mycompany.com -td www.
   myrealcompany.com -su /news.html -tu /realnews.html
 Done
> show policy map myOtherMappingPolicy
1)      Name: myOtherMappingPolicy
        Source Domain: www.mycompany.com        Source Url: /news.html
        Target Domain: www.myrealcompany.com    Target Url: /realnews.
           html
 Done
<!--NeedCopy-->
```

Konfigurieren einer Zuordnungsrichtlinie für den Reverse-Proxymodus mit der GUI

1. Navigieren Sie zu **Traffic Management > Cache-Umleitung > Zuordnungsrichtlinien**.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Kartenrichtlinie erstellen Werte für die folgenden Parameter an:
   - Name*- mapPolicyName
   - Source Domain*-sd
   - Target Domain*-td
   - Source URL-su
   - Target URL-tu

   * Ein erforderlicher Parameter
4. Klicken Sie auf Erstellenund dann auf Schließen. Im Zuordnungsbereich wird die neue Zuordnungsrichtlinie angezeigt.

Binden Sie die Zuordnungsrichtlinie an den virtuellen Cache-Umleitungsserver mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Zuordnungsrichtlinie an den virtuellen Cache-Umleitungsserver zu binden und die Konfiguration zu überprüfen:

```
-  bind cr vserver <name> -policyName <string> [<targetVserver>]
-  show cr vserver <name>
<!--NeedCopy-->
```


Beispiel:

```
> bind cr vserver Vserver-CRD-3 -policyName myMappingPolicy Vserver-LB-
   CR
 Done
> show cr vserver Vserver-CRD-3
        Vserver-CRD-3 (10.102.29.50:88) - HTTP  Type: CONTENT
        State: UP
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default: Vserver-LB-CR  Content Precedence: RULE        Cache:
           REVERSE
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Policy:         Target: Vserver-LB-CR   Priority: 0     Hits: 0
1)      Map: myMappingPolicy Target: Vserver-LB-CR
 Done
<!--NeedCopy-->
```

Binden Sie die Zuordnungsrichtlinie an den virtuellen Cache-Umleitungsserver mit der GUI

1. Navigieren Sie zu **Traffic Management > Cache-Umleitung > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, von dem Sie die Zuordnungsrichtlinie binden möchten, und klicken Sie dann auf **Öffnen**.
3. Wählen **Sie im Konfigurieren des virtuellen Servers**(Cache-Umleitung) auf der Registerkarte **Richtlinien** die Option **Zuordnung**aus, und klicken Sie dann auf **Richtlinie einfügen**.
4. Wählen Sie in der Spalte **Richtlinienname** die Richtlinie aus der Dropdownliste aus.
5. Klicken Sie in der Spalte **Ziel** auf den Abwärtspfeil, und wählen Sie dann den virtuellen Server aus der Dropdownliste aus.
6. Klicken Sie auf **OK**.

Selektive Cache-Umleitung

October 5, 2021

Die selektive Cache-Umleitung sendet Anforderungen für bestimmte Inhaltstypen, z. B. Bilder, an einen Cacheserver oder eine Gruppe von Cacheservern und sendet andere Inhaltstypen an einen an-

deren Cacheserver oder eine andere Cache-Gruppe. Sie können die erweiterte Cache-Umleitung im Modus Transparent, Reverse Proxy oder Forward Proxy konfigurieren.

Bei der selektiven Cache-Umleitung fängt die Citrix ADC Appliance eine Clientanforderung ab und leitet nicht zwischenspeicherbare Anforderungen an das ursprüngliche Ziel in der Clientanforderung weiter. Bei zwischenspeicherbaren Anforderungen sendet die Appliance die Anforderungen an den Ziel-Cacheserver, der Inhalte eines bestimmten Inhaltstyps bereitstellen kann.

Bei der selektiven Cache-Umleitung wird zusätzlich zu den Cache-Umleitungsrichtlinien für Content Switching konfiguriert. Die Appliance wertet zunächst die Cache-Umleitungsrichtlinien aus, die an den virtuellen Cache-Umleitungsserver gebunden sind. Wenn eine Anforderung mit einer Cache-Umleitungsrichtlinie übereinstimmt, sendet der virtuelle Cache-Umleitungsserver die Anforderung an den Ursprungsserver oder an einen virtuellen Lastausgleichsserver für den Ursprung. Wenn keine Cache-Umleitungsrichtlinien mit der Anforderung übereinstimmen, wertet die Appliance die Content Switching-Richtlinien aus, die an den virtuellen Server der Cache-Umleitung gebunden sind. Wenn eine Content Switching-Richtlinie mit der Anforderung übereinstimmt, leitet der virtuelle Cache-Umleitungsserver die Anforderung an einen virtuellen Lastausgleichsserver für den Cache um.

Um die selektive Cache-Umleitung zu konfigurieren, aktivieren Sie zunächst die Cache-Umleitung, den Lastenausgleich und Content Switching auf der Citrix ADC Appliance. Konfigurieren Sie dann einen virtuellen Lastausgleichsserver für den Cache und einen zugeordneten HTTP-Dienst. Konfigurieren Sie anschließend einen virtuellen Cache-Umleitungsserver und binden Sie sowohl die Cache-Umleitung als auch die Content Switching-Richtlinien an diesen. Sobald Sie die Richtlinien gebunden haben, können Sie den virtuellen Server so konfigurieren, dass entweder regelbasierte oder URL-basierte Content Switching-Richtlinien Vorrang eingeräumt werden.

Wenn die Appliance für die Cache-Umleitung im transparenten Modus in einer Edge-Bereitstellungstopologie konfiguriert ist, sendet die Appliance den gesamten zwischengespeicherten HTTP-Datenverkehr an eine transparente Cache-Farm. Clients greifen über die Appliance auf das Internet zu, die als Layer 4-Switch konfiguriert ist, der Datenverkehr an Port 80 empfängt.

Die Appliance kann Anforderungen für Bilder (z. B. GIF- und JPG-Dateien) an einen Server in der transparenten Cache-Farm und alle anderen Anforderungen für statische Inhalte an andere Server in der Farm leiten. Für diese Konfiguration konfigurieren Sie Content Switching-Richtlinien, um Bilder an den Bildercache zu senden und alle anderen zwischenspeicherbaren Inhalte in einen Standardcache zu senden.

Hinweis: Die hier beschriebene Konfiguration dient der transparenten selektiven Cache-Umleitung. Daher ist kein virtueller Lastausgleichsserver für den Ursprung erforderlich, ebenso wie eine Reverse-Proxy-Konfiguration.

Um diesen Typ der selektiven Cache-Umleitung zu konfigurieren, aktivieren Sie zunächst die Cache-Umleitung, den Lastenausgleich und Content Switching. Konfigurieren Sie dann einen virtuellen Las-

tausgleichsserver für den Cache und konfigurieren Sie einen zugeordneten HTTP-Dienst. Konfigurieren Sie dann einen virtuellen Cache-Umleitungsserver und erstellen und binden Sie sowohl Cache-Umleitung als auch Content Switching-Richtlinien an diesen virtuellen Server.

Weitere Informationen zum Aktivieren der Cache-Umleitung und des Lastausgleichs auf der Appliance finden Sie unter Aktivieren der Cache-Umleitung und des Lastausgleichs.

Content Switching aktivieren

October 5, 2021

Um die selektive Cache-Umleitung zu konfigurieren, müssen Sie Content Switching aktivieren, nachdem Sie sowohl die Funktionen für den Lastausgleich als auch die Cache-Umleitung auf der Appliance aktiviert haben.

Aktivieren von Content Switching mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
-  enable ns feature CS

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

Beispiel:

```
> enable ns feature cs
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  ON
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 4)     Content Switching               CS                  ON
 5)     Cache Redirection               CR                  ON
          ...
          ...
          ...
```



```
15   23)    HTML Injection                HTMLInjection        ON
16   24)    appliance Push                push                 OFF
17   Done
18 <!--NeedCopy-->
```

Aktivieren der Cache-Umleitung und des Lastenausgleichs mit der GUI

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

Konfigurieren eines virtuellen Lastausgleichsservers für den Cache

October 5, 2021

Erstellen Sie einen virtuellen Lastausgleichsserver und einen HTTP-Dienst für jeden verwendeten Cacheservertyp. Wenn Sie beispielsweise JPEG-Dateien von einem Cacheserver und GIF-Dateien von einem anderen Cacheserver bereitstellen und für den Rest des Inhalts einen dritten Cacheserver verwenden möchten, erstellen Sie für jeden der drei Typen von Cacheservern einen HTTP-Dienst und einen virtuellen Server. Binden Sie dann jeden Dienst an seinen jeweiligen virtuellen Server.

Weitere Informationen zum Erstellen eines virtuellen Lastausgleichsservers finden Sie unter Erstellen eines virtuellen Lastausgleichsservers.

Weitere Informationen zur Konfiguration von Diensten, die den Cache-Server darstellen, finden Sie unter Konfigurieren eines HTTP-Dienstes.

Weitere Informationen zum Binden des Dienstes an einen virtuellen Server finden Sie unter Binden/Aufheben eines Dienstes an/von einem virtuellen Lastausgleichsserver.

Weitere Informationen zum Erstellen eines transparenten Proxy-Cache-Umleitungsservers finden Sie unter Konfigurieren eines virtuellen Cache-Umleitungsserversund Erstellen eines virtuellen Servers vom Typ TRANSPARENT.

Weitere Informationen zum Binden integrierter Cache-Umleitungsrichtlinien an den virtuellen Cache-Umleitungsserver finden Sie unter Binden von Richtlinien an den virtuellen Cache-Umleitungsserver.

Konfigurieren einer Cache-Umleitungsrichtlinie für einen bestimmten Inhaltstyp

Um Anforderungen mit einer Erweiterung GIF oder JPEG als zwischenspeicherbar zu identifizieren, konfigurieren Sie eine Cache-Umleitungsrichtlinie und binden sie an den virtuellen Server der Cache-Umleitung.

Hinweis: Wenn eine Anforderung mit einer Richtlinie übereinstimmt, leitet die Citrix ADC Appliance sie an den Ursprungsserver weiter. Daher konfigurieren Sie im folgenden Verfahren Richtlinien, um Anforderungen abzugleichen, die
keine Erweiterungen .png oder .jpeg haben.

Um die Cache-Umleitung für einen bestimmten Inhaltstyp zu konfigurieren, konfigurieren Sie eine Richtlinie, die einen einfachen Ausdruck verwendet, wie unter Cache-Umleitungsrichtlinie konfigurierenbeschrieben.

Konfigurieren von Richtlinien für Content Switching

October 5, 2021

Sie müssen eine Content Switching-Richtlinie erstellen, um bestimmte Inhaltstypen zu identifizieren, die in einem Cacheserver oder -farm zwischengespeichert werden sollen, und andere Inhaltstypen zu identifizieren, die von einem anderen Cacheserver oder -farm bereitgestellt werden sollen. Sie können beispielsweise eine Richtlinie konfigurieren, um den Speicherort für Bilddateien mit den Erweiterungen GIF und JPEG zu bestimmen.

Nachdem Sie die Content Switching-Richtlinie definiert haben, binden Sie sie an einen virtuellen Cache-Umleitungsserver und geben einen virtuellen Lastausgleichsserver an. Anforderungen, die der Richtlinie entsprechen, werden an den benannten virtuellen Lastausgleichsserver weitergeleitet. Anforderungen, die nicht mit der Content Switching-Richtlinie übereinstimmen, werden an den standardmäßigen virtuellen Lastausgleichsserver für den Cache weitergeleitet.

Weitere Informationen zur Funktion zum Content Switching und zum Konfigurieren von Richtlinien zum Content Switching finden Sie unter Content Switching.

Sie müssen zuerst die Content Switching-Richtlinie erstellen und dann an den virtuellen Cache-Umleitungsserver binden.

Erstellen einer Content Switching-Richtlinie über die CLI

Geben Sie in der Befehlszeile Folgendes ein:


```
-  add cs policy <policyName> [-url <string> | -rule <expression>]
-  show cs policy [<policyName>]
<!--NeedCopy-->
```

Beispiele:

```
> add cs policy Policy-CS-JPEG -rule ”REQ.HTTP.URL == '/\*.jpeg'”
 Done
> show cs policy Policy-CS-JPEG
         Rule: REQ.HTTP.URL == '/\*.jpeg'         Policy: Policy-CS-
            JPEG
         Hits: 0
 Done
>

> add cs policy Policy-CS-GIF -rule ”REQ.HTTP.URL == '/ *.png'”
 Done
> show cs policy Policy-CS-GIF
         Rule: REQ.HTTP.URL == '/ *.png'         Policy: Policy-CS-GIF
         Hits: 0
 Done
>

> add cs policy Policy-CS-JPEG-URL -url /\*.jpg
 Done
> show cs policy Policy-CS-JPEG-URL
         URL: /\*.jpg     Policy: Policy-CS-JPEG-URL
         Hits: 0
 Done
>

> add cs policy Policy-CS-GIF-URL -url /\*.png
 Done
> show cs policy Policy-CS-GIF-URL
         URL: /\*.png     Policy: Policy-CS-GIF-URL
         Hits: 0
 Done
<!--NeedCopy-->
```

Erstellen einer URL-basierten Content Switching-Richtlinie über die GUI

1. Navigieren Sie zu Traffic Management > Content Switching > Richtlinien.

2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld “Content Switching-Richtlinie erstellen” im Textfeld Name einen Namen für die Richtlinie ein.
4. Wählen Sie das Optionsfeld URL aus.
5. Geben Sie im Textfeld Wert den Zeichenfolgenwert ein (z. B. **/sports**).
6. Klicken Sie auf Erstellen und auf Schließen. Die erstellte Richtlinie wird auf der Seite “Content Switching-Richtlinien” angezeigt.

Erstellen einer regelbasierten Content Switching-Richtlinie über die GUI

1. Navigieren Sie zu Traffic Management > Content Switching > Richtlinien.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld “Content Switching-Richtlinie erstellen” im Textfeld Name einen Namen für die Richtlinie ein.
4. Wählen Sie das Optionsfeld Ausdruck aus, und klicken Sie dann auf Konfigurieren.
5. Wählen Sie im Dialogfeld Ausdruck erstellen die Ausdruckssyntax aus, die Sie verwenden möchten.

   - Wenn Sie die Standardsyntax verwenden möchten, übernehmen Sie die Standardsyntax und fahren Sie mit dem nächsten Schritt fort.
   - Wenn Sie die klassische Syntax verwenden möchten, klicken Sie auf Zur klassischen Syntax wechseln.

   Der Abschnitt Ausdruck des Dialogfelds ändert sich entsprechend Ihrer Wahl. Die Standardsyntax Ausdrucksansicht enthält weniger Elemente als die klassische Syntaxausdruckansicht. In der Standardsyntax Expression-Ansicht ermöglicht eine Schaltfläche anstelle eines Vorschaufenfensters den Zugriff auf einen Ausdrucksauswerter. Der Evaluator wertet den eingegebenen Ausdruck aus, um sicherzustellen, dass er gültig ist, und zeigt eine Analyse des Ausdrucks an.
6. Geben Sie Ihre Richtlinienausdrücke ein.

   Informationen zur Verwendung der erweiterten Syntax finden Sie unter Konfigurieren des erweiterten Richtlinienausdrucks: Erste Schritte.
7. Klicken Sie auf **Erstellen** und auf **Schließen**. Die erstellte Richtlinie wird im Bereich **Content Switching-Richtlinien** angezeigt.

Binden Sie die Content Switching-Richtlinie an einen virtuellen Cache-Umleitungsserver mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Content Switching-Richtlinie an einen virtuellen Cache-Umleitungsserver zu binden und die Konfiguration zu überprüfen:

```
-  bind cs vserver <name> <targetVserver> [-policyName <string>]
-  show cs vserver [<name>]
<!--NeedCopy-->
```

Beispiel:

```
> bind cs vserver Vserver-CR-1 lbcachejpeg -policyName Policy-CS-JPEG
 Done
> bind cs vserver Vserver-CR-1 lbcachegif -policyName Policy-CS-GIF
 Done
> show cs vserver Vserver-CR-1
        Vserver-CR-1 (10.102.29.60:80) - HTTP   Type: CONTENT
        State: UP
        Last state change was at Fri Jul  2 12:53:45 2010
        Time since last state change: 0 days, 00:00:58.920
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Port Rewrite : DISABLED
        State Update: DISABLED
        Default:        Content Precedence: RULE
        Cacheable: YES
        Vserver IP and Port insertion: OFF
        Case Sensitivity: ON
        Push: DISABLED  Push VServer:
        Push Label Rule: none

1)      Policy: Policy-CS-JPEG  Target: lbcachejpeg     Priority: 0
       Hits: 0
2)      Policy: Policy-CS-GIF   Target: lbcachegif      Priority: 0
       Hits: 0
 Done
>
<!--NeedCopy-->
```


Binden Sie die Content Switching-Richtlinie an einen virtuellen Cache-Umleitungsserver mit der GUI

1. Navigieren Sie zu **Verkehrsmanagement** > **Content Switching** > **Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie die Richtlinie binden möchten (z. B. **vServer-CS-1**), und klicken Sie dann auf **Öffnen**.
3. Klicken Sie im Dialogfeld Virtuellen Server konfigurieren (Content Switching) auf der Registerkarte **Richtlinien** auf CSW, und klicken Sie dann auf **Richtlinie einfügen** .
4. Wählen Sie in der Spalte **Richtlinienname** die Richtlinie aus, die Sie für den virtuellen Content Switching-Server konfigurieren möchten.
5. Klicken Sie in der Spalte **Ziel** auf den grünen Pfeil, und wählen Sie den virtuellen Zielserver für Lastenausgleich aus der Liste aus.
6. Klicken Sie auf **OK**.

Konfigurieren der Rangfolge für die Richtlinienbewertung

October 5, 2021

Sie können eine Content Switching-Richtlinie basierend auf einer Regel konfigurieren, bei der es sich um eine generische Konfiguration für verschiedene Inhaltstypen handelt, oder auf einer URL, die spezifischer ist und genau den Inhaltstyp definiert, der an einen bestimmten Cacheserver gesendet werden muss. Im Wesentlichen kann derselbe Inhalt entweder durch eine regelbasierte Richtlinie oder eine URL-basierte Richtlinie definiert werden.

Nachdem Sie Content Switching-Richtlinien eines beliebigen Typs an einen virtuellen Cache-Umleitungsserver gebunden haben, können Sie den virtuellen Server so konfigurieren, dass entweder regelbasierte oder URL-basierte Richtlinien Vorrang eingeräumt werden. Dies entscheidet wiederum, auf welche Server die jeweiligen Anfragen gerichtet sind.

Um die Priorität für die Richtlinienbewertung zu konfigurieren, verwenden Sie den Parameter precedence, der den Typ der Richtlinie (URL oder RULE) angibt, der Vorrang auf dem virtuellen Server zur Inhaltsumleitung hat.

Mögliche Werte: RULE, URL

Standardwert: RULE

Konfigurieren der Rangfolge für die Richtlinienbewertung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Priorität für die Richtlinienbewertung zu konfigurieren und die Konfiguration zu überprüfen:

```
-  set cr vserver <name> [-precedence (RULE | URL)]
-  show cr vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
> set cr vserver Vserver-CRD-1 -precedence URL
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
>
<!--NeedCopy-->
```

Konfigurieren der Rangfolge für die Richtlinienbewertung mit der GUI

1. Navigieren Sie zu Traffic Management > Content Switching > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie die Priorität konfigurieren möchten (z. B. **vServer-CS-1**), und klicken Sie dann auf Öffnen.
3. Klicken Sie im Dialogfeld “Virtuellen Server konfigurieren (Content Switching)” auf der Registerkarte Erweitert neben Priorität auf Regel oder URL, und klicken Sie dann auf OK.

Verwalten eines virtuellen Cache-Umleitungsservers

October 5, 2021

Um einen virtuellen Cache-Umleitungsserver zu verwalten, müssen Sie Cache-Umleitungsstatistiken anzeigen. Möglicherweise müssen Sie Cache-Umleitungsserver aktivieren oder deaktivieren oder Richtlinientreffer in den Cache anstelle des Ursprungs leiten. Zu den administrativen Aufgaben gehören auch das Sichern eines virtuellen Cache-Umleitungsservers und das Verwalten von Clientverbindungen.

Statistiken zum virtuellen Server zur Cache-Umleitung anzeigen

October 5, 2021

Sie können Eigenschaften eines virtuellen Cache-Umleitungsservers und Statistiken über den Datenverkehr anzeigen, der einen virtuellen Cache-Umleitungsserver durchlaufen hat. Sie können auch die virtuellen Server und Richtlinien für die Cache-Umleitung anzeigen, die Sie für den Lastenausgleich von virtuellen Servern gebunden haben.

Um Statistiken für bestimmte virtuelle Cache-Umleitungsserver anzuzeigen, geben Sie mithilfe des Name-Parameters den Namen des virtuellen Servers an, für den Statistiken angezeigt werden sollen. Andernfalls werden Statistiken für alle virtuellen Cache-Umleitungsserver angezeigt. Maximale Länge: 127

Anzeigen von Statistiken für einen virtuellen Cache-Umleitungsserver mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat cr vserver [<name>]
```

Beispiel:

```
1 > stat cr vserver Vserver-CRD-1
2
3 Vserver Summary
4                            IP  port     Protocol        State
5 Vser...CRD-1          0.0.0.0    80         HTTP           UP
6
7 VServer Stats:
8                                        Rate (/s)
                                            Total
```



```
 9  Requests                                                  0
                          0
10  Responses                                                 0
                          0
11  Request bytes                                             0
                          0
12  Response bytes                                            0
                          0
13
14   Done
15  >
16  <!--NeedCopy-->
```

Anzeigen von Statistiken für einen virtuellen Cache-Umleitungsserver mit der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie Statistiken anzeigen möchten (z. B. **vServer-CRD-1**), und klicken Sie dann auf Statistiken.

Geben Sie den Servernamen aus, um grundlegende Statistiken für alle virtuellen Cache-Umleitungsserver anzuzeigen. Geben Sie den Servernamen ein, um detaillierte Statistiken für diesen virtuellen Server anzuzeigen, einschließlich Anzahl und Größe der Anforderungen und Antworten, die den virtuellen Server durchlaufen

Anzeigen der Statistiken eines virtuellen Cache-Umleitungsservers mit der Überwachungs- und Dashboard-Dienstprogramme

1. Um die Statistiken mit der Überwachungsdienstprogramme anzuzeigen, klicken Sie auf die Registerkarte Überwachung.
2. Wählen Sie im Dropdownmenü Gruppe auswählen die Option Virtuelle CR Server. Eine Liste der virtuellen Cache-Umleitungsserver wird angezeigt.
3. Um die Statistiken mit der Dashboard-Dienstprogramme anzuzeigen, klicken Sie auf die Registerkarte Dashboard.
4. Klicken Sie neben Statistisches Dienstprogramm auf Applet Client oder Webstart-Client.
5. Wählen Sie im Dropdownmenü Gruppe auswählen die Option Virtuelle CR Server. Das Dashboard zeigt zusammenfassende Statistiken für die virtuellen Server der Cache-Umleitung an.
6. Klicken Sie auf Diagramm, um ein Diagramm der virtuellen Serveraktivität anzuzeigen. Eine grafische Darstellung der Statistiken des virtuellen Servers wird angezeigt.

Aktivieren oder Deaktivieren eines virtuellen Cache-Umleitungsservers

October 5, 2021

Wenn Sie einen virtuellen Cache-Umleitungsserver erstellen, ist er standardmäßig aktiviert. Wenn Sie einen virtuellen Cache-Umleitungsserver deaktivieren, ändert sich sein Status in OUT OF SERVICE, und es beendet die Umleitung von zwischengespeicherten Clientanforderungen. Die Citrix ADC Appliance reagiert jedoch weiterhin auf ARP- und Ping-Anforderungen für die IP-Adresse dieses virtuellen Servers.

Aktivieren oder Deaktivieren eines virtuellen Cache-Umleitungsservers mit der CLI

Geben Sie in der Befehlszeile einen der folgenden Befehle ein:

```
-  enable cr vserver <name>
-  show cr vserver <name>
-  disable cr vserver <name>
-  show cr vserver <name>
<!--NeedCopy-->
```

Beispiele:

```
> enable cr vserver Vserver-CRD-1
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
>

> disable cr vserver Vserver-CRD-1
 Done
```



```
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: OUT OF SERVICE  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: ORIGIN L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
>
<!--NeedCopy-->
```

Aktivieren oder Deaktivieren eines virtuellen Cache-Umleitungsservers mit der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server.
2. Erweitern Sie im Navigationsbereich Cache-Umleitung, und klicken Sie dann auf Virtuelle Server.
3. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie aktivieren oder deaktivieren möchten (z. B. **vServer-CRD-1**), und klicken Sie dann auf Statistiken.
4. Klicken Sie im Dialogfeld Fortfahren auf Ja.

Direkte Richtlinienanfragen zum Cache anstelle des Ursprungswebservers

October 5, 2021

Wenn eine Anforderung mit einer Richtlinie übereinstimmt, leitet die Citrix ADC Appliance die Anforderung standardmäßig entweder direkt an den Ursprungsserver oder an einen virtuellen Lastausgleichsserver für den Ursprung weiter, je nachdem, wie Sie die Cache-Umleitung konfiguriert haben.

Sie können das Standardverhalten so ändern, dass, wenn eine Anforderung mit einer Richtlinie übereinstimmt, die Anforderung an einen virtuellen Lastausgleichsserver für den Cache weitergeleitet wird.

Um das Ziel für eine Richtlinienanforderung an den Ursprung oder den Cache zu ändern, verwenden Sie den `onPolicyMatch` Parameter, der angibt, wohin Anforderungen gesendet werden sollen, die der Cache-Umleitungsrichtlinie entsprechen.

Die gültigen Optionen sind:

1. CACHE - Leitt alle übereinstimmenden Anfragen an den Cache weiter.
2. ORIGIN - Leitt alle übereinstimmenden Anfragen an den Ursprungsserver weiter.

> **Hinweis:**
>
> Damit diese Option funktioniert, müssen Sie den Cache-Umleitungstyp als auswählen POLICY.

Mögliche Werte: CACHE, ORIGIN

Standardwert:ORIGIN

Ändern Sie das Ziel für eine Richtlinienanforderung mit der CLI in den Ursprung oder den Cache

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um das Ziel für einen Richtlinientreffer zu ändern und die Konfiguration zu überprüfen:

```
set cr vserver <name> [-onPolicyMatch (ORIGIN | CACHE)]
<!--NeedCopy-->
```

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

Beispiel:

```
> set cr vserver Vserver-CRD-1 -onPolicyMatch CACHE
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```


Ändern des Ziels für einen Richtlinientreffer auf den Ursprung oder den Cache mit der GUI

1. Navigieren Sie zu **Traffic Management > Cache-Umleitung > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie das Ziel für eine Richtlinienanforderung ändern möchten (z. B. **vServer-CRD-1**), und klicken Sie dann auf Öffnen.
3. Klicken **Sie im Dialogfeld Virtuellen Server konfigurieren (Cache-Umleitung)** auf **Erweitert**.
4. Wählen Sie **CACHE** oder **ORIGIN** aus der Dropdownliste **Umleiten zu** aus.
5. Klicken Sie auf **OK**.

Sichern eines virtuellen Cache-Umleitungsservers

October 5, 2021

Die Cache-Umleitung kann fehlschlagen, wenn der primäre virtuelle Server ausfällt oder übermäßigen Datenverkehr nicht verarbeiten kann. Sie können einen virtuellen Sicherungsserver angeben, der die Verarbeitung des Datenverkehrs übernimmt, wenn der primäre virtuelle Server ausfällt.

Um einen virtuellen Backup-Cache-Umleitungsserver anzugeben, verwenden Sie den Parameter BackupVServer, der den virtuellen Backup-Server angibt. Maximale Länge: 127

Angeben eines virtuellen Backup-Cache-Umleitungsservers mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen virtuellen Backup-Cache-Umleitungsserver anzugeben und die Konfiguration zu überprüfen:

```
-  set cr vserver <name> [-backupVServer <string>]
-  show cr vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
> set cr vserver Vserver-CRD-1 -backupVServer Vserver-CRD-2
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
```



```
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```

Angeben eines virtuellen Backup-Cache-Umleitungsservers mit der GUI

1. Navigieren Sie zu **Traffic Management > Cache-Umleitung > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie das Ziel für eine Richtlinienanforderung ändern möchten (z. B. **vServer-CRD-1**), und klicken Sie dann auf Öffnen.
3. Wählen Sie im Dialogfeld Virtuellen Server konfigurieren (Cache-Umleitung) die Registerkarte Erweitert aus.
4. Wählen Sie in der Dropdownliste Virtueller Server sichern den virtuellen Server aus.
5. Klicken Sie auf OK.

Verwalten von Clientverbindungen für einen virtuellen Server

October 5, 2021

Sie können Timeouts auf einem virtuellen Cache-Umleitungsserver so konfigurieren, dass Clientverbindungen nicht unbegrenzt geöffnet bleiben. Sie können auch Via Header in Anforderungen einfügen. Um die Netzwerküberlastung möglicherweise zu reduzieren, können Sie offene TCP-Verbindungen wiederverwenden. Sie können die verzögerte Bereinigung von virtuellen Serververbindungen für die Cache-Umleitung aktivieren oder deaktivieren.

Sie können die Appliance so konfigurieren, dass ICMP-Antworten an PING-Anforderungen gemäß Ihren Einstellungen gesendet werden. Legen Sie auf der IP-Adresse, die dem virtuellen Server entspricht, ICMP RESPONSE auf VSVR_CNTRLD fest, und legen Sie auf dem virtuellen Server den ICMP VSERVER RESPONSE fest.

Die folgenden Einstellungen können auf einem virtuellen Server vorgenommen werden:

- Wenn Sie ICMP VSERVER RESPONSE auf allen virtuellen Servern auf PASSIVE festlegen, reagiert die Appliance immer.

- Wenn Sie ICMP VSERVER RESPONSE auf allen virtuellen Servern auf ACTIVE festlegen, reagiert die Appliance selbst dann, wenn ein virtueller Server UP ist.
- Wenn Sie ICMP VSERVER RESPONSE für einige auf ACTIVE und für andere PASSIVE festlegen, reagiert die Appliance selbst dann, wenn ein virtueller Server, der auf ACTIVE eingestellt ist, auf UP eingestellt ist.

Dieses Dokument enthält die folgenden Informationen:

- Client-Timeout konfigurieren
- Via Header in die Anforderungen einfügen
- TCP-Verbindungen wiederverwenden
- Konfigurieren verzögerter Verbindungsbereinigung

Client-Timeout konfigurieren

Sie können den Ablauf von Clientanforderungen angeben, indem Sie einen Timeoutwert für den virtuellen Cache-Umleitungsserver festlegen. Der Zeitüberschreitungswert ist die Anzahl der Sekunden, für die der virtuelle Cache-Umleitungsserver wartet, um eine Antwort für die Clientanforderung zu erhalten.

Um einen Timeoutwert zu konfigurieren, verwenden Sie den Parameter CLTTimeout, der die Zeit in Sekunden angibt, nach der die Citrix ADC Appliance alle ungenutzten Clientverbindungen schließt. Der Standardwert ist 180sec für HTTP/SSL-basierte Dienste und 9000sec für TCP-basierte Dienste.

Konfigurieren des Client-Timeouts mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um das Client-Timeout zu konfigurieren und die Konfiguration zu überprüfen:

```
-  set cr vserver <name> [-cltTimeout <secs>]
-  show cr vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
> set cr vserver Vserver-CRD-1 -cltTimeout 6000
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
```



```
6          Client Idle Timeout: 6000 sec
7          Down state flush: ENABLED
8          Disable Primary Vserver On Down : DISABLED
9          Default:        Content Precedence: URL Cache: TRANSPARENT
10         On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
11         Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
12         Backup: Vserver-CRD-2
13
14 1)      Cache bypass  Policy: bypass-cache-control
15 2)      Cache bypass  Policy: Policy-CRD
16  Done
17 <!--NeedCopy-->
```

Konfigurieren des Client-Timeouts mit der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie das Client-Timeout konfigurieren möchten (z. B. **vServer-CRD-1**), und klicken Sie dann auf Öffnen.
3. Wählen Sie im Dialogfeld Virtuellen Server konfigurieren (Cache-Umleitung) die Registerkarte Erweitert aus.
4. Geben Sie im Textfeld Client-Timeout (Sekunden) den Zeitüberschreitungswert in Sekunden ein.
5. Klicken Sie auf OK.

Via Header in die Anforderungen einfügen

Ein Va-Header listet die Protokolle und Empfänger zwischen den Start- und Endpunkten für eine Anforderung oder eine Antwort auf und informiert den Server über Proxys, über die die Anforderung gesendet wurde. Sie können den virtuellen Cache-Umleitungsserver so konfigurieren, dass er in jede HTTP-Anforderung einen Va-Header einfügt. Der Parameter via ist standardmäßig aktiviert, wenn Sie einen virtuellen Cache-Umleitungsserver erstellen.

Um das Einfügen von VIA-Header in Client-Anforderungen zu aktivieren oder zu deaktivieren, verwenden Sie den Parameter via, der den Zustand des Systems beim Einfügen eines Va-Headers in die HTTP-Anfragen angibt.

Mögliche Werte: ON, OFF

Standardwert: ON

Aktivieren oder Deaktivieren der VIA-Header-Einfügung in Client-Anforderungen mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
-  set cr vserver <name> [-via (ON|OFF)]
-  show cr vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
> set cr vserver Vserver-CRD-1 -via ON
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
>
<!--NeedCopy-->
```

Aktivieren oder Deaktivieren der VIA-Header-Einfügung in Client-Anforderungen mit der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie das Client-Timeout konfigurieren möchten (z. B. **vServer-CRD-1**), und klicken Sie dann auf Öffnen.
3. Wählen Sie im Dialogfeld Virtuellen Server konfigurieren (Cache-Umleitung) die Registerkarte Erweitert aus.
4. Aktivieren Sie das Kontrollkästchen Via.
5. Klicken Sie auf OK.

TCP-Verbindungen wiederverwenden

Sie können die Citrix ADC Appliance so konfigurieren, dass TCP-Verbindungen zum Cache- und Ursprungsserver über Clientverbindungen hinweg wiederverwendet werden. Dies kann die Leistung

verbessern, indem Sie die Zeit spart, die für die Einrichtung einer Sitzung zwischen dem Server und der Appliance erforderlich ist. Die Option Wiederverwendung ist standardmäßig aktiviert, wenn Sie einen virtuellen Cache-Umleitungsserver erstellen.

Um die Wiederverwendung von TCP-Verbindungen zu aktivieren oder zu deaktivieren, verwenden Sie den Wiederverwendungsparameter, der den Wiederverwendungszustand von TCP-Verbindungen zum Cache- oder Ursprungsserver über Clientverbindungen hinweg angibt.

Mögliche Werte: ON, OFF

Standardwert: ON

Aktivieren oder Deaktivieren der Wiederverwendung von TCP-Verbindungen mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
-  set cr vserver <name> [-reuse (ON|OFF)]
-  show cr vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
> set cr vserver Vserver-CRD-1 -reuse ON
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Default:        Content Precedence: URL Cache: TRANSPARENT
        On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
        Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
        Backup: Vserver-CRD-2

1)      Cache bypass  Policy: bypass-cache-control
2)      Cache bypass  Policy: Policy-CRD
 Done
<!--NeedCopy-->
```


Aktivieren oder Deaktivieren der Wiederverwendung von TCP-Verbindungen mit der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie das Client-Timeout konfigurieren möchten (z. B. **vServer-CRD-1**), und klicken Sie dann auf Öffnen.
3. Wählen Sie im Dialogfeld Virtuellen Server konfigurieren (Cache-Umleitung) die Registerkarte Erweitert aus.
4. Aktivieren Sie das Kontrollkästchen Wiederverwenden.
5. Klicken Sie auf OK.

Konfigurieren verzögerter Verbindungsbereinigung

Die Option Down-State-Flush führt verzögerte Bereinigung von Verbindungen auf einem virtuellen Cache-Umleitungsserver durch. Die Option Downstate Flush ist standardmäßig aktiviert, wenn Sie einen virtuellen Cache-Umleitungsserver erstellen.

Um die Downstatusbereinigungsoption zu aktivieren oder zu deaktivieren, legen Sie den DownStateFlush-Parameter fest.

Mögliche Werte: ENABLED, DISABLED

Standardwert: ENABLED

Aktivieren der Deaktivierung der Down-State-Flush-Option mit der CLI

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

```
-  set cr vserver <name> [-downStateFlush (ENABLED | DISABLED)]
-  show cr vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
> set cr vserver Vserver-CRD-1 -downStateFlush ENABLED
 Done
> show cr vserver Vserver-CRD-1
        Vserver-CRD-1 (*:80) - HTTP     Type: CONTENT
        State: UP  ARP:DISABLED
        Client Idle Timeout: 6000 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
```



```
9          Default:        Content Precedence: URL Cache: TRANSPARENT
10         On Policy Match: CACHE  L2Conn: OFF     OriginUSIP: OFF
11         Redirect: POLICY        Reuse: ON       Via: ON ARP: OFF
12         Backup: Vserver-CRD-2
13
14 1)      Cache bypass  Policy: bypass-cache-control
15 2)      Cache bypass  Policy: Policy-CRD
16  Done
17 <!--NeedCopy-->
```

Aktivieren oder Deaktivieren der Wiederverwendung von TCP-Verbindungen mit der GUI

1. Navigieren Sie zu Traffic Management > Cache-Umleitung > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie das Client-Timeout konfigurieren möchten (z. B. **vServer-CRD-1**), und klicken Sie dann auf Öffnen.
3. Klicken Sie im Dialogfeld Virtuellen Server konfigurieren (Cache-Umleitung) auf Erweitert.
4. Aktivieren Sie das Kontrollkästchen “Down State Flush”.
5. Klicken Sie auf OK.

Externe TCP-Zustandsprüfung für virtuelle UDP-Server aktivieren

October 5, 2021

In Public Clouds können Sie die Citrix ADC Appliance als Load Balancer der zweiten Ebene verwenden, wenn der native Load Balancer als erste Stufe verwendet wird. Der native Load Balancer kann ein Application Load Balancer (ALB) oder ein Network Load Balancer (NLB) sein. Die meisten Public Clouds unterstützen keine UDP-Integritätstrübe in ihren nativen Lastausgleichsdiensten. Um die Integrität der UDP-Anwendung zu überwachen, empfehlen Public Clouds, Ihrem Dienst einen TCP-basierten Endpunkt hinzuzufügen. Der Endpunkt spiegelt die Integrität der UDP-Anwendung wider.

Die Citrix ADC Appliance unterstützt externe TCP-basierte Integritätsprüfung für einen virtuellen UDP-Server. Mit dieser Funktion wird ein TCP-Listener auf der VIP des virtuellen Cacheumleitungsservers und des konfigurierten Ports eingeführt. Der TCP-Listener gibt den Status des virtuellen Servers wieder.

So aktivieren Sie die externe TCP-Zustandsprüfung für virtuelle UDP-Server über die Befehlszeile

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine externe TCP-Integritätsprüfung mit der Option TCPProbePort zu aktivieren:


```
add cr vserver <name> <serviceType> -tcpProbePort <tcpProbePort>

<!--NeedCopy-->
```

Beispiel:

```
add cr vserver Vserver-CR-1 HTTP -tcpProbePort 80
<!--NeedCopy-->
```

So aktivieren Sie die externe TCP-Zustandsprüfung für virtuelle UDP-Server mit der GUI

1. Navigieren Sie zu **Datenverkehrsverwaltung > Cacheumleitung > Virtuelle Server**, und erstellen Sie dann einen virtuellen Server.
2. Klicken Sie auf **Hinzufügen**, um einen virtuellen Server zu erstellen.
3. Fügen Sie im Bereich **Grundeinstellungen** die Portnummer im Feld **TCP-Probe-Port** hinzu.
4. Klicken Sie auf **OK**.

N-Tier-Cache-Umleitung

October 5, 2021

Um große Mengen zwischengespeicherter Daten, in der Regel mehrere Gigabyte pro Sekunde, effizient zu verarbeiten, stellt ein Internetdienstanbieter mehrere dedizierte Cacheserver bereit. Die Cache-Umleitungsfunktion der Citrix ADC Appliance kann den Lastausgleich der Cacheserver erleichtern, aber eine einzelne Appliance oder ein paar Appliances kann das große Datenvolumen nicht effizient verarbeiten.

Sie können das Problem lösen, indem Sie die Citrix ADC Appliances auf zwei Tiers (Ebenen) bereitstellen, wobei die Upper-Tier-Appliances Load Balancing mit den Lower-Tier-Appliances und Lower-Tier-Appliances Load Balancing mit dem Cacheserver durchführen. Diese Anordnung wird *n-Tier-Cache-Umleitung*genannt.

Zu Zwecken wie Auditing und Sicherheit muss ein ISP Client-Details wie die IP-Adresse, die bereitgestellten Informationen und den Zeitpunkt der Interaktion verfolgen. Daher müssen Clientverbindungen über eine Citrix ADC Appliance vollständig transparent sein. Wenn Sie jedoch die transparente Cache-Umleitung konfigurieren, wobei die Citrix ADC Appliances parallel bereitgestellt

werden, muss die IP-Adresse des Clients für alle Appliances freigegeben werden. Die Freigabe der Client-IP-Adresse führt zu einem Konflikt, der dazu führt, dass Netzwerkgeräte wie Router, Cacheserver, Ursprungsserver und andere Citrix ADC Appliances die Appliance und damit den Client, an den die Antwort gesendet werden soll, nicht ermitteln können.

Implementierung der n-Tier-Cache-Umleitung

Um das Problem zu lösen, teilt die Appliance n-Tier-Cache-Umleitung den Quellportbereich auf die Appliances der unteren Ebene auf und schließt die Client-IP-Adresse in die Anforderung ein, die an die Cacheserver gesendet wird. Die Citrix ADC Upper-Tier-Appliances sind so konfiguriert, dass sie einen sitzungslosen Lastausgleich durchführen, um unnötige Auslastung der Appliances zu vermeiden.

Wenn die Citrix ADC Lower-Tier-Appliance mit einem Cacheserver kommuniziert, verwendet sie eine zugeordnete IP-Adresse (MIP), um die Quell-IP-Adresse darzustellen. Daher kann der Cacheserver die Appliance identifizieren, von der er die Anforderung empfangen hat, und die Antwort an dieselbe Appliance senden.

Die Citrix ADC Lower-Tier-Appliance fügt die Client-IP-Adresse in den Header der Anforderung ein, die an den Cacheserver gesendet wird. Die Client-IP im Header hilft der Appliance, den Client zu bestimmen, an den das Paket weitergeleitet werden soll, wenn es die Antwort von einem Cacheserver empfängt, oder den Ursprungsserver im Falle eines Cache-Fehlers. Der Ursprungsserver bestimmt die Antwort, die gesendet werden soll, entsprechend der Client-IP, die in den Request-Header eingefügt ist.

Der Ursprungsserver sendet die Antwort an eine Upper-Tier-Appliance, einschließlich der Quellportnummer, von der der Ursprungsserver die Anforderung empfangen hat. Der gesamte Quellportbereich (1024 bis 65535) wird auf die Citrix ADC Lower-Tier-Appliances verteilt. Jeder Lower-Tier-Appliance wird ausschließlich eine Gruppe von Adressen innerhalb des Bereichs zugewiesen. Mit dieser Zuteilung kann die Upper-Tier-Appliance eindeutig die Citrix ADC Lower-Tier-Appliance identifizieren, die die Anforderung an den Ursprungsserver gesendet hat. Die Upper-Tier-Appliance kann daher die Antwort an die richtige Lower-Tier-Appliance weiterleiten.

Die Citrix ADC Upper-Tier-Appliance sind für richtlinienbasiertes Routing konfiguriert, und die Routingrichtlinien werden definiert, um die IP-Adresse der Ziel-Appliance aus dem Quellportbereich zu bestimmen.

Zur Konfiguration der N-Tier-CRD erforderliche Einrichtung

Das folgende Setup ist für das Funktionieren der n-Tier-Cache-Umleitung erforderlich:

Für jede Citrix ADC Upper-Tier-Appliance:

- Aktivieren Sie den Layer-3-Modus.

- Definieren Sie Richtlinien für richtlinienbasierte Routen (PBRs), damit der Datenverkehr entsprechend dem Bereich des Zielports weitergeleitet wird.
- Konfigurieren Sie einen virtuellen Lastenausgleichsserver.
- Konfigurieren Sie den virtuellen Server so, dass er den gesamten Datenverkehr vom Client abhört. Legen Sie den Diensttyp/das Protokoll auf ANY und die IP-Adresse als Sternchen (*) fest.
- Aktivieren Sie den sitzungslosen Lastausgleich mit dem MAC-basierten Umleitungsmodus, um unnötige Auslastung der Citrix ADC Upper-Tier-Appliance zu vermeiden.
- Stellen Sie sicher, dass die Option Proxyport verwenden aktiviert ist.
- Erstellen Sie einen Dienst für jede Lower-Tier-Appliance, und binden Sie alle Dienste an den virtuellen Server.

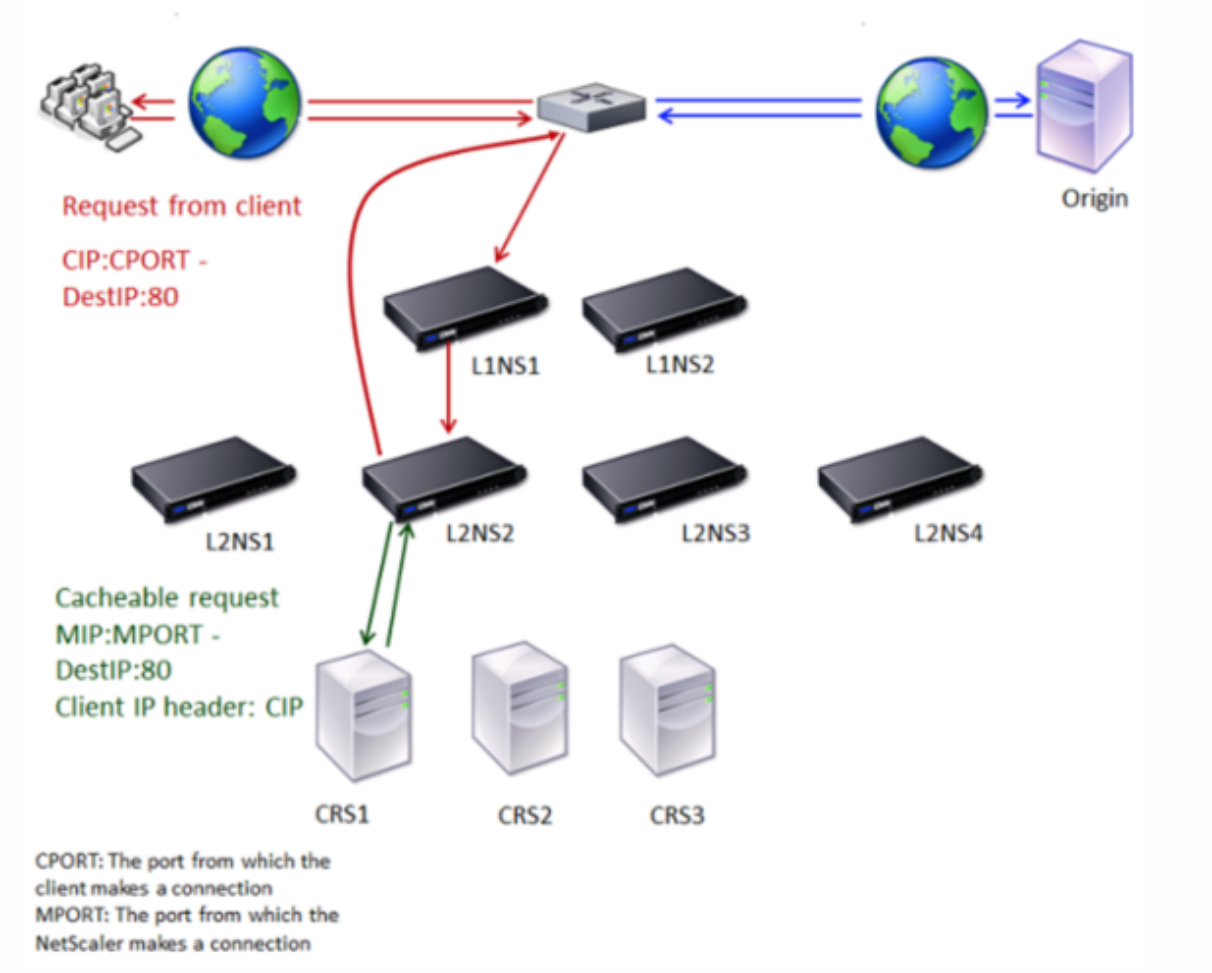
Für jede Citrix ADC Lower-Tier-Appliance:

- Konfigurieren Sie den Portbereich für die Cache-Umleitung auf der Appliance. Weisen Sie jeder Lower-Tier-Appliance einen exklusiven Bereich zu.
- Konfigurieren Sie einen virtuellen Lastausgleichsserver und aktivieren Sie die MAC-basierte Umleitung.
- Erstellen Sie einen Dienst für jeden Cacheserver, der von dieser Appliance geladen werden soll. Aktivieren Sie beim Erstellen des Dienstes das Einfügen der Client-IP in den Header. Binden Sie dann alle Dienste an den virtuellen Lastausgleichsserver.
- Konfigurieren Sie einen virtuellen Server zur Cache-Umleitung im transparenten Modus mit den folgenden Einstellungen:
  - Aktivieren Sie die Option Origin USIP.
  - Fügen Sie einen Quell-IP-Ausdruck hinzu, um die Client-IP in den Header aufzunehmen.
  - Aktivieren Sie die Option Portbereich verwenden.

Funktionsweise der n-Tier-Cache-Umleitung während eines Cache-Treffers

Die folgende Abbildung zeigt, wie die Cache-Umleitung funktioniert, wenn eine Clientanforderung zwischengespeichert werden kann und die Antwort von einem Cacheserver gesendet wird.

Abbildung 1. Cache-Umleitung bei einem Cache-Treffer



Zwei Citrix ADC Appliances, L1NS1 und L1NS2, werden in der oberen Ebene bereitgestellt, und vier Citrix ADC Appliances, L2NS1, L2NS2, L2NS3 und L2NS4, werden in der unteren Ebene bereitgestellt. Client A sendet eine Anforderung, die vom Router weitergeleitet wird. Cacheserver CRS1, CRS2 und CRS3 dienen die Cache-Anforderungen. Origin Server O betretet die nicht gespeicherten Anforderungen.

Verkehrsfluss

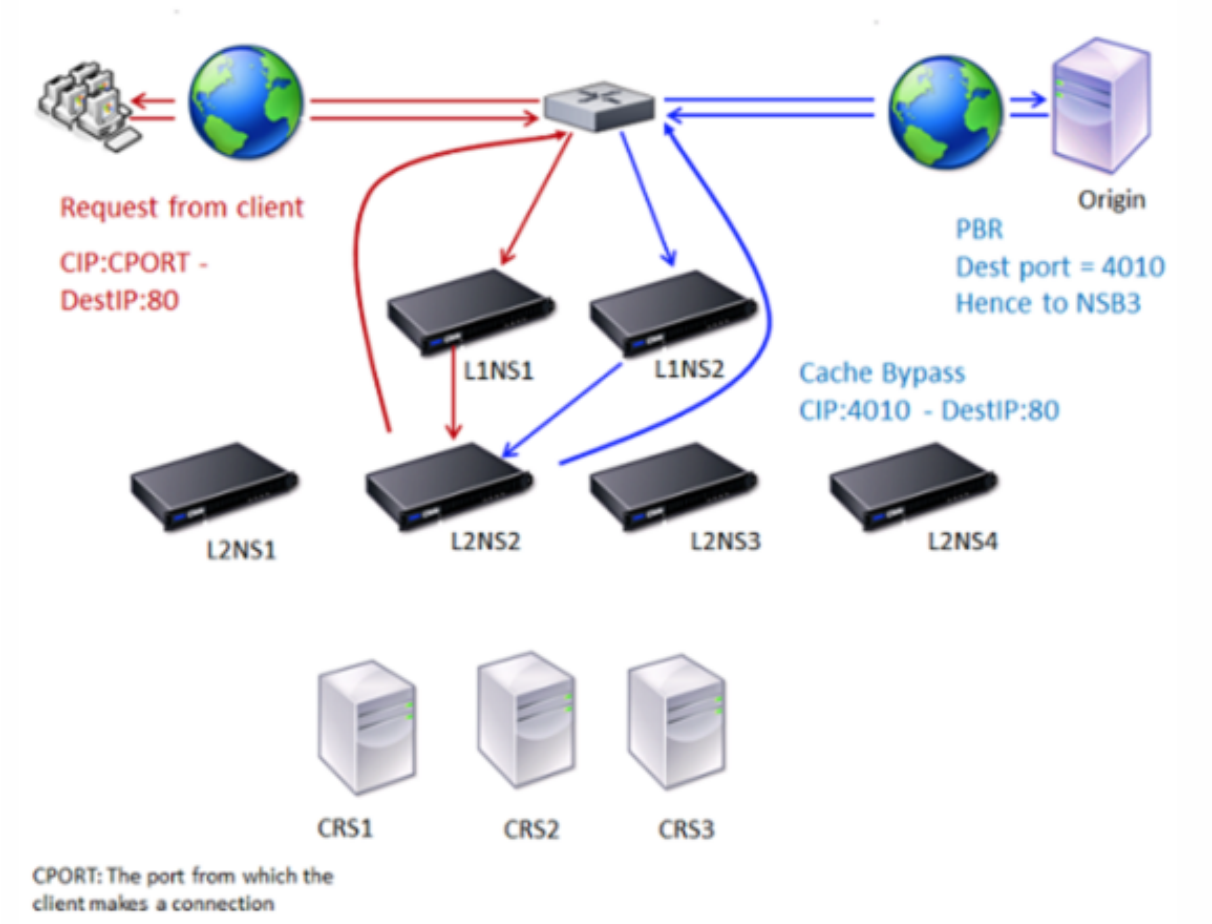
1. Client sendet eine Anforderung und der Router leitet sie an L1NS1 weiter.
2. L1NS1-Lastverteilung der Anforderung an L2NS2.
3. L2NS2-Lastverteilung der Anforderung an den Cacheserver CRS1, und die Anforderung kann zwischengespeichert werden. L2NS2 enthält die Client-IP in den Anforderungs-Header.
4. CRS1 sendet die Antwort an L2NS2, da L2NS2 seine MIP als Quell-IP-Adresse beim Herstellen einer Verbindung mit CRS1 verwendet hat.
5. Mit Hilfe der Client-IP-Adresse im Request-Header identifiziert L2NS2 den Client, von dem die Anforderung stammt. L2NS2 sendet die Antwort direkt an den Router, wodurch unnötige Belastung der Appliance in der oberen Ebene vermieden wird.

6. Der Router leitet die Antwort an Client A weiter.

Funktionsweise der n-Tier-Cache-Umleitung während einer Cache-Umgehung

Die folgende Abbildung zeigt, wie die Cache-Umleitung funktioniert, wenn eine Clientanforderung an einen Ursprungsserver für eine Antwort gesendet wird.

Abbildung 2. Cache-Umleitung bei Cache-Umgehung



Zwei Citrix ADC Appliances, L1NS1 und L1NS2, werden in der oberen Ebene bereitgestellt, und vier Citrix ADC Appliances, L2NS1, L2NS2, L2NS3 und L2NS4, werden in der unteren Ebene bereitgestellt. Client A sendet eine Anforderung, die vom Router weitergeleitet wird. Cacheserver CRS1, CRS2 und CRS3 dienen die Cache-Anforderungen. Origin Server O betretet die nicht gespeicherten Anforderungen.

Verkehrsfluss

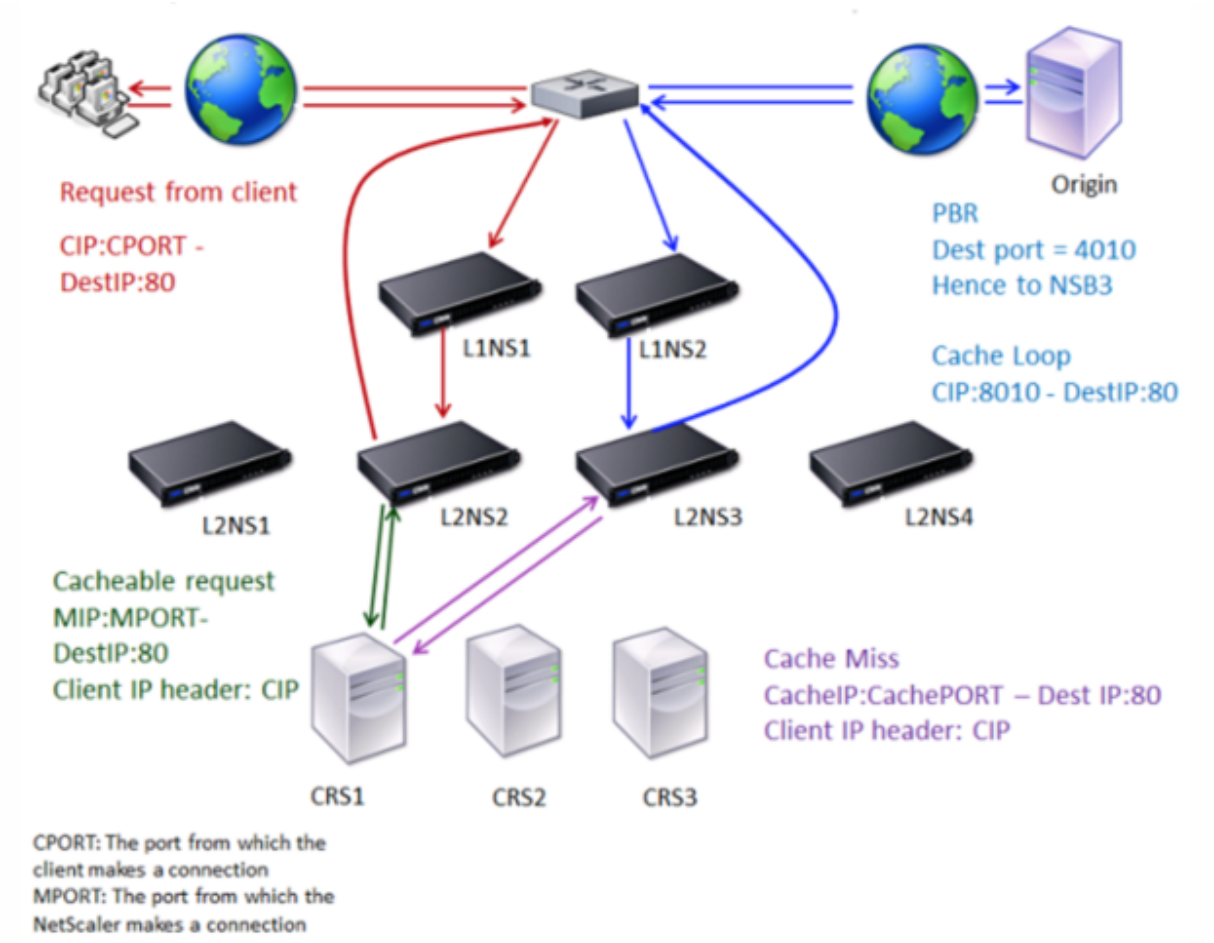
1. Client sendet eine Anforderung und der Router leitet sie an L1NS1 weiter.
2. L1NS1-Lastverteilung der Anforderung an L2NS2.

3. Die Anforderung ist nicht möglich (Cache-Bypass). Daher sendet L2NS2 die Anforderung über den Router an den Ursprungsserver.
4. Der Ursprungsserver sendet die Antwort an eine Upper-Tier-Appliance, L1NS2.
5. Gemäß den PBR-Richtlinien leitet L1NS2 den Datenverkehr an die entsprechende Appliance in der unteren Ebene L2NS2 weiter.
6. L2NS2 verwendet die Client-IP-Adresse im Anforderungs-Header, um den Client zu identifizieren, von dem die Anforderung stammt, und sendet die Antwort direkt an den Router, wodurch unnötige Belastung der Appliance in der oberen Ebene vermieden wird.
7. Der Router leitet die Antwort an Client A weiter.

Funktionsweise der n-Tier-Cache-Umleitung während eines Cache-Fehlers

Die folgende Abbildung zeigt, wie Cache-Umleitung funktioniert, wenn eine Clientanforderung nicht zwischengespeichert wird.

Abbildung 3. Cache-Umleitung im Falle eines Cache-Fehlers



Zwei Citrix ADC Appliances, L1NS1 und L1NS2, werden in der oberen Ebene bereitgestellt, und vier Citrix ADC Appliances, L2NS1, L2NS2, L2NS3 und L2NS4, werden in der unteren Ebene bereitgestellt.

Client A sendet eine Anforderung, die vom Router weitergeleitet wird. Cacheserver CRS1, CRS2 und CRS3 dienen die Cache-Anforderungen. Origin Server O betretet die nicht gespeicherten Anforderungen.

Verkehrsfluss

1. Client sendet eine Anforderung und der Router leitet sie an L1NS1 weiter.
2. L1NS1-Lastverteilung der Anforderung an L2NS2.
3. L2NS2-Lastverteilung der Anforderung an den Cacheserver CRS1, da die Anforderung zwischengespeichert werden kann.
4. CRS1 hat nicht die Antwort (Cache Miss). CRS1 leitet die Anforderung an den Ursprungsserver über die Appliance in der unteren Ebene weiter. L2NS3 fängt den Datenverkehr ab.
5. L2NS3 übernimmt die Client-IP aus dem Header und leitet die Anforderung an den Ursprungsserver weiter. Der im Paket enthaltene Quellport ist der L2NS3-Port, von dem die Anforderung an den Ursprungsserver gesendet wird.
6. Der Ursprungsserver sendet die Antwort an eine Upper-Tier-Appliance, L1NS2.
7. Gemäß den PBR-Richtlinien leitet L1NS2 den Datenverkehr an die entsprechende Appliance in der unteren Ebene L2NS3 weiter.
8. L2NS3 leitet die Antwort an den Router weiter.
9. Der Router leitet die Antwort an Client A weiter.

Konfigurieren der Citrix ADC Upper-Tier-Appliances

October 5, 2021

Konfigurieren Sie die Citrix ADC Upper-Tier-Appliances wie folgt.

Konfigurieren einer Upper-Tier-Appliance für die n-Tier-Cache-Umleitung mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add service \<name\>@ \<serviceIP\> \<serviceType\> \<port\>`

  Führen Sie diesen Befehl für jeden hinzuzufügenden Dienst aus.

- `add lb vserver \<name\>@ ANY \* \<port\> -persistenceType \<persistenceMethod \> -lbMethod \<lbMethod\> -m MAC -sessionless ENABLED -cltTimeout \< client\\_Timeout\\_Value\>`

- `bind lb vserver \<name\>@ \<serviceName\>`

  Führen Sie diesen Befehl für jeden zu gebundenen Dienst aus.

- `enable ns mode l3`
- `add ns pbr \<name\> \<action\> -srcPort \<sourcePortNumber\> -destPort \<startPortNumber-endPortNumber\> -nexthop \<serviceIpAddress\> -protocol TCP`
- `apply ns pbrs`

  Führen Sie diesen Befehl aus, nachdem Sie alle erforderlichen PBRs hinzugefügt haben.

Konfigurieren einer Upper-Tier-Appliance für die n-Tier-Cache-Umleitung mit der GUI

1. L3-Modus aktivieren:
   a) Klicken Sie im Navigationsbereich auf System, und klicken Sie dann auf Einstellungen.
   b) Klicken Sie in der Gruppe Einstellungen auf den Link Modi konfigurieren.
   c) Aktivieren Sie das Kontrollkästchen Layer 3-Modus (IP-Weiterleitung).
   d) Klicken Sie auf OK.
2. Konfigurieren Sie richtlinienbasiertes Routing (PBR):
   a) Navigieren Sie zu System > Netzwerk > PBRs.
   b) Klicken Sie im Bereich Policy-Based Routing (PBRs) auf Hinzufügen.
   c) Geben Sie einen Namen für die PBR ein.
   d) Wählen Sie die Aktion als Zulassen aus.
   e) Geben Sie im Feld Nächster Hop die IP-Adresse des Dienstes ein, der eine Lower-Tier-Appliance darstellt.
   f) Wählen Sie TCP aus der Dropdownliste Protokoll aus.
   g) Geben Sie den Quellport und den Bereich des Zielports ein, der der hinzuzufügenden Lower-Tier-Appliance entspricht.
   h) Klicken Sie auf Erstellen.
   i) Wählen Sie im Detailbereich die PBR aus, und klicken Sie auf Übernehmen.
   j) Wiederholen Sie Schritt i bis Schritt vii für jede Lower-Tier-Appliance.
3. Erstellen Sie einen Service für jede Lower-Tier-Appliance:
   a) Navigieren Sie zu Traffic Management > Load Balancing > Services.
   b) Klicken Sie im Detailbereich auf “Hinzufügen”.
   c) Geben Sie den Namen, das Protokoll, die IP-Adresse und den Port an. Das Protokoll sollte ANY sein.
   d) Klicken Sie auf Erstellen.
4. Konfigurieren Sie einen virtuellen Lastausgleichsserver:
   a) Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
   b) Klicken Sie im Detailbereich auf “Hinzufügen”.
   c) Geben Sie den Namen, das Protokoll, die IP-Adresse und den Port an. Das Protokoll sollte ANY und die IP-Adresse sollte * sein.

d) Wählen Sie auf der Registerkarte Dienste die Dienste aus, die die Citrix ADC Lower-Tier-Appliances darstellen.
e) Aktivieren Sie auf der Registerkarte Erweitert den Umleitungsmodus als MAC-basiert und aktivieren Sie das Kontrollkästchen Sitzungslos.
f) Klicken Sie auf Erstellen.

Konfigurieren der Citrix ADC Lower-Tier-Appliances

October 5, 2021

Konfigurieren Sie jede der Citrix ADC Lower-Tier-Appliances wie folgt.

Konfigurieren einer Lower-Tier-Appliance für die n-Tier-Cache-Umleitung mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- `add service <name>@ <cacheServiceIP> <serviceType> <port> -cip ENABLED "ClientIP"-cachetype transparent`

  Wiederholen Sie den Vorgang für jeden Cacheserver.

- `add lb vserver <name>@ <serviceType> -m MAC`
- `bind lb vserver <name>@ <cacheServiceName>`

  Wiederholen Sie den Vorgang für jeden Cacheserver.

- `add cr vserver <name> <serviceType> * <port> -srcIPExpr "HTTP.REQ. HEADER("ClientIP")"-originusip ON -usePortRange ON`
- `set ns param-crPortRange <startPortNumber-endPortNumber>`

Konfigurieren einer Lower-Tier-Appliance für die n-Tier-Cache-Umleitung mit der GUI

1. Erstellen Sie einen Dienst für jeden Cacheserver. So erstellen Sie einen Service:
   a) Navigieren Sie zu Traffic Management > Load Balancing > Services.
   b) Klicken Sie im Detailbereich auf Hinzufügen, und geben Sie den Namen und das Protokoll an. Deaktivieren Sie das Kontrollkästchen Direkt adressierbar.
   c) Aktivieren Sie auf der Registerkarte Erweitert das Kontrollkästchen Global überschreiben und Client-IP, und geben Sie dann im Feld Header ClientIP ein.
   d) Wählen Sie im Feld Cachetyp die Option Transparenter Cache aus.
   e) Klicken Sie auf Erstellen.
2. Konfigurieren Sie einen virtuellen Lastausgleichsserver:

a) Navigieren Sie zu Traffic Management > Load Balancing > Virtual Services.
b) Klicken Sie im Detailbereich auf Hinzufügen, und geben Sie den Namen, das Protokoll, die IP-Adresse und den Port an. Die IP-Adresse sollte ein Sternchen (*) sein.
c) Wählen Sie auf der Registerkarte Dienste die Dienste aus, die die Cacheserver darstellen.
d) Wählen Sie auf der Registerkarte Erweitert für Umleitungsmodus die Option MAC-basiert aus.
e) Klicken Sie auf Erstellen.

3. Konfigurieren eines virtuellen Cache-Umleitungsservers:
   a) Navigieren Sie zu Traffic Management > Load Balancing > Virtual Services.
   b) Klicken Sie im Detailbereich auf Hinzufügen, und geben Sie den Namen, das Protokoll, die IP-Adresse und den Port an. Die IP-Adresse sollte * sein.
   c) Wählen Sie unter Cache-Typ die Option Transparent aus.
   d) Aktivieren Sie auf der Registerkarte Erweitert im Feld Cacheserver den neuen virtuellen Lastausgleichsserver, und aktivieren Sie die Kontrollkästchen Origin USIP und Portbereich verwenden. Geben Sie im Feld Quell-IP-Ausdruck HTTP.REQ.HEADER (ClientIP) ein.
   e) Klicken Sie auf Erstellen.
4. Weisen Sie der Appliance einen Quellportbereich zu:
   a) Klicken Sie im Navigationsbereich auf System, und klicken Sie dann auf Einstellungen.
   b) Klicken Sie in der Gruppe Einstellungen auf den Link Globale Systemeinstellungen ändern.
   c) Geben Sie in der Gruppe Cache-Umleitungs-Portbereich den Portbereich für die Appliance an, indem Sie eine Portnummer für Startport und eine Portnummer für Endport eingeben.
   d) Klicken Sie auf OK.

Ziel-IP-Adresse einer Anforderung in Ursprungs-IP-Adresse übersetzen

October 5, 2021

Sie können den virtuellen Forward-Proxy-Cache-Umleitungsserver auf der Citrix ADC Appliance so konfigurieren, dass die Ziel-IP-Adresse der Anforderung, die auf dem virtuellen Cache-Umleitungsserver landet, in die IP-Adresse des Ursprungsservers übersetzt wird. Diese Übersetzung erfolgt unabhängig davon, ob die Anforderung an die zwischengespeicherten Server oder den Ursprungsserver gesendet wird.

Bisher konnte der virtuelle Server für die Weiterleitung von Proxy-Cache-Umleitung in der Service-Provider-Umgebung aufgrund der Einschränkungen bei der Cache-Umleitung mit von Content Switching-Richtlinien nicht effektiv verwendet werden, um Datenverkehr über die Firewall zu senden. Der virtuelle Cache-Umleitungsserver hat die Ursprungs-IP-Adresse nicht in die Ziel-IP übersetzt, wenn das Paket in den Cache gesendet wurde. Die Ziel-IP-Adresse war die des Ursprungsservers nur, wenn die Anforderungen vom zwischengespeicherten Server gesendet wurden.

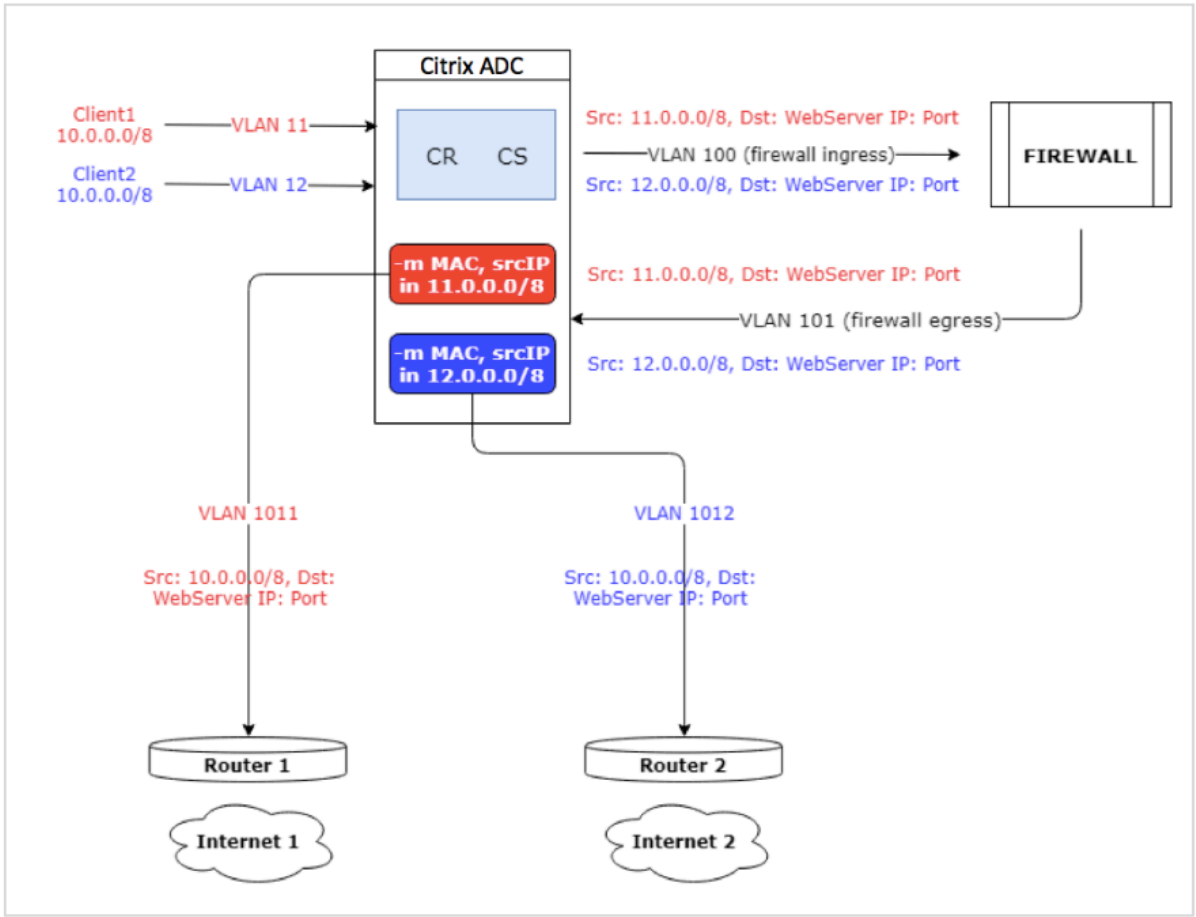
Hinweis: Die Übersetzung der Ziel-IP-Adresse einer Anforderung in die Ursprungs-IP-Adresse wird für einen virtuellen Server mit transparenter Cache-Umleitung nicht unterstützt. Für einen virtuellen Cache-Umleitungsserver muss diese Option auf OFF gesetzt sein.

Anwendungsfall

In einer Bereitstellung, bei der Citrix ADC Appliance für die Weiterleitungsproxy-Cache-Umleitung, Firewall und wiederverwendete Client-IP-Adressen konfiguriert ist, kann die Firewall die wiederverwendeten IP-Adressen nicht unterscheiden/verwenden. Daher müssen diese wiederverwendeten IP-Adressen in verschiedene IP-Adressen übersetzt werden. Um die wiederverwendeten IP-Adressen zu übersetzen, muss die Citrix ADC Appliance Folgendes ausführen:

1. Fragen Sie einen virtuellen DNS-Load Balancing Server für die Auflösung des Ziels ab.
2. Aktualisieren Sie die Ursprungs-IP-Adresse und Portnummer im Ziel.
3. Senden Sie die Anfrage zurück an die Firewall.

Betrachten Sie die folgende Bereitstellung, die eine Citrix ADC Appliance für die Weiterleitungsproxy-Cache-Umleitung, Firewall und zwei Router (Router 1 und Router 2) konfiguriert hat. Der Netzwerkverkehr fließt zu Internet 1 über Router 1 und Internet 2 über Router 2.



In diesem Beispiel stammen Eingabeanforderungen von Clients aus zwei verschiedenen VLANs, VLAN11 oder VLAN12. Die Client-IP-Adresse (10.0.0.0) wird wiederverwendet.
Basierend auf den Richtlinien zur Cache-Umleitung und zum Content Switching kann die Anforderung direkt an den Ursprungsserver oder an die Firewall gesendet werden.

- Wenn die Anforderung die Firewall umgehen und ins Internet gehen muss, wird basierend auf der Eingabeanforderung VLAN entweder Router 1 oder Router 2 ausgewählt und die Anforderung an Internet 1 oder Internet 2 gesendet.
- Wenn die Anforderung durch die Firewall gehen muss, muss die Quell-IP der Anfrage in eine bestimmte IP-Adresse übersetzt werden. Die übersetzte IP-Adresse kann verwendet werden, um das VLAN zu identifizieren, über das die Anfrage gekommen ist. Wenn die Eingabeanforderung beispielsweise von VLAN11 stammt, wird die Quell-IP-Adresse in 11.x.x.x übersetzt. Wenn die Anfrage von VLAN12 kommt, wird die Quell-IP-Adresse in 12.x.x.x übersetzt.

Nachdem die Firewall die Anforderung verarbeitet hat, wird die Anforderung an die Appliance zurückgesendet. mit der Kombination aus Listenrichtlinie und Netzprofilen übersetzt die Appliance die Quell-IP-Adresse zurück in die ursprüngliche IP-Adresse und sendet die Anforderung basierend auf der Eingabe-VLAN-ID an Router 1 oder Router 2.

Hinweis: Der Modus des virtuellen Lastausgleichsservers, der an den Cache gebunden ist, muss immer auf den MAC-Modus eingestellt sein. Obwohl der IP-Modus für diese Funktion nicht blockiert ist, führt das Festlegen des IP-Modus zu unerwartetem Verhalten.

So übersetzen Sie die Ziel-IP-Adresse und Portnummer der Anforderung mit der CLI in die Ursprungs-IP-Adresse

Geben Sie an der Eingabeaufforderung;

```
set cr vserver <vsname> -useoriginIpPortForCache <YES|NO>
<!--NeedCopy-->
```

Beispiel:

```
set cr vserver cvsrv1 -useoriginIpPortForCache YES
<!--NeedCopy-->
```

Wenn UseOriginipPortForCache auf Ja festgelegt ist und die Anforderung von den zwischengespeicherten Servern bedient werden muss, wird die Ziel-IP der Anforderung in die IP-Adresse des Ursprungsservers übersetzt.

Hinweis: Wenn UseOriginipPortForCache aktiviert ist, setzen Sie immer den virtuellen Lastausgleichsserver, der an den Cache gebunden ist, in den MAC-Modus.

So übersetzen Sie die Ziel-IP-Adresse und den Port der Anforderung mit der GUI in die Ursprungs-IP-Adresse

1. Navigieren Sie zu **Traffic Management** > **Cache-Umleitung** > **Virtuelle Server**, und klicken Sie auf **Hinzufügen** .
2. Geben Sie die Details des virtuellen Cache-Umleitungsservers an.
3. Wählen Sie **Ursprungs-IP-Port für Cache verwenden**, um die Übersetzung der Ziel-IP-Adresse der Anforderung in die Ursprungs-IP-Adresse zu aktivieren.
4. Klicken Sie auf **OK**.

Clustering

October 5, 2021

> **Hinweis:**
>
> Diese Funktion ist mit einer Lizenz für Citrix ADC Advanced oder Premium Edition verfügbar.

Ein Citrix ADC Cluster ist eine Gruppe von nCore Appliances, die als einzelnes Systemimage zusammenarbeiten. Jedes Gerät des Clusters wird als Knoten bezeichnet. Der Cluster kann über eine Appliance oder bis zu 32 Citrix ADC nCore Hardware oder virtuelle Appliances als Knoten verfügen.

Der Clientdatenverkehr wird auf die Knoten verteilt, um hohe Verfügbarkeit, hohen Durchsatz und Skalierbarkeit bereitzustellen.

Um einen Cluster zu erstellen, müssen Sie die folgenden Schritte ausführen:

- Fügen Sie die Geräte als Clusterknoten hinzu.
- Richten Sie die Kommunikation zwischen den Knoten ein.
- Richten Sie Links zu den Client- und Server-Netzwerken ein.
- Konfigurieren Sie die Appliances und konfigurieren Sie die Verteilung von Client- und Serverdatenverkehr.

Unterstützungsmatrix für Citrix ADC Cluster

October 5, 2021

Das Clustering in der Citrix ADC Appliance unterstützt eine breite Verbreitung von Funktionen in Citrix ADC-Konfigurationen.

Die folgende Tabelle listet die Citrix ADC-Funktionen auf und enthält den Supportabilitätsstatus für verschiedene Citrix ADC-Versionen von Cluster-Setups. Der Supportabilitätsstatus einiger Citrix ADC-Funktionen in einem 13.0 Citrix ADC BLX-Cluster unterscheidet sich von einem 13,0 Citrix ADC Nicht-BLX (MPX oder VPX, SDX ADC) -Cluster.

> **Wichtig**
>
> Der Eintrag Node-Level in der Tabelle gibt an, dass die Funktion nur auf einzelnen Clusterknoten unterstützt wird.

Citrix ADC Funktionen	11.1	12.1	13.0	13.0 Citrix ADC BLX-Cluster
SSL FIPS	Nein	Nein	Nein	Nein
SSL-Zertifikatbündel	Nein	Nein	Nein	Nein
SSL-Interception	Nicht verfügbar	Nein	Nein	Nein
Content Switching-Aktionen	Ja	Ja	Ja	Ja
Richtlinienbasierte Protokollierung für Content Switching-Richtlinien	Ja	Ja	Ja	Ja
Ratenbegrenzung	Ja	Ja	Ja	Ja
Aktionsanalysen	Ja	Ja	Ja	Nein
GSLB	Ja	Ja	Ja	Ja
RTSP	Ja	Ja	Ja	Ja
DNSSEC	Nein	Nein	Nein	Nein
DNS64	Nein	Nein	Nein	Nein
FTP	Ja	Ja	Ja	Nein
TFTP	Nein	Ja	Ja	Ja
Verbindungsspiegelung	Nein	Nein	Nein	no

Citrix ADC Funktionen	11.1	12.1	13.0	13.0 Citrix ADC BLX-Cluster
Integriertes Caching	Knotenebene	Knotenebene	Knotenebene	Nein
Großer gemeinsam genutzter Cache	Knotenebene	Knotenebene	Knotenebene	Nein
Front-End-Optimierung	Knotenebene	Knotenebene	Knotenebene	Nein
Anwendungs-Firewall	Ja	Ja	Ja	Nein
HTTP-Denial-of-Service-Schutz (HDOSP)	Knotenebene	Knotenebene	Knotenebene	Veraltet
Prioritätswarteschlange (PQ)	Knotenebene	Knotenebene	Knotenebene	Veraltet
Sicherer Anschluss (SC)	Knotenebene	Knotenebene	Knotenebene	Veraltet
AppQoE	Ja	Ja	Ja	Nein
Überspannungsschl	Knotenebene	Knotenebene	Knotenebene	Ja
MPTCP	Ja	Ja	Ja	Nein
Gestreifte SNIPs	Ja; **Hinweis:** Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; **Hinweis:** Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; **Hinweis:** Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; **Hinweis:** Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.
MSR	Ja; **Hinweis:** Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; **Hinweis:** Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; **Hinweis:** Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; **Hinweis:** Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.

Citrix ADC Funktionen	11.1	12.1	13.0	13.0 Citrix ADC BLX-Cluster
IS-IS (IPv4 und IPv6)	Ja	Ja	Ja	Nein
Jumbo Frames	Ja	Ja	Ja	Nein
IP-IP-Tunneling	Ja	Ja	Ja	Nein
Link-Lastenausgleich	Ja	Ja	Ja	Ja
FIS (Failover-schnittstellen-satz)	Ja	Ja	Ja	Nein
Link-Redundanz (LR)	Ja	Ja	Ja	Nein
NAT46	Nein	Nein	Ja	Ja
NAT64	Nein	Nein	Ja	Ja
RNAT6	Ja	Ja	Ja	Ja
LSN/CGNAT	Nein	Ja	Ja	Nein
IPv6 ReadyLogo	Nein	Ja	Ja	Nein
Traffic-Domänen	Ja; **Hinweis:** Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; **Hinweis:** Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja; **Hinweis:** Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Nein
Routenüberwachu	Ja; nur mit DR.	Ja; **Hinweis:** Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Ja **Hinweis:** Unterstützt in L2-Clustern. Wird in L3-Clustern nicht unterstützt.	Nein
GRE Tunnelbau (CB)	Nein	Nein	Nein	Nein
Layer-2-Modus	Ja	Ja	Ja	Nein

Citrix ADC Funktionen	11.1	12.1	13.0	13.0 Citrix ADC BLX-Cluster
Netzprofile	Ja	Ja	Ja	Nein
HTTPS-Callout	Ja	Ja	Ja	Ja
AAA-TM	Knotenebene	Ja	Ja	Nein
AppFlow	Knotenebene	Knotenebene	Knotenebene	Nein
Web Insight	Ja	Ja	Ja	Nein
HDX Insight	Ja	Ja	Ja	Nein
VMAC/VRRP	Ja	Ja	Ja	Nein
NetScaler Push	Nein	Nein	Nein	Nein
Stateful Connection Failover	Nein	Nein	Nein	Nein
Ordnungsgemäße Herunterfahren	Nein	Ja	Ja	Ja
DBS Autoscale	Nein	Nein	Ja	Ja
DSR mit TOS	Nein	Nein	Nein	Ja
Finer Startup-RR Control	Knotenebene	Knotenebene	Knotenebene	Nein
XML XSM	Nein	Nein	Nein	Nein
DHCP RA	Nein	Nein	Nein	Nein
Bridge-Gruppe	Ja	Ja	Ja	Nein
Netzwerkbrücke	Nein	Nein	Nein	Nein
Webinterface auf Citrix ADC (WIonNS)	Ja	Ja	Ja	Nein
EdgeSight-Überwachung	Veraltet	Veraltet	Veraltet	Nein
Metrik-Tabellen - Lokal	Nein	Nein	Nein	Nein
DNS-Zwischenspeicherung	Knotenebene	Knotenebene	Knotenebene	Knotenebene
Call Home	Knotenebene	Knotenebene	Knotenebene	Nein

Citrix ADC Funktionen	11.1	12.1	13.0	13.0 Citrix ADC BLX-Cluster
Citrix Gateway ICA-Proxymodus	Ja	Ja	Ja	Nein
Citrix Gateway (SSL VPN, vollständiges VPN und clientloses VPN)	Knotenebene	Knotenebene	Knotenebene	Nein
Citrix CloudBridge Connector	Nein	Ja	Ja	Nein
Richtlinienbasierte Routing (PBR/PBR6)	Ja	Ja	Ja	Nein
IPv4 Policy Based Routing (PBR) mit virtuellem LLB-Server als Next Hop	Nein	Nein	Ja	Nein
IPv6 Policy Based Routing (PBR6) mit virtuellem LLB-Server als Next Hop	Nein	Nein	Nein	Nein
Sensibilisierung des Teilnehmers	Nein	Nein	Nein	Nein
Dynamisches Routing	Ja mit v6-Protokollen (ospfv3, RIPng, ISIS6, BGP6) Unterstützung	Ja mit v6-Protokollen (ospfv3, RIPng, ISIS6, BGP6) Unterstützung	Ja mit v6-Protokollen (ospfv3, RIPng, ISIS6, BGP6) Unterstützung	Ja

Citrix ADC Funktionen	11.1	12.1	13.0	13.0 Citrix ADC BLX-Cluster
SYSLOG-TCP, Lastausgleich von Syslog-Servern, SNIP-Unterstützung und FQDN-Unterstützung für syslog	Ja; **Hinweis:** Unterstützt ab NetScaler 11.1 Build 54.16.	Ja	Ja	Ja
Bot-Verwaltung	Nein	Nein	Ja	Nein
VXLAN	Nein	Nein	Nein	Nein

Außerdem werden die folgenden Citrix ADC Konfigurationen unterstützt:

Lastenausgleich, Persistenz des Lastenausgleichs, DNS-Lastausgleich, SIP, MaxClient, Spillover (Verbindung und Dynamik). Spillover basierend auf Bandbreite, DataStream, Komprimierungskontrolle, Inhaltsfilterung, TCP-Pufferung, Cache-Umleitung, Distributed Denial-of-Service (DDoS). Client Keep-Alive, Basic-Netzwerke (IPv4 und IPv6), OSPF (IPv4 und IPv6), RIP (IPv4 und IPv6), RIP (IPv4 und IPv6). VLAN, ICMP, Fragmentation, MBF, ACL, Simple ACL, MSR, Path MTU Discovery, IP-IP, SNMP, Richtlinien (klassisch und fortgeschritten). Rewrite, Responder, HTTP-Callout, Webserver-Protokollierung, Audit-Protokollierung (NSLOG und Syslog). USIP, Location Befehle, HTML Injection, NITRO API, AppExpert, KRPC.

Voraussetzungen

February 24, 2022

Citrix ADC Appliances (MPX, VPX, SDX ADC, BLX), die einem Cluster hinzugefügt werden sollen, müssen die folgenden Voraussetzungen erfüllen:

- Alle Appliances müssen über die gleiche Softwareversion und den gleichen Build verfügen.
- Alle Appliances müssen vom gleichen Plattformtyp sein. Dies bedeutet, dass ein Cluster entweder über alle Hardware-Appliances (Citrix ADC MPX) oder alle Citrix ADC VPX Appliances oder alle Citrix BLX-Appliances oder alle Citrix SDX ADC-Instanzen verfügen muss.

  Hinweis:

  - Bei einem Cluster von Hardware-Appliances (MPX) müssen die Appliances vom gleichen Modelltyp sein.
  - Für die Bildung des heterogenen Clusters müssen alle Appliances vom MPX-Plattformtyp sein.
  - Für einen Cluster von virtuellen Appliances (VPX) müssen die Appliances auf den folgenden Hypervisoren bereitgestellt werden: XenServer, Hyper-V, VMware ESX und KVM.
  - Informationen zum Einrichten eines Clusters von SDX Citrix ADC-Instanzen finden Sie unter Einrichten eines Clusters von Citrix ADC-Instanzen.
  - Jumbo-Frames werden auf einem Citrix ADC Cluster unterstützt, der aus Citrix ADC SDX-Instanzen besteht.
  - Sie können L3-Cluster von SDX-Instanzen erstellen.
  - Informationen zum Einrichten eines Citrix ADC BLX-Clusters finden Sie unter Citrix ADC BLX-Cluster.

- Appliances können zu verschiedenen Netzwerken gehören.
- Zunächst konfiguriert und mit einem gemeinsamen clientseitigen und serverseitigen Netzwerk verbunden werden.
- Für einen Cluster virtueller Appliances (Citrix ADC VPX oder Citrix ADC BLX oder Citrix SDX ADC-Instanz) mit großen Konfigurationen wird empfohlen, 6 GB RAM für jeden Knoten des Clusters zu verwenden.

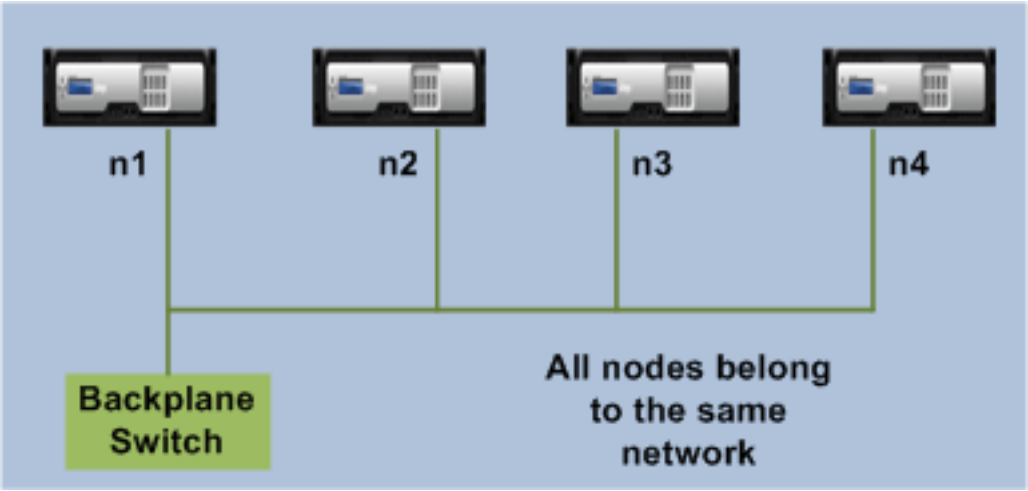
Clusterübersicht

October 5, 2021

Ein Citrix ADC Cluster wird gebildet, indem Citrix ADC Appliances zusammengefasst werden. Basierend auf dem Netzwerkstandort der Citrix ADC Appliances, die Sie den Cluster hinzufügen möchten, müssen Sie die folgenden Cluster-Setups kennen:

> **Hinweis:**
>
> Sofern nicht anders angegeben, sind Cluster-Features und -Konfigurationen für L2- und L3-Cluster identisch.

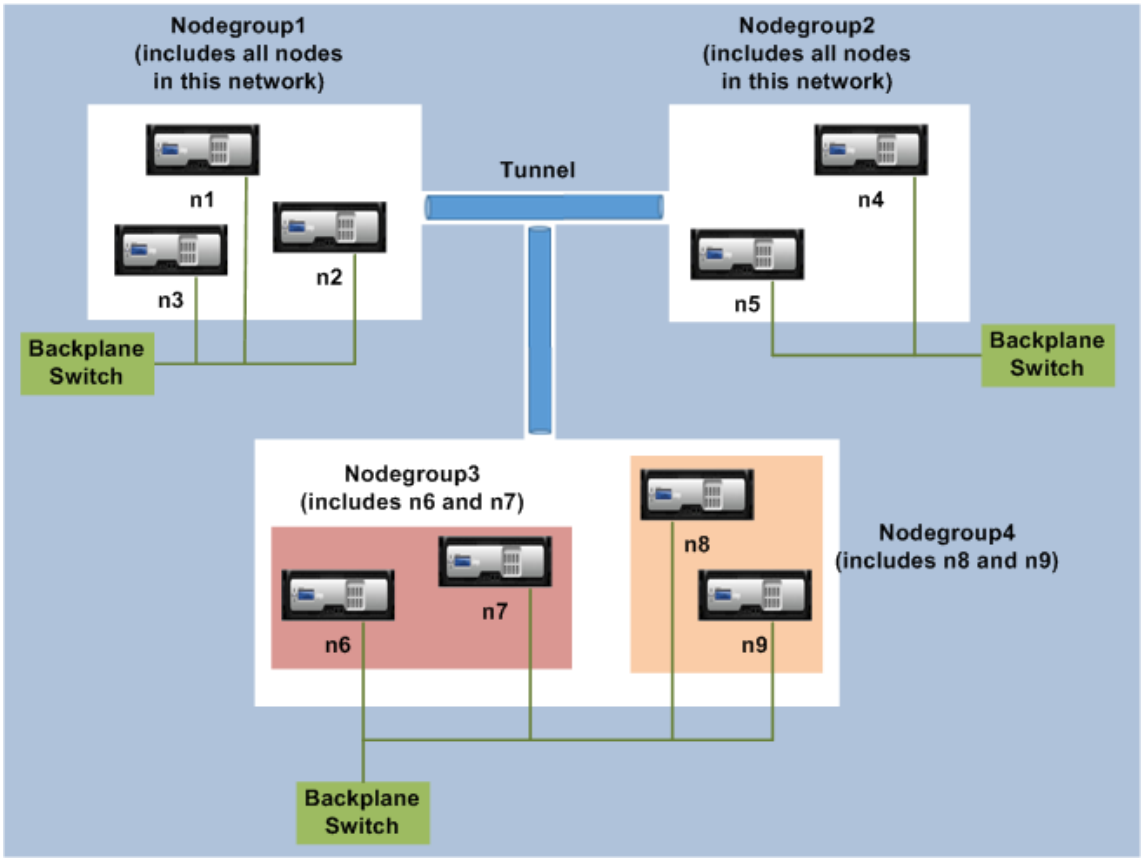
- **L2-Cluster:** In dieser Clusterbereitstellung gehören alle Clusterknoten zum selben Netzwerk.



- **L3-Cluster (auch als Cluster im INC-Modus bezeichnet):** In dieser Clusterbereitstellung können Clusterknoten zu verschiedenen Netzwerken gehören. Die Cluster-Knoten aus einem bestimmten Netzwerk müssen in Knotengruppen gruppiert werden, die nur Knoten aus diesem Netzwerk enthalten. Aus der folgenden Abbildung sehen wir, dass die Knoten n1, n2, n3 im selben Netzwerk sind und in Nodegroup1 gruppiert sind.

  Ähnlich gilt der Fall für Knoten n4 und n5, die in Nodegroup2 gruppiert sind. Im dritten Netzwerk gibt es zwei Knotengruppen. Nodegroup3 enthält n6 und n7 und Nodegroup4 enthält n8 und n9.

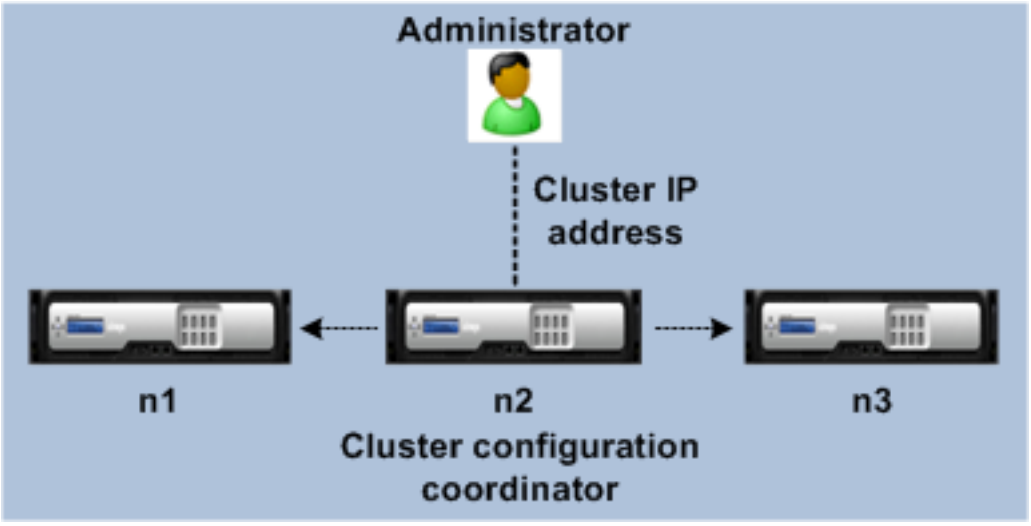
  > **Hinweis:**
  >
  > Unterstützt ab NetScaler 11.0.



Synchronisierung über Clusterknoten hinweg

October 5, 2021

Alle Konfigurationen auf einem Citrix ADC Cluster werden für die Cluster-IP-Adresse ausgeführt, d. h. die Verwaltungsadresse des Clusters. Der Cluster-Knoten besitzt die Cluster-IP-Adresse, die als Cluster-Konfigurationskoordinator (CCO) bezeichnet wird, wie in der folgenden Abbildung dargestellt:



Die Konfigurationen, die auf dem CCO verfügbar sind, werden automatisch an die anderen Cluster-Knoten weitergegeben und daher haben alle Cluster-Knoten die gleichen Konfigurationen.

- Mit Citrix ADC können nur wenige Konfigurationen auf einzelnen Clusterknoten über ihre NSIP-Adresse durchgeführt werden. In diesen Fällen müssen Sie die Konfigurationskonsistenz manuell über alle Knoten im Cluster hinweg sicherstellen. Diese Konfigurationen werden nicht über die anderen Clusterknoten verteilt. Weitere Informationen zu Operationen, die auf jedem Clusterknoten unterstützt werden, finden Sie unter Auf einzelnen Clusterknoten unterstützte Vorgänge.
- Die folgenden Befehle, wenn sie auf der Cluster-IP-Adresse ausgeführt werden, werden nicht an andere Clusterknoten weitergegeben:
  - **shutdown.** Beenden Sie nur den Konfigurationskoordinator.
  - **reboot.** Startet nur den Konfigurationskoordinator neu.
  - **rm cluster instance.** Entfernt die Clusterinstanz von dem Knoten, auf dem Sie den Befehl ausführen.
- Für einen Befehl, der an andere Clusterknoten weitergegeben werden soll:
  - Das Quorum muss für die Clusterinstanz konfiguriert werden.
  - Das meiste Clusterquorum mit (n/2 + 1) der Clusterknoten muss aktiv sein, damit der Cluster betriebsbereit ist.
  - Ein Cluster kann mit einer minimalen Anzahl von Knoten ausgeführt werden, wenn die Mehrheitsregel (n/2 + 1) gelockert ist.

Wenn ein Knoten zu einem Cluster hinzugefügt wird, werden die Konfigurationen und die Dateien (SSL-Zertifikate, Lizenzen, DNS usw.), die auf dem CCO verfügbar sind, mit dem neu hinzugefügten Clusterknoten synchronisiert. Wenn ein vorhandener Cluster-Knoten, der absichtlich deaktiviert wurde oder ausgefallen war, erneut hinzugefügt wird, vergleicht der Cluster die auf dem Knoten verfügbaren Konfigurationen mit den auf der CCO verfügbaren Konfigurationen. Wenn in Konfigurationen eine Abweichung vorliegt, wird der Knoten mithilfe einer der folgenden Synchronisierung synchronisiert:

- **Vollständige Synchronisation.** Wenn der Unterschied zwischen Konfigurationen 255 Befehle überschreitet, werden alle Konfigurationen des CCO auf den Knoten angewendet, der dem Cluster wieder beitritt. Der Knoten bleibt während der Synchronisation betrieblich nicht verfügbar.
- **Inkrementelle Synchronisation.** Wenn der Unterschied zwischen Konfigurationen kleiner oder gleich 255 Befehlen ist, werden nur die Konfigurationen angewendet, die nicht verfügbar sind, auf den Knoten angewendet, der dem Cluster erneut beitritt. Der Betriebszustand des Knotens bleibt unberührt.

> **Hinweis:**
>
> Sie können die Konfigurationen und Dateien auch manuell synchronisieren. Weitere Informationen finden Sie unterClusterkonfigurationen synchronisieren und Clusterdateien synchronisieren.

Striped-, Teil-Striped- und Spotted-Konfigurationen

October 5, 2021

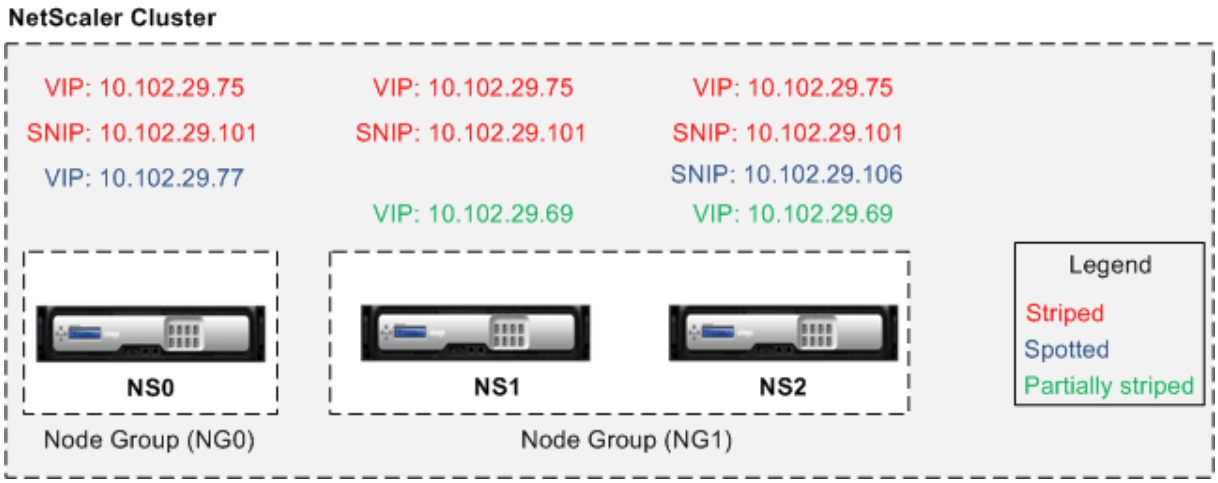
Aufgrund der Befehlsausbreitung haben alle Knoten in einem Cluster die gleichen Konfigurationen. Möglicherweise möchten Sie jedoch, dass einige Konfigurationen nur auf bestimmten Clusterknoten verfügbar sind. Obwohl Sie die Knoten, auf denen die Konfigurationen verfügbar sind, nicht einschränken können, können Sie die Knoten angeben, auf denen die Konfigurationen aktiv sind.

Beispiel:

- definieren Sie eine SNIP-Adresse, die nur auf einem Knoten aktiv ist, oder
- definieren Sie eine SNIP-Adresse, die auf allen Knoten aktiv ist, oder
- definieren Sie eine VIP-Adresse, die nur auf einem Knoten aktiv ist, oder
- eine VIP-Adresse definieren, die auf allen Knoten aktiv ist, oder
- Definieren Sie eine VIP-Adresse, die nur auf zwei Knoten eines 3-Knoten-Clusters aktiv ist

Abhängig von der Anzahl der Knoten, auf denen die Konfigurationen aktiv sind, werden Clusterkonfigurationen als gestreifte, teilweise gestreifte oder gepunktete Konfigurationen bezeichnet.

Abbildung 1. Cluster mit drei Knoten mit Striped-, Teil-Striped- und Spotted-Konfigurationen



Die folgende Tabelle enthält weitere Details zu den Konfigurationstypen:

Konfigurationstyp	Aktiv auf	Anwendbar für	Konfigurationen
Stripesetkonfiguration	Alle Clusterknoten	Alle Einträge	Es ist keine spezifische Konfiguration erforderlich, um eine Entität Striped zu erstellen. Standardmäßig werden alle Entitäten, die für eine Cluster-IP-Adresse definiert sind, auf allen Clusterknoten gestreift.
Teilweise gestreifte Konfiguration	Eine Teilmenge von Clusterknoten	Siehe Cluster-Knotengruppen.	Binden Sie die Entitäten, die teilweise gestreift werden sollen, an eine Knotengruppe. Die Konfiguration ist nur auf den Clusterknoten aktiv, die zur Knotengruppe gehören.

Konfigurationstyp	Aktiv auf	Anwendbar für	Konfigurationen
Spotted Konfiguration	Einzelner Clusterknoten	SNIP-Adresse, SNMP-Engine-ID, Hostname von Clusterknoten, Entitäten, die an eine Knotengruppe gebunden werden können	Eine Spotted-Konfiguration kann mit einem von zwei Ansätzen definiert werden. **SNIP-Adresse** Geben Sie beim Erstellen der SNIP-Adresse den Knoten an, auf dem die SNIP-Adresse aktiv sein soll, als Eigentümerknoten an. **Beispiel:** `add ns ip 10.102.29.106 255.255.255.0 -type SNIP -ownerNode 2` (vorausgesetzt, der NS2-ID ist 2). **Hinweis**: Sie können den Besitz einer Spotted-SNIP-Adresse zur Laufzeit nicht ändern. Um den Besitz zu ändern, müssen Sie zuerst die SNIP-Adresse löschen und sie erneut hinzufügen, indem Sie den neuen Besitzer angeben. **Entitäten, die an eine Knotengruppe gebunden werden können.** Durch Bindung der Entität an eine Knotengruppe mit einem einzelnen Mitglied.

Konfigurationstyp	Aktiv auf	Anwendbar für	Konfigurationen

Hinweis:

- Wenn Sie USIP deaktivieren, empfiehlt Citrix die Verwendung von Spotted-SNIP-Adressen. Sie können Striped SNIP-Adressen nur verwenden, wenn IP-Adressen fehlen. Die Verwendung von Striped-IP-Adressen kann zu ARP-Flussproblemen führen, wenn für die ARP-Auflösung keine Spotted-IP-Adressen im selben Subnetz vorhanden sind.
- Wenn Sie USIP aktivieren, empfiehlt Citrix, Striped SNIP-Adressen als Gateway für serverinitiierten Datenverkehr zu verwenden.

ARP-Besitzer-Unterstützung für Striped IP

In einem Cluster-Setup können Sie einen bestimmten Knoten so konfigurieren, dass er auf die ARP-Anforderung für eine Stripeset-IP antwortet. Der konfigurierte Knoten reagiert auf den ARP-Datenverkehr.

Ein neuer Parameter “ArPowner” wird in den Befehlen “IP hinzufügen, setzen und nicht gesetzt” eingeführt.

So aktivieren Sie den ARP-Besitzer auf einem Knoten mit der CLI.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns ip <ip_address> -arpOwner <node_id>
```

Hinweis:

Der ARP-Besitzerparameter wird nur im L2-Cluster unterstützt.

Unterstützung für Nachbarerkennungseigentümer für gestreifte IPv6-Adresse

In einem Cluster-Setup können Sie einen bestimmten Knoten als Neighbor Discovery (ND)-Besitzer für die Striped IPv6-Adresse konfigurieren, um die Link-Layer-Adresse zu bestimmen. Ein Client sendet eine Neighbor Solicitation (NS)-Nachricht an alle Knoten im Cluster-Setup. Der ND-Besitzer antwortet mit einer Neighbor Advertisement (NA)-Nachricht mit der Link-Layer-Adresse für die Striped IPv6-Adresse und dient dem Datenverkehr.

So aktivieren Sie ND-Besitzer auf einem Knoten über die Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add ns ip6 <IPv6Address> -ndOwner <node id>

set  ns ip6 <IPv6Address> -ndOwner <node id>
<!--NeedCopy-->
```

Beispiel:

```
add ns ip6 2001::21/64 -ndOwner 1

set ns ip6 2001::21/64 -ndOwner 1
<!--NeedCopy-->
```

So aktivieren Sie den ND-Besitzer auf einem Knoten mit der GUI

1. Navigieren Sie zu **System > Netzwerk > IPs**.
2. Wechseln Sie auf der **IPs-Seite** zur Registerkarte **IPv6s** und klicken Sie auf **Hinzufügen**.
3. Wählen **Sie auf der Seite IPv6 erstellen** eine der Knoten-IDs aus, die im Dropdownmenü **NDOwner im Cluster** aufgeführt sind.

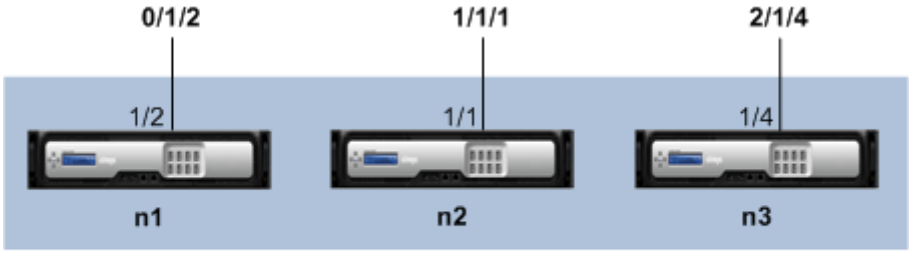
> **Hinweis:**
>
> Der ND-Besitzerparameter wird nur im L2-Cluster unterstützt.

Kommunikation in einem Cluster-Setup

October 5, 2021

Den Schnittstellen von Citrix ADC Appliances, die zu einem Cluster hinzugefügt werden, wird eine Knoten-ID vorangestellt. Es hilft bei der Identifizierung des Clusterknotens, zu dem die Schnittstelle gehört. Daher wird die Schnittstellenkennung c/u, wobei c die Controller Nummer und u die Einheiten-nummer ist, nun n/c/u, wobei n die Knoten-ID ist. In der folgenden Abbildung wird beispielsweise die Schnittstelle 1/2 des Knotens n1 als 0/1/2 dargestellt, die Schnittstelle 1/1 des Knotens n2 wird als 1/1/1 und die Schnittstelle 1/4 des Knotens n3 wird als 2/1/4 dargestellt.

Abbildung 1. Interface-Benennungskonvention in einem Cluster



Citrix ADC Cluster

- **Serverkommunikation**-
  Der Cluster kommuniziert mit dem Server über die physischen Verbindungen zwischen dem Clusterknoten und dem serverseitigen Verbindungsgerät. Die logische Gruppierung dieser physischen Verbindungen wird als Serverdatenebene bezeichnet.
- **Clientkommunikation**- Der Cluster kommuniziert mit dem Client über die physischen Verbindungen zwischen dem Clusterknoten und dem clientseitigen Verbindungsgerät. Die logische Gruppierung dieser physischen Verbindungen wird als Client-Datenebene bezeichnet.
- **Kommunikation zwischen Knoten -**Die Clusterknoten können auch miteinander kommunizieren. Die Art und Weise, wie sie kommunizieren, hängt davon ab, ob der Knoten im selben Netzwerk oder über Netzwerke hinweg vorhanden ist.
  - Clusterknoten innerhalb desselben Netzwerks kommunizieren über die Cluster-Backplane miteinander. Die Backplane ist ein Satz von Schnittstellen, bei denen eine Schnittstelle jedes Knotens mit einem gemeinsamen Switch verbunden ist, der als Cluster-Backplane-Switch bezeichnet wird. Die verschiedenen Arten von Datenverkehr, die durch die Backplane fließen, die von der Internode-Kommunikation verwendet wird, sind:
    * Knoten-zu-Knoten-Messaging (NNM)
    * Gelenkter Verkehr
    * Konfigurationspropagierung und Synchronisierung
  - Jeder Knoten des Clusters verwendet eine spezielle MAC-Cluster-Backplane-Switch-Adresse, um mit anderen Knoten über die Backplane zu kommunizieren. Der Cluster-Spezial-MAC hat die Form: `0x02 0x00 0x6F <cluster_id> <node_id> <reserved >)`, wobei `cluster_id` die Clusterinstanz-ID `node_id` ist, ist die Knotennummer der Citrix ADC Appliance, die zu einem Cluster hinzugefügt wird.

Die folgenden Abbildungen zeigen die Kommunikationsschnittstellen in L2-Clustern und L3-Clustern.

Abbildung 2. Clusterkommunikationsschnittstellen - L2-Cluster

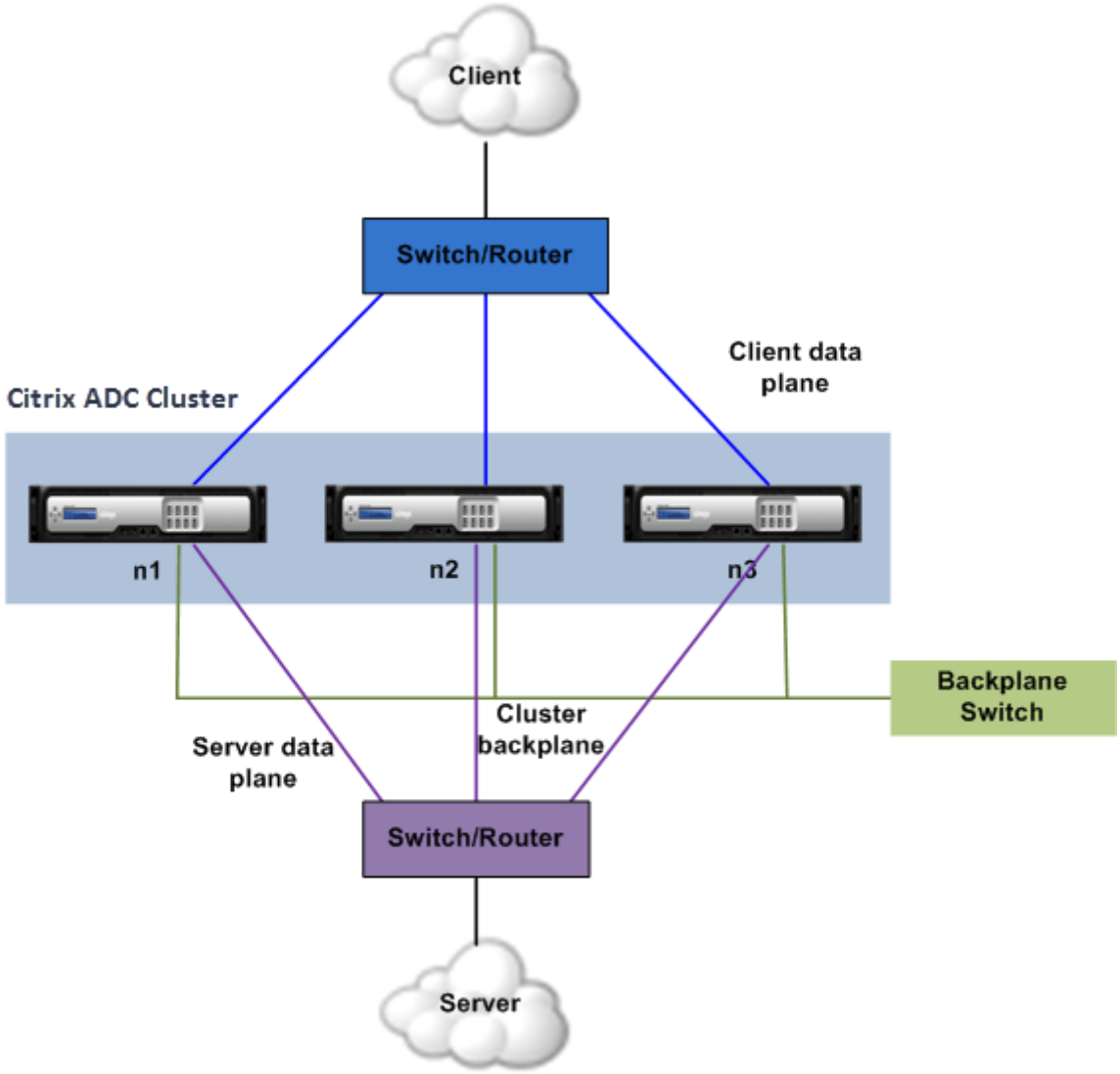
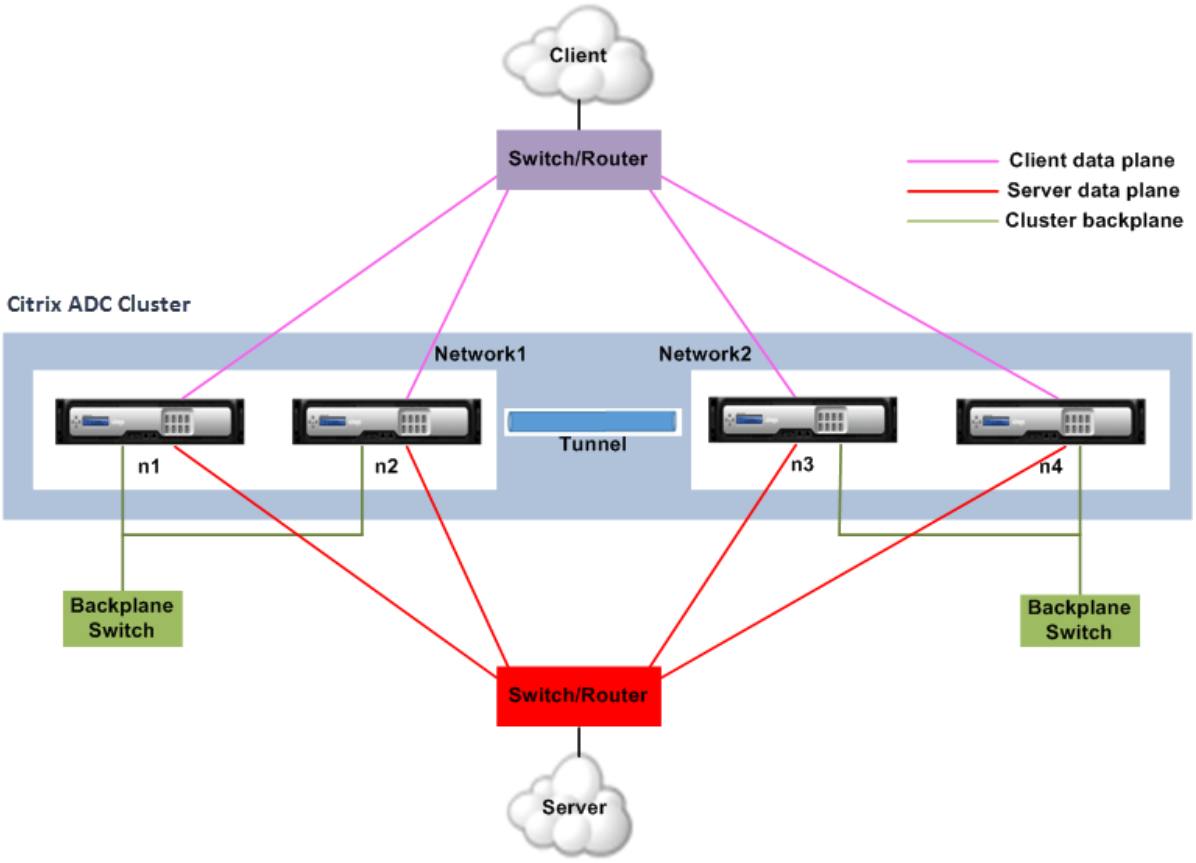


Abbildung 3. Clusterkommunikationsschnittstellen - L3-Cluster



Verkehrsverteilung in einem Cluster-Setup

October 5, 2021

In einem Cluster-Setup zeigen externe Netzwerke die Sammlung von Citrix ADC Appliances als einzelne Entität an. Daher muss der Cluster einen einzelnen Knoten auswählen, der den Datenverkehr empfangen muss. Der Cluster führt diese Auswahl mithilfe des Verteilungsmechanismus für den Datenverkehr mit gleichen Kosten (ECMP) oder der Verteilung des Datenverkehrs von Cluster-Links durch. Der ausgewählte Knoten wird als Flow Receiver bezeichnet.

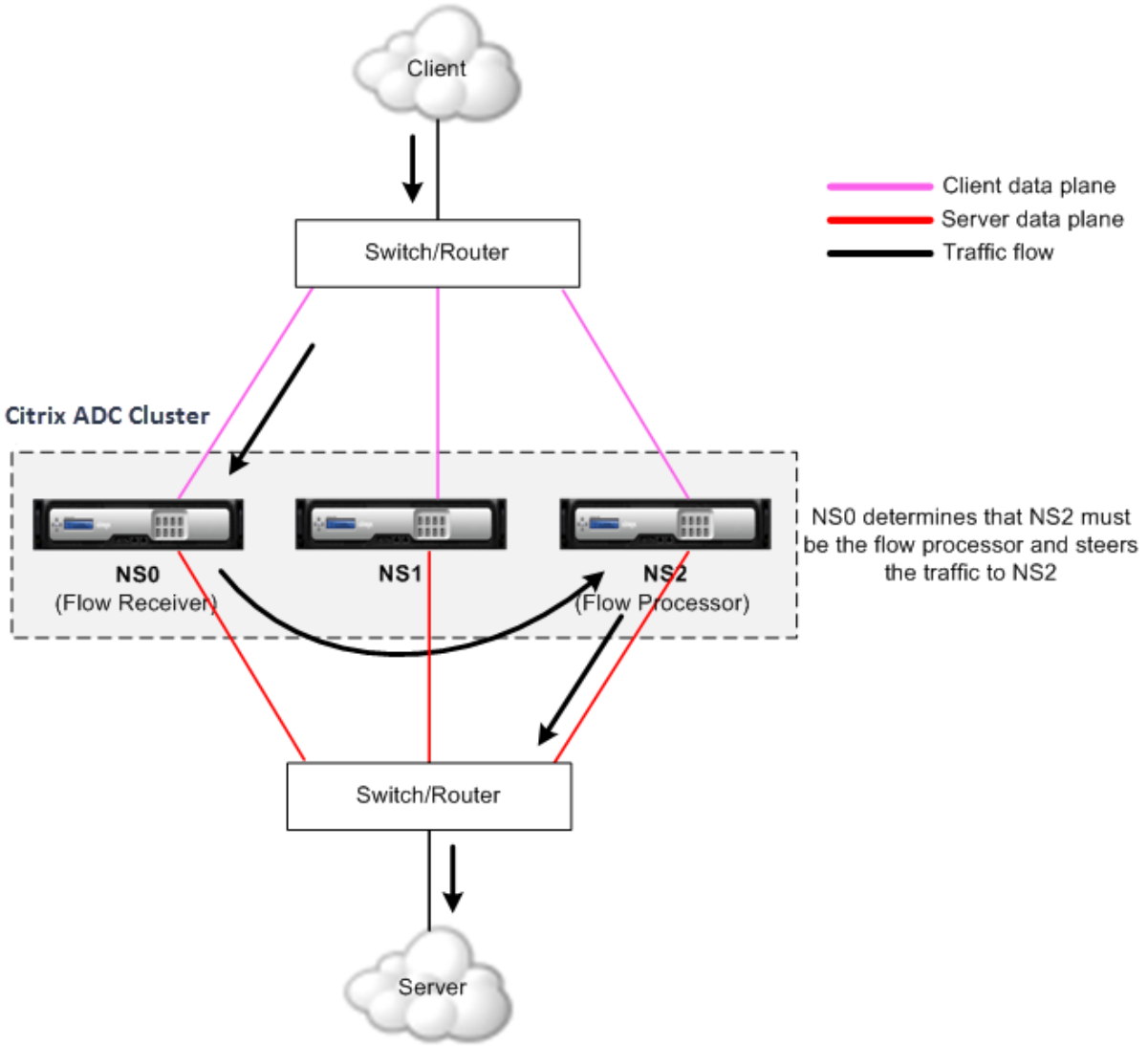
> **Hinweis:**
>
> Für einen L3-Cluster (Knoten über verschiedene Netzwerke) kann nur die ECMP-Verkehrsverteilung verwendet werden.

Der Flussempfänger ruft den Datenverkehr ab und bestimmt dann mithilfe der internen Clusterlogik den Knoten, der den Datenverkehr verarbeiten muss. Dieser Knoten wird als Flow-Prozessor bezeichnet. Der Flow-Empfänger steuert den Datenverkehr zum Flow-Prozessor über die Backplane, wenn

sich der Flow-Empfänger und der Flow-Prozessor im selben Netzwerk befinden. Der Verkehr wird durch den Tunnel gelenkt, wenn sich der Flow-Empfänger und der Flow-Prozessor in verschiedenen Netzwerken befinden.

> **Hinweis:**
>
> - Der Flow-Empfänger und der Flow-Prozessor müssen Knoten sein, die den Datenverkehr bedienen können.
> - Ab NetScaler 11 können Sie die Steuerung auf der Cluster-Backplane deaktivieren. Weitere Informationen finden Sie unter Deaktivieren der Lenkung auf der Cluster-Backplane.

Abbildung 1. Datenverkehrsverteilung in einem Cluster



Die vorangehende Abbildung zeigt eine Client-Anfrage, die durch den Cluster fließt. Der Client sendet eine Anforderung an eine virtuelle IP (VIP) -Adresse. Ein auf der Clientdatenebene konfigurierter

Verkehrsverteilungsmechanismus wählt einen der Clusterknoten als Flow-Empfänger aus. Der Flussempfänger empfängt den Datenverkehr, bestimmt den Knoten, der den Datenverkehr verarbeiten muss, und steuert die Anforderung an diesen Knoten (es sei denn, der Flow-Empfänger wählt sich selbst als Flow-Prozessor aus).

Der Flow-Prozessor stellt eine Verbindung mit dem Server her. Der Server verarbeitet die Anforderung und sendet die Antwort an die Subnetz-IP-Adresse (SNIP), die die Anforderung an den Server gesendet hat.

- Wenn es sich bei der SNIP-Adresse um eine gestreifte oder teilweise gestreifte IP-Adresse handelt, wählt der auf der Serverdatenebene konfigurierte Verkehrsverteilungsmechanismus einen der Clusterknoten als Flow-Empfänger aus. Der Flow-Empfänger empfängt den Datenverkehr, bestimmt den Flow-Prozessor und steuert die Anforderung über die Cluster-Rückwandplatine an den Flow-Prozessor.
- Wenn es sich bei der SNIP-Adresse um eine gepunktete IP-Adresse handelt, erhält der Knoten, dem die SNIP-Adresse gehört, die Antwort vom Server.

In einer asymmetrischen Cluster-Topologie (alle Clusterknoten sind nicht mit dem externen Switch verbunden) müssen Sie Linksets entweder ausschließlich oder in Kombination mit ECMP- oder Clusterlinkaggregation verwenden. Weitere Informationen finden Sie unter Verwenden von Linksets.

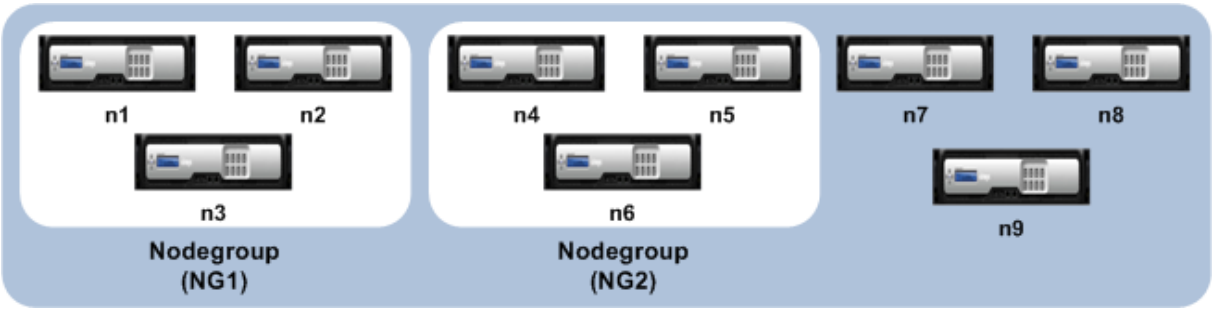
Clusterknotengruppen

October 5, 2021

> **Hinweis:**
>
> Knotengruppen werden ab NetScaler 10.1 unterstützt.

Wie der Name schon sagt, ist eine Clusterknotengruppe eine Gruppe von Clusterknoten.

Abbildung 1. Citrix ADC Cluster mit Knotengruppen



Die vorhergehende Abbildung zeigt einen Cluster mit den Knotengruppen NG1 und NG2, die jeweils 3 Clusterknoten enthalten. Der Cluster hat auch 3 Knoten, die nicht Teil einer Knotengruppe sind.

Eine Knotengruppe kann für Folgendes konfiguriert werden:

- Definieren von Spotted- und Teil-Striped-Konfigurationen. Weitere Informationen finden Sie unter Knotengruppen für Spotted und Partiell Striped Configurations.
- So konfigurieren Sie Redundanz von Knotengruppen. Weitere Informationen finden Sie unter Konfigurieren von Redundanz für Knotengruppen.
  Hinweis: Unterstützt ab NetScaler 10.5 Build 52.1115.e.
- Definieren eines L3-Clusters (auch Cluster im INC-Modus genannt). In einem L3-Cluster können Clusterknoten aus verschiedenen Netzwerken stammen. Sie müssen Knoten, die zu einem Netzwerk gehören, in einer einzelnen Knotengruppe gruppieren. Wenn beispielsweise n1, n2, n3 in netzwerk1 und n4, n5, n6 sind in netzwerk2, dann muss NG1 Knoten von netzwerk1 und NG2 müssen Knoten von netzwerk2 enthalten. Informationen zum Einrichten eines L3-Clusters finden Sie unter Erstellen eines Citrix ADC-Clusters.

> **Hinweis:**
>
> - Unterstützt ab NetScaler 11.
> - Die vorangehenden Funktionen einer Knotengruppe schließen sich gegenseitig aus. Dies bedeutet, dass eine Knotengruppe nur eine der oben genannten Funktionen bereitstellen kann.

Cluster- und Knotenstatus

October 5, 2021

Damit ein Cluster funktionsfähig ist, müssen die meisten Knoten (n/2 + 1) operativ aktiv sein (der Betriebszustand ist ACTIVE).

> **Wichtig**
>
> Ab NetScaler Release 10.5 können Sie den Cluster so konfigurieren, dass er funktionsfähig ist, auch wenn die Mehrheitskriterien nicht erfüllt sind. Diese Konfiguration muss beim Erstellen eines Clusters durchgeführt werden.

Weitere Informationen zu den Status eines Clusterknotens finden Sie unter Status eines Clusterknotens.

Routing in einem Cluster

October 5, 2021

Das Routing in einem Cluster funktioniert genauso wie das Routing in einem eigenständigen System. Ein paar Punkte zu beachten:

- Alle Routingkonfigurationen müssen über die Cluster-IP-Adresse ausgeführt werden, und die Konfigurationen werden an die anderen Clusterknoten weitergegeben.
- Routen sind auf die maximale Anzahl von ECMP-Routen begrenzt, die vom Upstream-Router unterstützt werden.
- Knotenspezifische Routing-Konfigurationen müssen mithilfe des Owner-Node-Arguments wie folgt durchgeführt werden:

```
  router ospf
    owner-node 0
      ospf router-id 97.131.0.1
    exit-owner-node
  !
<!--NeedCopy-->
```

Der folgende Befehl zeigt die konsolidierte Clusterkonfiguration für alle Knoten in VTYSH an.

```
show cluster-config
```

Der folgende Befehl zeigt den Clusterstatus auf jedem Knoten an.

```
show cluser node
```

IPv4-Routing im L2-Cluster

Der folgende Abschnitt enthält Beispielkonfigurationen, die Ihnen bei der Konfiguration von IPv4-OSPF- und BGP-Routing im L2-Cluster helfen.

Hinzufügen von Spotted-SNIP-Adresse und Aktivieren von dynamischem Routing

In der folgenden Konfiguration sind OSPF und BGP-Routing aktiviert. Außerdem werden gespotte SNIP-Adressen hinzugefügt und dynamisches Routing für diese SNIP-Adressen aktiviert.

```
en ns fea ospf bgp
add vlan 10
add ns ip 10.10.10.1 255.255.255.0 -dynamicrouting enabled -ownernode 1
add ns ip 10.10.10.2 255.255.255.0 -dynamicrouting enabled -ownernode 2
add ns ip 10.10.10.3 255.255.255.0 -dynamicrouting enabled -ownernode 3
bind vlan 10 -ipaddress 10.10.10.1 255.255.255.0
```



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

VTYSH IPv4 OSPF-Konfiguration

Um IPv4 OSPF im L2-Cluster zu konfigurieren, müssen Sie:

- Legen Sie die Priorität auf Null fest.
- Konfigurieren Sie die Router-ID als Spotted Konfiguration.

> **Hinweis:**
>
> Die OSPF-Konfigurationsrichtlinien für den L2-Cluster gelten auch für Ospfv3.

In der folgenden Beispielkonfiguration wird IPv4 OSPF konfiguriert.

```
       interface vlan10
        IP OSPF PRIORITY 0
        !
       router ospf
           owner-node 1
             ospf router-id 97.131.0.1
           exit-owner-node
           owner-node 2
             ospf router-id 97.131.0.2
           exit-owner-node
           owner-node 3
             ospf router-id 97.131.0.3
           exit-owner-node
       network 10.10.10.0/24 area 0
       redistribute kernel
        !
<!--NeedCopy-->
```

VTYSH IPv4 BGP-Konfiguration

In der folgenden VTYSH Beispielkonfiguration ist IPv4 BGP konfiguriert.

```
    router bgp 100
      neighbor 10.10.10.10 remote-as 200
     owner-node 1
      neighbor 10.10.10.10 update-source 10.10.10.1
     exit-owner-node
```



```
6       owner-node 2
7        neighbor 10.10.10.10 update-source 10.10.10.2
8       exit-owner-node
9       owner-node 3
10       neighbor 10.10.10.10 update-source 10.10.10.3
11      exit-owner-node
12     redistribute kernel
13     !
14 <!--NeedCopy-->
```

> **Hinweis:**
>
> Der Befehl update-source wird für jeden Nachbarn mit dem Argument Besitzer-Node in der folgenden Konfiguration verwendet, um eine Verbindung mit der richtigen Quell-IP herzustellen.

IPv6-Routing im L2-Cluster

Der folgende Abschnitt enthält Beispielkonfigurationen, die Ihnen bei der Konfiguration von IPv6-OSPF- und BGP-Routing im L2-Cluster helfen.

IPv6-Routing aktivieren

Bevor Sie IPv6-Routing in einem L2-Cluster konfigurieren, müssen Sie das IPv6-Feature aktivieren.

So aktivieren Sie IPv6-Routing mit der CLI,

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `enable ns fea ipv6pt`

Hinzufügen von gespotted SNIP6-Adresse und Aktivieren von dynamischem Routing

In der folgenden Konfiguration sind OSPF und BGP-Routing aktiviert. Außerdem werden gespotte SNIP6-Adressen hinzugefügt und dynamisches Routing für diese SNIP6-Adressen aktiviert.

```
1 add ns ip6 3ffa::1/64 -dynamicrouting enabled -ownernode 1
2 add ns ip6 3ffa::2/64 -dynamicrouting enabled -ownernode 2
3 add ns ip6 3ffa::3/64 -dynamicrouting enabled -ownernode 3
4 add vlan 10
5 bind vlan 10 -ipaddress 3ffa::1/64
6 <!--NeedCopy-->
```


VTYSH IPv6 BGP-Konfiguration

In der folgenden VTYSH Beispielkonfiguration ist IPv6 BGP konfiguriert.

```
  router bgp 100
   neighbor 3ffa::10 remote-as 200
     owner-node 1
      neighbor 3ffa::10 update-source 3ffa::1
     exit-owner-node
     owner-node-2
      neighbor 3ffa::10 update-source 3ffa::2
     exit-owner-node
     owner-node-3
      neighbor 3ffa::10 update-source 3ffa::3
     exit-owner-node
   no neighbor 3ffa::10 activate
   address-family ipv6
    redistribute kernel
    neighbor 3ffa::10 activate
   exit-address-family
  !
<!--NeedCopy-->
```

Installieren von IPv6-erlernten Routen

Der Citrix ADC Cluster kann Routen verwenden, die von verschiedenen Routingprotokollen gelernt wurden, nachdem Sie die Routen in der Citrix ADC Cluster-Routingtabelle installiert haben.

So installieren Sie IPv6-gelernte Routen in die interne Routingtabelle mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `ns route-install ipv6 bgp`
- `ns route-install ipv6 ospf`
- `ns route-install default`

> **Hinweis:**
>
> - Wenn Sie IPv4-Routen auf einem IPv6-Nachbarn austauschen müssen, müssen Sie den Befehl`no neighbor 3ffa::10 active` VTYSH aus der früheren Konfiguration entfernen.
> - Der `update-source` VTYSH-Befehl muss für jeden Besitzerknoten verwendet werden, um die richtige IPv6-Quell-IP anzugeben, während die Verbindung mit dem BGP-Peer

> hergestellt wird, wie in der BGP-IPv4-Konfiguration angegeben.

Routing in einem L3-Cluster

Das Routing in einem L3-Cluster funktioniert nur, wenn die folgenden Konfigurationen auf der Citrix ADC Appliance durchgeführt werden.

- Aktivieren Sie das dynamische Routing für ein VLAN.

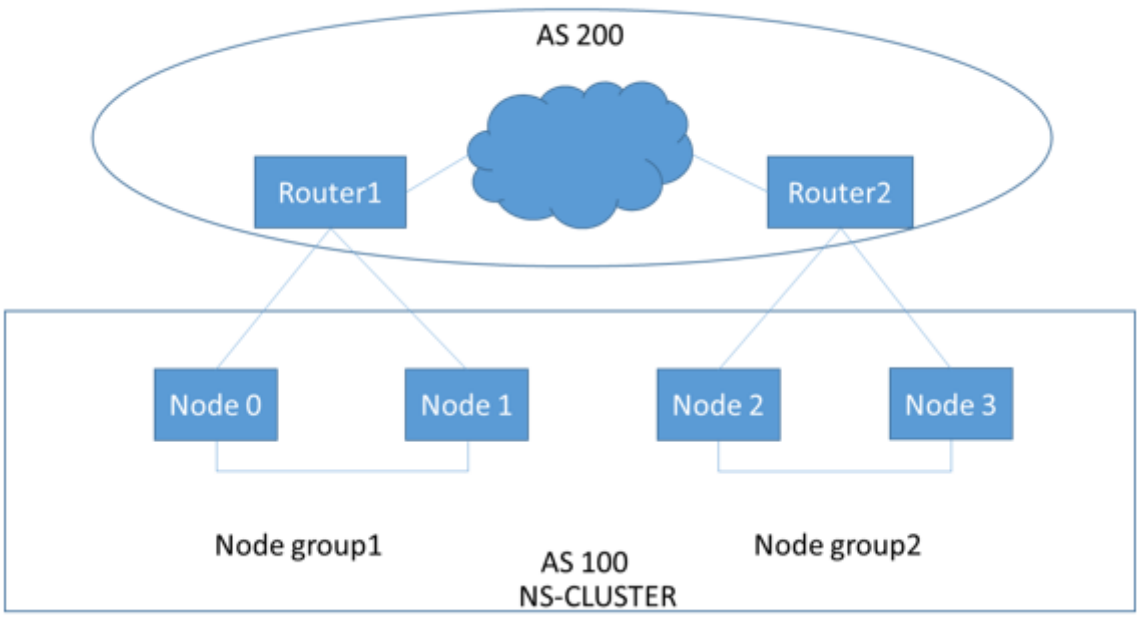
```
set vlan <id> -dynamicrouting enabled
<!--NeedCopy-->
```

- Um alle Cluster-Knoten zu erreichen, müssen VIP, CLIP und Citrix ADC IP (NSIP) zusammen mit dem `set vlan` Befehl durch Routingprotokolle beworben werden.

Bereitstellungsszenario für BGP im L3-Cluster

Betrachten Sie ein Beispiel, bei dem alle Clusterknoten im AS 100-Netzwerk gruppiert sind und sich die Upstream-Router in einem anderen AS 200 befinden.

Die folgende Abbildung zeigt die AS 100- und AS 200-Bereitstellung in einem Cluster-Setup.



In dieser Bereitstellung wirbt CLIP CCO für Upstream-Router an. Einige Cluster-Knoten löschen den angekündigten Datenverkehr, da eine AS-Schleife erkannt wird.

Um das Problem zu beheben, konfigurieren Sie den folgenden Befehl im VTYSH BGP-Router-Modus für jeden Nachbarn.

Geben Sie an der VTYSH Eingabeaufforderung Folgendes ein:

```
neighbor <peer_ip> allowas-in 1
```

Als bewährte Methode empfiehlt Citrix, eine der folgenden Optionen zu konfigurieren:

- Konfigurieren Sie Routenkarten, um nur die gewünschten Netzwerke wie Standardroute, Citrix ADC IP (NSIP) und NSIP-Subnetze auf Clusterknoten zu lernen.
- Konfigurieren Sie Upstream-Routen, um nur gewünschte Netzwerke wie CLIP und Citrix ADC IP (NSIP) im Cluster anzukündigen.

IP-Adressierung für einen Cluster

October 5, 2021

Zusätzlich zu den Standardtypen von Citrix ADC-eigenen IP-Adressen — Citrix ADC NSIP, Virtual IP (VIP) und Subnet IP (SNIP) — kann eine Cluster-Citrix ADC Appliance über eine Cluster-Verwaltungs-IP (CLIP) verfügen. Es kann auch gestreifte und gespotte IP-Adressen haben.

- **CLIP-Adresse.** Eine IP-Adresse, die dem Cluster Coordinator Node (CCO) gehört. Die CLIP-Adresse kann in einem Cluster-Setup zwischen verschiedenen Knoten schweben. Wenn der CLIP auf einen anderen Knoten des Clusters verschoben wird, wird dieser Knoten zum CCO. Der CCO ist die Citrix ADC Appliance, die für Verwaltungsaufgaben im Cluster zuständig ist. Ein Netzwerkadministrator verwendet die CLIP-Adresse, um eine Verbindung mit dem Cluster herzustellen, um Konfigurations- und Verwaltungsaufgaben durchzuführen, z. B. den Zugriff auf die einheitliche GUI, das Reporting, das Verfolgen des Paketflusses und das Sammeln von Protokollen. Sie können mehrere CLIP-Adressen in einem Cluster in demselben oder anderen Netzwerken hinzufügen. Nur Konfigurationen, die auf dem CCO über die Cluster-IP-Adresse durchgeführt werden, werden an andere Knoten im Cluster weitergegeben.
- **Striped IP-Adresse**. Eine logische IP-Adresse, die auf allen Knoten des Clusters verfügbar ist, kann es sich um eine VIP- oder SNIP-Adresse handeln.
- **Spotted IP-Adresse**. Eine logische IP (vorzugsweise SNIP-Adresse) ist nur auf einem Knoten verfügbar. Eine gespotte IP-Adresse hat Sichtbarkeit nur auf diesem Knoten. Um den Overhead für die Verkehrssteuerung zu minimieren, empfiehlt Citrix, eine gefleckte SNIP-Adresse für die Back-End-Kommunikation mit dem Server zu verwenden.

Die folgende Tabelle enthält die Details der Konfigurationen.

IP-Adresse	NSIP	VIP	SNIP
Gefleckt	Ja	Ja	Ja
Gestreift	Nein	Ja	Ja

Beispielsweise müssen Sie in einer Clustergruppe mit vier Knoten jeden Knoten mit einer gespotted SNIP-Adresse konfigurieren. Weitere Informationen zum Konfigurieren einer Spotted IP-Konfiguration finden Sie unter Striped, Partially Striped und Spotted Configurations.

Sie können eine SNIP-Adresse so definieren, dass sie nur auf einem Knoten aktiv ist oder auf allen Knoten aktiv ist. Wenn die virtuelle IP-Adresse und die Subnetz-IP-Adresse nur auf einem bestimmten Knoten verfügbar sind, ist sie von gepunkteter Konfiguration. Die Konfiguration ist als Striped definiert, wenn die Subnetz-IP-Adresse und die IP-Adresse des virtuellen Servers auf allen Knoten verfügbar sind. Gefleckte SNIP-Adressen helfen dabei, den Lenkungs- und Backplane-Verkehr zu reduzieren.

Best Practices für VLAN-Bindungen und Routenkonfiguration beim Beitritt eines Knotens mit dem Cluster

VLAN-IP-Bindungen

Wenn Sie ein VLAN mit der gepunkteten IP-Adresse binden, muss der Citrix ADC Cluster mit den gefleckten IP-Adressen im selben Subnetz auf allen Knoten konfiguriert werden. In einem Cluster mit zwei Knoten mit Knoten 0 und Knoten 1 können Sie beispielsweise die folgende Konfiguration haben:

```
1 add ns ip 192.254.101.101 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 1
2 add ns ip 192.254.101.102 255.255.255.0 -vServer DISABLED -
     dynamicRouting ENABLED -ownerNode 0
3 add vlan 100
4 bind vlan 100 -IPAddress 192.254.101.101 255.255.255.0
5 <!--NeedCopy-->
```

Routing-Konfiguration

Wenn eine Routingkonfiguration mit der gepunkteten IP-Adresse als Standard-Gateway erforderlich ist, muss der ADC-Cluster mit den gepunkteten IP-Adressen im selben Subnetz auf allen Knoten konfiguriert werden. In einem Cluster mit zwei Knoten mit Knoten 0 und Knoten 1 können Sie beispielsweise die folgende Konfiguration haben:


```
add ns ip 192.254.101.101 255.255.255.0 -vServer DISABLED -
    dynamicRouting ENABLED -ownerNode 1
add ns ip 192.254.101.102 255.255.255.0 -vServer DISABLED -
    dynamicRouting ENABLED -ownerNode 0

add route 192.254.102.0 255.255.255.0 192.254.101.103
<!--NeedCopy-->
```

> **Hinweis:**
>
> In einem L3-Cluster-Setup wird nur die SNIP-Konfiguration von Spotted unterstützt.

Konfigurieren von Layer-3-Clustering

October 5, 2021

Das L3-Cluster verstehen

Die Forderung, die Hochverfügbarkeitsbereitstellung zu erweitern und die Skalierbarkeit des Clientdatenverkehrs in verschiedenen Netzwerken zu erhöhen, wird zur Einrichtung des L3-Clusters geleitet. Mit dem L3-Cluster können Sie Citrix ADC Appliances über einzelne Subnetze (L2-Cluster) gruppieren.

L3-Cluster wird auch als Cluster in Independent Network Configuration (INC) -Modus bezeichnet. Bei der L3-Clusterbereitstellung werden die Clusterknoten im selben Netzwerk zu einer Node-Gruppe gruppiert. Der L3-Cluster verwendet GRE-Tunneling, um die Pakete über Netzwerke hinweg zu steuern. Die Heartbeat-Nachrichten in den L3-Clustern werden weitergeleitet.

Dieses Dokument enthält die folgenden Details:

- Architektur
- Beispiel

Architektur

Die L3-Cluster-Architektur besteht aus folgenden Komponenten:

- **Knotengruppe**. Die Clusterknoten aus jedem Netzwerk (n1, n2) und (n3, n4) sind, wie in der folgenden Abbildung dargestellt, zu einer Node-Gruppe gruppiert. Diese Node-Gruppen werden mit dem Layer-3-Switch auf beiden Seiten des Netzwerks beendet.

  - Der Cluster kommuniziert mit dem Client über die physischen Verbindungen zwischen dem Clusterknoten und dem clientseitigen Verbindungsgerät. Die logische Gruppierung dieser physischen Verbindungen wird als Client-Datenebene bezeichnet.
  - Der Cluster kommuniziert mit dem Server über die physischen Verbindungen zwischen dem Clusterknoten und dem serverseitigen Verbindungsgerät. Die logische Gruppierung dieser physischen Verbindungen wird als Serverdatenebene bezeichnet.
- **Backplane Switch.** Clusterknoten innerhalb desselben Netzwerks kommunizieren über die Cluster-Backplane miteinander. Die Backplane ist ein Satz von Schnittstellen, bei denen eine Schnittstelle jedes Knotens mit einem gemeinsamen Switch verbunden ist, der als Cluster-Backplane-Switch bezeichnet wird.
- **GRE Tunnel.** Die Pakete zwischen Knoten in einem L3-Cluster werden über einen unverschlüsselten GRE-Tunnel ausgetauscht, der die NSIP-Adressen der Quell- und Zielknoten für das Routing verwendet. Der Steuerungsmechanismus ändert sich für Knoten, die zu dem unterschiedlichen Netzwerk gehören. Die Pakete werden durch einen GRE-Tunnel zum Knoten im anderen Subnetz geleitet, anstatt den MAC neu zu schreiben.

Beispiel

Betrachten Sie ein Beispiel für eine L3-Clusterbereitstellung, die aus folgenden Komponenten besteht:

- Drei Citrix ADC Appliances (n1, n2 und n3) sind in Nodegroup1 gruppiert.
- Ebenso sind die Knoten n4 und n5 in Nodegroup2 gruppiert. Im dritten Netzwerk gibt es zwei Knotengruppen. Nodegroup3 enthält n6 und n7 und Nodegroup4 enthält n8 und n9.
- Die Citrix ADC Appliances, die zum selben Netzwerk gehören, werden zu einer Knotengruppe zusammengefasst.

Punkte, die vor der Konfiguration des L3-Clusters zu berücksichtigen sind

Berücksichtigen Sie die folgenden Punkte, bevor Sie den L3-Cluster auf einer Citrix ADC Appliance konfigurieren:

- Bei der Konfiguration von L3-Subnetzen ist die Rückwandplatine nicht erforderlich. Wenn die Rückwandplatine nicht angegeben ist, geht der Knoten nicht in den Fehlerstatus der Rückwandplatine.

  > **Hinweis:**
  >
  > Wenn Sie mehr als einen Knoten im selben L2-Netzwerk haben, ist es zwingend erforderlich, die Backplane-Schnittstelle zu definieren. Wenn die Backplane-Schnittstelle nicht erwähnt wird, gehen die Knoten in den Fehlerstatus der Rückwandplatine.

- L2-Funktionen und Stripeset-SNIPs werden im L3-Cluster nicht unterstützt.

- Die Verteilung des externen Datenverkehrs im L3-Cluster unterstützt nur Equal Cost Multiple Path (ECMP).
- Die ICMP-Fehler und die Fragmentierung werden nicht verarbeitet, wenn die Steuerung in einer L3-Clusterbereitstellung deaktiviert ist:
- Die Netzwerk-Entitäten (`route`, `route6`, `pbr` und `pbr6`) müssen an die Konfigurationsknotengruppe gebunden sein.
- VLAN, RNAT und IP-Tunnel können nicht an eine Konfigurationsknotengruppe gebunden werden.
- Die Konfigurationsknotengruppe muss immer die Eigenschaft STRICT “YES” haben.
- Die Cluster-Knoten dürfen nicht über den Befehl “Clusterknoten hinzufügen” zu einer Konfigurationsknotengruppe hinzugefügt werden.
- Der `add cluster instance -INC enabled` Befehl löscht die Netzwerkeinheiten (route, route6, PBR, pb6, RNAT, IP-Tunnel, ip6tunnel).
- Der `clear config extended`+ Befehl löscht die Entitäten (route, route6, PBR, pb6, RNAT, IP-Tunnel, ip6tunnel) in einem L3-Cluster nicht.

Konfigurieren des L3-Clusters

In einer L3-Clusterkonfiguration hat der Clusterbefehl verschiedene zu konfigurierende Attribute, die auf Knoten und Knotengruppen basieren. Die L3-Clusterkonfiguration umfasst neben IPv4-Profilen auch ein IPv6-Profil.

Das Konfigurieren eines L3-Clusters auf einer Citrix ADC Appliance besteht aus den folgenden Aufgaben:

- Erstellen einer Clusterinstanz
- Erstellen einer Knotengruppe im L3-Cluster
- Hinzufügen einer Citrix ADC Appliance zum Cluster und einer Gruppe mit Knotengruppe
- Cluster-IP-Adresse zum Knoten hinzufügen
- Aktivieren der Cluster-Instanz
- Speichern der Konfiguration
- Hinzufügen eines Knotens zu einer bestehenden Knotengruppe
- Erstellen einer Knotengruppe im L3-Cluster
- Gruppieren Sie neue Knoten in die neu erstellte Knotengruppe
- Verbinden Sie den Knoten mit dem Cluster

Konfigurieren des Folgenden über die CLI

- **So erstellen Sie eine Clusterinstanz**


```
add cluster instance <clid> -inc (<ENABLED|DISABLED>)[-processLocal <
ENABLED | DISABLED]
```

- **So erstellen Sie eine Knotengruppe im L3-Cluster**

  ```
  add cluster nodegroup <name>
  ```

- **So fügen Sie dem Cluster eine Citrix ADC Appliance hinzu und verknüpfen Sie sie mit Knotengruppe**

  ```
  add cluster node <nodeid> <nodeip> -backplane <interface_name> node
  group <ng>
  ```

- **So fügen Sie die Cluster-IP-Adresse auf diesem Knoten hinzu**

  ```
  add ns ip <IPAddress> <netmask> -type clip
  ```

- **Aktivieren der Cluster-Instanz**

  ```
  enable cluster instance <clId>
  ```

- **Speichern der Konfiguration**

  ```
  save ns config
  ```

- **Warmer Neustart der Appliance**

  ```
  reboot -warm
  ```

- **So fügen Sie einer vorhandenen Knotengruppe einen neuen Knoten hinzu**

  ```
  add cluster node <nodeid> <nodeip> -nodegroup <ng>
  ```

- **So erstellen Sie eine neue Knotengruppe im L3-Cluster**

  ```
  add cluster nodegroup <ng>
  ```

- **So gruppieren Sie neue Knoten zur neu erstellten Knotengruppe**

  ```
  add cluster node <nodeid> <nodeip> -nodegroup <ng>
  ```

- **So verbinden Sie den Knoten mit dem Cluster**

```
1     join cluster  - clip <ip_addr> -password <password>
2
3     add cluster instance 1  - inc ENABLED  - processLocal  ENABLED
4
5        Done
6 <!--NeedCopy-->
```


> **Hinweis:**
>
> Der “inc” -Parameter muss ENABLED für einen L3-Cluster sein.

```
    add cluster nodegroup ng1

       Done

    > add cluster node 0 1.1.1.1 -state ACTIVE -backplane 0/1/1 -
       nodegroup ng1

       Done

    > add ns ip 1.1.1.100 255.255.255.255 -type clip

       Done

    > enable cluster instance 1

       Done

    > save ns config

       Done

    > add cluster node 1 1.1.1.2 -state ACTIVE -nodegroup ng1

       Done

    > add cluster nodegroup ng2

       Done

    > add cluster node 4 2.2.2.1 -state ACTIVE -nodegroup ng2

       Done

    > add cluster node 5 2.2.2.2 -state ACTIVE -nodegroup ng2

       Done

    > join cluster -clip 1.1.1.100 -password nsroot
<!--NeedCopy-->
```


IP-Adresse des Werbeclusters eines L3-Clusters

Konfigurieren Sie die Cluster-IP-Adresse, die für den Upstream-Router beworben werden soll, um die Clusterkonfiguration von jedem Subnetz aus zugänglich zu machen.Die Cluster-IP-Adresse wird von den auf einem Knoten konfigurierten dynamischen Routingprotokollen als Kernel-Route angekündigt.

Die Werbung für die Cluster-IP-Adresse besteht aus folgenden Aufgaben:

- **Aktivieren Sie die Host-Route-Option der Cluster-IP-Adresse**.Die Option Host-Route überträgt die Cluster-IP-Adresse zur Umverteilung der Kernel-Route durch dynamische Routingprotokolle an eine ZeBoS-Routingtabelle.
- **Konfigurieren eines dynamischen Routingprotokolls auf einem Knoten**.Ein dynamisches Routingprotokoll gibt die Cluster-IP-Adresse an den Upstream-Router an. Weitere Informationen zum Konfigurieren eines dynamischen Routingprotokolls finden Sie unterKonfigurieren dynamischer Routen.

So aktivieren Sie die Host-Routenoption der Cluster-IP-Adresse mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
-  add nsip <IPAddress> <netmask> -hostRoute ENABLED

-  show nsip <IPAddress>

    > add ns ip 10.102.29.60 255.255.255.255 -hostRoute ENABLED

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

Striped-, Teil-Striped- und Spotted-Konfigurationen auf L3-Cluster

Die gefleckten und teilweise gestreiften Konfigurationen auf dem L3-Cluster unterscheiden sich geringfügig vom L2-Cluster. Die Konfiguration kann von Knoten zu Knoten unterschiedlich sein, da sich die Knoten in verschiedenen Subnetzen befinden. Die Netzwerkkonfigurationen können knotenspezifisch im L3-Cluster sein, daher müssen Sie die gepunkteten oder teilweise gestreiften Konfigurationen basierend auf den unten genannten Parametern konfigurieren.

Um gepunktete, teilweise gestreifte Konfigurationen auf einer Citrix ADC Appliance über den L3-Cluster zu konfigurieren, führen Sie die folgenden Aufgaben aus:

- Hinzufügen einer Clusterbesitzergruppe zu einer statischen IPv4-Routingtabelle

- Hinzufügen einer Clusterbesitzergruppe zu einer statischen IPv6-Routingtabelle
- Hinzufügen einer Clusterbesitzergruppe zu einem IPv4-richtlinienbasierten Routing (PBR)
- Hinzufügen einer Clusterbesitzergruppe zu einem IPv6 PBR
- Hinzufügen eines VLAN
- Binden eines VLAN an eine bestimmte Eigentümergruppe der Clusterknotengruppe

Konfigurieren des Folgenden über die CLI

- **So fügen Sie einer statischen IPv4-Routentabelle der Citrix ADC Appliance eine Clusterbesitzergruppe hinzu**

  ```
  add route <network> <netmask> <gateway> -owner group <ng>
  ```

- **So fügen Sie einer statischen IPv6-Routingtabelle der Citrix ADC Appliance eine Clusterbesitzergruppe hinzu**

  ```
  add route6 <network> -owner group <ng>
  ```

- **So fügen Sie einer IPv4-PBR eine Clusterbesitzergruppe hinzu**

  ```
  add pbr <name> <action> -owner group <ng>
  ```

- **So fügen Sie einer IPv6-PBR eine Clusterbesitzergruppe hinzu**

  ```
  add pbr6 <name> <action> -owner group <ng>
  ```

- **So fügen Sie ein VLAN hinzu**

  ```
  add vlan <id>
  ```

- **So binden Sie ein VLAN an eine bestimmte Eigentümergruppe der Clusterknotengruppe**

  ```
  bind vlan <id> -ifnum - [IPAddress <ip_addr | ipv6_addr> [-owner group
  <ng>]
  ```

  Die folgenden Befehle sind Beispielbeispiele für gepunktete und teilweise gestreifte Konfigurationen, die mit der CLI konfiguriert werden können.

```
1     > add route 10.102.29.0 255.255.255.0 10.102.29.2  - ownergroup ng2
2
3         Done
4
5     > add route6 fe80::9404:60ff:fedd:a464/64  - ownergroup ng1
6
7         Done
8
9     > add pbr pbr1 allow  - ownergroup ng1
10
```



```
11          Done
12
13      > add pbr6 pbr2 allow  -ownergroup ng2
14
15          Done
16
17      > add vlan 2
18
19          Done
20
21      > bind vlan 2  -ifnum 1/2  -[IPAddress 10.102.29.80 | fe80::9404:60
           ff:fedd:a464/64-ownergroup ng1
22
23          Done
24  <!--NeedCopy-->
```

Konfigurieren der Knotengruppe

Um in einem L3-Cluster dieselben Konfigurationen für mehr als eine Knotengruppe zu replizieren, werden die folgenden Befehle verwendet:

Konfigurieren des folgenden Mithilfe der CLU

- **So fügen Sie der Routingtabelle der Citrix ADC Appliance eine statische IPv4-Route hinzu**

  ```
  add route <network> <netmask> <gateway> -ownerGroup <ng>
  ```

Beispielkonfiguration:

```
1  add route 0 0 10.102.53.1  -ownerGroup ng1
2
3  add route 0 0 10.102.53.1  -ownerGroup ng2
4  <!--NeedCopy-->
```

Sie definieren eine neue Knotengruppe “all”, um die vorangehende Konfiguration zu unterstützen, und müssen die folgenden Befehle konfigurieren:

Konfigurieren des Folgenden über die CLI

- **So fügen Sie dem Cluster eine neue Knotengruppe mit dem Strict-Parameter hinzu**

  ```
  add cluster node group <name> -strict <YES | NO>
  ```


- **So binden Sie einen Clusterknoten oder eine Entität an die angegebene Knotengruppe**

  ```
  bind cluster nodegroup <name> -node <nodeid>
  ```

- **So fügen Sie der gesamten Eigentümergruppe eine statische IPv4-Route hinzu**

  ```
  add route <network> <netmask> <gateway> -ownerGroup <ng>
  ```

Beispielkonfiguration:

```
add cluster nodegroup all -strict YES

bind cluster nodegroup all -node 1

bind cluster nodegroup all -node 2

add route 0 0 10.102.53.1 -ownerGroup all
<!--NeedCopy-->
```

Verkehrsverteilung in einem L3-Cluster

In einem Cluster-Setup zeigen externe Netzwerke die Sammlung von Citrix ADC Appliances als einzelne Entität an. Daher muss der Cluster einen einzelnen Knoten auswählen, der den Datenverkehr empfangen muss. Im L3-Cluster erfolgt diese Auswahl mit dem ECMP. Der ausgewählte Knoten wird als Flow Receiver bezeichnet.

> **Hinweis:**
>
> Für einen L3-Cluster (Knoten über verschiedene Netzwerke) kann nur die ECMP-Verkehrsverteilung verwendet werden.

Der Flussempfänger ruft den Datenverkehr ab und bestimmt dann mithilfe der internen Clusterlogik den Knoten, der den Datenverkehr verarbeiten muss. Dieser Knoten wird als Flow-Prozessor bezeichnet. Der Flow-Empfänger steuert den Datenverkehr zum Flow-Prozessor über die Backplane, wenn sich der Flow-Empfänger und der Flow-Prozessor im selben Netzwerk befinden. Der Verkehr wird durch den Tunnel gelenkt, wenn sich der Flow-Empfänger und der Flow-Prozessor in verschiedenen Netzwerken befinden.

> **Hinweis:**
>
> - Der Flow-Empfänger und der Flow-Prozessor müssen Knoten sein, die den Datenverkehr bedienen können.
> - Ab NetScaler 11 können Sie die Steuerung auf der Cluster-Backplane deaktivieren. Weitere Informationen finden Sie unter Deaktivieren der Lenkung auf der Cluster-Backplane.

Die vorangehende Abbildung zeigt eine Client-Anfrage, die durch den Cluster fließt. Der Client sendet eine Anforderung an eine virtuelle IP (VIP) -Adresse. Ein auf der Clientdatenebene konfigurierter Verkehrsverteilungsmechanismus wählt einen der Clusterknoten als Flow-Empfänger aus. Der Flussempfänger empfängt den Datenverkehr, bestimmt den Knoten, der den Datenverkehr verarbeiten muss, und steuert die Anforderung an diesen Knoten (es sei denn, der Flow-Empfänger wählt sich selbst als Flow-Prozessor aus). Wenn sich der Flow-Prozessor und der Flow-Empfänger in derselben Knotengruppe befinden, wird das Paket über die Backplane gesteuert. Und wenn sich der Flow-Prozessor und der Flow-Receiver in verschiedenen Knotengruppen befinden, wird das Paket über den gerouteten Pfad durch den Tunnel gesteuert.

Der Flow-Prozessor stellt eine Verbindung mit dem Server her. Der Server verarbeitet die Anforderung und sendet die Antwort an die Subnetz-IP-Adresse (SNIP), die die Anforderung an den Server gesendet hat. Da der SNIP im L3-Cluster immer ein Spotted SNIP ist, erhält der Knoten, dem die SNIP-Adresse gehört, die Antwort vom Server.

Einrichten eines Citrix ADC-Clusters

October 5, 2021

Citrix ADC Appliances, die Sie dem Cluster hinzufügen möchten, müssen die unter Voraussetzungen für Clusterknotenangegebenen Kriterien erfüllen. Bevor Sie einen Cluster tatsächlich einrichten, müssen Sie die Cluster-Grundlagen kennen. Weitere Informationen finden Sie unter Cluster-Übersicht.

Für die Bildung eines Clusters müssen Sie die Kommunikation zwischen Knoten einrichten, den Cluster erstellen (indem Sie die erste Citrix ADC Appliance hinzufügen) und dann die anderen Clusterknoten hinzufügen. Jeder dieser Schritte wird mit relevanten Details in den nachfolgenden Themen erläutert.

> **Hinweis:**
>
> Obwohl es einige Unterschiede beim Einrichten eines L2- und L3-Clusters gibt, gibt es auch viele Ähnlichkeiten. In den nachfolgenden Themen wird das Setup für beide Clustertypen erläutert, während die Konfigurationen hervorgehoben werden, die spezifisch für L3-Cluster sind.

Einrichten der Kommunikation zwischen Knoten

October 5, 2021

Die Knoten in einem Cluster-Setup kommunizieren mit den folgenden Kommunikationsmechanismen zwischen Knoten:

- Knoten, die sich innerhalb des Netzwerks befinden (dasselbe Subnetz) kommunizieren miteinander über die Cluster-Backplane. Die Rückwandplatine muss explizit eingerichtet werden. Im Folgenden finden Sie die detaillierten Schritte.
- Über Netzwerke hinweg erfolgt die Steuerung von Paketen über einen GRE-Tunnel und andere Knoten-zu-Knode-Kommunikation wird bei Bedarf über Knoten weitergeleitet.

> **Wichtig**
>
> - Ab Release 11.0 kann ein Cluster Knoten aus verschiedenen Netzwerken enthalten.
> - Ab Release 13.0 Build 58.3 wird die GRE-Steuerung auf Fortville NICs in einem L3-Cluster unterstützt.

Um die Cluster-Backplane einzurichten, führen Sie für jeden Knoten die folgenden Schritte aus

1. Identifizieren Sie die Netzwerkschnittstelle, die Sie für die Rückwandplatine verwenden möchten.
2. Verbinden Sie ein Ethernet- oder optisches Kabel von der ausgewählten Netzwerkschnittstelle mit dem Cluster-Backplane-Switch.

Um beispielsweise Schnittstelle 1/2 als Backplane-Schnittstelle für Knoten 4 zu verwenden, schließen Sie ein Kabel von der 1/2 Schnittstelle von Knoten 4 an den Backplane-Switch an.

Wichtige Punkte beim Einrichten der Cluster-Backplane zu beachten

- Verwenden Sie die Verwaltungsschnittstelle der Appliance (0/x) nicht als Backplane-Schnittstelle. In einem Cluster wird die Schnittstelle 0/1/x folgendermaßen gelesen:

  0 -> Knoten-ID 0
  1/x -> Citrix ADC Schnittstelle

- Verwenden Sie keine Backplane-Schnittstellen für die Client- oder Serverdatenebenen.
- Citrix empfiehlt, den Link Aggregat-Kanal (LA) für die Cluster-Backplane zu verwenden.
- In einem Cluster mit zwei Knoten, in dem die Rückwandplatine Back-to-back verbunden ist, ist der Cluster unter einer der folgenden Bedingungen operativ DOWN:
  - Einer der Knoten wird neu gestartet.
  - Die Backplane-Schnittstelle eines der Knoten ist deaktiviert.

  Daher empfiehlt Citrix, dass Sie einen separaten Switch für die Rückwandplatine festlegen, damit der andere Clusterknoten und der Datenverkehr nicht beeinträchtigt werden. Sie können den Cluster nicht mit einer Back-to-Back-Link skalieren. Wenn Sie die Clusterknoten skalieren, kann es zu Ausfallzeiten in der Produktionsumgebung kommen.

- Backplane-Schnittstellen aller Knoten eines Clusters müssen an denselben Switch angeschlossen und an dasselbe L2-VLAN gebunden sein.
- Wenn Sie mehrere Cluster mit derselben Clusterinstanz-ID haben, stellen Sie sicher, dass die Backplane-Schnittstellen jedes Clusters an ein anderes VLAN gebunden sind.
- Die Backplane-Schnittstelle wird immer überwacht, unabhängig von den HA-Überwachungseinstellungen dieser Schnittstelle.
- Der Status des MAC-Spoofings auf den verschiedenen Virtualisierungsplattformen kann den Lenkmechanismus auf der Cluster-Backplane beeinflussen. Stellen Sie daher sicher, dass der entsprechende Status konfiguriert ist:
  - XenServer - MAC-Spoofing deaktivieren
  - Hyper-V - MAC-Spoofing aktivieren
  - VMware ESX - MAC-Spoofing aktivieren (stellen Sie außerdem sicher, dass Geschmiedete Übertragungen aktiviert ist)
- Die MTU für die Cluster-Backplane wird automatisch aktualisiert. Wenn jedoch Jumbo-Frames auf dem Cluster konfiguriert sind, muss die MTU der Cluster-Backplane explizit konfiguriert werden. Der Wert muss auf 78 + X gesetzt werden, wobei X die maximale MTU der Client- und Server-Datenebene ist. Beispiel: Wenn die MTU einer Serverdatenebene 7500 und die Clientdatenebene 8922 beträgt. Die MTU einer Cluster-Backplane muss auf 78 + 8922 = 9000 eingestellt sein. Verwenden Sie den folgenden Befehl, um diese MTU festzulegen:

  ```
  > set interface <backplane_interface> -mtu <value>
  ```
- Die MTU für die Schnittstellen des Backplane-Switches muss größer oder gleich 1.578 Bytes sein. Sie ist anwendbar, wenn der Cluster Features wie MBF, L2-Richtlinien, ACLs, Routing in CLAG-Bereitstellungen und vPath aufweist.

UDP-basierte Tunnelunterstützung für L2- und L3-Cluster

Ab Citrix ADC Version 13.0 Build 36.x kann der Citrix ADC L2 und L3-Cluster den Datenverkehr mithilfe von UDP-basiertem Tunneling steuern. Es ist für die Kommunikation zwischen Knoten von zwei Knoten in einem Cluster definiert. Mithilfe des Parameters “Tunnelmodus” können Sie den GRE- oder UDP-Tunnelmodus über den Befehl “Clusterknoten hinzufügen und setzen” einstellen.

In einer L3-Clusterbereitstellung werden Pakete zwischen Citrix ADC Knoten über einen unverschlüsselten GRE-Tunnel ausgetauscht, der die NSIP-Adressen der Quell- und Zielknoten für das Routing verwendet. Wenn dieser Austausch über das Internet erfolgt, werden die NSIPs in Ermangelung eines IPsec-Tunnels im Internet verfügbar gemacht, was zu Sicherheitsproblemen führen kann.

> **Wichtig**
>
> Citrix empfiehlt Kunden, bei Verwendung eines L3-Clusters eine eigene IPsec-Lösung einzurichten.

In der folgenden Tabelle können Sie die Tunnelunterstützung basierend auf verschiedenen Bereitstellungen kategorisieren.

Typen von Lenkung	AWS	Microsoft Azure	Auf dem Gelände
MAC	Nicht unterstützt	Nicht unterstützt	Unterstützt
GRE Tunnel	Unterstützt	Nicht unterstützt	Unterstützt
UDP-Tunnel	Unterstützt	Unterstützt	Unterstützt

> **Wichtig**
>
> In einem L3-Cluster ist der Tunnelmodus standardmäßig auf GRE eingestellt.

Konfigurieren von UDP-basiertem Tunnel

Sie können einen Clusterknoten hinzufügen, indem Sie die Parameter der Knoten-ID festlegen und den Status erwähnen. Konfigurieren Sie die Rückwandplatine, indem Sie den Schnittstellennamen angeben, und wählen Sie den Tunnelmodus Ihrer Wahl (GRE oder UDP) aus.

CLI-Verfahren

So aktivieren Sie den UDP-Tunnelmodus mit der CLI.

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add cluster node <nodeId>@ [-state <state>] [-backplane <interface_name>] [-tunnelmode <tunnelmode>]`
- `set cluster node <nodeId>@ [-state <state>] [-tunnelmode <tunnelmode>]`

> **Hinweis:**
>
> Mögliche Werte für den Tunnelmodus sind NONE, GRE, UDP.

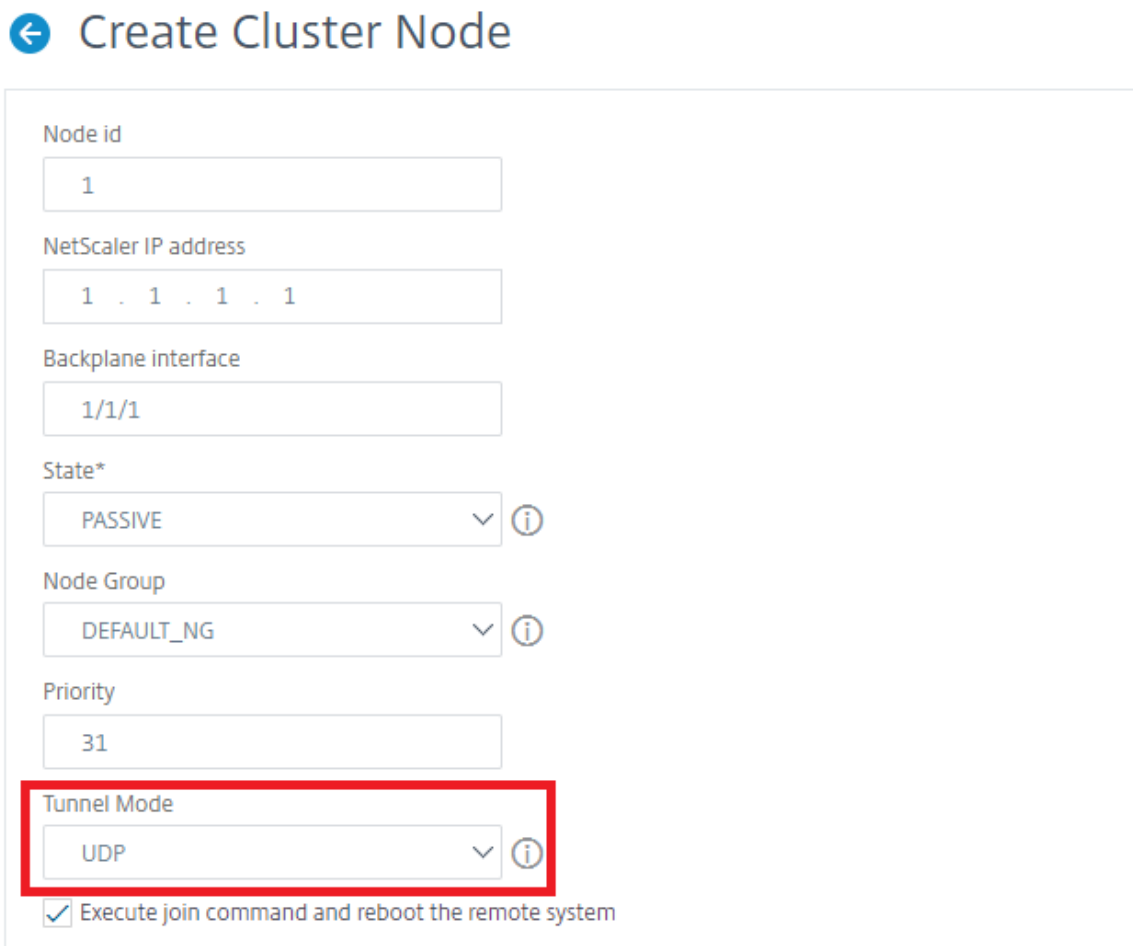
Beispiel

- `add cluster node 1 -state ACTIVE -backplane 1/1/1 -tunnelmode UDP`
- `set cluster node 1 -state ACTIVE -tunnelmode UDP`

GUI-Verfahren

So aktivieren Sie den UDP-Tunnelmodus mit der GUI.

1. Navigieren Sie zu **System > Cluster > Knoten**.
2. Klicken Sie auf der Seite **Clusterknoten** auf **Hinzufügen**.
3. Legen **Sie im Clusterknoten erstellen**den Parameter **Tunnelmodus** auf UDP fest, und klicken Sie auf **Erstellen**.



4. Klicken Sie auf **Schließen**.

Erstellen eines Citrix ADC-Clusters

October 5, 2021

Um einen Cluster zu erstellen, verwenden Sie zunächst eine der Citrix ADC Appliances, die Sie dem Cluster hinzufügen möchten. Auf diesem Knoten müssen Sie die Clusterinstanz erstellen und die

Cluster-IP-Adresse definieren. Dieser Knoten ist der erste Cluster-Knoten und wird als Cluster Configuration Coordinator (CCO) bezeichnet. Alle Konfigurationen, die für die Cluster-IP-Adresse ausgeführt werden, werden auf diesem Knoten gespeichert und dann an die anderen Clusterknoten weitergegeben.

Die Verantwortung von CCO in einem Cluster ist nicht auf einen bestimmten Knoten festgelegt. Es kann sich im Laufe der Zeit ändern, abhängig von den folgenden Faktoren:

- Die Priorität des Knotens. Der Knoten mit der höchsten Priorität (niedrigste Prioritätsnummer) wird zum CCO gemacht. Wenn daher ein Knoten mit einer niedrigeren Prioritätsnummer als der vorhandene CCO hinzugefügt wird, übernimmt der neue Knoten die CCO.

  > **Hinweis:**
  >
  > Knotenpriorität kann ab NetScaler 10.1 konfiguriert werden.

- Wenn der aktuelle CCO ausfällt, übernimmt der Node mit der nächstniedrigsten Prioritätsnummer die CCO. Wenn die Priorität nicht festgelegt ist oder mehrere Knoten mit der niedrigsten Prioritätsnummer vorhanden sind, wird der CCO aus einem der verfügbaren Knoten ausgewählt.

> **Hinweis:**
>
> Die Konfigurationen der Appliance (einschließlich SNIP-Adressen und VLANs) werden durch implizite Ausführung des `clear ns config extended` Befehls gelöscht. Das Standard-VLAN und NSVLAN werden jedoch nicht von der Appliance gelöscht. Wenn Sie das NSVLAN im Cluster verwenden möchten, stellen Sie daher sicher, dass es erstellt wird, bevor die Appliance dem Cluster hinzugefügt wird. Bei einem L3-Cluster (Clusterknoten in verschiedenen Netzwerken) werden Netzwerkkonfigurationen nicht von der Appliance gelöscht.
>
> **Wichtig**
>
> HA-Monitor (HAMON) auf einem Cluster-Setup wird verwendet, um die Integrität einer Schnittstelle auf jedem Knoten zu überwachen. Der HAMON-Parameter muss auf jedem Knoten aktiviert sein, um den Status der Schnittstelle zu überwachen. Wenn der Betriebszustand der HAMON aktivierten Schnittstelle aus irgendeinem Grund ausfällt, wird der jeweilige Clusterknoten als fehlerfrei markiert (NOT UP) und dieser Knoten kann den Datenverkehr nicht bedienen.

So erstellen Sie einen Cluster mit der Befehlszeilenschnittstelle

1. Melden Sie sich bei einer Appliance an (z. B. Appliance mit NSIP-Adresse 10.102.29.60), die Sie dem Cluster hinzufügen möchten.
2. Fügen Sie eine Clusterinstanz hinzu.

   ```
   add cluster instance <clId> -quorumType <NONE | MAJORITY> -inc <ENABLED
    | DISABLED> -backplanebasedview <ENABLED | DISABLED><!--NeedCopy-->
   ```


> **Hinweis:**
>
> ```
> 1    - Die Clusterinstanz-ID muss innerhalb eines LAN eindeutig
>        sein.
> ```
>
> - Der `-quorumType` Parameter muss in den folgenden Szenarien auf Mehrheit und nicht auf NONE gesetzt werden:
>   - Topologien, die keine redundanten Verbindungen zwischen Clusterknoten haben. Diese Topologien können aufgrund eines Single Point of Failure für die Netzwerkpartition anfällig sein.
>   - Bei allen Clustervorgängen, z. B. beim Hinzufügen oder Entfernen von Knoten.
> - Stellen Sie bei einem L3-Cluster sicher, dass der Parameter `-inc` auf ENABLED gesetzt ist. Der Parameter `-inc` muss für einen L2-Cluster deaktiviert sein.
> - Wenn der Parameter `-backplanebasedview` aktiviert ist, wird die Betriebsansicht (Satz von Knoten, die den Datenverkehr bedienen) basierend auf Heartbeats festgelegt, die nur auf der Backplane-Schnittstelle empfangen werden. Standardmäßig ist dieser Parameter deaktiviert. Wenn dieser Parameter deaktiviert ist, hängt ein Knoten nicht vom Heartbeat-Empfang nur auf der Backplane ab.

3. [Nur für einen L3-Cluster] Erstellen Sie eine Knotengruppe. Im nächsten Schritt muss der neu hinzugefügte Clusterknoten dieser Knotengruppe zugeordnet werden.

   > **Hinweis:**
   >
   > Diese Knotengruppe umfasst alle oder eine Teilmenge der Citrix ADC Appliances, die zum selben Netzwerk gehören.

   ```
   add cluster nodegroup <name><!--NeedCopy-->
   ```

4. Fügen Sie die Citrix ADC-Appliance zum Cluster hinzu.

   "'add cluster node -state -backplane -nodegroup

```
1 > **Hinweis** Für einen L3-Cluster:
2 >
3 >-  Der Knotengruppenparameter muss auf den Namen der erstellten
    Knotengruppe festgelegt werden.
4 >-  Der Backplane-Parameter ist für Knoten obligatorisch, die
    einer Knotengruppe zugeordnet sind, die mehr als einen Knoten
    hat, damit die Knoten innerhalb des Netzwerks miteinander
    kommunizieren können.</span>
5
```



```
6 Beispiel:
7
8 Hinzufügen eines Knotens für einen L2-Cluster (alle Clusterknoten
     befinden sich im selben Netzwerk).
```

add cluster node 0 10.102.29.60 -state PASSIVE -backplane 0/1/1

```
1   Hinzufügen eines Knotens für einen L3-Cluster, der einen
       einzelnen Knoten aus jedem Netzwerk enthält. Hier müssen Sie
       die Rückwandplatine nicht einstellen.
```

add cluster node 0 10.102.29.60 -state PASSIVE -nodegroup ng1

```
1   Hinzufügen eines Knotens für einen L3-Cluster, der mehrere
       Knoten aus jedem Netzwerk enthält. Hier müssen Sie die
       Backplane so einstellen, dass Knoten innerhalb eines
       Netzwerks miteinander kommunizieren können.
```

add cluster node 0 10.102.29.60 -state PASSIVE -backplane 0/1/1 -nodegroup ng1
‘‘‘

5. Fügen Sie die Cluster-IP-Adresse (z. B. 10.102.29.61) auf diesem Knoten hinzu.

```
1 add ns ip <IPAddress> <netmask> -type clip
2 <!--NeedCopy-->
```

Beispiel

```
1 > add ns ip 10.102.29.61 255.255.255.255 -type clip
2 <!--NeedCopy-->
```

6. Aktivieren Sie die Clusterinstanz.

   ```
   enable cluster instance <clId><!--NeedCopy-->
   ```

7. Speichern Sie die Konfiguration.

   ```
   save ns config<!--NeedCopy-->
   ```

8. Warmstarten Sie die Appliance.

   ```
   reboot -warm<!--NeedCopy-->
   ```


Überprüfen Sie die Clusterkonfigurationen mithilfe des Befehls clusterinstanz anzeigen. Stellen Sie sicher, dass die Ausgabe des Befehls die NSIP-Adresse der Appliance als Knoten des Clusters anzeigt.

9. Nachdem der Knoten UP ist, melden Sie sich beim CLIP an und ändern Sie die RPC-Anmeldeinformationen für die Cluster-IP-Adresse und die Node-IP-Adresse. Weitere Informationen zum Ändern eines RPC-Knotenkennworts finden Sie unter Ändern eines RPC-Knotenkennworts.

So erstellen Sie einen Cluster mit der GUI

1. Melden Sie sich bei einer Appliance an (z. B. einer Appliance mit der NSIP-Adresse 10.102.29.60), die Sie dem Cluster hinzufügen möchten.
2. Navigieren Sie zu **System > Cluster.**
3. Klicken Sie im Detailbereich auf den Link **Cluster verwalten** .
4. Legen Sie im Dialogfeld Clusterkonfiguration die Parameter fest, die zum Erstellen eines Clusters erforderlich sind. Um eine Beschreibung eines Parameters zu erhalten, bewegen Sie den Mauszeiger über das entsprechende Textfeld.
5. Klicken Sie auf **Erstellen**.
6. Aktivieren Sie im Dialogfeld Clusterinstanz konfigurieren das Kontrollkästchen Clusterinstanz aktivieren.
7. Wählen Sie im Bereich Clusterknoten den Knoten aus, und klicken Sie auf **Öffnen.**
8. Legen Sie im Dialogfeld Clusterknoten konfigurieren den Status fest.
9. Klicken Sie auf **OK**, und klicken Sie dann auf **Speichern.**
10. Warmstarten Sie die Appliance.
11. Nachdem der Knoten UP ist, melden Sie sich beim CLIP an und ändern Sie die RPC-Anmeldeinformationen für die Cluster-IP-Adresse und die Node-IP-Adresse. Weitere Informationen zum Ändern eines RPC-Knotenkennworts finden Sie unter Ändern eines RPC-Knotenkennworts.

Unterstützung des strikten Modus für den Synchronisierungsstatus des Clusters

Sie können jetzt einen Clusterknoten so konfigurieren, dass Fehler beim Anwenden der Konfiguration angezeigt werden. Ein neuer Parameter, “SyncStatusStrictMode”, wird sowohl im Befehl “add” als auch “set cluster instance” eingeführt, um den Status jedes Knotens in einem Cluster zu verfolgen. Standardmäßig ist der Parameter “SyncStatusStrictMode” deaktiviert.

So aktivieren Sie den strikten Modus über die Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set cluster instance <clID> [-syncStatusStrictMode (ENABLED | DISABLED)]
```

Beispiel:

```
set cluster instance 1 -syncStatusStrictMode ENABLED
```

So zeigen Sie den Status des strikten Modus über die Befehlszeile an

```
1      >show cluster instance
2      1) Cluster ID: 1
3          Dead Interval: 3 secs
4          Hello Interval: 200 msecs
5          Preemption: DISABLED
6          Propagation: ENABLED
7          Quorum Type: MAJORITY
8          INC State: DISABLED
9          Process Local: DISABLED
10         Retain Connections: NO
11         Heterogeneous: NO
12         Backplane based view: DISABLED
13         Cluster sync strict mode: ENABLED
14         Cluster Status: ENABLED(admin), ENABLED(operational), UP
15
16       WARNING(s):
17         (1) - There are no spotted SNIPs configured on the cluster.
               Spotted SNIPs can help improve cluster performance
18
19         Member Nodes:
20         Node ID     Node IP      Health     Admin State  Operational
               State
21         -------     -------      ------     -----------
               ------------------
22     1)      1           192.0.2.20      UP         ACTIVE       ACTIVE(
           Configuration Coordinator)
23     2)      2           192.0.2.21      UP         ACTIVE       ACTIVE
24     3)      3           192.0.2.19*     UP         ACTIVE       ACTIVE
25 <!--NeedCopy-->
```

So zeigen Sie den Grund für den Synchronisierungsfehler eines Clusterknotens mit der GUI an

1. Navigieren Sie zu **System > Cluster > Clusterknoten**.
2. Scrollen Sie auf der Seite “ **Clusterknoten** nach rechts, um die Details des Synchronisationsfehlers für die Cluster-Knoten anzuzeigen.

Hinzufügen eines Knotens zum Cluster

October 5, 2021

Sie können die Größe eines Clusters nahtlos auf maximal 32 Knoten skalieren. Wenn dem Cluster eine Citrix ADC Appliance hinzugefügt wird, werden die Konfigurationen dieser Appliance gelöscht (indem intern der Befehl clear ns config -extended ausgeführt wird). Die SNIP-Adressen, **MTU-Einstellungen** der Backplane-Schnittstelle und alle VLAN-Konfigurationen (mit Ausnahme des Standard-VLAN und des NSVLAN) werden ebenfalls von der Appliance gelöscht.

Die Clusterkonfigurationen werden dann auf diesem Knoten synchronisiert. Während der Synchronisierung kann es zu einem zeitweilig abfallenden Datenverkehr kommen.

> **Wichtig**
>
> Bevor Sie eine Citrix ADC Appliance zu einem Cluster hinzufügen:
>
> - Richten Sie die Backplane-Schnittstelle für den Knoten ein. Überprüfen Sie das vorangegangene Thema.
> - Überprüfen Sie, ob die auf der Appliance verfügbaren Lizenzen übereinstimmen, die im Konfigurationskoordinator verfügbar sind. Die Appliance wird nur hinzugefügt, wenn die Lizenzen übereinstimmen.
> - Wenn das NSVLAN im Cluster vorhanden sein soll, stellen Sie sicher, dass das NSVLAN auf der Appliance erstellt wird, bevor es dem Cluster hinzugefügt wird.
> - Citrix empfiehlt, den Knoten als passiven Knoten hinzuzufügen. Nachdem Sie den Knoten mit dem Cluster verbunden haben, schließen Sie die knotenspezifische Konfiguration von der Cluster-IP-Adresse ab. Führen Sie den Befehl force cluster sync aus, wenn der Cluster nur IP-Adressen entdeckt hat. Und das hat L3 VLAN-Bindung oder hat statische Routen.
> - Wenn einem Cluster eine Appliance mit einem vorkonfigurierten Link Aggregate (LA) -Kanal hinzugefügt wird, ist der LA-Kanal weiterhin in der Clusterumgebung vorhanden. Der LA-Kanal wird von LA/x in NodeId/LA/x umbenannt, wobei LA/x die LA-Kanal-ID ist.

So fügen Sie dem Cluster über die Befehlszeilenschnittstelle einen Knoten hinzu

> **Hinweis:**
>
> Wenn Sie einem Cluster-Setup einen Knoten hinzufügen und der Knoten über eine statische Standardroute verfügt, wird er dem Cluster-Koordinator-Knoten (CCO) hinzugefügt. Wenn diese standardmäßige statische Route auf ein falsches Gateway verweist, kann dies zu Ausfallzeiten der Dienste führen. Überprüfen Sie daher die standardmäßige statische Route des neuen Knotens, bevor Sie ihn zum Cluster-Setup hinzufügen.

1. Melden Sie sich an der Cluster-IP-Adresse an, an der Eingabeaufforderung, wie folgt vor:

- Fügen Sie die Appliance (z. B. 10.102.29.70) zum Cluster hinzu.

> **Hinweis:**
>
> Für einen L3-Cluster:
>
> ```
> - Der Knotengruppenparameter muss auf eine Knotengruppe
>   festgelegt werden, die über Knoten desselben Netzwerks verf
>   ügt.
> ```
>
> - Wenn dieser Knoten zum selben Netzwerk gehört wie der erste hinzugefügte Knoten, konfigurieren Sie die Knotengruppe, die für diesen Knoten verwendet wurde.
> - Wenn dieser Knoten zu einem anderen Netzwerk gehört, erstellen Sie eine Knotengruppe und binden Sie diesen Knoten an die Knotengruppe.
> - Der Backplane-Parameter ist für Knoten obligatorisch, die einer Knotengruppe zugeordnet sind, die mehr als einen Knoten hat, damit die Knoten innerhalb des Netzwerks miteinander kommunizieren können.

```
add cluster node <nodeId> <IPAddress> -state <state> -backplane <
   interface_name> -nodegroup <name>

Example:

add cluster node 1 10.102.29.70 -state PASSIVE -backplane 1/1/1
<!--NeedCopy-->
```

- Speichern Sie die Konfiguration.

```
save ns config
<!--NeedCopy-->
```

2. Melden Sie sich am neu hinzugefügten Knoten an (z. B. 10.102.29.70) und verbinden Sie den Knoten mit dem Cluster.

```
join cluster -clip <ip_addr> -password <password>

Example:

join cluster -clip 10.102.29.61 -password nsroot
```



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

3. Konfigurieren Sie die folgenden Befehle auf dem CLIP.

   - Binden Sie VLAN an eine Schnittstelle

   ```
   1 bind vlan <id> -ifnum <interface_name>
   2 <!--NeedCopy-->
   ```

   Beispiel:

   ```
   1 bind vlan 1 -ifnum 2/1/2
   2 <!--NeedCopy-->
   ```

   - Fügen Sie dem neu hinzugefügten Knoten eine gespottete IP-Adresse hinzu

   ```
   1 add ns ip <IpAddress> <netmask> -ownerNode <positive_interger
       >
   2 <!--NeedCopy-->
   ```

   Beispiel:

   ```
   1 add ns ip 97.131.0.3 255.0.0.0 -ownerNode 2
   2 <!--NeedCopy-->
   ```

   - VLAN auf NSIP überprüfen

   ```
   1 show vlan <id>
   2 <!--NeedCopy-->
   ```

   Beispiel:

   ```
   1 show vlan 1
   2 <!--NeedCopy-->
   ```

4. Führen Sie die folgenden Konfigurationen durch:

- Wenn der Knoten einem Cluster hinzugefügt wird, der nur Spotted IPs hat, werden die Konfigurationen synchronisiert, bevor die gespotted IP-Adressen diesem Knoten zugewiesen werden. In solchen Fällen können L3-VLAN-Bindungen verloren gehen. Um diesen Verlust zu vermeiden, fügen Sie entweder eine gestreifte IP hinzu oder fügen Sie die L3-VLAN-Bindungen hinzu.
- Definieren Sie die erforderlichen Spotted Konfigurationen.
- Stellen Sie die MTU für die Backplane-Schnittstelle ein.

5. Speichern Sie die Konfiguration.

```
save ns config
<!--NeedCopy-->
```

6. Warmstarten Sie die Appliance.

```
reboot -warm
<!--NeedCopy-->
```

7. Nachdem der Knoten UP ist und die Synchronisierung erfolgreich ist, ändern Sie die RPC-Anmeldeinformationen für den Knoten von der Cluster-IP-Adresse. Weitere Informationen zum Ändern eines RPC-Knotenkennworts finden Sie unter Ändern eines RPC-Knotenkennworts.

```
set rpcNode <node-NSIP> -password <passwd>

Example:

set rpcNode 192.0.2.4 -password mypassword
<!--NeedCopy-->
```

8. Setzen Sie den Clusterknoten auf Aktiv.

```
set cluster node <nodeID> -state active.

Example:

set cluster node 1 -state active
<!--NeedCopy-->
```


So fügen Sie dem Cluster über die GUI einen Knoten hinzu

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster > Knoten**.
3. Klicken Sie im Detailbereich auf **Hinzufügen**, um den neuen Knoten hinzuzufügen (z. B. 10.102.29.70).
4. Konfigurieren **Sie im Dialogfeld Clusterknoten erstellen** den neuen Knoten. Um eine Beschreibung eines Parameters zu erhalten, bewegen Sie den Mauszeiger über das entsprechende Textfeld.
5. Klicken Sie auf **Erstellen**. Wenn Sie aufgefordert werden, einen warmen Neustart durchzuführen, klicken Sie auf **Ja.**
6. Nachdem der Knoten UP ist und die Synchronisierung erfolgreich ist, ändern Sie die RPC-Anmeldeinformationen für den Knoten von der Cluster-IP-Adresse. Weitere Informationen zum Ändern eines RPC-Knotenkennworts finden Sie unter Ändern eines RPC-Knotenkennworts.
7. Navigieren Sie zu **System > Cluster > Knoten > Bearbeiten**.
8. Ändern Sie den Status in **ACTIVE** und bestätigen Sie.

So verbinden Sie einen zuvor hinzugefügten Knoten mit dem Cluster über die GUI

Wenn Sie die CLI verwendet haben, um dem Cluster einen Knoten hinzuzufügen, aber den Knoten nicht mit dem Cluster verbunden haben, können Sie das folgende Verfahren verwenden.

> **Hinweis:**
>
> Wenn ein Knoten dem Cluster beitritt, übernimmt er den Anteil des Datenverkehrs vom Cluster und daher kann eine vorhandene Verbindung beendet werden.

1. Melden Sie sich bei dem Knoten an, dem Sie dem Cluster beitreten möchten (z. B. 10.102.29.70).
2. Navigieren Sie zu **System > Cluster.**
3. Klicken Sie im Detailbereich unter Erste Schritte auf den Link Cluster beitreten.
4. Legen Sie im Dialogfeld Mit vorhandenem Cluster verbinden die Cluster-IP-Adresse und das `nsroot` Kennwort des Konfigurationskoordinators fest. Um eine Beschreibung eines Parameters zu erhalten, bewegen Sie den Mauszeiger über das entsprechende Textfeld.
5. Klicken Sie auf **OK.**

Anzeigen der Details eines Clusters

October 5, 2021

Sie können die Details der Clusterinstanz und der Clusterknoten anzeigen, indem Sie sich bei der Cluster-IP-Adresse anmelden.

So zeigen Sie Details einer Clusterinstanz mit der CLI an

Melden Sie sich bei der Cluster-IP-Adresse an und geben Sie an der Eingabeaufforderung Folgendes ein:

```
show cluster instance <clId>
```

> **Hinweis:**
>
> Wenn der vorhergehende Befehl von der NSIP-Adresse des Nicht-CCO-Knotens aus ausgeführt wird, zeigt der Befehl den Status des Clusters auf diesem Knoten an.

So zeigen Sie Details zu einem Clusterknoten mit der CLI an

Melden Sie sich bei der Cluster-IP-Adresse an und geben Sie an der Eingabeaufforderung Folgendes ein:

```
show cluster node <nodeId>
```

So zeigen Sie Details einer Clusterinstanz über die GUI an

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster.**
3. Klicken Sie im Detailbereich unter **Erste Schritte**auf den Link **Cluster verwalten**, um die Details des Clusters anzuzeigen.

So zeigen Sie Details zu einem Clusterknoten mit der GUI an

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster > Knoten.**
3. Klicken Sie im Detailbereich auf den Knoten, für den Sie die Details anzeigen möchten.

Verteilung des Datenverkehrs über Clusterknoten

October 5, 2021

Nachdem Sie den Citrix ADC Cluster erstellt und die erforderlichen Konfigurationen durchgeführt haben, müssen Sie ECMP (Equal Cost Multiple Path) oder Cluster Link Aggregation (LA) auf der Client-Datenebene (für Clientdatenverkehr) oder Serverdatenebene (für Serverdatenverkehr) bereitstellen. Diese Mechanismen verteilen externen Datenverkehr über die Clusterknoten.

Policy-basierte Steuerung der Rückwandplatine

Die Policy-basierte Backplane-Lenkung (PBS) ist ein Mechanismus in der Clusterbereitstellung, der den Datenverkehr über Clusterknoten basierend auf der für den Flow definierten Hash-Methode steuert. Der Flow wird durch eine Kombination von L2- und L3-Parametern definiert, ähnlich der Access Control List (ACL).

Der PBS unterstützt sowohl IPv4- als auch IPv6-Datenverkehr. Bei IPv6-Bereitstellungen unterstützt das Steering eine zusätzliche Option `[dfdprefix <positive_integer>]`. Es bietet die Flexibilität, denselben Flow-Prozessor für das gleiche IP-Präfix zu wählen. Die Präfixoption wird nur für Quell-IP- oder Ziel-IP-Hash-Methoden unterstützt.

> **Hinweis:**
>
> Wenn der PBS-Mechanismus nicht zur Lenkung des Datenverkehrs verwendet wird, wird der Datenverkehr über die Standardmethode gesteuert.

Um die neuen ACL-Attribute zu konfigurieren, geben Sie bei der CLI die folgenden Befehle ein:

CLI-Befehle für IPv4

- `add ns acl <aclname> <aclaction> [-type (classic | dfd)] [-dfdhash <dfdhash>]`
- `set ns acl <aclname> <aclaction> [-dfdhash <dfdhash>`
- `show ns acl [<aclname>][-type (classic | DFD)]`
- `apply ns acls [-type (classic | DFD)]`
- `clear ns acls [-type (classic | DFD)]`
- `renumber ns acls [-type (classic | DFD)]`

CLI-Befehle für IPv6

- `add ns acl6 <acl6name> <acl6action> [-type (classic | dfd)][-dfdhash <dfdhash>][-dfdprefix <positive_interger>]`
- `set ns acl6 <acl6name> <acl6action> [-dfdhash <dfdhash>][-dfdprefix <positive_interger>]`
- `show ns acl6 [<acl6name>][-type (classic | DFD)]`
- `apply ns acls6 [-type (classic | DFD)]`

- `clear ns acls6 [-type (classic | DFD)]`
- `renumber ns acls6 [-type (classic | DFD)]`

Im Folgenden finden Sie die verschiedenen Arten von Hash-Methoden, die Sie angeben können, um das Paket an den Flow-Prozessor zu steuern:

- SIP-SPORT-DIP-DPORT
- SIP
- DIP
- SIP-DIP
- SIP-SPORT

Einschränkungen

1. Die Verteilung des Datenverkehrsflusses über die Clusterknoten ist nicht gewährleistet, da der Flow-Prozessor durch die vom Administrator konfigurierten Regeln entschieden wird.
2. Der L2-Modus wird nicht unterstützt.
3. Die Knotengruppen und Stripeset-SNIPs werden nicht unterstützt, da es keine Bereitstellungsszenarien gibt.
4. MPTCP wird nicht unterstützt.
5. Unterstützung nur für TCP-, UDP- und ICMP-Datenverkehr.
6. Der Cluster-über-L3-Modus wird nicht unterstützt.
7. Prozess lokal auf Service-Level wird nicht unterstützt.

Verwenden des Multiple-Pfads mit gleichem Kostenfaktor (ECMP)

October 5, 2021

Mithilfe des ECMP-Mechanismus (Equal Cost Multiple Path) für eine Clusterbereitstellung geben aktive Clusterknoten die IP-Adressen des virtuellen Servers an. Der Clusterknoten, der den angekündigten Datenverkehr empfängt, steuert den Datenverkehr zu dem Knoten, der den Datenverkehr verarbeiten muss. Es kann redundante Steuerungen in gepunkteten und teilweise gestreiften virtuellen Servern geben. Aus diesem Grund werden ab NetScaler 11 die IP-Adressen von gespotteten und teilweise gestreiften virtuellen Servern für die Besitzerknoten angekündigt, wodurch die redundante Steuerung reduziert wird.

Sie benötigen detaillierte Kenntnisse der Routingprotokolle, um ECMP verwenden zu können. Weitere Informationen finden Sie unter Konfigurieren dynamischer Routen. Weitere Informationen zum Routing in einem Cluster finden Sie unter Routing in einem Cluster.

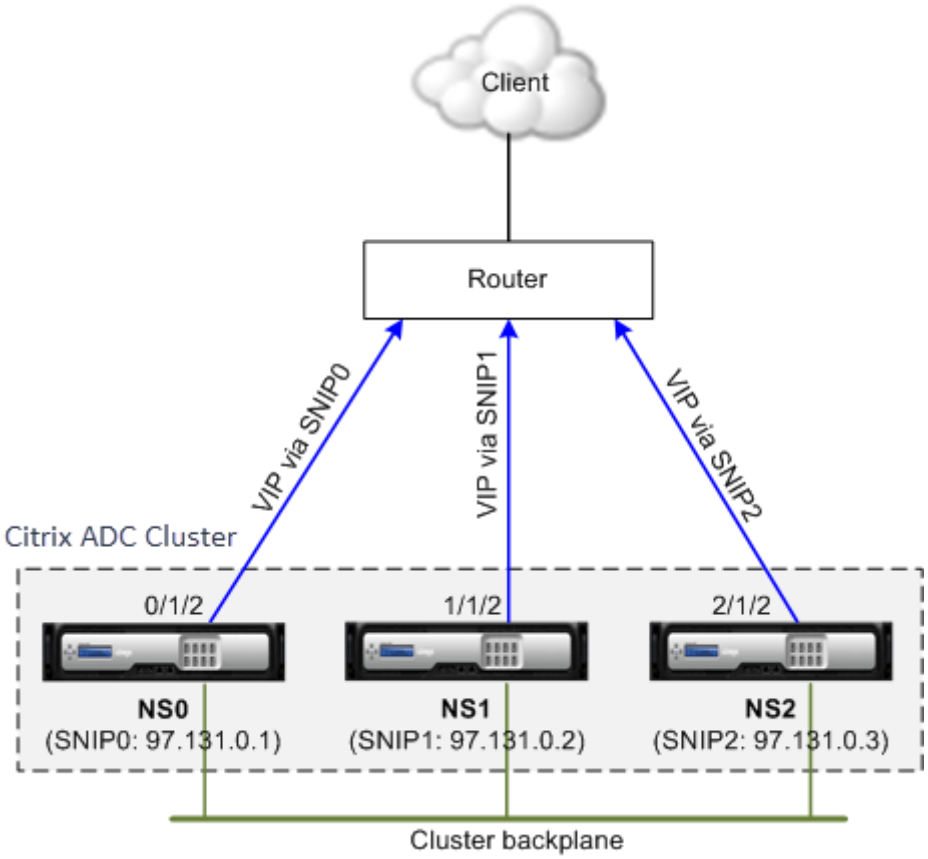
Um ECMP zu verwenden, müssen Sie zuerst Folgendes ausführen:

- Aktivieren Sie das erforderliche Routingprotokoll (OSPF, RIP, BGP oder ISIS) für die Cluster-IP-Adresse.
- Binden Sie die Schnittstellen und die gespotted IP-Adresse (mit aktiviertem dynamischem Routing) an ein VLAN.
- Konfigurieren Sie das ausgewählte Routingprotokoll und verteilen Sie die Kernel-Routen auf den ZeBOS mithilfe der VTYSH-Shell neu.

Führen Sie ähnliche Konfigurationen auf der Cluster-IP-Adresse und auf dem externen Verbindungsgerät durch.

> **Hinweis:**
>
> - Stellen Sie sicher, dass die Lizenzen auf dem Cluster dynamisches Routing unterstützen, andernfalls funktioniert ECMP nicht.
> - ECMP wird für virtuelle Platzhalterserver nicht unterstützt, da RHI eine VIP-Adresse benötigt, um Werbung für einen Router und virtuelle Platzhalterserver zu schalten. Da sie keine zugeordneten VIP-Adressen haben.

Abbildung 1. ECMP-Topologie



Wenn Sie den ECMP-Mechanismus für die Verkehrsverteilung in einer Clusterbereitstellung verwenden, kündigen die aktiven Cluster-Knoten die IP-Adressen des virtuellen Servers an den Upstream-

Router an. Der ECMP-Router kann die VIP-Adresse über SNIP0, SNIP1 oder SNIP2 erreichen. Der Verkehrsfluss in Abbildung 1 wird wie folgt beschrieben:

1. Der Kunde sendet eine Anfrage an den im Cluster gehosteten VIP.
2. Der Upstream-Router, basierend auf den erlernten Routen der VIP, leitet das Paket an einen der Knoten weiter. Sagen wir NS1. Der Knoten NS1 ist der Flow Receiver.
3. Der Flow Receiver (NS1) bestimmt den Knoten, der den Datenverkehr verarbeiten muss, der als Flow Processor bezeichnet wird. Beispiel: Knoten NS2 ist der Flussprozessor.
4. Der Durchflussempfänger (NS1) mit SNIP1 (97.131.0.2) steuert die Anforderung mit SNIP2 (97.131.0.3) an den Flussprozessor (NS2).
5. Der Flow Processor (NS2) stellt eine Verbindung mit dem Server her.
6. Der Server verarbeitet die Anforderung und sendet die Antwort an die SNIP-Adresse, die die Anforderung an den Server gesendet hat.

Hinweise:

- Nur ACTIVE Knoten kündigen VIP-Routen an.
- INACTIVE Knoten kündigen keine VIP-Routen an.
- Alle ACTIVE Knoten kündigen gestreifte VIPs an.
- Nur ACTIVE Besitzerknoten kündigen Spotted- oder Teil-Striped-VIPs an.

So konfigurieren Sie ECMP auf dem Cluster mit der Befehlszeilenschnittstelle

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Aktivieren Sie das Routingprotokoll.

```
enable ns feature <feature>
```

Beispiel: Um das OSPF-Routingprotokoll zu aktivieren.

```
enable ns feature ospf
```

3. Fügen Sie ein VLANhinzu.

```
add vlan <id>
```

Beispiel


```
1 add vlan 97
```

4. Binden Sie die Schnittstellen der Clusterknoten an das VLAN.

```
1 bind vlan <id> -ifnum <interface_name>
```

Beispiel

```
1 bind vlan 97 -ifnum 0/1/2 1/1/2 2/1/2
```

5. Fügen Sie für jeden Knoten eine gespotted SNIP-Adresse hinzu, und aktivieren Sie dynamisches Routing.

```
1 add ns ip <SNIP> <netmask> -ownerNode <positive_integer> -
     dynamicRouting ENABLED
```

Beispiel

```
1 add ns ip 97.131.0.1 255.0.0.0 -ownerNode 0 -dynamicRouting
     ENABLED -type SNIP
2 add ns ip 97.131.0.2 255.0.0.0 -ownerNode 1 -dynamicRouting
     ENABLED -type SNIP
3 add ns ip 97.131.0.3 255.0.0.0 -ownerNode 2 -dynamicRouting
     ENABLED -type SNIP
```

6. Binden Sie eine der Spotted-SNIP-Adressen an das VLAN. Wenn Sie eine Spotted-SNIP-Adresse an ein VLAN binden, werden alle anderen SNIP-Adressen, die auf dem Cluster in diesem Subnetz definiert sind, automatisch an das VLAN gebunden.

```
1 bind vlan <id> -IPAddress <SNIP> <netmask>
```

Beispiel

```
1 bind vlan 97 -ipAddress 97.131.0.1 255.0.0.0
```


> **Hinweis:**
>
> Sie können NSIP-Adressen der Clusterknoten verwenden, anstatt SNIP-Adressen hinzuzufügen. Wenn ja, müssen Sie die Schritte 3 - 6 nicht ausführen.

7. Konfigurieren Sie das Routingprotokoll auf ZeBOS mit der VTYSH-Shell.

   Beispiel:

   So konfigurieren Sie ein OSPF-Routingprotokoll für die Knoten-IDs 0, 1 und 2.

```
vtysh
! interface vlan97 !
 router ospf   owner-node 0
ospf router-id 97.131.0.1   exit-owner-node
owner-node 1    ospf router-id 97.131.0.2
exit-owner-node
owner-node 2
ospf router-id 97.131.0.3   exit-owner-node   redistribute kernel
   network 97.0.0.0/8 area 0  !
```

> **Hinweis:**
>
> Für VIP-Adressen, die angekündigt werden sollen, wird die RHI-Einstellung mithilfe des Parameters vserverRHILevel wie folgt durchgeführt:

```
add ns ip <IPAddress> <netmask> -type VIP -vserverRHILevel <
   vserverRHILevel>
```

   Für OSPF-spezifische RHI-Einstellungen gibt es weitere Einstellungen, die wie folgt durchgeführt werden können:

```
add ns ip <IPAddress> <netmask> -type VIP -ospfLSAType ( TYPE1 |
   TYPE5 ) -ospfArea <positive_integer>
```

   Verwenden Sie den Befehl add ns ip6, um die vorherigen Befehle für IPv6-Adressen auszuführen.

8. Konfigurieren Sie ECMP auf dem externen Switch. Die folgenden Beispielkonfigurationen werden für den Cisco® Nexus 7000 C7010 Release 5.2 (1) Switch bereitgestellt. Ähnliche Konfigurationen müssen auf anderen Switches durchgeführt werden.


```
//For OSPF (IPv4 addresses) Global config: Configure terminal
    feature ospf    Interface config:  Configure terminal
    interface Vlan10      no shutdown      ip address 97.131.0.5/8
       Configure terminal  router ospf 1  network 97.0.0.0/8 area
    0.0.0.0  ---------------------------------

//For OSPFv3 (IPv6 addresses) Global config:  Configure terminal
    feature ospfv3    Configure terminal  interface Vlan10      no
    shutdown      ipv6 address use-link-local-only      ipv6 router
     ospfv3 1 area 0.0.0.0    Configure terminal  router ospfv3 1
```

Router-Monitoring-Clusterknoten in der ECMP-Bereitstellung

In einem Cluster-Setup können Sie auf einem Besitzerknoten mit einer SNIP-Adresskonfiguration nun die Option OwnerDownResponse deaktivieren. Standardmäßig ist die Option aktiviert, sodass der Knoten auf eine ICMP/ARP/ICMP6/ND6-Anforderung vom Upstream-Router reagieren kann. Sie können diese Option jetzt deaktivieren, damit der Router überwachen kann, ob ein Clusterknoten aktiv oder inaktiv ist. Wenn der Router eine Anforderung sendet und die Option deaktiviert ist, identifiziert er den Besitzerknoten als inaktiv und nicht für die Verkehrsverteilung verfügbar.

So konfigurieren Sie ECMP für die Verteilung statischer Routen mit der Befehlszeilenschnittstelle

```
add ns ip <ipddress> <netmask> -ownernode <node-id>  - ownerDownResponse
    disable
```

Anwendungsfall: ECMP mit BGP-Routing

October 5, 2021

So konfigurieren Sie ECMP mit BGP-Routingprotokoll:

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Aktivieren Sie das BGP-Routingprotokoll.

```
> enable ns feature bgp
```


3. Fügen Sie VLAN hinzu und binden Sie die erforderlichen Schnittstellen.

```
1 > add vlan 985
2 > bind vlan 985 -ifnum 0/0/1 1/0/1
```

4. Fügen Sie die gespotted IP-Adresse hinzu und binden Sie sie an das VLAN.

```
1 > add ns ip 10.100.26.14 255.255.255.0 -ownerNode 1 -
     dynamicRouting ENABLED
2 > add ns ip 10.100.26.15 255.255.255.0 -ownerNode 2 -
     dynamicRouting ENABLED
3 > bind vlan 985 -ipAddress 10.100.26.10 255.255.255.0
```

5. Konfigurieren Sie das BGP-Routing-Protokoll auf ZeBOS mit der VTYSH-Shell.

```
1 > vtysh conf t router bgp 65535 neighbor 10.100.26.1 remote-as
     65535
```

6. Konfigurieren Sie BGP am externen Switch. Die folgenden Beispielkonfigurationen werden für den Cisco® Nexus 7000 C7010 Release 5.2 (1) Switch bereitgestellt. Ähnliche Konfigurationen müssen auf anderen Switches durchgeführt werden.

```
1 > router bgp 65535 no synchronization
2   bgp log-neighbor-changes neighbor 10.100.26.14 remote-as 65535
       neighbor 10.100.26.15 remote-as 65535 no auto-summary
3   dont-capability-negotiate
4   dont-capability-negotiate
5   no dynamic-capability
```

Konfiguration des Clusters ECMP mit Cisco Nexus 7000 Switch mit Routing-Protokoll

October 5, 2021

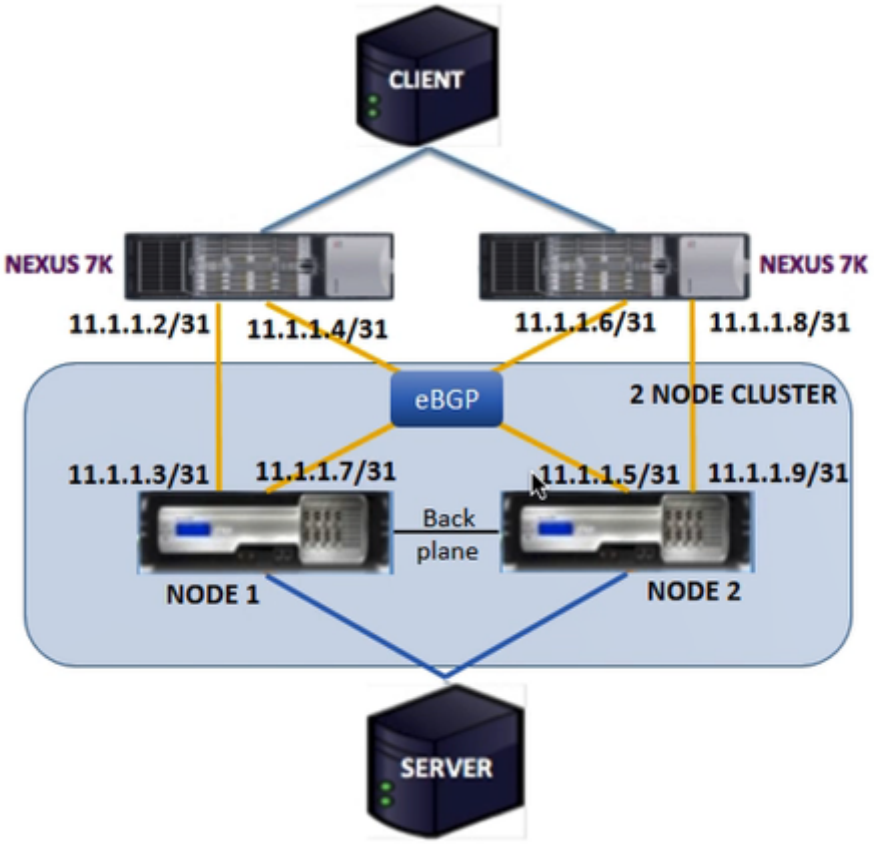
Mit ECMP über ein Cluster-Setup kann eine Citrix ADC Appliance den Datenverkehr über ein Routing-protokoll verarbeiten. Der ECMP-Mechanismus hilft bei der Werbung für die IP-Adressen des virtuellen Servers über alle aktiven Clusterknoten.

Um ECMP verwenden zu können, müssen Sie zuerst das BGP-Protokoll auf der Cluster-IP-Adresse aktivieren. Binden Sie die Schnittstellen und die gespotted IP-Adresse (mit aktiviertem dynamischem Routing) an ein VLAN. Konfigurieren Sie das ausgewählte Routingprotokoll und verteilen Sie die Kernel-Routen auf den ZeBOS mithilfe der VTYSH-Shell neu.

Anwendungsfall: Cluster ECMP mit Cisco Nexus 7000 Switch mit Routing-Protokoll

Betrachten Sie ein Beispiel für eine Clusterbereitstellung mit einem Cisco Nexus 7000 Switch:

- Zwei Citrix ADC Appliances (Knoten 1 und Knoten 2), die mit dem Nexus-Switch verbunden sind (Upstream).
- Zwei Cisco Nexus 7000 Switch.
- Client und Server (Zeichnen des HTTP-Datenverkehrs über den Nexus-Switch). Mit aktiviertem Hot Standby Router Protocol (HSRP) auf der Client-Seite.



Voraussetzungen

Berücksichtigen Sie die folgenden Punkte, bevor Sie Clusterknoten auf einer Citrix ADC Appliance konfigurieren.

1. Alle Appliances müssen vom gleichen Plattformtyp sein.

2. Border Gateway Protocol (BGP) muss auf den Clusterknoten aktiviert sein.

Konfigurieren mit der CLI auf einer Citrix ADC Appliance

1. Melden Sie sich an einer Appliance an (z. B. Appliance mit NSIP-Adresse 1.1.1.1)
2. So fügen Sie einen Clusterknoten hinzu.

```
add cluster node 0 1.1.1.2 -state ACTIVE -backplane 0/10/8
```

3. So fügen Sie die Cluster-IP-Adresse hinzu

```
add ns ip 1.1.1.10 255.255.255.254 -type clip
```

4. Speichern der Konfiguration

```
save ns config
```

5. Warmer Neustart der Appliance

```
reboot -warm
```

6. So fügen Sie Knoten 1 mit CLIP hinzu

```
add cluster node 1 2.2.2.2 -state ACTIVE -backplane 1/10/8
```

7. So verbinden Sie einen Knoten mit dem Cluster

```
join cluster -clip 1.1.1.10 -password nsroot
```

8. Führen Sie die folgende Konfiguration auf CLIP durch
   - `enable ns feature bgp ospf DYNAMICROUTING`
   - `add ns ip 11.1.1.3 255.255.255.254 -dynamicRouting ENABLED -ownerNode 0`

- `add ns ip 11.1.1.7 255.255.255.254 -dynamicRouting ENABLED -ownerNode 0`
- `add ns ip 11.1.1.5 255.255.255.254 -dynamicRouting ENABLED -ownerNode 1`
- `add ns ip 11.1.1.9 255.255.255.254 -dynamicRouting ENABLED -ownerNode 1`

Auf dem Cisco Nexus Router (11.1.1.2/31 und 11.1.1.4/31) müssen Sie die folgenden Konfigurationen über die Befehlszeile ausführen:

- `feature ospf`
- `feature bgp`
- `feature interface-vlan`
- `feature hsrp`

```
>  interface vlan100
    no shutdown
    ip address 50.1.1.1/8
     hsrp 50
      ip 50.50.50.50

>  interface Ethernet 4/15
     ip address 11.1.1.2/31
     no shutdown

>  interface Ethernet 4/19
     ip address 11.1.1.4/31
     no shutdown

>  interface Ethernet 4/22
     switchport
      switchport access vlan 100
```

Auf dem Cisco Nexus Router (11.1.1.6/31 und 11.1.1.8/31) müssen Sie die folgenden Konfigurationen über die Befehlszeile ausführen:

- `feature ospf`
- `feature bgp`
- `feature interface-vlan`
- `feature hsrp`


```
> interface vlan100
 no shutdown
 no ip redirects
 ip address 50.1.1.2/8
  hsrp 50
  ip 50.50.50.50

> interface Ethernet 4/13
 ip address 11.1.1.6/31
 no shutdown

> interface Ethernet 4/15
 ip address 11.1.1.8/31
 no shutdown

> interface Ethernet 4/22
 switchport
 switchport access vlan 100
```

Für das BGP-Protokoll müssen Sie die folgenden Konfigurationen auf CLIP der Citrix ADC Appliance durchführen:

```
> vtysh
ns# router bgp 1
 redistribute kernel
 owner-node 0
 neighbor 11.1.1.2 remote-as 2
 neighbor 11.1.1.2 as-origination-interval 1
 neighbor 11.1.1.2 advertisement-interval 0
 neighbor 11.1.1.6 remote-as 2
 neighbor 11.1.1.6 as-origination-interval 1
 neighbor 11.1.1.6 advertisement-interval 0
owner-node 1
 neighbor 11.1.1.4 remote-as 2
 neighbor 11.1.1.4 as-origination-interval 1
 neighbor 11.1.1.4 advertisement-interval 0
 neighbor 11.1.1.8 remote-as 2
 neighbor 11.1.1.8 as-origination-interval 1
 neighbor 11.1.1.8 advertisement-interval 0
exit-owner-node
```

Durchführen der folgenden Konfigurationen auf dem Cisco Nexus-Router (11.1.1.3 und 11.1.1.5)


```
> ip access-list acl1
  10 permit ip 50.0.0.0/8 any
  route-map test permit
  match ip address acl1
 router bgp 2
  address-family ipv4 unicast
   redistribute direct route-map test
   maximum-paths 2
 neighbor 11.1.1.3 remote-as 1
  address-family ipv4 unicast
  neighbor 11.1.1.5 remote-as 1
 address-family ipv4 unicast
```

Durchführen der folgenden Konfigurationen auf dem Cisco Nexus-Router (11.1.1.7 und 11.1.1.9)

```
> ip access-list acl1
   10 permit ip 50.0.0.0/8 any
  route-map test permit 1
   match ip address acl1
  router bgp 2
   address-family ipv4 unicast
   redistribute direct route-map test
   maximum-paths 2
  neighbor 11.1.1.7 remote-as 1
   address-family ipv4 unicast
  neighbor 11.1.1.9 remote-as 1
   address-family ipv4 unicast
```

Für das OSPF-Protokoll müssen Sie die folgenden Konfigurationen auf CLIP der Citrix ADC Appliance durchführen:

```
> vtysh
ns# router osfp 1
redistribute kernel
owner-node 0
 network 15.1.1.2/31 area 0
 network 15.1.1.6/31 area 0
exit-owner-node

owner-node 1
```



```
 network 15.1.1.4/31 area 0
 network 15.1.1.8/31 area 0
exit-owner-node

route-map map2 permit 1
set metric 10
```

Auf dem Cisco Nexus Router (11.1.1.2/31 und 11.1.1.4/31) müssen Sie die folgenden Konfigurationen über die Befehlszeile ausführen:

```
> route-map- map2 permit 1
   set metric 10

   interface Ethernet4/15
     ip address 15.1.1.2/31
     ip router ospf 1 area 0.0.0.0
     no shutdown

   interface Ethernet4/19
     ip address 15.1.1.4/31
     ip router ospf 1 area 0.0.0.0
     no shutdown

   router ospf 1
    router-id 1.1.1.1
    redistribute direct route-map map2
```

Auf dem Cisco Nexus Router (11.1.1.7/31 und 11.1.1.9/31) müssen Sie die folgenden Konfigurationen über die Befehlszeile ausführen:

```
> route-map- map2 permit 1
    set metric 10

   interface Ethernet4/13
     ip address 15.1.1.6/31
     ip router ospf 1 area 0.0.0.0
     no shutdown

    interface Ethernet4/15
     ip address 15.1.1.8/31
     ip router ospf 1 area 0.0.0.0
     no shutdown
```



```
13
14      router ospf 1
15        router-id 1.1.1.2
16        redistribute direct route-map map2
```

Cluster-Link-Aggregation verwenden

October 5, 2021

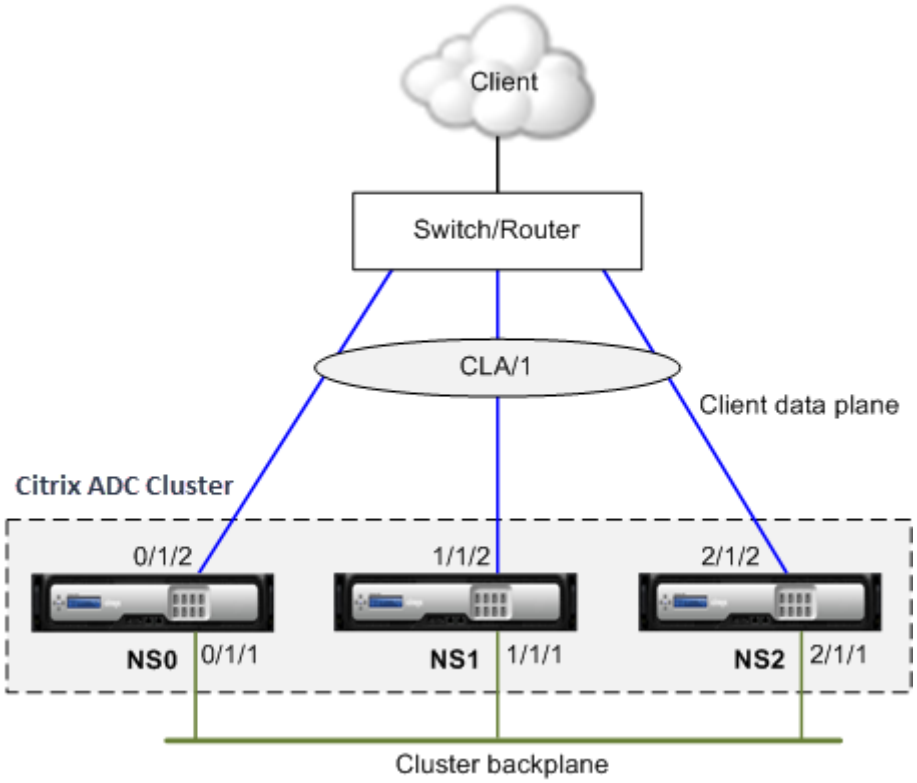
Die Cluster-Link-Aggregation ist eine Gruppe von Schnittstellen von Clusterknoten. Es handelt sich um eine Erweiterung der Citrix ADC-Link-Aggregation. Der einzige Unterschied besteht darin, dass die Schnittstellen in der Cluster-Link-Aggregation zwar von demselben Gerät stammen müssen, die Schnittstellen zwar von verschiedenen Knoten des Clusters stammen. Weitere Informationen zur Link-Aggregation finden Sie unter Konfigurieren der Link-Aggregation.

> **Wichtig**
>
> - Cluster Link-Aggregation wird für einen Cluster von Hardware (MPX) Appliances unterstützt.
> - Cluster-Link-Aggregation wird für einen Cluster virtueller (VPX) Appliances unterstützt, die auf ESX- und KVM-Hypervisoren bereitgestellt werden, mit folgenden Einschränkungen:
> - Dedizierte Schnittstellen müssen verwendet werden. Dies bedeutet, dass die Schnittstellen nicht mit anderen virtuellen Maschinen geteilt werden dürfen.
> - Wenn ein Knoten INAKTIV wird, wird die entsprechende Cluster-LA-Schnittstelle als Power DOWN markiert, sodass der Datenverkehr nicht an einen INACTIVE Node gesendet wird.
> - Wenn ein Knoten zu ACTIVE wird, wird die entsprechende Cluster-LA-Schnittstelle als Power ON markiert.
> - Wenn die Mitgliedsschnittstellen der Cluster-Link-Aggregation manuell deaktiviert sind oder wenn die Cluster-Link-Aggregation selbst manuell deaktiviert ist, wird die Funktion zum Ausschalten der Schnittstelle nur durch den LACP-Timeout-Mechanismus erreicht.
> - Jumbo MTU wird bei der LACP-Cluster-Link-Aggregation nicht unterstützt.
>
> **Hinweis:** Cluster-Link-Aggregation wird auf VPX-Appliances, die auf XenServer, AWS und Hyper-V bereitgestellt werden, nicht unterstützt.
>
> - Ab Version 12. 0 wird die Cluster-Link-Aggregation auf Citrix ADC SDX-Appliances unterstützt.
> - Die Anzahl der Schnittstellen, die an Cluster LA gebunden werden können, beträgt 16 (von jedem Knoten). Die maximale Anzahl von Schnittstellen in Cluster LA kann (16 * n) sein,

> wobei n die Anzahl der Knoten in einem Cluster ist. Die Gesamtzahl der Schnittstellen in Cluster LA hängt von der Anzahl der Schnittstellen für jeden Portkanal auf dem Upstream-Switch ab.
> - Wenn eine Citrix ADC Appliance Intel Fortville-Schnittstellen verwendet, kann die Umstellung eines Clusterknotens in den passiven Modus einige Sekunden mit CLAG zu einem Ausfall führen. Das Problem tritt auf, weil LACP aktiviert ist, damit CLAG ordnungsgemäß funktioniert, und die Ausfallzeit hängt von NIC LACP Timer.

Betrachten Sie beispielsweise einen Cluster mit drei Knoten, in dem alle drei Knoten mit dem Upstream-Switch verbunden sind. Ein Cluster LA-Kanal (CLA/1) wird durch Bindungsschnittstellen 0/1/2, 1/1/2 und 2/1/2 gebildet.

Abbildung 1. Cluster-Link-Aggregationstopologie

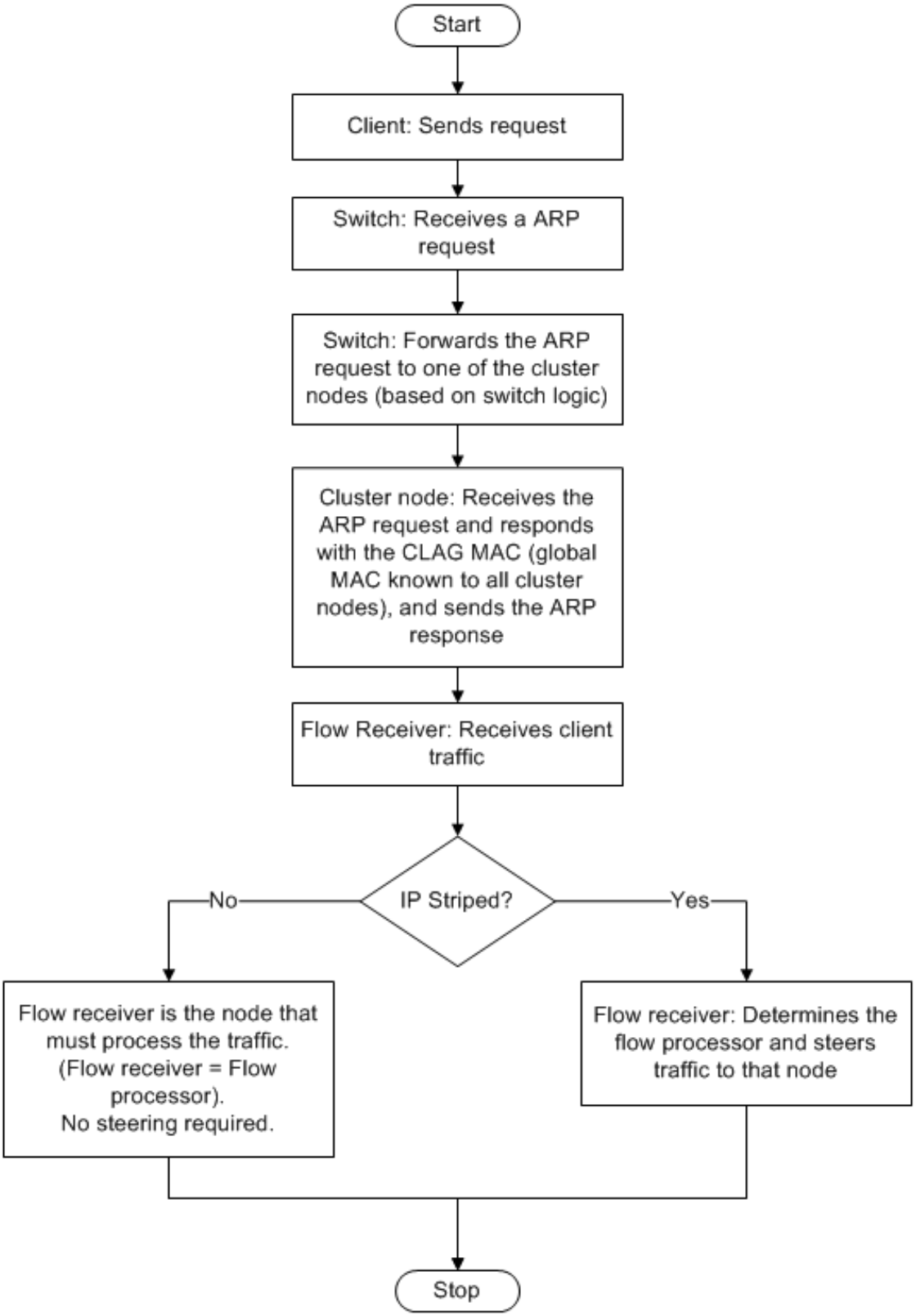


Ein Cluster-LA-Kanal weist die folgenden Attribute auf:

- Jeder Kanal verfügt über einen eindeutigen MAC, der von Clusterknoten vereinbart wurde.
- Der Kanal kann sowohl lokale als auch entfernte Knoten Schnittstellen binden.
- In einem Cluster werden maximal vier Cluster-LA-Kanäle unterstützt.
- Backplane-Schnittstellen können nicht Teil eines Cluster-LA-Kanals sein.
- Wenn eine Schnittstelle an einen Cluster-LA-Kanal gebunden ist, haben die Kanalparameter Vorrang vor den Netzwerkschnittstellenparametern. Eine Netzwerkschnittstelle kann nur an einen Kanal gebunden werden.

- Der Verwaltungszugriff auf einen Clusterknoten darf nicht auf einem Cluster-LA-Kanal (z. B. CLA/1) oder seinen Mitgliedsschnittstellen konfiguriert werden. Dies liegt daran, dass, wenn der Knoten INACTIVE ist, die entsprechende Cluster-LA-Schnittstelle als Herunterfahren gekennzeichnet ist und daher den Verwaltungszugriff verliert.

Abbildung 2. Verkehrsverteilungsfluss mit Cluster-LA



Unterstützung für Backup und Wiederherstellung von Cluster LA auf Citrix ADC MPX

Sie können das Cluster-Setup von LA auf Citrix ADC MPX sichern und wiederherstellen. Die Cluster-LA-MAC-Adresse ist unabhängig von der physischen Schnittstellen-MAC-Adresse der Cluster-Knoten und kann sich nach dem Sicherungs- und Wiederherstellungsprozess ändern. Der Cluster LA kann den Datenverkehr bedienen, nachdem ein Cluster-Wiederherstellungsprozess abgeschlossen ist. Weitere Informationen zum Backup und Wiederherstellen finden Sie unter Sichern und Wiederherstellen des Cluster-Setups

Statische Cluster-Link-Aggregation

October 5, 2021

Sie müssen einen statischen Cluster-LA-Kanal auf der Cluster-IP-Adresse und auf dem externen Verbindungsgerät konfigurieren. Konfigurieren Sie nach Möglichkeit den Upstream-Switch so, dass der Datenverkehr auf der Grundlage der IP-Adresse oder des Ports statt der MAC-Adresse verteilt wird.

So konfigurieren Sie einen statischen Cluster-LA-Kanal mit der CLI

1. Melden Sie sich bei der Cluster-IP-Adresse an.

   > **Hinweis:**
   >
   > Stellen Sie sicher, dass Sie den Cluster-LA Kanal für die Cluster-IP-Adresse konfigurieren, bevor Sie die Linkaggregation auf dem externen Switch konfigurieren. Andernfalls leitet der Switch den Datenverkehr zum Cluster weiter, obwohl der Cluster-LA-Kanal nicht konfiguriert ist. Dies kann zu Verkehrsverlust führen.

2. Erstellen Sie einen Cluster-LA-Kanal.

```
add channel <id> -speed <speed>
```

Beispiel

```
add channel CLA/1 -speed 1000
```

> **Hinweis:**
>
> Sie dürfen die Geschwindigkeit nicht als AUTO angeben. Vielmehr müssen Sie die Geschwindigkeit explizit als 10, 100, 1000 oder 10000 angeben. Nur Schnittstellen mit

> der Geschwindigkeit, die mit dem <speed> Attribut im Cluster-LA-Kanal übereinstimmt, werden der aktiven Verteilerliste hinzugefügt.

3. Binden Sie die erforderlichen Schnittstellen an den Cluster-LA-Kanal. Stellen Sie sicher, dass die Schnittstellen nicht für die Clusterrückwandplatine verwendet werden.

```
bind channel <id> <ifnum>
```

Beispiel

```
bind channel CLA/1 0/1/2 1/1/2 2/1/2
```

4. Überprüfen Sie die Konfigurationen.

```
show channel <id>
```

Beispiel

```
show channel CLA/1
```

> **Hinweis:**
>
> Sie können den Cluster-LA-Kanal mit dem `bind vlan` Befehl an ein VLAN binden. Die Schnittstellen des Kanals werden automatisch an das VLAN gebunden.

5. Konfigurieren Sie statische LA am externen Switch. Die folgenden Beispielkonfigurationen werden für das Cisco® Nexus 7000 C7010 Release 5.2 (1) bereitgestellt. Ähnliche Konfigurationen müssen auf anderen Switches durchgeführt werden.

```
Global config:
Configure terminal

Interface level config:

interface Ethernet2/47
switchport
switchport access vlan 10
channel-group 7 mode on
```



```
no shutdown

interface Ethernet2/48
switchport
switchport access vlan 10
channel-group 7 mode on
no shutdown
```

Dynamische Cluster-Link-Aggregation

October 5, 2021

Der dynamische Cluster-LA-Kanal verwendet das Link Aggregation Control Protocol (LACP).

Sie müssen ähnliche Konfigurationen für die Cluster-IP-Adresse und auf dem externen Verbindungsgerät durchführen. Konfigurieren Sie nach Möglichkeit den Upstream-Switch so, dass der Datenverkehr auf der Grundlage der IP-Adresse oder des Ports statt der MAC-Adresse verteilt wird.

> **Wichtige Punkte**
>
> - Aktivieren Sie LACP (indem Sie den LACP-Modus entweder als ACTIVE oder PASSIVE angeben).

```
>**Note**
>
> Make sure the LACP mode is not set as PASSIVE on both the Citrix ADC
    cluster and the external connecting device.
```

> - Geben Sie auf jeder Schnittstelle denselben LACP-Schlüssel an, der Teil des Kanals sein soll. Zum Erstellen eines Cluster-LA-Kanals kann der LACP-Schlüssel einen Wert von 5 bis 8 haben. Wenn Sie beispielsweise die LACP-Taste auf den Schnittstellen 0/1/2, 1/1/2 und 2/1/2 bis 5 festlegen, wird CLA/1 erstellt. Die Schnittstellen 0/1/2, 1/1/2 und 2/1/2 werden automatisch an CLA/1 gebunden. Wenn Sie den LACP-Schlüssel auf 6 setzen, wird der CLA/2-Kanal erstellt.
> - Geben Sie den LAG-Typ als Cluster an.

So konfigurieren Sie einen dynamischen Cluster-LA-Kanal mit der CLI

Geben Sie auf der Cluster-IP-Adresse für jede Schnittstelle, die Sie dem LA-Kanal des Clusters hinzufügen möchten, Folgendes ein:


```
set interface <id> -lacpMode <lacpMode> -lacpKey <positive_integer> -
lagType CLUSTER<!--NeedCopy-->
```

Beispiel:

Konfigurieren eines Cluster-LA-Kanals CLA/1 mit 3 Schnittstellen.

```
> set interface 0/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 1/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
> set interface 2/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
```

> **Hinweis:**
>
> Optional können Sie Link-Redundanz in einem Cluster mit LACPaktivieren.

Konfigurieren Sie dynamisches LA auf dem externen Switch. Die folgenden Beispielkonfigurationen werden für das Cisco® Nexus 7000 C7010 Release 5.2 (1) bereitgestellt. Ähnliche Konfigurationen müssen auf anderen Switches durchgeführt werden.

```
Global config:
Configure terminal
feature lacp
Interface level config:

interface Ethernet2/47
switchport
switchport access vlan 10
channel-group 7 mode active
no shutdown

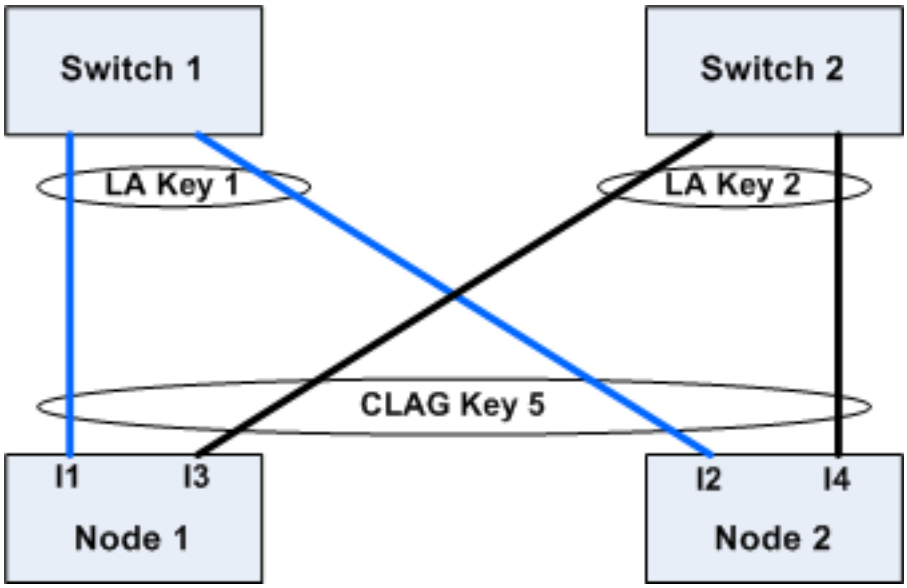
interface Ethernet2/48
switchport
switchport access vlan 10
channel-group 7 mode active
no shutdown
```

Verknüpfen von Redundanz in einem Cluster mit LACP

October 5, 2021

Ein Citrix ADC Cluster bietet Link-Redundanz für LACP, um sicherzustellen, dass alle Knoten über denselben Partnerschlüssel verfügen.

Um die Notwendigkeit für Link-Redundanz zu verstehen, lassen Sie uns das Beispiel der folgenden Cluster-Setup zusammen mit den begleitenden Fällen betrachten (mit Aufmerksamkeit auf Fall 3):



In diesem Setup sind die Schnittstellen I1, I2, I3 und I4 mit KEY 5 an den LACP-Kanal gebunden. Auf der Partnerseite sind I1 und I2 mit Switch 1 verbunden, um einen einzelnen LA-Kanal mit KEY 1 zu bilden. Ebenso sind I3 und I4 mit Switch 2 verbunden, um einen einzelnen LA-Kanal mit KEY 2 zu bilden.

Betrachten wir nun die folgenden Fälle, um die Notwendigkeit für Link-Redundanz zu verstehen:

- **Fall 1: Schalter 1 ist hochgefahren und Schalter 2 ist ausgefallen**

  In diesem Fall würde Cluster LA auf beiden Knoten aufhören, LACPDUs von Key2 zu empfangen und LACPDUs von Key1 zu empfangen. Auf beiden Knoten ist der Cluster LA mit KEY 1 und I1 verbunden und I2 ist UP und der Kanal auf beiden Knoten wäre UP.

- **Fall 2: Switch1 geht aus und Switch2 wird UP**

  In diesem Fall würde Cluster LA auf beiden Knoten aufhören, LACPDUs von Key1 zu empfangen und LACPDUs von Key2 zu empfangen. Auf beiden Knoten ist der Cluster LA mit Key2 und I3 verbunden und I4 ist UP und der Kanal auf beiden Knoten wäre UP.

- **Fall 3: Sowohl Switch1 als auch Switch2 sind UP**

  In diesem Fall ist es möglich, dass Cluster LA auf Knoten1 Key1 als Partner wählt und Cluster LA auf Knoten2 Key2 als Partner wählt. Dies bedeutet, dass I1 auf Knoten1 und I4 auf node2 Datenverkehr empfängt, was unerwünscht ist. Dies kann passieren, weil die LACP-Zustandsmaschine auf Knotenebene ist und ihre Partner auf Erstbedienste-Basis auswählt.

  Um diese Probleme zu lösen, wird Link-Redundanz von dynamischen Cluster-LA unterstützt.

Um die Link-Redundanz auf einem Kanal oder einer Schnittstelle zu konfigurieren, müssen Sie diese aktivieren und optional den Schwellendurchsatz wie folgt angeben:

```
set channel CLA/1 -linkRedundancy ON -lrMinThroughput <positive_integer
>
```

Der Durchsatz der Partnerkanäle wird anhand des konfigurierten Schwellenwert-Durchsatzes überprüft. Der Partnerkanal, der den Schwellenwertdurchsatz erfüllt, wird auf First-In-First-Out-Weise (FIFO) ausgewählt. Wenn keiner der Partnerkanäle den Schwellenwert erreicht oder der Schwellenwert nicht konfiguriert ist, wird der Partnerkanal mit der maximalen Anzahl von Links ausgewählt.

> **Hinweis:**
>
> Der Schwellendurchsatz kann ab NetScaler 11 konfiguriert werden.

Verwenden des USIP-Modus im Cluster

October 5, 2021

Im Modus “Quell-IP” (USIP) leitet der Cluster oder die Citrix ADC Appliance jedes Paket mit der Client-IP-Adresse an den entsprechenden Back-End-Server weiter.

Verkehrsverteilung im USIP-Modus

Das Verhalten im USIP-Modus unterscheidet die Verteilung des Datenverkehrs über die Client-datenebene und die Serverdatenebene in der ECMP- und CLAG-Bereitstellung. Der folgende Abschnitt enthält weitere Informationen zum Verhalten im USIP-Modus. Weitere Informationen zu CLAG im USIP-Modus finden Sie unter Verwenden der Cluster-Link-Aggregation.

USIP-Modus

Der Cluster verwendet die Client-IP, um die serverseitige Verbindung zu öffnen. Der Quellport wird möglicherweise basierend auf der `useproxyport` Einstellung beibehalten oder auch nicht.

USIP `useproxyport`-Szenarien

Der USIP `useproxyport` ist für den Verkehrsfluss EIN, der Quellport wird so ausgewählt, dass der umgekehrte Datenverkehr zum Flow-Prozessor hasht. Es gewährleistet eine einzelne Lenkung auf der Serverseite.

Der USIP `useproxyport` ist für den Verkehrsfluss AUS, der Quellport bleibt erhalten und daher gibt es eine doppelte Lenkung auf der Serverseite.

> **Wichtig**
>
> - Wenn USIP eingeschaltet ist, wird die Client-IP in der Back-End-Serververbindung verwendet, und die Verteilung des Datenverkehrs für die Reaktion ist über Clusterknoten hinweg erforderlich. Sie können die ECMP- oder CLAG-Bereitstellung für die Datenverkehrsverteilung serverseitig verwenden. In Ermangelung einer Datenverkehrsverteilung auf der Serverseite könnte der gesamte Rücklaufverkehr auf einem einzigen Clusterknoten landen, was zu Staus führt.
> - Der `set rsskeytype -rsskey symmetric` Befehl wird verwendet, um die doppelte Lenkung auf eine einzelne Steuerung des Verkehrs in den `useproxyport` Off-Bereitstellungen zu reduzieren. Wo das 4-Tupel für die Verbindung für die Server- und Clientseite gleich bleibt. Zum Beispiel virtueller Server im Platzhaltermodus im MAC-Modus.

Einschränkungen

Die USIP funktioniert nicht, wenn der lokale Prozess deaktiviert ist.

Bereitstellung im USIP-Modus

Die folgende Abbildung zeigt eine Bereitstellung im USIP-Modus in einem Cluster-Setup.

Konfigurieren Sie Folgendes mit CLI

1. Aktivieren Sie das Routingprotokoll.

```
enable ns feature <feature>
```

Beispiel:

```
enable ns feature ospf
```

2. Fügen Sie für jeden Knoten eine gespotted SNIP-Adresse hinzu, und aktivieren Sie dynamisches Routing.


```
add ns ip <SNIP> <netmask> -dynamicRouting ( ENABLED | DISABLED )
    - ownerNode <positive_interger>  - ownerdownResponse ( YES | NO
    )
```

Beispiel

```
- add ns ip 192.0.2.1 255.255.255.0 -dynamicRouting ENABLED -
  ownerNode 0 - ownerDownResponse NO
- add ns ip 192.0.2.2 255.255.255.0 -dynamicRouting ENABLED -
  ownerNode 1 - ownerDownResponse NO
- add ns ip 192.0.2.3 255.255.255.0 -dynamicRouting ENABLED -
  ownerNode 2 - ownerDownResponse NO
```

3. Fügen Sie ein VLANhinzu.

```
add vlan <id>
```

Beispiel

```
add vlan 300
```

4. Binden Sie die Schnittstellen der Clusterknoten an das VLAN.

```
bind vlan <id> -ifnum <interface_name>
```

Beispiel

```
bind vlan 300 -ifnum 0/1/2 1/1/2 2/1/2
```

5. Binden Sie eine der Spotted-SNIP-Adressen an das VLAN. Wenn Sie eine Spotted-SNIP-Adresse an ein VLAN binden, werden alle anderen SNIP-Adressen, die auf dem Cluster in diesem Subnetz definiert sind, automatisch an das VLAN gebunden.

```
bind vlan <id> -IPAddress <ip_addr | ipv6_addr> -netmask
```


Beispiel

```
bind vlan 300  - IPAddress 192.0.2.1 255.255.255.0
```

6. Konfigurieren Sie das Routingprotokoll auf ZeBOS mit der VTYSH-Shell. Konfigurieren Sie das OSPF-Routingprotokoll für Knoten-IDs 0, 1 und 2.

```
vtysh
configure terminal
ns block-sec-rtadv
router ospf
owner -node 0
router-id 192.0.2.1
exit-owner-node
owner-node 1
router-id 192.0.2.2
exit-owner-node
owner-node 2
router-id 192.0.2.3
exit-owner-node
network 192.0.2.0/24 area 0

default-information originate always
```

7. Führen Sie die folgenden Konfigurationen auf dem Router Cisco 3750 über die Befehlszeilenschnittstelle durch.

```
Configure terminal
feature ospf
interface vlan300
no shutdown
ip address 192.0.2.100/24
Configure terminal
router ospf 1
router-id 192.0.2.100
network 192.0.2.0 0.0.0.255 area 0
```

Hinweise

- Die Datenverkehrsverteilung auf Client und Server muss nicht identisch sein. Beispiel-

> sweise können Sie ECMP auf der Clientseite und CLAG serverseitig oder umgekehrt konfigurieren.
>
> - Planen Sie für zusätzliche Kapazität der Backplane, da es im USIP-Einsatz mehr Lenkungsaufwand gibt.
> - Die Konfiguration im Zusammenhang mit CLAG und Static Route (MSR) überwachen muss auf Serverseite gleich bleiben.
> - Die Verkehrssteuerung befindet sich eher in den Bereitstellungen im USIP-Modus.

Verwalten des Citrix ADC Clusters

October 5, 2021

Nachdem Sie einen Cluster erstellt und den erforderlichen Verkehrsverteilungsmechanismus konfiguriert haben, kann der Cluster Datenverkehr bereitstellen. Während der Lebensdauer des Clusters können Sie die folgenden Clusteraufgaben ausführen:

- Konfigurieren von Knotengruppen
- Deaktivieren von Knoten eines Clusters
- Erkennen von Citrix ADC-Appliances
- Anzeigen von Statistiken
- Synchronisieren von Cluster-Konfigurationen und Cluster-Dateien
- Synchronisieren der Zeit über die Knoten
- Upgrade oder Herabstufung der Software von Cluster-Knoten

Konfigurieren von Linksets

October 5, 2021

Linkset ist eine Gruppe von Schnittstellen von Clusterknoten, die zur selben Broadcast-Domäne gehören. In Linksets enthält jeder Knoten die Informationen darüber, welche Schnittstellen anderer Knoten mit derselben Broadcast-Domäne verbunden sind.

> **Hinweis:**
>
> Linksets sind eine obligatorische Konfiguration in den folgenden Szenarien:
>
> - Für Bereitstellungen, die eine MAC-basierte Weiterleitung (MBF) erfordern.
> - Für den Modus “-m MAC”, der auf dem virtuellen Server zusammen mit dem globalen MBF-Modus aktiviert ist.

> - Verbesserung der Verwaltbarkeit von ACL- und L2-Richtlinien mit Schnittstellen. Sie definieren einen Linksatz der Schnittstellen und fügen ACL- und L2-Richtlinien basierend auf Linksets hinzu.

In einem Cluster-Setup verwenden die folgenden Funktionen MBF intern.

- Weiterleitungssitzung
- L2Conn
- MAC-Modus virtueller Server
- Transparenter Monitor
- LLB

Linksets müssen nur über die Cluster-IP-Adresse konfiguriert werden.

Betrachten Sie ein Beispiel mit einem Drei-Knoten-Cluster. In der folgenden Abbildung befinden sich die Schnittstellen 0/1/2, 1/1/2 und 2/1/2 in derselben Broadcast-Domäne und können daher als Linkset (LS/1) konfiguriert werden.

Abbildung 1. Linksetstopologie

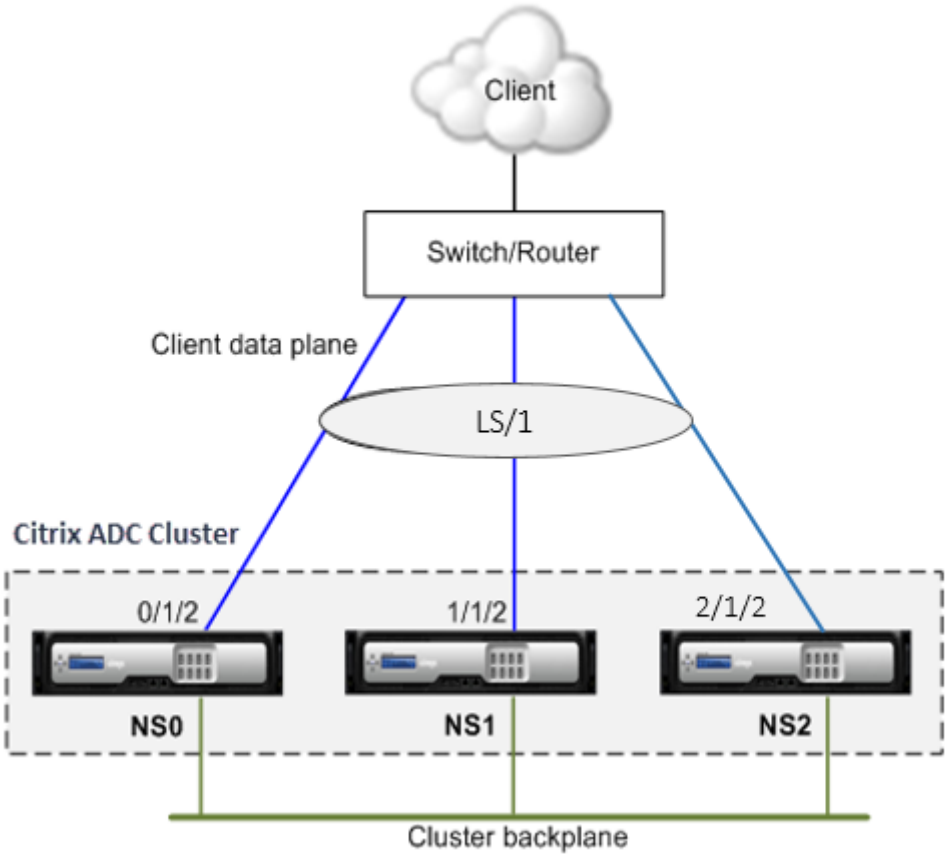
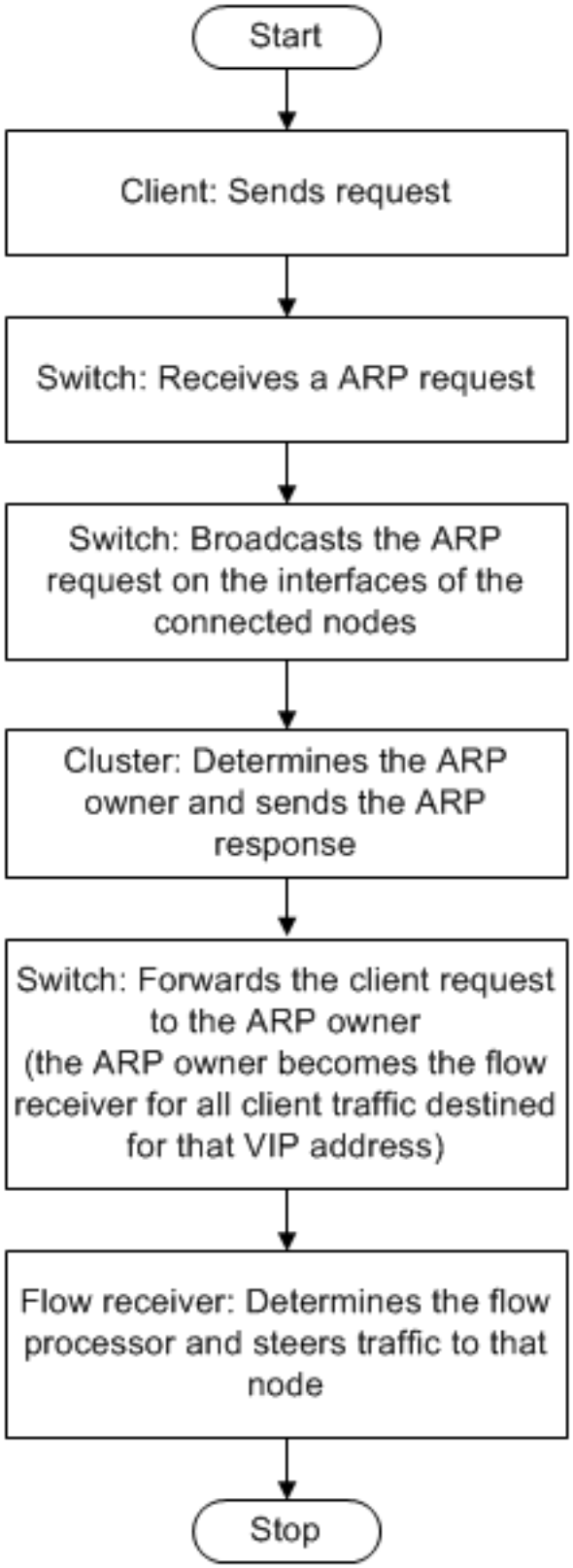


Abbildung 2. Verkehrsverteilungsfluss mit Linksets



So konfigurieren Sie ein Linkset mit der CLI

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Erstellen Sie einen Linksatz.

   “‘add linkset

```
**Beispiel**

```add linkset LS/1<!--NeedCopy-->
```

3. Binden Sie die erforderlichen Schnittstellen an das Linkset. Stellen Sie sicher, dass die Schnittstellen nicht für die Cluster-Rückwandplatine verwendet werden.

   “‘bind linkset -ifnum ...

```
**Beispiel**

```bind linkset LS/1 -ifnum 0/1/2 1/1/2 2/1/2<!--NeedCopy-->
```

4. Überprüfen Sie die Linkset-Konfigurationen.

   “‘show linkset

```
**Beispiel**

```show linkset LS/1<!--NeedCopy-->
```

> **Hinweis:**
>
> Sie können das Linkset mit dem `bind vlan` Befehl an ein VLAN binden. Die Schnittstellen des Linksets werden automatisch an das VLAN gebunden.

So konfigurieren Sie ein Linkset mit der GUI

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Netzwerk > Linksets**.
3. Klicken Sie im Detailbereich auf **Hinzufügen**.
4. Im Dialogfeld **Linkset erstellen**:
   - Geben Sie den Namen des Linksets an, indem Sie den Linkset-Parameter festlegen.


```

- Geben Sie die Schnittstellen an, die dem Linkset hinzugefügt werden sollen, und klicken Sie auf Hinzufügen. Wiederholen Sie diesen Schritt für jede Schnittstelle, die Sie dem Linkset hinzufügen möchten.

5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

## Knotengruppen für gepunktete und teilweise gestreifte Konfigurationen

October 5, 2021

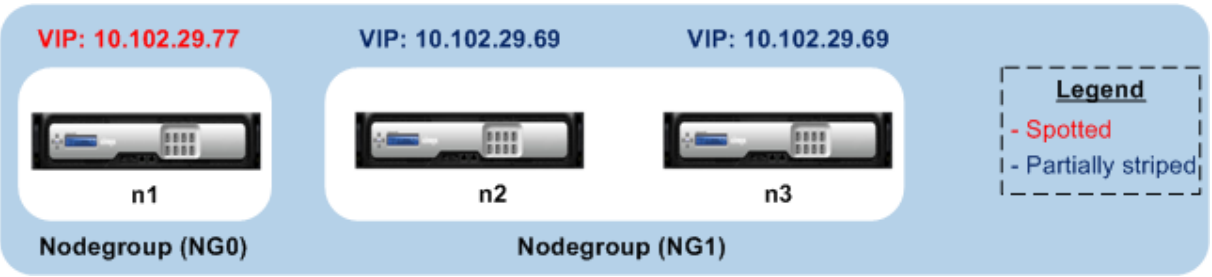
Aufgrund des standardmäßigen Cluster-Verhaltens sind alle Konfigurationen, die für die Cluster-IP-Adresse ausgeführt werden, auf allen Knoten des Clusters verfügbar. Es kann jedoch vorkommen, dass einige Konfigurationen nur auf bestimmten Clusterknoten verfügbar sind.

Sie können diese Anforderung erreichen, indem Sie eine Knotengruppe definieren, die die spezifischen Clusterknoten enthält, und dann die Konfiguration an diese Knotengruppe binden. Es stellt sicher, dass die Konfiguration nur auf diesen Cluster-Knoten aktiv ist. Diese Konfigurationen werden als teilweise gestreift oder gepunktet bezeichnet (wenn nur ein einzelner Knoten aktiv ist). Weitere Informationen finden Sie unter Gestreifte, teilweise gestreifte und gepunktete Konfigurationen.

Betrachten Sie beispielsweise einen Cluster mit drei Knoten. Sie erstellen eine Knotengruppe NG0, die den Knoten n1 und eine andere Knotengruppe NG1 enthält, die n2 und n3 enthält. Binden Sie virtuelle Server mit Lastenausgleich von 0,77 an NG0 und den virtuellen Lastausgleichsserver 0,69 an NG1.

Dies bedeutet, dass der virtuelle Server 0.77 nur auf n1 aktiv ist und daher nur n1 den Datenverkehr empfängt, der auf 0,77 gerichtet ist. In ähnlicher Weise ist der virtuelle Server 0.69 nur auf den Knoten n2 und n3 aktiv und daher empfängt nur n2 und n3 Datenverkehr, der auf 0,69 gerichtet ist.

Abbildung 1. Citrix ADC Cluster mit Knotengruppen, die für gepunktete und partial gestreifte Konfigurationen konfiguriert sind




Die Entitäten oder Konfigurationen, die Sie an eine Knotengruppe binden können, sind:

- Lastenausgleich, Content Switching, Cache-Umleitung, Authentifizierung, Autorisierung und Überwachung virtueller Server

> **Hinweis:**
>
> Virtuelle FTP-Lastausgleichsserver können nicht an Knotengruppen gebunden werden.

- Virtueller VPN-Server (unterstützt ab NetScaler 10.5 Build 50.10)
- Global Server Load Balancing (GSLB) -Sites und andere GSLB-Entitäten (unterstützt ab NetScaler 10.5 Build 52.11)
- Bezeichner und Stream-Bezeichner beschränken

## Verhalten von Knotengruppen

October 5, 2021

Aufgrund der Interoperabilität von Knotengruppen mit verschiedenen Citrix ADC Funktionen und -Entitäten sind einige Verhaltensaspekte zu beachten. Knoten in einer Knotengruppe können ebenfalls gesichert werden. Lesen Sie weiter für weitere Informationen.

### Allgemeines Verhalten einer Clusterknotengruppe

- Eine Knotengruppe, an die Entitäten gebunden sind, kann nicht entfernt werden.
- Ein Clusterknoten, der zu einer Knotengruppe gehört, an die Entitäten gebunden sind, kann nicht entfernt werden.
- Eine Clusterinstanz, die Knotengruppen mit an sie gebundenen Entitäten hat, kann nicht entfernt werden.
- Sie können keine Entität hinzufügen, die von einer anderen Entität abhängig ist. Es darf kein Teil der Knotengruppe sein. Wenn Sie dies tun müssen, entfernen Sie zuerst die Abhängigkeit. Fügen Sie dann beide Entitäten der Knotengruppe hinzu und ordnen Sie die Entitäten erneut zu.

  **Beispiele:**

  - Angenommen Sie haben einen virtuellen Server, VS1, dessen Sicherung virtuellen Server VS2 ist. Um VS1 zu einer Knotengruppe hinzuzufügen, stellen Sie zunächst sicher, dass VS2 als Backup-Server von VS1 entfernt wird. Binden Sie dann jeden Server einzeln an die Knotengruppe und konfigurieren Sie dann VS2 als Backup für VS1.
  - Angenommen, Sie haben einen virtuellen Content Switching-Server, CSVS1, dessen Ziel-Lastausgleichsserver ist LBVS1. Um CSVS1 zu einer Knotengruppe hinzuzufügen, entfernen Sie zuerst LBVS1 als Ziel. Binden Sie dann jeden Server einzeln an die Knotengruppe und konfigurieren Sie dann LBVS1 als Ziel.

  - Angenommen Sie haben einen virtuellen Lastausgleichsserver, LBVS1, der eine Richtlinie aufweist, die einen anderen virtuellen Lastausgleichsserver, LBVS2, aufruft. Um einen der virtuellen Server hinzuzufügen, entfernen Sie zuerst die Zuordnung. Binden Sie dann jeden Server einzeln an die Knotengruppe und verknüpfen Sie dann die virtuellen Server erneut.

- Sie können eine Entität nicht an eine Knotengruppe binden. Es hat keine Knoten und die strikte Option ist aktiviert. Daher können Sie den letzten Knoten einer Knotengruppe nicht aufheben, an die Entitäten gebunden sind und für die die strikte Option aktiviert ist.
- Die strikte Option kann nicht für eine Knotengruppe geändert werden, die keine Knoten hat, aber Entitäten an sie gebunden ist.

### Sichern von Nodes in einer Knotengruppe

Standardmäßig ist eine Knotengruppe so konzipiert, dass sie Backup-Knoten für Mitglieder einer Knotengruppe bereitstellt. Wenn ein Knotengruppenmitglied ausfällt, ersetzt ein Clusterknoten, der kein Mitglied der Knotengruppe ist, den ausgefallenen Knoten dynamisch. Dieser Knoten wird als Ersatzknoten bezeichnet.

> **Hinweis:**
>
> Für eine Einzelmitglieder-Knotengruppe wird ein Backup-Knoten automatisch vorausgewählt, wenn eine Entität an die Knotengruppe gebunden ist.

Wenn das ursprüngliche Mitglied der Knotengruppe auftaucht, wird der Ersatzknoten standardmäßig durch den ursprünglichen Mitgliedsknoten ersetzt.

Ab NetScaler 10.5 Build 50.10 können Sie jedoch mit dem Citrix ADC dieses Ersetzungsverhalten ändern. Wenn Sie die Sticky-Option aktivieren, wird der Ersatzknoten beibehalten, auch wenn der ursprüngliche Elementknoten angezeigt wird. Der ursprüngliche Knoten übernimmt nur, wenn der Ersatzknoten ausfällt.

Sie können auch die Sicherungsfunktion deaktivieren. Um dies zu tun, müssen Sie die strikte Option aktivieren. In diesem Szenario wird bei einem Ausfall eines Knotengruppenmitglieds kein anderer Clusterknoten als Backup-Knoten aufgenommen. Der ursprüngliche Knoten ist weiterhin Teil der Knotengruppe, wenn er auftaucht. Diese Option stellt sicher, dass an eine Knotengruppe gebundene Entitäten nur für Knotengruppenmitglieder aktiv sind.

> **Hinweis:**
>
> Die Option “Strict and Sticky” kann nur beim Erstellen einer Knotengruppe festgelegt werden.

# Konfigurieren von Knotengruppen für gepunktete und teilweise gestreifte Konfigurationen

October 5, 2021

Um eine Knotengruppe für gepunktete und teilweise gestreifte Konfigurationen zu konfigurieren, müssen Sie zuerst eine Knotengruppe erstellen und dann die erforderlichen Knoten an die Knotengruppe binden. Sie ordnen dann die erforderlichen Entitäten dieser Knotengruppe zu. Die Entitäten, die an die Knotengruppe gebunden sind, gehören zu den folgenden:

- **Entdeckt** - Wenn an eine Knotengruppe gebunden ist, die einen einzelnen Knoten hat.
- **Teilweise gestreift** - Wenn es an eine Knotengruppe gebunden ist, die mehr als einen Knoten hat.

**Einige Punkte, an die Sie sich erinnern sollten:**

- GSLB wird auf einem Cluster nur unterstützt, wenn GSLB-Sites an Knotengruppen gebunden sind, die einen einzelnen Cluster-Knoten haben. Weitere Informationen finden Sie unter Einrichten von GSLB in einem Cluster.
- Citrix Gateway wird auf einem Cluster nur unterstützt, wenn die virtuellen VPN-Server an Knotengruppen gebunden sind, die über einen einzelnen Clusterknoten verfügen. Die Sticky-Option muss für die Knotengruppe aktiviert sein.
- Für Versionen vor NetScaler 11 wird die Anwendungs-Firewall nur auf einzelnen Cluster-Knoten unterstützt (Spotted-Konfiguration). Profile der Anwendungsfirewall können nur virtuellen Servern zugeordnet werden, die an Knotengruppen mit einem einzelnen Clusterknoten gebunden sind. Dies bedeutet, dass Sie Folgendes nicht ausführen dürfen:
  - Binden Sie Anwendungs-Firewall-Profile an virtuelle Stripes- oder teilweise gestreifte Server.
  - Binden Sie die Richtlinie an einen globalen Bindungspunkt oder an benutzerdefinierte Richtlinienbeschriftungen.
  - Lösen Sie die Bindung von einer Knotengruppe, einem virtuellen Server, der über Anwendungsfirewallprofile verfügt.
- NetScaler 11 hat Anwendungsfirewall-Unterstützung für gestreifte und teilweise gestreifte Konfigurationen eingeführt. Weitere Informationen finden Sie unter Application Firewall-Unterstützung für Clusterkonfigurationen.

Überprüfen Sie die in einem Cluster unterstützten Citrix ADC Features, um die NetScaler-Versionen anzuzeigen, von denen GSLB, Citrix Gateway und Application Firewall in einem Cluster unterstützt werden.

### So konfigurieren Sie eine Knotengruppe mit der Befehlszeilenschnittstelle

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Erstellen Sie eine Knotengruppe. Typ:

   ```
   add cluster nodegroup <name> -strict (YES | NO)<!--NeedCopy-->
   ```

   Beispiel

   ```
   1 add cluster nodegroup NG0 -strict YES
   ```

3. Binden Sie die erforderlichen Knoten an die Knotengruppe. Geben Sie für jedes Mitglied der Knotengruppe den folgenden Befehl ein:

   ```
   bind cluster nodegroup <name> -node <nodeId><!--NeedCopy-->
   ```

   Beispiel

   So binden Sie Knoten mit IDs 1, 5 und 6.

   ```
   1 > bind cluster nodegroup NG0 -node 1
   2 > bind cluster nodegroup NG0 -node 5
   3 > bind cluster nodegroup NG0 -node 6
   ```

4. Binden Sie die Entität an die Knotengruppe. Geben Sie den folgenden Befehl einmal für jede Entität ein, die Sie binden möchten:

   ```
   bind cluster nodegroup <name> (-vServer <string> | -identifierName <
   string> | -gslbSite <string> -service <string>)<!--NeedCopy-->
   ```

   > **Hinweis:**
   >
   > Die Parameter GSLBSite und Service sind ab NetScaler 10.5 verfügbar.

   Beispiel

   Zum Binden virtueller Server VS1 und VS2 und der Begrenzungskennung mit dem Namen identifiier1.

   ```
   1 > bind cluster nodegroup NG0 -vServer VS1
   2 > bind cluster nodegroup NG0 -vServer VS2
   3 > bind cluster nodegroup NG0 -identifierName identifier1
   ```


5. Überprüfen Sie die Konfigurationen, indem Sie die Details der Knotengruppe anzeigen. Typ:

   ```
   show cluster nodegroup <name><!--NeedCopy-->
   ```

   Beispiel

   ```
   1 > show cluster nodegroup NG0
   ```

So konfigurieren Sie eine Knotengruppe mit dem Konfigurationsdienstprogramm

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster > Knotengruppen.**
3. Klicken Sie im Detailbereich auf **Hinzufügen.**
4. Konfigurieren **Sie im Dialogfeld "Knotengruppe erstellen** " die Knotengruppe:
   a) Klicken Sie unter **Clusterknoten**auf die Schaltfläche **Hinzufügen**.
      - Die Liste Verfügbare zeigt die Knoten an, die Sie an die Knotengruppe binden können, und in der Liste Konfiguriert werden die Knoten angezeigt, die an die Knotengruppe gebunden sind.
      - Klicken Sie auf das **+** -Zeichen in der Liste Verfügbar, um den Knoten zu binden. Klicken Sie auf das **-** Zeichen in der Liste Konfiguriert, um die Bindung des Knotens aufzuheben.

   b) Wählen Sie unter **Virtuelle Server**die Registerkarte aus, die dem Typ des virtuellen Servers entspricht, den Sie an die Knotengruppe binden möchten. Klicken Sie auf die Schaltfläche **Add**.
      - In der Liste Verfügbare werden die virtuellen Server angezeigt, die Sie an die Knotengruppe binden können, und in der Liste Konfiguriert werden die virtuellen Server angezeigt, die an die Knotengruppe gebunden sind.
      - Klicken Sie auf das **+** -Zeichen in der Liste Verfügbar, um den virtuellen Server zu binden. Klicken Sie auf das - Zeichen in der Liste Konfiguriert, um die Bindung des virtuellen Servers aufzuheben.

Konfigurieren von Redundanz für Knotengruppen

October 5, 2021

> **Hinweis:**
>
> Unterstützt ab NetScaler 10.5 Build 52.1115.e.

Knotengruppen können so konfiguriert werden, dass eine andere Knotengruppe bei einem Ausfallen einer Knotengruppe den Datenverkehr übernehmen und verarbeiten kann. Wenn beispielsweise eine Knotengruppe NG1 ausfällt, übernimmt NG2 die Kontrolle.

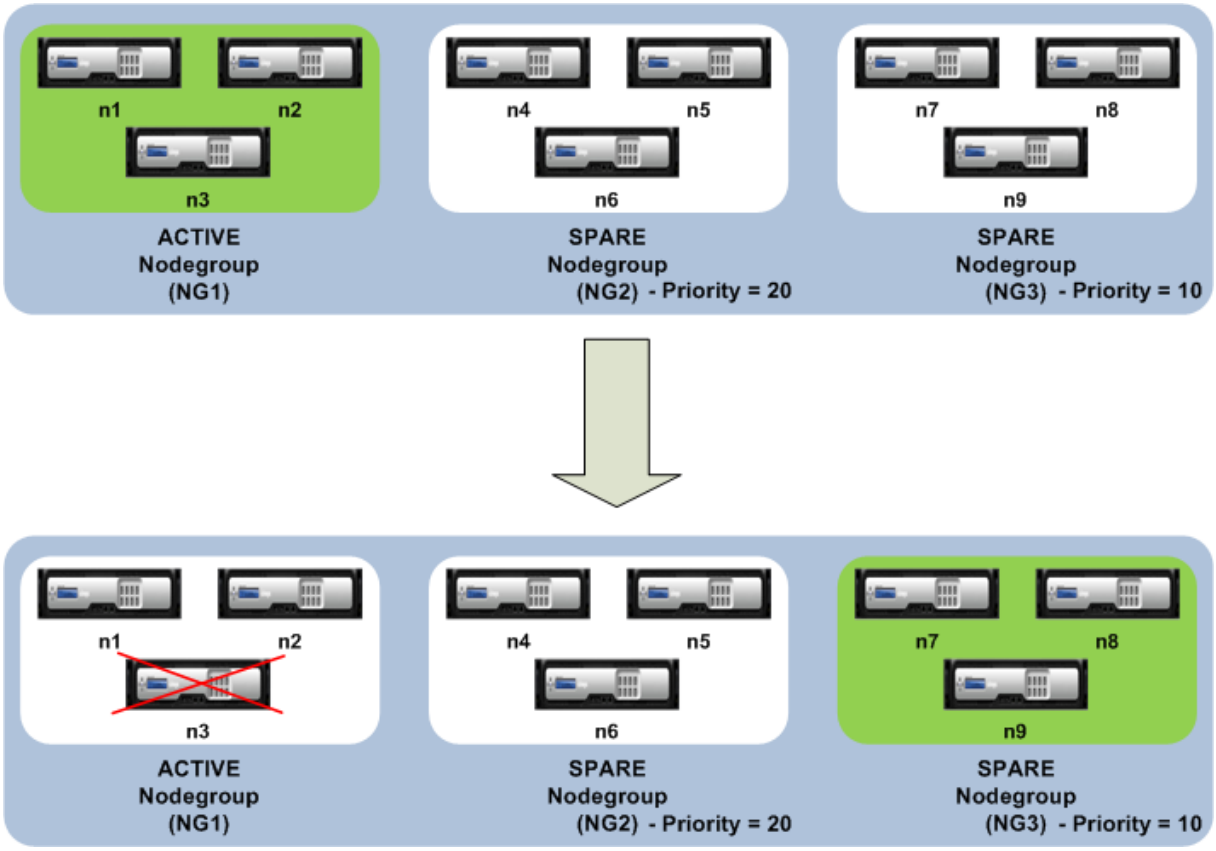
> **Hinweis:**
>
> Diese Funktionalität kann verwendet werden, um Redundanz von Rechenzentren zu konfigurieren, bei der jede Knotengruppe als Rechenzentrum konfiguriert ist.

Um diesen Anwendungsfall zu erreichen, müssen Clusterknoten logisch in Knotengruppen gruppiert werden, in denen einige Knotengruppen als ACTIVE und andere als SPARE konfiguriert werden müssen. Die aktive Knotengruppe mit der höchsten Priorität (d. h. der niedrigsten Prioritätsnummer) wird operativ aktiv und dient daher dem Datenverkehr. Wenn ein Knoten aus dieser operativ aktiven Knotengruppe ausfällt, wird die Knotenanzahl dieser Knotengruppe mit der Knotenanzahl der anderen aktiven Knotengruppen in der Reihenfolge ihrer Priorität verglichen. Wenn eine Knotengruppe eine höhere oder gleiche Knotenanzahl hat, wird diese Knotengruppe operativ aktiv gemacht. Andernfalls werden die Reserve-Knotengruppen überprüft.

> **Hinweis:**
>
> - Zu einem bestimmten Zeitpunkt kann nur eine statusspezifische Knotengruppe aktiv sein.
> - Ein Clusterknoten übernimmt den Status der Knotengruppe. Wenn also ein Knoten mit dem Status “SPARE” zur Knotengruppe mit dem Status “ACTIVE” hinzugefügt wird, verhält sich der Knoten automatisch wie ein aktiver Knoten.
> - Der für die Clusterinstanz definierte Preemption-Parameter entscheidet darüber, ob die anfängliche aktive Knotengruppe die Kontrolle übernimmt, wenn sie wieder auftaucht.
> - Eine Ersatzknotengruppe kann eine Knotengruppe aufnehmen und aktiven Datenverkehr hosten, wenn eine aktive Knotengruppe ausfällt.

Die folgende Abbildung zeigt ein Knotengruppen-Setup, bei dem die Redundanz der Knotengruppe definiert ist. NG1 ist zunächst die aktive Knotengruppe. Wenn er einen der Knoten verliert, beginnt die Spare-Node-Gruppe (NG3) mit der höchsten Priorität, den Datenverkehr zu bedienen.

Abbildung 1. Citrix ADC Cluster mit konfigurierter Redundanz der Knotengruppe.



Konfigurieren von Redundanz für Knotengruppen

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Erstellen Sie die aktive Knotengruppe und binden Sie die erforderlichen Cluster-Knoten.

```
1 > add cluster nodegroup NG1 -state ACTIVE
2 > bind cluster nodegroup NG1 -node n1
3 > bind cluster nodegroup NG1 -node n2
4 > bind cluster nodegroup NG1 -node n3
```

3. Erstellen Sie die Reserveknotengruppe und binden Sie die erforderlichen Knoten.

```
1 > add cluster nodegroup NG2 -state SPARE -priority 20
2 > bind cluster nodegroup NG2 -node n4
3 > bind cluster nodegroup NG2 -node n5
4 > bind cluster nodegroup NG2 -node n6
```

4. Erstellen Sie eine weitere Reserveknotengruppe und binden Sie die erforderlichen Knoten.


```
> add cluster nodegroup NG3 -state SPARE -priority 10
> bind cluster nodegroup NG3 -node n7
> bind cluster nodegroup NG3 -node n8
> bind cluster nodegroup NG3 -node n9
```

Deaktivieren der Steuerung auf der Clusterrückwandplatine

October 5, 2021

> **Hinweis:**
>
> Unterstützt ab NetScaler 11.

Das Standardverhalten eines Citrix ADC Clusters besteht darin, den empfangenen Datenverkehr (Flow Receiver) auf einen anderen Node (Flow Processor) zu leiten. Der Flow-Prozessor muss dann den Datenverkehr verarbeiten. Dieser Prozess der Leitung des Datenverkehrs vom Flowempfänger zum Flowprozessor erfolgt über die Cluster-Backplane und wird als Lenkung bezeichnet.

Bei Bedarf können Sie die Lenkung deaktivieren, damit der Prozess lokal für den Durchflussempfänger wird und daher den Durchflussempfänger zum Durchflussprozessor wird. Ein solches Konfigurations-Setup kann nützlich sein, wenn Sie eine Verbindung mit hoher Latenz haben.

> **Hinweis:**
>
> Diese Konfiguration ist nur für virtuelle Stripeset-Server anwendbar.

- Wenn der Flow-Empfänger bei teilweise gestreiften virtuellen Servern ein Nicht-Eigentümer-Knoten ist, wird der Datenverkehr auf einen Besitzerknoten geleitet. Wenn der Flow-Empfänger jedoch ein Besitzerknoten ist, ist die Steuerung deaktiviert.
- Bei gepunkteten virtuellen Servern ist der Flow-Empfänger der Flow-Prozessor, und daher ist keine Steuerung erforderlich.

Einige Punkte, die Sie beim Deaktivieren des Lenkmechanismus beachten sollten:

- Striped SNIPs werden nicht unterstützt, da die Steuerung deaktiviert ist.
- MPTCP und FTP funktionieren nicht.
- Der L2-Modus muss deaktiviert sein.
- Wenn USIP aktiviert ist, reicht der Datenverkehr möglicherweise nicht an denselben Knoten zurück, an dem die Steuerung deaktiviert ist.
- Der an die Cluster-IP-Adresse gerichtete Datenverkehr wird an den Konfigurationskoordinator gesteuert.

- Wenn ein Knoten einem Cluster beitritt oder diesen verlässt, ist es möglich, dass mehr als 1/N-Verbindungen betroffen sind. Dies liegt daran, dass eine Änderung der verfügbaren Knoten dazu führen kann, dass die Routen erneut aufbereitet werden. Infolgedessen wird der Verkehr an einen anderen Knoten weitergeleitet und aufgrund der Nichtverfügbarkeit der Steuerung wird der Verkehr nicht verarbeitet.

Die Steuerung kann auf individueller virtueller Serverebene oder auf globaler Ebene deaktiviert werden. Die globale Konfiguration hat Vorrang vor der Einstellung des virtuellen Servers.

- Deaktivieren der Steuerung der Rückwandplatine für alle virtuellen Stripes-Server

  Konfiguriert auf Clusterinstanzebene. Der für einen gestreifte virtuelle Server gerichtete Datenverkehr wird nicht auf die Cluster-Backplane gesteuert.

  ```
  add cluster instance \<clId\> -processLocal ENABLED<!--NeedCopy-->
  ```

- Deaktivieren der Steuerung der Rückwandplatine für einen bestimmten virtuellen gestreiften Server

  Konfiguriert auf einem virtuellen Stripeset-Server. Der für den virtuellen Server bedeutende Datenverkehr wird nicht auf die Cluster-Backplane gesteuert.

  ```
  add lb vserver <name> <serviceType> -processLocal ENABLED<!--NeedCopy
  -->
  ```

Synchronisieren von Clusterkonfigurationen

October 5, 2021

Citrix ADC Konfigurationen, die im Konfigurationskoordinator verfügbar sind, werden mit den anderen Knoten des Clusters synchronisiert, wenn:

- Ein Knoten schließt sich dem Cluster an
- Ein Knoten schließt sich dem Cluster wieder an
- Ein neuer Befehl wird über die Cluster-IP-Adresse ausgeführt

Außerdem können Sie die Konfigurationen, die im Konfigurationskoordinator (vollständige Synchronisierung) verfügbar sind, zwangsweise mit einem bestimmten Clusterknoten synchronisieren. Stellen Sie sicher, dass Sie jeweils einen Clusterknoten synchronisieren, andernfalls kann der Cluster betroffen sein.

So synchronisieren Sie Clusterkonfigurationen mit der CLI

Geben Sie an der Eingabeaufforderung der Appliance, auf der Sie die Konfigurationen synchronisieren möchten, Folgendes ein:


```
force cluster sync
```

So synchronisieren Sie Clusterkonfigurationen mit der GUI

1. Melden Sie sich bei der Appliance an, auf der Sie die Konfigurationen synchronisieren möchten.
2. Navigieren Sie zu **System > Cluster.**
3. Klicken Sie im Detailbereich unter **Dienstprogramme**auf Clustersynchronisierung erzwingen.
4. Klicken Sie auf **OK.**

Synchronisieren der Zeit über Clusterknoten hinweg

October 5, 2021

Der Cluster verwendet ein Precision Time Protocol (PTP), um die Zeit über Clusterknoten hinweg zu synchronisieren. PTP verwendet Multicastpakete, um die Zeit zu synchronisieren. Wenn bei der Zeitsynchronisierung einige Probleme auftreten, müssen Sie PTP deaktivieren und NTP (Network Time Protocol) auf dem Cluster konfigurieren.

So aktivieren/deaktivieren Sie PTP mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung der Cluster-IP-Adresse Folgendes ein:

```
set ptp -state disable
```

So aktivieren/deaktivieren Sie PTP mit dem Konfigurationsdienstprogramm

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster.**
3. Klicken Sie im Detailbereich unter **Dienstprogramme**auf **PTP-Einstellungen konfigurieren.**
4. Wählen Sie im Dialogfeld **PTP aktivieren/deaktivieren** aus, ob Sie PTP aktivieren oder deaktivieren möchten.
5. Klicken Sie auf **OK.**

Synchronisieren von Clusterdateien

October 5, 2021

Die im Konfigurationskoordinator verfügbaren Dateien werden Clusterdateien genannt. Diese Dateien werden automatisch auf den anderen Clusterknoten synchronisiert, wenn der Knoten dem Cluster hinzugefügt wird, und in regelmäßigen Abständen während der Lebensdauer des Clusters. Außerdem können Sie die Clusterdateien manuell synchronisieren.

Wichtig: Das Entfernen von Zertifikaten oder Schlüsseldateien in einer Clusterumgebung schränkt die weitere Konfiguration auf der ADC-Appliance ein. Fügen Sie die Dateien am selben Speicherort hinzu, um Konfigurationsänderungen vorzunehmen.

Die synchronisierten Verzeichnisse und Dateien des Konfigurationskoordinators sind:

- /nsconfig/ssl/
- /var/netscaler/ssl/
- /var/vpn/bookmark/
- /nsconfig/dns/
- /nsconfig/htmlinjection/
- /netscaler/htmlInjection/ens/
- /nsconfig/monitors/
- /nsconfig/nstemplates/
- /nsconfig/ssh/
- /nsconfig/rc.netscaler
- /nsconfig/resolv.conf
- /nsconfig/inetd.conf
- /nsconfig/syslog.conf
- /nsconfig/snmpd.conf
- /nsconfig/ntp.conf
- /nsconfig/httpd.conf
- /nsconfig/sshd_config
- /nsconfig/hosts
- /nsconfig/enckey
- /var/nslw.bin/etc/krb5.conf
- /var/nslw.bin/etc/krb5.keytab
- /var/lib/likee/db/
- /var/download/
- /var/wi/tomcat/webapps/
- /var/wi/tomcat/conf/Catalina/Localhost/
- /var/wi/java_home/lib/security/cacerts

- /var/wi/java_home/jre/lib/security/cacerts
- /nsconfig/license/
- /nsconfig/rc.conf

> **Tipp**
>
> Dateien (Zertifikate und Schlüsseldateien), die manuell (oder über die Shell) in den Clusterkonfigurationskoordinator kopiert werden, sind auf den anderen Clusterknoten nicht automatisch verfügbar. Führen Sie den Befehl "Clusterdateien synchronisieren" von der Cluster-IP-Adresse aus, bevor Sie einen Befehl ausführen, der von diesen Dateien abhängt.

So synchronisieren Sie Clusterdateien mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung der Cluster-IP-Adresse Folgendes ein:

```
sync cluster files <mode>
```

So synchronisieren Sie Clusterdateien mit dem Konfigurationsdienstprogramm

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster.**
3. Klicken Sie im Detailbereich unter **Dienstprogramme**auf Clusterdateien synchronisieren.
4. Wählen Sie im Dialogfeld Clusterdateien **synchronisieren** die zu synchronisierenden Dateien in der Dropdownliste Modus aus.
5. Klicken Sie auf **OK.**

Anzeigen der Statistiken eines Clusters

October 5, 2021

Sie können die Statistiken einer Clusterinstanz und Clusterknoten anzeigen, um die Leistung zu bewerten oder den Betrieb des Clusters zu beheben.

So zeigen Sie die Statistiken einer Clusterinstanz mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung der Cluster-IP-Adresse Folgendes ein:

```
stat cluster instance <clId>
```


So zeigen Sie die Statistiken eines Clusterknotens mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung der Cluster-IP-Adresse Folgendes ein:

```
1 stat cluster node <nodeid>
```

> **Hinweis:**
>
> Der `stat cluster node <nodeid>` Befehl zeigt die Statistiken auf Clusterebene an, wenn Sie den Befehl von der Cluster-IP-Adresse aus ausführen. Wenn Sie jedoch von der NSIP-Adresse eines Clusterknotens aus ausführen, zeigt der Befehl Statistiken auf Knotenebene an.

So zeigen Sie die Statistiken einer Clusterinstanz mit dem Konfigurationsdienstprogramm an

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster.**
3. Klicken Sie im Detailbereich in der Mitte der Seite auf **Statistik.**

So zeigen Sie die Statistiken eines Clusterknotens mit dem Konfigurationsdienstprogramm an

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster > Knoten.**
3. Wählen Sie im Detailbereich einen Knoten aus, und klicken Sie auf **Statistik**, um die Statistiken des Knotens anzuzeigen. Um die Statistiken aller Knoten anzuzeigen, klicken Sie auf **Statistik**, ohne einen bestimmten Knoten auszuwählen.

Erkennen von Citrix ADC-Appliances

October 5, 2021

Sie können die Appliances erkennen, die sich im selben Subnetz wie der aktuelle Knoten befinden. Die erforderlichen erkannten Appliances können dann selektiv dem Cluster hinzugefügt werden. Dieser Vorgang kann entweder zum Erstellen eines Clusters oder zum Hinzufügen von Knoten zu einem vorhandenen Cluster durchgeführt werden.

> **Hinweis:**
>
> - Der Ermittlungsvorgang kann nur über das Konfigurationsdienstprogramm ausgeführt wer-

> den.
> - Dieser Vorgang kann Citrix ADC Appliances aus verschiedenen Netzwerken nicht erkennen.
> - Wenn Sie diesen Vorgang ausführen, um Knoten zu einem vorhandenen Cluster hinzuzufügen, werden die L3-VLAN-Konfigurationen vom Knoten gelöscht. Sie stellen sicher, dass Sie diese Konfigurationen definieren, sobald die Appliance dem Cluster hinzugefügt wurde.

So entdecken Sie Appliances mit der GUI

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Navigieren Sie zu **System > Cluster > Knoten.**
3. Klicken Sie im Detailbereich unten auf der Seite auf **NetScalers entdecken.**
4. Legen **Sie im Dialogfeld NetScalers Discover** die folgenden Parameter fest:
   - **IP-Adressbereich** - Geben Sie den Bereich der IP-Adressen an, in dem Appliances gefunden werden sollen. Beispielsweise können Sie nach allen NSIP-Adressen zwischen 10.102.29.4 und 10.102.29.15 suchen, indem Sie diese Option als 10.102.29.4 - 15 angeben.
   - **Backplane-Schnittstelle** - Geben Sie die Schnittstellen an, die als Backplane-Schnittstelle verwendet werden sollen. Dies ist ein optionaler Parameter. Wenn Sie diesen Parameter nicht angeben, müssen Sie ihn aktualisieren, nachdem der Knoten dem Cluster hinzugefügt wurde.
5. Klicken Sie auf **OK.**
6. Wählen Sie die Appliances aus, die Sie dem Cluster hinzufügen möchten.
7. Klicken Sie auf **OK.**

Deaktivieren eines Clusterknotens

October 5, 2021

Sie können einen Knoten vorübergehend aus einem Cluster entfernen, indem Sie die Clusterinstanz auf diesem Knoten deaktivieren. Ein deaktivierter Knoten wird nicht mit den Clusterkonfigurationen synchronisiert. Wenn der Knoten wieder aktiviert ist, werden die Clusterkonfigurationen automatisch synchronisiert. Weitere Informationen finden Sie unter Synchronisation über Clusterknotenhinweg.

Ein deaktivierter Knoten kann keinen Datenverkehr bereitstellen, und alle vorhandenen Verbindungen auf diesem Knoten werden beendet.

> **Hinweis:**
>
> Wenn die Konfigurationen eines deaktivierten Koordinatorknotens ohne Konfiguration geändert werden (über die NSIP-Adresse des Knotens), werden die Konfigurationen auf diesem Knoten nicht automatisch synchronisiert. Sie können die Konfigurationen wie unter Clusterkonfigura-

> tionen synchronisierenbeschrieben manuell synchronisieren.

So deaktivieren Sie einen Clusterknoten mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung des Knotens, den Sie deaktivieren möchten, Folgendes ein:

```
1 disable cluster instance <clId>
```

> **Hinweis:**
>
> Führen Sie zum Deaktivieren des Clusters den Befehl
> disable cluster instance für die Cluster-IP-Adresse aus.

So deaktivieren Sie einen Clusterknoten mit dem Konfigurationsdienstprogramm

1. Navigieren Sie auf dem Knoten, den Sie deaktivieren möchten, zu **System > Cluster**, und klicken Sie auf **Cluster verwalten.**
2. Deaktivieren **Sie im Dialogfeld Clusterinstanz konfigurieren** das Kontrollkästchen Clusterinstanz **aktivieren**.

   > **Hinweis:**
   >
   > Um die Clusterinstanz auf allen Knoten zu deaktivieren, führen Sie das vorherige Verfahren für die Cluster-IP-Adresse aus.

Entfernen eines Clusterknotens

October 5, 2021

Wenn ein Knoten aus dem Cluster entfernt wird, werden die Clusterkonfigurationen vom Knoten gelöscht (indem intern der Befehl clear ns config -extended ausgeführt wird). Die SNIP-Adressen, **MTU-Einstellungen** der Backplane-Schnittstelle und alle VLAN-Konfigurationen (mit Ausnahme des Standard-VLAN und des NSVLAN) werden ebenfalls von der Appliance gelöscht.

> **Hinweis:**
>
> - Wenn der gelöschte Knoten der Clusterkonfigurationskoordinator (CCO) war, wird automatisch ein anderer Knoten als CCO ausgewählt, und die Cluster-IP-Adresse wird diesem Knoten zugewiesen. Alle aktuellen Cluster-IP-Adresssitzungen sind ungültig und Sie müssen eine neue Sitzung starten.
> - Um den gesamten Cluster zu löschen, müssen Sie jeden Knoten einzeln entfernen. Wenn

> Sie den letzten Knoten entfernen, werden die Cluster-IP-Adressen gelöscht.
> - Wenn ein aktiver Knoten entfernt wird, wird die Traffic Serving-Fähigkeit des Clusters um einen Knoten reduziert. Vorhandene Verbindungen auf diesem Knoten werden beendet.

So entfernen Sie einen Clusterknoten mit der CLI

Für NetScaler 10.1 und höher

1. Melden Sie sich bei der Cluster-IP-Adresse an und geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm cluster node <nodeId>

save ns config
```

2. Melden Sie sich am entfernten Knoten, der NSIP-Adresse an und geben Sie an der Eingabeaufforderung Folgendes ein:

```
save ns config
```

> **Hinweis:**
>
> Wenn die Cluster-IP-Adresse vom Knoten aus nicht erreichbar ist, führen Sie den Befehl RM-Clusterinstanz-Befehl für die NSIP-Adresse dieses Knotens selbst aus.

Für NetScaler 10

1. Melden Sie sich bei dem Knoten an, den Sie aus dem Cluster entfernen möchten, und entfernen Sie den Verweis auf die Clusterinstanz.

```
rm cluster instance <clId>

save ns config
```

2. Melden Sie sich bei der Cluster-IP-Adresse an, und entfernen Sie den Knoten, von dem Sie die Clusterinstanz entfernt haben.


```
rm cluster node <nodeId>

save ns config
```

Stellen Sie sicher, dass Sie den `rm cluster node` Befehl nicht vom lokalen Knoten ausführen. Dies führt zu inkonsistenten Konfigurationen zwischen dem CCO und dem Knoten.

So entfernen Sie einen Clusterknoten mit der GUI

Navigieren Sie auf der Cluster-IP-Adresse zu **System > Cluster > Knoten, wählen Sie den Knoten**aus, den Sie entfernen möchten, und klicken Sie auf **Entfernen.**

Entfernen eines Knotens aus einem Cluster, der mit der Clusterverknüpfungsaggregation bereitgestellt wird

October 5, 2021

Um einen Knoten aus einem Cluster zu entfernen, der Clusterverknüpfungsaggregation als Verkehrsverteilungsmechanismus verwendet, müssen Sie sicherstellen, dass der Knoten passiv ist, damit er keinen Datenverkehr empfängt, und entfernen Sie dann auf dem Upstream-Switch die entsprechende Schnittstelle aus dem Kanal.

Ausführliche Informationen zur Cluster-Link-Aggregation finden Sie unter Verwenden der Cluster-Link-Aggregation.

So entfernen Sie einen Knoten aus einem Cluster, der die Clusterverknüpfungsaggregation als Verkehrsverteilungsmechanismus verwendet

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Legen Sie den Status des Clusterknotens, den Sie entfernen möchten, auf PASSIVE fest.

```
set cluster node <nodeId> -state PASSIVE
```

3. Entfernen Sie auf dem Upstream-Switch die entsprechende Schnittstelle mit schaltspezifischen Befehlen aus dem Kanal.

> **Hinweis:**
>
> Sie müssen die Knotenschnittstelle auf dem Cluster-Link-Aggregationskanal nicht manuell entfernen. Es wird automatisch entfernt, wenn der Knoten im nächsten Schritt gelöscht wird.

4. Entfernen Sie den Knoten aus dem Cluster.

```
rm cluster node <nodeId>
```

Erkennen von Jumbo-Sonden auf einem Cluster

October 5, 2021

Wenn ein Jumbo-Frame auf einer Clusterschnittstelle aktiviert ist, muss die Backplane-Schnittstelle groß genug sein, um alle Pakete im Jumbo-Frame zu unterstützen. Dies wird erreicht, indem die Maximum Transmission Unit (MTU) der Rückwandplatine wie folgt eingestellt wird:

backplane_MTU = Maximum (alle Cluster-Schnittstelle MTUs) + 78

Um die vorangehende Konfiguration zu überprüfen, müssen Sie einen Jumbo-Prüfpunkt (der vorherigen Berechnungsgröße) an alle Peer-Knoten eines Cluster-Setups senden. Wenn der Prüfpunkt nicht erfolgreich ist, zeigt die Appliance eine Warnmeldung in der Ausgabe des Befehls Clusterinstanz anzeigen an.

Geben Sie im Befehlszeilenschnittstellenmodus den folgenden Befehl ein:

```
> show cluster instance
  Cluster ID: 1
  Dead Interval: 3 secs
  Hello Interval: 200 msecs
  Preemption: DISABLED
  Propagation: ENABLED
  Quorum Type: MAJORITY
  INC State: DISABLED
  Process Local: DISABLED
  Cluster Status: ENABLED(admin),    ENABLED(operational), UP
```


> **Warnung**
>
> Die MTU für eine Backplane-Schnittstelle muss groß genug sein, um alle Pakete im Rahmen zu verarbeiten. Es muss gleich <MTU_VAL> sein. Wenn der empfohlene Wert nicht vom Benutzer konfigurierbar ist, müssen Sie den MTU-Wert von Jumbo-Schnittstellen überprüfen.

Sl. no	Mitgliedsknoten	Integrität	Admin-Status	Betriebszustand
1	Node ID: 1; Node IP: 10.102.53.167	BEREIT	Aktiv	ACTIVE (Configuration Coordinator)
2	Node ID: 2; Node IP: 10.102.53.168	BEREIT	Aktiv	Aktiv

Routenüberwachung für dynamische Routen im Cluster

October 5, 2021

Sie können einen Routenmonitor verwenden, um einen Clusterknoten von der internen Routingtabelle abhängig zu machen, unabhängig davon, ob er eine dynamisch erlernte Route enthält oder nicht. Ein Routenmonitor auf jedem Knoten überprüft die interne Routingtabelle, um sicherzustellen, dass immer ein Routeneintrag zum Erreichen eines bestimmten Netzwerks vorhanden ist. Wenn der Routeneintrag nicht vorhanden ist, ändert sich der Status des Routenmonitors in DOWN.

Wenn in einer Clusterbereitstellung der clientseitige oder serverseitige Link eines Knotens ausfällt, wird der Datenverkehr zu diesem Knoten über die Peer-Knoten zur Verarbeitung gelenkt. Die Steuerung des Datenverkehrs wird implementiert, indem dynamisches Routing konfiguriert und statische ARP-Einträge hinzugefügt werden, die auf die spezielle MAC-Adresse jedes Knotens zeigen, auf allen Knoten. Wenn es in einer Clusterbereitstellung viele Knoten gibt, ist das Hinzufügen und Verwalten von statischen ARP-Einträgen mit speziellen MAC-Adressen auf allen Knoten eine umständliche Aufgabe. Jetzt verwenden Knoten implizit spezielle MAC-Adressen für die Steuerung von Paketen. Daher müssen statische ARP-Einträge, die auf spezielle MAC-Adressen verweisen, nicht mehr zu den Clusterknoten hinzugefügt werden.

So binden Sie einen Clusterknoten mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
bind cluster node <nodeId> (-routeMonitor <ip_addr|ipv6_addr|*> [<
    netmask>])
unbind cluster node <nodeId> (-routeMonitor <ip_addr|ipv6_addr|*> [<
    netmask>])
```

Betrachten Sie ein Szenario, in dem Knoten 1 an den Routenmonitor 1.1.1.0 255.255.255.0 gebunden ist. Wenn eine dynamische Route fehlschlägt, wird Knoten 1 INAKTIV. Der Integritätsstatus steht im folgenden `show cluster node` Befehl nach Knoten-ID zur Verfügung.

```
Node ID: 1
IP:  10.102.169.96
Backplane:  1/1/2
Health: NOT UP
Reason(s): Route Monitor(s) of the node have failed
Route Monitor -  Network: 1.1.1.0   Netmask: 255.255.255.0   State:
    DOWN
```

Überwachung der Cluster-Setup mit SNMP MIB mit SNMP-Verbindung

October 5, 2021

SNMP MIB sind gerätespezifische Informationen, die auf dem SNMP-Agenten zur Identifizierung einer Citrix ADC Appliance konfiguriert sind. Es kann Informationen wie Appliance-Name, Administrator und Standort identifizieren. In einem Cluster-Setup können Sie jetzt die SNMP-MIB in jedem Knoten konfigurieren, indem Sie den Parameter “OwnerNode” in den eingestellten SNMP-MIB-Befehl einbeziehen. Ohne diesen Parameter gilt der eingestellte SNMP-MIB-Befehl nur für den Cluster Coordinator (CCO) -Knoten.

Um die MIB-Konfiguration für einen anderen Clusterknoten als den CCO anzuzeigen, schließen Sie den Parameter “OwnerNode” in den Befehl show SNMP MIB ein.

Konfigurieren von SNMP MIB auf CLIP

So konfigurieren und anzeigen Sie die MIB-Konfiguration auf CLIP mit der Befehlszeilenschnittstelle.

```
set snmp mib [-contact <string>] [-name <string>] [-location <string>]
      [-customID <string>] [-ownerNode <positive_integer>]
Done
```



```
show snmp mib [-ownerNode <positive_integer>]

 > set mib -contact John -name NS59 -location San Jose -customID 123 -
    ownerNode 3
Done
> sh mib -ownerNode 3
        --------------------
         Cluster Node ID: 3
        --------------------
        NetScaler system MIB:
        sysDescr:    NetScaler NS11.1: Build 46.4.a.nc, Date: Jun  7
           2016, 10:27:29
        sysUpTime:   124300
        sysObjectID: .1.3.6.1.4.1.5951.1.1
        sysContact:  John
        sysName:     NS59
        sysLocation: San Jose
        sysServices: 72
        Custom ID: 123
 Done

> unset mib -contact -name -location -customID -ownerNode 3
 Done
> sh mib -ownerNode 3
        --------------------
         Cluster Node ID: 3
        --------------------
        NetScaler system MIB:
        sysDescr:    NetScaler NS11.1: Build 46.4.a.nc, Date: Jun 7
           2016, 10:27:29
        sysUpTime:   146023
        sysObjectID: .1.3.6.1.4.1.5951.1.1
        sysContact:  WebMaster (default)
        sysName:     NetScaler
        sysLocation: POP (default)
        sysServices: 72
        Custom ID: Default
 Done
```

Cluster SNMP-Trap-Nachrichten

Beim Cluster-Setup müssen die Konfigurationen des SNMP-Trap-Alarms vom CLIP aus durchgeführt werden. Die Befehle werden an jeden der Knoten weitergegeben.

Weitere Informationen zum Konfigurieren von SNMP finden Sie unter Konfigurieren des Citrix ADC zum Generieren von SNMP-Traps.

Im Folgenden sind die Cluster-spezifischen Traps aufgeführt, die verfügbar sind:

```
>sh snmp alarm | grep cluster
    CLUSTER-BACKPLANE-HB-MISSING N/A N/A 86400   ENABLED - ENABLED
    CLUSTER-CCO-CHANGE N/A N/A N/A ENABLED - ENABLED
    CLUSTER-NODE-HEALTH N/A N/A 86400 ENABLED - ENABLED
    CLUSTER-NODE-QUORUM N/A N/A 86400 ENABLED - ENABLED
    CLUSTER-OVS-CHANGE N/A N/A N/A ENABLED - ENABLED
    CLUSTER-PROP-FAILURE N/A N/A N/A ENABLED - ENABLED
    CLUSTER-SYNC-FAILURE N/A N/A N/A ENABLED - ENABLED
    CLUSTER-SYNC-PARTIAL-SUCCESS N/A N/A N/A ENABLED - ENABLED
    CLUSTER-VERSION-MISMATCH N/A N/A 86400 ENABLED - ENABLED
```

Überwachen von Befehlsausbreitungsfehlern in einer Clusterbereitstellung

October 5, 2021

In einer Clusterbereitstellung können Sie den neuen Befehl “Requisiten-Status anzeigen” verwenden, um Probleme schneller zu überwachen und zu beheben. Die Probleme im Zusammenhang mit dem Ausfall der Befehlsverbreitung auf Nicht-CCO-Knoten. Mit diesem Befehl werden bis zu 20 der letzten Befehlsausbreitungsfehler auf allen Nicht-CCO-Knoten angezeigt. Sie können entweder die Citrix ADC Appliance CLI oder GUI verwenden, um diesen Vorgang auszuführen. Sie können über die CLIP-Adresse oder über die NSIP-Adresse eines beliebigen Knotens in der Clusterbereitstellung darauf zugreifen.

Ordnungsgemäßes Herunterfahren von Knoten

October 5, 2021

Bei einem Cluster-Setup gehen einige der vorhandenen Verbindungen (1/N Verbindungen, wobei N die Clustergröße ist) auf Clusterebene oder bestimmte virtuelle Serverebene verloren. Dieses Verhalten wird beobachtet, wenn ein Knoten das System verlässt oder verbindet. Um den Verlust zu beheben, müssen Sie die vorhandenen Verbindungen ordnungsgemäß behandeln. Die ordnungsgemäße Hand-

habung erfolgt durch Konfigurieren der Option “Verbindungen im Cluster beibehalten” in der CLIP-Adresse und Angabe eines Timeout-Intervalls im NSIP des Knotens.

Die ordnungsgemäße Handhabung von Verbindungen ist in zwei Szenarien anwendbar:

1. Cluster-Upgrade
2. Hinzufügen eines neuen Knotens

Ordnungsgemäße Behandlung von Knoten im Cluster-Upgrade

Um ein Cluster zu aktualisieren, müssen Sie jeweils einen Knoten aktualisieren. Bevor Sie einen Knoten aktualisieren, müssen Sie ihn auf den passiven Zustand einstellen und ihn nach dem Upgrade auf den aktiven Status festlegen. Um das Beenden vorhandener Verbindungen beim Aktualisieren des Knotens zu vermeiden, schließen Sie ihn ordnungsgemäß mit einem konfigurierten Zeitüberschreitungsintervall ab. Andernfalls wird 1/Nth (wobei N die Clustergröße ist) der Verbindungen des Clusters beendet.

> **Hinweis:**
>
> Wenn vorhandene Sitzungen nicht innerhalb des konfigurierten Zeitüberschreitungsintervalls abgeschlossen werden, werden sie nach der Kulanzzeit beendet.

Im Folgenden sind die Schritte, um Knoten in einem Cluster-Upgrade-Szenario ordnungsgemäß zu behandeln:

1. Betrachten Sie ein Cluster-Setup von fünf Knoten (n0, n1, n2, n3, n4).
2. Bevor Sie einen Knoten herunterfahren, müssen Sie die Option “retainConnectionsOnCluster” konfigurieren. Es hilft, alle vorhandenen Verbindungen dieses Knotens auf Cluster- oder virtueller Serverebene für ein bestimmtes Zeitintervall beizubehalten.

   Beispiel

   Auf CLIP

   “‘set cluster instance –retainConnectionsOnCluster YES

   ```
   ODER

   ```set lb vserver <vserver name>  - retainConnectionsOnCluster Yes
      <!--NeedCopy-->
   ```

3. Melden Sie sich nun an der NSIP-Adresse des Knotens n3 an und setzen Sie den Knoten n3 auf PASSIVE mit einem internen Timeout.

   Beispiel


   ```

“‘set cluster node n3 –state PASSIVE –delay 60

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

4. Schließen Sie nach Ablauf der Kulanzfrist alle Verbindungen, fahren Sie n3 herunter und starten Sie die Citrix ADC Appliance neu.
5. Aktualisieren Sie die Appliance. Legen Sie dann, wenn die CLI mit der NSIP-Adresse der Appliance verbunden ist, den Knoten auf ACTIVE fest.

   Beispiel

   “‘set cluster node n3 –state ACTIVE

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

6. Wiederholen Sie die Schritte 4 bis 6 für alle Knoten im Cluster.
7. Nachdem alle Knoten aktualisiert und auf ACTIVE festgelegt wurden, setzen Sie die Option RetainConnectionsOnCluster von der CLIP-Adresse zurück.

   Beispiel

   “‘set cluster instance -retainConnectionsOnCluster NO

```
ODER

```set lb vserver <vserver name>  - retainConnectionsOnCluster NO
   <!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn beim Upgrade eines Clusters eine nicht übereinstimmende Version vorliegt, wird die Clusterausbreitung automatisch deaktiviert, und es sind keine Befehle auf dem CLIP zulässig.

Ordnungsgemäße Handhabung von Knoten während einer neuen Knotenzufügung

Die ordnungsgemäße Behandlung von Knoten beschreibt, wie ein neuer Knoten dem vorhandenen Citrix ADC Cluster hinzugefügt werden kann. Angenommen, Sie haben einen Citrix ADC Cluster,


```

der bereits Datenverkehr bereitstellt. Und Sie möchten dem Cluster eine zusätzliche Appliance als Knoten hinzufügen, ohne die vorhandenen Verbindungen zu beenden. Um das vorhergehende Szenario durchzuführen, legen Sie die Option fest, vorhandene Verbindungen entweder auf globaler Ebene oder auf einer bestimmten virtuellen Serverebene beizubehalten. Sobald Sie fertig sind, speichern Sie die Konfiguration. Setzen Sie nun die Option, Verbindungen auf NO beizubehalten, damit vorhandene Verbindungen von anderen Knoten dem neuen Knoten neu zugewiesen werden können.

Im Folgenden sind die Schritte, um Knoten ordnungsgemäß behandeln, wenn ein Knoten neu hinzugefügt:

1. Sie speichern die vorhandene Konfiguration, für die die Option “RetainConnectionsOnCluster” aktiviert ist. Auf diese Weise können Sie alle vorhandenen Verbindungen dieses Knotens auf Cluster- oder virtueller Serverebene für ein bestimmtes Zeitintervall beibehalten.

   Auf CLIP

   ```
   set cluster instance x - retainConnectionsOnCluster YES
   ```

   ODER

   ```
   set lb vserver xxxx -retainConnectionsOnCluster Yes
   ```

2. Fügen Sie dem Cluster-Setup einen Knoten ‘n5’ hinzu.
3. Deaktivieren Sie die Option “RetainConnectionOnCluster” auf “NO”, um vorhandene Verbindungen von anderen Knoten an den neu hinzugefügten Knoten n5 zu verteilen.

   Auf CLIP

   ```
   set cluster instance x - retainConnectionsOnCluster NO
   ```

   ODER

   ```
   set lb vserver xxxx -retainConnectionsOnCluster NO
   ```

> **Hinweis:**
>
> Die Backplane-Steuerung hängt von der Art des Verkehrsverteilungsmechanismus (ECMP, CLAG und USIP) bei einem Cluster-Setup ab. Der Anstieg der Backplane-Lenkung basiert auf der

> Verkehrsart.

Konfigurieren des ordnungsgemäßen Herunterfahrens von Knoten in einem Cluster

Gehen Sie folgendermaßen vor, um das ordnungsgemäße Herunterfahren von Knoten in einem Cluster zu konfigurieren:

1. Konfigurieren Sie die Option “RetainConnectionsonCluster” auf globaler Ebene (Cluster).
2. Konfigurieren Sie die Option “RetainConnectionsOnCluster” auf der Ebene des virtuellen Servers.
3. Setzen Sie den Knoten (das System verlassen) auf den passiven Zustand mit einem ordnungsgemäßen Timeout-Intervall, das in der NSIP-Adresse des Knotens angegeben ist.
4. Überwachen Sie die vorhandenen Verbindungen, um sicherzustellen, dass alle Transaktionen innerhalb der Kulanzfrist abgeschlossen sind.

So behalten Sie vorhandene Verbindungen auf globaler (Cluster-) Ebene über die Befehlszeilenschnittstelle

Sie können vorhandene Verbindungen entweder auf globaler Ebene oder auf einer bestimmten virtuellen Serverebene beibehalten. Diese Option ist so konfiguriert, dass alle vorhandenen Verbindungen auf globaler Ebene beibehalten werden. Standardmäßig ist diese Option deaktiviert.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 - set cluster instance <clusterID> - retainConnectionsOnCluster YES
2
3 - set cluster instance 60 - retainConnectionsOnCluster YES
```

So behalten Sie vorhandene Verbindungen eines bestimmten virtuellen Servers im Cluster über die Befehlszeilenschnittstelle

Diese Option ist so konfiguriert, dass vorhandene Verbindungen, die für einen virtuellen Lastausgleichsserver spezifisch sind, beibehalten werden. Um diese Verbindungen beizubehalten, aktivieren wir diese Option auf der Ebene des virtuellen Servers. Standardmäßig ist diese Option deaktiviert.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 - set lb vserver <clusterID> - retainConnectionsOnCluster Yes
2
3 - set lb vserver v1 - retainConnectionsOnCluster Yes
```


So setzen Sie einen Clusterknoten mit der CLI auf den passiven Status

So stellen Sie einen Clusterknoten in passiven Zustand mit einem ordnungsgemäßen Timeout-Intervall ein. Diese Einstellung wird im NSIP des Knotens durchgeführt, da die Propagierung während des Cluster-Upgrades deaktiviert ist.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1  -  set cluster node <clusterID> -state passive
2 -backplane <interface_name>@
3 -priority <positive_integer>
4 -delay <mins>
5
6  -  set cluster node 4  - state PASSIVE -delay 60
7
8  -  set cluster instance 60  -  retainConnectionsOnCluster YES
9  -  set lb vserver v1  - retainConnectionsOnCluster Yes
10 -  set cluster node 4  - state PASSIVE -delay 60
```

> **Hinweis:**
>
> Sie können das folgende Verhalten auf einem Clusterknoten beobachten, wenn er mit einer aus einem CLIP konfigurierten Verzögerungsoption auf passiv gesetzt ist:
>
> - Nach dem Timeout wird der Knoten vom NSIP des Knotens als passiv angezeigt.
> - Der Befehl **show cluster instance** auf CLIP zeigt den Knoten als aktiv aus dem CLIP an. Während der Befehl **show cluster node** auf dem CLIP den Knoten als passiv anzeigt.

So konfigurieren Sie das ordnungsgemäße Herunterfahren von Knoten mit der GUI

1. Navigieren Sie zu **Konfiguration > System > Cluster**, und klicken Sie auf **Cluster verwalten.**
2. Wählen Sie auf der Seite **Cluster verwalten** die Option **Verbindungen im Cluster beibehalten** aus.
3. Klicken Sie auf **OK**, und klicken Sie dann auf **Fertig**.

Ordnungsgemäßes Herunterfahren von Diensten

October 5, 2021

Ab NetScaler 12.1 Build 49.xx unterstützen Citrix ADC Cluster das ordnungsgemäße Herunterfahren von Diensten. Um die Dienste ordnungsgemäß herunterzufahren, können Sie eine der folgenden Aufgaben ausführen.

- Deaktivieren Sie den Dienst explizit und
  - Stellen Sie eine Verzögerung (in Sekunden) ein.
  - Aktivieren Sie das ordnungsgemäße Herunterfahren.
- Fügen Sie dem Monitor einen TROFS-Code oder eine Zeichenfolge hinzu.

Weitere Informationen finden Sie unter Graceful Shutdown von Diensten.

So konfigurieren Sie ein ordnungsgemäßes Herunterfahren für einen Dienst mit der CLI

Deaktivieren Sie nur mit ordnungsgemäßer Option:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
disable service <name> [-graceFul (YES|NO)]

show service <name>
<!--NeedCopy-->
```

Beispiel

```
disable service svc1 -graceFul YES
Done
sh service svc1
                svc1 (10.102.225.11:80) - HTTP
                State: GOING OUT OF SERVICE   Graceful (number of
                   active clients: 1)
                Last state change was at Wed Jul 25 10:46:29 2018
                Time since last state change: 0 days, 00:00:02.680
                ... ... ... .
                ... ... ... .
                Traffic Domain: 0

1)            Monitor Name: tcp-default
                                State: UP              Weight: 1
                                                Passive: 0
                                Probes: 26           Failed [Total: 0
                                   Current: 0]
                                Last response: Success - TCP syn+ack
                                   received.
                                Response Time: 0.0 millisec
<!--NeedCopy-->
```


Deaktivieren Sie mit Timeout und ordnungsgemäßer Option:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
disable service <name> [<delay>] [-graceFul (YES|NO)]

show service <name>
<!--NeedCopy-->
```

Beispiel

```
disable service svc1 2000 -graceFul YES

Done
> sh service svc1
                svc1 (10.102.225.11:80) - HTTP
                State: GOING OUT OF SERVICE (Graceful (number of active
                    clients: 1), Out Of Service in 1998 seconds)
                Last state change was at Wed Jul 25 10:49:08 2018
                Time since last state change: 0 days, 00:00:01.710
                ……..
                ……..
                Traffic Domain: 0

1)            Monitor Name: tcp-default
                                State: UP              Weight: 1
                                                Passive: 0
                                Probes: 57            Failed [Total: 0
                                    Current: 0]
                                Last response: Success - TCP syn+ack
                                    received.
                                Response Time: 0.0 millisec
Done
<!--NeedCopy-->
```

Dienstgruppe mit Timeout und ordnungsgemäßer Option deaktivieren:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
disable serviceGroup <serviceGroupName>@ [<serverName>@ <port>] [-delay
<secs>] [-graceFul ( YES | NO )]
Show service group <serviceGroupName>
```



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

Beispiel:

```
disable servicegroup sg -delay 2000 -graceFul yes
sh servicegroup sg
                sg - HTTP
                State: DISABLED                Effective State: OUT OF
                   SERVICE Monitor Threshold : 0
                Max Conn: 0       Max Req: 0          Max Bandwidth: 0
                   kbits
                Use Source IP: NO
                Client Keepalive(CKA): NO
                ... ... ... .
                ... ... ...



                1)   200.200.10.21:80       Server Name: server3
                   Server ID: None Weight: 1
                                State:    GOING OUT OF SERVICE (learnt
                                   from node:2 )     Graceful (number
                                   of active clients: 6), Out Of
                                   Service in 1993 seconds
                                Last state change was at Mon Aug 13
                                   15:15:11 2018
                                ... ... ...

                2)   200.200.10.22:80       Server Name: server4
                   Server ID: None Weight: 1
                                State:    GOING OUT OF SERVICE (learnt
                                   from node:2 )     Graceful (number
                                   of active clients: 7), Out Of
                                   Service in 1993 seconds
                                Last state change was at Mon Aug 13
                                   15:15:11 2018
<!--NeedCopy-->
```

> **Hinweis**
> CLIP zeigt den aggregierten Wert aller aktiven Clientverbindungen von allen Cluster-Knoten an.

So konfigurieren Sie ein ordnungsgemäßes Herunterfahren für einen Dienst mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Öffnen Sie den Dienst, und klicken Sie in der Liste Aktion auf **Deaktivieren**. Geben Sie eine Wartezeit ein und wählen Sie Graceful aus.

So konfigurieren Sie einen TROFS-Code oder eine Zeichenfolge in einem Monitor mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
add lb monitor <monitor-name> HTTP -trofsCode <respcode>
add lb monitor <monitor-name> HTTP-ECV  -trofsString <resp string>
add lb monitor <monitor-name> TCP-ECV  -trofsString <resp string>
<!--NeedCopy-->
```

So konfigurieren Sie einen TROFS-Code oder eine Zeichenfolge in einem Monitor mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Klicken Sie im Bereich Monitore auf Hinzufügen, und führen Sie einen der folgenden Schritte aus:
   - Wählen Sie Typ als HTTP aus, und geben Sie einen TROFS-Code an.
   - Wählen Sie Typ als HTTP-ECV oder TCP-ECV aus, und geben Sie einen TROFS-String an.

IPv6-fähige Logo-Unterstützung für Cluster

October 5, 2021

Sie können Cluster-Appliances für die IPv6-Ready-Logo-Zertifizierung testen. Modifizierte Befehle zum Testen von IPv6-Kernprotokollen, z. B. für ND-Testfälle, Routeranforderungsverarbeitung und das Senden von Routenankündigungs- und Routerumleitungsnachrichten stehen in einem Cluster-Setup zur Verfügung. Im Folgenden sind die IPv6-Funktionalitäten zum Testen der IPv6-Kernprotokolle verfügbar.

Im Folgenden finden Sie die geänderten Funktionalitäten, die verfügbar sind, um IPv6-Core-Protokolle zu bestehen, wie ND-Testfälle, Router Solicitation-Verarbeitung und das Senden von Route-Werbung und Router-Umleitungsnachrichten in der Phase2-Testsuite IPv6ReadyLogo.

- Lokale SNIPs verknüpfen
- Adressenauflösung und Neighbor Unerreichbarkeit
- Router- und Präfixerkennung
- Routerumleitung
- DoDAD

Mit diesen geänderten Befehlen werden die folgenden Konfigurationen in einer Cluster-Appliance unterstützt.

Unterstützbare Konfigurationen zum Testen von IPv6-Kernprotokollen

Damit ein Cluster-Setup IPv6 Ready Logo-Testfälle bestehen kann, können Sie die folgenden Konfigurationen für die Cluster Management-IP-Adresse (CLIP) ausführen.

- global IP6 configuration
- basic IPv6 configuration
- weitere IPv6-Konfigurationen

Globale Konfiguration

Eine globale IPv6-Konfiguration ermöglicht es Ihnen, die globalen IPv6-Parameter (wie Relearning, RoutereDirection, NdBaseReachTime, NreTransLissionTime `natprefix`, td und doodad) so einzustellen, dass die grundlegende IPv6-Konfiguration ausgeführt wird.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ipv6 [-ralearning ( ENABLED | DISABLED )] [-routerRedirection (
    ENABLED | DISABLED )] [-ndBasereachTime<positive_integer>][-
    ndRetransmissionTime <positive_integer>] [-natprefix <ipv6_addr|*>[-
    td<positive_integer>]] [-doDAD ( ENABLED | DISABLED )]
```

Grundlegende IPv6-Konfiguration

Die grundlegende IPv6-Konfiguration ermöglicht es Ihnen, eine IPv6-Adresse zu erstellen und an eine VLAN-Schnittstelle zu binden. Sie können die folgenden Konfigurationen durchführen, um die IPv6-Core-Protokolle zu testen.

So fügen Sie dem Cluster-Setup über die Befehlszeilenschnittstelle ein VLAN hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add vlan <id>
```

So fügen Sie dem Cluster-Setup mit der CLI ein weiteres VLAN hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add vlan <id>
```

So binden Sie eine Schnittstelle mit der CLI an ein VLAN

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind vlan <id> -ifnum <interface_name>
```

So binden Sie eine Schnittstelle mit der CLI an ein VLAN

Mit diesem Befehl wird das globale Präfix als On-Link-Präfix in RA-Informationen für nachfolgende Router-Advertisements hinzugefügt. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind vlan <id> -ifnum <interface_name>
```

So fügen Sie die IPv6-SNIP-Adresse in einem VLAN mit der CLI hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns ip6 <IPv6Address>@ [-scope ( global | link-local )][-type <type>
```

So fügen Sie die IPv6-Adresse im VLAN mit der CLI hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns ip6 <IPv6Address>@ [-scope ( global | link-local )][-type <type>
```

So binden Sie die IPv6-Adresse mit der CLI an VLAN

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
bind vlan <id> [-ifnum <interface_name> [-tagged]][-IPAddress <ip_addr|
    ipv6_addr|
```

So binden Sie die IPv6-Adresse mit der CLI an VLAN

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind vlan <id> [-ifnum <interface_name> [-tagged]][-IPAddress <ip_addr|
    ipv6_addr|
```

So zeigen Sie die lokale IPv6-Adresse des Links an, die mit dem VLAN mit der CLI verbunden ist

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
sh VLAN
```

Beispiel 1

```
add vlan 2
add vlan 3
bind vlan 2 -ifnum 1/2
bind vlan 3 -ifnum 1/3
add ip6 fe80::9404:60ff:fedd:a464/64 -vlan 2 -scope link-local -type
    SNIP
add ip6 fe80::c0ee:7bff:fede:263f/64 -vlan 3 -scope link-local -type
    SNIP
add ip6 3ffe:501:ffff:100:9404:60ff:fedd:a464/64 -vlan 2
add ip6 3ffe:501:ffff:101:c0ee:7bff:fede:263f/64 -vlan 3
bind vlan 2 -ipAddress 3ffe:501:ffff:100:9404:60ff:fedd:a464/64
bind vlan 3 -ipAddress 3ffe:501:ffff:101:c0ee:7bff:fede:263f/64
```

Beispiel 2

```
sh vlan
1)      VLAN ID: 2      VLAN Alias Name:
        Interfaces : 1/6
        IPs :
             3ffe:501:ffff:100:2e0:edff:fe15:ea2a/64
3)      VLAN ID: 3      VLAN Alias Name:
```



```
7          Link-local IPv6 addr: fe80::9404:60ff:fedd:a464/64
8          Interfaces : 1/5
9          IPs :
10              3ffe:501:ffff:101:2e0:edff:fe15:ea2b/64
11   Done
```

Mehr IPv6-Cluster-Konfiguration

Zum Testen von IPv6-Kernprotokollen können Sie die folgenden neuen oder geänderten IPv6-Konfigurationen verwenden.

So legen Sie VLAN-spezifische Router Advertisement-Parameter mit der CLI fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set nd6RAvariables -vlan <positive_integer> [-ceaseRouterAdv ( YES | NO
      )] [-sendRouterAdv ( YES | NO )] [-srcLinkLayerAddrOption ( YES | NO
       )][-onlyUnicastRtAdvResponse ( YES | NO )] [-managedAddrConfig (
      YES | NO)] [-otherAddrConfig ( YES | NO )] [-currHopLimit <
      positive_integer>][-maxRtAdvInterval <positive_integer>] [-
      minRtAdvInterval<positive_integer>] [-linkMTU <positive_integer>] [-
      reachableTime<positive_integer>] [-retransTime <positive_integer>]
      [-defaultLifeTime<integer>]
```

So legen Sie die konfigurierbaren Parameter eines globalen On-Link-Präfixes über die Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set onLinkIPv6Prefix <ipv6Prefix> [-onlinkPrefix ( YES | NO )][-
      autonomusPrefix ( YES | NO )] [-depricatePrefix ( YES | NO )][-
      decrementPrefixLifeTimes ( YES | NO )] [-prefixValideLifeTime   <
      positive_integer>] [-prefixPreferredLifeTime <positive_integer>]
```

So fügen Sie einem globalen On-Link-Präfix mit der CLI konfigurierbare Parameter hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add onLinkIPv6Prefix <ipv6Prefix> [-onlinkPrefix ( YES | NO )][-
      autonomusPrefix ( YES | NO )] [-depricatePrefix ( YES | NO )][-
      decrementPrefixLifeTimes ( YES | NO )]-prefixValideLifeTime <
      positive_integer>][-prefixPreferredLifeTime <positive_integer>]
```


So richten Sie einen On-Link zu den konfigurierbaren Parametern des IPv6-Präfixes mit der CLI ein

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
help set onLinkIPv6Prefix
```

So binden Sie einen On-Link mit den konfigurierbaren Parametern des IPv6-Präfixes mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
help bind nd6RAvariables
```

So zeigen Sie Nd6raVariables mit der CLI an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
help sh nd6RAvariables
```

Beispiel

```
> sh nd6RAvariables
  1) Vlan : 1
     SendAdvert      : NO   CeaseAdv       : NO        SourceLLAddress:
        YES
     UnicastOnly     : NO   ManagedFlag    : NO        OtherConfigFlag:
        NO
     CurHopLimit     : 64   MaxRtrAdvInterv: 600       MinRtrAdvInterv:
        198
     LinkMTU         : 0    ReachableTime  : 0          RetransTimer   :
         0
     DefaultLifetime: 1800 LastRAsentTime : 0          NextRAdelay    :
         0

  2) Vlan : 2
     SendAdvert      : NO   CeaseAdv       : NO         SourceLLAddress:
         YES
     UnicastOnly     : NO   ManagedFlag    : NO         OtherConfigFlag:
         NO
     CurHopLimit     : 64   MaxRtrAdvInterv: 600        MinRtrAdvInterv:
         198
```



```
13      LinkMTU         : 0    ReachableTime   : 0          RetransTimer    :
            0
14      DefaultLifetime: 1800 LastRAsentTime : 0          NextRAdelay     :
            0
15  Done
16  >
17  > sh nd6Ravariables  -vlan 2
18    1) Vlan : 2
19      SendAdvert      : NO   CeaseAdv       : NO         SourceLLAddress:
            YES
20      UnicastOnly     : NO   ManagedFlag    : NO         OtherConfigFlag:
            NO
21      CurHopLimit     : 64   MaxRtrAdvInterv: 600        MinRtrAdvInterv:
            198
22      LinkMTU         : 0    ReachableTime   : 0          RetransTimer    :
            0
23      DefaultLifetime: 1800 LastRAsentTime : 0          NextRAdelay     :
            0
24      Prefix :
25  3ffe:501:ffff:100::/64
26  Done
```

Verwalten von Cluster-Heartbeat-Meldungen

October 5, 2021

Das Verwalten von Heartbeat-Nachrichten in einem Cluster ähnelt der Verwaltung dieser Nachrichten in einer Hochverfügbarkeitskonfiguration. Knoten können Heartbeat-Nachrichten an und voneinander auf allen aktivierten Schnittstellen senden und empfangen. Um erhöhten Datenverkehr zu vermeiden, der aus Heartbeat-Nachrichten resultiert, können Sie jetzt die Heartbeat-Option auf Knotenschnittstellen deaktivieren. Die Heartbeat-Option auf der Backplane-Schnittstelle kann jedoch nicht deaktiviert werden, da sie für die Aufrechterhaltung der Konnektivität zwischen den Clusterknoten erforderlich ist.

Weitere Informationen zum Verwalten von Herzmeldungen finden Sie unter Verwalten von Heartbeat-Nachrichten für hohe Verfügbarkeit auf einer NetScaler Appliance.

So verwalten Sie Heartbeat-Meldungen auf einer Knotenschnittstelle mit der Citrix ADC CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set interface <ID> [-HAHeartBeat (ON | OFF)]
Show interface <ID>
```

Antwortstatus des Besitzerknotens konfigurieren

October 5, 2021

Sie können die Option OwnerDownResponse auf einem Knoten konfigurieren, der über eine gepunktete SNIP-Adresse verfügt. Standardmäßig ist die Option aktiviert. Dadurch kann die gepunktete IP-Adresse auf PING- oder ARP-Anfragen (vom Upstream-Router) reagieren, wenn der Knoten inaktiv ist. Wenn Sie die Option deaktivieren, kann die IP-Adresse nicht auf die Router-Anforderungen reagieren, wenn der Besitzer-Knoten inaktiv ist.

Um zu erfahren, wie diese Funktion zur Überwachung statischer Routen in der ECMP-Bereitstellung verwendet wird, finden Sie unter Verwenden von Equal Cost Multiple Path (ECMP) .

So legen Sie den Antwortstatus des Besitzerknotens mit der Citrix ADC CLI fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns ip <IPAddress> [-ownerNode <positive_integer>] [-
    ownerDownResponse (YES | NO )] [-td <positive_integer>]
```

Beispiel

```
add ns ip 2.2.2.2 255.255.255.0 -ownernode 6  - ownerdownResponse YES
```

So legen Sie den Antwortstatus des Besitzerknotens über die Citrix ADC GUI fest

1. Navigieren Sie zu **System > Netzwerk > IPs**, und klicken Sie auf **Hinzufügen**, um eine gespotted SNIP-Adresse zu erstellen.
2. Aktivieren oder deaktivieren Sie auf der Seite “ **IP-Adresse erstellen** “ das Kontrollkästchen **OwnerDownResponse**.

So bearbeiten Sie den Antwortstatus des Besitzerknotens über die Citrix ADC GUI

Navigieren Sie zu **System > Netzwerk > IPs**, wählen Sie eine IP-Adresse aus, und klicken Sie auf **Bearbeiten**, um das Kontrollkästchen **OwnerDownResponse**zu aktivieren oder zu deaktivieren.

Überwachung der Unterstützung für statische Routen (MSR) für inaktive Knoten in einer Spotted Cluster-Konfiguration

October 5, 2021

In einem Cluster, der mit der MSR-Option auf der Route aktiviert ist, können nur aktive Knoten auf eine statische Route untersuchen. Es kann ein Netzwerk erreichen, während inaktive und Reserveknoten keine Verbindung zur Route haben und nicht mit ihr nachforschen können. Sie können jetzt einen inaktiven oder Ersatzknoten konfigurieren, um PING und ARP Probe an IPv4-Route zu senden und ping6 und nd6 Probe an IPv6-Route zu senden. Sie können dies nur in einer Spotted Cluster-Konfiguration durchführen, in der die SNIP-Adresse aktiv ist und ausschließlich einem Knoten gehört.

VRRP-Schnittstellenbindung in einem aktiven Cluster mit einem einzelnen Knoten

October 5, 2021

Wenn Sie ein Hochverfügbarkeitssetup zu einem Cluster-Setup migrieren, müssen alle Konfigurationen kompatibel sein und im Cluster unterstützt werden. Um dies zu erreichen, können Sie jetzt virtuelle Router-IDs (VRIDs und VRID6s) auf einer Knotenschnittstelle konfigurieren.

> **Wichtig**
>
> Derzeit unterstützt nur ein aktives Clustersystem mit einem Knoten VRIDs und VRID6s.

Anweisungen zum Konfigurieren von VRIDs und vRID6s finden Sie unter Konfigurieren von Virtual MAC-Adressen.

Um eine virtuelle Router-ID auf einem aktiven Cluster mit einem Knoten zu konfigurieren, fügen Sie die VRID oder VRID6 hinzu und binden Sie sie an die Cluster-Knoten-Schnittstelle.

So fügen Sie eine VRID mit der Citrix ADC CLI hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add vrID <ID>
```

So binden Sie eine VRID mit der Citrix ADC CLI an die Cluster-Knoten-Schnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
Bind vrid <ID> -ifnum <interface_name> | -trackifNum <interface_name

Add vrID 100
Bind vrid 100  - ifnum 1/1  1/2
done
```

So fügen Sie einen VRID6 mit der Citrix ADC CLI hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add vrID6 <ID>
```

So binden Sie einen VRID6 mit der CLI an eine Clusterknotenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind vrid6 <ID> -ifnum <interface_name> | -trackifNum <interface_name>

Add vrID6 100
Bind vrid6 100  - ifnum 1/1  1/2
Done
```

Cluster-Setup und -verwendungsszenarien

October 5, 2021

In diesem Abschnitt werden einige Szenarien erläutert, in denen der Citrix ADC Cluster eingerichtet und für verschiedene Features und Netzwerktopologien konfiguriert werden kann. Geben Sie Feedback, wenn Sie andere Szenarien dokumentieren möchten.

Erstellen eines Clusters mit zwei Knoten

October 5, 2021

Ein Cluster mit zwei Knoten stellt eine Ausnahme von der Regel dar, dass ein Cluster nur dann funktionsfähig ist, wenn mindestens (n/2 +1) Knoten, wobei n die Anzahl der Clusterknoten ist, in der Lage sind, Datenverkehr zu bedienen. Wenn dieselbe Formel auf einen Zwei-Knoten-Cluster angewendet wird, würde der Cluster fehlschlagen, wenn ein Knoten ausfällt (n/2 +1=2).

Ein Cluster mit zwei Knoten ist auch dann funktionsfähig, wenn nur ein Knoten den Datenverkehr bedienen kann.

Das Erstellen eines Clusters mit zwei Knoten entspricht dem Erstellen eines anderen Clusters. Sie fügen einen einen Knoten als Konfigurationskoordinator und den anderen Knoten als den anderen Clusterknoten hinzu.

> **Hinweis:**
>
> Die inkrementelle Konfigurationssynchronisierung wird in einem Cluster mit zwei Knoten nicht unterstützt. Es wird nur eine vollständige Synchronisation unterstützt.

Migrieren eines HA-Setups zu einem Cluster-Setup

December 7, 2021

Wenn Sie ein vorhandenes Hochverfügbarkeit-Setup zu einem Cluster-Setup migrieren, müssen Sie zuerst die Citrix ADC Appliances aus dem HA-Setup entfernen und eine Sicherung der HA-Konfigurationsdatei erstellen. Sie können dann die beiden Appliances verwenden, um einen Cluster zu erstellen und die gesicherten Konfigurationsdatei in den Cluster hochzuladen.

> **Hinweis:**
>
> - Bevor Sie die gesicherte HA-Konfigurationsdatei in den Cluster hochladen, müssen Sie sie so ändern, dass sie Clusterkompatibel ist. Beziehen Sie sich auf den relevanten Schritt des Verfahrens.
> - Verwenden Sie den Befehl <backup_filename> batch -f, um die gesicherte Konfigurationsdatei hochzuladen.

Der vorhergehende Ansatz ist eine grundlegende Migrationslösung, die zu Ausfallzeiten für die bereitgestellte Anwendung führt. Daher darf es nur in Bereitstellungen verwendet werden, bei denen die Anwendungsverfügbarkeit nicht berücksichtigt wird.

In den meisten Bereitstellungen ist jedoch die Verfügbarkeit der Anwendung von größter Bedeutung. In solchen Fällen müssen Sie den Ansatz verwenden, bei dem ein HA-Setup ohne daraus resultierende

Ausfallzeiten zu einem Cluster-Setup migriert werden kann. Bei diesem Ansatz wird ein vorhandenes HA-Setup zu einem Cluster-Setup migriert, indem zunächst die sekundäre Appliance entfernt und diese Appliance zum Erstellen eines Clusters mit einem Knoten verwendet wird. Nachdem der Cluster betriebsbereit ist und Datenverkehr bedient wird, wird die primäre Appliance des HA-Setups dem Cluster hinzugefügt.

So konvertieren Sie ein HA-Setup in Cluster-Setup (ohne Ausfallzeiten) mit der Befehlszeilenschnittstelle

Betrachten wir das Beispiel eines HA-Setup mit primärer Appliance (NS1) - 10.102.97.131 und sekundäre Appliance (NS2) - 10.102.97.132.

1. Stellen Sie sicher, dass die Konfigurationen des HA-Paares stabil sind.
2. Melden Sie sich bei einer der HA-Appliances an, wechseln Sie zur Shell und erstellen Sie eine Kopie der Datei ns.conf (z. B. ns_backup.conf).
3. Melden Sie sich bei der sekundären Appliance NS2 an, und löschen Sie die Konfigurationen. Dieser Vorgang entfernt NS2 aus dem HA-Setup und macht es zu einer eigenständigen Appliance.

```
> clear ns config full
```

> **Hinweis:**
>
> - Dieser Schritt ist erforderlich, um sicherzustellen, dass NS2 keine VIP-Adressen besitzt, da es sich nun um eine eigenständige Appliance handelt.
> - In diesem Stadium ist die primäre Appliance NS1 weiterhin aktiv und dient weiterhin dem Datenverkehr.

4. Erstellen Sie einen Cluster auf NS2 (jetzt keine sekundäre Appliance mehr), und konfigurieren Sie ihn als PASSIVE-Knoten.

```
> add cluster instance 1

> add cluster node 0 10.102.97.132 -state PASSIVE -backplane
   0/1/1

> add ns ip 10.102.97.133 255.255.255.255 -type CLIP

> enable cluster instance 1

```



```
> save ns config

> reboot -warm
```

5. Ändern Sie die gesicherte Konfigurationsdatei wie folgt:

   - Entfernen Sie die Features, die in einem Cluster nicht unterstützt werden. Eine Liste der nicht unterstützten Funktionen finden Sie unter Citrix ADC Features, die von einem Cluster unterstützt werden. Dies ist ein optionaler Schritt. Wenn Sie diesen Schritt nicht ausführen, schlägt die Ausführung von nicht unterstützten Befehlen fehl.
   - Entfernen Sie die Konfigurationen, die Schnittstellen haben, oder aktualisieren Sie die Schnittstellennamen von der c/u-Konvention auf die n/c/u-Konvention.

     Beispiel

     ```
     > add vlan 10 -ifnum 0/1
     ```

     muss geändert werden in

     ```
     > add vlan 10 -ifnum 0/0/1 1/0/1
     ```

   - Die Sicherungskonfigurationsdatei kann SNIP-Adressen haben. Diese Adressen werden auf allen Clusterknoten gestreift. Es wird empfohlen, dass Sie für jeden Knoten gespottete IP-Adressen hinzufügen.

     Beispiel

     ```
     > add ns ip 1.1.1.1 255.255.255.0 -ownerNode 0

     > add ns ip 1.1.1.2 255.255.255.0 -ownerNode 1
     ```

   - Aktualisieren Sie den Hostnamen, um den Besitzerknoten anzugeben.

     Beispiel

     ```
     > set ns hostname ns0 -ownerNode 0

     > set ns hostname ns1 -ownerNode 1
     ```


- Ändern Sie alle anderen relevanten Netzwerkkonfigurationen, die von gefleckten IPs abhängen. Zum Beispiel, L3 VLAN, RNAT Konfiguration, die SNIPs als NATIP verwendet, INAT Regeln, die sich auf SNIPs/MIPs bezieht).

6. Führen Sie auf dem Cluster die folgenden Schritte aus:

   - Nehmen Sie die topologischen Änderungen am Cluster vor, indem Sie die Clusterrückwandplatine, den Clusterverknüpfungsaggregationskanal usw. verbinden.
   - Wenden Sie Konfigurationen aus der gesicherten und geänderten Konfigurationsdatei über die Cluster-IP-Adresse auf den Konfigurationskoordinator an.

     ```
     1  > batch -f ns_backup.conf
     ```

   - Konfigurieren Sie externe Verkehrsverteilungsmechanismen wie ECMP oder Cluster-Link-Aggregation.

7. Wechseln Sie den Datenverkehr vom HA-Setup zum Cluster.

   - Melden Sie sich bei der primären Appliance NS1 an, und deaktivieren Sie alle Schnittstellen darauf.

     ```
     1  > disable interface <interface_id>
     ```

   - Melden Sie sich bei der Cluster-IP-Adresse an, und konfigurieren Sie NS2 als ACTIVE-Knoten.

     ```
     1  > set cluster node 0 -state ACTIVE
     ```

   > **Hinweis:**
   >
   > Zwischen dem Deaktivieren der Schnittstellen und der Aktivierung des Clusterknotens kann es zu einer geringen Anzahl (in der Reihenfolge von Sekunden) kommen.

8. Melden Sie sich bei der primären Appliance NS1 an, und entfernen Sie sie aus dem HA-Setup.

   - Löschen Sie alle Konfigurationen. Dieser Vorgang entfernt NS1 aus dem HA-Setup und macht es zu einer eigenständigen Appliance.

     ```
     1  > clear ns config full
     ```


- Aktivieren Sie alle Schnittstellen.

```
> enable interface <interface_id>
```

9. Fügen Sie NS1 zum Cluster hinzu.
   - Melden Sie sich bei der Cluster-IP-Adresse an, und fügen Sie NS1 zum Cluster hinzu.

```
> add cluster node 1 10.102.97.131 -state PASSIVE -backplane
   1/1/1
```

   - Melden Sie sich bei NS1 an und verbinden Sie es mit dem Cluster, indem Sie die folgenden Befehle sequenziell ausführen:

```
> join cluster -clip 10.102.97.133 -password nsroot

> save ns config

> reboot -warm
```

10. Melden Sie sich bei NS1 an, und führen Sie die erforderlichen topologischen und Konfigurationsänderungen durch.
11. Melden Sie sich bei der Cluster-IP-Adresse an, und legen Sie NS1 als ACTIVE-Knoten fest.

```
    > set cluster node 1 -state ACTIVE
```

Übergang zwischen einem L2- und L3-Cluster

October 5, 2021

> **Hinweis:**
>
> Unterstützt ab NetScaler 11.

Ein L2-Cluster ist einer, bei dem alle Knoten aus demselben Netzwerk stammen und ein L3-Cluster ist einer, der Knoten aus verschiedenen Netzwerken enthalten kann. Sie können nahtlos von einem Clustertyp zum anderen wechseln, ohne Ausfallzeiten für die Anwendungen, die auf dem Citrix ADC bereitgestellt werden.

Übergang eines Clusters von L2 zu L3

Sie können zu einem L3-Cluster wechseln, wenn der Cluster Knoten aus anderen Netzwerken enthalten soll.

Gehen Sie auf der Cluster-IP-Adresse folgendermaßen vor:

1. Erstellen Sie eine Knotengruppe.

   Beispiel

   ```
   1 > add cluster nodegroup NG0
   ```

   Diese Knotengruppe wird im nächsten Schritt verwendet, um alle Knoten aus dem bestehenden L2-Cluster zu gruppieren.

2. Übergang des L2-Clusters zu einem L3-Cluster.

   Beispiel

   ```
   1 > set cluster instance 1 -inc ENABLED -nodegroup NG0
   ```

   Dieser Befehl erreicht den doppelten Zweck der Umstellung auf den L3-Cluster und das Hinzufügen aller Knoten des L2-Clusters zur Knotengruppe.

3. Jetzt können Sie dem Cluster weitere Knoten hinzufügen, wie unter Hinzufügen eines Knotens zum Clusterbeschrieben.

Übergang eines Clusters von L3 zu L2

Sie können zu einem L2-Cluster wechseln, wenn Sie Knoten beibehalten möchten, die zu einem einzelnen Netzwerk gehören.

Gehen Sie auf der Cluster-IP-Adresse folgendermaßen vor:

1. Entfernen Sie die Clusterknoten aus den Netzwerken, die Sie nicht beibehalten möchten.

   Beispiel

   ```
   1 > rm cluster node <nodeId>
   ```

2. Übergang des L3-Clusters zu einem L2-Cluster.

   Beispiel


```
1 > set cluster instance 1 -inc DISABLED
```

Der Cluster enthält jetzt nur Knoten eines einzelnen Netzwerks.

Einrichten von GSLB in einem Cluster

October 5, 2021

> **Hinweis:**
>
> Unterstützt ab NetScaler 10.5 Build 52.11.

Um GSLB in einem Cluster einzurichten, müssen Sie die verschiedenen GSLB-Entitäten an eine Knotengruppe binden. Die Knotengruppe muss über einen einzelnen Mitgliedsknoten verfügen.

> **Hinweise**
>
> - Wenn Sie die statische Proximity-GSLB-Methode konfiguriert haben, stellen Sie sicher, dass die statische Proximity-Datenbank auf allen Cluster-Knoten vorhanden ist. Dies geschieht standardmäßig, wenn die Datenbankdatei am Standardspeicherort verfügbar ist. Wenn die Datenbankdatei jedoch in einem anderen Verzeichnis als /var/netscaler/locdb/ gespeichert wird, müssen Sie die Datei manuell mit allen Cluster-Knoten synchronisieren.
> - Der `show gslb domain` Befehl wird in einem Cluster-Setup nicht unterstützt.

So richten Sie GSLB in einem Cluster mit der CLI ein:

Melden Sie sich bei der Cluster-IP-Adresse an, und führen Sie die folgenden Vorgänge an der Eingabeaufforderung aus:

1. Konfigurieren Sie die verschiedenen GSLB-Entitäten. Weitere Informationen finden Sie unter GSLB-Konfigurations-Entitäten.

   > **Hinweis:**
   >
   > Stellen Sie beim Erstellen der GSLB-Site sicher, dass Sie die Cluster-IP-Adresse und die IP-Adresse des öffentlichen Clusters angeben. Die IP-Adresse des öffentlichen Clusters wird nur benötigt, wenn der Cluster hinter einem NAT-Gerät bereitgestellt wird. Beim Konfigurieren einer GSLB-Site müssen Sie die Cluster-IP-Adresse desselben Standorts verwenden. Diese Parameter sind erforderlich, um die Verfügbarkeit der GSLB-Auto-Synchronisierungsfunktion zu gewährleisten.

   ```
   add gslb site <siteName> <siteType> <siteIPAddress> -publicIP <ip_addr>
    -clip <ip_addr> <publicCLIP><!--NeedCopy-->
   ```


2. Erstellen Sie eine Cluster-Knotengruppe.

   ```
   add cluster nodegroup <name> <name>@ [-strict ( YES | NO )] [-sticky (
   YES | NO )] [-state <state>] [-priority <positive_integer>]<!--NeedCopy
   -->
   ```

   > **Hinweis:**
   >
   > Aktivieren Sie die Sticky-Option, wenn Sie GSLB-basiert für VPN-Benutzer einrichten möchten.

3. Binden Sie einen einzelnen Clusterknoten an die Knotengruppe.

   ```
   bind cluster nodegroup <name> -node <nodeId><!--NeedCopy-->
   ```

4. Binden Sie die lokale GSLB-Site an die Knotengruppe.

   ```
   bind cluster nodegroup <name> -gslbSite <string><!--NeedCopy-->
   ```

   > **Hinweis:**
   >
   > Stellen Sie sicher, dass die IP-Adresse der lokalen GSLB-Site-IP-Adresse gestreift ist (verfügbar über alle Clusterknoten).

5. Binden Sie den ADNS- (oder ADNS-TCP-Dienst) oder den DNS- (oder DNS-TCP) Lastausgleichsserver an die Knotengruppe.

   So binden Sie den ADNS-Dienst:

   “‘bind cluster nodegroup -service

   ```
   **So binden Sie den virtuellen DNS-Lastausgleichsserver:**

   ```bind cluster nodegroup <name> -vServer <string><!--NeedCopy-->
   ```

6. Binden Sie den virtuellen GSLB-Server an die Knotengruppe.

   ```
   bind cluster nodegroup <name> -vServer <string><!--NeedCopy-->
   ```

7. [Optional] Um GSLB basierend auf VPN-Benutzern einzurichten, binden Sie den virtuellen VPN-Server an die GSLB-Knotengruppe.

   ```
   bind cluster nodegroup <name> -vServer <string><!--NeedCopy-->
   ```

8. Überprüfen Sie die Konfigurationen.

   ```
   show gslb runningConfig<!--NeedCopy-->
   ```

So richten Sie GSLB in einem Cluster mit der GUI ein:

Melden Sie sich bei der Cluster-IP-Adresse an, und führen Sie die folgenden Vorgänge auf der Registerkarte Konfiguration aus:


   ```

1. Konfigurieren Sie die GSLB-Entitäten.

   Navigieren Sie zu **Traffic Management > GSLB**, um die erforderlichen Konfigurationen durchzuführen.

2. Erstellen Sie eine Knotengruppe und führen Sie andere Knotengruppen-bezogene Konfigurationen durch.

   Navigieren Sie zu **System > Cluster > Knotengruppen**, um die erforderlichen Konfigurationen durchzuführen.

Die detaillierten Konfigurationen finden Sie in der Beschreibung des vorherigen CLI-Verfahrens.

## Unterstützung für GSLB-Topologie für übergeordnete und untergeordnete GSLB-Topologie in einem Cluster

Beginnend mit NetScaler 12.1 Build 49.xx wird GSLB Parent-Child-Topologie im Cluster unterstützt.

Weitere Informationen zur Eltern-Kind-Topologie finden Sie unter Bereitstellung von Eltern-Kind-Topologie unter Verwendung des MEP-Protokolls.

### So richten Sie die übergeordnete und untergeordnete GSLB-Topologie in einem Cluster mit der Befehlszeilenschnittstelle ein

#### Übergeordnete Site

Führen Sie die folgende Konfiguration durch:

1. Erstellen Sie eine Cluster-Knotengruppe.

   ```
   add cluster nodegroup <name>
   ```

   Beispiel:

   ```
   add cluster nodegroup parentng
   ```

2. Binden Sie einen einzelnen Clusterknoten an die Knotengruppe.

   ```
   bind cluster nodegroup <name> -node <nodeId>
   ```

   Beispiel:

   ```
   bind cluster nodegroup parentng -node n2
   ```

3. Binden Sie die lokale GSLB-Site an die Knotengruppe.

   ```
   bind cluster nodegroup <name> -gslbSite <string>
   ```

   Beispiel:

   ```
   bind cluster nodegroup parentng -gslbSite site1
   ```


4. Binden Sie den ADNS- (oder ADNS-TCP-Dienst) oder den DNS- (oder DNS-TCP) Lastausgleichsserver an die Knotengruppe.

   ```
   bind cluster nodegroup <name> -service <string>
   ```

   Beispiel:

   ```
   bind cluster nodegroup parentng - service ADNS
   ```

5. Binden Sie den virtuellen GSLB-Server an die Knotengruppe.

   ```
   bind cluster nodegroup <name> -vServer <string>
   ```

   Beispiel:

   ```
   bind cluster nodegroup parentng -vServce gslbvs1
   ```

Untergeordnete Site

Führen Sie die folgende Konfiguration durch:

1. Erstellen Sie eine Cluster-Knotengruppe.

   ```
   add cluster nodegroup <name>
   ```

   Beispiel:

   ```
   add cluster nodegroup childng
   ```

2. Binden Sie einen einzelnen Clusterknoten an die Knotengruppe.

   ```
   bind cluster nodegroup <name> -node <nodeId>
   ```

   Beispiel:

   ```
   bind cluster nodegroup childng -node -n3
   ```

3. Binden Sie die lokale GSLB-Site an die Knotengruppe.

   ```
   bind cluster nodegroup <name> -gslbSite <string>
   ```

   Beispiel:

   ```
   bind cluster nodegroup childng -gslbSite site1
   ```

> **Hinweis:**
>
> Damit übergeordnete und untergeordnete Standorte aggregierte Statistiken in metrikbasierten Lastausgleichsmethoden austauschen können, müssen Sie lokale GSLB-Dienste auf dem untergeordneten Standort hinzufügen. Die metrikbasierten Load Balancing-Methoden sind die geringste Verbindung, die geringste Bandbreite und die geringsten Pakete.

So richten Sie die übergeordnete und untergeordnete GSLB-Topologie in einem Cluster mit der GUI ein

1. Konfigurieren Sie die GSLB-Entitäten.

   Navigieren Sie zu **Traffic Management** > **GSLB**, um die erforderlichen Konfigurationen durchzuführen.

2. Erstellen Sie eine Knotengruppe.

   Navigieren Sie zu **System** > **Cluster** > **Knotengruppen**, um die erforderlichen Konfigurationen durchzuführen.

3. Wählen Sie auf der Seite "Knotengruppe" die Knotengruppe aus, an die Sie einen Knoten binden möchten, klicken Sie auf **"Bearbeiten"**und führen Sie die folgenden Aufgaben aus. Sie können diese Aufgaben auch ausführen, wenn Sie eine Knotengruppe hinzufügen.

   - Binden Sie einen Knoten an die Knotengruppe.

     Klicken Sie in **Advance Settings**auf **Clusterknoten** und führen Sie die folgenden Aufgaben aus:

     - Klicken Sie im Abschnitt " **Clusterknoten** " auf **Kein Clusterknoten**.
     - Klicken **Sie in Clusterknoten**auswählen auf > und wählen Sie den Knoten aus, den Sie an die Knotengruppe binden möchten. Sie können auch einen Cluster-Knoten hinzufügen.

   - Binden Sie die lokale GSLB-Site an die Knotengruppe.

     Klicken Sie in Advance Settings auf GSLB-Sites, und führen Sie die folgenden Aufgaben aus:

     - Klicken Sie im Abschnitt **GSLB Sites** auf Keine GSLB-Site.
     - Klicken **Sie auf der GSLB-Site**auswählen auf > und wählen Sie die GSLB-Site aus, die Sie an die Knotengruppe binden möchten. Sie können auch eine GSLB-Site hinzufügen.

   - Binden Sie den virtuellen GSLB-Server an die Knotengruppe.

     Klicken Sie in **Advance Settings**auf **Virtual Servers** und führen Sie die folgende Aufgabe aus

     - Klicken Sie im Bereich " **Virtuelle Server** " auf +.
     - **Wählen Sie unter Choose Virtual Server**den Server aus, den Sie an die Knotengruppe binden möchten.

   - Binden Sie den ADNS- (oder ADNS-TCP-Dienst) oder den DNS- (oder DNS-TCP) Lastausgleichsserver an die Knotengruppe.

     Klicken Sie in **Advance Settings**auf **Services** und führen Sie die folgenden Aufgaben aus:

     - Klicken Sie im Abschnitt " **Dienste** " auf **Kein Dienst**.

- **Wählen Sie unter Dienst**auswählen den Dienst aus, den Sie an die Knotengruppe binden möchten. Sie können auch einen Dienst hinzufügen.

> **Hinweis:**
>
> Für untergeordnete Sites müssen Sie nur den Clusterknoten und den lokalen GSLB-Site an die Knotengruppe binden.

Verwenden der Cache-Umleitung in einem Cluster

October 5, 2021

Die Cache-Umleitung in einem Cluster funktioniert genauso wie bei einer eigenständigen Citrix ADC Appliance. Der einzige Unterschied besteht darin, dass die Konfigurationen für die Cluster-IP-Adresse durchgeführt werden. Weitere Informationen zur Cache-Umleitung finden Sie unter Cache-Umleitung.

Punkte, die bei der Verwendung der Cache-Umleitung im transparenten Modus auf einem Cluster zu beachten sind:

- Stellen Sie vor der Konfiguration der Cache-Umleitung sicher, dass alle Knoten mit dem externen Switch verbunden sind und dass Sie Linksets konfiguriert haben. Andernfalls werden Kundenanfragen gelöscht.
- Wenn der MAC-Modus auf einem virtuellen Lastausgleichsserver aktiviert ist, stellen Sie sicher, dass der MBF-Modus auf dem Cluster aktiviert ist, indem Sie den Befehl enable ns mode MBF verwenden. Andernfalls werden die Anforderungen direkt an den Ursprungsserver gesendet, anstatt an den Cacheserver gesendet zu werden.

Verwenden des L2-Modus in einem Cluster-Setup

October 5, 2021

> **Hinweis:**
>
> Unterstützt von NetScaler 10.5 und höher.

Um den L2-Modus in einem Cluster-Setup zu verwenden, müssen Sie Folgendes sicherstellen:

- Gefleckte IP-Adressen müssen bei Bedarf auf allen Knoten verfügbar sein.
- Linksets müssen verwendet werden, um mit dem externen Netzwerk zu kommunizieren.
- Asymmetrische Topologien oder asymmetrische Cluster-LA Gruppen werden nicht unterstützt.
- Cluster-LA-Gruppe wird empfohlen.

- Der Datenverkehr wird auf die Clusterknoten nur für Bereitstellungen verteilt, in denen Dienste vorhanden sind.

Verwenden des Cluster-LA Kanals mit Linksets

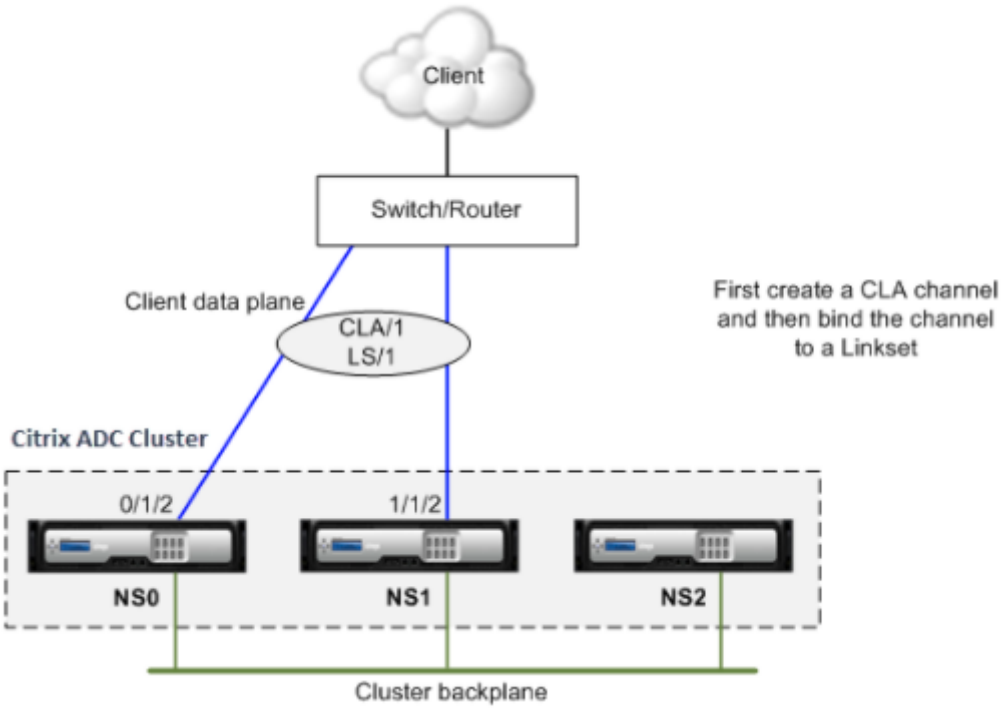
October 5, 2021

In einer asymmetrischen Cluster-Topologie sind einige Clusterknoten nicht mit dem Upstream-Netzwerk verbunden. In einem solchen Fall müssen Sie Linksets verwenden. Um die Leistung zu optimieren, können Sie die Schnittstellen, die mit dem Switch verbunden sind, als Cluster-LA-Kanal binden und dann den Kanal an einen Linkset binden.

Um zu verstehen, wie eine Kombination aus Cluster-LA-Kanal und Linksets verwendet werden kann, sollten Sie einen Cluster mit drei Knoten betrachten, für den der Upstream-Switch nur zwei Ports verfügbar ist. Sie können zwei Clusterknoten mit dem Switch verbinden und den anderen Knoten nicht verbunden lassen.

> **Hinweis:**
>
> In ähnlicher Weise können Sie auch eine Kombination aus ECMP und Linksets in einer asymmetrischen Topologie verwenden.

Abbildung 1. Linksets und Cluster-LA Kanaltopologie



So konfigurieren Sie Cluster LA-Channel und Linksets mit der CLI

1. Melden Sie sich bei der Cluster-IP-Adresse an.
2. Binden Sie die angeschlossenen Schnittstellen an einen Cluster-LA-Kanal.

```
add channel CLA/1 -ifnum 0/1/2 1/1/2
```

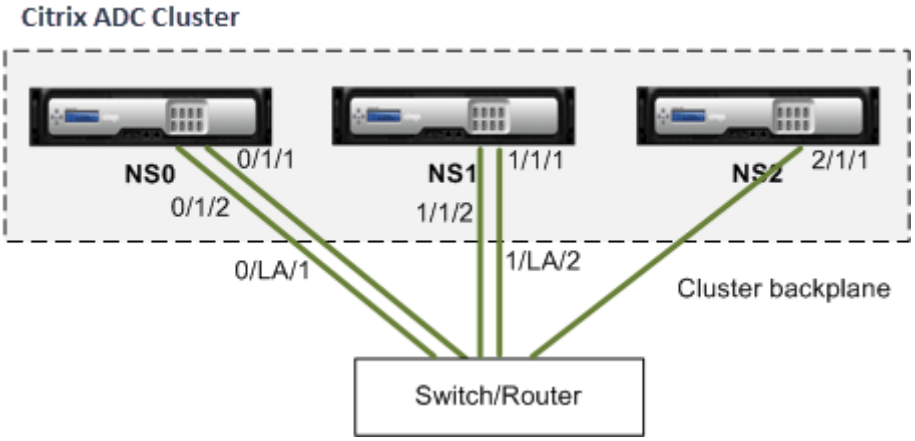
3. Binden Sie den Cluster LA-Kanal an den Linkset.

```
add linkset LS/1 -ifnum CLA/1
```

Rückwandplatine auf LA-Kanal

October 5, 2021

In dieser Bereitstellung werden LA-Kanäle für die Cluster-Rückwandplatine verwendet.



- NS0 - nodeId: 0, NSIP: 10.102.29.60
- NS1 - nodeId: 1, NSIP: 10.102.29.70
- NS2 - nodeId: 2, NSIP: 10.102.29.80

So stellen Sie einen Cluster mit den Backplane-Schnittstellen als LA-Kanäle bereit

1. Erstellen Sie einen Cluster von Knoten NS0, NS1 und NS2.

a) Melden Sie sich beim ersten Knoten an, den Sie dem Cluster hinzufügen möchten, und führen Sie folgende Schritte aus:

```
> create cluster instance 1
> add cluster node 0 10.102.29.60 -state ACTIVE
> enable cluster instance 1
> add ns ip 10.102.29.61 255.255.255.255 -type CLIP
> save ns config
> reboot -warm
```

b) Melden Sie sich bei der Cluster-IP-Adresse an, und führen Sie folgende Schritte aus:

```
> add cluster node 1 10.102.29.70 -state ACTIVE
> add cluster node 2 10.102.29.80 -state ACTIVE
```

c) Melden Sie sich bei den Knoten 10.102.29.70 und 10.102.29.80 an, um die Knoten mit dem Cluster zu verbinden.

```
> join cluster -clip 10.102.29.61 -password nsroot
> save ns config
> reboot -warm
```

Wie in den vorhergehenden Befehlen zu sehen ist, sind die Schnittstellen 0/1/1, 1/1/1 und 2/1/1 als Backplane-Schnittstellen der drei Clusterknoten konfiguriert.

2. Melden Sie sich bei der Cluster-IP-Adresse an, und führen Sie folgende Schritte aus:

a) Erstellen Sie die LA-Kanäle für die Knoten NS0 und NS1.

```
> add channel 0/LA/1 -ifnum 0/1/1 0/1/2
> add channel 1/LA/2 -ifnum 1/1/1 1/1/2
```

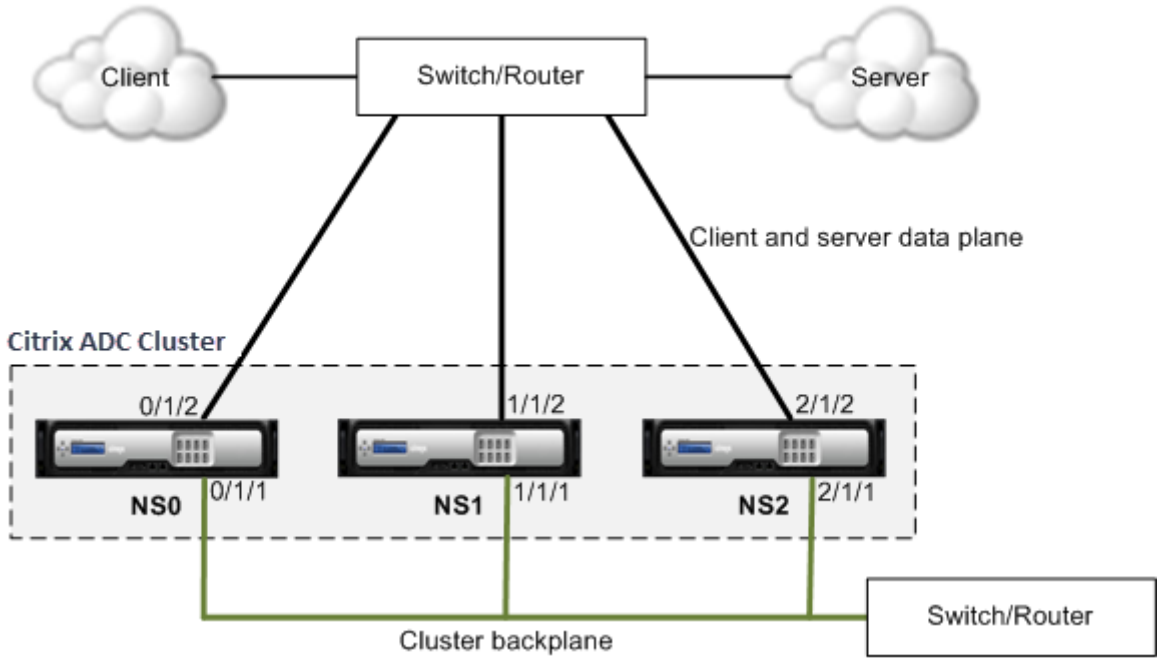
b) Konfigurieren Sie die Rückwandplatine für die Clusterknoten.

```
> set cluster node 0 -backplane 0/LA/1
> set cluster node 1 -backplane 1/LA/2
> set cluster node 2 -backplane 2/1/1
```


Gemeinsame Schnittstellen für Client und Server und dedizierte Schnittstellen für Backplane

October 5, 2021

Es handelt sich um eine einarmige Bereitstellung des Citrix ADC Clusters. In dieser Bereitstellung verwenden Client- und Servernetzwerke die gleichen Schnittstellen für die Kommunikation mit dem Cluster. Die Cluster-Backplane verwendet dedizierte Schnittstellen für die Kommunikation zwischen Knoten.



- NS0 - nodeId: 0, NSIP: 10.102.29.60
- NS1 - nodeId: 1, NSIP: 10.102.29.70
- NS2 - nodeId: 2, NSIP: 10.102.29.80

So stellen Sie einen Cluster mit einer gemeinsamen Schnittstelle für Client und Server und einer anderen Schnittstelle für die Clusterrückwandplatine bereit

1. Erstellen Sie einen Cluster von Knoten NS0, NS1 und NS2.
2. Melden Sie sich beim ersten Knoten an, den Sie dem Cluster hinzufügen möchten, und führen Sie folgende Schritte aus:

```
1 > create cluster instance 1
2 > add cluster node 0 10.102.29.60 -state ACTIVE -backplane
     0/1/1
```



```
3 > enable cluster instance 1
4 > add ns ip 10.102.29.61 255.255.255.255 -type CLIP
5 > save ns config
6 > reboot -warm
```

3. Melden Sie sich bei der Cluster-IP-Adresse an, und führen Sie folgende Schritte aus:

```
1 > add cluster node 1 10.102.29.70 -state ACTIVE -backplane
     1/1/1
2 > add cluster node 2 10.102.29.80 -state ACTIVE -backplane
     2/1/1
```

4. Melden Sie sich bei den Knoten 10.102.29.70 und 10.102.29.80 an, um die Knoten mit dem Cluster zu verbinden.

```
1 > join cluster -clip 10.102.29.61 -password nsroot
2 > save ns config
3 > reboot -warm
```

Wie in den vorhergehenden Befehlen zu sehen ist, sind die Schnittstellen 0/1/1, 1/1/1 und 2/1/1 als Backplane-Schnittstellen der drei Clusterknoten konfiguriert.

1. Erstellen Sie auf der Cluster-IP-Adresse VLANs für die Backplane-Schnittstellen sowie für die Client- und Serverschnittstellen.

   //For the backplane interfaces

```
1 > add vlan 10
2 > bind vlan 10 0/1/1 1/1/1 2/1/1
```

   //Für die Schnittstellen, die mit dem Client- und Server-Netzwerk verbunden sind.

```
1 > add vlan 20
2 > bind vlan 20 0/1/2 1/1/2 2/1/2
```

2. Erstellen Sie auf dem Switch VLANs für die Schnittstellen, die den Backplaneschnittstellen sowie den Client- und Serverschnittstellen entsprechen. Die folgenden Beispielkonfigurationen werden für den Cisco® Nexus 7000 C7010 Release 5.2 (1) Switch bereitgestellt. Ähnliche Konfigurationen müssen auf anderen Switches durchgeführt werden.

//For the backplane interfaces. Für jede Schnittstelle wiederholen…

```
> interface Ethernet2/47
  switchport access vlan 100
  switchport mode access
  end
```

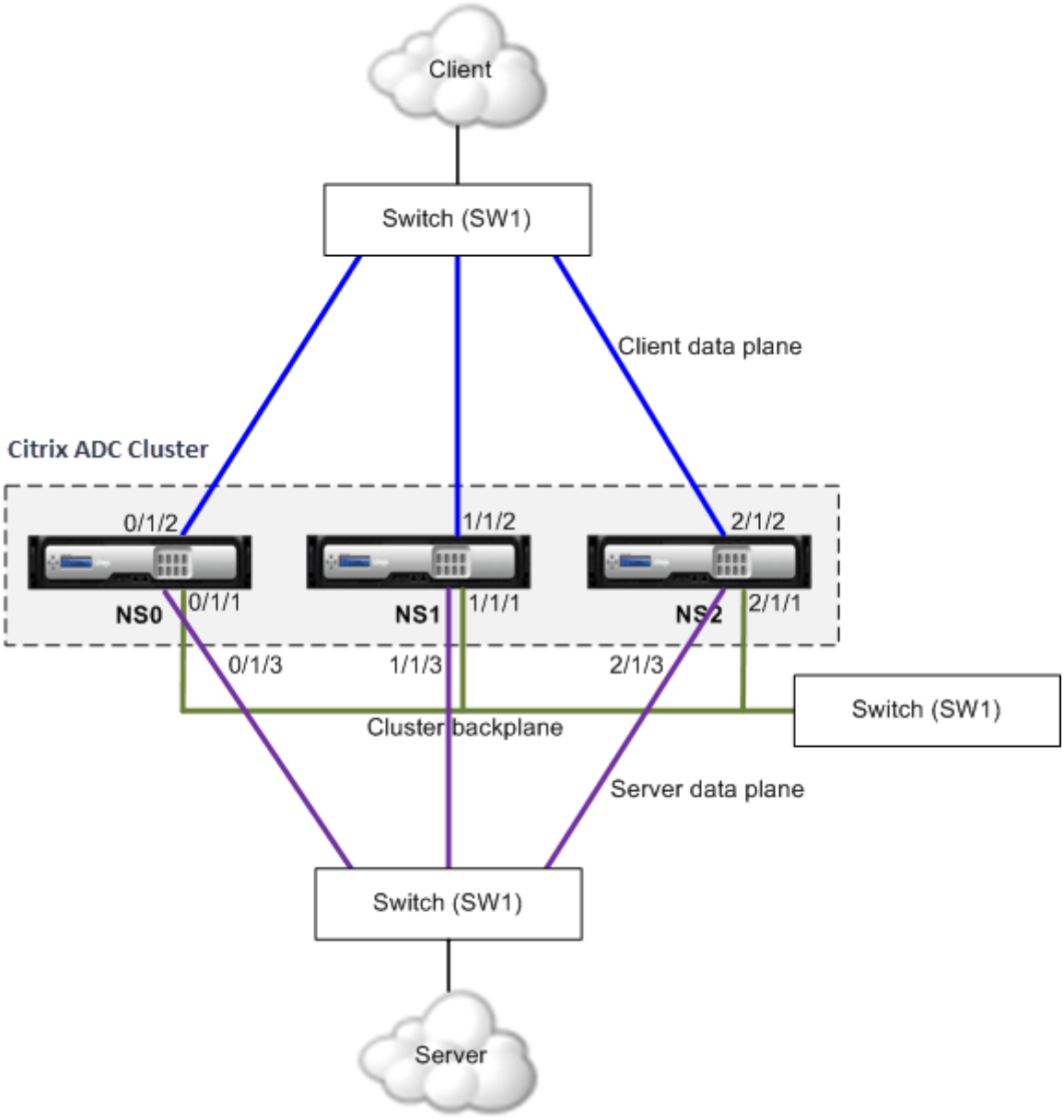
//Für die Schnittstellen, die mit dem Client- und Server-Netzwerk verbunden sind. Für jede Schnittstelle wiederholen…

```
> interface Ethernet2/47
  switchport access vlan 200
  switchport mode access
  end
```

Gemeinsamer Switch für Client, Server und Backplane

October 5, 2021

In dieser Bereitstellung verwenden Client, Server und Rückwandplatine dedizierte Schnittstellen auf demselben Switch für die Kommunikation mit dem Citrix ADC-Cluster.



- NS0 - nodeId: 0, NSIP: 10.102.29.60
- NS1 - nodeId: 1, NSIP: 10.102.29.70
- NS2 - nodeId: 2, NSIP: 10.102.29.80

So stellen Sie einen Cluster mit einem gemeinsamen Switch für Client, Server und Rückwandplatine bereit

1. Erstellen Sie einen Cluster von Knoten NS0, NS1 und NS2.
2. Melden Sie sich beim ersten Knoten an, den Sie dem Cluster hinzufügen möchten, und führen Sie folgende Schritte aus:


```
> create cluster instance 1
> add cluster node 0 10.102.29.60 -state ACTIVE -backplane
   0/1/1
> enable cluster instance 1
> add ns ip 10.102.29.61 255.255.255.255 -type CLIP
> save ns config
> reboot -warm
```

3. Melden Sie sich bei der Cluster-IP-Adresse an, und führen Sie folgende Schritte aus:

```
> add cluster node 1 10.102.29.70 -state ACTIVE -backplane
   1/1/1
> add cluster node 2 10.102.29.80 -state ACTIVE -backplane
   2/1/1
```

4. Melden Sie sich bei den Knoten 10.102.29.70 und 10.102.29.80 an, um die Knoten mit dem Cluster zu verbinden.

```
> join cluster -clip 10.102.29.61 -password nsroot
> save ns config
> reboot -warm
```

Wie in den vorhergehenden Befehlen zu sehen ist, sind die Schnittstellen 0/1/1, 1/1/1 und 2/1/1 als Backplane-Schnittstellen der drei Clusterknoten konfiguriert.

1. Erstellen Sie auf der Cluster-IP-Adresse VLANs für die Backplane-, Client- und Server-schnittstellen.

   //For the backplane interfaces

```
> add vlan 10
> bind vlan 10 0/1/1 1/1/1 2/1/1
```

   //For the client-side interfaces

```
> add vlan 20
> bind vlan 20 0/1/2 1/1/2 2/1/2
```


//For the server-side interfaces

```
> add vlan 30
> bind vlan 30 0/1/3 1/1/3 2/1/3
```

2. Erstellen Sie auf dem Switch VLANs für die Schnittstellen, die den Backplaneschnittstellen sowie den Client- und Serverschnittstellen entsprechen. Die folgenden Beispielkonfigurationen werden für den Cisco® Nexus 7000 C7010 Release 5.2 (1) Switch bereitgestellt. Ähnliche Konfigurationen müssen auf anderen Switches durchgeführt werden.

   //For the backplane interfaces. Für jede Schnittstelle wiederholen…

```
> interface Ethernet2/47
  switchport access vlan 100
  switchport mode access
  end
```

   //Für die Client-Schnittstellen. Für jede Schnittstelle wiederholen…

```
> interface Ethernet2/48
  switchport access vlan 200
  switchport mode access
  end
```

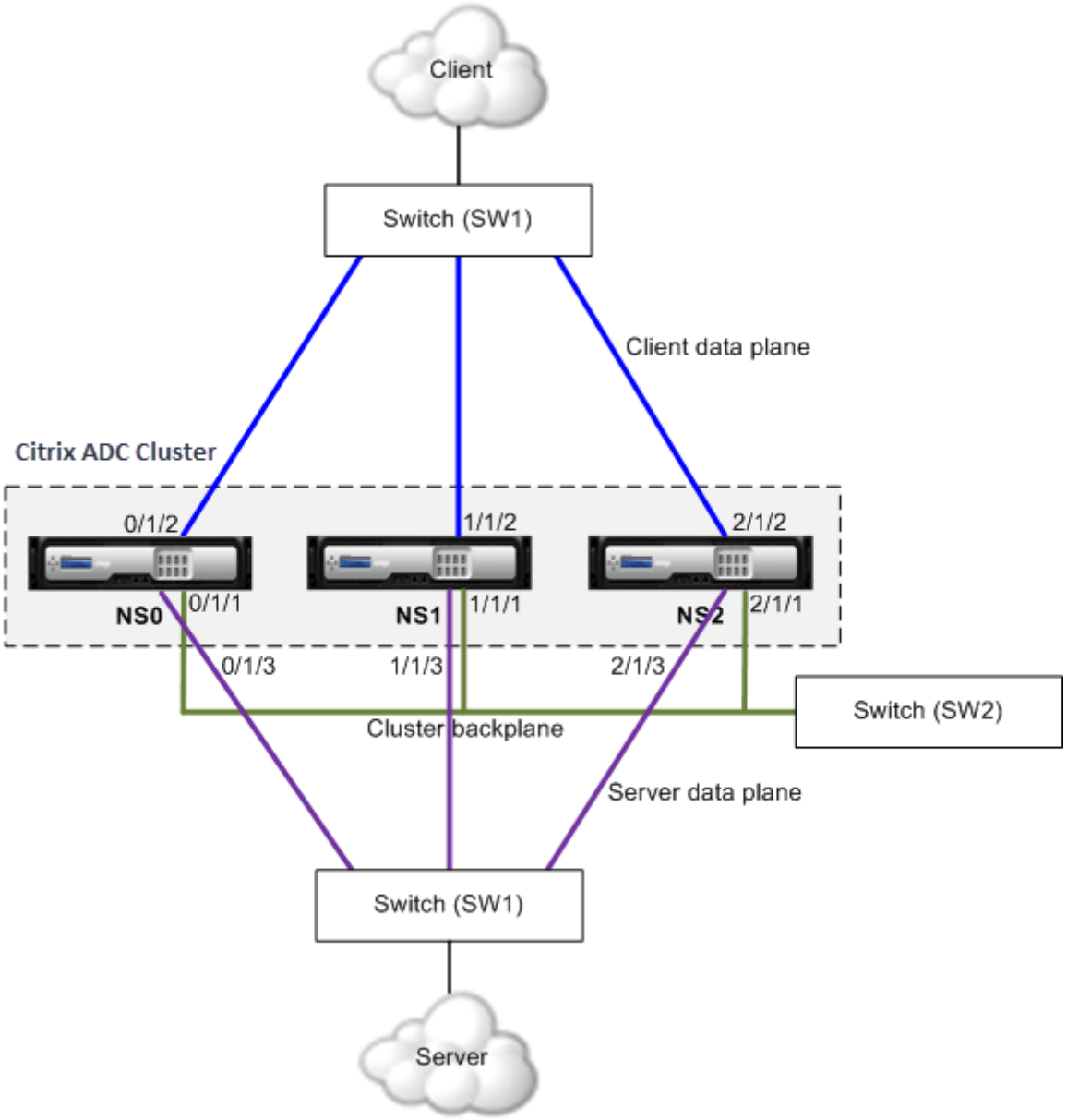
   //Für die Serverschnittstellen. Für jede Schnittstelle wiederholen…

```
> interface Ethernet2/49
  switchport access vlan 300
  switchport mode access
  end
```

Gemeinsamer Switch für Client und Server und dedizierter Switch für Backplane

October 5, 2021

In dieser Bereitstellung verwenden die Clients und Server unterschiedliche Schnittstellen auf demselben Switch für die Kommunikation mit dem Citrix ADC-Cluster. Die Cluster-Backplane verwendet einen dedizierten Switch für die Kommunikation zwischen Knoten.



- NS0 - nodeId: 0, NSIP: 10.102.29.60
- NS1 - nodeId: 1, NSIP: 10.102.29.70
- NS2 - nodeId: 2, NSIP: 10.102.29.80

So stellen Sie einen Cluster mit demselben Switch für die Clients und Server und einen anderen Switch für die Clusterrückwandplatine bereit

1. Erstellen Sie einen Cluster von Knoten NS0, NS1 und NS2.

   - Melden Sie sich beim ersten Knoten an, den Sie dem Cluster hinzufügen möchten, und führen Sie folgende Schritte aus:

   ```
   > create cluster instance 1
   > add cluster node 0 10.102.29.60 -state ACTIVE -backplane
      0/1/1
   > enable cluster instance 1
   > add ns ip 10.102.29.61 255.255.255.255 -type CLIP
   > save ns config
   > reboot -warm
   ```

   - Melden Sie sich bei der Cluster-IP-Adresse an, und führen Sie folgende Schritte aus:

   ```
   > add cluster node 1 10.102.29.70 -state ACTIVE -backplane
      1/1/1
   > add cluster node 2 10.102.29.80 -state ACTIVE -backplane
      2/1/1
   ```

   - Melden Sie sich bei den Knoten 10.102.29.70 und 10.102.29.80 an, um die Knoten mit dem Cluster zu verbinden.

   ```
   > join cluster -clip 10.102.29.61 -password nsroot
   > save ns config
   > reboot -warm
   ```

   Wie in den vorhergehenden Befehlen zu sehen ist, sind die Schnittstellen 0/1/1, 1/1/1 und 2/1/1 als Backplane-Schnittstellen der drei Clusterknoten konfiguriert.

2. Erstellen Sie auf der Cluster-IP-Adresse VLANs für die Backplane-, Client- und Server-schnittstellen.

   //For the backplane interfaces

   ```
   > add vlan 10
   > bind vlan 10 0/1/1 1/1/1 2/1/1
   ```

   //For the client-side interfaces


```
> add vlan 20
> bind vlan 20 0/1/2 1/1/2 2/1/2
```

//For the server-side interfaces

```
> add vlan 30
> bind vlan 30 0/1/3 1/1/3 2/1/3
```

3. Erstellen Sie auf dem Switch VLANs für die Schnittstellen, die den Backplaneschnittstellen sowie den Client- und Serverschnittstellen entsprechen. Die folgenden Beispielkonfigurationen werden für den Cisco® Nexus 7000 C7010 Release 5.2 (1) Switch bereitgestellt. Ähnliche Konfigurationen müssen auf anderen Switches durchgeführt werden.

   //For the backplane interfaces. Für jede Schnittstelle wiederholen…

```
> interface Ethernet2/47
> switchport access vlan 100
> switchport mode access
> end
```

   //Für die Client-Schnittstellen. Für jede Schnittstelle wiederholen…

```
> interface Ethernet2/48
> switchport access vlan 200
> switchport mode access
> end
```

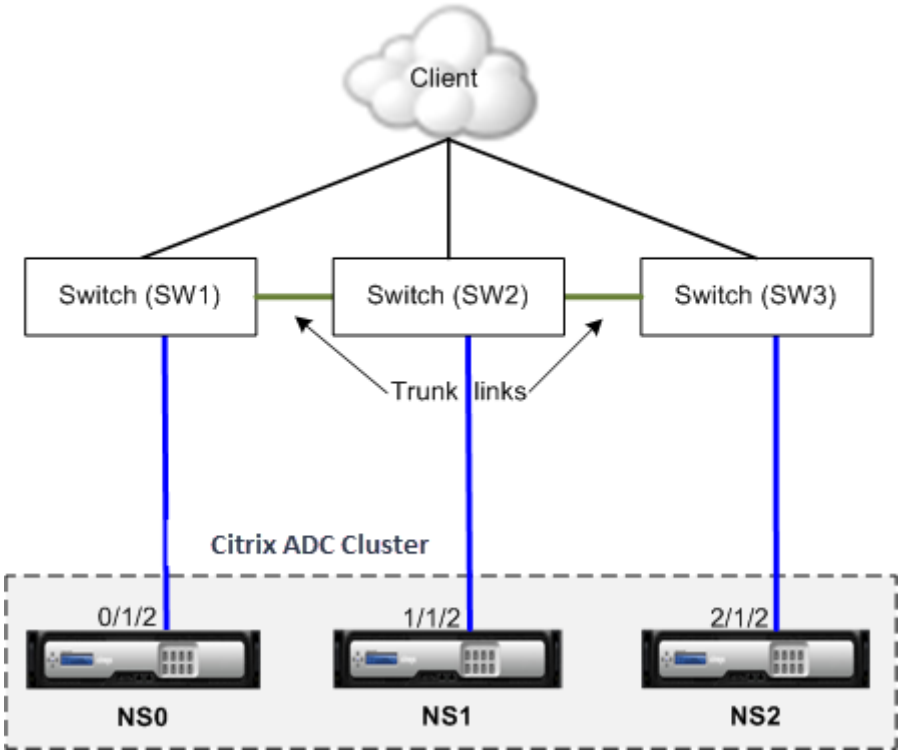
   //Für die Serverschnittstellen. Für jede Schnittstelle wiederholen…

```
> interface Ethernet2/49
> switchport access vlan 300
> switchport mode access
> end
```


Unterschiedliche Schalter für jeden Knoten

October 5, 2021

In dieser Bereitstellung ist jeder Clusterknoten mit einem anderen Switch verbunden, und zwischen den Switches werden Trunk-Links konfiguriert.



Die Clusterkonfigurationen sind die gleichen wie die anderen Bereitstellungsszenarien. Die meisten clientseitigen Konfigurationen werden auf den clientseitigen Switches durchgeführt.

Beispiel-Clusterkonfigurationen

October 5, 2021

Das folgende Beispiel kann verwendet werden, um einen Cluster mit vier Knoten mit ECMP, Cluster LA oder Linksets zu konfigurieren.

1. Erstellen Sie den Cluster.
    - Melden Sie sich beim ersten Knoten an.
    - Fügen Sie die Clusterinstanz hinzu.


```
1   > add cluster instance 1
```

- Fügen Sie dem Cluster den ersten Knoten hinzu.

```
1   > add cluster node 0 10.102.33.184 -backplane 0/1/1
```

- Aktivieren Sie die Clusterinstanz.

```
1   > enable cluster instance 1
```

- Fügen Sie die Cluster-IP-Adresse hinzu.

```
1   > add ns ip 10.102.33.185 255.255.255.255 -type CLIP
```

- Speichern Sie die Konfigurationen.

```
1   > save ns config
```

- Warmstarten Sie die Appliance.

```
1   > reboot -warm
```

2. Fügen Sie dem Cluster die anderen drei Knoten hinzu.
   - Melden Sie sich bei der Cluster-IP-Adresse an.
   - Fügen Sie dem Cluster den zweiten Knoten hinzu.

```
1   > add cluster node 1 10.102.33.187 -backplane 1/1/1
```

   - Fügen Sie dem Cluster den dritten Knoten hinzu.

```
1   > add cluster node 2 10.102.33.188 -backplane 2/1/1
```


- Fügen Sie dem Cluster den vierten Knoten hinzu.

```
1   > add cluster node 3 10.102.33.189 -backplane 3/1/1
```

3. Verbinden Sie die hinzugefügten Knoten mit dem Cluster. Dieser Schritt gilt nicht für den ersten Knoten.
   - Melden Sie sich bei jedem neu hinzugefügten Knoten an.
   - Verbinden Sie den Knoten mit dem Cluster.

```
1   > join cluster -clip 10.102.33.185 -password nsroot
```

   - Speichern Sie die Konfiguration.

```
1   > save ns config
```

   - Warmstarten Sie die Appliance.

```
1   > reboot -warm
```

4. Konfigurieren Sie den Citrix ADC-Cluster über die Cluster-IP-Adresse.

   // Lastausgleichsfunktion aktivieren

```
1      > enable ns feature lb
```

   // Hinzufügen eines virtuellen Load Balancing Servers

```
1      > add lb vserver first_lbvserver http
2      ....
3      ....
```

5. Konfigurieren Sie einen der folgenden Verkehrsverteilungsmechanismen (ECMP, Cluster LA oder Linkset) für den Cluster.

   ECMP

- Melden Sie sich bei der Cluster-IP-Adresse an.
- Aktivieren Sie das OSPF-Routingprotokoll.

```
1 > enable ns feature ospf
```

- Fügen Sie ein VLANhinzu.

```
1 > add vlan 97
```

- Binden Sie die Schnittstellen der Clusterknoten an das VLAN.

```
1 > bind vlan 97 -ifnum 0/1/4 1/1/4 2/1/4 3/1/4
```

- Fügen Sie auf jedem Knoten ein Spotted SNIP hinzu und aktivieren Sie dynamisches Routing darauf.

```
1 > add ns ip 1.1.1.10 255.255.255.0 -ownerNode 0 -
    dynamicRouting ENABLED
2 > add ns ip 1.1.1.11 255.255.255.0 -ownerNode 1 -
    dynamicRouting ENABLED
3 > add ns ip 1.1.1.12 255.255.255.0 -ownerNode 2 -
    dynamicRouting ENABLED
4 > add ns ip 1.1.1.13 255.255.255.0 -ownerNode 3 -
    dynamicRouting ENABLED
```

- Binden Sie eine der SNIP-Adressen an das VLAN.

```
1 > bind vlan 97 -ipAddress 1.1.1.10 255.255.255.0
```

- Konfigurieren Sie das Routing-Protokoll auf ZeBOS mit der VTYSH-Shell.

  Statischer Cluster LA

  - Melden Sie sich bei der Cluster-IP-Adresse an.
  - Fügen Sie einen Cluster-LA-Kanal hinzu.


```
> add channel CLA/1 -speed 1000
```

- Binden Sie die Schnittstellen an den Cluster-LA-Kanal.

```
> bind channel CLA/1 0/1/5 1/1/5 2/1/5 3/1/5
```

- Führen Sie eine äquivalente Konfiguration auf dem Switch durch

  Dynamischer Cluster LA

  * Melden Sie sich bei der Cluster-IP-Adresse an.
  * Fügen Sie die Schnittstellen zum Cluster-LA-Kanal hinzu.

```
> set interface 0/1/5 -lacpmode active -lacpkey 5 -
    lagtype cluster
> set interface 1/1/5 -lacpmode active -lacpkey 5 -
    lagtype cluster
> set interface 2/1/5 -lacpmode active -lacpkey 5 -
    lagtype cluster
> set interface 3/1/5 -lacpmode active -lacpkey 5 -
    lagtype  cluster
```

  * Führen Sie eine äquivalente Konfiguration auf dem Switch durch

  Linksets. Angenommen, der Knoten mit NodeID 3 ist nicht mit dem Switch verbunden. Sie müssen ein Linkset so konfigurieren, dass der nicht verbundene Knoten die anderen Knotenschnittstellen verwenden kann, um mit dem Switch zu kommunizieren.

a) Melden Sie sich bei der Cluster-IP-Adresse an.

b) Fügen Sie einen Linksatz hinzu.

```
> add linkset LS/1
```

c) Binden Sie die verbundenen Schnittstellen an das Linkset.

```
> bind linkset LS/1 -ifnum 0/1/6 1/1/6 2/1/6
```


6. Aktualisieren Sie den Status der Clusterknoten auf ACTIVE.

```
> set cluster node 0 -state ACTIVE
> set cluster node 1 -state ACTIVE
> set cluster node 2 -state ACTIVE
> set cluster node 3 -state ACTIVE
```

Verwenden von VRRP in einem Cluster-Setup

October 5, 2021

Virtual Router Redundancy Protocol (VRRP) wird in einem Cluster-Setup für IPv4 und IPv6 unterstützt. Die beiden VRRP-Funktionen, die in einem Cluster-Setup unterstützt werden, sind schnittstellenbasiertes VRRP und IP-basiertes VRRP.

IP-basiertes VRRP

In IP-basiertem VRRP werden gestreifte VIP-Adressen, die an dieselbe VRID gebunden sind, auf allen Knoten eines Cluster-Setups konfiguriert. Diese VIP-Adressen sind auf allen Knoten aktiv

Einer der Clusterknoten fungiert als VRID-Besitzer und sendet die VRRP-Ankündigung an andere Knoten. Wenn der VRID-Besitzerknoten fehlschlägt, übernimmt ein anderer Knoten im Cluster den Besitz der VRID und beginnt mit dem Senden von VRRP-Ankündigungen. Sie können auch einen bestimmten Clusterknoten als Besitzer der VRID zuweisen.

> **Hinweis:**
>
> Citrix empfiehlt, die IP-basierte Methode für die VRRP-Bereitstellung im Cluster zu verwenden.

Konfigurieren von IP-basiertem VRRP für IPv4

Führen Sie die folgenden Aufgaben für ein Cluster-Setup zum Konfigurieren von IP-basiertem VRRP für IPv4 aus:

- **Fügen Sie eine VRID hinzu**. Eine VRID ist eine Ganzzahl, die vom Cluster-Setup verwendet wird, um eine virtuelle MAC-Adresse zu bilden. Die generische VMAC-Adresse hat die Form 00:00:5 e: 00:02: <VRID>.
- **(Optional) Weisen Sie einen Knoten als Besitzer der virtuellen MAC-Adresse**zu. Sie können den Ownernode-Parameter (beim Hinzufügen oder Ändern von VRID6) auf die ID des Clusterknotens festlegen, um ihn als Besitzer der virtuellen MAC-Adresse zuzuweisen. Wenn der

zugewiesene Besitzerknoten fehlschlägt, wird einer der UP Clusterknoten dynamisch als Besitzer der virtuellen MAC-Adresse gewählt. Sie können den Besitzerknoten mit dem `set vrID <id> -ownerNode <positive_interger>` Befehl festlegen.

- **Binden Sie die VRID an die VIP-Adresse der Knoten**. Binden Sie die erstellte VRID an die gestreifte VIP-Adresse.

So fügen Sie eine VRID über die Befehlszeile hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 -  add vrid <ID> [-ownerNode <positive_integer>]
2 -  show vrid <ID>
```

So binden Sie die VRID mit der CLI an die VIP-Adresse

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `set ns ip <IPv4Address> -vrid <ID><!--NeedCopy-->`
- `show vrid <ID><!--NeedCopy-->`

So fügen Sie eine VRID mit der GUI hinzu

1. Navigieren Sie zu **System > Netzwerk > VMAC**, und klicken Sie auf der Registerkarte **VMAC** auf **Hinzufügen**.
2. Geben Sie auf der Seite **VMAC** erstellen einen Wert im Feld **Virtual Router ID** an, und klicken Sie dann auf **Erstellen** .

So binden Sie die VRID mit der GUI an eine VIP-Adresse

1. Navigieren Sie zu **System > Netzwerk > IPs**, wählen Sie auf der Registerkarte **IPv4s**eine VIP-Adresse aus und klicken Sie auf **Bearbeiten**.
2. Legen Sie während der Bearbeitung der VIP-Konfiguration den **Virtual Router ID-Parameter** fest.

```
1 > add vrid 90
2  Done
3 > set ns ip 192.0.2.90  - vrid 90
4  Done
```


Konfigurieren von IP-basiertem VRRP für IPv6

Führen Sie die folgenden Aufgaben für ein Cluster-Setup zum Konfigurieren von IP-basiertem VRRP für IPv6 aus:

- **Fügen Sie einen VRID6 hinzu**. Ein VRID6 ist eine Ganzzahl, die vom Cluster-Setup verwendet wird, um eine virtuelle MAC6-Adresse zu bilden. Die generische VMAC6-Adresse hat die Form 00:00:5 e: 00:02: <VRID6>.
- **(Optional) Weisen Sie einen Knoten als Besitzer der virtuellen MAC6-Adresse**zu. Sie können den Ownernode-Parameter (beim Hinzufügen oder Ändern von VRID6) auf die ID des Clusterknotens festlegen, um ihn als Besitzer der virtuellen MAC6-Adresse zuzuweisen. Wenn der zugewiesene Besitzerknoten fehlschlägt, wird einer der UP Clusterknoten dynamisch als Besitzer der virtuellen MAC6-Adresse gewählt.
- **Binden Sie den VRID6 an die VIP6-Adresse der Knoten**. Binden Sie den erstellten VRID6 an die gestreifte VIP6-Adresse.

So fügen Sie eine VRID6 über die Befehlszeile hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add vrid6 <ID> [-ownerNode <positive_integer>]<!--NeedCopy-->`
- `show vrid6 <ID><!--NeedCopy-->`

So binden Sie die VRID6 mit der CLI an die VIP6-Adresse

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `set ns ip6 <IPv6Address> -vrid6 <ID><!--NeedCopy-->`
- `show vrid6 <ID><!--NeedCopy-->`

So fügen Sie eine VRID6 mit der GUI hinzu

1. Navigieren Sie zu **System > Netzwerk > VMAC**, und klicken Sie auf der Registerkarte **VMAC6** auf **Hinzufügen** .
2. Geben Sie auf der Seite **Virtuellen MAC6 erstellen** einen Wert im Feld **Virtual Router ID** an, und klicken Sie dann auf **Erstellen** .

So binden Sie den VRID6 mit der GUI an eine VIP6-Adresse

1. Navigieren Sie zu **System > Netzwerk > IPs**, wählen Sie auf der Registerkarte **IPv6s**eine VIP-Adresse aus und klicken Sie auf **Bearbeiten**.

2. Legen Sie den **Virtual Router ID-Parameter** fest, während Sie die VIP6-Konfiguration bearbeiten.

```
1 > add vrid6 90
2  Done
3 > set ns ip6 2001:db8::5001  - vrid6 90
4  Done
```

Schnittstellenbasiertes VRRP

In der schnittstellenbasierten VRRP-Funktion wird dieselbe virtuelle MAC-Adresse auf beiden Knoten des Clusters konfiguriert. Diese virtuelle MAC-Adresse wird in GARP-Ankündigungen und ARP-Antworten für die auf einem Knoten konfigurierten IP-Adressen verwendet. Diese Funktion ist nützlich in einem Cluster-Setup mit zwei Knoten, das über externe Geräte/Router verfügt, die keine GARP-Ankündigungen akzeptieren.

> **Hinweis:**
>
> Die schnittstellenbasierte VRRP-Funktion ist nur für einen Cluster mit zwei Knoten anwendbar, bei dem ein Knoten im aktiven Zustand und der andere Knoten als Ersatz fungiert.

Bei der gleichen virtuellen MAC-Adresse auf beiden Clusterknoten bleibt die MAC-Adresse für die IP-Adressen auf dem neuen aktiven Knoten unverändert und die ARP-Tabellen auf den externen Geräten/Routern nicht aktualisiert werden müssen.

Konfigurieren von schnittstellenbasiertem VRRP für IPv4

Führen Sie die folgenden Aufgaben für ein Cluster-Setup aus, um schnittstellenbasiertes VRRP für IPv4 zu konfigurieren:

- **Fügen Sie eine VRID hinzu**. Eine VRID ist eine Ganzzahl, die vom Cluster-Setup verwendet wird, um eine virtuelle MAC-Adresse zu bilden.
- **Binden Sie die VRID an Knotenschnittstellen**. Binden Sie die Schnittstellen an die erstellte VRID. Die gebundenen Schnittstellen (im aktuellen aktiven Knoten) verwenden die virtuelle MAC-Adresse in GARP-Ankündigungen und ARP-Antworten für ihre IPv4-Adressen. Sie müssen die VRID den Schnittstellen beider Knoten des Active-Spare Cluster-Setups zuordnen. Dies liegt daran, dass im Gegensatz zu einer Hochverfügbarkeits-Konfiguration Schnittstellen-IDs in einem Cluster-Setup unterschiedlich sind.

So fügen Sie eine VRID über die Befehlszeile hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
1 - add vrid <ID>
2 - show vrid <ID>
```

So binden Sie die VRID über die Befehlszeile an eine Schnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 - bind vrid <ID> -ifnum <interface_name>
2 - show vrid <ID>
```

So fügen Sie eine VRID hinzu und binden sie mit der GUI an Schnittstellen

1. Navigieren Sie zu **System > Netzwerk > VMAC**, und klicken Sie auf der Registerkarte **VMAC** auf **Hinzufügen**.
2. Geben Sie auf der Seite **Virtuellen MAC erstellen** einen Wert im Feld **Virtuelle Router-ID*** an, binden Sie Schnittstellen im Abschnitt **Schnittstellen zuordnen**, und klicken Sie dann auf **Erstellen** .

```
1 > add vrid 300
2  Done
3 > bind vrid 300 -ifnum 1/1/2 2/1/3
4  Done
```

Konfigurieren von schnittstellenbasiertem VRRP für IPv6

Führen Sie die folgenden Aufgaben für ein Cluster-Setup aus, um schnittstellenbasiertes VRRP für IPv6 zu konfigurieren:

- **Fügen Sie einen VRID6 hinzu**. Ein VRID6 ist eine Ganzzahl, die vom Cluster-Setup verwendet wird, um eine virtuelle MAC6-Adresse zu bilden. Die generische VMAC6-Adresse hat die Form 00:00:5 e: 00:01: <VRID6>.
- **Binden Sie die VRID6 an Knotenschnittstellen**. Binden Sie die Schnittstellen an das erstellte VRID6. Die gebundenen Schnittstellen (im aktuellen aktiven Knoten) verwenden die virtuelle MAC6-Adresse in GARP-Ankündigungen und ARP-Antworten für ihre IPv6-Adressen. Sie müssen den VRID6 den Schnittstellen beider Knoten des Active-Spare Cluster-Setups zuordnen. Dies

liegt daran, dass im Gegensatz zu einer Hochverfügbarkeits-Konfiguration Schnittstellen-IDs in einem Cluster-Setup unterschiedlich sind.

So fügen Sie eine VRID6 über die Befehlszeile hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 -  add vrid6 <ID>
2 -  show vrid6 <ID>
```

So binden Sie den VRID6 über die Befehlszeile an eine Schnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `bind vrid6 <ID> -ifnum <interface_name><!--NeedCopy-->`
- `show vrid6 <ID><!--NeedCopy-->`

So fügen Sie ein VRID6 hinzu und binden es mit der GUI an Schnittstellen

1. Navigieren Sie zu **System > Netzwerk > VMAC**, und klicken Sie auf der Registerkarte **VMAC6** auf **Hinzufügen** .
2. Geben Sie auf der Seite **Virtuellen MAC6 erstellen** einen Wert im Feld **Virtuelle Router-ID** an, binden Sie Schnittstellen im Abschnitt **Schnittstellen zuordnen**, und klicken Sie dann auf **Erstellen** .

```
1 > add vrid6 100
2  Done
3 > bind vrid6 100 -ifnum 0/1/1 1/1/2 2/1/3
4  Done
```

Überwachung von Diensten in einem Cluster mit der Pfadüberwachung

October 5, 2021

In einem Cluster-Setup wird der Besitz für Überwachungsdienste auf die Knoten verteilt. Daher überwachen verschiedene Knoten verschiedene Dienste. Der Knoten, der einen Dienst überwacht,

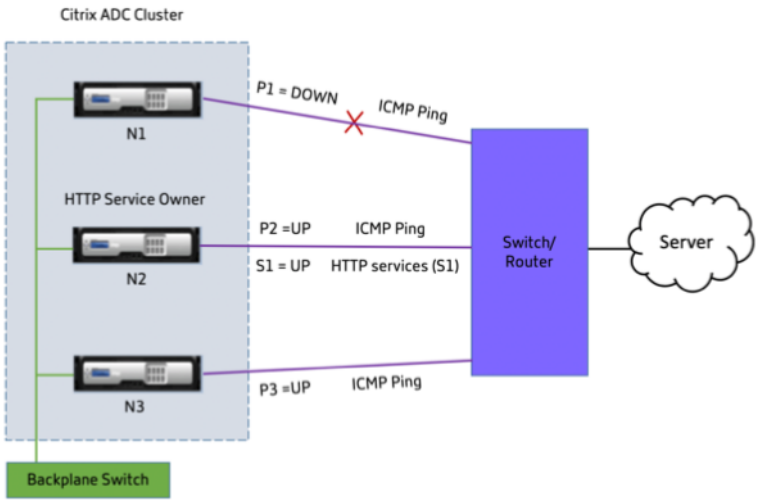
wird als Diensteigentümer bezeichnet. Nur der Diensteigentümer überprüft den Server, um den Status der ihm zugewiesenen Dienste zu überwachen. Weiterhin kommuniziert er den Status der Dienste an alle anderen Knoten innerhalb des Clusters. Der Nachteil bei der verteilten Überwachung besteht darin, dass die Netzwerkkonnektivität und der Verbindungsstatus zwischen allen Knoten und dem Server nicht ermittelt werden. Um diesen Nachteil zu überwinden, können Sie die Pfadüberwachung verwenden.

> **Hinweis:**
>
> Sie können keinen Knoten auswählen, um einen Dienst zu überwachen. Die Auswahl von Knoten zur Überwachung eines Dienstes erfolgt über einen internen Mechanismus. Sie können den Besitzerknoten anzeigen, um Dienste mithilfe des `show serviceGroup <service group name>` Befehls `show service <service name>` und zu überwachen.

Die Pfadüberwachung überprüft die Netzwerkkonnektivität und den Verbindungsstatus zwischen einem Knoten und dem vom Server bereitgestellten Dienst. Ein Knoten sendet ICMP-Pings, um zu überprüfen, ob der Server erreichbar ist oder nicht.

Funktionsweise der Pfadüberwachung

Betrachten Sie ein Beispiel für einen Citrix ADC Cluster, der aus drei Knoten N1, N2 und N3 besteht. N2 ist der Dienstbesitzer, der den Status von HTTP-Diensten (S1) überwacht. Es gibt den Dienststatus an andere Knoten im Cluster bekannt. Die Pfadüberwachung ist für alle Knoten im Cluster für alle Dienste aktiviert. Jeder Knoten sendet nur einen ICMP-Ping an den Server. Der Diensteigentümer sendet sowohl die HTTP-Dienstanforderung als auch einen ICMP-Ping. Jeder Knoten meldet seinen Pfadüberwachungsstatus an den Diensteigentümer.



Die folgenden beiden Parameter bestimmen den Dienststatus eines Knotens:

- S = vom Dienstleistungseigentümer angekündigter Servicestatus

- P = Pfadüberwachungsstatus jedes Knotens

Ob ein Knoten einen Server erreichen kann oder nicht, bestimmt den Pfadüberwachungsstatus für diesen Knoten.

Die folgende Tabelle zeigt den Dienststatus basierend auf dem Pfadüberwachungsstatus, wenn der PathMonitorinDV-Parameter aktiviert oder deaktiviert ist.

Parameter	Pfadüberwachungsstatus	Servicestatus
pathmonitorinDV = NO; Ist die Standardkonfiguration.	P1 = DOWN	S1 = DOWN
	P2 = UP	S1 = DOWN
	P3 = UP	S1 = DOWN
pathMonitorIndv = YES	P1 = DOWN	S1 = DOWN
	P2 = UP	S1 = UP
	P3 = UP	S1 = UP

In diesem Beispiel entscheidet der Diensteigentümer den Dienststatus für alle Knoten basierend auf dem Knoten, dessen Pfadüberwachungsstatus auf DOWN festgelegt ist. Wenn der Pfadüberwachungsstatus für einen der Knoten DOWN ist, legt der Diensteigentümer den Dienststatus für alle Knoten auf DOWN fest. Der Dienststatus für alle Knoten wird nur dann auf UP gesetzt, wenn der Pfadüberwachungsstatus für jeden Knoten UP ist.

Sie können die Pfadüberwachung für einzelne Knoten verwenden, indem Sie den Parameter PathMonitorIndV aktivieren. Dieser Parameter ermöglicht es dem Diensteigentümer, den Dienststatus für jeden Knoten basierend auf dem Pfadüberwachungsstatus dieses jeweiligen Knotens festzulegen.

> **Hinweis:**
>
> Wenn der PathMonitorindv-Parameter festgelegt ist, können einige Funktionen wie die Persistenz unterbrochen werden.

Konfigurieren der Pfadüberwachung

Die Pfadüberwachung ist für alle Dienste und Servicegruppen anwendbar. Der Parameter Pfadüberwachung ist standardmäßig deaktiviert.

So aktivieren Sie die Pfadüberwachung für Dienste/Servicegruppen mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add service <service name> <IP address> <service type> <port> [-
    pathMonitor <YES | NO>] [-pathMonitorIndv <YES | NO>]

add servicegroup <servicegroup name> <service type> [-pathMonitor <YES
    | NO>] [-pathMonitorIndv <YES | NO>]
<!--NeedCopy-->
```

Beispiel:

```
add service s1 1.1.1.1 HTTP 80 -pathMonitor YES
add servicegroup sg_1 HTTP -pathMonitor YES

add service s1 1.1.1.1 HTTP 80 -pathMonitor YES -pathMonitorIndv YES
add servicegroup sg_1 HTTP -pathMonitor YES -pathMonitorIndv YES
<!--NeedCopy-->
```

Sie können den Parameter für die Pfadüberwachung auch über den Befehl set wie folgt festlegen:

```
set service <service name> [-pathMonitor <YES | NO>] [-pathMonitorIndv
    <YES | NO>]
set servicegroup <servicegroup name> [-pathMonitor <YES | NO>] [-
    pathMonitorIndv <YES | NO>]
<!--NeedCopy-->
```

Beispiel:

```
set service s1 -pathMonitor YES
set servicegroup sg_1 -pathMonitor YES


set service s1 -pathMonitorIndv YES
set servicegroup sg_1 -pathMonitorIndv NO
<!--NeedCopy-->
```

So aktivieren Sie die Pfadüberwachung für Services/Servicegruppen mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienste**.

   Navigieren Sie für Servicegruppen zu **Traffic Management** > **Load Balancing** > **Service Groups**.

2. Wählen Sie im Bereich **Dienste/Dienstgruppen eine Servicegruppe** aus der Liste aus, und doppelklicken Sie dann, um sie zu öffnen.
3. Klicken Sie auf der Registerkarte **Diensteinstellungen** auf **Bearbeiten**.
4. Wählen Sie **Pfadüberwachung** aus.
5. Wählen Sie **Individuelle Pfadüberwachung** aus, wenn Sie sie anwenden möchten, und klicken Sie dann auf **OK**.

> **Hinweis:**
>
> Sie können die Überwachung einzelner Pfade nur aktivieren, wenn Sie die Pfadüberwachung aktivieren.

Backup und Wiederherstellung des Cluster-Setups

October 5, 2021

Sie können den aktuellen Status eines Citrix ADC Clusterknotens sichern. Später können Sie die gesicherten Dateien verwenden, um den Knoten in denselben Clusterstatus zurückzusetzen. Als Vorsichtsmaßnahme müssen Sie diese Funktion verwenden, bevor Sie ein Upgrade auf den Clusterknoten durchführen.

Sichern eines Cluster-Setups

Abhängig von den folgenden Optionen können Sie ein grundlegendes oder vollständiges Backup erstellen:

- Art der zu sicherenden Daten.
- Häufigkeit, mit der Sie ein Backup erstellen.
- **Grundlegende Sicherung.** Sichert nur Konfigurationsdateien. Möglicherweise möchten Sie diese Art der Sicherung häufig durchführen, da sich die Dateien, die sie sichern, ständig ändern. Die Dateien, die gesichert werden, werden in der Tabelle aufgeführt.

Verzeichnis

Unterverzeichnis oder Dateien

/nsconfig/

- ns.conf
- Zebos.conf
- rc.netscaler
- snmpd.conf

- nsbefore.sh
- nsafter.sh
- inetd.conf
- ntp.conf
- syslog.conf
- newsyslog.conf
- crontab
- host.conf
- hosts
- ttys
- sshd_config
- httpd.conf
- monitrc
- rc.conf
- ssh_config
- lokale Zeit
- issue
- issue.net

/var/

- download/*
- log/wicmd.log
- wi/tomcat/webapps/*
- wi/tomcat/logs/*
- wi/tomcat/conf/catalina/localhost/*
- nslw.bin/etc/krb.conf
- nslw.bin/etc/krb.keytab
- netscaler/locdb/*
- lib/likewise/db/*
- vpn/bookmark/*
- netscaler/crl
- nstemplates/*
- learnt_data/*

/netscaler/

- custom.html
- vsr.html
- **Vollständiges Backup.** Abgesehen von den Dateien, die durch ein Basis-Backup gesichert werden, sichert ein vollständiges Backup einige weniger häufig aktualisierte Dateien. Die Dateien, die bei einem vollständigen Backup gesichert werden, sind in der Tabelle aufgeführt.

Verzeichnis

Unterverzeichnis oder Dateien

/nsconfig/

- ssl/*
- license/*
- fips/*

/var/

- netscaler/ssl/*
- wi/java_home/jre/lib/security/cacerts/*
- wi/java_home/lib/security/cacerts/*

> **Wichtig**
>
> Die Sicherung und Wiederherstellung funktionieren nicht, wenn CLAG für ein SDX-Cluster-Setup konfiguriert ist.

Das Backup wird als komprimierte TAR-Datei im Verzeichnis /var/ns_sys_backup/ gespeichert. Um Probleme aufgrund der Nichtverfügbarkeit von Speicherplatz zu vermeiden, können Sie maximal 50 Backupdateien in diesem Verzeichnis speichern. Mit dem Befehl rm system backup können Sie vorhandene Backupdateien löschen, damit Sie weitere Sicherungen erstellen können.

Wenn Sie den Sicherungsvorgang für einen CLIP eines Cluster-Setups ausführen, werden Sicherungsdateien auf jedem Cluster-Knoten erstellt.

So sichern Sie ein Cluster-Setup

Sichern des Cluster-Setups auf CLIP mit der Citrix ADC CLI.

Führen Sie an der Eingabeaufforderung die folgenden Schritte aus:

- Speichern Sie die Konfiguration.

  ```
  save ns config<!--NeedCopy-->
  ```

- Erstellen Sie die Backupdatei (Basic oder Full).

  “‘create system backup [][–level (basic | full)][-comment]

```
1  **Beispiel**
2
3  ```create system backup cluster-backup-1  - level basic<!--
     NeedCopy-->
```


Der vorhergehende Befehl erstellt eine Sicherungs-TAR-Datei auf jedem Cluster-Knoten mit dem angegebenen Dateinamen. Beispielsweise wird die Cluster-backup-1.tgz-Datei auf jedem Cluster-Knoten erstellt.

> **Hinweis:**
>
> Wenn der Dateiname nicht angegeben wird, werden Backup-TAR-Dateien auf jedem Cluster-Knoten mit der folgenden Namenskonvention erstellt:
>
> - backup_<level>_<nsip_address of the cluster node 0>_<date-timestamp>.tgz<!--NeedCopy-->
> - backup_<level>_<nsip_address of the cluster node 1>_<date-timestamp>.tgz<!--NeedCopy-->
>
> Beispielsweise bei einem Cluster-Setup mit drei Knoten
>
> - backup_<level>_<nsip_address of the cluster node 0>_<date-timestamp>.tgz<!--NeedCopy--> wird auf node0 erstellt
> - backup _<level>_<nsip_address of the cluster node 1>_<date-timestamp>.tgz<!--NeedCopy--> wird auf node1 erstellt
> - backup_<level>_<nsip_address of the cluster node 2>_<date-timestamp>.tgz<!--NeedCopy--> wird auf node2 erstellt

- Überprüfen Sie die erstellten Backupdateien auf CLIP.

  ```
  show system backup<!--NeedCopy-->
  ```

Wiederherstellen eines Cluster-Setups

Wenn ein Clusterknoten fehlerhaft wird, können Sie diesen Knoten durch einen neuen Knoten ersetzen. Sie können den neuen Knoten für einen Cluster mithilfe einer Sicherungsdatei des fehlerhaften Knotens festlegen.

In einem Cluster-Setup mit drei Knoten können Sie beispielsweise, wenn node1 fehlerhaft wird, diesen fehlerhaften Knoten durch einen neuen Knoten als Knoten1 ersetzen. Mit dem Wiederherstellungsvorgang können Sie eine der Backupdateien des fehlerhaften Knotens auf dem neuen Knoten wiederherstellen.

> **Hinweis:**
>
> Der Wiederherstellungsvorgang ist nicht erfolgreich, wenn die Backupdatei umbenannt wird oder wenn der Inhalt der Datei geändert wird.

So stellen Sie einen Clusterknoten wieder her

So stellen Sie einen Clusterknoten mit der CLI wieder her

Führen Sie an der Eingabeaufforderung die folgenden Schritte aus:

- Erhalten Sie eine Liste der Backupdateien, die auf CLIP verfügbar sind.

  ```
  show system backup<!--NeedCopy-->
  ```

- Kopieren Sie die Backup-Tar-Datei in das Verzeichnis /var/ns_sys_backup des Clusterknotens, das wiederhergestellt werden soll.
- Fügen Sie die Backup-Tar-Datei zum Cluster-Knotenspeicher hinzu, indem Sie den folgenden Befehl auf dem Cluster-Knoten ausführen.

  “‘add system backup

  ```
  **Beispiel**

  ```add system backup CLUSTER-BACKUP-1.tgz<!--NeedCopy-->
  ```

  > **Hinweis:**
  >
  > Der Befehl muss auf dem Clusterknoten ausgeführt werden, der wiederhergestellt werden soll.

- Stellen Sie den Clusterknoten wieder her, indem Sie die Backupdatei angeben.

  “‘restore system backup

  ```
  **Beispiel**

  ```restore system backup CLUSTER-BACKUP-1.tgz<!--NeedCopy-->
  ```

  > **Hinweis:**
  >
  > Der Befehl muss auf dem Clusterknoten ausgeführt werden, der wiederhergestellt werden soll.

- Starten Sie den Clusterknoten neu.

  reboot

  > **Hinweis:**
  >
  > Der Befehl muss auf dem Clusterknoten ausgeführt werden, der wiederhergestellt werden soll.

Aktualisieren oder Herabstufen des Citrix ADC Clusters

October 5, 2021

Auf allen Knoten eines Citrix ADC Clusters muss dieselbe Softwareversion ausgeführt werden. Daher müssen Sie zum Upgrade oder Downgrade des Clusters jede Citrix ADC Appliance des Clusters jeweils einen Knoten aktualisieren oder herabstufen.

Ein Knoten, der aktualisiert oder heruntergestuft wird, wird nicht aus dem Cluster entfernt. Der Knoten bleibt Teil des Clusters und bedient den Datenverkehr ohne Unterbrechung, mit Ausnahme der Ausfallzeit, wenn der Knoten nach dem Upgrade oder Herabstufung neu gestartet wird.

Aufgrund der Nichtübereinstimmung der Softwareversionen zwischen den Clusterknoten ist die Konfigurationspropagierung auf dem Cluster deaktiviert. Die Konfigurationspropagierung ist nur aktiviert, wenn alle Clusterknoten dieselbe Version haben. Da die Konfigurationspropagierung während des Upgrades beim Downgrade eines Clusters deaktiviert ist, können Sie während dieser Zeit keine Konfigurationen über die Cluster-IP-Adresse durchführen.

> **Wichtig**
>
> - In einem Cluster-Setup mit maximaler Verbindung (MaxConn), der auf einen Wert ungleich Null festgelegt ist, schlagen CLIP-Verbindungen möglicherweise fehl, wenn eine der folgenden Bedingungen erfüllt ist:
>
> ```
> - Upgrading the setup from Citrix ADC 13.0 76.x build to
>   Citrix ADC 13.0 79.x build.
> - Restarting the CCO node in a cluster setup running Citrix
>   ADC 13.0 76.x build.
> ```
>
> Problemumgehungen:
>
> ```
> \- Vor dem Upgrade eines Cluster-Setups von Citrix ADC 13.0
>    76.x Build auf Citrix ADC 13.0 79.x Build muss der globale
>    Parameter der maximalen Verbindung (MaxConn) auf Null
>    gesetzt werden. Nach dem Upgrade des Setups können Sie den
>    MaxConn-Parameter auf einen gewünschten Wert setzen und dann
>     die Konfiguration speichern.
> \- Citrix ADC 13.0 76.x Build ist nicht für Cluster-Setups
>    geeignet. Citrix empfiehlt, den Citrix ADC 13.0 76.x Build
>    nicht für ein Cluster-Setup zu verwenden.
> ```


- In einem Cluster-Setup stürzt eine Citrix ADC Appliance möglicherweise ab, wenn:

```
- upgrading the setup from Citrix ADC 13.0 47.x or 13.0 52.x
  build to a later build, or
- upgrading the setup to Citrix ADC 13.0 47.x or 13.0 52.x
  build
```

Problemumgehung: Führen Sie während des Upgrade-Vorgangs die folgenden Schritte aus:

```
\- Deaktivieren Sie alle Clusterknoten und aktualisieren Sie
  dann jeden Clusterknoten.
\- Aktivieren Sie alle Clusterknoten, nachdem alle Knoten
  aktualisiert wurden.
```

Punkte, die vor dem Upgrade oder Herabstufen des Clusters zu beachten sind

- Sie können keine Clusterknoten hinzufügen, während Sie die Cluster-Softwareversion aktualisieren oder herabstufen.
- Sie können Konfigurationen auf Knotenebene über die NSIP-Adresse einzelner Knoten durchführen. Stellen Sie sicher, dass Sie die gleichen Konfigurationen auf allen Knoten durchführen, um sie synchron zu halten.
- Sie können den `start nstrace` Befehl nicht von der Cluster-IP-Adresse aus ausführen, wenn der Cluster aktualisiert wird. Sie können jedoch die Spur einzelner Knoten abrufen, indem Sie diesen Vorgang auf einzelnen Clusterknoten mit ihrer NSIP-Adresse ausführen.
- Citrix ADC 13.0 76.x Build ist nicht für Cluster-Setups geeignet. Citrix empfiehlt, den Citrix ADC 13.0 76.x Build nicht für ein Cluster-Setup zu verwenden.
- Citrix ADC 13.0 47.x- und 13.0 52.x-Builds sind nicht für ein Cluster-Setup geeignet. Dies liegt daran, dass die Kommunikation zwischen den Knoten in diesen Builds nicht kompatibel ist.
- Wenn ein Cluster aktualisiert wird, ist es möglich, dass für die aktualisierten Knoten einige zusätzliche Funktionen aktiviert sind, die auf den Knoten, die noch nicht aktualisiert wurden, nicht verfügbar sind. Dies führt zu einer Warnung zur Nichtübereinstimmung der Lizenz, während der Cluster aktualisiert wird. Diese Warnung wird automatisch behoben, wenn alle Cluster-Knoten aktualisiert werden.

Wichtig

- Citrix empfiehlt, dass Sie warten, bis der vorherige Knoten aktiv wird, bevor Sie den näch-

> sten Knoten aktualisieren oder herunterstufen.
>
> - Citrix empfiehlt, dass der Clusterkonfigurationsknoten zuletzt aktualisiert/heruntergestuft werden muss, um mehrere Verbindungsabbrüche von Cluster-IP-Sitzungen zu vermeiden.

So aktualisieren oder Downgrade der Software der Clusterknoten

1. Stellen Sie sicher, dass der Cluster stabil ist und die Konfigurationen auf allen Knoten synchronisiert sind.
2. Greifen Sie über die NSIP-Adresse auf jeden Knoten zu, und führen Sie die folgenden Schritte aus:
   - Aktualisieren oder Herabstufen des Clusterknotens. Ausführliche Informationen zum Upgrade und Downgrade der Software einer Appliance finden Sie unter Upgrade und Downgrade einer NetScaler Appliance.
   - Speichern Sie die Konfigurationen.
   - Starten Sie die Appliance neu.
3. Wiederholen Sie Schritt 2 für jeden der anderen Clusterknoten.

Auf einzelnen Clusterknoten unterstützte Vorgänge

October 5, 2021

Citrix ADC Appliances, die Teil eines Clusters sind, können in der Regel nicht einzeln von ihrer NSIP-Adresse konfiguriert werden. Es gibt jedoch einige Vorgänge, die eine Ausnahme von dieser Regel darstellen. Diese Vorgänge werden, wenn sie von der NSIP-Adresse aus ausgeführt werden, nicht auf andere Clusterknoten übertragen.

Die Operationen sind:

- cluster instance (set | rm | enable | disable)
- cluster node (set | rm)
- ns trace (start | show | stop)
- interface (set | enable | disable)
- route (add | rm | set | unset)
- ARP (add | rm | send -all)
- force cluster sync
- sync cluster files
- deaktivieren NTP Sync
- save ns config

- reboot
- shutdown

Wenn Sie beispielsweise den Befehl `disable interface 1/1/1` von der NSIP-Adresse eines Clusterknotens ausführen, ist die Schnittstelle nur auf diesem Knoten deaktiviert. Da der Befehl nicht weitergegeben wird, bleibt die Schnittstelle 1/1/1 auf allen anderen Clusterknoten aktiviert.

Unterstützung für heterogene Cluster

October 5, 2021

Citrix ADC Appliance unterstützt einen heterogenen Cluster in einer Clusterbereitstellung. Ein heterogener Cluster umfasst Knoten unterschiedlicher Citrix ADC Hardware, und Sie können eine Kombination verschiedener Plattformen im selben Cluster haben.

> **Wichtig**
>
> Die Bildung oder Unterstützung eines heterogenen Clusters ist möglich und nur auf MPX-Hardwareplattformen beschränkt.

Die Unterstützung und Bildung des heterogenen Clusters hängen von bestimmten Citrix ADC Modellen ab. Die folgende Tabelle listet die Plattformen auf, die bei der Bildung eines heterogenen Clusters mit einer gleichen Anzahl von Paket-Engines unterstützt werden.

Anzahl der Paket-Engines	MPX-Hardwareplattformen	Unterstützte MPX-Hardwareplattformen zur Bildung eines heterogenen Clusters
5	MPX 11500	MPX 14020
7	MPX 11515	MPX 14040
9	MPX 11530	MPX 14060

In der folgenden Tabelle sind die Plattformen aufgeführt, die bei der Bildung eines heterogenen Clusters mit einer ungleichen Anzahl von Paket-Engines unterstützt werden.

Hardware-Plattformen	Unterstützte Hardwareplattformen zur Bildung eines heterogenen Clusters
MPX 150XX	MPX 140XX

Weitere Informationen zur Bildung einer heterogenen Clusterbereitstellung von Citrix ADC MPX-Appliances mit der unterschiedlichen Anzahl von Paket-Engines über verschiedene SSL-Chipsätze hinweg finden Sie im Abschnitt **Heterogene Clusterbereitstellungen** in der SSL-Offload-Konfiguration.

> **Hinweis**
>
> Vor Release 13.0 Build 47.x wird die folgende Fehlermeldung angezeigt, wenn Sie den Befehl "Cluster verbinden" von dem Knoten aus ausführen, der eine ungleiche Anzahl von Paket-Engines aufweist: "Nichtübereinstimmung der Anzahl aktiver PPEs zwischen CCO und lokalem Knoten".

Punkte zu beachten

1. Die zusätzliche Management-CPU-Einstellung muss auf allen Cluster-Knoten gleich sein.
2. Der neu hinzugefügte Knoten muss die gleiche Kapazität auf den Datenebenen und der Rückwandplatine aufweisen wie die der vorhandenen Clusterknoten.
3. Wenn gemischte Plattformgeräte vorhanden sind, die verschiedene Chiffre unterstützen, würde sich der Cluster auf eine gemeinsame Chiffre Liste einigen.

FAQ

October 5, 2021

Eine Liste der FAQ zum Thema Clustering.

Wie viele Citrix ADC Appliances können in einem einzelnen Citrix ADC Cluster aufgenommen werden?

Ein Citrix ADC-Cluster kann eine Appliance oder bis zu 32 Citrix ADC nCore Hardware oder virtuelle Appliances enthalten. Jeder dieser Knoten muss die unter Voraussetzungen für Clusterknotenangegebenen Kriterien erfüllen.

Kann eine Citrix ADC-Appliance Teil mehrerer Cluster sein?

Nein. Eine Citrix ADC Appliance kann nur zu einem Cluster gehören.

Was ist eine Cluster-IP-Adresse? Was ist seine Subnetzmaske?

Die Cluster-IP-Adresse ist die Verwaltungsadresse eines Citrix ADC-Clusters. Alle Clusterkonfigurationen müssen durch Zugriff auf den Cluster über diese Adresse ausgeführt werden. Die Subnetzmaske der Cluster-IP-Adresse ist auf 255.255.255.255 festgelegt.

Wie kann ich einen bestimmten Clusterknoten als Clusterkonfigurationskoordinator erstellen?

Um einen bestimmten Knoten manuell als Clusterkonfigurationskoordinator festzulegen, müssen Sie die Priorität dieses Knotens auf den niedrigsten numerischen Wert (höchste Priorität) festlegen. Um zu verstehen, lassen Sie uns einen Cluster mit drei Knoten betrachten, die die folgenden Prioritäten haben:

n1 - 29, n2 - 30, n3 - 31

Hier ist n1 der Konfigurationskoordinator. Wenn Sie n2 zum Konfigurationskoordinator machen möchten, müssen Sie seine Priorität auf einen Wert festlegen, der niedriger als n1 ist, z. B. 28. Beim Speichern der Konfiguration wird n2 zum Konfigurationskoordinator.

> **Hinweis:**
>
> n2 mit seinem ursprünglichen Prioritätswert von 30 wird der Konfigurationskoordinator, wenn n1 ausfällt. Der Knoten mit dem nächstniedrigsten Prioritätswert wird ausgewählt, falls der Konfigurationskoordinator ausfällt.

Warum werden die Netzwerkschnittstellen eines Clusters in 3-Tupel-Notation (n/u/c) anstelle der regulären 2-Tupel-Notation (u/c) dargestellt?

Wenn eine Citrix ADC Appliance Teil eines Clusters ist, müssen Sie in der Lage sein, den Knoten zu identifizieren, zu dem die Schnittstelle gehört. Daher wird die Netzwerkschnittstellennamenskonvention für Clusterknoten von u/c in n/u/c geändert, wobei n die Knoten-ID bezeichnet.

Wie kann ich den Hostnamen für einen Cluster-Knoten festlegen?

Der Hostname eines Clusterknotens muss angegeben werden, indem der Befehl **set ns hostname** über die Cluster-IP-Adresse ausgeführt wird. Um beispielsweise den Hostnamen des Clusterknotens mit ID 2 festzulegen, lautet der Befehl:

set ns hostname hostName1 -**ownerNode** 2

Kann ich Citrix ADC-Appliances automatisch erkennen, damit ich sie einem Cluster hinzufügen kann?

Ja. Mit dem Konfigurationsdienstprogramm können Sie Appliances ermitteln, die sich im selben Subnetz wie die NSIP-Adresse des Konfigurationskoordinators befinden. Weitere Informationen finden Sie unter Discovering NetScaler Appliances.

Ist die Traffic Serving-Funktion eines Clusters betroffen, wenn ein Knoten entfernt oder deaktiviert wird, neu gestartet oder heruntergefahren oder inaktiv gemacht wird?

Ja. Wenn einer dieser Vorgänge auf einem aktiven Knoten des Clusters ausgeführt wird, hat der Cluster einen Knoten weniger, um den Datenverkehr zu bedienen. Außerdem werden vorhandene Verbindungen auf diesem Knoten beendet.

Ich habe mehrere eigenständige Appliances, von denen jede unterschiedliche Konfigurationen hat. Kann ich sie einem einzelnen Cluster hinzufügen?

Ja. Sie können Appliances mit unterschiedlichen Konfigurationen zu einem einzelnen Cluster hinzufügen. Wenn die Appliance jedoch dem Cluster hinzugefügt wird, werden die vorhandenen Konfigurationen gelöscht. Um die Konfigurationen zu verwenden, die für die einzelnen Appliances verfügbar sind, müssen Sie:

1. Erstellen Sie eine einzelne Datei *.conf für alle Konfigurationen.
2. Bearbeiten Sie die Konfigurationsdatei, um Features zu entfernen, die in einer Clusterumgebung nicht unterstützt werden.
3. Aktualisieren Sie die Namenskonvention von Schnittstellen vom 2-Tupel-Format (u/c) in das 3-Tupel-Format (n/u/c).
4. Wenden Sie die Konfigurationen mit dem Batch-Befehl auf den Konfigurationskoordinatorknoten des Clusters an.

Kann ich die Konfigurationen einer eigenständigen Citrix ADC-Appliance oder eines HA-Setups zum Cluster-Setup migrieren?

Nein. Wenn ein Knoten zu einem Cluster-Setup hinzugefügt wird, werden seine Konfigurationen implizit mit dem Befehl **clear ns config** (mit der **erweiterten** Option) gelöscht. Darüber hinaus werden die SNIP-Adressen und alle VLAN-Konfigurationen (außer Standard-VLAN und NSVLAN) gelöscht. Daher wird empfohlen, die Konfigurationen zu sichern, bevor Sie die Appliance zu einem Cluster hinzufügen. Bevor Sie die gesicherte Konfigurationsdatei für den Cluster verwenden, müssen Sie:

1. Bearbeiten Sie die Konfigurationsdatei, um Features zu entfernen, die in einer Clusterumgebung nicht unterstützt werden.
2. Aktualisieren Sie die Namenskonvention von Schnittstellen vom Zwei-Tupel-Format (x/y) in das Drei-Tupel-Format (x/y/z).
3. Wenden Sie die Konfigurationen mit dem **Batch-Befehl** auf den Konfigurationskoordinatorknoten des Clusters an.

Sind Backplane-Schnittstellen Teil der L3-VLANs?

Ja, standardmäßig sind Backplane-Schnittstellen auf allen L3-VLANs vorhanden, die im Cluster konfiguriert sind.

Wie kann ich einen Cluster konfigurieren, der Knoten aus verschiedenen Netzwerken enthält?

> **Hinweis:**
>
> Unterstützt ab NetScaler 11.0.

Ein Cluster, der Knoten aus verschiedenen Netzwerken enthält, wird als L3-Cluster (manchmal als Cluster im INC-Modus bezeichnet) bezeichnet. In einem L3-Cluster müssen alle Knoten, die zu einem einzelnen Netzwerk gehören, in einer einzelnen Knotengruppe gruppiert sein. Wenn ein Cluster jeweils zwei Knoten aus drei verschiedenen Netzwerken enthält, müssen Sie daher 3 Knotengruppen (eine für jedes Netzwerk) erstellen und jede dieser Knotengruppen mit den Knoten verknüpfen, die zu diesem Netzwerk gehören. Informationen zur Konfiguration finden Sie in den Schritten zum Einrichten eines Clusters.

Wie kann ich das NSVLAN auf einem Cluster konfigurieren/aufheben?

Führen Sie einen der folgenden Schritte aus:

- Um das NSVLAN in einem Cluster verfügbar zu machen, stellen Sie sicher, dass für jede Appliance dasselbe NSVLAN konfiguriert ist, bevor es zu einem Cluster hinzugefügt wird.
- Um das NSVLAN von einem Clusterknoten zu entfernen, entfernen Sie zuerst den Knoten aus dem Cluster, und löschen Sie dann das NSVLAN aus der Appliance.

Ich habe einen Cluster eingerichtet, bei dem einige Citrix ADC -Knoten nicht mit dem externen Netzwerk verbunden sind. Kann der Cluster immer noch normal funktionieren?

Ja. Der Cluster unterstützt einen Mechanismus namens Linksets, der es nicht verbundenen Knoten ermöglicht, Datenverkehr mithilfe der Schnittstellen von verbundenen Knoten zu bedienen. Die nicht verbundenen Knoten kommunizieren über die Cluster-Backplane mit den verbundenen Knoten. Weitere Informationen finden Sie unter Verwenden von Linksets.

Wie können Bereitstellungen, die eine MAC-basierte Weiterleitung (MBF) erfordern, in einem Cluster-Setup unterstützt werden?

Bereitstellungen, die MBF verwenden, müssen Linksets verwenden. Weitere Informationen finden Sie unter Verwenden von Linksets.

Kann ich Befehle von der NSIP-Adresse eines Cluster-Knotens ausführen?

Nein. Der Zugriff auf einzelne Clusterknoten über die NSIP-Adressen ist schreibgeschützt. Wenn Sie sich an der NSIP-Adresse eines Clusterknotens anmelden, können Sie daher nur die Konfigurationen und die Statistiken anzeigen. Sie können nichts konfigurieren. Es gibt jedoch einige Vorgänge, die Sie von der NSIP-Adresse eines Clusterknotens ausführen können. Weitere Informationen finden Sie unter Auf einzelnen Knoten unterstützte Vorgänge.

Kann ich die Konfigurationsverbreitung zwischen Clusterknoten deaktivieren?

Nein, Sie können die Weitergabe von Clusterkonfigurationen zwischen Clusterknoten nicht explizit deaktivieren. Während eines Software-Upgrades oder Downgrades kann ein Versionsfehler die Konfigurationspropagierung jedoch automatisch deaktivieren.

Kann ich die NSIP-Adresse ändern oder das NSVLAN einer Citrix ADC Appliance ändern, wenn sie Teil des Clusters ist?

Nein. Um solche Änderungen vorzunehmen, müssen Sie zuerst die Appliance aus dem Cluster entfernen, die Änderungen vornehmen und dann die Appliance dem Cluster hinzufügen.

Unterstützt der Citrix ADC Cluster L2- und L3-VLANs?

Ja. Ein Cluster unterstützt VLANs zwischen Clusterknoten. Die VLANs müssen für die Cluster-IP-Adresse konfiguriert sein.

- **L2-VLAN.** Sie können ein Layer2-VLAN erstellen, indem Sie Schnittstellen binden, die zu verschiedenen Knoten des Clusters gehören.
- **L3-VLAN.** Sie können ein Layer3-VLAN erstellen, indem Sie IP-Adressen binden, die zu verschiedenen Knoten des Clusters gehören. Die IP-Adressen müssen zum selben Subnetz gehören. Stellen Sie sicher, dass eines der folgenden Kriterien erfüllt ist. Andernfalls können die L3-VLAN-Bindungen fehlschlagen.
  - Alle Knoten haben eine IP-Adresse im selben Subnetz wie das an das VLAN gebundene Subnetz.
  - Der Cluster verfügt über eine gestreifte IP-Adresse, und das Subnetz dieser IP-Adresse ist an das VLAN gebunden.

Wenn Sie einen Knoten zu einem Cluster hinzufügen, der nur IPs erkannt hat, erfolgt die Synchronisierung, bevor gepunktete IP-Adressen diesem Knoten zugewiesen werden. In solchen Fällen können L3-VLAN-Bindungen verloren gehen. Um diesen Verlust zu vermeiden, fügen Sie entweder eine gestreifte IP hinzu oder fügen Sie die L3-VLAN-Bindungen auf dem NSIP des neu hinzugefügten Knotens hinzu.

Wie kann ich SNMP auf einem Citrix ADC-Cluster konfigurieren?

SNMP überwacht den Cluster und alle Knoten des Clusters auf die gleiche Weise wie eine eigenständige Appliance. Der einzige Unterschied besteht darin, dass SNMP auf einem Cluster über die Cluster-IP-Adresse konfiguriert werden muss. Beim Generieren hardwarespezifischer Traps sind zwei weitere Varbinds enthalten, um den Knoten des Clusters zu identifizieren: Knoten-ID und NSIP-Adresse des Knotens.

Welche Details muss ich zur Verfügung haben, wenn ich mich bei Clusterproblemen an den technischen Support wende?

Die Citrix ADC Appliance bietet einen **Clusterbefehl show techsupport -scope**, der Konfigurationsdaten, statistische Informationen und Protokolle aller Clusterknoten extrahiert. Führen Sie diesen Befehl für die Cluster-IP-Adresse aus.

Die Ausgabe dieses Befehls wird in einer Datei namens **collector_cluster_ <nsip_CCO> _P_ <date-timestamp> .tar.gz gespeichert, die im Verzeichnis */var/tmp/support/cluster/* des Konfigurationskoordinators verfügbar ist.

Senden Sie dieses Archiv an das technische Support-Team, um das Problem zu beheben.

Kann ich Striped IP-Adressen als Standard-Gateway von Servern verwenden?

Stellen Sie bei Clusterbereitstellungen sicher, dass das Standard-Gateway des Servers auf eine gestreifte IP-Adresse verweist (wenn Sie eine IP-Adresse im Besitz von Citrix ADC verwenden). Bei LB-Bereitstellungen mit aktiviertem USIP muss das Standard-Gateway beispielsweise eine gestreifte SNIP-Adresse sein.

Kann ich die Routing-Konfigurationen eines bestimmten Clusterknotens von der Cluster-IP-Adresse aus anzeigen?

Ja. Sie können die für einen Knoten spezifischen Konfigurationen anzeigen und löschen, indem Sie den Besitzerknoten angeben, während Sie die VTYSH-Shell eingeben.

Um beispielsweise die Ausgabe eines Befehls auf den Knoten 0 und 1 anzuzeigen, lautet der Befehl wie folgt:

```
\> vtysh
ns# owner-node 0 1
ns(node-0 1)\# show cluster state
ns(node-0 1)\# exit-cluster-node
ns\#
```


Wie kann ich den Knoten angeben, für den ich die LACP-Systempriorität festlegen möchte?

> **Hinweis:**
>
> Unterstützt ab NetScaler 10.1.

In einem Cluster müssen Sie diesen Knoten mithilfe des Befehls **set lacp** als Besitzerknoten festlegen.

Beispiel: Solegen Sie die LACP-Systempriorität für einen Knoten mit ID 2 fest:

```
set lacp -sysPriority 5 -ownerNode 2<!--NeedCopy-->
```

Wie werden IP-Tunnel in einem Cluster-Setup konfiguriert?

> **Hinweis:**
>
> Unterstützt ab NetScaler 10.1.

Das Konfigurieren von IP-Tunneln in einem Cluster ist identisch mit einer eigenständigen Appliance. Der einzige Unterschied besteht darin, dass bei einem Cluster-Setup die lokale IP-Adresse eine Striped SNIP-Adresse sein muss.

Wie kann ich einen Failover Interface Set (FIS) auf den Knoten eines Citrix ADC Clusters hinzufügen?

> **Hinweis:**
>
> Unterstützt ab NetScaler 10.5.

Geben Sie unter der Cluster-IP-Adresse die ID des Clusterknotens an, dem die FIS hinzugefügt werden muss. Verwenden Sie dazu den folgenden Befehl:

```
add fis <name> -ownerNode <nodeId>
```

> **Hinweise**
>
> - Der FIS Name für jeden Clusterknoten muss eindeutig sein.
> - Ein Cluster LA-Kanal kann zu einer FIS hinzugefügt werden. Sie stellen sicher, dass der Cluster-LA-Kanal über eine lokale Schnittstelle als Mitgliederschnittstelle verfügt.

Weitere Informationen zu FIS finden Sie unter Konfigurieren des Failover-Interface-Sets.

Wie werden Netzprofile in einem Cluster-Setup konfiguriert?

> **Hinweis:**
>
> Unterstützt ab NetScaler 10.5.

Sie können Spotted-IP-Adressen an ein Netzprofil binden. Dieses Netzprofil kann dann an einen virtuellen Spotted Load Balancing-Server oder -Dienst (der mit einer Knotengruppe definiert wird)

gebunden werden. Die folgenden Empfehlungen müssen befolgt werden, andernfalls werden die Netzprofilkonfigurationen nicht berücksichtigt und die USIP/USNIP-Einstellungen verwendet werden:

> **Hinweis:**
>
> - Wenn der **strenge** Parameter der Knotengruppe auf **Ja**festgelegt ist, muss das Netzprofil mindestens eine IP-Adresse von jedem Knotengruppenmitglied enthalten.
> - Wenn der **strenge** Parameter der Knotengruppe auf **Nein**festgelegt ist, muss das Netzprofil mindestens eine IP-Adresse von jedem der Clusterknoten enthalten.

Wie kann ich WIonNS in einem Cluster-Setup konfigurieren?

> **Hinweis:**
>
> Unterstützt ab NetScaler 11.0 Build 62.x.

Um WIonNS auf einem Cluster zu verwenden, müssen Sie Folgendes tun:

1. Stellen Sie sicher, dass das Java-Paket und das WI-Paket in demselben Verzeichnis auf allen Clusterknoten vorhanden sind.
2. Erstellen Sie einen virtuellen Lastausgleichsserver, auf dem Persistenz konfiguriert ist.
3. Erstellen Sie Dienste mit IP-Adressen als NSIP-Adresse aller Clusterknoten, für die Sie den WI-Datenverkehr bereitstellen möchten. Dieser Schritt kann nur mit der Citrix ADC CLI konfiguriert werden.
4. Binden Sie die Dienste an den virtuellen Lastenausgleichsserver.

> **Hinweis:**
>
> Wenn Sie WIonNS über eine VPN-Verbindung verwenden, stellen Sie sicher, dass der virtuelle Lastausgleichsserver als WIHOME festgelegt ist.

Kann der Cluster LA-Kanal für den Verwaltungszugriff verwendet werden?

Nein. Der Verwaltungszugriff auf einen Clusterknoten darf nicht auf einem Cluster-LA-Kanal (z. B. CLA/1) oder seinen Mitgliedsschnittstellen konfiguriert werden. Dies liegt daran, dass, wenn der Knoten INACTIVE ist, die entsprechende Cluster-LA-Schnittstelle als Herunterfahren gekennzeichnet ist und daher den Verwaltungszugriff verliert.

Wie kommunizieren Clusterknoten miteinander und was sind die verschiedenen Arten von Datenverkehr, die durch die Backplane laufen?

Eine Backplane ist ein Satz von Schnittstellen, bei denen eine Schnittstelle jedes Knotens mit einem gemeinsamen Switch verbunden ist, der als Cluster-Backplane-Switch bezeichnet wird. Die

verschiedenen Arten von Datenverkehr, die durch eine Backplane laufen, die von der Internode-Kommunikation verwendet wird, sind:

- Knoten-zu-Knoten-Messaging (NNM)
- Gelenkter Verkehr
- Konfigurationspropagierung und Synchronisierung

Jeder Knoten des Clusters verwendet eine spezielle MAC-Cluster-Backplane-Switch-Adresse, um mit anderen Knoten über die Backplane zu kommunizieren. Der Cluster-Spezial-MAC hat die Form: **0x02 0x00 0x6F**<cluster_id> <node_id> <reserved>, wobei <cluster_id> die Clusterinstanz-ID ist. Der <node_id> ist die Knotennummer der Citrix ADC Appliance, die zu einem Cluster hinzugefügt wird.

> **Hinweis:**
>
> Die Menge an Datenverkehr, die von einer Backplane abgewickelt wird, hat einen vernachlässigbaren CPU-Overhead.

Was wird über den GRE-Tunnel für den Layer-3-Cluster geleitet?

Nur der gelenkte Datenverkehr geht über den GRE-Tunnel. Die Pakete werden durch den GRE-Tunnel zum Knoten im anderen Subnetz geleitet.

Wie werden Node to Node Messaging (NNM) und Heartbeat-Nachrichten ausgetauscht und wie werden sie weitergeleitet?

NNM-, Heartbeat-Meldungen und Clusterprotokoll sind nicht steuernden Datenverkehr. Diese Nachrichten werden nicht durch den Tunnel gesendet, sondern direkt weitergeleitet.

Was sind die Empfehlungen der MTU, wenn Jumbo-Frames für den Tunnelverkehr mit Layer 3 Cluster aktiviert sind?

Im Folgenden sind die Layer-3-Clusterempfehlungen der Jumbo MTU über den GRE-Tunnel aufgeführt:

- Die Jumbo-MTU kann zwischen Clusterknoten über den L3-Pfad konfiguriert werden, um den GRE-Tunnel-Overhead zu unterstützen.
- Die Fragmentierung findet nicht bei Paketen in voller Größe statt, die gesteuert werden müssen.
- Die Steuerung des Verkehrs funktioniert weiterhin, auch wenn Jumbo-Frames nicht erlaubt sind, aber mit mehr Overhead aufgrund von Fragmentierung.

Wie wird der globale Hash-Schlüssel generiert und über alle Knoten verteilt?

Die `rsskey` für eine Standalone-Appliance wird beim Booten generiert. In einem Cluster-Setup enthält der erste Knoten den `rsskey` des Clusters. Jeder neue Knoten, der dem Cluster beitritt, synchronisiert den `rsskey`.

Was ist der Bedarf an `set rsskeytype -rsskey symmetric` Befehl für*: *: *, USIP on, `useproxyport` off, Topologien?

Es ist nicht spezifisch für einen Cluster, gilt auch für eine eigenständige Appliance. Bei eingeschalteter USIP und deaktiviertem Proxy-Port `rsskey` reduziert symmetrisch sowohl die Kern- zu Core (C2C) -Lenkung als auch die Knoten-zu-Knotensteuerung.

Welche Faktoren tragen dazu bei, den CCO-Knoten zu verändern?

Der erste Knoten, der zu einem Cluster-Setup hinzugefügt wurde, wird zum Knoten des Konfigurationskoordinators (CCO). Die folgenden Faktoren tragen dazu bei, den CCO-Knoten im Cluster-Setup zu ändern:

- Wenn der aktuelle CCO-Knoten aus dem Cluster-Setup entfernt wird
- Wenn der aktuelle CCO-Knoten abstürzt
- Wenn die Priorität des Nicht-CCO-Knotens geändert wird (niedrigere Priorität hat einen höheren Vorrang)
- Unter dynamischen Bedingungen wie der Erreichbarkeit des Netzwerks zwischen den Knoten
- Wenn es Änderungen in den Knotenzuständen gibt - aktiv, spare und passiv. Aktive Knoten werden als CCO bevorzugt.
- Wenn es eine Änderung in der Konfiguration gibt und der Knoten mit der neuesten Konfiguration als CCO bevorzugt wird.

Problembehandlung beim Citrix ADC-Cluster

October 5, 2021

Wenn ein Fehler in einem Citrix ADC Cluster auftritt, besteht der erste Schritt bei der Fehlerbehebung darin, Informationen über die Clusterinstanz zu erhalten. Sie können die Informationen abrufen, indem Sie die `show cluster node nodeId` Befehle `show cluster instance clId` und auf den Cluster-Knoten ausführen.

Wenn Sie das Problem nicht finden können, indem Sie die beiden oben genannten Ansätze verwenden, können Sie einen der folgenden Methoden verwenden:

- **Isolieren Sie die Ursache des Fehlers.** Versuchen Sie, den Cluster zu umgehen, um den Server zu erreichen. Wenn der Versuch erfolgreich ist, liegt das Problem wahrscheinlich beim Cluster-Setup.
- **Überprüfen Sie die kürzlich ausgeführten Befehle.** Führen Sie den Verlaufsbefehl aus, um die zuletzt auf dem Cluster ausgeführten Konfigurationen zu überprüfen. Sie können auch die Datei ns.conf überprüfen, um die implementierten Konfigurationen zu überprüfen.
- **Überprüfen Sie die ns.log-Dateien.** Verwenden Sie die Protokolldateien, die im Verzeichnis /var/log/ jedes Knotens verfügbar sind, um die ausgeführten Befehle, den Status der Befehle und die Statusänderungen zu identifizieren.
- **Überprüfen Sie die newnslog-Dateien.** Verwenden Sie die `newnslog` Dateien, die im /var/nslog/-Verzeichnis jedes Knotens verfügbar sind, um die Ereignisse zu identifizieren, die auf den Clusterknoten aufgetreten sind. Sie können mehrere `newnslog` Dateien als eine einzige Datei anzeigen, indem Sie die Dateien in ein einzelnes Verzeichnis kopieren und dann den folgenden Befehl ausführen:

```
nsconmsg -K newnslog-node<id> -K     newnslog.node<id> -d current
```

Wenn Sie das Problem immer noch nicht lösen können, können Sie versuchen, die Pakete auf dem Cluster zu verfolgen oder den `techsupport -scope cluster` Befehl show zu verwenden. Sie können den Befehl verwenden, um den Bericht an das technische Support-Team zu senden.

Protokollierung der Pakete eines Citrix ADC-Clusters

October 5, 2021

Das Citrix ADC Betriebssystem bietet ein Dienstprogramm namens *ns trace*, um einen Dump der Pakete zu erhalten, die von einer Appliance empfangen und gesendet werden. Das Dienstprogramm speichert die Pakete in Ablaufverfolgungsdateien. Sie können diese Dateien verwenden, um Probleme im Fluss von Paketen zu den Clusterknoten zu debuggen. Die Trace-Dateien müssen mit der Wireshark-Anwendung angezeigt werden.

Einige hervorstechende Aspekte des ns-trace-Dienstprogramms sind:

- Kann so konfiguriert werden, dass Pakete selektiv mit klassischen Ausdrücken und Standardausdrücken verfolgt werden.
- Kann den Trace in mehreren Formaten erfassen: ns Trace Format (.cap) und TCP-Dump-Format (.pcap).

- Kann die Ablaufverfolgungsdateien aller Clusterknoten auf dem Konfigurationskoordinator aggregieren.
- Kann mehrere Trace-Dateien in einer einzigen Trace-Datei zusammenführen (nur für.cap-Dateien).

Sie können das ns-Trace-Dienstprogramm von der Citrix ADC Befehlszeile oder der Citrix ADC Shell verwenden.

So verfolgen Sie Pakete einer eigenständigen Appliance

Führen Sie den Befehl start ns trace auf der Appliance aus. Der Befehl erstellt Ablaufverfolgungsdateien im <date-timestamp> Verzeichnis /var/nstrace/. Die Namen der Trace-Dateien haben die Form nstrace.cap<id\ >.

Sie können den Status anzeigen, indem Sie den Befehl show ns trace ausführen. Sie können das Tracing der Pakete beenden, indem Sie den Befehl stop ns trace ausführen.

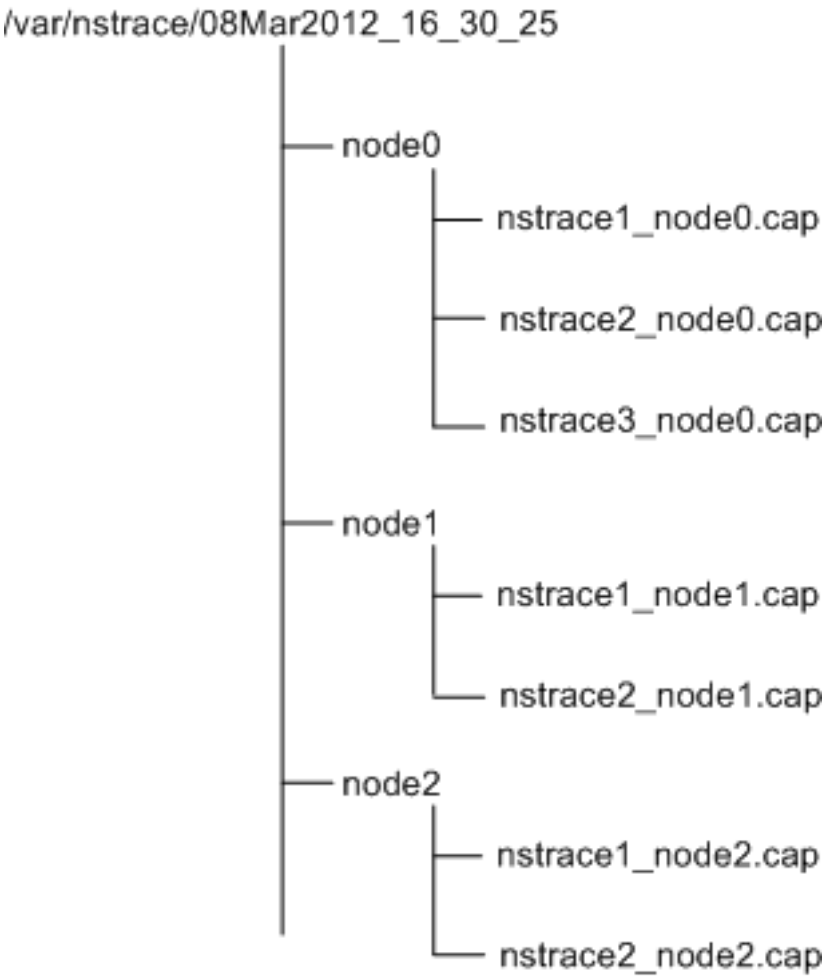
> **Hinweis:**
>
> Sie können das ns-Turn-Dienstprogramm auch von der Citrix ADC Shell aus ausführen, indem Sie die Datei
> nstrace.sh ausführen. Es wird jedoch empfohlen, das ns-Turn-Dienstprogramm über die Citrix ADC Befehlszeilenschnittstelle zu verwenden.

So verfolgen Sie Pakete eines Clusters

Sie können die Pakete auf allen Clusterknoten verfolgen und alle Ablaufverfolgungsdateien auf dem Konfigurationskoordinator abrufen.

Führen Sie den Befehl start ns trace für die Cluster-IP-Adresse aus. Der Befehl wird weitergegeben und auf allen Cluster-Knoten ausgeführt. Die Trace-Dateien werden in einzelnen Cluster-Knoten im<date-timestamp> Verzeichnis /var/nstrace/ gespeichert. Die Namen der Trace-Dateien haben die Form nstrace <id> _node.cap<id\ >.

Sie können die Ablaufverfolgungsdateien jedes Knotens verwenden, um die Knoten Operationen zu debuggen. Wenn Sie jedoch die Trace-Dateien aller Cluster-Knoten an einem Ort haben möchten, müssen Sie den Befehl stop ns trace für die Cluster-IP-Adresse ausführen. Die Trace-Dateien aller Knoten werden wie folgt auf dem Cluster-Konfigurationskoordinator im<date-timestamp> Verzeichnis /var/nstrace/ heruntergeladen:



Mehrere Trace-Dateien zusammenführen

Sie können eine einzelne Datei aus den Trace-Dateien vorbereiten (nur für unterstützt. Cap-Dateien), die von den Clusterknoten erhalten werden. Die einzelnen Ablaufverfolgungsdateien geben Ihnen eine kumulative Ansicht der Ablaufverfolgung der Clusterpakete. Die Ablaufverfolgungseinträge in der einzelnen Ablaufverfolgungsdatei werden basierend auf der Zeit sortiert, an der die Pakete auf dem Cluster empfangen wurden.

Um die Ablaufverfolgungsdateien zusammenzuführen, geben Sie in der Citrix ADC-Shell Folgendes ein:

```
1 > nstracemerge.sh -srcdir \<DIR\> -dstdir \<DIR\> -filename \<name\> -
    filesize \<num\>
```

Hierbei gilt:

- `srcdir` ist das Verzeichnis, aus dem die Trace-Dateien zusammengeführt werden. Alle Trace-Dateien in diesem Verzeichnis werden in einer einzigen Datei zusammengeführt.
- `dstdir` ist das Verzeichnis, in dem die zusammengeführte Trace-Datei erstellt wird.
- `Filename` ist der Name der erstellten Trace-Datei.
- `Filesize` ist die Größe der Trace-Datei.

Beispiele

Im Folgenden finden Sie einige Beispiele für die Verwendung des ns-Trace-Dienstprogramms zum Filtern von Paketen.

- So verfolgen Sie die Pakete auf den Backplane-Schnittstellen von drei Knoten:

  Klassische Ausdrücke verwenden:

```
1  > start nstrace -filter "INTF == 0/1/1 && INTF == 1/1/1 && INTF
     == 2/1/1"
```

  Standardausdrücke verwenden:

```
1  > start nstrace -filter "CONNECTION.INTF.EQ("0/1/1") &&
     CONNECTION.INTF.EQ("1/1/1") && CONNECTION.INTF.EQ("2/1/1")"
```

- So verfolgen Sie die Pakete von einer Quell-IP-Adresse 10.102.34.201 oder von einem System, dessen Quellport größer als 80 ist und der Dienstname nicht "s1" lautet:

  Verwenden klassischer Ausdrücke

```
1  > start nstrace -filter "SOURCEIP == 10.102.34.201 || (SVCNAME !=
     s1 && SOURCEPORT > 80)"
```

  Verwenden von Standardausdrücken

```
1  > start nstrace -filter "CONNECTION.SRCIP.EQ(10.102.34.201) || (
     CONNECTION.SVCNAME.NE("s1") && CONNECTION.SRCPORT.GT(80))"
```

> **Hinweis:**
>
> Weitere Informationen zu Filtern, die in ns trace verwendet werden, finden Sie unter ns trace.

Erfassen von SSL-Sitzungsschlüsseln während einer Ablaufverfolgung

Wenn Sie den Befehl “start ns trace” ausführen, können Sie den neuen `capsslkeys` Parameter festlegen, um die SSL-Hauptschlüssel für alle SSL-Sitzungen zu erfassen. Wenn Sie diesen Parameter einschließen, wird zusammen mit der Paketverfolgung eine Datei namens nstrace.sslkeys generiert. Diese Datei kann in Wireshark importiert werden, um den SSL-Datenverkehr in der entsprechenden Trace-Datei zu entschlüsseln.

Diese Funktionalität ähnelt Webbrowsern, die Sitzungsschlüssel exportieren, die später in Wireshark importiert werden können, um SSL-Datenverkehr zu entschlüsseln.

Vorteile der Verwendung von SSL-Sitzungsschlüsseln

Im Folgenden sind die Vorteile der Verwendung von SSL-Sitzungsschlüsseln:

1. Generiert kleinere Ablaufverfolgungsdateien, die nicht die zusätzlichen Pakete enthalten, die im SSLPLAIN Modus der Erfassung erstellt wurden.
2. Bietet die Möglichkeit, Klartext [SP (1] aus der Ablaufverfolgung anzuzeigen und auszuwählen, ob die Hauptschlüsseldatei freigeben oder vertrauliche Daten geschützt werden soll, indem sie nicht freigegeben wird.

Einschränkungen bei der Verwendung von SSL-Sitzungsschlüsseln

Im Folgenden sind die Einschränkungen der Verwendung von SSL-Sitzungsschlüsseln:

1. SSL-Sitzungen können nicht entschlüsselt werden, wenn die anfänglichen Pakete der Sitzung nicht erfasst werden.
2. SSL-Sitzungen können nicht erfasst werden, wenn der FIPS-Modus (Federal Information Processing Standard) aktiviert ist.

So erfassen Sie SSL-Sitzungsschlüssel mit der Befehlszeilenschnittstelle (CLI)

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um SSL-Sitzungsschlüssel in einer Ablaufverfolgungsdatei zu aktivieren oder zu deaktivieren und den Ablaufverfolgungsvorgang zu überprüfen.

```
1 > start nstrace -capsslkeys ENABLED
2 > show nstrace
3 Example
4 > start nstrace -capsslkeys ENABLED
5 > show nstrace
```



```
6       State:  RUNNING          Scope:  LOCAL            TraceLocation:
            "/var/nstrace/04May2016_17_51_54/..."
7       Nf:  24                  Time:  3600              Size:  164
                        Mode:  TXB NEW_RX
8       Traceformat:  NSCAP      PerNIC:  DISABLED        FileName:  04
           May2016_17_51_54 Link:  DISABLED
9       Merge:  ONSTOP           Doruntimecleanup:  ENABLED TraceBuffers:
             5000      SkipRPC:  DISABLED
10      SkipLocalSSH:  DISABLED  Capsslkeys:  ENABLED     InMemoryTrace:
            DISABLED
11  Done
```

So konfigurieren Sie SSL-Sitzungsschlüssel über die Citrix ADC GUI

1. Navigieren Sie zu **Konfiguration > System > Diagnose > Technischer Support Tools**, und klicken Sie auf **Neue Ablaufverfolgung starten**, um mit der Verfolgung verschlüsselter Pakete auf einer Appliance zu beginnen.
2. Aktivieren Sie auf der Seite **Trace starten** das Kontrollkästchen **SSL-Masterschlüssel erfassen**.
3. Klicken Sie auf **OK** und **Fertig**.

So importieren Sie die SSL-Master Keys in Wireshark

Navigieren Sie auf der Wireshark GUI zu **Bearbeiten > Voreinstellungen > Protokolle > SSL > (Pre) -Master-Secret Protokolldateiname und geben Sie die Masterschlüsseldateien** an, die von der Appliance erhalten wurden.

Problembehandlung häufiger Probleme

April 25, 2022

Beim Verbinden eines Knotens zum Cluster erhalte ich folgende Meldung: “FEHLER: Ungültiger Schnittstellenname/Nummer. “ Was muss ich tun, um diesen Fehler zu beheben?

Der genannte Fehler tritt auf, wenn Sie eine ungültige oder falsche Backplane-Schnittstelle angegeben haben, während Sie den Befehl ”Clusterknoten hinzufügen” zum Hinzufügen des Knotens verwendet haben. Um diesen Fehler zu beheben, überprüfen Sie die Schnittstelle, die Sie beim Hinzufügen des Knotens angegeben haben. Stellen Sie sicher, dass Sie die Verwaltungsschnittstelle der Appliance nicht als Backplane-Schnittstelle angegeben haben und dass das Bit <nodeId> der Schnittstelle

mit der ID des Knotens übereinstimmt. Wenn die nodeID beispielsweise 3 ist, muss die Backplane-Schnittstelle 3/<c>/sein<u>.

Beim Verbinden eines Knotens zum Cluster erhalte ich folgende Meldung: “FEHLER: Clustering kann nicht aktiviert werden, da der lokale Knoten kein Mitglied des Clusters ist. “ Was muss ich tun, um diesen Fehler zu beheben?

Dieser Fehler tritt auf, wenn Sie versuchen, einen Knoten zu verbinden, ohne das NSIP des Knotens zum Cluster hinzuzufügen. Um diesen Fehler zu beheben, müssen Sie zuerst die NSIP-Adresse des Knotens dem Cluster hinzufügen hinzufügen, indem Sie den Befehl “ **Clusterknoten hinzufügen** “ verwenden und dann den Befehl “ **Cluster beitreten** “ ausführen.

Beim Verbinden eines Knotens zum Cluster erhalte ich folgende Meldung: “FEHLER: Verbindung verweigert. “ Was muss ich tun, um diesen Fehler zu beheben?

Dieser Fehler kann aus folgenden Gründen auftreten:

- **Verbindungsprobleme.** Der Knoten kann keine Verbindung zur Cluster-IP-Adresse herstellen. Versuchen Sie, die Cluster-IP-Adresse von dem Knoten zu pingen, dem Sie beitreten möchten.
- **Duplizierte Cluster-IP-Adresse.** Überprüfen Sie, ob die Cluster-IP-Adresse auf einem Nicht-Clusterknoten vorhanden ist. Wenn dies der Fall ist, erstellen Sie eine Cluster-IP-Adresse und versuchen Sie, dem Cluster wieder beizutreten.

Beim Verbinden eines Knotens mit dem Cluster erhalte ich die folgende Meldung: FEHLER: Lizenzkonflikt zwischen dem Konfigurationskoordinator und dem lokalen Knoten. Was muss ich tun, um diesen Fehler zu beheben?

Die Appliance, die Sie dem Cluster beitreten, muss über die gleichen Lizenzen wie der Konfigurationskoordinator verfügen. Dieser Fehler tritt auf, wenn die Lizenzen auf dem Knoten, dem Sie beitreten, nicht mit den Lizenzen auf dem Konfigurationskoordinator übereinstimmen. Um diesen Fehler zu beheben, führen Sie die folgenden Befehle auf beiden Knoten aus und vergleichen Sie die Ausgaben.

Von der Befehlszeile aus:

- `show ns hardware`
- `show ns license`

Aus der Schale:

- `nsconmsg -g feature -d stats`
- `ls /nsconfig/license`

- Anzeigen des Inhalts der Datei /var/log/license.log

Was muss ich tun, wenn die Konfigurationen eines Clusterknotens nicht mit den Clusterkonfigurationen synchronisiert sind?

Normalerweise werden die Konfigurationen automatisch zwischen allen Clusterknoten synchronisiert. Wenn Sie jedoch der Meinung sind, dass die Konfigurationen auf einem bestimmten Knoten nicht synchronisiert sind, müssen Sie die Synchronisierung erzwingen, indem Sie den Befehl force cluster sync von dem Knoten ausführen, den Sie synchronisieren möchten. Weitere Informationen finden Sie unter Clusterkonfigurationen synchronisieren.

Wenn Sie einen Clusterknoten konfigurieren, erhalte ich die folgende Meldung: “FEHLER: Sitzung ist schreibgeschützt; verbinden Sie sich mit der Cluster-IP-Adresse, um die Konfiguration zu ändern. “

Alle Konfigurationen auf einem Cluster müssen über die Cluster-IP-Adresse erfolgen, und die Konfigurationen werden an die anderen Clusterknoten weitergegeben. Alle Sitzungen, die über die NSIP-Adresse einzelner Knoten eingerichtet werden, sind schreibgeschützt.

Warum zeigt der Knotenstatus “INACTIVE” an, wenn der Knotenzustand “UP” anzeigt?

Ein fehlerweiter Knoten kann sich aus verschiedenen Gründen im Status INACTIVE befinden. Ein Scan der ns.log oder Fehlerzähler kann Ihnen helfen, den genauen Grund zu ermitteln.

Wie kann ich den Zustand eines Knotens auflösen, wenn sein Zustand NICHT UP anzeigt?

Knotenintegrität “**Nicht UP**” zeigt an, dass es einige Probleme mit dem Knoten gibt. Um die Ursache zu kennen, müssen Sie den Befehl **show cluster node** ausführen. Dieser Befehl zeigt die Knoteneigenschaften und den Grund für den Knotenfehler an.

Was muss ich tun, wenn der Zustand eines Knotens als NICHT UP angezeigt wird und der Grund darauf hinweist, dass Konfigurationsbefehle auf einem Knoten fehlgeschlagen sind?

Dieses Problem tritt auf, wenn einige Befehle nicht auf den Cluster-Knoten ausgeführt werden. In solchen Fällen müssen Sie sicherstellen, dass die Konfigurationen mit einer der folgenden Optionen synchronisiert werden:

- Wenn sich einige der Clusterknoten in diesem Zustand befinden, müssen Sie die Clustersynchronisierung auf diesen Knoten erzwingen. Weitere Informationen finden Sie unter Clusterkonfigurationen synchronisieren.

- Wenn sich alle Clusterknoten in diesem Zustand befinden, müssen Sie die Clusterinstanz auf allen Clusterknoten deaktivieren und aktivieren.

Wenn ich den Befehl set virtual server ausführe, erhalte ich die folgende Meldung: “Keine solche Ressource.” Was muss ich tun, um dieses Problem zu beheben?

Der Befehl **set vserver** wird beim Clustering nicht unterstützt. Die Befehle **“unset vserver”, “enable vserver”, “disable vserver”** und **rm vserver** werden ebenfalls nicht unterstützt. Der Befehl **show vserver** wird jedoch unterstützt.

Ich kann den Cluster nicht über eine Telnet-Sitzung konfigurieren. Was soll ich tun?

Über eine Telnet-Sitzung kann auf die Cluster-IP-Adresse nur im schreibgeschützten Modus zugegriffen werden. Daher können Sie keinen Cluster über eine Telnet-Sitzung konfigurieren.

Ich stelle einen signifikanten Zeitunterschied über die Clusterknoten fest. Was muss ich tun, um dieses Problem zu beheben?

Wenn PTP-Pakete aufgrund des Backplane-Switches verworfen werden oder wenn die physischen Ressourcen in einer virtuellen Umgebung zu stark beauftragen, wird die Zeit nicht synchronisiert.

Um die Zeiten zu synchronisieren, müssen Sie die folgenden Schritte für die Cluster-IP-Adresse ausführen:

1. PTP deaktivieren.

   sett ptp -state disable

2. Konfigurieren Sie Network Time Protocol (NTP) für den Cluster. Weitere Informationen finden Sie unter Einrichten der Uhrsynchronisation.

Was muss ich tun, wenn keine Verbindung zur Cluster-IP-Adresse und der NSIP-Adresse eines Clusterknotens besteht?

Wenn Sie nicht auf die Cluster-IP-Adresse oder den NSIP eines Clusterknotens zugreifen können, müssen Sie über die serielle Konsole auf die Appliance zugreifen. Wenn die NSIP-Adresse erreichbar ist, können Sie SSH von der Shell aus an die Cluster-IP-Adresse senden, indem Sie an der Shell-Eingabeaufforderung den folgenden Befehl ausführen:

“‘# ssh nsroot@


```
## Was muss ich tun, um einen Clusterknoten wiederherzustellen, der
   Verbindungsprobleme aufweist?

So stellen Sie einen Knoten mit Verbindungsproblemen wieder her:

1.  Deaktivieren Sie die Clusterinstanz auf diesem Knoten (da Sie keine
    Befehle vom NSIP eines Clusterknotens ausführen können).

1.  Führen Sie die zum Wiederherstellen des Knotens erforderlichen
   Befehle aus.

1.  Aktivieren Sie die Clusterinstanz auf diesem Knoten.

## Einige Knoten des Clusters haben zwei Standardrouten. Wie kann ich
   die zweite Standardroute vom Clusterknoten entfernen?

Um die zusätzliche Standardroute zu löschen, gehen Sie auf jedem Knoten
    mit der zusätzlichen Route folgendermaßen vor:

1.  Deaktivieren Sie die Clusterinstanz.

    ```disable cluster instance <clId><!--NeedCopy-->
```

1. Entfernen Sie die Route.

   ```
   rm route <network> <netmask> <gateway><!--NeedCopy-->
   ```

2. Aktivieren Sie die Clusterinstanz.

   ```
   enable cluster instance <clId><!--NeedCopy-->
   ```

Die Clusterfunktionalität wird beeinträchtigt, wenn ein vorhandener Clusterknoten online geschaltet wird. Was muss ich tun, um dieses Problem zu beheben?

Wenn das RPC-Kennwort eines Knotens von der Cluster-IP-Adresse geändert wird, wenn dieser Knoten nicht im Cluster ist, besteht eine Nichtübereinstimmung bei RPC-Anmeldeinformationen, die die Clusterfunktionalität beeinträchtigen. Um dieses Problem zu lösen, verwenden Sie den Befehl set ns Rpc-Node, um das Kennwort auf dem NSIP des Knotens zu aktualisieren, der online ist.

Content Switching

October 5, 2021


   ```

Auf den komplexen Websites von heute möchten Sie möglicherweise verschiedenen Benutzern unterschiedliche Inhalte präsentieren. Beispielsweise möchten Sie möglicherweise Benutzern aus dem IP-Bereich eines Kunden oder Partners den Zugriff auf ein spezielles Webportal ermöglichen. Möglicherweise möchten Sie Benutzern aus diesem Bereich Inhalte präsentieren, die für ein bestimmtes geografisches Gebiet relevant sind. Vielleicht möchten Sie den Sprechern dieser Sprachen Inhalte in verschiedenen Sprachen präsentieren. Vielleicht möchten Sie ihnen, die die Geräte verwenden, Inhalte präsentieren, die auf bestimmte Geräte wie Smartphones zugeschnitten sind. Die Citrix ADC Content Switching-Funktion ermöglicht es der Appliance, Clientanfragen auf mehrere Server zu verteilen, basierend auf bestimmten Inhalten, die Sie diesen Benutzern präsentieren möchten.

Um Content Switching zu konfigurieren, erstellen Sie zunächst ein grundlegendes Content Switching-Setup, und passen Sie es dann an Ihre Anforderungen an. Dies beinhaltet die Aktivierung der Content Switchings, das Einrichten des Lastenausgleichs für den Server oder die Server, die jede Version des zu wechselnden Inhalts hosten, das Erstellen eines virtuellen Content Switching-Servers, das Erstellen von Richtlinien zur Auswahl, welche Anforderungen an den virtuellen Lastausgleichsserver gerichtet werden, und Bindung der Richtlinien an den virtuelle Content Switching-Server. Anschließend können Sie das Setup an Ihre Anforderungen anpassen, indem Sie Vorrang für Ihre Richtlinien festlegen, Ihr Setup schützen, indem Sie einen virtuellen Backupserver konfigurieren und die Leistung Ihres Setups verbessern, indem Sie Anforderungen an einen Cache umleiten.

### Funktionsweise von Content Switching

Content Switching ermöglicht es der Citrix ADC Appliance, Anforderungen, die an denselben Webhost gesendet werden, an verschiedene Server mit unterschiedlichen Inhalten weiterzuleiten. Beispielsweise können Sie die Appliance so konfigurieren, dass Anforderungen für dynamischen Inhalt (z. B. URLs mit dem Suffix .asp, .dll oder .exe) an einen Server und Anforderungen für statische Inhalte an einen anderen Server weitergeleitet werden. Sie können die Appliance so konfigurieren, dass Content Switching basierend auf TCP/IP-Headern und Nutzlast durchgeführt wird.

Sie können Content Switching auch verwenden, um die Appliance so zu konfigurieren, dass Anfragen basierend auf verschiedenen Clientattributen an verschiedene Server mit unterschiedlichen Inhalten weitergeleitet werden. Einige dieser Client-Attribute sind:

- **Gerätetyp.** Die Appliance untersucht den Benutzeragenten oder benutzerdefinierten HTTP-Header in der Clientanforderung auf den Gerätetyp, von dem die Anforderung stammt. Basierend auf dem Gerätetyp leitet es die Anforderung an einen bestimmten Webserver. Wenn die Anfrage beispielsweise von einem Mobiltelefon stammt, wird die Anfrage an einen Server weitergeleitet, der Inhalte bereitstellen kann, die der Benutzer auf dem Mobiltelefon anzeigen kann. Eine Anfrage von einem Computer wird an einen anderen Server weitergeleitet, der Inhalte bereitstellen kann, die für einen Computerbildschirm entwickelt wurden.
- **Sprache.** Die Appliance untersucht den Accept-Language HTTP-Header in der Clientanforderung und bestimmt die Sprache, die vom Browser des Clients verwendet wird. Die

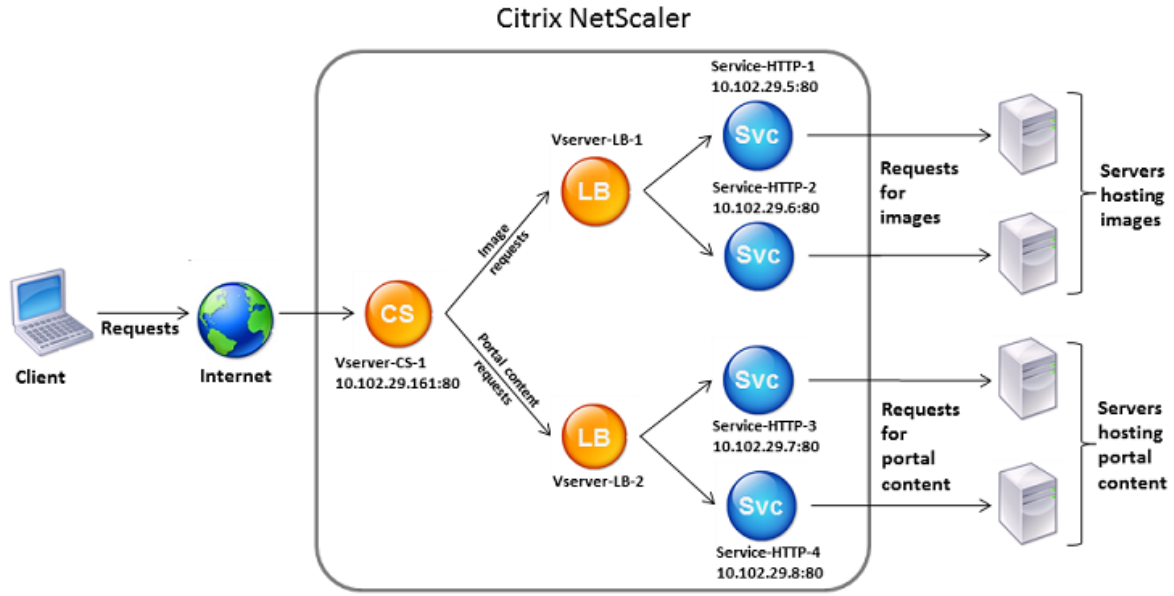
Appliance sendet die Anforderung dann an einen Server, der Inhalte in dieser Sprache bereitstellt. Beispielsweise kann die Appliance mit sprachbasiertem Content Switching jemanden, dessen Browser so konfiguriert ist, Inhalte auf Französisch an einen Server mit der französischen Version einer Zeitung angefordert werden. Es kann eine andere Person senden, deren Browser so konfiguriert ist, Inhalte in englischer Sprache an einen Server mit der englischen Version anzufordern.

- **Cookie.** Die Appliance untersucht die HTTP-Anforderungsheader auf ein Cookie, das der Server zuvor gesetzt hat. Wenn es das Cookie findet, leitet es Anfragen an den entsprechenden Server, der benutzerdefinierte Inhalte hostet. Wenn beispielsweise ein Cookie gefunden wird, das angibt, dass der Client Mitglied eines Kundenbindungsprogramms ist, wird die Anfrage an einen schnelleren Server oder einen mit speziellen Inhalten weitergeleitet. Wenn es kein Cookie findet oder wenn das Cookie anzeigt, dass der Benutzer kein Mitglied ist, wird die Anfrage an einen Server für die breite Öffentlichkeit weitergeleitet.
- **HTTP-Methode.** Die Appliance untersucht den HTTP-Header auf die verwendete Methode und sendet die Clientanforderung an den richtigen Server. Beispielsweise können GET-Anforderungen für Bilder an einen Image-Server geleitet werden, während POST-Anforderungen an einen schnelleren Server weitergeleitet werden können, der dynamische Inhalte verarbeitet.
- **Layer 3/4 Daten.** Die Appliance prüft Anforderungen für die Quell- oder Ziel-IP, den Quell- oder Zielport oder alle anderen Informationen, die in den TCP- oder UDP-Headern vorhanden sind, und leitet die Clientanforderung an den richtigen Server weiter. Beispielsweise können Anfragen von Quell-IPs, die Kunden gehören, an ein benutzerdefiniertes Webportal auf einem schnelleren Server oder eines mit speziellen Inhalten weitergeleitet werden.

Eine typische Content Switching-Bereitstellung besteht aus den im folgenden Diagramm beschriebenen Entitäten.

Abbildung 1. Content Switching-Architektur




Eine Content Switching-Konfiguration besteht aus einem virtuellen Content Switching-Server, einem Load Balancing-Setup, bestehend aus virtuellen Servern und Diensten für den Lastenausgleich und Richtlinien für Content Switching. Um Content Switching zu konfigurieren, müssen Sie einen virtuellen Content Switching-Server konfigurieren und ihn mit Richtlinien und virtuellen Lastausgleichsservern verknüpfen. Dieser Prozess erstellt eine Content-Gruppe—* eine Gruppe aller virtuellen Server und Richtlinien, die an einer bestimmten Content Switching-Konfiguration beteiligt sind.

Content Switching kann mit HTTP-, HTTPS-, TCP- und UDP-Verbindungen verwendet werden. Für HTTPS müssen Sie SSL-Offload aktivieren.

Wenn eine Anforderung den virtuellen Content Switching-Server erreicht, wendet der virtuelle Server die zugeordneten Content Switching-Richtlinien auf diese Anforderung an. Die Priorität der Richtlinie definiert die Reihenfolge, in der die Richtlinien ausgewertet werden, die an den virtuellen Content Switching-Server gebunden sind. Wenn Sie Standard-Syntaxrichtlinien verwenden und eine Richtlinie an den virtuellen Content Switching-Server binden, müssen Sie dieser Richtlinie eine Priorität zuweisen. Wenn Sie klassische Citrix ADC Richtlinien verwenden, können Sie Ihren Richtlinien eine Priorität zuweisen, sind dies jedoch nicht erforderlich. Wenn Sie Prioritäten zuweisen, werden die Richtlinien in der von Ihnen festgelegten Reihenfolge ausgewertet. Andernfalls wertet die Citrix ADC Appliance Ihre Richtlinien in der Reihenfolge aus, in der sie erstellt wurden.

Zusätzlich zum Konfigurieren von Richtlinienprioritäten können Sie die Reihenfolge der Richtlinienbewertung mithilfe von Goto-Ausdrücken und Policy-Bank-Aufrufen ändern. Weitere Informationen zur Standardkonfiguration von Syntaxrichtlinien finden Sie unter Konfigurieren von Standardsyntaxrichtlinien.

Nachdem die Richtlinien ausgewertet wurden, leitet der virtuelle Content Switching-Server die An-

forderung an den entsprechenden virtuellen Lastausgleichsserver weiter, der sie an den entsprechenden Dienst sendet.

Virtuelle Content Switching-Server können nur Anforderungen an andere virtuelle Server senden. Wenn Sie einen externen Load Balancer verwenden, müssen Sie einen virtuellen Lastausgleichsserver für diesen erstellen und den virtuellen Server als Dienst an den virtuellen Content Switching-Server binden.

## Konfigurieren des grundlegenden Content Switchings

December 7, 2021

Bevor Sie Content Switching konfigurieren, müssen Sie verstehen, wie Content Switching eingerichtet wird und wie die Dienste und virtuellen Server verbunden sind.

Um ein grundlegendes, funktionales Content Switching-Setup zu konfigurieren, aktivieren Sie zunächst das Content Switching. Erstellen Sie dann mindestens eine Content-Gruppe. Erstellen Sie für jede Inhaltsgruppe einen virtuellen Content Switching-Server, um Anforderungen an eine Gruppe von Websites anzunehmen, die Content Switching verwenden. Erstellen Sie außerdem ein Lastausgleichssetup, das eine Gruppe von virtuellen Servern mit Lastenausgleich enthält, an die der virtuelle Content Switching-Server Anforderungen weiterleitet. Um anzugeben, welche Anforderungen an welchen Lastenausgleichsserver geleitet werden sollen, erstellen Sie mindestens zwei Content Switching-Richtlinien, eine für jede Art von Anforderung, die umgeleitet werden soll. Wenn Sie die virtuellen Server und Richtlinien erstellt haben, binden Sie die Richtlinien an den virtuellen Content Switching-Server. Sie können eine Richtlinie auch an mehrere virtuelle Content Switching-Server binden. Wenn Sie eine Richtlinie binden, geben Sie den virtuellen Lastenausgleichsserver an, an den Anforderungen gerichtet werden sollen, die der Richtlinie entsprechen.

Zusätzlich zum Binden einzelner Richtlinien an einen virtuellen Content Switching-Server können Sie Richtlinienbeschriftungen binden. Wenn Sie mehr Content-Gruppen erstellen, können Sie eine Richtlinie oder ein Richtlinienlabel an mehr als einen der virtuellen Content Switching-Server binden.

> **Hinweis:**
>
> Nachdem Sie eine Inhaltsgruppe erstellt haben, können Sie den virtuellen Content Switching-Server ändern, um die Konfiguration anzupassen.

### Aktivieren des Content Switchings

Um das Content Switching verwenden zu können, müssen Sie Content Switching aktivieren. Sie können Content Switching-Entitäten konfigurieren, obwohl das Content Switching deaktiviert ist. Die Entitäten funktionieren jedoch nicht.

### So aktivieren Sie Content Switching über die CLI

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

```
enable ns feature CS

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

Beispiel:

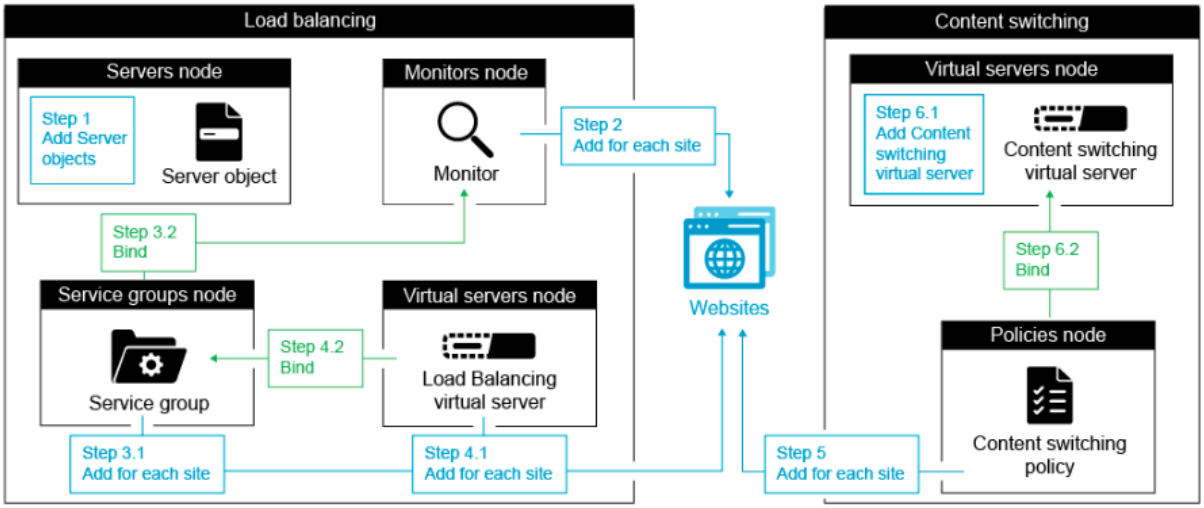
```
> enable  feature ContentSwitch
    Done
> show feature

    Feature                       Acronym             Status
    -------                       -------             ------
1)     Web Logging                   WL                  OFF
2)     Surge Protection              SP                  ON
3)     Load Balancing                LB                  ON
4)     Content Switching             CS                  ON
.
.
.
22)    Responder                     RESPONDER           ON
23)    HTML Injection                HTMLInjection       ON
24)    NetScaler Push                push                OFF
Done
<!--NeedCopy-->
```

So aktivieren Sie Content Switching über die GUI

Navigieren Sie zu **System > Einstellungen**, und wählen Sie in der Gruppe **Modi und Features** die Option **Grundfunktionen konfigurieren** aus, und wählen Sie **Content Switching** aus.

Die folgende Abbildung zeigt die schrittweise Konfiguration von Content Switching.



Erstellen von virtuellen Content Switching-Servern

Sie können virtuelle Content Switching-Server hinzufügen, ändern und entfernen. Der Status eines virtuellen Servers ist DOWN, wenn Sie ihn erstellen, da der virtuelle Lastausgleichsserver noch nicht an ihn gebunden ist.

So erstellen Sie einen virtuellen Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cs vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

Beispiel:

```
add cs vserver Vserver-CS-1 HTTP 10.102.29.161 80
<!--NeedCopy-->
```

So fügen Sie mit der GUI einen virtuellen Content Switching hinzu

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und fügen Sie einen virtuellen Server hinzu.
2. Geben Sie einen Namen für den virtuellen Content Switching-Server an.

> **Hinweis:**
>
> Für jedes Protokoll gibt es unterschiedliche virtuelle Content Switching-Server. (Zum Beispiel HTTP und SSL).

3. Füllen Sie die relevanten Felder aus, und klicken Sie auf **OK**.

Statistiken über den virtuellen Content Switching-Server

Die Statistiken des virtuellen Content Switching-Servers zeigen Informationen wie Auswahl virtueller Server, Anforderungsbytes, Antwortbytes, empfangene Gesamtpakete, gesendete Pakete insgesamt, gesendete Pakete, Spillover-Schwellenwert, Spillover-Auswahl, aktuell vom Client festgelegte Verbindungen und Auswahl für heruntergefahrene virtuelle Server.

Die Statistiken für virtuelle Content Switching-Server zeigen auch die zusammenfassenden Details des gebundenen standardmäßigen Lastausgleichsservers an.

So zeigen Sie Statistiken über den virtuellen Content Switching-Server mit der CLI an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat cs vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
stat cs vserver CS_stats
<!--NeedCopy-->
```



```
Vserver Summary
                                IP  port     Protocol        State
CS_stats                   1.1.1.1    80         HTTP           UP

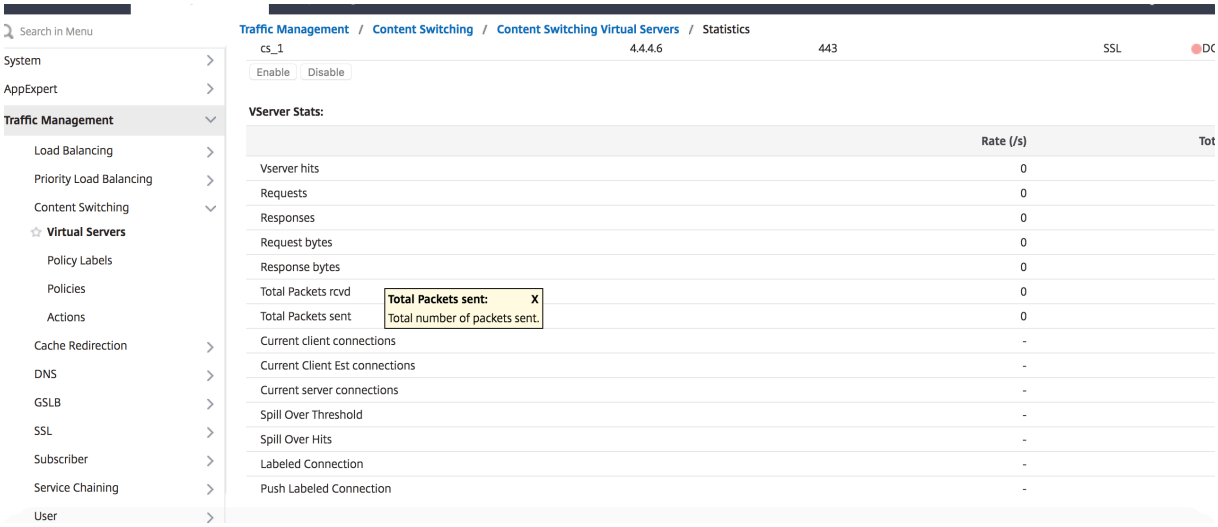
VServer Stats:
                                                  Rate (/s)                Total
Vserver hits                                              0                    0
Requests                                                  0                    0
Responses                                                 0                    0
Request bytes                                             0                    0
Response bytes                                            0                    0
Total Packets rcvd                                        0                    0
Total Packets sent                                        0                    0
Current client connections                               --                    0
Current Client Est connections                           --                    0
Current server connections                               --                    0
Spill Over Threshold                                     --                    0
Spill Over Hits                                          --                    0
Labeled Connection                                       --                    0
Push Labeled Connection                                  --                    0
Deferred Request                                          0                    0
Invalid Request/Response                                 --                    0
Invalid Request/Response Dropped                         --                    0
Vserver Down Backup Hits                                 --                    0
Current Multipath TCP sessions                           --                    0
Current Multipath TCP subflows                           --                    0
Apdex for client response times.                         --                 1.00
Average client TTLB                                      --                    0

 Done
```

So zeigen Sie Statistiken über den virtuellen Content Switching-Server mit der GUI an

1. Navigieren Sie zu **Verkehrsmanagement** > **Content Switching** > **Virtuelle Server**.

2. Wählen Sie den virtuellen Server aus, und klicken Sie auf **Statistiken**.



Konfigurieren eines Lastausgleichs für Content Switching

Der virtuelle Content Switching-Server leitet alle Anforderungen an einen virtuellen Lastausgleichsserver um. Sie müssen einen virtuellen Lastausgleichsserver für jede Version des Inhalts erstellen, der gewechselt wird. Dies gilt auch dann, wenn Ihr Setup nur einen Server für jede Version des Inhalts hat und Sie daher keinen Lastenausgleich mit diesen Servern durchführen. Sie können den tatsächlichen Lastenausgleich auch mit mehreren Servern mit Lastenausgleich konfigurieren, die jede Version des Inhalts spiegeln. In beiden Szenarios muss dem virtuellen Content Switching-Server jeder Version des Inhalts, der gewechselt wird, ein bestimmter virtueller Lastausgleichsserver zugewiesen sein.

Der virtuelle Lastausgleichsserver leitet die Anforderung dann an einen Dienst weiter. Wenn nur ein Dienst an ihn gebunden ist, wählt er diesen Dienst aus. Wenn mehrere Dienste an ihn gebunden sind, verwendet er die konfigurierte Lastausgleichsmethode, um einen Dienst für die Anforderung auszuwählen und leitet diese Anforderung an den ausgewählten Dienst weiter.

Um ein grundlegendes Lastausgleichs-Setup zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

- Erstellen von virtuellen Lastenausgleichs-Servern
- Dienste erstellen
- Binden von Diensten an den virtuellen Lastausgleichsserver

Weitere Informationen zum Lastenausgleich finden Sie unter Funktionsweise des Lastenausgleichs. Ausführliche Anweisungen zum Einrichten einer grundlegenden Load Balancing-Konfiguration finden Sie unter Einrichten des grundlegenden Lastenausgleichs.

Konfigurieren einer Content Switching-Aktion

Sie geben den virtuellen Zielserver für den Lastenausgleich für eine Content Switching-Richtlinie an, wenn Sie die Richtlinie an den virtuellen Content Switching-Server binden. Daher müssen Sie eine Richtlinie für jeden virtuellen Lastausgleichsserver konfigurieren, zu dem der Datenverkehr geleitet werden soll.

Wenn Ihre Content Switching-Richtlinie jedoch eine Standard-Syntaxregel verwendet, können Sie eine Aktion für die Richtlinie konfigurieren. In der Aktion können Sie den Namen des virtuellen Zielservers für den Lastausgleich angeben oder einen anforderungsbasierten Ausdruck konfigurieren, der zur Laufzeit den Namen des virtuellen Lastausgleichsservers berechnet, an den die Anforderung gesendet werden soll. Der Aktionsausdruck muss in der Standardsyntax angegeben werden.

Die Ausdruckoption kann die Größe Ihrer Content Switching-Konfiguration drastisch reduzieren, da pro virtueller Server nur eine Richtlinie erforderlich ist. Content Switching-Richtlinien, die eine Aktion verwenden, können auch an mehrere virtuelle Server gebunden werden, da der virtuelle Zielserver für den Lastenausgleich nicht mehr in der Content Switching-Richtlinie angegeben ist. Die Möglichkeit,

eine einzelne Richtlinie an mehrere virtuelle Content Switching-Server zu binden, trägt dazu bei, die Größe Ihrer Konfiguration für das Content Switching weiter zu reduzieren.

Nachdem Sie eine Aktion erstellt haben, erstellen Sie eine Content Switching-Richtlinie und geben die Aktion in der Richtlinie an, sodass die Aktion ausgeführt wird, wenn diese Richtlinie einer Anforderung entspricht.

> **Hinweis:**
>
> Sie können auch für eine Content Switching-Richtlinie , die eine Standard-Syntaxregel verwendet, den virtuellen Zielserver für Lastenausgleich angeben, wenn Sie die Richtlinie an einen virtuellen Content Switching-Server binden, anstatt eine separate Aktion zu verwenden. Für domänenbasierte Richtlinien, URL-basierte Richtlinien und regelbasierte Richtlinien, die klassische Ausdrücke verwenden, ist eine Aktion nicht verfügbar. Bei diesen Richtlinientypen geben Sie also den Namen des virtuellen Zielservers für den Lastenausgleich an, wenn Sie die Richtlinie an einen virtuellen Content Switching-Server mit binden.

Konfigurieren einer Aktion, die den Namen des virtuellen Zielservers für den Lastenausgleich angibt

Wenn Sie den Namen des virtuellen Zielservers für den Lastenausgleich in einer Content Switching-Aktion angeben, benötigen Sie so viele Content Switching-Richtlinien wie virtuelle Zielserver für den Lastenausgleich. Entscheidungen zum Content Switching basieren in diesem Fall auf der Regel in der Content Switching-Richtlinie , und die Aktion gibt lediglich den virtuellen Zielserver für Lastenausgleich an. Wenn eine Anforderung mit der Richtlinie übereinstimmt, wird die Anforderung an den angegebenen virtuellen Lastausgleichsserver weitergeleitet.

So erstellen und überprüfen Sie eine Content Switching-Aktion, die den Namen des virtuellen Ziel-Lastausgleichsservers angibt, indem Sie die CLI verwenden

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cs action <name> -targetLBVserver <string> [-comment <string>]

show cs action <name>
<!--NeedCopy-->
```

Beispiel:

```
> add cs action mycsaction -targetLBVserver mylbvserver -comment ”
    Forwards requests to mylbvserver.”
```



```
 Done
> show cs action mycsaction
    Name: mycsaction
    Target LB Vserver: mylbvserver
    Hits: 0
    Undef Hits: 0
    Action Reference Count: 0
    Comment: "Forwards requests to mylbvserver."

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

So konfigurieren Sie eine Content Switching-Aktion, die den Namen des virtuellen Ziel-Lastausgleichsservers mit der GUI angibt

1. Navigieren Sie zu **Traffic Management > Content Switching > Aktionen**.
2. Konfigurieren Sie eine Content Switching-Aktion, und geben Sie den Namen des virtuellen Zielservers für den Lastenausgleich an.

Konfigurieren einer Aktion, die einen Ausdruck für die Auswahl des Ziels zur Laufzeit angibt

Wenn Sie einen anforderungsbasierten Ausdruck konfigurieren, der den Namen des virtuellen Zielservers für den Lastenausgleich dynamisch berechnen kann, müssen Sie nur eine Content Switching-Richtlinie konfigurieren, um den entsprechenden virtuellen Server auszuwählen. Die Regel für die Richtlinie kann eine einfaches TRUE sein (die Richtlinie entspricht allen Anforderungen), da in diesem Fall Entscheidungen zum Content Switching auf dem Ausdruck in der Aktion basieren. Durch die Konfiguration eines Ausdrucks in einer Aktion können Sie die Größe Ihrer Content Switching-Konfiguration drastisch reduzieren.

Wenn Sie einen anforderungsbasierten Ausdruck zum Berechnen des Namens des virtuellen Zielservers für den Lastausgleich zur Laufzeit konfigurieren, müssen Sie sorgfältig überlegen, wie die virtuellen Server für den Lastausgleich in der Konfiguration benannt werden. Sie müssen in der Lage sein, ihre Namen mithilfe des anforderungsbasierten Richtlinienausdrucks in der Aktion abzuleiten.

Wenn Sie beispielsweise Änderungsanforderungen basierend auf dem URL-Suffix (Erweiterung der angeforderten Ressource) ändern, können Sie bei der Benennung der virtuellen Lastausgleichsserver der Konvention folgen, das URL-Suffix an eine vorbestimmte Zeichenfolge anzuhängen, z. `mylb_` Beispielsweise können virtuelle Server mit Lastenausgleich für HTML-Seiten und PDF-Dateien `mylb_html` bzw. `mylb_pdf` benannt werden. In diesem Fall ist die Regel, die Sie in der Content Switching-Aktion verwenden können, um den entsprechenden virtuellen Lastausgleichsserver

auszuwählen”mylb_”+HTTP.REQ.URL.SUFFIX. Wenn der virtuelle Content Switching-Server eine Anforderung für eine HTML-Seite erhält, wird der Ausdruck zurückgegeben mylb_html, und die Anforderung wird auf den virtuellen Server umgestellt mylb_html.

So erstellen Sie eine Content Switching-Aktion, die einen Ausdruck angibt, indem Sie die CLI verwenden

Geben Sie in der Befehlszeile die folgenden Befehle ein, um eine Content Switching-Aktion zu erstellen, die einen Ausdruck angibt, und überprüfen Sie die Konfiguration:

```
add cs action <name> -targetVserverExpr <expression>) [-comment <string
    >]

show cs action <name>
<!--NeedCopy-->
```

Beispiel:

```
> add cs action mycsaction1 -targetvserverExpr '”mylb_” + HTTP.REQ.URL.
    SUFFIX'
 Done
> show cs action mycsaction1
    Name: mycsaction1
    Target Vserver Expression: ”mylb_” + HTTP.REQ.URL.SUFFIX
    Target LB Vserver: No_Target
                ...
 Done
>
<!--NeedCopy-->
```

So konfigurieren Sie eine Content Switching-Aktion, die einen Ausdruck mit der GUI angibt

1. Navigieren Sie zu **Traffic Management > Content Switching > Aktionen**.
2. Konfigurieren Sie eine Content Switching-Aktion, und geben Sie einen Ausdruck an, der den Namen des virtuellen Zielservers für den Lastenausgleich dynamisch berechnet.

Konfigurieren von Content Switching-Richtlinien

Eine Content Switching-Richtlinie definiert einen Anforderungstyp, der an einen virtuellen Lastausgleichsserver weitergeleitet werden soll. Diese Richtlinien werden in der Reihenfolge der ihnen

zugewiesenen Prioritäten oder (wenn Sie klassische Citrix ADC Richtlinien verwenden und beim Binden keine Prioritäten zuweisen) in der Reihenfolge angewendet, in der die Richtlinien erstellt wurden.

Die Richtlinien können folgendermaßen sein:

- **Domänenbasierte Richtlinien.** Die Citrix ADC Appliance vergleicht die Domäne einer eingehenden URL mit den in den Richtlinien angegebenen Domänen. Die Appliance gibt dann den am besten geeigneten Inhalt zurück. Domänenbasierte Richtlinien müssen klassische Richtlinien sein. Standard-Syntaxrichtlinien werden für diesen Typ von Content Switching-Richtlinien nicht unterstützt.
- **URL-basierte Richtlinien.** Die Appliance vergleicht eine eingehende URL mit den in den Richtlinien angegebenen URLs. Die Appliance gibt dann den am besten geeigneten URL-basierten Inhalt zurück, der normalerweise die längste übereinstimmende konfigurierte URL ist. URL-basierte Richtlinien müssen klassische Richtlinien sein. Standard-Syntaxrichtlinien werden für diesen Typ von Content Switching-Richtlinien nicht unterstützt.
- **Regelbasierte Richtlinien.** Die Appliance vergleicht eingehende Daten mit Ausdrücken, die in den Richtlinien angegeben sind. Sie erstellen regelbasierte Richtlinien entweder mit einem klassischen Ausdruck oder einem Standardsyntaxausdruck. Sowohl klassische als auch standardmäßige Syntaxrichtlinien werden für regelbasierte Content Switching-Richtlinien unterstützt.

  > **Hinweis:**
  >
  > Eine regelbasierte Richtlinie kann mit einer optionalen Aktion konfiguriert werden. Eine Richtlinie mit einer Aktion kann an mehrere virtuelle Server oder Richtlinienbeschriftungen gebunden werden.

  Wenn Sie beim Binden der Richtlinien an den virtuellen Content Switching-Server eine Priorität festlegen, werden die Richtlinien in der Reihenfolge der Priorität ausgewertet. Wenn Sie beim Binden der Richtlinien keine spezifischen Prioritäten festlegen, werden die Richtlinien in der Reihenfolge ausgewertet, in der sie erstellt wurden.

Informationen zu klassischen Richtlinien und Ausdrücken von Citrix ADC finden Sie unter Konfigurieren klassischer Richtlinien und Ausdrücke. Informationen zu Standardsyntaxrichtlinien finden Sie unter Konfigurieren von Standardsyntaxausdrücken.

So erstellen Sie eine Content Switching-Richtlinie mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
add cs policy <policyName> -domain <domain>
```



```
add cs policy <policyName> -url <URLValue>

add cs policy <policyName> -rule <RULEValue>

add cs policy <policyName> -rule <RULEValue> -action <actionName>
<!--NeedCopy-->
```

Beispiel:

```
add cs policy Policy-CS-1 -url "http://example.com"

add cs policy Policy-CS-1 -domain "example.com"

add cs policy Policy-CS-1 -rule "CLIENT.IP.SRC.SUBNET(24).EQ
   (10.217.84.0)"

add cs policy Policy-CS-2 -rule "SYS.TIME.BETWEEN(GMT 2009 Nov,GMT 2009
    Dec)"

add cs policy Policy-CS-3 -rule "http.req.method.eq(GET)" -action act1
<!--NeedCopy-->
```

So benennen Sie eine Content Switching-Richtlinie mit der CLI um

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rename cs policy <policyName> <newName>
<!--NeedCopy-->
```

Beispiel:

```
rename cs policy myCSPolicy myCSPolicy1
<!--NeedCopy-->
```

So benennen Sie eine Content Switching-Richtlinie über die GUI um

Navigieren Sie zu **Traffic Management > Content Switching > Policies**, wählen Sie eine Richtlinie aus, und wählen Sie in der Liste Aktion die Option Umbenennen aus.

So erstellen Sie eine Content Switching-Richtlinie über die GUI

1. Navigieren Sie zu **Traffic Management > Content Switching > Policies**, und klicken Sie auf **Hinzufügen**.
2. Füllen Sie die relevanten Felder aus, und klicken Sie auf **Erstellen**.

Konfigurieren von Content Switching-Richtlinienbeschriftungen

Eine Richtlinienbezeichnung ist ein benutzerdefinierter Bindepunkt, an den Richtlinien gebunden sind. Wenn eine Richtlinienbezeichnung aufgerufen wird, werden alle an sie gebundenen Richtlinien in der Reihenfolge der Priorität ausgewertet, die Sie ihnen zugewiesen haben. Eine Richtlinienbezeichnung kann eine oder mehrere Richtlinien enthalten, von denen jeder ein eigenes Ergebnis zugewiesen werden kann. Eine Übereinstimmung einer Richtlinie in der Richtlinienbezeichnung kann dazu führen, dass mit der nächsten Richtlinie fortgefahren wird, eine andere Richtlinienbezeichnung oder eine geeignete Ressource aufgerufen wird, oder ein sofortiges Ende der Richtlinienauswertung und eine Rückgabe der Kontrolle an die Richtlinie, die die Richtlinienbezeichnung aufgerufen hat. Sie können Richtlinienbeschriftungen nur für Standard-Syntaxrichtlinien erstellen.

Ein Content Switching-Richtlinienlabel besteht aus einem Namen, einem Beschriftungstyp und einer Liste von Richtlinien, die an das Richtlinienlabel gebunden sind. Der Richtlinienbeschriftungstyp gibt das Protokoll an, das den Richtlinien zugewiesen wurde, die an das Label gebunden sind. Sie muss mit dem Diensttyp des virtuellen Content Switching-Servers übereinstimmen, an den die Richtlinie gebunden ist, die die Richtlinienbezeichnung aufruft. Beispielsweise können Sie TCP-Payload-Richtlinien nur an eine Richtlinienbezeichnung vom Typ TCP binden. Das Binden von TCP-Payload-Richtlinien an eine Richtlinienbezeichnung vom Typ HTTP wird nicht unterstützt.

Jede Richtlinie in einem Content Switching-Richtlinienlabel ist entweder mit einem Ziel (das der Aktion entspricht, die anderen Arten von Richtlinien zugeordnet ist, wie Rewrite- und Responder-Richtlinien) oder einer gotoPriorityExpression-Option und einer Invoke-Option. Das heißt, für eine bestimmte Richtlinie in einem Content Switching-Richtlinienlabel können Sie ein Ziel angeben oder die gotoPriorityExpression- und die Invoke-Option festlegen. Wenn mehrere Richtlinien als wahr bewerten, wird nur das Ziel der letzten Richtlinie berücksichtigt, das als wahr bewertet wird.

Sie können entweder die Citrix ADC CLI oder die GUI verwenden, um Content Switching-Richtlinienlabel zu konfigurieren. In der Citrix ADC CLI erstellen Sie zuerst eine Richtlinienbezeichnung, indem Sie den Befehl add cs policy label verwenden. Anschließend binden Sie Richtlinien an die Richtlinienbezeichnung, eine Richtlinie nach der anderen, indem Sie den Richtlinienbezeichnungsbefehl bind cs verwenden. In der Citrix ADC GUI führen Sie beide Tasks in einem einzigen Dialogfeld aus.

So erstellen Sie ein Content Switching-Richtlinienlabel mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add cs policylabel <labelName> <cspolicylabelTypetype>`
2 <!--NeedCopy-->
```

Beispiel:

```
1 add cs policylabel testpollab http
2 <!--NeedCopy-->
```

So benennen Sie ein Content Switching-Richtlinienlabel mit der CLI um

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 rename cs policylabel <labelName> <newName>`
2 <!--NeedCopy-->
```

Beispiel:

```
1 rename cs policylabel oldPolicyLabelName newPolicyLabelName
2 <!--NeedCopy-->
```

So benennen Sie ein Content Switching-Richtlinienlabel über die GUI um

Navigieren Sie zu **Traffic Management > Content Switching > Policy Labels**, wählen Sie eine Richtlinienbezeichnung aus, und wählen Sie in der Liste Aktion die Option Umbenennen aus.

So binden Sie eine Richtlinie über die CLI an ein Content Switching-Richtlinienlabel

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Richtlinie an eine Richtlinienbezeichnung zu binden, und überprüfen Sie die Konfiguration:


```
bind cs policylabel <labelName> <policyName> <priority>[-targetVserver
    <string>] | [-gotoPriorityExpression <expression>] | [-invoke <
    labeltype> <labelName>] ]

show cs policylabel <labelName>
<!--NeedCopy-->
```

Beispiel:

```
bind cs policylabel testpollab test_Pol 100 -targetVserver LBVIP
show cs policylabel testpollab
        Label Name: testpollab
        Label Type: HTTP
        Number of bound policies: 1
        Number of times invoked: 0
        Policy Name: test_Pol
        Priority: 100
        Target Virtual Server: LBVIP
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn eine Richtlinie mit einer Aktion konfiguriert ist, gehen Sie zum virtuellen Zielserver (TargetvServer), zum Prioritätsausdruck (GotoPriorityExpression), und die Parameter aufrufen (Aufrufen) sind nicht erforderlich. Wenn eine Richtlinie nicht mit einer Aktion konfiguriert wird, müssen Sie mindestens einen der folgenden Parameter konfigurieren: targetVserver, gotoPriorityExpression und invoke.

So heben Sie die Bindung einer Richtlinie von einer Richtlinienbezeichnung auf, indem Sie die CLI verwenden

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Bindung einer Richtlinie von einer Richtlinienbezeichnung aufzuheben und die Konfiguration zu überprüfen:

```
unbind cs policylabel <labelName> <policyName>

show cs policylabel <labelName>
<!--NeedCopy-->
```

Beispiel:


```
unbind cs policylabel testpollab test_Pol
show cs policylabel testpollab
        Label Name: testpollab
        Label Type: HTTP
        Number of bound policies: 0
        Number of times invoked: 0
<!--NeedCopy-->
```

So entfernen Sie ein Richtlinienlabel mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm cs policylabel <labelName>
<!--NeedCopy-->
```

So verwalten Sie ein Content Switching-Richtlinienlabel über die GUI

Navigieren Sie zu **Traffic Management > Content Switching > Policy Labels**, konfigurieren Sie eine Richtlinienbezeichnung, binden Sie Richtlinien an das Label und geben Sie optional eine Priorität, einen GoToPriority-Ausdruck und eine Aufrufoption an.

Binden von Richtlinien an einen virtuellen Content Switching-Server

Nachdem Sie den virtuellen Server und die Richtlinien für Content Switching erstellt haben, binden Sie jede Richtlinie an den virtuellen Content Switching-Server. Wenn Sie die Richtlinie an den virtuellen Content Switching-Server binden, geben Sie den virtuellen Zielserver für den Lastenausgleich an.

> **Hinweis:**
>
> Wenn Ihre Content Switching-Richtlinie eine Standard-Syntaxregel verwendet, können Sie eine Content Switching-Aktion für die Richtlinie konfigurieren. Wenn Sie eine Aktion konfigurieren, müssen Sie den virtuellen Zielserver für Lastenausgleich angeben, wenn Sie die Aktion konfigurieren, und nicht, wenn Sie die Richtlinie an den virtuellen Content Switching-Server binden. Weitere Informationen zum Konfigurieren einer Content Switching-Aktion finden Sie im Abschnitt Konfigurieren einer Content Switching-Aktion.

So binden Sie eine Richtlinie an einen virtuellen Content Switching-Server und wählen einen virtuellen Ziel-Lastausgleichsserver mit der CLI aus

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind cs vserver <name>[-lbvserver<string> -targetLBVServer<string> -
    policyname <string> -priority <positive_integer>] [-
    gotoPriorityExpression <expression>] [-type ( REQUEST | RESPONSE )]
    [-invoke (<labelType> <labelName>)]
<!--NeedCopy-->
```

Beispiel:

```
bind cs vserver csw-vip2 -policyname csw-ape-policy2 -priority 14 -
    gotoPriorityExpression NEXT

bind cs vserver csw-vip3 -policyname rewrite-policy1 -priority 17 -
    gotoPriorityExpression
'q.header(”a”).count' -flowtype REQUEST -invoke policylabel label1

bind cs vserver Vserver-CS-1 Vserver-LB-1 -policyname Policy-CS-1 -
    priority 20
<!--NeedCopy-->
```

> **Hinweis:**
>
> Die Parameter, der virtuelle Ziel-Lastausgleichsserver (targetVserver), gehen Sie zum Prioritätsausdruck (gotoPriorityExpression) und die Aufrufmethode (invoke) können nicht verwendet werden, wenn eine Richtlinie über eine Aktion verfügt.

So binden Sie eine Richtlinie an einen virtuellen Content Switching-Server und wählen über die GUI einen virtuellen Ziel-Lastausgleichsserver

Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, öffnen Sie einen virtuellen Server, und binden Sie im Abschnitt
Content Switching Policy Binding eine Richtlinie an den virtuellen Server, und geben Sie einen virtuellen Ziel-Lastausgleichsserver an.

Konfigurieren der richtlinienbasierten Protokollierung für Content Switching

Sie können die richtlinienbasierte Protokollierung für eine Content Switching-Richtlinie konfigurieren. Mit der Richtlinienbasierten Protokollierung können Sie ein Format für Protokollmeldungen angeben. Der Inhalt der Protokollnachricht wird mithilfe eines Standardsyntaxausdrucks in der Content Switching-Richtlinie definiert. Wenn die in der Richtlinie angegebene Content Switching-Aktion ausgeführt wird, erstellt die Citrix ADC Appliance die Protokollnachricht aus dem Ausdruck und schreibt die Nachricht in die Protokolldatei. Die richtlinienbasierte Protokollierung ist besonders nützlich, wenn Sie eine Konfiguration testen und beheben möchten, bei der Content Switching-Aktionen den virtuellen Zielserver zur Laufzeit identifizieren.

> **Hinweis:**
>
> Wenn mehrere Richtlinien, die an einen bestimmten virtuellen Server gebunden sind, auf TRUE ausgewertet werden und mit einer Auditbenachrichtigungsaktion konfiguriert sind, führt die Citrix ADC Appliance nicht alle Auditbenachrichtigungsaktionen aus. Es führt nur die Auditbenachrichtigungsaktion aus, die für die Richtlinie konfiguriert ist, deren Content Switching-Aktion ausgeführt wird.

Um die richtlinienbasierte Protokollierung für eine Content Switching-Richtlinie zu konfigurieren, müssen Sie zunächst eine Auditbenachrichtigungsaktion konfigurieren. Weitere Informationen zum Konfigurieren einer Überwachungsnachrichtenaktion finden Sie unter Konfigurieren der Citrix ADC Appliance für die Überwachungsprotokollierung. Nachdem Sie die Auditbenachrichtigungsaktion konfiguriert haben, geben Sie die Aktion in einer Content Switching-Richtlinie an.

So konfigurieren Sie die richtlinienbasierte Protokollierung für eine Content Switching-Richtlinie über die CLI

Geben Sie in der Befehlszeile die folgenden Befehle ein, um die richtlinienbasierte Protokollierung für eine Content Switching-Richtlinie zu konfigurieren und die Konfiguration zu überprüfen:

```
set cs policy <policyName> -logAction <string>

show cs policy <policyName>
<!--NeedCopy-->
```

Beispiel:

```
> set cs policy cspol1 -logAction csLogAction
 Done
> show cs policy cspol1
```



```
4
5      Policy: cspol1  Rule: TRUE  Action: csact1
6      LogAction: csLogAction
7      Hits: 0
8
9  1)  CS Vserver: csvs1
10     Priority: 10
11  Done
12 >
13 <!--NeedCopy-->
```

So konfigurieren Sie die richtlinienbasierte Protokollierung für eine Content Switching-Richtlinie über die GUI

Navigieren Sie zu **Verkehrsverwaltung > Content Switching > Richtlinien**, öffnen Sie eine Richtlinie, und wählen Sie in der Liste Protokollaktion eine Protokollaktion für die Richtlinie aus.

Überprüfen der Konfiguration

Um zu überprüfen, ob die Konfiguration des Content Switchings korrekt ist, müssen Sie die Content Switching-Entitäten anzeigen. Um den ordnungsgemäßen Betrieb zu überprüfen, nachdem die Content Switching-Konfiguration bereitgestellt wurde, können Sie die Statistiken anzeigen, die beim Zugriff auf die Server generiert werden.

Anzeigen der Eigenschaften von virtuellen Content Switching-Servern

Sie können die Eigenschaften von virtuellen Content Switching-Servern anzeigen, die Sie auf der Citrix ADC Appliance konfiguriert haben. Sie können die Informationen verwenden, um zu überprüfen, ob der virtuelle Server korrekt konfiguriert ist, und, falls erforderlich, zur Fehlerbehebung. Zusätzlich zu Details wie Name, IP-Adresse und Port können Sie die verschiedenen Richtlinien, die an einen virtuellen Server gebunden sind, sowie die Einstellungen für die Verkehrsverwaltung anzeigen.

Die Content Switching-Richtlinien werden in der Reihenfolge ihrer Priorität angezeigt. Wenn mehrere Richtlinien dieselbe Priorität haben, werden sie in der Reihenfolge angezeigt, in der sie an den virtuellen Server gebunden sind.

> **Hinweis:**
>
> Wenn Sie den virtuellen Content Switching-Server so konfiguriert haben, dass Datenverkehr an einen virtuellen Lastausgleichsserver weitergeleitet wird, können Sie auch die Content

> Switching-Richtlinien anzeigen, indem Sie die Eigenschaften des virtuellen Lastausgleichsservers anzeigen.

So zeigen Sie die Eigenschaften von virtuellen Content Switching-Servern mit der CLI an

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um die grundlegenden Eigenschaften aller virtuellen Content Switching-Server in Ihrer Konfiguration oder detaillierte Eigenschaften eines bestimmten virtuellen Servers aufzulisten:

```
show cs vserver

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

Beispiel

```
1.
show cs vserver Vserver-CS-1
Vserver-CS-1 (10.102.29.161:80) - HTTP Type: CONTENT
State: UP
Last state change was at Thu Jun 30 10:48:59 2011
Time since last state change: 6 days, 20:03:00.760
Client Idle Timeout: 180 sec
Down state flush: ENABLED
Disable Primary Vserver On Down : DISABLED
Appflow logging: DISABLED
Port Rewrite : DISABLED
State Update: DISABLED
Default: Content Precedence: RULE
Vserver IP and Port insertion: OFF
Case Sensitivity: ON
Push: DISABLED Push VServer:
Push Label Rule: none

...
1) Policy : __ESNS_PREBODY_POLICY Priority:0
2) Policy : __ESNS_POSTBODY_POLICY Priority:0

1) Compression Policy Name: __ESNS_CMP_POLICY Priority: 2147483647
GotoPriority Expression: END
```



```
Flowtype: REQUEST

2) Rewrite Policy Name: __ESNS_REWRITE_POLICY Priority: 2147483647
GotoPriority Expression: END
Flowtype: REQUEST

3) Cache Policy Name: dfbx Priority: 10
GotoPriority Expression: END
Flowtype: REQUEST

4) Responder Policy Name: __ESNS_RESPONDER_POLICY Priority: 2147483647
GotoPriority Expression: END

1) Policy: wiki Target: LBVIP2 Priority: 25 Hits: 0
2) Policy: plain Target: LBVIP1 Priority: 90 Hits: 0
3) Policy: DispOrderTest2 Target: KerbAuthLBVS Priority: 91 Hits: 0
4) Policy: test_Pol Target: LBVIP1 Priority: 92 Hits: 0
5) Policy: PolicyNameTesting Target: LBVIP1 Priority: 100 Hits: 0
 Done
>

show cs vserver
1) Vserver-CS-1 (10.102.29.161:80) - HTTP Type: CONTENT
State: UP
…
Appflow logging: DISABLED
Port Rewrite : DISABLED
State Update: DISABLED

2) apubendpt (10.111.111.1:80) - HTTP Type: CONTENT
State: UP
…
Client Idle Timeout: 180 sec
Down state flush: DISABLED
…

3) apubendpt1 (10.111.111.2:80) - HTTP Type: CONTENT
State: UP
…
Disable Primary Vserver On Down : DISABLED
Appflow logging: DISABLED
Port Rewrite : DISABLED
State Update: DISABLED
…
<!--NeedCopy-->
```


Anzeigen von Content Switching-Richtlinien

Sie können die Eigenschaften der von Ihnen definierten Content Switching-Richtlinien anzeigen, wie den Namen, die Domäne und die URL oder den Ausdruck, und die Informationen verwenden, um Fehler in der Konfiguration zu finden oder Probleme zu beheben, wenn etwas nicht so funktioniert, wie es muss.

So zeigen Sie die Eigenschaften von Content Switching-Richtlinien über die CLI an

Um entweder die grundlegenden Eigenschaften aller Content Switching-Richtlinien in Ihrer Konfiguration oder die detaillierten Eigenschaften einer bestimmten Content Switching-Richtlinie aufzulisten, geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
show cs policy

show cs policy <PolicyName>
<!--NeedCopy-->
```

Beispiel:

```
show cs policy

show cs policy Policy-CS-1
<!--NeedCopy-->
```

So zeigen Sie die Eigenschaften von Content Switching-Richtlinien über die GUI an

Navigieren Sie zu **Traffic Management** > **Content Switching** > **Policies**, wählen Sie eine Richtlinie aus, und wählen Sie in der Liste Aktion die Option **Bindings anzeigen** aus.

Anzeigen der Konfiguration des virtuellen Content Switching-Servers mit Visualizer

Der Content Switching Visualizer ist ein Tool, mit dem Sie eine Content Switching-Konfiguration im grafischen Format anzeigen können. Mit dem Visualizer können Sie die folgenden Konfigurationselemente anzeigen:

- Eine Zusammenfassung der virtuellen Lastausgleichsserver, an die der virtuelle Content Switching-Server gebunden ist.
- Alle Dienste und Dienstgruppen, die an den virtuellen Lastausgleichsserver gebunden sind, und alle Monitore, die an die Dienste gebunden sind.
- Die Konfigurationsdetails jedes angezeigten Elements.
- Alle Richtlinien, die an den virtuellen Content Switching-Server gebunden sind. Diese Richtlinien müssen keine Content Switching-Richtlinien sein. Viele Arten von Richtlinien, z. B. Umschreibrichtlinien, können an einen virtuellen Content Switching-Server gebunden werden.

Nachdem Sie die verschiedenen Elemente in einem Content Switching- und Lastausgleichs-Setup konfiguriert haben, können Sie die gesamte Konfiguration in eine Anwendungsvorlagendatei exportieren.

> **Hinweis:**
>
> Der Visualizer benötigt eine grafische Oberfläche, daher ist sie nur über die GUI verfügbar.

So zeigen Sie eine Content Switching-Konfiguration mit dem Visualizer in der GUI an

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie anzeigen möchten, und klicken Sie dann auf **Visualizer**.
3. Im Fenster **Content Switching Visualizer** können Sie den sichtbaren Bereich wie folgt anpassen:
    - Klicken Sie auf die Symbole **Vergrößern und Verkleinern**, um den sichtbaren Bereich zu vergrößern oder zu verkleinern.
    - Klicken Sie auf das Symbol **Bild speichern**, um das Diagramm als Bilddatei zu speichern.
    - Geben Sie im Textfeld Suchen im Textfeld Geben Sie den Namen des gesuchten Elements ein. Wenn Sie genügend Zeichen eingegeben haben, um das Element zu identifizieren, wird dessen Position hervorgehoben. Um die Suche einzuschränken, klicken Sie auf das Dropdownmenü und wählen Sie den Typ des Elements aus, nach dem Sie suchen möchten.
4. Um Konfigurationsdetails für Entitäten anzuzeigen, die an diesen virtuellen Server gebunden sind, können Sie Folgendes tun:
    - Um Richtlinien anzuzeigen, die an den virtuellen Server gebunden sind, wählen Sie in der Symbolleiste oben im Dialogfeld ein oder mehrere funktionsspezifische Richtliniensymbole aus. Wenn Richtlinienbeschriftungen konfiguriert sind, werden sie im Hauptansichtsbereich angezeigt.

- Um die Konfigurationsdetails für einen gebundenen Dienst oder eine gebundene Dienstgruppe anzuzeigen, klicken Sie auf das Symbol für den Dienst, klicken Sie auf die Registerkarte Zugehörige Aufgaben, und klicken Sie dann auf Mitgliedsdienste anzeigen.
- Um die Konfigurationsdetails für einen Monitor anzuzeigen, klicken Sie auf das Symbol für den Monitor, klicken Sie auf die Registerkarte **Zugehörige Aufgaben**, und klicken Sie dann auf **Monitor anzeigen** .

5. Um detaillierte Statistiken für jeden virtuellen Server in der Content Switching-Konfiguration anzuzeigen, klicken Sie auf den virtuellen Server, für den Sie Statistiken anzeigen möchten, und klicken Sie dann auf die Registerkarte Zugehörige Aufgaben, und klicken Sie dann auf **Statistiken**.
6. Um eine Vergleichsliste der Parameter anzuzeigen, deren Werte sich für einen virtuellen Lastenausgleichsserver unterscheiden oder nicht in Dienstcontainern definiert sind, klicken Sie auf das Symbol für einen Container, klicken Sie auf die Registerkarte **Zugehörige Aufgaben**, und klicken Sie dann auf **Dienstattribute Diff** .
7. Um Überwachungs-Bindungsdetails für die Dienste in einem Container anzuzeigen, klicken Sie im Dialogfeld Dienstattribute Diff in der Spalte Gruppe für den Container auf **Details**. Diese Vergleichsliste hilft Ihnen, festzustellen, welcher Service-Container die Konfiguration hat, die Sie auf alle Service-Container anwenden möchten.
8. Um die Anzahl der Anfragen anzuzeigen, die pro Sekunde zu einem bestimmten Zeitpunkt von den virtuellen Servern in der Konfiguration empfangen wurden, und die Anzahl der ausgewählten pro Sekunde zu einem bestimmten Zeitpunkt für Umschreibungs-, Responder- und Cache-Richtlinien, klicken Sie auf Statistiken anzeigen. Die statistischen Informationen werden auf den jeweiligen Knoten im Visualizer angezeigt. Diese Informationen werden nicht in Echtzeit aktualisiert. Es wird manuell aktualisiert. Klicken Sie auf Statistiken aktualisieren, um die Informationen zu aktualisieren.

   > **Hinweis:**
   >
   > Diese Option ist nur bei Citrix ADC nCore Builds verfügbar.

9. Um Konfigurationsdetails für ein Element in ein Dokument oder eine Tabelle zu kopieren, klicken Sie auf das Symbol für dieses Element, klicken Sie auf Zugehörige Aufgaben, klicken Sie auf Eigenschaften kopieren, und fügen Sie die Informationen dann in ein Dokument ein.
10. Um die gesamte Konfiguration, die im Visualizer angezeigt wird, in eine Anwendungsvorlagendatei zu exportieren, klicken Sie auf das Symbol für den virtuellen Content Switching-Server, klicken Sie auf Verwandte Aufgaben, und klicken Sie dann auf Vorlage erstellen. Beim Erstellen der Anwendungsvorlage können Sie Variablen in einigen Richtlinienausdrücken und -aktionen konfigurieren. Weitere Informationen zum Erstellen der Anwendungsvorlagendatei und zum Konfigurieren von Variablen für eine Vorlage finden Sie unter AppExpert.

Anpassen der grundlegenden Content Switching-Konfiguration

October 5, 2021

Nachdem Sie ein grundlegendes Content Switching-Setup konfiguriert haben, müssen Sie es möglicherweise an Ihre Anforderungen anpassen. Wenn Ihre Webserver UNIX-basiert sind und Pfadnamen berücksichtigen, können Sie die Groß-/Kleinschreibung für die Richtlinienbewertung konfigurieren. Sie können auch Vorrang für die Auswertung der von Ihnen konfigurierten Content Switching-Richtlinien festlegen. Sie können HTTP- und SSL-Content Switching-Server so konfigurieren, dass sie mehrere Ports überwachen, anstatt separate virtuelle Server zu erstellen. Wenn Sie Content Switching für ein bestimmtes virtuelles LAN konfigurieren möchten, können Sie einen virtuellen Server mit einer Listenrichtlinie konfigurieren.

Konfigurieren der Berücksichtigung der Groß-/Kleinschreibung für

Sie können den virtuellen Content Switching-Server so konfigurieren, dass URLs in URL-basierten Richtlinien unter Berücksichtigung der Groß- und Kleinschreibung behandelt werden. Wenn die Berücksichtigung der Groß-/Kleinschreibung konfiguriert ist, berücksichtigt die Citrix ADC Appliance den Fall bei der Auswertung von Richtlinien. Wenn beispielsweise die Groß-/Kleinschreibung deaktiviert ist, werden die URLs /a/1.htm und /A/1.HTM als identisch behandelt. Wenn die Groß-/Kleinschreibung aktiviert ist, werden diese URLs als getrennt behandelt und können auf verschiedene Ziele umgestellt werden.

So konfigurieren Sie die Groß-/Kleinschreibung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cs vserver \<name\> -caseSensitive (ON|OFF)
```

Beispiel:

```
1 set cs vserver Vserver-CS-1 -caseSensitive ON
2 <!--NeedCopy-->
```

So konfigurieren Sie die Groß-/Kleinschreibung mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie **unter Erweiterte Einstellungen**die Option **Verkehrseinstellungen**aus, und wählen Sie dann Groß-/Kleinschreibung beachten.

Festlegen der Priorität für die Richtlinienbewertung

Priorität bezieht sich auf die Reihenfolge, in der Richtlinien ausgewertet werden, die an einen virtuellen Server gebunden sind. Sie müssen die Priorität nicht konfigurieren, die Standardrangfolge funktioniert oft korrekt.

Sie können entweder URL-basierte Priorität oder regelbasierte Priorität in den folgenden Szenarien konfigurieren:

- Eine Richtlinie oder ein Satz von Richtlinien muss zuerst angewendet werden
- Eine andere Richtlinie oder ein Satz von Richtlinien wird nur angewendet, wenn der erste Satz nicht mit einer Anforderung übereinstimmt.

Vorrang mit URL-basierten Richtlinien

Wenn mehrere übereinstimmende URLs für die eingehende Anforderung vorhanden sind, lautet die Priorität (Priorität) für URL-basierte Richtlinien:

1. Domain und genaue URL
2. Domäne, Präfix und Suffix
3. Domäne und Suffix
4. Domäne und Präfix
5. Nur Domain
6. Exakte URL
7. Präfix und Suffix
8. Nur Suffix
9. Nur Präfix
10. Standard

Wenn Sie die Priorität basierend auf URL konfigurieren, wird die Anforderungs-URL mit den konfigurierten URLs verglichen. Wenn keine der konfigurierten URLs mit der Anforderungs-URL übereinstimmt, werden regelbasierte Richtlinien überprüft. Wenn die Anforderungs-URL keinen regelbasierten Richtlinien entspricht oder wenn die für die Anforderung ausgewählte Inhaltsgruppe ausgefallen ist, wird die Anforderung wie folgt verarbeitet:

- Wenn Sie eine Standardgruppe für den virtuellen Content Switching-Server konfigurieren, wird die Anforderung an die Standardgruppe weitergeleitet.
- Wenn die konfigurierte Standardgruppe ausgefallen ist oder keine Standardgruppe konfiguriert ist, wird eine Fehlermeldung “HTTP 404 Not Found” an den Client gesendet.

> **Hinweis:**
>
> Sie müssen die URL-basierte Priorität konfigurieren, wenn der Inhaltstyp (z. B. Bilder) für alle Clients gleich ist. Wenn jedoch unterschiedliche Inhaltstypen basierend auf Client-Attributen

> bereitgestellt werden müssen (z. B. Accept-Language), müssen Sie regelbasierte Priorität verwenden.

Vorrang mit regelbasierten Richtlinien

Wenn Sie die Priorität basierend auf Regeln konfigurieren, was die Standardeinstellung ist, wird die Anforderung basierend auf den von Ihnen konfigurierten regelbasierten Richtlinien getestet. Wenn die Anforderung keinen regelbasierten Richtlinien entspricht oder wenn die für die eingehende Anforderung ausgewählte Inhaltsgruppe ausgefallen ist, wird die Anforderung folgendermaßen verarbeitet:

- Wenn eine Standardgruppe für den virtuellen Content Switching-Server konfiguriert ist, wird die Anforderung an die Standardgruppe weitergeleitet.
- Wenn die konfigurierte Standardgruppe heruntergefahren ist oder keine Standardgruppe konfiguriert ist, wird eine Fehlermeldung “HTTP 404 Not Found” an den Client gesendet.

So konfigurieren Sie die Rangfolge mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cs vserver \<name\> -precedence ( RULE | URL )
```

Beispiel:

```
set cs vserver Vserver-CS-1 -precedence RULE
```

So konfigurieren Sie die Rangfolge mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus, und geben Sie dann Priorität an.

Unterstützung für mehrere Ports virtuelle Content Switching-Server der Typen HTTP und SSL

Sie können den Citrix ADC so konfigurieren, dass HTTP- und SSL-Content Switching-Server über mehrere Ports abhören, ohne separate virtuelle Server konfigurieren zu müssen. Diese Funktion ist besonders nützlich, wenn Sie eine Entscheidung über das Content Switching auf einem Teil der URL und anderen L7-Parametern basieren möchten. Anstatt mehrere virtuelle Server mit derselben IP-Adresse und unterschiedlichen Ports zu konfigurieren, können Sie eine IP-Adresse konfigurieren und den Port als * angeben. Dadurch wird auch die Konfigurationsgröße reduziert.

So konfigurieren Sie einen HTTP- oder SSL-Content Switching-Server für das Abhören mehrerer Ports mit der Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cs vserver \<name\> \<serviceType\> \<IPAddress\> Port \*
```

Beispiel

```
> add cs vserver cs1 HTTP 10.102.92.215 *
 Done
> sh cs vserver cs1
        cs1 (10.102.92.215:*) - HTTP    Type: CONTENT
        State: UP
        Last state change was at Tue May 20 01:15:49 2014
        Time since last state change: 0 days, 00:00:03.270
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Appflow logging: ENABLED
        Port Rewrite : DISABLED
        State Update: DISABLED
        Default:        Content Precedence: RULE
        Vserver IP and Port insertion: OFF
        L2Conn: OFF     Case Sensitivity: ON
        Authentication: OFF
        401 Based Authentication: OFF
        Push: DISABLED  Push VServer:
        Push Label Rule: none
        IcmpResponse: PASSIVE
        RHIstate:  PASSIVE
        TD: 0
 Done
<!--NeedCopy-->
```

So konfigurieren Sie einen HTTP- oder SSL-Content Switching-Server für das Abhören mehrerer Ports mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und erstellen Sie einen virtuellen Server vom Typ HTTP oder SSL.
2. Verwenden Sie ein Sternchen (*), um den Port anzugeben.

Konfigurieren von virtuellen Platzhalter-Servern pro VLAN

Wenn Sie Content Switching für Datenverkehr in einem bestimmten VLAN konfigurieren möchten, können Sie einen virtuellen Platzhalterserver mit einer Listening-Richtlinie erstellen, die ihn auf den Verarbeitungsdatenverkehr nur im angegebenen VLAN beschränkt.

So konfigurieren Sie einen virtuellen Platzhalterserver, der ein bestimmtes VLAN mit der Befehlszeilenschnittstelle abhört

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cs vserver <name> <serviceType> IPAddress `* Port *` -listenpolicy
   <expression> [-listenpriority <positive_integer>]
<!--NeedCopy-->
```

Beispiel:

```
add cs vserver Vserver-CS-vlan1 ANY * *
-listenpolicy ”CLIENT.VLAN.ID.EQ(2)”  -listenpriority 10
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Platzhalterserver, der ein bestimmtes VLAN mit dem Konfigurationsdienstprogramm abhört

Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und konfigurieren Sie einen virtuellen Server. Geben Sie eine Listenrichtlinie an, die darauf beschränkt, Datenverkehr nur im angegebenen VLAN zu verarbeiten.

Nachdem Sie diesen virtuellen Server erstellt haben, binden Sie ihn an einen oder mehrere Dienste, wie unter Basic Load Balancing einrichtenbeschrieben.

Konfigurieren der Microsoft SQL Server-Versionseinstellung

Sie können die Version von Microsoft® SQL Server® für einen virtuellen Content Switching-Server vom Typ MSSQL angeben. Die Versionseinstellung wird empfohlen, wenn Sie erwarten, dass einige Clients nicht dieselbe Version wie Ihr Microsoft SQL Server-Produkt ausführen. Die Versionseinstellung stellt die Kompatibilität zwischen den clientseitigen und serverseitigen Verbindungen bereit, indem sichergestellt wird, dass die gesamte Kommunikation der Serverversion entspricht.

So legen Sie den Microsoft SQL Server-Versionsparameter mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den Microsoft SQL Server-Versionsparameter für einen virtuellen Content Switching-Server festzulegen und die Konfiguration zu überprüfen:

- `set cs vserver \<name\> -mssqlServerVersion \<mssqlServerVersion\>`
- `show cs vserver \<name\>`

Beispiel

```
> set cs vserver myMSSQLcsvip -mssqlServerVersion 2008R2 Done > show cs
    vserver myMSSQLcsvip myMSSQLcsvip (192.0.2.13:1433) - MSSQL Type:
   CONTENT State: UP . . . . . . MSsql Server Version: 2008R2 . . . . .
    . Done >
<!--NeedCopy-->
```

So legen Sie den Microsoft SQL Server-Versionsparameter mit dem Konfigurationsdienstprogramm fest

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, konfigurieren Sie einen virtuellen Server und geben Sie das Protokoll als MYSQL an.
2. Wählen Sie unter **Erweiterte Einstellungen** die Option **MySQL** aus, und geben Sie die **Serverversion**an.

Externe TCP-Zustandsprüfung für virtuelle UDP-Server aktivieren

In Public Clouds können Sie die Citrix ADC Appliance als Load Balancer der zweiten Ebene verwenden, wenn der native Load Balancer als erste Stufe verwendet wird. Der native Load Balancer kann ein Application Load Balancer (ALB) oder ein Network Load Balancer (NLB) sein. Die meisten Public Clouds unterstützen keine UDP-Integritätstrübe in ihren nativen Lastausgleichsdiensten. Um die Integrität der UDP-Anwendung zu überwachen, empfehlen Public Clouds, Ihrem Dienst einen TCP-basierten Endpunkt hinzuzufügen. Der Endpunkt spiegelt die Integrität der UDP-Anwendung wider.

Die Citrix ADC Appliance unterstützt die externe TCP-basierte Zustandsprüfung für einen virtuellen UDP-Server. Mit dieser Funktion wird ein TCP-Listener auf der VIP des virtuellen Content Switching-Servers und des konfigurierten Ports eingeführt. Der TCP-Listener gibt den Status des virtuellen Servers wieder.

So aktivieren Sie die externe TCP-Zustandsprüfung für virtuelle UDP-Server über die Befehlszeile

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine externe TCP-Integritätsprüfung mit der Option TCPProbePort zu aktivieren:

```
1 add cs vserver <name> <protocol> <IPAddress> <port> -tcpProbePort <
     tcpProbePort>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add cs vserver Vserver-CS-1 UDP 10.102.29.161 5002 -tcpProbePort 5000
2 <!--NeedCopy-->
```

So aktivieren Sie die externe TCP-Zustandsprüfung für virtuelle UDP-Server mit der GUI

1. Navigieren Sie zu **Datenverkehrsverwaltung > Content Switching > Virtuelle Server**, und erstellen Sie dann einen virtuellen Server.
2. Klicken Sie auf **Hinzufügen**, um einen virtuellen Server zu erstellen.
3. Fügen Sie im Bereich **Grundeinstellungen** die Portnummer im Feld **TCP-Probe-Port** hinzu.
4. Klicken Sie auf **OK**.

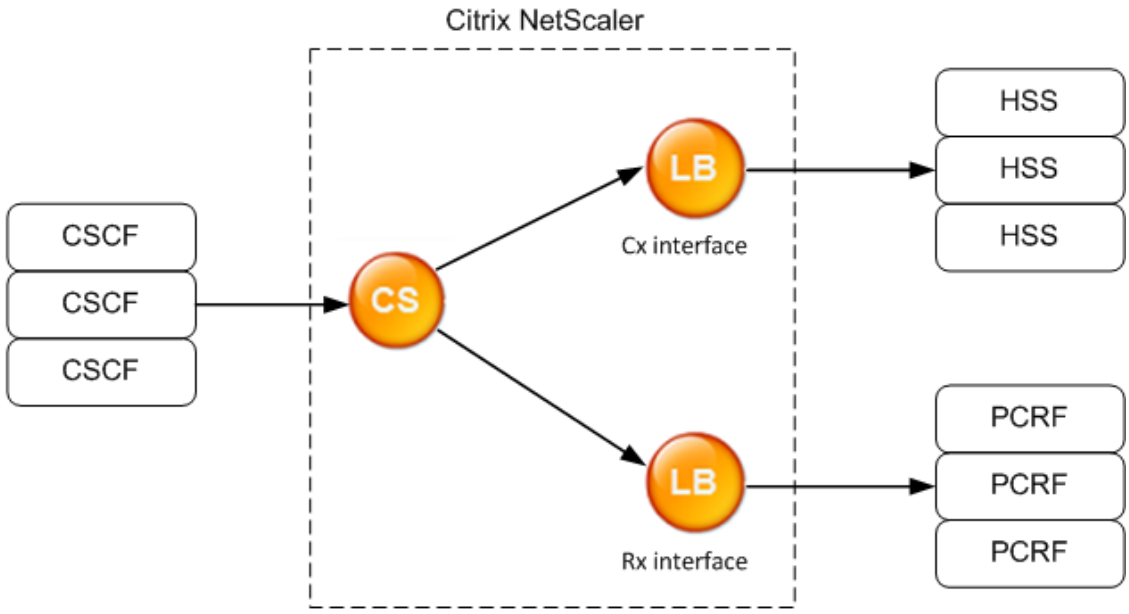
Content Switching für das Diameter-Protokoll

October 5, 2021

Für den Datenverkehr im Diameter-Protokoll können Sie die Citrix ADC Appliance (oder virtuelle Appliance) so konfigurieren, dass sie als Relay-Agent fungiert, der ein Paket basierend auf dem Nachrichteninhalt (AVP-Wert in der Nachricht) an das entsprechende Ziel weiterleitet. Da die Appliance keine Verarbeitung auf Anwendungsebene durchführt, stellt sie Relaying-Dienste für alle Anwendungen mit Durchmesser bereit, die in den konfigurierten Richtlinien für das Content Switching angegeben sind. Daher gibt die Appliance die Relay Application ID in der Meldung Capability Exchange answer (CEA) an, wenn der Client eine Durchmesserverbindung aufbaut. Sie müssen einen virtuellen Content Switching-Server, virtuelle Lastausgleichsserver und Dienste konfigurieren, um die Diameter-Knoten darzustellen. Wenn eine Anforderung den virtuellen Content Switching-Server erreicht, wendet der virtuelle Server die Content Switching-Richtlinien an, die diesem Anforderungstyp

zugeordnet sind. Nach der Auswertung der Richtlinien leitet der virtuelle Content Switching-Server die Anforderung an den entsprechenden virtuellen Lastausgleichsserver weiter, der sie an den entsprechenden Dienst sendet.

Eine Durchmesserschnittstelle stellt eine Verbindung zwischen den verschiedenen Durchmesserknoten bereit. Die folgende Beispielbereitstellung verwendet Cx- und Rx-Schnittstellen. Eine Cx-Schnittstelle stellt eine Verbindung zwischen einem CSCF und einem HSS zur Verfügung. Eine Rx-Schnittstelle stellt eine Verbindung zwischen einem CSCF und einem PCRF bereit. Alle Nachrichten erreichen die Citrix ADC Appliance. Abhängig davon, ob die Nachricht für eine Cx- oder eine RX-Schnittstelle ist, und von den definierten Content Switching-Richtlinien wählt Citrix ADC einen geeigneten Load Balancing Server-Pool aus.



CSCF=Call Session Control Function
HSS=Home Subscriber Server
PCRF=Policy and Charging Rules Function

Beispielkonfiguration

1. Erstellen Sie für jede Entität einen Dienst, einen Lastausgleichsserver, und binden Sie den Dienst an den virtuellen Server.

```
1 add service svc_pcrf[1-3] 1.1.1.1[1-3] DIAMETER 3868
2 add service svc_hss[1-3] 1.1.1.2[1-3] DIAMETER 3868
3 add lb vserver vs_rx DIAMETER -persistenceType DIAMETER -
     persistavpno 263
```



```
4 add lb vserver vs_cx DIAMETER -persistenceType DIAMETER -
    persistavpno 263
5 bind lb vserver vs_rx svc_pcrf[1-3]
6 bind lb vserver vs_cx svc_hss[1-3]
7 <!--NeedCopy-->
```

2. Erstellen Sie einen virtuellen Content Switching-Server und zwei Aktionen (eine für jeden virtuellen Lastausgleichsserver). Erstellen Sie zwei Content Switching-Richtlinien, und binden Sie diese Richtlinien an den virtuellen Content Switching-Server, wobei eine Priorität für jede Richtlinie angegeben wird.

```
1 add cs vserver cs_diameter DIAMETER 10.1.1.10 3868
2 add cs action cx_action -targetLBVserver vs_cx
3 add cs action rx_action - targetLBvserver vs_rx
4 add cs policy cx_policy -rule "DIAMETER.REQ.AUTH_APPLICATION_ID.EQ
    (16777216)" -action cx_action
5 add cs policy rx_policy -rule "DIAMETER.REQ.AUTH_APPLICATION_ID.EQ
    (16777236)" -action rx_action
6 bind cs vserver cs_diameter -policyName rx_policy -priority 100
7 bind cs vserver cs_diameter -policyName cx_policy -priority 110
8 <!--NeedCopy-->
```

Schutz des Content Switching-Setups

October 5, 2021

Content Switching kann fehlschlagen, wenn der virtuelle Content Switching-Server herunterfährt oder übermäßigen Datenverkehr nicht verarbeitet, oder aus anderen Gründen. Um die Ausfallchancen zu verringern, können Sie die folgenden Maßnahmen ergreifen, um die Einrichtung des Content Switchings vor Fehlern zu schützen:

Konfigurieren eines virtuellen Backup-Servers

Wenn der primäre virtuelle Content Switching-Server mit DOWN oder DISABLED gekennzeichnet ist, kann die Citrix ADC Appliance Anforderungen an einen virtuellen Backup-Content Switching-Server weiterleiten. Es kann auch eine Benachrichtigung an den Client über den Standortausfall oder die Wartung senden. Der virtuelle Backup-Content Switching-Server ist ein Proxy und ist für den Client transparent.

Wenn Sie den virtuellen Sicherungsserver konfigurieren, können Sie den Konfigurationsparameter Primäres deaktivieren bei Down angeben, um sicherzustellen, dass der primäre virtuelle Server beim Wiederherstellen des primären Servers der sekundäre bleibt, bis Sie ihn manuell erzwingen, als primärer Server zu übernehmen. Es ist nützlich, wenn Sie sicherstellen möchten, dass alle Aktualisierungen der Datenbank auf dem Server für die Sicherung erhalten bleiben, sodass Sie die Datenbanken vor der Wiederherstellung des primären virtuellen Servers synchronisieren können.

Sie können einen virtuellen Backup-Content Switching-Server konfigurieren, wenn Sie einen virtuellen Content Switching-Server erstellen oder wenn Sie die optionalen Parameter eines vorhandenen virtuellen Content Switching-Servers ändern. Sie können auch einen virtuellen Backup-Content Switching-Server für einen vorhandenen virtuellen Backup-Content Switching-Server konfigurieren und somit kaskadierte Backup-Inhalte erstellen, die virtuelle Server wechseln. Die maximale Tiefe von kaskadierten virtuellen Backup-Content Switching-Server beträgt 10. Die Appliance sucht nach einem virtuellen Backup-Content Switching-Server, der aktiviert ist, und greift auf diesen virtuellen Content Switching-Server zu, um den Inhalt bereitzustellen.

> **Hinweis:**
>
> Wenn ein virtueller Content Switching-Server sowohl mit einem virtuellen Backup-Content Switching-Server als auch mit einer Umleitungs-URL konfiguriert ist, hat der virtuelle Backupserver Vorrang vor der Umleitungs-URL. Die Umleitung wird verwendet, wenn die primären und virtuellen Backup-Server ausfallen.

So richten Sie einen virtuellen Content Switching-Backupserver über die CLI ein

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cs vserver <name> -backupVserver <string> -disablePrimaryOnDown (ON
    |OFF)
<!--NeedCopy-->
```

Beispiel

```
set cs vserver Vserver-CS-1 -backupVserver Vserver-CS-2 -
    disablePrimaryOnDown ON
<!--NeedCopy-->
```


So richten Sie einen virtuellen Content Switching-Backupserver über die GUI ein

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, konfigurieren Sie einen virtuellen Server und geben Sie das Protokoll als MYSQL an.
2. Wählen Sie **unter Erweiterte Einstellungen**die Option **Schutz**aus, und geben Sie einen **virtuellen Sicherungsserver**an.

Umleiten von überschüssigem Datenverkehr auf einen virtuellen Backup-Server

Mit der Option Spillover werden neue Verbindungen, die zu einem virtuellen Content Switching-Server ankommen, auf einen virtuellen Backup-Content Switching-Server umgeleitet, wenn die Anzahl der Verbindungen zum virtuellen Content Switching-Server den konfigurierten Schwellenwert überschreitet. Der Schwellenwert wird dynamisch berechnet, oder Sie können den Wert festlegen. Die Anzahl der etablierten Verbindungen (in TCP) auf dem virtuellen Server wird mit dem Schwellenwert verglichen. Wenn die Anzahl der Verbindungen den Schwellenwert erreicht, werden neue Verbindungen zum virtuellen Backup-Content Switching-Server umgeleitet.

Wenn die virtuellen Backup-Content Switching Server den konfigurierten Schwellenwert erreichen und die Last nicht übernehmen können, leitet der primäre virtuelle Content Switching-Server alle Anforderungen an die Umleitungs-URL um. Wenn keine Umleitungs-URL auf dem primären virtuellen Content Switching-Server konfiguriert ist, werden nachfolgende Anforderungen gelöscht.

So konfigurieren Sie einen virtuellen Content Switching-Server so, dass er neue Verbindungen mit der CLI auf einen virtuellen Backupserver umleitet

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cs vserver <name> -soMethod <methodType> -soThreshold <
    thresholdValue> -soPersistence <persistenceValue> -
    soPersistenceTimeout <timeoutValue>
<!--NeedCopy-->
```

Beispiel

```
set cs vserver Vserver-CS-1 -soMethod Connection -soThreshold 1000 -
    soPersistence enabled -soPersistenceTimeout 2
<!--NeedCopy-->
```


So richten Sie einen virtuellen Content Switching-Server ein, um neue Verbindungen mit der GUI auf einen virtuellen Backupserver umzuleiten

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, konfigurieren Sie einen virtuellen Server und geben Sie das Protokoll als MYSQL an.
2. Wählen Sie **unter Erweiterte Einstellungen**die Option **Schutz**aus, und konfigurieren Sie Spillover.

Konfigurieren einer Umleitungs-URL

Sie können eine Umleitungs-URL konfigurieren, um den Status der Citrix ADC Appliance zu kommunizieren, wenn ein virtueller Content Switching-Server vom Typ HTTP oder HTTPS DOWN oder DISABLED ist. Diese URL kann lokal oder remote sein.

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

Citrix empfiehlt die Verwendung einer absoluten URL. Das heißt, eine URL, die auf/endet, zum Beispiel www.example.com/ statt einer relativen URL. Eine relative URL-Umleitung kann dazu führen, dass der Schwachstellen-Scanner ein falsches Positiv meldet.

> **Hinweis:**
>
> Wenn ein virtueller Content Switching-Server sowohl mit einem virtuellen Backupserver als auch mit einer Umleitungs-URL konfiguriert ist, hat der virtuelle Backupserver Vorrang vor der Umleitungs-URL. Eine Umleitungs-URL wird verwendet, wenn die primären und virtuellen Backup-Server ausfallen.

Wenn die Umleitung konfiguriert ist und der virtuelle Content Switching-Server nicht verfügbar ist, gibt die Appliance eine HTTP 302-Umleitung an den Browser des Benutzers aus.

So konfigurieren Sie eine Umleitungs-URL für den Fall, dass der virtuelle Content Switching-Server nicht verfügbar ist, mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cs vserver <name> -redirectURL <URLValue>
<!--NeedCopy-->
```


Beispiel

```
set cs vserver Vserver-CS-1 -redirectURL http://www.newdomain.com/
   mysite/maintenance
<!--NeedCopy-->
```

So konfigurieren Sie eine Umleitungs-URL für den Fall, dass der virtuelle Content Switching-Server nicht verfügbar ist, mit der GUI

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, konfigurieren Sie einen virtuellen Server und geben Sie das Protokoll als MYSQL an.
2. Wählen Sie **unter Erweiterte Einstellungen**die Option **Schutz**aus, und geben Sie eine Umleitungs-URL an.

Konfigurieren der Option für Statusaktualisierung

Die Content Switching-Funktion ermöglicht die Verteilung von Clientanfragen auf mehreren Servern basierend auf den spezifischen Inhalten, die den Benutzern präsentiert werden. Für ein effizientes Content Switching verteilt der virtuelle Content Switching-Server den Datenverkehr entsprechend dem Inhaltstyp auf die virtuellen Load Balancing-Server, und die virtuellen Load Balancing-Server verteilen den Datenverkehr gemäß der angegebenen Load Balancing-Methode an die physischen Server.

Für eine reibungslose Datenverkehrsverwaltung ist es wichtig, dass der virtuelle Content Switching-Server den Status der virtuellen Lastausgleichsserver kennt. Die Statusaktualisierungsoption hilft, den virtuellen Content Switching-Server DOWN zu markieren, wenn der an ihn gebundene virtuelle Lastausgleichsserver als DOWN markiert ist. Ein virtueller Lastausgleichsserver wird mit DOWN gekennzeichnet, wenn alle an ihn gebundenen physischen Server als DOWN gekennzeichnet sind.

Wenn Statusaktualisierung deaktiviert ist:

Der Status des virtuellen Content Switching-Servers wird als UP markiert. Es bleibt UP, selbst wenn kein gebundener Lastausgleichsserver vorhanden ist, der UP ist.

Wenn Statusaktualisierung aktiviert ist:

Wenn Sie einen virtuellen Content Switching-Server hinzufügen, wird sein Status zunächst als DOWN angezeigt. Wenn Sie einen virtuellen Lastausgleichsserver binden, dessen Status UP ist, wird der Status des virtuellen Content Switching-Servers UP.

Wenn mehr als ein virtueller Lastausgleichsserver gebunden ist und einer von ihnen als Standard angegeben ist, spiegelt der Status des virtuellen Content Switching-Servers den Status des standardmäßigen virtuellen Lastausgleichsservers wider.

Wenn mehr als ein virtueller Lastausgleichsserver gebunden ist, ohne dass einer von ihnen als Standard angegeben wird, wird der Status des virtuellen Content Switching-Servers nur dann als UP markiert, wenn alle gebundenen virtuellen Server für den Lastausgleich UP sind.

So konfigurieren Sie die Option für Statusaktualisierungen mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add cs vserver <name> <protocol> <ipAddress> <port> -stateUpdate
     ENABLED
2 <!--NeedCopy-->
```

Beispiel

```
1  add cs vserver csw_vserver HTTP 10.18.250.154 80 -stateupdate ENABLED
      -cltTimeout 180
2 <!--NeedCopy-->
```

So konfigurieren Sie die Option für Statusaktualisierungen mit der GUI

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, konfigurieren Sie einen virtuellen Server und geben Sie das Protokoll als MYSQL an.
2. Wählen Sie unter **Erweiterte Einstellungen** die Option **Verkehrseinstellungen** und wählen Sie dann **Statusaktualisierung**.

Flush der Surge Queue

Wenn ein physischer Server eine Welle von Anforderungen empfängt, wird es langsam, auf die Clients zu reagieren, die derzeit mit ihm verbunden sind, was die Benutzer unzufrieden und verärgert lässt. Oft führt die Überlastung auch dazu, dass Clients Fehlerseiten erhalten. Um solche Überlastungen zu vermeiden, bietet die Citrix ADC Appliance Funktionen wie Überspannungsschutz, die die Geschwindigkeit steuert, mit der neue Verbindungen zu einem Dienst hergestellt werden können.

Die Appliance verbindet Multiplexing zwischen Clients und physischen Servern. Wenn es eine Clientanforderung für den Zugriff auf einen Dienst auf einem Server erhält, sucht die Appliance nach einer bereits eingerichteten Verbindung mit dem Server, die frei ist. Wenn eine freie Verbindung gefunden wird, wird diese Verbindung verwendet, um eine virtuelle Verbindung zwischen dem Client und dem Server herzustellen. Wenn es keine vorhandene freie Verbindung findet, baut die Appliance

eine neue Verbindung mit dem Server auf und stellt eine virtuelle Verbindung zwischen dem Client und dem Server her. Wenn die Appliance jedoch keine neue Verbindung mit dem Server herstellen kann, sendet sie die Clientanforderung an eine Überspannungswarteschlange. Wenn alle physischen Server, die an den virtuellen Lastausgleichs- oder Content Switching-Server gebunden sind, die obere Grenze für Clientverbindungen erreichen (maximaler Clientwert, Überspannungsschutzschwelle oder maximale Kapazität des Dienstes), kann die Appliance keine Verbindung zu einem Server herstellen. Die Überspannungsschutzfunktion verwendet die Überspannungswarteschlange, um die Geschwindigkeit zu regulieren, mit der Verbindungen mit den physischen Servern geöffnet werden. Die Appliance verwaltet eine andere Überspannungswarteschlange für jeden Dienst, der an den virtuellen Server gebunden ist.

Die Länge einer Überspannungswarteschlange erhöht sich, wenn eine Anforderung eingeht, für die die Appliance keine Verbindung herstellen kann, und die Länge nimmt ab, wenn eine Anforderung in der Warteschlange an den Server gesendet wird oder eine Anforderung ein Timeout erreicht und aus der Warteschlange entfernt wird.

Wenn die Überspannungswarteschlange für einen Dienst oder eine Dienstgruppe zu lang wird, sollten Sie sie möglicherweise leeren. Sie können die Überspannungswarteschlange eines bestimmten Dienstes oder einer bestimmten Dienstgruppe oder aller Dienste und Dienstgruppen, die an einen virtuellen Lastausgleichsserver gebunden sind, leeren. Das Leeren einer Überspannungswarteschlange wirkt sich nicht auf die vorhandenen Verbindungen aus. Nur die Anforderungen, die in der Überspannungswarteschlange vorhanden sind, werden gelöscht. Für diese Anfragen muss der Kunde eine neue Anfrage stellen.

Sie können auch die Überspannungswarteschlange eines virtuellen Content Switching-Servers löschen. Wenn ein virtueller Content Switching-Server einige Anfragen an einen bestimmten virtuellen Lastausgleichsserver weiterleitet und der virtuelle Lastausgleichsserver auch einige andere Anfragen empfängt, wenn Sie die Überspannungswarteschlange des virtuellen Content Switching-Servers leeren, nur die Anfragen, die von diesem Content Switching empfangen wurden virtuelle Server werden geleert. Die anderen Anforderungen in der Überspannungswarteschlange des virtuellen Lastausgleichsservers werden nicht geleert.

> **Hinweis:**
>
> Sie können die Anstiegswarteschlangen von Cache-Umleitungen, Authentifizierung, VPN oder virtuellen GSLB-Servern oder GSLB-Diensten nicht leeren.
> Verwenden Sie die Überspannungsschutzfunktion nicht, wenn die Option “Quell-IP (USIP) verwenden” aktiviert ist.

So leeren Sie eine Überspannungswarteschlange mit der CLI

Der Befehl flush ns SurgeQ funktioniert wie folgt:

- Sie können den Namen eines Dienstes, einer Dienstgruppe oder eines virtuellen Servers angeben, dessen Überspannungswarteschlange geleert werden muss.
- Wenn Sie während der Ausführung des Befehls einen Namen angeben, wird die Überspannungswarteschlange der angegebenen Entität geleert. Wenn mehr als eine Entität denselben Namen hat, lötet die Appliance die Überspannungswarteschlangen aller dieser Entitäten.
- Wenn Sie den Namen einer Dienstgruppe und einen Servernamen und einen Port angeben, während der Befehl ausgeführt wird, löscht die Appliance die Überspannungswarteschlange nur des angegebenen Dienstgruppenmitglieds.
- Sie können ein Dienstgruppenmitglied (<serverName> und <port>) nicht direkt angeben, ohne den Namen der Dienstgruppe (<name>) anzugeben, und Sie können nicht <port> ohne einen angeben <serverName>. Geben Sie die <serverName> und an, <port> wenn Sie die Überspannungswarteschlange für ein bestimmtes Dienstgruppenmitglied leeren möchten.
- Wenn Sie den Befehl ausführen, ohne Namen anzugeben, legt die Appliance die Überspannungswarteschlangen aller auf der Appliance vorhandenen Entitäten.
- Wenn ein Dienstgruppenmitglied mit einem Servernamen identifiziert wird, müssen Sie den Servernamen in diesem Befehl angeben. Sie können die IP-Adresse nicht angeben.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
flush ns surgeQ [-name <name>] [-serverName <serverName> <port>].
<!--NeedCopy-->
```

Beispiele

```
1. flush ns surgeQ -name SVC1ANZGB -serverName 10.10.10.1 80
The above command flushes the surge queue of the service or virtual
   server that is named SVC1ANZGB and has IP address as 10.10.10

2. flush ns surgeQ
The above command flushes all the surge queues on the appliance.
<!--NeedCopy-->
```

So leeren Sie eine Überspannungswarteschlange mit der GUI

Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, wählen Sie einen virtuellen Server aus und wählen Sie in der Liste Aktion die Option **Flush Surge Queue** löschen aus.

Verwalten eines Content Switching-Setups

October 5, 2021

Nachdem ein Content Switching-Setup konfiguriert wurde, sind möglicherweise regelmäßige Änderungen erforderlich. Wenn Betriebssysteme oder Software aktualisiert werden oder die Hardware verschleißt und ersetzt wird, müssen Sie möglicherweise Ihre Einrichtung abbauen. Die Belastung Ihres Setups kann zunehmen und mehr Ressourcen erfordern. Sie können die Konfiguration auch ändern, um die Leistung zu verbessern.

Diese Aufgaben erfordern möglicherweise die Aufhebung der Bindung von Richtlinien vom virtuellen Content Switching-Server oder das Deaktivieren oder Entfernen virtueller Content Switching-Server. Nachdem Sie Ihr Setup geändert haben, müssen Sie möglicherweise Server und Nachbindungsrichtlinien erneut aktivieren. Möglicherweise möchten Sie auch Ihre virtuellen Server umbenennen.

Aufheben der Bindung von Richtlinien vom virtuellen Content Switching-Server

Wenn Sie die Bindung einer Content Switching-Richtlinie von ihrem virtuellen Server aufheben, enthält der virtuelle Server diese Richtlinie nicht mehr, wenn Sie festlegen, wohin Anforderungen weitergeleitet werden sollen.

So heben Sie die Bindung einer Richtlinie von einem virtuellen Content Switching-Server mit der CLI auf

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
unbind cs vserver <name> -policyname <string>
```

Beispiel:

```
unbind cs vserver Vserver-CS-1 -policyname Policy-CS-1
```

So heben Sie die Bindung einer Richtlinie von einem virtuellen Content Switching-Server mit der GUI auf

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie den virtuellen Server.
2. Klicken Sie auf **Richtlinien**, wählen Sie die Richtlinie aus, und klicken Sie auf **Binden** .

Entfernen virtueller Content Switching-Server

Normalerweise entfernen Sie einen virtuellen Content Switching-Server nur, wenn Sie den virtuellen Server nicht mehr benötigen. Wenn Sie einen virtuellen Content Switching-Server entfernen, hebt die Citrix ADC Appliance zunächst alle Richtlinien vom virtuellen Content Switching-Server auf und entfernt ihn dann.

So entfernen Sie einen virtuellen Content Switching-Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm cs vserver <name>
```

Beispiel:

```
rm cs vserver Vserver-CS-1
```

So entfernen Sie einen virtuellen Content Switching-Server mit der GUI

Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, wählen Sie einen virtuellen Server aus, und klicken Sie auf **Löschen**.

Deaktivieren und erneutes Aktivieren virtueller Content Switching-Server

Virtuelle Content Switching-Server sind standardmäßig aktiviert, wenn Sie sie erstellen. Sie können einen virtuellen Content Switching-Server für die Wartung deaktivieren. Wenn Sie den virtuellen Content Switching-Server deaktivieren, ändert sich der Status des virtuellen Content Switching-Servers zur in Out of Service. Wenn der virtuelle Content Switching-Server nicht verfügbar ist, reagiert er nicht auf Anforderungen.

So deaktivieren oder reaktivieren Sie einen virtuellen Server mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- `disable cs vserver <name>`
- `enable cs vserver <name>`

Beispiel:

```
disable cs vserver Vserver-CS-1
enable cs vserver Vserver-CS-1
```


So deaktivieren oder reaktivieren Sie einen virtuellen Server mit der GUI

Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, wählen Sie einen virtuellen Server aus, und wählen Sie in der Liste **Aktion** die Option **Aktivieren** oder **Deaktivieren** aus.

Umbenennen von virtuellen Content Switching-Servern

Sie können einen virtuellen Content Switching-Server umbenennen, ohne die Bindung aufzuheben. Der neue Name wird automatisch an alle betroffenen Teile der Citrix ADC Konfiguration weitergegeben.

So benennen Sie einen virtuellen Server mit der CLI um

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rename cs vserver <name> <newName>
```

Beispiel:

```
1 `rename cs vserver Vserver-CS-1 Vserver-CS-2`
```

So benennen Sie einen virtuellen Server mit der GUI um

Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, wählen Sie einen virtuellen Server aus, und wählen Sie in der Liste **Aktion** die Option **Umbenennen** aus.

Verwalten von Content Switching-Richtlinien

Sie können eine vorhandene Richtlinie ändern, indem Sie die Regeln konfigurieren oder die URL der Richtlinie ändern, oder Sie können eine Richtlinie entfernen. Sie können auch eine vorhandene erweiterte Content Switching-Richtlinie umbenennen. Sie können verschiedene Richtlinien basierend auf der URL erstellen. URL-basierte Richtlinien können von verschiedenen Typen sein, wie in der folgenden Tabelle beschrieben.

Weitere Informationen finden Sie unter Beispiele für URL-basierte Richtlinien.

> **Hinweis:**
>
> Sie können regelbasiertes Content Switching mit klassischen Richtlinienausdrücken oder erweiterten Richtlinienausdrücken konfigurieren.

So ändern, entfernen oder benennen Sie eine Richtlinie über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- `set cs policy <policyName> [-domain <domainValue>] [-rule <ruleValue>] [-url <URLValue>]`
- `rm cs policy <policyName>`
- `rename cs policy <policyName> <newPolicyName>`

Beispiel:

```
set cs policy Policy-CS-1 -domain ”www.domainxyz.com”

set cs policy Policy-CS-1 -rule ”CLIENT.IP.SRC.SUBNET(22).EQ
    (10.100.148.0)”

set cs policy Policy-CS-2 -rule ”SYS.TIME.BETWEEN(GMT 2010 Jun,GMT 2010
     Jul)”

set cs policy Policy-CS-1 -url /sports/*

rename cs policy Policy-CS-1 Policy-CS-11

rm cs policy Policy-CS-1
```

So ändern, entfernen oder benennen Sie eine Richtlinie über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > Content Switching > Richtlinien**.
2. Wählen Sie die Richtlinie aus, löschen Sie sie, bearbeiten Sie sie oder klicken Sie in der Liste **Aktion** auf **Umbenennen** .

Verwalten von Clientverbindungen

October 5, 2021

Um eine effiziente Verwaltung der Clientverbindungen zu gewährleisten, können Sie die virtuellen Content Switching-Server auf der Citrix ADC Appliance so konfigurieren, dass die folgenden Funktionen verwendet werden:

- **Konfigurieren der ICMP-Antwort.** Sie können die Citrix ADC Appliance so konfigurieren, dass ICMP-Antworten an PING-Anforderungen entsprechend Ihren Einstellungen gesendet werden.

Legen Sie unter der IP-Adresse, die dem virtuellen Server entspricht, die ICMP RESPONSE auf VSVR_CNTRLD und auf dem virtuellen Server den virtuellen ICMP-Server RESPONSE fest.
Die folgenden Einstellungen können auf einem virtuellen Server vorgenommen werden:

- Wenn Sie den virtuellen ICMP-Server RESPONSE auf allen virtuellen Servern auf PASSIVE festlegen, antwortet die Citrix ADC Appliance immer.
- Wenn Sie den virtuellen ICMP-Server RESPONSE auf allen virtuellen Servern auf ACTIVE festlegen, antwortet die ADC-Appliance, selbst wenn ein virtueller Server UP ist.
- Wenn Sie den virtuellen ICMP-Server RESPONSE auf ACTIVE und bei anderen PASSIVE festlegen, reagiert die ADC-Appliance auch dann, wenn ein auf ACTIVE gesetzter virtueller Server UP ist.

Umleiten von Clientanforderungen in einen Cache

Die Citrix ADC Cache-Umleitungsfunktion leitet HTTP-Anforderungen an einen Cache um. Sie können den Aufwand für die Beantwortung von HTTP-Anfragen erheblich reduzieren und die Leistung Ihrer Website durch die ordnungsgemäße Implementierung der Cache-Umleitungsfunktion verbessern.

Ein Cache speichert häufig angeforderten HTTP-Inhalt. Wenn Sie die Cache-Umleitung auf einem virtuellen Server konfigurieren, sendet die Citrix ADC Appliance zwischenspeicherbare HTTP-Anforderungen an den Cache und nicht zwischenspeicherbare HTTP-Anforderungen an den Ursprungs-Webserver. Weitere Informationen zur Cache-Umleitung finden Sie unter “Cache-Umleitung.

So konfigurieren Sie die Cache-Umleitung auf einem virtuellen Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cs vserver \<name\> -cacheable \<Value\>
```

Beispiel

```
set cs vserver Vserver-CS-1 -cacheable yes
```

So konfigurieren Sie die Cache-Umleitung auf einem virtuellen Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter **Erweiterte Einstellungen** die Option **Verkehrseinstellungen** und wählen Sie **Cacheable**.

Aktivieren der verzögerten Bereinigung von virtuellen Serververbindungen

Unter bestimmten Bedingungen können Sie die Einstellung Downstate Flush so konfigurieren, dass vorhandene Verbindungen beendet werden, wenn ein Dienst oder ein virtueller Server als DOWN gekennzeichnet ist. Durch das Beenden vorhandener Verbindungen werden Ressourcen freigegeben und in bestimmten Fällen wird die Wiederherstellung überlasteter Lastausgleichseinstellungen beschleunigt.

So konfigurieren Sie die Einstellung zum Ausfallzustand auf einem virtuellen Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cs vserver \<name\> -downStateFlush \<Value\>
```

Beispiel

```
1 set cs vserver Vserver-CS-1 -downStateFlush enabled
2 <!--NeedCopy-->
```

So konfigurieren Sie die Einstellung zum Ausfallzustand auf einem virtuellen Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter **Erweiterte Einstellungen** die Option **Verkehrseinstellungen** aus, und wählen Sie dann **Down State Flush**aus.

Umschreiben von Ports und Protokollen für die Umleitung

Virtuelle Server und die an sie gebundenen Dienste verwenden möglicherweise verschiedene Ports. Wenn ein Dienst auf eine HTTP-Verbindung mit einer Weiterleitung reagiert, müssen Sie möglicherweise die Citrix ADC Appliance so konfigurieren, dass der Port und das Protokoll geändert werden, um sicherzustellen, dass die Umleitung erfolgreich durchgeführt wird. Sie tun dies, indem Sie die Einstellung redirectPortRewrite aktivieren und konfigurieren.

So konfigurieren Sie die HTTP-Umleitung auf einem virtuellen Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cs vserver \<name\> -redirectPortRewrite \<Value\>
```


Beispiel

```
set cs vserver Vserver-CS-1 -redirectPortRewrite enabled
<!--NeedCopy-->
```

So konfigurieren Sie die HTTP-Umleitung auf einem virtuellen Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie **unter Erweiterte Einstellungen**die Option **Verkehrseinstellungen**und dann **Umschreiben**aus.

Einfügen der IP-Adresse und des Ports eines virtuellen Servers in den Request-Header

Wenn Sie über mehrere virtuelle Server verfügen, die mit verschiedenen Anwendungen auf demselben Dienst kommunizieren, müssen Sie die Citrix ADC Appliance so konfigurieren, dass die IP-Adresse und Portnummer des entsprechenden virtuellen Servers den HTTP-Anforderungen hinzugefügt werden, die an diesen Dienst gesendet werden. Mit dieser Einstellung können Anwendungen, die auf dem Dienst ausgeführt werden, den virtuellen Server identifizieren, der die Anforderung gesendet hat.

Wenn der primäre virtuelle Server ausgefallen ist und der virtuelle Backupserver hochgefahren ist, werden die Konfigurationseinstellungen des virtuellen Backupservers den Clientanforderungen hinzugefügt. Wenn dasselbe Header-Tag hinzugefügt werden soll, unabhängig davon, ob die Anforderungen vom primären virtuellen Server oder virtuellen Backup-Server stammen, müssen Sie das erforderliche Header-Tag auf beiden virtuellen Servern konfigurieren.

> **Hinweis:**
>
> Diese Option wird nicht für virtuelle Platzhalterserver oder virtuelle Dummy-Server unterstützt.

So fügen Sie die IP-Adresse und den Port des virtuellen Servers in die Clientanforderungen mit der CLI ein

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cs vserver \<name\> -insertVserverIPPort \<vServerIPPORT\>
```

Beispiel


```
set cs vserver Vserver-CS-1 -insertVserverIPPort 10.201.25.136:80
<!--NeedCopy-->
```

So fügen Sie die IP-Adresse und den Port des virtuellen Servers in die Clientanforderungen mit der GUI ein

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie in **Erweiterte Einstellungen**die Option **Verkehrseinstellungen** und wählen Sie in der Liste IP-Porteinfügung des virtuellen Servers die Option VIPADDR oder V6TOV4MAPPING aus, und geben Sie einen Port-Header im IP-Port-Einfügewert des virtuellen Servers an.

Festlegen eines Timeoutwerts für Leerlauf-Clientverbindungen

Sie können einen virtuellen Server so konfigurieren, dass alle inaktiv gefahrenen Clientverbindungen beendet werden, nachdem ein konfigurierter Zeitüberschreitungszeitraum abgelaufen ist. Wenn Sie diese Einstellung konfigurieren, wartet die Citrix ADC Appliance auf die angegebene Zeit und schließt die Clientverbindung, wenn sich der Client nach diesem Zeitpunkt im Leerlauf befindet.

So legen Sie einen Timeoutwert für Leerlauf-Clientverbindungen mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cs vserver \<name\> -cltTimeout \<Value\>
```

Beispiel

```
set cs vserver Vserver-CS-1 -cltTimeout 100
<!--NeedCopy-->
```

So legen Sie einen Timeoutwert für Leerlauf-Clientverbindungen mit der GUI fest

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie **unter Erweiterte Einstellungen**die Option **Verkehrseinstellungen**aus, und geben Sie einen Wert für die **Zeitüberschreitung des Clients**an.

Identifizieren von Verbindungen mit den Verbindungsparametern 4-Tupeln und Layer 2

Sie können nun die Option L2Conn für einen virtuellen Content Switching-Server festlegen. Mit der Option L2Conn werden Verbindungen zum virtuellen Content Switching-Server durch die Kombination der Verbindungsparameter 4-Tupeln (<source IP>:<source port>::<destination IP>:<destination port>) und Layer 2 identifiziert. Die Layer-2-Verbindungsparameter sind die MAC-Adresse, die VLAN-ID und die Kanal-ID.

So legen Sie die Option L2Conn für einen virtuellen Content Switching-Server über die CLI fest

Geben Sie in der Befehlszeile die folgenden Befehle ein, um den Parameter L2Conn für einen virtuellen Content Switching-Server zu konfigurieren und die Konfiguration zu überprüfen:

```
1 -  set cs vserver \<name\> -l2Conn (**ON** | **OFF**)
2 -  show cs vserver \<name\>
```

Beispiel

```
1  > set cs vserver mycsvserver -l2Conn ON
2  Done
3  > show cs vserver mycsvserver
4       mycsvserver (192.0.2.56:80) - HTTP   Type: CONTENT
5       State: UP
6           . . .
7           . . .
8       L2Conn: ON Case Sensitivity: ON
9           . . .
10          . . .
11 Done
12 >
13 <!--NeedCopy-->
```

So legen Sie die Option L2Conn für einen virtuellen Content Switching-Server über die GUI fest

1. Navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie **unter Erweiterte Einstellungen**die Option **Verkehrseinstellungen**und dann **Layer-2-Parameter**aus.

Persistenzunterstützung für virtuellen Content Switching-Server

December 7, 2021

Anwendungen bewegen sich von monolithischen Architekturen hin zu Microservices-Architektur. Verschiedene Versionen derselben Anwendung können in der Microservices-Architektur koexistieren. Die Citrix ADC Appliance muss die kontinuierliche Bereitstellung von Anwendungen unterstützen. Dies wird von Plattformen erreicht, die Canary-Bereitstellungen durchführen (wie Spinnaker). Bei einer kontinuierlichen Bereitstellung wird eine neuere Version einer Anwendung automatisch bereitgestellt und dem Clientdatenverkehr in Stufen ausgesetzt, bis die Anwendung stabil ist, um vollständigen Datenverkehr zu übernehmen. Außerdem müssen ununterbrochene Dienste für den Client vorhanden sein.

Mit Citrix ADC Content Switching kann Citrix ADC die Appliance Clientanforderungen auf mehrere virtuelle Lastausgleichsserver verteilen, basierend auf den Richtlinien, die an den virtuellen Content Switching-Server gebunden sind.

Bei kontinuierlichen Bereitstellungen wird Content Switching verwendet, um den virtuellen Lastausgleichsserver auszuwählen, der verschiedene Versionen einer Anwendung bedient.

Beim Content Switching ändert sich die Auswahl eines virtuellen Lastausgleichsservers für eine bestimmte Anwendungsversion zur Laufzeit aufgrund der Änderung der Content Switching-Richtlinien. Wenn während dieses Übergangs einige Sitzungen mit älteren Versionen der Anwendung vorhanden sind, muss dieser Datenverkehr weiterhin nur von älteren Versionen bedient werden. Um die Anforderung zu unterstützen, behält die Citrix ADC Appliance die Persistenz über mehrere Lastausgleichsgruppen hinter einem virtuellen Content Switching-Server bei. Persistenz für virtuelle Content Switching-Server ermöglicht einen nahtlosen Übergang von Clients von einer Version zur anderen.

Unterstützte Persistenztypen auf einem virtuellen Content Switching-Server

Die folgenden Persistenztypen werden auf virtuellen Content Switching-Servern unterstützt.

Persistenzart	Beschreibung
Quell-IP	**SOURCEIP**. Verbindungen von derselben Client-IP-Adresse sind Teile derselben Persistenzsitzung. Weitere Informationen finden Sie unter Persistenz der Quell-IP-Adresse.

Persistenzart	Beschreibung
HTTP-Cookie	**COOKIEINSERT**. Verbindungen, die denselben HTTP-Cookie-Header haben, sind Teile derselben Persistenzsitzung. Das Cookie-Format, das von der Citrix ADC Appliance eingefügt wird, lautet: NSC_<vid_str of CSvserver> = <vid_str of Lbvserver> wobei NSC_XXXX die virtuelle Server-ID ist, die vom virtuellen Servernamen abgeleitet wird. Weitere Informationen finden Sie unter HTTP-Cookie-Persistenz.
SSL Session ID	**SSLSESSION**. Verbindungen, die dieselbe SSL-Sitzungs-ID haben, sind Teile derselben Persistenzsitzung. Weitere Informationen finden Sie unter SSL-Sitzungs-ID-Persistenz.

Sie können einen Timeout-Wert für die Persistenz konfigurieren, der auf HTTP-Cookies basiert. Wenn Sie den Timeout-Wert auf 0 festlegen, gibt die ADC-Appliance unabhängig von der verwendeten HTTP-Cookie-Version die Ablaufzeit nicht an. Die Ablaufzeit hängt dann von der Client-Software ab, und solche Cookies sind nur gültig, wenn die Software läuft.

Abhängig vom Typ der Persistenz, die Sie konfiguriert haben, kann der virtuelle Server entweder 250.000 gleichzeitige persistente Verbindungen oder eine beliebige Anzahl persistenter Verbindungen unterstützen, bis zu den Grenzwerten, die der Arbeitsspeicher auf Ihrer Citrix ADC Appliance auferlegt wird. Die folgende Tabelle zeigt, welche Persistenzarten in jede Kategorie fallen.

Persistenzart	Anzahl der gleichzeitig unterstützten persistenten Verbindungen
Quell-IP, SSL-Sitzungs-ID	250,000
HTTP-Cookie	Speicherbegrenzung. Wenn in CookieInsert das Timeout nicht 0 ist, ist die Anzahl der Verbindungen durch den Arbeitsspeicher begrenzt.

Einige Persistenzarten sind spezifisch für bestimmte Arten von virtuellen Servern. In der folgenden Tabelle werden die einzelnen Persistenztypen aufgelistet und angegeben, welche Persistenzarten auf welchen Arten von virtuellen Servern unterstützt werden.

Persistenzart	HTTP	HTTPS	TCP	UDP/IP	SSL_Bridge	SSL_TCP	RTSP	SIP_UDP
SOURCEI	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
COOKIEINSERT	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
SSLSESSI	Nein	Ja	Nein	Nein	Ja	Ja	Nein	Nein

Unterstützung für Backup-Persistenzunterstützung

Sie können den virtuellen Content Switching-Server so konfigurieren, dass er den Quell-IP-Persistenztyp als Backup-Persistenztyp verwendet, wenn der Cookie-Persistenztyp fehlschlägt. Es ist nützlich für kanarische Bereitstellungen in der Microservices-Architektur.

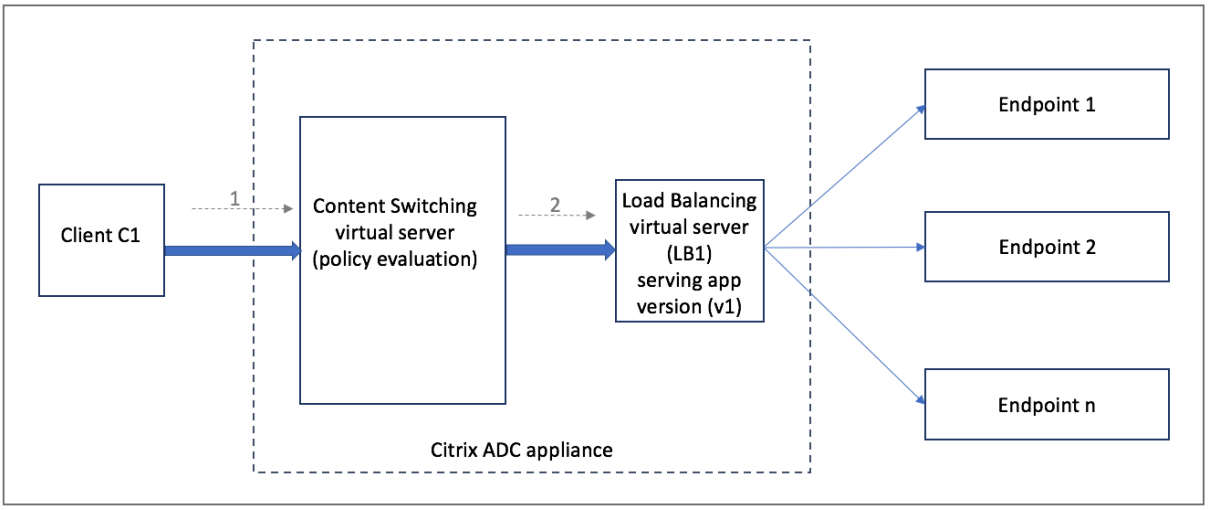
Wenn der Cookie-Persistenztyp fehlschlägt, greift die Appliance nur dann auf die Quell-IP-basierte Persistenz zurück, wenn der Client-Browser kein Cookie in der Anforderung zurückgibt. Wenn der Browser jedoch ein Cookie zurückgibt (nicht notwendigerweise das Persistenz-Cookie), wird davon ausgegangen, dass der Browser Cookies unterstützt und somit Backup-Persistenz nicht ausgelöst wird.

Sie können auch einen Timeout-Wert für die Backup-Persistenz festlegen. Timeout ist der Zeitraum, für den eine Persistenzsitzung in Kraft ist.

Funktionsweise der Persistenz des virtuellen Content Switching-Servers

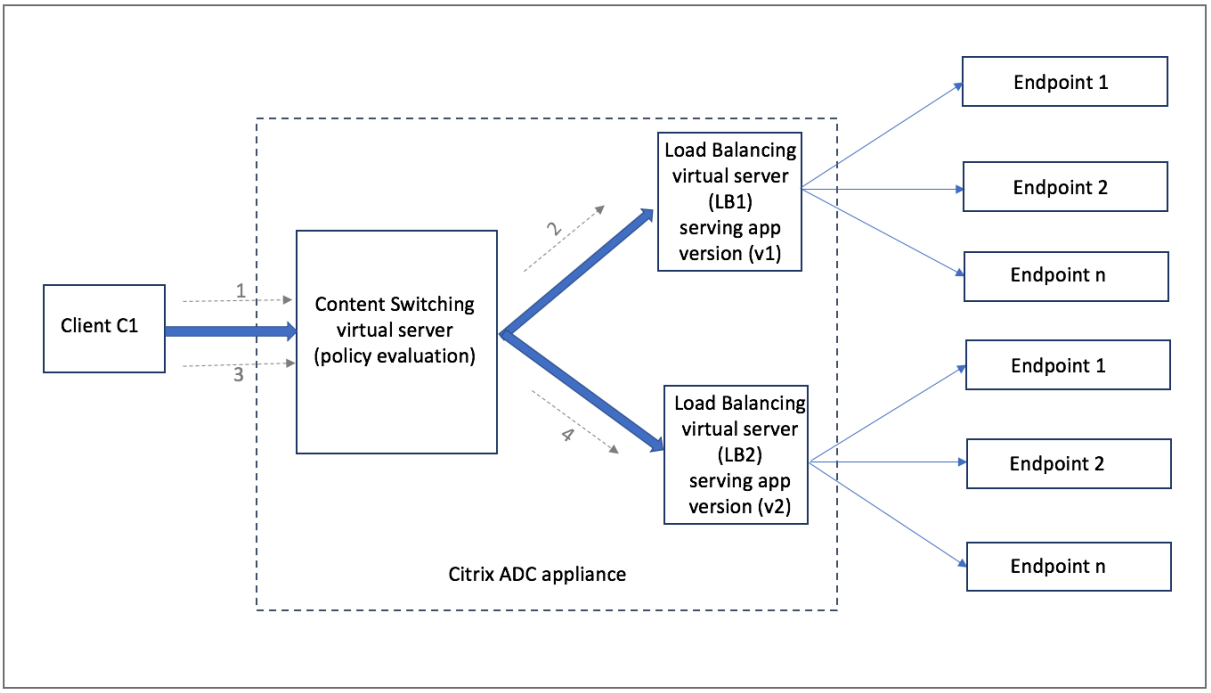
Szenario 1: Ein virtueller Content Switching-Server ohne Persistenz

Das folgende Beispiel veranschaulicht die Bereitstellung mehrerer Versionen einer Anwendung mit einem virtuellen Content Switching-Server ohne Persistenz.



Wenn Client C1 eine Anforderung an die Anwendung sendet, wird die Anforderung an den virtuellen

Content Switching-Server in der Citrix ADC Appliance gesendet. Der virtuelle Content Switching-Server wertet die Richtlinie aus und leitet die Anforderung an den virtuellen Lastausgleichsserver (LB1) weiter, der Version v1 der Anwendung bereitstellt.

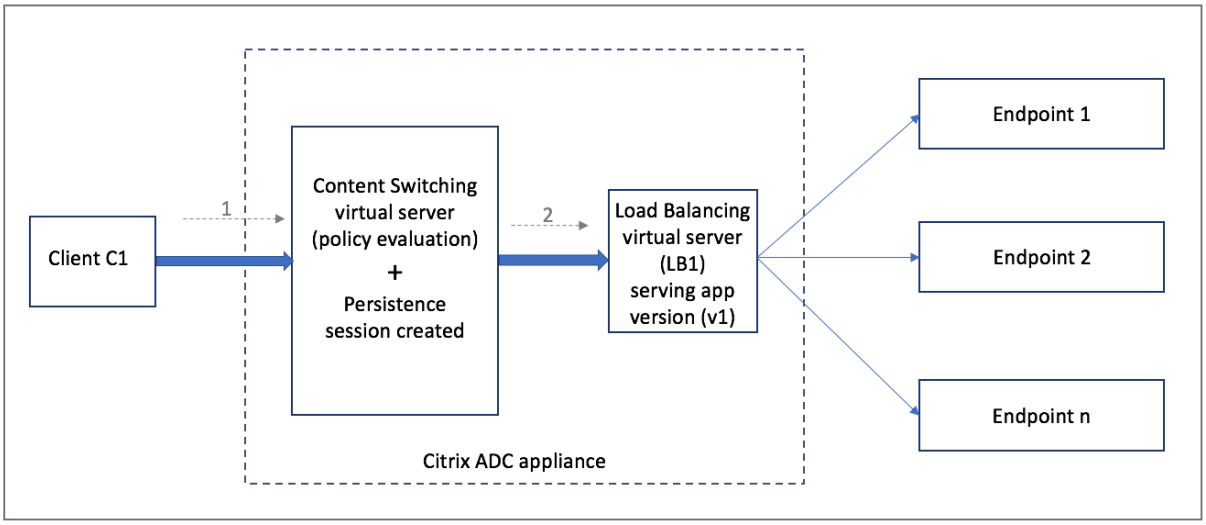


Betrachten Sie, dass eine neue Version v2 der Anwendung bereitgestellt wird und einer Teilmenge von Benutzern zugänglich gemacht werden muss. Der neue virtuelle Lastausgleichsserver (LB2), der die v2-Version bedient, ist durch die entsprechende Content Switching-Richtlinie an den virtuellen Content Switching-Server gebunden.

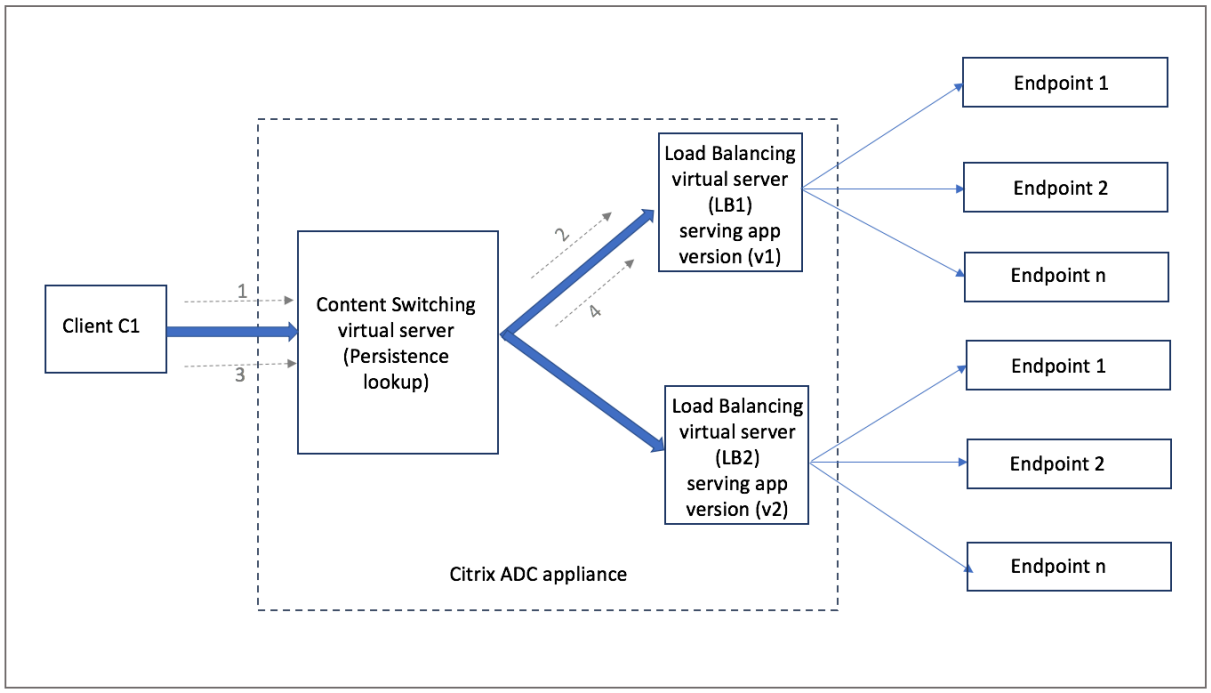
Wenn Client C1 eine neue Anforderung sendet, wird die Richtlinie erneut ausgewertet und die Anforderung wird an den virtuellen Lastausgleichsserver LB2 weitergeleitet. Daher schlagen die Transaktionen für statusbehaftete Anwendungen fehl, wenn mehrere Versionen der Anwendung bereitgestellt werden.

Szenario 2: Virtueller Content Switching-Server mit Persistenz

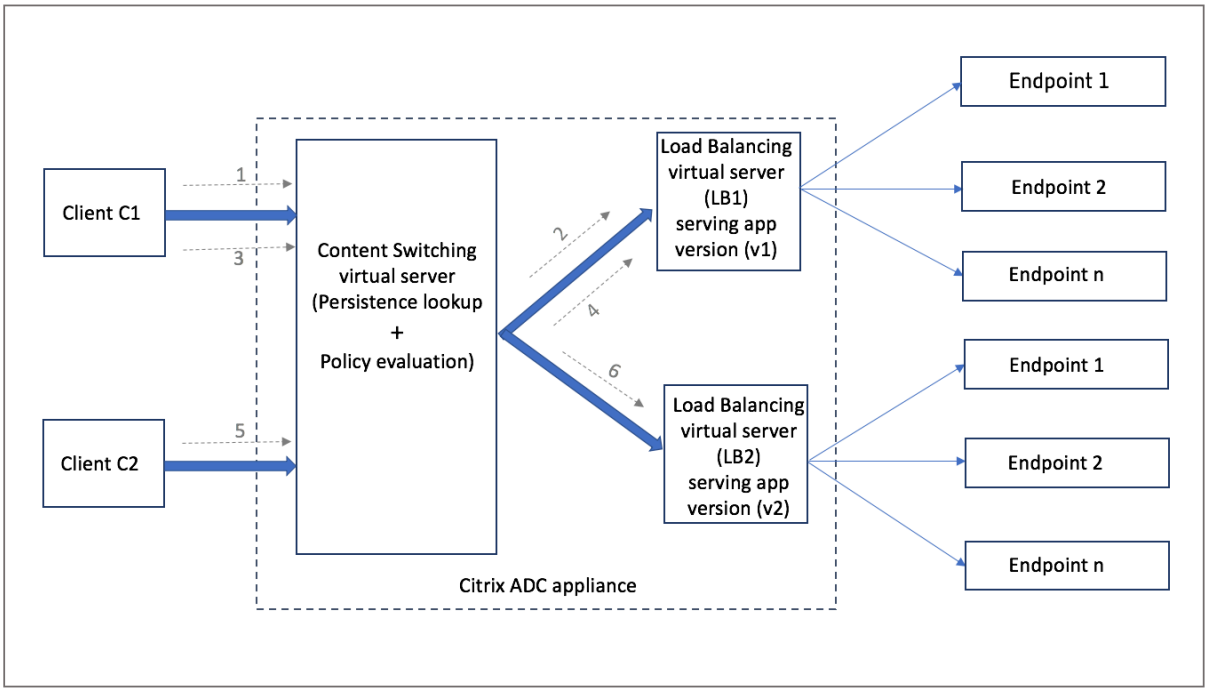
Das folgende Beispiel veranschaulicht die Bereitstellung mehrerer Versionen der Anwendung mit einem virtuellen Content Switching-Server mit Persistenz.



Wenn Client C1 eine Anforderung an die Anwendung sendet, wird die Anforderung an den virtuellen Content Switching-Server in der Citrix ADC Appliance gesendet. Der virtuelle Content Switching-Server wertet die Richtlinie aus, erstellt einen Persistenzsitzungseintrag und leitet die Anforderung an den virtuellen Lastausgleichsserver LB1 weiter, der Version v1 der Anwendung bedient.



Dasselbe Client C1 fordert erneut für die Anwendung an, und die Anforderung wird an den virtuellen Content Switching-Server in der Citrix ADC Appliance gesendet. Eine Suche nach der Persistenzsitzung wird durchgeführt, und der virtuelle Lastausgleichsserver LB1 wird aus der vorhandenen Persistenzsitzung entnommen und die Anforderung wird an LB1 weitergeleitet. Bei dieser Lösung findet kein Bruch der bestehenden Transaktion statt, wodurch der zustandsbehaftete Charakter der Anwendung beibehalten wird.



Betrachten wir einen neuen Client C2. Die neue Anforderung C2 wird über die Richtlinienbewertung an die neuere Version der Anwendung gesendet, da für diesen Client keine Persistenzsitzung vorhanden ist. Es führt zu einem erfolgreichen Rollout der neueren Version der Anwendung, ohne ihre Statefulnigkeit zu brechen.

Aufgrund der Persistenzunterstützung können Kunden mehrere Inhalte oder verschiedene Versionen der Anwendung nahtlos bereitstellen, ohne die vorhandenen Transaktionen zu beeinträchtigen, insbesondere für statusbehaftete Anwendungen. Es ist nicht ohne Beharrlichkeit im Bild möglich.

Konfigurieren des Persistenztyps auf dem virtuellen Content Switching-Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cs vserver <name> -PersistenceType <type> [-timeout <integer>]
<!--NeedCopy-->
```

Beispiel:

```
set cs vserver Vserver-CS-1 -persistenceType SOURCEIP -timeout 60
<!--NeedCopy-->
```


Konfigurieren des Persistenztyps auf dem virtuellen Content Switching-Server mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Content Switching** > **Virtuelle Server**, und klicken Sie auf **Hinzufügen** .
2. Konfigurieren Sie in den **Grundeinstellungen**die Persistenzdetails.

Problembehandlung

October 5, 2021

Wenn Content Switching nach der Konfiguration nicht wie erwartet funktioniert, können Sie einige gängige Tools verwenden, um auf Citrix ADC Ressourcen zuzugreifen und das Problem zu diagnostizieren.

Ressourcen zur Problembehandlung bei Content Switching

Verwenden Sie die folgenden Ressourcen, um ein Problem beim Content Switching auf einer Citrix ADC Appliance zu beheben, um optimale Ergebnisse zu erzielen:

- Konfigurationsdatei
- Relevante `newnslog` Datei
- Trace-Dateien
- Netzwerktopologie-Diagramm für die Netzwerkeinrichtung des Kunden
- Citrix Dokumentation, wie Versionshinweise, Artikel im Knowledge Center und Produktdokumentation.

Zusätzlich zu den vorherigen Ressourcen beschleunigen die folgenden Tools die Fehlerbehebung:

- Das `iehttpheaders` oder ein ähnliches Dienstprogramm
- Die für Citrix ADC C-Trace-Dateien angepasste Wireshark-Anwendung
- Ein SSH-Dienstprogramm für den Befehlszeilenzugriff
- Ein HyperTerminal-Dienstprogramm für den Zugriff auf die Konsole

Problembehandlung bei Problemen mit dem Content Switching

Die häufigsten Probleme beim Content Switching sind, dass Content Switching überhaupt nicht funktioniert oder nur zeitweise funktioniert und die Antwort “Service nicht verfügbar” ist.

- **Problem**

  Content Switching funktioniert nicht.

Lösung

Überprüfen Sie die Konfiguration wie folgt:

- Stellen Sie sicher, dass die Appliance für Content Switching lizenziert ist.
- Stellen Sie sicher, dass das Feature aktiviert ist.
- Stellen Sie in der Konfigurationsdatei sicher, dass gültige Content Switching-Richtlinien korrekt an die virtuellen Lastenausgleichsserver gebunden sind.

- **Problem**

  Der Client erhält eine Antwort 503 - Service nicht verfügbar.

  Lösung

  - Überprüfen Sie die URL- und Richtlinienbindungen. Der Client erhält die Antwort 503, wenn keine der von Ihnen konfigurierten Richtlinien ausgewertet wird und kein standardmäßiger virtueller Lastausgleichsserver definiert und an den virtuellen Content Switching-Server gebunden ist.
  - Überprüfen Sie in der Konfiguration die Richtlinien und auf die URL, auf die der Client abgerufen wird.
  - Stellen Sie sicher, dass für jede Art von Anforderung die entsprechende Richtlinie ausgewertet wird. Wenn die Richtlinie nicht ausgewertet wird, überprüfen Sie den Richtlinienausdruck und aktualisieren Sie ihn gegebenenfalls.
  - Überprüfen Sie die URL- und HTTP-Anforderungs- und Antwort-Header. Zeichnen Sie dazu einen `HTTPHeader` Trace auf und zeichnen Sie ggf. die Paketspuren auf der Appliance und dem Client auf.

- **Problem**

  Zeitweise funktioniert Content Switching nicht wie erwartet.

  Lösung

  - Studieren Sie das Netzwerktopologiediagramm des Setups, falls verfügbar, um die verschiedenen zwischen dem Client und den Servern installierten Geräte zu verstehen.
  - Überprüfen Sie die Konfiguration und die Richtlinienbindungen. Stellen Sie sicher, dass die URL im Richtlinienausdruck mit der URL in der Clientanforderung übereinstimmt.
  - Stellen Sie sicher, dass den Richtlinien entsprechende Prioritäten zugewiesen sind. Eine falsche Priorität oder Priorität, die einer Richtlinie zugewiesen wurde, kann ein Problem verursachen.
  - Führen Sie die folgenden Befehle aus, um die Bindungen und die Werte der Richtlinienauswahlindikatoren in der Ausgabe der Befehle zu überprüfen:

    ```
    show cs vserver \<CS VServer\>
    ```



```
show cs policy \<CS Policy\>

stat cs vserver \<CS VServer\>
```

- Bestimmen Sie mit `iehttpheaders` einem ähnlichen Dienstprogramm, ob die HTTP-Header für die Anfragen oder Antworten Hinweise auf das Problem liefern.
- Überprüfen Sie die Versionshinweise und Knowledge Center-Artikel.
- Wenn das Problem weiterhin nicht behoben ist, wenden Sie sich an den technischen Support von Citrix, um die entsprechenden Daten für weitere Untersuchungen zu erhalten.

DataStream

October 5, 2021

Die Citrix ADC DataStream Funktion stellt einen intelligenten Mechanismus für die Anforderungsumschaltung auf der Datenbankebene bereit, indem Anforderungen basierend auf der gesendeten SQL-Abfrage verteilt werden.

Bei der Bereitstellung vor Datenbankservern gewährleistet eine Citrix ADC Appliance eine optimale Verteilung des Datenverkehrs von den Anwendungsservern und Webservern. Administratoren können den Datenverkehr nach Informationen in der SQL-Abfrage und basierend auf Datenbanknamen, Benutzernamen, Zeichensätzen und Paketgröße segmentieren.

Sie können Load Balancing für Switch-Anforderungen basierend auf Load Balancing-Algorithmen konfigurieren. Alternativ können Sie die Umschaltkriterien erarbeiten, indem Sie Content Switching so konfigurieren, dass eine Entscheidung basierend auf einem SQL-Abfrageparameter getroffen wird. Sie können Monitore weiter konfigurieren, um den Status von Datenbankservern zu verfolgen.

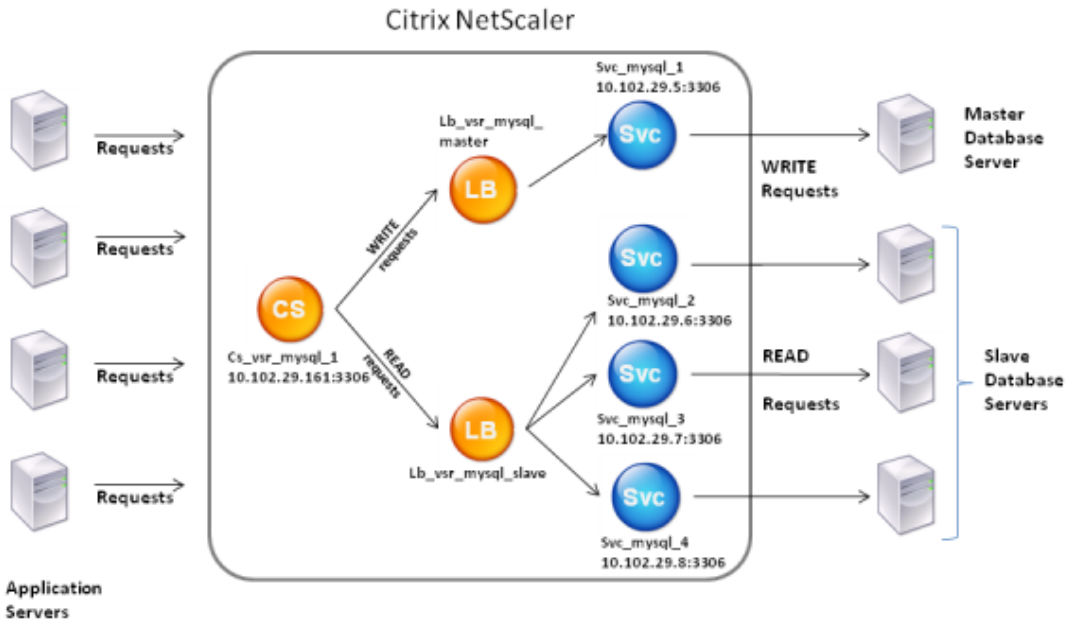
> **Hinweis:**
>
> Citrix ADC DataStream wird nur für MySQL- und MS SQL-Datenbanken unterstützt. Weitere Informationen über die unterstützte Protokollversion, Zeichensätze, spezielle Abfragen und Transaktionen finden Sie unter DataStream Reference.

Wie funktioniert DataStream

In DataStream wird die ADC-Appliance inline zwischen der Anwendung oder den Webservern und den Datenbankservern platziert. Auf der Appliance werden die Datenbankserver durch Dienste dargestellt.

Eine typische DataStream Bereitstellung besteht aus den im folgenden Diagramm beschriebenen Entitäten.

Abbildung 1. DataStream Entitätsmodell



Wie in dieser Abbildung gezeigt, kann eine DataStream-Konfiguration bestehen aus:

- Ein optionaler virtueller Content Switching-Server (CS).
- Ein Load Balancing-Setup, das aus virtuellen Lastenausgleichsservern (LB1 und LB2) besteht.
- Dienste (Svc1, Svc2, Svc3 und Svc4).
- Content Switching-Richtlinien (optional).

Die Clients (Anwendungs- oder Webserver) senden Anforderungen an die IP-Adresse eines virtuellen Content Switching-Servers (CS), der auf der Citrix ADC Appliance konfiguriert ist. Anschließend authentifiziert die Appliance die Clients mithilfe der auf der Appliance konfigurierten Datenbankbenutzeranmeldeinformationen. Der virtuelle Content Switching-Server (CS) wendet die zugeordneten Content Switching-Richtlinien auf die Anforderungen an. Nach der Auswertung der Richtlinien leitet der virtuelle Content Switching-Server (CS) die Anforderungen an den entsprechenden virtuellen Lastausgleichsserver (LB1 oder LB2) weiter. Anschließend verteilt der virtuelle Lastausgleichsserver die Anforderungen basierend auf dem Lastausgleichsalgorithmus an die entsprechenden Datenbankserver (dargestellt durch Dienste auf der Appliance). Die Citrix ADC Appliance verwendet dieselben Anmeldeinformationen für Datenbankbenutzer, um die Verbindung mit dem Datenbankserver zu authentifizieren.

Wenn ein virtueller Content Switching-Server auf der Appliance nicht konfiguriert ist, senden die Clients (Anwendung oder Webserver) ihre Anfragen an einen virtuellen Lastausgleichsserver, der auf der Appliance konfiguriert ist. Die Citrix ADC Appliance authentifiziert den Client mithilfe der auf der Appliance konfigurierten Datenbankbenutzeranmeldeinformationen und verwendet dann dieselben Anmeldeinformationen, um die Verbindung mit dem Datenbankserver zu authentifizieren. Der virtuelle Lastausgleichsserver verteilt die Anforderungen entsprechend dem Lastausgleichsalgorithmus an die Datenbankserver. Der effektivste Lastausgleichsalgorithmus für die Datenbankumschaltung ist die geringste Verbindungsmethode.

DataStream verwendet Verbindungsmultiplexing, um mehrere clientseitige Anforderungen über dieselbe serverseitige Verbindung zu ermöglichen. Folgende Verbindungseigenschaften werden berücksichtigt:

- Benutzername
- Database name
- Paketgröße
- Zeichensatz

Konfigurieren von Datenbankbenutzern

October 5, 2021

In Datenbanken ist eine Verbindung immer statusbehaftet, was bedeutet, dass beim Herstellen einer Verbindung authentifiziert werden muss.

Konfigurieren Sie den Benutzernamen und das Kennwort Ihrer Datenbank auf der NetScaler Appliance. Wenn Sie beispielsweise einen Benutzer John in der Datenbank konfiguriert haben, müssen Sie den Benutzer John auch auf dem ADC konfigurieren. Durch das Hinzufügen von Datenbankbenutzernamen und Kennwörtern auf dem ADC werden sie der `nsconfig` Datei hinzugefügt.

> **Hinweis:**
>
> Bei Namen wird zwischen Groß- und Kleinschreibung unterschieden.

Der ADC verwendet diese Benutzeranmeldeinformationen, um die Clients zu authentifizieren und dann die Serververbindungen mit den Datenbankservern zu authentifizieren.

Hinzufügen eines Datenbankbenutzers mit der CLI

Geben Sie an der Eingabeaufforderung

```
add db user <username> - password <password>
```

Beispiel:


```
add db user nsdbuser -password dd260427edf
<!--NeedCopy-->
```

Fügen Sie einen Datenbankbenutzer über die grafische Benutzeroberfläche hinzu

Navigieren Sie zu **System > Benutzerverwaltung > Datenbankbenutzer**, und konfigurieren Sie einen Datenbankbenutzer.

Wenn Sie das Kennwort des Datenbankbenutzers auf dem Datenbankserver geändert haben, müssen Sie das Kennwort des entsprechenden Benutzers zurücksetzen, der auf der ADC-Appliance konfiguriert ist.

Zurücksetzen des Kennworts eines Datenbankbenutzers mit der CLI

Geben Sie an der Eingabeaufforderung

```
set db user <username> -password <password>
<!--NeedCopy-->
```

Beispiel:

```
set db user nsdbuser -password dd260538abs
<!--NeedCopy-->
```

Setzen Sie das Kennwort von Datenbankbenutzern über die grafische Benutzeroberfläche zurück

Navigieren Sie zu **System > Benutzerverwaltung > Datenbankbenutzer**, wählen Sie einen Benutzer aus, und geben Sie neue Werte für das Kennwort ein.

Wenn ein Datenbankbenutzer nicht mehr auf dem Datenbankserver vorhanden ist, können Sie den Benutzer aus der ADC-Appliance entfernen. Wenn der Benutzer jedoch weiterhin auf dem Datenbankserver vorhanden ist und Sie den Benutzer aus der ADC-Appliance entfernen, wird jede Anforderung vom Client mit diesem Benutzernamen nicht authentifiziert. Daher wird die Anfrage nicht an den Datenbankserver weitergeleitet.

Entfernen eines Datenbankbenutzers mit der CLI

Geben Sie an der Eingabeaufforderung

```
rm db user <username>
<!--NeedCopy-->
```

Beispiel:

```
rm db user nsdbuser
<!--NeedCopy-->
```

Entfernen eines Datenbankbenutzers mit der GUI

Navigieren Sie zu **System > Benutzerverwaltung > Datenbankbenutzer**, wählen Sie einen Benutzer aus, und klicken Sie auf **Löschen**.

Konfigurieren eines Datenbankprofils

October 5, 2021

Ein Datenbankprofil ist eine benannte Sammlung von Parametern, die einmal konfiguriert, aber auf mehrere virtuelle Server angewendet wird, für die bestimmte Parametereinstellungen erforderlich sind. Nachdem Sie ein Datenbankprofil erstellt haben, binden Sie es an den virtuellen Lastausgleichs- oder Content Switching-Server. Sie können beliebig viele Profile erstellen.

Erstellen eines Datenbankprofils mit der CLI

Geben Sie in der Befehlszeile die folgenden Befehle ein, um ein Datenbankprofil zu erstellen und die Konfiguration zu überprüfen:

```
add db dbProfile <name> [-interpretQuery ( YES | NO )] [-stickiness (
    YES | NO )] [-kcdAccount <string>]

show db dbProfile
<!--NeedCopy-->
```


Beispiel:

```
> add dbProfile myDBProfile -interpretQuery YES -stickiness YES -
    kcdAccount mykcdaccnt
 Done
> show dbProfile myDBProfile
    Name: myDBProfile
    Interpret Query: YES
    Stickyness: YES
    KCD Account: mykcdaccnt
    Reference count: 0

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

Erstellen eines Datenbankprofils mit der GUI

Navigieren Sie zu **System > Profile**, und konfigurieren Sie auf der Registerkarte **Datenbankprofile** ein Datenbankprofil.

Binden eines Datenbankprofils an einen virtuellen Lastenausgleichs- oder Content Switching-Server mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

```
set (lb | cs) vserver <name> -dbProfileName <string>
<!--NeedCopy-->
```

Binden eines Datenbankprofils an einen virtuellen Lastenausgleichs- oder Content Switching-Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server oder Traffic Management > Content Switching > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter **Erweiterte Einstellungen** die Option **Profile**aus, und wählen Sie in der Liste **DB-Profil** ein Profil aus, das an den virtuellen Server gebunden werden soll. Um ein Profil zu erstellen, klicken Sie auf plus (+).

Konfigurieren des Lastenausgleichs für DataStream

October 5, 2021

Bevor Sie ein Lastausgleichs-Setup konfigurieren, müssen Sie die Lastenausgleichsfunktion aktivieren. Erstellen Sie dann mindestens einen Dienst für jeden Datenbankserver in der Lastausgleichsgruppe. Wenn die Dienste konfiguriert sind, können Sie einen virtuellen Lastausgleichsserver erstellen und die Dienste an den virtuellen Server binden.

> **Hinweis**:
>
> Bei Datenbanken kann der Lastenausgleich nur auf homogenen Datenbankservern erfolgen (Datenbankservern, die genau dieselben Datenbanken enthalten). Für eine Konfiguration, die eindeutige Datenbanken auf verschiedenen Servern enthält, müssen Sie Content Switching verwenden. Wenn einige Ihrer Datenbankserver identischen Inhalt hosten, können Sie den Lastenausgleich nur auf diesen Servern verwenden. Anschließend können Sie Content Switching-Richtlinien verwenden, um Anforderungen an den virtuellen Lastausgleichsserver zu senden, der den Lastausgleich für diese Datenbanken verwaltet.
>
> Die Citrix ADC Appliance speichert derzeit den Datenbanknamen und die Anmeldeinformationen während der Datenbanksitzung. Wenn eine Abfrage an die Datenbank erfolgt, werden diese Informationen verwendet, um eine Verbindung mit dem bestimmten Datenbankserver herzustellen.

DataStream spezifische Parameterwerte

- Protokoll

  Verwenden Sie den MySQL Protokolltyp für MySQL-Datenbanken und den MSSQL-Protokolltyp für MS SQL-Datenbanken, während Sie virtuelle Server und Dienste konfigurieren. Die Protokolle MySQL und TDS werden von den Clients verwendet, um mit den jeweiligen Datenbankservern über SQL-Abfragen zu kommunizieren. Hinweise zum MySQL Protokoll finden Sie unter http://dev.mysql.com/doc/internals/en/client-server-protocol.html. Hinweise zum TDS-Protokoll finden Sie unter http://msdn.microsoft.com/en-us/library/dd304523(v=prot.13).aspx.

- Port

  Port, auf dem der virtuelle Server auf Clientverbindungen wartet. Verwenden Sie Port 3306 für MySQL Datenbankserver.

- Methode

  Es wird empfohlen, die Methode Kleinste Verbindung für einen besseren Lastausgleich und eine geringere Serverlast zu verwenden. Andere Methoden wie Round Robin, Least Response Time,

Source IP Hash, Source IP Destination IP Hash, Least Bandwidth, Least Packets und Source IP Source Port Hash werden ebenfalls unterstützt.

Hinweis: URL-Hash-Methode wird für DataStream nicht unterstützt.

- Version von MS SQL Server

  Wenn Sie den Microsoft SQL Server verwenden und erwarten, dass einige Clients eine andere Version als Ihr Microsoft SQL Server-Produkt ausführen, legen Sie den Parameter Serverversion für den virtuellen Lastenausgleich fest. Die Versionseinstellung stellt die Kompatibilität zwischen den clientseitigen und serverseitigen Verbindungen bereit, indem sichergestellt wird, dass die gesamte Kommunikation der Serverversion entspricht. Weitere Informationen zum Festlegen des Parameters "Serverversion" finden Sie unter Konfigurieren der Versionseinstellung MySQL und Microsoft SQL Server.

- MySQL-Serverversion

  Wenn Sie den MySQL-Server verwenden und erwarten, dass einige Clients eine andere Version als Ihr MySQL-Server-Produkt ausführen, legen Sie den Parameter Serverversion für den virtuellen Lastausgleichsserver fest. Die Versionseinstellung stellt die Kompatibilität zwischen den clientseitigen und serverseitigen Verbindungen bereit, indem sichergestellt wird, dass die gesamte Kommunikation der Serverversion entspricht. Weitere Informationen zum Festlegen des Parameters "Serverversion" finden Sie unter Konfigurieren der Versionseinstellung MySQL und Microsoft SQL Server.

Content Switching für DataStream konfigurieren

October 5, 2021

Sie können den Datenverkehr basierend auf den Informationen in der SQL-Abfrage basierend auf Datenbanknamen, Benutzernamen, Zeichensätzen und Paketgröße segmentieren.

Sie können Content Switching-Richtlinien mit Standardsyntaxausdrücken konfigurieren, um Content Switching basierend auf Verbindungseigenschaften durchzuführen. Zum Beispiel Benutzername und Datenbankname, Befehlsparameter und die SQL-Abfrage zur Auswahl des Servers.

Die Standardsyntaxausdrücke werten den Datenverkehr aus, der mit MYSQL- und MS SQL-Datenbankservern verknüpft ist. Verwenden Sie anforderungsbasierte Ausdrücke in Standardsyntaxrichtlinien, um Entscheidungen zum Ändern von Anfragen am Bindepunkt des virtuellen Content Switching-Servers zu treffen. Verwenden Sie antwortbasierte Ausdrücke (Ausdrücke, die mit MYSQL.RES beginnen), um Serverreaktionen auf benutzerkonfigurierte Integritätsmonitore auszuwerten.

Informationen zu Standardsyntaxausdrücken finden Sie unter Standardsyntaxausdrücke: DataStream.

> **Hinweis:**
>
> Bei Datenbanken kann der Lastenausgleich nur auf homogenen Datenbankservern erfolgen (Datenbankservern, die genau dieselben Datenbanken enthalten). Für eine Konfiguration, die eindeutige Datenbanken auf verschiedenen Servern enthält, müssen Sie Content Switching verwenden. Wenn einige Ihrer Datenbankserver identischen Inhalt hosten, können Sie den Lastenausgleich nur auf diesen Servern verwenden. Anschließend können Sie Content Switching-Richtlinien verwenden, um Anforderungen an den virtuellen Lastausgleichsserver zu senden, der den Lastausgleich für diese Datenbanken verwaltet.
>
> Die Citrix ADC Appliance speichert derzeit den Datenbanknamen und die Anmeldeinformationen während der Datenbanksitzung. Wenn eine Abfrage an die Datenbank erfolgt, werden diese Informationen verwendet, um eine Verbindung mit dem bestimmten Datenbankserver herzustellen.

DataStream spezifische Parameterwerte

- Protokoll

  Verwenden Sie den MySQL Protokolltyp für MySQL-Datenbanken und den MSSQL-Protokolltyp für MS SQL-Datenbanken, während Sie virtuelle Server und Dienste konfigurieren. Die Protokolle MySQL und TDS werden von den Clients verwendet, um mit den jeweiligen Datenbankservern über SQL-Abfragen zu kommunizieren. Hinweise zum MySQL Protokoll finden Sie unter http://dev.mysql.com/doc/internals/en/client-server-protocol.html. Hinweise zum TDS-Protokoll finden Sie unter http://msdn.microsoft.com/en-us/library/dd304523(v=prot.13).aspx.

- Port

  Port, auf dem der virtuelle Server auf Clientverbindungen wartet. Verwenden Sie Port 3306 für MySQL Datenbankserver.

- Version von MS SQL Server

  Wenn Sie Microsoft SQL Server verwenden und erwarten, dass einige Clients eine andere Version als Ihr Microsoft SQL Server-Produkt ausführen, legen Sie den Parameter Serverversion für den virtuellen Content Switching-Server fest. Die Versionseinstellung stellt die Kompatibilität zwischen den clientseitigen und serverseitigen Verbindungen bereit, indem sichergestellt wird, dass die gesamte Kommunikation der Serverversion entspricht. Weitere Informationen zum Festlegen des Parameters “Serverversion” finden Sie unter Konfigurieren der Microsoft SQL Server-Versionseinstellung.

Konfigurieren von Monitoren für DataStream

October 5, 2021

Um den Status jedes Lastausgleichs-Datenbankservers in Echtzeit zu verfolgen, müssen Sie einen Monitor an jeden Dienst binden. Der Monitor ist so konfiguriert, dass er den Dienst testet, indem er regelmäßige Probes an den Dienst sendet, der manchmal als Durchführen einer Zustandsprüfung bezeichnet wird. Wenn der Monitor eine rechtzeitige Antwort auf seine Sonden erhält, markiert er den Dienst als UP. Wenn es keine rechtzeitige Antwort auf die angegebene Anzahl von Sonden erhält, markiert es den Dienst als DOWN.

Für DataStream müssen Sie die integrierten Monitore verwenden: MYSQL-ECV und MSSQL-ECV. Mit diesem Monitor können Sie eine SQL-Anfrage senden und die Antwort für eine Zeichenfolge analysieren.

Bevor Sie Monitore für DataStream konfigurieren, müssen Sie Ihrer NetScaler er-Appliance Datenbank-Benutzeranmeldeinformationen hinzufügen. Informationen zum Konfigurieren von Monitoren finden Sie unter Konfigurieren von Monitoren in einem Load Balancing-Setup.

Wenn Sie einen Monitor erstellen, wird eine TCP-Verbindung mit dem Datenbankserver hergestellt, und die Verbindung wird mithilfe des Benutzernamens authentifiziert, der beim Erstellen des Monitors angegeben wird. Anschließend können Sie eine SQL-Abfrage an den Datenbankserver ausführen und die Serverantwort auswerten, um zu überprüfen, ob sie mit der konfigurierten Regel übereinstimmt.

Die folgenden Beispiele sind für MySQL Server.

Beispiele:

Im folgenden Beispiel wird der Wert der Fehlermeldung ausgewertet, um den Status des Servers zu bestimmen.

```
1 add lb monitor lb_mon1 MYSQL-ECV -sqlQuery ”select * from
2 table2;” -evalrule ”mysql.res.error.message.contains(”Invalid
3 User”)”-database ”NS” -userName ”user1”
4 <!--NeedCopy-->
```

Im folgenden Beispiel wird die Anzahl der Zeilen in der Antwort ausgewertet, um den Status des Servers zu bestimmen.

```
1 add lb monitor lb_mon4 MYSQL-ECV -sqlQuery ”select * from
2 table4;” -evalrule ”mysql.res.atleast_rows_count(7)” -database ”NS” -
     userName ”user2”
```



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

Im folgenden Beispiel wird der Wert einer bestimmten Spalte ausgewertet, um den Status des Servers zu bestimmen.

```
add lb monitor lb_mon3 MYSQL-ECV
-sqlQuery "select * from ABC;" -evalrule "mysql.res.row(1).double_elem
   (2) == 345.12"
-database "NS" -userName "user3"
<!--NeedCopy-->
```

Die folgenden Beispiele sind für MSSQL-Server.

Beispiele:

Im folgenden Beispiel wird der Wert der Fehlermeldung ausgewertet, um den Status des Servers zu bestimmen.

```
add lb monitor lb_mon1 MSSQL-ECV -sqlQuery "select * from
table2;" -evalrule "mssql.res.error.message.contains("Invalid
User")"-database "NS" -userName "user1"
<!--NeedCopy-->
```

Im folgenden Beispiel wird die Anzahl der Zeilen in der Antwort ausgewertet, um den Status des Servers zu bestimmen.

```
add lb monitor lb_mon4 MSSQL-ECV -sqlQuery "select * from
table4;" -evalrule "mssql.res.atleast_rows_count(7)" -database "NS" -
   userName "user2"
<!--NeedCopy-->
```

Im folgenden Beispiel wird der Wert einer bestimmten Spalte ausgewertet, um den Status des Servers zu bestimmen.

```
add lb monitor lb_mon3 MSSQL-ECV
-sqlQuery "select * from ABC;" -evalrule "mssql.res.row(1).double_elem
   (2) == 345.12"
-database "NS" -userName "user3"
<!--NeedCopy-->
```


Anwendungsfall 1: Konfigurieren von DataStream für eine Primär-/Sekundärdatenbankarchitektur

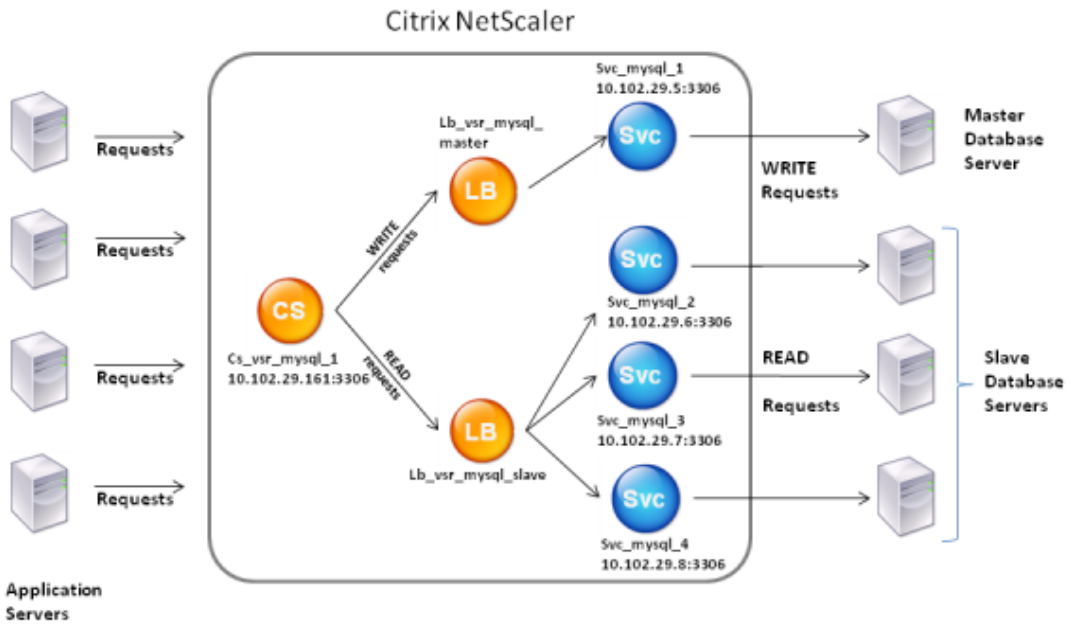
April 25, 2022

Ein häufig verwendetes Bereitstellungsszenario ist die primäre und sekundäre Datenbankarchitektur, bei der die Primärdatenbank alle Informationen in die sekundären Datenbanken repliziert

Bei der primären/sekundären Datenbankarchitektur möchten Sie möglicherweise, dass alle WRITE-Anforderungen an die Primärdatenbank und alle READ-Anforderungen an die sekundären Datenbanken gesendet werden.

Die folgende Abbildung zeigt die Entitäten und die Werte der Parameter, die Sie auf der Appliance konfigurieren müssen.

Abbildung 1. DataStream-Entitätsmodell für Primär-/Sekundärdatenbank-Setup



In diesem Beispielszenario wird ein Dienst (SVC_MySql_1) erstellt, um die Primärdatenbank darzustellen, und ist an einen virtuellen Lastausgleichsserver (LB_VSR_MySql_Primary) gebunden. Drei weitere Dienste (SVC_MySql_2, SVC_MySql_3 und SVC_MySql_4) werden erstellt, um die drei

sekundären Datenbanken darzustellen, und sie sind an einen anderen virtuellen Lastausgleichsserver (LB_VSR_MySql_Secondary) gebunden.

Ein virtueller Content Switching-Server (CS_VSR_MySql_1) ist mit zugehörigen Richtlinien konfiguriert, um alle WRITE-Anforderungen an den virtuellen Lastausgleichsserver zu senden, lb_vsr_mysql_Primary. Alle READ-Anforderungen werden an den virtuellen Lastausgleichsserver LB_VSR_MySql_Secondary gesendet.

Wenn eine Anforderung den virtuellen Content Switching-Server erreicht, wendet der virtuelle Server die zugeordneten Content Switching-Richtlinien auf diese Anforderung an. Nach der Auswertung der Richtlinien leitet der virtuelle Content Switching-Server die Anforderung an den entsprechenden virtuellen Lastausgleichsserver weiter, der sie an den entsprechenden Dienst sendet.

In der folgenden Tabelle sind die Namen und Werte der Entitäten sowie die auf der Citrix ADC Appliance konfigurierte Richtlinie aufgeführt.

Typ der Entität	Name	IP-Adresse	Protokoll	Port	Ausdruck
Services	Svc_mysql_1	198.51.100.5	MYSQL	3306	Nicht zutreffend
	Svc_mysql_2	198.51.100.6	MYSQL	3306	Nicht zutreffend
	Svc_mysql_3	198.51.100.7	MYSQL	3306	Nicht zutreffend
	Svc_mysql_4	198.51.100.8	MYSQL	3306	Nicht zutreffend
Überwachung	lb_mon1	Nicht zutreffend	MYSQL-ECV	Nicht zutreffend	mysql.res.atleast_rows_cou
Virtuelle Lastenausgleichsserver	Lb_vsr_mysql_primary	198.51.100.201	MYSQL	3306	Nicht zutreffend
	Lb_vsr_mysql_	198.51.100.202	MYSQL	3306	Nicht zutreffend
Virtuelle Content Switching-Server	Cs_vsr_mysql_1	198.51.100.161	MYSQL	3306	Nicht zutreffend

Typ der Entität	Name	IP-Adresse	Protokoll	Port	Ausdruck
Content Switching-Richtlinie	Cs_select	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	`MYSQL.REQ.QUERY.COMMAND.contains("select")`

Tabelle 1. Namen und Werte von Entitäten und Richtlinien

So konfigurieren Sie DataStream für ein Primär-/Sekundärdatenbank-Setup mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung

```
add db user user1 -password user1

add service Svc_mysql_1 198.51.100.5 mysql 3306

add service Svc_mysql_2 198.51.100.6 mysql 3306

add service Svc_mysql_3 198.51.100.7 mysql 3306

add service Svc_mysql_4 198.51.100.8 mysql 3306

add lb monitor lb_mon1 MYSQL-ECV -sqlQuery "select * from table1;" -
    evalrule "mysql.res.atleast_rows_count(1)" -database "NS" -userName
     "user1"

add lb vserver Lb_vsr_mysql_primary mysql 198.51.100.201 3306

add lb vserver Lb_vsr_mysql_secondary mysql 198.51.100.202 3306

bind lb vserver Lb_vsr_mysql_primary svc_mysql_1

bind lb vserver Lb_vsr_mysql_secondary svc_mysql_2

bind lb vserver Lb_vsr_mysql_secondary svc_mysql_3

bind lb vserver Lb_vsr_mysql_secondary svc_mysql_4
```

```
24
25 add cs vserver Cs_vsr_mysql_1 mysql 198.51.100.161 3306
26
27 add cs policy Cs_select -rule "MYSQL.REQ.QUERY.COMMAND.contains("
   select")"
28
29 bind cs vserver Cs_vsr_mysql_1 Lb_vsr_mysql_primary
30
31 bind cs vserver Cs_vsr_mysql_1 Lb_vsr_mysql_secondary -policy
   Cs_select -priority 10
32
33 bind service Svc_mysql_1 -monitorName lb_mon1
34
35 bind service Svc_mysql_2 -monitorName lb_mon1
36
37 bind service Svc_mysql_3 -monitorName lb_mon1
38
39 bind service Svc_mysql_4 -monitorName lb_mon1
40 <!--NeedCopy-->
```

Anwendungsfall 2: Konfigurieren der Token-Methode des Load Balancing für DataStream

October 5, 2021

Sie können die Token-Methode des Lastenausgleichs für DataStream so konfigurieren, dass die Auswahl der Datenbankserver auf dem Wert des Tokens basiert, das aus den Clientanforderungen (Anwendung oder Webserver) extrahiert wurde. Diese Token werden mithilfe von SQL-Ausdrücken definiert. Bei nachfolgenden Anforderungen mit demselben Token sendet die Citrix ADC Appliance die Anforderungen an denselben Datenbankserver, der die ursprüngliche Anforderung verarbeitet hat. Anforderungen mit demselben Token werden an denselben Datenbankserver gesendet, bis die maximale Verbindungsgrenze erreicht ist oder der Sitzungseintrag veraltete ist.

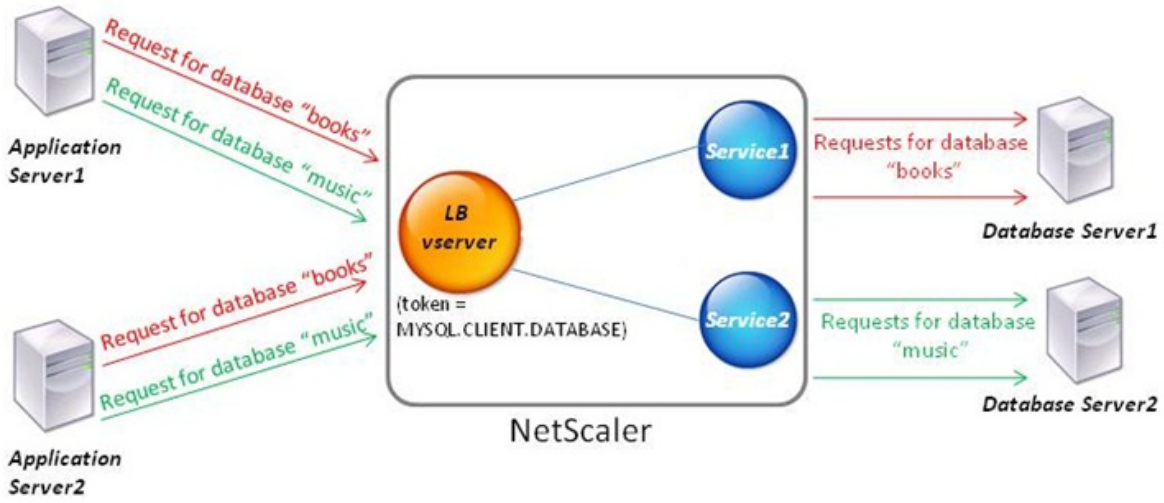
Sie können die folgenden SQL-Beispielausdrücke verwenden, um Token zu definieren:

MySQL	MS SQL
MYSQL.REQ.QUERY.TEXT	MSSQL.REQ.QUERY.TEXT
MYSQL.REQ.QUERY.TEXT(n)	MSSQL. REQ.QUERY.TEXT(n)
MYSQL.REQ.QUERY.COMMAND	MSSQL.REQ.QUERY.COMMAND

MySQL	MS SQL
MYSQL.CLIENT.USER	MSSQL.CLIENT.USER
MYSQL.CLIENT.DATABASE	MSSQL.CLIENT.DATABASE
MYSQL.CLIENT.CAPABILITIES	

Das folgende Beispiel zeigt, wie die Citrix ADC DataStream Funktion funktioniert, wenn Sie die Token-Methode des Lastenausgleichs konfigurieren.

Abbildung 1. DataStream und die Token-Methode des Load Balancing



In diesem Beispiel ist das Token der Name der Datenbank. Eine Anforderung mit Token-Büchern wird an Database Server1 gesendet und eine Anforderung mit Token-Musik wird an Database Server2 gesendet. Alle nachfolgenden Anforderungen mit Token-Büchern werden an Database Server1 gesendet und Anforderungen mit Token-Musik werden an Database Server2 gesendet. Diese Konfiguration bietet Pseudopersistenz mit den Datenbankservern.

Konfigurieren dieses Beispiels mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add service Service1 192.0.2.9 MYSQL 3306
2
3 add service Service2 192.0.2.11 MYSQL 3306
4
```



```
add lb vserver token_lb_vserver MYSQL 192.0.2.15 3306 -lbmethod token -
    rule MYSQL.CLIENT.DATABASE

bind lb vserver token_lb_vserver Service1

bind lb vserver token_lb_vserver Service2
<!--NeedCopy-->
```

Konfigurieren dieses Beispiels mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, konfigurieren Sie einen virtuellen Server und geben Sie das Protokoll als **MYSQL**an.
2. Klicken Sie in den Abschnitt **Dienst** und konfigurieren Sie zwei Dienste, die das Protokoll als MYSQL angeben. Binden Sie diese Dienste an den virtuellen Server.
3. Klicken Sie in **Erweiterte Einstellungen** auf **Methode** und wählen Sie in der Liste **Load Balancing Method** die Option **TOKEN** aus und geben Sie den Ausdruck als **MYSQL.CLIENT.DATABASE**an.

Anwendungsfall 3: Protokollieren von MSSQL-Transaktionen im transparenten Modus

October 5, 2021

Sie können die Citrix ADC Appliance so konfigurieren, dass sie transparent zwischen MSSQL-Clients und Servern funktioniert und nur Details aller Client-Server-Transaktionen protokolliert oder analysiert. Der transparente Modus ist so konzipiert, dass die Citrix ADC Appliance nur MSSQL-Anforderungen an den Server weiterleitet und dann die Antworten des Servers an die Clients weiterleitet. Während die Anforderungen und Antworten die Appliance durchlaufen, protokolliert die Appliance die von ihnen erfassten Informationen, wie in der Auditprotokollierung oder der AppFlow Konfiguration angegeben, oder sammelt Statistiken, wie in der Action Analytics-Konfiguration angegeben. Sie müssen der Appliance keine Datenbankbenutzer hinzufügen.

Wenn Sie im transparenten Modus arbeiten, führt die Citrix ADC Appliance für die Anforderungen keinen Lastausgleich, Content Switching oder Verbindungsmultiplexing durch. Es reagiert jedoch auf das Pre-Login-Paket eines Clients im Namen des Servers, so dass es verhindern kann, dass Verschlüsselung während des Pre-Login-Handshake vereinbart wird. Das Anmeldepaket und die nachfolgenden Pakete werden an den Server weitergeleitet.

Zusammenfassung der Konfigurationsaufgaben

Um MSSQL-Anfragen im transparenten Modus zu protokollieren oder zu analysieren, müssen Sie Folgendes tun:

- Konfigurieren Sie die Citrix ADC Appliance als Standard-Gateway für Clients und Server.
- Führen Sie auf der Citrix ADC Appliance einen der folgenden Schritte aus:
  - **Konfigurieren Sie die Option Quell-IP-Adresse (USIP) verwenden global:** Erstellen Sie einen virtuellen Lastausgleichsserver mit einer Platzhalter-IP-Adresse und der Portnummer, auf der die MSSQL-Server auf Anfragen hören (ein portspezifischer virtueller Platzhalterserver). Aktivieren Sie dann die USIP-Option global. Wenn Sie einen portspezifischen virtuellen Wildcard-Server konfigurieren, müssen Sie keine MSSQL-Dienste auf der Appliance erstellen. Die Appliance erkennt die Dienste basierend auf der Ziel-IP-Adresse in den Client-Anfragen.
  - **Wenn Sie die USIP-Option nicht global konfigurieren möchten:** Erstellen Sie MSSQL-Services mit aktivierter USIP-Option. Wenn Sie Dienste konfigurieren, müssen Sie keinen portspezifischen virtuellen Platzhalterserver erstellen.
- Konfigurieren Sie die Auditprotokollierung, AppFlow oder Action Analytics, um Statistiken zu den Anforderungen zu protokollieren oder zu sammeln. Wenn Sie einen virtuellen Server konfigurieren, können Sie Ihre Richtlinien entweder an den virtuellen Server oder an den globalen Bindungspunkt binden. Wenn Sie keinen virtuellen Server konfigurieren, können Sie Ihre Richtlinien nur an den globalen Bindungspunkt binden.

Konfigurieren des transparenten Modus mithilfe eines virtuellen Platzhalterservers

Sie können den transparenten Modus konfigurieren, indem Sie einen portspezifischen virtuellen Wildcard-Server konfigurieren und den USIP-Modus (Source IP) global aktivieren. Wenn ein Client sein Standard-Gateway (die Citrix ADC Appliance) eine Anforderung mit der IP-Adresse eines MSSQL-Servers im Ziel-IP-Adress-Header sendet, überprüft die Appliance, ob die Ziel-IP-Adresse verfügbar ist. Wenn die IP-Adresse verfügbar ist, leitet der virtuelle Server die Anforderung an den Server weiter. Andernfalls wird die Anfrage verfallen.

Erstellen eines virtuellen Platzhalterservers mit der CLI

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

```
1 add lb vserver <name> <serviceType> <IPAddress> <port>
2
3 show lb vserver <name>
```



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

Beispiel:

```
> add lb vserver wildcardLbVs MSSQL * 1433
 Done
> show lb vserver wildcardLbVs
    wildcardLbVs (*:1433) - MSSQL   Type: ADDRESS
    State: UP
    . . .

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

Erstellen eines virtuellen Platzhalterservers mit der GUI

Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und erstellen Sie einen virtuellen Server. Geben Sie MSSQL als Protokoll und * als IP-Adresse an.

Aktivieren Sie den Modus “Quell-IP (USIP) verwenden” global mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den USIP-Modus global zu aktivieren und die Konfiguration zu überprüfen:

```
enable ns mode USIP

show ns mode
<!--NeedCopy-->
```

Beispiel:

```
> enable ns mode USIP
 Done
> show ns mode

    Mode                                Acronym
        Status
```



```
6      -------                              -------
           ------
7                  . . .
8    3) Use Source IP                  USIP                           ON
9                  . . .
10   Done
11  >
12  <!--NeedCopy-->
```

Aktivieren Sie den USIP-Modus global mit der GUI

1. Navigieren Sie zu **System > Einstellungen**, und wählen Sie unter Modi und Features die Option **Modi konfigurieren** aus.
2. Wählen Sie **Quell-IP verwenden** aus.

Konfigurieren des transparenten Modus mithilfe von MSSQL-Diensten

Sie können den transparenten Modus konfigurieren, indem Sie MSSQL-Dienste konfigurieren und USIP für jeden Dienst aktivieren. Wenn ein Client sein Standard-Gateway (die Citrix ADC Appliance) eine Anforderung mit der IP-Adresse eines MSSQL-Servers im Ziel-IP-Adress-Header sendet, leitet die Appliance die Anforderung an den Zielserver weiter.

Erstellen Sie einen MSSQL-Dienst und aktivieren Sie den USIP-Modus für den Dienst über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen MSSQL-Dienst mit aktiviertem USIP zu erstellen, und überprüfen Sie die Konfiguration:

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

Beispiel

```
1  > add service myDBservice 192.0.2.0 MSSQL 1433 -usip YES
2   Done
```



```
> show service myDBservice
    myDBservice (192.0.2.0:1433) - MSSQL
    State: UP
                . . .
    Use Source IP: YES      Use Proxy Port: YES
                . . .
 Done
>
<!--NeedCopy-->
```

Erstellen Sie einen MSSQL-Dienst mit aktivierter USIP über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und konfigurieren Sie einen Service.
2. Geben Sie das Protokoll als **MSSQL** an und wählen Sie **unter Einstellungen**die Option **Quell-IP verwenden**aus.

Anwendungsfall 4: Datenbankspezifischer Lastenausgleich

December 7, 2021

Eine Datenbankserverfarm muss nicht nur basierend auf den Status der Server, sondern auch auf der Verfügbarkeit der Datenbank auf jedem Server Lastenausgleich sein. Ein Dienst ist möglicherweise hochgeladen, und ein Lastausgleichsgerät zeigt möglicherweise den Status UP an, aber die angeforderte Datenbank ist für diesen Dienst möglicherweise nicht verfügbar. Die Anforderung wird nicht gesendet, wenn eine Abfrage an einen Dienst weitergeleitet wird, für den die Datenbank nicht verfügbar ist. Daher muss ein Lastausgleichsgerät die Verfügbarkeit einer Datenbank für jeden Dienst bewusst sein. Und wenn Sie eine Lastausgleichsentscheidung treffen, müssen nur die Dienste berücksichtigt werden, auf denen die Datenbank verfügbar ist.

Betrachten Sie als Beispiel, dass Datenbankserver server1, server2 und server3 Datenbanken mydatabase1 und mydatabase2 host-Datenbanken. Wenn mydatabase1 auf server2 nicht verfügbar ist, muss das Lastausgleichsgerät diese Statusänderung beachten. Es muss Anforderungen für mydatabase1 nur auf server1 und server3 ausgleichen. Nachdem mydatabase1 auf server2 verfügbar ist, muss das Lastausgleichsgerät server2 in Lastausgleichsentscheidungen enthalten. Wenn mydatabase2 auf server3 nicht verfügbar ist, muss das Gerät Anforderungen für mydatabase2 nur auf server1 und server2 ausgleichen. Es muss server3 nur dann in seine Lastausgleichsentscheidungen einbeziehen, wenn mydatabase2 verfügbar ist. Dieses Lastenausgleichsverhalten muss in allen Datenbanken konsistent sein, die in der Serverfarm gehostet werden.

Die Citrix ADC Appliance implementiert dieses Verhalten, indem eine Liste aller Datenbanken abgerufen wird, die für einen Dienst aktiv sind. Zum Abrufen der Liste der aktiven Datenbanken verwendet die Appliance einen Monitor, der mit einer entsprechenden SQL-Abfrage konfiguriert ist. Wenn die angeforderte Datenbank für einen Dienst nicht verfügbar ist, schließt die Appliance den Dienst von Lastausgleichsentscheidungen aus, bis er verfügbar ist. Dieses Verhalten stellt einen ununterbrochenen Dienst für Clients sicher.

> **Hinweis:**
>
> Datenbankspezifischer Lastausgleich wird nur für MSSQL- und MySQL Diensttypen unterstützt. Diese Unterstützung ist auch für Microsoft SQL Server 2012 Hochverfügbarkeitsbereitstellung verfügbar.

Zum Einrichten eines datenbankspezifischen Lastenausgleichs müssen Sie Folgendes konfigurieren:

- Aktivieren Sie die Lastausgleichsfunktion, und konfigurieren Sie einen virtuellen Lastausgleichsserver vom Typ MSSQL oder MySQL.
- Konfigurieren Sie die Dienste, die die Datenbank hosten, und binden Sie die Dienste an den virtuellen Server. Der Monitor benötigt gültige Benutzeranmeldeinformationen, um sich am Datenbankserver anzumelden. Daher müssen Sie auf jedem Server ein Datenbankbenutzerkonto konfigurieren und dann das Benutzerkonto der Citrix ADC Appliance hinzufügen.
- Anschließend konfigurieren Sie einen MSSQL-ECV- oder MYSQL-ECV-Monitor und binden den Monitor an jeden Dienst.
- Schließlich müssen Sie die Konfiguration testen, um sicherzustellen, dass sie wie vorgesehen funktioniert. Bevor Sie diese Konfigurationsaufgaben ausführen, vergewissern Sie sich, wie datenbankspezifischer Lastenausgleich funktioniert.

Funktionsweise des datenbankspezifischen Lastenausgleichs

Für den datenbankspezifischen Lastenausgleich konfigurieren Sie einen Monitor, der jeden Datenbankserver regelmäßig nach den Namen aller aktiven Datenbanken abfragt. Die Citrix ADC Appliance speichert die Ergebnisse und aktualisiert die Datensätze regelmäßig basierend auf den durch die Überwachung abgerufenen Informationen. Wenn ein Client eine bestimmte Datenbank abfragt, verwendet die Appliance die konfigurierte Lastausgleichsmethode, um einen Dienst auszuwählen, und überprüft dann die Datensätze, um festzustellen, ob die Datenbank für diesen Dienst verfügbar ist. Wenn die Datensätze angeben, dass die Datenbank nicht verfügbar ist, verwendet sie die konfigurierte Lastausgleichsmethode, um den nächsten verfügbaren Dienst auszuwählen, und wiederholt die Überprüfung. Die Appliance leitet die Abfrage an den ersten verfügbaren Dienst weiter, auf dem die Datenbank aktiv ist.

Lastenausgleich aktivieren

Sie können Load Balancing-Entitäten wie Dienste und virtuelle Server konfigurieren, wenn die Lastausgleichsfunktion deaktiviert ist. Die Entitäten funktionieren erst, wenn Sie das Feature aktivieren.

Aktivieren des Load Balancing mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um den Lastausgleich zu aktivieren und die Konfiguration zu überprüfen:

```
enable ns feature LB

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

Beispiel:

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 .
 .
 .
 24)    NetScaler Push                  push                OFF
 Done
<!--NeedCopy-->
```

Aktivieren des Lastenausgleichs mit der GUI

Navigieren Sie zu **System > Einstellungen** und wählen **Sie unter Configure Basic Features Load Balancing**aus.

Konfigurieren eines virtuellen Lastausgleichsservers für datenbankspezifisches Load Balancing

Um einen virtuellen Server für den Lastausgleich von Datenbanken basierend auf Verfügbarkeit zu konfigurieren, aktivieren Sie den datenbankspezifischen Lastausgleichsparameter auf dem virtuellen Server. Durch Aktivieren des Parameters wird die Load Balancing-Logik so geändert, dass die Citrix ADC Appliance die Ergebnisse des an den ausgewählten Dienst gesendeten Monitoring-Prüfpunkts verweist, bevor die Abfrage an diesen Dienst weitergeleitet wird.

Konfigurieren eines virtuellen Lastausgleichsservers für datenbankspezifisches Load Balancing mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um einen virtuellen Lastausgleichsserver für den datenbankspezifischen Lastenausgleich zu konfigurieren und die Konfiguration zu überprüfen:

```
add lb vserver <name> <serviceType> <ipAddress> <port> -dbsLb ENABLED

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

Konfigurieren von Diensten

Nachdem Sie die Lastenausgleichsfunktion aktiviert haben, müssen Sie mindestens einen Dienst für jeden Anwendungsserver erstellen, der in das Lastausgleichs-Setup aufgenommen werden soll. Die von Ihnen konfigurierten Dienste stellen die Verbindungen zwischen der Citrix ADC Appliance und den Servern mit Lastausgleich bereit. Jeder Dienst hat einen Namen und gibt eine IP-Adresse, einen Port und den Typ der bereitgestellten Daten an.

Wenn Sie einen Dienst erstellen, ohne vorher ein Serverobjekt zu erstellen, ist die IP-Adresse des Dienstes auch der Name des Servers, der den Dienst hostet. Wenn Sie Server lieber nach Namen und nicht nach IP-Adresse identifizieren möchten, können Sie Serverobjekte erstellen und dann beim Erstellen eines Dienstes anstelle der IP-Adresse einen Servernamen angeben.

Konfigurieren von Datenbankbenutzern

In Datenbanken ist eine Verbindung immer statusbehaftet, was bedeutet, dass beim Herstellen einer Verbindung authentifiziert werden muss.

Konfigurieren Sie den Benutzernamen und das Kennwort Ihrer Datenbank auf dem Citrix ADC. Wenn Sie beispielsweise einen Benutzer John in der Datenbank konfiguriert haben, müssen Sie den Be-

nutzer John auch auf dem ADC konfigurieren. Die dem ADC hinzugefügten Benutzernamen und Kennwörter der Datenbank werden der `nsconfig` Datei hinzugefügt.

> **Hinweis:**
>
> Bei Namen wird zwischen Groß- und Kleinschreibung unterschieden.

Der ADC verwendet diese Benutzeranmeldeinformationen, um die Clients zu authentifizieren und dann die Serververbindungen mit den Datenbankservern zu authentifizieren.

Hinzufügen eines Datenbankbenutzers mit der CLI

Geben Sie an der Eingabeaufforderung

```
add db user <username> - password <password>
<!--NeedCopy-->
```

Beispiel:

```
add db user nsdbuser -password dd260427edf
<!--NeedCopy-->
```

Fügen Sie einen Datenbankbenutzer über die grafische Benutzeroberfläche hinzu

Navigieren Sie zu **System > Benutzerverwaltung > Datenbankbenutzer**, und konfigurieren Sie einen Datenbankbenutzer.

Wenn Sie das Kennwort des Datenbankbenutzers auf dem Datenbankserver geändert haben, müssen Sie das Kennwort des entsprechenden Benutzers zurücksetzen, der auf der Citrix ADC Appliance konfiguriert ist.

Zurücksetzen des Kennworts eines Datenbankbenutzers mit der CLI

Geben Sie an der Eingabeaufforderung

```
set db user <username> -password <password>
<!--NeedCopy-->
```

Beispiel:


```
set db user nsdbuser -password dd260538abs
<!--NeedCopy-->
```

Setzen Sie das Kennwort von Datenbankbenutzern über die grafische Benutzeroberfläche zurück

Navigieren Sie zu **System > Benutzerverwaltung > Datenbankbenutzer**, wählen Sie einen Benutzer aus, und geben Sie neue Werte für das Kennwort ein.

Wenn auf dem Datenbankserver kein Datenbankbenutzer mehr vorhanden ist, können Sie den Benutzer aus der Citrix ADC Appliance entfernen. Wenn der Benutzer jedoch weiterhin auf dem Datenbankserver vorhanden ist und Sie den Benutzer aus der ADC-Appliance entfernen, wird jede Anforderung vom Client mit diesem Benutzernamen nicht authentifiziert. Daher wird der Benutzername nicht an den Datenbankserver weitergeleitet.

Entfernen eines Datenbankbenutzers mit der CLI

Geben Sie an der Eingabeaufforderung

```
rm db user <username>
<!--NeedCopy-->
```

Beispiel:

```
rm db user nsdbuser
<!--NeedCopy-->
```

Entfernen eines Datenbankbenutzers mit der GUI

Navigieren Sie zu **System > Benutzerverwaltung > Datenbankbenutzer**, wählen Sie einen Benutzer aus, und klicken Sie auf **Löschen**.

Konfigurieren Sie einen Monitor, um die Namen aktiver Datenbanken abzurufen

Sie können einen Monitor erstellen, um die Liste aller aktiven Datenbanken auf einer Datenbankinstanz abzurufen. Der Monitor meldet sich mit gültigen Benutzeranmeldeinformationen am Datenbankserver an und führt eine entsprechende SQL-Abfrage aus. Die SQL-Abfrage, die Sie verwenden müssen, hängt von Ihrer SQL Server-Bereitstellung ab. Beispielsweise können Sie in einem

MSSQL-Datenbankspiegelungs-Setup die folgende Abfrage verwenden, um eine Liste der aktiven Datenbanken abzurufen, die auf einer Serverinstanz verfügbar sind.

```
select name from sys.databases where state=0
<!--NeedCopy-->
```

In einem MySQL Datenbank-Setup können Sie die folgenden Abfragen verwenden, um eine Liste der aktiven Datenbanken abzurufen, die auf einer Serverinstanz verfügbar sind.

Datenbanken anzeigen:

Sie konfigurieren den Monitor auch, um die Antwort auf eine Fehlerbedingung auszuwerten und die Ergebnisse zu speichern, wenn kein Fehler vorliegt. Wenn die Antwort einen Fehler enthält, markiert der Monitor den Dienst als DOWN. Die Appliance schließt den Dienst von Lastausgleichsentscheidungen aus, bis ein Fehler nicht mehr zurückgegeben wird.

> **Hinweis:**
>
> Die datenbankspezifische Lastenausgleichsfunktion wird nur für die Diensttypen MSSQL und MySQL unterstützt. Daher muss der Monitortyp MSSQL-ECV oder MYSQL-ECV sein.

Konfigurieren Sie einen Monitor, um die Namen aller aktiven Datenbanken abzurufen, die in einem Dienst über die Befehlszeilenschnittstelle gehostet werden

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Namen aller aktiven Datenbanken abzurufen, die auf einem Dienst gehostet werden, und überprüfen Sie die Konfiguration:

```
add lb monitor <monitorName> <type> -userName <string> -sqlQuery <text>
    -evalRule <expression> -storedb ENABLED

show lb monitor <monitorName>
<!--NeedCopy-->
```

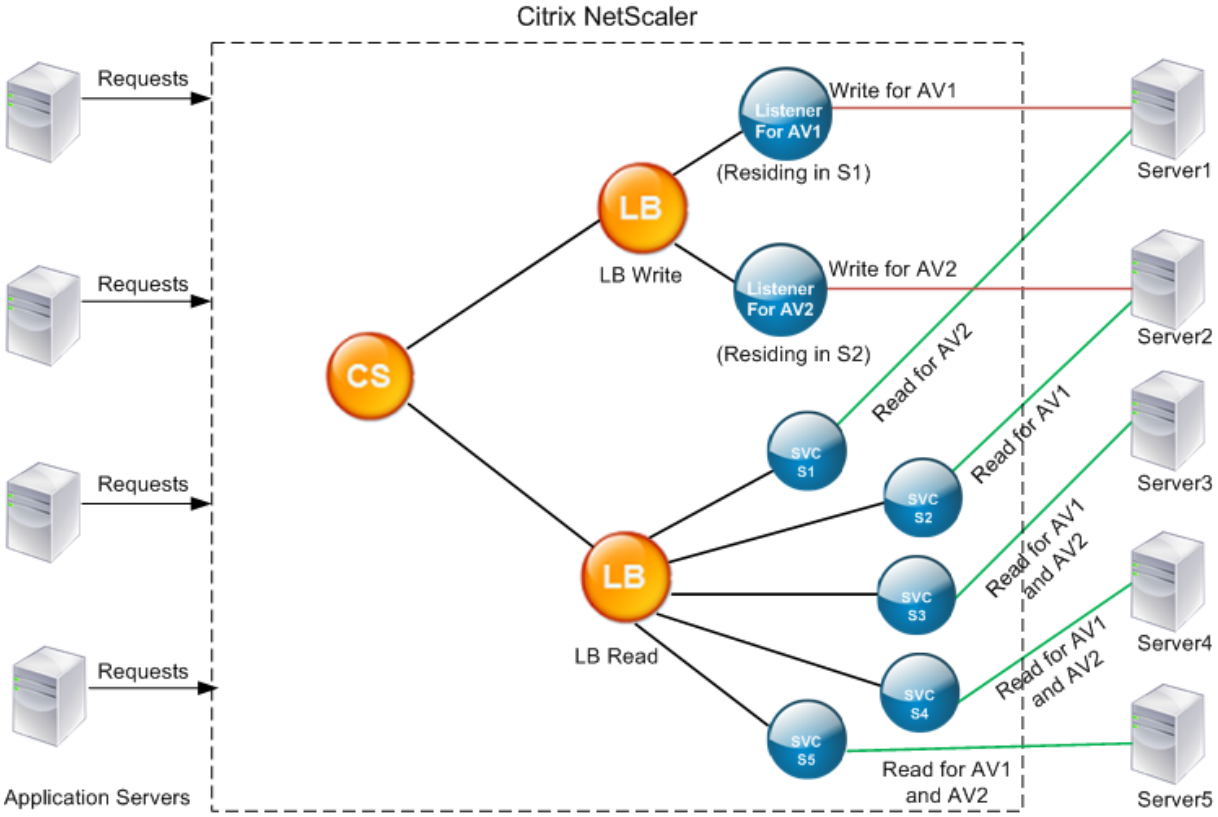
Konfigurieren Sie einen Monitor, um die Namen aller aktiven Datenbanken abzurufen, die in einem Dienst über die grafische Benutzeroberfläche gehostet werden

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**, und konfigurieren Sie einen Monitor vom Typ MSSQL-ECV oder MYSQL-ECV.
2. Geben Sie unter **Spezielle Parameter**einen Benutzernamen, eine Abfrage und eine Regel an. Beispiel: Bei MSSQL-ECV muss die Abfrage “Name aus sys.databases where state = 0 auswählen”

sein, und eine Regel muss MSSQL.RES.TYPE.NE (ERROR) sein. Für MYSQL-ECV muss die Abfrage “Datenbanken anzeigen” sein und eine Regel muss MYSQL.RES.TYPE.NE (ERROR) sein.

Unterstützung für Bereitstellungsgruppen für MSSQL

Betrachten Sie das folgende Szenario, in dem datenbankspezifischer Lastausgleich in einer Hochverfügbarkeitsgruppenbereitstellung konfiguriert ist. S1 bis S5 sind die Dienste auf der ADC-Appliance. DB1 bis DB4 sind die Datenbanken auf den Servern, die von den Diensten S1 bis S5 dargestellt werden. AV1 und AV2 sind die Verfügbarkeitsgruppen. Jede Verfügbarkeitsgruppe enthält bis zu einer primären Datenbankserverinstanz und bis zu vier sekundäre Datenbankserverinstanzen. Ein Dienst, der die Server in der Verfügbarkeitsgruppe darstellt, kann primär für eine Verfügbarkeitsgruppe und sekundär für eine andere Verfügbarkeitsgruppe sein. Jede Verfügbarkeitsgruppe enthält verschiedene Datenbanken und einen Listener, bei dem es sich um einen Dienst handelt. Alle Anforderungen kommen im Listener-Dienst an, der sich in der primären Datenbank befindet. AVI enthält Datenbanken DB1 und DB2. AV2 enthält Datenbanken DB3 und DB4. L1 und L2 sind die Listener auf AV1 bzw. AV2. S1 ist der primäre Dienst für AV1 und S2 ist der primäre Dienst für AV2.



Service	Liste der aktiven Datenbanken auf dem Dienst
S1	DB1, DB2, DB3, DB4
S2	DB3, DB4

Service	Liste der aktiven Datenbanken auf dem Dienst
S3	DB3, DB4
S4	DB1, DB2
S5	DB1, DB2

Verfügbarkeitsgruppe	Datenbanken	Dienste, die die Server in der Verfügbarkeitsgruppe repräsentieren
AV1	DB1, DB2	S1, S4, S5
AV2	DB3, DB4	S1, S2, S3

Abfragen werden wie folgt ausgeführt:

1. Eine READ-Abfrage für AV1 ist Lastausgleich zwischen S4 und S5. S1 ist die primäre für AV1.
2. Eine WRITE Abfrage für AV1 wird an L1 geleitet.
3. Eine READ-Abfrage für AV2 ist Lastenausgleich zwischen S1 und S3. S2 ist die primäre für AV2.
4. Eine WRITE Abfrage für AV1 wird an L2 geleitet.

Beispielkonfiguration

1. Konfigurieren Sie die virtuellen Lastenausgleichs- und Content Switching-Server.
   - `add lb vserver lbwrite -dbslb enabled`
   - `add lbvserver lbread MSSQL -dbslb enabled`
   - `add csvserver csv MSSQL 1.1.1.10 1433`
2. Konfigurieren Sie zwei Listener-Dienste, einen für jede Verfügbarkeitsgruppe und fünf Dienste S1 bis S5, die Datenbanken DB1 bis DB4 darstellen.
   - `add service L1 1.1.1.11 MSSQL 1433`
   - `add service L2 1.1.1.12 MSSQL 1433`
   - `add service s1 1.1.1.13 MSSQL 1433`
   - `add service s2 1.1.1.14 MSSQL 1433`
   - `add service s3 1.1.1.15 MSSQL 1433`
   - `add service s4 1.1.1.16 MSSQL 1433`
   - `add service s5 1.1.1.17 MSSQL 1433`
3. Binden Sie die Dienste an die virtuellen Server mit Lastenausgleich.
   - `bind lbvserver lbwrite L1`
   - `bind lbvserver lbwrite L2`

- `bind lbvserver lbread s1`
- `bind lbvserver lbread s2`
- `bind lbvserver lbread s3`
- `bind lbvserver lbread s4`
- `bind lbvserver lbread s5`

4. Datenbankbenutzer konfigurieren.
   - `add db user nsdbuser1 -password dd260427edf`
   - `add db user nsdbuser2 -password ccd1234xyzw`
5. Konfigurieren Sie zwei Monitore, Monitor_l1 und Monitor_l2 für jeden Listener-Dienst, um die Liste der aktiven Datenbanken in dieser Verfügbarkeitsgruppe abzurufen. Fügen Sie einen Monitor Monitor1 hinzu, um die Liste der Datenbanken für die sekundäre Datenbankserverinstanz abzurufen.
   - `add lb monitor monitor_L1 MSSQL-ECV -userName user1 -sqlQuery ” SELECT name FROM sys.databases a INNER JOIN sys.dm_hadr_availability_replica_ b ON a.replica_id=b.replica_id INNER JOIN sys.availability_group_listeners c on b.group_id = c.group_id INNER JOIN sys.availability_group_listener_ip_a d on c.listener_id = d.listener_id WHERE b.role = 1 and d.ip_address like '1.1.1.11'”-evalRule ”MSSQL.RES.TYPE.NE(ERROR)” -storedb ENABLED`
   - `add lb monitor monitor_L2 MSSQL-ECV -userNameuser1 -sqlQuery ” SELECT name FROM sys.databases a INNER JOIN sys.dm_hadr_availability_replicca b ON a.replica_id=b.replica_id INNER JOIN sys.availability_group_listeners c on b.group_id = c.group_id INNER JOIN sys.availability_group_listener_ip_a d on c.listener_id = d.listener_id WHERE b.role = 1 and d.ip_address like '1.1.1.12'”-evalRule ”MSSQL.RES.TYPE.NE(ERROR)”-storedb ENABLED`
   - `add lb monitor monitor1 MSSQL-ECV -userNameuser1 -sqlQuery ”SELECT name FROM sys.databases a INNER JOIN sys.dm_hadr_availability_replica_states b ON a.replica_id=b.replica_id WHERE b.role = 2”-evalRule ”MSSQL. RES.TYPE.NE(ERROR)”-storedb ENABLED`
6. Konfigurieren Sie Lese- und Schreibrichtlinien.
   - `add cs policy pol_write -rule ”MSSQL.REQ.QUERY.TEXT.CONTAINS(” insert”)”`
   - `add cs policy pol_read -rule ”MSSQL.REQ.QUERY.TEXT.CONTAINS(”select ”)”`
7. Binden Sie die Richtlinien an den virtuellen Content Switching-Server.
   - `bind csvserver csv -targetLBVserver lbwrite -policyName pol_write - priority 11`
   - `bind csvserver csv -targetLBVserver lbread -policyName pol_read -`


```
priority 12
```

8. Binden Sie Monitore an die Dienste. Binden Sie Monitore an die Dienste L1 und L2, um die Liste der aktiven Datenbanken für die Verfügbarkeitsgruppe zu erhalten, für die sie der Listener ist. Binden Sie Monitore an alle Dienste, die an den schreibgeschützten virtuellen Server gebunden sind.
   - `bind service L1 -monitorName monitor_L1`
   - `bind service L2 -monitorName monitor_L2`
   - `bind service s1 -monitorName monitor1`
   - `bind service s2 -monitorName monitor1`
   - `bind service s3 -monitorName monitor1`
   - `bind service s4 -monitorName monitor1`
   - `bind service s5 -monitorName monitor1`

Konfigurationsbeispiele für den virtuellen MSSQL-Server

So konfigurieren Sie einen virtuellen Lastausgleichsserver für den datenbankspezifischen Lastenausgleich:

```
1  add lb vserver DBSpecificLB1 MSSQL 192.0.2.10 1433 -dbsLb ENABLED
2
3  Done
4
5  show lb vserver DBSpecificLB1
6
7  DBSpecificLB1 (192.0.2.10:1433) - MSSQL Type: ADDRESS
8  . . .
9  DBS_LB: ENABLED
10
11 Done
12 <!--NeedCopy-->
```

So konfigurieren Sie Dienste:

Dienst hinzufügen msservice1 5.5.5.5 MSSQL 1433

So konfigurieren Sie einen Monitor zum Abrufen der Namen aller aktiven Datenbanken, die in einem Dienst gehostet werden, mithilfe der Befehlszeile:

```
1  add lb monitor mssql-monitor1 MSSQL-ECV -userName user1 -sqlQuery ”
       select name from sys.databases where state=0” -evalRule ”MSSQL.RES.
       TYPE.NE(ERROR)” -storedb EN
```



```
2
3 Done
4
5 show lb monitor mssql-monitor1
6
7 1)   Name.......: mssql-monitor1    Type......: MSSQL-ECV
8
9 ...
10
11 Special parameters: Database.....:""
12
13 User name.....:"user1"
14
15 Query..:select name from sys.databases where state=0 EvalRule...:MSSQL.
      RES.TYPE.NE(ERROR)
16
17 Version...:70 STORE_DB...:ENABLED
18
19 Done
20 <!--NeedCopy-->
```

Konfigurationsbeispiele für den virtuellen MySQL -Server

So konfigurieren Sie einen virtuellen Lastausgleichsserver für den datenbankspezifischen Lastenausgleich:

```
1 add lb vserver DBSpecificLB1 MYSQL 192.0.2.10 3306 -dbsLb ENABLED
2
3 Done
4
5 show lb vserver DBSpecificLB1
6
7 DBSpecificLB1 (192.0.2.10:3306) - MYSQL Type: ADDRESS
8
9 . . .
10
11 DBS_LB: ENABLED
12
13 Done
14 <!--NeedCopy-->
```

So konfigurieren Sie Dienste:


```
add service msservice1 5.5.5.5 MYSQL 3306
<!--NeedCopy-->
```

So konfigurieren Sie einen Monitor zum Abrufen der Namen aller aktiven Datenbanken, die in einem Dienst gehostet werden, mithilfe der Befehlszeile:

```
add lb monitor mysql-monitor1 MYSQL-ECV -userName user1 -sqlQuery "show
    databases" -evalRule "MYSQL.RES.TYPE.NE(ERROR)" -storedb ENABLED

Done

show lb monitor mysql-monitor1

1)     Name.......: mysql-monitor1  Type......: MYSQL-ECV  State....:
   ENABLED

...

Special parameters: Database.....:""

User name.....:"user1" Query..:show databases

EvalRule...:MYSQL.RES.TYPE.NE(ERROR) STORE_DB...:ENABLED

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

DataStream Referenz

April 25, 2022

Diese Referenz beschreibt die Protokolle MySQL und TDS, die Datenbankversionen, die Authentifizierungsmethoden und die Zeichensätze, die von der DataStream Funktion unterstützt werden. Außerdem wird beschrieben, wie Citrix ADC Transaktionsanforderungen und spezielle Abfragen verarbeitet, die den Status einer Verbindung ändern.

Sie können die Citrix ADC Appliance auch so konfigurieren, dass Auditprotokollmeldungen für die DataStream -Funktion generiert werden.

Unterstützte Datenbankversionen, Protokolle und Authentifizierungsmethoden

	MySQL Datenbank	MS SQL-Datenbank
Datenbankversionen	MySQL Datenbankversionen 4.1, 5.0, 5.1, 5.4, 5.5, 5.6	MS SQL-Datenbankversionen 2000, 2000SP1, 2005, 2008, 2008R2, 2012, 2014 (Unterstützung für Kerberos-Authentifizierung)
Protokolle	MySQL Protokoll Version 10. Informationen zum MySQL-Protokoll finden Sie unter MySQL Client/Server Protocol	Tabular Data Stream (TDS) Protokoll Version 7.1 und höher. Informationen zum TDS-Protokoll finden Sie unter Tabular Data Stream Protocol
Authentifizierungsmethoden	Die native MySQL Authentifizierung wird unterstützt.	SQL Server-Authentifizierung und Windows-Authentifizierung (Kerberos/NTLM) werden unterstützt.

Zeichen-Sätze

Die DataStream Funktion unterstützt nur den UTF-8-Zeichensatz.

Der Zeichensatz, der vom Client beim Senden einer Anforderung verwendet wird, kann sich von dem Zeichensatz unterscheiden, der in den Antworten des Datenbankservers verwendet wird. Obwohl der charset-Parameter während des Verbindungsaufbaus festgelegt wird, kann er jederzeit durch Senden einer SQL-Abfrage geändert werden. Der Zeichensatz ist einer Verbindung zugeordnet, und daher kann kein Multiplexing von Anfragen für Verbindungen mit einem Zeichensatz auf eine Verbindung mit einem anderen Zeichensatz stattfinden.

Die Citrix ADC Appliance analysiert die vom Client gesendeten Abfragen und die vom Datenbankserver gesendeten Antworten.

Der mit einer Verbindung verknüpfte Zeichensatz kann nach dem ersten Handshake mithilfe der folgenden beiden Abfragen geändert werden:

```
1 SET NAMES <charset> COLLATION <collation>
2
3 SET CHARACTER SET <charset>
```



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

Transaktionen

In MySQL werden Transaktionen mithilfe des Verbindungsparameters AUTOCOMMIT oder der BEGIN:COMMIT Abfragen identifiziert. Der AUTOCOMMIT Parameter kann während des ersten Handshake oder nach der Verbindung mit der Abfrage SET AUTOCOMMIT gesetzt werden.

Die Citrix ADC Appliance analysiert jede Abfrage explizit, um den Anfang und das Ende einer Transaktion zu bestimmen.

Im MySQL-Protokoll enthält die Antwort zwei Flags, die angeben, ob es sich bei der Verbindung um eine Transaktion handelt: die Signs TRANSACTION und AUTOCOMMIT.

Wenn es sich bei der Verbindung um eine Transaktion handelt, wird das TRANSACTION-Flag gesetzt. Oder wenn der AutoCommit-Modus OFF ist, ist das AUTOCOMMIT Flag nicht gesetzt. Die ADC-Appliance analysiert die Antwort, und wenn entweder das TRANSACTION-Flag gesetzt ist oder das AUTOCOMMIT Flag nicht gesetzt ist, wird kein Verbindungsmultiplexing durchgeführt. Wenn diese Bedingungen nicht mehr zutreffen, beginnt die ADC-Appliance das Verbindungsmultiplexing.

> **Hinweis:**
>
> Transaktionen werden auch für MS SQL unterstützt.

Spezielle Anfragen

Es gibt spezielle Abfragen, wie SET und PREPARE, die den Status der Verbindung ändern und möglicherweise das Umschalten der Anforderung unterbrechen. Daher müssen diese Abfragen anders behandelt werden.

Beim Empfang einer Anforderung mit speziellen Abfragen sendet die Citrix ADC Appliance eine OK-Antwort an den Client und speichert die Anforderung auch in der Verbindung.

Wenn eine nicht spezielle Abfrage wie INSERT und SELECT zusammen mit einer gespeicherten Abfrage empfangen wird, sucht die ADC-Appliance nach der serverseitigen Verbindung, auf der die gespeicherte Abfrage bereits an den Datenbankserver gesendet wurde. Wenn keine solchen Verbindungen vorhanden sind, erstellt die ADC-Appliance eine Verbindung und sendet zuerst die gespeicherte Abfrage und sendet dann die Anforderung mit der nicht speziellen Abfrage.

In den Sonderabfragen SET, USE db und INIT_DB ändert die Appliance ein Feld in der serverseitigen Verbindung, das der speziellen Abfrage entspricht. Diese Änderung führt zu einer besseren Wiederverwendung der serverseitigen Verbindung.

In jeder Verbindung werden nur 16 Abfragen gespeichert.

Im Folgenden finden Sie eine Liste der speziellen Abfragen, für die die ADC-Appliance ein geändertes Verhalten hat.

- SET-Abfrage

  Die SET SQL-Abfragen definieren Variablen, die der Verbindung zugeordnet sind. Diese Abfragen werden auch verwendet, um globale Variablen zu definieren, aber ab sofort kann die ADC-Appliance nicht zwischen lokalen und globalen Variablen unterscheiden. Für diese Abfrage verwendet die ADC-Appliance den Mechanismus Speichern und Weiterleiten.

- <db>“ USE-Abfrage

  Mit dieser Abfrage kann der Benutzer die Datenbank ändern, die einer Verbindung zugeordnet ist. In diesem Fall analysiert die ADC-Appliance den gesendeten<db> Wert und ändert ein Feld in der serverseitigen Verbindung, um die neue zu verwendende Datenbank wiederzugeben.

- INIT_DB (Befehl)

  Mit dieser Abfrage kann der Benutzer die Datenbank ändern, die einer Verbindung zugeordnet ist. In diesem Fall analysiert die ADC-Appliance den gesendeten<init_db> Wert und ändert ein Feld in der serverseitigen Verbindung, um die neue zu verwendende Datenbank wiederzugeben.

- COM_PREPARE

  Die ADC-Appliance beendet die Anforderungsschaltung beim Empfang dieses Befehls.

- PREPARE-Abfrage

  Diese Abfrage wird verwendet, um vorbereitete Anweisungen zu erstellen, die einer Verbindung zugeordnet sind. Für diese Abfrage verwendet die ADC-Appliance den Mechanismus Speichern und Weiterleiten.

Unterstützung von Überwachungsprotokollmeldungen

Sie können jetzt die Citrix ADC Appliance so konfigurieren, dass Auditprotokollmeldungen für die DataStream -Funktion generiert werden. Auditprotokollmeldungen werden generiert, wenn clientseitige und serverseitige Verbindungen hergestellt, geschlossen oder gelöscht werden. Die Kategorien von Nachrichten, die Sie protokollieren und anzeigen können, sind ERROR und INFO. Fehlermeldungen für clientseitige Verbindungen beginnen mit CS und Fehlermeldungen für serverseitige Verbindungen beginnen mit SS. Zusätzliche Informationen werden erforderlichenfalls zur Verfügung gestellt. Beispielsweise enthalten Protokollmeldungen für geschlossene Verbindungen (CS_CONN_CLOSED) nur die Verbindungs-ID. Protokollmeldungen für etablierte Verbindungen (CS_CONN_ESTD) enthalten jedoch Informationen wie Benutzername, Datenbankname und Client-IP-Adresse zusätzlich zur Verbindungs-ID.

Domain-Namenssystem

October 5, 2021

Hinweis: Ab Release 13.0 Build 41.x ist die Citrix ADC Appliance im ADNS- und Proxy-Modus vollständig mit dem DNS-Flag-Tag 2019 kompatibel.

Sie können die Citrix ADC Appliance so konfigurieren, dass sie als autorisierender Domänennamenserver (ADNS-Server) für eine Domäne fungiert. Fügen Sie die DNS-Ressourceneinträge hinzu, die zu der Domäne gehören, für die die Appliance autorisierend ist, und konfigurieren Sie Ressourceneintragsparameter. Sie können die Appliance auch als Proxy-DNS-Server konfigurieren, der eine Farm von DNS-Namensservern ausgleicht, die sich innerhalb oder außerhalb des Netzwerks befinden. Konfigurieren Sie die Appliance als Resolver und Forwarder. Sie können DNS-Suffixe konfigurieren, die die Namensauflösung aktivieren, wenn vollqualifizierte Domänennamen nicht konfiguriert sind. Die Appliance unterstützt auch die DNS ANY-Abfrage, die alle Datensätze abruft, die zu einer Domäne gehören.

Sie können die Appliance so konfigurieren, dass sie gleichzeitig als autorisierender DNS-Server für eine Domäne und als DNS-Proxyserver für eine andere Domäne fungiert. Wenn Sie die Appliance als autorisierenden DNS-Server oder DNS-Proxyserver für eine Zone konfigurieren, können Sie die Appliance aktivieren, TCP für Antwortgrößen zu verwenden, die die für das User Datagram Protocol (UDP) angegebene Größenbeschränkung überschreiten.

Funktionsweise von DNS auf Citrix ADC

Sie können die Citrix ADC Appliance so konfigurieren, dass sie als ADNS-Server, DNS-Proxyserver, Resolver und Forwarder fungiert. Sie können DNS-Ressourceneinträge auf der Citrix ADC Appliance hinzufügen, einschließlich der folgenden Datensätze:

- Service-Einträge (SRV)
- IPv6-Einträge (AAAA)
- Adressdatensätze (A)
- Mail-Austausch-Einträge (MX)
- Canonical Name (CNAME) -Datensätze
- Pointer (PTR) -Datensätze
- Beginn der Autoritätsdatensätze (SOA)
- Texteinträge (TXT)

Außerdem können Sie Citrix ADC für den Lastenausgleich externer DNS-Nameserver konfigurieren.

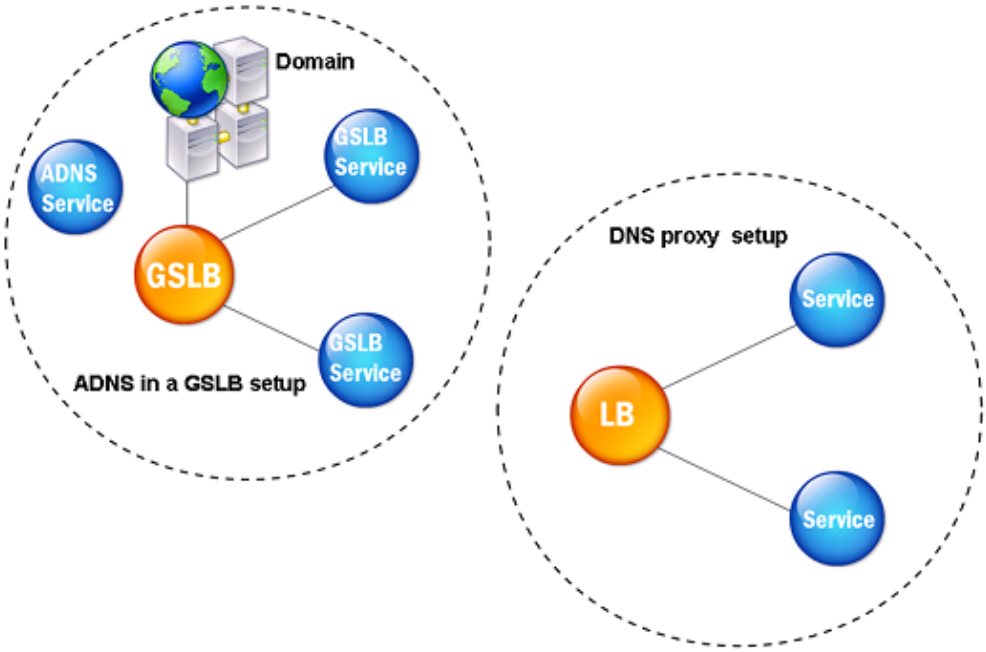
Die Citrix ADC Appliance kann als Autorität für eine Domäne konfiguriert werden. Fügen Sie gültige SOA- und NS-Einträge für die Domäne hinzu.

Ein ADNS-Server ist ein DNS-Server, der vollständige Informationen zu einer Zone enthält.

Um die Citrix ADC Appliance als ADNS-Server für eine Zone zu konfigurieren, müssen Sie einen ADNS-Dienst hinzufügen und dann die Zone konfigurieren. Dazu fügen Sie gültige SOA- und NS-Einträge für die Domäne hinzu. Wenn ein Client eine DNS-Anforderung sendet, durchsucht die Citrix ADC Appliance die konfigurierten Ressourceneinträge nach dem Domänennamen. Sie können den ADNS-Dienst für die Verwendung mit der Citrix ADC Funktion Global Server Load Balancing (GSLB) konfigurieren.

Sie können eine Subdomäne delegieren, indem Sie NS-Einträge für die Subdomäne zur Zone der übergeordneten Domäne hinzufügen. Anschließend können Sie Citrix ADC autorisierend für die Subdomäne machen, indem Sie für jeden der Subdomain-Nameserver einen Glue Record hinzufügen. Wenn GSLB konfiguriert ist, trifft Citrix ADC basierend auf seiner Konfiguration eine GSLB-Lastausgleichsentscheidung und antwortet mit der IP-Adresse des ausgewählten virtuellen Servers. Die folgende Abbildung zeigt die Entitäten in einem ADNS-GSLB-Setup und einem DNS-Proxy-Setup.

Abbildung 1. DNS-Proxy-Entitätsmodell



Die Citrix ADC Appliance kann als DNS-Proxy fungieren. Die Zwischenspeicherung von DNS-Einträgen, die eine wichtige Funktion eines DNS-Proxy darstellt, ist standardmäßig auf der Citrix ADC Appliance aktiviert. Caching ermöglicht es der Citrix ADC Appliance, schnelle Antworten auf wiederholte Übersetzungen bereitzustellen. Erstellen Sie einen virtuellen DNS-Server mit Lastenausgleich und DNS-Dienste, und binden Sie diese Dienste dann an den virtuellen Server.

Der Citrix ADC bietet zwei Optionen: Mindestzeitdauer (TTL) und maximale TTL für die Konfiguration der Lebensdauer der zwischengespeicherten Daten. Das Timeout der zwischengespeicherten Daten gemäß den Einstellungen für diese beiden Optionen. Citrix ADC überprüft die TTL des DNS-Eintrags, der vom Server stammt. Wenn die TTL kleiner als die konfigurierte Mindest-TTL ist, wird sie durch die konfigurierte Mindest-TTL ersetzt. Wenn die TTL größer als die konfigurierte maximale TTL ist, wird sie durch die konfigurierte maximale TTL ersetzt.

Der Citrix ADC ermöglicht auch das Zwischenspeichern von negativen Antworten für eine Domäne. Eine negative Antwort gibt an, dass Informationen zu einer angeforderten Domäne nicht vorhanden sind oder dass der Server keine Antwort für die Abfrage bereitstellen kann. Die Speicherung dieser Informationen wird als *negatives Caching*bezeichnet. Negatives Caching hilft, die Antworten auf Abfragen in einer Domäne zu beschleunigen und kann optional den Datensatztyp bereitstellen.

Eine negative Antwort kann eine der folgenden sein:

- NXDOMAIN Fehlermeldung - Wenn eine negative Antwort im lokalen Cache vorhanden ist, gibt der Citrix ADC eine Fehlermeldung (NXDOMAIN) zurück. Wenn sich die Antwort nicht im lokalen Cache befindet, wird die Abfrage an den Server weitergeleitet, und der Server gibt einen NXDOMAIN-Fehler an den Citrix ADC zurück. Citrix ADC speichert die Antwort lokal und gibt dann die Fehlermeldung an den Client zurück.
- NODATA-Fehlermeldung - Citrix ADC sendet eine NODATA-Fehlermeldung, wenn der Domänenname in der Abfrage gültig ist, Datensätze des angegebenen Typs jedoch nicht verfügbar sind.

Citrix ADC unterstützt die rekursive Auflösung von DNS-Anforderungen. In rekursiver Auflösung sendet der Resolver (DNS-Client) eine rekursive Abfrage an einen Nameserver für einen Domänennamen. Wenn der abgefragte Nameserver autorisierend für die Domäne ist, antwortet er mit dem angeforderten Domänennamen. Andernfalls fragt Citrix ADC die Nameserver rekursiv ab, bis der angeforderte Domänenname gefunden wird.

Bevor Sie die rekursive Abfrageoption anwenden können, müssen Sie sie zuerst aktivieren. Sie können auch festlegen, wie oft der DNS-Resolver eine Auflösungsanforderung senden muss (DNS-Wiederholungsversuche), wenn eine DNS-Suche fehlschlägt.

Sie können den Citrix ADC als DNS-Weiterleitung konfigurieren. Eine Weiterleitung übergibt DNS-Anforderungen an externe Nameserver. Mit dem Citrix ADC können Sie externe Nameserver hinzufügen und eine Namensauflösung für Domänen außerhalb des Netzwerks bereitstellen. Mit dem Citrix ADC können Sie auch die Priorität für die Namenssuche auf DNS oder Windows Internet Name Service (WINS) festlegen.

Aktivieren Sie die ADC-Appliance, DNS zum Auflösen des Hostnamens in die entsprechende IP-Adresse zu verwenden

Hinweis: Sie benötigen ein SSH-Dienstprogramm, um auf die Befehlszeilenschnittstelle (CLI) der Appliance zuzugreifen.

Standardmäßig kann die ADC-Appliance den Hostnamen nicht in die entsprechende IP-Adresse auflösen. Führen Sie die folgenden Aufgaben aus, um die Namensauflösung auf der Appliance zu aktivieren:

1. Definieren Sie Namensserver.
2. Definieren Sie ein DNS-Suffix.

Punkte zu beachten

Führen Sie die DNS-Suche von der CLI aus. DNS-Lookups von der Shell-Eingabeaufforderung des FreeBSD-Betriebssystems schlagen fehl, da der Eintrag in der Datei /etc/resolv.conf auf die IP-Adresse 127.0.0.2 verweist.

Die folgenden Befehle sind in der Befehlszeilenschnittstelle der Appliance nicht verfügbar:

```
- host
- dig
- getent/MIP
- nslookup
<!--NeedCopy-->
```

Wenn die Appliance den DNS-Server an der SNIP-Adresse nicht pingen kann, wird der Serverstatus als heruntergefahren angezeigt. Erfolgreiches Ping ist wichtig, wenn sich die Appliance hinter einer Firewall befindet.

CLI-Konfiguration

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add dns nameServer <Name_Server_IP_Address>
add dns suffix <DNS_Suffix>
<!--NeedCopy-->
```

Geben Sie Folgendes ein, um die Konfiguration zu überprüfen:

```
show dns nameServer
show dns suffix
<!--NeedCopy-->
```


Geben Sie Folgendes ein, um die DNS-Auflösung zu testen:

```
show dns addrec <Host_Name>
<!--NeedCopy-->
```

GUI-Konfiguration

1. Navigieren Sie zu **Traffic Management > DNS > Namensserver > Hinzufügen**.
2. Geben **Sie im Dialogfeld Nameserver erstellen** die IP-Adresse des Nameservers ein, und klicken Sie auf **Erstellen**.
3. Navigieren Sie zu **Traffic Management > DNS > DNS Suffix > Hinzufügen**.
4. Geben Sie im Dialogfeld **DNS-Suffix erstellen** das DNS-Suffix ein, z. B. example.com, das für alle Hostabfragen verwendet werden soll, und klicken Sie auf **Erstellen**.

Round Robin DNS

Wenn ein Client eine DNS-Anforderung sendet, um den DNS-Ressourceneintrag zu finden, erhält er eine Liste von IP-Adressen, die in den Namen in der DNS-Anforderung aufgelöst werden. Der Client verwendet dann eine der IP-Adressen in der Liste, in der Regel den ersten Datensatz oder die IP-Adresse. Daher wird ein einzelner Server für die gesamte TTL des Cache verwendet und ist überlastet, wenn viele Anfragen eintreffen.

Wenn Citrix ADC eine DNS-Anforderung empfängt, reagiert es, indem die Reihenfolge der Liste der DNS-Ressourceneinträge in einer Roundrobin-Methode geändert wird. Diese Funktion wird *Round Robin DNS* genannt. Round Robin verteilt den Datenverkehr gleichmäßig zwischen Rechenzentren. Citrix ADC führt diese Funktion automatisch aus. Sie müssen dieses Verhalten nicht konfigurieren.

Funktionsübersicht

Wenn Citrix ADC als ADNS-Server konfiguriert ist, werden die DNS-Einträge in der Reihenfolge zurückgegeben, in der die Datensätze konfiguriert sind. Wenn Citrix ADC als DNS-Proxy konfiguriert ist, gibt es die DNS-Einträge in der Reihenfolge zurück, in der er die Datensätze vom Server empfängt. Die Reihenfolge der im Cache vorhandenen Datensätze entspricht der Reihenfolge, in der Datensätze vom Server empfangen werden.

Citrix ADC ändert dann die Reihenfolge, in der Datensätze in der DNS-Antwort in einer Roundrobin-Methode gesendet werden. Die erste Antwort enthält den ersten Datensatz in Folge, die zweite Antwort enthält den zweiten Datensatz in Folge und die Reihenfolge wird in derselben Reihenfolge fortgesetzt. Daher können Clients, die denselben Namen anfordern, eine Verbindung zu verschiedenen IP-Adressen herstellen.

Beispiel für Round-Robin-DNS

Als Beispiel für Roundrobin-DNS nehmen Sie DNS-Einträge, die wie folgt hinzugefügt wurden:

```
1   add dns addRec ns1 1.1.1.1  add dns addRec ns1 1.1.1.2  add dns
       addRec ns1 1.1.1.3  add dns addRec ns1 1.1.1.4
2 <!--NeedCopy-->
```

Die Domäne abc.com ist wie folgt mit einem NS-Eintrag verknüpft:

```
1   add dns nsrec abc.com. ns1
2 <!--NeedCopy-->
```

Wenn der Citrix ADC eine Abfrage für den A-Datensatz ns1 empfängt, werden die Adressdatensätze in einer Roundrobin-Methode wie folgt bereitgestellt. In der ersten DNS-Antwort wird 1.1.1.1 als erster Datensatz bereitgestellt:

```
1   ns1.                    1H IN A         1.1.1.1  ns1.
                           1H IN A         1.1.1.2  ns1.
                           1H IN A         1.1.1.3  ns1.
                           1H IN A         1.1.1.4
2 <!--NeedCopy-->
```

In der zweiten DNS-Antwort wird die zweite IP-Adresse 1.1.1.2 als erster Datensatz bereitgestellt:

```
1   ns1.                    1H IN A         1.1.1.2  ns1.
                           1H IN A         1.1.1.3  ns1.
                           1H IN A         1.1.1.4  ns1.
                           1H IN A         1.1.1.1
2 <!--NeedCopy-->
```

In der dritten DNS-Antwort wird die dritte IP-Adresse 1.1.1.2 als erster Datensatz bereitgestellt:

```
1   ns1.                    1H IN A         1.1.1.3  ns1.
                           1H IN A         1.1.1.4  ns1.
                           1H IN A         1.1.1.1  ns1.
                           1H IN A         1.1.1.2
2 <!--NeedCopy-->
```


Konfigurieren von DNS-Ressourceneinträgen

October 5, 2021

Sie konfigurieren Ressourceneinträge auf der Citrix® ADC-Appliance, wenn Sie die Appliance als ADNS-Server für eine Zone konfigurieren. Sie können Ressourceneinträge auch auf der Appliance konfigurieren, wenn die Ressourceneinträge zu einer Zone gehören, für die die Appliance ein DNS-Proxyserver ist. Auf der Appliance können Sie die folgenden Datensatztypen konfigurieren:

- Service-Aufzeichnungen
- AAAA-Datensätze
- Adressdatensätze
- Mail-Exchange-Einträge
- Nameserver-Einträge
- Kanonische Aufzeichnungen
- Zeigereinträge
- NAPTR-Einträge
- Beginn der Aufzeichnungen der Behörde
- Textdatensätze

In der folgenden Tabelle sind die Datensatztypen aufgeführt, die Sie für einen Domänennamendatensatz auf der Citrix ADC Appliance konfigurieren können. Beispielsweise können Sie maximal 25 IP-Adressen für einen Datensatz konfigurieren.

Tabelle 1. Datensatztyp und -nummer konfigurierbar

Datensatztyp	Anzahl der Datensätze
Adresse (A)	25
IPv6 (AAAA)	5
Briefwechsel (MX)	12
Namensserver (NS)	16
Service (SRV)	8
Zeiger (PTR)	20
Kanonischer Name (CNAME)	1
Beginn der Behörde (SOA)	1
Text (TXT)	20
Namensbefugnis Zeiger (NAPTR)	20

> **Hinweis:**
>
> Die maximale Anzahl von IP-Adressen für einen bestimmten Hostnamen beträgt 25. Die Anzahl der verschiedenen Adressdatensätze kann jedoch mehr als 25 betragen.

Erstellen von SRV-Datensätzen für einen Dienst

October 5, 2021

Der SRV-Eintrag enthält Informationen zu den Diensten, die auf der Citrix ADC Appliance verfügbar sind. Ein SRV-Eintrag enthält die folgenden Informationen:

- Name des Dienstes und des Protokolls
- Domänenname
- TTL
- DNS-Klasse
- Priorität des Ziels
- Gewicht der Datensätze mit der gleichen Priorität
- Port des Dienstes
- Hostname des Dienstes

Citrix ADC wählt zuerst den SRV-Eintrag mit der niedrigsten Priorität aus. Wenn ein Dienst mehrere SRV-Datensätze mit derselben Priorität hat, verwenden Clients das Gewichtungsfeld, um zu bestimmen, welcher Host verwendet werden soll.

Hinzufügen eines SRV-Datensatzes mit der CLI

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

```
1 -  add dns srvRec <domain> <target> -priority <positive_integer> -
     weight <positive_integer> -port <positive_integer> [-TTL <secs>]
2 -  sh dns srvRec <domain>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add dns srvRec _http._tcp.example.com nameserver1.com -priority 1 -
     weight 1 -port 80
```



```
 Done
> show dns srvRec _http._tcp.example.com
1)      Domain Name : _http._tcp.example.com
        Target Host : nameserver1.com
        Priority : 1    Weight : 1
        Port : 80       TTL : 3600 secs
 Done
<!--NeedCopy-->
```

Ändern oder Entfernen eines SRV-Datensatzes mit der CLI

- Um einen SRV-Datensatz zu ändern, geben Sie ein:
  - Den Befehl `set dns srvRec`
  - Der Name der Domäne, für die der SRV-Eintrag konfiguriert ist
  - Der Name des Zielhosts, der den zugehörigen Dienst hostet
  - Die zu ändernden Parameter mit ihren neuen Werten
- Um einen SRV-Record zu entfernen, geben Sie Folgendes ein:
  - Den Befehl `rm dns srvRec`
  - Der Name der Domäne, für die der SRV-Eintrag konfiguriert ist
  - Der Name des Zielhosts, der den zugehörigen Dienst hostet

Konfigurieren eines SRV-Datensatzes mit der GUI

Navigieren Sie zu **Traffic Management > DNS > Records > SRV Records** und erstellen Sie einen SRV-Eintrag.

Erstellen von AAAA-Einträgen für einen Domainnamen

October 5, 2021

Ein AAAA-Ressourceneintrag speichert eine einzelne IPv6-Adresse.

Hinzufügen eines AAAA-Datensatzes mit der CLI

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

```
-  add dns aaaaRec <hostName> <IPv6Address> ... [-TTL <secs>]
```



```
2 -  show dns aaaaRec <hostName>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add dns aaaaRec www.example.com 2001:0db8:0000:0000:0000:0000:1428:57
     ab
2  Done
3 > show dns aaaaRec www.example.com
4 1)      Host Name : www.example.com
5         Record Type : ADNS              TTL : 5 secs
6         IPV6 Address : 2001:db8::1428:57ab
7  Done
8 <!--NeedCopy-->
```

Um einen AAAA-Eintrag und alle mit dem Domainnamen verbundenen IPv6-Adressen zu entfernen, geben Sie den `rm dns aaaaRec` Befehl und den Domänennamen ein, für den der AAAA-Eintrag konfiguriert ist. Um nur eine Teilmenge der IPv6-Adressen zu entfernen, die mit dem Domainnamen in einem AAAA-Eintrag verknüpft sind, geben Sie Folgendes ein:

- `rm dns aaaaRec` Befehl
- Der Domainname, für den der AAAA-Eintrag konfiguriert ist
- Die IPv6-Adressen, die Sie entfernen möchten

Hinzufügen eines AAAA-Datensatzes mit der GUI

Navigieren Sie zu **Traffic Management > DNS > Records > AAAA Records** und erstellen Sie einen AAAA-Eintrag.

Erstellen von Adressdatensätzen für einen Domänennamen

October 5, 2021

Address (A) -Einträge sind DNS-Einträge, die einen Domänennamen einer IPv4-Adresse zuordnen.

Adressdatensätze für einen Host, der am globalen Server Load Balancing (GSLB) beteiligt ist, können nicht gelöscht werden. Der Citrix ADC löscht jedoch Adressdatensätze, die für GSLB-Domänen hinzugefügt wurden, wenn Sie die Bindung der Domäne von einem virtuellen GSLB-Server aufheben. Nur vom Benutzer konfigurierte Datensätze können manuell gelöscht werden. Sie können keinen Datensatz für einen Host löschen, auf den durch Datensätze wie NS, MX oder CNAME verwiesen wird.

Hinzufügen eines Adressdatensatzes mit der CLI

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

```
-  add dns addRec <hostName> <IPAddress> [-TTL <secs>]
-  show dns addRec <hostName>
<!--NeedCopy-->
```

Beispiel:

```
> add dns addRec ns.example.com 192.0.2.0
 Done
> show dns addRec ns.example.com
1)      Host Name : ns.example.com
        Record Type : ADNS                      TTL : 5 secs
        IP Address : 192.0.2.0
 Done
<!--NeedCopy-->
```

Um einen Adressdatensatz und alle mit dem Domainnamen verknüpften IP-Adressen zu entfernen, geben Sie den `rm dns addRec` Befehl und den Domänennamen ein, für den der Adressdatensatz konfiguriert ist. Um nur eine Teilmenge der IP-Adressen zu entfernen, die mit dem Domainnamen in einem Adressdatensatz verknüpft sind, geben Sie Folgendes ein:

- `rm dns addRec` Befehl
- Der Domänenname, für den der Adressdatensatz konfiguriert ist
- Die IP-Adressen, die Sie entfernen möchten

Hinzufügen eines Adressdatensatzes mit der GUI

Navigieren Sie zu **Traffic Management > DNS > Datensätze > Adressdatensätze** und erstellen Sie einen Adressdatensatz.

Erstellen von MX-Datensätzen für einen Mail-Exchange-Server

October 5, 2021

Mail Exchange (MX) -Datensätze werden verwendet, um E-Mail-Nachrichten über das Internet zu leiten. Ein MX-Eintrag enthält eine MX-Voreinstellung, die den zu verwendenden MX-Server angibt.

Die MX-Voreinstellungswerte reichen von 0 bis 65536. Ein MX-Eintrag enthält eine eindeutige MX-Präferenznummer. Sie können die MX-Voreinstellung und die TTL-Werte für einen MX-Eintrag festlegen.

Wenn eine E-Mail-Nachricht über das Internet gesendet wird, sendet ein E-Mail-Übertragungs-Agent eine DNS-Abfrage, die den MX-Eintrag für den Domänennamen anfordert. Diese Abfrage gibt eine Liste der Hostnamen von Mail-Exchange-Servern für die Domäne zusammen mit einer Einstellungsnummer zurück. Wenn keine MX-Einträge vorhanden sind, wird die Anforderung für den Adressdatensatz dieser Domäne gestellt. Eine einzelne Domäne kann mehrere Mail-Exchange-Server haben.

Hinzufügen eines MX-Datensatzes mit der CLI

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

```
1 -  add dns mxRec <domain> -mx <string> -pref <positive_integer> [-TTL <
     secs>]
2 -  show dns mxRec <domain>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add dns mxRec example.com -mx mail.example.com -pref 1
2  Done
3 > show dns mxRec example.com
4 1)      Domain : example.com    MX Name : mail.example.com
5         Preference :   1        TTL : 5 secs
6  Done
7 <!--NeedCopy-->
```

Ändern oder Entfernen eines MX-Datensatzes mit der CLI

- Um einen MX-Record zu ändern, geben Sie den `set dns mxRec` Befehl, den Namen der Domäne, für die der MX-Eintrag konfiguriert ist, den Namen des MX-Records und die zu ändernden Parameter mit ihren neuen Werten ein.
- Um den TTL-Parameter auf seinen Standardwert festzulegen, geben Sie den `unset dns mxRec` Befehl, den Namen der Domäne, für die der MX-Eintrag konfiguriert ist, den Namen des MX-Records und -TTL ohne TTL-Wert ein. Sie können den `unset dns mxRec` Befehl verwenden, um nur den TTL-Parameter aufzuheben.

- Um einen MX-Eintrag zu entfernen, geben Sie den `rm dns mxRec` Befehl, den Namen der Domäne, für die der MX-Eintrag konfiguriert ist, und den Namen des MX-Records ein.

Hinzufügen eines MX-Datensatzes mit der GUI

Navigieren Sie zu **Traffic Management > DNS > Datensätze > Mail Exchange-Datensätze** und erstellen Sie einen MX-Eintrag.

Erstellen von NS-Datensätzen für einen autorisierenden Server

October 5, 2021

NS-Einträge (Name Server) geben den autorisierenden Server für eine Domäne an. Sie können maximal 16 NS-Einträge konfigurieren. Sie können einen NS-Eintrag verwenden, um das Steuerelement einer Subdomäne an einen DNS-Server zu delegieren.

Erstellen eines NS-Datensatzes mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen NS-Datensatz zu erstellen und die Konfiguration zu überprüfen:

```
1 -  add dns nsRec <domain> <nameServer> [-TTL <secs>]
2 -  show dns nsRec <domain>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add dns nsRec example.com nameserver1.example.com
2  Done
3 > show dns nsRec example.com
4 1)      Domain : example.com    NameServer : nameserver1.example.com
5         TTL : 5 sec
6  Done
7 <!--NeedCopy-->
```

Um einen NS-Eintrag zu entfernen, geben Sie den `rm dns nsRec` Befehl, den Namen der Domäne, zu der der NS-Eintrag gehört, und den Namen des Nameservers ein.

Erstellen eines NS-Datensatzes mit der GUI

Navigieren Sie zu **Traffic Management > DNS > Datensätze > Namenserver-Einträge** und erstellen Sie einen NS-Datensatz.

Erstellen von CNAME-Datensätzen für eine Subdomäne

October 5, 2021

Ein kanonischer Namenseintrag (CNAME-Eintrag) ist ein Alias für einen DNS-Namen. Diese Datensätze sind nützlich, wenn mehrere Dienste den DNS-Server abfragen. Der Host mit einem Adressdatensatz (A) kann keinen CNAME-Eintrag haben.

Manchmal fordert eine Citrix ADC Appliance im Proxy-Modus einen Adressdatensatz aus dem Cache anstelle des Servers an.

Hinzufügen eines CNAME-Datensatzes mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen CNAME-Datensatz zu erstellen und die Konfiguration zu überprüfen:

```
-  add dns cnameRec <aliasName> <canonicalName> [-TTL <secs>]
-  show dns cnameRec <aliasName>
<!--NeedCopy-->
```

Beispiel:

```
> add dns cnameRec www.example.com www.examplenw.com
 Done
> show dns cnameRec www.example.com
        Alias Name      Canonical Name  TTL
1)      www.example.com        www.examplenw.com       5 secs
 Done
<!--NeedCopy-->
```

Um einen CNAME-Eintrag für eine bestimmte Domäne zu entfernen, geben Sie den `rm dns cnameRec` Befehl und den Alias des Domänennamens ein.

Hinzufügen eines CNAME-Datensatzes mit der GUI

Navigieren Sie zu **Traffic Management > DNS > Datensätze > Kanonische Datensätze** und erstellen Sie einen CNAME-Datensatz.

CNAME-Einträge zwischenspeichern

Bei der Bereitstellung in einem Proxy-Modus sendet die ADC-Appliance die Abfrage für einen Adressdatensatz nicht immer an den Back-End-Server. Dieses Verhalten tritt auf, wenn für eine Antwort auf eine Abfrage nach einem Adressdatensatz eine partielle CNAME-Kette im Cache vorhanden ist. Es gibt nur wenige Bedingungen, unter denen der ADC den partiellen CNAME-Datensatz zwischenspeichert und die Abfrage aus dem Cache dient. Im Folgenden sind die Bedingungen:

- Citrix ADC muss in einem Proxy-Modus bereitgestellt werden.
- Die Antwort vom Back-End-Server muss eine CNAME-Kette haben, für die der Datensatztyp des letzten Eintrags im Antwortbereich ein CNAME und der Fragetyp kein CNAME sein muss.
- Die Antwort des Backend-Servers kann keine No-Data oder NX-Domain sein.
- Die Antwort des Back-End-Servers muss eine autorisierende Antwort sein.

Erstellen von NAPTR-Datensätzen für Telekommunikationsdomäne

October 5, 2021

NAPTR (Naming Address Pointer) ist einer der am häufigsten verwendeten DNS-Einträge im Telekommunikationsbereich. NAPTR-Datensätze ordnen den Internet-Telefonieadressraum dem Internetadressraum zu. Sie ermöglichen es einem mobilen Gerät, eine Anfrage an den richtigen Server zu senden. Die Kombination von NAPTR-Datensätzen mit Service Records (SRV) ermöglicht die Verkettung mehrerer Datensätze zu komplexen Rewrite-Regeln, die neue Domänenlabels oder Uniform Resource Identifiers (URIs) erzeugen. Der DNS-Code für NAPTR ist 35.

Citrix ADCs unterstützen NAPTR in zwei Modi: ADNS-Modus und Proxy-Modus. Im Proxymodus speichert der ADC die Antwort von den Servern und verwendet die zwischengespeicherten Datensätze, um zukünftige Abfragen zu serveren. Für eine bestimmte Domäne in Citrix ADC können maximal 20 NAPTR-Einträge hinzugefügt werden. Citrix ADC speichert die Antwort auf eine DNS-NAPTR-Datensatzabfrage. Alle nachfolgenden Anfragen für den NAPTR Record werden aus dem Cache bedient.

Erstellen eines NAPTR-Datensatzes mithilfe von CLI

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


```
add dns naptrRec <order> <preference>[flags<string>][services<string>](
regexp<expressions>|-replacement<string>)[-TTL<secs>]
```

Entfernen eines NAPTR-Datensatzes mithilfe von CLU

```
rm dns naptrRec<domain> (<order> <preference> [-flags <string>] [-services
 <string>] (-regexp <expression> | -replacement <string>))| -recordId <
positive_integer>@)
```

Konfigurieren eines NAPTR-Datensatzes mit GUI

Navigieren Sie zu **Traffic Management > DNS > Datensätze > NAPTR Records** und erstellen Sie einen NAPTR Record.

Erstellen von PTR-Datensätzen für IPv4- und IPv6-Adressen

October 5, 2021

Ein Zeigerdatensatz (PTR) übersetzt eine IP-Adresse in den Domänennamen. IPv4-PTR-Datensätze werden durch die Oktette einer IP-Adresse in umgekehrter Reihenfolge mit der Zeichenfolge in-addr.arpa dargestellt. am Ende angehängt. Beispielsweise ist der PTR-Eintrag für die IP-Adresse 1.2.3.4 4.3.2.1.in-addr.arpa.

IPv6-Adressen werden in umgekehrter Reihenfolge unter der Domäne IP6.ARPA zugeordnet. IPv6 Reverse-Maps verwenden eine Folge von Nibbles, die durch Punkte getrennt sind, mit dem Suffix .IP6.ARPA, wie in RFC 3596 definiert. Der Reverse-Lookup-Domänenname, der der Adresse 4321:0:1:2:3:4:567:89ab wäre z. B. b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.ARPA.

Hinzufügen eines PTR-Datensatzes mit der CLI

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

```
1 -  add dns ptrRec <reverseDomain> <domain> [-TTL <secs>]
2 -  show dns ptrRec <reverseDomain>
3 <!--NeedCopy-->
```

Beispiel:


```
> add dns ptrRec 0.2.0.192.in-addr.arpa example.com
 Done
> show dns ptrRec 0.2.0.192.in-addr.arpa
1)      Reverse Domain Name : 0.2.0.192.in-addr.arpa
        Domain Name : example.com               TTL : 3600 secs
 Done
<!--NeedCopy-->
```

Um einen PTR-Eintrag zu entfernen, geben Sie den `rm dns ptrRec` Befehl und den Namen der umgekehrten Domäne ein, der dem PTR-Datensatz zugeordnet ist.

Hinzufügen eines PTR-Datensatzes mit der GUI

Navigieren Sie zu **Traffic Management > DNS > Datensätze > PTR-Datensätze** und erstellen Sie einen PTR-Datensatz.

Erstellen von SOA-Datensätzen für autorisierende Informationen

October 5, 2021

Ein SOA-Eintrag (Start of Authority) wird nur an der Zonenspitze erstellt und enthält Informationen über die Zone. Der Datensatz enthält unter anderem den primären Nameserver, Kontaktinformationen (E-Mail) und standardmäßige (Mindest-) Time-to-Live-Werte (TTL) für Datensätze.

Erstellen eines SOA-Datensatzes mit der CLI

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

```
-  add dns soaRec <domain> -originServer <originServerName> -contact <
    contactName>
-  sh dns soaRec <do main>
<!--NeedCopy-->
```

Beispiel:

```
> add dns soaRec example.com -originServer nameserver1.example.com -
    contact admin.example.com
```



```
 Done
> show dns soaRec example.com
1)      Domain Name : example.com
        Origin Server : nameserver1.example.com
        Contact : admin.example.com
        Serial No. : 100        Refresh : 3600 secs     Retry : 3 secs
        Expire : 3600 secs      Minimum : 5 secs        TTL : 3600 secs
 Done
<!--NeedCopy-->
```

Ändern oder Entfernen eines SOA-Datensatzes mit der CLI

- Um einen SOA-Eintrag zu ändern, geben Sie den`set dns soaRec` Befehl, den Namen der Domäne, für die der Datensatz konfiguriert ist, und die zu ändernden Parameter mit den neuen Werten ein.
- Um einen SOA-Eintrag zu entfernen, geben Sie den`rm dns soaRec` Befehl und den Namen der Domäne ein, für die der Datensatz konfiguriert ist.

Konfigurieren eines SOA-Datensatzes mit der GUI

Navigieren Sie zu **Traffic Management > DNS > Records > SOA-Einträge** und erstellen Sie einen SOA-Eintrag.

Erstellen von TXT-Datensätzen zum Halten von beschreibendem Text

October 5, 2021

Domain-Hosts speichern TXT-Einträge zu informativen Zwecken. Die RDATA-Komponente eines TXT-Records, die aus einer oder mehreren Zeichenketten variabler Länge besteht, kann praktisch alle Informationen speichern, die ein Empfänger möglicherweise über die Domäne wissen muss. Es kann auch Informationen über den Dienstanbieter, den Ansprechpartner, E-Mail-Adressen und zugehörige Details enthalten. Der SPF-Schutz (Sender Policy Framework) war der wichtigste Anwendungsfall für den TXT-Eintrag.

Alle Konfigurationstypen (autorisierende DNS, DNS-Proxy, Endauflöser und Weiterleitungskonfigurationen) auf der Citrix ADC Appliance unterstützen TXT-Einträge. Sie können einer Domäne maximal 20 TXT-Ressourceneinträge hinzufügen. Jeder Ressourceneintrag wird mit einer eindeutigen, intern generierten Datensatzkennung gespeichert. Sie können die ID eines Datensatzes anzeigen und damit den Datensatz löschen. Sie können jedoch keinen TXT-Ressourceneintrag ändern.

Erstellen eines TXT-Ressourceneintrags mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen TXT-Ressourceneintrag zu erstellen und die Konfiguration zu überprüfen:

```
1 -  add dns txtRec <domain> <string> ... [-TTL <secs>]
2 -  show dns txtRec [<domain> | -type <type>]
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add dns txtRec www.example.com ”Contact: Mark” ”Email: mark@example.
     com” -TTL 36000
2  Done
3 > show dns txtRec www.example.com
4 1)  Domain : www.example.com    Record id: 13783       TTL : 36000 secs
      Record Type : ADNS
5         ”Contact: Mark”
6         ”Email: mark@example.com”
7  Done
8 <!--NeedCopy-->
```

Entfernen eines TXT-Ressourceneintrags mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen TXT-Ressourceneintrag zu entfernen und die Konfiguration zu überprüfen:

```
1 -  rm dns txtRec <domain> (<string> ... | -recordId <positive_integer>)
2 -  show dns txtRec [<domain> | -type <type>]
3 <!--NeedCopy-->
```

Beispiel:

Sie können den `show dns txtRec` Befehl zuerst verwenden, um die Datensatz-ID des TXT-Ressourceneintrags anzuzeigen, den Sie entfernen möchten, wie hier gezeigt:

```
1 > show dns txtRec www.example.com
2 1)  Domain : www.example.com    Record id: 36865       TTL : 36000 secs
      Record Type : ADNS
```



```
        ”Contact: Evan”
        ”Email: evan@example.com”
2)  Domain : www.example.com    Record id: 14373       TTL : 36000 secs
    Record Type : ADNS
        ”Contact: Mark”
        ”Email: mark1@example.com”
 Done
<!--NeedCopy-->
```

Die einfachere Methode zum Löschen eines TXT-Datensatzes besteht darin, die Datensatz-ID zu verwenden. Wenn Sie die Zeichenfolgen angeben möchten, geben Sie sie in der Reihenfolge ein, in der sie im Datensatz gespeichert sind. Im folgenden Beispiel wird der TXT-Datensatz mit seiner Datensatz-ID gelöscht.

```
>rm dns txtRec www.example.com -recordID 36865
 Done
> show dns txtRec www.example.com
1)  Domain : www.example.com    Record id: 14373       TTL : 36000 secs
    Record Type : ADNS
        ”Contact: Mark”
        ”Email: mark1@example.com”
 Done
<!--NeedCopy-->
```

Konfigurieren eines TXT-Datensatzes mit der GUI

Navigieren Sie zu **Traffic Management > DNS > Records > TXT Records** und erstellen Sie einen TXT-Eintrag.

DNS-Statistiken anzeigen

October 5, 2021

Sie können die von der Citrix ADC Appliance generierten DNS-Statistiken anzeigen. Die DNS-Statistiken umfassen Laufzeit-, Konfigurations- und Fehlerstatistiken.

Anzeigen von DNS-Datensatzstatistiken mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
stat dns
```

Beispiel:

```
> stat dns
DNS Statistics

Runtime Statistics
Dns queries                             21
NS queries                               8
SOA queries                             18
.
.
.
Configuration Statistics
AAAA records                            17
A records                               36
MX records                               9
.
.
.
Error Statistics
Nonexistent domain                      17
No AAAA records                          0
No A records                            13
.
.
.
Done
<!--NeedCopy-->
```

Anzeigen von DNS-Datensatzstatistiken mit der GUI

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Klicken Sie im Detailbereich auf **Statistiken**.

Konfigurieren einer DNS-Zone

October 5, 2021

Eine DNS-Zonenentität auf der Citrix ADC Appliance erleichtert den Besitz einer Domäne auf der Appliance. Mit einer Zone auf der Appliance können Sie auch DNS-Sicherheitserweiterungen (DNSSEC) für die Zone implementieren oder die DNSSEC-Vorgänge der Zone von den DNS-Servern auf die Appliance auslagern. DNSSEC-Zeichenvorgänge werden für alle Ressourceneinträge in einer DNS-Zone ausgeführt. Wenn Sie eine Zone signieren oder DNSSEC-Vorgänge für eine Zone auslagern möchten, müssen Sie daher zuerst die Zone auf der Citrix ADC Appliance erstellen.

Erstellen Sie in den folgenden Szenarien eine DNS-Zone auf der Appliance:

- Die Citrix ADC Appliance besitzt alle Datensätze in einer Zone, d. h. die Appliance fungiert als autorisierender DNS-Server für die Zone. Die Zone muss mit dem ProxyMode-Parameter auf NO erstellt werden.
- Die Citrix ADC Appliance besitzt nur eine Teilmenge der Datensätze in einer Zone. Alle anderen Ressourceneinträge in der Zone werden auf einer Reihe von Backend-Nameservern gehostet. Die Appliance ist als DNS-Proxyserver für diese Backend-Server konfiguriert. Eine typische Konfiguration, bei der die Citrix ADC Appliance nur eine Teilmenge der Ressourceneinträge in der Zone besitzt, ist eine GSLB-Konfiguration (Global Server Load Balancing). Die Citrix ADC Appliance besitzt nur die GSLB-Domänennamen, während die Back-End-Nameserver alle anderen Datensätze besitzen. Die Zone muss mit dem ProxyMode-Parameter auf YES erstellt werden.
- Sie möchten DNSSEC-Vorgänge für eine Zone von Ihren autorisierenden DNS-Servern auf die Appliance auslagern. Die Zone muss mit dem ProxyMode-Parameter auf YES erstellt werden. Möglicherweise müssen Sie weitere Einstellungen für die Zone konfigurieren.

Im aktuellen Thema wird beschrieben, wie eine Zone für die ersten beiden Szenarien erstellt wird. Weitere Informationen zum Konfigurieren einer Zone zum Auslagern von DNSSEC-Vorgängen auf die Appliance finden Sie unter Auslagern von DNSSEC-Vorgängen auf die Citrix ADC Appliance.

> **Hinweis:**
>
> Wenn die ADC-Appliance als autorisierender DNS-Server für eine Zone arbeitet, müssen Sie die Einträge Start of Authority (SOA) und Namenserver (NS) für die Zone erstellen, bevor Sie die Zone erstellen. Wenn Citrix ADC als DNS-Proxyserver für eine Zone arbeitet, dürfen SOA- und NS-Einträge auf der Citrix ADC Appliance nicht erstellt werden. Weitere Informationen zum Erstellen von SOA- und NS-Datensätzen finden Sie unter Konfigurieren von DNS-Ressourceneinträgen.

Wenn Sie eine Zone erstellen, werden alle vorhandenen Domänennamen und Ressourceneinträge, die mit dem Namen der Zone enden, automatisch als Teil der Zone behandelt. Außerdem werden alle neuen Ressourceneinträge, die mit einem Suffix erstellt wurden, das dem Namen der Zone entspricht, implizit in die Zone aufgenommen.

Erstellen einer DNS-Zone auf der Citrix ADC Appliance mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um der Citrix ADC Appliance eine DNS-Zone hinzuzufügen und die Konfiguration zu überprüfen:


```
-  add dns zone <zoneName> -proxyMode ( YES | NO )
-  show dns zone [<zoneName> | -type <type>]
<!--NeedCopy-->
```

Beispiel:

```
> add dns zone example.com -proxyMode Yes
 Done
> show dns zone example.com
          Zone Name : example.com
          Proxy Mode : YES
Done
<!--NeedCopy-->
```

Ändern oder Entfernen einer DNS-Zone mit der CLI

- Um eine DNS-Zone zu ändern, geben Sie den`set dns zone` Befehl, den Namen der DNS-Zone und die zu ändernden Parameter mit ihren neuen Werten ein.
- Um eine DNS-Zone zu entfernen, geben Sie den `rm dns zone` Befehl und den Namen der DNS-Zone ein.

Konfigurieren einer DNS-Zone mit der GUI

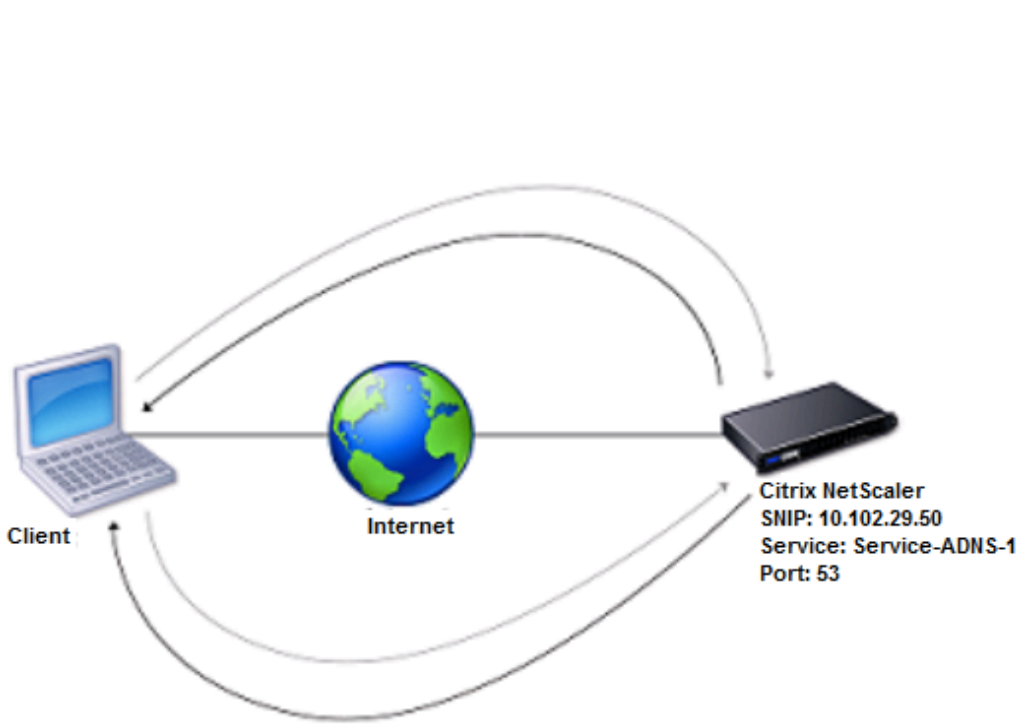
Navigieren Sie zu **Traffic Management > DNS > Zones** und erstellen Sie eine DNS-Zone.

Konfigurieren des Citrix ADC als ADNS-Server

October 5, 2021

Sie können die ADC-Appliance so konfigurieren, dass sie als autorisierender Domain Name Server (ADNS) für eine Domäne fungiert. Als ADNS-Server für eine Domäne löst Citrix ADC DNS-Anforderungen für alle Typen von DNS-Einträgen, die zur Domäne gehören. Um Citrix ADC so zu konfigurieren, dass sie als ADNS-Server für eine Domäne fungiert, müssen Sie einen ADNS-Dienst erstellen und NS- und Adressdatensätze für die Domäne auf dem Citrix ADC konfigurieren. Der ADNS-Dienst kann mit der Subnetz-IP-Adresse (SNIP) oder einer separaten IP-Adresse konfiguriert werden. Das folgende Topologiediagramm zeigt eine Beispielkonfiguration und den Ablauf von Anforderungen und Antworten.

Abbildung 1. Citrix ADC als ADNS



Die folgende Tabelle zeigt die Parameter, die für den ADNS-Dienst konfiguriert sind, wie im vorhergehenden Topologiediagramm dargestellt.

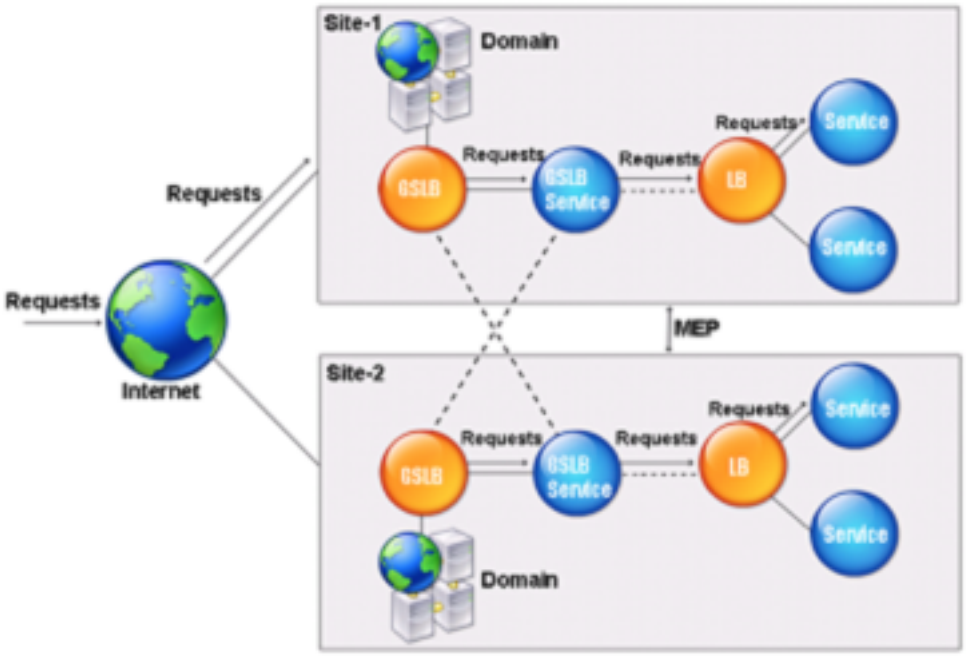
Entitätstyp	Name	IP-Adresse	Typ	Port
ADNS-Dienst	Service-ADNS-1	10.102.29.51	ADNS	53

Tabelle 1. Beispiel für die Konfiguration des ADNS-Dienstes

Um ein ADNS-Setup zu konfigurieren, müssen Sie den ADNS-Dienst konfigurieren. Anweisungen zum Konfigurieren des ADNS-Dienstes finden Sie unter Lastenausgleich.

Während der DNS-Auflösung leitet der ADNS-Server den DNS-Proxy oder lokalen DNS-Server an, den Citrix ADC nach der IP-Adresse der Domäne abzufragen. Da Citrix ADC autorisierend für die Domäne ist, wird die IP-Adresse an den DNS-Proxy oder den lokalen DNS-Server gesendet. Das folgende Diagramm beschreibt die Platzierung und Rolle des ADNS-Servers in einer GSLB-Konfiguration.

Abbildung 2. GSLB-Entitätsmodell



Hinweis: Wenn Sie im ADNS-Modus SOA- und ADNS-Datensätze entfernen, funktioniert Folgendes nicht für die Domäne, die von der Citrix ADC: ANY-Abfrage gehostet wird (weitere Informationen zur ANY-Abfrage finden Sie unter DNS ANY-Abfrage) und negative Antworten wie NODATA und NXDOMAIN.

Erstellen eines ADNS-Dienstes

Ein ADNS-Dienst wird für den globalen Lastausgleich von Diensten verwendet. Weitere Informationen zum Erstellen eines GSLB-Setups finden Sie unter Globaler Server-Lastenausgleich. Sie können einen ADNS-Dienst hinzufügen, ändern, aktivieren, deaktivieren und entfernen. Anweisungen zum Erstellen eines ADNS-Dienstes finden Sie unter Konfigurieren von Diensten.

Hinweis: Sie können den ADNS-Dienst so konfigurieren, dass er SNIP oder eine neue IP-Adresse verwendet.

Wenn Sie einen ADNS-Dienst erstellen, antwortet Citrix ADC auf DNS-Abfragen auf der konfigurierten ADNS-Dienst-IP und -Port.

Sie können die Konfiguration überprüfen, indem Sie die Eigenschaften des ADNS-Dienstes anzeigen. Sie können Eigenschaften wie Name, Status, IP-Adresse, Port, Protokoll und maximale Clientverbindungen anzeigen.

Konfigurieren des ADNS-Setups für die Verwendung von TCP

Standardmäßig verwenden einige Clients das User Datagram Protocol (UDP) für DNS, das eine Grenze von 512 Byte für die Nutzlastlänge von UDP-Paketen angibt. Um Nutzlasten mit einer Größe von mehr als 512 Byte zu handhaben, muss der Client TCP verwenden. Um die DNS-Kommunikation über TCP zu aktivieren, müssen Sie die Citrix ADC Appliance so konfigurieren, dass das TCP-Protokoll für DNS verwendet wird. Der Citrix ADC legt dann das Kürzungsbit in den DNS-Antwortpaketen fest. Das Kürzungsbit gibt an, dass die Antwort für UDP zu groß ist und dass der Client die Anforderung über eine TCP-Verbindung senden muss. Der Client verwendet dann das TCP-Protokoll auf Port 53 und öffnet eine neue Verbindung zum Citrix ADC. Citrix ADC überwacht Port 53 mit der IP-Adresse des ADNS-Dienstes, um die neuen TCP-Verbindungen vom Client zu akzeptieren.

Um Citrix ADC für die Verwendung des TCP-Protokolls zu konfigurieren, müssen Sie einen ADNS_TCP-Dienst konfigurieren. Anweisungen zum Erstellen eines ADNS_TCP-Dienstes finden Sie unter Lastenausgleich.

> **Wichtig**
>
> Um Citrix ADC für die Verwendung von UDP für DNS zu konfigurieren und TCP nur zu verwenden, wenn die Nutzlastlänge von UDP 512 Byte überschreitet, müssen Sie die Dienste ADNS und ADNS_TCP konfigurieren. Die IP-Adresse des ADNS_TCP-Dienstes muss mit der IP-Adresse des ADNS-Dienstes übereinstimmen.

Hinzufügen von DNS-Ressourceneinträgen

Nachdem Sie einen ADNS-Dienst erstellt haben, können Sie DNS-Einträge hinzufügen. Anweisungen zum Hinzufügen von DNS-Datensätzen finden Sie unter Konfigurieren von DNS-Ressourceneinträgen.

ADNS-Dienste entfernen

Anweisungen zum Entfernen von Diensten finden Sie unter Lastenausgleich

Konfigurieren der Domänendelegierung

Domänendelegierung ist der Prozess der Zuweisung der Zuständigkeit für einen Teil des Domänenraums zu einem anderen Nameserver. Daher wird während der Domänendelegierung die Verantwortung für die Antwort auf die Abfrage an einen anderen DNS-Server delegiert. Delegierung verwendet NS-Datensätze.

Im folgenden Beispiel ist sub1.abc.com die Subdomain für abc.com. Das Verfahren beschreibt die Schritte zum Delegieren der Subdomäne an den Nameserver ns2.sub1.abc.com und Hinzufügen eines Adressdatensatzes für ns2.sub1.abc.com.

Um die Domänendelegierung zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen, die in den folgenden Abschnitten beschrieben werden:

1. Erstellen Sie einen SOA-Eintrag für eine Domäne.
2. Erstellen Sie einen NS-Eintrag, um einen Nameserver für die Domäne hinzuzufügen.
3. Erstellen Sie einen Adressdatensatz für den Nameserver.
4. Erstellen Sie einen NS-Datensatz, um die Subdomäne zu delegieren.
5. Erstellen Sie einen Klebedatensatz für den Nameserver.

Erstellen eines SOA-Datensatzes

Anweisungen zum Konfigurieren von SOA-Datensätzen finden Sie unter Erstellen von SOA-Datensätzen für autoritative Informationen.

Erstellen eines NS-Datensatzes für einen Nameserver

Anweisungen zum Konfigurieren eines NS-Datensatzes finden Sie unter Erstellen von NS-Datensätzen für einen autoritativen Server. Wählen Sie in der Liste **Namensserver** den primären autoritativen Nameserver aus, z. B. ns1.abc.com.

Erstellen eines Adressdatensatzes

Anweisungen zum Konfigurieren von Adressdatensätzen finden Sie unter Erstellen von Adressdatensätzen für einen Domainnamen. Geben Sie in die Textfelder Hostname und IP-Adresse den Domänennamen für den DNS-Adressdatensatz und die IP-Adresse ein, z. B. ns1.abc.com bzw. 10.102.11.135.

Erstellen eines NS-Datensatzes für die Domänendelegierung

Anweisungen zum Konfigurieren von NS-Datensätzen finden Sie unter Erstellen von NS-Datensätzen für einen autoritativen Server. Wählen Sie in der Liste **Name Server** den primären autoritativen Nameserver aus, z. B. ns2.sub1.abc.com.

Erstellen eines Leimdatensatzes

NS-Einträge werden in der Regel unmittelbar nach dem SOA-Eintrag definiert (keine Einschränkung). Eine Domain muss mindestens zwei NS-Einträge haben. Wenn ein NS-Eintrag innerhalb einer Domäne definiert ist, muss er über einen übereinstimmenden Adressdatensatz verfügen. Dieser Adressdatensatz wird als Klebedatensatz bezeichnet. Glue-Datensätze beschleunigen DNS-Abfragen.

Anweisungen zum Hinzufügen von Glue-Datensätzen für eine Subdomain finden Sie im Verfahren zum Hinzufügen eines Address (A) -Datensatzes unter Konfigurieren von DNS-Ressourceneinträgen.

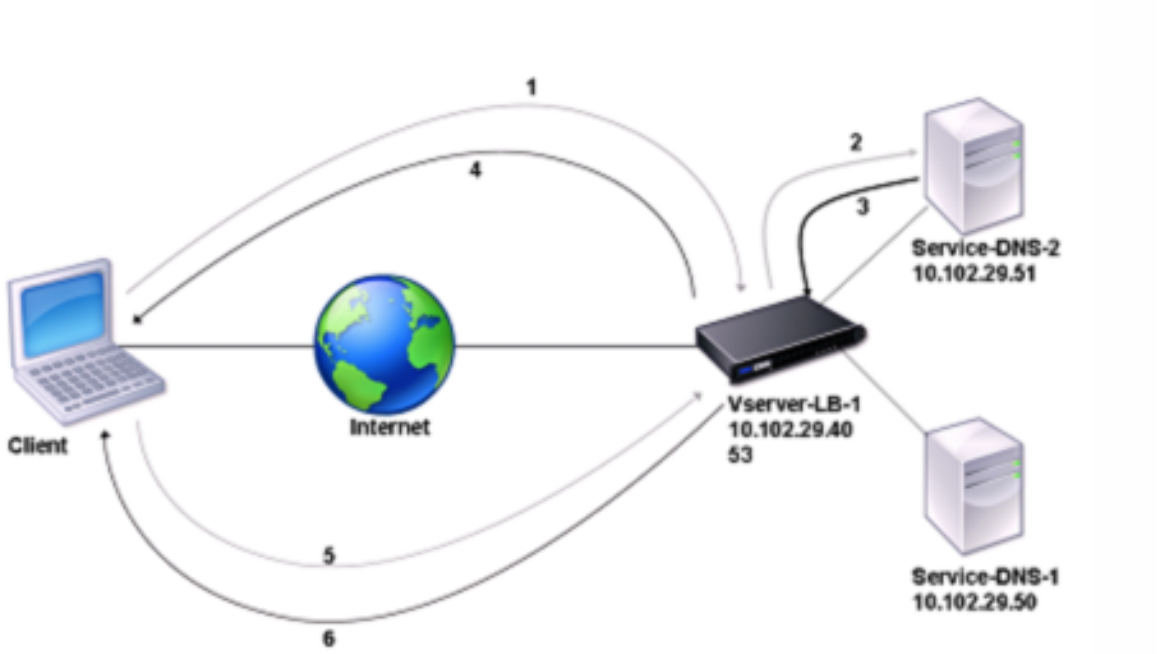
Anweisungen zum Konfigurieren von Adressdatensätzen finden Sie unter Erstellen von Adressdatensätzen für einen Domainnamen. Geben Sie in die Textfelder Hostname und IP-Adresse den Domänennamen für den DNS-Adressdatensatz und die IP-Adresse ein, z. B. ns2.sub1.abc.com bzw. 10.102.12.135.

Konfigurieren der Citrix ADC Appliance als DNS-Proxyserver

October 5, 2021

Als DNS-Proxyserver kann die ADC-Appliance als Proxy für einen einzelnen DNS-Server oder eine Gruppe von DNS-Servern fungieren. Der Ablauf von Anforderungen und Antworten wird im folgenden Beispieltopologiediagramm veranschaulicht.

Abbildung 1. Citrix ADC als DNS-Proxy



Standardmäßig speichert die Citrix ADC Appliance Antworten von DNS-Nameservern. Wenn die Appliance eine DNS-Abfrage empfängt, sucht sie in ihrem Cache nach der abgefragten Domäne. Wenn die Adresse der abgefragten Domäne im Cache vorhanden ist, gibt der Citrix ADC die entsprechende Adresse an den Client zurück. Andernfalls wird die Abfrage an einen DNS-Nameserver weitergeleitet, der die Verfügbarkeit der Adresse prüft und an den Citrix ADC zurückgibt. Der Citrix ADC gibt dann die Adresse an den Client zurück.

Bei Anforderungen für eine zuvor zwischengespeicherte Domäne dient Citrix ADC den Adressdatensatz der Domäne aus dem Cache, ohne den konfigurierten DNS-Server abzufragen.

Die Appliance verwirft einen im Cache gespeicherten Datensatz, wenn der TTL-Wert (Time-to-Live) des Datensatzes den konfigurierten Wert erreicht. Ein Client, der einen abgelaufenen Datensatz anfordert, muss warten, bis der Citrix ADC den Datensatz vom Server abruft und seinen Cache aktualisiert. Um diese Verzögerung zu vermeiden, aktualisiert Citrix ADC den Cache proaktiv, indem er den Datensatz vom Server abruft, bevor der Datensatz abläuft.

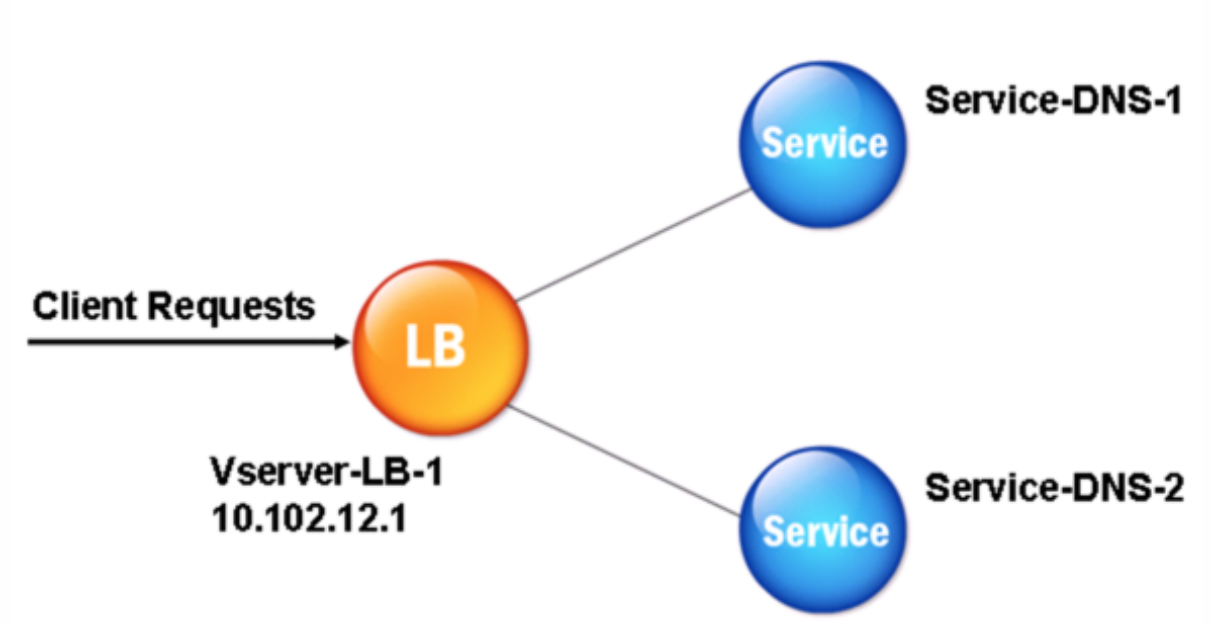
In der folgenden Tabelle sind Beispielnamen und Werte der Entitäten aufgeführt, die auf dem Citrix ADC konfiguriert werden müssen.

Tabelle 1. Beispiel für die Konfiguration der DNS-Proxy-Entitäten

Entitätstyp	Name	IP-Adresse	Typ	Port
Virtueller LB-Server	Vserver-DNS-1	10.102.29.40	DNS	53
Services	Service-DNS-1	10.102.29.50	DNS	53
Services	Service-DNS-2	10.102.29.51	DNS	53

Das folgende Diagramm zeigt die Entitäten eines DNS-Proxy und die Werte der Parameter, die auf dem Citrix ADC konfiguriert werden sollen.

Abbildung 2. DNS-Proxy-Entitätsmodell



> **Hinweis:**
>
> Um die DNS-Proxy-Funktion zu konfigurieren, müssen Sie wissen, wie Sie Load Balancing-

> Dienste und virtuelle Server konfigurieren.

Erstellen eines virtuellen Lastausgleichsservers

Um einen DNS-Proxy auf dem Citrix ADC zu konfigurieren, konfigurieren Sie einen virtuellen Lastausgleichsserver vom Typ DNS. Um einen virtuellen DNS-Server für den Lastenausgleich einer Gruppe von DNS-Servern zu konfigurieren, die rekursive Abfragen unterstützen, müssen Sie die Option Rekursion verfügbar festlegen. Mit dieser Option wird das RA-Bit in den DNS-Antworten vom virtuellen DNS-Server auf ON gesetzt.

Anweisungen zum Erstellen eines virtuellen Lastenausgleichsservers finden Sie unter Load Balancing.

Erstellen von DNS-Diensten

Nachdem Sie einen virtuellen Lastausgleichsserver vom Typ DNS erstellt haben, müssen Sie DNS-Dienste erstellen. Sie können einen DNS-Dienst hinzufügen, ändern, aktivieren, deaktivieren und entfernen. Anweisungen zum Erstellen eines DNS-Dienstes finden Sie unter Load Balancing.

Binden eines virtuellen Lastausgleichsservers an DNS-Dienste

Um die DNS-Proxykonfiguration abzuschließen, müssen Sie die DNS-Dienste an den virtuellen Lastausgleichsserver binden. Anweisungen zum Binden eines Dienstes an einen virtuellen Lastausgleichsserver finden Sie unter Load Balancing.

Konfigurieren des DNS-Proxy-Setups für die Verwendung von TCP

Einige Clients verwenden das User Datagram Protocol (UDP) für die DNS-Kommunikation. UDP gibt jedoch eine maximale Paketgröße von 512 Byte an. Wenn die Nutzlastlängen 512 Byte überschreiten, muss der Client TCP verwenden. Wenn ein Client der Citrix ADC Appliance eine DNS-Abfrage sendet, leitet die Appliance die Abfrage an einen der Nameserver weiter. Wenn die Antwort für ein UDP-Paket zu groß ist, legt der Nameserver das Abkürzungsbit in seiner Antwort auf das Citrix ADC fest. Das Kürzungsbit zeigt an, dass die Antwort für UDP zu groß ist und dass der Client die Abfrage über eine TCP-Verbindung senden muss. Die ADC-Appliance gibt die Antwort an den Client weiter, wobei das Kürzungsbit intakt ist. Es wartet darauf, dass der Client eine TCP-Verbindung mit der IP-Adresse des virtuellen DNS-Lastausgleichsservers auf Port 53 initiiert. Der Client sendet die Anforderung über eine TCP-Verbindung. Die Citrix ADC Appliance leitet die Anforderung dann an den Nameserver weiter und leitet die Antwort an den Client weiter.

Um Citrix ADC für die Verwendung des TCP-Protokolls für DNS zu konfigurieren, müssen Sie einen virtuellen Lastausgleichsserver und Dienste vom Typ DNS_TCP konfigurieren. Sie können Monitore

vom Typ DNS_TCP konfigurieren, um den Status der Dienste zu überprüfen. Anweisungen zum Erstellen virtueller Server, Dienste und Monitore von DNS_TCP finden Sie unter Load Balancing.

Um die Datensätze proaktiv zu aktualisieren, verwendet Citrix ADC eine TCP-Verbindung zum Server, um die Datensätze abzurufen.

> **Wichtig**
>
> Um den Citrix ADC so zu konfigurieren, dass er UDP für DNS verwendet und TCP nur verwendet, wenn die Nutzlastlänge von UDP 512 Byte überschreitet, müssen Sie sowohl DNS- als auch DNS_TCP-Dienste konfigurieren. Die IP-Adresse des DNS_TCP-Dienstes muss mit der IP-Adresse des DNS-Dienstes übereinstimmen.

Konfigurieren von Time-to-live-Werten für DNS-Einträge

Die TTL ist für alle DNS-Einträge mit demselben Domänennamen und demselben Datensatztyp identisch. Wenn der TTL-Wert für einen der Datensätze geändert wird, wird der neue Wert in allen Datensätzen mit demselben Domänennamen und demselben Typ wiedergegeben. Der Standardwert TTL ist 3600 Sekunden. Das Minimum ist 0, und das Maximum ist 604800. Wenn ein DNS-Eintrag einen TTL-Wert kleiner als das Minimum oder größer als das Maximum aufweist, wird er als minimaler bzw. maximaler TTL-Wert gespeichert.

Geben Sie die minimale und maximale TTL mit der CLI an

Geben Sie an der Citrix ADC Eingabeaufforderung die folgenden Befehle ein, um die minimale und maximale TTL anzugeben, und überprüfen Sie die Konfiguration:

```
-  set dns parameter [-minTTL <secs>] [-maxTTL <secs>]
-  show dns parameter
<!--NeedCopy-->
```

Beispiel:

```
> set dns parameter -minTTL 1200 -maxTTL 1800
 Done
> show dns parameter
        DNS parameters:
        DNS retries: 5
        Minimum TTL: 1200               Maximum TTL: 1800
            .
            .
```



```
9                .
10  Done
11 >
12 <!--NeedCopy-->
```

Geben Sie die minimale und maximale TTL mit der GUI an

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Klicken Sie im Detailbereich unter Einstellungen auf DNS-Einstellungen ändern.
3. Geben Sie im Dialogfeld DNS-Parameter konfigurieren in TTL in die Textfelder Minimum und Maximum die minimale bzw. maximale Livezeit (in Sekunden) ein, und klicken Sie dann auf OK.

Hinweis: Wenn die TTL abläuft, wird der Datensatz aus dem Cache gelöscht. Citrix ADC kontaktiert proaktiv die Server und ruft den DNS-Eintrag kurz vor Ablauf des DNS-Eintrags ab.

DNS-Einträge leeren

Sie können alle DNS-Einträge löschen, die im Cache vorhanden sind. Beispielsweise können Sie DNS-Einträge leeren, wenn ein Server nach Änderungen neu gestartet wird.

Löschen aller Proxydatensätze mit der CLI

Geben Sie an der Citrix ADC Eingabeaufforderung Folgendes ein:

```
flush dns proxyRecords
```

Löschen aller Proxydatensätze mit der GUI

1. Navigieren Sie zu **Traffic Management > DNS > Datensätze**.
2. Klicken Sie im Detailbereich auf “ Proxy-Datensätze leeren”.

Hinzufügen von DNS-Ressourceneinträgen

Sie können DNS-Einträge zu einer Domäne hinzufügen, für die die Citrix ADC Appliance als DNS-Proxyserver konfiguriert ist. Informationen zum Hinzufügen von DNS-Datensätzen finden Sie unter Konfigurieren von DNS-Ressourceneinträgen.

Entfernen eines virtuellen DNS-Servers für Lastenausgleich

Informationen zum Entfernen eines virtuellen Lastenausgleichsservers finden Sie unter Load Balancing.

Begrenzen der Anzahl gleichzeitiger DNS-Anforderungen für eine Clientverbindung

Sie können die Anzahl gleichzeitiger DNS-Anforderungen für eine einzelne Clientverbindung begrenzen, die durch das <clientip:port>-<vserver ip:port> Tupel identifiziert wird. Gleichzeitige DNS-Anforderungen sind die Anforderungen, die die Citrix ADC Appliance an die Nameserver weitergeleitet hat und für die die Appliance Antworten erwartet. Durch die Begrenzung der Anzahl gleichzeitiger Anforderungen für eine Clientverbindung können Sie die Nameserver schützen, wenn ein feindseliger Client einen DDoS-Angriff (Distributed Denial of Service) versucht, indem er eine Flut von DNS-Anforderungen sendet. Wenn das Limit für eine Clientverbindung erreicht ist, werden nachfolgende DNS-Anfragen für die Verbindung gelöscht, bis die Anzahl der ausstehenden Anfragen unter das Limit fällt. Dieses Limit gilt nicht für die Anforderungen, die die Citrix ADC Appliance außerhalb des Caches bereitstellt.

Der Standardwert für diesen Parameter ist 255. Dieser Standardwert ist in den meisten Szenarien ausreichend. Wenn die Nameserver viele gleichzeitige DNS-Anforderungen unter normalen Betriebsbedingungen bedienen, können Sie entweder einen großen Wert oder einen Wert von Null (0) angeben. Der Wert 0 deaktiviert dieses Feature und gibt an, dass es keine Begrenzung für die Anzahl der DNS-Anforderungen gibt, die für eine einzelne Clientverbindung zulässig sind. Dieser Parameter ist ein globaler Parameter und gilt für alle virtuellen DNS-Server, die auf der Citrix ADC Appliance konfiguriert sind.
Der Standardwert für diesen Parameter ist 255. Dieser Standardwert ist in den meisten Szenarien ausreichend. Wenn die Nameserver viele gleichzeitige DNS-Anforderungen unter normalen Betriebsbedingungen bedienen, können Sie entweder einen großen Wert oder einen Wert von Null (0) angeben. Der Wert 0 deaktiviert dieses Feature und gibt an, dass es keine Begrenzung für die Anzahl der DNS-Anforderungen gibt, die für eine einzelne Clientverbindung zulässig sind. Dieser Parameter ist ein globaler Parameter und gilt für alle virtuellen DNS-Server, die auf der Citrix ADC Appliance konfiguriert sind.
Der Standardwert für diesen Parameter ist 255. Dieser Standardwert ist in den meisten Szenarien ausreichend. Wenn die Nameserver viele gleichzeitige DNS-Anforderungen unter normalen Betriebsbedingungen bedienen, können Sie entweder einen großen Wert oder einen Wert von Null (0) angeben. Der Wert 0 deaktiviert dieses Feature und gibt an, dass es keine Begrenzung für die Anzahl der DNS-Anforderungen gibt, die für eine einzelne Clientverbindung zulässig sind. Dieser Parameter ist ein globaler Parameter und gilt für alle virtuellen DNS-Server, die auf der Citrix ADC Appliance konfiguriert sind.

Geben Sie die maximale Anzahl gleichzeitiger DNS-Anforderungen an, die für eine einzelne Clientverbindung zulässig sind, mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die maximale Anzahl gleichzeitiger DNS-Anforderungen anzugeben, die für eine einzelne Clientverbindung zulässig sind, und überprüfen Sie die Konfiguration:


```
-  set dns parameter -maxPipeline <positive_integer>
-  show dns parameter
<!--NeedCopy-->
```

Beispiel:

```
> set dns parameter -maxPipeline 1000
 Done
> show dns parameter
        DNS parameters:
        DNS retries: 5
        .
        .
        .
        Max DNS Pipeline Requests: 1000
 Done
<!--NeedCopy-->
```

Geben Sie die maximale Anzahl gleichzeitiger DNS-Anforderungen an, die für eine einzelne Clientverbindung zulässig sind, mit der GUI

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Klicken Sie im Detailbereich auf DNS-Einstellungen ändern.
3. Geben Sie im Dialogfeld DNS-Parameter konfigurieren einen Wert für Max. DNS-Pipeline-Anforderungen an.
4. Klicken Sie auf OK.

Konfigurieren des Citrix ADC als Endauflöser

October 5, 2021

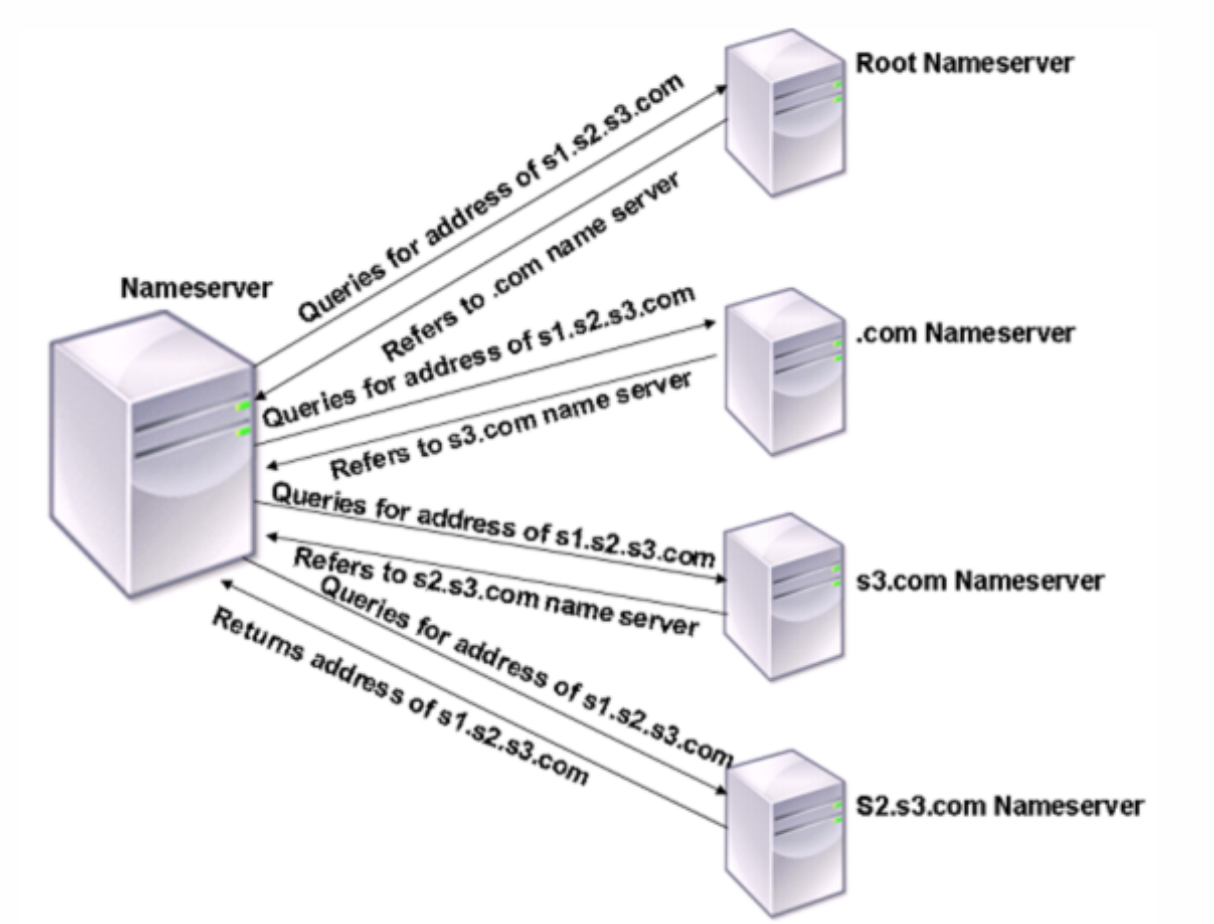
Ein Resolver ist eine Prozedur, die von einem Anwendungsprogramm aufgerufen wird, das einen Domain/Hostnamen in seinen Ressourcendatensatz übersetzt. Der Resolver interagiert mit dem LDNS, der nach dem Domänennamen sucht, um seine IP-Adresse zu erhalten. Der Citrix ADC kann eine End-to-End-Auflösung für DNS-Abfragen bereitstellen.

In rekursiver Auflösung fragt die Citrix ADC Appliance verschiedene Nameserver rekursiv ab, um auf die IP-Adresse einer Domäne zuzugreifen. Wenn der Citrix ADC eine DNS-Anforderung empfängt, über-

prüft er seinen Cache auf den DNS-Eintrag. Wenn der Datensatz nicht im Cache vorhanden ist, fragt er die in der Datei ns.conf konfigurierten Stammserver ab. Der Stammnamenserver meldet mit der Adresse eines DNS-Servers zurück, der detaillierte Informationen über die Domäne der zweiten Ebene enthält. Der Vorgang wird wiederholt, bis der erforderliche Datensatz gefunden wird.

Wenn Sie die Citrix ADC Appliance zum ersten Mal starten, werden der Datei ns.conf 13 Stammname-Server hinzugefügt. Die NS- und Adressdatensätze für die 13 Stammserver werden ebenfalls hinzugefügt. Sie können die Datei ns.conf ändern, aber der Citrix ADC erlaubt Ihnen nicht, alle 13 Datensätze zu löschen. Es ist mindestens ein Nameservereintrag erforderlich, damit die Appliance die Namensauflösung durchführen kann. Das folgende Diagramm veranschaulicht den Prozess der Namensauflösung.

Abbildung 1. Rekursive Auflösung



Wenn der Namenserver in dem Diagramm eine Abfrage für die Adresse von s1.s2.s3.com empfängt, überprüft er zunächst die Stammnamenserver auf s1.s2.s3.com. Ein Root-Name-Server meldet mit der Adresse des com-Nameservers zurück. Wenn die Adresse von s1.s2.s3.com im Nameserver gefunden wird, antwortet er mit einer geeigneten IP-Adresse. Andernfalls werden andere Nameserver für s3.com abgefragt, und dann für s2.s3.com, um die Adresse von s1.s2.s3.com abzurufen. Auf diese Weise beginnt die Auflösung immer von Root-Name-Servern und endet mit dem autorisierenden Nameserver der Domäne.

Hinweis: Für Funktionen für rekursive Auflösung muss das Caching aktiviert sein.

Rekursive Auflösung aktivieren

Um die Citrix ADC Appliance so zu konfigurieren, dass sie als Endauflösung fungiert, müssen Sie die rekursive Auflösung auf der Appliance aktivieren.

Aktivieren Sie die rekursive Auflösung mit der CLI

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

```
-  set dns parameter -recursion ENABLED
-  show dns parameter
<!--NeedCopy-->
```

Beispiel:

```
> set dns parameter -recursion ENABLED
 Done
> show dns parameter
        DNS parameters:
            .
            .
            .
        Recursive Resolution : ENABLED
            .
            .
            .
 Done
<!--NeedCopy-->
```

Aktivieren Sie die rekursive Auflösung mit der GUI

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Klicken Sie im Detailbereich unter Einstellungen auf DNS-Einstellungen ändern.
3. Aktivieren Sie im Dialogfeld DNS-Parameter konfigurieren das Kontrollkästchen Rekursion aktivieren, und klicken Sie dann auf OK.

Festlegen der Anzahl der Wiederholungen

Konfigurieren Sie die ADC-Appliance so, dass sie eine vorkonfigurierte Anzahl von Versuchen (so genannte DNS-Retries) ausführt, wenn sie keine Antwort von dem Server erhält, an den sie eine Abfrage sendet. Standardmäßig ist die Anzahl der DNS-Wiederholungen auf 5 festgelegt.

Legen Sie die Anzahl der DNS-Wiederholungsversuche mit der CLI fest

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Anzahl der Wiederholungen festzulegen und die Konfiguration zu überprüfen:

```
1 -  set dns parameter -retries <positive_integer>
2 -  show dns parameter
3 <!--NeedCopy-->
```

Beispiel:

```
1 > set DNS parameter -retries 3
2  Done
3 > show dns parameter
4         DNS parameters:
5         DNS retries: 3
6             .
7             .
8             .
9  Done
10 <!--NeedCopy-->
```

Legen Sie die Anzahl der Wiederholungen mit der GUI fest

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Klicken Sie im Detailbereich unter Einstellungen auf DNS-Einstellungen ändern.
3. Geben Sie im Dialogfeld DNS-Parameter konfigurieren im Textfeld DNS-Wiederholungen die Anzahl der DNS-Auflösungsanforderungen ein, und klicken Sie dann auf OK.

Konfigurieren Sie die Citrix ADC Appliance als Forwarder

June 1, 2022

Ein Forwarder ist ein Server, der DNS-Anfragen an DNS-Server weiterleitet, die sich außerhalb des Netzwerks des Forwarder-Servers befinden. Abfragen, die lokal nicht gelöst werden können, werden an andere DNS-Server weitergeleitet. Ein Forwarder sammelt externe DNS-Informationen in seinem Cache, während er DNS-Abfragen auflöst. Um die Citrix ADC Appliance als Forwarder zu konfigurieren, müssen Sie einen externen Namenserver hinzufügen.

Mit der Citrix ADC Appliance können Sie externe Namenserver hinzufügen, an die sie die Namensauflösungsabfragen weiterleiten kann, die lokal nicht aufgelöst werden können. Um die Citrix ADC Appliance als Forwarder zu konfigurieren, müssen Sie die Namenserver hinzufügen, an die sie Abfragen zur Namensauflösung weiterleiten muss. Sie können die Lookup-Priorität angeben, um den Namen-Service anzugeben, den die Citrix ADC Appliance für die Namensauflösung verwenden muss.

Informationen zur Konfiguration der Citrix ADC Appliance als Forwarder finden Sie unter Hinzufügen eines Namenservers (wenn die Citrix ADC Appliance als Forwarder fungiert) mithilfe der CLI.

> **Hinweis:**
>
> Die Citrix ADC Appliance im Forwarder-Modus unterstützt TCP-, UDP- und UDP-TCP-Namensserver.
>
> - Wenn Sie einen TCP-Namenserver konfiguriert haben, sendet die Citrix ADC Appliance die DNS-Anfrage über TCP.
> - Wenn Sie einen UDP-Namenserver konfiguriert haben, sendet die Citrix ADC Appliance die DNS-Anfrage über UDP.
> - Wenn Sie einen UDP-TCP-Namenserver konfiguriert haben, sendet die Citrix ADC Appliance die DNS-Anfrage über UDP. Wenn jedoch das abgeschnittene Bit in der DNS-Antwort festgelegt ist, sendet die Appliance solche DNS-Anforderungen über TCP.

Hinzufügen eines Nameservers

October 5, 2021

Sie können einen Nameserver erstellen, indem Sie die IP-Adresse angeben oder einen vorhandenen virtuellen Server als Nameserver konfigurieren.

- **IP-adressbasierter Nameserver** - Ein externer Nameserver, der für die Domänennamenauflösung kontaktiert werden soll. Wenn mehrere IP-Adressen-basierte Nameserver auf der Appliance konfiguriert sind und der lokale Parameter auf keinen von ihnen festgelegt ist, werden eingehende DNS-Abfragen in Round-Robin-Art und Weise auf alle Nameserver ausgeglichen.
- **Virtueller serverbasierter Nameserver** - Ein virtueller DNS-Server, der im Citrix ADC konfiguriert ist. Um eine feinere Kontrolle darüber zu erhalten, wie externe DNS-Namenserver Lastenausgleich sind (z. B. möchten Sie eine andere Load Balancing-Methode als Round-Robin), gehen Sie wie folgt vor:

- Konfigurieren eines virtuellen DNS-Servers auf der Appliance
- Binden Sie die externen Nameserver als seine Dienste
- Geben Sie in diesem Befehl den Namen des virtuellen Servers an.

Um die Konfiguration zu überprüfen, können Sie den`show dns nameServer` Befehl verwenden.

Um einen Nameserver zu entfernen, geben Sie an der Citrix ADC CLI den`rm dns nameServer` Befehl gefolgt von der IP-Adresse des Nameservers ein.

Um die Details des DNS-Nameservers anzuzeigen, geben Sie bei der Citrix ADC CLI den `show dns nameServer` Befehl gefolgt von der IP-Adresse des Namenservers ein.

Hinzufügen eines Nameservers (wenn die Citrix ADC Appliance als Weiterleitung fungiert) mit der CLI

Geben Sie an der Eingabeaufforderung;

```
add dns nameServer ((<IP>) | <dnsVserverName>)
<!--NeedCopy-->
```

oder

```
add dns nameServer ((<IP> | <dnsVserverName>) [-type <type>]
<!--NeedCopy-->
```

Beispiele:

```
add dns nameServer dnsVirtualNS

add dns nameServer 192.0.2.11 -type TCP

add dns nameServer 192.0.2.12 -type UDP_TCP


add dns nameServer 192.0.2.10
show dns nameServer 192.0.2.10

1) 192.0.2.10  -  State: UP  Protocol: UDP
Done
<!--NeedCopy-->
```


> **Hinweis:**
>
> Wenn der Namenservertyp nicht angegeben ist, wird standardmäßig ein UDP-Nameserver erstellt. Um einen Nameserver vom Typ TCP oder UDP_TCP zu erstellen, müssen Sie den Typ angeben.
>
> Wenn Sie den Typ als UDP_TCP angeben, werden zwei Nameserver (ein UDP-Namenserver und ein TCP-Namenserver) für die angegebene IP-Adresse erstellt.

Hinzufügen eines Nameservers (wenn die Citrix ADC Appliance als Resolver fungiert) mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add dns nameServer ((<IP> [-local]) | <dnsVserverName>)
<!--NeedCopy-->
```

Beispiel:

```
add dns nameServer 10.102.9.19 -local
show dns nameServer
1)  10.102.9.19 LOCAL -  State: UP  Protocol: UDP
Done
<!--NeedCopy-->
```

Lokal - Markieren Sie die IP-Adresse als eine IP-Adresse, die zu einem lokalen rekursiven DNS-Server auf der Citrix ADC Appliance gehört. Die Appliance löst rekursiv Abfragen auf, die für eine IP-Adresse empfangen wurden, die als lokal markiert ist.
Damit die rekursive Auflösung funktioniert, muss auch der globale DNS-Parameter`recursion`, festgelegt werden.
Wenn kein Nameserver als lokal markiert ist, fungiert die Appliance als Stub-Resolver und gleicht die Nameserver aus.

Hinzufügen eines Nameservers mit der GUI

Navigieren Sie zu **Traffic Management** > **DNS** > **Namensserver**, und erstellen Sie einen Nameserver.

DNS-Lookup-Priorität festlegen

October 5, 2021

Sie können die Lookup-Priorität entweder auf DNS oder WINS festlegen. Diese Option wird im SSL-VPN-Betriebsmodus verwendet.

Festlegen der Lookup-Priorität auf DNS mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Suchpriorität auf DNS festzulegen und die Konfiguration zu überprüfen:

```
1 -  set dns parameter -nameLookupPriority (DNS | WINS)
2 -  show dns parameter
3 <!--NeedCopy-->
```

Beispiel:

```
1 > set dns parameter -nameLookupPriority DNS
2  Done
3 > show dns parameter
4              .
5              .
6              .
7          Name lookup priority : DNS
8              .
9              .
10             .
11  Done
12 <!--NeedCopy-->
```

Lookup-Priorität auf DNS mit der GUI festlegen

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf DNS-Einstellungen ändern.
3. Wählen **Sie im Dialogfeld DNS-Parameter konfigurieren** unter **Namenssuchpriorität** die Option DNS oder WINS aus, und klicken Sie dann auf OK.

> **Hinweis:**
>
> Wenn der virtuelle DNS-Server, den Sie konfiguriert haben, DOWN ist und wenn `-nameLookupPriority` Sie DNS festlegen, versucht Citrix ADC keine WINS-Suche. Wenn ein virtueller DNS-Server nicht konfiguriert oder deaktiviert ist, legen Sie den `-nameLookupPriority` auf WINS fest.

Deaktivieren und Aktivieren von Namenservern

October 5, 2021

Im folgenden Verfahren werden die Schritte zum Aktivieren oder Deaktivieren eines vorhandenen Nameservers beschrieben.

Aktivieren oder Deaktivieren eines Nameservers mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen Nameserver zu aktivieren oder zu deaktivieren und die Konfiguration zu überprüfen:

```
1 -  (enable | disable) dns nameServer <IPAddress>
2 -  show dns nameServer <IPAddress>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > disable dns nameServer 10.102.9.19
2  Done
3 > show dns nameServer 10.102.9.19
4 1)       10.102.9.19: LOCAL  -  State: OUT OF SERVICE
5  Done
6 <!--NeedCopy-->
```

Aktivieren oder Deaktivieren eines Nameservers mit der GUI

1. Navigieren Sie zu **Traffic Management > DNS > Namensserver**.
2. Wählen Sie im Detailbereich den Namenserver aus, den Sie aktivieren oder deaktivieren möchten.

3. Klicken Sie auf Aktivieren oder Deaktivieren. Wenn ein Nameserver aktiviert ist, ist die Option Deaktivieren verfügbar. Wenn ein Namenserver deaktiviert ist, ist die Option Aktivieren verfügbar.

Konfigurieren von Citrix ADC als nicht validierenden, sicherheitsbezogene Stub-Resolver

October 5, 2021

Beginnend mit Citrix ADC 12.1 Build 49.xx fungiert Citrix ADC als nicht validierender, sicherheitsrelevante Stub-Resolver. Um diese Unterstützung zu aktivieren, wird das AD Bit im DNS-Header gesetzt und das DO-Bit im OPT-Header nicht gesetzt. Wenn das AD-Bit gesetzt ist und das DO-Bit nicht gesetzt ist, validiert der rekursive Resolver der Originalautoren die DNSSEC-Antwort. Wenn die Validierung erfolgreich ist, antwortet der rekursive Resolver ohne DNSSEC-RRs. Wenn die DNSSEC-Validierung fehlschlägt, gibt der rekursive Resolver mit einer SERVFAIL-Antwort zurück.

> **Wichtig:**
>
> Das AD-Bit wird standardmäßig in der ADC-Weiterleitung festgelegt. Das AD-Bit ist nicht für DBS-initiierte Abfragen festgelegt.

Jumbo-Frames-Unterstützung für DNS, um Antworten großer Größen zu verarbeiten

October 5, 2021

Ab Citrix ADC 12.1 Build 49.xx unterstützt DNS Jumbo-Frames für die Verarbeitung von UDP-Antworten größer als 1.280 Byte. Zuvor unterstützte die Citrix ADC Appliance nur die UDP-Paketgröße von bis zu 1.280 Byte.

Sie können die maximale UDP-Paketgröße festlegen, die die Appliance im Proxy-, ADNS- und Weiterleitungsmodus verarbeiten kann, indem Sie den Parameterwert Maximale UDP-Paketgröße konfigurieren. Wenn beispielsweise der Parameterwert Maximale UDP-Paketgröße auf 4096 festgelegt ist, kann die Appliance DNS-Antwort mit der Größe 4.096 Byte verarbeiten.

> **Wichtig**
>
> - Im Proxy-Modus wird die geringste Größe zwischen der OPT-Nutzlastgröße für Clientanfragen und dem Wert für Maximale UDP-Paketgröße für das Senden von DNS-Abfragen an das Back-End berücksichtigt. Wenn die OPT-Nutzlastgröße für Clientanfragen beispielsweise

> 3000 beträgt und der Wert für maximale UDP-Paketgröße 4096 beträgt, werden 3.000 Byte DNS-Abfragen an das Back-End gesendet.
>
> Außerdem kann das Gerät vom Back-End Antworten großer Größe erhalten und Reaktionen großer Größe verarbeiten.
>
> - Im Weiterleitungsmodus legt die Appliance die OPT-Nutzlastgröße gleich dem Wert der UDP-Paketgröße fest.
> - Wenn die DNS-Einträge lokal in der Appliance sind, kann die Appliance Antwortgrößen erstellen, die so groß sind wie der Parameterwert Maximale UDP-Paketgröße. Diese Einstellung gilt für ADNS, Proxy und rekursive Resolver.

So konfigurieren Sie die maximale UDP-Paketgröße mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set dns parameter [-maxUDPPacketSize <positive_integer>]
<!--NeedCopy-->
```

Beispiel:

```
set dns parameter -maxUDPPacketSize 10000
<!--NeedCopy-->
```

> **Hinweis**: Der Minimal- und Maximalwert, den Sie für den Parameter Maximale UDP-Paketgröße festlegen können, ist 512 bzw. 16384. Der Standardwert ist 1280.

So konfigurieren Sie die maximale UDP-Paketgröße mit der CLI

1. Navigieren Sie zu **Traffic Management** > **DNS**.
2. Klicken Sie im Detailbereich auf **DNS-Einstellungen ändern**.
3. Geben Sie unter Maximale UDP-Paketgröße die maximale UDP-Paketgröße an.
4. Klicken Sie auf **OK**.

Konfigurieren der DNS-Protokollierung

December 7, 2021

Sie können die Citrix ADC Appliance so konfigurieren, dass die von ihr verarbeiteten DNS-Anforderungen und -Antworten protokolliert werden. Die Appliance protokolliert die DNS-Anforderungen und -Antworten im SYSLOG-Format. Sie können entweder DNS-Anforderungen oder DNS-Antworten oder beides protokollieren und die Syslog-Nachrichten an einen Remoteprotokollserver senden. Die Protokollmeldungen können verwendet werden, um:

- Überwachen der DNS-Antworten auf den Client
- Überwachen von DNS-Clients
- DNS-Angriffe erkennen und verhindern
- Problembehandlung

Eine Citrix ADC Appliance kann die folgenden Abschnitte in der DNS-Anfrage oder -Antwort basierend auf Ihrer Konfiguration protokollieren:

- Kopfzeilenabschnitt
- Abschnitt Fragen
- Antwortbereich
- Abschnitt Autorität
- **Zusätzlicher** Abschnitt

DNS-Profile

Sie können ein DNS-Profil verwenden, um die verschiedenen DNS-Parameter zu konfigurieren, die der DNS-Endpunkt auf den DNS-Verkehr anwenden soll. Im Profil können Sie Protokollierung, Caching und negatives Caching aktivieren.

Wichtig: Ab dem NetScaler 11.0-Release ist das Aktivieren des DNS-Cachings mit globalen DNS-Parametern veraltet. Sie können die DNS-Zwischenspeicherung mithilfe von DNS-Profilen aktivieren oder deaktivieren. Sie können jetzt DNS-Caching für einen einzelnen virtuellen Server aktivieren, indem Sie DNS-Caching in einem DNS-Profil aktivieren und das DNS-Profil auf den einzelnen virtuellen Server festlegen.

DNS-Profile unterstützen die folgenden Arten von DNS-Protokollierung:

- DNS-Abfrageprotokollierung
- Protokollierung von DNS-Antwortabschnitten
- Erweiterte DNS-Protokollierung
- DNS-Fehlerprotokollierung

DNS-Abfrageprotokollierung

Sie können eine Citrix ADC Appliance so konfigurieren, dass nur die DNS-Abfragen protokolliert werden, die von den DNS-Endpunkten auf der Appliance empfangen werden.

Hinweis: Wenn bei der Verarbeitung einer Abfrage Fehler auftreten, werden diese protokolliert, wenn diese Option im DNS-Profil festgelegt ist.

Es folgt ein Beispiel für eine Abfrageprotokollmeldung:

```
DNS DNS_QUERY 143 0 :  U:10.102.27.70#61297:10.102.27.73#53/22142/Q/
(RD)/NO/1/0/0/0#test.com./1#
<!--NeedCopy-->
```

Protokollierung des DNS-Antwortabschnitts

Sie können eine Citrix ADC Appliance so konfigurieren, dass alle **Antwortabschnitte** in den DNS-Antworten, die die Appliance an den Client sendet, protokolliert. Die Protokollierung des DNS-Antwortabschnitts ist nützlich, wenn der Citrix ADC als DNS-Resolver oder in GLSB-Anwendungsfällen konfiguriert ist.

Es folgt ein Beispiel für ein DNS-Antwortabschnittprotokoll:

```
DNS DNS_RESPONSE 6678 0 :  U:100.100.100.210#32776:100.100.100.10#
53/61373/Q/(RD,AA,RA,R)/NO/1/1/2/4#n1.citrix.com1./
28#ANS#AAAA/120/1111:2345:6789:ffab:abcd:effa:1234:3212##
<!--NeedCopy-->
```

Erweiterte DNS-Protokollierung

Um eine Citrix ADC Appliance für die Protokollierung von Authority und **Additional** Sections in den DNS-Antworten zu konfigurieren, aktivieren Sie die erweiterte Protokollierung mit Antwortabschnitt.

Hinweis: Wenn bei der Verarbeitung von Abfragen oder Antworten Fehler auftreten, werden die Fehler protokolliert, wenn diese Option im DNS-Profil festgelegt ist.

Es folgt ein Beispiel für eine Meldung, die protokolliert wird, wenn die Cache-Suche abgeschlossen ist und die Antwort in das Paket eingebettet ist:

```
DNS DNS_RESPONSE 2252 0 :  T:100.100.100.118#21411:100.100.100.10
#53/48537/Q/(RD,AA,CD,RA,R)/NO/1/1/2/6#a1.citrix.com1./1#ANS#A/
120/1.1.1.1##AUTH#citrix.com1/NS/120/n2.citrix.com1#n1.citrix.com1##ADD
   #n1.citrix.com1
/A/120/1.1.1.1#1.1.1.2##n1.citrix.com1/AAAA/120/
1111:2345:6789:ffab:abcd:effa:1234:3212##n2.citrix.com1/A/120/2.1.1.2
```



```
##n2.citrix.com1/AAAA/120/2222:faff:3212:8976:123:1241:64:ff9b##OPT
   /0/1280/DO##
<!--NeedCopy-->
```

DNS-Fehlerprotokollierung

Sie können eine Citrix ADC Appliance so konfigurieren, dass die Fehler oder Fehler protokolliert werden, die bei der Verarbeitung einer DNS-Abfrage oder -Antwort auftreten. Bei diesen Fehlern protokolliert die Appliance den DNS-Header, die **Fragen-Abschnitte** und die OPT-Datensätze.

Es folgt ein Beispiel für eine Meldung, die protokolliert wird, wenn während der Verarbeitung einer DNS-Anforderung oder -Antwort ein Fehler auftritt:

```
DNS DNS_ERROR 149 0 :  U:10.102.27.70#27832:10.102.27.73#53/61153/Q/
(RD)/NO/1/0/0/0#test.com./1140#Packet Dropped
<!--NeedCopy-->
```

Richtlinienbasierte Protokollierung

Sie können benutzerdefinierte Protokollierung basierend auf DNS-Ausdrücken konfigurieren, indem Sie die Richtlinien LogAction für DNS-Richtlinien, Rewrite oder Responder konfigurieren. Sie können angeben, dass die Protokollierung nur erfolgt, wenn eine bestimmte DNS-Richtlinie als true ausgewertet wird. Weitere Informationen finden Sie unter Konfigurieren der richtlinienbasierten Protokollierung für DNS.

Verstehen des Citrix ADC Syslog-Nachrichtenformats

Citrix ADC Appliance protokolliert DNS-Anforderungen und -Antworten im folgenden Syslog-Format:

```
<transport> :<client IP>#<client ephemeral port>:<DNS endpoint IP>#<
   port>
 : <query id> /opcode/header flags/rcode/question section count/answer
    section count
/ auth section count / additional section count #<queried domain name>
/<queried type>#...
<!--NeedCopy-->
```

- **:**<transport>
  - T = TCP

  - U = UDP

- <client IP>#< client ephemeral port >: DNS-Client-IP-Adresse und Portnummer
- <DNS endpoint IP># <port>: IP-Adresse und Portnummer des Citrix ADC DNS-Endpunkts
- <query id>:
  Abfrage-ID
- <opcode>: Betriebscode. Unterstützte Werte:
  - F: Anfrage
  - I: inverse Abfrage
  - S: Status
  - X0: nicht zugewiesen
  - N: benachrichtigen
  - U: update
  - X1-10: nicht zugewiesene Werte
- <header flags>: Fahnen. Unterstützte Werte:
  - RD: Wiederholung erwünscht
  - TC: gekürzt
  - AA: maßgebliche Antwort
  - CD: check deaktiviert
  - AD: authentifizierte Daten
  - Z: nicht zugewiesen
  - RA: Rekursion verfügbar
  - R: Antwort
- <rcode>: Antwortcode. Unterstützte Werte:
  - NEIN: kein Fehler
  - F-Formatfehler
  - S: Serverausfall
  - NX: nicht existierende Domäne
  - NI: nicht implementiert
  - R: Abfrage abgelehnt
  - YX: Name Existiert wenn es nicht darf
  - YXR: RR Set Existiert wenn es nicht darf
  - NXR: RR Set das existieren muss nicht
  - NAS: Server ist nicht autorisierend für Zone
  - NA: Nicht autorisiert
  - NZ: Name nicht in Zone enthalten
  - X1-5: nicht zugewiesen

- **/question Abschnitt Count/Antwort Abschnitt Count/Auth Abschnitt Count/zusätzliche Abschnittsanzahl: Anzahl der zusätzlichen Abschnitte: Anzahl** der Bereiche “Frage”, Anzahl der Authority-Abschnitte und Anzahl **zusätzlicher** Abschnitte in der DNS-Anfrage
- **<queried domain name>/<queried type>:** Abgefragte Domäne und abgefragter Typ in der DNS-Anfrage
- **#ANS#<record type>/<ttl>/.. #AUTH#<domain name>/<record type>/<ttl>.. #ADD#<domain name>/<record type>/<ttl>...:**

  In DNS-Antworten:

  Antwortabschnitt wird protokolliert, wenn die Protokollierung der Antwortabschnitte im DNS-Profil aktiviert ist. Authority und **Zusätzliche** Abschnitte werden protokolliert, wenn die erweiterte Protokollierung im DNS-Profil aktiviert ist. Das Protokollformat unterscheidet sich je nach Datensatztyp. Weitere Informationen finden Sie unter Understanding the Record Logging Format.

  - ANS: Antwortbereich
  - AUTH: Autorität
  - ADD: **Zusätzlicher** Abschnitt
- **OPT/<edns version>/UDP max payload size/DO:** OPT record format in the DNS log
- **OPT/<EDNS version>/<UDP payload size>/<“DO”or empty based on whether DNSSEC OK bit is set or not>/<value of RDLEN>/ECS/<Q/R>/<option length>/<Family>/<Source Prefix-Length>/<Scope Prefix-Length>/<ECS Address>:**

  Wenn die DNS-Abfrage oder -Antwort die Option EDNS-Client-Subnetz (ECS) enthält, wird diese auch im OPT-Eintragsformat in der DNS-Protokolldatei protokolliert.

  Wenn eine DNS-Abfrage mit einer ECS-Option gesendet wird, die entweder eine IPv4- oder IPv6-Adresse enthält, wird die ECS-Option mit einer der folgenden Optionen protokolliert:

  - “ECS/Q”, das angibt, dass die Werte im Protokoll von der Abfrage stammen
  - “ECS/R” zeigt an, dass die Werte im Protokoll von der Antwort stammen.

  Der Wert von Scope Prefix-Length wird ebenfalls entsprechend festgelegt. In der DNS-Abfrage ist sie auf Null festgelegt, und für die Antwort wird sie auf den berechneten Wert festgelegt.

  In der folgenden Tabelle werden die protokollierten Details in verschiedenen Szenarien beschrieben:

Szenario	ECS-Option in der DNS-Abfrage festgelegt	ECS-Option, die in der DNS-Antwort festgelegt ist	Protokollierte Details
Sowohl die Abfrageprotokollierung als auch die erweiterte Protokollierung aktiviert	Ja	Ja	ECS-Option wird mit der Zeichenfolge ECS/R/ protokolliert und die Scope Prefix-Length wird auf den berechneten Wert gesetzt.
Sowohl die Abfrageprotokollierung als auch die erweiterte Protokollierung aktiviert	Ja	Nein	ECS-Option wird mit der Zeichenfolge ECS/Q protokolliert und die Scope Prefix-Length ist auf Null gesetzt.
Die Abfrageprotokollierung ist aktiviert, aber die erweiterte Protokollierung ist nicht aktiviert	Ja	Ja	ECS-Option wird mit der Zeichenfolge ECS/Q/ protokolliert und die Scope Prefix-Length ist auf Null gesetzt.
Abfrageprotokollierung und erweiterte Protokollierung sind nicht aktiviert	Ja	Ja	ECS-Option wird nicht protokolliert.
Die Abfrageprotokollierung ist aktiviert, aber die erweiterte Protokollierung ist nicht aktiviert	Ja	Nein	ECS-Option wird mit der Zeichenfolge ECS/Q/ protokolliert und die Scope Prefix-Length ist auf Null gesetzt.

Szenario	ECS-Option in der DNS-Abfrage festgelegt	ECS-Option, die in der DNS-Antwort festgelegt ist	Protokollierte Details
Die Abfrageprotokollierung ist nicht aktiviert, aber die erweiterte Protokollierung ist aktiviert	Ja	Ja	ECS-Option wird mit der Zeichenfolge ECS/R/ protokolliert und die Scope Prefix-Length wird auf den berechneten Wert gesetzt.
Die Abfrageprotokollierung ist nicht aktiviert, aber die erweiterte Protokollierung ist aktiviert	Ja	Nein	ECS-Option wird nicht protokolliert.

Verstehen des Datensatzprotokollierungsformats

Es folgt ein Beispiel für das Datensatzprotokollierungsformat in einer Syslog-Nachricht:

```
1 <domainname>/<record type>/ <record ttl> / <resource record data>#<
     resource record data>#......##
2 <!--NeedCopy-->
```

Wobei:

Datensatztyp	Beispielformat	Ressourceneintragsdaten/-format
Adressdatensatz (A)	A/5/1.1.1.1#1.1.1.2#1.1.1.3##	IPv4-Adresse
AAAA Rekord	AAAA/5/1::1#1::2#1::3##	IPv6-Adresse
SOA-Datensatz	SOA/3600/ns1.dnslogging.test./	Ursprungsserver, Kontakt und andere Details. Resource record format is: <originServer>/<contact>/<serial number>/<refresh rate>/<retry>/<expire>/<minimum>##

Datensatztyp	Beispielformat	Ressourceneintragsdaten/-format
NS-Datensatz	NS/5/ns1.dnslogging.test	Hostname des Nameservers.
MX-Eintrag	#MX/5/10/host1.dnslogging.test	Voreinstellung gefolgt von Mail-Exchange-Server-Hostname
CNAME-Datensatzprotokollierung	CNAME/5/host1.dnslogging.test.##	Kanonischer Name
SRV-Datensatz	SRV/5/1/2/3/host1.dnslogging.te	Resource record format: ## <priority>/<weight>/<port>/<target>#
TXT-Eintrag	TXT/5/dns+logging##	Die Daten umfassen alle Texte.
NAPTR-Datensatz	NAPTR/5/10/11////dnslogging#2	Resource record format: # <order>/<preference>/<flags>/<services>/<re expression>/<replacement string>#
DNSKEY-Eintrag	DNSKEY/5/1/3/5/AwEAAanP0K+i5	Resource record format: <flags>/<protocol>/<algorithm>/<public key in base64 encoding>#
PTR-Datensatz	PTR/3600/test.com.#test4.com.	Domänenname

Einschränkungen der DNS-Protokollierung

DNS-Protokollierung hat folgende Einschränkungen:

- Wenn die Antwortprotokollierung aktiviert ist, werden nur die folgenden Datensatztypen protokolliert:
  - Adressdatensatz (A)
  - AAAA Rekord
  - SOA-Datensatz
  - NS-Datensatz
  - MX-Eintrag
  - CNAME-Eintrag
  - SRV-Datensatz
  - TXT-Eintrag
  - NAPTR-Datensatz
  - DNSKEY-Eintrag

- PTR-Datensatz

Für alle anderen Datensatztypen werden nur L3/L4-Parameter, DNS-Header und Fragenabschnitt protokolliert.

- RRSIG-Datensätze werden nicht protokolliert, auch wenn die Antwortprotokollierung aktiviert ist.
- DNS64 wird nicht unterstützt.
- Proaktive DNS-Aktualisierungsanforderungen oder -Antworten werden entsprechend den Einstellungen im Standardprofil protokolliert.
- Wenn auf dem virtuellen Server die Option Sitzungslose und Antwortprotokollierung aktiviert ist, werden L3/L4-Parameter, DNS-Header und DNS-Frageabschnitt anstelle der Antwort protokolliert.
- Die maximale Größe der Syslog-Nachricht beträgt 1024 Byte.
- Wenn Sie ein DNS-Profil für eine DNS-Richtlinie mit Aktionstyp Rewrite Response festgelegt haben, protokolliert die Citrix ADC Appliance die Abfrage oder die manipulierten Antworten nicht. Um die erforderlichen Informationen zu protokollieren, müssen Sie eine Überwachungsnachrichtenaktion in der DNS-Richtlinie verwenden.
- DNS-Transaktionen, die auf den DNS-Überwachungsdatenverkehr zurückzuführen sind, werden nicht protokolliert.

Konfigurieren der DNS-Protokollierung

Im Folgenden finden Sie eine Übersicht über die Konfiguration der DNS-Protokollierung:

1. Erstellen Sie eine Syslog-Aktion und aktivieren Sie DNS in der Aktion.
2. Erstellen Sie eine Syslog-Richtlinie, und geben Sie die Syslog-Aktion in der Richtlinie an.
3. Globale Bindung der Syslog-Richtlinie, um die Protokollierung aller Citrix ADC -Systemereignisse zu aktivieren. Oder binden Sie die Syslog-Richtlinie an einen bestimmten virtuellen Lastausgleichsserver.
4. Erstellen Sie ein DNS-Profil und definieren Sie eine der folgenden Arten von Protokollierung, die Sie aktivieren möchten:
   - DNS-Abfrageprotokollierung
   - Protokollierung von DNS-Antwortabschnitten
   - Erweiterte DNS-Protokollierung
   - DNS-Fehlerprotokollierung
5. Konfigurieren Sie je nach Anforderung eine der folgenden Optionen:
   - DNS-Dienst und virtueller Server für DNS
   - ADNS-Dienst

- Citrix ADC als Weiterleitung
- Citrix ADC als Resolver

6. Legen Sie das erstellte DNS-Profil auf eine der DNS-Entitäten fest.

Konfigurieren der DNS-Protokollierung für Citrix ADC, die als DNS-Proxy mit der CLI konfiguriert ist

1. Fügen Sie eine Syslog-Aktion hinzu, und aktivieren Sie DNS in der Aktion. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add audit syslogAction <name> (<serverIP> | -lbVserverName <string
    >) [-serverPort <port>] -logLevel <logLevel> ... [-dateFormat <
    dateFormat>] [-logFacility <logFacility>] [-tcp ( NONE | ALL )]
     [-acl ( ENABLED | DISABLED )] [-timeZone ( GMT_TIME |
    LOCAL_TIME )] [-userDefinedAuditlog ( YES | NO )] [-
    appflowExport ( ENABLED |DISABLED )] [-lsn ( ENABLED | DISABLED
     )] [-alg ( ENABLED | DISABLED )] [-transport ( TCP | UDP )] [-
    tcpProfileName <string>] [-maxLogDataSizeToHold <
    positive_integer>] [-dns ( ENABLED | DISABLED)]
<!--NeedCopy-->
```

Beispiel:

```
add audit syslogAction nssyslogact1 10.102.151.136 -logLevel CRITICAL
ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -timeZone
LOCAL_TIME -dns ENABLED
```

2. Erstellen Sie eine Syslog-Richtlinie, und geben Sie die erstellte Syslog-Aktion in der Richtlinie an. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add audit syslogPolicy <name> <rule> <action>
```

Beispiel:

```
add audit syslogPolicy syslogpol1 ns_true nssyslogact1
```

3. Binden Sie die Syslog-Richtlinie global. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind system global [<policyName> [-priority <positive_integer>]]
```

Beispiel:

```
bind system global syslogpol1
```

4. Erstellen Sie ein DNS-Profil, und aktivieren Sie einen der folgenden Protokolltypen, die Sie konfigurieren möchten:

- DNS-Abfrageprotokollierung
- Protokollierung von DNS-Antwortabschnitten
- Erweiterte DNS-Protokollierung
- DNS-Fehlerprotokollierung

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add dns profile <dnsProfileName> [-dnsQueryLogging ( ENABLED | DISABLED
 )] [-dnsAnswerSecLogging ( ENABLED | DISABLED )] [-dnsExtendedLogging
 (ENABLED | DISABLED )] [-dnsErrorLogging ( ENABLED | DISABLED )] [-
cacheRecords ( ENABLED | DISABLED )] [-cacheNegativeResponses ( ENABLED
 | DISABLED )]
```

Beispiel:

```
add dns profile dnsprofile1 -dnsQueryLogging ENABLED
```

5. Konfigurieren Sie den Dienst vom Typ DNS. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   add service <name> <serverName> <serviceType> <port>
   ```

   Beispiel:

   ```
   add service svc1 10.102.84.140 dns 53
   ```

6. Konfigurieren Sie einen virtuellen Lastausgleichsserver des Diensttyps DNS.

   ```
   add lb vserver <name> <serviceType> <ip> <port>
   ```

   Beispiel:

   ```
   add lb vserver lb1 dns 100.100.100.10 53
   ```

7. Binden Sie den Dienst an den virtuellen Server. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   bind lb vserver <name> <serviceName>
   ```

   Beispiel:

   ```
   bind lb vserver lb1 svc1
   ```

8. Legen Sie das erstellte DNS-Profil auf den virtuellen Server fest. Geben Sie an der Eingabeaufforderung Folgendes ein:

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

   Beispiel:

   ```
   set lb vserver lb1 -dnsProfileName dnsprofile1
   ```


Beispiel-DNS-Protokollierungskonfiguration für Citrix ADC Appliance, die als DNS-Proxy konfiguriert ist

```
> add audit syslogAction nssyslogact1 10.102.151.136 -logLevel
CRITICAL ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -
    timeZone
LOCAL_TIME -dns ENABLED
Done
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> add lb vserver lb1 dns 100.100.100.10 53  - dnsProfileName dnsprofile1
Done
> add service svc1 10.102.84.140 dns 53
Done
> bind lb vserver lb1 svc1
Done
<!--NeedCopy-->
```

Beispiel-DNS-Protokollierungskonfiguration für Citrix ADC Appliance, die als ADNS konfiguriert ist

```
> add audit syslogAction nssyslogact1 10.102.151.136 -logLevel CRITICAL
ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -timeZone
    LOCAL_TIME
-dns ENABLED
Done
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> add lb vserver lb1 dns 100.100.100.10 53  - dnsProfileName dnsprofile1
Done
> add service svc1 10.102.84.140 dns 53
Done
> bind lb vserver lb1 svc1
Done
<!--NeedCopy-->
```


Beispiel-DNS-Protokollierungskonfiguration für Citrix ADC Appliance, die als Weiterleitung konfiguriert ist

```
> add audit syslogAction nssyslogact1 10.102.151.136 -logLevel CRITICAL
ERROR WARNING NOTICE INFORMATIONAL DEBUG -logFacility LOCAL4 -timeZone
    LOCAL_TIME
-dns ENABLED
Done
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> add dns nameserver 8.8.8.8  - dnsProfileName dnsprofile1
Done
<!--NeedCopy-->
```

Beispielkonfiguration für DNS-Protokollierung für Citrix ADC Appliance, die als Resolver konfiguriert ist

```
> add audit syslogAction nssyslogact1 10.102.151.136
-logLevel CRITICAL ERROR WARNING NOTICE INFORMATIONAL DEBUG -
    logFacility LOCAL4
-timeZone LOCAL_TIME -dns ENABLED
Done
> add audit syslogPolicy syslogpol1 ns_true nssyslogact1
Done
> bind system global syslogpol1
Done
> add dns profile dnsprofile1 -dnsqueryLogging ENABLED
Done
> set dns parameter -recursion enABLED
Done
> add nameserver 1.1.1.100 -local dnsProfileName dnsprofile1
Done
<!--NeedCopy-->
```


Konfigurieren der richtlinienbasierten Protokollierung für DNS

Mit der Richtlinienbasierten Protokollierung können Sie ein Format für Protokollmeldungen angeben. Der Inhalt einer Protokollnachricht wird mithilfe eines Standardsyntaxausdrucks definiert. Wenn die in der Richtlinie angegebene Nachrichtenaktion ausgeführt wird, erstellt die Citrix ADC Appliance die Protokollnachricht aus dem Ausdruck und schreibt die Nachricht in die Protokolldatei. Sie können die Appliance so konfigurieren, dass sie nur protokolliert wird, wenn eine bestimmte DNS-Richtlinie auf True ausgewertet wird.

> **Hinweis:**
>
> Wenn Sie eine DNS-Richtlinie mit einem DNS-Profil für die Anforderungsseite festgelegt haben, protokolliert die Citrix ADC Appliance nur die Abfrage.

Um die richtlinienbasierte Protokollierung für eine DNS-Richtlinie zu konfigurieren, müssen Sie zunächst eine Auditmeldungsaktion konfigurieren. Weitere Informationen zum Konfigurieren einer Überwachungsnachrichtenaktion finden Sie unter Konfigurieren der NetScaler Appliance für die Audit-Protokollierung. Geben Sie nach dem Konfigurieren der Auditmeldungsaktion die Meldungsaktion in einer DNS-Richtlinie an.

Konfigurieren der richtlinienbasierten Protokollierung für eine DNS-Richtlinie mit der CLI

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

```
1 - add dns action <actionName> <actionType> [-IPAddress <ip_addr|
    ipv6_addr> ... | -viewName <string> | -preferredLocList <string>
    ...] [-TTL <secs>] [-dnsProfileName <string>]
2 - set dns policy <name> [<rule>] [-actionName <string>] [-logAction <
    string>]
3 - show dns policy [<name>]
4 <!--NeedCopy-->
```

Beispiel 1:

Wenn Sie in einer GSLB-Bereitstellung mit unterschiedlichen IP-Adressen auf Clientanforderungen reagieren möchten, die aus einem bestimmten Subnetz stammen, können Sie eine DNS-Richtlinie mit dem Aktionstyp als DNS-Ansicht konfigurieren, wenn Sie in einer GSLB-Bereitstellung mit unterschiedlichen IP-Adressen antworten möchten. In diesem Fall können Sie die DNS-Protokollierung für die angegebene DNS-Aktion so konfigurieren, dass Sie die spezifischen Antworten protokollieren können.


```
> add dns profile dns_prof1 -dnsqueryLogging enABLED -
   dnsanswerSecLogging enABLED
 Done
> add dns view dns_view1
 Done
> add dns action dns_act1 viewName -view dns_view1  - dnsprofilename
   dns_prof1
 Done
> add dns policy dns_pol1 "CLIENT.IP.SRC.APPLY_MASK(255.255.255.0).EQ
   (100.100.100.0)"
dns_act1
 Done
> bind dns global dns_pol1 100 -gotoPriorityExpression END -type
   REQ_DEFAULT
 Done
> bind gslb service site_1_svc -viewName dns_view1 123.1.1.1
 Done
> bind gslb service site_5_svc -view dns_view1 132.1.1.1
 Done
<!--NeedCopy-->
```

Hinweis: Wenn Sie in der vorherigen Konfiguration die auf einem virtuellen GSLB-Server konfigurierte Domäne abfragen, z. B. *sampletest.com*, werden alle internen Benutzer des Subnetzes 100.100.100.0/24 mit den IP-Adressen der DNS-Ansicht bedient und die Antworten werden protokolliert. Clientanforderungen für andere Subnetze werden nicht protokolliert.

Beispiel 2:

Wenn Sie nur die Abfragen für die Domäne *example.com*protokollieren möchten, können Sie ein DNS-Profil mit aktivierter Abfrageprotokollierung erstellen und das DNS-Profil auf eine DNS-Aktion mit dem Aktionstyp
NOOPfestlegen, dann eine DNS-Richtlinie erstellen und die DNS-Aktion festlegen. Beispiel:

```
>add dns profile query_logging -dnsqueryLogging ENABLED
Done
>add dns action dns_act1 NOOP -dnsprofileName query_logging
Done
>add dns policy dns_pol1 DNS.REQ.QUESTION.DOMAIN.EQ("example.com")
   dns_act1
Done
<!--NeedCopy-->
```


Konfigurieren von DNS-Suffixe

October 5, 2021

Sie können DNS-Suffixe konfigurieren, die es der Citrix ADC Appliance ermöglichen, nicht vollständig qualifizierte Domänennamen während der Namensauflösung zu vervollständigen. Wenn beispielsweise beim Auflösen eines nicht vollständig qualifizierten Domänennamens abc ein DNS-Suffix example.com konfiguriert ist, hängt die Appliance das Suffix an den Domänennamen an. Dann wird der Domainname aufgelöst. In diesem Fall würde es abc.example.com auflösen. Wenn DNS-Suffixe nicht konfiguriert sind, hängt die Appliance einen Zeitraum an die nicht vollständig qualifizierten Domänennamen an und löst den Domänennamen auf.

DNS-Suffixe erstellen

DNS-Suffixe haben eine Bedeutung und sind nur gültig, wenn der Citrix ADC als Endauflöser oder Weiterleitung konfiguriert ist. Sie können ein Suffix von bis zu 127 Zeichen angeben.

Hinweis: Die Reihenfolge der DNS-Suffixe ist wichtig. Die ADC-Appliance versucht die konfigurierten Suffixe in einer seriellen Reihenfolge und stoppt, wenn sie eine erfolgreiche Antwort auf ein Suffix erhält.

Erstellen von DNS-Suffixe mit der CLI

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

```
1 -  add dns suffix <dnsSuffix>
2 -  show dns suffix <dnsSuffix>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add dns suffix example.com
2  Done
3 > show dns suffix example.com
4 1)      Suffix: example.com
5 Done
6
7 <!--NeedCopy-->
```


Um ein DNS-Suffix mit der Citrix ADC-Befehlszeile zu entfernen, geben Sie an der Eingabeaufforderung den `rm dns suffix` Befehl und den Namen des DNS-Suffixes ein.

Erstellen von DNS-Suffixe mit der GUI

Navigieren Sie zu **Traffic Management > DNS > DNS Suffix**, und erstellen Sie DNS-Suffixe.

DNS ANY-Abfrage

October 5, 2021

Eine ANY-Abfrage ist ein Typ von DNS-Abfrage, die alle Datensätze abruft, die für einen Domänennamen verfügbar sind. Die ANY-Abfrage muss an einen Nameserver gesendet werden, der für eine Domäne autorisierend ist.

Verhalten im ADNS-Modus

Im ADNS-Modus gibt die Citrix ADC Appliance die im lokalen Cache gespeicherten Datensätze zurück. Wenn keine Datensätze im Cache vorhanden sind, gibt die Appliance die NXDOMAIN (negative) Antwort zurück.

Wenn Citrix ADC den Domänendelegierungsdatensätzen entsprechen kann, werden die NS-Einträge zurückgegeben. Andernfalls werden die NS-Einträge der Stammdomäne zurückgegeben.

Verhalten im DNS-Proxymodus

Im Proxymodus überprüft die Citrix ADC Appliance ihren lokalen Cache. Wenn sich keine Datensätze im Cache befinden, übergibt die Appliance die Abfrage an den Server.

Verhalten bei Global Server Load Balancing (GSLB) Domänen

Wenn auf der ADC-Appliance eine GSLB-Domäne konfiguriert ist und eine ANY-Abfrage für die GSLB-Domäne (Standort) gesendet wird, gibt die Appliance die IP-Adresse des GSLB-Dienstes zurück. Er wählt diesen Dienst durch eine Lastausgleichsentscheidung aus. Wenn die Option Multiple IP Response (MIR) aktiviert ist, werden die IP-Adressen aller GSLB-Dienste gesendet.

Damit der Citrix ADC diese Datensätze zurückgibt, wenn er auf die ANY-Abfrage antwortet, müssen alle Datensätze, die einer GSLB-Domäne entsprechen, auf dem Citrix ADC konfiguriert werden.

> **Hinweis:**
>
> Wenn Datensätze für eine Domäne zwischen Citrix ADC und einem Server verteilt werden, werden nur Datensätze zurückgegeben, die auf dem Citrix ADC konfiguriert sind.

Das Citrix ADC bietet die Möglichkeit, DNS-Ansichten und DNS-Richtlinien zu konfigurieren. Diese Ansichten und Richtlinien werden für die Durchführung des globalen Lastenausgleichs von Servern verwendet. Weitere Informationen finden Sie unter Globaler Server-Lastenausgleich.

Konfigurieren der negativen Zwischenspeicherung von DNS-Einträgen

October 5, 2021

Die Citrix ADC Appliance unterstützt das Caching negativer Antworten für eine Domäne. Eine negative Antwort gibt an, dass Informationen zu einer angeforderten Domäne nicht vorhanden sind oder dass der Server keine Antwort für die Abfrage bereitstellen kann. Die Speicherung dieser Informationen wird als negatives Caching bezeichnet. Negatives Caching hilft, die Antworten auf Abfragen zu einer Domäne zu beschleunigen.

> **Hinweis:**
>
> Negatives Caching wird nur unterstützt, wenn der Back-End-Server als autoritativer DNS-Server (ADNS) für die abgefragte Domäne konfiguriert ist.

Eine negative Antwort kann eine der folgenden sein:

- NXDOMAIN-Fehlermeldung — Die autorisierenden DNS-Server reagieren mit der NXDOMAIN-Fehlermeldung, wenn der abgefragte Domänenname keine Datensätze auf dem Server konfiguriert sind. Diese Meldung impliziert, dass die abgefragte Domäne ein ungültiger oder nicht vorhandener Domainname ist.
- NODATA error message — Wenn der Domänenname in der Abfrage gültig ist, aber Datensätze des angegebenen Typs nicht verfügbar sind, sendet die Appliance eine NODATA Fehlermeldung.

Wenn das negative Caching aktiviert ist, speichert die Appliance die negative Antwort vom DNS-Server und bedient nur die zukünftigen Anforderungen aus dem Cache. Diese Aktion hilft, die Antworten auf Abfragen zu beschleunigen und den Back-End-DNS-Datenverkehr zu reduzieren. Negatives Caching kann in allen Bereitstellungen verwendet werden, d. h. wenn eine Citrix ADC Appliance als Proxy, Endresolver oder Weiterleitung fungiert.

Sie können negatives Caching mit einem DNS-Profil aktivieren oder deaktivieren, weitere Informationen finden Sie unter DNS-Profile. Standardmäßig ist das negative Zwischenspeichern im Standard-DNS-Profil (`default-dns-profile`) aktiviert, das standardmäßig an einen virtuellen DNS-Server oder im neu erstellten DNS-Profil gebunden ist.

Aktivieren oder Deaktivieren von negativem Caching mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um das negative Caching zu aktivieren oder zu deaktivieren und die Konfiguration zu überprüfen:

```
1 -  add dns profile <dnsProfileName> [-cacheRecords ( ENABLED | DISABLED
     )] [-cacheNegativeResponses (ENABLED | DISABLED )]
2 -  show dns profile [<dnsProfileName>]
3 <!--NeedCopy-->
```

Beispiel für ein Standard-DNS-Profil:

```
1 > sh dns profile default-dns-profile
2     1)   default-dns-profile
3         Query logging : DISABLED        Answer section logging :
             DISABLED
4         Extended logging : DISABLED     Error logging : DISABLED
5         Cache Records : ENABLED     Cache Negative Responses: ENABLED
6 Done
7 <!--NeedCopy-->
```

Beispiel für ein neu erstelltes DNS-Profil:

```
1 > add dnsprofile dns_profile1 -cacheRecords ENABLED -
     cacheNegativeResponses ENABLED
2 Done
3 > show dns profile dns_profile1
4     1)   dns_profile1
5         Query logging : DISABLED        Answer section logging :
             DISABLED
6         Extended logging : DISABLED     Error logging : DISABLED
7         Cache Records : ENABLED     Cache Negative Responses: ENABLED
8 Done
9 <!--NeedCopy-->
```

Angeben von DNS-Parametern auf Dienst- oder virtueller Serverebene mit der Befehlszeilenschnittstelle

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Konfigurieren Sie das DNS-Profil.

   ```
   add dns profile <dnsProfileName> [-cacheRecords ( ENABLED | DISABLED )]
    [-cacheNegativeResponses (ENABLED | DISABLED )]
   ```

2. Binden Sie das DNS-Profil an den Dienst oder den virtuellen Server.

   So binden Sie das DNS-Profil an den Dienst:

   ```
   set service <name> [-dnsProfileName <string>]
   ```

Beispiel:

```
>set service service1 -dnsProfileName dns_profile1
Done
<!--NeedCopy-->
```

So binden Sie das DNS-Profil an den virtuellen Server:

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

Beispiel:

```
>set lb vserver lbvserver1 -dnsProfileName dns_profile1
Done
<!--NeedCopy-->
```

Angeben von DNS-Parametern auf Dienst- oder virtueller Serverebene mit der GUI

1. Konfigurieren Sie das HTTP-Profil.

   Navigieren Sie zu **System** > **Profile** > **DNS-Profil**, und erstellen Sie das DNS-Profil.

2. Binden Sie das HTTP-Profil an den Dienst oder den virtuellen Server.

   Navigieren Sie zu **Datenverkehrsverwaltung** > **Lastenausgleich**> **Dienste/virtuelle Server**, und erstellen Sie das DNS-Profil, das an den Dienst oder den virtuellen Server gebunden sein muss.

Begrenzende negative Reaktion der Appliance

Sie können einen Schwellenwert für negative Antworten festlegen, die von der Citrix ADC Appliance aus dem Cache bereitgestellt werden. Wenn der Schwellenwert festgelegt ist, bedient die Appliance die Antwort aus dem Cache, bis der Schwellenwert erreicht ist. Sobald der Schwellenwert erreicht ist, löscht die Appliance die Anforderungen, anstatt mit einer NXDOMAIN-Antwort zu antworten.

Das Festlegen eines Grenzwerts für negative Antworten hat folgende Vorteile:

- Speichern Sie die Ressourcen auf der Citrix ADC Appliance.
- Verhindern Sie schädliche Abfragen für nicht vorhandene Domänennamen.

> **Hinweis:** Sie können einen Schwellenwert für negative Antworten nur für die Domänen festlegen, für die die ADC-Appliance als autorisierender Domänennamenserver konfiguriert ist. Sie können keinen Schwellenwert für zwischengespeicherte Datensätze festlegen, die von den autoritativen Backend-Nameservern empfangen wurden.

Rate Begrenzung der negativen Antwort durch den Cache mit der CLI

Geben Sie an der Eingabeaufforderung

```
set dns parameter -NXDOMainRateLimitThreshold <positive-integer>
<!--NeedCopy-->
```

Beispiel:

```
set dns parameter -NXDOMainRateLimitThreshold 1000
<!--NeedCopy-->
```

NXDOMainRateLimitThreshold: Wenn dieser Parameter auf einen positiven ganzzahligen Wert gesetzt ist, werden Antworten aus dem Cache bereitgestellt, bis dieser Schwellenwert (in Sekunden) erreicht ist. Sobald der Schwellenwert überschreitet, werden die Anforderungen gelöscht. Der konfigurierte Schwellenwert ist pro Paketmodul.

Rate Begrenzung der negativen Antwort durch den Cache mit der GUI

1. Navigieren Sie zu **Datenverkehrsverwaltung > DNS**, und klicken Sie auf **DNS-Einstellungen ändern**.
2. Geben **Sie auf der Seite DNS-Parameter konfigurieren** im Feld **NXDOMAIN-Rate Limit Threshold** den Schwellenwert ein, bis zu dem die Antworten aus dem Cache bereitgestellt werden müssen.

Hinweis: Der Wert im **NXDOMAIN Threshold Crossed** zeigt an, wie oft die Anforderungen gelöscht werden, nachdem der Schwellenwert erreicht wurde.

Zwischenspeichern von EDNS0-Client-Subnetzdaten, wenn sich die Citrix ADC Appliance im Proxy-Modus befindet

October 5, 2021

Wenn im Citrix ADC Proxy-Modus ein Back-End-Server, der ein EDNS0 Client Subnet (ECS) unterstützt, eine Antwort mit der ECS-Option sendet, führt die Citrix ADC Appliance Folgendes aus:

- Es leitet die Antwort so weiter an den Kunden und
- Speichert die Antwort zusammen mit den Client-Subnetzinformationen im Cache.

DNS-Anfragen, die aus demselben Subnetz derselben Domäne stammen und für die der Server die gleiche Antwort senden würde, werden dann aus dem Cache bedient.

Hinweis:

- ECS-Caching ist standardmäßig deaktiviert. Aktivieren Sie das Zwischenspeichern von EDNS0-Clientsubnetzdaten im zugehörigen DNS-Profil.
- Die Anzahl der Subnetze, die Sie für eine Domäne zwischenspeichern können, ist auf die verfügbaren Subnetz-IDs beschränkt, d. h. 1270 in der Citrix ADC Appliance. Optional können Sie den Grenzwert auf eine niedrigere Zahl festlegen (Mindestwert: 1 ipv4/ipv6).

Caching von ECS-Antworten mit der CLI aktivieren

Geben Sie an der Eingabeaufforderung Folgendes ein:

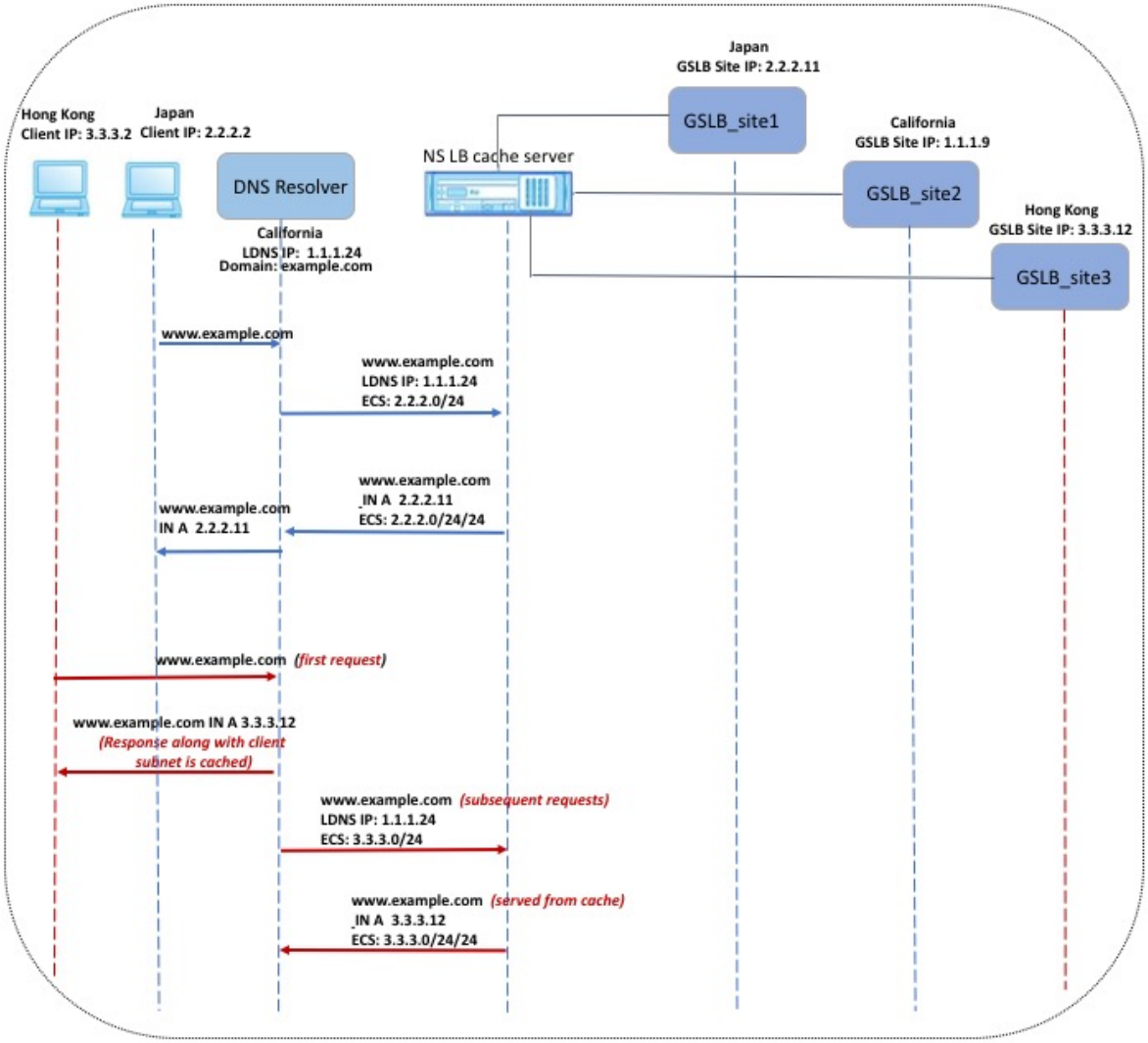
```
set dns profile <dnsProfileName> -cacheECSSubnet ( ENABLED | DISABLED )
```

Begrenzen Sie die Anzahl der Subnetze, die pro Domäne zwischengespeichert werden können, mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set dns profile <dnsProfileName> -maxSubnetsPerDomain <positive_integer>
```

Beispiel:



In dem in der vorherigen Abbildung gezeigten Beispiel sendet der Client unter IP-Adresse 2.2.2.2 eine Anfrage für www.example.com an den DNS-Resolver. Der DNS-Resolver sendet die folgende Antwort:

www.beispiel.com IN A, IP ist 2.2.2.11 und ECS 2.2.2.0/24/24

Zu diesem Zeitpunkt werden die Antwort und der Client-Subnetz-Bezeichner (2.2.2.0/24) zwischengespeichert. Weitere Anfragen von demselben Subnetz und derselben Domäne werden aus dem Cache bedient.

Wenn die IP-Adresse des Clients beispielsweise 2.2.2.100 lautet und die Abfrage für www.example.com gilt, wird die Abfrage aus dem Cache bedient, anstatt an den Back-End-Server gesendet zu werden.

Domänennamen-System-Sicherheitserweiterungen

October 5, 2021

DNS Security Extensions (DNSSEC) ist ein Internet Engineering Task Force (IETF) Standard. Ziel ist es, Datenintegrität und Datenherkunftsauthentifizierung bei der Kommunikation zwischen Nameservern und Clients bereitzustellen und gleichzeitig UDP-Antworten in Klartext zu übertragen. DNSSEC gibt einen Mechanismus an, der asymmetrische Schlüsselkryptographie und einen Satz neuer Ressourceneinträge verwendet, die spezifisch für die Implementierung sind.

Die DNSSEC-Spezifikation ist beschrieben in:

- RFC 4033, "Einführung und Anforderungen der DNS-Sicherheit"
- RFC 4034, "Ressourceneinträge für die DNS-Sicherheitserweiterungen"
- RFC 4035, "Protokolländerungen für die DNS-Sicherheitserweiterungen"

Die operativen Aspekte der Implementierung von DNSSEC innerhalb von DNS werden in RFC 4641, DNSSEC Operational Practices, diskutiert.

Sie können DNSSEC auf dem Citrix ADC konfigurieren. Sie können Schlüssel zum Signieren von DNS-Zonen generieren und importieren. Sie können DNSSEC für Zonen konfigurieren, für die der Citrix ADC autorisierend ist. Sie können den ADC als DNS-Proxyserver für signierte Zonen konfigurieren, die in einer Farm von Back-End-Nameservern gehostet werden. Wenn der ADC für eine Teilmenge der Datensätze autorisierend ist, die zu einer Zone gehören, für die der ADC als DNS-Proxyserver konfiguriert ist, können Sie die Teilmenge der Datensätze in die DNSSEC-Implementierung aufnehmen.

DNSSEC konfigurieren

October 5, 2021

Führen Sie die folgenden Schritte aus, um DNSSEC zu konfigurieren:

1. Aktivieren Sie DNSSEC auf der Citrix ADC Appliance.
2. Erstellen Sie einen Zonensignierungsschlüssel und einen Schlüsselsignierungsschlüssel für die Zone.
3. Fügen Sie die beiden Schlüssel zur Zone hinzu.
4. Unterschreiben Sie die Zone mit den Schlüsseln.

Die Citrix ADC Appliance fungiert nicht als DNSSEC-Resolver. DNSSEC auf dem ADC wird nur in den folgenden Bereitstellungsszenarien unterstützt:

1. ADNS — Citrix ADC ist das ADNS und generiert die Signaturen selbst.
2. Proxy: Citrix ADC fungiert als DNSSEC-Proxy. Es wird davon ausgegangen, dass Citrix ADC in einem vertrauenswürdigen Modus vor den ADNS/LDNS-Servern platziert wird. Der ADC fungiert nur als Proxy-Caching-Entität und überprüft keine Signaturen.

DNSSEC aktivieren und deaktivieren

Aktivieren Sie DNSSEC auf dem Citrix ADC, damit der ADC auf DNSSEC-fähige Clients reagiert. Standardmäßig ist DNSSEC aktiviert.

Sie können die DNSSEC-Funktion deaktivieren, wenn Citrix ADC nicht auf Clients mit DNSSEC-spezifischen Informationen antworten soll.

Aktivieren oder Deaktivieren von DNSSEC mit der CLI

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

```
1 -  set dns parameter -dnssec ( ENABLED | DISABLED )
2 -  show dns parameter
3 <!--NeedCopy-->
```

Beispiel:

```
1 > set dns parameter -dnssec ENABLED
2  Done
3 > show dns parameter
4         DNS parameters:
5         DNS retries: 5
6          .
7          .
8          .
9          DNSEC Extension: ENABLED
10        Max DNS Pipeline Requests: 255
11 Done
12
13 <!--NeedCopy-->
```

Aktivieren oder Deaktivieren von DNSSEC mit der GUI

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Klicken Sie im Detailbereich auf DNS-Einstellungen ändern.
3. Aktivieren oder deaktivieren Sie im Dialogfeld **DNS-Parameter konfigurieren** das Kontrollkästchen **DNSSEC-Erweiterung aktivieren**.

Erstellen von DNS-Schlüsseln für eine Zone

Für jede DNS-Zone, die Sie signieren möchten, müssen Sie zwei Paare asymmetrischer Schlüssel erstellen. Ein Paar, der Zonensignierungsschlüssel (ZSK) genannt, wird verwendet, um alle Ressourcendatensätze in der Zone zu signieren. Das zweite Paar wird als Schlüsselsignierungsschlüssel (Key Signing Key, KSK) bezeichnet und wird verwendet, um nur die DNSKEY-Ressourceneinträge in der Zone zu signieren.

Wenn ZSK und KSK erstellt werden, wird `suffix.key` an die Namen der öffentlichen Komponenten der Schlüssel angehängt. `suffix.private` wird an die Namen ihrer privaten Komponenten angehängt. Das Anhängen erfolgt automatisch.

Der Citrix ADC erstellt auch einen Delegation Signer (DS)-Datensatz und fügt das Suffix .ds an den Namen des Datensatzes an. Wenn es sich bei der übergeordneten Zone um eine signierte Zone handelt, müssen Sie den DS-Eintrag in der übergeordneten Zone veröffentlichen, um die Vertrauensskette einzurichten.

Wenn Sie einen Schlüssel erstellen, wird der Schlüssel im Verzeichnis `/nsconfig/dns/` gespeichert, aber er wird nicht automatisch in der Zone veröffentlicht. Nachdem Sie einen Schlüssel mit dem Befehl `create dns key` erstellt haben, müssen Sie den Schlüssel explizit mit dem Befehl `add dns key` in der Zone veröffentlichen. Der Prozess zum Generieren eines Schlüssels ist getrennt vom Prozess der Veröffentlichung des Schlüssels in einer Zone, damit Sie alternative Mittel zum Generieren von Schlüsseln verwenden können. Sie können beispielsweise Schlüssel importieren, die von anderen Schlüsselgenerierungsprogrammen (z. B. `bind-keygen`) generiert wurden, indem Sie Secure FTP (SFTP) verwenden und dann die Schlüssel in der Zone veröffentlichen. Weitere Informationen zum Veröffentlichen eines Schlüssels in einer Zone finden Sie unter Veröffentlichen eines DNS-Schlüssels in einer Zone.

Führen Sie die in diesem Thema beschriebenen Schritte aus, um einen Zonensignierungsschlüssel zu erstellen, und wiederholen Sie dann die Schritte zum Erstellen eines Schlüsselsignierungsschlüssels. Im Beispiel, das der Befehlssyntax folgt, wird zunächst ein Schlüsselpaar für Zonensignierung für die Zone example.com erstellt. Das Beispiel verwendet dann den Befehl, um ein Schlüsselsignierungsschlüsselpaar für die Zone zu erstellen.

Ab Version 13.0 Build 61.x unterstützt die Citrix ADC Appliance jetzt stärkere Krypto-Algorithmen, wie RSASHA256 und RSASHA512, um eine DNS-Zone zu authentifizieren. Bisher wurde nur der RSASHA1-Algorithmus unterstützt.

Erstellen eines DNS-Schlüssels mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

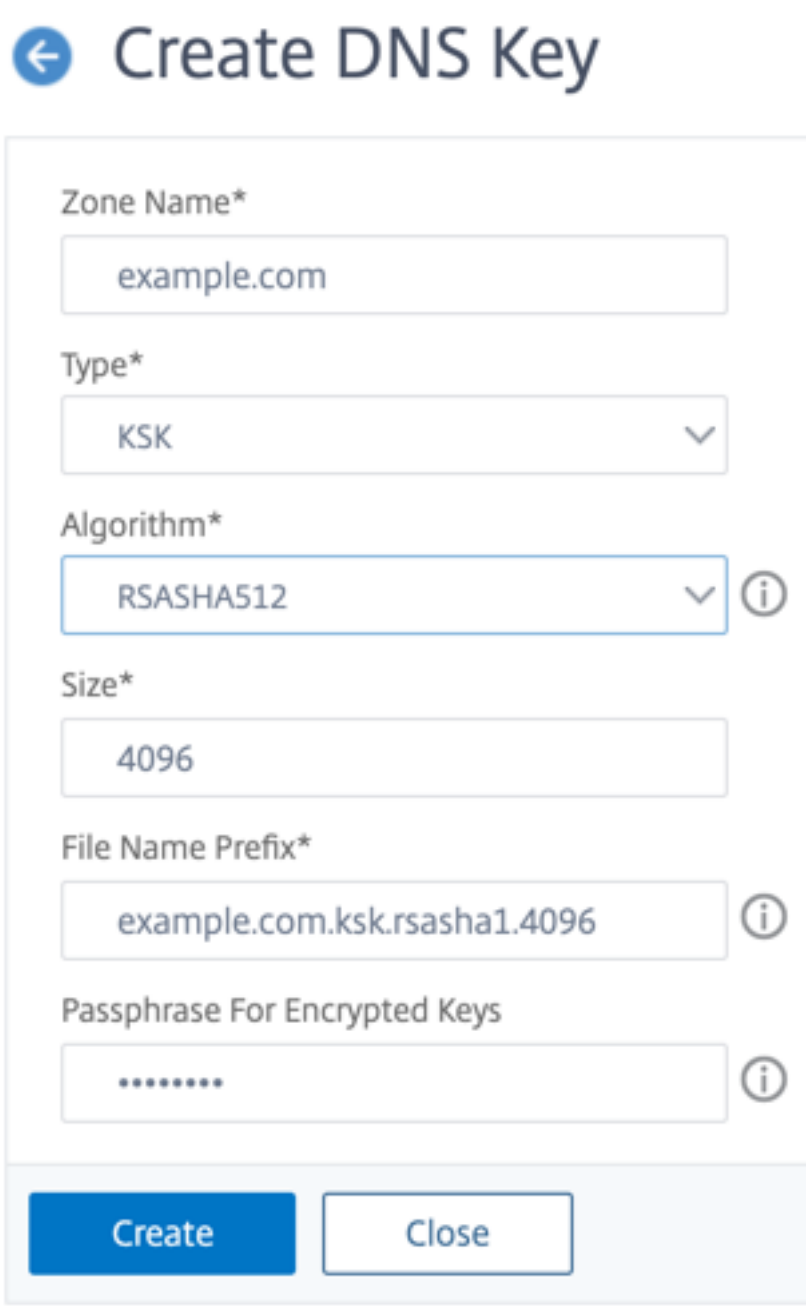
```
create dns key -zoneName <string> -keyType <keyType> -algorithm <algorithm>
 -keySize <positive_integer> -fileNamePrefix <string>
```


Beispiel:

```
> create dns key -zoneName example.com -keyType zsk -algorithm
   RSASHA256 -keySize 1024 -fileNamePrefix example.com.zsk.rsasha1.1024
File Name: /nsconfig/dns/example.com.zsk.rsasha1.1024.key (public); /
   nsconfig/dns/example.com.zsk.rsasha1.1024.private (private); /
   nsconfig/dns/example.com.zsk.rsasha1.1024.ds (ds)
This operation may take some time, Please wait...
 Done
> create dns key -zoneName example.com -keyType ksk -algorithm
   RSASHA512 -keySize 4096 -fileNamePrefix example.com.ksk.rsasha1.4096
File Name: /nsconfig/dns/example.com.ksk.rsasha1.4096.key (public); /
   nsconfig/dns/example.com.ksk.rsasha1.4096.private (private); /
   nsconfig/dns/example.com.ksk.rsasha1.4096.ds (ds)
This operation may take some time, Please wait...
 Done
<!--NeedCopy-->
```

Erstellen eines DNS-Schlüssels mit der GUI

1. Navigieren Sie zu **Traffic Management > DNS**.
2. Klicken Sie im Detailbereich auf **DNS-Schlüssel erstellen**.
3. Geben Sie Werte für die verschiedenen Parameter ein, und klicken Sie auf **Erstellen**.



Hinweis: So ändern Sie das Dateinamenpräfix eines vorhandenen Schlüssels:

- Klicken Sie auf den Pfeil neben der Schaltfläche **Durchsuchen**.
- Klicken Sie entweder auf **Lokal** oder **Appliance** (je nachdem, ob der vorhandene Schlüssel auf Ihrem lokalen Computer oder im `/nsconfig/dns/` Verzeichnis auf der Appliance gespeichert ist).
- Navigieren Sie zum Speicherort des Schlüssels, und doppelklicken Sie dann auf den Schlüssel.
  Das Feld **Dateinamenpräfix** wird nur mit dem Präfix des vorhandenen Schlüssels gefüllt.

Ändern Sie das Präfix entsprechend.

Veröffentlichen eines DNS-Schlüssels in einer Zone

Ein Schlüssel (Zonensignierungsschlüssel oder Schlüsselsignierungsschlüssel) wird in einer Zone veröffentlicht, indem der Schlüssel zur ADC-Appliance hinzugefügt wird. Ein Schlüssel muss in einer Zone veröffentlicht werden, bevor Sie die Zone signieren.

Bevor Sie einen Schlüssel in einer Zone veröffentlichen, muss der Schlüssel im Verzeichnis **/nsconfig/dns/** verfügbar sein. Wenn Sie den DNS-Schlüssel auf einem anderen Computer erstellt haben (z. B. mithilfe des `bind-keygen` Programms), stellen Sie sicher, dass der Schlüssel dem `/nsconfig/dns/` Verzeichnis hinzugefügt wird. Veröffentlichen Sie dann den Schlüssel in der Zone. Verwenden Sie die ADC-GUI, um den Schlüssel zum `/nsconfig/dns/` Verzeichnis hinzuzufügen. Oder verwenden Sie ein anderes Programm, um den Schlüssel in das Verzeichnis zu importieren, z. B. das Secure FTP (SFTP).

Verwenden Sie den `add dns key` Befehl für jedes Public-Private-Schlüsselpaar, das Sie in einer bestimmten Zone veröffentlichen möchten. Wenn Sie ein ZSK-Paar und ein KSK-Paar für eine Zone erstellt haben, verwenden Sie den `add dns key` Befehl, um zuerst eines der Schlüsselpaare in der Zone zu veröffentlichen. Wiederholen Sie den Befehl, um das andere Schlüsselpaar zu veröffentlichen. Für jeden Schlüssel, den Sie in einer Zone veröffentlichen, wird in der Zone ein DNSKEY-Ressourceneintrag erstellt.

Im Beispiel, das der Befehlssyntax folgt, wird zuerst das Schlüsselpaar für die Zonensignierung (das für die Zone example.com erstellt wurde) in der Zone veröffentlicht. Das Beispiel verwendet dann den Befehl, um das Schlüsselsignierungsschlüsselpaar in der Zone zu veröffentlichen.

Veröffentlichen eines Schlüssels in einer Zone mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um einen Schlüssel in einer Zone zu veröffentlichen und die Konfiguration zu überprüfen:

```
1 -  add dns key <keyName> <publickey> <privatekey> [-expires <
    positive_integer> [<units>]] [-notificationPeriod <positive_integer>
     [<units>]] [-TTL <secs>]
2 -  show dns zone [<zoneName> | -type <type>]
3 <!--NeedCopy-->
```

Beispiel:


```
> add dns key example.com.zsk example.com.zsk.rsasha1.1024.key example.com.zsk.rsasha1.1024.private
 Done
> add dns key example.com.ksk example.com.ksk.rsasha1.4096.key example.com.ksk.rsasha1.4096.private
 Done
> show dns zone example.com
         Zone Name : example.com
         Proxy Mode : NO
         Domain Name : example.com
                 Record Types : NS SOA DNSKEY
         Domain Name : ns1.example.com
                 Record Types : A
         Domain Name : ns2.example.com
                 Record Types : A
 Done
<!--NeedCopy-->
```

Veröffentlichen eines Schlüssels in einer DNS-Zone mit der GUI

Navigieren Sie zu **Verkehrsverwaltung > DNS > Schlüssel**.

Hinweis: Um einen Schlüssel hinzuzufügen, der auf dem lokalen Computer gespeichert ist, klicken Sie auf den Pfeil neben der Schaltfläche **Durchsuchen**, klicken Sie auf **Lokal**, navigieren Sie zum Speicherort des Schlüssels, und doppelklicken Sie dann auf den Schlüssel.

Konfigurieren eines DNS-Schlüssels

Sie können die Parameter eines Schlüssels konfigurieren, der in einer Zone veröffentlicht wurde. Sie können die Ablaufzeit, den Benachrichtigungszeitraum und die Gültigkeitsdauer (TTL) des Schlüssels ändern. Wenn Sie die Ablaufzeit eines Schlüssels ändern, signiert die Appliance automatisch alle Ressourcendatensätze in der Zone mit dem Schlüssel neu. Das erneute Signieren geschieht, wenn die Zone mit dem bestimmten Schlüssel signiert ist.

Konfigurieren eines Schlüssels mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um einen Schlüssel zu konfigurieren und die Konfiguration zu überprüfen:

```
-  set dns key <keyName> [-expires <positive_integer> [<units>]] [-notificationPeriod <positive_integer> [<units>]] [-TTL <secs>]
```



```
-  show dns key [<keyName>]
<!--NeedCopy-->
```

Beispiel:

```
> set dns key example.com.ksk -expires 30 DAYS -notificationPeriod 3
   DAYS -TTL 3600
 Done
> show dns key example.com.ksk
1)      Key Name: example.com.ksk
        Expires: 30 DAYS        Notification: 3 DAYS    TTL: 3600
        Public Key File: example.com.ksk.rsasha1.4096.key
        Private Key File: example.com.ksk.rsasha1.4096.private
 Done
<!--NeedCopy-->
```

Konfigurieren eines Schlüssels mit der GUI

1. Navigieren Sie zu **Verkehrsverwaltung > DNS > Schlüssel**.
2. Klicken Sie im Detailbereich auf den Schlüssel, den Sie konfigurieren möchten, und klicken Sie dann auf Öffnen.
3. Ändern Sie im Dialogfeld DNS-Schlüssel konfigurieren die Werte der folgenden Parameter wie gezeigt:
   - Ablaufdatum — expires
   - Benachrichtigungszeitraum — notificationPeriod
   - TTL—TTL
4. Klicken Sie auf OK.

Signieren und Aufheben der Signatur einer DNS-Zone

Um eine DNS-Zone zu sichern, müssen Sie die Zone mit den in der Zone veröffentlichten Schlüsseln signieren. Wenn Sie eine Zone signieren, erstellt Citrix ADC für jeden Besitzernamen einen NSEC-Ressourceneintrag (Next Secure). Anschließend wird der Schlüsselsignierungsschlüssel verwendet, um den DNSKEY-Ressourcendatensatz zu signieren. Schließlich wird das ZSK verwendet, um alle Ressourcendatensätze in der Zone zu signieren, einschließlich der DNSKEY-Ressourcendatensätze und NSEC-Ressourcendatensätze. Jeder Vorzeichenvorgang führt zu einer Signatur für die Ressourcendatensätze in der Zone. Die Signatur wird in einem neuen Ressourceneintrag erfasst, der RRSIG-Ressourceneintrag genannt wird.

Nachdem Sie eine Zone signiert haben, speichern Sie die Konfiguration.

Signieren einer Zone mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine Zone zu signieren und die Konfiguration zu überprüfen:

```
1 -  sign dns zone <zoneName> [-keyName <string> ...]
2 -  show dns zone [<zoneName> | -type (ADNS | PROXY | ALL)]
3 -  save config
4 <!--NeedCopy-->
```

Beispiel:

```
1 > sign dns zone example.com -keyName example.com.zsk example.com.ksk
2  Done
3 > show dns zone example.com
4          Zone Name : example.com
5          Proxy Mode : NO
6          Domain Name : example.com
7                  Record Types : NS SOA DNSKEY RRSIG NSEC
8          Domain Name : ns1.example.com
9                  Record Types : A RRSIG NSEC
10         Domain Name : ns2.example.com
11                 Record Types : A RRSIG
12         Domain Name : ns2.example.com
13                 Record Types : RRSIG NSEC
14 Done
15 > save config
16  Done
17 <!--NeedCopy-->
```

Aufheben der Signatur einer Zone mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die Signierung einer Zone aufzuheben und die Konfiguration zu überprüfen:

```
1 -  unsign dns zone <zoneName> [-keyName <string> ...]
2 -  show dns zone [<zoneName> | -type (ADNS | PROXY | ALL)]
```



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

Beispiel:

```
> unsign dns zone example.com -keyName example.com.zsk example.com.ksk
 Done
> show dns zone example.com
         Zone Name : example.com
         Proxy Mode : NO
         Domain Name : example.com
                 Record Types : NS SOA DNSKEY
         Domain Name : ns1.example.com
                 Record Types : A
         Domain Name : ns2.example.com
                 Record Types : A
 Done
<!--NeedCopy-->
```

Signieren oder Aufheben der Signatur einer Zone mit der GUI

1. Navigieren Sie zu **Verkehrsverwaltung > DNS > Zonen**.
2. Klicken Sie im Detailbereich auf die Zone, die Sie signieren möchten, und klicken Sie dann auf Sign/Unsign.
3. Führen Sie im Dialogfeld DNS-Zone signieren/unsignieren eine der folgenden Aktionen aus:
   - Um die Zone zu signieren, aktivieren Sie die Kontrollkästchen für die Schlüssel (Zonensignierungsschlüssel und Schlüsselsignierungsschlüssel), mit denen Sie die Zone signieren möchten.
     Sie können die Zone mit mehr als einem Zonensignierungsschlüssel oder Schlüsselsignierungsschlüsselpaar signieren.
   - Um die Signierung der Zone aufzuheben, deaktivieren Sie die Kontrollkästchen für die Schlüssel (Zonensignierungsschlüssel und Schlüsselsignierungsschlüssel), mit denen Sie die Signierung der Zone aufheben möchten.
     Sie können die Signierung der Zone mit mehr als einem Zonensignierungsschlüssel oder Schlüsselsignierungsschlüsselpaar aufheben.
4. Klicken Sie auf OK.

Anzeigen der NSEC-Einträge für einen bestimmten Datensatz in einer Zone

Sie können die NSEC-Datensätze anzeigen, die der Citrix ADC automatisch für jeden Eigentümernamen in der Zone erstellt.

Anzeigen des NSEC-Datensatzes für einen bestimmten Datensatz in einer Zone mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um den NSEC-Eintrag für einen bestimmten Datensatz in einer Zone anzuzeigen:

```
show dns nsecRec [<hostName> | -type (ADNS | PROXY | ALL)]
```

Beispiel:

```
> show dns nsecRec example.com
1)      Domain Name : example.com
        Next Nsec Name: ns1.example.com
        Record Types : NS SOA DNSKEY RRSIG NSEC
 Done
<!--NeedCopy-->
```

Anzeigen des NSEC-Datensatzes für einen bestimmten Datensatz in einer Zone mit der GUI

1. Navigieren Sie zu **Datenverkehrsverwaltung > DNS > Datensätze > Nächste sichere Datensätze**.
2. Klicken Sie im Detailbereich auf den Namen des Datensatzes, für den Sie den NSEC-Datensatz anzeigen möchten. Der NSEC-Eintrag für den ausgewählten Datensatz wird im Detailbereich angezeigt.

Entfernen eines DNS-Schlüssels

Entfernen Sie einen Schlüssel aus der Zone, in der er veröffentlicht wird, wenn der Schlüssel abgelaufen ist oder wenn der Schlüssel kompromittiert wurde. Wenn Sie einen Schlüssel aus der Zone entfernen, wird die Zone automatisch mit dem Schlüssel nicht signiert. Wenn Sie den Schlüssel mit diesem Befehl entfernen, werden die im Verzeichnis /nsconfig/dns/ vorhandenen Schlüsseldateien nicht entfernt. Wenn die Schlüsseldateien nicht mehr benötigt werden, müssen sie explizit aus dem Verzeichnis entfernt werden.

Entfernen eines Schlüssels aus dem Citrix ADC mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um einen Schlüssel zu entfernen und die Konfiguration zu überprüfen:

```
-  rm dns key <keyName>
-  show dns key <keyName>
```



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

Beispiel:

```
> rm dns key example.com.zsk
 Done
> show dns key example.com.zsk
ERROR: No such resource [keyName, example.com.zsk]

<!--NeedCopy-->
```

Entfernen eines Schlüssels aus dem Citrix ADC mit der GUI

1. Navigieren Sie zu **Verkehrsverwaltung > DNS > Schlüssel**.
2. Klicken Sie im Detailbereich auf den Namen des Schlüssels, den Sie aus dem ADC entfernen möchten, und klicken Sie dann auf Entfernen.

Konfigurieren von DNSSEC, wenn Citrix ADC für eine Zone autorisierend ist

October 5, 2021

Wenn Citrix ADC für eine bestimmte Zone autorisierend ist, werden alle Ressourceneinträge in der Zone auf dem ADC konfiguriert. Um die autoritative Zone zu signieren, müssen Sie die Zonensignierung und die Schlüsselsignierschlüssel für die Zone erstellen, die Schlüssel zum ADC hinzufügen und dann die Zone signieren. Weitere Informationen:

- Erstellen von DNS-Schlüsseln für eine Zone
- Veröffentlichen eines DNS-Schlüssels in einer Zone
- Unterschreiben und unterschreiben Sie eine DNS-Zone.

Wenn auf dem ADC konfigurierte GSLB-Domänen zur Zone gehören, die signiert wird, werden die GSLB-Domainnamen zusammen mit den anderen Datensätzen, die zur Zone gehören, signiert.

Nachdem Sie eine Zone signiert haben, enthalten Antworten auf Anforderungen von DNSSEC-fähigen Clients die RRSIG-Ressourceneinträge zusammen mit den angeforderten Ressourceneinträgen. DNSSEC muss auf dem ADC aktiviert sein. Weitere Informationen zum Aktivieren von DNSSEC finden Sie unter Aktivieren und Deaktivieren von DNSSEC.

Nachdem Sie DNSSEC für die autorisierende Zone konfiguriert haben, müssen Sie die Citrix ADC Konfiguration speichern.

Konfigurieren von DNSSEC für eine Zone, für die Citrix ADC ein DNS-Proxyserver ist

October 5, 2021

Das Verfahren zum Signieren einer Zone, für die der Citrix ADC als DNS-Proxyserver konfiguriert ist, hängt davon ab, ob der ADC eine Teilmenge der Zoneninformationen besitzt, die den Back-End-Namenservern gehören. Wenn dies der Fall ist, wird die Konfiguration als Teilzoneneigentumskonfigurationbetrachtet. Wenn der ADC keine Teilmenge der Zoneninformationen besitzt, wird die Citrix ADC-Konfiguration zur Verwaltung der Backend-Server als zonenlose DNS-Proxy-Serverkonfiguration betrachtet. Die grundlegenden DNSSEC-Konfigurationsaufgaben für beide Citrix ADC Konfigurationen sind identisch. Das Signieren der Teilzone auf dem Citrix ADC erfordert jedoch einige zusätzliche Konfigurationsschritte.

Hinweis: Die Begriffe zonenlose Proxy-Serverkonfiguration und Teilzone werden nur im Kontext der Citrix ADC Appliance verwendet.

Wichtig: Wenn der ADC im Proxy-Modus konfiguriert ist, führt der ADC keine Signaturüberprüfung für DNSSEC-Antworten durch, bevor er den Cache aktualisiert.

Wenn Sie den ADC als DNS-Proxy für den Lastenausgleich DNSSEC-fähiger Resolver (Server) konfigurieren, müssen Sie bei der Konfiguration des virtuellen DNS-Servers die Option Rekursion verfügbar festlegen. Wenn eine DNSSEC-Abfrage mit dem eingestellten CD-Bit “Checking Disabled” eingeht, wird die Abfrage an den Server weitergegeben, wobei das CD-Bit beibehalten wird. Die Antwort vom Server wird nicht zwischengespeichert.

Konfigurieren von DNSSEC für eine zonenfreie DNS-Proxyserver-Konfiguration

Für eine zonenlose DNS-Proxy-Serverkonfiguration muss die Zonensignierung auf den Back-End-Nameservern durchgeführt werden. Auf dem Citrix ADC konfigurieren Sie den ADC als DNS-Proxyserver für die Zone. Erstellen Sie einen virtuellen Lastausgleichsserver vom Protokolltyp DNS. Konfigurieren Sie Dienste auf dem ADC so, dass sie die Namensserver darstellen. Binden Sie dann die Dienste an den virtuellen Lastausgleichsserver. Weitere Informationen zu diesen Konfigurationsaufgaben finden Sie unter Konfigurieren des NetScaler als DNS-Proxyserver.

Wenn ein Client dem ADC eine DNS-Anforderung mit dem DNSSEC OK (DO) -Bit sendet, überprüft der ADC seinen Cache auf die angeforderten Informationen. Wenn die Ressourceneinträge nicht in seinem Cache verfügbar sind, leitet der ADC die Anfrage an einen der DNS-Nameserver weiter. Anschließend wird die Antwort vom Nameserver an den Client weitergeleitet. Außerdem speichert der ADC die RRSIG-Ressourceneinträge zusammen mit der Antwort vom Nameserver im Cache. Nachfolgende Anforderungen von DNSSEC-fähigen Clients werden vom Cache (einschließlich der RRSIG-Ressourceneinträge) bedient, abhängig vom Time-to-Live (TTL) -Parameter. Wenn ein Client

eine DNS-Anfrage sendet, ohne das DO-Bit festzulegen, antwortet der ADC nur mit den angeforderten Ressourceneinträgen. Es enthält nicht die RRSIG-Ressourceneinträge, die für DNSSEC spezifisch sind.

Konfigurieren von DNSSEC für eine Teilzoneneigentumskonfiguration

In einigen ADC-Konfigurationen kann eine Teilmenge der Ressourceneinträge, die zur Zone gehören, auf dem ADC konfiguriert werden, obwohl die Berechtigung für eine Zone bei den Back-End-Namensservern liegt. Der ADC besitzt (oder ist autorisierend für) nur diese Teilmenge von Datensätzen. Eine solche Teilmenge von Datensätzen kann als *Teilzone* auf dem ADC angesehen werden. Der ADC ist Eigentümer der Teilzone. Alle anderen Datensätze gehören den Back-End-Namenservern.

Eine typische Teilzonenkonfiguration auf dem Citrix ADC wird angezeigt, wenn:

- Global Server Load Balancing (GSLB) -Domänen werden auf dem ADC konfiguriert
- Die GSLB-Domains sind Teil einer Zone, für die die Back-End-Nameserver autorisierend sind.

Die Unterzeichnung einer Zone, die nur eine Teilzone auf dem ADC umfasst, beinhaltet:

- Einschließen der Teilzoneninformationen in den Back-End-Namensserver-Zonendateien
- Signieren der Zone auf den Back-End-Namenservern
- Unterzeichnung der Teilzone auf dem ADC.

Der gleiche Schlüsselsatz muss verwendet werden, um die Zone auf den Nameservern und die Teilzone auf dem ADC zu signieren.

Die Zone auf den Back-End-Namenservern signieren

1. Fügen Sie die in der Teilzone enthaltenen Ressourceneinträge in die Zonendateien der Nameserver ein.
2. Erstellen Sie Schlüssel und verwenden Sie die Schlüssel, um die Zone auf den Back-End-Nameservern zu signieren.

Signieren der Teilzone auf dem Citrix ADC

1. Erstellen Sie eine Zone mit dem Namen der Zone, die den Back-End-Nameservern gehört. Wenn Sie die Teilzone konfigurieren, setzen Sie den ProxyMode-Parameter auf YES. Diese Zone ist die Teilzone, die die Ressourceneinträge des ADC enthält.

   Wenn der Name der Zone, die auf den Back-End-Nameservern konfiguriert ist, beispielsweise example.com lautet, müssen Sie eine Zone mit dem Namen example.com auf dem ADC erstellen. Setzen Sie den ProxyMode-Parameter auf YES. Weitere Informationen zum Hinzufügen einer Zone finden Sie unter Konfigurieren einer DNS-Zone.

> **Hinweis:**
>
> Fügen Sie keine SOA- und NS-Datensätze für die Zone hinzu. Diese Aufzeichnungen müssen auf dem ADC für eine Zone existieren, für die der ADC maßgeblich ist.

2. Importieren Sie die Schlüssel (von einem der Back-End-Nameserver) in den ADC und fügen Sie sie dann dem /nsconfig/dns/ -Verzeichnis hinzu. Weitere Informationen darüber, wie Sie einen Schlüssel importieren und zum ADC hinzufügen können, finden Sie unter Veröffentlichen eines DNS-Schlüssels in einer Zone.
3. Signieren Sie die Teilzone mit den importierten Schlüsseln. Wenn Sie die Teilzone mit den Schlüsseln signieren, generiert der ADC RRSIG- und NSEC-Datensätze für die Ressourceneintragsgruppen bzw. einzelne Ressourceneinträge in der Teilzone. Weitere Informationen zum Signieren einer Zone finden Sie unter Signieren und Aufheben einer DNS-Zone.

Konfigurieren von DNSSEC für globale GSLB-Domänennamen (Server Load Balancing)

October 5, 2021

Wenn GSLB auf dem Citrix ADC konfiguriert ist und der ADC für die Zone, zu der die GSLB-Domänennamen gehören, autorisierend ist, werden alle GLSB-Domänennamen signiert, wenn die Zone signiert wird. Weitere Informationen zum Signieren einer Zone, für die der ADC autoritativ ist, finden Sie unter Konfigurieren von DNSSEC, wenn die Citrix ADC Appliance für eine Zone autoritativ ist.

Wenn die GSLB-Domains zu einer Zone gehören, für die die Back-End-Nameserver autorisierend sind, müssen Sie:

- Unterschreiben Sie zuerst die Zone auf den Nameservern.
- Unterschreiben Sie dann die Teilzone auf dem ADC, um die DNSSEC-Konfiguration für die Zone abzuschließen.

Weitere Informationen finden Sie unter Konfigurieren von DNSSEC für eine Konfiguration des Teilzonenbesitzes.

Zonenwartung

October 5, 2021

Aus DNSSEC-Perspektive umfasst die Zonenwartung das Überführen von Zonensignaturschlüsseln und Schlüsselsignaturschlüsseln, wenn der Schlüsselablauf bevorsteht. Diese Zonenwartungsaufgaben müssen manuell ausgeführt werden. Die Zone wird automatisch neu signiert und erfordert keinen manuellen Eingriff.

Erneut signieren einer aktualisierten Zone

Wenn eine Zone aktualisiert wird (einen Datensatz hinzufügen oder einen vorhandenen Datensatz ändern), signiert die Appliance den neuen (oder geänderten) Datensatz automatisch neu. Wenn eine Zone mehrere Zonensignaturschlüssel enthält, signiert die Appliance den neuen (oder geänderten) Datensatz erneut mit dem Schlüssel, der zum Signieren der Zone verwendet wird.

Überrollen von DNSSEC-Schlüsseln

Hinweis: Führen Sie die DNSSEC-Schlüssel (KSK, ZSK) manuell durch, bevor sie ablaufen.

Auf dem Citrix ADC können Sie die Prepublish- und Double-Signaturmethoden verwenden, um ein Rollover des Zonensignaturschlüssels und des Schlüsselsignaturschlüssels durchzuführen. Weitere Informationen zu diesen beiden Rollover-Methoden finden Sie in RFC 4641, DNSSEC Operational Practices.

Die folgenden Themen ordnen Befehle im ADC den Schritten in den in RFC 4641 beschriebenen Rollover-Prozeduren zu.

Die Schlüsselablaufbenachrichtigung wird über ein SNMP-Trap namens DNSKeyExpiry gesendet. Drei MIB-Variablen, DNSKeyName, DNSKeyTimeToExpire und DNSKeyUnitsOfExpiry werden zusammen mit dem SNMP-Trap DNSKeyExpiry gesendet. Weitere Informationen finden Sie unter *Citrix NetScaler SNMP OID-Referenz* bei NetScaler 12.0 SNMP OID Reference.

Schlüsselrollover für die Vorveröffentlichung

RFC 4641, “DNSSEC Operational Practices” definiert vier Phasen für die prepublish-Key-Rollover-Methode: anfängliche, neue DNSKEY, neue RRSIGs und DNSKEY-Entfernung. Jede Stufe ist mit einer Reihe von Aufgaben verknüpft, die Sie auf dem ADC ausführen müssen. Im Folgenden finden Sie die Beschreibungen der einzelnen Schritte und die Aufgaben, die Sie ausführen müssen. Das hier beschriebene Rollover-Verfahren kann sowohl für Schlüsselsignaturschlüssel als auch für Zonensignaturschlüssel verwendet werden.

- **Stufe 1: Initial.** Die Zone enthält nur die Schlüsselsätze, mit denen die Zone derzeit signiert wurde. Der Status der Zone in der Anfangsphase ist der Zustand der Zone, kurz bevor Sie mit dem Schlüsselrollover-Prozess beginnen.

  Beispiel:

Betrachten Sie den Schlüssel example.com.zsk1, mit dem die Zone example.com signiert ist. Die Zone enthält nur die RRSIGs, die durch den Schlüssel example.com.zsk1 generiert werden, der für den Ablauf fällig ist. Der Schlüsselsignaturschlüssel lautet example.com.ksk1.

- **Stufe 2: Neuer DNSKEY.** Ein neuer Schlüssel wird erstellt und in der Zone veröffentlicht. Das heißt, der Schlüssel wird dem ADC hinzugefügt, aber die Zone wird erst mit dem neuen Schlüssel signiert, wenn die Preroll-Phase abgeschlossen ist. In dieser Phase enthält die Zone den alten Schlüssel, den neuen Schlüssel und die vom alten Schlüssel generierten RRSIGs. Durch die Veröffentlichung des neuen Schlüssels für die gesamte Dauer der Preroll-Phase erhält der DNSKEY-Ressourcendatensatz, der der neuen Schlüsselzeit für die Verbreitung auf die sekundären Nameserver entspricht.

  Beispiel:

  Ein neuer Schlüssel example.com.zsk2 wird zur Zone example.com hinzugefügt. Die Zone wird erst mit example.com.zsk2 signiert, wenn die Pre-Roll-Phase abgeschlossen ist. Die Zone example.com enthält DNSKEY-Ressourceneinträge für example.com.zsk1 und example.com.zsk2.

  Citrix ADC Befehle:

  Führen Sie die folgenden Aufgaben auf dem ADC aus:

  - Erstellen Sie mit dem Befehl `create dns key` einen DNS-Schlüssel.

    Weitere Informationen zum Erstellen eines DNS-Schlüssels, einschließlich eines Beispiels, finden Sie unter Erstellen von DNS-Schlüsseln für eine Zone.

  - Veröffentlichen Sie den neuen DNS-Schlüssel in der Zone mithilfe des`add dns key` Befehls.

    Weitere Informationen zum Veröffentlichen des Schlüssels in der Zone, einschließlich eines Beispiels, finden Sie unter Veröffentlichen eines DNS-Schlüssels in einer Zone.

- **Stufe 3: Neue RRSIGs.** Die Zone wird mit dem neuen DNS-Schlüssel signiert und dann mit dem alten DNS-Schlüssel nicht signiert. Der alte DNS-Schlüssel wird nicht aus der Zone entfernt und bleibt veröffentlicht, bis die vom alten Schlüssel generierten RRSIGs ablaufen.

  Beispiel:

  Die Zone wird mit example.com.zsk2 signiert und dann mit example.com.zsk1 nicht signiert. Die Zone veröffentlicht example.com.zsk1 weiter, bis die von example.com.zsk1 generierten RRSIGs ablaufen.

  Citrix ADC Befehle:

  Führen Sie die folgenden Aufgaben auf dem ADC aus:

  - Signieren Sie die Zone mit dem neuen DNS-Schlüssel mit dem`sign dns zone` Befehl.
  - Heben Sie die Signatur der Zone mit dem alten DNS-Schlüssel mithilfe des`unsign dns zone` Befehls auf.

Weitere Informationen zum Signieren und Aufheben einer Zone, einschließlich Beispielen, finden Sie unter Signieren und Aufheben der Unterzeichnung einer DNS-Zone.

- **Stufe 4: DNSKEY Entfernung.** Wenn die vom alten DNS-Schlüssel generierten RRSIGs ablaufen, wird der alte DNS-Schlüssel aus der Zone entfernt.

  Beispiel:

  Der alte DNS-Schlüssel example.com.zsk1 wird aus der Zone example.com entfernt.

  Citrix ADC Befehle

  Auf dem ADC entfernen Sie den alten DNS-Schlüssel mit dem Befehl `rm dns key`. Weitere Informationen zum Entfernen eines Schlüssels aus einer Zone, einschließlich eines Beispiels, finden Sie unter Entfernen eines DNS-Schlüssels.

Doppelte Signaturschlüssel Rollover

RFC 4641, DNSSEC Operational Practices definiert drei Stufen für Doppelsignaturschlüssel Rollover: anfängliche, neue DNSKEY und DNSKEY Entfernung. Jede Stufe ist mit einer Reihe von Aufgaben verknüpft, die Sie auf dem ADC ausführen müssen. Im Folgenden finden Sie die Beschreibungen der einzelnen Schritte und die Aufgaben, die Sie ausführen müssen. Das hier beschriebene Rollover-Verfahren kann sowohl für Schlüsselsignaturschlüssel als auch für Zonensignaturschlüssel verwendet werden.

- **Stufe 1: Initial.** Die Zone enthält nur die Schlüsselsätze, mit denen die Zone derzeit signiert wurde. Der Status der Zone in der Anfangsphase ist der Zustand der Zone, kurz bevor Sie mit dem Schlüsselrollover-Prozess beginnen.

  Beispiel:

  Betrachten Sie den Schlüssel example.com.zsk1, mit dem die Zone example.com signiert ist. Die Zone enthält nur die RRSIGs, die durch den Schlüssel example.com.zsk1 generiert werden, der für den Ablauf fällig ist. Der Schlüsselsignaturschlüssel lautet example.com.ksk1.

- **Stufe 2: Neuer DNSKEY.** Der neue Schlüssel wird in der Zone veröffentlicht und die Zone ist mit dem neuen Schlüssel signiert. Die Zone enthält die RRSIGs, die von den alten und den neuen Schlüsseln generiert werden. Die Mindestdauer, für die die Zone beide Sätze von RRSIGs enthalten muss, ist die Zeit, die benötigt wird, bis alle RRSIGs ablaufen.

  Beispiel:

  Ein neuer Schlüssel example.com.zsk2 wird zur Zone example.com hinzugefügt. Die Zone ist mit example.com.zsk2 signiert. Die example.com-Zone enthält nun die von beiden Schlüsseln generierten RRSIGs.

  Citrix ADC Befehle

Führen Sie die folgenden Aufgaben auf dem ADC aus:

- Erstellen Sie mit dem Befehl `create dns key` einen DNS-Schlüssel.

  Weitere Informationen zum Erstellen eines DNS-Schlüssels, einschließlich eines Beispiels, finden Sie unter Erstellen von DNS-Schlüsseln für eine Zone.

- Veröffentlichen Sie den neuen Schlüssel in der Zone mithilfe des`add dns key` Befehls.

  Weitere Informationen zum Veröffentlichen des Schlüssels in der Zone, einschließlich eines Beispiels, finden Sie unter Veröffentlichen eines DNS-Schlüssels in einer Zone.

- Signieren Sie die Zone mit dem neuen Schlüssel, indem Sie den`sign dns zone` Befehl verwenden.

  Weitere Informationen zum Signieren einer Zone, einschließlich Beispielen, finden Sie unter Signieren und Aufheben einer DNS-Zone.

- **Stufe 3: DNSKEY Entfernung.** Wenn die vom alten DNS-Schlüssel generierten RRSIGs ablaufen, wird der alte DNS-Schlüssel aus der Zone entfernt.

  Beispiel:

  Der alte DNS-Schlüssel example.com.zsk1 wird aus der Zone example.com entfernt.

  Citrix ADC Befehle:

  Auf dem ADC entfernen Sie den alten DNS-Schlüssel mit dem Befehl `rm dns key`.

  Weitere Informationen zum Entfernen eines Schlüssels aus einer Zone, einschließlich eines Beispiels, finden Sie unter Entfernen eines DNS-Schlüssels.

DNSSEC-Vorgänge an Citrix ADC auslagern

October 5, 2021

Für DNS-Zonen, für die Ihre DNS-Server autorisierend sind, können DNSSEC-Vorgänge auf die ADC-Appliance übertragen werden. In einer DNSSEC-Offloading-Bereitstellung sendet ein DNS-Server nicht signierte Antworten. Der ADC signiert die Antwort dynamisch, bevor er sie an den Client weiterleitet. Der ADC speichert auch die signierte Antwort. Neben der Verringerung der Belastung der DNS-Server bietet das Auslagern von DNSSEC-Vorgängen an den ADC folgende Vorteile:

- Sie können Datensätze signieren, die von den DNS-Servern programmgesteuert generiert werden. Solche Datensätze können nicht durch routinemäßige Zonensignierungsvorgänge signiert werden, die auf den DNS-Servern ausgeführt werden.
- Sie können signierte Antworten an Clients senden, auch wenn Sie DNSSEC auf Ihren Servern nicht implementiert haben.

Zum Einrichten der DNSSEC-Abladung müssen Sie einen virtuellen DNS-Lastausgleichsserver konfigurieren, Dienste konfigurieren, die die DNS-Server darstellen, und dann die Dienste an den virtuellen Server binden. Informationen zum Konfigurieren eines virtuellen DNS-Lastenausgleichsservers, zum Konfigurieren von Diensten und zum Binden der Dienste an den virtuellen Server finden Sie unter Konfigurieren einer DNS-Zone.

Erstellen Sie eine Zonen-Entity auf dem ADC für jede DNS-Zone, deren DNSSEC-Vorgänge Sie auslagern möchten. Für jede DNS-Zone müssen Sie die Parameter Proxy Mode und DNSSEC Offload aktivieren. Sie können optional die NSEC-Datensatzgenerierung für eine ausgelagerte Zone konfigurieren. Um eine DNS-Zonenentität für DNSSEC-Abladung zu erstellen, folgen Sie den Anweisungen in diesem Thema.

Um die Konfiguration abzuschließen, müssen Sie DNS-Schlüssel für die Zone generieren, die Schlüssel zur Zone hinzufügen und dann die Zone mit den Schlüsseln signieren. Dieser Prozess ist der gleiche wie für normale DNSSEC. Informationen zum Erstellen von Schlüsseln, zum Hinzufügen von Schlüsseln zu einer Zone und zum Signieren der Zone finden Sie unter Sicherheitserweiterungen für Domänennamen.

Nachdem Sie DNS-Abladung konfiguriert haben, müssen Sie den DNS-Cache auf dem Citrix ADC leeren. Durch das Leeren des DNS-Cache wird sichergestellt, dass alle nicht signierten Datensätze im Cache entfernt und dann durch signierte Datensätze ersetzt werden. Informationen zum Löschen des DNS-Caches finden Sie unter Flush DNS-Datensätze.

Aktivieren der DNSSEC-Abladung für eine Zone mit der CLI

Geben Sie in der Befehlszeile die folgenden Befehle ein, um DNSSEC-Verschiebung für eine Zone zu aktivieren und die Konfiguration zu überprüfen:

```
1 -  add dns zone <zoneName> -proxyMode YES -dnssecOffload ENABLED [-nsec
      ( ENABLED | DISABLED )
2 -  show dns zone
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add dns zone example.com -proxyMode YES -dnssecOffload ENABLED nsec
     ENABLED
2  Done
3 > show dns zone example.com
4       Zone Name : example.com
5       Proxy Mode : YES
```



```
6       DNSSEC Offload: ENABLED    NSEC: ENABLED
7   Done
8 <!--NeedCopy-->
```

Aktivieren der DNSSEC-Abladung für eine Zone mit der GUI

1. Navigieren Sie zu **Verkehrsverwaltung > DNS > Zonen**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Klicken Sie auf Hinzufügen, um eine Zone auf dem Citrix ADC zu erstellen.
   - Um DNSSEC-Abladung für eine vorhandene Zone zu konfigurieren, doppelklicken Sie auf die Zone.
3. Aktivieren Sie im Dialogfeld DNS-Zone erstellen oder DNS-Zone konfigurieren die Kontrollkästchen Proxymodus und DNSSEC-Abladung.
4. Aktivieren Sie optional das Kontrollkästchen NSEC, wenn Citrix ADC NSEC-Einträge für die Zone generieren soll.

Unterstützung für Administratorpartition für DNSSEC

October 5, 2021

In einer partitionierten Citrix ADC Appliance werden die generierten DNS-Schlüssel an den folgenden Speicherorten gespeichert:

- Standardpartition: /nsconfig/dns/
- Nicht-Standard-Partition: /nsconfig/partitions/<partitionname>/dns/

Sie können nun dem DNS-Schlüssel ein Kennwort hinzufügen. Um dem DNS-Taste ein Kennwort hinzuzufügen, müssen Sie zuerst das Kennwort im `create dns key` Befehl hinzufügen. Geben Sie dann im `add dns key` Befehl das gleiche Kennwort an, wenn Sie der ADC-Appliance den DNS-Schlüssel hinzufügen. Beispiel:

```
create dns key -zoneName com -keytype ksK -algorithm rsASHA1 -keysize 4096
- fileNamePrefix com.ksk.rsasha1.4096 -password 1jsfd3Wa

add dns key com.zsk.4096 /nsconfig/dns/com.zsk.rsasha1.4096.private -
password 1jsfd3Wa
```

Hinweis:

- Für eine standardmäßige partitionierte Umgebung werden die Schlüssel aus dem Standardspeicherort/nsconfig/dns/ gelesen. Wenn die Schlüssel jedoch an einem anderen Ort gespeichert sind, muss der Pfadname im `add dns key -private` Befehl angegeben werden. Beispiel: `add dns key -private <path name>`.

- Für eine nicht standardmäßige partitionierte Umgebung werden die Schlüssel vom Standardspeicherort gelesen /nsconfig/partitions/<partitionname>/dns/.

Unterstützung von Wildcard-DNS-Domänen

October 5, 2021

Wildcard-DNS-Domänen werden verwendet, um Anfragen nach nicht existierenden Domains und Subdomains zu bearbeiten. Verwenden Sie in einer Zone Platzhalterdomänen, um Abfragen für alle nicht vorhandenen Domänen oder Subdomains auf einen bestimmten Server umzuleiten, anstatt für jede Domäne einen separaten Ressourceneintrag (RR) zu erstellen. Die häufigste Verwendung einer Wildcard-DNS-Domäne besteht darin, eine Zone zu erstellen, die verwendet werden kann, um E-Mails aus dem Internet an ein anderes E-Mail-System weiterzuleiten.

In der DNS-Auflösung unterstützen Wildcard-RRs die Platzhalterdomäne. Die Platzhalter-RRs werden verwendet, um die Antworten auf Abfragen für einen nicht vorhandenen Domänennamen zu synthetisieren. Wenn Sie beispielsweise abgefragt `http://image.example.com`haben und die Subdomain “image” nicht existiert hat, werden Sie möglicherweise zu example.com weitergeleitet.

Ein Platzhalterdatensatz hat ein Sternchen (*) als die ganz links markierte Bezeichnung eines Domänennamens. Beispiel: `*.example.com`. Ein Sternchen an einer anderen Stelle im Domänennamen bedeutet einen Platzhalter-DNS-Eintrag. Zum Beispiel **new**`.*.example.com` ist kein gültiger Platzhalter-DNS-Eintrag.

> **Hinweis:**
>
> - Platzhalterdomäne wird nur unterstützt, wenn die Citrix ADC Appliance autorisierend für die Zone ist und als ADNS- oder DNS-Proxyserver konfiguriert ist.
> - Platzhalterdomäne wird für NS- und SOA-Einträge nicht unterstützt.
> - Platzhalterdomäne kann nicht angewendet werden, wenn sich die Abfrage in einer anderen Zone befindet.
> - Platzhalterdomäne kann nicht angewendet werden, wenn der QNAME oder ein Name zwischen der Platzhalterdomäne und dem QNAME bekanntermaßen vorhanden ist.

Beispielkonfiguration

```
1 add dns soaRec example.com -originServer n1.example.com -contact admin.
     example.com
2
3 add dns nsRec example.com n1.example.com
4
```



```
add dns nsRec example.com n2.example.com

add dns zone example.com  -proxyMode no

add dns addrec www.example.com 2.2.2.2

add dns addrec *.example.com 10.10.10.10

add dns addrec *.example.com 10.10.10.11

add dns aaaarec *.example.com 2001::1
<!--NeedCopy-->
```

Im Beispiel wird ein Platzhalterdomänenname für einen A- und AAAA-Datensatz hinzugefügt.

Wenn eine Abfrage für einen Domänennamen empfangen wird, der in der Zone vorhanden ist, antwortet die Citrix ADC Appliance mit der entsprechenden Antwort. Zum `www.example.com` Beispiel antwortet die Appliance mit 2.2.2.2 im Beispiel.

Für einen nicht vorhandenen Domänennamen, der mit einem Platzhaltertyp übereinstimmt, wird eine synthetisierte Antwort geliefert.

Im Beispiel antwortet die Citrix ADC Appliance mit 10.10.10.10 und 10.10.10.11 auf einen Domainnamen nonexist.example.com oder xyz.example.com.

Die Platzhaltersynthese gilt nicht für einen Domainnamen, der in der Zone existiert.

Beispielsweise wird für die Abfrage `www.example.com` und der Typ AAAA die Citrix ADC Appliance nicht mit Platzhaltern synthetisiert, da sie mit Typ A `www.example.com` existiert. Im Beispiel reagiert die Citrix ADC Appliance mit einer NODATA-Antwort.

Für eine Abfrage sagen wir abc.example.com und geben Sie AAAA ein, die Citrix ADC Appliance antwortet mit einer synthetisierten Antwort. Zum `www.example.com`Beispiel antwortet die Appliance mit 2001:: 1 im Beispiel.

Minderung von DNS-DDoS-Angriffen

October 5, 2021

DNS-Server sind eine der wichtigsten Komponenten eines Netzwerks und müssen vor Angriffen geschützt werden. Eine der grundlegendsten Arten von DNS-Angriffen ist der DDoS-Angriff. Angriffe dieser Art sind auf dem Vormarsch und können destruktiv sein. Sie können Folgendes tun, um DDoS-Angriffe abzuschwächen:

- Flush negativer Einträge.

- Beschränken Sie die Lebenszeit (TTL) negativer Einträge.
- Bewahren Sie Citrix ADC-Speicher auf, indem Sie den vom DNS-Cache verbrauchten Speicher einschränken.
- Behalten Sie DNS-Einträge im Cache bei.
- Aktivieren Sie den DNS-Cache-Umgehung.

Negative Datensätze leeren

Ein DNS-Angriff füllt den Cache mit negativen Datensätzen (NXDOMAIN und NODATA). Daher werden Antworten auf legitime Anforderungen nicht zwischengespeichert, so dass neue Anforderungen an einen Back-End-Server zur DNS-Auflösung gesendet werden. Die Antworten verzögern sich daher.

Sie können jetzt die negativen DNS-Einträge aus dem DNS-Cache der Citrix ADC Appliance leeren.

Leeren negativer Cache-Datensätze mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
flush dns proxyrecords -type (dnsRecordType | negRecType)NXDOMAIN | NODATA
```

Beispiel:

```
flush dns proxyrecords -negRecType NODATA
```

Leeren von negativen Cache-Datensätzen mit der GUI

1. Navigieren Sie zu **Konfiguration** > **Datenverkehrsverwaltung** > **DNS** > **Datensätze**.
2. Klicken Sie im Detailbereich auf " **Proxy-Datensätze leeren**".
3. Wählen Sie im Feld **Flush Type** die Option **Negative Datensätze** aus.
4. Wählen Sie im Feld **Negative Datensatztyp** entweder **NXDOMAIN** oder **NODATA** aus.

Schutz vor zufälligen Subdomain- und NXDOMAIN-Angriffen

Um zufällige Subdomain- und NXDOMAIN-Angriffe zu verhindern, können Sie den DNS-Cachespeicher einschränken und die TTL-Werte für negative Datensätze anpassen.

Um die vom DNS-Cache verbrauchte Speichermenge zu begrenzen, geben Sie die maximale Cachegröße (in MB) und auch die Cachegröße (in MB) zum Speichern negativer Antworten an. Wenn eine der beiden Grenzwerte erreicht ist, werden dem Cache keine weiteren Einträge hinzugefügt. Außerdem werden Syslog-Nachrichten protokolliert, und wenn Sie SNMP-Traps konfiguriert haben, werden SNMP-Traps generiert. Wenn diese Grenzwerte nicht festgelegt sind, wird das Caching fortgesetzt, bis der Systemspeicher erschöpft ist.

Ein höherer TTL-Wert für negative Datensätze kann dazu führen, dass Datensätze gespeichert werden, die lange Zeit nicht wertvoll sind. Ein niedrigerer TTL-Wert führt dazu, dass weitere Anforderungen an den Back-End-Server gesendet werden.

Die TTL des negativen Datensatzes wird auf einen Wert gesetzt, der der kleinere des TTL-Werts oder der Wert "Expires" des SOA-Datensatzes sein kann.

Hinweis:

- Diese Einschränkung wird pro Paket-Engine hinzugefügt. Wenn beispielsweise MaxCache-Size auf 5 MB festgelegt ist und die Appliance über 3 Paketmodule verfügt, beträgt die Gesamtcachegröße 15 MB.
- Die Cachegröße für die negativen Datensätze muss kleiner oder gleich der maximalen Cachegröße sein.
- Wenn Sie das DNS-Cache-Speicherlimit auf einen Wert reduzieren, der niedriger ist als die Menge der bereits zwischengespeicherten Daten, bleibt die Cachegröße über dem Limit, bis die Daten älter werden. Das heißt, es übersteigt TTL0 oder ist geleert (Befehl `flush dns proxyrecords` oder Flush Proxy Records in der Citrix ADC GUI).
- Informationen zum Konfigurieren von SNMP-Traps finden Sie unter Konfigurieren des NetScaler zum Generieren von SNMP-Traps.

Beschränken Sie den vom DNS-Cache belegten Speicher mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set dns parameter -maxCacheSize <MBytes> -maxNegativeCacheSize <MBytes>
```

Beispiel:

```
set dns parameter - maxCacheSize 100 -maxNegativeCacheSize 25
```

Beschränken Sie den vom DNS-Cache belegten Speicher mit der GUI

Navigieren Sie zu **Konfiguration** > **Verkehrsverwaltung** > **DNS**, klicken Sie auf **DNS-Einstellungen ändern**, und legen Sie die folgenden Parameter fest:

- Max. Cachegröße in MB
- Maximale negative Cachegröße in MB

Beschränken Sie die TTL negativer Datensätze mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set dns parameter -maxnegcacheTTL <secs>
```

Beispiel:


```
set dns parameter -maxnegcacheTTL 360
```

Beschränken Sie die TTL negativer Datensätze mit der GUI

1. Navigieren Sie zu **Konfiguration** > **Datenverkehrsverwaltung** > **DNS**.
2. Klicken Sie auf **DNS-Einstellungen ändern**, und legen Sie den Parameter **Max Negative Cache TTL in sec** fest.

DNS-Einträge im Cache aufbewahren

Ein Angriff kann den DNS-Cache mit nicht wichtigen Einträgen überfluten, kann jedoch dazu führen, dass die bereits zwischengespeicherten legitimen Datensätze geleert werden, um Platz für die neuen Einträge zu schaffen. Um zu verhindern, dass Angriffe den Cache mit ungültigen Daten füllen, können Sie die legitimen Datensätze beibehalten, auch wenn sie ihre TTL-Werte überschreiten.

Wenn Sie den Parameter CacheNoExpire aktivieren, werden die aktuell im Cache befindlichen Datensätze beibehalten, bis Sie den Parameter deaktivieren.

Hinweis:

- Diese Option kann nur verwendet werden, wenn die maximale Cache-Größe angegeben ist (Parameter MaxCacheSize).
- Wenn maxnegcacheTTL konfiguriert ist und cacheNoExpire aktiviert ist, hat cacheNoExpire Priorität.

Behalten Sie DNS-Einträge im Cache mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set dns parameter -cacheNoExpire ( ENABLED | DISABLED)
```

Beispiel:

```
set dns parameter -cacheNoExpire ENABLED
```

Behalten Sie DNS-Einträge im Cache mit der GUI

1. Navigieren Sie zu **Konfiguration** > **Verkehrsverwaltung** > **DNS**, und klicken Sie auf **DNS-Einstellungen ändern**.
2. Wählen Sie **Cache läuft nicht ab** aus.

DNS-Cache-Umgehung aktivieren

Um die Transparenz und Kontrolle über DNS-Anforderungen zu verbessern, legen Sie den Parameter cachehitBypass so fest, dass er alle Anforderungen an die Back-End-Server weiterleitet und den Aufbau des Cache zulässt, aber nicht verwendet wird. Nachdem der Cache erstellt wurde, können Sie den Parameter deaktivieren, damit Anforderungen aus dem Cache bedient werden.

Aktivieren des DNS-Cache-Umgehens mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set dns parameter -cacheHitBypass ( ENABLED | DISABLED )
```

Beispiel:

```
set dns parameter -cacheHitBypass ENABLED
```

Aktivieren des DNS-Cache-Umgehens mit der GUI

1. Navigieren Sie zu **Konfiguration** > **Verkehrsverwaltung** > **DNS**, und klicken Sie auf **DNS-Einstellungen ändern**.
2. Wählen Sie **Cache Hit Bypass** aus.

`Slowloris`-Angriff verhindern

Eine DNS-Abfrage, die mehrere Pakete umfasst, stellt die potenzielle Bedrohung eines `Slowloris`-Angriffs dar. Die Citrix ADC Appliance kann DNS-Abfragen, die in mehrere Pakete aufgeteilt sind, im Hintergrund löschen.

Sie können den Parameter `splitPktQueryProcessing` auf ALLOW oder DROP eine DNS-Abfrage festlegen, wenn die Abfrage in mehrere Pakete aufgeteilt ist.

Hinweis: Diese Einstellung gilt nur für DNS-TCP.

Beschränken Sie die DNS-Abfragen auf ein einzelnes Paket mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set dns parameter -splitPktQueryProcessing ( ALLOW | DROP )
```

Beispiel:

```
set dns parameter -splitPktQueryProcessing DROP
```


Beschränken von DNS-Abfragen auf ein einzelnes Paket mit der GUI

1. Navigieren Sie zu **Konfiguration** > **Verkehrsverwaltung** > **DNS**, und klicken Sie auf **DNS-Einstellungen ändern**.
2. Wählen Sie im Feld **Split Packet Query Processing** die Option **ALLOW** oder **DROP**.

Sammeln Sie Statistiken der DNS-Antworten, die aus dem Cache bereitgestellt werden

Sie können Statistiken der DNS-Antworten sammeln, die aus dem Cache bereitgestellt werden. Verwenden Sie dann diese Statistiken, um einen Schwellenwert zu erstellen, über den hinaus mehr DNS-Datenverkehr fallen gelassen wird, und setzen Sie diesen Schwellenwert mit einer bandbreitenbasierten Richtlinie durch. Zuvor war die Bandbreitenberechnung für einen virtuellen DNS-Lastausgleichsserver nicht korrekt, da die Anzahl der vom Cache bereitgestellten Anforderungen nicht gemeldet wurde.

Im Proxy-Modus werden die Statistiken für Anforderungsbytes, Antwortbytes, empfangene Gesamtpakete und Gesamtzahl der gesendeten Pakete kontinuierlich aktualisiert. Zuvor wurden diese Statistiken nicht immer aktualisiert, insbesondere für einen virtuellen DNS-Lastausgleichsserver.

Im Proxymodus können Sie nun auch die Anzahl der DNS-Antworten ermitteln, die aus dem Cache bereitgestellt werden. Um diese Statistiken zu sammeln, wurden dem `stat lb vserver <DNSvirtualServerName>` Befehl die folgenden Optionen hinzugefügt:

- **Anfragen** — Gesamtanzahl der Anfragen, die vom DNS- oder DNS_TCP-Server empfangen wurden. Enthält die an das Back-End weitergeleiteten Anforderungen und die aus dem Cache beantworteten Anforderungen.
- **Vserver-Treffer** : Gesamtzahl der Anfragen, die an das Back-End weitergeleitet wurden. Die Anzahl der Anfragen, die aus dem Cache bereitgestellt werden, ist die Differenz zwischen der Gesamtzahl der Anfragen und der Anzahl der vom virtuellen Server bereitgeSTELLTEN Anforderungen.
- **Antworten** — Gesamtanzahl der von diesem virtuellen Server gesendeten Antworten. Wenn beispielsweise ein virtueller DNS-LB-Server 5 DNS-Anforderungen empfangen hat, 3 von ihnen an das Back-End weitergeleitet und 2 von ihnen aus dem Cache bereitgestellt werden, würde der entsprechende Wert jeder dieser Statistiken wie folgt lauten:
  - **Vserver Treffer**: 3
  - **Anfragen**: 5
  - **Antworten**: 5

Firewall-Lastenausgleich

October 5, 2021

Der Firewall-Lastausgleich verteilt den Datenverkehr auf mehrere Firewalls und bietet Fehlertoleranz und erhöhten Durchsatz. Der Firewall-Lastenausgleich schützt Ihr Netzwerk durch:

- Unterteilen der Last zwischen den Firewalls, wodurch ein einzelner Fehlerpunkt beseitigt wird und das Netzwerk skaliert werden kann.
- Erhöhte Hochverfügbarkeit.

Das Konfigurieren einer Citrix ADC Appliance für den Firewall-Lastausgleich ähnelt dem Konfigurieren des Lastenausgleichs, mit der Ausnahme, dass der empfohlene Diensttyp ANY ist, der empfohlene Überwachungstyp PING ist und der Modus für den Lastenausgleich auf MAC festgelegt ist.

Sie können den Firewall-Lastausgleich in einem Sandwich, einer Enterprise- oder einer Multiple-Firewall-Umgebungskonfiguration einrichten. Die Sandwich-Umgebung wird für den Lastenausgleich von außen in das Netzwerk eintretenden Datenverkehr und den Datenverkehr, der das Netzwerk ins Internet verlässt, verwendet und beinhaltet die Konfiguration von zwei Citrix ADC Appliances, jeweils eine auf jeder Seite eines Firewalls. Sie konfigurieren eine Unternehmensumgebung für den Lastenausgleich Datenverkehr, der das Netzwerk zum Internet verlässt. Die Unternehmensumgebung umfasst die Konfiguration einer einzelnen Citrix ADC Appliance zwischen dem internen Netzwerk und den Firewalls, die Zugriff auf das Internet ermöglichen. Die Multiple-Firewall-Umgebung wird für den Lastausgleich verwendet, der von einer anderen Firewall stammt. Wenn der Firewall-Lastausgleich auf beiden Seiten der Citrix ADC Appliance aktiviert ist, verbessert der Datenverkehr sowohl in der Aus- als auch in der Einlaufrichtung und sorgt für eine schnellere Verarbeitung des Datenverkehrs. Die Umgebung mit mehreren Firewalls umfasst die Konfiguration einer Citrix ADC Appliance zwischen zwei Firewalls.

Wichtig: Wenn Sie statische Routen auf der Citrix ADC Appliance für die Ziel-IP-Adresse konfigurieren und den L3-Modus aktivieren, verwendet die Citrix ADC-Appliance ihre Routingtabelle, um den Datenverkehr zu leiten, anstatt den Datenverkehr an den Load Balancing vserver zu senden.

Hinweis: Damit FTP funktioniert, sollte ein zusätzlicher virtueller Server oder Dienst auf der Citrix ADC Appliance mit IP-Adresse und Port als * bzw. 21 konfiguriert werden und der als FTP angegebene Servicetyp. In diesem Fall verwaltet die Citrix ADC Appliance das FTP-Protokoll, indem sie die FTP-Steuerverbindung akzeptiert, die Nutzlast modifiziert und die Datenverbindung über dieselbe Firewall verwaltet.

Firewall Load Balancing unterstützt nur einige der Lastausgleichsmethoden, die von der Citrix ADC Appliance unterstützt werden. Außerdem können Sie nur wenige Arten von Persistenz und Monitoren konfigurieren.

Firewall-Load-Balancing-Methoden

Die folgenden Lastenausgleichsmethoden werden für den Lastenausgleich der Firewall unterstützt.

- Geringste Verbindungen

- Runde Robin
- Am wenigsten Pakete
- Geringste Bandbreite
- Quell-IP-Hash
- Ziel-IP-Hash
- Quell-IP-Ziel-IP-Hash
- Quell-IP-Quellport-Hash
- Methode für die geringste Antwortzeit (LRTM)
- Benutzerdefinierte Last

Firewall-Persistenz

Für den Lastenausgleich der Firewall werden nur SOURCEIP-, DESTIP- und SOURCEIPDESTIP-basierte Persistenz unterstützt.

Firewall-Server-Überwachung

Nur PING und transparente Monitore werden beim Lastenausgleich der Firewall unterstützt. Sie können einen PING-Monitor (Standard) an den Backend-Dienst binden, der die Firewall darstellt. Wenn eine Firewall so konfiguriert ist, dass sie nicht auf Ping-Pakete reagiert, können Sie transparente Monitore konfigurieren, um Hosts auf der vertrauenswürdigen Seite über einzelne Firewalls zu überwachen.

Sandwich-Umgebung

December 7, 2021

Eine Citrix ADC Bereitstellung in einem Sandwich-Modus kann den Netzwerkverkehr durch Firewalls in beide Richtungen ausgleichen: Eindringen (Datenverkehr, der von außen in das Netzwerk gelangt, z. B. das Internet) und Ausstieg (Datenverkehr, der das Netzwerk dem Internet verlässt).

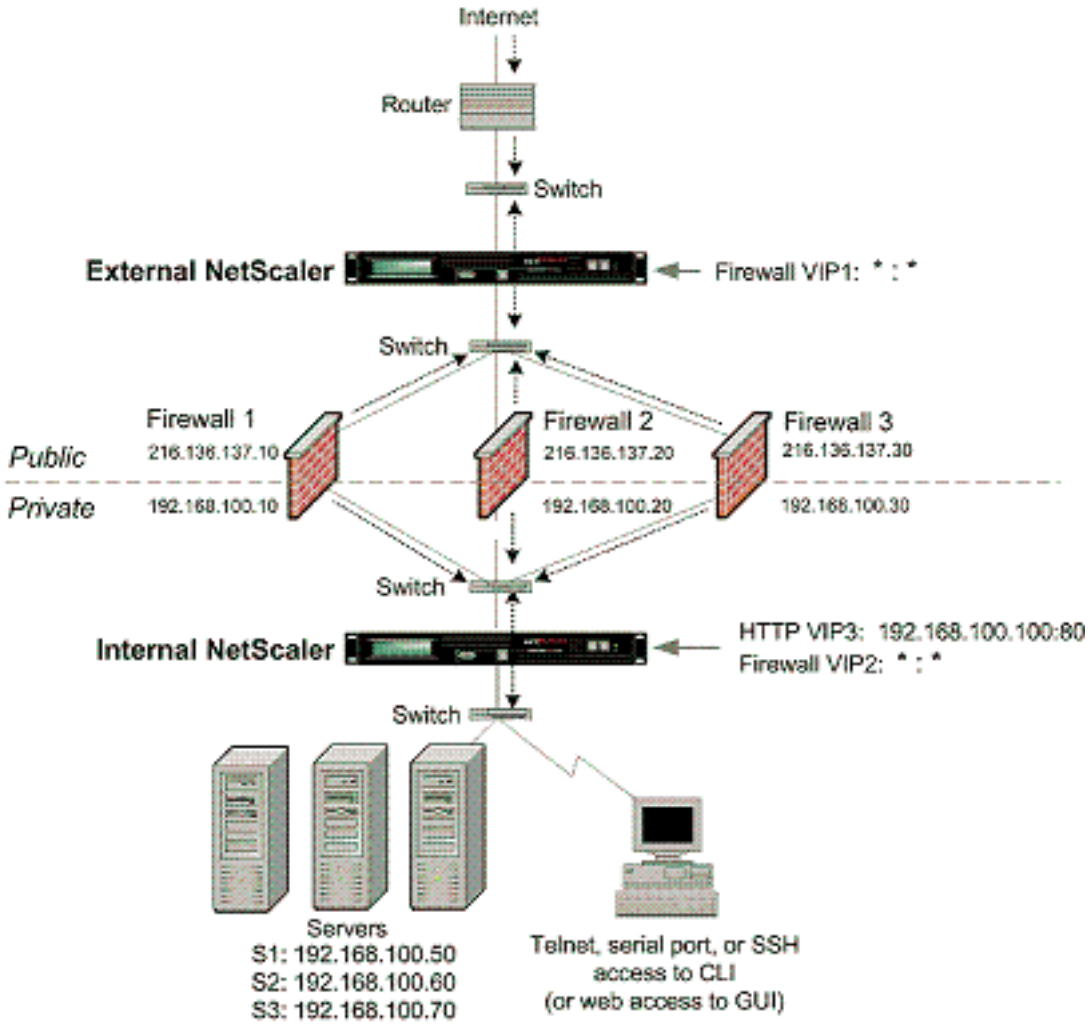
In diesem Setup befindet sich ein Citrix ADC auf jeder Seite eines Satzes von Firewalls. Das zwischen den Firewalls und dem Internet platzierte Citrix ADC, das als externes Citrix ADC bezeichnet wird, wählt basierend auf der konfigurierten Methode die beste Firewall aus. Der Citrix ADC zwischen den Firewalls und dem privaten Netzwerk, der so genannte interne Citrix ADC, verfolgt die Firewall, von der das anfängliche Paket für eine Sitzung empfangen wird. Es stellt dann sicher, dass alle nachfolgenden Pakete für diese Sitzung an dieselbe Firewall gesendet werden.

Der interne Citrix ADC kann als regulärer Traffic-Manager konfiguriert werden, um den Datenverkehr über die privaten Netzwerkserver hinweg auszugleichen. Diese Konfiguration ermöglicht auch den

Lastausgleich von Datenverkehr aus dem privaten Netzwerk (Egress) über die Firewalls hinweg.

Das folgende Diagramm zeigt die Sandwich-Firewall-Lastausgleichsumgebung.

Abbildung 1. Firewall-Lastenausgleich (Sandwich)



Der Diensttyp ANY konfiguriert den Citrix ADC so, dass er den gesamten Datenverkehr akzeptiert.

Um Vorteile im Zusammenhang mit HTTP und TCP zu nutzen, konfigurieren Sie den Dienst und den virtuellen Server mit dem Typ HTTP oder TCP. Damit FTP funktioniert, konfigurieren Sie den Dienst mit dem Typ FTP.

Konfigurieren des externen Citrix ADC in einer Sandwich-Umgebung

Führen Sie die folgenden Aufgaben aus, um den externen Citrix ADC in einer Sandwich-Umgebung zu konfigurieren.

- Aktivieren Sie die Funktion Lastausgleich.
- Konfigurieren Sie einen Platzhalterdienst für jede Firewall.

- Konfigurieren Sie einen Monitor für jeden Platzhalterdienst.
- Konfigurieren Sie einen virtuellen Wildcard-Server für Datenverkehr aus dem Internet.
- Konfigurieren Sie den virtuellen Server im MAC-Umschreibmodus.
- Binden Sie Dienste an den virtuellen Platzhalterserver.
- Speichern und Überprüfen der Konfiguration.

Lastenausgleichs-Funktion aktivieren

So aktivieren Sie den Lastausgleich mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um den Lastausgleich zu aktivieren und die Konfiguration zu überprüfen:

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

Beispiel:

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 .
 .
 .
 24)    NetScaler Push                  push                OFF
 Done
<!--NeedCopy-->
```

So aktivieren Sie den Lastenausgleich mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **System > Einstellungen** und wählen **Sie unter Configure Basic Features Load Balancing**aus.

Konfigurieren eines Platzhalterdiensts für jede Firewall

So konfigurieren Sie einen Platzhalterdienst für jede Firewall mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name> <serverName> ANY *
<!--NeedCopy-->
```

Beispiel:

```
add service Service-HTTP-1 10.102.29.5 ANY *
<!--NeedCopy-->
```

So konfigurieren Sie einen Platzhalterdienst für jede Firewall mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und fügen Sie einen Dienst hinzu. Geben Sie **ANY** im Feld **Protokoll** und im Feld Port * an.

Konfigurieren eines Monitors für jeden Platzhalterdienst

Ein PING-Monitor ist standardmäßig an den Dienst gebunden. Sie müssen einen transparenten Monitor konfigurieren, um Hosts auf der vertrauenswürdigen Seite durch einzelne Firewalls zu überwachen. Anschließend können Sie den transparenten Monitor an Dienste binden. Der standardmäßige PING-Monitor überwacht nur die Konnektivität zwischen der Citrix ADC Appliance und dem Upstream-Gerät. Der transparente Monitor überwacht alle Geräte, die im Pfad von der Appliance zu dem Gerät vorhanden sind, dem die im Monitor angegebene Ziel-IP-Adresse gehört. Wenn kein transparenter Monitor konfiguriert ist und der Status der Firewall UP ist, aber eines der nächsten Hop-Geräte dieser Firewall ausgefallen ist, schließt die Appliance die Firewall während des Lastenausgleichs ein und leitet das Paket an die Firewall weiter. Das Paket wird jedoch nicht an das endgültige Ziel geliefert, da eines der nächsten Hop-Geräte ausgefallen ist. Wenn eines der Geräte (einschließlich der Firewall) ausgefallen ist, wird der Dienst durch Bindung eines transparenten Monitors als DOWN gekennzeichnet, und die Firewall ist nicht enthalten, wenn die Appliance den Lastausgleich der Firewall durchführt.

Das Binden eines transparenten Monitors überschreibt den PING-Monitor. Um einen PING-Monitor zusätzlich zu einem transparenten Monitor zu konfigurieren, müssen Sie nach dem Erstellen und Binden eines transparenten Monitors einen PING-Monitor an den Dienst binden.

So konfigurieren Sie einen transparenten Monitor mit der Befehlszeilenschnittstelle

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

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
    transparent (YES | NO )]
bind lb monitor <monitorName> <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
bind monitor monitor-HTTP-1 fw-svc1
To bind a PING monitor, type the following command:
bind monitor PING fw-svc1
<!--NeedCopy-->
```

So erstellen und binden Sie einen transparenten Monitor mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**, und erstellen und binden Sie dann einen transparenten Monitor.

Konfigurieren eines virtuellen Wildcard-Servers für Datenverkehr aus dem Internet

So konfigurieren Sie einen virtuellen Platzhalterserver für Datenverkehr aus dem Internet mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> ANY * *
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```


So konfigurieren Sie einen virtuellen Platzhalterserver für Datenverkehr aus dem Internet mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und erstellen Sie einen virtuellen Platzhalterserver. Geben Sie **ANY** im Feld **Protokoll** und im Feld Port * an.

Konfigurieren des virtuellen Servers im MAC-Umschreibmodus

So konfigurieren Sie den virtuellen Server im MAC-Umschreibmodus mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

So konfigurieren Sie den virtuellen Server im MAC-Umschreibmodus mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und wählen Sie den virtuellen Server aus, für den Sie den Umleitungsmodus konfigurieren möchten (z. B. vServer-LB-1).
2. Bearbeiten Sie den Abschnitt **Grundeinstellungen** und klicken Sie auf **mehr**.
3. Wählen Sie in der Dropdownliste **Umleitungsmodus** die Option **MAC-basiert** aus.

Binden von Diensten an den virtuellen Wildcard-Server

So binden Sie einen Dienst mit der Befehlszeilenschnittstelle an den virtuellen Platzhalterserver

Geben Sie an der Eingabeaufforderung Folgendes ein:

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


Beispiel:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

So binden Sie einen Dienst mit dem Konfigurationsdienstprogramm an den virtuellen Platzhalterserver

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server** und wählen Sie den virtuellen Server aus, für den Sie den Dienst binden möchten.
2. Klicken Sie im Abschnitt **Dienste** und wählen Sie einen zu bindenden Dienst aus.

Speichern und Überprüfen der Konfiguration

Wenn Sie die Konfigurationsaufgaben abgeschlossen haben, speichern Sie die Konfiguration. Stellen Sie sicher, dass die Einstellungen korrekt sind.

So speichern und überprüfen Sie die Konfiguration mit der Befehlszeilenschnittstelle

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

```
save ns config
show vserver
<!--NeedCopy-->
```

Beispiel:

```
save config
sh lb vserver FWLBVIP1
FWLBVIP1 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 06:40:14 2010
        Time since last state change: 0 days, 00:00:11.240
        Effective State: UP  ARP:DISABLED
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
```



```
        Configured Method: SRCIPDESTIPHASH
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw_svc_1 (10.102.29.251: *) - ANY State: UP  Weight: 1
2) fw_svc_2 (10.102.29.18: \*) - ANY State: UP   Weight: 1
 Done
show service fw-svc1
        fw-svc1 (10.102.29.251:\*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 10:04:50 2010
        Time since last state change: 0 days, 00:00:38.120
        Server Name: 10.102.29.251
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): YES
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
                State: DOWN     Weight: 1
                Probes: 5       Failed [Total: 5 Current: 5]
                Last response: Failure - Time out during TCP connection
                    establishment stage
                Response Time: 2000.0 millisec
2)      Monitor Name: ping
                State: UP       Weight: 1
                Probes: 3       Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.415 millisec
 Done
<!--NeedCopy-->
```


Konfigurieren des internen Citrix ADC in einer Sandwich-Umgebung

Führen Sie die folgenden Aufgaben aus, um den internen Citrix ADC in einer Sandwich-Umgebung zu konfigurieren.

Für den Datenverkehr vom Server (ausgehend)

- Aktivieren Sie die Funktion Lastausgleich.
- Konfigurieren Sie einen Platzhalterdienst für jede Firewall.
- Konfigurieren Sie einen Monitor für jeden Platzhalterdienst.
- Konfigurieren Sie einen virtuellen Wildcard-Server, um den Lastenausgleich des an die Firewalls gesendeten Datenverkehrs zu erhalten.
- Konfigurieren Sie den virtuellen Server im MAC-Umschreibmodus.
- Binden Sie Firewall-Dienste an den virtuellen Wildcard-Server.

Für Datenverkehr über private Netzwerkserver

- Konfigurieren Sie einen Dienst für jeden virtuellen Server.
- Konfigurieren Sie einen Monitor für jeden Dienst.
- Konfigurieren Sie einen virtuellen HTTP-Server, um den an die Server gesendeten Datenverkehr auszugleichen.
- Binden Sie HTTP-Dienste an den virtuellen HTTP-Server.
- Speichern und Überprüfen der Konfiguration.

Lastenausgleichs-Funktion aktivieren

Sie können Load Balancing-Entitäten wie Dienste und virtuelle Server konfigurieren, wenn die Lastausgleichsfunktion deaktiviert ist. Sie funktionieren jedoch erst, wenn Sie die Funktion aktivieren.

So aktivieren Sie den Lastausgleich mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um den Lastausgleich zu aktivieren und die Konfiguration zu überprüfen:

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

Beispiel:

```
> enable ns feature LoadBalancing
 Done
```



```
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 .
 .
 .
 24)    NetScaler Push                  push                OFF
 Done
<!--NeedCopy-->
```

So aktivieren Sie den Lastenausgleich mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **System > Einstellungen** und wählen Sie unter Basisfunktionen konfigurieren die Option **Load Balancing**aus.

Konfigurieren eines Platzhalterdiensts für jede Firewall

So konfigurieren Sie einen Platzhalterdienst für jede Firewall mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name> <serverName> ANY *
<!--NeedCopy-->
```

Beispiel:

```
add service Service-HTTP-1 10.102.29.5 ANY *
<!--NeedCopy-->
```

So konfigurieren Sie einen Platzhalterdienst für jede Firewall mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und fügen Sie einen Dienst hinzu. Geben Sie **ANY** im Feld **Protokoll** und im Feld Port * an.

Konfigurieren eines Monitors für jeden Platzhalterdienst

Ein PING-Monitor ist standardmäßig an den Dienst gebunden. Sie müssen einen transparenten Monitor konfigurieren, um Hosts auf der vertrauenswürdigen Seite durch einzelne Firewalls zu überwachen. Anschließend können Sie den transparenten Monitor an Dienste binden. Der standardmäßige PING-Monitor überwacht nur die Konnektivität zwischen der Citrix ADC Appliance und dem Upstream-Gerät. Der transparente Monitor überwacht alle Geräte, die im Pfad von der Appliance zu dem Gerät vorhanden sind, dem die im Monitor angegebene Ziel-IP-Adresse gehört. Wenn kein transparenter Monitor konfiguriert ist und der Status der Firewall UP ist, aber eines der nächsten Hop-Geräte dieser Firewall ausgefallen ist, schließt die Appliance die Firewall während des Lastenausgleichs ein und leitet das Paket an die Firewall weiter. Das Paket wird jedoch nicht an das endgültige Ziel geliefert, da eines der nächsten Hop-Geräte ausgefallen ist. Wenn eines der Geräte (einschließlich der Firewall) ausgefallen ist, wird der Dienst durch Bindung eines transparenten Monitors als DOWN gekennzeichnet, und die Firewall ist nicht enthalten, wenn die Appliance den Lastausgleich der Firewall durchführt.

Das Binden eines transparenten Monitors überschreibt den PING-Monitor. Um einen PING-Monitor zusätzlich zu einem transparenten Monitor zu konfigurieren, müssen Sie nach dem Erstellen und Binden eines transparenten Monitors einen PING-Monitor an den Dienst binden.

So konfigurieren Sie einen transparenten Monitor mit der Befehlszeilenschnittstelle

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

```
1 add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
     transparent (YES | NO )]
2 bind lb monitor <monitorName> <serviceName>
3 <!--NeedCopy-->
```

Beispiel:

```
1 add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
2 bind monitor monitor-HTTP-1 fw-svc1
3 <!--NeedCopy-->
```

So erstellen und binden Sie einen transparenten Monitor mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**, und erstellen Sie einen Monitor.
2. Geben **Sie im Dialogfeld Monitor erstellen** die erforderlichen Parameter ein und wählen Sie **Transparent**aus.

Konfigurieren eines virtuellen Wildcard-Servers zum Lastenausgleich des an die Firewalls gesendeten Datenverkehrs

So konfigurieren Sie einen virtuellen Platzhalterserver für den Lastausgleich des an die Firewalls gesendeten Datenverkehrs mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> ANY * *
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Platzhalterserver für Datenverkehr aus dem Internet mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und erstellen Sie einen virtuellen Platzhalterserver.
2. Geben Sie **ANY** im Feld Protokoll und ***** im Feld Port an.

So konfigurieren Sie einen virtuellen Platzhalterserver für den Lastausgleich des an die Firewalls gesendeten Datenverkehrs mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Virtuellen Server erstellen (Load Balancing) Werte für die folgenden Parameter an:
   - Name — Name
4. Wählen Sie unter Protokoll die Option ANY, und wählen Sie unter IP-Adresse und Port die Option * aus.

5. Klicken Sie auf Erstellenund dann auf Schließen. Der erstellte virtuelle Server wird im Bereich Virtuelle Server für Lastenausgleich angezeigt.

Konfigurieren des virtuellen Servers im MAC-Umschreibmodus

So konfigurieren Sie den virtuellen Server im MAC-Umschreibmodus mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

So konfigurieren Sie den virtuellen Server im MAC-Umschreibmodus mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und wählen Sie den virtuellen Server aus, für den Sie den Umleitungsmodus konfigurieren möchten (z. B. vServer-LB-1).
2. Bearbeiten Sie den Abschnitt **Grundeinstellungen** und klicken Sie auf **mehr**.
3. Wählen Sie in der Dropdownliste **Umleitungsmodus** die Option **MAC-basiert** aus.

Binden von Firewalldiensten an den virtuellen Wildcard-Server

So binden Sie Firewalldienste mit der Befehlszeilenschnittstelle an den virtuellen Wildcard-Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel:


```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

So binden Sie Firewalldienste mit dem Konfigurationsdienstprogramm an den virtuellen Platzhalterserver

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und wählen Sie einen virtuellen Server aus.
2. Klicken Sie in den Abschnitt Service und wählen Sie einen Dienst aus, den Sie binden möchten.

Hinweis: Sie können einen Dienst an mehrere virtuelle Server binden.

Konfigurieren eines Dienstes für jeden virtuellen Server

So konfigurieren Sie einen Dienst für jeden virtuellen Server mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name> <serverName> HTTP <port>
<!--NeedCopy-->
```

Beispiel:

```
add service Service-HTTP-1 10.102.29.5 HTTP 80
<!--NeedCopy-->
```

So konfigurieren Sie einen Dienst für jeden virtuellen Server mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und konfigurieren Sie einen Dienst für jeden virtuellen Server.
2. Geben Sie **HTTP** im Feld **Protokoll** an und wählen Sie unter **Verfügbare Monitore** die Option **HTTP**aus.

So konfigurieren Sie einen Dienst für jeden virtuellen Server mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.

2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Dienst erstellen Werte für die folgenden Parameter an, wie gezeigt:
   - Dienstname — Name
   - Server — Servername
   - Port — Port
4. Geben Sie unter Protokoll HTTP an. Wählen Sie unter Verfügbare Monitore die Option HTTP aus.
5. Klicken Sie auf Erstellenund dann auf Schließen. Der erstellte Dienst wird im Bereich Dienste angezeigt.

Konfigurieren eines Monitors für jeden Dienst

So binden Sie einen Monitor mit der Befehlszeilenschnittstelle an einen Dienst

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb monitor <monitorName> <ServiceName>
<!--NeedCopy-->
```

Beispiel:

```
bind mon monitor-HTTP-1 Service-HTTP-1
<!--NeedCopy-->
```

So binden Sie einen Monitor mit dem Konfigurationsdienstprogramm an einen Dienst

Navigieren Sie zu **Traffic Management > Load Balancing > Services**, doppelklicken Sie auf einen Dienst und fügen Sie einen Monitor hinzu.

Konfigurieren eines virtuellen HTTP-Servers zum Ausgleich des an die Server gesendeten Datenverkehrs

So konfigurieren Sie einen virtuellen HTTP-Server für den Ausgleich des Datenverkehrs, der über die Befehlszeilenschnittstelle an die Server gesendet wird

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> HTTP <ip> <port>
<!--NeedCopy-->
```


Beispiel:

```
add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen HTTP-Server für den Ausgleich des Datenverkehrs, der an die Server gesendet wird, mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Dienste**, und konfigurieren Sie einen virtuellen HTTP-Server.
2. Geben Sie **HTTP** im Feld **Protokoll** an.

So konfigurieren Sie einen virtuellen HTTP-Server für den Ausgleich des Datenverkehrs, der an die Server gesendet wird, mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Virtuellen Server erstellen (Load Balancing) Werte für die folgenden Parameter an:
   - Name — Name
   - IP-Adresse — IP-Adresse
     Hinweis: Wenn der virtuelle Server
     IPv6 verwendet, aktivieren Sie das Kontrollkästchen IPv6 und geben Sie die Adresse im IPv6-Formatein (z. B.
     1000:0000:0000:0000:0005:0600:700a:888b)
   - Port — Port
4. Wählen Sie unter Protokoll die Option HTTP aus.
5. Klicken Sie auf Erstellenund dann auf Schließen. Der erstellte virtuelle Server wird im Bereich Virtuelle Server für Lastenausgleich angezeigt.

Speichern und Überprüfen der Konfiguration

Wenn Sie die Konfigurationsaufgaben abgeschlossen haben, speichern Sie die Konfiguration. Sie sollten auch überprüfen, ob die Einstellungen korrekt sind.

So speichern und überprüfen Sie die Konfiguration mit der Befehlszeilenschnittstelle

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

- save ns config
- show vserver

Beispiel:

```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw-int-svc1 (10.102.29.5: *) - ANY State: UP Weight: 1
2) fw-int-svc2 (10.102.29.9: \*) - ANY State: UP Weight: 1
 Done
show service fw-int-svc1
        fw-int-svc1 (10.102.29.5:\*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 14:44:51 2010
        Time since last state change: 0 days, 00:01:50.240
        Server Name: 10.102.29.5
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED
```



```
40
41 1)      Monitor Name: monitor-HTTP-1
42                 State: DOWN     Weight: 1
43                 Probes: 9       Failed [Total: 9 Current: 9]
44                 Last response: Failure - Time out during TCP connection
                       establishment stage
45                 Response Time: 2000.0 millisec
46 2)      Monitor Name: ping
47                 State: UP       Weight: 1
48                 Probes: 3       Failed [Total: 0 Current: 0]
49                 Last response: Success - ICMP echo reply received.
50                 Response Time: 1.275 millisec
51  Done
52 <!--NeedCopy-->
```

So speichern und überprüfen Sie die Konfiguration mit dem Konfigurationsdienstprogramm

1. Klicken Sie im **Detailbereich** auf **Speichern**.
2. Klicken Sie im Dialogfeld **Konfiguration speichern** auf **Ja**.
3. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
4. Wählen Sie im **Detailbereich** den virtuellen Server aus, den Sie in Schritt 5 erstellt haben.
5. Stellen Sie sicher, dass die im **Detailbereich** angezeigten Einstellungen korrekt sind.
6. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
7. Wählen Sie im **Detailbereich** die Services aus, die Sie in Schritt 5 erstellt haben.
8. Stellen Sie sicher, dass die im **Detailbereich** angezeigten Einstellungen korrekt sind.

Überwachen eines Firewall-Lastenausgleichs in einer Sandwich-Umgebung

Nachdem die Konfiguration ausgeführt wurde und ausgeführt wurde, sollten Sie die Statistiken für jeden Dienst und jeden virtuellen Server anzeigen, um auf mögliche Probleme zu überprüfen.

Anzeigen der Statistiken eines virtuellen Servers

Um die Leistung virtueller Server zu bewerten oder Probleme zu beheben, können Sie Details der virtuellen Server anzeigen, die auf der Citrix ADC Appliance konfiguriert sind. Sie können eine Zusammenfassung der Statistiken für alle virtuellen Server anzeigen, oder Sie können den Namen eines virtuellen Servers angeben, um die Statistiken nur für diesen virtuellen Server anzuzeigen. Sie können die folgenden Details anzeigen:

- Name
- IP-Adresse
- Port

- Protokoll
- Status des virtuellen Servers
- Rate der empfangenen Anfragen
- Trefferrate

So zeigen Sie Statistiken über virtuelle Server mit der Befehlszeilenschnittstelle an

Um eine Zusammenfassung der Statistiken für alle virtuellen Server anzuzeigen, die derzeit auf dem Citrix ADC konfiguriert sind, oder für einen einzelnen virtuellen Server, geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat lb vserver [-detail] [<name>]
<!--NeedCopy-->
```

Beispiel:

```
>stat lb vserver -detail
Virtual Server(s) Summary
                       vsvrIP  port     Protocol        State    Req/s
                            Hits/s
One                         *    80         HTTP           UP      5/s
        0/s
Two                         *     0          TCP         DOWN      0/s
        0/s
Three                       *  2598          TCP         DOWN      0/s
        0/s
dnsVirtualNS    10.102.29.90    53          DNS         DOWN      0/s
        0/s
BRVSERV            10.10.1.1    80         HTTP         DOWN      0/s
        0/s
LBVIP           10.102.29.66    80         HTTP           UP      0/s
        0/s
 Done

<!--NeedCopy-->
```

So zeigen Sie Statistiken über virtuelle Server mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server > Statistiken**.
2. Wenn Sie die Statistiken für nur einen virtuellen Server anzeigen möchten, wählen Sie im Detailbereich den virtuellen Server aus und klicken Sie auf **Statistik**.

Statistiken eines Dienstes anzeigen

Mithilfe der Dienststatistiken können Sie die Rate von Anforderungen, Antworten, Anforderungsbytes, Antwortbytes, aktuelle Clientverbindungen, Anforderungen in Überspannungswarteschlange, aktuelle Serververbindungen usw. anzeigen.

So zeigen Sie die Statistiken eines Dienstes mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat service <name>
<!--NeedCopy-->
```

Beispiel:

```
stat service Service-HTTP-1
<!--NeedCopy-->
```

So zeigen Sie die Statistiken eines Dienstes mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services > Statistiken**.
2. Wenn Sie die Statistiken für nur einen Dienst anzeigen möchten, wählen Sie den Dienst aus und klicken Sie auf **Statistiken**.

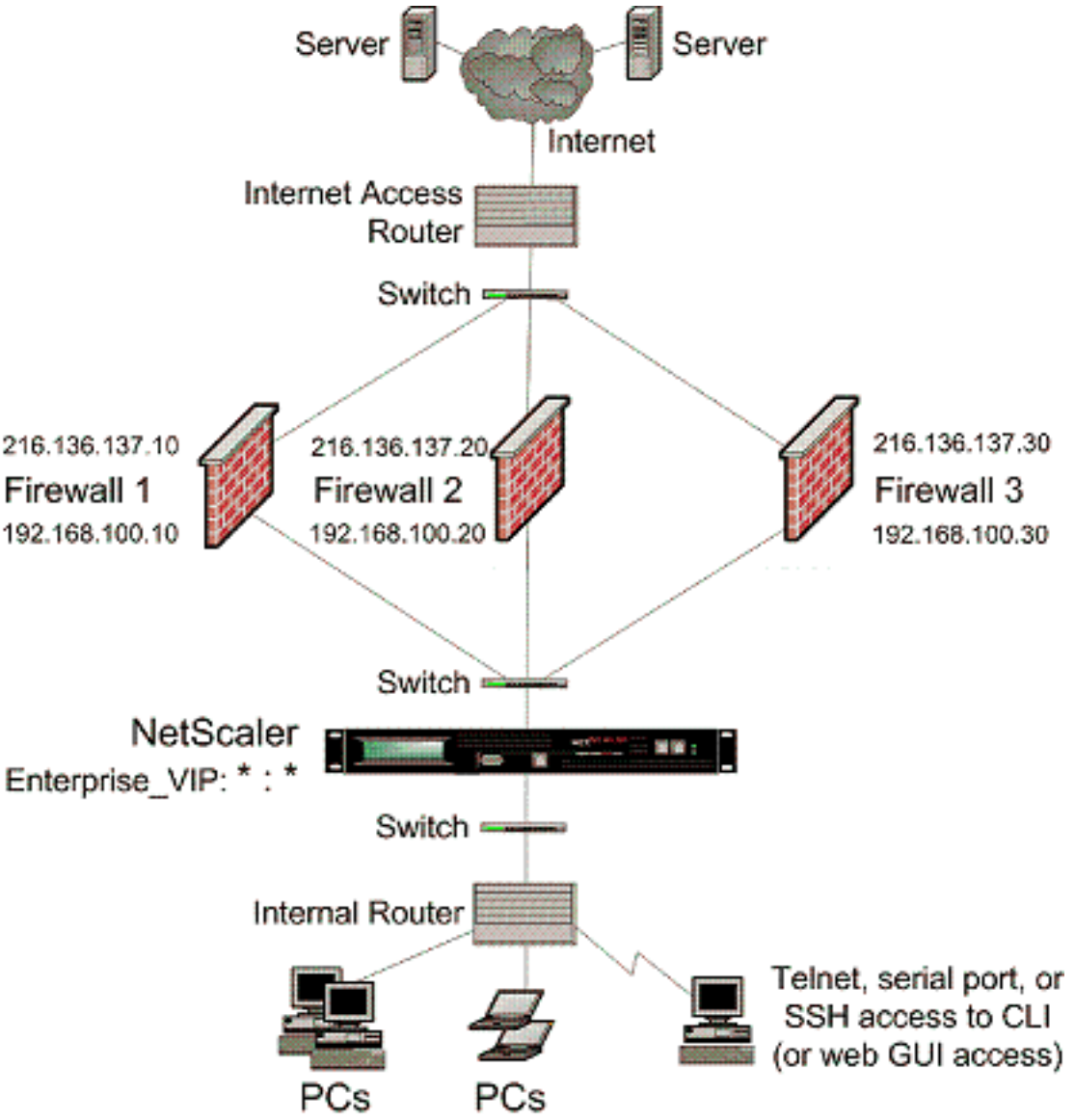
Unternehmensumgebung

October 5, 2021

Im Enterprise-Setup wird der Citrix ADC zwischen den Firewalls platziert, die eine Verbindung mit dem öffentlichen Internet herstellen, und dem internen privaten Netzwerk herstellen und den Datenausgang verarbeiten. Citrix ADC wählt basierend auf der konfigurierten Lastausgleichsrichtlinie die beste Firewall aus.

Das folgende Diagramm zeigt die Enterprise-Firewall-Load Balancing-Umgebung

Abbildung 1. Firewall-Lastenausgleich (Enterprise)



Der Diensttyp ANY konfiguriert den Citrix ADC so, dass er den gesamten Datenverkehr akzeptiert.

Um Vorteile im Zusammenhang mit HTTP und TCP zu nutzen, konfigurieren Sie den Dienst und den vserver mit dem Typ HTTP oder TCP. Damit FTP funktioniert, konfigurieren Sie den Dienst mit dem Typ FTP.

Konfigurieren des Citrix ADC in einer Unternehmensumgebung

Führen Sie die folgenden Aufgaben aus, um einen Citrix ADC in einer Unternehmensumgebung zu konfigurieren.

Für den Datenverkehr vom Server (ausgehend)

- Aktivieren Sie die Funktion Lastausgleich.

- Konfigurieren Sie einen Platzhalterdienst für jede Firewall.
- Konfigurieren Sie einen Monitor für jeden Platzhalterdienst.
- Konfigurieren Sie einen virtuellen Wildcard-Server, um den Lastenausgleich des an die Firewalls gesendeten Datenverkehrs zu erhalten.
- Konfigurieren Sie den virtuellen Server im MAC-Umschreibmodus.
- Binden Sie Firewall-Dienste an den virtuellen Wildcard-Server.

Für Datenverkehr über private Netzwerkserver

- Konfigurieren Sie einen Dienst für jeden virtuellen Server.
- Konfigurieren Sie einen Monitor für jeden Dienst.
- Konfigurieren Sie einen virtuellen HTTP-Server, um den an die Server gesendeten Datenverkehr auszugleichen.
- Binden Sie HTTP-Dienste an den virtuellen HTTP-Server.
- Speichern und Überprüfen der Konfiguration.

Lastenausgleichs-Funktion aktivieren

Sie können Lastausgleichs-Entitäten wie Dienste und virtuelle Server konfigurieren, wenn die Lastenausgleichsfunktion deaktiviert ist, aber sie funktionieren erst, wenn Sie das Feature aktivieren.

So aktivieren Sie den Lastausgleich mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um den Lastausgleich zu aktivieren und die Konfiguration zu überprüfen:

- enable ns feature LB
- show ns feature

Beispiel:

```
> enable ns feature LoadBalancing
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  OFF
 2)     Surge Protection                SP                  ON
 3)     Load Balancing                  LB                  ON
 .
 .
 .
```



```
 24)    NetScaler Push                push                  OFF
 Done
<!--NeedCopy-->
```

So aktivieren Sie den Lastenausgleich mit dem Konfigurationsdienstprogramm

Navigieren Sie zu System > Einstellungen und wählen Sie unter Configure Basic FeaturesLoad Balancingaus.

Konfigurieren eines Platzhalterdiensts für jede Firewall

So konfigurieren Sie einen Platzhalterdienst für jede Firewall mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name> <serverName> ANY *
<!--NeedCopy-->
```

Beispiel:

```
add service Service-HTTP-1 10.102.29.5 ANY *
<!--NeedCopy-->
```

So konfigurieren Sie einen Platzhalterdienst für jede Firewall mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Dienst erstellen Werte für die folgenden Parameter an, wie gezeigt:
   - Dienstname — Name
   - Server — Servername
4. Wählen Sie unter Protokoll die Option ANY, und wählen Sie in Port die Option * aus.
5. Klicken Sie auf Erstellenund dann auf Schließen. Der erstellte Dienst wird im Bereich Dienste angezeigt.

Konfigurieren eines Monitors für jeden Platzhalterdienst

Ein PING-Monitor ist standardmäßig an den Dienst gebunden. Sie müssen einen transparenten Monitor konfigurieren, um Hosts auf der vertrauenswürdigen Seite über einzelne Firewalls zu überwachen. Anschließend können Sie den transparenten Monitor an Dienste binden. Der standardmäßige PING-Monitor überwacht nur die Konnektivität zwischen der Citrix ADC Appliance und dem Upstream-Gerät. Der transparente Monitor überwacht alle Geräte, die im Pfad von der Appliance zu dem Gerät vorhanden sind, dem die im Monitor angegebene Ziel-IP-Adresse gehört. Wenn kein transparenter Monitor konfiguriert ist und der Status der Firewall UP ist, aber eines der nächsten Hop-Geräte dieser Firewall ausgefallen ist, schließt die Appliance die Firewall während des Lastenausgleichs ein und leitet das Paket an die Firewall weiter. Das Paket wird jedoch nicht an das endgültige Ziel geliefert, da eines der nächsten Hop-Geräte ausgefallen ist. Wenn eines der Geräte (einschließlich der Firewall) ausgefallen ist, wird der Dienst durch Bindung eines transparenten Monitors als DOWN gekennzeichnet, und die Firewall ist nicht enthalten, wenn die Appliance den Lastausgleich der Firewall durchführt.

Das Binden eines transparenten Monitors überschreibt den PING-Monitor. Um einen PING-Monitor zusätzlich zu einem transparenten Monitor zu konfigurieren, müssen Sie nach dem Erstellen und Binden eines transparenten Monitors einen PING-Monitor an den Dienst binden.

So konfigurieren Sie einen transparenten Monitor mit der Befehlszeilenschnittstelle

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

```
1 add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
     transparent (YES | NO )]
2 bind lb monitor <monitorName> <serviceName>
3 <!--NeedCopy-->
```

Beispiel:

```
1 add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
2 bind monitor monitor-HTTP-1 fw-svc1
3 <!--NeedCopy-->
```

So erstellen und binden Sie einen transparenten Monitor mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu Traffic Management > Load Balancing > Monitore.

2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Monitor erstellen folgende Werte an:
    - Namen*
    - Typ*—Typ
    - Ziel-IP
    - Folie

    -* Ein erforderlicher Parameter
4. Klicken Sie auf Erstellenund dann auf Schließen. Wählen Sie im Bereich Monitore den Monitor aus, den Sie gerade konfiguriert haben, und stellen Sie sicher, dass die am unteren Bildschirmrand angezeigten Einstellungen korrekt sind.

Konfigurieren eines virtuellen Wildcard-Servers zum Lastenausgleich des an die Firewalls gesendeten Datenverkehrs

So konfigurieren Sie einen virtuellen Platzhalterserver für den Lastausgleich des an die Firewalls gesendeten Datenverkehrs mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> ANY * *
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Platzhalterserver für den Lastausgleich des an die Firewalls gesendeten Datenverkehrs mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Virtuellen Server erstellen (Load Balancing) Werte für die folgenden Parameter an:
    - Name — Name
4. Wählen Sie unter Protokoll die Option ANY, und wählen Sie unter IP-Adresse und Port die Option * aus.

5. Klicken Sie auf Erstellenund dann auf Schließen. Der erstellte virtuelle Server wird im Bereich Virtuelle Server für Lastenausgleich angezeigt.

Konfigurieren des virtuellen Servers im MAC-Umschreibmodus

So konfigurieren Sie den virtuellen Server im MAC-Umschreibmodus mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

So konfigurieren Sie den virtuellen Server im MAC-Umschreibmodus mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie den Umleitungsmodus konfigurieren möchten (z. B. vServer-LB-1), und klicken Sie dann auf Öffnen.
3. Klicken Sie auf der Registerkarte Erweitert unter Umleitungsmodus auf MAC-basiert.
4. Klicken Sie auf OK.

Binden von Firewalldiensten an den virtuellen Wildcard-Server

So binden Sie Firewalldienste mit der Befehlszeilenschnittstelle an den virtuellen Wildcard-Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel:


```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

So binden Sie Firewalldienste mit dem Konfigurationsdienstprogramm an den virtuellen Platzhalterserver

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server, und wählen Sie einen virtuellen Server aus.
2. Klicken Sie in den Abschnitt Service und wählen Sie einen Dienst aus, den Sie binden möchten.

Hinweis: Sie können einen Dienst an mehrere virtuelle Server binden.

Konfigurieren eines Dienstes für jeden virtuellen Server

So konfigurieren Sie einen Dienst für jeden virtuellen Server mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name> <serverName> HTTP <port>
<!--NeedCopy-->
```

Beispiel:

```
add service Service-HTTP-1 10.102.29.5 HTTP 80
<!--NeedCopy-->
```

So konfigurieren Sie einen Dienst für jeden virtuellen Server mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Dienst erstellen Werte für die folgenden Parameter an, wie gezeigt:
   - Dienstname — Name
   - Server — Servername
   - Port — Port
4. Geben Sie unter Protokoll HTTP an. Wählen Sie unter Verfügbare Monitore die Option HTTP aus.
5. Klicken Sie auf Erstellenund dann auf Schließen. Der erstellte Dienst wird im Bereich Dienste angezeigt.

Konfigurieren eines Monitors für jeden Dienst

So binden Sie einen Monitor mit der Befehlszeilenschnittstelle an einen Dienst

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb monitor <monitorName> <ServiceName>
<!--NeedCopy-->
```

Beispiel:

```
bind mon monitor-HTTP-1 Service-HTTP-1
<!--NeedCopy-->
```

So binden Sie einen Monitor mit dem Konfigurationsdienstprogramm an einen Dienst

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Öffnen Sie den Dienst, und fügen Sie einen Monitor hinzu.

Konfigurieren eines virtuellen HTTP-Servers zum Ausgleich des an die Server gesendeten Datenverkehrs

So konfigurieren Sie einen virtuellen HTTP-Server für den Ausgleich des Datenverkehrs, der über die Befehlszeilenschnittstelle an die Server gesendet wird

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> HTTP <ip> <port>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen HTTP-Server für den Ausgleich des Datenverkehrs, der an die Server gesendet wird, mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Virtuellen Server erstellen (Load Balancing) Werte für die folgenden Parameter an:
   - Name — Name
   - IP-Adresse — IPAddress
     Hinweis: Wenn der virtuelle Server IPv6 verwendet, aktivieren Sie das Kontrollkästchen IPv6, und geben Sie die Adresse im IPv6-Format ein (z. B. **1000:0000:0000:0000:0005:0600:700 a:888b**).
   - Port — Port
4. Wählen Sie unter Protokoll die Option HTTP aus.
5. Klicken Sie auf Erstellenund dann auf Schließen. Der erstellte virtuelle Server wird im Bereich Virtuelle Server für Lastenausgleich angezeigt.

Binden von HTTP-Diensten an den virtuellen HTTP-Server

So binden Sie HTTP-Dienste mit der Befehlszeilenschnittstelle an den virtuellen Wildcard-Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

So binden Sie HTTP-Dienste mit dem Konfigurationsdienstprogramm an den virtuellen Platzhalterserver

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server, und wählen Sie einen virtuellen Server aus.
2. Klicken Sie in den Abschnitt Service und wählen Sie einen Dienst aus, den Sie binden möchten.

Hinweis: Sie können einen Dienst an mehrere virtuelle Server binden.

Speichern und Überprüfen der Konfiguration

Wenn Sie die Konfigurationsaufgaben abgeschlossen haben, speichern Sie die Konfiguration. Sie sollten auch überprüfen, ob die Einstellungen korrekt sind.

So speichern und überprüfen Sie die Konfiguration mit der Befehlszeilenschnittstelle

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

- save ns config
- show vserver

Beispiel:

```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw-int-svc1 (10.102.29.5: *) - ANY State: UP Weight: 1
2) fw-int-svc2 (10.102.29.9: \*) - ANY State: UP Weight: 1
 Done
show service fw-int-svc1
        fw-int-svc1 (10.102.29.5:\*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 14:44:51 2010
        Time since last state change: 0 days, 00:01:50.240
        Server Name: 10.102.29.5
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
```



```
30          Client Keepalive(CKA): NO
31          Access Down Service: NO
32          TCP Buffering(TCPB): NO
33          HTTP Compression(CMP): NO
34          Idle timeout: Client: 120 sec   Server: 120 sec
35          Client IP: DISABLED
36          Cacheable: NO
37          SC: OFF
38          SP: OFF
39          Down state flush: ENABLED
40
41  1)      Monitor Name: monitor-HTTP-1
42                  State: DOWN     Weight: 1
43                  Probes: 9       Failed [Total: 9 Current: 9]
44                  Last response: Failure - Time out during TCP connection
                        establishment stage
45                  Response Time: 2000.0 millisec
46  2)      Monitor Name: ping
47                  State: UP       Weight: 1
48                  Probes: 3       Failed [Total: 0 Current: 0]
49                  Last response: Success - ICMP echo reply received.
50                  Response Time: 1.275 millisec
51   Done
52  <!--NeedCopy-->
```

So speichern und überprüfen Sie die Konfiguration mit dem Konfigurationsdienstprogramm

1. Klicken Sie im Detailbereich auf Speichern.
2. Klicken Sie im Dialogfeld Konfiguration speichern auf Ja.
3. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
4. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie in Schritt 5 erstellt haben, und überprüfen Sie, ob die im Detailbereich angezeigten Einstellungen korrekt sind.
5. Navigieren Sie zu Traffic Management > Load Balancing > Services.
6. Wählen Sie im Detailbereich den Dienst aus, den Sie in Schritt 5 erstellt haben, und überprüfen Sie, ob die im Detailbereich angezeigten Einstellungen korrekt sind.

Überwachung eines Firewall-Load Balancing-Setups in einer Unternehmensumgebung

Nachdem die Konfiguration ausgeführt wurde und ausgeführt wurde, sollten Sie die Statistiken für jeden Dienst und jeden virtuellen Server anzeigen, um auf mögliche Probleme zu überprüfen.

Anzeigen der Statistiken eines virtuellen Servers

Um die Leistung virtueller Server zu bewerten oder Probleme zu beheben, können Sie Details der virtuellen Server anzeigen, die auf der Citrix ADC Appliance konfiguriert sind. Sie können eine Zusammenfassung der Statistiken für alle virtuellen Server anzeigen, oder Sie können den Namen eines virtuellen Servers angeben, um die Statistiken nur für diesen virtuellen Server anzuzeigen. Sie können die folgenden Details anzeigen:

- Name
- IP-Adresse
- Port
- Protokoll
- Status des virtuellen Servers
- Rate der empfangenen Anfragen
- Trefferrate

So zeigen Sie Statistiken über virtuelle Server mit der Befehlszeilenschnittstelle an

Um eine Zusammenfassung der Statistiken für alle virtuellen Server anzuzeigen, die derzeit auf der Citrix ADC Appliance oder für einen einzelnen virtuellen Server konfiguriert sind, geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat lb vserver [-detail] [<name>]
<!--NeedCopy-->
```

Beispiel:

```
>stat lb vserver -detail
Virtual Server(s) Summary
                        vsvrIP  port     Protocol        State    Req/s
                             Hits/s
One                          *    80         HTTP           UP      5/s
        0/s
Two                          *     0          TCP         DOWN      0/s
        0/s
Three                        *  2598          TCP         DOWN      0/s
        0/s
dnsVirtualNS    10.102.29.90    53          DNS         DOWN      0/s
        0/s
BRVSERV            10.10.1.1    80         HTTP         DOWN      0/s
        0/s
```



```
LBVIP            10.102.29.66    80          HTTP            UP       0/s
         0/s
 Done


<!--NeedCopy-->
```

So zeigen Sie Statistiken über virtuelle Server mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server > Statistiken.
2. Wenn Sie die Statistiken nur für einen virtuellen Server anzeigen möchten, wählen Sie im Detailbereich den virtuellen Server aus und klicken Sie auf Statistiken.

Statistiken eines Dienstes anzeigen

Aktualisierung: 28.08.2013

Mithilfe der Dienststatistiken können Sie die Rate von Anforderungen, Antworten, Anforderungsbytes, Antwortbytes, aktuelle Clientverbindungen, Anforderungen in Überspannungswarteschlange, aktuelle Serververbindungen usw. anzeigen.

So zeigen Sie die Statistiken eines Dienstes mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat service <name>
<!--NeedCopy-->
```

Beispiel:

```
stat service Service-HTTP-1
<!--NeedCopy-->
```

So zeigen Sie die Statistiken eines Dienstes mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu Traffic Management > Load Balancing > Services > Statistiken.
2. Wenn Sie die Statistiken für nur einen Dienst anzeigen möchten, wählen Sie den Dienst aus und klicken Sie auf Statistiken.

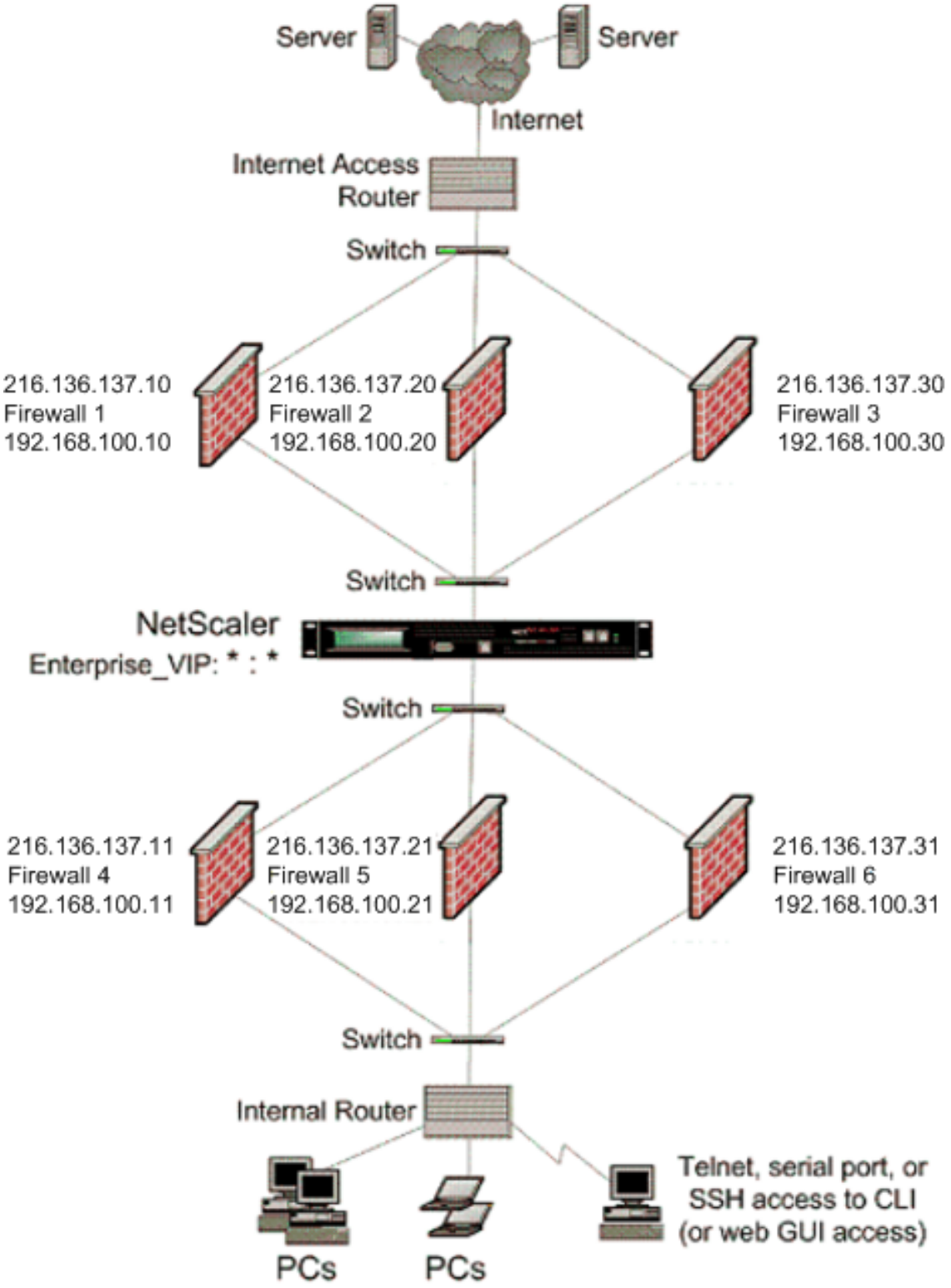
Multiple-Firewall-Umgebung

October 5, 2021

In einer Umgebung mit mehreren Firewalls befindet sich die Citrix ADC Appliance zwischen zwei Gruppen von Firewalls, dem externen Satz, der eine Verbindung mit dem öffentlichen Internet herstellt, und dem internen Satz, der eine Verbindung mit dem internen privaten Netzwerk herstellt. Der externe Satz behandelt in der Regel den Egress-Datenverkehr. Diese Firewalls implementieren hauptsächlich Zugriffssteuerungslisten, um den Zugriff auf externe Ressourcen zu erlauben oder zu verweigern. Der interne Satz behandelt normalerweise den eingehenden Datenverkehr. Diese Firewalls implementieren Sicherheit, um das Intranet vor bösartigen Angriffen abgesehen vom Lastenausgleich des eingehenden Datenverkehrs zu schützen. In der Umgebung mit mehreren Firewalls können Sie den Lastenausgleich von einem anderen Firewall ausgehenden Datenverkehr ausgleichen. Standardmäßig wird der von einer Firewall ausgehende Datenverkehr auf der anderen Firewall über eine Citrix ADC Appliance nicht Lastausgleich ausgeführt. Die Aktivierung des Firewall-Lastausgleichs auf beiden Seiten von Citrix ADC verbessert den Datenverkehr sowohl in der Aus- als auch in der Einlaufrichtung und sorgt für eine schnellere Verarbeitung des Datenverkehrs.

Die folgende Abbildung zeigt eine Lastausgleichsumgebung mit mehreren Firewalls

Abbildung 1. Firewall-Lastenausgleich (Multiple-Firewall)



Mit einer Konfiguration wie in Abbildung 1 können Sie Citrix ADC so konfigurieren, dass der Datenverkehr über die interne Firewall Lastverteilung erfolgt, auch wenn er von einer externen Firewall aus-

geglichen wird. Wenn diese Funktion konfiguriert ist, wird beispielsweise der Datenverkehr, der von den externen Firewalls (Firewalls 1, 2 und 3) kommt, auf den internen Firewalls (Firewalls 4, 5 und 6) Lastausgleich und umgekehrt.

Der Firewall-Lastausgleich wird nur für den virtuellen MAC-Modus LB Server unterstützt.

Der Diensttyp ANY konfiguriert den Citrix ADC so, dass er den gesamten Datenverkehr akzeptiert.

Um Vorteile im Zusammenhang mit HTTP und TCP zu nutzen, konfigurieren Sie den Dienst und den virtuellen Server mit dem Typ HTTP oder TCP. Damit FTP funktioniert, konfigurieren Sie den Dienst mit dem Typ FTP.

Konfigurieren des Citrix ADC in einer Umgebung mit mehreren Firewalls

Um eine Citrix ADC Appliance in einer Umgebung mit mehreren Firewalls zu konfigurieren, müssen Sie die Lastenausgleichsfunktion aktivieren, einen virtuellen Server für den Lastausgleich des ausgehenden Datenverkehrs über die externen Firewalls konfigurieren, einen virtuellen Server für den Lastausgleich des eingehenden Datenverkehrs über die internen Firewalls konfigurieren und aktivieren Sie den Firewall-Lastausgleich auf der Citrix ADC Appliance. Um einen virtuellen Server für den Lastenausgleich über eine Firewall in der Umgebung mit mehreren Firewalls zu konfigurieren, müssen Sie:

1. Konfigurieren eines Platzhalterdiensts für jede Firewall
2. Konfigurieren eines Monitors für jeden Platzhalterdienst
3. Konfigurieren eines virtuellen Wildcard-Servers zum Lastenausgleich des an die Firewalls gesendeten Datenverkehrs
4. Konfigurieren des virtuellen Servers im MAC-Umschreibmodus
5. Binden von Firewalldiensten an den virtuellen Wildcard-Server

Aktivieren der Lastausgleichs-Funktion

Um Lastausgleichseinheiten wie Dienste und virtuelle Server zu konfigurieren und zu implementieren, müssen Sie die Lastenausgleichsfunktion auf dem Citrix ADC Gerät aktivieren.

So aktivieren Sie den Lastenausgleich mit der CLI:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um den Lastausgleich zu aktivieren und die Konfiguration zu überprüfen:

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


Beispiel:

```
enable ns feature LoadBalancing
Done
show ns feature
Feature Acronym Status
------- ------- ------
1) Web Logging WL OFF
2) Surge Protection SP ON
3) Load Balancing LB ON
.
.
.
24) NetScaler Push push OFF
Done
<!--NeedCopy-->
```

So aktivieren Sie den Lastausgleich mit der GUI:

1. Erweitern Sie im Navigationsbereich System, und klicken Sie dann auf Einstellungen.
2. Klicken Sie im Bereich Einstellungen unter Modi und Features auf Grundfunktionen ändern.
3. Aktivieren Sie im Dialogfeld Grundfunktionen konfigurieren das Kontrollkästchen Lastenausgleich, und klicken Sie dann auf OK.

Konfigurieren eines Platzhalterdiensts für jede Firewall

Um Datenverkehr aus allen Protokollen zu akzeptieren, müssen Sie den Platzhalterdienst für jede Firewall konfigurieren, indem Sie die Unterstützung für alle Protokolle und Ports angeben.

So konfigurieren Sie einen Platzhalterdienst für jede Firewall mit der CLI:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die Unterstützung für alle Protokolle und Ports zu konfigurieren:

```
add service <name>@ <serverName> <serviceType> <port_number>
<!--NeedCopy-->
```

Beispiel:

```
add service fw-svc1 10.102.29.5 ANY *
<!--NeedCopy-->
```


So konfigurieren Sie einen Platzhalterdienst für jede Firewall mit der GUI:

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Dienste erstellen Werte für die folgenden Parameter an:
   - Dienstname — Name
   - Server — Servername

   -* Ein erforderlicher Parameter
4. Wählen Sie unter Protokoll die Option Beliebig und in Port die Option * aus.
5. Klicken Sie auf Erstellenund dann auf Schließen. Der erstellte Dienst wird im Bereich Dienste angezeigt.

Konfigurieren eines Monitors für jeden Dienst

Ein PING-Monitor ist standardmäßig an den Dienst gebunden. Sie müssen einen transparenten Monitor konfigurieren, um Hosts auf der vertrauenswürdigen Seite über einzelne Firewalls zu überwachen. Anschließend können Sie den transparenten Monitor an Dienste binden. Der standardmäßige PING-Monitor überwacht nur die Konnektivität zwischen der Citrix ADC Appliance und dem Upstream-Gerät. Der transparente Monitor überwacht alle Geräte, die im Pfad von der Appliance zu dem Gerät vorhanden sind, dem die im Monitor angegebene Ziel-IP-Adresse gehört. Wenn kein transparenter Monitor konfiguriert ist und der Status der Firewall UP ist, aber eines der nächsten Hop-Geräte dieser Firewall ausgefallen ist, schließt die Appliance die Firewall während des Lastenausgleichs ein und leitet das Paket an die Firewall weiter. Das Paket wird jedoch nicht an das endgültige Ziel geliefert, da eines der nächsten Hop-Geräte ausgefallen ist. Wenn eines der Geräte (einschließlich der Firewall) ausgefallen ist, wird der Dienst durch Bindung eines transparenten Monitors als DOWN gekennzeichnet, und die Firewall ist nicht enthalten, wenn die Appliance den Lastausgleich der Firewall durchführt.

Das Binden eines transparenten Monitors überschreibt den PING-Monitor. Um einen PING-Monitor zusätzlich zu einem transparenten Monitor zu konfigurieren, müssen Sie nach dem Erstellen und Binden eines transparenten Monitors einen PING-Monitor an den Dienst binden.

So konfigurieren Sie einen transparenten Monitor mit der CLI:

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

```
1 add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
     transparent (YES | NO )]
2 bind lb monitor <monitorName> <serviceName>
3 <!--NeedCopy-->
```


Beispiel:

```
add monitor monitor-HTTP-1 HTTP -destip 10.10.10.11 -transparent YES
bind monitor monitor-HTTP-1 fw-svc1
<!--NeedCopy-->
```

Die Citrix ADC Appliance lernt die Server-L2-Parameter vom Monitor, der an den Dienst gebunden ist. Konfigurieren Sie für UDP-ECV-Monitore eine Empfangszeichenfolge, damit die Appliance die L2-Parameter des Servers erlernen kann. Wenn die Empfangszeichenfolge nicht konfiguriert ist und der Server nicht antwortet, lernt die Appliance die L2-Parameter nicht, aber der Dienst ist auf UP festgelegt. Der Verkehr für diesen Dienst wird in ein schwarzes Loch gestellt.

So konfigurieren Sie eine Empfangszeichenfolge mit der CLI:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr|*>] [-
    transparent (YES | NO )] [-send <string>] [-recv <string>]
<!--NeedCopy-->
```

Beispiel:

```
add lb monitor monitor-udp-1 udp-ecv -destip 10.10.10.11 -transparent
    YES  - send "test message"  - recv "site_is_up"
<!--NeedCopy-->
```

So erstellen und binden Sie einen transparenten Monitor mit der GUI:

1. Navigieren Sie zu Traffic Management > Load Balancing > Monitore.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Monitor erstellen Werte für die folgenden Parameter an:
   - Namen*
   - Typ*—Typ
   - Ziel-IP
   - Folie

   -* Ein erforderlicher Parameter
4. Klicken Sie auf Erstellenund dann auf Schließen. Wählen Sie im Bereich Monitore den Monitor aus, den Sie gerade konfiguriert haben, und stellen Sie sicher, dass die am unteren Bildschirmrand angezeigten Einstellungen korrekt sind.

Konfigurieren eines virtuellen Servers zum Lastenausgleich des an die Firewalls gesendeten Datenverkehrs

Um den Lastausgleich jeder Art von Datenverkehr auszugleichen, müssen Sie einen virtuellen Platzhalterserver konfigurieren, der das Protokoll und den Port als beliebigen Wert angibt.

So konfigurieren Sie einen virtuellen Server für den Lastenausgleich des an die Firewalls gesendeten Datenverkehrs mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
add lb vserver <name>@ <serviceType> <IPAddress> <port_number>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-1 ANY * *
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Server für den Lastausgleich des Datenverkehrs, der über die GUI an die Firewalls gesendet wird:

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Wählen Sie unter Protokoll die Option Any aus, und wählen Sie unter IP Address und Port die Option * aus.
4. Klicken Sie auf Erstellenund dann auf Schließen. Der erstellte virtuelle Server wird im Bereich Virtuelle Server für Lastenausgleich angezeigt.

Konfigurieren des virtuellen Servers für den MAC-Umschreibmodus

Um den virtuellen Server so zu konfigurieren, dass die MAC-Adresse für die Weiterleitung des eingehenden Datenverkehrs verwendet wird, müssen Sie den MAC-Umschreibmodus aktivieren.

So konfigurieren Sie den virtuellen Server im MAC-Umschreibmodus mithilfe der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set lb vserver <name>@ -m <RedirectionMode>
<!--NeedCopy-->
```


Beispiel:

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```

So konfigurieren Sie den virtuellen Server im MAC-Umschreibmodus mit der GUI:

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie den Umleitungsmodus konfigurieren möchten (z. B. vServer-LB1), und klicken Sie dann auf Öffnen.
3. Klicken Sie auf der Registerkarte Erweitert unter Umleitungsmodus auf Öffnen.
4. Klicken Sie auf OK.

Binden von Firewalldiensten an den virtuellen Server

Um auf einen Dienst auf der Citrix ADC Appliance zuzugreifen, müssen Sie ihn an einen virtuellen Platzhalterserver binden.

So binden Sie Firewalldienste mit der CLI an den virtuellen Server:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

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

Beispiel:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

So binden Sie Firewall-Dienste mit der GUI an den virtuellen Server:

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie den Umleitungsmodus konfigurieren möchten (z. B. vServer-LB1), und klicken Sie dann auf Öffnen.
3. Aktivieren Sie im Dialogfeld Virtuellen Server konfigurieren (Load Balancing) auf der Registerkarte Dienste das Kontrollkästchen Aktiv neben dem Dienst, den Sie an den virtuellen Server binden möchten (z. B. Service-HTTP-1).
4. Klicken Sie auf OK.

Konfigurieren des Lastenausgleichs mit mehreren Firewalls auf der Citrix ADC Appliance

Um den Lastenausgleich auf beiden Seiten eines Citrix ADC über den Firewall-Lastenausgleichs zu verwenden, müssen Sie den Lastenausgleich Mulit-Firewall-Firewall-Parameter mit dem vServerSpecificMac-Parameters aktivieren.

So konfigurieren Sie den Lastenausgleich mit mehreren Firewalls mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set lb parameter -vServerSpecificMac <status>
<!--NeedCopy-->
```

Beispiel:

```
set lb parameter -vServerSpecificMac ENABLED
<!--NeedCopy-->
```

So konfigurieren Sie den Lastenausgleich mit mehreren Firewalls mit der GUI:

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie im Detailbereich den virtuellen Server aus, für den Sie den Umleitungsmodus konfigurieren möchten (z. B. Load Balancing Parameter konfigurieren).
3. Aktivieren Sie im Dialogfeld Lastausgleichsparameter festlegen das Kontrollkästchen Virtual Server Specific MAC.
4. Klicken Sie auf OK.

Speichern und Überprüfen der Konfiguration

Wenn Sie die Konfigurationsaufgaben abgeschlossen haben, speichern Sie die Konfiguration. Sie sollten auch überprüfen, ob die Einstellungen korrekt sind.

So speichern und überprüfen Sie die Konfiguration mit der CLI:

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

- save ns config
- show vserver

Beispiel:


```
save config
show lb vserver FWLBVIP2
        FWLBVIP2 (\*:\*) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Mon Jun 14 07:22:54 2010
        Time since last state change: 0 days, 00:00:32.760
        Effective State: UP
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  2 (Total)       2 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: A new service is bound
        Mode: MAC
        Persistence: NONE
        Connection Failover: DISABLED

1) fw-int-svc1 (10.102.29.5: *) - ANY State: UP Weight: 1
2) fw-int-svc2 (10.102.29.9: \*) - ANY State: UP Weight: 1
 Done
show service fw-int-svc1
        fw-int-svc1 (10.102.29.5:\*) - ANY
        State: DOWN
        Last state change was at Thu Jul  8 14:44:51 2010
        Time since last state change: 0 days, 00:01:50.240
        Server Name: 10.102.29.5
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): NO
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
                State: DOWN     Weight: 1
                Probes: 9       Failed [Total: 9 Current: 9]
                Last response: Failure - Time out during TCP connection
```



```
                        establishment stage
45                  Response Time: 2000.0 millisec
46 2)      Monitor Name: ping
47                  State: UP       Weight: 1
48                  Probes: 3       Failed [Total: 0 Current: 0]
49                  Last response: Success - ICMP echo reply received.
50                  Response Time: 1.275 millisec
51  Done
52 <!--NeedCopy-->
```

So speichern und überprüfen Sie die Konfiguration mit der GUI:

1. Klicken Sie im Detailbereich auf Speichern.
2. Klicken Sie im Dialogfeld Konfiguration speichern auf Ja.
3. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
4. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie in Schritt 5 erstellt haben, und überprüfen Sie, ob die im Detailbereich angezeigten Einstellungen korrekt sind.
5. Navigieren Sie zu Traffic Management > Load Balancing > Services.
6. Wählen Sie im Detailbereich den Dienst aus, den Sie in Schritt 5 erstellt haben, und überprüfen Sie, ob die im Detailbereich angezeigten Einstellungen korrekt sind.

Überwachen eines Firewall-Load Balancing-Setups in einer Umgebung mit mehreren Firewall

Nachdem die Konfiguration ausgeführt wurde und ausgeführt wurde, sollten Sie die Statistiken für jeden Dienst und jeden virtuellen Server anzeigen, um auf mögliche Probleme zu überprüfen.

Anzeigen der Statistiken eines virtuellen Servers

Um die Leistung virtueller Server zu bewerten oder Probleme zu beheben, können Sie Details der virtuellen Server anzeigen, die auf der Citrix ADC Appliance konfiguriert sind. Sie können eine Zusammenfassung der Statistiken für alle virtuellen Server anzeigen, oder Sie können den Namen eines virtuellen Servers angeben, um die Statistiken nur für diesen virtuellen Server anzuzeigen. Sie können die folgenden Details anzeigen:

- Name
- IP-Adresse
- Port
- Protokoll
- Status des virtuellen Servers
- Rate der empfangenen Anfragen
- Trefferrate

So zeigen Sie Statistiken über virtuelle Server mit der Befehlszeilenschnittstelle an

Um eine Zusammenfassung der Statistiken für alle virtuellen Server anzuzeigen, die derzeit auf der Citrix ADC Appliance oder für einen einzelnen virtuellen Server konfiguriert sind, geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat lb vserver [-detail] [<name>]
<!--NeedCopy-->
```

Beispiel:

```
>stat lb vserver -detail
Virtual Server(s) Summary
                        vsvrIP  port     Protocol        State    Req/s
                             Hits/s
One                          *    80         HTTP           UP      5/s
        0/s
Two                          *     0          TCP         DOWN      0/s
        0/s
Three                        *  2598          TCP         DOWN      0/s
        0/s
dnsVirtualNS    10.102.29.90    53          DNS         DOWN      0/s
        0/s
BRVSERV            10.10.1.1    80         HTTP         DOWN      0/s
        0/s
LBVIP           10.102.29.66    80         HTTP           UP      0/s
        0/s
 Done


<!--NeedCopy-->
```

So zeigen Sie virtuelle Serverstatistiken mit der GUI an:

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server > Statistiken.
2. Wenn Sie die Statistiken nur für einen virtuellen Server anzeigen möchten, wählen Sie im Detailbereich den virtuellen Server aus und klicken Sie auf Statistiken.

Statistiken eines Dienstes anzeigen

Mithilfe der Dienststatistiken können Sie die Rate von Anforderungen, Antworten, Anforderungsbytes, Antwortbytes, aktuelle Clientverbindungen, Anforderungen in Überspannungswarteschlange,

aktuelle Serververbindungen usw. anzeigen.

So zeigen Sie die Statistiken eines Dienstes mithilfe der Befehlszeilenschnittstelle an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat service <name>
<!--NeedCopy-->
```

Beispiel:

```
stat service Service-HTTP-1
<!--NeedCopy-->
```

So zeigen Sie die Statistiken eines Dienstes mit der GUI an:

1. Navigieren Sie zu Traffic Management > Load Balancing > Services > Statistiken.
2. Wenn Sie die Statistiken für nur einen Dienst anzeigen möchten, wählen Sie den Dienst aus und klicken Sie auf Statistiken.

Globaler Serverlastausgleich

October 5, 2021

> **Hinweise:**
>
> - Ab Release 13.0 Build 41.x sind Global Server Load Balancing (GSLB) -Bereitstellungen, die die Citrix ADC Appliance verwenden, vollständig mit dem DNS-Flag-Tag 2019 kompatibel.
> - Die GSLB-Funktion ist in den Lizenzen Citrix ADC Advance und Premium Edition enthalten. Die Citrix ADC Optionslizenz wird von der Standard Edition unterstützt.

Für GSLB konfigurierte Citrix ADC Appliances bieten Disaster Recovery und gewährleisten eine kontinuierliche Verfügbarkeit von Anwendungen, indem sie vor Ausfallpunkten in einem WAN schützen. GSLB gleicht die Last über Rechenzentren hinweg aus, indem Clientanforderungen an das nächstgelegene oder leistungsstärkste Rechenzentrum oder an überlebende Rechenzentren weitergeleitet werden, wenn ein Ausfall vorliegt.

In einer typischen Konfiguration sendet ein lokaler DNS-Server Clientanforderungen an einen virtuellen GSLB-Server, an den GSLB-Dienste gebunden sind. Ein GSLB-Dienst identifiziert einen virtuellen Lastausgleichs- oder Content Switching-Server, der sich am lokalen Standort oder an einem Remotestandort befinden kann. Wenn der virtuelle GSLB-Server einen virtuellen Lastausgleichs-

oder Content Switching-Server an einem Remotestandort auswählt, sendet er die IP-Adresse des virtuellen Servers an den DNS-Server. Der DNS-Server sendet es an den Client. Der Client sendet die Anforderung dann erneut an den neuen virtuellen Server mit der neuen IP.

Die GSLB-Entitäten, die Sie konfigurieren müssen, sind die GSLB-Sites, die GSLB-Dienste, die virtuellen GSLB-Server, Lastausgleichs- oder Content Switching-Server sowie autorisierende DNS-Dienste (ADNS). Sie müssen auch MEP konfigurieren. Sie können DNS-Ansichten auch so konfigurieren, dass Clients, die von verschiedenen Standorten aus auf das Netzwerk zugreifen, verschiedene Teile des Netzwerks verfügbar gemacht werden.

> **Hinweis:**
>
> Um die Vorteile der GSLB-Funktionen voll auszunutzen, verwenden Sie ADC-Appliances für Lastausgleich oder Content Switching in jedem Rechenzentrum, damit Ihre GSLB-Konfiguration den proprietären MEP zum Austausch von Standortmetriken verwenden kann.

Funktionsweise von GSLB

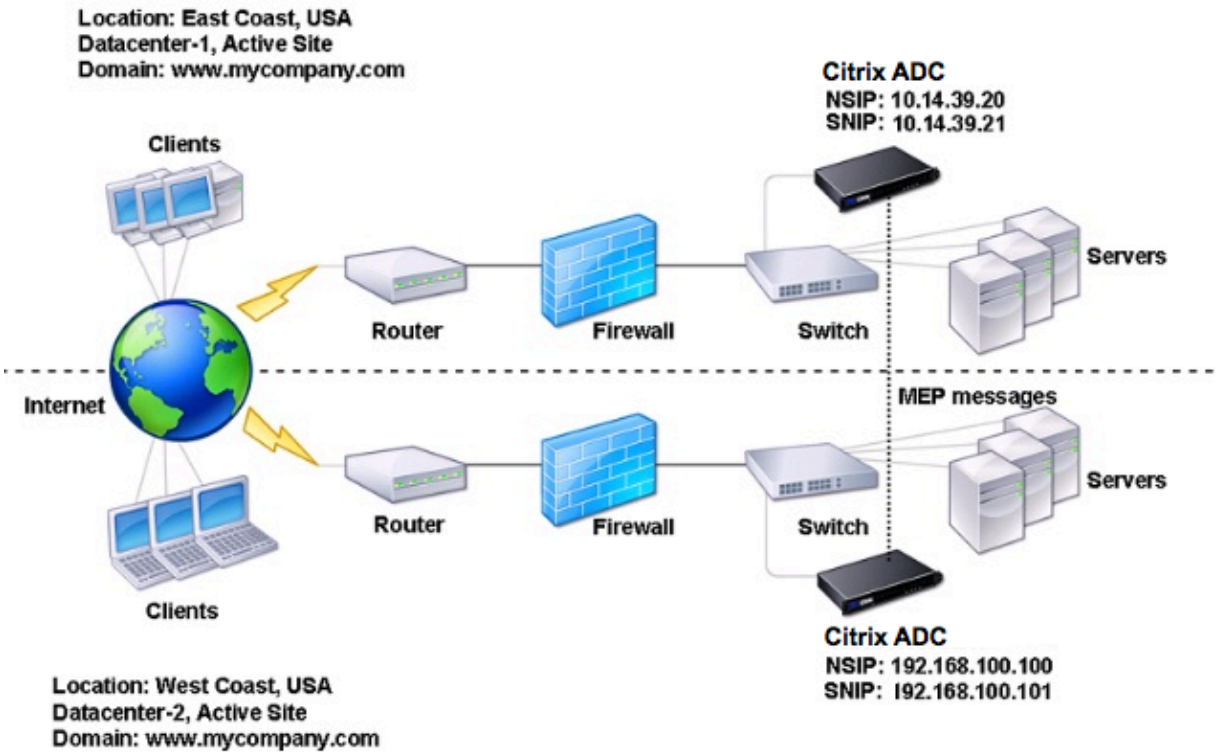
Bei gewöhnlichem DNS erhält ein Client, wenn eine DNS-Anforderung (Domain Name System) sendet, eine Liste der IP-Adressen der Domäne oder des Dienstes. Im Allgemeinen wählt der Client die erste IP-Adresse in der Liste aus und initiiert eine Verbindung mit diesem Server. Der DNS-Server verwendet eine Technik namens DNS Round Robin, um die IP-Adressen in der Liste zu drehen. Es sendet die erste IP-Adresse an das Ende der Liste und fördert die anderen, nachdem sie auf jede DNS-Anforderung reagiert. Diese Technik gewährleistet eine gleichmäßige Verteilung der Last, unterstützt jedoch keine Disaster Recovery, Lastausgleich basierend auf Last oder Nähe von Servern oder Persistenz.

Wenn Sie GSLB auf ADC-Appliances konfigurieren und MEP aktivieren, wird die DNS-Infrastruktur verwendet, um den Client mit dem Rechenzentrum zu verbinden, das die festgelegten Kriterien am besten erfüllt. Die Kriterien können Folgendes bezeichnen:

- Am wenigsten belastetes Rechenzentrum
- Das nächste Rechenzentrum
- Rechenzentrum, das am schnellsten auf Anfragen vom Standort des Kunden reagiert
- Eine Kombination dieser Metriken und SNMP-Metriken.

Eine Appliance verfolgt den Standort, die Leistung, die Last und die Verfügbarkeit jedes Rechenzentrums. Diese Faktoren werden verwendet, um das Rechenzentrum auszuwählen, das die Clientanforderung gesendet werden soll.

Die folgende Abbildung zeigt eine grundlegende GSLB-Topologie.



Eine GSLB-Konfiguration besteht aus einer Gruppe von GSLB-Entitäten auf jeder Appliance in der Konfiguration. Zu diesen Entitäten gehören GSLB-Sites, GSLB-Dienste, GSLB-Servicegruppen, virtuelle GSLB-Server, Lastausgleichsserver, Content Switching-Server und ADNS-Dienste.

GSLB-Bereitstellungstypen

October 5, 2021

Citrix ADC Appliances, die für den globalen Server Load Balancing (GSLB) konfiguriert sind, sorgen für die Disaster Recovery und gewährleisten die kontinuierliche Verfügbarkeit von Anwendungen, indem sie vor Fehlerpunkten in einem WAN (Wide Area Network) schützen. GSLB kann die Last über Rechenzentren hinweg ausgleichen, indem Clientanforderungen an das nächstgelegene oder leistungsstärkste Rechenzentrum weitergeleitet werden oder im Falle eines Ausfalls an überlebende Rechenzentren weitergeleitet werden.

Im Folgenden sind einige der typischen GSLB-Bereitstellungstypen aufgeführt:

- Aktiv-aktive Standortbereitstellung
- Aktiv-Passiv-Standortbereitstellung
- Übergeordnete und untergeordnete Topologiebereitstellung

Aktiv-aktive Standortbereitstellung

October 5, 2021

Ein aktiv-aktiver Standort besteht aus mehreren aktiven Rechenzentren. Clientanforderungen werden über aktive Rechenzentren hinweg Lastausgleich durchgeführt. Dieser Bereitstellungstyp kann verwendet werden, wenn Sie eine globale Verteilung des Datenverkehrs in einer verteilten Umgebung benötigen.

Alle Sites in einer Aktiv-Aktiv-Bereitstellung sind aktiv, und alle Dienste für eine bestimmte Anwendung/Domäne sind an denselben virtuellen GSLB-Server gebunden. Sites tauschen Metriken über das Metrics Exchange Protocol (MEP) aus. Standortmetriken, die zwischen den Sites ausgetauscht werden, umfassen den Status der einzelnen Lastausgleichs- und Content Switching-Server, die aktuelle Anzahl der Verbindungen, die aktuelle Paketrate und die aktuelle Bandbreitenauslastung. Die Citrix ADC Appliance benötigt diese Informationen, um den Lastausgleich an den Sites durchzuführen.

Eine aktive Bereitstellung kann maximal 32 GSLB-Sites umfassen, da MEP nicht mehr als 32 Sites synchronisieren kann. In diesem Bereitstellungstyp sind keine Backupsites konfiguriert.

Die Citrix ADC Appliance sendet Clientanforderungen an den entsprechenden GSLB-Site gemäß der in der GSLB-Konfiguration angegebenen GSLB-Methode.

Für eine aktive Bereitstellung können Sie die folgenden GSLB-Methoden konfigurieren.

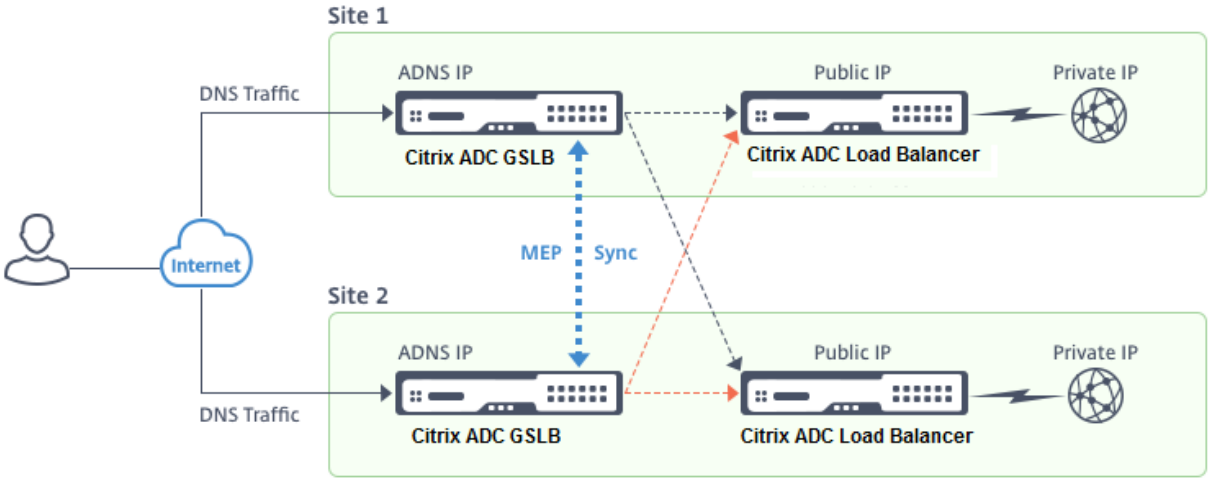
- Runde Robin
- Geringste Verbindungen
- Kleinste Reaktionszeit
- Geringste Bandbreite
- Am wenigsten Pakete
- Quell-IP-Hash
- Benutzerdefinierte Last
- Roundtrip-Zeit (RTT)
- Statische Nähe

> Hinweis:
>
> - Wenn MEP deaktiviert ist, werden die folgenden GSLB-Methoden standardmäßig auf die Round Robin-Methode eingestellt.
>   - RTT
>   - Kleinste Verbindungen
>   - Kleinste Bandbreite
>   - Kleinste Pakete
>   - Kleinste Reaktionszeit

- Bei der statischen Näherungsmethode GLSB sendet die Appliance die Anforderung an die IP-Adresse des Standorts, die den Näherungskriterien am besten entspricht.
- Bei der Round Trip Time -Methode werden die Werte der dynamischen Round Trip Time (RTT) die IP-Adresse des am besten ausführenden Standorts ausgewählt. RTT ist ein Maß für die Verzögerung im Netzwerk zwischen dem lokalen DNS-Server des Clients und einer Datenressource.

GSLB Aktiv-Aktiv-Rechenzentrum-Topologie

Im Diagramm sind Standort 1 und Standort 2 aktive GLSB-Sites.



Wenn der Client eine DNS-Anforderung sendet, landet er an einem der aktiven Sites.

Wenn Standort 1 die Clientanforderung empfängt, wählt der virtuelle GSLB-Server in Standort 1 einen virtuellen Lastausgleichs- oder Content Switching-Server aus und sendet die IP-Adresse des virtuellen Servers an den DNS-Server, der ihn an den Client sendet. Der Client sendet die Anforderung dann erneut an den neuen virtuellen Server unter der neuen IP-Adresse.

Da beide Sites aktiv sind, wertet der GSLB-Algorithmus die Dienste an beiden Sites aus, wenn eine Auswahl gemäß der konfigurierten GSLB-Methode getroffen wird.

Aktiv-Passiv-Standortbereitstellung

October 5, 2021

Ein aktiv-passiver Standort besteht aus einem aktiven und einem passiven Rechenzentrum. Dieser Bereitstellungstyp ist ideal für die Notfallwiederherstellung.

Bei dieser Art der Bereitstellung sind einige Sites (Remotesites) nur für die Notfallwiederherstellung reserviert. Diese Sites nehmen nicht an einer Entscheidungsfindung teil, bis alle aktiven Sites DOWN

sind. Ein passiver Standort wird erst betriebsbereit, wenn ein Notfallereignis ein Failover auslöst.

Nachdem Sie das primäre Rechenzentrum konfiguriert haben, replizieren Sie die Konfiguration für das Backupdatenzentrum und legen Sie es als passiven GSLB-Standort fest, indem Sie einen virtuellen GSLB-Server an diesem Standort als virtuellen Backupserver festlegen.

Eine aktive und passive Bereitstellung kann maximal 32 GSLB-Sites umfassen, da MEP nicht mehr als 32 Sites synchronisieren kann.

Für eine aktiv-passive Bereitstellung können Sie die folgenden GSLB-Methoden konfigurieren.

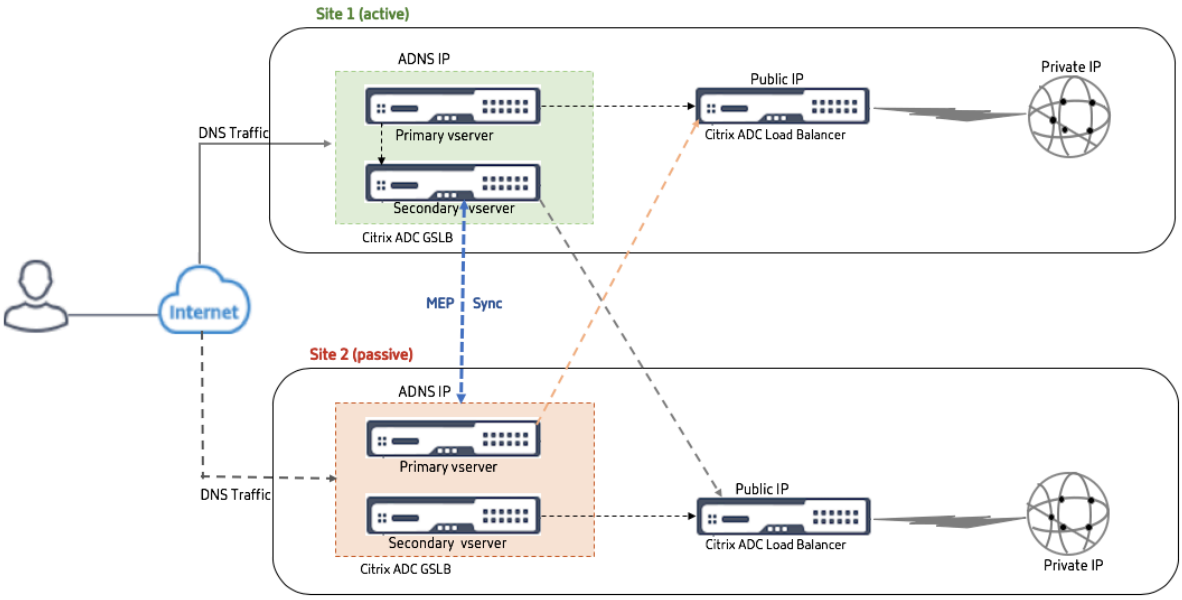
- Runde Robin
- Geringste Verbindungen
- Kleinste Reaktionszeit
- Geringste Bandbreite
- Am wenigsten Pakete
- Quell-IP-Hash
- Benutzerdefinierte Last
- Roundtrip-Zeit (RTT)
- Statische Nähe

Hinweis:

- Wenn MEP deaktiviert ist, werden die folgenden Algorithmusmethoden standardmäßig Round Robin verwendet.
  - RTT
  - Geringste Verbindungen
  - Geringste Bandbreite
  - Am wenigsten Pakete
  - Kleinste Reaktionszeit
- Bei der statischen Näherungsmethode GLSB sendet die Appliance die Anforderung an die IP-Adresse des Standorts, die den Näherungskriterien am besten entspricht.
- Bei der Round Trip Time -Methode werden die Werte der dynamischen Round Trip Time (RTT) die IP-Adresse des am besten ausführenden Standorts ausgewählt. RTT ist ein Maß für die Verzögerung im Netzwerk zwischen dem lokalen DNS-Server des Clients und einer Datenressource.

Aktiv-passives GSLB-Rechenzentrumtopologie

Im Diagramm ist Standort 1 ein aktiver Standort und Standort 2 ein passiver Standort mit derselben Konfiguration wie Standort 1.



Wenn Standort 1 ausfällt, wird Standort 2 betriebsbereit.

Wenn der Client eine DNS-Anforderung sendet, kann die Anforderung an jedem der Sites landen. Die Dienste werden jedoch nur von der aktiven Site (Site1) ausgewählt, solange sie UP ist.

Dienste vom passiven Standort (Standort 2) werden nur ausgewählt, wenn der aktive Standort (Standort 1) DOWN ist.

Bereitstellung von Übergeordnet-Untergeordnet-Topologie mit MEP-Protokoll

March 8, 2022

Citrix ADC GSLB bietet Global Server Load Balancing und Notfallwiederherstellung, indem Mesh-Verbindungen zwischen allen beteiligten Sites hergestellt und intelligente Entscheidungen für den Lastenausgleich getroffen werden. Jede Site kommuniziert mit den anderen, um Server- und Netzwerkmetriken über das Metric Exchange Protocol (MEP) in regelmäßigen Abständen auszutauschen. Mit der Zunahme der Anzahl der Peersites nimmt das Volumen des MEP-Verkehrs jedoch aufgrund der Mesh-Topologie exponentiell zu. Um dies zu umgehen, können Sie eine Übergeordnet-Untergeordnet-Topologie verwenden. Die übergeordnete und untergeordnete Topologie unterstützt auch größere Bereitstellungen. Zusätzlich zu den 32 übergeordneten Sites können Sie 1024 untergeordnete Sites konfigurieren.

Die übergeordnete und untergeordnete GSLB-Topologie ist ein zweistufiges hierarchisches Design mit den folgenden Merkmalen:

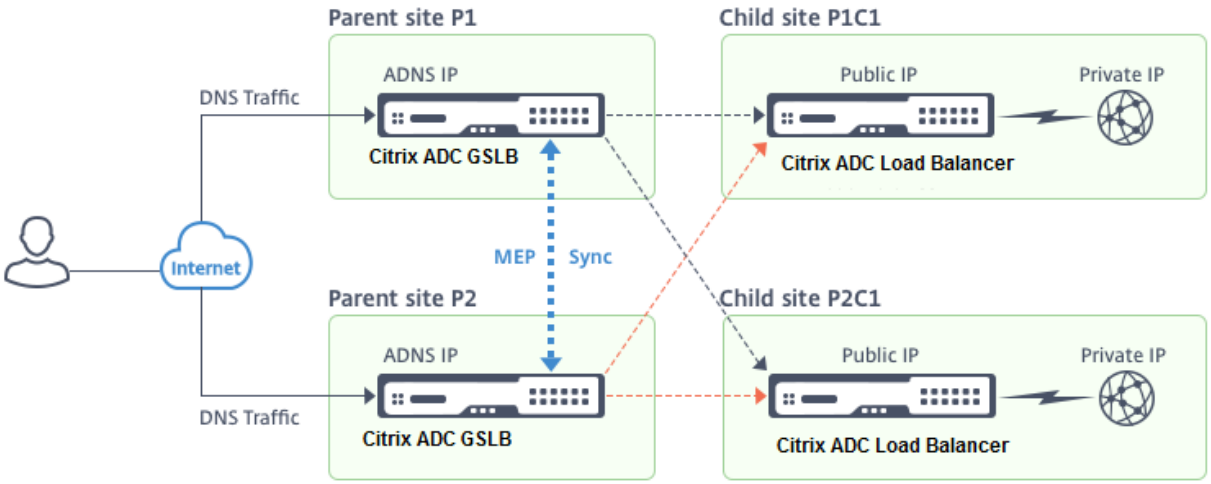
- Auf der obersten Ebene befinden sich übergeordnete Sites, die Peer-Beziehungen zu anderen Eltern haben.
- Jeder Elternteil kann mehrere untergeordnete Sites haben.
- Jede übergeordnete Site tauscht Integritätsinformationen mit den untergeordneten Sites und mit anderen übergeordneten Sites aus.
- Eine untergeordnete Site kommuniziert nur mit ihrer übergeordneter Site.
- In einer Übergeordnet-Untergeordnet-Beziehung für GSLB antwortet nur die übergeordnete Site auf ADNS-Abfragen. Die untergeordneten Sites fungieren als normale Lastausgleichssites.
- Konfigurieren Sie einen ADNS-Dienst oder virtuellen DNS-Lastausgleichsserver nur für die übergeordneten Site.
- Eine übergeordnete Site kann eine normale GSLB-Konfiguration haben, d. h. Dienste von lokalen und allen Remotesites, aber eine untergeordnete Site kann nur lokale Dienste haben. Außerdem sind nur für die übergeordneten Sites virtuelle GSLB-Server konfiguriert.

> **Hinweis**
>
> - In einer übergeordneten und untergeordneten Topologie wird der Austausch von Standortmetriken von der unteren von zwei IP-Adressen initiiert. Ab Citrix ADC Release 11.1 Build 51.x initiieren die übergeordneten Sites jedoch Verbindungen zu den untergeordneten Sites und nicht umgekehrt. Weil die übergeordneten Sites Informationen zu allen untergeordneten Sites im GSLB-Setup enthalten.

- In einer Übergeordnet-Übergeordnet-Verbindung wird der Austausch von Standortmetriken immer noch von der unteren IP von zwei IP-Adressen initiiert.
- In einer Übergeordnet-Untergeordnet-Topologie müssen GSLB-Dienste nicht immer auf einer untergeordneten Site konfiguriert werden. Wenn Sie jedoch über mehr Konfigurationen wie Clientauthentifizierung, Einfügen von Client-IP-Adressen oder andere SSL-spezifische Anforderungen verfügen, müssen Sie für die untergeordnete Site einen expliziten GSLB Service hinzufügen und ihn entsprechend konfigurieren.
- In einer Übergeordnet-Untergeordnet-Topologie können die übergeordnete Site und die untergeordnete Site unterschiedliche Citrix ADC-Softwareversionen haben. Um jedoch die GSLB AutomaticConfigSync-Option zum Synchronisieren der Konfiguration über die übergeordneten Sites hinweg zu verwenden, müssen alle übergeordneten Sites dieselbe Citrix ADC-Softwareversion haben. Wenn Sie die Option AutomaticConfigSync nicht verwenden, können die übergeordnete Site und die untergeordnete Site unterschiedliche Citrix ADC-Softwareversionen haben. Stellen Sie jedoch sicher, dass Sie keine der neuen Features in der neuesten Version verwenden. Dies gilt im Allgemeinen auch für zwei Citrix ADC-Knoten, die an GSLB teilnehmen.

Grundlegende Übergeordnet-Untergeordnet-Topologie

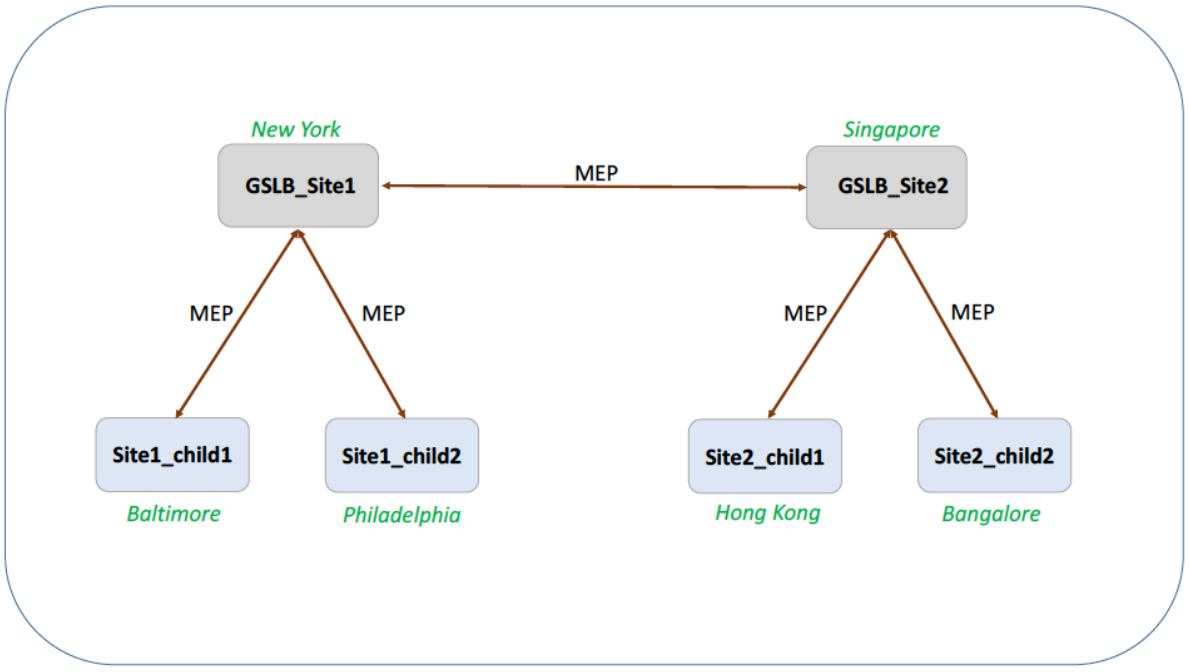
Im Diagramm sind SiteP1 und SiteP2 übergeordnete Sites in einer Peer-Beziehung. Site P1C1 und P2C1 sind die untergeordneten Sites von P1 bzw. P2.



Einrichten einer Übergeordnet-Untergeordnet-Konfiguration für GSLB

Wenn Sie eine Firewall für eine GSLB-Site konfiguriert haben, stellen Sie sicher, dass Port 3011 geöffnet ist.

Das folgende Diagramm zeigt ein Beispiel für eine Übergeordnet-Untergeordnet-Konfiguration.



- Die Konfiguration einer untergeordneten Site umfasst die untergeordnete Site und deren übergeordnete Site, aber keine anderen übergeordneten oder untergeordneten Sites.

- Netzwerkmetriken wie RTT- und Persistenzsitzungsinformationen werden nur über die übergeordneten Sites hinweg synchronisiert. Daher sind Parameter wie nwMetricExchange und sessionExchange standardmäßig auf allen untergeordneten Sites deaktiviert.
- Um die korrekte Übergeordnet-Untergeordnet-Konfiguration zu überprüfen, überprüfen Sie den Status aller GSLB Services, die an die übergeordneten Sites gebunden sind.

So richten Sie über die CLI eine Übergeordnet-Untergeordnet-Konfiguration für GSLB ein:

1. Konfigurieren Sie für jede übergeordnete Site alle untergeordneten Sites, die übergeordneten Peer-Sites und die untergeordneten Sites, die mit den Peer-Sites verknüpft sind:

   Verwenden Sie beim Hinzufügen einer übergeordneten Site den folgenden Befehl:

   ```
   add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
       ipv6_addr|*>]
   <!--NeedCopy-->
   ```

   Verwenden Sie beim Hinzufügen einer untergeordneten Site den folgenden Befehl:

   ```
   add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
       ipv6_addr|*>] [-parentSite <string>]
   <!--NeedCopy-->
   ```

2. Konfigurieren Sie für untergeordneten Sites die jeweilige untergeordnete Site und ordnen Sie die untergeordnete Site auch der übergeordneten Site zu:

   > **Hinweis:**
   >
   > Konfigurieren Sie die übergeordnete Site und die Verknüpfung mit der untergeordneten Sie korrekt. Sie müssen beispielsweise site1_child1 mit GSLB_Site1 konfigurieren. Sie können site1_child1 nicht mit GSLB_Site2 konfigurieren.

   Verwenden Sie den folgenden Befehl, um die übergeordnete Site zu konfigurieren, mit der die untergeordnete Site verknüpft ist:

   ```
   add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
       ipv6_addr|*>]
   <!--NeedCopy-->
   ```

   Verwenden Sie den folgenden Befehl, um eine untergeordnete Site hinzuzufügen und sie der übergeordneten Site zuzuordnen:


```
add gslb site <siteName> <siteIPAddress> [-publicIP <ip_addr|
    ipv6_addr|*>] [-parentSite <string>]
<!--NeedCopy-->
```

Ein vollständiges Beispiel für eine Übergeordnet-Untergeordnet-Konfiguration über die Befehlszeilenschnittstelle finden Sie unter Beispiel einer vollständigen Übergeordnet-Untergeordnet-Konfiguration über die CLI.

> **Hinweis**
>
> Wenn die IP-Adresse des virtuellen Lastausgleichsservers eine private IP-Adresse ist und sich die öffentliche IP-Adresse von dieser IP-Adresse unterscheidet, müssen Sie einen GSLB Service für den lokalen virtuellen Lastausgleichsserver für die untergeordneten Site konfigurieren. Dies ist für die Statistikerfassung zwischen der übergeordneten und der untergeordneten Site erforderlich.
>
> Geben Sie für die untergeordnete Site an der Eingabeaufforderung Folgendes ein:
>
> `add gslb service <name> <private IP/lb vserver IP> http 80 -sitename <childsite name> -publicip <public IP of LB vserver>`
>
> **Beispiel:**
>
> `add gslb service Service-GSLB 192.168.1.3 http 80 -GSLB_Site11 site 11_lb1 172.16.1.1`
>
> Wobei 192.168.1.3 eine private IP-Adresse des virtuellen Lastausgleichsservers und 172.16.1.1 eine öffentliche IP-Adresse des virtuellen Lastausgleichsservers ist.

Backup einer übergeordneten Site

Hinweis: Diese Funktion wurde in Citrix ADC Release 11.1 Build 51.x eingeführt. Um die Topologie der übergeordneten Backupsite zu verwenden, stellen Sie sicher, dass die übergeordnete Site und die untergeordneten Sites auf Citrix ADC 11.1 Build 51.x und höher sind.

Die Topologie der übergeordneten Backupsite ist in Szenarien nützlich, in denen viele untergeordnete Sites einer übergeordneten Site zugeordnet sind. Wenn diese übergeordnete Site DOWN ist, sind alle untergeordneten Sites nicht mehr verfügbar. Um dies zu verhindern, können Sie jetzt eine übergeordnete Backupsite konfigurieren, zu der die untergeordneten Sites eine Verbindung herstellen können, wenn die ursprüngliche übergeordnete Site DOWN ist. Die übergeordnete Site sendet die übergeordnete Backupliste über die MEP-Nachrichten an die untergeordneten Sites.

Wenn eine übergeordnete Site DOWN ist, erfahren die anderen übergeordneten Sites in der GSLB über MEP, dass eine bestimmte übergeordnete Site DOWN ist, da MEP für diese übergeordnete Site DOWN ist. Die anderen übergeordneten Sites im GSLB-Setup suchen die Backupkette des Peer-

Parent. Die übergeordnete Site mit der höchsten Präferenz übernimmt die untergeordneten Sites der übergeordneten Site, die DOWN ist. Das neue übergeordnete Objekt stellt dann eine Verbindung mit der untergeordneten Site her. Eine untergeordnete Site kann die Verbindung annehmen oder ablehnen, nachdem sie die vorhandenen Verbindungen und die Informationen in der Backupliste ausgewertet hat. Es dauert einige Sekunden, bis die übergeordnete Backupsite die untergeordneten Sites übernommen hat.
Wenn die ursprüngliche übergeordnete Site wieder in Betrieb ist, versucht sie, Verbindungen zu ihren untergeordneten Sites herzustellen, die zu einer anderen übergeordneten Site migriert wurden. Wenn ein Verbindungsversuch erfolgreich ist, wird die untergeordnete Site wieder ihrer ursprünglichen übergeordneten Site zugewiesen.

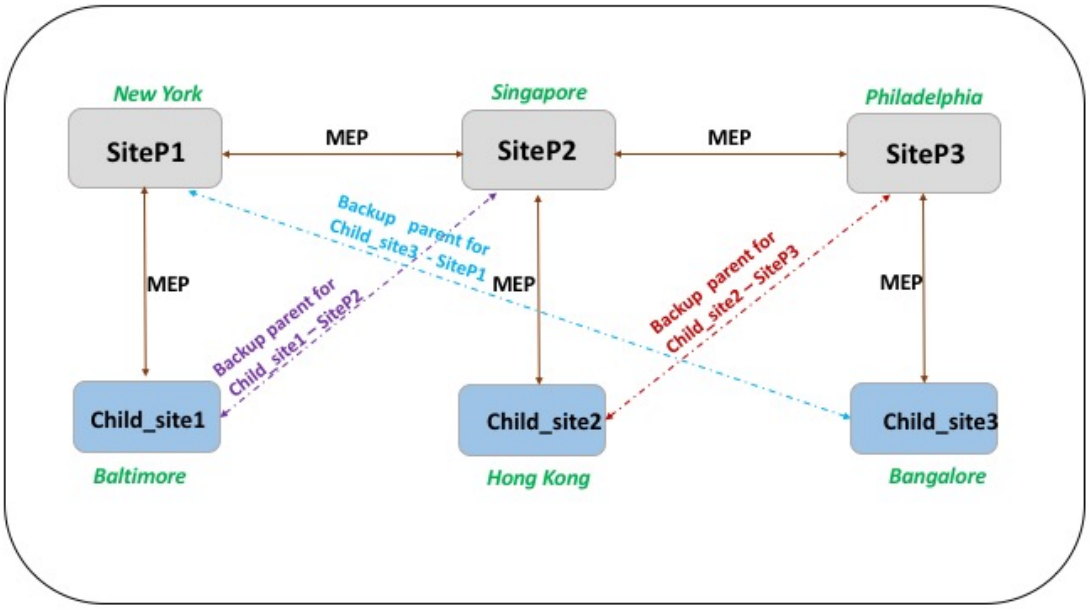
Hinweis:

- Nur übergeordnete Sites können als Backups konfiguriert werden, und diese Konfiguration kann nur in der übergeordneten Site durchgeführt werden.
- Alle untergeordneten Sites verwenden die übergeordnete Backupgruppe.
- Die Synchronisierung erfolgt nur auf den übergeordneten Sites. Die Konfiguration der untergeordneten GSLB-Sites ist von der Synchronisierung nicht betroffen. Dies liegt daran, dass die übergeordnete Site und die untergeordneten Sitekonfigurationen nicht identisch sind. Die Konfiguration der untergeordneten Sites besteht nur aus den Details ihrer eigenen und ihrer übergeordneten Site. Außerdem müssen GSLB-Dienste nicht immer in den untergeordneten Sites konfiguriert werden.

Betrachten Sie die in der folgenden Abbildung gezeigte Konfiguration:

- SiteP1, SiteP2 und SiteP3 sind die übergeordneten Sites.
- child_site1, child_site2 und child_site3 sind die untergeordneten Sites von siteP1, siteP2 und siteP3.
- Backup der übergeordneten Sites;
  - SiteP1-Backup-Übergeordnet— SiteP2 (höhere Präferenz) und SiteP3
  - SiteP2 Backup-Übergeordnet— SiteP3 (höhere Präferenz) und siteP1
  - SiteP3 Backup-Übergeordnet— SiteP1 (höhere Präferenz) und SiteP2

Hinweis: Zur Veranschaulichung zeigt die Abbildung nur ein übergeordnetes Backupobjekt für jede übergeordnete Site.



Die folgende Liste fasst das Verhalten der übergeordneten und untergeordneten Sites in verschiedenen Szenarien zusammen:

- Szenario 1: SiteP1 geht DOWN.
  - SiteP2 und SiteP3 erkennen, dass die MEP-Verbindung von SiteP1 DOWN ist. SiteP2 ist in der Einstellungsliste von Backup-Übergeordnet für SiteP1 höher und versucht daher, eine Verbindung zu child_Site1 herzustellen. SiteP3 geht davon aus, dass child_site1 jetzt die untergeordnete Site der übergeordneter SiteP2 ist.
  - SiteP2 sendet Child_Site1 die Liste von Backup-Übergeordnet von SiteP1 (SiteP2 und SiteP3) an child_Site1. child_site1 verwendet die Liste, um zu entscheiden, ob die Verbindung von SiteP2 akzeptiert oder abgelehnt werden soll. Es akzeptiert die Verbindung und wird untergeordnet zu SiteP2.
  - Wenn SiteP1 wieder aktiv ist, sendet sie child_Site1 eine Verbindungsanfrage. Die neue Anforderung hat Vorrang und child_Site 1 migriert zu SiteP1.
- Szenario 2: Nur die MEP-Verbindung zwischen SiteP1 und SiteP2 ist DOWN. child_site1 lehnt die Verbindungsanfrage von SiteP2 ab, da das übergeordnete Objekt, SiteP1, immer noch UP ist.
- Szenario 3: SiteP3 und Child_Site1 erkennen, dass SiteP1 DOWN ist und die MEP-Verbindung zwischen SiteP3 und SiteP2 ebenfalls DOWN ist. SiteP2 erkennt jedoch, dass SiteP1 aktiv ist und die MEP-Verbindung zwischen SiteP1 und SiteP2 UP ist.
  - SiteP2 ergreift keine Maßnahmen.
  - SiteP3 überprüft die Backupliste von SiteP1 und stellt fest, dass SiteP2 eine höhere Präferenz als SiteP3 hat. Aber SiteP2 ist DOWN, also versucht SiteP3 eine Verbindung mit

child_site1 herzustellen. child_site1 hat erkannt, dass SiteP1 DOWN ist und akzeptiert daher die Verbindungsanfrage von SiteP3.

- Jetzt geht die Verbindung zwischen SiteP1 und SiteP2 DOWN. SiteP2 überprüft die Backupliste von SiteP1 und findet sich als das am meisten bevorzugte Backup wieder, sodass es versucht, eine Verbindung zu child_Site1 herzustellen. child_site1 wertet die neue Verbindungsanforderung basierend auf der Liste von SiteP1 aus und findet SiteP2 als das am meisten bevorzugte Backup, sodass es von SiteP3 auf SiteP2 migriert.

So konfigurieren Sie eine übergeordneten Backupsite über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set gslb site <sitename> -backupParentlist <bkp_site1> <bkp_site2> ... <
   bkp_site5>
<!--NeedCopy-->
```

<sitename> ist die aktuelle übergeordnete Site.

Beispiel:

Für die übergeordneten Site (SiteP1) werden die Sites (SiteP2 und SiteP3) als übergeordnete Backupsites konfiguriert.

```
set gslb site SiteP1 -backupParentlist SiteP2 SiteP3
<!--NeedCopy-->
```

Hinweis:

- Sie können keine neue Site als übergeordnetes Backupobjekt hinzufügen. Sie müssen zuerst alle Sites hinzufügen und dann die Site als übergeordnetes Backupobjekt konfigurieren.
- Um ein übergeordnetes Backupobjekt zu entfernen, müssen Sie den Befehl unset verwenden, mit dem alle Sites aufgehoben werden, die zuvor als übergeordnete Backupsites konfiguriert wurden.

So konfigurieren Sie eine übergeordnete Backupsite über die GUI

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **GSLB** > **Sites**.
2. Fügen Sie eine neue Site hinzu oder wählen Sie eine vorhandene Site aus.
3. Wählen Sie beim Erstellen oder Konfigurieren der GSLB-Site das Optionsfeld **Backup Parent Sites** .

GSLB-Konfigurationsobjekte

October 5, 2021

Eine GSLB-Konfiguration besteht aus einer Gruppe von GSLB-Entitäten auf jeder Appliance in der Konfiguration. Zu diesen Entitäten gehören:

- GSLB-Sites
- GSLB Dienstleistungen
- Virtuelle GSLB Server
- Virtuelle Lastenausgleichs- oder Content Switching-Server
- ADNS-Dienste
- DNS-VIPs

GSLB-Sites

Ein typisches GSLB-Setup besteht aus Rechenzentren, von denen jedes über verschiedene Netzwerk-Appliances verfügt, die möglicherweise Citrix ADC Appliances sind oder nicht. Die Rechenzentren werden GSLB-Sites genannt. Jeder GSLB-Site wird von einer Citrix ADC Appliance verwaltet, die lokal für diese Site ist. Jede dieser Appliances behandelt ihre eigene Site als lokale Site und alle anderen, von anderen Appliances verwalteten Sites als Remotesites.

Wenn die Appliance, die eine Site verwaltet, die einzige Citrix ADC Appliance in diesem Rechenzentrum ist, fungiert die auf dieser Appliance gehostete GSLB-Site als Buchhaltungsplatzhalter für Überwachungszwecke, da keine Metriken erfasst werden können. Dies geschieht in der Regel, wenn die Appliance nur für GSLB verwendet wird und andere Produkte im Rechenzentrum zum Lastenausgleich oder zum Content Switching verwendet werden.

Beziehungen zwischen GSLB-Sites

Das Konzept der Sites ist für Citrix ADC GSLB-Implementierungen von zentraler Bedeutung. Sofern nicht anders angegeben, bilden Websites untereinander eine Peer-Beziehung. Diese Beziehung wird zuerst zum Austausch von Integritätsinformationen und dann zur Verteilung der Last gemäß dem ausgewählten Algorithmus verwendet. In vielen Situationen ist jedoch eine Peer-Beziehung zwischen allen GSLB-Sites nicht wünschenswert. Gründe für die Nichteinführung einer All-Peer-Implementierung könnten sein;

- Um die GSLB-Sites klar zu trennen. Zum Beispiel, um Websites zu trennen, die beim Auflösen von DNS-Abfragen von den Verkehrsverwaltungssites beteiligt sind.
- Reduzieren Sie das Volumen des Metric Exchange Protocol (MEP) Datenverkehrs, der exponentiell mit einer zunehmenden Anzahl von Peer-Sites zunimmt.

Diese Ziele können durch die Verwendung von übergeordneten und untergeordneten GSLB-Sites erreicht werden.

GSLB Dienstleistungen

Ein GSLB-Dienst ist in der Regel eine Darstellung eines virtuellen Lastausgleichs- oder Content Switching-Servers, obwohl er jede Art von virtuellem Server darstellen kann. Der GSLB-Dienst identifiziert die IP-Adresse, die Portnummer und den Diensttyp des virtuellen Servers. GSLB-Dienste sind an virtuelle GSLB-Server auf den Citrix ADC Appliances gebunden, die die GSLB-Sites verwalten. Ein GSLB-Dienst, der an einen virtuellen GSLB-Server im selben Rechenzentrum gebunden ist, ist lokal auf den virtuellen GSLB-Server. Ein GSLB-Dienst, der an einen virtuellen GSLB-Server in einem anderen Rechenzentrum gebunden ist, ist von diesem virtuellen GSLB-Server entfernt.

> **Hinweis:**
>
> Websites und Dienstleistungen sind von Natur aus verbunden, um die Nähe zwischen den beiden anzuzeigen. Das heißt, alle Dienste müssen zu einer Site gehören, und es wird angenommen, dass sie sich aus Gründen der Nähe am gleichen Standort wie die GSLB-Site befinden. Ebenso sind Dienste und virtuelle Server verknüpft, so dass die Logik mit den verfügbaren Ressourcen verknüpft ist.

Virtuelle GSLB Server

Ein virtueller GSLB-Server ist an einen oder mehrere GSLB-Dienste gebunden, und der Lastausgleich zwischen diesen Diensten. Es wertet die konfigurierten GSLB-Methoden (Algorithmen) aus, um den entsprechenden Dienst auszuwählen, an den eine Clientanforderung gesendet werden soll. Da die GSLB-Dienste entweder lokale oder Remote-Server darstellen können, hat die Auswahl des optimalen GSLB-Dienstes für eine Anforderung die Auswählen des Rechenzentrums, das der Clientanforderung dienen soll.

Die Domäne, für die der globale Server-Lastausgleich konfiguriert ist, muss an den virtuellen GSLB-Server gebunden sein, da ein oder mehrere an den virtuellen Server gebundene Dienste Anforderungen für diese Domäne erfüllen.

Im Gegensatz zu anderen virtuellen Servern, die auf einer Citrix ADC Appliance konfiguriert sind, verfügt ein virtueller GSLB-Server nicht über eine eigene virtuelle IP-Adresse (VIP).

Virtuelle Lastenausgleichs- oder Content Switching-Server

Ein virtuellen Lastausgleichs- oder Content Switching-Server stellt einen oder mehrere physische Server im lokalen Netzwerk dar. Clients senden ihre Anforderungen an die virtuelle IP-Adresse (VIP) des virtuellen Lastausgleichs- oder Content Switching-Server, und der virtuelle Server gleicht

die Last auf den physischen Servern aus. Nachdem ein virtueller GSLB-Server einen GSLB-Dienst auswählt, der entweder einen lokalen oder einen Remote-Lastausgleich oder einen virtuellen Content Switching-Server darstellt, sendet der Client die Anforderung an die VIP-Adresse dieses virtuellen Servers.

Weitere Informationen zum Lastenausgleich oder zum Content Switching von virtuellen Servern und Diensten finden Sie unter Load Balancing oder Content Switching.

ADNS-Dienste

Ein ADNS-Dienst ist eine besondere Art von Dienst, der nur auf DNS-Anforderungen für Domänen reagiert, für die die Citrix ADC Appliance autorisierend ist. Wenn ein ADNS-Dienst konfiguriert ist, besitzt die Appliance diese IP-Adresse und gibt sie bekannt. Beim Empfang einer DNS-Anforderung durch einen ADNS-Dienst sucht die Appliance nach einem virtuellen GSLB-Server, der an diese Domäne gebunden ist. Wenn ein virtueller GSLB-Server an die Domäne gebunden ist, wird er nach der besten IP-Adresse abgefragt, an die die DNS-Antwort gesendet werden soll.

DNS-VIPs

Eine virtuelle DNS-IP-Adresse ist eine virtuelle IP-Adresse (VIP), die einen virtuellen DNS-Server für Lastenausgleich auf der Citrix ADC Appliance darstellt. DNS-Anforderungen für Domänen, für die die Citrix ADC Appliance autorisierend ist, können an eine DNS-VIP gesendet werden.

GSLB-Methoden

October 5, 2021

Im Gegensatz zu herkömmlichen DNS-Servern, die einfach mit den IP-Adressen der konfigurierten Server reagieren, reagiert eine für GSLB konfigurierte Citrix ADC Appliance mit den IP-Adressen der Dienste, wie sie durch die konfigurierte GSLB-Methode bestimmt werden. Standardmäßig ist der virtuelle GSLB-Server auf die geringste Verbindungsmethode festgelegt. Wenn alle GSLB-Dienste ausgefallen sind, antwortet die Appliance mit den IP-Adressen aller konfigurierten GSLB-Dienste.

GSLB-Methoden sind Algorithmen, die der virtuelle GSLB-Server verwendet, um den am besten leistungsfähigen GSLB-Dienst auszuwählen. Nachdem der Hostname in der Webadresse aufgelöst wurde, sendet der Client Datenverkehr direkt an die aufgelöste Dienst-IP-Adresse.

Die Citrix ADC Appliance stellt die folgenden GSLB-Methoden bereit:

- Runde Robin
- Geringste Verbindungen

- Kleinste Reaktionszeit
- Geringste Bandbreite
- Am wenigsten Pakete
- Quell-IP-Hash
- Benutzerdefinierte Last
- Roundtrip-Zeit (RTT)
- Statische Nähe

Damit GSLB-Methoden mit einem Remotestandort arbeiten können, muss entweder MEP aktiviert sein, oder explizite Monitore müssen an die Remotedienste gebunden sein. Wenn MEP deaktiviert ist, werden die Methoden RTT, Geringste Verbindungen, geringste Bandbreite, geringste Pakete und geringste Antwortzeit standardmäßig Round Robin verwendet.

Die Methoden Static Proximity und RTT Load Balancing sind spezifisch für GSLB.

Angeben einer anderen GSLB-Methode als statische Nähe oder dynamische RTT

Informationen zum Round-Robin, zu den kleinsten Verbindungen, der kleinsten Reaktionszeit, der geringsten Bandbreite, den kleinsten Paketen, dem Quell-IP-Hash oder zur benutzerdefinierten Load-Methode finden Sie unter Load Balancing.

So ändern Sie die GSLB-Methode mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set gslb vserver <name> -lbMethod GSLBMethod
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver Vserver-GSLB-1 -lbMethod ROUNDROBIN
<!--NeedCopy-->
```

So ändern Sie die GSLB-Methode mit der GUI

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**.
2. Wählen Sie im Detailbereich einen virtuellen GSLB-Server aus, und klicken Sie auf **Öffnen**.
3. Wählen Sie im Dialogfeld Virtueller GSLB Server konfigurieren auf der Registerkarte Methode und Persistenz unter Methode eine Methode aus der Liste Methode auswählen aus.

4. Klicken Sie auf **OK**, und stellen Sie sicher, dass die ausgewählte Methode unten unter Details angezeigt wird.

GSLB-Algorithmen

October 5, 2021

Der folgende Algorithmus wird für GSLB unterstützt.

- **Round Robin**: Wenn ein virtueller GSLB-Server für die Verwendung der Roundrobin-Methode konfiguriert ist, rotiert er kontinuierlich eine Liste der Dienste, die an ihn gebunden sind. Wenn der virtuelle Server eine Anforderung erhält, weist er die Verbindung dem ersten Dienst in der Liste zu und verschiebt diesen Dienst dann an den unteren Rand der Liste.
- **Geringste Antwortzeit**: Wenn der virtuelle GSLB-Server so konfiguriert ist, dass er die Methode der geringsten Antwortzeit verwendet, wählt er den Dienst mit dem niedrigsten Wert aus. Wo, niedrigster Wert = aktuelle aktive Verbindungen X durchschnittliche Antwortzeit.

  Sie können diese Methode nur für HTTP und Secure Sockets Layer (SSL) -Dienste konfigurieren. Die Antwortzeit (auch Time to First Byte oder TTFB genannt) ist das Zeitintervall zwischen dem Senden eines Anforderungspakets an einen Dienst und dem Empfangen des ersten Antwortpakets vom Dienst. Die NetScaler Appliance verwendet den Antwortcode 200, um TTFB zu berechnen.
- **Geringste Verbindungen**: Wenn ein virtueller GSLB-Server so konfiguriert ist, dass er den GSLB-Algorithmus (oder Methode) mit der geringsten Verbindung verwendet, wählt er den Dienst mit den wenigsten aktiven Verbindungen aus. Dies ist die Standardmethode, da sie in den meisten Fällen die beste Leistung bietet.
- **Geringste Bandbreite**: Ein virtueller GSLB-Server, der für die Verwendung der Methode der geringsten Bandbreite konfiguriert ist, wählt den Dienst aus, der derzeit den geringsten Datenverkehr bereitstellt, gemessen in Megabit pro Sekunde (Mbit/s).
- **Geringste Pakete**: Ein virtueller GSLB-Server, der für die Verwendung der Methode der wenigsten Pakete konfiguriert ist, wählt den Dienst aus, der die wenigsten Pakete in den letzten 14 Sekunden empfangen hat.
- **Quell-IP-Hash**: Ein virtueller GSLB-Server, der für die Verwendung der Quell-IP-Hash-Methode konfiguriert ist, verwendet den Hashwert der Client-IPv4- oder IPv6-Adresse, um einen Dienst auszuwählen. Um alle Anforderungen von Quell-IP-Adressen, die zu einem bestimmten Netzwerk gehören, an einen bestimmten Zielserver zu leiten, müssen Sie die Quell-IP-Adresse maskieren. Verwenden Sie für IPv4-Adressen den NetMask -Parameter. Verwenden Sie für IPv6-Adressen den Parameter v6NetMaskLength.

- **Benutzerdefinierter Lastenausgleich**: Der benutzerdefinierte Lastenausgleich wird für Serverparameter wie CPU-Auslastung, Arbeitsspeicher und Antwortzeit durchgeführt. Bei Verwendung der benutzerdefinierten Lademethode wählt die Citrix ADC Appliance normalerweise einen Dienst aus, der keine aktiven Transaktionen verarbeitet. Wenn alle Dienste im GSLB-Setup aktive Transaktionen verarbeiten, wählt die Appliance den Dienst mit der kleinsten Last aus. Ein spezieller Monitortyp, der als Lastmonitor bezeichnet wird, berechnet die Last für jeden Dienst im Netzwerk. Die Lastmonitore markieren nicht den Status eines Dienstes, aber sie nehmen Dienste aus der GSLB-Entscheidung heraus, wenn diese Dienste nicht UP sind.

Weitere Informationen finden Sie unter Load Balancing.

Statische Nähe

October 5, 2021

Die statische Näherungsmethode für GSLB verwendet eine auf IP-Adresse basierende statische Näherungsdatenbank, um die Nähe zwischen dem lokalen DNS-Server des Clients und den GSLB-Sites zu bestimmen. Die Citrix ADC Appliance antwortet mit der IP-Adresse eines Standorts, der den Näherungskriterien am besten entspricht.

Wenn zwei oder mehr GSLB-Sites an verschiedenen geografischen Sites denselben Inhalt bereitstellen, verwaltet die Citrix ADC Appliance eine Datenbank mit IP-Adressbereichen und verwendet die Datenbank für Entscheidungen über die GSLB-Sites, an die eingehende Clientanforderungen weitergeleitet werden sollen.

Damit die statische Näherungsmethode funktioniert, müssen Sie entweder die Citrix ADC Appliance so konfigurieren, dass eine vorhandene statische Näherungsdatenbank verwendet wird, die über eine Standortdatei aufgefüllt wird, oder benutzerdefinierte Einträge zur statischen Näherungsdatenbank hinzufügen. Nachdem Sie benutzerdefinierte Einträge hinzugefügt haben, können Sie deren Standortqualifizierer festlegen. Nachdem Sie die Datenbank konfiguriert haben, können Sie die statische Nähe als GSLB-Methode angeben.

Weitere Informationen zum Konfigurieren der statischen Nähe finden Sie unter Konfigurieren der statischen Nähe.

Dynamische Round-Trip-Zeitmethode

October 5, 2021

Dynamic Round Trip Time (RTT) ist ein Maß für die Zeit oder Verzögerung im Netzwerk zwischen dem lokalen DNS-Server des Clients und einer Datenressource. Zur Messung des dynamischen

RTT untersucht die Citrix ADC Appliance den lokalen DNS-Server des Clients und sammelt RTT-Metrikinformationen. Die Appliance verwendet diese Metrik dann, um ihre Lastausgleichsentscheidung zu treffen. Globaler Server Load Balancing überwacht den Echtzeitstatus des Netzwerks und leitet die Clientanforderung dynamisch an das Rechenzentrum mit dem niedrigsten RTT-Wert.

Wenn die DNS-Anforderung eines Clients für eine Domäne an die Citrix ADC Appliance gesendet wird, die als autorisierendes DNS für diese Domäne konfiguriert ist, verwendet die Appliance den RTT-Wert, um die IP-Adresse der am besten ausführenden Site auszuwählen, um sie als Antwort auf die DNS-Anforderung zu senden.

Die Citrix ADC Appliance verwendet verschiedene Mechanismen wie ICMP-Echoanforderung oder Antwort (PING), UDP und TCP, um die RTT-Metriken für Verbindungen zwischen dem lokalen DNS-Server und den teilnehmenden Sites zu sammeln. Die Appliance sendet zuerst einen Ping-Prüfpunkt, um den RTT zu ermitteln. Wenn der Ping-Prüfpunkt fehlschlägt, wird ein DNS-UDP-Prüfpunkt verwendet. Wenn dieser Prüfpunkt ebenfalls fehlschlägt, verwendet die Appliance einen DNS-TCP-Sonde.

Diese Mechanismen werden auf der Citrix ADC Appliance als Load Balancing Monitore dargestellt und können aufgrund der Verwendung des Präfixes ldns leicht identifiziert werden. Die drei Monitore sind in ihrer Standardreihenfolge:

- `ldns-ping`
- `ldns-dns`
- `ldns-tcp`

Diese Monitore sind in die Appliance integriert und auf sichere Standardeinstellungen eingestellt. Sie sind jedoch wie jeder andere Monitor auf der Appliance anpassbar.

Sie können die Standardreihenfolge ändern, indem Sie sie explizit als GSLB-Parameter festlegen. Geben Sie beispielsweise den folgenden Befehl ein, um die DNS-UDP-Abfrage, gefolgt von PING und dann TCP festzulegen:

```
1 set gslb parameter -ldnsprobeOrder DNS PING TCP
2 <!--NeedCopy-->
```

Sofern sie nicht angepasst wurden, führt die Citrix ADC Appliance UDP- und TCP-Sonden an Port 53 durch. Im Gegensatz zu normalen Load Balancing-Monitoren müssen die Sonden jedoch keine gültigen RTT-Informationen bereitstellen. ICMP-Port nicht verfügbare Meldungen, TCP-Resets und DNS-Fehlerantworten, die normalerweise einen Fehler darstellen würden, sind alle akzeptabel für die Berechnung des RTT-Werts.

Nach der Kompilierung der RTT-Daten verwendet die Appliance das proprietäre Metrikaustauschprotokoll (MEP), um RTT-Werte zwischen teilnehmenden Sites auszutauschen. Nach der Berechnung der RTT-Metriken sortiert die Appliance die RTT-Werte, um das Rechenzentrum mit der besten (kleinsten) RTT-Metrik zu identifizieren.

Wenn keine RTT-Informationen verfügbar sind (z. B. wenn der lokale DNS-Server eines Clients zum ersten Mal auf den Standort zugreift), wählt die Citrix ADC Appliance einen Standort mithilfe der Roundrobin-Methode aus und leitet den Client an den Standort weiter.

Um die dynamische Methode zu konfigurieren, konfigurieren Sie den virtuellen GSLB-Server der Site für dynamischen RTT. Sie können auch das Intervall, in dem lokale DNS-Server untersucht werden, auf einen anderen Wert als den Standardwert festlegen.

Konfigurieren eines virtuellen GSLB-Servers für dynamischen RTT

Um einen virtuellen GSLB-Server für dynamischen RTT zu konfigurieren, geben Sie die RTT-Load Balancing-Methode an.

Die Citrix ADC Appliance überprüft regelmäßig die Zeitinformationen für einen bestimmten lokalen Server. Wenn eine Änderung der Latenz den konfigurierten Toleranzfaktor überschreitet, aktualisiert die Appliance ihre Datenbank mit den neuen Zeitinformationen und sendet den neuen Wert durch einen MEP-Austausch an andere GSLB-Sites. Der Standardtoleranzfaktor ist 5 Millisekunden (ms).

Der RTT-Toleranzfaktor muss in der GSLB-Domäne gleich sein. Wenn Sie es für einen Standort ändern, müssen Sie identische RTT-Toleranzfaktoren auf allen Citrix ADC Appliances konfigurieren, die in der GSLB-Domäne bereitgestellt werden.

So konfigurieren Sie einen virtuellen GSLB-Server für dynamischen RTT mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set gslb vserver <name> -lbMethod RTT -tolerance <value>
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver Vserver-GSLB-1 -lbMethod RTT -tolerance 10
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen GSLB-Server für dynamischen RTT mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**, und doppelklicken Sie auf den virtuellen Server.

Festlegen des Probing-Intervalls lokaler DNS-Server

Die Citrix ADC Appliance verwendet verschiedene Mechanismen wie ICMP-Echoanforderung oder Antwort (PING), TCP und UDP, um RTT-Metriken für Verbindungen zwischen dem lokalen DNS-Server und teilnehmenden GSLB-Sites zu erhalten. Standardmäßig verwendet die Appliance einen Ping-Monitor und überprüft den lokalen DNS-Server alle 5 Sekunden. Die Appliance wartet dann 2 Sekunden auf die Antwort. Wenn in dieser Zeit keine Antwort empfangen wird, verwendet sie den TCP-DNS-Monitor für das Sondieren.

Sie können jedoch das Zeitintervall für die Untersuchung des lokalen DNS-Servers ändern, um Ihre Konfiguration anzupassen.

So ändern Sie das Sondierintervall mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb monitor <monitorName> <type> -interval <integer> <units> -
   resptimeout <integer> <units>
<!--NeedCopy-->
```

Beispiel:

```
set lb monitor ldns-tcp LDNS-TCP -interval 10 sec -resptimeout 5 sec
<!--NeedCopy-->
```

So ändern Sie das Probing-Intervall mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Monitore**, und doppelklicken Sie auf den Monitor, den Sie ändern möchten (z. B. Ping).

API-Methode

October 5, 2021

Sie können die API-Methode verwenden, um den GSLB-Dienst mit der besten Leistung zu ermitteln. Die API-Methode für GSLB verwendet eine REST-API, um den am besten ausführenden GSLB-Dienst zu ermitteln.

Wenn GSLB in der API-Methode eine DNS-Anforderung von einem Client empfängt, wertet sie die Anforderung anhand der angegebenen Regel aus. Wenn GSLB den HTTP-Callout-Ausdruck SYS.HTTP_CALLOUT (<name>) trifft, ruft es eine REST-API-Anforderung an einen HTTP-Callout-Agent auf. GSLB verwendet die Antwort des HTTP-Callout-Agenten, um den Dienst am besten zu bestimmen. In der DNS-Antwort gibt GSLB die IP-Adresse des leistungsstärksten Dienstes zurück an den Client zurück.

So konfigurieren Sie eine GSLB-API-Methode mit der CLI

Gehen Sie folgendermaßen vor, um die GSLB-API-Methode zu konfigurieren:

1. Konfigurieren Sie ein HTTP-Callout.

   Weitere Informationen finden Sie unter Konfigurieren eines HTTP-Callouts.

   Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add policy httpCallout <name> [-IPAddress <ip_addr|ipv6_addr>] [-
    port <port>] [-vServer <string>] [-returnType <returnType>] [-
    httpMethod (GET | POST)] [-hostExpr <string>] [-urlStemExpr <
    string>] [-headers <name(value)> ...] [-parameters <name(value)
    > ...] [-bodyExpr <string>] [-fullReqExpr <string>] [-scheme (
    http | https)] [-resultExpr <string>] [-cacheForSecs <secs>] [-
    comment <string>]
<!--NeedCopy-->
```

   Beispiel:

```
add policy httpCallout GSLB_Method_API -IPAddress 208.111.39.237 -
    port 443 -returnType TEXT -hostExpr  "\" hopx.gslb.com\ ""  -
    urlStemExpr  "\" /zones/1/customers/92395/apps/6/decision\ ""
    -headers Authorization( "Basic 19fbe6db-4332-4e3f-a8bc-
    ee47bdc726f8") -parameters ip(DNS.REQ.OPT.ECS.IP.
    TYPECAST_TEXT_T ALT CLIENT.IP.SRC.TYPECAST_TEXT_T) -scheme
    https -resultExpr  "HTTP.RES.BODY(HTTP.RES.CONTENT_LENGTH).
    XPATH_JSON(xp%/providers/Val[1]/provider%)"  -cacheForSecs 30
<!--NeedCopy-->
```

2. Geben Sie die API-Methode für den Lastenausgleich an. GSLB wertet die DNS-Anforderung anhand der angegebenen Regel aus.

   Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add gslb vserver <name> <serviceType>  [-lbMethod <lbMethod>] [-
    backupLBMethod <backupLBMethod>] -rule <expression>
<!--NeedCopy-->
```

Beispiel:

```
add gslb vserver vs1 HTTP -lbMethod API -backupLBMethod ROUNDROBIN
    -rule  “sys.http_callout(GSLB_Method_API)”
<!--NeedCopy-->
```

Beispielkonfiguration für die Integration von GSLB und ITM mit API als LB-Methode

Diese Konfiguration ermöglicht es GSLB, die Internetsichtbarkeitsaspekte des Citrix Intelligent Traffic Management (ITM) zu verwenden, um den leistungsstärksten GSLB-Dienst zu ermitteln.

```
/* Enable ns features */

enable ns feature lb gslb cs

/* This is a named expression that is used in the HTTP callout, used
    for result expression. */

add policy expression exp1 ”HTTP.RES.BODY(HTTP.RES.CONTENT_LENGTH).
    XPATH_JSON(xp%/providers/Val[1]/provider%)”

/* This is a named expression that is used in HTTP callout, used for
    host expression. */

add policy expression exp2 ””hopx.cedexis.com””

/* This is the HTTP callout configured to request the ITM for the GSLB
    decision. */

add policy httpCallout ITM_OpenMix_API -IPAddress 208.111.39.237 -port
    80 -returnType TEXT -hostExpr exp2 -urlStemExpr ””/zones/1/customers
    /61770/apps/3/decision”” -headers Authorization(”Basic a310697a-1d69
    -48bf-8f36-55742a8e894e”) -parameters ip(DNS.REQ.OPT.ECS.IP.
    TYPECAST_TEXT_T ALT CLIENT.IP.SRC.TYPECAST_TEXT_T) -scheme http -
    resultExpr exp1 -cacheForSecs 30
```



```
16
17 /* Add service 1 */
18 add service sg1 98.136.103.24 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
       -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -
      svrTimeout 360 -CKA NO -TCPB NO -CMP NO
19
20 /* Add service 2 */
21 add service sg2 172.217.194.113 HTTP 80 -gslb NONE -maxClient 0 -maxReq
       0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180
      -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
22
23 /* Add ADNS service */
24
25 add service adns1 10.102.217.106 ADNS 53 -gslb NONE -maxClient 0 -
      maxReq 0 -cip DISABLED -usip NO -useproxyport NO -sp OFF -cltTimeout
       120 -svrTimeout 120 -CKA NO -TCPB NO -CMP NO
26
27 /* Add lb vserver 1 for service 1 */
28 add lb vserver lbvs1 HTTP 10.102.217.116 80 -persistenceType NONE -
      cltTimeout 180
29
30 /* Add lb vserver 2 for service 2 */
31 add lb vserver lbvs2 HTTP 10.102.217.117 80 -persistenceType NONE -
      cltTimeout 180
32
33 /* Bind service 1 to lb vserver 1 */
34
35 bind lb vserver lbvs1 sg1
36
37 /* Bind service 2 to lb vserver 2 */
38
39 bind lb vserver lbvs2 sg2
40
41 /* Configure API GSLB method on GSLB virtual server to call the HTTP
      callout. This HTTP callout requests the ITM for the GSLB decision
      and returns GSLB service name, which should serve the request. */
42
43 add gslb vserver vs1 HTTP -lbMethod API -backupLBMethod ROUNDROBIN -
      rule "sys.http_callout(ITM_OpenMix_API)" -tolerance 0
44
45 /* Add GSLB site */
46
47 add gslb site site1 10.102.217.106 -publicIP 10.102.217.106
48
49 /* Add GSLB service 1 */
```



```
50
51 add gslb service aws_ec2_ap_south_1_asia_pacific_mumbai_1
       10.102.217.116 HTTP 80 -publicIP 10.102.217.116 -publicPort 80 -
       maxClient 0 -siteName site1 -sitePersistence HTTPRedirect -
       sitePrefix gs2. -cltTimeout 180 -svrTimeout 360 -downStateFlush
       ENABLED
52
53 /* Add GSLB service 2 */
54
55 add gslb service aws_ec2_ap_south_1_asia_pacific_mumbai 10.102.217.117
       HTTP 80 -publicIP 10.102.217.117 -publicPort 80 -maxClient 0 -
       siteName site1 -sitePersistence HTTPRedirect -sitePrefix gs1. -
       cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
56
57 /* Bind the GSLB service 1 to GSLB server 1 */
58 bind gslb vserver vs1 -serviceName
       aws_ec2_ap_south_1_asia_pacific_mumbai_1
59
60 /* Bind the GSLB service 2 to GSLB server 2 */
61 bind gslb vserver vs1 -serviceName
       aws_ec2_ap_south_1_asia_pacific_mumbai
62
63 /* Bind a domain name to the GSLB virtual server */
64 bind gslb vserver vs1 -domainName testruchit104.com -TTL 5
65
66 <!--NeedCopy-->
```

Statische Nähe konfigurieren

October 5, 2021

Damit die statische Näherungsmethode funktioniert, müssen Sie entweder die Citrix ADC Appliance so konfigurieren, dass eine vorhandene statische Näherungsdatenbank verwendet wird, die über eine Standortdatei aufgefüllt wird, oder benutzerdefinierte Einträge zur statischen Näherungsdatenbank hinzufügen. Nachdem Sie benutzerdefinierte Einträge hinzugefügt haben, können Sie deren Standortqualifizierer festlegen. Nachdem Sie die Datenbank konfiguriert haben, können Sie die statische Nähe als GSLB-Methode angeben.

Dieses Dokument enthält die folgenden Informationen:

- Hinzufügen einer Standortdatei zum Erstellen einer statischen Näherungsdatenbank
- Hinzufügen von benutzerdefinierten Einträgen zu einer statischen Näherungsdatenbank

- Festlegen der Standortbezeichner
- Angeben der Proximity-Methode
- Statische GSLB-Näherungsdatenbank synchronisieren

Hinzufügen einer Standortdatei zum Erstellen einer statischen Proximitydatenbank

April 7, 2022

Eine statische Näherungsdatenbank ist eine UNIX-basierte ASCII-Datei. Einträge, die aus einer Standortdatei zu dieser Datenbank hinzugefügt wurden, werden als statische Einträge bezeichnet. Es kann nur eine Standortdatei auf eine Citrix ADC-Appliance geladen werden. Durch das Hinzufügen einer neuen Standortdatei wird die vorhandene Datei überschrieben. Die Anzahl der Einträge in der statischen Näherungsdatenbank wird durch den konfigurierten Speicher in der Citrix ADC-Appliance begrenzt.

Die statische Näherungsdatenbank kann im Standardformat oder in einem Format erstellt werden, das aus kommerziell konfigurierten Datenbanken Dritter (wie www.maxmind.com und www.ip2location.com) abgeleitet ist.

Die Citrix ADC-Appliance enthält die folgenden zwei IP-Geolocation-Datenbankdateien. Dies sind GeoLite2-Dateien, die von MaxMind veröffentlicht wurden.

- Citrix_NetScaler_Inbuilt_Geoip_db_IPv4
- Citrix_NetScaler_Inbuilt_Geoip_db_IPv6

Diese Datenbankdateien sind in einem von der Citrix ADC-Appliance unterstützten Format im Verzeichnis /var/netscaler/inbuilt_db verfügbar.

Sie können diese IP-Geolokalisierungsdatenbanken als Standortdatei für die statische Näherungsbasierte GSLB-Methode oder in standortbasierten Richtlinien verwenden.

Diese Datenbanken unterscheiden sich in den Details, die sie bereitstellen. Es gibt keine strikte Durchsetzung des Datenbankdateiformats, außer dass die Standarddatei über Format-Tags verfügt. Bei den Datenbankdateien handelt es sich um ASCII-Dateien, die ein Komma als Feldtrennzeichen verwenden. Es gibt Unterschiede in der Struktur der Felder und der Darstellung von IP-Adressen in den Sites.

Der Formatparameter beschreibt die Struktur der Datei für die Citrix ADC-Appliance. Wenn Sie einen falschen Wert für die Formatoption angeben, können die internen Daten beschädigt werden.

> **Hinweis**
>
> - Wenn das Verzeichnis /var/netscaler/inbuilt_db/ nach einem Upgrade die Datenbankdatei

(Citrix_Netscaler_InBuilt_GeoIP_DB.csv) aus den früheren Citrix ADC-Softwareversionen enthält, wird die Datei beibehalten.
- Der Standardspeicherort der Datenbankdatei ist /var/netscaler/locdb, und bei einem Hochverfügbarkeitssetup (HA) muss eine identische Kopie der Datei auf beiden Citrix ADC-Appliances am selben Speicherort vorhanden sein.
- Wenn die Standortdatei an einem anderen Ort als dem Standardspeicherort gespeichert ist, geben Sie den Pfad der Standortdatei an.
- Für Admin-Partitionen lautet der Standardpfad: /var/partitions/<partitionName> /netscaler/locdb.
- Einige Datenbanken enthalten kurze Ländernamen gemäß ISO-3166 und lange Ländernamen. Der Citrix ADC verwendet Kurznamen beim Speichern und Abgleichen von Qualifizierern.
- Um eine statische Näherungsdatenbank zu erstellen, melden Sie sich bei der UNIX-Shell der Citrix ADC-Appliance an und erstellen Sie mit einem Editor eine Datei mit den Standortdetails in einem der von Citrix ADC unterstützten Formate.
- Die Citrix ADC-Appliance wird mit der GeoLite2-Datenbank (IPv4 und IPv6) geliefert, aber Citrix verwaltet oder aktualisiert die MaxMind GeoLite2-Datenbank nicht regelmäßig. Bei Bedarf können Sie die GeoLite2-Datenbank von www.maxmind.com abrufen und in das Citrix ADC-Datenbankformat konvertieren. Weitere Informationen finden Sie unter Skript zum Konvertieren des MaxMind GeoLite2-Datenbankformats in das Citrix ADC-Datenbankformat.

So fügen Sie eine statische Standortdatei mit der CLI hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add locationFile <locationFile> [-format <format>]
-  show locationFile
<!--NeedCopy-->
```

Beispiel:

```
add locationFile /var/netscaler/locdb/nsgeo1.0 -format netscaler
Done

show locationFile
Location File: /var/netscaler/locdb/nsgeo1.0
Format: netscaler
 Done
```



```
8 >
9 <!--NeedCopy-->
```

Beispiel:

```
1 add locationFile /var/netscaler/inbuilt_db/
     Citrix_Netscaler_InBuilt_GeoIP_DB_IPv4 -format netscaler
2
3 add locationFile6 /var/netscaler/inbuilt_db/
     Citrix_Netscaler_InBuilt_GeoIP_DB_IPv6 -format netscaler
4 <!--NeedCopy-->
```

So fügen Sie eine statische Standortdatei mit der GUI hinzu:

1. Navigieren Sie zu **AppExpert** > **Standort**, und klicken Sie auf die Registerkarte **Statische Datenbank** .
2. Klicken Sie auf **Hinzufügen**, um eine statische Standortdatei hinzuzufügen.

Sie können eine importierte Standortdateidatenbank anzeigen, indem **Sie das Dialogfeld Datenbank anzeigen** im Konfigurationsdienstprogramm verwenden. Es gibt kein CLI-Äquivalent.

So zeigen Sie eine statische Standortdatei mit der GUI an:

1. Navigieren Sie zu **AppExpert** > **Standort**, und klicken Sie auf die Registerkarte **Statische Datenbank** .
2. Wählen Sie eine Datei mit statischem Speicherort aus, und klicken Sie in der Liste **Aktion** auf **Datenbank anzeigen**.

So konvertieren Sie eine Standortdatei in das Citrix ADC-Format:

Wenn Sie eine Standortdatei hinzufügen, wird sie standardmäßig im Citrix ADC-Format gespeichert. Sie können eine Standortdatei anderer Formate in das Citrix ADC-Format konvertieren.

> **Hinweis**: Auf die Option `nsmap` kann nur über die Befehlszeilenschnittstelle zugegriffen werden. Die Konvertierung ist nur in das Citrix ADC-Format möglich.

Um das statische Datenbankformat zu konvertieren, geben Sie an der CLI-Eingabeaufforderung den folgenden Befehl ein:

```
1 nsmap -f <inputFileFormat> -o <outputFileName> <inputFileName>
2 <!--NeedCopy-->
```

Beispiel:


```
1  nsmap -f ip-country-region-city -o nsfile.ns ip-country-region-city.
       csv
2 <!--NeedCopy-->
```

Skript zum Konvertieren des MaxMind GeoLite2-Datenbankformats in das Citrix ADC-Datenbankformat

MaxMind GeoIP-Datenbank kann nicht direkt in Citrix ADC verwendet werden. Die MaxMind GeoIP-Datenbank muss in das Citrix ADC-Format konvertiert und dann für die IP-Siteerkennung in der statischen GSLB-Näherungsmethode und anderen Funktionen wie Richtlinien geladen werden.
Sie können ein Skript verwenden, um das GeoLite2-Datenbankformat in das Citrix ADC-Datenbankformat zu konvertieren. Dieses Skript kann verwendet werden, um sowohl IPv4- als auch IPv6-Dateien zu konvertieren.
Das Skript ist an folgendem Ort verfügbar: https://github.com/citrix/MaxMind-GeoIP-Database-Conversion-Citrix-ADC-Format

Schritte zum Konvertieren der GeoIP2-Datenbank in das Citrix ADC-Format

1. Laden Sie die GeoLite2 City- oder GeoLite2-Länderdatenbank im.csv-Format von herunter https://dev.maxmind.com/geoip/geoip2/geolite2/.
2. Kopieren Sie die Datei in ein Citrix ADC-Verzeichnis (z. B. /var). Entpacken Sie die Datei mit dem folgenden Shell-Befehl, der ein Verzeichnis mit demselben Namen erstellen würde.

   ```
   tar -xf <filename>
   ```

3. Laden Sie das Skript Convert_GeoIPDB_to_NetScaler_Format.pl von https://github.com/citrix/MaxMind-GeoIP-Database-Conversion-Citrix-ADC-Format herunter und kopieren Sie es in das in Schritt #2 erstellte Verzeichnis.
4. Führen Sie den folgenden Befehl aus, um die zulässigen Optionen für die Skriptausführung zu überprüfen:

   ```
   perl Convert_GeoIPDB_To_Netscaler_Format.pl -help
   ```

   Verschiedene Optionen sind verfügbar:

   - <filename> IPv4-Ausgabedatei. Standardname der Ausgabedatei: Netscaler_Maxmind_GeoIP_DB_IP
   - -p <filename> IPv6-Ausgabedatei. Standardname der Ausgabedatei: Netscaler_Maxmind_GeoIP_DI
   - -logfile <filename> Datei mit einer Liste von Ereignissen/Nachrichten
   - -debug Druckt alle Nachrichten auf STDOUT

5. Führen Sie den folgenden Befehl aus, um das GeoLite2-Datenbankformat in das Citrix ADC-Datenbankformat zu konvertieren.

   ```
   perl Convert_GeoIPDB_To_Netscaler_Format.pl
   ```

   > **Hinweis:** Der Vorgang kann bis zu 5 Minuten dauern.

   Die im Skript verwendeten Standarddateinamen sind die der MaxMind GeoLite2 City-basierten Datenbank. Wenn Sie die GeoLite2-Länderdatenbank heruntergeladen haben, müssen Sie die Eingabedateinamen entsprechend der Liste angeben.

   - `-b <filename>` Name der zu konvertierenden IPv4-Blockdatei. Standarddateiname: GeoLite2-City-Blocks-IPv4.csv
   - `-i <filename>` Name der zu konvertierenden IPv6-Blockdatei. Standarddateiname: GeoLite2-City-Blocks-IPv6.csv
   - `-l <filename>` Name der zu konvertierenden Standortdatei. Standarddateiname: GeoLite2-City-Locations-en.csv

   Beispiel:

   ```
   perl Convert_GeoIPDB_To_Netscaler_Format.pl -b GeoLite2-Country-Blocks-IPv4.csv -i GeoLite2-Country-Blocks-IPv6.csv -l GeoLite2-Country-Locations-en.csv
   <!--NeedCopy-->
   ```

   Im Folgenden sind die Ausgabedateien aufgeführt, die nach der Ausführung des Skripts generiert wurden

   - Netscaler_Maxmind_GeoIP_DB_IPv4.csv
   - Netscaler_Maxmind_GeoIP_DB_IPv6.csv

6. Sobald die Konvertierung der Datenbank in das Citrix ADC-Format abgeschlossen ist, verwenden Sie den folgenden Befehl, um sie zu verwenden.

   ```
   add locationFile <locationFile>
   ```

Fügen Sie eine statische Datenbankdatei eines Drittanbieters auf einer Citrix ADC-Appliance hinzu

Führen Sie die folgenden Schritte aus, um eine statische Datenbankdatei eines Drittanbieters auf einer Citrix ADC-Appliance hinzuzufügen.

1. Beziehen Sie die Standortdatenbankdatei von einem Drittanbieter wie www.maxmind.com oder www.ip2location.com.

2. Kopieren Sie die Standortdatenbankdatei mit dem WinSCP-Dienstprogramm auf die Citrix ADC-Appliance.

   > **Hinweis**
   >
   > Der Standardspeicherort der Datenbankdatei auf der Appliance ist **/var/netscaler/locdb**.

3. Führen Sie den folgenden Befehl aus, um eine statische Standortdatei hinzuzufügen:

```
add location file <locationfile Name> -format LocationFormat
<!--NeedCopy-->
```

4. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die Standortdatenbank geladen ist:

```
show location parameter
<!--NeedCopy-->
```

   Dieser Befehl zeigt die Parameter an, z. B. die Anzahl der statischen Einträge. Wenn die Datenbank nicht richtig geladen wurde, zeigt dieser Befehl auch eine Fehlermeldung an. Es können maximal 3M-1-Einträge (3 Millionen minus eins) geladen werden.

5. Führen Sie den folgenden Befehl aus, um den Standort der GSLB-Site anzuzeigen:

```
show gslb service
<!--NeedCopy-->
```

   > **Hinweis**
   >
   > - Wenn die Datenbank korrekt geladen wurde, wird der Standort der GSLB-Sites automatisch in die Datenbank eingetragen.
   > - Sie können in der Konfiguration auf der Appliance nur eine Standortdatei angeben.
   > - Wenn sich die Appliances in einem Hochverfügbarkeitssetup befinden, muss eine Appliance die Datenbank von der anderen Appliance kopieren.
   > - Wenn keine Übereinstimmung für eine eingehende IP-Adresse gefunden wird, wird die Anforderung mit der Round-Robin-Methode verarbeitet.

6. Führen Sie den folgenden Befehl aus, um die GSLB-Methode auf der Appliance zu konfigurieren:

```
set gslb vserver GSLBVserverName -lbMethod MethodType
<!--NeedCopy-->
```


Hinzufügen benutzerdefinierter Einträge zu einer statischen Näherungsdatenbank

October 5, 2021

Benutzerdefinierte Einträge haben Vorrang vor statischen Einträgen in der Näherungsdatenbank. Sie können maximal 500 benutzerdefinierte Einträge hinzufügen. Bezeichnen Sie für einen benutzerdefinierten Eintrag alle ausgesprochenen Kriterien mit einem Sternchen (*), und setzen Sie den Parameter, wenn Kriterien einen Punkt oder ein Leerzeichen im Namen haben, in doppelte Anführungszeichen ein. Die ersten 31 Zeichen werden für jedes Qualifizierer ausgewertet. Sie können auch den Längen- und Breitengrad des geografischen Standorts des IP-Adressbereichs angeben, um einen Dienst mit der statischen Näherungsmethode GSLB auszuwählen.

So fügen Sie benutzerdefinierte Einträge mit der Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um der statischen Näherungsdatenbank einen benutzerdefinierten Eintrag hinzuzufügen und die Konfiguration zu überprüfen:

```
1 add location < IPfrom> < IPto> <preferredLocation> [-longitude <integer
     >[-latitude <integer>]]
2 show location
3 <!--NeedCopy-->
```

Beispiel:

```
1 >add location 192.168.100.1 192.168.100.100 *.us.ca.mycity
2 <!--NeedCopy-->
```

```
1 >show location
2 <!--NeedCopy-->
```

Parameter zum Hinzufügen von benutzerdefinierten Einträgen

- IPfrom

  Erste IP-Adresse im Bereich, in punktierter Dezimalnotation. Dies ist ein obligatorisches Argument.

- IPto

  Letzte IP-Adresse im Bereich, in punktierter Dezimalnotation. Dies ist ein obligatorisches Argument.

- preferredLocation

  Zeichenfolge von Qualifizierern in punktierter Notation, die die geografische Position des IP-Adressbereichs beschreibt. Jeder Qualifier ist spezifischer als derjenige, der ihm vorausgeht, wie in continent.country.region.city.isp.organization. Beispiel: “NA.US.CA.San Jose.ATT.citrix”.

  Hinweis: Ein Kriterium, das einen Punkt (.) oder ein Leerzeichen () enthält, muss in doppelte Anführungszeichen eingeschlossen werden.

  Dies ist ein obligatorisches Argument. Maximale Länge: 197

- longitude

  Numerischer Wert in Grad, der den Längengrad der geografischen Position des IP-Adressbereichs angibt.

  Hinweis: Längen- und Breitengradparameter werden verwendet, um einen Dienst mit der statischen Näherungsmethode GSLB auszuwählen. Wenn sie nicht angegeben sind, basiert die Auswahl auf den für den Standort angegebenen Kriterien.

  Maximalwert: 180

- latitude

  Numerischer Wert in Grad, der den Breitengrad der geografischen Position des IP-Adressbereichs angibt.

  Hinweis: Längen- und Breitengradparameter werden verwendet, um einen Dienst mit der statischen Näherungsmethode GSLB auszuwählen. Wenn sie nicht angegeben sind, basiert die Auswahl auf den für den Standort angegebenen Kriterien.

  Maximalwert: 180

So fügen Sie benutzerdefinierte Einträge mit dem Konfigurationsdienstprogramm hinzu

Navigieren Sie zu **AppExpert** > **Speicherort**, klicken Sie auf die Registerkarte **Benutzerdefinierte Einträge**, und fügen Sie die benutzerdefinierten Einträge hinzu.

Festlegen von Standortkennzeichnungen

April 25, 2022

Die zur Implementierung der statischen Nähe verwendete Datenbank enthält den Standort der GSLB-Standorte. Jeder Standort hat einen IP-Adressbereich und bis zu sechs Qualifizierer für diesen Bereich. Die Qualifikationszeichen sind wörtliche Zeichenfolgen und werden zur Laufzeit in einer vorgeschriebenen Reihenfolge verglichen. Jeder Standort muss mindestens einen Qualifier haben. Die Qualifier-Labels definieren die Bedeutung der Qualifier (Kontext), die benutzerdefiniert sind. Citrix ADC hat zwei eingebaute Kontexte:

Geografischer Kontext, der die folgenden Qualifier-Labels hat:

- Qualifier 1 — “Kontinent”
- Qualifikationsspiel 2 — “Land”
- Qualifier 3 — “Staat”
- Qualifikationsspiel 4 — “Stadt”
- Qualifikationsspiel 5 — “ISP”
- Qualifier 6 — “Organisation”

Benutzerdefinierte Einträge, die die folgenden Qualifier-Labels haben:

- Qualifikationsspiel 1 — “Qualifikationsspiel 1”
- Qualifikationsspiel 2 — “Qualifikationsspiel 2”
- Qualifikationsspiel 3 — “Qualifikationsspiel 3”
- Qualifikationsspiel 4 — “Qualifikationsspiel 4”
- Qualifikationsspiel 5 — “Qualifikationsspiel 5”
- Qualifikationsspiel 6 — “Qualifikationsspiel 6”

Wenn der geografische Kontext ohne Kontinentkennzeichen festgelegt ist, wird Kontinent vom Land abgeleitet. Sogar die eingebauten Qualifier-Labels basieren auf dem Kontext, und die Beschriftungen können geändert werden. Diese Qualifier-Labels geben die Standorte an, die den IP-Adressen zugeordnet sind, die für statische Näherungsentscheidungen verwendet werden.

Um eine statische Proximity-basierte Entscheidung zu treffen, vergleicht die Citrix ADC-Appliance die von der IP-Adresse des lokalen DNS-Server-Resolvers abgeleiteten Standortattribute (Qualifikatoren) mit den Standortattributen der teilnehmenden Sites. Wenn nur eine Site übereinstimmt, gibt die Appliance die IP-Adresse dieser Site zurück. Wenn es mehrere Übereinstimmungen gibt, ist die ausgewählte Site das Ergebnis eines Round Robin auf den übereinstimmenden GSLB-Sites. Wenn es keine Übereinstimmung gibt, ist die ausgewählte Site das Ergebnis eines Round Robin auf allen konfigurierten Standorten. Eine Seite, die keine Qualifikationsspiele hat, wird als Spiel betrachtet.

Mit den GEO-Regeln für den standortbasierten Richtlinienausdruck können Sie Platzhalterübereinstimmungen überprüfen. Diese Funktion prüft, ob Platzhalterqualifizierer mit anderen Qualifikationszeichen übereinstimmen, einschließlich Nicht-Platzhalter oder nicht. Die Platzhalterübereinstimmung erfolgt mithilfe des Attributs `matchWildcardtoany`, das dem Befehl `set locationParameter` hinzugefügt wurde.

Das Attribut `matchWildcardtoany` kann auf die folgenden Werte festgelegt werden:

- **Ja:** Wildcard-Qualifikationsspiele stimmen mit allen anderen Qualifikationsspielen überein.
- **Nein:** Platzhalter-Qualifikationsspiele stimmen nicht mit Nicht-Wildcard-Qualifikationsspielen überein, sondern stimmen mit anderen Platzhalter-Qualifikationsspielen überein. Die Standardoption ist " **Nein**".
- **Ausdruck:** Platzhalterqualifizierer in einem Ausdruck stimmen mit jedem Qualifikator an einer LDNS-Position überein, aber Platzhalterqualifizierer am LDNS-Speicherort stimmen nicht mit Nicht-Platzhalter-Qualifizierern in einem Ausdruck überein.

Beispiel:

```
1 add dns policy policy1 "CLIENT.IP.SRC.MATCHES_LOCATION("Continent.
     country \*.\*.\*.\* \ ")"  <action>
2 <!--NeedCopy-->
```

So stellen Sie die Standortparameter über die CLI ein

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set locationparameter -context <context> -q1label <string> [-q2label <
     string>] [-q3label <string>] [-q4label <string>] [-q5label <string>]
      [-q6label <string>] -matchWildcardtoany [Yes | No | Expression]
2 <!--NeedCopy-->
```

Beispiel:

```
1 set locationparameter -context custom -q1label asia -matchWildcardtoany
      Yes
2 <!--NeedCopy-->
```

So stellen Sie die Standortparameter über die GUI ein

1. Navigieren Sie zu **Traffic Management > GSLB > Datenbank und Einträge**.
2. Klicken Sie unter **Einstellungen**auf **Standortparameter ändern**.
3. Legen Sie auf der Seite **Standortparameter konfigurieren** die Standortparameter fest.

Konfigurationsbeispiel (mit CLI)

Erwägen Sie die folgende Netzwerkkonfiguration:

- Name des virtuellen GSLB-Servers: gv1
- IP-Adresse des virtuellen GSLB-Servers: 1.1.1.2
- GSLB-Dienst: gsvc1 an gv1 gebunden
- Speicherort DB-Dateiname: sample.csv
- Geolokalisierungsqualifizierer: Die Qualifizierer 1 und 2 sind konfiguriert. Rest ist so eingestellt, dass es mit dem Platzhalter übereinstimmt.
  - Qualifikationsspiel 1 — Asien
  - Qualifikationsspiel 2 — IR
  - Qualifikationsspiel 3-*
  - Qualifikationsspiel 4-*
  - Qualifikationsspiel 5-*
  - Qualifikationsspiel 6-*
- DNS-Richtlinie — Die Richtlinie pol1 ist so eingestellt, dass die Pakete verworfen werden, wenn es eine Übereinstimmung gibt.

Stellen Sie den Standortparameter ein und konfigurieren Sie die DNS-Richtlinie wie folgt:

```
set locationParameter -q2label Country_Code -q3label Subdivision_1_Name
    -q4label Subdivision_2_Name -q5label City

add locationFile "/var/netscaler/inbuilt_db/sample.csv"

add gslb vserver gv1 HTTP -backupLBMethod ROUNDROBIN -tolerance 0

add dns policy pol1 "CLIENT.IP.SRC.MATCHES_LOCATION("Asia.IR
   .\*.\*.\*.\*")||CLIENT.IP.SRC.MATCHES_LOCATION("Asia.SY.\*.\*.\*.\*"
   )||CLIENT.IP.SRC.MATCHES_LOCATION("Asia.SD.\*.\*.\*.\*")||CLIENT.IP.
   SRC.MATCHES_LOCATION("Asia.KP.\*.\*.\*.\*")||CLIENT.IP.SRC.
   MATCHES_LOCATION("North America.CU.\*.\*.\*.\*")||CLIENT.IP.SRC.
   MATCHES_LOCATION("Europe.UA.Crimea.\*.\*.\*.\*")"
   dns_default_act_Drop

bind dns global pol1 1 -gotoPriorityExpression 65535 -type REQ_DEFAULT

add gslb service gsvc1 1.1.1.2 HTTP 80 -publicIP 1.1.1.2 -publicPort 80
    -maxClient 0 -healthMonitor NO -siteName s1 -cltTimeout 180 -
   svrTimeout 360 -downStateFlush ENABLED

bind gslb vserver gv1 -serviceName gsvc1

bind gslb vserver gv1 -domainName www.gslbnew.com -TTL 5
<!--NeedCopy-->
```


Fügen Sie der Location-DB-Datei die folgenden Clienteinträge hinzu. In diesem Beispiel lautet der DB-Dateiname des Speicherorts sample.csv:

```
10.106.24.170,10.106.24.190,,,,,,,8.0000,47.0000

10.102.82.170,10.102.82.190,Asia,,,,,,-73.9924,40.7553

10.106.24.140,10.106.24.150,,IR,,,,,51.4231,35.6961
<!--NeedCopy-->
```

Gemäß der vorherigen Konfiguration haben die Clients zwischen 10.106.24.170 und 10.106.24.190 keine Platzhalterqualifizierer definiert. Die Clients zwischen 10.106.24.140 und 10.106.24.150 haben den Qualifizierer 2 als IR.

Setzen Sie den Match-Platzhalter-Qualifizierer auf NEIN:

```
set locationparameter -matchWildcardtoany no
<!--NeedCopy-->
```

Wenn der Übereinstimmungs-Platzhalter-Qualifizierer auf NEIN festgelegt ist, stimmen die Platzhalter-Qualifizierer nur mit den definierten Platzhalter-Qualifizierern überein. Es stimmt nicht mit anderen Nicht-Wildcard-Qualifizierern überein.

- Die DNS-Abfragen, die 10.106.24.147 kommen, entsprechen dem definierten Platzhalter-Qualifizierer (Qualifizierer 2 = IR). Daher tritt die DNS-Richtlinie in Kraft und löscht die Abfragen.

  Wenn Sie den Befehl `dig @10.102.82.13 www.gslbnew.com` auf dem Client 10.106.24.147 ausführen, zeigt die Ausgabe, dass die Server nicht erreichbar waren.

  ```
  root@ns#  dig @10.102.82.13 www.gslbnew.com

  ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
  ; (1 server found)
  ;; global options: +cmd
  ;; connection timed out; no servers could be reached
  <!--NeedCopy-->
  ```

- Die DNS-Abfragen von 10.106.24.180 stimmen nicht mit den definierten Qualifizierern überein. Die DNS-Richtlinie tritt nicht in Kraft und die Abfragen werden verarbeitet.

  Führen Sie den Befehl `dig @10.102.82.13 www.gslbnew.com` auf dem 10.106.24.180-Client aus. Die Ausgabe zeigt die IP-Adresse des virtuellen GSLB-Servers.


```
root@ns# dig @10.102.82.13 www.gslbnew.com

; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64265
;; flags: qr aa rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
   ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;www.gslbnew.com. IN    A

;; ANSWER SECTION:
www.gslbnew.com.    5   IN  A   1.1.1.2

;; Query time: 12 msec
;; SERVER: 10.102.82.13#53(10.102.82.13)
;; WHEN: Tue Mar 29 22:46:40 UTC 2022
;; MSG SIZE  rcvd: 60
<!--NeedCopy-->
```

Setzen Sie den Match-Platzhalter-Qualifizierer auf Ja:

```
set locationparameter -matchWildcardtoany yes
<!--NeedCopy-->
```

Wenn der Match-Platzhalter-Qualifizierer auf Ja festgelegt ist, stimmen die Platzhalter-Qualifizierer mit allen Platzhaltern überein (definierter und Nicht-Platzhalter-Qualifizierer).

- Die DNS-Abfragen, die 10.106.24.147 kommen, entsprechen dem definierten Qualifizierer (Qualifizierer 2 = IR). Daher tritt die DNS-Richtlinie in Kraft und löscht die Abfragen.

  Führen Sie den Befehl `dig @10.102.82.13 www.gslbnew.com` auf dem Client 10.106.24.147 aus. Die Ausgabe zeigt, dass Server nicht erreichbar waren.

```
root@ns#  dig @10.102.82.13 www.gslbnew.com

```



```
3   ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
4   ; (1 server found)
5   ;; global options: +cmd
6   ;; connection timed out; no servers could be reached
7   <!--NeedCopy-->
```

- Die Abfragen von 10.106.24.180 stimmen mit den Nicht-Wildcard-Qualifizierern überein. Daher tritt die DNS-Richtlinie in Kraft und löscht die Abfragen.

  Führen Sie den Befehl `dig @10.102.82.13 www.gslbnew.com` auf dem 10.106.24.180-Client aus. Die Ausgabe zeigt, dass Server nicht erreichbar waren.

```
1   root@ns# dig @10.102.82.13 www.gslbnew.com
2
3   ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
4   ; (1 server found)
5   ;; global options: +cmd
6   ;; connection timed out; no servers could be reached
7   <!--NeedCopy-->
```

Stellen Sie den Match-Platzhalter-Qualifizierer auf Ausdruck:

```
1 set locationparameter -matchWildcardtoany expression
2 <!--NeedCopy-->
```

Wenn der Übereinstimmungs-Platzhalter-Qualifizierer auf Ausdruck festgelegt ist, stimmen die Platzhalter-Qualifizierer entweder mit dem in der DNS-Richtlinie verfügbaren Qualifizierer oder mit den in der Speicherort-DB-Datei verfügbaren Qualifizierern überein.

- Die DNS-Abfragen, die 10.106.24.147 kommen, stimmen mit den definierten Platzhalter-Qualifizierern in der DNS-Richtlinie überein. Daher tritt die DNS-Richtlinie in Kraft und löscht die Abfragen.

  Führen Sie den Befehl `dig @10.102.82.13 www.gslbnew.com` auf dem Client 10.106.24.147 aus. Die Ausgabe zeigt, dass Server nicht erreichbar waren.

```
1   root@ns#  dig @10.102.82.13 www.gslbnew.com
2
3   ; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
4   ; (1 server found)
5   ;; global options: +cmd
```



```
;; connection timed out; no servers could be reached
<!--NeedCopy-->
```

- Die Abfragen von 10.106.24.180 stimmen nicht mit den Qualifizierern in der DNS-Richtlinie überein. Daher tritt die DNS-Richtlinie nicht in Kraft und die Abfragen werden verarbeitet.

  Führen Sie den Befehl `dig @10.102.82.13 www.gslbnew.com` auf dem 10.106.24.180-Client aus. Die Ausgabe zeigt die IP-Adresse des virtuellen GSLB-Servers.

```
root@ns# dig @10.102.82.13 www.gslbnew.com

; <<>> DiG 9.11.23 <<>> @10.102.82.13 www.gslbnew.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64265
;; flags: qr aa rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
   ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;www.gslbnew.com.  IN   A

;; ANSWER SECTION:
www.gslbnew.com.    5   IN  A   1.1.1.2

;; Query time: 12 msec
;; SERVER: 10.102.82.13#53(10.102.82.13)
;; WHEN: Tue Mar 29 22:46:40 UTC 2022
;; MSG SIZE  rcvd: 60
<!--NeedCopy-->
```

Angeben der Näherungsmethode

October 5, 2021

Wenn Sie die statische Näherungsdatenbank konfiguriert haben, können Sie die statische Nähe als GLSB-Methode angeben.

So legen Sie die statische Nähe mit der Befehlszeilenschnittstelle fest

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

```
set gslb vserver <name> -lbMethod STATICPROXIMITY
show gslb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver Vserver-GSLB-1 -lbMethod STATICPROXIMITY
show gslb vserver
<!--NeedCopy-->
```

So legen Sie die statische Nähe mit dem Konfigurationsdienstprogramm fest

1. Navigieren Sie zu Traffic Management > GSLB > Virtuelle Server, und doppelklicken Sie auf den virtuellen Server.
2. Klicken Sie auf den Abschnitt **Methode**, und wählen Sie in der Dropdownliste **Methode wählen** die Option **STATICPROXIMITY** aus.

GSLB statische Näherungsdatenbank synchronisieren

October 5, 2021

Für die Synchronisierung einer statischen GSLB-Datenbank (Global Server Load Balancing, Global Server Load Balancing, Global Server Load Balancing, GSLB) muss einer der Sites als Master-GSLB-Knoten identifiziert werden. Jeder Standort in der Topologie kann als Master-Knoten bezeichnet werden. Der Rest der GSLB-Knoten wird automatisch als Slave-Knoten bezeichnet.

Durch das Synchronisieren statischer GSLB-Näherungsdatenbanken werden die Dateien im Verzeichnis /var/netscaler/locdb über die Slave-Knoten hinweg synchronisiert. Während des Synchronisierungsprozesses ruft der Master-Knoten die laufende Konfiguration von jedem der Slave-Knoten ab und vergleicht sie mit der Konfiguration auf dem Master-Knoten. Der Master-GSLB-Knoten verwendet das rsync-Programm, um die statische Näherungsdatenbank über die Slave-Knoten hinweg zu synchronisieren. Um den Synchronisierungsvorgang zu beschleunigen, nimmt das rsync-Programm

nur genügend Änderungen vor, um die Unterschiede zwischen den beiden Dateien zu beseitigen. Der Synchronisierungsvorgang kann nicht zurückgesetzt werden.

Im folgenden Beispiel wird Site2, eine Slave-Site, mit Mastersite Site1 synchronisiert. Der Administrator gibt den Befehl **sync gslb config** auf Site1 ein:

```
sync gslb config -nowarn
Sync Time: Feb 24 2014 14:56:16
Retrieving local site info: ok
Retrieving all participating gslb sites info:
0 bytes in 0 blocks
ok
site1[Master]:
        Getting Config: ok
site2[Slave]:
        Syncing gslb static proximity database: ok
        Getting Config: ok
        Comparing config: ok
        Applying changes: ok
 Done
<!--NeedCopy-->
```

Konfigurieren der Site-zu-Site-Kommunikation

October 5, 2021

Die GSLB-Standort-zu-Standort-Kommunikation erfolgt zwischen den RPC-Knoten (Remote Procedure Call), die den kommunizierenden Sites zugeordnet sind. Ein Master-GSLB-Site stellt Verbindungen mit Slave-Sites her, um die GSLB-Konfigurationsinformationen zu synchronisieren und Standortmetriken auszutauschen.

Ein RPC-Knoten wird automatisch erstellt, wenn eine GSLB-Site erstellt wird und ein intern generierter Benutzername und Kennwort zugewiesen wird. Die Citrix ADC Appliance verwendet diesen Benutzernamen und das Kennwort, um sich während des Verbindungsaufbaus an GSLB-Sites zu authentifizieren. Für einen RPC-Knoten sind keine Konfigurationsschritte erforderlich. Sie können jedoch ein Kennwort Ihrer Wahl angeben, die Sicherheit erhöhen, indem Sie die Informationen verschlüsseln, die GSLB-Sites austauschen, und eine Quell-IP-Adresse für den RPC-Knoten angeben.

Die Appliance benötigt eine Citrix ADC eigene IP-Adresse, die als Quell-IP-Adresse bei der Kommunikation mit anderen GSLB-Sites verwendet werden kann. Standardmäßig verwenden die RPC-Knoten entweder eine Subnetz-IP (SNIP) -Adresse, aber Sie können eine IP-Adresse Ihrer Wahl angeben.

In den folgenden Themen wird das Verhalten und die Konfiguration von RPC-Knoten auf der Citrix ADC Appliance beschrieben:

Ändern des Kennworts eines RPC-Knotens

Citrix empfiehlt Ihnen, die Kommunikation zwischen Sites in Ihrem GSLB-Setup zu sichern, indem Sie das Kennwort jedes RPC-Knotens ändern. Nachdem Sie das Kennwort für den RPC-Knoten des lokalen Standorts geändert haben, müssen Sie die Änderung manuell an den RPC-Knoten an jedem Remotestandort weitergeben.

Das Kennwort wird verschlüsselt gespeichert. Sie können überprüfen, ob sich das Kennwort geändert hat, indem Sie den Befehl show rpcNode verwenden, um die verschlüsselte Form des Kennworts vor und nach der Änderung zu vergleichen.

> **Hinweis:** GSLB verwendet ein internes Benutzerkonto. Zur Verbesserung der Sicherheit empfiehlt Citrix, auch das Kennwort für das interne Benutzerkonto zu ändern. Das Kennwort des internen Benutzerkontos wird durch das RPC-Knotenkennwort geändert.

So ändern Sie das Kennwort eines RPC-Knotens mit der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile die folgenden Befehle ein, um das Kennwort eines RPC-Knotens zu ändern:

```
set ns rpcNode <IPAddress> {
 -password }

show ns rpcNode
<!--NeedCopy-->
```

Beispiel:

```
> set rpcNode 192.0.2.4 -password mypassword
 Done
> show rpcNode
.
.
.
2)  IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
    SrcIP:  *               Secure:  OFF
Done
>
```



```
11
12 <!--NeedCopy-->
```

So heben Sie das Kennwort eines RPC-Knotens mit der Befehlszeilenschnittstelle auf

Wenn Sie das Kennwort eines RPC-Knotens mit der Befehlszeilenschnittstelle aufheben möchten, geben Sie den Befehl unset RpcNode, die IP-Adresse des RPC-Knotens und den Parameter Kennwort ohne Wert ein.

So ändern Sie das Kennwort eines RPC-Knotens mit dem Konfigurationsdienstprogramm

Navigieren Sie zu System > Netzwerk > RPC, wählen Sie den RPC-Knoten aus und ändern Sie das Kennwort.

Verschlüsseln des Austauschs von Standortmetriken

Sie können die Informationen, die zwischen GSLB-Sites ausgetauscht werden, sichern, indem Sie die sichere Option für die RPC-Knoten im GSLB-Setup festlegen. Wenn die sichere Option festgelegt ist, verschlüsselt die Citrix ADC Appliance die gesamte Kommunikation, die vom Knoten an andere RPC-Knoten gesendet wird.

So verschlüsseln Sie den Austausch von Standortmetriken mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den Austausch von Standortmetriken zu verschlüsseln und die Konfiguration zu überprüfen:

```
1 set ns rpcNode <IPAddress> [-secure ( YES | NO )]
2 show rpcNode
3 <!--NeedCopy-->
```

Beispiel:

```
1 > set rpcNode 192.0.2.4 -secure YES
2  Done
3 >
4 > show rpcNode
5 .
6 .
7 .
```



```
3)  IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e SrcIP:
   192.0.2.3     Secure:  ON
 Done
>
<!--NeedCopy-->
```

So heben Sie die Einstellung des sicheren Parameters mit der Befehlszeilenschnittstelle auf

Wenn Sie den sicheren Parameter mit der CLI aufheben möchten, geben Sie den Befehl unset rpcNode, die IP-Adresse des RPC-Knotens und den sicheren Parameter ohne Wert ein.

So verschlüsseln Sie den Austausch von Standortmetriken mithilfe des Citrix ADC Konfigurationsdienstprogramms

1. Navigieren Sie zu System > Netzwerk > RPC, und doppelklicken Sie auf einen RPC-Knoten.
2. Wählen Sie die Option **Sichern** aus, und klicken Sie auf **OK** .

Konfigurieren der Quell-IP-Adresse für einen RPC-Knoten

Standardmäßig verwendet die Citrix ADC Appliance eine Subnetz-IP (SNIP) -Adresse (Citrix ADC) als Quell-IP-Adresse für einen RPC-Knoten. Sie können die Appliance jedoch so konfigurieren, dass sie eine bestimmte SNIP-Adresse verwendet. Wenn keine SNIP-Adresse verfügbar ist, kann die GSLB-Site nicht mit anderen Sites kommunizieren. In einem solchen Szenario müssen Sie entweder die NSIP-Adresse oder eine virtuelle IP-Adresse (VIP) als Quell-IP-Adresse für einen RPC-Knoten konfigurieren. Eine VIP-Adresse kann nur dann als Quell-IP-Adresse eines RPC-Knotens verwendet werden, wenn der RPC-Knoten ein Remote-Knoten ist. Wenn Sie eine VIP-Adresse als Quell-IP-Adresse konfigurieren und die VIP-Adresse entfernen, verwendet die Appliance eine SNIP-Adresse.

> **Hinweis:**
>
> Ab NetScaler 11.0.64.x können Sie die Appliance so konfigurieren, dass die GSLB-Site-IP-Adresse als Quell-IP-Adresse für einen RPC-Knoten verwendet wird.

So geben Sie mit der Befehlszeilenschnittstelle eine Quell-IP-Adresse für einen RPC-Knoten an

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Quell-IP-Adresse für einen RPC-Knoten zu ändern und die Konfiguration zu überprüfen:

```
set ns rpcNode <IPAddress> [-srcIP <ip_addr|ipv6_addr|*>]
show ns rpcNode
```



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

Beispiel:

```
set rpcNode 192.0.2.4 -srcIP 192.0.2.3
Done
show rpcNode
<!--NeedCopy-->
```

```
IPAddress: 192.0.2.4 Password: d336004164d4352ce39e SrcIP: 192.0.2.3
   Secure: OFF
Done
<!--NeedCopy-->
```

So heben Sie die Einstellung des Quell-IP-Adressparameters mit der Befehlszeilenschnittstelle auf

Um die Einstellung des Quell-IP-Adressparameters mit der Befehlszeilenschnittstelle aufzuheben, geben Sie den unset rpcNodecommand, die IP-Adresse des RPC-Knotens und den srcIP-Parameter ohne Wert ein.

So geben Sie mithilfe des Citrix ADC C-Konfigurationsdienstprogramms eine Quell-IP-Adresse für einen RPC-Knoten an

1. Navigieren Sie zu System > Netzwerk > RPC, und doppelklicken Sie auf einen RPC-Knoten.
2. Geben Sie im Feld Quell-IP-Adresse die IP-Adresse ein, die der RPC-Knoten als Quell-IP-Adresse verwenden soll, und klicken Sie auf OK.

> **Wichtig**
>
> Die Quell-IP-Adresse kann nicht über die an GSLB beteiligten Sites synchronisiert werden, da die Quell-IP-Adresse für einen RPC-Knoten spezifisch für jede Citrix ADC Appliance ist. Nachdem Sie eine Synchronisierung erzwungen haben (mit dem Befehl sync gslb config —ForceSync oder durch Auswahl der Option ForceSync in der GUI), müssen Sie die Quell-IP-Adressen auf den anderen Citrix ADC Appliances manuell ändern.

Konfigurieren des Metrikaustauschprotokolls

October 5, 2021

Die Rechenzentren in einer GSLB-Setupaustauschmetrik untereinander über das Metrics Exchange-Protokoll (MEP), das ein proprietäres Protokoll für Citrix ADC Appliance ist. Der Austausch der Metrikinformationen beginnt, wenn Sie eine GSLB-Site erstellen. Diese Metriken umfassen Last-, Netzwerk- und Persistenzinformationen.

MEP ist für die Zustandsprüfung von Rechenzentren erforderlich, um deren Verfügbarkeit sicherzustellen. Eine Verbindung zum Austausch von Netzwerkmetriken (Round-Trip-Zeit) kann von jedem der am Austausch beteiligten Rechenzentren initiiert werden. Eine Verbindung zum Austausch von Standortmetriken wird jedoch immer vom Rechenzentrum mit der niedrigeren IP-Adresse initiiert. Standardmäßig verwendet das Rechenzentrum eine Subnetz-IP-Adresse (SNIP), um eine Verbindung mit der IP-Adresse eines anderen Rechenzentrums herzustellen. Sie können jedoch eine bestimmte SNIP, eine virtuelle IP-Adresse (VIP) oder die NSIP-Adresse als Quell-IP-Adresse für den Metrikaustausch konfigurieren. Der Kommunikationsprozess zwischen GSLB-Sites verwendet TCP-Port 3011 oder 3009. Daher muss dieser Port auf Firewalls geöffnet sein, die sich zwischen den Citrix ADC Appliances befinden.

Hinweis: Sie können eine SNIP- oder eine GSLB-Site-IP-Adresse als Quell-IP-Adresse für den Metrikaustausch konfigurieren. Weitere Informationen finden Sie unter Konfigurieren der Quell-IP-Adresse für einen RPC-Knoten.

Wenn die Quell- und Zielsites (der Standort, der eine MEP-Verbindung initiiert, bzw. der Standort, der die Verbindungsanforderung empfängt) sowohl private als auch öffentliche IP-Adressen konfiguriert haben, tauschen die Sites MEP-Informationen mithilfe der öffentlichen IP-Adressen aus.

Sie können Monitore auch binden, um den Zustand der Remote-Dienste zu überprüfen, wie unter “Überwachung von GSLB-Diensten beschrieben. “ Wenn Monitore gebunden sind, steuert der Metrikaustausch nicht den Status des Remote-Dienstes. Wenn ein Monitor an einen Remotedienst gebunden ist und Metrikaustausch aktiviert ist, steuert der Monitor den Integritätsstatus. Durch das Binden der Monitore an den Remote-Dienst kann die Citrix ADC Appliance mit einem nicht von Citrix ADC Load Balancing-Gerät interagieren. Die Citrix ADC Appliance kann Nicht-Citrix ADC-Geräte überwachen, kann jedoch keinen Lastenausgleich auf ihnen durchführen, es sei denn, Monitore sind an alle GSLB-Dienste gebunden und es werden nur statische Lastausgleichsmethoden (wie Round-Robin, statische Nähe oder Hash-basierte Methoden) verwendet.

Mit NetScaler Version 11.1.51.x oder höher können Sie eine Zeitverzögerung für die Kennzeichnung von GSLB-Diensten als DOWN festlegen, um unnötige Unterbrechungen von Diensten zu vermeiden.

MEP-Status in einem Hochverfügbarkeitssetup

In einem Hochverfügbarkeitssetup stellt der primäre Knoten Verbindungen mit den Remote-Standorten her und der MEP-Status wird nicht vom primären Knoten zu sekundären Knoten synchronisiert. Daher bleibt der MEP-Status im sekundären Knoten DOWN. Wenn der sekundäre Knoten primär wird, stellt er MEP-Verbindungen mit dem neuen GSLB-Standort her und aktualisiert den MEP-Status entsprechend.

Austausch von Standortmetriken aktivieren

Standortmetriken, die zwischen den GSLB-Sites ausgetauscht werden, umfassen den Status jedes Lastausgleichs oder eines virtuellen Content Switching-Servers, die aktuelle Anzahl von Verbindungen, die aktuelle Paketrate und Informationen zur aktuellen Bandbreitennutzung.

Die Citrix ADC Appliance benötigt diese Informationen, um den Lastenausgleich zwischen den Sites durchzuführen. Das Sitemetrikaustauschintervall beträgt 1 Sekunde. Ein Remote-GSLB-Dienst muss an einen lokalen virtuellen GSLB-Server gebunden sein, um den Austausch von Standortmetriken mit dem Remotedienst zu ermöglichen.

So aktivieren oder deaktivieren Sie den Austausch von Standortmetriken mit der Befehlszeilenschnittstelle

Geben Sie an einer Eingabeaufforderung die folgenden Befehle ein, um den Standortmetrikaustausch zu aktivieren oder zu deaktivieren und die Konfiguration zu überprüfen:

```
set gslb site <siteName> -metricExchange (ENABLED|DISABLED)
show gslb site** <siteName>
<!--NeedCopy-->
```

Beispiel:

```
set gslb site Site-GSLB-East-Coast -metricExchange ENABLED
set gslb site Site-GSLB-East-Coast -metricExchange DISABLED
show gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

So aktivieren oder deaktivieren Sie den Standortmetrikaustausch mit der GUI

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Sites**, und wählen Sie die Site aus.
2. Wählen Sie im Dialogfeld **GSLB-Site konfigurieren** die Option **Metrikaustausch** aus.

Netzwerkmetrikaustausch aktivieren

Wenn Ihre GSLB-Sites die Roundtrip Time (RTT) Lastausgleichsmethode verwenden, können Sie den Austausch von RTT-Informationen über den lokalen DNS-Dienst des Clients aktivieren oder deaktivieren. Diese Informationen werden alle 5 Sekunden ausgetauscht.

Weitere Informationen zum Ändern der GSLB-Methode in eine auf RTT basierende Methode finden Sie unter GSLB-Methoden.

So aktivieren oder deaktivieren Sie den Austausch von Netzwerkmetrikinformationen mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den Austausch von Netzwerkmetrikinformationen zu aktivieren oder zu deaktivieren und die Konfiguration zu überprüfen:

```
set gslb site <siteName> -nwmetricExchange (ENABLED|DISABLED)
show gslb site <<siteName>
<!--NeedCopy-->
```

Beispiel:

```
set gslb site Site-GSLB-East-Coast -nwmetricExchange ENABLED
set gslb site Site-GSLB-East-Coast -nwmetricExchange DISABLED
show gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

So aktivieren oder deaktivieren Sie den Austausch von Netzwerkmetrikinformationen mit der GUI

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Sites**.
2. Wählen **Sie im Dialogfeld GSLB-Site konfigurieren** die Option **Netzwerkmetrikaustausch** aus.

Konfigurieren einer Zeitverzögerung für die GSLB-Dienste, die als DOWN markiert werden, wenn eine MEP-Verbindung heruntergeht

Wenn sich der Status einer MEP-Verbindung zu einem Remotestandort in DOWN ändert, wird der Status jedes GSLB-Dienstes auf diesem Remotestandort als DOWN markiert, obwohl der Standort möglicherweise nicht tatsächlich DOWN ist.

Sie können jetzt eine Verzögerung festlegen, um einige Zeit für die Wiederherstellung der MEP-Verbindung einzuräumen, bevor der Standort als DOWN markiert wird. Wenn die MEP-Verbindung vor Ablauf der Verzögerung wieder UP ist, sind die Dienste nicht betroffen.

Wenn Sie beispielsweise die Verzögerung 10 festlegen, werden die GSLB-Dienste als DOWN markiert, bis die MEP-Verbindung 10 Sekunden lang DOWN war. Wenn die MEP-Verbindung innerhalb von 10 Sekunden wieder UP ist, bleiben die GSLB-Dienste im Status UP.

Hinweis: Diese Verzögerung gilt nur für Dienste, die nicht an einen Monitor gebunden sind. Die Verzögerung hat keinen Einfluss auf die Trigger-Monitore.

So legen Sie eine Zeitverzögerung mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set gslb parameter** - GSLBSvcStateDelayTime <sec>
<!--NeedCopy-->
```

Beispiel:

set gslb parameter - GSLBSvcStateDelayTime 10

> **Hinweis:**
>
> Wenn Sie in einer hierarchischen Bereitstellung (Parent-Child-Topologie) den GSLB-Dienst sowohl auf den übergeordneten als auch an den untergeordneten Standorten konfigurieren, legen Sie den GSLB-Parameter sowohl auf den übergeordneten als auch auf den untergeordneten Sites fest. Wenn Sie den GSLB-Dienst nicht auf der untergeordneten Site konfigurieren, legen Sie den GSLB-Parameter nur auf der übergeordneten Site fest.

So legen Sie eine Zeitverzögerung mit der GUI fest

1. Navigieren Sie zu **Konfiguration** > **Verkehrsverwaltung** > **GSLB** > **GSLB-Einstellungen ändern**.
2. Geben Sie im Feld **GSLB-Dienststatus-Verzögerungszeit (Sekunden)** die Zeitverzögerung in Sekunden ein.

Konfigurieren Sie eine Lernzeit für GSLB-Dienste, wenn der MEP-Verbindungsstatus auftaucht, um Klappen bei GSLB-Diensten zu vermeiden

Wenn ein Knoten neu gestartet wird oder während des HA-Failovers, wird das System initialisiert. Dann muss der Knoten aktuelle Informationen über die konfigurierten lokalen und untergeordneten Dienste erfahren, um den Dienststatus über MEP an Remote-Knoten zu kommunizieren. Der

Knoten braucht einige Zeit, um die richtigen Informationen zu erfahren. Wenn ein Peer-Knoten eine Verbindung zu diesem Knoten herstellt und ein Update anfordert, sendet der Knoten möglicherweise einen falschen Dienststatus und Statistiken. Diese falschen Informationen können zu Service-Flap und anderen funktionalbezogenen Problemen auf den Remote-Peer-Knoten führen. Um dieses Szenario zu vermeiden, können Sie jetzt eine Lernzeit für den lokalen und untergeordneten GSLB Service festlegen.

Wenn ein Lern-Timeout konfiguriert ist, erhält die GSLB-Site etwas Pufferzeit (Lern-Timeout), um die richtigen Statistiken über ihren lokalen und untergeordneten Service zu erfahren. Wenn sich ein Dienst in einer Lernphase befindet, erhält die Remote-GSLB-Site diese Informationen im MEP-Update und berücksichtigt nicht den primären Standortstatus und die Statistiken, die von MEP für diesen Dienst erhalten wurden.

GSLB-Dienste treten in einem der folgenden Szenarien in die Lernphase ein.

- Citrix ADC Appliance wird neu gestartet
- Ein Failover mit hoher Verfügbarkeit ist aufgetreten
- Owner-Knoten in einem Cluster GSLB-Setup wird geändert
- MEP ist auf einem lokalen Knoten aktiviert
- Die GSLB-Site kommt aus dem Inselszenario heraus. Eine GSLB-Site wird zur Insel, wenn sie mit keiner anderen Site verbunden ist.

In einer Eltern-Kind-Bereitstellung verschiebt das übergeordnete Backup-Element (falls konfiguriert) die GSLB-Dienste der übernommenen untergeordneten Website selektiv in die Lernphase, in der das primäre Elternteil NACH UNTEN geht.

So legen Sie eine Lernzeit für den Service-Status mit der CLI fest

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set gslb parameter - SvcStateLearningTime <sec>
<!--NeedCopy-->
```

Sie können “SvcStateLearningTime” in Sekunden einstellen. Der Standardwert ist 0 und der Maximalwert beträgt 3600. Dieser Parameter ist nur anwendbar, wenn Monitore nicht an GSLB-Dienste gebunden sind.

Beispiel:

```
set gslb parameter - SvcStateLearningTime 10
<!--NeedCopy-->
```


So legen Sie eine Lernzeit für den Service-Status mit der GUI fest

1. Navigieren Sie zu **Konfiguration > Traffic Management > GSLB > Dashboard > GSLB-Einstellungen ändern**.

   Die Seite **GSLB-Parameter festlegen** wird angezeigt.

2. Geben Sie im Feld **GSLB Service State Learning Time (Sekunden)** die Lernzeit in Sekunden ein.

Persistenzinformationsaustausch aktivieren

Sie können die Citrix ADC Appliance so konfigurieren, dass sie persistente Verbindungen bereitstellt, sodass eine Clientübertragung an einen beliebigen virtuellen Server in einer Gruppe an einen Server weitergeleitet werden kann, der frühere Übertragungen vom selben Client empfangen hat.

Sie können den Austausch von Persistenzinformationen an jedem Standort aktivieren oder deaktivieren. Diese Informationen werden alle 5 Sekunden zwischen Citrix ADC Appliances ausgetauscht, die an GSLB teilnehmen.

Weitere Informationen zum Konfigurieren von Persistenz finden Sie unter Persistente Verbindungen konfigurieren.

So aktivieren oder deaktivieren Sie den Persistenzinformationsaustausch mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den Persistenzinformationsaustausch zu aktivieren oder zu deaktivieren und die Konfiguration zu überprüfen:

```
set gslb site <siteName> -sessionExchange (ENABLED|DISABLED)
show gslb site** <siteName>
<!--NeedCopy-->
```

Beispiel:

```
set gslb site Site-GSLB-East-Coast -sessionExchange  ENABLED
set gslb site Site-GSLB-East-Coast -sessionExchange  DISABLED
show gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```


So aktivieren oder deaktivieren Sie den Persistenzinformationsaustausch mit der GUI

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Sites**, und doppelklicken Sie auf die Site.
2. Aktivieren oder deaktivieren **Sie im Dialogfeld GSLB-Site konfigurieren** das Kontrollkästchen **Persistence Session Entry Exchange**.

Konfigurieren von GSLB mit einem Assistenten

October 5, 2021

Sie können nun einen Assistenten verwenden, um die GSLB-Bereitstellungstypen zu konfigurieren: active-active, active-passive und übergeordnet-child.

Dieser Assistent ist in der GUI verfügbar. Um auf den Assistenten zuzugreifen, navigieren Sie zu **Konfiguration** > **Traffic Management** > **GSLB** und klicken Sie auf **Erste Schritte** .

Sie können diesen Assistenten auch über das GSLB-Dashboard aufrufen. Navigieren Sie zu **Konfiguration** > **Verkehrsverwaltung** > **GSLB** > **Dashboard**, und klicken Sie auf **GSLB konfigurieren** .

Hinweis: Sie können die GSLB-Entitäten auch einzeln konfigurieren.

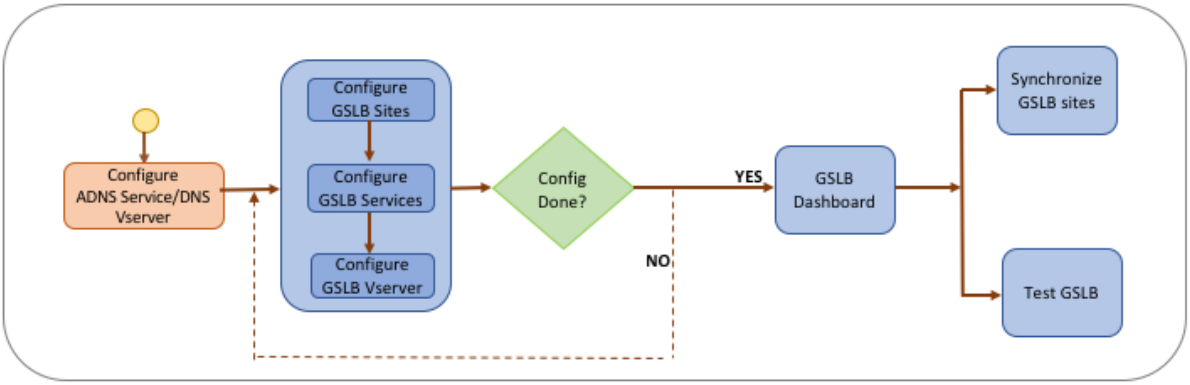
- Active-Active-Sitekonfiguration
- Aktiv-Passiv-Standort-Konfigurationon
- Konfiguration der übergeordneten und untergeordneten Topologie

> **Wichtig**
>
> Diese Funktion wird in der Hochverfügbarkeitsbereitstellung und nicht in Adminpartitions- und Clusterbereitstellungen unterstützt.

Aktiv-Aktiv-Site konfigurieren

October 5, 2021

Die folgende Abbildung zeigt den Workflow, der an einer aktiven GSLB-Sitekonfiguration beteiligt ist.



Bevor Sie mit der Konfiguration eines Active-Active-Site beginnen, stellen Sie sicher, dass Sie für jede Serverfarm oder jedes Rechenzentrum eine standardmäßige Lastausgleichseinrichtung konfiguriert haben.

Für die Synchronisierung der GSLB-Konfiguration über die GSLB-Sites in der Bereitstellung stellen Sie außerdem Folgendes sicher:

- Lokale GLSB-Sites werden auf allen Appliances in der GSLB-Konfiguration konfiguriert.
- Sie haben den Verwaltungszugriff auf alle GSLB-Sites in der Konfiguration aktiviert.
- Sie haben die Firewall so konfiguriert, dass sie die automatische Synchronisierung und MEP-Verbindungen akzeptiert.
- Auf den Master- und Slave-Citrix ADC Appliances werden dieselben Citrix ADC-Softwareversionen ausgeführt.
- Alle Citrix ADC Appliances, die an Sites teilnehmen, sollten dieselbe Citrix ADC -Softwareversion aufweisen (die Sites befinden sich nicht in einer Master-Slave-Beziehung).
- Das RPC-Knotenkennwort ist für alle GSLB-Sites in der GSLB-Konfiguration identisch.

So konfigurieren Sie eine aktive Site mit dem Assistenten

Gehen Sie auf der Registerkarte Konfiguration folgendermaßen vor:

1. Navigieren Sie zu **Traffic Management** > **GSLB**, und klicken Sie dann auf **Erste Schritte**.
2. Wenn Sie keinen ADNS-Dienst oder einen virtuellen DNS-Server für die Site konfiguriert haben, können Sie dies jetzt tun.
   a) Klicken Sie auf **Ansicht** und dann auf **Hinzufügen**.
   b) Geben Sie den Dienstnamen und die IP-Adresse ein und wählen Sie das Protokoll (ADNS/ADNS_TCP) aus, über das die Daten mit dem Dienst ausgetauscht werden.
3. Wählen Sie **Aktiv-Aktive Site**aus.
4. Geben Sie den vollqualifizierten Domänennamen ein und geben Sie den Zeitraum an, für den der Datensatz von DNS-Proxys zwischengespeichert werden muss.
5. Konfigurieren Sie die GSLB-Sites. Jede Site muss mit einer lokalen GSLB-Site konfiguriert werden, und die Konfiguration jeder Site muss alle anderen Sites als Remote-GSLB-Sites enthalten.

Es kann nur eine lokale Site geben, alle anderen Sites sind Remotesites.

a) Geben Sie die Sitedetails ein, z. B. den Sitename und die Site-IP-Adresse.
b) Wählen Sie für den Sitetyp entweder REMOTE oder LOCAL.
c) Optional können Sie das RPC-Kennwort ändern und ggf. sichern.
d) Wenn ein Monitor an den GSLB-Dienst gebunden werden soll, wählen Sie die Bedingung, unter der der Monitor den Dienst überwachen soll. Dies wird erst wirksam, wenn ein Monitor an die Dienste gebunden ist. Mögliche Bedingungen sind:
   - **ALWAYS**. Überwachen Sie den GSLB-Dienst jederzeit.
   - **MEP Fails**. Überwachen Sie den GSLB-Dienst nur, wenn der Austausch von Metriken über MEP fehlschlägt.
   - **MEP Fails and Service ID Down**. Der Austausch von Metriken über MEP ist aktiviert, aber der Status des Dienstes, der durch den Metrikaustausch aktualisiert wird, ist DOWN.

6. Konfigurieren Sie die GSLB-Dienste. Um eine aktive Website zu erstellen, müssen Sie mindestens zwei GSLB-Dienste hinzufügen.
   a) Geben Sie die Service-Details ein, wie Dienstname, Diensttyp und Portnummer.
   b) Ordnen Sie den Dienst einem Standort (lokal oder remote) zu, indem Sie den GSLB-Site auswählen, zu dem der GSLB-Dienst gehört.
   c) Wählen Sie den Monitor aus, der bei einem Ausfall des MEP an den Dienst gebunden werden muss. Der Dienst kann ein vorhandener Server sein, oder Sie können einen neuen Server oder einen virtuellen Server erstellen.
   d) Um einen vorhandenen Server zuzuordnen, wählen Sie den Servernamen aus. Die Dienst-IP-Adresse wird automatisch ausgefüllt.
      - Wenn sich die öffentliche IP-Adresse von der Server-IP-Adresse unterscheidet, die in einer NAT-Umgebung auftreten kann, geben Sie die öffentliche IP-Adresse und die Portnummer des öffentlichen Ports ein.
      - Um einen neuen Server zuzuordnen, erstellen Sie einen Server, indem Sie die IP-Details des Servers, die öffentliche IP-Adresse und die öffentliche Portnummer eingeben.
      - Um einen virtuellen Server zuzuordnen, wählen Sie einen bereits vorhandenen virtuellen Server aus, oder klicken Sie auf +, und fügen Sie einen neuen virtuellen Server hinzu. Dieser vserver ist der Lastenausgleich vserver, dem dieser GSLB-Dienst zugeordnet wird.

7. Konfigurieren Sie die virtuellen GSLB-Server.
   a) Geben Sie den Namen des virtuellen GSLB-Servers ein, und wählen Sie den DNS-Eintragstyp aus.
   b) Klicken Sie im Feld **Dienst auswählen** auf **>**, und wählen Sie die GSLB-Dienste aus, die an den virtuellen GSLB-Server gebunden werden sollen.
   c) Klicken Sie im Feld **Domänenbindung** auf **>**, um die Domäne auszuwählen, die an diesen

virtuellen GSLB-Server gebunden werden soll.

d) Wählen Sie die GSLB-Methode zur Auswahl des leistungsstärksten GSLB-Dienstes. Die Standardwerte für die GSLB-Methode, die Backupmethode und die dynamische Gewichtung werden standardmäßig automatisch ausgefüllt. Sie können sie bei Bedarf ändern.

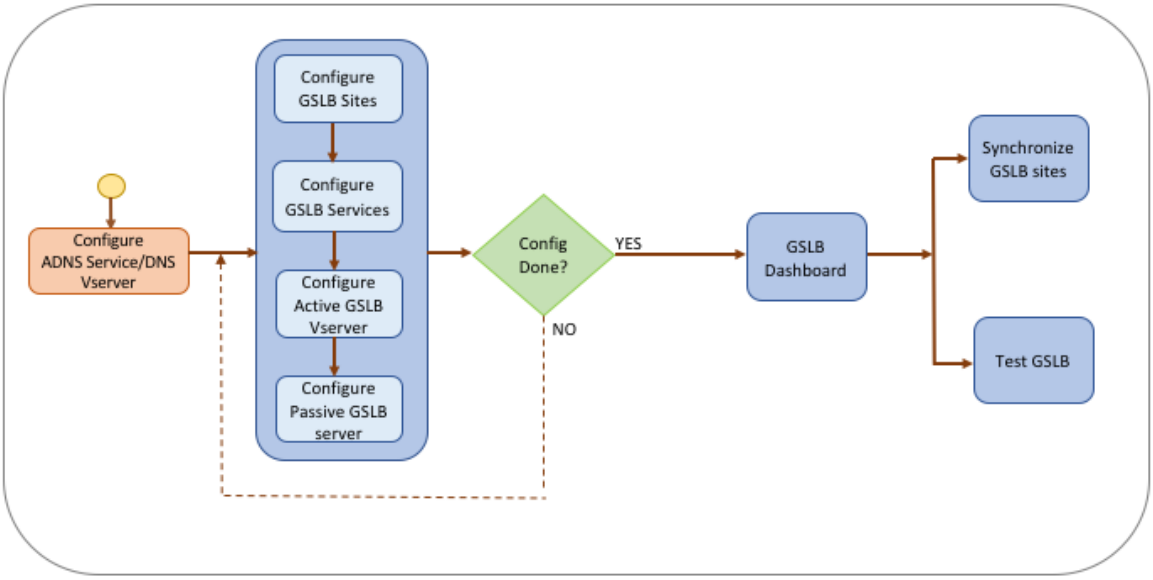
- Wenn Sie die **Algorithmus-basierte** Methode wählen, wählen Sie die primäre Methode und die Backupmethode aus, und geben Sie auch die Option für die dynamische Gewichtung an.
- Wenn Sie die **Statische Proximity-Methode** wählen, wählen Sie die Backupmethode und die dynamische Gewichtungsmethode aus. Geben Sie außerdem den Speicherort der Datenbankdatei an, indem Sie auf das Symbol > klicken oder einen neuen Speicherort hinzufügen, indem Sie im Feld Standortdatenbank auswählen auf **+** klicken.
- Wenn Sie die **RTT-Methode (Dynamic Proximity)** wählen, wählen Sie die Backupmethode aus, und geben Sie die Option für die dynamische Gewichtung und den Wert für die Roundtrip an, basierend auf dem der leistungsstärkste Dienst ausgewählt werden soll.

8. Klicken Sie auf **Fertig**, wenn die Konfiguration abgeschlossen ist. Das GSLB-Dashboard wird angezeigt.
9. Wenn Sie die GSLB-Sitekonfiguration geändert haben, klicken Sie im Dashboard auf **Autosynchronize GSLB**, um die Konfiguration mit anderen Sites im GSLB-Setup zu synchronisieren.
   - Stellen Sie vor der Synchronisierung sicher, dass die Konfiguration des lokalen Standorts Informationen zu den Remotesites enthält. Damit die Synchronisierung erfolgreich ist, muss der lokale Standort auf den anderen Citrix ADC Appliances konfiguriert werden.
   - Wenn die Echtzeitsynchronisierung aktiviert ist, müssen Sie nicht auf **GSLB automatisch synchronisieren** klicken. Die Synchronisation erfolgt automatisch. Gehen Sie folgendermaßen vor, um die Echtzeitsynchronisierung zu aktivieren:
     a) Navigieren Sie zu **Traffic Management** > **GSLB** > **Dashboard** und klicken Sie auf **GSLB-Einstellungen ändern**.
     b) Aktivieren Sie das Kontrollkästchen **Automatische Synchronisierung der Konfiguration**.
10. Klicken Sie auf **GSLB-Setup testen**, um sicherzustellen, dass die ADNS-Dienste oder DNS-Server mit der richtigen IP-Adresse für den Domänennamen reagieren, der im GSLB-Setup konfiguriert ist.

Aktiv-Passiv-Site konfigurieren

December 7, 2021

Die folgende Abbildung zeigt den Workflow, der an der aktiv-passiven Sitekonfiguration beteiligt ist.



Bevor Sie mit der Konfiguration eines aktiven und passiven Standorts beginnen, stellen Sie sicher, dass Sie für jede Serverfarm oder jedes Rechenzentrum eine standardmäßige Lastausgleichseinrichtung konfiguriert haben.

Für die Synchronisierung der GSLB-Konfiguration über die GSLB-Sites in der Bereitstellung stellen Sie außerdem Folgendes sicher:

- Lokale GLSB-Sites werden auf allen Appliances in der GSLB-Konfiguration konfiguriert.
- Sie haben den Verwaltungszugriff auf alle GSLB-Sites in der Konfiguration aktiviert.
- Sie haben die Firewall so konfiguriert, dass sie die automatische Synchronisierung und MEP-Verbindungen akzeptiert.
- Auf den Master- und Slave-Citrix ADC Appliances werden dieselben Citrix ADC-Softwareversionen ausgeführt.
- Alle Citrix ADC Appliances, die an Sites teilnehmen, sollten dieselbe Citrix ADC -Softwareversion aufweisen (die Sites befinden sich nicht in einer Master-Slave-Beziehung).
- Das RPC-Knotenkennwort ist für alle GSLB-Sites in der GSLB-Konfiguration identisch.

So konfigurieren Sie eine aktive-passive Site mit dem Assistenten

Gehen Sie auf der Registerkarte Konfiguration folgendermaßen vor:

1. Navigieren Sie zu **Traffic Management** > **GSLB**, und klicken Sie dann auf **Erste Schritte**.
2. Wenn Sie keinen ADNS-Dienst oder einen virtuellen DNS-Server für die Site konfiguriert haben, können Sie dies jetzt tun.
   a) Klicken Sie auf **Ansicht** und dann auf **Hinzufügen**.

b) Geben Sie den Dienstnamen und die IP-Adresse ein und wählen Sie das Protokoll (ADNS/ADNS_TCP) aus, über das die Daten mit dem Dienst ausgetauscht werden.

3. Wählen Sie **Aktiv-Passive Site**aus.
4. Geben Sie den vollqualifizierten Domänennamen ein und geben Sie den Zeitraum an, für den der Datensatz von DNS-Proxys zwischengespeichert werden muss.
5. Konfigurieren Sie die GSLB-Sites. Jede Site muss mit einer lokalen GSLB-Site konfiguriert werden, und die Konfiguration jeder Site muss alle anderen Sites als Remote-GSLB-Sites enthalten. Es kann nur eine lokale Site geben, alle anderen Sites sind Remotesites.
   a) Geben Sie die Sitedetails ein, z. B. den Sitename und die Site-IP-Adresse.
   b) Wählen Sie für den Sitetyp entweder REMOTE oder LOCAL.
   c) Optional können Sie das RPC-Kennwort ändern und ggf. sichern.
   d) Wenn ein Monitor an den GSLB-Dienst gebunden werden soll, wählen Sie die Bedingung, unter der der Monitor den Dienst überwachen soll. Dies wird erst wirksam, wenn ein Monitor an die Dienste gebunden ist. Mögliche Bedingungen sind:
      - **ALWAYS**. Überwachen Sie den GSLB-Dienst jederzeit.
      - **MEP Fails**. Überwachen Sie den GSLB-Dienst nur, wenn der Austausch von Metriken über MEP fehlschlägt.
      - **MEP Fails and Service ID Down**. Der Austausch von Metriken über MEP ist aktiviert, aber der Status des Dienstes, der durch den Metrikaustausch aktualisiert wird, ist DOWN.
6. Konfigurieren Sie die GSLB-Dienste.
   a) Geben Sie die Service-Details ein, wie Dienstname, Diensttyp und Portnummer.
   b) Ordnen Sie den Dienst einem Standort (lokal oder remote) zu, indem Sie den GSLB-Site auswählen, zu dem der GSLB-Dienst gehört.
   c) Wählen Sie den Monitor aus, der bei einem Ausfall des MEP an den Dienst gebunden werden muss. Der Dienst kann ein vorhandener Server sein, oder Sie können einen neuen Server oder einen virtuellen Server erstellen.
   d) Um einen vorhandenen Server zuzuordnen, wählen Sie den Servernamen aus. Die Dienst-IP-Adresse wird automatisch ausgefüllt.
      - Wenn sich die öffentliche IP-Adresse von der Server-IP-Adresse unterscheidet, die in einer NAT-Umgebung auftreten kann, geben Sie die öffentliche IP-Adresse und die Portnummer des öffentlichen Ports ein.
      - Um einen neuen Server zuzuordnen, erstellen Sie einen Server, indem Sie die IP-Details des Servers, die öffentliche IP-Adresse und die öffentliche Portnummer eingeben.
      - Um einen virtuellen Server zuzuordnen, wählen Sie einen bereits vorhandenen virtuellen Server aus, oder klicken Sie auf **+**, und fügen Sie einen neuen virtuellen Server hinzu. Dieser vserver ist der Lastenausgleich vserver, dem dieser GSLB-Dienst zugeordnet wird.

7. Konfigurieren Sie die virtuellen GSLB-Backup-Server. Die GSLB Backup virtuellen Server werden nur dann betriebsbereit, wenn auf die primären virtuellen GSLB Server nicht zugegriffen werden kann oder sie aus irgendeinem Grund als DOWN gekennzeichnet ist.
   a) Geben Sie den Namen des virtuellen GSLB-Servers ein, und wählen Sie den DNS-Eintragstyp aus.
   b) Klicken Sie unter **Dienstbindung** auf **>**, und wählen Sie die GSLB-Dienste aus, die an den virtuellen GSLB-Server gebunden werden müssen.
   c) Wählen Sie die GSLB-Methode zur Auswahl des leistungsstärksten GSLB-Dienstes. Die Standardwerte für die GSLB-Methode, die Backupmethode und die dynamische Gewichtung werden standardmäßig automatisch ausgefüllt. Sie können sie bei Bedarf ändern.
      - Wenn Sie die **Algorithmus-basierte** Methode wählen, wählen Sie die primäre und die Backupmethode aus.
      - Wenn Sie die **Statische Proximity-Methode** wählen, wählen Sie die Backupmethode aus, und geben Sie den Speicherort der Datenbankdatei an.
      - Wenn Sie die **RTT-Methode (Dynamic Proximity)** wählen, wählen Sie die Backupmethode aus, und geben Sie das Dienstgewicht und den RTT-Wert an, basierend auf dem der leistungsstärkste Dienst ausgewählt werden soll.
8. Konfigurieren Sie die virtuellen GSLB-Server.
   a) Geben Sie den Namen des virtuellen GSLB-Servers ein, und wählen Sie den DNS-Eintragstyp aus.
   b) Klicken Sie im Feld **Dienst auswählen** auf **>**, und wählen Sie die GSLB-Dienste aus, die an den virtuellen GSLB-Server gebunden werden sollen.
   c) Klicken Sie im Feld **Domänenbindung** auf **>**, um die Domäne auszuwählen, die an diesen virtuellen GSLB-Server gebunden werden soll.
   d) Wählen Sie die GSLB-Methode zur Auswahl des leistungsstärksten GSLB-Dienstes. Die Standardwerte für die GSLB-Methode, die Backupmethode und die dynamische Gewichtung werden standardmäßig automatisch ausgefüllt. Sie können sie bei Bedarf ändern.
      - Wenn Sie die **Algorithmus-basierte** Methode wählen, wählen Sie die primäre Methode und die Backupmethode aus, und geben Sie auch die Option für die dynamische Gewichtung an.
      - Wenn Sie die **Statische Proximity-Methode** wählen, wählen Sie die Backupmethode und die dynamische Gewichtungsmethode aus. Geben Sie außerdem den Speicherort der Datenbankdatei an, indem Sie auf das Symbol klicken oder einen neuen Speicherort hinzufügen, indem Sie im Feld Standortdatenbank auswählen auf **+** klicken.
      - Wenn Sie die **RTT-Methode (Dynamic Proximity)** wählen, wählen Sie die Backupmethode aus, und geben Sie die Option für die dynamische Gewichtung und den Wert

für die Roundtrip an, basierend auf dem der leistungsstärkste Dienst ausgewählt werden soll.

9. Klicken Sie auf **Fertig**, wenn die Konfiguration abgeschlossen ist. Das GSLB-Dashboard wird angezeigt.
10. Wenn Sie die GSLB-Sitekonfiguration geändert haben, klicken Sie im Dashboard auf **Autosynchronize GSLB**, um die Konfiguration mit anderen Sites im GSLB-Setup zu synchronisieren.
    - Stellen Sie vor der Synchronisierung sicher, dass die Konfiguration des lokalen Standorts Informationen zu den Remotesites enthält. Damit die Synchronisierung erfolgreich ist, muss der lokale Standort auf den anderen Citrix ADC Appliances konfiguriert werden.
    - Wenn die Echtzeitsynchronisierung aktiviert ist, müssen Sie nicht auf **GSLB automatisch synchronisieren** klicken. Die Synchronisation erfolgt automatisch. Gehen Sie folgendermaßen vor, um die Echtzeitsynchronisierung zu aktivieren:
      a) Navigieren Sie zu **Traffic Management** > **GSLB** > **Dashboard** und klicken Sie auf **GSLB-Einstellungen ändern**.
      b) Aktivieren Sie das Kontrollkästchen **Automatische Synchronisierung der Konfiguration**.
11. Klicken Sie auf **GSLB-Setup testen**, um sicherzustellen, dass die ADNS-Dienste oder DNS-Server mit der richtigen IP-Adresse für den Domänennamen reagieren, der im GSLB-Setup konfiguriert ist.

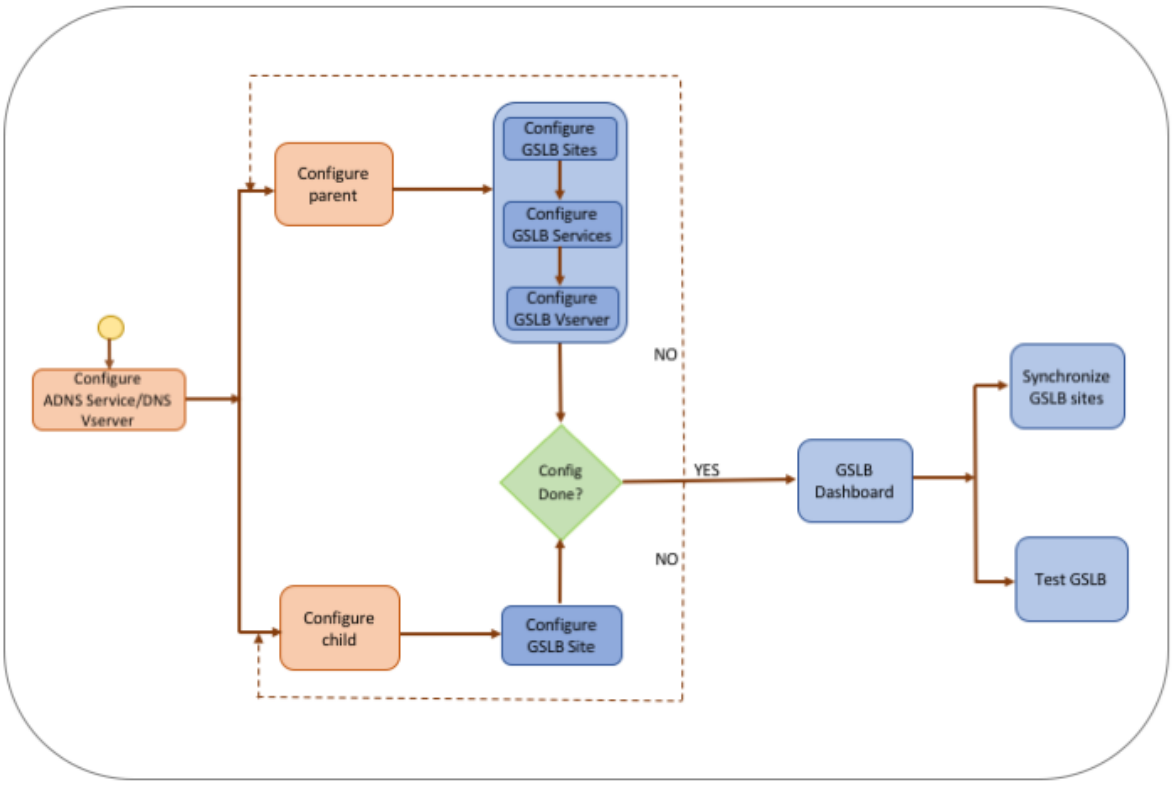
> **Hinweis:**
>
> Weitere Informationen zum Konfigurieren von GSLB-Entitäten eines aktiv-passiven GSLB-Setups für Disaster Recovery finden Sie unter Konfigurieren von GSLB für Disaster Recovery.

Konfigurieren der übergeordneten und untergeordneten Topologie

December 7, 2021

In einer übergeordneten und untergeordneten Topologie befinden sich auf der obersten Ebene übergeordnete Websites, die Peer-Beziehungen zu anderen übergeordneten Elementen aufweisen. Jeder übergeordnete Standort kann über mehrere untergeordnete Sites verfügen, und jeder übergeordnete Standort tauscht Integritätsinformationen mit seinen untergeordneten Sites und mit anderen übergeordneten Sites aus. Eine untergeordnete Website kommuniziert jedoch nur mit ihrer übergeordneten Website.

Die folgende Abbildung zeigt den Workflow, der an einer GSLB-Topologiekonfiguration für übergeordnete und untergeordnete Elemente beteiligt ist.



Bevor Sie mit der Konfiguration der übergeordneten und untergeordneten Topologiebereitstellung beginnen, stellen Sie sicher, dass Sie für jede Serverfarm oder jedes Rechenzentrum eine standardmäßige Lastausgleichseinrichtung konfiguriert haben.

Für die Synchronisierung der GSLB-Konfiguration über die GSLB-Sites in der Bereitstellung stellen Sie außerdem Folgendes sicher:

- Lokale GLSB-Sites werden auf allen Appliances in der GSLB-Konfiguration konfiguriert.
- Sie haben den Verwaltungszugriff auf alle GSLB-Sites in der Konfiguration aktiviert.
- Sie haben die Firewall so konfiguriert, dass sie die automatische Synchronisierung und MEP-Verbindungen akzeptiert.
- Alle Citrix ADC Appliances, die an Sites teilnehmen, sollten dieselbe Citrix ADC -Softwareversion aufweisen (die Sites befinden sich nicht in einer Master-Slave-Beziehung).
- Das RPC-Knotenkennwort ist für alle GSLB-Sites in der GSLB-Konfiguration identisch.

So konfigurieren Sie eine übergeordnete und untergeordnete Bereitstellung mit dem Assistenten

Gehen Sie auf der Registerkarte Konfiguration folgendermaßen vor:

1. Navigieren Sie zu **Traffic Management** > **GSLB**, und klicken Sie dann auf **Erste Schritte**.

2. Wenn Sie keinen ADNS-Server oder einen virtuellen DNS-Server für die Site konfiguriert haben, können Sie dies jetzt tun.
   a) Klicken Sie auf **Ansicht** und dann auf **Hinzufügen**.
   b) Geben Sie den Dienstnamen und die IP-Adresse ein und wählen Sie das Protokoll (ADNS/ADNS_TCP) aus, über das die Daten mit dem Dienst ausgetauscht werden.
3. Wählen Sie **Übergeordnete und untergeordnete Topologie**aus.
4. Wählen Sie im Feld Standorttyp auswählen die Option;
   - **Übergeordnetes Element** — Beim Konfigurieren des übergeordneten Standorts müssen Sie die zugehörigen untergeordneten Sites konfigurieren und auch die anderen übergeordneten Sites im GSLB-Setup konfigurieren.
   - **Untergeordnetes Element** — Beim Konfigurieren des untergeordneten Standorts müssen Sie nur den untergeordneten Standort und den übergeordneten Standort konfigurieren.

So konfigurieren Sie eine übergeordnete Site

1. Geben Sie den vollqualifizierten Domänennamen ein und geben Sie den Zeitraum an, für den der Datensatz von DNS-Proxys zwischengespeichert werden muss.
2. Konfigurieren Sie die GSLB-Sites. Jede Site muss mit einer lokalen GSLB-Site konfiguriert werden, und die Konfiguration jeder Site muss alle anderen Sites als Remote-GSLB-Sites enthalten. Es kann nur eine lokale Site geben. Alle anderen Sites sind Remotesites. Wenn die angegebene Site-IP-Adresse der Appliance gehört (z. B. eine MIP-Adresse oder eine SNIP-Adresse), ist der Standort ein lokaler Standort. Andernfalls handelt es sich um eine Remotesite.
3. Geben Sie die Sitedetails ein, z. B. den Sitename und die Site-IP-Adresse.
   a) Wählen Sie den Sitetyp aus.
   b) Optional können Sie das RPC-Kennwort ändern und ggf. sichern.
   c) Wenn ein Monitor an den GSLB-Dienst gebunden werden soll, wählen Sie die Bedingung, unter der der Monitor den Dienst überwachen soll. Dies wird erst wirksam, wenn ein Monitor an die Dienste gebunden ist. Mögliche Bedingungen sind:
      - **Always**. Überwachen Sie den GSLB-Dienst jederzeit.
      - **MEP Fails**. Überwachen Sie den GSLB-Dienst nur, wenn der Austausch von Metriken über MEP fehlschlägt.
      - **MEP Fails and Service is DOWN**. Der Austausch von Metriken über MEP ist aktiviert, aber der Status des Dienstes, der durch den Metrikaustausch aktualisiert wird, ist DOWN.
4. Konfigurieren Sie die GSLB-Dienste.
   a) Geben Sie die Service-Details wie Dienstname, Diensttyp und Portnummer ein.
   b) Ordnen Sie den Dienst einem Standort (lokal oder remote) zu, indem Sie den GSLB-Site auswählen, zu dem der GSLB-Dienst gehört.
   c) Wählen Sie den Monitor aus, der bei einem Ausfall des MEP an den Dienst gebunden werden muss. Der Dienst kann ein vorhandener Server sein, oder Sie können einen neuen

Server oder einen virtuellen Server erstellen.

- Um einen vorhandenen Server zuzuordnen, wählen Sie den Servernamen aus. Die Dienst-IP-Adresse wird automatisch ausgefüllt.
- Um einen neuen Server zuzuordnen, erstellen Sie einen Server, indem Sie die IP-Details des Servers, die öffentliche IP-Adresse und die öffentliche Portnummer eingeben.
- Um einen virtuellen Server zuzuordnen, wählen Sie einen bereits vorhandenen virtuellen Server aus, oder klicken Sie auf **+**, und fügen Sie einen neuen virtuellen Server hinzu. Dieser vserver ist der Lastenausgleich vserver, dem dieser GSLB-Dienst zugeordnet wird. Wenn sich die öffentliche IP-Adresse von der Server-IP-Adresse unterscheidet, die in einer NAT-Umgebung auftreten kann, geben Sie die öffentliche IP-Adresse und die öffentliche Portnummer ein.

5. Konfigurieren Sie die virtuellen GSLB-Server.
   a) Geben Sie den Namen des virtuellen GSLB-Servers ein, und wählen Sie den DNS-Eintragstyp aus.
   b) Klicken Sie im Feld **Dienst auswählen** auf **>**, und wählen Sie die GSLB-Dienste aus, die an den virtuellen GSLB-Server gebunden werden sollen.
   c) Klicken Sie im Feld **Domänenbindung** auf **>**, um den Domänennamen anzuzeigen, der an den virtuellen GSLB-Server gebunden ist.
   d) Wählen Sie die GSLB-Methode zur Auswahl des leistungsstärksten GSLB-Dienstes. Die Standardwerte für die GSLB-Methode, die Backupmethode und die dynamische Gewichtung werden standardmäßig automatisch ausgefüllt. Sie können sie bei Bedarf ändern.
      - Wenn Sie die **Algorithmus-basierte** Methode wählen, wählen Sie die primäre Methode und die Backupmethode aus, und geben Sie auch die Option für die dynamische Gewichtung an.
      - Wenn Sie die **Statische Proximity-Methode** wählen, wählen Sie die Backupmethode und die dynamische Gewichtungsmethode aus. Geben Sie außerdem den Speicherort der Datenbankdatei an, indem Sie auf das Symbol klicken oder einen neuen Speicherort hinzufügen, indem Sie im Feld Standortdatenbank auswählen auf **+** klicken.
      - Wenn Sie die **RTT-Methode (Dynamic Proximity)** wählen, wählen Sie die Backupmethode aus, und geben Sie das Dienstgewicht und den RTT-Wert an, basierend auf dem der leistungsstärkste Dienst ausgewählt werden soll.
6. Klicken Sie auf **Fertig**, wenn die Konfiguration abgeschlossen ist. Das GSLB-Dashboard wird angezeigt.
7. Wenn Sie die GSLB-Eltern-Site-Konfiguration geändert haben, klicken Sie auf **GSLB automatisch synchronisieren**, um die Konfiguration mit den anderen übergeordneten Sites im GSLB-Setup zu synchronisieren. In einer übergeordneten und untergeordneten Topologie wird die

Synchronisierung für die untergeordneten Sites übersprungen.

- Stellen Sie vor der Synchronisierung sicher, dass die Konfiguration des lokalen Standorts Informationen zu den Remotesites enthält.
- Wenn die Echtzeitsynchronisierung aktiviert ist, müssen Sie nicht auf **GSLB automatisch synchronisieren** klicken. Die Synchronisation erfolgt automatisch. Gehen Sie folgendermaßen vor, um die Echtzeitsynchronisierung zu aktivieren:
  a) Navigieren Sie zu **Traffic Management** > **GSLB** > **Dashboard** und klicken Sie auf **GSLB-Einstellungen ändern**.
  b) Aktivieren Sie das Kontrollkästchen **Automatische Synchronisierung der Konfiguration**.

8. Klicken Sie auf **GSLB-Setup testen**, um sicherzustellen, dass die ADNS-Dienste oder DNS-Server mit der richtigen IP-Adresse für den Domänennamen reagieren, der im GSLB-Setup konfiguriert ist.

So konfigurieren Sie eine untergeordnete Site

1. Konfigurieren Sie die GSLB-Sites.
   a) Geben Sie die Sitedetails ein, z. B. den Sitename und die Site-IP-Adresse.
   b) Wählen Sie den Sitetyp aus.
   c) Optional können Sie das RPC-Kennwort ändern und ggf. sichern. 4. Wenn ein Monitor an den GSLB-Dienst gebunden ist, wählen Sie die Bedingung, unter der der Monitor den Dienst überwachen soll. Mögliche Bedingungen sind:
      - **Always**. Überwachen Sie den GSLB-Dienst jederzeit.
      - **MEP Fails**. Überwachen Sie den GSLB-Dienst nur, wenn der Austausch von Metriken über MEP fehlschlägt.
      - **MEP Fails and Service is DOWN**. Der Austausch von Metriken über MEP ist aktiviert, aber der Status des Dienstes, der durch den Metrikaustausch aktualisiert wird, ist DOWN.
2. Klicken Sie auf **Fertig**, wenn die Konfiguration abgeschlossen ist. Das GSLB-Dashboard wird angezeigt.
3. Klicken Sie auf **GSLB-Setup testen**, um sicherzustellen, dass die ADNS-Dienste oder DNS-Server mit der richtigen IP-Adresse für den Domänennamen reagieren, der im GSLB-Setup konfiguriert ist.

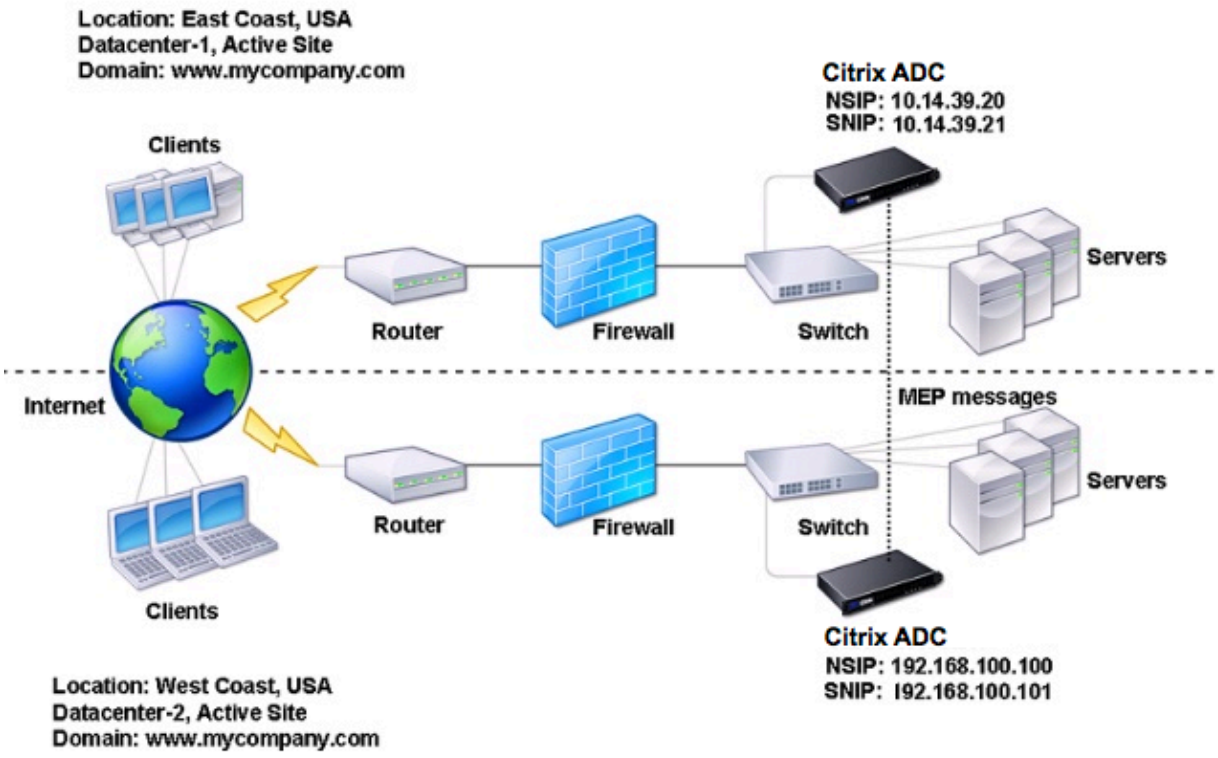
GSLB-Entitäten einzeln konfigurieren

October 5, 2021

Der globale Server-Lastausgleich wird verwendet, um den Datenverkehr zu einer Website zu verwal-

ten, die auf zwei separaten Serverfarmen gehostet wird, die sich idealerweise an unterschiedlichen geografischen Sites befinden. Betrachten Sie beispielsweise eine Website, www.mycompany.com, die auf zwei geografisch getrennten Serverfarmen oder Rechenzentren gehostet wird. Beide Serverfarmen verwenden Citrix ADC Appliances. Die Citrix ADC Appliances in diesen Serverfarmen werden im Einarmmodus eingerichtet und fungieren als autorisierende DNS-Server für die Domäne www.mycompany.com. Die folgende Abbildung veranschaulicht diese Konfiguration.

Abbildung 1. Grundlegende GSLB-Topologie



Um ein solches GSLB-Setup zu konfigurieren, müssen Sie zunächst für jede Serverfarm oder jedes Rechenzentrum ein Standard-Setup für den Lastausgleich konfigurieren. Auf diese Weise können Sie die Last auf den verschiedenen Servern in jeder Serverfarm ausgleichen. Konfigurieren Sie dann beide Citrix ADC Appliances als autoritative DNS-Server (ADNS). Erstellen Sie als Nächstes eine GSLB-Site für jede Serverfarm, konfigurieren Sie virtuelle GSLB-Server für jeden Standort, erstellen Sie GLSB-Dienste und binden Sie die GSLB-Dienste an die virtuellen GSLB-Server. Schließlich binden Sie die Domäne an die virtuellen GSLB-Server. Die GSLB-Konfigurationen auf den beiden Appliances an den beiden verschiedenen Sites sind identisch, obwohl die Lastausgleichs-Konfigurationen für jeden Standort spezifisch für diesen Standort sind.

Hinweis: Informationen zum Konfigurieren einer GSLB-Site in einem Citrix ADC Cluster-Setup finden Sie unter Einrichten von GSLB in einem Cluster.

Konfigurieren eines Standard-Lastausgleichs

Ein virtueller Lastausgleichsserver gleicht die Last auf verschiedene physische Server im Rechenzentrum aus. Diese Server werden als Dienste auf der Citrix ADC Appliance dargestellt, und die Dienste sind an den virtuellen Lastausgleichsserver gebunden.

Weitere Informationen zum Konfigurieren eines grundlegenden Load Balancing-Setups finden Sie unter Load Balancing.

Konfigurieren eines autorisierenden DNS-Dienstes

October 5, 2021

Wenn Sie die Citrix ADC Appliance als autorisierenden DNS-Server konfigurieren, akzeptiert sie DNS-Anforderungen vom Client und antwortet mit der IP-Adresse des Rechenzentrums, an das der Client Anforderungen senden soll.

Hinweis: Damit die Citrix ADC Appliance autorisierend ist, müssen Sie auch SOA- und NS-Datensätze erstellen. Weitere Informationen zu SOA- und NS-Datensätzen finden Sie unter Domänennamensystem.

So erstellen Sie einen ADNS-Dienst mit der Befehlszeilenschnittstelle

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

```
add service <name> <IP>@ ADNS <port>

show service <name>
<!--NeedCopy-->
```

Beispiel:

```
add service Service-ADNS-1 10.14.39.21 ADNS 53

show service Service-ADNS-1
<!--NeedCopy-->
```


So ändern Sie einen ADNS-Dienst mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set service <name> <IPAddress> ADNS <port>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-ADNS-1 10.14.39.21 ADNS 53
<!--NeedCopy-->
```

So entfernen Sie einen ADNS-Dienst mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
rm service <name>
<!--NeedCopy-->
```

Beispiel:

```
rm service Service-ADNS-1
<!--NeedCopy-->
```

So konfigurieren Sie einen ADNS-Dienst mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienste**.
2. Fügen Sie einen neuen ADNS-Dienst hinzu, oder wählen Sie einen vorhandenen Dienst aus, und bearbeiten Sie dessen Einstellungen.

Konfigurieren einer grundlegenden GSLB-Site

October 5, 2021

Eine GSLB-Site ist eine Darstellung eines Rechenzentrums in Ihrem Netzwerk und ist eine logische Gruppierung virtueller GSLB-Server, Dienste und anderer Netzwerkeinheiten. In der Regel gibt es in

einem GSLB eingerichtet viele GSLB-Sites, die dazu ausgestattet sind, denselben Inhalt an einen Client bereitzustellen. Diese sind in der Regel geografisch getrennt, um sicherzustellen, dass die Domain aktiv ist, auch wenn ein Standort vollständig ausfällt. Alle Sites in der GSLB-Konfiguration müssen auf jeder Citrix ADC Appliance konfiguriert werden, die einen GSLB-Site hostet. Mit anderen Worten, an jedem Standort konfigurieren Sie den lokalen GSLB-Site und jede entfernte GSLB-Site.

Sobald GSLB-Sites für eine Domäne erstellt wurden, sendet die Citrix ADC Appliance Clientanforderungen an den entsprechenden GSLB-Site, wie durch die konfigurierten GSLB-Algorithmen festgelegt.

So erstellen Sie eine GSLB-Site mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine GSLB-Site zu erstellen und die Konfiguration zu überprüfen:

```
add gslb site <siteName> <siteIPAddress>
show gslb site <siteName>
<!--NeedCopy-->
```

Beispiel:

```
add gslb site Site-GSLB-East-Coast 10.14.39.21
show glsb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

So ändern oder entfernen Sie eine GSLB-Site mit der Befehlszeilenschnittstelle

- Um eine GSLB-Site zu ändern, verwenden Sie den Befehl set gslb site, der genauso wie mit dem Befehl add gslb site entspricht, mit der Ausnahme, dass Sie den Namen einer vorhandenen GSLB-Site eingeben.
- Um die Einstellung eines Siteparameters aufzuheben, verwenden Sie den Befehl unset gslb site, gefolgt von dem Wert siteName und dem Namen des Parameters, der auf den Standardwert zurückgesetzt werden soll.
- Um eine GSLB-Site zu entfernen, verwenden Sie den Befehl rm gslb site, der nur das<name> Argument akzeptiert.

So konfigurieren Sie eine grundlegende GSLB-Site mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Sites**.

2. Fügen Sie eine neue GSLB-Site hinzu, oder wählen Sie eine vorhandene GSLB-Site aus und bearbeiten Sie deren Einstellungen.

So zeigen Sie die Statistiken einer GSLB-Site mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat gslb site <siteName>
<!--NeedCopy-->
```

Beispiel:

```
stat gslb site Site-GSLB-East-Coast
<!--NeedCopy-->
```

So zeigen Sie die Statistiken einer GSLB-Site mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Sites**.
2. Wählen Sie die GSLB-Site aus, und klicken Sie auf **Statistiken**.

Konfigurieren eines GSLB-Dienstes

October 5, 2021

Ein GSLB-Dienst ist eine Darstellung eines virtuellen Lastausgleichs- oder Content Switching-Servers. Ein lokaler GSLB-Dienst stellt einen lokalen Lastenausgleich oder einen virtuellen Content Switching-Server dar. Ein Remote-GSLB-Dienst stellt einen Lastenausgleich oder einen virtuellen Content Switching-Server dar, der an einem der anderen Sites im GSLB-Setup konfiguriert ist. An jedem Standort im GSLB-Setup können Sie einen lokalen GSLB-Dienst und eine beliebige Anzahl von GSLB-Remote-Diensten erstellen.

> **Wichtig**:
>
> Wenn sich der virtuelle Lastausgleichsserver entweder in einem GSLB-Knoten selbst befindet oder sich in einem untergeordneten Knoten (in der Eltern-Kind-Bereitstellung) befindet und keine Monitore an den GSLB-Dienst gebunden sind, stellen Sie sicher, dass Folgendes:

> Die IP-Adresse des GLSB-Dienstes, die Portnummer und das Protokoll übereinstimmen der virtuelle Server, den der Dienst darstellt. Andernfalls wird der Dienststatus als DOWN markiert.

So erstellen Sie einen GSLB-Dienst mit der Befehlszeilenschnittstelle

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

```
add gslb service <serviceName> <serverName | IP> <serviceType> <port>-
   siteName <string>
show gslb service <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
add gslb service Service-GSLB-1 10.14.39.14 HTTP 80  - siteName Site-
   GSLB-East-Coast
show gslb service Service-GSLB-1
<!--NeedCopy-->
```

So ändern oder entfernen Sie einen GSLB-Dienst mit der Befehlszeilenschnittstelle

- Um einen GSLB-Dienst zu ändern, verwenden Sie den<serviceName> Befehl set gslb service. Geben Sie für diesen Befehl den Namen des GSLB-Dienstes an, dessen Konfiguration Sie ändern möchten. Sie können die vorhandenen Werte der von Ihnen angegebenen Parameter ändern oder standardmäßig festlegen. Sie können den Wert von mehr als einem Parameter im selben Befehl ändern. Weitere Informationen zu den Parametern finden Sie im Befehl add gslb service. Beispiel

```
> set gslb service SKP_GSLB_NOTCNAME_SVC2 -maxBandWidth 25 -
   maxClient 8
Done
> sh gslb service SKP_GSLB_NOTCNAME_SVC2
SKP_GSLB_NOTCNAME_SVC2 (21.211.21.21: 80)- HTTP
...
Max Conn: 8  Max Bandwidth: 25 kbits
<!--NeedCopy-->
```


- Um einen Parameter auf seinen Standardwert zurückzusetzen, können Sie den<serviceName> Befehl unset gslb service und die zu löschenden Parameter verwenden. Beispiel

```
> unset gslb service SKP_GSLB_NOTCNAME_SVC2 maxBandWidth
Done
> sh gslb service SKP_GSLB_NOTCNAME_SVC2
SKP_GSLB_NOTCNAME_SVC2 (21.211.21.21: 80)- HTTP
...
Max Conn: 8  Max Bandwidth: 0 kbits
<!--NeedCopy-->
```

- Um einen GSLB-Dienst zu entfernen, verwenden Sie den<serviceName> Befehl rm gslb service.

So erstellen Sie einen GSLB-Dienst mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Services**.
2. Fügen Sie einen neuen GSLB-Dienst hinzu, oder wählen Sie einen vorhandenen Dienst aus und bearbeiten Sie dessen Einstellungen.

So zeigen Sie die Statistiken eines GSLB-Diensts mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat gslb service <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
stat gslb service Service-GSLB-1
<!--NeedCopy-->
```

So zeigen Sie die Statistiken eines GSLB-Diensts mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Services**.
2. Wählen Sie den GSLB-Dienst aus, und klicken Sie auf **Statistiken**.

Konfigurieren einer GSLB-Dienstgruppe

February 24, 2022

Mit der Dienstgruppe können Sie eine Gruppe von Diensten so einfach wie einen einzigen Dienst verwalten. Wenn Sie beispielsweise eine Option wie Komprimierung, Zustandsüberwachung oder ordnungsgemäßes Herunterfahren für eine Dienstgruppe aktivieren oder deaktivieren, wird die Option für alle Mitglieder der Dienstgruppe aktiviert oder deaktiviert.

Nachdem Sie eine Dienstgruppe erstellt haben, können Sie sie an einen virtuellen Server binden und der Gruppe Dienste hinzufügen. Sie können auch Monitore an die Dienstgruppen binden.

> **Wichtig**
>
> Wenn sich der virtuelle Lastausgleichsserver entweder in einem GSLB-Knoten selbst oder in einem untergeordneten Knoten (in der Eltern-Kind-Bereitstellung) befindet und keine Monitore an den GSLB Service gebunden sind, stellen Sie Folgendes sicher: IP-Adresse, Portnummer und Protokoll
>
> der GLSB-Dienstgruppe stimmen mit den virtuellen überein Server, den der Dienst repräsentiert. Ansonsten ist der Dienstzustand als DOWN gekennzeichnet.

Der Citrix ADC unterstützt die folgenden Typen von GSLB-Dienstgruppen.

- IP-Adressbasierte Dienstgruppen
- Auf Domainnamen basierende Dienstgruppen
- Auf Domainnamen basierende Autoscale-Dienstgruppen

GSLB Domainnamen basierte Autoscale-Dienstgruppen

Die Citrix ADC Hybrid- und Multi-Cloud Global Server Load Balancing (GSLB) -Lösung ermöglicht es Kunden, den Anwendungsverkehr auf mehrere Rechenzentren in Hybrid Clouds, mehreren Clouds und on-premises zu verteilen. Die Citrix ADC GSLB-Lösung unterstützt verschiedene Load Balancing-Lösungen wie den Citrix ADC Load Balancer, Elastic Load Balancing (ELB) für AWS und andere Load Balancer von Drittanbietern. Darüber hinaus führt die GSLB-Lösung einen globalen Lastausgleich durch, auch wenn die GSLB- und Load-Balancing-Schichten unabhängig verwaltet werden.

In Cloud-Bereitstellungen erhalten Benutzer einen Domänennamen als Referenz, wenn sie zu Verwaltungszwecken auf die Load Balancing-Lösung zugreifen. Es wird empfohlen, dass externe Entitäten nicht die IP-Adressen verwenden, in die diese Domainnamen auflösen. Außerdem werden die Load-Balancing-Schichten basierend auf der Last nach oben oder unten skaliert, und es wird nicht garantiert, dass die IP-Adressen statisch sind. Daher wird empfohlen, den Domänennamen anstelle von IP-Adressen zu verwenden, um auf die Endpunkte des Lastenausgleichs zu verweisen. Dies erfordert, dass die GSLB-Dienste unter Verwendung des Domainnamens anstelle von IP-Adressen

referenziert werden, und es muss alle IP-Adressen verbrauchen, die für den Domänennamen der Lastausgleichsschicht zurückgegeben werden, und eine Repräsentation dafür in GSLB haben.

Um Domänennamen anstelle von IP-Adressen zu verwenden, wenn Sie auf die Lastausgleichs-Endpunkte verweisen, können Sie die auf Domänennamen basierenden Dienstgruppen für GSLB verwenden.

Überwachen Sie auf GSLB-Domänennamen

Die Citrix ADC Appliance verfügt über zwei integrierte Monitore, die TCP-basierte Anwendungen überwachen: TCP-Standard und Ping-Standard. Der TCP-Standardmonitor ist an alle TCP-Dienste gebunden und der Ping-Standardmonitor ist an alle Nicht-TCP-Dienste gebunden. Die eingebauten Monitore sind standardmäßig an die GSLB-Dienstgruppen gebunden. Es wird jedoch empfohlen, einen anwendungsspezifischen Monitor an die GSLB-Dienstgruppen zu binden.

Empfehlung für die Einstellung der Trigger-Monitor-Option auf MEPDOWN

Die Option Trigger-Monitore kann verwendet werden, um anzugeben, ob die GSLB-Site die Monitore immer verwenden muss, oder Monitore verwenden, wenn das Metrik-Austauschprotokoll (MEP) DOWN ist.

Die Option Monitore auslösen ist standardmäßig auf IMMER eingestellt.

Wenn die Option Monitore auslösen auf IMMER gesetzt ist, löst jeder GSLB-Knoten die Monitore unabhängig voneinander aus. Wenn jeder GSLB-Knoten die Monitore unabhängig auslöst, arbeitet jeder GSLB-Knoten möglicherweise mit einem anderen Satz von GSLB-Diensten. Dies kann zu Abweichungen bei den DNS-Antworten für die DNS-Anforderungen führen, die auf diesen GSLB-Knoten landen. Wenn jeder GSLB-Knoten unabhängig überwacht, erhöht sich außerdem die Anzahl der Monitor-Prüfpunkte, die die Load Balancer-Einheit erreichen. Die Persistenzeinträge werden auch über die GSLB-Knoten hinweg inkompatibel.

Daher wird empfohlen, dass die Option Monitore auslösen in der GSLB-Standorteinheit auf MEPDOWN festgelegt ist. Wenn die Option Monitore auslösen auf MEPDOWN festgelegt ist, liegt die Domänenauflösung und die Überwachung des Lastausgleichs beim lokalen GSLB-Knoten. Wenn die Option Monitore auslösen auf MEPDOWN gesetzt ist, erfolgt die Load-Balancing-Domänenauflösung und die anschließende Überwachung durch den lokalen GSLB-Knoten einer GSLB-Dienstgruppe. Die Ergebnisse werden dann mithilfe des Metrik-Austauschprotokolls (MEP) an alle anderen an GSLB teilnehmenden Knoten weitergegeben.

Wenn der Satz von IP-Adressen, die einer Load Balancing-Domäne zugeordnet sind, aktualisiert wird, wird er außerdem über MEP benachrichtigt.

Einschränkungen von GSLB-Dienstgruppen

- Bei einer Load Balancing-Domäne ist die IP-Adresse, die in der DNS-Antwort zurückgegeben wird, im Allgemeinen die öffentliche IP-Adresse. Die private IP-Adresse kann nicht dynamisch angewendet werden, wenn die Load-Balancing-Domäne aufgelöst wird. Daher sind der öffentliche IP-Port und der private IP-Port für die IP-Portbindungen der GSLB-Domänennamen, die auf Autoscale-Dienstgruppen basieren, identisch. Diese Parameter können nicht explizit für die auf Domänennamen basierenden Autoscale-Dienstgruppen festgelegt werden.
- Sitepersistenz, DNS-Ansichten und Clustering werden für GSLB-Dienstgruppen nicht unterstützt.

Konfigurieren und Verwalten von GSLB-Dienstgruppen mithilfe der CLI

So fügen Sie eine GSLB-Dienstgruppe hinzu:

```
1 add gslb serviceGroup <serviceGroupName>@ <serviceType> [-autoScale (
     DISABLED | DNS )] -siteName <string>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add gslb serviceGroup Service-Group-1 http -siteName Site1 -autoScale
     DNS
2 <!--NeedCopy-->
```

So binden Sie eine GSLB-Dienstgruppe an einen virtuellen Server

```
1 bind gslb serviceGroup <serviceGroupName> ((<IP>@ <port>) | <serverName
     >@ | (-monitorName <string>@))
2 <!--NeedCopy-->
```

Beispiel:

```
1 bind gslb serviceGroup Service-Group-1 203.0.113.2
2 bind gslb serviceGroup Service-Group-1 S1 80
3 bind gslb serviceGroup Service-Group-1 -monitorName Mon1
4 <!--NeedCopy-->
```


So trennen Sie die Bindung einer GSLB-Dienstgruppe an einen virtuellen Server:

```
unbind gslb serviceGroup <serviceGroupName> ((<IP>@ <port>) | <
    serverName>@ | -monitorName <string>@)
<!--NeedCopy-->
```

Beispiel:

```
unbind gslb serviceGroup Service-Group-1 -monitorName Mon1
<!--NeedCopy-->
```

So legen Sie Parameter für eine GSLB-Dienstgruppe fest:

```
set gslb serviceGroup <serviceGroupName>@ [(<serverName>@ <port> [-
    weight <positive_integer>] [-hashId <positive_integer>] [-publicIP <
    ip_addr|ipv6_addr|*>] [-publicPort <port>]) | -maxClient <
    positive_integer> | -cip ( ENABLED | DISABLED ) | <cipHeader> | -
    cltTimeout <secs> | -svrTimeout <secs> | -maxBandwidth <
    positive_integer> | -monThreshold <positive_integer> | -
    downStateFlush ( ENABLED | DISABLED )] [-monitorName <string> -
    weight <positive_integer>] [-healthMonitor ( YES | NO )] [-comment <
    string>] [-appflowLog ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

So heben Sie die Einstellung von Parametern aus einer GSLB-Dienstgruppe auf:

```
unset gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port> [-
    weight] [-hashId] [-publicIP] [-publicPort]] [-maxClient] [-cip] [-
    cltTimeout] [-svrTimeout] [-maxBandwidth] [-monThreshold] [-
    appflowLog] [-monitorName] [-weight] [-healthMonitor] [-cipHeader]
    [-downStateFlush] [-comment]
<!--NeedCopy-->
```

So aktivieren Sie eine GSLB-Dienstgruppe:

```
enable gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port>]
<!--NeedCopy-->
```


Beispiel:

```
enable gslb serviceGroup SG1 S1 80
<!--NeedCopy-->
```

So deaktivieren Sie eine GSLB-Dienstgruppe:

```
disable gslb serviceGroup <serviceGroupName>@ [<serverName>@ <port>] [-
    delay <secs>] [-graceFul ( YES /| NO )]
<!--NeedCopy-->
```

Beispiel:

```
disable gslb serviceGroup SRG2 S1 80
<!--NeedCopy-->
```

> **Hinweis**:
>
> Die zu deaktivierende Dienstgruppe muss eine DBS-Dienstgruppe und keine Autoscale-Dienstgruppe sein.

So entfernen Sie eine GSLB-Dienstgruppe:

```
rm gslb serviceGroup <serviceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
rm gslb serviceGroup Service-Group-1
<!--NeedCopy-->
```

So zeigen Sie die Statistiken einer GSLB-Dienstgruppe an:

```
stat gslb serviceGroup [<serviceGroupName>]
<!--NeedCopy-->
```


Beispiel:

```
stat gslb serviceGroup Service-Group-1
<!--NeedCopy-->
```

So zeigen Sie die Eigenschaften einer GSLB-Dienstgruppe an:

```
show gslb serviceGroup [<serviceGroupName>  -includeMembers]
<!--NeedCopy-->
```

Beispiel:

```
show gslb serviceGroup SG1
show gslb serviceGroup -includeMembers
<!--NeedCopy-->
```

Änderungen an den vorhandenen GSLB CLI-Befehlen

Die folgenden Änderungen werden an den vorhandenen GSLB-Befehlen nach der Einführung der GSLB-Dienstgruppen vorgenommen:

- `bind gslb vserver` - Der Name der Dienstgruppe wird zum Befehl bind hinzugefügt.

  Beispiel:

  ```
  bind gslb vserver <name> ((-serviceName <string> [-weight <
     positive_integer>] ) | <serviceGroupName>@ | | (-domainName <
     string> [-TTL <secs>] [-backupIP<ip_addr|ipv6_addr|*>] [-
     cookieDomain <string>] [-cookieTimeout <mins>][-sitedomainTTL
     <secs>]) | (-policyName <string>@ [-priority<positive_integer
     >] [-gotoPriorityExpression <expression>] [-type REQUEST |
     RESPONSE )]))
  <!--NeedCopy-->
  ```

- `unbind gslb vserver` - Die Dienstgruppe wurde zum Befehl unbind hinzugefügt.

  Beispiel:


```
unbind gslb vserver <name> (-serviceName <string> <
    serviceGroupName> @ /(-domainName <string> [-backupIP] [-
    cookieDomain]) | -policyName <string>@)
<!--NeedCopy-->
```

- `show gslb site` - Wenn dieser Befehl ausgeführt wird, werden auch die GSLB-Dienstgruppen angezeigt.
- `show gslb vs` - Wenn dieser Befehl ausgeführt wird, werden die GSLB-Dienstgruppen angezeigt.
- `stat gslb vs` - Wenn dieser Befehl ausgeführt wird, werden auch die Statistiken der GSLB-Dienstgruppen angezeigt.
- `show lb monitor bindings` - Wenn dieser Befehl ausgeführt wird, werden auch die GSLB-Dienstgruppenbindungen angezeigt.

Konfigurieren von GSLB-Dienstgruppen mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Dienstgruppen**.
2. Erstellen Sie eine Dienstgruppe und setzen Sie den AutoScale-Modus auf DNS.

Konfigurieren der Sitepersistenz für die GSLB-Dienstgruppen

Sie können die Sitepersistenz für die auf IP-Adressen und Domänennamen basierenden Dienstgruppen konfigurieren. Sitepersistenz wird für Domänennamen-basierte Autoscale-Dienstgruppen nicht unterstützt.

So stellen Sie die Sitepersistenz basierend auf HTTP-Cookies mithilfe der CLI ein

- Für die Persistenz des Verbindungsproxys müssen Sie das Site-Präfix nicht festlegen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set gslb service group <serviceGroupName> [-sitePersistence <
    sitePersistence>]
<!--NeedCopy-->
```

- Für die Persistenz der HTTP-Umleitung müssen Sie zuerst das Standortpräfix für ein Mitglied der Dienstgruppe festlegen und dann den HTTPRedirect-Persistenzparameter für die Dienstgruppe festlegen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set gslb servicegroup <serviceGroupName>  <serviceGroup member name|Ip>
     <port>  [-sitePrefix <string>]

set gslb servicegroup <serviceGroupName> [-sitePersistence <
   sitePersistence>]
<!--NeedCopy-->
```

Beispiele:

- Persistenz des Verbindungsproxys

```
set gslbservicegroup sg1 -sitePersistence connectionProxy
<!--NeedCopy-->
```

- HTTPRedirect-Persistenz

```
set gslb servicegroup sg2 test1 80 -sitePrefix vserver-GSLB-1
<!--NeedCopy-->
```

```
set gslb servicegroup sg2 -sitePersistence HTTPRedirect
<!--NeedCopy-->
```

So legen Sie die Sitepersistenz basierend auf Cookies über die GUI fest

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Services Groups** und wählen Sie die Dienstgruppe aus, die Sie für die Sitepersistenz konfigurieren möchten (z. B. ServiceGroup-GSLB-1).
2. Klicken Sie auf den Abschnitt **Sitepersistenz** und legen Sie die Persistenz fest, die Ihren Anforderungen entspricht.

> **Tipp**
>
> Informationen zum Bereitstellungsszenario und zur Beispielkonfiguration von GSLB-Dienstgruppen finden Sie in den folgenden Themen:
>
> - Anwendungsfall: Bereitstellung einer auf Domänennamen basierenden Autoscale-Dienstgruppe

- Anwendungsfall: Bereitstellung der IP-adressbasierten Autoscale-Dienstgruppe

Konfigurieren eines virtuellen GSLB-Servers

October 5, 2021

Ein virtueller GSLB-Server ist eine Entität, die einen oder mehrere GSLB-Dienste darstellt und den Datenverkehr zwischen ihnen ausgleicht. Es wertet die konfigurierten GSLB-Methoden oder Algorithmen aus, um einen GSLB-Dienst auszuwählen, an den die Clientanforderung gesendet werden soll.

> **Hinweis:**
>
> Eine Anforderung für das virtuelle GSLB Server-Protokoll besteht hauptsächlich darin, eine Beziehung zwischen dem virtuellen Server und den Diensten zu erstellen, die an den virtuellen Server gebunden sind. Dies hält auch CLI/APIs für andere Arten von virtuellen Servern konsistent. Der Diensttyp-Parameter auf einem Dienst oder einem virtuellen Server wird beim Servieren der DNS-Anforderungen nicht verwendet. Es wird stattdessen während der Standortpersistenz, Überwachung und für die Durchführung von Lookups über MEP referenziert.

So erstellen Sie einen virtuellen GSLB-Server mit der Befehlszeilenschnittstelle

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

```
1 -  add gslb vserver <name> <serviceType> -ipType (IPv4 | IPv6)
2 -  show gslb vserver <name>
3 <!--NeedCopy-->
```

Beispiel:

```
1 add gslb vserver Vserver-GSLB-1 HTTP -ipType IPv4
2 add gslb vserver Vserver-GSLB-2 HTTP -ipType IPv6
3 show gslb vserver Vserver-GSLB-1
4 show gslb vserver Vserver-GSLB-2
5 <!--NeedCopy-->
```


So ändern oder entfernen Sie einen virtuellen GSLB-Server mit der Befehlszeilenschnittstelle

- Verwenden Sie den`set gslb vserver` Befehl, um einen virtuellen GSLB-Server zu ändern. Dieser Befehl funktioniert ähnlich dem`add gslb vserver` Befehl, mit der Ausnahme, dass Sie den Namen eines vorhandenen virtuellen GSLB-Servers eingeben.
- Um einen Parameter auf den Standardwert zurückzusetzen, können Sie den`unset gslb vserver` Befehl, gefolgt von dem Wert vServerName und dem Namen des Parameters verwenden, der aufgehoben werden soll.
- Um einen virtuellen GSLB-Server zu entfernen, verwenden Sie den`rm gslb vserver` Befehl, der nur das Argument name akzeptiert.

So konfigurieren Sie einen virtuellen GSLB-Server mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**.
2. Fügen Sie einen neuen virtuellen GSLB Server hinzu, oder wählen Sie einen vorhandenen virtuellen GSLB Server aus und bearbeiten Sie die Einstellungen.

So zeigen Sie die Statistiken eines virtuellen GSLB-Servers mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat gslb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
stat gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

So zeigen Sie die Statistiken eines virtuellen GSLB-Servers mit dem Konfigurationsdienstprogramm an

Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**, wählen Sie den virtuellen Server aus und klicken Sie auf **Statistiken** .

Statistiken des virtuellen GSLB Servers

Ab Citrix ADC Version 12.1 Build 51.xx und höher zeigt die Statistik des virtuellen GSLB Server zusätzlich zu Details wie: VServer-Treffer, aktuelle Persistenzsitzung, Anforderungsbytes, Antwortbytes,

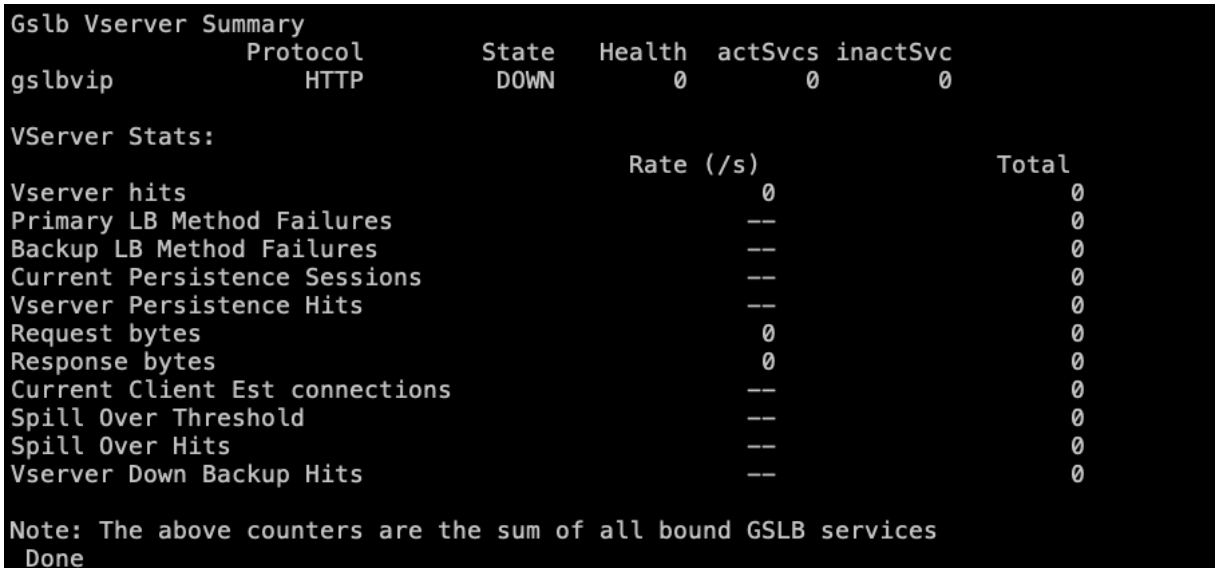
Spillover-Schwellenwert, Spillover-Treffer, aktueller Client eingerichtet Verbindungen und vserver nach unten Backup-Treffer.

- **Fehler derprimären LB-Methode**: Anzahl der Fehlschlägeder primären GSLB-Methode.
- **Backup LB-Methodenfehler**: Anzahl der Fehlschläge der GSLB-Backup-Methode.
- **Vserver-Persistenztreffer**: Gibt an, wie oft die Anforderung durch die Persistenzsitzungen bedient wird.

Die Statistiken des virtuellen GSLB-Servers zeigen auch die Statistiken der Dienstgruppenmitglieder an, die an den virtuellen Server gebunden sind.

> **Hinweis:**
> Die primäre Methode oder die Backupmethode kann fehlschlagen, wenn die primäre Methode statische Nähe ist und die Backupmethode RTT lautet. In diesem Szenario, wenn es keinen Speicherort für LDNS IP entspricht, schlägt die statische Nähe fehl und Backupmethode wird versucht. Die Statistiken werden auf folgender Grundlage aktualisiert:
>
> - Wenn die Backupmethode erfolgreich ist, werden nur Statistiken zum Ausfall der primären Methode erhöht.
> - Wenn die RTT-Berechnung nicht erfolgreich ist, schlägt auch die Backupmethode fehl. In diesem Fall werden sowohl primäre als auch die Fehlerstatistiken der Backupmethode inkrementiert.
>
> Wenn die Backupmethode fehlschlägt, wird die letzte Methode von Round Robin verwendet.

Das folgende Bild ist ein Beispiel für virtuelle GSLB-Serverstatistiken von CLI.

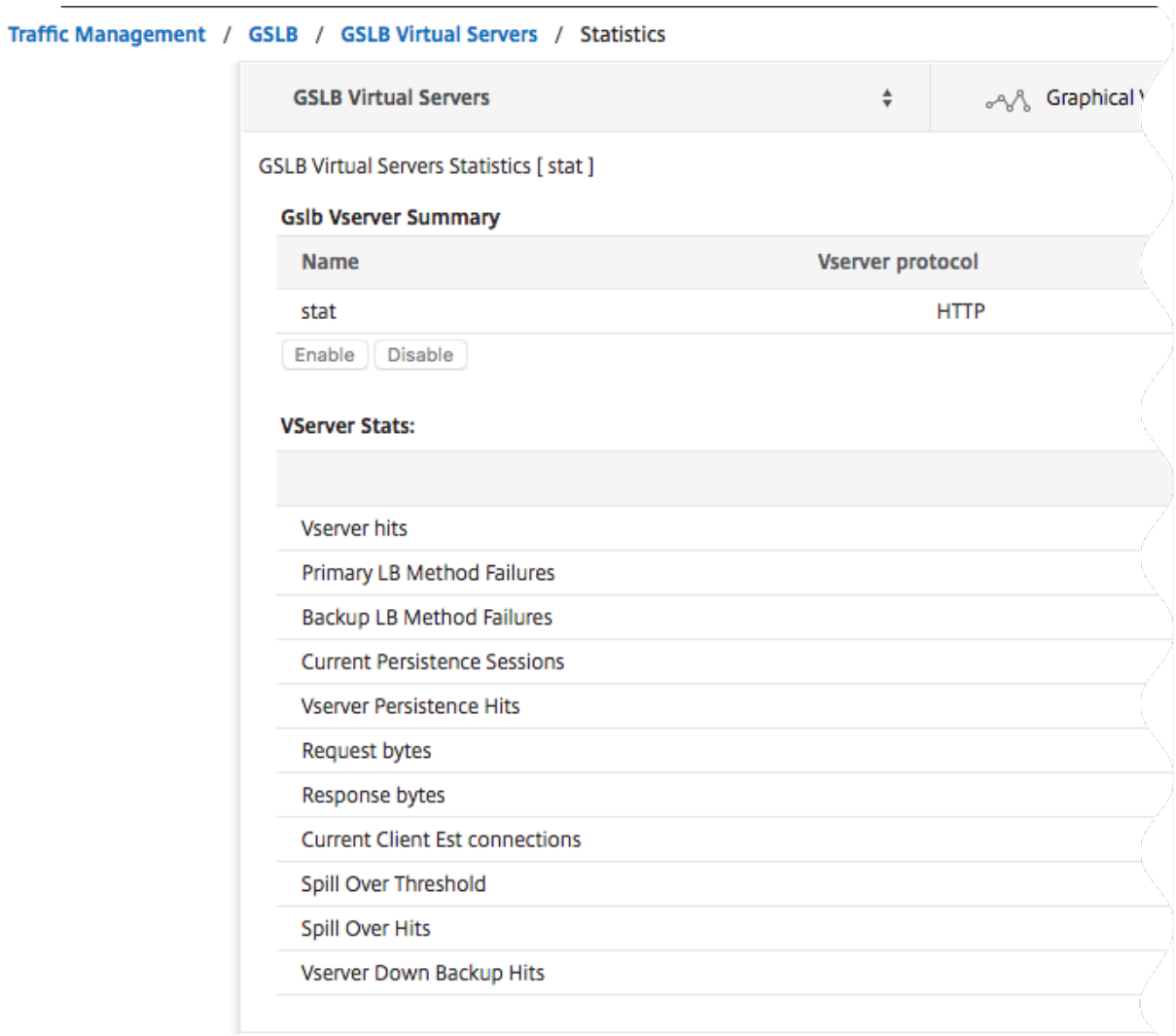


```
Gslb Vserver Summary
                Protocol        State   Health  actSvcs inactSvc
gslbvip             HTTP         DOWN        0        0        0

VServer Stats:
                                        Rate (/s)               Total
Vserver hits                                 0                      0
Primary LB Method Failures                  --                      0
Backup LB Method Failures                   --                      0
Current Persistence Sessions                --                      0
Vserver Persistence Hits                    --                      0
Request bytes                                0                      0
Response bytes                               0                      0
Current Client Est connections              --                      0
Spill Over Threshold                        --                      0
Spill Over Hits                             --                      0
Vserver Down Backup Hits                    --                      0

Note: The above counters are the sum of all bound GSLB services
 Done
```

Das folgende Bild ist ein Beispiel für virtuelle GSLB-Serverstatistiken von GUI.



GSLB-Dienststatistik

Wenn Sie den Befehl stat gslb service über die Befehlszeile ausführen oder im Konfigurationsprogramm auf den **Link Statistiken** klicken, werden die folgenden Details des Dienstes angezeigt:

- **Bytes anfordern.** Gesamtzahl der Anforderungsbytes, die auf diesem Dienst oder virtuellen Server empfangen wurden.
- **Antwortbytes.** Anzahl der Antwortbytes, die von diesem Dienst oder dem virtuellen Server empfangen werden.
- **Der aktuelle Client hat Verbindungen hergestellt.** Anzahl der Clientverbindungen mit dem Status ESTABLISHED.
- **Aktuelle Belastung des Dienstes.** Laden des Dienstes (Berechnet aus dem an den Dienst gebundenen Lastmonitor).

Die Daten der Anzahl der Anforderungen und Antworten sowie die Anzahl der aktuellen Client-

und Serververbindungen werden möglicherweise nicht angezeigt oder nicht mit den Daten des entsprechenden virtuellen Lastenausgleichsservers synchronisiert.

Löschen der virtuellen GSLB-Server- oder Dienststatistiken

Hinweis: Diese Funktion ist in NetScaler Version 10.5.e verfügbar.

Sie können nun die Statistiken eines virtuellen GSLB-Servers und -Dienstes löschen. Citrix ADC bietet die folgenden beiden Optionen zum Löschen der Statistiken:

- **Basic**: Löscht die Statistiken, die spezifisch für den virtuellen Server sind, behält jedoch die Statistiken bei, die vom gebundenen GLSB-Dienst bereitgestellt werden.
- **Vollständig**: Löscht sowohl den virtuellen Server als auch die gebundene GSLB-Dienststatistik.

So löschen Sie die Statistiken eines virtuellen GSLB-Servers mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat gslb vserver <name> -clearstats <basic | full>
<!--NeedCopy-->
```

Beispiel:

```
stat gslb vserver Vserver-GSLB-1 - clearstats basic
<!--NeedCopy-->
```

So löschen Sie die Statistiken eines GSLB-Dienstes mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat gslb service <name> -clearstats <basic | full>
<!--NeedCopy-->
```

Beispiel:

```
stat gslb service service-GSLB-1 - clearstats basic
<!--NeedCopy-->
```


So löschen Sie die Statistiken eines virtuellen GSLB-Servers mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**.
2. Wählen Sie den virtuellen GSLB-Server aus, klicken Sie auf **Statistiken**, und klicken Sie dann auf **Löschen**.
3. Wählen Sie in der Dropdownliste **Löschen** die Option **Einfach** oder **Vollständig** aus, und klicken Sie dann auf **OK**.

So löschen Sie die Statistiken eines GSLB-Diensts mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Services**.
2. Wählen Sie den GSLB-Dienst aus, klicken Sie auf **Statistiken**, und klicken Sie dann auf **Löschen**.
3. Wählen Sie in der Dropdownliste **Löschen** die Option **Einfach** oder **Vollständig** aus, und klicken Sie dann auf **OK**.

Aktivieren und Deaktivieren von virtuellen GSLB Servern

Wenn Sie einen virtuellen GSLB-Server erstellen, ist er standardmäßig aktiviert. Wenn Sie den virtuellen GSLB-Server deaktivieren, trifft die Citrix ADC Appliance beim Empfang einer DNS-Anforderung keine GSLB-Entscheidung basierend auf der konfigurierten GSLB-Methode. Stattdessen enthält die Antwort auf die DNS-Abfrage die IP-Adressen aller Dienste, die an den virtuellen Server gebunden sind.

So aktivieren oder deaktivieren Sie einen virtuellen GSLB-Server mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
enable gslb vserver <name>@

disable gslb vserver <name>@
<!--NeedCopy-->
```

Beispiel:

```
enable gslb vserver Vserver-GSLB-1
disable gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```


So aktivieren oder deaktivieren Sie einen virtuellen GSLB-Server mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**.
2. Wählen Sie einen virtuellen Server aus, und wählen Sie in der Liste **Aktion** die Option **Aktivieren** oder **Deaktivieren** aus.

Binden von GSLB-Diensten an einen virtuellen GSLB-Server

October 5, 2021

Sobald die GSLB-Dienste und der virtuelle Server konfiguriert sind, müssen relevante GSLB-Dienste an den virtuellen GSLB-Server gebunden werden, um die Konfiguration zu aktivieren.

So binden Sie einen GSLB-Dienst mit der Befehlszeilenschnittstelle an einen virtuellen GSLB-Server

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

```
bind gslb vserver <name> -serviceName <string>

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

Beispiel:

```
bind gslb vserver Vserver-GSLB-1 -serviceName Service-GSLB-1
show gslb vserver Vserver-GSLB-1
<!--NeedCopy-->
```

So heben Sie die Bindung eines GSLB-Diensts von einem virtuellen GSLB-Server mit der Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
unbind gslb vserver <name> -serviceName <string>
<!--NeedCopy-->
```

So binden Sie GSLB-Dienste mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**, und doppelklicken Sie auf einen virtuellen Server.
2. Klicken Sie in den Abschnitt **Domänen**, konfigurieren Sie eine Domäne und binden Sie die Domäne.

Binden einer Domäne an einen virtuellen GSLB-Server

October 5, 2021

Um eine Citrix ADC Appliance zum autorisierenden DNS-Server für eine Domäne zu machen, müssen Sie die Domäne an den virtuellen GSLB-Server binden. Wenn Sie eine Domäne an einen virtuellen GSLB-Server binden, fügt die Citrix ADC Appliance einen Adressdatensatz für die Domäne hinzu, der den Namen des virtuellen GSLB-Servers enthält. Die Einträge für den Start von Autorität (SOA) und Nameserver (NS) für die GSLB-Domäne müssen manuell hinzugefügt werden.

Weitere Informationen zum Konfigurieren von SOA- und NS-Datensätzen finden Sie unter Domänennamensystem.

So binden Sie eine Domäne über die Befehlszeilenschnittstelle an einen virtuellen GSLB-Server

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

```
bind gslb vserver <name> -domainName <string>
show gslb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
bind gslb vserver Vserver-GSLB-1 -domainName www.mycompany.com
show gslb vserver Vserver-GSLB-1
```



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

So heben Sie die Bindung einer GSLB-Domäne von einem virtuellen GSLB-Server mit der Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
unbind gslb vserver <name> -domainName <string>
<!--NeedCopy-->
```

So binden Sie eine Domäne mit einem virtuellen GSLB-Server mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**.
2. Wählen Sie im Bereich GSLB Virtual Servers den GSLB Virtual Server aus, an den Sie die Domäne binden möchten (z. B. vServer-GSLB-1), und klicken Sie auf Öffnen.
3. Führen Sie im Dialogfeld Virtueller GSLB Server konfigurieren auf der Registerkarte Domänen eine der folgenden Aktionen aus:
   - Klicken Sie auf **Hinzufügen**, um eine neue Domäne zu erstellen.
   - Um eine vorhandene Domäne zu ändern, wählen Sie die Domäne aus, und klicken Sie dann auf **Öffnen**.
4. Geben Sie im Dialogfeld GSLB-Domäne erstellen oder GSLB-Domäne konfigurieren Werte für die folgenden Parameter an:
   - Domänenname*—domainName (z. B. www.mycompany.com)

   * Ein erforderlicher Parameter
5. Klicken Sie auf Erstellen.
6. Klicken Sie auf OK.

So zeigen Sie die Statistiken einer Domäne mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat gslb domain <name>
<!--NeedCopy-->
```


Beispiel:

```
stat gslb domain www.mycompany.com
<!--NeedCopy-->
```

Hinweis: Um Statistiken für eine bestimmte GSLB-Domäne anzuzeigen, geben Sie den Namen der Domäne genau so ein, wie er der Citrix ADC Appliance hinzugefügt wurde. Wenn Sie den Domänennamen nicht angeben oder einen falschen Domänennamen angeben, werden Statistiken für alle konfigurierten GSLB-Domänen angezeigt.

So zeigen Sie die Statistiken einer Domäne mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**.
2. Wählen Sie im Bereich GSLB Virtual Servers den virtuellen GSLB Server (z. B. vServer-GSLB-1) aus, und klicken Sie auf Öffnen.
3. Wählen Sie im Dialogfeld GSLB Virtual Server konfigurieren auf der Registerkarte Domänen die Domäne aus, und klicken Sie dann auf **Statistik**s.

So zeigen Sie die Konfigurationsdetails der an eine GSLB-Domäne gebundenen Entitäten mithilfe der Befehlszeile an

Hinweis: Diese Funktion ist in NetScaler Version 10.5.e verfügbar.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show gslb domain <name>
<!--NeedCopy-->
```

Beispiel:

```
show gslb domain gslb1.com
        gslb1.com
        gvs1 - HTTP    state: DOWN
        DNS Record Type: A
        Configured Method: LEASTCONNECTION
        Backup Method: ROUNDROBIN
        Persistence Type: NONE
        Empty Down Response: DISABLED
        Multi IP Response: DISABLED
```



```
        Dynamic Weights: DISABLED

        gsvc1 (10.102.239.165: 80)- HTTP State: DOWN    Weight: 1
               Dynamic Weight: 0    Cumulative Weight: 1
               Effective State: DOWN
               Threshold : BELOW

               Monitor Name : http
                      State: DOWN   Weight: 1
                      Probes: 144   Failed [Total: 144 Current: 144]
                      Last response: Failure - TCP syn sent, reset
                         received.
                      Response Time: 2000 millisec

        gsvc2 (10.102.239.179: 80)- HTTP State: DOWN    Weight: 1
               Dynamic Weight: 0    Cumulative Weight: 1
               Effective State: DOWN
               Threshold : BELOW

               Monitor Name : http-ecv
                      State: DOWN   Weight: 1
                      Probes: 141   Failed [Total: 141 Current: 141]
                      Last response: Failure - TCP syn sent, reset
                         received.
                      Response Time: 2000 millisec
Done
<!--NeedCopy-->
```

So zeigen Sie die Konfigurationsdetails der an eine GSLB-Domäne gebundenen Entitäten mit dem Konfigurationsdienstprogramm an

Hinweis: Diese Funktion ist in NetScaler Version 10.5.e verfügbar.

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**, und doppelklicken Sie auf einen virtuellen Server.
2. Klicken Sie auf das Feld unterhalb des Bereichs **Domänen** .
3. Wählen Sie im Dialogfeld **GSLB-Domänenbindung für virtuelle Server** eine Domäne aus, und klicken Sie dann auf **Bindungen anzeigen** .

Beispiel für eine GSLB Einrichtung und Konfiguration

October 5, 2021

Eine Organisation verfügt über ein geografisch verteiltes Netzwerk und verfügt über drei Rechenzentren in den USA, Mexiko und Kolumbien. In der Konfiguration, die sich auf diese Sites bezieht, werden diese als US, MX und CO bezeichnet. An jedem Standort verfügt das Unternehmen über eine Serverfarm, die den gleichen Inhalt bereitstellt, und das Setup funktioniert wie erwartet. Die Citrix ADC Appliance an jedem Standort wird über einen virtuellen Server mit dem HTTP-Protokoll an Port 80 konfiguriert.

Die Organisation hat das GSLB-Setup implementiert, indem an jedem Standort eine Standort-ID hinzugefügt wurde. Die Standortbezeichnung enthält einen Standortnamen und eine IP-Adresse, die der Citrix ADC Appliance gehört und für die GSLB-Kommunikation verwendet wird.
Jeder Standort verfügt über einen Standort, der auf der Appliance lokal ist. Außerdem verfügt jeder Standort über zwei Sites, die von der lokalen Appliance entfernt sind. Auf jedem Standort wird ein virtueller GSLB-Server mit dem gleichen Namen erstellt. Dieser virtuelle Server identifiziert die Website der Organisation global und ist mit keiner IP-Adresse verbunden.
Das Setup hat auch GSLB-Dienste konfiguriert, die auf die virtuellen Lastausgleichsserver verweisen, die auf jedem GSLB-Site konfiguriert sind, indem die IP-Adresse, das Protokoll und die Portnummer des jeweiligen virtuellen Servers angegeben werden. Diese Dienste sind an den virtuellen GSLB Server gebunden.

Hinweis: Im nachfolgenden Verfahren verwenden die Befehle private IP-Adressen für die GSLB-Sites. Stellen Sie bei öffentlichen Sites und GSLB-Diensten sicher, dass Sie öffentliche IP-Adressen für diese Sites verwenden.

In der folgenden Tabelle sind die im Beispiel verwendeten IP-Adressen und Speicherorte aufgeführt:

IP-Adresse	Standort/Ortung
10.3.1.101	Site-IP des lokalen Citrix ADC.
172.16.1.101	Site-IP des Remote-Standort-MX.
192.168.1.101	Site-IP des Remote-Standort-CO.
172.16.1.100	Service-IP des Remote-Standort-MX.
10.3.1.100	Service-IP des lokalen Citrix ADC.
192.168.1.100	Service-IP des Remote-Standort-CO.

Wenn Sie eine GSLB-Site hinzufügen, wenn die Website nur über das Internet kommuniziert, dann verwenden Sie das Feld Öffentliche IP. Zum Beispiel, wenn keine Standort-zu-Standort-VPN-

Konnektivität zwischen den GSLB-Sites vorhanden ist.

So konfigurieren Sie das GSLB-Setup mit Citrix ADC Appliances mit der CLI-Befehle

1. Aktivieren Sie die GSLB-Funktion, falls dies noch nicht geschehen ist.

```
enable ns feature gslb
<!--NeedCopy-->
```

2. Identifizieren Sie eine SNIP, die zum Hinzufügen einer lokalen GSLB-Site.
3. Fügen Sie die GSLB-Site für die lokale Citrix ADC Appliance hinzu.

```
add gslb site site-US 10.3.1.101
<!--NeedCopy-->
```

4. Fügen Sie die GSLB-Sites für die Citrix ADC Remote-Appliances hinzu.

```
add gslb site site-MX 172.16.1.101
add gslb site site-CO 192.168.1.101
<!--NeedCopy-->
```

5. Fügen Sie den virtuellen GSLB-Server hinzu, der auf einen Dienst verweist, der im GSLB-Setup verwendet wird:

```
add gslb vserver gslb-lb HTTP
<!--NeedCopy-->
```

6. Fügen Sie die GSLB-Dienste für jede Site hinzu, die am GSLB-Setup teilnehmen:

```
add gslb service gslb_SVC30 172.16.1.100 HTTP 80 -siteName site-MX
add gslb service gslb_SVC10 10.3.1.100 HTTP 80 -siteName site-US
add gslb service gslb_SVC20 192.168.1.100 HTTP 80 -siteName site-
   CO
<!--NeedCopy-->
```

7. Binden Sie die GSLB-Dienste an den virtuellen GSLB-Server:


```
bind gslb vserver gslb-lb -serviceName gslb_SVC10
bind gslb vserver gslb-lb -serviceName gslb_SVC20
bind gslb vserver gslb-lb -serviceName gslb_SVC30
<!--NeedCopy-->
```

8. Binden Sie die Domäne an den virtuellen GSLB-Server.

```
bind gslb vserver gslb-lb -domainName www.mycompany.com -TTL 30
<!--NeedCopy-->
```

9. Fügen Sie einen ADNS-Dienst hinzu, der die DNS-Abfragen überwacht.

```
set service Service-ADNS-1 10.14.39.21 ADNS 53
<!--NeedCopy-->
```

Synchronisieren der Konfiguration in einem GSLB-Setup

October 5, 2021

In der Regel verfügt ein GSLB-Setup über einige Rechenzentren mit einem GSLB-Site, der für jedes Rechenzentrum konfiguriert ist. Konfigurieren Sie in jedem Citrix ADC, der an GSLB beteiligt ist, einen GSLB-Site als lokalen Standort und die anderen als Remotesites. Wenn Sie zu einem späteren Zeitpunkt einen anderen GSLB-Site hinzufügen, müssen Sie sicherstellen, dass die Konfiguration über alle GSLB-Sites hinweg identisch ist. Sie können die GSLB-Konfigurationssynchronisierungsoption des Citrix ADC verwenden, um die Konfiguration über die GSLB-Sites hinweg zu synchronisieren.

Die Citrix ADC Appliance, von der Sie die Synchronisierungsoption verwenden, wird als “Hauptsitz” und die GSLB-Sites bezeichnet, auf denen die Konfiguration als “untergeordnete Websites” kopiert wird. Wenn Sie eine GSLB-Konfiguration synchronisieren, werden die Konfigurationen auf allen GSLB-Sites, die am GSLB-Setup teilnehmen, ähnlich der Konfiguration auf der Hauptsite vorgenommen.

Die Synchronisierung erfolgt nur auf den übergeordneten Sites. Die Synchronisierung hat keinen Einfluss auf die Konfiguration der untergeordneten GSLB-Websites. Dies liegt daran, dass die übergeordnete Website und die untergeordneten Sitekonfigurationen nicht identisch sind. Die Konfiguration der untergeordneten Websites besteht nur aus den Details ihrer eigenen und ihrer übergeordneten Site. Außerdem müssen GSLB-Dienste nicht immer in den untergeordneten Sites konfiguriert werden.

- Der Hauptknoten findet die Unterschiede zwischen der Konfiguration des Hauptknotens und des untergeordneten Knotens und ändert die Konfiguration des untergeordneten Knotens, um ihn dem Hauptknoten ähnlich zu machen.

  Wenn Sie eine Synchronisation erzwingen (verwenden Sie die Option “Sync erzwingen”), löscht die Appliance die GSLB-Konfiguration aus dem untergeordneten Knoten und konfiguriert dann den Untergebenen so, dass er dem Hauptknoten ähnelt.

- Wenn während der Synchronisation ein Befehl fehlschlägt, wird die Synchronisation nicht abgebrochen, und die Fehlermeldung wird in einer **ERR-Datei** im Verzeichnis **/var/netscaler/gslb** protokolliert.

- Die Synchronisierung erfolgt nur auf den übergeordneten Sites. Die Synchronisierung hat keinen Einfluss auf die Konfiguration der untergeordneten GSLB-Websites. Dies liegt daran, dass die übergeordnete Website und die untergeordneten Sitekonfigurationen nicht identisch sind. Die Konfiguration der untergeordneten Websites besteht nur aus den Details ihrer eigenen und ihrer übergeordneten Site. Außerdem müssen GSLB-Dienste nicht immer in den untergeordneten Sites konfiguriert werden.

- Wenn Sie die interne Benutzeranmeldung deaktivieren, verwendet die GSLB Auto-Synchronisierung die SSH-Schlüssel, um die Konfiguration zu synchronisieren. Um jedoch die automatische GSLB-Synchronisierung in der Partitionsumgebung verwenden zu können, müssen Sie die interne Benutzeranmeldung aktivieren und sicherstellen, dass der Partitionsbenutzername in den lokalen und Remote-GSLB-Sites identisch ist.

> **Hinweis:**
>
> - Konfigurieren Sie auf dem RPC-Knoten des Remote-GSLB-Sites die Firewall so, dass sie Autosync-Verbindungen akzeptiert, indem Sie die Remote-Site-IP (Cluster-IP-Adresse für Cluster-Setup) und den Port (3010 für RPC und 3008 für sicheren RPC) angeben. Wenn sich die Standardroute zum Erreichen der Remote-Standorte wie in den meisten Fällen im Verwaltungssubnetz befindet, wird NSIP als Quell-IP-Adresse verwendet.
>
> Um eine andere Quell-IP-Adresse zu konfigurieren, müssen Sie die GSLB-Site-IP-Adresse und das SNIP in einem anderen Subnetz haben. Außerdem müssen Sie über ein IP-Subnetz der GSLB-Standort-IP-Adresse eine explizite Route zur IP-Adresse des Remote-Standorts definiert haben.
>
> Zur Erhöhung der Sicherheit empfiehlt Citrix, dass Sie die Kennwörter für das interne Benutzerkonto und den RPC-Knoten ändern. Das Kennwort des internen Benutzerkontos wird durch das RPC-Knotenkennwort geändert. Weitere Informationen finden Sie unter Ändern eines RPC-Knotenkennworts.

Wenn Sie die Option saveconfig verwenden, speichern die Sites, die am Synchronisierungsprozess teilnehmen, ihre Konfiguration automatisch auf folgende Weise:

Konfigurieren Sie auf dem RPC-Knoten des Remote-GSLB-Sites die Firewall so, dass sie Autosync-

Verbindungen akzeptiert, indem Sie die Remote-Site-IP (Cluster-IP-Adresse für Cluster-Setup) und den Port (3010 für RPC und 3008 für sicheren RPC) angeben. Wenn sich die Standardroute zum Erreichen der Remote-Standorte wie in den meisten Fällen in einem Verwaltungssubnetz befindet, wird NSIP als Quell-IP-Adresse verwendet.

Um eine andere Quell-IP-Adresse zu konfigurieren, müssen Sie die GSLB-Site-IP-Adresse und das SNIP in einem anderen Subnetz haben. Außerdem müssen Sie über das IP-Subnetz der GSLB-Site eine explizite Route zur IP-Adresse des Remote-Standorts definiert haben. Die Quell-IP-Adresse kann nicht über die an GSLB beteiligten Sites synchronisiert werden, da die Quell-IP-Adresse für einen RPC-Knoten für jede Citrix ADC Appliance spezifisch ist. Nachdem Sie eine Synchronisierung erzwungen haben (mit dem Befehl sync gslb config -ForceSync oder durch Auswahl der Option ForceSync in der GUI), müssen Sie die Quell-IP-Adressen auf den anderen Citrix ADC Appliances manuell ändern. Port 22 ist auch für die Synchronisierung der Datenbankdateien mit dem Remotestandort erforderlich.

Verbesserung der Zeit für die Konfigurationssynchronisierung auf allen GSLB-Sites

Konfigurieren Sie die TCP-Profileinstellungen an der Eingabeaufforderung wie folgt:

```
set tcpprofile nstcp_internal_apps -bufferSize 4194304 -sendBuffsize
    4194304 -tcpmode ENDPOINT
<!--NeedCopy-->
```

Einschränkungen der Synchronisation

- Auf der Hauptwebsite müssen die Namen der Remote-GSLB-Sites mit den Namen der Sites identisch sein, die auf den Citrix ADC Appliances konfiguriert sind, die diese Websites hosten.
- Während der Synchronisation können Verkehrsstörungen auftreten.
- Citrix ADC wird getestet, um bis zu 200.000 Zeilen der Konfiguration zu synchronisieren.
- Die Synchronisierung kann fehlschlagen:
  - Wenn die Überlaufmethode von CONNECTION in DYNAMIC CONNECTION geändert wird.
  - Wenn Sie das Standortpräfix der GSLB-Dienste austauschen, die an einen virtuellen GSLB-Server auf dem Hauptknoten gebunden sind, und versuchen Sie dann zu synchronisieren.
  - Wenn die RPC-Knotenkennwörter für NSIP- und Loopback-IP-Adresse unterschiedlich sind.
  - Wenn Sie die Synchronisierung auf GSLB-Sites durchführen, die in verschiedenen Partitionen derselben Citrix ADC Appliance konfiguriert sind.
- Wenn Sie die GSLB-Sites als Hochverfügbarkeitspaare (HA) konfiguriert haben, müssen die RPC-Knotenkennwörter von primären und sekundären Knoten identisch sein.

- Wenn Sie eine GLSB-Entität umbenennen, die Teil Ihrer GSLB-Konfiguration ist (verwenden Sie den Befehl “show gslb runningConfig”, um die GSLB-Konfiguration anzuzeigen). Sie müssen die Option Sync erzwingen verwenden, um die Konfiguration mit anderen GSLB-Sites zu synchronisieren.

> **Hinweis:**
>
> - Bei der inkrementellen Synchronisation müssen Sie die Option Sync erzwingen nicht verwenden, um die Konfiguration mit anderen GSLB-Sites zu synchronisieren. Dies gilt ab Citrix ADC Release 13.0 Build 79.x ab.

Hinweis: Um die Einschränkungen aufgrund einiger Einstellungen in der GSLB-Konfiguration zu überwinden, können Sie die Option “Synchronisierung erzwingen” verwenden. Wenn Sie jedoch die Option Sync erzwingen verwenden, werden die GSLB-Entitäten entfernt und in die Konfiguration gelesen und die GSLB-Statistiken werden auf Null zurückgesetzt. Daher wird der Datenverkehr während der Konfigurationsänderung unterbrochen.

Punkte, die vor dem Start der Synchronisierung eines GSLB-Setups zu beachten sind

Bevor Sie die Synchronisierung eines GSLB-Setups starten, stellen Sie sicher, dass:

- Auf allen GSLB-Sites einschließlich des Hauptstandorts müssen Verwaltungszugriff und SSH für die IP-Adresse der entsprechenden GSLB-Site aktiviert sein. Die IP-Adresse eines GSLB-Sites muss eine IP-Adresse sein, die der Citrix ADC Appliance gehört. Weitere Informationen zum Hinzufügen der IP-Adressen der GSLB-Site und zum Aktivieren des Verwaltungszugriffs finden Sie unter “Konfigurieren einer grundlegenden GSLB-Site”.
- Die GSLB-Konfiguration auf der Citrix ADC Appliance, die als Hauptstandort angesehen wird, ist vollständig und geeignet, um auf allen Standorten kopiert zu werden.
- Wenn Sie die GSLB-Konfiguration zum ersten Mal synchronisieren, müssen alle an GSLB teilnehmenden Websites über die GSLB-Standorteinheit ihrer jeweiligen lokalen Sites verfügen.
- Sie synchronisieren keine Sites, die nach Entwurf nicht über die gleiche Konfiguration verfügen.
- Der Hauptstandort und die untergeordneten Sites führen dieselben Citrix ADC-Versionen aus. Ab Version 12.1, Build 50.x, sucht die Appliance auf Haupt- und Unterstandorten nach der Firmware-Version, bevor die Synchronisierung initiiert wird. Wenn die Haupt- und die untergeordneten Websites verschiedene Versionen ausführen, wird die Synchronisierung für diesen Remote-Standort abgebrochen, um zu vermeiden, dass inkompatible Änderungen über die Versionen hinweg vorgenommen werden. Außerdem wird eine Fehlermeldung mit den Standortdetails angezeigt, auf denen die Synchronisation abgebrochen wurde.

  Die folgenden Abbildungen zeigen Beispielfehlermeldungen von CLI und GUI.


```
> sh gslb syncStatus -summary
Displaying the status summary of the manual GSLB configuration synchronization:

-------------------------------------------------------------------------------------------------------------
        Site Name                Status        Reason
-------------------------------------------------------------------------------------------------------------
        s2                       Failure       Error: Different netscaler release on the remote site. Local Site: 13.0, Remote Site: 12.1
        s1                       Success       All Done
        s3                       Success       All Done
Done
>
```

```
> sh gslb syncStatus -summary
Displaying the status summary of the manual GSLB configuration synchronization:

-------------------------------------------------------------------------------------------------------------
        Site Name                Status        Reason
-------------------------------------------------------------------------------------------------------------
        s2                       Failure       Error: Different netscaler release on the remote site. Local Site: 13.0, Remote Site: 12.1
        s1                       Success       All Done
        s3                       Success       All Done
Done
>
```

> **Wichtig**
>
> Die folgenden Verzeichnisse werden im Rahmen der GSLB-Konfigurationssynchronisation synchronisiert.
>
> - /var/netscaler/locdb/
> - /var/netscaler/ssl/
> - /var/netscaler/inbuilt_db/

Manuelle Synchronisation zwischen Sites, die an GSLB teilnehmen

October 5, 2021

Die manuelle Synchronisierung der GSLB-Konfiguration auf der Master Site und den Slave-Sites erfolgt auf folgende Weise:

- Die Master-Site erkennt die Unterschiede zwischen der Konfiguration ihrer eigenen Site und der Slave-Site.
- Die Master Site wendet den Unterschied in der Konfiguration auf die Slave-Site an.
- Die Master Site führt die Konfigurationssynchronisierung mit allen Slave-Sites im GSLB-Setup durch und schließt den Synchronisierungsprozess ab.

Wichtig: Nachdem eine GSLB-Konfiguration synchronisiert wurde, kann die Konfiguration auf keinem der GSLB-Sites zurückgesetzt werden. Führen Sie die Synchronisierung nur durch, wenn

Sie sicher sind, dass der Synchronisierungsprozess die Konfiguration auf der Remote-Site nicht überschreibt. Die Site-Synchronisierung ist unerwünscht, wenn die lokalen und Remote-Standorte unterschiedliche Konfigurationen nach Design haben, was zu einem Ausfall der Site führt. Wenn einige Befehle fehlschlagen und einige Befehle erfolgreich sind, werden die erfolgreichen Befehle nicht zurückgesetzt.

Punkte zu beachten

- Wenn Sie eine Synchronisierung erzwingen (verwenden Sie die Option “Synchronisierung erzwingen”), löscht die Citrix ADC Appliance die GSLB-Konfiguration von der Slave-Site. Anschließend konfiguriert die Master-Site die Slave-Site so, dass sie ihrer eigenen Site ähnelt.
- Wenn während der Synchronisation ein Befehl fehlschlägt, wird die Synchronisierung nicht abgebrochen. Die Fehlermeldungen werden in einer ERR-Datei im Verzeichnis /var/netscaler/gslb protokolliert.
- Wenn Sie die Option `saveconfig` verwenden, speichern die am Synchronisierungsprozess beteiligten Sites automatisch ihre Konfiguration wie folgt:
  - Die Master Site speichert ihre Konfiguration unmittelbar bevor sie den Synchronisierungsprozess einleitet.
  - Die Slave-Sites speichern ihre Konfiguration, nachdem der Synchronisierungsprozess abgeschlossen ist. Eine Slave-Site speichert ihre Konfiguration nur, wenn der Konfigurationsunterschied erfolgreich darauf angewendet wurde. Wenn die Synchronisierung auf einer Slave-Site fehlschlägt, müssen Sie die Ursache des Fehlers manuell untersuchen und Korrekturmaßnahmen ergreifen.

So synchronisieren Sie eine GSLB-Konfiguration mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um GSLB-Sites zu synchronisieren und die Konfiguration zu überprüfen:

```
sync gslb config [-preview | -forceSync <string> | -nowarn | -
   saveconfig] [-debug]
show gslb syncStatus
<!--NeedCopy-->
```

Beispiel:

```
sync gslb config

[WARNING]: Syncing config may cause configuration loss on other site.

```



```
5 Please confirm whether you want to sync-config (Y/N)? [N]:y
6
7 Sync Time: Dec 9 2011 10:56:9
8
9 Retrieving local site info: ok
10
11 Retrieving all participating gslb sites info: ok
12
13 Gslb_site1[Master]:
14
15 Getting Config: ok
16
17 Gslb_site2[Slave]:
18
19 Getting Config: ok
20
21 Comparing config: ok
22
23 Applying changes: ok
24
25 Done
26 <!--NeedCopy-->
```

So synchronisieren Sie eine GSLB-Konfiguration mit der GUI:

1. Navigieren Sie zu **Traffic Management > GSLB > Dashboard**.
2. Klicken Sie auf **Auto-Synchronisation GSLB** und wählen Sie **ForceSYN** aus.
3. Wählen Sie unter **GSLB-Standortname**die GSLB-Sites aus, die mit der Master-Knotenkonfiguration synchronisiert werden sollen.

Vorschau der GSLB-Synchronisation

Durch die Vorschau des GSLB-Synchronisationsvorgangs können Sie die Unterschiede zwischen dem Master-Knoten und jedem Slave-Knoten sehen. Wenn es Abweichungen gibt, können Sie Probleme beheben, bevor Sie die GSLB-Konfiguration synchronisieren.

So zeigen Sie eine Vorschau der GSLB-Synchronisationsausgabe mit der CLI an:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1 sync gslb config -preview
2 <!--NeedCopy-->
```

So zeigen Sie eine Vorschau der GSLB-Synchronisationsausgabe mit der GUI an:

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **GSLB** > **Dashboard**.
2. Klicken Sie auf **Auto-Synchronisation GSLB** und wählen Sie **Vorschau** aus.
3. Klicken Sie auf **Ausführen**.In
   einem Fortschrittsfenster werden eventuelle Abweichungen in der Konfiguration angezeigt.

Debuggen der während des Synchronisierungsprozesses ausgelösten Befehle

Sie können den Status (Erfolg oder Fehler) jedes Befehls anzeigen, der während des Synchronisierungsprozesses ausgelöst wurde, und die Fehlerbehebung entsprechend durchführen.

So debuggen Sie die GSLB-Synchronisationsbefehle mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
sync gslb config -debug
<!--NeedCopy-->
```

So debuggen Sie die GSLB-Synchronisationsbefehle mit der GUI:

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **GSLB** > **Dashboard.**
2. Klicken Sie auf **Auto-Synchronisation GSLB** und wählen Sie **Debug** aus.
3. Klicken Sie auf **Ausführen**. Ein Fortschrittsfenster zeigt den Status jedes Befehls an, der während der Synchronisation ausgelöst wurde.

Echtzeit-Synchronisation zwischen Websites, die an GSLB teilnehmen

December 7, 2021

Sie können die Option “AutomaticConfigSync” verwenden, um die GSLB-Konfiguration des Hauptstandorts in Echtzeit automatisch mit allen untergeordneten Standorten zu synchronisieren. Sie müssen die AutoSync-Option nicht manuell auslösen, um die Konfiguration zu synchronisieren.

Sie können die GSLB-Konfiguration des Hauptstandorts automatisch mit allen untergeordneten Standorten synchronisieren, indem Sie inkrementelle Synchronisation oder vollständige Synchronisation verwenden. Mit dem Parameter “gslbSyncMode” können Sie den Synchronisationsmodus wählen.

> Hinweis:
>
> Ab Citrix ADC Release 13.0 Build 79.x wird die inkrementelle Synchronisation der GSLB-Synchronisation unterstützt. Standardmäßig wird die Synchronisation mittels inkrementeller

> Synchronisation durchgeführt. Die inkrementelle Synchronisation kann durch Aktivieren des Parameters “IncrementalSync” durchgeführt werden.

Best Practices für die Verwendung der Echtzeitsynchronisierungsfunktion

- Es wird empfohlen, dass alle Citrix ADC Appliances, die als Sites teilnehmen, über die gleiche Citrix ADC-Software-Version verfügen.
- Um das RPC-Knotenkennwort zu ändern, ändern Sie zuerst das Kennwort auf der untergeordneten Website und dann auf der Hauptwebsite.
- Konfigurieren Sie lokale GSLB-Sites auf jedem Standort, der an GSLB beteiligt ist.
- Aktivieren Sie AutomaticConfigSync auf einem der Sites, an denen die Konfiguration durchgeführt wird. Diese Seite wird schließlich mit anderen GSLB-Sites synchronisiert.
- Wenn eine neue Konfiguration vorhanden ist oder Änderungen an der vorhandenen Konfiguration vorgenommen werden, überprüfen Sie den Status mit dem Befehl show gslb syncStatus, um zu bestätigen, ob die Änderungen an allen Sites synchronisiert sind oder ob ein Fehler aufgetreten ist.
- Die RSYNC-Portüberwachung muss aktiviert sein.

So aktivieren Sie die Echtzeitsynchronisierung mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set gslb parameter -automaticConfigSync (ENABLED | DISABLED)
<!--NeedCopy-->
```

Beispiel:

```
set gslb parameter -automaticConfigSync ENABLED
<!--NeedCopy-->
```

So aktivieren Sie die Echtzeitsynchronisierung mit der GUI

1. Navigieren Sie zu **Konfiguration** > **Verkehrsverwaltung** > **GSLB** > **GSLB-Einstellungen ändern**.
2. Wählen Sie **Automatic ConfigSync**aus.

   Hinweis: Diese Option muss nur an dem Standort aktiviert werden, an dem die Konfiguration ausgeführt wird.

Informationen zu den folgenden Themen finden Sie unter Manuelle Synchronisierung zwischen Websites, die an GSLB teilnehmen.

- Vorschau der GSLB-Synchronisation
- Debuggen der während des Synchronisierungsprozesses ausgelösten Befehle

Punkte zu beachten

- Die konsolidierte Protokolldatei, die sich auf die Echtzeitsynchronisation bezieht, wird im Verzeichnis /var/netscaler/gslb/periodic_sync.log gespeichert.
- Die Standardkonfigurationsdatei wird im Verzeichnis /var/netscaler/gslb_sync/ gespeichert.
- Die Hauptwebsite verwendet die folgende Verzeichnisstruktur:
  - Die Hauptwebsite speichert alle ihre Dateien im Verzeichnis /var/netscaler/gslb_sync/master.
  - Die Hauptwebsite speichert ihre Konfigurationsdatei, die mit den untergeordneten Sites synchronisiert werden muss, im Verzeichnis /var/netscaler/gslb_sync/master/gslbconf/.
  - Die Statusdateien, die von allen untergeordneten Sites abgerufen werden, werden im Verzeichnis /var/netscaler/gslb_sync/master/slavestatus/ gespeichert.
- Die untergeordnete Site verwendet die folgende Verzeichnisstruktur:
  - Die untergeordnete Site nimmt die neueste Konfigurationsdatei ab, die aus dem Verzeichnis /var/netscaler/gslb_sync/slave/gslbconf angewendet werden soll.
  - Die untergeordnete Site speichert ihre Statusdatei im Verzeichnis /var/netscaler/gslb_sync/slave/gslbst
- In einem Admin-Partitions-Setup wird dieselbe Verzeichnisstruktur am Speicherort beibehalten: /var/partitions/`partition name`/netscaler/gslb_sync.
- Die Uhren auf allen Standorten müssen genau auf einen Echtzeitstandard wie Coordinated Universal Time (UTC) eingestellt sein.

Inkrementelle Synchronisation der GSLB-Konfiguration

Die automatische GSLB-Konfigurationssynchronisierungsfunktion prüft im Intervall alle 10 Sekunden auf die Konfigurationsänderungen am Hauptstandort und führt eine Synchronisation durch. Dieser Wert des Synchronisierungsintervalls ist konfigurierbar.

Bei der inkrementellen Synchronisation werden nur die Konfigurationen, die sich am Hauptstandort zwischen der letzten Synchronisation und dem anschließenden Synchronisierungsintervall (10 Sekunden) geändert haben, an allen untergeordneten Standorten synchronisiert. Die inkrementelle Synchronisation ist das Standardverhalten. Wenn Sie nur die inkrementellen Konfigurationen drücken, wird die Größe der Konfigurationsdatei und damit die Synchronisationszeit erheblich reduziert. Wenn eine inkrementelle Synchronisation fehlschlägt, führt das System automatisch eine vollständige Konfigurationssynchronisation durch.

Die inkrementelle Synchronisation wird auf folgende Weise durchgeführt:

- Die Haupt-Site verschiebt die Konfigurationsdatei, die nur aus den neuesten Änderungen besteht, an alle untergeordneten Websites. Die letzte Änderung bezieht sich auf die Konfigurationen, die sich zwischen der letzten Synchronisation und dem anschließenden Synchronisierungsintervall (10 Sekunden) geändert haben.
- Jede untergeordnete Website wendet die letzte Änderung auf ihre eigene Website an.
- Inkrementelle Synchronisation wird nicht auf den untergeordneten Standorten versucht, die sich im Zustand DOWN befinden. Wenn die Site wieder nach oben kommt, wird erneut die Synchronisierung durchgeführt.
- Die untergeordnete Site generiert bei jedem Schritt Statusprotokolle und kopiert sie in eine Datei an einem bestimmten Speicherort.
- Die Haupt-Site ruft die Statusprotokolldateien vom angegebenen Speicherort ab.
- Die Hauptwebsite erstellt eine Protokolldatei mit Protokollen, die von allen untergeordneten Websites kombiniert werden.
- Diese kombinierte Protokolldatei wird in der Datei /var/netscaler/gslb/periodic_sync.log gespeichert.

Weitere Informationen zu den Verzeichnissen, in denen die Konfigurationsdateien gespeichert sind, finden Sie im Abschnitt “Zu beachtende Punkte”.

So aktivieren Sie die inkrementelle Synchronisation der GSLB-Konfiguration mit der CLI

```
1 set gslb parameter -AutomaticConfigSync (ENABLED | DISABLED) -
     GSLBSyncMode (IncrementalSync | FullSync) -GslbConfigSyncMonitor (
     ENABLED | DISABLED) -GSLBSyncInterval <secs> -GSLBSyncLocFiles (
     ENABLED | DISABLED)
2 <!--NeedCopy-->
```

Beispiel:

```
1 set gslb parameter -AutomaticConfigSync ENABLED -GSLBSyncMode
     IncrementalSync
2 <!--NeedCopy-->
```

Die inkrementelle Synchronisation bietet die folgenden konfigurierbaren Parameter, die die Gesamtzeit für die Synchronisierung der GSLB-Konfiguration reduzieren.

- **gslbConfigSyncMonitor**—Aktivieren Sie den GSLB Config Sync Monitor-Parameter, um den Status des RSYNC-Ports der untergeordneten Websites zu überwachen, bei dem es sich um den SSH-Port 22 an der IP-Adresse des Remote-GSLB-Standorts handelt. Wenn der Monitor den untergeordneten Standortstatus als DOWN anzeigt, wird der RSYNC-Vorgang zu dieser Site über-

sprungen. Dies reduziert die Verzögerungen bei der Synchronisation, die durch den Versuch verursacht werden, eine Verbindung zu den Remote-Standorten herzustellen, die DOWN sind.

Beispiel zum Aktivieren der RSYNC-Portüberwachung in der CLI:

```
set gslb parameter -GSLBSyncMode IncrementalSync -
   GslbConfigSyncMonitor ENABLED
<!--NeedCopy-->
```

- **gslbSyncInterval**—Legt das Zeitintervall (in Sekunden) fest, in dem die GSLB-Konfigurationssynchronisation stattfindet. Standardmäßig synchronisiert die Funktion zur automatischen GSLB-Konfiguration die GSLB-Konfiguration automatisch alle 10 Sekunden. Sie können das Zeitintervall auf einen beliebigen Wert ändern. Verzichten Sie darauf, dies auf einen niedrigeren Wert zu setzen, z. B. nicht weniger als 5 Sekunden. Denn das häufige Synchronisieren kann den CPU-Verbrauch der Verwaltungs-CPU erhöhen.

  > Hinweis:
  >
  > In einem Setup der Admin-Partition kann das Zeitintervall nur in der Standardpartition festgelegt werden, da es sich um einen globalen Parameter handelt.

  Beispiel zum Festlegen des Synchronisierungsintervalls:

```
set gslb parameter -AutomaticConfigSync ENABLED -GSLBSyncMode
   IncrementalSync -GSLBSyncInterval 7
<!--NeedCopy-->
```

- **gslbSynclocFiles**—Während der GSLB-Konfigurationssynchronisation werden die Änderungen an den Speicherort DB-Dateien standardmäßig erkannt und automatisch synchronisiert. Da sich die Speicherort-DB-Verzeichnisse nicht häufig ändern, können Administratoren die automatische Synchronisierung der Speicherort-DB-Dateien deaktivieren. Stattdessen müssen Administratoren die DB-Dateien des Speicherorts manuell auf die untergeordneten GSLB-Websites kopieren. Das Synchronisieren von StandortdB-Dateien benötigt viel Zeit. Dadurch wird die gesamte Synchronisationszeit reduziert.

  Beispiel zum Deaktivieren der automatischen Synchronisierung der Speicherort-DB-Dateien:

```
set gslb parameter -GSLBSyncMode IncrementalSync -
   GSLBSyncLocFiles DISABLED
<!--NeedCopy-->
```


So aktivieren Sie die inkrementelle GSLB-Synchronisation mit der GUI

1. Navigieren Sie zu **Traffic Management > GSLB > Dashboard > GSLB-Einstellungen ändern**.
2. Auf der Seite **GSLB-Parameter festlegen** können Sie Folgendes ausführen:
    - Um die inkrementelle Synchronisation zu aktivieren, wählen Sie **IncrementalSync** aus dem Dropdownmenü **GSLB Sync Mode** aus.
    - Um das Intervall für die automatische GSLB-Konfiguration einzustellen, geben Sie die Zeit in Sekunden in das Feld **GSLB-Synchronisierungsintervall** ein.
    - Um die RSYNC-Portüberwachung zu aktivieren, aktivieren Sie das Kontrollkästchen **GSLB Config Sync Monitor** .
    - Deaktivieren Sie das Kontrollkästchen **GSLB Sync Loc Files, um die automatische Synchronisierung der Speicherort DB-Dateien** zu deaktivieren.

Vollständige Synchronisation der GSLB-Konfiguration

Immer wenn es eine Konfigurationsänderung am Hauptstandort gibt, wird die vollständige GSLB-laufende Konfiguration auf dem Hauptstandort an alle untergeordneten Standorte weitergeleitet. Selbst wenn die inkrementelle Synchronisation konfiguriert ist, wird eine vollständige Synchronisation durchgeführt, wenn der Hauptstandort den Konfigurationsstatus des untergeordneten Standorts nicht kennt. Einige dieser Szenarien lauten wie folgt:

- Aktivieren Sie zum ersten Mal die Funktion zur automatischen GSLB-Konfigurationssynchronisierung.
- Starten Sie die Citrix ADC Appliance neu.
- Die GSLB-Bereitstellung verfügt über mehrere Hauptstandorte, und eine andere Hauptwebsite wird zur aktiven Hauptwebsite.
- Fügen Sie der GSLB-Bereitstellung eine neue untergeordnete Site hinzu.

Die vollständige Synchronisation der GSLB-Konfiguration erfolgt auf folgende Weise:

- Die Haupt-Site verschiebt ihre neueste Konfigurationsdatei an alle untergeordneten Sites.
- Jede untergeordnete Site vergleicht ihre eigene Konfiguration mit der neuesten Konfigurationsdatei, die vom Hauptstandort gesendet wird. Die untergeordnete Site identifiziert den Unterschied in der Konfiguration und wendet die Delta-Konfiguration für einen eigenen Standort an.
- Die untergeordnete Site generiert bei jedem Schritt Statusprotokolle und kopiert sie in eine Datei an einem bestimmten Speicherort.
- Die Haupt-Site ruft die Statusprotokolldateien vom angegebenen Speicherort ab.
- Die Hauptwebsite erstellt eine Protokolldatei mit Protokollen, die von allen untergeordneten Websites kombiniert werden.
- Diese kombinierte Protokolldatei wird in der Datei /var/netscaler/gslb/periodic_sync.log gespeichert.

Wenn Sie versuchen, eine Site manuell (mit dem`sync gslb config` Befehl) zu synchronisieren,

während sie automatisch synchronisiert wird, wird eine Fehlermeldung “Sync in progress” angezeigt. Die automatische Synchronisierung kann nicht für einen Standort ausgelöst werden, der derzeit manuell synchronisiert wird.

> **Achtung:**
>
> Ab Citrix ADC 12.1 Build 49.37 werden SNMP-Traps generiert, wenn Sie die GSLB-Konfiguration synchronisieren. Bei der Echtzeitsynchronisierung wird der Synchronisationsstatus im ersten SNMP-Trap als Ausfall erfasst. Sie können diesen Status ignorieren, da unmittelbar nach dem ersten Trap mit dem aktuellen Synchronisationsstatus automatisch ein zweites SNMP-Trap generiert wird. Wenn die Synchronisierung jedoch auch im zweiten Versuch fehlgeschlagen ist, wird SNMP-Trap nicht generiert, da sich der Synchronisationsstatus nicht vom vorherigen Synchronisationsstatus geändert hat.

Weitere Informationen zum Konfigurieren der Citrix ADC Appliance zum Generieren von Traps finden Sie unter Konfigurieren des Citrix ADC zum Generieren von SNMP-Traps.

So aktivieren Sie die vollständige GSLB-Synchronisation mit der CLI

```
set gslb parameter -GSLBSyncMode (IncrementalSync | FullSync)
<!--NeedCopy-->
```

Beispiel:

```
set gslb parameter -GSLBSyncMode FullSync
<!--NeedCopy-->
```

So aktivieren Sie die inkrementelle GSLB-Synchronisation mit der GUI:

1. Navigieren Sie zu **Traffic Management > GSLB > Dashboard > GSLB-Einstellungen ändern**.
2. Wählen **Sie auf der Seite GSLB-Parameter festlegen** im Dropdownmenü **GSLB-Synchronisierungsmodus die Option FullSync Mode** aus.

Mehrere Hauptstandorte in einer GSLB-Bereitstellung

Die Citrix ADC Appliance unterstützt mehrere Hauptstandorte in einer aktiv-passiven Bereitstellung. Es wird empfohlen, zwei Hauptstandorte in einer GSLB-Bereitstellung zu haben, um den Ausfall des GSLB-Hauptstandorts zu bewältigen. Zwei Hauptstandorte können einen einzelnen Ausfallpunkt der GSLB-Konfigurationssynchronisation vermeiden. Zu jeder Zeit kann nur ein Hauptstandort die GSLB-Konfiguration vom Benutzer aktiv verarbeiten. Wenn die Konfigurationsänderungen gleichzeitig an mehreren Hauptstandorten durchgeführt werden, kann dies zu Konfigurationsinkonsistenz oder

Konfigurationsverlusten führen. Daher wird empfohlen, Konfigurationsänderungen von jeweils nur einem Hauptstandort aus durchzuführen und den anderen Hauptstandort als Backup zu verwenden, wenn der aktive Hauptstandort ausfällt.

> Hinweis:
>
> Wenn mehrere Hauptstandorte in einer GSLB-Bereitstellung verwendet werden, muss die RSYNC-Überwachung aktiviert sein.

Führen Sie den folgenden Befehl aus, um einen GSLB-Knoten als einen der Hauptstandorte für die GSLB-Konfigurationssynchronisation zu erstellen:

```
set gslb parameter -automaticConfigSync Enabled
<!--NeedCopy-->
```

GSLB-Synchronisationsstatus und Zusammenfassung anzeigen

December 7, 2021

Nachdem die GSLB-Konfiguration über die GSLB-Sites synchronisiert wurde, können Sie den detaillierten Status und die Zusammenfassung des letzten GSLB-Synchronisierungsvorgangs anzeigen. Dies gilt sowohl für die manuelle als auch für die Echtzeitsynchronisation GSLB.

So zeigen Sie den GSLB-Synchronisationsstatus oder die Zusammenfassung mit der CLI an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show gslb sync status
<!--NeedCopy-->
```

oder

```
show gslb syncStatus -summary
<!--NeedCopy-->
```


Beispiel-Konfigurationsausgabe für die manuelle GSLB-Synchronisierung

Die folgende Ausgabe zeigt den Status der manuellen GSLB-Konfigurationssynchronisierung an.

```
> sh gslb syncStatus
Displaying the status of the manual GSLB configuration synchronization:

gslb_site1[Master]:
        Getting Config:  ok
gslb_site2[Slave]:
        Syncing gslb static proximity database:  ok
        Syncing inbuilt gslb static proximity database : ok
        Getting Config:  ok
        Comparing config:  ok
        Applying changes:  ok
gslb_natsite1[Slave]:
        Syncing gslb static proximity database:  ok
        Syncing inbuilt gslb static proximity database : ok
        Getting Config:  ok
        Comparing config:  ok
        Applying changes:  ok
 Done
>
```

Die folgende Ausgabe zeigt die Statusübersicht der manuellen GSLB-Konfigurationssynchronisierung an.

```
> sh gslb syncStatus -summary
Displaying the status summary of the manual GSLB configuration synchronization:

-------------------------------------------------------------------------------------------------------------
        Site Name                Status          Reason
-------------------------------------------------------------------------------------------------------------
        gslb_site1               Success         All Done
        gslb_site2               Failure         Error executing command on gslb site...ERROR: Connection failed
        gslb_natsite1            Success         All Done
Done
>
```


Beispiel-Konfigurationsausgabe für GSLB-Echtzeitsynchronisation

Die folgende Ausgabe zeigt den Status der Echtzeit-GSLB-Konfigurationssynchronisierung für die Master Site an:

```
> sh gslb syncStatus
Displaying the status of the real time GSLB configuration
   synchronization as master node:

site2[Master]:
                New GSLB configuration detected at Fri Jan 23 20:54:24
                   2020
                Fetching current configuration: Done
                Updating default.conf file: Done
site1[Slave]:
                Syncing gslb static proximity database to node site1:
                   Done
                Syncing inbuilt GSLB static proximity database to node
                   site1: Done
                Syncing ssl certificates, keys and CRLS to node site1:
                   Done
                Syncing current configuration to site1: Done
                Pulling status files from site1: Status file not
                   available yet(Sync in progress)
                Pulling status files from site1: Done
                site1 received new configuration from 10.102.217.205 in
                    file 2JNSzClRHK5+pdek6szQ3g-default-10.102.217.210.
                   conf
                Firing set gslb parameter -startConfigSync ENABLED
                   command: Done
                Fetching running GSLB Config: Done
                Comparing config: Done
                Applying changes: Done
                Firing set gslb parameter -startConfigSync DISABLED
                   command: Done
                Updating default.conf file: Done
Done
<!--NeedCopy-->
```

Die folgende Ausgabe zeigt den Status der Echtzeit-GSLB-Konfigurationssynchronisierung für die Slave-Site an:


```
> sh gslb syncStatus
Displaying the status of the real time GSLB configuration
    synchronization as slave node:

                site1 received new configuration from 10.102.217.205 in
                     file 2JNSzClRHK5+pdek6szQ3g-default-10.102.217.210.
                    conf
                Firing set gslb parameter -startConfigSync ENABLED
                    command: Done
                Fetching running GSLB Config: Done
                Comparing config: Done
                Applying changes: Done
                Firing set gslb parameter -startConfigSync DISABLED
                    command: Done
                Updating default.conf file: Done
Done
<!--NeedCopy-->
```

Die folgende Ausgabe zeigt die Statusübersicht der Echtzeit-GSLB-Konfigurationssynchronisierung für die Master Site an:

```
> sh gslb syncStatus -summary
Displaying the status summary of the real time GSLB configuration
    synchronization as master node:

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

                Site Name                                   Status
                                  Reason
------------------------------------------------------------------------------

                site2                                       Success
                                 All Done
                site1                                       Success
                                 All Done

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

Die folgende Ausgabe zeigt die Statusübersicht der Echtzeit-GSLB-Konfigurationssynchronisierung für Slave-Site an:


```
> sh gslb syncStatus  - summary
Displaying the status summary of the real time GSLB configuration
    synchronization as slave node:

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

                Site Name                                   Status
                                  Reason
--------------------------------------------------------------------------------

                site1                                       Success
                                 All Done

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

So zeigen Sie den GSLB-Synchronisationsstatus oder die Zusammenfassung mit der GUI an

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **GSLB** > **Dashboard**.
2. Klicken Sie bei Bedarf auf **Synchronisationsübersicht anzeigen oder Synchronisationsstatus** anzeigen.

SNMP-Traps für GSLB-Konfigurationssynchronisation

October 5, 2021

Ab Citrix ADC 12.1 Build 49.xx generiert die Citrix ADC Appliance SNMP-Traps für lokale und Remotesites, wenn Sie die GSLB-Konfiguration synchronisieren. SNMP-Traps werden sowohl für die manuelle Synchronisation als auch für die Echtzeitsynchronisierung generiert.

Wenn Sie die GSLB-Konfiguration zum ersten Mal synchronisieren, werden SNMP-Traps generiert. Bei den nachfolgenden Synchronisationsversuchen werden die SNMP-Traps nur generiert, wenn sich der Synchronisationsstatus gegenüber dem vorherigen Synchronisationsstatus ändert. Außerdem werden die SNMP-Traps nur für Sites generiert, für die sich der Synchronisierungsstatus gegenüber dem vorherigen Status geändert hat.

Betrachten Sie beispielsweise, dass die erste GSLB-Konfigurationssynchronisation erfolgreich ist. Wenn Sie die Konfiguration zum zweiten Mal synchronisieren und die Synchronisation erneut erfolgreich ist, werden SNMP-Traps nicht generiert, da der Status nicht geändert wird. Wenn jedoch beim dritten Versuch die Synchronisierung für einen der Sites fehlschlägt, wird nur für diesen Standort SNMP-Trap generiert.

Bei einer Hochverfügbarkeit und einem Cluster-Setup generiert die Appliance die SNMP-Traps, wenn Sie die GSLB-Konfiguration vom neuen Knoten unabhängig vom vorherigen Synchronisationsstatus synchronisieren. Wenn die SNMP-Trap-Option zuvor deaktiviert und dann aktiviert wurde, werden SNMP-Traps ab diesem Zeitpunkt unabhängig vom vorherigen Synchronisationsstatus generiert.

Die SNMP-Traps der GSLB-Konfigurationssynchronisation enthalten folgende Details:

- Name der GSLB-Site, für die die SNMP-Trap gesendet wird.
- Synchronisationsstatus der GSLB-Konfiguration: Erfolg oder Misserfolg.
- GSLB-Konfigurationssynchronisierungsmodus: Inkrementelle Synchronisierung oder Vollsynchronisierung.
- (Optional) Detaillierte Informationen zu den SNMP-Fallen.

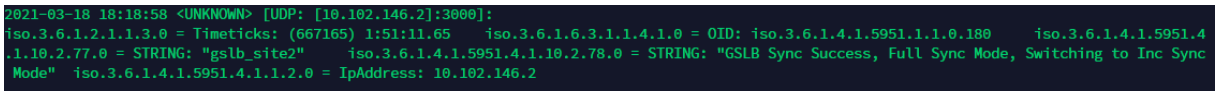
Die SNMP-Traps werden in den folgenden Szenarien generiert:

- Der GSLB-Synchronisationsstatus für eine GSLB-Site wechselt von Erfolg zu Failure und umgekehrt.
- Der GSLB-Synchronisationsmodus wechselt von der inkrementellen Synchronisation zur vollständigen Synchronisation und umgekehrt.

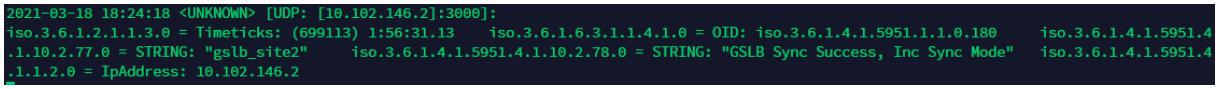
> Hinweis:
>
> Selbst wenn die inkrementelle Synchronisation aktiviert ist und die vollständige Synchronisation aus irgendeinem Grund auf einer GSLB-Site durchgeführt wird, wird der Grund für die vollständige Synchronisierung im Abschnitt “Detaillierte Informationen” der Fallenmeldung erwähnt. Zum Beispiel, wenn der GSLB-Konfiguration eine neue GSLB-Site hinzugefügt wird.

Beispiel für SNMP-Trap-Nachrichten

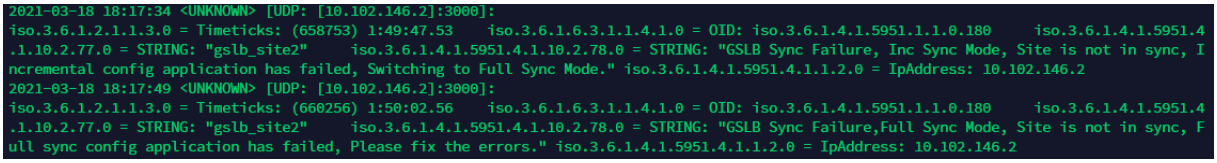
Die folgende Abbildung zeigt eine Beispiel-SNMP-Trap für gslb_site2, bei der die GSLB-Konfigurationssynchronisati
im Vollsynchronisierungsmodus erfolgreich ist.



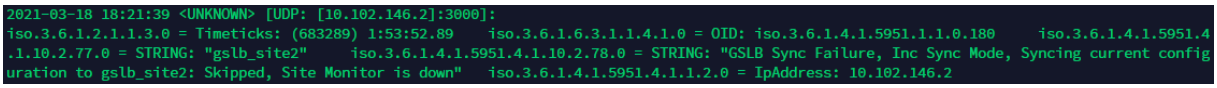
Die folgende Abbildung zeigt eine Beispiel-SNMP-Trap für gslb_site2, bei der die GSLB-Konfigurationssynchronisati
im inkrementellen Synchronisierungsmodus erfolgreich ist.



Die folgende Abbildung zeigt eine Beispiel-SNMP-Trap für gslb_site2, bei der die GSLB-Konfigurationssynchronisati
im inkrementellen Synchronisierungsmodus fehlgeschlagen ist. Die Fehlermeldung zeigt an, dass Sie die Fehler manuell beheben müssen, um die Synchronisation abzuschließen.



Die folgende Abbildung zeigt eine Beispiel-SNMP-Trap für gslb_site2, bei der die GSLB-Konfigurationssynchronisati im inkrementellen Synchronisierungsmodus fehlgeschlagen ist. Es gibt auch den Grund für den Synchronisierungsfehler an, dh der Site-Monitor ist DOWN.



GSLB-Dashboard

October 5, 2021

Sie können den Gesamtstatus der GSLB-Sites, die an GSLB teilnehmen, auf dem GSLB-Dashboard anzeigen.

Sie können über das Dashboard auf die GSLB-Einstellungen zugreifen. Sie können den GSLB-Konfigurationsassistenten auch über das Dashboard starten. Darüber hinaus können Sie die Synchronisierung durchführen und das GSLB-Setup über das Dashboard testen.

Um auf das GSLB-Dashboard zuzugreifen, navigieren Sie zu **Konfiguration** > **Traffic Management** > **GSLB** > **Dashboard** .

Überwachen von GSLB-Diensten

October 5, 2021

Wenn Sie einen Remotedienst an einen virtuellen GSLB-Server binden, tauschen die GSLB-Sites Metrikinformationen aus, einschließlich Netzwerkmetrikinformationen, d. h. die Round-Trip-Zeit- und Persistenzinformationen.

Wenn eine Metrik-Austauschverbindung zwischen einem der teilnehmenden Sites vorübergehend unterbrochen wird, wird der Remote-Standort als DOWN markiert, und der Lastausgleich wird auf den verbleibenden Sites durchgeführt, die UP sind. Wenn der Metrikaustausch für einen Standort DOWN ist, werden auch die Remote-Dienste, die zum Standort gehören, als DOWN markiert.

Die Citrix ADC Appliance wertet den Status der Remote-GSLB-Dienste regelmäßig mithilfe von MEP oder Monitoren aus, die explizit an die Remotedienste gebunden sind. Das Binden von expliziten Monitoren an lokale Dienste ist nicht erforderlich, da der Status des lokalen GSLB-Dienstes standardmäßig

mit dem MEP aktualisiert wird. Sie können jedoch explizite Monitore an einen Remotedienst binden. Wenn Monitore explizit gebunden sind, wird der Status des Remote-Dienstes nicht vom Metrikaustausch gesteuert.

Wenn Sie einen Monitor an einen GSLB-Remote-Dienst binden, verwendet die Citrix ADC Appliance standardmäßig den Status des vom Monitor gemeldeten Dienstes. Sie können jedoch die Citrix ADC Appliance so konfigurieren, dass Monitore verwendet werden, um Dienste in den folgenden Situationen auszuwerten:

- Verwenden Sie immer Monitore (Standardeinstellung).
- Verwenden Sie Monitore, wenn MEP DOWN ist.
- Verwenden Sie Monitore, wenn Remote-Dienste und MEP DOWN sind.

Die zweite und dritte der oben genannten Einstellungen ermöglichen es der Appliance, die Überwachung zu beenden, wenn MEP auf UP eingestellt ist. In einer hierarchischen GSLB-Setup stellt ein GSLB-Site beispielsweise die MEP-Informationen über seine untergeordneten Sites an seinen übergeordneten Standort bereit. Ein solcher Zwischenstandort kann den Status des untergeordneten Standorts aufgrund von Netzwerkproblemen als DOWN auswerten, obwohl der tatsächliche Status des Standorts UP ist. In diesem Fall können Sie Monitore an die Dienste des übergeordneten Standorts binden und MEP deaktivieren, um den tatsächlichen Status des Remotedienstes zu bestimmen. Mit dieser Option können Sie steuern, wie die Zustände der Remote-Dienste ermittelt werden.

Um Monitore zu verwenden, erstellen Sie sie zuerst und binden sie dann an GSLB-Dienste.

Monitorauslöser konfigurieren

Sie können eine GSLB-Site so konfigurieren, dass sie immer Monitore verwenden (Standardeinstellung), Monitore verwenden, wenn der MEP ausgefallen ist, oder Monitore verwenden, wenn der Remotedienst und der MEP ausgefallen sind. In den beiden letztgenannten Fällen stoppt die Citrix ADC Appliance die Überwachung, wenn MEP in den UP-Status zurückkehrt.

So konfigurieren Sie die Monitorauslösung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set gslb site <siteName> -triggerMonitor (ALWAYS | MEPDOWN |
     MEPDOWN_SVCDOWN)
2 <!--NeedCopy-->
```

Beispiel:


```
set gslb site Site-GSLB-North-America  -triggerMonitor Always
<!--NeedCopy-->
```

So konfigurieren Sie die Monitorauslösung mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Sites**, und doppelklicken Sie auf die Site.
2. Wählen Sie in der Dropdownliste **Triggermonitore** eine Option für die Auslösung der Überwachung aus.

Hinzufügen oder Entfernen von Monitoren

Um einen Monitor hinzuzufügen, geben Sie den Typ und den Port an. Sie können keinen Monitor entfernen, der an einen Dienst gebunden ist. Sie müssen zuerst die Bindung des Monitors vom Dienst aufheben.

So fügen Sie einen Monitor mit der Befehlszeilenschnittstelle hinzu

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

```
add lb monitor <monitorName> -type <monitorType> -destPort <portNumber>

show lb monitor <monitorName>
<!--NeedCopy-->
```

Beispiel:

```
add lb monitor monitor-HTTP-1 -type HTTP -destPort 80
show lb monitor monitor-HTTP-1
<!--NeedCopy-->
```

So entfernen Sie einen Monitor mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm lb monitor <monitorName>
<!--NeedCopy-->
```


So fügen Sie einen Monitor mit dem Konfigurationsdienstprogramm hinzu

Navigieren Sie zu
Traffic Management > Load Balancing > Monitore, und fügen Sie einen Monitor hinzu oder löschen Sie ihn.

Binden von Monitoren an einen GSLB-Dienst

Sobald Sie Monitore erstellt haben, müssen Sie sie an GSLB-Dienste binden. Wenn Sie Monitore an die Dienste binden, können Sie eine Gewichtung für den Monitor angeben. Nach dem Binden eines oder mehrerer gewichteter Monitore können Sie einen Überwachungsschwellenwert für den Dienst konfigurieren. Dieser Schwellenwert nimmt den Dienst ab, wenn die Summe der gebundenen Monitorgewichte unter den Schwellenwert fällt.

Hinweis: Im Konfigurationsprogramm können Sie sowohl die Gewichtung als auch den Überwachungsschwellenwert festlegen, während Sie den Monitor binden. Wenn Sie die Befehlszeile verwenden, müssen Sie einen separaten Befehl ausführen, um den Überwachungsschwellenwert des Dienstes festzulegen.

So binden Sie den Monitor mit der Befehlszeilenschnittstelle an den GSLB-Dienst

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind monitor <name> <serviceName> [ -state (Enabled | Disabled) ] -
   weight <positiveInteger>
<!--NeedCopy-->
```

Beispiel:

```
bind monitor monitor-HTTP-1 service-GSLB-1 -state enabled -weight 2
<!--NeedCopy-->
```

So legen Sie den Überwachungsschwellenwert für einen GSLB-Dienst mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set gslb service <ServiceName> -monThreshold <PositiveInteger>
<!--NeedCopy-->
```


Beispiel:

```
set gslb service service-GSLB-1 -monThreshold 9
<!--NeedCopy-->
```

So binden Sie den Monitor mit dem Konfigurationsdienstprogramm an den GSLB-Dienst

1. Navigieren Sie zu Traffic Management > GSLB > Services.
2. Klicken Sie auf den Abschnitt **Monitor**, und binden Sie den Monitor an den GSLB-Dienst.

So legen Sie den Überwachungsschwellenwert für einen GSLB-Dienst mit dem Konfigurationsdienstprogramm fest

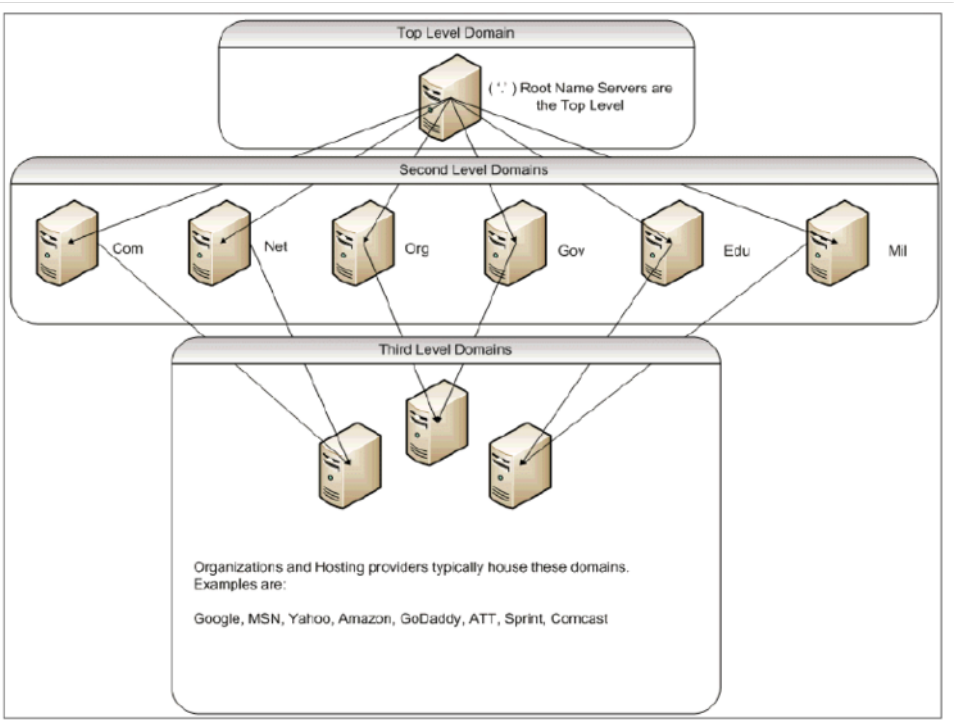
1. Navigieren Sie zu Traffic Management > GSLB > Services.
2. Klicken Sie auf den Abschnitt **Schwellenwert überwachen**, und geben Sie einen Schwellenwert ein.

Wie das Domänennamensystem GSLB unterstützt

October 5, 2021

Das Domänennamensystem (DNS) wird als verteilte Datenbank betrachtet, die die Client/Server-Architektur verwendet. Nameserver sind die Server in der Architektur, und die Resolver sind die Clients, bei denen es sich um Bibliotheksroutinen handelt, die auf einem Betriebssystem installiert sind und Abfragen über das Netzwerk erstellen und senden.

Die logische Hierarchie des DNS ist im folgenden Diagramm dargestellt:



> Hinweis:
>
> Die Stammserver der zweiten Ebene sind dafür verantwortlich, Name-Server-zu-Adress-Zuordnungen für Name-Server-Delegationen innerhalb der Domänen .com, .net, .org, .gov usw. zu pflegen. Jede Domäne innerhalb der Domänen der zweiten Ebene ist für die Pflege von Nameserver-zu-Adress-Zuordnungen für die untergeordneten Organisationsdomänen verantwortlich. Auf Organisationsebene werden die einzelnen Hostadressen für www, FTP und andere Dienste, die Hosts bereitstellen, aufgelöst.

Delegation

Der Hauptzweck der aktuellen DNS-Topologie besteht darin, die Aufrechterhaltung aller Adressaufzeichnungen in einer Behörde zu verringern. Dies ermöglicht die Delegation eines Organisationsnamenraums an diese bestimmte Organisation. Die Organisation kann ihren Raum dann weiter an Subdomains innerhalb der Organisation delegieren. Unter citrix.com können Sie beispielsweise Subdomains namens `sales.citrix.comeducation.citrix.com`, und erstellen `support.citrix.com`. Die entsprechenden Abteilungen können ihre eigenen Nameserver verwalten, die für ihre Subdomain autoritativ sind, und dann ihren eigenen Satz von Hostnamen verwalten, um Zuordnungen zu adressieren. Keine einzige Abteilung ist für die Pflege aller Citrix Adressdatensätze verantwortlich. Jede Abteilung kann Adressen ändern und Topologien ändern und nicht mehr Arbeit in der übergeordneten Domäne oder Organisation auferlegen.

Vorteile der hierarchischen Topologie

Einige der Vorteile der hierarchischen Topologie sind:

- Skalierbarkeit
- Hinzufügen von Caching-Funktionen zu Nameservern auf jeder Ebene, wo eine DNS-Anfrage von einem Host bedient wird, der für eine bestimmte Domäne nicht autoritativ ist, aber die Antwort auf die Abfrage beitragen und die Staus- und Antwortzeit verkürzt.
- Das Caching erzeugt auch Redundanz und Ausfallsicherheit gegenüber Serverausfällen. Wenn ein Nameserver ausfällt, ist es weiterhin möglich, dass Datensätze von anderen Servern bereitgestellt werden können, die kürzlich zwischengespeicherte Kopien derselben Datensätze enthalten.

Resolver

Resolver sind die Clientkomponente im DNS-System. Programme, die auf einem Host ausgeführt werden, die Informationen aus dem Domänennamenbereich benötigen, verwenden den Resolver. Der Resolver behandelt:

- Abfragen eines Nameservers.
- Interpretieren von Antworten (dies können Ressourceneinträge oder ein Fehler sein).
- Rückgabe der Informationen an die Programme, die sie angefordert haben.

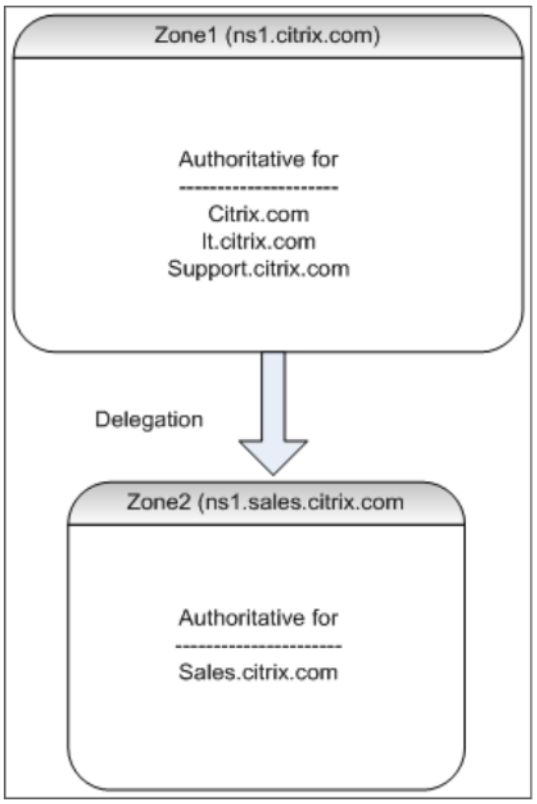
Der Resolver besteht aus einer Reihe von Bibliotheksroutinen, die in Programme wie Telnet, FTP und Ping kompiliert werden. Es sind keine getrennten Prozesse. Die Resolver können eine Anfrage zusammenstellen, senden und auf eine Antwort warten. Und senden Sie es erneut (möglicherweise an einen sekundären Nameserver), wenn es nicht innerhalb einer bestimmten Zeit beantwortet wird. Diese Arten von Resolvern werden als Stub-Resolver bezeichnet. Einige Resolver verfügen über die zusätzliche Funktionalität, um Datensätze zu zwischenspeichern und die Zeit zu leben (TTL). In Windows ist diese Funktionalität über den DNS-Clientdienst verfügbar, der über die Konsole “services.msc” sichtbar ist.

Namen-Server

Nameserver speichern im Allgemeinen vollständige Informationen über einen bestimmten Teil eines Domänennamenraums (Zone genannt). Der Nameserver soll dann die Berechtigung für diese Zone haben. Sie können auch für mehrere Zonen maßgeblich sein.

Der Unterschied zwischen einer Domäne und einer Zone ist subtil. Eine Domäne ist der vollständige Satz von Entitäten einschließlich ihrer Subdomains, während eine Zone nur die Informationen innerhalb einer Domäne ist, die nicht an einen anderen Nameserver delegiert wird. Ein Beispiel für eine Zone ist `citrix.com`, während es `sales.citrix.com` sich um eine separate Zone handelt, wenn diese Zone an einen anderen Nameserver innerhalb der Subdomäne delegiert wird. In diesem Fall

kann die primäre Citrix Zone `citrix.comit.citrix.com`, und enthalten `support.citrix.com`. Da der delegiert `sales.citrix.com` wird, ist es nicht Teil der Zone, über die der `citrix.com` Nameserver autoritativ ist. Das folgende Diagramm zeigt die beiden Zonen.

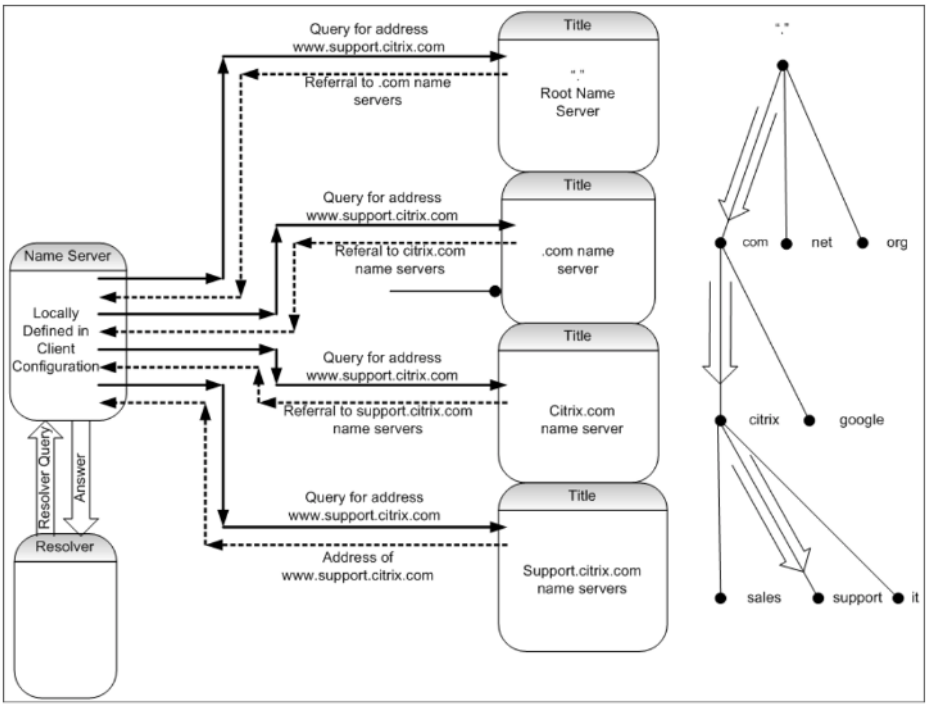


Um eine Subdomain ordnungsgemäß zu delegieren, müssen Sie verschiedenen Nameservern die Berechtigung für die Subdomain zuweisen. Im vorhergehenden Beispiel enthält der `ns1.citrix.com` keine Informationen über die `sales.citrix.com` Subdomain. Stattdessen enthält es Zeiger auf die Name-Server, die für die `ns1.sales.citrix.com` Subdomain autoritativ sind.

Stammnameserver und Abfrageauflösung

Root-Name-Server kennen die IP-Adressen aller Name-Server, die für die Domänen der zweiten Ebene autoritativ sind. Wenn ein Nameserver keine Informationen über eine bestimmte Domäne in seinen eigenen Datendateien hat, muss er sich nur an einen Stammserver wenden, um den richtigen Zweig der **DNS-Baumstruktur** zu durchqueren, um schließlich zur angegebenen Domäne zu gelangen. Dies beinhaltet eine Reihe von Anfragen an mehrere Nameserver, um beim Traversal des Baums zu helfen, den nächsten autoritativen Nameserver zu finden, der zur weiteren Lösung kontaktiert werden muss.

Das folgende Diagramm zeigt eine typische DNS-Anforderung, vorausgesetzt, dass während der Durchquerung kein zwischengespeicherter Datensatz für den angeforderten Namen vorhanden ist. Im folgenden Beispiel wird ein Mock Up der Citrix Domäne verwendet.



Rekursive und nicht rekursive Abfragen

Das vorhergehende Beispiel veranschaulicht die beiden Arten von Abfragen, die auftreten können.

- Rekursive Abfrage: Die Abfrage zwischen dem Resolver und dem lokal konfigurierten Name-Server ist rekursiv. Dies bedeutet, dass der Name-Server die Abfrage erhält und nicht auf den Resolver reagiert, bis die Abfrage vollständig beantwortet wurde oder ein Fehler zurückgegeben wird. Wenn der Nameserver eine Verweisung an die Abfrage erhält, folgt der Name-Server der Überweisung, bis der Name-Server die zurückgegebene Antwort (IP-Adresse) schließlich erhält.
- Nicht rekursive Abfrage: Die Abfrage, die der lokal konfigurierte Name-Server an den nachfolgenden autoritativen Nameserver auf Domänenebene stellt, ist nicht rekursiv (oder iterativ). Jede Anfrage wird sofort entweder mit einer Verweisung an einen autoritativen Server auf niedrigerer Ebene oder mit der Antwort auf die Abfrage beantwortet, wenn der abgefragte Name-Server die Antwort in seinen Datendateien oder seinem Cache enthält.

Zwischenspeichern

Obwohl der Lösungsprozess involviert ist und möglicherweise kleine Anfragen an mehrere Hosts erfordert, ist er schnell. Einer der Faktoren, der die Geschwindigkeit der DNS-Auflösung erhöht, ist das Caching. Jedes Mal, wenn ein Name-Server eine rekursive Abfrage erhält, muss er möglicherweise mit anderen Servern kommunizieren, um schließlich zum richtigen autoritativen Server für die spezifische Anforderung zu gelangen. Es speichert alle Informationen, die es zur späteren Bezugnahme

erhält. Wenn der nächste Client eine ähnliche Anfrage stellt, z. B. einen anderen Host, aber in derselben Domäne, kennt er bereits den Name-Server, der für diese Domäne autoritativ ist, und kann eine Anfrage direkt dorthin senden, anstatt am Root-Name-Server zu starten.

Caching kann auch für negative Antworten auftreten, z. B. für Abfragen nach Hosts, die nicht existieren. In diesem Fall darf der Server den autoritativen Nameserver nicht nach der angeforderten Domäne abfragen, um herauszufinden, dass der Host nicht existiert. Um Zeit zu sparen, prüft der Name-Server einfach den Cache und antwortet mit dem negativen Datensatz zurück.

Nameserver zwischenspeichern Datensätze nicht auf unbestimmte Zeit, sonst können Sie die IP-Adressen niemals aktualisieren. Um Synchronisationsprobleme zu vermeiden, enthalten DNS-Antworten eine Time to live (TTL). In diesem Feld wird das Zeitintervall beschrieben, für das der Cache einen Datensatz speichern kann, bevor er ihn verwerfen und beim autoritativen Nameserver nach aktualisierten Datensätzen suchen muss. Wenn sich die Datensätze nicht geändert haben, ermöglicht die Verwendung von TTL auch schnelle dynamische Antworten von Geräten, die GSLB ausführen.

Arten von Ressourceneintrags

Verschiedene RFCs bieten eine umfassende Liste der DNS-Ressourceneinzeichnungstypen und deren Beschreibung. In der folgenden Tabelle sind die gängigen Ressourcendatensatztypen aufgeführt.

Typ des Ressourceneintrags	Beschreibung	RFC
A	Eine Host-Adresse	RFC 1035
NS	Ein autoritativer Nameserver	RFC 1035
MD	Ein E-Mail-Ziel (Obsolete - benutze MX)	RFC 1035

Typ des Ressourceneintrags	Beschreibung	RFC			
MF	Ein Mail-Forwarder (Obsolet - benutze MX)	RFC 1035			
CNAME	The canonical name for an alias	RFC 1035	SOA	Marks the start of a zone of authority	RFC 1035
WKS	A well known service description	RFC 1035			
PTR	A domain name pointer	RFC 1035			
HINFO	Host information	RFC 1035			
MINFO	Mailbox or mail list information	RFC 1035			
MX	Mail exchange	RFC 1035			
TXT	Text strings	RFC 1035			
AAAA	IP6 Address	RFC 3596			
SRV	Server selection	RFC 2782]			

Wie GSLB DNS unterstützt

GSLB verwendet Algorithmen und Protokolle, die entscheiden, welche IP-Adresse für eine DNS-Abfrage gesendet werden muss. GSLB-Sites sind geografisch verteilt, und an jedem Standort befindet sich ein autoritativer DNS-Nameserver, der als Dienst auf der Citrix ADC Appliance ausgeführt wird.

Alle Nameserver an den verschiedenen beteiligten Standorten sind für dieselbe Domain maßgeblich. Jede der GSLB-Domänen ist eine Subdomain, für die eine Delegation konfiguriert ist. Daher sind die GSLB-Name-Server autoritativ und können einen der verschiedenen Load Balancing-Algorithmen verwenden, um zu entscheiden, welche IP-Adresse zurückgegeben werden soll.

Eine Delegation wird erstellt, indem ein Name-Server-Datensatz für die GSLB-Domäne in den übergeordneten Domänen-Datenbankdateien und einen nachfolgenden Adressdatensatz für die Nameserver hinzugefügt wird, die für die Delegierung verwendet werden. Wenn Sie beispielsweise GSLB für verwenden möchten `www.citrix.com`, kann die folgende Bind SOA-Datei verwendet werden, um Anfragen an Nameserver `www.citrix.com` zu delegieren: Netscaler1 und Netscaler2.

```
############################################################################

@ IN SOA citrix.com. hostmaster.citrix.com. (
1 ; serial
3h ; refresh
1h ; retry
1w ; expire
1h ) ; negative caching TTL
IN NS ns1
IN NS ns2
IN MX 10 mail

ns1   IN A 10.10.10.10
ns2   IN A 10.10.10.20
mail  IN A 10.20.20.50

### Old Configuration if www was not delegated to a GSLB name server
www IN A 10.20.20.50

### Updated Configuration
Netscaler1 IN A xxx.xxx.xxx.xxx
Netscaler2 IN A yyy.yyy.yyy.yyy
www IN NS Netscaler1.citrix.com.
www IN NS Netscaler2.citrix.com.
###
IN MX 20 mail2
mail2 IN A 10.50.50.20
############################################################################


<!--NeedCopy-->
```


Das Verständnis von BIND ist keine Voraussetzung für die Konfiguration von DNS. Alle konformen DNS-Server-Implementierungen verfügen über eine Methode, um die äquivalente Delegation zu erstellen. Microsoft DNS-Server können mithilfe der Anweisungen unter [Zonendelegation erstellen für die Delegation](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc785881(v=ws.10)konfiguriert werden? redirectedFrom=MSDN).

Was GSLB auf der Citrix ADC Appliance von der Verwendung des Standard-DNS-Dienstes für die Verteilung des Datenverkehrs unterscheidet, ist, dass die Citrix ADC GSLB-Sites Daten mithilfe eines proprietären Protokolls namens Metric Exchange Protocol (MEP) austauschen. Mit MdEP können die GSLB-Sites Informationen über alle anderen Websites aufbewahren. Wenn eine DNS-Anfrage eingegangen ist, berücksichtigt der Abgeordnete die GSLB-Metriken, um Informationen wie die folgenden zu ermitteln:

- Site mit der geringsten Anzahl aktueller Verbindungen
- Site, die dem LDNS-Server am nächsten liegt und die Anfrage basierend auf Round-Trip-Zeiten (RTT) gesendet hat.

Es gibt mehrere Load Balancing-Algorithmen, die verwendet werden können, aber GSLB ist ein DNS, wobei das Gehirn darunter dem Nameserver (gehostet auf der Citrix ADC Appliance) mitteilt, welche Adresse basierend auf Metriken der teilnehmenden Sites gesendet werden muss.

Weitere Vorteile, die GSLB bietet, sind die Fähigkeit, Persistenz (oder Site-Affinität) aufrechtzuerhalten. Antworten auf die eingehenden DNS-Abfragen können mit der Quell-IP-Adresse verglichen werden, um festzustellen, ob diese Adresse in der jüngsten Vergangenheit an eine bestimmte Site weitergeleitet wurde. In diesem Fall wird dieselbe Adresse in der DNS-Antwort gesendet, um sicherzustellen, dass die Clientsitzung beibehalten wird.

Eine andere Form der Persistenz wird auf Standortebene durch Verwendung von HTTP-Weiterleitungen oder HTTP-Proxy erhalten. Diese Formen der Persistenz treten auf, nachdem die DNS-Reaktion aufgetreten ist. Wenn Sie also eine HTTP-Anfrage auf einer Website erhalten, die ein Cookie enthält, um die Anfrage an eine andere teilnehmende Website zu leiten, können Sie entweder mit einer Weiterleitung antworten oder die Anfrage an die entsprechende Website stellen.

Metrisches Austauschprotokoll

Metric Exchange Protocol (MEP) wird verwendet, um die in GSLB-Berechnungen verwendeten Daten über Standorte hinweg freizugeben. Mithilfe von MEP-Verbindungen tauschen Sie drei Arten von Daten aus. Diese Verbindungen müssen über TCP-Port 3011 nicht sicher sein oder können mit SSL über TCP-Port 3009 sicher sein.

Die folgenden drei Arten von Daten werden ausgetauscht und haben ihre eigenen Intervalle und Austauschmethoden.

- **Austausch von Standortmetrik:** Dies ist ein Polling-Exchange-Modell. Wenn Site1 beispielsweise eine Konfiguration für Site2-Dienste hat, fragt jede zweite Site1 Site2 nach dem Status der GSLB-Dienste. Site2 antwortet mit dem Status und anderen Ladedetails.
- **Austausch von Netzwerkmetriken:** Dies ist der LDNS-RTT-Informationsaustausch, der im dynamischen Proximity-Load Balancing-Algorithmus verwendet wird. Dies ist ein Push-Exchange-Modell. Alle fünf Sekunden leitet jede Site ihre Daten an andere teilnehmende Websites weiter.
- **Persistenzaustausch:** Dies ist für den Sourceip-Persistenzaustausch. Dies ist auch ein Push-Exchange-Modell. Alle fünf Sekunden leitet jede Site ihre Daten an andere teilnehmende Websites weiter.

Standardmäßig werden Website-Dienste über den Abgeordneten nur basierend auf Abfrageinformationen überwacht. Wenn Sie Monitore basierend auf dem Monitorintervall binden, wird der Status aktualisiert und Sie können die Häufigkeit der Updates steuern, indem Sie das Überwachungsintervall entsprechend einstellen.

Upgradeempfehlungen für die GSLB-Bereitstellung

October 5, 2021

Dieser Abschnitt enthält Empfehlungen zur Reihenfolge, in der GSLB-Knoten in verschiedenen GSLB-Setups aktualisiert werden müssen. Es befasst sich auch mit einigen FAQs.

Hinweis: Die Citrix ADC-Appliance, von der aus die GSLB-Synchronisierung gestartet wird, wird als “Hauptsitz” und die GSLB-Sites bezeichnet, auf denen die Konfiguration als “untergeordnete Standorte” kopiert wird.

Bevor Sie mit dem Upgrade-Prozess beginnen, lesen Sie die in den folgenden Themen genannten Voraussetzungen:

- Voraussetzungen
- Aktualisieren Sie ein Paar mit hoher Verfügbarkeit.
- Aktualisieren Sie einen Cluster.

Zu beachtende Punkte beim Upgrade von GSLB-Setups

- Aktualisieren Sie in einem HA-Setup zuerst die untergeordneten Standorte und dann die Hauptwebsite.
- In einem HA-Setup werden Dienststatus möglicherweise nicht von einem älteren Build-Primärknoten zu einem neueren sekundären Build-Knoten weitergegeben. Wenn die Builds jedoch aus verschiedenen Versionen bestehen, aber dieselbe HA-Version haben, wird der Dienststatus möglicherweise weiterhin verbreitet.

- Wenn GSLB in einem Cluster konfiguriert ist, aktualisieren Sie zuerst die Nicht-Besitzer-Knoten, und aktualisieren Sie dann den Eigentümerknoten. Wenn sich ein Standort oder mehrere Standorte in einem Cluster befinden, folgen Sie an jeder Site dieselbe Upgrade-Sequenz.
- Aktivieren Sie neue GSLB-Funktionen erst, nachdem Sie alle Knoten auf einen neueren Build aktualisiert haben.
- Aktualisieren Sie alle GSLB-Knoten auf den neuesten Build. Es gibt keine funktionalen Auswirkungen auf die verfügbaren Funktionen, wenn einige der GSLB-Knoten eine ältere Version verwenden und einige der GSLB-Knoten auf eine neuere Version aktualisiert werden.

FAQ

- **Werden GSLB-Dienstzustände propagiert, wenn Instanzen verschiedene Softwareversionen ausführen?**

  GSLB MEP ist funktionsfähig, wenn Instanzen, die auf verschiedenen Versionen und GSLB-Dienstzuständen ausgeführt werden, über GSLB-Sites verteilt werden. Es gibt keine Auswirkungen auf die MEP-Kommunikation, wenn Instanzen nach einem Upgrade verschiedene Versionen ausführen.

- **Ist es empfehlenswert, während eines Upgrades Konfigurationsänderungen vorzunehmen?**

  In a GSLB setup, when a main site is being upgraded, it is not recommended to do configuration changes on any other GSLB nodes.

Zugehörige Ressourcen

Die folgenden Ressourcen enthalten Informationen zum Upgrade einer Citrix ADC-Instanz mit Citrix ADM:

- 10 Möglichkeiten, wie Citrix ADM Service einfachere Citrix ADC-Upgrades unterstützt
- Verwenden Sie den Citrix ADM Service, um Citrix ADC-Instanzen zu aktualisieren
- Verwenden Sie Citrix ADM-Software, um Citrix ADC Instanzen zu aktualisieren

Anwendungsfall: Bereitstellung einer Domainnamen-basierten Autoscale-Dienstgruppe

October 5, 2021

> **Tipp**
>
> Informationen zu den GSLB-Dienstgruppen finden Sie unter Konfigurieren einer GSLB-Dienstgruppe

Bereitstellungsszenario

Zwei Rechenzentren werden in zwei AWS-Regionen bereitgestellt, eine in Sydney und eine in North Virginia. Ein anderes Rechenzentrum wird in Azure bereitgestellt. Ein AWS-ELB in jeder AWS-Region wird zum Lastenausgleich der Anwendungsserver verwendet. ALB wird für Azure zum Lastenausgleich des Anwendungsservers verwendet. Die Citrix ADC Appliances werden für GSLB für die ELBs und ALB mithilfe der GSLB-Domänennamen-basierten Autoscale-Dienstgruppe konfiguriert.

> **Wichtig**
>
> Sie müssen die erforderlichen Sicherheitsgruppen in AWS konfigurieren und an die GSLB-Instanz anhängen. Port 53 muss in den Sicherheitsgruppen eingehende und ausgehende Regeln zugelassen sein. Außerdem müssen Ports (3009 oder 3011 je nach sicherer MEP-Konfiguration) für die MEP-Kommunikation offen sein. Für die Anwendungsüberwachung müssen die entsprechenden Ports in den ausgehenden Regeln der Sicherheitsgruppe zugelassen sein.

Die Konfigurationsschritte für das obige Bereitstellungsszenario und die entsprechenden CLI-Befehle lauten wie folgt:

1. Erstellen von Rechenzentren (dargestellt durch GSLB-Sites).

   ```
   add gslb site aws-sydney 192.0.2.2

   add gslb site aws-nvirginia 198.51.100.111

   add gslb site alb-southindia 203.0.113.6
   ```

2. Fügen Sie einen Nameserver mit der DNS-Gateway IP-Adresse hinzu, an die der GSLB-Knoten hinzugefügt wird. Dies muss in allen Rechenzentren erfolgen.

   ```
   add dns nameServer 8.8.8.8
   ```

3. Server für ELB und ALB hinzufügen.

   ```
   add server aws-sydney_server lb-sydney-1052691850.ap-southeast-2.elb.
   amazonaws.com

   add server aws-nvirginia_server LB-nvirginia-860559595.us-east-1.elb.
   amazonaws.com

   add server alb-southindia_server alb.southindia.cloudapp.azure.com
   ```

4. Fügen Sie GSLB Autoscale-Dienstgruppen für jede ELB und ALB hinzu und binden Sie jeden Server an die jeweilige Servicegruppe.


```
add gslb serviceGroup aws-nvirginia_sg HTTP -autoScale DNS -siteName
aws-nvirginia

add gslb serviceGroup aws-sydney_sg HTTP -autoScale DNS -siteName aws-
sydney

add gslb serviceGroup alb-southindia_sg HTTP -autoScale DNS -siteName
alb-southindia

bind gslb serviceGroup aws-nvirginia_sg aws-nvirginia_server 80

bind gslb serviceGroup aws-sydney_sg aws-sydney_server 80

bind gslb serviceGroup alb-southindia_sg alb-southindia_server 80
```

5. Fügen Sie einen virtuellen GSLB-Server hinzu, und binden Sie die Anwendungsdomäne und die Dienstgruppen an diesen virtuellen Server.

```
add gslb vserver gv1 HTTP

bind gslb vserver gv1 -serviceGroupName aws-nvirginia_sg

bind gslb vserver gv1 -serviceGroupName aws-sydney_sg

bind gslb vserver gv1 -serviceGroupName alb-southindia_sg
```

Anwendungsfall: Bereitstellung einer IP-Adressbasierten GSLB-Dienstgruppe

October 5, 2021

> **Tipp**
>
> Informationen zu den GSLB-Dienstgruppen finden Sie unter Konfigurieren einer GSLB-Dienstgruppe.

Bereitstellungsszenario

Wenn mehrere Anwendungen auf demselben Anwendungsserver gehostet werden, sollte die GSLB diese Anwendungen untersuchen, um zu sehen, ob die Anwendungen reagieren oder nicht. Wenn eine Anwendung nicht antwortet, muss der Benutzer an den Server weitergeleitet werden, auf dem die Anwendung UP ist. Wenn eine der Anwendungen DOWN ist, sollte der Server nicht mit DOWN gekennzeichnet werden, da die anderen Anwendungen UP sind.

Im folgenden Beispiel werden mehrere Anwendungen (HTTPS) auf einem Server in jeder GSLB-Site gehostet und daher alle diese Anwendungen auf eine IP-Adresse der jeweiligen Site aufgelöst.

Mit den GSLB-Dienstgruppen können Sie denselben Server mit einer IP-Adresse und einem Port haben, der an mehrere Dienstgruppen gebunden ist, wobei jede Dienstgruppe eine andere Anwendung darstellt.

Ein anwendungsspezifischer Monitor ist an die Dienstgruppen gebunden, die die Dienstgruppe als DOWN kennzeichnen, wenn die Anwendung DOWN ist. Wenn also eine Anwendung DOWN ist, wird nur diese Anwendung aus dem Setup und nicht vom Server entfernt.

```
```
add gslb serviceGroup app1_site1 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s1

add gslb serviceGroup app2_site1 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s1

add gslb serviceGroup app1_site2 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s2

add gslb serviceGroup app2_site2 HTTP -maxClient 0 -cip DISABLED -
    cltTimeout 180 -svrTimeout 360 -siteName s2

add lb monitor http_app2 HTTP -respCode 200 -httpRequest ”GET /testsite
    /app2.html”

add lb monitor http_app1 HTTP -respCode 200 -httpRequest ”GET /testsite
    /app1.html”

bind gslb serviceGroup app1_site1 192.0.2.140 80

bind gslb serviceGroup app1_site1 -monitorName http_app1

bind gslb serviceGroup app2_site1 192.0.2.140 80

bind gslb serviceGroup app2_site1 -monitorName http_app2

bind gslb serviceGroup app1_site2 192.0.2.142 80

bind gslb serviceGroup app1_site2 -monitorName http_app1

bind gslb serviceGroup app2_site2 192.0.2.142 80

bind gslb serviceGroup app2_site2 -monitorName http_app2
<!--NeedCopy--> ```
```

 
```

Anleitungsartikel

October 5, 2021

Die GSLB-Anleitungen enthalten Informationen über einige der wichtigen GSLB-Konfigurationen wie das Anpassen der GSLB-Konfiguration, das Konfigurieren von persistenten Verbindungen, die Notfallwiederherstellung usw.

Anpassen Ihrer GSLB-Konfiguration

Persistente Verbindungen konfigurieren

Verwalten von Clientverbindungen

Konfigurieren von GSLB für Nähe

Schützen des GSLB-Setups vor Fehlern

Konfigurieren von GSLB für Disaster Recovery

Überschreiben des statischen Näherungsverhaltens durch Konfigurieren bevorzugter Speicherorte

Konfigurieren der GSLB-Dienstauswahl über Content Switching

Konfigurieren des globalen Server-Lastausgleichs für DNS-Abfragen mit NAPTR-Einträgen

Verwenden der EDNS0-Client-Subnetzoption für den globalen Server-Lastausgleich

Beispiel für eine vollständige übergeordnete und untergeordnete Konfiguration mithilfe des Metriks-Exchange-Protokolls

Anpassen der GSLB-Konfiguration

October 5, 2021

Sobald Ihre grundlegende GSLB-Konfiguration betriebsbereit ist, können Sie sie anpassen, indem Sie die Bandbreite eines GSLB-Dienstes ändern, CNAME-basierte GSLB-Dienste, statische Nähe, dynamische RTT, persistente Verbindungen oder dynamische Gewichtungen für Dienste konfigurieren oder die GSLB-Methode ändern.

Sie können auch die Überwachung für GSLB-Dienste konfigurieren, um deren Status zu bestimmen.

Diese Einstellungen hängen von der Netzwerkbereitstellung und den Clienttypen ab, die Sie mit Ihren Servern verbinden möchten.

Ändern der maximalen Verbindungen oder der maximalen Bandbreite für einen GSLB-Dienst

Sie können die Anzahl der neuen Clients einschränken, die gleichzeitig eine Verbindung zu einem virtuellen Lastausgleichs- oder Content Switching-Server herstellen können, indem Sie die maximale Anzahl von Clients und/oder die maximale Bandbreite für den GSLB-Dienst konfigurieren, der den virtuellen Server darstellt.

So ändern Sie die maximale Clients oder Bandbreite eines GSLB-Dienstes mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die maximale Anzahl von Clientverbindungen oder die maximale Bandbreite eines GSLB-Dienstes zu ändern, und überprüfen Sie die Konfiguration:

```
set gslb service <serviceName> [-maxClients <positive_integer>] [-
   maxBandwidth <positive_integer>]
show gslb service <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
set glsb service Service-GSLB-1  -maxBandwidth 100  -maxClients 100
show gslb service Service-GSLB-1
<!--NeedCopy-->
```

So ändern Sie die maximale Clients oder Bandbreite eines GSLB-Diensts mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Services**, und doppelklicken Sie auf einen Dienst.
2. Klicken Sie in den Abschnitt **Weitere Einstellungen** und legen Sie die folgenden Parameter fest:
   - Max Clients — maxClients
   - Max. Bandbreite — maxBandwidth

Erstellen von CNAME-basierten GSLB-Diensten

Um einen GSLB-Dienst zu konfigurieren, können Sie die IP-Adresse des Servers oder einen kanonischen Namen des Servers verwenden. Wenn Sie mehrere Dienste (wie FTP und Webserver, die jeweils

auf verschiedenen Ports ausgeführt werden) von einer einzelnen IP-Adresse aus ausführen möchten oder mehrere HTTP-Dienste auf demselben Port mit unterschiedlichen Namen auf demselben physischen Host ausführen möchten, können Sie kanonische Namen (CNAMES) für die Dienste verwenden.

Beispielsweise können Sie zwei Einträge in DNS als ftp.example.com und www.example.com für FTP-Dienste und HTTP-Dienste in derselben Domäne haben, beispiel.com. CNAME-basierte GSLB-Dienste sind nützlich in einer Konfiguration mit mehreren Ebenen Domänenauflöser oder im Lastenausgleich von mehreren Ebenen. Die Konfiguration eines CNAME-basierten GSLB-Dienstes kann auch hilfreich sein, wenn sich die IP-Adresse des physischen Servers wahrscheinlich ändert.

Wenn Sie CNAME-basierte GSLB-Dienste für eine GSLB-Domäne konfigurieren und eine Abfrage für die GSLB-Domäne gesendet wird, stellt die Citrix ADC Appliance anstelle einer IP-Adresse einen CNAME bereit. Wenn der A-Eintrag für diesen CNAME-Eintrag nicht konfiguriert ist, muss der Client die CNAME-Domäne nach der IP-Adresse abfragen. Wenn der A-Eintrag für diesen CNAME-Eintrag konfiguriert ist, stellt die Citrix ADC Appliance dem CNAME den entsprechenden A-Datensatz (IP-Adresse) zur Verfügung. Die Citrix ADC Appliance verarbeitet die endgültige Auflösung der DNS-Abfrage, wie sie von der GSLB-Methode bestimmt wird. Die CNAME-Einträge können auf einer anderen Citrix ADC Appliance oder auf einem Drittanbietersystem verwaltet werden.

In einem IP-adressbasierten GSLB-Dienst wird der Status eines Dienstes durch den Status des Servers bestimmt, den er darstellt. Der Status eines CNAME-basierten GSLB-Diensts ist jedoch standardmäßig auf UP festgelegt. Die IP-Adresse (VIP) des virtuellen Servers oder das Metric Exchange Protocol (MEP) werden nicht zur Bestimmung des Zustands verwendet. Wenn ein Desktop-basierter Monitor an einen CNAME-basierten GSLB-Dienst gebunden ist, wird der Status des Dienstes anhand des Ergebnisses der Monitorsonden ermittelt.

Sie können einen CNAME-basierten GSLB-Dienst nur an einen virtuellen GSLB-Server binden, der den DNS-Eintragstyp als CNAME aufweist. Außerdem kann eine Citrix ADC Appliance höchstens einen GSLB-Dienst mit einem bestimmten CNAME-Eintrag enthalten.

Im Folgenden finden Sie einige der Funktionen, die für einen CNAME-basierten GSLB-Dienst unterstützt werden:

- GSLB-Policy basierte Site-Affinität wird unterstützt, wobei der CNAME als bevorzugter Speicherort verwendet wird.
- Quell-IP-Persistenz wird unterstützt. Der Persistenzeintrag enthält die CNAME-Informationen anstelle der IP-Adresse und des Ports des ausgewählten Dienstes.

Im Folgenden sind die Einschränkungen von CNAME-basierten GSLB-Diensten aufgeführt:

- Standortpersistenz wird nicht unterstützt, da der Dienst, auf den ein CNAME verweist, an jedem Standort eines Drittanbieters vorhanden sein kann.
- Die Antwort mit mehreren IP-Adressen wird nicht unterstützt, da eine Domäne nicht mehrere CNAME-Einträge haben kann.

- Quell-IP-Hash und Round-Robin sind die einzigen unterstützten Load Balancing-Methoden. Die statische Proximity-Methode wird nicht unterstützt, da ein CNAME keiner IP-Adresse zugeordnet ist und die statische Nähe nur gemäß den IP-Adressen beibehalten werden kann.

Hinweis: Die Funktion “Leer-Down-Response” sollte auf dem virtuellen GSLB-Server aktiviert sein, an den Sie den CName-basierten GSLB-Dienst binden. Wenn Sie die Funktion “Leer-Down-Response” aktivieren, wenn ein virtueller GSLB-Server DOWN oder deaktiviert ist, enthält die Antwort auf eine DNS-Abfrage für die an diesen virtuellen Server gebundenen Domänen einen leeren Datensatz ohne IP-Adressen anstelle eines Fehlercodes.

So erstellen Sie einen CNAME-basierten GSLB-Dienst mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add gslb service <serviceName> -cnameEntry <string> -siteName <string>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add gslb service Service-GSLB-1 -cnameEntry transport.mycompany.com -
     siteName Site-GSLB-East-Coast
2 add gslb service Service-GSLB-2 -cnameEntry finance.mycompany.com -
     siteName Site-GSLB-West-Coast
3 <!--NeedCopy-->
```

So erstellen Sie einen CNAME-basierten GSLB-Dienst mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Services**.
2. Erstellen Sie einen Service, und legen Sie den **Typ auf Kanonischer Name Based** fest.

Konfigurieren des Übergangsstatus außerhalb des Dienstes (TROFS) in GSLB

Wenn Sie die Persistenz auf einem virtuellen GSLB-Server konfigurieren, an den ein Dienst gebunden ist, erfüllt der Dienst weiterhin Anforderungen vom Client, auch nachdem er deaktiviert ist, und akzeptiert neue Anforderungen oder Verbindungen nur, um die Persistenz zu berücksichtigen. Nach einem konfigurierten Zeitraum, der als graaceful Shutdown bezeichnet wird, werden keine neuen Anforderungen oder Verbindungen an den Dienst weitergeleitet, und alle vorhandenen Verbindungen werden geschlossen.

Wenn Sie einen Dienst deaktivieren, können Sie mithilfe des Arguments delay einen ordnungsgemäßen Herunterfahren in Sekunden angeben. Wenn der Dienst während des ordnungsgemäßen Herunterfahrens an einen virtuellen Server gebunden ist, wird sein Status als Out of Service angezeigt.

Dynamische Gewichtungen für Dienste konfigurieren

In einem typischen Netzwerk gibt es Server, die eine höhere Kapazität für den Datenverkehr haben als andere. Bei einer regulären Lastausgleichskonfiguration wird die Last jedoch gleichmäßig über alle Dienste verteilt, obwohl verschiedene Dienste Server mit unterschiedlichen Kapazitäten darstellen.

Um Ihre GSLB-Ressourcen zu optimieren, können Sie dynamische Gewichtungen auf einem virtuellen GSLB-Server konfigurieren. Die dynamischen Gewichtungen können entweder auf der Gesamtzahl der an den virtuellen Server gebundenen Dienste oder auf der Summe der Gewichtungen der einzelnen an den virtuellen Server gebundenen Dienste basieren. Die Verkehrsverteilung basiert dann auf den Gewichten, die für die Dienste konfiguriert wurden.

Wenn dynamische Gewichtungen auf dem virtuellen GSLB-Server konfiguriert sind, werden Anforderungen entsprechend der Lastausgleichsmethode, der Gewichtung des GSLB-Dienstes und der dynamischen Gewichtung verteilt. Das Produkt des Gewichts des GSLB-Dienstes und des dynamischen Gewichts wird als kumulatives Gewicht bezeichnet. Wenn also dynamische Gewichtung auf dem virtuellen GSLB-Server konfiguriert ist, werden Anforderungen auf der Grundlage der Lastausgleichsmethode und des kumulativen Gewichts verteilt.

Wenn die dynamische Gewichtung für einen virtuellen Server deaktiviert ist, wird der numerische Wert auf 1 festgelegt. Dadurch wird sichergestellt, dass das kumulative Gewicht jederzeit eine Ganzzahl ungleich Null ist.

Die dynamische Gewichtung kann auf der Gesamtzahl der aktiven Dienste basieren, die an virtuelle Server mit Lastenausgleich gebunden sind, oder auf den Gewichtungen, die den Diensten zugewiesen sind.

Betrachten Sie eine Konfiguration mit zwei GSLB-Sites, die für eine Domäne konfiguriert sind, und jeder Standort verfügt über zwei Dienste, die dem Client dienen können. Wenn ein Dienst an einem beliebigen Standort ausfällt, muss der andere Server in dieser Site doppelt so viel Datenverkehr verarbeiten wie ein Dienst am anderen Standort. Wenn die dynamische Gewichtung auf der Anzahl der aktiven Dienste basiert, hat die Website mit beiden aktiven Diensten doppelt so viel Gewicht wie die Website mit einem ausgefallenen Service und erhält somit doppelt so viel Traffic.

Alternativ können Sie eine Konfiguration in Betracht ziehen, bei der die Dienste am ersten Standort Server darstellen, die doppelt so leistungsfähig sind wie Server am zweiten Standort. Wenn dynamisches Gewicht auf den Gewichten basiert, die den Diensten zugewiesen sind, kann doppelt so viel Datenverkehr an die erste Site gesendet werden wie an die zweite.

Hinweis: Weitere Informationen zum Zuweisen von Gewichtungen zu Lastenausgleichsdiensten finden Sie unter Zuweisen von Gewichten zu Diensten.

Betrachten Sie als Veranschaulichung der Berechnung der dynamischen Gewichtung einen virtuellen GSLB-Server, der über einen GSLB-Dienst gebunden ist. Der GSLB-Dienst stellt einen virtuellen Lastausgleichsserver dar, der wiederum zwei an ihn gebundene Dienste hat. Das dem GSLB-Dienst zugewiesene Gewicht beträgt 3. Die den beiden Diensten zugewiesenen Gewichte sind 1 und 2. Wenn in diesem Beispiel die dynamische Gewichtung auf:

- **Deaktiviert**: Das kumulative Gewicht des virtuellen GSLB-Servers ist das Produkt des dynamischen Gewichts (deaktiviert = 1) und des Gewichts des GSLB-Dienstes (3). Das kumulative Gewicht beträgt also 3.
- **SERVICECOUNT**: Die Anzahl ist die Summe der Anzahl der Dienste, die an die virtuellen Lastausgleichsserver gebunden sind, die dem GSLB-Dienst entsprechen (2), und das kumulative Gewicht ist das Produkt des dynamischen Gewichts (2) und des Gewichts des GSLB-Dienstes (3), also 6.
- **SERVICEWEIGHT**: Das dynamische Gewicht ist die Summe der Gewichte der Dienste, die an die virtuellen Lastausgleichsserver gebunden sind, die dem GSLB-Dienst entsprechen (3), und das kumulative Gewicht ist das Produkt des dynamischen Gewichts (3) und des Gewichts des GSLB-Dienstes (3), also 9.

Hinweis: Dynamische Gewichtungen sind nicht anwendbar, wenn virtuelle Content Switching-Server konfiguriert sind.

So konfigurieren Sie einen virtuellen GSLB-Server für die Verwendung dynamischer Gewichtungen mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set gslb vserver <name> -dynamicWeight SERVICECOUNT | SERVICEWEIGHT
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver vserver-GSLB-1 -dynamicWeight SERVICECOUNT
<!--NeedCopy-->
```


So legen Sie den virtuellen GSLB-Server für die Verwendung dynamischer Gewichtungen mit dem Konfigurationsdienstprogramm fest

1. Navigieren Sie zu Traffic Management > GSLB > Virtuelle Server, doppelklicken Sie auf den virtuellen GSLB-Server, dessen Methode Sie ändern möchten (z. B. vServer-GSLB-1).
2. Klicken Sie auf den Abschnitt **Methode**, und wählen Sie in der Dropdownliste **Dynamisches Gewicht** die Option **SERVICECOUNT** oder **SERVICEWEIGHT** aus.

Wie konfiguriere ich Persistenz in GSLB

October 5, 2021

Persistenz stellt sicher, dass eine Reihe von Clientanforderungen für einen bestimmten Domänennamen an dasselbe Rechenzentrum gesendet wird, anstatt Lastenausgleich zu werden. Wenn die Persistenz für eine bestimmte Domäne konfiguriert ist, hat sie Vorrang vor der konfigurierten GSLB-Methode. Sie können Persistenz für Bereitstellungen verwenden, bei denen Informationen im Zusammenhang mit einer Clienttransaktion lokal in einer Instanz gespeichert werden, die die ersten Anforderungen erfüllt hat. Zum Beispiel die Bereitstellungen für E-Commerce, die einen Einkaufswagen verwenden, in dem der Server den Status der Verbindung beibehalten muss, um die Transaktion zu verfolgen. Die Citrix ADC Appliance wählt ein Rechenzentrum aus, um eine Clientanfrage zu bearbeiten. Wenn die Persistenz aktiviert ist, leitet es die gleiche IP-Adresse des ausgewählten Rechenzentrums für alle nachfolgenden DNS-Anfragen (Domain Name System) weiter. Wenn eine Persistenzsitzung auf ein Rechenzentrum verweist, das DOWN ist, verwendet die Citrix ADC Appliance die konfigurierte GSLB-Methode, um ein neues Rechenzentrum auszuwählen. Es wird dann für spätere Anfragen des Kunden hartnäckig.
Für die Persistenz in GSLB muss derselbe Satz von Persistenzkennungen (PersistID) auf den virtuellen GSLB-Servern in allen Rechenzentren konfiguriert werden. Das GSLB-Modul verwendet den Persistenzbezeichner, um einen virtuellen GSLB-Server eindeutig zu identifizieren. Wenn die Quell-IP-Persistenz auf dem virtuellen GSLB-Server aktiviert ist, werden die Persistenzsitzungen auch im Rahmen des Metrikaustauschs ausgetauscht. Damit die Citrix ADC Appliance die Persistenz über mehrere Standorte hinweg unterstützt, muss persistenzbezogene Konfiguration auf allen teilnehmenden GSLB-Sites durchgeführt werden. Citrix empfiehlt Persistenz in GSLB für statusbehaftete Anwendungen, bei denen Clients sich für die nachfolgenden Anforderungen erneut mit derselben Anwendungsinstanz verbinden müssen.

Sie können Persistenz in GSLB auf folgende Weise erreichen:

- Persistenz auf dem virtuellen GSLB-Server
- Beharrlichkeit der Website bei GSLB-Diensten

Persistenz auf dem virtuellen GSLB-Server

Die Persistenz auf dem virtuellen GSLB-Server wird während der DNS-Anfragen verwendet. Die Quell-IP-Adresse der DNS-Anfrage wird verwendet, um eine Persistenzsitzung zwischen dem Client und dem Rechenzentrum zu erstellen. DNS-Clients sind im Allgemeinen die lokalen DNS (LDNS) oder DNS-Gateways, die eine Reihe von Clients hinter ihnen (in ISPs) weiterführen. Die Persistenz auf einem virtuellen GSLB-Server ist unabhängig von Anwendungsprotokollen.
Im Allgemeinen werden mehrere DNS-Gateways oder lokale Domänennamenserver (LDNS) im Clientnetzwerk konfiguriert. Citrix empfiehlt Ihnen, eine geeignete Persistenzmaske zu konfigurieren, da der Client für die nachfolgenden DNS-Anfragen unabhängig von den Upstream-LDNS-Geräten, die zur Verbindung mit der ADC-Appliance verwendet wurden, in der Lage ist, bei demselben Rechenzentrum zu bestehen, das die früheren Anfragen erfüllt hat. Nachdem die Persistenzsitzung für eine LDNS-IP-Adresse erstellt wurde, erhalten alle Endclients, die sich mit diesem LDNS verbinden, die gleiche IP-Adresse des Rechenzentrums.

Beharrlichkeit der Website bei GSLB-Diensten

Die Standortpersistenz wird während der Verarbeitung der Anwendungsanfragen wirksam. Die Standortpersistenz funktioniert nur für HTTP- und HTTPS-Datenverkehr, da die Persistenz mit HTTP-Cookie erreicht wird. Da Cookies auf HTTP-Clients (Browsern) verwaltet werden, geben sie Einblick in die Kunden, die hinter den DNS-Gateways sitzen. Wenn Sie Cookies verwenden, um Persistenz für Kunden zu erreichen, werden für jeden eingehenden Client keine Ressourcen auf der ADC-Appliance verbraucht. Wenn Sie einen GSLB-Dienst mit einer Verzögerungszeit herunterbringen, geht der Dienst in den Status “Out Of Service” (TROFS) über. Persistenz wird unterstützt, solange sich der Dienst im Status UP oder TROFS befindet. Das heißt, wenn derselbe Client innerhalb der angegebenen Verzögerungszeit eine Anforderung für denselben Dienst sendet, nachdem ein Dienst als TROFS markiert wurde, wird die Anfrage von derselben GSLB-Site (Rechenzentrum) bearbeitet.

Wenn Sie über einen Alias auf eine Anwendung zugreifen, stellen Sie sicher, dass der CNAME-Datensatz auch auf der Citrix ADC Appliance konfiguriert ist. In einer übergeordneten und untergeordneten Topologie funktioniert die Standortpersistenz nicht, wenn Sie über einen Alias auf eine Anwendung zugreifen.

> Hinweis:
>
> Wenn der Verbindungsproxy als Standortpersistenzmethode angegeben ist und Sie auch die Persistenz auf virtuellen LB-Servern konfigurieren möchten, wird die Quell-IP-Persistenz nicht empfohlen. Wenn die Verbindung über die Proxy-Proxy-Klasse geführt wird, wird eine IP-Adresse verwendet, die sich im Besitz der ADC-Appliance befindet, und nicht die tatsächliche IP-Adresse des Clients.
> Konfigurieren Sie eine geeignete Persistenz, die keine Quell-IP der HTTP (S) -Anfrage verwendet,

> um den Client zu identifizieren, beispielsweise die Cookie-Persistenz oder die regelbasierte Persistenz.

Persistenz basierend auf Quell-IP-Adresse konfigurieren

Wenn die Quell-IP-Persistenz auf dem virtuellen GSLB-Server konfiguriert ist, werden Persistenzsitzungen für die Quell-IP-Adresse der DNS-Anfrage erstellt. Abhängig von der Funktion Extended Client Subnet (ECS) wird die Quell-IP-Adresse der DNS-Anfrage einem der folgenden Punkte entnommen:

- Die Quell-IP im IP-Header des eingehenden DNS-Request-Pakets
- Die Option ECS in der DNS-Anfrage Weitere Informationen zu ECS finden Sie unter Verwenden der EDNS0-Client-Subnetzoption für den globalen Server-Lastenausgleich.

Persistenzsitzungen für einen Client dauern bis zum Persistenz-Timeout. Nach Ablauf des Timeout-Zeitraums werden bestehende Persistenzsitzungen gelöscht. Für nachfolgende Anfragen wird eine neue GSLB-Entscheidung getroffen und eine andere IP-Adresse des GSLB-Dienstes kann ausgewählt werden.
Die Quell-IP-Persistenz auf dem virtuellen GSLB-Server und die Standortpersistenz des GSLB-Dienstes ergänzen sich gegenseitig. Wenn die Quell-IP-Persistenz auf dem virtuellen GSLB-Server deaktiviert ist, wählt der virtuelle GSLB-Server jedes Mal einen anderen GSLB-Dienst aus, wenn der DNS versucht, die Auflösung durchzuführen. Der Client verbindet sich auch mit einem anderen GSLB-Dienst und dem Rechenzentrum, das den Anwendungsanforderungsproxy die Verbindung mit dem Rechenzentrum erhält, das dem Client zuerst bedient hat. Dies könnte zu einer gewissen Latenz führen. Durch die Aktivierung der Quell-IP-Persistenz auf dem virtuellen GSLB-Server können daher häufig mehrere Hops für Anwendungsanfragen vermieden werden. Wenn die Quell-IP-Persistenzsitzung abgelaufen ist und der Client danach erneut eine Verbindung herstellt, verbindet die Standortpersistenz den Client mit dem Rechenzentrum, das den Client ursprünglich bedient hat. Wenn der Client eine Verbindung über ein DNS-Gateway herstellt, das nicht in den konfigurierten Persistenzmasken-Bereich fällt, hilft auch der Standortpersistenz den Clients, sich an das Rechenzentrum zu halten, das die erste Anfrage bedient hat.

So konfigurieren Sie die Persistenz basierend auf der Quell-IP-Adresse über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set gslb vserver <name> -persistenceType (SOURCEIP|NONE) -persistenceId
    <positive_integer> [-persistMask <netmask>]  - [timeout <mins>]
<!--NeedCopy-->
```

Beispiel:


```
set gslb vserver vserver-GSLB-1 -persistenceType SOURCEIP -
    persistenceId 23 -persistMask 255.255.255.255  - timeout 2
<!--NeedCopy-->
```

So konfigurieren Sie Persistenz basierend auf der Quell-IP-Adresse über die GUI

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server** und doppelklicken Sie auf den virtuellen GSLB-Server, dessen Methode Sie ändern möchten (z. B. vServer-GSLB-1).
2. Klicken Sie auf den Abschnitt **Persistenz**, und wählen Sie in der Dropdownliste **Persistenz** die Option **SOURCEIP** aus, und legen Sie die folgenden Parameter fest:
   - Persistenz-ID — persistenceID
   - Timeout — Timeout
   - IPv4-Netzmaske oder IPv6-Maskenlänge — persistMask

Konfigurieren Sie die Persistenz der Website basierend auf HTTP-Cookies

Die Standortpersistenz wird mithilfe von HTTP-Cookies (bekannt als “Site-Cookie”) erreicht, um den Client wieder mit demselben Server zu verbinden. Wenn die GSLB-Appliance auf eine Client-DNS-Anfrage durch Senden der IP-Adresse der ausgewählten GSLB-Site antwortet, sendet der Client eine HTTP-Anfrage an diese GSLB-Site. Der Anwendungsendpunkt auf dieser GSLB-Site fügt dem HTTP-Header ein Site-Cookie hinzu, und die Standortpersistenz ist in Kraft.
Wenn der Client eine DNS-Abfrage sendet, nachdem der Client-Cache abgelaufen ist, wird die DNS-Anfrage möglicherweise an eine andere GSLB-Site weitergeleitet. Die neue GSLB-Site verwendet das im Kopfzeilen der Clientanforderung vorhandene Website-Cookie, um die Persistenz zu implementieren. Die Funktion für die Standortpersistenz wird unter den folgenden Bedingungen aktiv:

- Wenn der Domainname im Host-Header mit einer der GSLB-Domains übereinstimmt
- Wenn die Standortpersistenz für den GSLB-Dienst aktiviert ist, der den virtuellen Server darstellt, der den Anwendungsdatenverkehr empfängt.

Das Site-Cookie enthält Informationen über den ausgewählten GSLB-Dienst, auf dem der Client eine dauerhafte Verbindung hat. Wenn der GSLB-Dienst, auf den das Cookie zeigt, DOWN oder aus der GLSB-Konfiguration entfernt wird, verarbeitet der virtuelle Server, der den Datenverkehr empfängt, den Datenverkehr weiter. Der Cookie-Ablauf basiert auf dem Cookie-Zeitlimit, das auf der Citrix ADC Appliance konfiguriert wurde. Wenn die Namen des virtuellen Servers nicht auf allen Sites identisch sind, müssen Sie die Persistenzkennung verwenden. Die eingefügten Cookies entsprechen RFC 2109.

Citrix ADC unterstützt zwei Arten von Standortpersistenz:

- Proxy für Verbindung
- HTTP-Umleitung

Proxy für Verbindung

Im Verbindungsproxy-Modus der Standortpersistenz führt das Rechenzentrum, das die nachfolgende Anwendungsanforderung empfängt, die folgenden Aufgaben aus, um eine Verbindung herzustellen:

1. Erstellt eine Verbindung mit der GSLB-Site, die das Site-Cookie eingefügt hat.
2. Proxy der Kundenanfrage an die ursprüngliche Site.

   > **Hinweis:**
   >
   > Der Proxyserver stellt mithilfe der folgenden Details eine Verbindung mit der ursprünglichen Site her:
   >
   > ```
   > 1 -  Der SNIP der neuen Site ist die Quell-IP-Adresse.
   > ```
   >
   > - Die öffentliche IP-Adresse des GSLB-Dienstes der ursprünglichen Site ist die Ziel-IP-Adresse.
   > - Ein flüchtiger Port ist der Quellport und GSLB-Dienstport ist der Zielport.
   > - Verwendet je nach GSLB-Diensttyp entweder HTTP- oder HTTPS-Protokolle.

3. Erhält eine Antwort von der ursprünglichen GSLB-Site.
4. Lässt diese Antwort an den Kunden zurück.
5. Schließt die Verbindung.

HTTP-Umleitung

Wenn die GSLB-Konfiguration HTTP-Umleitungspersistenz verwendet, leitet die neue Site die Anforderung an die Site um, die das Cookie ursprünglich eingefügt hat. Der Domainname in der Umleitungs-URL ist die Site-Domain. Stellen Sie sicher, dass sowohl Cookies als auch SSL-Zertifikate sowohl für die GSLB-Domain als auch für die Site-Domain gelten. Um Cookies sowohl für GSLB als auch für die Site-Domain anzuwenden, muss die Cookie-Domain die Website der GSLB-Domain sein. Um SSL-Zertifikate sowohl auf GSLB als auch auf die Site-Domain anzuwenden, muss das an den virtuellen SSL-Server gebundene Zertifikat ein Platzhalterzertifikat sein.

Verbindungsproxy tritt auf, wenn die folgenden Bedingungen erfüllt sind:

- Es werden Anfragen für eine an GSLB beteiligte Domain gesendet. Die Domäne wird aus dem URL/Host-Header abgerufen.
- Für den lokalen GSLB-Dienst ist der Verbindungsproxy aktiviert.
- Die Anforderung enthält ein gültiges Cookie, das die IP-Adresse eines aktiven GSLB-Remote-Dienstes enthält.

> **Hinweis:**
>
> In einer GSLB-Eltern-Kind-Konfiguration funktioniert der Verbindungsproxy wie vorgesehen, auch wenn ein GSLB-Dienst nicht auf einer untergeordneten Site konfiguriert ist. Wenn Sie jedoch über eine zusätzliche Konfiguration wie Clientauthentifizierung, Client-IP-Adresseneinfügung oder andere SSL-spezifische Anforderungen verfügen, müssen Sie einen expliziten GSLB-Dienst auf der Site hinzufügen und entsprechend konfigurieren.
>
> Weitere Informationen zur Eltern-Kind-Topologie finden Sie unter Bereitstellung von Eltern-Kind-Topologie mit dem MEP-Protokoll.

So legen Sie die Persistenz basierend auf HTTP-Cookies über die Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set gslb service <serviceName> -sitePersistence (ConnectionProxy [-
   sitePrefix <prefix>] | HTTPredirect -sitePrefix <prefix>)
<!--NeedCopy-->
```

Beispiel:

```
set gslb service service-GSLB-1 -sitePersistence ConnectionProxy
set gslb service service-GSLB-1 -sitePersistence HTTPRedirect -
   sitePrefix vserver-GSLB-1
<!--NeedCopy-->
```

So legen Sie die Persistenz basierend auf Cookies über die GUI fest

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Services** und wählen Sie den Dienst aus, den Sie für die Standortpersistenz konfigurieren möchten (z. B. service-GSLB-1).
2. Klicken Sie auf den Abschnitt **Site-Persistenz** und legen Sie die Persistenz basierend auf Cookies fest.

Verwalten von Clientverbindungen

October 5, 2021

Um die Verwaltung von Clientverbindungen zu erleichtern, können Sie die verzögerte Bereinigung von Verbindungen zum virtuellen Server aktivieren. Anschließend können Sie den lokalen DNS-Datenverkehr verwalten, indem Sie DNS-Richtlinien konfigurieren.

Verzögerte Bereinigung virtueller Serververbindungen aktivieren

Der Status eines virtuellen Servers hängt von den Zuständen der an ihn gebundenen Dienste ab, und der Status jedes Dienstes hängt von den Monitoren ab, die an ihn gebunden sind. Wenn ein Server langsam oder heruntergefahren ist, wird ein Timeout der Überwachung geprüft, und der Dienst, der den Server darstellt, wird als DOWN markiert. Ein virtueller Server wird nur dann als DOWN markiert, wenn alle an ihn gebundenen Dienste als DOWN markiert sind. Sie können Dienste und virtuelle Server so konfigurieren, dass entweder alle Verbindungen beendet werden, wenn sie ausfallen, oder dass die Verbindungen durchlaufen. Letztere Einstellung gilt für Situationen, in denen ein Dienst aufgrund eines langsamen Servers als DOWN markiert ist.

Wenn Sie die Option Down-State-Flush konfigurieren, führt die Citrix ADC Appliance eine verzögerte Bereinigung von Verbindungen zu einem heruntergeführten GSLB-Dienst durch.

So aktivieren Sie die verzögerte Bereinigung von virtuellen Serververbindungen mit der Befehlszeilenschnittstelle

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

```
set gslb service <name> -downStateFlush (ENABLED | DISABLED)
show gslb service <name>
<!--NeedCopy-->
```

Beispiel:

```
set gslb service Service-GSLB-1 -downStateFlush ENABLED
Done

show gslb service Service-GSLB-1
Done
<!--NeedCopy-->
```


So aktivieren Sie die verzögerte Bereinigung von virtuellen Serververbindungen mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Services** und doppelklicken Sie auf den Dienst.
2. Klicken Sie auf den Abschnitt **Weitere Einstellungen**, und wählen Sie die Option **Abwärtszustand Flush** aus.

Verwalten des lokalen DNS-Datenverkehrs mithilfe von DNS-Richtlinien

Sie können DNS-Richtlinien verwenden, um Standortaffinität zu implementieren, indem Sie den Datenverkehr von der IP-Adresse eines lokalen DNS-Resolvers oder Netzwerkes zu einer vordefinierten GSLB-Site leiten. Dies wird konfiguriert, indem DNS-Richtlinien mit DNS-Ausdrücken erstellt und die Richtlinien global auf der Citrix ADC Appliance gebunden werden.

DNS-Ausdrücke

Die Citrix ADC Appliance stellt bestimmte vordefinierte DNS-Ausdrücke bereit, die zum Konfigurieren von domänenspezifischen Aktionen verwendet werden können. Solche Aktionen können beispielsweise bestimmte Anforderungen löschen, eine bestimmte Ansicht für eine bestimmte Domäne auswählen oder bestimmte Anforderungen an einen bestimmten Speicherort umleiten.

Diese DNS-Ausdrücke (auch *Regeln*genannt) werden kombiniert, um DNS-Richtlinien zu erstellen, die dann global auf der Citrix ADC Appliance gebunden sind.

Es folgt die Liste der vordefinierten DNS-Qualifikationen, die auf der Citrix ADC Appliance verfügbar sind:

- CLIENT.UDP.DNS.DOMAIN.EQ (Domainname)
- CLIENT.UDP.DNS.IS_AREC
- CLIENT.UDP.DNS.IS_AAAAREC
- CLIENT.UDP.DNS.IS_SRVREC
- CLIENT.UDP.DNS.IS_MXREC
- CLIENT.UDP.DNS.IS_SOAREC
- CLIENT.UDP.DNS.IS_PTRREC
- CLIENT.UDP.DNS.IS_CNAME
- CLIENT.UDP.DNS.IS_NSREC
- CLIENT.UDP.DNS.IS_ANYREC

Der DNS-Ausdruck CLIENT.UDP.DNS.DOMAIN kann mit Zeichenfolgenausdrücken verwendet werden. Wenn Sie Domänennamen als Teil des Ausdrucks verwenden, müssen diese mit einem Punkt (.) enden. Beispiel: CLIENT.UDP.DNS.DOMAIN.ENDSWITH (abc.com.)

So erstellen Sie einen Ausdruck mit dem Konfigurationsdienstprogramm

1. Klicken Sie auf das Symbol neben dem Textfeld Ausdruck. Klicken Sie auf Hinzufügen. (Lassen Sie die Dropdownlistenfelder Flow Type und Protokoll leer.) Gehen Sie folgendermaßen vor, um eine Regel zu erstellen.
2. Wählen Sie im Feld Qualifier einen Kriterium aus (z. B. LOCATION).
3. Wählen Sie im Feld Operator einen Operator aus (z. B. ==).
4. Geben Sie im Feld Wert einen Wert ein (z. B. Asien, Japan…).
5. Klicken Sie auf OK. Klicken Sie auf Erstellen und auf Schließen. Die Regel wird erstellt.
6. Klicken Sie auf OK.

Konfigurieren von DNS-Aktionen

Eine DNS-Richtlinie enthält den Namen einer DNS-Aktion, die ausgeführt werden soll, wenn die Richtlinienregel TRUE ausgewertet wird. Eine DNS-Aktion kann eine der folgenden Aktionen ausführen:

- Senden Sie dem Client eine IP-Adresse, für die Sie eine DNS-Ansicht konfiguriert haben. Weitere Informationen zu DNS-Ansichten finden Sie unter Hinzufügen von DNS-Ansichten.
- Senden Sie dem Client die IP-Adresse eines GSLB-Dienstes, nachdem Sie auf eine Liste der bevorzugten Speicherorte verwiesen haben, die das statische Näherungsverhalten außer Kraft setzen. Weitere Informationen zu bevorzugten Standorten finden Sie unter Überschreiben des statischen Näherungsverhaltens durch Konfigurieren bevorzugter Standorte.
- Senden Sie dem Client eine bestimmte IP-Adresse, die durch die Auswertung der DNS-Abfrage oder -Antwort (DNS-Antwort-Rewrite) bestimmt wird.
- Leiten Sie eine Anforderung an den Nameserver weiter, ohne eine Suche im DNS-Cache der Appliance durchzuführen.
- Lassen Sie eine Anfrage.

Sie können keine DNS-Aktion zum Löschen einer DNS-Anforderung oder zum Umgehen des DNS-Cache auf der Appliance erstellen. Wenn Sie eine DNS-Anforderung löschen möchten, verwenden Sie die integrierte Aktion DNS_default_act_drop. Wenn Sie den DNS-Cache umgehen möchten, verwenden Sie die integrierte Aktion DNS_default_act_cacheByPass. Beide Aktionen sind zusammen mit benutzerdefinierten Aktionen in den Dialogfeldern DNS-Richtlinie erstellen und DNS-Richtlinie konfigurieren verfügbar. Diese integrierten Aktionen können nicht geändert oder entfernt werden.

So konfigurieren Sie eine DNS-Aktion mit der Befehlszeilenschnittstelle

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


```
add dns action <actionName> <actionType> (-IPAddress <ip_addr |
    ipv6_addr> ... | -viewName <string> | -preferredLocList <string>
    ...) [-TTL <secs>]

show dns action [<actionName>]
<!--NeedCopy-->
```

Beispiele

Beispiel 1: Konfigurieren von DNS-Antwort-Rewrite. Die folgende DNS-Aktion sendet dem Client eine vorkonfigurierte IP-Adresse, wenn die Richtlinie, an die die Aktion gebunden ist, auf true ausgewertet wird:

```
add dns action dns_act_response_rewrite Rewrite_Response -IPAddress
    192.0.2.20 192.0.2.56 198.51.100.10
 Done

show dns action dns_act_response_rewrite
1)  ActionName:  dns_act_response_rewrite ActionType:  Rewrite_Response
     TTL:  3600              IPAddress:  192.0.2.20 192.0.2.56
    198.51.100.10
 Done
<!--NeedCopy-->
```

Beispiel 2: Konfigurieren einer DNS-View basierten Antwort. Die folgende DNS-Aktion sendet dem Client eine IP-Adresse, für die Sie eine DNS-Ansicht konfiguriert haben:

```
add dns action send_ip_from_view_internal_ip ViewName -viewName
    view_internal_ip
Done

show dns action send_ip_from_view_internal_ip
1)  ActionName:  send_ip_from_view_internal_ip ActionType:  ViewName
      ViewName:  view_internal_ip
 Done
<!--NeedCopy-->
```

Beispiel 3: Konfigurieren einer Antwort basierend auf einer Liste der bevorzugten Sites. Die folgende DNS-Aktion sendet dem Client die IP-Adresse, die dem bevorzugten Speicherort entspricht, den er aus der angegebenen Liste von Speicherorten auswählt:


```
add dns action send_preferred_location GslbPrefLoc -preferredLocList NA
    .tx.ns1.\*.\*.* NA.tx.ns2.\*.\*.* NA.tx.ns3.\*.\*.*
Done

show dns action  send_preferred_location
1)  ActionName:  send_preferred_location ActionType:  GslbPrefLoc
    PreferredLocList:  "NA.tx.ns1.\*.\*.\*" "NA.tx.ns2.\*.\*.\*" "NA.tx.
    ns3.\*.\*.*"
 Done
<!--NeedCopy-->
```

So konfigurieren Sie eine DNS-Aktion mithilfe des Citrix ADC Konfigurationsdienstprogramms

1. Navigieren Sie zu Traffic Management > DNS > Aktionen, erstellen oder bearbeiten Sie eine DNS-Aktion.
2. Legen Sie im Dialogfeld DNS-Aktion erstellen oder DNS-Aktion konfigurieren die folgenden Parameter fest:
   - Aktionsname (kann nicht für eine vorhandene DNS-Aktion geändert werden)
   - Typ (kann für eine vorhandene DNS-Aktion nicht geändert werden)
     Führen Sie einen der folgenden Schritte aus, um den Parameter
     Type festzulegen:
     - Um eine DNS-Aktion zu erstellen, die einer DNS-Ansicht zugeordnet ist, wählen Sie Namen anzeigen. Wählen Sie dann in der Liste Ansichtsname die DNS-Ansicht aus, die Sie in der Aktion verwenden möchten.
     - Um eine DNS-Aktion mit einer bevorzugten Standortliste zu erstellen, wählen Sie Liste der bevorzugten Sites aus. Geben Sie unter Bevorzugter Speicherort einen Speicherort ein, und klicken Sie dann auf Hinzufügen. Fügen Sie beliebig viele DNS-Sites hinzu.
     - Um eine DNS-Aktion für das Umschreiben einer DNS-Antwort auf der Grundlage der Richtlinienbewertung zu konfigurieren, wählen Sie Antwort umschreiben aus. Geben Sie unter IP-Adresse eine IP-Adresse ein, und klicken Sie dann auf Hinzufügen. Fügen Sie beliebig viele IP-Adressen hinzu.
   - TTL (gilt nur für den Aktionstyp Antwort umschreiben)

Konfigurieren von DNS-Richtlinien

DNS-Richtlinien funktionieren auf einer Standortdatenbank, die statische und benutzerdefinierte IP-Adressen verwendet. Die Attribute der eingehenden lokalen DNS-Anforderung werden als Teil eines Ausdrucks definiert, und die Zielsite wird als Teil einer DNS-Richtlinie definiert. Beim Definieren von

Aktionen und Ausdrücken können Sie ein Paar von einfachen Anführungszeichen (‘) als Platzhalterkennung verwenden, um mehr als eine Position anzugeben. Wenn eine DNS-Richtlinie konfiguriert ist und eine GSLB-Anforderung empfangen wird, wird zuerst die benutzerdefinierte IP-Adressdatenbank nach einem Eintrag abgefragt, der die Standortattribute für die Quelle definiert:

- Wenn eine DNS-Abfrage von einem LDNS stammt, werden die Eigenschaften des LDNS anhand der konfigurierten Richtlinien ausgewertet. Wenn sie übereinstimmen, wird eine entsprechende Aktion (Standortaffinität) ausgeführt. Wenn die LDNS-Eigenschaften mit mehr als einem Standort übereinstimmen, wird die Anforderung zwischen den Sites ausgeglichen, die den LDNS-Merkmalen entsprechen.
- Wenn der Eintrag nicht in der benutzerdefinierten Datenbank gefunden wird, wird die statische IP-Adressdatenbank nach einem Eintrag abgefragt, und wenn eine Übereinstimmung vorliegt, wird die obige Richtlinienbewertung wiederholt.
- Wenn der Eintrag weder in der benutzerdefinierten noch in der statischen Datenbank gefunden wird, wird die beste Site ausgewählt und in der DNS-Antwort auf der Grundlage der konfigurierten Lastausgleichsmethode gesendet.

Die folgenden Einschränkungen gelten für DNS-Richtlinien, die auf der Citrix ADC Appliance erstellt wurden.

- Es werden maximal 64 Richtlinien unterstützt.
- DNS-Richtlinien sind global für die Citrix ADC Appliance und können nicht auf einen bestimmten virtuellen Server oder eine bestimmte Domäne angewendet werden.
- Domänen- oder virtuelle serverspezifische Bindung der Richtlinie wird nicht unterstützt.

Sie können DNS-Richtlinien verwenden, um Clients, die einem bestimmten IP-Adressbereich entsprechen, an eine bestimmte Site weiterzuleiten. Wenn Sie beispielsweise ein GSLB-Setup mit mehreren geografisch getrennten GSLB-Sites haben, können Sie alle Clients, deren IP-Adresse sich innerhalb eines bestimmten Bereichs befindet, an ein bestimmtes Rechenzentrum leiten.

Sowohl TCP-basierter als auch UDP-basierter DNS-Datenverkehr können ausgewertet werden. Richtlinienausdrücke sind für UDP-basierten DNS-Datenverkehr auf dem Server und sowohl für UDP-basierten DNS-Datenverkehr als auch für TCP-basierten DNS-Datenverkehr auf der Clientseite verfügbar. Darüber hinaus können Sie Ausdrücke konfigurieren, um Abfragen und Antworten auszuwerten, die nur die folgenden DNS-Fragentypen (oder QTYPE-Werte) beinhalten:

- A
- AAAA
- NS
- SRV
- PTR
- CNAME
- SOA

- MX
- ANY

Die folgenden Antwortcodes (RCODE Werte) werden ebenfalls unterstützt:

- NOERROR - Kein Fehler
- FORMERR - Formatfehler
- SERVFAIL - Serverfehler
- NXDOMAIN - Nicht vorhandene Domäne
- NOTIMP - Abfragetyp nicht implementiert
- REFUSED - Abfrage abgelehnt

Sie können Ausdrücke zum Auswerten des DNS-Datenverkehrs konfigurieren. Ein DNS-Ausdruck beginnt mit den Präfixen DNS.REQ oder DNS.RES. Zur Auswertung der abgefragten Domäne, des Abfragetyps und des Trägerprotokolls stehen Funktionen zur Verfügung. Weitere Informationen zu DNS-Ausdrücken finden Sie unter “Ausdrücke zum Auswerten einer DNS-Nachricht und Identifizierung ihres Carrier-Protokolls” unter “Richtlinienkonfiguration und Referenz”.

So fügen Sie mit der Befehlszeilenschnittstelle eine DNS-Richtlinie hinzu

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

```
add dns policy <name> <rule> <actionName>
show dns policy <name>
<!--NeedCopy-->
```

Beispiel:

```
> add dns policy policy-GSLB-1 'CLIENT.UDP.DNS.DOMAIN.EQ(”domainname”)'
    my_dns_action
 Done
> show dns policy policy-GSLB-1
    Name: policy-GSLB-1
    Rule: CLIENT.UDP.DNS.DOMAIN.EQ(”domainname”)
    Action Name: my_dns_action
    Hits: 0
    Undef Hits: 0

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


So entfernen Sie eine konfigurierte DNS-Richtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 rm dns policy <name>
2 <!--NeedCopy-->
```

So konfigurieren Sie eine DNS-Richtlinie mithilfe des Citrix ADC Konfigurationsdienstprogramms

1. Navigieren Sie zu Verkehrsverwaltung > DNS > Richtlinien, und erstellen Sie eine DNS-Richtlinie.
2. Legen Sie im Dialogfeld DNS-Richtlinie erstellen oder DNS-Richtlinie konfigurieren die folgenden Parameter fest:
   - Richtlinienname (kann für eine vorhandene Richtlinie nicht geändert werden)
   - Aktion
   - Ausdruck

     Gehen Sie folgendermaßen vor, um einen Ausdruck anzugeben:

     a) Klicken Sie auf Hinzufügen, und wählen Sie dann im angezeigten Dropdownfeld das Ausdruckselement aus, mit dem Sie den Ausdruck beginnen möchten. Eine zweite Liste wird angezeigt. Die Liste enthält eine Reihe von Ausdruckselementen, die Sie unmittelbar nach dem Firs-Ausdruckselement verwenden können.

     b) Wählen Sie in der zweiten Liste das gewünschte Ausdruckselement aus, und geben Sie dann einen Punkt ein.

     c) Wenn Sie nach jeder Auswahl einen Punkt eingeben, wird der nächste Satz gültiger Ausdruckselemente in einer Liste angezeigt. Wählen Sie Ausdruckselemente aus, und füllen Sie Argumente für Funktionen aus, bis Sie den gewünschten Ausdruck haben.
3. Klicken Sie auf Erstellen oder OK und dann auf Schließen.

Binden von DNS-Richtlinien

DNS-Richtlinien sind global auf der Citrix ADC Appliance gebunden und sind für alle konfigurierten virtuellen GSLB-Server verfügbar. Obwohl DNS-Richtlinien global gebunden sind, kann die Richtlinienausführung auf einen bestimmten virtuellen GSLB-Server beschränkt werden, indem die Domäne im Ausdruck angegeben wird.

Hinweis: Obwohl der globale Befehl bind dns REQ_OVERRIDE und RES_OVERRIDE als gültige Bindepunkte akzeptiert, sind diese Bindepunkte redundant, da DNS-Richtlinien nur global gebunden werden können. Binden Sie Ihre DNS-Richtlinien nur an die BIND-Punkte REQ_DEFAULT und RES_DEFAULT.

So binden Sie eine DNS-Richtlinie global mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine DNS-Richtlinie global zu binden und die Konfiguration zu überprüfen:

```
bind dns global <policyName> <priority> [-gotoPriorityExpression <
    string>] [-type <type>]
show dns global -type <type>
<!--NeedCopy-->
```

Beispiel:

```
bind dns global policy-GSLB-1 10 -gotoPriorityExpression END
 Done
show dns global -type REQ_DEFAULT
1)  Policy Name: policy-GSLB-1
    Priority: 10
    GotoPriorityExpression: END
 Done
<!--NeedCopy-->
```

So binden Sie eine DNS-Richtlinie global mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu Traffic Management > DNS > Richtlinien.
2. Klicken Sie im Detailbereich auf Globale Bindungen.
3. Klicken Sie im Dialogfeld DNS-Richtlinie (en) an Global binden/entbinden auf Richtlinie einfügen.
4. Wählen Sie in der Spalte Richtlinienname aus der Liste die Richtlinie aus, die Sie binden möchten. Alternativ klicken Sie in der Liste auf Neue Richtlinie, und erstellen Sie dann eine DNS-Richtlinie, indem Sie Parameter im Dialogfeld DNS-Richtlinie erstellen festlegen.
5. Um eine Richtlinie zu ändern, die bereits global gebunden ist, klicken Sie auf den Namen der Richtlinie, und klicken Sie dann auf Richtlinie ändern. Ändern Sie dann im Dialogfeld DNS-Richtlinie konfigurieren die Richtlinie, und klicken Sie dann auf OK.
6. Um die Bindung einer Richtlinie aufzuheben, klicken Sie auf den Namen der Richtlinie und dann auf Richtlinie aufheben.
7. Um die Priorität zu ändern, die einer Richtlinie zugewiesen ist, doppelklicken Sie auf den Prioritätswert, und geben Sie dann einen neuen Wert ein.
8. Um zugewiesene Prioritäten neu zu generieren, klicken Sie auf Prioritäten neu generieren. Die Prioritätswerte werden so geändert, dass sie bei 100 beginnen, mit Schritten von 10, ohne dass die Reihenfolge der Auswertung beeinträchtigt wird.

9. Klicken Sie auf OK.

So zeigen Sie die globalen Bindungen einer DNS-Richtlinie mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show dns global
```

So zeigen Sie die globalen Bindungen einer DNS-Richtlinie mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu **Traffic Management** > **DNS** > **Richtlinien**.
2. Klicken Sie im Detailbereich auf **Globale Bindungen**. Die globalen Bindungen aller DNS-Richtlinien werden in diesem Dialogfeld angezeigt.

Hinzufügen von DNS-Ansichten

Sie können DNS-Ansichten konfigurieren, um verschiedene Arten von Clients zu identifizieren und eine entsprechende IP-Adresse für eine Gruppe von Clients bereitzustellen, die dieselbe GSLB-Domäne abfragen. DNS-Ansichten werden mithilfe von DNS-Richtlinien konfiguriert, die die an den Client zurückgesendeten IP-Adressen auswählen.

Wenn Sie beispielsweise GSLB für die Domäne Ihres Unternehmens konfiguriert haben und den Server im Netzwerk Ihres Unternehmens gehostet haben, können Clients, die die Domäne aus dem internen Netzwerk Ihres Unternehmens abfragen, die interne IP-Adresse des Servers anstelle der öffentlichen IP-Adresse zur Verfügung gestellt werden. Clients, die DNS für die Domäne aus dem Internet abfragen, können dagegen die öffentliche IP-Adresse der Domäne bereitgestellt werden.

Um eine DNS-Ansicht hinzuzufügen, weisen Sie ihr einen Namen von bis zu 31 Zeichen zu. Das führende Zeichen muss eine Zahl oder ein Buchstabe sein. Folgende Zeichen sind ebenfalls zulässig: @ _ -. (Punkt): (Doppelpunkt) # und Leerzeichen (). Nachdem Sie die Ansicht hinzugefügt haben, konfigurieren Sie eine Richtlinie, um sie mit Clients und einem Teil des Netzwerks zu verknüpfen, und binden die Richtlinie global. Informationen zum Konfigurieren und Binden einer DNS-Richtlinie finden Sie unter **Verwalten des lokalen DNS-Datenverkehrs mithilfe von DNS-Richtlinien**.

So fügen Sie mit der Befehlszeilenschnittstelle eine DNS-Ansicht hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine DNS-Ansicht zu erstellen und die Konfiguration zu überprüfen:


```
add dns view <viewName>
show dns view <viewName>
<!--NeedCopy-->
```

Beispiel:

```
add dns view PrivateSubnet
show dns view PrivateSubnet
<!--NeedCopy-->
```

So entfernen Sie eine DNS-Ansicht mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm dns view <viewName>
<!--NeedCopy-->
```

So fügen Sie mit dem Konfigurationsdienstprogramm eine DNS-Ansicht hinzu

Navigieren Sie zu Traffic Management > DNS > Views, und fügen Sie eine DNS-Ansicht hinzu.

Weitere Informationen zum Erstellen einer DNS-Richtlinie und zum globalen Binden von DNS-Richtlinien finden Sie unter **Verwalten des lokalen DNS-Datenverkehrs mithilfe von DNS-Richtlinien**.

Konfigurieren von GSLB für die Nähe

October 5, 2021

Wenn Sie GSLB für die Nähe konfigurieren, werden Clientanforderungen an das nächstgelegene Rechenzentrum weitergeleitet. Der Hauptvorteil der proximitätsbasierten GSLB-Methode liegt in der schnelleren Reaktionszeiten, die sich aus der Auswahl des nächstgelegenen verfügbaren Rechenzentrums ergeben. Eine solche Bereitstellung ist für Anwendungen von entscheidender Bedeutung, die schnellen Zugriff auf große Datenmengen erfordern.

Sie können GSLB für die Nähe basierend auf der Round Trip Time (RTT), der statischen Nähe oder einer Kombination aus beiden konfigurieren.

Konfigurieren der RTT-Methode (Dynamic Round Trip Time)

Dynamic Round Trip Time (RTT) ist ein Maß für die Zeit oder Verzögerung im Netzwerk zwischen dem lokalen DNS-Server des Clients und einer Datenressource. Zur Messung des dynamischen RTT untersucht die Citrix ADC Appliance den lokalen DNS-Server des Clients und sammelt RTT-Metrikinformationen. Die Appliance verwendet diese Metrik dann, um ihre Lastausgleichsentscheidung zu treffen. Globaler Server Load Balancing überwacht den Echtzeitstatus des Netzwerks und leitet die Clientanforderung dynamisch an das Rechenzentrum mit dem niedrigsten RTT-Wert

Um GSLB für die Nähe mit dynamischer Methode zu konfigurieren, müssen Sie zuerst die grundlegende GSLB einrichten und dann den dynamischen RTT konfigurieren.

Erstellen Sie zunächst zwei GSLB-Sites, lokal und remote. Erstellen Sie dann für den lokalen Standort einen virtuellen GSLB-Server und GSLB-Dienste und binden Sie die Dienste an den virtuellen Server. Erstellen Sie dann ADNS-Dienste und binden Sie die Domäne, für die Sie GSLB konfigurieren, an den virtuellen GSLB-Server am lokalen Standort. Erstellen Sie schließlich einen virtuellen Lastausgleichsserver mit der gleichen virtuellen Server-IP-Adresse wie der GSLB-Dienst.

Weitere Informationen zur Konfiguration eines grundlegenden GSLB-Setups finden Sie unter Konfigurieren von GSLB-Entitäten einzeln.

Nachdem Sie eine grundlegende GSLB-Setup konfiguriert haben, konfigurieren Sie die dynamische RTT-Methode.

Weitere Informationen zur Konfiguration des virtuellen GSLB-Servers für die Verwendung der dynamischen RTT-Methode für den Lastenausgleich finden Sie unter Konfigurieren von dynamischem RTT.

Statische Nähe konfigurieren

Die statische Näherungsmethode für GSLB verwendet eine IP-adressbasierte statische Näherungsdatenbank, um die Nähe zwischen dem lokalen DNS-Server des Clients und den GSLB-Sites zu bestimmen. Die Citrix ADC Appliance antwortet mit der IP-Adresse eines Standorts, der den Näherungskriterien am besten entspricht.

Wenn zwei oder mehr GSLB-Sites an verschiedenen geografischen Sites denselben Inhalt bereitstellen, verwaltet die Citrix ADC Appliance eine Datenbank mit IP-Adressbereichen und verwendet die Datenbank für Entscheidungen über die GSLB-Sites, an die eingehende Clientanforderungen weitergeleitet werden sollen.

Um GSLB für die Nähe mit statischer Nähe zu konfigurieren, müssen Sie zuerst die grundlegende GSLB-Einrichtung konfigurieren und dann die statische Näherung konfigurieren.

Erstellen Sie zunächst zwei GSLB-Sites, lokal und remote. Erstellen Sie dann für den lokalen Standort einen virtuellen GSLB-Server und GSLB-Dienste und binden Sie die Dienste an den virtuellen

Server. Erstellen Sie dann ADNS-Dienste und binden Sie die Domäne, für die Sie GSLB konfigurieren, an den virtuellen GSLB-Server am lokalen Standort. Erstellen Sie schließlich einen virtuellen Lastausgleichsserver mit der gleichen virtuellen Server-IP-Adresse wie der GSLB-Dienst.

Weitere Informationen zur Konfiguration eines grundlegenden GSLB-Setups finden Sie unter Konfigurieren von GSLB-Entitäten einzeln.

Nachdem Sie eine grundlegende GSLB-Setup konfiguriert haben, konfigurieren Sie die statische Nähe.

Weitere Informationen zur Konfiguration des virtuellen GSLB-Servers für die Verwendung der statischen Nähe für den Lastenausgleich finden Sie unter Konfigurieren der statischen Nähe.

Konfigurieren der statischen Nähe und dynamischen RTT

Sie können den virtuellen GSLB-Server so konfigurieren, dass er eine Kombination aus statischer Nähe und dynamischem RTT verwendet, wenn einige Clients aus einem internen Netzwerk wie einer Zweigstelle kommen. Sie können GSLB so konfigurieren, dass die Clients, die von der Zweigstelle oder einem anderen internen Netzwerk stammen, an einen bestimmten GSLB-Site weitergeleitet werden, der geographisch nahe am Client-Netzwerk liegt. Für alle anderen Anforderungen können Sie dynamische RTT verwenden.

Erstellen Sie zunächst zwei GSLB-Sites, lokal und remote. Erstellen Sie dann für den lokalen Standort einen virtuellen GSLB-Server und GSLB-Dienste und binden Sie die Dienste an den virtuellen Server. Erstellen Sie dann ADNS-Dienste und binden Sie die Domäne, für die Sie GSLB konfigurieren, an den virtuellen GSLB-Server am lokalen Standort. Erstellen Sie schließlich einen virtuellen Lastausgleichsserver mit der gleichen virtuellen Server-IP-Adresse wie der GSLB-Dienst.

Weitere Informationen zur Konfiguration eines grundlegenden GSLB-Setups finden Sie unter Konfigurieren von GSLB-Entitäten einzeln.

Nachdem Sie ein grundlegendes GSLB-Setup konfiguriert haben, konfigurieren Sie den virtuellen GSLB-Server so, dass er statische Nähe für den gesamten Datenverkehr verwendet, der von einem internen Netzwerk stammt, und verwenden Sie dann den dynamischen RTT für den gesamten anderen Datenverkehr.

Weitere Informationen zur Konfiguration der statischen Nähe finden Sie unter Konfigurieren der statischen Nähe und weitere Informationen zur Konfiguration von dynamischem RTT finden Sie unter Konfigurieren von dynamischem RTT.

Schützen des GSLB-Setups vor Ausfällen

October 5, 2021

Sie können Ihr GSLB-Setup vor dem Ausfall einer GSLB-Site oder eines virtuellen GSLB-Servers schützen, indem Sie Folgendes konfigurieren:

- Ein virtueller GSLB-Server
- Eine Citrix ADC Appliance, um mit mehreren IP-Adressen zu antworten
- Eine Backup-IP-Adresse für eine GSLB-Domäne

Sie können überschüssigen Datenverkehr auch auf einen virtuellen Backup-Server umleiten, indem Sie Spillover verwenden.

Konfigurieren eines virtuellen GSLB-Backupservers

Das Konfigurieren einer Backupeinheit für einen virtuellen GSLB-Server stellt sicher, dass der DNS-Datenverkehr zu einer Site nicht unterbrochen wird, wenn der virtuelle GSLB-Server ausfällt. Die Backupeinheit kann ein anderer virtueller GSLB-Server sein, oder es kann sich um eine Backup-IP-Adresse handeln. Wenn eine Backupeinheit konfiguriert ist, verarbeitet die Backupeinheit DNS-Anforderungen, wenn der primäre virtuelle GSLB-Server ausfällt. Um anzugeben, was passieren muss, wenn der primäre virtuelle GSLB-Server erneut angezeigt wird, können Sie die Sicherungseinheit so konfigurieren, dass sie den Datenverkehr fortsetzt, bis Sie den primären virtuellen Server manuell die Übernahme aktivieren (mit der Option DisablePrimaryOnDown).

Hinweis: Sie können eine einzelne Backup-Entität als Backup für mehrere virtuelle GSLB-Server konfigurieren.

So konfigurieren Sie einen virtuellen GSLB-Backupserver mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen virtuellen GSLB-Server als virtuellen Sicherungsserver zu konfigurieren und die Konfiguration zu überprüfen:

```
1 set gslb vserver <name> -backupVServer <name> [-disablePrimaryOnDown (
     ENABLED | DISABLED)]
2
3 show gslb vserver <name>
4 <!--NeedCopy-->
```

Beispiel:

```
1 set gslb vserver vserver-GSLB-1 -backupVServer vserver-GSLB-2 -
     disablePrimaryOnDown ENABLED
2 show gslb vserver vserver-GSLB-1
3 <!--NeedCopy-->
```


So legen Sie den virtuellen GSLB-Server als virtuellen Backupserver mit dem Konfigurationsdienstprogramm fest

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**, und doppelklicken Sie auf den virtuellen GSLB-Server.
2. Wählen Sie den Abschnitt **Virtuellen Server Backup** und den virtuellen Backup-Server wählen.

Konfigurieren eines GSLB-Setups für die Reaktion mit mehreren IP-Adressen

Eine typische DNS-Antwort enthält die IP-Adresse des am besten leistungsfähigen GSLB-Dienstes. Wenn Sie jedoch mehrere IP-Antworten (MIR) aktivieren, sendet die Citrix ADC Appliance den besten GSLB Service als ersten Datensatz in der Antwort und fügt die verbleibenden aktiven Dienste als zusätzliche Datensätze hinzu. Wenn MIR deaktiviert ist (Standardeinstellung), sendet die Citrix ADC Appliance den besten Service als einzigen Datensatz als Antwort.

So konfigurieren Sie einen virtuellen GSLB-Server für mehrere IP-Antworten mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen virtuellen GSLB-Server für mehrere IP-Antworten zu konfigurieren und die Konfiguration zu überprüfen:

```
set gslb vserver<name> -MIR (ENABLED | DISABLED)
-  show gslb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver vserver-GSLB-1 -MIR ENABLED
 show gslb vserver <vserverName>
<!--NeedCopy-->
```

So legen Sie einen virtuellen GSLB-Server für mehrere IP-Antworten mit dem Konfigurationsdienstprogramm fest

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**, und doppelklicken Sie auf den virtuellen GSLB-Server, für den Sie einen virtuellen Backupserver konfigurieren möchten (z. B. vServer-GSLB-1).
2. Aktivieren Sie auf der Registerkarte **Erweitert** unter Wenn dieser virtuelle Server “UP” ist, das Kontrollkästchen Alle “aktiven” Dienst-IP als Antwort (MIR) senden, und wählen Sie **OK**aus.

Konfigurieren eines virtuellen GSLB-Servers für die Reaktion mit einem leeren Adressdatensatz bei DOWN

Eine DNS-Antwort kann entweder die IP-Adresse der angeforderten Domäne oder eine Antwort enthalten, die besagt, dass die IP-Adresse für die Domäne vom DNS-Server nicht bekannt ist. In diesem Fall wird die Abfrage an einen anderen Nameserver weitergeleitet. Dies sind die einzigen möglichen Antworten auf eine DNS-Abfrage.

Wenn ein virtueller GSLB-Server deaktiviert ist oder sich im Zustand DOWN befindet, enthält die Antwort auf eine DNS-Abfrage für die an diesen virtuellen Server gebundene GSLB-Domäne die IP-Adressen aller Dienste, die an den virtuellen Server gebunden sind. Sie können jedoch den virtuellen GSLB-Server so konfigurieren, dass er in diesem Fall eine leere Down Response (EDR) sendet. Wenn diese Option festgelegt ist, enthält eine DNS-Antwort von einem virtuellen GSLB-Server, der sich im Zustand DOWN befindet, keine IP-Adressdatensätze, aber der Antwortcode ist erfolgreich. Dadurch wird verhindert, dass Clients versuchen, eine Verbindung mit heruntergeschaltetem GSLB-Sites herzustellen.

Hinweis: Sie müssen diese Einstellung für jeden virtuellen Server konfigurieren, auf den sie angewendet werden soll.

So konfigurieren Sie einen virtuellen GSLB-Server für leere Antworten mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set gslb vserver<name> -EDR (ENABLED | DISABLED)
<!--NeedCopy-->
```

Beispiel:

```
> set gslb vserver vserver-GSLB-1 -EDR ENABLED
 Done
<!--NeedCopy-->
```

So legen Sie einen virtuellen GSLB-Server für leere Antworten mit dem Konfigurationsdienstprogramm fest

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**, und doppelklicken Sie auf den virtuellen GSLB-Server, für den Sie einen virtuellen Backupserver konfigurieren möchten (z. B. vServer-GSLB-1).

2. Aktivieren Sie auf der Registerkarte Erweitert unter Wenn dieser virtuelle Server “Nicht” ist, das Kontrollkästchen Die IP-Adresse in Antwort (EDR) keinen Dienst senden.
3. Klicken Sie auf **OK**.

Konfigurieren einer Backup-IP-Adresse für eine GSLB-Domäne

Sie können eine Backup-Site für Ihre GSLB-Konfiguration konfigurieren. Wenn bei dieser Konfiguration alle primären Standorte NACH UNTEN gehen, wird die IP-Adresse der Backup-Site in der DNS-Antwort angegeben.

Wenn ein virtueller GSLB-Server aktiv ist, sendet dieser virtuelle Server in der Regel eine DNS-Antwort mit einer der aktiven Site-IP-Adressen, die von der konfigurierten GSLB-Methode ausgewählt wurde. Wenn alle konfigurierten primären Standorte auf dem virtuellen GSLB-Server inaktiv sind (im Status DOWN), sendet der autoritative Domänennamensystem (ADNS) -Server oder der DNS-Server eine DNS-Antwort mit der IP-Adresse des Backup-Site.

Hinweis: Wenn eine Backup-IP-Adresse gesendet wird, wird die Persistenz nicht berücksichtigt.

So legen Sie eine Backup-IP-Adresse für eine Domäne mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Backup-IP-Adresse festzulegen und die Konfiguration zu überprüfen:

```
set gslb vserver <name> -domainName <string> -backupIP <IPAddress>
show gslb vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver vserver-GSLB-1 -domainName www.abc.com -backupIP
   10.102.29.66
show gslb vserver vserver-GSLB-1
<!--NeedCopy-->
```

So legen Sie eine Backup-IP-Adresse für eine Domäne mit dem Konfigurationsdienstprogramm fest

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**, und doppelklicken Sie auf den virtuellen GSLB-Server, an den Sie die Backupdomäne binden möchten (z. B. vServer-GSLB-1).

2. Klicken Sie auf den Abschnitt **Domänen**, konfigurieren Sie die GSLB-Domäne und geben Sie die IP-Adresse der Backupdomäne im Feld **Backup-IP** an.

Überschüssigen Datenverkehr auf einen virtuellen Backup-Server umleiten

Sobald die Anzahl der Verbindungen zu einem primären virtuellen GSLB-Server den konfigurierten Schwellenwert überschreitet, können Sie die Option Spillover verwenden, um neue Verbindungen auf einen virtuellen GSLB-Backup-Server umzuleiten. Dieser Schwellenwert kann dynamisch berechnet oder manuell eingestellt werden. Sobald die Anzahl der Verbindungen zum primären virtuellen Server unter den Schwellenwert fällt, nimmt der primäre virtuelle GSLB-Server die Bereitstellung von Clientanforderungen wieder auf.

Sie können Persistenz mit Spillover konfigurieren. Wenn die Persistenz konfiguriert ist, werden neue Clients auf den virtuellen Backupserver umgeleitet, wenn dieser Client noch nicht mit einem primären virtuellen Server verbunden ist. Wenn die Persistenz konfiguriert ist, werden Verbindungen, die an den virtuellen Backupserver umgeleitet wurden, nicht wieder auf den primären virtuellen Server verschoben, nachdem die Anzahl der Verbindungen zum primären virtuellen Server unter den Schwellenwert fällt. Stattdessen verarbeitet der virtuelle Backupserver diese Verbindungen weiter, bis sie vom Benutzer beendet werden. Inzwischen akzeptiert der primäre virtuelle Server neue Clients.

Der Schwellenwert kann anhand der Anzahl der Verbindungen, der Bandbreite und der Integrität der Dienste gemessen werden.

Wenn der virtuelle Backupserver den konfigurierten Schwellenwert erreicht und keine zusätzliche Last übernehmen kann, leitet der primäre virtuelle Server alle Anforderungen an die angegebene Umleitungs-URL um. Wenn keine Umleitungs-URL auf dem primären virtuellen Server konfiguriert ist, werden nachfolgende Anforderungen gelöscht.

Die Spillover-Funktion verhindert, dass der Remote Backup GSLB-Dienst (Backup GSLB Site) mit Client-Anforderungen überschwemmt wird, wenn der primäre virtuelle GSLB Server ausfällt. Dies tritt auf, wenn ein Monitor an einen entfernten GSLB-Dienst gebunden ist und der Dienst einen Fehler auftritt, der dazu führt, dass der Status zu DOWN geht. Der Monitor behält jedoch weiterhin den Status des Remote-GSLB-Dienstes UP, wegen der Spillover-Funktion.

Als Teil der Lösung dieses Problems werden zwei Zustände für einen GSLB-Dienst beibehalten, der primäre Zustand und der effektive Zustand. Der primäre Status ist der Status des primären virtuellen Servers und der effektive Status ist der kumulative Status der virtuellen Server (primäre und Backupkette). Der effektive Status wird auf UP festgelegt, wenn einer der virtuellen Server in der Kette der virtuellen Server UP ist. Ein Flag, das angibt, dass der primäre VIP den Schwellenwert erreicht hat, wird ebenfalls angegeben. Der Schwellenwert kann entweder anhand der Anzahl der Verbindungen oder der Bandbreite gemessen werden.

Ein Dienst wird für GSLB nur dann berücksichtigt, wenn sein primärer Status UP ist. Der Datenverkehr

wird nur dann an den GSLB-Backupdienst weitergeleitet, wenn alle primären virtuellen Server heruntergefahren sind. In der Regel haben solche Bereitstellungen nur einen Sicherungs-GSLB-Dienst.

Das Hinzufügen von primären und effektiven Zuständen zu einem GSLB-Dienst hat folgende Auswirkungen:

- Wenn die Quell-IP-Persistenz konfiguriert ist, wird der lokale DNS nur dann an den zuvor ausgewählten Standort weitergeleitet, wenn der primäre virtuelle Server auf dem ausgewählten Standort UP und unter dem Schwellenwert liegt. Persistenz kann im Round-Robin-Modus ignoriert werden.
- Wenn die Cookie-basierte Persistenz konfiguriert ist, werden Clientanforderungen nur dann umgeleitet, wenn der primäre virtuelle Server auf dem ausgewählten Standort UP ist.
- Wenn der primäre virtuelle Server seine Sättigung erreicht hat und die Backup-VIPs nicht vorhanden oder heruntergefahren sind, wird der effektive Status auf DOWN festgelegt.
- Wenn externe Monitore an einen virtuellen HTTP-HTTPS-Server gebunden sind, entscheidet der Monitor den Primärzustand.
- Wenn kein virtueller Backupserver auf dem primären virtuellen Server vorhanden ist und der primäre virtuelle Server seinen Schwellenwert erreicht hat, wird der effektive Status auf DOWN festgelegt.

So konfigurieren Sie den virtuellen Backup-GSLB-Server mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den virtuellen GSLB-Server zu konfigurieren und die Konfiguration zu überprüfen:

```
1 set gslb vserver <name> -soMethod <method> -soThreshold <threshold> -
     soPersistence ( \*\*ENABLED\*\* | \*\*DISABLED\*\* ) -
     soPersistenceTimeout <timeout>
2 show gslb vserver <name>
3 <!--NeedCopy-->
```

Beispiel:

```
1 set gslb vserver Vserver-GSLB-1 -soMethod CONNECTION -soThreshold 1000
     -soPersistence ENABLED -soPersistenceTimeout 2
2 show gslb vserver Vserver-GSLB-1
3 <!--NeedCopy-->
```


So konfigurieren Sie den virtuellen Backup-GSLB-Server mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **GSLB** > **Virtuelle Server**, und doppelklicken Sie auf den virtuellen Server, den Sie als Backup konfigurieren möchten (z. B. vServer-LB-1).
2. Klicken Sie auf den Abschnitt **SpillOver**, und legen Sie die folgenden Parameter fest:
   - Methode: soMethod
   - Schwellenwert— soThreshold
   - Persistenz-Timeout (min) — soPersistenceTimeout
3. Wählen Sie die Option Persistenz aus, und klicken Sie auf **OK**.

Konfigurieren von GSLB für Disaster Recovery

October 5, 2021

Die Disaster Recovery-Funktion ist von entscheidender Bedeutung, da Ausfallzeiten kostspielig sind. Eine für GSLB konfigurierte Citrix ADC Appliance leitet den Datenverkehr an das am wenigsten belastete oder das leistungsstärkste Rechenzentrum weiter. Diese Konfiguration, die als aktiv-aktives Setup bezeichnet wird, verbessert nicht nur die Leistung, sondern bietet auch eine sofortige Notfallwiederherstellung, indem Datenverkehr an andere Rechenzentren weitergeleitet wird, wenn ein Rechenzentrum, das Teil des Setups ist, ausfällt. Alternativ können Sie ein GSLB-Setup mit aktivem Standby nur für die Disaster Recovery konfigurieren.

Konfigurieren von GSLB für Disaster Recovery in einem Active-Standby-Rechenzentrums-Setup

Ein herkömmliches Notfallwiederherstellungs-Setup umfasst ein aktives Rechenzentrum und ein Standby-Rechenzentrum. Das Standby-Rechenzentrum ist ein Remote-Standort. Wenn ein Failover als Folge eines Notfallereignisses auftritt, das dazu führt, dass das primäre aktive Rechenzentrum inaktiv ist, wird das Standby-Rechenzentrum betriebsbereit.

Die Konfiguration der Disaster Recovery in einem Active-Standby-Rechenzentrums-Setup umfasst die folgenden Aufgaben:

- Erstellen Sie das aktive Rechenzentrum.
  - Fügen Sie eine lokale GSLB-Site hinzu.
  - Fügen Sie einen GSLB-vserver hinzu, der das aktive Rechenzentrum darstellt.
  - Binden Sie die Domäne an den virtuellen GSLB-Server.
  - Fügen Sie gslb-Dienste hinzu und binden Sie die Dienste an den aktiven virtuellen GSLB Server.
- Erstellen Sie das Standby-Rechenzentrum.

- Fügen Sie eine entfernte gslb-Site hinzu.
- Fügen Sie einen gslb-vserver hinzu, der das Standby-Rechenzentrum darstellt.
- Fügen Sie gslb-Dienste hinzu, die das Standby-Rechenzentrum darstellen, und binden Sie die Dienste an den Standby-gslb-vserver.
- Bestimmen Sie das Standby-Rechenzentrum, indem Sie den virtuellen Standbyserver GSLB als virtuellen Backupserver für den aktiven virtuellen GSLB-Server konfigurieren.

Nachdem Sie das primäre Rechenzentrum konfiguriert haben, replizieren Sie die Konfiguration für das Backupdatenzentrum und legen Sie es als Standby GSLB-Site fest, indem Sie einen virtuellen GSLB-Server an diesem Standort als virtuellen Backupserver festlegen.

Weitere Informationen zur Konfiguration eines grundlegenden GSLB-Setups finden Sie unter Konfigurieren von GSLB-Entitäten einzeln.

So weisen Sie die Standby GSLB-Site mit der Befehlszeilenschnittstelle aus

Geben Sie an der Eingabeaufforderung sowohl am aktiven Standort als auch am Remotestandort Folgendes ein:

```
1 set gslb vserver <name> -backupVserver <string>
2 <!--NeedCopy-->
```

Beispiel:

```
1 set gslb vserver vserver-GSLB-1 -backupVServer vserver-GSLB-2
2 <!--NeedCopy-->
```

So konfigurieren Sie den Standby-Standort mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu Traffic Management > GSLB > Virtuelle Server, und doppelklicken Sie auf den virtuellen GSLB-Server für den primären Standort.
2. Klicken Sie auf den Abschnitt **Virtueller Server sichern**, und wählen Sie einen virtuellen Backupserver aus.

Sobald der primäre virtuelle Server aktiv wird, wird standardmäßig der Datenverkehr empfangen. Wenn Sie jedoch möchten, dass der Datenverkehr auch nach dem aktiven primären virtuellen Server an den virtuellen Backupserver weitergeleitet wird, verwenden Sie die Option
primäre bei Herunterfahren deaktivieren.

Konfigurieren für Disaster Recovery in einem Active-Active-Active-Active-Rechenzentrums-Setup

Eine aktiv-aktive GSLB-Bereitstellung, bei der beide GSLB-Sites aktiv sind, beseitigt alle Risiken, die bei der Einrichtung eines Standby-Rechenzentrums auftreten können. Mit einer solchen Einrichtung können Web- oder Anwendungsinhalte an geografisch getrennten Sites gespiegelt werden. Dadurch wird sichergestellt, dass die Daten in jedem verteilten Rechenzentrum konsistent verfügbar sind.

Um GSLB für die Notfallwiederherstellung in einem aktiv-aktiven Rechenzentrum zu konfigurieren, müssen Sie zunächst das grundlegende GSLB-Setup auf dem ersten Rechenzentrum konfigurieren und dann alle anderen Rechenzentren konfigurieren.

Erstellen Sie zunächst mindestens zwei GSLB-Sites. Erstellen Sie dann für den lokalen Standort einen virtuellen GSLB-Server und GSLB-Dienste und binden Sie die Dienste an den virtuellen Server. Erstellen Sie dann ADNS-Dienste und binden Sie die Domäne, für die Sie GSLB konfigurieren, an den virtuellen GSLB-Server am lokalen Standort. Erstellen Sie schließlich am lokalen Standort einen virtuellen Lastausgleichsserver mit derselben IP-Adresse des virtuellen Servers wie der GSLB-Dienst.

Nachdem Sie das erste Rechenzentrum konfiguriert haben, replizieren Sie die Konfiguration für andere Rechenzentren, die Teil der Einrichtung sind.

Weitere Informationen zur Konfiguration eines grundlegenden GSLB-Setups finden Sie unter Konfigurieren von GSLB-Entitäten einzeln.

Konfigurieren für Disaster Recovery mit gewichtetem Round Robin

Wenn Sie GSLB für die Verwendung der gewichteten Roundrobin-Methode konfigurieren, werden den GSLB-Diensten Gewichtungen hinzugefügt, und der konfigurierte Prozentsatz des eingehenden Datenverkehrs wird an jede GSLB-Site gesendet. Beispielsweise können Sie Ihr GSLB-Setup so konfigurieren, dass 80 Prozent des Datenverkehrs an einen Standort und 20 Prozent des Datenverkehrs an einen anderen weitergeleitet werden. Danach sendet die Citrix ADC Appliance vier Anforderungen an den ersten Standort für jede Anforderung, die sie an die zweite sendet.

Um die gewichtete Round-Robin-Methode einzurichten, erstellen Sie zunächst zwei GSLB-Sites, lokal und remote. Erstellen Sie als Nächstes für den lokalen Standort einen virtuellen GSLB-Server und GSLB-Dienste, und binden Sie die Dienste an den virtuellen Server. Konfigurieren Sie die GSLB-Methode als Round-Robin. Erstellen Sie als Nächstes ADNS-Dienste und binden Sie die Domäne, für die Sie GSLB konfigurieren, an den virtuellen GSLB-Server. Erstellen Sie schließlich einen virtuellen Lastausgleichsserver mit der gleichen virtuellen Server-IP-Adresse wie der GSLB-Dienst.

Jedem Dienst, der einen physischen Server im Netzwerk darstellt, sind Gewichtungen zugeordnet. Daher wird dem GSLB-Dienst ein dynamisches Gewicht zugewiesen, das die Summe der Gewichte aller an ihn gebundenen Dienste darstellt. Der Verkehr wird dann auf die GSLB-Dienste aufgeteilt,

basierend auf dem Verhältnis des dynamischen Gewichts des jeweiligen Dienstes zum Gesamtgewicht. Sie können auch einzelne Gewichtungen für jeden GSLB-Service anstelle der dynamischen Gewichtung konfigurieren.

Wenn den Diensten keine Gewichtungen zugeordnet sind, können Sie den virtuellen GSLB-Server so konfigurieren, dass die Anzahl der an ihn gebundenen Dienste verwendet wird, um die Gewichtung dynamisch zu berechnen.

Weitere Informationen zur Konfiguration eines grundlegenden GSLB-Setups finden Sie unter Konfigurieren von GSLB-Entitäten einzeln.

Nachdem Sie ein grundlegendes GSLB-Setup konfiguriert haben, müssen Sie die gewichtete Round-Robin-Methode so konfigurieren, dass der Datenverkehr auf die konfigurierten GSLB-Sites aufgeteilt wird, entsprechend den für die einzelnen Dienste konfigurierten Gewichtungen.

So konfigurieren Sie einen virtuellen Server zum Zuweisen von Gewichtungen zu Diensten mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, je nachdem, ob Sie einen neuen virtuellen Lastausgleichsserver erstellen oder einen vorhandenen konfigurieren möchten:

```
add lb vserver <name>@ -weight <WeightValue> <ServiceName>
set lb vserver <name>@ -weight <WeightValue> <ServiceName>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-1 -weight 4 Service-HTTP-1
set lb vserver Vserver-LB-1 -weight 4 Service-HTTP-1
<!--NeedCopy-->
```

So legen Sie die dynamische Gewichtung mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set gslb vserver <name> -dynamicWeight DynamicWeightType
<!--NeedCopy-->
```

Beispiel:


```
set gslb vserver Vserver-GSLB-1 -dynamicWeight ServiceWeight
<!--NeedCopy-->
```

So fügen Sie den GSLB-Diensten Gewichtungen über die Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set gslb vserver <name> -serviceName GSLBServiceName -weight
   WeightValue
<!--NeedCopy-->
```

Beispiel:

```
set gslb vserver Vserver-GSLB-1 -serviceName Service-GSLB-1 -weight 1
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Server zum Zuweisen von Gewichtungen zu Diensten mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server, und doppelklicken Sie auf den virtuellen Server (z. B. vServer-LB-1).
2. Klicken Sie auf den Abschnitt Dienste, und legen Sie die Gewichtung eines Dienstes fest.

So fügen Sie Gewichtungen zu den GSLB-Diensten mit dem Konfigurationsdienstprogramm hinzu

1. Navigieren Sie zu Traffic Management > GSLB > Virtuelle Server, und doppelklicken Sie auf den virtuellen Server (z. B. vServer-GSLB-1)
2. Klicken Sie auf den Abschnitt Dienste, und legen Sie die Gewichtung des Dienstes im Feld Gewicht fest.

So legen Sie die dynamische Gewichtung mit dem Konfigurationsdienstprogramm fest

1. Navigieren Sie zu Traffic Management > GSLB > Virtuelle Server, und doppelklicken Sie auf den virtuellen Server (z. B. vServer-GSLB-1).
2. Klicken Sie auf den Abschnitt **Methode**, und wählen Sie in der Dropdownliste **Dynamisches Gewicht** die Option **SERVICEWEIGHT** aus.

Konfigurieren für Disaster Recovery mit Rechenzentrumspersistenz

Die Persistenz des Rechenzentrums ist für Webanwendungen erforderlich, die eine Verbindung mit demselben Server aufrechterhalten müssen, anstatt die Anforderungen mit dem Lastenausgleich auszugleichen. Beispielsweise ist in einem E-Commerce-Portal die Aufrechterhaltung einer Verbindung zwischen dem Client und demselben Server entscheidend. Für solche Anwendungen kann die HTTP-Umleitungspersistenz in einem aktiv-aktiven Setup konfiguriert werden.

Um GSLB für die Disaster Recovery mit der Persistenz des Rechenzentrums zu konfigurieren, müssen Sie zunächst die grundlegende GSLB-Einrichtung konfigurieren und dann die HTTP-Umleitungspersistenz konfigurieren.

Erstellen Sie zunächst zwei GSLB-Sites, lokal und remote. Erstellen Sie als Nächstes für den lokalen Standort einen virtuellen GSLB-Server und GSLB-Dienste und binden Sie die Dienste an den virtuellen Server. Erstellen Sie als Nächstes ADNS-Dienste und binden Sie die Domäne, für die Sie GSLB konfigurieren, an den virtuellen GSLB-Server am lokalen Standort. Erstellen Sie als Nächstes einen virtuellen Lastausgleichsserver mit derselben IP-Adresse des virtuellen Servers wie der GSLB-Dienst. Duplizieren Sie abschließend die vorherigen Schritte für die Remotekonfiguration oder konfigurieren Sie die Citrix ADC Appliance, um Ihre GSLB-Konfiguration automatisch zu synchronisieren.

Weitere Informationen zur Konfiguration eines grundlegenden GSLB-Setups finden Sie unter Konfigurieren von GSLB-Entitäten einzeln.

Nachdem Sie eine grundlegende GSLB-Setup konfiguriert haben, konfigurieren Sie die Priorität der HTTP-Umleitung, um die Persistenz des Rechenzentrums zu aktivieren.

So konfigurieren Sie die HTTP-Umleitung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die HTTP-Umleitung zu konfigurieren und die Konfiguration zu überprüfen:

```
1 set gslb service <serviceName> -sitePersistence <sitePersistence> -
     sitePrefix <string>
2 show gslb service <serviceName>
3 <!--NeedCopy-->
```

Beispiel:

```
1 set gslb service Service-GSLB-1 -sitePersistence HTTPRedirect -
     sitePrefix vserver-GSLB-1
2 show gslb service Service-GSLB-1
3 <!--NeedCopy-->
```


So konfigurieren Sie die HTTP-Umleitung mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu Traffic Management > GSLB > Services, und doppelklicken Sie auf den zu konfigurierenden GSLB-Dienst.
2. Klicken Sie auf den Abschnitt **Site-Persistenz**, wählen Sie die Option **HttpRedirect** aus, und geben Sie im Textfeld **Site-Präfix** das Site-Präfix ein (z. B. vServer-GSLB-1).

> **Hinweis:**
>
> Wenn die Standortpersistenz nicht konfiguriert ist und ein virtueller Lastausgleichsserver, der als lokaler GSLB-Dienst konfiguriert ist, DOWN ist, werden die HTTP-Anforderungen mithilfe einer 302-Umleitung an andere fehlerfreie GSLB-Sites umgeleitet.

Überschreiben des statischen Näherungsverhaltens durch Konfigurieren bevorzugter Speicherorte

October 5, 2021

Möglicherweise möchten Sie den Datenverkehr von einem lokalen DNS-Server (LDNS) oder Netzwerk zu einem anderen GSLB-Dienst als dem GSLB-Dienst leiten, den die statische Näherungsmethode für diesen Datenverkehr auswählt. Das heißt, Sie haben einen *bevorzugten Standort* für diesen Datenverkehr. Um die statische Näherungsmethode mit bevorzugten Positionen zu überschreiben, können Sie Folgendes tun:

1. Konfigurieren Sie eine DNS-Aktion, die aus einer Liste der bevorzugten Speicherorte besteht. Weitere Informationen zum Konfigurieren einer DNS-Aktion finden Sie unter Konfigurieren einer DNS-Aktion.
2. Konfigurieren Sie eine DNS-Richtlinie, um den Datenverkehr zu identifizieren, der vom LDNS-Server oder Netzwerk eintrifft, für den Sie die statische Nähe überschreiben möchten, und wenden Sie die Aktion in der Richtlinie an.
3. Binden Sie die Richtlinie an den globalen Anforderungs-Bindpunkt.

In der DNS-Aktion können Sie eine Liste mit bis zu 8 bevorzugten Speicherorten konfigurieren. Die Positionen müssen in der gepunkteten Kriteriennotation angegeben werden. Dies ist die Notation, in der Sie der statischen Näherungsdatenbank benutzerdefinierte Positionen hinzufügen. Die Speicherorte können Platzhalter für Kriterien enthalten, die Sie weglassen möchten. Informationen zur gepunkteten Qualifikator-Notation für Standorte finden Sie unter Benutzerdefinierte Einträge zu einer statischen Proximity-Datenbank hinzufügen. Bei der Eingabe der bevorzugten Positionen müssen Sie diese in absteigender Reihenfolge der Priorität eingeben.

Wenn eine Richtlinie auf
TRUE ausgewertet wird, gleicht die Citrix ADC Appliance die bevorzugten Speicherorte in der Priorität-

sreihenfolge mit den Speicherorten der GSLB-Dienste ab. Übereinstimmungen sind von den folgenden zwei Arten:

- Wenn alle Nicht-Platzhalterqualifizierer an einem bevorzugten Ort mit den entsprechenden Qualifikationen am Standort eines GSLB-Dienstes übereinstimmen, wird die Übereinstimmung als perfekte Übereinstimmung angesehen. Zum Beispiel passt ein GSLB-Servicestandort von *.UK.*.* oder Europa.UK.*.* perfekt zum bevorzugten Standort *.UK.*.*.
- Wenn nur eine Teilmenge der Kriterien ohne Platzhalterzeichen übereinstimmt, wird die Übereinstimmung als Teilübereinstimmung betrachtet. Beispielsweise ist ein GSLB-Dienststandort von Europe.eg eine Teilübereinstimmung für den bevorzugten Standort Europe.uk.

Wenn eine DNS-Richtlinie auf
TRUE ausgewertet wird, wird der folgende Algorithmus verwendet, um einen GSLB-Dienst auszuwählen:

1. Die Appliance wertet den bevorzugten Standort aus, der die höchste Priorität hat, und verschiebt die Prioritätsreihenfolge nach unten, bis eine perfekte Übereinstimmung zwischen einem bevorzugten Standort und dem Standort eines GSLB-Dienstes gefunden wird.

   Wenn eine perfekte Übereinstimmung gefunden wird, überprüft die Appliance, ob der entsprechende GSLB-Dienst hochläuft. Wenn es aktiviert ist, gibt es die IP-Adresse des GSLB-Dienstes in der DNS-Antwort zurück. Wenn mehrere perfekte Übereinstimmungen gefunden werden (was passieren kann, wenn ein oder mehrere Platzhalter an einem bevorzugten Ort verwendet werden), überprüft die Appliance den Status jeder der entsprechenden GSLB-Dienste und gleicht die hochgeladenen GSLB-Dienste aus.

2. Wenn keine perfekte Übereinstimmung für einen der bevorzugten Sites gefunden wird, kehrt die Appliance an den bevorzugten Standort zurück, der die höchste Priorität hat, und verschiebt die Prioritätsreihenfolge nach unten, bis eine Teilübereinstimmung zwischen einem bevorzugten Standort und dem Standort eines GSLB-Dienstes gefunden wird.

   Wenn eine Teilübereinstimmung gefunden wird, prüft die Appliance, ob der entsprechende GSLB-Dienst hochläuft. Wenn es aktiviert ist, gibt es die IP-Adresse des GSLB-Dienstes in der DNS-Antwort zurück. Wenn mehrere Teilübereinstimmungen gefunden werden, überprüft die Appliance den Status der jeweiligen GSLB-Dienste und gleicht die hochgeladenen GSLB-Dienste aus.

3. Wenn keine der perfekten und partiellen Übereinstimmungen angezeigt werden, gleicht die Appliance alle anderen verfügbaren GSLB-Dienste aus.

   Auf diese Weise implementiert die Appliance einen Typ von Standortaffinität für Datenverkehr, der der DNS-Richtlinie entspricht.

Beispiel

Betrachten Sie eine GSLB-Konfiguration, die aus den folgenden acht GSLB-Diensten besteht:

- Asia.IN
- Asia.JPN
- Asia.HK
- Europe.UK
- Europe.RU
- Europe.EG
- Africa.SD
- Africa.ZMB

Beachten Sie außerdem die folgende DNS-Aktion und Richtlinienkonfiguration:

```
1 > add dns action prefLoc11 GslbPrefLoc -preferredLocList ”Asia.HK” ”
    Europe.UK”
2  Done
3 > add dns policy dnsPolPrefLoc ”CLIENT.IP.SRC.MATCHES_LOCATION(”\*.ZMB
    .\*.*”)” prefLoc11
4  Done
5 <!--NeedCopy-->
```

Wenn die Appliance eine Anforderung vom Speicherort erhält
. *ZMB..** werden die bevorzugten Sites wie folgt ausgewertet:

1. Die Appliance versucht, einen GSLB-Dienst zu finden, dessen Standort perfekt mit Asia.hk übereinstimmt. Dabei handelt es sich um den bevorzugten Standort, der die höchste Priorität hat. Es stellt fest, dass der GSLB Service bei Asia.hk perfekt passt. Wenn der GSLB-Dienst hochgesetzt ist, sendet er dem Client die IP-Adresse des GSLB-Dienstes.
2. Wenn der GSLB-Dienst bei Asia.hk nicht verfügbar ist, versucht das Gerät, eine perfekte Übereinstimmung für den zweiten bevorzugten Standort Europe.uk zu finden. Es stellt fest, dass der GSLB-Dienst bei Europe.uk perfekt zusammenpasst. Wenn der GSLB-Dienst hochgesetzt ist, sendet er dem Client die IP-Adresse des Dienstes.
3. Wenn der GSLB-Dienst bei Europe.uk nicht verfügbar ist, kehrt er an den bevorzugten Standort zurück, der die höchste Priorität hat, Asia.hk, und sucht nach Teilübereinstimmungen. Für Asia.hk stellt es fest, dass Asia.in und Asia.jpn partielle Übereinstimmungen sind. Wenn nur einer der entsprechenden GSLB-Dienste ausgeführt wird, sendet er dem Client die IP-Adresse des Dienstes. Wenn beide Sites hochgeladen sind, werden die beiden Dienste vom Lastausgleich ausgeglichen.
4. Wenn alle Teilübereinstimmungen für Asia.hk ausgefallen sind, sucht die Appliance nach Teilübereinstimmungen für Europe.uk. Es stellt fest, dass Europe.ru und Europe.eg teilweise

Übereinstimmungen für den bevorzugten Standort sind. Wenn nur einer der entsprechenden GSLB-Dienste ausgeführt wird, sendet er dem Client die IP-Adresse des Dienstes. Wenn beide Sites hochgeladen sind, werden die beiden Dienste vom Lastausgleich ausgeglichen.

5. Wenn alle Teilübereinstimmungen für Europe.uk ausgefallen sind, gleicht die Appliance alle anderen verfügbaren GSLB-Dienste aus. Im aktuellen Beispiel gleicht die Appliance-Lastverteilung Africa.sd und Africa.zmb aus, da die verbleibenden sechs GSLB-Dienste als ausgefallen wurden.

Konfigurieren der GSLB-Dienstauswahl über Content Switching

October 5, 2021

In einer typischen GSLB-Bereitstellung können Sie die Auswahl eines Satzes von GSLB-Diensten priorisieren, die an einen virtuellen GSLB-Server gebunden sind. Folgende Aktionen können jedoch nicht durchgeführt werden:

- Beschränken Sie die Auswahl eines GSLB-Dienstes aus einer Teilmenge von GSLB-Diensten, die an einen virtuellen GSLB-Server für die angegebene Domäne gebunden sind.
- Wenden Sie unterschiedliche Load Balancing-Methoden auf die verschiedenen Teilmengen von GSLB-Diensten in der Bereitstellung an.
- Wenden Sie Spillover-Richtlinien auf eine Teilmenge von GSLB-Diensten an, und Sie können kein Backup für eine Teilmenge von GSLB-Diensten haben.
- Konfigurieren Sie eine Teilmenge von GSLB-Diensten, um unterschiedliche Inhalte bereitzustellen. Das heißt, Sie können nicht zwischen Servern auf verschiedenen GSLB-Sites wechseln. Die GSLB-Konfiguration setzt voraus, dass die Server denselben Inhalt enthalten.
- Definieren Sie einen GSLB-Teilsatz mit unterschiedlichen Prioritäten und geben Sie eine Reihenfolge an, in der die Dienste in der Teilmenge auf eine Anforderung angewendet werden.

Sie können nun eine Content Switching-Richtlinie (CS) konfigurieren, um die GSLB-Bereitstellung anzupassen. Konfigurieren Sie zunächst einen Satz von GSLB-Diensten und binden Sie ihn an einen virtuellen GSLB-Server. Konfigurieren Sie dann einen virtuellen CS Server vom Zieltyp GSLB, definieren Sie eine CS-Richtlinie und -Aktion mit dem virtuellen GSLB-Server als virtuellen Zielserver und binden Sie die CS-Richtlinie an den virtuellen CS Server.

> **Wichtig**
>
> - Nur CS-Richtlinien mit DNS-basierten Ausdrücken können an einen virtuellen CS Server vom Zieltyp GSLB gebunden werden.
> - Wenn ein GLSB-Dienst über einen virtuellen GSLB-Server an einen virtuellen CS Server gebunden ist, können Sie keinen anderen virtuellen GSLB-Server binden, der mit demselben GSLB-Dienst an den virtuellen CS Server gebunden ist.

Beispiel

Betrachten Sie eine GLSB-Bereitstellung, die zwei GSLB-Sites enthält. An jedem Standort sind vier GSLB-Dienste (S-1, S-2, S-3 und S-4) an den virtuellen GSLB-Server VS-1 gebunden. Sie können einen virtuellen CS-Server (Content Switching) vom Zieltyp GSLB konfigurieren und eine CS-Richtlinie und -Aktion mit VS-1 als virtuellen Zielserver definieren, sodass Anfragen für Inhalte in Englisch nur von S-1 und S-2 bedient werden und Anforderungen für Inhalte in der lokalen Sprache nur von S-3 und S-4 bedient werden.

Sie können S-1 Priorität einräumen, indem Sie einen virtuellen Backupserver für VS-1 konfigurieren und S-2 an den virtuellen Backupserver binden. S-1 bedient die Client-Anfragen. Wenn der Server S-1 ausfällt, erfüllt S-2 die Anforderungen. Wenn sowohl S-1 als auch S-2 ausgefallen sind, erhalten Clients eine leere Antwort.

So konfigurieren Sie die GSLB-Dienstauswahl über Content Switching:

1. Konfigurieren Sie GSLB. Anweisungen finden Sie unter Konfigurieren des globalen Server-Lastenausgleichs.
2. Konfigurieren Sie einen virtuellen Content Switching-Server (CS) des Zieltyps GSLB. Weitere Informationen finden Sie unter Erstellen virtueller Server mit Content Switching.
3. Konfigurieren von Content Switching-Richtlinien (CS). Weitere Informationen finden Sie unter Content Switching-Richtlinien konfigurieren.
4. Konfigurieren Sie CS-Aktionen, die einen virtuellen GSLB-Server als virtuellen Zielserver festlegen. Weitere Informationen finden Sie unter Konfigurieren einer Content Switching-Aktion.
5. Binden Sie die CS-Richtlinien an den virtuellen CS Server. Weitere Informationen finden Sie unter Binden von Richtlinien an einen virtuellen Content Switching-Server.
6. Binden Sie die Domäne an den virtuellen CS Server anstelle des virtuellen GSLB-Servers.

Beispielkonfiguration

Die folgende Beispielkonfiguration sendet Anforderungen vom Client mit der IP-Adresse 5.5.5.5 an SERVICE_GSLB1 und SERVICE_GSLB2. SERVICE_GSLB1 hat eine höhere Priorität als SERVICE_GSLB2, und SERVICE_GSLB2 bedient die Client-Anforderungen nur, wenn SERVICE_GSLB1 heruntergefahren ist. Wenn sowohl SERVICE_GSLB1 als auch SERVICE_GSLB2 ausgefallen sind, werden SERVICE_GSLB3 und SERVICE_GSLB4 nicht berücksichtigt, und eine leere Antwort wird an den Client gesendet.

```
1 add cs vs CSVSERVER_GSLB http  -targettype GSLB
2 Done
3 add gslb vs VSERVER_GSLB1 http
4 Done
5 add gslb vs VSERVER_GSLB2 http
6 Done
7 add gslb vs VSERVER_GSLB_BACKUP1 http
8 Done
```



```
set gslb vs VSERVER_GSLB1 -backupvserver VSERVER_GSLB_BACKUP1
Done
add gslb service SERVICE_GSLB1 1.1.1.1 HTTP 80 -sitename site1
Done
add gslb service SERVICE_GSLB2 1.1.1.2 HTTP 80 -sitename site1
Done
add gslb service SERVICE_GSLB3 1.1.1.3 HTTP 80 -sitename site2
Done
add gslb service SERVICE_GSLB4 1.1.1.4 HTTP 80 -sitename site2
Done
bind gslb vs VSERVER_GSLB1 -servicename SERVICE_GSLB1
Done
bind gslb vs VSERVER_GSLB_BACKUP1 -servicename SERVICE_GSLB2
Done
bind gslb vs VSERVER_GSLB2 -servicename SERVICE_GSLB3
Done
bind gslb vs VSERVER_GSLB2 -servicename SERVICE_GSLB4
Done
add cs action a1 -targetvserver VSERVER_GSLB1
Done
add cs policy p1 -rule "CLIENT.IP.SRC.EQ(5.5.5.5)" -action a1
Done
bind cs vs CSVSERVER_GSLB -domainName www.abc.com
Done
bind cs vs CSVSERVER_GSLB -policyname p1 -priority 1
Done
add cs action a2 -targetvserver VSERVER_GSLB2
Done
add cs policy p2 -rule "CLIENT.IP.SRC.EQ(6.6.6.6)" -action a2
Done
bind cs vs CSVSERVER_GSLB -policyname p2 -priority 2
Done
<!--NeedCopy-->
```

Zuordnen eines virtuellen Zielserverausdrucks zu einer GSLB-Content Switching-Aktion

Sie können nun einen virtuellen Zielserverausdruck einer GSLB-Content Switching-Aktion zuordnen. Dadurch kann der virtuelle GSLB-Content Switching-Server Richtlinienausdrücke verwenden, um den Namen des virtuellen GSLB Zielservers während der Verarbeitung der DNS-Anforderungen zu erstellen.

So konfigurieren Sie eine Content Switching-Aktion, die einen Ausdruck mit der CLI angibt

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die Content Switching-Aktion so zu konfigurieren, dass die HTTP-Callout-Antwort abgerufen wird.

```
1 add cs action <name> -targetVserverExpr <expression>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add cs action csact_GSLB_VServer -targetVserverExpr ”SYS.HTTP_CALLOUT(
     GSLB_Method_API)”
2 <!--NeedCopy-->
```

So konfigurieren Sie eine Content Switching-Aktion, die einen Ausdruck mit der GUI angibt

1. Navigieren Sie zu **Traffic Management > Content Switching > Aktionen**.
2. Konfigurieren Sie eine Content Switching-Aktion, und geben Sie einen **Ausdruck** an, der den Namen des virtuellen Zielservers für den Lastenausgleich dynamisch berechnet.

Konfigurieren von GSLB für DNS-Abfragen mit NAPTR-Einträgen

October 5, 2021

In einer typischen GSLB-Bereitstellung (Global Server Load Balancing) empfängt die Citrix ADC Appliance DNS-Abfragen für A/AAAA-Einträge, wählt den am besten geeigneten GSLB-Dienst gemäß der konfigurierten Lastausgleichsmethode aus und gibt die IP-Adresse des Dienstes als Antwort auf die DNS-Abfrage zurück. Sie können die Appliance jetzt so konfigurieren, dass DNS-Abfragen für NAPTR-Einträge empfangen und mit der Liste der für eine Domäne konfigurierten Dienste antworten. Die Appliance überwacht auch den Zustand der Dienste, und in der Antwort stellt sie eine Liste der Dienste bereit, die ausgeführt werden.

Beispiel:

In Telco-Bereitstellungen können Sie eine Citrix ADC Appliance so konfigurieren, dass DNS-Abfragen mit NAPTR-Einträgen von Clients wie Mobile Management Entities (MMEs) empfangen werden, die die Rolle eines DNS-Resolvers spielen, um alle Dienste zu ermitteln, die vom Domänennamen angeboten werden. Die Appliance antwortet auf die Abfrage mit NAPTR-Datensätzen für alle Dienste, die ausgeführt werden. Die MME kann diese NAPTR-Antwort verwenden, um die S-NAPTR-Prozedur

auszuführen, um die Knoten auf der Grundlage des angebotenen Dienstes, der Colocation, der topologischen Nähe usw. auszuwählen.

Wenn mehrere Knoten ausgewählt werden können, kann das MME das Einstellungsfeld im NAPTR-Eintrag von der Citrix ADC Appliance verwenden, um den Knoten zu ermitteln.

NAPTR-Datensatzformat

Bei der Reaktion auf eine DNS-Abfrage mit NAPTR-Eintrag erstellt eine Citrix ADC Appliance einen Antwort-NAPTR-Eintrag für jeden GSLB-Dienst.

Die folgende Tabelle listet die Dateien im NAPTR-Datensatz auf:

Feld	
Domäne	Die GSLB-Domain
TTL	Die Zeitspanne, für die der NAPTR-Datensatz zwischengespeichert werden kann.
Klasse	Die Klasse des Datensatzes. Standardmäßig ist dieser Wert auf IN festgelegt.
Typ	Der DNS-Eintragstyp.
Bestellung	Gibt die Reihenfolge an, in der der NAPTR-Datensatz verarbeitet werden muss. Sie können die Reihenfolge im GSLB-Dienst angeben. Andernfalls ist es auf 1 gesetzt.
Präferenz	Gibt die Reihenfolge an, in der NAPTR-Datensätze mit gleichen order -Werten verarbeitet werden sollen, wobei niedrige Zahlen vor hohen Zahlen verarbeitet werden. Wenn die Bestellung nicht im GSLB-Dienst angegeben ist, wird sie auf 1 gesetzt.
Flags	Steuert die Aspekte des Umschreibens und der Interpretation der Felder im Datensatz. Die Citrix ADC Appliance legt diesen Wert auf A fest.
Service	Gibt die verfügbaren Dienste an.
Regulärer Ausdruck	Reguläre Ausdrücke werden nicht unterstützt, daher wird dieser Wert auf NULL gesetzt.
Ersatz	Der Domänenname des Knotens, der die Dienste hostet.

Konfigurationsprozedur

Ausführliche Anweisungen zur GSLB-Konfiguration finden Sie unter Konfigurieren des globalen Server-Lastenausgleichs (GSLB). Stellen Sie sicher, dass Sie Folgendes tun:

- Legen Sie beim Hinzufügen des virtuellen GSLB-Servers die folgenden Parameter fest:
  - serviceType: ANY
  - dnsRecordType: NAPTR
  - lbMethod: CUSTOMLOAD

Beispiel:

```
add gslb vserver gslb_vs ANY -dnsRecordType NAPTR -lbMethod CUSTOMLOAD
<!--NeedCopy-->
```

- Legen Sie beim Hinzufügen einer GSLB-Site den Parameter *NaptrReplacementSuffix* auf den Domänennamen fest, den Sie in die NAPTR-Datensätze einbetten möchten.

Beispiel:

```
add gslb site site1 10.102.218.200  -naptrReplacementSuffix example.com
<!--NeedCopy-->
```

- Legen Sie beim Hinzufügen des GSLB-Dienstes die folgenden Parameter fest:
  - naptrreplacement
  - naptrOrder
  - naptrServices
  - naptrDomainTTL
  - naptrPreference

Beispielkonfiguration

```
add gslb vserver gslb_vs ANY -dnsRecordType NAPTR -lbMethod CUSTOMLOAD

Done

add gslb site site1 10.102.218.200  -naptrReplacementSuffix example.com

Done

```



```
add gslb service sgw1 3.3.3.13 ANY *  -siteName site1 -naptrreplacement sgw1.site1. -naptrOrder 2 -naptrServices x-3gpp-sgw:x-s5-gtp -naptrDomainTTL 20 -naptrPreference   200

Done

add gslb service sgw2 3.3.3.11 ANY *  -siteName site1 -naptrreplacement sgw2.site1. -naptrOrder 5 -naptrServices x-3gpp-sgw:x-s5-gtp  -naptrDomainTTL 20  naptrPreference  100

Done

add gslb service sgw3 3.3.3.12 ANY *  -siteName site2 -naptrreplacement sgw3.site1. -naptrOrder 10 -naptrServices x-3gpp-sgw:x-s5-gtp  -naptrDomainTTL 20 naptrPreference   300

bind gslb vserver gslb_vs -serviceName sgw1

Done

bind gslb vserver gslb_vs -serviceName sgw2

Done

bind gslb vserver gslb_vs -serviceName sgw3

Done

bind gslb service sgw1 -monitorName ping

Done

bind gslb service sgw2 -monitorName ping

Done

bind gslb service sgw3 -monitorName ping

Done

bind gslb vserver gslb_vs -domainName gslb.com -TTL 5

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


> **Hinweis:**
>
> DNS-Abfragen mit NAPTR-Einträgen werden in der übergeordneten und untergeordneten Konfiguration nicht unterstützt.

Konfigurieren von GSLB für Wildcard-Domäne

October 5, 2021

Sie können eine Wildcard-DNS-Domäne an einen virtuellen GSLB-Server binden. Benutzer, die auf die Anwendungen hinter einer Platzhalterdomäne zugreifen, werden an das optimale Rechenzentrum weitergeleitet, in dem diese Anwendungen gehostet werden. Die Platzhalterdomäne verarbeitet Anforderungen für nicht vorhandene Domänen und Unterdomänen. Weitere Informationen zu Platzhalter-Domänen finden Sie unter Unterstützen von Platzhalter-DNS-Domänen.

Um GSLB für eine Platzhalterdomäne zu konfigurieren, müssen Sie zunächst das grundlegende GSLB-Setup konfigurieren. Weitere Informationen zur Konfiguration eines grundlegenden GSLB-Setups finden Sie unter Konfigurieren von GSLB-Entitäten einzeln.

So konfigurieren Sie ein GSLB-Setup für Platzhalterdomäne mit der CLI

Führen Sie die folgenden Schritte aus, um ein GSLB-Setup für die Platzhalterdomäne zu konfigurieren:

1. Erstellen Sie die GSLB-Sites.

```
add gslb site site1 10.0.1.10
add gslb site site2 20.0.1.10
<!--NeedCopy-->
```

2. Fügen Sie die GSLB-Dienste für jeden Standort hinzu, der am GSLB-Setup beteiligt ist.

```
add gslb service svc1 -sitename site1 10.0.1.10  http 80
add gslb service svc2 -sitename site1 10.0.1.10  http 80
add gslb service svc3 -sitename site2 20.0.1.10  http 80
add gslb service svc4 -sitename site2 20.0.1.10  http 80
<!--NeedCopy-->
```

3. Fügen Sie den virtuellen GSLB-Server hinzu, der auf einen Dienst verweist, der im GSLB-Setup verwendet wird.


```
add gslb vserver gslb_vs http
<!--NeedCopy-->
```

4. Fügen Sie einen ADNS-Dienst hinzu, der die DNS-Abfragen überwacht.

```
add service adns_udp 10.14.39.21 ADNS 53
<!--NeedCopy-->
```

5. Binden Sie die GSLB-Dienste an den virtuellen GSLB-Server.

```
bind gslb vserver gslb_vs -service svc1
bind gslb vserver gslb_vs -service svc2
bind gslb vserver gslb_vs -service svc3
bind gslb vserver gslb_vs -service svc4
<!--NeedCopy-->
```

6. Erstellen Sie eine Zone.

```
add dns soaRec test.com -originServer n1.test.com -contact n1.test
    .com
add dns nsrec test.com n1.test.com
add dns nsrec test.com n2.test.com
add dns zone test.com -proxymode no
<!--NeedCopy-->
```

7. Binden Sie den Domänennamen an den virtuellen GSLB-Server.

```
bind gslb vserver gslb_vs -domainName *.test.com
<!--NeedCopy-->
```

Verwenden Sie die Option für das EDNS0-Clientsubnetz für den globalen Server-Lastenausgleich

October 5, 2021

EDNS Client Subnet (ECS) ist eine Domänennamenserver-Header-Erweiterung (DNS), die die Details zum Client-Subnetz enthält. Sie können diese Details verwenden, um die Genauigkeit von Citrix ADC Global Server Load Balancing (GSLB) zu verbessern, indem Sie den Speicherort des Clientnetzwerks anstelle des DNS-Auflösungsortes verwenden, um die topologische Nähe des Clients zu bestimmen.

> **Hinweis:**
>
> Citrix ADC unterstützt nur EDNS0.

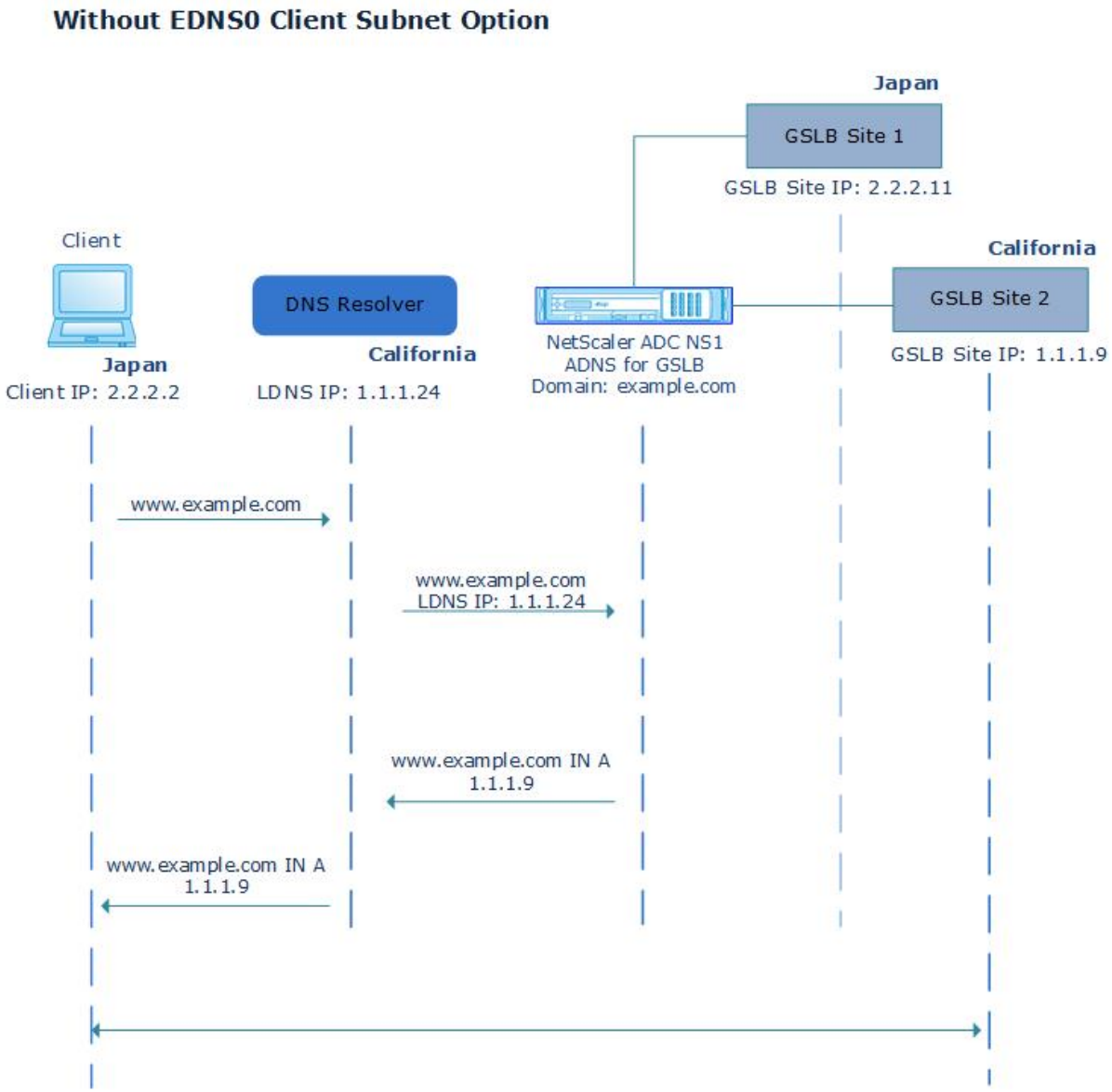
Wichtig:

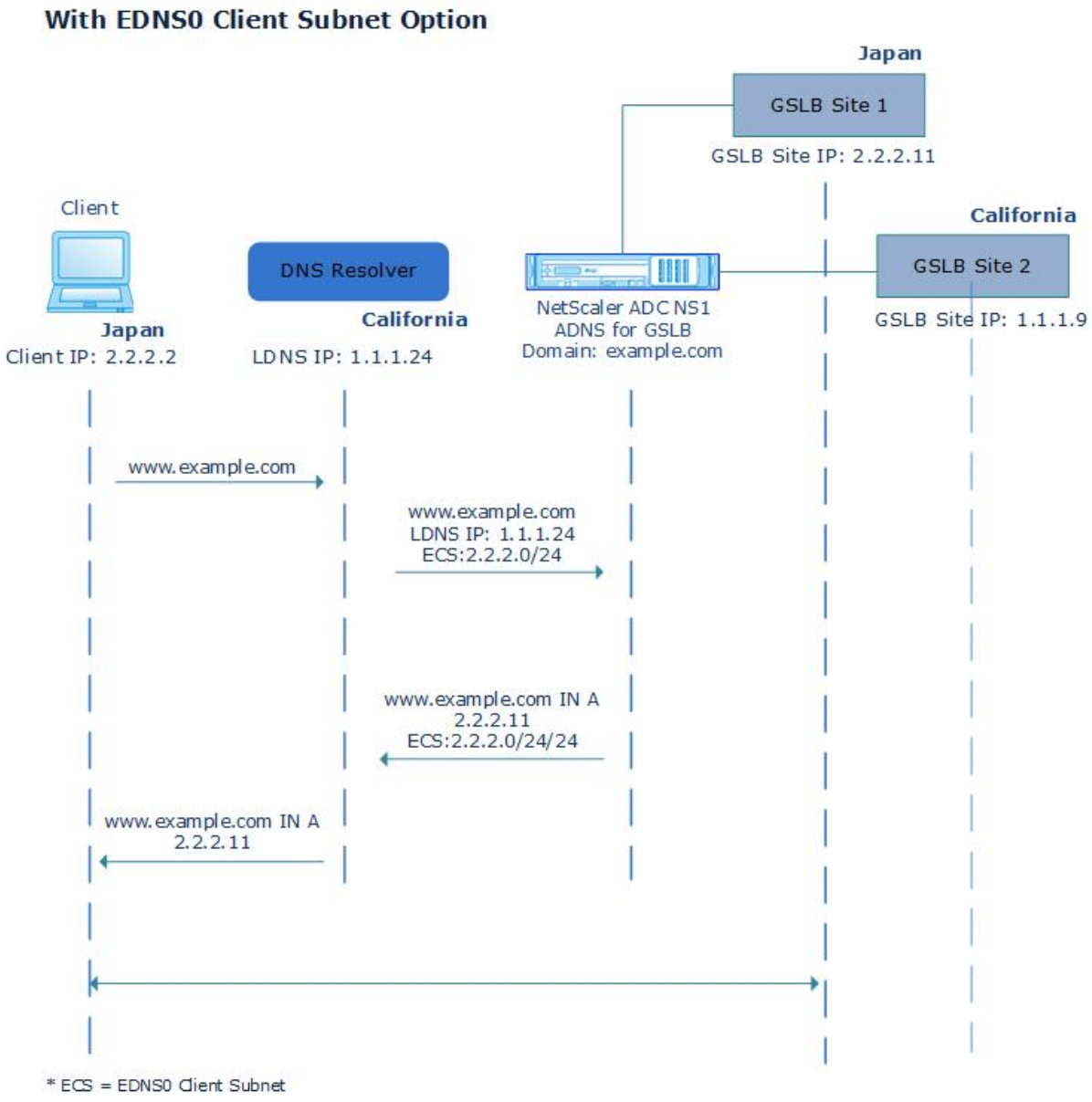
> Stellen Sie sicher, dass der lokale Domänennamenserver (LDNS) in Ihrer Bereitstellung das EDNS0-Clientsubnetz unterstützt, sodass die eingehenden DNS-Abfragen die Option EDNS0 Client Subnet enthalten und die Citrix ADC Appliance während der Verarbeitung der DNS-Abfrage die ECS-Adresse verwendet.

Die Citrix ADC Appliance verwendet die LDNS-IP-Adresse zur Bestimmung der topologischen Nähe des Clients und führt GSLB aus, wenn Sie proximitätsbasierte Load Balancing-Methoden wie statische Nähe oder dynamische Roundtrip-Zeit (RTT) verwenden. Dies geschieht in einer typischen GSLB-Bereitstellung. Wenn jedoch ein zentralisierter DNS-Resolver wie Google DNS oder OpenDNS an der Bereitstellung beteiligt ist, sendet die Citrix ADC Appliance die DNS-Anfrage an ein Rechenzentrum in der Nähe des zentralisierten DNS-Resolvers, der möglicherweise nicht in der Nähe des Clients liegt. Beispielsweise wird in einer typischen Citrix ADC GSLB-Bereitstellung mit der statischen Proximity-Load-Balancing-Methode eine Endbenutzeranforderung aus Japan an ein Rechenzentrum in Japan gesendet und eine Endbenutzeranforderung aus Kalifornien an ein Rechenzentrum in Kalifornien gesendet. Wenn jedoch ein zentralisierter DNS-Resolver beteiligt ist, sendet die Citrix ADC Appliance möglicherweise eine Anfrage aus Japan an ein Rechenzentrum in Kalifornien.

Sie können die ECS-Option in Bereitstellungen verwenden, die die Citrix ADC Appliance enthalten, die als autoritativer DNS-Server (ADNS) für eine GSLB-Domäne konfiguriert ist. Wenn Sie statische Nähe als Load Balancing-Methode verwenden, können Sie anstelle der LDNS-IP-Adresse das IP-Subnetz im EDNS-Header verwenden. Dies hilft, die geografische Nähe des Kunden zu bestimmen. Bei der Bereitstellung im Proxymodus leitet die Citrix ADC Appliance eine ECS-fähige DNS-Abfrage unverändert an die Backend-Server weiter. Die Appliance speichert keine ECS-fähigen DNS-Antworten.

> **Hinweis:**
>
> Die ECS-Option ist nicht für alle anderen Bereitstellungsmodi anwendbar, z. B. den ADNS-Modus für Nicht-GSLB-Domänen, den Auflösungsmodus und den Weiterleitungsmodus. Die ECS-Option wird von der Citrix ADC Appliance in den oben genannten Modi ignoriert. Außerdem ist ECS standardmäßig für die GSLB-Bereitstellung deaktiviert.





So aktivieren Sie die Option EDNS0 Client Subnet über die Befehlszeile:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set gslb vserver <vserver_name> **-ECS ENABLED

set gslb vserver vserver-GSLB-1 -ECS ENABLED
<!--NeedCopy-->
```


Adress-Validierung

Sie können einen virtuellen GSLB-Server konfigurieren, um sicherzustellen, dass die von der Option EDNS0 Client Subnet (ECS) der DNS-Abfrage zurückgegebene Adresse keine private oder nicht routable IP-Adresse ist. Wenn die Adressprüfung aktiviert ist, ignoriert die Citrix ADC Appliance die ECS-Adresse in der DNS-Abfrage, wenn sie in der folgenden Tabelle aufgeführt ist, und verwendet stattdessen die LDNS-IP-Adresse für den globalen Server-Lastausgleich.

> **Hinweis:**
>
> Standardmäßig ist die Adressprüfung deaktiviert.

Adresstyp	Adresse	Beschreibung
IPV4	10.0.0.0/8	Für den privaten Gebrauch
	172.16.0.0/12	Für den privaten Gebrauch
	192,168.0.0/16	Für den privaten Gebrauch
	0.0.0.0/8	Bezieht sich auf den Host im Netzwerk
	100.64.0.0/10	Gemeinsamer Adressraum
	127.0.0.0/8	Loopback-Adresse
	169.254.0.0/16	Lokale IPv4-Adresse gemäß RFC 3927 verknüpfen
	192.0.0.0/24	Wird für IETF-Protokollzuweisungen verwendet, enthält den privaten Bereich 192.168.0.0/16
	192.0.2.0/24	Für Dokumentationszwecke verwendet
	192,88,99,0/24	Verwendet für 6to4 Relais Anycast
	198.18.0.0/15	Wird in Geräte-Benchmark-Tests verwendet
	198.51.100.0/24	Für Dokumentationszwecke verwendet

Adresstyp	Adresse	Beschreibung
	203.0.113.0/24	Für Dokumentationszwecke verwendet
	240.0.0.0/4	Wird als reserviert verwendet
	255,255,255,255/32	Wird für Broadcast verwendet
IPv6	::1/128	Loopback-Adresse
	::/128	nicht angegebene Adresse
	::ffff:0:0/96	IPv4-zugeordnete Adresse
	100::/64	Nur Adressblock verworfen
	2001::/23	Wird für IETF-Protokollzuweisungen verwendet
	2001::/32	TEREDO
	2001:2::/48	Verwendet für Benchmarking
	2001:db8::/32	Für Dokumentationszwecke verwendet
	2001:10::/28	ORCHID
	2002::/16	Verwendet für 6to4 Relais Anycast
	fc00::/7	Unique-local
	fe80::/10	Lokale Unicast-Adressen verknüpfen

So aktivieren Sie die Adressprüfung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set gslb vserver <vserver_name> -ecsAddrValidation ENABLED

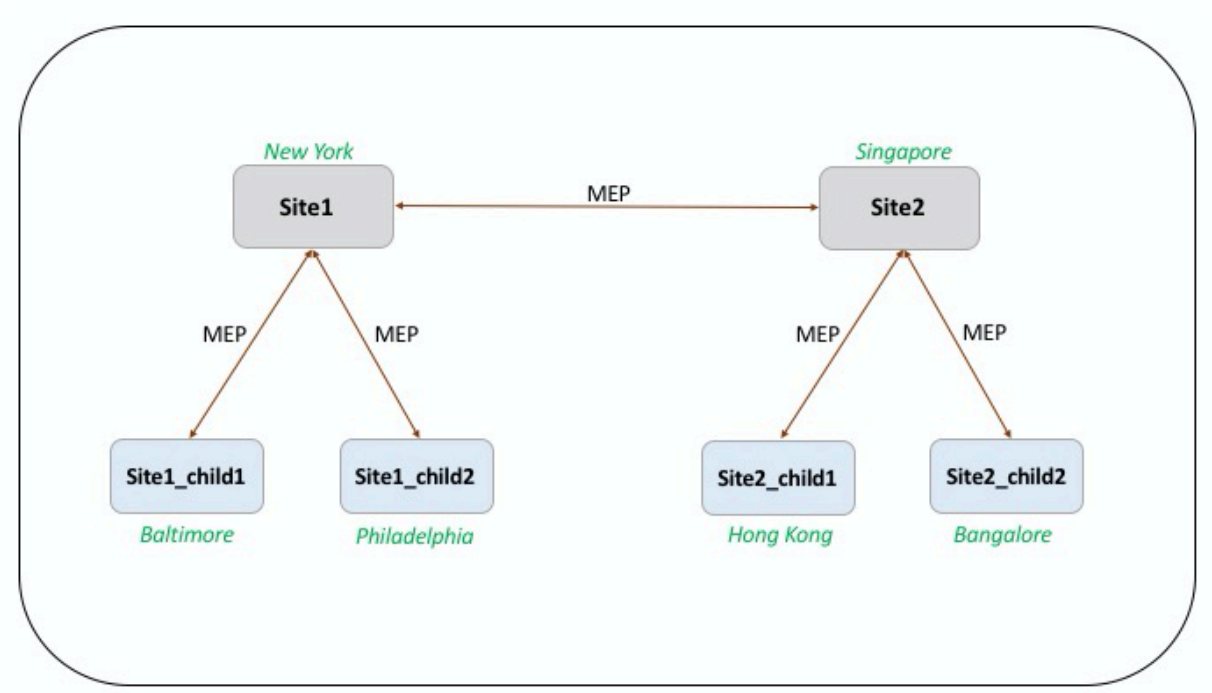
set gslb vserver vserver-GSLB-1 -ecsAddrValidation ENABLED
<!--NeedCopy-->
```


Beispiel für eine vollständige Parent-Child-Konfiguration mit dem Metrics Exchange Protocol

October 5, 2021

Betrachten Sie die folgende übergeordnete und untergeordnete Topologie, in der die GSLB-Sites global verteilt sind.

- Site1 und Site2 sind die übergeordneten Sites.
- Site1_Child1 und Site1_Child2 sind die untergeordneten Sites von Site1.
- Site2_Child1 und Site2_Child2 sind die untergeordneten Sites von Site2.



Die folgenden Befehle veranschaulichen die vollständige Konfiguration der über-/untergeordneten Topologie.

site1

```
1 add gslb site site1 10.102.82.164 -publicIP 10.102.82.164
2
3 add gslb site site2 10.106.24.164 -publicIP 10.106.24.164
4
5 add gslb site site1_child1 10.102.82.131 -publicIP 10.102.82.131 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1
```



```
6
7  add gslb site site1_child2 10.102.82.67 -publicIP 10.102.82.67 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site1
8
9  add gslb site site2_child1 10.106.24.132 -publicIP 10.106.24.132 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site2
10
11 add gslb site site2_child2 10.106.24.67 -publicIP 10.106.24.67 -
       nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
       site2
12
13 add gslb service site1_child1_http_gsvc1 10.102.82.132 HTTP 80 -
       publicIP 10.102.82.132 -publicPort 80 -maxClient 0 -siteName
       site1_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
14
15 add gslb service site1_child2_http_gsvc1 10.102.82.68 HTTP 80 -publicIP
        10.102.82.68 -publicPort 80 -maxClient 0 -siteName site1_child2 -
       cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
16
17 add gslb service site2_child1_http_gsvc1 10.106.24.134 HTTP 80 -
       publicIP 10.106.24.134 -publicPort 80 -maxClient 0 -siteName
       site2_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
18
19 add gslb service site2_child2_http_gsvc1 10.106.24.68 HTTP 80 -publicIP
        10.106.24.68 -publicPort 80 -maxClient 0 -siteName site2_child2 -
       cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED
20
21 add gslb vserver gv1 HTTP -backupLBMethod ROUNDROBIN -tolerance 0 -
       appflowLog DISABLED
22
23 bind gslb vserver gv1 -serviceName site1_child1_http_gsvc1
24
25 bind gslb vserver gv1 -serviceName site1_child2_http_gsvc1
26
27 bind gslb vserver gv1 -serviceName site2_child2_http_gsvc1
28
29 bind gslb vserver gv1 -serviceName site2_child1_http_gsvc1
30
31 bind gslb vserver gv1 -domainName www.gslb.com -TTL 5
32 <!--NeedCopy-->
```


site1_child1

```
add gslb site site1 10.102.82.164 -publicIP 10.102.82.164

add gslb site site1_child1 10.102.82.131 -publicIP 10.102.82.131 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1
<!--NeedCopy-->
```

Sie können die folgenden Befehle für die Konfiguration des Lastenausgleichs hinzufügen:

```
add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
     -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -
    svrTimeout 360 -CKA NO -TCPB NO -CMP NO

add lb vserver lb1 HTTP 10.102.82.132 80 -persistenceType NONE -
    cltTimeout 180

bind lb vserver lb1 svc1
<!--NeedCopy-->
```

site1_child2

```
add gslb site site1 10.102.82.164 -publicIP 10.102.82.164

add gslb site site1_child2 10.102.82.67 -publicIP 10.102.82.67 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1

You can add the following commands for load balancing configuration:

add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
     -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -
    svrTimeout 360 -CKA NO -TCPB NO -CMP NO

add lb vserver lb1 HTTP 10.102.82.68 80 -persistenceType NONE -
    cltTimeout 180

bind lb vserver lb1 svc1
<!--NeedCopy-->
```


site2

```
add gslb site site1 10.102.82.164 -publicIP 10.102.82.164

add gslb site site2 10.106.24.164 -publicIP 10.106.24.164

add gslb site site1_child1 10.102.82.131 -publicIP 10.102.82.131 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1

add gslb site site1_child2 10.102.82.67 -publicIP 10.102.82.67 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site1

add gslb site site2_child1 10.106.24.132 -publicIP 10.106.24.132 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site2

add gslb site site2_child2 10.106.24.67 -publicIP 10.106.24.67 -
    nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
    site2

add gslb service site1_child1_http_gsvc1 10.102.82.132 HTTP 80 -
    publicIP 10.102.82.132 -publicPort 80 -maxClient 0 -siteName
    site1_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED

add gslb service site1_child2_http_gsvc1 10.102.82.68 HTTP 80 -publicIP
     10.102.82.68 -publicPort 80 -maxClient 0 -siteName site1_child2 -
    cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED

add gslb service site2_child1_http_gsvc1 10.106.24.134 HTTP 80 -
    publicIP 10.106.24.134 -publicPort 80 -maxClient 0 -siteName
    site2_child1 -cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED

add gslb service site2_child2_http_gsvc1 10.106.24.68 HTTP 80 -publicIP
     10.106.24.68 -publicPort 80 -maxClient 0 -siteName site2_child2 -
    cltTimeout 180 -svrTimeout 360 -downStateFlush ENABLED

add gslb vserver gv1 HTTP -backupLBMethod ROUNDROBIN -tolerance 0 -
    appflowLog DISABLED

bind gslb vserver gv1 -serviceName site1_child1_http_gsvc1

bind gslb vserver gv1 -serviceName site1_child2_http_gsvc1
```



```
26
27 bind gslb vserver gv1 -serviceName site2_child2_http_gsvc1
28
29 bind gslb vserver gv1 -serviceName site2_child1_http_gsvc1
30
31 bind gslb vserver gv1 -domainName www.gslb.com -TTL 5
32 <!--NeedCopy-->
```

site2_child1

```
1 add gslb site site2 10.106.24.164 -publicIP 10.106.24.164
2
3 add gslb site site2_child1 10.106.24.132 -publicIP 10.106.24.132 -
     nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
     site2
4 <!--NeedCopy-->
```

You can add the following commands for load balancing configuration:

```
1 add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
      -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -
     svrTimeout 360 -CKA NO -TCPB NO -CMP NO
2
3 add lb vserver lb1 HTTP 10.106.24.134 80 -persistenceType NONE -
     cltTimeout 180
4
5 bind lb vserver lb1 svc1
6 <!--NeedCopy-->
```

site2_child2

```
1 add gslb site site2 10.106.24.164 -publicIP 10.106.24.164
2
3 add gslb site site2_child2 10.106.24.67 -publicIP 10.106.24.67 -
     nwMetricExchange DISABLED -sessionExchange DISABLED -parentSite
     site2
4 <!--NeedCopy-->
```

You can add the following commands for load balancing configuration:


```
add service svc1 10.102.82.25 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0
     -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -
    svrTimeout 360 -CKA NO -TCPB NO -CMP NO

add lb vserver lb1 HTTP 10.106.24.68 80 -persistenceType NONE -
    cltTimeout 180

bind lb vserver lb1 svc1
\`\`\`
<!--NeedCopy-->
```

Link-Lastenausgleich

October 5, 2021

Link Load Balancing (LLB) gleicht ausgehenden Datenverkehr über mehrere Internetverbindungen aus, die von verschiedenen Dienstanbietern bereitgestellt werden. LLB ermöglicht es der Citrix ADC Appliance, den Datenverkehr zu überwachen und zu steuern, sodass Pakete nahtlos über die bestmögliche Verbindung übertragen werden. Im Gegensatz zum Server Load Balancing, bei dem ein Dienst einen Server darstellt, mit LLB, stellt ein Dienst einen Router oder den nächsten Hop dar. Eine Verbindung ist eine Verbindung zwischen der Citrix ADC Appliance und dem Router.

Um den Link-Load Balancing zu konfigurieren, konfigurieren viele Benutzer zunächst ein grundlegendes Setup mit Standardeinstellungen. Ein grundlegendes Setup umfasst Dienste, virtuelle Server, Monitore, Routen, eine LLB-Methode und Persistenz (optional). Sobald ein Basis-Setup betriebsbereit ist, können Sie es für Ihre Umgebung anpassen.

Load Balancing-Methoden, die für LLB gelten, sind Round Robin, Ziel-IP-Hash, geringste Bandbreite und geringste Pakete. Sie können optional Persistenz für Verbindungen konfigurieren, die auf einem bestimmten Link aufrechterhalten werden. Die verfügbaren Persistenztypen sind Quell-IP-Adressen, Ziel-IP-Adressen und Quell-IP- und Ziel-IP-Adressen. PING ist der Standardmonitor, aber die Konfiguration eines transparenten Monitors wird empfohlen.

Sie können Ihre Einrichtung anpassen, indem Sie Reverse NAT (RNAT) und Backup-Links konfigurieren.

Konfigurieren einer grundlegenden LLB-Setup

December 7, 2021

Um LLB zu konfigurieren, erstellen Sie zuerst Dienste, die jeden Router für die Internet Service Provider (ISPs) darstellen. Ein PING-Monitor ist standardmäßig an jeden Dienst gebunden. Die Bindung eines transparenten Monitors ist optional, wird jedoch empfohlen. Anschließend erstellen Sie einen virtuellen Server, binden die Dienste an den virtuellen Server und konfigurieren eine Route für den virtuellen Server. Die Route identifiziert den virtuellen Server als Gateway zu den physischen Routern, die von den Diensten dargestellt werden. Der virtuelle Server wählt einen Router mithilfe der von Ihnen angegebenen Load Balancing-Methode aus. Optional können Sie Persistenz konfigurieren, um sicherzustellen, dass der gesamte Datenverkehr für eine bestimmte Sitzung über einen bestimmten Link gesendet wird.

Gehen Sie folgendermaßen vor, um eine grundlegende LLB-Setup zu konfigurieren:

- Konfigurieren von Diensten
- Konfigurieren eines virtuellen LLB-Servers und Binden eines Dienstes
- Konfigurieren der LLB-Methode und der Persistenz
- Konfigurieren einer LLB-Route
- Erstellen und Binden eines transparenten Monitors

Konfigurieren von Diensten

Ein Standardmonitor (PING) wird beim Erstellen des Dienstes automatisch an einen Servicetyp von ANY gebunden, Sie können jedoch den Standardmonitor durch einen transparenten Monitor ersetzen, wie unter Erstellen und Binden eines transparenten Monitorsbeschrieben.

So erstellen Sie einen Dienst mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name> <IP> <serviceType> <port>

show service <name>
<!--NeedCopy-->
```

Beispiel:

```
add service ISP1R_svc_any 10.10.10.254 any *
show service ISP1R_svc_any
        ISP1R_svc_any (10.10.10.254:*) - ANY
        State: DOWN
```



```
        Last state change was at Tue Aug 31 04:31:13 2010
        Time since last state change: 2 days, 05:34:18.600
        Server Name: 10.10.10.254
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): YES
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: ping
                State: UP       Weight: 1
                Probes: 244705  Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.322 millisec
 Done
<!--NeedCopy-->
```

So erstellen Sie Dienste mit dem Konfigurationsdienstprogramm

Navigieren Sie zu Traffic Management > Load Balancing > Services, und erstellen Sie einen Dienst.

So erstellen Sie Dienste mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Geben Sie im Dialogfeld Dienst erstellen Werte für die folgenden Parameter an:
   - Dienstname* — Name
   - Server — IP
   - Protokol* — ServiceType (Wählen Sie ANY aus der Dropdownliste aus.)
   - Anschluss* — Anschluss

Ein erforderlicher Parameter

1. Klicken Sie auf Erstellen.

2. Wiederholen Sie die Schritte 2-4, um einen anderen Dienst zu erstellen.
3. Klicken Sie auf Schließen.
4. Wählen Sie im Bereich Dienste die Dienste aus, die Sie gerade konfiguriert haben, und überprüfen Sie, ob die am unteren Bildschirmrand angezeigten Einstellungen korrekt sind.

Konfigurieren eines virtuellen LLB-Servers und Binden eines Dienstes

Nachdem Sie einen Dienst erstellt haben, erstellen Sie einen virtuellen Server und binden Dienste an den virtuellen Server. Die standardmäßige LB-Methode der geringsten Verbindungen wird in LLB nicht unterstützt. Informationen zum Ändern der LB-Methode finden Sie unter Konfigurieren der LLB-Methode und Persistenz.

So erstellen Sie einen virtuellen Link-Lastausgleichsserver und binden einen Dienst mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <serviceType>

bind lb vserver < name> <serviceName>

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

Beispiel:

```
add lb vserver LLB-vip any
bind lb vserver LLB-vip ISP1R_svc_any
sh lb vserver LLB-vip
        LLB-vip (0.0.0.0:0) - ANY    Type: ADDRESS
        State: DOWN
        Last state change was at Thu Sep  2 10:51:32 2010
        Time since last state change: 0 days, 17:51:46.770
        Effective State: DOWN
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  1 (Total)       0 (Active)
        Configured Method: ROUNDROBIN
        Mode: IP
```



```
        Persistence: NONE
        Connection Failover: DISABLED

1) ISP1R_svc_any (10.10.10.254: *) - ANY State: DOWN    Weight: 1
 Done
<!--NeedCopy-->
```

So erstellen Sie einen virtuellen Link-Lastausgleichsserver und binden einen Dienst mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und erstellen Sie einen virtuellen Server für den Link-Lastenausgleich. Geben Sie **ANY** im Feld **Protokoll** an.
2. Wählen Sie in der Dropdownliste **IP-Adresstyp** die gewünschte Option aus. Wählen Sie **Nicht Adressierbar**, um einen virtuellen Server zu erstellen, auf den nicht direkt zugegriffen werden kann.
3. Aktivieren Sie auf der Registerkarte **Dienste** in der Spalte **Aktiv** das Kontrollkästchen für den Dienst, den Sie an den virtuellen Server binden möchten.

Konfigurieren der LLB-Methode und der Persistenz

Standardmäßig verwendet die Citrix ADC Appliance die Methode der wenigsten Verbindungen, um den Dienst für die Umleitung jeder Clientanforderung auszuwählen, aber Sie sollten die LLB-Methode auf eine der unterstützten Methoden festlegen. Sie können die Persistenz auch so konfigurieren, dass verschiedene Übertragungen vom selben Client an denselben Server weitergeleitet werden.

So konfigurieren Sie die LLB-Methode und/oder die Persistenz mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

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

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

Beispiel:


```
set lb vserver LLB-vip -lbmethod ROUNDROBIN -persistencetype SOURCEIP

show lb vserver LLB-vip
        LLB-vip (0.0.0.0:0) - ANY    Type: ADDRESS
        State: DOWN
        Last state change was at Fri Sep  3 04:46:48 2010
        Time since last state change: 0 days, 00:52:21.200
        Effective State: DOWN
        Client Idle Timeout: 120 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        No. of Bound Services :  0 (Total)       0 (Active)
        Configured Method: ROUNDROBIN
        Mode: IP
        Persistence: SOURCEIP
     Persistence Mask: 255.255.255.255       Persistence v6MaskLength:
         128   Persistence Timeout: 2 min
        Connection Failover: DISABLED
<!--NeedCopy-->
```

So konfigurieren Sie die Link-Load-Balancing-Methode und/oder die Persistenz mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server, und wählen Sie den virtuellen Server aus, für den Sie die Lastausgleichsmethode und/oder Persistenzeinstellungen konfigurieren möchten.
2. Wählen Sie im Abschnitt **Erweiterte Einstellungen** die Option Methode aus, und konfigurieren Sie die Lastausgleichsmethode.
3. Wählen Sie im Abschnitt **Erweiterte Einstellungen Persistenz** aus, und konfigurieren Sie die Persistenzparameter.

Konfigurieren einer LLB-Route

Nach der Konfiguration der IPv4- oder IPv6-Dienste, der virtuellen Server, der LLB-Methoden und der Persistenz konfigurieren Sie eine IPv4- oder IPv6-LLB-Route für das Netzwerk, die den virtuellen LLB-Server als Gateway angibt. Eine Route ist eine Sammlung von Links, die Lastenausgleich sind. Anforderungen werden an die IP-Adresse des virtuellen LLB-Servers gesendet, die als Gateway für den gesamten ausgehenden Datenverkehr fungiert und den Router basierend auf der konfigurierten LLB-Methode auswählt.

So konfigurieren Sie eine IPv4-LLB-Route mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb route <network> <netmask> <gatewayName>

show lb route [<network> <netmask>]
<!--NeedCopy-->
```

Beispiel:

```
add lb route 0.0.0.0 0.0.0.0 LLB-vip
show lb route 0.0.0.0 0.0.0.0
       Network          Netmask        Gateway/VIP               Flags
     -----------      -------------   --------------          --------
1)     0.0.0.0          0.0.0.0        LLB-vip                UP
<!--NeedCopy-->
```

So konfigurieren Sie eine IPv6-LLB-Route mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb route6 <network> <gatewayName>

show lb route6
<!--NeedCopy-->
```

Beispiel:

```
add lb route6 ::/0 llb6_vs show lb route6 Network VIP Flags -----------
     --------- -------- 1) ::/0 llb6_vs UP
<!--NeedCopy-->
```

So konfigurieren Sie eine LLB-Route mit dem Konfigurationsdienstprogramm

Navigieren Sie zu System > Netzwerk > Routen, wählen Sie **LLB**aus, und konfigurieren Sie die LLB-Route.

Hinweis: Wählen Sie LLBV6, um eine IPV6-Route zu konfigurieren.

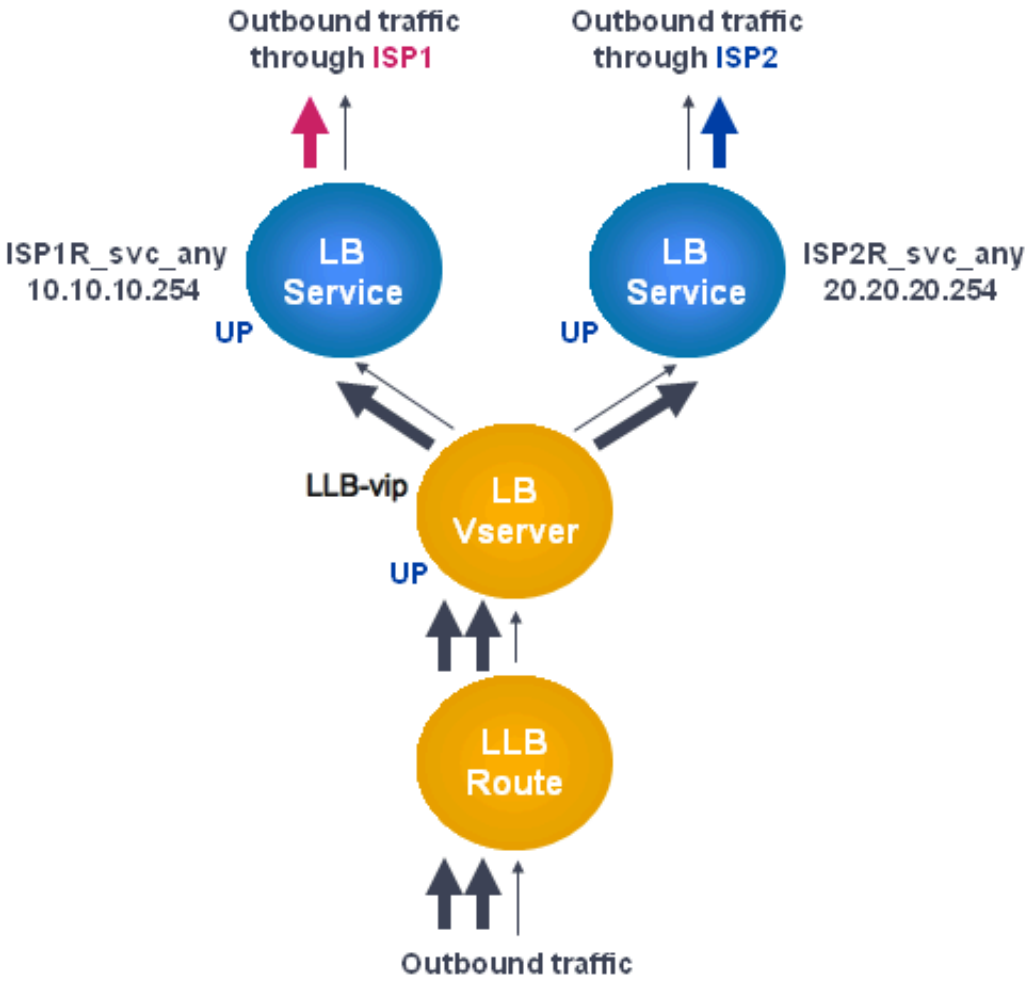
So konfigurieren Sie eine LLB-Route mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu System > Netzwerk > Routen.
2. Wählen Sie im Detailbereich eine der folgenden Optionen aus:
   - Klicken Sie auf LLB, um eine IPv4-Route zu konfigurieren.
   - Klicken Sie auf LLBV6, um eine IPv4-Route zu konfigurieren.
3. Legen Sie im Dialogfeld LB-Route erstellen oder LB-IPV6-Route erstellen die folgenden Parameter fest:
   - Netzwerk*
   - Netmask* — Erforderlich für IPV4-Routen.
   - Gatewayname* — GatewayName

     * Ein erforderlicher Parameter
4. Klicken Sie auf Erstellenund dann auf Schließen. Die gerade erstellte Route wird auf der Registerkarte LLB oder LLB6 im Bereich Routen angezeigt.

Das folgende Diagramm zeigt eine grundlegende LLB-Setup. Für jeden der beiden Links (ISPs) wird ein Dienst konfiguriert, und PING-Monitore sind standardmäßig an diese Dienste gebunden. Ein Link wird basierend auf der konfigurierten LLB-Methode ausgewählt.

Abbildung 1. Grundlegende LLB-Setup



> **Hinweis:**
>
> Wenn Ihr Internetdienstanbieter eine IPv6-Adresse angegeben hat, ersetzen Sie den IPv4-Dienst durch einen IPv6-Dienst in der obigen Abbildung.

Erstellen und Binden eines transparenten Monitors

Sie erstellen einen transparenten Monitor, um den Zustand von Upstream-Geräten wie Routern zu überwachen. Anschließend können Sie den transparenten Monitor an Dienste binden. Der standardmäßige PING-Monitor überwacht nur die Konnektivität zwischen der Citrix ADC Appliance und dem Upstream-Gerät. Der transparente Monitor überwacht alle Geräte, die im Pfad von der Appliance zu dem Gerät vorhanden sind, dem die im Monitor angegebene Ziel-IP-Adresse gehört. Wenn ein transparenter Monitor nicht konfiguriert ist und der Status des Routers UP ist, aber eines der nächsten Hop-Geräte dieses Routers ausgefallen ist, schließt die Appliance den Router während des Lastausgleichs ein und leitet das Paket an den Router weiter. Das Paket wird jedoch nicht an das endgültige

Ziel geliefert, da eines der nächsten Hop-Geräte ausgefallen ist. Wenn eines der Geräte (einschließlich des Routers) ausgefallen ist, wird der Dienst durch Bindung eines transparenten Monitors als DOWN gekennzeichnet, und der Router ist nicht im Lieferumfang enthalten, wenn die Appliance den Link-Load-Balancing durchführt.

So erstellen Sie einen transparenten Monitor mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb monitor <monitorName> <type> -destIP <ip_addr|*> -transparent
   YES

show lb monitor [<monitorName>]
<!--NeedCopy-->
```

Beispiel:

```
add lb monitor monitor-1 PING -destIP 10.10.10.11 -transparent YES
> show lb monitor monitor-1
1)   Name.......: monitor-1  Type......:      PING   State....:
   ENABLED
Standard parameters:
  Interval.........:            5 sec   Retries..........:
                    3
  Response timeout.:            2 sec   Down time.........:
      30 sec
  Reverse..........:              NO   Transparent.......:
                  YES
  Secure...........:              NO   LRTM..............:
      ENABLED
  Action...........:   Not applicable   Deviation.........:
      0 sec
  Destination IP...:      10.10.10.11
  Destination port.:    Bound service
  Iptunnel.........:              NO
  TOS..............:              NO   TOS ID............:
                    0
  SNMP Alert Retries:               0     Success Retries..:
                    1
  Failure Retries..:                0
<!--NeedCopy-->
```


So erstellen Sie einen transparenten Monitor mit dem Konfigurationsdienstprogramm

Navigieren Sie zu Traffic Management > Load Balancing > Monitore, und konfigurieren Sie einen transparenten Monitor.

So erstellen Sie einen transparenten Monitor mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu Traffic Management > Load Balancing > Monitore.
2. Klicken Sie im Bereich Monitore auf Hinzufügen.
3. Legen Sie im Dialogfeld Monitor erstellen die folgenden Parameter fest:
   - Namen*
   - Typ*
   - Ziel-IP
   - Folie

   * Ein erforderlicher Parameter
4. Klicken Sie auf Erstellenund dann auf Schließen.
5. Wählen Sie im Bereich Monitore den Monitor aus, den Sie gerade konfiguriert haben, und stellen Sie sicher, dass die im Detailbereich angezeigten Einstellungen korrekt sind.

So binden Sie einen Monitor mit dem Konfigurationsdienstprogramm an einen Dienst

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Wählen Sie auf der Registerkarte **Monitore** unter **Verfügbar** den Monitor aus, den Sie an den Dienst binden möchten, und klicken Sie dann auf **Hinzufügen** .

So binden Sie einen Monitor mit der Befehlszeilenschnittstelle an einen Dienst

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb monitor <monitorName> <serviceName>

show service <name>
<!--NeedCopy-->
```

Beispiel:


```
bind lb monitor monitor-HTTP-1 ISP1R_svc_any
 Done
> show service ISP1R_svc_any
        ISP1R_svc_any (10.10.10.254:*) - ANY
        State: UP
        Last state change was at Thu Sep  2 10:51:07 2010
        Time since last state change: 0 days, 18:41:55.130
        Server Name: 10.10.10.254
        Server ID : 0   Monitor Threshold : 0
        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits
        Use Source IP: NO
        Client Keepalive(CKA): NO
        Access Down Service: NO
        TCP Buffering(TCPB): YES
        HTTP Compression(CMP): NO
        Idle timeout: Client: 120 sec   Server: 120 sec
        Client IP: DISABLED
        Cacheable: NO
        SC: OFF
        SP: OFF
        Down state flush: ENABLED

1)      Monitor Name: monitor-HTTP-1
                State: UP  Weight: 1
                Probes: 1256       Failed [Total: 0 Current: 0]
                Last response: Success - ICMP echo reply received.
                Response Time: 1.322 millisec
 Done
<!--NeedCopy-->
```

So binden Sie einen Monitor mit dem Konfigurationsdienstprogramm an einen Dienst

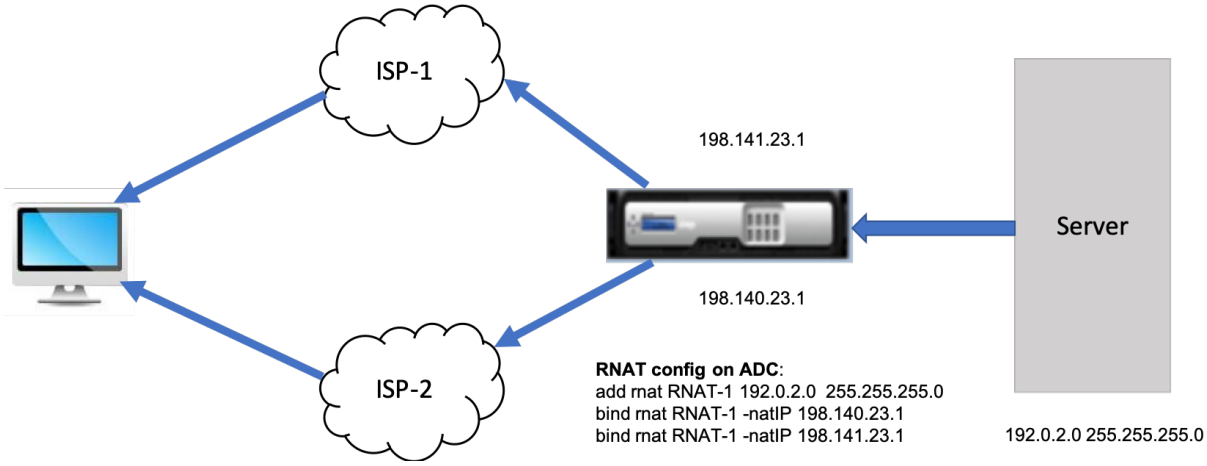
1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Wählen Sie im Detailbereich einen Dienst aus, an den Sie einen Monitor binden möchten, und klicken Sie dann auf Öffnen.
3. Wählen Sie im Dialogfeld Dienst konfigurieren auf der Registerkarte Monitore unter Verfügbar den Monitor aus, den Sie an den Dienst binden möchten, und klicken Sie dann auf Hinzufügen.
4. Klicken Sie auf OK.
5. Wählen Sie im Bereich Dienste den Dienst aus, den Sie gerade konfiguriert haben, und überprüfen Sie, ob die im Detailbereich angezeigten Einstellungen korrekt sind.

Konfigurieren Sie RNAT mit LLB

October 5, 2021

Sie können eine LLB-Setup für die Reverse Network Address Translation (RNAT) für ausgehenden Datenverkehr konfigurieren. Es stellt sicher, dass der Rückkehr-Netzwerkverkehr für einen bestimmten Flow über denselben Pfad geleitet wird. Konfigurieren Sie zuerst die grundlegende LLB, wie unter Konfigurieren eines grundlegenden LLB-Setupsbeschrieben, und konfigurieren Sie dann RNAT wie unter RNAT konfigurierenbeschrieben. Aktivieren Sie dann den Modus “Subnetz-IP (USNIP) verwenden”.

Im folgenden Diagramm verwendet die Citrix ADC Appliance LLB, um ausgehenden Datenverkehr an verschiedene Links weiterzuleiten. Während des RNAT-Vorgangs ersetzt die ADC-Appliance die Quell-IP-Adressen des ausgehenden Datenverkehrs durch die öffentliche NAT-IP-Adresse (198.141.23.1), um den Datenverkehr durch ISP-1 zu leiten. In ähnlicher Weise ersetzt die ADC-Appliance die Quell-IP-Adressen durch 198.140.23.1, um den Datenverkehr durch ISP-2 zu leiten.



So fügen Sie SNIPs für ISP-Router mit der CLI hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add NS IP <subnet of first ISP in the IP router> <subnet mask> -type
     SNIP
2
3 add NS IP <subnet of second ISP in the IP router> <subnet mask> -type
     SNIP
4 <!--NeedCopy-->
```

Beispiel:


```
add ns ip 198.140.23.1 255.255.255.0 -type snip

add ns ip 198.141.23.1 255.255.255.0 -type snip
<!--NeedCopy-->
```

So konfigurieren Sie RNAT mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add rnat <name> (<network> | (<aclname> [-redirectPort <port>]))

bind rnat <name> <natIP>@ …

show rnat <name>
<!--NeedCopy-->
```

Beispiel:

```
add rnat RNAT-1 192.0.2.0 255.255.255.0
bind rnat RNAT-1 -natIP 198.140.23.1
bind rnat RNAT-1 -natIP 198.141.23.1

> show rnat RNAT-1
    1) RNAT Name: RNAT-1     Network: 192.0.2.0      Netmask:
       255.255.255.0     Traffic Domain: 0
        UseProxyPort: ENABLED

        NatIP: 198.140.23.1
        NatIP: 198.141.23.1
<!--NeedCopy-->
```

So konfigurieren Sie RNAT mit der GUI

1. Navigieren Sie zu **System** > **Netzwerk** > **NATs** .
2. Klicken Sie auf der Registerkarte **RNAT** auf **RNAT konfigurieren** .
3. Geben Sie das Netzwerk an, in dem RNAT ausgeführt werden soll.

> **Hinweis:**
>
> Sie können RNAT auch mithilfe von Zugriffssteuerungslisten (Access Control Lists, ACLs) konfigurieren. Weitere Informationen finden Sie unter RNAT konfigurieren .

So aktivieren Sie den Subnetz-IP-Modus verwenden mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns mode USNIP

show ns mode
<!--NeedCopy-->
```

Beispiel:

```
enable ns mode USNIP

show ns mode
        Mode                            Acronym             Status
        -------                         -------             ------
 1)     Fast Ramp                       FR                  ON
 2)     ….
 8)     Use Subnet IP                   USNIP               ON
 9)     …
<!--NeedCopy-->
```

So aktivieren Sie den Subnetz-IP-Modus verwenden mit der GUI

1. Navigieren Sie zu **System** > **Einstellungen**, und klicken Sie unter **Modi und Features** auf **Modi konfigurieren** .
2. Wählen **Sie im Dialogfeld Modi konfigurieren** die Option **Subnetz-IP verwenden** aus, und klicken Sie dann auf **OK** .

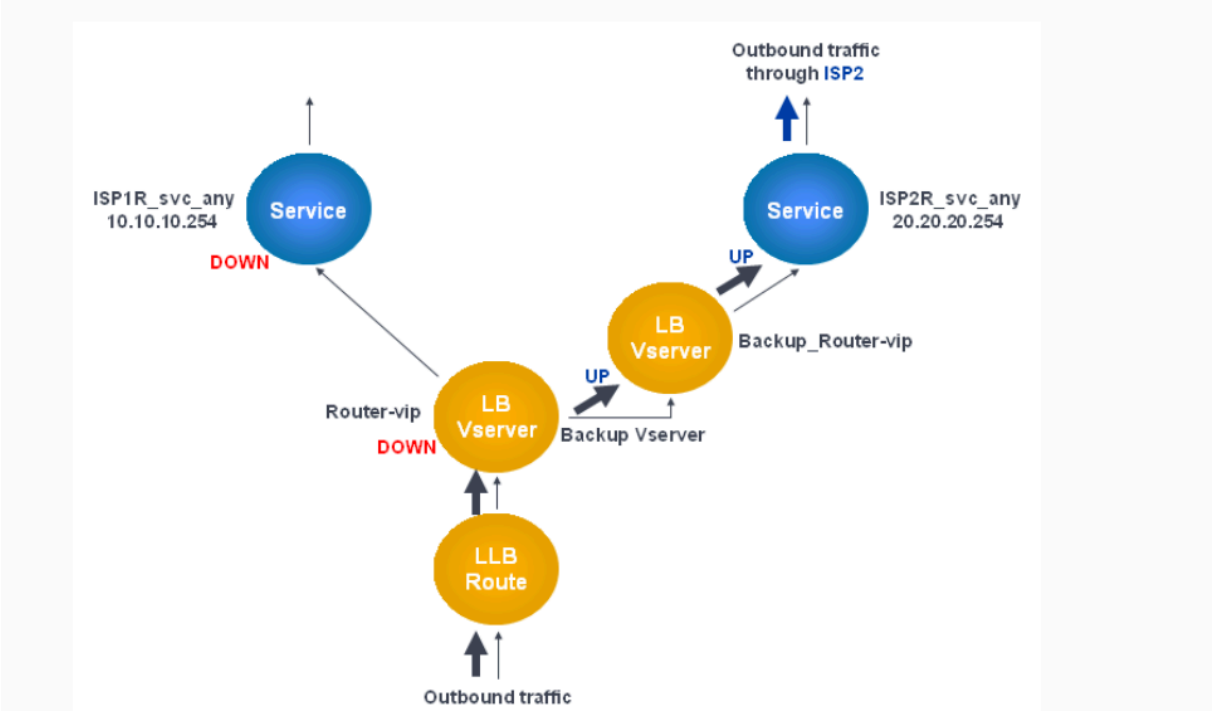
Konfigurieren einer Backup-Route

October 5, 2021

Um Unterbrechungen bei Diensten zu vermeiden, wenn die primäre Route ausgefallen ist, können Sie eine Backuproute konfigurieren. Nach der Konfiguration der Backuproute verwendet die Citrix ADC Appliance diese automatisch, wenn die primäre Route fehlschlägt. Erstellen Sie zunächst einen primären virtuellen Server, wie unter Konfigurieren eines virtuellen LLB-Servers und Binden eines Dienstesbeschrieben. Um eine Backuproute zu konfigurieren, erstellen Sie einen sekundären virtuellen Server, der einem primären virtuellen Server ähnlich ist, und weisen Sie diesen virtuellen Server als virtuellen Backupserver (Route) an.

Im folgenden Diagramm ist **Router-VIP** der primäre virtuelle Server, und **Backup_router-VIP** ist der sekundäre virtuelle Server, der als virtueller Backupserver bezeichnet wird.

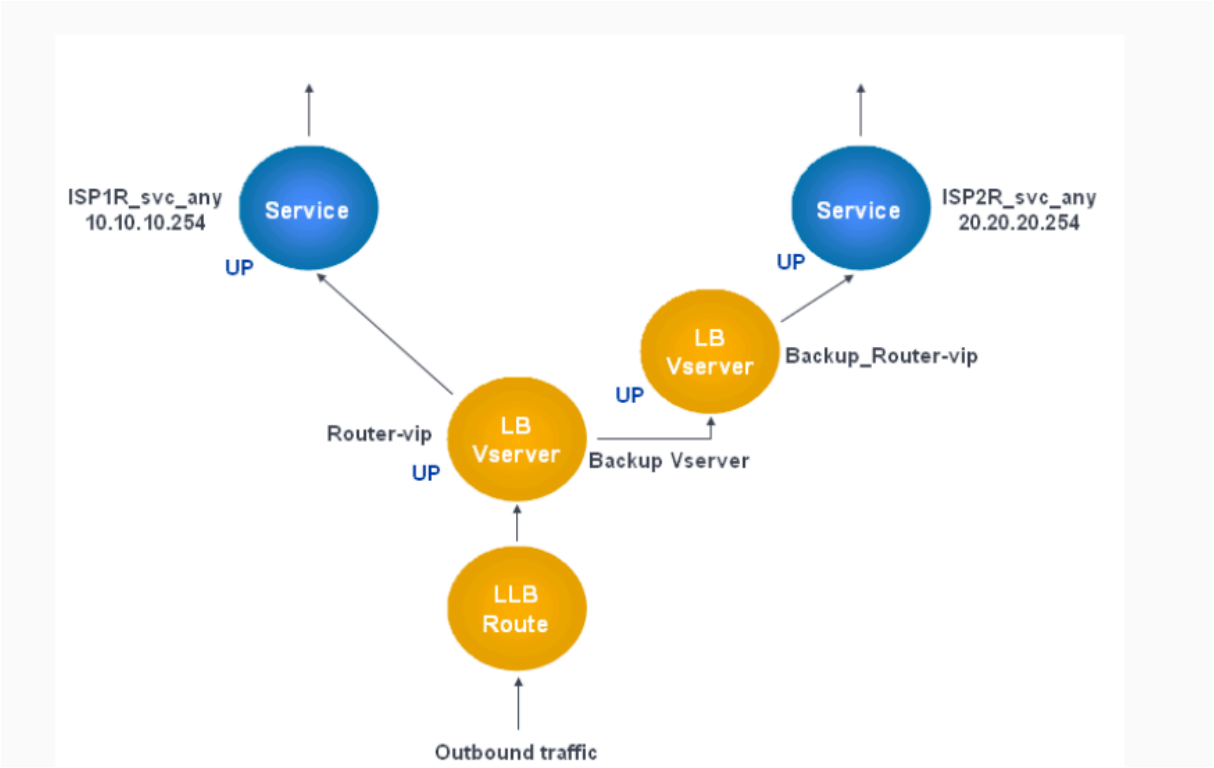
Abbildung 1. Backuproute einrichten



Hinweis: Wenn Ihr ISP eine IPv6-Adresse angegeben hat, ersetzen Sie den IPv4-Dienst durch einen IPv6-Dienst in der vorherigen Abbildung.

Standardmäßig wird der gesamte Datenverkehr über die primäre Route gesendet. Wenn jedoch die primäre Route fehlschlägt, wird der gesamte Datenverkehr auf die Backuproute umgeleitet, wie im folgenden Diagramm dargestellt.

Abbildung 2. Sichern des Routings im Betrieb



Hinweis: Wenn Ihr ISP eine IPv6-Adresse angegeben hat, ersetzen Sie den IPv4-Dienst durch einen IPv6-Dienst in der vorherigen Abbildung.

So legen Sie den sekundären virtuellen Server als virtuellen Backupserver mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -backupVserver <string>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Router-vip -backupVServer Backup_Router-vip
> show lb vserver Router-vip
        Router-vip (0.0.0.0:0) - ANY    Type: ADDRESS
        State: UP
        Last state change was at Fri Sep  3 04:46:48 2010
        Time since last state change: 0 days, 03:09:45.600
        Effective State: UP
        Client Idle Timeout: 120 sec
```



```
9          Down state flush: ENABLED
10         Disable Primary Vserver On Down : DISABLED
11         No. of Bound Services :  1 (Total)       1 (Active)
12         Configured Method: ROUNDROBIN
13         Mode: IP
14         Persistence: DESTIP     Persistence Mask: 255.255.255.255
                     Persistence v6MaskLength: 128   Persistence Timeout: 2
               min
15         Backup: Router2-vip
16         Connection Failover: DISABLED
17  Done
18 <!--NeedCopy-->
```

So legen Sie den sekundären virtuellen Server als virtuellen Backupserver mit dem Konfigurationsdienstprogramm fest

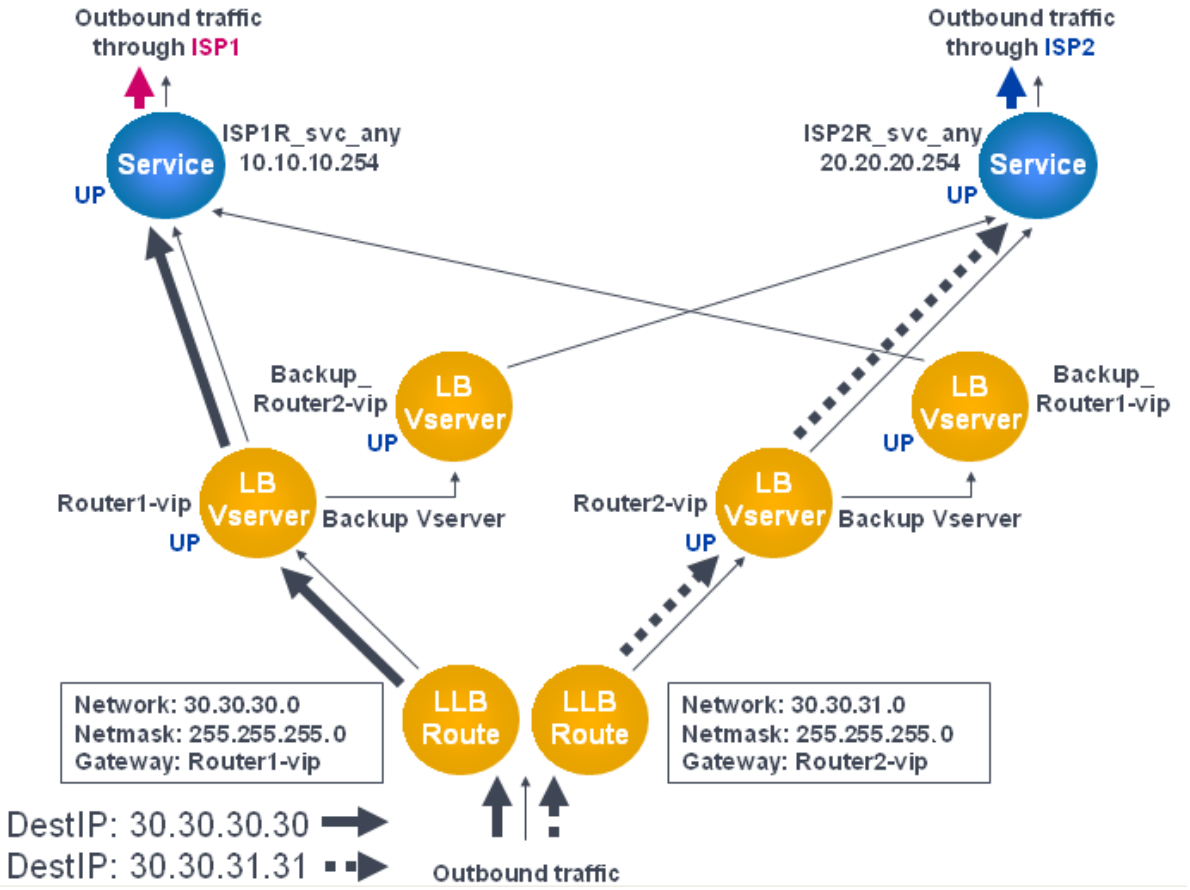
1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server** und wählen Sie den sekundären virtuellen Server aus, für den Sie den virtuellen Backup-Server konfigurieren möchten.
2. Wählen Sie im Dialogfeld **Load Balancing Virtual Server** unter **Erweitert** die Option **Schutz** aus.
3. Wählen Sie in der Dropdownliste **Virtueller Server** sichern den sekundären virtuellen Backupserver aus, und klicken Sie dann auf **OK** .

Resilientes LLB-Bereitstellungsszenario

October 5, 2021

Im folgenden Diagramm gibt es zwei Netzwerke: 30.30.30.0 und 30.30.31.0. Der Link-Lastausgleich wird basierend auf der Ziel-IP-Adresse konfiguriert. Zwei Routen sind mit Gateways **Router1-VIP** und **Router2-VIP** konfiguriert. **Router1-VIP** ist als Backup für **Router2-VIP** und umgekehrt konfiguriert. Der gesamte Datenverkehr mit der Ziel-IP, die als 30.30.30.30 angegeben ist, wird über **Router1-VIP** gesendet und der Datenverkehr mit der als 30.30.31.31 angegebenen Ziel-IP wird über **Router2-VIP** gesendet.

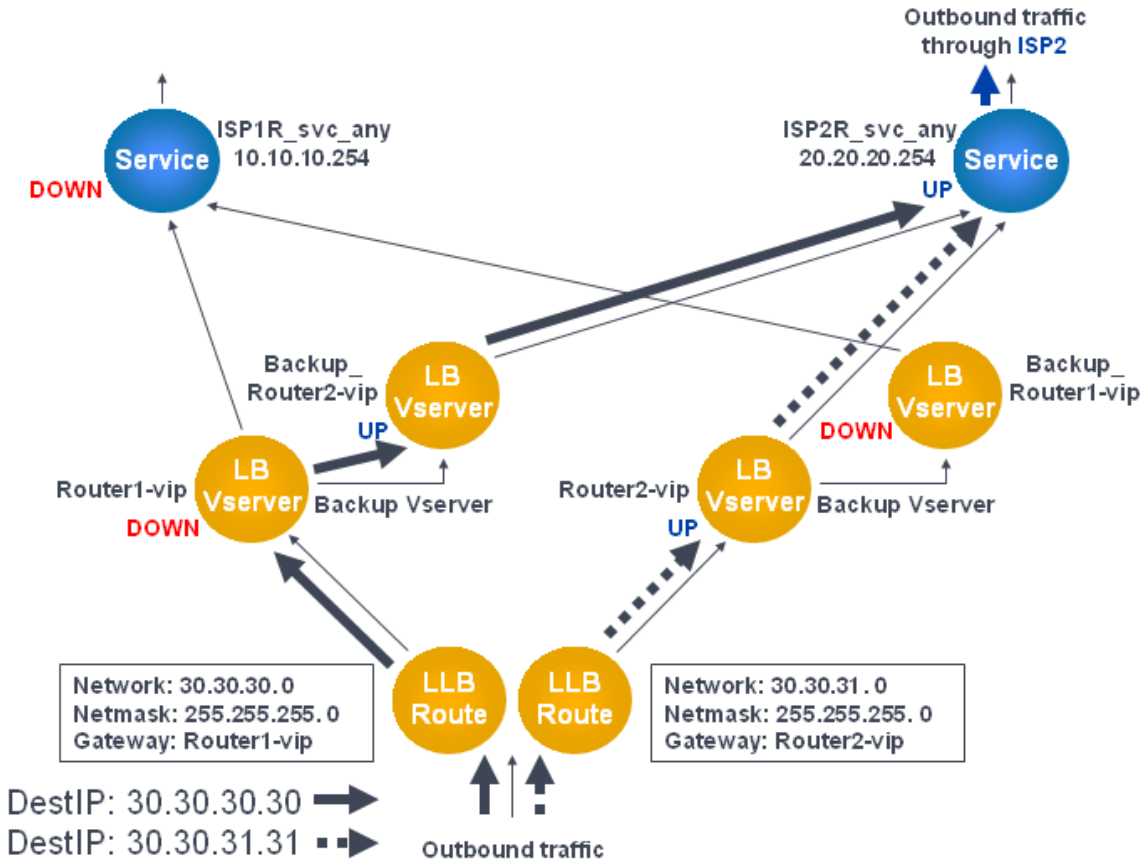
Abbildung 1. Resilient LLB-Bereitstellungs-Setup



Hinweis: Wenn Ihr ISP eine IPv6-Adresse angegeben hat, ersetzen Sie den IPv4-Dienst durch einen IPv6-Dienst in der vorherigen Abbildung.

Wenn jedoch eines der Gateways (**Router1-VIP** oder **Router2-VIP**) DOWN ist, wird der Datenverkehr über den Backup-Router weitergeleitet. Im folgenden Diagramm ist **Router1-VIP** für ISP1 DOWN, sodass der gesamte Datenverkehr mit der Ziel-IP, die als 30.30.30.30 angegeben ist, ebenfalls über ISP2 gesendet wird.

Abbildung 2. Resilient LLB-Bereitstellungsszenario



Hinweis: Wenn Ihr ISP eine IPv6-Adresse angegeben hat, ersetzen Sie den IPv4-Dienst durch einen IPv6-Dienst in der vorherigen Abbildung.

Überwachen eines LLB-Setups

October 5, 2021

Nachdem die Konfiguration läuft, können Sie die Statistiken für jeden Dienst und virtuellen Server anzeigen, um nach möglichen Problemen zu suchen.

Die Statistiken eines virtuellen Servers anzeigen

Um die Leistung virtueller Server zu bewerten oder Probleme zu beheben, können Sie Details der virtuellen Server anzeigen, die auf der Citrix ADC Appliance konfiguriert sind. Sie können eine Zusammenfassung der Statistiken für alle virtuellen Server anzeigen. Sie können auch den Namen eines virtuellen Servers angeben, um die Statistiken nur für diesen virtuellen Server anzuzeigen. Sie können die folgenden Details anzeigen:

- Name
- IP-Adresse
- Port
- Protokoll
- Status des virtuellen Servers
- Rate der empfangenen Anfragen
- Rate of hits

Anzeigen von Statistiken virtueller Server mit der CLI

Um eine Zusammenfassung der Statistiken für alle virtuellen Server anzuzeigen, die derzeit auf dem Citrix ADC konfiguriert sind, oder für einen einzelnen virtuellen Server, geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat lb vserver -detail] [<name>]
<!--NeedCopy-->
```

Beispiel:

```
stat lb vserver -detail
Virtual Server(s) Summary
                        vsvrIP  port     Protocol        State    Req/s
                             Hits/s
One                          *    80         HTTP           UP      5/s
        0/s
Two                          *     0          TCP         DOWN      0/s
        0/s
Three                        *  2598          TCP         DOWN      0/s
        0/s
dnsVirtualNS    10.102.29.90    53          DNS         DOWN      0/s
        0/s
BRVSERV            10.10.1.1    80         HTTP         DOWN      0/s
        0/s
LBVIP           10.102.29.66    80         HTTP           UP      0/s
        0/s
 Done
<!--NeedCopy-->
```


Anzeigen von Statistiken virtueller Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server > Statistiken**.
2. Wenn Sie die Statistiken nur für einen virtuellen Server anzeigen möchten, wählen Sie im Detailbereich den virtuellen Server aus und klicken Sie auf Statistiken.

Die Statistiken eines Dienstes anzeigen

Sie können die Rate der Anfragen, Antworten, Anforderungsbytes, Antwortbytes, aktuelle Clientverbindungen, Anfragen in der Überspannungswarteschlange, aktuelle Serververbindungen usw. mithilfe der Dienststatistiken anzeigen.

Zeigen Sie die Statistiken eines Dienstes mit der CLI an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat service <name>
<!--NeedCopy-->
```

Beispiel:

```
stat service Service-HTTP-1
<!--NeedCopy-->
```

Zeigen Sie die Statistiken eines Dienstes über die GUI an

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services > Statistiken**.
2. Wenn Sie die Statistiken für nur einen Dienst anzeigen möchten, wählen Sie den Dienst aus und klicken Sie auf Statistiken.

Lastausgleich

October 5, 2021

Die Lastenausgleichsfunktion verteilt Benutzeranfragen für Webseiten und andere geschützte Anwendungen auf mehrere Server, die alle denselben Inhalt hosten (oder spiegeln). Sie verwenden den Lastenausgleich in erster Linie, um Benutzeranforderungen an stark genutzte Anwendungen zu verwalten, schlechte Leistung und Ausfälle zu vermeiden und sicherzustellen, dass Benutzer auf Ihre

geschützten Anwendungen zugreifen können. Der Lastenausgleich bietet auch Fehlertoleranz. Wenn ein Server, der eine geschützte Anwendung hostet, nicht verfügbar wird, verteilt die Funktion Benutzeranfragen an die anderen Server, die dieselbe Anwendung hosten.

Sie können die Lastenausgleichsfunktion konfigurieren:

- Verteilen Sie alle Anforderungen für eine bestimmte geschützte Website, Anwendung oder Ressource zwischen zwei oder mehr identisch konfigurierten Servern.
- Verwenden Sie einen der verschiedenen Algorithmen, um zu ermitteln, welcher Server jede eingehende Benutzeranforderung empfangen muss, wobei die Entscheidung auf verschiedene Faktoren beruht, z. B. welcher Server über die wenigsten aktuellen Benutzerverbindungen verfügt oder welcher Server die geringste Last hat.

Die Lastausgleichsfunktion ist ein Kernmerkmal der Citrix ADC Appliance. Die meisten Benutzer richten zunächst eine funktionierende Grundkonfiguration ein und passen dann verschiedene Einstellungen an, einschließlich Persistenz für Verbindungen. Darüber hinaus können Sie Funktionen konfigurieren, um die Konfiguration vor Fehlern zu schützen, Clientdatenverkehr zu verwalten, Server zu verwalten und zu überwachen und eine umfangreiche Bereitstellung zu verwalten.

Funktionsweise des Lastenausgleichs

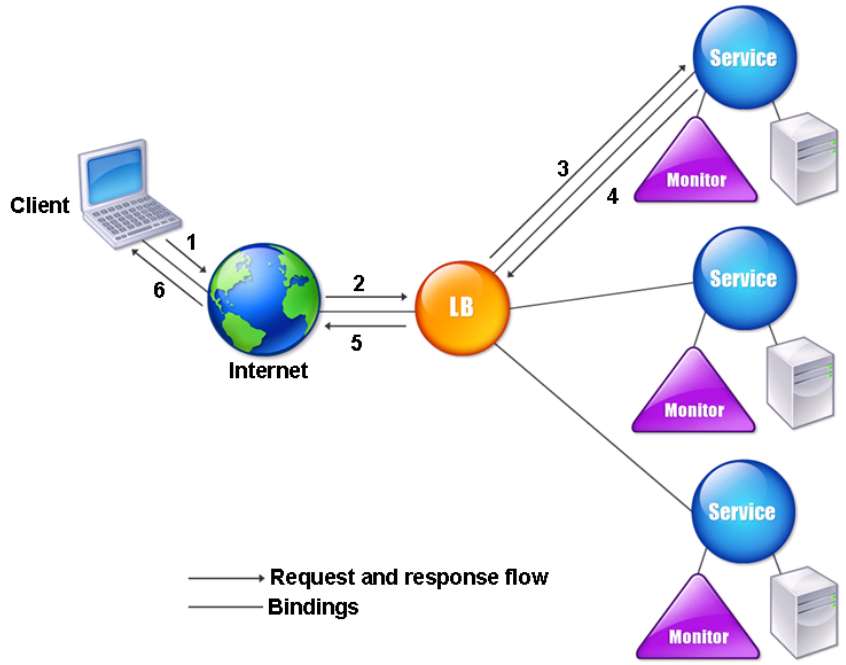
October 5, 2021

In einem einfachen Lastausgleichs-Setup senden Clients ihre Anforderungen an die IP-Adresse eines virtuellen Servers, der auf der Citrix ADC Appliance konfiguriert ist. Der virtuelle Server verteilt sie an die Anwendungsserver mit Lastenausgleich nach einem voreingestellten Muster, dem sogenannten Lastausgleichsalgorithmus. Manchmal möchten Sie dem virtuellen Lastenausgleichsserver möglicherweise eine Platzhalteradresse anstelle einer bestimmten IP-Adresse zuweisen. Anweisungen zum Angeben eines globalen HTTP-Ports auf der Appliance finden Sie unter **Globale HTTP-Ports**.

Grundlagen des Lastenausgleichs

Ein Lastausgleichs-Setup umfasst einen virtuellen Lastenausgleichsserver und mehrere Anwendungsserver mit Lastenausgleich. Der virtuelle Server empfängt eingehende Clientanforderungen, verwendet den Lastausgleichsalgorithmus, um einen Anwendungsserver auszuwählen, und leitet die Anforderungen an den ausgewählten Anwendungsserver weiter. Die folgende konzeptionelle Zeichnung veranschaulicht eine typische Lastausgleichsbereitstellung. Eine andere Variante beinhaltet die Zuweisung eines globalen HTTP-Ports.

Abbildung 1. Lastenausgleich-Architektur



Der virtuelle Lastausgleichsserver kann mehrere Algorithmen (oder Methoden) verwenden, um zu bestimmen, wie die Last auf die von ihm verwaltlichen Lastausgleichsserver verteilt werden kann. Die Standardmethode für den Lastenausgleich ist die geringste Verbindungsmethode, bei der die Citrix ADC Appliance jede eingehende Clientverbindung an den Anwendungsserver mit Lastenausgleich weiterleitet, der derzeit die wenigsten aktiven Benutzerverbindungen aufweist.

Die Entitäten, die Sie in einem typischen Citrix ADC Lastausgleichs-Setup konfigurieren, sind:

- **Lastenausgleich virtueller Server.** Die Kombination von IP-Adresse, Port und Protokoll, an die ein Client Verbindungsanforderungen für eine bestimmte Website oder Anwendung mit Lastenausgleich sendet. Wenn die Anwendung über das Internet zugänglich ist, ist die IP-Adresse des virtuellen Servers (VIP) eine öffentliche IP-Adresse. Wenn die Anwendung nur vom LAN oder WAN aus zugänglich ist, ist der VIP normalerweise eine private (nicht routfähige ICANN-IP-Adresse).
- **Service.** Die Kombination von IP-Adresse, Port und Protokoll, die verwendet wird, um Anforderungen an einen bestimmten Anwendungsserver mit Lastenausgleich weiterzuleiten. Ein Dienst kann eine logische Darstellung des Anwendungsservers selbst oder einer Anwendung sein, die auf einem Server ausgeführt wird, der mehrere Anwendungen hostet. Nachdem Sie einen Dienst erstellt haben, binden Sie ihn an einen virtuellen Lastausgleichsserver.
- **Server-Objekt.** Eine virtuelle Entität, mit der Sie einem physischen Server einen Namen

zuweisen können, anstatt den Server anhand seiner IP-Adresse zu identifizieren. Wenn Sie ein Serverobjekt erstellen, können Sie beim Erstellen eines Dienstes seinen Namen anstelle der IP-Adresse des Servers angeben. Andernfalls müssen Sie die IP-Adresse des Servers angeben, wenn Sie einen Dienst erstellen, und die IP-Adresse wird zum Namen des Servers.

- **Überwachen.** Eine Entität auf der Citrix ADC Appliance, die einen Dienst verfolgt und sicherstellt, dass er ordnungsgemäß funktioniert. Der Monitor prüft regelmäßig jeden Dienst, dem Sie ihn zuweisen, oder führt eine Zustandsprüfung durch. Wenn der Dienst nicht innerhalb der durch das Timeout angegebenen Zeit reagiert und eine bestimmte Anzahl von Integritätsprüfungen fehlschlägt, wird dieser Dienst mit DOWN gekennzeichnet. Die Citrix ADC Appliance überspringt diesen Dienst beim Lastenausgleich, bis die Probleme behoben wurden, durch die der Dienst beendet wurde.

Die virtuellen Server, Dienste und Lastausgleichsserver in einem Lastausgleichs-Setup können entweder IPv4 (Internet Protocol Version 4) oder IPv6 (Internet Protocol Version 6) IP-Adressen verwenden. Sie können IPv4- und IPv6-Adressen in einem einzelnen Lastausgleichs-Setup mischen.

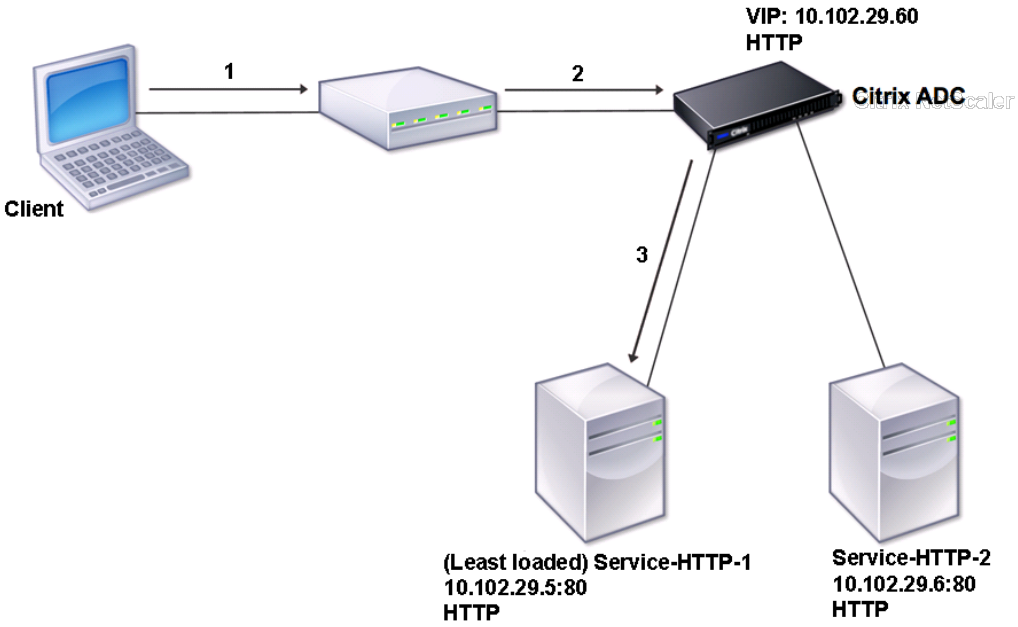
Variationen im Lastausgleichs-Setup finden Sie in den folgenden Anwendungsfällen:

- Konfigurieren des Lastenausgleichs im Direct Server-Rückgabemodus
- Konfigurieren von LINUX-Servern im DSR-Modus
- Konfigurieren des DSR-Modus bei Verwendung von TOS
- Konfigurieren des Lastenausgleichs im DSR-Modus mithilfe von IP over IP
- Konfigurieren des Lastenausgleichs im Einarmmodus
- Konfigurieren des Lastenausgleichs im Inline-Modus
- Lastenausgleich von Intrusion Detection Systemservern
- Load Balance-Remotedesktopprotokollserver

Grundlegendes zur Topologie

In einem Lastausgleichs-Setup befindet sich der Lastausgleichsserver logisch zwischen dem Client und der Serverfarm und verwaltet den Datenverkehr zu den Servern in der Serverfarm. Auf der Citrix ADC Appliance werden die Anwendungsserver durch virtuelle Entitäten dargestellt, die Dienste genannt werden. Das folgende Diagramm zeigt die Topologie einer grundlegenden Lastausgleichskonfiguration.

Abbildung 2. Grundlegende Load Balancing-Topologie



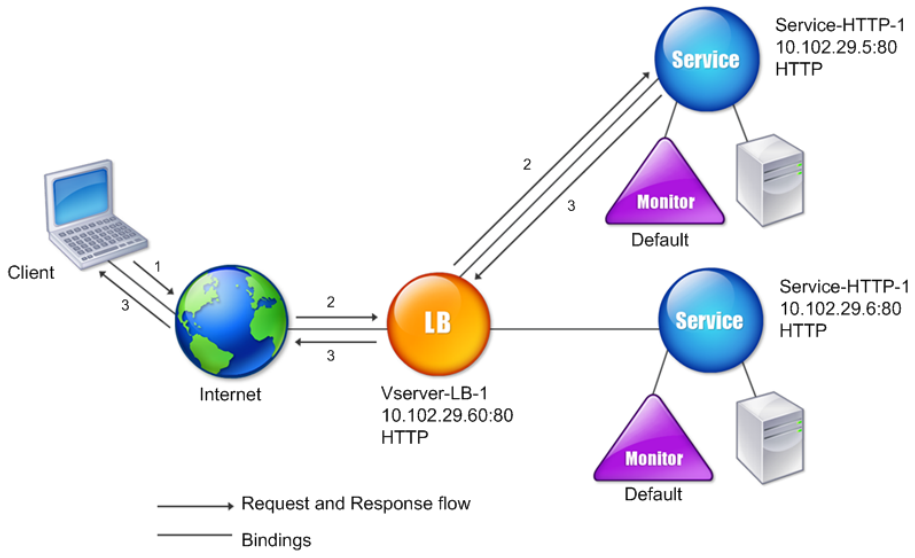
Im Diagramm wird der Lastenausgleich verwendet, um den Datenfluss zu den Servern zu verwalten. Der virtuelle Server wählt den Dienst aus und weist ihn zu, um Clientanforderungen zu erfüllen. Stellen Sie sich ein Szenario vor, in dem die Dienste Service-HTTP-1 und Service-HTTP-2 erstellt und an den virtuellen Server mit dem Namen vServer-LB-1 gebunden werden. VServer-LB-1 leitet die Clientanforderung entweder an Service-HTTP-1 oder Service-HTTP-2 weiter. Die Citrix ADC Appliance verwendet die Methode des Lastenausgleichs für die geringste Verbindung, um den Dienst für jede Anforderung auszuwählen. In der folgenden Tabelle sind die Namen und Werte der Basiseinheiten aufgeführt, die auf der Appliance konfiguriert werden müssen.

Entität	Name	IP-Adresse	Port	Protokoll
Virtueller Server	Vserver-LB-1	10.102.29.60	80	HTTP
Services	Service-HTTP-1	10.102.29.5	80	HTTP
	Service-HTTP-2	10.102.29.6	80	HTTP
Monitore	Standard	Ohne	Ohne	Ohne

Das folgende Diagramm zeigt die Lastausgleichsprobenwerte und die obligatorischen Parameter, die

in der vorhergehenden Tabelle beschrieben werden.

Abbildung 3. Load Balancing Entity Modell



Verwendung von Platzhaltern anstelle von IP-Adressen und Ports

Manchmal müssen Sie möglicherweise einen Platzhalter für die IP-Adresse oder den Port eines virtuellen Servers oder für den Port eines Dienstes verwenden. Die folgenden Fälle erfordern möglicherweise die Verwendung eines Platzhalters:

- Wenn die Citrix ADC Appliance als transparenter Durchgang konfiguriert ist, muss der gesamte Datenverkehr akzeptiert werden, der an sie gesendet wird, unabhängig von der IP oder dem Port, an den sie gesendet wird.
- Wenn ein oder mehrere Dienste auf Ports hören, die nicht bekannt sind.
- Ändern Sie bei einem oder mehreren Diensten im Laufe der Zeit die Ports, auf die sie hören.
- Wenn Sie das Limit für die Anzahl der IP-Adressen und Ports erreichen, die Sie auf einer einzelnen Citrix ADC Appliance konfigurieren können.
- Wenn Sie virtuelle Server erstellen möchten, die den gesamten Datenverkehr in einem bestimmten virtuellen LAN überwachen.

Wenn ein mit Platzhalter konfigurierter virtueller Server oder Dienst Datenverkehr empfängt, ermittelt

die Citrix ADC Appliance die tatsächliche IP-Adresse oder den tatsächlichen Port und erstellt Datensätze für den Dienst und den zugehörigen Lastausgleichsanwendungsserver. Diese dynamisch erstellten Datensätze werden als dynamisch erlernte Server- und Dienstdatensätze bezeichnet.

Beispielsweise kann eine Firewall-Lastausgleichskonfiguration Platzhalter für die IP-Adresse und den Port verwenden. Wenn Sie einen Platzhalter-TCP-Service an diesen Typ eines virtuellen Lastausgleichsservers binden, empfängt und verarbeitet der virtuelle Server den gesamten TCP-Datenverkehr, der keinem anderen Dienst oder virtuellen Server entspricht.

In der folgenden Tabelle werden einige der verschiedenen Arten von Platzhalterkonfigurationen beschrieben und wann sie verwendet werden müssen.

IP	Port	Protokoll	Beschreibung
*	*	TCP	Ein allgemeiner virtueller Wildcard-Server, der Datenverkehr akzeptiert, der an eine beliebige IP-Adresse und Port der Citrix ADC Appliance gesendet wird. Bei Verwendung eines virtuellen Platzhalterservers lernt die Appliance dynamisch die IP und den Port jedes Dienstes und erstellt die erforderlichen Datensätze, während sie den Datenverkehr verarbeitet.

IP	Port	Protokoll	Beschreibung
*	*	TCP	Ein virtueller Server für den Lastenausgleich der Firewall. Sie können Firewalldienste an diesen virtuellen Server binden, und die Citrix ADC Appliance leitet den Datenverkehr durch die Firewall an das Ziel weiter.
IP-Adresse	*	TCP, UDP und ANY	Ein virtueller Server, der den gesamten Datenverkehr akzeptiert, der an die angegebene IP-Adresse gesendet wird, unabhängig vom Port. Sie müssen explizit an diesen virtuellen Server die Dienste binden, zu denen der Datenverkehr umgeleitet wird. Es lernt sie nicht dynamisch.

IP	Port	Protokoll	Beschreibung
			Hinweis: Sie konfigurieren keine Dienste oder virtuelle Server für einen globalen HTTP-Port. In diesem Fall konfigurieren Sie einen bestimmten Port als globaler HTTP-Port (z. B. ns-param -httpPort 80). Die Appliance akzeptiert dann den gesamten Datenverkehr, der der Portnummer entspricht, und verarbeitet ihn als HTTP-Datenverkehr. Die Appliance lernt dynamisch und erstellt Dienste für diesen Datenverkehr.

IP	Port	Protokoll	Beschreibung
*	Port	SSL, SSL_TCP	Ein virtueller Server, der den gesamten Datenverkehr akzeptiert, der an eine beliebige IP-Adresse an einem bestimmten Port gesendet wird. Wird für globale transparente SSL-Abladung verwendet. Die gesamte SSL-, HTTP- und TCP-Verarbeitung, die normalerweise für einen Dienst desselben Protokolltyps ausgeführt wird, wird auf den Datenverkehr angewendet, der an diesen bestimmten Port gerichtet ist. Die Appliance verwendet den Port, um dynamisch die IP des Dienstes zu erlernen, den sie verwenden muss. Wenn —cleartext nicht angegeben ist, verwendet die Citrix ADC Appliance End-to-End-SSL.

IP	Port	Protokoll	Beschreibung
*	Port	Nicht zutreffend	Alle anderen virtuellen Server, die Datenverkehr zum Port akzeptieren können. Sie binden Dienste nicht an diese virtuellen Server. Die Citrix ADC Appliance lernt sie dynamisch.

Hinweis: Wenn Sie Ihre Citrix ADC Appliance als transparenten Durchgang konfiguriert haben, der globale (Platzhalter-) Ports verwendet, möchten Sie möglicherweise den Edge-Modus aktivieren. Weitere Informationen finden Sie unter "Edge-Modus konfigurieren. "

Die Citrix ADC Appliance versucht, virtuelle Server und Dienste zu finden, indem sie zunächst eine exakte Übereinstimmung versucht. Wenn keine gefunden wird, sucht sie weiterhin nach einer Übereinstimmung, die auf Platzhaltern basiert, in der folgenden Reihenfolge:

1. Spezifische IP-Adresse und spezifische Portnummer
2. Spezifische IP-Adresse und ein * (Platzhalter) Port
3. • (Platzhalter-) IP-Adresse und einen bestimmten Port
4. • (Platzhalter-) IP-Adresse und ein * (Platzhalter) Port

Wenn die Appliance einen virtuellen Server nicht nach IP-Adresse oder Portnummer auswählen kann, sucht sie in der folgenden Reihenfolge nach einem virtuellen Server, der auf dem in der Anforderung verwendeten Protokoll basiert:

1. HTTP
2. TCP
3. ANY

Konfigurieren globaler HTTP-Ports

Sie konfigurieren keine Dienste oder virtuelle Server für einen globalen HTTP-Port. Stattdessen konfigurieren Sie einen bestimmten Port mithilfe des Befehls set ns param. Nach der Konfiguration dieses Ports akzeptiert die Citrix ADC Appliance den gesamten Datenverkehr, der der Portnummer entspricht, und verarbeitet ihn als HTTP-Datenverkehr, wobei Dienste für diesen Datenverkehr dynamisch erlernen und erstellt werden.

Sie können mehr als eine Portnummer als globaler HTTP-Port konfigurieren. Wenn Sie mehr als eine Portnummer in einem einzelnen Satz ns param Befehl angeben, trennen Sie die Portnummern durch einen einzelnen Leerraum. Wenn ein oder mehrere Ports bereits als globale HTTP-Ports angegeben wurden und Sie einen oder mehrere Ports hinzufügen möchten, ohne die derzeit konfigurierten Ports zu entfernen, müssen Sie im Befehl alle Portnummern (aktuell und neu) angeben. Bevor Sie Portnummern hinzufügen, verwenden Sie den Befehl show ns param, um die derzeit konfigurierten Ports anzuzeigen.

So konfigurieren Sie einen globalen HTTP-Port mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen globalen HTTP-Port zu konfigurieren und die Konfiguration zu überprüfen:

```
set ns param  - httpPort <port>

show ns param
<!--NeedCopy-->
```

Beispiel 1: Konfigurieren eines Ports als globalen HTTP-Port

In diesem Beispiel wird Port 80 als globaler HTTP-Port konfiguriert.

```
set ns param -httpPort 80
Done
show ns param
         Global configuration settings:
                            HTTP port(s): 80
                        Max connections: 0
           Max requests per connection: 0
                   Client IP insertion: DISABLED
                        Cookie version: 0
         Persistence Cookie Secure Flag: ENABLED
         ...
         ...
<!--NeedCopy-->
```

Beispiel 2: Hinzufügen von Ports, wenn ein oder mehrere globale HTTP-Ports bereits konfiguriertsind**

In diesem Beispiel wird Port 8888 zur globalen HTTP-Portliste hinzugefügt. Port 80 ist bereits als globaler HTTP-Port konfiguriert.

```
> show ns param
        Global configuration settings:
                            HTTP port(s): 80
                        Max connections: 0
           Max requests per connection: 0
                    Client IP insertion: DISABLED
                         Cookie version: 0
        Persistence Cookie Secure Flag: ENABLED
                            Min Path MTU: 576
        ...
        ...
 Done
> set ns param -httpPort 80 8888
 Done
>  show ns param

        Global configuration settings:
                            HTTP port(s): 80,8888
                        Max connections: 0
           Max requests per connection: 0
                    Client IP insertion: DISABLED
                         Cookie version: 0
        Persistence Cookie Secure Flag: ENABLED
                            Min Path MTU: 576

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

So konfigurieren Sie einen globalen HTTP-Port mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **System > Einstellungen > HTTP-Parameter ändern**, und fügen Sie dann eine HTTP-Portnummer hinzu.

Einrichten des grundlegenden Lastenausgleichs

October 5, 2021

Aktivieren Sie vor der Konfiguration des ersten Lastausgleichs die Funktion für den Lastausgleich. Erstellen Sie dann mindestens einen Dienst für jeden Server in der Lastausgleichsgruppe. Wenn die Dienste konfiguriert sind, können Sie einen virtuellen Lastausgleichsserver erstellen und jeden Dienst an den virtuellen Server binden. Damit ist die erste Einrichtung abgeschlossen. Bevor Sie mit der weiteren Konfiguration fortfahren, überprüfen Sie Ihre Konfiguration, um sicherzustellen, dass jedes Element ordnungsgemäß konfiguriert wurde und wie erwartet funktioniert.

Lastenausgleich aktivieren

Sie können Lastausgleichs-Entitäten wie Dienste und virtuelle Server konfigurieren, wenn die Lastenausgleichsfunktion deaktiviert ist, aber sie funktionieren erst, wenn Sie das Feature aktivieren.

So aktivieren Sie den Lastenausgleich mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um den Lastausgleich zu aktivieren und die Konfiguration zu überprüfen:

- enable ns feature LB
- show ns feature

Beispiel

```
> enable ns feature LoadBalancing

 Done

> show ns feature


        Feature                         Acronym             Status

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

 1)     Web Logging                     WL                  OFF

 2)     Surge Protection                SP                  ON

```



```
      3) Load Balancing LB ON

      .

      .

      .

      24)    NetScaler Push                push                OFF

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

So aktivieren Sie den Lastausgleich mit der GUI

Navigieren Sie zu **System** > **Einstellungen** und wählen Sie unter **Basisfunktionen konfigurieren**die Option **Load Balancing**aus.

Konfigurieren eines Serverobjekts

Erstellen Sie einen Eintrag für Ihren Server auf der Citrix ADC Appliance. Die Citrix ADC Appliance unterstützt IP-Adressserver und domänenbasierte Server. Wenn Sie einen IP-adressbasierten Server erstellen, können Sie beim Erstellen eines Dienstes den Namen des Servers anstelle seiner IP-Adresse angeben. Informationen zum Einrichten von DNS für einen domänenbasierten Server finden Sie unter Domänennamensystem.

So erstellen Sie ein Serverobjekt mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add server `<name>`@ `<IPAddress>`@ | `<domain>`
<!--NeedCopy-->
```

Beispiel für das Hinzufügen eines IP-Adressen-basierten Nameservers:

```
add server web_serv 10.102.27.150
<!--NeedCopy-->
```

Beispiel für das Hinzufügen eines domänenbasierten Servers:


```
add server web_serv test.com
<!--NeedCopy-->
```

So erstellen Sie ein Serverobjekt mit der GUI

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Server**, und fügen Sie ein Serverobjekt hinzu.

Konfigurieren von Diensten

Nachdem Sie die Lastenausgleichsfunktion aktiviert haben, müssen Sie mindestens einen Dienst für jeden Anwendungsserver erstellen, der in das Lastausgleichs-Setup aufgenommen werden soll. Die von Ihnen konfigurierten Dienste stellen die Verbindungen zwischen der Citrix ADC Appliance und den Servern mit Lastausgleich bereit. Jeder Dienst hat einen Namen und gibt eine IP-Adresse, einen Port und den Typ der bereitgestellten Daten an.

Wenn Sie einen Dienst erstellen, ohne vorher ein Serverobjekt zu erstellen, ist die IP-Adresse des Dienstes auch der Name des Servers, der den Dienst hostet. Wenn Sie Server lieber nach Namen und nicht nach IP-Adresse identifizieren möchten, können Sie Serverobjekte erstellen und dann beim Erstellen eines Dienstes anstelle der IP-Adresse einen Servernamen angeben.

Wenn Sie einen Dienst erstellen, der UDP als Transportschichtprotokoll verwendet, wird ein Ping-Monitor automatisch an den Dienst gebunden. Ein Ping-Monitor ist der grundlegendste der eingebauten Monitore. Wenn Sie einen Dienst erstellen, der TCP als Transportschichtprotokoll verwendet, wird ein TCP_Default-Monitor automatisch an den Dienst gebunden. Wenn Sie eine Strategie für die Verwaltung des Lastausgleichs entwickeln, können Sie einen anderen Monitortyp oder mehrere Monitore an den Dienst binden.

Erstellen eines Dienstes

Bevor Sie einen Dienst erstellen, müssen Sie die verschiedenen Diensttypen und die Verwendung dieser Dienste verstehen. In der folgenden Liste werden die von der Citrix ADC Appliance unterstützten Diensttypen beschrieben.

HTTP

Wird für Server mit Lastenausgleich verwendet, die HTTP-Datenverkehr akzeptieren, z. B. Standardwebsites und Webanwendungen. Der HTTP-Diensttyp ermöglicht es der Citrix ADC Appliance, Komprimierung, Inhaltsfilterung, Zwischenspeicherung und Client-Keepalive-Unterstützung für Ihre Layer

7-Webserver bereitzustellen. Dieser Diensttyp unterstützt auch das Einfügen von IP-Ports virtueller Server, das Umleitungsport, das Web 2.0-Push und die URL-Umleitungsunterstützung.

Da HTTP ein TCP-basiertes Anwendungsprotokoll ist, können Sie auch den TCP-Diensttyp für Webserver verwenden. In diesem Fall kann die Citrix ADC Appliance jedoch nur den Layer 4-Lastenausgleich durchführen. Es kann keine der zuvor beschriebenen Layer 7-Unterstützungen bereitstellen.

SSL

Wird für Server verwendet, die HTTPS-Datenverkehr akzeptieren, wie E-Commerce-Websites und Warenkorb-Anwendungen. Der SSL-Diensttyp ermöglicht es der Citrix ADC Appliance, SSL-Datenverkehr zu verschlüsseln und zu entschlüsseln (SSL-Abladung durchführen) für Ihre sicheren Webanwendungen. Es unterstützt auch HTTP-Persistenz, Content Switching, Umschreiben, Einfügen von IP-Ports virtueller Server, Web 2.0 Push und URL-Umleitung.

Sie können auch die Diensttypen SSL_BRIDGE, SSL_TCP oder TCP verwenden. In diesem Fall führt die Appliance jedoch nur Layer 4 Lastenausgleich aus. Es kann keine SSL-Abladung oder eine der beschriebenen Layer-7-Unterstützungen bereitstellen.

FTP

Wird für Server verwendet, die FTP-Datenverkehr akzeptieren. Der FTP-Diensttyp ermöglicht es der Citrix ADC Appliance, bestimmte Details des FTP-Protokolls zu unterstützen.

Sie können auch TCP- oder ANY-Servicetypen für FTP-Server verwenden.

TCP

Wird für Server verwendet, die viele verschiedene Arten von TCP-Datenverkehr akzeptieren oder einen Typ von TCP-Datenverkehr akzeptieren, für den ein spezifischerer Diensttyp nicht verfügbar ist.

Sie können auch den Diensttyp ANY für diese Server verwenden.

SSL_TCP

Wird für Server verwendet, die nicht-HTTP-basierten SSL-Datenverkehr akzeptieren, um SSL-Abladung zu unterstützen.

Sie können auch den TCP-Diensttyp für diese Dienste verwenden. In diesem Fall führt die Citrix ADC Appliance sowohl den Layer 4-Lastausgleich als auch die SSL-Abladung durch.

UDP

Wird für Server verwendet, die UDP-Datenverkehr akzeptieren. Sie können auch den Diensttyp ANY verwenden.

SSL_BRIDGE

Wird für Server verwendet, die SSL-Datenverkehr akzeptieren, wenn die Citrix ADC Appliance keine SSL-Abladung durchführen soll. Alternativ können Sie den Diensttyp SSL_TCP verwenden.

NNTP

Wird für Server verwendet, die NNTP-Datenverkehr (Network News Transfer Protocol) akzeptieren, in der Regel Usenet-Websites.

DNS

Wird für Server verwendet, die DNS-Datenverkehr akzeptieren, typischerweise Nameserver. Mit dem DNS-Diensttyp überprüft die Citrix ADC Appliance das Paketformat jeder DNS-Anforderung und -Antwort. Es kann auch DNS-Antworten zwischenspeichern. Sie können DNS-Richtlinien auf DNS-Dienste anwenden.

Sie können auch den UDP-Diensttyp für diese Dienste verwenden. In diesem Fall kann die Citrix ADC Appliance jedoch nur den Lastenausgleich von Layer 4 durchführen. DNS-spezifische Funktionen können nicht unterstützt werden.

ANY

Wird für Server verwendet, die jede Art von TCP-, UDP- oder ICMP-Datenverkehr akzeptieren. Der Parameter ANY wird hauptsächlich für den Lastausgleich der Firewall und den Link-Load Balancing verwendet.

SIP-UDP

Wird für Server verwendet, die UDP-basierten SIP-Datenverkehr (Session Initiation Protocol) akzeptieren. SIP initiiert, verwaltet und beendet Multimedia-Kommunikationssitzungen und hat sich als Standard für Internet-Telefonie (VoIP) entwickelt.

Sie können auch den UDP-Diensttyp für diese Dienste verwenden. In diesem Fall führt die Citrix ADC Appliance jedoch nur Layer 4 Lastenausgleich aus. SIP-spezifische Funktionen können nicht unterstützt werden.

DNS-TCP

Wird für Server verwendet, die DNS-Datenverkehr akzeptieren, wobei die Citrix ADC Appliance als Proxy für TCP-Datenverkehr fungiert, der an DNS-Server gesendet wird. Bei Diensten des DNS-TCP-Diensttyps überprüft die Citrix ADC Appliance das Paketformat jeder DNS-Anforderung und -Antwort und kann DNS-Antworten zwischenspeichern, wie beim DNS-Diensttyp.

Sie können auch den TCP-Diensttyp für diese Dienste verwenden. In diesem Fall führt die Citrix ADC Appliance jedoch nur den Layer 4-Lastenausgleich externer DNS-Nameserver durch. Es kann keine DNS-spezifischen Funktionen unterstützen.

RTSP

Wird für Server verwendet, die RTSP-Datenverkehr (Real Time Streaming Protocol) akzeptieren. RTSP bietet die Bereitstellung von Multimedia- und anderen Streaming-Daten. Wählen Sie diesen Typ aus, um Audio-, Video- und andere Arten von gestreamten Medien zu unterstützen.

Sie können auch den TCP-Diensttyp für diese Dienste verwenden. In diesem Fall führt die Citrix ADC Appliance jedoch nur Layer 4 Lastenausgleich aus. Es kann den RTSP-Stream nicht analysieren oder RTSPID-Persistenz oder RTSP NAT unterstützen.

DHCPRA

Wird für Server verwendet, die DHCP-Datenverkehr akzeptieren. Der DHCPRA-Diensttyp kann verwendet werden, um DHCP-Anforderungen und -Antworten zwischen VLANs weiterzuleiten.

DIAMETER

Wird für den Lastausgleich des Diameter-Verkehrs zwischen mehreren Diameter-Servern verwendet. Diameter verwendet nachrichtenbasierten Lastenausgleich.

SSL_DIAMETER

Wird für den Lastausgleich des Diameter-Verkehrs über SSL verwendet.

Dienste werden als DISABLED festgelegt, bis die Citrix ADC Appliance eine Verbindung mit dem zugeordneten Server mit Lastenausgleich herstellt und überprüft, ob sie betriebsbereit ist. Zu diesem Zeitpunkt wird der Dienst als ENABLED bezeichnet. Danach überwacht die Citrix ADC Appliance regelmäßig den Status der Server und versetzt alle, die nicht auf Überwachungsprüfungen (sogenannte Zustandsprüfungen) reagieren, in den Zustand DISABLED, bis sie reagieren.

Hinweis: Sie können einen Bereich von Diensten aus einem einzelnen CLI-Befehl oder demselben Dialogfeld erstellen. Die Namen im Bereich variieren durch eine Zahl, die als Suffix/Präfix verwendet

wird. Zum Beispiel service1, service2 usw. Aus dem Konfigurationsdienstprogramm können Sie einen Bereich nur im letzten Oktett der IP-Adresse angeben, der bei einer IPv4-Adresse und bei einer IPv6-Adresse der vierte Bereich ist. Über die Befehlszeile können Sie den Bereich in einem beliebigen Oktett der IP-Adresse angeben.

QUIC

Wird von Load Balancing-Servern verwendet, die UDP-basierten QUIC-Videoverkehr akzeptieren. Der Dienst ermöglicht es der Citrix ADC Appliance, den verschlüsselten ABR-Videoverkehr über das UDP-Protokoll zu optimieren.

So erstellen Sie einen Dienst mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name> <serverName> <serviceType> <port>

add service Service-HTTP-1 192.0.2.5 HTTP 80
<!--NeedCopy-->
```

So erstellen Sie einen Service mit der GUI

1. Navigieren Sie zu **Traffic Management**> **Load Balancing**> **Services**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie im Dialogfeld Dienst erstellen Werte für die folgenden Parameter an:
   - Dienstname — Name
   - Server — Servername
   - Protokoll — ServiceType
   - Port — Port
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**. Der erstellte Dienst wird im Bereich Dienste angezeigt.

Erstellen eines virtuellen Servers

Nachdem Sie Ihre Dienste erstellt haben, müssen Sie einen virtuellen Server erstellen, um Datenverkehr für Websites, Anwendungen oder Server mit Lastausgleich zu akzeptieren. Sobald der Lastenausgleich konfiguriert ist, stellen Benutzer über die IP-Adresse oder den FQDN des virtuellen Servers eine Verbindung zur Website, Anwendung oder dem Server her.

Hinweis:

- Virtuelle Servernamen mit dem Präfix app_ erscheinen nicht in der GUI, obwohl sie in der Datei ns.conf vorhanden sind und beim Ausführen des Befehls show angezeigt werden. Allerdings werden virtuelle Servernamen mit dem Präfix app in der GUI angezeigt.
- Der virtuelle Server wird als DOWN festgelegt, bis Sie die erstellten Dienste an ihn binden und bis die Citrix ADC Appliance eine Verbindung zu diesen Diensten herstellt und überprüft, ob sie funktionsfähig sind. Erst dann wird der virtuelle Server als UP bezeichnet.

So erstellen Sie einen virtuellen Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <serviceType> <ip> <port>

add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

So erstellen Sie einen virtuellen Server mit der GUI

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und erstellen Sie dann einen virtuellen Server.

Binden von Diensten an den virtuellen Server

Hinweis: Ein Dienst kann an maximal 500 virtuelle Server gebunden werden.

Nachdem Sie Dienste und einen virtuellen Server erstellt haben, müssen Sie die Dienste an den virtuellen Server binden. Normalerweise sind Dienste an virtuelle Server desselben Typs gebunden, aber Sie können bestimmte Arten von Diensten an bestimmte verschiedene Arten von virtuellen Servern binden, wie unten gezeigt.

Virtueller Servertyp	Servicetyp	Kommentar
HTTP	SSL	Normalerweise würden Sie einen SSL-Dienst an einen virtuellen HTTP-Server binden, um Verschlüsselung zu tun.

Virtueller Servertyp	Servicetyp	Kommentar
SSL	HTTP	Normalerweise würden Sie einen HTTP-Dienst an einen virtuellen SSL-Server binden, um SSL-Abladen zu tun.
SSL_TCP	TCP	Normalerweise würden Sie einen TCP-Dienst an einen virtuellen SSL_TCP-Server binden, um SSL-Abladung für andere TCP (SSL-Entschlüsselung ohne Inhaltsbewusstsein) durchzuführen.

Der Status der Dienste, die an einen virtuellen Server gebunden sind, bestimmt den Status des virtuellen Servers: Wenn alle gebundenen Dienste DOWN sind, wird der virtuelle Server mit DOWN gekennzeichnet, und wenn einer der gebundenen Dienste UP oder OUT OF SERVICE ist, ist der Status des virtuellen Servers UP.

So binden Sie einen Dienst mit der CLI an einen virtuellen Lastausgleichsserver

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name> <serviceName>

bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

So binden Sie einen Dienst mit der GUI an einen virtuellen Lastausgleichsserver

1. Navigieren Sie zu **Traffic Management**> **Load Balancing**> **Virtuelle Server**, und wählen Sie einen virtuellen Server aus.
2. Klicken Sie in den Abschnitt **Service** und wählen Sie einen Dienst aus, den Sie binden möchten.

Hinweis: Sie können einen Dienst an mehrere virtuelle Server binden.

Überprüfen der Konfiguration

Nach Abschluss der Basiskonfiguration können Sie die Eigenschaften jedes Dienstes und des virtuellen Lastenausgleichsservers in Ihrem Load Balancing-Setup anzeigen, um zu überprüfen, ob jeder korrekt konfiguriert ist. Nachdem die Konfiguration ausgeführt wurde, können Sie die Statistiken für jeden Dienst und den virtuellen Lastenausgleichsserver anzeigen, um nach möglichen Problemen zu suchen.

Anzeigen der Eigenschaften eines Serverobjekts

Sie können Eigenschaften wie Name, Status und IP-Adresse eines beliebigen Serverobjekts in der Citrix ADC Appliance-Konfiguration anzeigen.

So zeigen Sie die Eigenschaften von Serverobjekten mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show server <serverName>

show server server-1
<!--NeedCopy-->
```

So zeigen Sie die Eigenschaften von Serverobjekten mit dem Konfigurationsdienstprogramm an

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Server**. Die Parameterwerte der verfügbaren Server werden im Detailbereich angezeigt.

Anzeigen der Eigenschaften eines virtuellen Servers

Sie können Eigenschaften wie Name, Status, effektiver Status, IP-Adresse, Port, Protokoll, Methode und Anzahl der gebundenen Dienste für Ihre virtuellen Server anzeigen. Wenn Sie mehr als die grundlegenden Lastenausgleichseinstellungen konfiguriert haben, können Sie die Persistenzeinstellungen für Ihre virtuellen Server, alle an sie gebundenen Richtlinien sowie alle virtuellen Cache-Umleitungs- und Content Switching-Server anzeigen, die an die virtuellen Server gebunden wurden.

So zeigen Sie die Eigenschaften eines virtuellen Lastausgleichsservers mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
show lb vserver <name>

show lb vserver Vserver-LB-1
<!--NeedCopy-->
```

So zeigen Sie die Eigenschaften eines virtuellen Lastausgleichsservers mit der GUI an

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Klicken Sie im Detailbereich auf einen virtuellen Server, um seine Eigenschaften unten im Detailbereich anzuzeigen.
3. Um die Cache-Umleitung und die virtuellen Server mit Content Switching anzuzeigen, die an diesen virtuellen Server gebunden sind, klicken Sie auf **CS/CR-Bindungen anzeigen**.

Anzeigen der Eigenschaften eines Dienstes

Sie können den Namen, den Status, die IP-Adresse, den Port, das Protokoll, die maximale Clientverbindung, die maximalen Anforderungen pro Verbindung und den Servertyp der konfigurierten Dienste anzeigen und diese Informationen verwenden, um Fehler in der Dienstkonfiguration zu beheben.

So zeigen Sie die Eigenschaften von Diensten mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show service <name>

show service Service-HTTP-1
<!--NeedCopy-->
```

So zeigen Sie die Eigenschaften von Diensten mit der GUI an

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienste**. Die Details der verfügbaren Dienste werden im Bereich Dienste angezeigt.

Anzeigen der Bindungen eines Dienstes

Sie können die Liste der virtuellen Server anzeigen, an die der Dienst gebunden ist. Die Bindungsinformationen enthalten außerdem den Namen, die IP-Adresse, den Port und den Status der virtuellen Server, an die die Dienste gebunden sind. Sie können die Bindungsinformationen verwenden, um Probleme mit der Bindung der Dienste an virtuelle Server zu beheben.

So zeigen Sie die Bindungen eines Dienstes mit der CLI an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show service bindings <name>

show service bindings Service-HTTP-1
<!--NeedCopy-->
```

So zeigen Sie die Bindungen eines Dienstes mit der GUI an

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienste**.
2. Wählen Sie im Detailbereich den Dienst aus, dessen Bindungsinformationen Sie anzeigen möchten.
3. Klicken Sie auf der Registerkarte **Aktion** auf **Bindungen anzeigen** .

Anzeigen der Statistiken eines virtuellen Servers

Um die Leistung virtueller Server zu bewerten oder Probleme zu beheben, können Sie Details der virtuellen Server anzeigen, die auf der Citrix ADC Appliance konfiguriert sind. Sie können eine Zusammenfassung der Statistiken für alle virtuellen Server anzeigen, oder Sie können den Namen eines virtuellen Servers angeben, um die Statistiken nur für diesen virtuellen Server anzuzeigen. Sie können die folgenden Details anzeigen:

- Name
- IP-Adresse
- Port
- Protokoll
- Status des virtuellen Servers
- Rate der empfangenen Anfragen
- Trefferrate

So zeigen Sie virtuelle Serverstatistiken mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein, um eine Zusammenfassung der Statistiken für alle virtuellen Server anzuzeigen, die derzeit auf der Appliance konfiguriert sind, oder für einen einzelnen virtuellen Server:

```
stat lb vserver [`<name>`]
<!--NeedCopy-->
```

Beispiel:

```
stat lb vserver server-1
<!--NeedCopy-->
```

Die folgende Abbildung zeigt eine Beispielstatistik.


```
> stat lbvserver
[
Virtual Server(s) Summary
                        vsvrIP  port     Protocol        State    Req/s
vserver1        10.102.20.200    80          SSL         DOWN      0/s

lb1               203.1.113.5   443         DTLS         DOWN      0/s

vicap                       *     0          TCP         DOWN      0/s

lbicap                2.2.3.4  1344          TCP         DOWN      0/s

app_...stest          0.0.0.0     0         HTTP         DOWN      0/s

app_...ttest          0.0.0.0     0         HTTP         DOWN      0/s

app_...fault          0.0.0.0     0         HTTP         DOWN      0/s

app_...test1          0.0.0.0     0         HTTP         DOWN      0/s

app_...1test          0.0.0.0     0         HTTP         DOWN      0/s

app_...fault          0.0.0.0     0         HTTP         DOWN      0/s

app_...est12          0.0.0.0     0         HTTP         DOWN      0/s

app_...sting          0.0.0.0     0         HTTP         DOWN      0/s

test                  2.2.2.2    80         HTTP         DOWN      0/s

shar...lt-lb          0.0.0.0     0         HTTP         DOWN      0/s

shar...es-lb          0.0.0.0     0         HTTP           UP      0/s

shar...es-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...nt-lb          0.0.0.0     0         HTTP           UP      0/s

shar...ts-lb          0.0.0.0     0         HTTP           UP      0/s

shar...ns-lb          0.0.0.0     0         HTTP           UP      0/s

shar...as-lb          0.0.0.0     0         HTTP           UP      0/s

forward-vs            0.0.0.0     0          TCP         DOWN      0/s

tcpcs                 0.0.0.0     0          TCP         DOWN      0/s

test124               0.0.0.0     0          SSL         DOWN      0/s

testssl               0.0.0.0     0          SSL         DOWN      0/s
```


So zeigen Sie Statistiken über virtuelle Server mit der GUI an

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Wenn Sie die Statistiken nur für einen virtuellen Server anzeigen möchten, wählen Sie im Detailbereich den virtuellen Server aus, dessen Statistik Sie anzeigen möchten.
3. Klicken Sie im Detailbereich auf **Statistiken**.

Statistiken eines Dienstes anzeigen

Sie können die Rate der Anfragen, Antworten, Anforderungsbytes, Antwortbytes, aktuelle Clientverbindungen, Anfragen in der Überspannungswarteschlange, aktuelle Serververbindungen usw. mithilfe der Dienststatistiken anzeigen.

So zeigen Sie die Statistiken eines Dienstes mit der CLI an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat service <name>
<!--NeedCopy-->
```

Beispiel:

```
stat service Service-HTTP-1
<!--NeedCopy-->
```

So zeigen Sie die Statistiken eines Dienstes mit der GUI an

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienste**.
2. Wählen Sie im Detailbereich den Dienst aus, dessen Statistiken Sie anzeigen möchten (z. B. Service-HTTP-1).
3. Klicken Sie auf **Statistik**. Die Statistiken werden in einem neuen Fenster angezeigt.

Lastenausgleich virtueller Server und Dienststatus

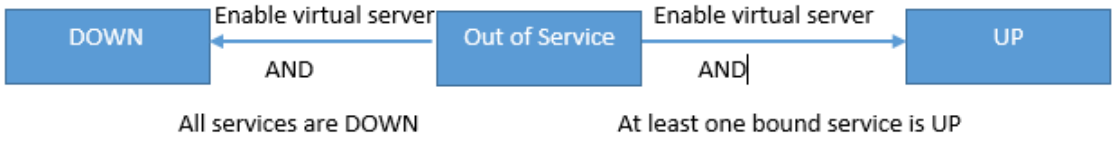
October 5, 2021

Ein virtueller Lastausgleichsserver, der keinen virtuellen Backup-Server hat, kann je nach Status der an ihn gebundenen Dienste und ob er administrativ deaktiviert ist, die folgenden Status annehmen:

- **UP**: Mindestens einer der an den virtuellen Server gebundenen Dienste ist UP.
- **DOWN**: Alle an den virtuellen Server gebundenen Dienste sind DOWN, oder die Lastausgleichsfunktion ist nicht aktiviert.
- **Out of Service (OFS)**: Wenn Sie den virtuellen Server administrativ deaktivieren, wechselt er in den OFS-Status, aber sein effektiver Status ist DOWN. Der Administrator kann den Übergang zum OFS-Status vom Status DOWN oder UP oder in den Status DOWN oder UP aus dem OFS-Status steuern.

Der Status und der effektive Status eines virtuellen Servers sind identisch, wenn ein virtueller Backupserver nicht konfiguriert ist. Wenn jedoch ein virtueller Backup-Server oder eine Kette virtueller Backup-Server konfiguriert wird, wird der effektive Status von den Status der Dienste abgeleitet, die an den primären virtuellen Server und die virtuellen Backup-Server gebunden sind. Wenn einer der virtuellen Backupserver in der Kette UP ist, ist der effektive Status des primären virtuellen Servers UP, selbst wenn alle an den primären virtuellen Server gebundenen Dienste DOWN sind.

Die folgenden Diagramme zeigen die Bedingungen, unter denen ein virtueller Server von einem Status in einen anderen übergeht.



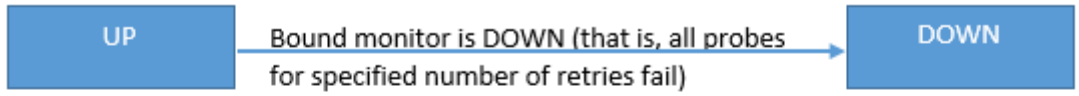
Ein Dienst kann die folgenden Zustände annehmen:

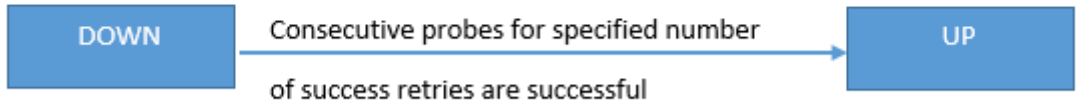
- **UP:** Wenn Prüfpunkte von allen Monitoren, die an den Dienst gebunden sind, erfolgreich sind.
- **DOWN**: Wenn Monitorprüfungen an den Dienst nicht innerhalb der konfigurierten Frist beantwortet werden.
- **OUT OF SERVICE**: Wenn Sie den Dienst administrativ deaktivieren oder wenn Sie den Dienst ordnungsgemäß herunterfahren und keine aktiven Transaktionen für den Dienst vorhanden sind
- **GOING OUT OF SERVICE (TROFS)**: Wenn Sie den Dienst administrativ mit Verzögerung deaktivieren oder den Dienst ordnungsgemäß herunterfahren und aktive Transaktionen für den Dienst vorhanden sind. Weitere Informationen finden Sie unter Graceful Herunterfahren von Diensten.
- **DOWN WHEN OUT OF SERVICE (TROFS_DOWN)[]** Eine Überwachungssonde schlägt fehl, während der Dienst den Status “GOING OUT OF SERVICE” hat.

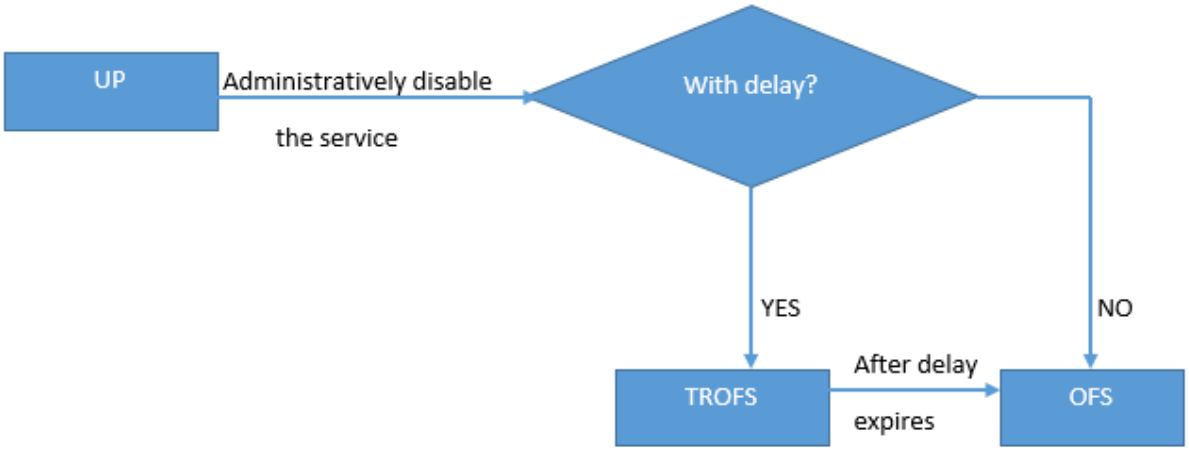
Ein Dienst beim Übergang von UP zu OFS befindet sich im Status GOING OUT OF SERVICE. Ein Dienst, der von DOWN zu OFS wechselt, befindet sich im Zustand DOWN WHEN GOING OUT OF SERVICE. Wenn ein Dienst z. B. DOWN ist und Sie ihn mit Verzögerung deaktivieren, wechselt der Dienst zu DOWN WHEN GOING OUT OF SERVICE und dann in den Zustand OUT OF SERVICE. Wenn ein Dienst UP ist und Sie ihn mit Verzögerung deaktivieren, wechselt der Dienst zu GOING OUT OF SERVICE. Wenn während dieser Zeit eine Überwachungssonde zum Server ausfällt, wechselt der Dienst zu DOWN WHEN GOING OUT OF SERVICE und tritt nach Ablauf der Verzögerungszeit in den OFS-Zustand ein.

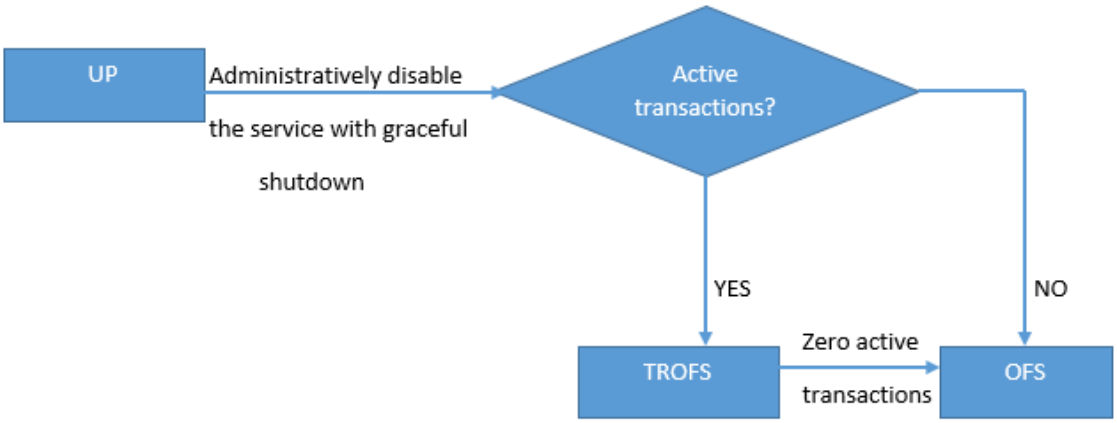
> **Hinweis:**
>
> Sie können Spillover auf einen virtuellen Backup-Server konfigurieren, indem Sie den Parameter HealthThreshold auf einen positiven Wert ungleich Null setzen. Wenn dann ein einzelner Dienst, der an den primären virtuellen Server gebunden ist, in den Zustand DOWN WHEN GOING OUT OF SERVICE wechselt und der Integritätsschwellenwert nicht erreicht wird, wird der primäre virtuelle Server mit DOWN markiert, und neue Verbindungen werden an den virtuellen Backupserver weitergeleitet.

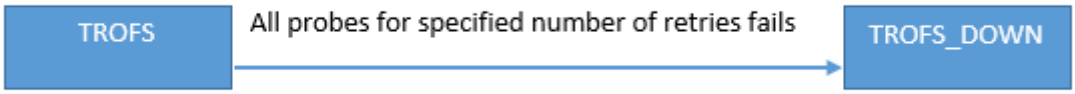
Die folgenden Diagramme zeigen die Bedingungen, unter denen ein Dienst von einem Status in einen anderen übergeht.











Unterstützung für Lastausgleichsprofil

October 5, 2021

Eine Load Balancing-Konfiguration hat viele Parameter, so dass das Festlegen der gleichen Parameter auf mehreren virtuellen Servern mühsam werden kann. Ab Release 11.1 erleichtert ein Load Balancing (LB) Profil diese Aufgabe. Sie können nun Lastausgleichsparameter in einem Profil festlegen und dieses Profil virtuellen Servern zuordnen, anstatt diese Parameter auf jedem virtuellen Server festzulegen.

Die folgenden Parameter werden derzeit in einem LB-Profil unterstützt:

- `HTTPonlyflag`— Schließe das HttpOnly-Attribut in Persistenz-Cookies ein Das Attribut HttpOnly beschränkt den Umfang eines Cookies auf HTTP-Anforderungen und hilft dabei, das Risiko von Cross-Site-Skripting-Angriffen zu verringern.
- UseSecuredPersistenceCookie — Verschlüsseln Sie die Persistenz-Cookie-Werte mithilfe des SHA2-Hash-Algorithmus.
- `Cookiepassphrase`— Geben Sie die Passphrase an, die verwendet wird, um einen gesicherten Persistenz-Cookie-Wert zu erzeugen.
- DBS_LB — Aktiviert den datenbankspezifischen Lastausgleich für MySQL - und MSSQL-Diensttypen.
- Cl_process_local — Pakete, die für einen virtuellen Server in einem Cluster bestimmt sind, werden nicht gesteuert. Aktivieren Sie die Option für den Antwortmodus für einzelne Paketanfragen oder wenn das Upstream-Gerät einen richtigen RSS für die verbindungsbasierte Verteilung ausführt.
- lbhashalgorithm: Geben Sie den Hashing-Algorithmus an, der für die folgenden hashbasierten Load Balancing-Methoden verwendet werden soll:
  - URL-Hash-Methode
  - Domänen-Hash-Methode
  - Ziel-IP-Hash-Methode
  - Quell-IP-Hash-Methode
  - Quell-IP-Ziel-IP-Hash-Methode

- Quell-IP-Quellport-Hash-Methode
- Call ID-Hash-Methode
- Token-Methode

Mögliche Werte: DEFAULT, PRAC, JARH
Standardwert: DEFAULT

- LBHashfinger: Geben Sie die Anzahl der Finger an, die in PRAC- und JARH-Algorithmen für hashbasierte LB-Methoden verwendet werden sollen. Die Erhöhung der Anzahl der Finger ermöglicht eine bessere Verteilung des Datenverkehrs auf Kosten des zusätzlichen Speichers.

Standardwert: 256
Minimaler Wert: 1
Maximaler Wert: 1024

> **Hinweis:**
>
> Sie können DBS_LB und CL_Process_Local-Parameter auf einem virtuellen Server und im Profil festlegen. Wenn Sie diese Parameter auf einem virtuellen Server aktivieren und dann ein Profil für diesen virtuellen Server festlegen, werden die Parameter in der Ausgabe des "show lb vserver" Befehls für diesen virtuellen Server als deaktiviert angezeigt. Überprüfen Sie das Profil, um den aktuellen Status dieser Parameter zu sehen. Wenn Sie ein Profil für einen virtuellen Server festlegen und dann aufheben, werden die Parameter mit Standardwerten für diesen virtuellen Server festgelegt.

So erstellen Sie ein LB-Profil mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb profile <lbprofilename> -dbsLb ( ENABLED | DISABLED ) -
    processLocal ( ENABLED | DISABLED ) -httpOnlyCookieFlag ( ENABLED |
    DISABLED ) -cookiePassphrase -useSecuredPersistenceCookie ( ENABLED
    | DISABLED ) -lbHashAlgorithm <lbHashAlgorithm> -lbHashFingers <
    positive_integer>
<!--NeedCopy-->
```

Beispiel:

```
> sh lb profile p1
LB Profile name:  p1
DBS LB : DISABLED   Process Local: DISABLED
Persistence Cookie HttpOnly Flag: ENABLED
```



```
Use Encrypted Persistence Cookie: DISABLED
No of vservers bound: 0
Store MQTT clientid and username in transactional logs: NO
Hash LB algorithm used in LB decision: DEFAULT
Number of fingers for Hash LB algorithm: 256
Done

<!--NeedCopy-->
```

So erstellen Sie ein LB-Profil mit der GUI

Navigieren Sie zu **System** > **Profile** > **LB-Profil**, und fügen Sie ein Profil hinzu.

So verknüpfen Sie ein LB-Profil mit einem virtuellen LB-Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -lbprofilename <string>
<!--NeedCopy-->
```

Beispiel

```
set lbvserver lbvip1 -lbprofile p1

Done

sh lb vserver lbvip1

lbvip1 (203.0.113.1:80) - HTTP       Type: ADDRESS
State: UP
Last state change was at Wed May 25 12:36:20 2016
Time since last state change: 0 days, 00:01:26.140
Effective State: UP  ARP:DISABLED
Client Idle Timeout: 180 sec
Down state flush: ENABLED
Disable Primary Vserver On Down : DISABLED
Appflow logging: ENABLED
Port Rewrite : DISABLED
No. of Bound Services :  2 (Total)       2 (Active)
Configured Method: LEASTCONNECTION      BackupMethod: ROUNDROBIN
Mode: IP
```



```
Persistence: NONE
Vserver IP and Port insertion: OFF
Push: DISABLED  Push VServer:
Push Multi Clients: NO
Push Label Rule: none
L2Conn: OFF
Skip Persistency: None
Listen Policy: NONE
IcmpResponse: PASSIVE
RHIstate: PASSIVE
New Service Startup Request Rate: 0 PER_SECOND, Increment Interval: 0
Mac mode Retain Vlan: DISABLED
DBS_LB: DISABLED
Process Local: DISABLED
Traffic Domain: 0
LB Profile: p1
Done
<!--NeedCopy-->
```

So verknüpfen Sie ein LB-Profil mit einem virtuellen LB-Server mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Wählen Sie einen virtuellen Server aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie unter **Erweiterte Einstellungen** auf **Profile**.
4. Wählen Sie in der Liste **LB-Profil** das Profil aus, das mit diesem virtuellen Server verknüpft werden soll.

Lastausgleichsalgorithmen

October 5, 2021

Der Lastausgleichsalgorithmus definiert die Kriterien, die die Citrix ADC Appliance verwendet, um den Dienst auszuwählen, an den jede Clientanforderung umgeleitet werden soll. Unterschiedliche Lastausgleichsalgorithmen verwenden unterschiedliche Kriterien. Beispielsweise wählt der Algorithmus für die geringste Verbindung den Dienst mit den wenigsten aktiven Verbindungen aus, während der Roundrobin-Algorithmus eine laufende Warteschlange mit aktiven Diensten verwaltet, jede Verbindung an den nächsten Dienst in der Warteschlange verteilt und diesen Dienst dann an das Ende der Warteschlange sendet.

Einige Load Balancing-Algorithmen eignen sich am besten für die Verarbeitung von Datenverkehr auf Websites, andere für die Verwaltung des Datenverkehrs zu DNS-Servern und andere für die Verar-

beitung komplexer Webanwendungen, die im E-Commerce oder in Unternehmens-LANs oder WANs verwendet werden. In der folgenden Tabelle sind alle Lastausgleichsalgorithmen aufgeführt, die von der Citrix ADC Appliance unterstützt werden, mit einer kurzen Beschreibung der jeweiligen Funktionsweise.

Name	Serverauswahl basierend auf
LEASTCONNECTION	Welcher Dienst hat derzeit die wenigsten Clientverbindungen. Dies ist der standardmäßige Lastausgleichsalgorithmus.
ROUNDROBIN	Welcher Dienst steht ganz oben in einer Liste von Diensten. Nachdem dieser Dienst für eine Verbindung ausgewählt wurde, wird er an den unteren Rand der Liste verschoben.
LEASTRESPONSETIME	Welcher Server mit Lastausgleich hat derzeit die schnellste Reaktionszeit.
URLHASH	Ein Hash der Ziel-URL.
DOMAINHASH	Ein Hash der Zieldomäne.
DESTINATIONIPHASH	Ein Hash der Ziel-IP-Adresse.
SOURCEIPHASH	Ein Hash der Quell-IP-Adresse.
SRCIPDESTIPHASH	Ein Hash der Quell- und Ziel-IP-Adressen.
CALLIDHASH	Ein Hash der Anruf-ID im SIP-Header.
SRCIPSRCPORTHASH	Ein Hash der IP-Adresse und des Ports des Clients.
LEASTBANDWIDTH	Welcher Dienst hat derzeit die wenigsten Bandbreitenbeschränkungen.
LEASTPACKETS	Welcher Dienst empfängt derzeit die wenigsten Pakete.
CUSTOMLOAD	Daten von einem Lastmonitor.
TOKEN	Das konfigurierte Token.
LRTM	Die wenigsten aktiven Verbindungen und die niedrigste durchschnittliche Reaktionszeit.

Abhängig vom Protokoll des Dienstes, für den der Lastausgleich ausgeführt wird, richtet die Citrix ADC Appliance jede Verbindung zwischen Client und Server so ein, dass sie für ein anderes Zeitin-

tervall hält. Dies wird als Load Balancing Granularität bezeichnet, von denen drei Typen sind: anforderungsbasierte, verbindungsbasierte und zeitbasierte Granularität. In der folgenden Tabelle werden die einzelnen Granularitätstypen und die jeweilige Verwendung beschrieben.

Granularität	Typen des Lastausgleichsdiensts	Gibt an
Anforderungsbasiert	HTTP oder HTTPS	Für jede HTTP-Anforderung wird ein neuer Dienst ausgewählt, unabhängig von TCP-Verbindungen. Wie bei allen HTTP-Anforderungen wird die Verbindung geschlossen, nachdem der Webserver die Anforderung erfüllt hat.
Verbindungsbasiert	TCP- und TCP-basierte Protokolle außer HTTP	Für jede neue TCP-Verbindung wird ein Dienst ausgewählt. Die Verbindung bleibt bestehen, bis sie entweder vom Dienst oder vom Client beendet wird.
Zeitbasiert	UDP und andere IP-Protokolle	Für jedes UDP-Paket wird ein neuer Dienst ausgewählt. Bei Auswahl eines Dienstes wird eine Sitzung zwischen dem Dienst und einem Client für einen bestimmten Zeitraum erstellt. Wenn die Zeit abgelaufen ist, wird die Sitzung gelöscht und ein neuer Dienst für zusätzliche Pakete ausgewählt, selbst wenn diese Pakete vom selben Client stammen.

Beim Start eines virtuellen Servers oder wenn sich der Status eines virtuellen Servers ändert, kann der virtuelle Server zunächst die Roundrobin-Methode verwenden, um die Clientanforderungen auf

die physischen Server zu verteilen. Diese Art der Verteilung, die als *Start-Round-Robin bezeichnet wird, hilft,* unnötige Auslastung auf einem einzelnen Server zu verhindern, wenn die anfänglichen Anforderungen erfüllt werden. Nach der Verwendung der Roundrobin-Methode beim Start wechselt der virtuelle Server zur Lastenausgleichsmethode, die auf dem virtuellen Server angegeben ist.

Der Startup-RR-Faktor funktioniert wie folgt:

- Wenn der Start-RR-Faktor auf Null festgelegt ist, wechselt die Appliance je nach Anforderungsrate zur angegebenen Lastausgleichsmethode.
- Wenn der Start-RR-Faktor eine andere Zahl als Null ist, verwendet die Appliance die Roundrobin-Methode für die angegebene Anzahl von Anforderungen, bevor sie zu der angegebenen Lastausgleichsmethode wechselt.
- Standardmäßig ist der Start-RR-Faktor auf Null festgelegt.

Hinweis: Sie können den Start-RR-Faktor für einen einzelnen virtuellen Server nicht festlegen. Der angegebene Wert gilt für alle virtuellen Server auf der Citrix ADC Appliance.

So legen Sie den Start-Round-Robin-Faktor mit der CLI fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb parameter -startupRRFactor <positive_integer>
```

Beispiel

```
set lb parameter -startupRRFactor 25000
```

So legen Sie den Start-Round-Robin-Faktor mit der GUI fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Lastenausgleichsparameter konfigurieren**, und legen Sie den Start-RR-Faktor fest.

Am wenigsten Verbindungsmethode

October 5, 2021

Wenn ein virtueller Server so konfiguriert ist, dass er den Algorithmus (oder die Methode) für den geringsten Verbindungslastausgleich verwendet, wählt er den Dienst mit den wenigsten aktiven Verbindungen aus. Dies ist die Standardmethode, da sie in den meisten Fällen die beste Leistung bietet.

Für TCP-, HTTP-, HTTP- und SSL_TCP-Dienste enthält die Citrix ADC Appliance die folgenden Verbindungstypen in der Liste der vorhandenen Verbindungen:

- **Aktive Verbindungen zu einem Dienst.** Verbindungen, die Anforderungen darstellen, die ein Client an den virtuellen Server gesendet hat und die der virtuelle Server an einen Dienst weitergeleitet hat. Bei HTTP- und HTTPS-Diensten stellen aktive Verbindungen nur die HTTP- oder HTTPS-Anforderungen dar, die noch keine Antwort erhalten haben.
- **Warten von Verbindungen in der Überspannungswarteschlange.** Alle Verbindungen zum virtuellen Server, die in einer Überspannungswarteschlange warten und noch nicht an einen Dienst weitergeleitet wurden. Verbindungen können aus folgenden Gründen jederzeit in der Überspannungswarteschlange aufgebaut werden:
  - Ihre Dienste haben Verbindungsbeschränkungen, und alle Dienste in Ihrer Load Balancing-Konfiguration sind an dieser Grenze.
  - Die Überspannungsschutzfunktion ist konfiguriert und wurde durch eine Überspannung von Anforderungen an den virtuellen Server aktiviert.
  - Der Lastausgleichsserver hat ein internes Limit erreicht und öffnet daher keine neuen Verbindungen. (Beispielsweise ist das Verbindungslimit eines Apache-Servers erreicht.)

Wenn ein virtueller Server die Methode der geringsten Verbindung verwendet, betrachtet er die wartenden Verbindungen als zu dem spezifischen Dienst. Daher werden keine neuen Verbindungen zu diesen Diensten geöffnet.

Bei UDP-Diensten umfassen die Verbindungen, die der geringste Verbindungsalgorithmus berücksichtigt, alle Sitzungen zwischen dem Client und einem Dienst. Bei diesen Sitzungen handelt es sich um logische, zeitbasierte Entitäten. Wenn das erste UDP-Paket in einer Sitzung eintrifft, erstellt die Citrix ADC Appliance eine Sitzung zwischen Quell-IP-Adresse und -port sowie der Ziel-IP-Adresse und -port.

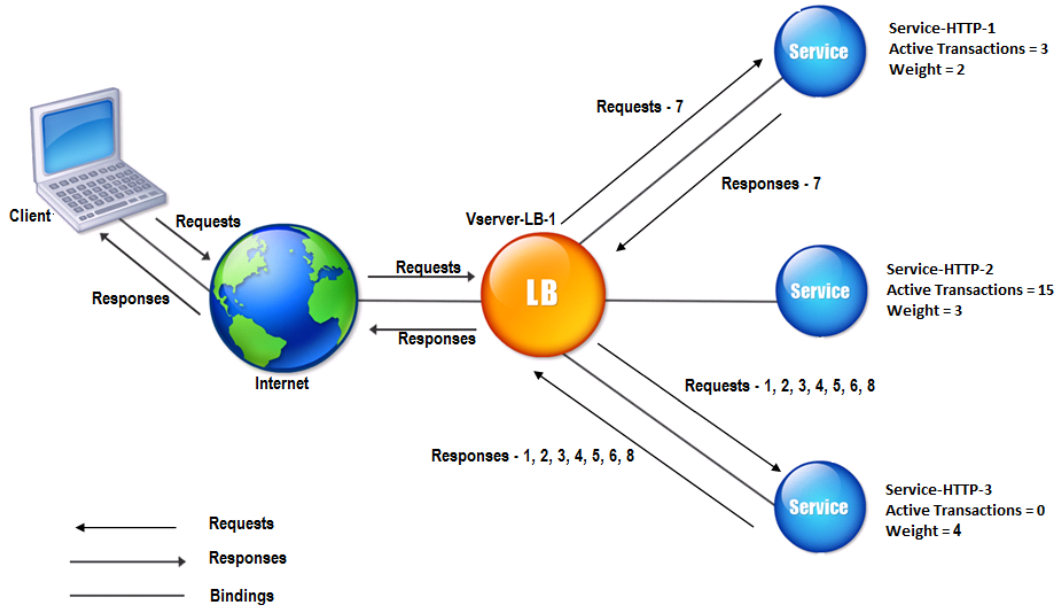
Bei RTSP-Verbindungen (Real-Time Streaming Protocol) verwendet die Citrix ADC Appliance die Anzahl der aktiven Steuerungsverbindungen, um die niedrigste Anzahl von Verbindungen zu einem RTSP-Dienst zu ermitteln.

Das folgende Beispiel zeigt, wie ein virtueller Server einen Dienst für den Lastenausgleich mithilfe der Methode der geringsten Verbindung auswählt. Betrachten Sie die folgenden drei Dienste:

- Service-HTTP-1 behandelt 3 aktive Transaktionen.
- Service-HTTP-2 behandelt 15 aktive Transaktionen.
- Service-HTTP-3 verarbeitet keine aktiven Transaktionen.

Das folgende Diagramm veranschaulicht, wie die Citrix ADC Appliance eingehende Anforderungen weiterleitet, wenn die Methode der geringsten Verbindung verwendet wird.

Abbildung 1. Mechanismus der Load Balancing-Methode Least Connections



In diesem Diagramm wählt der virtuelle Server den Dienst für jede eingehende Verbindung aus, indem er den Server mit den wenigsten aktiven Transaktionen auswählt.

Verbindungen werden wie folgt weitergeleitet:

- Service-HTTP-3 empfängt die erste Anforderung, da es keine aktiven Transaktionen verarbeitet.

  Hinweis: Der Service ohne aktive Transaktion wird zuerst ausgewählt.

- Service-HTTP-3 empfängt die zweite und dritte Anforderung, da der Dienst die nächstgeringste Anzahl von aktiven Transaktionen hat.
- Service-HTTP-1 erhält die vierte Anforderung, da Service-HTTP-1 und Service-HTTP-3 die gleiche Anzahl aktiver Transaktionen haben, der virtuelle Server verwendet die Round-Robin-Methode, um zwischen ihnen zu wählen.
- Service-HTTP-3 empfängt die fünfte Anforderung.
- Service-http-1 empfängt die sechste Anforderung usw., bis sowohl Service-http-1 als auch Service-http-3 dieselbe Anzahl von Anforderungen verarbeiten wie Service-http-2. Dann beginnt die Citrix ADC Appliance mit der Weiterleitung von Anfragen an Service-HTTP-2, wenn es sich um den am wenigsten geladenen Dienst handelt oder in der Round-Robin-Warteschlange an der Reihe ist.

  Hinweis: Wenn Verbindungen zu Service-HTTP-2 geschlossen werden, werden möglicherweise neue Verbindungen erhalten, bevor jeder der beiden anderen Dienste 15 aktive Transaktionen

aufweist.

In der folgenden Tabelle wird erläutert, wie Verbindungen in dem zuvor beschriebenen Load Balancing-Setup mit drei Diensten verteilt werden.

Eingehende Verbindung	Ausgewählter Service	Aktuelle Anzahl aktiver Verbindungen	Bemerkungen
Request-1	Service-HTTP-3; (N = 0)	1	Service-HTTP-3 hat die wenigsten aktiven Verbindungen.
Request-2	Service-HTTP-3; (N = 1)	2	Service-HTTP-3 hat die wenigsten aktiven Verbindungen.
Request-3	Service-HTTP-3; (N = 2)	3	-
Request-4	Service-HTTP-1; (N = 3)	4	Service-http-1 und Service-http-3 haben die gleiche Anzahl von aktiven Verbindungen.
Request-5	Service-HTTP-3; (N = 3)	4	Service-http-1 und Service-http-3 haben die gleiche Anzahl von aktiven Verbindungen.
Request-6	Service-HTTP-1; (N = 4)	5	-
Request-7	Dienst-HTTP-3; (N = 4)	5	-
Request-8	Service-HTTP-1; (N = 5)	6	-

Service-HTTP-2 wird für den Lastenausgleich ausgewählt, wenn seine aktiven Transaktionen abgeschlossen und die aktuellen Verbindungen zu ihm geschlossen werden oder wenn die anderen Dienste (Service-HTTP-1 und Service-HTTP-3) über 15 oder mehr Verbindungen verfügen.

Die Citrix ADC Appliance kann auch die geringste Verbindungsmethode verwenden, wenn Dienstgewichte zugewiesen werden. Es wählt einen Dienst mit dem Wert (Nw) des folgenden Ausdrucks aus:

Nw = (Anzahl der aktiven Transaktionen) * (10000/Gewicht)

Das folgende Beispiel zeigt, wie die Citrix ADC Appliance einen Dienst für den Lastausgleich auswählt, indem sie die geringste Verbindungsmethode verwendet, wenn Dienstgewichte zugewiesen werden. Im vorangegangenen Beispiel wird Service-http-1 eine Gewichtung von 2 zugewiesen, Service-http-2 wird eine Gewichtung von 3 zugewiesen und Service-http-3 wird die Gewichtung 4 zugewiesen. Verbindungen werden wie folgt weitergeleitet:

- Service-HTTP-3 erhält die erste, da der Dienst keine aktiven Transaktionen verarbeitet.

  Hinweis: Wenn die Dienste keine aktiven Transaktionen abwickeln, verwendet die Citrix ADC Appliance die Round-Robin-Methode unabhängig von den Gewichten, die jedem der Dienste zugewiesen sind.

- Service-HTTP-3 erhält die zweite, dritte, vierte, fünfte, sechste und siebte Anforderung, da der Dienst den niedrigsten Nw-Wert aufweist.
- Service-HTTP-1 empfängt die achte Anforderung. Da Service-HTTP-1 und Service-HTTP-3 jetzt denselben Nw-Wert haben, führt die Appliance Load Balancing auf Round-Robin-Weise durch. Daher erhält Service-HTTP-3 die neunte Anforderung.

In der folgenden Tabelle wird erläutert, wie Verbindungen für das zuvor beschriebene Drei-Service-Load Balancing-Setup verteilt werden.

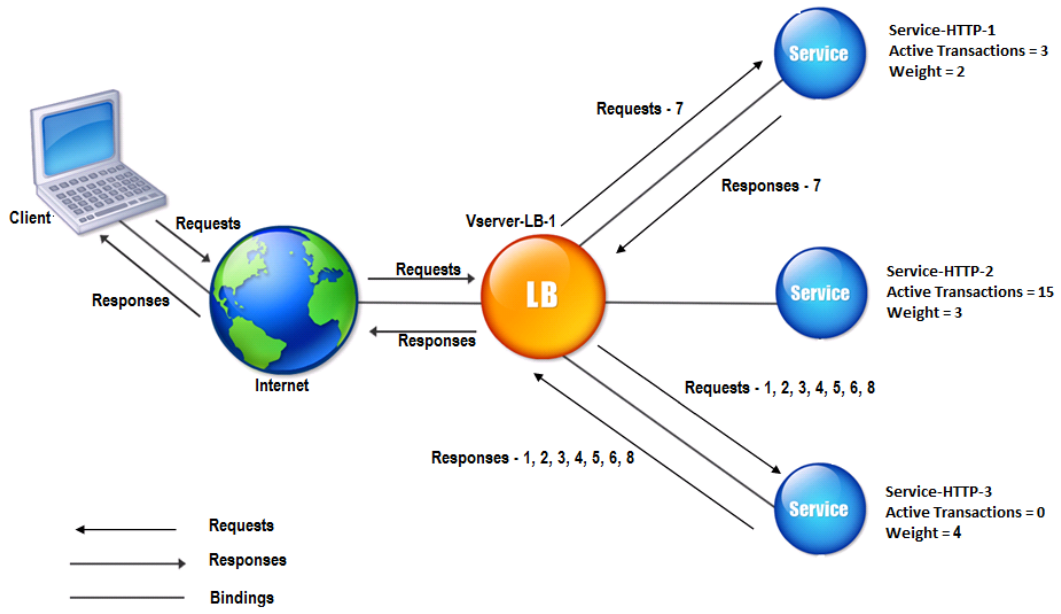
Anfrage erhalten	Ausgewählter Service	Aktueller Nw (Anzahl der aktiven Transaktionen) * (10000/Gewicht) Wert	Bemerkungen
Request-1	Service-HTTP-3; (Nw = 0)	Nw = 2500	Service-http-3 hat den niedrigsten Nw-Wert.
Request-2	Service-HTTP-3; (Nw = 2500)	Nw= 5000	
Request-3	Dienst-HTTP-3; (Nw = 5000)	Nw= 7500	
Request-4	Service-HTTP-3; (Nw = 7500)	Nw= 10000	
Request-5	Service-HTTP-3; (Nw = 10000)	Nw= 12500	
Request-6	Service-HTTP-3; (Nw = 12500)	Nw= 15000	

Anfrage erhalten	Ausgewählter Service	Aktueller Nw (Anzahl der aktiven Transaktionen) * (10000/Gewicht) Wert	Bemerkungen
Request-7	Service-HTTP-1; (Nw = 15000)	Nw= 20000	Service-http-1 und Service-http-3 haben die gleichen Nw-Werte
Request-8	Service-HTTP-3; (Nw = 15000)	Nw= 17500	

Service-HTTP-2 wird für den Lastenausgleich ausgewählt, wenn er seine aktiven Transaktionen abschließt oder wenn der Nw-Wert anderer Dienste (Service-HTTP-1 und Service-HTTP-3) 50000 ist.

Das folgende Diagramm veranschaulicht, wie die Citrix ADC Appliance die geringste Verbindungsmethode verwendet, wenn den Diensten Gewichtungen zugewiesen werden.

Abbildung 2. Mechanismus der Load Balancing-Methode Lost Connections, wenn Gewichtungen zugewiesen werden



Informationen zum Konfigurieren der kleinsten Verbindungsmethode finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

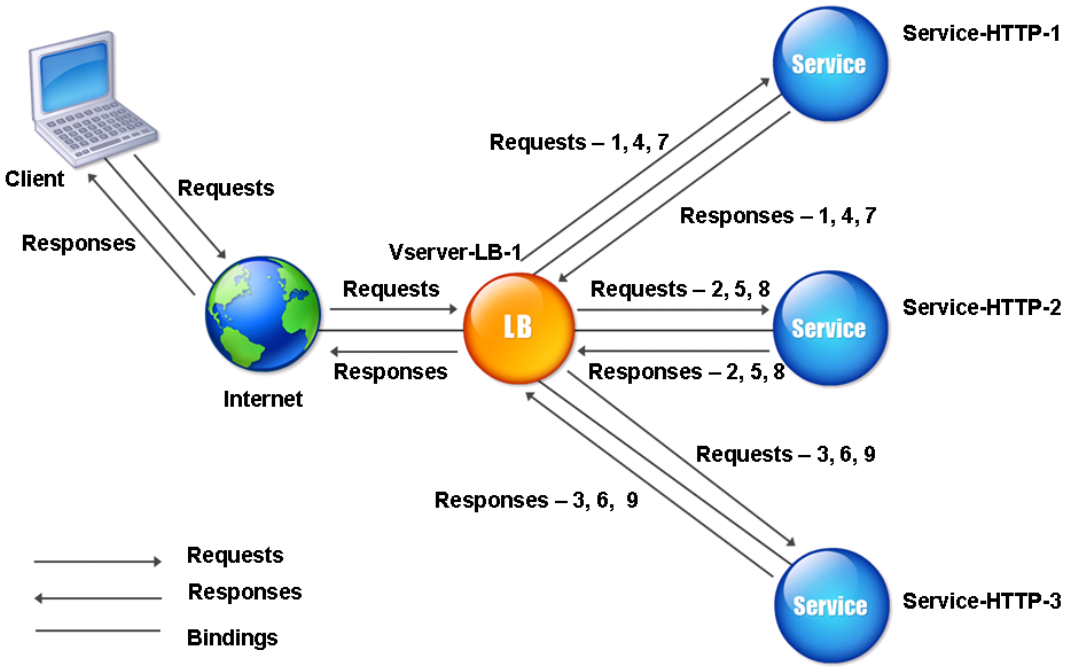
Round-Robin-Methode

October 5, 2021

Wenn ein virtueller Lastausgleichsserver für die Verwendung der Roundrobin-Methode konfiguriert ist, rotiert er kontinuierlich eine Liste der Dienste, die an ihn gebunden sind. Wenn der virtuelle Server eine Anforderung erhält, weist er die Verbindung dem ersten Dienst in der Liste zu und verschiebt diesen Dienst dann an den unteren Rand der Liste.

Das folgende Diagramm veranschaulicht, wie die Citrix ADC Appliance die Roundrobin-Methode mit einem Lastausgleichs-Setup verwendet, das drei Server mit Lastenausgleich und die zugehörigen Dienste enthält.

Abbildung 1. Funktionsweise der Round-Robin-Load Balancing-Methode



Wenn Sie jedem Dienst ein anderes Gewicht zuweisen, führt die Citrix ADC Appliance die gewichtete Round-Robin-Verteilung eingehender Verbindungen durch. Dies geschieht, indem die niedriger gewichteten Dienste in geeigneten Intervallen übersprungen werden.

Angenommen, Sie haben ein Lastausgleichs-Setup mit drei Diensten. Sie setzen Service-http-1 auf ein Gewicht von 2, Service-http-2 auf ein Gewicht von 3 und Service-http-3 auf ein Gewicht von 4. Die

Dienste sind an vServer-LB-1 gebunden, der für die Verwendung der Roundrobin-Methode konfiguriert ist. Bei dieser Einrichtung werden eingehende Anfragen wie folgt zugestellt:

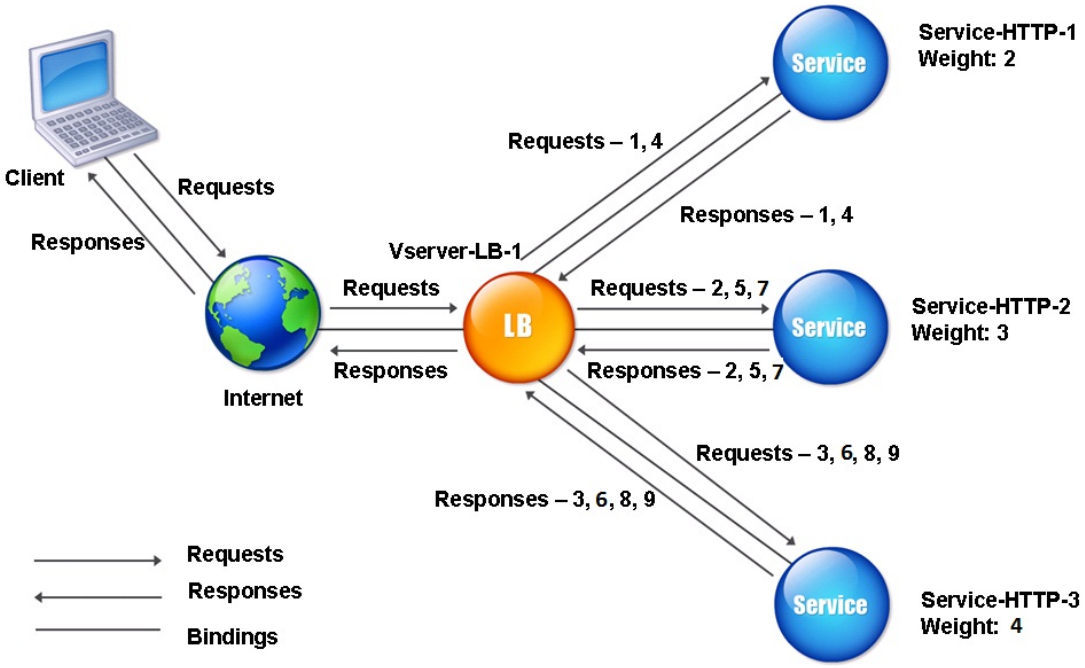
- Service-HTTP-1 empfängt die erste Anforderung.
- Service-HTTP-2 empfängt die zweite Anforderung.
- Service-HTTP-3 empfängt die dritte Anforderung.
- Service-HTTP-1 empfängt die vierte Anforderung.
- Service-HTTP-2 empfängt die fünfte Anforderung.
- Service-http-3 empfängt die sechste Anforderung.
- Service-HTTP-2 empfängt die siebte Anforderung.
- Service-HTTP-3 empfängt sowohl die achte als auch die neunte Anforderung.

Hinweis: Sie können auch Gewichtungen für Dienste konfigurieren, um zu verhindern, dass mehrere Dienste denselben Server verwenden und den Server überladen.

Ein neuer Zyklus beginnt dann mit dem gleichen Muster.

Das folgende Diagramm veranschaulicht die gewichtete Roundrobin-Methode.

Abbildung 2. Wie die Round Robin Load Balancing-Methode Gewichtete Dienste unterstützt



Informationen zum Konfigurieren der Round-Robin-Methode finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Methode der geringsten Antwortzeit

October 5, 2021

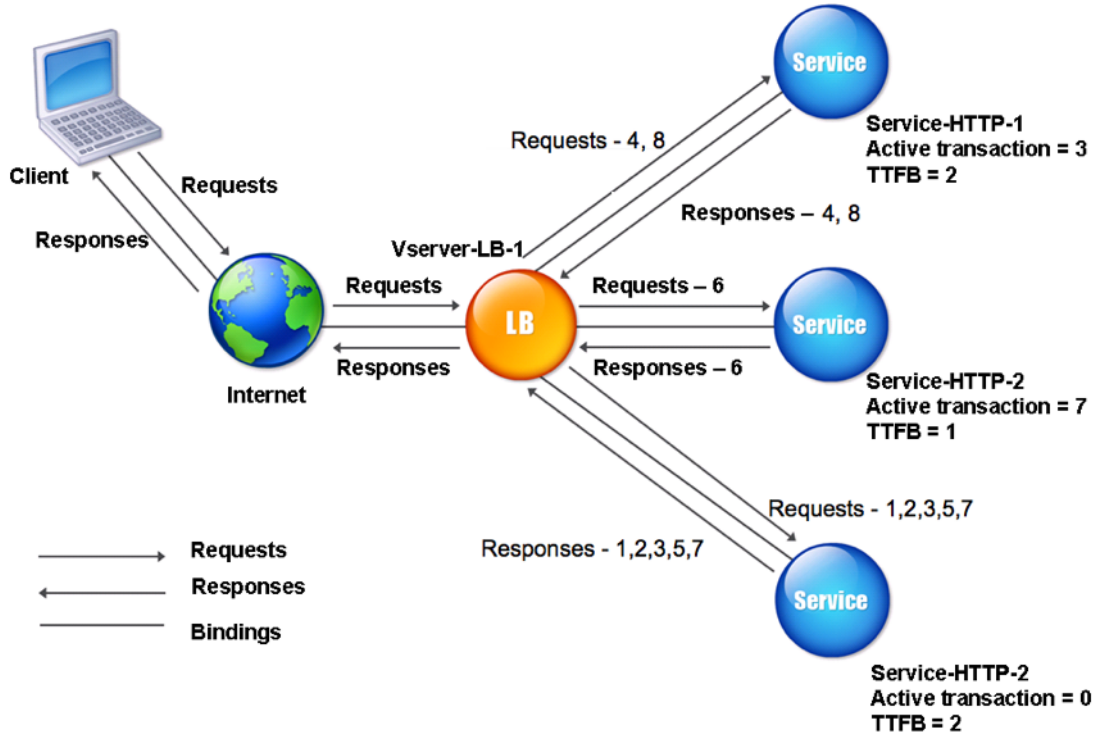
Wenn der virtuelle Lastausgleichsserver so konfiguriert ist, dass er die Methode der geringsten Antwortzeit verwendet, wählt er den Dienst mit den wenigsten aktiven Verbindungen und der niedrigsten durchschnittlichen Antwortzeit aus. Sie können diese Methode nur für HTTP und Secure Sockets Layer (SSL) -Lastausgleich von virtuellen Servern konfigurieren. Die Antwortzeit (auch Time to First Byte oder TTFB genannt) ist das Zeitintervall zwischen dem Senden eines Anforderungspakets an einen Dienst und dem Empfangen des ersten Antwortpakets vom Dienst. Die Citrix ADC Appliance verwendet den Antwortcode 200, um TTFB zu berechnen.

Das folgende Beispiel zeigt, wie ein virtueller Server einen Dienst für den Lastenausgleich mithilfe der Methode für die geringste Antwortzeit auswählt. Betrachten Sie die folgenden drei Dienste:

- Service-HTTP-1 behandelt drei aktive Transaktionen und TTFB ist zwei Sekunden.
- Service-HTTP-2 behandelt sieben aktive Transaktionen und TTFB ist eine Sekunde.
- Service-HTTP-3 verarbeitet keine aktiven Transaktionen und TTFB ist zwei Sekunden.

Das folgende Diagramm veranschaulicht, wie die Citrix ADC Appliance die Methode der geringsten Antwortzeit verwendet, um die Verbindungen weiterzuleiten.

Abbildung 1. Funktionsweise der Load Balancing-Methode für die geringste Antwortzeit



Der virtuelle Server wählt einen Dienst aus, indem die Anzahl der aktiven Transaktionen mit dem TTFB für jeden Dienst multipliziert und dann den Dienst mit dem niedrigsten Ergebnis ausgewählt wird. Für das oben gezeigte Beispiel leitet der virtuelle Server Anforderungen wie folgt weiter:

- Service-HTTP-3 empfängt die erste Anforderung, da der Dienst keine aktiven Transaktionen verarbeitet.
- Service-HTTP-3 erhält auch die zweite und dritte Anforderung, da das Ergebnis der niedrigste der drei Dienste ist.
- Service-HTTP-1 empfängt die vierte Anforderung. Da Service-HTTP-1 und Service-HTTP-3 dasselbe Ergebnis haben, wählt die Citrix ADC Appliance mit der Round-Robin-Methode zwischen ihnen aus.
- Service-HTTP-3 empfängt die fünfte Anforderung.
- Service-HTTP-2 empfängt die sechste Anforderung, da sie zu diesem Zeitpunkt das niedrigste Ergebnis hat.
- Da Service-http-1, Service-http-2 und Service-http-3 zu diesem Zeitpunkt alle dasselbe Ergebnis haben, wechselt die Appliance zur Roundrobin-Methode und verteilt weiterhin Verbindungen mit dieser Methode.

In der folgenden Tabelle wird erläutert, wie Verbindungen in dem zuvor beschriebenen Load Balancing-Setup mit drei Diensten verteilt werden.

Anfrage erhalten	Ausgewählter Service	Aktueller N-Wert (Anzahl der aktiven Transaktionen * TTFB)	Bemerkungen
Request-1	Service-HTTP-3; (N = 0)	N = 2	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-2	Service-HTTP-3; (N = 2)	N = 4	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-3	Dienst-HTTP-3; (N = 4)	N = 6	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-4	Dienst-HTTP-1; (N = 6)	N = 8	Service-http-1 und Service-http-3 haben die gleichen N-Werte. Die Appliance verwendet die Roundrobin-Methode, um die Anforderungen zu verteilen.
Request-5	Dienst-HTTP-3; (N = 6)	N = 8	Service-http-1 und Service-http-3 haben die gleichen N-Werte.
Request-6	Service-HTTP-2; (N = 7)	N = 8	Service-HTTP-2 hat den niedrigsten N-Wert.

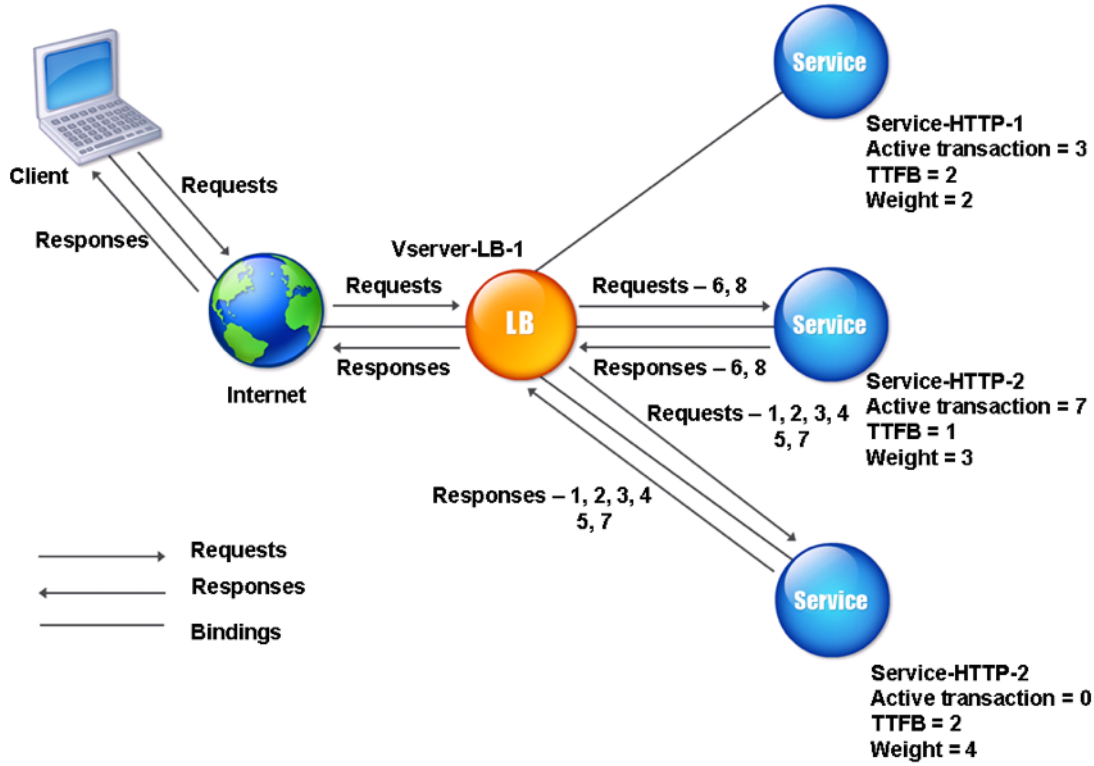
Anfrage erhalten	Ausgewählter Service	Aktueller N-Wert (Anzahl der aktiven Transaktionen * TTFB)	Bemerkungen
Request-7	Service-HTTP-3; (N = 8)	N = 10	Service-http-1, service-http-2 und service-http-3 haben die gleichen N-Werte. Die Citrix ADC Appliance verwendet die Roundrobin-Methode, um die Anforderungen zu verteilen.
Request-8	Service-HTTP-1; (N = 8)	N = 10	Service-HTTP-1 und Service-HTTP-2 haben die gleichen N-Werte, die Appliance verwendet die Roundrobin-Methode, um die Anforderungen zu verteilen.

Service-HTTP-1 wird erneut für den Lastenausgleich ausgewählt, wenn es seine aktiven Transaktionen abschließt oder wenn sein N-Wert kleiner ist als die anderen Dienste (Service-HTTP-2 und Service-HTTP-3).

Auswahl der Dienste bei der Zuweisung von Gewichten

Das folgende Diagramm veranschaulicht, wie die Citrix ADC Appliance die Methode der geringsten Antwortzeit verwendet, wenn Gewichtungen zugewiesen werden.

Abbildung 2. Funktionsweise der Load Balancing-Methode für die geringste Antwortzeit bei Zuweisung von Gewichten



Der virtuelle Server wählt einen Dienst mithilfe des Wertes (Nw) im folgenden Ausdruck aus:

Nw = (N) * (10000/Gewicht), wobei N = (Anzahl der aktiven Transaktionen * TTFB)

Angenommen, Service-HTTP-1 wird eine Gewichtung von 2 zugewiesen, Service-HTTP-2 wird Gewicht von 3 zugewiesen und Service-HTTP-3 wird Gewicht von 4 zugewiesen.

Die Citrix ADC Appliance verteilt Anforderungen wie folgt:

- Service-HTTP-3 empfängt die erste Anforderung, da es keine aktiven Transaktionen verarbeitet.

  Wenn die Dienste keine aktiven Transaktionen abwickeln, wählt die Appliance sie unabhängig von den ihnen zugewiesenen Gewichten aus.
- Service-http-3 empfängt die zweite, dritte, vierte und fünfte Anforderung, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-2 empfängt die sechste Anforderung, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-http-3 empfängt die siebte Anforderung, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-2 empfängt die achte Anforderung, da dieser Dienst den niedrigsten Nw-Wert hat.

Service-HTTP-1 hat das niedrigste Gewicht und daher den höchsten Nw-Wert, so dass der virtuelle Server ihn nicht für den Lastenausgleich auswählt.

In der folgenden Tabelle wird erläutert, wie Verbindungen in dem zuvor beschriebenen Load Balancing-Setup mit drei Diensten verteilt werden.

Anfrage erhalten	Ausgewählter Service	Aktueller Nw-Wert = (N) * (10000/Gewicht)	Bemerkungen
Request-1	Service-HTTP-3; (Nw = 0)	Nw= 5000	Service-http-3 hat den niedrigsten Nw-Wert.
Request-2	Dienst-HTTP-3; (Nw = 5000	Nw= 10000	Service-http-3 hat den niedrigsten Nw-Wert.
Request-3	Service-HTTP-3; (Nw = 10000)	Nw= 15000	Service-http-3 hat den niedrigsten Nw-Wert.
Request-4	Service-HTTP-3; (Nw = 15000)	Nw= 20000	Service-http-3 hat den niedrigsten Nw-Wert.
Request-5	Service-HTTP-3; (Nw = 20000)	Nw= 25000	Service-http-3 hat den niedrigsten Nw-Wert.
Request-6	Dienst-HTTP-2; (Nw = 23333,34)	Nw = 26666,67	Service-HTTP-2 hat den niedrigsten Nw-Wert.
Request-7	Service-HTTP-3; (Nw = 25000)	Nw = 30000	Service-http-3 hat den niedrigsten Nw-Wert.
Request-8	Dienst-HTTP-2; (Nw = 26666,67)	Nw= 30000	Service-HTTP-2 hat den niedrigsten Nw-Wert.

Service-HTTP-1 wird für den Lastenausgleich ausgewählt, wenn er seine aktiven Transaktionen abschließt oder wenn sein Nw-Wert kleiner ist als andere Dienste (Service-http-2 und Service-http-3).

So konfigurieren Sie die Methode für den Lastausgleich mit der Befehlszeilenschnittstelle für die geringste Antwortzeit

Geben Sie an der Eingabeaufforderung ein;


```
set lb vserver <name> -lbMethod LEASTRESPONSETIME
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -lbMethod LEASTRESPONSETIME
<!--NeedCopy-->
```

So konfigurieren Sie die Methode für den Lastausgleich mit der Benutzeroberfläche für die geringste Antwortzeit

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter Erweiterte Einstellungen die Option **LEASTRESPONSETIME**aus.

Weitere Informationen zum Konfigurieren von Monitoren finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

LRTM-Methode

October 5, 2021

Hinweis: LRTM steht für Least response time method using monitors (LRTM).

Wenn ein virtueller Lastausgleichsserver für die Verwendung der LRTM-Methode konfiguriert ist, verwendet er die vorhandene Überwachungsinfrastruktur, um die schnellste Reaktionszeit zu erhalten. Der virtuelle Lastausgleichsserver wählt dann den Dienst mit der kleinsten Anzahl aktiver Transaktionen und der geringsten Antwortzeit aus. Bevor Sie die LRTM-Methode verwenden, müssen Sie anwendungsspezifische Monitore an jeden Dienst binden und den LRTM-Modus auf diesen Monitoren aktivieren. Die Citrix ADC Appliance trifft dann Lastenausgleichsentscheidungen basierend auf den Reaktionszeiten, die sie anhand von Monitoring-Prüfpunkten berechnet.

Sie können die LRTM-Methode verwenden, um auch Nicht-HTTP- und Nicht-HTTPS-Dienste zu Lastenausgleich. Sie können diese Methode auch verwenden, wenn mehrere Monitore an einen Dienst gebunden sind. Jeder Monitor bestimmt die Antwortzeit mithilfe des Protokolls, das er für den Dienst misst, an den er gebunden ist. Der virtuelle Server berechnet dann eine durchschnittliche Antwortzeit für diesen Dienst, indem die Ergebnisse gemittelt werden.

In der folgenden Tabelle wird zusammengefasst, wie die Reaktionszeiten für die verschiedenen Monitore berechnet werden.

Überwachung	Reaktionszeitberechnung
PING	Zeitunterschied zwischen der ICMP-ECHO-Anforderung und der ICMP-ECHO-Antwort.
TCP	Zeitunterschied zwischen der SYN-Anforderung und der SYN+ACK-Antwort.
HTTP	Zeitunterschied zwischen der HTTP-Anforderung (nachdem die TCP-Verbindung hergestellt wurde) und der HTTP-Antwort.
TCP-ECV	Zeitunterschied zwischen dem Zeitpunkt, zu dem die Daten-Sendezeichenfolge gesendet wird und der Datenempfangszeichenfolge zurückgegeben wird. Es wird davon ausgegangen, dass ein TCP-ECV-Monitor ohne die Sende- und Empfangszeichenfolgen eine falsche Konfiguration hat.
HTTP-ECV	Zeitunterschied zwischen der HTTP-Anforderung und der HTTP-Antwort.
UDP-ECV	Zeitunterschied zwischen der Sendezeichenfolge des UDP und der Empfangszeichenfolge. Ein UDP-ECV-Monitor ohne Empfangszeichenfolge wird als falsch konfiguriert.
DNS	Zeitunterschied zwischen einer DNS-Abfrage und der DNS-Antwort.
TCPS	Zeitunterschied zwischen einer SYN-Anfrage und der SSL-Handshake-Abschluss.
FTP	Zeitunterschied zwischen dem Senden des Benutzernamens und dem Abschluss der Benutzerauthentifizierung.
HTTPS (überwacht HTTPS-Anfragen)	Der Zeitunterschied ist der gleiche wie für den HTTP-Monitor.

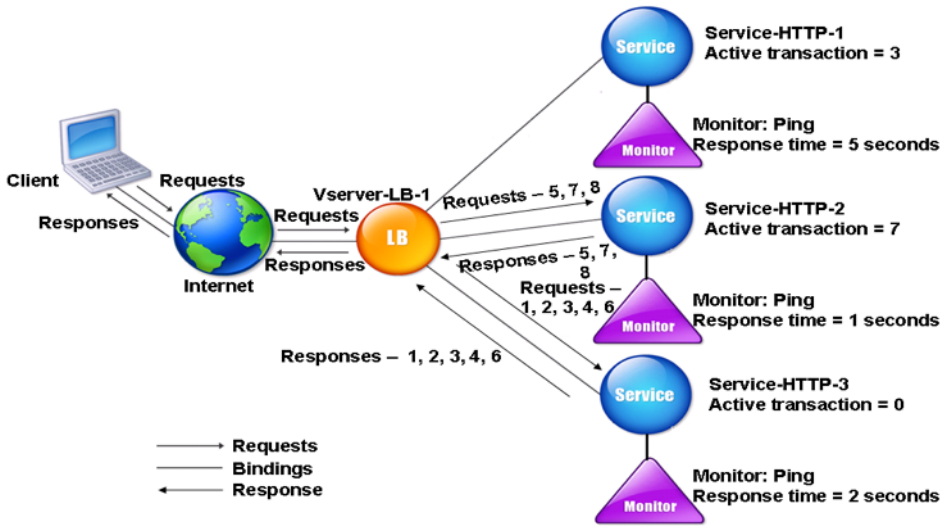
Überwachung	Reaktionszeitberechnung
HTTPS-ECV (überwacht HTTPS-Anfragen)	Der Zeitunterschied ist der gleiche wie beim HTTP-ECV-Monitor
USER	Zeitdifferenz zwischen dem Zeitpunkt, zu dem eine Anforderung an den Dispatcher gesendet wird, und dem Zeitpunkt, zu dem die Dispatcher-Antwort empfangen wird.

Das folgende Beispiel zeigt, wie die Citrix ADC Appliance einen Dienst für den Lastenausgleich mithilfe der LRTM-Methode auswählt. Betrachten Sie die folgenden drei Dienste:

- Service-HTTP-1 verarbeitet 3 aktive Transaktionen und die Antwortzeit beträgt fünf Sekunden.
- Service-HTTP-2 behandelt 7 aktive Transaktionen und die Antwortzeit beträgt eine Sekunde.
- Service-HTTP-3 verarbeitet keine aktiven Transaktionen und die Antwortzeit beträgt zwei Sekunden.

Das folgende Diagramm veranschaulicht den Prozess, den die Citrix ADC Appliance beim Weiterleiten von Anforderungen folgt.

Abbildung 1. Funktionsweise der LRTM-Methode



Der virtuelle Server wählt einen Dienst mithilfe des Wertes (N) im folgenden Ausdruck aus:

N = (Anzahl der aktiven Transaktionen * Antwortzeit, die vom Monitor bestimmt wird)

Der virtuelle Server liefert Anforderungen wie folgt:

- Service-HTTP-3 erhält die erste Anforderung, da dieser Dienst keine aktive Transaktion verarbeitet.
- Service-HTTP-3 erhält die zweite, dritte und vierte Anforderung, da dieser Dienst den niedrigsten N-Wert hat.
- Service-HTTP-2 empfängt die fünfte Anforderung, da dieser Dienst den niedrigsten N-Wert hat.
- Da sowohl Service-HTTP-2 als auch Service-HTTP-3 derzeit denselben N-Wert haben, wechselt die Citrix ADC Appliance zur Round-Robin-Methode. Daher erhält Service-HTTP-3 die sechste Anfrage.
- Service-HTTP-2 empfängt die siebte und achte Anforderung, da dieser Dienst den niedrigsten N-Wert hat.

Service-HTTP-1 wird für den Lastausgleich nicht berücksichtigt, da er im Vergleich zu den anderen beiden Diensten stärker geladen ist (hat den höchsten N-Wert). Wenn Service-HTTP-1 jedoch die aktiven Transaktionen abschließt, berücksichtigt die Citrix ADC Appliance diesen Dienst erneut für den Lastenausgleich.

In der folgenden Tabelle wird zusammengefasst, wie N für die Dienste berechnet wird.

Anfrage erhalten	Ausgewählter Service	Aktueller N-Wert (Anzahl der aktiven Transaktionen * TTFB)	Bemerkungen
Request-1	Service-HTTP-3; (N = 0)	N = 2	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-2	Service-HTTP-3; (N = 2)	N = 4	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-3	Dienst-HTTP-3; (N = 4)	N = 6	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-4	Dienst-HTTP-3; (N = 6)	N = 8	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-5	Service-HTTP-2; (N = 7)	N = 8	Service-HTTP-2 hat den niedrigsten N-Wert.

Anfrage erhalten	Ausgewählter Service	Aktueller N-Wert (Anzahl der aktiven Transaktionen * TTFB)	Bemerkungen
Request-6	Service-HTTP-3; (N = 8)	N = 10	Service-HTTP-2 und Service-HTTP-3 haben die gleichen N-Werte. Citrix ADC Appliance wechselt auf die Roundrobin-Methode und wählt Service-HTTP-3 aus
Request-7	Service-HTTP-2; (N = 8)	N = 9	Service-HTTP-2 hat den niedrigsten N-Wert.
Request-8	Service-HTTP-2; (N = 9)	N = 10	Service-HTTP-2 hat den niedrigsten N-Wert.

Service-HTTP-1 wird erneut für den Lastenausgleich ausgewählt, wenn es seine aktiven Transaktionen abschließt oder wenn sein N-Wert kleiner ist als die anderen Dienste (Service-HTTP-2 und Service-HTTP-3).

Auswahl der Dienste bei der Zuweisung von Gewichten

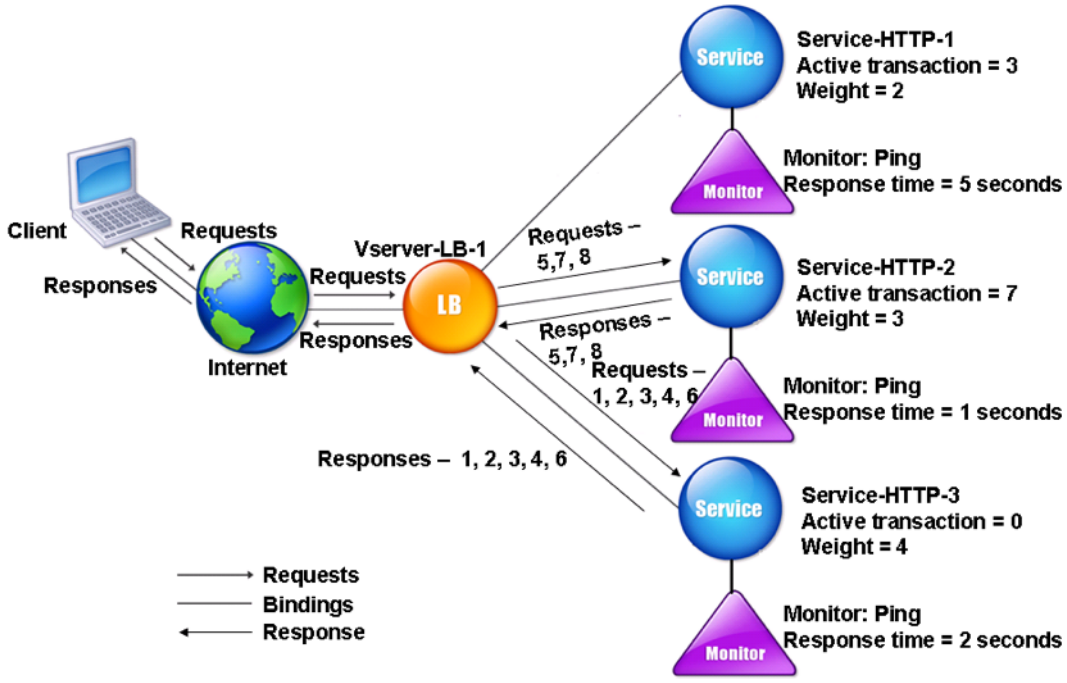
Die Citrix ADC Appliance führt außerdem Lastenausgleich durch, indem die Anzahl der aktiven Transaktionen, die Antwortzeit und Gewichtungen verwendet wird, wenn Dienste unterschiedliche Gewichtungen zugewiesen werden. Die Citrix ADC Appliance wählt den Dienst mithilfe des Wertes (Nw) im folgenden Ausdruck aus:

Nw = (N) * (10000/Gewicht)

Wobei N = (Anzahl der aktiven Transaktionen * Antwortzeit, die vom Monitor bestimmt wird)

Das folgende Diagramm veranschaulicht, wie der virtuelle Server die LRTM-Methode verwendet, wenn Gewichtungen zugewiesen werden.

Abbildung 2. Funktionsweise der Load Balancing-Methode für die geringste Antwortzeit bei Zuweisung von Gewichten



In diesem Beispiel wird Service-http-1 eine Gewichtung von 2 zugewiesen, Service-http-2 wird eine Gewichtung von 3 zugewiesen und Service-http-3 wird die Gewichtung 4 zugewiesen.

Die Citrix ADC Appliance stellt Anforderungen wie folgt bereit:

- Service-HTTP-3 empfängt die erste Anforderung, da es keine aktiven Transaktionen verarbeitet.
- Service-http-3 empfängt die zweite, dritte, vierte und fünfte Anforderung, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-2 empfängt die sechste Anforderung, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-http-3 empfängt die siebte Anforderung, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-2 empfängt die achten Anforderungen, da dieser Dienst den niedrigsten Nw-Wert hat.

Service-HTTP-1 hat das niedrigste Gewicht und den höchsten Nw-Wert. Daher wählt die Citrix ADC Appliance sie nicht für den Lastausgleich aus.

Die folgende Tabelle fasst zusammen, wie Nw für verschiedene Monitore berechnet wird.

Anfrage erhalten	Ausgewählter Service	Aktueller Nw-Wert (N) * (10000/Gewicht)	Bemerkungen
Request-1	Service-HTTP-3; (Nw = 0)	Nw= 5000	Service-http-3 hat den niedrigsten Nw-Wert.
Request-2	Dienst-HTTP-3; (Nw = 5000	Nw= 10000	Service-http-3 hat den niedrigsten Nw-Wert.
Request-3	Service-HTTP-3; (Nw = 10000)	Nw= 15000	Service-http-3 hat den niedrigsten Nw-Wert.
Request-4	Service-HTTP-3; (Nw = 15000)	Nw= 20000	Service-http-3 hat den niedrigsten Nw-Wert.
Request-5	Service-HTTP-3; (Nw = 20000)	Nw= 25000	Service-http-3 hat den niedrigsten Nw-Wert.
Request-6	Dienst-HTTP-2; (Nw = 23333,34)	Nw = 26666,67	Service-HTTP-2 hat den niedrigsten Nw-Wert.
Request-7	Service-HTTP-3; (Nw = 25000)	Nw = 30000	Service-http-3 hat den niedrigsten Nw-Wert.
Request-8	Dienst-HTTP-2; (Nw = 26666,67)	Nw= 30000	Service-HTTP-2 hat den niedrigsten Nw-Wert.

Service-HTTP-1 wird für den Lastenausgleich ausgewählt, wenn er seine aktiven Transaktionen abschließt oder wenn sein Nw-Wert kleiner ist als andere Dienste (Service-http-2 und Service-http-3).

So konfigurieren Sie die LRTM-Load Balancing-Methode mit der CLI

Geben Sie an der Eingabeaufforderung ein;

```
set lb vserver <name> [-lbMethod <lbMethod>]
<!--NeedCopy-->
```


Beispiel:

```
set lb vserver Vserver-LB-1 -lbMethod LRTM
<!--NeedCopy-->
```

So konfigurieren Sie die LRTM-Load Balancing-Methode mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter Erweiterte Einstellungen **LRTM**aus.

So aktivieren Sie die LRTM-Option in Monitoren mit der CLI

Geben Sie an der Eingabeaufforderung ein;

```
set lb monitor <monitorName> <type> [-LRTM ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Beispiel:

```
set lb monitor monitor-HTTP-1 HTTP -LRTM ENABLED
<!--NeedCopy-->
```

So aktivieren Sie die LRTM-Option in Monitoren mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Monitore**, und öffnen Sie einen Monitor.
2. Wählen Sie unter Erweiterte Parameter die Option **LRTM (Least Reaktionszeit using Monitoring)**aus.

Weitere Informationen zum Konfigurieren von Monitoren finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

Hashing-Methoden

October 5, 2021

Load Balancing-Methoden, die auf Hashes bestimmter Verbindungsinformationen oder Header-Informationen basieren, stellen die meisten Load Balancing-Methoden der Citrix ADC Appliance dar. Hashes sind kürzer und einfacher zu verwenden als die Informationen, auf denen sie basieren, während genügend Informationen beibehalten werden, um sicherzustellen, dass keine zwei verschiedenen Informationsstücke denselben Hash generieren und daher miteinander verwechselt werden.

Sie können die Hashing-Load Balancing-Methoden in einer Umgebung verwenden, in der ein Cache eine breite Palette von Inhalten aus dem Internet oder bestimmten Ursprungsservern bereitstellt. Caching-Anforderungen reduzieren die Anforderungs- und Antwortlatenz und gewährleistet eine bessere Ressourcenauslastung (CPU), wodurch das Caching auf stark genutzten Websites und Anwendungsservern populär wird. Da diese Sites auch vom Lastenausgleich profitieren, sind Hashing-Load Balancing-Methoden sehr nützlich.

Die Citrix ADC Appliance stellt die folgenden Hashmethoden bereit:

- URL-Hash-Methode
- Domänen-Hash-Methode
- Ziel-IP-Hash-Methode
- Quell-IP-Hash-Methode
- Quell-IP-Ziel-IP-Hash-Methode
- Quell-IP-Quellport-Hash-Methode
- Call ID-Hash-Methode
- Token-Methode

Die meisten Hashing-Algorithmen berechnen zwei Hash-Werte:

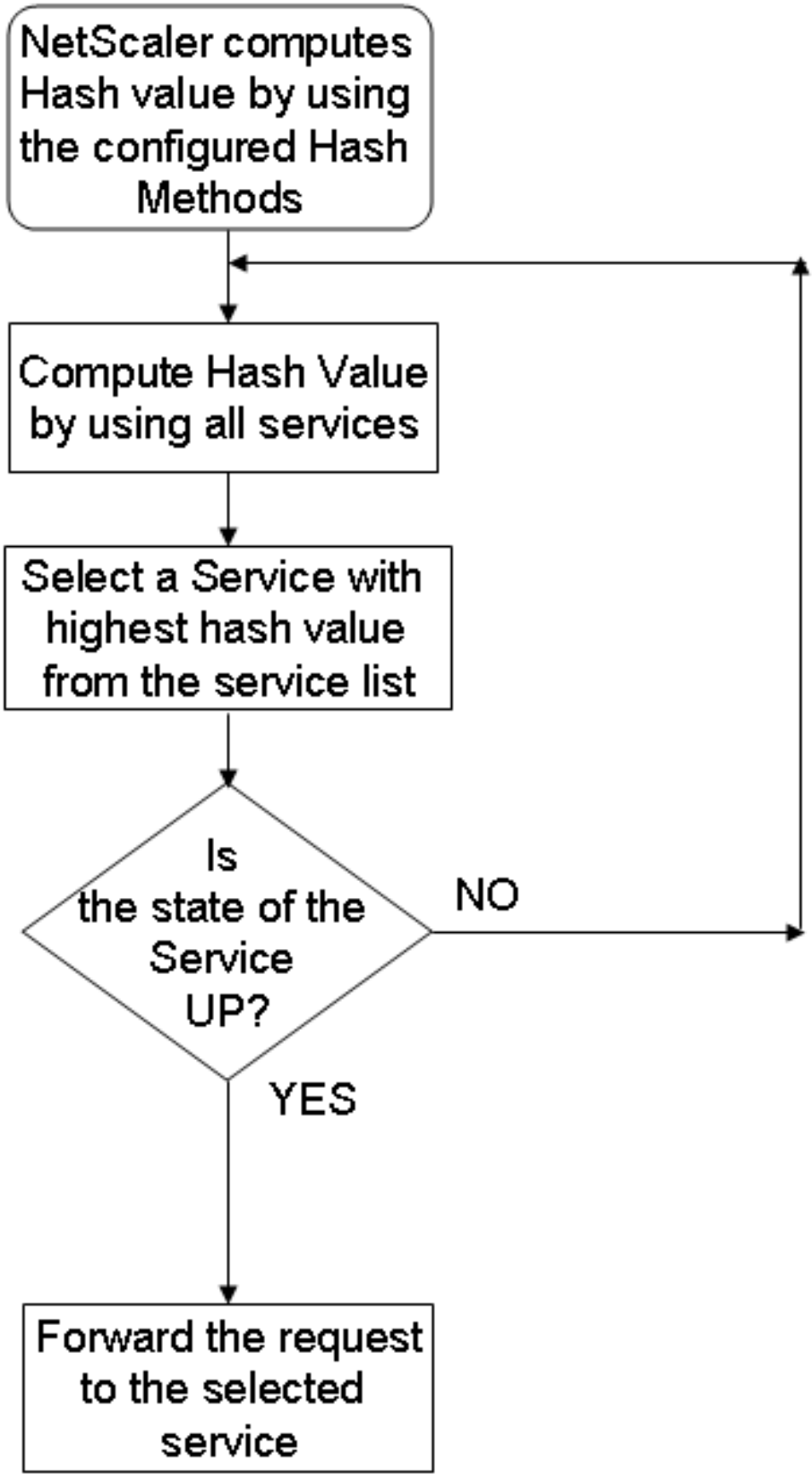
- Ein Hash der IP-Adresse und des Ports des Dienstes.
- Ein Hash der eingehenden URL, des Domänennamens, der Quell-IP-Adresse, der Ziel-IP-Adresse oder der Quell- und Ziel-IP-Adressen, abhängig von der konfigurierten Hash-Methode.

Die Citrix ADC Appliance generiert dann einen neuen Hash-Wert, indem beide Hash-Werte verwendet werden. Schließlich leitet es die Anforderung an den Dienst mit dem höchsten Hashwert weiter. Da die Appliance für jede Anforderung einen Hashwert berechnet und den Dienst auswählt, der die Anforderung verarbeitet, füllt sie einen Cache. Nachfolgende Anforderungen mit demselben Hash-Wert werden an denselben Dienst gesendet. Das folgende Flussdiagramm veranschaulicht diesen Prozess.

> Hinweis:
>
> Ab Citrix ADC Release 13.0 Build 79.x werden konsistente Hashing-Algorithmen von Prime Re-Shuffled Assisted CARP (PRAC) und Jump Table Assisted Ring Hash (JARH) unterstützt. Die konsistenten Hashing-Algorithmen sorgen für minimale Unterbrechungen, wenn Dienste zu Ihrem Load Balancing-Setup oder während eines Service Flap-Ereignisses im Load Balancing-Setup hinzugefügt oder aus diesem gelöscht werden. Weitere Informationen finden Sie unter Konsis-

> tente Hashing-Algorithmen.

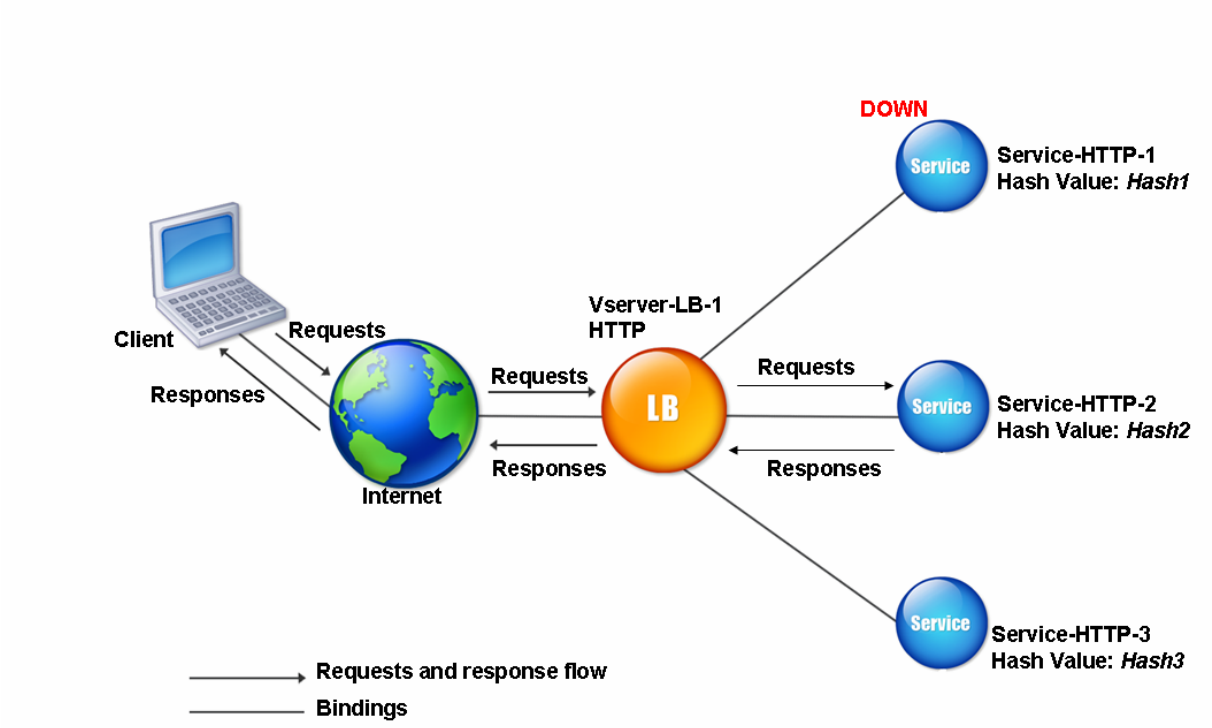
Abbildung 1. Wie die Hashing-Methoden Anforderungen verteilen



Hashing-Methoden können auf IPv4- und IPv6-Adressen angewendet werden.

Betrachten Sie ein Szenario, in dem drei Dienste (service-http-1, service-http-2 und service-http-3) an einen virtuellen Server gebunden sind, eine beliebige Hash-Methode konfiguriert ist und der Hash-Wert Hash1 lautet. Wenn die konfigurierten Dienste UP sind, wird die Anforderung an Service-HTTP-1 gesendet. Wenn Service-HTTP-1 heruntergefahren ist, berechnet die Citrix ADC Appliance den Hash-Wert für das letzte Protokoll der Anzahl der Dienste. Anschließend wählt die Appliance den Dienst mit dem höchsten Hash-Wert aus, z. B. Service-HTTP-2. Das folgende Diagramm veranschaulicht diesen Vorgang.

Abbildung 2. Entitätsmodell für Hashing-Methoden



> Hinweis:
>
> Wenn die Citrix ADC Appliance einen Dienst nicht mithilfe einer Hashing-Methode auswählen kann, wird standardmäßig die kleinste Verbindungsmethode verwendet, um einen Dienst für die eingehende Anforderung auszuwählen. Passen Sie Server-Pools an, indem Sie Dienste in Zeiten mit geringem Datenverkehr entfernen, damit die Caches neu aufgefüllt werden können, ohne die Leistung Ihres Lastenausgleichs-Setups zu beeinträchtigen.

Konsistente Hashing-Algorithmen

Die konsistenten Hashing-Algorithmen werden verwendet, um zustandslos Persistenz zu erreichen. Die hashbasierten LB-Methoden verwenden einen der folgenden drei konsistenten Hashing-Algorithmen:

- **Cache-Array-Routing-Protokoll (CARP)**

  Der CARP-Algorithmus wird zum Lastenausgleich von HTTP-Anfragen auf mehreren Proxy-Cache-Servern verwendet. Dieser Algorithmus ist standardmäßig aktiviert.

- **Prime Re-Shuffled Assisted CARP (PRAC)**

  Die Citrix ADC Appliance verwendet den proprietären PRAC-Algorithmus, um eine einheitliche Verkehrsverteilung bereitzustellen.

- **Sprungtisch Assisted Ring Hash (JARH)**

  Die Citrix ADC Appliance verwendet den proprietären JARH-Algorithmus, um eine Konsistenz und einheitliche Verteilung des Datenverkehrs zu gewährleisten. Dieser Algorithmus verwendet Hash-Finger. Eine höhere Anzahl von Finger sorgt für eine bessere Verkehrsverteilung. Die Erhöhung der Anzahl der Finger erhöht jedoch auch die Speicherauslastung.

So wählen Sie den konsistenten Hashing-Algorithmus mit CLI aus

```
set lb parameter [-lbHashAlgorithm [DEFAULT|JARH|PRAC] [-lbHashFingers
   <positive_integer>]
<!--NeedCopy-->
```

Beispiel:

```
set lb parameter -lbHashAlgorithm JARH -lbHashFingers 10
<!--NeedCopy-->
```

ARGUMENTE:

- **lbhashalgorithm**-Geben Sie den Hashing-Algorithmus an, der für die folgenden Hash-basierten Load Balancing-Methoden verwendet werden soll:
  - URL-Hash-Methode
  - Domänen-Hash-Methode
  - Ziel-IP-Hash-Methode
  - Quell-IP-Hash-Methode
  - Quell-IP-Ziel-IP-Hash-Methode
  - Quell-IP-Quellport-Hash-Methode
  - Call ID-Hash-Methode
  - Token-Methode

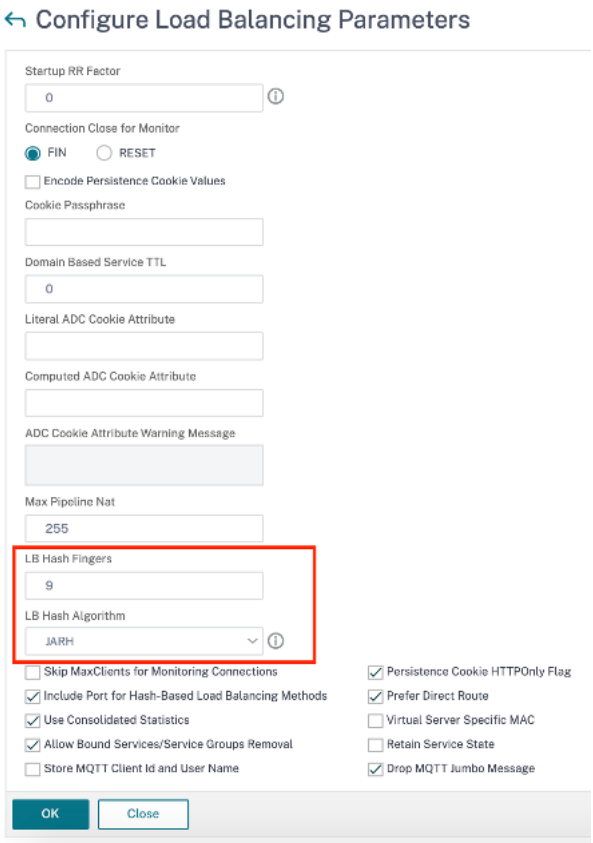
  Mögliche Werte: DEFAULT, PRAC, JARH
  Standardwert: DEFAULT

- **lbHashFingers**-Geben Sie die Anzahl der Finger an, die in PRAC- und JARH-Algorithmen für hashbasierte LB-Methoden verwendet werden sollen. Die Erhöhung der Anzahl der Finger ermöglicht eine bessere Verteilung des Datenverkehrs auf Kosten des zusätzlichen Speichers.

  Standardwert: 256
  Minimaler Wert: 1
  Maximaler Wert: 1024

So wählen Sie den konsistenten Hashing-Algorithmus mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Load Balancing-Parameter ändern**.
2. Geben **Sie im Bereich Load Balancing-Parameter konfigurieren** die entsprechenden Werte für die folgenden Felder ein, basierend auf Ihrer Anforderung:
   - LB Hash Finger
   - Wählen Sie im Feld **LB Hash Algorithm** den konsistenten Hashing-Algorithmus aus dem Dropdownmenü aus.



Die URL-Hash-Methode

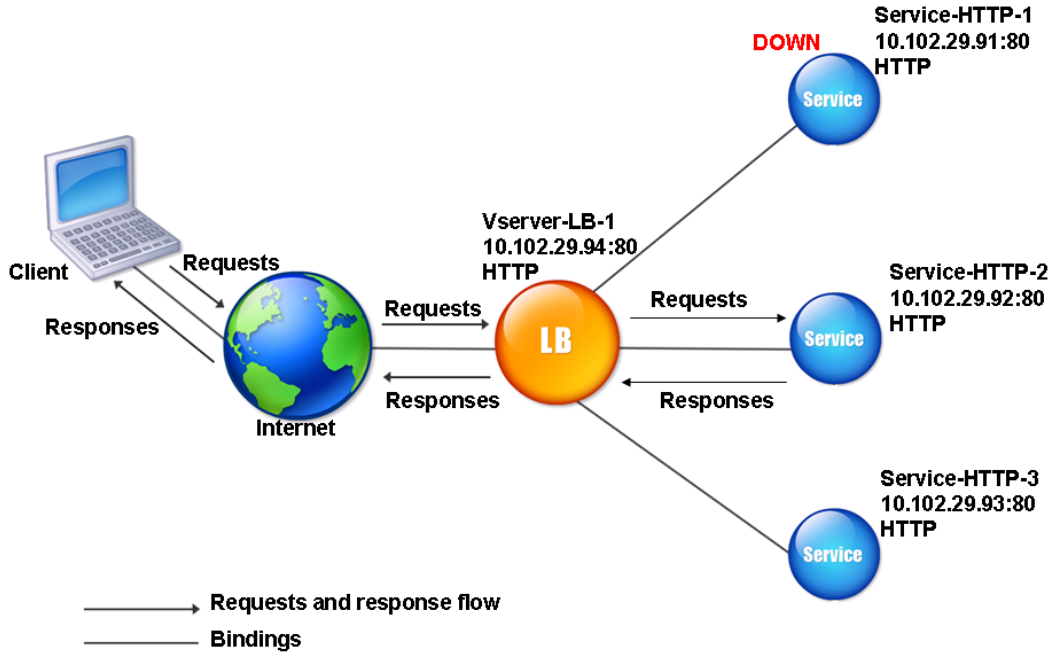
Wenn Sie die Citrix ADC Appliance so konfigurieren, dass die URL-Hash-Methode für den Lastenausgleich der Dienste verwendet wird, generiert die Appliance einen Hashwert der HTTP-URL, die in der eingehenden Anforderung vorhanden ist. Wenn der durch den Hash-Wert ausgewählte Dienst DOWN ist, verfügt der Algorithmus über eine Methode, um einen anderen Dienst aus der Liste der aktiven Dienste auszuwählen. Die Appliance speichert den Hashwert der URL, und wenn sie nachfolgende Anforderungen empfängt, die dieselbe URL verwenden, leitet sie sie an denselben Dienst weiter. Wenn die Appliance eine eingehende Anforderung nicht analysieren kann, verwendet sie die Roundrobin-Methode für den Lastenausgleich anstelle der URL-Hash-Methode.

Zum Generieren des Hash-Werts verwendet die Appliance einen bestimmten Algorithmus und berücksichtigt einen Teil der URL. Standardmäßig berücksichtigt die Appliance die ersten 80 Bytes der URL. Wenn die URL kleiner als 80 Bytes ist, wird die vollständige URL verwendet. Sie können eine andere Länge angeben. Die Hash-Länge kann zwischen 1 Byte und 4096 Byte liegen. Wenn lange URLs verwendet werden, bei denen nur wenige Zeichen unterschiedlich sind, empfiehlt es sich, die Hash-Länge so hoch wie möglich zu gestalten, um eine gleichmäßigere Lastverteilung sicherzustellen.

Betrachten Sie ein Szenario, in dem drei Dienste, service-http-1, service-http-2 und service-http-3, an einen virtuellen Server gebunden sind und die auf dem virtuellen Server konfigurierte Lastausgleichsmethode die URL-Hash-Methode ist. Der virtuelle Server erhält eine Anforderung und der Hashwert der URL ist U1. Appliance wählt Service-HTTP-1 aus. Wenn Service-HTTP-1 auf DOWN festgelegt ist, wählt die Appliance Service-HTTP-2 aus.

Das folgende Diagramm veranschaulicht diesen Vorgang.

Abbildung 3. Funktionsweise von URL-Hashing



Wenn sowohl Service-HTTP-1 als auch Service-HTTP-2 DOWN sind, sendet die Appliance Anfragen mit dem Hashwert U1 an Service-HTTP-3.

Wenn Service-HTTP-1 und Service-HTTP-2 ausgefallen sind, werden Anforderungen, die den Hash-URL1 generieren, an Service-HTTP-3 gesendet. Wenn diese Dienste UP sind, werden die Anfragen, die den Hash-URL1 erzeugen, auf folgende Weise verteilt:

- Wenn der Service-HTTP-2 hochgeladen ist, wird die Anforderung an Service-HTTP-2 gesendet.
- Wenn der Service-HTTP-1 hochgeladen ist, wird die Anforderung an Service-HTTP-1 gesendet.
- Wenn Service-HTTP-1 und Service-HTTP-2 gleichzeitig hochgeladen sind, wird die Anforderung an Service-HTTP-1 gesendet.

Informationen zum Konfigurieren der URL-Hash-Methode finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält. Wählen Sie die Load Balancing-Methode als URL-Hash aus, und legen Sie die Hashlänge auf die Anzahl der Bytes fest, die zum Generieren des Hash-Werts verwendet werden sollen.

Die Domain-Hash-Methode

Ein virtueller Lastausgleichsserver, der für die Verwendung der Domänen-Hash-Methode konfiguriert ist, verwendet den Hashwert des Domänennamens in der HTTP-Anforderung, um einen Dienst

auszuwählen. Der Domänenname wird entweder von der eingehenden URL oder vom Host-Header der HTTP-Anforderung übernommen. Wenn der Domänenname sowohl in der URL als auch im Host-Header angezeigt wird, bevorzugt die Appliance die URL.

Wenn Sie Domänennamen-Hashing konfigurieren und eine eingehende HTTP-Anforderung keinen Domänennamen enthält, verwendet die Citrix ADC Appliance standardmäßig die Roundrobin-Methode für diese Anforderung.

Die Hash-Wert-Berechnung verwendet die Namenslänge oder den Hashlängenwert, je nachdem, welcher Wert kleiner ist. Standardmäßig berechnet die Citrix ADC Appliance den Hash-Wert aus den ersten 80 Byte des Domänennamens. Um bei der Berechnung des Hash-Werts eine andere Anzahl von Bytes im Domänennamen anzugeben, können Sie den Parameter hashlength (HashLength im Konfigurationsdienstprogramm) auf einen Wert von 1 bis 4096 (Byte) festlegen.

Informationen zum Konfigurieren der Domänen-Hash-Methode finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Die Ziel-IP-Hash-Methode

Ein virtueller Lastausgleichsserver, der für die Verwendung der Ziel-IP-Hash-Methode konfiguriert ist, verwendet den Hashwert der Ziel-IP-Adresse, um einen Server auszuwählen. Sie können die Ziel-IP-Adresse maskieren, um anzugeben, welcher Teil davon in der Hashwertberechnung verwendet werden soll, sodass Anforderungen, die aus verschiedenen Netzwerken stammen, aber für dasselbe Subnetz bestimmt sind, an denselben Server weitergeleitet werden. Diese Methode unterstützt IPv4- und IPv6-basierte Zielserver.

Diese Load Balancing-Methode ist für die Verwendung mit der Cache-Umleitungsfunktion geeignet.

Um die Ziel-IP-Hash-Methode für einen IPv4-Zielserver zu konfigurieren, legen Sie den NetMask-Parameter fest. Um diese Methode für einen IPv6-Zielserver zu konfigurieren, verwenden Sie den V6NetMasklen-Parameter. Im Konfigurationsdienstprogramm werden Textfelder zum Festlegen dieser Parameter angezeigt, wenn Sie die **Ziel-IP-Hash-Methode**auswählen.

Informationen zum Konfigurieren der Ziel-IP-Hash-Methode finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Die Quell-IP-Hash-Methode

Ein virtueller Lastausgleichsserver, der für die Verwendung der Quell-IP-Hash-Methode konfiguriert ist, verwendet den Hashwert der Client-IPv4- oder IPv6-Adresse, um einen Dienst auszuwählen. Um alle Anforderungen von Quell-IP-Adressen, die zu einem bestimmten Netzwerk gehören, an einen bestimmten Zielserver zu leiten, müssen Sie die Quell-IP-Adresse maskieren. Verwenden Sie für IPv4-Adressen den NetMask -Parameter. Verwenden Sie für IPv6-Adressen den Parameter v6NetMaskLength.

Informationen zum Konfigurieren der Quell-IP-Hash-Methode finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Die IP-Hash-Methode des Quell-IP-Ziels

Ein virtueller Lastausgleichsserver, der für die Verwendung der Quell-IP-Ziel-Hash-Methode konfiguriert ist, verwendet den Hashwert der Quell- und Ziel-IP-Adressen (IPv4 oder IPv6), um einen Dienst auszuwählen. Hashing ist symmetrisch. Der Hashwert ist unabhängig von der Reihenfolge der Quell- und Ziel-IPs gleich. Dadurch wird sichergestellt, dass alle Pakete, die von einem bestimmten Client zum selben Ziel fließen, an denselben Server weitergeleitet werden.

Um alle Anforderungen, die zu einem bestimmten Netzwerk gehören, an einen bestimmten Zielserver zu leiten, müssen Sie die Quell-IP-Adresse maskieren. Verwenden Sie für IPv4-Adressen den NetMask -Parameter. Verwenden Sie für IPv6-Adressen den Parameter v6NetMaskLength.

Informationen zum Konfigurieren der IP-Ziel-IP-Hash-Methode des Quell-IP-Ziels finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Die Quell-IP-Quellport-Hash-Methode

Ein virtueller Lastausgleichsserver, der für die Verwendung der Hash-Methode des Quell-IP-Quellports konfiguriert ist, verwendet den Hashwert der Quell-IP (entweder IPv4 oder IPv6) und des Quellports, um einen Dienst auszuwählen. Dadurch wird sichergestellt, dass alle Pakete auf einer bestimmten Verbindung an denselben Dienst weitergeleitet werden.

Diese Methode wird bei der Verbindungsspiegelung und beim Lastenausgleich der Firewall verwendet. Weitere Informationen zur Verbindungsspiegelung finden Sie unter Verbindungs-Failover.

Um alle Anforderungen, die zu einem bestimmten Netzwerk gehören, an einen bestimmten Zielserver zu leiten, müssen Sie die Quell-IP-Adresse maskieren. Verwenden Sie für IPv4-Adressen den NetMask -Parameter. Verwenden Sie für IPv6-Adressen den Parameter v6NetMaskLength.

Informationen zum Konfigurieren der Hash-Methode für Quell-IP-Quellport finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Die Call-ID-Hash-Methode

Ein virtueller Lastausgleichsserver, der für die Verwendung der Call-ID-Hash-Methode konfiguriert ist, verwendet den Hash-Wert der Call-ID im SIP-Header, um einen Dienst auszuwählen. Pakete für eine bestimmte SIP-Sitzung werden daher immer an denselben Proxyserver weitergeleitet.

Diese Methode ist für den SIP-Lastenausgleich anwendbar. Weitere Informationen zum SIP-Lastenausgleich finden Sie unter Überwachen von SIP-Diensten.

Informationen zum Konfigurieren der Call-ID-Hash-Methode finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Methode der geringsten Bandbreite

October 5, 2021

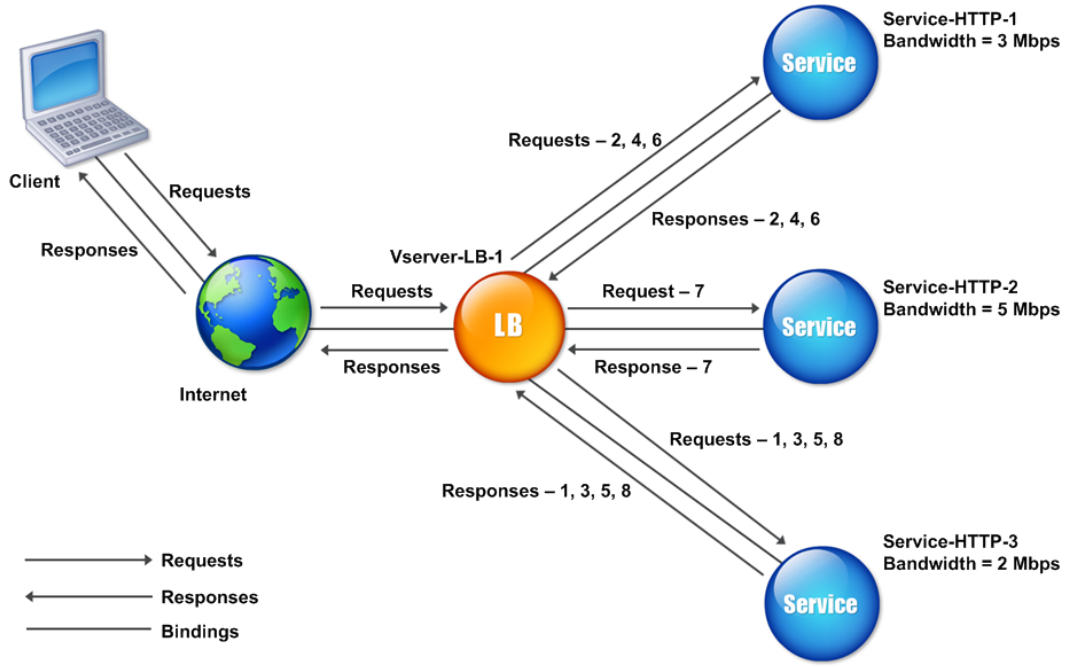
Ein virtueller Lastausgleichsserver, der für die Verwendung der Methode der geringsten Bandbreite konfiguriert ist, wählt den Dienst aus, der derzeit den geringsten Datenverkehr bereitstellt, gemessen in Megabit pro Sekunde (Mbit/s). Das folgende Beispiel zeigt, wie der virtuelle Server einen Dienst für den Lastenausgleich mithilfe der Methode der geringsten Bandbreite auswählt.

Betrachten Sie drei Dienste, Service-Http-1, Service-Http-2 und Service-Http-3.

- Service-HTTP-1 hat 3 Mbit/s Bandbreite.
- Service-HTTP-2 verfügt über eine Bandbreite von 5 Mbit/s.
- Service-HTTP-3 hat 2 Mbit/s Bandbreite.

Das folgende Diagramm veranschaulicht, wie der virtuelle Server die Methode der geringsten Bandbreite verwendet, um Anforderungen an die drei Dienste weiterzuleiten.

Abbildung 1. Funktionsweise der Load Balancing-Methode der geringsten Bandbreite



Der virtuelle Server wählt den Dienst mithilfe des Bandbreitenwerts (N) aus. Dies ist die Summe der Anzahl der Bytes, die in den letzten 14 Sekunden übertragen und empfangen wurden. Wenn jede Anforderung eine Bandbreite von 1 Mbit/s erfordert, sendet die Citrix ADC Appliance Anforderungen wie folgt:

- Service-HTTP-3 empfängt die erste Anforderung, da dieser Dienst den niedrigsten N-Wert hat.
- Da Service-HTTP-1 und Service-HTTP-3 jetzt denselben N-Wert haben, wechselt der virtuelle Server abwechselnd zwischen ihnen zur Round-Robin-Methode für diese Server. Service-http-1 empfängt die zweite Anforderung, Service-http-3 erhält die dritte Anforderung, Service-http-1 erhält die vierte Anforderung, Service-http-3 erhält die fünfte Anforderung und Service-http-1 erhält die sechste Anforderung.
- Da Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3 jetzt alle denselben N-Wert haben, enthält der virtuelle Server Service-HTTP-2 in die Round-Robin-Liste. Daher erhält Service-http-2 die siebte Anforderung, Service-http-3 erhält die achte Anforderung usw.

Die folgende Tabelle fasst zusammen, wie N berechnet wird.

Anfrage erhalten	Ausgewählter Service	Aktueller N-Wert	Bemerkungen
Request-1	Service-HTTP-3; (N = 2)	N = 3	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-2	Service-HTTP-1; (N = 3)	N = 4	Service-http-1 und Service-http-3 haben die gleichen N-Werte.
Request-3	Service-HTTP-3; (N = 3)	N = 4	Service-http-1 und Service-http-3 haben die gleichen N-Werte.
Request-4	Service-HTTP-1; (N = 4)	N = 5	-
Request-5	Dienst-HTTP-3; (N = 4)	N = 5	-
Request-6	Service-HTTP-1; (N = 5)	N = 6	Service-http-1, service-http-2 und service-http-3 haben die gleichen N-Werte.
Request-7	Dienst-HTTP-2; (N = 5)	N = 6	Service-http-1, service-http-2 und service-http-3 haben die gleichen N-Werte.
Request-8	Service-HTTP-3; (N = 5)	N = 6	-

Hinweis: Wenn Sie die RTSP-NAT-Option auf dem virtuellen Server aktivieren, verwendet die Citrix ADC Appliance die Anzahl der ausgetauschten Daten und Kontrollbytes, um die Bandbreitenauslastung für RTSP-Dienste zu bestimmen. Weitere Informationen zur RTSP-NAT-Option finden Sie unter RTSP-Verbindungen verwalten.

Die Citrix ADC Appliance führt außerdem Lastenausgleich durch, indem Bandbreite und Gewichte verwendet werden, wenn den Diensten unterschiedliche Gewichtungen zugewiesen werden. Es wählt einen Dienst mithilfe des Wertes (Nw) im folgenden Ausdruck aus:

Nw = (N) * (10000/Gewicht)

Wie im vorangegangenen Beispiel wird Service-http-1 eine Gewichtung von 2 zugewiesen, Service-http-2 wird eine Gewichtung von 3 zugewiesen und Service-http-3 wird eine Gewichtung von 4 zugewiesen. Die Citrix ADC Appliance stellt Anforderungen wie folgt bereit:

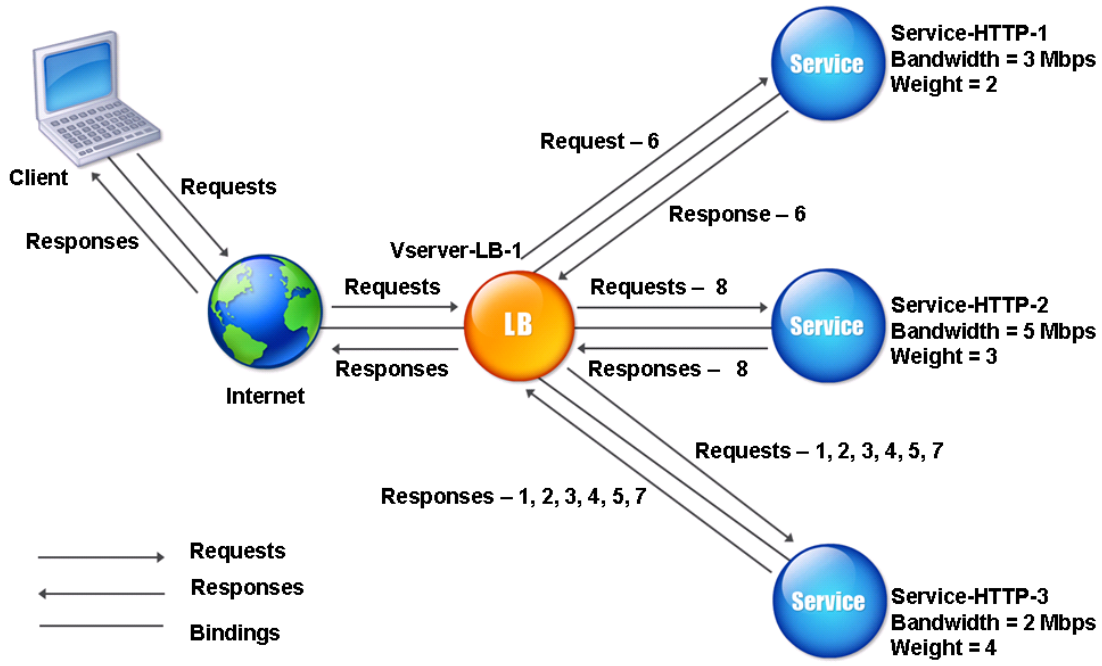
- Service-http-3 empfängt die erste zweite, dritte, vierte und fünfte Anforderung, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-1 empfängt die sechste Anforderung, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-http-3 empfängt die siebte Anforderung, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-2 empfängt die achte Anforderung, da dieser Dienst den niedrigsten Nw-Wert hat.

Die folgende Tabelle fasst zusammen, wie Nw berechnet wird.

Anfrage erhalten	Ausgewählter Service	Aktueller Nw-Wert (Anzahl der aktiven Transaktionen) * (10000/Gewicht)	Bemerkungen
Request-1	Dienst-HTTP-3; (Nw = 5000)	Nw= 5000	Service-http-3 hat den niedrigsten Nw-Wert.
Request-2	Dienst-HTTP-3; (Nw = 5000)	Nw= 7500	-
Request-3	Service-HTTP-3; (Nw = 7500)	Nw= 10000	-
Request-4	Service-HTTP-3; (Nw = 10000)	Nw= 12500	-
Request-5	Service-HTTP-3; (Nw = 12500)	Nw= 15000	-
Request-6	Service-HTTP-1; (Nw = 15000)	Nw= 20000	Service-http-1 und Service-http-3 haben den gleichen Nw-Wert.
Request-7	Service-HTTP-3; (Nw = 15000)	Nw= 17500	Service-http-1 und Service-http-3 haben den gleichen Nw-Wert.
Request-8	Dienst-HTTP-2; (Nw = 16666,67)	Nw= 20000	Service-HTTP-2 hat den niedrigsten Nw-Wert.

Das folgende Diagramm veranschaulicht, wie der virtuelle Server die Methode mit der geringsten Bandbreite verwendet, wenn den Diensten Gewichtungen zugewiesen werden.

Abbildung 2. Funktionsweise der Load Balancing-Methode mit der geringsten Bandbreite bei Zuweisung von Gewichten



Informationen zum Konfigurieren der Methode mit der geringsten Bandbreite finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Methode der kleinsten Pakete

October 5, 2021

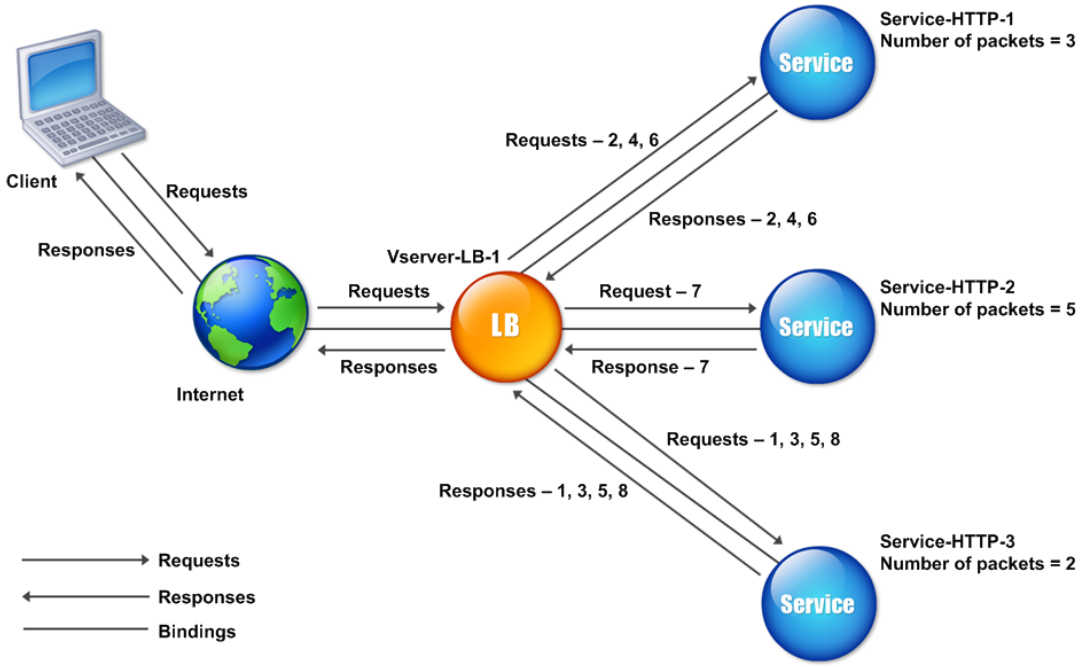
Ein virtueller Lastausgleichsserver, der für die Verwendung der Methode am wenigsten Pakete konfiguriert ist, wählt den Dienst aus, der die wenigsten Pakete in den letzten 14 Sekunden empfangen hat.

Betrachten Sie beispielsweise drei Dienste, Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3.

- Service-HTTP-1 hat in den letzten 14 Sekunden drei Pakete bearbeitet.
- Service-HTTP-2 hat in den letzten 14 Sekunden fünf Pakete verarbeitet.
- Service-HTTP-3 hat in den letzten 14 Sekunden zwei Pakete bearbeitet.

Das folgende Diagramm veranschaulicht, wie die Citrix ADC Appliance für jede empfangene Anforderung die Methode der wenigsten Pakete verwendet, um einen Dienst auszuwählen.

Abbildung 1. Funktionsweise der Load Balancing-Methode Lost Packets



Die Citrix ADC Appliance wählt einen Dienst aus, indem die Anzahl der Pakete (N) verwendet wird, die von jedem Dienst in den letzten 14 Sekunden übertragen und empfangen wurden. Mit dieser Methode liefert es Anforderungen wie folgt:

- Service-HTTP-3 empfängt die erste Anforderung, da dieser Dienst den niedrigsten N-Wert hat.
- Da Service-http-1 und Service-http-3 jetzt denselben N-Wert haben, wechselt der virtuelle Server zur Roundrobin-Methode. Service-http-1 erhält daher die zweite Anforderung, Service-http-3 erhält die dritte Anforderung, Service-http-1 erhält die vierte Anforderung, Service-http-3 erhält die fünfte Anforderung und Service-http-1 erhält die sechste Anforderung.
- Da Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3 jetzt alle den gleichen N-Wert haben, wechselt der virtuelle Server auch zur Round-Robin-Methode für Service-HTTP-2, einschließlich dieser in der Round-Robin-Liste. Daher erhält Service-http-2 die siebte Anforderung, Service-http-3 erhält die achte Anforderung usw.

Die folgende Tabelle fasst zusammen, wie N berechnet wird.

Anfrage erhalten	Ausgewählter Service	Aktueller N-Wert	Bemerkungen
Request-1	Service-HTTP-3; (N = 2)	N = 3	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-2	Service-HTTP-1; (N = 3)	N = 4	Service-http-1 und Service-http-3 haben die gleichen N-Werte.
Request-3	Service-HTTP-3; (N = 3)	N = 4	Service-http-1 und Service-http-3 haben die gleichen N-Werte.
Request-4	Service-HTTP-1; (N = 4)	N = 5	-
Request-5	Dienst-HTTP-3; (N = 4)	N = 5	-
Request-6	Service-HTTP-1; (N = 5)	N = 6	Service-http-1, service-http-2 und service-http-3 haben die gleichen N-Werte.
Request-7	Dienst-HTTP-2; (N = 5)	N = 6	Service-http-1, service-http-2 und service-http-3 haben die gleichen N-Werte.
Request-8	Service-HTTP-3; (N = 5)	N = 6	-

Hinweis: Wenn Sie die Option RTSP NAT auf dem virtuellen Server aktivieren, berechnet die Appliance die Anzahl der Daten- und Steuerpakete, um die Anzahl der Pakete für RTSP-Dienste zu berechnen. Weitere Informationen zur RTSP-NAT-Option finden Sie unter RTSP-Verbindungen verwalten.

Die Citrix ADC Appliance führt außerdem Lastenausgleich durch, indem die Anzahl der Pakete und Gewichte verwendet wird, wenn jedem Dienst ein anderes Gewicht zugewiesen wird. Es wählt einen Dienst mithilfe des Wertes (Nw) im folgenden Ausdruck aus:

Nw = (N) * (10000/Gewicht)

Wie im vorangegangenen Beispiel wird Service-http-1 eine Gewichtung von 2 zugewiesen, Service-http-2 wird eine Gewichtung von 3 zugewiesen und Service-http-3 wird eine Gewichtung von 4 zugewiesen. Die Citrix ADC Appliance stellt Anforderungen wie folgt bereit:

- Service-http-3 empfängt die erste zweite, dritte, vierte und fünfte Anforderung, da dieser Dienst

den niedrigsten Nw-Wert hat.

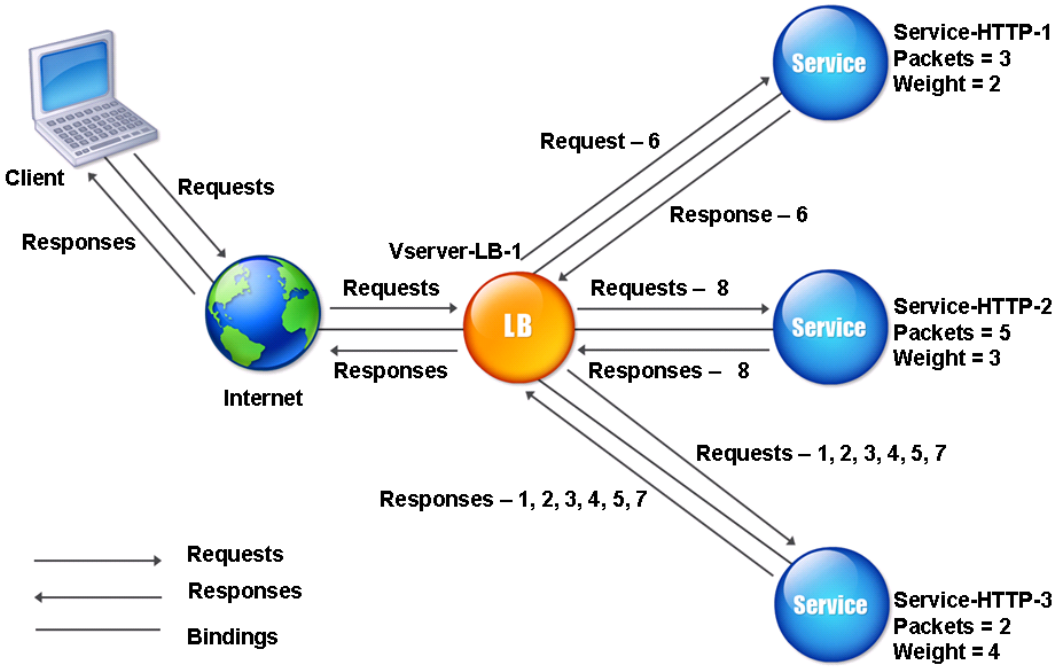
- Service-HTTP-1 empfängt die sechste Anforderung, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-http-3 empfängt die siebte Anforderung, da dieser Dienst den niedrigsten Nw-Wert hat.
- Service-HTTP-2 empfängt die achte Anforderung, da dieser Dienst den niedrigsten Nw-Wert hat.

Die folgende Tabelle fasst zusammen, wie Nw berechnet wird.

Anfrage erhalten	Ausgewählter Service	Aktueller Nw-Wert (Anzahl der aktiven Transaktionen) * (10000/Gewicht)	Bemerkungen
Request-1	Dienst-HTTP-3; (Nw = 5000)	Nw= 5000	Service-http-3 hat den niedrigsten Nw-Wert.
Request-2	Dienst-HTTP-3; (Nw = 5000)	Nw= 7500	-
Request-3	Service-HTTP-3; (Nw = 7500)	Nw= 10000	-
Request-4	Service-HTTP-3; (Nw = 10000)	Nw= 12500	-
Request-5	Service-HTTP-3; (Nw = 12500)	Nw= 15000	-
Request-6	Service-HTTP-1; (Nw = 15000)	Nw= 20000	Service-http-1 und Service-http-3 haben den gleichen Nw-Wert.
Request-7	Service-HTTP-3; (Nw = 15000)	Nw= 17500	Service-http-1 und Service-http-3 haben den gleichen Nw-Wert.
Request-8	Dienst-HTTP-2; (Nw = 16666,67)	Nw= 20000	Service-HTTP-2 hat den niedrigsten Nw-Wert.

Das folgende Diagramm veranschaulicht, wie der virtuelle Server bei der Zuweisung von Gewichtungen die Methode der wenigsten Pakete verwendet.

Abbildung 2. Funktionsweise der Methode Kleinste Pakete, wenn Gewichte zugewiesen werden



Informationen zum Konfigurieren der Methode der kleinsten Pakete finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

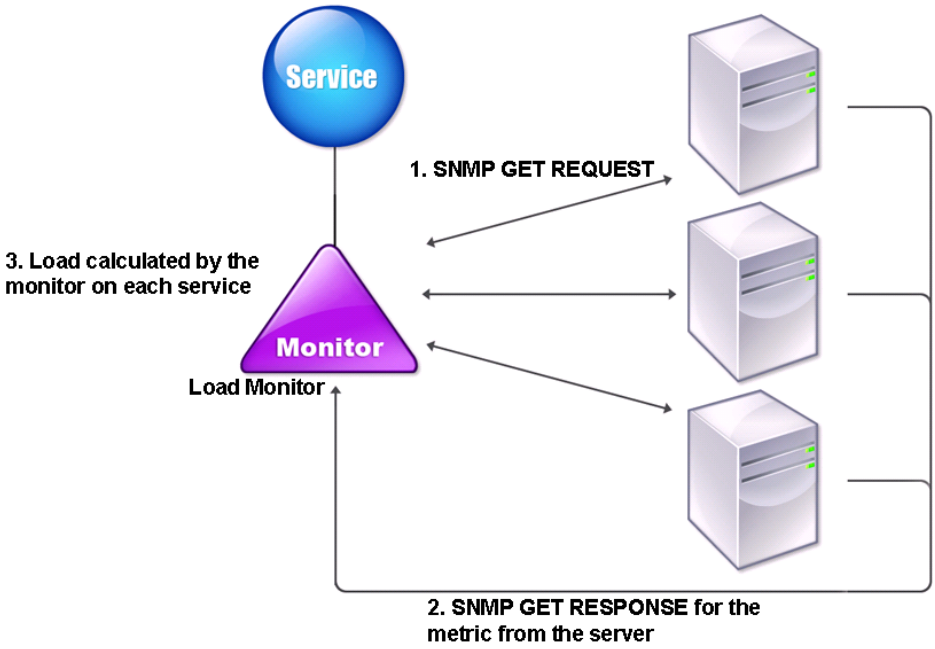
Benutzerdefinierte Lademethode

October 5, 2021

Benutzerdefinierter Lastenausgleich wird für Serverparameter wie CPU-Auslastung, Arbeitsspeicher und Antwortzeit durchgeführt. Bei Verwendung der benutzerdefinierten Lademethode wählt die Citrix ADC Appliance normalerweise einen Dienst aus, der keine aktiven Transaktionen verarbeitet. Wenn alle Dienste im Load Balancing-Setup aktive Transaktionen verarbeiten, wählt die Appliance den Service mit der kleinsten Last aus. Ein spezieller Monitortyp, der als Lastmonitor bezeichnet wird, berechnet die Last für jeden Dienst im Netzwerk. Die Lastüberwachungen markieren nicht den Status eines Dienstes, aber sie nehmen Dienste aus der Lastausgleichsentscheidung heraus, wenn diese Dienste nicht UP sind.

Weitere Informationen zu Lastmonitoren finden Sie unter Grundlegendes zu Lastmonitoren. Das folgende Diagramm veranschaulicht, wie ein Lastmonitor funktioniert.

Abbildung 1. Funktionsweise von Lastmonitoren



Der Lastmonitor berechnet mithilfe von SNMP-Sonden die Belastung jedes Dienstes, indem er eine SNMP GET-Anfrage an den Dienst sendet. Diese Anforderung enthält eine oder mehrere Objekt-IDs (OIDs). Der Dienst antwortet mit einer SNMP-GET-Antwort mit Metriken, die den SNMP-OIDs entsprechen. Der Lastmonitor berechnet anhand der Antwortmetriken die Belastung des Dienstes.

Der Lastmonitor berechnet die Last auf einem Dienst mithilfe der folgenden Parameter:

- Metrikwerte, die über SNMP-Prüfpunkte abgerufen werden, die als Tabellen in der Citrix ADC Appliance vorhanden sind.
- Schwellenwert für jede Metrik festgelegt.
- Gewicht, das jeder Metrik zugewiesen wird.

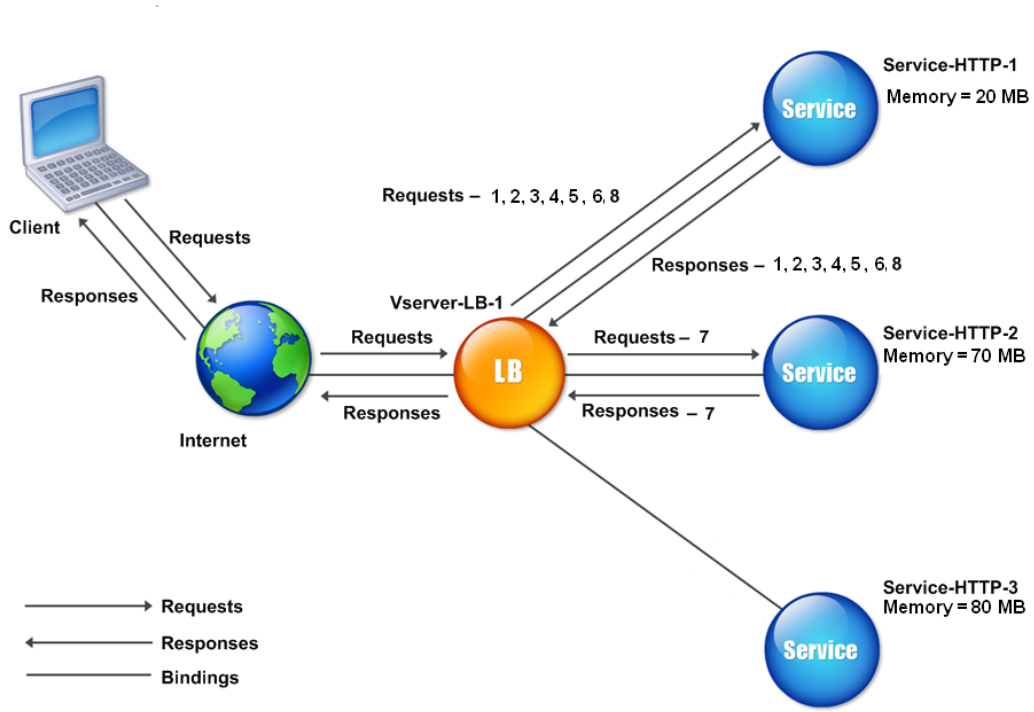
Betrachten Sie beispielsweise drei Dienste, Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3.

- Service-HTTP-1 verwendet 20 MB Speicher.
- Service-HTTP-2 verwendet 70 MB Arbeitsspeicher.
- Service-HTTP-3 verwendet 80 MB Arbeitsspeicher.

Die Server mit Lastausgleich können Metriken wie CPU- und Speicherauslastung in die Dienste exportieren, was sie wiederum dem Lastmonitor zur Verfügung stellen kann. Der Lastmonitor sendet eine SNMP-GET-Anforderung mit den OIDs 1.3.6.1.4.1.5951.4.1.1.41.1.5, 1.3.6.1.4.1.5951.4.1.1.41.1.4 und

1.3.6.1.4.1.5951.4.1.1.41.1.3 an die Dienste. SNMP-OIDs vom Typ STRING werden nicht unterstützt, da Sie die Last nicht mithilfe einer STRING OID berechnen können. Lasten können mit anderen Datentypen wie INT und Gauge32 berechnet werden. Die drei Dienste beantworten die Anfrage. Die Citrix ADC Appliance vergleicht die exportierten Metriken und wählt dann Service-HTTP-1 aus, da mehr Speicher verfügbar ist. Das folgende Diagramm veranschaulicht diesen Vorgang.

Abbildung 2. Funktionsweise der benutzerdefinierten Lademethode



Wenn jede Anforderung 10 MB Arbeitsspeicher verwendet, sendet die Citrix ADC Appliance Anforderungen wie folgt:

- Service-HTTP-1 empfängt die erste, zweite, dritte, vierte und fünfte Anforderung, da dieser Dienst den niedrigsten N-Wert hat.
- Service-HTTP-1 und Service-HTTP-2 haben jetzt die gleiche Last, so dass der virtuelle Server auf die Roundrobin-Methode für diese Server zurückkehrt. Daher erhält Service-HTTP-2 die sechste Anforderung, und Service-HTTP-1 empfängt die siebte Anforderung.
- Da Service-HTTP-1, Service-HTTP-2 und Service-HTTP-3 jetzt alle dieselbe Last haben, kehrt der virtuelle Server auch auf die Round-Robin-Methode für Service-HTTP-3 zurück. Daher erhält Service-HTTP-3 die achte Anforderung.

Die folgende Tabelle fasst zusammen, wie N berechnet wird.

Anfrage erhalten	Service ausgewählt	Aktueller N-Wert (Anzahl der aktiven Transaktionen)	Bemerkungen
Request-1	Service-HTTP-1; (N = 20)	N = 30	Service-HTTP-3 hat den niedrigsten N-Wert.
Request-2	Dienst-HTTP-1; (N = 30)	N = 40	-
Request-3	Service-HTTP-1; (N = 40)	N = 50	-
Request-4	Service-HTTP-1; (N = 50)	N = 60	-
Request-5	Dienst-HTTP-1; (N = 60)	N = 70	-
Request-6	Dienst-HTTP-1; (N = 70)	N = 80	Service-HTTP-2 und Service-HTTP-3 haben die gleichen N-Werte.
Request-7	Dienst-HTTP-2; (N = 70)	N = 80	Service-HTTP-3 haben die gleichen N-Werte.
Request-8	Service-HTTP-1; (N = 80)	N = 90	Service-http-1, service-http-2 und service-http-3 haben die gleichen N-Werte.

Wenn den Diensten unterschiedliche Gewichtungen zugewiesen werden, berücksichtigt der benutzerdefinierte Lastalgorithmus sowohl die Last für jeden Dienst als auch das Gewicht, das jedem Service zugewiesen ist. Es wählt einen Dienst mithilfe des Wertes (Nw) im folgenden Ausdruck aus:

Nw = (N) * (10000/Gewicht)

Wie im vorangegangenen Beispiel wird Service-http-1 eine Gewichtung von 4 zugewiesen, Service-http-2 wird eine Gewichtung von 3 zugewiesen und Service-http-3 wird eine Gewichtung von 2 zugewiesen. Wenn jede Anforderung 10 MB Arbeitsspeicher verwendet, sendet die Citrix ADC Appliance Anforderungen wie folgt:

- Service-http-1 empfängt die erste, zweite, dritte, vierte, fünfte, sechste, siebte und achte Anforderungen, da dieser Dienst den niedrigsten Nw-Wert hat.

- Service-HTTP-2 empfängt die neunte Anforderung, da dieser Dienst den niedrigsten Nw-Wert hat.

Service-HTTP-3 hat den höchsten Nw-Wert und wird daher nicht für den Lastausgleich berücksichtigt.

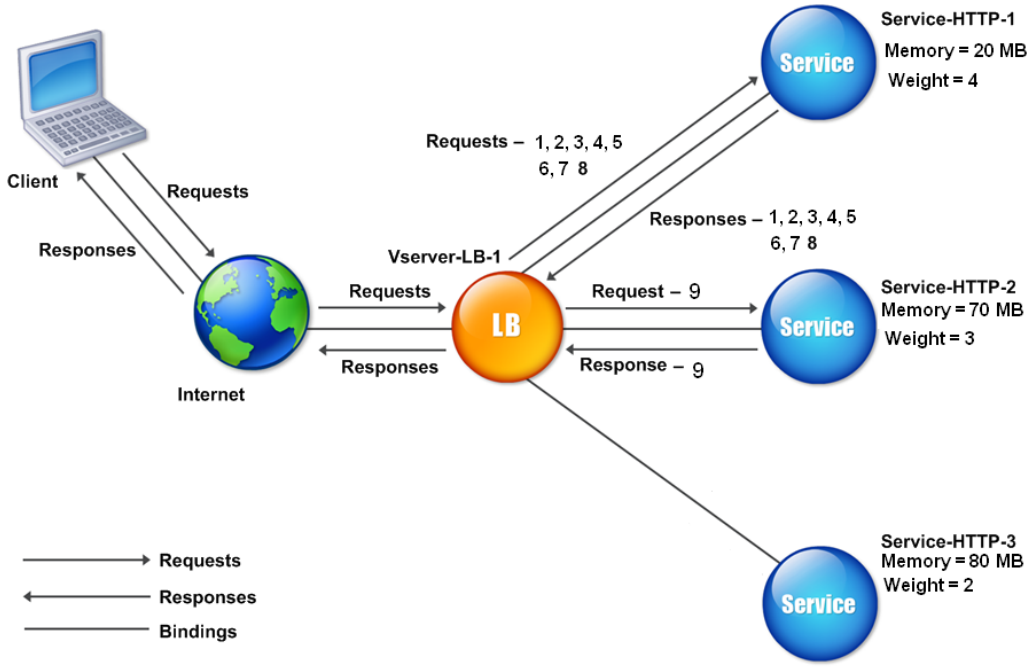
Die folgende Tabelle fasst zusammen, wie Nw berechnet wird.

Anfrage erhalten	Service ausgewählt	Aktueller Nw-Wert (Anzahl der aktiven Transaktionen) * (10000/Gewicht)	Bemerkungen
Request-1	Service-HTTP-1; (Nw = 50000)	Nw = 75000	Service-HTTP-1 hat den niedrigsten Nw-Wert.
Request-2	Dienst-HTTP-1; (Nw = 5000)	Nw = 100000	-
Request-3	Service-HTTP-1; (Nw = 15000)	Nw = 125000	-
Request-4	Service-HTTP-1; (Nw = 20000)	Nw = 150000	-
Request-5	Service-HTTP-1; (Nw = 23333,34)	Nw = 175000	-
Request-6	Service-HTTP-1; (Nw = 25000)	Nw = 200000	-
Request-7	Service-HTTP-1; (Nw = 23333,34)	Nw = 225000	-
request-8	service-http-1; (Nw = 25000)	Nw = 250000	-
request-9	service-http-2; (Nw = 233333,34)	Nw = 266666.67	Service-http-2 hat den niedrigsten Nw-Wert.

Service-HTTP-1 wird für den Lastenausgleich ausgewählt, wenn er seine aktiven Transaktionen abschließt oder wenn der Nw-Wert anderer Dienste (Service-HTTP-2 und Service-HTTP-3) 400.000 beträgt.

Das folgende Diagramm veranschaulicht, wie die Citrix ADC Appliance die benutzerdefinierte Lademethode verwendet, wenn Gewichtungen zugewiesen werden.

Abbildung 3. Funktionsweise der benutzerdefinierten Lademethode beim Zuweisen von Gewichten



Informationen zum Konfigurieren der benutzerdefinierten Lademethode finden Sie unter Konfigurieren einer Load Balancing-Methode, die keine Richtlinie enthält.

Statische Näherungsmethode

October 5, 2021

Wenn ein virtueller Server für die Verwendung der statischen Näherungsmethode konfiguriert ist, wählt er den Dienst aus, der den Näherungskriterien am besten entspricht.

Damit die statische Näherungsmethode funktioniert, müssen Sie entweder die Citrix ADC Appliance so konfigurieren, dass eine vorhandene statische Näherungsdatenbank verwendet wird, die über eine Standortdatei aufgefüllt wird, oder benutzerdefinierte Einträge zur statischen Näherungsdatenbank hinzufügen. Nachdem Sie benutzerdefinierte Einträge hinzugefügt haben, können Sie deren Standortqualifizierer festlegen. Nachdem Sie die Datenbank konfiguriert haben, können Sie die statische

Nähe als Load Balancing-Methode angeben.

Weitere Details finden Sie in den folgenden Themen.

- Hinzufügen einer Standortdatei zum Erstellen einer statischen Näherungsdatenbank
- Hinzufügen von benutzerdefinierten Einträgen zu einer statischen Näherungsdatenbank
- Festlegen der Standortbezeichner
- Festlegen der statischen Proximity-Methode

Angeben der Proximity-Methode

Wenn Sie die statische Näherungsdatenbank konfiguriert haben, können Sie die statische Nähe als GLSB-Methode angeben.

So legen Sie die statische Nähe mit der Befehlszeilenschnittstelle fest

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

```
set lb vserver <name> -lbMethod STATICPROXIMITY

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

Beispiel:

```
set lb vserver Vserver-LB-1 -lbMethod STATICPROXIMITY

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

So legen Sie die statische Nähe mit der GUI fest

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und wählen Sie den virtuellen Server aus.
2. Klicken Sie auf **Bearbeiten**, und erweitern Sie den Abschnitt **Methode**.
3. Wählen Sie in der Liste **Load Balancing Method** die Option **STATICPROXIMITY** aus.

Token-Methode

October 5, 2021

Ein virtueller Lastausgleichsserver, der für die Verwendung der Token-Methode konfiguriert ist, basiert seine Auswahl eines Dienstes auf dem Wert eines Datensegments, das aus der Clientanforderung extrahiert wurde. Das Datensegment wird Token genannt. Sie konfigurieren den Speicherort und die Größe des Tokens. Für nachfolgende Anforderungen mit demselben Token wählt der virtuelle Server denselben Dienst aus, der die ursprüngliche Anforderung verarbeitet hat.

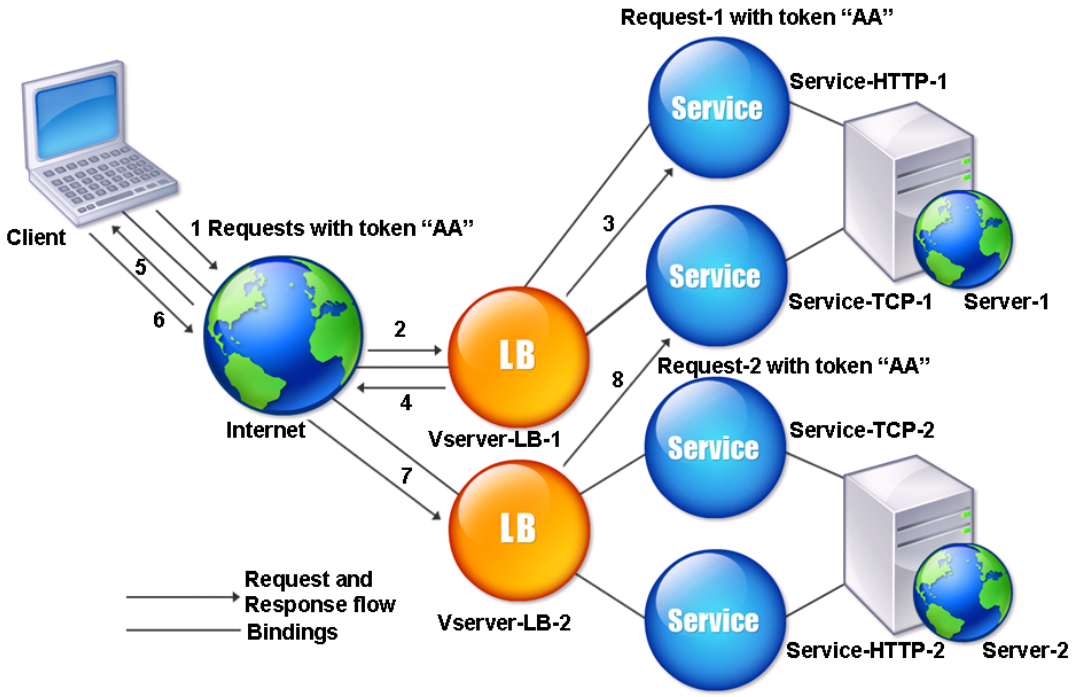
Diese Methode ist inhaltsbewusst. Es funktioniert unterschiedlich für TCP-, HTTP- und HTTPS-Verbindungen. Bei HTTP- oder HTTPS-Diensten befindet sich das Token in den HTTP-Headern, der URL oder im BODY. Um das Token zu finden, geben oder erstellen Sie einen klassischen oder erweiterten Ausdruck. Weitere Informationen zu klassischen oder erweiterten Ausdrücken finden Sie unter Richtlinienkonfiguration und Referenz.

Bei HTTP-Diensten sucht der virtuelle Server nach dem konfigurierten Token in den ersten 24 Kilobyte (KB) der TCP-Nutzlast. Bei Nicht-HTTP-Diensten (TCP, SSL und SSL_TCP) sucht der virtuelle Server nach dem konfigurierten Token in den ersten 16 Paketen, wenn die Gesamtgröße der 16 Pakete weniger als 24 KB beträgt. Wenn die Gesamtgröße der 16 Pakete jedoch größer als 24 KB ist, sucht die Appliance in den ersten 24 KB Nutzlast nach dem Token. Sie können diese Lastenausgleichsmethode über virtuelle Server verschiedener Typen hinweg verwenden, um sicherzustellen, dass Anforderungen, die dasselbe Token darstellen, unabhängig vom verwendeten Protokoll an die entsprechenden Dienste weitergeleitet werden.

Betrachten Sie beispielsweise ein Lastausgleichs-Setup, das aus Servern besteht, die Webinhalte enthalten. Sie möchten die Citrix ADC Appliance so konfigurieren, dass sie im URL-Abfragebereich der Anforderung nach einer bestimmten Zeichenfolge (dem Token) sucht. Server-1 verfügt über zwei Dienste, Service-HTTP-1 und Service-TCP-1, und Server-2 hat zwei Dienste, Service-HTTP-2 und Service-TCP-2. Die TCP-Dienste sind an vServer-LB-2 gebunden, und die HTTP-Dienste sind an vServer-LB-1 gebunden.

Wenn vServer-LB-1 eine Anforderung mit dem Token AA empfängt, wählt er den Service Service-HTTP-1 (gebunden an server-1), um die Anforderung zu verarbeiten. Wenn vServer-LB-2 eine andere Anforderung mit demselben Token (AA) empfängt, leitet es diese Anforderung an den Dienstdienst-TCP-1 weiter. Das folgende Diagramm veranschaulicht diesen Vorgang.

Abbildung 1. Funktionsweise der Token-Methode



So konfigurieren Sie die Token-Load Balancing-Methode mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Token-Load-Balancing-Methode zu konfigurieren und die Konfiguration zu überprüfen:

```
set lb vserver <name> -lbMethod TOKEN -rule <rule> -datalength <length>
    -dataoffset <offset>

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

Beispiel:

```
set lb vserver LB-VServer-1 -lbMethod TOKEN -rule 'AA' -datalength 2 -
   dataoffset 25

```



```
show lb vserver LB-VServer-1
<!--NeedCopy-->
```

So konfigurieren Sie die Token-Load-Balancing-Methode mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Klicken Sie unter Erweiterte Einstellungen auf Methode
3. Wählen Sie in der Liste Load Balancing Method die Option Token aus, und geben Sie einen Ausdruck an.

Konfigurieren einer Lastausgleichsmethode, die keine Richtlinie enthält

October 5, 2021

Nachdem Sie einen Lastausgleichsalgorithmus für das Lastausgleichs-Setup ausgewählt haben, müssen Sie die Citrix ADC Appliance so konfigurieren, dass dieser Algorithmus verwendet wird. Sie können es mit der Befehlszeilenschnittstelle oder mit dem Konfigurationsdienstprogramm konfigurieren.

Hinweis:

Die Token-Methode ist richtlinienbasiert und erfordert mehr Konfiguration als hier beschrieben. Informationen zum Konfigurieren der Token-Methode finden Sie unter Token-Methode.

Bei einigen hash-basierten Methoden können Sie eine IP-Adresse maskieren, um Anforderungen zu demselben Subnetz an denselben Server zu leiten. Weitere Informationen finden Sie unter Hashing-Methoden.

So legen Sie die Load Balancing-Methode mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -lbMethod <method>
<!--NeedCopy-->
```

Beispiel:


```
set lb vserver Vserver-LB-1 -lbMethod LeastConnection
<!--NeedCopy-->
```

So legen Sie die Load Balancing-Methode mit dem Konfigurationsdienstprogramm fest

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Klicken Sie unter Erweiterte Einstellungen auf **Methode**, und wählen Sie in der Liste Load Balancing Method eine Methode aus.

Persistenz und persistente Verbindungen

September 28, 2022

Ein zustandsloses Lastenausgleichsprotokoll wie HTTP unterbricht die Pflege von Statusinformationen über Clientverbindungen, wenn die Persistenz nicht konfiguriert ist. Verschiedene Übertragungen desselben Clients können an verschiedene Server weitergeleitet werden, obwohl alle Übertragungen Teil derselben Sitzung sind. Sie können die Persistenz auf einem virtuellen Lastenausgleichsserver konfigurieren, der bestimmte Arten von Webanwendungen wie Einkaufswagen-Anwendungen verarbeitet.

Bevor Sie Persistenz konfigurieren können, müssen Sie die verschiedenen Arten von Persistenz verstehen, wie sie verwendet werden und welche Auswirkungen sie haben. Anschließend müssen Sie die Citrix ADC Appliance so konfigurieren, dass sie dauerhafte Verbindungen für die Websites und Webanwendungen bereitstellt, die sie benötigen.

Sie können auch die Backup-Persistenz konfigurieren, die wirksam wird, wenn der primäre Persistenztyp, der für einen virtuellen Lastausgleichsserver konfiguriert ist, fehlschlägt. Sie können Persistenzgruppen so konfigurieren, dass eine Clientübertragung an einen beliebigen virtuellen Server in einer Gruppe an einen Server weitergeleitet werden kann, der frühere Übertragungen vom selben Client empfangen hat.

Informationen zur Persistenz beim RADIUS-Lastenausgleich finden Sie unter Konfigurieren des RADIUS-Lastenausgleichs mit Persistenz.

Über Persistence

October 5, 2021

Sie können zwischen verschiedenen Arten von Persistenz für einen bestimmten virtuellen Lastenausgleichsserver wählen, der dann alle Verbindungen vom selben Benutzer an Ihre Einkaufswagenanwendung, webbasierte E-Mail oder andere Netzwerkanwendung an denselben Dienst weiterleitet. Die Persistenzsitzung bleibt für die von Ihnen angegebene Zeit in Kraft.

Wenn ein an einer Persistenzsitzung teilnehmender Server heruntergefahren wird, verwendet der virtuelle Lastausgleichsserver die konfigurierte Lastenausgleichsmethode, um einen neuen Dienst auszuwählen, und richtet eine neue Persistenzsitzung mit dem von diesem Dienst vertretenen Server ein. Wenn der Server OUT OF SERVICE wechselt, verarbeitet er weiterhin bestehende Persistenzsitzungen, aber der virtuelle Server leitet keinen neuen Datenverkehr an ihn weiter. Nach Ablauf des Herunterfahrenzeitraums hört der virtuelle Server auf, Verbindungen von vorhandenen Clients zum Dienst zu leiten, vorhandene Verbindungen zu schließen und diese Clients bei Bedarf an neue Dienste weiterzuleiten.

Abhängig vom konfigurierten Persistenztyp kann die Citrix ADC Appliance die Quell-IPs, Ziel-IPs, SSL-Sitzungs-IDs, Host- oder URL-Header oder eine Kombination dieser Elemente untersuchen, um jede Verbindung in der richtigen Persistenzsitzung zu platzieren. Es kann auch die Persistenz auf einem Cookie basieren, das vom Webserver ausgegeben wird, auf einem willkürlich zugewiesenen Token oder auf einer logischen Regel. Fast alles, was es der Appliance ermöglicht, Verbindungen mit der richtigen Persistenzsitzung abzugleichen, und wird als Grundlage für Persistenz verwendet.

In der folgenden Tabelle werden die Persistenztypen zusammengefasst, die auf der Citrix ADC Appliance verfügbar sind.

Persistenz-Typ	Beschreibung
Quell-IP	SOURCEIP. Verbindungen von derselben Client-IP-Adresse sind Teile derselben Persistenzsitzung.
HTTP-Cookie	COOKIEINSERT. Verbindungen, die denselben HTTP-Cookie-Header haben, sind Teile derselben Persistenzsitzung.
SSL Session ID	SSLSESSION. Verbindungen, die dieselbe SSL-Sitzungs-ID haben, sind Teile derselben Persistenzsitzung.
URL Passive	URLPASSIVE. Verbindungen mit derselben URL werden als Teile derselben Persistenzsitzung behandelt.
Benutzerdefinierte Server-ID	CUSTOMSERVERID. Verbindungen mit demselben HTTP-HOST-Header werden als Teile derselben Persistenzsitzung behandelt.

Persistenz-Typ	Beschreibung
Ziel-IP	DESTIP. Verbindungen mit derselben Ziel-IP werden als Teile derselben Persistenzsitzung behandelt.
Quell- und Ziel-IPs	SRCIPDESTIP. Verbindungen, die sowohl von derselben Quell-IP als auch von derselben Ziel-IP stammen, werden als Teile derselben Persistenzsitzung behandelt.
SIP-Anruf-ID	CALLID. Verbindungen, die dieselbe Aufruf-ID im SIP-Header haben, werden als Teile derselben Persistenzsitzung behandelt.
RTSP Sitzungs-ID	RTSPSID. Verbindungen, die dieselbe RTSP-Sitzungs-ID haben, werden als Teile derselben Persistenzsitzung behandelt.
Benutzerdefinierte Regel	RULE. Verbindungen, die einer benutzerdefinierten Regel entsprechen, werden als Teile derselben Persistenzsitzung behandelt.

Tabelle 1. Arten der Persistenz

Je nach Typ der Persistenz, die Sie konfiguriert haben, kann der virtuelle Server entweder 250.000 gleichzeitige persistente Verbindungen oder eine beliebige Anzahl persistenter Verbindungen unterstützen, bis zu den Grenzen, die durch die Menge an RAM auf Ihrer Citrix ADC Appliance auferlegt werden. Die folgende Tabelle zeigt, welche Persistenzarten in jede Kategorie fallen.

Persistenz-Typ	Anzahl der gleichzeitig unterstützten persistenten Verbindungen
Quell-IP, SSL-Sitzungs-ID, Regel, Ziel-IP, Quell-IP/Ziel-IP, SIP-Anruf-ID, RTSP Sitzungs-ID	250 K
Cookie, URL-Server-ID, Benutzerdefinierte Server-ID	Speicherbegrenzung. Wenn in CookieInsert ein Timeout nicht 0 ist, wird die Anzahl der Verbindungen durch den Speicher begrenzt.

Tabelle 2. Unterstützte Persistenztypen und Anzahl gleichzeitiger Verbindungen

Einige Persistenzarten sind spezifisch für bestimmte Arten von virtuellen Servern. In der folgenden

Tabelle werden die einzelnen Persistenztypen aufgelistet und angegeben, welche Persistenzarten auf welchen Arten von virtuellen Servern unterstützt werden.

Persistenz-Typ	HTTP	HTTPS	TCP	UDP/IP	SSL_Bridge	SSL_TCP	RTSP	SIP_UDP
SOURCEI	JA	JA	JA	JA	JA	JA	NEIN	NEIN
COOKIEINSERT	JA	JA	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN
SSLSESS	NEIN	JA	NEIN	NEIN	JA	JA	NEIN	NEIN
URLPASSIVE	JA	JA	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN
CUSTOM	JA	JA	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN
RULE	JA	JA	JA	NEIN	NEIN		NEIN	NEIN
SRCIPDE	JA	JA	JA	JA	JA	JA	NEIN	NEIN
DESTIP	JA	JA	JA	JA	JA	JA	NEIN	NEIN
CALLID	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	JA
RTSPID	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	JA	NEIN

Tabelle 3. Beziehung des Persistenztyps zum virtuellen Servertyp

Quell-IP-Adresse Persistenz

October 5, 2021

Wenn die Quell-IP-Persistenz konfiguriert ist, verwendet der virtuelle Lastausgleichsserver die konfigurierte Lastausgleichsmethode, um einen Dienst für die anfängliche Anforderung auszuwählen, und verwendet dann die Quell-IP-Adresse (Client-IP-Adresse), um nachfolgende Anforderungen von diesem Client zu identifizieren und sie an denselben Dienst zu senden. Sie können einen Timeoutwert festlegen, der den maximalen Inaktivitätszeitraum für die Sitzung angibt. Wenn der Timeout-Wert abläuft, wird die Sitzung verworfen, und der konfigurierte Lastausgleichsalgorithmus wird verwendet, um einen neuen Server auszuwählen.

Achtung: Unter bestimmten Umständen kann die Verwendung von Persistenz basierend auf Quell-IP-Adresse Ihre Server überlasten. Alle Anfragen an eine einzelne Website oder Anwendung werden über das einzelne Gateway zur Citrix ADC Appliance weitergeleitet, obwohl sie dann an mehrere Standorte umgeleitet werden. In mehreren Proxy-Umgebungen haben Clientanfragen häufig unterschiedliche Quell-IP-Adressen, selbst wenn sie vom selben Client gesendet werden, was zu einer schnellen Multiplikation von Persistenzsitzungen führt, in denen eine einzelne Sitzung erstellt werden muss. Dieses

Problem wird als Mega Proxy Problem bezeichnet. Sie können HTTP-Cookie-basierte Persistenz anstelle der Quell-IP-basierten Persistenz verwenden, um dies zu verhindern.

Informationen zum Konfigurieren der Persistenz basierend auf der Quell-IP-Adresse finden Sie unter Konfigurieren von Persistenztypen, die keine Regel erfordern.

Hinweis: Wenn der gesamte eingehende Datenverkehr hinter einem NAT (Network Address Translation) -Gerät oder -Proxy stammt, scheint der Datenverkehr für die Citrix ADC Appliance von einer einzigen Quell-IP-Adresse zu stammen. Dadurch wird verhindert, dass die Quell-IP-Persistenz ordnungsgemäß funktioniert. In diesem Fall müssen Sie einen anderen Persistenztyp auswählen.

HTTP-Cookie-Persistenz

October 5, 2021

Wenn die Persistenz von HTTP-Cookies konfiguriert ist, setzt die Citrix ADC Appliance ein Cookie in den HTTP-Headern der anfänglichen Clientanforderung. Das Cookie enthält die IP-Adresse und den Port des vom Lastausgleichsalgorithmus ausgewählten Dienstes. Wie bei jeder HTTP-Verbindung schließt der Client dieses Cookie dann mit allen nachfolgenden Anfragen ein.

Wenn die Citrix ADC Appliance das Cookie erkennt, leitet sie die Anforderung an die Dienst-IP und den Port im Cookie weiter, wobei die Persistenz für die Verbindung beibehalten wird. Sie können diese Art der Persistenz mit virtuellen Servern vom Typ HTTP oder HTTPS verwenden. Dieser Persistenztyp verbraucht keine Appliance-Ressourcen und kann daher eine unbegrenzte Anzahl persistenter Clients aufnehmen.

Hinweis: Wenn der Webbrowser des Clients so konfiguriert ist, dass er Cookies ablehnt, funktioniert die auf HTTP-Cookie basierende Persistenz nicht. Es kann ratsam sein, einen Cookie-Check auf der Website zu konfigurieren und Kunden, die Cookies anscheinend nicht ordnungsgemäß speichern, zu warnen, dass sie Cookies für die Website aktivieren müssen, wenn sie sie verwenden möchten.

Das Cookie-Format, das von der Citrix ADC Appliance eingefügt wird, lautet:

```
NSC_XXXX=<ServiceIP ><ServicePort>
```

Wobei:

- NSC_XXXX ist die virtuelle Server-ID, die vom Namen des virtuellen Servers abgeleitet wird.
- ServiceIP und ServicePort sind codierte Darstellungen der Dienst-IP-Adresse bzw. des Dienstports. IP-Adresse und Port werden separat codiert.

Sie können einen Timeoutwert für diesen Persistenztyp festlegen, um einen Inaktivitätszeitraum für die Sitzung anzugeben. Wenn die Verbindung für den angegebenen Zeitraum inaktiv war, verwirft die Citrix ADC Appliance die Persistenzsitzung. Jede nachfolgende Verbindung von demselben

Client führt dazu, dass ein neuer Server basierend auf der konfigurierten Lastausgleichsmethode ausgewählt wird und eine neue Persistenzsitzung eingerichtet wird.

Hinweis: Wenn Sie den Timeoutwert auf 0 festlegen, gibt die Citrix ADC Appliance keine Ablaufzeit an, sondern legt ein Sitzungscookie fest, das nicht gespeichert wird, wenn der Browser des Clients heruntergefahren wird.

Standardmäßig setzt die Citrix ADC Appliance HTTP-Cookies der Version 0 für maximale Kompatibilität mit Client-Browsern. (Nur bestimmte HTTP-Proxys verstehen Cookies der Version 1; am häufigsten verwendete Browser nicht.) Sie können die Appliance so konfigurieren, dass HTTP-Cookies der Version 1 eingestellt werden, um die Einhaltung von RFC2109 zu gewährleisten. Bei HTTP-Cookies der Version 0 fügt die Appliance das Ablaufdatum und die Uhrzeit des Cookies als absolute koordinierte Weltzeit (GMT) ein. Er berechnet diesen Wert als Summe der aktuellen GMT-Zeit auf der Appliance und des Timeoutwerts. Bei HTTP-Cookies der Version 1 fügt die Appliance eine relative Ablaufzeit ein, indem sie das Attribut “Max-Age” des HTTP-Cookies setzt. In diesem Fall berechnet der Browser des Clients die tatsächliche Ablaufzeit.

Informationen zum Konfigurieren der Persistenz basierend auf einem von der Appliance eingefügten Cookie finden Sie unter Konfigurieren von Persistenztypen, die keine Regel erfordern.

Im HTTP-Cookie legt die Appliance standardmäßig das `HTTPOnly` Flag fest, um anzuzeigen, dass das Cookie nicht skriptfähig ist und der Clientanwendung nicht bekannt gegeben werden darf. Daher kann ein clientseitiges Skript nicht auf das Cookie zugreifen, und der Client ist nicht anfällig für siteübergreifende Skripterstellung.

Bestimmte Browser unterstützen das `HTTPOnly` Flag jedoch nicht und geben das Cookie daher möglicherweise nicht zurück. Infolgedessen ist die Beharrlichkeit gebrochen. Für Browser, die das Flag nicht unterstützen, können Sie das `HTTPOnly` Flag im Persistenz-Cookie weglassen.

So ändern Sie die `HTTPOnly` Flag-Einstellung mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb parameter -httpOnlyCookieFlag (ENABLED|DISABLED)
<!--NeedCopy-->
```

Beispiel:

```
>  set lb parameter -httpOnlyCookieFlag disabled
   Done
> show lb parameter
  Global LB parameters:
```



```
        Persistence Cookie HttpOnly Flag: DISABLED
        Use port for hash LB: YES
 Done
<!--NeedCopy-->
```

So ändern Sie die HTTPOnly Flag-Einstellung mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Load Balancing Parameter konfigurieren**, und wählen oder deaktivieren Sie das Flag “ **Persistenz-Cookie HttpOnly**”.

Verschlüsseln des Cookies

Ab Release 10.5 Build 55.8 können Sie das Cookie zusätzlich zu jeder SSL-Verschlüsselung verschlüsseln.

Um das Cookie mit der Befehlszeilenschnittstelle zu verschlüsseln, geben Sie an der Eingabeaufforderung

```
set lb parameter -UseEncryptedPersistenceCookie ENABLED -
    cookiePassphrase test
<!--NeedCopy-->
```

So verschlüsseln Sie das Cookie mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **Lastausgleichsparameter ändern**, wählen Sie **Persistenz-Cookie-Werte codieren** und geben Sie eine Passphrase in **Cookie-Passphrase** ein.

SSL-Sitzungs-ID-Persistenz

October 5, 2021

Wenn die SSL-Sitzungs-ID-Persistenz konfiguriert ist, verwendet die Citrix ADC Appliance die SSL-Sitzungs-ID, die Teil des SSL-Handshake-Prozesses ist, um eine Persistenzsitzung zu erstellen, bevor die anfängliche Anforderung an einen Dienst weitergeleitet wird. Der virtuelle Lastenausgleichsserver leitet nachfolgende Anforderungen mit derselben SSL-Sitzungs-ID an denselben Dienst. Diese Art der Persistenz wird für SSL-Brückendienste verwendet.

Hinweis:

Es gibt zwei Probleme, die Benutzer berücksichtigen müssen, bevor sie sich für diese Art von Persistenz entscheiden. Erstens verbraucht dieser Persistenztyp Ressourcen auf der Citrix ADC Appliance, wodurch die Anzahl der gleichzeitig unterstützten Persistenzsitzungen begrenzt wird. Wenn Sie erwarten, mehrere Persistenzsitzungen zu unterstützen, sollten Sie möglicherweise eine andere Art von Persistenz wählen.

Zweitens, wenn der Client und der Server mit Lastausgleich die Sitzungs-ID während ihrer Transaktionen neu verhandeln müssen, wird die Persistenz nicht beibehalten, und eine neue Persistenzsitzung wird erstellt, wenn die nächste Anforderung des Clients empfangen wird. Dies kann dazu führen, dass die Aktivitäten des Kunden auf der Website unterbrochen werden und der Client möglicherweise aufgefordert wird, sich erneut zu authentifizieren oder die Sitzung neu zu starten. Dies kann auch zu einer großen Anzahl verlassener Sitzungen führen, wenn das Timeout auf einen zu großen Wert eingestellt ist.

Informationen zum Konfigurieren der Persistenz basierend auf der SSL-Sitzungs-ID finden Sie unter Konfigurieren von Persistenztypen, die keine Regel erfordern.

> **Hinweis:**
>
> SSL-Sitzungs-ID-Persistenz wird bei Sitzungstickets nicht unterstützt.

Sichern Sie die Persistenzunterstützung für SSL-Sitzungs-ID

Ab NetScaler Version 12.0 Build 56.20 wird die Quell-IP-Persistenz als Backuppersistenztyp für die SSL-Sitzungs-ID-Persistenz unterstützt. Wenn der Client und der Server mit Lastenausgleich die Sitzung neu verhandeln und die Quell-IP-Persistenz als Backup-Persistenz konfiguriert ist, werden Clientanforderungen an denselben Server weitergeleitet.

Zur Unterstützung der Backup-Persistenz für SSL-Sitzungs-ID erstellt die Citrix ADC Appliance Sitzungseinträge für Quell-IP und SSL-Sitzungs-ID, wenn eine Clientanforderung zum ersten Mal empfangen wird. Für die nachfolgenden Anforderungen, die dieselbe Sitzungs-ID enthalten, wird die SSL-Sitzungs-ID verwendet. Wenn der Client und der Server mit Lastenausgleich die Sitzung neu verhandeln, wird die Clientanforderung mit der Quell-IP-Persistenz an denselben Server weitergeleitet und ein neuer SSL-Sitzungs-ID-Persistenzeintrag erstellt.

Informationen zum Konfigurieren der Backup-Persistenz finden Sie unter Konfigurieren der Backuppersistenz.

Diameter-AVP-Nummer Persistenz

October 5, 2021

Sie können Persistenz basierend auf der AVP-Nummer (Attribut-Value Pair) einer Diameter Message verwenden, um persistente Diameter Sitzungen zu erstellen. Wenn die Citrix ADC Appliance den AVP in der Diameter-Nachricht findet, erstellt sie eine Persistenzsitzung basierend auf dem Wert des AVP. Alle nachfolgenden Meldungen, die dem Wert des AVP entsprechen, werden an den zuvor ausgewählten Server weitergeleitet. Wenn der Wert des AVP nicht mit der Persistenzsitzung übereinstimmt, wird eine neue Sitzung für den neuen Wert erstellt.

Hinweis: Wenn die AVP-Nummer nicht in Diameter-Basisprotokoll RFC 6733 definiert ist und die Nummer in einem gruppierten AVP verschachtelt ist, müssen Sie eine Folge von AVP-Nummern (maximal 3) in übergeordneter und untergeordneter Reihenfolge definieren. Wenn beispielsweise die persistente AVP-Nummer X innerhalb von AVP Y verschachtelt ist, das in Z verschachtelt ist, definieren Sie die Liste als Z Y X.

So konfigurieren Sie die Diameter-basierte Persistenz auf einem virtuellen Server mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set lb vserver <name> -PersistenceType <type-> persistAVPno <
   positive_integer>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver diameter_vs -persistenceType DIAMETER -persistAVPno 263
<!--NeedCopy-->
```

Benutzerdefinierte Server-ID-Persistenz

October 5, 2021

In der Persistenzmethode Custom Server ID wird die in der Clientanforderung angegebene Server-ID zur Aufrechterhaltung der Persistenz verwendet. Damit dieser Persistenztyp funktioniert, müssen Sie zunächst eine Server-ID für die Dienste festlegen. Die Citrix ADC Appliance überprüft die URL der Clientanforderung und stellt eine Verbindung mit dem Server her, der der angegebenen Server-ID zugeordnet ist. Der Dienstanbieter muss sicherstellen, dass die Benutzer die Server-IDs kennen, die in ihren Anfragen für bestimmte Dienste bereitgestellt werden sollen.

Wenn Ihre Website beispielsweise verschiedene Datentypen wie Bilder, Text und Multimedia von verschiedenen Servern bereitstellt, können Sie jedem Server eine Server-ID zuweisen. Auf der Citrix ADC Appliance geben Sie diese Server-IDs für die entsprechenden Dienste an, und konfigurieren Sie die Persistenz der benutzerdefinierten Server-ID auf dem entsprechenden virtuellen Lastausgleichsserver. Beim Senden einer Anforderung fügt der Client die Server-ID in die URL ein, die den erforderlichen Datentyp angibt.

So konfigurieren Sie die Persistenz der benutzerdefinierten Server-ID:

- Weisen Sie in Ihrem Lastausgleichs-Setup jedem Dienst, für den Sie die benutzerdefinierte Server-ID verwenden möchten, eine Server-ID zu, um die Persistenz beizubehalten. Alphanumerische Server-IDs sind zulässig.
- Geben Sie Regeln in der Standard-Syntaxausdruckssprache an, um die URL-Abfragen für die Server-ID zu untersuchen und den Datenverkehr an den entsprechenden Server weiterzuleiten.
- Konfigurieren Sie die Persistenz der benutzerdefinierten Server-ID.

Hinweis: Der Wert für das Persistenz-Timeout wirkt sich nicht auf den Persistenztyp der benutzerdefinierten Server-ID aus. Es gibt keine Begrenzung für die maximale Anzahl von persistenten Clients, da dieser Persistenztyp keine Clientinformationen speichert.

Beispiel:

Weisen Sie in einem Lastausgleichs-Setup mit zwei Diensten die Server-ID 2345-photo-56789 zu Service-1 und die Server-ID 2345-drawing-abb123 zu Service-2 zu. Binden Sie diese Dienste an einen virtuellen Server mit dem Namen Web11.

```
1 set service Service-1 10.102.29.5 -CustomServerID 2345-photo-56789
2
3 set service Service-2 10.102.29.6 -CustomServerID 2345-drawing-abb123
4 <!--NeedCopy-->
```

Aktivieren Sie auf dem virtuellen Server Web11 die Persistenz der benutzerdefinierten Server-ID.

Erstellen Sie den folgenden Ausdruck, damit alle URL-Abfragen, die die Zeichenfolge sid= enthalten, untersucht werden.

HTTP.REQ.URL.AFTER_STR (sid=)

Beispiel:

```
1 set lb vserver Web11 -persistenceType customserverID -rule "HTTP.REQ.
     URL.AFTER_STR("sid=")"
2
3 bind lb vserver Web11 Service-[1-2]
```



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

Wenn ein Client eine Anforderung mit der folgenden URL an die IP-Adresse von Web11 sendet, leitet die Appliance die Anforderung an Service-2 weiter und berücksichtigt die Persistenz.

Beispiel:

```
http://www.example.com/index.asp?&sid=2345-drawing-abb123
```

Weitere Informationen zu Standardsyntaxrichtlinienausdrücken finden Sie in der Richtlinienkonfiguration und -referenz.

So konfigurieren Sie die Persistenz der benutzerdefinierten Server-ID mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Öffnen Sie den Dienst, und legen Sie eine Server-ID fest.
3. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie den virtuellen Server.
4. Wählen Sie unter Erweiterte Einstellungen Persistenz aus.
5. Wählen Sie CUSTOMESERVERID, und geben Sie einen Ausdruck an.

Persistenz der IP-Adresse

October 5, 2021

Sie können die Persistenz auf Ziel-IP-Adressen oder auf Quell-IP- und Ziel-IP-Adressen basieren.

Persistenz basierend auf Ziel-IP-Adressen

Wenn die Citrix ADC Appliance eine Anforderung von einem neuen Client empfängt, erstellt sie eine Persistenzsitzung basierend auf der IP-Adresse des vom virtuellen Server ausgewählten Dienstes (der Ziel-IP-Adresse). Später leitet es Anfragen an dieselbe Ziel-IP an denselben Dienst weiter. Diese Art der Persistenz wird beim Link-Load-Balancing verwendet. Weitere Informationen zum Link-Lastenausgleich finden Sie unter Link Load Balancing.

Der Timeout-Wert für die Ziel-IP-Persistenz entspricht dem für die Persistenz der Quell-IP-Persistenz, beschrieben unter Persistenz basierend auf Quell-IP-Adresse.

Informationen zum Konfigurieren der Persistenz basierend auf der Ziel-IP-Adresse finden Sie unter Konfigurieren von Persistenztypen, die keine Regel erfordern.

Persistenz basierend auf Quell- und Ziel-IP-Adressen

Wenn die Citrix ADC Appliance eine Anforderung erhält, erstellt sie eine Persistenzsitzung, die sowohl auf der IP-Adresse des Clients (der Quell-IP-Adresse) als auch auf der IP-Adresse des vom virtuellen Server ausgewählten Dienstes (der Ziel-IP-Adresse) basiert. Später leitet es Anfragen von derselben Quell-IP und an dieselbe Ziel-IP an denselben Dienst weiter.

Der Timeout-Wert für die Ziel-IP-Persistenz entspricht dem für die Persistenz der Quell-IP-Persistenz, beschrieben unter Persistenz basierend auf Quell-IP-Adresse.

Informationen zum Konfigurieren der Persistenz basierend auf Quell- und Ziel-IP-Adressen finden Sie unter Konfigurieren von Persistenztypen, die keine Regel erfordern.

SIP-Anruf-ID-Persistenz

October 5, 2021

Bei der Persistenz der SIP-Anruf-ID wählt die Citrix ADC Appliance einen Dienst basierend auf der Anruf-ID im SIP-Header aus. Dadurch kann er Pakete für eine bestimmte SIP-Sitzung an denselben Dienst und damit an denselben Lastausgleichsserver weiterleiten. Dieser Persistenztyp ist speziell für den SIP-Lastenausgleich anwendbar. Weitere Informationen zum SIP-Lastenausgleich finden Sie unter Überwachen von SIP-Diensten.

Informationen zum Konfigurieren der Persistenz basierend auf SIP-Anruf-ID finden Sie unter Konfigurieren von Persistenztypen, die keine Regel erfordern.

RTSP-Sitzungs-ID-Persistenz

October 5, 2021

Wenn die Citrix ADC Appliance eine Anforderung von einem neuen Client empfängt, erstellt sie eine Persistenzsitzung basierend auf der RTSP- Sitzungs-ID (Real-Time Streaming Protocol) im RTSP-Paket-Header und leitet die Anforderung dann an den RTSP-Dienst weiter, der vom konfigurierten Load Balancing ausgewählt wurde -Methode. Es leitet nachfolgende Anforderungen, die dieselbe Sitzungs-ID enthalten, an denselben Dienst weiter. Dieser Persistenztyp ist speziell für den SIP-Lastenausgleich anwendbar. Weitere Informationen zum SIP-Lastenausgleich finden Sie unter Überwachen von SIP-Diensten.

Hinweis: Die Persistenz der RTSP-Sitzungs-ID ist standardmäßig auf virtuellen RTSP-Servern konfiguriert, und Sie können diese Einstellung nicht ändern.

Manchmal geben verschiedene RTSP Server dieselben Sitzungs-IDs aus. In diesem Fall können keine eindeutigen Sitzungen zwischen dem Client und dem RTSP-Server erstellt werden, indem nur die RTSP-Sitzungs-ID verwendet wird. Wenn Sie mehrere RTSP-Server haben, die möglicherweise dieselben Sitzungs-IDs ausgeben, können Sie die Appliance so konfigurieren, dass die IP-Adresse und den Port des Servers an die Sitzungs-ID angehängt wird und ein eindeutiges Token erstellen, mit dem die Persistenz festgestellt werden kann. Dies wird als Sitzungs-ID-Zuordnung bezeichnet.

Informationen zum Konfigurieren von Persistenz basierend auf RTSP-Sitzungs-IDs finden Sie unter Konfigurieren von Persistenztypen, die keine Regel erfordern.

Wichtig: Wenn Sie die Session-ID-Zuordnung verwenden müssen, müssen Sie den folgenden Parameter festlegen, wenn Sie jeden Service innerhalb der Load Balancing-Einrichtung konfigurieren. Stellen Sie außerdem sicher, dass keine nicht persistenten Verbindungen über den virtuellen RTSP Server weitergeleitet werden.

Konfigurieren der passiven URL-Persistenz

October 5, 2021

Bei der passiven URL-Persistenz extrahiert die Citrix ADC Appliance, wenn eine Anforderung von einem Client empfängt, die Server-IP-Adress-Port-Informationen (ausgedrückt als einzelne Hexadezimalzahl) aus der Clientanforderung.

Die passive URL-Persistenz erfordert die Konfiguration eines erweiterten Ausdrucks, der das Abfrageelement angibt, das die IP-Adressen-Port-Informationen des Servers enthält. Weitere Informationen zu klassischen und erweiterten Richtlinienausdrücken finden Sie unter Richtlinien und Ausdrücke.

Mit dem folgenden Ausdruck wird die Appliance so konfiguriert, dass Anforderungen für URL-Abfragen untersucht werden, die die Zeichenfolge urlp= enthalten, die Server-IP-Adressen-Port-Informationen extrahiert, sie aus einer hexadezimalen Zeichenfolge in eine IP- und Portnummer konvertiert und die Anforderung an den Dienst weitergeleitet, der mit dieser IP-Adresse und Portnummer.

HTTP.REQ.URL.AFTER_STR(“urlp=”)

Wenn die passive URL-Persistenz aktiviert ist und der vorherige Ausdruck konfiguriert ist, wird eine Anforderung mit der folgenden URL- und Server-IP-Adressen-Port-Zeichenfolge an 10.102.29.10:80 weitergeleitet.

```
http://www.example.com/index.asp?&urlp=0A661D0A0050
```

Der Persistenz-Timeout-Wert hat keinen Einfluss auf diesen Persistenztyp. Die Persistenz bleibt erhalten, solange die IP-Adressen-Portinformationen des Servers aus Clientanforderungen extrahiert

werden können. Dieser Persistenztyp verbraucht keine Appliance-Ressourcen, so dass er eine unbegrenzte Anzahl persistenter Clients aufnehmen kann.

Um die passive URL-Persistenz zu konfigurieren, konfigurieren Sie zunächst die Persistenz wie unter Persistenztypen konfigurieren beschrieben, die keine Regel erfordern. Sie setzen den Persistenztyp auf URLPASSIVE. Sie führen dann die folgenden Verfahren aus.

So konfigurieren Sie die passive URL-Persistenz mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

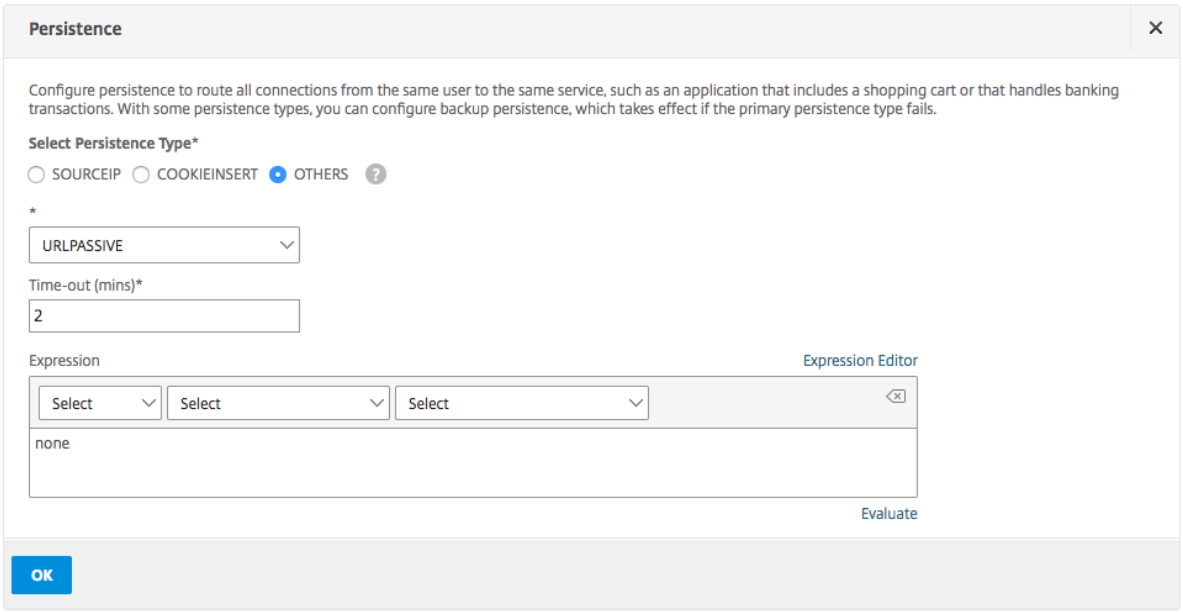
```
set lb vserver <vserverName>  [-persistenceType <persistenceType>]  [-
    rule <expression>]
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver LB-VServer-1 -persistenceType URLPASSIVE  -rule HTTP.REQ
    .URL.AFTER_STR( "urlp=" )
<!--NeedCopy-->
```

So konfigurieren Sie die Persistenz auf einem virtuellen Server mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie den virtuellen Server.
2. Wählen Sie im Abschnitt Persistenz den Persistenztyp aus, der Ihrer Anforderung entspricht. Der am besten geeignete Persistenztyp für den virtuellen Server ist als Optionsschaltflächen verfügbar. Andere Persistenztypen, die auf den spezifischen virtuellen Servertyp anwendbar sind, können aus der Liste Andere ausgewählt werden.



Hinweis:

Vor NetScaler Release 12.0 Build 56.20 sind alle Persistenztypen in einer einzigen Persistence-Dropdownliste ohne Optionsschaltflächen verfügbar.

Konfigurieren der Persistenz basierend auf benutzerdefinierten Regeln

October 5, 2021

Wenn eine regelbasierte Persistenz konfiguriert ist, erstellt die Citrix ADC Appliance eine Persistenzsitzung basierend auf dem Inhalt der übereinstimmenden Regel, bevor sie die Anforderung an den Dienst leitet, der von der konfigurierten Lastausgleichsmethode ausgewählt wurde. Später leitet es alle Anfragen, die mit der Regel übereinstimmen, an denselben Dienst weiter. Sie können regelbasierte Persistenz für Dienste vom Typ HTTP, SSL, RADIUS, ANY, TCP und SSL_TCP konfigurieren.

Regelbasierte Persistenz erfordert einen klassischen oder standardmäßigen Syntaxausdruck. Sie können einen klassischen Ausdruck zum Auswerten von Anforderungskopfzeilen verwenden, oder Sie können einen Standard-Syntaxausdruck verwenden, um Anforderungskopfzeilen, Webformulardaten in einer Anforderung, Antwortkopfzeilen oder Antwortkörpern auszuwerten. Sie können beispielsweise einen klassischen Ausdruck verwenden, um die Persistenz basierend auf dem Inhalt des HTTP-Host-Headers zu konfigurieren. Sie können auch einen Standardsyntaxausdruck verwenden, um die Persistenz basierend auf Informationen zu Anwendungssitzungen in einem Antwort-Cookie oder einem benutzerdefinierten Header zu konfigurieren. Weitere Informationen zum Erstellen und Verwenden von klassischen Syntaxausdrücken und Standardsyntaxausdrücken finden Sie unter Richtlinien und Ausdrücke.

Die Ausdrücke, die Sie konfigurieren können, hängen von der Art des Dienstes ab, für den Sie regelbasierte Persistenz konfigurieren. Beispielsweise sind bestimmte RADIUS-spezifische Ausdrücke für andere Protokolle als RADIUS nicht zulässig, und TCP-Options-basierte Ausdrücke sind für andere Diensttypen als den Typ ANY nicht zulässig. Für TCP- und SSL_TCP-Diensttypen können Sie Ausdrücke verwenden, die TCP/IP-Protokolldaten, Layer-2-Daten, TCP-Optionen und TCP-Nutzlasten auswerten.

Hinweis: Für einen Anwendungsfall, der die Konfiguration regelbasierter Persistenz auf Basis von Financial Information Exchange (“FIX”) -Protokolldaten beinhaltet, die über TCP übertragen werden, finden Sie unter Konfigurieren regelbasierter Persistenz basierend auf einem Name-Wert-Paar in einem TCP-Byte-Stream.

Regelbasierte Persistenz kann verwendet werden, um die Persistenz mit Entitäten wie Citrix SD-WAN-Appliances, Citrix SD-WAN SD-WAN-Plug-Ins, Cache-Servern und Anwendungsservern aufrechtzuerhalten.

Hinweis: Auf einem beliebigen virtuellen Server können Sie keine regelbasierte Persistenz für die Antworten konfigurieren.

Um die Persistenz basierend auf einer benutzerdefinierten Regel zu konfigurieren, konfigurieren Sie zunächst die Persistenz wie unter Persistenztypen konfigurieren beschrieben, die keine Regel erfordern, und legen den Persistenztyp auf REGEL fest. Sie können dann die folgenden Verfahren ausführen. Sie können die regelbasierte Persistenz mit dem Konfigurationsdienstprogramm oder der CLI konfigurieren.

So konfigurieren Sie die Persistenz anhand benutzerdefinierter Regeln mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <vserverName> [-rule <expression>][-resRule <expression
    >]
<!--NeedCopy-->
```

Beispiel:

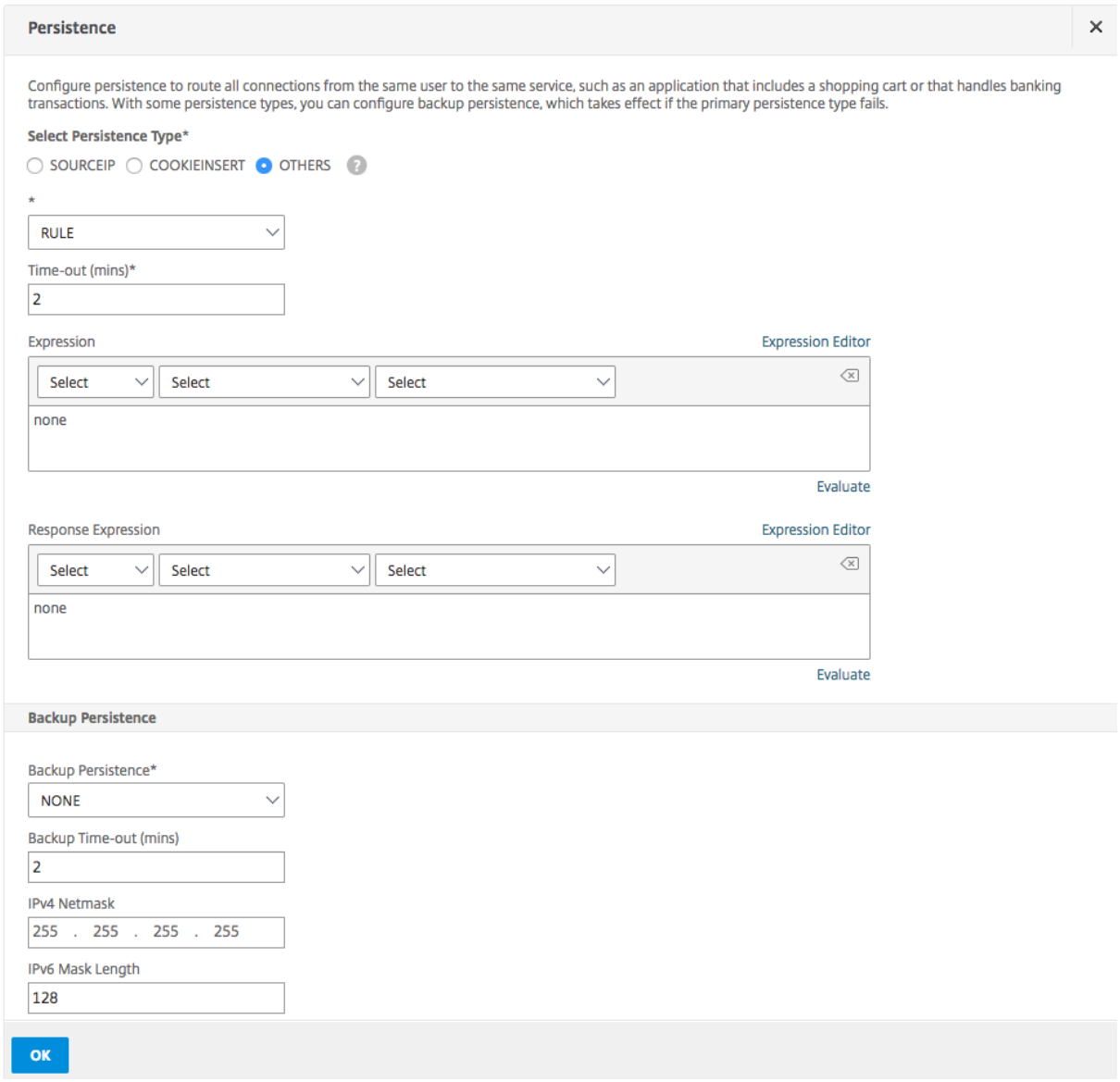
```
set lb vserver vsvr_name -rule http.req.header(”cookie”).value(0).
    typecast_nvlist_t('=',';').value(”server”)

set lb vserver vsvr_name -resrule http.res.header(”set-cookie”).value
    (0).typecast_nvlist_t('=',';').value(”server”)

<!--NeedCopy-->
```


So konfigurieren Sie die Persistenz basierend auf benutzerdefinierten Regeln mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie den virtuellen Server.
2. Wählen Sie im Abschnitt Persistenz den Persistenztyp aus, der Ihrer Anforderung entspricht. Der am besten geeignete Persistenztyp für den virtuellen Server ist als Optionsschaltflächen verfügbar. Andere Persistenztypen, die auf den spezifischen virtuellen Servertyp anwendbar sind, können aus der Liste Andere ausgewählt werden.



> **Hinweis:**
>
> Vor NetScaler Release 12.0 Build 56.20 sind alle Persistenztypen in einer einzigen Persistence-

> Dropdownliste ohne Optionsschaltflächen verfügbar.

Beispiel: Klassischer Ausdruck für eine Anforderungs-Nutzlast

Der folgende klassische Ausdruck erstellt eine Persistenzsitzung basierend auf dem Vorhandensein eines User-Agent-HTTP-Headers, der die Zeichenfolge “MyBrowser” enthält, und leitet alle nachfolgenden Clientanforderungen, die diesen Header und String enthalten, an denselben Server, der für die erste Anforderung ausgewählt wurde.

```
http header User-Agent contains MyBrowser
<!--NeedCopy-->
```

Beispiel: Standard-Syntaxausdruck für einen Anforderungskopf

Der folgende Standardsyntaxausdruck macht dasselbe wie der vorherige klassische Ausdruck.

HTTP.REQ.HEADER (User-Agent) .CONTAINS (MyBrowser)

Beispiel: Standard-Syntaxausdruck für ein Antwort-Cookie

Der folgende Ausdruck untersucht Antworten auf Server -Cookies und leitet dann alle Anfragen, die dieses Cookie enthalten, an denselben Server, der für die erste Anforderung ausgewählt wurde.

HTTP.RES.HEADER(“SET-COOKIE”).VALUE(0).TYPECAST_NVLIST_T(‘=’,’;’).VALUE(“server”)

Konfigurieren von Persistenztypen, für die keine Regel erforderlich ist

October 5, 2021

Um die Persistenz zu konfigurieren, müssen Sie zuerst einen virtuellen Lastausgleichsserver einrichten, wie unter Basic Load Balancing einrichtenbeschrieben. Anschließend konfigurieren Sie die Persistenz auf dem virtuellen Server.

So konfigurieren Sie die Persistenz auf einem virtuellen Server mit der CLI

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


```
set lb vserver <name> -PersistenceType <type> [-timeout <integer>]

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

Beispiel:

```
set lb vserver Vserver-LB-1 -persistenceType SOURCEIP -timeout 60

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

Timeout ist der Zeitraum, für den eine Persistenzsitzung in Kraft ist. Die Standard- und Minimalwerte für Timeout (in Minuten) variieren je nach Persistenztyp, wie in der folgenden Tabelle aufgeführt.

Persistenztyp	Standardwert	Minimum	Maximum
Cookie-Einfüge/Gruppen-Cookie-Einsatz	2	0	1440
Andere Persistenzarten	2	2	1440

> **Hinweis:**
>
> - Gruppen-Cookie-Einfügepersistenztyp kann für die Lastausgleichsgruppe festgelegt werden.
> - Für IP-basierte Persistenz können Sie auch den Parameter PersistMask festlegen.
> - Der Persistenztyp ist standardmäßig auf NONE festgelegt.

So konfigurieren Sie die Persistenz auf einem virtuellen Server mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie den virtuellen Server.
2. Wählen Sie im Abschnitt Persistenz den Persistenztyp aus, der Ihrer Anforderung entspricht. Der am besten geeignete Persistenztyp für den virtuellen Server ist als Optionsschaltflächen verfügbar. Andere Persistenztypen, die auf den spezifischen virtuellen Servertyp anwendbar sind, können aus der Liste **Andere** ausgewählt werden.

> **Hinweis** Vor Citrix ADC Release 12.0 Build 56.20 sind alle Persistenztypen in einer einzigen Persistenz-Dropdownliste ohne Optionsfelder verfügbar.

Konfigurieren der Backup-Persistenz

December 7, 2021

Sie können einen virtuellen Server so konfigurieren, dass er den Persistenztyp der Quell-IP verwendet, wenn der primäre Persistenztyp fehlschlägt.

In der folgenden Tabelle werden die Kombinationen von primären und sekundären Backup-Persistenztypen sowie die Bedingungen beschrieben, bei denen die Backup-Persistenz verwendet wird.

Primäre Persistenz	Backup-Persistenz	Wenn die primäre Persistenzsuche fehlschlägt…
CookieInsert	Quell-IP	Die Appliance greift nur dann auf Source-IP-basierte Persistenz zurück, wenn der Client-Browser in der Anforderung kein Cookie zurückgibt. Wenn der Browser jedoch ein Cookie zurückgibt (nicht notwendigerweise das Persistenz-Cookie), wird davon ausgegangen, dass der Browser Cookies unterstützt und somit Backup-Persistenz nicht ausgelöst wird.
Regel	Quell-IP	Die Appliance verwendet Source-IP-basierte Persistenz, wenn der in der Regel angegebene Parameter in der eingehenden Anforderung fehlt.

Hinweis:

- Wenn der primäre Persistenztyp HTTP-Cookie-basierte Persistenz ist und der Backup-Persistenztyp Quell-IP-basiert ist, können Sie einen Timeout-Wert für die Backup-Persistenz festlegen. Anweisungen finden Sie unter Festlegen eines Timeout-Werts für Idle Clientverbindungen.
- Sie können keinen Timeout-Wert für die Backup-Persistenz festlegen, wenn die primäre Persistenz auf Regel basiert, da in diesem Fall der Timeout-Wert für die sekundäre Persistenz mit dem für die primäre Persistenz übereinstimmen muss. Daher laufen die primären und sekundären zur gleichen Zeit ab.

So legen Sie die Backup-Persistenz für einen virtuellen Server mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -persistenceType <PersistenceType> -
    persistenceBackup <BackupPersistenceType>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -persistenceType CookieInsert -
    persistenceBackup SourceIP

set lb vserver Vserver-LB-1 -persistenceType sslsession -
    persistenceBackup SourceIP

set lb vserver Vserver-LB-1  - persistenceType RULE  - rule http.req.
    header("User-Agent").value(0).contains("MyBrowser")  -
    persistenceBackup SOURCEIP

set lb vserver Vserver-LB-1 -persistenceType sslsession -
    persistenceBackup SourceIP
<!--NeedCopy-->
```


So legen Sie die Backup-Persistenz für einen virtuellen Server mit dem Konfigurationsdienstprogramm fest

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie den virtuellen Server.
2. Wählen Sie **unter Erweiterte Einstellungen Persistenz**aus, und geben Sie einen Backup-Persistenztyp an.

Hinweis: Die primäre Persistenz muss auf COOKIEINSERT, RULE oder SSLSESSION festgelegt sein.

Persistenzgruppen konfigurieren

October 5, 2021

Wenn Sie über Server mit Lastenausgleich verfügen, die verschiedene Arten von Verbindungen verarbeiten (z. B. Webserver, die Multimedia hosten), können Sie eine virtuelle Servergruppe so konfigurieren, dass diese Verbindungen verarbeitet werden. Um eine virtuelle Servergruppe zu erstellen, binden Sie verschiedene Typen von virtuellen Servern, einen für jeden Verbindungstyp, den Ihre Server mit Lastausgleich akzeptieren, in eine einzelne Gruppe. Anschließend konfigurieren Sie einen Persistenztyp für die gesamte Gruppe.

Sie können entweder Quell-IP-basierte Persistenz oder HTTP-Cookie-basierte Persistenz für Persistenzgruppen konfigurieren. Nachdem Sie die Persistenz für die gesamte Gruppe festgelegt haben, können Sie sie nicht für einzelne virtuelle Server in der Gruppe ändern. Wenn Sie die Persistenz für eine Gruppe konfigurieren und der Gruppe dann einen neuen virtuellen Server hinzufügen, wird die Persistenz des neuen virtuellen Servers so geändert, dass sie mit der Persistenzeinstellung der Gruppe übereinstimmt.

Wenn die Persistenz auf einer Gruppe virtueller Server konfiguriert ist, werden Persistenzsitzungen für anfängliche Anforderungen erstellt, und nachfolgende Anforderungen werden an denselben Dienst wie die Erstanforderung weitergeleitet, unabhängig vom virtuellen Server in der Gruppe, der jede Clientanforderung empfängt.

Wenn Sie einen virtuellen Server mit Persistenzsitzungen zu einer Lastausgleichsgruppe mit einem anderen Persistenztyp hinzufügen, werden die vorhandenen persistenten Sitzungen, die für einen alten Persistenztyp spezifisch sind, gelöscht. Die persistenten Sitzungen entscheiden, ob der Datenverkehr auf denselben virtuellen Server oder auf einen anderen Server übertragen werden muss. Daher sind bestehende Verbindungen nicht betroffen.

Der Persistenztyp einer Lastausgleichsgruppe wird unabhängig vom Protokolltyp des virtuellen Servers auf alle an diese Gruppe gebundenen virtuellen Server angewendet. Eine Load Balancing-Gruppe unterstützt die folgenden Persistenztypen:

- sourceIP
- CookieInsert
- Regel

Einige virtuelle Server unterstützen nur bestimmte Persistenzarten. Beispielsweise kann ein virtueller Server vom Typ SSL_BRIDGE nur den sourceIP-Persistenztyp für eine LB-Gruppe verwenden.

Wenn Sie HTTP-Cookie-basierte Persistenz konfigurieren, wird das Domänenattribut des HTTP-Cookies gesetzt. Diese Einstellung bewirkt, dass die Clientsoftware das HTTP-Cookie in Clientanforderungen hinzufügt, wenn verschiedene virtuelle Server unterschiedliche öffentliche Hostnamen haben. Weitere Informationen zum Persistenztyp von CookieInsert finden Sie unter Persistenz basierend auf HTTP-Cookies.

So erstellen Sie eine Persistenzgruppe virtueller Server mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind lb group <vServerGroupName> <vServerName> -persistenceType <
     PersistenceType>
2 <!--NeedCopy-->
```

Beispiel:

```
1 bind lb group Vserver-Group-1 Vserver-LB-1 -persistenceType
     CookieInsert
2 <!--NeedCopy-->
```

So ändern Sie eine virtuelle Servergruppe mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Persistency Groups**, erstellen Sie eine Persistenzgruppe und geben Sie die virtuellen Server an, die Teil dieser Gruppe sein müssen.

So ändern Sie eine virtuelle Servergruppe mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set lb group <vServerGroupName> -PersistenceBackup <
    BackupPersistenceType> -persistMask <SubnetMaskAddress>
<!--NeedCopy-->
```

Beispiel:

```
set lb group vserver-Group-1 -PersistenceBackup SourceIP -persistMask
    255.255.255.255
<!--NeedCopy-->
```

Freigeben von persistenten Sitzungen zwischen virtuellen Servern

October 5, 2021

In einigen Kundenumgebungen (Telekommunikation und ISP) übernimmt ein einzelner Server sowohl die Kontrolle als auch den Datenverkehr. Bei einer bestimmten Client-IP-Adresse müssen sowohl der Steuer- als auch der Datenverkehr an denselben Back-End-Server weitergeleitet werden. Dazu ist ein virtueller Server für die Verarbeitung des Clientauthentifizierungsdatenverkehrs erforderlich, und normalerweise wird auf ihm regelbasierte Persistenz konfiguriert. Beispiel: Radius.req.avp (8) .value.typecast_text_t'. Der zweite virtuelle Server für die Verarbeitung von Datenverkehr. Normalerweise ist SourceIP Persistenz darauf konfiguriert.

Zuvor waren Persistenzeinträge lokal für den virtuellen Server. Wenn Sie Persistenz auf mehrere virtuelle Server anwenden mussten, mussten Sie den virtuellen Server einer Load Balancing-Gruppe hinzufügen und dann einen gemeinsamen Persistenztyp auf die Gruppe anwenden. Diese Anforderung kann nicht erfüllt werden, da alle virtuellen Server, die an eine Lastausgleichsgruppe gebunden sind, die für die Gruppe konfigurierte Persistenz geerbt haben.

Mit der Funktion "Persistenzfreigabe zwischen virtuellen Servern" können Sie den neuen `useVserverPersistency` Parameter für eine Lastausgleichsgruppe festlegen, damit der virtuelle Server in der Gruppe seine eigenen Persistenzparameter verwenden kann, anstatt sie von den Gruppeneinstellungen zu erben. Sie können auf jedem virtuellen Server eine separate regelbasierte Persistenz konfigurieren.

Optional können Sie einen der virtuellen Server in der Gruppe auch als virtuellen Hauptserver festlegen. Wenn ein virtueller Server als virtueller Hauptserver bezeichnet wird, erstellt nur dieser virtuelle Server die Persistenzeinträge, die von allen virtuellen Servern in der Gruppe verwendet werden. Wenn der virtuelle Hauptserver ausgefallen ist, erstellt die Citrix ADC Appliance keine Persistenzeinträge.

Hinweis: Die Persistenzfreigabe auf den virtuellen Servern wird nur für regelbasierte Persistenzmethoden unterstützt. Konfigurieren Sie kompatible regelbasierte Persistenzparameter auf den virtuellen Servern des Mitglieds.

Beispiel:

Angenommen, v1 und v2 sind an eine Lastausgleichsgruppe gebunden, v1 ist ein virtueller Server vom Typ RADIUS und v2 ist ein virtueller Server vom Typ HTTP. 'Radius.req.avp (8) .value.typecast_text_t' Persistenz ist auf v1 konfiguriert und 'client.ip.src' ist auf v2 konfiguriert.

Wenn Datenverkehr durch den virtuellen RADIUS-Server v1 fließt, erstellt er einen dauerhaften Eintrag basierend auf der ausgewerteten Regelzeichenfolge. Später, wenn der Datenverkehr den virtuellen Server des HTTP-Typs v2 erreicht, sucht v2 nach den Persistenzeinträgen in der Load Balancing-Gruppe und leitet den Datenverkehr mit derselben Persistenzsitzung auf denselben Back-End-Server weiter.

Konfigurieren der Freigabe von persistenten Sitzungen

Um Persistenzparameter über den virtuellen Server in einer Load Balancing-Gruppe freizugeben, müssen Sie zuerst den UsevServerPersistency-Parameter aktivieren und dann einen der virtuellen Server in der Gruppe als Hauptserver festlegen.

So aktivieren Sie den Parameter UseVServerPersistency mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set lb group <name> -useVserverPersistency ( ENABLED)
2 <!--NeedCopy-->
```

Beispiel:

```
1 set lb group lb_grp1 -useVserverPersistency ENABLED
2 <!--NeedCopy-->
```

So aktivieren Sie den Parameter UseVServerPersistency mit der GUI

1. Navigieren Sie zu **Konfiguration** > **Verkehrsverwaltung** > **Lastausgleich** > **Persistenzgruppen** .

2. Klicken Sie auf **Hinzufügen**, um eine neue Gruppe hinzuzufügen, oder wählen Sie eine vorhandene Gruppe aus und klicken Sie auf **Bearbeiten** .
3. Wählen Sie **Vserver-Persistenz verwenden**aus.

So weisen Sie einen virtuellen Server mit der Befehlszeilenschnittstelle als virtuellen Hauptserver aus

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb group <name> -useVserverPersistency ( ENABLED ) -masterVserver <
    string>
<!--NeedCopy-->
```

Beispiel:

```
set lb group lb_grp1 -useVserverPersistency ENABLED - masterVserver vs1
<!--NeedCopy-->
```

So weisen Sie einen virtuellen Server mit der GUI als virtuellen Hauptserver aus

1. Navigieren Sie zu **Konfiguration** > **Verkehrsverwaltung** > **Lastausgleich** > **Persistenzgruppen** .
2. Klicken Sie auf **Hinzufügen**, um eine neue Gruppe hinzuzufügen, oder wählen Sie eine vorhandene Gruppe aus und klicken Sie auf **Bearbeiten** .
3. Wählen Sie **Vserver-Persistenz verwenden**aus.
4. Klicken Sie im Feld **Name des virtuellen Servers** auf **+**, um den virtuellen Server der Gruppe hinzuzufügen. Sie können den verfügbaren virtuellen Server auswählen oder einen virtuellen Server erstellen.
5. Klicken Sie auf **Erstellen**, wenn Sie eine neue Gruppe hinzufügen, oder auf **Schließen**, wenn Sie eine vorhandene Gruppe ändern.
6. Wählen Sie die Gruppe aus, für die Sie den UsevServerPersistency-Parameter aktiviert haben, und klicken Sie auf **Bearbeiten**, um einen virtuellen Server als Hauptserver zum Erstellen von Persistenzeinträgen festzulegen.
7. Wählen Sie aus der Liste **Master vServer** den virtuellen Server aus, der als virtueller Hauptserver bezeichnet werden muss.

Argumente

UseVServerPersistenz

Erlauben Sie den virtuellen Servern in einer Gruppe, ihre eigenen Persistenzparameter zum Erstellen persistenter Sitzungen zu verwenden, anstatt die Persistenzeinstellungen von den Gruppeneinstellungen zu erben. Wenn dieser Parameter aktiviert ist, kann die Persistenz für die Lastausgleichsgruppe nicht festgelegt werden.

Wenn dieser Parameter deaktiviert ist, erben die virtuellen Server der Gruppe die Persistenzparameter aus den Gruppeneinstellungen.

Wenn dieser Parameter in der Lastausgleichsgruppe eingeschaltet ist, leert die Citrix ADC Appliance alle entsprechenden Persistenzeinträge der Gruppe und der virtuellen Mitgliedsserver.

Mögliche Werte: ENABLED, DISABLED

Standard: DISABLED

Beispiel:

```
set lb group lb_grp1 -useVserverPersistency ENABLED
<!--NeedCopy-->
```

MasterVServer

Bestimmen Sie einen virtuellen Server als virtuellen Hauptserver in seiner Load Balancing-Gruppe. Nach der Bezeichnung kann nur der virtuelle Hauptserver die von der Gruppe verwendeten persistenten Einträge erstellen.

Hinweis: Dieser Parameter kann nur festgelegt werden, wenn der Parameter UseVServerPersistency aktiviert ist.

Beispiel:

```
set lb group lb_grp1 -masterVserver vs1
<!--NeedCopy-->
```

Beispielkonfiguration für die Freigabe von persistenten Sitzungen mit der Befehlszeilenschnittstelle

Die virtuellen Server werden erstellt


```
add lb vs vs1 http 10.1.10.11 80 -persistence rule -rule 'client.ip.src'

add lb vs vs2 radius 10.2.2.2 1812 -persistenceType rule -rule 'Radius.req.avp(8).value.typecast_text_t'
<!--NeedCopy-->
```

Die Gruppen werden erstellt.

```
add lb group lb_grp1 -persistenceType NONE -useVserverPersistency ENABLED
<!--NeedCopy-->
```

Ein virtueller Server in einer Gruppe wird als virtueller Hauptserver bezeichnet.

```
set lb group lb_grp1 -masterVserver vs1
<!--NeedCopy-->
```

Die virtuellen Server sind an die Gruppe gebunden.

```
bind lb group lb_grp1 vs1
bind lb group lb_grp1 vs2
<!--NeedCopy-->
```

Weitere Informationen finden Sie unter Einrichten des Basis-Lastenausgleichs und Konfigurieren von Persistenzgruppen.

Konfigurieren des RADIUS-Lastausgleichs mit Persistenz

October 5, 2021

Die heutige komplexe Netzwerkumgebung erfordert häufig die Koordination einer Lastausgleichskonfiguration mit hoher Kapazität mit robuster Authentifizierung und Autorisierung. Anwendungsbenutzer können sich über mobile Zugangspunkte wie DSL- oder Kabelverbindungen für Verbraucher, WiFi oder sogar DFÜ-Knoten mit einem VPN verbinden. Diese Verbindungen verwenden normalerweise dynamische IPs, die sich während der Verbindung ändern können.

Wenn Sie den RADIUS-Lastenausgleich auf der Citrix ADC Appliance so konfigurieren, dass persistente Clientverbindungen zu RADIUS-Authentifizierungsservern unterstützt werden, verwendet die Appliance die Benutzeranmeldung oder das angegebene RADIUS-Attribut anstelle der Client-IP als Sitzungs-ID und leitet alle Verbindungen und Datensätze, die mit dieser -Benutzersitzung auf denselben RADIUS-Server. Benutzer können sich daher von mobilen Zugriffspunkten an Ihrem VPN anmelden, ohne dass die Verbindung getrennt wird, wenn sich die Client-IP oder WLAN-Zugriffspunkt ändert.

Um den RADIUS-Lastausgleich mit Persistenz zu konfigurieren, müssen Sie zuerst die RADIUS-Authentifizierung für Ihr VPN konfigurieren. Informationen und Anweisungen finden Sie im Kapitel Authentifizierung, Autorisierung, Auditing (AAA) in AAA Application Traffic. Wählen Sie auch entweder die Funktion Load Balancing oder Content Switching als Grundlage für Ihre Konfiguration und stellen Sie sicher, dass die von Ihnen gewählte Funktion aktiviert ist. Der Konfigurationsprozess mit beiden Funktionen ist fast identisch.

Anschließend konfigurieren Sie entweder zwei virtuelle Load Balancing- oder zwei Content Switching-Server, einer für die Verarbeitung des RADIUS-Authentifizierungsdatenverkehrs und der andere für den Umgang mit RADIUS-Kontoführungsdatenverkehr. Als Nächstes konfigurieren Sie zwei Dienste, einen für jeden virtuellen Lastausgleichsserver, und binden jeden virtuellen Lastausgleichsserver an seinen Dienst. Schließlich erstellen Sie eine Lastausgleichspersistenzgruppe und legen den Persistenztyp auf RULE fest.

Aktivieren der Funktion Lastausgleich oder Content Switching

Um die Funktion Load Balancing oder Content Switching verwenden zu können, müssen Sie zunächst sicherstellen, dass das Feature aktiviert ist. Wenn Sie eine neue Citrix ADC Appliance konfigurieren, die noch nicht konfiguriert wurde, sind beide Funktionen bereits aktiviert, sodass Sie zum nächsten Abschnitt springen können. Wenn Sie eine Citrix ADC Appliance mit einer vorherigen Konfiguration konfigurieren und Sie nicht sicher sind, ob die von Ihnen verwendete Funktion aktiviert ist, müssen Sie dies jetzt tun.

- Anweisungen zum Aktivieren der Lastenausgleichsfunktion finden Sie unter Load Balancing aktivieren.
- Anweisungen zum Aktivieren der Content Switching-Funktion finden Sie unter Aktivieren des Inhaltswechsels

Konfigurieren virtueller Server

Nachdem Sie die Funktion Lastenausgleich oder Content Switching aktiviert haben, müssen Sie als nächstes zwei virtuelle Server zur Unterstützung der RADIUS-Authentifizierung konfigurieren:

- **Virtueller RADIUS-Authentifizierungsserver.** Dieser virtuelle Server und der zugehörige

Dienst verarbeiten den Authentifizierungsdatenverkehr zu Ihrem RADIUS-Server. Der Authentifizierungsdatenverkehr besteht aus Verbindungen, die mit Benutzern verbunden sind, die sich bei Ihrer geschützten Anwendung oder VPN (Virtual Private Network) anmelden.

- **RADIUS Accounting Virtual Server.** Dieser virtuelle Server und der zugehörige Service verarbeiten Buchhaltungsverbindungen zu Ihrem RADIUS-Server. Accounting Traffic besteht aus Verbindungen, die die Aktivitäten eines authentifizierten Benutzers in Ihrer geschützten Anwendung oder VPN verfolgen.

Wichtig: Sie müssen entweder ein Paar virtueller Server mit Lastenausgleich oder ein Paar virtueller Server für Content Switching erstellen, die in der RADIUS-Persistenzkonfiguration verwendet werden können. Virtuelle Servertypen können nicht gemischt werden.

So konfigurieren Sie einen virtuellen Lastausgleichsserver mit der Befehlszeilenschnittstelle

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

```
1 add lb vserver <name> RADIUS <IP address> <port> -lbmethod TOKEN -rule
     <rule>
2
3 show lb vserver <name>
4 <!--NeedCopy-->
```

Um einen vorhandenen virtuellen Lastenausgleichsserver zu konfigurieren, ersetzen Sie den vorhergehenden `add lb virtual server` Befehl durch den `set lb vserver` Befehl, der dieselben Argumente annimmt.

So konfigurieren Sie einen virtuellen Content Switching-Server über die Befehlszeilenschnittstelle

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

```
1 add cs vserver <name> RADIUS <IP address> <port> -lbmethod TOKEN -rule
     <rule>
2
3 show cs vserver <name>
4 <!--NeedCopy-->
```


Um einen vorhandenen virtuellen Content Switching-Server zu konfigurieren, ersetzen Sie den vorherigen `add cs vserver` Befehl durch den `set cs vserver` Befehl, der dieselben Argumente annimmt.

Beispiel:

```
add lb vserver radius_auth_vs1 RADIUS 192.168.46.33 1812 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

add lb vserver radius_acct_vs1 RADIUS 192.168.46.34 1813 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

set lb vserver radius_auth_vs1 RADIUS 192.168.46.33 1812 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

set lb vserver radius_auth_vs1 RADIUS 192.168.46.34 1813 -lbmethod
    TOKEN -rule CLIENT.UDP.RADIUS.USERNAME
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Lastausgleichs- oder Content Switching-Server mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server** oder navigieren Sie zu **Traffic Management > Content Switching > Virtuelle Server>**und konfigurieren Sie einen virtuellen Server.

Konfigurieren von Diensten

Nachdem Sie die virtuellen Server konfiguriert haben, müssen Sie als nächstes zwei Dienste konfigurieren, einen für jeden der von Ihnen erstellten virtuellen Server.

Hinweis: Nach der Konfiguration befinden sich diese Dienste im Status DEAKTIVIERT, bis die Citrix ADC Appliance eine Verbindung mit den Authentifizierungs- und Accounting-IPs Ihres RADIUS-Servers herstellen und deren Status überwachen kann. Anweisungen finden Sie unter Dienste konfigurieren.

Binden virtueller Server an Dienste

Nach der Konfiguration Ihrer Dienste müssen Sie als Nächstes jeden der von Ihnen erstellten virtuellen Server an den entsprechenden Dienst binden.Anweisungen finden Sie unter Binding Services an den virtuellen Server.

Konfigurieren einer Persistenzgruppe für Radius

Nachdem Sie die virtuellen Load Balancing Server an die entsprechenden Dienste gebunden haben, müssen Sie die RADIUS-Lastausgleichskonfiguration so einrichten, dass die Persistenz unterstützt wird. Dazu konfigurieren Sie eine Persistenzgruppe für Lastausgleich, die Ihre virtuellen RADIUS-Load Balancing Server und -Dienste enthält, und konfigurieren Sie diese Lastausgleichspersistenzgruppe für die Verwendung regelbasierter Persistenz. Eine Persistenzgruppe ist erforderlich, da die virtuellen Authentifizierungs- und Buchhaltungsserver unterschiedlich sind und sowohl die Authentifizierungs- als auch die Buchhaltungsnachricht für einen einzelnen Benutzer denselben RADIUS-Server erreichen sollten. Persistenzgruppe ermöglicht es, dieselbe Sitzung für beide virtuellen Server zu verwenden. Anweisungen finden Sie unter Konfigurieren von Persistenzgruppen.

Konfigurieren von RADIUS Shared Secret

Ab Release 12.0 unterstützt eine Citrix ADC Appliance RADIUS Shared Secret. Ein RADIUS-Client und ein Server kommunizieren miteinander über einen gemeinsamen Schlüssel, der auf dem Client und auf dem Server konfiguriert ist. Transaktionen zwischen einem RADIUS-Client und Server werden mithilfe eines Shared Secret authentifiziert. Dieses Geheimnis wird auch verwendet, um einige der Informationen im RADIUS-Paket zu verschlüsseln.

RADIUS-Validierungsszenarien für gemeinsame geheime Schlüssel

Die Validierung des **freigegebenen geheimen RADIUS-Schlüssels** erfolgt in den folgenden Szenarien:

- Der**gemeinsam genutzte geheime RADIUS-Schlüssel ist sowohl für den Radiusclient als auch für den Radius-Server konfiguriert:** Die Citrix ADC Appliance verwendet den geheimen RADIUS-Schlüssel sowohl für die Client- als auch für die Serverseite. Wenn die Überprüfung erfolgreich ist, lässt die Appliance die RADIUS-Nachricht durchlaufen. Andernfalls wird die RADIUS-Nachricht abgelegt.
- Der**gemeinsam genutzte geheime RADIUS-Schlüssel ist weder für den Radiusclient noch für den Radius-Server konfiguriert:** Die Citrix ADC Appliance löscht die RADIUS-Nachricht, da die Freigabe-Secret-Schlüsselüberprüfung nicht auf einem Knoten durchgeführt werden kann, für den kein Radkey konfiguriert ist.
- Der**gemeinsame geheime RADIUS-Schlüssel ist nicht sowohl für den RADIUS-Client als auch für den RADIUS-Server konfiguriert:** Die Citrix ADC Appliance umgeht die Überprüfung des geheimen RADIUS-Schlüssels und ermöglicht das Durchlaufen der RADIUS-Nachrichten.

Sie können einen standardmäßigen RADIUS-gemeinsamen Schlüssel konfigurieren oder auf Client- oder Subnetzbasis konfigurieren. Es wird empfohlen, einen gemeinsam genutzten geheimen RADIUS-Schlüssel für alle Bereitstellungen mit konfigurierter RADIUS-Richtlinie hinzuzufügen. Die Appliance

verwendet die Quell-IP-Adresse des RADIUS-Pakets, um zu entscheiden, welcher gemeinsame Schlüssel verwendet werden soll. Sie können einen RADIUS-Client und Server und den entsprechenden Shared Secret wie folgt konfigurieren:

Geben Sie an der CLI-Eingabeaufforderung Folgendes ein:

```
add radiusNode <clientPrefix/Subnet> -radKey <Shared_secret_key>
<!--NeedCopy-->
```

Argumente

IP-Adresse

IP-Adresse oder Subnetz des RADIUS-Clients im CIDR-Format. Die Appliance verwendet die Quell-IP-Adresse eines eingehenden Anforderungspakets, um der Client-IP-Adresse zuzustimmen. Anstatt eine Client-IP-Adresse zu konfigurieren, können Sie die Client-Netzwerkadresse konfigurieren. Das längste Präfix wird zugeordnet, um den gemeinsamen Schlüssel für eine eingehende Clientanforderung zu identifizieren.

Radkey

Gemeinsamer geheimer Schlüssel zwischen dem Client, der Citrix ADC Appliance und dem Server. Maximale Länge: 31

```
add lb vserver radius_auth_vs1 RADIUS 192.168.46.33 1812 -lbmethod
   TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

add lb vserver radius_acct_vs1 RADIUS 192.168.46.34 1813 -lbmethod
   TOKEN -rule CLIENT.UDP.RADIUS.USERNAME

add service radius_auth_service1 192.168.41.68 RADIUS 1812

add service radius_acct_service1 192.168.41.70 RADIUS 1813

bind lb vserver radius_auth_vs1 radius_auth_service1

bind lb vserver radius_acct_vs1 radius_acct_service[1-3]

add radiusNode 192.168.41.0/24 -radKey  serverkey123

add radiusNode 203.0.113.0/24 -radkey clientkey123
```



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

Ein gemeinsamer Schlüssel muss sowohl für einen RADIUS-Client als auch für einen Server konfiguriert werden. Der Befehl ist derselbe. Das Subnetz bestimmt, ob der gemeinsame Schlüssel für einen Client oder einen Server ist.

Wenn das angegebene Subnetz beispielsweise ein Client-Subnetz ist, gilt der gemeinsame Schlüssel für den Client. Wenn das angegebene Subnetz ein Serversubnetz ist (192.168.41.0/24 im vorherigen Beispiel), ist das Shared Secret für den Server.

Ein Subnetz von 0.0.0.0/0 bedeutet, dass es der Standardgeheimnis für alle Clients und Server ist.

> **Hinweis:**
>
> Nur die PAP- und CHAP-Authentifizierungsmethoden werden mit RADIUS Shared Secret unterstützt.

Persistenzsitzungen anzeigen

October 5, 2021

Sie können die verschiedenen Persistenzsitzungen anzeigen, die global oder für einen bestimmten virtuellen Server gültig sind.

> **Hinweis**: Eine Citrix ADC NCore-Appliance verwendet mehrere CPU-Kerne für die Paketbehandlung. Der CPU-Kern besitzt jede Sitzung auf der Appliance. Wenn die Appliance eine Anforderung erhält, für die keine Sitzung existiert, wird eine Sitzung erstellt, und einer der Kerne wird als Eigentümer dieser Sitzung bezeichnet.
>
> Nachfolgende Anforderungen, die zu dieser Sitzung gehören, kommen möglicherweise nicht immer an und werden vom Eigentümerkern behandelt. In diesem Fall stellt Inter-Core-Messaging sicher, dass die Sitzungsinformationen auf dem Eigentümerkern immer aktuell sind.

Wenn jedoch ein Kern eine Anforderung empfängt, die zu einer Persistenzsitzung gehört, die einem anderen Kern gehört, aktualisiert das Inter-Core-Messaging den Timeout-Wert für die Persistenzsitzung nicht.

In der Ausgabe von sukzessive run show lb persistentSessions -Befehlen, die nur Timeout-Werte von Besitzerkernen anzeigen, kann der Timeout-Wert für eine Persistenzsitzung auf 0 (Null) abnehmen, selbst wenn die Persistenzsitzung aktiv bleibt.

So zeigen Sie Persistenzsitzungen mit der Befehlszeilenschnittstelle an

Um Persistenzsitzungen für alle virtuellen Server anzuzeigen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
show lb persistentSessions [<vServer>]
<!--NeedCopy-->
```

Geben Sie an der Eingabeaufforderung Folgendes ein, um Persistenzsitzungen für einen virtuellen Server anzuzeigen:

```
show lb persistentSessions <vServername>
<!--NeedCopy-->
```

Beispiel:

```
show lb persistentSessions myVserver
<!--NeedCopy-->
```

So zeigen Sie Persistenzsitzungen mit der GUI an

Navigieren Sie zu **Traffic Management** > **Persistente Sitzungen für virtuelle Server**.

Persistenzsitzungen löschen

October 5, 2021

Möglicherweise müssen Sie Persistenzsitzungen von der Citrix ADC Appliance löschen, wenn ein Timeout für Sitzungen fehlschlägt. Sie haben folgende Optionen:

- Löschen Sie alle Sitzungen für alle virtuellen Server gleichzeitig.
- Löschen Sie alle Sitzungen für einen bestimmten virtuellen Server auf einmal.
- Löschen Sie eine bestimmte Sitzung, die einem bestimmten virtuellen Server zugeordnet ist.

So löschen Sie eine Persistenzsitzung mit der Befehlszeilenschnittstelle

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


```
clear lb persistentSessions [<vServer> [-persistenceParam <string>]]

show persistentSessions <vServer>
<!--NeedCopy-->
```

Beispiele:

Beispiel 1 löscht alle Persistenzsitzungen für den Lastenausgleich des virtuellen Servers lbvip1.

Beispiel 2 zeigt zuerst die Persistenzsitzungen für den Lastenausgleich des virtuellen Servers lbvip1 an, löscht die Sitzung mit dem Persistenzparameter xls und zeigt dann die Persistenzsitzungen an, um zu überprüfen, ob die Sitzung gelöscht wurde.

Beispiel 1:

```
> clear persistentSessions lbvip1
 Done
> show persistentSessions
 Done
>
<!--NeedCopy-->
```

Beispiel 2:

```
> show persistentSessions lbvip1
Type        SRC-IP    ...    PERSISTENCE-PARAMETER
RULE        0.0.0.0   ...    xls
RULE        0.0.0.0   ...    txt
RULE        0.0.0.0   ...    html
 Done
> clear persistentSessions lbvip1 -persistenceParam xls
 Done
> show persistentSessions lbvip1
Type        SRC-IP    ...    PERSISTENCE-PARAMETER
RULE        0.0.0.0   ...    txt
RULE        0.0.0.0   ...    html
 Done
>
<!--NeedCopy-->
```


So löschen Sie Persistenzsitzungen mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Persistente Sitzungen löschen**.

Überschreiben der Persistenzeinstellungen für überladene Dienste

October 5, 2021

Wenn ein Dienst ausgelastet ist oder anderweitig nicht verfügbar ist, wird der Dienst für Clients herabgesetzt. In diesem Fall müssen Sie möglicherweise die Citrix ADC Appliance so konfigurieren, dass die Anforderungen, die sonst in die Persistenzsitzung aufgenommen würden, die mit dem überladenen Dienst verknüpft ist, vorübergehend an andere Dienste weiterleitet. Mit anderen Worten, Sie müssen möglicherweise die Persistenzeinstellung überschreiben, die für den virtuellen Lastausgleichsserver konfiguriert ist. Sie können diese Funktionalität erreichen, indem Sie den Parameter Skippersistency festlegen. Wenn dieser Skippersistence-Parameter festgelegt ist und der virtuelle Server neue Verbindungen für einen überlasteten Dienst erhält, passiert Folgendes.

- Der virtuelle Server ignoriert alle vorhandenen Persistenzsitzungen, die mit diesem Dienst verknüpft sind, bis der Dienst in einen Status zurückkehrt, in dem er Anfragen annehmen kann.
- Persistenzsitzungen, die mit anderen Diensten verknüpft sind, sind nicht betroffen.

Diese Funktion ist nur für virtuelle Server verfügbar, deren Typ ANY oder UDP ist.

In Branch Repeater Lastausgleich-Konfigurationen müssen Sie auch einen Lastmonitor konfigurieren und ihn an den Dienst binden. Der Monitor nimmt den Dienst aus nachfolgenden Lastausgleichsentscheidungen heraus, bis die Last auf dem Dienst unter den konfigurierten Schwellenwert gebracht wird. Informationen zum Konfigurieren eines Lastmonitors für Ihren virtuellen Server finden Sie unter Grundlegendes zu Lastmonitoren.

Sie können den virtuellen Server so konfigurieren, dass er eine der folgenden Aktionen mit den Anforderungen durchführt, die andernfalls Teil der Persistenzsitzung wären:

- **Senden Sie jede Anfrage an einen der anderen Dienste.** Der virtuelle Server trifft eine Lastenausgleichsentscheidung und sendet jede Anforderung basierend auf der Load Balancing-Methode an einen der anderen Dienste. Wenn alle Dienste überlastet sind, werden Anforderungen gelöscht, bis ein Dienst verfügbar ist.

  Sowohl Platzhalter- als auch IP-Adressenbasierte virtuelle Server unterstützen diese Option. Diese Aktion ist für alle Bereitstellungen geeignet, einschließlich Bereitstellungen, in denen der virtuelle Server Branch Repeater Appliances oder Firewalls Lastausgleich ausführt.

- **Umgehen Sie die Konfiguration des virtuellen Server-Services.** Der virtuelle Server trifft keine Lastausgleichsentscheidung. Stattdessen überbrückt es einfach jede Anforderung an einen physischen Server basierend auf der Ziel-IP-Adresse in der Anforderung.

Nur virtuelle Wildcard-Server vom Typ ANY und UDP unterstützen die Umgehungsoption. Virtuelle Wildcard-Server haben eine *:* IP- und Portkombination. Diese Aktion ist für Bereitstellungen geeignet, in denen Sie den virtuellen Server zum Lastenausgleich von Branch Repeater-Appliances oder Firewalls verwenden. In diesen Bereitstellungen leitet die Citrix ADC Appliance zunächst eine Anforderung an eine Branch Repeater-Appliance oder eine Firewall weiter und leitet die verarbeitete Antwort dann an einen physischen Server weiter. Der virtuelle Server sendet Anfragen unter den folgenden Bedingungen direkt an seine Ziel-IP-Adressen.

- Sie konfigurieren den virtuellen Server so, dass er die Konfiguration des virtuellen Server-Servers für überladene Dienste Bypass.
- Die Branch Repeater Appliance oder Firewall wird überlastet.

Der virtuelle Server sendet Anfragen direkt an seine Ziel-IP-Adressen, bis die Branch Repeater Appliance oder Firewall Anfragen annehmen kann.

So überschreiben Sie Persistenzeinstellungen für überlastete Dienste über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um Persistenzeinstellungen für überladene Dienste außer Kraft zu setzen und die Konfiguration zu überprüfen:

```
set lb vserver <name> -skippersistency <skippersistency>

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

Beispiel

```
> set lb vserver mylbvserver -skippersistency ReLb
 Done
> show lb vserver mylbvserver
    mylbvserver (\*:\*) - ANY Type: ADDRESS
      . . .
      . . .
 Skip Persistency: ReLb
      . . .
 Done
>
<!--NeedCopy-->
```


So überschreiben Sie Persistenzeinstellungen für überlastete Dienste über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server** und wählen Sie den virtuellen Server vom Typ UDP oder ANY aus.
2. Wählen Sie im Bereich Erweiterte Einstellungen die Option Verkehrseinstellungen aus, und geben Sie den Typ der Persistenz überspringen an.

Problembehandlung

October 5, 2021

- **Die Statistiken der Citrix ADC VPX Appliance zeigen an, dass die Appliance das Limit der Sitzungspersistenz erreicht hat. Infolgedessen schlagen Persistenzsitzungen fehl. Ist es möglich, das Sitzungspersistenzlimit zu erhöhen?**

  Ursache: Die Citrix ADC Appliance hat die Systemgrenze von 250.000 Persistenzsitzungen für einen Kern.

  Lösung: Um dieses Problem zu beheben, können Sie eine der folgenden Aufgaben ausführen:

  - Reduzieren Sie den Timeout-Wert für Persistenz
  - Erhöhen Sie die Anzahl der Kerne für die Appliance

- **Nach der Konfiguration der Cookie-Insert-Persistenz auf der Citrix ADC Appliance melden die Benutzer, dass die Verbindungen für einige Zeit einwandfrei funktionieren, beginnen aber dann getrennt zu werden. Welche bewährten Methoden sollte ich bei der Konfiguration der Persistenz beachten?**

  Ursache: Standardmäßig beträgt der Timeoutwert für Cookie-Insert-Persistenz 120 Sekunden.

  Lösung: Wenn Sie Persistenz für Anwendungen konfigurieren, für die die Leerlaufzeit nicht ermittelt werden kann, setzen Sie den Wert für die Persistenz-Timeoutwert für Cookie Insert auf 0. Mit dieser Einstellung führt die Verbindung kein Timeout aus.

- **Nachdem ich einen virtuellen HTTP-Server auf der Citrix ADC Appliance konfiguriert habe, muss ich sicherstellen, dass ein Benutzer immer eine Verbindung zum gleichen Server für den angeforderten Inhalt herstellt. Daher habe ich die SourceIP Persistenz konfiguriert. Das Erhöhen des Timeoutwerts für die Persistenz führt nun zu Latenz. Wie kann ich den Timeout-Wert erhöhen, ohne die Leistung zu beeinträchtigen?**

  Lösung: Erwägen Sie die Verwendung von Cookie-Insert-Persistenz mit dem Timeout-Wert auf 0. Mit dieser Einstellung werden die Persistenzeinstellungen für lange Dauer aktiviert, da die Appliance keine Zeit für den Ablauf des Cookies angibt.

- **Nach der Konfiguration der Cookie-Insert-Persistenz auf der Citrix ADC Appliance funktioniert sie erwartungsgemäß, wenn Clients aus derselben Zeitzone auf den Inhalt zugreifen. Wenn jedoch ein Client aus einer anderen Zeitzone versucht, eine Verbindung herzustellen, wird die Verbindung sofort Timeout.**

  Ursache: Die zeitbasierte Cookie-Insert-Persistenz funktioniert wie erwartet, wenn ein Client aus derselben Zeitzone eine Verbindung herstellt. Wenn sich der Clientcomputer und die Citrix ADC Appliance jedoch in verschiedenen Zeitzonen befinden, ist das Cookie ungültig. Wenn beispielsweise ein Client in der EST-Zeitzone um 11:00 Uhr EST ein Cookie an eine Citrix ADC Appliance in der PST-Zeitzone sendet, erhält die Appliance das Cookie um 14:00 Uhr PST. Aufgrund des Zeitunterschieds ist das Cookie nicht gültig und die Verbindung ist sofort Timeout.

  Auflösung: Setzen Sie den Timeout-Wert für Cookie-Insert-Persistenz auf 0.

- **Eine Citrix ADC Appliance wird zum Lastenausgleich von Anwendungsservern wie dem Oracle Weblogic-Server verwendet. Um sicherzustellen, dass Clients persistente Verbindungen zu diesen Servern erhalten, wird SourceIP Persistenz konfiguriert. Es funktioniert wie erwartet, wenn eine Verbindung von einem Computer hergestellt wird. Wenn Thin Clients jedoch eine Verbindung über einen Terminalserver herstellen und infolgedessen empfängt die Appliance Anfragen von mehreren Clients von derselben IP-Adresse (der IP-Adresse des Terminalservers). Daher werden die Verbindungen von allen Thin Clients auf denselben Anwendungsserver geleitet. Ist es möglich, Persistenz für Anfragen einzelner Thin Clients basierend auf der Client-IP-Adresse zu konfigurieren?**

  Ursache: Die Citrix ADC Appliance empfängt Anforderungen vom Terminalserver und die Quell-IP-Adresse der Anforderung bleibt unverändert. Daher kann die Appliance nicht zwischen den von den Thin Clients empfangenen Anforderungen unterscheiden und Persistenz entsprechend den Anforderungen von Thin Clients bereitstellen.

  Lösung: Um dieses Problem zu vermeiden, können Sie die Persistenz der Regel basierend auf einem eindeutigen Parameterwert für jeden Thin Client konfigurieren.

- **Die Citrix ADC Appliance wird zum Lastenausgleich von Webinterface-Servern verwendet. Beim Zugriff auf die Server erhält der Benutzer die Fehlermeldung Statusfehler. Darüber hinaus, wenn einer der Webinterface-Server heruntergefahren oder nicht verfügbar ist, erhalten einige der Benutzer eine Fehlermeldung.**

  Ursache: Mangelnde Persistenz auf den Webinterface-Servern kann zu Fehlermeldungen führen, wenn ein Benutzer versucht, eine Verbindung mit dem Server herzustellen.

  Lösung: Citrix empfiehlt, dass Sie die Cookie-Insert-Persistenzmethode auf der Citrix ADC Appliance beim Lastenausgleich von Webinterface-Servern angeben.

Einfügen von Cookie-Attributen zu ADC-generierten Cookies

December 7, 2021

Die Webadministratoren können andere Cookie-Attribute in die von der Citrix ADC Appliance generierten Cookies einfügen. Diese zusätzlichen Cookie-Attribute helfen bei der Durchsetzung der erforderlichen Richtlinien für die von ADC generierten Cookies basierend auf dem Anwendungszugriffsmuster.

Die folgenden Funktionen verwenden die vom ADC generierten Cookies, um Persistenz zu erreichen.

- Load Balancing-Cookie-Persistenz
- Ausgleichsgruppen-Cookie-Persistenz
- GSLB-Standort-Beharrlichkeit
- Cookie-Persistenz beim Content Switching

Sie können mit den folgenden Parametern andere Cookie-Attribute in die von ADC generierten Cookies einfügen:

- **literalAdcCookieAttribute:** Hängen Sie andere Cookie-Attribute als String an das von ADC generierte Cookie an.
- **ComputedADCCookieAttribute:** Verwenden Sie eine ADC ns-Variable, um Cookie-Attribute an das von ADC generierte Cookie anzuhängen, basierend auf den Client- oder Serverattributen, z. B.

> **Hinweis:**
>
> Sie können sowohl das literale ADC-Cookie-Attribut als auch das berechnete ADC-Cookie-Attribut nicht gleichzeitig für den Lastausgleichsparameter oder in einem einzigen Lastausgleichsprofil konfigurieren.

Anwendungsfall: Konfigurieren des SameSite-Cookie-Attri

Mit jedem Cookie ist eine Domain verknüpft. Wenn die Domäne eines Cookies mit der Website-Domain in der Adressleiste des Benutzers übereinstimmt, wird dies als Kontext derselben Site (oder Erstanbieter) betrachtet. Wenn die mit einem Cookie verknüpfte Domain mit einem externen Dienst und nicht mit der Website in der Adressleiste des Benutzers übereinstimmt, gilt dies als standortübergreifender Kontext (oder Drittanbieter).

Das **SameSite-Attribut** gibt dem Browser an, ob das Cookie für standortübergreifenden Kontext oder nur für den gleichen Site-Kontext verwendet werden kann. Wenn eine Anwendung beabsichtigt, im standortübergreifenden Kontext zugegriffen zu werden, kann sie dies nur über die HTTPS-Verbindung tun. Weitere Informationen finden Sie unter RFC6265.

Bis Februar 2020 wurde die **SameSite-Eigenschaft** nicht explizit in Citrix ADC festgelegt. Der Browser nahm den Standardwert “Keine” an und hat keine Auswirkungen auf die Citrix ADC Bereitstellungen.

Bei einem Upgrade bestimmter Browser, wie Google Chrome 80, ändert sich jedoch das standardmäßige domänenübergreifende Verhalten von Cookies. Das **SameSite-Attribut** kann auf einen der folgenden Werte festgelegt werden. Der Standardwert für Google Chrome ist auf Lax festgelegt.

- **Keine:** Zeigt an, dass der Browser ein Cookie im siteübergreifenden Kontext nur für sichere Verbindungen verwendet.
- **Lax:** Zeigt an, dass der Browser ein Cookie für Anfragen im Kontext derselben Website verwendet. Im Cross-Site-Kontext können nur sichere HTTP-Methoden wie GET-Request das Cookie verwenden.
- **Streng:** Verwenden Sie das Cookie nur im Kontext derselben Site.

Wenn das Cookie kein SameSite -Attribut enthält, geht Google Chrome von der Funktionalität von SameSite =LAX aus.

> **Hinweis:**
>
> Für bestimmte Versionen anderer Browser ist der Standardwert für das SameSite-Attribut möglicherweise auf **Keine**festgelegt. In einigen Browser-Versionen kann “SameSite = none” anders behandelt werden. Beispielsweise lehnen die folgenden Browser ein Cookie mit “SameSite = none” ab:
>
> - Versionen von Chrome von Chrome 51 bis Chrome 66 (an beiden Enden inklusive)
> - Versionen des UC-Browsers auf Android vor Version 12.13.2

Konfigurieren von ADC-generierten Cookies

Um ADC-generierte Cookie-Attribute zu konfigurieren, müssen Sie Folgendes ausführen:

1. Erstellen eines virtuellen Lastausgleichsservers
2. Legen Sie die ADC-Cookie-Attribute für den virtuellen Lastausgleichsserver fest, entweder über LB-Parameter oder über das LB-Profil.
3. Wenn Sie ein LB-Profil verwenden, legen Sie das LB-Profil auf einen virtuellen Lastausgleichsserver fest.
4. Wenn Sie das Cookie-Attribut für berechnete ADC verwenden, konfigurieren Sie die zugehörige Richtlinie zum Umschreiben.

> **Hinweis:**
>
> Wenn ein LB-Profil an einen virtuellen LB-Server gebunden ist, wird die Profilparameterkonfiguration anstelle der globalen LB-Parameterkonfiguration berücksichtigt.

Sie können die vom ADC generierten Cookie-Attribute auf folgende Weise festlegen:

- Festlegen der ADC-Cookie-Attribute in Lastenausgleichsparametern

- Festlegen der ADC-Cookie-Attribute im Load Balancing-Profil

Festlegen der ADC-Cookie-Attribute in den Lastenausgleichsparametern über die Befehlszeilenschnittstelle

Um eine Richtlinie einheitlich auf von ADC generierte Cookies aller auf der Citrix ADC Appliance konfigurierten Anwendungen anzuwenden, können Sie das ADC-Cookie-Attribut in den globalen LB-Parametern festlegen.

Die Einstellung **Literal ADC Cookie Attribut** ermöglicht es Ihnen, die Cookie-Attribute bedingungslos in das von ADC generierte Cookie einzufügen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set lb parameter -LiteralADCCookieAttribute <string>
2 <!--NeedCopy-->
```

Beispiel:

```
1 set lb parameter -LiteralADCCookieAttribute SameSite=None
2 <!--NeedCopy-->
```

Die Einstellung **“Berechnetes ADC-Cookie-Attribut”** ermöglicht es Ihnen, die Cookie-Attribute basierend auf den Client- oder Serverattributen in das von ADC generierte Cookie einzufügen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set lb parameter -ComputedADCCookieAttribute <ns variable>
2 <!--NeedCopy-->
```

Beispiel:

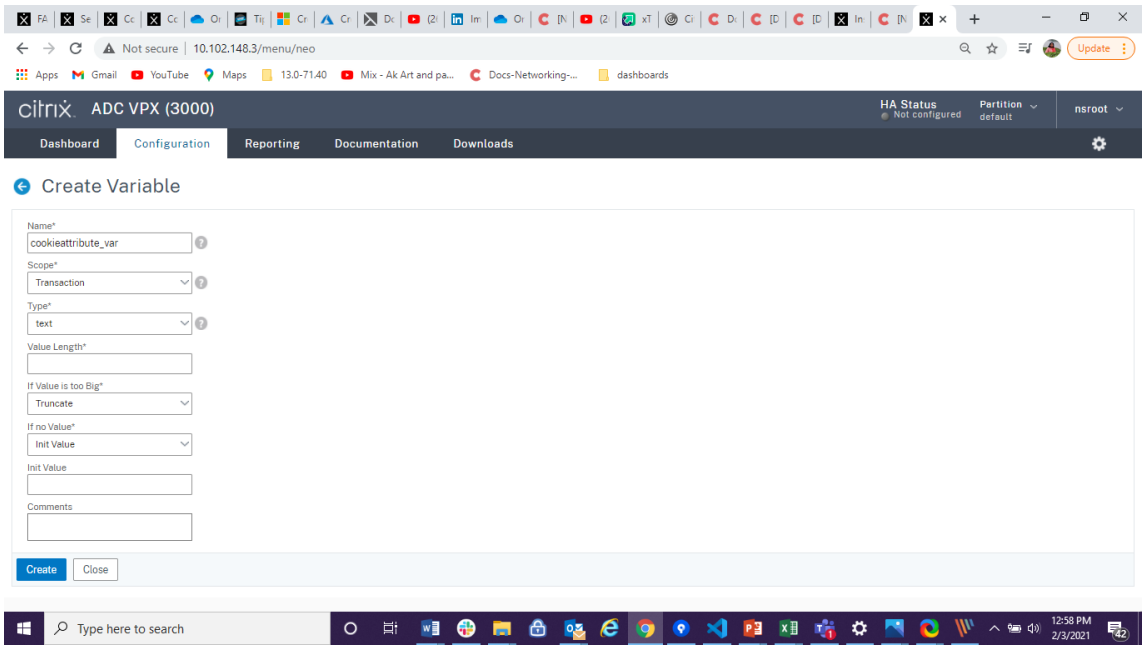
```
1 add ns variable cookieattribute_var -type ”text(100)” -scope
     transaction
2 set lb parameter -ComputedADCCookieAttributE ”$cookieattribute_var”
3 add ns assignment samesiteassign -variable ”$cookieattribute_var” -set
     ””SameSite=None””
4
```



```
5  add policy expression pol_iphone "(HTTP.REQ.HEADER("User-Agent").
       CONTAINS("iP") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/OS
       \d+\\_/).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).EQ(12).
       typecast_text_t ALT "false").eq("true"))"
6  add policy expression pol_chrome "(HTTP.REQ.HEADER("User-Agent").
       CONTAINS("Chrom") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/
       Chrom.*\d+./).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).BETWEEN
       (51,66).typecast_text_t ALT "false").eq("true"))"
7  add rewrite policy exception_samesite_attribute "pol_iphone ||
       pol_chrome " NOREWRITE
8  add rewrite policy append_samesite_attribute true samesiteassign
9
10 bind rewrite global exception_samesite_attribute 90 110 -type
       RES_OVERRIDE
11 bind rewrite global append_samesite_attribute 100 110 -type
       RES_OVERRIDE
12 <!--NeedCopy-->
```

Konfigurieren von Variablen mit der GUI

1. Navigieren Sie zu **AppExpert > Variables**, und klicken Sie auf **Hinzufügen**.
2. Wählen **Sie auf der Seite "Variable erstellen** " im Dropdownmenü **Geltungsbereich** als **Transaktion** und als **Text eingeben** aus.

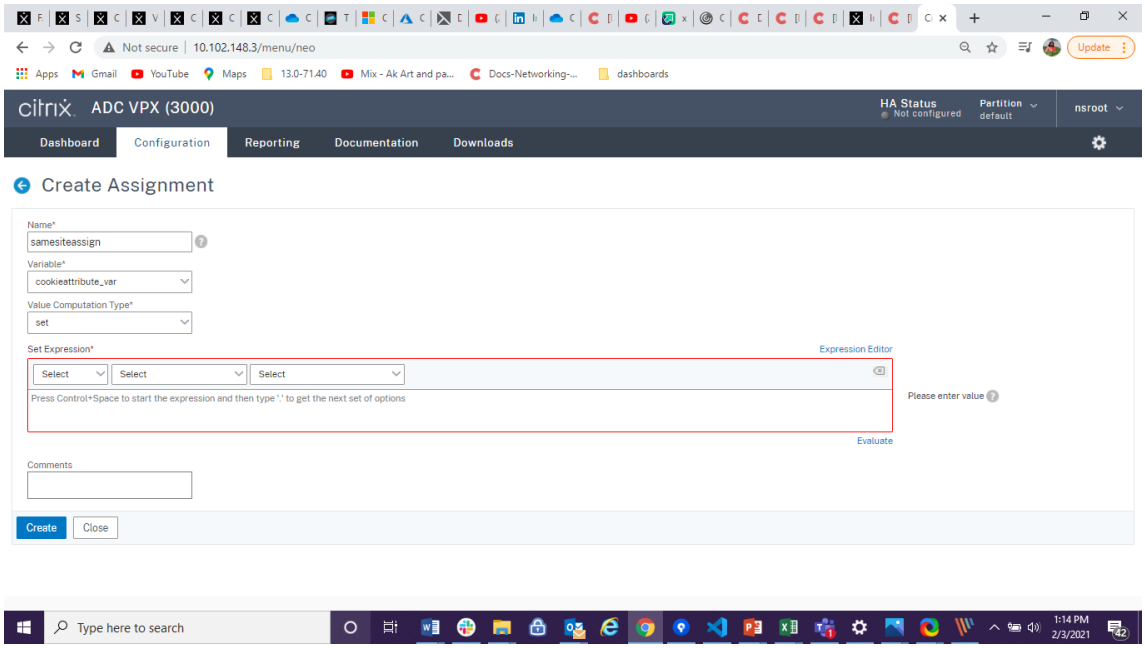


3. Geben Sie weitere Details ein und klicken Sie auf **Erstellen**.

Erstellen einer Aufgabe mit der GUI

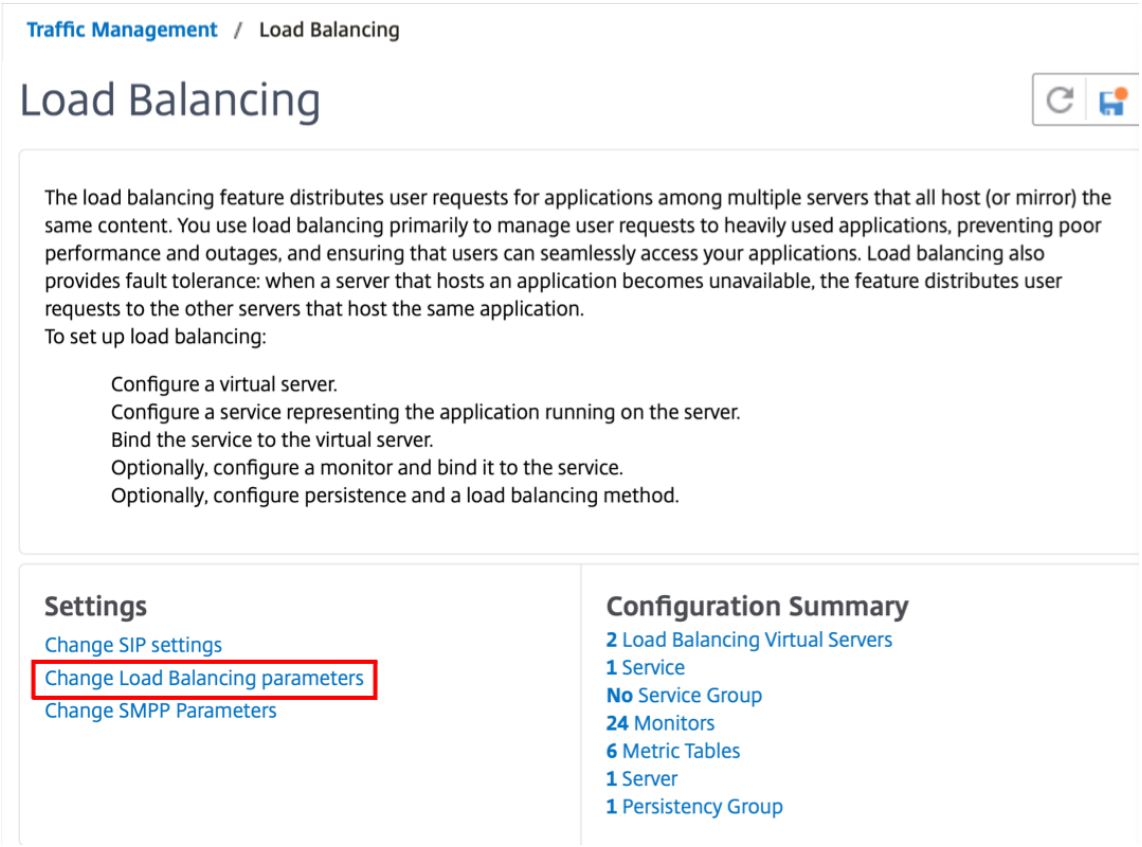
Nachdem Sie eine Variable konfiguriert haben, können Sie einen Wert zuweisen oder die Operation angeben, die für die Variable ausgeführt werden soll, indem Sie eine Zuweisung erstellen.

1. Navigieren Sie zu **AppExpert > Zuweisungen**und klicken Sie auf **Hinzufügen**.
2. Geben **Sie auf der Seite Zuweisung erstellen** die Details ein und klicken Sie auf **Erstellen**.



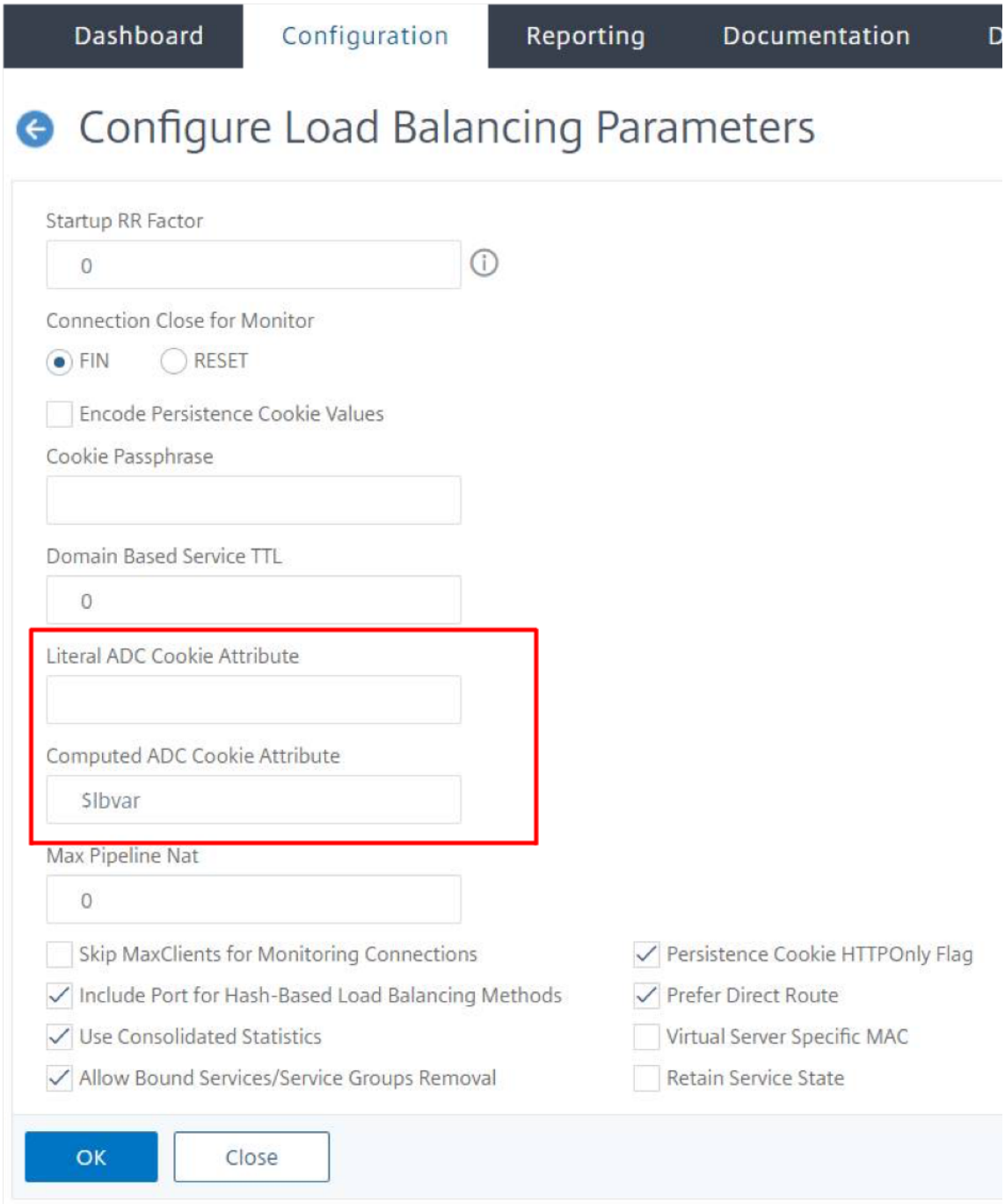
Festlegen der ADC-Cookie-Attribute in Lastenausgleichsparametern über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > Load Balancing > Load Balancing-Parameter ändern**.



2. Geben **Sie im Bereich Load Balancing-Parameter konfigurieren** die entsprechenden Werte für eines der Felder ein, basierend auf Ihren Anforderungen:

   - **Literales ADC-Cookie-Attribut**
   - **Berechnetes ADC-Cookie-Attribut**



3. Klicken Sie auf **OK**.

Festlegen der ADC-Cookie-Attribute im Load Balancing-Profil über die Befehlszeilenschnittstelle

Um eine Richtlinie für eine bestimmte Anwendung anzuwenden, die auf der Citrix ADC Appliance konfiguriert ist, können Sie die Cookie-Attributparameter im LB-Profil festlegen, das an den anwen-

dungsspezifischen virtuellen LB-Server gebunden ist.

Die Einstellung **Literal ADC Cookie Attribute** im LB-Profil ermöglicht es Ihnen, die Cookie-Attribute bedingungslos in das von ADC generierte Cookie einzufügen, das für einen virtuellen Server spezifisch ist.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb profile <profile name> -LiteralADCCookieAttribute <string>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add lb profile LB-Vserver-Profile-1 -LiteralADCCookieAttribute SameSite
     =None
2 add lb vserver LB-VServer-1 SSL 10.102.148.37 443 -persistenceType
     COOKIEINSERT -lbprofilename LB-Vserver-Profile-1
3 <!--NeedCopy-->
```

Die Einstellung **“Berechnetes ADC-Cookie-Attribut”** im LB-Profil ermöglicht es Ihnen, die Cookie-Attribute basierend auf den Client- oder Serverattributen in das ADC-generierte Cookie einzufügen. Stellen Sie dieses LB-Profil dann auf einen virtuellen LB-Server ein.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb profile <profile name> -ComputedADCCookieAttribute <ns variable>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add ns variable cookieattribute_var -type ”text(100)” -scope
     transaction
2 add ns assignment samesiteassign -variable ”$cookieattribute_var” -set
     ””SameSite=None””
3 add lb profile LB-Vserver-Profile-1 -ComputedADCCookieAttributE ”
     $cookieattribute_var”
4
5 add policy expression pol_iphone ”(HTTP.REQ.HEADER(”User-Agent”).
     CONTAINS(”iP”) && (HTTP.REQ.HEADER(”User-Agent”).REGEX_SELECT(re/OS
     \d+\\_/).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).EQ(12).
     typecast_text_t ALT ”false”).eq(”true”))”
```

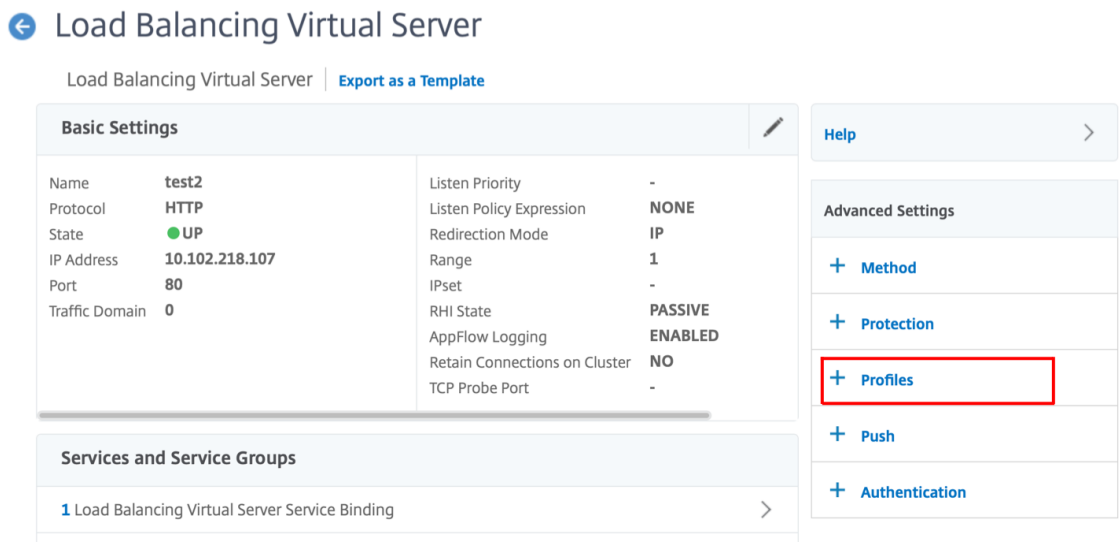


```
add policy expression pol_chrome "(HTTP.REQ.HEADER("User-Agent").
    CONTAINS("Chrom") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/
    Chrom.*\d+./).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).BETWEEN
    (51,66).typecast_text_t ALT "false").eq("true"))"
add rewrite policy exception_samesite_attribute "pol_iphone ||
    pol_chrome " NOREWRITE
add rewrite policy append_samesite_attribute true samesiteassign

add lb vserver LB-VServer-1 SSL 10.102.148.37 443 -persistenceType
    COOKIEINSERT -lbprofilename LB-Vserver-Profile-1
bind lb vserver LB-VServer-1 -policyName exception_samesite_attribute -
    priority 90 -gotoPriorityExpression 110 -type RESPONSE
bind lb vserver LB-VServer-1 -policyName append_samesite_attribute -
    priority 100 -gotoPriorityExpression 110 -type RESPONSE
<!--NeedCopy-->
```

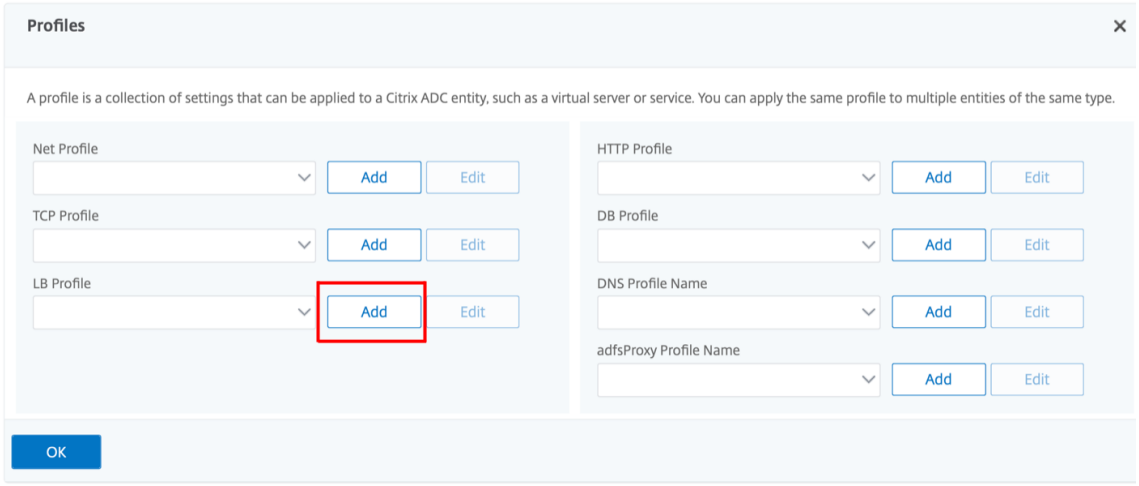
Festlegen der ADC Cookie-Attribute im Load Balancing-Profil über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie einen virtuellen Server aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Profile hinzufügen**.



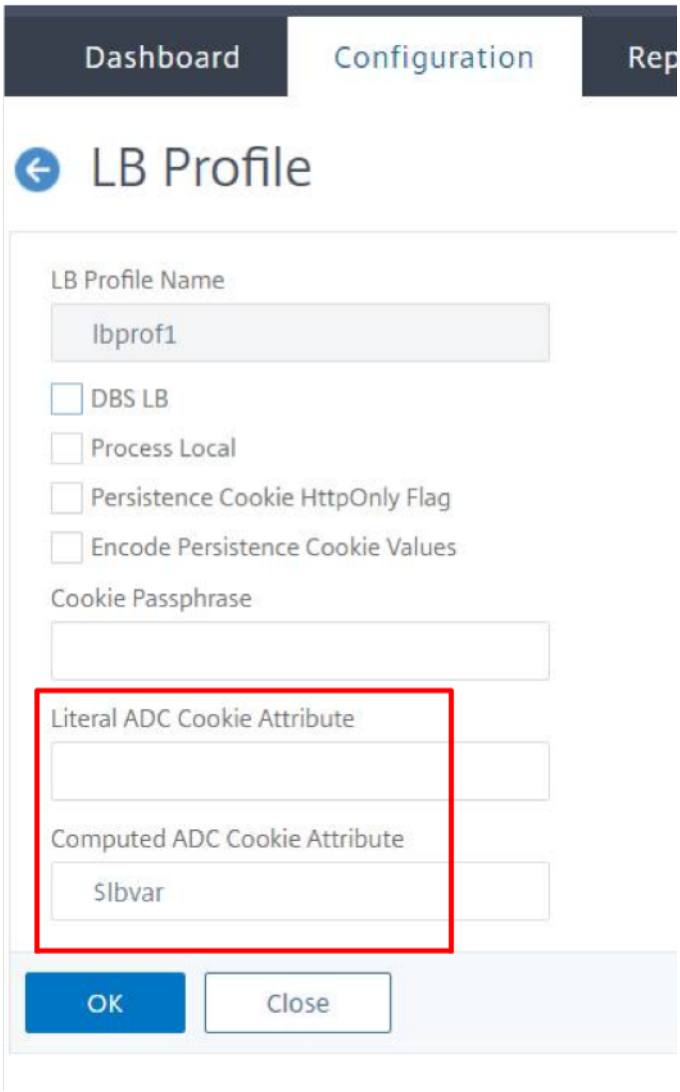
4. Klicken Sie im Abschnitt **Profile** auf **Hinzufügen**, um ein LB-Profil zu erstellen.

   Wenn Sie bereits ein Profil erstellt haben, wählen Sie es aus dem Dropdownmenü **LB-Profil** aus.



5. Geben Sie im Bereich **LB-Profil** die entsprechenden Werte für eines der Felder ein, die auf Ihrer Anforderung basieren:

- **Literales ADC-Cookie-Attribut**
- **Berechnetes ADC-Cookie-Attribut**



1. Klicken Sie auf **OK**.
2. Legen Sie das erstellte LB-Profil auf den in **Schritt 1**erstellten virtuellen LB-Server fest.

Überprüfen der ns-Variablen

Um zu überprüfen, ob die ADC nss-Variable in LB-Parametern oder LB-Profil angemessen konfiguriert ist, verwenden Sie den Parameter show lb oder show lb profile.

In der folgenden Tabelle sind die verschiedenen Warnmeldungen und deren Ursache aufgeführt, wenn die Variable ns nicht korrekt konfiguriert ist.

Warnmeldung	Gründe
Die NS-Variable ist nicht konfiguriert. Konfigurieren Sie es mit Typ text () und Scope Transaction für Variable	Die NS-Variable ist noch nicht konfiguriert.
Der Umfang der konfigurierten NS-Variablen ist keine Transaktion.	Variable ist konfiguriert, aber der Bereich ist nicht auf “Transaktion” festgelegt.
Der Typ der Variablen ist nicht Text ().	Variable ist konfiguriert, aber der Typ ist nicht auf “Text” gesetzt.
Die konfigurierte Wert-Max-Größe für die NS-Variable ist größer als 255.	Der für die NS-Variable konfigurierte Wert beträgt mehr als 255 Zeichen. **Hinweis:** Eine maximale Länge von 255 Zeichen kann an ein ADC-generiertes Cookie angehängt werden. Die Zeichen, die die maximale Länge überschreiten, werden abgeschnitten.

Beispiel-Ausgabe

Im folgenden Beispiel wird die Warnmeldung angezeigt, wenn die ns-Variable nicht konfiguriert ist.

```
1 set lb parameter -ComputedADCCookieAttribute ”$lbvar”
2
3 Warning: NS Variable is not configured. Please configure it with type
     text() and scope transaction
4 Done
5 <!--NeedCopy-->
```

Die Warnmeldung wird in der folgenden Ausgabe des Befehls `show lb parameter` angezeigt.

```
1 show lb parameter
2
3 Global LB parameters:
4 Persistence Cookie HttpOnly Flag: ENABLED
5 Use Encrypted Persistence Cookie: DISABLED
6 Use Port For Hash LB: YES
7 Prefer direct route: YES
8 Retain Service State: OFF
9 Start RR Factor: 0
```



```
Skip Maxclient for Monitoring: DISABLED
Monitor Connection Close: FIN
Use consolidated stats for LeastConnection: YES
Allow mac mode based vserver to pick thereturn traffic from services:
    DISABLED
Allow bound service removal: ENABLED
TTL for Domain Based Server: 0 secs

Citrix ADC Cookie Variable Name: $lbvar(NS Variable is not configured.
    Please configure it with type text() and scope transaction)

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

Beispielkonfiguration zum Einfügen von Cookie-Attributen in die GSLB-Bereitstellung

Die folgende Beispielkonfiguration gilt für die Site-Persistenz, die auf GSLB-Diensten konfiguriert ist, die einem virtuellen LB-Server entsprechen. Um einige zusätzliche Cookie-Attribute an die GSLB-Cookies anzuhängen, führen Sie die folgende Konfiguration durch.

- Legen Sie die ADC-Cookie-Attribute im LB-Profil (LB-VServer-Profile-1) fest.
- Legen Sie den Wert des Literal ADC Cookie-Attributs fest, z. B. “SameSite=None”, im LB-Profil.
- Legen Sie das LB-Profil auf den virtuellen Lastausgleichsserver (LB-vServer-1) fest, der den GSLB-Dienst darstellt.

```
add gslb vserver GSLB-VServer-1 SSL -backupLBMethod ROUNDROBIN -
    tolerance 0 -appflowLog DISABLED
add gslb site site1 10.102.148.4 -publicIP 10.102.148.4
add gslb service site1_gsvc1 10.102.148.35 SSL 443 -publicIP
    10.102.148.35 -publicPort 443 -maxClient 0 -siteName site1 -
    sitePersistence HTTPRedirect -sitePrefix ss1 -cltTimeout 180 -
    svrTimeout 360 -downStateFlush ENABLED

bind gslb vserver GSLB-VServer-1 -serviceName site1_gsvc1
bind gslb vserver GSLB-VServer-1 -domainName www.gslb.com -TTL 5

add service service-1 10.102.84.140 SSL 443

add lb profile LB-Vserver-Profile-1 -LiteralADCCookieAttribute SameSite
    =None
add lb vserver LB-VServer-1 SSL 10.102.148.37 443 -persistenceType
    COOKIEINSERT -lbprofilename LB-Vserver-Profile-1
```



```
12
13 bind lb vserver LB-VServer-1 service-1
14 <!--NeedCopy-->
```

> **Hinweis:**
>
> Sie können die Cookie-Attribute auch bedingt mit dem Berechneten ADC-Cookie-Attribut einfügen.

Beispielkonfiguration für das Einfügen des Cookie-Attributs in die Content Switching-Bereitstellung

Die folgende Beispielkonfiguration gilt, wenn mehrere Anwendungen hinter einem virtuellen Content Switching-Server gehostet werden. Um dieselbe Richtlinie auf alle Anwendungen anzuwenden, binden Sie die Umschreibrichtlinien wie folgt an den virtuellen Content Switching-Server anstelle des virtuellen LB-Servers:

- Setzen Sie die ADC-Cookie-Attribute in den LB-Parametern.

  > **Hinweis:**
  >
  > Sie können die ADC-Cookie-Attribute auch im LB-Profil festlegen.

- Konfigurieren Sie die ns-Variable (cookieattribute_var) des Typs, der auf Text und Scope auf Transaktion festgelegt ist.
- Setzen Sie das Berechnete ADC-Cookie-Attribut in den globalen LB-Parametern mithilfe der ns-Variablen.
- Legen Sie die Rewrite-Richtlinien (exception_samesite_attribute und append_samesite_attribute) auf die virtuellen Content Switching-Server für das Einfügen der Cookie-Attribute fest.

```
1 add ns variable cookieattribute_var -type "text(100)" -scope
     transaction
2 set lb parameter -ComputedADCCookieAttributE "$cookieattribute_var"
3 add ns assignment samesiteassign -variable "$cookieattribute_var" -set
     ""SameSite=None""
4
5 add policy expression pol_iphone "(HTTP.REQ.HEADER("User-Agent").
     CONTAINS("iP") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/OS
     \d+\\_/).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).EQ(12).
     typecast_text_t ALT "false").eq("true"))"
6 add policy expression pol_chrome "(HTTP.REQ.HEADER("User-Agent").
     CONTAINS("Chrom") && (HTTP.REQ.HEADER("User-Agent").REGEX_SELECT(re/
```



```
    Chrom.*\d+./).REGEX_SELECT(re/\d+/).TYPECAST_NUM_T(DECIMAL).BETWEEN
    (51,66).typecast_text_t ALT "false").eq("true"))"
add rewrite policy exception_samesite_attribute "pol_iphone ||
    pol_chrome " NOREWRITE
add rewrite policy append_samesite_attribute true samesiteassign

add lb vserver LB-VServer-1 SSL 10.102.148.35 443
add lb vserver LB-VServer-2 SSL 10.102.148.36 443

add cs vserver CS-VServer-1 SSL 10.102.148.42 443 -persistenceType
    COOKIEINSERT

add cs action act1 -targetLBVserver v1
add cs action act2 -targetLBVserver v2
add cs policy CS-policy-1 -rule "HTTP.REQ.URL.CONTAINS("file1.html")" -
    action act1
add cs policy CS-policy-2 -rule "HTTP.REQ.URL.CONTAINS("file2.html")" -
    action act2

bind cs vserver CS-VServer-1 -policyName CS-policy-1 -priority 1
bind cs vserver CS-VServer-1 -policyName CS-policy-2 -priority 2

bind cs vserver -policyname exception_samesite_attribute 90 110 -type
    RES_OVERRIDE
bind cs vserver -policyname append_samesite_attribute 100 110 -type
    RES_OVERRIDE
<!--NeedCopy-->
```

Anpassen einer Lastausgleichskonfiguration

October 5, 2021

Nachdem Sie ein grundlegendes Load Balancing-Setup konfiguriert haben, können Sie mehrere Änderungen daran vornehmen, damit die Last genau nach Bedarf verteilt wird. Das Lastenausgleichs-Feature ist komplex. Sie können die Grundelemente ändern, indem Sie eine oder mehrere der folgenden Aktionen ausführen:

- Ändern des Load Balancing-Algorithmus
- Konfigurieren von Load Balancing-Gruppen und deren Verwendung zum Erstellen Ihrer Load Balancing-Konfiguration
- Persistente Client-Server-Verbindungen konfigurieren
- Konfigurieren des Umleitungsmodus

- Zuweisung verschiedener Gewichte zu verschiedenen Diensten mit unterschiedlichen Kapazitäten.

Der Standard-Lastenausgleichsalgorithmus auf der Citrix ADC Appliance ist die kleinste Verbindungsmethode. In der kleinsten Verbindungsmethode sendet die Appliance jede eingehende Verbindung an den Dienst, der derzeit die wenigsten Verbindungen verarbeitet. Sie können verschiedene Load Balancing-Algorithmen angeben, von denen jeder für unterschiedliche Bedingungen geeignet ist.

Um Anwendungen wie Einkaufswagen, die erfordern, dass alle Anforderungen desselben Benutzers an denselben Server weitergeleitet werden, können Sie die Appliance so konfigurieren, dass persistente Verbindungen zwischen Clients und Servern aufrechterhalten werden. Sie können auch Persistenz für eine Gruppe virtueller Server angeben. Persistence ermöglicht es der Appliance, einzelne Clientanfragen an denselben Dienst zu richten, unabhängig davon, welcher virtuelle Server in der Gruppe die Clientanforderung erhält.

Sie können den Umleitungsmodus aktivieren und konfigurieren, den die Appliance beim Umleiten von Benutzeranforderungen verwendet, indem Sie zwischen IP-basierter und MAC-basierter Weiterleitung wählen. Sie können verschiedenen Diensten auch Gewichtungen zuweisen und angeben, wie viel Prozent der eingehenden Last an jeden Dienst gerichtet werden muss. Durch die Zuweisung von Gewichten können Sie Server mit unterschiedlichen Kapazitäten in dasselbe Lastenausgleichs-Setup einbeziehen, ohne;

- Überlastung der Server mit geringerer Kapazität oder
- damit die Server mit höherer Kapazität im Leerlauf sitzen können.

Anpassen des Hash-Algorithmus für die Persistenz über virtuelle Server hinweg

October 5, 2021

Die Citrix ADC Appliance verwendet hash-basierte Algorithmen, um die Persistenz über virtuelle Server hinweg aufrechtzuerhalten. Standardmäßig verwendet die hash-basierte Load Balancing-Methode einen Hash-Wert der IP-Adresse und Portnummer des Dienstes. Wenn ein Dienst an verschiedenen Ports auf demselben Server zur Verfügung gestellt wird, generiert der Algorithmus unterschiedliche Hash-Werte. Daher können unterschiedliche virtuelle Server mit Lastenausgleich Anforderungen für dieselbe Anwendung an verschiedene Dienste senden, wodurch die Pseudopersistenz unterbrochen wird.

Alternativ zur Verwendung der Portnummer zum Generieren des Hash-Werts können Sie für jeden Dienst einen eindeutigen Hash-Bezeichner angeben. Für einen Dienst muss derselbe Hash-Bezeichnerwert auf allen virtuellen Servern angegeben werden. Wenn ein physischer Server mehr als

einen Anwendungstyp bedient, sollte jeder Anwendungstyp über einen eindeutigen Hash-Bezeichner verfügen.

Der Algorithmus zum Berechnen des Hash-Werts für einen Dienst funktioniert wie folgt:

- Standardmäßig gibt eine globale Einstellung die Verwendung der Portnummer in einer Hash-Berechnung an.
- Wenn Sie einen Hash-Bezeichner für einen Dienst konfigurieren, wird er verwendet, und die Portnummer ist nicht, unabhängig von der globalen Einstellung.
- Wenn Sie keinen Hash-Bezeichner konfigurieren, sondern den Standardwert der globalen Einstellung ändern, sodass keine Verwendung der Portnummer angegeben wird, basiert der Hash-Wert nur auf der IP-Adresse des Dienstes.
- Wenn Sie keinen Hash-Bezeichner konfigurieren oder den Standardwert der globalen Einstellung ändern, um die Portnummer zu verwenden, basiert der Hash-Wert auf der IP-Adresse und der Portnummer des Dienstes.

Sie können auch Hash-Bezeichner angeben, wenn Sie die CLI verwenden, um Dienste an eine Dienstgruppe zu binden. Im Konfigurationsdienstprogramm können Sie eine Dienstgruppe öffnen und Hash-Bezeichner auf der Registerkarte Mitglieder hinzufügen.

So ändern Sie die globale Einstellung Use-Port-Nummer mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb parameter -usePortForHashLb (YES          NO)
```

Beispiel:

```
> set lb parameter -usePortForHashLb NO
 Done
>show lb parameter
Global LB parameters:
        Persistence Cookie HttpOnly Flag: DISABLED
        Use port for hash LB: NO
 Done
<!--NeedCopy-->
```

So ändern Sie die globale Einstellung Use-Port-Nummer mit der GUI

1. Navigieren Sie zu Traffic Management > Load Balancing > Load Balancing-Parameter konfigurieren.

2. Aktivieren oder deaktivieren Sie Port für Hash-basierte LB-Methoden verwenden.

So erstellen Sie einen neuen Dienst und geben einen Hash-Bezeichner für einen Dienst mit der CLI an

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Hash-ID festzulegen und die Einstellung zu überprüfen:

add service < name > (< ip >	< serverName >) < serviceType > < port > -hashId < positive_integer >

```
show service <name>
<!--NeedCopy-->
```

Beispiel:

```
> add service flbkng 10.101.10.1 http 80 -hashId 12345
 Done
>show service flbkng
        flbkng (10.101.10.1:80) - HTTP
        State: DOWN
        Last state change was at Thu Nov  4 10:14:52 2010
        Time since last state change: 0 days, 00:00:15.990
        Server Name: 10.101.10.1
        Server ID : 0   Monitor Threshold : 0

        Down state flush: ENABLED
        Hash Id: 12345

1)      Monitor Name: tcp-default
                State: DOWN     Weight: 1

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

So geben Sie einen Hash-Bezeichner für einen vorhandenen Dienst mit der CLI an

Geben Sie den Befehl set service, den Namen des Dienstes und **-hashID** gefolgt vom ID-Wert ein.

So geben Sie beim Hinzufügen eines Servicegruppenmitglieds einen Hash-Bezeichner an

Um einen Hash-Bezeichner für jedes Mitglied anzugeben, das der Gruppe hinzugefügt werden soll, und die Einstellung zu überprüfen, geben Sie an der Eingabeaufforderung die folgenden Befehle ein (Stellen Sie sicher, dass Sie für jedes Mitglied eine eindeutige HashID angeben.):

```
bind servicegroup <serviceGroupName> <memberName> <port> -hashId <
    positive_integer>

show servicegroup <serviceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
 bind servicegroup http_svc_group 10.102.27.153 80 -hashId 2222222

>show servicegroup SRV
        SRV - HTTP
        State: ENABLED  Monitor Threshold : 0
        …

        1)         1.1.1.1:80   State: DOWN     Server Name: 1.1.1.1
              Server ID: 123  Weight: 1
        Hash Id: 32211

                Monitor Name: tcp-default       State: DOWN
        …

        2)         2.2.2.2:80   State: DOWN     Server Name: 2.2.2.2
              Server ID: 123  Weight: 1
        Hash Id: 12345

                Monitor Name: tcp-default       State: DOWN
        …
Done

<!--NeedCopy-->
```


So geben Sie einen Hash-Bezeichner für einen Dienst mit der GUI an

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Erstellen Sie einen neuen Dienst, oder öffnen Sie einen vorhandenen Dienst und geben Sie die Hash-ID an.

So geben Sie mit der GUI einen Hash-Bezeichner für ein bereits konfiguriertes Dienstgruppenmitglied an

1. Navigieren Sie zu Traffic Management > Load Balancing > Dienstgruppen.
2. Öffnen Sie ein Mitglied und geben Sie eine eindeutige Hash-ID ein.

Konfigurieren des Umleitungsmodus

October 5, 2021

Im Umleitungsmodus wird die Methode konfiguriert, die von einem virtuellen Server verwendet wird, um zu bestimmen, wo eingehenden Datenverkehr weitergeleitet werden soll. Die Citrix ADC Appliance unterstützt die folgenden Umleitungsmodi:

- IP-basierte Weiterleitung (Standardeinstellung)
- MAC-basierte Weiterleitung

Sie können die MAC-basierte Weiterleitung in Netzwerken konfigurieren, die die DSR-Topologie (Direct Server Return, DSR-Topologie), den Link-Lastausgleich oder den Firewall-Lastausgleich verwenden. Weitere Informationen zur MAC-basierten Weiterleitung finden Sie unter Konfigurieren der MAC-basierten Weiterleitung.

So konfigurieren Sie den Umleitungsmodus mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -m <RedirectionMode>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -m MAC
<!--NeedCopy-->
```


> **Hinweis:**
>
> Für einen Dienst, der an einen virtuellen Server gebunden ist, auf dem die Option -m MAC aktiviert ist, müssen Sie einen Nicht-Benutzermonitor binden.

So konfigurieren Sie den Umleitungsmodus mit der GUI

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Öffnen Sie einen virtuellen Server und wählen Sie den Umleitungsmodus aus.

Konfigurieren von virtuellen Servern mit Wildcard-Funktion pro VLAN

October 5, 2021

Wenn Sie den Lastenausgleich für den Datenverkehr in einem bestimmten VLAN (Virtual Local Area Network) konfigurieren möchten, können Sie einen virtuellen Server mit Wildcards mit einer Listenrichtlinie erstellen, die darauf beschränkt, Datenverkehr nur im angegebenen VLAN zu verarbeiten.

So konfigurieren Sie einen virtuellen Server mit Platzhalterzeichen, der ein bestimmtes VLAN mit der CLI überwacht

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen virtuellen Wildcard Server zu konfigurieren, der ein bestimmtes VLAN überwacht, und überprüfen Sie die Konfiguration:

```
add lb vserver <name> <serviceType> IPAddress * Port * -listenpolicy <
    expression> [-listenpriority <positive_integer>]

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

Beispiel:

```
add lb vserver Vserver-LB-vlan1 ANY -listenpolicy "CLIENT.VLAN.ID.EQ(2)
    " -listenpriority 10

show vserver Vserver-LB-vlan1
<!--NeedCopy-->
```


So konfigurieren Sie einen virtuellen Server mit Platzhalterzeichen, der ein bestimmtes VLAN mit der GUI überwacht

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Erstellen Sie einen neuen virtuellen Server oder öffnen Sie einen vorhandenen virtuellen Server.
3. Geben Sie eine Priorität und einen Ausdruck der Listenrichtlinie an.

Nachdem Sie diesen virtuellen Server erstellt haben, binden Sie ihn an einen oder mehrere Dienste, wie unter Einrichten von Basic Load Balancingbeschrieben.

Zuweisen von Gewichten zu Diensten

October 5, 2021

In einer Lastausgleichskonfiguration weisen Sie Diensten Gewichtungen zu, um den Prozentsatz des Datenverkehrs anzugeben, der an jeden Dienst gesendet werden soll. Dienste mit höheren Gewichten können mehr Anforderungen verarbeiten; Dienste mit geringerer Gewichtung können weniger Anforderungen verarbeiten. Durch das Zuweisen von Gewichten zu Diensten kann die Citrix ADC Appliance bestimmen, wie viel Datenverkehr jeder Lastausgleichsserver verarbeiten kann und damit die Last effektiver ausgleicht.

Hinweis: Wenn Sie eine Lastausgleichsmethode verwenden, die die Gewichtung von Diensten unterstützt (z. B. die Roundrobin-Methode), können Sie dem Service eine Gewichtung zuweisen.

In der folgenden Tabelle werden die Lastausgleichsmethoden beschrieben, die die Gewichtung unterstützen, und kurz beschrieben, wie die Gewichtung beeinflusst, wie ein Dienst für jeden Dienst ausgewählt wird.

Lastenausgleichsmethoden	Service-Auswahl mit Gewichten
Runde Robin	Der virtuelle Server priorisiert die Warteschlange der verfügbaren Dienste so, dass Dienste mit den höchsten Gewichten häufiger an die Spitze der Warteschlange kommen als diejenigen mit den niedrigsten Gewichten und proportional mehr Datenverkehr erhalten. Eine vollständige Beschreibung finden Sie unter Die Round-Robin-Methode.

Lastenausgleichsmethoden	Service-Auswahl mit Gewichten
Geringste Verbindung	Der virtuelle Server wählt den Dienst mit der besten Kombination aus den wenigsten aktiven Transaktionen und dem höchsten Gewicht aus. Eine vollständige Beschreibung finden Sie unter Die kleinste Verbindungsmethode.
Methode der geringsten Antwortzeit und der geringsten Antwortzeit mit Monitoren	Der virtuelle Server wählt den Dienst mit der besten Kombination aus den wenigsten aktiven Transaktionen und der schnellsten durchschnittlichen Antwortzeit aus. Eine vollständige Beschreibung finden Sie unter Die Methode der kleinsten Reaktionszeit.
Geringste Bandbreite	Der virtuelle Server wählt den Dienst mit der besten Kombination aus geringstem Datenverkehr und höchster Bandbreite aus. Eine vollständige Beschreibung finden Sie unter Die Methode der geringsten Bandbreite.
Am wenigsten Pakete	Der virtuelle Server wählt den Dienst mit der besten Kombination aus den wenigsten Paketen und dem höchsten Gewicht aus. Eine vollständige Beschreibung finden Sie unter Die Methode der kleinsten Pakete.
Benutzerdefinierte Last	Der virtuelle Server wählt den Dienst mit der besten Kombination aus niedrigster Last und höchstem Gewicht aus. Eine vollständige Beschreibung finden Sie unter Die benutzerdefinierte Load-Methode.
Hashing-Methoden und Token-Methode	Die Gewichtung wird von diesen Lastausgleichsmethoden nicht unterstützt.

So konfigurieren Sie einen virtuellen Server zum Zuweisen von Gewichtungen zu Diensten mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -weight <Value> <ServiceName>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -weight 10 Service-HTTP-1
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen Server zum Zuweisen von Gewichtungen zu Diensten mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Öffnen Sie den virtuellen Server, und klicken Sie dann im Abschnitt **Dienste** .
3. Weisen Sie dem Service in der Spalte Gewichtung eine Gewichtung zu.

Konfigurieren der Versionseinstellung für MySQL und Microsoft SQL Server

October 5, 2021

Sie können die Version von Microsoft® SQL Server® und den MySQL -Server für einen Lastausgleichsserver angeben, der vom Typ MSSQL bzw. MySQL ist. Die Versionseinstellung wird empfohlen, wenn Sie erwarten, dass einige Clients nicht dieselbe Version wie Ihr MySQL - oder Microsoft SQL Server-Produkt ausführen. Die Versionseinstellung stellt die Kompatibilität zwischen den clientseitigen und serverseitigen Verbindungen bereit, indem sichergestellt wird, dass die gesamte Kommunikation der Serverversion entspricht.

So legen Sie den Microsoft SQL Server-Versionsparameter mit der CLI fest

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den Microsoft SQL Server-Versionsparameter für einen virtuellen Lastausgleichsserver festzulegen und die Konfiguration zu überprüfen:

```
set lb vserver <name> -mssqlServerVersion <mssqlServerVersion>

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


Beispiel

```
> set lb vserver myMSSQLvip -mssqlServerVersion 2008R2
 Done
> show lb vserver myMSSQLvip
    myMSSQLvip (190.0.2.12:1433) - MSSQL    Type: ADDRESS
 . . .
 . . .
    MSsql Server Version: 2008R2
    . . .
    . . .
 Done
>
<!--NeedCopy-->
```

So legen Sie den MySQL -Serververversionsparameter mit der CLI fest

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den MySQL Server-Versionsparameter für einen Lastausgleichsserver festzulegen und die Konfiguration zu überprüfen:

```
set lb vserver <name> -mysqlServerVersion <string>

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

Beispiel

```
> set lb vserver mysqlsvr -mysqlserverversion 5.5.30
 Done
> sh lb vserver mysqlsvr
     mysqlsvr (2.22.2.222:3306) - MYSQL      Type: ADDRESS
 . . .
 . . .
     Mysql Server Version: 5.5.30
    . . .
    . . .
 Done
>
<!--NeedCopy-->
```


So legen Sie den MySQL - oder Microsoft SQL-Serververversionsparameter mit der GUI fest

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Öffnen Sie einen virtuellen Server vom Typ MySQL oder MSSQL, und legen Sie die Serverversion fest.

Virtuelle Multi-IP-Server

June 1, 2022

Der Citrix ADC unterstützt die Erstellung eines einzelnen virtuellen Lastausgleichsservers mit mehreren nicht konsekutiven/aufeinanderfolgenden IPv4- und IPv6-Adressen vom Typ VIP. Jede an einen virtuellen Server gebundene VIP-Adresse wird als einzelner virtueller Server behandelt. Diese virtuellen Server haben dasselbe Protokoll und andere Einstellungen auf virtueller Serverebene. Ein virtueller Server mit mehreren VIP-Adressen wird auch als virtueller Multi-IP-Server bezeichnet.

Im Folgenden sind einige Vorteile der Verwendung von virtuellen Multi-IP-Servern aufgeführt:

- Ein virtueller Multi-IP-Server entlastet die Erstellung vieler virtueller Server mit denselben Einstellungen und Dienstbindungen.
- Virtuelle Multi-IP-Server reduzieren effektiv die Möglichkeit, die Höchstgrenze für virtuelle Serverentitäten zu erreichen.
- Ein virtueller Multi-IP-Server kann für Clients in verschiedenen Subnetzen verwendet werden, um eine Verbindung zu derselben Gruppe von Servern herzustellen.
- Nur ein virtueller Multi-IP-Server kann für IPv6- und IPv4-Clients verwendet werden, um eine Verbindung zu derselben Gruppe von Servern herzustellen.

Konfiguration eines virtuellen Multi-IP-Servers

Die Konfiguration eines virtuellen Multi-IP-Servers umfasst die folgenden Aufgaben:

- Erstellen Sie ein IPset und binden Sie mehrere IP-Adressen daran.
- Binden Sie das IPset an virtuelle Server mit Lastausgleich.

Beachten Sie die folgenden Punkte in Bezug auf die IPset-Konfiguration:

- Ein IPset kann Folgendes haben:
  - nicht konsekutive/aufeinanderfolgende IPv4-Adressen und IPv6-Adressen
  - Kombinationen von IPv4- und IPv6-Adressen.
- Alle IPv4/IPv6-Adressen, die virtuellen Servern zugeordnet werden sollen, die IPset verwenden, müssen vom Typ VIP sein.

- Ein einzelnes IPset kann an mehrere virtuelle Server gebunden werden.
- IPv4/IPv6-Adressen können unabhängig von vorhandenen IPset-Bindungen an virtuelle Server an IPset gebunden/ungebunden sein.
- Sie müssen die IPset-Bindung an einen virtuellen Server aufheben, bevor Sie ein neues IPset daran binden.

So fügen Sie mithilfe der CLI ein IPset hinzu und binden mehrere VIP-Adressen daran

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ipset <name>

bind ipset <name> <IPaddress1 ... >

bind ipset <name> <IPaddress2... >

show ipset <name>
<!--NeedCopy-->
```

So binden Sie das IPset mithilfe der CLI an einen virtuellen Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -ipset <ipset name>

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

So fügen Sie ein IPset hinzu und binden mehrere VIP-Adressen mithilfe der GUI daran

Navigieren Sie zu **System** > **Netzwerk** > **IPsets**, und erstellen Sie ein IPset mit mehreren VIP-Adressen.

So binden Sie das IPset mithilfe der GUI an einen virtuellen Server

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie einen virtuellen Server, an den Sie das erstellte IPset binden möchten.
2. Legen Sie in den **Grundeinstellungen**den **IPset**-Parameter auf den Namen des erstellten IPset fest.


```
> add ipset IPSET-1


Done

> bind ipset IPSET-1 9.9.9.10


Done

> bind ipset IPSET-1 1000::20


Done

> add lb vserver LBVS-1 HTTP 8.8.8.10 80  - ipset IPSET-1


Done

> add service SVC-1 3.3.3.10 HTTP 80


Done

> add service SVC-2 3.3.3.100 HTTP 80


Done

> bind lb vserver LBVS-1 SVC-1


Done

> bind lb vserver LBVS-1 SVC-2


Done
```


GSLB-Unterstützung für virtuelle Multi-IP-Server

Floating-IP-Adressen sind für die Hochverfügbarkeitsbereitstellungen erforderlich. Cloud-Bereitstellungen unterstützen keine Floating-IP. Die IP-Set-Funktion unterstützt Sie also bei der Unterstützung von Hochverfügbarkeit in Cloud-Bereitstellungen. Mit der IP-Set-Funktion können Sie jeder der primären und sekundären Instanzen eine private IP-Adresse zuordnen. Eine der privaten IP-Adressen wird beim Erstellen des virtuellen Servers hinzugefügt. Die andere IP-Adresse ist an einen IP-Set gebunden. Das IP-Set wird dann mit dem virtuellen Server verknüpft. In der Regel wird eine öffentliche IP-Adresse einer der privaten IP-Adressen zugeordnet, basierend darauf, welche Appliance den Datenverkehr empfängt. Während des Failovers ändert sich diese Zuordnung dynamisch, um den Datenverkehr an den neuen Primärdatenverkehr weiterzuleiten.

In GSLB-Bereitstellungen stellt der GSLB-Dienst den virtuellen Server dar und erfordert sowohl die private als auch die öffentliche IP-Adresse des virtuellen Servers. In Cloud-Bereitstellungen werden mehrere private IP-Adressen als IP-Set dargestellt, aber der GSLB-Dienst kann nur eine private IP-Adresse akzeptieren. Daher wird empfohlen, bei der Konfiguration des GSLB-Dienstes die IP-Adresse anzugeben, die beim Hinzufügen des virtuellen Servers oder einer der IP-Adressen im IP-Set konfiguriert wurde. Sie müssen die IP-Set-Funktion im GSLB-Dienst nicht konfigurieren. Der auf dem virtuellen Lastausgleichsserver konfigurierte IP-Set, der mit dem GSLB-Dienst verknüpft ist, ist ausreichend.

In der übergeordneten GSLB-Topologie kann den virtuellen Lastausgleichsservern auf den untergeordneten Sites der IP-Satz zugeordnet sein. Der GSLB-Dienst, der dieser Topologie entspricht, trägt die öffentliche IP-Adresse und eine der privaten IP-Adressen. Die private IP-Adresse kann eine IP-Adresse im IP-Set sein oder diejenige, die beim Hinzufügen des virtuellen Servers auf der untergeordneten Site konfiguriert wurde. Die Kommunikation zwischen den übergeordneten und den untergeordneten Sites verwendet immer die öffentliche IP-Adresse und den öffentlichen Port des GSLB-Dienstes.

Mit IP-Set-Unterstützung können Sie auch einen einzigen virtuellen Serverendpunkt für IPv4- und IPv6-Datenverkehr haben. Zuvor mussten Sie verschiedene virtuelle Server für IPv4- und IPv6-Verkehr konfigurieren. Mit der Unterstützung von IP-Sätzen können Sie IPv4- und IPv6-IP-Adressen demselben IP-Set zuordnen. Sie können verschiedene GSLB-Dienste hinzufügen, die die IPv4- und IPv6-Endpunkte darstellen.

Begrenzen der Anzahl gleichzeitiger Anforderungen für eine Clientverbindung

October 5, 2021

Sie können die Anzahl gleichzeitiger Anforderungen für eine einzelne Clientverbindung einschränken. Sie können die Server vor Sicherheitslücken schützen, indem Sie die Anzahl der gleichzeitigen Anforderungen einschränken. Wenn die Clientverbindung die angegebene Höchstgrenze erreicht, löscht

die Citrix ADC Appliance nachfolgende Anforderungen für die Verbindung, bis die Anzahl der ausstehenden Anforderungen unter den Grenzwert liegt.

Sie können den Parameter MaxPipelineAt so konfigurieren, dass die Anzahl gleichzeitiger Anforderungen für eine einzelne Clientverbindung begrenzt wird. Dieser Parameter ist nur für die folgenden Diensttypen anwendbar und wenn “SvrTimeout” auf Null gesetzt ist:

- ANY
- Alle UDP-Diensttypen außer DNS

Der Standardwert des Parameters MaxPipelineAt ist 255. Der Wert Null (0) weist keine Begrenzung auf die Anzahl der Hintergrundprozesse zu. Wenn kein Limit festgelegt ist, führt die Citrix ADC Appliance alle Anforderungen aus.

> **Hinweis:**
>
> Wenn Sie MaxpipelineNAT auf einen höheren Wert setzen, kann die Wahrscheinlichkeit eines Spoofing-Angriffs höher sein. Daher wird empfohlen, MaxpipelineNAT auf einen niedrigeren Wert zu setzen.

So beschränken Sie die Anzahl gleichzeitiger Verbindungen für einen Client mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb parameter -maxPipelineNat <positive_integer>
<!--NeedCopy-->
```

Beispiel:

```
set lb parameter -maxPipelineNat 199
<!--NeedCopy-->
```

So beschränken Sie die Anzahl gleichzeitiger Verbindungen für einen Client mit der GUI

Navigieren Sie zu **Traffic Management > Load Balancing > Configure Load Balancing Parameters**, und geben Sie einen Wert für Max Pipeline NAT-Anforderungen an.

Konfigurieren des Durchmesser-Lastausgleichs

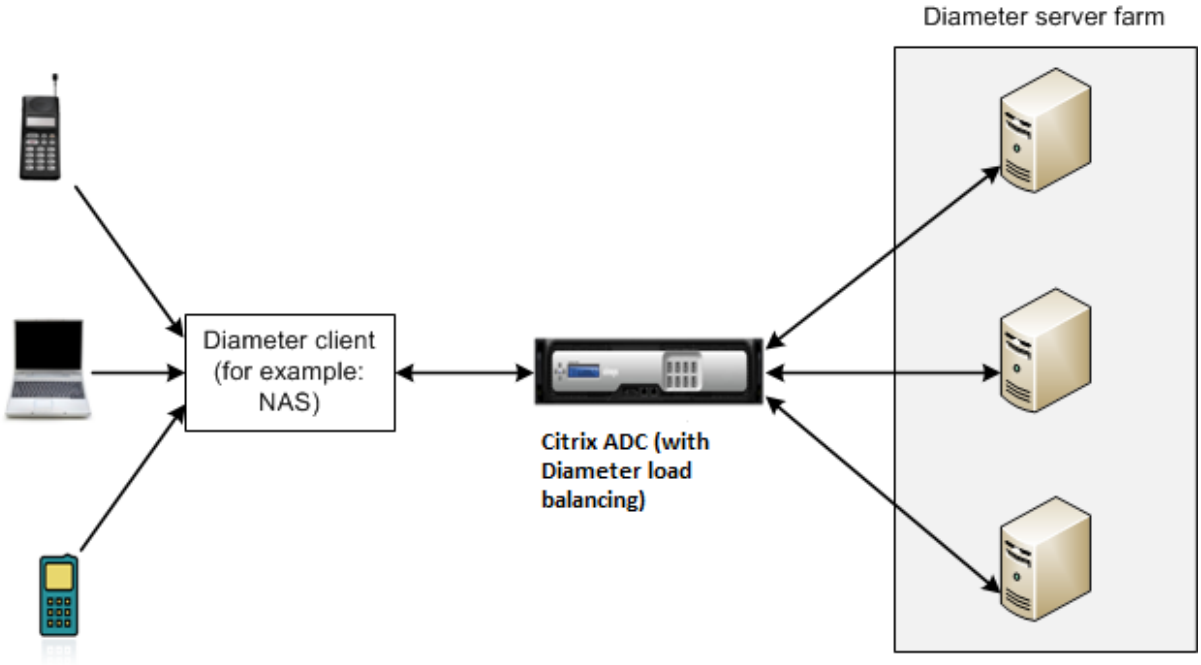
October 5, 2021

Das Diameter Protocol ist ein AAA (Authentication, Authorization and Accounting) Signalprotokoll der nächsten Generation, das hauptsächlich auf mobilen Geräten wie Laptops und Mobiltelefonen verwendet wird. Es handelt sich um ein Peer-to-Peer-Protokoll, im Gegensatz zu dem traditionellen Client-Server-Modell, das von den meisten anderen Protokollen verwendet wird. In den meisten Diameter Deployments stammen die Clients jedoch die Anforderung, und der Server antwortet auf die Anforderung.

Wenn Diameter Nachrichten ausgetauscht werden, führt der Diameter Server in der Regel viel mehr Verarbeitung als der Diameter Client. Mit der Zunahme des Signalisierungsvolumens der Steuerebene wird der Diameter Server zu einem Engpass. Daher müssen Diameter-Meldungen auf mehrere Server ausbalanciert werden. Ein virtueller Server, der Lastenausgleich von Diameter-Meldungen durchführt, bietet folgende Vorteile:

- Geringere Belastung von Diameter Servern, was zu einer schnelleren Reaktionszeit für Endbenutzer führt.
- Überwachung des Serverzustands und bessere Failover-Funktionen.
- Bessere Skalierbarkeit in Bezug auf die Serverzufügung ohne Änderung der Clientkonfiguration.
- Hohe Verfügbarkeit.
- SSL-Diameter-Offloading.

Die folgende Abbildung zeigt ein Diameter System in einer Citrix ADC Bereitstellung:



Ein Diameter-System besteht aus folgenden Komponenten:

- **Diameter Client.** Unterstützt Diameter Client-Anwendungen zusätzlich zum Basisprotokoll. Durchmesser-Clients werden häufig in Geräten am Rande eines Netzwerks implementiert und

bieten Zugangskontrolldienste für dieses Netzwerk. Typische Beispiele für Diameter Clients sind ein Network Access Server (NAS) und der Mobile IP Foreign Agent (FA).

- **Diameter Agent.** Bietet Relay-, Proxy-, Umleitungs- oder Übersetzungsdienste. Die Citrix ADC Appliance (konfiguriert mit einem virtuellen Diameter Load Balancing Server) spielt die Rolle eines Diameter Agents.
- **Diameter Server.** Behandelt die Authentifizierungs-, Autorisierungs- und Buchhaltungsanforderungen für einen bestimmten Bereich. Ein Diameter Server muss Diameter Server-Anwendungen zusätzlich zum Basisprotokoll unterstützen.

Wenn ein Endbenutzergerät (z. B. ein Mobiltelefon) einen Dienst benötigt, sendet es in einer typischen Diameter Topologie eine Anforderung an einen Diameter Client. Jeder Diameter Client stellt eine einzelne Verbindung (TCP-Verbindung — SCTP wird noch nicht unterstützt) mit einem Diameter Server wie im Diameter Base-Protokoll RFC 6733 angegeben. Die Verbindung ist langlebig und alle Nachrichten zwischen den beiden Diameter Knoten (Client und Server) werden über diese Verbindung ausgetauscht. Citrix ADC verwendet nachrichtenbasierten Lastenausgleich.

Beispiel:

Ein Mobilfunkanbieter verwendet Diameter für sein Abrechnungssystem. Wenn ein Abonnent eine Prepaid-Nummer verwendet, sendet der Diameter Client wiederholt Anfragen an den Server, um den verfügbaren Saldo zu überprüfen. Das Diameter Protokoll stellt eine Verbindung zwischen dem Client und dem Server her, und alle Anforderungen werden über diese Verbindung ausgetauscht. Verbindungsbasierter Lastausgleich wäre sinnlos, da es nur eine Verbindung gibt. Angesichts der großen Anzahl von Nachrichten auf der Verbindung beschleunigt der nachrichtenbasierte Lastausgleich jedoch die Abrechnung des Prepaid-Mobilfunkteilnehmers.

Funktionsweise des Durchmesser-Lastausgleichs

Eine Disconnect Peer Request (DPR) gibt die Absicht des Peers an, die Verbindung zu schließen, mit dem Grund für das Schließen der Verbindung. Der Peer antwortet mit einem DPA (TCP bietet immer einen erfolgreichen DPA).

- Wenn die Appliance eine DPR vom Client empfängt, sendet sie die DPR an alle Server und antwortet sofort mit einem DPA an den Client. Die Server antworten mit DPAs, aber die Appliance ignoriert sie. Der Client sendet eine FIN, die die Appliance an alle Server sendet.
- Wenn die Appliance eine DPR vom Server empfängt, antwortet sie allein mit einem DPA an diesen Server und entfernt den Server nicht aus dem Wiederverwendungspool. Wenn der Server eine FIN sendet, antwortet die Appliance mit FIN/ACK und entfernt Verbindungen aus dem Wiederverwendungspool.
- Wenn die Appliance eine FIN vom Client erhält, sendet sie dem Client eine FIN/ACK, sendet die FIN und entfernt die Serververbindung sofort aus dem Wiederverwendungspool.
- Wenn die Appliance eine FIN vom Server empfängt, sendet sie eine FIN/ACK und entfernt sie

aus dem Wiederverwendungspool. Jede neue Nachricht für diesen Server wird über eine neue Verbindung gesendet.

Load Balancing von Diameter-Verkehr

Wenn ein Client eine Anforderung an die Citrix ADC Appliance sendet, analysiert die Appliance die Anforderung und gleicht sie kontextuell auf einen Diameter-Server basierend auf einem Persist-AVP aus. Die Appliance hat dem Server die Clientidentität angekündigt, sodass keine Routeneinträge hinzugefügt werden, da der Server Nachrichten direkt vom Client erwartet.

Serverinitiierte Anforderungen sind nicht so häufig wie Clientanforderungen. Serverinitiierte Anforderungen ähneln Client-initiierten Anforderungen, außer:

- Da Nachrichten von mehreren Servern empfangen werden, behält die Appliance den Transaktionsstatus bei, indem jeder weitergeleiteten Anforderungsnachricht eine eindeutige Hop-by-Hop-Nummer (HByH) hinzugefügt wird. Wenn die Nachrichtenantwort eintrifft (mit derselben HByH-Nummer), übersetzt die Appliance diese HByH-Nummer in die HByH-Nummer, die beim Eintreffen der Anforderung auf dem Server empfangen wurde.
- Die Citrix ADC Appliance fügt einen Routeneintrag hinzu, indem sie ihre Identität ablegt, da der Client die Appliance als Relay-Agent sieht.

Hinweis: Wenn eine Diameter-Nachricht mehr als ein Paket umfasst, sammelt die Appliance die Pakete in einer unvollständigen Header-Warteschlange und leitet sie an den Server weiter, wenn die vollständige Nachricht angesammelt wird. Wenn ein einzelnes Paket mehr als eine Diameter-Nachricht enthält, teilt die Appliance das Paket auf und leitet die Nachrichten an Server weiter, wie vom virtuellen Lastausgleichsserver festgelegt.

Trennen einer Sitzung

Eine Disconnect Peer Request (DPR) gibt die Absicht des Peers an, die Verbindung zu schließen, mit dem Grund für das Schließen der Verbindung. Der Peer antwortet mit einem DPA (TCP bietet immer einen erfolgreichen DPA).

- Wenn die Citrix ADC Appliance eine DPR vom Client empfängt, sendet sie die DPR an alle Server und antwortet sofort mit einem DPA an den Client. Die Server antworten mit DPAs, aber die Appliance ignoriert sie. Der Client sendet eine FIN, die die Appliance an alle Server sendet.
- Wenn die Appliance eine DPR vom Server empfängt, antwortet sie allein mit einem DPA an diesen Server und entfernt den Server nicht aus dem Wiederverwendungspool. Wenn der Server eine FIN sendet, antwortet die Appliance mit FIN/ACK und entfernt Verbindungen aus dem Wiederverwendungspool.
- Wenn die Appliance eine FIN vom Client erhält, sendet sie dem Client eine FIN/ACK, sendet die FIN und entfernt die Serververbindung sofort aus dem Wiederverwendungspool.

- Wenn die Appliance eine FIN vom Server empfängt, sendet sie eine FIN/ACK und entfernt sie aus dem Wiederverwendungspool. Jede neue Nachricht für diesen Server wird über eine neue Verbindung gesendet.

Konfigurieren des Lastausgleichs für Durchmesserverkehr

Um die Citrix ADC Appliance für den Lastausgleich des Diameter-Verkehrs zu konfigurieren, müssen Sie zuerst die Parameter Diameter auf der Appliance festlegen, dann den Diameter-Monitor hinzufügen, die Diameter-Dienste hinzufügen, die Dienste an den Monitor binden, den virtuellen Server mit Diameter-Lastausgleich hinzufügen und die Dienste an den virtuellen Server.

So konfigurieren Sie den Lastausgleich für Durchmesserverkehr mit der Befehlszeilenschnittstelle

Konfigurieren Sie die Durchmesserparameter.

```
set ns diameter -identity <string> -realm <string> -
   serverClosePropagation <YES|NO>
<!--NeedCopy-->
```

Beispiel:

```
set ns diameter -identity mydomain.org -realm org -
   serverClosePropagation YES
<!--NeedCopy-->
```

Fügen Sie einen Diameter-Monitor hinzu.

```
add lb monitor <monitorName> DIAMETER -originHost <string> -originRealm
    <string>
<!--NeedCopy-->
```

Beispiel:

```
add lb monitor diameter_mon DIAMETER -originHost mydomain.org -
   originRealm org
<!--NeedCopy-->
```


Erstellen Sie die Diameter Services.

```
add service <name> <IP> DIAMETER <port>
<!--NeedCopy-->
```

Beispiel:

```
add service diameter_svc0 10.102.82.86 DIAMETER 3868

add service diameter_svc1 10.102.82.87 DIAMETER 3868

add service diameter_svc2 10.102.82.88 DIAMETER 3868

add service diameter_svc3 10.102.82.89 DIAMETER 3868
<!--NeedCopy-->
```

Binden Sie die Diameter Services an den Diameter Monitor.

```
bind service <name>@ monitorName <monitorName>
<!--NeedCopy-->
```

Beispiel:

```
bind service diameter_svc0 -monitorName diameter_mon

bind service diameter_svc1 -monitorName diameter_mon

bind service diameter_svc2 -monitorName diameter_mon

bind service diameter_svc3 -monitorName diameter_mon
<!--NeedCopy-->
```

Fügen Sie einen virtuellen Diameter Load Balancing Server mit Diameter-Persistenz hinzu.

```
add lb vserver <name> DIAMETER <IPAddress> <port> -persistenceType
   DIAMETER -persistAVPno <positive_integer>
<!--NeedCopy-->
```


Beispiel:

```
add lb vserver diameter_vs DIAMETER 10.102.112.152 3868 -
   persistenceType DIAMETER -persistAVPno 263
<!--NeedCopy-->
```

Binden Sie die Diameter Services an den virtuellen Diameter Load Balancing Server.

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

Beispiel:

```
bind lb vserver diameter_vs diameter_svc0

bind lb vserver diameter_vs diameter_svc1

bind lb vserver diameter_vs diameter_svc2

bind lb vserver diameter_vs diameter_svc3
<!--NeedCopy-->
```

Speichern Sie die Konfiguration.

```
save ns config
<!--NeedCopy-->
```

Hinweis: Sie können auch den Lastausgleich von Diameter-Verkehr über SSL konfigurieren, indem Sie den Diensttyp **SSL_DIAMETER**verwenden.

So konfigurieren Sie den Lastausgleich für den Diameter-Verkehr mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **System** > **Einstellungen** > **Diameter-Parameter ändern**, und legen Sie die Diameter-Parameter fest.
2. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und erstellen Sie einen virtuellen Lastausgleichsserver vom Typ Diameter.
3. Erstellen Sie einen Service vom Typ Diameter.

4. Erstellen Sie einen Monitor vom Typ Diameter. Legen Sie unter Spezielle Parameter den Ursprungshost und den Ursprungsbereich fest.
5. Binden Sie den Monitor an den Dienst, und binden Sie den Dienst an den virtuellen Diameter Server.
6. Klicken Sie unter Erweiterte Einstellungen auf **Persistenz**, geben Sie den Durchmesser an, und geben Sie eine Persistenz-AVP-Nummer ein.
7. Klicken Sie auf **Speichern**, und klicken Sie auf **Fertig**.

FIX-Lastausgleich konfigurieren

October 5, 2021

Financial Information Exchange (FIX) -Protokoll ist ein Open-Message-Standard, der in der Finanzindustrie für den elektronischen Austausch von Informationen im Zusammenhang mit Wertpapiertransaktionen zwischen Handelspartnern verwendet wird. Das FIX/SSL_FIX-Protokoll wird ausführlich von Buy-Side- und Sell-Side-Firmen, Handelsplattformen und Regulierungsbehörden für die Kommunikation von Handelsinformationen verwendet.

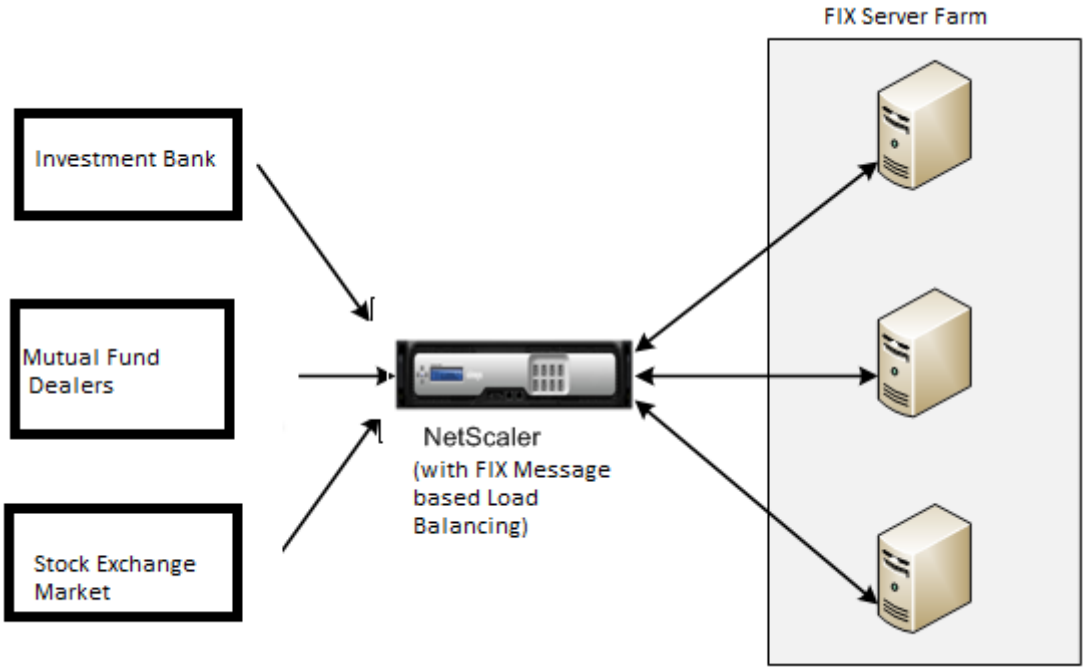
Mit dieser Funktion können Sie einen virtuellen FIX- oder SSL_FIX-Server für den Lastenausgleich konfigurieren, um eingehende FIX-Nachrichten zu verteilen und die Sicherheit in FIX-Messaging bereitzustellen. Citrix ADC unterstützt den nachrichtenbasierten FIX-Lastenausgleich (MBLB) für die Versionen FIX 4.1, FIX 4.2, FIX 4.3 und FIX 4.4.

FIX MBLB auf einer Citrix ADC Appliance bietet die folgenden Vorteile:

1. Effiziente Verwaltung von FIX- oder SSL_FIX-Servern mit überlegener HA- und Zustandsüberwachung.
2. SYN-Schutz für alle FIX- oder SSL_FIX-Server.
3. FIX-Sitzungsbeständigkeit.

Funktionsweise des FIX-Lastausgleichs

Ein FIX MBLB-Setup enthält einen virtuellen FIX-Lastausgleichsserver und mehrere FIX-Server mit Lastenausgleich. Der virtuelle FIX-Server empfängt eingehenden Clientdatenverkehr, analysiert den eingehenden Datenverkehr in FIX-Nachrichten, wählt für jede FIX-Nachricht einen FIX-Server aus und leitet die Nachricht an den ausgewählten FIX-Server weiter. Die folgende konzeptionelle Zeichnung veranschaulicht ein typisches FIX-Lastenausgleichs-Setup.



In einem einfachen FIX MBLB-Setup verteilt der virtuelle FIX-Server FIX-Nachrichten von Clients an die FIX-Server mit Lastenausgleich mit der Roundrobin-Load-Balancing-Methode. Wenn die Persistenz vom Typ FIXSESSION aktiviert ist, wählt der virtuelle FIX-Server denselben Server für verschiedene FIX-Meldungen aus, die zu derselben FIX-Sitzung gehören. Die FIX-Sitzung wird basierend auf den Werten der **FIX-Felder** SenderCompId (Tag 49) und targetCompid (Tag 56) bestimmt.

Konfigurieren und Überwachen des Lastausgleichs für FIX-Datenverkehr

Im Folgenden sind die Konfigurationen, die Sie tun müssen, um den Lastenausgleich FIX-Nachrichtenverkehr:

1. Konfigurieren des virtuellen FIX-Lastausgleichsservers
2. Konfigurieren des virtuellen SSL_FIX-Lastenausgleichsservers
3. Konfigurieren des FIX-Lastausgleichsdiensts
4. Konfigurieren des SSL_FIX-Lastenausgleichsdiensts
5. Konfigurieren der FIXSESSION-Persistenz
6. Festlegen der Persistenzzeitüberschreitung
7. FIX/SSL_FIX-Statistiken anzeigen
8. Überwachung persistenter FIX/SSL_FIX Sitzungen

So konfigurieren Sie einen FIX-Lastausgleichsserver mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add lb vserver <name> FIX <IP> <PORT>
<!--NeedCopy-->
```

Beispiel

```
add lb vserver vs1 FIX 10.102.82.86 3868
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen SSL_FIX-Lastausgleichsserver mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> SSL_FIX <IP> <PORT>
<!--NeedCopy-->
```

Beispiel

```
add lb vserver vs1 SSL_FIX 10.102.82.86 3868
<!--NeedCopy-->
```

So konfigurieren Sie einen FIX-Dienst mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name> <ip-addr> FIX <port>
<!--NeedCopy-->
```

Beispiel

```
add service_svc1 10.102.82.86 FIX 3868
<!--NeedCopy-->
```


So konfigurieren Sie einen SSL_FIX-Dienst mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name> <ip-addr> SSL_FIX <port>
<!--NeedCopy-->
```

Beispiel

```
add service svc1 10.102.82.86 SSL_FIX 3868
<!--NeedCopy-->
```

So konfigurieren Sie die FIXSESSION Persistenz mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -persistenceType FIXSESSION
<!--NeedCopy-->
```

Beispiel

```
set lb vserver vs1 -persistenceType FIXSESSION
<!--NeedCopy-->
```

So legen Sie Persistenz-Timeout mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -timeout <value>
<!--NeedCopy-->
```

Beispiel

```
set lb vserver vs1  - timeout 2
<!--NeedCopy-->
```


So zeigen Sie FIX-Statistiken mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel

```
stat lb vserver_svc1
<!--NeedCopy-->
```

So binden Sie den FIX-Dienst mit der Befehlszeilenschnittstelle an den virtuellen FIX-Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name> <service name>
<!--NeedCopy-->
```

Beispiel

```
bind lb vserver vs1 svc1
<!--NeedCopy-->
```

So zeigen Sie permanente FIX-Sitzungen mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel

```
show lb persistentSessions vs1
<!--NeedCopy-->
```


> **Hinweis:**
>
> Hinweis: Sie können nun den Lastenausgleich von FIX-Datenverkehr über SSL mithilfe des Diensttyps SSL_FIX konfigurieren. Dieser Dienst bietet eine sichere Kommunikation für FIX-Nachrichten.

So konfigurieren Sie den virtuellen FIX-Lastausgleichsserver mit der GUI

1. Navigieren Sie zur Seite **Konfiguration** > **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und klicken Sie auf **Hinzufügen**, um einen virtuellen FIX Load Balancing Server zu erstellen.
2. Legen Sie auf der Seite **Load Balancing Virtual Server** die Serverparameter fest:
   a) Virtueller Servername
   b) Protokolltyp als FIX
   c) IP-Adresstyp des Servers
   d) Server-IP-Adresse
   e) Serverportnummer
3. Klicken Sie auf **OK** und **Weiter**, um andere Parameter festzulegen.
4. Wählen Sie im Abschnitt **Dienste** einen neuen virtuellen FIX-Lastausgleichsdienst aus oder fügen Sie ihn hinzu, und binden Sie ihn an den FIX-Server.
5. Legen Sie im Abschnitt **Persistenz** die folgenden Parameter fest:
   a) Persistenztyp als 'FIXSESSION'
   b) Zeitüberschreitungsintervall
6. Klicken Sie auf **OK** und dann auf **Fertig**.

So bearbeiten Sie einen virtuellen FIX-Lastausgleichsserver mit der GUI

Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Virtuelle Server**, wählen Sie einen FIX-Server aus und klicken Sie auf **Bearbeiten** .

So löschen Sie einen virtuellen FIX-Lastausgleichsserver mit der GUI

Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Virtuelle Server**, wählen Sie einen FIX-Server aus und klicken Sie auf **Löschen**.

So konfigurieren Sie den virtuellen FIX-Lastausgleichsdienst mit der GUI

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Services**, und klicken Sie auf **Hinzufügen**, um einen virtuellen FIX Load Balancing-Dienst zu erstellen.

2. Legen Sie auf der Seite **Dienste** die folgenden Parameter fest. Sie können auf den Pfeil “Mehr” klicken, um andere Parameter wie Verkehrsdomäne, Hash-ID, Server-ID, Cache-Typ und Anzahl der aktiven Verbindungen festzulegen.
   a) Dienstname — FIX Virtual Service Name
   b) Virtueller Servertyp als (Neu oder Bestehend) auswählen
   c) Protokoll — Protokolltyp als ‘FIX’
   d) Server — IP-Adresse des virtuellen Servers
   e) Port — Serverportnummer
3. Klicken Sie auf **OK** und **Weiter**, um weitere Parameter wie Monitore, Schwellenwert und Time-out, Profile und Richtlinien festzulegen.
4. Klicken Sie auf **OK** und dann auf **Fertig**.

So bearbeiten Sie einen virtuellen FIX-Lastausgleichsdienst mit der GUI

Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Services**, wählen Sie einen **FIX-Dienst** aus, und klicken Sie auf **Bearbeiten** .

So löschen Sie einen virtuellen FIX-Lastausgleichsdienst mit der GUI

Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Services** Seite, wählen Sie einen FIX-Dienst aus und klicken Sie auf **Löschen**.

So zeigen Sie FIX-Lastausgleichserver-Statistiken an

Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und klicken Sie dann auf **Statistiken**, um die FIX-Serverstatistik anzuzeigen.

So zeigen Sie beständige Sitzungen für einen FIX-Server mit der GUI an

Navigieren Sie zur Seite **Konfiguration** > **Datenverkehrsverwaltung**, und klicken Sie unter **Überwachungssitzungen** auf **Persistente virtuelle Server-Sitzungen** .

So löschen Sie Persistente Sitzungen für einen FIX-Server mit der GUI

1. Navigieren Sie zur Seite **Konfiguration** > **Verkehrsverwaltung**, und klicken Sie unter **Überwachungssitzungen** auf **Persistente Sitzungen löschen** .
2. Legen Sie auf der Seite **Persistente Sitzungen löschen** die folgenden Parameter fest:
   a) Virtueller Server — Wählen Sie einen virtuellen FIX-Server
   b) Persistence-Parameter — Wählen Sie einen FIX-Persistenz-Parameter
3. Klicken Sie auf **OK**.

MQTT Load Balancing

October 5, 2021

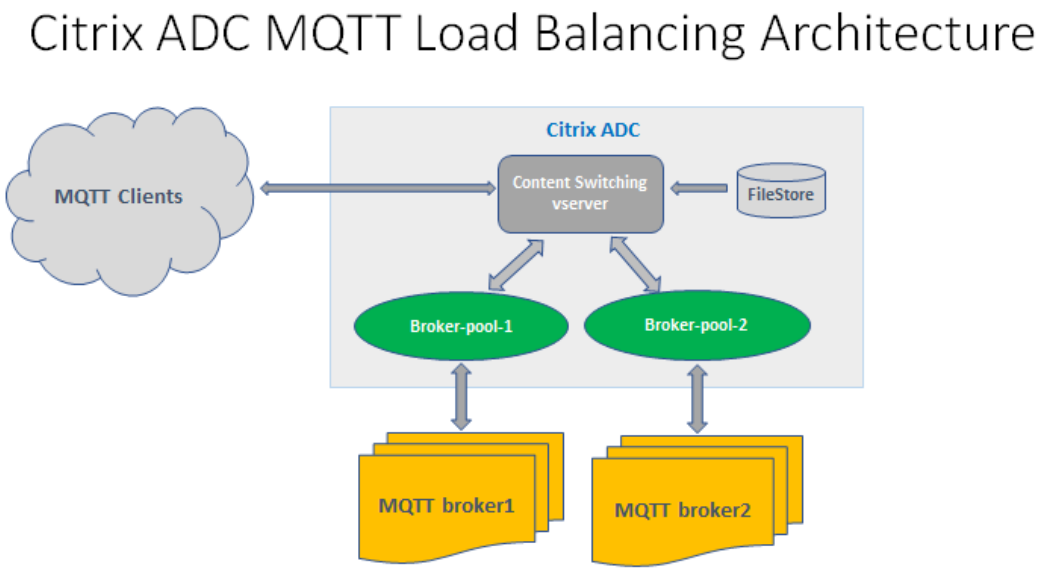
Der Message Queuing Telemetry Transport (MQTT) ist ein OASIS-Standard-Messaging-Protokoll für das Internet der Dinge (IoT). MQTT ist eine flexible und einfach zu bedienende Technologie, die eine effektive Kommunikation innerhalb eines IoT-Systems ermöglicht. MQTT ist ein Broker-basiertes Protokoll und wird häufig verwendet, um den Austausch von Nachrichten zwischen Kunden und Brokern zu erleichtern.

Die folgenden Hauptvorteile von MQTT machen es zu einer geeigneten Option für Ihr IoT-Gerät:

- Zuverlässigkeit
- Schnelle Reaktionszeit
- Möglichkeit zur Unterstützung einer unbegrenzten Anzahl von Geräten
- Veröffentlichen/Abonnieren von Nachrichten, die perfekt für Viele-zu-Viele-Kommunikation geeignet sind

IoT ist das Netzwerk von miteinander verbundenen Geräten, die in Sensoren, Software, Netzwerkkonnektivität und notwendige Elektronik eingebettet sind. Die eingebetteten Komponenten ermöglichen es IoT-Geräten, Daten zu sammeln und auszutauschen. Die zunehmende Nutzung von IoT-Geräten bringt die Netzwerkinfrastruktur mit sich aus, wobei Scale die herausragende darstellt. Bei einer großen Bereitstellung von IoT-Geräten müssen die von jedem IoT-Gerät generierten Daten schnell analysiert werden. Um die Skalierungsanforderungen und die effiziente Nutzung der Ressourcen zu erfüllen, muss die Belastung des Brokerpools gleichmäßig verteilt werden. Mit Unterstützung des MQTT-Protokolls können Sie die Citrix ADC Appliance in IoT-Bereitstellungen verwenden, um den MQTT-Datenverkehr auszugleichen.

Die folgende Abbildung zeigt die MQTT-Architektur, die eine Citrix ADC Appliance verwendet, um den Lastausgleich des MQTT-Datenverkehrs zu verwenden.



Eine IoT-Bereitstellung mit MQTT-Protokoll besteht aus folgenden Komponenten:

- **MQTT-Broker.** Ein Server, der alle Nachrichten von den Clients empfängt und die Nachrichten dann an die entsprechenden Zielclients weiterleitet. Der Broker ist dafür verantwortlich, alle Nachrichten zu empfangen, die Nachrichten zu filtern, zu bestimmen, wer jede Nachricht abonniert hat, und das Senden der Nachricht an diese abonnierten Clients. Der Broker ist der zentrale Knotenpunkt, durch den jede Nachricht hinausgehen muss.
- **MQTT-Client.** Jedes Gerät, von einem Mikrocontroller bis zu einem vollwertigen Server, der eine MQTT-Bibliothek betreibt und über ein Netzwerk mit einem MQTT-Broker verbunden ist. Sowohl Publisher als auch Abonnenten sind MQTT-Kunden. Die Verlags- und Abonnentenlabels beziehen sich darauf, ob der Kunde Nachrichten veröffentlicht oder Nachrichten abonniert hat.
- **MQTT Load Balancer** Die Citrix ADC Appliance ist mit einem virtuellen MQTT-Lastausgleichsserver konfiguriert, um den Lastausgleich des MQTT-Datenverkehrs zu erstellen.

In einer typischen IoT-Bereitstellung verwaltet der Broker (Servercluster) die Gruppe der IoT-Geräte (IoT-Clients). Die Last der Citrix ADC Appliance gleicht den MQTT-Verkehr an die Broker basierend auf verschiedenen Parametern wie Client-ID, Thema und Benutzername aus.

Konfigurieren des Load Balancing für MQTT-Datenverkehr

Damit die Citrix ADC Appliance den Lastausgleich von MQTT-Datenverkehr ermöglicht, führen Sie die folgenden Konfigurationsaufgaben aus:

1. Konfigurieren Sie die Dienste oder Dienstgruppen von MQTT/MQTT_TLS.
2. Konfigurieren Sie den virtuellen Lastenausgleichsserver MQTT/MQTT_TLS.

3. Binden Sie die MQTT/MQTT_TLS-Dienste an den virtuellen Server des Lastenausgleichs MQTT/MQTT_TLS.
4. Konfigurieren Sie den virtuellen MQTT/MQTT_TLS-Content Switching-Server.
5. Konfigurieren einer Content Switching-Aktion, die den virtuellen Ziel-Lastausgleichsserver angibt
6. Konfigurieren Sie eine Content Switching-Richtlinie.
7. Binden Sie die Content Switching-Richtlinie an einen virtuellen Content Switching-Server, der bereits für die Umleitung auf den spezifischen virtuellen Lastausgleichsserver konfiguriert ist.
8. Speichern Sie die Konfiguration.

So konfigurieren Sie den Lastenausgleich für MQTT-Datenverkehr mit der CLI

Konfigurieren Sie die Dienste oder Dienstgruppen von MQTT/MQTT_TLS.

```
add service <name> <IP> <protocol> <port>
add servicegroup <ServiceGroupName> <Protocol>
bind servicegroup <serviceGroupName> <IP> <port>
<!--NeedCopy-->
```

Beispiel:

```
add service srvc1 10.106.163.3 MQTT 1883
add servicegroup srvcg1 MQTT
bind servicegroup srvcg1 10.106.163.3 1883
<!--NeedCopy-->
```

Konfigurieren Sie den virtuellen Lastenausgleichsserver MQTT/MQTT_TLS.

```
add lb vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver lb1 MQTT 10.106.163.9 1883
<!--NeedCopy-->
```

Binden Sie die Dienste oder Dienstgruppen von MQTT/MQTT_TLS an den virtuellen MQTT-Lastausgleichserver.


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

Beispiel:

```
bind lb vserver lb1 srvc1
bind lb vserver lb1 srvcg1
<!--NeedCopy-->
```

Konfigurieren Sie den virtuellen MQTT/MQTT_TLS-Content Switching-Server.

```
add cs vserver <name> <protocol> <IPAddress> <port>
<!--NeedCopy-->
```

Beispiel:

```
add cs vserver cs1 MQTT 10.106.163.13 1883
<!--NeedCopy-->
```

Konfigurieren Sie eine Content Switching-Aktion, die den virtuellen Ziel-Lastausgleichsserver angibt

```
add cs action <name> -targetLBVserver <string> [-comment <string>]
<!--NeedCopy-->
```

Beispiel:

```
add cs action act1 -targetlbvserver lbv1
<!--NeedCopy-->
```

Konfigurieren Sie eine Content Switching-Richtlinie.

```
add cs policy <policyName> [-url <string> | -rule <expression>] -
    action <actName>
<!--NeedCopy-->
```


Beispiel:

```
add cs policy cspol1  -rule   “MQTT.COMMAND.EQ(CONNECT) && MQTT.CONNECT
   .FLAGS.QOS.eq(2)”  -action act1
<!--NeedCopy-->
```

Binden Sie die Content Switching-Richtlinie an einen virtuellen Content Switching-Server, der bereits für die Umleitung auf den spezifischen virtuellen Lastausgleichsserver konfiguriert ist.

```
bind cs vserver <virtualServerName> -policyName <policyName> -priority
   <positiveInteger>
<!--NeedCopy-->
```

Beispiel:

```
bind cs vserver cs1  - policyName cspol1 -priority 20
<!--NeedCopy-->
```

Speichern Sie die Konfiguration.

```
save ns config
<!--NeedCopy-->
```

So konfigurieren Sie Load Balancing für MQTT-Datenverkehr mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und erstellen Sie einen virtuellen Lastausgleichsserver vom Typ **MQTT** oder **MQTT_TLS**.
2. Erstellen Sie einen Dienst oder eine Dienstgruppe vom Typ MQTT.
3. Binden Sie den Dienst an den virtuellen MQTT-Server.
4. Klicken Sie auf **Speichern**.

MQTT-Nachrichtenlängenbegrenzung

Die Citrix ADC Appliance behandelt die Nachrichten mit einer Nachrichtenlänge von mehr als 65536 Byte als Jumbo-Pakete und verwirft sie standardmäßig. Der `dropmqttjumbomessage` lb-Parameter entscheidet, ob die Jumbo-Pakete verarbeitet werden oder nicht. Dieser Parameter ist standardmäßig auf **YES**gesetzt, was bedeutet, dass die Jumbo-MQTT-Pakete standardmäßig verworfen

werden. Wenn dieser Parameter auf **NO**gesetzt ist, verarbeitet die ADC-Appliance selbst die Pakete mit einer Nachrichtenlänge von mehr als 65536 Bytes.

So konfigurieren Sie die ADC-Appliance für die Verarbeitung von Jumbo-Paketen mit CLI:

```
Set lb parameter -dropMqttJumboMessage [YES | NO]
<!--NeedCopy-->
```

Beispiel:

```
set lb parameter -dropMqttJumboMessage no
<!--NeedCopy-->
```

Schützen einer Lastausgleichskonfiguration vor Fehlern

October 5, 2021

Wenn ein virtueller Lastausgleichsserver ausfällt oder wenn der virtuelle Server nicht übermäßigen Datenverkehr verarbeiten kann, kann das Lastausgleichs-Setup fehlschlagen. Sie können Ihr Load Balancing-Setup vor einem Ausfall schützen, indem Sie

- die Citrix ADC Appliance, um überschüssigen Datenverkehr auf eine alternative URL umzuleiten,
- einem virtuellen Backup-Lastausgleichsserver und
- ein stateful Verbindungs-Failover.

Clientanforderungen an eine alternative URL umleiten

October 5, 2021

Sie können Anfragen an eine alternative URL umleiten, indem Sie eine HTTP 302-Weiterleitung verwenden, wenn ein virtueller Lastausgleichsserver vom Typ HTTP oder HTTPS HERUNTERGEHT oder deaktiviert ist. Die alternative URL kann Informationen über den Status des Servers liefern. Die konfigurierte Umleitungs-URL wird im Standort-Header der HTTP-Antwort angegeben. Die genaue URL, die in der Antwort angegeben wird, hängt von den folgenden Konfigurationsoptionen ab:

- Wenn die konfigurierte Umleitungs-URL nur den Domänennamen enthält, wie z. B. http://www.sample1.example.com, hängt die in der HTTP-Antwort angegebene Umleitungs-URL den Uniform Resource Identifier (URI) an. Sie wird in der HTTP-Anforderung an den

konfigurierten Domänennamen angegeben. Wenn die Anforderung beispielsweise den http://www.sample2.example.com/images/site_nav.png GET-Header enthält, gibt der Standort-Header in der Umleitungsantwort den Speicherort an: http://www.sample1.example.com/images/site_nav.png Header.

> **Hinweis**
>
> Die Domainnamen in der Anfrage und Antwort können abweichen. In diesem Artikel werden die beiden Domänen als sample1.example.com und sample2.example.com bezeichnet, um das Konzept zu erläutern.

- Wenn die konfigurierte Umleitungs-URL einen vollständigen Pfad enthält, gibt die Umleitungsantwort die vollständig konfigurierte URL an, unabhängig von der URI in der Anfrage. Zum Beispiel sind die folgenden URLs:
  - Angeforderte URL - http://www.redirect.com/en/index.html
  - Umleitungs-URL - http://www.redirect.com/en/site_down.html

In der folgenden Tabelle sind die vorherigen Konfigurationsoptionen aufgeführt:

Konfigurierte Umleitungs-URL	URL in HTTP-Anfrage	Header in HTTP-Antwort
http://www.sample1.example.com	http://www.sample2.example.com/en/index.html	http://www.sample1.example.com/en/index.html
http://www.sample1.example.com/en/error.html	http://www.sample2.example.com/en/index.html	http://www.sample1.example.com/en/error.html

> **Hinweis:**
>
> - Bei der Konfiguration einer http://example.com Umleitungs-URL entspricht die URL nicht mit der http://example.com/ URL, da diese den vollständigen Pfad zum Webroot-Pfad /en-thält.
> - Wenn ein virtueller Lastausgleichsserver sowohl mit einem virtuellen Backupserver als auch mit einer Umleitungs-URL konfiguriert ist, hat der virtuelle Backupserver Vorrang vor der Weiterleitungs-URL. Eine Umleitung wird nur verwendet, wenn sowohl der primäre als auch der virtuelle Backup-Server DOWN sind.

So konfigurieren Sie einen virtuellen Server für die Umleitung der Clientanforderung an eine URL mit der CLI

1. Erstellen Sie einen virtuellen Lastausgleichsserver.

```
set lb vserver -redirect url
```


2. Stellen Sie sicher, dass die Option “URL umleiten” wie erwartet funktioniert. Deaktivieren Sie den virtuellen Server.

   ```
   disable vserver <vserver_name>
   ```

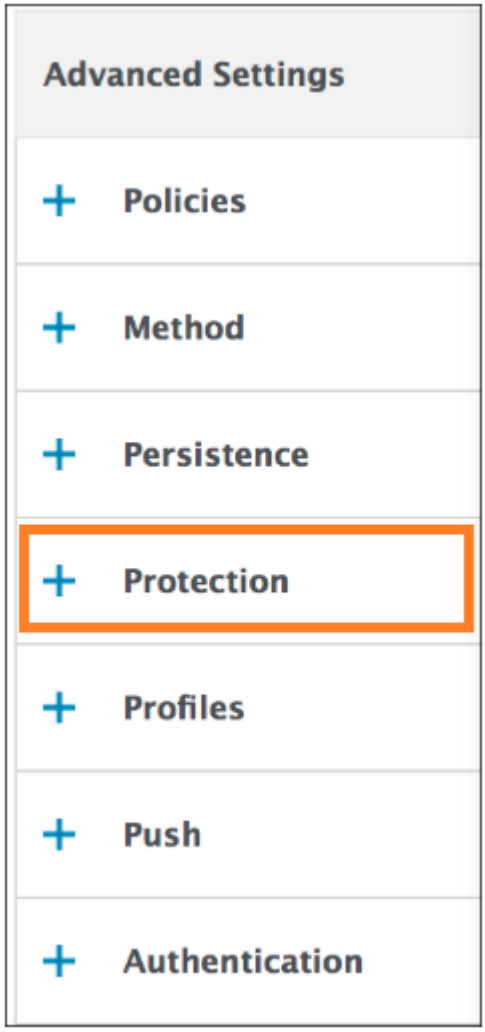
3. Greifen Sie von einem Webbrowser aus auf die Website-URL zu, um zu überprüfen, ob die Anfrage wie erwartet umgeleitet wird. Möglicherweise müssen Sie den Webbrowser-Cache löschen und eine neue Verbindung herstellen, bevor Sie auf die Website zugreifen.

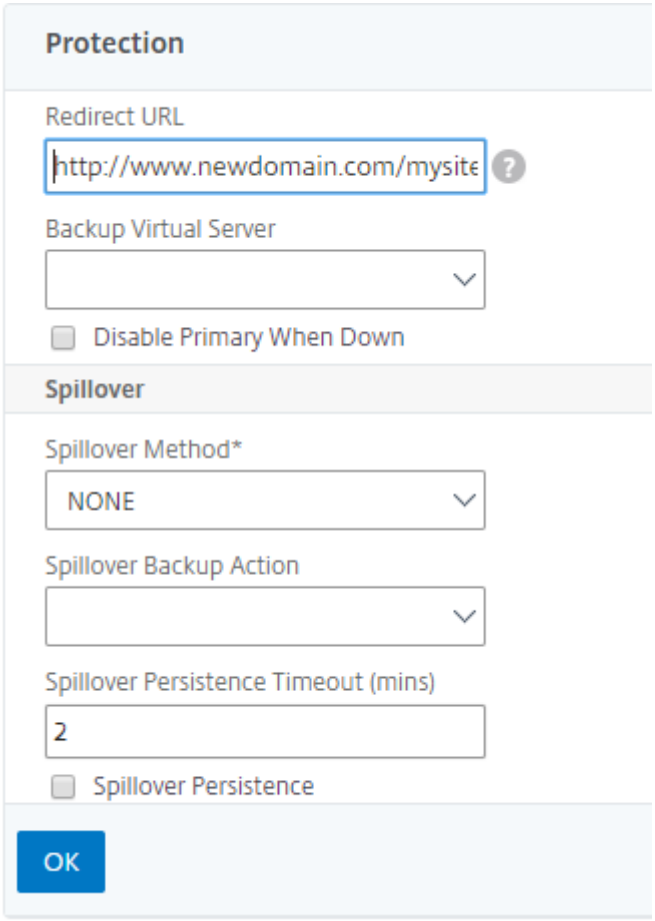
4. Aktivieren Sie den virtuellen Server.

   ```
   enable vserver <vserver_name>
   ```

So konfigurieren Sie einen virtuellen Server für die Umleitung der Clientanforderung an eine URL mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie im Detailbereich auf Hinzufügen, um einen neuen virtuellen Server **hinzuzufügen**.
3. Um einen vorhandenen virtuellen Server zu bearbeiten, wählen Sie den virtuellen Server aus der Liste aus und klicken Sie auf **Bearbeiten**.
4. Klicken Sie auf der Registerkarte **Erweiterte Einstellungen** auf **Schutz**. Geben Sie im Feld **Umleitungs-URL** die Umleitungs-URL ein (z. B. http://www.newdomain.com/mysite/maintenance).





5. Klicken Sie auf **OK**.

Konfigurieren eines virtuellen Backup-Load-Balancing-Servers

October 5, 2021

Sie können die Citrix ADC Appliance so konfigurieren, dass Anfragen an einen virtuellen Sicherungsserver geleitet werden, wenn der virtuelle Server für den primären Lastausgleich DOWN oder nicht verfügbar ist. Der virtuelle Backup-Server ist ein Proxy und ist für den Client transparent. Die Appliance kann auch eine Benachrichtigung über den Standortausfall an den Client senden.

> Hinweis:
>
> Der virtuelle Backup-Server verarbeitet weiterhin die vorhandenen Verbindungen, auch nachdem der primäre virtuelle Server gelöscht oder deaktiviert wurde.

Sie können einen virtuellen Backup-Load Balancing Server konfigurieren, wenn Sie ihn erstellen, oder Sie können die optionalen Parameter eines vorhandenen virtuellen Servers ändern. Sie können auch

einen virtuellen Backup-Server für einen vorhandenen virtuellen Backup-Server konfigurieren und so virtuelle Backup-Server erstellen. Die maximale Tiefe der Kaskadierung virtueller Backup-Server beträgt 10.

Wenn Sie mehrere virtuelle Server haben, die eine Verbindung zu zwei Servern herstellen, haben Sie die Wahl, was passiert, wenn der primäre virtuelle Server ausfällt und dann wieder aktiviert wird. Das Standardverhalten besteht darin, dass der primäre virtuelle Server seine Rolle als primär fortsetzt. Sie können den virtuellen Backup-Server jedoch so konfigurieren, dass er bei Übernahme die Kontrolle behält. Sie können beispielsweise die Updates auf dem virtuellen Backup-Server mit dem primären virtuellen Server synchronisieren und dann den ursprünglichen Primärserver manuell zwingen, seine Rolle fortzusetzen. In diesem Fall können Sie festlegen, dass der virtuelle Sicherungsserver die Kontrolle behält, wenn der primäre virtuelle Server NACH UNTEN geht und dann wieder hochfährt.

Sie können eine Umleitungs-URL auf dem virtuellen primären Lastausgleichsserver als Fallback konfigurieren, wenn sowohl der primäre als auch der virtuelle Backupserver DOWN sind oder deren Schwellenwert für die Verarbeitung von Anforderungen erreicht haben. Wenn Dienste, die an virtuelle Server gebunden sind, Out of Service sind, verwendet die Appliance die Umleitungs-URL.

Hinweis: Wenn ein virtueller Lastausgleichsserver sowohl mit einem virtuellen Backupserver als auch mit einer Umleitungs-URL konfiguriert ist, hat der virtuelle Backupserver Vorrang vor der Weiterleitungs-URL. Eine Umleitung wird nur verwendet, wenn die primären und virtuellen Backup-Server ausfallen.

So legen Sie einen virtuellen Backupserver mit der CLI fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <vServerName> -backupVserver <BackupVServerName> [-
    disablePrimaryOnDown]
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -backupVserver Vserver-LB-2 -
    disablePrimaryOnDown
<!--NeedCopy-->
```


So legen Sie einen virtuellen Backupserver mit der GUI fest

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie den virtuellen Server.
2. Klicken Sie unter Erweiterte Einstellungen auf **Schutz**, und wählen Sie einen virtuellen Backupserver aus.
3. Wenn der virtuelle Backupserver die Kontrolle behalten soll, bis Sie den primären virtuellen Server manuell aktivieren, selbst wenn der primäre virtuelle Server wieder aktiviert ist, wählen Sie **Primär deaktivieren, wenn heruntergefahren**wird.

> **Hinweis:** Ab Citrix ADC Version 12.1 Build 51.xx zeigt die grafische Benutzeroberfläche den Status des Servers an, der angibt, ob das Backup aktiv ist oder nicht.
>
> Der effektive Status des aktuellen Servers kann einer der folgenden sein:
>
> - **UP** — Gibt an, dass der Server UP ist
> - **DOWN** — Gibt an, dass der Server DOWN ist
> - **UP (Backup Active)** — Gibt an, dass der primäre oder der sekundäre virtuelle Server UP ist und der Datenverkehr an den virtuellen Backupserver weitergeleitet wird.
> - **DOWN (Backup Active)** — Gibt an, dass sowohl der primäre als auch der virtuelle Backupserver ausgefallen sind und der Datenverkehr an den virtuellen Backupserver weitergeleitet wird.
>
> Wenn auf dem **primären virtuellen Server die Option Primär deaktivieren** aktiviert ist und der primäre Server ausfällt und wieder auf UP geht, wird der Datenverkehr immer noch vom virtuellen Backupserver bedient, bis der primäre virtuelle Server explizit wieder aktiviert wird. Sie können den Befehl`enable lb vserver <vserver_name>` Befehl verwenden, um den primären virtuellen Server wieder zu aktivieren.

Spillover konfigurieren

October 5, 2021

Eine Spillover-Konfiguration auf der Appliance besteht aus einem primären virtuellen Server, der mit einer Spillover-Methode, einem Spillover-Schwellenwert und einem virtuellen Backupserver konfiguriert ist. Virtuelle Backup-Server können auch für Spillover konfiguriert werden, wodurch eine Kette von Backup-Servern erstellt wird.

Die Spillover-Methode gibt die Betriebsbedingung an, auf der die Spillover-Konfiguration basieren soll (z. B. die Anzahl der etablierten Verbindungen, die Bandbreite oder die kombinierte Integrität der Serverfarm). Wenn eine neue Verbindung eintrifft, überprüft die Appliance, ob der primäre virtuelle Server hochfährt, und vergleicht den Betriebszustand mit dem konfigurierten Spillover-

Schwellenwert. Wenn der Schwellenwert erreicht ist, leitet das Spillover-Feature neue Verbindungen an den ersten verfügbaren virtuellen Server in der Backupkette um. Der virtuelle Backupserver verwaltet die empfangenen Verbindungen, bis die Last auf dem primären Server unter den Schwellenwert fällt.

Wenn Sie die Spillover-Persistenz konfigurieren, verarbeitet der virtuelle Backup-Server die empfangenen Verbindungen, auch wenn die Last auf dem primären Schwellenwert unterschritten wird. Wenn Sie die Persistenz von Überschreitungen und ein Timeout für die Persistenz von Überschreitungen konfigurieren, verarbeitet der virtuelle Backupserver Verbindungen nur für den angegebenen Zeitraum, nachdem die Last auf dem primären Wert unter den Schwellenwert fällt.

Hinweis: Normalerweise wird Spillover ausgelöst, wenn der mit der Spillover-Methode verknüpfte Wert den Schwellenwert überschreitet (z. B. Anzahl der Verbindungen). Bei der Server-Health-Spillover-Methode wird Spillover jedoch ausgelöst, wenn der Zustand der Serverfarm unter den Schwellenwert fällt.

Sie können Spillover auf eine der folgenden Arten konfigurieren:

- Geben Sie eine vordefinierte Spillover-Methode an. Es stehen vier vordefinierte Methoden zur Verfügung, die gängige Spillover-Anforderungen erfüllen.
- Konfigurieren Sie richtlinienbasiertes Spillover. In richtlinienbasiertem Spillover verwenden Sie eine Citrix ADC Regel, um die Bedingungen für das Auftreten von Spillover anzugeben. Mit den Citrix ADC Regeln können Sie Spillover für verschiedene Betriebsbedingungen konfigurieren.

Verwenden Sie richtlinienbasiertes Spillover, wenn eine vordefinierte Methode Ihre Anforderungen nicht erfüllt. Wenn Sie beide für einen primären virtuellen Server konfigurieren, hat die richtlinienbasierte Spillover-Konfiguration Vorrang vor der vordefinierten Methode.

Zuerst erstellen Sie den primären virtuellen Server und die virtuellen Server, die Sie für die Backupkette benötigen. Sie richten die Backupkette ein, indem Sie einen virtuellen Server als Backup für den primären Server angeben (d. h. Sie erstellen einen sekundären virtuellen Server), einen virtuellen Server als Backup für den sekundären (d. h. Sie erstellen einen tertiären virtuellen Server) usw. Anschließend konfigurieren Sie Spillover, indem Sie entweder eine vordefinierte Spillover-Methode angeben oder Spillover-Richtlinien erstellen und binden.

Anweisungen zum Zuweisen eines virtuellen Servers als Backup für einen anderen virtuellen Server finden Sie unter Konfigurieren eines virtuellen Backup-Lastausgleichsservers.

Konfigurieren einer vordefinierten Spillover-Methode

Vordefinierte Spillover-Methoden erfüllen einige der häufigsten Spillover-Anforderungen. Um eine der vordefinierten Spillover-Methoden zu verwenden, konfigurieren Sie Spillover-Parameter auf dem primären virtuellen Server. Um eine Kette von virtuellen Backup-Servern zu erstellen, konfigurieren Sie auch Spillover-Parameter auf virtuellen Backup-Servern.

Wenn die virtuellen Backup-Server ihre eigenen Schwellenwerte erreichen und der Diensttyp TCP lautet, sendet die Citrix ADC Appliance Clients einen TCP-Reset. Bei den Diensttypen HTTP, SSL und RTSP werden neue Anforderungen an die für den primären virtuellen Server konfigurierte Umleitungs-URL umgeleitet. Eine Umleitungs-URL kann nur für virtuelle HTTP-, SSL- und RTSP-Server angegeben werden. Wenn keine Umleitungs-URL konfiguriert ist, sendet die Citrix ADC Appliance Clients einen TCP-Reset (wenn der virtuelle Server vom Typ TCP ist) oder eine HTTP 503-Antwort (wenn der virtuelle Server vom Typ HTTP oder SSL ist).

Hinweis: Bei virtuellen RTSP-Servern verwendet die Citrix ADC Appliance nur Datenverbindungen für Spillover. Wenn der virtuelle Backupserver RTSP nicht verfügbar ist, werden die Anforderungen an eine RTSP-URL umgeleitet und eine RTSP-Umleitungsnachricht an den Client gesendet.

So konfigurieren Sie eine vordefinierte Spillover-Methode für einen virtuellen Server mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <vServerName> -soMethod <spillOverType> -soThreshold <
    positiveInteger> -soPersistence ENABLED -soPersistenceTimeout <
    positiveInteger>
<!--NeedCopy-->
```

Beispiel

```
set lb vserver Vserver-LB-1 -soMethod Connection -soThreshold 1000 -
    soPersistence enabled -soPersistenceTimeout 2
<!--NeedCopy-->
```

So konfigurieren Sie eine vordefinierte Spillover-Methode für einen virtuellen Server mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie den virtuellen Server.
2. Klicken Sie unter Erweiterte Einstellungen auf **Schutz**, und legen Sie die Spillover-Parameter fest.

Richtlinienbasiertes Spillover konfigurieren

Spillover-Richtlinien, die auf Regeln (Ausdrücke) basieren, ermöglichen es Ihnen, die Appliance für eine breitere Palette von Spillover-Szenarien zu konfigurieren. Beispielsweise können Sie den Spillover basierend auf der Reaktionszeit des virtuellen Servers oder basierend auf der Anzahl der Verbindungen in der Überspannungswarteschlange des virtuellen Servers konfigurieren.

Um richtlinienbasierte Spillover zu konfigurieren, erstellen Sie zunächst eine Spillover-Aktion. Anschließend wählen Sie den Ausdruck aus, den Sie in der Spillover-Richtlinie verwenden möchten, konfigurieren die Richtlinie und verknüpfen die Aktion mit ihr. Schließlich binden Sie die Spillover-Richtlinie an einen virtuellen Lastausgleich, Content Switching oder globalen Server Lastausgleichsserver. Sie können mehrere Spillover-Richtlinien mit Prioritätsnummern an einen virtuellen Server binden. Die Appliance wertet die Spillover-Richtlinien in aufsteigender Reihenfolge der Prioritätsnummern aus und führt die Aktion aus, die der letzten Richtlinie zugeordnet ist, die auf TRUE ausgewertet werden soll.

Ein virtueller Server kann auch eine Backupaktion durchführen. Die Backupaktion wird ausgeführt, wenn der virtuelle Server nicht über einen oder mehrere virtuelle Backup-Server verfügt oder alle virtuellen Backup-Server DOWN oder deaktiviert sind oder ihre eigenen Spillover-Grenzen erreicht haben.

Wenn eine Spillover-Richtlinie zu einer UNDEF-Bedingung führt (eine Ausnahme, die ausgelöst wird, wenn das Ergebnis der Richtlinienbewertung nicht definiert ist), wird eine UNDEF-Aktion ausgeführt. Die UNDEF-Aktion ist immer ACCEPT. Sie können keine UNDEF-Aktion Ihrer Wahl angeben.

Konfigurieren einer Spillover-Aktion

Eine Spillover-Aktion wird ausgeführt, wenn die Spillover-Richtlinie, mit der sie verknüpft ist, TRUE ausgewertet wird. Derzeit ist SPILLOVER die einzige unterstützte Spillover-Aktion.

So konfigurieren Sie richtlinienbasierte Spillover mit der Befehlszeilenschnittstelle

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

```
1 add spillover action <name> -action SPILLOVER
2
3 show spillover action <name>
4 <!--NeedCopy-->
```


Beispiel

```
add spillover action mySoAction -action SPILLOVER
Done
<!--NeedCopy-->
```

```
show spillover action mySoAction
1) Name: mySoAction Action: SPILLOVER
Done
<!--NeedCopy-->
```

Auswählen eines Ausdrucks für die Spillover-Richtlinie

Im Richtlinienausdruck können Sie einen beliebigen virtualserver-basierten Ausdruck verwenden, der einen booleschen Wert zurückgibt. Zum Beispiel können Sie einen der folgenden Ausdrücke verwenden:

```
SYS.VSERVER("vserver").RESPTIME.GT(<int>)
SYS.VSERVER("vserver").STATE.EQ( " <string> " ), and
SYS.VSERVER("vserver").THROUGHPUT.LT    (<int>)
<!--NeedCopy-->
```

Zusätzlich zu den vorhandenen Funktionen wie RESPTIME, STATE und THROUGHPUT können Sie die folgenden virtuellen serverbasierten Funktionen verwenden, die mit dieser Funktion eingeführt wurden:

`Averagesurgecount`

Gibt die durchschnittliche Anzahl von Anforderungen in den Überspannungswarteschlangen aktiver Dienste zurück. Gibt 0 (Null) zurück, wenn keine aktiven Dienste vorhanden sind. Löst eine UNDEF-Bedingung aus, wenn sie mit einem virtuellen Content Switching- oder globalen Server Load Balancing-Server verwendet wird.

`Activeservices`

Gibt die Anzahl der aktiven Dienste zurück. Löst eine UNDEF-Bedingung aus, wenn sie mit einem virtuellen Content Switching- oder globalen Server Load Balancing-Server verwendet wird.

`Activetransactions`

Gibt den Wert des Leistungsindikators auf Virtual-Serverebene für aktuelle aktive Transaktionen zurück.

is_dynamic_limit_reached

Gibt einen booleschen TRUE zurück, wenn die Anzahl der Verbindungen, die der virtuelle Server verwaltet, dem dynamisch berechneten Schwellenwert entspricht. Der dynamische Schwellenwert ist die Summe der maximalen Clienteinstellungen (Max Clients) der gebundenen Dienste, die UP sind.

Sie können einen Richtlinienausdruck verwenden, um eine der vordefinierten Spillover-Methoden zu implementieren. In der folgenden Tabelle werden die vordefinierten Spillover-Methoden den Ausdrücken zugeordnet, mit denen Sie sie implementieren können:

Tabelle 1. Konvertieren vordefinierter Spillover-Methoden in Richtlinienausdrücke

Vordefinierte Spillover-Methode	Entsprechender Ausdruck
CONNECTION	SYS.VSERVER(“<vserver-name>”).CONNECTIONS, used with the GT(int) arithmetic function.
BANDWIDTH	SYS.VSERVER(“<vserver-name>”).THROUGHPUT, used with the GT(int) arithmetic function.
HEALTH	SYS.VSERVER(“<vserver-name>”).HEALTH, used with the LT(int) arithmetic function.
DYNAMICCONNECTION	SYS.VSERVER (“<vserver-name>”) .IS_DYNAMIC_LIMIT_REACHED **Hinweis**: Wenn Sie einen richtlinienbasierten Spillover mit der Funktion IS_DYNAMIC_LIMIT_REACHED implementieren, müssen Sie auch die vordefinierte DYNAMICCONNECTION-Methode für den virtuellen Server konfigurieren, damit die für Spillover erforderlichen Statistiken funktionieren werden gesammelt.

Konfigurieren einer Spillover-Richtlinie

Eine Spillover-Richtlinie verwendet in der Regel einen booleschen Ausdruck, um die Bedingungen anzugeben, die erfüllt werden müssen, damit Spillover auftreten kann.

So konfigurieren Sie eine Spillover-Richtlinie mit der Befehlszeilenschnittstelle

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

```
1 add spillover policy <name> -rule <expression> -action <string> [-
     comment <string>]
2
3 show spillover policy <name>
4 <!--NeedCopy-->
```

Beispiel

```
1 > add spillover policy mySoPolicy -rule SYS.VSERVER(”v1”).RESPTIME.GT
     (50) -action mySoAction -comment ”Triggers spillover when the
     vserver's response time is greater than 50 ms.”
2 Done
3
4 > show spillover policy mySoPolicy
5
6 1)  Name: mySoPolicy Rule: ”SYS.VSERVER(”v1”).RESPTIME.GT(50)” Action:
     mySoAction Hits: 0 ActivePolicy: 0
7 Comment: ”Triggers spillover when the vserver's response time is
     greater than 50 ms.”
8 Done
9 >
10 <!--NeedCopy-->
```

Binden einer Spillover-Richtlinie an einen virtuellen Server

Sie können eine Spillover-Richtlinie an virtuelle Lastausgleichs-, Content Switching- oder globale Server Load Balancing-Server binden). Sie können mehrere Richtlinien an einen virtuellen Server binden, wobei Goto-Ausdrücke den Auswertungsablauf steuern.

So binden Sie eine Spillover-Richtlinie mit der Befehlszeilenschnittstelle an einen virtuellen Server

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Spillover-Richtlinie an einen Lastausgleich, Content Switching oder einen globalen Server Lastausgleichsserver zu binden, und überprüfen Sie die Konfiguration:


```
bind (lb | cs | gslb) vserver <name> -policyName <string> -priority <
    positive_integer> [-gotoPriorityExpression <expression>]

show (lb | cs | gslb) vserver <name>
<!--NeedCopy-->
```

Beispiel

```
> bind lb vserver vserver1 -policyName mySoPolicy -priority 5
Done
> show lb vserver vserver1
vserver1 (2.2.2.12:80) - HTTP Type: ADDRESS
. . .

1)  Spillover Policy Name: mySoPolicy Priority: 5
GotoPriority Expression: END
Flowtype: REQUEST
Done
>
<!--NeedCopy-->
```

Konfigurieren einer Backupaktion für ein Spillover-Ereignis

Eine Backupaktion gibt an, was zu tun ist, wenn der Spillover-Schwellenwert erreicht wird, aber mindestens ein virtueller Backup-Server entweder nicht konfiguriert oder heruntergefahren oder deaktiviert sind oder ihre eigenen Schwellenwerte erreicht haben.

Hinweis: Für die vordefinierten Spillover-Methoden, die direkt auf dem virtuellen Server konfiguriert sind (als Werte des Parameters Spillover-Methode), ist die Backupaktion nicht konfigurierbar. Standardmäßig sendet die Appliance Clients einen TCP-Reset (wenn der virtuelle Server vom Typ TCP ist) oder eine HTTP 503-Antwort (wenn der virtuelle Server vom Typ HTTP oder SSL ist).

Die Backupaktion wird auf dem virtuellen Server konfiguriert. Sie können den virtuellen Server so konfigurieren, dass er Anfragen annimmt (nachdem der in der Richtlinie angegebene Schwellenwert erreicht wurde), Clients an eine URL umleiten oder Anfragen einfach löschen, bevor TCP- oder SSL-Verbindungen hergestellt werden, bis die Anzahl der Anforderungen unter den Schwellenwert fällt. Daher werden weniger Speicherressourcen verwendet, wenn die Verbindungen zurückgesetzt werden, noch bevor Datenstrukturen zugewiesen werden.

So konfigurieren Sie eine Backupaktion für Spillover mit der CLI

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

```
set lb vserver <name> -soBackupAction <soBackupAction>

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

Beispiel:

```
set lb vserver vs1 -soBackupAction REDIRECT -redirectURL `http://www.
   mysite.com/maintenance`
Done
> show lb vserver vs1
vs1 (10.102.29.76:80) - HTTP Type: ADDRESS
State: UP
. . .
Redirect URL: `http://www.mysite.com/maintenance`
. . .
Done
<!--NeedCopy-->
```

So konfigurieren Sie eine Backupaktion für Spillover mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie den virtuellen Server.
2. Klicken Sie unter Erweiterte Einstellungen auf **Schutz**, und geben Sie dann eine Spillover-Backupaktion an.

Verbindungsfailover

July 8, 2022

Das Verbindungsfailover verhindert eine Unterbrechung des Zugriffs auf Anwendungen, die in einer verteilten Umgebung bereitgestellt werden. In einer Citrix ADC High Availability (HA) -Setup bezieht sich *Verbindungsfailover* (oder *Verbindungsspiegelung-CM*) darauf, eine etablierte TCP- oder UDP-Verbindung aktiv zu halten, wenn ein Failover auftritt. Die neue primäre Citrix ADC-Appliance verfügt

über Informationen zu den Verbindungen, die vor dem Failover hergestellt wurden, und bedient diese Verbindungen weiterhin. Nach dem Failover bleibt der Client mit demselben physischen Server verbunden. Die neue primäre Appliance synchronisiert die Informationen mit der neuen sekundären Appliance. Wenn der Parameter L2Conn gesetzt ist, werden Layer 2-Verbindungsparameter ebenfalls mit dem sekundären synchronisiert.

> Hinweis:
>
> Betrachten Sie ein HA-Setup, bei dem ein Client eine Sitzung mit dem primären Knoten einrichtet, der wiederum eine Sitzung mit dem Back-End-Server einrichtet. Wenn in diesem Zustand ein Failover ausgelöst wird, werden die Pakete, die von den vorhandenen Client- und Serverknoten auf einem neuen Primärgerät empfangen werden, als veraltete Pakete behandelt, und die Client- und Serververbindungen werden zurückgesetzt. Wenn ein zustandsloses Verbindungsfailover aktiviert ist (USIP ist ON), werden die Verbindungen nach dem Failover nicht zurückgesetzt, wenn Sie Pakete von Client- oder Serverknoten erhalten. Stattdessen werden die Client- und Serververbindungen dynamisch erstellt.

Sie können das Verbindungs-Failover entweder im zustandslosen oder im statusbehafteten Modus einrichten. Im Failover-Modus für statuslose Verbindungen tauschen die HA-Knoten keine Informationen über die Verbindungen aus, bei denen ein Failover durchgeführt wurde. Diese Methode hat keinen Laufzeit-Overhead.

Im statusbehafteten Verbindungsfailover-Modus synchronisiert das primäre Gerät die Daten der Failover-Verbindungen mit dem neuen sekundären Gerät.

Verbindungs-Failover ist hilfreich, wenn Ihre Bereitstellung über langlebige Verbindungen verfügt. Wenn Sie beispielsweise eine große Datei über FTP herunterladen und während des Downloads ein Failover auftritt, wird die Verbindung unterbrochen, und der Download wird abgebrochen. Wenn Sie das Verbindungs-Failover jedoch im Stateful-Modus konfigurieren, wird der Download auch nach dem Failover fortgesetzt.

Funktionsweise des Verbindungs-Failovers auf Citrix ADC-Appliances

In einem zustandslosen Verbindungsfailover versucht die neue primäre Appliance, den Paketfluss gemäß den Informationen, die in den empfangenen Paketen enthalten sind, neu zu erstellen.

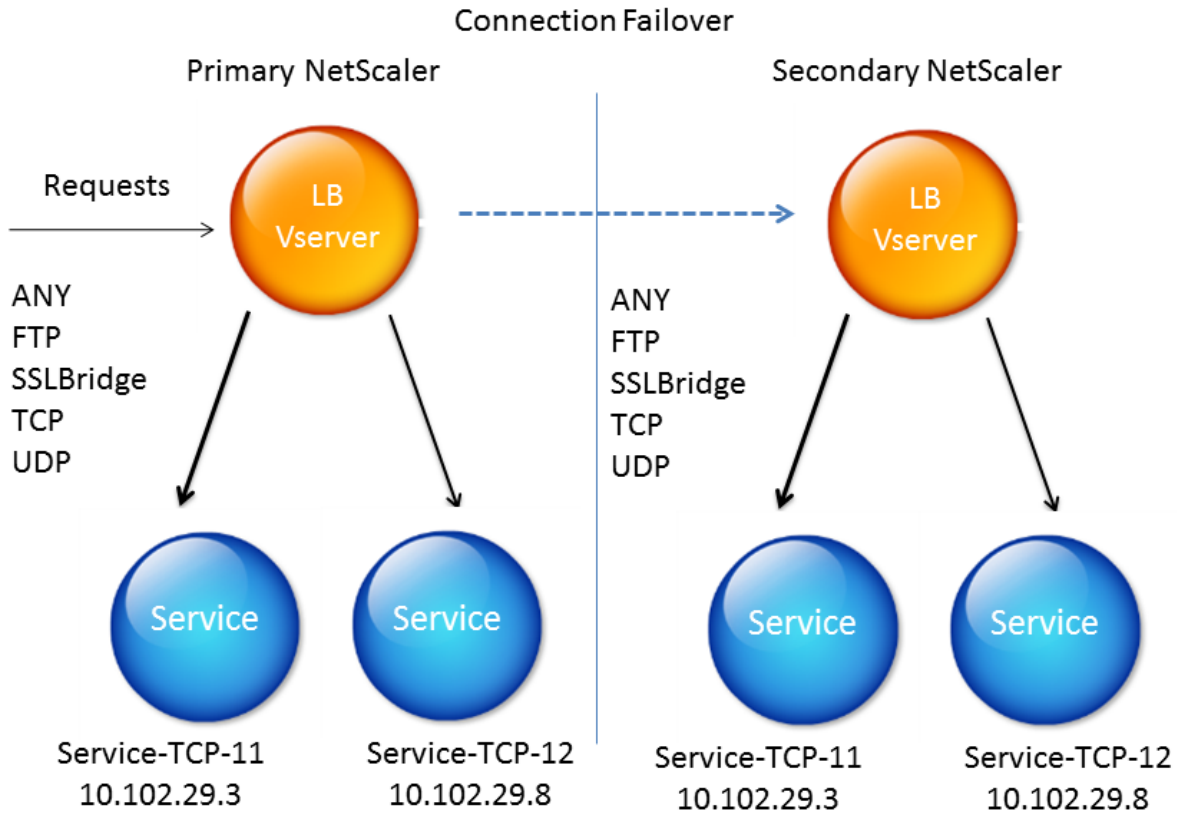
Im statusbehafteten Failover sendet die primäre Appliance Nachrichten an die sekundäre Appliance, um aktuelle Informationen über die gespiegelten Verbindungen beizubehalten. Die sekundäre Appliance verwaltet die Daten, die sich auf die Pakete beziehen, verwendet sie jedoch nur im Falle eines Failovers. Wenn ein Failover auftritt, verwendet die neue primäre (alte sekundäre) Appliance die gespeicherten Daten über die gespiegelten Verbindungen und akzeptiert Datenverkehr. Während der Übergangsphase können der Client und der Server eine kurze Unterbrechung und erneute Übertragung erfahren.

Hinweis:

Stellen Sie sicher, dass sich die primäre Appliance auf der sekundären Appliance selbst autorisieren kann. Um die korrekte Konfiguration der Kennwörter zu überprüfen, verwenden Sie den Befehl show `rpcnode` von der Befehlszeile aus oder verwenden Sie die RPC-Option des Menüs **Netzwerk** in der GUI.

Eine grundlegende HA-Konfiguration mit Verbindungs-Failover enthält die in der folgenden Abbildung gezeigten Entitäten.

Abbildung 1. Verbindungs-Failover-Entitätsdiagramm



Hinweis

Verbindungs-Failover wird nach einem der folgenden Ereignisse nicht unterstützt:

```
- An upgrade to a later release.
- An upgrade to a later build within the same release, if the new
    build uses a different HA version.
```


Unterstützte Einrichtung

Das Verbindungsfailover kann nur auf virtuellen Servern mit Lastausgleich konfiguriert werden. Es kann nicht auf virtuellen Content Switching-Servern konfiguriert werden. Wenn Sie das Verbindungs-Failover auf virtuellen Lastenausgleichs-Servern aktivieren, die an einen virtuellen Content Switching-Server angeschlossen sind, funktioniert das Verbindungs-Failover nicht, da die virtuellen Server mit Lastenausgleich den Datenverkehr zunächst nicht akzeptieren.

In der folgenden Tabelle wird das Setup beschrieben, das für Verbindungs-Failover unterstützt wird.

Tabelle 1. Verbindungsfailover — Unterstütztes Setup

Einstellung	Zustandslos	Zustandsvoll
Typ des Dienstes	ANY.	ANY, UDP, TCP, FTP, SSL_BRIDGE.
Load Balancing-Methoden	Alle für den Diensttyp ANY unterstützten Methoden. Wenn die Source IP-Persistenz jedoch nicht festgelegt ist, muss die Methode SRCIPSRCPORTHASH verwendet werden.	Alle Methoden, die für die unterstützten Diensttypen gelten.
Persistence-Typen	SOURCEIP-Beständigkeit.	Alle Typen, die für die unterstützten Servicetypen gelten, werden unterstützt.
USIP	Muss AN sein.	Keine Einschränkung. Es kann EIN oder AUS sein.
Service-Bindungen	Der Dienst kann nur an einen virtuellen Server gebunden werden.	Der Dienst kann an einen oder mehrere virtuelle Server gebunden sein.
Internet Protocol (IP) -Versionen	IPv4 und IPv6	IPV4 und IPv6
Unterstützung für Redundanz	Clustering und Hochverfügbarkeit	Hohe Verfügbarkeit

> Hinweis:
>
> Stateful-Verbindungs-Failover wird nur für verbindungsbasierte Switching-Dienste unterstützt, z. B. Da HTTP anforderungsbasiertes Switching verwendet, unterstützt es kein Verbindungs-

> Failover. In SSL werden die vorhandenen Verbindungen nach dem Failover zurückgesetzt.

Features, die von Verbindungs-Failover betroffen sind

In der folgenden Tabelle sind die Funktionen aufgeführt, die von der Konfiguration des Verbindungsfailovers betroffen sind.

Tabelle 2. Wie sich das Verbindungsfailover auf die Citrix ADC-Funktionen auswirkt

Feature	Auswirkungen des Verbindungs-Failovers
SYN-Schutz	Wenn bei jeder Verbindung ein Failover auftritt, nachdem die Appliance SYN-ACK ausgegeben hat, aber bevor sie das endgültige ACK erhält, wird die Verbindung vom Verbindungs-Failover nicht unterstützt. Der Client muss die Anforderung erneut ausstellen, um die Verbindung herzustellen.
Überlastungsschutz	Wenn das Failover auftritt, bevor eine Verbindung mit dem Server hergestellt wird, versucht die neue primäre Appliance, die Verbindung mit dem Server herzustellen. Es überträgt auch alle Pakete, die während des Überlastungsschutzes aufbewahrt werden.
Zugriff nicht verfügbar	Wenn diese Option aktiviert ist, hat die Access-Down-Funktionalität Vorrang vor dem Verbindungs-Failover.
Anwendungs-Firewall	Die Funktion der Anwendungs-Firewall wird nicht unterstützt.
INC	Eine unabhängige Netzwerkkonfiguration wird im Hochverfügbarkeitsmodus nicht unterstützt.
TCP-Pufferung	Die TCP-Pufferung ist mit der Verbindungsspiegelung nicht kompatibel.
Nach Antwort schließen	Nach dem Failover werden die NATPCBs bei der Antwort möglicherweise nicht geschlossen.

So konfigurieren Sie das Verbindungs-Failover mit der GUI

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**. Öffnen Sie den virtuellen Server, klicken Sie in den **Erweiterten Einstellungen**auf **Schutz**und wählen Sie **Verbindungsfailover** als **zustandsbehaftet**aus.

So konfigurieren Sie das Verbindungsfailover mithilfe von CLI

An der Eingabeaufforderung:

```
set lb vserver <vServerName> -connFailover <Value>
show lb vserver <vServerName>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -connFailover stateful
Done
<!--NeedCopy-->
```

Wenn das Verbindungs-Failover auf einem virtuellen Server deaktiviert ist, werden die dem virtuellen Server zugewiesenen Ressourcen freigegeben.

So deaktivieren Sie das Verbindungsfailover mithilfe von CLI

An der Eingabeaufforderung:

```
set lb vserver <vServerName> -connFailover <Value>
show lb vserver <vServerName>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -connFailover disable
Done
<!--NeedCopy-->
```


So deaktivieren Sie das Verbindungs-Failover mit der GUI

Navigieren Sie zu **Traffic Management**> **Load Balancing**> **Virtuelle Server**. Öffnen Sie den virtuellen Server, wählen Sie **unter SchutzVerbindungsfailover** als Deaktiviert aus.

Überspannungswarteschlange leeren

October 5, 2021

Wenn ein physischer Server eine Welle von Anforderungen empfängt, wird es langsam, auf die Clients zu reagieren, die derzeit mit ihm verbunden sind, was die Benutzer unzufrieden und verärgert lässt. Oft führt die Überlastung auch dazu, dass Clients Fehlerseiten erhalten. Die Citrix ADC Appliance bietet Funktionen wie Überspannungsschutz, der die Rate steuert, mit der neue Verbindungen zu einem Dienst hergestellt werden können, und so Überlastungen vermeiden.

Die Appliance verbindet Multiplexing zwischen Clients und physischen Servern. Wenn es eine Clientanforderung für den Zugriff auf einen Dienst auf einem Server erhält, sucht die Appliance nach einer bereits eingerichteten Verbindung mit dem Server, die frei ist. Wenn eine freie Verbindung gefunden wird, wird diese Verbindung verwendet, um eine virtuelle Verbindung zwischen dem Client und dem Server herzustellen. Wenn es keine vorhandene freie Verbindung findet, baut die Appliance eine neue Verbindung mit dem Server auf und stellt eine virtuelle Verbindung zwischen dem Client und dem Server her. Wenn die Appliance jedoch keine neue Verbindung mit dem Server herstellen kann, sendet sie die Clientanforderung an eine Überspannungswarteschlange. Wenn alle physischen Server, die an den virtuellen Lastausgleichs- oder Content Switching-Server gebunden sind, die obere Grenze für Clientverbindungen erreichen (maximaler Clientwert, Überspannungsschutzschwelle oder maximale Kapazität des Dienstes), kann die Appliance keine Verbindung zu einem Server herstellen. Die Überspannungsschutzfunktion verwendet die Überspannungswarteschlange, um die Geschwindigkeit zu regulieren, mit der Verbindungen mit den physischen Servern geöffnet werden. Die Appliance verwaltet eine andere Überspannungswarteschlange für jeden Dienst, der an den virtuellen Server gebunden ist.

Die Länge einer Überspannungswarteschlange erhöht sich, wenn eine Anforderung gestellt wird, für die die Appliance keine Verbindung herstellen kann. Die Länge einer Überspannungswarteschlange nimmt unter einer der folgenden Bedingungen ab:

- Eine Anfrage in der Warteschlange wird an den Server gesendet.
- Eine Anfrage wird zeitüberschreitend und wird aus der Warteschlange entfernt.

Wenn die Überspannungswarteschlange für einen Dienst oder eine Dienstgruppe zu lang wird, sollten Sie sie möglicherweise leeren. Sie können die Überspannungswarteschlange eines bestimmten Dienstes oder einer bestimmten Dienstgruppe oder aller Dienste und Dienstgruppen,

die an einen virtuellen Lastausgleichsserver gebunden sind, leeren. Das Leeren einer Überspannungswarteschlange wirkt sich nicht auf die vorhandenen Verbindungen aus. Nur die Anforderungen, die in der Überspannungswarteschlange vorhanden sind, werden gelöscht. Für diese Anfragen muss der Kunde eine neue Anfrage stellen.

Sie können auch die Überspannungswarteschlange eines virtuellen Content Switching-Servers löschen. Wenn ein virtueller Content Switching-Server einige Anfragen an einen bestimmten virtuellen Lastausgleichsserver weiterleitet und der virtuelle Lastausgleichsserver auch einige andere Anfragen empfängt, wenn Sie die Überspannungswarteschlange des virtuellen Content Switching-Servers leeren, nur die Anfragen, die von diesem Content Switching empfangen wurden virtuelle Server werden geleert. Die anderen Anforderungen in der Überspannungswarteschlange des virtuellen Lastausgleichsservers werden nicht geleert.

Hinweis: Sie können die Überspannungswarteschlangen der Cache-Umleitung, Authentifizierung, VPN oder virtuellen GSLB-Servern oder GSLB-Diensten nicht leeren.

Hinweis: Verwenden Sie die Funktion Überspannungsschutz nicht, wenn die Quell-IP (USIP) aktiviert ist.

So leeren Sie eine Überspannungswarteschlange mit der CLI

Der Befehl flush ns SurgeQ funktioniert wie folgt:

- Sie können den Namen eines Dienstes, einer Dienstgruppe oder eines virtuellen Servers angeben, dessen Überspannungswarteschlange geleert werden muss.
- Wenn Sie während der Ausführung des Befehls einen Namen angeben, wird die Überspannungswarteschlange der angegebenen Entität geleert. Wenn mehr als eine Entität denselben Namen hat, lötet die Appliance die Überspannungswarteschlangen aller dieser Entitäten.
- Wenn Sie den Namen einer Dienstgruppe und einen Servernamen und einen Port angeben, während der Befehl ausgeführt wird, löscht die Appliance die Überspannungswarteschlange nur des angegebenen Dienstgruppenmitglieds.
- Sie können ein Dienstgruppenmitglied (<serverName> und <port>) nicht direkt angeben, ohne den Namen der Dienstgruppe (<name>) anzugeben, und Sie können nicht <port> ohne <serverName> angeben. Geben Sie <serverName> und <port> an, wenn Sie die Überspannungswarteschlange für ein bestimmtes Dienstgruppenmitglied leeren möchten.
- Wenn Sie den Befehl ausführen, ohne Namen anzugeben, legt die Appliance die Überspannungswarteschlangen aller auf der Appliance vorhandenen Entitäten.
- Wenn ein Dienstgruppenmitglied mit einem Servernamen identifiziert wird, müssen Sie den Servernamen in diesem Befehl angeben. Sie können die IP-Adresse nicht angeben.

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
flush ns surgeQ [-name <name>] [-serverName <serverName> <port>]
<!--NeedCopy-->
```

Beispiele

```
flush ns surgeQ  -name SVC1ANZGB  -serverName 10.10.10.1 80
<!--NeedCopy-->
```

Der vorherige Befehl spült die Überspannungswarteschlange des Dienstes oder virtuellen Servers mit dem Namen SVC1ANZGB und hat die IP-Adresse als 10.10.10

```
flush ns surgeQ
<!--NeedCopy-->
```

Der vorherige Befehl spült alle Überspannungswarteschlangen auf der Appliance.

So leeren Sie eine Überspannungswarteschlange mit der GUI

Navigieren Sie zu **Traffic Management** > **Content Switching** > **Virtuelle Server**, wählen Sie einen virtuellen Server aus und wählen Sie in der Liste Aktion die Option **Überspannungswarteschlange leeren**aus.

Verwalten eines Lastausgleichs

October 5, 2021

Ein vorhandenes Lastenausgleichs-Setup erfordert nicht viel Arbeit, solange es unverändert ist, aber die meisten bleiben nicht lange unverändert. Die Erhöhung der Last erfordert neue Server mit Lastenausgleich und schließlich neue Citrix ADC Appliances, die konfiguriert und dem vorhandenen Setup hinzugefügt werden müssen. Alte Server verschleißen und müssen ausgetauscht werden, sodass einige Server entfernt und andere hinzugefügt werden müssen. Upgrades Ihrer Netzwerkausrüstung oder Änderungen an der Topologie erfordern möglicherweise auch Änderungen an Ihrem Lastenausgleichs-Setup. Daher müssen Sie Vorgänge auf Serverobjekten, Diensten und virtuellen Servern ausführen. Der Visualizer kann Ihre Konfiguration grafisch anzeigen, und Sie können Operationen an den Entitäten in der Anzeige ausführen. Sie können auch andere Funktionen nutzen, die die Verwaltung des Datenverkehrs durch Ihr Load Balancing-Setup erleichtern.

Verwalten von Serverobjekten

December 7, 2021

Während des grundlegenden Load Balancing-Setups wird beim Erstellen eines Dienstes ein Serverobjekt mit der IP-Adresse des Dienstes erstellt, falls eines nicht vorhanden ist. Wenn Sie für Ihre Dienstobjekte bevorzugen, die mit Domänennamen anstelle von IP-Adressen benannt sind, haben Sie möglicherweise auch ein oder mehrere Serverobjekte manuell erstellt. Sie können jedes Serverobjekt aktivieren, deaktivieren oder entfernen.

Wenn Sie ein Serverobjekt aktivieren oder deaktivieren, aktivieren oder deaktivieren Sie alle mit dem Serverobjekt verknüpften Dienste. Wenn Sie die Citrix ADC Appliance nach dem Deaktivieren eines Serverobjekts aktualisieren, wird der Status des Dienstes als OUT OF SERVICE angezeigt. Wenn Sie beim Deaktivieren eines Serverobjekts eine Wartezeit angeben, verarbeitet das Serverobjekt weiterhin bestehende Verbindungen für die angegebene Zeit, weist jedoch neue Verbindungen zurück. Wenn Sie ein Serverobjekt entfernen, wird auch der Dienst gelöscht, an den es gebunden ist.

So aktivieren Sie einen Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable server <name>
<!--NeedCopy-->
```

Beispiel:

```
enable server 10.102.29.5
<!--NeedCopy-->
```

So aktivieren oder deaktivieren Sie ein Serverobjekt mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Server**.
2. Wählen Sie den Server aus und wählen Sie in der Liste Aktion **Aktivieren** oder **Deaktivieren** aus.

So deaktivieren Sie ein Serverobjekt mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
disable server <name> <delay>
<!--NeedCopy-->
```

Beispiel:

```
disable server 10.102.29.5 30
<!--NeedCopy-->
```

So entfernen Sie ein Serverobjekt mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm server <name>
<!--NeedCopy-->
```

Beispiel:

```
rm server 10.102.29.5
<!--NeedCopy-->
```

So entfernen Sie ein Serverobjekt mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Server**.
2. Wählen Sie einen Server aus und klicken Sie auf **Entfernen**.

Verwalten von Services

October 5, 2021

Dienste sind standardmäßig aktiviert, wenn Sie sie erstellen. Sie können jeden Dienst einzeln deaktivieren oder aktivieren. Wenn Sie einen Dienst deaktivieren, geben Sie normalerweise eine Wartezeit an, während der der Dienst weiterhin bestehende Verbindungen verarbeitet, aber neue Verbindungen ablehnt, bevor Sie das Herunterfahren beenden. Wenn Sie keine Wartezeit angeben, wird der Dienst sofort heruntergefahren. Während der Wartezeit ist der Status des Dienstes außer Betrieb.

Sie können einen Dienst entfernen, wenn er nicht mehr verwendet wird. Wenn Sie einen Dienst entfernen, wird er vom virtuellen Server aufgehoben und aus der Citrix ADC Konfiguration gelöscht.

So aktivieren oder deaktivieren Sie einen Dienst mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable service <name>

disable service <name> <DelayInSeconds>
<!--NeedCopy-->
```

Beispiele:

```
enable service Service-HTTP-1
disable service Service-HTTP-1 30
<!--NeedCopy-->
```

So aktivieren oder deaktivieren Sie einen Dienst mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Öffnen Sie einen Dienst, und wählen Sie in der Liste **Aktion** die Option **Aktivieren** oder **Deaktivieren** aus.

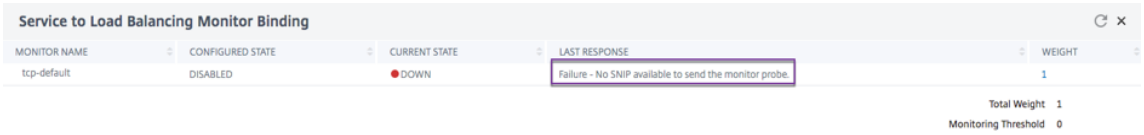
Identifizieren Sie die Ursache für den Dienststatus, der mit DOWN gekennzeichnet ist, mit der GUI

Ab Citrix ADC Version 13.0 Build 41.20 können Sie die Monitorsondeninformationen auf der GUI für die Dienste anzeigen, die DOWN sind, ohne zur Monitorbindungsschnittstelle zu navigieren. Der Wert in der Spalte **Serverstatus** der Seite Dienste kann angeklickt werden. Sie können auf **DOWN** klicken, um die Ursache zu identifizieren, aufgrund der der Dienst als DOWN gekennzeichnet ist.

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Klicken Sie auf **DOWN** in der Spalte **Serverstatus** entsprechend dem Dienst, der DOWN ist.

Die Seite Service to Load Balancing Monitor Bindung wird angezeigt.

In der Spalte **Letzte Antwort** wird der Grund angezeigt, aufgrund dessen der Dienst mit DOWN gekennzeichnet ist.



Verwalten eines virtuellen Lastausgleichsservers

October 5, 2021

Virtuelle Server sind standardmäßig aktiviert, wenn Sie sie erstellen. Sie können virtuelle Server manuell deaktivieren und aktivieren. Wenn Sie einen virtuellen Server deaktivieren, wird der Status des virtuellen Diensts als “Out of Service” angezeigt. In diesem Fall beendet der virtuelle Server alle Verbindungen, je nach Einstellung des Parameters DownStateFlush, entweder sofort oder nachdem bereits vorhandene Verbindungen abgeschlossen wurden. Wenn DownStateFlush ENABLED (Standard) ist, werden alle Verbindungen geleert. Wenn DEAKTIVIERT, sendet der virtuelle Server weiterhin Anforderungen für vorhandene Verbindungen.

Sie entfernen einen virtuellen Server nur, wenn Sie den virtuellen Server nicht mehr benötigen. Bevor Sie es entfernen, müssen Sie die Bindung aller Dienste aufheben.

So aktivieren oder deaktivieren Sie einen virtuellen Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

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

Beispiele:

```
enable lb vserver Vserver-LB-1
disable lb vserver Vserver-LB-1
<!--NeedCopy-->
```


So aktivieren oder deaktivieren Sie einen virtuellen Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie einen virtuellen Server aus, und wählen Sie in der Liste **Aktion** die Option **Aktivieren** oder **Deaktivieren** aus.

So heben Sie die Bindung eines Dienstes von einem virtuellen Server mit der CLI auf

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
unbind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
unbind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

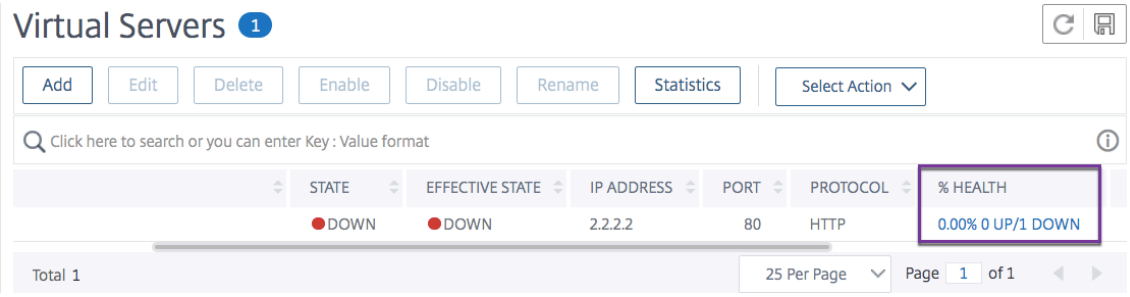
So heben Sie die Bindung eines Dienstes von einem virtuellen Server mit der GUI auf

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen Server, und klicken Sie auf den Abschnitt **Dienste** .
3. Wählen Sie einen Dienst aus, und klicken Sie auf **Bindung aufheben**.

Identifizieren Sie die Ursache für den Status des virtuellen Servers, der mit DOWN gekennzeichnet ist, mit der GUI

Ab Citrix ADC Version 13.0 Build 41.20 können Sie die Monitor-Sond-Informationen auf der GUI für die virtuellen Server anzeigen, die DOWN sind, ohne zur Monitor Bindungsschnittstelle zu navigieren. Der Wert in der **Spalten% HEALTH** der Seite Virtual Server kann angeklickt werden. Sie können auf den Wert in der **Spalten% HEALTH** klicken, um die Ursache zu identifizieren, aufgrund der der virtuelle Server als DOWN gekennzeichnet ist.

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie auf den Wert in der **Spalten% HEALTH**, der dem virtuellen Server entspricht, der ausgefallen ist.

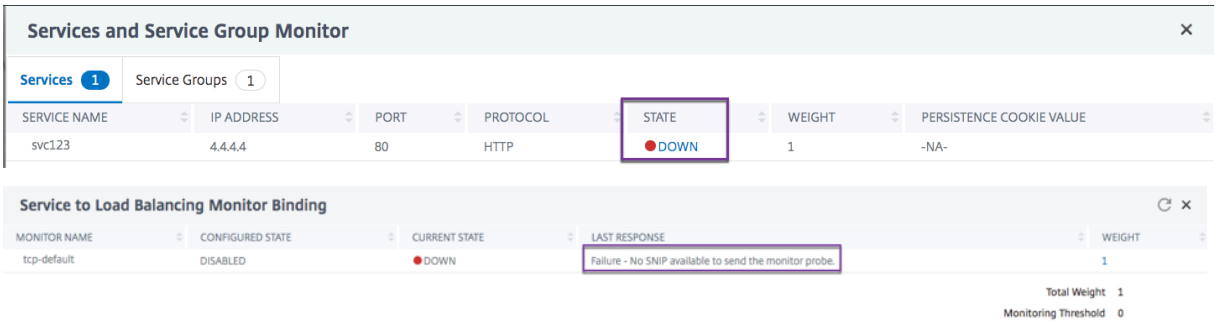


Die Seite Service und Service Group Monitor wird angezeigt. Die an diesen virtuellen Server gebundenen Dienste und Servicegruppen werden in den entsprechenden Registerkarten angezeigt.

Wenn Sie Dienste verwenden, die an den Lastenausgleich virtuell gebunden sind, führen Sie Folgendes aus:

Klicken Sie auf der Registerkarte **Dienste** auf DOWN, der dem **heruntergeschickten** Dienst entspricht.

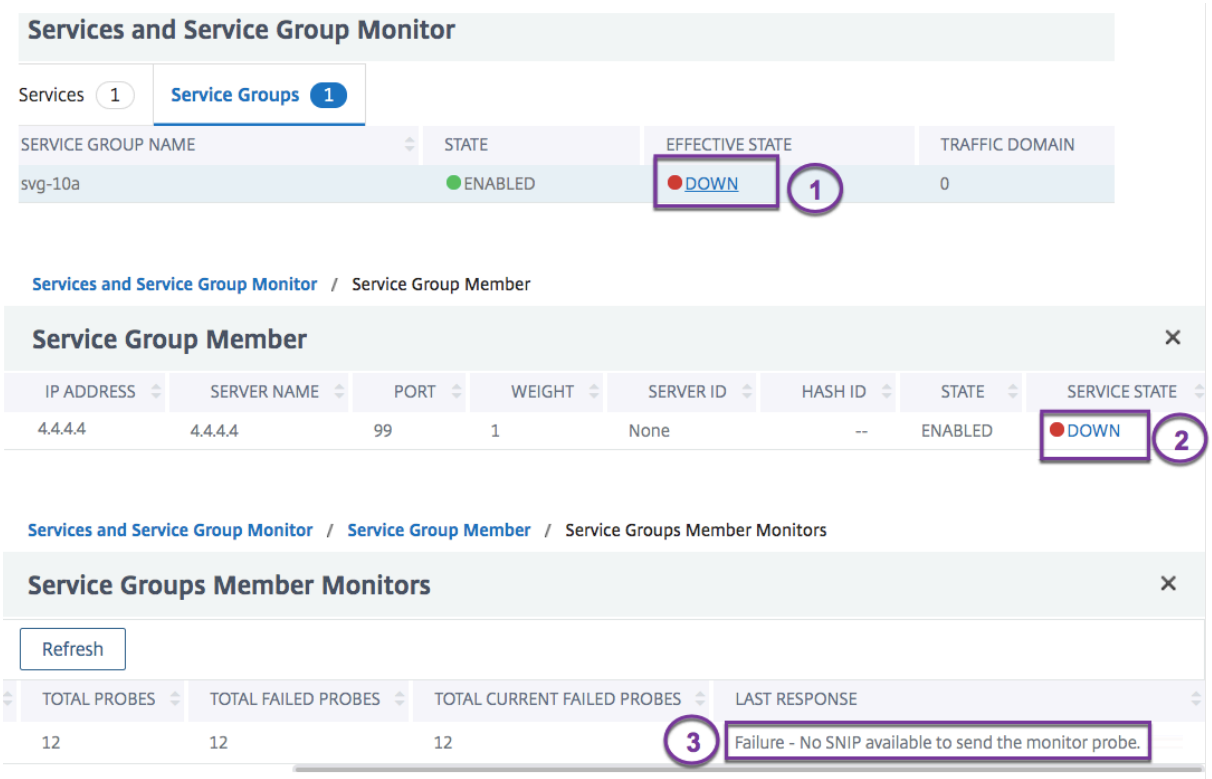
In der Spalte **Letzte Antwort auf** der Seite Service to Load Balancing Monitor Bindung wird der Grund angezeigt, aufgrund dessen der virtuelle Server markiert ist.



Wenn Sie Service-Gruppen verwenden, die an den Lastenausgleich virtuell gebunden sind, führen Sie Folgendes aus:

Klicken Sie auf der Registerkarte **Dienstgruppen** auf der Seite Dienste und **Dienstgruppenmonitor** auf **DOWN**, und klicken Sie dann auf der Seite Dienstgruppenmitglied auf DOWN.

In der Spalte **Letzte Antwort auf** der Seite Mitgliederüberwachung von Dienstgruppen wird der Grund angezeigt, aufgrund dessen der virtuelle Server markiert ist.



Visualisierer für Lastenausgleich

October 5, 2021

Der Load Balancing Visualizer ist ein Werkzeug, mit dem Sie die Load Balancing Konfiguration in einem grafischen Format anzeigen und ändern können. Es folgt ein Beispiel für die Visualizer-Anzeige.

Abbildung 1. Anzeige des Load Balancing Visualizers

Sie können den Visualizer verwenden, um Folgendes anzuzeigen:

- Die Dienste und Dienstgruppen, die an einen virtuellen Server gebunden sind.
- Die Monitore, die an jeden Dienst gebunden sind.
- Die Richtlinien, die an den virtuellen Server gebunden sind.
- Die Richtlinienbeschriftungen, falls konfiguriert.
- Konfigurationsdetails eines angezeigten Elements.

Sie können den Visualizer auch verwenden, um neue Objekte hinzuzufügen und zu binden, vorhandene Objekte zu ändern und Objekte zu aktivieren oder zu deaktivieren. Die meisten im Visualizer angezeigten Konfigurationselemente werden unter den gleichen Namen wie in anderen Teilen des Konfigurationsdienstprogramms angezeigt. Im Gegensatz zum Rest des Konfigurationsdienstprogramms gruppiert Visualizer Dienste, die dieselben Konfigurationsdetails aufweisen, und überwacht

Bindungen in eine Entität, die als Dienstcontainer bezeichnet wird.

Ein Dienstcontainer besteht aus ähnlichen Diensten und Dienstgruppen, die an einen einzelnen virtuellen Lastausgleichsserver gebunden sind. Die Dienste im Container haben die gleichen Eigenschaften, mit Ausnahme des Namens, der IP-Adresse und des Port, und ihre Monitorbindungen müssen das gleiche Gewicht und den gleichen Bindungsstatus haben. Wenn Sie einen neuen Dienst an einen virtuellen Server binden, wird er in einen vorhandenen Container abgelegt, wenn seine Konfigurations- und Überwachungsbindungen mit denen anderer Dienste übereinstimmen. Ansonsten wird es in einen eigenen Behälter gelegt.

Die folgenden Verfahren enthalten nur die grundlegenden Schritte zur Verwendung des Visualizers. Da der Visualizer Funktionen in anderen Bereichen der Load Balancing-Funktion dupliziert, werden in der gesamten Load Balancing-Dokumentation andere Methoden zum Anzeigen oder Konfigurieren aller Einstellungen bereitgestellt, die im Visualizer konfiguriert werden können.

Hinweis: Der Visualizer benötigt eine grafische Oberfläche, so dass er nur über das Konfigurationsprogramm verfügbar ist.

So zeigen Sie die Eigenschaften des Lastenausgleichs virtueller Server mithilfe des Visualizers an

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie anzeigen möchten, und klicken Sie dann auf **Visualizer**.

So zeigen Sie Konfigurationsdetails für Dienste, Dienstgruppen und Monitore mithilfe des Visualizers an

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie anzeigen möchten, und klicken Sie dann auf **Visualizer**.
3. Doppelklicken Sie im Dialogfeld Load Balancing Visualizer auf die Entität, um die Konfigurationsdetails der Entität anzuzeigen, die an diesen virtuellen Server gebunden ist. Sie können folgende Aktionen ausführen:

So zeigen Sie Konfigurationsdetails für Richtlinien und Richtlinienbeschriftungen mithilfe des Visualizers im Konfigurationsdienstprogramm an

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie anzeigen möchten, und klicken Sie dann auf Visualizer.

3. Doppelklicken Sie im Dialogfeld Load Balancing Visualizer auf die Richtlinienentität, um die Richtlinien anzuzeigen, die an diesen virtuellen Server gebunden sind.

So ändern Sie eine Ressource in einer Lastausgleichskonfiguration mithilfe des Visualizers

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie konfigurieren möchten, und klicken Sie dann auf Visualizer.
3. Doppelklicken Sie im Dialogfeld Load Balancing Visualizer im Visualizer-Image auf die Ressource, die Sie ändern möchten.

So fügen Sie eine Lastausgleichskonfiguration mithilfe des Visualizers hinzu

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, den Sie konfigurieren möchten, und klicken Sie dann auf Visualizer.
3. Klicken Sie im Dialogfeld Load Balancing Visualizer auf **+**, um die Ressource hinzuzufügen.

Verwalten des Client-Datenverkehrs

October 5, 2021

Die ordnungsgemäße Verwaltung von Clientverbindungen stellt sicher, dass Ihre Anwendungen auch dann für Benutzer verfügbar bleiben, wenn Ihre Citrix ADC Appliance hohe Auslastung aufweist. Verschiedene Lastausgleichsfunktionen und andere auf der Appliance verfügbare Funktionen können in ein Lastausgleichs-Setup integriert werden, um die Last effizienter zu verarbeiten, bei Bedarf umzuleiten und die Aufgaben zu priorisieren, die die Appliance ausführen muss:

- **Sitzungsloser Lastausgleich.** Sie können virtuelle Server mit sitzungslosem Lastenausgleich konfigurieren und Lastenausgleich durchführen, ohne Sitzungen in Konfigurationen zu erstellen, die DSR- oder Intrusion Detection Systems (IDS) verwenden.
- **Integriertes Caching.** Sie können HTTP-Anforderungen an einen Cache umleiten.
- **Prioritätswarteschlange.** Sie können Anforderungen basierend auf Priorität richten, indem Sie Ihre Konfiguration mit der Funktion Priority Queuing integrieren.
- **SureConnect.** Sie können den Lastenausgleich mit der Sure Connect-Funktion verwenden, um wichtige Anfragen an eine benutzerdefinierte Webseite umzuleiten und sie vor Verzögerungen aufgrund von Netzwerküberlastung zu schützen.

- **Verzögerte Bereinigung.** Sie können die verzögerte Bereinigung von virtuellen Serververbindungen konfigurieren, um zu verhindern, dass der Cleanup-Prozess CPU-Zyklen in Zeiten verwendet, in denen die Citrix ADC Appliance hohe Belastungen aufweist.
- **Umschreiben.** Sie können die Funktion Umschreiben verwenden, um Port und Protokoll beim Ausführen der HTTP-Umleitung zu ändern oder die IP-Adresse und den Port des virtuellen Servers in einen benutzerdefinierten Request-Header einfügen.
- **RTSP NAT.**
- **Ratenbasierte Überwachung.** Sie können die ratenbasierte Überwachung aktivieren, um überschüssigen Datenverkehr umzuleiten.
- **Layer-2-Parameter.** Sie können einen virtuellen Server so konfigurieren, dass die L2-Parameter verwendet werden, um eine Verbindung zu identifizieren.
- **ICMP-Antwort**. Sie können die Appliance so konfigurieren, dass ICMP-Antworten an PING-Anforderungen gemäß Ihren Einstellungen gesendet werden. Stellen Sie auf der dem virtuellen Server entsprechenden IP-Adresse die ICMP RESPONSE auf VSVR_CNTRLD ein, und legen Sie auf dem virtuellen Server die fest `ICMP VSERVER RESPONSE`.
  Die folgenden Einstellungen können auf einem virtuellen Server vorgenommen werden:
  - Wenn Sie auf allen virtuellen Servern auf PASSIV eingestellt `ICMP VSERVER RESPONSE` sind, antwortet die Appliance immer.
  - Wenn Sie auf allen virtuellen Servern auf ACTIVE eingestellt `ICMP VSERVER RESPONSE` sind, reagiert die Appliance auch dann, wenn ein virtueller Server UP ist.
  - Wenn Sie bei einigen `ICMP VSERVER RESPONSE` auf ACTIVE und auf anderen PASSIV eingestellt sind, reagiert die Appliance auch dann, wenn ein auf ACTIVE gesetzter virtueller Server UP ist.

Konfigurieren von virtuellen Servern ohne Sitzungsaufwand für den Lastenausgleich

October 5, 2021

Wenn die Citrix ADC Appliance Lastenausgleich durchführt, erstellt und verwaltet sie Sitzungen zwischen Clients und Servern. Die Wartung von Sitzungsinformationen belastet die Appliance-Ressourcen erheblich, und Sitzungen sind möglicherweise nicht in Szenarien wie einem Direct Server Return (DSR) Setup und dem Lastausgleich von Intrusion Detection Systemen (IDS) erforderlich. Um das Erstellen von Sitzungen zu vermeiden, wenn sie nicht erforderlich sind, können Sie einen virtuellen Server auf der Appliance für den sitzungslosen Lastenausgleich konfigurieren. Beim sitzungslosen Lastausgleich führt die Appliance den Lastausgleich pro Paket durch.

Der Sitzungslose Lastausgleich kann im MAC-basierten Weiterleitungsmodus oder im IP-basierten Weiterleitungsmodus ausgeführt werden.

Für die MAC-basierte Weiterleitung muss die IP-Adresse des virtuellen Servers ohne Sitzungszugriffe auf allen physischen Servern angegeben werden, an die der Datenverkehr weitergeleitet wird.

Für die IP-basierte Weiterleitung im sitzungslosen Lastenausgleich müssen die IP-Adresse und der Port des virtuellen Servers nicht auf den physischen Servern angegeben werden, da diese Informationen in den weitergeleiteten Paketen enthalten sind. Wenn ein Paket vom Client an den physischen Server weitergeleitet wird, lässt die Appliance Clientdetails wie IP-Adresse und Port unverändert und fügt die IP-Adresse und den Port des Ziels hinzu.

Unterstützte Einrichtung

Der sitzungslose Lastausgleich von Citrix ADC unterstützt die folgenden Diensttypen und Lastausgleichsmethoden:

Servicetypen

- ANY für MAC-basierte Umleitung
- ANY, DNS und UDP für IP-basierte Umleitung

Lastenausgleichsmethoden

- Runde Robin
- Geringste Bandbreite
- LRTM (Methode der geringsten Antwortzeit)
- Quell-IP-Hash
- Ziel-IP-Hash
- Quell-IP-Ziel-IP-Hash
- Quell-IP-Quellport-Hash
- Benutzerdefinierte Last

Einschränkungen

Der Sitzungslose Lastausgleich hat folgende Einschränkungen:

- Die Appliance muss im Zweiarm-Modus bereitgestellt werden.
- Ein Dienst muss nur an einen virtuellen Server gebunden sein.
- Sitzungsloser Lastausgleich wird für Dienstgruppen nicht unterstützt.
- Sitzungsloser Lastenausgleich wird für domänenbasierte Dienste (DBS-Dienste) nicht unterstützt.
- Sitzungsloser Lastenausgleich im IP-Modus wird für einen virtuellen Server, der als Backup auf einem primären virtuellen Server konfiguriert ist, nicht unterstützt.

- Sie können den Spillover-Modus nicht aktivieren.
- Für alle Dienste, die an einen virtuellen Server mit sitzungslosem Lastenausgleich gebunden sind, muss die Option Quell-IP (USIP) verwenden aktiviert sein.
- Für einen virtuellen Platzhalterserver oder -dienst wird die Ziel-IP-Adresse nicht geändert.

Hinweis:

- Geben Sie beim Konfigurieren eines virtuellen Servers für den sitzungslosen Lastenausgleich explizit eine unterstützte Lastausgleichsmethode an. Die Standardmethode Least Connection kann nicht für den sitzungslosen Lastausgleich verwendet werden.
- Um den sitzungslosen Lastenausgleich im MAC-basierten Umleitungsmodus auf einem virtuellen Server zu konfigurieren, muss die MAC-basierte Weiterleitungsoption auf der Citrix ADC Appliance aktiviert sein.

So fügen Sie einen virtuellen Server ohne Sitzungssuche mit der CLI hinzu

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

```
add lb vserver <name>@ <serviceType> <IPAddress>@ <port> -m <
   redirectionMode> -sessionless <(ENABLED|DISABLED)> -lbMethod <
   load_balancing_method>

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

Beispiel:

```
 add lb vserver sesslessv1 any 11.11.12.123 54 -sessionless ENABLED -
    lbMethod roundrobin -m ip
      Done
 show lb vserver sesslessv1
      sesslessv1 (11.11.12.123:54) - ANY Type: ADDRESS
      State: DOWN
      ...
      Effective State: DOWN
      Client Idle Timeout: 120 sec
      Down state flush: ENABLED
      ...
      Persistence: NONE
      Sessionless LB: ENABLED
```



```
13        Connection Failover: DISABLED
14        L2Conn: OFF
15        1) Policy : cmp_text Priority:8680 Inherited
16        2) Policy : cmp_nocmp_ie60 Priority:8690 Inherited
17  <!--NeedCopy-->
```

So konfigurieren Sie den sitzungslosen Lastenausgleich auf einem vorhandenen virtuellen Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1  set lb vserver <name>@ -m <redirectionMode> -sessionless <(ENABLED|
       DISABLED)> -lbMethod <load_balancing_method>
2  <!--NeedCopy-->
```

Beispiel

```
1  set lb vserver sesslessv1 -m mac -sessionless ENABLED -lbmethod lrtm
2    Done
3  <!--NeedCopy-->
```

> **Hinweis:**
>
> Für einen Dienst, der an einen virtuellen Server gebunden ist, auf dem die `-m MAC` Option aktiviert ist, müssen Sie einen Nicht-Benutzermonitor binden.

So konfigurieren Sie einen virtuellen Server ohne Session mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie den virtuellen Server, klicken Sie unter Erweiterte Einstellungen auf Verkehrseinstellungen, und wählen Sie dann Sitzungsloser Lastenausgleich aus.

Umleiten von HTTP-Anforderungen an einen Cache

October 5, 2021

Die Citrix ADC Cache-Umleitungsfunktion leitet HTTP-Anforderungen an einen Cache um. Sie können die Auswirkungen der Reaktion auf HTTP-Anfragen erheblich reduzieren und die Leistung Ihrer Website durch die ordnungsgemäße Implementierung der Cache-Umleitungsfunktion verbessern.

Ein Cache speichert häufig angeforderten HTTP-Inhalt. Wenn Sie die Cache-Umleitung auf einem virtuellen Server konfigurieren, sendet die Citrix ADC Appliance zwischenspeicherbare HTTP-Anforderungen an den Cache und nicht zwischenspeicherbare HTTP-Anforderungen an den Ursprungs-Webserver.

So konfigurieren Sie die Cache-Umleitung auf einem virtuellen Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -cacheable <Value>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -cacheable yes
<!--NeedCopy-->
```

So konfigurieren Sie die Cache-Umleitung auf einem virtuellen Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie den virtuellen Server.
2. Klicken Sie unter Erweiterte Einstellungen auf Verkehrseinstellungen, und wählen Sie Cacheable aus.

Direkte Anfragen nach Priorität

October 5, 2021

Die Citrix ADC Appliance unterstützt die Priorisierung von Clientanforderungen mit ihrer Prioritätswarteschlangenfunktion. Mit dieser Funktion können Sie bestimmte Anforderungen, z. B. solche von wichtigen Clients, als Prioritätsanforderungen festlegen und sie an die “Vorderseite der Zeile” senden, damit die Appliance zuerst darauf reagiert. Auf diese Weise können Sie diesen Kunden einen ununterbrochenen Service durch Nachfragestiege oder DDoS-Angriffe auf Ihre Website bereitstellen.

So konfigurieren Sie die Prioritätswarteschlange auf einem virtuellen Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -pq <Value>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -pq yes
<!--NeedCopy-->
```

So konfigurieren Sie die Prioritätswarteschlange auf einem virtuellen Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie den virtuellen Server.
2. Klicken Sie unter Erweiterte Einstellungen auf Verkehrseinstellungen, und wählen Sie Prioritätswarteschlange aus.

Hinweis: Konfigurieren Sie die Prioritätswarteschlange global, damit es ordnungsgemäß funktioniert.

Direkte Anfragen an eine benutzerdefinierte Webseite

December 3, 2021

Die Citrix ADC Appliance stellt die SureConnect Option bereit, um sicherzustellen, dass Webanwendungen trotz Verzögerungen reagieren, die durch begrenzte Serverkapazität oder Verarbeitungsgeschwindigkeit verursacht werden. SureConnect zeigt dazu eine alternative Webseite Ihrer Wahl an, wenn der Server, der die primäre Webseite hostet, entweder nicht verfügbar ist oder langsam reagiert.

Um SureConnect auf einem virtuellen Server zu konfigurieren, müssen Sie zunächst den alternativen Inhalt konfigurieren. Informationen zum Konfigurieren einer SureConnect-Website finden Sie unter SureConnect. Aktivieren Sie nach der Konfiguration der Website SureConnect auf dem virtuellen Load Balancing-Server, um Ihre benutzerdefinierte SureConnect-Webseite zu verwenden.

Hinweis: Damit SureConnect ordnungsgemäß funktioniert, müssen Sie es global konfigurieren.

So aktivieren Sie SureConnect auf einem virtuellen Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -sc <Value>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -sc yes
<!--NeedCopy-->
```

So aktivieren Sie SureConnect auf einem virtuellen Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie den virtuellen Server.
2. Klicken Sie unter Erweiterte Einstellungen auf Verkehrseinstellungen, und wählen Sie SureConnect aus.

Bereinigung virtueller Serververbindungen aktivieren

October 5, 2021

Unter bestimmten Bedingungen können Sie die Einstellung DownStateFlush so konfigurieren, dass vorhandene Verbindungen sofort beendet werden, wenn ein Dienst oder ein virtueller Server als DOWN markiert ist. Durch das Beenden vorhandener Verbindungen werden Ressourcen freigegeben und in bestimmten Fällen wird die Wiederherstellung überlasteter Lastausgleichseinstellungen beschleunigt.

Der Status eines virtuellen Servers hängt von den Zuständen der an ihn gebundenen Dienste ab. Der Status jedes Dienstes hängt von den Antworten der Server mit Lastausgleich auf Prüfpunkte und Zustandsprüfungen ab, die von den Monitoren gesendet werden, die an diesen Dienst gebunden sind. Manchmal reagieren die Server mit Lastausgleich nicht. Wenn ein Server langsam oder ausgelastet ist, kann ein Timeout der Überwachung von Prüfpunkten erfolgen. Wenn wiederholte Überwachungssonden nicht innerhalb der konfigurierten Zeitüberschreitungszeit beantwortet werden, wird der Dienst mit DOWN gekennzeichnet.

Ein virtueller Server wird nur dann als DOWN markiert, wenn alle an ihn gebundenen Dienste mit DOWN gekennzeichnet sind. Wenn ein virtueller Server heruntergeht, werden alle Verbindungen

beendet, entweder sofort oder nachdem bereits vorhandene Verbindungen abgeschlossen werden können.

Aktivieren Sie die DownStateFlush-Einstellung nicht auf den Anwendungsservern, die ihre Transaktionen abschließen müssen. Sie können diese Einstellung auf Webservern aktivieren, deren Verbindungen sicher beendet werden können, wenn sie DOWN markiert haben.

In der folgenden Tabelle werden die Auswirkungen dieser Einstellung auf eine Beispielkonfiguration zusammengefasst, die aus einem virtuellen Server, vServer-LB-1, besteht und an diesen Dienst gebunden ist, Dienst-TCP-1. In der Tabelle bezeichnen E und D den Status der Einstellung DownStateFlush: E bedeutet Aktiviert und D bedeutet Deaktiviert.

Vserver-LB-1	Service-TCP-1	Zustand der Verbindungen
E	E	Sowohl Client- als auch Serververbindungen werden beendet.
E	D	Bei einigen Diensttypen, z. B. TCP, für die die Citrix ADC Appliance die Wiederverwendung der Verbindung nicht unterstützt, werden sowohl Client- als auch Serververbindungen beendet. Bei Diensttypen wie HTTP, für die die Appliance die Wiederverwendung der Verbindung unterstützt, werden sowohl Client- als auch Serververbindungen nur beendet, wenn eine Transaktion für diese Verbindungen aktiv ist. Wenn eine Transaktion nicht aktiv ist, werden nur Clientverbindungen beendet.

Vserver-LB-1	Service-TCP-1	Zustand der Verbindungen
D	E	Bei einigen Diensttypen, z. B. TCP, für die die Citrix ADC Appliance die Wiederverwendung der Verbindung nicht unterstützt, werden sowohl Client- als auch Serververbindungen beendet. Bei Diensttypen wie HTTP, für die die Appliance die Wiederverwendung der Verbindung unterstützt, werden sowohl Client- als auch Serververbindungen nur beendet, wenn eine Transaktion für diese Verbindungen aktiv ist. Wenn eine Transaktion nicht aktiv ist, werden nur Serververbindungen beendet.
D	D	Weder Client- noch Serververbindungen werden beendet.

Wenn Sie einen Dienst nur deaktivieren möchten, wenn alle etablierten Verbindungen vom Server oder vom Client geschlossen werden, können Sie die Option ordnungsgemäßes Herunterfahren verwenden. Informationen zum ordnungsmäßigen Herunterfahren eines Dienstes finden Sie unter Graceful Shutdown of Services.

So konfigurieren Sie die Einstellung zum Ausfallzustand auf einem virtuellen Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -downStateFlush <Value>
<!--NeedCopy-->
```


Beispiel:

```
set lb vserver Vserver-LB-1 -downStateFlush enabled
<!--NeedCopy-->
```

So konfigurieren Sie die Einstellung zum Ausfallzustand auf einem virtuellen Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie den virtuellen Server.
2. Klicken Sie unter Erweiterte Einstellungen auf Verkehrseinstellungen, und wählen Sie Down State Flush aus.

Rewrite von Ports und Protokollen für die HTTP-Umleitung

October 5, 2021

Virtuelle Server und die an sie gebundenen Dienste verwenden möglicherweise verschiedene Ports. Wenn ein Dienst mit einer Umleitung auf eine HTTP-Verbindung reagiert, müssen Sie möglicherweise die Citrix ADC Appliance so konfigurieren, dass der Port und das Protokoll geändert werden, um sicherzustellen, dass die Umleitung erfolgreich durchgeführt wird. Dazu aktivieren und konfigurieren Sie die Einstellung RedirectPortRewrite.

Diese Einstellung betrifft nur HTTP- und HTTPS-Datenverkehr. Wenn diese Einstellung auf einem virtuellen Server aktiviert ist, schreibt der virtuelle Server den Port bei Weiterleitungen neu und ersetzt den vom Dienst verwendeten Port durch den vom virtuellen Server verwendeten Port.

Wenn der virtuelle Server oder Dienst vom Typ SSL ist, müssen Sie die SSL-Umleitung auf dem virtuellen Server oder Dienst aktivieren. Wenn sowohl der virtuelle Server als auch der Dienst vom Typ SSL sind, aktivieren Sie die SSL-Umleitung auf dem virtuellen Server.

Die Einstellung RedirectPortRewrite kann in den folgenden Szenarien verwendet werden:

- Der virtuelle Server ist vom Typ HTTP und die Dienste sind vom Typ SSL.
- Der virtuelle Server ist vom Typ SSL und die Dienste sind vom Typ HTTP.
- Der virtuelle Server ist vom Typ HTTP und die Dienste sind vom Typ HTTP.
- Der virtuelle Server ist vom Typ SSL und die Dienste sind vom Typ SSL.

Szenario 1: Der virtuelle Server ist vom Typ HTTP und Dienste vom Typ SSL. SSL-Umleitung und optional Port-Rewrite ist für den Dienst aktiviert. Wenn die Portumschreibung aktiviert ist, wird der Port der HTTPS-URLs neu geschrieben. HTTP-URLs vom Server werden wie sie an den Client gesendet.

Nur die SSL-Umleitung ist aktiviert. Der virtuelle Server kann an jedem Port konfiguriert werden. Siehe folgende Tabelle:

URL vom Server umleiten	Umleitungs-URL, die an den Client gesendet wird
/http://domain.com	/http://domain.com
/http://domain.com:8080	/http://domain.com:8080
/https://domain.com	/https://domain.com
/https://domain.com:444	/https://domain.com:444

SSL-Umleitung und Portumschreibung sind aktiviert. Der virtuelle Server ist auf Port 80 konfiguriert. Siehe folgende Tabelle:

URL vom Server umleiten	Umleitungs-URL, die an den Client gesendet wird
/http://domain.com	/http://domain.com
/http://domain.com:8080	/http://domain.com:8080
/https://domain.com	/https://domain.com
/https://domain.com:444	/https://domain.com

SSL-Umleitung und Portumschreibung sind aktiviert. Virtueller Server ist auf Port 8080 konfiguriert. Siehe folgende Tabelle:

URL vom Server umleiten	Umleitungs-URL, die an den Client gesendet wird
/http://domain.com	/http://domain.com
/http://domain.com:8080	/http://domain.com:8080
/https://domain.com	/http://domain.com:8080
/https://domain.com:444	/http://domain.com:8080

Szenario 2: Der virtuelle Server ist vom Typ SSL und Dienste vom Typ HTTP. Wenn Port-Rewrite aktiviert ist, wird nur der Port von HTTP-URLs neu geschrieben. HTTPS-URLs vom Server werden wie sie an den Client gesendet.

SSL-Umleitung ist auf dem virtuellen Server aktiviert. Der virtuelle Server kann an jedem Port konfiguri-

ert werden. Siehe folgende Tabelle.

URL vom Server umleiten	Umleitungs-URL, die an den Client gesendet wird
/http://domain.com	/https://domain.com
/http://domain.com:8080	/https://domain.com:8080
/https://domain.com	/https://domain.com
/https://domain.com:444	/https://domain.com:444

SSL-Umleitung und Port-Rewrite sind auf dem virtuellen Server aktiviert. Der virtuelle Server ist auf Port 443 konfiguriert. Siehe folgende Tabelle:

URL vom Server umleiten	Umleitungs-URL, die an den Client gesendet wird
/http://domain.com	/https://domain.com
/http://domain.com:8080	/https://domain.com
/https://domain.com	/https://domain.com
/https://domain.com:444	/https://domain.com:444

SSL-Umleitung und Portumschreibung sind aktiviert. Der virtuelle Server ist auf Port 444 konfiguriert. Siehe folgende Tabelle:

URL vom Server umleiten	Umleitungs-URL, die an den Client gesendet wird
/http://domain.com	/https://domain.com:444
/http://domain.com:8080	/https://domain.com:444
/https://domain.com	/https://domain.com
/https://domain.com:445	/https://domain.com:445

Szenario 3: Der virtuelle Server und der Dienst sind vom Typ HTTP. Port-Rewrite muss auf dem virtuellen Server aktiviert sein. Nur der Port von HTTP-URLs wird neu geschrieben. HTTPS-URLs vom Server werden wie sie an den Client gesendet.

Der virtuelle Server ist auf Port 80 konfiguriert. Siehe folgende Tabelle:

URL vom Server umleiten	Umleitungs-URL, die an den Client gesendet wird
/http://domain.com	/http://domain.com
/http://domain.com:8080	/http://domain.com
/https://domain.com	/https://domain.com
/https://domain.com:444	/https://domain.com:444

Der virtuelle Server ist auf Port 8080 konfiguriert. Siehe folgende Tabelle:

URL vom Server umleiten	Umleitungs-URL, die an den Client gesendet wird
/http://domain.com	/http://domain.com:8080
/http://domain.com:8080	/http://domain.com:8080
/https://domain.com	/https://domain.com
/https://domain.com:445	/https://domain.com:445

Szenario 4: Der virtuelle Server und der Dienst sind vom Typ SSL. Wenn die Portumschreibung aktiviert ist, wird nur der Port der HTTPS-URLs neu geschrieben. HTTP-URLs vom Server werden wie sie an den Client gesendet.

SSL-Umleitung ist auf dem virtuellen Server aktiviert. Der virtuelle Server kann an jedem Port konfiguriert werden. Siehe folgende Tabelle:

URL vom Server umleiten	Umleitungs-URL, die an den Client gesendet wird
/http://domain.com	/http://domain.com
/http://domain.com:8080	/http://domain.com:8080
/https://domain.com	/https://domain.com
/https://domain.com:444	/https://domain.com:444

SSL-Umleitung und Port-Rewrite sind auf dem virtuellen Server aktiviert. Der virtuelle Server ist auf Port 443 konfiguriert. Siehe folgende Tabelle:

URL vom Server umleiten	Umleitungs-URL, die an den Client gesendet wird
/http://domain.com	/http://domain.com
/http://domain.com:8080	/http://domain.com:8080
/https://domain.com	/https://domain.com
/https://domain.com:444	/https://domain.com

SSL-Umleitung und Port-Rewrite sind auf dem virtuellen Server aktiviert. Der virtuelle Server ist auf Port 444 konfiguriert. Siehe folgende Tabelle:

URL vom Server umleiten	Umleitungs-URL, die an den Client gesendet wird
/http://domain.com	/http://domain.com
/http://domain.com:8080	/http://domain.com:8080
/https://domain.com	/https://domain.com:444
/https://domain.com:445	/https://domain.com:444

So konfigurieren Sie die HTTP-Umleitung auf einem virtuellen Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -redirectPortRewrite (ENABLED | DISABLED)
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -redirectPortRewrite enabled
<!--NeedCopy-->
```

So konfigurieren Sie die HTTP-Umleitung auf einem virtuellen Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie den virtuellen Server, klicken Sie im Bereich Erweiterte Einstellungen auf Verkehrseinstellungen, und wählen Sie dann Umschreiben aus.

So konfigurieren Sie SSL-Umleitung auf einem virtuellen SSL-Server oder -Dienst mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl vserver <vServerName> - sslRedirect (ENABLED | DISABLED)

set ssl service <serviceName> - sslRedirect (ENABLED | DISABLED)
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver Vserver-SSL-1 -sslRedirect enabled

set ssl service service-SSL-1 -sslRedirect enabled
<!--NeedCopy-->
```

So konfigurieren Sie SSL-Umleitung und SSL-Port-Umschreibung auf einem virtuellen SSL-Server oder -Dienst mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie den virtuellen Server.
2. Klicken Sie unter Erweiterte Einstellungen auf SSL-Parameter, und wählen Sie SSL-Umleitung aus.

IP-Adresse und Port eines virtuellen Servers in den Request-Header einfügen

October 5, 2021

Wenn Sie mehrere virtuelle Server haben, die mit verschiedenen Anwendungen im selben Dienst kommunizieren, müssen Sie Folgendes tun:

Konfigurieren Sie die Citrix ADC Appliance so, dass die IP-Adresse und die Portnummer des entsprechenden virtuellen Servers zu den HTTP-Anforderungen hinzugefügt werden, die an diesen Dienst gesendet werden. Mit dieser Einstellung können Anwendungen, die auf dem Dienst ausgeführt werden, den virtuellen Server identifizieren, der die Anforderung gesendet hat.

Wenn der primäre virtuelle Server ausgefallen ist und der virtuelle Backupserver hochgefahren ist, werden die Konfigurationseinstellungen des virtuellen Backupservers den Clientanforderungen hinzugefügt. Wenn dasselbe Header-Tag hinzugefügt werden soll, unabhängig davon, ob die Anforderungen vom primären virtuellen Server oder virtuellen Backup-Server stammen, müssen Sie das erforderliche Header-Tag auf beiden virtuellen Servern konfigurieren.

Hinweis: Diese Option wird nicht für virtuelle Wildcard-Server oder virtuelle Dummy-Server unterstützt.

So fügen Sie die IP-Adresse und den Port des virtuellen Servers in die Clientanforderungen mit der CLI ein

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -insertVserverIPPort <insertVserverIPPort> [<
    vipHeader>]
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -insertVserverIPPort VipAddr
<!--NeedCopy-->
```

So fügen Sie die IP-Adresse und den Port des virtuellen Servers in die Clientanforderungen mit der GUI ein

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie den virtuellen Server, klicken Sie im Bereich Erweiterte Einstellungen auf **Verkehrseinstellungen**, wählen Sie dann Einfügen des virtuellen Servers IP-Port aus, und geben Sie einen IP-Port-Header des virtuellen Servers an.

Verwenden Sie eine angegebene Quell-IP für Back-End-Kommunikation

December 3, 2021

Für die Kommunikation mit den physischen Servern oder anderen Peer-Geräten verwendet die Citrix ADC Appliance eine IP-Adresse, die ihr gehört, als Quell-IP-Adresse. Die Citrix ADC Appliance verwaltet

einen Pool ihrer IP-Adressen und wählt dynamisch eine IP-Adresse aus, während sie sich mit einem Server verbindet. Abhängig vom Subnetz, in dem der physische Server abgelegt ist, entscheidet die Appliance, welche IP-Adresse verwendet werden soll. Dieser Adresspool wird zum Senden von Traffic- und Monitor-Sonden verwendet.

In vielen Situationen möchten Sie möglicherweise, dass die Appliance eine bestimmte IP-Adresse oder eine IP-Adresse von einem bestimmten Satz von IP-Adressen für die Back-End-Kommunikation verwendet. Im Folgenden finden Sie einige Beispiele:

- Ein Server kann Monitorprobes vom Datenverkehr unterscheiden, wenn die Quell-IP-Adresse, die für Monitorprobes verwendet wird, zu einem bestimmten Satz gehört.
- Um die Serversicherheit zu verbessern, kann ein Server so konfiguriert werden, dass er auf Anfragen von einem bestimmten Satz von IP-Adressen oder manchmal von einer einzigen bestimmten IP-Adresse reagiert. In diesem Fall kann die Appliance nur die vom Server akzeptierten IP-Adressen als Quell-IP-Adresse verwenden.
- Die Appliance kann ihre internen Verbindungen effizient verwalten, wenn sie ihre IP-Adressen in IP-Sets verteilen und eine Adresse aus einem Satz nur für die Verbindung zu einem bestimmten Dienst verwenden kann.

Um die Appliance für die Verwendung einer angegebenen Quell-IP-Adresse zu konfigurieren, erstellen Sie Netzprofile (Netzwerkprofile) und konfigurieren Sie die Appliance-Entitäten für die Verwendung des Profils. Ein Netzprofil kann an den Lastenausgleich oder an virtuelle Server mit Content Switching, virtuelle Server, Dienste, Dienstgruppen oder Monitore von Citrix Gateway VPN gebunden werden. Ein Netzprofil verfügt über IP-Adressen im Besitz von Citrix ADC (SNIPs und VIPs), die als Quell-IP-Adresse verwendet werden können. Es kann sich um eine einzelne IP-Adresse oder eine Reihe von IP-Adressen handeln, die als IP-Set bezeichnet werden. Wenn ein Netzprofil über eine IP verfügt, wählt die Appliance dynamisch eine IP-Adresse aus der zum Zeitpunkt der Verbindung eingestellten IP aus. Wenn ein Profil eine einzelne IP-Adresse hat, wird dieselbe IP-Adresse als Quell-IP verwendet.

Wenn ein Netzprofil an einen virtuellen Load Balancing- oder Content Switching-Server gebunden ist, wird das Profil zum Senden von Datenverkehr an alle an ihn gebundenen Dienste verwendet. Wenn ein Netzprofil an eine Dienstgruppe gebunden ist, verwendet die Appliance das Profil für alle Mitglieder der Dienstgruppe. Wenn ein Netzprofil an einen Monitor gebunden ist, verwendet die Appliance das Profil für alle vom Monitor gesendeten Prüfpunkte.

> **Hinweis:**
>
> - Wenn eine Citrix ADC Appliance eine VIP-Adresse verwendet, um mit einem Server zu kommunizieren, identifiziert sie anhand von Sitzungseinträgen, ob der für die VIP-Adresse bestimmte Datenverkehr eine Antwort von einem Server oder eine Anforderung eines Clients ist.
> - Sie können ein Netzprofil an virtuelle VPN-Server von Citrix Gateway binden. Beim Binden

> eines Netzprofils müssen Sie jedoch einige Punkte notieren. Weitere Informationen finden Sie unter Punkte, die beim Binden eines Netzprofils an einen virtuellen VPN-Server zu beachtensind.
>
> - Die an einen Dienst oder eine Dienstgruppe gebundenen Netzprofil-IPs werden nicht nur zum Senden von Datenverkehr an die entsprechenden Back-End-Server verwendet, sondern auch für die DNS-Anforderungen, die durch ungelöste Back-End-FQDN ausgelöst werden.

Verwendung eines Netzprofils zum Senden von Traffic

Wenn die Option Quell-IP-Adresse (USIP) verwenden aktiviert ist, verwendet die Appliance die IP-Adresse des Clients und ignoriert alle Netzprofile. Wenn die USIP-Option nicht aktiviert ist, wählt die Appliance die Quell-IP auf folgende Weise aus:

- Wenn auf dem virtuellen Server oder der Service-Gruppe kein Netzprofil vorhanden ist, verwendet die Appliance die Standardmethode.
- Wenn nur ein Netzprofil in der Service-Gruppe vorhanden ist, verwendet die Appliance dieses Netzprofil.
- Wenn nur auf dem virtuellen Server ein Netzprofil vorhanden ist, verwendet die Appliance das Netzprofil.
- Wenn sowohl auf dem virtuellen Server als auch auf der Service-/Servicegruppe ein Netzprofil vorhanden ist, verwendet die Appliance das an die Service/Servicegruppe gebundene Netzprofil.

Verwendung eines Netzprofils zum Senden von Monitor-Prüfungen:

Bei Monitor-Prüfungen wählt die Appliance die Quell-IP auf folgende Weise aus:

- Wenn an den Monitor ein Netzprofil gebunden ist, verwendet die Appliance das Netzprofil des Monitors. Es ignoriert die Netzprofile, die an den virtuellen Server oder die Dienstleistungsgruppe gebunden sind.
- Wenn kein Netzprofil an den Monitor gebunden ist,
  - Wenn in der Service-Gruppe ein Netzprofil vorhanden ist, verwendet die Appliance das Netzprofil der Service-/Servicegruppe.
  - Wenn selbst in der Service-/Servicegruppe kein Netzprofil vorhanden ist, verwendet die Appliance die Standardmethode zur Auswahl einer Quell-IP.

Hinweis: Wenn kein Netzwerkprofil an einen Dienst gebunden ist, sucht die Appliance nach einem Netzprofil in der Dienstgruppe, wenn der Dienst an eine Dienstgruppe gebunden ist.

Gehen Sie wie folgt vor, um eine angegebene Quell-IP-Adresse für die Kommunikation zu verwenden:

1. Erstellen Sie IP-Sets aus dem Pool von SNIPs und VIPs, die der Citrix ADC Appliance gehören. Ein IP-Set kann sowohl aus SNIP- als auch VIP-Adressen bestehen. Anweisungen finden Sie unter

Erstellen von IP-Sets.

2. Erstellen von Netzprofilen. Anweisungen finden Sie unter Erstellen eines Netzprofils.
3. Binden Sie die Netzprofile an die Appliance-Entitäten. Anweisungen finden Sie unter Binden eines Netzprofils an eine Citrix ADC Entität.

> **Hinweis:**
>
> - Ein Netzprofil kann nur die IP-Adressen haben, die auf der Citrix ADC Appliance als SNIP und VIP angegeben sind.
> - Die Quell-IP-Persistenz wird für von Citrix ADC initiierte Pakete nicht berücksichtigt.

Netzprofile verwalten

Ein Netzprofil (oder Netzwerkprofil) enthält eine IP-Adresse oder einen IP-Satz. Während der Kommunikation mit physischen Servern oder Peers verwendet die Citrix ADC Appliance die im Profil angegebenen Adressen als Quell-IP-Adresse.

- Anweisungen zum Erstellen eines Netzwerkprofils finden Sie unter Erstellen eines Netzwerkprofils.
- Anweisungen zum Binden eines Netzwerkprofils an eine Citrix ADC-Entität finden Sie unter Binden eines Netzprofils an eine Citrix ADC-Entität.

Erstellen eines IP-Sets

Ein IP-Set ist ein Satz von IP-Adressen, die auf der Citrix ADC Appliance als Subnetz-IP-Adressen (SNIPs) oder virtuelle IP-Adressen (VIPs) konfiguriert sind. Ein IP-Satz wird mit einem aussagekräftigen Namen identifiziert, der bei der Identifizierung der Verwendung der darin enthaltenen IP-Adressen hilft. Um einen IP-Satz zu erstellen, fügen Sie einen IP-Satz hinzu und binden Sie IP-Adressen im Besitz von Citrix ADC daran. SNIP-Adressen und VIP-Adressen können im gleichen IP-Set vorhanden sein.

So erstellen Sie einen IP-Satz mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
add ipset <name>

bind ipset <name> <IPAddress>
<!--NeedCopy-->
```

Oder


```
bind ipset <name> <IPAddress>

show ipset [<name>]
<!--NeedCopy-->
```

Der vorhergehende Befehl zeigt die Namen aller IP-Sets auf der Appliance an, wenn Sie keinen Namen übergeben. Es zeigt die IP-Adressen, die an den angegebenen IP-Satz gebunden sind, wenn Sie einen Namen übergeben.

Beispiele

```
1.
> add ipset skpnwipset
 Done
> bind ipset skpnwipset 21.21.20.1
 Done

2.
 > add ipset testnwipset
 Done
> bind ipset testnwipset 21.21.21.[21-25]
 IPAddress ”21.21.21.21” bound
 IPAddress ”21.21.21.22” bound
 IPAddress ”21.21.21.23” bound
 IPAddress ”21.21.21.24” bound
 IPAddress ”21.21.21.25” bound
 Done

3.
 > bind ipset skpipset 11.11.11.101
 ERROR: Invalid IP address
[This IP address could not be added because this is not an IP address
   owned by the Citrix ADC appliance]
 > add ns ip 11.11.11.101 255.255.255.0 -type SNIP
 ip ”11.11.11.101” added
 Done
 > bind ipset skpipset 11.11.11.101
 IPAddress ”11.11.11.101” bound
 Done
4.
> sh ipset
1) Name: ipset-1
```



```
2) Name: ipset-2
3) Name: ipset-3
4) Name: skpnewipset
 Done

5.
> sh ipset skpnewipset
IP:21.21.21.21
IP:21.21.21.22
IP:21.21.21.23
IP:21.21.21.24
IP:21.21.21.25
 Done
<!--NeedCopy-->
```

So erstellen Sie einen IP-Satz mit der GUI

Navigieren Sie zu **System > Netzwerk > IP-Sets**, und erstellen Sie ein IP-Set.

Erstellen Sie ein Netzprofil

Ein Netzprofil (Netzwerkprofil) besteht aus einer oder mehreren SNIP
- oder VIP-Adressen der Citrix ADC Appliance.

So erstellen Sie ein Netzprofil mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add netprofile <name> [-srcIp <srcIpVal>]
<!--NeedCopy-->
```

Wenn SrCipval in diesem Befehl nicht angegeben ist, kann er später mit dem `set netprofile` Befehl bereitgestellt werden.

Beispiele

```
add netprofile skpnetprofile1 -srcIp 21.21.20.1
Done

```



```
add netprofile baksnp -srcIp bakipset
Done

set netprofile yahnp -srcIp 12.12.23.1
Done

set netprofile citkbnp -srcIp citkbipset
Done
<!--NeedCopy-->
```

Binden eines Netzprofils an eine Citrix ADC-Entität

Ein Netzprofil kann an einen virtuellen Lastausgleichsserver, einen Dienst, eine Dienstgruppe oder einen Monitor gebunden werden.

Hinweis: Sie können ein Netzprofil zum Zeitpunkt der Erstellung einer Citrix ADC-Entität binden oder an eine vorhandene Entität binden.

So binden Sie ein Netzprofil mithilfe der Befehlszeilenschnittstelle an einen Server

Sie können ein Netzprofil an virtuelle Server mit Lastenausgleich und virtuelle Content Switching-Server binden. Geben Sie den entsprechenden virtuellen Server an.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -netProfile <net_profile_name>
<!--NeedCopy-->
```

Oder

```
set cs vserver <name> -netProfile <net_profile_name>
<!--NeedCopy-->
```

Beispiele

```
set lb vserver skpnwvs1 -netProfile gntnp
 Done
set cs vserver mmdcsv -netProfile mmdnp
```



```
4   Done
5 <!--NeedCopy-->
```

So binden Sie ein Netzprofil mithilfe der GUI an einen virtuellen Server

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie den virtuellen Server.
2. Klicken Sie in den erweiterten Einstellungen auf **Profile**, und legen Sie ein Netzprofil fest.

So binden Sie ein Netzprofil mithilfe der CLI an einen Dienst

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set service <name> -netProfile <net_profile_name>
2 <!--NeedCopy-->
```

Beispiel

```
1 set service brnssvc1 -netProfile brnsnp
2  Done
3 <!--NeedCopy-->
```

So binden Sie ein Netzprofil mithilfe der GUI an einen Dienst

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und öffnen Sie einen Dienst.
2. Klicken Sie in den erweiterten Einstellungen auf **Profile**, und legen Sie ein Netzprofil fest.

So binden Sie ein Netzprofil mithilfe der CLI an eine Dienstgruppe

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set servicegroup <serviceGroupName> -netProfile <net_profile_name>
2 <!--NeedCopy-->
```


Beispiel

```
set servicegroup ndhsvcgrp -netProfile ndhnp
 Done
<!--NeedCopy-->
```

So binden Sie ein Netzprofil mithilfe der GUI an eine Dienstgruppe

1. Navigieren Sie zu **Traffic Management > Load Balancing > Dienstgruppen**, und öffnen Sie eine Dienstgruppe.
2. Klicken Sie in den erweiterten Einstellungen auf **Profile**, und legen Sie ein Netzprofil fest.

So binden Sie ein Netzprofil mithilfe der CLI an einen Monitor

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set monitor <monitor_name> -netProfile <net_profile_name>
```

Beispiel

```
set monitor brnsecvmon1 -netProfile brnsmonnp
 Done
<!--NeedCopy-->
```

So binden Sie ein Netzprofil mithilfe der GUI an einen Monitor

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Öffnen Sie einen Monitor und legen Sie das Netzprofil fest.

Festlegen eines Timeoutwerts für Leerlauf-Clientverbindungen

October 5, 2021

Sie können einen virtuellen Server so konfigurieren, dass alle untätigen Clientverbindungen beendet werden, nachdem ein konfigurierter Zeitüberschreitungszeitraum (in Sekunden) abgelaufen ist. Wenn Sie diese Einstellung konfigurieren, wartet die Citrix ADC Appliance auf die angegebene Zeit und schließt die Clientverbindung, wenn sich der Client nach diesem Zeitpunkt im Leerlauf befindet. Standardmäßig ist der Zeitüberschreitungswert des Clients auf 180 Sekunden festgelegt.

So legen Sie einen Timeoutwert für Leerlauf-Clientverbindungen mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -cltTimeout <Value>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -cltTimeout 100
<!--NeedCopy-->
```

So legen Sie einen Timeoutwert für Leerlauf-Clientverbindungen mit der GUI fest

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Klicken Sie **unter Erweiterte Einstellungen** auf **Verkehrseinstellungen**, und legen Sie den Wert für die Leerlaufzeit des Clients in Sekunden fest.

RTSP-Verbindungen verwalten

October 5, 2021

Die Citrix ADC Appliance kann eine der zwei Topologien (NAT-Ein-Modus oder NAT-Aus-Modus) zum Lastenausgleich von RTSP-Servern verwenden. Im NAT-on-Modus ist Network Address Translation (NAT) aktiviert und auf der Appliance konfiguriert. RTSP-Anfragen und -Antworten werden durch die Appliance weitergeleitet. Daher müssen Sie die Appliance so konfigurieren, dass die Netzwerkadressübersetzung (Network Address Translation, NAT) durchgeführt wird, um die Datenverbindung zu identifizieren.

Weitere Informationen zum Aktivieren und Konfigurieren von NAT finden Sie unter IP-Adressierung.

Im NAT-Aus-Modus ist NAT nicht aktiviert und konfiguriert. Die Appliance empfängt RTSP-Anforderungen vom Client und leitet sie an den Dienst weiter, den sie mit der konfigurierten Lastausgleichsmethode auswählt. Die Lastausgleichs-RTSP-Server senden ihre Antworten direkt an den Client unter Umgehung der Appliance. Daher müssen Sie die Appliance so konfigurieren, dass der DSR-Modus (Direct Server Return) verwendet wird, und den RTSP-Servern öffentlich zugängliche FQDNs in DNS zuweisen.

Weitere Informationen zum Aktivieren und Konfigurieren des DSR-Modus finden Sie unter Konfigurieren des Lastenausgleichs im Rückgabemodus für Direktserver. Weitere Informationen zum Konfigurieren von DNS finden Sie unter Domänennamensystem. In beiden Fällen müssen Sie bei der Konfiguration des RTSP-Lastenausgleichs auch Rtspnat so konfigurieren, dass er der Topologie des Lastausgleichs entspricht.

So konfigurieren Sie RTSP NAT mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name>  -RTSPNAT <ValueOfRTSPNAT>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver vserver-LB-1  -RTSPNAT ON
<!--NeedCopy-->
```

So konfigurieren Sie RTSP NAT mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie einen virtuellen Server vom Typ RTSP.
2. Klicken Sie unter Erweiterte Einstellungen auf **Verkehrseinstellungen**, und wählen Sie **RTSP Natting**aus.

Verwalten Sie den Clientdatenverkehr basierend auf der Verkehrsrate

October 5, 2021

Sie können die Datenverkehrsrate überwachen, die durch virtuelle Server mit Lastenausgleich fließt, und das Verhalten der Citrix ADC Appliance basierend auf der Datenverkehrsrate steuern. Beispiel:

- Drosseln Sie den Verkehrsfluss, wenn er zu hoch ist.
- Cache Informationen basierend auf der Datenverkehrsrate.
- Wenn die Datenverkehrsrate zu hoch ist, leiten Sie überschüssigen Datenverkehr auf einen anderen virtuellen Lastausgleichsserver um.
- Wenden Sie die ratenbasierte Überwachung auf HTTP- und Domainnamen-System-Anfragen (DNS) an.

Weitere Informationen zu zinsbasierten Richtlinien finden Sie unter Zinsbegrenzung.

Identifizieren einer Verbindung mit Layer-2-Parametern

October 5, 2021

Zur Identifizierung einer Verbindung verwendet die Citrix ADC Appliance im Allgemeinen das 4-Tupel der Client-IP-Adresse, des Clientports, der Ziel-IP-Adresse und des Zielports. Wenn Sie die Option L2-Verbindung aktivieren, werden zusätzlich zum normalen 4-Tupel die Layer-2-Parameter der Verbindung (Kanalnummer, MAC-Adresse und VLAN-ID) verwendet.

Wenn Sie den Parameter L2Conn für einen virtuellen Lastausgleichsserver aktivieren, können mehrere TCP- und Nicht-TCP-Verbindungen mit demselben 4-Tupel (<source IP>:<source port>::<destination IP>:<destination port>), um auf der Citrix ADC Appliance nebeneinander zu existieren. Die Appliance verwendet sowohl den 4-Tupel- als auch den Layer 2-Parameter, um TCP- und Nicht-TCP-Verbindungen zu identifizieren.

Sie können die Option L2Conn in den folgenden Szenarien aktivieren:

- Mehrere VLANs werden auf der Citrix ADC Appliance konfiguriert, und für jedes VLAN wird eine Firewall eingerichtet.
- Sie möchten, dass der Datenverkehr, der von den Servern in einem VLAN stammt und für einen virtuellen Server in einem anderen VLAN gebunden ist, die für beide VLANs konfigurierten Firewalls durchläuft.

Wenn daher eine nCore Citrix ADC Appliance, auf der der Parameter L2conn für einen oder mehrere virtuelle Lastausgleichsserver festgelegt ist, auf einen klassischen Build oder auf einen nCore Build heruntergestuft wird, der den Parameter L2Conn nicht unterstützt, werden die Lastausgleichskonfigurationen, die den Parameter L2conn verwenden, unwirksam.

So konfigurieren Sie die L2-Verbindungsoption mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb vserver <name> <serviceType> <IPAddress>@ <port> -l2Conn ON
2 <!--NeedCopy-->
```

Beispiel


```
 add lb vserver LB-VIP1 HTTP 10.1.1.254 80 -l2Conn ON
<!--NeedCopy-->
```

So konfigurieren Sie die L2-Verbindungsoption mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter Erweiterte Einstellungen die Option Verkehrseinstellungen und dann Layer-2-Parameter aus.

Konfigurieren Sie die Option Direkte Route bevorzugen

October 5, 2021

Wenn Sie auf einem virtuellen Wildcard-Load Balancing Server explizit eine Route zu einem Ziel konfigurieren, leitet die Citrix ADC Appliance den Datenverkehr entsprechend der konfigurierten Route weiter. Wenn die Appliance nicht nach der konfigurierten Route suchen soll, können Sie die Option Direkte Route bevorzugen auf NO einstellen.

Wenn ein Gerät direkt mit einer Citrix ADC Appliance verbunden ist, leitet die Appliance den Datenverkehr direkt an das Gerät weiter. Wenn das Ziel eines Pakets beispielsweise eine Firewall ist, muss das Paket nicht über eine andere Firewall weitergeleitet werden. Manchmal möchten Sie jedoch möglicherweise, dass der Datenverkehr durch die Firewall fließt, selbst wenn das Gerät direkt mit ihm verbunden ist. In solchen Fällen können Sie die Option Direkte Route bevorzugen auf NO setzen.

Hinweis: Die Einstellung PreferDirectRoute gilt für alle virtuellen Platzhalterserver auf der Citrix ADC Appliance.

So legen Sie die Option Direkte Route bevorzugen mit der CLI fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb parameter -preferDirectRoute (YES | NO)
<!--NeedCopy-->
```

Beispiel:


```
set lb parameter -preferDirectRoute YES
<!--NeedCopy-->
```

So legen Sie die Option Direkte Route bevorzugen mit der GUI fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Load Balancing-Parameter konfigurieren**.
2. Wählen Sie Direkte Route bevorzugen.

Verwenden Sie einen Quellport aus einem bestimmten Portbereich für Back-End-Kommunikation

October 5, 2021

Standardmäßig kommuniziert die Citrix ADC Appliance bei Konfigurationen mit deaktivierter USIP-Option oder mit aktivierten Proxy-Port-Optionen mit den Servern über einen zufälligen Quellport (größer als 1024).

Die Appliance unterstützt die Verwendung eines Quellports aus einem angegebenen Portbereich für die Kommunikation mit den Servern. Einer der Anwendungsfälle dieser Funktion ist Server, die so konfiguriert sind, dass sie den empfangenen Datenverkehr, der zu einem bestimmten Satz gehört, basierend auf dem Quellport für Protokollierungs- und Überwachungszwecke identifizieren. Beispiel: Identifizieren des internen und externen Datenverkehrs für Protokollierungszwecke.

Die Konfiguration der Citrix ADC Appliance für die Verwendung eines Quellports aus einem Portbereich für die Kommunikation mit den Servern besteht aus den folgenden Aufgaben:

- **Erstellen Sie ein Netzprofil und legen Sie den Quellportbereichsparameter fest**. Ein Parameter für den Quellportbereich gibt einen oder mehrere Portbereiche an. Die Appliance wählt nach dem Zufallsprinzip einen der freien Ports aus den angegebenen Portbereichen aus und verwendet ihn als Quellport für jede Verbindung zu Servern.
- **Binden Sie das Netzprofil an den Lastenausgleich von virtuellen Servern, Diensten oder Dienstgruppen**: Ein Netzprofil mit Quellportbereichseinstellung kann an einen virtuellen Server, einen Dienst oder eine Dienstgruppe einer Lastausgleichskonfiguration gebunden werden. Für eine Verbindung mit einem virtuellen Server wählt die Appliance nach dem Zufallsprinzip einen der freien Ports aus den angegebenen Portbereichen eines Netzprofils aus und verwendet diesen Port als Quellport für die Verbindung mit einem der gebundenen Server.

So geben Sie einen Quellportbereich oder -bereiche mit der CLI an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind netProfile <name> (-srcPortRange <int[-int]> ...)

show netprofile <name>
<!--NeedCopy-->
```

So geben Sie einen Quellportbereich oder -bereiche mit der GUI an

1. Navigieren Sie zu **System** > **Netzwerk** > **Net Profile**.
2. Legen Sie den Parameter **Source Port Range** fest, während Sie NetProfiles hinzufügen oder ändern.

Beispielkonfiguration

In der folgenden Beispielkonfiguration hat das Netzprofil PARTIAL-NAT-1 teilweise NAT-Einstellungen und ist an den Lastenausgleich des virtuellen Servers LBVS-1 gebunden, der vom Typ ANY ist. Bei Paketen, die von 192.0.0.0/8 auf LBVS-1 empfangen wurden, übersetzt die Citrix ADC Appliance das letzte Oktett der Quell-IP-Adresse des Pakets in 100. Ein Paket mit Quell-IP-Adresse 192.0.2.30, das auf LBVS-1 empfangen wurde, übersetzt die Citrix ADC Appliance die Quell-IP-Adresse in 100.0.2.30, bevor sie einen der gebundenen Server sendet.

```
```
> add netprofile CUSTOM-SRCPORT-NP-1
Done
> bind netprofile CUSTOM-SRCPRT-NP-1 - srcportrange 2000-3000

Done
> bind netprofile CUSTOM-SRCPRT-NP-1 - srcportrange 5000-6000

Done
> add lb vserver LBVS-1 ANY 203.0.113. 61 * -netprofile PARTIAL-NAT-1

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

 
```

Konfigurieren der Quell-IP-Persistenz für Back-End-Kommunikation

October 5, 2021

Standardmäßig verwendet die Citrix ADC Appliance für eine Lastausgleichskonfiguration mit deaktivierter USIP-Option und einem Netzprofil, das an einen virtuellen Server oder Dienste oder Dienstgruppen gebunden ist, den Roundrobin-Algorithmus, um eine IP-Adresse aus dem Netzprofil für die Kommunikation mit den Servern auszuwählen. Aufgrund dieser Auswahlmethode kann die ausgewählte IP-Adresse für verschiedene Sitzungen eines bestimmten Clients unterschiedlich sein.

Einige Situationen erfordern, dass die Citrix ADC Appliance den gesamten Datenverkehr eines bestimmten Clients von derselben IP-Adresse leitet, wenn der Datenverkehr an Server gesendet wird. Die Server können dann beispielsweise Datenverkehr, der zu einem bestimmten Satz gehört, für Protokollierungs- und Überwachungszwecke identifizieren.

Die Quell-IP-Persistenzoption eines Netzprofils ermöglicht es der Citrix ADC Appliance, dieselbe Adresse zu verwenden, die im Netzprofil angegeben ist, um mit Servern über alle Sitzungen zu kommunizieren, die von einem bestimmten Client zu einem virtuellen Server initiiert wurden.

So aktivieren Sie die Quell-IP-Persistenz in einem Netzprofil mit der CLI

Um die Quell-IP-Persistenz beim Hinzufügen eines Netzprofils zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add netProfile <name> -srcippersistency ( ENABLED | DISABLED )
2
3 show netprofile <name>
4 <!--NeedCopy-->
```

Um die Quell-IP-Persistenz in einem vorhandenen Netzprofil zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set netProfile <name> -srcippersistency ( ENABLED | DISABLED )
2
3 show netprofile <name>
4 <!--NeedCopy-->
```

So aktivieren Sie die Quell-IP-Persistenz in einem Netzprofil mit der GUI

1. Navigieren Sie zu **System** > **Netzwerk** > **Net Profile**.

2. Wählen Sie **Quell-IP-Persistenz** aus, während Sie ein Netzprofil hinzufügen oder ändern.

Beispiel

In der folgenden Beispielkonfiguration hat Netprofil NETPROFILE-IPPRSTNCY-1 die Quell-IP-Persistenzoption aktiviert und ist an den Lastenausgleich des virtuellen Servers LBVS-1 gebunden.

Die Citrix ADC Appliance verwendet immer dieselbe IP-Adresse (in diesem Beispiel 192.0.2.11), um mit Servern zu kommunizieren, die an LBVS-1 gebunden sind, für alle Sitzungen, die von einem bestimmten Client zum virtuellen Server initiiert wurden.

```
```
> add ipset IPSET-1

Done
> bind ipset IPSET-1 192.0.2.[11-15]
 IPAddress ”192.0.2.11” bound
 IPAddress ”192.0.2.12” bound
 IPAddress ”192.0.2.13” bound
 IPAddress ”192.0.2.14” bound
 IPAddress ”192.0.2.15” bound
 Done
> add netprofile NETPROFILE-IPPRSTNCY-1 -srcIp IPSET-1 -
   srcippersistency ENABLED

Done
> set lb vserver LBVS-1 -netprofile NETPROFILE-IPPRSTNCY-1

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

## Verwenden Sie lokale IPv6-Linkadressen auf der Serverseite eines Load Balancing-Setups

October 5, 2021

Die lokale IPv6-Link-Adresse wird für Dienste, Dienstgruppen und Server einer Lastausgleichskonfiguration unterstützt. Sie können eine lokale IPv6-Adresse des Links zusammen mit der zugehörigen VLAN-ID in Diensten, Dienstgruppen und Serverkonfigurationen angeben. Die Citrix ADC Appliance

 
```

verwendet die lokale SNIP6-Adresse des Links aus demselben VLAN, wie in den Diensten, Dienstgruppen und Serverkonfigurationen angegeben, um mit ihnen zu kommunizieren.

Eine lokale IPv6-Adresse und die zugehörige VLAN-ID werden in Diensten, Dienstgruppen und Serverkonfigurationen im folgenden Format angegeben: <IPv6_Addrs>%<vlan_id>

Beispielsweise ist fe80:123:4567::a%2048:, fe80:123:4567::a die link-lokale Adresse UND 2048 ist die VLAN-ID.

```
> add service SERVICE-1 fe80:123:4567::a%2048 HTTP 80

Done
> bind servicegroup SERVICE-GROUP-1 fe80::1%24 80

Done
> add server SERVER-1 fe80:b:c:d::e:f:a/64%1028

Done
```

Erweiterte Lastenausgleichseinstellungen

October 5, 2021

Neben der Konfiguration virtueller Server können Sie erweiterte Einstellungen für Dienste konfigurieren.

Informationen zum Konfigurieren der erweiterten Lastenausgleichseinstellungen finden Sie in den folgenden Abschnitten:

- Schrittweise die Last eines neuen Dienstes mit langsamem Start auf virtueller Serverebene erhöhen
- Die Option ohne Monitor für Dienste
- Schützen von Anwendungen auf geschützten Servern vor Überlastung des Datenverkehrs
- Bereinigung von virtuellen Server- und Dienstverbindungen aktivieren
- Ordnungsgemäßes Herunterfahren von Diensten
- Aktivieren oder Deaktivieren der Persistenzsitzung auf TROFS-Diensten
- Direkte Anfragen an eine benutzerdefinierte Webseite
- Zugriff auf Dienste aktivieren, wenn sie deaktiviert sind
- TCP-Pufferung von Antworten aktivieren
- Komprimierung aktivieren
- Verwalten der Clientverbindung für mehrere Clientanforderungen

- IP-Adresse des Clients in den Request-Header einfügen
- Standortdetails von der Benutzer-IP-Adresse mit der Geolocation-Datenbank abrufen
- Verwenden Sie die Quell-IP-Adresse des Clients, wenn Sie eine Verbindung zum Server herstellen
- Konfigurieren des Quellports für serverseitige Verbindungen
- Festlegen eines Grenzwerts für die Anzahl der Clientverbindungen
- Festlegen eines Grenzwerts für die Anzahl der Anforderungen pro Verbindung zum Server
- Festlegen eines Schwellenwerts für die an einen Dienst gebundenen Monitore
- Festlegen eines Timeoutwerts für Leerlauf-Clientverbindungen
- Festlegen eines Zeitüberschreitungswertes für Serververbindungen im Leerlauf
- Festlegen eines Grenzwerts für die Bandbreitenauslastung durch Clients
- Umleiten von Clientanforderungen an einen Cache
- VLAN-Bezeichner für VLAN-Transparenz beibehalten
- Konfigurieren des automatischen Statusübergangs basierend auf dem prozentualen Zustand der gebundenen Dienste

Schrittweise die Last eines neuen Dienstes mit langsamem Start auf virtueller Serverebene erhöhen

October 5, 2021

Sie können die Citrix ADC Appliance so konfigurieren, dass die Auslastung eines Dienstes (die Anzahl der Anforderungen, die der Dienst pro Sekunde erhält) schrittweise erhöht, nachdem der Dienst entweder zu einer Lastenausgleichskonfiguration hinzugefügt wurde oder eine Statusänderung von DOWN zu UP vorgenommen hat (in diesem Dokument lautet der Begriff “neuer Dienst” wird für beide Situationen verwendet). Sie können die Last entweder manuell mit Lastwerten und Intervallen Ihrer Wahl erhöhen (manueller langsamer Start) oder die Appliance so konfigurieren, dass sie die Last in einem bestimmten Intervall erhöht (automatischer langsamer Start), bis der Dienst so viele Anforderungen erhält wie die anderen Dienste in der Konfiguration. Während des Hochlaufzeitraums für den neuen Dienst verwendet die Appliance die konfigurierte Lastausgleichsmethode.

Diese Funktionalität ist nicht global verfügbar. Es muss für jeden virtuellen Server konfiguriert werden. Die Funktionalität ist nur für virtuelle Server verfügbar, die eine der folgenden Lastausgleichsmethoden verwenden:

- Round Robin
- Geringste Verbindung
- Geringste Reaktionszeit
- Geringste Bandbreite
- Am wenigsten Pakete

- LRTM (Methode der geringsten Antwortzeit)
- Benutzerdefiniertes Laden

Für diese Funktionalität müssen Sie die folgenden Parameter festlegen:

- Die neue Serviceanforderungsrate, d. h. der Betrag, um den die Anzahl oder den Prozentsatz der Anforderungen erhöht werden, die bei jeder Erhöhung der Rate an einen neuen Dienst gesendet werden. Das heißt, Sie geben die Größe des Inkrements entweder in Bezug auf die Anzahl der Anforderungen pro Sekunde oder den Prozentsatz der Last an, die zu diesem Zeitpunkt von den vorhandenen Diensten getragen wird. Wenn dieser Wert auf 0 (Null) festgelegt ist, wird der langsame Start für neue Dienste nicht ausgeführt.

  Hinweis: In einem automatisierten Langsamstartmodus ist das letzte Inkrement kleiner als der angegebene Wert, wenn der angegebene Wert den neuen Dienst stärker belasten würde als bei den anderen Diensten.

- Das Inkrementintervall in Sekunden. Wenn dieser Wert auf 0 (Null) gesetzt ist, wird die Last nicht automatisch erhöht. Sie müssen es manuell erhöhen.

Bei einem automatisierten langsamen Start wird ein Dienst aus der langsamen Startphase herausgenommen, wenn eine der folgenden Bedingungen zutrifft:

- Die tatsächliche Anforderungsrate ist niedriger als die neue Serviceanforderungsrate.
- Der Dienst empfängt keinen Datenverkehr für drei aufeinanderfolgende Inkrementintervalle.
- Die Anforderungsrate wurde 200 Mal erhöht.
- Der Prozentsatz des Datenverkehrs, den der neue Dienst empfangen muss, ist größer oder gleich 100.

Beim manuellen langsamen Start bleibt der Dienst in der langsamen Startphase, bis Sie ihn aus dieser Phase herausnehmen.

Manueller langsamer Start

Wenn Sie die Last für einen neuen Dienst manuell erhöhen möchten, geben Sie kein Inkrementintervall für den virtuellen Lastausgleichsserver an. Geben Sie nur die neue Serviceanforderungsrate und die Einheiten an. Da kein Intervall angegeben ist, erhöht die Appliance die Last nicht periodisch. Es behält die Last auf den neuen Dienst mit dem Wert bei, der durch die Kombination aus der neuen Serviceanforderungsrate und Einheiten angegeben wird, bis Sie einen der Parameter manuell ändern. Wenn Sie beispielsweise die neue Serviceanforderungsrate und die Einheitsparameter auf 25 bzw. “pro Sekunde” festlegen, behält die Appliance die Last für den neuen Dienst bei 25 Anforderungen pro Sekunde bei, bis Sie einen der Parameter ändern. Wenn der neue Dienst den langsamen Startmodus beenden und so viele Anforderungen wie die vorhandenen Dienste empfangen soll, legen Sie den neuen Parameter für die Serviceanforderungsrate auf 0 fest.

Nehmen Sie beispielsweise an, dass Sie einen virtuellen Server zum Lastenausgleich 2 Dienste, Service1 und Service2, im Round-Robin-Modus verwenden. Ferner wird davon ausgegangen, dass der virtuelle Server 240 Anforderungen pro Sekunde empfängt und dass er die Last gleichmäßig über die Dienste verteilt. Wenn ein neuer Dienst, Service3, zur Konfiguration hinzugefügt wird, sollten Sie die Last auf ihn manuell durch Werte von 10, 20 und 40 Anforderungen pro Sekunde erhöhen, bevor Sie den vollen Anteil der Last senden. Die folgende Tabelle zeigt die Werte, auf die Sie die drei Parameter festlegen.

Tabelle 1. Parameterwerte

Parameter	Wert
Intervall in Sekunden	0
Neue Serviceanforderungsrate	10, 20, 40 und 0, in Intervallen, die Sie wählen
Einheiten für die neue Serviceanforderungsrate	Anfragen pro Sekunde

Wenn Sie den neuen Service-Requestrate-Parameter auf 0 setzen, wird Service3 nicht mehr als neuer Dienst betrachtet und erhält seinen vollen Anteil der Last.

Angenommen Sie, Sie einen anderen Dienst, Service4, während der Hochlaufzeit für Service3 hinzufügen. In diesem Beispiel wird Service4 hinzugefügt, wenn der neue Parameter für die Serviceanfrage auf 40 festgelegt ist. Daher beginnt Service4 40 Anfragen pro Sekunde zu empfangen.

Die folgende Tabelle zeigt die Lastverteilung der Dienste während des in diesem Beispiel beschriebenen Zeitraums.

Tabelle 2. Lastverteilung auf Services beim manuellen Aufstieg der Last

	Rate der neuen Serviceanfrage = 10 Anforderungen/Sek. (Service3added)	Rate der neuen Serviceanfrage = 20 Anforderungen/Sek.	Rate der neuen Serviceanfrage = 40 Anforderungen/Sek. (Service4added)	Neue Serviceanforderungsrate = 0 req/sec (neue Dienste beenden langsamen Startmodus)
Service1	115	110	80	60
Service2	115	110	80	60
Service3	10	20	40	60
Service4	-	-	40	60

	Rate der neuen Serviceanfrage = 10 Anforderungen/Sek. (Service3added)	Rate der neuen Serviceanfrage = 20 Anforderungen/Sek.	Rate der neuen Serviceanfrage = 40 Anforderungen/Sek. (Service4added)	Neue Serviceanforderungsrate = 0 req/sec (neue Dienste beenden langsamen Startmodus)
Gesamte Req/sec (Last auf dem virtuellen Server)	240	240	240	240

Automatischer langsamer Start

Wenn Sie möchten, dass die Appliance die Last eines neuen Dienstes automatisch in bestimmten Intervallen erhöht, bis der Dienst als fähig angesehen werden kann, seinen vollen Anteil der Last zu verarbeiten, legen Sie den neuen Parameter für die Serviceanfrage, den Einheitenparameter und das Inkrementintervall fest. Wenn alle Parameter auf andere Werte als 0 eingestellt sind, erhöht die Appliance die Belastung eines neuen Dienstes im angegebenen Intervall um den Wert der neuen Serviceanforderungsrate, bis der Dienst seinen vollen Anteil an der Last erhält.

Angenommen, vier Dienste, Service1, Service2, Service3 und Service4, sind an einen virtuellen Lastausgleichsserver vserver1 gebunden. Nehmen Sie ferner an, dass vserver1 100 Anforderungen pro Sekunde empfängt und die Last gleichmäßig auf die Dienste verteilt (25 Anforderungen pro Sekunde pro Dienst). Wenn Sie der Konfiguration einen fünften Dienst, Service5, hinzufügen, möchten Sie möglicherweise, dass die Appliance den neuen Dienst 4 Anforderungen pro Sekunde für die ersten 10 Sekunden, 8 Anforderungen pro Sekunde für die nächsten 10 Sekunden usw. sendet, bis 20 Anforderungen pro Sekunde empfangen wird. Für diese Anforderung zeigt die folgende Tabelle die Werte, auf die Sie die drei Parameter einstellen:

Tabelle 3. Parameterwerte

Parameter	**Wert**
Intervall in Sekunden	10
Inkrementwert	4
Einheiten für die neue Serviceanforderungsrate	Anfragen pro Sekunde

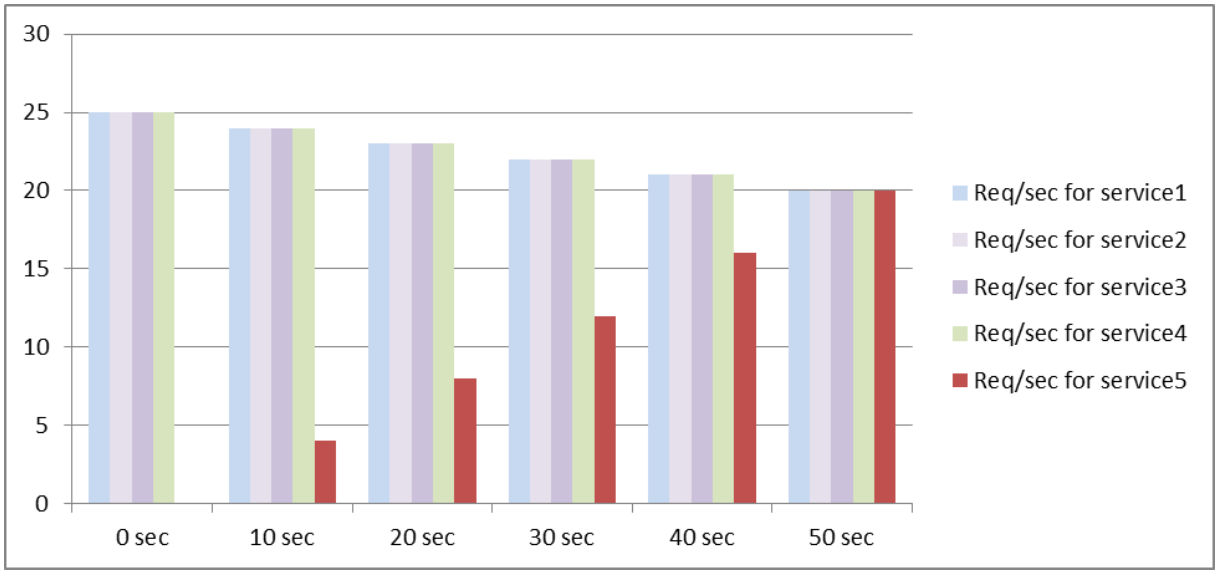
Mit dieser Konfiguration beginnt der neue Dienst 50 Sekunden, nachdem er hinzugefügt wurde oder

sein Status von DOWN in UP geändert wurde, so viele Anforderungen wie die vorhandenen Dienste zu empfangen. Während jedes Intervalls in diesem Zeitraum verteilt die Appliance den Überschuss an Anforderungen, die ohne schrittweise Inkremente an den neuen Dienst gesendet worden wären, an die vorhandenen Server. In Ermangelung von schrittweisen Schritten hätte jeder Dienst, einschließlich Service5, 20 Anfragen pro Sekunde erhalten. In schrittweisen Schritten verteilt die Appliance während der ersten 10 Sekunden, wenn Service5 nur 4 Anforderungen pro Sekunde empfängt, den Überschuss von 16 Anforderungen pro Sekunde an die vorhandenen Dienste, was zu dem Verteilungsmuster in der folgenden Tabelle und Abbildung über den Zeitraum von 50 Sekunden führt. Nach der 50-Sekunden-Periode gilt Service5 nicht mehr als neuer Dienst und erhält seinen normalen Anteil am Verkehr.

Tabelle 4. Lastverteilungsmuster für alle Dienste für den 50-Sekunden-Zeitraum unmittelbar nach dem Hinzufügen von Service5

	0 Sek.	10 Sek.	20 Sek.	30 Sek.	40 s	50 s
Anruf/Sek für Service1	25	24	23	22	21	20
Anruf/Sek für Service2	25	24	23	22	21	20
Anruf/Sek für Service3	25	24	23	22	21	20
Anruf/Sek für Service4	25	24	23	22	21	20
Anruf/Sek für Service5	0	4	8	12	16	20
Gesamte Req/sec (Last auf dem virtuellen Server)	100	100	100	100	100	100

Abbildung 1. Diagramm des Lastverteilungsmusters für alle Dienste für den 50-Sekunden-Zeitraum unmittelbar nach dem Hinzufügen von Service5



Eine alternative Anforderung besteht möglicherweise darin, dass die Appliance Service5 25% der Auslastung der vorhandenen Dienste in den ersten 5 Sekunden, 50% in den nächsten 5 Sekunden usw. sendet, bis 20 Anforderungen pro Sekunde empfangen wird. Für diese Anforderung zeigt die folgende Tabelle die Werte, auf die Sie die drei Parameter festlegen.

Tabelle 5. Parameterwerte

Parameter	Wert
Intervall in Sekunden	5
Inkrementwert	25
Einheiten für die neue Serviceanforderungsrate	Prozent

Mit dieser Konfiguration beginnt der Dienst 20 Sekunden, nachdem er hinzugefügt wurde oder sein Status von DOWN in UP geändert wurde, so viele Anforderungen wie die vorhandenen Dienste zu empfangen. Die Verkehrsverteilung während der Hochlaufzeit für den neuen Dienst ist identisch mit der zuvor beschriebenen, wobei die Einheit für die Schrittschritte “Anforderungen pro Sekunde” war.

Setze die Parameter für den langsamen Start

Sie legen die Parameter für den langsamen Start fest, indem Sie entweder den Befehl `set lb vserver` oder den `add lb vserver` Befehl verwenden. Der folgende Befehl dient zum Festlegen von langsamen Startparametern beim Hinzufügen eines virtuellen Servers.

So konfigurieren Sie stufenweise Lastinkremente für einen neuen Dienst mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um schrittweise Inkremente der Last für einen Dienst zu konfigurieren und die Konfiguration zu überprüfen:

```
add lb vserver <name> <serviceType> <IPAddress> <port> [-
    newServiceRequest <positive_integer>] [<newServiceRequestUnit>] [-
    newServiceRequestIncrementInterval <positive_integer>]

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

Beispiel

```
set lb vserver BR_LB -newServiceRequest 5 PER_SECOND -
    newServiceRequestIncrementInterval 10
Done

show lb vserver BR_LB
BR_LB (192.0.2.33:80) - HTTP Type: ADDRESS
State: UP
...
...
New Service Startup Request Rate: 5 PER_SECOND, Increment Interval: 10
...
...
Done
<!--NeedCopy-->
```

So konfigurieren Sie schrittweise Lastinkremente für einen neuen Dienst mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter Erweiterte Einstellungen die Option Methode aus, und legen Sie die folgenden langsamen Startparameter fest:
   - Rate der neuen Dienststartanforderung.
   - Neue Serviceanforderungseinheit.

- Inkrementierungsintervall.

Die Option ohne Monitor für Dienste

October 5, 2021

Wenn Sie ein externes System zum Durchführen von Integritätsprüfungen für die Dienste verwenden und nicht möchten, dass die Citrix ADC Appliance den Zustand eines Dienstes überwacht, können Sie die Option Kein Monitor für den Dienst festlegen. In diesem Fall sendet die Appliance keine Prüfpunkte, um den Zustand des Dienstes zu überprüfen, sondern zeigt den Dienst als UP an. Selbst wenn der Dienst heruntergefahren wird, sendet die Appliance weiterhin Datenverkehr vom Client an den Dienst, wie durch die Lastausgleichsmethode angegeben.

Der Monitor kann den Status ENABLED oder DISABLED haben, wenn Sie die Option no-monitor festlegen und wenn Sie die Option no-monitor entfernen, wird der frühere Status des Monitors fortgesetzt.

Sie können die Option Kein Monitor für einen Dienst beim Erstellen des Dienstes festlegen. Sie können auch die Option Kein Monitor für einen vorhandenen Dienst festlegen.

Die folgenden Folgen haben die Einstellung der Option Kein Monitor:

- Wenn ein Dienst, für den Sie die Option Kein Monitor aktiviert haben, ausfällt, zeigt die Appliance den Dienst weiterhin als UP an und leitet den Datenverkehr weiter an den Dienst weiter. Eine dauerhafte Verbindung zum Dienst kann die Situation verschlechtern. In diesem Fall oder wenn viele Dienste, die als UP angezeigt werden, tatsächlich DOWN sind, kann das System fehlschlagen. Um eine solche Situation zu vermeiden, entfernen Sie den Dienst aus der Citrix ADC-Konfiguration, wenn der externe Mechanismus, der die Dienste überwacht, einen Dienst als DOWN meldet.
- Wenn Sie die Option Kein Monitor für einen Dienst konfigurieren, können Sie den Lastausgleich im Direct Server Return (DSR) -Modus nicht konfigurieren. Wenn Sie für einen vorhandenen Dienst die Option Kein Monitor festlegen, können Sie den DSR-Modus für den Dienst nicht konfigurieren.

So legen Sie die Option Kein Monitor für einen neuen Dienst mithilfe der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen Dienst mit der Option Integritätsmonitor zu erstellen, und überprüfen Sie die Konfiguration:

```
1 add service <serviceName> <IP | serverName> <serviceType> <port> -
     healthMonitor (YES|NO)
```



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

Beispiel:

```
add service nomonsrvc 10.102.21.21 http 80 -healthMonitor no
Done

show service nomonsrvc
nomonsrvc (10.102.21.21:80) - HTTP
State: UP
Last state change was at Mon Nov 15 22:41:29 2010
Time since last state change: 0 days, 00:00:00.970
Server Name: 10.102.21.21
 Server ID : 0 Monitor Threshold : 0
...
Access Down Service: NO
...
Down state flush: ENABLED
Health monitoring: OFF

1 bound monitor:
1) Monitor Name: tcp-default
State: UNKNOWN Weight: 1
Probes: 3 Failed [Total: 3 Current: 3]
Last response: Probe skipped - Health monitoring is turned off.
Response Time: N/A
Done
<!--NeedCopy-->
```

So legen Sie die Option Kein Monitor für einen vorhandenen Dienst mithilfe der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die Integritätsüberwachungsoption festzulegen:

```
set service <name> -healthMonitor (YES|NO)
<!--NeedCopy-->
```

Beispiel:


```
By default, the state of a service and the state of the corresponding
   monitor are UP.
 >show service LB-SVC1
LB-SVC1 (10.102.29.5:80) - HTTP
State: UP


1) Monitor Name: http-ecv
 State: UP Weight: 1
Probes: 99992 Failed [Total: 0 Current: 0]
Last response: Success - Pattern found in response.
Response Time: 3.76 millisec
Done

When the no-monitor option is set on a service, the state of the
   monitor changes to UNKNOWN.
set service LB-SVC1 -healthMonitor NO
Done

show service LB-SVC1
LB-SVC1 (10.102.29.5:80) - HTTP
State: UP
Last state change was at Fri Dec 10 10:17:37 2010.
Time since last state change: 5 days, 18:55:48.710
Health monitoring: OFF

1) Monitor Name: http-ecv
   State: UNKNOWN Weight: 1
         Probes: 100028 Failed [Total: 0 Current: 0]
   Last response: Probe skipped - Health monitoring is turned off.
     Response Time: 0.0 millisec
  Done
When the no-monitor option is removed, the earlier state of the monitor
    is resumed.
> set service LB-SVC1 -healthMonitor YES
Done
>show service LB-SVC1
LB-SVC1 (10.102.29.5:80) - HTTP
State: UP
Last state change was at Fri Dec 10 10:17:37 2010
Time since last state change: 5 days, 18:57:47.880
1) Monitor Name: http-ecv
   State: UP Weight: 1
   Probes: 100029 Failed [Total: 0 Current: 0]
```



```
    Last response: Success - Pattern found in response.
    Response Time: 5.690 millisec
    Done
<!--NeedCopy-->
```

So legen Sie die Option Kein Monitor für einen Dienst mit der GUI fest

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Öffnen Sie den Dienst, und deaktivieren Sie die Integritätsüberwachung.

Schützen von Anwendungen auf geschützten Servern vor Überlastung des Datenverkehrs

October 5, 2021

Die Citrix ADC Appliance bietet die Überspannungsschutzoption, um die Kapazität eines Servers oder Caches aufrechtzuerhalten. Die Appliance regelt den Fluss von Clientanforderungen an Server und steuert die Anzahl der Clients, die gleichzeitig auf die Server zugreifen können. Die Appliance blockiert alle an den Server übergebenen Überspannungen und verhindert so eine Überlastung des Servers.

Damit der Überspannungsschutz ordnungsgemäß funktioniert, müssen Sie ihn global aktivieren. Weitere Informationen zum Überspannungsschutz finden Sie unter Überspannungsschutz.

So legen Sie Überspannungsschutz für den Dienst mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -sp <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -sp ON
<!--NeedCopy-->
```


So stellen Sie den Überspannungsschutz für den Dienst mit der GUI ein

1. Navigieren Sie zu **Traffic Management > Load Balancing > Dienste**, und öffnen Sie eine Quelle.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und wählen Sie **Überspannungsschutz**aus.

Bereinigung von virtuellen Server- und Dienstverbindungen aktivieren

October 5, 2021

Der Status eines virtuellen Servers hängt von den Zuständen der an ihn gebundenen Dienste ab. Der Status jedes Dienstes hängt von den Antworten der Server mit Lastausgleich auf Probes oder Zustandsprüfungen ab, die von den Monitoren gesendet werden, die an diesen Dienst gebunden sind. Manchmal reagieren die Server mit Lastausgleich nicht. Wenn ein Server langsam oder ausgelastet ist, kann ein Timeout der Überwachung von Prüfpunkten erfolgen. Wenn wiederholte Überwachungssonden nicht innerhalb der konfigurierten Zeitüberschreitungszeit beantwortet werden, wird der Dienst mit DOWN gekennzeichnet. Wenn ein Dienst oder virtueller Server als DOWN gekennzeichnet ist, müssen die server- und clientseitigen Verbindungen geleert werden. Durch das Beenden vorhandener Verbindungen werden Ressourcen freigegeben und in bestimmten Fällen wird die Wiederherstellung überlasteter Lastausgleichseinstellungen beschleunigt.

Unter bestimmten Bedingungen können Sie die Einstellung **DownStateFlush** so konfigurieren, dass vorhandene Verbindungen sofort beendet werden, wenn ein Dienst oder ein virtueller Server als DOWN markiert ist. Aktivieren Sie die DownStateFlush-Einstellung nicht auf den Anwendungsservern, die ihre Transaktionen abschließen müssen. Sie können diese Einstellung auf Webservern aktivieren, deren Verbindungen sicher beendet werden können, wenn sie DOWN markiert haben.

In der folgenden Tabelle werden die Auswirkungen dieser Einstellung auf eine Beispielkonfiguration zusammengefasst, die aus einem virtuellen Server, vServer-LB-1, besteht und an diesen Dienst gebunden ist, Service-1. In der Tabelle bezeichnen E und D den Status der Einstellung DownStateFlush: E bedeutet Aktiviert und D bedeutet Deaktiviert.

Vserver-LB-1	Service-1	Zustand der Verbindungen
E	E	Sowohl Client- als auch Serververbindungen werden beendet.

Vserver-LB-1	Service-1	Zustand der Verbindungen
E	D	Bei einigen Diensttypen, z. B. TCP, für die die Citrix ADC Appliance die Wiederverwendung der Verbindung nicht unterstützt, werden sowohl Client- als auch Serververbindungen beendet. Bei Diensttypen wie HTTP, für die die Appliance die Wiederverwendung der Verbindung unterstützt, werden sowohl Client- als auch Serververbindungen nur beendet, wenn eine Transaktion für diese Verbindungen aktiv ist. Wenn eine Transaktion nicht aktiv ist, werden nur Clientverbindungen beendet.

Vserver-LB-1	Service-1	Zustand der Verbindungen
D	E	Bei einigen Diensttypen, z. B. TCP, für die die Citrix ADC Appliance die Wiederverwendung der Verbindung nicht unterstützt, werden sowohl Client- als auch Serververbindungen beendet. Bei Diensttypen wie HTTP, für die die Appliance die Wiederverwendung der Verbindung unterstützt, werden sowohl Client- als auch Serververbindungen nur beendet, wenn eine Transaktion für diese Verbindungen aktiv ist. Wenn eine Transaktion nicht aktiv ist, werden nur Serververbindungen beendet.
D	D	Weder Client- noch Serververbindungen werden beendet.

Wenn Sie einen Dienst nur deaktivieren möchten, wenn alle etablierten Verbindungen vom Server oder vom Client geschlossen werden, können Sie die Option ordnungsgemäßes Herunterfahren verwenden. Informationen zum ordnungsmäßigen Herunterfahren eines Dienstes finden Sie unter Graceful Shutdown of Services.

So legen Sie Down State Flush auf dem Dienst mit der CLI fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name>  -downStateFlush (ENABLED | DISABLED )
<!--NeedCopy-->
```

Beispiel:


```
set service Service-HTTP-1 -downStateFlush enabled
<!--NeedCopy-->
```

So legen Sie Down State Flush auf dem Dienst mit der GUI fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und wählen Sie **Nach unten Status Flush**aus.

So legen Sie Down State Flush auf dem virtuellen Server mit der CLI fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name>  -downStateFlush (ENABLED | DISABLED )
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver vsvr1 -downStateFlush enabled
<!--NeedCopy-->
```

So legen Sie Down State Flush auf dem virtuellen Server mit der GUI fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und wählen Sie **Nach unten Status Flush**aus.

Ordnungsgemäßes Herunterfahren von Diensten

October 5, 2021

Während geplanter Netzwerkausfälle wie Systemaktualisierungen oder Hardwarewartung müssen Sie möglicherweise einige Dienste schließen oder deaktivieren. Sie können den Dienst später mithilfe des<name> Befehls enable service aktivieren.

Um zu vermeiden, dass etablierte Sitzungen unterbrochen werden, können Sie einen Dienst im TROFS-Status (Transition Out of Service) platzieren, indem Sie einen der folgenden Schritte ausführen:

- Hinzufügen eines TROFS-Codes oder einer Zeichenfolge zum Monitor: Konfigurieren Sie den Server so, dass er einen bestimmten Code oder eine bestimmte Zeichenfolge als Antwort auf einen Monitor Probe sendet.
- Deaktivieren Sie den Dienst explizit und:
  - Stellen Sie eine Verzögerung (in Sekunden) ein.
  - Aktivieren Sie das ordnungsgemäße Herunterfahren.

Hinzufügen eines TROFS-Codes oder einer Zeichenfolge

Wenn Sie nur einen Monitor an einen Dienst binden und der Monitor TROFS-fähig ist, kann er den Dienst auf der Grundlage der Antwort des Servers auf einen Monitor Probe in den TROFS-Status versetzen. Diese Antwort wird mit dem Wert im Parameter TrofsCode für einen HTTP-Monitor oder dem Parameter TrofsString für einen HTTP-ECV oder TCP-ECV Monitor verglichen. Wenn der Code übereinstimmt, wird der Dienst in den TROFS-Status abgelegt. In diesem Zustand werden die persistenten Verbindungen weiterhin berücksichtigt.

Wenn mehrere Monitore an einen Dienst gebunden sind, wird der effektive Status des Dienstes auf der Grundlage des Zustands aller Monitore berechnet, die an den Dienst gebunden sind. Nach Erhalt einer TROFS-Antwort wird der Status des TROFS-fähigen Monitors für die Zwecke dieser Berechnung als UP angesehen. Weitere Informationen darüber, wie eine Citrix ADC Appliance einen Dienst als UP bezeichnet, finden Sie unter Festlegen eines Schwellenwerts für die an einen Dienst gebundenen Monitore.

Wichtig:

- Sie können mehrere Monitore an einen Dienst binden, dürfen jedoch nicht mehr als einen von ihnen für TROFS aktivieren.
- Sie können einen TROFS-fähigen Monitor in einen Monitor konvertieren, der nicht TROFS-fähig ist, aber nicht umgekehrt.

So konfigurieren Sie einen TROFS-Code oder eine Zeichenfolge in einem Monitor mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
add lb monitor <monitor-name> HTTP -trofsCode <respcode>

add lb monitor <monitor-name> HTTP-ECV  -trofsString <resp string>

```



```
add lb monitor <monitor-name> TCP-ECV  -trofsString <resp string>
<!--NeedCopy-->
```

So ändern Sie den TROFS-Code oder die Zeichenfolge mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
set lb monitor <trofs monitorname> HTTP -trofscode <newcode>

set lb monitor <trofs monitorname> HTTP-ECV -trofsstring <new string>

set lb monitor <trofs monitorname> TCP-ECV -trofsstring <new string>
<!--NeedCopy-->
```

Hinweis: Sie können den Befehl set nur verwenden, wenn früher ein TROFS-fähiger Monitor hinzugefügt wurde. Sie können diesen Befehl nicht verwenden, um den TROFS-Code oder die Zeichenfolge für einen Monitor festzulegen, der nicht TROFS aktiviert ist.

So konfigurieren Sie einen TROFS-Code oder eine Zeichenfolge in einem Monitor mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu Traffic Management > Load Balancing > Monitore.
2. Klicken Sie im Bereich Monitore auf Hinzufügen, und führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie Typ als HTTP aus, und geben Sie einen TROFS-Code an.
   - Wählen Sie Typ als HTTP-ECV oder TCP-ECV aus, und geben Sie einen TROFS-String an.

Deaktivieren eines Dienstes

Häufig können Sie jedoch nicht schätzen, wie viel Zeit für alle Verbindungen zu einem Dienst benötigt wird, um die vorhandenen Transaktionen abzuschließen. Wenn eine Transaktion nach Ablauf der Wartezeit nicht abgeschlossen ist, kann das Herunterfahren des Dienstes zu Datenverlust führen. In diesem Fall können Sie ein ordnungsgemäßes Herunterfahren für den Dienst angeben, sodass der Dienst nur deaktiviert wird, wenn alle aktuellen aktiven Clientverbindungen entweder vom Server oder vom Client geschlossen werden. In der folgenden Tabelle finden Sie das Verhalten, wenn Sie zusätzlich zum ordnungsgemäßes Herunterfahren eine Wartezeit angeben.

Die Persistenz wird gemäß der angegebenen Methode beibehalten, auch wenn Sie ein ordnungsgemäßes Herunterfahren aktivieren. Das System bedient weiterhin alle persistenten Clients, einschließlich neuer Verbindungen von den Clients, es sei denn, der Dienst wird während des

ordnungsgemäßen Herunterfahrens als Ergebnis der von einem Monitor durchgeführten Prüfungen auf DOWN markiert.

In der folgenden Tabelle werden die Optionen zum ordnungsmäßigen Herunterfahren beschrieben.

Status	Ergebnisse
Das ordnungsgemäße Herunterfahren ist aktiviert und eine Wartezeit wird angegeben.	Der Dienst wird heruntergefahren, nachdem die letzte der aktuellen aktiven Clientverbindungen bereitgestellt wurde, selbst wenn die Wartezeit nicht abgelaufen ist. Die Appliance überprüft den Status der Verbindungen einmal pro Sekunde. Wenn die Wartezeit abläuft, werden alle offenen Sitzungen geschlossen.
Das ordnungsgemäße Herunterfahren ist deaktiviert und eine Wartezeit wird angegeben.	Der Dienst wird erst nach Ablauf der Wartezeit heruntergefahren, selbst wenn alle etablierten Verbindungen vor Ablauf bereitgestellt werden.
Das ordnungsgemäße Herunterfahren ist aktiviert und es wird keine Wartezeit angegeben.	Der Dienst wird erst heruntergefahren, nachdem die letzte der zuvor eingerichteten Verbindungen bereitgestellt wurde, unabhängig von der Zeit, die für die letzte Verbindung gebraucht wurde.
Das ordnungsgemäße Herunterfahren ist deaktiviert und es wird keine Wartezeit angegeben.	Kein ordnungsgemäßes Herunterfahren. Der Dienst wird sofort heruntergefahren, nachdem die Deaktivierungsoption ausgewählt wurde oder der Deaktivierungsbefehl ausgegeben wurde. (Die Standard-Wartezeit beträgt 0 Sekunden.)

Um vorhandene Verbindungen zu beenden, wenn ein Dienst oder ein virtueller Server als DOWN markiert ist, können Sie die Option Down-State-Flush verwenden. Weitere Informationen finden Sie unter Bereinigung virtueller Serververbindungen aktivieren.

So konfigurieren Sie ein ordnungsgemäßes Herunterfahren für einen Dienst mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen Dienst ordnungsgemäß herunterzufahren und die Konfiguration zu überprüfen:


```
disable service <name> [<delay>] [-graceFul (YES|NO)]

show service <name>
<!--NeedCopy-->
```

Beispiel:

```
> disable service svc1 6000 -graceFul YES
Done
>show service svc1
svc1 (10.102.80.41:80) - HTTP
State: GOING OUT OF SERVICE (Graceful, Out Of Service in 5998 seconds)
Last state change was at Mon Nov 15 22:44:15 2010
Time since last state change: 0 days, 00:00:01.160
...
Down state flush: ENABLED

1 bound monitor:
1) Monitor Name: tcp-default
State: UP              Weight: 1
Probes: 13898    Failed [Total: 0 Current: 0]
Last response: Probe skipped - live traffic to service.
Response Time: N/A
Done

>show service svc1
svc1 (10.102.80.41:80) - HTTP
State: OUT OF SERVICE
Last state change was at Mon Nov 15 22:44:19 2010
Time since last state change: 0 days, 00:00:03.250
Down state flush: ENABLED

1 bound monitor:
1)  Monitor Name: tcp-default
State: UNKNOWN           Weight: 1
Probes: 13898    Failed [Total: 0 Current: 0]
Last response: Probe skipped - service state OFS.
Response Time: N/A
Done
<!--NeedCopy-->
```


So konfigurieren Sie das ordnungsgemäße Herunterfahren für einen Dienst mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Öffnen Sie den Dienst, und klicken Sie in der Liste Aktion auf Deaktivieren. Geben Sie eine Wartezeit ein und wählen Sie Graceful aus.

Aktivieren oder Deaktivieren der Persistenzsitzung auf TROFS-Diensten

October 5, 2021

Sie können das TrofsPersistence-Flag festlegen, um anzugeben, ob ein Dienst im Status Transition Out of Service (TROFS) persistente Sitzungen beibehalten muss. Wenn ein Monitor TROFS aktiviert ist, kann er einen Dienst auf der Grundlage der Antwort des Servers auf einen Monitor Probe in den TROFS-Status versetzen. Diese Antwort wird mit dem Wert im Parameter TrofsCode für einen HTTP-Monitor oder dem Parameter TrofsString für einen HTTP-ECV oder TCP-ECV Monitor verglichen. Wenn der Code übereinstimmt, wird der Dienst in den TROFS-Status abgelegt. In diesem Zustand werden die aktiven Clientverbindungen weiterhin berücksichtigt. In einigen Fällen müssen die geehrten aktiven Sitzungen möglicherweise dauerhafte Sitzungen enthalten. In anderen Fällen, insbesondere solchen, die langlebige Persistenzsitzungen oder Persistenzmethoden wie benutzerdefinierte Server-ID beinhalten, kann die Einhaltung der persistenten Sitzungen jedoch verhindern, dass der Dienst in den Out-of-Service-Status übergeht.

Wenn Sie das TROFSPersistence-Flag auf ENABLED setzen, werden persistente Sitzungen berücksichtigt. Wenn Sie es auf DEAKTIVIERT setzen, sind sie dies nicht.

So legen Sie das TROFSPersistence-Flag mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um das`trofsPersistence` Flag für einen neuen virtuellen Server oder einen vorhandenen virtuellen Server festzulegen oder um die Einstellung auf den Standardwert zurückzusetzen:

```
add lb vserver <name> [-trofsPersistence ( ENABLED | DISABLED )]

set lb vserver <name> [-trofsPersistence ( ENABLED | DISABLED )]

unset lb vserver <name> [-trofsPersistence]
<!--NeedCopy-->
```


Argument

trofsPersistence. Beachten Sie aktuelle aktive Clientverbindungen und neue Anforderungen für Persistenzsitzungen, wenn sich der Dienst im TROFS-Status befindet.

Mögliche Werte: ENABLED, DISABLED. Standard: ENABLED.

Beispiele:

```
add lb vserver v1 http 10.102.217.42 80 -persistencetype SOURCEIP -
    trofsPersistence ENABLED

set lb vserver v1 -trofsPersistence DISABLED

unset lb vserver v1 -trofsPersistence
<!--NeedCopy-->
```

Direkte Anfragen an eine benutzerdefinierte Webseite

December 3, 2021

> **Warnung**
>
> SureConnect (SC) ist ab NetScaler 12.0 Build 56.20 veraltet. Alternativ empfiehlt Citrix die Verwendung der AppQOE-Funktion. Weitere Informationen finden Sie unterAppQoE.

Damit SureConnect richtig funktioniert, müssen Sie es global festlegen. Citrix ADC stellt die SureConnect Option bereit, um die Antwort einer Anwendung sicherzustellen.
Weitere Informationen zur SureConnect-Option finden Sie unter Sure Connect.

So legen Sie SureConnect für den Dienst mit der CLI fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -sc <Value>
<!--NeedCopy-->
```

Beispiel:


```
set service Service-HTTP-1 -sc ON
<!--NeedCopy-->
```

So legen Sie SureConnect für den Dienst mit der GUI fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen die Option Verkehrseinstellungen aus und wählen Sie **Sicher Verbinden**aus.

Zugriff auf Dienste aktivieren, wenn sie deaktiviert sind

October 5, 2021

Sie können den Zugriff auf einen Dienst aktivieren, wenn er deaktiviert ist oder in einem DOWN Zustand ist, indem Sie die Citrix ADC Appliance so konfigurieren, dass der Layer-2-Modus verwendet wird, um die an den Dienst gesendeten Pakete zu überbrücken. Wenn Anforderungen an Dienste weitergeleitet werden, die DOWN sind, werden die Anforderungspakete normalerweise gelöscht. Wenn Sie die Einstellung **Access Down** aktivieren, werden diese Anforderungspakete jedoch direkt an die Server mit Lastausgleich gesendet.

Weitere Informationen zu den Modi Layer 2 und Layer 3 finden Sie unter IP-Adressierung.

Damit die Appliance Pakete überbrückt, die an die DOWN-Services gesendet werden, aktivieren Sie den Layer-2-Modus mit dem AccessDown-Parameter.

So aktivieren Sie den Zugriff auf einen Dienst mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -accessDown <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -accessDown YES
<!--NeedCopy-->
```


So aktivieren Sie den Zugriff auf einen Dienst mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und wählen Sie **Zugriff nach unten**aus.

TCP-Pufferung von Antworten aktivieren

October 5, 2021

Die Citrix ADC Appliance bietet eine TCP-Pufferungsoption, die nur Antworten vom Server mit Lastausgleich puffert. Auf diese Weise kann die Appliance Serverantworten an den Client mit der maximalen Geschwindigkeit übermitteln, die der Client sie akzeptieren kann. Die Appliance weist 0 bis 4095 MB (MB) Speicher für TCP-Pufferung und von 4 bis 20480 Kilobyte (KB) Speicher pro Verbindung zu.

Hinweis: TCP-Pufferung auf Service-Ebene hat Vorrang vor der globalen Einstellung.
Weitere Informationen zum globalen Konfigurieren von TCP-Pufferung finden Sie unter TCP-Pufferung.

So aktivieren Sie die TCP-Pufferung für einen Dienst mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -TCPB <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -TCPB YES
<!--NeedCopy-->
```

So aktivieren Sie die TCP-Pufferung für einen Dienst mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und wählen Sie **TCP-Pufferung**aus.

Komprimierung aktivieren

October 5, 2021

Die Citrix ADC Appliance stellt eine Komprimierungsoption zur transparenten Komprimierung von HTML- und Textdateien mithilfe einer Reihe integrierter Komprimierungsrichtlinien bereit. Durch die Komprimierung werden die Bandbreitenanforderungen reduziert und die Reaktionsfähigkeit der Server in Setups mit eingeschränkter Bandbreite erheblich verbessert. Die Komprimierungsrichtlinien sind Diensten zugeordnet, die an den virtuellen Server gebunden sind. Die Richtlinien legen fest, ob eine Antwort komprimiert werden kann, und senden Sie komprimierbare Inhalte an die Appliance, die sie komprimiert und an den Client sendet.

Hinweis: Damit die Komprimierung ordnungsgemäß funktioniert, müssen Sie sie global aktivieren. Weitere Informationen zum globalen Konfigurieren der Komprimierung finden Sie unter Komprimierung.

So aktivieren Sie die Komprimierung für einen Dienst mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -CMP <YES | NO>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -CMP YES
<!--NeedCopy-->
```

So aktivieren Sie die Komprimierung für einen Dienst mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und wählen Sie **Komprimierung**aus.

Externe TCP-Zustandsprüfung für virtuelle UDP-Server aktivieren

October 5, 2021

In Public Clouds können Sie die Citrix ADC Appliance als Load Balancer der zweiten Ebene verwenden, wenn der native Load Balancer als erste Stufe verwendet wird. Der native Load Balancer kann ein Application Load Balancer (ALB) oder ein Network Load Balancer (NLB) sein. Die meisten Public Clouds unterstützen keine UDP-Integritätstrübe in ihren nativen Lastausgleichsdiensten. Um die Integrität der UDP-Anwendung zu überwachen, empfehlen Public Clouds, Ihrem Dienst einen TCP-basierten Endpunkt hinzuzufügen. Der Endpunkt spiegelt die Integrität der UDP-Anwendung wider.

Die Citrix ADC Appliance unterstützt die externe TCP-basierte Zustandsprüfung für einen virtuellen UDP-Server. Diese Funktion führt einen TCP-Listener für die VIP des virtuellen Servers und den konfigurierten Port ein. Der TCP-Listener gibt den Status des virtuellen Servers wieder.

So aktivieren Sie eine externe TCP-Integritätsprüfung für virtuelle UDP-Server nach CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine externe TCP-Integritätsprüfung mit der Option TCPProbePort zu aktivieren:

```
1 add lb vserver <name> <serviceType> <IPAddress> <port> -tcpProbePort <
     tcpProbePort>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add lb vserver Vserver-UDP-1 UDP 10.102.29.60 80 tcpProbePort 5000
2 <!--NeedCopy-->
```

So aktivieren Sie eine externe TCP-Integritätsprüfung für virtuelle UDP-Server nach GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und erstellen Sie dann einen virtuellen Server.
2. Klicken Sie auf **Hinzufügen**, um einen virtuellen Server zu erstellen.
3. Fügen Sie im Bereich **Grundeinstellungen** die Portnummer im Feld **TCP-Probe-Port** hinzu.
4. Klicken Sie auf **OK**.

Verwalten der Clientverbindung für mehrere Clientanforderungen

October 5, 2021

Sie können den Keepalive-Parameter des Clients festlegen, um einen HTTP- oder SSL-Dienst so zu konfigurieren, dass eine Clientverbindung zu einer Website über mehrere Clientanforderungen hinweg geöffnet bleibt. Wenn Client Keep-Alive aktiviert ist, selbst wenn der Webserver mit Lastausgleich eine Verbindung schließt, hält die Citrix ADC Appliance die Verbindung zwischen dem Client und sich selbst offen. Diese Einstellung ermöglicht es Diensten, mehrere Clientanforderungen auf einer einzelnen Clientverbindung zu bedienen.

Wenn Sie diese Einstellung nicht aktivieren, öffnet der Client für jede Anfrage, die er an die Website sendet, eine neue Verbindung. Die Client-Keepalive-Einstellung speichert die Paket-Round-Trip-Zeit, die zum Herstellen und Schließen von Verbindungen erforderlich ist. Diese Einstellung verkürzt auch die Zeit, bis jede Transaktion abgeschlossen ist. Client Keep-Alive kann nur für HTTP- oder SSL-Diensttypen aktiviert werden.

Client-Keepalive-Einstellung auf Service-Ebene hat Vorrang vor der globalen Client-Keepalive-Einstellung. Weitere Informationen über das Keep-Alive des Clients finden Sie unter Client Keep-Alive.

So aktivieren Sie den Client Keep-Alive für einen Dienst über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -CKA <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -CKA YES
<!--NeedCopy-->
```

So aktivieren Sie den Client Keep-Alive für einen Dienst über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und öffnen Sie einen Dienst.

2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und wählen Sie **Client Keep-Alive**aus.

IP-Adresse des Clients in den Request-Header einfügen

October 5, 2021

Ein Citrix ADC verwendet die Subnetz-IP (SNIP) -Adresse, um eine Verbindung mit dem Server herzustellen. Der Server muss den Client nicht kennen.

In manchen Situationen muss der Server jedoch den Client kennen, den er bedienen muss. Wenn Sie die Client-IP-Einstellung aktivieren, fügt die Appliance die IPv4- oder IPv6-Adresse des Clients ein, während die Anforderungen an den Server weitergeleitet werden. Der Server fügt diese Client-IP in den Header der Antworten ein. Dem Server ist somit der Client bekannt.

> **Hinweis**: Um mehrere Header einzufügen, müssen Sie einen der folgenden Schritte ausführen:
>
> - Fügen Sie Rewrite-Richtlinien hinzu, um CLIENT.IS_SSL zu überprüfen, und fügen Sie entsprechende Header ein.
> - Binden Sie die entsprechende Rewrite-Richtlinie für jeden virtuellen Server basierend auf dem Typ.

So fügen Sie die Client-IP-Adresse über die Befehlszeilenschnittstelle in die Clientanfrage ein

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -CIP <Value> <cipHeader>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -CIP enabled X-Forwarded-For
<!--NeedCopy-->
```


So fügen Sie die Client-IP-Adresse über die grafische Benutzeroberfläche in die Clientanfrage ein

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**, und bearbeiten Sie einen Service.
2. Klicken Sie im Bereich **Diensteinstellungen** auf das **Bearbeitungssymbol**.
3. Aktivieren Sie im Bereich **Lastenausgleichsdienst** das Kontrollkästchen **Client-IP-Adresse einfügen**.

Standortdetails von der Benutzer-IP-Adresse mit der Geolocation-Datenbank abrufen

October 5, 2021

> **Hinweis** Diese Funktion ist ab Citrix ADC Release 12.1 Build 50.x und höher verfügbar.

Die Citrix ADC Appliance kann Details zum Benutzerstandort wie Kontinent, County und Stadt abrufen. Für jede öffentliche IP-Adresse aus einer Geostandortdatenbank. Es wird unter Verwendung der erweiterten Richtlinieninfrastruktur durchgeführt. Die abgerufenen Standortdetails werden dann in einer Umschreibaktion oder einer Responder-Aktion zum Ausführen der folgenden Anwendungsfälle verwendet.

- Fügen Sie beim Senden der Clientanforderung an den Back-End-Server einen HTTP-Header mit Benutzerstandortdetails ein (z. B. Land, Stadt)
- Fügen Sie Ländernamen in der HTML-Seitenantwort für einen ungültigen Benutzer hinzu.

Die Appliance kann die Standortdetails auch mit dem Überwachungsprotokollierungsmechanismus protokollieren.

Abrufen von Benutzerstandortdetails mithilfe von Geolocation-Funktionen

Die Komponenten interagieren wie folgt:

1. Der Benutzer sendet eine Clientanforderung von einem bestimmten geografischen Standort aus.
2. Die Citrix ADC Appliance sucht nach der Benutzer-IP-Adresse aus der Client-Anfrage und ruft die Geo-Standortdetails ab. Zu den Details gehören Kontinent, Land, Region, Stadt, ISP, Organisation oder benutzerdefinierte Details aus einer Geolocation-Datenbank.
3. Sobald die Standortdetails abgerufen wurden, verwendet die Appliance entweder eine Responderrichtlinie oder eine Rewrite-Richtlinie, um die Anforderung auszuwerten.

4. In einer Rewrite-Richtlinie fügt die Appliance einen Header mit den Geo-Standortdetails hinzu und sendet ihn an den Back-End-Server. Fügen Sie beispielsweise einen benutzerdefinierten HTTP-Header mit Länderinformationen ein.
5. In einer Responder-Richtlinie wertet die Appliance die HTTP-Anfrage aus und ermöglicht auf der Grundlage der Richtlinienbewertung den Zugriff auf die Benutzer oder leitet den Benutzer auf eine Fehlerseite um. Es gibt an, dass die Region, von der aus sie auf die Anwendung zugreifen, keinen Zugriff hat.

Geolocation-Datenbank einrichten

Als Voraussetzung benötigen Sie eine Geolocation-Datenbank, um auf der Citrix ADC Appliance ausgeführt werden zu können. Die Geolocation-Datenbankdateien sind mit der Citrix ADC Firmware verfügbar. Um die Datenbankdateien von einem Anbieter herunterzuladen, konvertieren Sie sie in das Citrix ADC Format und importieren Sie sie in Ihre Appliance.
Weitere Informationen zur Geolokalisierungsdatenbank finden Sie unter Hinzufügen einer Standortdatei zum Erstellen einer statischen Näherungsdatenbank .

Geolocation-Funktionen

Die folgende Tabelle enthält eine Liste der Geolocation-Funktionen, die Standortdetails einer öffentlichen IP-Adresse abrufen. Diese Funktionen können in Rewrite- oder Responder-Richtlinien verwendet werden.

Geolocation-Funktion	Beispiel
CLIENT.IP.SRC.LOCATION	Asien.In.Karnataka.Bangalore
CLIENT.IP.SRC.LOCATION.GET (1) .LOCATION_LONG	Indien
CLIENT.IP.SRC.LOCATION (3)	Asien. Karnataka
CLIENT.IP.SRC.LAT_LONG	12,77
CLIENT.IPV6.SRC.LOCATION	Nordamerika.us.California.Santa Clara.Verizon.Citrix
CLIENT.IPV6.SRC.LOCATION(3)	Nordamerika.US.Kalifornien
CLIENT.IPV6.SRC.LOCATION.GET (1) .LOCATION_LONG	Vereinigte Staaten
CLIENT.IPV6.SRC.LOCATION.GET (3)	Kalifornien
CLIENT.IPV6.SRC.LAT_LONG	36, -119

Konfigurieren von Geolocation-Funktionen

Um Geolocation-Funktionen mit einer erweiterten Richtlinieninfrastruktur zu konfigurieren, müssen Sie die Funktionen für Lastenausgleich, Neuschreiben und Responder-Funktion aktivieren und dann die folgenden Anwendungsfälle abschließen.

Lastenausgleich, Responder, Rewrite Features aktivieren

Wenn Sie möchten, dass die Citrix ADC Appliance den Benutzerzugriff von einem bestimmten Geostandort aus autorisiert, müssen Sie die Funktionen für Load Balancing, Rewrite und Responder aktivieren.

```
1 enable ns feature loadbalancing rewrite responder
2 <!--NeedCopy-->
```

Anwendungsfall 1: Konfigurieren der Geolocation-Funktion zum Umleiten ungültiger Benutzer außerhalb des Geo-Sitess

Wenn ein Benutzer aus Indien Zugriff auf eine Webseite anfordert, blockieren Sie die Anfrage und antworten Sie mit einer HTML-Seite mit Ländernamen.

Die folgenden Schritte helfen Ihnen, die Konfiguration dieses Anwendungsfalls abzuschließen.

- Responderaktion hinzufügen
- Responder-Richtlinie hinzufügen
- Bind-Responderrichtlinie an den Lastausgleichsserver

Weitere Informationen zu den GUI-Prozeduren zum Umschreiben von Aktionen und zum Umschreiben der Richtlinienkonfiguration finden Sie unter Responder.

Responderaktion hinzufügen

Fügen Sie eine Responder-Aktion hinzu, um mit HTML-Seite mit Ländernamen zu antworten.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add responder action <name> <type> (<target> | <htmlpage>) [-comment <
     string>] [-responseStatusCode <positive_integer>][-reasonPhrase <
     string>]
2 <!--NeedCopy-->
```


Beispiel:

```
add responder action responder_act respondwith "HTTP.REQ.VERSION + "
    304 Requested Page not allowed in your country - " + CLIENT.IP.SRC.
    LOCATION.GET (1).LOCATION_LONG + "\r\n""
<!--NeedCopy-->
```

Aktion für Audit-Protokollmeldungen hinzufügen

Sie können Überwachungsnachrichtenaktionen so konfigurieren, dass Nachrichten auf verschiedenen Protokollebenen protokolliert werden, entweder nur im Syslog-Format oder sowohl in Syslog als auch in newnslog Formaten. Auditmeldungsaktionen verwenden Ausdrücke, um das Format der Auditmeldungen anzugeben.
So erstellen Sie eine Auditmeldungsaktionen mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add audit messageaction <name> <logLevel> <stringBuilderExpr> [-logtoNewnslog
 (YES|NO)] [-bypassSafetyCheck (YES|NO)]
```

Beispiel:

```
add audit messageaction msg1 DEBUG ""Request Location: "+CLIENT.IP.SRC.
    LOCATION"
<!--NeedCopy-->
```

Responder-Richtlinie hinzufügen

Fügen Sie eine Responderrichtlinie hinzu, um Anfragen aus Indien zu identifizieren und die Responderaktion dieser Richtlinie zuzuordnen.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add responder policy <name> <rule> <action> [<undefAction>] [-comment <
    string>] [-logAction <string>] [-appflowAction <string>]
<!--NeedCopy-->
```

Beispiel:


```
add responder policy responder_pol CLIENT.IP.SRC.MATCHES_LOCATION("Asia
    .India.\*.\*.\*.\*") responder_act -logaction msg1
<!--NeedCopy-->
```

Bind-Responderrichtlinie an den Lastausgleichsserver

Binden Sie die Responderrichtlinie an einen virtuellen Lastausgleichsserver vom Typ HTTP/SSL.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <vserver name> -policyName < policy_name >  -priority
    <> -type <L7InlineREQUEST | L4Inline-REQUEST>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver http_vserver -policyName responder_pol -priority 100 -
    type REQUEST
<!--NeedCopy-->
```

Anwendungsfall 2: Konfigurieren der Geolocation-Funktion zum Einfügen eines neuen HTTP-Headers mit Standortdetails für das Back-End

Stellen Sie sich ein Szenario vor, in dem eine Citrix ADC Appliance den Benutzerspeicherort in den HTTP-Header einer an den Anwendungsserver gesendeten Anfrage einfügen muss, damit der Server die Informationen für eine bestimmte Geschäftslogik verwenden kann.
Die folgenden Schritte helfen Ihnen, die Konfiguration dieses Anwendungsfalls abzuschließen.

- Neuschreibaktion hinzufügen
- Richtlinie zum Umschreiben hinzufügen
- Umschreibrichtlinie an Lastenausgleich binden

Weitere Informationen zu den GUI-Prozeduren zum Umschreiben von Aktionen und zum Umschreiben der Richtlinienkonfiguration finden Sie unter Thema Responder .

Neuschreibaktion hinzufügen

Fügen Sie eine Rewrite-Aktion hinzu, um einen benutzerdefinierten HTTP-Header mit Benutzergeolocation-Details in die Anforderung einzufügen und ihm Back-End-Server zu senden.
Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-
    pattern <expression> | -search <expression>] [-refineSearch <string
    >][-comment <string>]
<!--NeedCopy-->
```

Beispiel:

```
add rewrite action rewrite_act insert_http_header "User_location"
    CLIENT.IP.SRC.LOCATION
<!--NeedCopy-->
```

Richtlinie zum Umschreiben hinzufügen

Fügen Sie eine Richtlinie zum Umschreiben hinzu, um zu bewerten, ob die Umschreibungsaktion ausgeführt werden muss. In diesem Fall müssen alle Anforderungen, die an den Anwendungsserver gehen, über einen benutzerdefinierten HTTP-Header verfügen, damit die Regel true sein kann.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add rewrite policy <name> <rule> <action> [<undefAction>] [-comment <
    string>] [-logAction <string>]
<!--NeedCopy-->
```

Beispiel:

```
add rewrite policy rewrite_pol true rewrite_act -logaction log_act
<!--NeedCopy-->
```

Umschreibrichtlinie an Lastenausgleich binden

Binden Sie die Rewrite-Richtlinie an den erforderlichen virtuellen Lastenausgleichsserver vom Typ HTTP/SSL.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <vserver name> -policyName < policy_name >  -priority
    <> -type <L7InlineREQUEST | L4Inline-REQUEST>
<!--NeedCopy-->
```


Beispiel:

```
bind lb vserver http_vserver -policyName rewrite_pol -priority 100 -
    type REQUEST
<!--NeedCopy-->
```

Syslog-Unterstützung für die Protokollierung von Geolocation-Details (optional)

Wenn Sie die Geolocation-Details des Benutzers protokollieren möchten, müssen Sie die SYSLOG-Aktion angeben, die ausgeführt werden soll, wenn eine Anforderung mit der Richtlinie übereinstimmt. Die Appliance speichert die Details als Protokollmeldung in der Datei ns.log.
Weitere Informationen zur SYSLOG- und NSLOG-Überwachung finden Sie unter Thema Audit-Protokollierung .

Ausgabe für Benutzergeolocation-Details

Die folgende Ausgabe wird in der Appliance mit dem SYSLOG oder der `newnslog` Aktion protokolliert, wenn Sie versuchen, vom Standort in Bangalore aus auf eine Anwendung zuzugreifen und wenn die Appliance die Geolokalisierungsfunktion “CLIENT.IP.SRC.LOCATION” verwendet.

```
Asia.India.Karnataka.Banglore
<!--NeedCopy-->
```

Beispielausgabeprotokoll:

```
07/23/2018:19:03:54 GMT  Debug 0-PPE-0 : default REWRITE Message 22 0 :
     ”Request Location: asia.in.karnataka.bangalore.\*.\*”
07/23/2018:19:23:55 GMT  Debug 0-PPE-0 : default RESPONDER Message 32 0
Done
<!--NeedCopy-->
```

Verwenden Sie die Quell-IP-Adresse des Clients, wenn Sie eine Verbindung zum Server herstellen

October 5, 2021

Sie können die Citrix ADC Appliance so konfigurieren, dass Pakete vom Client an den Server weitergeleitet werden, ohne die Quell-IP-Adresse zu ändern. Dies ist nützlich, wenn Sie die Client-IP-Adresse nicht in einen Header einfügen können, z. B. wenn Sie mit Nicht-HTTP-Diensten arbeiten.

Weitere Informationen zum globalen Konfigurieren von USIP finden Sie unter Aktivieren der Verwendung des Quell-IP-Modus.

So aktivieren Sie den USIP-Modus für einen Dienst mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -usip (YES | NO)
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -usip YES
<!--NeedCopy-->
```

So aktivieren Sie den USIP-Modus für einen Dienst mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienste**, und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen im Abschnitt Diensteinstellungen die Option **Quell-IP-Adresse verwenden**aus.

Verwenden Sie die Clientquell-IP-Adresse für Back-End-Kommunikation in einer v4-v6-Lastenausgleichskonfiguration

October 5, 2021

Bei Diensten mit deaktiviertem USIP kommuniziert die Citrix ADC Appliance in einer v4-zu-v6-Load Balancing-Konfiguration mit den zugehörigen Servern von einer der konfigurierten IPv6-SNIP-Adressen (SNIP6).

Für Dienste mit aktiviertem USIP müssen Sie den globalen USIP-NAT-Präfixparameter festlegen, damit die zugehörigen Server die IP-Adresse des Clients der Anforderungspakete erkennen. Das USIP NAT

Präfix ist ein globales IPv6-Präfix der Länge 32/40/48/56/64/96 Bit, das auf der Citrix ADC Appliance konfiguriert ist.

Bei einem Lastausgleichsdienst, bei dem USIP aktiviert ist, übersetzt die Appliance das IPv4-Anforderungspaket in ein IPv6-Paket und setzt die Quell-IP-Adresse des übersetzten IPv6-Pakets auf eine Verkettung von:

- das USIP NAT Präfix der Länge von 32/40/48/56/64/96 Bit.
- Nullen aufgefüllt, wenn die USIP NAT-Präfixlänge kleiner als 96 Bit ist. Anzahl der mit Nullen aufgefüllten Bits = 96-USIP NAT-Präfixlänge. Wenn beispielsweise die USIP NAT-Präfixlänge 64 ist, dann ist die Anzahl der mit Nullen aufgefüllten Bits = 96-64 = 32.
- die IPv4-Quelladresse [32 Bit], die im Anforderungspaket empfangen wurde. Mit anderen Worten, die letzten 32 Bits der Quell-IPv6-Adresse werden auf die IPv4-Adresse des Clients gesetzt.

Beim Empfang eines IPv6-Antwortpakets vom Server übersetzt die Citrix ADC Appliance das IPv6-Paket in ein IPv4-Paket und setzt die Ziel-IP-Adresse des übersetzten IPv4-Pakets auf die letzten 32 Bits der Ziel-IP-Adresse des IPv6-Pakets.

> **Hinweis**: Diese Funktion wird nicht für Citrix Gateway Konfiguration und für Konfigurationen für den Lastausgleich von Content Switching und Cache-Umleitung unterstützt.

Konfigurationsschritte

Das Konfigurieren von USIP für eine v4-zu-v6-Lastausgleichskonfiguration besteht aus den folgenden Aufgaben:

- **Fügen Sie das globale USIP NAT-Präfix**hinzu. Es ist ein globales IPv6-Präfix der Länge 32/40/48/56/64/96 Bit, das auf der Appliance konfiguriert werden soll.
- **Aktivieren Sie den globalen USIP-Modus**. Weitere Informationen finden Sie unter Aktivieren des Quell-IP-Modus verwenden.
- **Aktivieren Sie den USIP-Modus für Lastausgleichsdienste**. Weitere Informationen finden Sie unter Verwenden der Quell-IP-Adresse des Clients beim Herstellen einer Verbindung mit dem Server.

So fügen Sie mit der CLI ein globales USIP-NAT-Präfixhinzu:

- `set ipv6 -usipnatprefix <prefix/prefix_length>`
- `show ipv6`

So fügen Sie mit der GUI ein globales USIP-NAT-Präfixhinzu:

1. Navigieren Sie zu **System** > **Netzwerk**, und klicken Sie auf **IPv6-Einstellungen ändern** .
2. Legen Sie auf dem Bildschirm **Konfiguration für IPV6 konfigurieren** den Parameter **USIP NAT-Präfix** fest.

Beispielkonfiguration

```
> set ipv6 -usipnatprefix 2001:DB8:90::/64
Done

> enable ns mode USIP
Done

> add lb vserver LBVS-1 HTTP 203.0.113.90 80
Done

> add service SVC-1 2001:DB8:5001::30 HTTP 80 -usip yes
Done

> add service SVC-2 2001:DB8:5001::60 HTTP 80 -usip yes
Done

> bind lb vserver LBVS-1 SVC-1
Done

> bind lb vserver LBVS-1 SVC-2
Done

<!--NeedCopy-->
```

Konfigurieren des Quellports für serverseitige Verbindungen

October 5, 2021

Wenn die Citrix ADC Appliance eine Verbindung zu einem physischen Server herstellt, kann sie den Quellport aus der Anforderung des Clients verwenden oder einen Proxy-Port als Quellport für die Verbindung verwenden. Sie können den Parameter Proxy-Port verwenden auf YES festlegen, um Situationen wie das folgende Szenario zu behandeln:

- Die Citrix ADC Appliance ist mit zwei virtuellen Load Balancing-Servern LBVS1 und LBVS2 konfiguriert.
- Beide virtuellen Server sind an den gleichen Dienst gebunden, S-ANY.
- Die Verwendung der Quell-IP-Adresse (USIP) des Clients ist für den Dienst aktiviert.
- Client C1 sendet zwei Anforderungen, Req1 und Req2, für denselben Dienst.
- LBVS1 erhält Req1 und LBVS2 erhält Req2.
- LBVS1 und LBVS2 leiten die Anfrage an S-ANY weiter, und wenn S-ANY die Antwort sendet, leiten

LBVS1 und LBVS2 die Antwort an den Client weiter.

- Betrachten Sie zwei Fälle:
  - Verwenden Sie den Clientport. Wenn die Appliance den Clientport verwendet, verwenden sowohl die virtuellen Server die IP-Adresse des Clients (weil USIP ON ist) als auch den Port des Clients, wenn eine Verbindung zum Server hergestellt wird. Wenn der Dienst die Antwort sendet, kann die Appliance daher nicht feststellen, welcher virtuelle Server die Antwort erhalten muss.
  - Proxy-Port verwenden. Wenn die Appliance einen Proxyport verwendet, verwenden die virtuellen Server die IP-Adresse des Clients (weil USIP eingeschaltet ist), aber bei der Verbindung mit dem Server unterschiedliche Ports. Wenn der Dienst die Antwort sendet, identifiziert die Portnummer daher den virtuellen Server, der die Antwort erhalten muss.

Wenn Sie jedoch eine vollständig transparente Konfiguration benötigen, z. B. eine vollständig transparente Cache-Umleitungskonfiguration, müssen Sie die Einstellung Proxy-Port verwenden deaktivieren, damit die Citrix ADC Appliance den Quellport aus der Clientanforderung verwenden kann.

Die Option Proxy-Port verwenden wird relevant, wenn die Option USIP (Source IP) verwenden aktiviert ist. Für TCP-basierte Diensttypen wie TCP, HTTP und SSL ist die Option standardmäßig aktiviert. Bei UDP-basierten Diensttypen, wie UDP und DNS, einschließlich ANY, ist die Option standardmäßig deaktiviert. Weitere Informationen zur USIP-Option finden Sie unter "Aktivieren des Quell-IP-Modus. "

Sie können die Einstellung **Proxy-Port verwenden** entweder global oder für einen bestimmten Dienst konfigurieren.

Konfigurieren der Einstellung Proxyport verwenden für einen Dienst

Sie konfigurieren die Einstellung **ProxyPort verwenden** für den Dienst, wenn Sie die globale Einstellung außer Kraft setzen möchten.

So konfigurieren Sie die Einstellung Proxyport verwenden für einen Dienst mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -useProxyPort (YES | NO)
<!--NeedCopy-->
```

Beispiel:

```
set service svc1 -useproxyport YES
```



```
Done

show service svc1
svc1 (10.102.29.30:80) - HTTP
State: UP
. . .
Use Source IP: YES Use Proxy Port: YES
. . .
Done
<!--NeedCopy-->
```

So konfigurieren Sie die Einstellung Proxyport verwenden für einen Dienst mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen die Option Verkehrseinstellungen aus und wählen Sie **Proxyport verwenden**aus.

Konfigurieren der Einstellung für die Verwendung von Proxy-Ports global

Sie konfigurieren die Einstellung **Proxyport verwenden** global, wenn Sie die Einstellung auf alle Dienste auf der Citrix ADC Appliance anwenden möchten. Die **servicespezifischen Einstellungen "Proxy-Port verwenden** " überschreibt die globale Einstellung.

So konfigurieren Sie die Einstellung Proxyport global verwenden mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Einstellung **Proxy-Port verwenden** global zu konfigurieren und die Konfiguration zu überprüfen:

```
set ns param -useproxyport ( ENABLED | DISABLED )`
show ns param`
<!--NeedCopy-->
```

Beispiel:

```
set ns param -useproxyport ENABLED

Done

```



```
show ns param
Global configuration settings:
. . .
Use Proxy Port: ENABLED
Done
<!--NeedCopy-->
```

So konfigurieren Sie die Einstellung Proxyport global verwenden mit der GUI

Navigieren Sie zu **System > Einstellungen > Globale Systemeinstellungen ändern**, und wählen oder deaktivieren Sie Proxyport verwenden.

Festlegen eines Grenzwerts für die Anzahl der Clientverbindungen

October 5, 2021

Sie können eine maximale Anzahl von Clientverbindungen angeben, die jeder Lastausgleichsserver verarbeiten kann. Die Citrix ADC Appliance öffnet dann Clientverbindungen zu einem Server nur, bis dieser Grenzwert erreicht ist. Wenn der Lastausgleichsserver seine Grenze erreicht, werden Monitorsonden übersprungen, und der Server wird erst für den Lastausgleich verwendet, wenn er die Verarbeitung bestehender Verbindungen abgeschlossen hat und die Kapazität freigibt.

Weitere Informationen zur Einstellung " **Maximum Client** " finden Sie unter Load Balancing Domainname Based Services.

Hinweis: Verbindungen, die im Prozess des Schließens sind, werden für dieses Limit nicht berücksichtigt.

So legen Sie eine Begrenzung der Anzahl der Clientverbindungen mit der CLI fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -maxclient <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -maxClient 1000
<!--NeedCopy-->
```


So legen Sie eine Begrenzung der Anzahl der Clientverbindungen mit der GUI fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen **Schwellenwerte und Timeouts**aus und wählen Sie **Maximale Clients**aus.

Festlegen eines Grenzwerts für die Anzahl der Anforderungen pro Verbindung zum Server

October 5, 2021

Die Citrix ADC Appliance kann so konfiguriert werden, dass Verbindungen wiederverwendet werden, um die Leistung zu verbessern. In einigen Szenarien können Webserver mit Lastausgleich jedoch Probleme haben, wenn Verbindungen für zu viele Anfragen wiederverwendet werden. Verwenden Sie für HTTP- oder SSL-Dienste die Option max request, um die Anzahl der Anforderungen zu begrenzen, die über eine einzelne Verbindung an einen Lastausgleichswebserver gesendet werden.

Hinweis: Sie können die maximale Anforderungsoption nur für HTTP- oder SSL-Dienste konfigurieren.

So beschränken Sie die Anzahl der Clientanforderungen pro Verbindung mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <ServiceName> -maxReq <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -maxReq 100
<!--NeedCopy-->
```

So beschränken Sie die Anzahl der Clientanforderungen pro Verbindung mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen **Schwellenwerte und Timeouts**aus und wählen Sie **Maximale Anforderungen**aus.

Festlegen eines Schwellenwerts für die an einen Dienst gebundenen Monitore

October 5, 2021

Die Citrix ADC Appliance weist einen Dienst nur dann als UP aus, wenn die Summe der Gewichtungen aller Monitore, die an ihn gebunden sind und die UP dem für den Dienst konfigurierten Schwellenwert entspricht oder größer ist. Die Gewichtung für einen Monitor gibt an, wie viel dieser Monitor dazu beiträgt, den Dienst, an den er gebunden ist, als UP festzulegen.

Standardmäßig ist der Schwellenwert für den Monitor auf 0 und die Monitorgewichte auf 1 festgelegt. Alle Monitore haben dann gleiche Gewichtung und ein Service kann heruntergehen, wenn einer der Monitore ausfällt.

Nehmen wir beispielsweise an, dass drei Monitore mit den Namen Monitor-HTTP-1, Monitor-HTTP-2 und Monitor-HTTP-3 an Service-HTTP-1 gebunden sind und dass der für den Dienst konfigurierte Schwellenwert drei ist. Angenommen, jedem Monitor werden folgende Gewichtungen zugewiesen:

- Das Gewicht von Monitor-HTTP-1 ist 1.
- Das Gewicht von Monitor-HTTP-2 ist 3.
- Das Gewicht von Monitor-HTTP-3 ist 1.

Der Dienst wird nur dann als UP gekennzeichnet, wenn einer der folgenden Punkte zutrifft:

- Monitor-HTTP-2 ist UP.
- Monitor-HTTP-2 und Monitor-HTTP-1 oder Monitor-HTTP-3 sind UP
- Alle drei Monitore sind UP.

So legen Sie den Überwachungsschwellenwert für einen Dienst mit der CLI fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -monThreshold <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -monThreshold 100
<!--NeedCopy-->
```


So legen Sie den Überwachungsschwellenwert für einen Dienst mit der GUI fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen **Schwellenwerte und Timeouts**aus und wählen Sie **Schwellenwert überwachen**aus.

Festlegen eines Timeoutwerts für Leerlauf-Clientverbindungen

October 5, 2021

Sie können den Dienst mit einem Timeoutwert konfigurieren, um alle untätigen Clientverbindungen zu beenden, wenn die konfigurierte Zeit abgelaufen ist. Wenn sich der Client während der konfigurierten Zeit im Leerlauf befindet, schließt die Citrix ADC Appliance die Clientverbindung.

So legen Sie einen Timeoutwert für Leerlauf-Clientverbindungen mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -cltTimeout <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -cltTimeout 100
<!--NeedCopy-->
```

So legen Sie einen Timeoutwert für Leerlauf-Clientverbindungen mit der GUI fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen **Schwellenwerte und Timeouts**aus, und wählen Sie **Timeout für Client-Idle**aus.

Festlegen eines Zeitüberschreitungswertes für Serververbindungen im Leerlauf

October 5, 2021

Sie können einen Dienst mit einem Timeout-Wert so konfigurieren, dass alle inaktiv gegebenen Serververbindungen beendet werden, wenn die konfigurierte Zeit (in Sekunden) abgelaufen ist. Wenn sich der Server für den konfigurierten Zeitraum im Leerlauf befindet, schließt die Citrix ADC Appliance die Serververbindung.

So legen Sie einen Timeoutwert für Serververbindungen im Leerlauf mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -svrTimeout <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -svrTimeout 100
<!--NeedCopy-->
```

So legen Sie einen Timeoutwert für Serververbindungen im Leerlauf mit der GUI fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen **Schwellenwerte und Timeouts**aus, und wählen Sie **Timeout für Serverinaktivität**aus.

Festlegen eines Grenzwerts für die Bandbreitenauslastung durch Clients

October 5, 2021

Manchmal haben Server möglicherweise eine begrenzte Bandbreite für die Bearbeitung von Clientanforderungen und können überlastet werden. Um ein Überladen eines Servers zu verhindern, können

Sie eine maximale Grenze für die vom Server verarbeitete Bandbreite in Kbps angeben. Die Citrix ADC Appliance leitet Anforderungen nur dann an einen Server mit Lastausgleich weiter, bis dieser Grenzwert erreicht ist.

So legen Sie eine maximale Bandbreite für einen Dienst mit der CLI fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -maxBandwidth <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -maxBandwidth 100
<!--NeedCopy-->
```

So legen Sie eine maximale Bandbreite für einen Dienst mit der GUI fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und öffnen Sie einen Dienst.
2. Wählen Sie unter Erweiterte Einstellungen **Schwellenwerte und Timeouts**aus und wählen Sie **Maximale Bandbreite**aus.

Umleiten von Clientanforderungen an einen Cache

October 5, 2021

Sie können einen Dienst so konfigurieren, dass Clientanforderungen an einen Cache umgeleitet werden und die nicht zwischenspeicherbaren Anforderungen an einen Dienst weitergeleitet werden, der von der konfigurierten Lastausgleichsmethode ausgewählt wurde.

So legen Sie die Cache-Umleitung für einen Dienst mit der CLI fest

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set service <name> -cacheable <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-HTTP-1 -cacheable YES
<!--NeedCopy-->
```

So legen Sie die Cache-Umleitung für einen Dienst mit der GUI fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Öffnen Sie einen Dienst, und legen Sie den Cache-Typ fest.

VLAN-Bezeichner für VLAN-Transparenz beibehalten

October 5, 2021

Sie können einen virtuellen Lastausgleichsserver so konfigurieren, dass die VLAN-ID des Clients in Paketen beibehalten wird, die an Server weitergeleitet werden sollen. Der virtuelle Server muss ein virtueller Platzhalterserver vom Typ ANY sein und im MAC-Modus funktionieren.

So konfigurieren Sie einen virtuellen Lastausgleichsserver, um die Client-VLAN-ID mit der CLI beizubehalten

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um einen virtuellen Lastausgleichsserver so zu konfigurieren, dass die Client-VLAN-ID beibehalten und die Konfiguration überprüft wird:

```
set lb vserver <name> -m MAC -macmodeRetainvlan ENABLED

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

> **Hinweis:**

> Für einen Dienst, der an einen virtuellen Server gebunden ist, auf dem die `-m MAC` Option aktiviert ist, müssen Sie einen Nicht-Benutzermonitor binden.

So konfigurieren Sie einen virtuellen Lastausgleichsserver, um die Client-VLAN-ID mit der GUI beizubehalten

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und wählen Sie **VLAN-ID beibehalten**aus.

Konfigurieren des automatischen Statusübergangs basierend auf dem prozentualen Zustand der gebundenen Dienste

October 5, 2021

Sie können einen virtuellen Lastausgleichsserver so konfigurieren, dass er automatisch vom Status UP in den DOWN wechselt, wenn der Prozentsatz der aktiven Dienste unter einen konfigurierten Schwellenwert fällt. Wenn Sie z. B. 10 Dienste an einen virtuellen Server mit Lastenausgleich binden und für diesen virtuellen Server einen Schwellenwert von 50% konfigurieren, wechselt er von UP nach DOWN, wenn sechs oder mehr Dienste DOWN sind. Wenn die prozentuale Integrität über den Schwellenwert steigt, kehrt der virtuelle Server in den Status UP zurück.

Sie können auch einen SNMP-Alarm namens ENTITY-STATE aktivieren, wenn Sie von der Citrix ADC Appliance benachrichtigt werden sollen, wenn der prozentuale Zustand gebundener Dienste dazu führt, dass sich ein virtueller Server ändert.

So konfigurieren Sie prozentuale automatische Statusübergänge mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen automatischen Zustandsübergang für einen virtuellen Server zu konfigurieren und die Konfiguration zu überprüfen:

```
set lb vserver <name> -healthThreshold <positive_integer>

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


So konfigurieren Sie den prozentualen automatischen Statusübergang mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Verkehrseinstellungen**aus und legen Sie einen **Integritätsschwellenwert**fest.

So aktivieren Sie den ENTITY-STATE-Alarm mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den ENTITY-STATE SNMP-Alarm zu aktivieren und die Konfiguration zu überprüfen:

```
1 enable snmp alarm ENTITY-STATE
2
3 show snmp alarm
4 <!--NeedCopy-->
```

So aktivieren Sie den ENTITY-STATE-Alarm mit der GUI

1. Navigieren Sie zu **System > SNMP > Alarme**.
2. Wählen Sie **ENTITY-STATE** aus und wählen Sie in der Liste Aktion **Aktivieren**aus.

Integrierte Monitore

October 5, 2021

Die Citrix ADC Appliance enthält verschiedene integrierte Monitore, mit denen Sie Ihre Dienste überwachen können. Diese integrierten Monitore verarbeiten die meisten gängigen Protokolle. Sie bieten Optionen zum Ändern einiger Parameter, z. B. Intervall, Reaktions-Timeout, um Ihre Anforderungen zu erfüllen. Sie können jedoch den Monitornamen und das Protokoll nicht ändern. Weitere Informationen finden Sie unter Monitore ändern. Sie können einen integrierten Monitor auch an einen Dienst binden und ihn vom Service trennen.

> **Hinweis**
>
> Sie können einen benutzerdefinierten Monitor basierend auf einem integrierten Monitor erstellen. Weitere Informationen zum Erstellen benutzerdefinierter Monitore finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

TCP-basierte Anwendungsüberwachung

October 5, 2021

Die Citrix ADC-Appliance verfügt über zwei integrierte Monitore, die TCP-basierte Anwendungen überwachen: `tcp-default` und `ping-default`. Wenn Sie einen Dienst erstellen, wird der entsprechende Standardmonitor automatisch an ihn gebunden, sodass der Dienst sofort verwendet werden kann, wenn er UP ist. Der tcp-Standardmonitor ist an alle TCP-Dienste gebunden. Der Ping-Standardmonitor ist an alle Nicht-TCP-Dienste gebunden.

Sie können Standardmonitore nicht löschen oder ändern. Wenn Sie einen anderen Monitor an einen TCP-Dienst binden, ist der Standardmonitor vom Dienst nicht gebunden. In der folgenden Tabelle sind die Monitortypen sowie die Parameter und Überwachungsprozesse aufgeführt, die jedem Typ zugeordnet sind.

Monitor-Typ	Spezifische Parameter	Prozess
tcp	Nicht zutreffend	Die Citrix ADC-Appliance richtet einen 3-Wege-Handshake mit dem Monitorziel ein und schließt dann die Verbindung. Wenn die Appliance TCP-Datenverkehr zum Ziel beobachtet, sendet sie keine TCP-Überwachungsanfragen. Dies tritt auf, wenn LRTM deaktiviert ist. Standardmäßig ist LRTM auf diesem Monitor deaktiviert.

Monitor-Typ	Spezifische Parameter	Prozess
http	http prequest [“HEAD/”] - HTTP-Anfrage, die an den Dienst gesendet wird. respcode [200] - Eine Reihe von HTTP-Antwortcodes wird vom Dienst erwartet.	Die Citrix ADC-Appliance richtet einen 3-Wege-Handshake mit dem Monitorziel ein. Nachdem die Verbindung hergestellt wurde, sendet die Appliance HTTP-Anforderungen und vergleicht dann den Antwortcode mit dem konfigurierten Satz von Antwortcodes.
tcp-ecv	send [””] - sind die Daten, die an den Dienst gesendet werden. Die maximal zulässige Länge der Zeichenfolge beträgt 512 Bytes. recv [””] - erwartete Antwort des Dienstes. Die maximal zulässige Länge der Zeichenfolge beträgt 128 Byte. Das letzte Zeichen ist die NULL Kündigung.	Die Citrix ADC-Appliance richtet einen 3-Wege-Handshake mit dem Monitorziel ein. Wenn die Verbindung hergestellt wird, sendet die Appliance mit dem Sendeparameter bestimmte Daten an den Dienst und erwartet eine bestimmte Antwort über den Empfangsparameter. Verschiedene Server senden verschiedene Segmentgrößen. Das Muster muss jedoch innerhalb von 16 TCP-Segmenten liegen.

Monitor-Typ	Spezifische Parameter	Prozess
http-ecv	send [””] - HTTP-Daten, die an den Dienst gesendet werden; recv [””] - die erwarteten HTTP-Antwortdaten vom Dienst	Die Citrix ADC-Appliance richtet einen 3-Wege-Handshake mit dem Monitorziel ein. Wenn die Verbindung hergestellt wird, sendet die Appliance den Sendeparameter, um die HTTP-Daten an den Dienst zu senden, und erwartet die HTTP-Antwort, die der Empfangsparameter angibt. (HTTP-Body-Teil ohne HTTP-Header enthalten). Leere Antwortdaten entsprechen jeder Antwort. Die erwarteten Daten können sich irgendwo in den ersten 24 K Bytes des HTTP-Textes der Antwort befinden.
ping	Nicht zutreffend	Die Citrix ADC-Appliance sendet eine ICMP-Echoanforderung an das Ziel des Monitors und erwartet eine ICMP-Echoantwort.

Informationen zum Konfigurieren integrierter Monitore für TCP-basierte Anwendungen finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

So konfigurieren Sie TCP-basierte Monitore mit CLI

Geben Sie den folgenden Befehl ein:

```
add lb monitor <monitorName> <type> -respCode <int[-int]> -httpRequest
    <string> -resptimeout <integer> [<units>] -retries <integer> -
    downTime <integer> [<units>] -action <action>
```



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

Beispiel für TCP-Monitortyp:

```
add lb monitor Exch2010-RPC-AddressBook TCP -LRTM ENABLED -interval 10
    -resptimeout 5 -destPort 59601
<!--NeedCopy-->
```

Beispiel für den HTTP-Monitortyp:

```
add lb monitor Mon_S4B_FE_2 HTTP -respCode 200 -httpRequest "GET /
    Autodiscover/XFrame/XFrame.html" -LRTM ENABLED -retries 10 -secure
    YES
<!--NeedCopy-->
```

Beispiel für den HTTP-ECV-Monitortyp:

```
add lb monitor STM_EXC2016_SSLBridge_MON HTTP-ECV -send "GET /owa/
    healthcheck.htm" -recv "200 OK" -LRTM ENABLED -destPort 443 -secure
    YES
<!--NeedCopy-->
```

Beispiel für PING-Monitortyp:

```
add lb monitor lbmon-localhost-ping PING -LRTM DISABLED -destIP
    127.0.0.1
<!--NeedCopy-->
```

SSL-Dienstüberwachung

October 5, 2021

Die Citrix ADC Appliance verfügt über integrierte sichere Monitore, TCPS und HTTPS. Sie können die sicheren Monitore verwenden, um HTTP- und Nicht-HTTP-Datenverkehr zu überwachen. Um einen sicheren HTTP-Monitor zu konfigurieren, wählen Sie den Monitortyp als HTTP aus, und legen Sie dann das Secure Flag fest. Um einen sicheren TCP-Monitor zu konfigurieren, wählen Sie den Monitortyp als TCP aus, und legen Sie dann das Secure Flag fest. Die sicheren Monitore funktionieren wie folgt:

- **Sichere TCP-Überwachung.** Die Citrix ADC Appliance stellt eine TCP-Verbindung her. Nachdem die Verbindung hergestellt wurde, führt die Appliance einen SSL-Handshake mit dem Server durch. Nachdem der Handshake beendet ist, schließt die Appliance die Verbindung.
- **Sichere HTTP-Überwachung.** Die Citrix ADC Appliance stellt eine TCP-Verbindung her. Nachdem die Verbindung hergestellt wurde, führt die Appliance einen SSL-Handshake mit dem Server durch. Wenn die SSL-Verbindung hergestellt wird, sendet die Appliance HTTP-Anforderungen über den verschlüsselten Kanal und überprüft die Antwortcodes.

In der folgenden Tabelle werden die verfügbaren integrierten Monitore für die Überwachung von SSL-Diensten beschrieben.

Monitortyp	Sonde	Erfolgskriterien (Direkte Bedingung)
TCP	TCP-Verbindung; SSL-Handshake	Erfolgreiche TCP-Verbindung hergestellt und erfolgreicher SSL-Handshake.
HTTP	TCP-Verbindung; SSL-Handshake; Verschlüsselte HTTP-Anfrage	Eine erfolgreiche TCP-Verbindung wird hergestellt, ein erfolgreicher SSL-Handshake wird ausgeführt und der erwartete HTTP-Antwortcode in der HTTP-Antwort des Servers wird verschlüsselt.
TCP-ECV	TCP-Verbindung. SSL-Handshake (Daten, die an einen Server gesendet werden, sind verschlüsselt.)	Eine erfolgreiche TCP-Verbindung wird hergestellt, ein erfolgreicher SSL-Handshake wird ausgeführt und erwartete TCP-Daten werden vom Server empfangen.
HTTP-ECV	TCP-Verbindung; SSL-Handshake (Verschlüsselte HTTP-Anfrage)	Eine erfolgreiche TCP-Verbindung wird hergestellt, ein erfolgreicher SSL-Handshake wird ausgeführt und erwartete HTTP-Daten werden vom Server empfangen.

Beispielkonfiguration für HTTPS-ECV Health Check Monitor

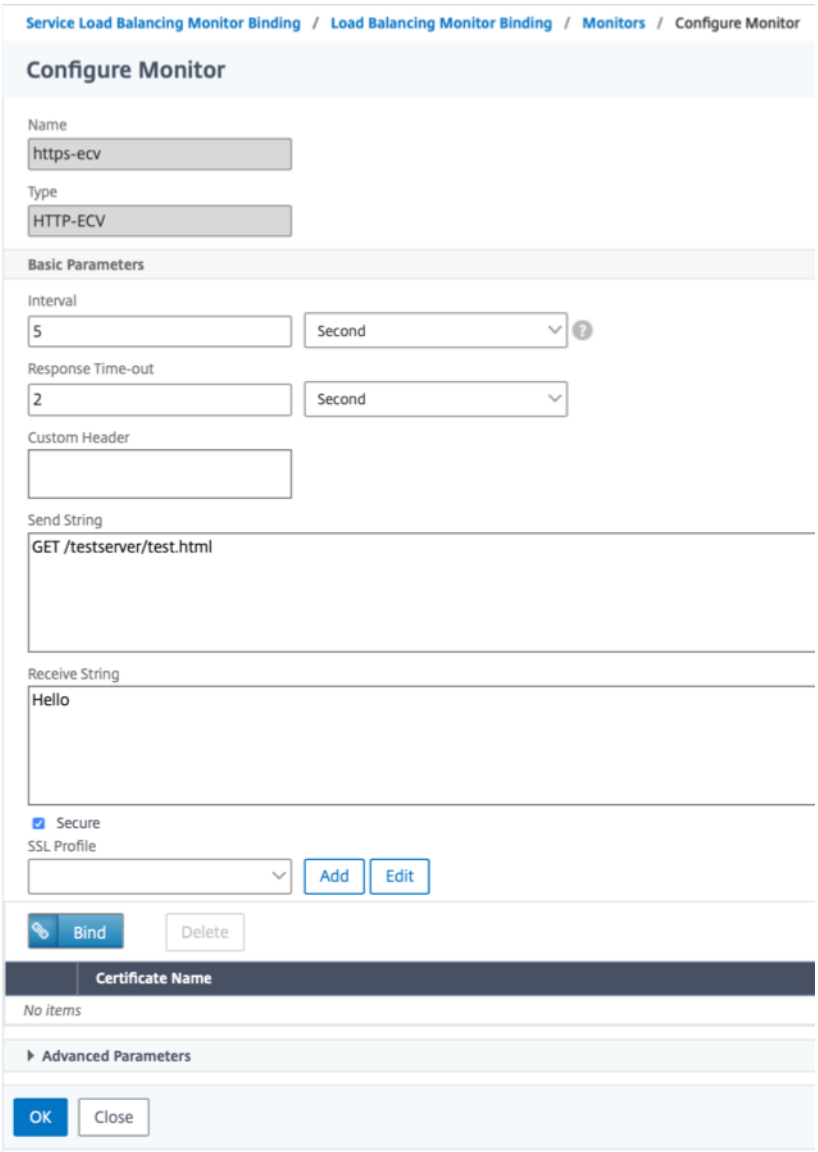
HTTP-Dienste verfügen über vordefinierte Monitore, die zur Extended Content Verification (ECV) fähig sind.
Diese Monitore werden verwendet, wenn eine Validierung über eine erfolgreiche TCP-Verbindung hinaus erforderlich ist. Diese Monitore validieren den Dienst als UP, wenn alle folgenden Kriterien erfüllt sind:

- Eine erfolgreiche TCP-Verbindung.
- Es muss eine bestimmte Art von Anforderung generiert werden.
- Eine bestimmte Nachricht wird als Antwort von der **Empfangszeichenfolge**erwartet.

Für diese Monitore wird eine Anforderungszeichenfolge zusammen mit einer Antwortzeichenfolge konfiguriert. Wenn die vom Citrix ADC Monitor empfangene Antwortzeichenfolge mit der konfigurierten Zeichenfolge übereinstimmt, wird der Dienst als UP markiert.

Binden eines Monitors an einen Dienst mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**, erstellen Sie einen Dienst und geben Sie das Protokoll als **SSL**an. Klicken Sie auf **OK**.
2. Klicken Sie im Bereich **Service to Load Balancing Monitorbindung**, und klicken Sie auf **Bindung hinzufügen** .
3. Wählen Sie den Monitortyp als **HTTPS-ECV** aus und klicken Sie auf **Bearbeiten** .
4. Geben **Sie im Bereich Monitor konfigurieren** auf der Registerkarte **Grundparameter** Werte für die folgenden Parameter ein:
    - **Send String** — Die Zeichenfolge, die der Monitor an den Dienst senden muss.
    - **Empfangszeichenfolge** — Die Zeichenfolge, die der Monitor empfangen muss, um den Dienst als UP zu markieren.



5. Klicken Sie auf **OK**, um die Monitorkonfiguration abzuschließen.
6. Klicken Sie auf **Select**.
7. Klicken Sie auf **Binden**, um den **HTTPS-ECV-Monitor** an den Dienst zu binden.
8. Klicken Sie auf **Schließen**.

Binden eines Monitors an einen Dienst mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind service <servicename> -monitorName https-ecv
2 <!--NeedCopy-->
```


Beispiel:

```
bind services1 -monitorName https-ecv
<!--NeedCopy-->
```

HTTP/2-Dienstüberwachung

October 5, 2021

Die Citrix ADC Appliance unterstützt HTTP/2-Monitore zur Überwachung des Integritätsstatus von HTTP/2-Diensten.

Der HTTP/2-Monitor kann auf zwei verschiedene Arten konfiguriert werden. Je nach Datenverkehrstyp können Sie einen HTTP/2-Monitor konfigurieren.

- **HTTP/2 Direkt.** Sie können HTTP/2 Direct für die Überwachung nicht sicherer HTTP/2-Dienste konfigurieren.
- **HTTP/2 SSL.** Sie können HTTP/2 SSL für die Überwachung des sicheren Datenverkehrs über SSL konfigurieren. Aktivieren Sie den Secure Flag-Parameter im HTTP/2, um den SSL-Datenverkehr zu überwachen.

Der http2direct und http2ssl sind die beiden verschiedenen integrierten Monitore, die für das HTTP/2-Protokoll unterstützt werden.

In der folgenden Tabelle sind die Konfigurationstypen und Überwachungsprozesse aufgeführt, die jedem Typ zugeordnet sind.

Typ der Konfiguration	Sonde	Erfolgskriterien
HTTP/2 Direkt	TCP-Verbindung; HTTP2-Verbindungsvorwort & Einstellungsaushandlung; HTTP2-Anfrage	Der HTTP/2-Antwortstatuscode muss mit dem konfigurierten Antwortcode übereinstimmen.

Typ der Konfiguration	Sonde	Erfolgskriterien
HTTP/2 SSL	TCP-Verbindung; SSL-Handshake; HTTP2-Verbindungsvorwort & Einstellungen Negotiation; HTTP2-Anfrage	Der Server muss immer ALPN mit dem HTTP/2-Protokoll auswählen und der HTTP/2-Antwortstatuscode muss mit dem konfigurierten Antwortcode übereinstimmen.

Binden Sie den HTTP/2-Monitor über die Befehlszeilenschnittstelle an einen Dienst

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `bind service <servicename> -monitorName <name>`
- `bind service <servicename> -monitorName <name>`

Beispiel:

- `bind service s1 -monitorName http2direct`
- `bind service s2 -monitorName http2ssl`

Überwachung des Proxy-Protokolldienstes

October 5, 2021

Die Citrix ADC Appliance mit einem Proxy-Protokoll unterstützt die Monitorprüfung. Die Monitorprüfung stellt sicher, dass der Back-End-Server auch das Proxy-Protokoll unterstützt. Die Citrix ADC Appliance verfügt über vier integrierte Monitortypen für HTTP- oder TCP-bezogene Dienste: HTTP, HTTPS, HTTP-ECV und TCP-ECV.

In der folgenden Tabelle sind die Monitortypen sowie die Parameter und Überwachungsprozesse aufgeführt, die jedem Typ zugeordnet sind.

Typ der Konfiguration	Sonde	Erfolgskriterien
HTTP	`httprequest` [“HEAD/”] - HTTP-Anfrage, die an den Dienst gesendet wird. `respcode` [200] - Eine Reihe von HTTP-Antwortcodes wird vom Dienst erwartet.	Die Citrix ADC Appliance richtet einen 3-Wege-Handshake mit dem Monitorziel ein. Nachdem die Verbindung hergestellt wurde, sendet die Appliance HTTP-Anforderungen und vergleicht dann den Antwortcode mit dem konfigurierten Satz von Antwortcodes.
HTTPS	`httprequest` [“HEAD/”] - HTTPS-Anfrage, die an den Dienst gesendet wird. `respcode` [200] - Eine Reihe von HTTPS-Antwortcodes wird vom Dienst erwartet.	Die Citrix ADC Appliance richtet einen 3-Wege-Handshake mit dem Monitorziel ein. Nachdem die Verbindung hergestellt wurde, sendet die Appliance HTTPS-Anfragen und vergleicht dann den Antwortcode mit dem konfigurierten Satz von Antwortcodes.

Typ der Konfiguration	Sonde	Erfolgskriterien
HTTP-ECV	send [””] - HTTP-Daten, die an den Dienst gesendet werden. Empfangen [””] - die erwarteten HTTP-Antwortdaten vom Dienst	Die Citrix ADC Appliance richtet einen 3-Wege-Handshake mit dem Monitorziel ein. Wenn die Verbindung hergestellt wird, verwendet die Appliance den senden-Parameter, um die HTTP-Daten an den Dienst zu senden, und erwartet die vom empfangenden Parameter HTTP-Antwort. (HTTP-Body-Teil ohne einschließlich HTTP-Header). Leere Antwortdaten entsprechen jeder Antwort. Die erwarteten Daten können sich irgendwo in den ersten 24 K Bytes des HTTP-Textes der Antwort befinden.
TCP-ECV	send[””]- sind die Daten, die an den Dienst gesendet werden. Die maximal zulässige Länge der Zeichenfolge beträgt 512 K Bytes. erhalten [””] - die erwartete Antwort vom Dienst. Die maximal zulässige Länge der Zeichenfolge beträgt 128 KB Byte.	Die Citrix ADC Appliance richtet einen 3-Wege-Handshake mit dem Monitorziel ein. Wenn die Verbindung hergestellt wird, verwendet die Appliance den Parameter send, um bestimmte Daten an den Dienst zu senden und erwartet eine spezifische Antwort über den Empfangsparameter. Verschiedene Server senden unterschiedliche Segmentgrößen. Das Muster muss jedoch innerhalb von 16 TCP-Segmenten liegen.

Sie können den Proxy-Protokollmonitor mit konfigurieren `netprofile`.

Konfigurieren Sie den Proxy-Protokollmonitor mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

1. Netzprofil mit aktiviertem Proxy-Protokoll hinzufügen

   ```
   add netprofile <name> -proxyProtocol ( ENABLED | DISABLED )
   ```

Beispiel:

```
1 add netprofile profile1 - proxyProtocol ENABLED
```

1. Binden Sie das Netzprofil an einen Dienst.

   ```
   set service <name> -netprofile <netprofile-name>
   ```

Beispiel:

```
1 set service S1 - netprofile profile1
```

> **Hinweis:**
>
> Sie können den vorherigen Befehl ausführen, wenn Sie möchten, dass netprofile an einen Dienst gebunden werden soll.

1. Binden Sie das Netzprofil an einen Monitor.

   ```
   set lb monitor <monitor-name> <type> -netprofile <netprofile-name>
   ```

Beispiel:

```
1 set lb monitor http1 HTTPS - netprofile profile1
```

> **Hinweis:**
>
> - Sie können den vorherigen Befehl ausführen, wenn das Netzprofil an einen Monitor gebunden sein soll.
> - Sie können einen Monitortyp Ihrer Wahl auswählen. Es kann HTTP, HTTPS, TCP-ECV oder HTTP-ECV sein.
>
> **Wichtig**
>
> - In einem allgemeinen Fall wird das an einen Dienst gebundene Netzprofil (Proxy-Protokoll

> aktiviert) berücksichtigt.
> - Wenn das Nettoprofil sowohl an den Monitor als auch an den Dienst gebunden ist, wird das an die Überwachung gebundene Netzprofil berücksichtigt. Das an den Dienst gebundene Netzprofil wird ignoriert.

FTP-Dienstüberwachung

October 5, 2021

Um FTP-Dienste zu überwachen, öffnet die Citrix ADC Appliance zwei Verbindungen zum FTP-Server. Es stellt zunächst eine Verbindung mit dem Kontrollport her, der verwendet wird, um Befehle zwischen einem Client und einem FTP-Server zu übertragen. Nachdem die erwartete Antwort empfangen wurde, stellt sie eine Verbindung mit dem Datenport her, der verwendet wird, um Dateien zwischen einem Client und einem FTP-Server zu übertragen. Nur wenn der FTP-Server wie erwartet reagiert, wird er auf beiden Verbindungen als UP markiert.

Hinweis: Monitorsonden stammen von der NSIP-Adresse.

Die Citrix ADC Appliance verfügt über zwei integrierte Monitore für FTP-Dienste: den FTP-Monitor und den FTP-EXTENDED-Monitor. Der FTP-EXTENDED Monitor ist ein skriptfähiger Monitor. Es verwendet das Skript nsftp.pl. Das FTP-EXTENDED-Monitorskript wurde erweitert, um sichere Prüfpunkte an FTP-Dienste zu senden. Sie können einen Monitor vom Typ FTP-EXTENDED erstellen. Das Skript nsftp.pl wird automatisch aus dem Standardverzeichnis übernommen.

So senden Sie sichere FTP-Sonden mit der CLI an FTP-Dienste

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb monitor <monitorName> <type> -username <string> -password <
   string> -filename <filename>
<!--NeedCopy-->
```

Beispiel

```
add monitor mon1 FTP-EXTENDED -username root -password freebsd -
   filename fsdf
<!--NeedCopy-->
```


So senden Sie mit der GUI sichere FTP-Sonden an FTP-Dienste

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Monitore**.
2. Geben Sie den Monitortyp als **FTP-EXTENDED** an, und legen Sie die Parameter fest.
3. Geben Sie unter **Spezielle Parameter**einen **Dateinamen**, einen **Benutzernamen**und **ein Kennwort**an.

Informationen zum Konfigurieren integrierter Monitore zur Überprüfung des Status von FTP-Diensten finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

Sichere Überwachung von Servern mit SFTP

December 7, 2021

Ein Benutzerskript 'nssftp.pl' wird hinzugefügt, um die SFTP-Überwachung (SSH File Transfer Protocol) zu unterstützen. Sie ist in der aktuellen Liste der integrierten Citrix ADC Benutzermonitore verfügbar und befindet sich im Verzeichnis /netscaler/monitors. Der SFTP-Monitor verwendet den angegebenen Benutzernamen und das angegebene Kennwort, um zu prüfen, ob die Datei auf dem Server vorhanden ist.

So konfigurieren Sie die sichere Überwachung mithilfe von SFTP mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb monitor <monitorName> <type> -scriptName <string> -scriptArgs <
     string> -secure ( YES | NO )
2 <!--NeedCopy-->
```

Beispiel:

```
1 add monitor SFTP_MON USER -scriptname nssftp.pl -scriptargs "file=
     example.txt;user=sam;password=sam_passwd"
2 <!--NeedCopy-->
```

So konfigurieren Sie die sichere Überwachung mithilfe von SFTP mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Monitore** und geben Sie unter **Typ USER** an.

2. Wählen Sie unter **Spezielle Parameter**unter **Skriptname**die Option nssftp.pl aus.
3. Geben Sie die **Skriptargumente**an.

Festlegen von SSL-Parametern auf einem sicheren Monitor

October 5, 2021

> **Wichtig**
>
> Diese Funktion wird nur bei den neuen Standardprofilen unterstützt. Weitere Informationen zu diesen Profilen finden Sie unter Überblick über die Infrastruktur der erweiterten SSL-Profile.

Ein Monitor erbt entweder die globalen Einstellungen oder die Einstellungen des Dienstes, an den er gebunden ist. Wenn ein Monitor an einen Nicht-SSL- oder Nicht-SSL_TCP-Dienst gebunden ist, z. B. SSL_BRIDGE, können Sie ihn nicht mit SSL-Einstellungen wie der Protokollversion oder den zu verwendenden Verschlüsselungen konfigurieren. Wenn Ihre Bereitstellung eine SSL-basierte Überwachung der Back-End-Server erfordert, ist die Überwachung daher unwirksam.

Sie können mehr Kontrolle über die SSL-basierte Überwachung von Back-End-Servern haben, indem Sie ein SSL-Profil an einen Monitor binden. Ein SSL-Profil enthält SSL-Parameter, Verschlüsselungsbindungen und ECC-Bindungen. Beispielsweise können Sie Serverauthentifizierung, Verschlüsselung und Protokollversion in einem SSL-Profil festlegen und das Profil an einen Monitor binden. Um die Serverauthentifizierung durchzuführen, müssen Sie auch ein CA-Zertifikat an einen Monitor binden. Um die Clientauthentifizierung durchzuführen, müssen Sie ein Clientzertifikat an den Monitor binden. Neue Parameter für den Befehl bind lb monitor ermöglichen dies.

> **Hinweis:**
>
> Die SSL-Einstellungen werden nur wirksam, wenn Sie einen sicheren Monitor hinzufügen. Außerdem muss der SSL-Profiltyp **BackEnd**sein.

Monitortypen, die SSL-Profile unterstützen

SSL-Profile können an folgende Monitortypen gebunden werden:

- HTTP
- HTTP-ECV
- TCP
- TCP-ECV
- HTTP-INLINE

So geben Sie beim Hinzufügen eines Monitors mithilfe der Befehlszeile ein SSL-Profil an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb monitor <monitorName> <type> -secure  YES   -sslprofile <string>

set lb monitor <monitorName> <type> -secure YES -sslprofile <string>
<!--NeedCopy-->
```

Beispiel:

```
add ssl profile prof1 -sslProfileType  BackEnd

add lb monitor mon1 HTTP -secure  YES -sslprofile prof1
<!--NeedCopy-->
```

So binden Sie ein Zertifikatschlüsselpaar mit der Befehlszeile an einen Monitor

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind monitor  <monitor name> -certkeyName <string>  [(-CA  [-crlCheck (
    Mandatory | Optional ) | -ocspCheck ( Mandatory | Optional )]
<!--NeedCopy-->
```

SIP-Service-Überwachung

October 5, 2021

Ein Citrix ADC verfügt über zwei integrierte Monitore, mit denen Sie SIP-Dienste überwachen können: die **SIP-UDP-** und **SIP-TCP-Monitore** . Ein SIP-Monitor überprüft regelmäßig den SIP-Dienst, an den der SIP-Monitor gebunden ist, indem er SIP-Anforderungsmethoden an den SIP-Dienst sendet. Wenn der SIP-Dienst mit einem Antwortcode antwortet, markiert der Monitor den Dienst als UP. Wenn der SIP-Dienst nicht antwortet oder falsch reagiert, wird er als DOWN markiert.

Parameter	Gibt an
sipURI	SIP-Adressierungsschema des SIP-Servers.

Parameter	Gibt an
sipmethod	Typ der SIP-Anforderung, die zum Testen des SIP-Dienstes verwendet wird. Geben Sie eine der folgenden Methoden an: INVITE, OPTION (Standardeinstellung), REGISTER
respcode	SIP-Antwortcode, mit dem der SIP-Dienst die Prüfungsanforderung antwortet. Standard: 200.

RADIUS-Dienstüberwachung

October 5, 2021

Der RADIUS-Monitor der Citrix ADC Appliance überprüft regelmäßig den Status des RADIUS-Diensts, an den er gebunden ist, indem er eine Authentifizierungsanforderung an den Dienst sendet. Der RADIUS-Server authentifiziert den RADIUS-Monitor und sendet eine Antwort. Standardmäßig erwartet der Monitor, dass er vom RADIUS-Server den Antwortcode 2, die standardmäßige Access-Accept-Antwort, erhält. Solange der Monitor die entsprechende Antwort erhält, markiert er den Dienst UP.

Hinweis: Der RADIUS-Monitor unterstützt nur die PAP-Authentifizierung.

- Wenn der Client erfolgreich authentifiziert wurde, sendet der RADIUS-Server eine Access-Accept-Antwort. Der Standardantwortcode für Access-Accept-Accept ist 2, und dies ist der Code, den die Appliance verwendet.
- Wenn sich der Client nicht erfolgreich authentifizieren kann (z. B. wenn der Benutzername, das Kennwort oder der geheime Schlüssel nicht übereinstimmt), sendet der RADIUS-Server eine Access-Reject-Antwort. Der standardmäßige Antwortcode für Zugriffsverweigerung ist 3, und dies ist der Code, den die Appliance verwendet.

Parameter	Gibt an
userName	Benutzername auf dem RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3-Server. Dieser Benutzername wird im Prüfpunkt verwendet.
Kennwort	Kennwort für die Überwachung von RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/LDAP-Servern.

Parameter	Gibt an
radKey	Shared Secret Key Wert, den der RADIUS-Server während der Clientauthentifizierung verwendet.
radNASid	NAS-ID, die in der Nutzlast gekapselt ist, wenn eine Zugriffsanforderung gestellt wird.
radNASip	Die IP-Adresse, die in der Nutzlast gekapselt ist, wenn eine Zugriffsanforderung gestellt wird. Wenn RadNASip nicht konfiguriert ist, sendet die Citrix ADC Appliance die zugeordnete IP-Adresse (MIP) als NAS-IP-Adresse an den RADIUS-Server.

Um einen RADIUS-Dienst zu überwachen, müssen Sie den RADIUS-Server, an den er gebunden ist, wie folgt konfigurieren:

1. Fügen Sie den Benutzernamen und das Kennwort des Clients hinzu, den der Monitor zur Authentifizierung verwendet, in die RADIUS-Authentifizierungsdatenbank.
2. Fügen Sie die IP-Adresse und den geheimen Schlüssel des Clients zur entsprechenden RADIUS-Datenbank hinzu.
3. Fügen Sie die IP-Adressen hinzu, die die Appliance zum Senden von RADIUS-Paketen an die RADIUS-Datenbank verwendet. Wenn die Citrix ADC Appliance mehr als eine zugeordnete IP-Adresse hat oder wenn eine Subnetz-IP-Adresse (SNIP) verwendet wird, müssen Sie für alle IP-Adressen denselben geheimen Schlüssel hinzufügen.

   Achtung: Wenn die von der Appliance verwendete IP-Adresse nicht zur RADIUS-Datenbank hinzugefügt wird, verwirft der RADIUS-Server alle Pakete.

Informationen zum Konfigurieren integrierter Monitore zur Überprüfung des Status des RADIUS-Servers finden Sie unter Konfigurieren von Monitoren in einem Lastenausgleichs-Setup.

Überwachen der Abrechnungsinformationen von einem RADIUS-Server

October 5, 2021

Sie können einen Monitor, der als *RADIUS-Buchhaltungsmonitor* bezeichnet wird, konfigurieren, um festzustellen, ob der für Authentifizierung, Autorisierung und Accounting (Citrix ADC AAA) verwendete

RADIUS-Server erwartungsgemäß Buchhaltungsinformationen liefert. Der Monitor ist vom Typ RADIUS_ACCOUNTING. Der Prüfpunkt wird durch ein Perl-Skript namens nsbmradius.pl generiert, das sich im Verzeichnis /nsconfig/monitors/ befindet. Das Skript sendet aufeinanderfolgende Abrechnungsanforderungsprüfungen an den RADIUS-Server. Der Prüfpunkt wird nur dann als erfolgreich angesehen, wenn der RADIUS-Buchhaltungsserver mit einem Paket antwortet, dessen Codefeld auf 5 gesetzt ist, was gemäß RFC 2866 ein Accounting-Response-Paket anzeigt.

Wenn Sie einen RADIUS-Kontoführungsmonitor konfigurieren, müssen Sie einen geheimen Schlüssel angeben. Sie können optionale Parameter angeben, die jeweils ein RADIUS-Attribut darstellen, z. B. Informationen zu diesen Attributen finden Sie unter RFC 2865, Remote Authentication Dial In User Service (RADIUS) und RFC 2866, RADIUS Accounting.

So konfigurieren Sie einen RADIUS-Kontoführungsmonitor mit der Befehlszeilenschnittstelle

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

```
add lb monitor <monitorName> RADIUS_ACCOUNTING [-userName <string>] {
 -password  }
  {
 -radKey  }
  [-radNASip <ip_addr>] [-radAccountType <positive_integer>] [-
     radFramedIP <ip_addr>] [-radAPN <string>] [-radMSISDN <string>] [-
     radAccountSession <string>]

show lb monitor <monitorName>
<!--NeedCopy-->
```

Beispiel

```
add lb monitor radAccntMon RADIUS_ACCOUNTING -radKey "8d#>9jr4rV)L7%a2-
   zW13sM"
<!--NeedCopy-->
```

DNS- und DNS-TCP-Dienstüberwachung

October 5, 2021

Die Citrix ADC Appliance verfügt über zwei integrierte Monitore, mit denen DNS-Dienste überwacht werden können: DNS und DNS-TCP. Wenn sie an einen Dienst gebunden sind, überprüft jeder Monitor regelmäßig den Status dieses DNS-Dienstes, indem er eine DNS-Abfrage an ihn sendet. Die Abfrage wird in eine IPv4- oder IPv6-Adresse aufgelöst. Diese IP-Adresse wird dann mit der Liste der von Ihnen konfigurierten Test-IP-Adressen überprüft. Die Liste kann bis zu fünf IP-Adressen enthalten. Wenn die aufgelöste IP-Adresse mit mindestens einer IP-Adresse in der Liste übereinstimmt, wird der DNS-Dienst als oben markiert. Wenn die aufgelöste IP keine IP-Adressen in der Liste übereinstimmt, wird der DNS-Dienst als unten markiert.

Parameter	Beschreibung
Abfrage	Die DNS-Abfrage (Domänenname), die an den überwachten DNS-Dienst gesendet wird. Standardwert: "\ 007" Wenn die DNS-Abfrage erfolgreich ist, wird der Dienst als UP gekennzeichnet. Ansonsten ist es als DOWN gekennzeichnet. Wenn die DNS-Abfrage erfolgreich ist, wird der Dienst bei einem Rückwärtsmonitor als DOWN gekennzeichnet. Ansonsten ist es als UP gekennzeichnet. Wenn keine Antwort empfangen wird, wird der Dienst als DOWN markiert.
QueryType	Der Typ der gesendeten DNS-Abfrage. Mögliche Werte: Adresse, Zone.
`IPAddress`	Liste der IP-Adressen, die gegen die Antwort auf die DNS-Überwachungsprobe überprüft werden.
IPv6	Aktivieren Sie dieses Kontrollkästchen, wenn die IP-Adresse das IPv6-Format verwendet.

Informationen zum Konfigurieren der integrierten DNS- oder DNS-TCP-Monitore finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

LDAP-Dienstüberwachung

October 5, 2021

Die Citrix ADC Appliance verfügt über einen integrierten Monitor, mit dem LDAP-Dienste überwacht

werden können: den LDAP-Monitor. Er überprüft regelmäßig den LDAP-Dienst, an den er gebunden ist, indem er eine Suchanfrage authentifiziert und an ihn sendet. Wenn die Suche erfolgreich ist, wird der Dienst als UP markiert. Wenn der LDAP-Server den Eintrag nicht findet, wird eine Fehlermeldung an den LDAP-Monitor gesendet, und der Dienst wird mit DOWN gekennzeichnet.

Konfigurieren Sie den LDAP-Monitor so, dass er die Suche definiert, die er beim Senden einer Abfrage durchführen muss. Sie können den Basis-DN-Parameter verwenden, um einen Speicherort in der Verzeichnishierarchie anzugeben, an dem der LDAP-Server die Testabfrage starten muss. Sie können den Parameter Attribut verwenden, um ein Attribut der Zielentität anzugeben.

Hinweis: Monitorsonden stammen von der NSIP-Adresse.

Parameter	Gibt an
BasedN	Basisname für den LDAP-Monitor, von dem aus die LDAP-Suche gestartet werden muss. Wenn der LDAP-Server lokal läuft, ist der Standardwert von base dc=`netscaler`, dc=com.
BindDN	BDN-Name für den LDAP-Monitor.
Filter	Filter für den LDAP-Monitor. Verwenden Sie den Filterparameter in einer Abfrage, um die Anzahl der Ergebnisse zu begrenzen. Wenn Sie diesen Parameter nicht in der Abfrage angeben, gilt der Filter für die gesamte Objektklasse, was eine kostspielige Operation sein kann, z. B. eine hohe CPU-Auslastung.
Kennwort	Kennwort, das bei der Überwachung von LDAP-Servern verwendet wird.
Attribut	Attribut für den LDAP-Monitor.

Informationen zum Konfigurieren des integrierten LDAP-Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

MySQL Dienstüberwachung

October 5, 2021

Die Citrix ADC Appliance verfügt über einen integrierten Monitor, mit dem MySQL Dienste überwacht

werden können: den MySQL-Monitor. Er überprüft regelmäßig den MySQL Dienst, an den er gebunden ist, indem er eine Suchanfrage sendet. Wenn die Suche erfolgreich ist, wird der Dienst als UP markiert. Wenn der MySQL -Server nicht antwortet oder die Suche fehlschlägt, wird eine Fehlermeldung an den MySQL Monitor gesendet und der Dienst wird als DOWN markiert.

Hinweis: Monitorsonden stammen von der NSIP-Adresse.

Parameter	Gibt an
Datenbank	Datenbank, die für den MySQL Monitor verwendet wird.
sqlQuery	SQL-Abfrage, die für den MySQL Monitor verwendet wird.

Informationen zum Konfigurieren eines integrierten MySQL-Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

So konfigurieren Sie MySQL-Monitore mit CLI

Geben Sie den folgenden Befehl ein:

```
1 add lb monitor <monitorName> <type> -scriptName <string> -scriptArgs <
     string>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add lb monitor mysql1 USER -scriptName nsmysql.pl -scriptArgs ”database
     =cloud;user=cloud;password=password;query=show tables from cloud”
2 <!--NeedCopy-->
```

SNMP-Dienstüberwachung

October 5, 2021

Die Citrix ADC Appliance verfügt über einen integrierten Monitor, mit dem SMNP-Dienste überwacht werden können: den SNMP-Monitor. Er überprüft regelmäßig den SNMP-Agent auf dem Dienst, an

den er gebunden ist, indem er eine Abfrage für die Enterprise Identification ID (OID) sendet, die Sie für die Überwachung konfigurieren. Wenn die Abfrage erfolgreich ist, wird der Dienst als UP markiert. Wenn der SNMP-Dienst die von Ihnen angegebene OID findet, ist die Abfrage erfolgreich und der SNMP-Monitor markiert den Dienst UP. Wenn die OID nicht gefunden wird, schlägt die Abfrage fehl und der SNMP-Monitor markiert Dienst DOWN.

Hinweis: Monitorsonden stammen von der NSIP-Adresse.

Parameter	Gibt an
SNMPOID	OID, die für den SNMP-Monitor verwendet wird.
snmpCommunity	Community, die für den SNMP-Monitor verwendet wird.
snmpThreshold	Schwellenwert, der für den SNMP-Monitor verwendet wird.
snmpVersion	SNMP-Version, die für die Lastüberwachung verwendet wird. Mögliche Werte: V1, V2.

Informationen zum Konfigurieren des integrierten SNMP-Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

NNTP-Dienstüberwachung

October 5, 2021

Die Citrix ADC Appliance verfügt über einen integrierten Monitor, der zur Überwachung von NNTP-Diensten verwendet werden kann: den NNTP-Monitor. Er überprüft regelmäßig den NNTP-Dienst, an den er gebunden ist, indem er eine Verbindung zum Dienst herstellt und überprüft, ob die von Ihnen angegebene Newsgroup vorhanden ist. Wenn die Newsgroup vorhanden ist, ist die Suche erfolgreich und der Dienst wird als UP gekennzeichnet. Wenn der NNTP-Dienst nicht antwortet oder die Suche fehlschlägt, wird der Dienst mit DOWN gekennzeichnet.

Hinweis: Monitorsonden stammen von der NSIP-Adresse.

Der NNTP-Monitor kann optional so konfiguriert werden, dass auch eine Testnachricht an die Newsgroup gesendet wird.

Parameter	Gibt an
`userName`	Benutzername auf dem RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3-Server. Dieser Benutzername wird im Prüfpunkt verwendet.
Kennwort	Kennwort für die Überwachung von RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/LDAP-Servern.
Gruppe	Gruppenname, der für den NNTP-Monitor abgefragt werden soll.

Informationen zum Konfigurieren des integrierten NNTP-Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

POP3-Dienstüberwachung

October 5, 2021

Die Citrix ADC Appliance verfügt über einen integrierten Monitor, mit dem POP3-Dienste überwacht werden können: den POP3-Monitor. Er überprüft regelmäßig den POP3-Dienst, an den er gebunden ist, indem er eine Verbindung mit einem POP3-Server öffnet. Wenn der POP3-Server innerhalb des konfigurierten Zeitraums mit den richtigen Antwortcodes antwortet, markiert er den Dienst UP. Wenn der POP3-Dienst nicht antwortet oder falsch reagiert, markiert er den Dienst DOWN.

Hinweis: Monitorsonden stammen von der NSIP-Adresse.

Parameter	Gibt an
userName	Benutzername POP3-Server. Dieser Benutzername wird im Prüfpunkt verwendet.
Kennwort	Kennwort, das bei der Überwachung von POP3-Servern verwendet wird.
scriptName	Der Pfad und der Name des auszuführenden Skripts.
dispatcherIP	Die IP-Adresse des Dispatchers, an den der Prüfpunkt gesendet wird.

Parameter	Gibt an
dispatcherPort	Der Port des Dispatchers, an den der Prüfpunkt gesendet wird.

Informationen zum Konfigurieren des integrierten POP3-Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

So konfigurieren Sie POP3-Monitore mit CLI

Geben Sie den folgenden Befehl ein:

```
add lb monitor <monitorName> <type> -scriptName <string> -scriptArgs <
    string>
<!--NeedCopy-->
```

Beispiel:

```
add lb monitor pop31 USER -scriptName nspop3.pl -scriptArgs "user=
    test@lbmon1.net;password=Freebsd123"

<!--NeedCopy-->
```

SMTP-Dienstüberwachung

October 5, 2021

Die Citrix ADC Appliance verfügt über einen integrierten Monitor, der zur Überwachung von SMTP-Diensten verwendet werden kann: den SMTP-Monitor. Der Monitor überprüft den SMTP-Dienst, an den er gebunden ist, indem er eine Verbindung mit ihm öffnet und eine Reihe von Handshakes durchführt, um sicherzustellen, dass der Server ordnungsgemäß funktioniert. Wenn der SMTP-Dienst die Handshakes ordnungsgemäß abgeschlossen hat, markiert der Monitor den Dienst UP. Andernfalls, wenn der SMTP-Dienst nicht reagiert oder falsch reagiert, markiert er den Dienst DOWN.

Hinweis: Monitorsonden stammen von der NSIP-Adresse.

Parameter	Gibt an
scriptName	Der Pfad und der Name des auszuführenden Skripts.
dispatcherIP	Die IP-Adresse des Dispatchers, an den der Prüfpunkt gesendet wird.
dispatcherPort	Der Port des Dispatchers, an den der Prüfpunkt gesendet wird.

Informationen zum Konfigurieren des integrierten SMTP-Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

RTSP-Dienstüberwachung

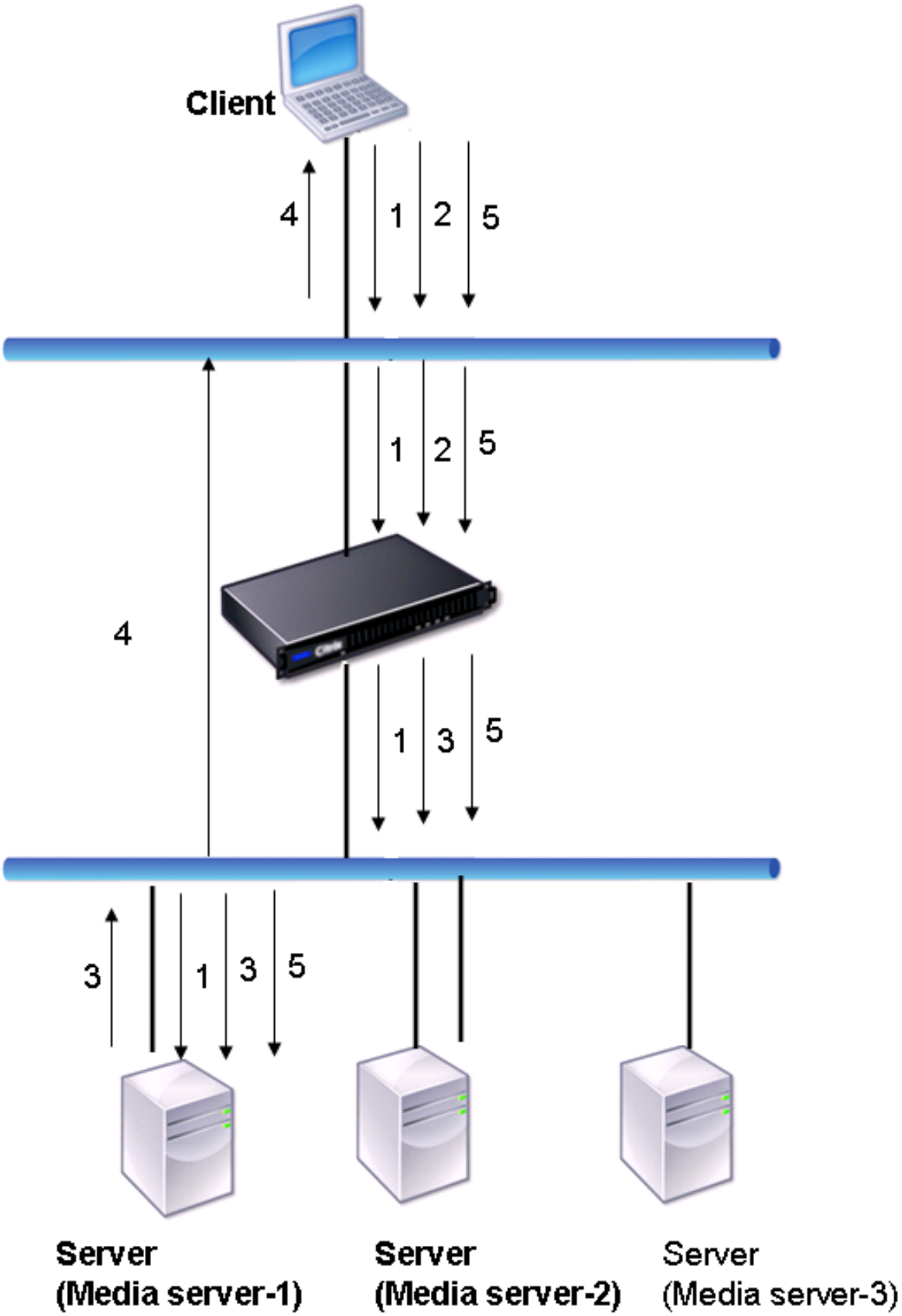
October 5, 2021

Die Citrix ADC Appliance verfügt über einen integrierten Monitor, mit dem RTSP-Dienste überwacht werden können: den RTSP-Monitor. Er überprüft regelmäßig den RTSP-Dienst, an den er gebunden ist, indem er eine Verbindung mit dem Lastausgleichsserver öffnet. Die Art der Verbindung, die sie öffnet, und die Antwort, die sie erwartet, unterscheiden sich je nach Netzwerkkonfiguration. Wenn der RTSP-Dienst innerhalb des konfigurierten Zeitraums wie erwartet reagiert, markiert er den Dienst UP. Wenn der Dienst nicht antwortet oder falsch reagiert, markiert er den Dienst DOWN.

Die Citrix ADC Appliance kann für den Lastausgleich von RTSP-Servern mit zwei Topologien konfiguriert werden: NAT-Off und NAT-On. RTSP-Server senden ihre Antworten direkt an den Client unter Umgehung der Appliance. Die Appliance muss so konfiguriert sein, dass RTSP-Dienste unterschiedlich überwacht werden, je nachdem, welche Topologie Ihr Netzwerk verwendet. Die Appliance kann sowohl im Inline-Modus als auch im Nicht-Inline-Modus im NAT-Off- als auch im NAT-on-Modus bereitgestellt werden.

Im NAT-Off-Modus arbeitet die Appliance als Router: Sie empfängt RTSP-Anfragen vom Client und leitet sie an den Dienst weiter, den sie mit der konfigurierten Lastausgleichsmethode auswählt. Wenn Ihren RTSP-Servern mit Lastausgleich öffentlich zugänglichen FQDNs in DNS zugewiesen werden, senden die Server mit Lastausgleich ihre Antworten direkt an den Client unter Umgehung der Appliance. Die folgende Abbildung veranschaulicht diese Konfiguration.

Abbildung 1. RTSP im Nat-Off-Modus



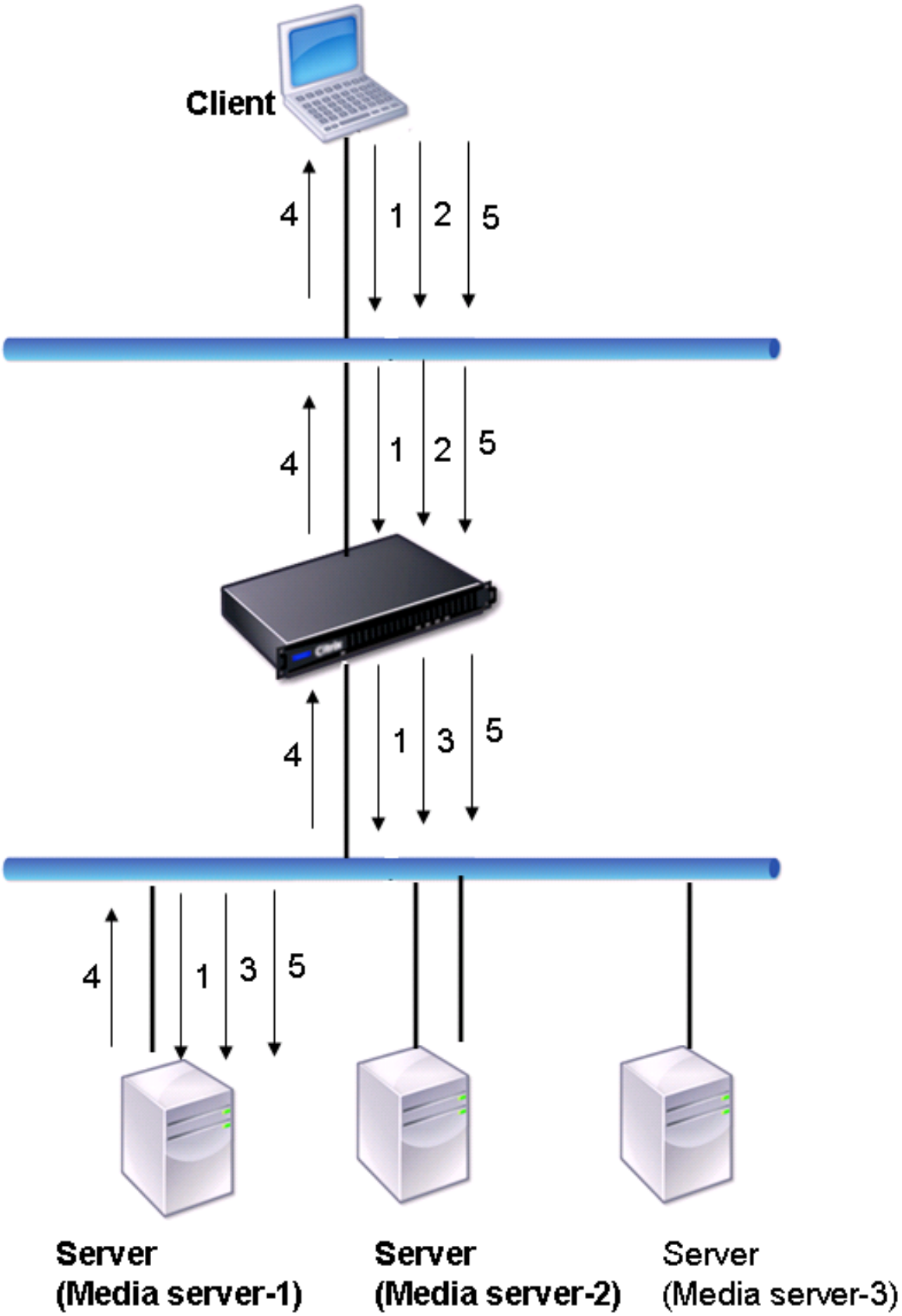
Der Ablauf von Anfragen und Antworten in diesem Szenario ist wie folgt:

1. Der Client sendet eine DESCRIBE Anforderung an die Appliance. Die Appliance verwendet die konfigurierte Lastausgleichsmethode, um einen Dienst auszuwählen, und leitet die Anforderung an Media Server-1 weiter.
2. Der Client sendet eine SETUP-Anforderung an die Appliance. Wenn die RTSP-Sitzungs-ID in der DESCRIBE-Anforderung ausgetauscht wird, leitet die Appliance mithilfe der RTSPSID-Persistenz die Anforderung an Media Server-1 weiter. Wenn die RTSP-Sitzungs-ID in der SETUP-Anforderung ausgetauscht wird, führt die Appliance einen der folgenden Schritte aus:
   - Wenn die RTSP-Anforderung auf dieselbe TCP-Verbindung kommt, leitet sie die Anforderung an Media Server-1 weiter, wobei die Persistenz beibehalten wird.
   - Wenn die Anforderung mit einer anderen TCP-Verbindung eintrifft, verwendet sie die konfigurierte Lastausgleichsmethode, um einen Dienst auszuwählen, und sendet die Anforderung an diesen Dienst, ohne die Persistenz beizubehalten. Dies bedeutet, dass die Anfrage möglicherweise an einen anderen Dienst gesendet wird.
3. Media Server-1 empfängt die SETUP-Anforderung von der Appliance, weist Ressourcen für die Verarbeitung der RTSP-Anforderung zu und sendet die entsprechende Sitzungs-ID an den Client.

   Hinweis: Die Appliance führt NAT nicht aus, um die RTSP-Verbindung zu identifizieren, da die RTSP-Verbindungen sie umgehen.
4. Bei nachfolgenden Anforderungen verwendet der Client dann die Sitzungs-ID, um die Sitzung zu identifizieren und Kontrollmeldungen an den Medienserver zu senden. Media Server-1 führt die angeforderten Aktionen aus, z. B. Wiedergabe, Weiterleitung oder Zurückspulen.

Im NAT-on-Modus empfängt die Appliance RTSP-Anforderungen vom Client und leitet diese Anforderungen mithilfe der konfigurierten Lastausgleichsmethode an den entsprechenden Medienserver weiter. Der Medienserver sendet dann seine Antworten über die Appliance an den Client, wie im folgenden Diagramm dargestellt.

Abbildung 2. RTSP im NAT-on-Modus



Der Ablauf von Anfragen und Antworten in diesem Szenario ist wie folgt:

1. Der Client sendet eine DESCRIBE Anforderung an die Appliance. Die Appliance verwendet die konfigurierte Lastausgleichsmethode, um einen Dienst auszuwählen, und leitet die Anforderung an Media Server-1 weiter.
2. Der Client sendet eine SETUP-Anforderung an die Appliance. Wenn die RTSP-Sitzungs-ID in der DESCRIBE-Anforderung ausgetauscht wird, leitet die Appliance die Anforderung mithilfe der RTSPSID-Persistenz an Media Server-1 weiter. Wenn die RTSP-Sitzungs-ID in der SETUP-Anforderung ausgetauscht wird, führt die Appliance einen der folgenden Schritte aus:
   - Wenn die RTSP-Anforderung auf dieselbe TCP-Verbindung kommt, leitet sie die Anforderung an Media Server-1 weiter, wobei die Persistenz beibehalten wird.
   - Wenn die Anforderung mit einer anderen TCP-Verbindung eintrifft, verwendet sie die konfigurierte Lastausgleichsmethode, um einen Dienst auszuwählen, und sendet die Anforderung an diesen Dienst, ohne die Persistenz beizubehalten. Dies bedeutet, dass die Anfrage möglicherweise an einen anderen Dienst gesendet wird.
3. Media Server-1 empfängt die SETUP-Anforderung von der Appliance, weist Ressourcen für die Verarbeitung der RTSP-Anforderung zu und sendet die entsprechende Sitzungs-ID an den Client.
4. Die Appliance führt NAT aus, um den Client für RTSP-Datenverbindungen zu identifizieren, und die RTSP-Verbindungen werden durch die Appliance geleitet und an den richtigen Client weitergeleitet.
5. Bei nachfolgenden Anforderungen verwendet der Client dann die Sitzungs-ID, um die Sitzung zu identifizieren und Kontrollmeldungen an die Appliance zu senden. Die Appliance verwendet die RTSPSID-Persistenz, um den entsprechenden Dienst zu identifizieren, und leitet die Anforderung an Media Server-1 weiter. Media Server-1 führt die angeforderte Aktion aus, z. B. Wiedergeben, Vorwärts oder Zurückspulen.

Der RTSP-Monitor verwendet das RTSP-Protokoll, um den Status der RTSP-Dienste zu bewerten. Der RTSP-Monitor stellt eine Verbindung zum RTSP Server her und führt eine Folge von Handshakes durch, um sicherzustellen, dass der Server ordnungsgemäß funktioniert.

Parameter	Gibt an
RTSPrequest	Die RTSP-Anforderungszeichenfolge, die an den RTSP-Server gesendet wird (z. B. OPTIONS*). Der Standardwert ist 07. Die Länge der Anforderung darf 163 Zeichen nicht überschreiten.
RespCode	Satz von Antwortcodes, die vom Dienst erwartet werden.

Anweisungen zum Konfigurieren eines RTSP-Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

Überwachung des XML-Brokerdienstes

October 5, 2021

Die Citrix ADC Appliance verfügt über einen integrierten Monitortyp, CITRIX-XML-SERVICE, mit dem Sie Monitore zur Überwachung der XML Broker Services erstellen können. Die XML Broker Services werden von Citrix XenApp verwendet. Der Monitor öffnet eine Verbindung zum Dienst und prüft regelmäßig die XML-Dienste, an die er gebunden ist. Wenn der Server innerhalb des konfigurierten Zeitraums wie erwartet reagiert, markiert der Monitor den Dienst UP. Wenn der Dienst nicht antwortet oder falsch reagiert, markiert der Monitor den Dienst DOWN.

Um einen CITRIX-XML-SERVICE Monitor zu konfigurieren, müssen Sie zusätzlich zur Einstellung der Standardparameter den Anwendungsnamen angeben. Der Anwendungsname ist der Name der Anwendung, die ausgeführt werden muss, um den Status des XML-Brokerdienstes zu überwachen. Die Standardanwendung ist Notepad.

Informationen zum Konfigurieren von Monitoren für XML Broker Services finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

> **Hinweis:**
>
> Der Parameter “Anwendungsname” für den Citrix-XML-Service-Monitor ist für XenApp und Citrix Virtual Desktops Version 7 und höher ungültig. Es wird empfohlen, diesen Parameter nicht in XA/XD 7 zu verwenden. Wenn Sie diesen Parameter konfigurieren, wird dieser Parameter nicht intern verwendet. Die Prüfkriterien unterscheiden sich ab XA/XD 7. Sie können jedoch die Parameter Anwendungsname in Versionen vor XA/XD 7 verwenden.

ARP-Anforderungsüberwachung

October 5, 2021

Die Citrix ADC Appliance verfügt über einen integrierten Monitor, mit dem ARP-Anforderungen überwacht werden können: den ARP-Monitor. Dieser Monitor sendet regelmäßig eine ARP-Anforderung an den Dienst, an den er gebunden ist, und überwacht die erwartete Antwort. Wenn es die erwartete Antwort empfängt, markiert es den Dienst UP. Wenn es keine Antwort oder die falsche Antwort erhält, markiert es den Dienst DOWN.

ARP sucht eine Hardwareadresse für einen Lastausgleichsserver, wenn nur die Netzwerk-Layer-Adresse bekannt ist. ARP ist mit IPv4 kompatibel, um IP-Adressen in Ethernet-MAC-Adressen zu übersetzen. Die ARP-Überwachung ist für IPv6-Netzwerke nicht relevant und wird daher in diesen Netzwerken nicht unterstützt.

Es gibt keine speziellen Parameter für den ARP-Monitor.

Anweisungen zum Konfigurieren eines ARP-Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

Überwachung des XenDesktop Delivery Controller Dienstes

December 7, 2021

In der Desktop-Virtualisierung kann die Citrix ADC Appliance zum Lastenausgleich der Webinterface-Server (WI) und der von der Citrix XenDesktop-Umgebung bereitgestellten XenDesktop Delivery Controller-Server verwendet werden. Die Citrix ADC Appliance bietet einen integrierten Monitor, `CITRIX-XD-DDC` Monitor, der die XenDesktop Delivery Controller-Server überwacht. Zusätzlich zur Integritätsprüfung können Sie auch überprüfen, ob der Prüfpunkt von einem gültigen Benutzer des XenDesktop Delivery Controller -Servers gesendet wird.

Der Monitor sendet einen Prüfpunkt in Form einer XML-Nachricht an den XenDesktop Delivery Controller er-Server. Wenn der Server auf den Prüfpunkt mit der Identität der Serverfarm antwortet, wird der Prüfpunkt als erfolgreich angesehen, und der Serverstatus wird als UP markiert. Wenn die HTTP-Antwort keinen Erfolgscode enthält oder die Identität der Serverfarm in der Antwort nicht vorhanden ist, wird der Prüfpunkt als Fehler angesehen, und der Serverstatus wird als DOWN gekennzeichnet.

Die Option Anmeldeinformationen validieren bestimmt den Prüfpunkt, der vom Monitor an den XenDesktop Delivery Controller -Server gesendet werden soll, d. h., ob nur der Servername angefordert oder die Anmeldeinformationen überprüft werden sollen.

Hinweis: Unabhängig davon, ob die Benutzeranmeldeinformationen (Benutzername, Kennwort und Domäne) auf dem
`CITRIX-XD-DDC` Monitor angegeben sind, validiert der XenDesktop Delivery Controller-Server die Benutzeranmeldeinformationen nur, wenn die Option zum Validieren von Anmeldeinformationen auf dem Monitor aktiviert ist.

Wenn Sie den Assistenten zum Konfigurieren des Lastenausgleichs der XenDesktop-Server verwenden, wird der `CITRIX-XD-DDC` Monitor automatisch erstellt und an die XenDesktop Delivery Controller-Dienste gebunden.

So fügen Sie mit der Befehlszeilenschnittstelle einen XD-DDC-Monitor mit der Option Anmeldeinformationen validieren hinzu

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen XD-DDC-Monitor hinzuzufügen und die Konfiguration zu überprüfen:

```
add lb monitor <monitorName> <monitorType> -userName <userName> -
    password <password> -domain <domain_name> -validateCred YES

show lb monitor <monitorName>
<!--NeedCopy-->
```

Beispiel:

```
 > add lb monitor xdddcmon Citrix-xd-ddc -userName Administrator -
    password E12Dc35450a1 -domain dhop -validateCred YES
 Done
> show lb monitor xdddcmon
1) Name......:xdddcmon Type......:CITRIX-XD-DDC State......: ENABLED

Standard parameters:
Interval......:..5 sec...Retries......:..3
Response timeout......:..2 sec...Down time......:..30 sec
Reverse......:..NO...Transparent......:..NO
Secure......:..NO...LRTM......:..ENABLED
Action......:..Not applicable...Deviation......:..0 sec
Destination IP......:..Bound service
Destination port......:..Bound service
Iptunnel......:..NO
TOS......:..NO...TOS ID......:..0
SNMP Alert Retries......:..0...Success Retries......:..1
Failure Retries......:..0

Special parameters:
User Name..........:"Administrator"
Password...........:** ***
DDC Domain.........: "dhop"
Done
<!--NeedCopy-->
```


So geben Sie die Option Anmeldeinformationen validieren auf einem XD-DDC-Monitor mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb monitor <monitorName> <monitorType> -userName -password -domain
    <domain_name> -validateCred YES
<!--NeedCopy-->
```

Beispiel:

```
 set lb monitor XD_DDC_21.21.21.22_443_mn CITRIX-xd-ddc -userName
    Administrator -password D123S1R2A123 -domain dhop -validateCred YES
Done
<!--NeedCopy-->
```

So konfigurieren Sie einen XD-DDC-Monitor mit der Option Anmeldeinformationen validieren mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**, und erstellen Sie einen Monitor des Typs `Citrix-XD-DDC`.

Überwachung von Citrix StoreFront Stores

October 5, 2021

Sie können einen Benutzermonitor für einen Citrix StoreFront-Store konfigurieren. Der Monitor bestimmt den Status des StoreFront-Speichers, indem er nacheinander den Kontodienst, den Erkennungsdienst und den Authentifizierungsendpunkt untersucht (wenn der Citrix StoreFront Store ein authentifizierter Speicher ist). Wenn einer dieser Dienste nicht auf den Prüfpunkt reagiert, schlägt der Monitor Probe fehl, und der StoreFront -Speicher wird als DOWN markiert. Der Monitor sendet Prüfpunkte an die IP-Adresse und den Port des gebundenen Dienstes. Weitere Informationen finden Sie unter Citrix StoreFront Store Services-API.

Hinweis: Monitorsonden stammen von der NSIP-Adresse. Wenn sich das Subnetz eines StoreFront -Servers jedoch von dem der Appliance unterscheidet, wird die Subnetz-IP (SNIP) -Adresse verwendet.

Ab Version 10.1 Build 120.13 können Sie einen StoreFront Monitor auch an eine Servicegruppe binden. Ein Monitor ist an jedes Mitglied der Dienstgruppe gebunden und Probes werden an die IP-Adresse

und den Port des gebundenen Mitglieds (Dienst) gesendet. Da nun jedes Mitglied einer Dienstgruppe mithilfe der IP-Adresse des Mitglieds überwacht wird, können Sie nun den StoreFront-Monitor verwenden, um StoreFront-Clusterknoten zu überwachen, die als Mitglieder der Dienstgruppe hinzugefügt werden.

In früheren Versionen hat der StoreFront Monitor versucht, anonyme Stores zu authentifizieren. Infolgedessen kann ein Dienst als DOWN markiert werden und Sie können XenApp oder XenDesktop nicht mithilfe der URL des virtuellen Lastausgleichsservers starten.

Ab Build 64.x hat sich die Sondenreihenfolge geändert. Der Monitor bestimmt nun den Status des StoreFront -Speichers, indem er nacheinander den Kontodienst, das Ermittlungsdokument und dann den Authentifizierungsdienst untersucht und die Authentifizierung für anonyme Speicher überspringt.

Der Hostnamenparameter für StoreFront-Monitore ist veraltet. Der sichere Parameter wird nun verwendet, um zu bestimmen, ob HTTP (Standard) oder HTTPS zum Senden von Monitorprüfungen verwendet werden soll.

Um HTTPS zu verwenden, setzen Sie die sichere Option auf Ja.

So erstellen Sie einen StoreFront Monitor mit der Befehlszeilenschnittstelle

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

```
1 add lb monitor <monitorName> STOREFRONT <string> -storeName <string> [-
     storefrontacctservice ( YES | NO )] -secure ( YES | NO )
2
3 show lb monitor <monitorName>
4 <!--NeedCopy-->
```

Beispiel

```
1 add lb monitor storefront_ssl STOREFRONT -storename myStore -
     storefrontacctservice YES -secure YES
2 <!--NeedCopy-->
```

So erstellen Sie einen StoreFront Monitor mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**, und erstellen Sie einen Monitor vom Typ **STOREFRONT**.

> **Hinweis:**
>
> Weitere Informationen zu den StoreFront-Monitoren finden Sie in der StoreFront-Dokumentation.

Benutzerdefinierte Monitore

October 5, 2021

Zusätzlich zu den integrierten Monitoren können Sie benutzerdefinierte Monitore verwenden, um den Status Ihrer Dienste zu überprüfen. Die Citrix ADC Appliance bietet verschiedene Arten von benutzerdefinierten Monitoren, die auf Skripten basieren, die im Citrix ADC-Betriebssystem enthalten sind. Die Skripts können verwendet werden, um den Status der Dienste basierend auf der Belastung des Dienstes oder des an den Dienst gesendeten Netzwerkverkehrs zu bestimmen. Benutzerdefinierte Monitore sind die Inline-Monitore, Benutzermonitore und Lastmonitore.

Mit diesen Monitortypen können Sie die mitgelieferte Funktionalität verwenden oder Ihre eigenen Skripts erstellen und diese Skripts verwenden, um den Status des Dienstes zu bestimmen, an den der Monitor gebunden ist.

Konfigurieren von HTTP-Inline-Monitoren

October 5, 2021

Inline-Monitore analysieren und untersuchen die Antworten der Dienste, an die sie gebunden sind, nur wenn diese Dienste Clientanforderungen empfangen. Der Inline-Monitor ist vom Typ HTTP-INLINE und kann nur mit HTTP- und HTTPS-Diensten konfiguriert werden. Ein Inline-Monitor bestimmt, dass der Dienst, an den er gebunden ist, UP ist, indem er seine Antworten auf die Anforderungen überprüft, die an ihn gesendet werden. Wenn keine Clientanforderungen an den Dienst gesendet werden, überprüft der Inline-Monitor den Dienst mithilfe der konfigurierten URL.

Hinweis: Inline-Monitore können nicht an HTTP oder HTTPS Global Server Load Balancing (GSLB) -Remotedienste oder lokale Dienste gebunden werden, da diese Dienste virtuelle Server und nicht tatsächliche Lastausgleichsserver darstellen.

Inline-Monitore haben einen Timeoutwert und eine Wiederholungsanzahl, wenn Prüfpunkte fehlschlagen. Sie können einen der folgenden Aktionstypen auswählen, die die Citrix ADC Appliance ausführen soll, wenn ein Fehler auftritt:

- **KEINE.** Es werden keine expliziten Maßnahmen ergriffen. Sie können den Dienst und die Überwachung anzeigen, und der Monitor gibt die Anzahl der aktuellen zusammenhängenden Fehlerantworten und kumulativen Antworten an.

- **LOG.** Protokolliert das Ereignis in ns/syslog und zeigt die Leistungsindikatoren an.
- **DOWN.** Markiert den Dienst und leitet keinen Traffic an den Dienst weiter. Diese Einstellung unterbricht alle persistenten Verbindungen mit dem Dienst. Diese Aktion protokolliert auch das Ereignis und zeigt Leistungsindikatoren an.

Nachdem der Dienst ausgefallen ist, bleibt der Dienst für die konfigurierte Ausfallzeit DOWN. Nach Ablauf der Ausfallzeit verwendet der Inline-Monitor die konfigurierte URL, um den Dienst zu untersuchen, um festzustellen, ob er wieder verfügbar ist. Wenn der Prüfpunkt erfolgreich ist, wird der Status des Dienstes in UP geändert. Der Datenverkehr wird an den Dienst geleitet, und die Überwachung wird wie zuvor fortgesetzt.

Informationen zum Konfigurieren von Inline-Monitoren finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

So konfigurieren Sie HTTP-Inline-Monitore mit CLI

Geben Sie den folgenden Befehl ein:

```
1 add lb monitor <monitorName> <type> -respCode <int[-int]> -httpRequest
     <string> -resptimeout <integer> [<units>] -retries <integer> -
     downTime <integer> [<units>] -action <action>
2 <!--NeedCopy-->
```

Beispiel:

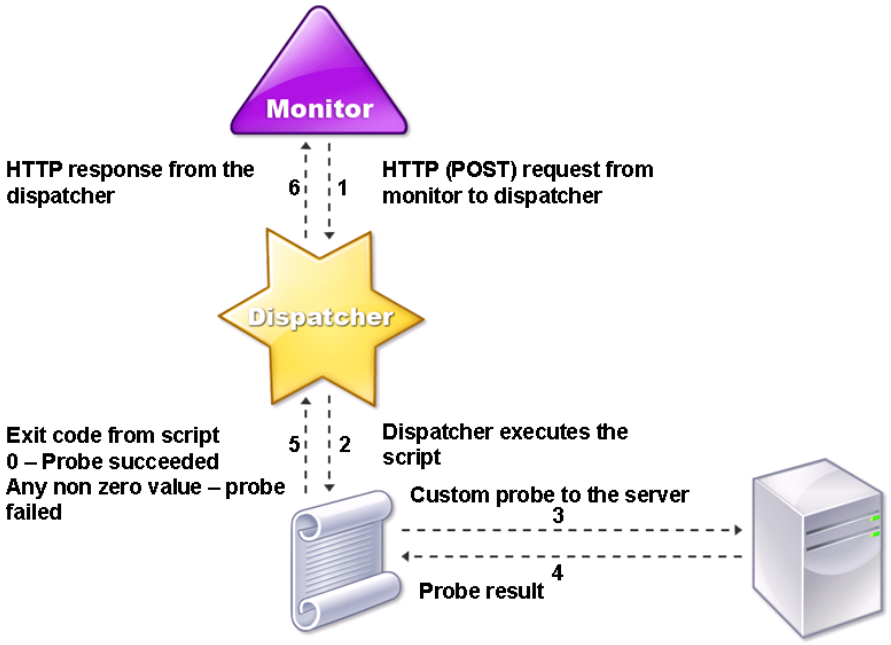
```
1 add lb monitor http_inline HTTP-INLINE -respCode 200 304 -httpRequest "
     HEAD /var/static/empty.htm" -resptimeout 4 -retries 1 -downTime 2 -
     action NONE
2 <!--NeedCopy-->
```

Benutzermonitore verstehen

August 11, 2022

Benutzermonitore erweitern den Umfang von benutzerdefinierten Monitoren. Sie können Benutzermonitore erstellen, um den Zustand benutzerdefinierter Anwendungen und Protokolle zu verfolgen, die die Citrix ADC-Appliance nicht unterstützt. Das folgende Diagramm zeigt, wie ein Benutzermonitor funktioniert.

Abbildung 1. Benutzer-Monitore



Für einen Benutzermonitor sind die folgenden Komponenten erforderlich.

- **Dispatcher.** Ein Prozess auf der Appliance, der Überwachungsanfragen abhört. Ein Dispatcher kann sich auf der Loopback-IP-Adresse (127.0.0.1) und Port 3013 befinden. Dispatcher werden auch als interne Dispatcher bezeichnet. Ein Dispatcher kann auch ein Webserver sein, der das Common Gateway Interface (CGI) unterstützt. Solche Dispatcher werden auch als externe Dispatcher bezeichnet. Sie werden für benutzerdefinierte Skripts verwendet, die nicht in der FreeBSD-Umgebung ausgeführt werden, z. B.

  Hinweis: Sie können den Monitor und den Dispatcher so konfigurieren, dass sie HTTPS anstelle von HTTP verwenden, indem Sie die Option “sicher” auf dem Monitor aktivieren und sie als externen Dispatcher konfigurieren. Ein interner Dispatcher versteht jedoch nur HTTP und kann HTTPS nicht verwenden.

  In einem HA-Setup wird der Dispatcher sowohl auf den primären als auch auf den sekundären Citrix ADC-Appliances ausgeführt. Der Dispatcher bleibt auf dem sekundären Gerät inaktiv.

Script. Das Skript ist ein Programm, das benutzerdefinierte Prüfpunkte an den Server mit Lastausgleich sendet und den Antwortcode an den Dispatcher zurückgibt. Das Skript kann einen beliebigen Wert an den Dispatcher zurückgeben, aber wenn eine Prüfung erfolgreich ist, muss das Skript einen

Wert von Null (0) zurückgeben. Der Dispatcher betrachtet jeden anderen Wert als Sondenausfall.

Die Citrix ADC-Appliance ist mit Beispielskripten für häufig verwendete Protokolle gebündelt. Die Skripts sind im Verzeichnis /nsconfig/monitors vorhanden. Wenn Sie ein Script hinzufügen möchten, fügen Sie es dort hinzu. Um ein vorhandenes Skript anzupassen, erstellen Sie eine Kopie mit einem neuen Namen und ändern Sie es.

Wichtig:

- Ab Citrix ADC Release 13.0 Build 41.20 können Sie das Skript `nsntlm-lwp.pl` verwenden, um einen Monitor zur Überwachung eines sicheren NTLM-Servers zu erstellen.
- Ab Version 10.1 Build 122.17 befinden sich die Skriptdateien für Benutzermonitore an einem neuen Speicherort.

  Wenn Sie eine virtuelle MPX- oder VPX-Appliance auf Version 10.1 Build 122.17 oder höher aktualisieren, lauten die Änderungen wie folgt:

  - Ein neues Verzeichnis namens conflicts wird in /nsconfig/monitors/ erstellt und alle integrierten Skripts der vorherigen Builds werden in dieses Verzeichnis verschoben.
  - Alle neuen integrierten Skripts sind im Verzeichnis /netscaler/monitors/ verfügbar. Alle benutzerdefinierten Skripts sind im Verzeichnis /nsconfig/monitors/ verfügbar.
  - Speichern Sie ein neues benutzerdefiniertes Skript im Verzeichnis /nsconfig/monitors/.
  - Wenn nach Abschluss des Upgrades ein benutzerdefiniertes Skript erstellt und im Verzeichnis /nsconfig/monitors/ gespeichert wird, mit demselben Namen wie das integrierte Skript, hat das Skript im Verzeichnis /netscaler/monitors/ Vorrang. Das benutzerdefinierte Skript wird nicht ausgeführt.

  Wenn Sie eine virtuelle Appliance mit Version 10.1 Build 122.17 oder höher bereitstellen, lauten die Änderungen wie folgt:

  - Alle integrierten Skripts sind im Verzeichnis /netscaler/monitors/ verfügbar.
  - Das Verzeichnis /nsconfig/monitors/ ist leer.
  - Wenn Sie ein benutzerdefiniertes Skript erstellen, müssen Sie es im Verzeichnis /nsconfig/monitors/ speichern.

Damit die Skripts korrekt funktionieren:

- Die maximale Anzahl von Zeichen im Namen des Skripts darf 63 nicht überschreiten.
- Die maximale Anzahl von Script-Argumenten, die einem Script zur Verfügung gestellt werden können, darf 512 nicht überschreiten.
- Die maximale Anzahl von Zeichen, die in den Argumenten des Parameterskripts angegeben werden können, darf 639 nicht überschreiten.

Um das Skript zu debuggen, müssen Sie es mithilfe des nsumon-debug.pl-Skripts von der CLI ausführen. Sie verwenden den Skriptnamen (mit seinen Argumenten), die IP-Adresse und den Port als

Argumente des nsumon-debug.pl-Skripts. Benutzer müssen den Skriptnamen, die IP-Adresse, den Port, das Timeout und die Skript-Argumente für das nsumon-debug.pl-Skript verwenden.

Geben Sie bei der CLI Folgendes ein:

```
1 nsumon-debug.pl <scriptname> <IP> <port> <timeout> <partitionID> [
     scriptarguments][is_secure]
2 <!--NeedCopy-->
```

Wichtig: Ab Version 10.5 Build 57.x und 11.0 Skriptdateien für Benutzermonitore unterstützen IPv6-Adressen und beinhalten folgende Änderungen:

- Für die folgenden Protokolle wurden neue `pm files` für die IPv6-Unterstützung aufgenommen.
  - RADIUS
  - NNTP
  - POP3
  - SMTP
- Die folgenden Beispielskripte in /netscaler/monitors/ wurden für die IPv6-Unterstützung aktualisiert:
  - nsbmradius.pl
  - nsldap.pl
  - nsnntp.pl
  - nspop3 nssf.pl
  - nssnmp.pl
  - nswi.pl
  - nstftp.pl
  - nssmtp.pl
  - nsrdp.pl
  - nsntlm-lwp.pl
  - nsftp.pl
  - nsappc.pl

  Stellen Sie nach dem Upgrade auf Version 10.5 Build 57.x oder 11.0 sicher, dass Sie die vorhandenen benutzerdefinierten Skripts mit IPv6-Diensten verwenden möchten, die vorhandenen

benutzerdefinierten Skripts mit den Änderungen in den aktualisierten Beispielskripten in /netscaler/monitors/aktualisieren.

Hinweis: Das Beispielskript nsmysql.pl unterstützt die IPv6-Adresse nicht. Wenn ein IPv6-Dienst an einen Benutzermonitor gebunden ist, der nsmysql.pl verwendet, schlägt der Test fehl.

- Die folgenden LB-Monitortypen wurden aktualisiert, um IPv6-Adressen zu unterstützen:
  - USER
  - SMTP
  - NNTP
  - LDAP
  - SNMP
  - POP3
  - FTP_EXTENDED
  - StoreFront
  - APPC
  - CITRIX_WI_EXTENDED

  Wenn Sie ein benutzerdefiniertes Skript erstellen, das einen dieser LB-Monitortypen verwendet, stellen Sie sicher, dass Sie IPv6-Unterstützung in das benutzerdefinierte Skript aufnehmen. Beziehen Sie sich auf das zugehörige Beispielskript in /netscaler/monitors/ für die Änderungen, die Sie im benutzerdefinierten Skript für die IPv6-Unterstützung vornehmen müssen.

Um den Status des Servers zu verfolgen, sendet der Monitor eine HTTP-POST-Anforderung an den konfigurierten Dispatcher. Diese POST-Anfrage enthält die IP-Adresse und den Port des Servers sowie das Skript, das ausgeführt werden muss. Der Dispatcher führt das Skript als untergeordneten Prozess mit benutzerdefinierten Parametern (falls vorhanden) aus. Anschließend sendet das Skript einen Prüfpunkt an den Server. Das Skript sendet den Status der Sonde (Antwortcode) an den Dispatcher. Der Dispatcher wandelt den Antwortcode in eine HTTP-Antwort um und sendet ihn an den Monitor. Basierend auf der HTTP-Antwort markiert der Monitor den Dienst als hoch oder unten.

Die Citrix ADC-Appliance protokolliert die Fehlermeldungen in der Datei /var/nslog/nsumond.log, wenn die Prüfungen der Benutzerüberwachung fehlschlagen. Diese detaillierten Fehlermeldungen werden in der GUI und in der CLI für die Befehle `show service`/`service group` angezeigt.

In der folgenden Tabelle sind die Benutzermonitore und die möglichen Gründe für einen Fehler aufgeführt.

Typ des Benutzermonitors	Gründe für Sondenausfall
SMTP	Monitor stellt keine Verbindung zum Server her.
NNTP	Monitor stellt keine Verbindung zum Server her.
	Fehlende oder ungültige Skriptargumente, die eine ungültige Anzahl von Argumenten oder Argumentformat enthalten können.
	Monitor findet die NNTP-Gruppe nicht.
LDAP	Monitor stellt keine Verbindung zum Server her.
	Fehlende oder ungültige Skriptargumente, die eine ungültige Anzahl von Argumenten oder Argumentformat enthalten können.
	Monitor bindet nicht an den LDAP-Server.
	Monitor findet keinen Eintrag für die Zielentität im LDAP-Server.
FTP	Die Verbindung zum Server ist ab.
	Fehlende oder ungültige Skriptargumente, die eine ungültige Anzahl von Argumenten oder Argumentformat enthalten können.
	Anmeldung fehlgeschlagen.
	Monitor findet die Datei nicht auf dem Server.
POP3	Monitor stellt keine Verbindung zur Datenbank her.
	Fehlende oder ungültige Skriptargumente, die eine ungültige Anzahl von Argumenten oder Argumentformat enthalten können.
	Anmeldung fehlgeschlagen.
POP3	Monitor stellt keine Verbindung zur Datenbank her.
	Fehlende oder ungültige Skriptargumente, die eine ungültige Anzahl von Argumenten oder Argumentformat enthalten können.

Typ des Benutzermonitors	Gründe für Sondenausfall
	Anmeldung fehlgeschlagen.
	Die Vorbereitung der SQL-Abfrage schlägt fehl.
	Die Ausführung der SQL-Abfrage schlägt fehl.
SNMP	Monitor stellt keine Verbindung zur Datenbank her.
	Fehlende oder ungültige Skriptargumente, die eine ungültige Anzahl von Argumenten oder Argumentformat enthalten können.
	Anmeldung fehlgeschlagen.
	Monitor kann die SNMP-Sitzung nicht erstellen.
	Monitor findet den Objektbezeichner nicht.
	Die Einstellung des Monitorschwellenwerts ist größer oder gleich dem tatsächlichen Schwellenwert des Monitors.
RDP (Windows Terminalserver)	Fehlende oder ungültige Skriptargumente, die eine ungültige Anzahl von Argumenten oder Argumentformat enthalten können.
	Monitor kann keinen Socket erstellen.
	In Versionen stimmt nicht überein.
	Der Monitor kann die Verbindung nicht bestätigen.

Sie können die Protokolldatei von der CLI aus anzeigen, indem Sie die folgenden Befehle verwenden, die eine BSD-Shell öffnen, die Protokolldatei auf dem Bildschirm anzeigen und dann die BSD-Shell schließen und Sie zur CLI zurückkehren:

```
1 > shell
2 root@ns# cat /var/nslog/nsumond.log
3 root@ns# exit
4 >
5 <!--NeedCopy-->
```

Vor Citrix ADC Version 13.0 Build 52.X zeigte der Befehl `show service/service group` eine generische Fehlermeldung an, die besagte, dass “Probe fehlgeschlagen” als Ursache für den Fehler des

Benutzermonitorprüfens war.

Beispiel:

```
show service ftp

Monitor Name: mon2
State: UNKNOWN  Weight: 1   Passive: 0
Probes: 3    Failed [Total: 0 Current: 0]
Last response: Failure - Probe failed.
Response Time: 1071.838 millisec
<!--NeedCopy-->
```

Ab Citrix ADC Version 13.0 Build 52.X zeigt der Befehl `show service/service group` die tatsächliche Ursache für den Fehler des Benutzermonitorprüfens an.

Beispiel:

```
show service ftp

Monitor Name: mon2
State: DOWN   Weight: 1   Passive: 0
Probes: 729   Failed [Total: 726 Current: 726]
Last response: Failure - Login failed.
Response Time: 8000.0 millisec
<!--NeedCopy-->
```

Benutzermonitore haben auch einen Timeout-Wert und eine Anzahl von Wiederholungsversuchen für Sondenausfälle. Sie können Benutzermonitore mit Nicht-Benutzermonitoren verwenden. Bei hoher CPU-Auslastung ermöglicht ein Nicht-Benutzermonitor eine schnellere Erkennung eines Serverausfalls.

Wenn der Prüfpunkt des Benutzermonitors bei hoher CPU-Auslastung eine Zeitdauer aufweist, bleibt der Status des Dienstes unverändert.

Example1:

```
add lb monitor <name> USER  -scriptname <script-name> -resptimeout 5
    seconds
<!--NeedCopy-->
```


> **Hinweis**
>
> :
>
> Für skriptfähige Monitore muss das Antwort-Timeout auf einen Wert konfiguriert werden, der dem erwarteten Timeout entspricht + 1 Sekunde. Wenn Sie beispielsweise erwarten, dass das Timeout 4 Sekunden beträgt, konfigurieren Sie das Antwort-Timeout auf 5 Sekunden.

Example2:

```
add lb monitor <name> USER -scriptname <script-name> -scriptargs <
    Arguments> -secureargs <Arguments>
<!--NeedCopy-->
```

> **Hinweis**
>
> :
>
> Citrix empfiehlt, den Parameter `secureargs` anstelle des Parameters `scriptargs` für vertrauliche Daten in den Skripts zu verwenden.

Wie benutzt man einen Benutzermonitor, um Websites zu überprüfen

October 5, 2021

Sie können einen Benutzermonitor so konfigurieren, dass er nach bestimmten Websiteproblemen prüft, die von HTTP-Servern mit bestimmten HTTP-Codes gemeldet werden. In der folgenden Tabelle sind die HTTP-Antwortcodes aufgeführt, die dieser Benutzermonitor erwartet.

HTTP-Antwortcode	Bedeutung
200 - Erfolg	Sonde erfolgreich.
503 - Service nicht verfügbar	Prüfpunktfehler.
404 - nicht gefunden	Das Skript wurde nicht gefunden oder kann nicht ausgeführt werden.
500 - Interner Serverfehler	Interner Fehler/Ressourceneinschränkungen im Dispatcher (nicht genügend Arbeitsspeicher, zu viele Verbindungen, unerwarteter Systemfehler oder zu viele Prozesse). Der Dienst ist nicht mit DOWN gekennzeichnet.

HTTP-Antwortcode	Bedeutung
400 - schlechte Anfrage	Fehler beim Analysieren der HTTP-Anforderung.
502 - schlechtes Gateway	Fehler beim Decodieren der Antwort des Skripts.

Konfigurieren Sie den Benutzermonitor für HTTP mithilfe der folgenden Parameter.

Parameter	Gibt an
scriptName	Der Pfad und der Name des auszuführenden Skripts.
scriptArgs	Die Zeichenfolgen, die in den POST-Daten hinzugefügt werden. Sie werden wörtlich in die Anforderung kopiert.
dispatcherIP	Die IP-Adresse des Dispatchers, an den der Prüfpunkt gesendet wird.
dispatcherPort	Der Port des Dispatchers, an den der Prüfpunkt gesendet wird.
localfileName	Der Name einer Monitorskriptdatei auf dem lokalen System.
destPath	Ein bestimmter Speicherort auf der Citrix ADC Appliance, in dem die hochgeladene lokale Datei gespeichert ist.

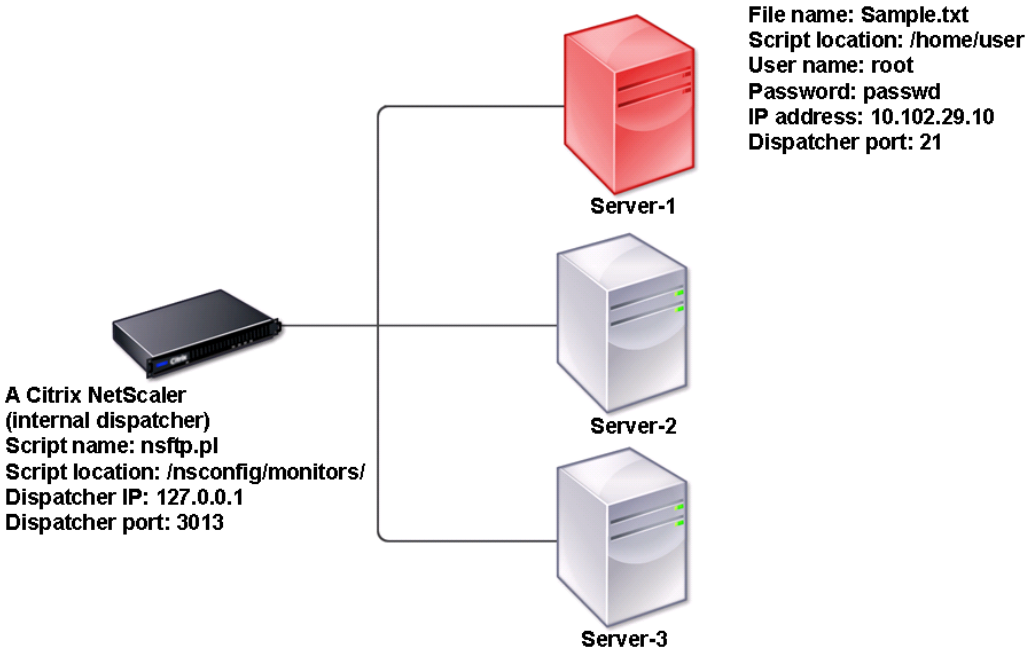
Informationen zum Erstellen eines Benutzermonitors zur Überwachung von HTTP finden Sie unter Konfigurieren von Monitoren in einem Load Balancing Setup.

Den internen Dispatcher verstehen

October 5, 2021

Sie können einen benutzerdefinierten Benutzermonitor mit dem internen Dispatcher verwenden. Betrachten Sie einen Fall, in dem Sie den Zustand eines Servers basierend auf dem Vorhandensein einer Datei auf dem Server verfolgen müssen. Das folgende Diagramm veranschaulicht dieses Szenario.

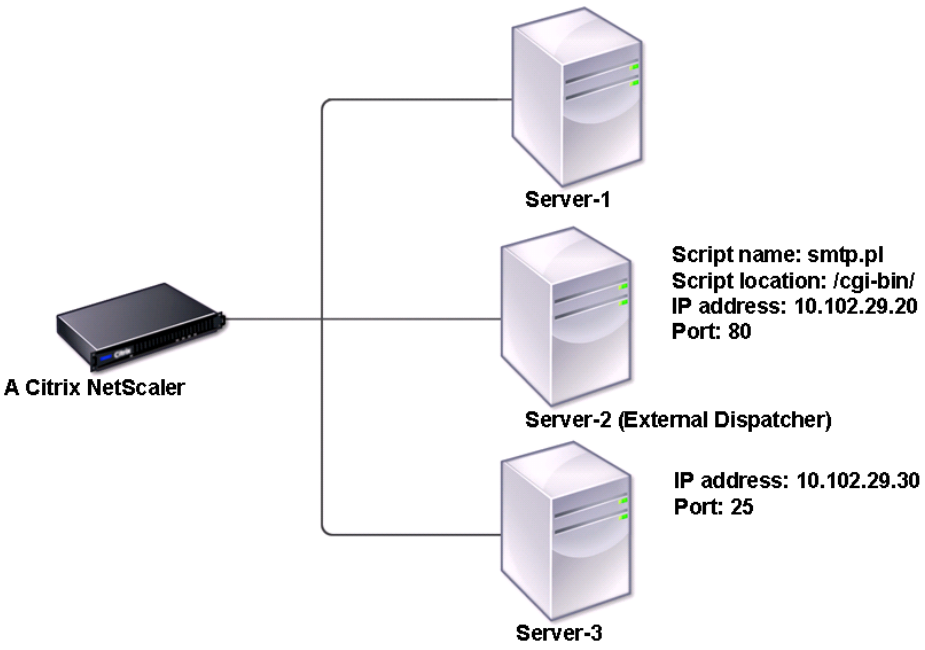
Abbildung 1. Verwenden eines Benutzermonitors mit dem internen Dispatcher



Eine mögliche Lösung besteht darin, ein Perl-Skript zu verwenden, das eine FTP-Sitzung mit dem Server initiiert und auf das Vorhandensein der Datei überprüft. Anschließend können Sie einen Benutzermonitor erstellen, der das Perl-Skript verwendet. Die Citrix ADC Appliance enthält ein solches Perl-Skript (nsftp.pl) im Verzeichnis /nsconfig/monitors/.

Sie können einen Benutzermonitor mit einem externen Dispatcher verwenden. Betrachten Sie einen Fall, in dem Sie den Zustand eines Servers basierend auf dem Status eines SMTP-Dienstes auf einem anderen Server verfolgen müssen. Dieses Szenario wird im folgenden Diagramm veranschaulicht.

Abbildung 2. Verwenden eines Benutzermonitors mit einem externen Dispatcher



Eine mögliche Lösung wäre das Erstellen eines Perl-Skripts, das den Status des SMTP-Dienstes auf dem Server überprüft. Anschließend können Sie einen Benutzermonitor erstellen, der das Perl-Skript verwendet.

Konfigurieren eines Benutzermonitors

August 11, 2022

Benutzermonitore verfolgen den Zustand benutzerdefinierter Anwendungen und Protokolle, die eine Citrix ADC-Appliance nicht unterstützt. Dies ist ein erweiterter Umfang an benutzerdefinierten Monitoren. Um einen Benutzermonitor zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

- Schreiben Sie ein Skript, das die daran gebundenen Dienste überwachen kann.
- Laden Sie das Skript in das Verzeichnis `/nsconfig/monitors` auf der Citrix ADC-Appliance hoch.
- Geben Sie eine ausführbare Berechtigung für das Skript.

Wenn der Monitortyp ein Protokoll ist, das die Appliance nicht unterstützt, müssen Sie nur einen Monitor vom Typ **USER**verwenden. Benutzermonitore unterstützen nur Perl- und Bash-Skripte. Sie unter-

stützen keine Python-Skripte.

> **Hinweis**
>
> Monitorsonden stammen von der NSIP-Adresse. Für den Monitortyp **USER** konfigurierte `scriptargs` wird in den laufenden Konfigurations- und ns.conf-Dateien angezeigt.

Weitere Informationen zu Monitoren finden Sie unter Konfigurieren von Monitoren.

So konfigurieren Sie einen Benutzermonitor über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb monitor <monitorName> USER -scriptname <NameOfScript> -
     scriptargs <Arguments> -secureargs <Arguments>
2 <!--NeedCopy-->
```

Example1:

```
1 add monitor Monitor-User-1 USER -scriptname nsftp.pl -scriptargs "file
     =/home/user/
2 sample.txt;user=root;password=passwd"
3 <!--NeedCopy-->
```

Example2:

```
1 add monitor Monitor-User-1 USER -scriptname nsftp.pl -scriptargs "file
     =/home/user/
2 sample.txt -secureargs "user=root;password=passwd"
3 <!--NeedCopy-->
```

> Hinweis
>
> Der Parameter `secureargs` speichert die Skriptsrgumente in einem verschlüsselten Format anstelle des Nur-Text-Formats. Citrix empfiehlt, den Parameter `secureargs` anstelle des scriptargs-Parameters für alle vertraulichen Daten in den Skripts zu verwenden, z. B. Benutzername und Kennwort. Wenn Sie beide Parameter zusammen verwenden möchten, muss das in `-scriptname` angegebene Skript die Argumente in dieser Reihenfolge akzeptieren: `<scriptargs> <secureargs>`. Geben Sie die ersten Argumente im Parameter `<scriptargs>` an; und den Rest der Argumente im Parameter `<secureargs>`. Das heißt, behalten Sie die

> für die Argumente definierte Reihenfolge bei. Sichere Argumente gelten nur für den internen Dispatcher. Wenn Sie einen externen Dispatcher verwenden möchten, empfiehlt Citrix, die anfälligen Daten in Ihren Skripten zu sichern.

Beispiel 3:

Angenommen, Sie haben den Parameter `scriptargs` bereits mit den Argumenten konfiguriert: “a=b; c=d; e=f”.

```
add monitor mon1 USER -scriptargs ”a=b;c=d;e=f”
<!--NeedCopy-->
```

Wenn Sie den arameter `secureargs` anstelle des Parameters `scriptargs` verwenden möchten, gehen Sie wie folgt vor:

- Nullifizieren Sie den Parameter `scriptargs`.
- Geben Sie alle Argumente unter Parameter `secureargs` an.

```
set monitor mon1 USER -scriptargs ”” -secureargs ”a=b;c=d;e=f”
<!--NeedCopy-->
```

So konfigurieren Sie einen Benutzermonitor über die GUI

1. Navigieren Sie zu **Traffic Management> Load Balancing> Monitore**und klicken Sie auf **Hinzufügen**.
2. Gehen Sie auf der Seite **Monitor erstellen** wie folgt vor:
   - Wählen Sie den Monitortyp als **USER**aus.
   - Wähle das Script aus dem Dropdown-Menü aus oder lade dein eigenes Script hoch.
   - Geben Sie die entsprechenden Werte für die Felder **Script-Argumente** und **sichere Argumente** ein.
   - Klicken Sie auf **Erstellen**.

   Ein Benutzermonitor wird erstellt.

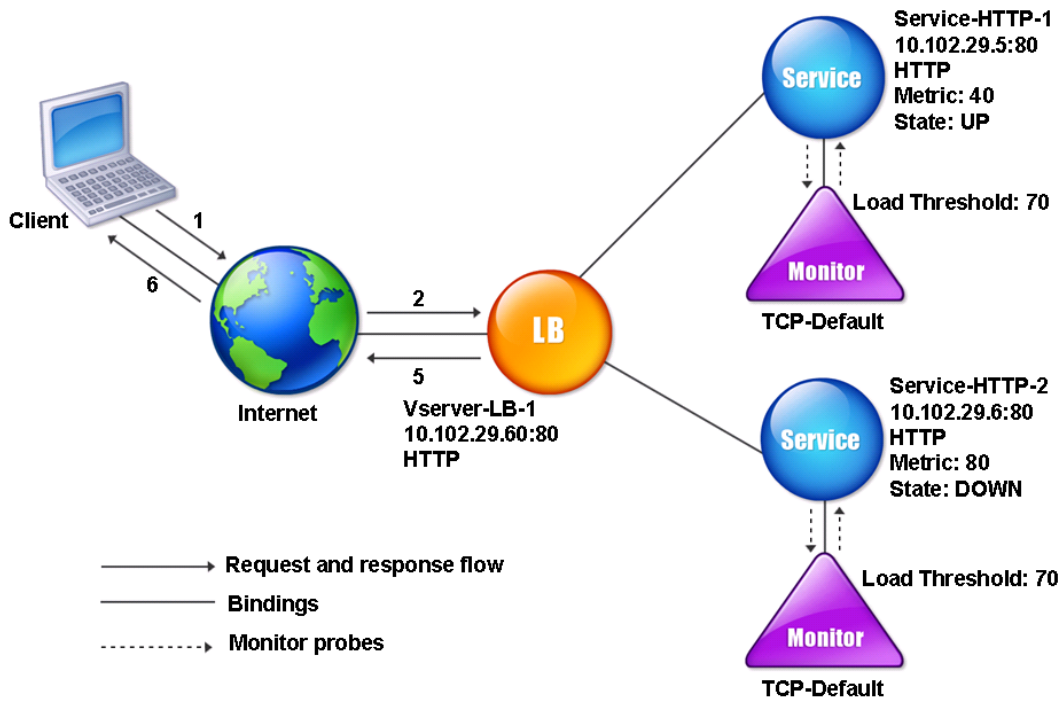
Verstehen von Lastmonitoren

October 5, 2021

Lastmonitore verwenden SNMP-abgefragte OIDs, um die Last zu berechnen. Der Lastmonitor verwendet zum Abrufen die IP-Adresse des Dienstes, an den er gebunden ist (die Ziel-IP-Adresse). Es sendet eine SNMP-Abfrage an den Dienst und gibt die OID für eine Metrik an. Die Metriken können CPU, Arbeitsspeicher oder Anzahl der Serververbindungen sein. Der Server antwortet auf die Abfrage mit einem Metrikwert. Der Metrikwert in der Antwort wird mit dem Schwellenwert verglichen. Die Citrix ADC Appliance berücksichtigt den Dienst für den Lastausgleich nur, wenn die Metrik kleiner als der Schwellenwert ist. Der Dienst mit dem niedrigsten Lastwert wird zuerst betrachtet.

Das folgende Diagramm veranschaulicht einen Lastmonitor, der für die Dienste konfiguriert ist, die im grundlegenden Lastenausgleichs-Setup beschrieben sind, das unter Einrichten von Basic Load Balancingbeschrieben wurde.

Abbildung 1. Betrieb von Lastmonitoren



Hinweis: Der Lastmonitor bestimmt nicht den Status des Dienstes. Es ermöglicht nur die Appliance, den Dienst für den Lastausgleich in Betracht zu ziehen.

Nachdem Sie den Lastmonitor konfiguriert haben, müssen Sie dann die Metriken konfigurieren, die der Monitor verwendet. Zur Lastbewertung berücksichtigt der Lastmonitor Serverparameter, die als Metriken bezeichnet werden, die in den Metriktabellen in der Appliance-Konfiguration definiert sind. Metrik-Tabellen können von zwei Typen sein:

- **Lokal:** Standardmäßig ist diese Tabelle in der Appliance vorhanden. Es besteht aus vier Metriken: Verbindungen, Pakete, Antwortzeit und Bandbreite. Die Appliance gibt diese Metriken für einen Dienst an, und SNMP-Abfragen stammen nicht für diese Dienste. Diese Metriken können nicht geändert werden.
- **Benutzerdefiniert.** Eine benutzerdefinierte Tabelle. Jede Metrik ist einer OID zugeordnet.

Standardmäßig generiert die Appliance die folgenden Tabellen:

- NetScaler
- RADWARE
- CISCO-CSS
- LOCAL
- FOUNDRY
- ALTEON

Sie können entweder die von der Anwendung generierten Metriktabellen hinzufügen oder Tabellen Ihrer eigenen Wahl hinzufügen, wie in der folgenden Tabelle dargestellt. Die Werte in der Metriktabelle werden nur als Beispiele angegeben. Berücksichtigen Sie in einem tatsächlichen Szenario die realen Werte für die Metriken.

Metrikname	OIDs	Gewicht	Schwellenwert
CPU	1.2.3.4	2	70
Speicher	4.5.6.7	3	80
Verbindungen	5.6.7.8	4	90

Um die Last für eine oder mehrere Metriken zu berechnen, weisen Sie jeder Metrik eine Gewichtung zu. Die Standardgewichtung ist 1. Die Gewichtung stellt die Priorität dar, die jeder Metrik zugewiesen wird. Wenn das Gewicht hoch ist, ist die Priorität hoch. Die Appliance wählt einen Dienst basierend auf dem SOURCEIPDESTIP-Hash-Algorithmus aus.

Sie können auch den Schwellenwert für jede Metrik festlegen. Der Schwellenwert ermöglicht es der Appliance, einen Dienst für den Lastausgleich auszuwählen, wenn der Metrikwert für den Dienst kleiner als der Schwellenwert ist. Der Schwellenwert bestimmt auch die Last für jeden Dienst.

Konfigurieren von Lastmonitoren

October 5, 2021

Um einen Lastmonitor zu konfigurieren, erstellen Sie zuerst den Lastmonitor. Anweisungen zum Erstellen eines Monitors finden Sie unter Erstellen von Monitoren. Wählen oder erstellen Sie als Nächstes

die Metriktabelle, um eine Reihe von Metriken zu definieren, die den Status des Servers bestimmen, und (wenn Sie eine Metriktabelle erstellen) jede Metrik an die Metriktabelle binden.

So erstellen Sie eine Metriktabelle mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
add lb metricTable <metricTableName>

bind lb metricTable <metricTableName> <metric> <SNMPOID>
<!--NeedCopy-->
```

Beispiel:

```
add metricTable Table-Custom-1

bind metricTable Table-Custom-1 1.3.6.1.4.1.5951.4.1.1.41.1.5 11
<!--NeedCopy-->
```

So erstellen Sie eine Metriktabelle und binden Metriken mit dem Konfigurationsdienstprogramm an sie

1. Navigieren Sie zu **Traffic Management > Load Balancing > Metriktabellen**, und erstellen Sie eine Metriktabelle.
2. Um Metriken zu binden, klicken Sie auf **Binden** und geben Sie eine Metrik und eine SNMP-OID an.

Aufheben der Bindung von Metriken aus einer Metriktabelle

October 5, 2021

Sie können die Bindung von Metriken aus einer Metriktabelle aufheben, wenn die Metriken geändert werden müssen oder wenn Sie die Metriktabelle vollständig entfernen möchten.

So heben Sie die Bindung von Metriken aus einer Metrik-Tabelle mit der Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
unbind lb metricTable <metricTable> <metric>
<!--NeedCopy-->
```

Beispiel:

```
unbind metricTable Table-Custom-1 1.3.6.1.4.1.5951.4.1.1.41.1.5
<!--NeedCopy-->
```

So heben Sie die Bindung von Metriken aus einer Metrik-Tabelle mit dem Konfigurationsdienstprogramm auf

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Metrik-Tabellen** .
2. Öffnen Sie eine Metriktabelle, wählen Sie eine Metrik aus, und klicken Sie auf **Löschen**.

Sie können die Details aller konfigurierten Metriktabellen anzeigen, wie Name und Typ, um festzustellen, ob die Metriktabelle intern oder erstellt und konfiguriert ist.

Konfigurieren der umgekehrten Überwachung für einen Dienst

October 5, 2021

Ein Rückwärtsmonitor markiert einen Dienst als DOWN, wenn die Prüfpunktkriterien erfüllt sind, und UP, wenn sie nicht erfüllt sind. Wenn ein Backupdienst beispielsweise nur dann Datenverkehr empfangen soll, wenn der primäre Dienst DOWN ist, können Sie einen Rückwärtsmonitor an den sekundären Dienst binden, ihn jedoch so konfigurieren, dass er den primären Dienst untersucht.

Die Citrix ADC Appliance unterstützt die folgenden Reverse-Monitore:

- HTTP
- ICMP
- TCP (ab Release 11.1 Build 49.x)

Konfigurieren der HTTP-Reverse-Überwachung für einen Dienst

In der folgenden Tabelle werden die Bedingungen für die direkte und umgekehrte HTTP-Überwachung für einen Dienst beschrieben:

Bedingung	Direkte	Rückwärtsgang
Verbindung wurde nicht hergestellt.	Fehlschlagen	Fehlschlagen
HTTP-Antwortcode entspricht den Spezifikationen des Prüfpunkts.	Erfolg	Fehlschlagen
HTTP-Antwortcode stimmt nicht mit den Spezifikationen des Prüfpunkts überein.	Fehlschlagen	Erfolg
Timeout des Prüfpunktes.	Fehlschlagen	Fehlschlagen

So konfigurieren Sie die HTTP-Reverse-Überwachung für einen Dienst mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb monitor <Monitor_Name> HTTP -respCode 200 -httpRequest "HEAD /"
   -destIP <Primary_Service_IP_Address> -destPort 80 -reverse YES

bind service <Secondary_Service_Name> -monitorname <Monitor_Name>
<!--NeedCopy-->
```

Konfigurieren der ICMP-Reverse-Überwachung für einen Dienst

In der folgenden Tabelle werden die Bedingungen der direkten und umgekehrten ICMP-Überwachung für einen Dienst beschrieben:

Bedingung	Direkte	Rückwärtsgang
ICMP-Echoantwort wird empfangen.	Erfolg	Fehlschlagen
Timeout des Prüfpunktes.	Fehlschlagen	Erfolg

So konfigurieren Sie die ICMP-Reverseüberwachung für einen Dienst mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
1 add lb monitor <Monitor_Name> PING -destIP <Primary_Service_IP_Address>
      -reverse YES
2
3 bind service <Secondary_Service_Name> -monitorname <Monitor_Name>
4 <!--NeedCopy-->
```

Konfigurieren der TCP-Reverse-Überwachung für einen Dienst

Wenn ein direkter TCP-Monitor als Reaktion auf eine Monitorsonde ein RESET erhält, wird der Dienst als DOWN markiert. Wenn jedoch ein umgekehrter TCP-Monitor eine RESET-Antwort erhält, gilt der Prüfpunkt als erfolgreich, und der Dienst wird als UP markiert.

In der folgenden Tabelle werden die Bedingungen der TCP-Reverseüberwachung für einen Dienst beschrieben:

Bedingung	Direkte	Rückwärtsgang
TCP-Verbindung wird hergestellt.	Erfolg	Fehlschlagen
Timeout des Prüfpunktes.	Fehlschlagen	Fehlschlagen
Antwort auf den Prüfpunkt ist RESET.	Fehlschlagen	Erfolg

So konfigurieren Sie die TCP-Reverseüberwachung für einen Dienst mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb monitor <Monitor_Name> TCP  - destip <Primary_Service_IP_Address>
      -destport <primary_service_port>  - reverse YES
2
3 bind service <Secondary_Service_Name> -monitorname <Monitor_Name>
4 <!--NeedCopy-->
```

So konfigurieren Sie die umgekehrte Überwachung mit der GUI

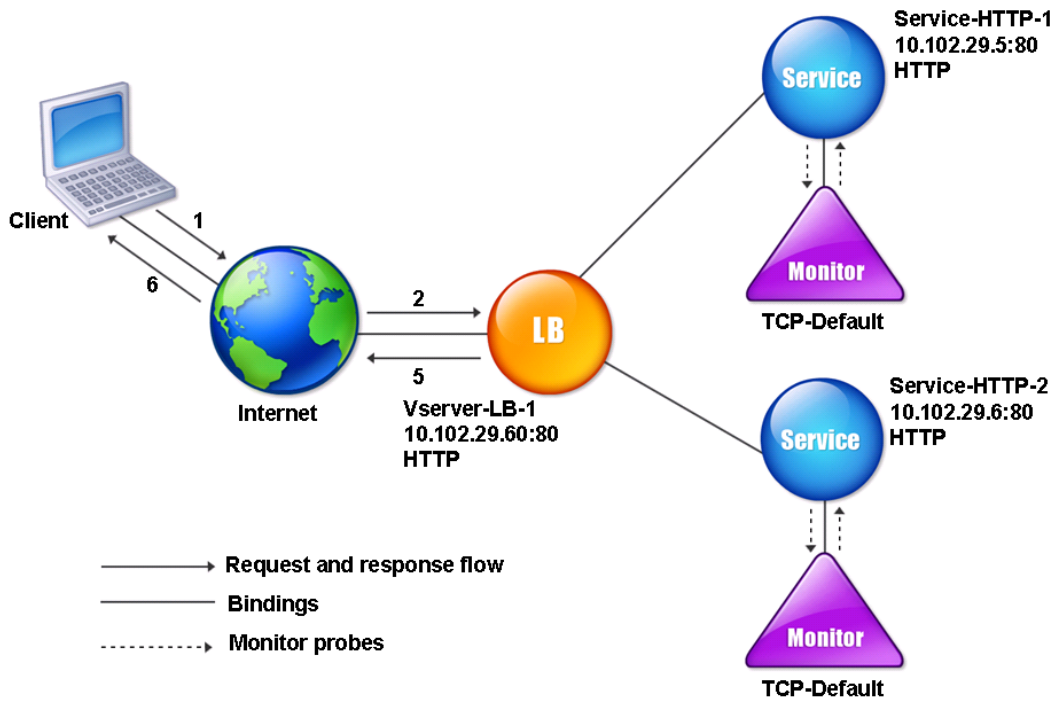
1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Monitore**.
2. Erstellen Sie einen HTTP-, ICMP- oder TCP-Monitor und wählen Sie **Reverse**aus.

Konfigurieren von Monitoren in einem Lastausgleichs-Setup

October 5, 2021

Um Monitore auf einer Website zu konfigurieren, entscheiden Sie zunächst, ob Sie einen integrierten Monitor verwenden oder einen eigenen Monitor erstellen möchten. Wenn Sie einen Monitor erstellen, können Sie wählen, ob Sie einen Monitor basierend auf einem integrierten Monitor erstellen oder einen benutzerdefinierten Monitor erstellen, der ein Skript verwendet, das Sie zur Überwachung des Dienstes schreiben. Weitere Informationen zum Erstellen benutzerdefinierter Monitore finden Sie unter Benutzerdefinierte Monitore. Sobald Sie einen Monitor ausgewählt oder erstellt haben, binden Sie ihn dann an den entsprechenden Dienst. Die Monitornamen können bis zu 255 Zeichen lang sein. Das folgende Konzeptdiagramm veranschaulicht eine grundlegende Lastausgleichseinrichtung mit Monitoren.

Abbildung 1. Funktionsweise von Monitoren



Wie gezeigt, hat jeder Dienst einen Monitor an ihn gebunden. Der Monitor untersucht den Lastausgleichsserver über seinen Service. Solange der Lastausgleichsserver auf die Sonden reagiert, markiert der Monitor ihn auf UP. Wenn der Lastausgleichsserver innerhalb des festgelegten Zeitraums nicht auf die angegebene Anzahl von Sonden reagiert, markiert der Monitor ihn nach UNTEN.

Dieser Abschnitt enthält die folgenden Details:

- Monitore erstellen
- Konfigurieren von Überwachungsparametern zum Ermitteln des Dienstintegritätszustands
- Binden von Monitoren an Dienste
- Monitore ändern
- Aktivieren und Deaktivieren von Monitoren
- Aufheben der Bindung von Monitoren
- Entfernen von Monitoren
- Anzeigen von Monitoren
- Schließen von Monitorverbindungen
- Ignorieren der Obergrenze für Clientverbindungen für Monitorprobes

Monitore erstellen

October 5, 2021

Die Citrix ADC Appliance bietet eine Reihe integrierter Monitore. Es ermöglicht Ihnen auch, benutzerdefinierte Monitore zu erstellen, entweder basierend auf den integrierten Monitoren oder von Grund auf neu.

So erstellen Sie einen Monitor mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb monitor <monitorName> <monitorType> [<interval>]

add lb mon monitor-HTTP-1 HTTP

add lb mon monitor-HTTP-2 TCP 2
<!--NeedCopy-->
```

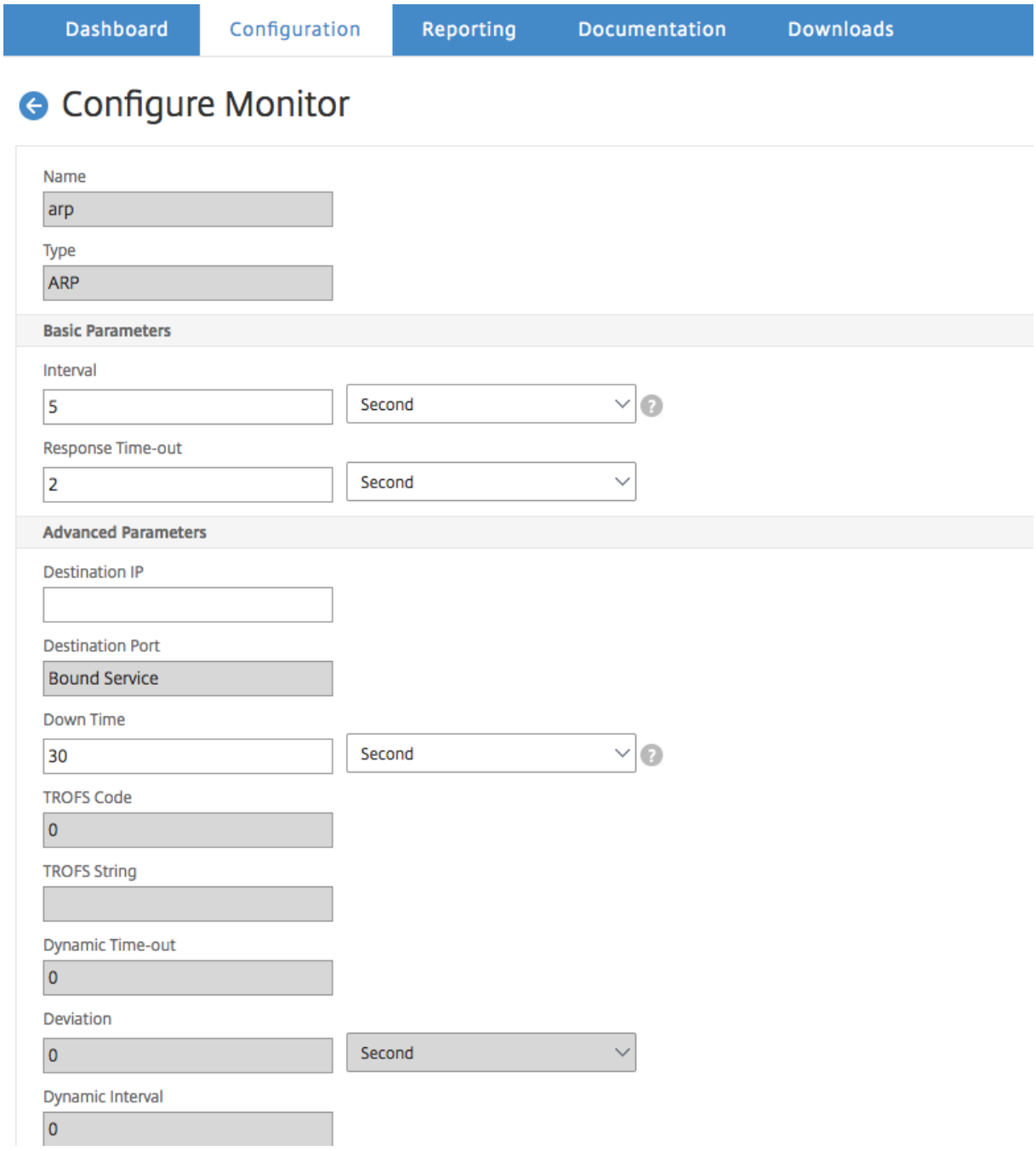
So erstellen Sie einen Monitor mit der GUI

1. Navigieren Sie zu **Traffic Management**> **Load Balancing**> **Monitore**.
2. Klicken Sie auf **Hinzufügen**, und erstellen Sie einen Monitortyp, der Ihren Anforderungen entspricht.

Das Fenster Monitor erstellen enthält zwei Abschnitte: **Basic Parameters** und **Advanced Parameters**.

Je nach Monitortyp enthält der Abschnitt **Grundparameter** die Parameter, die für jeden Monitor festgelegt werden müssen. Der Abschnitt **Erweiterte Parameter** enthält die Parameter, die in erweiterten Anwendungsfällen verwendet werden können.

Die folgende Abbildung ist ein Beispiel für eine Seite Monitor erstellen des ARP-Monitortyps.



> **Hinweis:**
>
> Vor NetScaler Release 12.0 Build 56.20 werden Basisparameter und Advanced Parameters als

> Standard Parameters bzw. Special Parameters bezeichnet.

Konfigurieren von Monitorparametern zum Bestimmen des Dienstzustands

October 5, 2021

Sie können die folgenden Überwachungsparameter konfigurieren, um einen Dienst basierend auf den Überwachungssonden als DOWN zu markieren.

Wiederholte Versuche

Maximale Anzahl der zu sendenden Prüfpunkte, um den Status eines Dienstes festzulegen, für den ein Überwachungssonde ausfällt.

failureRetries

Anzahl der Wiederholungen, die fehlschlagen müssen, außerhalb der für den Parameter Wiederholungen angegebenen Nummer, damit ein Dienst als DOWN markiert wird. Wenn der Parameter Wiederholungen beispielsweise auf 10 festgelegt ist und der Parameter Failure Retries auf 6 gesetzt ist, müssen von den 10 gesendeten Sonden mindestens sechs Sonden fehlschlagen, wenn der Dienst als DOWN gekennzeichnet werden soll.

alertRetries

Anzahl aufeinanderfolgender Prüfpunktfehler, nach denen die Appliance einen SNMP-Trap namens MonProbeFailed generiert.

AlertRetries auf einen Wert setzen, der höher ist als der Wert “Wiederholungen”

Der Parameter AlertRetries, der die maximale Anzahl aufeinanderfolgender Monitoringprobenfehler angibt, nach denen die Citrix ADC Appliance ein SNMP-Trap namens MonProbeFailed generiert, kann nun auf einen Wert festgelegt werden, der höher ist als der Wert Retries (der die maximale Anzahl von Prüfpunkten angibt, die gesendet werden sollen, um die Status eines Dienstes, für den ein Monitoring-Test fehlgeschlagen ist). Wenn der Wert alertRetries höher als der Wert für Retries ist, wird die SNMP-Trap erst gesendet, nachdem der Dienst DOWN ist.

Wenn Sie z. B. Wiederholungen auf 3, AlertRetries auf 12 und das Zeitintervall auf 5 Sekunden festlegen, wird der Dienst nach 15 Sekunden (3*5) als DOWN markiert, es wird jedoch keine Warnung generiert.*

Wenn die Monitorsonden nach 60 Sekunden (125) weiterhin ausfallen, generiert die Citrix ADC Appliance eine monProbeFailed-Trap. Wenn ein Prüfpunkt zu einem bestimmten Zeitpunkt zwischen 15 und 60 Sekunden erfolgreich ist, wird der Dienst als UP markiert, und es wird keine Warnung generiert.

Wenn Sie den Wert AlertRetries auf einen Wert setzen, der höher ist als der Wert Wiederholungen hilft, nur echte Alerts zu generieren und Fehlalarme während geplanter Neustarts zu vermeiden.

So legen Sie den AlertRetries Parameterwert mit der Befehlszeilenschnittstelle auf einen höheren Wert als den Wert Retries fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb monitor <monitorName> [-retries <integer>] [-alertRetries <
     integer>]
2 <!--NeedCopy-->
```

Beispiel:

add lb monitor monitor-HTTP-1 HTTP -retries 3 -alertRetries 12

So legen Sie den AlertRetries Parameterwert mit der GUI auf einen höheren Wert als den Wert Retries fest

1. Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Monitore**.
2. Klicken Sie auf **Hinzufügen**, um einen neuen Monitor hinzuzufügen, oder wählen Sie einen vorhandenen Monitor aus, und klicken Sie auf **Bearbeiten** .
3. Geben Sie im Feld **Wiederholungen** den Wert für den Parameter Wiederholungen ein.
4. Geben Sie im Feld **SNMP-Warnmeldungen** den Wert für den Parameter `alertRetries` ein.

Monitore an Dienste binden

October 5, 2021

Nachdem Sie einen Monitor erstellt haben, binden Sie ihn an einen Dienst. Sie können einen oder mehrere Monitore an einen Dienst binden. Wenn Sie einen Monitor an einen Dienst binden, bestimmt dieser Monitor, ob der Dienst als UP oder DOWN markiert ist.

Wenn Sie mehrere Monitore an einen Dienst binden, überprüft die Citrix ADC Appliance den Status aller Monitore und entscheidet dann den Status des Dienstes. Sie können verschiedene Gewichtungen für einen Monitor konfigurieren. Das Gewicht eines Monitors gibt an, wie viel dieser Monitor dazu

beiträgt, den Dienst als UP oder DOWN zu bezeichnen. Ein Monitor mit einem größeren Gewicht hat eine höhere Präferenz bei der Kennzeichnung des Dienstes UP oder DOWN. Standardgewicht ist 1. Selbst wenn einer der Monitore ausfällt, wird der Dienst daher als DOWN markiert. Weitere Informationen finden Sie unter Festlegen eines Schwellenwerts für die an einen Dienst gebundenen Monitore.

Hinweis: Die Ziel-IP-Adresse eines Monitor-Prüfpunkts kann von der IP-Adresse und dem Port des Servers abweichen.

So binden Sie einen Monitor über die Befehlszeilenschnittstelle an einen Dienst

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind service <name> (-monitorName <string>)
<!--NeedCopy-->
```

Beispiel:

```
bind service s1 -monitorName tcp
<!--NeedCopy-->
```

So binden Sie einen Monitor über die GUI an einen Dienst

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Öffnen Sie den Dienst, und fügen Sie einen Monitor hinzu.

Monitore ändern

October 5, 2021

Sie können die Einstellungen für jeden von Ihnen erstellten Monitor ändern.

Hinweis: Für Monitore gelten zwei Parametersätze: diejenigen, die unabhängig vom Typ für alle Monitore gelten, und diejenigen, die spezifisch für einen Monitortyp sind. Informationen zu Parametern für einen bestimmten Monitortyp finden Sie in der Beschreibung für diesen Monitortyp.

So ändern Sie einen vorhandenen Monitor mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set lb monitor <monitorName> <type> -interval <interval> -resptimeout <
    resptimeout>
<!--NeedCopy-->
```

Beispiel:

```
set mon monitor-HTTP-1 HTTP -interval 50 milli
-resptimeout 20 milli
<!--NeedCopy-->
```

So ändern Sie einen vorhandenen Monitor über die grafische Benutzeroberfläche

Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**, und öffnen Sie einen zu ändernden Monitor.

Aktivieren und Deaktivieren von Monitoren

October 5, 2021

Standardmäßig sind Monitore, die an Dienste und Dienstgruppen gebunden sind, aktiviert. Wenn Sie einen Monitor aktivieren, beginnt der Monitor mit der Untersuchung der Dienste, an die er gebunden ist. Wenn Sie einen an einen Dienst gebundenen Monitor deaktivieren, wird der Status, den der Dienst mithilfe der anderen an den Dienst gebundenen Monitore bestimmt. Wenn der Dienst nur an einen Monitor gebunden ist und Sie den Monitor deaktivieren, wird der Status des Dienstes mithilfe des Standardmonitors ermittelt.

So aktivieren Sie einen Monitor mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable lb monitor <monitorName>
<!--NeedCopy-->
```

Beispiel:


```
enable lb mon monitor-HTTP-1
<!--NeedCopy-->
```

So aktivieren Sie einen Monitor mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Wählen Sie einen Monitor aus, und wählen Sie in der Liste Aktion die Option Aktivieren oder Deaktivieren aus.

So deaktivieren Sie einen Monitor mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
disable lb monitor <monitorName>
<!--NeedCopy-->
```

Beispiel:

```
disable lb mon monitor-HTTP-1
<!--NeedCopy-->
```

Monitore aufheben

October 5, 2021

Sie können die Bindung von Monitoren aus einer Service- und Servicegruppe aufheben. Wenn Sie die Bindung eines Monitors von der Servicegruppe aufheben, werden die Monitore von den einzelnen Diensten, die die Servicegruppe bilden, nicht gebunden. Wenn Sie die Bindung eines Monitors an einen Dienst oder eine Servicegruppe aufheben, untersucht der Monitor weder den Dienst noch die Servicegruppe.

Hinweis: Wenn Sie die Bindung aller vom Benutzer konfigurierten Monitore an einen Dienst oder eine Servicegruppe aufheben, ist der Standardmonitor an den Dienst und die Servicegruppe gebunden. Die Standardüberwachung prüft dann den Dienst oder die Servicegruppen.

So trennen Sie die Bindung eines Monitors von einem Dienst über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
unbind lb monitor <monitorName>
<!--NeedCopy-->
```

Beispiel:

```
unbind mon monitor-HTTP-1 Service-HTTP-1
<!--NeedCopy-->
```

So trennen Sie die Bindung eines Monitors von einem Dienst über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > Load Balancing > Dienste**, und öffnen Sie einen zu ändernden Dienst.
2. Klicken Sie in den Abschnitt Monitore, wählen Sie einen Monitor aus und klicken Sie auf **Binden aufheben**.

Monitore entfernen

October 5, 2021

Nachdem Sie einen Monitor, den Sie von seinem Dienst erstellt haben, aufgehoben haben, können Sie diesen Monitor aus der Citrix ADC Konfiguration entfernen. (Wenn ein Monitor an einen Dienst gebunden ist, kann er nicht entfernt werden.)

Hinweis: Wenn Sie Monitore entfernen, die an einen Dienst gebunden sind, ist der Standardmonitor an den Dienst gebunden. Standardmonitore können nicht entfernt werden.

So entfernen Sie einen Monitor mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
rm lb monitor <monitorName> <type>
<!--NeedCopy-->
```

Beispiel:

```
rm lb monitor monitor-HTTP-1 HTTP
<!--NeedCopy-->
```

So entfernen Sie einen Monitor mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Wählen Sie einen Monitor aus und klicken Sie auf **Löschen**.

Monitore anzeigen

October 5, 2021

Sie können die Dienste und Servicegruppen anzeigen, die an einen Monitor gebunden sind. Sie können die Einstellungen eines Monitors überprüfen, um die Citrix ADC Konfiguration zu beheben. Im folgenden Verfahren werden die Schritte zum Anzeigen der Bindungen eines Monitors an die Dienste und Dienstgruppen beschrieben.

So zeigen Sie Monitorbindungen mit der CLI an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show lb monbindings <MonitorName>
<!--NeedCopy-->
```

Beispiel:

```
show lb monbindings monitor-HTTP-1
<!--NeedCopy-->
```


So zeigen Sie Monitorbindungen mit der GUI an

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Wählen Sie einen Monitor aus, und klicken Sie in der Liste Aktion auf **Bindungen anzeigen**.

So zeigen Sie Monitore mit der CLI an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show lb monitor <monitorName>
<!--NeedCopy-->
```

Beispiel:

```
show lb mon monitor-HTTP-1
<!--NeedCopy-->
```

So zeigen Sie Monitore mit der GUI an

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**. Die Details der verfügbaren Monitore werden im Bereich Monitore angezeigt.

Schließen von Monitorverbindungen

October 5, 2021

Die Citrix ADC Appliance sendet Prüfpunkte über die an die Dienste gebundenen Monitore an die Dienste. Standardmäßig folgen der Monitor auf der Appliance und dem physischen Server auch bei Monitorsonden dem vollständigen Handshake-Vorgang. Dieses Verfahren erhöht jedoch den Aufwand für den Überwachungsprozess und ist möglicherweise nicht immer erforderlich.

Für den TCP-Typ-Monitor können Sie die Appliance so konfigurieren, dass eine Monitor-Probe-Verbindung geschlossen wird, nachdem SYN-ACK vom Dienst empfangen wurde. Legen Sie dazu den Wert des Parameters MonitorConnectionClose auf RESET fest. Wenn die Monitor-Sondenverbindung den vollständigen Vorgang durchlaufen soll, setzen Sie den Wert auf FIN.

Hinweis: Die Einstellung MonitorConnectionClose ist nur für Monitore vom Typ TCP und TCP-Standard anwendbar.

So konfigurieren Sie die Schließung der Monitorverbindung mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb parameter -monitorConnectionClose <monitor_conn_close_option>
<!--NeedCopy-->
```

Beispiel

```
set lb parameter -monitorConnectionClose RESET
<!--NeedCopy-->
```

So konfigurieren Sie die Schließung der Monitorverbindung mit dem Konfigurationsdienstprogramm:

1. Navigieren Sie zu **Traffic Management > Load Balancing > Load Balancing-Parameter konfigurieren**.
2. Wählen Sie **FIN** oder **Zurücksetzen** .

Schließen von Monitorverbindungen auf Dienst- oder Servicegruppenebene

Sie können die Appliance auch so konfigurieren, dass eine Monitor-Probe-Verbindung auf Dienst- und Dienstgruppenebene geschlossen wird, indem Sie den Parameter MonConnectionClose festlegen. Wenn dieser Parameter nicht gesetzt ist, wird die Monitorverbindung mit dem Wert geschlossen, der in den globalen Lastausgleichsparametern festgelegt ist. Wenn dieser Parameter auf Dienst- oder Dienstgruppenebene festgelegt ist, wird die Monitorverbindung geschlossen, indem eine Verbindungsabschlussmeldung mit dem FIN oder RESET Bit gesetzt wird, an den Dienst oder die Servicegruppe gesendet wird.

So konfigurieren Sie die Schließung der Monitorverbindung auf Service-Ebene mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <service_name> -monConnectionClose ( RESET | FIN )
<!--NeedCopy-->
```


So konfigurieren Sie die Schließung der Monitorverbindung auf Servicegruppenebene mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1  set serviceGroup <service_name> -monConnectionClose ( RESET | FIN )
2 <!--NeedCopy-->
```

So konfigurieren Sie die Schließung der Monitorverbindung auf Service-Ebene mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienste**.
2. Fügen Sie einen Dienst hinzu oder bearbeiten Sie, und legen Sie in den **Grundeinstellungen**das **Überwachungsverbindungs-Bit**fest.

So konfigurieren Sie die Schließung der Monitorverbindung auf Servicegruppenebene mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.
2. Fügen Sie eine Dienstgruppe hinzu oder bearbeiten Sie sie, und legen Sie in den **Grundeinstellungen**das **Überwachungsverbindungs-Close Bit**fest.

> **Hinweis:** Zum Schließen einer Monitor-Probe-Verbindung mit globalen Lastausgleichsparametern können Sie MonitorConnectionClose auf FIN oder RESET konfigurieren. Wenn Sie den Parameter MonitorConnectionClose auf;
>
> - FIN: Die Appliance führt einen vollständigen TCP-Handshake durch.
> - RESET: Die Appliance schließt die Verbindung, nachdem sie den SYN-ACK vom Dienst erhalten hat.
>
> In der leichteren Version von Citrix ADC CPX ist der Parameterwert MonitorConnectionClose standardmäßig auf RESET festgelegt und kann auf globaler Ebene nicht in FIN geändert werden. Sie können jedoch den Parameter MonitorConnectionClose auf der Service-Ebene in FIN ändern.

Ignorieren der Obergrenze für Clientverbindungen für Monitorsonden

October 5, 2021

Abhängig von Überlegungen wie der Kapazität eines physischen Servers können Sie eine Begrenzung für die maximale Anzahl von Clientverbindungen festlegen, die mit einem beliebigen Dienst

hergestellt werden. Wenn Sie einen solchen Grenzwert für einen Dienst festgelegt haben, beendet die Citrix ADC Appliance das Senden von Anfragen an den Dienst, wenn der Schwellenwert erreicht ist, und setzt das Senden von Verbindungen an den Dienst fort, nachdem die Anzahl der vorhandenen Verbindungen innerhalb der Grenzen liegt. Sie können die Appliance so konfigurieren, dass diese Überprüfung überspringt, wenn sie Monitor-Probe-Verbindungen an einen Dienst sendet.

Hinweis: Sie können die Maximum-Client-Verbindungsprüfung für einen einzelnen Dienst nicht überspringen. Wenn Sie diese Option angeben, gilt sie für alle Monitore, die an alle auf der Citrix ADC Appliance konfigurierten Dienste gebunden sind.

So legen Sie die Option "MaxClients für Monitorverbindungen überspringen" über die Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb parameter -monitorSkipMaxClient (ENABLED|DISABLED)
<!--NeedCopy-->
```

Beispiel:

```
set lb parameter -monitorSkipMaxClient enabled
<!--NeedCopy-->
```

So legen Sie die Option "MaxClients für Monitorverbindungen überspringen" mit der GUI fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Load Balancing-Parameter konfigurieren**.
2. Wählen Sie **MaxClients für die Überwachung von Verbindungen überspringen**aus.

Verwalten einer umfangreichen Bereitstellung

October 5, 2021

Die Citrix ADC Appliance enthält mehrere Funktionen, die hilfreich sind, wenn Sie eine große Lastausgleichsbereitstellung konfigurieren. Anstatt virtuelle Server und Dienste einzeln zu konfigurieren, können Sie Gruppen von virtuellen Servern und Diensten erstellen. Sie können auch eine Reihe von

virtuellen Servern und Diensten erstellen und virtuelle Server- und Dienst-IP-Adressen übersetzen oder maskieren.

Sie können die Persistenz für eine Gruppe virtueller Server festlegen. Sie können Monitore an eine Gruppe von Diensten binden. Durch das Erstellen einer Reihe virtueller Server und Dienste identischen Typs können Sie diese Server in einem einzigen Verfahren einrichten und konfigurieren. Dies verkürzt die für die Konfiguration dieser virtuellen Server und Dienste erforderliche Zeit erheblich.

Durch das Übersetzen oder Maskieren von IP-Adressen können Sie virtuelle Server und Dienste ausschalten. Sie können dann Änderungen an Ihrer Infrastruktur vornehmen, ohne Ihre Service- und virtuellen Serverdefinitionen umfassend neu zu konfigurieren.

Bereiche virtueller Server und Services

October 5, 2021

Wenn Sie den Lastenausgleich konfigurieren, können Sie Bereiche von virtuellen Servern und Diensten erstellen, sodass virtuelle Server und Dienste nicht einzeln konfiguriert werden müssen. Sie können beispielsweise eine einzige Prozedur verwenden, um drei virtuelle Server mit drei entsprechenden IP-Adressen zu erstellen. Wenn mehr als ein Argument einen Bereich verwendet, müssen die Bereiche dieselbe Größe haben.

Im Folgenden sind die Typen von Bereichen aufgeführt, die Sie beim Hinzufügen von Diensten und virtuellen Servern zur Konfiguration angeben können:

- **Numerische Bereiche.** Anstatt eine einzelne Zahl einzugeben, können Sie einen Bereich von fortlaufenden Zahlen angeben.

  Beispielsweise können Sie einen Bereich virtueller Server erstellen, indem Sie eine Start-IP-Adresse angeben, z. B. 10.102.29.30, und dann einen Wert für das letzte Byte eingeben, das den Bereich angibt, z. B. 34. In diesem Beispiel werden fünf virtuelle Server mit IP-Adressen erstellt, die zwischen 10.102.29.30 und 10.102.29.34 liegen.

  Hinweis: Die IP-Adressen der virtuellen Server und Dienste müssen fortlaufend sein.

- **Alphabetische Bereiche.** Anstatt einen wörtlichen Buchstaben einzugeben, können Sie einen Bereich für einen einzelnen Buchstaben ersetzen [,]z. B. Dies führt dazu, dass alle Buchstaben des Bereichs einbezogen werden, in diesem Fall C, D, E, F und G.

  Wenn Sie beispielsweise drei virtuelle Server mit dem Namen haben `Vserver-xVserver-y Vserver-z`, und anstatt sie separat `vserver [x-z]` zu konfigurieren, können Sie sie alle konfigurieren.

Erstellen einer Reihe von virtuellen Servern

So erstellen Sie einen Bereich virtueller Server mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
add lb vserver <name>@ <protocol> -range <rangeValue> <IPAddress> [<
    port>]

add lb vserver <name>@[<rangeValue>]> <protocol> <IPAddress[<rangeValue
    >]> [<port>]
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-2 http -range 6 10.102.29.30 80
<!--NeedCopy-->
```

ODER

```
add lb vserver vserver[P-R] http 10.102.29.[26-28] 80

vserver "vserverP" added

vserver "vserverQ" added

vserver "vserverR" added

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

So erstellen Sie einen Bereich virtueller Server mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
add lb vserver <name>@ <protocol> -range <rangeValue> <IPAddress> [<
    port>]

```



```
add lb vserver <name>@\*\*[\*\*<rangeValue>\*\*]\*\*> <protocol> <
    IPAddress[<rangeValue>]> [<port>]
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-2 http -range 6 10.102.29.30 80
<!--NeedCopy-->
```

ODER

```
add lb vserver vserver[P-R] http 10.102.29.[26-28] 80
vserver "vserverP" added
vserver "vserverQ" added
vserver "vserverR" added
Done
<!--NeedCopy-->
```

So erstellen Sie eine Reihe virtueller Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Fügen Sie einen virtuellen Server hinzu, und geben Sie einen Bereich an.

Erstellen einer Reihe von Dienstleistungen

Wenn Sie einen Bereich für den Dienstnamen angeben, geben Sie auch einen Bereich für die IP-Adresse an.

So erstellen Sie ein Leistungsspektrum mit der CLI

Geben Sie an der Eingabeaufforderung den Befehl ein:

```
add service <name>@ <IP>@ <protocol> <port>
<!--NeedCopy-->
```

Beispiel:


```
> add service serv[1-3] 10.102.29.[102-104] http 80
service ”serv1” added
service ”serv2” added
service ”serv3” added
 Done
<!--NeedCopy-->
```

Konfigurieren von Dienstgruppen

October 5, 2021

Durch die Konfiguration einer Servicegruppe können Sie eine Gruppe von Diensten so einfach wie ein einzelner Dienst verwalten. Wenn Sie beispielsweise eine Option wie Komprimierung, Integritätsüberwachung oder ordnungsmiges Herunterfahren für eine Servicegruppe aktivieren oder deaktivieren, wird die Option für alle Mitglieder der Dienstgruppe aktiviert.

Nachdem Sie eine Dienstgruppe erstellt haben, können Sie sie an einen virtuellen Server binden und der Gruppe Dienste hinzufügen. Sie können Monitore auch an Servicegruppen binden.

Die Mitglieder einer Dienstgruppe werden durch IP-Adresse oder Servernamen identifiziert.

Die Verwendung von DBS-Gruppenmitgliedern (Domain Name Based Service) ist von Vorteil, da Sie das Mitglied auf der Citrix ADC Appliance nicht neu konfigurieren müssen, wenn sich die IP-Adresse des Mitglieds ändert. Die Appliance erkennt solche Änderungen automatisch über den konfigurierten Nameserver. Diese Funktion ist in Cloud-Szenarien nützlich, in denen der Dienstanbieter einen physischen Server ändern oder die IP-Adresse für einen Dienst ändern kann. Wenn Sie ein DBS-Gruppenmitglied angeben, lernt die Appliance die IP-Adresse dynamisch.

Sie können sowohl IP-basierte als auch DBS-Mitglieder an dieselbe Dienstgruppe binden.

Hinweis: Wenn Sie DBS-Dienstgruppenmitglieder verwenden, stellen Sie sicher, dass entweder ein Nameserver angegeben ist oder ein DNS-Server auf der Citrix ADC Appliance konfiguriert ist. Ein Domänenname wird nur in eine IP-Adresse aufgelöst, wenn der entsprechende Adressdatensatz auf der Appliance oder dem Nameserver vorhanden ist.

Erstellen von Servicegruppen

Sie können bis zu 8192 Dienstgruppen auf der Citrix ADC Appliance konfigurieren.

So erstellen Sie eine Dienstgruppe mit der Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add servicegroup <ServiceGroupName> <Protocol>
<!--NeedCopy-->
```

Beispiel:

```
add servicegroup Service-Group-1 HTTP
<!--NeedCopy-->
```

So erstellen Sie eine Dienstgruppe mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**, und fügen Sie eine Servicegruppe hinzu.

Binden einer Dienstgruppe an einen virtuellen Server

Wenn Sie eine Dienstgruppe an einen virtuellen Server binden, sind die Mitgliedsdienste an den virtuellen Server gebunden.

So binden Sie eine Dienstgruppe mit der Befehlszeilenschnittstelle an einen virtuellen Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name>@ <serviceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver Vserver-LB-1 Service-Group-1
<!--NeedCopy-->
```

So binden Sie eine Dienstgruppe über die GUI an einen virtuellen Server

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie unter Erweiterte Einstellungen die Option **Dienstgruppen**aus.

Binden eines Mitglieds an eine Servicegruppe

Durch das Hinzufügen von Diensten zu einer Dienstgruppe kann die Dienstgruppe die Server verwalten. Sie können die Server zu einer Dienstgruppe hinzufügen, indem Sie die IP-Adressen oder die Namen der Server angeben.

Wenn Sie in der GUI ein domänennamenbasiertes Dienstgruppenmitglied hinzufügen möchten, wählen Sie **Serverbasiert**aus.

Mit dieser Option können Sie jeden Server hinzufügen, dem ein Name zugewiesen wurde, unabhängig davon, ob es sich bei dem Namen um eine IP-Adresse oder einen vom Benutzer zugewiesenen Namen handelt.

So fügen Sie einer Dienstgruppe mit der Befehlszeilenschnittstelle Mitglieder hinzu

Um eine Dienstgruppe zu konfigurieren, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind servicegroup <serviceGroupName> (<IP>@ | <serverName>) <port>
<!--NeedCopy-->
```

Beispiele:

```
bind servicegroup Service-Group-1 10.102.29.30 80

bind servicegroup Service-Group-2 1000:0000:0000:0000:0005:0600:700a
    :888b 80

bind servicegroup CitrixEdu s1.citrite.net
<!--NeedCopy-->
```

So fügen Sie einer Dienstgruppe mit dem Konfigurationsdienstprogramm Mitglieder hinzu

1. Navigieren Sie zu **Traffic Management > Load Balancing > Dienstgruppen**, und öffnen Sie eine Dienstgruppe.
2. Klicken Sie in den Abschnitt Dienstgruppe, und führen Sie eine der folgenden Aktionen aus:
   - Um ein IP-basiertes Dienstgruppenmitglied hinzuzufügen, wählen Sie IP-basiert aus.
   - Um ein servernamenbasiertes Dienstgruppenmitglied hinzuzufügen, wählen Sie Serverbasiert aus.

Wenn Sie ein Domänennamenbasiertes Dienstgruppenmitglied hinzufügen möchten, wählen Sie **Serverbasiert**aus. Mit dieser Option können Sie jeden Server hinzufügen, dem ein Name zugewiesen wurde, unabhängig davon, ob es sich bei dem Namen um eine IP-Adresse oder einen vom Benutzer zugewiesenen Namen handelt.

3. Wenn Sie ein neues IP-basiertes Element hinzufügen, geben Sie im Textfeld IP-Adresse die IP-Adresse ein. Wenn die IP-Adresse IPv6-Format verwendet, aktivieren Sie das Kontrollkästchen IPv6, und geben Sie die Adresse in das Textfeld IP-Adresse ein.

   Hinweis: Sie können einen Bereich von IP-Adressen hinzufügen. Die IP-Adressen im Bereich müssen fortlaufend sein. Geben Sie den Bereich an, indem Sie die Start-IP-Adresse in das Textfeld IP-Adresse eingeben (z. B. 10.102.29.30). Geben Sie das Endbyte des IP-Adressbereichs im Textfeld unter Bereich an (z. B. 35). Geben Sie im Textfeld Port den Port ein (z. B. 80), und klicken Sie dann auf Hinzufügen.

4. Klicken Sie auf Erstellen.

Binden eines Monitors an eine Servicegruppe

Wenn Sie eine Dienstgruppe erstellen, wird der Standardmonitor des für die Gruppe geeigneten Typs automatisch an sie gebunden. Monitore untersuchen regelmäßig die Server in der Dienstgruppe, an die sie gebunden sind, und aktualisieren den Status der Dienstgruppen.

Sie können einen anderen Monitor Ihrer Wahl an die Servicegruppe binden.

So binden Sie einen Monitor mit der Befehlszeilenschnittstelle an eine Dienstgruppe

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind serviceGroup <serviceGroupName> -monitorName <string> -monState (
     ENABLED | DISABLED)
2 <!--NeedCopy-->
```

Beispiel:

```
1 bind serviceGroup Service-Group-1 -monitorName monitor-HTTP-1
2 <!--NeedCopy-->
```

An einen Bindungsmonitor an eine Servicegruppe mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.

2. Öffnen Sie eine Dienstgruppe, und klicken Sie unter Erweiterte Einstellungen auf **Monitore**.

Nach dem Deaktivieren und Aktivieren eines virtuellen Servers den ursprünglichen Status eines Dienstgruppenmitglieds beibehalten

Ab Build 64.x können Sie mit der neuen globalen Option —RetainDisableServer den Status eines Dienstgruppenmitglieds beibehalten, wenn ein Server deaktiviert und erneut aktiviert wird.

Zuvor änderte sich der Status eines Mitglieds unter den folgenden Bedingungen von DISABLED in ENABLED:

- Zwei Anwendungen werden auf demselben Port auf einem virtuellen Server bereitgestellt.
- Zwei Dienstgruppen mit einem gemeinsamen Mitglied sind an diesen virtuellen Server gebunden, und das gemeinsame Mitglied ist in einer Gruppe aktiviert und in der anderen deaktiviert.
- Der Server ist deaktiviert und dann wieder aktiviert.

Unter diesen Bedingungen werden durch das Deaktivieren des Servers alle Mitglieder der Dienstgruppe deaktiviert, und das erneute Aktivieren des Servers werden standardmäßig alle Mitglieder unabhängig von ihrem früheren Status aktiviert. Um die Mitglieder wieder in den ursprünglichen Status zurück zu setzen, müssen Sie diese Mitglieder in der Servicegruppe manuell deaktivieren. Dies ist eine umständliche Aufgabe und anfällig für Fehler.

Verwalten von Servicegruppen

October 5, 2021

Sie können die Einstellungen der Dienste in einer Dienstgruppe ändern und Aufgaben wie Aktivieren, Deaktivieren und Entfernen von Dienstgruppen ausführen. Sie können auch die Bindung von Mitgliedern aus einer Dienstgruppe aufheben. Weitere Informationen zu Dienstgruppen finden Sie unter Konfigurieren von Dienstgruppen.

Ändern einer Servicegruppe

Sie können die Attribute von Dienstgruppenmitgliedern ändern. Sie können mehrere Attribute der Dienstgruppe festlegen, z. B. den maximalen Client, Sure Connect und die Komprimierung. Die Attribute werden auf den einzelnen Servern in der Servicegruppe festgelegt. Sie können keine Parameter für die Dienstgruppe festlegen, z. B. Transportinformationen (IP-Adresse und Port), Gewicht und Server-ID.

Hinweis: Ein Parameter, den Sie für eine Dienstgruppe festlegen, wird auf die Mitgliedsserver in der Gruppe angewendet, nicht auf einzelne Dienste.

So ändern Sie eine Dienstgruppe mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl mit einem oder mehreren der optionalen Parameter ein:

```
set servicegroup <serviceGroupName> [-type <type>] [-maxClient <
    maxClient>] [-maxReq <maxReq>] [-cacheable (YES|NO)] [-cip (ENABLED|
    DISABLED)] [-cipHeader <cipHeader>] [-usip (YES|NO)] [-sc (ON|OFF)]
    [-sp (ON|OFF)] [-cltTimeout <cltTimeout>] [-svrTimeout <svrTimeout>]
     [-cka (YES|NO)] [-TCPB (YES|NO)] [-CMP (\*\*YES\*\*|\*\*NO\*\*)] [-
    maxBandwidth <maxBandwidth>] [-maxThreshold <maxThreshold>] [-state
    (ENABLED|DISABLED)] [-downStateFlush (ENABLED|DISABLED)
<!--NeedCopy-->
```

Beispiel:

```
set servicegroup Service-Group-1 -type TRANSPARENT

set servicegroup Service-Group-1 -maxClient 4096

set servicegroup Service-Group-1 -maxReq 16384

set servicegroup Service-Group-1 -cacheable YES
<!--NeedCopy-->
```

So ändern Sie eine Dienstgruppe mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service Groups**, und öffnen Sie die zu ändernde Servicegruppe.

Entfernen einer Dienstgruppe

Wenn Sie eine Dienstgruppe entfernen, behalten die an die Gruppe gebundenen Server ihre individuellen Einstellungen bei und sind weiterhin auf der Citrix ADC Appliance vorhanden.

So entfernen Sie eine Dienstgruppe mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
rm servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
rm servicegroup Service-Group-1
<!--NeedCopy-->
```

So entfernen Sie eine Dienstgruppe mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.
2. Wählen Sie eine Dienstgruppe aus, und klicken Sie auf **Löschen**.

Bindung eines Mitglieds aus einer Servicegruppe aufheben

Wenn Sie ein Mitglied von der Servicegruppe aufheben, gelten die für die Dienstgruppe festgelegten Attribute nicht mehr für das Mitglied, das Sie nicht gebunden haben. Die Mitgliedsdienste behalten jedoch ihre individuellen Einstellungen bei und existieren weiterhin auf der Citrix ADC Appliance.

So heben Sie die Bindung von Mitgliedern aus einer Dienstgruppe mit der Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
unbind servicegroup <serviceGroupName> <IP>@ [<port>]
<!--NeedCopy-->
```

Beispiel:

```
unbind servicegroup Service-Group-1 10.102.29.30 80
<!--NeedCopy-->
```

So heben Sie die Bindung von Mitgliedern aus einer Dienstgruppe mit dem Konfigurationsdienstprogramm auf

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.

2. Öffnen Sie eine Dienstgruppe, und klicken Sie auf den Abschnitt Dienstgruppenmitglieder.
3. Wählen Sie ein Dienstgruppenmitglied aus, und klicken Sie auf **Bindung aufheben**.

Aufheben der Bindung einer Dienstgruppe von einem virtuellen Server

Wenn Sie die Bindung einer Dienstgruppe von einem virtuellen Server aufheben, werden die Mitgliedsdienste vom virtuellen Server nicht gebunden und sind weiterhin auf der Citrix ADC Appliance vorhanden.

So heben Sie die Bindung einer Dienstgruppe von einem virtuellen Server mit der Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
unbind lb vserver <name>@ <ServiceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
unbind lb vserver Vserver-LB-1 Service-Group-1
<!--NeedCopy-->
```

So heben Sie die Bindung einer Dienstgruppe von einem virtuellen Server mit dem Konfigurationsdienstprogramm auf

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Öffnen Sie den virtuellen Server, und klicken Sie auf den Abschnitt Dienstgruppe.
3. Wählen Sie die Dienstgruppe aus, und klicken Sie auf **Bindung aufheben**.

Aufheben der Bindung von Monitoren aus Servicegruppen

Wenn Sie die Bindung eines Monitors an eine Servicegruppe aufheben, überwacht der Monitor, den Sie nicht mehr die einzelnen Dienste, die die Gruppe bilden.

So heben Sie die Bindung eines Monitors von einer Servicegruppe mit der Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
unbind serviceGroup <serviceGroupName> -monitorName <string>
<!--NeedCopy-->
```

Beispiel:

```
unbind serviceGroup Service-Group-1 -monitorName monitor-HTTP-1
<!--NeedCopy-->
```

So heben Sie die Bindung eines Monitors von einer Servicegruppe mit dem Konfigurationsdienstprogramm auf

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.
2. Öffnen Sie eine Dienstgruppe, und klicken Sie auf den Abschnitt Monitore.
3. Wählen Sie einen Monitor aus, und klicken Sie auf **Bindung aufheben**.

Aktivieren oder Deaktivieren einer Dienstgruppe

Wenn Sie eine Dienstgruppe und die Server aktivieren, werden die zur Dienstgruppe gehörenden Dienste aktiviert. Wenn ein Dienst, der zu einer Dienstgruppe gehört, aktiviert ist, sind die Dienstgruppe und der Dienst aktiviert. Standardmäßig sind Dienstgruppen aktiviert.

Nachdem Sie einen aktivierten Dienst deaktiviert haben, können Sie den Dienst mit dem Konfigurationsdienstprogramm oder der Befehlszeile anzeigen, um die verbleibende Zeit anzuzeigen, bevor der Dienst heruntergefahren wird.

So deaktivieren Sie eine Dienstgruppe mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
disable servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
disable servicegroup Service-Group-1
<!--NeedCopy-->
```


So deaktivieren Sie eine Dienstgruppe mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.
2. Wählen Sie eine Dienstgruppe aus, und klicken Sie in der Liste Aktion auf **Deaktivieren**.

So aktivieren Sie eine Dienstgruppe mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
enable servicegroup Service-Group-1
<!--NeedCopy-->
```

So aktivieren Sie eine Dienstgruppe mit dem Konfigurationsdienstprogramm

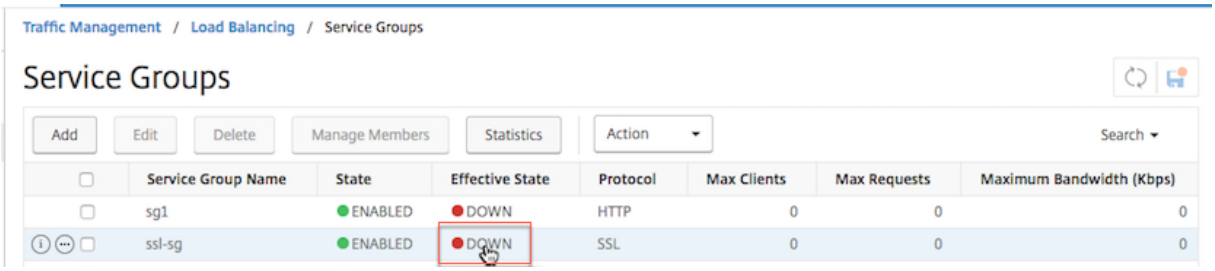
1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.
2. Wählen Sie eine Dienstgruppe aus, und klicken Sie in der Liste Aktion auf **Aktivieren**.

Anzeigen des Status von Servicegruppenmitgliedern

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.

Auf der Seite “Dienstgruppen” wird in der Spalte **Effektiver Status** der Status der Dienstgruppen angezeigt. Der Status UP/DOWN in der Spalte **Effektiver Status** ist anklickbar. Sie können auf den Status klicken und die Liste der Mitglieder zusammen mit ihrem Status in derselben Ansicht abrufen. Wählen Sie ein Mitglied aus und klicken Sie auf die Schaltfläche **Monitor-Details**, um den Grund für den Status “DOWN” anzuzeigen.

Hinweis: Vor dem Release von NetScaler 12.0 Build 56.20 war der Status in der Spalte **Effektiver Status** nicht anklickbar.



Anzeigen der Eigenschaften einer Servicegruppe

Sie können die folgenden Einstellungen der konfigurierten Dienstgruppen anzeigen:

- Name
- IP-Adresse
- Status
- Protokoll
- Maximale Client-Verbindungen
- Maximale Anfragen pro Verbindung
- Maximale Bandbreite
- Schwellenwert überwachen

Das Anzeigen der Details der Konfiguration kann hilfreich sein, um die Konfiguration zu beheben.

So zeigen Sie die Eigenschaften einer Dienstgruppe mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um die Gruppeneigenschaften oder die Eigenschaften und die Gruppenmitglieder anzuzeigen:

```
show servicegroup <ServiceGroupName>

show servicegroup <ServiceGroupName> -includemembers
<!--NeedCopy-->
```

Beispiel:

```
show servicegroup Service-Group-1
<!--NeedCopy-->
```

So zeigen Sie die Eigenschaften einer Dienstgruppe mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.
2. Klicken Sie auf den Pfeil neben der Dienstgruppe.

Servicegruppenstatistiken anzeigen

Sie können Service-Gruppen-Statistikdaten anzeigen, z. B. die Rate der Anforderungen, Antworten, Anforderungsbytes und Antwortbytes. Die Citrix ADC Appliance verwendet die Statistiken einer Dienstgruppe, um die Belastung der Dienste auszugleichen.

So zeigen Sie die Statistiken einer Dienstgruppe mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat servicegroup <ServiceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
stat servicegroup Service-Group-1
<!--NeedCopy-->
```

So zeigen Sie die Statistiken einer Dienstgruppe mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.
2. Wählen Sie eine Dienstgruppe aus, und klicken Sie auf **Statistiken**.

An eine Dienstgruppe gebundene virtuelle Server mit Lastenausgleich

In umfangreichen Bereitstellungen kann dieselbe Servicegruppe an mehrere virtuelle Server mit Lastenausgleich gebunden werden. In einem solchen Fall können Sie, anstatt jeden virtuellen Server anzuzeigen, um die Dienstgruppe anzuzeigen, an die er gebunden ist, eine Liste aller virtuellen Lastenausgleichsserver anzeigen, die an eine Dienstgruppe gebunden sind. Sie können die folgenden Details zu jedem virtuellen Server anzeigen:

- Name
- Status
- IP-Adresse
- Port

So zeigen Sie die virtuellen Server an, die an eine Dienstgruppe gebunden sind, mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die virtuellen Server anzuzeigen, die an eine Dienstgruppe gebunden sind:

```
show servicegroupbindings <serviceGroupName>
<!--NeedCopy-->
```


Beispiel:

```
> show servicegroupbindings SVCGRPDTLS
SVCGRPDTLS - State :ENABLED
1) Test-pers (10.10.10.3:80) - State : DOWN
2) BRVSERV (10.10.1.1:80) - State : DOWN
3) OneMore (10.102.29.136:80) - State : DOWN
4) LBVIP1 (10.102.29.66:80) - State : UP
Done
>
<!--NeedCopy-->
```

So zeigen Sie die virtuellen Server an, die an eine Dienstgruppe gebunden sind, mit dem Konfigurationsdienstprogramm an

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.
2. Wählen Sie eine Dienstgruppe aus, und klicken Sie in der Liste Aktion auf **Bindungen anzeigen**.

Konfigurieren eines gewünschten Satzes von Servicegruppenmitgliedern für eine Servicegruppe in einem NITRO API-Aufruf

October 5, 2021

Es wird Unterstützung hinzugefügt, um eine gewünschte Gruppe von Service-Gruppenmitgliedern für eine Service-Gruppe in einem NITRO API-Aufruf zu konfigurieren. Zur Unterstützung dieser Konfiguration wird eine neue API, die die gewünschte Zustands-API, hinzugefügt. Mit der API für den gewünschten Zustand können Sie:

- Geben Sie eine Liste von Dienstgruppenmitgliedern in einer einzelnen PUT-Anforderung für die Ressource servicegroupmemberlist_binding an.
- Geben Sie ihr Gewicht und ihren Status (optional) in dieser PUT-Anforderung an.
- Effektive Synchronisierung der Appliance-Konfiguration mit Bereitstellungsänderungen um Anwendungsserver.

Die Citrix ADC Appliance vergleicht die angeforderte gewünschte Elementgruppe mit der konfigurierten Elementgruppe. Dann bindet es automatisch die neuen Elemente und entbindet die Elemente, die nicht in der Anforderung vorhanden sind.

Hinweis:

- Diese Funktion wird nur für Service-Gruppen vom Typ`API`.
- Sie können IP-adressbasierte Dienste nur mit der API für den gewünschten Zustand binden. Domänennamenbasierte Dienste sind nicht zulässig.
- Zuvor kann nur ein Servicegruppenmitglied in einem NITRO -Aufruf gebunden werden.

> **Wichtig**
>
> Die gewünschte State-API für die ServiceGroup-Mitgliedschaft wird bei der Citrix ADC Clusterbereitstellung unterstützt.

Anwendungsfall: Synchronisieren von Bereitstellungsänderungen mit Citrix ADC Appliance in großen Bereitstellungen, z. B. Kubernetes

In großen und hochdynamischen Bereitstellungen (z. B. Kubernetes) besteht die Herausforderung darin, die Appliance-Konfiguration mit der Geschwindigkeit der Änderungen der Bereitstellungen auf dem neuesten Stand zu halten, um den Anwendungsdatenverkehr genau zu bedienen. In solchen Bereitstellungen sind Controller (Ingress oder E-W Controller) für die Aktualisierung der ADC-Konfiguration verantwortlich. Wann immer Änderungen an der Bereitstellung vorgenommen werden, `kube-api server` sendet den effektiven Satz von Endpunkten über "Endpunkte-Ereignis" an den Controller. Der Controller verwendet den Read-Delta-Modify-Ansatz, bei dem er Folgendes durchführt:

- Ruft den aktuell konfigurierten Endpunktsatz (Dienstgruppenmitgliedsatz einer Dienstgruppe) für den Dienst von der ADC-Appliance ab.
- Vergleicht den konfigurierten Endpunktsatz mit dem Satz im empfangenen Ereignis.
- Bindet die neuen Endpunkte (Servicegruppenmitglieder) oder entbindet die gelöschten Endpunkte.

Da die Änderungsrate und die Größe der Dienste in dieser Umgebung hoch ist, ist diese Konfigurationsmethode nicht effizient und kann Konfigurationsupdates verzögern.

Die gewünschte Status-API löst das Problem, indem sie die beabsichtigte Mitgliedergruppe für eine Servicegruppe in einer einzigen API akzeptiert und die Konfiguration effektiv aktualisiert.

Erstellen einer Service-Gruppe vom Typ-API mit der CLI

Geben Sie an der Eingabeaufforderung;

```
add serviceGroup <serviceGroupName>@ <serviceType> [-autoScale <
    autoScale>]
```

Beispiel:


```
add serviceGroup svg1 HTTP -autoScale API
```

Sie können die Parameterautodisablegraceful, autoDisabledelay und autoScale und konfigurieren, indem Sie den Befehl serviceGroup hinzufügen oder den Befehl serviceGroup festlegen.

```
add serviceGroup <serviceGroupName>@ <serviceType> [-autoScale <
    autoScale>] [-autoDisablegraceful ( YES | NO)] [-autoDisabledelay <
    secs>]

add serviceGroup <serviceGroupName>@ <serviceType> [-autoScale (API |
    CLOUD | DISABLED| DNS |POLICY)]

set serviceGroup <serviceGroupName [-autoDisablegraceful ( YES | NO)]
    [-autoDisabledelay <secs>]

set serviceGroup <serviceGroupName [-autoScale (API |CLOUD | DISABLED|
    DNS |POLICY)]
```

Beispiel:

```
add serviceGroup svg1 HTTP autoDisablegraceful YES -autoDisabledelay
    100

add serviceGroup svg1 HTTP -autoScale API

set serviceGroup svg1 -autoDisablegraceful  YES -autoDisabledelay 100

set serviceGroup svg1 -autoScale API
```

Argumente

autoDisablegraceful

Zeigt ein ordnungsgemäßes Herunterfahren des Dienstes an. Wenn diese Option aktiviert ist, wartet die Appliance darauf, dass alle ausstehenden Verbindungen zu diesem Dienst geschlossen werden, bevor der Dienst gelöscht wird. Für Clients, die bereits eine dauerhafte Sitzung auf dem System haben, werden neue Verbindungen oder Anforderungen weiterhin an diesen Dienst gesendet. Das Dienstmitglied wird nur gelöscht, wenn keine ausstehenden Verbindungen vorhanden sind. Standardwert: NO

autoDisabledelay

Gibt die zulässige Zeit (in Sekunden) für ein ordnungsgemäßes Herunterfahren an. Während dieser Zeit werden neue Verbindungen oder Anforderungen an diesen Dienst für Clients gesendet, die bereits eine dauerhafte Sitzung auf dem System haben. Verbindungen oder Anforderungen von neuen Clients, die keine Persistenzsitzungen auf dem System haben, werden nicht an den Dienst gesendet. Stattdessen werden sie unter anderen verfügbaren Diensten lastausgeglichen. Nach Ablauf der Verzögerungszeit wird das Dienstmitglied gelöscht.

Autoscale-API

Aktiviert die Verwendung der API für den gewünschten Status, um die Elementgruppe an eine beabsichtigte Dienstgruppe zu binden. Sie können die Dienstgruppe von nicht automatisch skalieren auf den Typ “Gewünschte Zustands-API” festlegen, wenn alle angegebenen Bedingungen übereinstimmen.

Der Befehl “ServiceGroup automatisch skalieren festlegen” schlägt möglicherweise fehl, wenn die vorhandenen Elementbindungen eine der folgenden Bedingungen erfüllen:

- Wenn der an die Dienstgruppe gebundene Server entweder ein Nameserver oder ein domänenbasierter Server ist.
- Wenn der Name des an die Dienstgruppe gebundenen Servers eine IP-Adresse ist, muss er mit der tatsächlichen Server-IP-Adresse übereinstimmen. Im folgenden Beispiel stimmen der Servername und die Server-IP-Adresse nicht überein.
  - **CLI:***Server-IP-Adresse Servernamen*hinzufügen
  - **Beispiel:** add server 1.2.3.4 4.3.2.1
- Wenn der Name des Loopback-Servers einen anderen Wert als 127.0.0.1 oder 0000:0000:0000:0000:0000:000 hat.
- Wenn Sie verschiedene Arten von Autoscale (Cloud, API, DNS und Policy) in einem Satz auswählen serviceGroup-Befehl und fügen Sie den Befehl “ServiceGroup” hinzu.

Wichtig:

- Die Parameter AutoDisableGraceful und AutoDisableDelay sind nur für die Dienstgruppen des Typs “API” und “CLOUD” anwendbar.
- Wenn die Parameter autoDisablegraceful oder autoDisabledelay nicht konfiguriert sind, werden Dienstmitglieder sofort gelöscht.

Bindung eines Servicegruppenmitglieds ordnungsgemäß aufheben

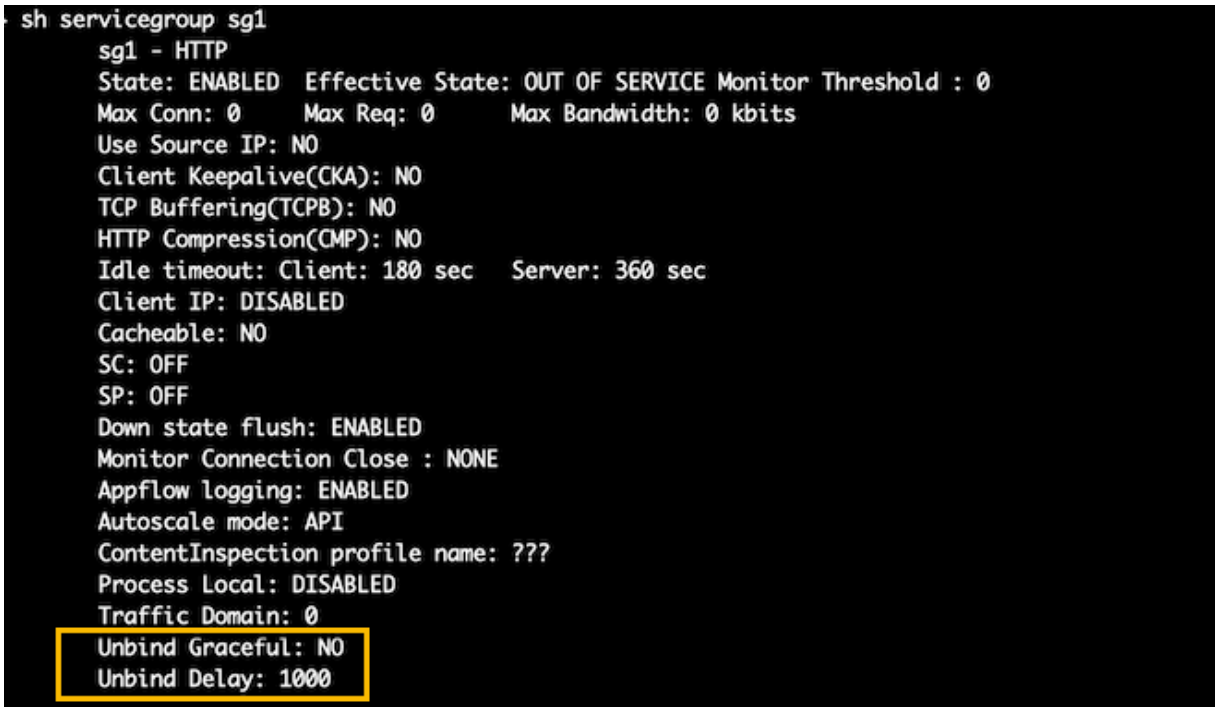
Wenn sich eines der Dienstgruppenmitglieder nicht in der Liste des gewünschten Zustands befindet, werden diese Mitglieder aufgrund der Parameterkonfiguration`autoDisablegraceful` oder `autoDisabledelay` ordnungsgemäß ungebunden.

- Wenn einer dieser Parameter festgelegt ist, wird das Dienstgruppenmitglied ordnungsgemäß ungebunden.
- Wenn keiner dieser Parameter festgelegt ist, wird das Dienstgruppenmitglied sofort ungebunden.

Hinweis:

- Dienstgruppenmitglieder, die für “ordnungsgemäß unbind” identifiziert wurden, werden nur angezeigt, wenn der Befehl show service group ausgeführt wird.
- Sie können keinen Vorgang (z. B. Set, Unset) für das Dienstgruppenmitglied ausführen, das für die ordnungsgemäße Aufheben der Bindung identifiziert wurde.

Die folgende Abbildung zeigt ein Beispiel für den Befehl show service group.

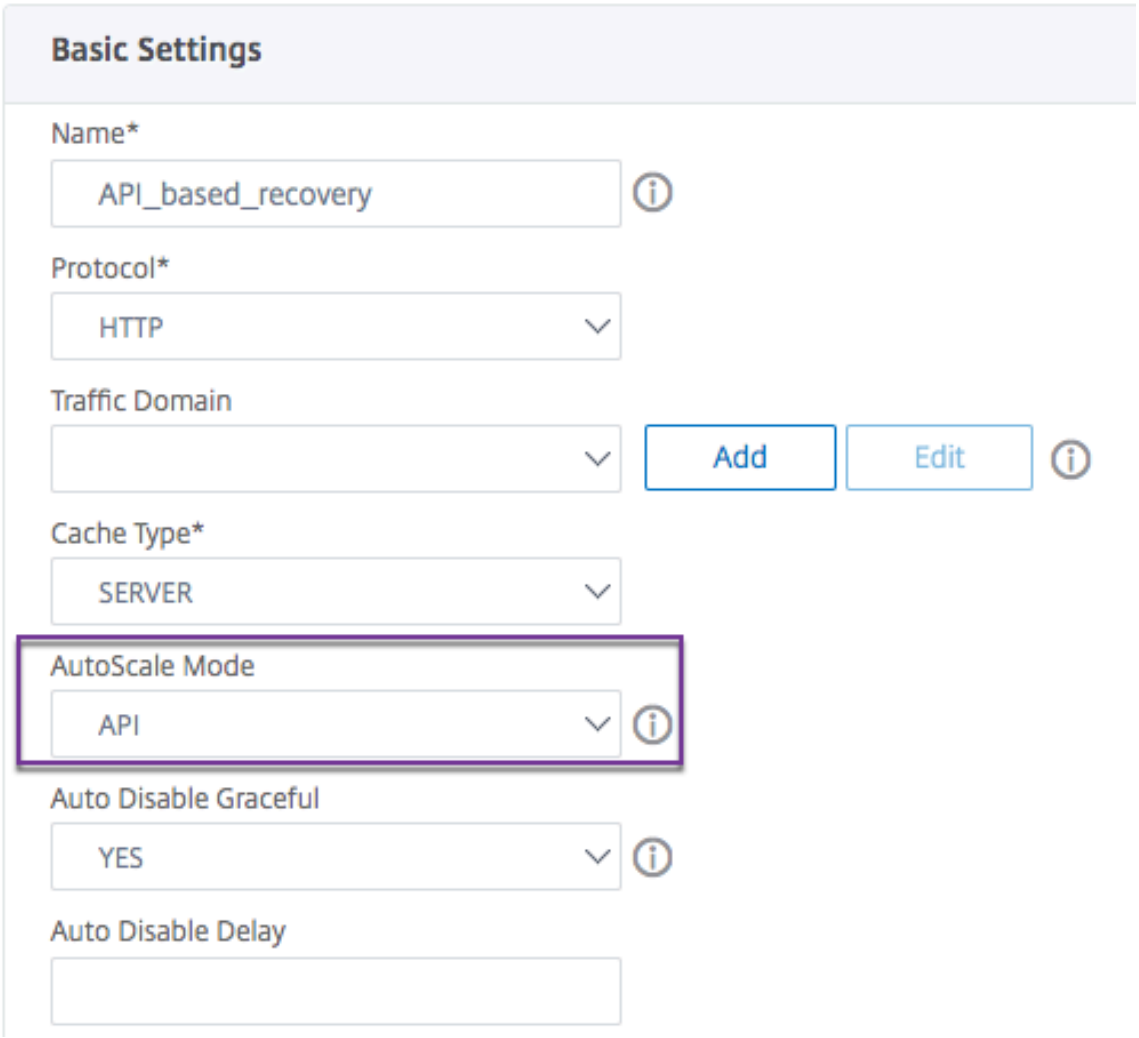


Erstellen einer Service-Gruppe vom Typ-API mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Service Groups**, und klicken Sie auf **Hinzufügen**.
2. Wählen Sie für **AutoScale Mode** die Option **API** aus.

Konfigurieren eines ordnungsgemäßen Herunterfahrens oder einer Zeitverzögerung für eine API-Typ-Servicegruppe mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Dienstgruppen**.



2. Wählen Sie für **AutoScale Mode** die Option **API** aus.
3. Wählen Sie unter **Auto Disable Graceful** die Option **YES** aus.
4. Geben Sie unter **Automatische Deaktivierungsverzögerung** die Wartezeit für ein ordnungsgemäßes Herunterfahren ein.

Hinweis: Die Felder **Auto Disable Gracefu** oder **Automatische Anzeigeverzögerung** sind nur aktiviert, wenn Sie für **AutoScale Mode** die Option **API** oder **CLOUD** auswählen.

Konfigurieren der automatischen domänenbasierten Dienstgruppenskalierung

February 24, 2022

Eine domänenbasierte Dienstgruppe besteht aus Mitgliedern, deren IP-Adressen durch Auflösen der

Domänennamen von Servern abgerufen werden, die an die Dienstgruppe gebunden sind. Die Domänennamen werden von einem Nameserver aufgelöst, dessen Details Sie auf der Appliance konfigurieren. Eine domänenbasierte Dienstgruppe kann auch Mitglieder auf der Grundlage von IP-Adressen enthalten.

Der Prozess der Namensauflösung für einen domänenbasierten Server gibt möglicherweise mehr als eine IP-Adresse zurück. Die Anzahl der IP-Adressen in der DNS-Antwort wird durch die Anzahl der Adresseinträge (A) bestimmt, die für den Domänennamen auf dem Nameserver konfiguriert sind. Selbst wenn der Namensauflösungsprozess mehrere IP-Adressen zurückgibt, ist nur eine IP-Adresse an die Dienstgruppe gebunden. Um eine Servicegruppe nach oben oder nach unten zu skalieren, müssen Sie andere domänenbasierte Server manuell an bzw. von der Servicegruppe binden und aufheben.

Sie können jedoch eine domänenbasierte Dienstgruppe so konfigurieren, dass sie automatisch basierend auf dem vollständigen Satz von IP-Adressen skaliert wird, der von einem DNS-Nameserver für einen domänenbasierten Server zurückgegeben wird. Um die automatische Skalierung zu konfigurieren, aktivieren Sie beim Binden eines domänenbasierten Servers an eine Dienstgruppe die automatische Skalierungsoption. Im Folgenden finden Sie die Schritte zum Konfigurieren einer domänenbasierten Dienstgruppe, die automatisch skaliert:

- Fügen Sie einen Nameserver zum Auflösen von Domänennamen hinzu. Weitere Informationen zum Konfigurieren eines Nameservers auf der Appliance finden Sie unter Hinzufügen eines Nameservers.
- Fügen Sie einen domänenbasierten Server hinzu. Informationen zum Hinzufügen eines domänenbasierten Servers finden Sie unter Konfigurieren eines Serverobjekts.
- Fügen Sie eine Dienstgruppe hinzu, und ordnen Sie den domänenbasierten Server der Dienstgruppe zu, wobei die Autoscale-Option auf DNS festgelegt ist. Informationen zum Hinzufügen einer Dienstgruppe finden Sie unter Konfigurieren von Dienstgruppen.

Wenn ein domänenbasierter Server an eine Dienstgruppe gebunden ist und die Option für die automatische Skalierung auf der Bindung festgelegt ist, werden automatisch ein UDP-Monitor und ein TCP-Monitor erstellt und an den domänenbasierten Server gebunden. Die beiden Monitore fungieren als Resolver. Der TCP-Monitor ist standardmäßig deaktiviert, und die Appliance verwendet den UDP-Monitor, um DNS-Abfragen an den Namenserver zu senden, um den Domänennamen aufzulösen. Wenn die DNS-Antwort gekürzt wird (das TC-Flag auf 1 gesetzt ist), greift die Appliance auf TCP zurück und verwendet den TCP-Monitor, um die DNS-Abfragen über TCP zu senden. Danach verwendet die Appliance weiterhin nur den TCP-Monitor.

Die DNS-Antwort des Nameservers kann mehrere IP-Adressen für den Domainnamen enthalten. Wenn die automatische Skalierungsoption festgelegt ist, fragt die Appliance jede der IP-Adressen mithilfe des Standardmonitors ab und nimmt dann nur die IP-Adressen in die Dienstgruppe auf, die aktiv und verfügbar sind. Nachdem die IP-Adresseinträge, wie durch ihre Time-to-Live (TTL) -Werte definiert, ablaufen, fragt der UDP-Monitor (oder der TCP-Monitor, falls die Appliance wieder

den TCP-Monitor verwendet hat) den Nameserver nach der Domänenauflösung ab und schließt alle neuen IP-Adressen in der Dienstgruppe ein. Wenn eine IP-Adresse, die Teil der Dienstgruppe ist, in der DNS-Antwort nicht vorhanden ist, entfernt die Appliance diese Adresse aus der Dienstgruppe, nachdem vorhandene Verbindungen zum Gruppenmitglied ordnungsgemäß geschlossen wurden. In diesem Prozess können keine neuen Verbindungen mit dem Mitglied hergestellt werden. Wenn ein Domainname, der in der Vergangenheit erfolgreich aufgelöst wurde, zu einer NXDOMAIN-Antwort führt, werden alle mit dieser Domäne verknüpften Dienstgruppenmitglieder entfernt.

Statische (auf IP-Adressen basierende) Mitglieder und dynamisch skalierende domänenbasierte Mitglieder können in einer Dienstgruppe koexistieren. Sie können auch Mitglieder mit unterschiedlichen Domänennamen mit der Option für die automatische Skalierung an eine Dienstgruppe binden. Jeder Domänenname, der einer Dienstgruppe zugeordnet ist, muss jedoch innerhalb der Dienstgruppe eindeutig sein. Sie müssen die automatische Skalierungsoption für jeden domänenbasierten Server aktivieren, den Sie für die automatische Dienstgruppenskalierung verwenden möchten. Wenn eine IP-Adresse einer oder mehreren Domänen gemeinsam ist, wird die IP-Adresse nur einmal zur Dienstgruppe hinzugefügt.

> **Wichtig**
>
> - DNS Autoscale wird in einer Cluster-Bereitstellung unterstützt.
> - Die Pfadüberwachung für Autoscale-Dienstgruppen wird in der Cluster-Bereitstellung nicht unterstützt.

So konfigurieren Sie eine Dienstgruppe für die automatische Skalierung mithilfe der Befehlszeilenschnittstelle

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

```
add serviceGroup <serviceGroupName> -autoScale (YES | NO)

show serviceGroup <serviceGroupName>
<!--NeedCopy-->
```

Beispiel

Im folgenden Beispiel ist Server1 ein domänenbasierter Server. Die DNS-Antwort enthält mehrere IP-Adressen. Fünf Adressen sind verfügbar und werden der Servicegruppe hinzugefügt.

```
> add serviceGroup servGroup -autoScale YES
```



```
 Done
> sh servicegroup servGroup
        servGroup - HTTP
         State: ENABLED  Monitor Threshold : 0
                . . .
                . . .
         1)   192.0.2.31:80   State: UP       Server Name: server1 (Auto
              scale)    Server ID: None Weight: 1

                 Monitor Name: tcp-default       State: UP
                 Probes: 2       Failed [Total: 0 Current: 0]
                 Last response: Success - TCP syn+ack received.

         2)   192.0.2.32:80   State: UP       Server Name: server1 (Auto
              scale)    Server ID: None Weight: 1

                 Monitor Name: tcp-default       State: UP
                 Probes: 2       Failed [Total: 0 Current: 0]
                 Last response: Success - TCP syn+ack received.

         3)   192.0.2.36:80   State: UP       Server Name: server1 (Auto
              scale)    Server ID: None Weight: 1

                 Monitor Name: tcp-default       State: UP
                 Probes: 2       Failed [Total: 0 Current: 0]
                 Last response: Success - TCP syn+ack received.

         4)   192.0.2.55:80   State: UP       Server Name: server1 (Auto
              scale)    Server ID: None Weight: 1

                 Monitor Name: tcp-default       State: UP
                 Probes: 2       Failed [Total: 0 Current: 0]
                 Last response: Success - TCP syn+ack received.

         5)   192.0.2.80:80   State: UP       Server Name: server1 (Auto
              scale)    Server ID: None Weight: 1

                 Monitor Name: tcp-default       State: UP
                 Probes: 2       Failed [Total: 0 Current: 0]
                 Last response: Success - TCP syn+ack received.
 Done
<!--NeedCopy-->
```


So konfigurieren Sie eine Dienstgruppe für die automatische Skalierung mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.
2. Erstellen Sie eine Dienstgruppe und setzen Sie den Autoscale-Modus auf DNS.

TTL-Werte überschreiben

> **Hinweis:**
>
> Diese Option wird von Citrix ADC 12.1 Build 51.xx und höher unterstützt.

Die Citrix ADC Appliance ist so konfiguriert, dass sie den DNS-Server während des Anwendungsstarts regelmäßig nach einem Update im SRV-Eintrag abfragt, der mit der Anwendung verknüpft ist. Standardmäßig hängt die Periodizität für diese Abfrage von der im SRV-Datensatz veröffentlichten TTL ab. In Microservice- oder Cloud-World-Anwendungen ändern sich Bereitstellungen dynamischer. Daher müssen Proxys Änderungen an der Anwendungsbereitstellung schneller aufnehmen. Daher wird Benutzern empfohlen, den TTL-Parameter des domänenbasierten Dienstes explizit auf einen Wert festzulegen, der niedriger als der SRV-Datensatz-TTL ist und für Ihre Bereitstellung optimal ist. Sie können den TTL-Wert mit zwei Methoden überschreiben:

- Beim Binden eines Mitglieds an die Dienstgruppe
- Festlegen des TTL-Werts global mithilfe des Befehls set lb parameter.

Falls der TTL-Wert sowohl beim Binden des Dienstgruppenmitglieds als auch global konfiguriert wird, hat der beim Binden des Dienstgruppenmitglieds angegebene TTL-Wert Vorrang.
Wenn der TTL-Wert weder beim Binden eines Dienstgruppenmitglieds noch auf globaler Ebene angegeben wird, wird das DBS-Überwachungsintervall vom TTL-Wert in der DNS-Antwort abgeleitet.

Überschreiben der TTL-Werte mit der CLI

- Um den TTL-Wert beim Binden zu überschreiben, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind serviceGroup <serviceGroupName> (<serverName> [-dbsTTL <secs
   >])
<!--NeedCopy-->
```

Beispiel:

```
bind servicegroup svc_grp_1 web_serv -dbsTTL 10
<!--NeedCopy-->
```


- Um den TTL-Wert global zu überschreiben, geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb parameter [-dbsTTL <secs>]
<!--NeedCopy-->
```

Beispiel:

```
set lb parameter -dbsTTL 15
<!--NeedCopy-->
```

Überschreiben der TTL-Werte mit der GUI

Um den TTL-Wert beim Binden zu überschreiben:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.
2. Wählen Sie auf der Seite **Dienstgruppen** die Dienstgruppe aus, die Sie erstellt haben, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Load Balancing-Dienstgruppen** auf **Dienstgruppenmitglieder**.
4. Wählen Sie auf der Seite **Bindung von Dienstgruppenmitgliedern** den Server aus, den Sie erstellt haben, und klicken Sie auf **Bearbeiten** .
5. Geben Sie im Feld **Domänenbasierter Dienst TTL**den TTL-Wert ein.

Um den TTL-Wert auf globaler Ebene zu überschreiben:

1. Navigieren Sie zu **Verkehrsmanagement** > **Load Balancing** > **Load Balancing-Parameter ändern**
2. Geben Sie im Feld **Domänenbasierter Dienst TTL**den TTL-Wert ein.

> **Hinweis:**
>
> Wenn der TTL-Wert des domänenbasierten Servers auf 0 gesetzt ist, wird der TTL-Wert aus dem Datenpaket verwendet.

Festlegen verschiedener Nameserver für Dienstgruppen- und Domänennamenbindungen

> **Hinweis:**
>
> Diese Option wird von Citrix ADC 12.1 Build 51.xx und höher unterstützt.

Sie können verschiedene Nameserver für verschiedene Domainnamen in einer bestimmten Gruppe konfigurieren. Das Festlegen des NameServer-Parameters ist optional, während ein DBS-Server an die Dienstgruppe gebunden wird. Wenn kein Nameserver angegeben wird, während ein Mitglied an die Dienstgruppe gebunden wird, wird der global konfigurierte Nameserver berücksichtigt.

Angeben von Nameservern beim Binden eines Servers an Dienstgruppen mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind serviceGroup <serviceGroupName> (<serverName> [-nameServer <
   ip_addr>] [-dbsTTL <secs>])
<!--NeedCopy-->
```

Beispiel:

```
bind servicegroup svc_grp_1 web_serv  -ns.nameserver.com 10.102.27.155
   -dbsTTL 10
<!--NeedCopy-->
```

Angabe von Nameservern beim Binden eines Servers an Dienstgruppen mithilfe der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.
2. Wählen Sie auf der Seite **Dienstgruppen** die Dienstgruppe aus, die Sie erstellt haben, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Load Balancing-Dienstgruppen** auf **Dienstgruppenmitglieder**.
4. Wählen Sie auf der Seite **Bindung von Dienstgruppenmitgliedern** den Server aus, den Sie erstellt haben, und klicken Sie auf **Bearbeiten** .
5. Geben Sie **unter**Nameserver den Namen des Nameservers an, an den die Abfrage für die gebundene Domäne gesendet werden muss.

Diensterkennung mit DNS-SRV-Einträgen

October 5, 2021

Ein SRV-Datensatz (Dienstdatensatz) ist eine Spezifikation der Daten im Domain Name System, die den Speicherort definiert, d. h. den Hostnamen und die Portnummer der Server für bestimmte Dienste. Der Datensatz definiert auch das Gewicht und die Priorität der einzelnen Server.

Beispiel für einen SRV-Datensatz:

_http._tcp.example.com. 100 IN SRV 10 60 5060 a.example.com.

In der folgenden Tabelle werden die einzelnen Elemente in einem SRV-Datensatz beschrieben:

Service	Protocol	Name	TTL	Class	SRV	Priority	Weight	Port	Target
HTTP	TCP	example.com	100	IN	SRV	10	60	5060	a.example.com

Sie können die DNS-SRV-Einträge verwenden, um die Dienstendpunkte zu ermitteln. Die Citrix ADC Appliance ist so konfiguriert, dass sie regelmäßig die DNS-Server mit dem SRV-Eintrag abfragt, der einem Dienst zugeordnet ist. Beim Empfang des SRV-Datensatzes ist jeder im SRV-Datensatz veröffentlichte Zielhost an eine dem Dienst zugeordnete Dienstgruppe gebunden. Jede Bindung erbt den Port, die Priorität und das Gewicht aus dem SRV-Datensatz. Für jede Dienstbereitstellung muss der Benutzer die Citrix ADC Appliance einmal konfigurieren, während er sie hochbringt, sodass sie zu einer einzigen Touch-Bereitstellung für Anwendungen wird.

Wichtig: Die Gewichtung dynamisch erlernter Servicegruppenmitglieder kann nicht mit der CLI oder der GUI geändert werden.

Anwendungsfall: Load Balancing Microservices

Anwendungen bewegen sich in Richtung Microservice-Architektur aus monolithischen Architekturen. Durch die Umstellung auf die Microservice-Architektur zusammen mit der automatischen Back-End-Server-Lösung wird die Anwendungsbereitstellung dynamischer. Um eine solche dynamische Bereitstellung zu unterstützen, müssen die Proxys oder ADC in der Lage sein, die Back-End-Anwendungs- oder Service-Instanzen dynamisch zu erkennen und in die Proxy-Konfiguration aufzunehmen.
Die Service Discovery mit DNS SRV-Aufzeichnungen hilft bei der Konfiguration der Citrix ADC Appliance in einem solchen dynamischen Bereitstellungsszenario. Anwendungsentwickler können einige Orchestrierungsplattformen verwenden, um die Anwendung bereitzustellen. Orchestrierungsplattformen beim Instanziieren von Containern während der Anwendungsbereitstellung weisen möglicherweise nicht den protokollspezifischen Standardport für jeden dieser Container zu. In solchen Szenarien wird das Erkennen der Portinformationen der Schlüssel zur Konfiguration der Citrix ADC Appliance. SRV-Datensätze sind in einem solchen Szenario hilfreich. SRV-Record-Parameter wie Priorität und Gewicht können für einen besseren Lastausgleich von Anwendungen verwendet werden.

- Priority Parameter kann verwendet werden, um die Priorität des Server-Pools zu diktieren.
- Der Weight Parameter kann verwendet werden, um die Kapazität der Back-End-Dienstinstanzen zu bestimmen und kann daher für den gewichteten Lastausgleich verwendet werden.
- Wenn eine Änderung im Back-End-Server-Pool vorliegt, z. B. eine Back-End-Instanz aus dem Pool entfernt wird, wird die Instanz nur dann gnadenlos entfernt, nachdem alle vorhandenen Clientverbindungen berücksichtigt wurden.

> **Hinweis:**
>
> - Bei einer A/AAAA datensatzbasierten Service-Erkennung haben alle aufgelösten IP-Adressen das gleiche Gewicht, da Sie die Gewichtung der aufgelösten Domäne zuweisen.
> - Wenn die Gewichtung in der SRV-Antwort größer als 100 ist, werden keine Dienste erstellt.

Prioritätsbasierter Lastausgleich mit SRV-Datensätzen

Sie können SRV-Datensätze verwenden, um prioritätsbasierte Lastenausgleich durchzuführen. Der prioritätsbasierte Serverpool kann eine Alternative für die virtuellen Backup-Server sein. Die Datei ns.conf erfordert eine minimale Konfiguration im Vergleich zu den virtuellen Backup-Servern.

Beim prioritätsbasierten Lastenausgleich mit SRV-Datensätzen wird jedem Serverpool eine Prioritätsnummer zugewiesen. Die kleinste Zahl hat die höchste Priorität. Einer der Server im Pool der höchsten Priorität wird für den Lastenausgleich ausgewählt, basierend auf dem Zustand und der Verfügbarkeit des Servers. Wenn alle Server im Serverpool mit höchster Priorität ausgefallen sind, werden die Server mit der nächsthöheren Priorität für den Lastenausgleich ausgewählt. Wenn jedoch die Server im Serverpool mit höchster Priorität erneut hochgesetzt sind, werden die Server erneut aus dem Pool der höchsten Priorität ausgewählt.

Der Wechsel von einem Prioritätsserverpool zu einem anderen Serverpool erfolgt gnädig, indem die vorhandenen Client-Transaktionen entlüftet werden. Daher sehen die aktuellen Clients keine Unterbrechung im Anwendungszugriff.

So aktivieren Sie die Abfrage von SRV-Datensätzen mit der CLI

Führen Sie die folgenden Aufgaben durch, um die Abfrage von SRV-Datensätzen zu ermöglichen:

1. Erstellen Sie einen Server, indem Sie den Abfragetypparameter als SRV angeben.

   Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add server <name> <domain> [-queryType <queryType>])
<!--NeedCopy-->
```

   Beispiel:

```
add server web_serv example.com -queryType SRV
<!--NeedCopy-->
```

   Hinweis:

- Standardmäßig werden IPv4-Abfragen gesendet. Um IPv6-Abfragen zu senden, müssen Sie die IPv6-Domäne aktivieren.
- Der SRV-Zieldomänenname darf 127 Zeichen nicht überschreiten.

2. Erstellen Sie eine Dienstgruppe mit dem Autoskalierungsmodus als DNS.

   Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add serviceGroup <serviceGroupName> <serviceType> [-autoScale <
   autoScale>]
<!--NeedCopy-->
```

   Beispiel:

```
add servicegroup svc_grp_1 http -autoscale dns
<!--NeedCopy-->
```

3. Binden Sie den in Schritt 1 erstellten Server an die Dienstgruppe als Mitglied.

   Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind serviceGroup <serviceGroupName> <serverName>
<!--NeedCopy-->
```

   Beispiel:

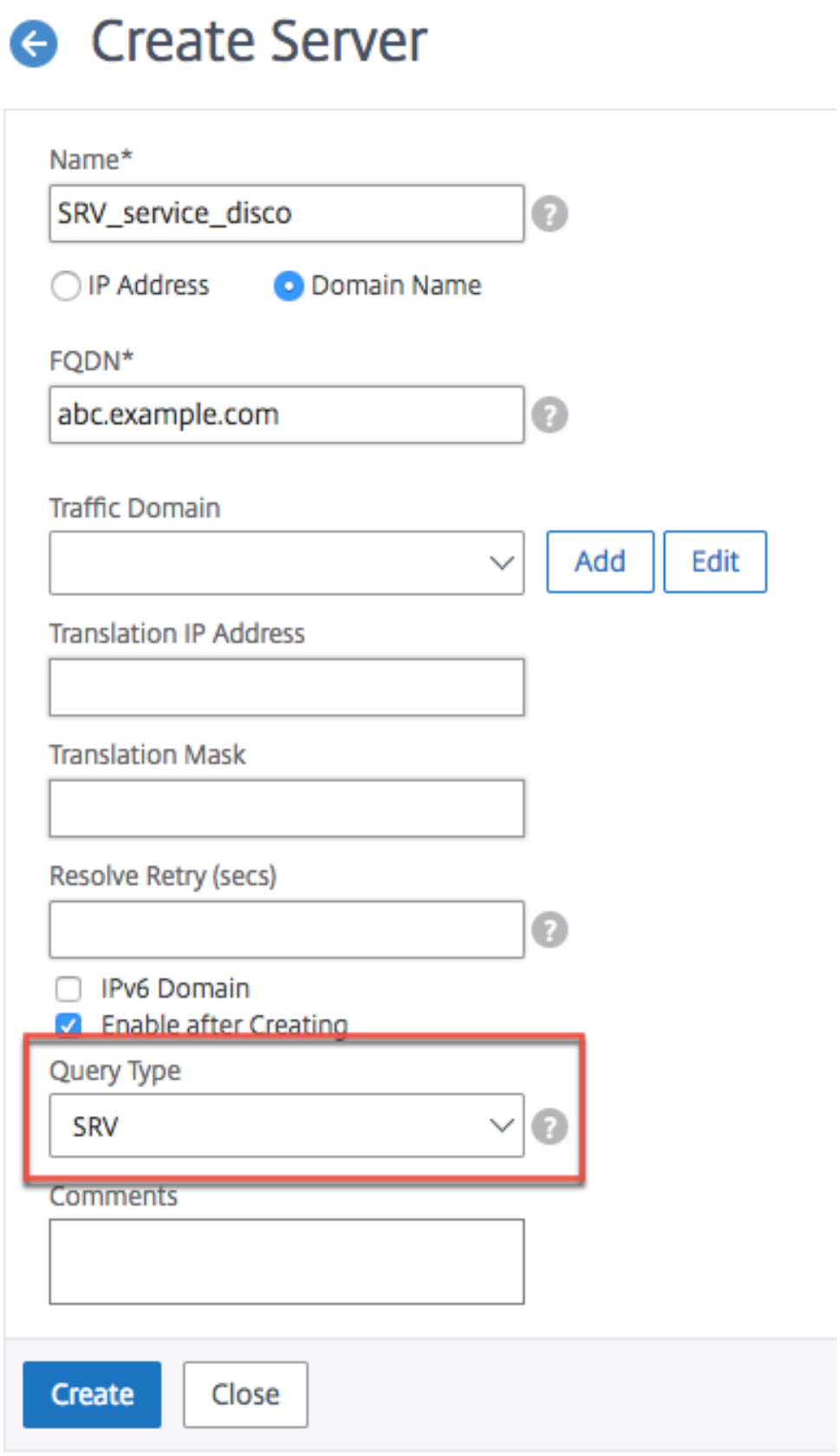
```
bind servicegroup svc_grp_1 web_serv
<!--NeedCopy-->
```

> **Hinweis:**
>
> - Wenn Sie Server an Servicegruppenmitglieder binden, müssen Sie die Portnummer für SRV-Servertypen nicht eingeben. Wenn Sie eine Portnummer für den SRV-Servertyp angeben, wird eine Fehlermeldung angezeigt.
> - Sie können optional einen Nameserver und einen TTL-Wert angeben, während Sie einen Server an die Dienstgruppe binden.

So aktivieren Sie die Abfrage von SRV-Datensätzen mit der GUI

Erstellen eines Servers

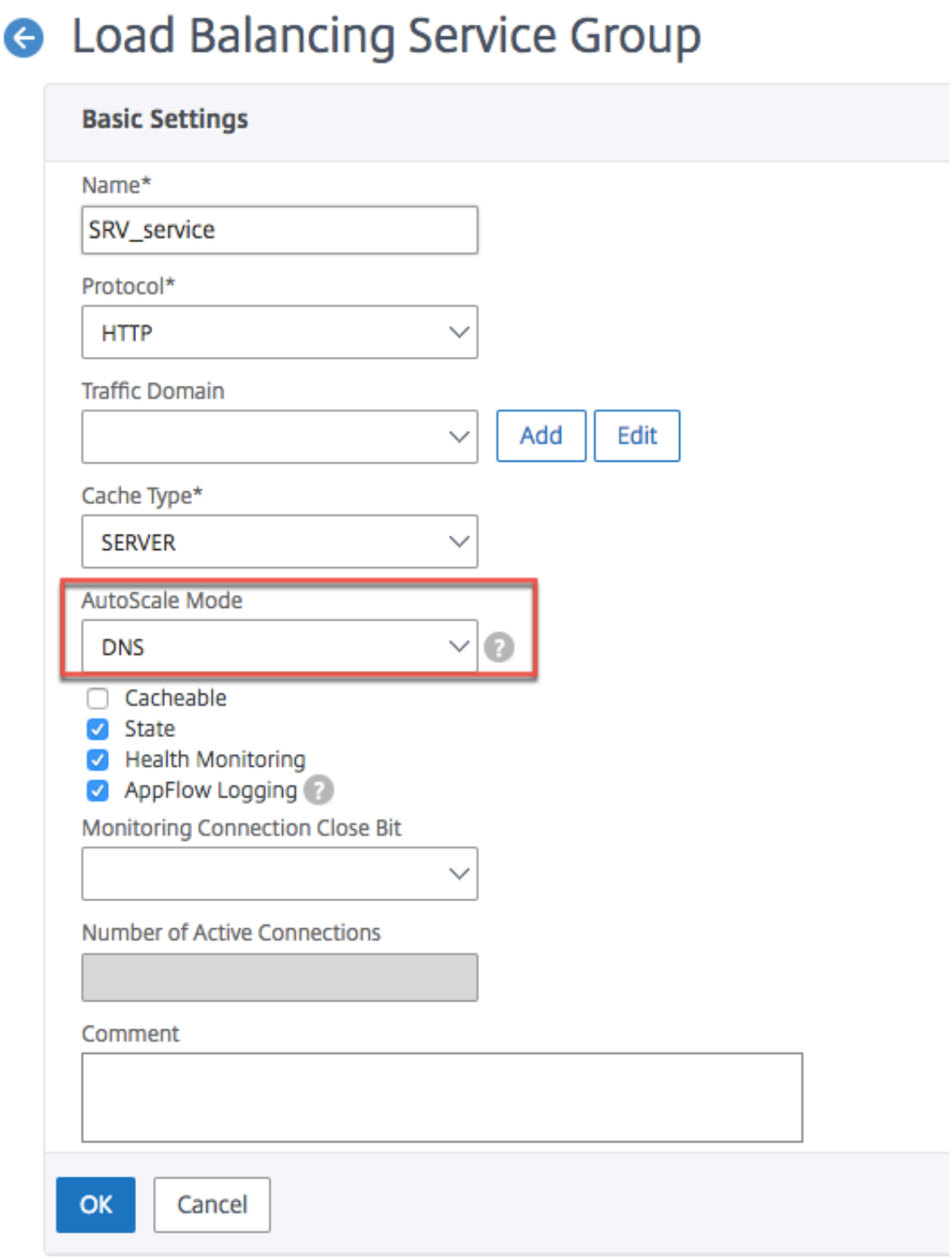
1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Server**, und klicken Sie auf **Hinzufügen** .



2. Wählen Sie auf der Seite **Server erstellen** den Domänennamen aus.
3. Geben Sie die Details aller erforderlichen Parameter ein.
4. Wählen Sie unter **Abfragetyp**die Option **SRV**aus.
5. Klicken Sie auf **Erstellen**.

Erstellen einer Dienstgruppe mit Autoskalierungsmodus als DNS

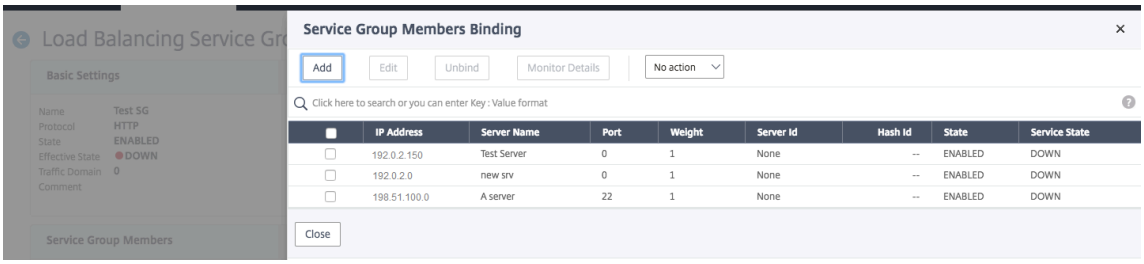
1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.
2. Geben Sie auf der Seite **Lastausgleichsdienstgruppe** Details aller erforderlichen Parameter ein.
3. Wählen Sie für **AutoScale Mode** die Option **DNS** aus.



4. Klicken Sie auf **OK**.

Server an das Dienstgruppenmitglied binden

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.
2. Wählen Sie auf der Seite **Dienstgruppen** die von Ihnen erstellte Dienstgruppe aus, und klicken Sie auf **Bearbeiten** .
3. Klicken Sie auf der Seite **Lastausgleichsdienstgruppen** auf **Dienstgruppenmitglieder** .
4. Wählen Sie auf der Seite **Bindung von Dienstgruppenmitgliedern** den Server aus, den Sie erstellt haben, und klicken Sie auf **Schließen** .



Hinweis:

- Während der Bindung müssen Sie die Portnummer für SRV-Servertypen nicht eingeben. Wenn Sie eine Portnummer für den SRV-Servertyp eingeben, wird eine Fehlermeldung angezeigt.
- Sie können optional einen Nameserver und einen TTL-Wert angeben, während Sie einen Server an die Dienstgruppe binden.

TTL-Werte überschreiben

Die Citrix ADC Appliance ist so konfiguriert, dass sie den DNS-Server während des Anwendungsstarts regelmäßig nach einem Update im SRV-Eintrag abfragt, der mit der Anwendung verknüpft ist. Standardmäßig hängt die Periodizität für diese Abfrage von der im SRV-Datensatz veröffentlichten TTL ab. In Microservice- oder Cloud-World-Anwendungen ändern sich die Bereitstellungen dynamischer. Daher müssen Proxys schneller Änderungen an der Anwendungsbereitstellung absorbieren. Daher wird empfohlen, den domänenbasierten Dienst-TTL-Parameter explizit auf einen Wert festzulegen, der niedriger ist als die TTL des SRV-Datensatzes und optimal für Ihre Bereitstellung ist. Sie können den TTL-Wert mit zwei Methoden überschreiben:

- Beim Binden eines Mitglieds an die Servicegruppe
- Festlegen des TTL-Werts global mithilfe des Befehls set lb parameter.

Falls der TTL-Wert sowohl beim Binden des Dienstgruppenmitglieds als auch global konfiguriert wird, hat der beim Binden des Dienstgruppenmitglieds angegebene TTL-Wert Vorrang.
Wenn der TTL-Wert weder beim Binden eines Dienstgruppenmitglieds noch auf globaler Ebene angegeben wird, wird das DBS-Überwachungsintervall vom TTL-Wert in der DNS-Antwort abgeleitet.

Überschreiben der TTL-Werte mit der CLI

- Um den TTL-Wert während der Bindung zu überschreiben, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind serviceGroup <serviceGroupName> (<serverName> [-dbsTTL <secs
    >])
<!--NeedCopy-->
```

Beispiel:

```
bind servicegroup svc_grp_1 web_serv -dbsTTL 10
<!--NeedCopy-->
```

- Um den TTL-Wert global zu überschreiben, geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb parameter [-dbsTTL <secs>]
<!--NeedCopy-->
```

Beispiel:

```
set lb parameter -dbsTTL 15
<!--NeedCopy-->
```

Überschreiben der TTL-Werte mit der GUI

So überschreiben Sie den TTL-Wert während der Bindung:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.
2. Wählen Sie auf der Seite **Dienstgruppen** die von Ihnen erstellte Dienstgruppe aus, und klicken Sie auf **Bearbeiten** .
3. Klicken Sie auf der Seite **Lastausgleichsdienstgruppen** auf **Dienstgruppenmitglieder** .
4. Wählen Sie auf der Seite **Bindung von Dienstgruppenmitgliedern** den Server aus, den Sie erstellt haben, und klicken Sie auf **Bearbeiten** .
5. Geben Sie unter **Domänenbasierter Dienst-TTL**den TTL-Wert ein.

So überschreiben Sie den TTL-Wert auf globaler Ebene:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Load Balancing Parameter ändern** .
2. Geben Sie unter **Domänenbasierter Dienst-TTL**den TTL-Wert ein.

> **Hinweis**: Wenn der TTL-Wert des domänenbasierten Servers auf 0 festgelegt ist, wird der TTL-Wert aus dem Datenpaket verwendet.

Angeben verschiedener Nameserver für Dienstgruppen- und Domänennamensbindungen

Sie können verschiedene Nameserver für verschiedene Domänennamen in einer bestimmten Gruppe konfigurieren. Das Festlegen des NameServer-Parameters ist optional, während ein DBS-Server an die Dienstgruppe gebunden wird. Wenn beim Binden eines Mitglieds an die Dienstgruppe kein Nameserver angegeben wird, wird der global konfigurierte Nameserver berücksichtigt.

Angeben von Namensservern während der Bindung eines Servers an Servicegruppen mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind serviceGroup <serviceGroupName> (<serverName> [-nameServer <
    ip_addr>] [-dbsTTL <secs>])
<!--NeedCopy-->
```

Beispiel:

```
bind servicegroup svc_grp_1 web_serv  -ns.nameserver.com 10.102.27.155
    -dbsTTL 10
<!--NeedCopy-->
```

Angeben von Namensservern während der Bindung eines Servers an Servicegruppen mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienstgruppen**.
2. Wählen Sie auf der Seite **Dienstgruppen** die von Ihnen erstellte Dienstgruppe aus, und klicken Sie auf **Bearbeiten** .

3. Klicken Sie auf der Seite **Lastausgleichsdienstgruppen** auf **Dienstgruppenmitglieder** .
4. Wählen Sie auf der Seite **Bindung von Dienstgruppenmitgliedern** den Server aus, den Sie erstellt haben, und klicken Sie auf **Bearbeiten** .
5. Geben Sie **unter**Nameserver den Namen des Nameservers an, an den die Abfrage für die gebundene Domäne gesendet werden muss.

Übersetzen der IP-Adresse eines domänenbasierten Servers

October 5, 2021

Um die Wartung der Citrix ADC Appliance und der domänenbasierten Server zu vereinfachen, die mit der Citrix ADC-Appliance verbunden sind, können Sie IP-Adressmasken und Übersetzungs-IP-Adressen konfigurieren. Diese Funktionen arbeiten zusammen, um eingehende DNS-Pakete zu analysieren und eine neue IP-Adresse durch eine DNS-aufgelöste IP-Adresse zu ersetzen.

Wenn sie für einen domänenbasierten Server konfiguriert ist, ermöglicht die IP-Adressübersetzung die Appliance, eine alternative Server-IP-Adresse zu finden, wenn Sie den Server zur Wartung abschalten oder wenn Sie andere Infrastrukturänderungen vornehmen, die sich auf den Server auswirken.

Bei der Konfiguration der Maske müssen Sie Standard-IP-Maskenwerte (eine Potenz von zwei, minus eins) und Nullen verwenden, z. B. 255.255.0.0. Werte ungleich Null sind nur in den Startoktetten zulässig.

Wenn Sie eine Übersetzungs-IP für einen Server konfigurieren, erstellen Sie eine 1:1 -Korrespondenz zwischen einer Server-IP-Adresse und einem alternativen Server, der führende oder nachfolgende Oktette in seiner IP-Adresse freigibt. Die Maske blockiert bestimmte Oktette in der IP-Adresse des ursprünglichen Servers. Die DNS-aufgelöste IP-Adresse wird durch Anwenden der Übersetzungs-IP-Adresse und der Übersetzungsmaske in eine neue IP-Adresse umgewandelt.

Beispielsweise können Sie eine Übersetzungs-IP-Adresse 10.20.0.0 und eine Übersetzungsmaske 255.255.0.0 konfigurieren. Wenn eine DNS-aufgelöste IP-Adresse für einen Server 40.50.27.3 ist, wird diese Adresse in 10.20.27.3 umgewandelt. In diesem Fall liefert die Übersetzungs-IP-Adresse die ersten beiden Oktette der neuen Adresse, und die Maske durchläuft die letzten beiden Oktette von der ursprünglichen IP-Adresse. Der Verweis auf die ursprüngliche IP-Adresse, wie von DNS aufgelöst, geht verloren. Monitore für alle Dienste, an die der Server gebunden ist, berichten auch über die transformierte IP-Adresse.

Bei der Konfiguration einer Übersetzungs-IP-Adresse für einen domänenbasierten Server geben Sie eine Maske und eine IP-Adresse an, in die die DNS-aufgelöste IP-Adresse übersetzt werden soll.

Hinweis: Die Übersetzung der IP-Adresse ist nur für domänenbasierte Server möglich. Sie können diese Funktion nicht für IP-basierte Server verwenden. Das Adressmuster kann nur auf IPv4-Adressen

basieren.

So konfigurieren Sie eine Übersetzungs-IP-Adresse für einen Server mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add server <name>@ <serverDomainName> -translationIp <
   translationIPAddress> -translationMask <netMask> -state <ENABLED|
   DISABLED>
<!--NeedCopy-->
```

Beispiel:

```
add server myMaskedServer www.example.com -translationIp 10.10.10.10 -
   translationMask
255.255.0.0 -state ENABLED
<!--NeedCopy-->
```

So konfigurieren Sie eine Übersetzungs-IP-Adresse für einen Server mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management > Load Balancing > Server**, erstellen Sie einen domänenbasierten Server und geben Sie eine Übersetzungs-IP-Adresse an.

Maskieren einer virtuellen Server-IP-Adresse

October 5, 2021

Sie können eine Maske und ein Muster anstelle einer festen IP-Adresse für einen virtuellen Server konfigurieren. Dadurch kann Datenverkehr, der an eine der IP-Adressen geleitet wird, die der Maske und dem Muster entsprechen, an einen bestimmten virtuellen Server umgeleitet werden. Beispielsweise können Sie eine Maske konfigurieren, mit der die ersten drei Oktette einer IP-Adresse variabel sein können, sodass der Datenverkehr zu 111.11.11.198, 22.22.22.198 und 33.33.33.198 an denselben virtuellen Server gesendet wird.

Wenn Sie eine Maske für eine IP-Adresse des virtuellen Servers konfigurieren, können Sie die Neukonfiguration Ihrer virtuellen Server aufgrund einer Änderung des Routing oder einer anderen Änderung

der Infrastruktur vermeiden. Die Maske ermöglicht es dem Datenverkehr, ohne umfangreiche Neukonfiguration Ihrer virtuellen Server weiterzufließen.

Die Maske für eine IP-Adresse eines virtuellen Servers funktioniert anders als die IP-Musterdefinition für einen Server, die unter Die IP-Adresse eines domänenbasierten Servers übersetzen beschrieben wird. Bei einer IP-Adressmaske des virtuellen Servers wird eine Maske ungleich Null als Oktett interpretiert, das berücksichtigt wird. Bei einem Dienst wird der Wert ungleich Null blockiert.

Für eine virtuelle Server-IP-Adresse können außerdem führende oder nachfolgende Werte berücksichtigt werden. Wenn die IP-Adressmaske des virtuellen Servers Werte von der linken Seite der IP-Adresse berücksichtigt, wird dies als Vorwärtsmaske bezeichnet. Wenn die Maske die Werte auf der rechten Seite der Adresse berücksichtigt, wird dies als umgekehrte Maske bezeichnet.

Hinweis: Die Citrix ADC Appliance wertet alle virtuellen Forwardmask-Server aus, bevor virtuelle Server mit Reverse Maskierung ausgewertet werden.

Beim Maskieren einer virtuellen Server-IP-Adresse müssen Sie außerdem ein IP-Adressmuster erstellen, um eingehenden Datenverkehr mit dem richtigen virtuellen Server abzugleichen. Wenn die Appliance ein eingehendes IP-Paket empfängt, stimmt sie die Ziel-IP-Adresse im Paket mit den Bits ab, die im IP-Adressmuster berücksichtigt werden. Nachdem sie eine Übereinstimmung gefunden hat, wendet sie die IP-Adressmaske an, um die endgültige Ziel-IP-Adresse zu erstellen.

Betrachten Sie das folgende Beispiel:

- Ziel-IP-Adresse im eingehenden Paket: 10.102.27.189
- IP-Adressmuster: 10.102.0.0
- IP-Maske: 255.255.0.0
- Konstruierte (endgültige) Ziel-IP-Adresse: 10.102.27.189.

In diesem Fall stimmen die ersten 16 Bits in der ursprünglichen Ziel-IP-Adresse mit dem IP-Adressmuster für diesen virtuellen Server überein, sodass dieses eingehende Paket an diesen virtuellen Server weitergeleitet wird.

Wenn eine Ziel-IP-Adresse den IP-Mustern für mehr als einen virtuellen Server entspricht, hat die längste Übereinstimmung Vorrang. Betrachten Sie das folgende Beispiel:

- Virtueller Server 1: IP-Muster 10.10.0.0, IP-Maske 255.255.0.0
- Virtual Server 2: IP-Muster 10.10.10.0, IP-Maske 255.255.255.0
- Ziel-IP-Adresse im Paket: 10.10.10.45.
- Ausgewählter virtueller Server: Virtueller Server 2.

Das mit Virtual Server 2 verknüpfte Muster stimmt mit mehr Bits überein als das mit Virtual Server 1 verknüpfte, sodass IPs, die damit übereinstimmen, an Virtual Server 2 gesendet werden.

Hinweis: Ports werden auch berücksichtigt, wenn ein Tie-Breaker erforderlich ist.

So konfigurieren Sie eine IP-Adressmaske des virtuellen Servers mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name>@ http -ipPattern <ipAddressPattern> -ipMask <
   ipMask> <listenPort>
<!--NeedCopy-->
```

Beispiel:

Musterabgleich basierend auf Präfixoktetten:

```
add lb vserver myLBVserver http -ippattern 10.102.0.0 -ipmask
   255.255.0.0 80
<!--NeedCopy-->
```

Musterabgleich basierend auf nachfolgenden Oktetten:

```
add lb vserver myLBVserver1 http -ippattern 0.0.22.74 -ipmask
   0.0.255.255 80
<!--NeedCopy-->
```

Ändern eines musterbasierten virtuellen Servers:

```
set lb vserver myLBVserver1 -ippattern 0.0.22.74 -ipmask 0.0.255.255
<!--NeedCopy-->
```

So konfigurieren Sie eine IP-Adressmaske des virtuellen Servers mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie in der Liste Adresstyp die Option IP-Muster aus, und geben Sie ein IP-Muster und eine IP-Maske an.

Konfigurieren des Lastenausgleichs für häufig verwendete Protokolle

October 5, 2021

Neben Websites und webbasierten Anwendungen erhalten andere Arten von netzwerkbereitgestellten Anwendungen, die andere gängige Protokolle verwenden, häufig große Datenverkehrsmengen und profitieren daher vom Lastenausgleich. Mehrere dieser Protokolle erfordern spezifische Konfigurationen, damit der Lastausgleich ordnungsgemäß funktioniert. Unter ihnen sind FTP, DNS, SIP und RTSP.

Wenn Sie Ihre Citrix ADC Appliance so konfigurieren, dass sie Domänennamen für Ihre Server anstelle von IPs verwendet, müssen Sie möglicherweise auch IP-Übersetzung und -Maskierung für diese Server einrichten.

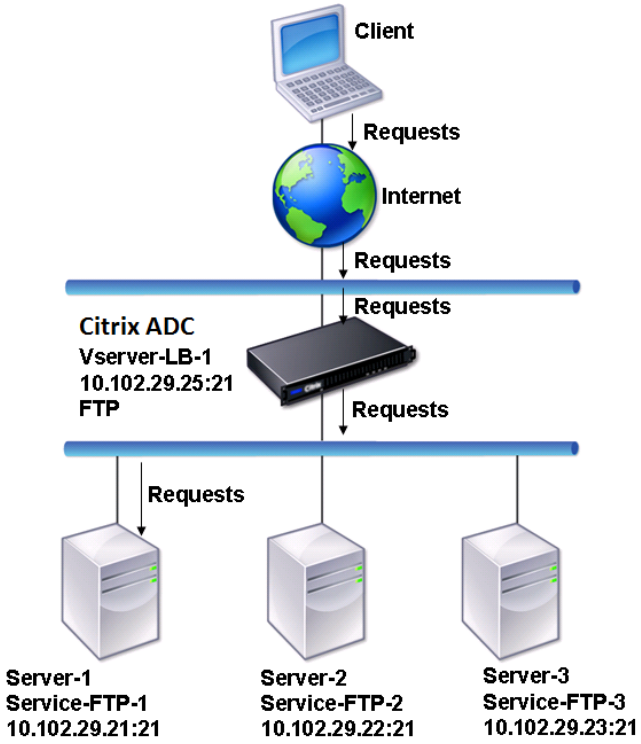
Lastverteilung einer Gruppe von FTP-Servern

October 5, 2021

Die Citrix ADC Appliance kann zum Lastenausgleich von FTP-Servern verwendet werden. FTP erfordert, dass der Benutzer zwei Verbindungen an zwei verschiedenen Ports zum selben Server initiiert: die Steuerverbindung, über die der Client Befehle an den Server sendet, und die Datenverbindung, über die der Server Daten an den Client sendet. Wenn der Client eine FTP-Sitzung initiiert, indem er eine Steuerungsverbindung zum FTP-Server öffnet, verwendet die Appliance die konfigurierte Lastausgleichsmethode, um einen FTP-Dienst auszuwählen und leitet die Steuerungsverbindung an ihn weiter. Der Lastausgleichs-FTP-Server öffnet dann eine Datenverbindung zum Client zum Informationsaustausch.

Das folgende Diagramm beschreibt die Topologie einer Lastausgleichskonfiguration für eine Gruppe von FTP-Servern.

Abbildung 1. Grundlegende Load Balancing-Topologie für FTP-Server



Im Diagramm sind die Dienste Service-FTP-1, Service-FTP-2 und Service-FTP-3 an den virtuellen Server vServer-LB-1 gebunden. vServer-LB-1 leitet die Verbindungsanforderung des Clients an einen der Dienste weiter, wobei die Methode für den Lastenausgleich mit der geringsten Verbindung verwendet wird. Nachfolgende Anforderungen werden an den Dienst weitergeleitet, den die Appliance ursprünglich für den Lastausgleich ausgewählt hat.

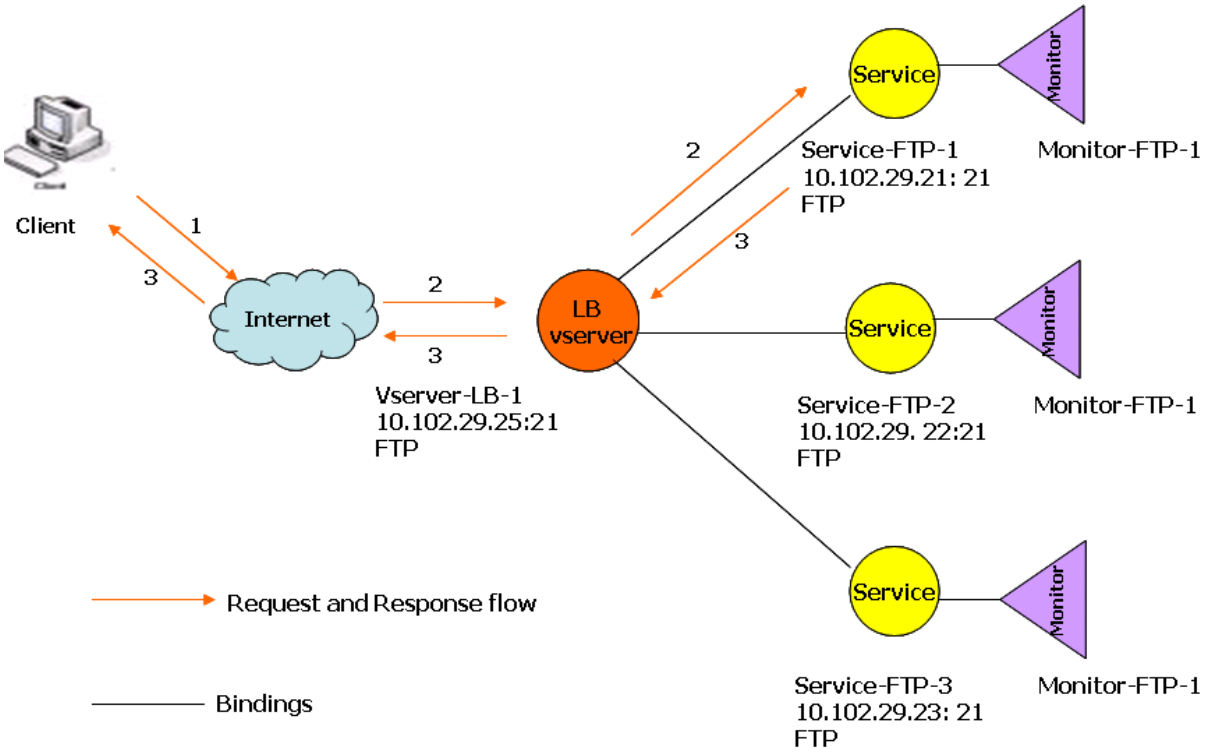
In der folgenden Tabelle sind die Namen und Werte der Basiseinheiten aufgeführt, die auf der Appliance konfiguriert sind.

Entitätstyp	Name	IP-Adresse	Port	Protokoll
Vserver	Vserver-LB-1	10.102.29.25	21	FTP
Services	Service-FTP-1	10.102.29.21	21	FTP
	Service-FTP-2	10.102.29.22	21	FTP
	Service-FTP-3	10.102.29.23	21	FTP
Monitore	FTP	Ohne	Ohne	Ohne

Das folgende Diagramm zeigt die Lastausgleichseinheiten und die Werte der Parameter, die auf der

Appliance konfiguriert werden müssen.

Abbildung 2. Lastenausgleich FTP-Server-Entitätsmodell



Die Appliance kann auch eine passive FTP-Option bereitstellen, um von außerhalb einer Firewall auf FTP-Server zuzugreifen. Wenn ein Client die passive FTP-Option verwendet und eine Steuerungsverbindung zum FTP-Server initiiert, initiiert der FTP-Server auch eine Steuerungsverbindung zum Client. Es initiiert dann eine Datenverbindung, um eine Datei über die Firewall zu übertragen.

Informationen zum Erstellen von Diensten und virtuellen Servern vom Typ FTP finden Sie unter Einrichten des Basic Load Balancing. Benennen Sie die Entitäten und legen Sie die Parameter auf die in den Spalten der vorherigen Tabelle beschriebenen Werte fest. Wenn Sie ein grundlegendes Lastausgleichs-Setup konfigurieren, ist ein Standardmonitor an die Dienste gebunden.

Binden Sie als Nächstes den FTP-Monitor an die Dienste, indem Sie das im Abschnitt Binden von Monitoren an Dienstebeschriebenen Verfahren befolgen.

So erstellen Sie FTP-Monitore mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb monitor <MonitorName> FTP -interval <Interval> -userName <
     UserName> -password <Password>
2 <!--NeedCopy-->
```


Beispiel:

```
add lb monitor monitor-FTP-1 FTP -interval 360 -userName User -password
    User
<!--NeedCopy-->
```

So erstellen Sie FTP-Monitore mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Erstellen Sie einen Monitor vom Typ FTP, und geben Sie unter Spezielle Parameter einen Benutzernamen und ein Kennwort an.

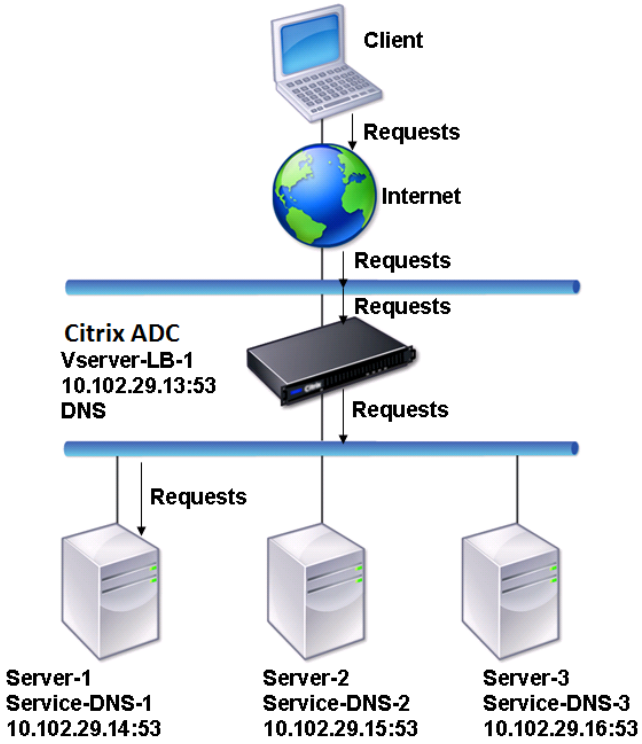
Lastenausgleich DNS-Server

October 5, 2021

Wenn Sie die DNS-Auflösung eines Domänennamens anfordern, verwendet die Citrix ADC Appliance die konfigurierte Lastausgleichsmethode, um einen DNS-Dienst auszuwählen. Der DNS-Server, an den der Dienst gebunden ist, löst dann den Domänennamen auf und gibt die IP-Adresse als Antwort zurück. Die Appliance kann auch DNS-Antworten zwischenspeichern und die zwischengespeicherten Informationen verwenden, um auf zukünftige Anforderungen zur Auflösung desselben Domänennamens zu antworten. Der Lastenausgleich von DNS-Servern verbessert die DNS-Reaktionszeiten.

Das folgende Diagramm beschreibt die Topologie einer Lastausgleichskonfiguration, die eine Gruppe von DNS-Diensten mit Lastenausgleich ausgleicht.

Abbildung 1. Grundlegende Load Balancing-Topologie für DNS-Server

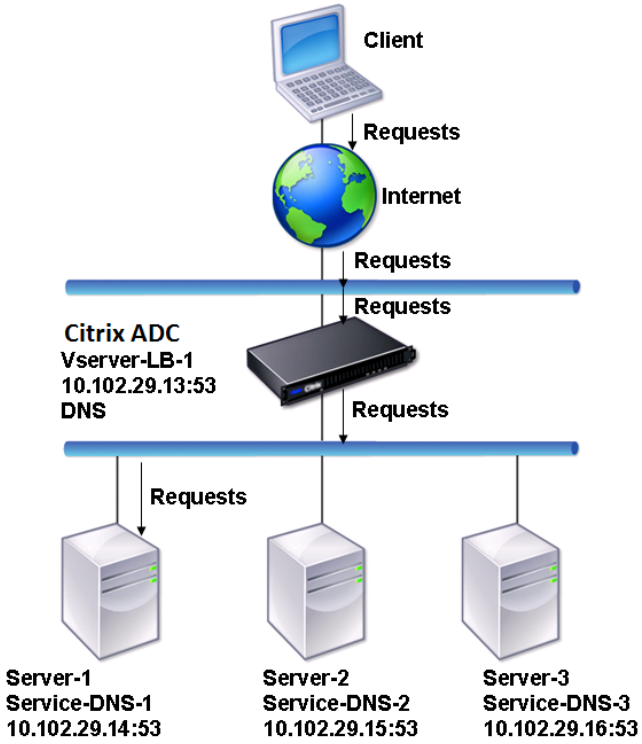


Im Diagramm sind die Dienste Service-DNS-1, Service-DNS-2 und Service-DNS-3 an den virtuellen Server vServer-LB-1 gebunden. Der virtuelle Server vServer-LB-1 leitet Clientanforderungen mithilfe der Methode Load Balancing an einen Dienst weiter. In der folgenden Tabelle sind die Namen und Werte der Basiseinheiten aufgeführt, die auf der Appliance konfiguriert sind.

Entitätstyp	Name	IP-Adresse	Port	Protokoll
Virtueller Server	Vserver-LB-1	10.102.29.13	53	DNS
Services	Service-DNS-1	10.102.29.14	53	DNS
	Service-DNS-2	10.102.29.15	53	DNS
	Service-DNS-3	10.102.29.16	53	DNS
Monitore	monitor-DNS-1	Ohne	Ohne	Ohne

Das folgende Diagramm zeigt die Lastausgleichseinheiten und die Werte der Parameter, die auf der Appliance konfiguriert werden müssen.

Abbildung 2. Load Balancing DNS-Server-Entitätsmodell



Informationen zum Konfigurieren eines grundlegenden DNS-Lastenausgleichs-Setups finden Sie unter Einrichten des Basic Load Balancing. Befolgen Sie die Verfahren zum Erstellen von Diensten und virtuellen Servern vom Typ DNS, benennen Sie die Entitäten und legen Sie die Parameter anhand der in der vorherigen Tabelle beschriebenen Werte fest. Wenn Sie ein grundlegendes Lastausgleichs-Setup konfigurieren, ist der standardmäßige Ping-Monitor an die Dienste gebunden. Anweisungen zum Binden eines DNS-Monitors an DNS-Dienste finden Sie auch unter Binden von Monitoren an Dienste.

Im folgenden Verfahren werden die Schritte zum Erstellen eines Monitors beschrieben, der basierend auf einer Abfrage einen Domänennamen der IP-Adresse zuordnet.

So konfigurieren Sie DNS-Monitore mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb monitor <monitorName> DNS -query <domainName> -queryType <
    Address|ZONE> -IPAddress <ipAddress>
<!--NeedCopy-->
```


Beispiel:

```
add lb monitor monitor-DNS-1 DNS -query www.citrix.com -queryType
    Address -IPAddress 10.102.29.66

add lb monitor monitor-DNS-2 DNS -query www.citrix2.com -queryType
    Address -IPAddress
1000:0000:0000:0000:0005:0600:700a::888b-888d
<!--NeedCopy-->
```

So konfigurieren Sie DNS-Monitore mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Erstellen Sie einen Monitor vom Typ DNS, und geben Sie unter Spezielle Parameter einen Abfrage- und Abfragetyp an.

Load Balance-Domainnamen-basierte Dienste

December 7, 2021

Wenn Sie einen Dienst für den Lastenausgleich erstellen, können Sie eine IP-Adresse angeben. Alternativ können Sie einen Server mit einem Domänennamen erstellen. Der Servername (Domänenname) kann mithilfe eines IPv4- oder IPv6-Nameservers oder durch Hinzufügen eines autorisierenden DNS-Eintrags (Ein Datensatz für IPv4 oder AAAA-Eintrag für IPv6) zur Citrix ADC Konfiguration aufgelöst werden.

Wenn Sie Dienste mit Domänennamen anstelle von IP-Adressen konfigurieren und der Nameserver den Domänennamen in eine neue IP-Adresse auflöst, führt der an den Dienst gebundene Monitor eine Zustandsprüfung für die neue IP-Adresse durch und aktualisiert die Dienst-IP-Adresse nur dann, wenn die IP-Adresse fehlerfrei ist. Der Monitor kann der Standardmonitor sein, der an den Dienst gebunden ist, oder Sie können jeden anderen unterstützten Monitor binden. Er untersucht den Dienst in regelmäßigen Abständen, die in den Monitorparametern definiert sind. Wenn der Domänenname in eine neue IP-Adresse aufgelöst wird, sendet der Monitor einen neuen Prüfpunkt, um den Zustand des Dienstes zu überprüfen. Alle nachfolgenden Prüfpunkte befinden sich im vordefinierten Intervall.

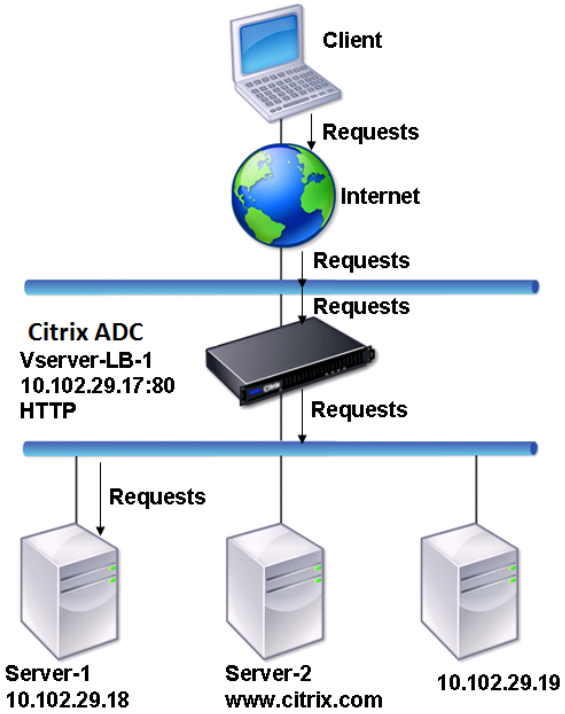
Hinweis: Wenn Sie die IP-Adresse eines Servers ändern, wird der entsprechende Dienst für die erste Clientanforderung markiert. Der Nameserver löst die Dienst-IP-Adresse in die geänderte IP-Adresse für die nächste Anforderung auf, und der Dienst wird als UP gekennzeichnet.

Domänennamenbasierte Dienste haben die folgenden Einschränkungen:

- Die maximale Länge des Domainnamens beträgt 255 Zeichen.
- Der Parameter Maximum Client wird verwendet, um einen Dienst zu konfigurieren, der den Domänennamenserver darstellt. Beispielsweise wird ein MaxClient von 1000 für die Dienste festgelegt, die an einen virtuellen Server gebunden sind. Wenn die Anzahl der Verbindungen auf dem virtuellen Server 2000 erreicht, ändert der DNS-Resolver die IP-Adresse der Dienste. Da der Verbindungszähler auf dem Dienst jedoch nicht zurückgesetzt wird, kann der virtuelle Server keine neuen Verbindungen aufnehmen, bis alle alten Verbindungen geschlossen sind.
- Wenn sich die IP-Adresse des Dienstes ändert, ist die Persistenz schwierig zu pflegen.
- Wenn die Domänennamenauflösung aufgrund eines Timeouts fehlschlägt, verwendet die Appliance die alten Informationen (IP-Adresse).
- Wenn die Überwachung feststellt, dass ein Dienst ausgefallen ist, führt die Appliance eine DNS-Auflösung für den Dienst aus (der den Domänennamenserver darstellt), um eine neue IP-Adresse zu erhalten.
- Statistiken werden für einen Dienst gesammelt und werden nicht zurückgesetzt, wenn sich die IP-Adresse ändert.
- Wenn eine DNS-Auflösung den Code Namensfehler (3) zurückgibt, markiert die Appliance den Dienst und ändert die IP-Adresse auf Null.

Wenn die Appliance eine Anforderung für einen Dienst erhält, wählt sie den Zieldienst aus. Auf diese Weise gleicht die Appliance die Belastung Ihrer Dienste aus. Das folgende Diagramm beschreibt die Topologie einer Lastausgleichskonfiguration, die eine Gruppe von domainnamenbasierten Servern (DBS) ausgleicht.

Abbildung 1. Grundlegende Load Balancing-Topologie für DBS-Server



Die Dienste Service-HTTP-1, Service-Http-2 und Service-Http-3 sind an den virtuellen Server vServer-LB-1 gebunden. Der virtuelle Server vServer-LB-1 verwendet die Methode für den Lastausgleich am wenigsten für die Verbindung, um den Dienst auszuwählen. Die IP-Adresse des Dienstes wird mit dem Nameserver vServer-LB-2 aufgelöst.

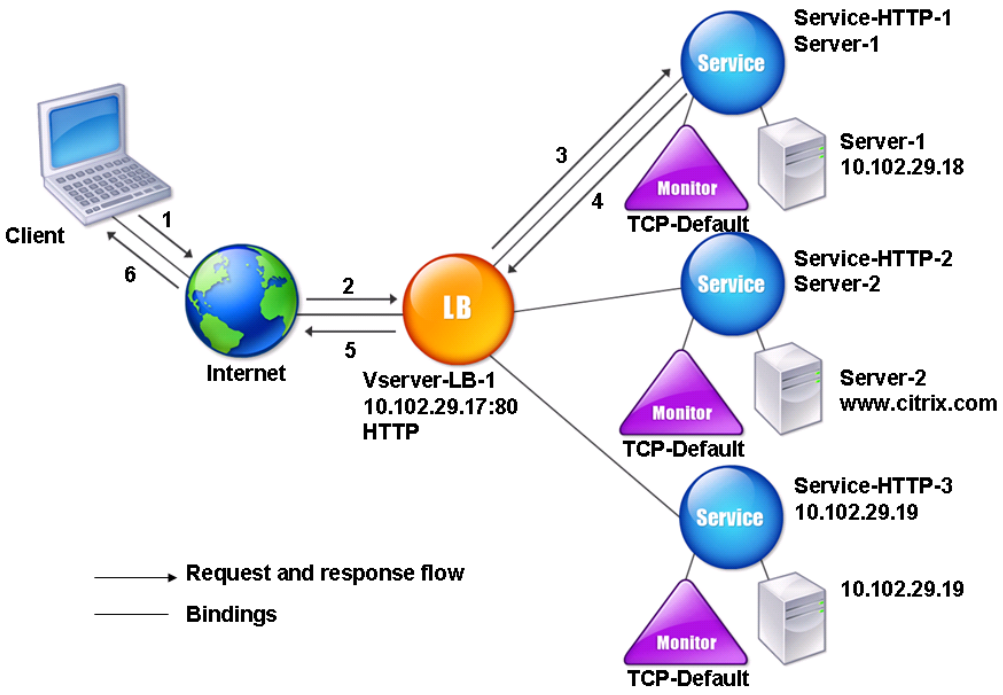
In der folgenden Tabelle sind die Namen und Werte der Basiseinheiten aufgeführt, die auf der Appliance konfiguriert sind.

Entitätstyp	Name	IP-Adresse	Port	Protokoll
Virtueller Server	Vserver-LB-1	10.102.29.17	80	HTTP
	Vserver-LB-2	10.102.29.20	53	DNS
Server	server-1	10.102.29.18	80	HTTP
	server-2	www.citrix.com	80	HTTP
Services	Service-HTTP-1	server-1	80	HTTP
	Service-HTTP-2	server-2	80	HTTP
	Service-HTTP-2	10.102.29.19	80	HTTP
Monitore	Standard	Ohne	Ohne	Ohne

Entitätstyp	Name	IP-Adresse	Port	Protokoll
Namensserver	Ohne	10.102.29.19	Ohne	Ohne

Das folgende Diagramm zeigt die Lastausgleichseinheiten und die Werte der Parameter, die auf der Appliance konfiguriert werden müssen.

Abbildung 2. Lastenausgleich DBS-Server-Entitätsmodell



Informationen zum Konfigurieren eines grundlegenden Load Balancing-Setups finden Sie unter Einrichten des Basic Load Balancing. Erstellen Sie die Dienste und virtuellen Server vom Typ HTTP, benennen Sie die Entitäten und legen Sie die Parameter anhand der in der vorherigen Tabelle beschriebenen Werte fest.

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

So fügen Sie einen Nameserver über die Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add dns nameServer <dnsVserverName>
<!--NeedCopy-->
```

Beispiel:

```
add dns nameServer Vserver-LB-2
<!--NeedCopy-->
```

So fügen Sie mit dem Konfigurationsdienstprogramm einen Nameserver hinzu

1. Navigieren Sie zu **Traffic Management** > **DNS** > **Nameserver**.
2. Erstellen Sie einen DNS-Nameserver vom Typ DNS Virtual Server, und wählen Sie einen Server aus der Liste Virtueller DNS-Server aus.

Sie können auch einen autorisierenden Nameserver hinzufügen, der den Domänennamen in eine IP-Adresse auflöst.

> **Hinweis:**
>
> Sie können einen Nameserver vom Typ TCP, UDP oder UDP_TCP zu Resolver-DBS-Sonden hinzufügen. Wenn jedoch TCP- und UDP-Nameserver koexistieren und ein UDP-Nameserver eine Antwort mit dem abgeschnittenen Bit erhält, wird diese Antwort über den TCP-Nameserver nicht wiederholt.

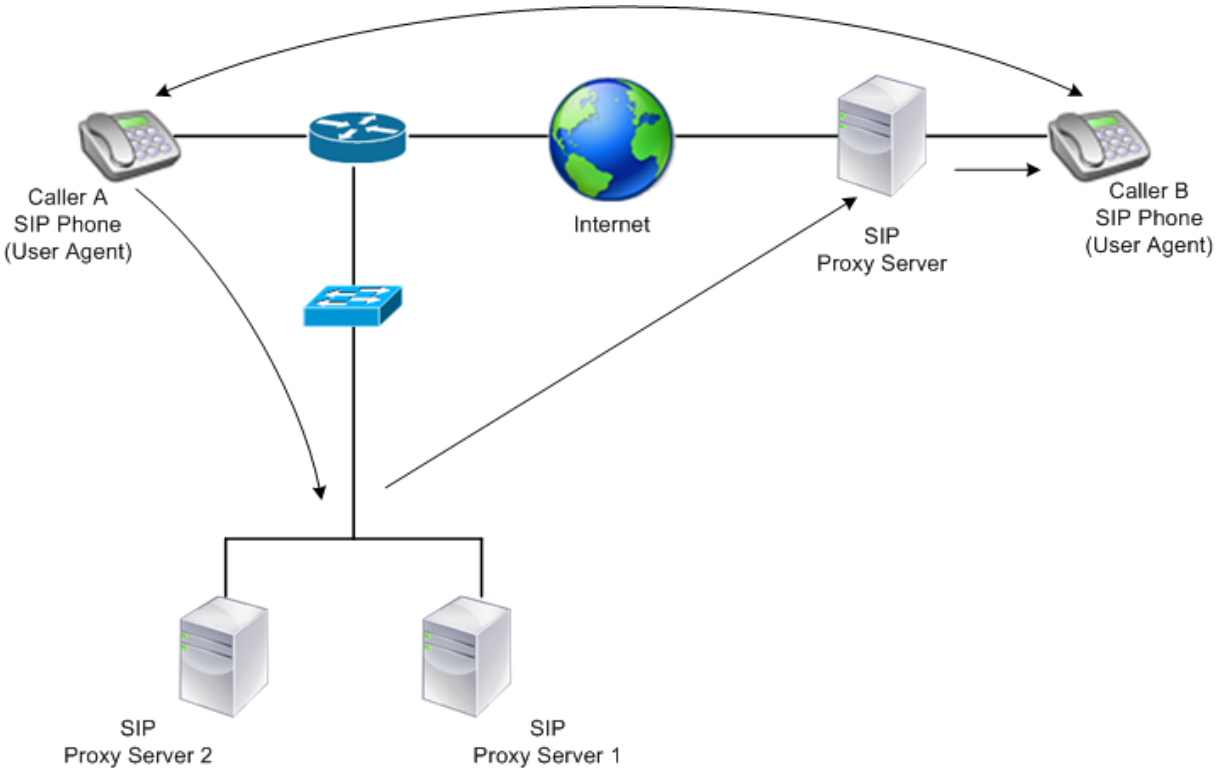
Lastverteilung einer Gruppe von SIP-Servern

October 5, 2021

Das Session Initiation Protocol (SIP) wurde entwickelt, um Multimedia-Kommunikationssitzungen zu initiieren, zu verwalten und zu beenden. Es hat sich als Standard für Internet-Telefonie (VoIP) entwickelt. SIP-Nachrichten können über TCP oder UDP übertragen werden. SIP-Nachrichten sind von zwei Arten: Anforderungsnachrichten und Antwortnachrichten.

Der Datenverkehr in einem SIP-basierten Kommunikationssystem wird über dedizierte Geräte und Anwendungen (Entitäten) geleitet. In einer Multimedia-Kommunikationssitzung tauschen diese Entitäten Nachrichten aus. Die folgende Abbildung zeigt ein grundlegendes SIP-basiertes Kommunikationssystem:

Abbildung 1. SIP-basiertes Kommunikationssystem



Mit einem Citrix ADC können Sie SIP-Nachrichten über UDP oder über TCP (einschließlich TLS) laden. Sie können den Citrix ADC so konfigurieren, dass SIP-Anforderungen an eine Gruppe von SIP-Proxyservern Lastenausgleich ausgeglichen werden. Dazu erstellen Sie einen virtuellen Lastausgleichsserver mit der Load Balancing-Methode und dem Persistenztyp auf eine der folgenden Kombinationen festgelegt:

- Call-ID-Hash-Lastausgleichsmethode ohne Persistenzeinstellung
- Call-ID-basierte Persistenz mit der geringsten Verbindung oder Roundrobin-Lastausgleichsmethode
- Regelbasierte Persistenz mit der geringsten Verbindungs- oder Roundrobin-Lastausgleichsmethode

Standardmäßig hängt der Citrix ADC RPORT über den Header der SIP-Anforderung an, so dass der Server die Antwort an die Quell-IP-Adresse und den Port zurücksendet, von dem die Anforderung stammt.

Hinweis: Damit der Lastenausgleich funktioniert, müssen Sie die SIP-Proxys so konfigurieren, dass sie keine privaten IP-Adressen oder privaten Domänen zum SIP-Header/Payload hinzufügen. SIP-Proxys müssen dem SIP-Header einen Domänennamen hinzufügen, der in die IP-Adresse des virtuellen SIP-Servers aufgelöst wird. Außerdem müssen die SIP-Proxys mit einer gemeinsamen Datenbank kommunizieren, um Registrierungsinformationen gemeinsam zu nutzen.

Serverinitiierter Datenverkehr

Konfigurieren Sie RNAT auf dem Citrix ADC für den SIP-Server initiierten ausgehenden Datenverkehr so, dass die von den Clients verwendeten privaten IP-Adressen in öffentliche IP-Adressen übersetzt werden.

Wenn Sie SIP-Parameter konfiguriert haben, die den RNAT Quell- oder Zielport enthalten, vergleicht die Appliance die Werte der Quell- und Zielports der Anforderungspakete mit dem RNAT Quellport und dem RNAT Zielport. Wenn einer der Werte übereinstimmt, aktualisiert die Appliance den VIA-Header mit RPORT. Die SIP-Antwort des Clients durchläuft dann denselben Pfad wie die Anforderung.

Für serverinitiierten SSL-Datenverkehr verwendet Citrix ADC ein integriertes Zertifikatschlüsselpaar. Wenn Sie ein benutzerdefiniertes Zertifikatschlüsselpaar verwenden möchten, binden Sie das benutzerdefinierte Zertifikatschlüsselpaar an den internen Dienst Citrix ADC namens **nsrnatsip-127.0.0.1-5061**.

Unterstützung für Richtlinien und Ausdrücke

Die Sprache der Citrix ADC Standardausdrücke enthält mehrere Ausdrücke, die mit SIP-Verbindungen (Session Initiation Protocol) arbeiten. Diese Ausdrücke können nur an SIP-basierte (sip_udp, sip_tcp oder sip_ssl) virtuelle Server und an globale Bindungspunkte gebunden werden. Sie können diese Ausdrücke in Content Switching-, Ratenbegrenzungs-, Responder- und Umschreibrichtlinien verwenden.

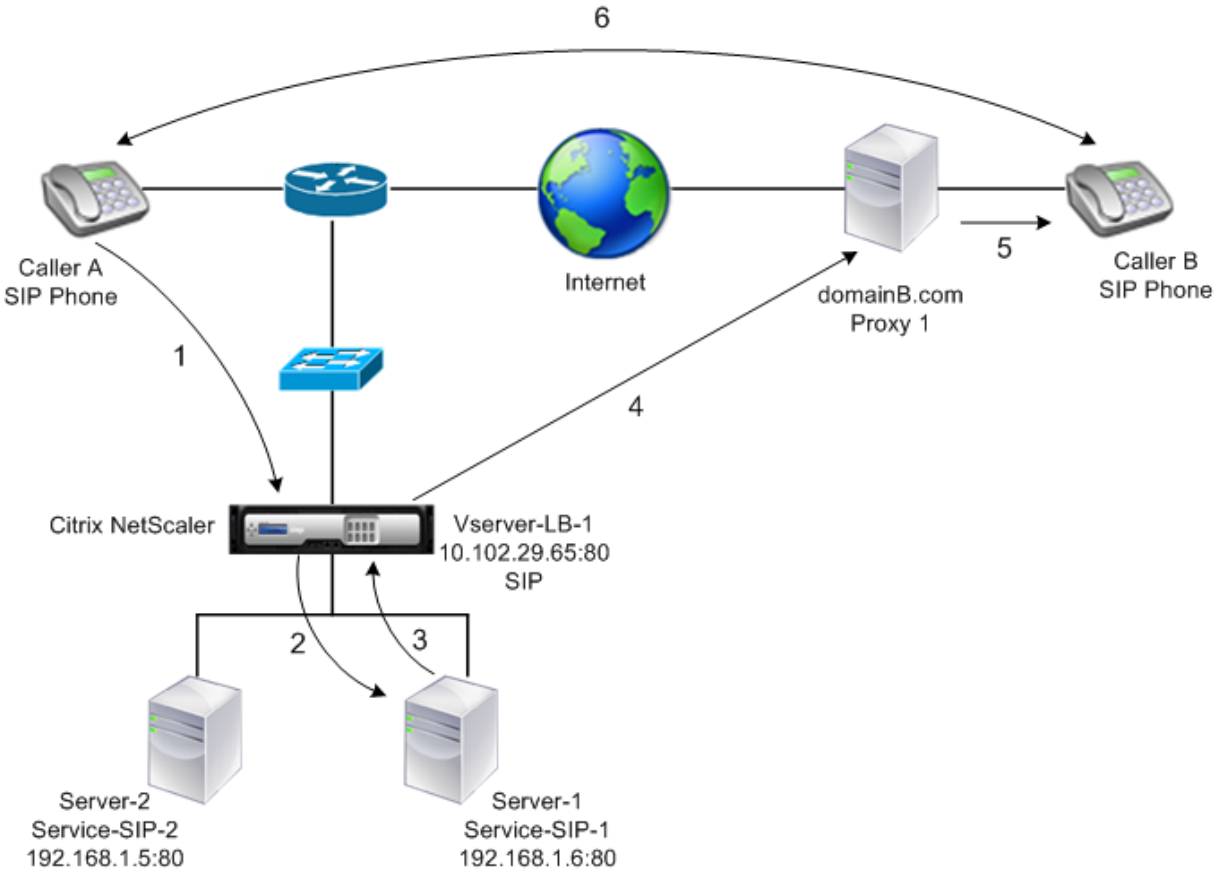
Konfigurieren des Lastenausgleichs für SIP-Signalverkehr über TCP oder UDP

Citrix ADC kann SIP-Server mit Lastenausgleich ausgleichen, die Anforderungen über UDP oder TCP senden, einschließlich TCP-Datenverkehr, der durch TLS gesichert ist. Der ADC stellt die folgenden Diensttypen zur Lastverteilung der SIP-Server bereit:

- SIP_UDP — Wird verwendet, wenn SIP-Server SIP-Nachrichten über UDP senden.
- SIP_TCP — Wird verwendet, wenn SIP-Server SIP-Nachrichten über TCP senden.
- SIP_SSL — Wird verwendet, um den SIP-Signalverkehr über TCP mithilfe von SSL oder TLS zu sichern. Citrix ADC unterstützt die folgenden Modi:
  - End-to-End-TLS-Verbindung zwischen dem Client, dem ADC und dem SIP-Server.
  - TLS-Verbindung zwischen dem Client und dem ADC und TCP-Verbindung zwischen dem ADC und dem SIP-Server.
  - TCP-Verbindung zwischen dem Client und dem ADC und TLS-Verbindung zwischen dem ADC und dem SIP-Server.

Die folgende Abbildung zeigt die Topologie eines Setups, das für den Lastausgleich einer Gruppe von SIP-Servern konfiguriert ist, die SIP-Nachrichten über TCP oder UDP senden.

Abbildung 2. SIP Load Balancing Topologie



Entitätstyp	Name	IP-Adresse	Port	Dienstart/Protokoll
Virtueller Server	Vserver-LB-1	10.102.29.65	80	SIP_UDP/SIP_TCP/SIP_SSL
Services	Service-SIP-1	192.168.1.6	80	SIP_UDP/SIP_TCP/SIP_SSL
	Service-SIP-2	192,168,1,5	80	SIP_UDP/SIP_TCP/SIP_SSL
Monitore	Standard	Ohne	80	SIP_UDP/SIP_TCP/SIP_SSL

Im Folgenden finden Sie eine Übersicht über die Konfiguration des grundlegenden Lastausgleichs für SIP-Datenverkehr:

1. Konfigurieren Sie Dienste, und konfigurieren Sie einen virtuellen Server für jeden SIP-Datenverkehr, den Sie Lastausgleich ausführen möchten:

   - **SIP_UDP** — Wenn Sie den SIP-Datenverkehr über UDP laden.
   - **SIP_TCP** — Wenn Sie den SIP-Datenverkehr über TCP laden.
   - **SIP_SSL** — Wenn Sie Lastausgleich und Sicherung des SIP-Datenverkehrs über TCP.

   Hinweis: Wenn Sie SIP_SSL verwenden, stellen Sie sicher, dass Sie ein SSL-Zertifikatschlüsselpaar erstellen. Weitere Informationen finden Sie unter Hinzufügen eines Zertifikatsschlüsselpaars.

2. Binden Sie die Dienste an die virtuellen Server.
3. Wenn Sie die Zustände der Dienste mit einem anderen Monitor als dem Standardmonitor überwachen möchten (**tcp-default**), erstellen Sie einen benutzerdefinierten Monitor und binden ihn an die Dienste. Das Citrix ADC bietet zwei benutzerdefinierte Monitortypen, **SIP-UDP** und **SIP-TCP**, zur Überwachung von SIP-Diensten.
4. Wenn Sie einen virtuellen SIP_SSL-Server verwenden, binden Sie ein SSL-Zertifikatschlüsselpaar an den virtuellen Server.
5. Wenn Sie den Citrix ADC als Gateway für die SIP-Server in Ihrer Bereitstellung verwenden, konfigurieren Sie RNAT.
6. Wenn Sie RPORT an die vom SIP-Server initiierten SIP-Nachrichten anhängen möchten, konfigurieren Sie die SIP-Parameter.

So konfigurieren Sie ein grundlegendes Lastausgleichs-Setup für SIP-Datenverkehr mit der Befehlszeilenschnittstelle

Erstellen Sie einen oder mehrere Dienste. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name> <serverName> (SIP_UDP | SIP_TCP | SIP_SSL) <port>
<!--NeedCopy-->
```

Beispiel:

```
add service Service-SIP-UDP-1 192.0.2.5 SIP_UDP 80
<!--NeedCopy-->
```

Erstellen Sie so viele virtuelle Server wie nötig, um die von Ihnen erstellten Dienste zu verarbeiten. Der virtuelle Servertyp muss mit dem Typ der Dienste übereinstimmen, die Sie an ihn binden. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <serverName> (SIP_UDP | SIP_TCP | SIP_SSL) <port>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-1 SIP_UDP 10.102.29.60 80
<!--NeedCopy-->
```


Binden Sie jeden Dienst an einen virtuellen Server. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name> <serverName>
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver Vserver-LB-1 Service-SIP-UDP-1
<!--NeedCopy-->
```

(Optional) Erstellen Sie einen benutzerdefinierten Monitor vom Typ SIP-UDP oder SIP-TCP, und binden Sie den Monitor an den Dienst. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb monitor <monitorName> <monitorType> [<interval>]

bind lb monitor <monitorName> <ServiceName>
<!--NeedCopy-->
```

Beispiel:

```
add lb monitor mon1 sip-UDP -sipMethod REGISTER -sipuRI sip:mon@test.
    com -sipregURI sip:mon@test.com -respcode 200

bind monitor mon1 Service-SIP-UDP-1
<!--NeedCopy-->
```

Wenn Sie einen virtuellen SIP_SSL-Server erstellt haben, binden Sie ein SSL-Zertifikatsschlüsselpaar an den virtuellen Server. Geben Sie an der Eingabeaufforderung Folgendes ein: Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName> -
    CA - skipCAName
<!--NeedCopy-->
```

Beispiel:


```
bind ssl vserver Vserver-LB-1 -certkeyName CertKey-SSL-1
<!--NeedCopy-->
```

Konfigurieren Sie RNAT entsprechend Ihrer Netzwerktopologie. Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um einen RNAT-Eintrag zu erstellen, der eine Netzwerkadresse als Bedingung verwendet, und SNIP als NAT-IP-Adresse, einen RNAT-Eintrag, der eine Netzwerkadresse als Bedingung verwendet, und eine eindeutige IP-Adresse als NAT-IP-Adresse, ein RNAT-Eintrag, der eine ACL verwendet die Bedingung und ein SNIP als NAT-IP-Adresse oder ein RNAT-Eintrag, der eine ACL als Bedingung und eine eindeutige IP-Adresse als NAT-IP-Adresse verwendet:

```
add rnat <name> (<network> | (<aclname> [-redirectPort <port>]))

bind rnat <name> <natIP>@ ...

show rnat
<!--NeedCopy-->
```

Beispiel:

```
add rnat RNAT-1 192.168.1.0 255.255.255.0

bind rnat RNAT-1 -natip 10.102.29.50
<!--NeedCopy-->
```

Wenn Sie ein benutzerdefiniertes Zertifikatschlüsselpaar verwenden möchten, binden Sie das benutzerdefinierte Zertifikatschlüsselpaar an den internen Dienst Citrix ADC namens nsrnatsip-127.0.0.1-5061.

```
add ssl certKey <certkeyName> -cert <string> [-key <string>]

bind ssl service <serviceName> -certkeyName <string>
<!--NeedCopy-->
```

Beispiel:

```
add ssl certKey c1 -cert cert.epm -key key.ky
```



```
2
3 bind ssl service nsrnatsip-127.0.0.1-5061 -certkeyName c1
4 <!--NeedCopy-->
```

Wenn Sie RPORT an die vom SIP-Server initiierten SIP-Nachrichten anhängen möchten, geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1 set lb sipParameters -rnatSrcPort <rnatSrcPort> -rnatDstPort<
     rnatDstPort> -retryDur <integer> -addRportVip <addRportVip> -
     sip503RateThreshold <sip503_rate_threshold_value>
2 <!--NeedCopy-->
```

Beispielkonfiguration für den Lastenausgleich des SIP-Datenverkehrs über UDP

```
1  add service service-UDP-1 10.102.29.5 SIP_UDP 80
2
3  Done
4
5  add lb vserver vserver-LB-1 SIP_UDP 10.102.29.60 80
6
7  Done
8
9  bind lb vserver vserver-LB-1 service-UDP-1
10
11 Done
12
13 add lb mon mon1 sip-udp -sipMethod REGISTER -sipuRI sip:mon@test.com -
     sipregURI sip:mon@test.com -respcode 200
14
15 Done
16
17 bind mon mon1 service-UDP-1
18
19 Done
20
21 add rnat RNAT-1 192.168.1.0 255.255.255.0
22
23 Done
24
25 set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur 1000
      -addRportVip ENABLED -sip503RateThreshold 1000
26
```



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

Beispielkonfiguration für den Lastenausgleich des SIP-Datenverkehrs über TCP

```
add service service-TCP-1 10.102.29.5 SIP_TCP 80

Done

add lb vserver vserver-LB-1 SIP_TCP 10.102.29.60 80

Done

bind lb vserver vserver-LB-1 service-TCP-1

Done

add lb mon mon1 sip-tcp -sipMethod REGISTER -sipuRI sip:mon@test.com -
    sipregURI sip:mon@test.com -respcode 200

Done

bind mon mon1 service-TCP-1

Done

add rnat RNAT-1 192.168.1.0 255.255.255.0

Done

set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur 1000
     -addRportVip ENABLED -sip503RateThreshold 1000

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

Beispielkonfiguration für Lastenausgleich und Sicherung des SIP-Datenverkehrs über TCP

```
add service service-SIP-SSL-1 10.102.29.5 SIP_SSL 80

```



```
Done

add lb vserver vserver-LB-1 SIP_SSL 10.102.29.60 80

Done

bind lb vserver vserver-LB-1 service-SIP-SSL

Done

add lb mon mon1 sip-tCP -sipMethod REGISTER -sipuRI sip:mon@test.com -
    sipregURI sip:mon@test.com -respcode 200

Done

bind mon mon1 service-SIP-SSL

Done

bind ssl vserver Vserver-LB-1 -certkeyName CertKey-SSL-1

Done

add rnat RNAT-1 192.168.1.0 255.255.255.0

Done

set lb sipParameters -rnatSrcPort 5060 -rnatDstPort 5060 -retryDur 1000
     -addRportVip ENABLED -sip503RateThreshold 1000

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

So konfigurieren Sie ein grundlegendes Load Balancing-Setup für SIP-Datenverkehr über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle**Server und fügen Sie einen virtuellen Server vom Typ SIP_UDP, SIP_TCP oder SIP_SSL hinzu.
2. Klicken Sie auf den Abschnitt **Service** und fügen Sie einen Dienst vom Typ SIP_UDP, SIP_TCP oder SIP_SSL hinzu.
3. (Optional) Klicken Sie auf den Abschnitt **Monitor** und fügen Sie einen Monitor des Typs hinzu: SIP-UDP oder SIP-TCP.

4. Binden Sie den Monitor an den Dienst, und binden Sie den Dienst an den virtuellen Server.
5. Wenn Sie einen virtuellen SIP_SSL-Server erstellt haben, binden Sie ein SSL-Zertifikatsschlüsselpaar an den virtuellen Server. Klicken Sie auf den Abschnitt Zertifikate, und binden Sie ein Zertifikatschlüsselpaar an den virtuellen Server.
6. Konfigurieren Sie RNAT entsprechend Ihrer Netzwerktopologie. So konfigurieren Sie RNAT:
   a) Navigieren Sie zu **System > Netzwerk > Routen**.
   b) Klicken Sie auf der Seite Routen auf die Registerkarte **RNAT** .
   c) Klicken Sie im Detailbereich auf **RNAT konfigurieren**.
   d) Führen Sie im Dialogfeld RNAT konfigurieren eine der folgenden Aktionen aus:
      - Wenn Sie die Netzwerkadresse als Bedingung für das Erstellen eines RNAT-Eintrags verwenden möchten, klicken Sie auf **Netzwerk** und legen Sie die folgenden Parameter fest:
        - Network
        - Netzmaske
      - Wenn Sie eine erweiterte ACL als Bedingung für das Erstellen eines RNAT-Eintrags verwenden möchten, klicken Sie auf **ACL** und legen Sie die folgenden Parameter fest:
        - ACL-Name
        - Umleitungsport
   e) Um eine SNIP-Adresse als NAT-IP-Adresse festzulegen, fahren Sie mit Schritt 7 fort.
   f) Um eine eindeutige IP-Adresse als NAT-IP festzulegen, wählen Sie in der Liste Verfügbare NAT-IP (n) die IP-Adresse aus, die Sie als NAT-IP festlegen möchten, und klicken Sie dann auf Hinzufügen. Die ausgewählte NAT-IP wird in der Liste der konfigurierten NAT-IPs angezeigt.
   g) Klicken Sie auf Erstellenund dann auf Schließen.

   Wenn Sie ein benutzerdefiniertes Zertifikatschlüsselpaar verwenden möchten, binden Sie das benutzerdefinierte Zertifikatschlüsselpaar an den internen Dienst Citrix ADC namens **nsrnatsip-127.0.0.1-5061**. So binden Sie das Paar:

   a) Navigieren Sie zu **Traffic Management > Load Balancing > Services** und klicken Sie auf die Registerkarte Interne Dienste.
   b) Wählen Sie nsrnatsip-127.0.0.1-5061 und klicken Sie auf **Bearbeiten**.
   c) Klicken Sie auf den Abschnitt **Zertifikate**, und binden Sie ein Zertifikatschlüsselpaar an den internen Dienst.
7. Wenn Sie RPORT an die vom SIP-Server initiierten SIP-Meldungen anhängen möchten, konfigurieren Sie die SIP-Parameter. Navigieren Sie zu **Traffic Management > Load Balancing** und klicken Sie auf SIP-Einstellungen ändern, legen Sie die verschiedenen SIP-Parameter fest.

Beispiel für SIP-Ausdruck und Richtlinie: Komprimierung in Clientanforderungen aktiviert

Ein Citrix ADC kann komprimierte Client-SIP-Anforderungen nicht verarbeiten, daher schlägt die Client-SIP-Anforderung fehl.

Sie können eine Responder-Richtlinie konfigurieren, die die SIP Negotiate-Nachricht vom Client abfängt und nach dem Komprimierungsheader sucht. Wenn die Nachricht einen Komprimierungsheader enthält, antwortet die Richtlinie mit 400 fehlerhafte Anforderung, sodass der Client die Anforderung erneut sendet, ohne sie zu komprimieren.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Responder-Richtlinie zu erstellen:

```
add responder action sipaction1 respondwith q{
 ”SIP/2.0 400 Bad Requestrnrn” }


Done

add responder policy sippol1

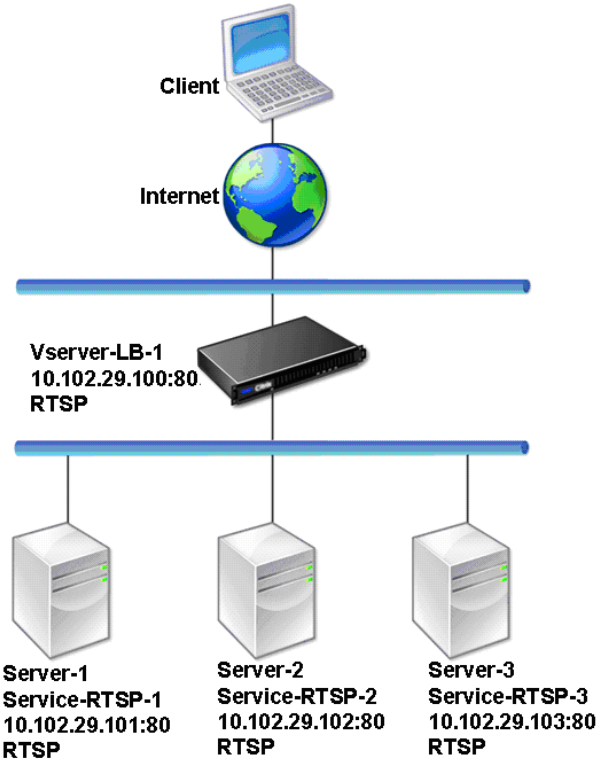
add responder policy sippol1 ”SIP.REQ.METHOD.EQ(”NEGOTIATE”)&&SIP.REQ.
   HEADER(”Compression”).EXISTS” sipaction1
<!--NeedCopy-->
```

Lastenausgleich RTSP Server

October 5, 2021

Die Citrix ADC Appliance kann die Belastung von RTSP-Servern ausgleichen, um die Leistung von Audio- und Videostreams über Netzwerke zu verbessern. Das folgende Diagramm beschreibt die Topologie eines Lastausgleichs-Setups, das für den Lastausgleich einer Gruppe von RTSP-Servern konfiguriert ist.

Abbildung 1. Load Balancing Topologie für RTSP

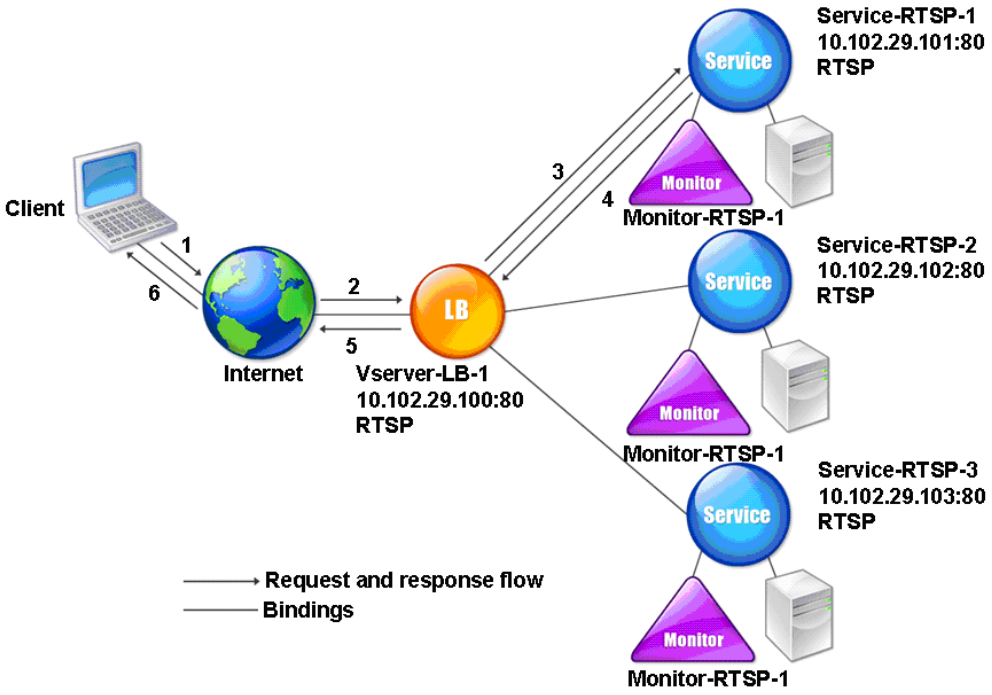


Im Beispiel sind die Dienste Service-RTSP-1, Service-RTSP-2 und Service-RTSP-3 an den virtuellen Server vServer-LB-1 gebunden. In der folgenden Tabelle sind die Namen und Werte der Beispielentitäten aufgeführt.

Entitätstyp	Name	IP-Adresse	Port	Protokoll
Virtueller Server	Vserver-LB-1	10.102.29.100	554	RTSP
Services	Service-RTSP-1	10.102.29.101	554	RTSP
	Service-RTSP-2	10.102.29.102	554	RTSP
	Service-RTSP-3	10.102.29.103	554	RTSP
Monitore	Monitor-RTSP-1	Ohne	554	RTSP

Das folgende Diagramm zeigt die Load Balancing-Entitäten, die in der RTSP-Konfiguration verwendet werden.

Abbildung 2. Load Balancing RTSP Server Entitätsmodell



Informationen zum Konfigurieren eines grundlegenden Lastenausgleichs-Setups für RTSP-Server finden Sie unter Einrichten des Basic Load Balancing. Erstellen Sie Dienste und virtuelle Server vom Typ RTSP. Wenn Sie ein grundlegendes Lastausgleichs-Setup konfigurieren, ist der standardmäßige TCP-Standardmonitor an die Dienste gebunden. Informationen zum Binden eines RTSP-Monitors an diese Dienste finden Sie unter Binden von Monitoren an Dienste. Im folgenden Verfahren wird beschrieben, wie ein Monitor erstellt wird, der RTSP-Server überprüft.

So konfigurieren Sie RTSP-Monitore mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb monitor <monitorName> <type>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add lb monitor Monitor-RTSP-1 RTSP
```



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

So konfigurieren Sie RTSP-Monitore mit der GUI

Navigieren Sie zu Traffic Management > Load Balancing > Monitore, und erstellen Sie einen Monitor vom Typ RTSP.

Load Balance-Remotedesktopprotokollserver

October 5, 2021

Remote Desktop Protocol (RDP) ist ein mehrkanalfähiges Protokoll, das separate virtuelle Kanäle für Präsentationsdaten, serielle Gerätekommunikation, Lizenzierungsinformationen, hochverschlüsselte Daten (Tastatur- und Mausaktivität) usw. ermöglicht.

RDP wird verwendet, um einem anderen Computer im Netzwerk eine GUI zur Verfügung zu stellen. RDP wird mit Windows-Terminalservern verwendet, um schnellen Zugriff mit fast Echtzeitübertragung von Mausbewegungen und Tastendrucken auch über Verbindungen mit geringer Bandbreite zu ermöglichen.

Wenn mehrere Terminalserver bereitgestellt werden, um Remotedesktopdienste bereitzustellen, bietet die Citrix ADC Appliance den Lastenausgleich der Terminalserver (Windows 2003 und 2008 Server Enterprise Editions). Manchmal möchte ein Benutzer, der remote auf eine Anwendung zugreift, die Anwendung möglicherweise auf dem Remotecomputer ausgeführt lassen, aber den lokalen Computer herunterfahren. Der Benutzer schließt daher die lokale Anwendung, ohne sich von der Remote-Anwendung abzumelden. Nach dem erneuten Verbinden mit dem Remote-Computer muss der Benutzer in der Lage sein, mit der Remote-Anwendung fortzufahren. Um diese Funktionalität bereitzustellen, berücksichtigt die Citrix ADC RDP-Implementierung das Routingtoken (Cookie), das vom Terminaldienstes-Sitzungsverzeichnis oder Broker festgelegt wurde, so dass der Client wieder eine Verbindung zu demselben Terminalserver herstellen kann, mit dem er zuvor verbunden war. Das auf Windows 2003-Terminalserver implementierte Sitzungsverzeichnis wird als Broker auf Windows 2008-Terminalserver bezeichnet.

Wenn eine TCP-Verbindung zwischen dem Client und dem virtuellen Lastausgleichsserver hergestellt wird, wendet Citrix ADC die angegebene Lastausgleichsmethode an und leitet die Anforderung an einen der Terminalserver weiter. Der Terminalserver überprüft das Sitzungsverzeichnis, um festzustellen, ob der Client eine Sitzung auf einem anderen Terminalserver in der Domäne ausgeführt hat.

Wenn auf einem anderen Terminalserver keine aktive Sitzung vorhanden ist, antwortet der Terminalserver mit der Clientanforderung, und die Citrix ADC Appliance leitet die Antwort an den Client

weiter.

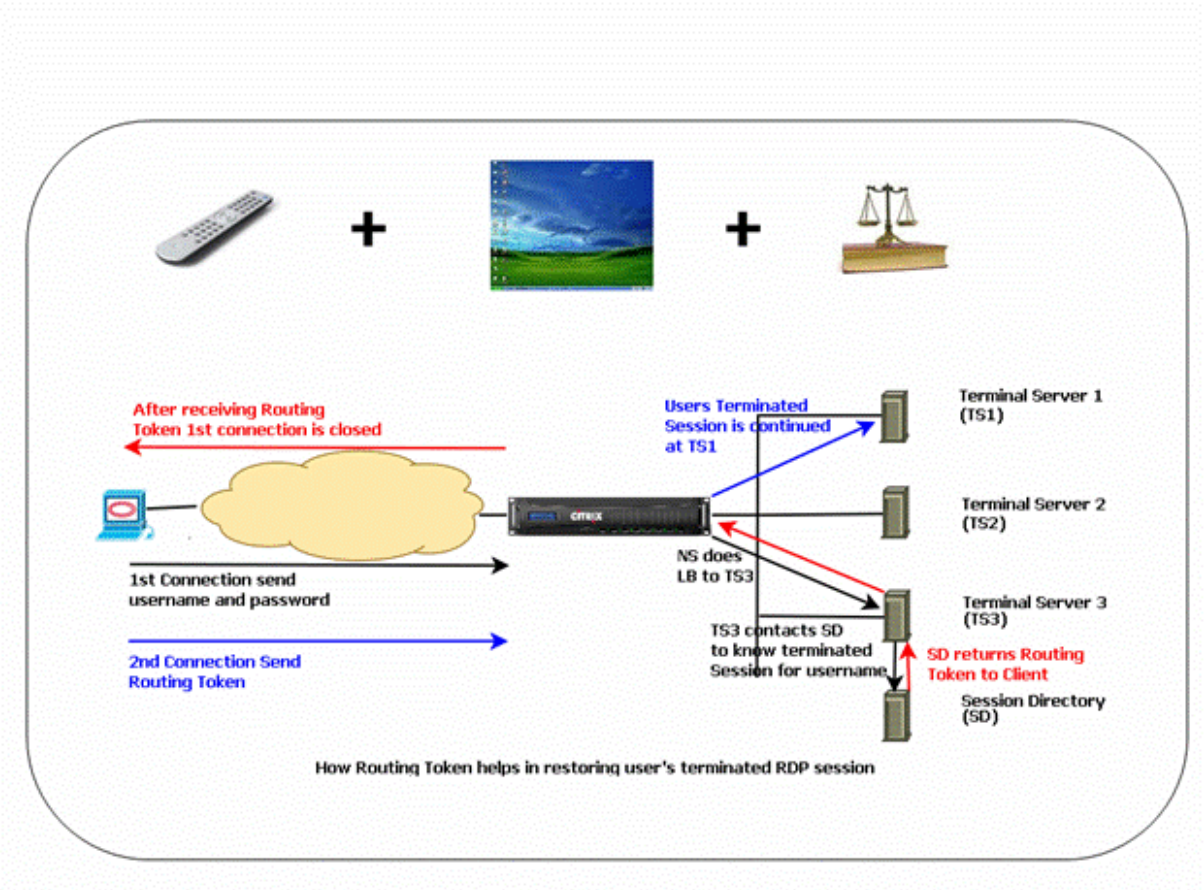
Wenn auf einem anderen Terminalserver eine aktive Sitzung stattfindet, fügt der Terminalserver, der die Anforderung erhält, ein Cookie (als Routing-Token bezeichnet) mit den Details der aktiven Sitzung ein und gibt die Pakete an die Citrix ADC Appliance zurück, die das Paket an den Client zurückgibt. Der Server schließt die Verbindung mit dem Client. Wenn der Client erneut versucht, eine Verbindung herzustellen, liest Citrix ADC die Cookie-Informationen und leitet das Paket an den Terminalserver weiter, auf dem der Client eine aktive Sitzung hat.

Der Benutzer auf dem Clientcomputer erlebt eine Fortsetzung des Dienstes und muss keine spezifischen Maßnahmen ergreifen.

Hinweis: Für das Windows-Sitzungsverzeichnisfeature ist der Remotedesktopclient erforderlich, der zuerst mit Windows XP veröffentlicht wurde. Wenn eine Sitzung mit einem Windows 2000- oder Windows NT 4.0-Terminalserver-Client getrennt wird und der Client wieder eine Verbindung herstellt, wird der Server, mit dem die Verbindung hergestellt wird, durch den Lastausgleichsalgorithmus ausgewählt.

Das folgende Diagramm beschreibt den RDP-Lastenausgleich.

Abbildung 1. Load Balancing Topologie für RDP



> **Hinweis:**
>
> - Wenn ein RDP-Dienst konfiguriert ist, wird die Persistenz automatisch mit einem Routing-token verwaltet. Sie müssen die Persistenz nicht explizit aktivieren.
> - Die Citrix ADC Appliance unterstützt nur IP-basierte Cookies.
> - Das nsrdp.pl-Skript wird auf keiner aktuellen Version von Windows-Servern unterstützt.

Stellen Sie sicher, dass die getrennten RDP-Sitzungen auf den Terminalservern am Backend gelöscht werden, um ein Flattern zwischen zwei Terminalservern zu vermeiden, wenn eine RDP-Sitzung ohne Abmeldung getrennt wird. Weitere Informationen finden Sie unter `https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc758177(v=ws.10)##BKMK_2`

Wenn Sie einen RDP-Dienst hinzufügen, fügt Citrix ADC standardmäßig einen Monitor vom Typ TCP hinzu und bindet ihn an den Dienst. Der Standardmonitor ist ein einfacher TCP-Monitor, der überprüft, ob ein Listening-Prozess an dem für den RDP-Dienst angegebenen 3389-Port auf dem Server existiert. Wenn ein Listing-Prozess bei 3389 vorhanden ist, markiert Citrix ADC diesen Dienst als UP, und wenn kein Listing-Prozess vorhanden ist, markiert er den Dienst als DOWN.

Für eine effizientere Überwachung eines RDP-Dienstes können Sie zusätzlich zum Standardmonitor einen Skriptmonitor konfigurieren, der für das RDP-Protokoll vorgesehen ist. Wenn Sie den Skriptmonitor konfigurieren, öffnet Citrix ADC eine TCP-Verbindung zum angegebenen Server und sendet ein RDP-Paket. Der Monitor markiert den Dienst nur dann als UP, wenn er eine Bestätigung der Verbindung vom physischen Server erhält. Aus diesem Grund kann Citrix ADC vom Skriptmonitor aus wissen, ob der RDP-Dienst bereit ist, eine Anforderung zu bedienen.

Der Monitor ist ein Benutzermonitor, und das Skript befindet sich im Citrix ADC unter /nsconfig/monitors/nsrdp.pl. Wenn Sie den Benutzermonitor konfigurieren, führt Citrix ADC das Skript automatisch aus. Um den Skriptmonitor zu konfigurieren, fügen Sie den Monitor hinzu und binden ihn an den RDP-Dienst.

Um den RDP-Lastenausgleich zu konfigurieren, erstellen Sie Dienste vom Typ RDP und binden sie an einen virtuellen RDP-Server.

So konfigurieren Sie RDP-Load Balancing-Dienste mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um ein RDP-Load Balancing-Setup zu konfigurieren und die Konfiguration zu überprüfen:

```
1 add service <name>@ <serverName> <serviceType> <port>
2 <!--NeedCopy-->
```

Hinweis: Wiederholen Sie den vorhergehenden Befehl, um weitere Services hinzuzufügen.

Beispiel

```
> add service ser1 10.102.27.182 RDP 3389
Done
> add service ser2 10.102.27.183 RDP 3389
Done
>show service ser1
ser1 (10.102. 27.182:3389) - RDP
        State: UP
…
            Server Name: 10.102.27.182
            Server ID : 0           Monitor Threshold : 0
        Down state flush: ENABLED
…
1)      Monitor Name: tcp-default
                State: UP       Weight: 1
…
                Response Time: 4.152 millisec
 Done
<!--NeedCopy-->
```

So konfigurieren Sie RDP-Load Balancing-Dienste mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und erstellen Sie Services vom Typ RDP.

So konfigurieren Sie einen virtuellen RDP-Load Balancing Server mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen virtuellen RDP-Load Balancing Server zu konfigurieren und die Konfiguration zu überprüfen:

```
add lb vserver <name>@ <serviceType> <ipAddress> <port>

bind lb vserver <name>@ <serviceName>

Bind all the RDP services to be load balanced to the virtual server.
<!--NeedCopy-->
```


Beispiel:

Dieses Beispiel verfügt über zwei RDP-Dienste, die an den virtuellen RDP-Server gebunden sind.

```
add lb vs v1 rdP 10.102.27.186 3389
Done

bind lb vs v1 ser1
service ”ser1” bound

bind lb vs v1 ser2
service ”ser2” bound
Done

sh lb vs v1
v1 (10.102.27.186:3389) - RDP   Type: ADDRESS
State: UP
…
No. of Bound Services :  2 (Total)       2 (Active)
Configured Method: LEASTCONNECTION
  Current Method: Round Robin, Reason: A new service is bound
Mode: IP
Persistence: NONE
  L2Conn: OFF

1) ser1 (10.102.27.182: 3389) - RDPState: UP   Weight: 1
2) ser2 (10.102.27.183: 3389) - RDPState: UP   Weight: 1
Done
<!--NeedCopy-->
```

So konfigurieren Sie einen virtuellen RDP-Lastausgleichsserver mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, erstellen Sie einen virtuellen Server vom Typ RDP und binden Sie RDP-Dienste an diesen virtuellen Server.

So konfigurieren Sie einen Skriptmonitor für RDP-Dienste mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:


```
add lb monitor <monitorName> USER -scriptName nsrdp.pl

bind lb monitor <monitorName> <rdpServiceName>
<!--NeedCopy-->
```

Beispiel:

```
add service ser1 10.102.27.182 RDP 3389

add lb monitor RDP_MON USER -scriptName nsrdp.pl

bind lb monitor RDP_MON ser1

<!--NeedCopy-->
```

So konfigurieren Sie einen Skriptmonitor für RDP-Dienste mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**, und erstellen Sie einen Monitor vom Typ USER.
2. Wählen Sie unter Spezielle Parameter in der Liste Skriptname die Option nsrdp.pl aus, und binden Sie diesen Monitor dann an einen RDP-Dienst.

Lastausgleich des Microsoft Exchange-Servers

May 10, 2022

Dieses Dokument enthält die empfohlenen Konfigurationsbeispiele für den Lastenausgleich des Microsoft Exchange-Servers mit der Citrix ADC-Appliance.

Citrix ADM StyleBooks vereinfacht Citrix ADC Load Balancing-Konfigurationen für Exchange. Weitere Informationen finden Sie unter Microsoft Exchange StyleBook.

> Hinweis:
>
> Der Lastenausgleich von Microsoft Exchange ist mit einem einzigen virtuellen Lastenausgleichsserver nicht möglich. Befolgen Sie stattdessen die empfohlenen Konfigurationen in diesem Dokument.

Unterschiede in Microsoft Exchange 2016 und neueren Versionen

- Sie müssen keine statischen RPC-Ports (Remote Procedure Call) an Exchange 2016 konfigurieren, da keine RPC-Ports verwendet werden.
- Alle Abschnitte mit der Bezeichnung “für Exchange-Versionen unter 2016” sind mit Exchange 2016 nicht erforderlich.
- Wenn Sie bereits eine der Versionen außerhalb von 2016 konfiguriert haben und auf 2016 migrieren, müssen Sie sie nicht entfernen. Denn selbst wenn sie existieren, gibt es keine Probleme.

Wichtige Hinweise

- Für Remoteprozeduraufrufe (RPC) mit dem Exchange-Server unter 2016 müssen die Exchange-CAS-Server für statische Portzuweisungen konfiguriert sein. Weitere Informationen finden Sie unter Exchange 2010-Clientzugriffsserver: Konfigurieren statischer RPC-Ports Microsoft-Dokumentation.
- Diese Konfiguration setzt voraus, dass die Citrix ADC-Appliance für SSL Offload verwendet wird. Weitere Informationen finden Sie unter Konfigurieren von SSL-Offloading in Exchange 2010 oder Konfigurieren von SSL-Abladungen in Exchange 2013.aspx.
- Wenn Sie die SSL-Offload-Funktion der Citrix ADC-Appliance nicht verwenden möchten, ändern Sie die Dienstgruppe `CAS_servicegroup_http` und die Monitore in Typ `SSL` und deren Bindungen an den Port `443`.
- Der Überlastungsschutz ist nicht mit Microsoft Exchange kompatibel. Aktivieren Sie es nicht für einen Dienst oder eine Dienstgruppe, die mit Microsoft Exchange in Verbindung steht. Die Aktivierung des Überlastungsschutzes verursacht Probleme mit der Konnektivität und Zuverlässigkeit.
- Ersetzen Sie die folgenden Variablen durch die richtigen Informationen:
  - {HTTP Public IP} —IP-Adresse für den öffentlichen Exchange-HTTP-Endpunkt
  - {RPC Public IP} —IP-Adresse für den öffentlichen Exchange RPC-Endpunkt (kann identisch mit HTTP Public IP sein)
  - {Timeout} —Gewünschtes Timeout (in Sekunden). Es wird empfohlen, so lang zu sein wie die Standard-Arbeitsschichtzeit (also 8 Stunden)
  - {perstimeOut} —Gewünschtes Timeout (in Minuten). Muss der vorherigen Timeout-Einstellung entsprechen.
  - {AB-Port} —TCP-Port des RPC-Adressbuchs (normalerweise 59601)
  - {CA Port} —RPC-Clientzugriff-TP-Port (normalerweise 59600)
  - {certKey} —SSL-Zertifikatsschlüssel
  - {CAS-1 Server} —IP-Adresse des CAS-Servers
  - {CAS-2 Server} —IP-Adresse des CAS-Servers

Empfohlene Konfigurationsbeispiele für alle Versionen von Microsoft Exchange Server

Service-Gruppen:

```
add serviceGroup CAS_servicegroup_http HTTP -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout { Timeout }
 -svrTimeout { Timeout }
 -CKA NO -TCPB NO -CMP YES
add serviceGroup CAS_servicegroup_rpc_epm TCP -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout { Timeout }
 -svrTimeout { Timeout }
 -CKA NO -TCPB NO -CMP NO
bind serviceGroup CAS_servicegroup_http {
 CAS-1 Server }
 80 -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_http {
 CAS-2 Server }
 80 -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_rpc_epm {
 CAS-1 Server }
 135 -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_rpc_epm {
 CAS-2 Server }
 135 -CustomServerID ""None""
<!--NeedCopy-->
```

Monitore:

```
add lb monitor CAS_monitor_rpc_epm TCP -LRTM ENABLED -destPort 135
add lb monitor mon_http_ecv HTTP-ECV -recv 403 -LRTM DISABLED
bind serviceGroup CAS_servicegroup_http -monitorName mon_http_ecv
bind serviceGroup CAS_servicegroup_rpc_epm -monitorName CAS_monitor_rpc_epm
<!--NeedCopy-->
```

Lastenausgleich virtueller Server:


```
add lb vserver CAS_vserver_owa SSL 0.0.0.0 0 -persistenceType
    COOKIEINSERT -timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }

add lb vserver CAS_vserver_as SSL 0.0.0.0 0 -persistenceType RULE -
    timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -rule "HTTP.REQ.HEADER("Authorization")" -
      cltTimeout {
 Timeout }

add lb vserver CAS_vserver_oa SSL 0.0.0.0 0 -timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }

add lb vserver CAS_vserver_ews SSL 0.0.0.0 0 -timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }

add lb vserver CAS_vserver_ad SSL 0.0.0.0 0 -timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }

add lb vserver CAS_vserver_oab SSL 0.0.0.0 0 -timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }

set ssl vserver CAS_vserver_owa -sslRedirect ENABLED
bind ssl vserver CAS_vserver_owa -certkeyName {
 CertKey }

bind ssl vserver CAS_vserver_oab -certkeyName {
 CertKey }

bind ssl vserver CAS_vserver_as -certkeyName {
 CertKey }

bind ssl vserver CAS_vserver_oa -certkeyName {
 CertKey }
```

```
43
44 bind ssl vserver CAS_vserver_ews -certkeyName {
45  CertKey }
46
47 bind ssl vserver CAS_vserver_ad -certkeyName {
48  CertKey }
49
50 bind lb vserver CAS_vserver_owa CAS_servicegroup_http
51 bind lb vserver CAS_vserver_oab CAS_servicegroup_http
52 bind lb vserver CAS_vserver_as CAS_servicegroup_http
53 bind lb vserver CAS_vserver_oa CAS_servicegroup_http
54 bind lb vserver CAS_vserver_ews CAS_servicegroup_http
55 bind lb vserver CAS_vserver_ad CAS_servicegroup_http
56 add lb vserver CAS_vserver_rpc_epm TCP {
57  RPC Public IP }
58   135 -timeout {
59  PersTimeout }
60   -cltTimeout {
61  Timeout }
62   -comment ”vserver for RPC End Point Mapper”
63 bind lb vserver CAS_vserver_rpc_epm CAS_servicegroup_rpc_epm
64 <!--NeedCopy-->
```

Persistenzgruppe:

```
1 add lb group CAS_persistency_group_sourceip
2 bind lb group CAS_persistency_group_sourceip CAS_vserver_oa
3 bind lb group CAS_persistency_group_sourceip CAS_vserver_oab
4 bind lb group CAS_persistency_group_sourceip CAS_vserver_ews
5 bind lb group CAS_persistency_group_sourceip CAS_vserver_ad
6 bind lb group CAS_persistency_group_sourceip CAS_vserver_rpc_epm
7 set lb group CAS_persistency_group_sourceip -persistenceType SOURCEIP -
     timeout {
8  PersTimeout }
9
10 <!--NeedCopy-->
```

Content Switching für HTTP-Dienste:

```
1 add cs vserver CAS_vserver_cs SSL {
2  Public IP }
3   443 -cltTimeout {
```



```
 Timeout }
  -caseSensitive OFF -comment "Exchange CS VServer"
bind ssl vserver CAS_vserver_cs -certkeyName {
 CertKey }

add cs action CAS_action_cs_owa -targetLBVserver CAS_vserver_owa
add cs action CAS_action_cs_oab -targetLBVserver CAS_vserver_oab
add cs action CAS_action_cs_as -targetLBVserver CAS_vserver_as
add cs action CAS_action_cs_oa -targetLBVserver CAS_vserver_oa
add cs action CAS_action_cs_ews -targetLBVserver CAS_vserver_ews
add cs action CAS_action_cs_autodiscover -targetLBVserver
   CAS_vserver_ad
add cs policy CAS_policy_cs_owa -rule "HTTP.REQ.URL.SET_TEXT_MODE(
   IGNORECASE).STARTSWITH("/owa")" -action CAS_action_cs_owa
add cs policy CAS_vserver_oab -rule "HTTP.REQ.URL.SET_TEXT_MODE (
   IGNORECASE).STARTSWITH("/OAB")"
add cs policy CAS_policy_cs_as -rule "HTTP.REQ.URL.SET_TEXT_MODE(
   IGNORECASE).STARTSWITH("/Microsoft-Server-ActiveSync")" -action
   CAS_action_cs_as
add cs policy CAS_policy_cs_autodiscover -rule "HTTP.REQ.URL.
   SET_TEXT_MODE(IGNORECASE).STARTSWITH("/Autodiscover")" -action
   CAS_action_cs_autodiscover
add cs policy CAS_policy_cs_oa -rule "HTTP.REQ.URL.SET_TEXT_MODE(
   IGNORECASE).STARTSWITH("/rpc")" -action CAS_action_cs_oa
add cs policy CAS_policy_cs_ews -rule "HTTP.REQ.URL.SET_TEXT_MODE(
   IGNORECASE).STARTSWITH("/EWS")" -action CAS_action_cs_ews

bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_oa -priority
   90
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_owa -priority
   100
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_oab -priority
   100
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_as -priority
   110
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_autodiscover -
   priority 120
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_ews -priority
   130
bind cs vserver CAS_vserver_cs -lbvserver CAS_vserver_owa
<!--NeedCopy-->
```


Empfohlene Konfigurationsbeispiele für Versionen von Microsoft Exchange Server unter 2016

Weitere Servicegruppen:

```
add serviceGroup CAS_servicegroup_rpc_ca TCP -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout {
 Timeout }
  -svrTimeout {
 Timeout }
  -CKA NO -TCPB NO -CMP NO
add serviceGroup CAS_servicegroup_rpc_ab TCP -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout {
 Timeout }
  -svrTimeout {
 Timeout }
  -CKA NO -TCPB NO -CMP NO
bind serviceGroup CAS_servicegroup_rpc_ca {
 CAS-1 Server }
  {
 CA Port }
  -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_rpc_ca {
 CAS-2 Server }
  {
 CA Port }
  -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_rpc_ab {
 CAS-1 Server }
  {
 AB Port }
  -CustomServerID ""None""
bind serviceGroup CAS_servicegroup_rpc_ab {
 CAS-2 Server }
  {
 AB Port }
  -CustomServerID ""None""
<!--NeedCopy-->
```

Weitere Monitore:

```
add lb monitor CAS_monitor_rpc_ca TCP -LRTM ENABLED -destPort {
```



```
 CA Port }

add lb monitor CAS_monitor_rpc_ab TCP -LRTM ENABLED -destPort {
 AB Port }

bind serviceGroup CAS_servicegroup_rpc_ca -monitorName
    CAS_monitor_rpc_ca
bind serviceGroup CAS_servicegroup_rpc_ab -monitorName
    CAS_monitor_rpc_ab
<!--NeedCopy-->
```

Zusätzliche virtuelle Lastenausgleichsserver:

```
add lb vserver CAS_vserver_rpc_ab TCP {
 RPC Public IP }
  {
 AB Port }
  -timeout {
 PersTimeout }
  -cltTimeout {
 Timeout }
  -comment ”vserver for  RPC Address Book”
add lb vserver CAS_vserver_rpc_ca TCP {
 RPC Public IP }
  {
 CA Port }
  -timeout {
 PersTimeout }
  -cltTimeout {
 Timeout }
  -comment ”vserver for  RPC Client Access”
bind lb vserver CAS_vserver_rpc_ab CAS_servicegroup_rpc_ab
bind lb vserver CAS_vserver_rpc_ca CAS_servicegroup_rpc_ca
<!--NeedCopy-->
```

Zusätzliche Persistenzgruppe:

```
bind lb group CAS_persistency_group_sourceip CAS_vserver_rpc_ab
bind lb group CAS_persistency_group_sourceip CAS_vserver_rpc_ca
<!--NeedCopy-->
```


Empfohlene Konfigurationsbeispiele für Versionen von Microsoft Exchange Server 2016 und neuer

Zusätzlicher virtueller Lastenausgleichsserver:

```
add lb vserver CAS_vserver_mapi SSL 0.0.0.0 0 -timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }

bind ssl vserver CAS_vserver_mapi -certkeyName {
 CertKey }

bind lb vserver CAS_vserver_mapi CAS_servicegroup_http
<!--NeedCopy-->
```

Zusätzliche Persistenzgruppe:

```
bind lb group CAS_persistency_group_sourceip CAS_vserver_mapi
<!--NeedCopy-->
```

Content Switching für HTTP-Dienste:

```
add cs action CAS_action_cs_mapi -targetLBVserver CAS_vserver_mapi
add cs policy CAS_policy_cs_mapi -rule ”HTTP.REQ.URL.SET_TEXT_MODE(
    IGNORECASE).STARTSWITH(”/mapi”)” -action CAS_action_cs_mapi
bind cs vserver CAS_vserver_cs -policyName CAS_policy_cs_mapi -priority
     140
<!--NeedCopy-->
```

Optionale Konfigurationen

HTTPS-Weiterleitung für Outlook Web App (OWA):

```
add lb vserver CAS_vserver_owa_http_redirect HTTP {
 HTTP Public IP }
  80 -persistenceType COOKIEINSERT -timeout {
 PersTimeout }
```



```
5    -lbMethod ROUNDROBIN -redirectURL "https://mail.example.com/owa" -
        cltTimeout {
6   Timeout }
7
8  <!--NeedCopy-->
```

HINWEIS: Ersetzen Sie durch die richtige HTTPS-Umleitungs-URL.

Richtlinie für /owa rewrite:

```
1  add rewrite action owa_rewrite replace http.REQ.URL ""/owa""
2  add rewrite policy owa_rewrite_policy "http.req.url.eq("/")"
      owa_rewrite
3  bind lb vserver CAS_vserver_owa -policyName owa_rewrite_policy -
      priority 100 -gotoPriorityExpression END -type REQUEST
4  add responder action action_responder_owa redirect ""https://www.
      example.com/owa""
5  add responder policy policy_responder_owa HTTP.REQ.IS_VALID
      action_responder_owa
6  set responder param -undefAction NOOP
7  bind lb vserver CAS_vserver_owa -policyName policy_responder_owa -
      priority 100 -gotoPriorityExpression END -type REQUEST
8  <!--NeedCopy-->
```

HINWEIS: Ersetzen Sie durch die richtige HTTPS-Umleitungs-URL.

Unterstützung für SMTP:

Für die folgende Konfiguration muss USIP aktiviert sein, damit die CAS-Server die IP-Adresse des sendenden SMTP-Servers zur Validierung sehen können. Diese Konfiguration erfordert auch, dass das Standardgateway des CAS-Servers so konfiguriert ist, dass es auf die SNIP-Adresse der ADC-Appliance zeigt.

```
1  add lb vserver CAS_vserver_smtp TCP {
2   HTTP Public IP }
3    25 -persistenceType SOURCEIP -timeout 60 -lbMethod LEASTCONNECTION -
        cltTimeout 30
4  add serviceGroup CAS_servicegroup_smtp TCP -maxClient 0 -maxReq 0 -cip
      DISABLED -usip YES -SP OFF -useproxyport YES -cltTimeout 30 -
      svrTimeout 30 -CKA NO -TCPB NO -CMP NO
5  bind serviceGroup CAS_servicegroup_smtp {
6   CAS-1 Server }
7    25 -CustomServerID ""None"" bind serviceGroup CAS_servicegroup_smtp {
```



```
 CAS-2 Server }
  25 -CustomServerID ””None””
bind lb vserver CAS_vserver_smtp CAS_servicegroup_smtp
<!--NeedCopy-->
```

Unterstützung für Post Office Protocol Version 3 (POP3):

```
add lb vserver CAS_vserver_pop3 TCP {
 HTTP Public IP }
  110 -persistenceType SOURCEIP -timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
 Timeout }

add serviceGroup CAS_servicegroup_pop3 TCP -maxClient 0 -maxReq 0 -cip
    DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout {
 Timeout }
  -svrTimeout {
 Timeout }
  -CKA NO -TCPB NO -CMP NO
bind serviceGroup CAS_servicegroup_pop3 {
 CAS-1 Server }
  110 -CustomServerID ””None”” bind serviceGroup CAS_servicegroup_pop3
      {
 CAS-2 Server }
  110 -CustomServerID ””None””
bind lb vserver CAS_vserver_pop3 CAS_servicegroup_pop3
<!--NeedCopy-->
```

> Hinweis:
>
> Sie können die vorhergehende Konfiguration für SSL-verschlüsseltes POP3 durchführen, indem Sie den Port auf 995 und die virtuellen Server-/Diensttypen in SSL ändern. Binden Sie auch ein geeignetes SSL-Zertifikat.

Unterstützung für IMAP:

```
add lb vserver CAS_vserver_imap TCP {
 HTTP Public IP }
  143 -persistenceType SOURCEIP -timeout {
 PersTimeout }
  -lbMethod LEASTCONNECTION -cltTimeout {
```



```
6   Timeout }
7
8  add serviceGroup CAS_servicegroup_imap TCP -maxClient 0 -maxReq 0 -cip
       DISABLED -usip NO -SP OFF -useproxyport YES -cltTimeout {
9   Timeout }
10   -svrTimeout {
11  Timeout }
12   -CKA NO -TCPB NO -CMP NO
13 bind serviceGroup CAS_servicegroup_imap {
14  CAS-1 Server }
15   143 -CustomServerID ""None"" bind serviceGroup CAS_servicegroup_imap
        {
16  CAS-2 Server }
17   143 -CustomServerID ""None""
18 bind lb vserver CAS_vserver_imap CAS_servicegroup_imap
19 <!--NeedCopy-->
```

> Hinweis:
>
> Sie können die vorhergehende Konfiguration für SSL-verschlüsselte IMAP durchführen, indem Sie den Port auf 993 und die virtuellen Server-/Diensttypen in SSL ändern. Binden Sie auch ein geeignetes SSL-Zertifikat.

Andere Ressourcen

- Konfigurieren von Load Balancing-Servern für Microsoft Exchange mit E-Mail-Sicherheitsfilterung
- Bereitstellen von NetScaler mit Microsoft Exchange 2016

Anwendungsfall 1: SMPP-Lastausgleich

October 5, 2021

Millionen von Kurznachrichten werden täglich zwischen Einzelpersonen und Mehrwertdienstleistern wie Banken, Werbetreibenden und Verzeichnisdiensten ausgetauscht, indem das Short Message Peer to Peer (SMPP) -Protokoll verwendet wird. Häufig verzögert sich die Nachrichtenübermittlung, da Server überlastet sind und der Datenverkehr nicht optimal auf die Server verteilt wird. Das Citrix ADC unterstützt den SMPP-Lastenausgleich und bietet eine optimale Verteilung der Nachrichten auf Ihre Server, wodurch schlechte Leistung und Ausfälle vermieden werden.

Citrix ADC führt den Lastenausgleich auf der Serverseite durch, wenn Nachrichten von Clients empfangen werden, und auf der Clientseite, wenn Nachrichten von Servern empfangen werden.

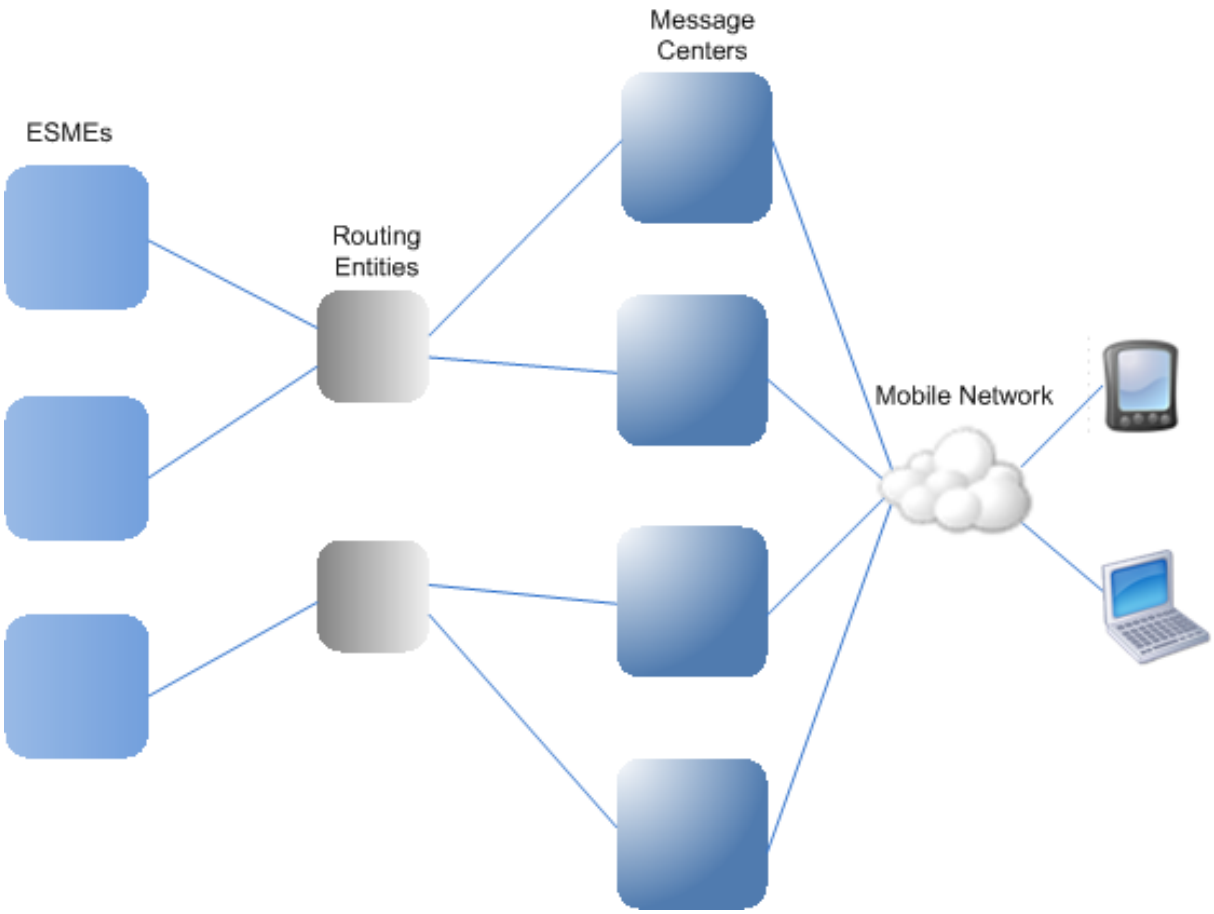
Der Lastenausgleich von SMPP-Nachrichten durch den Citrix ADC bietet folgende Vorteile:

- Bessere Lastverteilung auf Servern, was zu einer schnelleren Reaktionszeit für Endbenutzer führt
- Überwachung des Serverzustands und bessere Failover-Funktionen
- Schnelles und einfaches Hinzufügen neuer Server (Message Center) ohne Änderung der Client-Konfiguration
- Hohe Verfügbarkeit

Einführung in SMPP

SMPP ist ein Anwendungsschicht-Protokoll für die Übertragung von Kurznachrichten zwischen externen Kurznachrichtentitäten (ESME), Routing-Entitäten (RE) und Message Centers (MC) über langlebige TCP-Verbindungen. Es wird zum Senden von Kurznachrichtendiensten (SMS) zwischen Freunden, Kontakten und Dritten wie Banken (Mobile Banking), Werbetreibenden (Mobile Commerce) und Verzeichnisdiensten verwendet. Nachrichten von einer ESME (nicht mobile Entität) kommen am MC an, die sie an Kurznachrichteneinheiten (SMEs) wie Mobiltelefone verteilt. SMPP wird auch von SMEs verwendet, um Kurznachrichten an Dritte zu senden (zum Beispiel für den Kauf von Produkten, Rechnungszahlung und Geldüberweisung). Diese Meldungen kommen am MC an und werden an den Ziel-MC oder ESME weitergeleitet.

Das folgende Diagramm zeigt die verschiedenen SMPP-Entitäten: ESMEs, REs und MCs in einem Mobilfunknetz.



Architekturübersicht der verschiedenen SMPP-Entitäten in einem Mobilfunknetz

Hinweis: Die Begriffe Client und ESME werden im gesamten Dokument austauschbar verwendet.

Ein ESME (Client) öffnet eine Verbindung zum MC in einem der drei Modi: als Sender, Empfänger oder Transceiver. Als Transmitter kann er nur Nachrichten zur Zustellung senden. Als Empfänger kann er nur Nachrichten empfangen. Als Transceiver kann die ESME sowohl Nachrichten senden als auch empfangen. Die ESME sendet dem MC eine der drei Meldungen (auch PDUs genannt): bind_transmitter, bind_receiver oder bind_transceiver. Der MC antwortet je nach Anforderung mit einem bind_transmitter_resp, bind_receiver_resp oder bind_transceiver_resp.

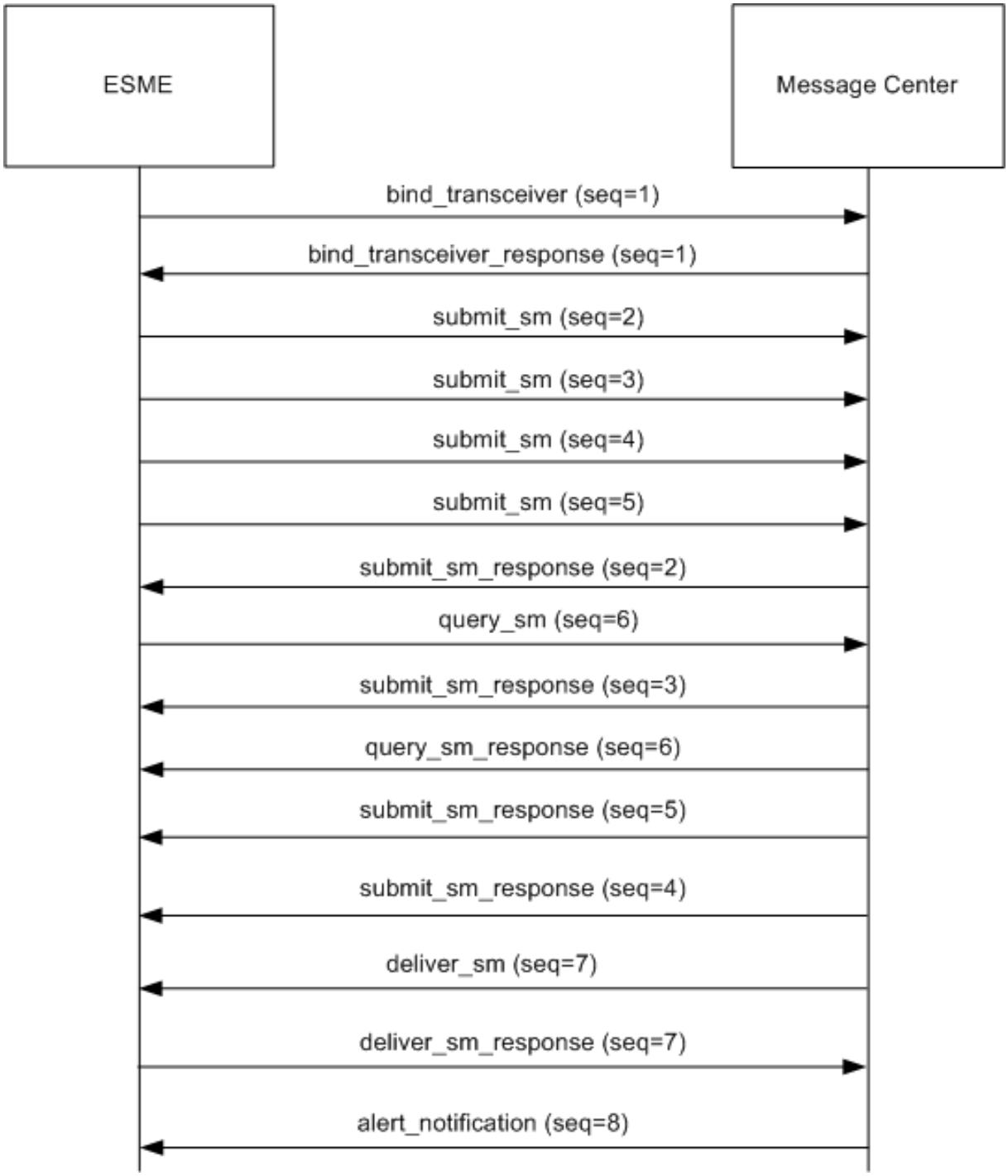
Nachdem die Verbindung hergestellt wurde, kann die ESME je nach Modus, in dem sie an den MC gebunden ist, eine submit_sm oder data_sm Nachricht senden, eine deliver_sm oder data_sm Nachricht empfangen oder diese Art von Nachrichten senden und empfangen. Die ESME kann auch Zusatznachrichten wie query_sm, replace_sm und cancel_sm senden, um den Status einer früheren Nachrichtenzustellung abzufragen, eine frühere Nachricht durch eine neue Nachricht zu ersetzen oder eine nicht zugestellte Nachricht abzubrechen.

Wenn eine Nachricht nicht zugestellt wird, weil eine ESME nicht verfügbar ist oder ein mobiler

Abonnent nicht online ist, wird die Nachricht in die Warteschlange gestellt. Später, wenn der MC erkennt, dass der mobile Teilnehmer jetzt erreichbar ist, sendet er eine alert_notification PDU über eine Empfänger- oder Transceiversitzung an die ESME und fordert die Zustellung aller Nachrichten in der Warteschlange an.

Jede Anforderung PDU hat eine eindeutige Sequenznummer. Die Antwort-PDU hat dieselbe Sequenznummer wie die ursprüngliche Anforderung. Da der Nachrichtenaustausch über SMPP im asynchronen Modus sein kann, kann ein ESME oder ein MC mehrere Anforderungen gleichzeitig senden. Die Sequenznummer spielt eine entscheidende Rolle bei der Rückgabe der Antwort in derselben SMPP-Sitzung. Mit anderen Worten, die Sequenznummer macht Anforderungs- und Antwortabgleich möglich.

Das folgende Diagramm zeigt, wie der Verkehrsfluss die verschiedenen PDUs verwendet, wenn der ESME als Transceiver bindet.



Einschränkung:

Die Citrix ADC Appliance unterstützt keine ausgehenden Vorgänge. Das heißt, ein Nachrichtencenter kann keine SMPP-Sitzung mit einer ESME über die Citrix ADC Appliance initiieren.

Funktionsweise des SMPP-Lastenausgleichs auf dem Citrix ADC

Ein ESME (Client) sendet eine Bindungsnachricht, um eine Verbindung zum Citrix ADC zu öffnen. Der ADC authentifiziert jeden ESME und antwortet, wenn er erfolgreich ist, mit einer entsprechenden Nachricht. Das Citrix ADC stellt eine Verbindung zu jedem Nachrichtencenter her und gleicht alle Nachrichten zwischen diesen Nachrichtencentern aus. Wenn der ADC eine Nachricht von einem Client empfängt, verwendet er eine offene Verbindung zum Nachrichtencenter oder sendet eine Bindungsanforderung an ein Nachrichtencenter, wenn keine offene Verbindung verfügbar ist.

Der ADC kann Lastenausgleich Nachrichten, die von den Clients und von den Servern stammen. Es kann den Zustand der Nachrichtencenter überwachen und verkettete Nachrichten verarbeiten. Es bietet auch Unterstützung für Content Switching für die Message Center.

Nachrichten, die von den ESMEs stammen

Jeder ESME muss als Benutzer auf dem Citrix ADC zur Authentifizierung hinzugefügt werden. Der Client stellt eine TCP-Verbindung mit einem virtuellen SMPP-Server her, der auf dem ADC konfiguriert ist, indem er eine Bindungsanforderung sendet. Der ADC authentifiziert den Client und analysiert, falls erfolgreich, die Bindungsnachricht. Der ADC sendet die Anforderung dann an das Nachrichtencenter, das von der konfigurierten Lastausgleichsmethode ausgewählt wurde. Wenn eine Verbindung zum Nachrichtencenter nicht zur Wiederverwendung verfügbar ist, öffnet der ADC eine TCP-Verbindung mit dem Nachrichtencenter, indem er eine neue Bindungsanforderung an das Nachrichtencenter sendet.

Bevor die Antwort (submit_sm_resp oder data_sm_resp) vom Nachrichtencenter an den Client weitergeleitet wird, fügt der ADC der Nachrichten-ID eine benutzerdefinierte Server-ID hinzu, um das Nachrichtencenter für Nebenvorgänge zu identifizieren, z. B. Abfragen, Ersetzen oder Abbrechen von Anforderungen für eine Nachricht durch den Client. Anfragen von anderen Clients werden auf die gleiche Weise Lastausgleich.

In der ursprünglichen Bindungsanforderung gibt ein Client den Adressbereich an, den er bedienen kann. Dieser Bereich wird verwendet, um deliver_sm oder data_sm Nachrichten von den Nachrichtencentern an die Clients weiterzuleiten.

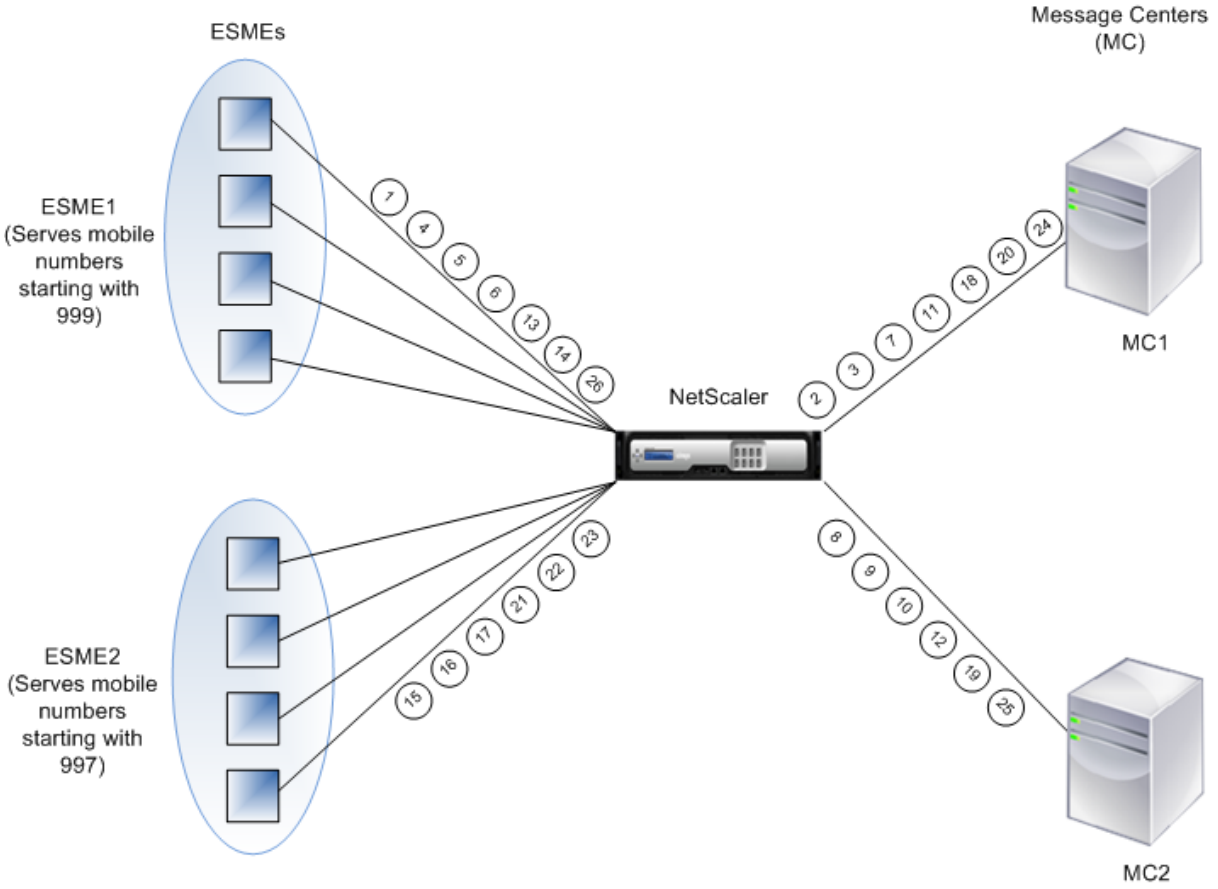
Nachrichten, die aus einem Nachrichtencenter stammen

ESMEs, die einen bestimmten Adressbereich verarbeiten können, werden in einem Cluster gruppiert. Alle Knoten in einem Cluster verfügen über die gleichen Anmeldeinformationen. Innerhalb eines Clusters wird nur die Roundrobin-Methode für den Lastenausgleich verwendet. Zum Übermitteln mobiler Nachrichten (MO-Nachrichten) sendet das Nachrichtencenter eine deliver_sm-Nachricht an den Citrix ADC. Wenn ein Cluster, der den Zieladressbereich bedienen kann (z. B. Zahlen, die mit 998 beginnen),

an den ADC gebunden ist, wählt er diesen Cluster aus und gleicht dann die Nachricht zwischen den ESME-Knoten in diesem Cluster aus.

Wenn eine ESME, die deliver_sm-Nachrichten für den Adressbereich bereitstellen kann, nicht an den ADC gebunden ist und die Nachrichtenwarteschlange aktiviert ist, wird die Nachricht in die Warteschlange gestellt, bis ein solcher Client in einem Empfänger- oder Transceiver-Modus an den ADC bindet. Sie können die Größe der Warteschlange angeben.

Das folgende Diagramm veranschaulicht den internen Fluss von PDUs zwischen ESMEs, Citrix ADC und den Nachrichtencentern. Der Einfachheit halber werden nur zwei ESMEs und zwei Message Center angezeigt.



Nachrichtenfluss (PDUs):

1. ESME1 sendet Bindungsanforderung an NetScaler
2. NetScaler sendet Bindungsanforderung an MC1
3. MC1 sendet Bindungsantwort an NetScaler
4. NetScaler sendet Bind-Antwort an ESME1
5. ESME1 sendet submit_sm (1) an NetScaler
6. ESME1 sendet submit_sm (2) an NetScaler
7. NetScaler leitet submit_sm (1) an MC1 weiter

8. NetScaler sendet Bindungsanforderung an MC2
9. MC2 sendet Bind-Antwort an NetScaler
10. NetScaler leitet submit_sm (2) an MC2 weiter
11. MC1 sendet submit_sm_resp (1) an NetScaler
12. MC2 sendet submit_sm_resp (2) an NetScaler
13. NetScaler leitet submit_sm_resp (1) an ESME1 weiter
14. NetScaler leitet submit_sm_resp (2) an ESME1 weiter
15. ESME2 sendet Bindungsanforderung an NetScaler
16. NetScaler sendet Bind-Antwort an ESME2
17. ESME2 sendet submit_sm (3) an NetScaler
18. NetScaler leitet submit_sm (3) an MC1 weiter
19. MC2 sendet deliver_sm an NetScaler (ESME2 dient dem in der Nachricht angegebenen Adressbereich)
20. MC1 sendet submit_sm_resp (3) an NetScaler
21. NetScaler leitet submit_sm_resp (3) an ESME2 weiter
22. NetScaler leitet deliver_sm an ESME2 weiter
23. ESME2 sendet deliver_sm_resp an NetScaler
24. MC1 sendet alert_notification an NetScaler (ESME1 dient dem in der Nachricht angegebenen Adressbereich)
25. NetScaler leitet deliver_sm_resp an MC2 weiter
26. NetScaler leitet die alert_notification an ESME1 weiter

Zustandsüberwachung von Message Centern

Standardmäßig ist ein TCP_Default-Monitor an einen SMPP-Dienst gebunden, Sie können jedoch einen benutzerdefinierten Monitor vom Typ SMPP binden. Der benutzerdefinierte Monitor öffnet eine TCP-Verbindung zum Nachrichtencenter und sendet ein enquire_link-Paket. Je nach Erfolg oder Ausfall des Prüfpunkts wird der Dienst als UP oder DOWN gekennzeichnet.

Content Switching auf Message Centern

Message Center können mehrere Verbindungen von ESMEs akzeptieren (oder Anfragen binden). Sie können den Citrix ADC so konfigurieren, dass diese Anforderungen basierend auf den SMPP-Bind-Parametern mit Inhalt wechselt. Im Folgenden finden Sie einige allgemeine Ausdrücke zum Konfigurieren von Methoden zum Auswählen eines Nachrichtenzentrums:

- Basierend auf dem Adressbereich: Im folgenden Beispielausdruck wählt der ADC ein bestimmtes Nachrichtencenter aus, wenn der Adressbereich bei 988 beginnt.

Beispiel:

SMPP.BINDINFO.ADDRESS_RANGE.CONTAINS(“^988”)

- Basierend auf der ESME-ID: Im folgenden Beispielausdruck wählt der ADC ein bestimmtes Nachrichtencenter aus, wenn die ESME-ID ESME1 entspricht.

Beispiel:

SMPP.BINDINFO.SYSTEM_ID.EQ(“ESME1”)

- Basierend auf dem ESME-Typ: Im folgenden Beispielausdruck wählt der ADC ein bestimmtes Nachrichtencenter aus, wenn der ESME-Typ VMS ist. VMS steht für Voicemail-System.

Beispiel:

SMPP.BINDINFO.SYSTEM_TYPE.EQ(“VMS”)

- Basierend auf dem Zahlentyp (TON) der ESME: Im folgenden Beispielausdruck wählt der ADC ein bestimmtes Nachrichtencenter aus, wenn TON gleich 1 ist (1 steht für eine internationale Nummer).

Beispiel:

SMPP.BINDINFO.ADDR_TON.EQ(1)

- Basierend auf dem Nummernplanindikator (NPI) der ESME: Im folgenden Beispielausdruck wählt der ADC ein bestimmtes Nachrichtencenter aus, wenn NPI gleich 0 ist (0 steht für eine unbekannte Verbindung.)

Beispiel:

SMPP.BINDINFO.ADDR_NPI.EQ(0)

- Basierend auf dem Bindungstyp: Im folgenden Beispielausdruck wählt der ADC ein bestimmtes Nachrichtencenter aus, wenn der Bindungstyp TRANSCEIVER lautet. (Ein Transceiver kann Nachrichten senden und empfangen.)

Beispiel:

SMPP.BINDINFO.TYPE.EQ(TRANSCEIVER)

Verkettete Nachrichtenverarbeitung

Eine SMS kann maximal 140 Bytes enthalten. Längere Nachrichten müssen in kleinere Teile aufgeteilt werden. Wenn das Zielmobilgerät in der Lage ist, werden die Nachrichten kombiniert und als eine lange SMS zugestellt. Citrix ADC leitet die Fragmente einer Nachricht an dasselbe Nachrichtencenter weiter. Jede Nachricht enthält eine Referenznummer, eine Sequenznummer und die Gesamtzahl der Fragmente. Die Referenznummer ist für jedes Fragment einer langen Nachricht gleich. Die Sequenznummer gibt die Position des bestimmten Fragments in der vollständigen Nachricht an. Nachdem alle Fragmente empfangen wurden, kombiniert die ESME die Fragmente zu einer langen Nachricht und übermittelt die Nachricht an den mobilen Abonnenten.

Wenn ein Client von einer aktiven Verbindung getrennt wird, wird die Verbindung zum Nachrichtencenter nicht geschlossen. Es wird für Anfragen von anderen Clients wiederverwendet.

Einschränkung

Message-IDs, die länger als 59 Bytes sind, werden nicht unterstützt. Wenn die vom Nachrichtencenter zurückgegebene Nachrichtenkennung mehr als 59 Byte beträgt, schlagen Nebenvorgänge fehl, und der Citrix ADC antwortet mit einer Fehlermeldung.

Konfigurieren des SMPP-Lastenausgleichs auf dem Citrix ADC

Führen Sie die folgenden Aufgaben aus, um den SMPP-Lastenausgleich auf dem ADC zu konfigurieren:

1. Fügen Sie einen SMPP-Benutzer hinzu. Der ADC authentifiziert den Benutzer, bevor er eine Bind-Anforderung des Benutzers akzeptiert. Der Benutzer ist in der Regel ein ESME.
2. Fügen Sie einen virtuellen Lastausgleichsserver hinzu, wobei das Protokoll als SMPP angegeben wird.
3. Fügen Sie einen Dienst hinzu, der das Protokoll als SMPP angibt, und eine benutzerdefinierte Server-ID, die für jeden Server eindeutig ist. Binden Sie den Dienst an den zuvor erstellten virtuellen Lastenausgleichsserver.
4. Erstellen Sie optional eine Dienstgruppe, und fügen Sie der Dienstgruppe Dienste hinzu.
5. Fügen Sie optional einen Monitor vom Typ SMPP-ECV hinzu und binden Sie ihn an den Dienst. Ein TCP-Standardmonitor ist standardmäßig gebunden.
6. Legen Sie die SMPP-Parameter fest, z. B. den Clientmodus und die Nachrichtenwarteschlange.

So konfigurieren Sie den SMPP-Lastenausgleich mithilfe der Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add smpp user <username> -password <password>
add service <name> <IP> SMPP <port>  - customserverID <customserverID>
add lb vserver <name> <IP> SMPP <port>
bind lb vserver <name> <service name>
set smpp param
<!--NeedCopy-->
```

Beispiel


```
add smpp user smppclient1 -password c03ebb540695b6110eb31172f32245a1 -encrypted -encryptmethod ENCMTHD_2
add smpp user smppclient2 -password c03ebb540695b6110eb31172f32245a1 -encrypted -encryptmethod ENCMTHD_2
add service smmpsvc 10.102.84.140 SMPP 2775 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -svrTimeout 360 -CustomServerID ab -CKA NO -TCPB NO -CMP NO
add service smmpsvc2 10.102.81.175 SMPP 2775 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -svrTimeout 360 -CustomServerID xy -CKA NO -TCPB NO -CMP NO
add lb vserver smppvs SMPP 10.102.239.179 2775 -persistenceType NONE -cltTimeout 180
bind lb vserver smppvs smmpsvc2
bind lb vserver smppvs smmpsvc
set smpp param -addrrange "d*"
<!--NeedCopy-->
```

So konfigurieren Sie den SMPP-Lastenausgleich mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **System > Benutzerverwaltung > SMPP-Benutzer**, und fügen Sie einen SMPP-Benutzer hinzu.
2. Navigieren Sie zu **Traffic Management > Load Balancing > SMPP-Parameter konfigurieren**, und legen Sie die für Ihre Bereitstellung erforderlichen Parameter fest.
3. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und fügen Sie einen virtuellen Server vom Typ SMPP hinzu.
4. Klicken Sie im Abschnitt Dienst, fügen Sie einen Dienst vom Typ SMPP hinzu, und geben Sie eine Server-ID an.

Anwendungsfall 2: Konfigurieren der regelbasierten Persistenz basierend auf einem Name-Wert-Paar in einem TCP-Byte-Stream

October 5, 2021

Einige Protokolle übertragen Name-Wert-Paare in einem TCP-Byte-Stream. Das Protokoll im TCP-Bytestream in diesem Beispiel ist das FIX-Protokoll (Financial Information eXchange). In der Nicht-XML-Implementierung ermöglicht das FIX-Protokoll zwei Hosts, die über ein Netzwerk kommunizieren, geschäftliche oder handelsbezogene Informationen als Liste von Name-Wert-Paaren (genannt "FIX-Felder") auszutauschen. Das Feldformat ist<tag>=<value><delimiter>. Dieses traditionelle Tag-Wert-Format macht das FIX-Protokoll ideal für den Anwendungsfall.

Das Tag in einem FIX-Feld ist ein numerischer Bezeichner, der die Bedeutung des Feldes angibt. Im Beispiel;

- Das Tag 35 gibt den Nachrichtentyp an.
- Der Wert nach dem Gleichheitszeichen hat eine bestimmte Bedeutung für das angegebene Tag und ist einem Datentyp zugeordnet. Der Wert A für das Tag 35 gibt an, dass es sich bei der Nachricht um eine Anmeldenachricht handelt.
- Das Trennzeichen ist das nicht druckende Start of Header (SOH) ASCII-Zeichen (0x01), welches das Caret-Symbol (^) ist.
- Jedem Feld wird außerdem ein Name zugewiesen. Das Feld mit Tag 35 ist das MsgType-Feld.

Es folgt ein Beispiel für eine Anmeldemeldung.

8=FIX.4.1 9=61 35=A 49=INVMGR 56=BRKR 34=1 52=20000426- 12:05:06 98=0 108=30 10=157

Ihre Wahl des Persistenztyps für eine Tag-Werteliste wie die oben dargestellte wird durch die Optionen bestimmt, die Ihnen zur Verfügung stehen, um eine bestimmte Zeichenfolge aus der Liste zu extrahieren. Token-basierte Persistenzmethoden erfordern, dass Sie den Offset und die Länge des Tokens angeben, das Sie aus der Nutzlast extrahieren möchten. Das FIX-Protokoll erlaubt dies nicht, da der Offset eines bestimmten Feldes und die Länge seines Wertes von Nachricht zu Nachricht variieren können. Diese Variation hängt vom Nachrichtentyp, den vorhergehenden Feldern und den Längen der vorhergehenden Werte ab. Es variiert auch je nach Implementierung von einer zur anderen, je nachdem, ob benutzerdefinierte Felder definiert wurden. Solche Variationen machen es unmöglich, den exakten Versatz eines bestimmten Feldes vorherzusagen oder die Länge des Wertes anzugeben, der als Token extrahiert werden soll. In diesem Fall ist die regelbasierte Persistenz der bevorzugte Persistenztyp.

Angenommen, ein virtueller Server fixlb1 ermöglicht den Lastenausgleich TCP-Verbindungen zu einer Farm von Servern, die Instanzen einer Fix-fähigen Anwendung hosten. Sie möchten die Persistenz für Verbindungen auf der Grundlage des Wertes des SenderCompid-Feldes konfigurieren, in dem das Unternehmen identifiziert wird, das die Nachricht sendet. Das Tag für dieses FIX-Feld ist 49 (im Beispiel der früheren Anmeldemeldung angezeigt).

Um die regelbasierte Persistenz für den virtuellen Lastausgleichsserver zu konfigurieren, legen Sie den Persistenztyp für den virtuellen Lastausgleichsserver auf RULE fest, und konfigurieren Sie den Regelparameter mit einem Ausdruck. Der Ausdruck muss ein Ausdruck sein, der den Teil der TCP-Nutzlast extrahiert, in dem Sie das Feld SenderCompid finden möchten, die resultierende Zeichenfolge in eine Name-Wert-Liste basierend auf den Trennzeichen eingeben und dann den Wert des Feldes SenderCompid (Tag 49) extrahiert:

```
set lb vserver fixlb1 -persistenceType RULE -rule "CLIENT.TCP.PAYLOAD(300).
TYPECAST_NVLIST_T('=','^').VALUE("\49\")"
```

Hinweis: Backslash Zeichen wurden im Ausdruck verwendet, da es sich um einen CLI-Befehl handelt. Wenn Sie das Konfigurationsprogramm verwenden, geben Sie die umgekehrten Schrägstriche nicht

ein.

Wenn der Client eine FIX-Nachricht sendet, die die Name-Wert-Liste im Beispiel einer früheren Anmeldemeldung enthält, extrahiert der Ausdruck den Wert INVMGR, und die Citrix ADC Appliance erstellt eine Persistenzsitzung basierend auf diesem Wert.

Das Argument für die Funktion PAYLOAD () kann so groß sein, wie Sie es für notwendig halten, um das Feld SenderCompid in die von der Funktion extrahierte Zeichenfolge aufzunehmen. Optional können Sie die Funktion SET_TEXT_MODE (IGNORECASE) verwenden, wenn die Appliance den Fall ignoriert, wenn Sie den Wert des Felds extrahieren, und die HASH-Funktion zum Erstellen einer Persistenzsitzung basierend auf einem Hash des extrahierten Wertes. Der folgende Ausdruck verwendet die Funktionen SET_TEXT_MODE (IGNORECASE) und HASH:

```
CLIENT.TCP.PAYLOAD(500).TYPECAST_NVLIST_T('=','^').SET_TEXT_MODE(IGNORECASE
).VALUE(”49”).HASH
```

Im Folgenden finden Sie weitere Beispiele für Regeln, die Sie zum Konfigurieren der Persistenz für FIX-Verbindungen verwenden können (<tag> ersetzen Sie durch das Tag des Feldes, dessen Wert Sie extrahieren möchten):

- Um den Wert eines beliebigen FIX-Felds in den ersten 300 Bytes der TCP-Nutzlast zu extrahieren, können Sie den Ausdruck CLIENT.TCP.PAYLOAD (300) .BEFORE_STR (^) .AFTER_STR (<tag>=) verwenden.
- Um eine Zeichenfolgen zu extrahieren, die 20 Byte lang ist und einen Offset von 80 hat, wandeln Sie die Zeichenfolge in eine name-value List um und extrahieren dann den Wert des gewünschten Felds. Verwenden Sie den Ausdruck CLIENT.TCP.PAYLOAD(100).SUBSTR(80,20).TYPECAST_NVLIST_T(“
  tag>”).
- Verwenden Sie den Ausdruck CLIENT.TCP.PAYLOAD (100) .TYPECAST_NVLIST_T (‘=’, ‘^’) .VALUE (<tag>,2), um die ersten 100 Bytes der TCP-Nutzlast zu extrahieren.
  Hinweis: Wenn das zweite Argument, das an die Funktion
  VALUE () übergeben wird,
  n ist, extrahiert die Appliance den Wert der
  (n+1)
  th Instanz des Feldes, da die Anzahl bei Null beginnt (
  0).

Im Folgenden finden Sie weitere Beispiele für Regeln, die Sie zum Konfigurieren der Persistenz verwenden können. Nur die nutzlastbasierten Ausdrücke können Daten auswerten, die über das FIX-Protokoll übertragen werden. Die anderen Ausdrücke sind allgemeinere Ausdrücke für die Konfiguration der Persistenz basierend auf niedrigeren Netzwerkprotokollen.

- CLIENT.TCP.PAYLOAD (100)
- CLIENT.TCP.PAYLOAD (100) .HASH
- CLIENT.TCP.PAYLOAD (100) .SUBSTR (5,10)

- CLIENT.TCP.SRCPORT
- CLIENT.TCP.DSTPORT
- CLIENT.IP.SRC
- CLIENT.IP.DST
- CLIENT.IP.SRC.GET4
- CLIENT.IP.DST.GET4
- CLIENT.ETHER.SRCMAC.GET6
- CLIENT.ETHER.DSTMAC.GET5
- CLIENT.VLAN.ID

Anwendungsfall 3: Konfigurieren des Lastausgleichs im Direktserverrückgabemodus

October 5, 2021

Der Lastenausgleich im DSR-Modus (Direct Server Return) ermöglicht es dem Server, direkt auf Clients zu reagieren, indem er einen Rückgabepfad verwendet, der nicht über die Citrix ADC Appliance fließt. Im DSR-Modus kann die Appliance jedoch weiterhin Integritätsprüfungen für Dienste durchführen. In einer Umgebung mit hohem Datenvolumen erhöht das direkte Senden von Serverdatenverkehr an den Client im DSR-Modus die gesamte Paketverarbeitungskapazität der Appliance, da die Pakete nicht durch die Appliance fließen.

DSR-Modus hat die folgenden Funktionen und Einschränkungen:

- Es unterstützt Einarm-Modus und Inline-Modus.
- Die Appliance altert Sitzungen basierend auf dem Leerlaufzeitlimit aus.
- Da die Appliance keine TCP-Verbindungen proxyiert (dh sie sendet SYN-ACK nicht an den Client), schließt sie SYN-Angriffe nicht aus. Mit dem SYN-Paketratenfilter können Sie die Rate von SYNs für den Server steuern. Um die Rate von SYNs zu steuern, legen Sie einen Schwellenwert für die Rate von SYNs fest. Um Schutz vor SYN-Angriffen zu erhalten, müssen Sie die Appliance so konfigurieren, dass für TCP-Verbindungen ein Proxy verwendet wird. Dies erfordert jedoch, dass der umgekehrte Datenverkehr durch die Appliance fließt.
- In einer DSR-Konfiguration ersetzt die Citrix ADC Appliance die IP-Adresse des virtuellen Lastenausgleichs nicht durch die IP-Adresse des Zielservers. Stattdessen leitet er Pakete an einen Dienst weiter, indem er die MAC-Adresse des Servers verwendet. Der VIP muss auf dem Server konfiguriert sein und ARP muss für den VIP deaktiviert sein, der auf dem Server konfiguriert ist. Dadurch wird verhindert, dass die Clientanforderung die Appliance umgeht, wenn sie im Einarmmodus konfiguriert ist. Beispielsweise muss ein Benutzer VIP in der Loopback-Schnittstelle konfigurieren und den ARP für denselben VIP deaktivieren.

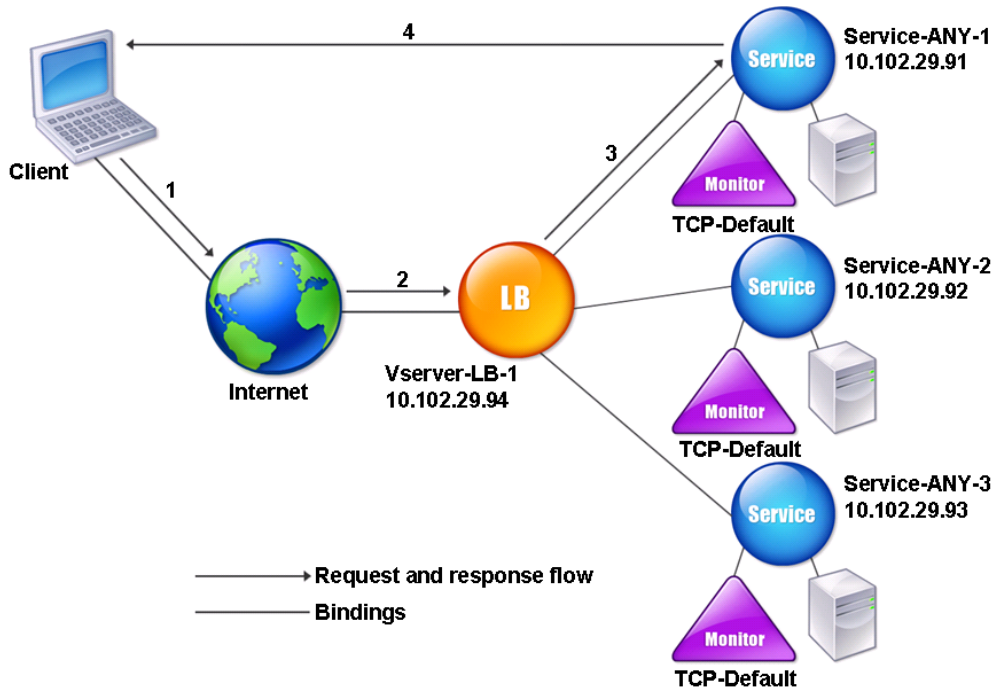
- Die Appliance ruft die MAC-Adresse des Servers vom Monitor ab, der an den Dienst gebunden ist. Benutzermonitore (Monitore vom Typ USER), die Skripts verwenden, die auf der Citrix ADC Appliance gespeichert sind, kennen jedoch nicht die MAC-Adresse eines Servers. Wenn Sie nur benutzerdefinierte Monitore in einer DSR-Konfiguration verwenden, versucht die Appliance für jede Anforderung, die der virtuelle Server empfängt, die Ziel-IP-Adresse in eine MAC-Adresse aufzulösen (indem Sie ARP-Anforderungen senden). Da es sich bei der Ziel-IP-Adresse um eine virtuelle IP-Adresse handelt, die der Citrix ADC Appliance gehört, werden die ARP-Anforderungen immer in die MAC-Adresse der Citrix ADC-Schnittstelle aufgelöst. Daher wird der gesamte vom virtuellen Server empfangene Datenverkehr auf die Appliance zurückgeführt. Wenn Sie Benutzermonitore in einer DSR-Konfiguration verwenden, müssen Sie auch einen anderen Monitor (z. B. einen PING-Monitor) für die Dienste konfigurieren, idealerweise mit einem längeren Intervall zwischen den Prüfpunkten, damit die MAC-Adresse der Server erlernt werden kann.
- Die Citrix ADC Appliance lernt die Server-L2-Parameter vom Monitor, der an den Dienst gebunden ist. Konfigurieren Sie für UDP-ECV-Monitore eine Empfangszeichenfolge, damit die Appliance die L2-Parameter des Servers erlernen kann. Wenn die Empfangszeichenfolge nicht konfiguriert ist und der Server nicht antwortet, lernt die Appliance die L2-Parameter nicht, aber der Dienst ist auf UP festgelegt. Der Verkehr für diesen Dienst wird in ein schwarzes Loch gestellt.

Im Beispielszenario werden die Dienste Service-ANY-1, Service-ANY-2 und Service-ANY-3 erstellt und an den virtuellen Server Vserver-LB-1 gebunden. Der virtuelle Server gleicht die Clientanforderung an einen Dienst aus, und der Dienst reagiert direkt auf Clients und umgeht die Citrix ADC Appliance. In der folgenden Tabelle sind die Namen und Werte der Entitäten aufgeführt, die auf der Citrix ADC Appliance im DSR-Modus konfiguriert sind.

Entitätstyp	Name	IP-Adresse	Protokoll
Virtueller Server	Vserver-LB-1	10.102.29.94	ANY
Services	Service-ANY-1	10.102.29.91	ANY
	Service-ANY-2	10.102.29.92	ANY
	Service-ANY-3	10.102.29.93	ANY
Monitore	TCP	Ohne	Ohne

Das folgende Diagramm zeigt die Lastausgleichseinheiten und die Werte der Parameter, die auf der Appliance konfiguriert werden sollen.

Abbildung 1. Entitätsmodell für Lastenausgleich im DSR-Modell



Damit die Appliance im DSR-Modus ordnungsgemäß funktioniert, muss die Ziel-IP in der Clientanforderung unverändert sein. Stattdessen ändert die Appliance den Ziel-MAC in den des ausgewählten Servers. Diese Einstellung ermöglicht es dem Server, die Client-MAC-Adresse für die Weiterleitung von Anforderungen an den Client unter Umgehung des Servers zu bestimmen.

Als Nächstes konfigurieren Sie ein grundlegendes Lastenausgleichs-Setup wie unter Einrichten des Basic Load Balancingbeschrieben, benennen die Entitäten und Festlegen der Parameter mit den in der vorherigen Tabelle beschriebenen Werten.

Nachdem Sie das grundlegende Lastausgleichs-Setup konfiguriert haben, müssen Sie es für den DSR-Modus anpassen. Zu diesem Zweck konfigurieren Sie eine unterstützte Lastausgleichsmethode, z. B. die Quell-IP-Hash-Methode mit einem virtuellen Server ohne Sitzungsvorgang. Sie müssen auch den Umleitungsmodus festlegen, damit der Server die Client-MAC-Adresse für die Weiterleitung von Antworten ermitteln und die Appliance umgehen kann.

Nachdem Sie die Load Balancing-Methode und den Umleitungsmodus konfiguriert haben, müssen Sie den USIP-Modus für jeden Dienst aktivieren. Der Dienst verwendet dann die Quell-IP-Adresse, wenn Antworten weitergeleitet werden.

So konfigurieren Sie die Load Balancing-Methode und den Umleitungsmodus für einen virtuellen Server ohne Sitzungsfunktion mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <vServerName> -lbMethod <LBMethodOption> -m <
   RedirectionMode> -sessionless <Value>
<!--NeedCopy-->
```

Beispiel

```
set lb vserver Vserver-LB-1 -lbMethod SourceIPHash -m MAC -sessionless
   enabled
<!--NeedCopy-->
```

> **Hinweis:**
>
> Für einen Dienst, der an einen virtuellen Server gebunden ist, auf dem die Option -m MAC aktiviert ist, müssen Sie einen Nicht-Benutzermonitor binden.

So konfigurieren Sie die Load Balancing-Methode und den Umleitungsmodus für einen virtuellen Server ohne Sitzungsfunktion mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen Server, wählen Sie Umleitungsmodus als MAC-basiert und Methode als SOURCEIPHASH.
3. Wählen Sie unter Verkehrseinstellungen die Option Sitzungsloser Lastenausgleich aus.

So konfigurieren Sie einen Dienst für die Verwendung der Quell-IP-Adresse mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <ServiceName> -usip <Value>
<!--NeedCopy-->
```

Beispiel:


```
set service Service-ANY-1 -usip yes
<!--NeedCopy-->
```

So konfigurieren Sie einen Dienst für die Verwendung der Quell-IP-Adresse mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Öffnen Sie einen Dienst und wählen Sie unter Verkehrseinstellungen die Option **Quell-IP-Adresse verwenden**aus.

Einige zusätzliche Schritte sind in bestimmten Situationen erforderlich, die in den nachfolgenden Abschnitten beschrieben werden.

Anwendungsfall 4: Konfigurieren von LINUX-Servern im DSR-Modus

October 5, 2021

Das LINUX-Betriebssystem erfordert, dass Sie auf jedem Lastausgleichsserver im DSR-Cluster eine Loopback-Schnittstelle mit der virtuellen IP-Adresse (VIP) der Citrix ADC Appliance einrichten.

So konfigurieren Sie den LINUX-Server im DSR-Modus

Um eine Rücklaufschnittstelle mit dem VIP der Citrix ADC Appliance auf jedem Server mit Lastausgleich zu erstellen, geben Sie an der Eingabeaufforderung des Linux-Betriebssystems die folgenden Befehle ein:

```
ifconfig dummy0 up

ifconfig dummy0:0 inet <netscaler vip> netmask 255.255.255.255 up

echo 1 > /proc/sys/net/ipv4/conf/dummy0/arp_ignore

echo 2 > /proc/sys/net/ipv4/conf/dummy0/arp_announce
<!--NeedCopy-->
```

Führen Sie dann die Software aus, die die TOS-ID neu zu VIP zuordnet.

Hinweis: Fügen Sie der Software die richtigen Zuordnungen hinzu, bevor Sie sie ausführen. In den vorhergehenden Befehlen verwendet der LINUX-Server dummy0, um eine Verbindung mit dem Net-

zwerk herzustellen. Wenn Sie diesen Befehl verwenden, geben Sie den Namen der Schnittstelle ein, die Ihr LINUX-Server für die Verbindung mit dem Netzwerk verwendet.

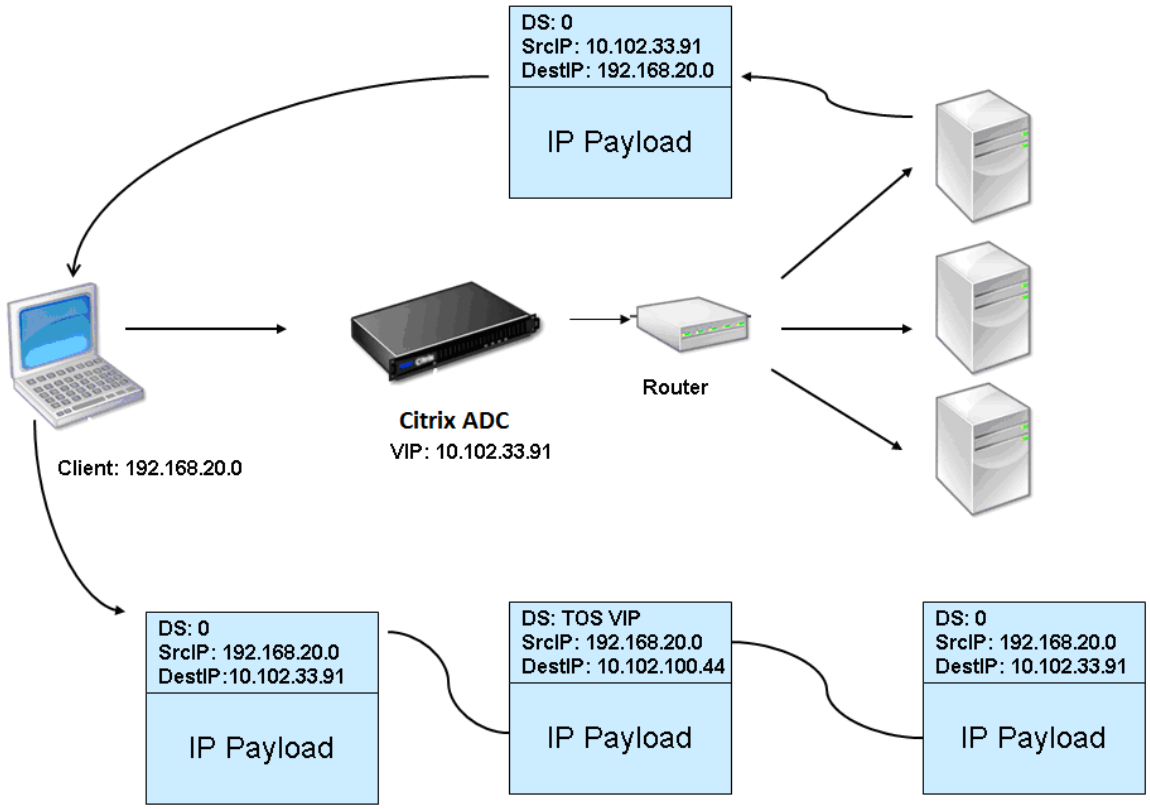
Anwendungsfall 5: Konfigurieren des DSR-Modus bei Verwendung von TOS

October 5, 2021

Differentiated Services (DS), auch TOS (Type of Service) genannt, ist ein Feld, das Teil des IPv4-Paket-Headers ist. Das entsprechende Feld im IPv6-Header ist Traffic Class. TOS wird von Protokollen der oberen Schicht verwendet, um den Pfad für ein Paket zu optimieren. Die TOS-Informationen kodieren die virtuelle IP-Adresse (VIP) der Citrix ADC Appliance, und die Server mit Lastausgleich extrahieren den VIP.

Im folgenden Szenario fügt die Appliance den VIP dem **TOS-Feld** im Paket hinzu und leitet das Paket dann an den Lastausgleichsserver weiter. Der Lastausgleichsserver reagiert dann direkt auf den Client und umgeht die Appliance, wie im folgenden Diagramm dargestellt.

Abbildung 1. Die Citrix ADC Appliance im DSR-Modus mit TOS



Die TOS-Funktion ist wie folgt für eine kontrollierte Umgebung angepasst:

- Die Umgebung darf keine statusbehafteten Geräte wie Stateful-Firewall und TCP-Gateways im Pfad zwischen der Appliance und den Lastausgleichs-Servern aufweisen.
- Router an allen Einstiegspunkten zum Netzwerk müssen das TOS-Feld aus allen eingehenden Paketen entfernen, um sicherzustellen, dass der Server mit Lastausgleich kein anderes TOS-Feld mit dem von der Appliance hinzugefügten Feld verwechselt.
- Jeder Server kann nur 63 VIPs haben.
- Der Zwischenrouter darf keine ICMP-Fehlermeldungen bezüglich Fragmentierung senden. Der Client versteht die Meldung nicht, da die Quell-IP-Adresse die IP-Adresse des Lastausgleichsservers und nicht der Citrix ADC VIP ist.
- TOS ist nur für IP-basierte Dienste gültig. Domänennamenbasierte Dienste können nicht mit TOS verwendet werden.

In diesem Beispiel wird Service-ANY-1 erstellt und an den virtuellen Server vServer-LB-1 gebunden. Der virtuelle Server gleicht die Clientanforderung an den Dienst aus, und der Dienst reagiert direkt auf Clients unter Umgehung der Appliance. In der folgenden Tabelle sind die Namen und Werte der Entitäten aufgeführt, die auf der Appliance im DSR-Modus konfiguriert sind.

Entitätstyp	Name	IP-Adresse	Protokoll
Virtueller Server	Vserver-LB-1	10.102.33.91	ANY
Services	Service-ANY-1	10.102.100.44	ANY
Monitore	PING	Ohne	Ohne

DSR mit TOS erfordert, dass der Lastenausgleich auf Schicht 3 eingerichtet ist. Informationen zum Konfigurieren eines grundlegenden Load Balancing-Setups für Layer 3 finden Sie unter Einrichten des Basic Load Balancing. Benennen Sie die Entitäten und legen Sie die Parameter anhand der in der vorherigen Tabelle beschriebenen Werte fest.

Nachdem Sie das Lastausgleichs-Setup konfiguriert haben, müssen Sie das Lastausgleichs-Setup für den DSR-Modus anpassen, indem Sie den Umleitungsmodus so konfigurieren, dass der Server das Datenpaket entkapselt und dann direkt auf den Client reagieren und die Appliance umgehen kann.

Nachdem Sie den Umleitungsmodus angegeben haben, können Sie die Appliance optional aktivieren, um den Server transparent zu überwachen. Dadurch kann die Appliance die Server mit Lastausgleich transparent überwachen.

So konfigurieren Sie den Umleitungsmodus für den virtuellen Server mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <vServerName> -m <Value> -tosId <Value>
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver Vserver-LB-1 -m TOS -tosId 3
<!--NeedCopy-->
```

So konfigurieren Sie den Umleitungsmodus für den virtuellen Server mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen Server, und wählen Sie im Umleitungsmodus TOS ID aus.

So konfigurieren Sie den transparenten Monitor für TOS mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add monitor <MonitorName> <Type> -destip <DestinationIP> -tos <Value> -
    tosId <Value>
<!--NeedCopy-->
```

Beispiel:

```
add monitor mon1 PING -destip 10.102.33.91 -tos Yes  -tosId 3
<!--NeedCopy-->
```

So erstellen Sie den transparenten Monitor für TOS mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Erstellen Sie einen Monitor, wählen Sie TOS aus, und geben Sie die TOS-ID ein, die Sie für den virtuellen Server angegeben haben.

Platzhalter-TOS-Monitore

Bei einer Lastausgleichskonfiguration im DSR-Modus mit dem TOS-Feld muss für die Überwachung der Dienste ein TOS-Monitor erstellt und an diese Dienste gebunden werden. Für jede Lastenausgleichskonfiguration im DSR-Modus unter Verwendung des TOS-Feldes ist ein separater TOS-Monitor erforderlich, da ein TOS-Monitor die VIP-Adresse und die TOS-ID benötigt, um einen kodierten Wert der VIP-Adresse zu erstellen. Der Monitor erstellt Probe-Pakete, in denen das **TOS-Feld** auf den codierten Wert der VIP-Adresse festgelegt ist. Anschließend werden die Prüfpunktpakete an die Server gesendet, die von den Diensten einer Lastausgleichskonfiguration dargestellt werden.

Bei vielen Load Balancing-Konfigurationen ist das Erstellen eines separaten benutzerdefinierten TOS-Monitors für jede Konfiguration eine wichtige, umständliche Aufgabe. Die Verwaltung dieser TOS-Monitore ist ebenfalls eine wichtige Aufgabe. Jetzt können Sie Platzhalter-TOS-Monitore erstellen. Erstellen Sie nur einen Platzhalter-TOS-Monitor für alle Load Balancing-Konfigurationen, die dasselbe Protokoll verwenden (z. B. TCP oder UDP).

Ein Platzhalter-TOS-Monitor verfügt über die folgenden obligatorischen Einstellungen:

- Typ = <protocol>

- TOS = Ja

Die folgenden Parameter können auf einen Wert gesetzt oder leer gelassen werden:

- Ziel-IP
- Zielport
- TOS-ID

Ein Platzhalter-TOS-Monitor (mit nicht festgelegten Ziel-IP, Ziel-Port und TOS-ID), der an einen DSR-Dienst gebunden ist, erlernt automatisch die TOS-ID und die VIP-Adresse des virtuellen Lastausgleichsservers. Der Monitor erstellt Prüfpakete mit dem TOS-Feld auf die codierte VIP-Adresse und sendet dann die Prüfpakete an den Server, der vom DSR-Dienst dargestellt wird.

So erstellen Sie einen Platzhalter-TOS-Monitor mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb monitor <monitorName> <Type> -tos YES

show lb monitor <monitorName>
<!--NeedCopy-->
```

So binden Sie einen Platzhalter-TOS-Monitor mit Hilfe der CLI an einen Dienst

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb monitor <monitorName> <serviceName>

show lb monitor <monitorName>
<!--NeedCopy-->
```

So erstellen Sie einen Platzhalter-TOS-Monitor mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Monitore**.
2. Fügen Sie einen Monitor mit den folgenden Parametereinstellungen hinzu:
   - Typ = <protocol>
   - TOS = JA

So binden Sie einen Platzhalter-TOS-Monitor mit der GUI an einen Dienst

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienste**.
2. Öffnen Sie einen Dienst und binden Sie einen Platzhalter-TOS-Monitor an ihn.

In der folgenden Beispielkonfiguration sind V1, V2 und V3 Lastenausgleichsserver vom Typ ANY und hat die TOS-ID auf 1, 2 und 3 festgelegt. S1, S2, S3, S4 und S5 sind Dienste des Typs ANY. S1 und S2 sind sowohl an V1 als auch an V2 gebunden. S3, S4 und S5 und gebunden an V1 und V3. WLCD-TOS-MON ist ein Platzhalter-TOS-Monitor mit dem Typ TCP und ist an S1, S2, S3, S4 und S5 gebunden.

WLCD-TOS-MON lernt automatisch die TOD-ID und die VIP-Adresse von virtuellen Servern, die an S1, S2, S3, S4 und S5 gebunden sind.

Da S1 an V1 und V2 gebunden ist, erstellt WLCD-TOS-MON zwei Arten von Prüfpaketen für S1, eines mit dem **TOS-Feld** auf die codierte VIP-Adresse (203.0.113.1) von V1 und das andere mit der VIP-Adresse (203.0.113.2) von V2. Der Citrix ADC sendet diese Prüfpakete dann an den durch S1 dargestellten Server. In ähnlicher Weise erstellt WLCD-TOS-MON Probe-Pakete für S2, S3, S4 und S5.

```
add lb monitor WLCD-TOS-MON  TCP -tos YES

Done

add lb vserver V1 ANY 203.0.113.1 * -m TOS  - tosID 1

Done

add lb vserver V2 ANY 203.0.113.2 * -m TOS  - tosID 2

Done

add lb vserver V3 ANY 203.0.113.3 * -m TOS  - tosID 3

Done

add service S1 198.51.100.1 ANY *

Done

add service S2 198.51.100.2 ANY *

Done

add service S3 198.51.100.3 ANY *

```



```
Done

add service S4 198.51.100.4 ANY *

Done

add service S5 198.51.100.5 ANY *

Done

bind lb monitor WLCD-TOS-MON S1

Done

bind lb monitor WLCD-TOS-MON S2

Done

bind lb monitor WLCD-TOS-MON S3

Done

bind lb monitor WLCD-TOS-MON S4

Done

bind lb monitor WLCD-TOS-MON S5

Done

bind lb vserver V1 S1, S2, S3, S4, S5

Done

bind lb vserver V2, S1, S2

Done

bind lb vserver V3 S3, S4, S5

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


Anwendungsfall 6: Konfigurieren des Lastausgleichs im DSR-Modus für IPv6-Netzwerke über das TOS-Feld

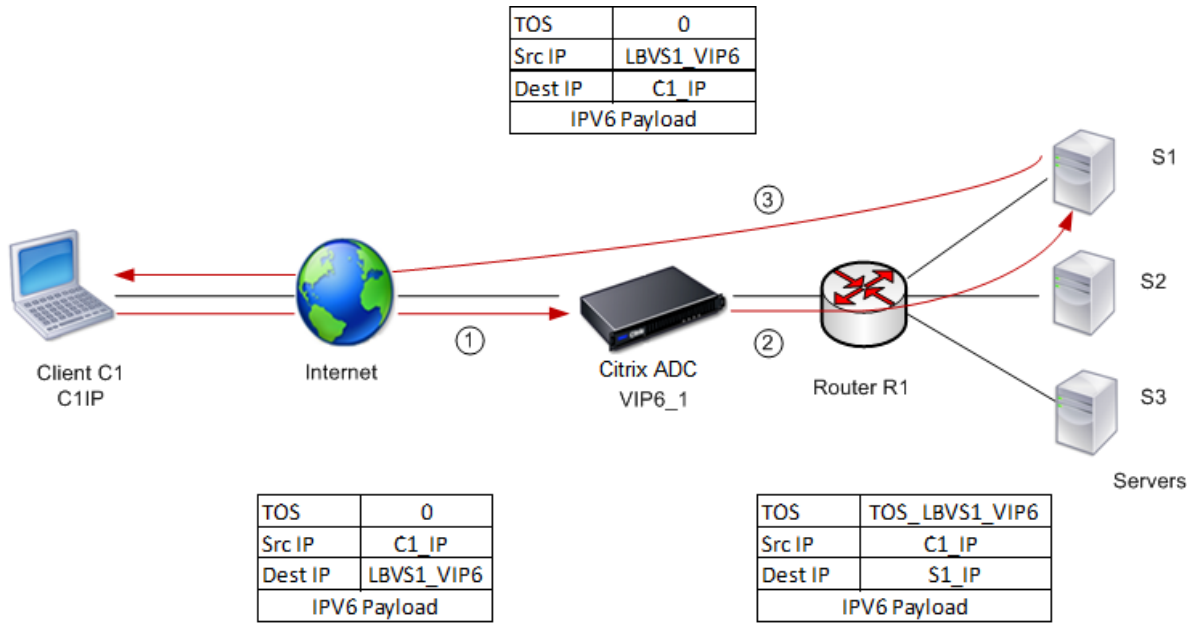
October 5, 2021

Sie können den Lastausgleich im Direct Server Return (DSR) -Modus für IPv6-Netzwerke konfigurieren, indem Sie das Feld Typ des Dienstes (TOS) verwenden, wenn sich die Citrix ADC Appliance und die Server in verschiedenen Netzwerken befinden.

Hinweis: Das TOS-Feld wird auch als Feld Traffic Class bezeichnet.

Wenn ein Client im DSR-Modus eine Anforderung an eine VIP6-Adresse auf einer Citrix ADC Appliance sendet, leitet die Appliance diese Anforderung an den Server weiter, indem sie die Ziel-IPv6-Adresse des Pakets in die IPv6-Adresse des Servers ändert und einen codierten Wert der VIP6-Adresse im TOS (auch als Verkehrsklasse bezeichnet) setzt. des IPv6-Headers. Sie können den Server so konfigurieren, dass die Informationen im Feld TOS verwendet werden, um die VIP6-Adresse aus dem codierten Wert abzuleiten, der dann als Quell-IP-Adresse in Antwortpaketen verwendet wird. Der Antwortdatenverkehr geht direkt an den Client unter Umgehung der Appliance.

Betrachten Sie ein Beispiel, in dem ein virtueller Lastausgleichsserver LBVS1, der auf einer Citrix ADC Appliance NS1 konfiguriert ist, zum Lastenausgleich zwischen den Servern S1, S2 und S3 verwendet wird. Die Citrix ADC Appliance NS1 und die Server S1, S2 und S3 befinden sich in verschiedenen Netzwerken, sodass Router R1 zwischen NS1 und den Servern bereitgestellt wird.



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt.

Entitäten	Name
IPv6-Adresse des Clients C1	C1_IP (nur zu Referenzzwecken)
Lastenausgleich virtueller Server auf NS1	LBVS1
IPv6-Adresse von LBVS1	LBVS1_VIP6 (nur für Referenzzwecke)
TOS-Wert	TOS_LBVS1_VIP6 (nur für Referenzzwecke)
Service für Server S1 auf NS1	SVC_S1
IPv6-Adresse für Server S1	S1_IP (nur für Referenzzwecke)
Service für Server S2 auf NS1	SVC_S2
IPv6-Adresse für Server S1	S2_IP (nur für Referenzzwecke)
Service für Server S3 auf NS1	SVC_S3
IPv6-Adresse für Server S1	S3_IP (nur für Referenzzwecke)

Im Folgenden ist der Verkehrsfluss im Beispielszenario:

1. Client C1 sendet eine Anforderung an den virtuellen Server LBVS1.
2. Der Lastausgleichsalgorithmus von LBVS1 wählt den Server S1 aus und die Appliance öffnet eine Verbindung zu S1. NS1 sendet die Anforderung an S1 mit:
   - TOS-Feld ist auf TOS_LBVS1_VIP6 gesetzt.
   - Quell-IP-Adresse als C1_IP.
3. Der Server S1 verwendet beim Empfang der Anforderung die Informationen im Feld TOS, um die LBVS1_VIP6-Adresse abzuleiten, d. h. die IP-Adresse des virtuellen Servers LBVS1 auf NS1. Der Server sendet die Antwort direkt an C1 unter Umgehung der Appliance mit:
   - Quell-IP-Adresse, die auf die Adresse DerivedLBVS1_VIP6 festgelegt ist, sodass der Client mit dem virtuellen Server LBVS1 auf NS1 und nicht mit dem Server S1 kommuniziert.

So konfigurieren Sie den Lastausgleich im DSR-Modus mithilfe von TOS: Führen Sie die folgenden Schritte auf der Appliance aus

1. Aktivieren Sie den USIP-Modus global.
2. Fügen Sie die Server als Dienste hinzu.
3. Konfigurieren Sie einen virtuellen Lastausgleichsserver mit einem TOS-Wert.
4. Binden Sie die Dienste an den virtuellen Server.

So konfigurieren Sie den Lastausgleich im DSR-Modus mithilfe von TOS mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns mode USIP

add service <serviceName> <IP> <serviceType> <port>
<!--NeedCopy-->
```

Wiederholen Sie den vorherigen Befehl so oft wie nötig, um jeden Server als Dienst auf der Citrix ADC Appliance hinzuzufügen.

```
add lb vserver <name> <serviceType> <ip> <port> -m <redirectionMode> -
    tosId <positive_integer>

bind lb vserver <vserverName> <serviceName>
<!--NeedCopy-->
```

So aktivieren Sie den USIP-Modus mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **System > Einstellungen > Modi konfigurieren**und wählen Sie **Quell-IP-Adresse verwenden**aus.

So erstellen Sie Dienste mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **Traffic Management > Load Balancing > Dienste**, und erstellen Sie einen Dienst.

So erstellen Sie einen virtuellen Lastausgleichsserver und binden Dienste mit dem Konfigurationsdienstprogramm

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und erstellen Sie einen virtuellen Server.
2. Klicken Sie im Abschnitt Dienst, um einen Dienst an diesen virtuellen Server zu binden.

Anwendungsfall 7: Konfigurieren des Lastausgleichs im DSR-Modus mit IP over IP

December 3, 2021

Sie können eine Citrix ADC Appliance so konfigurieren, dass sie den Direktserverrückkehrmodus (DSR) über Layer-3-Netzwerke hinweg verwendet, indem Sie IP-Tunneling verwenden, auch als *IP over IP-Konfiguration* bezeichnet. Wie bei Standard-Load Balancing-Konfigurationen für den DSR-Modus können Server direkt auf Clients reagieren, anstatt einen Rückkehrpfad über die Citrix ADC Appliance zu verwenden. Dies verbessert die Reaktionszeit und den Durchsatz. Wie im Standard-DSR-Modus überwacht die Citrix ADC Appliance die Server und führt Zustandsprüfungen an den Anwendungsports durch.

Bei der IP-over-IP-Konfiguration müssen sich die Citrix ADC Appliance und die Server nicht im selben Layer-2-Subnetz befinden. Stattdessen kapselt die Citrix ADC Appliance die Pakete, bevor sie an den Zielserver gesendet werden. Nachdem der Zielserver die Pakete empfängt, entkapselt er die Pakete und sendet dann seine Antworten direkt an den Client. Dies wird oft als L3DSR bezeichnet.

So konfigurieren Sie den L3-DSR-Modus auf Ihrer Citrix ADC Appliance:

- Erstellen Sie einen virtuellen Lastausgleichsserver. Stellen Sie den Modus auf IPTUNNEL ein und aktivieren Sie das sitzungslose Tracking.
- Erstellen Sie Dienste. Erstellen Sie für jede Back-End-Anwendung einen Dienst und binden Sie die Dienste an den virtuellen Server.
- Konfigurieren Sie für die Entkapselung. Konfigurieren Sie entweder eine Citrix ADC Appliance oder einen Back-End-Server als Entkapselungsgerät.

  > Hinweis:
  >
  > Wenn Sie eine Citrix ADC Appliance verwenden, ist das Entkapselungs-Setup ein IP-Tunnel zwischen den ADC-Appliances, wobei das Back-End L2DSR zu den realen Servern durchführt.

Konfigurieren eines virtuellen Lastausgleichsservers

Konfigurieren Sie einen virtuellen Server für die Verarbeitung von Anforderungen an Ihre Anwendungen. Weisen Sie den Diensttyp zu, der dem Dienst entspricht, oder verwenden Sie einen Typ ANY für mehrere Dienste.
Stellen Sie die Weiterleitungsmethode auf IPTUNNEL ein und ermöglichen Sie dem virtuellen Server, im sitzungslosen Modus zu arbeiten. Konfigurieren Sie jede Load Balancing-Methode, die Sie verwenden möchten.

So erstellen und konfigurieren Sie einen virtuellen Lastausgleichsserver für IP-über-IP-DSR mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um einen virtuellen Lastausgleichsserver für IP über IP-DSR zu konfigurieren und die Konfiguration zu überprüfen:

```
add lb vserver <name> serviceType <serviceType> IPAddress <ip> Port <
    port> -lbMethod <method> -m <ipTunnelTag> -sessionless [ENABLED |
    DISABLED]

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

Beispiel:

Im folgenden Beispiel haben wir die Load Balancing-Methode als SourcePhash gewählt und den sitzungslosen Lastenausgleich konfiguriert.

```
add lb vserver Vserver-LB-1 ANY 1.1.1.80 * -lbMethod SourceIPHash -m
    IPTUNNEL -sessionless ENABLED
<!--NeedCopy-->
```

So erstellen und konfigurieren Sie einen virtuellen Lastausgleichsserver für IP über IP-DSR mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Erstellen Sie einen virtuellen Server und geben Sie den Umleitungsmodus als **IP-Tunnel-basiert**an.

Konfigurieren von Diensten für IP-über-IP-DSR

Konfigurieren Sie nach dem Erstellen Ihres Servers mit Lastausgleich einen Dienst für jede Ihrer Anwendungen. Der Dienst verarbeitet den Datenverkehr von der Citrix ADC Appliance zu diesen Anwendungen und ermöglicht es der Citrix ADC-Appliance, den Zustand der einzelnen Anwendungen zu überwachen.

Weisen Sie die Dienste zu, um den USIP-Modus zu verwenden, und binden Sie einen Monitor vom Typ IPTUNNEL an den Dienst zur tunnelbasierten Überwachung.

So erstellen und konfigurieren Sie einen Dienst für IP-über-IP-DSR mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen Dienst zu erstellen, und erstellen Sie optional einen Monitor und binden Sie ihn an den Dienst:

```
add service <serviceName> <serverName> <serviceType> <port> -usip <usip
    >

add monitor <monitorName> <monitorType> -destip <ip> -iptunnel <
    iptunnel>

bind service <serviceName> -monitorName <monitorName>
<!--NeedCopy-->
```

Beispiel:

Im folgenden Beispiel wird ein Monitor vom Typ IPTUNNEL erstellt.

```
add monitor mon_DSR PING -destip 1.1.1.80 -iptunnel yes
add service svc_DSR01 2.2.2.100 ANY * -usip yes
bind service svc_DSR01 -monitorName mon_DSR
<!--NeedCopy-->
```

Ein alternativer Ansatz zur Vereinfachung des Routing sowohl auf dem Server als auch auf der ADC-Appliance besteht darin, sowohl den ADC als auch den Server so einzurichten, dass sie eine IP aus demselben Subnetz verwenden. Dadurch wird sichergestellt, dass jeder Datenverkehr mit einem Ziel eines Tunnelendpunkts über den Tunnel gesendet wird. Im Beispiel wird 10.0.1.0/30 verwendet.

> **Hinweis:**
>
> Der Zweck des Monitors besteht darin, sicherzustellen, dass der Tunnel aktiv ist, indem der Loopback jedes Servers durch den IP-Tunnel erreicht wird. Wenn der Dienst nicht verfügbar ist, überprüfen Sie, ob das äußere IP-Routing zwischen ADC und Server gut ist. Überprüfen Sie auch, ob die inneren IP-Adressen über den IP-Tunnel erreichbar sind. Auf dem Server sind möglicherweise Routen erforderlich, oder je nach gewählter Implementierung wird PBR zu ADC hinzugefügt.

Beispiel:

```
add ns ip 10.0.1.2 255.255.255.252 -vServer DISABLED
add netProfile netProfile_DSR -srcIP 10.0.1.2
```



```
3 add lb monitor mon_DSR PING -LRTM DISABLED -destIP 1.1.1.80 -ipTunnel
     YES -netProfile netProfile_DSR
4 <!--NeedCopy-->
```

So konfigurieren Sie einen Monitor mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore**.
2. Erstellen Sie einen Monitor und wählen Sie **IP-Tunnel**aus.

So erstellen und konfigurieren Sie einen Dienst für IP-über-IP-DSR mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Erstellen Sie einen Dienst und wählen Sie auf der Registerkarte **Einstellungen** die Option **Quell-IP-Adresse verwenden**aus.

So binden Sie einen Dienst mithilfe der Befehlszeilenschnittstelle an einen virtuellen Lastausgleichsserver

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
1 bind lb vserver <name> <serviceName>
2 <!--NeedCopy-->
```

Beispiel:

```
1 bind lb vserver Vserver-LB-1 Service-DSR-1
2 <!--NeedCopy-->
```

So binden Sie einen Dienst mithilfe der GUI an einen virtuellen Lastausgleichsserver

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen Server und klicken Sie in den Abschnitt “ **Dienste** “, um einen Dienst an den virtuellen Server zu binden.

Verwenden der Client-IP-Adresse im Outer Header von Tunnelpaketen

Der Citrix ADC unterstützt die Verwendung der Clientquell-IP-Adresse als Quell-IP-Adresse im äußeren Header von Tunnelpaketen, die sich auf den Rückgabemodus des Direktservers mit IP-Tunneling

beziehen. Diese Funktion wird für DSR mit IPv4 und DSR mit IPv6-Tunneling-Modi unterstützt. Um diese Funktion zu aktivieren, aktivieren **Sie den Parameter Clientquell-IP-Adresse verwenden** für IPv4 oder IPv6. Diese Einstellung wird global auf alle DSR-Konfigurationen angewendet, die IP-Tunneling verwenden.

So verwenden Sie eine Clientquell-IP-Adresse als Quell-IP-Adresse über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `set iptunnelparam -useclientsourceip [YES | NO]`
- `show iptunnelparam`

So verwenden Sie die Clientquell-IP-Adresse als Quell-IP-Adresse über die grafische Benutzeroberfläche

1. Navigieren Sie zu **System > Netzwerk**.
2. Klicken Sie auf der Registerkarte **Einstellungen** auf **Globale IPv4-Tunneleinstellungen**.
3. Wählen Sie auf der Seite **Globale IPv4-Tunnelparameter konfigurieren** die Option **Clientquell-IP verwenden** aus.
4. Klicken Sie auf **OK**.

So verwenden Sie die Clientquell-IP-Adresse als Quell-IP-Adresse über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `set ip6tunnelparam -useclientsourceip [YES | NO]`
- `show ip6tunnelparam`

So verwenden Sie die Clientquell-IP-Adresse als Quell-IP-Adresse über die grafische Benutzeroberfläche

1. Navigieren Sie zu **System > Netzwerk**.
2. Klicken Sie auf der Registerkarte **Einstellungen** auf **Globale IPv6-Tunneleinstellungen**.
3. Wählen Sie auf der Seite **Globale IPv6-Tunnelparameter konfigurieren** die Option **Clientquell-IP verwenden** aus.
4. Klicken Sie auf **OK**.

Konfiguration der Entkapselung

Sie können entweder eine Citrix ADC Appliance oder einen Back-End-Server als Entkapselung konfigurieren.

Citrix ADC Entkapselung

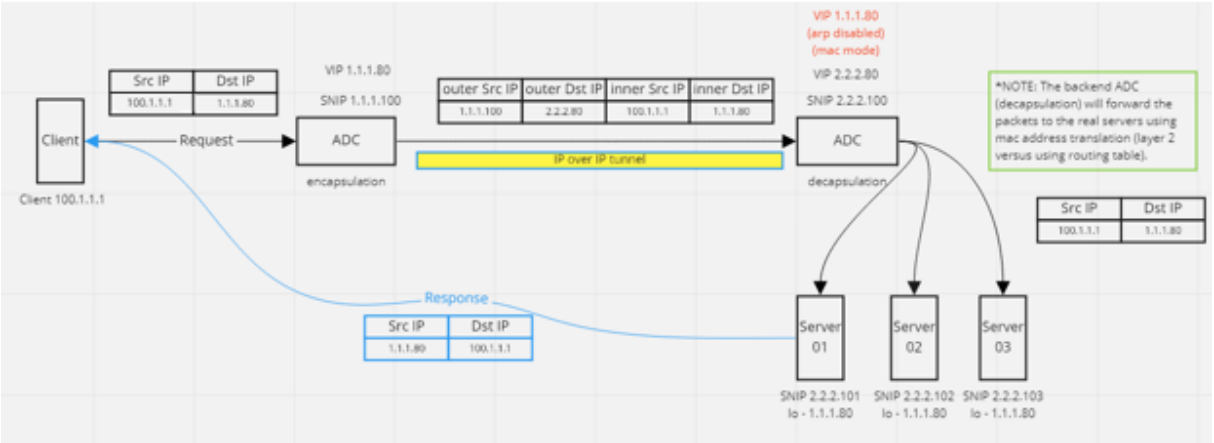
Wenn eine Citrix ADC Appliance als Entkapselung verwendet wird, muss in der Citrix ADC Appliance ein IP-Tunnel erstellt werden. Weitere Informationen finden Sie unter Konfigurieren von IP-Tunneln.

Das Citrix ADC Dekapselungs-Setup besteht aus den folgenden zwei virtuellen Servern:

- Der erste virtuelle Server empfängt das gekapselte Paket und entfernt die äußere IP-Kapselung.
- Der zweite virtuelle Server verfügt über die IP des ursprünglichen Dienstes im Front-End ADC und leitet das Paket mithilfe der MAC-Adresse der gebundenen Dienste mithilfe der MAC-Adresse der gebundenen Dienste an das Back-End weiter. Dieses Setup wird normalerweise als L2DSR bezeichnet. Stellen Sie sicher, dass Sie ARP auf diesem virtuellen Server deaktivieren.

Beispiel-Setup:

Die folgende Abbildung zeigt ein Entkapselungs-Setup mit den ADC-Appliances.



Die vollständige Konfiguration, die für das Setup erforderlich ist, lautet wie folgt.

Front-End-ADC-Konfiguration:

```
1 add service svc_DSR01 2.2.2.80 ANY * -usip YES -useproxyport NO
2 add lb vserver vip_DSR_ENCAP ANY 1.1.1.80 * -lbMethod SOURCEIPHASH -m
     IPTUNNEL -sessionless ENABLED
3 bind lb vserver vip_DSR_ENCAP svc_DSR01
4 <!--NeedCopy-->
```

Back-End-ADC-Konfiguration:


```
add ipTunnel DSR-IPIP 1.1.1.100 255.255.255.255 *

add service svc_DSR01_01 2.2.2.101 ANY * -usip YES -useproxyport NO
add service svc_DSR01_02 2.2.2.102 ANY * -usip YES -useproxyport NO
add service svc_DSR01_03 2.2.2.103 ANY * -usip YES -useproxyport NO

add lb vserver vs_DSR_DECAP ANY 2.2.2.80 * -lbMethod SOURCEIPHASH -m
    IPTUNNEL -sessionless ENABLED -netProfile netProf_DSR_MBF_noIP

add ns ip 1.1.1.80 255.255.255.255 -type VIP -arp DISABLED -snmp
    DISABLED
add lb vserver vs_DSR_Relay ANY 1.1.1.80 * -lbMethod SOURCEIPHASH -m
    MAC -sessionless ENABLED

bind lb vserver vs_DSR_DECAP svc_DSR01_01
bind lb vserver vs_DSR_DECAP svc_DSR01_02
bind lb vserver vs_DSR_DECAP svc_DSR01_03

bind lb vserver vip_DSR_Relay svc_DSR01_01
bind lb vserver vip_DSR_Relay svc_DSR01_02
bind lb vserver vip_DSR_Relay svc_DSR01_03

add netProfile netProf_DSR_MBF_noIP -MBF ENABLED
add lb monitor mon_DSR_MAC PING -netProfile netProf_DSR_MBF_noIP
bind service svc_DSR01_01 -monitorName mon_DSR_MAC
bind service svc_DSR01_02 -monitorName mon_DSR_MAC
bind service svc_DSR01_03 -monitorName mon_DSR_MAC
<!--NeedCopy-->
```

Das folgende Beispiel zeigt ein Test-Setup mit Ubuntu- und Red Hat Servern, auf denen apache2 ausgeführt wird. Diese Befehle werden auf jedem Back-End-Server eingerichtet.

```
sudo ip addr add 1.1.1.80 255.255.255.255 dev lo
sudo sysctl net.ipv4.conf.all.arp_ignore=1
sudo sysctl net.ipv4.conf.all.arp_announce=2
sudo sysctl net.ipv4.conf.eth4.rp_filter=2 (The interface has the
    external IP with route towards the ADC)
sudo sysctl net.ipv4.conf.all.forwarding=1
sudo ip link set dev lo arp on
<!--NeedCopy-->
```

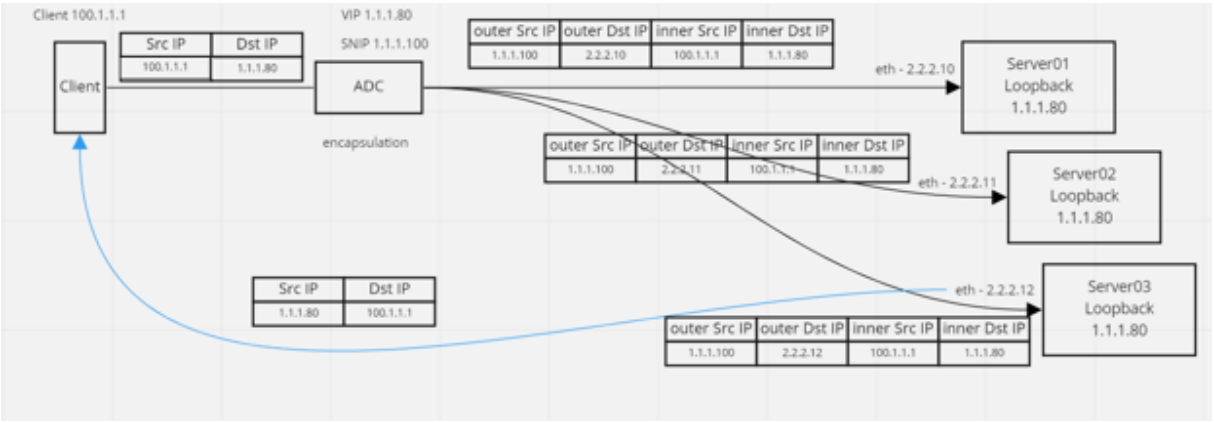

Entkapselung des Backend-Servers

Wenn Sie die Back-End-Server als Entkapselung verwenden, variiert die Back-End-Konfiguration je nach Serverbetriebssystemtyp. Sie können einen Back-End-Server als Entkapselung konfigurieren, indem Sie die folgenden Schritte ausführen:

1. Konfigurieren Sie eine Loop-Back-Schnittstelle mit IP für Dienst-IP.
2. Erstellen Sie eine Tunnelschnittstelle.
3. Fügen Sie eine Route über Tunnelschnittstelle hinzu.
4. Konfigurieren Sie die Einstellungen der Benutzeroberfläche nach Bedarf für den Datenverkehr

> Hinweis:
>
> Windows-Betriebssystem-Server können IP-Tunneln nicht nativ durchführen, daher werden die Befehle als Beispiele für Linux-basierte Systeme bereitgestellt. Plug-Ins von Drittanbietern sind für Windows-Betriebssystem-Server verfügbar, das liegt jedoch außerhalb des Geltungsbereichs dieses Beispiels.

Die folgende Abbildung zeigt ein Entkapselungs-Setup unter Verwendung der Back-End-Server.



Beispielkonfiguration:

In diesem Beispiel ist 1.1.1.80 die virtuelle IP-Adresse (VIP) von Citrix ADC und 2.2.2.10-2.2.2.12 sind die IP-Adressen des Back-End-Servers. Die VIP-Adresse ist in der Loopback-Schnittstelle konfiguriert und eine Route wird über die Tunnelschnittstelle hinzugefügt. Die Monitore verwenden die Server-IP und tunneln die Monitorpakete mithilfe der Tunnelendpunkte über den IP-Tunnel.

Die vollständige Konfiguration, die für das Setup erforderlich ist, lautet wie folgt.

Front-End-ADC-Konfiguration:

Die folgende Konfiguration erstellt einen Monitor, der den Tunnelendpunkt als Quelle verwendet. Senden Sie dann Pings über den Tunnel an die Dienst-IP-Adresse.

```
1 add ns ip 10.0.1.2 255.255.255.252 -vServer DISABLED
```



```
2 add netProfile netProfile_DSR -srcIP 10.0.1.2
3 add lb monitor mon_DSR PING -LRTM DISABLED -destIP 1.1.1.80 -ipTunnel
     YES -netProfile netProfile_DSR
4 <!--NeedCopy-->
```

Die folgende Konfiguration erstellt einen VIP für den Dienst, der die ursprüngliche Quell-IP-Adresse verwendet. Leitet dann den Datenverkehr über den IP-Tunnel an Back-End-Server weiter.

```
1 add service svc_DSR01 2.2.2.10 ANY * -usip YES -useproxyport NO
2 bind service svc_DSR01 -monitorName mon_DSR
3
4 add service svc_DSR02 2.2.2.11 ANY * -usip YES -useproxyport NO
5 bind service svc_DSR02 -monitorName mon_DSR
6
7 add service svc_DSR03 2.2.2.12 ANY * -usip YES -useproxyport NO
8 bind service svc_DSR03 -monitorName mon_DSR
9
10 add lb vserver vip_DSR_ENCAP ANY 1.1.1.80 * -lbMethod SOURCEIPHASH -m
     IPTUNNEL -sessionless ENABLED
11 bind lb vserver vip_DSR_ENCAP svc_DSR01
12 bind lb vserver vip_DSR_ENCAP svc_DSR02
13 bind lb vserver vip_DSR_ENCAP svc_DSR03
14 <!--NeedCopy-->
```

Back-End-Serverkonfiguration jedes Servers:

Die folgenden Befehle sind erforderlich, damit der Back-End-Server das IPIP-Paket empfangen, die äußere Kapselung entfernt und dann vom Loopback auf die ursprüngliche Client-IP reagiert. Dadurch wird sichergestellt, dass die IP-Adressen in dem vom Client empfangenen Paket mit den IP-Adressen in der ursprünglichen Anforderung übereinstimmen.

```
1 modprobe ipip
2 sudo ip addr add 1.1.1.80 255.255.255.255 dev lo
3 nmcli connection add type ip-tunnel ip-tunnel.mode ipip con-name tun0
4 ifname tun0 remote 198.51.100.5 local 203.0.113.10
5 nmcli connection modify tun0 ipv4.addresses '10.0.1.1/30'
6 nmcli connection up tun0
7 sudo sysctl net.ipv4.conf.all.arp_ignore=1
8 sudo sysctl net.ipv4.conf.all.arp_announce=2
9 sudo sysctl net.ipv4.conf.tun0.rp_filter=2
10 sudo sysctl net.ipv4.conf.all.forwarding=1
11 sudo ip link set dev lo arp off
```



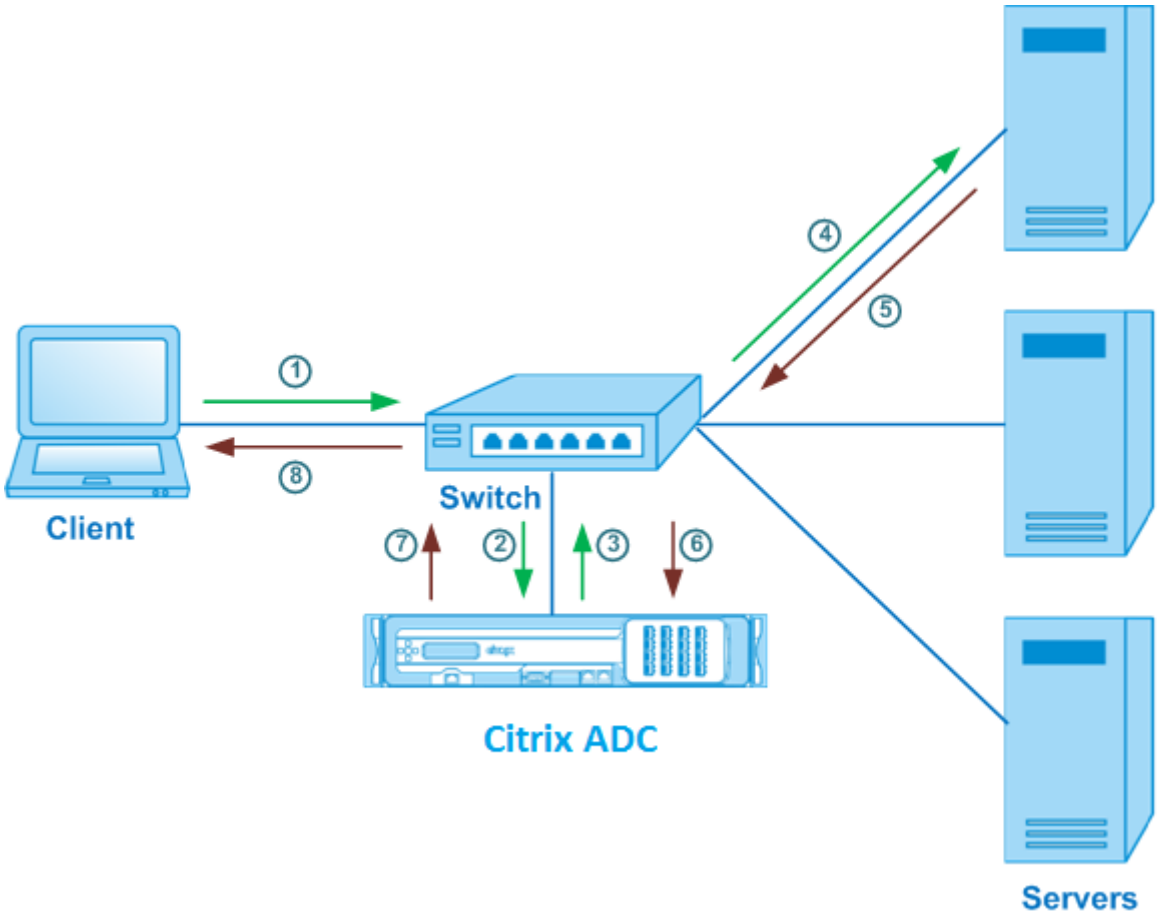
```
<!--NeedCopy-->
```

Anwendungsfall 8: Lastausgleich im Einarmmodus konfigurieren

October 5, 2021

In einem Einarm-Setup verbinden Sie die Citrix ADC Appliance über ein einzelnes VLAN mit dem Netzwerk. Die Appliance empfängt die Anforderung vom Client auf einem einzelnen VLAN und sendet die Anforderung an den Server auf demselben VLAN. Dies ist eines der einfachsten Bereitstellungsszenarien, bei denen der Router, die Server und die Appliance alle mit demselben Switch verbunden sind. Clientanforderungen am Switch werden an die Appliance weitergeleitet, und die Appliance verwendet die konfigurierte Lastausgleichsmethode, um den Dienst auszuwählen.

Abbildung 1. Lastausgleich im Einarmmodus



Im Beispielszenario werden die Dienste Service-ANY-1, Service-ANY-2 und Service-ANY-3 erstellt und an den virtuellen Server Vserver-LB-1 gebunden. Der virtuelle Server gleicht die Clientanforderung an

einen Dienst aus. In der folgenden Tabelle sind die Namen und Werte der Entitäten aufgeführt, die auf der Appliance im Einarmmodus konfiguriert sind.

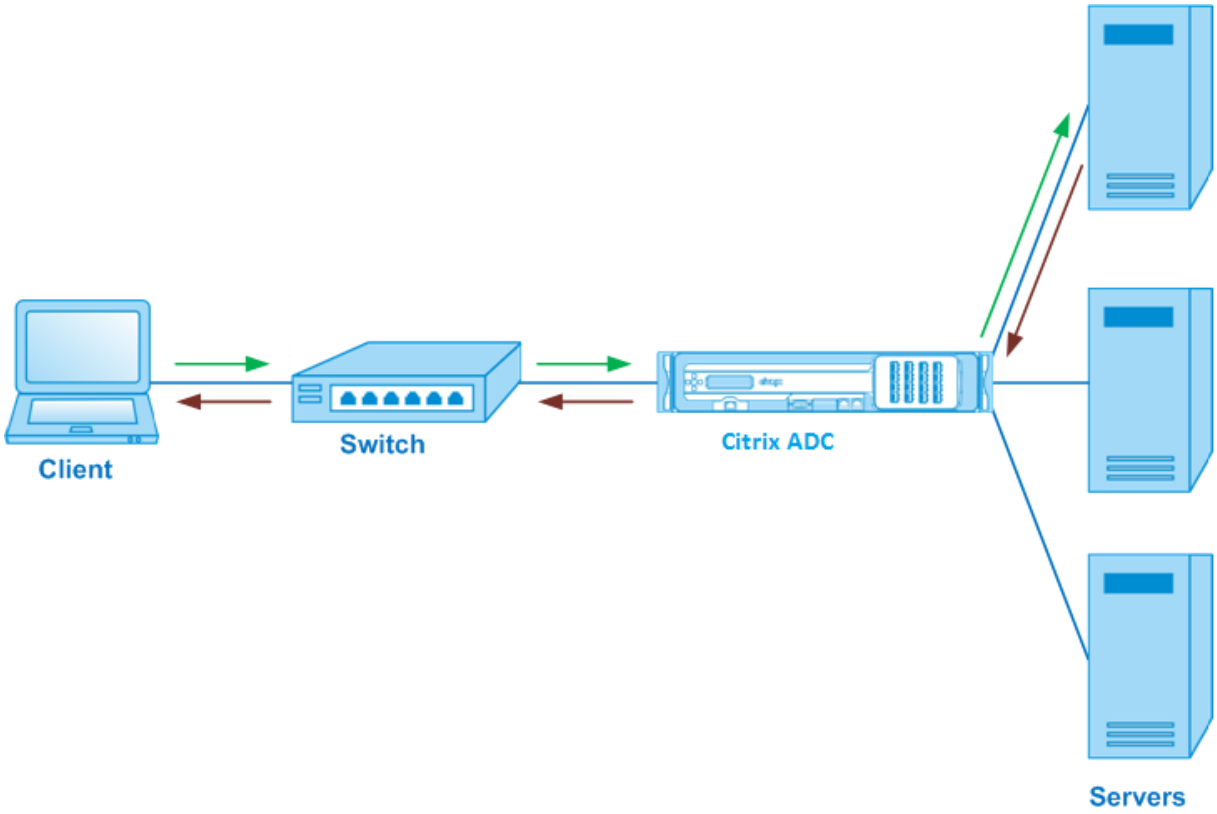
Entitätstyp	Name	IP-Adresse	Protokoll
Virtueller Server	Vserver-LB-1	10.102.29.94	ANY
Services	Service-ANY-1	10.102.29.91	ANY
	Service-ANY-2	10.102.29.92	ANY
	Service-ANY-3	10.102.29.93	ANY
Monitore	TCP	Ohne	Ohne

Informationen zum Konfigurieren eines Load Balancing-Setups im Einarmmodus finden Sie unter Einrichten des Basic Load Balancing.

Anwendungsfall 9: Konfigurieren des Lastausgleichs im Inline-Modus

October 5, 2021

In einem Inline-Modus (auch als Zwei-Arm-Modus bezeichnet) verbinden Sie die Citrix ADC Appliance über mehrere VLANs mit dem Netzwerk. Die Appliance empfängt die Anforderung vom Client auf einem VLAN und sendet die Anforderung an den Server in einem anderen VLAN. Im Zweiarm-Setup wird die Appliance zwischen den Servern und dem Client verbunden. Clientanforderungen am Switch werden an die Appliance weitergeleitet, und die Appliance verwendet die konfigurierte Lastausgleichsmethode, um den Dienst auszuwählen.



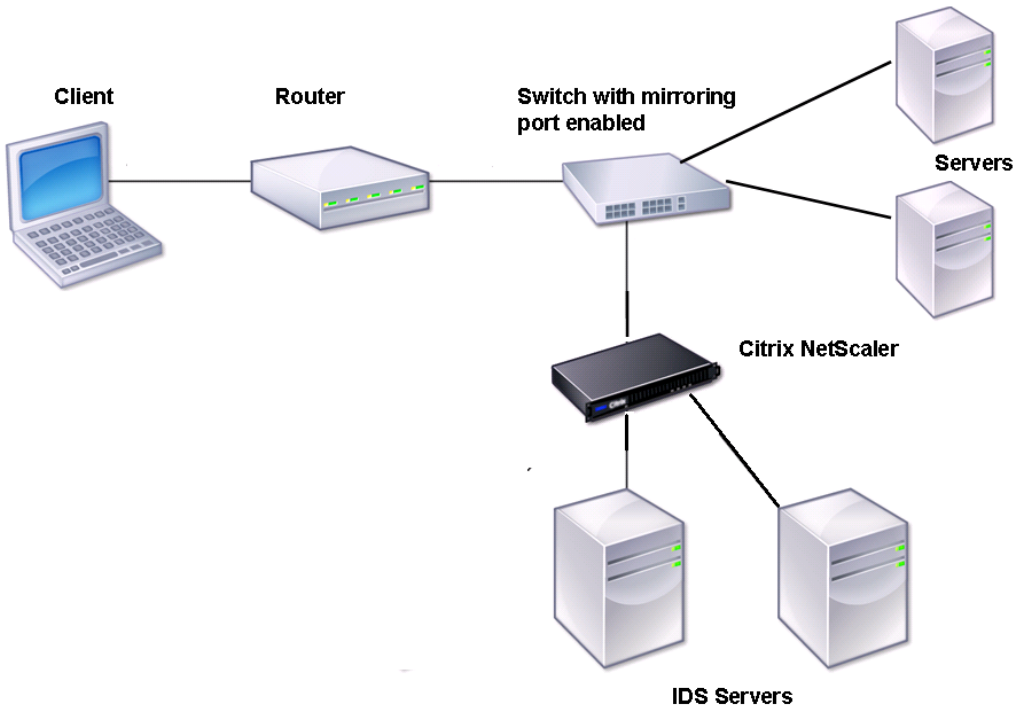
Die Konfiguration und das Entitätsdiagramm für den Inlinemodus sind die gleichen wie unter Load Balancing im Einarmmodus konfigurierenbeschrieben.

Anwendungsfall 10: Lastausgleich von Intrusion Detection Systemservern

October 5, 2021

Damit die Citrix ADC Appliance den Lastenausgleich von IDS-Servern (Intrusion Detection System) unterstützen kann, müssen die IDS-Server und -Clients über einen Switch mit aktivierter Portspiegelung verbunden sein. Der Client sendet eine Anforderung an den Server. Da die Portspiegelung auf dem Switch aktiviert ist, werden die Anforderungspakete kopiert oder an den virtuellen Serverport der Citrix ADC Appliance gesendet. Die Appliance verwendet dann die konfigurierte Lastausgleichsmethode, um einen IDS-Server auszuwählen, wie im folgenden Diagramm dargestellt.

Abbildung 1. Topologie von IDS-Servern mit Lastausgleich



Hinweis: Derzeit unterstützt die Appliance nur den Lastausgleich passiver IDS-Geräte.

Wie im vorhergehenden Diagramm dargestellt, funktioniert das IDS-Lastausgleichs-Setup wie folgt:

1. Die Clientanforderung wird an den IDS-Server gesendet, und ein Switch mit aktiviertem Spiegelungsport leitet diese Pakete an den IDS-Server weiter. Die Quell-IP-Adresse ist die IP-Adresse des Clients, und die Ziel-IP-Adresse ist die IP-Adresse des Servers. Die Quell-MAC-Adresse ist die MAC-Adresse des Routers, und die Ziel-MAC-Adresse ist die MAC-Adresse des Servers.
2. Der Datenverkehr, der über den Switch fließt, wird auf die Appliance gespiegelt. Die Appliance verwendet die Layer-3-Informationen (Quell-IP-Adresse und Ziel-IP-Adresse), um das Paket an den ausgewählten IDS-Server weiterzuleiten, ohne die Quell-IP-Adresse oder Ziel-IP-Adresse zu ändern. Es ändert die Quell-MAC-Adresse und die Ziel-MAC-Adresse in die MAC-Adresse des ausgewählten IDS-Servers.

Hinweis: Beim Lastenausgleich von IDS-Servern können Sie die Lastenausgleichsmethoden SRCIPHASH, DESTIPHASH oder SRCIPDESTIPHASH konfigurieren. Die SRCIPDESTIPHASH-Methode wird empfohlen, da Pakete, die vom Client zu einem Dienst auf der Appliance fließen, an einen einzelnen IDS-Server gesendet werden müssen.

Angenommen, service-ANY-1, service-ANY-2 und service-ANY-3 werden erstellt und an Vserver-LB-1

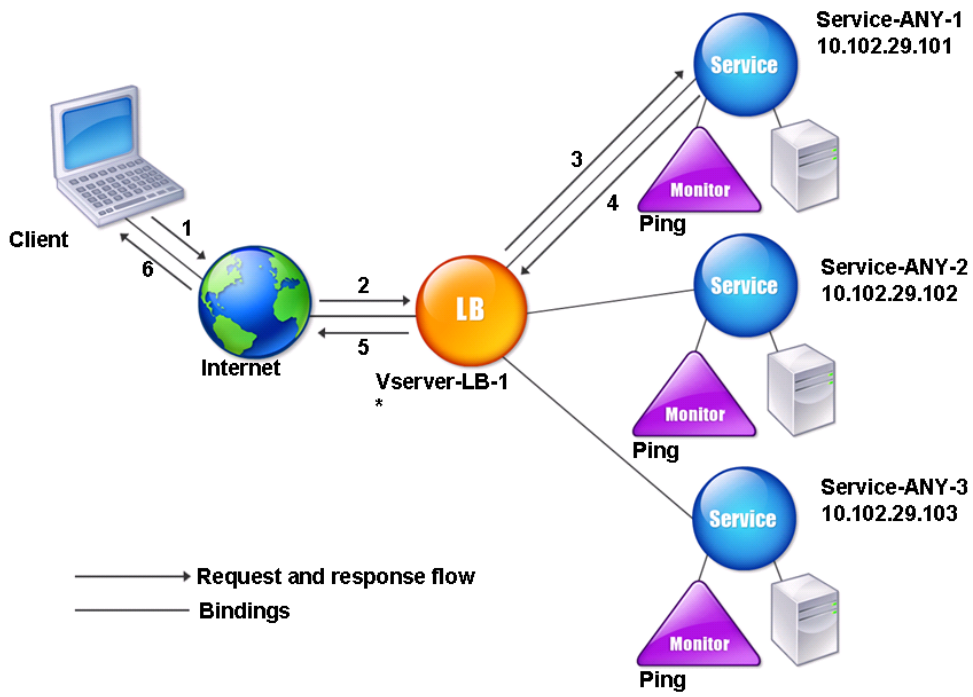
gebunden. Der virtuelle Server gleicht die Last der Dienste aus. In der folgenden Tabelle sind die Namen und Werte der auf der Appliance konfigurierten Entitäten aufgeführt.

Entitätstyp	Name	IP-Adresse	Port	Protokoll
Virtueller Server	Vserver-LB-1	*	*	ANY
Services	Service-ANY-1	10.102.29.101	*	ANY
	Service-ANY-2	10.102.29.102	*	ANY
	Service-ANY-3	10.102.29.103	*	ANY
Monitore	Ping	Ohne	Ohne	Ohne

Hinweis: Sie können den Inline-Modus oder den Einarmmodus für eine IDS-Lastausgleichseinrichtung verwenden.

Das folgende Diagramm zeigt die Lastausgleichseinheiten und die Werte der Parameter, die auf der Appliance konfiguriert werden sollen.

Abbildung 2. Entitätsmodell für Load Balancing IDS Server



Um ein IDS-Load Balancing-Setup zu konfigurieren, müssen Sie zunächst die MAC-basierte Weiterleitung aktivieren. Deaktivieren Sie auch die Layer-2- und Layer-3-Modi auf der Appliance.

So aktivieren Sie die MAC-basierte Weiterleitung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns mode <ConfigureMode>
<!--NeedCopy-->
```

Beispiel:

```
enable ns mode MAC
<!--NeedCopy-->
```

So aktivieren Sie die MAC-basierte Weiterleitung mit dem Konfigurationsdienstprogramm

Navigieren Sie zu **System > Einstellungen > Modi konfigurieren**und wählen Sie **MAC-basierte Weiterleitung**aus.

Als Nächstes finden Sie unter “Einrichten des Basic Load Balancing”, um ein grundlegendes Load Balancing-Setup zu konfigurieren.

Nachdem Sie das grundlegende Lastausgleichs-Setup konfiguriert haben, müssen Sie es für IDS anpassen, indem Sie eine unterstützte Lastausgleichsmethode konfigurieren (z. B. die SRCIPDESTIP-Hash-Methode auf einem virtuellen Server ohne Sitzungsfunktion) und den MAC-Modus aktivieren. Die Appliance behält den Status der Verbindung nicht bei und leitet die Pakete nur an die IDS-Server weiter, ohne sie zu verarbeiten. Die Ziel-IP-Adresse und der Port bleiben unverändert, da sich der virtuelle Server im MAC-Modus befindet.

So konfigurieren Sie eine Load Balancing-Methode und einen Umleitungsmodus für einen sitzungslosen virtuellen Server mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <vServerName> -lbMethod <LBMethodOption> -m <
    RedirectionMode> -sessionless <Value>
<!--NeedCopy-->
```


Beispiel:

```
set lb vserver Vserver-LB-1 -lbMethod SourceIPDestIPHash -m MAC -
    sessionless enabled
<!--NeedCopy-->
```

> **Hinweis:**
>
> Für einen Dienst, der an einen virtuellen Server gebunden ist, auf dem die Option -m MAC aktiviert ist, müssen Sie einen Nicht-Benutzermonitor binden.

So konfigurieren Sie eine Load Balancing-Methode und einen Umleitungsmodus für einen sitzungslosen virtuellen Server mithilfe des Konfigurationsdienstprogramms

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen Server, und wählen Sie im Umleitungsmodus MAC-basiert aus.
3. Klicken Sie unter Erweiterte Einstellungen auf Methoden, und wählen Sie SRCIPDESTIPHASH aus. Klicken Sie auf Verkehrseinstellungen, und wählen Sie Sitzungsloser Lastenausgleich aus.

So legen Sie einen Dienst zur Verwendung der Quell-IP-Adresse mithilfe der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <ServiceName> -usip <Value>
<!--NeedCopy-->
```

Beispiel:

```
set service Service-ANY-1 -usip yes
<!--NeedCopy-->
```

So legen Sie einen Dienst zur Verwendung der Quell-IP-Adresse mit dem Konfigurationsdienstprogramm fest

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienste**.
2. Öffnen Sie einen Dienst, und wählen Sie unter Einstellungen **Quell-IP-Adresse verwenden**aus.

Damit USIP korrekt funktioniert, müssen Sie es global festlegen. Weitere Informationen zum globalen Konfigurieren von USIP finden Sie unter IP-Adressierung.

Anwendungsfall 11: Isolieren des Netzwerkverkehrs mit Listening-Richtlinien

October 5, 2021

> **Hinweis**
>
> Die Traffic-Isolationslösung, die virtuelle Shadow-Server zur Simulation der Multitenant-Isolation verwendet, wird nicht mehr empfohlen. Alternativ empfiehlt Citrix, die Citrix ADC Admin Partitioning-Funktion für solche Bereitstellungen zu verwenden. Weitere Informationen finden Sie unter Admin-Partitionierung.

Eine häufige Sicherheitsanforderung in einem Rechenzentrum besteht darin, die Isolierung des Netzwerkpfads zwischen dem Datenverkehr verschiedener Anwendungen oder Mandanten aufrechtzuerhalten. Der Datenverkehr einer Anwendung oder eines Mandanten muss vom Datenverkehr anderer Anwendungen oder Mandanten isoliert werden. Beispielsweise möchte ein Finanzdienstleister den Datenverkehr der Anwendungen seiner Versicherungsabteilung von dem seiner Finanzdienstleistungsanwendungen trennen. In der Vergangenheit wurde dies leicht durch die physische Trennung von Netzwerkdienstgeräten wie Firewalls, Load Balancern und IdP sowie Netzwerküberwachung und logische Trennung in der Switching-Fabric erreicht.

Während sich Rechenzentrumsarchitekturen hin zu virtualisierten Rechenzentren mit mehreren Mandanten entwickeln, werden Netzwerkdienste im Aggregationslayer eines Rechenzentrums konsolidiert. Diese Entwicklung hat die Netzwerkpfadisolierung zu einer kritischen Komponente für Netzwerkdienstgeräte gemacht und führt dazu, dass ADCs Datenverkehr auf den Ebenen L4 bis L7 isolieren können. Darüber hinaus muss der gesamte Datenverkehr eines bestimmten Mandanten über eine Firewall laufen, bevor die Service-Schicht erreicht wird.

Um die Anforderung der Isolierung der Netzwerkpfade zu erfüllen, identifiziert eine Citrix ADC Appliance die Netzwerkdomänen und steuert den Datenverkehr in den Domänen. Die Citrix ADC Lösung besteht aus zwei Hauptkomponenten: Listen Policies und Shadow Virtual Server.

Jedem zu isolierenden Netzwerkpfad wird ein virtueller Server zugewiesen, auf dem eine Listenrichtlinie definiert ist, sodass der virtuelle Server nur Datenverkehr von einer angegebenen Netzwerkdomäne überwacht.

Um den Datenverkehr zu isolieren, können Abhörrichtlinien auf mehreren Clientparametern oder deren Kombinationen basieren, und den Richtlinien können Prioritäten zugewiesen werden. In

der folgenden Tabelle sind die Parameter aufgeführt, die in Listenrichtlinien zum Identifizieren des Datenverkehrs verwendet werden können.

Kategorie	Parameter
Ethernet-Protokoll	Quell-MAC-Adresse, Ziel-MAC-Adresse
Netzwerkschnittstelle	Netzwerk-ID, Empfangsdurchsatz, Sendedurchsatz, Übertragungsdurchsatz
IP-Protokoll	Quell-IP-Adresse, Ziel-IP-Adresse
IPv6-Protokoll	Quell-IPv6-Adresse, Ziel-IPv6-Adresse
TCP-Protokoll	Quellport, Zielport, maximale Segmentgröße, Nutzlast und andere Optionen
UDP-Protokoll	Quellport, Zielport
VLAN	ID

Tabelle 1. Client-Parameter, die zum Definieren von Listen Policies verwendet werden

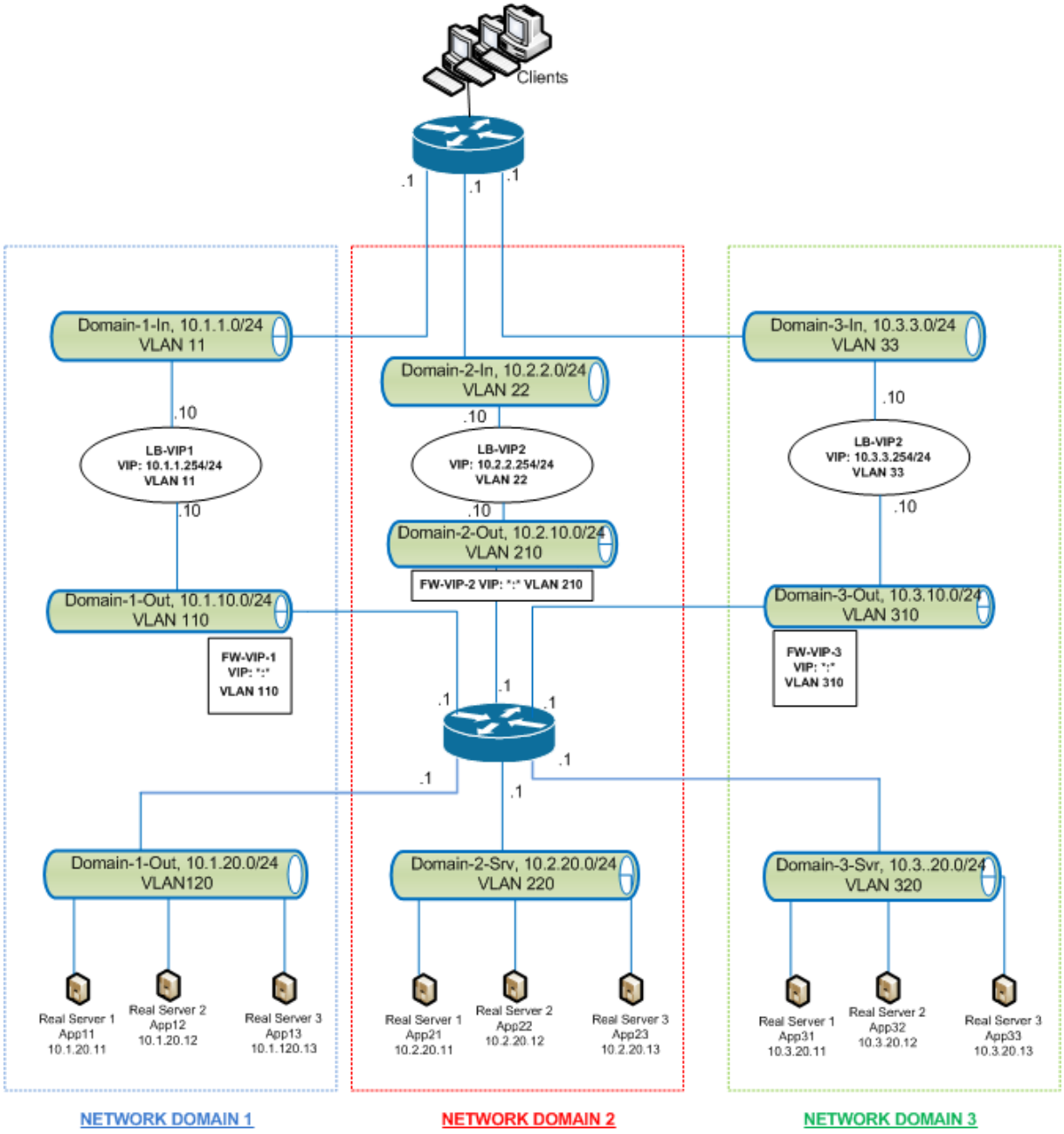
Auf der Citrix ADC Appliance wird für jede Domäne ein virtueller Server konfiguriert, mit einer Listenrichtlinie, die angibt, dass der virtuelle Server nur den Datenverkehr für diese Domäne überwachen soll. Außerdem wird für jede Domäne ein virtueller Schatten-Lastausgleichsserver konfiguriert, der den für jede Domäne bestimmten Datenverkehr überwacht. Jeder der virtuellen Shadow-Lastausgleichsserver verfügt über eine Platzhalter-IP-Adresse (*) und einen Port, und sein Diensttyp ist auf ANY festgelegt.

In jeder Domäne ist eine Firewall für die Domäne als Dienst an den virtuellen Schatten-Lastausgleichsserver gebunden, der den gesamten Datenverkehr über die Firewall weiterleitet. Lokaler Datenverkehr wird an das Ziel weitergeleitet, und der für eine andere Domäne bestimmte Datenverkehr wird an die Firewall für diese Domäne weitergeleitet. Die virtuellen Shadow-Lastausgleichsserver sind für die Umleitung des MAC-Modus konfiguriert.

Wie Netzwerkpfade isoliert werden

Die folgende Abbildung zeigt einen typischen Datenverkehr über Domänen hinweg. Betrachten Sie den Datenverkehr innerhalb der Netzwerkdomäne 1 und zwischen Netzwerkdomäne 1 und Netzwerkdomäne 2.

Abbildung 1. Netzwerkpfad isolieren



Datenverkehr innerhalb der Netzwerkdomäne 1

Netzwerkdomäne 1 verfügt über drei VLANs: VLAN 11, VLAN110 und VLAN120. In den folgenden Schritten wird der Verkehrsfluss beschrieben.

- Ein Client von VLAN 11 sendet eine Anforderung für einen Dienst, der aus dem Service-Pool in VLAN 120 verfügbar ist.
- Der virtuelle Lastausgleichsserver LB-VIP1, der für das Abhören des Datenverkehrs von VLAN 11 konfiguriert ist, empfängt die Anforderung und leitet die Anforderung an VLAN 110 weiter. Der

virtuelle Server in VLAN 110 leitet die Anforderung an den Schattenlastenausgleich virtuellen Server FW-VIP-1 weiter.
- FW-VIP-1, die für das Abhören von Datenverkehr von VLAN 110 konfiguriert ist, empfängt die Anforderung und leitet sie an VLAN 120 weiter.
- Der virtuelle Lastausgleichsserver in VLAN 120 gleicht die Anforderung an einen der physischen Server App11, App12 oder App13 aus.
- Die vom physischen Server gesendete Antwort gibt den gleichen Pfad an den Client in VLAN 11 zurück.

Diese Konfiguration stellt sicher, dass der Datenverkehr immer innerhalb des Citrix ADC für den gesamten Datenverkehr getrennt wird, der von einem Client stammt.

Datenverkehr zwischen Netzwerkdomäne 1 und Netzwerkdomäne 2

Netzwerkdomäne 1 verfügt über drei VLANs: VLAN 11, VLAN110 und VLAN120. Netzwerkdomäne 2 verfügt außerdem über drei VLANS: VLAN 22, VLAN 210 und VLAN 220. In den folgenden Schritten wird der Verkehrsfluss von VALN 11 zu VLAN 22 beschrieben.

- Ein Client von VLAN 11, der zur Netzwerkdomäne 1 gehört, sendet eine Anforderung für einen Dienst, der aus dem Dienstpool in VLAN 220 verfügbar ist, der zur Netzwerkdomäne 2 gehört.
- In Netzwerkdomäne 1 empfängt der virtuelle Lastausgleichsserver LB-VIP1, der für das Abhören des Datenverkehrs von VLAN 11 konfiguriert ist, die Anforderung und leitet die Anforderung an VLAN 110 weiter.
- Der virtuelle Schattenlastenausgleichsserver FW-VIP-1, der für das Abhören von VLAN 110-Datenverkehr konfiguriert ist, der an eine andere Domäne bestimmt ist, empfängt die Anforderung und leitet sie an den virtuellen Firewallserver FW-VIP-2 weiter, da die Anforderung an einen physischen Server in der Netzwerkdomäne 2 bestimmt ist.
- In Netzwerkdomäne 2 leitet FW-VIP-2 die Anforderung an VLAN 220 weiter.
- Der virtuelle Lastausgleichsserver in VLAN 220 gleicht die Anforderung an einen der physischen Server App21, App22 oder App23 aus.
- Die vom physischen Server gesendete Antwort kehrt über den gleichen Pfad über die Firewall in Netzwerkdomäne 2 und dann an Netzwerkdomäne 1 zurück, um den Client in VLAN 11 zu erreichen.

Konfigurationsschritte

Gehen Sie folgendermaßen vor, um die Netzwerkpfadisolation mithilfe von Listen Policies zu konfigurieren:

- Hinzufügen von Listenrichtlinienausdrücken. Jeder Ausdruck gibt eine Domäne an, für die Datenverkehr bestimmt ist. Sie können die VLAN-ID oder andere Parameter verwenden, um den Datenverkehr zu identifizieren.

- Konfigurieren Sie für jede Netzwerkdomäne zwei virtuelle Server wie folgt:
  - Erstellen Sie einen virtuellen Lastausgleichsserver, für den Sie eine Listenrichtlinie angeben, die den für diese Domäne bestimmten Datenverkehr identifiziert. Sie können den Namen eines zuvor erstellten Ausdrucks angeben oder beim Erstellen des virtuellen Servers einen Ausdruck erstellen.
  - Erstellen Sie einen anderen virtuellen Lastausgleichsserver, der als Schattenserver bezeichnet wird, für den Sie einen Listenrichtlinienausdruck angeben, der auf Datenverkehr für eine Domäne angewendet wird. Legen Sie auf diesem virtuellen Server den Diensttyp auf ANY und die IP-Adresse und den Port auf ein Sternchen (*) fest. Aktivieren Sie die MAC-basierte Weiterleitung auf diesem virtuellen Server.
  - Aktivieren Sie die Option L2-Verbindung auf beiden virtuellen Servern.
    Zur Identifizierung einer Verbindung verwendet die Citrix ADC Appliance im Allgemeinen das 4-Tupel der Client-IP-Adresse, des Clientports, der Ziel-IP-Adresse und des Zielports. Wenn Sie die Option L2-Verbindung aktivieren, werden zusätzlich zum normalen 4-Tupel die Layer-2-Parameter der Verbindung (Kanalnummer, MAC-Adresse und VLAN-ID) verwendet.
- Fügen Sie Dienste hinzu, die die Serverpools in der Domäne darstellen, und binden Sie sie an den virtuellen Server.
- Konfigurieren Sie die Firewall für jede Domäne als Dienst und binden Sie alle Firewall-Dienste an den virtuellen Shadow-Server.

So isolieren Sie den Netzwerkverkehr mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
1 add policy expression <expressionName> <listenPolicyExpression>
2
3 add lb vserver <name> <serviceType> <ip> <port> -l2conn ON -
     listenPolicy <expressionName>
4 <!--NeedCopy-->
```

Fügen Sie für jede Domäne einen virtuellen Lastausgleichsserver hinzu. Dieser virtuelle Server ist für den Datenverkehr derselben Domäne.

```
1 add lb vserver <name> ANY * * -l2conn ON -m MAC -listenPolicy <
     expressionName>
2 <!--NeedCopy-->
```


Fügen Sie für jede Domäne einen virtuellen Schatten-Lastausgleichsserver hinzu. Dieser virtuelle Server ist für den Datenverkehr anderer Domänen geeignet.

Beispiel:

```
add policy expression e110 client.vlan.id==110
add policy expression e210 client.vlan.id==210
add policy expression e310 client.vlan.id==310
add policy expression e11 client.vlan.id==11
add policy expression e22 client.vlan.id==22
add policy expression e33 client.vlan.id==33

add lb vserver LB-VIP1 HTTP 10.1.1.254 80 -persistenceType NONE -
    listenPolicy e11
-cltTimeout 180 -l2Conn ON

add lb vserver LB-VIP2 HTTP 10.2.2.254 80 -persistenceType NONE -
    listenPolicy e22
-cltTimeout 180 -l2Conn ON

add lb vserver LB-VIP3 HTTP 10.3.3.254 80 -persistenceType NONE -
    listenPolicy e33
-cltTimeout 180 -l2Conn ON


add lb vserver FW-VIP-1 ANY * * -persistenceType NONE -lbMethod
    ROUNDROBIN - listenPolicy e110 -Listenpriority 1 -m MAC -cltTimeout
    120

add lb vserver FW-VIP-2 ANY * * -persistenceType NONE -lbMethod
    ROUNDROBIN - listenPolicy e210 -Listenpriority 2 -m MAC -cltTimeout
    120

add lb vserver FW-VIP-3 ANY * * -persistenceType NONE -lbMethod
    ROUNDROBIN - listenPolicy e310 -Listenpriority 3 -m MAC -cltTimeout
    120


add service RD-1 10.1.1.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip
    DISABLED
-usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA
    NO -TCPB NO -CMP NO

add service RD-2 10.2.2.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip
```



```
    DISABLED
29 -usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA
    NO -TCPB NO -CMP NO
30
31 add service RD-3 10.3.3.1 ANY * -gslb NONE -maxClient 0 -maxReq 0 -cip
    DISABLED
32 -usip NO -useproxyport NO -sp ON -cltTimeout 120 -svrTimeout 120 -CKA
    NO -TCPB NO -CMP NO
33
34
35 bind lb vserver FW-VIP-1 RD-1
36
37 bind lb vserver FW-VIP-2 RD-2
38
39 bind lb vserver FW-VIP-3 RD-3
40 <!--NeedCopy-->
```

So isolieren Sie den Netzwerkverkehr mit dem Konfigurationsdienstprogramm

1. Fügen Sie Dienste hinzu, die die Server repräsentieren, wie unter Service erstellenbeschrieben.
2. Fügen Sie jede Firewall als Dienst hinzu:
   a) Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
   b) Erstellen Sie einen Dienst, indem Sie das Protokoll als ANY, den Server als IP-Adresse der Firewall und den Port als 80 angeben.
3. Konfigurieren Sie einen virtuellen Lastenausgleichsserver.
4. Konfigurieren Sie den virtuellen Shadow-Lastausgleichsserver.
5. Wiederholen Sie für jede Netzwerkdomäne die Schritte 3 und 4.
6. Öffnen Sie im Bereich Virtuelle Server für Lastenausgleich die von Ihnen erstellten virtuellen Server, und überprüfen Sie die Einstellungen.

Anwendungsfall 12: Konfigurieren von XenDesktop für den Lastenausgleich

October 5, 2021

Um die Leistung bei der Bereitstellung virtueller Desktopanwendungen zu verbessern, können Sie die Citrix ADC-Appliance in Citrix XenDesktop integrieren und die Lastausgleichsfunktion von Citrix ADC verwenden, um die Last auf die Webinterface-Server und die DDC-Server (Desktop Delivery Controller) zu verteilen.

Im Allgemeinen verwenden Sie XenDesktop in Situationen, in denen Anwendungen nicht mit der Ausführung auf einem Terminalserver oder XenApp kompatibel sind oder wenn jeder virtuelle Desktop eindeutige Anforderungen aufweist. In solchen Fällen benötigen Sie einen Desktop-Host für jeden Benutzer, der eine Verbindung herstellt. Die Hosts können jedoch so gepoolt werden, dass Sie für jeden aktuell verbundenen Benutzer nur einen Host benötigen.

Der für XenDesktop bereitgestellte Hauptanwendungsdienst ist der Desktop Delivery Controller (DDC). Der DDC ist auf einem Server installiert, und seine Hauptfunktion besteht darin, Desktop-Hosts und Broker-Client-Verbindungen zu ihnen zu registrieren.

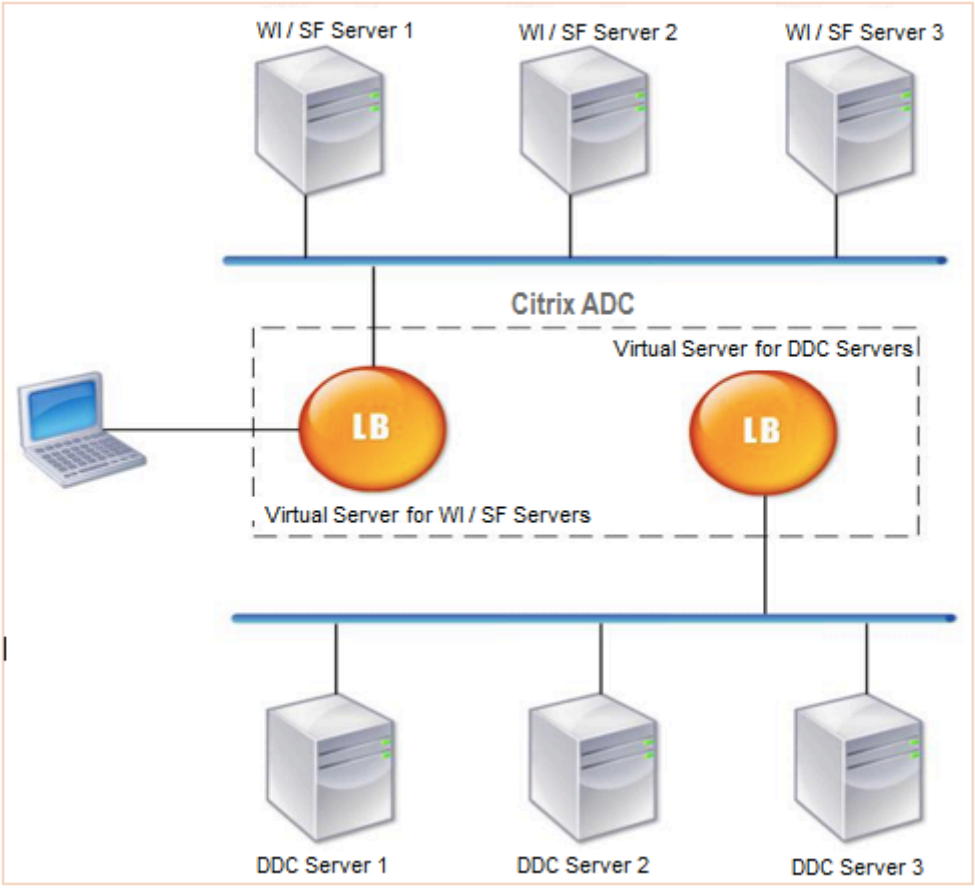
Der DDC authentifiziert auch Benutzer und verwaltet die Assembly der virtuellen Desktopumgebungen der Benutzer, indem er den Status der Desktops steuert und die Desktops startet und beendet.

Im Allgemeinen werden mehrere DDCs installiert, um die Verfügbarkeit zu verbessern.

Die Web Interface-Server bieten sicheren Zugriff auf virtuelle Desktops. Das Webinterface ist das anfängliche Verbindungsportal zum Desktop Delivery Controller (DDC). Der Webbrowser auf dem Gerät des Benutzers sendet Informationen an den Webserver, der mit der Serverfarm kommuniziert, um dem Benutzer Zugriff auf den virtuellen Desktop zu gewähren.

Die folgende Abbildung zeigt die Topologie einer Citrix ADC Appliance, die mit XenDesktop arbeitet.

Abbildung 1. Lastenausgleich von XenDesktop



Hinweis:

Obwohl Sie das HTTP-Protokoll verwenden können, empfiehlt Citrix, SSL für die Kommunikation zwischen dem Client und der Citrix ADC Appliance zu verwenden. Sie können das HTTP-Protokoll für die Kommunikation zwischen dem Citrix ADC und den DDC-Servern verwenden, obwohl Sie das SSL-Protokoll für die Kommunikation mit dem Client verwenden.

So konfigurieren Sie den Lastenausgleich für XenDesktop mit der GUI

1. Erstellen Sie einen Dienst.
   a) Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Services**, und klicken Sie auf **Hinzufügen** .
   b) Erstellen Sie einen Dienst, indem Sie einen Namen, eine IP-Adresse, einen Port und einen Protokolltyp angeben, und klicken Sie dann auf **OK**.
2. Erstellen Sie einen virtuellen Lastausgleichsserver.
   a) Navigieren Sie zu **Konfiguration** > **Verkehrsverwaltung** > **Lastenausgleich** > **Virtuelle Server**, und klicken Sie auf **Hinzufügen** .
   b) Erstellen Sie einen virtuellen Server, indem Sie einen Namen, eine IP-Adresse, einen Port

und einen Protokolltyp angeben, und klicken Sie dann auf **OK**.

3. Binden Sie den Dienst an den virtuellen Lastausgleichsserver.
4. Navigieren Sie zu **Konfiguration** > **Verkehrsverwaltung** > **Lastenausgleich** > **Virtuelle Server**, und wählen Sie einen Server aus.
   a) Klicken Sie auf **Edit**.
   b) Klicken Sie in den **Dienst- und Dienstgruppen**auf **>**und klicken Sie auf **Bindung hinzufügen**.
   c) Wählen Sie den Service aus, den Sie binden möchten, und geben Sie den Gewichtswert ein.
   d) Klicken Sie auf **Bind**.

So konfigurieren Sie den Lastenausgleich für XenDesktop mit der Befehlszeilenschnittstelle

- Um einen Dienst zu erstellen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name> <serverName> <serviceType> <port>
<!--NeedCopy-->
```

Beispiel:

```
add service Service-HTTP-1 192.0.2.5 HTTP 80
<!--NeedCopy-->
```

- Um einen virtuellen Server zu erstellen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <serviceType> <ip> <port>
<!--NeedCopy-->
```

Beispiel:

add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80

- Um einen Dienst an einen virtuellen Lastausgleichsserver zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

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


Beispiel:

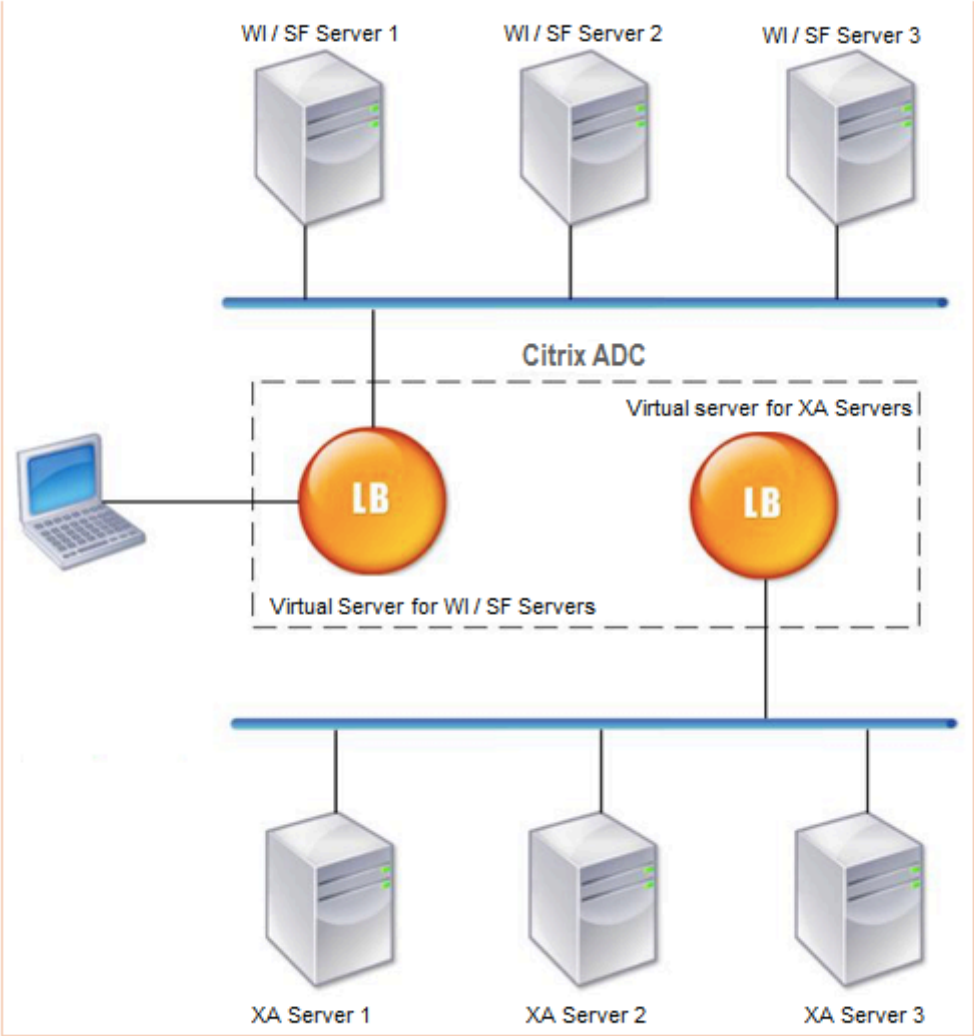
```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

Anwendungsfall 13: Konfigurieren von XenApp für den Lastenausgleich

October 5, 2021

Für eine effiziente Bereitstellung von Anwendungen können Sie die Citrix ADC-Appliance in Citrix XenApp integrieren und die Lastausgleichsfunktion von Citrix ADC verwenden, um die Last auf die XenApp-Serverfarmen zu verteilen. Die folgende Abbildung ist ein Topologiediagramm einer solchen Einrichtung.

Abbildung 1. Lastenausgleich von XenApp



Die Webinterface-Server bieten über den Webbrowser des Benutzers sicheren Zugriff auf XenApp -Anwendungsressourcen. Der Webinterface-Client präsentiert den Benutzern alle Ressourcen, z. B. Anwendungen, Inhalte und Desktops, die in den XenApp -Serverfarmen zur Verfügung gestellt werden. Benutzer können über einen Standard-Webbrowser oder über das Citrix Online-Plug-In auf die veröffentlichten Ressourcen zugreifen.

Der Webbrowser auf dem Gerät des Benutzers sendet Informationen an den Webserver, der mit den Servern in der Serverfarm kommuniziert, um dem Benutzer Zugriff auf die Ressourcen zu gewähren.

Das Web Interface und der XML Broker sind ergänzende Dienste. Das Webinterface bietet Benutzern Zugriff auf Anwendungen, und der XML-Broker wertet die Berechtigungen des Benutzers aus, um zu bestimmen, welche Anwendungen im Webinterface angezeigt werden.

Der XML-Dienst wird auf allen Servern in der Serverfarm installiert. Der im Webinterface angegebene

XML-Dienst fungiert als XML-Broker. Basierend auf den vom Webinterface-Server übergebenen Benutzeranmeldeinformationen sendet der XML-Broker-Server eine Liste der Anwendungen, auf die der Benutzer zugreifen kann.

In großen Unternehmen, in denen mehrere Webinterface-Server und XML-Broker-Server bereitgestellt werden, empfiehlt Citrix den Lastenausgleich dieser Server mithilfe der Citrix ADC Appliance. Konfigurieren Sie einen virtuellen Server für den Lastausgleich der Webinterface-Server und einen anderen für die XML Broker-Server. Die Load Balancing-Methode und andere Features können bei Bedarf auf dem virtuellen Server konfiguriert werden.

> **Hinweis:**
>
> Obwohl Sie das HTTP-Protokoll verwenden können, empfiehlt Citrix, SSL für die Kommunikation zwischen dem Client und dem Citrix ADC zu verwenden. Sie können das HTTP-Protokoll für die Kommunikation zwischen dem Citrix ADC und den WI-Servern verwenden, obwohl Sie das SSL-Protokoll für die Kommunikation mit dem Client verwenden.

So konfigurieren Sie den Lastenausgleich für XenApp mit der GUI

1. Erstellen Sie einen Dienst.
   a) Navigieren Sie zu **Konfiguration** > **Traffic Management** > **Load Balancing** > **Services**, und klicken Sie auf **Hinzufügen** .
   b) Erstellen Sie einen Dienst, indem Sie einen Namen, eine IP-Adresse, einen Port und einen Protokolltyp angeben, und klicken Sie dann auf **OK**.
2. Erstellen Sie einen virtuellen Lastausgleichsserver.
   a) Navigieren Sie zu **Konfiguration** > **Verkehrsverwaltung** > **Lastenausgleich** > **Virtuelle Server**, und klicken Sie auf **Hinzufügen** .
   b) Erstellen Sie einen virtuellen Server, indem Sie einen Namen, eine IP-Adresse, einen Port und einen Protokolltyp angeben, und klicken Sie dann auf **OK**.
3. Binden Sie den Dienst an den virtuellen Lastausgleichsserver.
4. Navigieren Sie zu **Konfiguration** > **Verkehrsverwaltung** > **Lastenausgleich** > **Virtuelle Server**, und wählen Sie einen Server aus.
   a) Klicken Sie auf **Edit**.
   b) Klicken Sie in den **Dienst- und Dienstgruppen**auf **>**und klicken Sie auf **Bindung hinzufügen**.
   c) Wählen Sie den Service aus, den Sie binden möchten, und geben Sie den Gewichtswert ein.
   d) Klicken Sie auf **Bind**.

So konfigurieren Sie den Lastenausgleich für XenApp mit der Befehlszeilenschnittstelle

- Um einen Dienst zu erstellen, geben Sie an der Eingabeaufforderung Folgendes ein:


```
add service <name> <serverName> <serviceType> <port>
<!--NeedCopy-->
```

Beispiel:

```
add service Service-HTTP-1 192.0.2.5 HTTP 80
<!--NeedCopy-->
```

- Um einen virtuellen Server zu erstellen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <serviceType> <ip> <port>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver Vserver-LB-1 HTTP 10.102.29.60 80
<!--NeedCopy-->
```

- Um einen Dienst an einen virtuellen Lastausgleichsserver zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiel:

```
bind lb vserver Vserver-LB-1 Service-HTTP-1
<!--NeedCopy-->
```

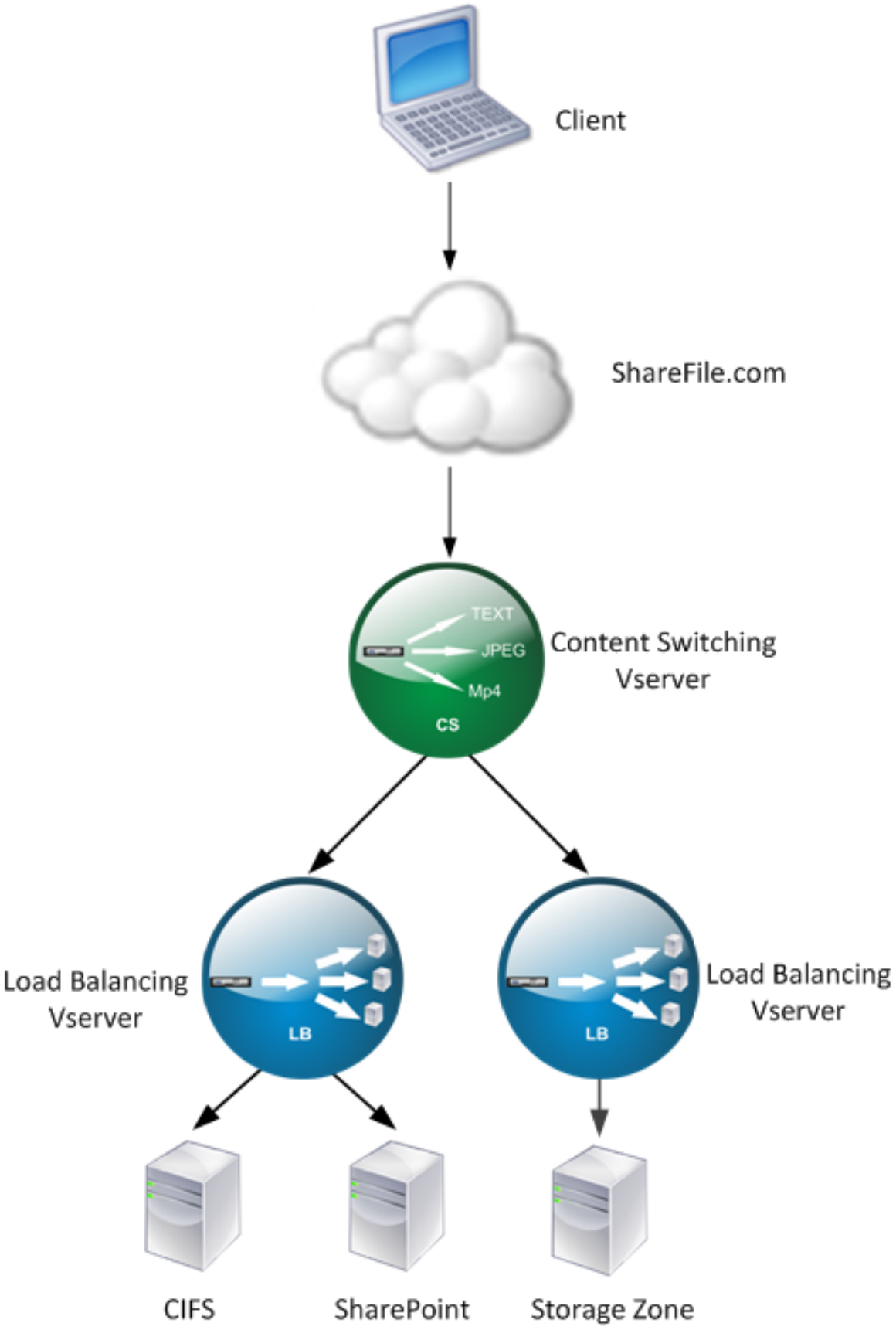
Anwendungsfall 14: ShareFile Assistent für den Lastenausgleich von Citrix ShareFile

October 5, 2021

Sie können den Lastenausgleich für Citrix ShareFile mit dem Assistenten konfigurieren. Der Citrix ShareFile Assistent hilft bei der Einrichtung der Load Balancing-Konfiguration für die ShareFile e-Website basierend auf dem angeforderten Inhaltstyp. Der Content Switching-Server leitet die Anforderung basierend darauf, ob es sich um eine StorageZone, CIFS oder eine SharePoint-Anfrage handelt. Content Switching basiert auf Richtlinien. Der Assistent generiert automatisch die Richtlinien, um festzustellen, ob die Anforderung für StorageZone, CIFS oder SharePoint gilt. Der virtuelle Content Switching-Server verwendet diese Richtlinien, um die Anforderung an den richtigen Lastausgleichsserver weiterzuleiten.

Ein typischer Datenfluss kann wie im folgenden Diagramm dargestellt werden.

Abbildung 1. ShareFile Daten-Lastenausgleich

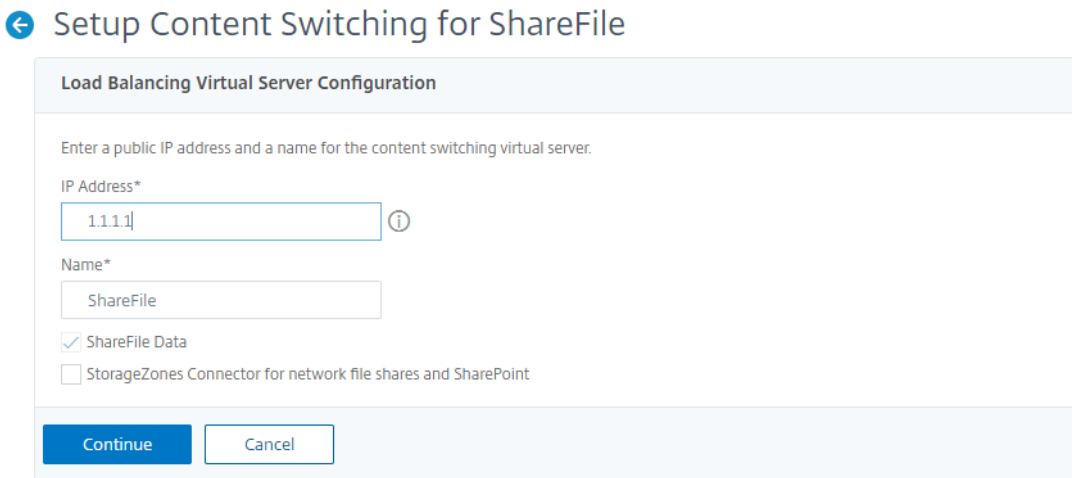


Sie können die virtuellen Lastausgleichsserver, die der ShareFile Assistent erstellt, anzeigen, indem Sie zu **Traffic Management > Virtuelle Server** and **Services > Virtuelle Server**navigieren. Sie können die virtuellen Server, die mit dem ShareFile e-Assistenten erstellt wurden, nicht manuell entfernen. Verwenden Sie den Assistenten, um die virtuellen Server zu entfernen.

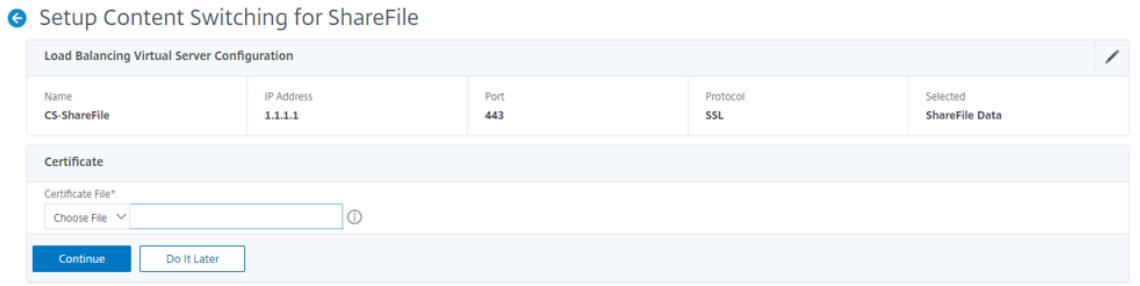
Citrix ADC verwendet die LDAP-Authentifizierung für SharePoint- oder CIFS-Anforderung. Die Hash-Authentifizierung wird zur Authentifizierung von Anforderungen für StorageZones verwendet.

So konfigurieren Sie eine Citrix ADC Appliance für den Lastenausgleich von Citrix ShareFile

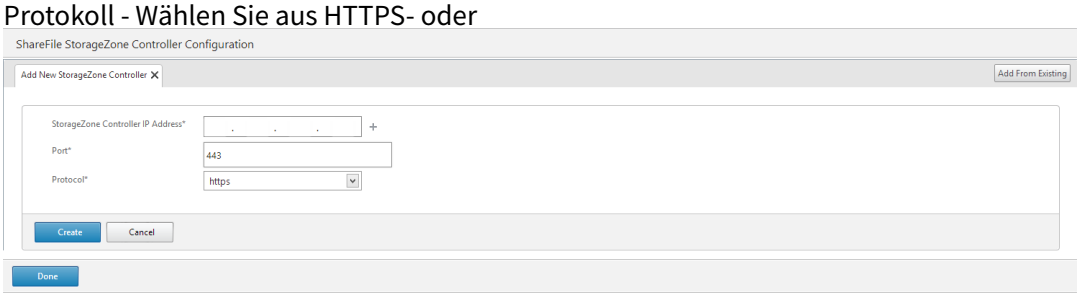
1. Klicken Sie im Navigationsbereich auf **Traffic Management**.
2. Klicken Sie im Abschnitt **Citrix ShareFile** auf **Citrix ADC für ShareFile einrichten**.
3. Geben Sie auf der Seite **Setup Content Switching for ShareFile** die folgenden Informationen an:
   - IP-Adresse: IP-Adresse des virtuellen Content Switching-Servers.
   - Name: Name des virtuellen Content Switching-Servers.
   - Wenn Sie Load Balancing für CIFS oder SharePoint einrichten möchten, klicken Sie auf das Kontrollkästchen **StorageZone Connector for Network File Shares/SharePoint**, und klicken Sie dann auf **Weiter**. Standardmäßig ist das Kontrollkästchen **ShareFile-Daten** aktiviert.



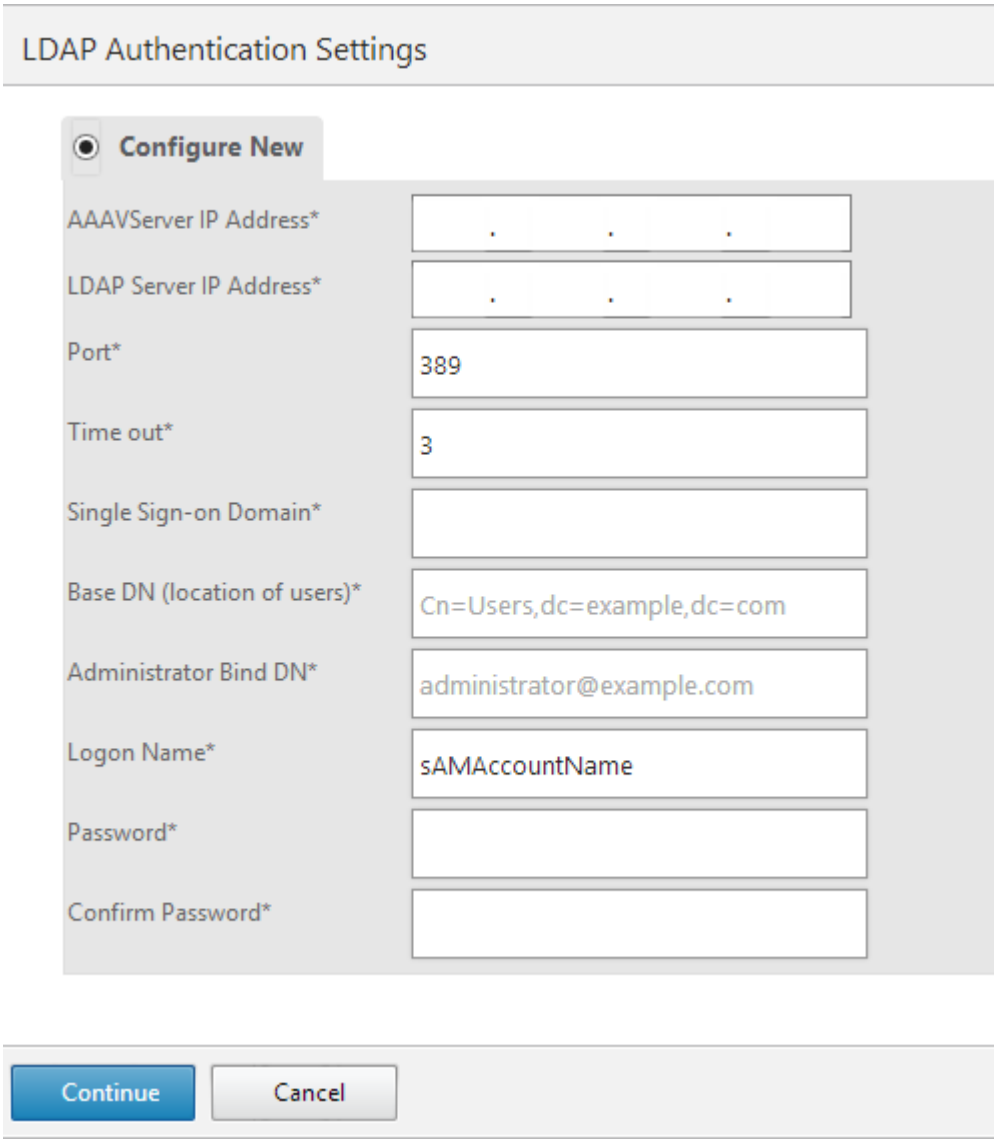
4. Geben Sie ein gültiges Zertifikat an. Wenn Sie ein Zertifikat haben, klicken Sie auf **Choose Certificate und wählen** Sie in der Dropdownliste das Zertifikat aus. Wenn Sie ein Zertifikat installieren müssen, klicken Sie auf **Zertifikat installieren** und geben Sie das Certificate-Key-Paar an.



5. Klicken Sie auf **Weiter**.
6. Geben **Sie im Dialogfeld Add New StorageZone Controller** die Werte der folgenden Parameter an:
   - StorageZone Controller-IP-Adresse — IP-Adresse
   - Port- Portnummer. Der Standardwert ist 443.
   - Protokoll - Wählen Sie aus HTTPS- oder



7. Klicken Sie auf **Erstellen** und dann auf **Fertig**. Der Assistent erstellt automatisch einen Dienst und generiert den Namen des Dienstes automatisch.
8. Wenn Sie den Lastenausgleich für CIFS oder SharePoint in Schritt 4.c ausgewählt haben, geben Sie die Werte für LDAP-Authentifizierungseinstellungen an:
   - IP-Adresse des virtuellen Citrix ADC AAA-Servers - IP-Adresse des virtuellen Citrix ADC AAA-Servers
   - LDAP-Server-IP-Adresse — IP-Adresse des LDAP-Servers
   - Port- Portnummer. Der Standardwert ist 389
   - Timeout - Der Timeout-Wert in Minuten
   - Single Sign-On-Domäne — Single-Sign-On-Domänenname
   - Basis-DN— Basisdomänenname
   - Administrator Bind-DN— LDAP-Kontoname mit dem Domänennamen, z. B. adminstrator@domainname.com
   - Anmeldename - Anmeldename ist der samAccountName
   - Kennwort und Kennwort bestätigen - Geben Sie das Kennwort ein und bestätigen Sie das Kennwort



9. Klicken Sie auf **Weiter** und dann auf **Fertig**.

So entfernen Sie die Lastausgleichskonfiguration für ShareFile

1. Klicken Sie im Navigationsbereich auf **Traffic Management**.
2. Klicken Sie im Abschnitt **Citrix ShareFile** auf **Remove ShareFile Configuration**.

Use case 15: Configure layer 4 load balancing on the Citrix ADC appliance

December 7, 2021

The layer 4 load balancer (TCP and UDP ports) uses information provided in the networking transport

layer for routing client requests across the server groups.

When a layer 4 connection is established between a client and a server, it has a packet view of traffic exchanged between them. The layer 4 load balancer makes its routing decisions based on the address information extracted from the first few packets in the TCP stream, and doesn't inspect the packet content. Therefore, the layer 4 load balancing is also called as connection-based load balancing.

The layer 4 load balancer monitors the health of a server. Traffic is not routed to the server if it is DOWN.

The layer 4 load balancing is useful for various applications that uses TCP or UDP payloads. Such protocols exchange data as TCP payload and don't have a specific structure to follow.

To configure layer 4 load balancing using the command line interface

At the command prompt, type:

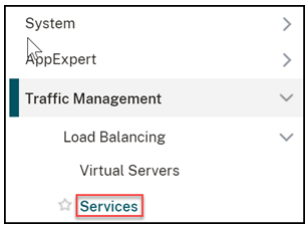
```
add service <name> <serverName> <serviceType> <port>
add lb vserver <name> <serviceType> <ip> <port>
bind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Example:

```
add service TCPservice 192.0.2.3 TCP 1
add lb vserver TCPserver TCP 192.0.2.4 1
bind lb vserver TCPserver TCPservice
<!--NeedCopy-->
```

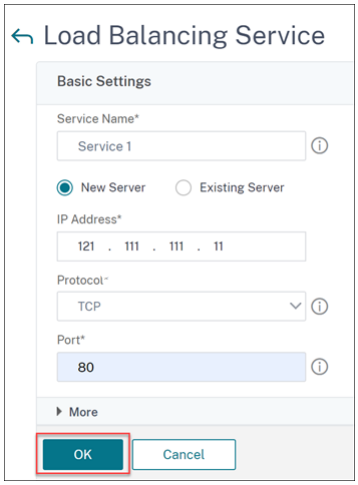
To configure layer 4 load balancing using the GUI

1. Navigate to **Traffic Management > Load Balancing > Services**.



2. Click **Add** to a create a service.
3. Specify the required details in **Service Name** and **IP Address**.

4. Select either **TCP** or **UDP** in **Protocol**.
5. Click **OK**.



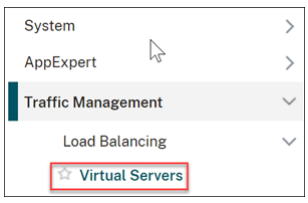
6. Click **Done**.

   A service is created.

   When you create a service using UDP as the transport layer protocol, a ping monitor (built-in monitor) is automatically bound to the service. When you create a service using TCP as the transport layer protocol, a **tcp_default** monitor is automatically bound to the service.

   For the load balancing setup, you can bind your service to a different type of monitor or multiple monitors. For advance monitoring requirements you can use the **tcp-ecv** monitor and configure the request and response messages.

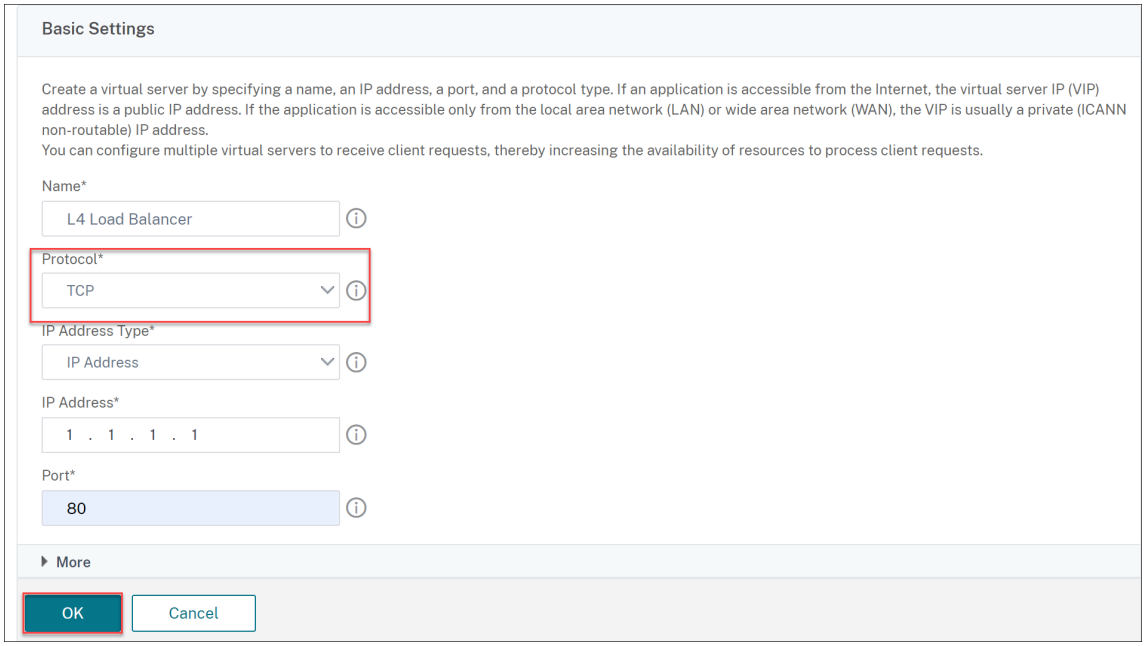
7. Navigate to **Traffic Management > Load Balancing > Virtual Servers**.



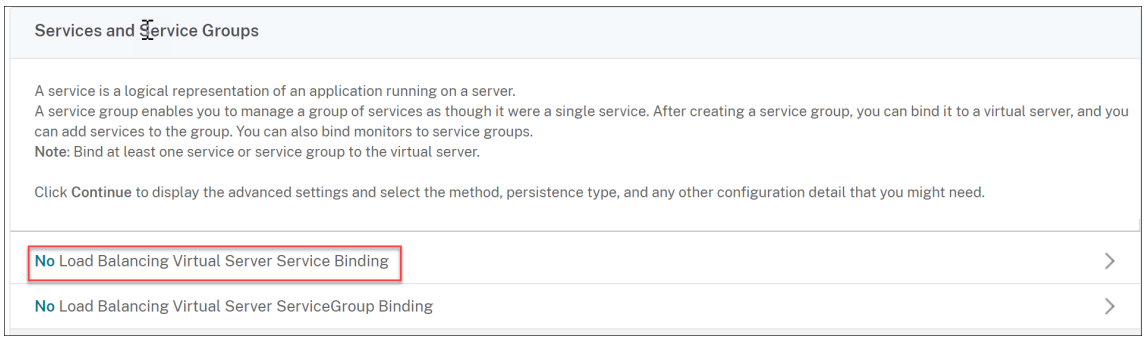
8. Click **Add** to create a new virtual server.

   When the load balancing is configured, you can connect to the load-balanced website, application, or server through the virtual server's IP address or FQDN.

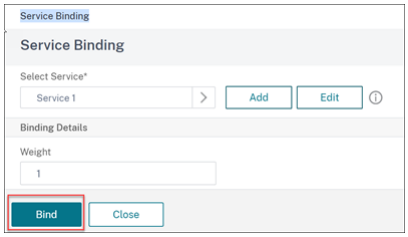
9. Specify the required details in **Name**, **IP Address Type**, and **IP Address**.
10. Select either **TCP** or **UDP** in **Protocol**.
11. Type a port number (0–1023 based on the type of service) in **Port**.
12. Click **OK**.



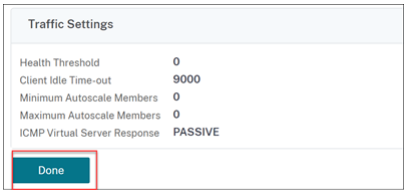
13. Click **No Load Balancing Virtual Server Service Binding** in **Services and Service Groups**.



14. In the **Service Binding** page, select **Click to Select** in **Select Service**.
15. Select the service to be bound and click **Select**.
16. Click **Bind** to bind the service to the virtual server.



17. Click **Continue**.
18. Click **Done**.



The layer 4 load balancing virtual server configuration is completed.

Problembehandlung

October 5, 2021

Wenn der Lastausgleich nach der Konfiguration nicht wie erwartet funktioniert, können Sie einige gängige Tools verwenden, um auf Citrix ADC Ressourcen zuzugreifen und das Problem zu diagnostizieren.

Ressourcen für die Fehlerbehebung bei Lastenausgleich

Verwenden Sie die folgenden Ressourcen, um ein Problem beim Content Switching auf einer Citrix ADC Appliance zu beheben, um optimale Ergebnisse zu erzielen:

- Neueste ns.conf-Datei
- Relevante `newnslog` Dateien
- Ätherische Paketspuren, die auf der Appliance und dem relevanten Client aufgezeichnet werden, wenn möglich
- Die Datei ns.log

Zusätzlich zu den oben genannten Ressourcen beschleunigen die folgenden Tools die Fehlerbehebung:

- Ein Browser-Add-On-Tool, das HTTP-Header anzeigen kann. Dies kann verwendet werden, um Persistenzprobleme zu beheben.
- Die Wireshark-Anwendung, die für die Citrix ADC -Trace-Dateien angepasst ist.

Problembehandlung bei Lastausgleichsproblemen

- **Problem**

Die CPU-Auslastung erreicht 100%, wenn ein Benutzermonitor an einen Dienst gebunden ist, der an einen virtuellen Server gebunden ist, auf dem die MAC-Option -m aktiviert ist.

- **Lösung**

Binden Sie einen Nicht-Benutzermonitor an den Dienst.

- **Problem**

  Ich habe ein Benutzerskript für die Überwachung erstellt, aber es funktioniert nicht.

  Lösung

  Überprüfen Sie die Anzahl der Argumente im Skript. Das Limit ist 512. Ein Skript mit mehr als 512 Argumenten funktioniert möglicherweise nicht ordnungsgemäß. Verwenden Sie das Skript nsumon-debug.pl aus der CLI, um das Skript zu debuggen.

- **Problem**

  Ich sehe viele Monitorsonden, und sie scheinen den Netzwerkverkehr unnötig zu erhöhen. Gibt es eine Möglichkeit, die Monitorsonden auszuschalten?

  Lösung

  Sie können die Monitor-Sondeverbindungen deaktivieren, indem Sie den Monitor deaktivieren oder den Wert des HealthMonitor-Parameters im Befehl set service auf NO einstellen. Mit der Option NO zeigt die Appliance den Dienst jederzeit als UP an.

- **Problem**

  Ich habe Monitore für Dienste eingerichtet, aber Verbindungen werden immer noch an Server weitergeleitet, die DOWN sind.

  Lösung

  Wahrscheinlich müssen Sie die Monitorsondenintervalle verringern. Die Citrix ADC Appliance erkennt den Zustand DOWN erst, wenn der Monitor einen Prüfpunkt sendet.

- **Problem**

  Eine an den Monitor gebundene Metrik ist in den lokalen und benutzerdefinierten Metriktabellen vorhanden.

  Lösung

  Fügen Sie dem Metriknamen das lokale Präfix hinzu, wenn die Metrik aus der lokalen Metriktabelle ausgewählt wird. Wenn die Metrik jedoch aus der benutzerdefinierten Tabelle ausgewählt wird, müssen Sie kein Präfix hinzufügen.

- **Problem**

  Die Monitor-Sonden zu einem Dienst erreichen den Dienst nicht.

  Lösung

  Überprüfen Sie, ob Sie eine Begrenzung für die Anzahl der Verbindungen für einen Dienst festgelegt haben. Wenn ja, nehmen Sie Verbindungen mit Monitor-Sproben von diesem Grenzwert aus, indem Sie den Parameter MonitorSkipMaxClient auf ENABLED setzen.

- **Problem**

  Ich bin in der Lage, die Server zu pingen, aber der Zustand der Dienste wird immer als DOWN angezeigt.

  Lösung

  Überprüfen Sie den Typ der konfigurierten Monitore. Wenn beispielsweise ein Server nicht für SSL konfiguriert ist und Sie einen HTTPS-Monitor verwenden, wird der Status des Dienstes als DOWN markiert. In diesem Fall muss die Verwendung eines TCP-Monitors den Status des Dienstes in UP ändern.

- **Problem**

  Das Festlegen eines Gewichts für Lastmonitore hilft nicht, den Status des Dienstes zu bestimmen.

  Lösung

  Lademonitore können den Status des Dienstes nicht bestimmen. Daher ist das Einstellen eines Gewichts auf den Lastmonitoren unangemessen.

- **Problem**

  Ein Dienst ist nicht stabil.

  Lösung

  Überlegen Sie die Fehlerbehebung der folgenden Komponenten:

  - Stellen Sie sicher, dass ein korrekter Server an den Dienst gebunden ist.
  - Überprüfen Sie den Typ des an den Dienst gebundenen Monitors.
  - Überprüfen Sie die Gründe für die Monitorfehler. Sie können einen Dienst auf der Seite Dienste öffnen und die Details zur Anzahl der Prüfungen, Ausfälle und den letzten Antwortstatus für den Monitor auf der Registerkarte Monitore des Dialogfelds Service konfigurieren überprüfen. Um die Details anzuzeigen, klicken Sie auf den konfigurierten Monitor.
  - Wenn es sich um einen benutzerdefinierten Monitor handelt, binden Sie einen TCP- oder Ping-Monitor an den Dienst und überprüfen Sie den Status des Monitors. Wenn das Problem dadurch behoben wird, liegt ein Problem mit dem benutzerdefinierten Monitor vor und der Monitor erfordert weitere Untersuchungen.
  - Sie können Paketverfolgungen auf der Citrix ADC Appliance aufzeichnen und die Monitorprüfungen und die Serverantwort für weitere Untersuchungen überprüfen.

- **Problem**

  Die virtuelle IP-Adresse (VIP) ist nicht stabil oder ihr Status wird als DOWN angezeigt.

  Lösung

  Überlegen Sie die Fehlerbehebung der folgenden Komponenten:

- Stellen Sie sicher, dass die Lastausgleichsfunktion lizenziert ist.
- Stellen Sie sicher, dass das Feature aktiviert ist.
- Stellen Sie sicher, dass ein geeigneter Dienst an den virtuellen Server gebunden ist.
- Wenn der Status der VIP-Adresse als DOWN angezeigt wird, stellen Sie sicher, dass der Dienst von einem Administrator aktiviert wurde. Ist dies nicht der Fall, muss der Status des Dienstes Out-Of-Service sein. In einem solchen Fall müssen Sie den Dienst aktivieren und überprüfen, ob das Problem behoben ist.
- Überprüfen Sie die Dienste, die an den virtuellen Server gebunden sind, und führen Sie die Schritte zur Fehlerbehebung durch, die für das Problem nicht stabil sind.
- Wenn die VIP-Adresse nicht stabil ist, müssen alle an den virtuellen Server gebundenen Dienste fehlschlagen. Überprüfen Sie daher, ob alle Dienste gleichzeitig fehlschlagen. Wenn dies der Fall ist, liegt ein Netzwerkproblem zwischen der Citrix ADC Appliance und den Servern vor.

- **Problem**

  Die Site hat einen ungleichmäßigen Lastenausgleich.

  Lösung

  Überlegen Sie die Fehlerbehebung der folgenden Komponenten:

  - Überprüfen Sie die auf der Appliance konfigurierte Load Balancing-Methode.
  - Überprüfen Sie, ob die mit den Diensten verknüpften Gewichte wie erwartet sind.
  - Wenn die Load Balancing-Methode eine andere als Round Robin ist, überprüfen Sie die Anzahl der Verbindungen mit dem in der `newnslog` Datei protokollierten Server. Sie können den folgenden Befehl ausführen, um die Nummer in der `newnslog` Datei zu überprüfen:

    ```
    ## nsconmsg -K <newnslog_file> -s ConLb=2 -d oldconmsg
    ```

    Überprüfen Sie die Dienste für den spezifischen virtuellen Server und prüfen Sie die Antwortzeit, Open Etablierte Verbindungen (OE), Anzahl der Anfragen, Persistente Anfragen und die dauerhafte Rate (P), um das Problem weiter zu beheben.
  - Wenn die Load Balancing-Methode Round-Robin ist, überprüfen Sie die dauerhaften Anforderungen wie im vorherigen Schritt erwähnt. Überprüfen Sie außerdem, ob der Dienst nicht stabil ist. Wenn dies nicht der Fall ist, führen Sie die Schritte zur Fehlerbehebung durch, die für das Problem nicht stabil aufgeführt sind.
  - Überprüfen Sie, ob die Persistenz auf der Appliance konfiguriert ist.
  - Überprüfen Sie, ob ein Dienst nicht stabil ist. Wenn ja, führen Sie die Schritte zur Fehlerbehebung durch, die für das Problem nicht stabil aufgeführt sind.

- **Problem**

  Der Dienststatus wird als DOWN angezeigt.

Lösung

Überlegen Sie die Fehlerbehebung der folgenden Komponenten:

- Überprüfen Sie, ob eine SNIP-Adresse konfiguriert ist.
- Stellen Sie sicher, dass entsprechende Monitore an den Dienst gebunden sind.
- Wenn benutzerdefinierte Monitore an den Dienst gebunden sind, binden Sie einen TCP- oder Ping-Monitor an den Dienst und überprüfen Sie den Status des Monitors. Wenn das Problem dadurch behoben wird, liegt ein Problem mit dem benutzerdefinierten Monitor vor und der Monitor erfordert weitere Untersuchungen.
- Überprüfen Sie, ob der Status des Dienstes als DOWN für den Server angezeigt wird, der sich in einem anderen Subnetz befindet. Wenn ja, überprüfen Sie, ob Use Subnet IP (USNIP) das Problem behebt, da dies darauf zurückzuführen sein kann, dass die MIP-Adresse nicht mit dem Server kommunizieren kann.

- **Problem**

  Es liegt ein Problem mit der Antwortzeit vor.

  Lösung

  Überlegen Sie die Fehlerbehebung der folgenden Komponenten:

  - Überprüfen Sie die Server-Antwortzeit aus den Dienststatistiken, indem Sie den folgenden Befehl ausführen:

    ```
    ## nsconmsg -K <newnslog_file> -s ConLb=2 -d oldconmsg
    ```

  - Überprüfen Sie, ob der Dienst nicht stabil ist und der Dienststatus als DOWN Probleme angezeigt wird.

- **Problem**

  Einer der Server erfüllt mehr Anforderungen als die anderen Server mit Lastausgleich.

  Lösung

  Überlegen Sie die Fehlerbehebung der folgenden Komponenten:

  - Überprüfen Sie die Load Balancing-Methode. Verwenden Sie die Roundrobin-Methode, um die Clientanforderung unabhängig von der Last auf den Servern gleichmäßig zu verteilen.
  - Bestimmen Sie, ob die Persistenz für die Lastausgleichskonfiguration aktiviert ist. Wenn Persistenz aktiviert ist, trägt ein bestimmter Server möglicherweise eine schwerere Last, um seine Sitzung aufrechtzuerhalten, insbesondere Wenn die Persistenzsitzungen lang sind.
  - Überprüfen Sie, ob jedem Dienst Gewichtungen zugewiesen sind. Das Zuweisen von richtigen Gewichten hilft bei der richtigen Lastverteilung.

- **Problem**

  Verbindungen zu einem bestimmten Lastausgleichsserver werden angehalten. Beispielsweise könnten alle Verbindungen zu einem Outlook-Server angehalten werden.

  Lösung

  Überlegen Sie die Fehlerbehebung der folgenden Komponenten:

  - Überprüfen Sie die Lastausgleichsmethode. Wenn es sich um Round Robin handelt, sollten Sie die Methode in die geringste Verbindung ändern.
  - Ziehen Sie in Betracht, die Zeitüberschreitung für den Monitor zu reduzieren. Ein kürzerer Timeout-Zeitraum hilft dabei, einen Dienst früher als DOWN zu markieren, was dazu beitragen würde, den Datenverkehr auf den funktionsfähigen Server zu lenken.
  - Wenn die Verbindungen über einen längeren Zeitraum ins Stocken geraten sind, kann sich eine Überspannungswarteschlange aufbauen. Erwägen Sie, die Überspannungswarteschlange zu leeren, um einen plötzlichen Anstieg der Belastung des Servers zu vermeiden.
  - Wenn die Server auf ihrer maximalen Ebene arbeiten, sollten Sie erwägen, einen neuen Server für eine bessere Leistung hinzuzufügen.

- **Problem**

  Ein Großteil der Verbindungen wird an einen bestimmten Server weitergeleitet, selbst wenn die Methode der geringsten Verbindungen für den Lastenausgleich konfiguriert ist.

  Lösung

  Bestimmen Sie, ob die Persistenz konfiguriert ist und vom Typ Quell-IP ist. Wenn die Quell-IP-Persistenz selbst mit der Methode der geringsten Verbindungen konfiguriert ist, gehen die Anforderungen an einen bestimmten Server. Die IP-Adresse des Servers ist für die Verwaltung der Sitzungsinformationen erforderlich. Erwägen Sie, HTTP-Cookies basierte Persistenz zu verwenden.

- **Tipps zur Fehlerbehebung**
  Bei anderen Problemen sollten Sie die folgenden Tipps beachten, um ein oben nicht aufgeführtes Problem zu beheben:

  - Wenn mehrere Lastmonitore an einen Dienst gebunden sind, ist die Last auf dem Dienst die Summe aller Werte auf den Lastmonitoren, die an ihn gebunden sind. Damit der Lastenausgleich ordnungsgemäß funktioniert, müssen Sie denselben Satz von Monitoren an alle Dienste binden.
  - Wenn Sie einen an den Dienst gebundenen Lastmonitor deaktivieren und der Dienst an einen virtuellen Server gebunden ist, verwendet der virtuelle Server die Roundrobin-Methode für den Lastenausgleich.

- Wenn Sie einen Dienst an einen virtuellen Server binden, auf dem die Lastausgleichsmethode CUSTOMLOAD lautet und der Dienststatus UP lautet, verwendet der virtuelle Server die erste Roundrobin-Methode für den Lastenausgleich. Es befindet sich weiterhin im Round-Robin, wenn der Dienst keine benutzerdefinierten Lastmonitore hat oder wenn der Status mindestens eines der benutzerdefinierten Lastmonitore nicht UP ist.
- Alle Dienste, die an einen virtuellen Server gebunden sind, auf dem die Lastausgleichsmethode CUSTOMLOAD lautet, müssen die Dienste über Lastüberwachungen verfügen, die an sie gebunden sind.
- Die CUSTOMLOAD Load Balancing-Methode folgt auch dem Start-Rund-Robin.
- Wenn Sie eine metrikbasierte Bindung deaktivieren und dies die letzte aktive Metrik ist, verwendet der spezifische virtuelle Server die Roundrobin-Methode für den Lastenausgleich. Eine Metrik wird deaktiviert, indem der Metrikschwellenwert auf Null gesetzt wird.
- Wenn eine an einen Monitor gebundene Metrik den Schwellenwert überschreitet, wird dieser bestimmte Dienst für den Lastausgleich nicht berücksichtigt. Wenn alle Dienste den Schwellenwert erreicht haben, verwendet der virtuelle Server die Roundrobin-Methode für den Lastenausgleich und eine Fehlermeldung 5xx - Server busy error wird angezeigt.
- Maximal 10 Metriken aus einer benutzerdefinierten Tabelle können an den Monitor gebunden werden.
- Die OIDs müssen skalare Variablen sein.
- Für einen erfolgreichen Lastausgleich muss das Intervall so niedrig wie möglich sein. Wenn das Intervall hoch ist, erhöht sich der Zeitraum für das Abrufen des Lastwerts. Infolgedessen erfolgt der Lastausgleich unter Verwendung falscher Werte.
- Ein Benutzer kann die lokale Tabelle nicht ändern.

Häufig gestellte Fragen zum Lastenausgleich

October 5, 2021

Welche verschiedenen Lastausgleichsrichtlinien kann ich auf der Citrix ADC Appliance erstellen?

Sie können die folgenden Typen von Lastausgleichsrichtlinien auf der Citrix ADC Appliance erstellen:

- Geringste Verbindungen
- Runde Robin
- Geringste Reaktionszeit
- Geringste Bandbreite
- Am wenigsten Pakete
- URL-Hashing

- Domänennamen-Hashing
- Quell-IP-Adress-Hashing
- Ziel-IP-Adress-Hashing
- Quell-IP - Ziel-IP-Hashing
- Zeichen
- LRTM

Kann ich die Sicherheit der Webfarm erreichen, indem ich den Lastausgleich mit der Citrix ADC Appliance implementiere?

Ja. Sie können die Sicherheit der Webfarm erreichen, indem Sie den Lastausgleich mit der Citrix ADC Appliance implementieren. Mit der Citrix ADC Appliance können Sie die folgenden Optionen der Lastausgleichsfunktion implementieren:

- Verstecken von IP-Adressen: Ermöglicht die Installation der tatsächlichen Server, die sich aus Sicherheitsgründen und zur Erhaltung der IP-Adresse im privaten IP-Adressraum befinden. Dieser Prozess ist für den Endbenutzer transparent, da die Citrix ADC Appliance Anforderungen im Auftrag des Servers akzeptiert. Im Adressenausblendmodus isoliert die Appliance die beiden Netzwerke vollständig. Daher kann ein Client über eine andere VIP auf der Appliance für diesen Dienst auf einen Dienst zugreifen, der im privaten Subnetz ausgeführt wird, z. B. FTP oder einen Telnet-Server.
- Portzuordnung: Ermöglicht, dass die tatsächlichen TCP-Dienste aus Sicherheitsgründen auf nicht standardmäßigen Ports gehostet werden. Dieser Vorgang ist für den Endbenutzer transparent, da die Citrix ADC Appliance Anforderungen im Namen des Servers an die standardmäßige angekündigte IP-Adresse und Portnummer annimmt.

Welche Geräte kann ich zum Lastenausgleich mit einer Citrix ADC Appliance verwenden?

Sie können die folgenden Geräte mit einer Citrix ADC Appliance ausgleichen:

- Serverfarmen
- Caches oder Reverse-Proxys
- Firewall-Geräte
- Intrusion Detection Systeme
- SSL-Abladungsgeräte
- Kompressionsgeräte
- Content Inspection Server

Warum implementiere ich die Load Balancing-Funktion für die Website?

Sie können die Funktion Lastenausgleich für die Website implementieren, um folgende Vorteile zu nutzen:

- Reduzieren Sie die Reaktionszeit: Wenn Sie die Load Balancing-Funktion für die Website implementieren, ist einer der Hauptvorteile, auf die Sie sich in der Ladezeit freuen können. Wenn zwei oder mehr Server die Last des Webdatenverkehrs gemeinsam nutzen, führt jeder Server weniger Datenverkehr aus als ein einzelner Server allein. Dies bedeutet, dass mehr Ressourcen verfügbar sind, um die Client-Anforderungen zu erfüllen. Dies führt zu einer schnelleren Website.
- Redundanz: Durch das Implementieren der Load Balancing-Funktion wird ein wenig Redundanz geboten. Wenn die Website beispielsweise über drei Server ausgeglichen ist und einer von ihnen überhaupt nicht reagiert, können die anderen beiden weiterhin laufen und die Websitebesucher bemerken keine Ausfallzeiten. Jede Load Balancing-Lösung sendet sofort den Datenverkehr an den Back-End-Server, der nicht verfügbar ist.

Warum muss ich die Mac Based Forwarding (MBF) Option für Link Load Balancing (LLB) deaktivieren?

- Wenn Sie die MBF-Option aktivieren, berücksichtigt die Citrix ADC Appliance, dass der eingehende Datenverkehr vom Client und der ausgehende Datenverkehr zum selben Client über denselben Upstream-Router fließt. Die LLB-Funktion erfordert jedoch den besten Pfad, der für den Rückverkehr gewählt werden muss.
- Das Aktivieren der MBF-Option unterbricht diesen Topologieentwurf, indem der ausgehende Datenverkehr über den Router gesendet wird, der den eingehenden Clientdatenverkehr weitergeleitet hat.

Netzwerke

October 5, 2021

Die folgenden Themen enthalten eine konzeptionelle Referenz und Anweisungen zum Konfigurieren der verschiedenen Netzwerkkomponenten auf der Citrix ADC Appliance.

IP-Adressierung	Erfahren Sie mehr über die verschiedenen Typen von IP-Adressen im Citrix ADC Besitz und wie Sie diese erstellen, anpassen und entfernen.

Schnittstellen	Konfigurieren Sie einige der grundlegenden Netzwerkkonfigurationen, die für den Einstieg durchgeführt werden müssen.
Zugriffssteuerungslisten (ACLs)	Konfigurieren Sie die verschiedenen Typen von Zugriffssteuerungslisten und wie Sie diese erstellen, anpassen und entfernen.
IP-Routing	Lernen und konfigurieren Sie die Routing-Funktionalität der Citrix ADC Appliance, sowohl statisch als auch dynamisch.
Internetprotokoll Version 6 (IPv6)	Erfahren Sie, wie die Citrix ADC Appliance IPv6 unterstützt.
Traffic-Domänen	Lernen und konfigurieren Sie Verkehrsdomänen, um den Netzwerkverkehr für verschiedene Anwendungen zu segmentieren.
VXLAN	Lernen und konfigurieren Sie VxLANs, um die Skalierbarkeitsanforderungen in Ihrem Rechenzentrum zu erfüllen.

IP-Adressierung

October 5, 2021

Bevor Sie die Citrix ADC Appliance konfigurieren können, müssen Sie die NSIP-Adresse zuweisen, die auch als Verwaltungs-IP-Adresse bezeichnet wird. Sie können auch andere IP-Adressen von Citrix ADC erstellen, um Server abstrahieren und Verbindungen mit den Servern herzustellen. Bei dieser Konfiguration dient die Appliance als Proxy für die abstrahierten Server. Sie können Proxys für Verbindungen auch über Netzwerkadressübersetzungen (INAT und RNAT) erzielen. Beim Proxyverfahren von Verbindungen kann sich die Appliance entweder als Bridging-Gerät (Layer 2) oder als Paketweiterleitungsgerät (Layer 3) verhalten. Um die Paketweiterleitung effizienter zu gestalten, können Sie statische ARP-Einträge konfigurieren. Für IPv6 können Sie die Neighbor Discovery (ND) konfigurieren.

Konfigurieren von IP-Adressen im Besitz von Citrix ADC

October 5, 2021

Die IP-Adressen im Besitz von Citrix ADC — NSIP-Adresse, virtuelle IP-Adressen (VIPs), Subnetz-IP-Adressen (SNIPs) und Global Server Load Balancing Site-IP-Adressen (GSLBIPs), existieren nur auf der Citrix ADC Appliance. Das NSIP identifiziert den Citrix ADC in Ihrem Netzwerk eindeutig und bietet Zugriff auf die Appliance. Ein VIP ist eine öffentliche IP-Adresse, an die ein Client Anfragen sendet. Citrix ADC beendet die Clientverbindung am VIP und initiiert eine Verbindung mit einem Server. Diese neue Verbindung verwendet eine SNIP oder eine MIP als Quell-IP-Adresse für Pakete, die an den Server weitergeleitet werden. Wenn Sie mehrere Rechenzentren haben, die geografisch verteilt sind, kann jedes Rechenzentrum durch eine eindeutige GSLBIP identifiziert werden. Sie können einige Citrix ADC-eigene IP-Adressen konfigurieren, um Zugriff für Verwaltungsanwendungen bereitzustellen.

Konfigurieren der NSIP-Adresse

October 5, 2021

Die NSIP-Adresse ist die IP-Adresse, mit der Sie zu Verwaltungszwecken auf die Citrix ADC Appliance zugreifen. Die Appliance kann nur über einen NSIP verfügen, der auch als Verwaltungs-IP-Adresse bezeichnet wird. Sie müssen diese IP-Adresse hinzufügen, wenn Sie Citrix ADC zum ersten Mal konfigurieren. Eine NSIP-Adresse kann nicht entfernt werden. Aus Sicherheitsgründen sollte der NSIP eine nicht routbare IP-Adresse im LAN Ihrer Organisation sein.

Wenn Sie diese Adresse ändern, müssen Sie die Citrix ADC Appliance neu starten. Wenn sich die Subnetzadresse der neuen NSIP-Adresse von der vorherigen unterscheidet, müssen Sie eine Standardroute für dieses Subnetz hinzufügen, damit die neue NSIP-Adresse von anderen Netzwerken im LAN erreichbar ist.

> **Wichtig**
>
> Die Konfiguration der NSIP-Adresse ist obligatorisch.

Das Ändern der NSIP-Adresse einer Citrix ADC Appliance besteht aus folgenden Aufgaben:

- Ändern Sie die NSIP-Adresse.
- Fügen Sie eine Standardroute für die Subnetzadresse der NSIP-Adresse hinzu, falls keine vorhanden ist.
- Speichern Sie die Konfiguration.
- Starten Sie die Appliance neu.

Befehlszeilenprozeduren

So ändern Sie die NSIP-Adresse mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **set ns config -IPAddress** <ip_addr> **-netmask** <netmask>
- **show ns config**

So fügen Sie eine Standardroute mit der CLI hinzu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add route 0 0** <gateway IP address>
- **show route**

So speichern Sie die Konfiguration mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **save config**

So starten Sie die Citrix ADC Appliance mit der CLI neu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **reboot**

GUI-Prozeduren

So konfigurieren Sie die NSIP-Adresse mit der GUI:

1. Klicken Sie auf das Zahnradsymbol in der oberen rechten Ecke der **Konfigurationsseite** .
2. Klicken Sie auf den Bereich **NSIP-Adress3**.
3. Legen Sie auf der Seite **NSIP-Adresse** die folgenden Parameter fest, und klicken Sie dann auf **Fertig** :
    - NSIP-Adresse
    - Netzmaske

So fügen Sie eine Standardroute mit der GUI hinzu:

Navigieren Sie zu **System** > **Netzwerk** > **Routen**, fügen Sie auf der Registerkarte **Basic** eine Standardroute mit den folgenden Parametereinstellungen hinzu, und klicken Sie dann auf **Erstellen**.

- Netzwerk (auf Null gesetzt)
- Netzmaske (auf Null gesetzt)
- Gateway (IP-Adresse des Gateways)

So starten Sie den Citrix ADC mit der GUI neu:

1. Klicken Sie auf der Registerkarte **Systeminformationen** des Knotens **System** auf **Neustart** .
2. Wenn Sie zum Neustart aufgefordert werden, wählen Sie **Konfiguration speichern** aus, um sicherzustellen, dass keine Konfigurationen verloren gehen.

Beispielkonfiguration

Im folgenden Beispiel wird die NSIP-Adresse einer Citrix ADC Appliance in 192.0.2.90 geändert, die eine andere Subnetzadresse (192.0.2.0/24) als die vorherige NSIP-Adresse aufweist. Daher wird eine Standardroute für dieses Subnetz hinzugefügt, so dass die neue NSIP-Adresse von anderen Netzwerken erreichbar ist.

```
> set nsconfig -ipAddress 192.0.2.90 -netmask 255.255.255.0

 Warning: The configuration must be saved and the system rebooted for
    these settings to take effect
> add route 0 0 192.0.2.1

 Warning: The configuration must be saved and the system rebooted for
    these settings to take effect
> save config

 Done
> reboot
```

Konfigurieren und Verwalten von Virtual IP (VIP) -Adressen

October 5, 2021

Die Konfiguration einer virtuellen Server-IP-Adresse (VIP) ist während der Erstkonfiguration des Citrix ADC nicht erforderlich. Wenn Sie den Lastenausgleich konfigurieren, weisen Sie virtuellen Servern VIP-Adressen zu.

Weitere Informationen zum Konfigurieren eines Load Balancing-Setups finden Sie unter Load Balancing.

In einigen Situationen müssen Sie VIP-Attribute anpassen oder eine VIP-Adresse aktivieren oder deaktivieren. Eine VIP-Adresse ist normalerweise mit einem virtuellen Server verknüpft, und einige der VIP-Attribute werden an die Anforderungen des virtuellen Servers angepasst. Sie können denselben virtuellen Server auf mehreren Citrix ADC Appliances in derselben Broadcastdomäne hosten, indem Sie ARP- und ICMP-Attribute verwenden. Nachdem Sie einen VIP (oder eine beliebige IP-Adresse)

hinzugefügt haben, sendet die Appliance ARP-Anforderungen und reagiert dann darauf. VIPs sind die einzigen IP-Adressen im Besitz von Citrix ADC, die deaktiviert werden können. Wenn eine VIP-Adresse deaktiviert ist, geht der virtuelle Server, der sie verwendet, aus und reagiert nicht auf ARP-, ICMP- oder L4-Dienstanforderungen. Alternativ zum Erstellen von VIP-Adressen einzeln können Sie einen aufeinanderfolgenden Bereich von VIP-Adressen angeben.

So erstellen Sie eine VIP-Adresse mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add ns ip <IPAddress> <netmask> -type <type>
- ns ip anzeigen <IPAddress>

Beispiel:

```
1 > add ns ip 10.102.29.59 255.255.255.0 -type VIP
2  Done
3 <!--NeedCopy-->
```

So erstellen Sie einen Bereich von VIP-Adressen mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add ns ip <IPAddress> <netmask> -type <type>
- ns ip anzeigen <IPAddress>

Beispiel:

```
1 > add ns ip 10.102.29.[60-64] 255.255.255.0 -type VIP
2 ip "10.102.29.60" added
3 ip "10.102.29.61" added
4 ip "10.102.29.62" added
5 ip "10.102.29.63" added
6 ip "10.102.29.64" added
7  Done
8 <!--NeedCopy-->
```

So aktivieren oder deaktivieren Sie eine IPv4-VIP-Adresse mit der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehlssätze ein, um einen VIP zu aktivieren oder zu deaktivieren, und überprüfen Sie die Konfiguration:

- enable ns ip <IPAddress>
- ns ip anzeigen <IPAddress>
- disable ns ip <IPAddress>

- ns ip anzeigen <IPAddress>

Beispiel:

```
> enable ns ip 10.102.29.79
 Done
> show ns ip 10.102.29.79

        IP: 10.102.29.79
        Netmask: 255.255.255.255
        Type: VIP
        state: Enabled
        arp: Enabled
        icmp: Enabled
        vserver: Enabled
        management access: Disabled
          telnet: Disabled
          ftp: Disabled
          ssh: Disabled
          gui: Disabled
          snmp: Disabled
        Restrict access: Disabled
        dynamic routing: Disabled
        hostroute: Disabled
 Done
> disable ns ip 10.102.29.79
 Done
> show ns ip 10.102.29.79

        IP: 10.102.29.79
        Netmask: 255.255.255.255
        Type: VIP
        state: Disabled
        arp: Enabled
        icmp: Enabled
        vserver: Enabled
        management access: Disabled
          telnet: Disabled
          ftp: Disabled
          ssh: Disabled
          gui: Disabled
          snmp: Disabled
        Restrict access: Disabled
        dynamic routing: Disabled
```



```
41         hostroute: Disabled
42
43  Done
44 <!--NeedCopy-->
```

So konfigurieren Sie eine VIP-Adresse mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv4s**, und fügen Sie eine neue IP-Adresse hinzu, oder bearbeiten Sie eine vorhandene Adresse.

So erstellen Sie mit der GUI einen Bereich von VIP-Adressen:

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv4s**.
2. Wählen Sie in der Liste **Aktion** die Option **Bereich hinzufügen**aus.

So aktivieren oder deaktivieren Sie eine VIP-Adresse mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv4s**.
2. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie eine VIP-Adresse aus.
   - Halten Sie die **Strg-Taste gedrückt**, und wählen Sie mehrere Serveradresseneinträge aus.
   - Halten Sie die **Umschalttaste gedrückt**, und wählen Sie einen Bereich von Serveradresseinträgen aus.
   - Markieren Sie alle Adressen, indem Sie das Kontrollkästchen auf der linken Seite der Kopfzeile aktivieren.
3. Wählen Sie in der Liste **Aktion** die Option **Deaktivieren** oder **Aktivieren** aus.

Erkennen einer Citrix ADC Appliance in einem UDP-Load Balancing-Setup über TTL-Updates

Die folgende Tabelle zeigt, wie eine Citrix ADC Appliance den TTL-Wert empfangener Pakete in verschiedenen Funktionalitäten verarbeitet.

Funktionalität	TTL-Wert
Virtueller Server	TTL wird auf 255 festgelegt, wenn die Anforderung an die Backend-Server weitergeleitet wird. TTL wird um 1 verringert, wenn die Antwort an den Client weitergeleitet wird.
L2-Modus	TTL wird nicht geändert.
L3-Modus	TTL ist auf 255 festgelegt.

Funktionalität	TTL-Wert
INAT	TTL wird auf 255 gesetzt, wenn die Anforderung an den Backend-Server weitergeleitet wird. TTL wird um 1 verringert, wenn die Antwort an den Client weitergeleitet wird.

Bei einigen Unternehmen/Szenarien, die eine Überwachungsanwendung ausführen, muss die Citrix ADC Appliance eines Lastausgleichs-Setups als einer der Hop in einer Traceroute erkannt werden. Eine Citrix ADC Appliance eines Lastausgleichs-Setups wird in einer Traceroute nicht erkannt, da die Appliance standardmäßig den TTL-Wert auf 255 setzt, anstatt ihn zu verringern, wenn die Anforderung an einen Backend-Server weitergeleitet wird.

Um diese Anforderung zu erfüllen, kann **Decrement TTL** Parameter einer VIP-Adresse verwendet werden. Dieser Parameter gilt für alle virtuellen UDP-Server, die diesen VIP verwenden.

Wenn Sie den Parameter **Decrement TTL** eines VIP aktivieren, verringert die Citrix ADC Appliance den TTL-Wert um 1, anstatt ihn beim Weiterleiten von Anforderungen auf 255 zu setzen, die auf den virtuellen UDP-Servern empfangen werden, die diesen VIP verwenden.

Bei der Überwachung von Anwendungen mit Traceroute-Daten kann nun das Vorhandensein einer Citrix ADC Appliance eines UDP-Load Balancing-Setups erkennen.

Bevor Sie beginnen

Bevor Sie mit der Konfiguration einer Citrix ADC Appliance beginnen, die in einer Traceroute eines Lastausgleichs-Setups erkannt wird, beachten Sie die folgenden Punkte:

- Der TTL-Parameter Decrement wird nur für virtuelle Server mit UDP-Lastenausgleich unterstützt.
- Der Parameter Decrement TTL wird sowohl für IPv4 VIP als auch IPv6 VIP (VIP6) -Adressen unterstützt.
- Der Parameter Decrement TTL wird sowohl für eigenständige Citrix ADC Appliances als auch für Hochverfügbarkeits- (HA) und Cluster-Setups unterstützt.

Konfigurationsschritte

Die Konfiguration einer Citrix ADC Appliance, die in einer Traceroute eines UDP-Lastausgleichs-Setups erkannt wird, besteht aus folgenden Aufgaben:

- Erstellen einer UDP-Lastausgleichskonfiguration
- Aktivieren Sie den Parameter Decrement TTL für die VIP-Adresse

CLI-Prozeduren

So aktivieren Sie die Option TTL für eine VIP-Adresse mit der CLI:

- Geben Sie an der Eingabeaufforderung Folgendes ein, um die Option TTL für eine VIP-Adresse zu aktivieren, während Sie die VIP-Adresse hinzufügen:
  - **add ns ip** <ip> <mask> -**type VIP** -**decrementTTL ENABLED**
  - **show ns ip** <VIP address>
- Geben Sie an der Eingabeaufforderung Folgendes ein, um die Option TTL für eine vorhandene VIP-Adresse zu aktivieren:
  - **set ns ip** <ip> <mask> -**decrementTTL ENABLED**
  - **show ns ip** <VIP address>

So aktivieren Sie die Option TTL für eine VIP6-Adresse mit der CLI:

- Geben Sie an der Eingabeaufforderung Folgendes ein, um die Option TTL für eine VIP6-Adresse zu aktivieren, während Sie die VIP6-Adresse hinzufügen:
  - **add ns ip6** <IP6/prefix> <mask> -**type VIP** -**decrementTTL ENABLED**
  - **show ns ip6** <VIP6/prefix>
- Geben Sie an der Eingabeaufforderung Folgendes ein, um die Option TTL für eine vorhandene VIP6-Adresse zu aktivieren:
  - **set ns ip6** <ip6/prefix> <mask> -**decrementTTL ENABLED**
  - **show ns ip6** <VIP6 address>

```
1     > add ns ip 203.0.113.30 -type VIP -decrementTTL ENABLED
2      Done
3
4     > add ns ip6  2001:DB8:5001::30 -type VIP -decrementTTL ENABLED
5      Done
6 <!--NeedCopy-->
```

GUI-Prozeduren

So aktivieren Sie die Option TTL für eine VIP-Adresse mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv4s**, und aktivieren Sie den Parameter **Decrement TTL**, während Sie eine neue VIP-Adresse hinzufügen oder eine vorhandene Adresse bearbeiten.

So aktivieren Sie die Option TTL für eine VIP6-Adresse mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv6s**, und aktivieren Sie den Parameter **Decrement TTL**, während Sie eine neue VIP6-Adresse hinzufügen oder eine vorhandene Adresse bearbeiten.

Konfigurieren der ARP-Antwortunterdrückung für virtuelle IP-Adressen (VIPs)

October 5, 2021

Sie können die Citrix ADC Appliance so konfigurieren, dass sie auf ARP-Anforderungen für eine virtuelle IP-Adresse (VIP) basierend auf dem Status der virtuellen Server reagiert, die diesem VIP zugeordnet sind.

Wenn beispielsweise virtuelle Server V1 vom Typ HTTP und V2 vom Typ HTTPs die VIP-Adresse 10.102.29.45 auf einer Citrix ADC Appliance freigeben, können Sie die Appliance so konfigurieren, dass sie nicht auf ARP-Anforderungen für VIP 10.102.29.45 reagiert, wenn sich sowohl V1 als auch V2 im Status DOWN befinden.

Die folgenden drei Optionen stehen zur Konfiguration der ARP-Response-Unterdrückung für eine virtuelle IP-Adresse zur Verfügung.

- **KEINE**. Die Citrix ADC Appliance reagiert auf jede ARP-Anforderung für die VIP-Adresse, unabhängig vom Status der virtuellen Server, die der Adresse zugeordnet sind.
- **ONE VSERVER**. Die Citrix ADC Appliance reagiert auf jede ARP-Anforderung für die VIP-Adresse, wenn sich mindestens einer der zugeordneten virtuellen Server im Status UP befindet.
- **ALL VSERVER**. Die Citrix ADC Appliance reagiert auf jede ARP-Anforderung für die VIP-Adresse, wenn sich alle zugeordneten virtuellen Server im UP-Status befinden.

Die folgende Tabelle zeigt das Beispielverhalten der Citrix ADC Appliance für eine VIP, die mit zwei virtuellen Servern konfiguriert ist:

Zugehörige virtuelle Server für einen VIP	STATE 1	STATE 2	STATE 3	STATE 4
NONE				
V1	BEREIT	BEREIT	INAKTIV	INAKTIV
V2	BEREIT	INAKTIV	BEREIT	INAKTIV
Beantworten Sie eine ARP-Anfrage für diesen VIP?	Ja	Ja	Ja	Ja
ONE VSERVER				
V1	BEREIT	BEREIT	INAKTIV	INAKTIV
V2	BEREIT	INAKTIV	BEREIT	INAKTIV

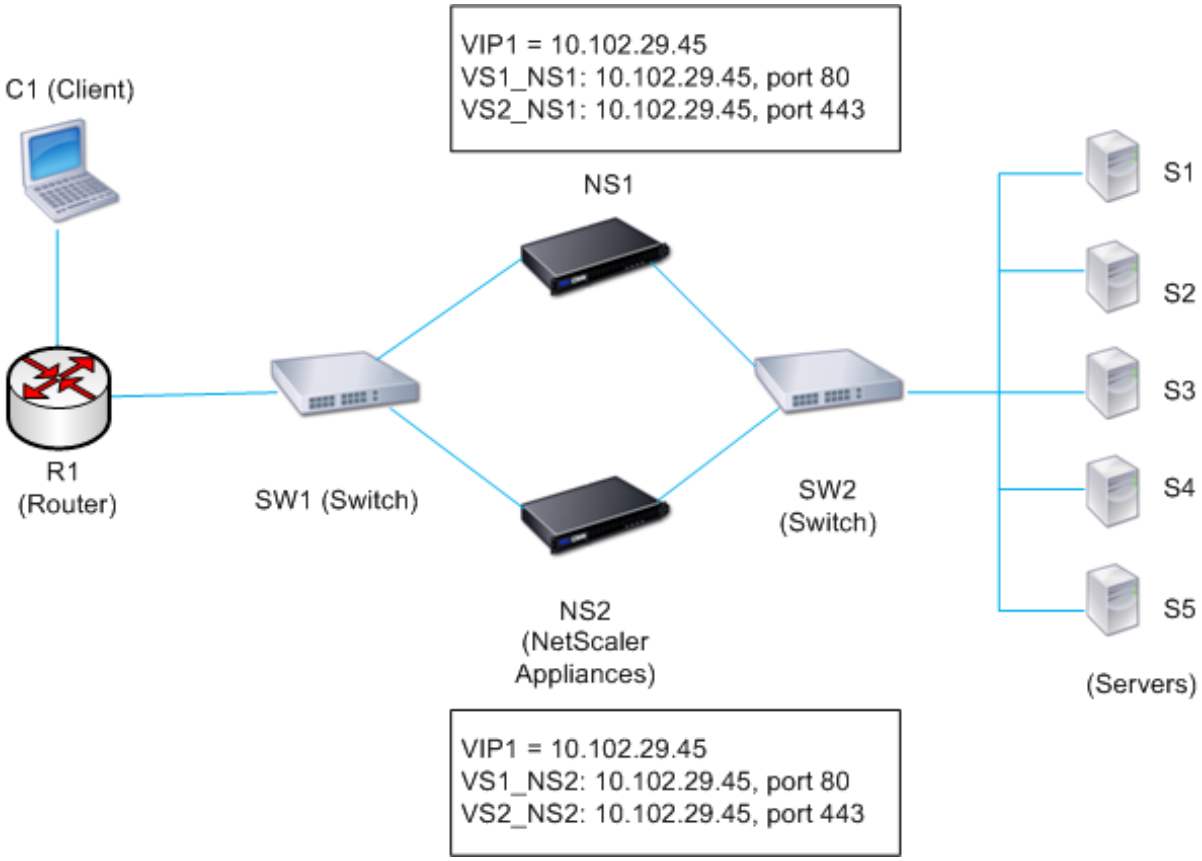
Zugehörige virtuelle Server für einen VIP	STATE 1	STATE 2	STATE 3	STATE 4
Beantworten Sie eine ARP-Anfrage für diesen VIP?	Ja	Ja	Ja	Nein
ALL VSERVER				
V1	BEREIT	BEREIT	INAKTIV	INAKTIV
V2	BEREIT	INAKTIV	BEREIT	INAKTIV
Beantworten Sie eine ARP-Anfrage für diesen VIP?	Ja	Nein	Nein	Nein

Betrachten Sie ein Beispiel, in dem Sie die Leistung von zwei virtuellen Servern, V1 und V2, testen möchten, die dieselbe VIP-Adresse haben, aber unterschiedliche Typen aufweisen und jeweils auf Citrix ADC Appliances NS1 und NS2 konfiguriert sind. Rufen wir die gemeinsame VIP-Adresse *VIP1*an.

V1-Lastverteilung der Server S1, S2 und S3. V2 Lastverteilung Server S4 und S5.

Auf NS1 und NS2 wird für VIP1 der ARP-Unterdrückungsparameter auf ALL_VSERVER festgelegt. Wenn Sie die Leistung von V1 und V2 auf NS1 testen möchten, müssen Sie V1 und V2 auf NS2 manuell deaktivieren, damit NS2 auf keine ARP-Anforderung für VIP1 reagiert.

Abbildung 1.



Der Ausführungsablauf ist wie folgt:

1. Client C1 sendet eine Anforderung an V1. Die Anforderung erreicht R1.
2. R1 hat keinen APR-Eintrag für die IP-Adresse (VIP1) von V1, daher sendet R1 eine ARP-Anfrage für VIP1.
3. NS1 antwortet mit Quell-MAC-Adresse MAC1 und Quell-IP-Adresse VIP1. NS2 antwortet nicht auf die ARP-Anfrage.
4. SW1 lernt den Port für VIP1 aus der ARP-Antwort und aktualisiert seine Bridge-Tabelle, und R1 aktualisiert den ARP-Eintrag mit MAC1 und VIP1.
5. R1 leitet das Paket an die Adresse VIP1 auf NS1 weiter.
6. Der Lastausgleichsalgorithmus von NS1 wählt Server S2 aus, und NS1 öffnet eine Verbindung zwischen einer seiner SNIP-Adressen und S2. Wenn S2 eine Antwort an den Client sendet, kehrt die Antwort im gleichen Pfad zurück.
7. Jetzt möchten Sie die Leistung von V1 und V2 auf NS2 testen, so dass Sie V1 und V2 auf NS2 aktivieren und sie auf NS1 deaktivieren. NS2 sendet jetzt eine ARP-Nachricht für VIP1. In der Nachricht ist MAC2 die Quell-MAC-Adresse und VIP1 die Quell-IP-Adresse.
8. SW1 lernt die Portnummer für den Erreichen von MAC2 aus dem ARP-Broadcast und aktualisiert die Bridge-Tabelle, um nachfolgende Clientanforderungen für VIP1 an NS2 zu senden. R1 aktualisiert seine ARP-Tabelle.
9. Nehmen wir nun an, der ARP-Eintrag für VIP1 Timeout in der ARP-Tabelle von R1, und Client

C1 sendet eine Anforderung für V1. Da R1 keinen APR-Eintrag für VIP1 hat, sendet es eine ARP-Anforderung für VIP1.

10. NS2 antwortet mit einer Quell-MAC-Adresse und VIP1 als Quell-IP-Adresse. NS1 antwortet nicht auf die ARP-Anfrage.

So konfigurieren Sie die Unterdrückung der ARP-Antwortvariablen mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **set ns ip** -**arpResponse** <arpResponse>]
- **sh ns ip** <IPAddress>

Beispiel:

```
1 > set ns ip 10.102.29.96 -arpResponse ALL_VSERVERS
2  Done
3 <!--NeedCopy-->
```

So konfigurieren Sie die ARP-Antwortunterdrückung mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv4s**.
2. Öffnen Sie einen IP-Adresseintrag, und wählen Sie den Typ der ARP-Antwort aus.

Konfigurieren von Subnetz-IP-Adressen (SNIPs)

October 5, 2021

Eine Subnetz-IP-Adresse (SNIP) ist eine IP-Adresse im Besitz von Citrix ADC, die vom Citrix ADC zur Kommunikation mit den Servern verwendet wird.

Citrix ADC verwendet die Subnetz-IP-Adresse als Quell-IP-Adresse als Proxy für Clientverbindungen zu Servern. Es verwendet auch die Subnetz-IP-Adresse, wenn eigene Pakete generiert werden, z. B. Pakete, die sich auf dynamische Routingprotokolle beziehen, oder um Monitorprüfungen zu senden, um den Zustand der Server zu überprüfen. Je nach Netzwerktopologie müssen Sie möglicherweise einen oder mehrere SNIPs für verschiedene Szenarien konfigurieren.

Um eine SNIP-Adresse auf einem Citrix ADC zu konfigurieren, fügen Sie die SNIP-Adresse hinzu und aktivieren Sie den globalen Use Subnet IP (USNIP) -Modus. Alternativ zum Erstellen von SNIPs einzeln können Sie einen aufeinanderfolgenden Bereich von SNIPs angeben.

So konfigurieren Sie eine SNIP-Adresse mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add ns ip <IPAddress> <netmask> -type SNIP

- ns ip anzeigen <IPAddress>

Beispiel:

```
> add ns ip 10.102.29.203 255.255.255.0 -type SNIP
 Done
<!--NeedCopy-->
```

So erstellen Sie einen Bereich von SNIP-Adressen mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add ns ip <IPAddress> <netmask> -type SNIP
- ns ip anzeigen <IPAddress>

Beispiel:

```
> add ns ip 10.102.29.[205-209] 255.255.255.0 -type SNIP
ip ”10.102.29.205” added
ip ”10.102.29.206” added
ip ”10.102.29.207” added
ip ”10.102.29.208” added
ip ”10.102.29.209” added
 Done
<!--NeedCopy-->
```

So aktivieren oder deaktivieren Sie den USNIP-Modus mit der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- enable ns modeUSNIP
- disable ns modeUSNIP

So konfigurieren Sie eine SNIP-Adresse mit der GUI:

Navigieren Sie zu System > Netzwerk > IPs > IPv4s, und fügen Sie eine neue SNIP-Adresse hinzu, oder bearbeiten Sie eine vorhandene Adresse.

So erstellen Sie mit der GUI einen Bereich von SNIP-Adressen:

1. Navigieren Sie zu System > Netzwerk > IPs > IPv4s.
2. Wählen Sie in der Liste Aktion die Option Bereich hinzufügenaus.

So aktivieren oder deaktivieren Sie den USNIP-Modus mit der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- enable ns mode USNIP

- disable ns mode USNIP

So aktivieren oder deaktivieren Sie den USNIP-Modus mit der GUI:

1. Navigieren Sie zu System > Einstellungen, klicken Sie in der Gruppe Modi und Features auf Modi ändern.
2. Aktivieren oder deaktivieren Sie die Option Subnetz-IP verwenden.

Verwenden von SNIPs für ein direkt verbundenes Server-Subnetz

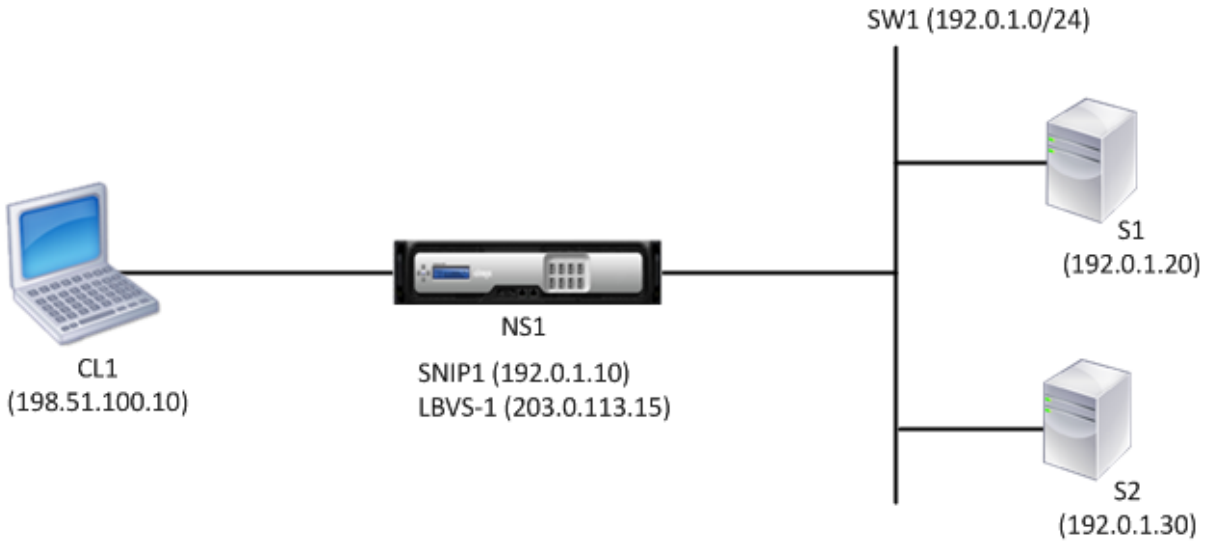
Um die Kommunikation zwischen Citrix ADC und einem Server zu ermöglichen, der entweder direkt mit dem Citrix ADC verbunden ist oder nur über einen L2-Switch verbunden ist, müssen Sie eine Subnetz-IP-Adresse konfigurieren, die zum Subnetz des Servers gehört. Sie müssen mindestens eine Subnetz-IP-Adresse für jedes direkt verbundene Subnetz konfigurieren, außer für das direkt verbundene Verwaltungssubnetz, das über NSIP verbunden ist.

Betrachten Sie ein Beispiel für ein Lastausgleichs-Setup, bei dem der Lastausgleich des virtuellen Servers LBVS1 auf Citrix ADC NS1 zum Lastenausgleich von Servern S1 und S2 verwendet wird, die über den L2-Switch SW1 mit NS1 verbunden sind. S1 und S2 gehören zum selben Subnetz.

Die SNIP-Adresse SNIP1, die zum selben Subnetz wie S1 und S2 gehört, ist auf NS1 konfiguriert. Sobald SNIP1 konfiguriert ist, sendet NS1 ARP-Pakete für SNIP1.

Die Dienste SVC-S1 und SVC-S2 auf NS1 repräsentieren S1 und S2. Sobald diese Dienste konfiguriert sind, sendet NS1 ARP-Anforderungen für S1 und S2, um die IP-zu-Mac-Zuordnung aufzulösen. Nachdem S1 und S2 antworten, sendet NS1 ihnen Überwachungssonden in regelmäßigen Abständen von der Adresse SNIP1, um ihre Gesundheit zu überprüfen.

Weitere Informationen zum Konfigurieren des Lastenausgleichs auf einem Citrix ADC finden Sie unter Load Balancing.



Es folgt der Verkehrsfluss in diesem Beispiel:

1. Client C1 sendet ein Anforderungspaket an LBVS-1. Das Anforderungspaket hat:
   - Quell-IP = IP-Adresse des Clients (198.51.100.10)
   - Ziel-IP = IP-Adresse von LBVS-1 (203.0.113.15)
2. LBVS1 von NS1 empfängt das Anforderungspaket.
3. Der Lastausgleichsalgorithmus von LBVS1 wählt Server S2 aus.
4. Da S2 direkt mit NS1 verbunden ist und SNIP1 (192.0.1.10) die einzige IP-Adresse auf NS1 ist, die zum selben Subnetz wie S2 gehört, öffnet NS1 eine Verbindung zwischen SNIP1 und S2.
5. NS1 sendet das Anforderungspaket von SNIP1 an S2. Das Anforderungspaket hat:
   - Quell-IP = SNIP1 (192.0.1.10)
   - Ziel-IP = IP-Adresse von S2 (192.0.1.30)
6. Die Antwort von S2 gibt den gleichen Pfad zurück.

Verwenden von SNIPs für Serversubnetze, die über einen Router verbunden sind

Um die Kommunikation zwischen Citrix ADC und Servern in Subnetzen zu ermöglichen, die über einen Router verbunden sind, müssen Sie mindestens eine Subnetz-IP-Adresse konfigurieren, die zum Subnetz der direkt verbundenen Schnittstelle zum Router gehört. Der ADC verwendet diese Subnetz-IP-Adresse, um mit Servern in Subnetzen zu kommunizieren, die über den Router erreichbar sind.

Betrachten Sie ein Beispiel für ein Lastausgleichs-Setup, bei dem der Lastausgleich des virtuellen Servers LBVS1 auf Citrix ADC NS1 zum Lastenausgleich von Servern S1, S2, S3 und S4 verwendet wird, die über Router R1 mit NS1 verbunden sind.

S1 und S2 gehören zu demselben Subnetz, 192.0.2.0/24, und sind mit R1 über L2-Switch SW1 verbunden. S3 und S4 gehören zu einem anderen Subnetz, 192.0.3.0/24, und sind mit R1 über L2-Switch SW2 verbunden.

Citrix ADC NS1 ist über das Subnetz 192.0.1.0/24 mit dem Router R1 verbunden. Die SNIP-Adresse SNIP1, die zum selben Subnetz gehört wie die direkt angeschlossene Schnittstelle zum Router (192.0.1.0/24), ist auf NS1 konfiguriert. NS1 verwendet diese Adresse für die Kommunikation mit Servern S1 und S2 sowie mit Servern S3 und S4.

Weitere Informationen zum Konfigurieren des Lastenausgleichs auf einem Citrix ADC finden Sie unter Load Balancing.

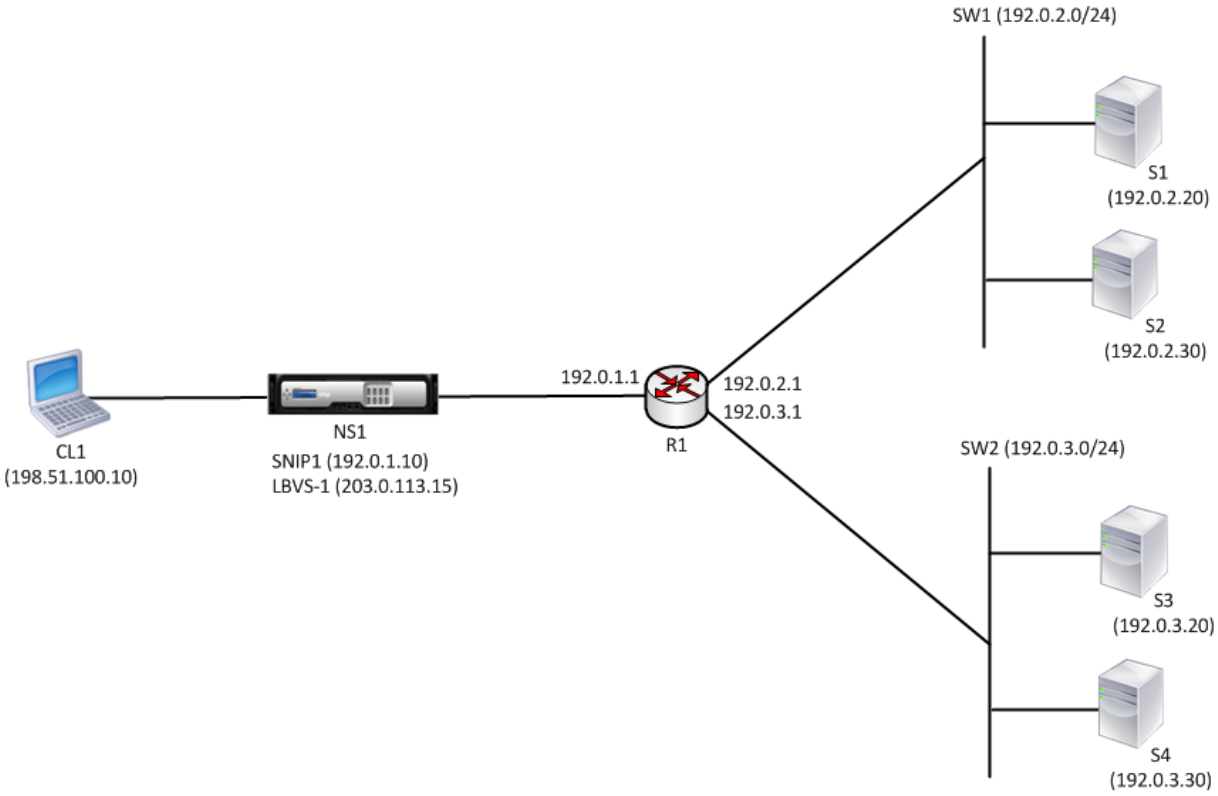
Sobald die Adresse SNIP1 konfiguriert ist, sendet NS1 ARP-Ankündigungspakete für SNIP1.

Die Routingtabelle von NS1 besteht aus Routeneinträgen für S1, S2, S3 und S4 bis R1. Bei diesen Routeneinträgen handelt es sich entweder um statische Routeneinträge oder die von R1 nach NS1 unter Verwendung dynamischer Routingprotokolle angekündigt werden.

Die Dienste SVC-S1, SVC-S2, SVC-S3 und SVC-S4 auf NS1 stellen die Server S1, S2, S3 und S4 dar. NS1 findet in seinen Routingtabellen, dass diese Server über R1 erreichbar sind. NS1 sendet ihnen

Überwachungssonden in regelmäßigen Abständen, von der Adresse SNIP1, um ihre Gesundheit zu überprüfen.

Weitere Informationen zum IP-Routing auf einem Citrix ADC finden Sie unter IP-Routing.



Es folgt der Verkehrsfluss in diesem Beispiel:

1. Client C1 sendet ein Anforderungspaket an LBVS-1. Das Anforderungspaket hat:
   - Quell-IP = IP-Adresse des Clients (198.51.100.10)
   - Ziel-IP = IP-Adresse von LBVS-1 (203.0.113.15)
2. LBVS1 von NS1 empfängt das Anforderungspaket.
3. Der Lastausgleichsalgorithmus von LBVS1 wählt Server S3 aus.
4. NS1 überprüft seine Routing-Tabelle und stellt fest, dass S3 über R1 erreichbar ist. SNIP1 (192.0.1.10) ist die einzige IP-Adresse auf NS1, die zum selben Subnetz wie Router R1 gehört, NS1 öffnet eine Verbindung zwischen SNIP1 und S3 über R1.
5. NS1 sendet das Anforderungspaket von SNIP1 an R1. Das Anforderungspaket hat:
   - Quell-IP-Adresse = SNIP1 (192.0.1.10)
   - Ziel-IP-Adresse = IP-Adresse von S3 (192.0.3.20)
6. Die Anforderung erreicht R1, die seine Routingtabelle überprüft und das Anforderungspaket an S3 weiterleitet.
7. Die Antwort von S3 gibt den gleichen Pfad zurück.

Verwenden von SNIPs für mehrere Server-Subnetze (VLANs) auf einem L2-Switch

Wenn Sie mehrere Serversubnetze (VLANs) auf einem L2-Switch haben, der mit einem Citrix ADC verbunden ist, müssen Sie mindestens eine SNIP-Adresse für jedes der Serversubnetze konfigurieren, damit Citrix ADC mit diesen Serversubnetzen kommunizieren kann.

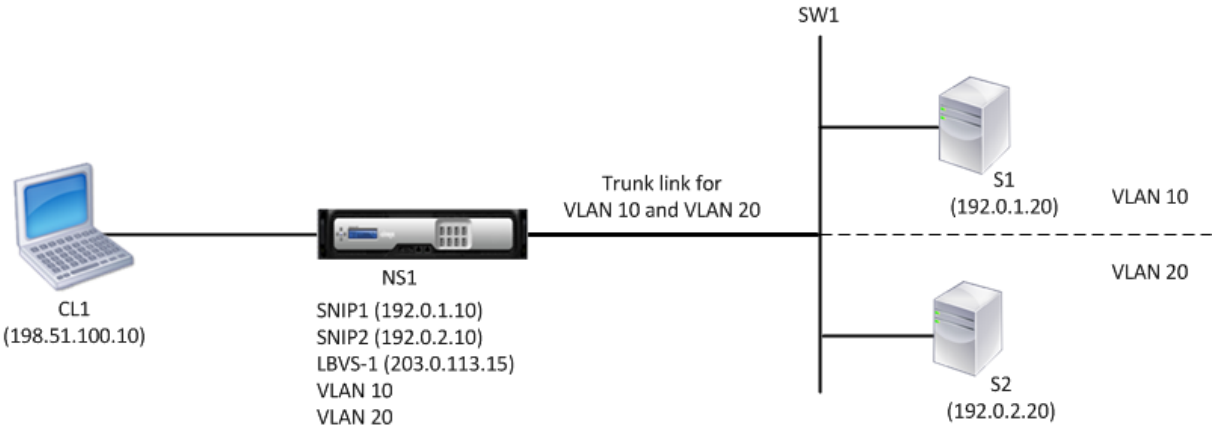
Betrachten Sie ein Beispiel für ein Lastausgleichs-Setup, bei dem der Lastausgleich des virtuellen Servers LBVS1 auf Citrix ADC NS1 zum Lastenausgleich von Servern S1 und S2 verwendet wird, die über den L2-Switch SW1 mit NS1 verbunden sind. S1 und S2 gehören zu verschiedenen Subnetzen und sind Teil von VLAN 10 bzw. VLAN20. Die Verbindung zwischen NS1 und SW1 ist eine Trunk-Verbindung und wird von VLAN10 und VLAN20 gemeinsam genutzt.

Weitere Informationen zum Konfigurieren des Lastenausgleichs auf einem Citrix ADC finden Sie unter Load Balancing.

Subnetz-IP-Adressen SNIP1 (nur zu Referenzzwecken) und SNIP2 (nur zu Referenzzwecken) werden auf NS1 konfiguriert. NS1 verwendet SNIP1 (auf VLAN 10) für die Kommunikation mit Server S1 und SNIP2 (auf VLAN 20) für die Kommunikation mit S2. Sobald SNIP1 und SNIP2 konfiguriert sind, sendet NS1 ARP-Ankündigungspakete für SNIP1 und SNIP2.

Weitere Informationen zum Konfigurieren von VLANs auf einem Citrix ADC finden Sie unter Konfigurieren eines VLAN.

Die Dienste SVC-S1 und SVC-S2 auf NS1 stellen Server S1 und S2 dar. Sobald diese Dienste konfiguriert sind, sendet NS1 ARP-Anforderungen für sie. Nachdem S1 und S2 reagiert haben, sendet NS1 ihnen in regelmäßigen Abständen Überwachungssonden, um ihren Zustand zu überprüfen. NS1 sendet Überwachungssonden an S1 von der Adresse SNIP1 und an S2 von der Adresse SNIP2.



Es folgt der Verkehrsfluss in diesem Beispiel:

1. Client C1 sendet ein Anforderungspaket an LBVS-1. Das Anforderungspaket hat:
   - Quell-IP = IP-Adresse des Clients (198.51.100.10)
   - Ziel-IP = IP-Adresse von LBVS-1 (203.0.113.15)
2. LBVS1 von NS1 empfängt das Anforderungspaket.

3. Der Lastausgleichsalgorithmus von LBVS1 wählt Server S2 aus.
4. Da S2 direkt mit NS1 verbunden ist und SNIP2 (192.0.2.10) die einzige IP-Adresse auf NS1 ist, die zum selben Subnetz wie S2 gehört, öffnet NS1 eine Verbindung zwischen SNIP2 und S2. Hinweis: Wenn S1 ausgewählt ist, öffnet NS1 eine Verbindung zwischen SNIP1 und S1.
5. NS1 sendet das Anforderungspaket von SNIP2 an S2. Das Anforderungspaket hat:
   - Quell-IP = SNIP1 (192.0.2.10)
   - Ziel-IP = IP-Adresse von S2 (192.0.2.20)
6. Die Antwort von S2 gibt den gleichen Pfad zurück.

Konfigurieren von GSLB-Site-IP-Adressen (GSLBIP)

October 5, 2021

Eine GSLB-Site-IP-Adresse (GSLBIP) ist eine IP-Adresse, die einem GSLB-Site zugeordnet ist. Es ist nicht zwingend erforderlich, eine GSLBIP-Adresse anzugeben, wenn Sie die Citrix ADC Appliance anfänglich konfigurieren. Eine GSLBIP-Adresse wird nur verwendet, wenn Sie eine GSLB-Site erstellen.

Weitere Informationen zum Erstellen einer GSLB-Site-IP-Adresse finden Sie unter Globaler Server-Lastenausgleich.

Entfernen einer Citrix ADC-eigenen IP-Adresse

October 5, 2021

Sie können jede IP-Adresse außer dem NSIP entfernen. Die folgende Tabelle enthält Informationen zu den Prozessen, die Sie befolgen müssen, um die verschiedenen Arten von IP-Adressen zu entfernen. Entfernen Sie vor dem Entfernen eines VIP den zugeordneten virtuellen Server.

IP-Adresstyp	Implikationen
Subnetz-IP-Adresse (SNIP)	Wenn die zu entfernende IP-Adresse die letzte IP-Adresse im Subnetz ist, wird die zugehörige Route aus der Routentabelle gelöscht. Wenn die zu entfernende IP-Adresse das Gateway im entsprechenden Routeneintrag ist, wird das Gateway für diese Subnetzroute in eine andere Citrix ADC-eigene IP-Adresse geändert.

IP-Adresstyp	Implikationen
IP-Adresse des virtuellen Servers (VIP)	Bevor Sie einen VIP entfernen, müssen Sie zuerst den damit verbundenen virtuellen Server entfernen. Informationen zum Entfernen des virtuellen Servers finden Sie unter Load Balancing.
GSLB-Site-IP-Adresse	Bevor Sie eine GSLB-Site-IP-Adresse entfernen, müssen Sie die zugehörige Site entfernen. Informationen zum Entfernen der Site finden Sie unter Globaler Server-Lastenausgleich.

So entfernen Sie eine IP-Adresse mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

<IPaddress>rm ns ip

Beispiel:

```
1 > rm ns ip 10.102.29.54
2 Done
3 <!--NeedCopy-->
```

So entfernen Sie eine IP-Adresse mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv4s**, löschen Sie die IP-Adresse.

Anwendungszugriffskontrollen konfigurieren

October 5, 2021

Anwendungszugriffskontrollen, auch als Verwaltungszugriffskontrollen bezeichnet, bilden einen einheitlichen Mechanismus zur Verwaltung der Benutzerauthentifizierung und Implementierung von Regeln, die den Benutzerzugriff auf Anwendungen und Daten bestimmen. Sie können SNIPs konfigurieren, um Zugriff für Verwaltungsanwendungen bereitzustellen. Der Verwaltungszugriff für das NSIP ist standardmäßig aktiviert und kann nicht deaktiviert werden. Sie können es jedoch mithilfe von ACLs steuern.

Informationen zur Verwendung von ACLs finden Sie unter Zugriffssteuerungslisten (ACLs).

Die Citrix ADC Appliance unterstützt keinen Verwaltungszugriff auf VIPs.

Die folgende Tabelle enthält eine Zusammenfassung der Interaktion zwischen Verwaltungszugriff und bestimmten Diensteinstellungen für Telnet.

Verwaltungszugriff	Telnet (Status konfiguriert auf dem Citrix ADC)	Telnet (effektiver Zustand auf IP-Ebene)
Smartcard	Smartcard	Smartcard
Smartcard	Deaktivieren	Deaktivieren
Deaktivieren	Smartcard	Deaktivieren
Deaktivieren	Deaktivieren	Deaktivieren

Die folgende Tabelle bietet einen Überblick über die IP-Adressen, die als Quell-IP-Adressen im ausgehenden Datenverkehr verwendet werden.

Anwendung/IP	NSIP	SNIP	VIP
ARP	Ja	Ja	Nein
Serverseitiger Datenverkehr	Nein	Ja	Nein
RNAT	Nein	Ja	Ja
ICMP-PING	Ja	Ja	Nein
Dynamisches Routing	Ja	Ja	Ja

Die folgende Tabelle bietet einen Überblick über die Anwendungen, die für diese IP-Adressen verfügbar sind.

Anwendung/IP	NSIP	SNIP	VIP
SNMP	Ja	Ja	Ja
Systemzugriff	Ja	Ja	Nein

Mithilfe von Anwendungen wie Telnet, SSH, GUI und FTP können Sie auf das Citrix ADC zugreifen und diese verwalten.

Hinweis: Telnet und FTP sind auf dem Citrix ADC aus Sicherheitsgründen deaktiviert. Wenden Sie sich an den Kundendienst, um sie zu aktivieren. Nachdem die Anwendungen aktiviert sind, können

Sie die Steuerelemente auf IP-Ebene anwenden.

Um Citrix ADC für die Reaktion auf diese Anwendungen zu konfigurieren, müssen Sie die spezifischen Verwaltungsanwendungen aktivieren. Wenn Sie den Verwaltungszugriff für eine IP-Adresse deaktivieren, werden vorhandene Verbindungen, die die IP-Adresse verwenden, nicht beendet, aber es können keine neuen Verbindungen initiiert werden.

Außerdem sind die nicht verwaltbaren Anwendungen, die auf dem zugrunde liegenden FreeBSD-Betriebssystem ausgeführt werden, für Protokollangriffe offen, und diese Anwendungen nutzen die Angriffsverhinderungsfunktionen der Citrix ADC Appliance nicht.

Sie können den Zugriff auf diese Nicht-Management-Anwendungen auf einem SNIP oder NSIP blockieren. Wenn der Zugriff blockiert ist, kann ein Benutzer, der über SNIP oder NSIP eine Verbindung mit einem Citrix ADC herstellt, nicht auf die nicht verwaltbaren Anwendungen zugreifen, die auf dem zugrunde liegenden Betriebssystem ausgeführt werden.

So konfigurieren Sie den Verwaltungszugriff für eine IP-Adresse mithilfe der Befehlszeile:

Geben Sie an der Eingabeaufforderung Folgendes ein:

set ns ip <IPAddress> -mgmtAccess <value> -**telnet** <value> -**ftp** <value> -**gui** <value> -**ssh** <value> -**snmp** <value> -**restrictAccess** (**ENABLED** | **DISABLED**)

Beispiel:

```
1  > set ns ip 10.102.29.54 -mgmtAccess enabled -restrictAccess ENABLED
2   Done
3 <!--NeedCopy-->
```

So aktivieren Sie den Verwaltungszugriff für eine IP-Adresse mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv4s**.
2. Öffnen Sie einen IP-Adresseintrag, und wählen Sie die Option **Verwaltungszugriff aktivieren**, um die aufgelisteten Anwendungen zu unterstützen.

Aktivieren des sicheren Zugriffs auf Citrix ADC GUI mit einer Subnetz-IP-Adresse (SNIP)

Der sichere Zugriff auf die Citrix ADC GUI ist standardmäßig für die Citrix ADC IP (NSIP) aktiviert. Sie können den sicheren Zugriff auf die Citrix ADC Appliance auch mithilfe einer Subnetz-IP-Adresse der Appliance aktivieren.

Nach dem Konfigurieren einer SNIP-Adresse für den sicheren Zugriff auf ein Hochverfügbarkeitspaar steht der sichere Zugriff auf die primäre Appliance zur Verfügung, wenn Sie auf die SNIP-Adresse zugreifen.

Citrix ADC CLI-Verfahren

So aktivieren Sie den sicheren Zugriff auf Citrix ADC GUI mit einer Subnetz-IP-Adresse (SNIP) über die Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

set ns ip <SNIP_Address>**-type SNIP -gui SECUREONLY -mgmtAccess ENABLED**

Beispiel:

```
> set ns ip 203.0.113.99 -mgmtAccess enabled -restrictAccess ENABLED

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

Wie Citrix ADC Proxies Verbindungen

October 5, 2021

Wenn ein Client eine Verbindung initiiert, beendet die Citrix ADC Appliance die Clientverbindung, initiiert eine Verbindung zu einem geeigneten Server und sendet das Paket an den Server. Die Appliance führt diese Aktion nicht für den Diensttyp UDP oder ANY aus.

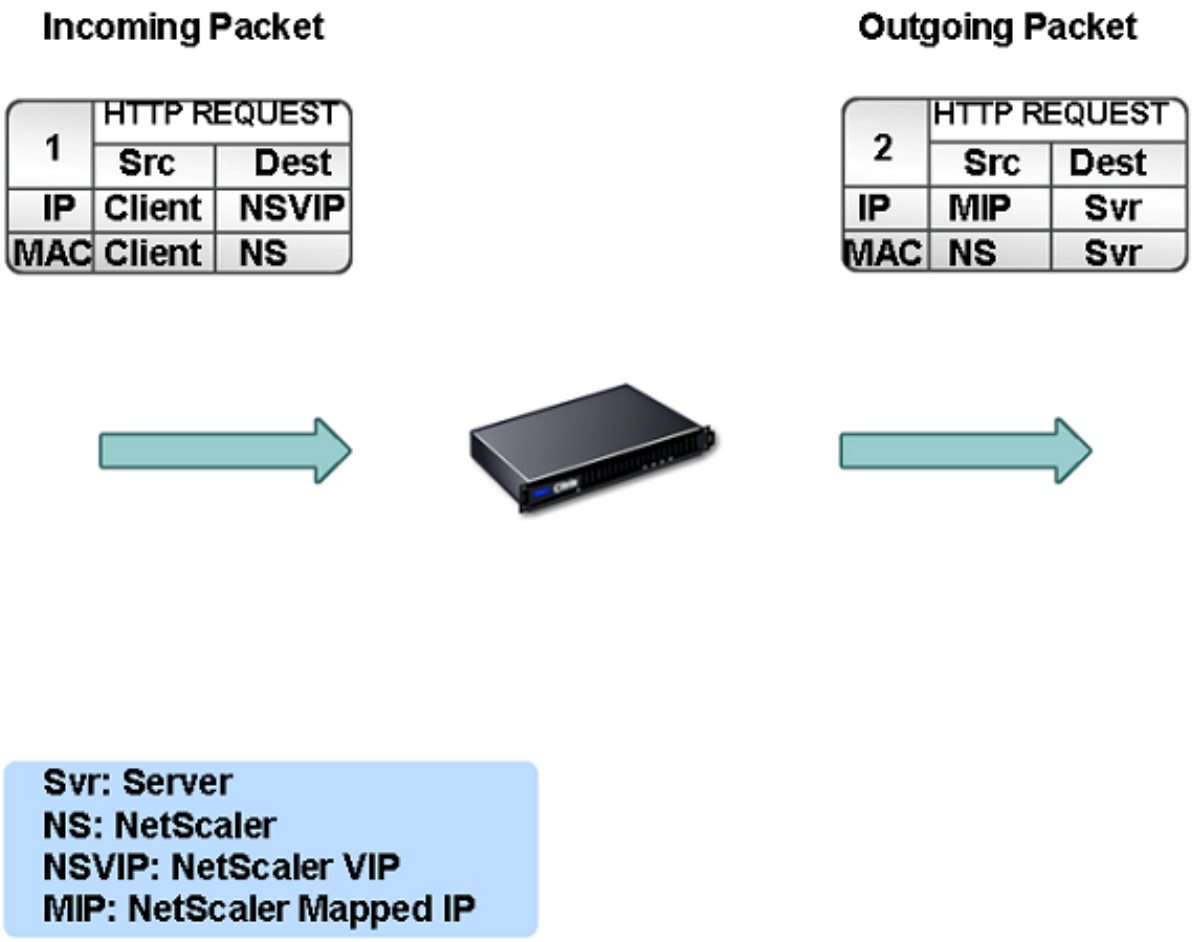
Weitere Informationen zu Diensttypen finden Sie unter Load Balancing.

Sie können den Citrix ADC so konfigurieren, dass das Paket verarbeitet wird, bevor Sie die Verbindung mit einem Server initiieren. Das Standardverhalten besteht darin, die Quell- und Ziel-IP-Adressen eines Pakets zu ändern, bevor das Paket an den Server gesendet wird. Sie können den Citrix ADC so konfigurieren, dass die Quell-IP-Adresse der Pakete beibehalten wird, indem Sie den Quell-IP-Modus verwenden aktivieren.

Auswählen der Ziel-IP-Adresse

Datenverkehr, der an die Citrix ADC Appliance gesendet wird, kann an einen virtuellen Server oder an einen Dienst gesendet werden. Die Appliance verarbeitet den Datenverkehr zu virtuellen Servern und Diensten unterschiedlich. Der Citrix ADC beendet den Datenverkehr, der an einer virtuellen Server-IP-Adresse (VIP) empfangen wurde, und ändert die Ziel-IP-Adresse in die IP-Adresse des Servers, bevor der Datenverkehr an den Server weitergeleitet wird, wie im folgenden Diagramm dargestellt.

Abbildung 1. Proxyverbindungen zu VIPs



Pakete, die für einen Dienst bestimmt sind, werden direkt an den entsprechenden Server gesendet, und Citrix ADC ändert die Ziel-IP-Adressen nicht. In diesem Fall fungiert das Citrix ADC als Proxy.

Auswählen der Quell-IP-Adresse

Wenn die Citrix ADC Appliance mit den physischen Servern oder Peer-Geräten kommuniziert, verwendet sie standardmäßig nicht die IP-Adresse des Clients. Citrix ADC verwaltet einen Pool von Subnetz-IP-Adressen (SNIPs) und wählt eine IP-Adresse aus diesem Pool aus, die als Quell-IP-Adresse einer Verbindung zum physischen Server verwendet werden soll. Abhängig vom Subnetz, in dem der physische Server abgelegt ist, wählt Citrix ADC eine bestimmte SNIP-Adresse aus.

Hinweis: Wenn die Option Quell-IP (USIP) verwenden aktiviert ist, verwendet die Appliance die IP-Adresse des Clients.

Quell-IP-Modus aktivieren

October 5, 2021

Wenn die Citrix ADC Appliance mit den physischen Servern oder Peer-Geräten kommuniziert, verwendet sie standardmäßig eine ihrer eigenen IP-Adressen als Quell-IP. Die Appliance verwaltet einen Pool von Subnetz-IP-Adressen (SNIPs) und wählt eine IP-Adresse aus diesem Pool aus, die als Quell-IP-Adresse für eine Verbindung mit dem physischen Server verwendet werden soll. Die Entscheidung, eine SNIP-Adresse auszuwählen, hängt vom Subnetz ab, in dem sich der physische Server befindet.

Bei Bedarf können Sie die Citrix ADC Appliance so konfigurieren, dass die IP-Adresse des Clients als Quell-IP verwendet wird. Einige Anwendungen benötigen die tatsächliche IP-Adresse des Clients. Die folgenden Anwendungsfälle sind einige Beispiele:

- Die IP-Adresse des Kunden im Webzugriffsprotokoll wird für Abrechnungszwecke oder Nutzungsanalysen verwendet.
- Die IP-Adresse des Kunden wird verwendet, um das Herkunftsland des Kunden oder den ursprünglichen ISP des Kunden zu bestimmen. So stellen beispielsweise viele Suchmaschinen wie Google Inhalte bereit, die für den Standort relevant sind, zu dem der Nutzer gehört.
- Die Anwendung muss die IP-Adresse des Clients kennen, um zu überprüfen, ob die Anforderung von einer vertrauenswürdigen Quelle stammt.
- Obwohl ein Anwendungsserver die IP-Adresse des Clients nicht benötigt, benötigt eine Firewall zwischen dem Anwendungsserver und dem Citrix ADC möglicherweise die IP-Adresse des Clients, um den Datenverkehr zu filtern.

Aktivieren Sie den USIP-Modus (Source IP mode), wenn Citrix ADC die IP-Adresse des Clients für die Kommunikation mit den Servern verwenden soll.

Die folgende Abbildung zeigt, wie die Appliance IP-Adressen im USIP-Modus verwendet.

Voraussetzungen

Bevor Sie den USIP-Modus aktivieren, beachten Sie die folgenden Punkte:

- Aktivieren Sie USIP in folgenden Situationen:
  - Lastenausgleich von IDS-Servern (Intrusion Detection System)
  - SMTP-Lastenausgleich
  - Zustandsloses Verbindungs-Failover
  - Sitzungsloser Lastausgleich
  - Wenn Sie den Direct Server Return (DSR) -Modus verwenden
- Die globale USIP-Einstellung gilt nur für Dienste, die erstellt werden, nachdem die globale USIP-Einstellung vorgenommen wurde. Mit anderen Worten, die globale USIP-Einstellung gilt nicht für die vorhandenen Dienste, wenn die globale USIP-Einstellung vorgenommen wird. Beispielsweise deaktiviert das globale Deaktivieren von USIP nicht USIP für die vorhandenen Dienste. Es verhindert jedoch, dass die nachfolgend erstellten Dienste USIP automatisch aktiviert haben.

  Um USIP für eine Reihe von vorhandenen Diensten zu aktivieren oder zu deaktivieren, müssen Sie USIP für jeden dieser Dienste aktivieren oder deaktivieren.
- Wenn USIP aktiviert ist, müssen Sie das Gateway des Servers auf eine der IP-Adressen des Citrix ADC festlegen (vom Typ Subnet IP (SNIP), damit die Antwort des Servers immer die Citrix ADC-Appliance durchläuft.
- Wenn Sie USIP aktivieren, setzen Sie das Leerlaufzeitlimit für Serververbindungen auf einen Wert, der niedriger ist als der Standardwert, so dass Leerlaufverbindungen auf der Serverseite schnell gelöscht werden.
- Aktivieren Sie für eine transparente Cache-Umleitung, wenn Sie USIP aktivieren, auch L2CONN.
- Da HTTP-Verbindungen nicht wiederverwendet werden, wenn USIP aktiviert ist, kann sich eine große Anzahl von serverseitigen Verbindungen ansammeln. Serververbindungen im Leerlauf können Verbindungen für andere Clients blockieren. Legen Sie daher Grenzwerte für die maximale Anzahl von Verbindungen zu einem Dienst fest. Citrix empfiehlt außerdem, den HTTP-Server-Timeoutwert für einen Dienst, für den USIP aktiviert ist, auf einen Wert festzulegen, der niedriger ist als der Standardwert, damit Verbindungen im Leerlauf schnell auf der Serverseite gelöscht werden.
- Alternativ zum USIP-Modus haben Sie die Möglichkeit, die IP-Adresse des Clients (CIP) in den Anforderungskopf der serverseitigen Verbindung für einen Anwendungsserver einzufügen, der die IP-Adresse des Clients benötigt.
- In früheren Citrix ADC Versionen hatte der USIP-Modus die folgenden Quellportoptionen für serverseitige Verbindungen:
  - **Verwenden Sie den Port des Clients**. Mit dieser Option können Verbindungen nicht

wiederverwendet werden. Für jede Anforderung des Clients wird eine neue Verbindung mit dem physischen Server hergestellt.

- **Verwenden Sie den Proxy-Port**. Mit dieser Option ist die Wiederverwendung der Verbindung für alle Anfragen desselben Clients möglich.

Wenn USIP in den späteren Citrix ADC Versionen aktiviert ist, wird standardmäßig ein Proxyport für serverseitige Verbindungen verwendet und keine Verbindungen wiederverwendet. Die Nichtwiederverwendung von Verbindungen beeinträchtigt möglicherweise nicht die Geschwindigkeit des Verbindungsaufbaus.

Standardmäßig ist die Option Proxyport verwenden aktiviert, wenn der USIP-Modus aktiviert ist.

Hinweis: Wenn Sie den USIP-Modus aktivieren, wird empfohlen, die Option Proxy-Port verwenden zu aktivieren.

Weitere Informationen zur Option Proxy-Port verwenden finden Sie unter Konfigurieren des Quellports für serverseitige Verbindungen.

Konfigurationsschritte

Aktivieren Sie den USIP-Modus (Source IP mode), wenn Citrix ADC die IP-Adresse des Clients für die Kommunikation mit den Servern verwenden soll. Standardmäßig ist der USIP-Modus deaktiviert. Der USIP-Modus kann global auf dem Citrix ADC oder auf einem bestimmten Dienst aktiviert werden. Wenn Sie es global aktivieren, ist USIP standardmäßig für alle nachfolgend erstellten Dienste aktiviert. Wenn Sie USIP für einen bestimmten Dienst aktivieren, wird die IP-Adresse des Clients nur für den Datenverkehr verwendet, der an diesen Dienst geleitet wird.

CLI-Verfahren

So aktivieren oder deaktivieren Sie den USIP-Modus mit der CLI global:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- **enable ns mode USIP**
- **disable ns mode USIP**

So aktivieren Sie den USIP-Modus für einen Dienst mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

set service <name>@ -**usip** (**YES** | **NO**)

Beispiel:


```
> set service Service-HTTP-1 -usip YES
Done
<!--NeedCopy-->
```

GUI-Verfahren

So aktivieren oder deaktivieren Sie den USIP-Modus mit der GUI global:

1. Navigieren Sie zu **System** > **Einstellungen**, klicken Sie in der Gruppe **Modi und Features** auf **Modi ändern**.
2. Aktivieren oder deaktivieren Sie die Option **Quell-IP verwenden**.

So aktivieren Sie den USIP-Modus für einen Dienst mit der GUI:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**, und bearbeiten Sie einen Service.
2. Wählen Sie unter **Erweiterte Einstellungen** die Option **Diensteinstellungen** aus, und wählen Sie **Quell-IP-Adresse verwenden**.

Konfigurieren der Netzwerkadressübersetzung

October 5, 2021

Network Address Translation (NAT) beinhaltet die Änderung der Quell- und/oder Ziel-IP-Adressen und/oder der TCP/UDP-Portnummern von IP-Paketen, die die Citrix ADC Appliance passieren. Wenn Sie NAT auf der Appliance aktivieren, erhöht sich die Sicherheit Ihres privaten Netzwerks und schützt es vor einem öffentlichen Netzwerk wie dem Internet, indem Sie die IP-Adressen der Netzwerkquelle ändern, wenn Daten über den Citrix ADC geleitet werden. Mit Hilfe von NAT-Einträgen kann Ihr gesamtes privates Netzwerk durch ein paar freigegebene öffentliche IP-Adressen dargestellt werden. Citrix ADC unterstützt die folgenden Arten der Netzwerkadressübersetzung:

- **Eingehende NAT (INAT).** Citrix ADC ersetzt die Ziel-IP-Adresse in den vom Client generierten Paketen durch die private IP-Adresse des Servers.
- **Reverse NAT (RNAT).** Citrix ADC ersetzt die Quell-IP-Adresse in den von den Servern generierten Paketen durch die öffentlichen NAT-IP-Adressen.

Adressübersetzung eingehender Netzwerke

October 5, 2021

Wenn ein Client ein Paket an eine Citrix ADC Appliance sendet, die für die Inbound Network Address Translation (INAT) konfiguriert ist, übersetzt die Appliance die öffentliche Ziel-IP-Adresse des Pakets in eine private Ziel-IP-Adresse und leitet das Paket an den Server an dieser Adresse weiter.

Folgende Konfigurationen werden unterstützt:

- **IPv4-IPv4-Zuordnung**: Eine öffentliche IPv4-Adresse auf der Citrix ADC Appliance überwacht Verbindungsanforderungen im Auftrag eines privaten IPv4-Servers. Die Citrix ADC Appliance übersetzt die IP-Adresse des Pakets an das öffentliche Ziel in die Ziel-IP-Adresse des Servers. Dann leitet die Appliance das Paket an den Server unter dieser Adresse weiter.
- **IPv4-IPv6-Zuordnung**: Eine öffentliche IPv4-Adresse auf der Citrix ADC Appliance überwacht Verbindungsanforderungen im Auftrag eines privaten IPv6-Servers. Die Citrix ADC Appliance erstellt ein IPv6-Anforderungspaket mit der IP-Adresse des IPv6-Servers als Ziel-IP-Adresse.
- **IPv6-IPv4-Zuordnung**: Eine öffentliche IPv6-Adresse auf der Citrix ADC Appliance überwacht Verbindungsanforderungen im Auftrag eines privaten IPv4-Servers. Die Citrix ADC Appliance erstellt ein IPv4-Anforderungspaket mit der IP-Adresse des IPv4-Servers als Ziel-IP-Adresse.
- **IPv6-IPv6-Zuordnung**: Eine öffentliche IPv6-Adresse auf der Citrix ADC Appliance überwacht Verbindungsanforderungen im Auftrag eines privaten IPv6-Servers. Die Citrix ADC Appliance übersetzt die IP-Adresse des Pakets an das öffentliche Ziel in die Ziel-IP-Adresse des Servers. Dann leitet die Appliance das Paket an den Server unter dieser Adresse weiter.

Wenn die Appliance ein Paket an einen Server weiterleitet, wird die dem Paket zugewiesene Quell-IP-Adresse wie folgt ermittelt:

- Wenn der Use Subnet IP (USNIP) -Modus aktiviert ist und der Use Source IP (USIP) -Modus deaktiviert ist, verwendet die Appliance eine Subnetz-IP-Adresse (SNIP) als Quell-IP-Adresse.
- Wenn der USIP-Modus aktiviert ist und der USNIP-Modus deaktiviert ist, verwendet die Appliance die Client-IP-Adresse (CIP) als Quell-IP-Adresse.
- Wenn sowohl USIP- als auch USNIP-Modi aktiviert sind, hat der USIP-Modus Vorrang.
- Sie können den Citrix ADC auch so konfigurieren, dass eine eindeutige IP-Adresse als Quell-IP-Adresse verwendet wird, indem Sie den ProxyIP-Parameter festlegen.
- Wenn keiner der oben genannten Modi aktiviert ist und keine eindeutige IP-Adresse angegeben wurde, versucht Citrix ADC, eine MIP als Quell-IP-Adresse zu verwenden.
- Wenn sowohl USIP- als auch USNIP-Modi aktiviert sind und eine eindeutige IP-Adresse angegeben wurde, lautet die Rangfolge wie folgt: USIP-Unique IP-USNIP-MIP-Fehler.

Um den Citrix ADC vor DoS-Angriffen zu schützen, können Sie TCP-Proxy aktivieren. Wenn jedoch andere Schutzmechanismen in Ihrem Netzwerk verwendet werden, können Sie diese deaktivieren.

Konfigurieren von INAT-Regeln

Sie können einen INAT-Eintrag erstellen, ändern oder entfernen.

CLI-Verfahren

So erstellen Sie einen INAT-Eintrag mit der CLI:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um einen INAT-Eintrag zu erstellen und dessen Konfiguration zu überprüfen:

- **add inat** <name> <publicIP> <privateIP> [-**tcpproxy** (**ENABLED** | **DISABLED**)] [-**ftp** (**ENABLED** | **DISABLED**)] [-**usip** (**ON** | **OFF**)] [-**usnip** (**ON** | **OFF**)] [-**proxyIP** <**ip_addr > ipv6_addr>**]
- **show inat** [<name>]

Beispiel:

```
1 > add inat ip4-ip4 172.16.1.2 192.168.1.1 -proxyip 10.102.29.171
2  Done
3 <!--NeedCopy-->
```

So ändern Sie einen INAT Eintrag mit der CLI:

Um einen INAT-Eintrag zu ändern, geben Sie den Befehl `set inat`, den Namen des Eintrags und die zu ändernden Parameter mit den neuen Werten ein.

So entfernen Sie eine INAT Konfiguration mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **rm inat** <name>

Beispiel:

```
1 > rm inat ip4-ip4
2  Done
3 <!--NeedCopy-->
```

GUI-Verfahren

So konfigurieren Sie einen INAT Eintrag mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **Routen** > **INAT**, fügen Sie einen INAT-Eintrag hinzu oder bearbeiten Sie einen vorhandenen INAT-Eintrag.

So entfernen Sie eine INAT Konfiguration mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **Routen** > **INAT**, löschen Sie die INAT-Konfiguration.

Verbindungs-Failover für INAT-Regeln

Verbindungs-Failover oder Verbindungsspiegelung ermöglicht es dem primären Knoten, Verbindungs- und Persistenzinformationen mit dem sekundären Knoten in hoher Verfügbarkeit zu duplizieren. Die Statusinformationen der Verbindung werden regelmäßig mit dem sekundären Knoten geteilt, wenn die Verbindungsspiegelung aktiviert ist.

Das Aktivieren des Verbindungs-Failovers bietet mehr Zuverlässigkeit, geht jedoch zu Kosten einer Systemzeit, die für die Weitergabe der Zustandsinformationen aufgebraucht wird. Die Verbindungsdaten werden bei jeder Aktualisierung des Paket- oder Flow-Status mit der Standby-Unit synchronisiert. Daher darf es nur an Orten eingesetzt werden, an denen die Zuverlässigkeit der Verbindungsebene von größter Bedeutung ist.

Hochverfügbarkeitssetups der Citrix ADC Appliance unterstützen Verbindungs-Failover für INAT-Verbindungen. Der primäre Knoten sendet in regelmäßigen Abständen INAT-Mappings und andere INAT-bezogene Verbindungsinformationen an den sekundären Knoten. Die sekundäre Appliance verwendet die Zuordnungs- und Verbindungsinformationen nur im Falle eines Failovers.

Wenn ein Failover auftritt, enthält der neue primäre Knoten Informationen über die INAT-Verbindungen, die vor dem Failover hergestellt wurden. Daher wird diese Verbindungen auch nach dem Failover weiterhin bedient.

Aus Sicht des Kunden ist das Failover transparent. Während der Übergangsphase können der Client und der Server eine kurze Unterbrechung und erneute Übertragung erfahren. Verbindungs-Failover kann pro INAT-Regel aktiviert werden.

Um das Verbindungs-Failover für eine INAT-Regel zu aktivieren, aktivieren Sie den `connFailover` Parameter dieser spezifischen RNAT-Regel mit CLI.

CLI-Verfahren

So aktivieren Sie das Verbindungsfailover für eine INAT Regel über die CLI:

Um das Verbindungs-Failover beim Hinzufügen einer INAT-Regel zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein:

- **add inat** <name> <publicIP> <privateIP> [-**tcpproxy** (**ENABLED** | **DISABLED**)] [-**ftp** (**ENABLED** | **DISABLED**)] [-**usip** (**ON** | **OFF**)] [-**usnip** (**ON** | **OFF**)] [-**proxyIP** <ip_addr|ipv6_addr>] -**connfailover** (**ENABLED** | **DISABLED**)
- **show inat** <name>

Um das Verbindungs-Failover beim Ändern einer vorhandenen INAT-Regel zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein:

- **set inat -connfailover** (**ENABLED** | **DISABLED**)
- **show inat** <name>

Koexistenz von INAT und virtuellen Servern

October 5, 2021

Wenn sowohl INAT als auch RNAT konfiguriert sind, hat die INAT-Regel Vorrang vor der RNAT Regel. Wenn RNAT mit einer NAT IP (Network Address Translation IP) -Adresse konfiguriert ist, wird die NAT-IP-Adresse als Quell-IP-Adresse für diesen RNAT Client ausgewählt.

Die standardmäßige öffentliche Ziel-IP in einer INAT-Konfiguration ist die virtuelle IP-Adresse (VIP) des Citrix ADC Geräts. Virtuelle Server verwenden auch VIPs. Wenn sowohl INAT als auch ein virtueller Server dieselbe IP-Adresse verwenden, überschreibt die Vserver-Konfiguration die INAT Konfiguration.

Im Folgenden finden Sie einige Beispiele für Konfigurations-Setup-Szenarien und deren Auswirkungen.

Fall	Ergebnis
Sie haben einen virtuellen Server und einen Dienst so konfiguriert, dass alle Datenpakete, die an einem bestimmten Citrix ADC Port empfangen werden, direkt an den Server gesendet werden. Sie haben auch INAT konfiguriert und TCP aktiviert. Wenn Sie INAT auf diese Weise konfigurieren, werden alle Datenpakete gesendet, die über eine TCP-Engine empfangen werden, bevor sie an den Server gesendet werden.	Alle Pakete, die auf dem Citrix ADC empfangen werden, mit Ausnahme der Pakete, die am angegebenen Port empfangen werden, werden durch das TCP-Modul übergeben.
Sie haben einen virtuellen Server und einen Dienst so konfiguriert, dass alle Datenpakete vom Diensttyp TCP, die an einem bestimmten Port des Citrix ADC empfangen werden, an den Server gesendet werden, nachdem das TCP-Modul übergeben wurde. Sie haben auch INAT konfiguriert und TCP deaktiviert. Wenn Sie INAT auf diese Weise konfigurieren, werden die empfangenen Datenpakete direkt an den Server gesendet.	Nur Pakete, die auf dem angegebenen Port empfangen werden, werden durch die TCP-Engine geleitet.

Fall	Ergebnis
Sie haben einen virtuellen Server und einen Dienst so konfiguriert, dass alle empfangenen Datenpakete an einen der zwei Server gesendet werden. Sie versuchen, INAT so zu konfigurieren, dass alle empfangenen Datenpakete an einen anderen Server gesendet werden.	Die INAT Konfiguration ist nicht zulässig.
Sie haben INAT so konfiguriert, dass alle empfangenen Datenpakete direkt an einen Server gesendet werden. Sie versuchen, einen virtuellen Server und einen Dienst so zu konfigurieren, dass alle empfangenen Datenpakete an zwei verschiedene Server gesendet werden.	Die vserver-Konfiguration ist nicht zulässig.

Stateless NAT46

December 7, 2021

Die zustandslose NAT46-Funktion ermöglicht die Kommunikation zwischen IPv4- und IPv6-Netzwerken über IPv4- zu IPv6-Paketübersetzung und umgekehrt, ohne Sitzungsinformationen auf der Citrix ADC Appliance zu verwalten.

Bei einer zustandslosen NAT46-Konfiguration übersetzt die Appliance ein IPv4-Paket in IPv6 oder ein IPv6-Paket in IPv4, wie in RFCs 6145 und 2765 definiert.

Eine zustandslose NAT46-Konfiguration auf der Citrix ADC Appliance verfügt über folgende Komponenten:

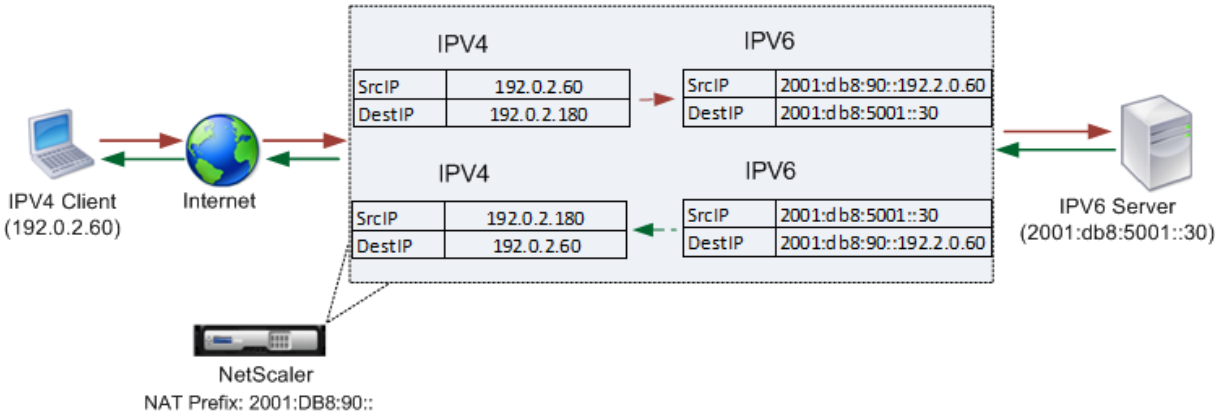
- **IPv4-IPv6 INAT Eintrag.** Ein INAT Eintrag, der eine 1:1 -Beziehung zwischen einer IPv4-Adresse und einer IPv6-Adresse definiert. Mit anderen Worten: Eine IPv4-Adresse auf der Appliance überwacht Verbindungsanforderungen im Auftrag eines IPv6-Servers. Ein IPv4-Anforderungspaket für diese IPv4-Adresse wird in ein IPv6-Paket übersetzt, und dann wird das IPv6-Paket an den IPv6-Server gesendet.

  Die Appliance übersetzt ein IPv6-Antwortpaket in ein IPv4-Antwortpaket, dessen Quell-IP-Adressfeld als IPv4-Adresse festgelegt ist, die im INAT Eintrag angegeben ist. Das übersetzte Paket wird dann an den Client gesendet.

- **NAT46 IPv6-Präfix.** Ein globales IPv6-Präfix der Länge 96 Bit (128-32=96), das auf der Appliance konfiguriert ist. Während der Übersetzung von IPv4-Paketen zu IPv6-Paketen setzt die Appliance die Quell-IP-Adresse des übersetzten IPv6-Pakets auf eine Verkettung des NAT46 IPv6-Präfixes [96 Bit] und der IPv4-Quelladresse [32 Bit] ein, die im Anforderungspaket empfangen wurde.

  Während der Übersetzung von IPv6-Paketen zu IPv4-Paketen setzt die Appliance die Ziel-IP-Adresse des übersetzten IPv4-Pakets auf die letzten 32 Bits der Ziel-IP-Adresse des IPv6-Pakets.

Betrachten Sie ein Beispiel, in dem ein Unternehmen Website www.example.com auf Server S1 hostet, der eine IPv6-Adresse hat. Um die Kommunikation zwischen IPv4-Clients und IPv6-Server S1 zu ermöglichen, wird die Citrix ADC Appliance NS1 mit einer zustandslosen NAT46-Konfiguration bereitgestellt, die einen IPv4-IPv6-INAT-Eintrag für Server S1 und ein NAT46-Präfix enthält. Der INAT Eintrag enthält eine IPv4-Adresse, unter der die Appliance Verbindungsanforderungen von IPv4-Clients im Auftrag des IPv6-Servers S1 überwacht.



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt:

Entitäten	Name	Wert
IP-Adresse des Clients	Client_IPv4 (nur zu Referenzzwecken)	192.0.2.60
IPv6-Adresse des Servers	SEVR_IPv6 (nur zu Referenzzwecken)	2001:DB8:5001::30
IPv4-Adresse, die im INAT Eintrag für IPv6-Server S1 definiert ist	Map-Sevr-IPv4 (nur zu Referenzzwecken)	192.0.2.180
IPv6-Präfix für NAT-46-Übersetzung	NAT46_Präfix (nur zu Referenzzwecken)	2001:DB8:90::

Es folgt der Verkehrsfluss in diesem Beispiel:

1. IPv4-Client CL1 sendet ein Anforderungspaket an die MAP-Sevr-IPv4-Adresse (192.0.2.180) auf der Citrix ADC Appliance.
2. Die Appliance empfängt das Anforderungspaket und durchsucht die NAT46-INAT-Einträge nach der IPv6-Adresse, die der Map-Sevr-IPv4-Adresse (192.0.2.180) zugeordnet ist. Es findet die Sevr-IPv6 (2001:DB 8:5001: :30) Adresse.
3. Die Appliance erstellt ein übersetztes IPv6-Anforderungspaket mit:
   - Ziel-IP-Adressfeld = SEVR-IPv6 = 2001:DB 8:5001: :30
   - Quell-IP-Adressfeld = Verkettung von NAT-Präfix (erste 96 Bit) und Client_IPv4 (letzte 32 Bit) = 2001:DB 8:90: :192.0.2.60
4. Die Appliance sendet die übersetzte IPv6-Anforderung an Sevr-IPv6.
5. Der IPv6-Server S1 antwortet, indem er ein IPv6-Paket an die Citrix ADC Appliance sendet:
   - Ziel-IP-Adressfeld = Verkettung von NAT-Präfix (erste 96 Bit) und Client_IPv4 (letzte 32 Bit) = 2001:DB 8:90: :192.0.2.60
   - Quell-IP-Adressfeld = SEVR-IPv6 = 2001:DB 8:5001: :30
6. Die Appliance empfängt das IPv6-Antwortpaket und überprüft, ob die Ziel-IP-Adresse mit dem auf der Appliance konfigurierten NAT46-Präfix übereinstimmt. Da die Zieladresse mit dem NAT46-Präfix übereinstimmt, durchsucht die Appliance die NAT46-INAT-Einträge nach der IPv4-Adresse, die der SevR-IPv6-Adresse zugeordnet ist (2001:DB 8:5001: :30). Es findet die Map-Sevr-IPv4-Adresse (192.0.2.180).
7. Die Appliance erstellt ein IPv4-Antwortpaket mit:
   - Ziel-IP-Adressenfeld = Das NAT46-Präfix, das von der Zieladresse der IPv6-Antwort entfernt wurde = Client_IPv4 (192.0.2.60)
   - Quell-IP-Adressfeld = Map-Sevr-IPv4-Adresse (192.0.2.180)
8. Die Appliance sendet die übersetzte IPv4-Antwort an Client CL1.

Einschränkungen der zustandslosen NAT46

Die folgenden Einschränkungen gelten für zustandslose NAT46:

- Die Übersetzung von IPv4-Optionen wird nicht unterstützt.
- Die Übersetzung von IPv6-Routing-Headern wird nicht unterstützt.
- Die Übersetzung von Hop-by-Hop-Erweiterungs-Headern von IPv6-Paketen wird nicht unterstützt.
- Die Übersetzung von ESP- und EH-Headern von IPv4-Paketen wird nicht unterstützt.
- Die Übersetzung von Multicastpaketen wird nicht unterstützt.
- Die Übersetzung von Zieloptionenköpfen und Quellrouting-Headern wird nicht unterstützt.
- Die Übersetzung von fragmentierten IPv4-UDP-Paketen, die keine UDP-Prüfsumme enthalten, wird nicht unterstützt.

Stateless NAT46 konfigurieren

Das Erstellen der erforderlichen Entitäten für die zustandslose NAT46-Konfiguration auf der Citrix ADC Appliance umfasst die folgenden Verfahren:

1. Erstellen Sie einen IPv4-IPv6-Zuordnungs-INAT-Eintrag mit aktiviertem zustandslosen Modus.
2. Erstellen Sie ein NAT46 IPv6-Präfix.

CLI-Verfahren

So konfigurieren Sie einen INAT Zuordnungseintrag mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add inat <name> <publicIPv4> <privateIPv6> -mode STATELESS
- show inat <name>

So erstellen Sie ein NAT46-Präfix mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- set inatparam -nat46v6Prefix <ipv6_addr|*>
- show inatparam

Beispiel:

```
 > add inat exmpl-com-stls-nat46 192.0.2.180
2001:DB8:5001::30 -mode stateless
Done

> set inatparam -nat46v6Prefix 2001:DB8:90::/96
Done
<!--NeedCopy-->
```

GUI-Verfahren

So erstellen Sie einen INAT-Zuordnungseintrag mit der GUI:

1. Navigieren Sie zu System > Netzwerk > Routen > INAT.
2. Fügen Sie einen neuen INAT Eintrag hinzu, oder bearbeiten Sie einen vorhandenen INAT Eintrag.
3. Legen Sie die folgenden Parameter fest:
    - Namen*
    - Öffentliche IP-Adresse*

- Private IP-Adresse* (Aktivieren Sie das Kontrollkästchen IPv6, und geben Sie die Adresse im IPv6-Format ein.)
- Modus (Wählen Sie Stateless aus der Dropdownliste aus.)

* Ein erforderlicher Parameter

So erstellen Sie ein NAT46-Präfix mit der GUI:

Navigieren Sie zu **System** > **Netzwerk**, klicken Sie in der Gruppe **Einstellungen auf INAT-Parameter konfigurieren**, und legen Sie den**Präfix-Parameter** fest.

Globale Parameter für stateless NAT46 festlegen

Die Appliance stellt einige optionale globale Parameter für zustandslose NAT46-Konfigurationen bereit.

So legen Sie globale Parameter für zustandslose NAT46 mit der CLI fest:

Geben Sie an der Eingabeaufforderung Folgendes ein:

set inatparam [-**Nat46IgNORETOS** (**JA**	**NEIN**)] [-**Nat46zeroChecksum** (**AKTIVIERT**	**DEAKTIVIERT**)] [-**Nat46v6MTU**] \ <positive_integer>[-**nat46FragHeader** (**AKTIVIERT**	**DEAKTIVIERT**)]

-
- **show inatparam**

Beispiel:

```
> set inatparam -nat46IgnoreTOS YES -nat46ZeroCheckSum DISABLED -
    nat46v6Mtu 1400 -nat46FragHeader DISABLED
 Done
<!--NeedCopy-->
```

So legen Sie globale Parameter für zustandslose NAT46 mit der GUI fest:

Navigieren Sie zu **System** > **Netzwerk**, klicken Sie in der Gruppe **Einstellungen** auf **INAT Parameter konfigurieren**.

DNS64

October 5, 2021

Die Citrix ADC DNS64-Funktion reagiert mit einem synthetisierten DNS-AAAA-Eintrag an einen IPv6-Client, der eine AAAA-Anforderung für eine reine IPv4-Domäne sendet. Die DNS64-Funktion wird zusammen mit der NAT64-Funktion verwendet, um eine nahtlose Kommunikation zwischen nur IPv6-Clients und nur IPv4-Servern zu ermöglichen. DNS64 ermöglicht die Erkennung der IPv4Domain durch nur IPV6-Clients, und NAT64 ermöglicht die Kommunikation zwischen den Clients und Servern.

Für die Synthese eines AAAA-Eintrags ruft die Citrix ADC Appliance einen DNS-A-Eintrag von einem DNS-Server ab. Das DNS64-Präfix ist ein 96-Bit-IPv6-Präfix, das auf der Citrix ADC Appliance konfiguriert ist. Die Citrix ADC Appliance synthetisiert den AAAA-Datensatz durch Verkettung des DNS64-Präfixes (96 Bit) und der IPv4-Adresse (32 Bit).

Um die Kommunikation zwischen IPv6-Clients und IPv4-Servern zu ermöglichen, kann eine Citrix ADC Appliance mit DNS64- und NAT64-Konfiguration entweder auf der IPv6-Clientseite oder auf der IPv4-Serverseite bereitgestellt werden. In beiden Fällen ist die DNS64-Konfiguration auf der Citrix ADC Appliance ähnlich und umfasst einen virtuellen Lastausgleichsserver, der als Proxyserver für DNS-Server fungiert. Wenn die Citrix ADC Appliance auf der Clientseite bereitgestellt wird, muss der virtuelle Lastausgleichsserver auf dem IPv6-Client als Nameserver für eine Domäne angegeben werden.

Betrachten Sie ein Beispiel, in dem eine Citrix ADC Appliance mit DNS64- und NAT64-Konfiguration auf der IPv4-Seite konfiguriert ist. In diesem Beispiel hostet ein Unternehmen Website www.example.com auf Server S1, der eine IPv4-Adresse hat. Um die Kommunikation zwischen IPv6-Clients und IPv4-Server S1 zu ermöglichen, wird die Citrix ADC Appliance NS1 mit einer DNS64- und statusbehafteten NAT64-Konfiguration bereitgestellt.

Die DNS64-Konfiguration umfasst den virtuellen DNS-Lastausgleichsserver LBVS-DNS64-1, auf dem die DNS64-Option aktiviert ist. Eine DNS64-Richtlinie mit dem Namen DNS64-Policy-1 und eine zugehörige DNS64-Aktion mit dem Namen DNS64-Action-1 werden ebenfalls auf NS1 konfiguriert und DNS64-Policy-1 ist an LBVS-DNS64-1 gebunden. LBVS-DNS64-1 fungiert als DNS-Proxyserver für DNS-Server DNS-1 und DNS-2.

Wenn der Datenverkehr, der bei LBVS-DNS64-1 eintrifft, den in DNS64-Policy-1 angegebenen Bedingungen entspricht, wird der Datenverkehr gemäß den Einstellungen in DNS64-Action-1 verarbeitet. DNS64-action-1 gibt das DNS64-Präfix an, das mit dem A-Eintrag, der von einem DNS-Server empfangen wird, zum Synthesisieren eines AAAA-Eintrags verwendet wird.

Die globalen DNS-Parametercacherecords sind auf der Citrix ADC Appliance aktiviert, sodass die Appliance DNS-Einträge zwischenspeichert. Diese Einstellung ist erforderlich, damit der DNS64 ordnungsgemäß funktioniert.

In der folgenden Tabelle sind die im obigen Beispiel verwendeten Einstellungen aufgeführt: DNS64-

Beispieleinstellungen.

Es folgt der Verkehrsfluss in diesem Beispiel:

1. IPv6-Client CL1 sendet eine DNS-AAAA-Anforderung für die IPv6-Adresse der Website www.example.com.
2. Die Anforderung wird vom virtuellen DNS-Lastausgleichsserver LBVS-DNS64-1 auf der Citrix ADC Appliance NS1 empfangen.
3. NS1 überprüft seine DNS-Cache-Einträge für den angeforderten AAAA-Eintrag und stellt fest, dass AAAA-Eintrag für die Website www.beispiel.com nicht im DNS-Cache vorhanden ist.
4. Der Lastausgleichsalgorithmus von LBVS-DNS64-1 wählt DNS-Server DNS-1 aus und leitet die AAAA-Anforderung an ihn weiter.
5. Da die Website www.example.com auf einem IPv4-Server gehostet wird, verfügt der DNS-Server DNS-1 über keinen AAAA-Eintrag für die Website www.example.com.
6. DNS-1 sendet entweder eine leere DNS-AAAA-Antwort oder eine Fehlermeldung an LBVS-DNS64-1.
7. Da DNS64-Option auf LBVS-DNS64-1 aktiviert ist und die AAAA-Anforderung von CL1 der in DNS64-Policy-1 angegebenen Bedingung entspricht, sendet NS1 eine DNS-A-Anforderung für die IPv4-Adresse von www.example.com an DNS-1.
8. DNS-1 antwortet, indem der DNS-A-Eintrag für www.example.com an LBVS-DNS64-1 gesendet wird. Der A-Eintrag enthält die IPv4-Adresse für www.example.com.
9. NS1 synthetisiert einen AAAA-Eintrag für die Website www.example.com mit:
    - IPv6-Adresse für Website www.example.com = Verkettung des DNS64-Präfixes (96 Bit), das in der zugehörigen DNS64Action angegeben ist, und IPv4-Adresse des DNS-A-Datensatzes (32 Bit) = 2001:DB 8:300: :192.0.2.60
10. NS1 sendet den synthetisierten AAAA-Datensatz an den IPv6-Client CL1. NS1 speichert auch den A-Datensatz in seinen Speicher. NS1 verwendet den zwischengespeicherten A-Datensatz, um AAAA-Datensätze für nachfolgende AAAA-Anforderungen zu synthetisieren.

Zu berücksichtigende Punkte für eine DNS64-Konfiguration

Berücksichtigen Sie vor der Konfiguration von DNS64 auf einer Citrix ADC Appliance die folgenden Punkte:

- Die DNS64-Funktion der Citrix ADC Appliance ist mit RFC 6174 kompatibel.
- Die DNS64-Funktion der Citrix ADC Appliance unterstützt DNSSEC nicht. Die Citrix ADC Appliance synthetisiert keinen AAAA-Eintrag aus einer DNSSEC-Antwort, die von einem DNS-Server empfangen wurde. Eine Antwort wird nur dann als DNSSEC-Antwort klassifiziert, wenn sie RRSIG-Datensätze enthält.
- Die Citrix ADC Appliance unterstützt das DNS64-Präfix mit einer Länge von nur 96 Bit.

- Obwohl die DNS64-Funktion mit der NAT64-Funktion verwendet wird, sind die Konfigurationen DNS64 und NAT64 unabhängig von der Citrix ADC Appliance. Für einen bestimmten Flow müssen Sie denselben IPv6-Präfixwert für das DNS64-Präfix und die NAT64-Präfixparameter angeben, damit die vom Client empfangenen synthetisierten IPv6-Adressen an die bestimmte NAT64-Konfiguration weitergeleitet werden. Weitere Informationen zum Konfigurieren von NAT64 auf einer Citrix ADC Appliance finden Sie unter Stateful NAT64.
- Im Folgenden sind die verschiedenen Fälle der DN64-Verarbeitung durch die Citrix ADC Appliance aufgeführt:
  - Wenn die AAAA-Antwort vom DNS-Server AAAA-Einträge enthält, wird jeder Datensatz in der Antwort auf den Satz der Ausschlussregel überprüft, der auf der Citrix ADC Appliance für die jeweilige DNS64-Konfiguration konfiguriert ist. Citrix ADC entfernt die IPv6-Adressen, deren Präfix mit der Ausschlussregel übereinstimmt, aus der Antwort. Wenn die resultierende Antwort mindestens einen IPv6-Eintrag enthält, leitet die Citrix ADC Appliance diese Antwort an den Client weiter. Andernfalls synthetisiert die Appliance eine AAAA-Antwort aus dem A-Datensatz der Domäne und sendet sie an den IPv6-Client.
  - Wenn die AAAA-Antwort vom DNS-Server eine leere Antwortantwort ist, fordert die Appliance nach A-Ressourceneinträgen mit demselben Domänennamen an oder sucht in eigenen Datensätzen, wenn es sich bei der Appliance um einen authentischen Domänennamenserver für die Domäne handelt. Wenn die Anfrage zu einer leeren Antwort oder einem leeren Fehler führt, wird diese an den Client weitergeleitet.
  - Wenn die Antwort des DNS-Servers RCODE=1 (Formatfehler) enthält, leitet die Citrix ADC Appliance dasselbe an den Client weiter. Wenn vor dem Timeout keine Antwort auftritt, sendet die Citrix ADC Appliance eine Antwort mit RCODE=2 (Serverfehler) an den Client.
  - Wenn die Antwort des DNS-Servers einen CNAME enthält, wird die Kette verfolgt, bis der abschließende A- oder AAAA-Eintrag erreicht ist. Wenn der CNAME keine AAAA-Ressourceneinträge enthält, ruft die Citrix ADC Appliance den DNS-A-Eintrag ab, der für die Synthese von AAAA-Einträgen verwendet werden soll. Die CNAME-Kette wird zusammen mit dem synthetisierten AAAA-Datensatz zum Antwortbereich hinzugefügt und dann an den Client gesendet.
- Die DNS64-Funktion der Citrix ADC Appliance unterstützt auch das Beantworten von PTR-Anfragen. Wenn eine PTR-Anforderung für eine Domäne einer IPv6-Adresse auf der Appliance empfangen wird und die IPv6-Adresse einem der konfigurierten DNS64-Präfix entspricht, erstellt die Appliance einen CNAME-Datensatz, der die IP6-ARPA-Domäne dem entsprechenden IN-ADDR zugeordnet. Die ARPA-Domäne und die neu gebildete IN-ADDR.ARPA-Domäne werden zur Auflösung verwendet. Die Appliance durchsucht die lokalen PTR-Einträge, und wenn die Datensätze nicht vorhanden sind, sendet die Appliance eine PTR-Anforderung für die IN-ADDR.ARPA-Domäne an den DNS-Server. Die Citrix ADC Appliance verwendet die Antwort des DNS-Servers, um die Antwort für die ursprüngliche PTR-Anforderung zu synthetisieren.

Konfigurationsschritte

Das Erstellen der erforderlichen Entitäten für die statusbehaftete NAT64-Konfiguration auf der Citrix ADC Appliance umfasst die folgenden Verfahren:

- **Fügen Sie DNS-Dienste hinzu.** DNS-Dienste sind logische Darstellung von DNS-Servern, für die die Citrix ADC Appliance als DNS-Proxyserver fungiert. Weitere Informationen zum Festlegen optionaler Parameter eines Dienstes finden Sie unter Load Balancing.
- **Fügen Sie DNS64-Aktion und DNS64-Richtlinie hinzu, und binden Sie dann die DNS64-Aktion an die DNS64-Richtlinie.** Eine DNS64-Richtlinie legt Bedingungen fest, die mit dem Datenverkehr für die DNS64-Verarbeitung gemäß den Einstellungen in der zugeordneten DNS64-Aktion abgeglichen werden sollen. Die DNS64-Aktion gibt das obligatorische DNS64-Präfix sowie die optionalen Ausschlussregel und zugeordnete Regeleinstellungen an.
- **Erstellen Sie einen virtuellen DNS-Lastausgleichsserver und binden Sie die DNS-Dienste und die DNS64-Richtlinie daran.** Der virtuelle DNS-Lastenausgleichsserver fungiert als DNS-Proxyserver für DNS-Server, die durch die gebundenen DNS-Dienste dargestellt werden. Datenverkehr, der auf dem virtuellen Server eintrifft, wird mit der gebundenen DNS64-Richtlinie für die DNS64-Verarbeitung abgeglichen. Weitere Informationen zum Festlegen optionaler Parameter eines virtuellen Lastausgleichsservers finden Sie unter Load Balancing.

  Hinweis: Die CLI verfügt über separate Befehle für diese beiden Aufgaben, aber die GUI kombiniert sie in einem einzigen Dialogfeld.

  Aktivieren Sie das Zwischenspeichern von DNS-Datensätzen. Aktivieren Sie den globalen Parameter für die Citrix ADC Appliance, um DNS-Einträge zwischenzuspeichern, die über DNS-Proxyvorgänge abgerufen werden. Weitere Informationen zum Aktivieren des Zwischenspeichers von DNS-Datensätzen finden Sie unter Domänennamensystem.

CLI-Verfahren

So erstellen Sie einen Dienst vom Typ DNS mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add service <name> <IP> <serviceType> <port> …

So erstellen Sie eine DNS64-Aktion mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add dns action64 <actionName>-Präfix <ipv6_addr|*> [-mappeDrule] <expression>[-ExcludeRule]<expression>

So erstellen Sie eine DNS64-Richtlinie mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add dns policy64 <name> -rule <expression> -action <string>

So erstellen Sie einen virtuellen DNS-Load Balancing Server mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add lb vserver <name>DNS <IPAddress><port>-dns64 (ENABLED | DEAKTIVIERT) [-BypassaAAA (JA | NEIN)]…

So binden Sie die DNS-Dienste und die DNS64-Richtlinie an den virtuellen DNS-Lastausgleichsserver mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- bind lb vserver <name> <serviceName> …
- bind lb vserver <name> -policyName <string> -priority <positive_integer> …

GUI-Verfahren

So erstellen Sie einen Dienst vom Typ DNS mit der GUI:

1. Navigieren Sie zu Traffic Management > Load Balancing > Services, und fügen Sie einen neuen Dienst hinzu.
2. Legen Sie die folgenden Parameter fest:
   - Servicename*
   - Server*
   - Protokoll* (Wählen Sie DNS aus der Dropdownliste aus.)
   - Port*

So erstellen Sie eine DNS64-Aktion mit der GUI:

Navigieren Sie zu Verkehrsverwaltung > DNS > Aktionen, fügen Sie auf der Registerkarte DNS-Aktionen64 eine neue DNS64-Aktion hinzu.

So erstellen Sie eine DNS64-Richtlinie mit der GUI:

Navigieren Sie zu Verkehrsverwaltung > DNS > Richtlinien. Fügen Sie auf der Registerkarte DNS-Richtlinien64 eine neue DNS64-Richtlinie hinzu.

So erstellen Sie einen virtuellen DNS-Lastenausgleichsserver und binden die DNS-Dienste und die DNS64-Richtlinie mit der GUI daran:

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server, und fügen Sie einen neuen virtuellen Server hinzu.
2. Legen Sie die folgenden Parameter fest:
   - Namen*
   - IP-Adresse*
   - Protokoll* (Wählen Sie DNS aus der Dropdownliste aus.)

- Port*

3. Wählen Sie die Option DNS64 aktivieren.
4. Binden Sie den Dienst im Bereich Dienste an den virtuellen Server.
5. Binden Sie die Richtlinie im Bereich Richtlinien an den virtuellen Server.

Beispielkonfiguration

```
 > add service SVC-DNS-1 203.0.113.50 DNS 53
 Done

> add service SVC-DNS-2 203.0.113.60 DNS 53
 Done

> add dns Action64 DNS64-Action-1 -Prefix 2001:DB8:300::/96
 Done

> add dns Policy64 DNS64-Policy-1 -rule ”CLIENT.IPv6.SRC.IN_SUBNET
   (2001:DB8:5001::/64)”
-action DNS64-Action-1
 Done

> add lb vserver LBVS-DNS64-1 DNS 2001:DB8:9999::99 53 -dns64 ENABLED
 Done

> bind lb vserver LBVS-DNS64-1 SVC-DNS-1
 Done

> bind lb vserver LBVS-DNS64-1 SVC-DNS-2
 Done

> bind lb vserver LBVS-DNS64-1 -policyname DNS64-Policy-1 -priority 2
 Done

<!--NeedCopy-->
```

Stateful-NAT64-Übersetzung

October 5, 2021

Die statusbehaftete NAT64-Funktion ermöglicht die Kommunikation zwischen IPv6-Clients und IPv4-Servern über IPv6- zu IPv4-Paketübersetzung und umgekehrt, während die Sitzungsinformationen

auf der Citrix ADC Appliance beibehalten werden.

Eine statusbehaftete NAT64-Konfiguration auf der Citrix ADC Appliance besteht aus folgenden Komponenten:

- **NAT64-Regel**— Ein Eintrag, der aus einer ACL6-Regel und einem Netzprofil besteht, der aus einem Pool von Citrix ADC eigenen SNIP-Adressen besteht.
- **NAT64 IPv6-Präfix**— Ein globales IPv6-Präfix der Länge 96 Bit (128-32=96), das auf der Appliance konfiguriert ist.
  Hinweis: Derzeit unterstützt die Citrix ADC Appliance nur ein Präfix, das häufig mit allen NAT 64-Regeln verwendet wird.

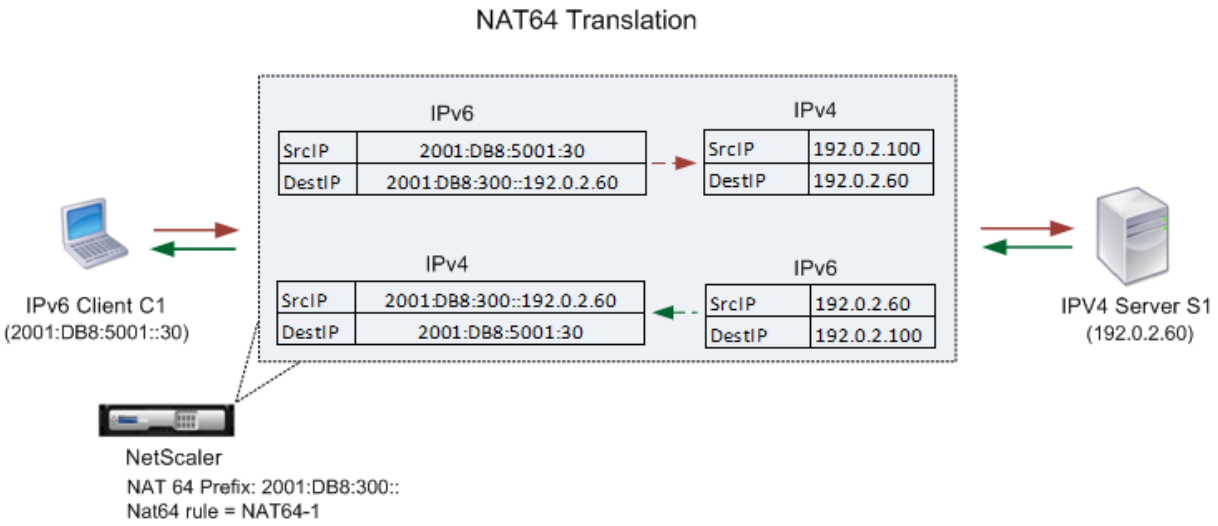
Die Citrix ADC Appliance berücksichtigt ein eingehendes IPv6-Paket für die NAT64-Übersetzung, wenn alle folgenden Bedingungen erfüllt sind:

- Das eingehende IPv6-Paket entspricht der ACL6-Regel, die an eine NAT64-Regel gebunden ist.
- Die Ziel-IP-Adresse des IPv6-Pakets entspricht dem NAT64-IPv6-Präfix.

Wenn ein von der Citrix ADC Appliance empfangenes IPv6-Anforderungspaket mit einem in einer NAT64-Regel definierten ACL6 übereinstimmt und die Ziel-IP des Pakets mit dem NAT64-IPv6-Präfix übereinstimmt, berücksichtigt die Citrix ADC-Appliance das IPv6-Paket zur Übersetzung.

Die Appliance übersetzt dieses IPv6-Paket in ein IPv4-Paket mit einer Quell-IP-Adresse, die einer der IP-Adresse entspricht, die an das in der NAT64-Regel definierte Netzprofil gebunden ist, und einer Ziel-IP-Adresse, die aus den letzten 32 Bits der Ziel-IPv6-Adresse des IPv6-Anforderungspakets besteht. Die Citrix ADC Appliance erstellt eine NAT64-Sitzung für diesen bestimmten Flow und leitet das Paket an den IPv4-Server weiter. Nachfolgende Antworten vom IPv4-Server und Anfragen vom IPv6-Client werden entsprechend von der Appliance übersetzt, basierend auf Informationen in der jeweiligen NAT64-Sitzung.

Betrachten Sie ein Beispiel, in dem ein Unternehmen Website www.example.com auf Server S1 hostet, der eine IPv4-Adresse hat. Um die Kommunikation zwischen IPv6-Clients und IPv4-Server S1 zu ermöglichen, wird die Citrix ADC Appliance NS1 mit einer statusbehafteten NAT64-Konfiguration bereitgestellt, die eine NAT64-Regel und ein NAT64-Präfix enthält. Eine zugeordnete IPv6-Adresse des Servers S1 wird gebildet, indem das NAT64 IPv6-Präfix [96 Bit] und die IPv4-Quelladresse [32 Bit]verkettet wird. Diese zugeordnete IPv6-Adresse wird dann manuell auf den DNS-Servern konfiguriert. Die IPv6-Clients erhalten die zugeordnete IPv6-Adresse von den DNS-Servern, um mit IPv4-Server S1 zu kommunizieren.



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt: Beispieleinstellungen für Stateful NAT64.

Es folgt der Verkehrsfluss in diesem Beispiel:

1. IPv6-Client CL1 sendet ein Anforderungspaket an Map-Sevr-IPv6 (2001:DB 8:300::192.0.2.60) Adresse.
2. Die Citrix ADC Appliance empfängt das Anforderungspaket. Wenn das Anforderungspaket mit dem in der NAT64-Regel definierten ACL6 übereinstimmt und die Ziel-IP-Adresse des Pakets mit dem NAT64-IPv6-Präfix übereinstimmt, berücksichtigt Citrix ADC das IPv6-Paket zur Übersetzung.
3. Die Appliance erstellt ein übersetztes IPv4-Anforderungspaket mit:
   - Ziel-IP-Adressfeld, das das NAT64-Präfix enthält, das von der Zieladresse der IPv6-Anforderung entfernt wurde (SEVR_IPv4 = 192.0.2.60)
   - Quell-IP-Adressfeld, das eine der an Netprofile-1 gebundenen IPv4-Adresse enthält (in diesem Fall 192.0.2.100)
4. Die Citrix ADC Appliance erstellt eine NAT64-Sitzung für diesen Flow und sendet die übersetzte IPv4-Anforderung an den Server S1.
5. IPv64-Server S1 antwortet, indem ein IPv4-Paket an die Citrix ADC Appliance gesendet wird:
   - Ziel-IP-Adressfeld mit 192.0.2.100
   - Quell-IP-Adressfeld mit der Adresse vonSevr_IPv4 (192.0.2.60)
6. Die Appliance empfängt das IPv4-Antwortpaket, durchsucht alle Sitzungseinträge und stellt fest, dass das IPv6-Antwortpaket mit dem in Schritt 4 erstellten NAT64-Sitzungseintrag übereinstimmt. Die Appliance berücksichtigt das IPv4-Paket zur Übersetzung.
7. Die Appliance erstellt ein übersetztes IPv6-Antwortpaket mit:

- Destination IP address field=Client_IPv6=2001:DB8:5001::30
- Source IP address field = Concatenation of NAT64 Prefix (First 96 bits) and Sevr_IPv4 (last 32 bits) =2001:DB8:300::192.0.2.60

8. Die Appliance sendet die übersetzte IPv6-Antwort an Client CL1.

Einschränkungen der Statelful NAT64

Die folgenden Einschränkungen gelten für statusbehaftete NAT64:

- Die Übersetzung von IPv4-Optionen wird nicht unterstützt.
- Die Übersetzung von IPv6-Routing-Headern wird nicht unterstützt.
- Die Übersetzung von Hop-by-Hop-Erweiterungs-Headern von IPv6-Paketen wird nicht unterstützt.
- Die Übersetzung von ESP- und EH-Headern von IPv6-Paketen wird nicht unterstützt.
- Die Übersetzung von Multicastpaketen wird nicht unterstützt.
- Pakete von SCTP (Stream Control Transmission Protocol), Datagram Congestion Control Protocol (DCCP) und IPsec werden nicht übersetzt.

Stateful NAT64 konfigurieren

Das Erstellen der erforderlichen Entitäten für die statusbehaftete NAT64-Konfiguration auf der Citrix ADC Appliance umfasst die folgenden Verfahren:

1. Fügen Sie eine ACL6-Regel mit der Aktion Allow hinzu.
2. Fügen Sie ein ipset hinzu, das mehrere IP-Adressen bindet.
3. Fügen Sie ein Netzprofil hinzu und binden Sie das ipset daran. Wenn Sie nur eine IP-Adresse binden möchten, müssen Sie keine ipset-Entität erstellen. Binden Sie in diesem Fall die IP-Adresse direkt an das Netzprofil.
4. Fügen Sie eine NAT64-Regel hinzu, die die ACl6-Regel und das Netprofile an die NAT 64-Regel bindet.
5. Fügen Sie ein NAT64-IPv6-Präfix hinzu.

CLI-Verfahren

So fügen Sie eine ACL6-Regel mit der CLI hinzu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add ns acl6 <acl6name> <acl6action> …

So fügen Sie ein IPSet hinzu und binden mehrere IPs mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add ipset <name>
- bind ipset <name> <IPaddress …>

So fügen Sie ein Netprofil mit der Befehlszeilenschnittstelle hinzu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add netprofile <name> -srcIP <IPaddress or IPset>

So fügen Sie eine NAT64-Regel mit der CLI hinzu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add nat64 <name> <acl6name> -netProfile <string>

So fügen Sie mit der CLI ein NAT64-Präfix hinzu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- set ipv6 -natprefix <ipv6_addr|*>

Beispiel:

```
 > add acl6 ACL6-1 ALLOW -srcIPv6 2001:DB8:5001::30
 Done

> apply acls6
 Done

> add ip 192.0.2.100 255.255.255.0  - type SNIP
 Done

> add ip 192.0.2.102 255.255.255.0   - type SNIP
 Done

> add ipset IPset-1
 Done

> bind ipset IPset-1 192.0.2.100 192.0.2.102
IPAddress ”192.0.2.100” bound
IPAddress ”192.0.2.102” bound
 Done

> add netprofile Netprofile-1 -srcIP IPset-1
 Done

> add nat64 NAT64-1 ACL6-1 -netprofile Netprofile-1
 Done
```



```
26
27 > set ipv6 -natprefix 2001:DB8:300::/96
28  Done
29 <!--NeedCopy-->
```

GUI-Verfahren

So fügen Sie mit der GUI eine NAT64-Regel hinzu:

Navigieren Sie zu System > Netzwerk > Routen > NAT64 und zu einer neuen NAT64-Regel, oder bearbeiten Sie eine vorhandene Regel.

So fügen Sie mit der GUI ein NAT64-Präfix hinzu:

Navigieren Sie zu System > Netzwerk, klicken Sie in der Gruppe Einstellungen auf INAT-Parameter konfigurieren, und legen Sie den Präfix-Parameter fest.

RNAT

October 5, 2021

In der Reverse Network Address Translation (RNAT) ersetzt die Citrix ADC Appliance die Quell-IP-Adressen in den von den Servern generierten Paketen durch öffentliche NAT-IP-Adressen. Standardmäßig verwendet die Appliance eine SNIP-Adresse als NAT-IP-Adresse. Sie können die Appliance auch so konfigurieren, dass sie für jedes Subnetz eine eindeutige NAT-IP-Adresse verwendet. Sie können RNAT auch mithilfe von Zugriffssteuerungslisten (Access Control Lists, ACLs) konfigurieren. Die Modi Source IP (USIP), Use Subnet IP (USNIP) und Link Load Balancing (LLB) beeinflussen den Betrieb von RNAT. Sie können Statistiken anzeigen, um RNAT zu überwachen.

Hinweis: Der flüchtige Portbereich für RNAT der Citrix ADC Appliance beträgt 1024-65535.

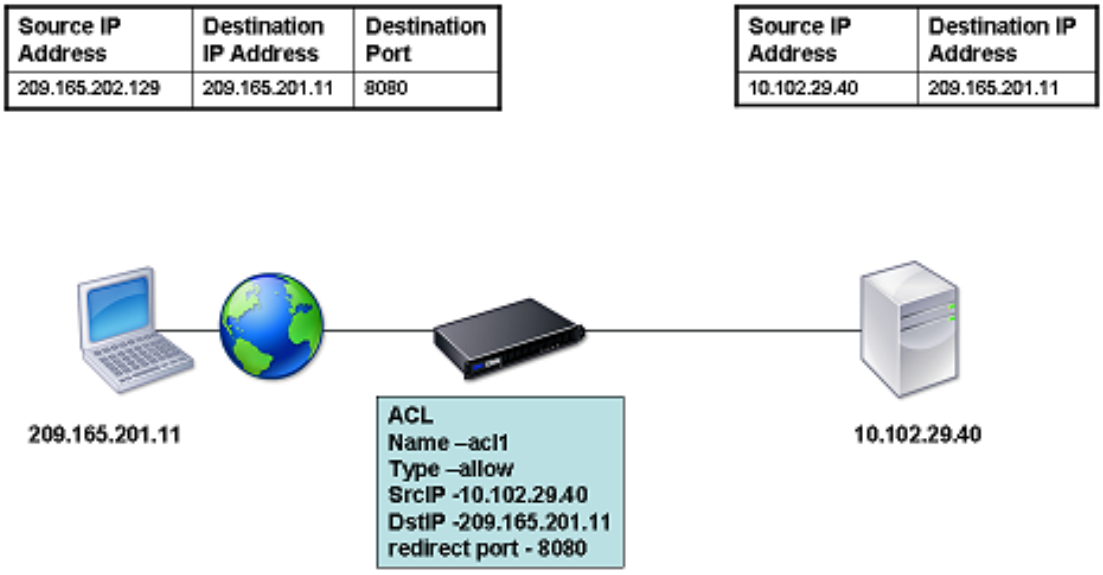
Sie können entweder eine Netzwerkadresse oder eine erweiterte ACL als Bedingung für einen RNAT Eintrag verwenden:

- **Verwenden einer Netzwerkadresse.** Wenn Sie eine Netzwerkadresse verwenden, wird die RNAT Verarbeitung für alle Pakete durchgeführt, die aus dem angegebenen Netzwerk stammen.
- **Verwenden von erweiterten ACLs.** Wenn Sie ACLs verwenden, wird die RNAT Verarbeitung für alle Pakete durchgeführt, die den ACLs entsprechen. Um die Citrix ADC Appliance so zu konfigurieren, dass eine eindeutige IP-Adresse für Datenverkehr verwendet wird, der mit einer ACL übereinstimmt, müssen Sie die folgenden drei Aufgaben ausführen:
  1. Konfigurieren Sie die ACL.
  2. Konfigurieren Sie RNAT, um die Quell-IP-Adresse und den Zielport zu ändern.

3. Wenden Sie die ACL an.

Das folgende Diagramm veranschaulicht die mit einer ACL konfigurierte RNAT.

Abbildung 1. RNAT mit ACL

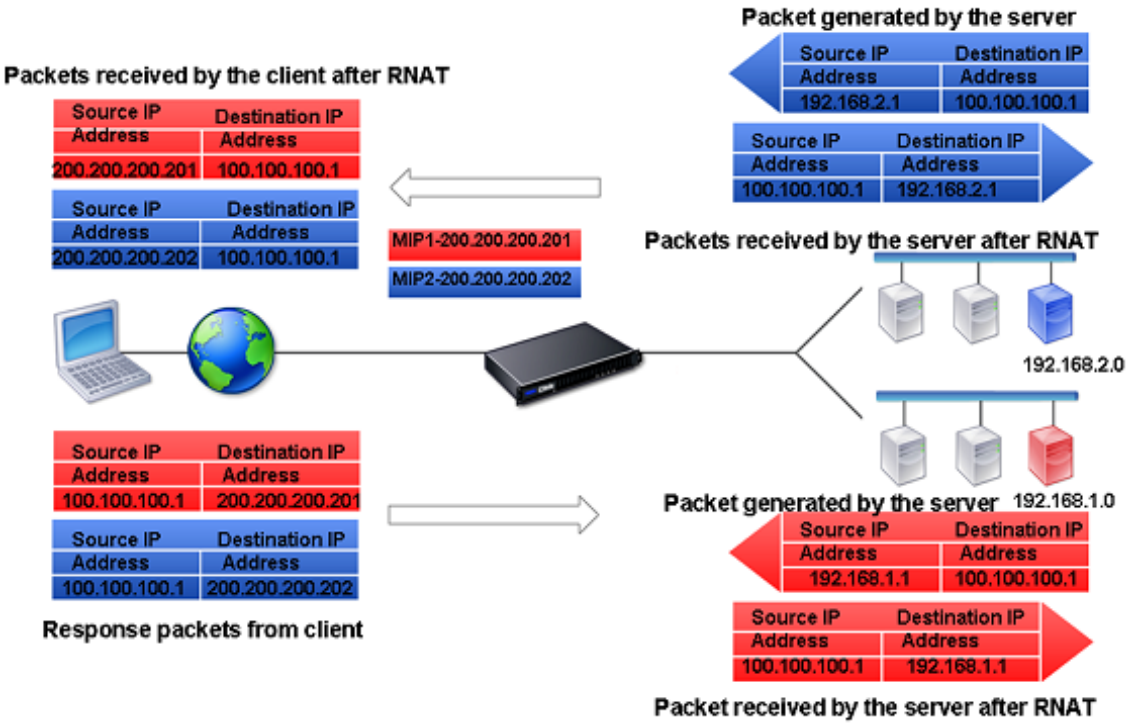


Sie haben die folgenden grundlegenden Optionen für den Typ der NAT-IP-Adresse:

- **Verwenden eines SNIP als NAT-IP-Adresse.** Wenn Sie ein SNIP als NAT-IP-Adresse verwenden, ersetzt die Citrix ADC Appliance die Quell-IP-Adressen von servergenerierten Paketen durch ein SNIP. Daher muss die SNIP-Adresse eine öffentliche IP-Adresse sein. Wenn Use Subnet IP (USNIP) -Modus aktiviert ist, kann Citrix ADC eine Subnetz-IP-Adresse (SNIP) als NAT-IP-Adresse verwenden.
- **Verwenden einer eindeutigen IP-Adresse als NAT-IP-Adresse.** Bei Verwendung einer eindeutigen IP-Adresse als NAT-IP-Adresse ersetzt die Citrix ADC Appliance die Quell-IP-Adressen von servergenerierten Paketen durch die angegebene eindeutige IP-Adresse. Die eindeutige IP-Adresse muss eine öffentliche Citrix ADC-eigene IP-Adresse sein. Wenn mehrere NAT-IP-Adressen für ein Subnetz konfiguriert sind, verwendet die NAT-IP-Auswahl den Roundrobin-Algorithmus.

  Diese Konfiguration wird im folgenden Diagramm veranschaulicht.

  Abbildung 2. Verwenden einer eindeutigen IP-Adresse als NAT-IP-Adresse



Voraussetzungen

Berücksichtigen Sie vor der Konfiguration einer RNAT Regel die folgenden Punkte:

- Wenn RNAT und Use Source IP (USIP) auf der Citrix ADC Appliance konfiguriert sind, hat RNAT Vorrang. Mit anderen Worten, die Quell-IP-Adresse der Pakete, die einer RNAT Regel entspricht, wird entsprechend der Einstellung in der RNAT Regel ersetzt.
- In einer Topologie, in der die Citrix ADC Appliance sowohl Link Load Balancing (LLB) als auch RNAT für den vom Server ausgehenden Datenverkehr ausführt, wählt die Appliance die Quell-IP-Adresse basierend auf dem Router aus. Die LLB-Konfiguration bestimmt die Auswahl des Routers. Weitere Informationen zu LLB finden Sie unter Link-Lastenausgleich.

RNAT konfigurieren

Die folgenden Anweisungen enthalten separate Befehlszeilenprozeduren zum Erstellen von RNAT Einträgen, die unterschiedliche Bedingungen und verschiedene Arten von NAT-IP-Adressen verwenden. In der GUI können alle Variationen im selben Dialogfeld konfiguriert werden, so dass es nur eine Prozedur für GUI-Benutzer gibt.

CLI-Verfahren

So erstellen Sie eine RNAT Regel mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein, um die Regel zu erstellen und die Konfiguration zu überprüfen:

- `add rnat <name> (<network> | (<aclname> [-redirectPort <port>]))`
- `bind rnat <name> <natIP>@ …`
- `show rnat`

So ändern oder entfernen Sie eine RNAT Regel mit der CLI:

- So ändern Sie eine RNAT Regel:

  `set rnat <name> (<aclname> [-redirectPort <port>])`

- Um eine RNAT-Regel zu entfernen, geben Sie den Befehl ein.

  `rm rnat <name>`

Verwenden Sie den folgenden Befehl, um die Konfiguration zu überprüfen:

- `show rnat`

Beispiele:

```
A network address as the condition and a SNIP address as the NAT IP address:

> add rnat RNAT-1 192.168.1.0 255.255.255.0
Done

A network address as the condition and a unique IP address as the NAT IP address:

> add rnat RNAT-2 192.168.1.0 255.255.255.0
Done

> bind rnat RNAT-2 -natip 10.102.29.50
Done

If instead of a single NAT IP address you specify a range, RNAT entries are created with all the Citrix ADC-owned IP addresses, except the NSIP, that fall within the range specified:

> add rnat RNAT-3 192.168.1.0 255.255.255.0
Done

> bind rnat RNAT-3 -natip 10.102.29.[50-110]
Done
```



```
21
22
23 An ACL as the condition and a SNIP address as the NAT IP address:
24
25 > add rnat RNAT-4 acl1
26 Done
27
28 An ACL as a condition and a unique IP address as the NAT IP address:
29
30 > add rnat RNAT-4 acl1
31 Done
32
33 > bind rnat RNAT-4 -natip 10.102.29.50
34 Done
35
36 If instead of a single NAT IP address you specify a range, RNAT entries
       are created with all the Citrix ADC-owned IP addresses, except the
     NSIP, that fall within the range specified:
37
38 > add rnat RNAT-5 acl1
39 Done
40
41 > bind rnat RNAT-5 -natip 10.102.29.[50-70]
42 Done
43
44 <!--NeedCopy-->
```

GUI-Verfahren

So erstellen Sie einen RNAT Eintrag mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **NATs**, klicken Sie auf die Registerkarte **RNAT**, und fügen Sie eine neue RNAT Regel hinzu, oder bearbeiten Sie eine vorhandene Regel.

Überwachen RNAT

Sie können RNAT-Statistiken anzeigen, um Probleme im Zusammenhang mit der IP-Adressenübersetzung zu beheben.

In der folgenden Tabelle werden die mit RNAT und RNAT IP verbundenen Statistiken beschrieben.

Statistische	Beschreibung
Empfangene Bytes	Während RNAT-Sitzungen empfangene Bytes

Statistische	Beschreibung
Gesendete Bytes	Bytes, die während RNAT-Sitzungen gesendet werden
Empfangene Pakete	Während RNAT-Sitzungen empfangene Pakete
Gesendete Pakete	Pakete, die während RNAT-Sitzungen gesendet werden
Syn hat gesendet	Anfragen für Verbindungen, die während RNAT-Sitzungen gesendet werden
Aktuelle Sitzungen	Derzeit aktive RNAT Sitzungen

So zeigen Sie RNAT Statistiken mit der CLI an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **Statistik rnat**

Beispiel:

```
> stat rnat

RNAT summary
                                Rate (/s)            Total
Bytes Received                    0                    0
Bytes Sent                        0                    0
Packets Received                  0                    0
Packets Sent                      0                    0
Syn Sent                          0                    0
Current RNAT sessions            --                    0
 Done
>
<!--NeedCopy-->
```

So überwachen Sie RNAT mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **NATs**, klicken Sie auf die Registerkarte **RNAT**, und klicken Sie dann auf **Statistiken** .

RNAT6 konfigurieren

RNAT (Reverse Network Address Translation) -Regeln für IPv6-Pakete werden RNAT6s genannt. Wenn ein von einem Server generiertes IPv6-Paket den in der RNAT6-Regel angegebenen Bedingungen

entspricht, ersetzt die Appliance die Quell-IPv6-Adresse des IPv6-Pakets durch eine konfigurierte NAT-IPv6-Adresse, bevor sie an das Ziel weiterleitet. Die NAT IPv6-Adresse ist eine der Citrix ADC Adressen im Besitz der SNIP6- oder VIP6-Adressen.

Beim Konfigurieren einer RNAT6-Regel können Sie entweder ein IPv6-Präfix oder eine ACL6 als Bedingung angeben:

- **Verwenden einer IPv6-Netzwerkadresse**. Wenn Sie ein IPv6-Präfix verwenden, führt die Appliance RNAT für die IPv6-Pakete durch, deren IPv6-Adresse mit dem Präfix übereinstimmt.
- **Verwenden von ACL6s**. Wenn Sie eine ACL6 verwenden, führt die Appliance RNAT für die IPv6-Pakete aus, die den in ACL6 angegebenen Bedingungen entsprechen.

Sie haben eine der folgenden Optionen, um die NAT-IP-Adresse festzulegen:

- Geben Sie einen Satz von Citrix ADC Adressen im Besitz von SNIP6- und VIP6-Adressen für eine RNAT6-Regel an. Die Citrix ADC Appliance verwendet eine der IPv6-Adressen aus diesem Satz als NAT-IP-Adresse für jede Sitzung. Die Auswahl basiert auf dem Roundrobin-Algorithmus und wird für jede Sitzung durchgeführt.
- Geben Sie für eine RNAT6-Regel keine SNIP6- oder VIP6-Adresse im Besitz von Citrix ADC an. Die Citrix ADC Appliance verwendet eine der Citrix ADC eigenen SNIP6- oder VIP6-Adressen als NAT-IP-Adresse. Die Auswahl basiert auf dem Next Hop-Netzwerk, für das ein IPv6-Paket bestimmt ist, das der RNAT Regel entspricht.

CLI-Verfahren

So erstellen Sie eine RNAT6-Regel mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein, um die Regel zu erstellen und die Konfiguration zu überprüfen:

- **füge rnat6** hinzu <name>(<network>| (<acl6name>[-**RedirectPort**]<port>))
- **bind rnat6** <name> <natIP6>@ …
- **show rnat6**

So ändern oder entfernen Sie eine RNAT6-Regel mit der CLI:

- Um eine RNAT6-Regel zu ändern, deren Bedingung eine ACL6 ist, geben Sie den <name> Befehl **set rnat6** ein, gefolgt von einem neuen Wert für den Parameter **RedirectPort** .
- Um eine RNAT6-Regel zu entfernen, geben Sie den <name> Befehl **clear rnat6** ein.

GUI-Verfahren

So konfigurieren Sie eine RNAT6-Regel mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **NATs**, klicken Sie auf die Registerkarte **RNAT6**, und fügen Sie eine neue RNAT6-Regel hinzu, oder bearbeiten Sie eine vorhandene Regel.

Überwachen Sie RNAT6

Sie können Statistiken im Zusammenhang mit der RNAT6-Funktion anzeigen, um die Leistung zu überwachen oder Probleme im Zusammenhang mit der RNAT6-Funktion zu beheben. Sie können eine Zusammenfassung der Statistiken der RNAT6-Regeln oder einer bestimmten RNAT6-Regel anzeigen. Die statistischen Leistungsindikatoren spiegeln Ereignisse seit dem letzten Neustart der Citrix ADC Appliance wider. Alle diese Leistungsindikatoren werden auf 0 zurückgesetzt, wenn die Citrix ADC Appliance neu gestartet wird.

Im Folgenden werden einige der Statistikindikatoren aufgeführt, die mit der RNAT6-Funktion verknüpft sind:

- **Empfangene Bytes** - Gesamtzahl der während RNAT6-Sitzungen empfangenen Bytes.
- **Gesendete Bytes** - Gesamtanzahl der während RNAT6-Sitzungen gesendeten Bytes.
- **Empfangene Pakete** - Gesamtanzahl der während RNAT6-Sitzungen empfangenen Pakete.
- **Gesendete Pakete** - Gesamtanzahl der während RNAT6-Sitzungen gesendeten Pakete.
- **Syn sent** - Gesamtzahl der Anfragen für Verbindungen, die während RNAT6-Sitzungen gesendet wurden
- **Aktuelle Sitzungen** - Derzeit aktive RNAT6-Sitzungen

So zeigen Sie eine zusammengefasste Statistik aller RNAT6-Regeln mit der CLI an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **stat rnat6**

So zeigen Sie Statistiken für eine angegebene RNAT6-Regel mit der Befehlszeilenschnittstelle an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **stat rnat6** []<rnat6 rule name>

So zeigen Sie RNAT6-Statistiken mit der GUI an:

Navigieren Sie zu **System** > **Netzwerk** > **NATs**, klicken Sie auf die Registerkarte **RNAT6**, und klicken Sie dann auf **Statistiken** .

```
1  > stat rnat6
2
3  RNAT6 summary
4
5                            Rate (/s)               Total
6
7  Bytes Received             178                 20644
8
9  Bytes Sent                 178                 20644
10
```



```
11 Packets Received              5                   401
12
13 Packets Sent                  5                   401
14
15 Syn Sent                      0                     2
16
17 Current RNAT6 sessions       --                     1
18
19 Done
20
21 <!--NeedCopy-->
```

Log-Startzeit und Verbindungsschlussgründe in RNAT Protokolleinträgen

Zur Diagnose oder Behebung von Problemen im Zusammenhang mit RNAT protokolliert die Citrix ADC Appliance RNAT-Sitzungen, wenn sie geschlossen werden.

Eine Protokollmeldung für eine RNAT-Sitzung besteht aus folgenden Informationen:

- Citrix ADC eigene IP-Adresse (NSIP-Adresse oder SNIP-Adresse), von der die Protokollnachricht stammt
- Zeitstempel der Protokollerstellung
- Protokoll der RNAT-Sitzung
- Quell-IP-Adresse
- RNAT IP-Adresse
- Ziel-IP-Adresse
- Startzeit der RNAT Sitzung
- Schließzeit der RNAT Sitzung
- Gesamtanzahl der von der Citrix ADC Appliance für diese RNAT-Sitzung gesendeten Bytes
- Gesamtanzahl der von der Citrix ADC Appliance für diese RNAT-Sitzung empfangenen Bytes
- Grund für den Abschluss der RNAT-Sitzung. Die Citrix ADC Appliance protokolliert Schließungsgrund für TCP-RNAT-Sitzungen, die den TCP-Proxy (TCP-Proxy deaktiviert) der Appliance nicht verwenden. Im Folgenden finden Sie die Art der Schließungsgründe, die für TCP-RNAT-Sitzungen protokolliert werden:
  - **TCP-FIN**. Die RNAT-Sitzung wurde aufgrund einer TCP-FIN geschlossen, die entweder vom Quell- oder Zielgerät gesendet wurde.
  - **TCP-RST**. Die RNAT-Sitzung wurde aufgrund eines TCP-Zurücksetzens geschlossen, der entweder vom Quell- oder Zielgerät gesendet wurde.
  - **TIMEOUT**. Die RNAT-Sitzung hat ein Zeitlimit überschritten.

Die folgende Tabelle zeigt einige Beispielprotokolleinträge für RNAT-Sitzungen.

Art des Eintrags	Beispielprotokolleintrag
Beispielprotokolleintrag für UDP-RNAT-Sitzung	Dec 1 15:28:12 10.102.53.114 12/01/2015:15:28:12 GMT 0-PPE-0 : default UDP NAT_OTHERCONN_DELINK 154 0 : Source 1.2.2.5:23431 - Destination 192.168.123.122:22 - NatIP 192.168.123.1:4045 - Destination 192.168.123.122:22 - Start Time 12/01/2015:15:26:58 GMT - Delink Time 12/01/2015:15:28:12 GMT - Total_bytes_send 2511 - Total_bytes_recv 3725
Beispielprotokolleintrag für TCP-RNAT-Sitzung. Der Protokolleintrag zeigt an, dass die Sitzung wegen TCP-Reset geschlossen wurde	Dec 1 15:29:59 10.102.53.114 12/01/2015:15:27:59 GMT 0-PPE-0 : default TCP NAT_OTHERCONN_DELINK 152 0 : Source 1.2.2.5:33826 - Destination 192.168.123.122:22 - NatIP 192.168.123.1:2384 - Destination 192.168.123.122:22 - Start Time 12/01/2015:15:27:40 GMT - Delink Time 12/01/2015:15:27:59 GMT - Total_bytes_send 2147 - Total_bytes_recv 3257 - Closure Reason TCP RST
Beispielprotokolleintrag für TCP-RNAT-Sitzung. Der Protokolleintrag zeigt an, dass die Sitzung Timeout	Dec 1 15:30:12 10.102.53.114 12/01/2015:15:30:12 GMT 0-PPE-0 : default TCP NAT_OTHERCONN_DELINK 155 0 : Source 1.2.2.5:64976 - Destination 192.168.123.115:22 - NatIP 192.168.123.1:19636 - Destination 192.168.123.115:22 - Start Time 12/01/2015:15:27:25 GMT - Delink Time 12/01/2015:15:30:12 GMT - Total_bytes_send 0 - Total_bytes_recv 0 - Closure Reason TIMEOUT

Stateful Connection Failover für RNAT

Verbindungs-Failover verhindert Unterbrechungen des Zugriffs auf Anwendungen, die in einer verteilten Umgebung bereitgestellt werden. Die Citrix ADC-Appliance unterstützt jetzt statusbehaftes Verbindungs-Failover für Verbindungen im Zusammenhang mit RNAT Regeln in einem Citrix ADC High Availability (HA) Setup. Bei einem HA-Setup bezieht sich das Verbindungs-Failover (oder Verbindungsspiegelung) auf den Vorgang, bei dem eine etablierte TCP- oder UDP-Verbindung aktiv bleibt, wenn ein Failover auftritt.

Die primäre Appliance sendet Nachrichten an die sekundäre Appliance, um aktuelle Informationen über die RNAT Verbindungen zu synchronisieren. Die sekundäre Appliance verwendet diese Verbindungsinformationen nur im Falle eines Failovers. Wenn ein Failover auftritt, verfügt die neue primäre Citrix ADC Appliance über Informationen zu den Verbindungen, die vor dem Failover hergestellt wurden, und wird diese Verbindungen auch nach dem Failover weiterhin bereitstellen. Aus Sicht des Clients ist dieses Failover transparent. Während der Übergangszeit können Client und Server eine kurze Unterbrechung und erneute Übertragungen auftreten.

Verbindungs-Failover kann pro RNAT Regel aktiviert werden. Zum Aktivieren des Verbindungs-Failovers auf einer RNAT-Regel aktivieren Sie den Parameter ConnFailover (Connection Failover) dieser spezifischen RNAT-Regel mit der CLI oder GUI.

So aktivieren Sie das Verbindungs-Failover für eine RNAT Regel mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `set rnat <name> -connfailover (ENABLED | DISABLED)`
- `show rnat`

So aktivieren Sie das Verbindungs-Failover für eine RNAT Regel mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **NATs**, und klicken Sie dann auf die Registerkarte **RNAT** .
2. Wählen Sie **Verbindungs-Failover** aus, während Sie eine neue RNAT-Regel hinzufügen oder eine vorhandene Regel bearbeiten.

Reservieren des Quellports für RNAT-Verbindungen zu Servern

Für eine Anforderung, die auf eine RNAT-Konfiguration trifft, bei der eine oder mehrere RNAT-IP-Adressen und “Proxy-Portparameter verwenden” deaktiviert sind, verwendet die Citrix ADC Appliance eine der RNAT-IP-Adresse und den Quellport der RNAT-Anforderung für die Verbindung mit Servern. Vor dem 13.0 47.x-Build schlägt die RNAT-Verbindung (unter Verwendung des Quellports des RNAT-Clients) zum Server fehl, wenn derselbe Quellport bereits in einigen anderen Verbindungen verwendet wurde.

- **Quellport weniger als 1024**. Standardmäßig behält sich die Citrix ADC Appliance die ersten 1024 Ports einer IP-Adresse im Besitz von Citrix ADC (einschließlich RNAT-IP-Adressen) vor. Vor dem 13.0 47.x-Build schlägt die RNAT-Verbindung (unter Verwendung des Quellports des RNAT-Clients) zum Server fehl, wenn der Quellport der RNAT-Anforderung kleiner oder gleich 1024 ist. Mit dem 13.0 47.x-Build ist die RNAT-Verbindung (unter Verwendung des Quellports des RNAT-Clients) zum Server erfolgreich, selbst wenn der Quellport der RNAT-Anforderung kleiner oder gleich 1024 ist.
- **Quellport größer als 1024**. Vor dem 13.0 47.x-Build schlägt die RNAT-Verbindung (unter Verwendung des Quellports des RNAT-Clients) zum Server fehl, wenn derselbe Quellport

bereits in einigen anderen Verbindungen verwendet wurde. Mit 13.0 47.x Build können Sie im `Retain Source Port range` (`retainsourceportrange`) -Parameter im Rahmen einer RNAT-Konfiguration einen Bereich von RNAT-Client-Quellports angeben. Die Citrix ADC Appliance behält diese RNAT-Client-Quellports an der RNAT-IP-Adresse vor, die nur für die RNAT-Verbindung zu Servern verwendet werden.

Entfernen von RNAT-Sitzungen

Sie können unerwünschte oder ineffiziente RNAT-Sitzungen von der Citrix ADC Appliance entfernen. Die Appliance gibt sofort Ressourcen frei (z. B. den Port der NAT-IP-Adresse und den Speicher), die für diese Sitzungen zugewiesen wurden, wodurch die Ressourcen für neue Sitzungen verfügbar sind. Die Appliance löscht auch alle nachfolgenden Pakete, die sich auf diese entfernten Sitzungen beziehen. Sie können alle oder ausgewählte RNAT-Sitzungen von der Citrix ADC Appliance entfernen.

So löschen Sie alle RNAT-Sitzungen mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **flush rnatsession**

So löschen Sie selektive RNAT-Sitzungen mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **flush rnatsession** ((-**network** <ip_addr> -**netmask** <netmask>) | -**natIP** <ip_addr> | -**aclname** <string>)

So löschen Sie alle oder selektive RNAT-Sitzungen mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **NATs**, und klicken Sie dann auf die Registerkarte **RNAT**.
2. Klicken Sie im Menü **Aktionen** auf **RNAT-Sitzungen leeren**, um alle oder selektive RNAT-Sitzungen zu entfernen (z. B. RNAT-Sitzungen mit einer bestimmten RNAT IP entfernen oder zu einer bestimmten Netzwerk- oder ACL-basierten RNAT-Sitzungsregel gehören).

Beispielkonfigurationen:

```
1     Clear all RNAT sessions existing on a Citrix ADC appliance
2
3     > flush rnatsession
4
5     Done
6
7     Clear all RNAT sessions belonging to network based RNAT rules that
         has 203.0.113.0/24 network as the matching condition.
8
```



```
9       > flush rnatsession -network 203.0.113.0 -netmask 255.255.255.0
10
11      Done
12
13      Clear all RNAT sessions with RNAT IP 192.0.2.90.
14
15      > flush rnatsession -natIP 192.0.2.90
16
17      Done
18
19      Clear all RNAT sessions belonging to ACL based RNAT rules that has
            ACL-RNAT-1 as the matching condition.
20
21      > flush rnatsession -aclname ACL-RNAT-1
22
23      Done
24  <!--NeedCopy-->
```

Konfigurieren der präfixbasierten IPv6-IPv4-Übersetzung

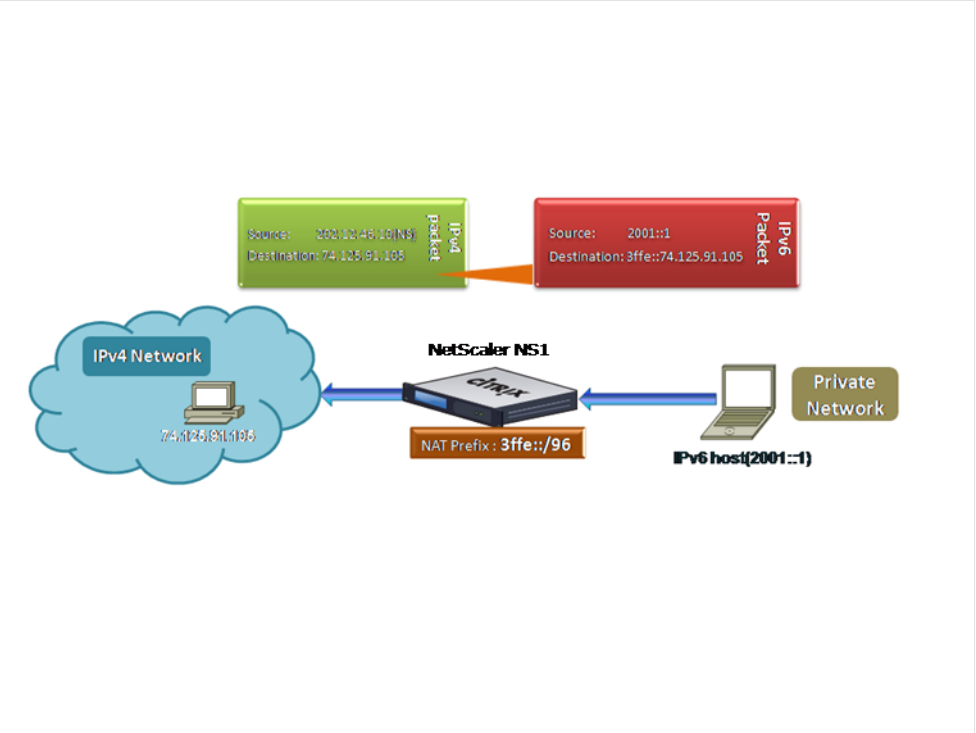
October 5, 2021

Präfixbasierte Übersetzung ist ein Prozess der Übersetzung von Paketen, die von privaten IPv6-Servern gesendet werden, in IPv4-Pakete unter Verwendung eines in der Citrix ADC Appliance konfigurierten IPv6-Präfixes. Dieses Präfix hat eine Länge von 96 Bit (128-32=96). Die IPv6-Server betten die Ziel-IP-Adresse der IPv4-Server oder -Hosts in die letzten 32 Bits des Ziel-IP-Adressfelds der IPv6-Pakete ein. Die ersten 96 Bits des Ziel-IP-Adressfelds werden als IPv6-NAT-Präfix festgelegt.

Die Citrix ADC Appliance vergleicht die ersten 96 Bits der Ziel-IP-Adresse aller eingehenden IPv6-Pakete mit dem konfigurierten Präfix. Wenn eine Übereinstimmung vorliegt, generiert die Citrix ADC Appliance ein IPv4-Paket und legt die Ziel-IP-Adresse als die letzten 32 Bits der Ziel-IP-Adresse des übereinstimmenden IPv6-Pakets fest. IPv6-Pakete, die an dieses Präfix adressiert werden, müssen an das Citrix ADC weitergeleitet werden, damit die IPv6-IPv4-Übersetzung vom Citrix ADC durchgeführt wird.

Im folgenden Diagramm wird 3ffe: :/96 als IPv6-NAT-Präfix auf Citrix ADC NS1 konfiguriert. Der IPv6-Host sendet ein IPv6-Paket mit der Ziel-IP-Adresse 3ffe: :74.125.91.105. NS1 vergleicht die ersten 96 Bits der Ziel-IP-Adresse aller eingehenden IPv6-Pakete mit dem konfigurierten Präfix, und sie stimmen überein. NS1 generiert dann ein IPv4-Paket und legt die Ziel-IP-Adresse als 74.125.91.105 fest.

Abbildung 1. IPv6-IPv4-Präfix-basierte Übersetzung



So konfigurieren Sie die präfixbasierte IPv6-IPv4-Übersetzung mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ipv6 [-natprefix <ipv6_addr                    *>]
```

-
- show ipv6

Beispiel:

```
1 > set ipv6 -natprefix 3ffe::/96
2  Done
3 <!--NeedCopy-->
```

So konfigurieren Sie die präfixbasierte IPv6-IPv4-Übersetzung mit der GUI:

Navigieren Sie zu System > Netzwerk, klicken Sie in der Gruppe Einstellungen auf INAT-Parameter konfigurieren, und legen Sie den Präfix-Parameter fest.

IP-Präfix NAT

October 5, 2021

Die Citrix ADC Appliance unterstützt die Übersetzung eines Teils der Quell-IP-Adresse anstelle der vollständigen Adresse der Pakete, die auf der Appliance empfangen werden. IP-Präfix NAT beinhaltet das Ändern eines oder mehrerer Oktette oder Bits der Quell-IP-Adresse.

Die Citrix ADC Appliance unterstützt IP-Präfix NAT für Lastausgleichskonfigurationen der folgenden Typen: ANY, UDP, DNS, TCP und HTTP.

Anwendungsfall: Zonifizierung von Clients für eine Bereitstellung einer Citrix ADC Appliance und eines Optimierungsgeräts

IP-Präfix NAT ist sehr nützlich in einer Bereitstellung, die eine Citrix ADC Appliance und ein Optimierungsgerät (z. B. Citrix ByteMobile) enthält. Dieser Bereitstellungstyp verfügt über unterschiedliche geografisch gelegene Clientnetzwerke, die dieselbe Netzwerkadresse verwenden. Die Citrix ADC Appliance muss den von jedem Client-Netzwerk empfangenen Datenverkehr an das Optimierungsgerät senden, bevor sie an das Ziel weiterleitet.

Das Gerät sendet den optimierten Datenverkehr zurück an die Citrix ADC Appliance. Da die Optimierungsanforderung für den Datenverkehr von jedem Client-Netzwerk unterschiedlich ist, muss das Optimierungsgerät das Client-Netzwerk jedes empfangenen Pakets erkennen. Die Lösung besteht darin, mithilfe von VLANs Datenverkehr von jedem Client-Netzwerk in eine andere Zone zu trennen. IP-Präfix NAT mit einer anderen Einstellung wird für jede Zone konfiguriert. Die Citrix ADC Appliance übersetzt das letzte Oktett der Quell-IP-Adresse jedes Pakets, und der übersetzte Oktettwert ist für jede Zone unterschiedlich.

Betrachten Sie ein Beispiel für zwei Zonen, Z1 und Z2, die Netzwerkadresse 192.0.2.0/24 gemeinsam nutzen. Auf der Citrix ADC Appliance werden IP-Präfix-NAT-Entitäten natrule-1 und natrule-2 für diese beiden Zonen konfiguriert. Bevor die Appliance ein Paket von Z1 weiterleitet, übersetzt natrule-1 das letzte Oktett der Quell-IP-Adresse des Pakets in 100. Ähnlich übersetzt natrule-2 für Pakete von Z2 das letzte Oktett der Quell-IP-Adresse in 200. Bei zwei Clients, CL1-Z1 in Zone Z1 und CL1-Z2 in Zone Z2, jeweils mit der IP-Adresse 192.0.2.30, übersetzt die Citrix ADC Appliance die Quell-IP-Adresse der Pakete CL1-Z1 in 100.0.2.30 und die Pakete von CL1-Z2 in 200.0.2.30. Das Optimierungsgerät, an das die Citrix ADC Appliance die übersetzten Pakete sendet, ist so konfiguriert, dass die Quell-IP-Adresse eines Pakets verwendet wird, um die Zone zu erkennen. Daher wendet es die für die Zone konfigurierte Optimierung an, aus der das Paket stammt.

Konfigurationsschritte

Die Konfiguration des IP-Präfix NAT besteht aus den folgenden Schritten:

- **Erstellen Sie ein Netzprofil und legen Sie den NAT-Regelparameter eines Netzprofils**fest. Eine NAT-Regel gibt zwei IP-Adressen und eine Netzmaske an. Die erste IP-Adresse (angegeben durch den Parameter IP Address) ist die Quell-IP-Adresse, die mit der zweiten übersetzt werden soll (angegeben durch IP Rewrite Parameter). Die Netzmaske gibt den Teil der Quell-IP-Adresse an, der mit demselben Teil der zweiten IP-Adresse übersetzt werden soll.
- **Binden Sie das Netzprofil an, um virtuelle Server oder Dienste mit Lastenausgleich auszugleichen**. Ein Netzprofil mit NAT-Regeleinstellung kann an einen virtuellen Server oder einen Dienst vom Typ ANY, UDP, DNS, TCP und HTTP gebunden werden. Nach dem Binden eines Netzprofils an einen virtuellen Server oder einen virtuellen Dienst stimmt die Citrix ADC Appliance die Quell-IP-Adresse der eingehenden Pakete im Zusammenhang mit dem virtuellen Server oder Dienst mit der NAT-Regeleinstellung ab. Citrix ADC führt dann IP-Präfix NAT für Pakete aus, die der NAT-Regel entsprechen.

So konfigurieren Sie die NAT-Übersetzung des IP-Präfix über die Befehlszeile:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **bind netProfile** <name> (-**natRule** <ip_addr> <netmask> <rewriteIp>)
- **show netprofile** <name>

So konfigurieren Sie das IP-Präfix NAT mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **Net Profile**.
2. Legen Sie die folgenden Parameter unter NAT-Regeln fest, während Sie NetProfiles hinzufügen oder ändern.
    - IP-Adresse
    - Netzmaske
    - IP neu schreiben

Beispielkonfiguration

In der folgenden Beispielkonfiguration hat das Netzprofil PARTIAL-NAT-1 IP-Präfix-NAT-Einstellungen und ist an den Lastenausgleich des virtuellen Servers LBVS-1 gebunden, der vom Typ ANY ist. Bei Paketen, die von 192.0.0.0/8 auf LBVS-1 empfangen wurden, übersetzt die Citrix ADC Appliance das letzte Oktett der Quell-IP-Adresse des Pakets in 100. Ein Paket mit Quell-IP-Adresse 192.0.2.30, das auf LBVS-1 empfangen wurde, übersetzt die Citrix ADC Appliance die Quell-IP-Adresse in 100.0.2.30, bevor sie einen der gebundenen Server sendet.

```
1 > add netprofile PARTIAL-NAT-1
2 Done
3
```



```
> bind netprofile PARTIAL-NAT-1  - natrule 192.0.0.0 255.0.0.0 100.0.0.0
Done

> add lb vserver LBVS-1 ANY 203.0.113. 61 * -netprofile PARTIAL-NAT-1
Done
<!--NeedCopy-->
```

Statische ARP

October 5, 2021

Sie können statische ARP-Einträge hinzufügen und statische ARP-Einträge aus der ARP-Tabelle entfernen. Nachdem Sie einen Eintrag hinzugefügt haben, sollten Sie die Konfiguration überprüfen. Wenn sich die IP-Adresse, der Port oder die MAC-Adresse ändert, nachdem Sie einen statischen ARP-Eintrag erstellt haben, müssen Sie den statischen Eintrag entfernen oder manuell anpassen. Daher wird das Erstellen statischer ARP-Einträge nicht empfohlen, es sei denn, dies ist erforderlich.

So fügen Sie mit der CLI einen statischen ARP-Eintrag hinzu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add arp -IPAddress** <ip_addr> -**mac**<mac_addr> -**ifnum** <interface_name>
- **show arp** <IPAddress>

Beispiel:

```
> add arp -ip 10.102.29.6 -mac 00:24:e8:73:ca:ec -ifnum 1/1
 Done
<!--NeedCopy-->
```

So entfernen Sie einen statischen ARP-Eintrag mit der CLI:

Geben Sie an der Eingabeaufforderung den Befehl **rm arp** und die IP-Adresse ein.

So fügen Sie mit der GUI einen statischen ARP-Eintrag hinzu:

Navigieren Sie zu **System** > **Netzwerk** > **ARP-Tabelle**, und fügen Sie einen statischen ARP-Eintrag hinzu.

Angeben eines VLAN in einem statischen ARP-Eintrag

In einem statischen ARP-Eintrag können Sie das VLAN angeben, über das auf das Zielgerät zugegriffen werden kann. Diese Funktion ist nützlich, wenn die im statischen ARP-Eintrag angegebene

Schnittstelle Teil mehrerer markierter VLANs ist und auf das Ziel über eines der VLANs zugegriffen werden kann. Die Citrix ADC Appliance enthält die angegebene VLAN-ID in den ausgehenden Paketen, die dem statischen ARP-Eintrag entsprechen. Wenn Sie keine VLAN-ID in einem ARP-Eintrag angeben und die angegebene Schnittstelle Teil mehrerer markierter VLANs ist, weist die Appliance dem ARP-Eintrag das native VLAN der Schnittstelle zu.

Angenommen, Citrix ADC Schnittstelle 1/2 ist Teil des nativen VLAN 2 und der getaggten VLANs 3 und 4, und Sie fügen einen statischen ARP-Eintrag für Netzwerkgerät A hinzu, das Teil von VLAN 3 ist und über Schnittstelle 1/2 zugänglich ist. Sie müssen VLAN 3 im ARP-Eintrag für Netzwerkgerät A angeben. Die Citrix ADC Appliance enthält dann VLAN 3 in allen Paketen, die für Netzwerkgerät A bestimmt sind, und sendet sie von Schnittstelle 1/2.

Wenn Sie keine VLAN-ID angeben, weist die Citrix ADC Appliance native VLAN 2 für den ARP-Eintrag zu. Pakete, die für Gerät A bestimmt sind, werden im Netzwerkpfad gelöscht, da sie nicht mit dem getaggten VLAN 3 angeben, d. h. das VLAN für Gerät A ist.

So geben Sie mit der CLI ein VLAN in einem statischen ARP-Eintrag an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add arp -ipAddress** <ip_addr>**-mac**<mac_addr>**-ifnum** <interface_name>[-**vlan**]<positive_integer>
- **show arp** <IPAddress>

Beispiel:

```
> add arp -ip 198.51.100.91 -mac 36:db:4b:f6:12:15 -ifnum 1/2 -vlan 3
Done
<!--NeedCopy-->
```

Festlegen des Timeouts für dynamische ARP-Einträge

October 5, 2021

Sie können global eine Alterungszeit (Timeout-Wert) für dynamisch erlernte ARP-Einträge festlegen. Der neue Wert gilt nur für ARP-Einträge, die dynamisch gelernt werden, nachdem der neue Wert festgelegt wurde. Frühere ARP-Einträge laufen nach der zuvor konfigurierten Alterungszeit ab. Sie können einen ARP-Timeoutwert von 1 bis 1200 Sekunden angeben.

So legen Sie das Timeout für dynamische ARP-Einträge mit der Befehlszeilenschnittstelle fest:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **set arpparam** -**timeout** <positive_integer>]

- **show arpparam**

Beispiel:

```
> set arpparam -timeout 500
 Done
<!--NeedCopy-->
```

So legen Sie das Timeout für dynamische ARP-Einträge mit der Befehlszeilenschnittstelle auf den Standardwert fest:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **unset arpparam**
- **show arpparam**

Beispiel:

```
> unset arpparam
 Done
<!--NeedCopy-->
```

So legen Sie das Timeout für dynamische ARP-Einträge mit der GUI fest:

Navigieren Sie zu **System** > **Netzwerk**, klicken Sie in der Gruppe **Einstellungen** auf **ARP Globale Parameter konfigurieren**, und legen Sie den Parameter **ARP Table Entry Timeout** fest.

Nachbarerkennung

October 5, 2021

Neighbor Discovery (ND) ist eines der wichtigsten Protokolle von IPv6. Es handelt sich um ein message-basiertes Protokoll, das die Funktionalität des Address Resolution Protocol (ARP), des Internet Control Message Protocol (ICMP) und der Routererkennung kombiniert. ND ermöglicht es Knoten, ihre Link-Layer-Adressen anzukündigen und die MAC-Adressen oder Link-Layer-Adressen der benachbarten Knoten abzurufen. Dieser Prozess wird durch das Neighbor Discovery-Protokoll (ND6) ausgeführt.

Die Nachbarermittlung kann die folgenden Funktionen ausführen:

- **Routererkennung**: Ermöglicht einem Host, die lokalen Router auf einem angeschlossenen Link zu erkennen und automatisch einen Standard-Router zu konfigurieren.

- **Präfixermittlung**: Ermöglicht dem Host, die Netzwerkpräfixe für lokale Ziele zu ermitteln.

  Hinweis: Die Citrix ADC Appliance unterstützt keine Präfixerkennung.

- **Parametererkennung**: Ermöglicht einem Host, zusätzliche Betriebsparameter zu erkennen, wie MTU und das Standard-Hop-Limit für ausgehenden Datenverkehr.
- **Automatische Adresskonfiguration**: Ermöglicht Hosts, IP-Adressen für Schnittstellen mit und ohne statusbehaftete Adresskonfigurationsdienste wie DHCPv6 automatisch zu konfigurieren. Citrix ADC unterstützt keine automatische Adresskonfiguration für globale IPv6-Adressen.
- **Adressenauflösung**: Entspricht ARP in IPv4, ermöglicht es einem Knoten, die IPv6-Adresse eines benachbarten Knotens in seine Link-Layer-Adresse aufzulösen.
- **Neighbor Unerreichbarkeitserkennung**: Ermöglicht einem Knoten, den Erreichbarkeitsstatus eines Nachbarn zu bestimmen.
- **Erkennung doppelter Adressen**: Ermöglicht einem Knoten, um zu bestimmen, ob eine NSIP-Adresse bereits von einem benachbarten Knoten verwendet wird.
- **Umleitung**: Entspricht der IPv4-ICMP-Umleitungsnachricht, ermöglicht es einem Router, den Host zu einer besseren First-Hop-IPv6-Adresse umzuleiten, um ein Ziel zu erreichen.

Hinweis: Die Citrix ADC Appliance unterstützt keine IPv6-Umleitung.

Konfigurationsschritte

Die Konfiguration der Nachbarermittlung umfasst die folgenden Aufgaben:

- Hinzufügen von IPv6-Nachbarn
- (Optional) Entfernen von IPv6-Nachbarn

CLI-Verfahren

So fügen Sie einen IPv6-Nachbarn mit der CLI hinzu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add nd6** <neighbor> <mac> <ifnum> [-**vlan** <integer>]
- **sh nd6**

Beispiel:

```
1 > add nd6 2001::1 00:04:23:be:3c:06 1/1  - vlan 1
2  Done
3
4 > show nd6
```



```
5    Neighbor                 MAC-Address(Vlan, Interface)       State
               TIME
6    --------                 ---------------------------        -----
              --------
7  1) ::1                     00:d0:68:0b:58:da(   1,  LO/1)   REACHABLE
         PERMANENT
8  2) fe80::2d0:68ff:fe0b:58da 00:d0:68:0b:58:da(   1,  LO/1)   REACHABLE
         PERMANENT
9  3) 2001::1                 00:04:23:be:3c:06(   1,   1/1)   REACHABLE
           STATIC
10  Done
11 <!--NeedCopy-->
```

So entfernen Sie einen Nachbarermittlungseintrag mithilfe der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **rm nd6** <Neighbor> -**vlan** <VLANID>

Beispiel:

```
1  rm nd6 3ffe:100:100::1 -vlan 1
2 <!--NeedCopy-->
```

So entfernen Sie alle Nachbarermittlungseinträge mithilfe der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **löschen nd6**

GUI-Verfahren

So fügen Sie mit der GUI einen IPv6-Nachbarn hinzu:

Navigieren Sie zu **System** > **Netzwerk** > **IPv6-Nachbarn**, und fügen Sie einen neuen IPv6-Nachbarn hinzu.

So entfernen Sie einen Neighbor Discovery-Eintrag mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **IPv6-Nachbarn**, löschen Sie den IPv6-Nachbarn.

So entfernen Sie alle Nachbarermittlungseinträge mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **IPv6-Nachbarn**, und klicken Sie auf **Löschen** .

IP-Tunnel

October 5, 2021

Ein IP-Tunnel ist ein Kommunikationskanal, der mithilfe von Kapselungstechnologien zwischen zwei Netzwerken erstellt werden kann, die keinen Routingpfad haben. Jedes IP-Paket, das zwischen den beiden Netzwerken geteilt wird, wird in einem anderen Paket gekapselt und dann über den Tunnel gesendet.

Die Citrix ADC Appliance implementiert IP-Tunneling auf folgende Weise:

- **Citrix ADC als Encapsulator (Load Balancing with DSR-Modus)**: Betrachten Sie eine Organisation, die über mehrere Rechenzentren in verschiedenen Ländern verfügt, wobei sich der Citrix ADC möglicherweise an einem Ort befindet und die Back-End-Server in einem anderen Land befinden. Im Wesentlichen befinden sich der Citrix ADC und die Back-End-Server in verschiedenen Netzwerken und sind über einen Router verbunden.

  Wenn Sie Direct Server Return (DSR) auf diesem Citrix ADC konfigurieren, wird das aus dem Quellsubnetz gesendete Paket vom Citrix ADC gekapselt und über einen Router und einen Tunnel an den entsprechenden Backend-Server gesendet. Der Back-End-Server entkapselt das Paket und antwortet direkt auf den Client, ohne dass das Paket über den Citrix ADC übergeben wird.

- **Citrix ADC als Decapsulator:** Betrachten Sie eine Organisation, die mehrere Rechenzentren mit jeweils Citrix ADCs und Back-End-Servern besitzt. Wenn ein Paket von Rechenzentrum A an Rechenzentrum B gesendet wird, wird es normalerweise über einen Vermittler gesendet, z. B. einen Router oder einen anderen Citrix ADC. Das Citrix ADC verarbeitet das Paket und leitet das Paket dann an den Back-End-Server weiter. Wenn jedoch ein gekapseltes Paket gesendet wird, muss der Citrix ADC in der Lage sein, das Paket zu entkapseln, bevor es an die Back-End-Server gesendet wird. Damit Citrix ADC als Decapsulator fungieren kann, wird ein Tunnel zwischen dem Router und dem Citrix ADC hinzugefügt. Wenn das gekapselte Paket mit zusätzlichen Header-Informationen den Citrix ADC erreicht, wird das Datenpaket entkapselt, d. h. die zusätzlichen Header-Informationen werden entfernt, und das Paket wird dann an die entsprechenden Back-End-Server weitergeleitet.

  Der Citrix ADC kann auch als Decapsulator für die Load Balancing-Funktion verwendet werden, insbesondere in Szenarien, in denen die Anzahl der Verbindungen auf einem vserver einen Schwellenwert überschreitet und alle neuen Verbindungen dann zu einem Backup-vserver umgeleitet werden.

Konfigurieren von IP-Tunneln

Die Konfiguration von IP-Tunneln auf einer Citrix ADC Appliance besteht aus der Erstellung von IP-Tunnel-Entitäten. Eine IP-Tunnelentität gibt die lokalen und Remote-Tunnelendpunkt-IP-Adressen und das Protokoll an, das für den IP-Tunnel verwendet werden soll.

Hinweis: Beim Konfigurieren eines IP-Tunnels in einem Cluster-Setup muss die lokale IP-Adresse eine Striped SNIP-Adresse sein.

CLI-Verfahren

So erstellen Sie einen IP-Tunnel mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add iptunnel** <name> <remote> <remoteSubnetMask> <local> -**type** -**protocol** (**ipoverip** | **GRE**)
- **iptunnel anzeigen**

So entfernen Sie einen IP-Tunnel mit der CLI:

Um einen IP-Tunnel zu entfernen, geben Sie den Befehl **rm iptunnel** und den Namen des Tunnels ein.

So erstellen Sie einen IPv6-Tunnel mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add ip6tunnel** <name> <remoteIp> <local>
- **ip6tunnel anzeigen**

So entfernen Sie einen IPv6-Tunnel mit der CLI:

Um einen IPv6-Tunnel zu entfernen, geben Sie den Befehl **rm ip6tunnel** und den Namen des Tunnels ein.

GUI-Verfahren

So erstellen Sie einen IP-Tunnel mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **IP-Tunnel**, fügen Sie einen neuen IP-Tunnel hinzu.

So erstellen Sie einen IPv6-Tunnel mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **IP-Tunnel** > **IPv6-Tunnel**, und fügen Sie einen neuen IPv6-Tunnel hinzu.

IP-Tunnel weltweit anpassen

Durch die globale Angabe der Quell-IP-Adresse können Sie eine gemeinsame Quell-IP-Adresse für alle Tunnel zuweisen. Da die Fragmentierung CPU-intensiv ist, können Sie global festlegen,

dass die Citrix ADC Appliance alle Pakete lösche, die fragmentiert werden müssen. Wenn Sie alle Pakete fragmentieren möchten, solange ein CPU-Schwellenwert nicht erreicht ist, können Sie den CPU-Schwellenwert global angeben.

CLI-Verfahren

So passen Sie IP-Tunnel global mit der CLI an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **set ipTunnelParam** -**srcIP** <sourceIPAddress>-**srciProundRobin** (**JA** | **NEIN**) -**DropFrag** [**JA** | **NEIN**] -**DropFragcPuThreshold** <Positive integer>
- **show ipTunnelParam**

Beispiel:

```
> set iptunnelparam  - srcIP 12.12.12.22 -dropFrag Yes  -
   dropFragCpuThreshold 50
 Done

> set iptunnelparam -srcIPRoundRobin YES -dropFrag Yes  -
   dropFragCpuThreshold 50
 Done
<!--NeedCopy-->
```

So passen Sie IPv6-Tunnel mit der CLI global an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **set ip6tunnelparam** -**srcIP** <IPv6Address> -**srcIPRoundRobin** (**YES** | NO)-**dropFrag** [**JA** | **NEIN**] -**dropFragCpuThreshold** <Positive integer>
- **show ip6tunnelparam**

GUI-Verfahren

So passen Sie IP-Tunnel global mit der GUI an:

Navigieren Sie zu **System** > **Netzwerk**, klicken Sie in der Gruppe Einstellungen auf **IPv4 Tunnel Global Settings** .

1. Navigieren Sie zu **System** > **Netzwerk**, klicken Sie in der Gruppe **Einstellungen** auf **IPv6-Tunnel Global Settings**.
2. Legen Sie im Dialogfeld **IP-Tunnel Globale Parameter konfigurieren** die Parameter fest.

So passen Sie IPv6-Tunnel mit der GUI global an:

1. Navigieren Sie zu **System** > **Netzwerk**, klicken Sie in der Gruppe **Einstellungen** auf **IPv6-Tunnel Global Settings**.
2. Legen Sie im Dialogfeld **IP-Tunnel Globale Parameter konfigurieren** die Parameter fest.

GRE-Nutzlastoptionen in einem GRE-IP-Tunnel

Bei einem konfigurierten GRE-IP-Tunnel kapselt die Citrix ADC Appliance das gesamte Layer-2-Paket, einschließlich des Ethernet-Headers und des VLAN-Headers (dot1q VLAN-Tag). IP-GRE-Tunnel zwischen Citrix ADC Appliances und einigen Geräten von Drittanbietern sind möglicherweise nicht stabil, da diese Geräte von Drittanbietern nicht so programmiert sind, dass einige oder die Layer-2-Paket-Header verarbeitet werden. Um einen stabilen IP-GRE-Tunnel zwischen einer Citrix ADC Appliance und einem Drittanbieter-Gerät zu konfigurieren, können Sie den GRE-Payload-Parameter des GRE-IP-Tunnel-Befehlssatzes verwenden. Die GRE-Nutzlasteinstellung kann auch auf einen GRE mit IPsec-Tunnel angewendet werden.

Sie können den GRE-Nutzlastparameter so einstellen, dass eine der folgenden Aktionen durchgeführt wird, bevor das Paket durch den GRE-Tunnel gesendet wird:

- **Ethernet mit DOT1Q**. Tragen Sie den Ethernet-Header sowie den VLAN-Header. Dies ist die Standardeinstellung. Bei einem Tunnel, der an eine Netbridge gebunden ist, enthält der innere Ethernet-Header und der VLAN-Header Informationen aus der ARP- und Bridge-Tabelle der Citrix ADC Appliance. Bei einem Tunnel, der als nächster Hop zu einer PBR-Regel festgelegt wird, wird die INNER Ethernet-Ziel-MAC-Adresse auf Null gesetzt, und der VLAN-Header gibt das Standard-VLAN an. Das vom Citrix ADC C-Tunnelendpunkt gesendete gekapselte (GRE) -Paket hat das folgende Format:

Outer Ethernet Header	Outer IP Header	GRE Header	Inner Ethernet	Inner VLAN header	Inner IP/IPv6/ARP header	Inner TCP/UDP Header	Payload

- **Ethernet**. Tragen Sie den Ethernet-Header, aber lassen Sie den VLAN-Header fallen. Da die Pakete keine VLAN-Informationen im Tunnel enthalten, müssen Sie für einen Tunnel mit dieser Einstellung, der an eine Netbridge gebunden ist, ein geeignetes VLAN an die Netbridge binden, damit der Citrix ADC diese Pakete beim Empfang von Paketen im Tunnel an das angegebene VLAN weiterleiten kann. Wenn der Tunnel als nächster Hop in einer PBR-Regel festgelegt ist, leitet der Citrix ADC die im Tunnel empfangenen Pakete weiter. Das vom Citrix ADC C-Tunnelendpunkt gesendete gekapselte (GRE) -Paket hat das folgende Format:

Outer Ethernet header	Outer IP header	GRE Header	Inner Ethernet header	Inner IP/IPv6/ARP header	Inner TCP/UDP header	Payload

- **IP**. Löschen Sie den Ethernet-Header sowie den VLAN-Header. Da Tunnel mit dieser Einstellung keine Layer-2-Header tragen, können diese Tunnel nicht an eine Netbridge gebunden werden, sondern als nächster Hop in einer PBR-Regel festgelegt werden. Das Peer-Tunnelendpunktgerät beim Empfang des Pakets verbraucht es oder leitet es weiter. Das vom Citrix ADC C-Tunnelendpunkt gesendete gekapselte (GRE) -Paket hat das folgende Format:

So löschen Sie Layer-2-Header von Paketen in einem GRE-IP-Tunnel mit der CLI:

- **add ipTunnel** <name> <remote> <remoteSubnetMask> <local> [-**protocol** <GRE> [-**vlan** <positive_integer>]] [-**grepayload** <grepayload>] [-**ipsecProfileName** <string>]
- **iptunnel anzeigen** <tunnelname>

Beispiel:

```
1 > add iptunnel IPTUNNEL-1 203.0.113.133 255.255.255.0 198.51.100.15 -
     protocol GRE - grepayload Ethernet -ipsecProfileName IPTUNNEL-IPSEC
     -1
2 Done
3 <!--NeedCopy-->
```

IPv6-Datenverkehr über GRE IPV4-Tunnel

Die Citrix ADC Appliance unterstützt die Übertragung von IPv6-Datenverkehr über einen IPV4-GRE-Tunnel. Diese Funktion kann verwendet werden, um die Kommunikation zwischen isolierten IPv6-Netzwerken zu ermöglichen, ohne die IPv4-Infrastruktur zwischen ihnen zu aktualisieren.

Zum Konfigurieren dieses Features verknüpfen Sie eine PBR6-Regel dem konfigurierten IPv4-GRE-Tunnel, über den der Citrix ADC IPv6-Datenverkehr senden und empfangen soll. Die IPv6-Quell- und Ziel-IPv6-Adressparameter der PBR6-Regel geben die IPv6-Netzwerke an, deren Datenverkehr den IPv4-GRE-Tunnel durchqueren soll.

Hinweis: IPsec-Protokoll wird auf GRE IPv4-Tunneln, die für die Übertragung von IPv6-Paketen konfiguriert sind, nicht unterstützt.

So erstellen Sie einen GRE IPv4-Tunnel mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add ipTunnel** <name> <remote> <remoteSubnetMask> <local> -**protocol GRE**
- **show ipTunnel** <name>

So verknüpfen Sie eine PBR6-Regel mit einem GRE-IPv4-Tunnel mit der CLI:

- **add ns pbr6** <pbrName> **ALLOW** -**srcIPv6** <network-range> -**dstIPv6** <network-range> -**ipTunnel** <tunnelName>
- **show pbr**

Beispielkonfiguration

In der folgenden Beispielkonfiguration wird der GRE IP-Tunnel Tunnel-V6onV4 mit der IP-Adresse 10.10.6.30 und der lokalen Tunnelendpunkt IP-Adresse 10.10.5.30 erstellt. Der Tunnel wird dann an pbr6 pBR6-v6onV4 gebunden. Die SRCIpv6 gibt das IPv6-Netzwerk an, das mit dem lokalen Endpunkt verbunden ist, und DestIPv6 gibt das IPv6-Netzwerk an, das mit dem entfernten Endpunkt verbunden ist. Der Datenverkehr von diesen IPv6-Netzwerken darf durch den GRE IPv4-Tunnel durchqueren.

```
1 > add ipTunnel TUNNEL-V6onV4 10.10.6.30 255.255.255.255 10.10.5.30 -
     protocol GRE
2 -ipsecProfileName None
3 Done
4 > add ns pbr6 PBR6-V6onV4 ALLOW -srcIPv6 = 2001:0db8:1::1-2001:0db8
     :1::255 -destIPv6 =
5 1-2001:0db8:4::255 -ipTunnel TUNNEL-V6onV4
6 <!--NeedCopy-->
```

Senden von Antwortdatenverkehr über einen IP-IP-Tunnel

Sie können eine Citrix ADC Appliance so konfigurieren, dass sie den Antwortdatenverkehr über einen IP-IP-Tunnel sendet, anstatt sie an die Quelle weiterzuleiten. Wenn die Appliance eine Anforderung von einem anderen Citrix ADC oder einem Drittanbieter-Gerät über einen IP-IP-Tunnel empfängt, leitet sie den Antwortdatenverkehr, anstatt ihn durch den Tunnel zu senden. Sie können richtlinienbasierte Routen (PBRs) verwenden oder MAC-basierte Weiterleitung (MBF) aktivieren, um die Antwort durch den Tunnel zu senden.

Geben Sie in einer PBR-Regel die Subnetze an beiden Endpunkten an, deren Datenverkehr den Tunnel durchqueren soll. Legen Sie auch den nächsten Hop als Tunnelnamen fest. Wenn der Antwortdatenverkehr mit der PBR-Regel übereinstimmt, sendet die Citrix ADC Appliance den Datenverkehr durch den Tunnel.

Alternativ können Sie MBF aktivieren, um diese Anforderung zu erfüllen, aber die Funktionalität ist auf den Datenverkehr beschränkt, für den die Citrix ADC Appliance Sitzungsinformationen speichert (z. B. Datenverkehr im Zusammenhang mit Lastenausgleich oder RNAT Konfigurationen). Die Appliance verwendet die Sitzungsinformationen, um den Antwortdatenverkehr durch den Tunnel zu senden.

CLI-Verfahren

So erstellen Sie eine PBR-Regel und ordnen den IP-IP-Tunnel mit der CLI zu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add ns pbr** <pbr_name> **ALLOW** -**srcIP** = <local_subnet_range> -**destIP** = <remote_subnet_range> -**ipTunnel** <tunnel_name>
- **apply ns pbrs**
- **show ns pbr** <pbr_name>

So aktivieren Sie die MAC-basierte Weiterleitung mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **enable ns mode MBF**
- **show ns mode**

GUI-Verfahren

So erstellen Sie eine PBR-Regel und ordnen den IP-IP-Tunnel mit der GUI zu:

1. Navigieren Sie zu **System** > **Netzwerk** > **PBRs**. Erstellen Sie auf der Registerkarte **PBRs** eine **PBR-Regel** .
2. Legen Sie beim Erstellen des PBR den **Next Hop-Typ** auf **IP-Tunnel** und **IP-Tunnelname** auf den konfigurierten IP-IP-Tunnelnamen fest.

So aktivieren Sie die MAC-basierte Weiterleitung mit der GUI:

1. Navigieren Sie zu **System** > **Einstellungen**, klicken Sie unter **Modi und Features** auf **Modi konfigurieren** .
2. Wählen Sie auf der Seite **Modi konfigurieren** die Option **MAC-basierte Weiterleitung** aus.

Beispielkonfiguration

Betrachten Sie ein Beispiel für einen IPIP-Tunnel, NS1-NS2-IPIP, der zwischen zwei Citrix ADC Appliances NS1 und NS2 eingerichtet ist.

Standardmäßig leitet NS2 für jede Anforderung, die über den Tunnel empfängt, den Antwortdatenverkehr an die Quelle, anstatt ihn (an NS1) durch den Tunnel zu senden.

Sie können richtlinienbasierte Routen (PBRs) konfigurieren oder MAC-basierte Weiterleitung (MBF) auf NS2 aktivieren, um die Antwort durch den Tunnel zu senden.

In der folgenden Beispielkonfiguration auf NS2 ist NS1-NS2-IPIP ein IPIP-Tunnel und NS1-NS2-IPIP-PBR eine PBR-Regel. Bei Anfragen (mit der inneren Quell-IP-Adresse im Bereich 10.102.147.0-10.102.147.255 und der inneren Ziel-IP-Adresse im Bereich 10.102.147.0-10.102.147.255), die von NS2

über den Tunnel empfangen werden, sendet NS2 die entsprechende Antwort durch den Tunnel (an NS1), anstatt sie an die Quelle. Die Funktionalität ist auf den Datenverkehr beschränkt, der der PBR-Regel entspricht.

```
> add iptunnel NS1-NS2-IPIP 192.0.2.99 255.255.255.255 203.0.113.99 -
    protocol IPIP

Done
> add pbr NS1-NS2-IPIP-PBR -srcIP 10.102.147.0-10.102.147.255  - destIP
    10.20.1.0-10.20.1.255  - ipTunnel NS1-NS2-IPIP

Done
> apply pbrs

Done
```

Alternativ kann MBF auf NS2 aktiviert werden. Die Funktionalität ist auf den Datenverkehr beschränkt, für den NS2 Sitzungsinformationen speichert (z. B. Datenverkehr im Zusammenhang mit Lastenausgleich oder RNAT Konfigurationen).

```
> enable ns mode MBF

Done
```

Klasse E IPv4-Pakete

October 5, 2021

Standardmäßig löscht die Citrix ADC Appliance alle Pakete, wenn sie eine Klasse E IPv4-Adresse in den Quell-IP- oder Ziel-IP-Feldern enthalten. Wenn Ihr Setup IPv4-Adressen der Klasse E verwendet, können Sie die Citrix ADC Appliance so konfigurieren, dass die Klasse E IPv4-Pakete verarbeitet werden.

Voraussetzungen

Bevor Sie mit der Konfiguration einer Citrix ADC Appliance für die Verarbeitung von IPv4-Paketen der Klasse E beginnen, beachten Sie die folgenden Punkte:

- Citrix ADC-Appliances unterstützen die Konfiguration von IPv4-Adressen im Besitz von Citrix ADC (z. B. SNIP und VIP) im Klasse E-Bereich nicht. Citrix ADC Appliances unterstützen nur die Verarbeitung von IPv4-Paketen der Klasse E.
- Eine Citrix ADC Appliance verwendet intern IPv4-Adressen der Klasse E für das IPv6-Feature. Die Citrix ADC Appliance unterstützt nicht beide Funktionen (Verarbeitungsklasse E IPv4-Pakete und IPv6-Unterstützung), die gleichzeitig funktionieren. Die Citrix ADC Appliance setzt eine Einschränkung auf, um die IPv6-Funktion nicht zu aktivieren, wenn die Verarbeitung von IPv4-Paketen der Klasse E aktiviert ist und umgekehrt.

Konfigurationsschritte

Die Konfiguration einer Citrix ADC Appliance für die Verarbeitung von IPv4-Paketen der Klasse E besteht aus der Aufgabe, den **IPv4-Class-E-Adressclients** (**AllowClasseIPv4**) Layer 3-Parameter zu aktivieren.

CLI-Verfahren

So konfigurieren Sie die Citrix ADC Appliance für die Verarbeitung von IPv4-Paketen der Klasse E mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **set l3param** -**allowClassEIPv4** (**ENABLED**|**DISABLED**)
- **show l3param**

Beispielkonfiguration:

```
> set l3param -allowClassEIPv4 ENABLED

Done

> sh l3param

    Network L3 related Configuration Parameters

    icmpgen_rate_threshold      : 100

    srcnat                      : ENABLED

    override_rnat               : DISABLED

    drop_df_flag                : DISABLED

```



```
17      .
18
19      .
20
21      .
22
23      IPv6DynamicRouting          : DISABLED
24
25      allowClassEIPv4             : ENABLED
26
27  Done
28  <!--NeedCopy-->
```

GUI-Verfahren

So konfigurieren Sie die Citrix ADC Appliance für die Verarbeitung von IPv4-Paketen der Klasse E mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk**, und klicken Sie dann im Abschnitt **Einstellungen** auf **Layer-3-Parameter konfigurieren**.
2. Wählen Sie **IPv4-Class E-Adress-Clients** aus, und klicken Sie auf **OK**.

Schnittstellen

October 5, 2021

Bevor Sie mit der Konfiguration von Schnittstellen beginnen, entscheiden Sie, ob Ihre Konfiguration den MAC-basierten Weiterleitungsmodus verwenden kann, und aktivieren oder deaktivieren Sie diese Systemeinstellung entsprechend. Die Anzahl der Schnittstellen in Ihrer Konfiguration unterscheidet sich für die verschiedenen Modelle der Citrix ADC Appliance. Neben der Konfiguration einzelner Schnittstellen können Sie Schnittstellen logisch gruppieren, indem Sie VLANs verwenden, um den Datenfluss innerhalb einer Gruppe von Schnittstellen zu beschränken, und Sie können Links zu Kanälen zusammenfassen. Bei einem Hochverfügbarkeitssetup können Sie bei Bedarf eine virtuelle MAC-Adresse konfigurieren. Wenn Sie den L2-Modus verwenden, können Sie die Alterung der Bridge-Tabelle ändern.

Entscheiden Sie nach Abschluss der Konfiguration, ob Sie die Systemeinstellung für die Pfad-MTU-Erkennung aktivieren sollen. Citrix ADC Appliances können mit VRRP im aktiven Modus bereitgestellt werden. Eine aktiv-aktive Bereitstellung nutzt nicht nur Ausfallzeiten, sondern auch alle Citrix ADC Appliances in der Bereitstellung effizient. Mit dem Tool Network Visualizer können Sie die

Netzwerkkonfiguration einer Citrix ADC Bereitstellung anzeigen und Schnittstellen, Kanäle, VLANs und Bridge-Gruppen konfigurieren.

Konfigurieren der MAC-basierten Weiterleitung

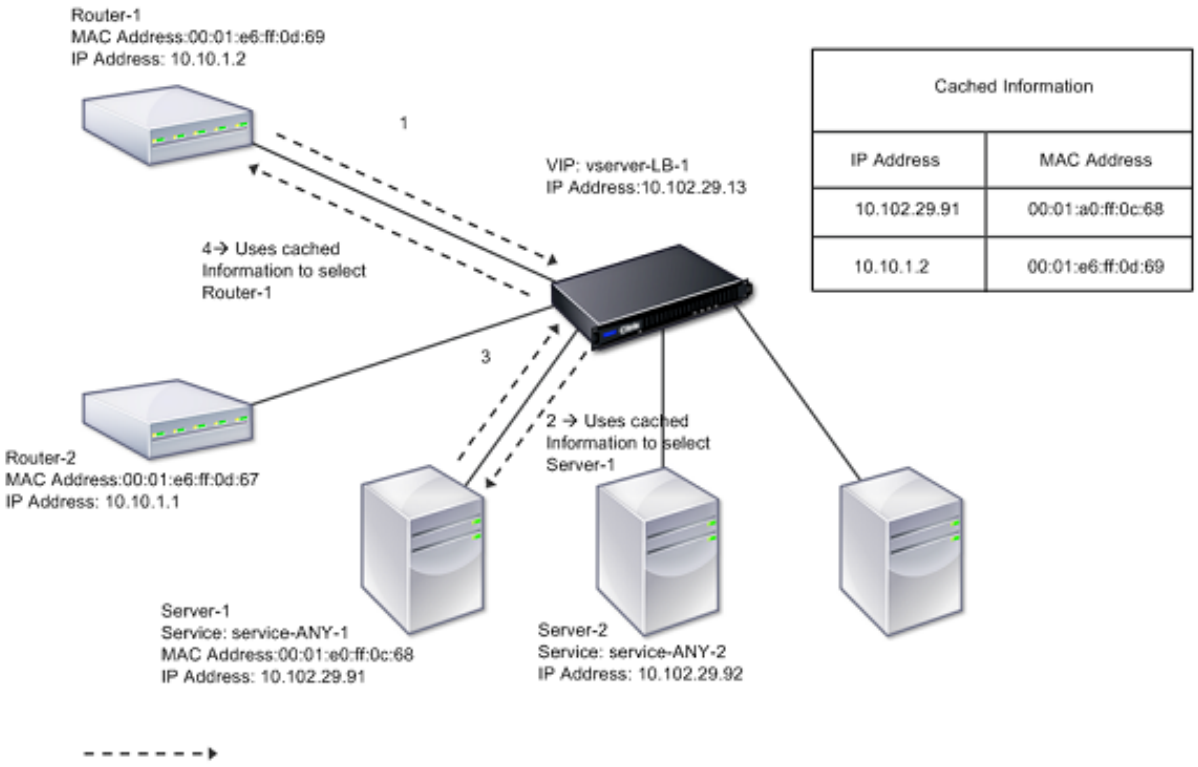
October 5, 2021

Wenn die MAC-basierte Weiterleitung (MBF) aktiviert ist, merkt sich die Appliance, wenn eine Anforderung die Citrix ADC Appliance erreicht, die Quell-MAC-Adresse des Frames und verwendet sie als Ziel-MAC-Adresse für die resultierenden Antworten. MAC-basierte Weiterleitung kann verwendet werden, um Multiple-Route/ARP-Lookups zu vermeiden und asymmetrische Paketflüsse zu vermeiden. MAC-basierte Weiterleitung ist möglicherweise erforderlich, wenn der Citrix ADC mit mehreren statusbehafteten Geräten wie VPNs oder Firewalls verbunden ist, da dadurch sichergestellt wird, dass der Rückkehrverkehr an dasselbe Gerät gesendet wird, von dem der anfängliche Datenverkehr stammt.

MAC-basierte Weiterleitung ist nützlich, wenn Sie VPN-Geräte verwenden, da dadurch sichergestellt wird, dass der gesamte Datenverkehr, der durch ein VPN fließt, über dasselbe VPN-Gerät weitergeleitet wird.

Das folgende Topologiediagramm veranschaulicht den Prozess der MAC-basierten Weiterleitung.

Abbildung 1. MAC-basierter Weiterleitungsmodus



Wenn MAC-basierte Weiterleitung (MBF) aktiviert ist, speichert Citrix ADC die MAC-Adresse von:

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

Wenn ein Server über die Citrix ADC Appliance antwortet, legt die Appliance die Ziel-MAC-Adresse des Antwortpakets auf die zwischengespeicherte Adresse fest. Dadurch wird sichergestellt, dass der Datenverkehr symmetrisch fließt, und leitet die Antwort dann an den Client weiter. Der Prozess umgeht die Routing-Tabellensuche und ARP-Suchfunktionen. Wenn der Citrix ADC jedoch eine Verbindung initiiert, verwendet er die Route- und ARP-Tabellen für die Nachschlagefunktion. In einer direkten Serverrückgabekonfiguration müssen Sie die MAC-basierte Weiterleitung aktivieren.

Weitere Informationen zu Konfigurationen für Direct Server Return finden Sie unter Lastenausgleich.

Einige Bereitstellungstopologien erfordern möglicherweise eingehende und ausgehende Pfade, um durch verschiedene Router zu fließen. MAC-basierte Weiterleitung würde diesen Topologieentwurf unterbrechen.

MBF sollte in folgenden Situationen deaktiviert werden:

- **Wenn ein Server eine Netzwerkschnittstellenkarte (NIC) -Teaming-Verbindung verwendet, ohne LACP (802.1ad Link Aggregation) zu verwenden.** Um die MAC-basierte Weiterleitung in diesem Fall zu aktivieren, müssen Sie ein Layer-3-Gerät zwischen Citrix ADC und Server verwenden.

Hinweis: MBF kann aktiviert werden, wenn der Server NIC zusammen mit LACP verwendet, da die virtuelle Schnittstelle eine MAC-Adresse verwendet.

- **Wenn Firewall-Clustering verwendet wird**. Firewall-Clustering geht davon aus, dass ARP verwendet wird, um die MAC-Adresse für eingehenden Datenverkehr aufzulösen. Manchmal kann die eingehende MAC-Adresse eine nicht gruppierte MAC-Adresse sein und sollte nicht für die Verarbeitung eingehender Pakete verwendet werden.

Wenn MBF deaktiviert ist, verwendet die Appliance die L2- oder L3-Konnektivität, um die Antworten von Servern an die Clients weiterzuleiten. Abhängig von der Routing-Tabelle können die Router, die für ausgehende Verbindung und eingehende Verbindungen verwendet werden, unterschiedlich sein. Bei umgekehrter Datenverkehr (Antwort vom Server):

- Wenn sich die Quelle und das Ziel in verschiedenen IP-Subnetzen befinden, verwendet die Appliance die Routensuche, um das Ziel zu finden.
- Wenn sich die Quelle im selben Subnetz wie das Ziel befindet, sucht Citrix ADC in der ARP-Tabelle nach der Netzwerkschnittstelle und leitet den Datenverkehr an sie weiter. Wenn die ARP-Tabelle nicht vorhanden ist, fordert Citrix ADC die ARP-Einträge an.

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

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **enable ns mode MBF**
- **ns-Modus MBF deaktivieren**

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

1. Navigieren Sie zu **System** > **Einstellungen**, klicken Sie in der Gruppe **Modi und Features** auf **Modi konfigurieren** .
2. Aktivieren oder deaktivieren Sie die Option **MAC-basierte Weiterleitung** .

MAC-basierte Weiterleitung für ein Lastausgleichs-Setup

Einige Lastausgleichseinstellungen erfordern, dass die Citrix ADC Appliance den globalen MBF (falls aktiviert) für diese Setups umgeht und stattdessen die Route/ARP-Suchups zum Senden von Paketen an das Ziel verwendet.

Der MBF-Parameter eines Netzprofils wird verwendet, um MBF für eine bestimmte Lastausgleichskonfiguration zu aktivieren oder zu deaktivieren. MBF kann sowohl für die Clientseite als auch für die Serverseite einer Lastausgleichskonfiguration festgelegt werden, indem Netzprofile (MBF aktiviert oder deaktiviert) an den virtuellen Server und die Dienste gebunden werden.

Wenn beispielsweise ein Netzprofil mit deaktiviertem MBF an den virtuellen Server einer Lastausgleichskonfiguration gebunden ist, umgeht die Citrix ADC Appliance den globalen MBF (falls aktiviert) und verwendet stattdessen die Route/ARP-Suchups zum Senden von Antwortpaketen an Clients.

Voraussetzungen

Bevor Sie mit der Konfiguration von MBF für eine Lastausgleichskonfiguration beginnen, beachten Sie die folgenden Punkte:

- In einer Lastausgleichskonfiguration können die Clientseite (virtueller Server) und die Serverseite (Servicegruppen) unterschiedliche MBF-Einstellungen haben.
- Eine Lastausgleichskonfiguration erbt die globale MBF-Einstellung, wenn MBF nicht explizit in den Netzprofilen festgelegt ist, die an den virtuellen Server und die Dienste gebunden sind.
- In einer Lastausgleichskonfiguration erbt serverseitig (Dienst) die clientseitige MBF-Einstellung des an den virtuellen Server gebundenen Netzprofils, wenn kein Netzprofil an den Dienst gebunden ist.
- In einer Load Balancing-Konfiguration mit direktem Server-Rückgabemodus erbt clientseitig die MBF-Einstellung im Netzprofil, das an den Dienst gebunden ist.
- Bei einer Content Switching-Konfiguration übernimmt die Clientseite die MBF-Einstellung im Netzprofil, die an den virtuellen Content Switching-Server gebunden ist, anstatt vom virtuellen Zielserver für Lastenausgleich.

Einschränkungen

Bevor Sie mit der Konfiguration von MBF für eine Lastausgleichskonfiguration beginnen, beachten Sie die folgenden Einschränkungen:

- MBF-Einstellung für Lastausgleichskonfigurationen wird in einem Cluster-Setup nicht unterstützt.
- Bei einem virtuellen Lastausgleichsserver mit MAC-Modus- oder L2Conn-Einstellungen wird MBF unabhängig von der MBF-Einstellung im gebundenen Netzprofil zum virtuellen Server aktiviert.
- Die Citrix ADC Appliance unterstützt die Einstellung MBF für Lastausgleich-Monitore mit Net Profile nicht. Mit anderen Worten, die MBF-Einstellung eines Netzprofils wird nicht auf die Monitore angewendet, an die das Netzprofil gebunden ist. Die globale MBF-Einstellung wird unabhängig von der MBF-Einstellung des gebundenen Netzprofils auf Monitore angewendet.

MBF für die Konfiguration des Lastenausgleichs konfigurieren

Die Konfiguration von MBF für eine Lastausgleichskonfiguration besteht aus folgenden Aufgaben:

- MBF-Parameter in einem Netzprofil aktivieren.
- Binden Sie das Netzprofil an einen virtuellen Server oder Dienste mit Lastenausgleich.

So aktivieren Sie MBF in einem Netzprofil mit der CLI:

- Um MBF beim Hinzufügen eines Netzprofils zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein:

  - **add netProfile** <name> -**MBF** (**ENABLED** | **DISABLED**)
  - **show netprofile** <name>
- Um MBF in einem vorhandenen Netzprofil zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein:
  - **set netProfile** <name> -**MBF** (**ENABLED** | **DISABLED**)
  - **show netprofile** <name>

So aktivieren Sie MBF in einem Netzprofil mithilfe von GUI**

1. Navigieren Sie zu **System** > **Netzwerk** > **Net Profile**.
2. Aktivieren Sie den **MBF-Parameter**, während Sie ein Netzprofil hinzufügen oder ändern.

In der folgenden Beispielkonfiguration hat Netprofil NETPROFILE-MBF-LBVS MBF aktiviert und ist an den Lastenausgleich des virtuellen Servers LBVS-1 gebunden. Außerdem hat Netprofil NETPROFILE-MBF-SVC MBF aktiviert und ist an einen Lastausgleichsdienst SVC-1 gebunden.

```
> add netprofile NETPROFILE-MBF-LBVS -MBF ENABLED

Done

> add netprofile NETPROFILE-MBF-SVC -MBF ENABLED

Done

> set lb vserver LBVS-1 -netprofile NETPROFILE-MBF-LBVS

Done

> set service SVC-1 -netprofile NETPROFILE-MBF-SVC

Done

<!--NeedCopy-->
```

Konfigurieren von Netzwerkschnittstellen

October 5, 2021

Netzwerkschnittstellen in der Citrix ADC Appliance sind in<slot><port> Schreibweise nummeriert. Nachdem Sie Ihre Schnittstellen konfiguriert haben, zeigen Sie die Schnittstellen und deren Einstellungen an, um die Konfiguration zu überprüfen. Sie können diese Informationen auch anzeigen, um

ein Problem in der Konfiguration zu beheben.

Um die Netzwerkschnittstellen zu verwalten, können Sie Folgendes tun:

- Aktivieren Sie einige Schnittstellen und deaktivieren Sie andere.
- Setzen Sie eine Schnittstelle zurück, um ihre Einstellungen neu zu verhandeln.
- Löschen Sie die kumulierten Statistiken für eine Schnittstelle.

Um die Konfiguration zu überprüfen, können Sie die Schnittstelleneinstellungen anzeigen. Sie können die Statistiken für eine Schnittstelle anzeigen, um deren Zustand zu bewerten.

Festlegen der Netzwerkschnittstellenparameter

Die Konfiguration der Netzwerkschnittstelle wird weder synchronisiert noch weitergegeben. Bei einem HA-Paar müssen Sie die Konfiguration für jede Einheit unabhängig durchführen.

So legen Sie die Netzwerkschnittstellenparameter mit der CLI fest:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 -  set interface <id> [-speed <speed>] [-duplex <duplex>] [-flowControl
      <flowControl>] [-autoneg ( DISABLED | ENABLED )] [-haMonitor ( ON |
      OFF )] [ ( ON | OFF )] [-tagall ( ON | OFF )] [-lacpMode <lacpMode
     >] [-lacpKey<positive_integer>] [-lacpPriority <positive_integer>]
     [-lacpTimeout (LONG | SHORT )] [-ifAlias <string>] [-throughput <
     positive_integer>][-bandwidthHigh <positive_integer> [-
     bandwidthNormal <positive_integer>]]
2 -  show interface [<id>]
3 <!--NeedCopy-->
```

Beispiel:

```
1 > set interface 1/8 -duplex full
2  Done
3 <!--NeedCopy-->
```

So legen Sie die Netzwerkschnittstellenparameter mit der GUI fest:

Navigieren Sie zu **System > Netzwerk > Schnittstellen**, wählen Sie die Netzwerkschnittstelle aus, die Sie ändern möchten (z. B. 1/8), klicken Sie auf **Bearbeiten**, und legen Sie dann die Parameter fest.

Festlegen der Empfangsringgröße und des Ringtyps für eine Schnittstelle

Sie können die Empfangsringgröße und den Ringtyp für IX-, F1X-, F2X- oder F4X-Schnittstellen auf Citrix ADC MPX- und SDX-Plattformen erhöhen.

Eine erhöhte Ringgröße bietet mehr Polsterung, um Burst-Traffic zu bewältigen, kann aber die Leistung beeinträchtigen. Für IX-Schnittstellen wird eine Ringgröße von bis zu 8192 unterstützt. Für F1X-, F2X- und F4X-Schnittstellen wird eine Ringgröße von bis zu 4096 unterstützt. Die Standardringgröße bleibt 2048.

Schnittstellenringtypen sind standardmäßig elastisch. Sie erhöhen oder verringern die Größe basierend auf der Rate der Paketankunft. Sie können den Ringtyp als fest konfigurieren. In diesem Fall ändert sich die Ringgröße nicht basierend auf der Verkehrsrate.

Hinweis: Diese Funktion wird ab Version 13.0 Build 41.x unterstützt und auf Plattformen mit IX-, F1X-, F2X- oder F4X-Schnittstellen unterstützt.

Verwenden Sie den`show hardware` Befehl, um festzustellen, ob Ihre Appliance über IX-, F1X-, F2X- oder F4X-Schnittstellen verfügt.

Beispiele:

Das folgende Modell hat 16 F1X (10G) Schnittstellen und 4 F4X (40G) Schnittstellen.

```
1  > sh hardware
2          Platform: NSMPX-25000-40G 20\*CPU+16\*F1X+4\*F4X+2\*E1K+2*CVM
               N3 250040
3          Manufactured on: 12/16/2016
4          CPU: 2800MHZ
5          Host Id: 234913926
6          Serial no: N43RJCRV3X
7          Encoded serial no: N43RJCRV3X
8          Netscaler UUID: 336a32d6-2cfa-11e8-bf01-00e0ed5dd23c
9          BMC Revision: 4.08
10  Done
11 <!--NeedCopy-->
```

Das folgende Modell hat 2 1X (10G) Schnittstellen.

```
1  > sh hardware
2          Platform: NSMPX-10500 8\*CPU+2\*E1K+8\*E1K+2\*IX+8*CVM 1620
               760100
3          Manufactured on: 12/27/2010
4          CPU: 2832MHZ
```



```
5          Host Id: 1707114630
6          Serial no: 7VZZV1ZXJ4
7          Encoded serial no: 7VZZV1ZXJ4
8          Netscaler UUID: eb1bfd72-5176-11e7-ba18-00e0ed1b0d12
9   Done
10 <!--NeedCopy-->
```

Um die Ringgröße und den Ringtyp mit der CLI
zu konfigurieren Geben Sie Folgendes ein:

```
1 set interface <id> -ringsize <positive_integer> -ringtype ( Elastic |
     Fixed )
2 <!--NeedCopy-->
```

Die Parameter:

`ringsize`:

Die Empfangsringgröße der Schnittstelle. Eine höhere Zahl bietet mehr Puffer, um eingehenden Datenverkehr zu verarbeiten.

Standardwert: 2048
Mindestwert: 512
Maximaler Wert: 16384

`ringtype`:

Der Empfangsringtyp der Schnittstelle. Ein fester Ringtyp weist die konfigurierte Anzahl von Puffern unabhängig von der Datenverkehrsrate vorab zu. Im Gegensatz dazu dehnt sich ein elastischer Ring basierend auf der eingehenden Verkehrsrate aus und schrumpft.

Mögliche Werte: Elastic, Fixed

Standardwert: Elastic

Beispiel:

```
1 > set interface 40/2 -ringsize 4096 -ringtype Fixed
2  Done
3 > show interface 40/2
4
5 1)      Interface 40/2 (40G Ethernet, CR4, 40 Gbit) #21  flags=0xc020 <
     ENABLED, UP, UP, autoneg, HAMON, HEARTBEAT, 802.1q> MTU=1500, native
      vlan=10, MAC=00:e0:ed:75:14:2a, uptime 119h26m32s
```



```
6          Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,
               throughput 0
7          Actual: media UTP, speed 40000, duplex FULL, fctl OFF,
               throughput 40000
8          LLDP Mode: NONE, LR Priority: 1024
9          RX: Pkts(1443972660032) Bytes(1457207315336105) Errs(0) Drops
               (53319) Stalls(0)
10         TX: Pkts(1452311431262) Bytes(1458534011197761) Errs(0) Drops
               (788) Stalls(0)
11         NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
12         Bandwidth thresholds are not set.
13         Rx Ring: Configured size=4096, Actual size=4096, Type: Fixed
14  Done
15 <!--NeedCopy-->
```

Die letzte Zeile zeigt die konfigurierte und tatsächliche Ringgröße sowie den Ringtyp.

So konfigurieren Sie Ringgröße und Ringtyp mit der GUI:

1. Navigieren Sie zu **System > Netzwerk > Interfaces**.
2. Wählen Sie Ihre Schnittstelle aus und klicken Sie auf **Bearbeiten**.
3. Geben Sie **unter Ringgröße**eine der folgenden Optionen an:
   - **IX-Schnittstellen:** 512, 1024, 2048, 4096 oder 8192.
   - **F1X-, F2X- oder F4X-Schnittstellen:** 512, 1024, 2048 oder 4096.
4. Wählen Sie **unter Ringtyp**die Option Elastic oder Fixed aus.
5. Klicken Sie auf **OK**.

Aktivieren und Deaktivieren von Netzwerkschnittstellen

Standardmäßig sind die Netzwerkschnittstellen aktiviert. Deaktivieren Sie jede Netzwerkschnittstelle, die nicht mit dem Netzwerk verbunden ist, sodass keine Pakete gesendet oder empfangen werden können. Das Deaktivieren einer Netzwerkschnittstelle, die in einem Hochverfügbarkeitssetup mit dem Netzwerk verbunden ist, kann zu einem Failover führen.

Weitere Informationen zur Hochverfügbarkeit finden Sie unter Hochverfügbarkeit.

So aktivieren oder deaktivieren Sie eine Netzwerkschnittstelle mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 -  enable interface <interface_num>
2 -  show interface <interface_num>
```



```
3 -  disable interface <interface_num>
4 -  show interface <interface_num>
5 <!--NeedCopy-->
```

Beispiel:

```
1 > enable interface 1/8
2  Done
3 > show interface 1/8
4         Interface 1/8 (Gig Ethernet 10/100/1000 MBits) #2
5         flags=0x4004000 <ENABLED, DOWN, BOUND to LA/1, down, autoneg,
              802.1q>
6         MTU=1514, MAC=00:d0:68:15:fd:3d, downtime 906h58m40s
7         Requested: media UTP, speed AUTO, duplex FULL, fctl OFF,
              throughput 0
8         RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
9         TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
10        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
11        Bandwidth thresholds are not set.
12 Done
13 <!--NeedCopy-->
```

So aktivieren oder deaktivieren Sie eine Netzwerkschnittstelle mit der GUI:

1. Navigieren Sie zu **System > Netzwerk > Interfaces**.
2. Wählen Sie die Netzwerkschnittstelle aus, und wählen Sie in der Liste **Aktion** die Option Aktivieren oder Deaktivieren aus.

Netzwerkschnittstellen zurücksetzen

Die Netzwerkschnittstelleneinstellungen steuern Eigenschaften wie Duplex und Geschwindigkeit. Um die Einstellungen einer Netzwerkschnittstelle neu zu verhandeln, müssen Sie sie zurücksetzen.

So setzen Sie eine Netzwerkschnittstelle mit der CLI zurück:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 -  reset interface <interface_num>
2 -  show interface <interface_num>
3 <!--NeedCopy-->
```

Beispiel:


```
> reset interface 1/8
 Done
<!--NeedCopy-->
```

So setzen Sie eine Netzwerkschnittstelle mit der GUI zurück:

1. Navigieren Sie zu **System > Netzwerk > Interfaces**.
2. Wählen Sie die Netzwerkschnittstelle aus, und wählen Sie in der Liste **Aktion** die Option **Schnittstelle zurücksetzen** aus.

Überwachen einer Netzwerkschnittstelle

Sie können Netzwerkschnittstellenstatistiken anzeigen, um Parameter zu überwachen und die Informationen verwenden, um den Zustand der Netzwerkschnittstelle zu überprüfen. Sie können Parameter überwachen, z. B. gesendete und empfangene Pakete, Durchsatz, LACP-Dateneinheiten (Link Aggregate Control Protocol) und Fehler. Sie können die Statistiken einer Netzwerkschnittstelle löschen, um ihre Statistiken ab dem Zeitpunkt zu überwachen, an dem die Statistiken gelöscht werden.

So zeigen Sie die Statistiken der Netzwerkschnittstellen mit der Befehlszeilenschnittstelle an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
-  stat interface <interface_num>
<!--NeedCopy-->
```

Beispiel:

```
> stat interface 1/8
 Done
<!--NeedCopy-->
```

So löschen Sie die Statistiken einer Netzwerkschnittstelle mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
-  clear interface <interface_num>
<!--NeedCopy-->
```

Beispiel:


```
> clear interface 1/8
 Done
<!--NeedCopy-->
```

So zeigen Sie die Statistiken einer Schnittstelle mit der GUI an:

Navigieren Sie zu **System > Netzwerk > Schnittstellen**, wählen Sie die Netzwerkschnittstelle aus, und klicken Sie auf **Schnittstellenstatistik**.

So löschen Sie die Statistiken einer Netzwerkschnittstelle mit der GUI:

1. Navigieren Sie zu **System > Netzwerk > Interfaces**.
2. Wählen Sie die Netzwerkschnittstelle aus, und wählen Sie in der Liste **Aktion** die Option **Statistik löschen** aus.

Konfigurieren von Weiterleitungssitzungsregeln

October 5, 2021

Standardmäßig erstellt die Citrix ADC Appliance keine Sitzungseinträge für Datenverkehr, den sie nur weiterleitet (L3-Modus). Für einen Fall, in dem eine Clientanforderung, die die Appliance an einen Server weiterleitet, zu einer Antwort führt, die über denselben Pfad zurückkehren muss, können Sie eine Weiterleitungssitzungsregel erstellen. Eine Forwarding-Sitzungsregel erstellt Forwarding-Sitzungseinträge für Datenverkehr, der von einem bestimmten Netzwerk stammt oder für ein bestimmtes Netzwerk bestimmt ist und vom Citrix ADC weitergeleitet wird. Sie können Weiterleitungssitzungsregeln für IPv4-Datenverkehr und IPv6-Datenverkehr erstellen.

Beim Konfigurieren einer IPv4-Weiterleitungssitzungsregel können Sie entweder eine IPv4-Netzwerkadresse oder eine erweiterte ACL als Bedingung für die Identifizierung des IPv4-Datenverkehrs angeben, für den ein Weiterleitungssitzungseintrag erstellt werden soll:

- **Netzwerkadresse**. Wenn Sie eine IPv4-Netzwerkadresse angeben, erstellt die Appliance Weiterleitungssitzungen für IPv4-Datenverkehr, deren Quelle oder Ziel mit der Netzwerkadresse übereinstimmt.
- **Erweiterte ACL-Regel**. Wenn Sie eine erweiterte ACL-Regel angeben, erstellt die Appliance Weiterleitungssitzungen für IPv4-Datenverkehr, die den in der erweiterten ACL-Regel angegebenen Bedingungen entsprechen.

Beim Konfigurieren einer IPv6-Weiterleitungssitzungsregel können Sie entweder ein IPv6-Präfix oder ein ACL6 als Bedingung für die Identifizierung von IPv6-Datenverkehr angeben, für den ein Weiterleitungssitzungseintrag erstellt werden soll:

- **IPv6-Präfix**. Wenn Sie ein IPv6-Präfix angeben, erstellt die Appliance Weiterleitungssitzungen für IPv6-Datenverkehr, deren Quelle oder Ziel mit dem IPv6-Präfix übereinstimmt.
- **ACL6-Regel**. Wenn Sie eine ACL6-Regel angeben, erstellt die Appliance Weiterleitungssitzungen für IPv6-Datenverkehr, die den in der ACL6-Regel angegebenen Bedingungen entsprechen.

So erstellen Sie eine IPv4-Weiterleitungssitzungsregel mit der CLI:

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

- add forwardingSession <name> [<network> <netmask>] | [-aclname <string>] -connfailover (ENABLED | DISABLED)
- show forwardingSession

Beispiel:

```
A network address as the condition:

> add forwardingSession fs-nw-1 10.102.105.51 255.255.255.255
 Done

An ACL as the condition:

> add forwardingSession fs-acl-1 acl1
 Done
<!--NeedCopy-->
```

So konfigurieren Sie eine IPv4-Weiterleitungssitzungsregel mit der GUI:

Navigieren Sie zu System > Netzwerk > Weiterleitungssitzungen, fügen Sie eine neue IPv4-Weiterleitungssitzung hinzu oder bearbeiten Sie eine vorhandene Weiterleitungssitzung.

So erstellen Sie eine IPv6-Weiterleitungssitzungsregel mit der CLI:

- Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Weiterleitungssitzungsregel zu erstellen und die Konfiguration zu überprüfen:
  - add forwardingSession <name> [<IPv6 prefix>] | [-acl6name <string>]
  - show forwardingSession

  Beispiel:

```
    An IPv6 prefix as the condition:

    > add forwardingSession fsv6-pfx-1 3ffe::/64
```



```
4       Done
5
6      An ACL6 rule as the condition:
7
8      > add forwardingSession fsv6-acl6-1  -acl6name ACL6-FS
9       Done
10 <!--NeedCopy-->
```

So konfigurieren Sie eine IPv6-Weiterleitungssitzungsregel mit der GUI:

Navigieren Sie zu System > Netzwerk > Weiterleitungssitzungen, fügen Sie eine neue IPv6-Weiterleitungssitzung hinzu oder bearbeiten Sie eine vorhandene Weiterleitungssitzung.

Zuweisen einer ACL-Regel zu einer vorhandenen Weiterleitungssitzungsregel

Sie können eine ACL-Regel einer Netzwerkadresse/IPv6-Präfix-basierten Weiterleitungssitzungsregel zuweisen. In diesem Fall wird sie zu einer ACL-basierten Weiterleitungssitzungsregel. Sie können eine vorhandene ACL-Regel auch in einer ACL-basierten Weiterleitungssitzungsregel in eine andere ACL-Regel ändern. Nachdem die vorhandenen zugehörigen Weiterleitungssitzungseinträge (falls vorhanden) ein Zeitlimit überschritten haben, verwenden die Regeln die neu zugewiesene ACL, um IPv4/IPv6-Datenverkehr zu identifizieren, für die ein Weiterleitungssitzungseintrag erstellt werden soll.

So weisen Sie einer vorhandenen IPv4-Weiterleitungssitzungsregel mit der CLI eine erweiterte ACL-Regel zu:

Geben Sie an der Eingabeaufforderung

- `set forwardingSession <name> [-aclname <string>]`
- `show forwardingSession <name>`

So weisen Sie einer vorhandenen IPv6-Weiterleitungssitzungsregel mit der CLI eine ACL6-Regel zu:

Geben Sie an der Eingabeaufforderung

- `set forwardingSession <name> [-acl6name <string>]`
- `show forwardingSession <name>`

Beispiel:

```
1 > add forwardingSession FS-1 -aclname ACL-9
2 Done
3
4 > add forwardingSession FS6-1  -acl6name ACL6-9
5 Done
```


Deaktivieren der Lenkung für Weiterleitungssitzungen in einem Cluster-Setup

Das Standardverhalten eines Citrix ADC Clusters besteht darin, dass der Knoten, der Datenverkehr empfängt (Flow Receiver), den Datenverkehr auf einen anderen Knoten (Flow Processor) leitet, der den Datenverkehr verarbeitet. Die Leitung des Datenverkehrs vom Flowempfänger zum Flowprozessor erfolgt über die Cluster-Backplane und wird als Lenkung bezeichnet.

Die Steuerung kann ein Overhead für die Echtzeitverarbeitung sein oder wenn das Setup Verbindungen mit hoher Latenz enthält.

Die Steuerung für Weiterleitungssitzungen kann nun deaktiviert werden, sodass die Verarbeitung lokal zum Flow-Empfänger wird. Das heißt, der Strömungsempfänger wird zum Flussprozessor.

Voraussetzungen

Beachten Sie die folgenden Punkte, bevor Sie Weiterleitungssitzungsregeln in einem Cluster-Setup konfigurieren:

- Sie müssen Linksets für Weiterleitungssitzungen konfigurieren.
- Sie müssen MAC Based Forwarding (MBF) im Cluster-Setup aktivieren.

Konfigurieren von Weiterleitungssitzungsregeln in einem Cluster-Setup

Das Deaktivieren der Steuerung für die Weiterleitung von Sitzungsregeln in einem Cluster-Setup kann auf den folgenden zwei Ebenen erfolgen:

- **Spezifische Weiterleitungssitzungsregelebene**. Aktivieren Sie den Parameter Lokal verarbeiten, während Sie eine neue Weiterleitungssitzungsregel hinzufügen oder eine vorhandene Weiterleitungssitzungsregel bearbeiten.
- **Globale Ebene**. Aktivieren Sie den Parameter Lokal verarbeiten, während Sie eine neue Clusterinstanz hinzufügen oder eine vorhandene Clusterinstanz bearbeiten. Die globale Einstellung hat Vorrang vor der Weiterleitungssitzungsregel.

CLI-Verfahren

So deaktivieren Sie die Steuerung für eine Weiterleitungssitzungsregel für ein Cluster-Setup mit der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehlssätze ein:

- Wenn Sie eine neue Weiterleitungssitzungsregel hinzufügen:
  - **add forwardingSession** <name> ((<network> [<netmask>]) | -**acl6name** <string> | -**aclname** <string>) -**processLocal ENABLED**
  - **show forwardingSession** <name>

- Wenn Sie eine vorhandene Weiterleitungssitzungsregel neu konfigurieren:
  - **set forwardingSession** <name> -**processLocal ENABLED**
  - **show forwardingSession** <name>

So deaktivieren Sie die Steuerung für alle Weiterleitungssitzungsregeln (globale Ebene) in einem Cluster-Setup mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehlssätze ein:

- Wenn Sie eine neue Clusterinstanz hinzufügen:
  - **add cluster instance** <clid> -**processLocal Enabled**
  - **show cluster instance** <clid>
- Wenn Sie eine vorhandene Clusterinstanz neu konfigurieren:
  - **set cluster instance** <clid> -**processLocal Enabled**
  - **show cluster instance** <clid>

Beispielkonfiguration:

Im Folgenden finden Sie zwei Beispiele für die Deaktivierung der Steuerung auf der Ebene der Weiterleitungssitzung und ein Beispiel für die Deaktivierung der Steuerung auf globaler Ebene.

```
An IPv4 forwarding session rule:

> add forwardingSession FWD-SESSN-PROCSS-LOCL-IPV4-1 10.102.105.51
    255.255.255.255 -processLocal Enabled
Done

An IPv6 forwarding session rule:

> add forwardingSession FWD-SESSN-PROCSS-LOCL-IPV6-1  - acl6name ACL6-
    FWD-SESSN-1 -processLocal Enabled
Done

A cluster setup, with an instance ID 10, has steering disabled at
    global level:

> set cluster instance 10 -processLocal Enabled
Done
<!--NeedCopy-->
```

GUI-Verfahren

So deaktivieren Sie die Steuerung für eine Weiterleitungssitzungsregel für ein Cluster-Setup mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **Weiterleitungssitzungen**, wählen Sie **Lokal verarbeiten** aus, während Sie eine neue Weiterleitungssitzungsregel hinzufügen oder eine vorhandene Weiterleitungssitzungsregel bearbeiten.

So deaktivieren Sie die Steuerung für alle Weiterleitungssitzungsregeln für ein Cluster-Setup mit der GUI:

Navigieren Sie zu **System** > **Cluster**, und wählen Sie **Lokal verarbeiten** aus, während Sie eine Clusterkonfiguration hinzufügen oder eine vorhandene Clusterkonfiguration ändern.

Grundlegendes zu VLANs

October 5, 2021

Eine Citrix ADC Appliance unterstützt Layer 2-Port und IEEE 802.1q getaggte VLANs. VLAN-Konfigurationen sind nützlich, wenn Sie den Verkehr auf bestimmte Gruppen von Stationen beschränken müssen. Sie können eine Netzwerkschnittstelle als Teil mehrerer VLANs konfigurieren, indem Sie IEEE 802.1q-Tagging verwenden.

Sie können VLANs konfigurieren und an IP-Subnetze binden. Das Citrix ADC führt dann die IP-Weiterleitung zwischen diesen VLANs durch (wenn es als Standardrouter für die Hosts in diesen Subnetzen konfiguriert ist).

Citrix ADC unterstützt die folgenden VLAN-Typen:

- **Port-basierte VLANs.** Die Mitgliedschaft in einem portbasierten VLAN wird durch eine Reihe von Netzwerkschnittstellen definiert, die eine gemeinsame, exklusive Layer-2-Broadcastdomäne verwenden. Sie können mehrere portbasierte VLANs konfigurieren. Standardmäßig sind alle Netzwerkschnittstellen auf dem Citrix ADC Mitglieder von VLAN 1.

  Wenn Sie 802.1q-Tagging auf den Port anwenden, gehört die Netzwerkschnittstelle zu einem portbasierten VLAN. Layer-2-Datenverkehr wird in einem portbasierten VLAN überbrückt, und Layer-2-Übertragungen werden an alle Mitglieder des VLAN gesendet, wenn der Layer-2-Modus aktiviert ist. Wenn Sie eine nicht markierte Netzwerkschnittstelle als Mitglied eines neuen VLAN hinzufügen, wird sie aus dem aktuellen VLAN entfernt.

- **Standard-VLAN.** Standardmäßig sind die Netzwerkschnittstellen des Citrix ADC in einem einzigen, portbasierten VLAN als nicht getaggte Netzwerkschnittstellen enthalten. Dieses VLAN ist das Standard-VLAN. Es hat eine VLAN-ID (VID) von 1. Dieses VLAN ist dauerhaft vorhanden. Es kann nicht gelöscht werden und seine VID kann nicht geändert werden.

Wenn Sie eine Netzwerkschnittstelle zu einem anderen VLAN als Mitglied ohne Tags hinzufügen, wird die Netzwerkschnittstelle automatisch aus dem Standard-VLAN entfernt. Wenn Sie die Bindung einer Netzwerkschnittstelle von ihrem aktuellen portbasierten VLAN aufheben, wird sie erneut dem Standard-VLAN hinzugefügt.

- **Mit VLANs gekennzeichnet.** 802.1q-Tagging (definiert im IEEE 802.1q-Standard) ermöglicht es einem Netzwerkgerät (z. B. dem Citrix ADC), einem Frame auf Layer 2 Informationen hinzuzufügen, um die VLAN-Mitgliedschaft des Frames zu identifizieren. Tagging ermöglicht Netzwerkumgebungen VLANs, die sich über mehrere Geräte erstrecken. Ein Gerät, das das Paket empfängt, liest das Tag und erkennt das VLAN, zu dem der Frame gehört. Einige Netzwerkgeräte unterstützen den Empfang von markierten und nicht markierten Paketen auf derselben Netzwerkschnittstelle nicht, insbesondere Force10-Switches. In solchen Fällen müssen Sie sich an den Kundendienst wenden, um Hilfe zu erhalten.

  Die Netzwerkschnittstelle kann ein markierter oder nicht markierter Member eines VLAN sein. Jede Netzwerkschnittstelle ist nur ein nicht getaggtes Mitglied eines VLAN (natives VLAN). Diese Netzwerkschnittstelle überträgt die Frames für das native VLAN als nicht markierte Frames. Eine Netzwerkschnittstelle kann Teil von mehr als einem VLAN sein, wenn die anderen VLANs getaggt sind.

  Achten Sie beim Konfigurieren der Tagging darauf, dass Sie mit der Konfiguration des VLAN an beiden Enden der Verbindung übereinstimmen. Der Port, zu dem der Citrix ADC eine Verbindung herstellt, muss sich im gleichen VLAN wie die Citrix ADC-Netzwerkschnittstelle befinden.

  Hinweis: Diese VLAN-Konfiguration ist weder synchronisiert noch weitergegeben, daher müssen Sie die Konfiguration für jede Einheit in einem HA-Paar unabhängig durchführen.

Regeln zum Klassifizieren von Frames anwenden

VLANs haben zwei Arten von Regeln zum Klassifizieren von Frames:

- **Eindringen Regeln.** Ingress-Regeln klassifizieren jeden Frame als nur zu einem einzelnen VLAN. Wenn ein Frame auf einer Netzwerkschnittstelle empfangen wird, werden die folgenden Regeln angewendet, um den Frame zu klassifizieren:
  - Wenn der Frame nicht markiert ist oder einen Tag-Wert gleich 0 hat, wird die VID des Frames auf den Port VID (PVID) der empfangenden Schnittstelle gesetzt, der als gehörend zum nativen VLAN klassifiziert wird. (PVIDs sind im IEEE 802.1q-Standard definiert.)
  - Wenn Frame einen Tag-Wert gleich FFF aufweist, wird der Frame gelöscht.
  - Wenn die VID des Frames ein VLAN angibt, dessen empfangende Netzwerkschnittstelle kein Mitglied ist, wird der Frame gelöscht. Wenn beispielsweise ein Paket aus einem Subnetz mit VLAN-ID 12 an ein Subnetz gesendet wird, das mit VLAN-ID 10 verknüpft ist, wird das Paket gelöscht. Wenn ein nicht getaggtes Paket mit VID 9 aus dem Subnetz mit VLAN-ID 10 an eine Netzwerkschnittstelle PVID 9 gesendet wird, wird das Paket gelöscht.

- **Ausreiher Regeln.** Es gelten folgende Regeln für den Ausstieg:
  - Wenn die VID des Frames ein VLAN angibt, dessen Übertragungsnetzwerkschnittstelle kein Mitglied ist, wird der Frame verworfen.
  - Während des Lernprozesses (definiert durch den IEEE 802.1q-Standard) werden Src MAC und VID verwendet, um die Bridge-Nachschlagetabelle des Citrix ADC zu aktualisieren.
  - Ein Frame wird verworfen, wenn seine VID ein VLAN angibt, das keine Mitglieder hat. (Sie definieren Elemente, indem Sie Netzwerkschnittstellen an ein VLAN binden.)

VLANs und Paketweiterleitung auf dem Citrix ADC

Der Weiterleitungsprozess auf der Citrix ADC Appliance ist ähnlich wie bei jedem Standard-Switch. Citrix ADC führt die Weiterleitung jedoch nur dann durch, wenn der Layer-2-Modus aktiviert ist. Die wichtigsten Merkmale des Weiterleitungsprozesses sind:

- Topologieeinschränkungen werden erzwungen. Die Erzwingung umfasst die Auswahl jeder Netzwerkschnittstelle im VLAN als Übertragungsport (abhängig vom Zustand der Netzwerkschnittstelle), Überbrückungsbeschränkungen (nicht auf der empfangenden Netzwerkschnittstelle weiterleiten) und MTU-Einschränkungen.
- Frames werden anhand von Informationen in der Bridge-Tabellensuche in der Forwarding Database (FDB) -Tabelle des Citrix ADC gefiltert. Die Bridge-Tabellensuche basiert auf dem Ziel-MAC und der VID. Pakete, die an die MAC-Adresse des Citrix ADC adressiert werden, werden auf den oberen Schichten verarbeitet.
- Alle Broadcast- und Multicast-Frames werden an jede Netzwerkschnittstelle weitergeleitet, die Mitglied des VLAN ist. Weiterleitung erfolgt jedoch nur, wenn der L2-Modus aktiviert ist. Wenn der L2-Modus deaktiviert ist, werden die Broadcast- und Multicastpakete gelöscht. Dies gilt auch für MAC-Adressen, die sich derzeit nicht in der Bridging-Tabelle befinden.
- Ein VLAN-Eintrag enthält eine Liste von Netzwerkschnittstellen, die Teil seiner nicht markierten Elementgruppe sind. Beim Weiterleiten von Frames an diese Netzwerkschnittstellen wird kein Tag in den Frame eingefügt.
- Wenn die Netzwerkschnittstelle ein markierter Member dieses VLAN ist, wird das Tag beim Weiterleiten des Frames in den Frame eingefügt.

Wenn ein Benutzer Broadcast- oder Multicastpakete sendet, ohne dass das VLAN identifiziert wird, d. h. bei der Erkennung von doppelten Adressen (DAD) für NSIP oder ND6 für den nächsten Hop der Route, wird das Paket auf allen Netzwerkschnittstellen gesendet, wobei entsprechende Tagging entweder auf den Ingress und Egress Regeln basieren. ND6 identifiziert normalerweise ein VLAN, und ein Datenpaket wird nur in diesem VLAN gesendet. Port-basierte VLANs sind für IPv4 und IPv6 üblich. Für IPv6 unterstützt Citrix ADC Präfix-basierte VLANs.

Konfigurieren eines VLAN

October 5, 2021

Sie können VLANs in den folgenden Umgebungen implementieren:

- Einzelnes Subnetz
- Mehrere Subnetze
- Einzelnes LAN
- VLANs (kein Tagging)
- VLANs (802.1q-Tagging)

Wenn Sie VLANs konfigurieren, die nur nicht getaggte Netzwerkschnittstellen als Mitglieder haben, ist die Gesamtzahl der möglichen VLANs auf die Anzahl der im Citrix ADC verfügbaren Netzwerkschnittstellen beschränkt. Wenn mehr IP-Subnetze mit einer VLAN-Konfiguration erforderlich sind, muss 802.1q-Tagging verwendet werden.

Wenn Sie eine Netzwerkschnittstelle an ein VLAN binden, wird die Netzwerkschnittstelle aus dem Standard-VLAN entfernt. Wenn die Netzwerkschnittstellen Teil von mehr als einem VLAN sein müssen, können Sie die Netzwerkschnittstellen als getaggte Mitglieder an die VLANs binden.

Sie können Citrix ADC so konfigurieren, dass Datenverkehr zwischen VLANs auf Layer 3 weitergeleitet wird. In diesem Fall ist ein VLAN einem einzelnen IP-Subnetz zugeordnet. Die Hosts in einem VLAN, die zu einem einzelnen Subnetz gehören, verwenden dieselbe Subnetzmaske und ein oder mehrere Standardgateways, die mit diesem Subnetz verbunden sind. Die Konfiguration von Layer 3 für ein VLAN ist optional. Layer 3 wird für die IP-Weiterleitung (Inter-VLAN-Routing) verwendet. Jedes VLAN verfügt über eine eindeutige IP-Adresse und Subnetzmaske, die ein IP-Subnetz für das VLAN definieren. In einer HA-Konfiguration wird diese IP-Adresse für die anderen Citrix ADC Appliances freigegeben. Das Citrix ADC leitet Pakete zwischen konfigurierten IP-Subnetzen (VLANs) weiter.

Wenn Sie Citrix ADC konfigurieren, dürfen Sie keine überlappenden IP-Subnetze erstellen. Dadurch wird die Layer-3-Funktionalität behindert.

Jedes VLAN ist eine eindeutige Layer-2-Übertragungsdomäne. Zwei VLANs, die jeweils an getrennte IP-Subnetze gebunden sind, können nicht zu einer einzigen Broadcastdomäne kombiniert werden. Für die Weiterleitung von Datenverkehr zwischen zwei VLANs ist ein Layer 3-Weiterleitungsgerät (Routing) erforderlich, z. B. die Citrix ADC Appliance.

Konfigurieren von VLANs in einem HA-Setup

Die VLAN-Konfiguration für ein Hochverfügbarkeitssetup erfordert, dass die Citrix ADC Appliances dieselbe Hardwarekonfiguration aufweisen, und die darauf konfigurierten VLANs müssen Spiegelbilder sein.

Die korrekte VLAN-Konfiguration wird automatisch implementiert, wenn die Konfiguration zwischen den Citrix ADC Appliances synchronisiert wird. Das Ergebnis sind identische Aktionen auf allen Appliances. Wenn Sie beispielsweise die Netzwerkschnittstelle 0/1 zu VLAN2 hinzufügen, wird diese Netzwerkschnittstelle VLAN 2 auf allen Appliances hinzugefügt, die am Hochverfügbarkeitssetup teilnehmen.

Hinweis: Wenn Sie netzwerkschnittstellenspezifische Befehle in einem HA-Setup verwenden, werden die von Ihnen erstellten Konfigurationen nicht an die andere Citrix ADC Appliance weitergegeben. Sie müssen diese Befehle auf jeder Appliance in einem HA-Paar ausführen, um sicherzustellen, dass die Konfiguration der beiden Appliances im HA-Paar synchronisiert bleibt.

Erstellen oder Ändern eines VLAN

Um ein VLAN zu konfigurieren, erstellen Sie eine VLAN-Entität und binden dann Netzwerkschnittstellen und IP-Adressen an das VLAN. Wenn Sie ein VLAN entfernen, werden seine Mitgliedsschnittstellen dem Standard-VLAN hinzugefügt.

CLI-Verfahren

So erstellen Sie ein VLAN mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add vlan <id> [-aliasName <string>] [-ipv6DynamicRouting (ENABLED|DISABLED)]`
- `sh vlan <id>`

Beispiel:

```
1   > add vlan 2 -aliasName "Network A"   Done
2 <!--NeedCopy-->
```

So binden Sie eine Schnittstelle mit der CLI an ein VLAN:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `bind vlan <id> -ifnum <slot/port>`
- `sh vlan <id>`

Beispiel:

```
1   > bind vlan 2 -ifnum 1/8   Done
2 <!--NeedCopy-->
```


So binden Sie eine IP-Adresse mit der CLI an ein VLAN:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `bind vlan <id> -IPAddress <IPAddress> <netMask>`
- `sh vlan <id>`

Beispiel:

```
1    > bind vlan 2 -IPAddress 10.102.29.54 255.255.255.0   Done
2 <!--NeedCopy-->
```

So entfernen Sie ein VLAN mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `rm vlan <id>`

GUI-Verfahren

So konfigurieren Sie ein VLAN mit der GUI:

1. Navigieren Sie zu System > Netzwerk > VLANs, fügen Sie ein neues VLAN hinzu oder bearbeiten Sie ein vorhandenes VLAN.
2. Um eine IP-Adresse an ein VLAN zu binden, wählen Sie unter IP-Bindungen die Option Aktiv aus, die der IP-Adresse entspricht, die Sie an das VLAN binden möchten (z. B. 10.102.29.54). In der Spalte Typ wird der IP-Adresstyp (z. B. zugeordnete IP, virtuelle IP oder Subnetz-IP) für jede IP-Adresse in der Spalte IP-Adresse angezeigt.
3. Um eine Netzwerkschnittstelle an ein VLAN zu binden, wählen Sie unter Interface Bindings die Option Aktiv aus, die der Schnittstelle entspricht, die Sie an das VLAN binden möchten.

Überwachung von VLANs

Sie können VLAN-Statistiken wie empfangene Pakete, empfangene Bytes, gesendete Pakete und gesendete Bytes anzeigen, und mithilfe der Informationen Anomalien identifizieren und ein VLAN debuggen.

So zeigen Sie die Statistiken eines VLAN mit der CLI an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `stat vlan <vlanID>`

Beispiel:


```
  stat vlan 2
<!--NeedCopy-->
```

So zeigen Sie die Statistiken eines VLAN mit der GUI an:

1. Navigieren Sie zu System > Netzwerk > VLANs.
2. Wählen Sie das VLAN aus, und klicken Sie auf Statistiken.

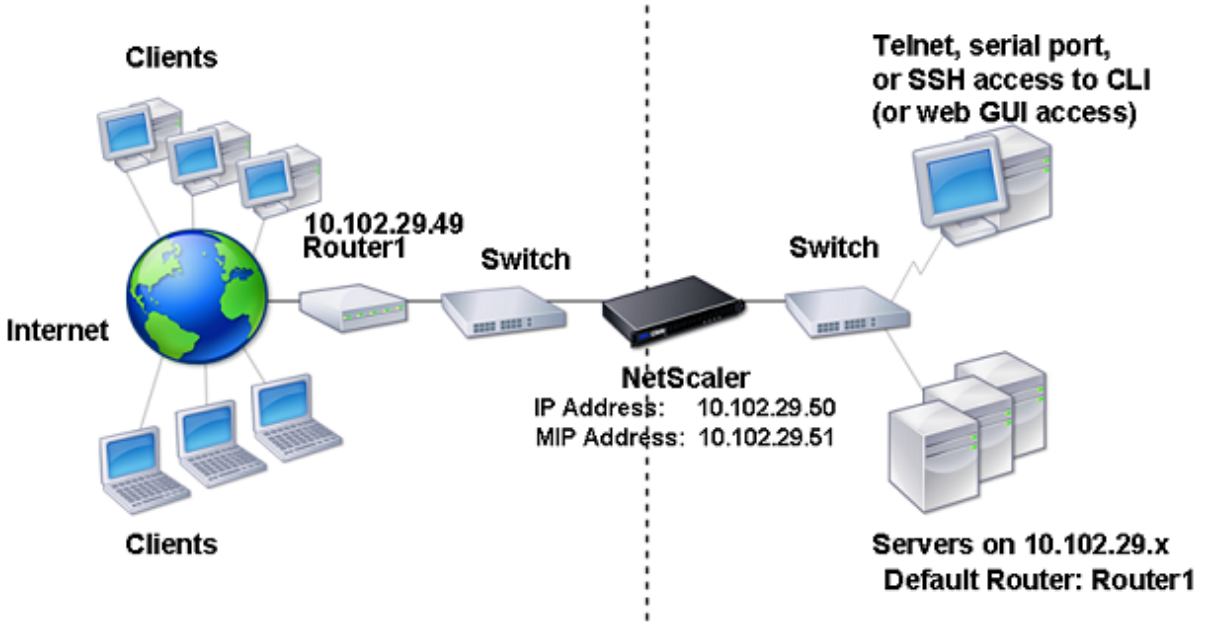
Konfigurieren von VLANs in einem einzelnen Subnetz

October 5, 2021

Bevor Sie ein VLAN in einem einzelnen Subnetz konfigurieren, stellen Sie sicher, dass Layer-2-Modus aktiviert ist.

Die folgende Abbildung zeigt eine einzelne Subnetzumgebung

Abbildung 1. VLAN in einem einzelnen Subnetz



In der obigen Abbildung:

1. Der Standardrouter für Citrix ADC und die Server ist Router 1.
2. Der Layer-2-Modus muss auf dem Citrix ADC aktiviert sein, damit der Citrix ADC direkten Zugriff auf die Server hat.
3. Für dieses Subnetz kann ein virtueller Server für den Lastenausgleich auf der Citrix ADC Appliance konfiguriert werden.

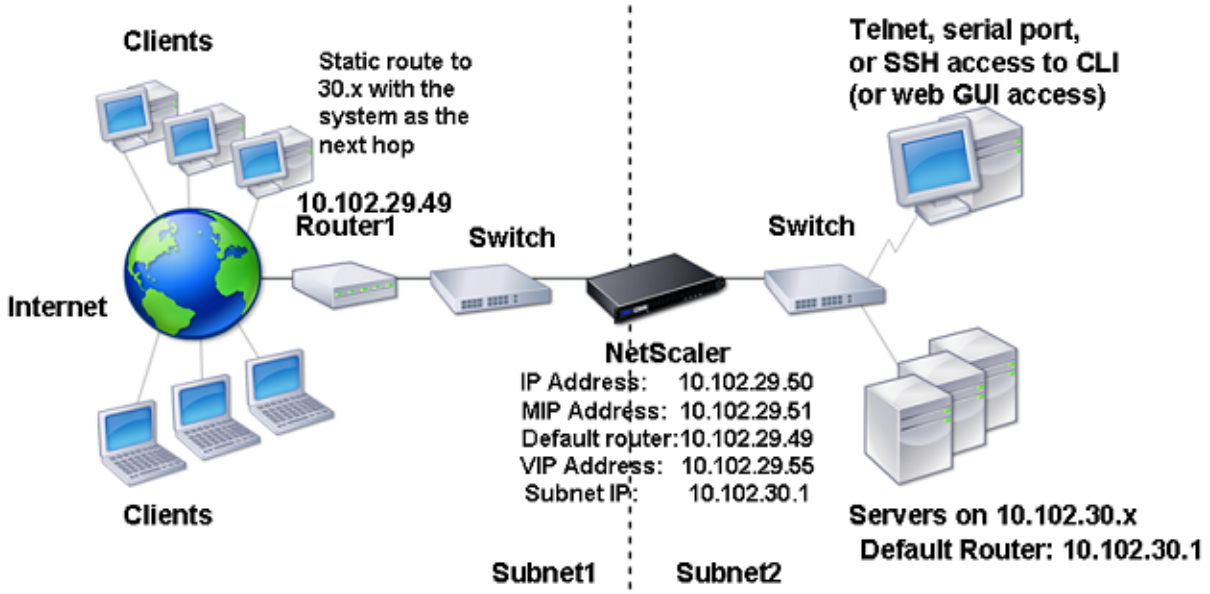
Um ein VLAN in einem einzelnen Subnetz zu konfigurieren, befolgen Sie die unter Konfigurieren eines VLANbeschriebenen Anweisungen.

Konfigurieren von VLANs auf mehreren Subnetzen

October 5, 2021

Um ein einzelnes VLAN über mehrere Subnetze hinweg zu konfigurieren, müssen Sie eine VIP für das VLAN hinzufügen und das Routing entsprechend konfigurieren. Die folgende Abbildung zeigt ein einzelnes VLAN, das über mehrere Subnetze konfiguriert ist.

Abbildung 1. Mehrere Subnetze in einem einzigen VLAN



So konfigurieren Sie ein einzelnes VLAN über mehrere Subnetze hinweg:

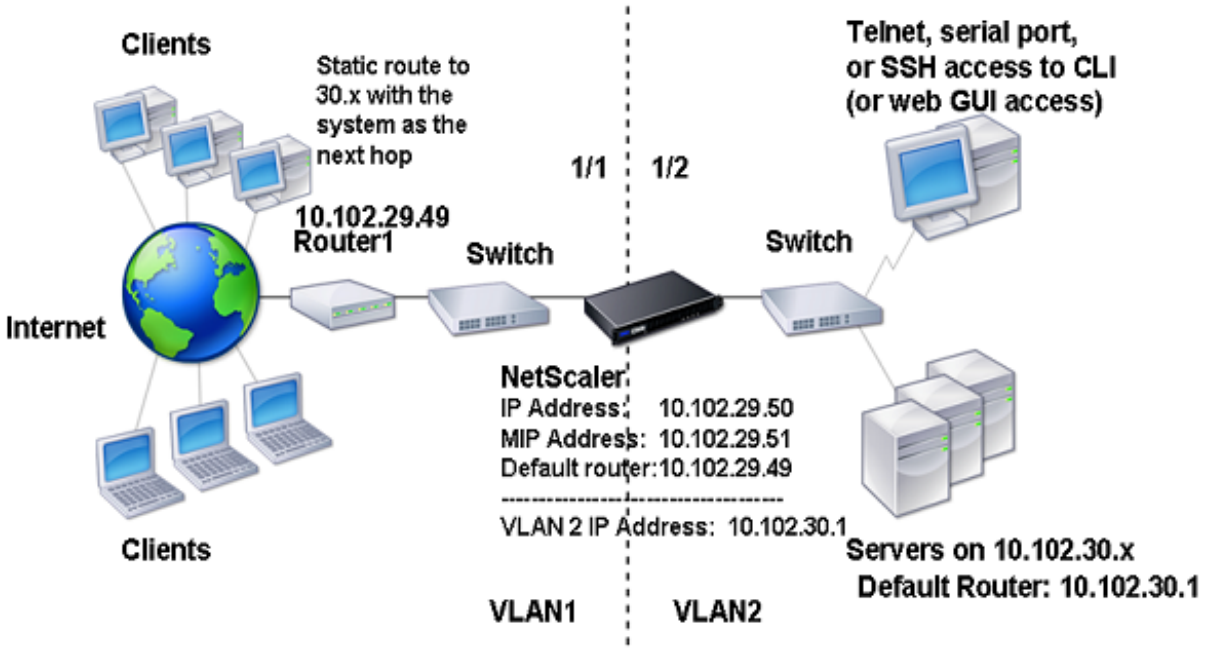
1. Deaktivieren Sie den Layer-2-Modus. Informationen zum Deaktivieren des Layer-2-Modus finden Sie unter Paketweiterleitungsmodi.
2. Fügen Sie eine VIP-Adresse hinzu. Informationen zum Hinzufügen einer VIP-Adresse finden Sie unter Konfigurieren und Verwalten virtueller IP-Adressen (VIPs).
3. RNAT Regel konfigurieren. Informationen zum Konfigurieren der RNAT-ID finden Sie unter Konfigurieren von RNAT.

Konfigurieren mehrerer nicht markierter VLANs über mehrere Subnetze hinweg

October 5, 2021

In Umgebungen mit mehreren nicht markierten VLANs über mehrere Subnetze hinweg wird für jedes IP-Subnetz ein VLAN konfiguriert. Eine Netzwerkschnittstelle ist nur an ein VLAN gebunden. Die folgende Abbildung zeigt diese Konfiguration.

Abbildung 1. Mehrere Subnetze mit VLANs - Kein Tagging



Um die in der obigen Abbildung gezeigte Konfiguration zu implementieren, führen Sie die folgenden Aufgaben aus:

1. Fügen Sie VLAN 2 hinzu.
2. Binden Sie die 1/2 Netzwerkschnittstelle des Citrix ADC als unmarkierte Netzwerkschnittstelle an VLAN 2.
3. Binden Sie die IP-Adresse und die Subnetzmaske an VLAN 2.

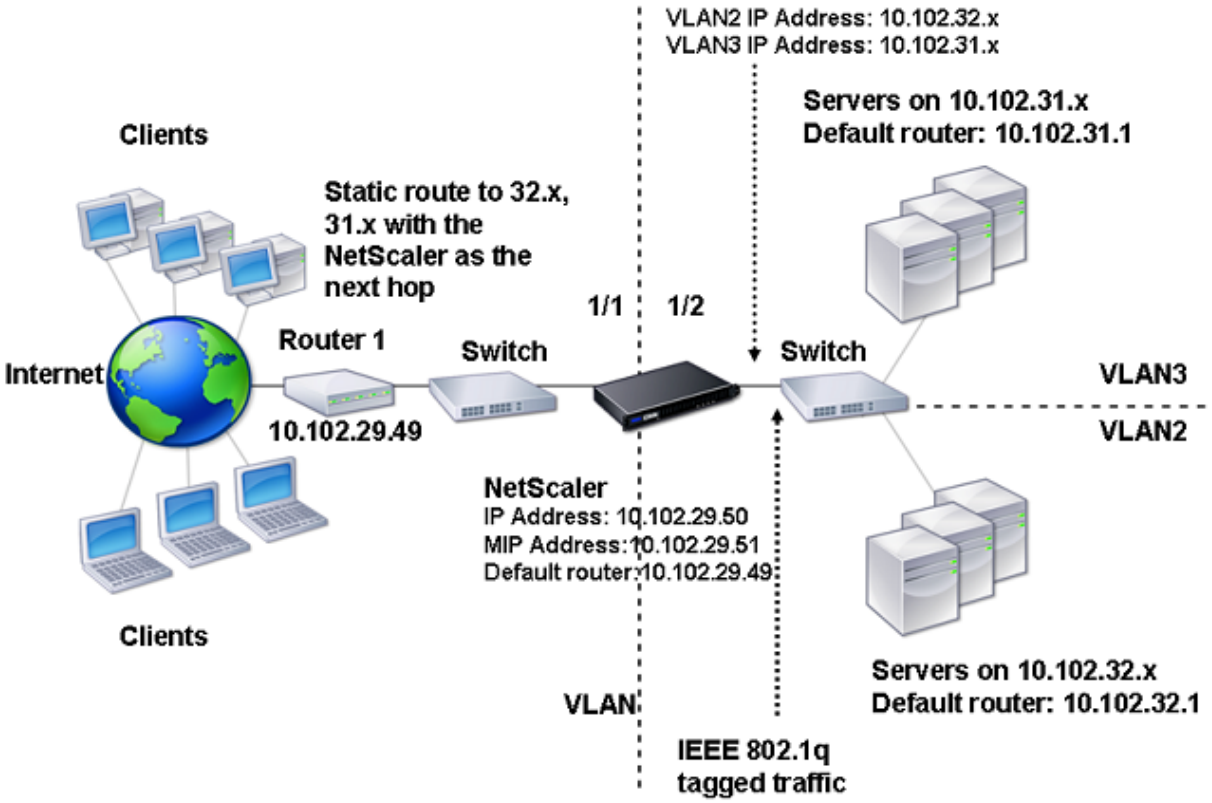
Anweisungen zu diesen Aufgaben finden Sie unter Konfigurieren eines VLAN.

Konfigurieren mehrerer VLANs mit 802.1q-Tagging

October 5, 2021

Bei mehreren VLANs mit 802.1q-Tagging wird jedes VLAN mit einem anderen IP-Subnetz konfiguriert. Jede Netzwerkschnittstelle befindet sich in einem VLAN. Einer der VLANs ist als Tagged eingerichtet. Die folgende Abbildung zeigt diese Konfiguration.

Abbildung 1. Mehrere VLANs mit IEEE 802.1q-Tagging



Um die in der obigen Abbildung gezeigte Konfiguration zu implementieren, führen Sie die folgenden Aufgaben aus:

1. Fügen Sie VLAN 2 hinzu.
2. Binden Sie die 1/2 Netzwerkschnittstelle des Citrix ADC als unmarkierte Netzwerkschnittstelle an VLAN 2.
3. Binden Sie die IP-Adresse und die Netzmaske an VLAN 2.
4. Fügen Sie VLAN hinzu 3.
5. Binden Sie die 1/2 Netzwerkschnittstelle des Citrix ADC als getaggte Netzwerkschnittstelle an VLAN 3.
6. Binden Sie die IP-Adresse und die Netzmaske an VLAN 3.

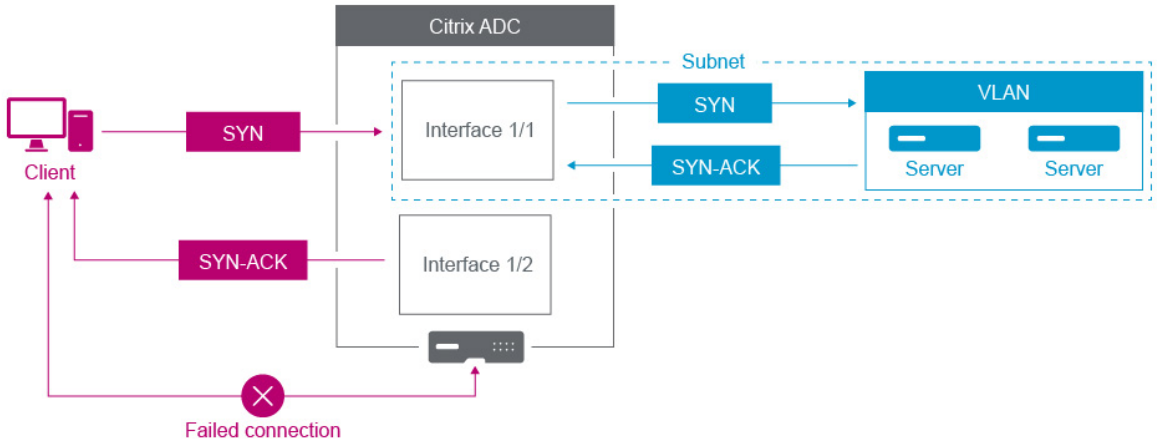
Anweisungen zu diesen Aufgaben finden Sie unter Konfigurieren eines VLAN.

Zuordnen eines IP-Subnetzes mit einer Citrix ADC Schnittstelle mithilfe von VLANs

October 5, 2021

Standardmäßig bietet eine Citrix ADC Appliance keine Unterscheidung zwischen Netzwerkschnittstellen. Die Appliance funktioniert eher wie ein Netzwerk-Hub als ein Switch. Dies kann zu Layer 3-Netzwerkschleifen führen, bei denen doppelter Datenverkehr auf mehreren Schnittstellen übertragen wird.

In solchen Szenarien ist es je nach Netzwerkdesign möglich, dass eine Anforderung auf einer Schnittstelle übertragen werden kann und die entsprechende Antwort auf einer anderen Schnittstelle empfangen wird.



Beispielsweise kann ein SYN-Paket, das auf einer Schnittstelle gesendet wird, und die SYN-ACK-Antwort, die auf einer anderen Schnittstelle empfangen wird, zu einer fehlgeschlagenen Verbindung führen, da die Appliance erwartet, den SYN-ACK auf derselben Schnittstelle zu empfangen, die das ursprüngliche SYN-Paket gesendet hat.

Um solche Probleme zu beheben, kann die Appliance interne oder externe VLANs verwenden, um bestimmte Subnetze Schnittstellen zuzuordnen.

Voraussetzungen

Bevor Sie mit der Zuordnung eines IP-Subnetzes mit einer Citrix ADC Schnittstelle mithilfe von VLANs beginnen, beachten Sie die folgenden Punkte:

- Die Netzwerkkonnektivität kann versehentlich verloren gehen, wenn ein VLAN dem Subnetz oder der Schnittstelle zugeordnet wird, das derzeit für den Zugriff auf die Citrix ADC GUI oder die Befehlszeilenschnittstelle verwendet wird. Daher wird in solchen Szenarien dringend empfohlen, dass die Änderung durch den Zugriff auf die Befehlszeilenschnittstelle über die serielle

Konsole einer physischen Citrix ADC-Appliance oder über die virtuelle serielle Konsole eines Citrix ADC VPX vorgenommen wird.

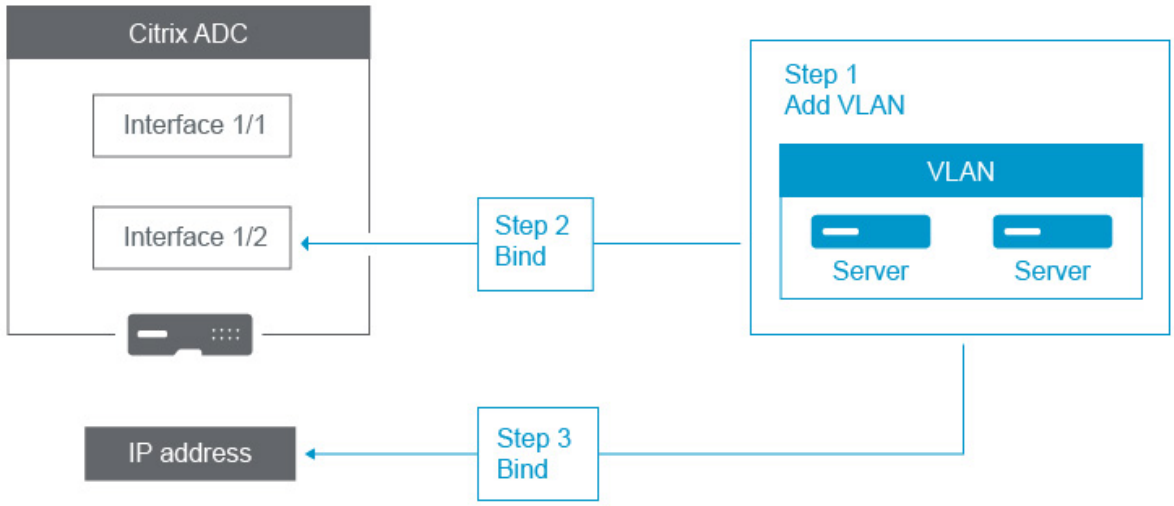
- Citrix ADC Verwaltungsschnittstellen fehlen bestimmte Hardware-Optimierungsfunktionen, was sie für die Verwendung mit dem Datenverkehr in der Produktion weniger wünschenswert macht. Daher wird empfohlen, Citrix ADC so zu konfigurieren, dass nur die Verwaltungsschnittstellen für den Verwaltungsverkehr (NSIP) verwendet werden. In der Standardkonfiguration gibt es keine logische Unterscheidung zwischen Verwaltungsschnittstellen und Datenschnittstellen auf einem Hardware-NetScaler. Um dieses Ziel zu erreichen, wird empfohlen, dass sich der NSIP auf einem separaten VLAN als Datenverkehr befindet, wodurch sich der Verwaltungsdatenverkehr auf einer separaten Schnittstelle befindet.

  Obwohl das Konzept identisch ist, müssen Sie NSVLAN anstelle der folgenden Anweisungen konfigurieren, um die VLAN-Zuordnungen des Subnetzes zu ändern, das die NSIP-Adresse enthält. Solche Änderungen erfordern auch einen Neustart des Citrix ADC, um wirksam zu werden. Weitere Informationen finden Sie unter Konfigurieren von NSVLAN.

- Bei Citrix ADC SDX wird dringend empfohlen, dass sich das NSIP jeder Instanz im selben Subnetz und VLAN befindet wie die SVM (Management Service GUI) und XenServer des SDX. Die SVM kommuniziert mit Instanzen über das Netzwerk. Wenn sich SVM, XenServer und Instanzen nicht im gleichen VLAN und Subnetz befinden, muss der Verwaltungsdatenverkehr außerhalb des SDX fließen. In diesem Fall können Netzwerkprobleme dazu führen, dass der Instanzstatus gelb oder rot angezeigt wird und dass Verwaltungs- und Konfigurationsänderungen der Citrix ADC Instanzen verhindert werden.

Konfigurationsschritte

Das Zuordnen eines IP-Subnetzes mit einer Citrix ADC Schnittstelle besteht aus den folgenden Aufgaben:



Fügen Sie ein VLANhinzu. Wenn Sie beim Hinzufügen eines VLAN das VLAN kennzeichnen, müssen Sie beim Hinzufügen eines VLAN eine VLAN-Nummer auswählen, die im Netzwerk-Switch für den zugeordneten Switch-Port definiert ist. Wenn das VLAN nicht markiert ist und intern zur Appliance ist, empfiehlt es sich, die VLAN-Nummer auszuwählen, die in der Switch-Konfiguration verfügbar ist.

Binden Sie eine Schnittstelle an das VLAN. Wenn Sie die Link Aggregation verwenden, verknüpfen Sie während der Bindung das VLAN anstelle der physischen Schnittstelle mit dem LA-Kanal (z. B. LA/1). Das VLAN muss nur einer Netzwerkschnittstelle zugeordnet sein.

Wenn Sie den Datenverkehr auf der Schnittstelle markieren möchten, verwenden Sie die Option Tagged (Tag). Andernfalls verlässt der Datenverkehr die Appliance unmarkiert und ist mit dem nativen VLAN des Switch-Port verknüpft.

Binden Sie eine IP-Adresse an das VLAN. Wenn Sie während der Bindung mehr als eine IP-Adresse aus demselben Subnetz binden, tritt ein Fehler auf. Wenn eine IP-Adresse mit einem VLAN verknüpft ist, werden alle IP-Adressen in diesem Subnetz automatisch mit dem VLAN verknüpft.

> **Hinweis:**
>
> In einem Hochverfügbarkeitssetup (HA) werden diese VLAN-Konfigurationen während der HA-Synchronisierung automatisch vom primären Knoten zum sekundären Knoten hinzugefügt. Weitere Informationen zu Hochverfügbarkeits-Setups finden Sie unter Hochverfügbarkeit.

CLI-Verfahren

So fügen Sie ein VLAN mit der CLI hinzu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add vlan** <id>
- **sh vlan** <id>

So binden Sie eine Schnittstelle mit der CLI an ein VLAN:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **bind vlan** <id> -**ifnum** <slot/port>
- **sh vlan** <id>

So binden Sie eine IP-Adresse mit der CLI an ein VLAN:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **bind vlan** <id> -**IPAddress** <IPAddress> <netMask>
- **sh vlan** <id>

Beispiel:


```
> add vlan 100

> bind vlan 100 -ifnum 1/1

> bind vlan 100 -ipAddress 10.0.1.0 255.255.255.0
<!--NeedCopy-->
```

GUI-Verfahren

So konfigurieren Sie ein VLAN mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **VLANs**, fügen Sie ein neues VLAN hinzu.
2. Um eine Netzwerkschnittstelle an ein VLAN zu binden, wählen Sie unter **Interface Bindings** die Option **Aktiv** aus, die der Schnittstelle entspricht, die Sie an das VLAN binden möchten.
3. Um eine IP-Adresse an ein VLAN zu binden, wählen Sie unter **IP-Bindungen** die Option **Aktiv** aus, die der IP-Adresse entspricht, die Sie an das VLAN binden möchten (z. B. 10.102.29.54). In der Spalte **Typ** wird der IP-Adresstyp für jede IP-Adresse in der Spalte **IP-Adresse** angezeigt.

Citrix ADC Appliance-Netzwerk- und VLAN-Best Practices

October 5, 2021

Eine Citrix ADC Appliance ermittelt anhand von VLANs, welche Schnittstelle für welchen Datenverkehr verwendet werden muss. Darüber hinaus ist die Citrix ADC Appliance nicht am Spanning Tree beteiligt. Ohne die richtige VLAN-Konfiguration kann die Citrix ADC Appliance nicht bestimmen, welche Schnittstelle verwendet werden soll, und sie kann eher wie ein HUB als ein Switch oder ein Router funktionieren. Mit anderen Worten, die Citrix ADC Appliance kann für jede Konversation alle Schnittstellen verwenden.

Symptome einer VLAN-Fehlkonfiguration

VLAN-Fehlkonfigurationsproblem kann sich in vielen Formen manifestieren, darunter Leistungsprobleme, Unfähigkeit, Verbindungen herzustellen, zufällig getrennte Sitzungen und in schweren Situationen Netzwerkunterbrechungen scheinbar nicht mit der Citrix ADC Appliance selbst zu tun. Die Citrix ADC Appliance kann außerdem berichten, dass MAC-Verschiebungen, stummgeschaltete Schnittstellen und/oder Management-Schnittstelle Pufferüberläufe übertragen oder empfangen, abhängig von der genauen Art der Interaktion mit Ihrem Netzwerk.

MAC Moves (Zähler nic_tot_bdg_mac_moved): Dieses Problem weist darauf hin, dass die Citrix ADC Appliance mehr als eine Schnittstelle für die Kommunikation mit demselben Gerät (MAC-Adresse) verwendet, da sie nicht richtig bestimmen konnte, welche Schnittstelle verwendet werden soll.

Stummgeschaltete Schnittstellen (Zähler nic_err_bdg_muted): Dieses Problem weist darauf hin, dass die Citrix ADC Appliance erkannt hat, dass sie aufgrund von VLAN-Konfigurationsproblemen eine Routingschleife erstellt und daher eine oder mehrere der störenden Schnittstellen heruntergefahren hat, um ein Netzwerk zu verhindern Ausfall.

Schnittstellenpufferüberläufe, die sich normalerweise auf Verwaltungsschnittstellen beziehen (counter nic_err_tx_overflow): Dieses Problem kann verursacht werden, wenn zu viel Datenverkehr über eine Management-Schnittstelle übertragen wird. Verwaltungsschnittstellen der Citrix ADC Appliance sind nicht für die Verarbeitung großer Datenmengen ausgelegt. Dies kann dazu führen, dass Netzwerk- und VLAN-Fehlkonfigurationen auftreten, die die Citrix ADC-Appliance dazu führen, eine Verwaltungsschnittstelle für den Datenverkehr in der Produktion zu verwenden. Dies tritt häufig auf, weil die Citrix ADC Appliance keine Möglichkeit hat, den Datenverkehr im VLAN/Subnetz des NSIP (NSVLAN) vom regulären Produktionsverkehr zu unterscheiden. Es wird dringend empfohlen, dass sich das NSIP in einem separaten VLAN und Subnetz von allen Produktionsgeräten wie Workstations und Servern befindet.

Orphan ACK (Leistungsindikator tcp_err_orphan_ack): Dieses Problem weist darauf hin, dass die Citrix ADC Appliance ein ACK-Paket empfangen hat, das sie nicht erwartet hat, normalerweise auf einer anderen Schnittstelle als der ACK-Datenverkehr. Diese Situation kann durch VLAN-Fehlkonfigurationen verursacht werden, bei denen die Citrix ADC Appliance auf einer anderen Schnittstelle überträgt, als das Zielgerät normalerweise für die Kommunikation mit der Citrix ADC-Appliance verwenden würde (häufig in Verbindung mit MAC-Verschiebungen).

Hohe Übertragungsraten oder Wiederübertragungsraten (Zähler: tcp_err_retransmit_giveups, tcp_err_7th_retransmit, verschiedene andere Wiederübertragungszähler): Die Citrix ADC Appliance versucht, ein TCP-Paket insgesamt 7 Mal neu zu übertragen, bevor sie aufgibt und die Verbindung beendet. Obwohl diese Situation durch Netzwerkbedingungen verursacht werden kann, tritt sie häufig als Folge von VLAN- und Schnittstellen-Fehlkonfiguration auf.

Hochverfügbarkeit Split Brain: Split Brain ist eine Bedingung, bei der beide Hochverfügbarkeitsknoten glauben, dass sie primär sind, was zu doppelten IP-Adressen und zum Verlust der Citrix ADC Appliance-Funktionalität führt. Dies wird verursacht, wenn die beiden Hochverfügbarkeitsknoten nicht miteinander über Hochverfügbarkeits-Heartbeats auf UDP-Port 3003 über das NSIP über eine beliebige Schnittstelle miteinander kommunizieren können. Dies wird in der Regel durch VLAN-Fehlkonfigurationen verursacht, bei denen das native VLAN auf den Citrix ADC Appliance-Schnittstellen keine Konnektivität zwischen Citrix ADC-Appliances aufweist.

Best Practices für VLAN- und Netzwerkkonfigurationen

1. Jedes Subnetz muss einem VLAN zugeordnet sein.
2. Mehrere Subnetze können demselben VLAN zugeordnet werden (abhängig vom Netzwerkdesign).
3. Jedes VLAN sollte nur einer Schnittstelle zugeordnet sein (für die Zwecke dieser Diskussion zählt ein LA-Kanal als eine einzige Schnittstelle).
4. Wenn mehr als ein Subnetz einer Schnittstelle zugeordnet werden muss, müssen die Subnetze mit Tags versehen sein.
5. Entgegen der landläufigen Meinung ist die Funktion Mac-Based-Forwarding (MBF) der Citrix ADC Appliance nicht dazu ausgelegt, diese Art von Problem zu verringern. MBF wurde in erster Linie für den DSR-Modus (Direct Server Return) der Citrix ADC Appliance entwickelt, der in den meisten Umgebungen selten verwendet wird (es ist so konzipiert, dass Datenverkehr die Citrix ADC-Appliance auf dem Rückgabepfad von den Back-End-Servern absichtlich umgehen kann). MBF kann VLAN-Probleme in einigen Fällen verbergen, aber es sollte nicht verlassen werden, um diese Art von Problem zu lösen.
6. Jede Schnittstelle der Citrix ADC Appliance erfordert ein natives VLAN (im Gegensatz zu Cisco, wo native VLANs optional sind), obwohl die TagAll-Einstellung auf einer Schnittstelle verwendet werden kann, sodass kein nicht markierter Datenverkehr die betreffende Schnittstelle verlässt.
7. Das native VLAN kann bei Bedarf für Ihr Netzwerkdesign getaggt werden (dies ist die TagAll-Option für die Schnittstelle).
8. Das VLAN für das Subnetz des NSIP Ihrer Citrix ADC Appliance ist ein Sonderfall. Dies wird NSVLAN genannt. Die Konzepte sind identisch, aber die Befehle zur Konfiguration sind unterschiedlich, und Änderungen am NSVLAN erfordern einen Neustart der Citrix ADC Appliance. Wenn Sie versuchen, ein VLAN an ein SNIP zu binden, das dasselbe Subnetz wie das NSIP teilt, erhalten Sie Operation not permitted. Dies liegt daran, dass Sie stattdessen die NSVLAN-Befehle verwenden müssen. Außerdem können Sie bei einigen Firmware-Versionen kein NSVLAN festlegen, wenn diese VLAN-Nummer mit dem`add VLAN` Befehl vorhanden ist. Entfernen Sie einfach das VLAN und stellen Sie dann das NSVLAN wieder ein.
9. Heartbeats mit hoher Verfügbarkeit verwenden immer das native VLAN der jeweiligen Schnittstelle (optional markiert, wenn die Option TagAll auf der Schnittstelle gesetzt ist).
10. Es muss eine Kommunikation zwischen mindestens einem Satz nativer VLANs auf den beiden Knoten eines Hochverfügbarkeitspaares erfolgen (dies kann direkt oder über einen Router erfolgen). Die nativen VLANs werden für Hochverfügbarkeits-Heartbeats verwendet. Wenn die Citrix ADC Appliances nicht zwischen nativen VLANs auf einer Schnittstelle kommunizieren können, führt dies zu Hochverfügbarkeits-Failovers und möglicherweise zu einer Split-Hirn-Situation, in

der beide Citrix ADC Appliances für primär halten (was unter anderem zu doppelten IP-Adressen führt).

11. Die Citrix ADC Appliance ist nicht am Spanning Tree beteiligt. Daher ist es nicht möglich, Spanning Tree zu verwenden, um Schnittstellenredundanz bei Verwendung einer Citrix ADC Appliance bereitzustellen. Verwenden Sie stattdessen eine Form der Link-Aggregation (LACP oder manuelle LAG) für diesen Zweck.

    Hinweis: Wenn Sie eine Link-Aggregation zwischen mehreren physischen Switches wünschen, müssen Sie die Switches als virtueller Switch konfiguriert haben, indem Sie eine Funktion wie den Switch-Stack von Cisco verwenden.

12. Die Synchronisation mit hoher Verfügbarkeit und Befehl Propagation verwenden standardmäßig das NSIP/NSVLAN. Um diese in ein anderes VLAN zu trennen, können Sie die SyncVLAN-Option des Befehls `set HA node` verwenden.

13. In der Standardkonfiguration der Citrix ADC Appliance ist nichts integriert, was darauf hinweist, dass eine Verwaltungsschnittstelle (0/1 oder 0/2) nur auf Verwaltungsdatenverkehr beschränkt ist. Diese Einschränkung muss vom Endbenutzer über die VLAN-Konfiguration erzwungen werden. Die Verwaltungsschnittstellen sind nicht für den Datenverkehr ausgelegt, daher muss Ihr Netzwerkdesign diesen Punkt berücksichtigen. Management-Schnittstellen, die auf dem Motherboard der Citrix ADC Appliance enthalten sind, fehlen verschiedene Abladungsfunktionen wie CRC-Abladung, größere Paketpuffer und andere Optimierungen, wodurch sie bei der Handhabung großer Datenmengen wesentlich weniger effizient sind. Um Produktionsdaten und Verwaltungsdatenverkehr zu trennen, darf sich der NSIP nicht auf demselben Subnetz/VLAN befinden wie Ihr Datenverkehr.

14. Wenn Sie eine Verwaltungsschnittstelle verwenden möchten, um den Verwaltungsdatenverkehr zu übertragen, empfiehlt es sich, dass sich die Standardroute in einem anderen Subnetz als dem Subnetz des NSIP (NSVLAN) befindet.

    In vielen Konfigurationen wird die Standardroute für die Arbeitsplatzkommunikation (in einem Internet-Szenario) verwendet. Wenn sich die Standardroute im selben Subnetz wie das NSIP befindet, kann die ADC-Appliance die Verwaltungsschnittstelle zum Senden und Empfangen von Datenverkehr verwenden. Diese Verwendung von Datenverkehr kann die Management-Schnittstelle überlasten.

15. Außerdem müssen ein SDX die SVM, XenServer und alle Citrix ADC Instanz-NSIPs im gleichen VLAN und Subnetz sein. Es gibt keine **Rückwandplatine** in der SDX-Appliance, die die Kommunikation zwischen SVM/Xen/Instanzen ermöglicht. Wenn sie sich nicht auf demselben VLAN/-Subnet/Interface befinden, muss der Datenverkehr zwischen ihnen die physische Hardware verlassen, im Netzwerk weitergeleitet werden und zurückkehren.

    Diese Konfiguration kann zu offensichtlichen Verbindungsproblemen zwischen den Instanzen und SVM führen und wird daher nicht empfohlen. Ein häufiges Symptom dafür ist ein Indikator

für den gelben Instanzstatus in der SVM für die betreffende VPX-Instanz und die Unfähigkeit, die SVM zur Neukonfiguration einer VPX-Instanz zu verwenden.

16. Wenn einige VLANs an Subnetze gebunden sind und andere nicht, werden GARP-Pakete während eines Hochverfügbarkeits-Failovers für IP-Adressen in keinem der Subnetze gesendet, die nicht an ein VLAN gebunden sind. Diese Konfiguration kann bei Hochverfügbarkeits-Failovers zu Verbindungsproblemen und Verbindungsproblemen führen. Dieses Problem wird dadurch verursacht, dass die Citrix ADC Appliance die Netzwerk-MAC-Besitzer-IP-Adressen auf Nicht-VMAC-konfigurierten Citrix ADC-Appliances nicht benachrichtigen kann.

    Die Symptome hierfür sind, dass der Leistungsindikator ip_tot_floating_ip_err nach einem Hochverfügbarkeits-Failover länger als einige Sekunden auf der früheren primären Citrix ADC Appliance inkrementiert wird, was darauf hinweist, dass das Netzwerk keine GARP-Pakete empfangen oder verarbeitet hat und das Netzwerk weiterhin Daten an die neue sekundäre Citrix ADC Appliance.

Konfigurieren von NSVLAN

September 1, 2022

NSVLAN ist ein VLAN, an das das Subnetz der Citrix ADC Management IP (NSIP)-Adresse gebunden ist. Das NSIP-Subnetz ist nur auf Schnittstellen verfügbar, die mit NSVLAN verknüpft sind. Standardmäßig ist NSVLAN VLAN 1, aber Sie können ein anderes VLAN als NSVLAN festlegen. In diesem Fall müssen Sie die Citrix ADC Appliance neu starten, damit die Änderung wirksam wird. Nach dem Neustart ist der NSIP-Subnetzverkehr auf das neue NSVLAN beschränkt.

Der Datenverkehr aus dem Citrix ADC IP-Subnetz kann mit der für NSVLAN angegebenen VLAN-ID (802.1q) gekennzeichnet werden. Sie müssen die angeschlossene Switch-Schnittstelle so konfigurieren, dass dieselbe VLAN-ID auf der verbundenen Schnittstelle markiert und zugelassen wird. Wenn Sie Ihre NSVLAN-Konfiguration entfernen, wird das NSIP-Subnetz automatisch an VLAN 1 gebunden, wodurch das Standard-NSVLAN wiederhergestellt wird.

So konfigurieren Sie NSVLAN mit der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- set ns config -nsvlan <positive_integer> -ifnum <interface_name> … [-tagged (YES|NO)]
- show ns config

  Hinweis: Die Konfiguration wird nach dem Neustart der Citrix ADC Appliance wirksam.

Beispiel:


```
> set ns config -nsvlan 300 -ifnum 1/1 1/2 1/3 -tagged YES
 Done

> save config
 Done
<!--NeedCopy-->
```

So stellen Sie die standardmäßige NSVLAN-Konfiguration über die CLI wieder her:

Geben Sie in der Befehlszeile Folgendes ein:

- nset ns config -nsvlan
- show ns config

Beispiel:

```
> unset ns config -nsvlan
 Done
<!--NeedCopy-->
```

So konfigurieren Sie NSVLAN mit der GUI:

Navigieren Sie zu System > Einstellungen, und klicken Sie in der Gruppe Einstellungen auf NSVLAN-Einstellungen ändern.

MTU auf dem NSVLAN einrichten

Standardmäßig ist die MTU des NSVLAN auf 1500 Byte eingestellt. Sie können diese Einstellung ändern, um den Durchsatz und die Netzwerkleistung zu optimieren. Beispielsweise können Sie das NSVLAN für die Verarbeitung von Jumbo-Frames konfigurieren.

So legen Sie die MTU des NSVLAN mit der CLI fest:

Geben Sie in der Befehlszeile Folgendes ein:

- **set vlan** <id> **-mtu** <positive_integer>
- **show vlan** <id>

So legen Sie die MTU des NSVLAN über die GUI fest:

Navigieren Sie zu **System** > **Netzwerk** > **VLANs**, öffnen Sie das NSVLAN und legen Sie den Parameter **Maximale Übertragungseinheit** fest.

Beispiel-Konfiguration:

In der folgenden Beispielkonfiguration ist VLAN 100 das NSVLAN.


```
> set ns config -nsvlan 100 -ifnum 1/1 -tagged no

  Warning: The configuration must be saved and the system rebooted for
      these settings to take effect

> set vlan 100 -mtu 1600

  Done

> sh vlan

  1)  VLAN ID: 1

      Link-local IPv6 addr:
    fe80::947b:52ff:fead:12d5/64

      Interfaces : 1/2 LO/1

  2)  VLAN ID: 100    VLAN Alias Name:

      MTU: 1600

      Interfaces : 1/1

      IPs :

          10.102.53.114     Mask: 255.255.255.0

  Done

> save config

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

Konfigurieren der zulässigen VLAN-Liste

October 5, 2021

Citrix ADC akzeptiert und sendet markierte Pakete eines VLAN auf einer Schnittstelle, wenn das VLAN explizit auf der Citrix ADC Appliance konfiguriert ist und die Schnittstelle an das VLAN gebunden ist.

Bei einigen Bereitstellungen (z. B. Bump in the wire) muss die Citrix ADC Appliance als transparentes Gerät fungieren, um markierte Pakete zu akzeptieren und weiterzuleiten, die mit einer großen Anzahl von VLANs zusammenhängen. Für diese Anforderung ist das Konfigurieren und Verwalten einer großen Anzahl von VLANs keine machbare Lösung.

Zulässige VLAN-Liste auf einer Schnittstelle gibt eine Liste von VLANs an. Die Schnittstelle akzeptiert und sendet markierte Pakete, die sich auf die angegebenen VLANs beziehen, transparent, ohne dass diese VLANs explizit auf der Appliance konfiguriert werden müssen.

Vor der Konfiguration der zulässigen VLAN-Liste zu berücksichtigende Punkte

Berücksichtigen Sie die folgenden Punkte, bevor Sie die zulässige VLAN-Liste konfigurieren

- In einem Hochverfügbarkeitssetup wird die zulässige VLAN-Liste nicht propagiert oder synchronisiert. Daher müssen Sie die zulässige VLAN-Liste auf beiden Knoten konfigurieren.
- Der Datenverkehr eines nativen VLAN kann zu den Nicht-Member-Schnittstellen führen, die das native VLAN in der zugelassenen VLAN-Liste angibt.
- Maximal 60 VLAN-Bereiche können als Teil der zulässigen VLAN-Liste für eine Schnittstelle angegeben werden.
- Die Citrix ADC Appliance unterstützt keine zulässigen VLAN-Liste auf Schnittstellen, die Teil von Linkaggregationskanälen oder redundanten Schnittstellensätzen sind. Weitere Informationen zum redundanten Schnittstellenset finden Sie unter Redundant Interface Set.
- Zulässige VLAN-Liste wird in einer Citrix ADC Clusterkonfiguration nicht unterstützt.
- Die Citrix ADC Appliance unterstützt keine zulässigen VLAN-Liste für Bridge-Gruppen.
- Die Citrix ADC Appliance unterstützt keine zulässigen VLAN-Liste für VXLANs.

Konfigurieren der zulässigen VLAN-Liste

So konfigurieren Sie die zulässige VLAN-Liste mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **set interface** <id> **-trunkmode** (ON|OFF) **-trunkAllowedVlan** <int[-int]> …
- **show interface** <id>

So konfigurieren Sie die zulässige VLAN-Liste mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **Schnittstellen**, wählen Sie eine Netzwerkschnittstelle aus, klicken Sie auf **Bearbeiten**, und legen Sie die folgenden Parameter fest:

- Trunk Mode
- Trunk Allowed VLAN

Beispielkonfiguration:

In der folgenden Beispielkonfiguration werden VLANS in den Bereichen 100-120, 190-200 und 300-330 als Teil der zulässigen VLAN-Liste für Schnittstelle 1/2 angegeben.

```
> set int 1/2 -trunkmode on -trunkallowedVlan 100-120 190-200 300-330

Done

> sh int 1/2

1)      Interface 1/2 (Gig Ethernet 10/100/1000 MBits) #6
        flags=0xc020

        <ENABLED, UP, UP, AUTONEG OFF, HEARTBEAT, 802.1q, trunkmode>

        Trunk Allowed Vlans:  100-120 190-200 300-330

Done

<!--NeedCopy-->
```

Bridge-Gruppen konfigurieren

October 5, 2021

Wenn Sie zwei oder mehr VLANs in einer einzelnen Domäne zusammenführen möchten, ändern Sie in der Regel die VLAN-Konfiguration auf allen Geräten in den separaten Domänen. Dies kann eine mühsame Aufgabe sein. Um mehrere VLANs einfacher in einer einzelnen Broadcastdomäne zusammenzuführen, können Sie Bridge-Gruppen verwenden.

Das Bridge-Gruppen-Feature funktioniert genauso wie ein VLAN. Mehrere VLANS können an eine einzelne Bridge-Gruppe gebunden werden, und alle VLANs, die an dieselbe Bridge-Gruppe gebunden sind, bilden eine einzelne Broadcast-Domäne. Sie können nur Layer 2-VLANs an eine Bridge-Gruppe binden. Für Layer-3-Funktionen müssen Sie einer Bridge-Gruppe eine IP-Adresse zuweisen.

Im Layer-2-Modus wird ein Broadcastpaket, das auf einer Schnittstelle zu einem bestimmten VLAN empfangen wird, zu anderen VLANs überbrückt, die zur gleichen Bridge-Gruppe gehören. Bei einem Unicastpaket durchsucht die Citrix ADC Appliance ihre Bridge-Tabelle nach den erlernten MAC-Adressen aller VLANs, die zu derselben Bridge-Gruppe gehören.

Im Layer 3-Weiterleitungsmodus ist ein IP-Subnetz an eine Bridge-Gruppe gebunden. Citrix ADC akzeptiert eingehende Pakete, die zum gebundenen Subnetz gehören, und leitet die Pakete nur auf

VLANs weiter, die an die Bridge-Gruppe gebunden sind.

IPv6-Routing kann für eine konfigurierte Bridge-Gruppe aktiviert werden.

> **Hinweis:**
>
> Die Bridge-Gruppen-Funktion und der Bridge-BPDU-Modus können nicht zusammen verwendet werden.

Konfigurationsschritte

Führen Sie die folgenden Schritte aus, um eine Bridge-Gruppe zu konfigurieren:

- Layer-2-Modus aktivieren
- Hinzufügen einer Bridgegroup und Binden von VLANs an die Bridgegroup

CLI-Verfahren

Um den Layer-2-Modus mit der CLI zu aktivieren: Geben
Sie an der Eingabeaufforderung Folgendes ein:

- **enable ns mode l2**
- **show ns mode**

So fügen Sie eine Bridge-Gruppe hinzu und binden VLANs mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add bridgegroup** <id> [-**ipv6DynamicRouting** (**ENABLED** | **DISABLED**)]
- **bind bridgegroup** <id> -**vlan** <positive_integer>
- **show bridgegroup** <id>

Beispiel:

```
> add bridgegroup 12
 Done
<!--NeedCopy-->
```

So entfernen Sie eine Bridge-Gruppe mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **rm bridgegroup** <id>

Beispiel:


```
1  rm bridgegroup 12
2 <!--NeedCopy-->
```

GUI-Prozeduren

So konfigurieren Sie eine Bridge-Gruppe mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **Bridge-Gruppen**, fügen Sie eine neue Bridge-Gruppe hinzu und binden Sie VLANs an die Bridgegroup, oder bearbeiten Sie eine vorhandene Bridge-Gruppe.

Konfigurieren von virtuellen MACs

October 5, 2021

Die primären und sekundären Knoten in einem Hochverfügbarkeitssetup (High Availability, HA) verwenden die schwebende Entität für virtuelle MAC-Adressen. Der primäre Knoten besitzt die schwebenden IP-Adressen (wie MIP, SNIP und VIP) und antwortet auf ARP-Anfragen für diese IP-Adressen mit einer eigenen MAC-Adresse. Daher wird die ARP-Tabelle eines externen Geräts, z. B. eines Upstream-Routers, mit der schwebenden IP-Adresse und der MAC-Adresse des primären Knotens aktualisiert.

Wenn ein Failover auftritt, übernimmt der sekundäre Knoten als neuer primärer Knoten. Der frühere sekundäre Knoten verwendet Gratuitous ARP (GARP), um die schwebenden IP-Adressen anzukündigen, die er vom alten Primärknoten gelernt hatte. Die MAC-Adresse, die der neue primäre Knoten angibt, ist die MAC-Adresse seiner eigenen Netzwerkschnittstelle. Einige Geräte (einige Router) akzeptieren diese GARP-Nachrichten nicht. Daher behalten diese externen Geräte die IP-Adressen-zu-MAC-Adressenzuordnung, die der alte primäre Knoten angekündigt hatte. Dies kann dazu führen, dass eine GSLB-Site heruntergeht.

Daher müssen Sie einen virtuellen MAC auf beiden Knoten eines HA-Paares konfigurieren. Dies bedeutet, dass beide Knoten identische MAC-Adressen haben. Wenn ein Failover auftritt, bleibt die MAC-Adresse des sekundären Knotens unverändert, und die ARP-Tabellen auf den externen Geräten müssen nicht aktualisiert werden.

Informationen zu den Verfahren zum Konfigurieren eines virtuellen MAC finden Sie unter Konfigurieren virtueller MAC-Adressen.

Konfigurieren der Link-Aggregation

October 5, 2021

Die Link-Aggregation kombiniert Daten aus mehreren Ports zu einer einzigen Hochgeschwindigkeits-Verbindung. Die Konfiguration der Linkaggregation erhöht die Kapazität und Verfügbarkeit des Kommunikationskanals zwischen der Citrix ADC Appliance und anderen angeschlossenen Geräten. Ein aggregierter Link wird auch als “Kanal. “ Sie können die Kanäle manuell konfigurieren oder LACP (Link Aggregation Control Protocol) verwenden. Sie können LACP weder auf einen manuell konfigurierten Kanal anwenden noch einen von LACP erstellten Kanal manuell konfigurieren.

Wenn eine Netzwerkschnittstelle an einen Kanal gebunden ist, haben die Kanalparameter Vorrang vor den Netzwerkschnittstellenparametern. (Das heißt, die Parameter der Netzwerkschnittstelle werden ignoriert.) Eine Netzwerkschnittstelle kann nur an einen Kanal gebunden werden.

Wenn eine Netzwerkschnittstelle an einen Kanal gebunden ist, wird die VLAN-Konfiguration abgesetzt. Wenn Netzwerkschnittstellen entweder manuell oder durch LACP an einen Kanal gebunden sind, werden sie aus den VLANs entfernt, zu denen sie ursprünglich gehörten, und dem Standard-VLAN hinzugefügt. Sie können den Kanal jedoch an das alte VLAN oder an ein neues binden. Wenn Sie beispielsweise die Netzwerkschnittstellen 1/2 und 1/3 an ein VLAN mit ID 2 binden und sie dann an einen Kanal LA/1 binden, werden die Netzwerkschnittstellen in das Standard-VLAN verschoben, Sie können sie jedoch wieder an VLAN 2 binden.

Manuelles Konfigurieren der Linkaggregation

Wenn Sie einen Linkaggregationskanal erstellen, ist der Status DOWN, bis Sie eine aktive Schnittstelle an ihn binden. Sie können einen Kanal jederzeit ändern. Sie können Kanäle entfernen, oder Sie können sie aktivieren/deaktivieren.

CLI-Verfahren

So erstellen Sie einen Link-Aggregationskanal mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add channel <id> [-ifnum <interfaceName> …] [-state (ENABLED | DISABLED)] [-speed <speed>] [-flowControl <flowControl>] [-haMonitor (ON | OFF)][-tagall (ON | OFF)] [-ifAlias <string>] [-throughput <positive_integer>] [-bandwidthHigh <positive_integer> [-bandwidthNormal <positive_integer>]]
- show channel

Beispiel:

```
1 > add channel LA/1 -ifnum 1/8
2 Done
3 <!--NeedCopy-->
```


So binden Sie eine Schnittstelle mit der Befehlszeilenschnittstelle an einen vorhandenen Verbindungsaggregationskanal oder lösen Sie die Bindung von einer Schnittstelle aus:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- bind channel <id> <interfaceName>
- unbind channel <id> <interfaceName>

Beispiel:

```
bind channel LA/1 1/8
<!--NeedCopy-->
```

So ändern Sie einen Link-Aggregationskanal mit der CLI:

Geben Sie an der Eingabeaufforderung den Befehl
set channel, die Kanal-ID und die zu ändernden Parameter mit ihren neuen Werten ein.

So entfernen Sie einen Link-Aggregationskanal mit der CLI:

Wichtig: Wenn ein Kanal entfernt wird, verursachen die Netzwerkschnittstellen, die an ihn gebunden sind, Netzwerkschleifen, die die Netzwerkleistung verringern. Sie müssen die Netzwerkschnittstellen deaktivieren, bevor Sie den Kanal entfernen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

- rm channel <id>

Beispiel:

```
> rm channel LA/1
 Done
<!--NeedCopy-->
```

GUI-Verfahren

So konfigurieren Sie einen Link-Aggregationskanal mit der GUI:

Navigieren Sie zu System > Netzwerk > Kanäle, fügen Sie einen neuen Kanal hinzu oder bearbeiten Sie einen vorhandenen Kanal.

So entfernen Sie einen Link-Aggregationskanal mit der GUI:

> **Wichtig:**
>
> Wenn ein Kanal entfernt wird, induzieren die Netzwerkschnittstellen, die an ihn gebunden sind, Netzwerkschleifen, die die Netzwerkleistung verringern. Sie müssen die Netzwerkschnittstellen deaktivieren, bevor Sie den Kanal entfernen.

Navigieren Sie zu System > Netzwerk > Kanäle, wählen Sie den Kanal aus, den Sie entfernen möchten, und klicken Sie auf Löschen.

Konfigurieren der Linkaggregation mithilfe des Link Aggregation Control-Protokolls

Das Link Aggregation Control Protocol (LACP) ermöglicht Netzwerkgeräten den Austausch von Verbindungsaggregationsinformationen durch den Austausch von LACP-Dateneinheiten (LACPDUs). Daher können Sie LACP nicht auf Netzwerkschnittstellen aktivieren, die Mitglieder eines Kanals sind, den Sie manuell erstellt haben.

Wenn Sie LACP zum Konfigurieren der Linkaggregation verwenden, verwenden Sie andere Befehle und Parameter zum Ändern von Linkaggregationskanälen als zum Erstellen von Linkaggregationskanälen. Um einen Kanal zu entfernen, müssen Sie LACP auf allen Schnittstellen deaktivieren, die Teil des Kanals sind.

Hinweis: In einer Hochverfügbarkeitskonfiguration werden LACP-Konfigurationen weder propagiert noch synchronisiert.

Konfigurieren der LACP-Systempriorität

Die LACP-Systempriorität bestimmt, welches Peer-Gerät eines LACP-LA-Kanals die Kontrolle über den LA-Kanal haben kann. Diese Nummer wird global auf alle LACP-Kanäle der Appliance angewendet. Je geringer der Wert, desto höher die Priorität.

So konfigurieren Sie die LACP-Systempriorität mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Priorität für eine eigenständige Appliance festzulegen und die Konfiguration zu überprüfen:

- set lacp -sysPriority <positive_integer>
- show lacp

Beispiel:

```
set lacp -sysPriority 50
<!--NeedCopy-->
```


Um die Priorität für einen bestimmten Clusterknoten festzulegen, melden Sie sich bei der Cluster-IP-Adresse an und geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- set lacp -sysPriority <positive_integer> -ownerNode <positive_integer>
- show lacp

Beispiel:

```
set lacp -sysPriority 50 -ownerNode 2
<!--NeedCopy-->
```

So konfigurieren Sie die LACP-Systempriorität mit der GUI:

1. Navigieren Sie zu System > Netzwerk > Schnittstellen, und wählen Sie in der Liste Aktion die Option LACP festlegen aus.
2. Geben Sie die Systempriorität und den Besitzerknoten an (gilt nur für ein Cluster-Setup).

Verknüpfungsaggregationskanäle erstellen

Um einen Link-Aggregationskanal mithilfe von LACP zu erstellen, müssen Sie LACP aktivieren und auf jeder Schnittstelle, die Teil des Kanals sein soll, denselben LACP-Schlüssel angeben. Wenn Sie beispielsweise LACP aktivieren und den LACP-Schlüssel auf 3 an den Schnittstellen 1/1 und 1/2 setzen, wird ein Link Aggregation Kanal LA/3 erstellt, und die Schnittstellen 1/1 und 1/2 werden automatisch daran gebunden.

Hinweis:

- Wenn Sie LACP auf einer Netzwerkschnittstelle aktivieren, müssen Sie den LACP-Schlüssel angeben.
- Standardmäßig ist LACP auf allen Netzwerkschnittstellen deaktiviert.

So erstellen Sie einen LACP-Kanal mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- set interface <id> [-lacpMode <lacpMode>] [-lacpKey<positive_integer>] [-lacpPriority <positive_integer>] [-lacpTimeout (LONG | SHORT)]
- show interface [<id>]

So erstellen Sie einen LACP-Kanal mit der GUI:

Navigieren Sie zu System > Netzwerk > Schnittstellen, öffnen Sie die Netzwerkschnittstelle und legen Sie die Parameter fest.

Verknüpfungsaggregationskanäle ändern

Nachdem Sie einen LACP-Kanal durch Angabe von Schnittstellen erstellt haben, können Sie die Eigenschaften des Kanals ändern.

So ändern Sie einen LACP-Kanal mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- set channel <id> [-ifnum <interfaceName> …] [-state (ENABLED | DISABLED)] [-speed <speed>] [-flowControl <flowControl>] [-haMonitor (ON | OFF)] [-ifAlias <string>] [-throughput <positive_integer>] [-tagall (ON | OFF)] [-bandwidthHigh <positive_integer> [-bandwidthNormal <positive_integer>]]
- show channel

Beispiel:

```
> set channel LA/3 -state ENABLED -speed 10000
 Done
<!--NeedCopy-->
```

So ändern Sie einen LACP-Kanal mit der GUI:

Navigieren Sie zu System > Netzwerk > Kanäle, und ändern Sie einen vorhandenen LACP-Kanal.

Entfernen eines Verknüpfungsaggregationskanals

Um einen Link Aggregation Kanal zu entfernen, der mit LACP erstellt wurde, müssen Sie LACP auf allen Schnittstellen deaktivieren, die Teil des Kanals sind.

So entfernen Sie einen LACP-Kanal mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- set interface <id> -lacpMode Disable
- show interface [<id>]

So entfernen Sie einen LACP-Kanal mit der GUI:

Navigieren Sie zu System > Netzwerk > Schnittstellen, öffnen Sie die Netzwerkschnittstelle und deaktivieren Sie die Option LACP aktivieren.

Link-Redundanz über LACP-Kanäle

Link-Redundanz mithilfe von LACP-Kanälen ermöglicht es dem Citrix ADC, einen LACP-Kanal in logische Subkanäle zu unterteilen, wobei ein Subkanal aktiv und der andere im Standby-Modus aktiv ist.

Wenn der aktive Subkanal einen minimalen Durchsatzschwellenwert nicht erreicht, wird einer der Standby-Unterkanäle aktiv und übernimmt die Übernahme.

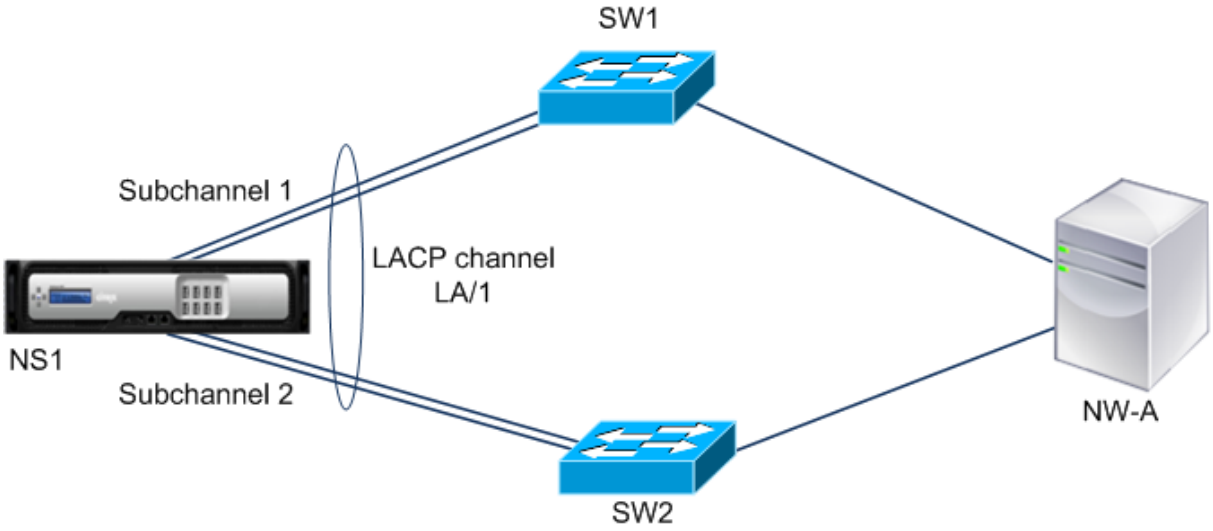
Ein Subchannel wird aus Links erstellt, die Teil des LACP-Kanals sind und mit einem bestimmten Gerät verbunden sind. Beispielsweise erstellt der ADC für einen LACP-Kanal mit vier Schnittstellen auf einem Citrix ADC, zwei der Schnittstellen, die mit Gerät A und die anderen beiden mit Gerät B verbunden sind, zwei logische Subkanäle, einen Subkanal mit zwei Links zu Gerät A und einen anderen Subkanal mit zwei Links zu Gerät B.

Um die Link-Redundanz für einen LACP-Kanal zu konfigurieren, legen Sie den Parameter LRMinThroughput fest, der den minimalen Durchsatzschwellenwert (in Mbit/s) angibt, der vom aktiven Subkanal erreicht werden soll. Wenn Sie diesen Parameter festlegen, werden die Unterkanäle automatisch erstellt. Wenn der maximal unterstützte Durchsatz des aktiven Kanals unter den Wert LRMinThroughput fällt, tritt ein Link-Failover auf und ein Standby-Unterkanal wird aktiv.

Wenn Sie den LRMinThroughput-Parameter eines LACP-Kanals deaktivieren oder den Wert auf Null setzen, ist die Verbindungsredundanz für diesen Kanal deaktiviert. Dies ist die Standardeinstellung.

Beispiel

Betrachten Sie ein Beispiel für Verbindungsredundanz, die zwischen Citrix ADC NS1 und Switches SW1 und SW2 konfiguriert wurde.



NS1 ist über SW1 und SW2 mit dem Netzwerkgerät NW-A verbunden.
Auf NS1 wird der LACP-Kanal LA/1 aus den Schnittstellen 1/1, 1/2, 1/3 und 1/4 erstellt. Die Schnittstellen 1/1 und 1/2 von NS1 sind mit SW1 verbunden, die Schnittstellen 1/3 und 1/4 sind an SW2 angeschlossen. Jeder der vier Links unterstützt einen maximalen Durchsatz von 1000Mbps.
Wenn der Parameter LRMinThroughput auf einen Wert gesetzt ist (z. B. 2000), erstellt NS1 zwei logische Subkanäle aus LA/1, einen Subkanal (zB Subkanal 1) mit den Schnittstellen 1/1 und 1/2 (verbunden

mit SW1) und den anderen Subkanal (Subkanal 2) unter Verwendung der Schnittstellen 1/3 und 1/4 (mit SW2 verbunden).

NS1 wendet einen Algorithmus an, um einen Subchannel (z. B. Subchannel 1) aktiv zu machen und den anderen in den Standby-Modus zu versetzen. NS1 und Netzwerkgerät NW-A sind nur über den aktiven Subkanal zueinander zugänglich.

Angenommen, Subchannel 1 ist aktiv und der maximal unterstützte Durchsatz unterschreitet den LRMinThroughput-Wert (z. B. eine seiner Verbindungen schlägt fehl, und der maximal unterstützte Durchsatz fällt auf 1000 Mbit/s). Subchannel 2 wird aktiv und übernimmt die Kontrolle.

Link-Redundanz mithilfe von LACP-Kanälen in einem Hochverfügbarkeit-Setup

Wenn Sie in einer High Availability (HA) -Konfiguration den Durchsatz (Durchsatzparameter) -basierten HA-Failover und Link-Redundanz (LRMinThroughput-Parameter) auf einem LACP-Kanal konfigurieren möchten, müssen Sie den Durchsatzparameter auf einen Wert festlegen, der kleiner oder gleich dem des Parameters LRMinThroughput ist.

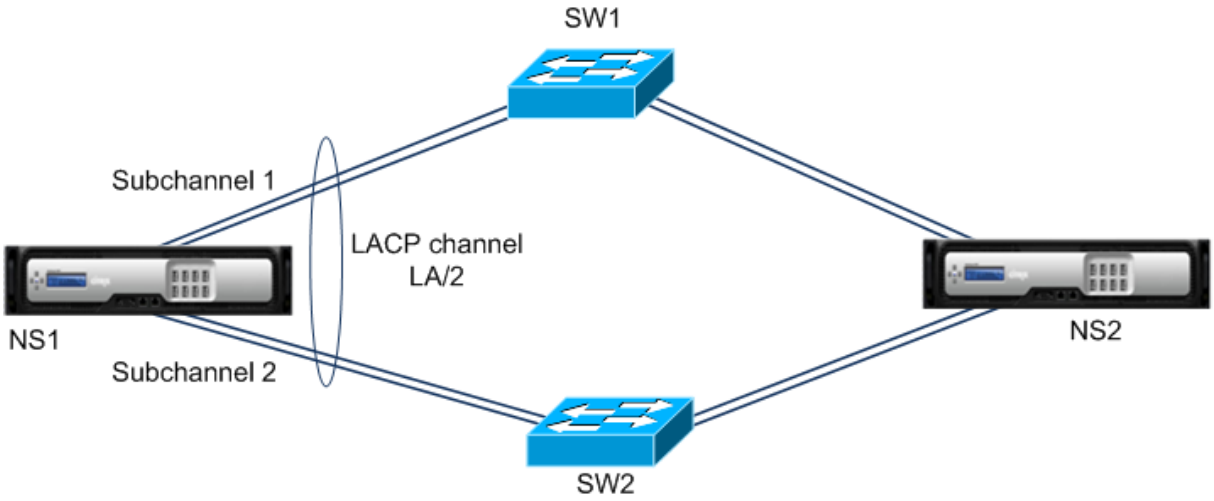
Der maximal unterstützte Durchsatz eines LACP-Kanals wird als der maximal unterstützte Durchsatz des aktiven Subkanals berechnet.

Wenn der Durchsatzparameterwert gleich oder kleiner als der lrminthroughput-Parameterwert ist, tritt ein HA-Failover auf, wenn beide der folgenden Bedingungen gleichzeitig vorhanden sind:

- Keiner der maximal unterstützten Durchsätze der Subkanäle entspricht dem LRMinThroughput-Parameterwert.
- Der maximal unterstützte Durchsatz des LACP-Kanals entspricht nicht dem Durchsatzparameterwert

Betrachten Sie ein Beispiel für ein HA-Setup mit Citrix ADCs NS1 und NS2 mit Switches SW1 und SW2. NS1 ist über SW1 und SW2 mit NS2 verbunden.

Auf NS1 wird der LACP-Kanal LA/1 aus den Schnittstellen 1/1, 1/2, 1/3 und 1/4 erstellt. Die Schnittstellen 1/1 und 1/2 von NS1 sind mit SW1 verbunden, die Schnittstellen 1/3 und 1/4 sind an SW2 angeschlossen. Jeder der vier Links unterstützt einen maximalen Durchsatz von 1000Mbps.



Im Folgenden sind die LACP-Parametereinstellungen in diesem Beispiel:

Parameter	Wert
Durchsatz	2000
lrminthroughput	2000

NS1 bildet zwei Subkanäle aus LA/1, einen Subkanal (z. B. Subkanal 1) über Schnittstellen 1/1 und 1/2 (verbunden mit SW1) und den anderen Subkanal (Subkanal 2) über Schnittstellen 1/3 und 1/4 (verbunden mit SW2). Jeder der beiden Subkanäle unterstützt einen maximalen Durchsatz von 2000 Mbit/s. Durch Anwenden eines Algorithmus macht NS1 einen Subchannel (z. B. Subchannel 1) und den anderen Standby aktiv.

Angenommen, Subchannel 1 ist aktiv und der maximal unterstützte Durchsatz unterschreitet den LRMinThroughput-Wert (z. B. eine seiner Verbindungen schlägt fehl, und der maximal unterstützte Durchsatz fällt auf 1000 Mbit/s). Subchannel 2 wird aktiv und übernimmt die Kontrolle. HA-Failover tritt nicht auf, da der maximal unterstützte Durchsatz des LACP-Kanals nicht kleiner als der Durchsatzparameterwert ist:

Maximaler unterstützter Durchsatz des LACP-Kanals = Maximaler unterstützter Durchsatz des aktiven Kanals = Maximaler unterstützter Durchsatz von Subchannel 2 = 2000 Mbit/s

Wenn der maximal unterstützte Durchsatz von Subchannel 2 auch unter den lrminthroughput-Wert fällt (z. B. eine seiner Verbindungen schlägt fehl und der maximal unterstützte Durchsatz auf 1000 Mbit/s fällt), tritt ein HA-Failover auf, da der maximal unterstützte Durchsatz des LACP-Kanals dann kleiner als der Durchsatzparameter ist Wert:

Konfigurieren der Link-Redundanz mithilfe von LACP-Kanälen

So konfigurieren Sie die Link-Redundanz für einen LACP-Kanal mit der CLI:

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

- **set channel** <id> -lrMinThroughput <positive_integer>
- **show channel**

Beispiel:

```
> set channel la/1 - lrMinThroughput 2000
Done
> set channel la/2 - throughput 2000 - lrMinThroughput 2000
Done
<!--NeedCopy-->
```

So konfigurieren Sie die Link-Redundanz für einen LACP-Kanal mit der GUI

1. Navigieren Sie zu System > Netzwerk > Kanäle.
2. Wählen Sie im Detailbereich einen LACP-Kanal aus, für den Sie die Link-Redundanz konfigurieren möchten, und klicken Sie dann auf Bearbeiten.
3. Legen Sie im Dialogfeld LACP-Kanal konfigurieren den Parameter LRMinThroughput fest.
4. Klicken Sie auf Schließen.

Redundante Schnittstellensatz

October 5, 2021

Ein redundanter Schnittstellensatz ist ein Satz von Schnittstellen, bei denen eine der Schnittstellen aktiv ist und die übrigen im Standby-Modus sind. Wenn die aktive Schnittstelle ausfällt, übernimmt eine der Standby-Schnittstellen und wird aktiv.

Die folgenden Hauptvorteile der Verwendung redundanter Schnittstellensätze sind:

- Ein redundantes Schnittstellensatz gewährleistet die Verbindungszuverlässigkeit zwischen der Citrix ADC Appliance und einem Peer-Gerät, indem Backup-Verbindungen zwischen ihnen bereitgestellt werden.
- Im Gegensatz zu Link-Redundanz mit LACP ist für einen redundanten Schnittstellensatz keine Konfiguration auf dem Peer-Gerät erforderlich. Für das Peer-Gerät erscheinen redundante Schnittstellensatz als einzelne Schnittstellen und nicht als Satz oder Sammlung.

- In einer Hochverfügbarkeitskonfiguration (HA) können redundante Schnittstellensätze die Anzahl der HA-Failovers minimieren.

> **Hinweis:**
>
> Redundant Interface Set wurde früher als NIC Bundling bezeichnet, als das erste Mal in Version 10.5 eingeführt wurde.

Funktionsweise redundanter Schnittstellensatz

Bei einem redundanten Schnittstellensatz leitet die Citrix ADC Appliance eine MAC-Adresse auf der Grundlage eines internen Algorithmus ab und weist sie dem redundanten Schnittstellensatz zu. Diese MAC-Adresse wird von allen Mitgliederschnittstellen gemeinsam genutzt und wird jeweils nur von der aktiven Schnittstelle verwendet. Die aktive Schnittstelle sendet GARP-Nachrichten, die die dem redundanten Schnittstellensatz zugewiesene MAC-Adresse und nicht die eigene physische MAC-Adresse der Schnittstelle enthalten. Wenn die aktuelle aktive Schnittstelle ausfällt und von einer anderen Schnittstelle übernommen wird, sendet die neue aktive Schnittstelle GARP-Nachrichten. Das Peer-Gerät aktualisiert seine Weiterleitungstabelle mit den neuen aktiven Schnittstelleninformationen. Die Standby-Schnittstellen senden keine GARP-Nachrichten. Die Standby-Schnittstellen senden keine Pakete und sie löschen alle empfangenen Pakete.

In einem redundanten Schnittstellensatz basiert die Auswahl der Memberschnittstelle als aktiv auf einem der folgenden Faktoren:

- **Redundante Schnittstellenpriorität**. Dies ist ein Parameter einer Schnittstelle und definiert die Priorität der Schnittstelle in einem redundanten Schnittstellensatz für die aktive Elementauswahl. Dieser Parameter gibt eine positive Ganzzahl an. Verringern Sie den Wert höher als die Priorität der aktiven Elementauswahl. Die Memberschnittstelle mit der höchsten Priorität (niedrigster Wert) wird als aktive Schnittstelle des redundanten Schnittstellensatzes ausgewählt.
- **Bindungsreihenfolge der Memberschnittstellen**. Wenn alle Mitgliedsschnittstellen dieselbe redundante Schnittstellenpriorität haben, wird die Memberschnittstelle, die zuerst an den redundanten Schnittstellensatz gebunden war, als aktive Schnittstelle des redundanten Schnittstellensatzes ausgewählt.

In einem redundanten Schnittstellensatz wird die aktive Schnittstellenauswahl in einem der folgenden Ereignisse ausgelöst:

- Wenn die aktuelle aktive Schnittstelle fehlschlägt oder Sie sie deaktivieren.
- Wenn Sie die Priorität einer Standby-Schnittstelle auf einen Wert festlegen, der niedriger ist als die der aktuellen aktiven Schnittstelle. Die Standby-Schnittstelle übernimmt als aktive Schnittstelle.
- Wenn Sie eine Schnittstelle binden, deren Priorität niedriger ist als die der aktuellen aktiven Schnittstelle. Die neu gebundene Schnittstelle übernimmt als aktive Schnittstelle.

Punkte, die bei der Konfiguration redundanter Schnittstellensätze berücksichtigt werden müssen

Berücksichtigen Sie die folgenden Punkte, bevor Sie einen redundanten Schnittstellensatz konfigurieren:

- In einer Standalone-Appliance oder einer Appliance in einem Hochverfügbarkeitssetup wird ein Verbindungsredundanzsatz in der LR/X-Notation angegeben, wobei X zwischen 1 und 4 liegen kann. Zum Beispiel LR/1.
- In einer Hochverfügbarkeitskonfiguration werden redundante Schnittstellenset-Konfigurationen nicht mit dem sekundären Knoten propagiert oder synchronisiert.
- Sie können maximal vier redundante Schnittstellensätze auf einer Citrix ADC Appliance konfigurieren.
- Sie können maximal 16 Schnittstellen an einen redundanten Schnittstellensatz binden.
- Mitgliedsschnittstellen eines redundanten Schnittstellensatzes können nicht an einen anderen redundanten Schnittstellensatz gebunden werden.
- Mitgliedsschnittstellen eines redundanten Schnittstellensatzes können nicht an einen Link-Aggregatkanal (LA) gebunden werden.
- LA-Kanäle können nicht an einen redundanten Schnittstellensatz gebunden werden.
- Redundante Schnittstellensätze können nicht an einen LA-Kanal gebunden werden.
- In einem Cluster-Setup:
  - Redundante Schnittstellensätze können nicht an eine Cluster-Link-Aggregation gebunden werden.
  - Ein redundanter Verbindungssatz wird in N/LR/X Notation angegeben (z. B. 1/LR/3). Dabei:
    N ist die ID des Clusterknotens, auf dem der redundante Schnittstellensatz erstellt werden soll.
    X ist ein link-redundanter Satz Bezeichner auf einem Clusterknoten. X kann von 1-4 reichen.
  - Eine Clusterverknüpfungsaggregation kann nicht an einen redundanten Schnittstellensatz gebunden werden.
  - Ein redundanter Schnittstellensatz kann nur die Schnittstellen des Knotens umfassen, zu dem der redundante Schnittstellensatz gehört.
  - Eine vorhandene elink-Redundanzsatzkonfiguration auf einer eigenständigen Appliance ändert sich automatisch in Cluster-Notation (N/LR/X), nachdem die Appliance zu einem Cluster-Setup hinzugefügt wurde.

Konfigurationsschritte

Die Konfiguration redundanter Schnittstellensets auf einer Citrix ADC Appliance umfasst die folgenden Aufgaben:

- **Erstellen Sie einen redundanten Schnittstellensatz**. Verwenden Sie den Kanalbefehl, um

einen redundanten Schnittstellensatz zu erstellen.

In einer Standalone-Appliance oder einer Appliance in einem Hochverfügbarkeitssetup wird ein Verbindungsredundanzsatz in der LR/X-Notation angegeben, wobei X zwischen 1 und 4 liegen kann. Zum Beispiel LR/1.

In einem Cluster-Setup wird in N/LR/X (z. B. 1/LR/3) ein Verbindungsredundanzsatz angegeben, wobei: N die ID des Clusterknotens ist, auf dem der redundante Schnittstellensatz erstellt werden soll, X ist der Link Redundant Set Identifier auf einem Clusterknoten. X kann von 1-4 reichen.

- **Binden Sie Schnittstellen an den redundanten Schnittstellensatz**. Ordnen Sie die gewünschten Schnittstellen dem redundanten Schnittstellensatz zu. Eine Schnittstelle kann nicht Teil mehrerer redundanter Schnittstellensätze sein.
- **(Optional) Legen Sie eine redundante Schnittstellenpriorität für die Memberschnittstelle**fest. Verwenden Sie den Schnittstellenbefehl, um die redundante Schnittstellenpriorität für eine gewünschte Memberschnittstelle eines redundanten Schnittstellensatzes festzulegen.

So erstellen Sie mit der CLI eine redundante Schnittstelle:

An der Eingabeaufforderung:

- add channel <ID>
- show channel <ID>

So binden Sie Schnittstellen an eine redundante Schnittstelle, die mit der CLI festgelegt wird:

An der Eingabeaufforderung:

- bind channel <ID> <ifnum>
- show channel <ID>

So legen Sie mit der CLI eine redundante Schnittstellenpriorität einer Schnittstelle fest:

An der Eingabeaufforderung:

- set interface <ID> -lrsetpriority <positive_integer>
- <ID>Schnittstelle anzeigen

Beispielkonfiguration 1:

Im folgenden Beispiel wird der redundante Schnittstellensatz LR/1 erstellt, und die Schnittstellen 1/1, 1/2, 1/3 und 1/4 sind an LR/1 gebunden. Die redundante Schnittstellenpriorität wird für alle diese Mitgliedsschnittstellen auf den Standardwert 1024 festgelegt. Die Ausgabe des Befehls show channel zeigt an, dass die Schnittstelle 1/1 die aktuelle aktive Schnittstelle für den redundanten Schnittstellensatz lr/1 ist.

```
1 > add channel lr/1
```



```
 Done
> bind channel lr/1 1/1 1/2 1/3 1/4
 Done
> show channel
1)    Interface LR/1 (Link Redundant) #23
        flags=0x100c020 <ENABLED, UP, LINKREDUNDANT, UP, HAMON, 802.1q>
        MTU=1500, native vlan=1, MAC=36:97:a2:b7:6b:a9, uptime 0h00m00s
        Requested: media NONE, speed AUTO, duplex NONE, fctl OFF,
                 throughput 0
        Actual: throughput 1000
        LLDP Mode: NONE,
        RX: Pkts(1) Bytes(52) Errs(0) Drops(1) Stalls(0)
        TX: Pkts(2) Bytes(84) Errs(0) Drops(4) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
        Bandwidth thresholds are not set.
                1/1: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Active Member
                1/2: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
                1/3: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
                1/4: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                   Inactive Member
Done
<!--NeedCopy-->
```

Beispielkonfiguration 2:

Im folgenden Beispiel ist die redundante Schnittstellenpriorität der Memberschnittstelle 1/4 auf 100 festgelegt, was niedriger ist als die festgelegte redundante Schnittstellenpriorität aller anderen Memberschnittstellen von LR/1.

Die Ausgabe des Befehls show channel zeigt an, dass die Schnittstelle 1/4 die aktuelle aktive Schnittstelle für den redundanten Schnittstellensatz LR/1 ist.

```
> set interface 1/4 -lrsetPriority 100
Done
> show channel
1)      Interface LR/1 (Link Redundant) #23
        flags=0x100c020 <ENABLED, UP, LINKREDUNDANT, UP, HAMON, 802.1q>
        MTU=1500, native vlan=1, MAC=36:97:a2:b7:6b:a9, uptime 0h00m00s
        Requested: media NONE, speed AUTO, duplex NONE, fctl OFF,
                 throughput 0
        Actual: throughput 1000
```



```
10          LLDP Mode: NONE,
11          RX: Pkts(1) Bytes(52) Errs(0) Drops(1) Stalls(0)
12          TX: Pkts(2) Bytes(84) Errs(0) Drops(4) Stalls(0)
13          NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
14          Bandwidth thresholds are not set.
15                  1/1: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                        Inactive Member
16                  1/2: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                        Inactive Member
17                  1/3: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                        Inactive Member
18                  1/4: UTP-1000-FULL-OFF          UP  0h14m06s    LR
                        Active Member
19  Done
20  <!--NeedCopy-->
```

Beispielkonfiguration 3:

Betrachten Sie ein Cluster-Setup von vier Knoten N1, N2, N3 und N4. In diesem Beispiel wird der redundante Schnittstellensatz 1/LR/3 auf Knoten N1 erstellt, und die Schnittstellen 1/1/1, 1/1/2 und 1/1/3 sind an ihn gebunden. Die redundante Schnittstellenpriorität wird für alle diese Mitgliedsschnittstellen auf den Standardwert 1024 festgelegt. Die Ausgabe des Befehls show channel zeigt an, dass Schnittstelle 1/1/1 die aktuelle aktive Schnittstelle für redundante Schnittstellensatz 1/LR/3 ist.

```
1       > add channel 1/LR/3
2
3       Done
4       > bind channel 1/LR/3 1/1/1 1/1/2 1/1/3
5
6       Done
7       > show channel
8       1)    Interface 1/LR/3 (Link Redundant) #14
9               flags=0x100c020 <ENABLED, UP, LINKREDUNDANT, UP, HAMON,
                   802.1q>
10              MTU=1500, native vlan=1, MAC=36:97:a2:b7:6b:a9, uptime 0
                   h00m00s
11              Requested: media NONE, speed AUTO, duplex NONE, fctl OFF,
12              throughput 0
13              Actual: throughput 1000
14              LLDP Mode: NONE,
15              RX: Pkts(66) Bytes(4406) Errs(0) Drops(82) Stalls(0)
16              TX: Pkts(55) Bytes(2626) Errs(0) Drops(145) Stalls(0)
17              NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted
```



```
                (0)
            Bandwidth thresholds are not set.

            1/1/1: UTP-1000-FULL-OFF UP  0h14m06s LR Active Member
            1/1/2: UTP-1000-FULL-OFF UP  0h14m06s LR Inactive Member
            1/1/3: UTP-1000-FULL-OFF UP  0h14m06s LR Inactive Member

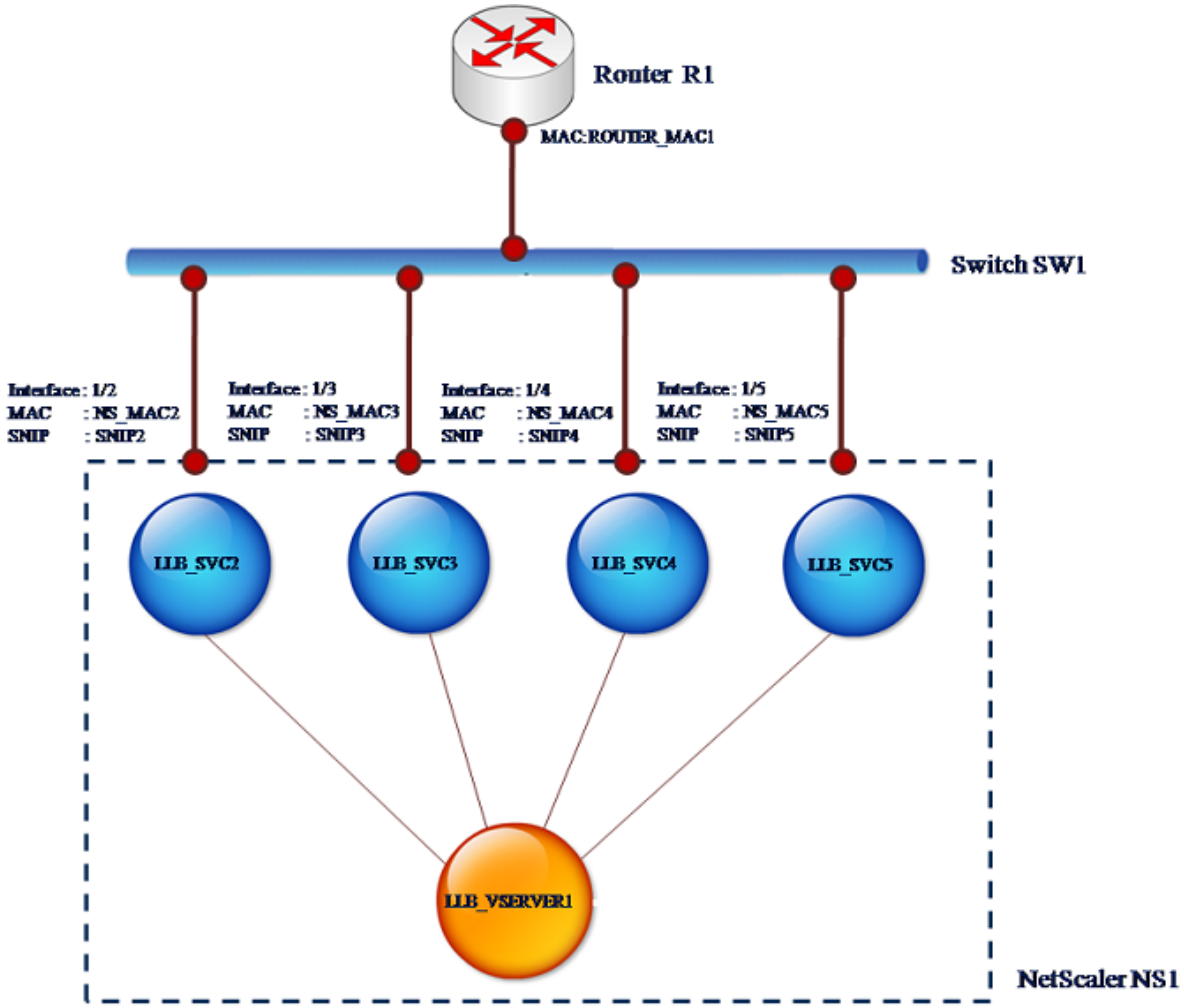
    Done
<!--NeedCopy-->
```

Binden einer SNIP-Adresse an eine Schnittstelle

October 5, 2021

Sie können jetzt eine Citrix ADC eigene SNIP-Adresse an eine Schnittstelle binden, ohne Layer 3-VLANs zu verwenden. Alle Pakete, die sich auf die SNIP-Adresse beziehen, gehen nur über die gebundene Schnittstelle.

Diese Funktion kann in einem Szenario nützlich sein, in dem der Upstream-Switch keine Link-Aggregation-Kanäle unterstützt und Sie möchten, dass die Citrix ADC Appliance Datenverkehr, der von einem Server stammt, über die vier Links zum Upstream-Switch verteilt, wie in der folgenden Abbildung dargestellt.



In den folgenden Tabellen werden die Beispieleinstellungen für das Szenario beschrieben:

Entität	Name	Wert
SNIP-Adressen auf NS1	SNIP2 (nur zu Referenzzwecken)	10.10.10.2
	SNIP3 (nur zu Referenzzwecken)	10.10.10.3
	SNIP4 (nur zu Referenzzwecken)	10.10.10.4
	SNIP5 (nur zu Referenzzwecken)	10.10.10.5
Virtueller LLB-Server auf NS1	LLB_VSERVER1	-

Entität	Name	Wert
Transparenter Monitor auf NS1	TRANS_MON	-
LLB-Dienste auf NS1	LLB_SVC2	10.10.10.240
	LLB_SVC3	10.10.10.120
	LLB_SVC4	10.10.10.60
	LLB_SVC5	10.10.10.30
MAC-Adresse der Schnittstelle 1/2 auf NS1	NS_MAC_2 (nur zu Referenzzwecken)	00:e0:ed:0f:bc:e0
MAC-Adresse der Schnittstelle 1/3 auf NS1	NS_MAC_3 (nur zu Referenzzwecken)	00:e0:ed:0f:bc:df
MAC-Adresse der Schnittstelle 1/4 auf NS1	NS_MAC_4 (nur zu Referenzzwecken)	00:e0:ed:0f:bc:de
MAC-Adresse der Schnittstelle 1/5 auf NS1	NS_MAC_5 (nur zu Referenzzwecken)	00:e0:ed:1c:89:53
IP-Adresse des Routers R1	Router_IP (nur zu Referenzzwecken)	10.10.10.1
MAC-Adresse der Schnittstelle von R1	ROUTER_MAC1 (nur zu Referenzzwecken)	00:21:a1:2d:db:cc

So konfigurieren Sie die Beispieleinstellungen:

1. Fügen Sie vier verschiedene SNIPs in verschiedenen Subnetzbereichen hinzu. Dies ist für ARP auf vier verschiedenen Links gelöst werden. Weitere Informationen zum Erstellen einer SNIP-Adresse finden Sie unter Konfigurieren von Subnetz-IP-Adressen (SNIPs).

   CLI-Beispiel:

```
1 > add ns ip 10.10.10.2 255.255.255.0 -type SNIP
2  Done
3 > add ns ip 10.10.10.3 255.255.255.128  - type SNIP
4 Done
5 > add ns ip 10.10.10.4 255.255.255.192  - type SNIP
6 Done
7 > add ns ip 10.10.10.5 255.255.255.224  - type SNIP
8 Done
9 <!--NeedCopy-->
```


2. Fügen Sie vier verschiedene Dummy-Dienste in den hinzugefügten SNIP-Subnetzen hinzu. Damit soll sichergestellt werden, dass der Datenverkehr mit Quell-IP als einer der vier konfigurierten SNIPs gesendet wird. Weitere Informationen zum Erstellen eines Dienstes finden Sie unter Einrichten des grundlegenden Lastenausgleichs.

   CLI-Beispiel:

```
> add service LLB_SVC2 10.10.10.240 any *
 Done
> add service LLB_SVC3 10.10.10.120 any *
 Done
> add service LLB_SVC4 10.10.10.60 any *
 Done
> add service LLB_SVC5 10.10.10.30 any *
 Done
<!--NeedCopy-->
```

3. Fügen Sie einen transparenten Ping-Monitor zur Überwachung des Gateway hinzu. Binden Sie den Monitor an jeden der konfigurierten Dummy-Dienste. Dies ist, um den Zustand der Dienste als UP zu machen. Weitere Informationen zum Erstellen eines transparenten Monitors finden Sie unter Konfigurieren von Monitoren in einem Load Balancing-Setup.

   CLI-Beispiel:

```
> add monitor TRANS_MON ping -destIP 10.10.10.1 -transparent YES
 Done
> bind monitor TRANS_MON LLB_SVC2
 Done
> bind monitor TRANS_MON LLB_SVC3
 Done
> bind monitor TRANS_MON LLB_SVC4
 Done
> bind monitor TRANS_MON LLB_SVC5
 Done
<!--NeedCopy-->
```

4. Fügen Sie einen Link Load Balancing (LLB) virtuellen Server hinzu und binden Sie die Dummy-Dienste an ihn. Weitere Informationen zum Erstellen eines virtuellen LLB-Servers finden Sie unter Konfigurieren eines grundlegenden LLB-Setups.

   CLI-Beispiel:


```
> add lb vserver LLB_VSERVER1 any
 Done
> set lb vserver LLB_VSERVER1 -lbmethod ROUNDROBIN
 Done
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
> bind lb vserver LLB_VSERVER1 LLB_SVC2
 Done
<!--NeedCopy-->
```

5. Fügen Sie den virtuellen LLB-Server als Standard-LLB-Route hinzu. Weitere Informationen zum Erstellen einer LLB-Route finden Sie unter Konfigurieren eines grundlegenden LLB-Setups.

   CLI-Beispiel:

```
> add lb route 0.0.0.0 0.0.0.0  LLB_VSERVER1
 Done
<!--NeedCopy-->
```

6. Fügen Sie für jeden Dummy-Dienst einen ARP-Eintrag mit der MAC-Adresse des Gateway hinzu. Auf diese Weise ist das Gateway über diese Dummy-Dienste erreichbar. Weitere Informationen zum Hinzufügen eines ARP-Eintrags finden Sie unter Konfigurieren von statischem ARP.

   CLI-Beispiel:

```
> add arp -ipaddress 10.10.10.240 -mac 00:21:a1:2d:db:cc -ifnum
   1/2
 Done
> add arp -ipaddress 10.10.10.120 -mac 00:21:a1:2d:db:cc -ifnum
   1/3
 Done
> add arp -ipaddress 10.10.10.60 -mac 00:21:a1:2d:db:cc -ifnum 1/4
 Done
> add arp -ipaddress 10.10.10.30 -mac 00:21:a1:2d:db:cc -ifnum 1/5
 Done
<!--NeedCopy-->
```


7. Binden Sie eine bestimmte Schnittstelle an ein SNIP, indem Sie für jede dieser SNIPs einen ARP-Eintrag hinzufügen. Dadurch soll sichergestellt werden, dass der Antwortdatenverkehr dieselbe Schnittstelle erreicht, über die die Anforderung ausgegangen ist. Weitere Informationen zum Hinzufügen eines ARP-Eintrags finden Sie unter Konfigurieren von statischem ARP.

   CLI-Beispiel:

```
> add arp -ipAddress 10.10.10.2 -mac 00:e0:ed:0f:bc:e0 -ifnum 1/2
 Done
> add arp -ipAddress 10.10.10.3 -mac 00:e0:ed:0f:bc:df -ifnum 1/3
 Done
> add arp -ipAddress 10.10.10.4 -mac 00:e0:ed:0f:bc:de -ifnum 1/4
 Done
> add arp -ipAddress 10.10.10.5 -mac 00:e0:ed:1c:89:53 -ifnum 1/5
 Done
<!--NeedCopy-->
```

Überwachen der Bridge-Tabelle und Ändern der Alterungszeit

December 7, 2021

Die Citrix ADC Appliance brückt Frames auf Basis der Bridge-Tabellensuche der Ziel-MAC-Adresse und der VLAN-ID. Die Appliance führt die Weiterleitung jedoch nur durch, wenn der Layer-2-Modus aktiviert ist.

Die Bridge-Tabelle wird dynamisch generiert, Sie können sie jedoch anzeigen, die Alterungszeit für die Bridge-Tabelle ändern und Bridging-Statistiken anzeigen. Alle MAC-Einträge in der Bridge-Tabelle werden mit der Alterungszeit aktualisiert.

So legen Sie die Alterungszeit von Bridge-Tabelleneinträgen mit der CLI fest:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **set l2param** -**bridgeagetimeout** <positive_integer>
- **show l2param**

Beispiel:

```
> set l2param -bridgeagetimeout 90
 Done
<!--NeedCopy-->
```


So zeigen Sie die Statistiken einer Bridge-Tabelle mit der CLI an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **stat bridge**

So legen Sie die Alterungszeit von Bridge-Tabelleneinträgen mit der GUI fest:

Navigieren Sie zu **System** > **Netzwerk**. Klicken Sie auf der Seite **Netzwerk** im Abschnitt **Einstellungen** auf **Layer2-Parameter konfigurieren, und legen Sie den Parameter Timeoutwert für die Bridge-Tabelleneinträge (Sekunden)** fest.

So zeigen Sie die Statistiken einer Bridge-Tabelle mit der GUI an:

Navigieren Sie zu **System** > **Netzwerk** > **Bridge-Tabelle**, wählen Sie die MAC-Adresse aus, und klicken Sie auf **Statistiken** .

Citrix ADC Appliances im Aktiv-Aktiv-Modus mit VRRP

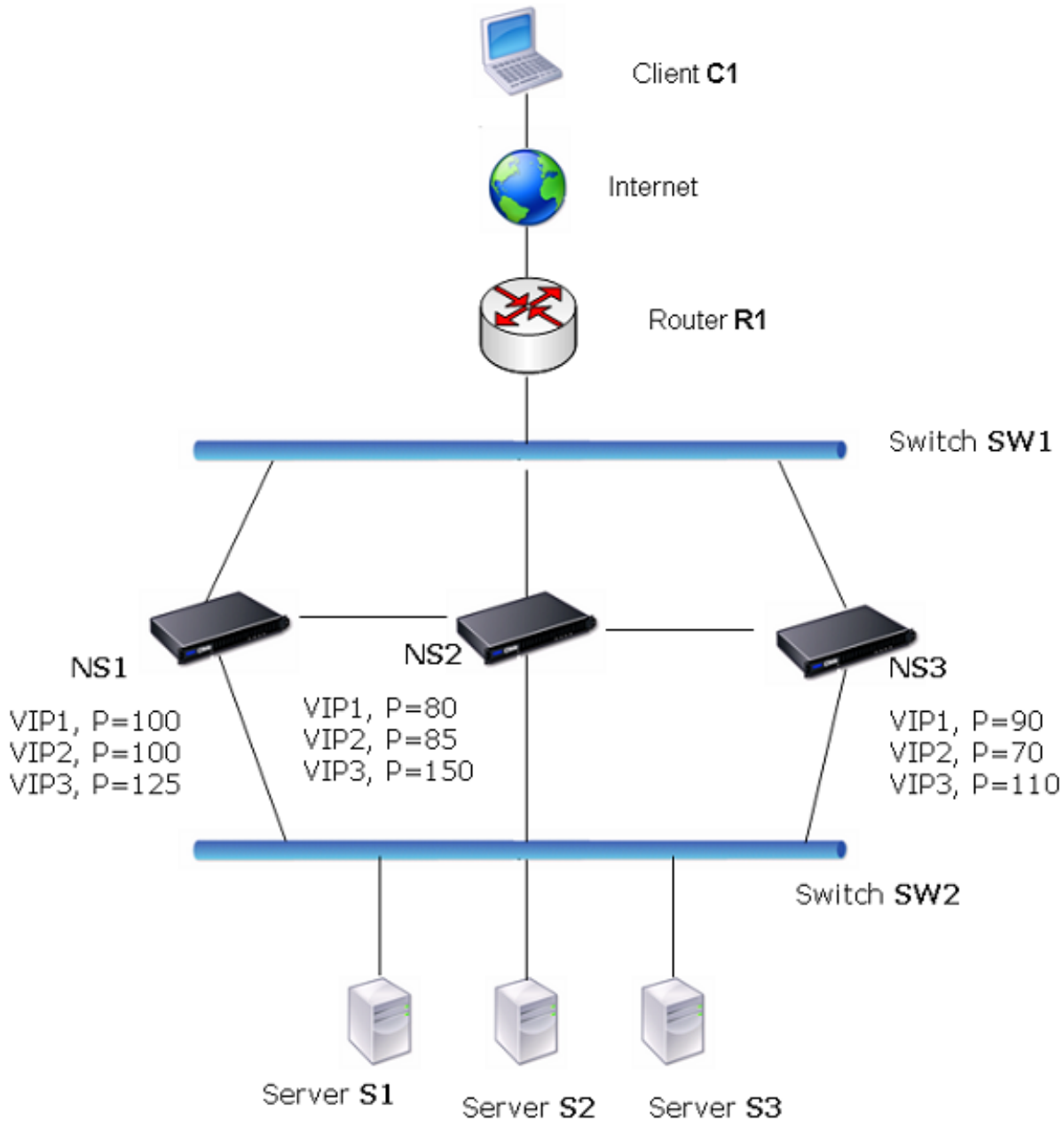
October 5, 2021

Eine aktiv-aktive Bereitstellung nutzt nicht nur Ausfallzeiten, sondern auch alle Citrix ADC Appliances in der Bereitstellung effizient. Im Aktiv-Aktiv-Bereitstellungsmodus werden dieselben VIPs auf allen Citrix ADC Appliances in der Konfiguration konfiguriert, jedoch mit unterschiedlichen Prioritäten, sodass ein bestimmter VIP nur auf einer Appliance gleichzeitig aktiv sein kann.

Der aktive VIP wird als Master-VIP bezeichnet, und die entsprechenden VIPs auf den anderen Citrix ADC Appliances werden als Backup-VIPs bezeichnet. Wenn ein Master-VIP fehlschlägt, übernimmt der Backup-VIP mit höchster Priorität und wird zum Master-VIP. Alle Citrix ADC Appliances in einer aktiven Bereitstellung verwenden das Virtual Router Redundancy Protocol (VRRP) -Protokoll, um ihre VIPs und die entsprechenden Prioritäten in regelmäßigen Abständen anzukündigen.

Citrix ADC-Appliances im Aktiv-Modus können so konfiguriert werden, dass kein Citrix ADC im Leerlauf ist. In dieser Konfiguration sind auf jedem Citrix ADC verschiedene VIPs aktiv. Im folgenden Diagramm sind beispielsweise VIP1, VIP2, VIP3 und VIP4 auf den Einheiten NS1, NS2 und NS3 konfiguriert. Aufgrund ihrer Prioritäten sind VIP1 und VIP 2 auf NS1 aktiv, VIP3 ist auf NS2 aktiv und VIP 4 ist auf NS3 aktiv. Wenn beispielsweise NS1 fehlschlägt, werden VIP1 auf NS3 und VIP2 auf NS2 aktiv.

Abbildung 1. Eine Active-Active-Konfiguration



Die Citrix ADC Appliances im obigen Diagramm verarbeiten den Datenverkehr wie folgt:

1. Client C1 sendet eine Anforderung an VIP1. Die Anforderung erreicht R1.
2. R1 hat keinen ARP-Eintrag für VIP1 und sendet daher eine ARP-Anforderung für VIP1.
3. VIP1 ist in NS1 aktiv, daher antwortet NS1 mit einer Quell-MAC-Adresse als virtueller MAC (z. B. virtueller MAC1), der mit VIP1 verknüpft ist, und VIP1 als Quell-IP-Adresse.
4. SW1 lernt den Port für VIP1 aus der ARP-Antwort und aktualisiert seine Bridge-Tabelle.
5. R1 aktualisiert den ARP-Eintrag mit virtuellem MAC1 und VIP1.

6. R1 leitet das Paket an das VIP1 auf NS1 weiter.
7. Der Lastausgleichsalgorithmus von NS1 wählt Server S2 aus, und NS1 öffnet eine Verbindung zwischen einer seiner SNIP-Adressen und S2.
8. S2 antwortet auf den SNIP auf dem Citrix ADC.
9. NS1 sendet die Antwort von S2 an den Client. In der Antwort fügt NS1 MAC-Adresse der physischen Schnittstelle als Quell-MAC-Adresse und VIP1 als Quell-IP-Adresse ein.
10. Sollte NS1 fehlschlagen, verwenden die Citrix ADC Appliances das VRRP-Protokoll, um VIP1 mit der höchsten Priorität auszuwählen. In diesem Fall wird VIP1 auf NS3 aktiv, und die folgenden beiden Schritte aktualisieren die aktiv-aktive Konfiguration.
11. NS3 sendet eine GARP-Nachricht für VIP1. In der Nachricht ist virtueller MAC1 die Quell-MAC-Adresse und VIP1 die Quell-IP-Adresse.
12. SW1 lernt den neuen Port für virtuellen MAC1 aus dem GARP-Broadcast und aktualisiert seine Bridge-Tabelle, um nachfolgende Clientanforderungen für VIP1 an NS3 zu senden. R1 aktualisiert seine ARP-Tabelle.

Die Priorität eines VIP kann durch Health Tracking geändert werden. Wenn Sie die Health Tracking aktivieren, sollten Sie sicherstellen, dass die Präemption ebenfalls aktiviert ist, damit ein VIP, dessen Priorität gesenkt ist, von einem anderen VIP abgezogen werden kann.

In manchen Situationen kann der Datenverkehr einen Backup-VIP erreichen. Um einen solchen Datenverkehr zu vermeiden, können Sie die Freigabe pro Knoten aktivieren, während Sie eine aktive Konfiguration erstellen. Oder Sie können die globale Option An Master senden aktivieren. Auf einem Knoten, auf dem die Freigabe aktiviert ist, hat er Vorrang vor dem Senden an Master.

Integritätstracking

Die Basispriorität (BP-Bereich 1-255) bestimmt normalerweise, welcher VIP der Master-VIP ist, aber die effektive Priorität (EP) kann auch die Bestimmung beeinflussen.

Wenn beispielsweise ein VIP auf NS1 die Priorität 101 hat und dieselbe VIP auf NS2 die Priorität 99 hat, ist der VIP auf NS1 aktiv. Wenn jedoch zwei vserver die VIP auf NS1 verwenden und einer von ihnen ausfällt, kann die Integritätsüberwachung die EP von VIP auf NS1 reduzieren. VRRP macht dann den VIP auf NS2 zum aktiven VIP.

Im Folgenden sind die Integritätsverfolgungsoptionen zum Ändern von EP aufgeführt:

- **KEINE.** Keine Verfolgung. EP = BP
- **ALLE.** Wenn alle virtuellen Server UP sind, dann EP = BP. Andernfalls EP = 0.
- **ONE.** Wenn mindestens ein virtueller Server UP ist, dann EP = BP. Andernfalls EP = 0.
- **PROGRESSIVE.** Wenn ALLE virtuelle Server UP sind, dann EP = BP. Wenn ALLE virtuelle Server DOWN sind, dann EP = 0. Ansonsten EP = BP (1 - K/N), wobei N die Gesamtzahl der virtuellen Server ist, die mit dem VIP verknüpft sind und k die Anzahl der virtuellen Server ist, die ausgefallen sind.

Hinweis: Wenn Sie einen anderen Wert als NONE angeben, sollte die Präemption aktiviert werden, damit die Backup-VIP mit der höchsten Priorität aktiv wird, wenn die Priorität des Master-VIP heruntergestuft wird.

Präemption

Die Einstellung eines aktiven VIP durch einen anderen VIP, der eine höhere Priorität erhält, ist standardmäßig aktiviert und sollte normalerweise aktiviert werden. In einigen Fällen möchten Sie es jedoch möglicherweise deaktivieren. Die Präemption ist eine Einstellung pro Knoten für jeden VIP.

Die Präemption kann in folgenden Situationen auftreten:

- Ein aktiver VIP fällt aus und ein VIP mit niedrigerer Priorität nimmt seinen Platz ein. Wenn der VIP mit höherer Priorität wieder online ist, wird der aktuell aktive VIP unterbrechen.
- Health Tracking bewirkt, dass die Priorität eines Backup-VIP höher ist als die des aktiven VIP. Der Backup-VIP setzt dann den aktiven VIP voraus.

Freigeben

Für den Fall, dass der Datenverkehr eine Backup-VIP erreicht, wird der Datenverkehr gelöscht, es sei denn, die Freigabeoption ist auf der Backup-VIP aktiviert. Dieses Verhalten ist eine Einstellung pro Knoten für jeden VIP und ist standardmäßig deaktiviert.

In der Abbildung **Eine aktive Konfiguration** VIP1 auf NS1 ist aktiv und VIP1-VIPs auf NS2 und NS3 sind Backups. Unter bestimmten Umständen kann der Datenverkehr VIP1 auf NS2 erreichen. Wenn die Freigabe auf NS2 aktiviert ist, wird dieser Datenverkehr verarbeitet und nicht gelöscht.

Aktiv-Aktiv-Modus konfigurieren

December 7, 2021

Auf jeder Citrix ADC Appliance, die Sie im aktiven Modus bereitstellen möchten, müssen Sie einen virtuellen MAC hinzufügen und den virtuellen MAC an einen VIP binden. Der virtuelle MAC für einen bestimmten VIP muss auf jeder Appliance identisch sein. Wenn beispielsweise VIP 10.102.29.5 auf den Appliances erstellt wird, muss auf jedem Citrix ADC eine virtuelle Router-ID (VRID) erstellt und an VIP 10.102.29.5 auf jedem Citrix ADC gebunden werden. Wenn Sie einen virtuellen MAC an einen VIP binden, sendet die Appliance VRRP-Anzeigen an jedes VLAN, das an diesen VIP gebunden ist. Der virtuelle MAC kann von verschiedenen VIPs freigegeben werden, die auf demselben Citrix ADC konfiguriert sind.

Konfigurieren des Active-Active-Active-Modus von IPv4

Führen Sie die folgenden Aufgaben für jede der Citrix ADC Appliances aus, die in die Active-Active-Konfiguration aufgenommen werden sollen:

- **Fügen Sie eine virtuelle MAC-Adresse**hinzu. Fügen Sie eine virtuelle MAC-Adresse hinzu, indem Sie eine VRID hinzufügen. Sie können auch eine Priorität angeben und die Freigabe und Freigabe für diese VRID-Adresse aktivieren oder deaktivieren.
- **Fügen Sie eine VIP-Adresse hinzu und ordnen Sie die VRID des virtuellen MAC zu**. Fügen Sie eine VIP-Adresse hinzu, und legen Sie den VRID-Parameter auf die neu erstellte VRID fest. Die Attribute der VRID (z.B. Priorität und Präemption) sind an diese VIP-Adresse gebunden.
  Hinweis: Die gleiche VIP-Adresse muss allen anderen Citrix ADC Appliances hinzugefügt werden.

So fügen Sie mit der CLI eine virtuelle MAC-Adresse hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add vrID** <id> [-**priority** <positive_integer>] [-**preemption** (**ENABLED**|**DISABLED**)][-**sharing** (**ENABLED**|**DISABLED**)] [-**tracking** <tracking>]
- **show vrid**

So fügen Sie eine VIP-Adresse mit der CLI hinzu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add ns ip** <IPv4Address> -type VIP -vrid <value>
- **show ns ip**

So konfigurieren Sie einen virtuellen MAC mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **VMAC**, fügen Sie auf der Registerkarte **VMAC** einen neuen virtuellen MAC hinzu, oder bearbeiten Sie einen vorhandenen virtuellen MAC.
2. Legen Sie die folgenden Parameter fest:
   - Virtuelle Router-ID
   - Priorität
   - Verfolgung
   - Präemption
   - Freigeben

So konfigurieren Sie eine VIP-Adresse und ordnen die VRID mit der GUI zu:

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs , fügen Sie auf der Registerkarte IPv4s** eine IP-Adresse vom Typ VIP hinzu.
2. Wählen Sie beim Hinzufügen der IP-Adresse die virtuelle Router-ID aus dem Dropdown-Feld **Virtual Router-ID** aus.

Beispielkonfiguration:

Die folgende Beispielkonfiguration ist für die Bereitstellung von Citrix ADC Appliances NS1 und NS2 im aktiven IPv4-Modus vorgesehen. Die VIP-Adresse 203.0.113.10 ist sowohl auf NS1 als auch auf NS2 konfiguriert, wobei für jede Einheit ein anderer Prioritätswert vorliegt. Auf jeder Appliance ist diese VIP-Adresse an eine virtuelle MAC-Adresse gebunden. 203.0.113.10 ist Master auf NS2, da ihre Priorität (200) auf NS2 höher ist als auf NS1 (100).

```
    Settings on NS1

    > add vrid 10 -Priority 100 -Preemption Enabled -sharing Enabled

    Done

    > add ns ip 203.0.113.10 -type VIP -vrid 10

    Done

    Settings on NS2

    > add vrid 10 -Priority 200 -Preemption Enabled -sharing Enabled

    Done

    > add ns ip 203.0.113.10 -type VIP -vrid 10

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

Konfigurieren des Active-Active-Active-Modus von IPv6

Führen Sie die folgenden Aufgaben für jede der Citrix ADC Appliances aus, die in die Active-Active-Konfiguration aufgenommen werden sollen:

- **Fügen Sie eine virtuelle MAC6-Adresse**hinzu. Fügen Sie eine virtuelle MAC6-Adresse hinzu, indem Sie eine VRID6 hinzufügen. Sie können auch eine Priorität angeben und die Freigabe und Freigabe für diese VRID6-Adresse aktivieren oder deaktivieren.
- **Fügen Sie eine VIP6-Adresse hinzu**. Fügen Sie eine VIP6-Adresse hinzu. Setzen Sie den VRID6-Parameter auf den VRID6 des neu erstellten virtuellen MAC6. Die Attribute des virtuellen MAC6 (z. B. Priorität und Präemption) sind an diese VIP6-Adresse gebunden.
  Hinweis: Die gleiche VIP6-Adresse muss allen anderen Citrix ADC Appliances hinzugefügt werden.

So fügen Sie mit der Befehlszeilenschnittstelle eine virtuelle MAC6-Adresse hinzu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add vrID6** <id> [-**priority** <positive_integer>] [-**preemption** (**ENABLED** | **DISABLED**)] [-**sharing** (**ENABLED** | **DISABLED**)]
- **show vrID6**

So fügen Sie eine VIP6-Adresse mit der CLI hinzu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add ns ip6** <IPv6Address> -**type** VIP -**vrid** <value>
- **show ns ip6**

So konfigurieren Sie einen virtuellen MAC6 mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **VMAC**, fügen Sie auf der Registerkarte **VMAC6** einen neuen virtuellen MAC6 hinzu, oder bearbeiten Sie einen vorhandenen **VMAC6**.
2. Legen Sie die folgenden Parameter fest:
   - Virtuelle Router-ID
   - Priorität
   - Präemption
   - Freigeben

So konfigurieren Sie eine VIP6-Adresse und ordnen die VRID mit der grafischen Benutzeroberfläche zu:

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs**, fügen Sie auf der Registerkarte **IPv6s** eine IPv6-Adresse vom Typ VIP hinzu.
2. Wählen Sie beim Hinzufügen der VIP6-Adresse den VRID6 aus dem Dropdown-Feld **Virtual Router Id** aus.

Beispielkonfiguration:

Die folgende Beispielkonfiguration ist für die Bereitstellung von Citrix ADC Appliances NS1 und NS2 im aktiven IPv6-Modus vorgesehen. Die VIP6-Adresse 2001:db8::5001 ist sowohl auf NS1 als auch auf NS2 konfiguriert, wobei für jede Einheit ein anderer Prioritätswert besteht. Auf jeder Appliance ist diese VIP6-Adresse an eine virtuelle MAC6-Adresse gebunden. 2001:db8::5001 ist Master auf NS2, da die Priorität (200) auf NS2 höher ist als auf NS1 (100).

```
1    Settings on NS1
2    > add vrid6 10 -Priority 100 -Preemption Enable -sharing Enable
3
4    Done
5    > add ns ip6 2001:db8::5001 -type VIP -vrid6 10
6
7    Done
```



```
8      Settings on NS2
9      > add vrid6 10 -Priority 200 -Preemption Enable -sharing Enable
10
11     Done
12     > add ns ip6 2001:db8::5001 -type VIP -vrid6 10
13
14     Done
15 <!--NeedCopy-->
```

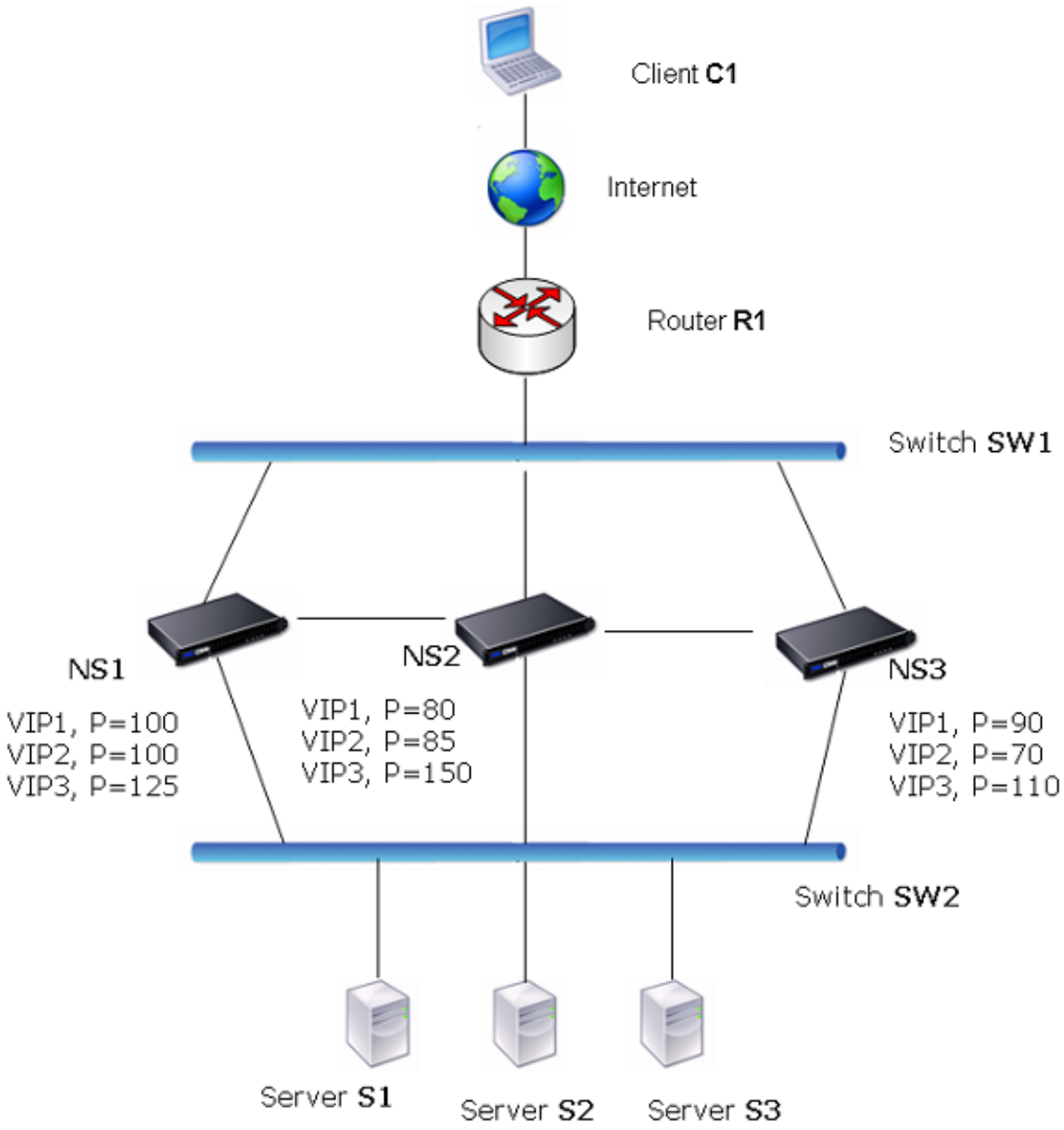
Senden an Master konfigurieren

October 5, 2021

Normalerweise erreicht der für einen VIP bestimmte Datenverkehr die Citrix ADC Appliance, auf der der VIP aktiv ist, da eine ARP-Anforderung mit dem VIP und einem virtuellen MAC auf dieser Appliance den Upstream-Router erreicht hat. In einigen Fällen, z. B. statische Routen, die auf dem Upstream-Router für das VIP-Subnetz konfiguriert sind, oder eine Topologie, die diese Route blockiert, kann der Datenverkehr jedoch eine Citrix ADC Appliance erreichen, auf der sich der VIP im Backup-Zustand befindet. Wenn diese Appliance die Datenpakete an die Appliance weiterleitet, auf der der VIP aktiv ist, müssen Sie die Option An Master senden aktivieren. Dieses Verhalten ist eine Einstellung pro Knoten und ist standardmäßig deaktiviert.

Im folgenden Diagramm ist beispielsweise VIP1 auf NS1, NS2 und NS3 konfiguriert und auf NS1 aktiv. Unter bestimmten Umständen kann der Datenverkehr für VIP1 (aktiv auf NS1) VIP1 auf NS3 erreichen. Wenn die Option An Master senden auf NS3 aktiviert ist, leitet NS3 den Datenverkehr an NS1 über NS2 weiter, indem Routeneinträge für NS1 verwendet werden.

Abbildung 1. Eine Active-Active-Konfiguration mit aktivierter Option An Master senden



So aktivieren Sie das Senden an Master mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set vrIDParam -sendToMaster (ENABLED          DISABLED)
```

Beispiel:


```
> set vrIDParam -sendToMaster ENABLED
 Done
<!--NeedCopy-->
```

So aktivieren Sie das Senden an Master mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk**, klicken Sie in der Gruppe **Einstellungen** auf **Virtuelle Router-Parameter**.
2. Wählen Sie die Option **An Master senden**.

Konfigurieren von VRRP-Kommunikationsintervallen

October 5, 2021

In einer aktiven Bereitstellung verwenden alle Citrix ADC Knoten das Virtual Router Redundancy Protocol (VRRP), um ihre Master-VIP-Adressen und die entsprechenden Prioritäten in VRRP-Anzeigenpaketen (Hallo Nachrichten) in regelmäßigen Abständen anzukündigen.

VRRP verwendet die folgenden Kommunikationsintervalle:

- **Hello Interval**. Intervall zwischen den VRRP-Hallo Nachrichten, die ein Knoten einer Master-VIP-Adresse an seine Peer-Knoten sendet.
- **Dead Intervall**. Zeit, nach der ein Knoten einer Backup-VIP-Adresse den Status der Master-VIP-Adresse als DOWN betrachtet, wenn VRRP-Hallo Nachrichten vom Knoten der Master-VIP-Adresse nicht empfangen werden. Nach dem toten Intervall übernimmt die Backup-VIP-Adresse und wird zur Master-VIP-Adresse.

Sie können diese Intervalle in einen gewünschten Wert ändern. Beide Kommunikationsintervalle gelten pro Knoten für alle VIP-Adressen in diesem Knoten.

So konfigurieren Sie VRRP-Kommunikationsintervalle mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **set vridParam** [-**HelloInterval**] <msecs>[-**DeadInterval**]<secs>
- **sh vrIDParam**

Beispiel:

```
> set vrIDParam -helloInterval 500 -deadInterval 2
 Done
<!--NeedCopy-->
```


So konfigurieren Sie VRRP-Kommunikationsintervalle mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk**, klicken Sie in der Gruppe **Einstellungen** auf **Virtuelle Router-Parameter**.
2. Legen Sie unter **Virtual Router Parameter konfigurieren** die Parameter **Hallo Intervall** und **Dead Interval** fest.
3. Klicken Sie auf **OK**.

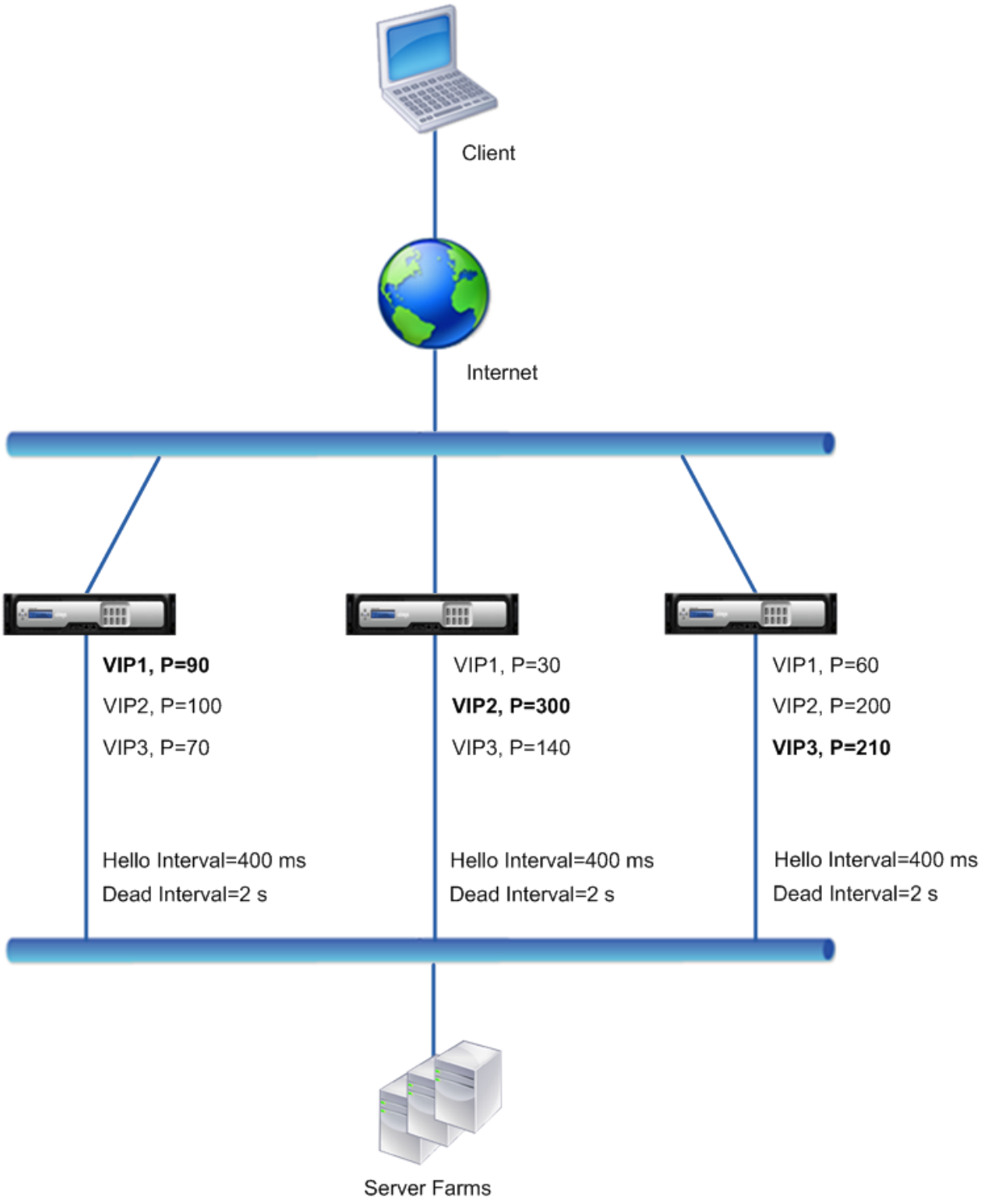
Beispiel 1: Knoten mit denselben VRRP-Deadintervallen

Betrachten Sie eine aktive Bereitstellung, die aus Citrix ADCs NS1, NS2 und NS3 besteht. Virtuelle IP-Adressen VIP1, VIP2, VIP3 sind auf jedem dieser ADCs konfiguriert. Aufgrund ihrer Prioritäten ist VIP1 auf NS1 aktiv, VIP2 ist auf NS2 aktiv und VIP3 ist auf NS3 aktiv.

Wie in der folgenden Tabelle gezeigt, wird das tote Intervall auf allen drei Knoten auf den gleichen Wert (2 Sekunden) gesetzt. Die VRRP-Kommunikationsintervalle (Hello Intervall und Dead Intervall) eines Knotens gelten für alle auf dem Knoten konfigurierten VRIDs und gelten wiederum für alle VIP-Adressen, die den VRIDs auf dem Knoten zugeordnet sind.

Auf jedem Knoten verwenden die aktiven VIP-Adressen (Master) auf diesem Knoten das Hello Intervall, und das Dead Intervall wird von den inaktiven VIP-Adressen (Backup) auf diesem Knoten verwendet. Die Präemption ist für die VIP-Adressen in allen drei Knoten deaktiviert.

In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt: VRRP-Intervall Beispiel 1 Einstellungen.



Der Ausführungsablauf ist wie folgt:

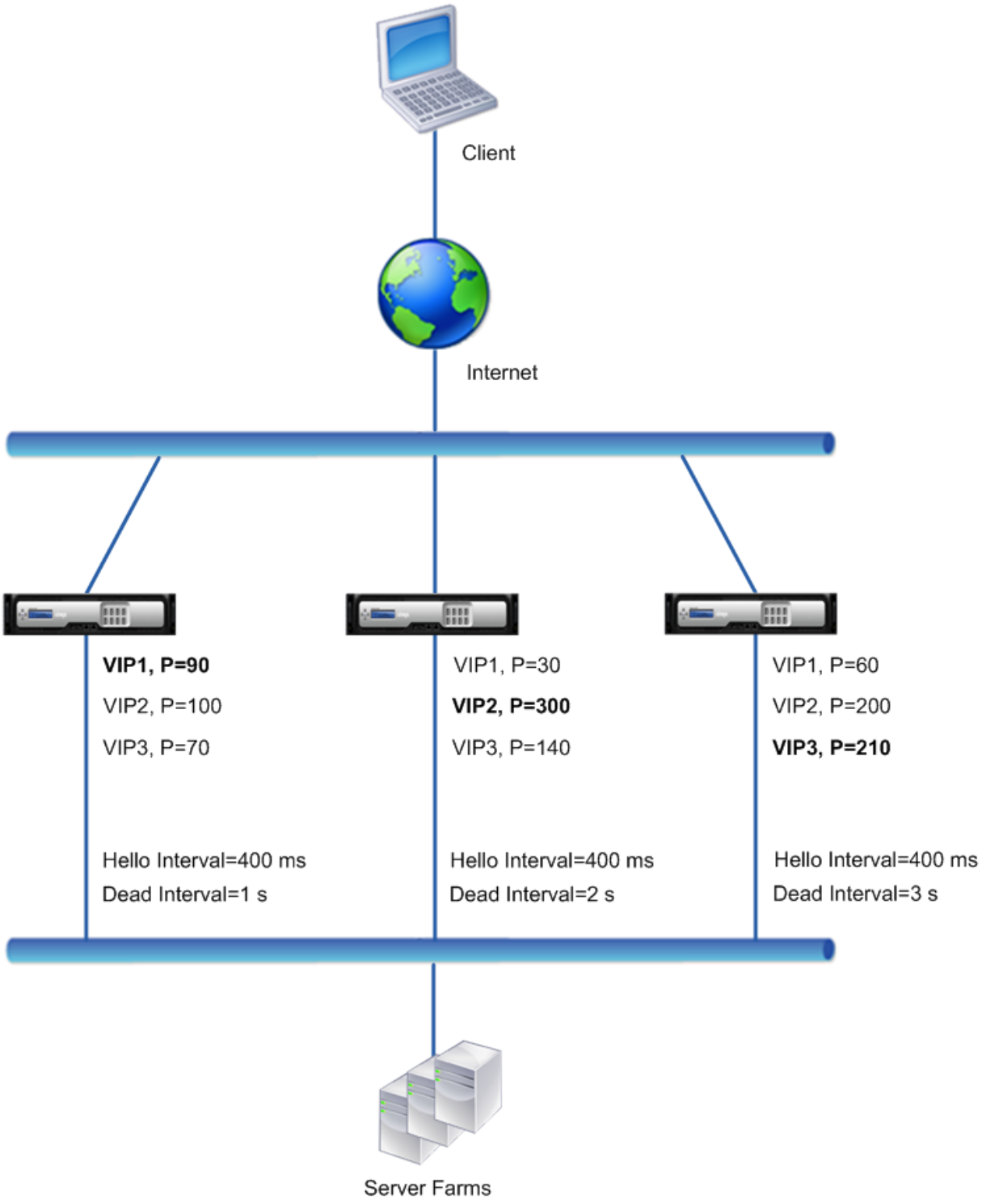
1. NS1 sendet Hallo Nachrichten in einem festgelegten Hallo Intervall von 400 ms an NS2 und NS3 für die VIP1-Adresse, da VIP1 (der Master) auf NS1 aktiv ist. In ähnlicher Weise sendet NS2 Hallo Nachrichten für VIP2 und NS3 sendet Hallo Nachrichten für VIP3.

2. Auf NS1 gilt das festgelegte Deadintervall für VIP2 und VIP3, da sie inaktiv sind (Backups) auf NS1. In ähnlicher Weise gilt für NS2 das festgelegte Dead-Intervall für VIP1 und VIP3, und auf NS3 gilt das festgelegte Dead-Intervall für VIP1 und VIP2.
3. Wenn NS1 ausfällt, betrachten NS2 und NS3 NS1 als ausgefallen, wenn sie für 2 Sekunden keine Hallo Nachrichten von NS1 erhalten (das tote Intervall). VIP1 auf NS3 übernimmt und wird aktiv (Master), da seine VRID-Priorität (60) höher ist als die von VIP1 von NS2 (30).

Beispiel 2: Knoten mit unterschiedlichen VRRP-Deadintervallen

Betrachten Sie eine VRRP-Bereitstellung ähnlich der in Beispiel1 beschriebenen Bereitstellung, jedoch mit einem anderen Deadintervall auf jedem Knoten (NS1, NS2 und NS3). Die Präemption ist für die VIP-Adressen in allen drei Knoten deaktiviert.

In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt: VRRP-Intervall Beispiel 2 Einstellungen.



Der Ausführungsablauf ist wie folgt, wenn NS1 ausfällt:

1. NS2 betrachtet NS1 als heruntergefahren, nachdem zwei Sekunden lang keine Hello Nachrichten von NS1 empfangen wurden (das tote Intervall von NS2).
2. VIP1 auf NS2 übernimmt und wird aktiv (Master). NS2 beginnt jetzt mit dem Senden von Hallo

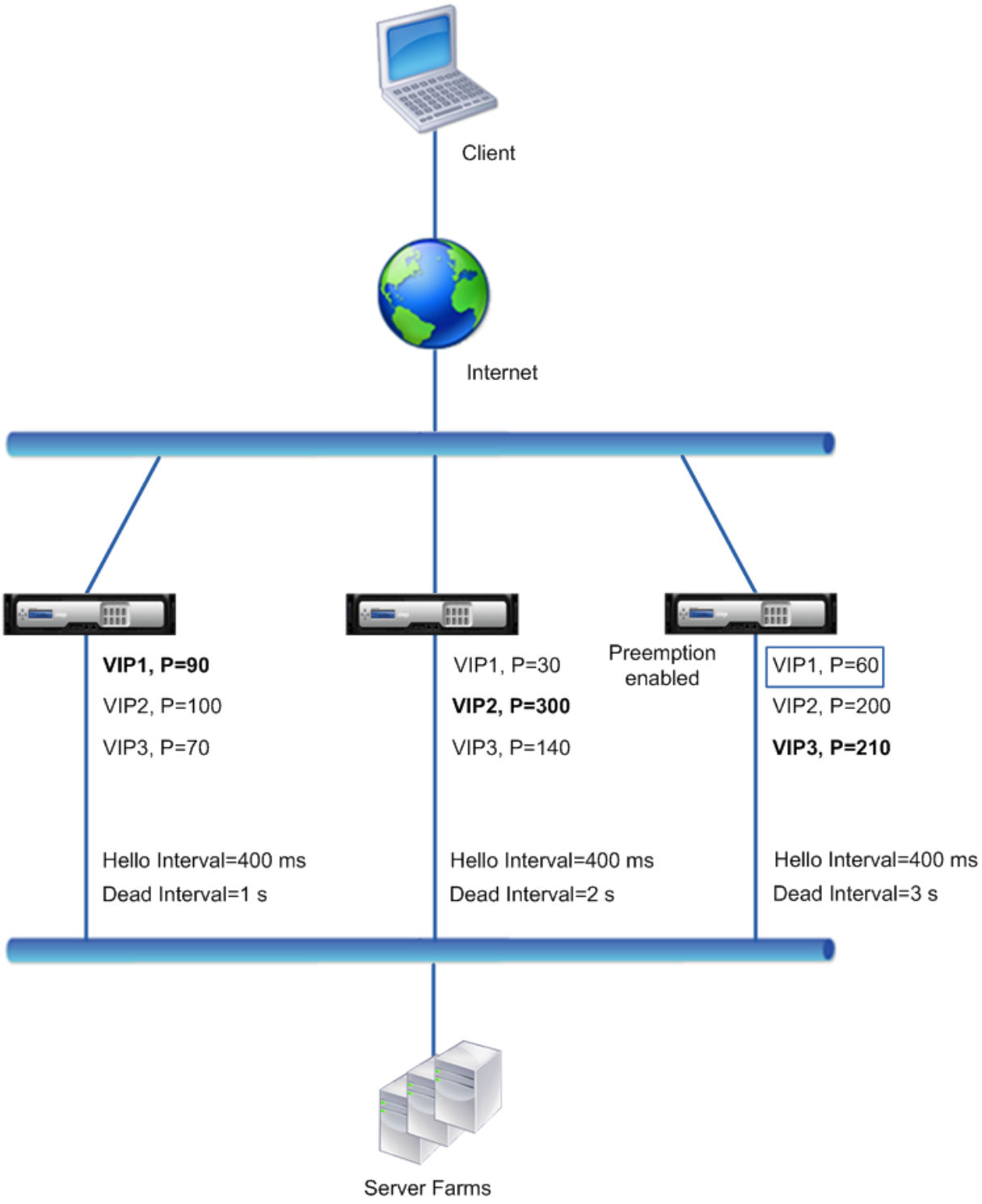
Nachrichten für VIP1.

Obwohl VIP1 auf NS3 eine höhere VRIP-Priorität (60) hat als VIP1 auf NS2 (30), das größere tote Intervall von NS3 (3 Sekunden gegenüber 2 Sekunden für NS2), verhindert, dass VIP1 auf NS3 übernimmt, bevor VIP 1 auf NS2 dies bereits getan hat.

Beispiel 3: Knoten mit unterschiedlichen Deadintervallen und aktivierter Präemption

Betrachten Sie eine VRRP-Bereitstellung ähnlich der in Beispiel1 beschriebenen Bereitstellung, jedoch mit unterschiedlichen Deadintervallen auf den drei Knoten NS1, NS2 und NS3 und mit aktivierter Präemption für die VIP1-Adresse auf NS3.

In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt: VRRP-Intervall Beispiel 3 Einstellungen.



Der Ausführungsablauf ist wie folgt, wenn NS1 ausfällt:

1. NS2 betrachtet NS1 als heruntergefahren, nachdem zwei Sekunden lang keine Hello Nachrichten von NS1 empfangen wurden (das festgelegte Dead Intervall von NS2). Zu diesem Zeitpunkt betrachtet NS3 mit einem toten Intervall von 3 Sekunden nicht NS1 als

heruntergefahren.
2. VIP1 auf NS2 übernimmt und wird aktiv (Master). NS2 beginnt jetzt mit dem Senden von Hallo Nachrichten für VIP1.
3. Beim Empfangen von Hello Messages von NS2 für VIP1 setzt NS3 NS2 für VIP1 voraus, da die Präemption für VIP1 von NS3 aktiviert ist und die VRID-Priorität (60) von VIP1 von NS3 höher ist als die (30) von VIP1 von NS2.
4. VIP1 auf NS3 übernimmt und wird aktiv (Master). NS3 beginnt jetzt mit dem Senden von Hallo Nachrichten für VIP1.

Konfigurieren der Health Tracking basierend auf dem Schnittstellenstatus

October 5, 2021

Um sicherzustellen, dass eine Backup-VIP-Adresse als Master-VIP übernommen wird, bevor der Knoten der aktuellen Master-VIP-Adresse vollständig ausfällt, können Sie einen Knoten so konfigurieren, dass er die Priorität einer VIP-Adresse ändert, wenn sich der Status einer Schnittstelle auf dem Knoten ändert. Beispielsweise verringert der Knoten die Priorität einer VIP-Adresse, wenn sich der Status einer Schnittstelle auf DOWN ändert, und erhöht die Priorität, wenn sich der Status der Schnittstelle in UP ändert. Bei dieser Funktion handelt es sich um eine Konfiguration pro Knoten für jede VIP-Adresse.

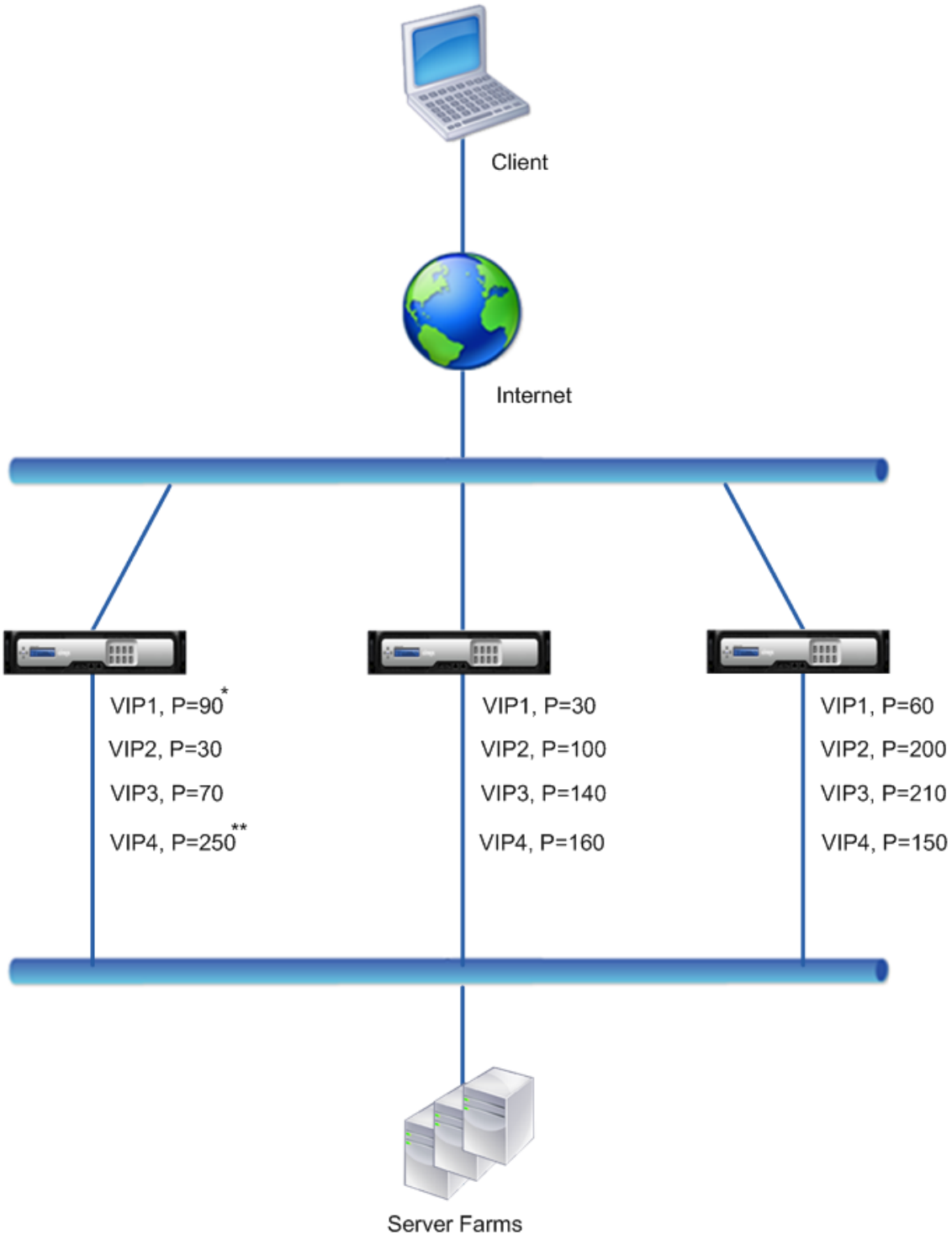
Beispiel

Betrachten Sie eine aktive Bereitstellung, die aus Citrix ADCs NS1, NS2 und NS3 besteht. Virtuelle IP-Adressen VIP1, VIP2, VIP3 und VIP4 werden auf jedem dieser ADCs konfiguriert. Aufgrund ihrer Prioritäten sind VIP1 und VIP4 auf NS1 aktiv, VIP2 ist auf NS2 aktiv und VIP3 ist auf NS3 aktiv.

Um sicherzustellen, dass die aktiven VIP-Adressen auf NS1 von NS2 oder NS3 übernommen werden, bevor NS1 vollständig ausfällt, wird die Schnittstellenbasierte Zustandsverfolgung für die VIP1- und VIP4-Adressen auf NS1 konfiguriert. Das Konfigurieren der schnittstellenbasierten Integritätsverfolgung für eine VIP-Adresse umfasst die Zuordnung der gewünschten Schnittstellen und das Festlegen des Parameters mit reduzierter Priorität (TrackIfNumPriority) für die zugeordnete VRID der VIP-Adresse. Beispielsweise sind auf NS1 Schnittstellen 1/2, 1/3 und 1/5 der VRID von VIP1 zugeordnet, und die reduzierte Priorität ist auf 20.

Die Präemption ist für diese VIP-Adressen in allen drei Knoten aktiviert.

In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt: Beispieleinstellungen für Health Tracking.



* Packet Interfaces = 1/2, 1/3, 1/5
Reduced Priority = 20

** Packet Interfaces = 1/5, 1/7
Reduced Priority = 55

Der Ausführungsablauf ist auf NS1 wie folgt, wenn mehrere Schnittstellen auf NS1 ausfallen:

1. Wenn Schnittstelle 1/3 ausfällt, wird die Priorität von Adresse VIP1 um 20 reduziert (der reduzierte Prioritätswert von VIP1), da Schnittstelle 1/3 mit VIP1 verknüpft ist:
   - Effektive Priorität von VIP1 = (Aktuelle Priorität - reduzierte Priorität) = (90-20) = 70
2. Ebenso wird bei Ausfall der Schnittstelle 1/5 die Priorität der Adresse VIP1 weiter reduziert:
   - Effektive Priorität von VIP1 = (Aktuelle Priorität - reduzierte Priorität) = (70-20) = 50
3. Zu diesem Zeitpunkt ist die effektive Priorität von VIP1 auf NS1 geringer als die Priorität von VIP1 auf NS3. NS3 setzt NS1 für VIP1 voraus. VIP1 auf NS3 übernimmt und wird aktiv (Master).
4. Da Schnittstelle 1/5 auch mit VIP4 verknüpft ist, wird die Priorität von VIP4 um den reduzierten Prioritätswert des VIP4 reduziert (55).
   - Effektive Priorität von VIP4 = (250 - 55) = 195
5. Wenn die Schnittstelle 1/7 ausfällt, wird die Priorität von VIP4 weiter reduziert:
   - Effektive Priorität von VIP4 = (Aktuelle Priorität - reduzierte Priorität) = (195-55) = 145
6. Zu diesem Zeitpunkt ist die effektive Priorität von VIP4 auf NS1 geringer als die Priorität von VIP4 auf NS2. NS2 setzt NS1 für VIP4 voraus. VIP4 auf NS3 übernimmt und wird aktiv (Master). Diese Konfiguration stellt sicher, dass keine der vier VIP-Adressen auf NS1 aktiv sind, bevor sie vollständig ausfällt.

Konfigurationsschritte für IPv4 Active-Active-Modus

Um diese Funktion auf einem Knoten für eine VIP-Adresse zu konfigurieren, legen Sie den Parameter Reduced Priority (TrackIfNumPriority) fest und ordnen dann die Schnittstellen zu, deren Status verfolgt werden soll, um die Priorität der VIP-Adresse zu ändern. Wenn sich eine der zugeordneten Schnittstelle Status auf DOWN oder UP ändert, reduziert oder erhöht der Knoten die Priorität der VIP-Adresse um den konfigurierten Wert mit reduzierter Priorität (TrackIfNumPriority).

So legen Sie mit der CLI eine reduzierte Priorität fest und binden Schnittstellen an die virtuelle Router-ID:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **set vRID** <id>[-**TrackifNumPriority**]<positive_integer>
- **bind vrID** <id> -**trackifNum** <interface_name>
- **show vrID** <id>

Beispiel:

```
1     > set vrID 125 -trackifNumPriority 10
2     Done
3
4     > bind vrID 125 -trackifNum 1/4 1/5
5     Done
```



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

So legen Sie mit der GUI eine reduzierte Priorität fest und binden Schnittstellen an die virtuelle Router-ID:

1. Navigieren Sie zu **System** > **Netzwerk** > **VMAC.**
2. Wählen Sie auf der Registerkarte **VMACs** eine virtuelle Router-ID aus, und klicken Sie auf **Bearbeiten**.
3. Legen Sie unter **Virtuelle MAC konfigurieren** den Parameter **Reduzierte Priorität** fest.
4. Wählen Sie die für die Option **Nachverfolgte Schnittstellen für VRID** aus, und fügen Sie der virtuellen Router-ID unter **Schnittstellen zuordnen** Schnittstellen hinzu.

Konfigurationsschritte für IPv6-Aktiv-Modus

Um dieses Feature auf einem Knoten für eine VIP6-Adresse zu konfigurieren, legen Sie den Parameter Reduced Priority (TrackIfNumPriority) fest und ordnen dann die Schnittstellen zu, deren Status verfolgt werden soll, um die Priorität der VIP6-Adresse zu ändern. Wenn sich eine der zugeordneten Schnittstelle Status in DOWN oder UP ändert, reduziert oder erhöht der Knoten die Priorität der VIP6-Adresse um den konfigurierten Wert mit reduzierter Priorität (TrackIfNumPriority).

So ändern Sie die Priorität einer VIP-Adresse automatisch mit der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehlssätze ein.

- Wenn Sie einen neuen virtuellen MAC6 hinzufügen:
  - **add vrID6** <id> [-**TrackifNumPriority**]
  - **bind vrID6** <id> -**trackifNum** <interface_name>
  - **show vrID6** <id>
- Wenn Sie einen vorhandenen virtuellen MAC6 neu konfigurieren:
  - **set vrID6** <id> [-**TrackifNumPriority**]
  - **bind vrID6** <id> -**trackifNum** <interface_name>
  - **show vrID6** <id>

Beispiel:

```
    > set vrID6 130 -trackifNumPriority 10
    Done

    > bind vrID6 130 -trackifNum 1/4 1/5
    Done
<!--NeedCopy-->
```


Verzögerung der Präemption

October 5, 2021

Standardmäßig überschreitet eine Backup-VIP-Adresse die Master-VIP-Adresse unmittelbar nachdem ihre Priorität höher ist als die des Master-VIP. Wenn Sie eine Backup-VIP-Adresse konfigurieren, können Sie angeben, wie lange die Präemption verzögert werden soll. Die Vorzugsverzögerungszeit ist eine Einstellung pro Knoten für jede Backup-VIP-Adresse.

Die Einstellung für die Vorzugsverzögerung für einen Backup-VIP gilt nicht unter den folgenden Bedingungen:

- Der Knoten des Master-VIP geht aus. In diesem Fall übernimmt die Backup-VIP als Master-VIP nach dem auf dem Backup-VIP-Knoten festgelegten Dead-Intervall.
- Die Priorität des Master-VIP ist auf Null gesetzt. Die Backup-VIP übernimmt als Master-VIP nach dem auf dem Backup-VIP-Knoten festgelegten Dead-Intervall.

Beispiel: Verzögerung der Präemption

Betrachten Sie eine aktive Bereitstellung, die aus Citrix ADC Appliances NS1 und NS2 besteht. Die virtuelle IP-Adresse VIP1 ist auf jeder dieser Appliances konfiguriert. Aufgrund ihrer Prioritäten ist VIP1 Master auf NS2. Die Präemption ist aktiviert, und die Vorzugsverzögerungszeit wird für VIP1 auf diesen beiden Knoten festgelegt.

In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt.

Entity und Parameter	Einstellungen auf NS1	Einstellungen auf NS2
VIP1 (nur zu Referenzzwecken)	**IP address:** 192.0.1.10, **VRID:** 10, **Priority:** 100, **Preemption:** Enabled, **Preemption delay time:** 1000 seconds	**IP address:** 192.0.1.10, **VRID: 10**, **Priority:** 200, **Preemption:** Enabled, **Preemption delay time:** 2000 seconds
Dead Intervall	1 Sekunden	2 Sekunden

Im Folgenden finden Sie einige Beispiele für ein mögliches Präemptionsverhalten in diesem Setup:

- Wenn die Priorität von VIP1 auf NS1 auf einen Wert (z. B. 210) festgelegt ist, der höher ist als der von VIP1 auf NS2, übernimmt VIP1 auf NS1 nach der festgelegten Vorzugsverzögerungszeit (1000 Sekunden) als Master.
- Wenn dieser Bereitstellung ein dritter Knoten NS3 mit den folgenden VRRP-Einstellungen hinzugefügt wird, wird VIP1 auf NS3 nach der festgelegten Vorzugsverzögerungszeit (3000

Sekunden) zum Master.
  - VIP1
    * VRID: 30
    * IP-Adresse:
    * Priorität = 300
    * Vorzugsverzögerungszeit = 3000 Sekunden
- Wenn NS2 ausfällt, übernimmt VIP1 auf NS1 nach 1 Sekunde als Master (Dead Intervall auf NS1). Die Vorzugsverzögerungszeit für VIP1 auf NS1 gilt in diesem Fall nicht.
- Wenn NS2 ausfällt und NS1 neu gestartet wird, wird VIP1 auf NS1 Master-1-Sekunden-Wert (set dead interval on NS1), nachdem NS1 auftaucht. Die Vorzugsverzögerungszeit für VIP1 auf NS1 gilt in diesem Fall nicht.
- Wenn die Priorität von VIP1 auf NS2 auf Null gesetzt ist, wechselt VIP1 in den Standby-Modus. VIP1 auf NS1 übernimmt nach 1 Sekunde als Master (Dead Intervall auf NS1 einstellen). Die Vorzugsverzögerungszeit für VIP1 auf NS1 gilt in diesem Fall nicht.

Konfigurieren der Verzögerungsvorspannung für den Aktiv-Aktiv-Modus IPv4

Um die Vorzugsverzögerungszeit für eine VIP-Adresse zu konfigurieren, legen Sie den Timer-Parameter für die Vorzugsverzögerung der zugeordneten virtuellen MAC-Adresse fest. Sie können diesen Parameter festlegen, wenn Sie die Adresse hinzufügen, oder Sie können eine vorhandene virtuelle MAC-Adresse ändern.

So konfigurieren Sie die Vorzugsverzögerungszeit mit der Befehlszeilenschnittstelle:

- Geben Sie an der Eingabeaufforderung Folgendes ein, um die Verzögerungszeit beim Hinzufügen eines virtuellen MAC festzulegen:
  - **add vrID** <id> -**preemptiondelaytimer** <secs>
  - **show vrID**
- Geben Sie an der Eingabeaufforderung Folgendes ein, um die Verzögerungszeit bei der Änderung eines virtuellen MAC festzulegen:
  - **set vrID** <id> -**preemptiondelaytimer** <secs>
  - **show vrID**

So konfigurieren Sie die Vorzugsverzögerungszeit mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **VMAC**.
2. Auf der Registerkarte **VMAC**. Legen Sie beim Hinzufügen eines neuen virtuellen MAC oder beim Bearbeiten eines vorhandenen virtuellen MAC den Parameter **Zeitüberschreitung** fest.

Beispielkonfiguration:

In der folgenden Konfiguration werden die Einstellungen verwendet, die in der Tabelle im Abschnitt Beispiel: Verzögerung der Präemption aufgeführt sind.


```
    Settings on NS1

    > set vrid param  -deadInterval 1

    Done

    > add ns ip 192.0.1.10 255.255.255.255  -type VIP

    Done

    > add vrid 10  -Priority 100  -Preemption Enable  -
       preemptiondelaytimer 1000

    Done

    > bind ns ip 192.0.1.10 255.255.255.255  -vrid 10

    Done

    Settings on NS2

    > set vrid param  -deadInterval 2

    Done

    > add ns ip 192.0.1.10 255.255.255.255  -type VIP

    Done

    > add vrid 20  -Priority 200  -Preemption Enable  -
       preemptiondelaytimer 2000

    Done

    > set ns ip 192.0.1.10 255.255.255.255  -vrid 10

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


Konfigurieren der Verzögerungsvorspannung für den aktiven IPv6-Modus

Um die Vorzugsverzögerungszeit für eine VIP6-Adresse zu konfigurieren, legen Sie den Zeitgeberparameter für die Vorzugsverzögerung der zugeordneten virtuellen MAC6-Adresse fest. Sie können diesen Parameter festlegen, wenn Sie die virtuelle MAC6-Adresse hinzufügen, oder Sie können eine vorhandene virtuelle MAC6-Adresse ändern.

So konfigurieren Sie die Vorzugsverzögerungszeit mit der Befehlszeilenschnittstelle:

- Geben Sie an der Eingabeaufforderung Folgendes ein, um die Verzögerungszeit beim Hinzufügen eines virtuellen MAC6 festzulegen:
  - **add vrID6** <id> -**preemptiondelaytimer** <secs>
  - **show vrID6**
- Geben Sie an der Eingabeaufforderung Folgendes ein, um die Verzögerungszeit bei der Änderung eines virtuellen MAC6 festzulegen:
  - **set vrID6** <id> -**preemptiondelaytimer** <secs>
  - **show vrID6**

So konfigurieren Sie die Vorzugsverzögerungszeit mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **VMAC**.
2. Auf der Registerkarte **VMAC6**. Legen Sie beim Hinzufügen einer virtuellen MAC6-Adresse oder beim Bearbeiten einer vorhandenen virtuellen MAC6-Adresse den Parameter **Zeitüberschreitung** fest.

Beibehalten einer VIP-Adresse im Backupstatus

October 5, 2021

Sie können erzwingen, dass eine VIP-Adresse immer im Backup-Zustand bleibt. Dieser Vorgang ist hilfreich bei der Wartung oder beim Testen einer VRRP-Bereitstellung.

Wenn eine VIP-Adresse gezwungen ist, im Backup-Zustand zu bleiben, nimmt sie nicht an VRRP-Statusübergängen teil. Außerdem kann es nicht Master werden, selbst wenn alle anderen Knoten heruntergehen.

Um zu erzwingen, dass eine VIP-Adresse im Backup-Zustand bleibt, legen Sie die Priorität der zugeordneten virtuellen MAC-Adresse auf Null fest. Um sicherzustellen, dass keine der VIP-Adressen eines Knotens Datenverkehr während eines Wartungsprozesses auf dem Knoten verarbeitet, setzen Sie alle Prioritäten auf Null.

Sie können die Priorität einer virtuellen MAC-Adresse festlegen, während Sie die Adresse hinzufügen oder ändern.

So erzwingen Sie, dass eine VIP-Adresse mit der CLI im Backup-Zustand bleibt:

- Um die Priorität beim Hinzufügen eines virtuellen MAC festzulegen, geben Sie an der Eingabeaufforderung Folgendes ein:
  - **add vrID** <id> -**priority** 0
  - **show vrID**
- Um die Priorität beim Ändern eines virtuellen MAC festzulegen, geben Sie an der Eingabeaufforderung Folgendes ein:
  - **set vrID** <id> -**priority** 0
  - **show vrID**

So erzwingen Sie, dass eine VIP-Adresse mit der GUI im Backup-Zustand bleibt:

1. Navigieren Sie zu **System** > **Netzwerk** > **VMAC**.
2. Legen Sie auf der Registerkarte **VMAC** beim Hinzufügen eines neuen virtuellen MAC oder beim Bearbeiten eines vorhandenen virtuellen MAC den Parameter **Priority** auf Null fest.

Netzwerk-Visualizer

October 5, 2021

Der Netzwerkvisualizer zeigt eine grafische Ansicht aller Schnittstellen, Kanäle, VLANs, IP-Adressen und Bindungen an VLANs auf einer Citrix ADC Appliance. Eine aktivierte Schnittstelle oder Kanal hat ein schwarzes Label. Eine deaktivierte Schnittstelle oder Kanal hat eine rote Bezeichnung.

Dieses vollständige Bild der Netzwerkverbindungen der Appliance kann nützlich sein, um Fehler im Netzwerkdesign zu erkennen und das Netzwerk zu optimieren. Es kann auch einem neuen Administrator helfen, die Netzwerkkonfiguration der Appliance leicht zu verstehen.

So öffnen Sie den Network Visualizer:

Navigieren Sie zu **System** > **Netzwerk**. Klicken Sie unter **Monitorverbindungen**auf **Network Visualizer**.

Konfigurieren des Link Layer Discovery-Protokolls

October 5, 2021

Der Citrix ADC unterstützt den Industriestandard (IEEE 802.1AB) Link Layer Discovery Protocol (LLDP). LLDP ist ein Layer-2-Protokoll, mit dem Citrix ADC seine Identität und Fähigkeiten an die direkt verbundenen Geräte weitergeben kann und die Identität und Fähigkeiten dieser Nachbargeräte erlernen kann.

> **Hinweis:**
> Das Link Layer Discovery Protocol (LLDP) wird nur in Citrix ADC MPX-Plattformen unterstützt.

Mithilfe von LLDP überträgt und empfängt Citrix ADC Informationen in Form von LLDP-Nachrichten, die als LLDP-Paketdateneinheiten (LLDPUs) bezeichnet werden. Eine LLDPU ist eine Folge von Typ, Länge, Wert (TLV) Informationselementen. Jede TLV enthält eine bestimmte Art von Informationen über das Gerät, das die LLDPDU überträgt. Citrix ADC sendet die folgenden TLVs in jeder LLDPU:

- Gehäuse-ID
- Port-ID
- Zeit-zu-Live-Wert
- Systemname
- Systembeschreibung
- Portbeschreibung
- Systemfunktionen
- Verwaltungsadresse
- Port VLAN-ID
- Link-Aggregation

Hinweis: Sie können die TLVs nicht angeben, die in LLDP-Nachrichten gesendet werden sollen.

Citrix ADC Schnittstellen unterstützen die folgenden LLDP-Modi:

- **KEINE**. Die Schnittstelle empfängt oder überträgt weder LLDP-Nachrichten an das direkt angeschlossene Gerät.
- **TRANSMITTER**. Die Schnittstelle überträgt LLDP-Nachrichten an das direkt angeschlossene Gerät, empfängt jedoch keine LLDP-Nachrichten von dem direkt verbundenen Gerät.
- **RECEIVER**. Die Schnittstelle empfängt LLDP-Nachrichten vom direkt verbundenen Gerät, überträgt jedoch keine LLDP-Nachrichten an das direkt angeschlossene Gerät.
- **TRANSCEIVER**. Die Schnittstelle überträgt LLDP-Nachrichten an das direkt verbundene Gerät und empfängt LLDP-Nachrichten.

Der LLDP-Modus einer Schnittstelle hängt vom LLDP-Modus ab, der auf globaler Ebene und der Schnittstellenebene konfiguriert ist. Die folgende Tabelle zeigt die Modi, die sich aus den verfügbaren Kombinationen von Einstellungen auf globaler und Schnittstellenebene ergeben: Interface- und LLDP-Modi auf globaler Ebene.

Beachten Sie die folgenden Punkte im Zusammenhang mit LLDP-Nachrichten, die vom Citrix ADC übertragen oder empfangen werden:

- **Übertragen von LLDP-Nachrichten.** Der Citrix ADC überträgt LLDPUs von Schnittstellen, die im TRANSMITTER- oder TRANSCEIVER LLDP-Modus arbeiten.

  Im Folgenden sind die globalen LLDP-Übertragungsparameter auf dem Citrix ADC aufgeführt:

  - **Timer** Intervall in Sekunden zwischen LLDPUs, die der Citrix ADC an ein direkt angeschlossenes Gerät sendet.
  - **Holdtime Multiplikator**. Ein Multiplikator zum Berechnen der Dauer, für die das empfangende Gerät die LLDP-Informationen in seiner Datenbank speichert, bevor es verworfen oder entfernt wird. Die Dauer wird als Parameterwert für **Holdtime Multiplier** berechnet, multipliziert mit dem Timer-Parameterwert.

- **Empfangen von LLDP-Nachrichten.** Citrix ADC speichert die LLDPDU-Informationen in seiner Management Information Base (MIB). Die gespeicherten LLDP-Informationen werden unter der ID der Schnittstelle klassifiziert oder gruppiert, die die LLDPDU erhalten hat. Der Citrix ADC behält diese LLDP-Informationen für die in der empfangenen LLDPU angegebene Dauer bei.

  Wenn der ADC eine weitere LLDPDU auf einer Schnittstelle empfängt, bevor die gespeicherten LLDP-Informationen für diese Schnittstelle verworfen werden, ersetzt der ADC die gespeicherten LLDP-Informationen für diese Schnittstelle durch Informationen in der neuen LLDPDU.

Konfigurationsschritte

Die Konfiguration von LLDP auf einer Citrix ADC Appliance umfasst die folgenden Aufgaben:

1. **Legen Sie LLDP-Parameter auf globaler Ebene fest.** In dieser Aufgabe legen Sie die globalen LLDP-Parameter wie LLDP Timer, Hold Time Multiplier und LLDP-Modus fest.
2. **Legen Sie die LLDP-Parameter der Schnittstellenebene fest.** In dieser Aufgabe legen Sie den LLDP-Modus für eine Schnittstelle fest.
3. **(Optional) Zeigt Informationen zu benachbarten Geräten an.** Sie können die LLDP-Informationen des benachbarten Geräts anzeigen, die auf allen Schnittstellen des Citrix ADC erfasst werden, oder nur die LLDP-Informationen, die auf bestimmten Schnittstellen gesammelt wurden. Wenn Sie keine Schnittstelle angeben, werden die Informationen für alle Schnittstellen angezeigt.

Im Folgenden sind die Voraussetzungen für die Konfiguration von LLDP auf einem Citrix ADC aufgeführt:

1. Stellen Sie sicher, dass Sie das standardmäßige LLDP-Protokoll (IEEE 802.1AB) verstehen.
2. Stellen Sie sicher, dass Sie LLDP auf den gewünschten direkt verbundenen Geräten konfiguriert haben.

CLI-Verfahren

So legen Sie LLDP-Parameter auf globaler Ebene mit der CLI fest:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- set lldp param [- [-holdTimeTxMult][-timer <positive_integer>] <positive_integer>[-Modus]<Mode>
- show lldp param

So konfigurieren Sie eine Schnittstelle für LLDP mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- set interface <id> -lldpmode <lldpmode>
- show interface <id>

So zeigen Sie Nachbargeräteinformationen mit der Befehlszeilenschnittstelle an:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- show lldp neighbors
- show lldp neighbors <ifnum>

GUI-Verfahren

So legen Sie die globalen LLDP-Parameter mit der GUI fest:

1. Navigieren Sie zu System > Netzwerk, und klicken Sie auf LLDP-Parameter konfigurieren.
2. Legen Sie die folgenden Parameter fest:
    - Timer-Multiplikator halten
    - Timer
    - Modus

So konfigurieren Sie eine Schnittstelle für LLDP mit der GUI:

Navigieren Sie zu System > Netzwerk > Schnittstellen, öffnen Sie die Schnittstelle und legen Sie den Parameter LLDP-Modus fest.

So zeigen Sie Nachbargeräteinformationen mit der GUI an:

Navigieren Sie zu System > Netzwerk > Schnittstellen, und wählen Sie in der Liste Aktion die Option LLDP-Nachbarn anzeigen aus.

LLDP-Unterstützung in einem Cluster-Setup

In einem Cluster-Setup zeigen die GUI und CLI die LLDP-Nachbarkonfiguration aller oder bestimmter Clusterknoten an, wenn über die Cluster-IP-Adresse (CLIP) auf die GUI oder CLI zugegriffen wird. Jede Änderung des LLDP-Modus auf globaler Ebene wird auf den globalen LLDP-Modus auf jedem der Clusterknoten angewendet.

Betrachten Sie ein Beispiel für ein Cluster-Setup von drei Knoten, NS1, NS2 und NS3. Jeder dieser Knoten ist mit beiden Routern Router-1 und Router-2 verbunden. Die folgende Ausgabe wird angezeigt, wenn der Vorgang **show lldp neighbor -summary** auf der Cluster-CLI ausgeführt wird,

auf die über die Cluster-IP-Adresse (CLIP) des Cluster-Setups zugegriffen wird. Die Ausgabe zeigt die LLDP-Nachbarinformationen aller dieser Knoten.

```
> show lldp neighbor -summary

Node Id: 1
------------------------------------------------------------
    Interface    ChassisId           PortId     System name
------------------------------------------------------------
1     1/1/1      fe:c7:3b:13:bd:11    1/1         Router-1

2     1/1/2      12:68:7b:9e:4c:11    1/1         Router-2

Node Id: 2
------------------------------------------------------------
    Interface    ChassisId           PortId     System name
------------------------------------------------------------
1     2/1/1      fe:c7:3b:13:bd:12    1/2        Router-1

2     2/1/2      12:68:7b:9e:4c:12    1/2        Router-2

Node Id: 3
------------------------------------------------------------
    Interface    ChassisId            PortId     System name
------------------------------------------------------------

1     3/1/1       fe:c7:3b:13:bd:13    1/3        Router-1

2     3/1/2       12:68:7b:9e:4c:13    1/3        Router-2

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

Jumbo Frames

October 5, 2021

Citrix ADC Appliances unterstützen den Empfang und die Übertragung von Jumbo-Frames mit bis zu 9216 Byte IP-Daten. Jumbo-Frames können große Dateien effizienter übertragen, als es mit der Standard-IP-MTU-Größe von 1500 Bytes möglich ist.

Eine Citrix ADC Appliance kann Jumbo-Frames in den folgenden Bereitstellungsszenarien verwenden:

- Jumbo an Jumbo. Die Appliance empfängt Daten als Jumbo-Frames und sendet sie als Jumbo-Frames.
- Nicht Jumbo an Jumbo. Die Appliance empfängt Daten als reguläre Frames und sendet sie als Jumbo-Frames.
- Jumbo an Nicht-Jumbo. Die Appliance empfängt Daten als Jumbo-Frames und sendet sie als reguläre Frames.

Die Citrix ADC Appliance unterstützt Jumbo-Frames in einer Load Balancing-Konfiguration für die folgenden Protokolle:

- TCP
- Beliebiges Protokoll über TCP (z. B. HTTP)
- SIP
- RADIUS

Konfigurieren der Unterstützung für Jumbo Frames auf einer Citrix ADC Appliance

October 5, 2021

Damit die Citrix ADC Appliance Jumbo-Frames unterstützen kann, legen Sie die MTU auf mehr als 1500 auf Schnittstellen oder LA-Kanälen und auf VLANs fest, auf denen die Citrix ADC Appliance Jumbo-Frames unterstützen soll.

Vor dem Festlegen der MTU von Schnittstellen, LA-Kanälen oder VLANs auf einer Citrix ADC Appliance zu berücksichtigende Punkte

1. Wenn Sie einen LA-Kanal erstellen, übernimmt der Kanal die MTU der ersten gebundenen Schnittstelle, wenn keine MTU für den Kanal angegeben ist.
2. Die MTU für einen Kanal wird an alle gebundenen Schnittstellen weitergegeben.
3. Wenn eine Schnittstelle an den Kanal gebunden ist, dessen MTU sich von der MTU der Schnittstelle unterscheidet, wechselt die Schnittstelle in die inaktive Liste.
4. Wenn Sie die MTU einer Mitgliederschnittstelle ändern, wechselt die Schnittstelle in die inaktive Liste.
5. Wenn eine Schnittstelle vom Kanal ungebunden ist, behält die Schnittstelle den MTU-Wert des Kanals bei.
6. Sie können die MTU für eine Schnittstelle, einen Kanal oder ein VLAN auf einen Wert im Bereich von 1500-9216 einstellen.

7. Sie können die MTU nicht für das Standard-VLAN festlegen. Die Citrix ADC Appliance verwendet die MTU der Schnittstelle, über die sie Daten von oder an das Standard-VLAN empfängt oder sendet.
8. Für TCP-basierten Datenverkehr in einer Lastausgleichskonfiguration auf einer Citrix ADC Appliance werden MSSs an jedem Endpunkt für die Unterstützung von Jumbo-Frames entsprechend festgelegt:
    - Bei einer Verbindung zwischen einem Client und einem virtuellen Lastausgleichsserver auf der Citrix ADC Appliance wird der MSS der Citrix ADC-Appliance in einem TCP-Profil festgelegt, das dann an den virtuellen Lastausgleichsserver gebunden wird.
    - Für eine Verbindung zwischen der Citrix ADC Appliance und einem Server wird der MSS auf NS1 in einem TCP-Profil festgelegt, das dann an den Dienst gebunden ist, der den Server auf der Citrix ADC-Appliance darstellt.
    - Standardmäßig ist ein TCP-Profil nstcp_default_profile an alle TCP-basierten Load Balancing-Server und -Dienste auf der Citrix ADC Appliance gebunden.
    - Zur Unterstützung von Jumbo-Frames können Sie entweder den MSS-Wert des TCP-Profils nstcp_default_profile ändern oder ein benutzerdefiniertes TCP-Profil erstellen und dessen MSS entsprechend festlegen und dann das benutzerdefinierte TCP-Profil an die gewünschten virtuellen Server und Dienste binden.
    - Der standardmäßige MSS-Wert eines beliebigen TCP-Profils ist 1460.

CLI-Verfahren

So legen Sie die MTU einer Schnittstelle mit der CLI fest:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- set interface <id> -mtu <positive_integer>
- show interface <id>

Beispiel:

```
1 > set interface 10/1  - mtu 9000
2 Done
3 <!--NeedCopy-->
```

So stellen Sie die MTU eines Kanals mit der CLI ein:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- set channel <id> -mtu <positive_integer>
- show channel <id>

Beispiel:

```
> set channel LA/1  - mtu 9000
Done
<!--NeedCopy-->
```

So legen Sie die MTU eines VLAN mit der CLI fest:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add vlan <id> -mtu <positive_integer>
- show vlan <id>

Beispiel:

```
> set vlan 20  - mtu 9000
Done
<!--NeedCopy-->
```

GUI-Verfahren

So legen Sie die MTU einer Schnittstelle mit der GUI fest:

Navigieren Sie zu System > Netzwerk > Schnittstellen, öffnen Sie die Schnittstelle und legen Sie den Parameter Maximale Übertragungseinheit fest.

So stellen Sie die MTU eines Kanals mit der GUI ein:

Navigieren Sie zu System > Netzwerk > Kanäle, öffnen Sie den Kanal und stellen Sie den Parameter Maximale Übertragungseinheit ein.

So legen Sie die MTU eines VLAN mit der GUI fest:

Navigieren Sie zu System > Netzwerk > VLANs, öffnen Sie das VLAN und legen Sie den Parameter Maximale Übertragungseinheit fest.

Anwendungsfall 1 — Jumbo-zu-Jumbo-Setup

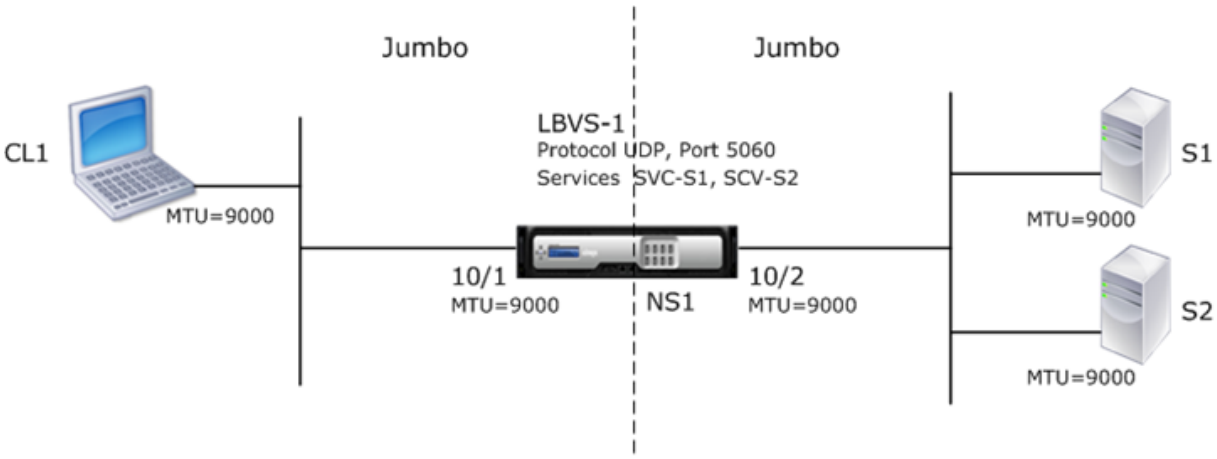
October 5, 2021

Betrachten Sie ein Beispiel für ein Jumbo-zu-Jumbo-Setup, bei dem SIP-Lastenausgleichsserver LBVS-1, der auf der Citrix ADC Appliance NS1 konfiguriert ist, zum Lastenausgleich des SIP-Datenverkehrs über die Server S1 und S2 verwendet wird. Die Verbindung zwischen Client CL1 und NS1 und die Verbindung zwischen NS1 und den Servern unterstützen Jumbo-Frames.

Schnittstelle 10/1 von NS1 empfängt oder sendet Datenverkehr vom oder zum Client CL1. Schnittstelle 10/2 von NS1 empfängt oder sendet Datenverkehr vom oder zum Server S1 oder S2. Die Schnittstellen 10/1 und 10/2 von NS1 sind Teil von VLAN 10 bzw. VLAN 20.

Für die Unterstützung von Jumbo-Frames ist die MTU unter NS1 für die Schnittstellen 10/1, 10/2 und VLANs VLAN 10, VLAN 20 auf 9216 eingestellt.

Alle anderen Netzwerkgeräte, einschließlich CL1, S1, S2, sind in diesem Setup-Beispiel auch für die Unterstützung von Jumbo-Frames konfiguriert.



In der folgenden Tabelle sind die im Beispiel verwendeten Einstellungen aufgeführt.

Entität	Name	Details
IP-Adresse des Clients CL1	-	192.0.2.10
IP-Adresse der Server	S1	198.51.100.19
	S2	198.51.100.20
SNIP-Adresse auf NS1		198.51.100.18
MTU für Schnittstellen und VLANs auf NS1 angegeben	10/1	9000
	10/2	9000
	VLAN 10	9000
	VLAN 20	9000

Entität	Name	Details
Dienste auf NS1, die Server darstellen	SVC-S1	**IP-Adresse:** 198.51.100.19, **Protokoll:** SIP, **Port:** 5060
	SVC-S2	**IP-Adresse:** 198.51.100.20, **Protokoll:** SIP, **Port:** 5060
Lastenausgleich virtueller Server auf VLAN 10	LBVS-1	**IP-Adresse:** 203.0.113.15, **Protokoll:** SIP, **Port:** 5060, **Gebundene Dienste:** SVC-S1, SVC-S2

Im Folgenden ist der Datenverkehr von CL1 Anforderung an NS1:

1. CL1 erstellt eine 20000-Byte-SIP-Anforderung zum Senden an LBVS-1 von NS1.
2. CL1 sendet die Anforderungsdaten in IP-Fragmenten an LBVS-1. Die Größe jedes IP-Fragments ist entweder gleich oder kleiner als die MTU (9000), die auf der Schnittstelle festgelegt ist, von der CL1 diese Fragmente an NS1 sendet.
    - Größe des ersten IP-Fragments = [IP-Header + UDP-Header + SIP-Datensegment] = [20 + 8 + 8972] = 9000
    - Größe des zweiten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 8980] = 9000
    - Größe des letzten IP-Fragment=[IP-Header + SIP-Datensegment] = [20 + 2048] = 2068
3. NS1 empfängt die IP-Fragmente der Anforderung an Schnittstelle 10/1. NS1 akzeptiert diese Fragmente, da die Größe jedes dieser Fragmente gleich oder kleiner als die MTU (9000) der Schnittstelle 10/1 ist.
4. NS1 setzt diese IP-Fragmente wieder zusammen, um die 20000-Byte-SIP-Anforderung zu bilden. NS1 verarbeitet diese Anforderung.
5. Der Lastausgleichsalgorithmus von LBVS-1 wählt Server S1 aus.
6. NS1 sendet die Anforderungsdaten in IP-Fragmenten an S1. Die Größe jedes IP-Fragments ist entweder gleich oder kleiner als die MTU (9000) der Schnittstelle 10/2, von der NS1 diese Fragmente an S1 sendet. Die IP-Pakete werden mit einer SNIP-Adresse von NS1 bezogen.
    - Größe des ersten IP-Fragments = [IP-Header + UDP-Header + SIP-Datensegment] = [20 + 8 + 8972] = 9000
    - Größe des zweiten IP-Fragments =[IP-Header + SIP-Datensegment] =[20 + 8980] = 9000
    - Größe des letzten IP-Fragment=[IP-Header + SIP-Datensegment] =[20 + 2048] = 2068

Im Folgenden ist der Verkehrsfluss der Antwort von S1 auf CL1 in diesem Beispiel:

1. Server S1 erstellt eine 30000-Byte-SIP-Antwort, die an die SNIP-Adresse von NS1 gesendet wird.

2. S1 sendet die Antwortdaten in IP-Fragmenten an die SNIP-Adresse von NS1. Die Größe jedes IP-Fragments ist entweder gleich oder kleiner als die MTU (9000), die auf der Schnittstelle festgelegt ist, von der S1 diese Fragmente an NS1 sendet.
    - Größe des ersten IP-Fragments = [IP-Header + UDP-Header + SIP-Datensegment] = [20 + 8 + 8972] = 9000
    - Größe des zweiten und dritten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 8980] = 9000
    - Größe des letzten IP-Fragment=[IP-Header + SIP-Datensegment] = [20 + 3068] = 3088
3. NS1 empfängt die Antwort-IP-Fragmente an Schnittstelle 10/2. NS1 akzeptiert diese Fragmente, da die Größe jedes Fragments gleich oder kleiner als die MTU (9000) der Schnittstelle 10/2 ist.
4. NS1 setzt diese IP-Fragmente wieder zusammen, um die 30000-Byte SIP-Antwort zu bilden. NS1 verarbeitet diese Antwort.
5. NS1 sendet die Antwortdaten in IP-Fragmenten an CL1. Die Größe jedes IP-Fragments ist entweder gleich oder kleiner als die MTU (9000) der Schnittstelle 10/1, von der NS1 diese Fragmente an CL1 sendet. Die IP-Fragmente werden mit der IP-Adresse von LBVS-1 bezogen.
    - Größe des ersten IP-Fragments = [IP-Header + UDP-Header + SIP-Datensegment] = [20 + 8 + 8972] = 9000
    - Größe des zweiten und dritten IP-Fragments = [IP-Header + SIP-Datensegment] = [20 + 8980] = 9000
    - Größe des letzten IP-Fragment=[IP-Header + SIP-Datensegment] =[20 + 3068] = 3088

Konfigurationsaufgaben

In der folgenden Tabelle sind die Tasks, Citrix ADC Befehle und Beispiele für die Erstellung der erforderlichen Konfiguration auf der Citrix ADC-Appliance aufgeführt.

Aufgabe	Citrix ADC Befehlssyntax	Beispiel
Stellen Sie die MTU der gewünschten Schnittstellen zur Unterstützung von Jumbo-Frames ein	set interface <id> -mtu <positive_integer>, show interface <id>	set int 10/1 -mtu 9000 set int 10/2 -mtu 9000
Erstellen Sie VLANs und legen Sie die MTU der gewünschten VLANs für die Unterstützung von Jumbo-Frames fest	add vlan <id> -mtu <positive_integer>, show vlan <id>	add vlan 10 -mtu 9000 add vlan 20 -mtu 9000

Aufgabe	Citrix ADC Befehlssyntax	Beispiel
Schnittstellen an VLANs binden	bind vlan <id> -ifnum <interface_name>, show vlan <id>	bind vlan 10 -ifnum 10/1 bind vlan 20 -ifnum 10/2
Hinzufügen einer SNIP-Adresse	add ns ip <IPAddress> <netmask> -type SNIP, show ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP
Erstellen von Diensten, die SIP-Server darstellen	add service <serviceName> <ip> SIP_UDP <port>, show service <name>	add service SVC-S1 198.51.100.19 SIP_UDP 5060 add service SVC-S2 198.51.100.20 SIP_UDP 5060
Erstellen Sie virtuelle SIP-Lastausgleichsserver und binden Sie die Dienste an sie	add lb vserver <name> SIP_UDP <ip> <port> bind lb vserver <vserverName> <serviceName>, show lb vserver <name>	add lb vserver LBVS-1 SIP_UDP 203.0.113.15 5060 bind lb vserver LBVS-1 SVC-S1 bind lb vserver LBVS-1 SVC-S2
Speichern der Konfiguration	save ns config, show ns config	

Anwendungsfall 2 — Nicht-Jumbo-zu-Jumbo-Setup

October 5, 2021

Betrachten Sie ein Beispiel für ein reguläres Jumbo-Setup, bei dem der Lastenausgleich des virtuellen Servers LBVS-1, der auf einer Citrix ADC Appliance NS1 konfiguriert ist, zum Lastenausgleich zwischen den Servern S1 und S2 verwendet wird. Die Verbindung zwischen Client CL1 und NS1 unterstützt reguläre Frames, und die Verbindung zwischen NS1 und den Servern unterstützt Jumbo-Frames.

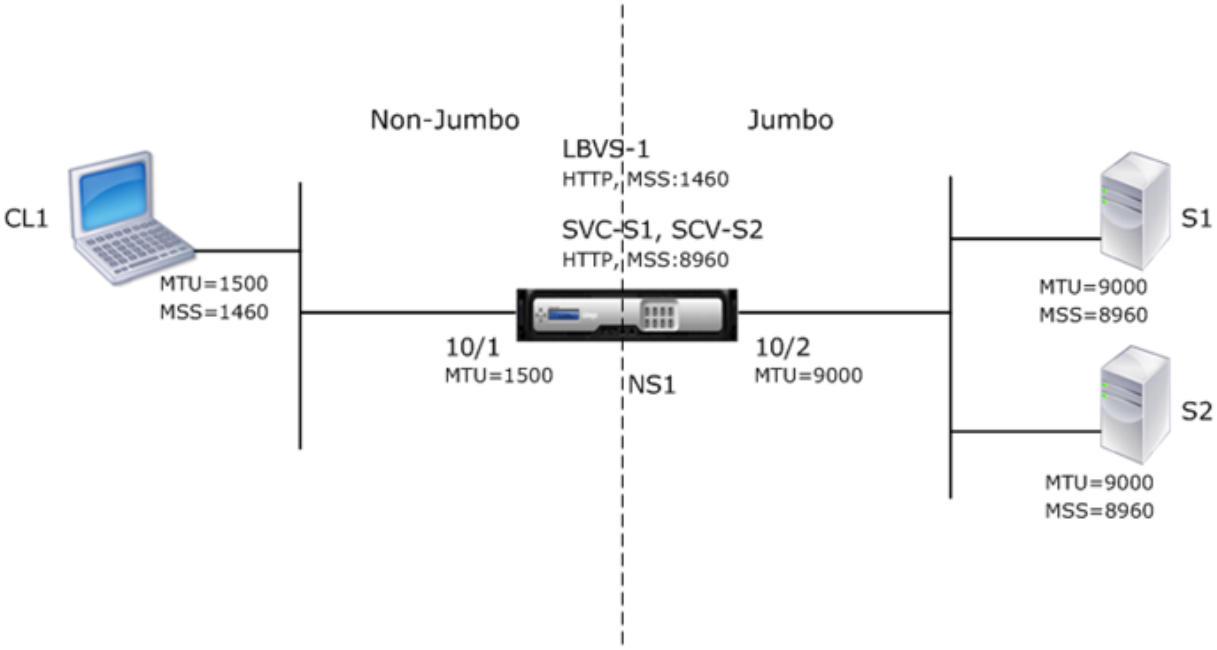
Schnittstelle 10/1 von NS1 empfängt oder sendet Datenverkehr vom oder zum Client CL1. Schnittstelle 10/2 von NS1 empfängt oder sendet Datenverkehr vom oder zum Server S1 oder S2.

Die Schnittstellen 10/1 und 10/2 von NS1 sind Teil von VLAN 10 bzw. VLAN 20. Um nur reguläre Frames zwischen CL1 und NS1 zu unterstützen, wird die MTU auf den Standardwert 1500 für Schnittstelle 10/1 und VLAN 10 gesetzt.

Für die Unterstützung von Jumbo-Frames zwischen NS1 und den Servern ist die MTU für die Schnittstelle 10/2 und VLAN 20 auf 9000 eingestellt. Server und alle anderen Netzwerkgeräte zwischen NS1 und den Servern sind ebenfalls für die Unterstützung von Jumbo-Frames konfiguriert.

Da HTTP-Datenverkehr auf TCP basiert, werden MSS an jedem Endpunkt für die Unterstützung von Jumbo-Frames entsprechend festgelegt.

- Zur Unterstützung von Jumbo-Frames für die Verbindung zwischen einer SNIP-Adresse von NS1 und S1 oder S2 wird der MSS auf NS1 entsprechend in einem benutzerdefinierten TCP-Profil festgelegt, das an die Dienste (SVC-S1 und SVC-S1) gebunden ist, die S1 und S2 auf NS1 darstellen.
- Um nur reguläre Frames für die Verbindung zwischen CL1 und dem virtuellen Server LBVS-1 von NS1 zu unterstützen, wird das standardmäßige TCP-Profil nstcp_default_profile verwendet, das standardmäßig an LBVS-1 gebunden ist und der MSS auf den Standardwert 1460 festgelegt ist.



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt.

Entität	Name	Details
IP-Adresse des Clients CL1		192.0.2.10
IP-Adresse der Server	S1	198.51.100.19
	S2	198.51.100.20
SNIP-Adresse auf NS1		198.51.100.18
MTU für Schnittstellen und VLANs auf NS1 angegeben	10/1	1500
	10/2	9000
	VLAN 10	1500
	VLAN 20	9000

Entität	Name	Details
Standard-TCP-Profil	nstcp_default_profile	MSS:1460
Benutzerdefiniertes TCP-Profil	NS1-SERVERS-JUMBO	MSS: 8960
Dienste auf NS1, die Server darstellen	SVC-S1	IP-Adresse: 198.51.100.19, Protokoll: HTTP, Port: 80, TCP-Profil: NS1-SERVERS-JUMBO (MSS: 8960)
	SVC-S2	IP-Adresse: 198.51.100.20, Protokoll: HTTP, Port: 80, TCP-Profil: NS1-SERVERS-JUMBO (MSS: 8960)
Lastenausgleich virtueller Server auf VLAN 10	LBVS-1	IP-Adresse = 203.0.113.15, Protokoll: HTTP, Port:80, Gebundene Dienste: SVC-S1, SVC-S2, TCP-Profil: nstcp_default_profile (MSS: 1460)

Im Folgenden ist der Datenfluss von CL1 Anforderung an S1 in diesem Beispiel:

1. Client CL1 erstellt eine 200-Byte-HTTP-Anforderung zum Senden an den virtuellen Server LBVS-1 von NS1.
2. CL1 öffnet eine Verbindung zu LBVS-1 von NS1. CL1 und NS1 tauschen beim Herstellen der Verbindung ihre jeweiligen TCP-MSS-Werte aus.
3. Da NS1 MSS größer ist als die HTTP-Anforderung, CL1 sendet die Anforderungsdaten in einem einzigen IP-Paket an NS1.

   Größe des Anforderungspakets = [IP-Header + TCP-Header + TCP-Anfrage] = [20 + 20 + 200] = 240
4. NS1 empfängt das Anforderungspaket an der Schnittstelle 10/1 und verarbeitet dann die HTTP-Anforderungsdaten im Paket.
5. Der Lastausgleichsalgorithmus von LBVS-1 wählt Server S1 aus, und NS1 öffnet eine Verbindung zwischen einer seiner SNIP-Adressen und S1. NS1 und CL1 tauschen beim Herstellen der Verbindung ihre jeweiligen TCP-MSS-Werte aus.

6. Da der MSS von S1 größer ist als die HTTP-Anforderung, sendet NS1 die Anforderungsdaten in einem einzigen IP-Paket an S1.

   Größe des Anforderungspakets = [IP-Header + TCP-Header + [TCP-Anforderung][20 + 20 + 200] = 240

Es folgt der Verkehrsfluss von S1 Antwort auf CL1 in diesem Beispiel:

1. Server S1 erstellt eine 18000-Byte-HTTP-Antwort, die an die SNIP-Adresse von NS1 gesendet wird.
2. S1 segmentiert die Antwortdaten in Vielfaches von NS1 MSS und sendet diese Segmente in IP-Paketen an NS1. Diese IP-Pakete werden von der IP-Adresse von S1 bezogen und an die SNIP-Adresse von NS1 bestimmt.
   - Größe der ersten beiden Pakete = [IP-Header + TCP-Header + (TCP-Segment = MSS-Größe von NS1)] = [20 + 20 + 8960] = 9000
   - Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 2080] = 2120
3. NS1 empfängt die Antwortpakete an Schnittstelle 10/2.
4. Aus diesen IP-Paketen baut NS1 alle TCP-Segmente zusammen, um die HTTP-Antwortdaten von 18000 Byte zu bilden. NS1 verarbeitet diese Antwort.
5. NS1 segmentiert die Antwortdaten in Vielfaches von CL1 MSS und sendet diese Segmente in IP-Paketen, von Schnittstelle 10/1, an CL1. Diese IP-Pakete werden von der IP-Adresse von LBVS-1 bezogen und an die IP-Adresse von CL1 bestimmt.
   - Größe aller Pakete mit Ausnahme des letzten = [IP-Header + TCP-Header + (TCP Payload=CL1s MSS-Größe)] = [20 + 20 + 1460] = 1500
   - Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 480] = 520

Konfigurationsaufgaben

In der folgenden Tabelle sind die Tasks, Citrix ADC Befehle und Beispiele für die Erstellung der erforderlichen Konfiguration auf der Citrix ADC-Appliance aufgeführt.

Aufgaben	CLI-Syntax	Beispiele
Stellen Sie die MTU der gewünschten Schnittstellen zur Unterstützung von Jumbo-Frames ein	set interface <id> -mtu <positive_integer>, show interface <id>	set int 10/1 -mtu 1500 set int 10/2 -mtu 9000

Aufgaben	CLI-Syntax	Beispiele
Erstellen Sie VLANs und legen Sie die MTU der gewünschten VLANs für die Unterstützung von Jumbo-Frames fest	add vlan <id> -mtu <positive_integer>, show vlan <id>	add vlan 10 -mtu 1500 add vlan 20 -mtu 9000
Schnittstellen an VLANs binden	bind vlan <id> -ifnum <interface_name>, show vlan <id>	bind vlan 10 -ifnum 10/1 bind vlan 20 -ifnum 10/2
Hinzufügen einer SNIP-Adresse	add ns ip <IPAddress> <netmask> -type SNIP, show ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP
Erstellen von Diensten, die HTTP-Server darstellen	add service <serviceName> <ip> HTTP <port>, show service <name>	add service SVC-S1 198.51.100.19 http 80, add service SVC-S2 198.51.100.20 http 80
Erstellen Sie virtuelle HTTP-Lastausgleichsserver und binden Sie die Dienste an sie	add lb vserver <name> HTTP <ip> <port>, bind lb vserver <vserverName> <serviceName>, show lb vserver <name>	add lb vserver LBVS-1 http 203.0.113.15 80, bind lb vserver LBVS-1 SVC-S1, bind lb vserver LBVS-1 SVC-S2
Erstellen eines benutzerdefinierten TCP-Profils und Festlegen des MSS für die Unterstützung von Jumbo-Frames	add tcpProfile <name> -mss <positive_integer>, show tcpProfile <name>	add tcpprofile NS1-SERVERS-JUMBO -mss 8960
Binden Sie das benutzerdefinierte TCP-Profil an die gewünschten Dienste	set service <Name> -tcpProfileName <string>, show service <name>	set service SVC-S1 -tcpProfileName NS1-SERVERS-JUMBO, set service SVC-S2 -tcpProfileName NS1-SERVERS-JUMBO
Speichern der Konfiguration	save ns config, show ns config	

Anwendungsfall 3 — Koexistenz von Jumbo- und Nicht-Jumbo-Flüssen auf demselben Satz von Schnittstellen

October 5, 2021

Betrachten Sie ein Beispiel, in dem virtuelle Server mit Lastenausgleich LBVS-1 und LBVS-2 auf der Citrix ADC Appliance NS1 konfiguriert sind. LBVS-1 wird zum Lastenausgleich von HTTP-Datenverkehr über Server S1 und S2 verwendet, und LBVS-2 wird zum Lastenausgleich von Datenverkehr über Server S3 und S4 verwendet.

CL1 befindet sich auf VLAN 10, S1 und S2 sind auf VLAN20, CL2 auf VLAN 30 und S3 und S4 auf VLAN 40. VLAN 10 und VLAN 20 unterstützen Jumbo-Frames, und VLAN 30 und VLAN 40 unterstützen nur normale Frames.

Mit anderen Worten, die Verbindung zwischen CL1 und NS1 und die Verbindung zwischen NS1 und Server S1 oder S2 unterstützen Jumbo-Frames. Die Verbindung zwischen CL2 und NS1 und die Verbindung zwischen NS1 und Server S3 oder S4 unterstützen nur reguläre Frames.

Schnittstelle 10/1 von NS1 empfängt oder sendet Datenverkehr von oder an Clients. Schnittstelle 10/2 von NS1 empfängt oder sendet Datenverkehr von oder an die Server.

Schnittstelle 10/1 ist sowohl an VLAN 10 als auch VLAN 30 als getaggte Schnittstelle gebunden, und Schnittstelle 10/2 ist sowohl an VLAN 20 als auch VLAN 40 als getaggte Schnittstelle gebunden.

Für die Unterstützung von Jumbo-Frames ist die MTU für die Schnittstellen 10/1 und 10/2 auf 9216 eingestellt.

Bei NS1 ist die MTU für VLAN 10 auf 9000 und VLAN 20 für Jumbo-Frames eingestellt, und die MTU ist auf den Standardwert 1500 für VLAN 30 und VLAN 40 für die Unterstützung nur regulärer Frames eingestellt.

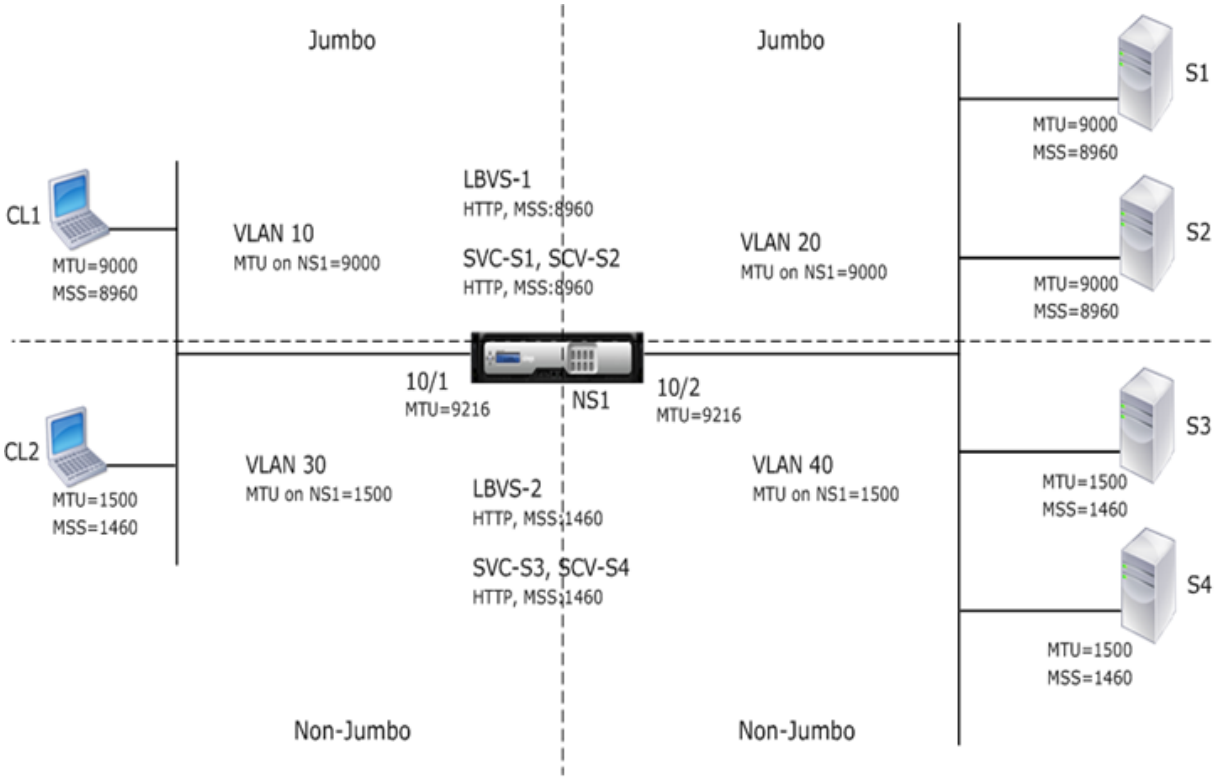
Die effektive MTU auf einer Citrix ADC Schnittstelle für VLAN-getaggte Pakete ist von der MTU der Schnittstelle oder der MTU des VLAN, je nachdem, welcher Wert niedriger ist. Beispiel:

- Die MTU der Schnittstelle 10/1 ist 9216. Die MTU von VLAN 10 ist 9000. Auf der Schnittstelle 10/1 ist die MTU von VLAN 10 getaggten Paketen 9000.
- Die MTU der Schnittstelle 10/2 ist 9216. Die MTU von VLAN 20 ist 9000. Auf der Schnittstelle 10/2 ist die MTU von VLAN 20 getaggten Paketen 9000.
- Die MTU der Schnittstelle 10/1 ist 9216. Die MTU von VLAN 30 ist 1500. Auf der Schnittstelle 10/1 beträgt die MTU von VLAN 30 getaggten Paketen 1500.
- Die MTU der Schnittstelle 10/2 ist 9216. Die MTU von VLAN 40 ist 1500. Auf der Schnittstelle 10/2 ist die MTU von VLAN 40 getaggten Paketen 9000.

CL1, S1, S2 und alle Netzwerkgeräte zwischen CL1 und S1 oder S2 sind für Jumbo-Frames konfiguriert.

Da HTTP-Datenverkehr auf TCP basiert, werden MSS an jedem Endpunkt für die Unterstützung von Jumbo-Frames entsprechend festgelegt.

- Für die Verbindung zwischen CL1 und dem virtuellen Server LBVS-1 von NS1 wird der MSS auf NS1 in einem TCP-Profil festgelegt, das dann an LBVS-1 gebunden ist.
- Für die Verbindung zwischen einer SNIP-Adresse von NS1 und S1 wird der MSS auf NS1 in einem TCP-Profil festgelegt, das dann an den Dienst (SVC-S1) gebunden ist, der S1 auf NS1 darstellt.



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt: Jumbo-Frames Anwendungsfall 3 Beispieleinstellungen.

Im Folgenden ist der Verkehrsfluss von CL1 Anforderung an S1:

1. Client CL1 erstellt eine 20000-Byte-HTTP-Anforderung zum Senden an den virtuellen Server LBVS-1 von NS1.
2. CL1 öffnet eine Verbindung zu LBVS-1 von NS1. CL1 und NS1 tauschen ihre TCP-MSS-Werte aus, während die Verbindung hergestellt wird.
3. Da der MSS-Wert von NS1 kleiner ist als die HTTP-Anforderung, segmentiert CL1 die Anforderungsdaten in Vielfaches von NS1 MSS und sendet diese Segmente in IP-Paketen, die als VLAN 10 gekennzeichnet sind, an NS1.
    - Größe der ersten beiden Pakete = [IP-Header + TCP-Header + (TCP-Segment = NS1 MSS)] = [20 + 20 + 8960] = 9000
    - Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 2080] = 2120

4. NS1 empfängt diese Pakete an Schnittstelle 10/1. NS1 akzeptiert diese Pakete, da die Größe dieser Pakete gleich oder kleiner ist als die effektive MTU (9000) der Schnittstelle 10/1 für VLAN 10-getaggte Pakete.
5. Aus den IP-Paketen baut NS1 alle TCP-Segmente zusammen, um die 20000-Byte-HTTP-Anforderung zu bilden. NS1 verarbeitet diese Anforderung.
6. Der Lastausgleichsalgorithmus von LBVS-1 wählt Server S1 aus, und NS1 öffnet eine Verbindung zwischen einer seiner SNIP-Adressen und S1. NS1 und CL1 tauschen beim Herstellen der Verbindung ihre jeweiligen TCP-MSS-Werte aus.
7. NS1 segmentiert die Anforderungsdaten in Vielfaches des MSS von S1 und sendet diese Segmente in IP-Paketen, die als VLAN 20 an S1 gekennzeichnet sind.
    - Größe der ersten beiden Pakete = [IP-Header + TCP-Header + (TCP PayLoad=S1 MSS)][20 + 20 + 8960] = 9000
    - Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 2080] = 2120

Im Folgenden ist der Verkehrsfluss von S1 Antwort auf CL1:

1. Server S1 erstellt eine 30000-Byte-HTTP-Antwort, die an die SNIP-Adresse von NS1 gesendet wird.
2. S1 segmentiert die Antwortdaten in Vielfaches von NS1 MSS und sendet diese Segmente in IP-Paketen, die als VLAN 20 gekennzeichnet sind, an NS1. Diese IP-Pakete werden von der IP-Adresse von S1 bezogen und an die SNIP-Adresse von NS1 bestimmt.
    - Größe des ersten drei Pakets = [IP-Header + TCP-Header + (TCP-Segment = MSS-Größe von NS1)][20 + 20 + 8960] = 9000
    - Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 3120] = 3160
3. NS1 empfängt die Antwortpakete an Schnittstelle 10/2. NS1 akzeptiert diese Pakete, da ihre Größe gleich oder kleiner als der effektive MTU-Wert (9000) der Schnittstelle 10/2 für VLAN 20-getaggte Pakete ist.
4. Aus diesen IP-Paketen baut NS1 alle TCP-Segmente zusammen, um die 30000-Byte-HTTP-Antwort zu bilden. NS1 verarbeitet diese Antwort.
5. NS1 segmentiert die Antwortdaten in Vielfaches von CL1 MSS und sendet diese Segmente in IP-Paketen, die als VLAN 10 gekennzeichnet sind, von Schnittstelle 10/1 an CL1. Diese IP-Pakete werden von der IP-Adresse von LBVS bezogen und zur IP-Adresse von CL1 bestimmt.
    - Größe des ersten drei Pakets = [IP-Header + TCP-Header + [(TCP PayLoad=MSS-Größe von CL1)][20 + 20 + 8960] = 9000
    - Größe des letzten Pakets = [IP-Header + TCP-Header + (verbleibendes TCP-Segment)] = [20 + 20 + 3120] = 3160

Konfigurationsaufgaben

In der folgenden Tabelle werden Aufgaben, Befehle und Beispiele zum Erstellen der erforderlichen Konfiguration auf der Citrix ADC Appliance aufgeführt: Jumbo-Frames Anwendungsfall 3 Konfigurationsaufgaben.

Citrix ADC Unterstützung für die Bereitstellung von Microsoft Direct Access

December 7, 2021

Microsoft Direct Access ist eine Technologie, die es Remote-Benutzern ermöglicht, nahtlos und sicher mit den internen Netzwerken des Unternehmens zu verbinden, ohne dass eine separate VPN-Verbindung hergestellt werden muss. Im Gegensatz zu VPN-Verbindungen, die Benutzereingriffe zum Öffnen und Schließen von Verbindungen erfordern, stellt ein Direct Access-fähiger Client automatisch eine Verbindung zu den internen Netzwerken des Unternehmens her, wenn der Client eine Verbindung zum Internet herstellt.

ManageOut ist eine Microsoft Direct Access-Funktion, mit der Administratoren innerhalb des Unternehmensnetzwerks eine Verbindung zu Direct Access-Clients außerhalb des Netzwerks herstellen und diese verwalten können (z. B. Verwaltungsaufgaben wie das Planen von Dienstaktualisierungen und die Bereitstellung von Remote-Support.

In einer Direct Access-Bereitstellung bieten Citrix ADC Appliances hohe Verfügbarkeit, Skalierbarkeit, hohe Leistung und Sicherheit. Die Citrix ADC Load Balancing-Funktionalität sendet Clientdatenverkehr über den am besten geeigneten Server. Die Appliances können auch ManageOut-Datenverkehr über den richtigen Pfad weiterleiten, um den Client zu erreichen.

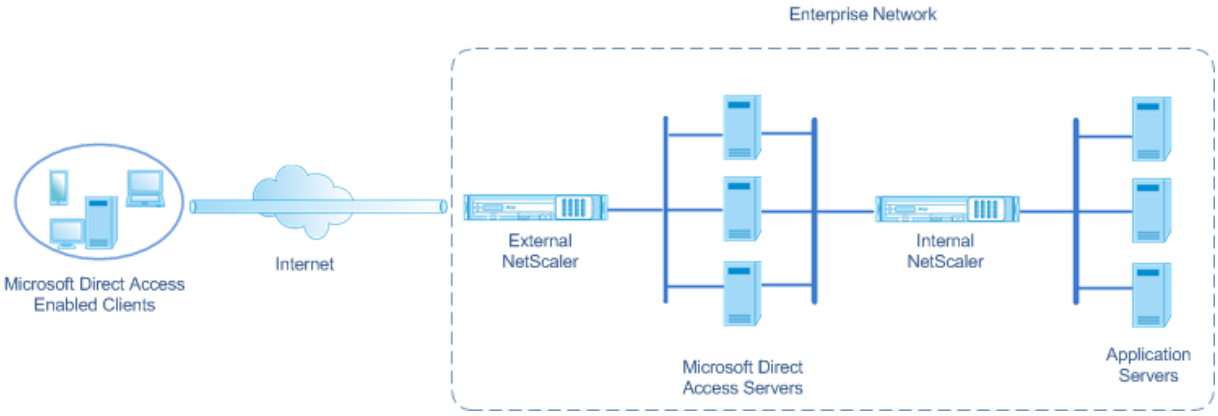
Architektur

Die Architektur einer Microsoft Direct Access-Bereitstellung besteht aus Direct Access-fähigen Clients, Direct Access-Servern, Anwendungsservern sowie internen und externen Citrix ADC Appliances. Clients stellen über einen Direct Access-Server eine Verbindung zu einem Anwendungsserver her. Eine externe Citrix ADC Appliance gleicht den Clientdatenverkehr zu einem Direct Access-Server aus, und eine interne Citrix ADC Appliance leitet den Clientdatenverkehr vom Direct Access-Server an den Zielanwendungsserver weiter. Direct Access wird verwendet, um den IPv6-Datenverkehr des Clients über das IPv4-Netzwerk zu tunneln. Ein virtueller IPv4-Server für Lastenausgleich auf der externen Citrix ADC Appliance gleicht den Tunnelverkehr des Clients zu einem der Direct Access-Server aus. Der Direct Access-Server extrahiert die IPv6-Pakete aus den IPv4-Paketen des empfangenen Clients und sendet sie über die interne Citrix ADC Appliance an den Zielanwendungsserver. Die interne Citrix

ADC Appliance verfügt über Weiterleitungssitzungsregeln, bei denen die Option Quellrouten Cache aktiviert ist, um Layer 2- und Layer 3-Verbindungsinformationen über den Datenverkehr des Clients vom Direct Access Server zu speichern. Die Citrix ADC Appliance speichert die folgenden Layer-2- und Layer-3-Informationen in einer Tabelle, die als Quell-Route-Cache-Tabelle bezeichnet wird:

- Quell-IP-Adresse des empfangenen Pakets
- MAC-Adresse des Direct Access-Servers, der das Paket gesendet hat
- VLAN-ID der Citrix ADC Appliance, die das Paket empfangen hat
- Schnittstellen-ID der Citrix ADC Appliance, die das Paket empfangen hat

Die Citrix ADC Appliance verwendet die Informationen in der Quellroute Cachetabelle für die Weiterleitung einer Antwort an denselben Direct Access-Server, da sie über die Tunnelinformationen verfügt, um den Client zu erreichen. Außerdem verwendet die Interne Appliance die Quellroute Cachetabelle, um den Verwaltungsdatenverkehr des Anwendungsservers an den entsprechenden Direct Access-Server weiterzuleiten, um einen bestimmten Client zu erreichen.



Konfigurieren der internen Citrix ADC Appliance in einer Microsoft Direct Access-Bereitstellung

Konfigurieren Sie die Weiterleitungssitzungsregeln, um die interne Citrix ADC Appliance für die Weiterleitung der Antwort eines Anwendungsservers und die Verwaltung des Datenverkehrs an das entsprechende Direct Access Gateway zu konfigurieren. Legen Sie in jeder Regel den Parameter sourceroutecache auf Enabled fest.

So erstellen Sie eine Weiterleitungssitzungsregel mithilfe der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add ForwardingSession** <name>((<network>[]<netmask>) | **-acl6name** <string>| **-aclname** <string>) **-sourceroutecache** (**AKTIVIERT** |DEAKTIVIERT**]
- **show forwardingsession** <name>

Beispielkonfiguration:

Im folgenden Beispiel wird die Weiterleitungssitzungsregel MS-DA-FW-1 auf der internen Citrix ADC Appliance erstellt. Die Weiterleitungssitzung speichert Layer-2- und Layer-3-Informationen für alle eingehenden IPv6-Pakete von einem Direct Access-Server, der dem Quell-IPv6-Präfix 2001:DB8::/96 entspricht.

```
> add forwardingSession MS-DA-FW-1 2001:DB8::/96 -sourceroutecache -
    ENABLED
 Done
```

Quell-Route-Cache-Tabelle anzeigen

Sie können die Quell-Route-Cache-Tabelle anzeigen, um unerwünschte Verbindungen zwischen Servern mit Direktzugriff und Anwendungsservern zu überwachen oder zu erkennen.

So zeigen Sie die Quell-Route-Cache-Tabelle mit der Befehlszeilenschnittstelle an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **show sourceroutecachetable**

Beispiel:

```
> show sourceroutecachetable
SOURCEIP            MAC                 VLAN    INTERFACE
2001:DB8:5001:10    56:53:24:3d:02:eb    30        1/2
2001:DB8:5003:30    60:54:35:3e:04:bd    60        1/3
Done
```

Löschen der Quellroute Cachetabelle

Sie können alle Einträge aus der Quellroute Cachetabelle auf einer Citrix ADC Appliance löschen.

So löschen Sie die Quell-Route-Cache-Tabelle mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **flush ns sourceroutecachetable**

Zugriffssteuerungslisten

October 5, 2021

Zugriffssteuerungslisten (Access Control Lists, ACLs) filtern den IP-Datenverkehr und schützen Ihr Netzwerk vor unbefugtem Zugriff. Eine ACL ist eine Reihe von Bedingungen, die vom Citrix ADC ausgewertet werden, um zu bestimmen, ob der Zugriff zugelassen werden soll. Beispielsweise möchte die Finanzabteilung wahrscheinlich nicht zulassen, dass andere Abteilungen, wie Personalabteilung und Dokumentation, auf ihre Ressourcen zugreifen können, und diese Abteilungen möchten den Zugriff auf ihre Daten beschränken.

Wenn der Citrix ADC ein Datenpaket empfängt, vergleicht er die Informationen im Datenpaket mit den in der ACL angegebenen Bedingungen und erlaubt oder verweigert den Zugriff. Der Administrator der Organisation kann ACLs so konfigurieren, dass sie in den folgenden Verarbeitungsmodi funktionieren:

- ALLOW— Verarbeiten des Pakets.
- BRIDGE— Brücken Sie das Paket zum Ziel, ohne es zu verarbeiten. Das Paket wird direkt von Layer 2 und Layer 3 weitergeleitet.
- DENY — Das Paket wird gelöscht.

ACL-Regeln sind die erste Verteidigungsebene auf dem Citrix ADC.

Citrix ADC unterstützt die folgenden Typen von ACLs:

- **Einfache ACLs** filtern Pakete basierend auf ihrer Quell-IP-Adresse und optional ihrem Protokoll, ihrem Zielport oder ihrer Verkehrsdomäne. Jedes Paket, das die in der ACL angegebenen Merkmale aufweist, wird gelöscht.
- **Erweiterte ACLs** filtern Datenpakete basierend auf verschiedenen Parametern wie Quell-IP-Adresse, Quellport, Aktion und Protokoll. Eine erweiterte ACL definiert die Bedingungen, die ein Paket erfüllen muss, damit Citrix ADC das Paket verarbeiten, das Paket überbrücken oder das Paket löschen kann.

Nomenklatur

In den Citrix ADC Benutzeroberflächen beziehen sich die Begriffe einfache ACL und erweiterte ACL auf ACLs, die IPv4-Pakete verarbeiten. Eine ACL, die IPv6-Pakete verarbeitet, wird als einfache ACL6 und erweiterte ACL6 bezeichnet. Bei der Diskussion beider Typen werden in dieser Dokumentation manchmal beide als einfache ACLs oder erweiterte ACLs bezeichnet.

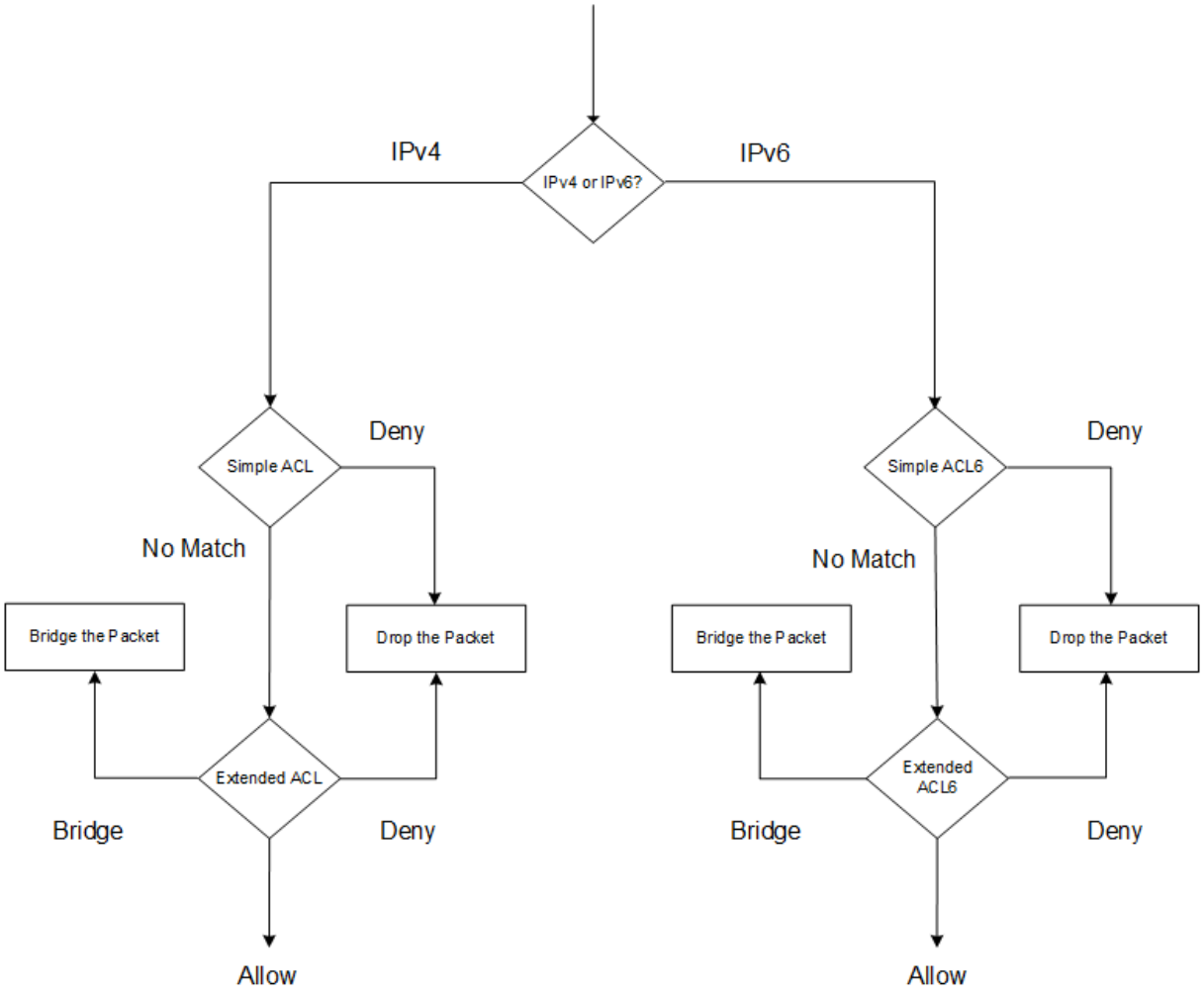
ACL-Priorität

Wenn sowohl einfache als auch erweiterte ACLs konfiguriert sind, werden eingehende Pakete zuerst mit den einfachen ACLs verglichen.

Der Citrix ADC bestimmt zunächst, ob es sich bei dem eingehenden Paket um ein IPv4- oder ein IPv6-Paket handelt, und vergleicht dann die Eigenschaften des Pakets mit einfachen ACLs oder einfachen ACL6s. Wenn eine Übereinstimmung gefunden wird, wird das Paket gelöscht. Wenn keine Übereinstimmung gefunden wird, wird das Paket mit erweiterten ACLs oder erweiterten ACL6s verglichen.

Wenn dieser Vergleich zu einer Übereinstimmung führt, wird das Paket wie in der ACL angegeben behandelt. Das Paket kann überbrückt, gelöscht oder erlaubt werden. Wenn keine Übereinstimmung gefunden wird, ist das Paket zulässig.

Abbildung 1. Einfache und erweiterte ACLs Flow Sequenz



Einfache ACLs und einfache ACL6s

October 5, 2021

Eine einfache ACL oder einfache ACL6 verwendet wenige Parameter und kann nur zum Löschen von IP-Paketen konfiguriert werden. Pakete können basierend auf ihrer Quell-IP-Adresse und optional ihres Protokolls, ihres Zielports oder ihrer Verkehrsdomäne gelöscht werden.

Wenn Sie eine einfache ACL oder eine einfache ACL6 erstellen, können Sie eine Time to Live (TTL) in Sekunden angeben, nach der die ACL abläuft. ACLs mit TTLs werden beim Speichern der Konfigura-

tion nicht gespeichert. Sie können einfache ACLs und einfache ACL6s anzeigen, um ihre Konfiguration zu überprüfen, und Sie können ihre Statistiken anzeigen.

Konfigurieren einfacher ACLs und einfacher ACL6s

Die Konfiguration einer einfachen ACL oder einer einfachen ACL6 auf einem Citrix ADC kann die folgenden Aufgaben umfassen.

- **Erstellen Sie einfache ACLs oder einfache ACL6s**. Erstellen einfacher ACLs oder einfacher ACL6s zum Löschen (Verweigern) von Paketen basierend auf ihrer Quell-IP-Adresse und optional ihrem Protokoll, ihrem Zielport oder ihrer Verkehrsdomäne.
- **Entfernen Sie einfache ACLs oder einfache ACL6s**. Diese ACLs können nach der Erstellung nicht geändert werden. Wenn Sie eine einfache ACL oder eine einfache ACL6 ändern müssen, müssen Sie sie entfernen und eine erstellen.

CLI-Verfahren

So erstellen Sie eine einfache ACL mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 -  ns simpleacl <aclname> DENY -srcIP <ip_addr> [-destPort <port> -
     protocol ( TCP | UDP )] [-TTL <positive_integer>]
2 -  show ns simpleacl [<aclname>]
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add simpleacl rule1 DENY -srcIP 10.102.29.5 -TTL 600
2 Done
3 <!--NeedCopy-->
```

So erstellen Sie eine einfache ACL6 mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 -  add ns simpleacl6 <aclname> DENY - srcIPv6 <ipv6_addr|null> [-
     destPort <port> -protocol ( TCP | UDP )] [-TTL <positive_integer>]
2 -  show ns simpleacl6 [<aclname>]
3 <!--NeedCopy-->
```


Beispiel:

```
1 >  add ns simpleacl6 rule1 DENY  -srcIPv6 3ffe:192:168:215::82 -
     destPort 80 -Protocol TCP -TTL 9000
2  Done
3 <!--NeedCopy-->
```

So entfernen Sie eine einzelne einfache ACL mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **rm ns simpleacl** <aclname>
- **show ns simpleacl**

So entfernen Sie eine einzelne einfache ACL6 mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **rm ns simpleacl6**<aclname>
- **show ns simpleacl6**

So entfernen Sie alle einfachen ACLs mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **clear ns simpleacl**
- **show ns simpleacl**

So entfernen Sie alle einfachen ACL6s mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **clear ns simpleacl6**
- **show ns simpleacl6**

GUI-Verfahren

So erstellen Sie eine einfache ACL mit der GUI:

Navigieren Sie zu **System > Netzwerk > ACLs** und fügen Sie auf der Registerkarte **Einfache ACLs** eine neue einfache ACL hinzu.

So erstellen Sie eine einfache ACL6 mit der GUI:

Navigieren Sie zu **System > Netzwerk > ACLs** und fügen Sie auf der Registerkarte **Einfache ACL6s** eine neue einfache ACL6 hinzu.

So entfernen Sie eine einzelne einfache ACL mit der GUI:

Navigieren Sie zu **System > Netzwerk > ACLs** und löschen Sie auf der Registerkarte **Einfache ACLs** die einfache ACL.

So entfernen Sie eine einzelne einfache ACL6 mit der GUI:

Navigieren Sie zu **System > Netzwerk > ACLs** und löschen Sie auf der Registerkarte **Einfache ACL6s** die einfache ACL6.

So entfernen Sie alle einfachen ACLs mit der GUI:

1. Navigieren Sie zu **System > Netzwerk > ACLs**.
2. Klicken Sie auf der Registerkarte **Einfache ACLs** in der Liste **Aktion** auf **Löschen**.

So entfernen Sie alle einfachen ACL6s mit der GUI:

1. Navigieren Sie zu **System > Netzwerk > ACLs**.
2. Klicken Sie auf der Registerkarte **Einfache ACL6s** in der Liste **Aktion** auf **Löschen**.

Anzeigen einfacher ACL- und einfacher ACL6-Statistiken

Sie können die einfachen ACL-Statistiken (oder einfache ACL6) anzeigen, die die Anzahl der Übereinstimmungen, die Anzahl der Fehler und die Anzahl der konfigurierten einfachen ACLs enthalten.

In der folgenden Tabelle werden die Statistiken beschrieben, die Sie für einfache ACLs und einfache ACL6s anzeigen können.

Statistik	Zeigt an
ACL übereinstimmen	Pakete, die mit einer ACL übereinstimmen
ACL Fehler	Pakete, die keiner ACL entsprechen
ACL-Anzahl	Anzahl der konfigurierten ACLs

CLI-Verfahren

So zeigen Sie einfache ACL-Statistiken mit der Befehlszeilenschnittstelle an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **stat ns simpleacl**

Beispiel:

```
1 > stat ns simpleacl
2
3 SimpleACL Statistics
```



```
4
5                                                Rate (/s)
                                                    Total
6  SimpleACL hits                                       0
                         0
7  SimpleACL misses                                     0
      51872
8  SimpleACLs count                                    --
                         2
9  Done
10 <!--NeedCopy-->
```

So zeigen Sie einfache ACL6-Statistiken mit der CLI an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **stat ns simpleacl6**

GUI-Verfahren

So zeigen Sie einfache ACL-Statistiken mit der GUI an:

Navigieren Sie zu **System** > **Netzwerk** > **ACLs**, und wählen Sie auf der Registerkarte **Einfache ACLs** die ACL aus, und klicken Sie auf **Statistiken**.

So zeigen Sie einfache ACL6-Statistiken mit der GUI an:

Navigieren Sie zu **System > Netzwerk > ACLs**, wählen Sie auf der Registerkarte **Einfache ACL6s** die einfache ACL6 aus und klicken Sie auf **Statistik**.

Aufgebaute Verbindungen beenden

Für eine einfache ACL oder eine einfache ACL6 blockiert Citrix ADC alle neuen Verbindungen, die den in der ACL angegebenen Bedingungen entsprechen. Pakete, die sich auf bestehende Verbindungen beziehen, die vor der Erstellung der ACL eingerichtet wurden, werden nicht blockiert. Um zuvor etablierte Verbindungen zu beenden, die mit einer vorhandenen ACL übereinstimmen, können Sie einen Flush-Vorgang über die CLI oder die GUI ausführen.

Flush kann in folgenden Fällen nützlich sein:

- Sie erhalten eine Liste der IP-Adressen in der Sperrliste und möchten diesen IP-Adressen den Zugriff auf das Citrix ADC vollständig blockieren. In diesem Fall erstellen Sie einfache ACLs oder einfache ACL6s, um neue Verbindungen von diesen IP-Adressen zu blockieren und dann alle vorhandenen Verbindungen zu leeren, die diesen Adressen zugeordnet sind.
- Sie möchten viele Verbindungen von einem bestimmten Netzwerk aus beenden, ohne sich die Zeit zu nehmen, sie einzeln zu beenden.

Voraussetzungen

- Wenn Sie Flush ausführen, durchsucht der Citrix ADC alle seine etablierten Verbindungen und beendet die Verbindungen, die den Bedingungen entsprechen, die in einer der einfachen ACLs angegeben sind, die auf dem ADC konfiguriert sind.
- Wenn Sie planen, mehr als eine einfache ACL zu erstellen und vorhandene Verbindungen zu leeren, die zu einer von ihnen passen, können Sie die Auswirkungen auf die Leistung minimieren, indem Sie zuerst alle einfachen ACLs erstellen und dann nur einmal Flush ausführen.

CLI-Verfahren

So beenden Sie alle etablierten IPv4-Verbindungen, die mit Ihren konfigurierten einfachen ACLs übereinstimmen, mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **flush simpleacl -estSessions**

So beenden Sie alle etablierten IPv6-Verbindungen, die mit Ihren konfigurierten einfachen ACL6s übereinstimmen, mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **flush simpleacl6 -estSessions**

GUI-Verfahren

So beenden Sie alle etablierten IPv4-Verbindungen, die mit Ihren konfigurierten einfachen ACLs übereinstimmen, mit der GUI:

1. Navigieren Sie zu **System > Netzwerk > ACLs**.
2. Klicken Sie auf der Registerkarte **Einfache ACLs** in der Liste **Aktion** auf **Flush**.

So beenden Sie alle etablierten IPv6-Verbindungen, die mit Ihren konfigurierten einfachen ACL6s übereinstimmen, mit der GUI:

1. Navigieren Sie zu **System > Netzwerk > ACLs**.
2. Klicken Sie auf der Registerkarte **Einfache ACL6s** in der Liste **Aktion** auf **Flush**.

Erweiterte ACLs und erweiterte ACL6s

October 5, 2021

Erweiterte ACLs und erweiterte ACL6s bieten Parameter und Aktionen, die mit einfachen ACLs nicht verfügbar sind. Sie können Daten basierend auf Parametern wie Quell-IP-Adresse, Quellport, Aktion und Protokoll filtern. Sie können Aufgaben angeben, um ein Paket zuzulassen, ein Paket zu verweigern oder ein Paket zu überbrücken.

Erweiterte ACLs und ACL6s können nach ihrer Erstellung geändert werden, und Sie können ihre Prioritäten neu nummerieren, um die Reihenfolge anzugeben, in der sie ausgewertet werden.

Hinweis: Wenn Sie sowohl einfache als auch erweiterte ACLs konfigurieren, haben einfache ACLs Vorrang vor erweiterten ACLs.

Die folgenden Aktionen können für erweiterte ACLs und ACL6s ausgeführt werden: Ändern, Anwenden, Deaktivieren, Aktivieren, Entfernen und Umnummerieren (Priorität). Sie können erweiterte ACLs und ACL6s anzeigen, um ihre Konfiguration zu überprüfen, und Sie können ihre Statistiken anzeigen.

Sie können den Citrix ADC so konfigurieren, dass Details für Pakete protokolliert werden, die einer erweiterten ACL entsprechen.

Anwenden erweiterter ACLs und erweiterter ACL6s: Im Gegensatz zu einfachen ACLs und ACL6s funktionieren erweiterte ACLs und ACL6s, die auf dem Citrix ADC erstellt wurden, erst dann, wenn sie angewendet werden. Wenn Sie Änderungen an einer erweiterten ACL oder ACL6 vornehmen, z. B. das Deaktivieren der ACLs, das Ändern einer Priorität oder das Löschen der ACLs, müssen Sie die erweiterten ACLs oder ACL6 erneut anwenden. Sie müssen sie erneut anwenden, nachdem Sie die Protokollierung aktiviert haben. Das Verfahren zum Anwenden erweiterter ACLs oder ACL6s wendet alle ACLs erneut an. Wenn Sie beispielsweise erweiterte ACL-Regeln 1 bis 10 angewendet haben und dann Regel 11 erstellen und anwenden, werden die ersten 10 Regeln neu angewendet.

Wenn eine Sitzung über eine DENY-ACL verfügt, wird diese Sitzung beendet, wenn Sie die ACLs anwenden.

Erweiterte ACLs und ACL6s sind standardmäßig aktiviert. Wenn sie angewendet werden, beginnt der Citrix ADC, eingehende Pakete mit ihnen zu vergleichen. Wenn Sie sie jedoch deaktivieren, werden sie erst verwendet, wenn Sie sie wieder aktivieren, selbst wenn sie erneut angewendet werden.

Neunummerierung der Prioritäten von Extended ACLs und Extended ACL6: Prioritätsnummern bestimmen die Reihenfolge, in der erweiterte ACLs oder ACL6 mit einem Paket abgeglichen werden. Eine ACL mit einer niedrigeren Prioritätsnummer hat eine höhere Priorität. Es wird vor ACLs mit höheren Prioritätsnummern (niedrigere Prioritäten) ausgewertet, und die erste ACL, die mit dem Paket übereinstimmt, bestimmt die auf das Paket angewendete Aktion.

Wenn Sie eine erweiterte ACL oder ACL6 erstellen, weist der Citrix ADC ihm automatisch eine Prioritätsnummer zu, die ein Vielfaches von 10 ist, sofern Sie nichts anderes angeben. Wenn beispielsweise zwei erweiterte ACLs Prioritäten von 20 bzw. 30 haben und Sie möchten, dass eine dritte ACL einen Wert zwischen diesen Zahlen hat, können Sie ihr einen Wert von 25 zuweisen. Wenn Sie später die Reihenfolge beibehalten möchten, in der die ACLs ausgewertet werden, aber ihre Nummerierung auf ein Vielfaches von 10 zurücksetzen möchten, können Sie die Neunummerierungsprozedur verwenden.

Konfigurieren von erweiterten ACLs und Extended ACL6s

Die Konfiguration einer erweiterten ACL oder ACL6 auf einem Citrix ADC besteht aus den folgenden Aufgaben.

- **Erstellen Sie eine erweiterte ACL oder ACL6.** Erstellen Sie eine erweiterte ACL oder ACL6, um ein Paket entweder zuzulassen, zu verweigern oder zu überbrücken. Sie können eine IP-Adresse oder einen Bereich von IP-Adressen angeben, die mit den Quell- oder Ziel-IP-Adressen der Pakete übereinstimmen. Sie können ein Protokoll angeben, das mit dem Protokoll eingehender Pakete übereinstimmt.
- (Optional) **Ändern Sie eine erweiterte ACL oder ACL6**. Sie können erweiterte ACLs oder ACL6s ändern, die Sie zuvor erstellt haben. Oder wenn Sie einen vorübergehend außer Betrieb nehmen möchten, können Sie ihn deaktivieren und später wieder aktivieren.
- **Wenden Sie erweiterte ACLs oder ACL6s**an. Nachdem Sie eine erweiterte ACL oder ACL6 erstellt, geändert, deaktiviert oder erneut aktiviert oder gelöscht haben, müssen Sie die erweiterten ACLs oder ACL6 anwenden, um sie zu aktivieren.
- (Optional) **Nummerieren Sie die Prioritäten von erweiterten ACLs oder ACL6**neu. Wenn Sie ACLs mit Prioritäten konfiguriert haben, die kein Vielfaches von 10 sind und die Nummerierung auf ein Vielfaches von 10 wiederherstellen möchten, verwenden Sie die Neunummerierungsprozedur.

CLI-Verfahren

So erstellen Sie eine erweiterte ACL mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add ns acl** <aclname> <aclaction> [-**srcIP** [<operator>] <srcIPVal>] [-**srcPort** [<operator>] <srcPortVal>] [-**destIP** [<operator>] <destIPVal>] [-**destPort** [<operator>] <destPortVal>] [-**TTL** <positive_integer>] [-**srcMac** <mac_addr>] [(-**protocol** <protocol> [-established]) | -**protocolNumber** <positive_integer>] [-**vlan** <positive_integer>] [-**interface** <interface_name>] [-**icmpType** <positive_integer> [-**icmpCode** <positive_integer>]] [-**priority** <positive_integer>] [-**state** (ENABLED | DISABLED)] [-**logstate** (ENABLED | DISABLED) [-**ratelimit** <positive_integer>]]
- **show ns acl** [<aclName>]

So erstellen Sie eine erweiterte ACL6 mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add ns acl6** <acl6name> <acl6action> [-**srcIPv6** [<operator>] <srcIPv6Val>] [-**srcPort** [<operator>] <srcPortVal>] [-**destIPv6** [<operator>] <destIPv6Val>] [-**destPort** [<operator>] <destPortVal>] [-**TTL** <positive_integer>] [-**srcMac** <mac_addr>] [(-**protocol** <protocol> [-established]) | -**protocolNumber** <positive_integer>] [-**vlan** <positive_integer>] [-**interface**

<interface_name>] [-**icmpType** <positive_integer> [-**icmpCode** <positive_integer>]] [-**priority** <positive_integer>] [-**state** (ENABLED | DISABLED)]

- **show ns acl6** [<aclName>]

So ändern Sie eine erweiterte ACL mit der CLI:

Um eine erweiterte ACL zu ändern, geben Sie den Befehl **set ns acl**, den Namen der erweiterten ACL und die zu ändernden Parameter mit ihren neuen Werten ein.

So ändern Sie eine erweiterte ACL6 mit der CLI:

Um eine erweiterte ACL6 zu ändern, geben Sie den Befehl **set ns acl6**, den Namen des erweiterten ACL6 und die zu ändernden Parameter mit ihren neuen Werten ein.

So deaktivieren oder aktivieren Sie eine erweiterte ACL mit der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- **disable ns acl** <aclname>
- **enable ns acl** <aclname>

So deaktivieren oder aktivieren Sie eine erweiterte ACL6 über die CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- **disable ns acl6** <aclname>
- **enable ns acl6** <aclname>

So wenden Sie erweiterte ACLs mit der CLIan:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **apply ns acls**

So wenden Sie erweiterte ACL6s über die CLI an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **apply ns acls6**

So nummerieren Sie die Prioritäten erweiterter ACLs über die CLIneu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **ns acls neu nummerieren**

So nummerieren Sie die Prioritäten erweiterter ACL6s über die CLI neu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **renumber ns acls6**

GUI-Verfahren

So konfigurieren Sie eine erweiterte ACL mit der GUI:

- Navigieren Sie zu **System** > **Netzwerk** > **ACLs** und fügen Sie auf der Registerkarte **Erweiterte ACLs** eine neue erweiterte ACL hinzu oder bearbeiten Sie eine vorhandene erweiterte ACL. Um eine vorhandene erweiterte ACL zu aktivieren oder zu deaktivieren, wählen Sie sie aus und wählen Sie dann **Aktivieren** oder **Deaktivieren** aus der **Aktionsliste** aus.

So konfigurieren Sie eine erweiterte ACL6s mit der GUI:

- Navigieren Sie zu **System** > **Netzwerk** > **ACLs** und fügen Sie auf der Registerkarte **Erweiterte ACL6s** eine neue erweiterte ACL6 hinzu oder bearbeiten Sie eine vorhandene erweiterte ACL6. Um eine vorhandene erweiterte ACL6 zu aktivieren oder zu deaktivieren, wählen Sie es aus und wählen Sie dann **Aktivieren** oder **Deaktivieren** aus der **Aktionsliste** aus.

So wenden Sie erweiterte ACLs mit der GUI an:

- Navigieren Sie zu **System** > **Netzwerk** > **ACLs**, und klicken Sie auf der Registerkarte **Erweiterte ACLs** in der Liste **Aktion** auf **Anwenden**.

So wenden Sie erweiterte ACL6s mit der GUI an:

- Navigieren Sie zu **System** > **Netzwerk** > **ACLs**, und klicken Sie auf der Registerkarte **Erweiterte ACL6s** in der Liste **Aktion** auf **Anwenden**.

So nummerieren Sie die Prioritäten erweiterter ACLs mithilfe der GUI neu:

- Navigieren Sie zu **System** > **Netzwerk** > **ACLs**, und klicken Sie auf der Registerkarte **Erweiterte ACLs** in der Liste **Aktion** auf **Priorität(n) neu nummerieren**.

So nummerieren Sie die Prioritäten von erweiterten ACL6s mithilfe der GUI neu:

- Navigieren Sie zu **System** > **Netzwerk** > **ACLs**, und klicken Sie auf der Registerkarte **Erweiterte ACL6s** in der Liste **Aktion** auf **Priorität(n) neu nummerieren**.

Beispielkonfigurationen

Die folgende Tabelle zeigt Beispiele für die Konfiguration erweiterter ACL-Regeln über die Befehlszeilenschnittstelle: ACLS-Beispielkonfigurationen.

Protokollieren von erweiterten ACLs

Sie können den Citrix ADC so konfigurieren, dass Details für Pakete protokolliert werden, die erweiterten ACLs entsprechen.

Zusätzlich zum ACL-Namen enthalten die protokollierten Details paketspezifische Informationen wie Quell- und Ziel-IP-Adressen. Die Informationen werden je nach Art der aktivierten globalen Protokollierung (`syslog or nslog`) entweder in der Syslog-Datei oder in der Datei `nslog` gespeichert.

Die Protokollierung muss sowohl auf globaler Ebene als auch auf ACL-Ebene aktiviert sein. Die globale Einstellung hat Vorrang.

Um die Protokollierung zu optimieren, werden, wenn mehrere Pakete aus demselben Flow mit einer ACL übereinstimmen, nur die Details des ersten Pakets protokolliert, und der Zähler wird für jedes Paket, das zum selben Flow gehört, inkrementiert. Ein Flow ist definiert als eine Reihe von Paketen, die dieselben Werte für die Quell-IP-Adresse, die Ziel-IP-Adresse, den Quellport, den Zielport und die Protokollparameter aufweisen. Um eine Überschwemmung von Protokollmeldungen zu vermeiden, führt der Citrix ADC eine interne Ratenbegrenzung durch, sodass Pakete, die zum selben Flow gehören, nicht wiederholt protokolliert werden. Die Gesamtzahl der verschiedenen Flows, die zu einem bestimmten Zeitpunkt protokolliert werden können, ist auf 10.000 begrenzt.

Hinweis: Sie müssen ACLs anwenden, nachdem Sie die Protokollierung aktiviert haben.

CLI-Verfahren

So konfigurieren Sie die erweiterte ACL-Protokollierung mit der CLI:

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

- **set ns acl** <aclName> [-**logState** (ENABLED | DISABLED)] [-**rateLimit** <positive_integer>]
- **apply acls**
- **show ns acl** [<aclName>]

GUI-Verfahren

So konfigurieren Sie die erweiterte ACL-Protokollierung mit der GUI:

1. Navigieren Sie zu **System > Netzwerk > ACLs** und öffnen Sie auf der Registerkarte **Erweiterte ACLs** die erweiterte ACL.
2. Legen Sie die folgenden Parameter fest:
   - **Protokollstatus**— Aktiviert oder deaktiviert die Protokollierung von Ereignissen, die sich auf die erweiterte ACL-Regel beziehen. Die Protokollmeldungen werden auf dem konfigurierten `syslog or auditlog` Server gespeichert.
   - **Log Rate Limit**— Maximale Anzahl von Protokollmeldungen, die pro Sekunde generiert werden sollen. Wenn Sie diesen Parameter festlegen, müssen Sie den Parameter Log State aktivieren.

Beispielkonfiguration

```
1 > set ns acl restrict -logstate ENABLED -ratelimit 120
2 Warning: ACL modified, apply ACLs to activate change
```



```
3
4 > apply ns acls
5 Done
6 <!--NeedCopy-->
```

Protokollieren von erweiterten ACL6s

Sie können die Citrix ADC-Appliance so konfigurieren, dass Details für Pakete protokolliert werden, die einer erweiterten ACL6-Regel entsprechen. Zusätzlich zum ACL6-Namen enthalten die protokollierten Details paketspezifische Informationen wie Quell- und Ziel-IP-Adressen. Die Informationen werden entweder in einem Syslog oder einer `nslog` Datei gespeichert, abhängig von der Art der Protokollierung (`syslog or nslog`), die Sie in der Citrix ADC-Appliance konfiguriert haben.

Wenn mehrere Pakete aus demselben Flow mit einer ACL6 übereinstimmen, werden nur die Details des ersten Pakets protokolliert, um die Protokollierung zu optimieren. Der Zähler wird für jedes andere Paket erhöht, das zum selben Flow gehört. Ein Flow ist definiert als eine Reihe von Paketen, die dieselben Werte für die folgenden Parameter haben:

- Quell-IP
- Ziel-IP
- Quell-Port
- Destination port
- Protokoll (TCP oder UDP)

Wenn ein eingehendes Paket nicht aus demselben Flow stammt, wird ein neuer Flow erstellt. Die Gesamtzahl der verschiedenen Flows, die zu einem bestimmten Zeitpunkt protokolliert werden können, ist auf 10.000 begrenzt.

CLI-Verfahren

So konfigurieren Sie die Protokollierung für eine erweiterte aCl6-Regel mit der CLI:

- Um die Protokollierung beim Hinzufügen der erweiterten ACL6-Regel zu konfigurieren, geben Sie an der Eingabeaufforderung Folgendes ein:
  - **add acl6** <acl6Name> <acl6action> [-**logState** (ENABLED | DISABLED)] [-**rateLimit** <positive_integer>]
  - **apply acls6**
  - **show acl6** [<acl6Name>]
- Um die Protokollierung für eine vorhandene erweiterte ACL6-Regel zu konfigurieren, geben Sie an der Eingabeaufforderung Folgendes ein:
  - **set acl6** <acl6Name> [-**logState** (ENABLED | DISABLED)] [-**rateLimit** <positive_integer>]

- **show acl6** [<acl6Name>]
- **apply acls6**

GUI-Verfahren

So konfigurieren Sie die erweiterte ACL6-Protokollierung mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **ACLs** und klicken Sie dann auf die Registerkarte **Extended ACL6s** .
2. Legen Sie die folgenden Parameter fest, während Sie eine vorhandene erweiterte ACL6-Regel hinzufügen oder ändern.
   - **Protokollstatus** — Aktivieren oder deaktivieren Sie die Protokollierung von Ereignissen im Zusammenhang mit der erweiterten ACL6s-Regel. Die Protokollmeldungen werden im konfigurierten Syslog oder im `auditlog` des Servers gespeichert.
   - **Log Rate Limit**— Maximale Anzahl von Protokollmeldungen, die pro Sekunde generiert werden sollen. Wenn Sie diesen Parameter festlegen, müssen Sie den Parameter **Log State** aktivieren.

Beispielkonfiguration

```
> set acl6 ACL6-1 -logstate ENABLED -ratelimit 120
Done

> apply acls6
Done
<!--NeedCopy-->
```

Anzeigen erweiterter ACLs und erweiterter ACL6s-Statistiken

Sie können Statistiken zu erweiterten ACLs und ACL6s anzeigen.

In der folgenden Tabelle sind die Statistiken aufgeführt, die mit erweiterten ACLs und ACL6s verknüpft sind, sowie deren Beschreibungen.

Statistik	Gibt an
ACL-Übereinstimmungen zulassen	Pakete, die ACLs entsprechen, wobei der Verarbeitungsmodus auf Allow festgelegt ist. Citrix ADC verarbeitet diese Pakete.
NAT ACL Begegnungen	Pakete, die mit einer NAT-ACL übereinstimmen, was zu einer NAT-Sitzung führt.

Statistik	Gibt an
ACL-Spiele verweigern	Pakete wurden gelöscht, weil sie ACLs mit dem Verarbeitungsmodus auf DENY festgelegt sind.
Bridge ACL Übereinstimmungen	Pakete, die einer Bridge-ACL entsprechen, die im transparenten Modus die Dienstverarbeitung umgeht.
ACL-Übereinstimmungen	Pakete, die mit einer ACL übereinstimmen.
ACL verpasst	Pakete, die keiner ACL entsprechen.
ACL-Anzahl	Gesamtzahl der von Benutzern konfigurierten ACL-Regeln.
Effektive ACL-Anzahl	Gesamtzahl der intern konfigurierten effektiven ACL. Für eine erweiterte ACL mit einer Reihe von IP-Adressen erstellt die Citrix ADC-Appliance intern eine erweiterte ACL für jede IP-Adresse. Für eine erweiterte ACL mit 1000 IPv4-Adressen (Bereich oder Datensatz) hat der Citrix ADC beispielsweise intern 1000 erweiterte ACLs erstellt.

CLI-Verfahren

So zeigen Sie die Statistiken aller erweiterten ACLs mit der CLI an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **stat ns acl**

So zeigen Sie die Statistiken aller erweiterten ACL6s mit der CLI an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **stat ns acl6**

GUI-Verfahren

So zeigen Sie die Statistiken einer erweiterten ACL mithilfe der GUI an:

- Navigieren Sie zu **System > Netzwerk > ACLs**, wählen Sie auf der Registerkarte **Erweiterte ACLs** die erweiterte ACL aus und klicken Sie auf **Statistik**.

So zeigen Sie die Statistiken einer erweiterten ACL6 mithilfe der GUI an:

- Navigieren Sie zu **System > Netzwerk > ACLs**, wählen Sie auf der Registerkarte **Erweiterte ACL6s** die erweiterte ACL aus und klicken Sie auf **Statistik**.

Stateful-ACLs

Eine statusbehaftete ACL-Regel erstellt eine Sitzung, wenn eine Anforderung mit der Regel übereinstimmt, und erlaubt die resultierenden Antworten, auch wenn diese Antworten mit einer Ablehnungs-ACL-Regel in der Citrix ADC-Appliance übereinstimmen. Eine stateful ACL entlastet die Arbeit, mehr ACL-Regeln/Weiterleitungssitzungsregeln zu erstellen, um diese spezifischen Antworten zuzulassen.

Stateful ACLs können am besten in einer Edge-Firewall-Bereitstellung einer Citrix ADC-Appliance verwendet werden, die folgende Anforderungen erfüllt:

- Die Citrix ADC-Appliance muss Anfragen zulassen, die von internen Clients initiiert wurden, und die zugehörigen Antworten aus dem Internet.
- Die Appliance muss die Pakete aus dem Internet löschen, die nicht mit Clientverbindungen zusammenhängen.

Voraussetzungen

Bevor Sie statusbehaftete ACL-Regeln konfigurieren, beachten Sie die folgenden Punkte:

- Die Citrix ADC-Appliance unterstützt statusbehaftete ACL-Regeln und stateful ACL6-Regeln.
- In einem Hochverfügbarkeitssetup werden die Sitzungen für eine statusbehaftete ACL-Regel nicht mit dem sekundären Knoten synchronisiert.
- Sie können eine ACL-Regel nicht als stateful konfigurieren, wenn die Regel an eine Citrix ADC NAT-Konfiguration gebunden ist. Einige Beispiele für Citrix ADC NAT-Konfigurationen sind:
  - RNAT
  - Large Scale NAT (Großmaßstab NAT44, DS-Lite, Großmaßstab NAT64)
  - NAT64
  - Weiterleitungssitzung
- Sie können eine ACL-Regel nicht als statusbehaftet konfigurieren, wenn TTL und Established Parameter für diese ACL-Regel festgelegt sind.
- Die für eine stateful ACL-Regel erstellten Sitzungen existieren unabhängig von den folgenden ACL-Operationen bis zum Timeout weiterhin:
  - ACL entfernen
  - Deaktivieren Sie ACL
  - Löschen Sie ACL
- Stateful-ACLs werden für die folgenden Protokolle nicht unterstützt:
  - Aktiv FTP
  - TFTP

Konfigurieren von stateful IPv4-ACL-Regeln

Die Konfiguration einer stateful ACL-Regel besteht darin, den stateful Parameter einer ACL-Regel zu aktivieren.

So aktivieren Sie den stateful Parameter einer ACL-Regel mithilfe der CLI:

- Um den statusbehafteten Parameter beim Hinzufügen einer ACL-Regel zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein:
  - **add acl** <lname> ALLOW -**stateful** (ENABLED | DISABLED)
  - **apply acls**
  - **show acl** <name>
- Um den statusbehafteten Parameter einer vorhandenen ACL-Regel zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein:
  - **set acl** <name> -**stateful** (ENABLED | DISABLED)
  - **apply acls**
  - **show acl** <name>

So aktivieren Sie den stateful Parameter einer ACL-Regel mithilfe der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **ACLs** und auf der Registerkarte **Erweiterte ACLs**.
2. Aktivieren Sie den **Stateful-Parameter**, während Sie eine vorhandene ACL-Regel hinzufügen oder ändern.

Beispielkonfiguration

```
> add acl ACL-1 allow -srciP 1.1.1.1 -stateful Yes

Done

> apply acls

Done

> show acl

1)          Name: ACL-1

    Action: ALLOW                          Hits: 0

    srcIP = 1.1.1.1

    destIP
```



```
18
19      srcMac:
20
21      Protocol:
22
23      Vlan:                                   Interface:
24
25      Active Status: ENABLED                   Applied Status: NOTAPPLIED
26
27      Priority: 10                             NAT: NO
28
29      TTL:
30
31      Log Status: DISABLED
32
33      Forward Session: NO
34
35      Stateful: YES
36  <!--NeedCopy-->
```

Konfigurieren Sie stateful ACL6-Regeln

Die Konfiguration einer stateful ACL6-Regel besteht darin, den stateful Parameter einer ACL6-Regel zu aktivieren.

So aktivieren Sie den stateful Parameter einer ACL6-Regel mithilfe der CLI:

- Um den statusbehafteten Parameter beim Hinzufügen einer ACL6-Regel zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein:
  - **add acl6** <name> ALLOW -stateful (ENABLED | DISABLD)
  - **apply acls6**
  - **show acl6** <name>
- Um den statusbehafteten Parameter einer vorhandenen ACL6-Regel zu aktivieren, geben Sie an der Eingabeaufforderung Folgendes ein:
  - **set acl6** <name> -**stateful** (ENABLED | DISABLED)
  - **apply acls6**
  - **show acl6** <name>

So aktivieren Sie den stateful Parameter einer ACL6-Regel mithilfe der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **ACLs** und auf der Registerkarte **Erweiterte ACL6s** .
2. Aktivieren Sie den **Stateful-Parameter**, während Sie eine vorhandene ACL6-Regel hinzufügen oder ändern.

Beispielkonfiguration

```
>  add acl6 ACL6-1 allow -srcipv6 1000::1  - stateful Yes

Done

>  apply acls6

Done

> show acl6

1)    Name: ACL6-1

    Action: ALLOW                          Hits: 0

    srcIPv6 = 1000::1

    destIPv6

    srcMac:

    Protocol:

    Vlan:                                 Interface:

    Active Status: ENABLED                 Applied Status: NOTAPPLIED

    Priority: 10                           NAT: NO

    TTL:

    Forward Session: NO

    Stateful: YES
<!--NeedCopy-->
```

Dataset-basierte erweiterte ACLs

Viele ACLs sind in einem Unternehmen erforderlich. Das Konfigurieren und Verwalten vieler ACLs ist schwierig und umständlich, wenn sie häufige Änderungen erfordern.

Eine Citrix ADC-Appliance unterstützt Datensätze in erweiterten ACLs. Dataset ist ein vorhandenes Feature einer Citrix ADC-Appliance. Ein Datensatz ist ein Array von indizierten Mustern von Typen:

Zahl (Ganzzahl), IPv4-Adresse oder IPv6-Adresse.

Die Unterstützung von Datensätzen in erweiterten ACLs ist nützlich, um mehrere ACL-Regeln zu erstellen, die gemeinsame ACL-Parameter erfordern.

Während Sie eine ACL-Regel erstellen, können Sie anstelle der allgemeinen Parameter ein Dataset angeben, das diese allgemeinen Parameter enthält.

Alle am Datensatz vorgenommenen Änderungen werden automatisch in den ACL-Regeln wiedergegeben, die diesen Datensatz verwenden. ACLs mit Datensätzen sind einfacher zu konfigurieren und zu verwalten. Sie sind auch kleiner und einfacher zu lesen als die herkömmlichen ACLs.

Derzeit unterstützt die Citrix ADC-Appliance nur das Dataset des IPv4-Adresstyps für erweiterte ACLs.

Voraussetzungen

Beachten Sie vor dem Konfigurieren von datensatzbasierten erweiterten ACL-Regeln die folgenden Punkte:

- Stellen Sie sicher, dass Sie mit der Dataset-Funktion einer Citrix ADC-Appliance vertraut sind. Weitere Informationen zu Datensätzen finden Sie unter Mustersätze und Datensätze.
- Die Citrix ADC-Appliance unterstützt Datasets nur für erweiterte IPv4-ACLs.
- Die Citrix ADC-Appliance unterstützt nur die IPv4-Datasets für erweiterte ACLs.
- Die Citrix ADC-Appliance unterstützt Dataset-basierte erweiterte ACLs für alle Setups: Standalone, Hochverfügbarkeit und Cluster.
- Für eine erweiterte ACL mit einer Reihe von IP-Adressen erstellt die Citrix ADC-Appliance intern eine erweiterte ACL für jede IP-Adresse. Für eine auf IPv4-Datensatz basierende erweiterte ACL mit 1000 IPv4-Adressen, die an den Datensatz gebunden sind, erstellte die Citrix ADC-Appliance intern 1000 erweiterte ACLs.
  - Die Citrix ADC-Appliance unterstützt maximal 10K erweiterte ACLs. Für eine IPv4-Dataset-basierte erweiterte ACL mit einer Reihe von IP-Adressen, die an den Datensatz gebunden sind, erstellt die Citrix ADC-Appliance keine internen ACLs, sobald die Gesamtzahl der erweiterten ACLs die maximale Grenze erreicht hat.
  - Die folgenden Zähler sind im Rahmen der erweiterten ACL-Statistik vorhanden:
    * **ACL-Zählung**. Gesamtzahl der von Benutzern konfigurierten ACL-Regeln.
    * **Effektive ACL-Anzahl**. Gesamtzahl der effektiven ACL-Regeln, die die Citrix ADC-Appliance intern konfiguriert.

    Weitere Informationen finden Sie unter Anzeigen von erweiterten ACL und erweiterten ACL6s-Statistiken.

- Die Citrix ADC-Appliance unterstützt keine Vorgänge `set` und `unset` zum Verbinden/Dissoziieren von Datensätzen mit den Parametern einer erweiterten ACL. Sie können die ACL-Parameter nur während des Vorgangs `add` auf ein Dataset einstellen.

Konfigurieren von datensatzbasierten erweiterten ACLs

Das Konfigurieren einer auf Dataset basierenden erweiterten ACL-Regel besteht aus den folgenden Aufgaben:

- **Fügen Sie einen Datensatz hinzu**. Ein Datensatz ist ein Array von indizierten Mustern von Typen: Zahl (Ganzzahl), IPv4-Adresse oder IPv6-Adresse. In dieser Aufgabe erstellen Sie einen Datasetyp, z. B. einen Datensatz vom Typ IPv4.
- **Binden Sie Werte an das Dataset**. Geben Sie einen Wert oder einen Wertebereich für das Dataset an. Die angegebenen Werte müssen vom gleichen Typ wie der Dataset-Typ sein. Sie können beispielsweise eine IPv4-Adresse oder einen Bereich von IPv4-Adressen für den Datensatz vom Typ IPv4 angeben.
- **Fügen Sie eine erweiterte ACL hinzu und legen Sie ACL-Parameter für das Dataset fest**. Fügen Sie eine erweiterte ACL hinzu und legen Sie die erforderlichen ACL-Parameter für den Datensatz fest. Diese Einstellung führt dazu, dass die Parameter auf die im Datensatz angegebenen Werte festgelegt sind.
- **Wenden Sie erweiterte ACLs an**. Wenden Sie die ACLs an, um neue oder geänderte erweiterte ACLs zu aktivieren.

So fügen Sie ein Richtlinien-Dataset mit der CLI hinzu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add policy dataset** <name> <type>
- **show policy dataset**

So binden Sie ein Muster mit der CLI an den Datensatz:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **bind policy dataset** <name> <value> [-endRange <string>]
- **show policy dataset**

So fügen Sie eine erweiterte ACL hinzu und legen die ACL-Parameter über die Befehlszeilenschnittstelle auf das Dataset fest:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add ns acl** <aclname> <aclaction> [-**srcIP** [<operator>] <srcIPVal>] [-**srcPort** [<operator>] <srcPortVal>] [-**destIP** [<operator>] <destIPVal>] [-**destPort** [<operator>] <destPortVal>] …
- **show acls**

So wenden Sie erweiterte ACLs mit der CLI an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **apply acls**

Beispielkonfiguration

In der folgenden Beispielkonfiguration einer datensatzbasierten erweiterten ACL wird ein IPv4-Dataset DATASET-ACL-1 erstellt. Zwei IPv4-Adressen: 192.0.2.30 und 192.0.2.60 und zwei IPv4-Adressbereiche: (198.51.100.15 - 45) und (203.0.113.60-90) sind an DATASET-ACL-1 gebunden. DATASET-ACL-1 wird dann für die srCIP- und DestIP-Parameter der erweiterten ACL ACL-1 angegeben.

```
add policy dataset DATASET-ACL-1 IPV4

bind dataset DATASET-ACL-1 192.0.2.30

bind dataset DATASET-ACL-1 192.0.2.60

bind dataset DATASET-ACL-1 198.51.100.15 -endrange 198.51.100.45

bind dataset DATASET-ACL-1 203.0.113.60 -endrange 203.0.113.90

add ns acl ACL-1 ALLOW -srcIP DATASET-ACL-1 -destIP DATASET-ACL-1

apply acls
<!--NeedCopy-->
```

MAC-Adress-Platzhaltermaske für ACLs

October 5, 2021

Ein Platzhaltermasken-Parameter wurde für erweiterte ACLs und ACL6s eingeführt und wird zusammen mit dem Quell-MAC-Adressparameter verwendet, um einen Bereich von MAC-Adressen zu definieren, die mit der Quell-MAC-Adresse eingehender Pakete übereinstimmen.

Platzhaltermasken geben an, welche Hexadezimalziffern der MAC-Adresse verwendet werden und welche Hexadezimalziffern ignoriert werden. Der Parameter Platzhaltermaske gibt eine Reihe von Einsen und Nullen an und hat eine Länge von 12 Ziffern. Jede Ziffer ist eine Maske für die entsprechende hexadezimale Ziffer der MAC-Adresse. Eine Nullziffer in der Platzhaltermaske gibt an,

dass die entsprechende Hexadezimalziffer der MAC-Adresse berücksichtigt werden muss, und eine Ziffer gibt an, dass die entsprechende Hexadezimalziffer ignoriert werden soll.

Die Platzhaltermaske muss die folgenden Bedingungen erfüllen:

- Hat nur eine Reihe von Nullen
- Hat nur eine Reihe von
- Beginnen Sie mit einer Reihe von Nullen

Im Folgenden finden Sie einige Beispiele für gültige Platzhaltermasken:

- 000000111111
- 000000011111
- 000011111111

Im Folgenden finden Sie einige Beispiele für ungültige Platzhaltermasken:

- 000000111100
- 111110000000
- 010101010101

Für eine ACL definiert eine Platzhaltermaske 000000111111 für MAC-Adresse 96:fa:95:1d:67:4a den MAC-Adressbereich 96:FA:95:00:00:00 - 96:FA:95:FF:FF:FF. Dieser MAC-Adressbereich wird mit der Quell-MAC-Adresse der eingehenden Pakete abgeglichen.

So geben Sie mit der CLI einen Bereich von Quell-MAC-Adressen in einer ACL-Regel an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 -  add ns acl <name> <action> -srcMac <mac_addr> -srcMacMask <string>
2 -  show ns acl <aclname>
3 <!--NeedCopy-->
```

Beispiel:

```
1 add ns acl ACL-1 ALLOW  - protocol TCP  - srcport 2000-3000 -srcMac 96:fa
     :95:1d:67:4a
2   - srcMacMask 000000111111
3 Done
4 <!--NeedCopy-->
```

So geben Sie mit der CLI einen Bereich von Quell-MAC-Adressen in einer ACL6-Regel an:

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
-  add ns acl6 <name> <action> -srcMac <mac_addr> -srcMacMask <string>
-  show ns acl6 <acl6name>
<!--NeedCopy-->
```

Beispiel:

```
> add ns acl6 ACL6-1 ALLOW -destIPv6 2001::45 -srcMac 96:fa:90:1d:67:4a
 -srcMacMask 000000001111
Done
<!--NeedCopy-->
```

Datenverkehr auf internen Ports blockieren

September 22, 2022

Standardmäßig blockiert eine Citrix ADC-Appliance keine Art von internem Datenverkehr, selbst wenn ACL-Regeln verwendet werden.

In der folgenden Tabelle sind die internen Datenverkehrstypen aufgeführt, die eine Citrix ADC-Appliance auch mit ACL-Regeln nicht blockiert:

Citrix ADC Setup	Protokoll	Ziel-Port	Ziel-IP-Adresse
Alle	TCP	3008–3011	NSIP oder SNIP
Alle	TCP	179	NSIP oder SNIP
Alle	UDP	520	NSIP oder SNIP
Hohe Verfügbarkeit	UDP	3003	NSIP
Hohe Verfügbarkeit	TCP	22	NSIP
Cluster	UDP	7000	NSIP

Diese Funktion, die zuvor genannten Datenverkehrstypen nicht zu blockieren, wird durch die Standardeinstellung des globalen Layer-3 `Implicit ACL Allow` (`implicitACLAllow`)-Parameters festgelegt.

Sie können diesen Parameter deaktivieren, wenn Sie die zuvor genannten Datenverkehrstypen mit den ACL-Regeln blockieren möchten. Eine Appliance in einem Hochverfügbarkeitssetup macht eine Ausnahme für ihren Partnerknoten (primär oder sekundär). Es blockiert nicht den Datenverkehr von

diesem Knoten.

So deaktivieren oder aktivieren Sie diesen Parameter mit der CLI:

Geben Sie in der Befehlszeile Folgendes ein:

- **set l3param** -**implicitACLAllow** [ENABLED|DISABLED]
- **sh l3param**

Hinweis: Der Parameter implicitACLAllow ist standardmäßig aktiviert.

Beispiel:

```
> set l3param –implicitACLAllow DISABLED
Done
<!--NeedCopy-->
```

IP-Routing

October 5, 2021

Citrix ADC Appliances unterstützen sowohl dynamisches als auch statisches Routing. Da einfaches Routing nicht die primäre Rolle eines Citrix ADC ist, besteht das Hauptziel der Ausführung dynamischer Routingprotokolle darin, die RoutenintegritätsInjection (RHI) zu aktivieren, damit ein Upstream-Router die besten unter mehreren Routen zu einem topografisch verteilten virtuellen Server auswählen kann.

Die meisten Citrix ADC Implementierungen verwenden einige statische Routen, um den Routing-Overhead zu reduzieren. Sie können statische Backup-Routen erstellen und Routen überwachen, um die automatische Umschaltung für den Fall zu aktivieren, dass eine statische Route ausfällt. Sie können auch Gewichtungen zuweisen, um den Lastausgleich zwischen statischen Routen zu erleichtern, Nullrouten zur Vermeidung von Routingschleifen zu erstellen und statische IPv6-Routen zu konfigurieren. Sie können richtlinienbasierte Routen (PBRs) konfigurieren, für die Routingentscheidungen auf von Ihnen angegebenen Kriterien basieren.

Dynamische Routen konfigurieren

October 5, 2021

Wenn ein dynamisches Routingprotokoll aktiviert ist, überwacht der entsprechende Routingprozess Routenaktualisierungen und kündigt Routen an. Routingprotokolle ermöglichen es einem Upstream-Router, die ECMP-Technik (Equal Cost Multipath) zum Lastausgleich von Datenverkehr zu identischen virtuellen Servern zu verwenden, die auf zwei eigenständigen Citrix ADC Appliances gehostet werden. Dynamisches Routing auf einer Citrix ADC Appliance verwendet drei Routingtabellen. In einem Setup mit hoher Verfügbarkeit spiegeln die Routingtabellen auf der sekundären Appliance die auf der primären Appliance.

Informationen zu Befehlsreferenzhandbüchern und nicht unterstützten Befehlen für das dynamische Routingprotokoll finden Sie unter Befehlsreferenzhandbücher für das dynamische Routing-Protokoll und nicht unterstützte Befehle.

Citrix ADC unterstützt die folgenden Protokolle:

- Routinginformationsprotokoll (RIP), Version 2
- Open Shortest Path First (OSPF) Version 2
- Border Gateway Protocol (BGP)
- Routing-Informationsprotokoll der nächsten Generation (RIPng) für IPv6
- Open Shortest Path First (OSPF) Version 3 für IPv6
- ISIS-Protokoll

Sie können mehrere Protokolle gleichzeitig aktivieren.

Routingtabellen in Citrix ADC

In einer Citrix ADC-Appliance enthalten die Kernel Routingtabelle Citrix ADC, die FreeBSD-Kernel-Routingtabelle und die NSM FIB-Routingtabelle jeweils unterschiedliche Routen und dienen einem anderen Zweck. Sie kommunizieren miteinander, indem Sie UNIX-Routing-Sockets verwenden. Routenaktualisierungen werden nicht automatisch von einer Routingtabelle in eine andere weitergegeben. Sie müssen die Propagierung von Routenaktualisierungen für jede Routingtabelle konfigurieren.

NS-Kernel-Routingtabelle

Die NS-Kernel-Routingtabelle enthält Subnetzrouten, die dem NSIP und jedem SNIP und MIP entsprechen. Normalerweise sind in der NS-Kernel-Routingtabelle keine VIPs entsprechende Routen vorhanden. Die Ausnahme ist ein VIP, der mithilfe des Befehls add ns ip hinzugefügt und mit einer anderen Subnetzmaske als 255.255.255.255 konfiguriert wurde. Wenn mehrere IP-Adressen zu demselben Subnetz gehören, werden sie als einzelne Subnetzroute abstrahiert. Darüber hinaus enthält diese Tabelle eine Route zum Loopback-Netzwerk (127.0.0.0) und alle statischen Routen, die über die CLI (CLI) hinzugefügt werden. Die Einträge in dieser Tabelle werden vom Citrix ADC bei der Paketweiterleitung verwendet. Von der CLI aus können sie mit dem Befehl show route überprüft werden.

FreeBSD-Routingtabelle

Der einzige Zweck der FreeBSD-Routing-Tabelle besteht darin, die Einleitung und Beendigung des Management-Datenverkehrs (Telnet, SSH usw.) zu erleichtern. In einer Citrix ADC Appliance sind diese Anwendungen eng mit FreeBSD verbunden, und es ist unerlässlich, dass FreeBSD über die erforderlichen Informationen verfügt, um den Datenverkehr zu und von diesen Anwendungen zu verarbeiten. Diese Routingtabelle enthält eine Route zum NSIP-Subnetz und eine Standardroute. Darüber hinaus fügt FreeBSD Routen vom Typ WasCloned(W) hinzu, wenn der Citrix ADC Verbindungen zu Hosts in lokalen Netzwerken aufbaut. Aufgrund des hochspezialisierten Dienstprogramms der Einträge in dieser Routingtabelle übergehen alle anderen Routenaktualisierungen aus dem NS-Kernel und NSM FIB-Routingtabellen die FreeBSD-Routingtabelle. Ändern Sie es nicht mit dem Befehl route. Die FreeBSD-Routingtabelle kann mit dem Befehl netstat aus jeder UNIX-Shell überprüft werden.

Netzwerkdienste-Modul (NSM) FIB

Die NSM FIB-Routingtabelle enthält die ankündigbaren Routen, die von den dynamischen Routingprotokollen an ihre Peers im Netzwerk verteilt werden. Es kann enthalten:

- **Verbundene Routen**. IP-Subnetze, die direkt vom Citrix ADC aus erreichbar sind. In der Regel sind Routen, die dem NSIP-Subnetz entsprechen, und Subnetzen, über die Routingprotokolle aktiviert sind, in NSM FIB als verbundene Routen vorhanden.
- **Kernel-Routen**. Alle VIP-Adressen, auf denen die Option -HostRoute aktiviert ist, sind in NSM FIB als Kernelrouten vorhanden, wenn sie die erforderlichen RHI-Levels erfüllen. Darüber hinaus enthält NSM FIB alle statischen Routen, die auf der CLI konfiguriert sind, für die die Option - advertise aktiviert ist. Wenn der Citrix ADC im SRADV-Modus (Static Route Advertisement) arbeitet, sind auch alle statischen Routen, die auf der CLI konfiguriert sind, in NSM FIB vorhanden. Diese statischen Routen werden in NSM FIB als Kernel-Routen markiert, da sie tatsächlich zur NS-Kernel-Routingtabelle gehören.
- **Statische Routen**. Normalerweise ist jede statische Route, die in VTYSH konfiguriert ist, in NSM FIB vorhanden. Wenn administrative Abstände von Protokollen geändert werden, kann dies nicht immer der Fall sein. Ein wichtiger Punkt ist, dass diese Routen nie in die NS-Kernel-Routing-Tabelle gelangen können.
- **Gelernte Routen**. Wenn Citrix ADC so konfiguriert ist, dass Routen dynamisch erlernen, enthält die NSM FIB Routen, die von den verschiedenen dynamischen Routingprotokollen gelernt werden. Routen, die von OSPF gelernt werden, erfordern jedoch eine spezielle Verarbeitung. Sie werden nur dann auf FIB heruntergeladen, wenn die fib-install Option für den OSPF-Prozess aktiviert ist. Dies kann über die Router-Config-Ansicht in VTYSH erfolgen.

Dynamisches Routing in einem Hochverfügbarkeitssetup

In einem Hochverfügbarkeitssetup führt der primäre Knoten den Routingprozess aus und leitet Routingtabellenaktualisierungen an den sekundären Knoten weiter. Die Routingtabelle des sekundären Knotens spiegelt die Routingtabelle auf dem primären Knoten wider.

Non-Stop-Weiterleitung

Nach dem Failover dauert der sekundäre Knoten einige Zeit, um das Protokoll zu starten, die Routen zu lernen und seine Routingtabelle zu aktualisieren. Dies hat jedoch keinen Einfluss auf das Routing, da die Routingtabelle auf dem sekundären Knoten mit der Routingtabelle auf dem primären Knoten identisch ist. Diese Betriebsart wird als Non-Stop-Weiterleitung bezeichnet.

Blackhole-Vermeidungsmechanismus

Nach dem Failover injiziert der neue primäre Knoten alle VIP-Routen in den Upstream-Router. Dieser Router behält jedoch die Routen des alten primären Knotens für 180 Sekunden bei. Da der Router das Failover nicht kennt, versucht er, den Datenverkehr zwischen den beiden Knoten auszugleichen. Während der 180 Sekunden vor Ablauf der alten Routen sendet der Router die Hälfte des Datenverkehrs an den alten, inaktiven primären Knoten, der tatsächlich ein schwarzes Loch ist.

Um dies zu verhindern, weist der neue primäre Knoten beim Einleiten einer Route eine Metrik zu, die etwas niedriger ist als die vom alten primären Knoten angegebene Metrik.

Schnittstellen zum Konfigurieren von dynamischem Routing

Um das dynamische Routing zu konfigurieren, können Sie entweder die GUI oder eine Befehlszeilenschnittstelle verwenden. Das Citrix ADC unterstützt zwei unabhängige Befehlszeilenschnittstellen: die CLI und die Virtual Teletype Shell (VTYSH). Die CLI ist die native Shell der Appliance. VTYSH wird von ZeBos freigelegt. Die Citrix ADC Routing-Suite basiert auf ZebOS, der kommerziellen Version von GNU Zebra.

> **Hinweis:**
>
> Citrix empfiehlt, VTYSH für alle Befehle zu verwenden, mit Ausnahme derer, die nur auf der CLI konfiguriert werden können. Die Verwendung der CLI sollte in der Regel auf Befehle zum Aktivieren der Routingprotokolle, zum Konfigurieren der Host-Routenankündigung und zum Hinzufügen statischer Routen für die Paketweiterleitung beschränkt sein.

Referenzhandbücher für Dynamic Routing-Protokoll und nicht unterstützte Befehle

In der folgenden Tabelle sind Links für Befehlsreferenzhandbücher für verschiedene dynamische Routingprotokolle und nicht unterstützte Befehle auf der Citrix ADC Appliance aufgeführt:

Referenzhandbücher für dynamische Routingprotokolle und nicht unterstützte Befehle.

RIP konfigurieren

October 5, 2021

Routing Information Protocol (RIP) ist ein Distance Vector Protokoll. Citrix ADC unterstützt RIP gemäß RFC 1058 und RFC 2453. RIP kann in jedem Subnetz ausgeführt werden.

Nachdem Sie RIP aktiviert haben, müssen Sie die Ankündigung von RIP-Routen konfigurieren. Zur Fehlerbehebung können Sie die RIP-Propagierung einschränken. Sie können RIP-Einstellungen anzeigen, um die Konfiguration zu überprüfen.

Aktivieren und Deaktivieren von RIP

Verwenden Sie eines der folgenden Verfahren, um RIP zu aktivieren oder zu deaktivieren. Nachdem Sie RIP aktiviert haben, startet die Citrix ADC Appliance den RIP-Prozess. Nachdem Sie RIP deaktiviert haben, stoppt die Appliance den RIP-Prozess.

So aktivieren oder deaktivieren Sie das RIP-Routing mit der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um RIP zu aktivieren oder zu deaktivieren:

- **enable ns feature RIP**
- **disable ns feature RIP**

So aktivieren oder deaktivieren Sie das RIP-Routing mit der GUI:

1. Navigieren Sie zu **System** > **Einstellungen**, klicken Sie in der Gruppe **Modi und Funktionen** auf **Erweiterte Funktionen ändern**.
2. Aktivieren oder deaktivieren Sie die Option **RIP-Routing**.

Routen ankündigen

RIP ermöglicht einem Upstream-Router den Lastausgleich zwischen zwei identischen virtuellen Servern, die auf zwei eigenständigen Citrix ADC Appliances gehostet werden. Routenankündigung ermöglicht es einem Upstream-Router, Netzwerkentitäten zu verfolgen, die sich hinter dem Citrix ADC befinden.

So konfigurieren Sie RIP, um Routen mithilfe der VTYSH Befehlszeile anzukündigen:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Gibt an
VTYSH	Zeigt die VTYSH Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
router rip	Starten Sie den RIP-Routing-Prozess und wechseln Sie in den Konfigurationsmodus für den Routing-Prozess.
redistribute static	Verteilen Sie statische Routen.
redistribute kernel	Verteilen Sie Kernel-Routen neu.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router rip
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
<!--NeedCopy-->
```

RIP-Propagierungen einschränken

Wenn Sie Probleme mit der Konfiguration beheben müssen, können Sie den Nur-Listenmodus auf einer beliebigen Schnittstelle konfigurieren.

So beschränken Sie die RIP-Propagierung mithilfe der VTYSH Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Gibt an
VTYSH	Zeigt die VTYSH Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
router rip	Starten Sie den RIP-Routing-Prozess und wechseln Sie in den Konfigurationsmodus für den Routing-Prozess.

Befehl	Gibt an
passive-interface < vlan_name>	Unterdrücken Sie Routing-Updates auf Schnittstellen, die an das angegebene VLAN gebunden sind.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router rip
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Überprüfen der RIP-Konfiguration

Sie können die Routingtabelle und andere RIP-Einstellungen anzeigen.

So zeigen Sie die RIP-Einstellungen mithilfe der VTYSH Befehlszeile an:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der folgenden Reihenfolge ein:

Befehl	Gibt an
VTYSH	Zeigt die VTYSH Eingabeaufforderung an.
sh rip	Zeigt die aktualisierte RIP-Routingtabelle an.
<vlan_name>sh rip-Schnittstelle	Zeigt RIP-Informationen für das angegebene VLAN an.

Beispiel:

```
NS# VTYSH
NS# sh rip
NS# sh rip interface VLAN0
<!--NeedCopy-->
```


Konfigurieren von OSPF

December 3, 2021

Der Citrix ADC unterstützt Open Shortest Path First (OSPF) Version 2 (RFC 2328). Die Funktionen von OSPF auf dem Citrix ADC sind:

- Wenn ein vserver aktiv ist, können die Host-Leitungen zum vserver in die Routingprotokolle eingespeist werden.
- OSPF kann in jedem Subnetz ausgeführt werden.
- Das von benachbarten OSPF-Routern beworbene Routenlernen kann auf dem Citrix ADC deaktiviert werden.
- Der Citrix ADC kann externe Typ-1- oder Typ-2-Metriken für alle Routen ankündigen.
- Der Citrix ADC kann vom Benutzer festgelegte Metrikeinstellungen für VIP-Routen ankündigen. Sie können beispielsweise eine Metrik pro VIP ohne spezielle Routenkarten konfigurieren.
- Sie können die OSPF-Bereichs-ID für den Citrix ADC angeben.
- Der Citrix ADC unterstützt nicht so stummelige Bereiche (NSSAs). Eine NSSA ähnelt einem OSPF-Stub-Bereich, ermöglicht jedoch die begrenzte Einschleusung externer Routen in den Stub-Bereich. Zur Unterstützung von NSSAs wurden ein neues Optionsbit (das N-Bit) und ein neuer Typ (Typ 7) des Link State Advertisement (LSA) -Bereichs definiert. LSAs vom Typ 7 unterstützen externe Routeninformationen innerhalb einer NSSA. Ein NSSA Area Border Router (ABR) übersetzt eine LSA vom Typ 7 in eine LSA vom Typ 5, die in die OSPF-Domäne übertragen wird. Die OSPF-Spezifikation definiert nur die folgenden allgemeinen Klassen der Flächenkonfiguration:
  - Typ 5 LSA: Ursprünglich von Routern innerhalb des Gebiets werden von AS-Boarder-Routern (ASBRs) in die Domäne überflutet.
  - Stub: Erlaubt keine Typ-5-LSAs in/im gesamten Gebiet zu übertragen und hängt stattdessen vom Standardrouting zu externen Zielen ab.

Nachdem Sie OSPF aktiviert haben, müssen Sie die Ankündigung von OSPF-Routen konfigurieren. Zur Fehlerbehebung können Sie die OSPF-Ausbreitung einschränken. Sie können OSPF-Einstellungen anzeigen, um die Konfiguration zu überprüfen.

OSPF aktivieren und deaktivieren

Um OSPF zu aktivieren oder zu deaktivieren, müssen Sie entweder die CLI oder die GUI verwenden. Wenn OSPF aktiviert ist, startet Citrix ADC den OSPF-Prozess. Wenn OSPF deaktiviert ist, stoppt der Citrix ADC den OSPF-Routingprozess.

So aktivieren oder deaktivieren Sie das OSPF-Routing mithilfe der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

1. **ns-Funktion aktivieren OSPF**
2. **Deaktivieren Sie die NS-Funktion OSPF**

So aktivieren oder deaktivieren Sie das OSPF-Routing mithilfe der GUI:

1. Navigieren Sie zu **System** > **Einstellungen**, klicken Sie in der Gruppe **Modi und Funktionen** auf **Erweiterte Funktionen ändern**.
2. Wählen oder löschen Sie die **OSPF-Routing-Option** .

Werbung für OSPF Routes

OSPF ermöglicht es einem Upstream-Router, den Datenverkehr zwischen zwei identischen virtuellen Servern auszugleichen, die auf zwei eigenständigen Citrix ADC Appliances gehostet werden. Routenwerbung ermöglicht es einem Upstream-Router, Netzwerkentitäten zu verfolgen, die sich hinter dem Citrix ADC befinden.

So konfigurieren Sie OSPF für die Ankündigen von Routen mithilfe der VTYSH-Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Der globale Konfigurationsmodus wechselt.
router OSPF	Starten Sie den OSPF-Routing-Prozess und wechseln Sie in den Konfigurationsmodus für den Routing-Prozess.
network A.B.C.D/M area <0-4294967295>	Routing in einem IP-Netzwerk aktivieren.
redistribute static	Verteilen Sie statische Routen neu.
redistribute kernel	Verteilen Sie Kernel-Routen neu.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router OSPF
NS(config-router)# network 10.102.29.0/24 area 0
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
<!--NeedCopy-->
```


Beschränken von OSPF-Propagierungen

Wenn Sie Ihre Konfiguration beheben müssen, können Sie den Nur-Listen-Modus für ein bestimmtes VLAN konfigurieren.

So beschränken Sie die OSPF-Propagierung mithilfe der VTYSH-Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
router OSPF	Starten Sie den OSPF-Routing-Prozess und wechseln Sie in den Konfigurationsmodus für den Routing-Prozess.
passive-interface < vlan_name>	Unterdrückt Routing-Aktualisierungen an Schnittstellen, die an das angegebene VLAN gebunden sind.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router OSPF
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Prüfen der OSPF-Konfiguration

Sie können aktuelle OSPF-Nachbarn und OSPF-Routen anzeigen.

So zeigen Sie die OSPF-Einstellungen mithilfe der VTYSH-Befehlszeile an:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
sh OSPF neighbor	Zeigt aktuelle Nachbarn an.

Befehl	Spezifiziert
sh OSPF route	Zeigt OSPF-Routen an.

Beispiel:

```
>VTYSH
NS# sh ip OSPF neighbor
NS# sh ip OSPF route
<!--NeedCopy-->
```

Konfigurieren des ordnungsgemäßen Neustarts für OSPF

In einem Nicht-INC-Hochverfügbarkeits-Setup (HA), in dem ein Routingprotokoll konfiguriert wird, werden nach einem Failover Routing-Protokolle konvergiert und Routen zwischen dem neuen primären Knoten und den benachbarten Nachbarroutern werden erlernt. Es dauert einige Zeit, bis das Routenlernen abgeschlossen ist. Während dieser Zeit verzögert sich die Weiterleitung von Paketen, die Netzwerkleistung kann gestört werden und Pakete können verworfen werden.

Ein ordnungsgemäßer Neustart ermöglicht es einem HA-Setup während eines Failovers, seine benachbarten Router anzuweisen, die gelernten Routen des alten primären Knotens nicht aus ihren Routing-Datenbanken zu entfernen. Unter Verwendung der Routing-Informationen des alten primären Knotens beginnen der neue primäre Knoten und die angrenzenden Router sofort mit der Weiterleitung von Paketen, ohne die Netzwerkleistung zu beeinträchtigen.

> **Hinweis:**
>
> Ein ordnungsgemäßer Neustart wird für Hochverfügbarkeits-Setups im INC-Modus nicht unterstützt.

Um einen ordnungsmäßigen Neustart für OSPF mithilfe der VTYSH-Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
VTYSH	VTYSH	Ruft die VTYSH-Eingabeaufforderung
configure terminal	NS# configure terminal	Der globale Konfigurationsmodus wechselt.

Befehl	Beispiel	Beschreibung des Befehls
router-id <id>	NS(config)# router-id 1.1.1.1	Legt eine Routerkennung für die Citrix ADC Appliance fest. Diese Kennung ist für alle dynamischen Routingprotokolle festgelegt. Dieselbe ID muss im anderen Knoten in einer Hochverfügbarkeits-Einrichtung angegeben werden, die für einen ordnungsgemäßen Neustart eingerichtet ist, damit sie in der HA-Einrichtung ordnungsgemäß funktioniert.
ospf restart grace-period <1-1800>	NS(config)# ospf restart grace-period 170	Gibt die Nachfrist in Sekunden an, für die die Routen in den Hilfsgeräten beibehalten werden sollen. Standardwert: 120 Sekunden.
ospf restart helper max-grace-period <1-1800>	NS(config)# ospf restart helper max-grace-period 180	Dies ist ein optionaler Befehl zum Begrenzen der maximalen Nachfrist, für die sich die Citrix ADC Appliance im Hilfsmodus befindet. Wenn die Citrix ADC Appliance eine undurchsichtige LSA mit einer Gnade erhält, die größer als die festgelegte Max-Grace-Periode des Helfers ist, wird die LSA verworfen und der Citrix ADC wird nicht in den Hilfsmodus versetzt.

Befehl	Beispiel	Beschreibung des Befehls
router ospf	NS(config)# router ospf	Startet den OSPF-Routing-Prozess und wechselt in den Konfigurationsmodus für den Routing-Prozess.
network A.B.C.D/M area <0-4294967295>	NS(config-router)# network 192.0.2.0/24 area 0	Ermöglicht das Routing in einem IP-Netzwerk.
capability restart graceful	NS(config-router)# capability restart graceful	Ermöglicht einen ordnungsgemäßen Neustart des OSPF-Routing-Prozesses.
redistribute kernel	NS(config-router)# redistribute kernel	Verteilt Kernel-Routen neu.

Konfigurieren von BGP

December 7, 2021

Die Citrix ADC Appliance unterstützt BGP (RFC 4271). Die Funktionen von BGP auf dem Citrix ADC sind:

- Der Citrix ADC kündigt Routen an BGP-Peers an.
- Der Citrix ADC injiziert Hostrouten an virtuelle IP-Adressen (VIPs), die durch den Zustand der zugrunde liegenden virtuellen Server bestimmt werden.
- Der Citrix ADC generiert Konfigurationsdateien für die Ausführung von BGP auf dem sekundären Knoten nach einem Failover in einer HA-Konfiguration.
- Dieses Protokoll unterstützt IPv6-Routenaustausch.
- Unterstützung als Override im Border Gateway-Protokoll

Nachdem Sie BGP aktiviert haben, müssen Sie die Ankündigung von BGP-Routen konfigurieren. Zur Fehlerbehebung können Sie die BGP-Ausbreitung einschränken. Sie können die BGP-Einstellungen anzeigen, um die Konfiguration zu überprüfen.

Voraussetzungen für IPv6 BGP

Bevor Sie mit der Konfiguration von IPv6 BGP beginnen, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass Sie das IPv6-BGP-Protokoll verstehen.
- Aktivieren Sie die IPv6-Funktion.

BGP aktivieren und deaktivieren

Um BGP zu aktivieren oder zu deaktivieren, müssen Sie entweder die CLI oder die GUI verwenden. Wenn BGP aktiviert ist, startet die Citrix ADC Appliance den BGP-Prozess. Wenn BGP deaktiviert ist, stoppt die Appliance den BGP-Prozess.

So aktivieren oder deaktivieren Sie das BGP-Routing mithilfe der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- enable ns feature BGP
- disable ns feature BGP

So aktivieren oder deaktivieren Sie das BGP-Routing mithilfe der GUI:

1. Navigieren Sie zu System > Einstellungen, klicken Sie in der Gruppe Modi und Funktionen auf Erweiterte Funktionen ändern.
2. Wählen oder löschen Sie die Option BGP-Routing.

Werbung für IPv4-Strecken

Sie können die Citrix ADC Appliance so konfigurieren, dass Hostrouten an VIPs angekündigt und Routen an nachgeschaltete Netzwerke angekündigt werden.

So konfigurieren Sie BGP mit der VTYSH-Befehlszeile für die Ankündigen von IPv4-Routen:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
router BGP < ASnumber>	Autonomes BGP-System. < ASnumber>ist ein erforderlicher Parameter. Mögliche Werte: 1 bis 4.294.967.295.
Neighbor < IPv4 address> remote-as < as-number>	Aktualisieren Sie die IPv4-BGP-Nachbartabelle mit der lokalen IPv4-Adresse des Nachbarn im angegebenen autonomen System.
Adress-Familie IPv4	Rufen Sie den Konfigurationsmodus für die
Neighbor < IPv4 address> activate	Tauschen Sie Präfixe für die IPv4-Routerfamilie zwischen dem Peer und dem lokalen Knoten mithilfe der lokalen Linkadresse aus.

Befehl	Spezifiziert
redistribute kernel	Verteilen Sie Kernel-Routen neu.
redistribute static	Verteilen Sie statische Routen neu.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router BGP 5
NS(config-router)# Neighbor 10.102.29.170 remote-as 100
NS(config-router)# Address-family ipv4
NS(config-router-af)# Neighbor 10.102.29.170 activate
NS(config-router)# redistribute kernel
NS(config-router)# redistribute static
<!--NeedCopy-->
```

Voraussetzungen für IPv6 BGP

Bevor Sie mit der Konfiguration von IPv6 BGP beginnen, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass Sie das IPv6-BGP-Protokoll verstehen.
- Aktivieren Sie die IPv6-Funktion.

Werbung für IPv6 BGP-Routen

Border Gateway Protocol (BGP) ermöglicht es einem Upstream-Router, den Datenverkehr zwischen zwei identischen virtuellen Servern auszugleichen, die auf zwei eigenständigen Citrix ADC Appliances gehostet werden. Routenwerbung ermöglicht es einem Upstream-Router, Netzwerkentitäten zu verfolgen, die sich hinter dem Citrix ADC befinden.

So konfigurieren Sie BGP mit der VTYSH-Befehlszeile für die Ankündigen von IPv6-Routen:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.

Befehl	Spezifiziert
router BGP < ASnumber>	Autonomes BGP-System. < ASnumber>ist ein erforderlicher Parameter. Mögliche Werte: 1 bis 4.294.967.295.
Nachbar < IPv6 address> Remote-as < as-number>	Aktualisieren Sie die IPv6-BGP-Nachbartabelle mit der lokalen IPv6-Adresse des Nachbarn im angegebenen autonomen System.
Adress-Familie IPv6	Rufen Sie den Konfigurationsmodus für die
Nachbar < IPv6 address> aktiviert	Tauschen Sie Präfixe für die IPv6-Routerfamilie zwischen dem Peer und dem lokalen Knoten mithilfe der lokalen Linkadresse aus.
redistribute kernel	Verteilen Sie Kernel-Routen neu.
redistribute static	Verteilen Sie statische Routen neu.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router BGP 5
NS(config-router)# Neighbor a1bc::102 remote-as 100
NS(config-router)# Address-family ipv6
NS(config-router-af)# Neighbor a1bc::102 activate
NS(config-router)# redistribute kernel
NS(config-router)# redistribute static
<!--NeedCopy-->
```

Überprüfung der BGP-Konfiguration

Sie können VTYSH verwenden, um BGP-Einstellungen anzuzeigen.

So zeigen Sie die BGP-Einstellungen mit der VTYSH-Befehlszeile an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
VTYSH
You are now in the VTYSH command prompt. An output similar to the
    following appears:
```



```
NS170#
At the VTYSH command prompt, type:
NS170# sh ip BGP
NS170# sh BGP
NS170# sh ip BGP neighbors
NS170# sh ip BGP summary
NS170# sh ip BGP route-map <map-tag>
<!--NeedCopy-->
```

Unterstützung als Override im Border Gateway-Protokoll

Als Teil der BGP-Schleifenverhinderungsfunktionalität lässt der Router das Paket fallen, wenn ein Router ein BGP-Paket empfängt, das die Autonome Systemnummer (ASN) des Routers im Pfad für Autonome Systeme (AS) enthält. Es wird davon ausgegangen, dass das Paket vom Router stammt und den Ort erreicht hat, von dem es stammt.

Wenn ein Unternehmen über mehrere Standorte mit derselben ASN verfügt, führt die BGP-Schleifenprävention dazu, dass die Standorte mit einer identischen ASN nicht durch eine andere ASN verknüpft werden. Routing-Aktualisierungen (BGP-Pakete) werden verworfen, wenn sie von einem anderen Standort empfangen werden.

Um dieses Problem zu lösen, wurde dem ZeBOS BGP-Routingmodul des Citrix ADC die BGP AS-Override-Funktionalität hinzugefügt.

Wenn AS-Override für ein Peer-Gerät aktiviert ist und die Citrix ADC Appliance ein BGP-Paket zur Weiterleitung an den Peer empfängt und die ASN des Pakets mit der des Peers übereinstimmt, ersetzt die Appliance die ASN des BGP-Pakets vor der Weiterleitung des Pakets durch eine eigene ASN-Nummer.

Sie können AS-Override für einen bestimmten Nachbarn oder eine Gruppe von Nachbarn (Peer-Group) aktivieren, indem Sie die VTYSH-Befehlszeile verwenden.

So konfigurieren Sie BGP AS-Override für einen IPv4-Nachbarn mithilfe der VTYSH-Befehlszeile:

Befehl	Spezifiziert
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
Router BGP < ASnumber>	Autonomes BGP-System. < ASnumber>ist ein erforderlicher Parameter.
Nachbar < IPv4 address> Remote-As < as-number>	Aktualisieren Sie die IPv4-BGP-Nachbartabelle mit der IPv4-Adresse des Nachbarn im angegebenen autonomen System.

Befehl	Spezifiziert
Nachbar <IPv4 address>als Override	Aktiviert BGP als Override für den angegebenen Nachbarn.

```
    > VTYSH NS# configure terminal
    NS(config)# router BGP 200
    NS(config-router)# Neighbor 192.0.2.100 remote-as 100
    NS(config-router)# Neighbor 10.102.29.100 as-override
<!--NeedCopy-->
```

So konfigurieren Sie BGP AS-Override für eine IPv4-BGP-Peer-Gruppe mithilfe der VTYSH-Befehlszeile:

Befehl	Spezifiziert
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
Router BGP < ASnumber>	Autonomes BGP-System. < ASnumber>ist ein erforderlicher Parameter.
Nachbar-Peer-Group <peer group name>	Erstellen Sie eine BGP-Peer-Gruppe.
Nachbar-Peer-Gruppe <IPv4 address><peer group name>	Ordnen Sie Nachbarn der angegebenen Peer-Gruppe zu.
Nachbar <peer group name>Remote-as < as-number>	Aktualisieren Sie die IPv4-BGP-Nachbartabelle mit der IPv4-Adresse des Nachbarn im angegebenen autonomen System.
Nachbar <peer group name>als Override	Aktiviert BGP als Override für alle Nachbarn, die mit der angegebenen Peer-Gruppe verknüpft sind.

```
    > VTYSH NS# configure terminal
    NS(config)# router BGP 200
    NS(config-router)# neighbor external-peers-1 peer-group
    NS(config-router)# neighbor 192.0.2.101 peer-group external-peers-1
    NS(config-router)# neighbor 192.0.2.102 peer-group external-peers-1
    NS(config-router)# neighbor 192.0.2.103 peer-group external-peers-1
    NS(config-router)# Neighbor external-peers-1 remote-as 100
```



```
8     NS(config-router)# Neighbor external-peers-1 as-override
9  <!--NeedCopy-->
```

So konfigurieren Sie BGP AS-Override für einen IPv6-Nachbarn mithilfe der VTYSH-Befehlszeile:

Befehl	Spezifiziert
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
Router BGP < ASnumber>	Autonomes BGP-System. < ASnumber>ist ein erforderlicher Parameter.
Nachbar < IPv6 address> Remote-as < as-number>	Aktualisieren Sie die IPv4-BGP-Nachbartabelle mit der IPv4-Adresse des Nachbarn im angegebenen autonomen System.
Nachbar <IPv6 address>als Override	Aktiviert BGP als Override für den angegebenen Nachbarn.
Adress-Familie IPv6	Rufen Sie den Konfigurationsmodus für die
Nachbar < IPv6 address> aktiviert	Tauschen Sie Präfixe für die IPv6-Routerfamilie zwischen dem angegebenen Nachbarn und dem Citrix ADC mithilfe der lokalen Linkadresse aus.
Nachbar <IPv6 address>als Override	Aktiviert BGP als Override für den angegebenen Nachbarn.

```
1     > VTYSH NS# configure terminal
2     NS(config)# router BGP 200
3     NS(config-router)# Neighbor a1bc::102 remote-as 100
4     NS(config-router)# Neighbor a1bc::102 as-override
5     NS(config-router)# Address-family ipv6
6     NS(config-router-af)# Neighbor a1bc::102 activate
7     NS(config-router)# Neighbor a1bc::102 as-override
8  <!--NeedCopy-->
```

So konfigurieren Sie BGP AS-Override für IPv6-Peer-Group mithilfe der VTYSH-Befehlszeile:

Befehl	Spezifiziert
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
Router BGP < ASnumber>	Autonomes BGP-System. < ASnumber>ist ein erforderlicher Parameter.
Nachbar-Peer-Group<peer group name>	Erstellen Sie eine BGP-Peer-Gruppe.
Nachbar-Peer-Group<IPv6 address><peer group name>	Ordnen Sie der angegebenen Peer-Gruppe einen Nachbarn zu.
Nachbar <peer group name>Remote-as < as-number>	Aktualisieren Sie die IPv4-BGP-Nachbartabelle mit der IPv4-Adresse des Nachbarn im angegebenen autonomen System.
Nachbar <peer group name>als Override	Aktiviert BGP als Override für alle Nachbarn, die mit der angegebenen Peer-Gruppe verknüpft sind.
Adress-Familie IPv6	Rufen Sie den Konfigurationsmodus für die
Nachbar <peer group name>aktiviert	Tauschen Sie Präfixe für die IPv6-Routerfamilie zwischen den Nachbarn der angegebenen Peer-Gruppe und dem Citrix ADC mithilfe der lokalen Linkadresse aus.
Nachbar <peer group name>als Override	Aktiviert BGP als Override für alle Nachbarn, die mit der angegebenen Peer-Gruppe verknüpft sind.

```
1      > VTYSH NS# configure terminal
2      NS(config)# router BGP 200
3      NS(config-router)# neighbor external-peers-2 peer-group
4      NS(config-router)# neighbor 2001::1 peer-group external-peers-2
5      NS(config-router)# neighbor 2001::2 peer-group external-peers-2
6      NS(config-router)# Neighbor external-peers-2 remote-as 100
7      NS(config-router)# Neighbor external-peers-2 as-override
8      NS(config-router)# Address-family ipv6
9      NS(config-router-af)# Neighbor external-peers-2 activate
10     NS(config-router)# Neighbor external-peers-2 as-override
11 <!--NeedCopy-->
```


Ordnungsgemäßer Neustart

In einem Nicht-INC-Hochverfügbarkeits-Setup (HA), in dem ein Routingprotokoll konfiguriert wird, werden nach einem Failover Routing-Protokolle konvergiert und Routen zwischen dem neuen primären Knoten und den benachbarten Nachbarroutern werden erlernt. Es dauert einige Zeit, bis das Routenlernen abgeschlossen ist. Während dieser Zeit verzögert sich die Weiterleitung von Paketen, die Netzwerkleistung kann gestört werden und Pakete können verworfen werden.

Ein ordnungsgemäßer Neustart ermöglicht es einem HA-Setup während eines Failovers, seine benachbarten Router anzuweisen, die gelernten Routen des alten primären Knotens nicht aus ihren Routing-Datenbanken zu entfernen. Unter Verwendung der Routing-Informationen des alten primären Knotens beginnen der neue primäre Knoten und die angrenzenden Router sofort mit der Weiterleitung von Paketen, ohne die Netzwerkleistung zu beeinträchtigen.

> **Hinweis:**
>
> Ein ordnungsgemäßer Neustart wird für Hochverfügbarkeits-Setups im INC-Modus nicht unterstützt.

Konfigurieren des ordnungsgemäßen Neustarts für BGP

Um einen ordnungsmäßigen Neustart für BGP über die VTYSH-Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
VTYSH	VTYSH	Ruft die VTYSH-Eingabeaufforderung
configure terminal	NS# configure terminal	Der globale Konfigurationsmodus wechselt.

Befehl	Beispiel	Beschreibung des Befehls
router-id <ID>	NS(config)# router-id 1.1.1.1	Eine Routerkennung für die Citrix ADC Appliance. Diese Kennung ist für alle dynamischen Routingprotokolle festgelegt. Derselbe Bezeichner muss auf dem anderen Knoten in einem Hochverfügbarkeits-Setup angegeben werden, damit ein ordnungsgemäßer Neustart ordnungsgemäß funktioniert.
router bgp <AS-number>	NS(config)# router bgp 5	Ruft den BGP-Konfigurationsmodus auf
bgp graceful-restart	NS(config)# bgp graceful-restart	Ermöglicht einen ordnungsgemäßen Neustart des BGP-Routing-Prozesses.
bgp graceful-restart restart-time <1-1800>	NS(config-router)# bgp graceful-restart restart-time 170	Gibt die Nachfrist in Sekunden an, in der die Helfer-Router nach einem Failover auf eine TCP-Verbindung vom neuen primären Knoten warten. Für diese Zeitspanne bewahren die Helfer-Router die Routen bei.
bgp graceful-restart stalepath-time <1-1800>	NS(config-router)# bgp graceful-restart stalepath-time 180	Gibt die Zeit in Sekunden an, zu der die Citrix ADC Appliance im Hilfsmodus die veralteten Routen für den Neustart von Nachbarroutern beibehält. Der Standardwert beträgt 360 Sekunden.

Befehl	Beispiel	Beschreibung des Befehls
neighbor <IPv4 address of the peer router> remote-as <AS-number>	NS(config-router)# neighbor 192.0.2.30 remote-as 2	Richtet BGP-Peering mit dem angegebenen Nachbar-Router-Gerät ein.
neighbor <IPv4 address of the peer router> capability graceful-restart	NS(config-router)# neighbor 192.0.2.30 capability graceful-restart	Ermöglicht einen ordnungsgemäßen Neustart mit dem angegebenen Nachbarn.
redistribute kernel	NS(config-router)# redistribute kernel	Verteilt Kernel-Routen neu.

Konfigurieren des ordnungsgemäßen Neustarts für IPv6 BGP

Um einen ordnungsmäßigen Neustart für IPv6 BGP mithilfe der VTYSH-Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
VTYSH	VTYSH	Ruft die VTYSH-Eingabeaufforderung
configure terminal	NS# configure terminal	Der globale Konfigurationsmodus wechselt.
router-id <id>	NS(config)# router-id 1.1.1.1	Legt eine Routerkennung für die Citrix ADC Appliance fest. Diese Kennung ist für alle dynamischen Routingprotokolle festgelegt. Dieselbe ID muss im anderen Knoten in einem Hochverfügbarkeits-Setup angegeben werden, damit ein ordnungsgemäßer Neustart ordnungsgemäß funktioniert.
router bgp <AS-number>	NS(config)# router bgp 5	Ruft den Konfigurationsmodus für das BGP-Protokoll auf

Befehl	Beispiel	Beschreibung des Befehls
bgp graceful-restart	NS(config)# bgp graceful-restart	Ermöglicht einen ordnungsgemäßen Neustart des BGP-Routing-Prozesses.
bgp graceful-restart restart-time <1-1800>	NS(config-router)# bgp graceful-restart restart-time 170	Gibt die Nachfrist in Sekunden an, in der die Helfer-Router nach einem Failover auf eine TCP-Verbindung vom neuen primären Knoten warten. Für diese Zeitspanne bewahren die Helfer-Router die Routen bei. Der Standardwert beträgt 360 Sekunden.
bgp graceful-restart stalepath-time <1-1800>	NS(config-router)# bgp graceful-restart stalepath-time 180	Gibt die Zeit in Sekunden an, zu der die Citrix ADC Appliance im Hilfsmodus die veralteten Routen für den Neustart von Nachbarroutern beibehält. Der Standardwert beträgt 360 Sekunden.
neighbor <IPv6 address> remote-as <AS-number>	NS(config-router)# neighbor 2001:db8::10 remote-as 2	Richtet BGP-Peering mit dem angegebenen Nachbar-Router-Gerät ein.
address-family ipv6	NS(config-router)#address-family ipv6	Geht in den Konfigurationsmodus für die Adressfamilie.
neighbor <IPv6 address of the neighbor> activate	NS(config-router-af)#neighbor 2001:db8::10 activate	Ermöglicht den Austausch von Adressfamilien-Routen mit dem angegebenen Nachbar-Router-Gerät.
neighbor <IPv6 address of the neighbor> capability graceful-restart	NS(config-router-af)#neighbor 2001:db8::10 capability graceful-restart	Ermöglicht einen ordnungsgemäßen Neustart mit dem angegebenen Nachbar-Router-Gerät.

Befehl	Beispiel	Beschreibung des Befehls
redistribute kernel	NS(config-router-af)#redistribute kernel	Verteilt Kernel-Routen neu.
exit-address-family	NS(config-router-af)#exit-address-family	Beenden des Konfigurationsmodus der Adressfamilie

Konfigurieren der MD5-Authentifizierung für IPv4 BGP

Die Citrix ADC Appliance unterstützt die MD5-Authentifizierung für das Border Gateway Protocol (BGP). Wenn die Authentifizierung aktiviert ist, wird jedes TCP-Segment, das zu BGP gehört, das zwischen der Citrix ADC Appliance und ihrem Peer-Gerät ausgetauscht wird, nur überprüft und akzeptiert, wenn die Authentifizierung erfolgreich ist. Damit die Authentifizierung erfolgreich ist, müssen beide Peers mit demselben MD5-Kennwort konfiguriert sein. Wenn die Authentifizierung fehlschlägt, wird die BGP-Nachbarbeziehung nicht hergestellt. Die Unterstützung der MD5-Authentifizierung für BGP in der Citrix ADC Appliance ist mit RFC 2385 kompatibel.

Bevor Sie beginnen

Beachten Sie die folgenden Punkte, bevor Sie mit der Konfiguration der BGP-MD5-Authentifizierung beginnen:

- Stellen Sie sicher, dass Sie die verschiedenen Komponenten der BGP-MD5-Authentifizierung verstehen, die in RFC 2385 beschrieben sind.
- Die BGP-MD5-Authentifizierung wird für Citrix ADC Administratorpartitionen nicht unterstützt.
- Die BGP-MD5-Authentifizierung wird für IPv6-BGP-Konfigurationen nicht unterstützt.
- Die BGP-MD5-Authentifizierung wird sowohl für Citrix ADC-Clusterkonfigurationen als auch für Konfigurationen mit hoher Verfügbarkeit unterstützt.
- Aufgrund des folgenden Problems in FreeBSD empfiehlt Citrix, niedrige Keep-Live- und Hold-Time-Werte (z. B. 5 und 15) festzulegen und einen ordnungsgemäßen Neustart für eine BGP-Sitzung in einer Layer-2-Hochverfügbarkeitskonfiguration zu konfigurieren. Andernfalls kann es bei aktivierter MD5-Authentifizierung länger dauern, bis BGP nach einem Failover eine Verbindung mit dem Nachbarn wiederhergestellt hat.
  - Das letzte ACK von FreeBSD enthält keinen md5-Digest:
    * https://forums.freebsd.org/threads/11170/
    * http://support.pfsense.narkive.com/povrH5HI/bgp-md5-weird-behavior-when-connection-closes

Konfigurieren der MD5-Authentifizierung für IPv4 BGP

Um die MD5-Authentifizierung für IPv4 BGP mithilfe der VTYSH-Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
vtysh	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Der globale Konfigurationsmodus wechselt.
router bgp <AS-number>	Ruft den Konfigurationsmodus für das BGP-Protokoll auf <AS-number>ist eine autonome BGP-Systemnummer und ist ein erforderlicher Parameter.
Nachbar <neighbour IPv4 address>Remote-as < AS-number >	Aktualisiert die IPv4-BGP-Tabelle mit der IPv4-Adresse des Nachbarn im angegebenen autonomen System.
< neighbour IPv4 address >Nachbar-Kennwort < password in double quotes>	Konfiguriert die MD5-Authentifizierung für den angegebenen Nachbarn mit dem angegebenen MD5-Kennwort. Damit die MD5-Authentifizierung erfolgreich ist, müssen Sie dasselbe MD5-Kennwort auf der Citrix ADC Appliance und der Nachbar-Appliance konfigurieren.

```
1  > vtysh
2
3  ns# configure terminal
4
5  ns(config)#router bgp 5
6
7  ns(config-router)#neighbor 20.20.20.138 remote-as 1
8
9  ns(config-router)#neighbor 20.20.20.138 password  “secret”
10
11 ns(config-router)#redistribute kernel
12
13 ns(config-router)#exit
14
15 <!--NeedCopy-->
```


Konfigurieren von IPv6 RIP

October 5, 2021

IPv6 Routing Information Protocol (RIP) oder RIPng ist ein Distance Vector Protokoll. Dieses Protokoll ist eine Erweiterung von RIP zur Unterstützung von IPv6. Nachdem Sie IPv6 RIP aktiviert haben, müssen Sie die Ankündigung von IPv6 RIP-Routen konfigurieren. Zur Fehlerbehebung können Sie die IPv6-RIP-Propagierung einschränken. Sie können IPv6-RIP-Einstellungen anzeigen, um die Konfiguration zu überprüfen.

Voraussetzungen für IPv6-RIP

Bevor Sie mit der Konfiguration von IPv6 RIP beginnen, gehen Sie wie folgt vor:

- Vergewissern Sie sich, dass Sie das IPv6-RIP-Protokoll verstehen.
- Installieren Sie die IPv6pt-Lizenz auf der Citrix ADC Appliance.
- Aktivieren Sie die IPv6-Funktion.

Werbung für IPv6-RIP-Routen

IPv6 RIP ermöglicht einem Upstream-Router den Lastausgleich zwischen zwei identischen vServern, die auf zwei eigenständigen Citrix ADC Geräten gehostet werden. Routenankündigung ermöglicht es einem Upstream-Router, Netzwerkentitäten zu verfolgen, die sich hinter dem Citrix ADC befinden.

So konfigurieren Sie IPv6 RIP für die Ankündigung von IPv6-Routen mithilfe der VTYSH Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Gibt an
VTYSH	Zeigt die VTYSH Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
router ipv6 rip	Starten Sie den IPv6-RIP-Routingprozess und wechseln Sie in den Konfigurationsmodus für den Routingprozess.
redistribute static	Verteilen Sie statische Routen.
redistribute kernel	Verteilen Sie Kernel-Routen neu.

Beispiel:


```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 rip
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
<!--NeedCopy-->
```

IPv6-RIP-Propagierungen einschränken

Wenn Sie Probleme mit der Konfiguration beheben müssen, können Sie den Nur-Listenmodus auf einer beliebigen Schnittstelle konfigurieren.

So beschränken Sie die IPv6-RIP-Propagierung mithilfe der VTYSH Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Gibt an
VTYSH	Zeigt die VTYSH Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
router ipv6 rip	Starten Sie den IPv6-RIP-Routingprozess und wechseln Sie in den Konfigurationsmodus für den Routingprozess.
passive-interface < vlan_name>	Unterdrücken Sie Routing-Updates auf Schnittstellen, die an das angegebene VLAN gebunden sind.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 rip
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```


Überprüfen der IPv6-RIP-Konfiguration

Sie können VTYSH verwenden, um die IPv6-RIP-Routingtabelle und IPv6-RIP-Informationen für ein bestimmtes VLAN anzuzeigen.

So zeigen Sie die IPv6-RIP-Einstellungen mithilfe der VTYSH Befehlszeile an:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehle	Gibt an
VTYSH	Zeigt die VTYSH Eingabeaufforderung an.
sh ipv6 rip	Zeigt die aktualisierte IPv6-RIP-Routingtabelle an.
sh ipv6 rip interface <vlan_name>	Zeigt IPv6-RIP-Informationen für das angegebene VLAN an.

Beispiel:

```
NS# VTYSH
NS# sh ipv6 rip
NS# sh ipv6 rip interface VLAN0
<!--NeedCopy-->
```

Konfigurieren von IPv6 OSPF

December 3, 2021

IPv6 OSPF oder OSPF Version 3 (OSPF v3) ist ein Link-State-Protokoll, das zum Austausch von IPv6-Routing-Informationen verwendet wird. Nachdem Sie IPv6-OSPF aktiviert haben, müssen Sie die Ankündigung von IPv6-OSPF-Routen konfigurieren. Zur Fehlerbehebung können Sie die IPv6-OSPF-Ausbreitung einschränken. Sie können IPv6-OSPF-Einstellungen anzeigen, um die Konfiguration zu überprüfen.

Voraussetzungen für IPv6 OSPF

Bevor Sie mit der Konfiguration von IPv6 OSPF beginnen, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass Sie das IPv6-OSPF-Protokoll verstehen.

- Installieren Sie die IPv6PT-Lizenz auf der Citrix ADC Appliance.
- Aktivieren Sie die IPv6-Funktion.

Werbung für IPv6-Strecken

IPv6-OSPF ermöglicht einem Upstream-Router den Lastenausgleich zwischen zwei identischen vServern, die auf zwei eigenständigen Citrix ADC-Geräten gehostet werden. Routenwerbung ermöglicht es einem Upstream-Router, Netzwerkentitäten zu verfolgen, die sich hinter dem Citrix ADC befinden.

So konfigurieren Sie IPv6-OSPF für die Beankündigen von IPv6-Routen mithilfe der VTYSH-Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehle	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
Router ipv6 OSPF	Starten Sie den IPv6-OSPF-Routing-Prozess und wechseln Sie in den Konfigurationsmodus für den Routing-Prozess.
redistribute static	Verteilen Sie statische Routen neu.
redistribute kernel	Verteilen Sie Kernel-Routen neu.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 OSPF
NS(config-router)# redistribute static
NS(config-router)# redistribute kernel
<!--NeedCopy-->
```

Beschränken von IPv6-OSPF-Propagierungen

Wenn Sie Ihre Konfiguration beheben müssen, verwenden Sie VTYSH, um den Nur-Listen-Modus für ein bestimmtes VLAN zu konfigurieren.

So beschränken Sie die IPv6-OSPF-Weitergabe mithilfe der VTYSH-Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehle	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
Router ipv6 OSPF	Starten Sie den IPv6-OSPF-Routing-Prozess und wechseln Sie in den Konfigurationsmodus für den Routing-Prozess.
passiv-schnittstelle < vlan_name >	Unterdrückt Routing-Aktualisierungen an Schnittstellen, die an das angegebene VLAN gebunden sind.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router ipv6 OSPF
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Überprüfung der IPv6-OSPF-Konfiguration

Sie verwenden VTYSH, um aktuelle IPv6-OSPF-Nachbarn und IPv6-OSPF-Routen anzuzeigen.

So zeigen Sie die IPv6-OSPF-Einstellungen mithilfe der VTYSH-Befehlszeile an:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Spezifiziert
VTYSH	Zeigt VTYSH-Eingabeaufforderung an.
sh ipv6 OSPF Nachbar	Zeigt aktuelle Nachbarn an.
sh ipv6 OSPF-Route	IPv6-OSPF-Routen anzeigen.

Beispiel:


```
>VTYSH
NS# sh ipv6 OSPF neighbor
NS# sh ipv6 OSPF route
<!--NeedCopy-->
```

OSPFv3-Authentifizierung

Um die Integrität, Datenherkunftsauthentifizierung und Datenvertraulichkeit von OSPFv3-Paketen sicherzustellen, muss die OSPFv3-Authentifizierung auf OSPFv3-Peers konfiguriert werden.

Die Citrix ADC Appliance unterstützt die OSPFv3-Authentifizierung und ist teilweise mit RFC 4552 kompatibel. Die OSPFv3-Authentifizierung basiert auf den beiden IPSec-Protokollen: Authentication Header (AH) und Encapsulating Security Payload (ESP). Die Citrix ADC Appliance unterstützt nur das AH-Protokoll für die OSPFv3-Authentifizierung.

Die OSPFv3-Authentifizierung verwendet manuell definierte IPSec-Sicherheitszuordnungen (SAs) zwischen den OSPFv3-Peers und stützt sich nicht auf das IKE-Protokoll für die Bildung dynamischer SAs. Manuelle SAs definieren die Sicherheitsparameter Index (SPI) -Werte, Algorithmen und Schlüssel, die zwischen den Peers verwendet werden sollen. Manuelle SAs erfordern keine Verhandlungen zwischen den Peers. Daher muss dieselbe SA für beide Peers definiert werden.

Sie können die OSPFv3-Authentifizierung in einem VLAN oder für einen OSPFv3-Bereich konfigurieren. Bei der Konfiguration für ein VLAN werden die Einstellungen auf alle Schnittstellen angewendet, die Mitglieder des VLAN sind. Wenn Sie die OSPFv3-Authentifizierung für einen OSPF-Bereich konfigurieren, werden die Einstellungen auf alle VLANs in diesem Bereich angewendet. Die Einstellungen werden wiederum auf alle Schnittstellen angewendet, die Mitglieder dieser VLANs sind. Diese Einstellungen gelten nicht für Mitglieds-VLANs, für die Sie die OSPFv3-Authentifizierung direkt konfiguriert haben.

Beachten Sie die folgenden Punkte und Einschränkungen, bevor Sie die OSPFv3-Authentifizierung auf einer Citrix ADC Appliance konfigurieren:

- Stellen Sie sicher, dass Sie die verschiedenen Komponenten der OSPFv3-Authentifizierung verstehen, die in RFC 4552 beschrieben sind.
- Für die OSPFv3-Authentifizierung wird nur das Authentifizierungs-Header-Protokoll unterstützt. Capsulating Security Payload (ESP) wird nicht unterstützt.
- Sie müssen eine SA mit derselben Einstellung auf der Peer-Schnittstelle definieren.
- Das erneute Keying von manuellen Tasten wird nicht unterstützt.

So konfigurieren Sie die OSPFv3-Authentifizierung auf einem VLAN über die VTYSH Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angezeigten Reihenfolge ein: VLAN-Befehle zur OspFv3-Authentifizierung.

Beispiel:

```
> VTYSH NS# configure terminal
NS(config)# interface vlan2
NS(config-if)# ipv6 ospf authentication ipsec spi 256 md5 123456789
    ABCDEF0123456789ABCDEF0
<!--NeedCopy-->
```

So konfigurieren Sie die OSPFv3-Authentifizierung in einem OSPF-Bereich über die VTYSH Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angezeigten Reihenfolge ein: OSPFv3-Authentifizierung OSPF-Bereichsbefehle.

Beispiel:

```
> VTYSH NS# configure terminal
ns(config)#router ipv6 ospf 30
ns(config-router)# area 1 authentication ipsec spi 256
    md5123456789ABCDEF0123456789ABCDEF0
<!--NeedCopy-->
```

Konfigurieren des ordnungsgemäßen Neustarts für IPv6 OSPF

In einem Nicht-INC-Hochverfügbarkeits-Setup (HA), in dem ein Routingprotokoll konfiguriert wird, werden nach einem Failover Routing-Protokolle konvergiert und Routen zwischen dem neuen primären Knoten und den benachbarten Nachbarroutern werden erlernt. Es dauert einige Zeit, bis das Routenlernen abgeschlossen ist. Während dieser Zeit verzögert sich die Weiterleitung von Paketen, die Netzwerkleistung kann gestört werden und Pakete können verworfen werden.

Ein ordnungsgemäßer Neustart ermöglicht es einem HA-Setup während eines Failovers, seine benachbarten Router anzuweisen, die gelernten Routen des alten primären Knotens nicht aus ihren Routing-Datenbanken zu entfernen. Unter Verwendung der Routing-Informationen des alten primären Knotens beginnen der neue primäre Knoten und die angrenzenden Router sofort mit der Weiterleitung von Paketen, ohne die Netzwerkleistung zu beeinträchtigen.

> **Hinweis:**
>
> Ein ordnungsgemäßer Neustart wird für Hochverfügbarkeits-Setups im INC-Modus nicht unterstützt.

Um einen ordnungsmäßigen Neustart für IPv6-OSPF mithilfe der VTYSH-Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
VTYSH	> VTYSH	Ruft die VTYSH-Eingabeaufforderung
configure terminal	NS# configure terminal	Der globale Konfigurationsmodus wechselt.
router-id id>	NS(config)#router-id 1.1.1.1	Legt eine Routerkennung für die Citrix ADC Appliance fest. Diese Kennung ist für alle dynamischen Routingprotokolle festgelegt. Dieselbe ID muss im anderen Knoten in einer Hochverfügbarkeits-Einrichtung angegeben werden, die für einen ordnungsgemäßen Neustart eingerichtet ist, damit sie in der HA-Einrichtung ordnungsgemäß funktioniert.
IPv6ospf restart grace-period <1-1800>	NS(config)# IPv6ospf restart grace-period 170	Gibt die Nachfrist in Sekunden an, für die die Routen in den Hilfsgeräten beibehalten werden sollen. Standardwert: 120 Sekunden.

Befehl	Beispiel	Beschreibung des Befehls
IPv6 ospf restart helper max-grace-period <1-1800>	NS(config)# IPv6 ospf restart helper max-grace-period 180	Dies ist ein optionaler Befehl zum Begrenzen der maximalen Nachfrist, für die sich die Citrix ADC Appliance im Hilfsmodus befindet. Wenn die Citrix ADC Appliance eine undurchsichtige LSA mit einer Gnade erhält, die größer als die festgelegte Max-Grace-Periode des Helfers ist, wird die LSA verworfen und der Citrix ADC wird nicht in den Hilfsmodus versetzt.
interface <VLANID>	NS(config)#interface vlan3	Ruft den VLAN-Konfigurationsmodus auf
ipv6 router ospf area <area_id> tag <tag_id>	NS(config-if)#ipv6 router ospf area 0 tag 1	Startet den IPv6-OSPF-Routing-Prozess in einem VLAN.
exit	NS(config-if)#exit	Beenden Sie den VLAN-Konfigurationsmodus.
router ipv6 ospf	NS(config)# router ipv6 ospf 1	Startet den IPv6-OSPF-Routing-Prozess und wechselt in den Konfigurationsmodus für den Routing-Prozess.
capability restart graceful	NS(config-router)#capability restart graceful	Ermöglicht einen ordnungsgemäßen Neustart des IPv6-OSPF-Routing-Prozesses.
redistribute kernel	NS(config-router)# redistribute kernel	Verteilt Kernel-Routen neu.

Konfigurieren von ISIS

October 5, 2021

Die Citrix ADC Appliance unterstützt das dynamische Routingprotokoll Intermediate System-to-Intermediate System (IS-IS oder ISIS). Dieses Protokoll unterstützt sowohl IPv4- als auch IPv6-Routenaustausch. IS⊠IS ist ein Verbindungsstatusprotokoll und ist daher weniger anfällig für Routingschleifen. Mit den Vorteilen einer schnelleren Konvergenz und der Fähigkeit, größere Netzwerke zu unterstützen, kann ISIS in Internet Service Provider (ISP) -Netzwerken sehr nützlich sein.

Voraussetzungen für die Konfiguration von ISIS

Bevor Sie mit der Konfiguration von ISIS beginnen, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass Sie das ISIS-Protokoll verstehen.
- Aktivieren Sie für IPV6-Routen:
  - IPv6-Protokollübersetzungsfunktion.
  - IPv6-Option Dynamisches Routing auf den VLANs, auf denen Sie das ISIS-Protokoll ausführen möchten.

ISIS aktivieren

Verwenden Sie eines der folgenden Verfahren, um die ISIS-Routingfunktion auf der Citrix ADC Appliance zu aktivieren.

So aktivieren Sie das ISIS-Routing mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

enable ns feature ISIS

So aktivieren Sie das ISIS-Routing mit der GUI:

1. Navigieren Sie zu System > Einstellungen, klicken Sie in der Gruppe Modi und Funktionen auf Erweiterte Funktionen ändern.
2. Aktivieren oder deaktivieren Sie die Option ISIS-Routing.

ISIS-Routing-Prozess erstellen und auf einem VLAN starten

Um einen ISIS-Routingprozess zu erstellen, müssen Sie die VTYSH Befehlszeile verwenden.

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Beschreibung
VTYSH	Zeigt die VTYSH Eingabeaufforderung an.
configure terminal	Wechselt in den globalen Konfigurationsmodus.
Router-ISIS-[Tag]	Erstellt einen ISIS-Routing- und Konfigurationsmodus für den Routingprozess.
net XX….XXXX.YYYY.YYYY.YYYY.00	Gibt einen NET-Wert für den Routing-Prozess an, wobei: ·**XX.. .XXXX** die Bereichsadresse (kann 1-13 Byte sein), ·**YYYY.YYYY.YYYY** die System-ID (6 Byte) und ·**00** der N-Selektor (1 Byte) ist.
is-type (level-1|level-1-2|level-2-only)	Legt den ISIS-Routingprozess auf die angegebene Weiterleitungsebene fest. Standard: level-1-2.
ns IPv6-routing	Startet den dynamischen IPv6-Routing-Daemon.
interface <vlan_name>	Wechselt in den VLAN-Konfigurationsmodus.
ip router ISIS	Aktiviert den ISIS-Routing-Prozess im VLAN für IPv4-Routenaustausch.
ipv6 router ISIS	Aktiviert den ISIS-Routing-Prozess im VLAN für IPv6-Routenaustausch.

Beispiel:

```
> VTYSH
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# net 15.aabb.ccdd.0097.00
NS(config-router)# is-type level-1
NS(config-router)# exit
NS(config)# ns IPv6-routing
NS(config)# interface vlan0
NS(config-if)#  ip router isis 11
NS(config-if)# ipv6 router isis 11
<!--NeedCopy-->
```


Routen ankündigen

Routenankündigung ermöglicht es einem Upstream-Router, Netzwerkentitäten zu verfolgen, die sich hinter der Citrix ADC Appliance befinden.

So konfigurieren Sie ISIS für die Ankündigung von Routen mithilfe der VTYSH Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Beschreibung
VTYSH	Zeigt die VTYSH Eingabeaufforderung an.
configure terminal	Wechselt in den globalen Konfigurationsmodus.
Router ISIS [Tag]	Startet die ISIS-Routinginstanz und wechselt in den Konfigurationsmodus für den Routingprozess.
redistribute connected (level-1 or level-1-2 or level-2)	Verteilt verbundene Routen neu, wobei: **level-1**: Verteilen Sie verbundene Routen in Level-1, **level-1-2**: Verteilen Sie verbundene Routen in Level-1 und Level-2, **level-2**: Verteilen Sie verbundene Routen in Level-2.
redistribute kernel (level-1 or level-1-2 or level-2)	Verteilt Kernel-Routen neu, wobei: **level-1**: Kernel-Routen in Level-1 umverteilen, **level-1-2**: Kernel-Routen neu in Level-1 und Level-2 verteilen, **level-2**: Kernel-Routen neu in Level-2 verteilen.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# redistribute connected level-1
NS(config-router)# redistribute kernel level-1
<!--NeedCopy-->
```


ISIS-Propagierungen einschränken

Wenn Sie Probleme mit der Konfiguration beheben müssen, können Sie den Nur-Liste-Modus auf einem beliebigen VLAN konfigurieren.

So beschränken Sie die ISIS-Propagierung mithilfe der VTYSH Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Beschreibung
VTYSH	Zeigt die VTYSH Eingabeaufforderung an.
configure terminal	Wechselt in den globalen Konfigurationsmodus.
router isis [Tag]	Wechselt in den Konfigurationsmodus für den Routing-Prozess.
passive-interface <vlan_name>	Unterdrückt Routingaktualisierungen auf Schnittstellen, die an das angegebene VLAN gebunden sind.

Beispiel:

```
>VTYSH
NS# configure terminal
NS(config)# router isis 11
NS(config-router)# passive-interface VLAN0
<!--NeedCopy-->
```

Überprüfen der ISIS-Konfiguration

Sie können VTYSH verwenden, um die ISIS-Routingtabelle und ISIS-Informationen für ein spezifiziertes VLAN anzuzeigen.

So zeigen Sie die ISIS-Einstellungen mithilfe der VTYSH Befehlszeile an:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehle	Beschreibung
VTYSH	Zeigt die VTYSH Eingabeaufforderung an.

Befehle	Beschreibung
show ip isis route	Zeigt die aktualisierte IPv4-ISIS-Routingtabelle an.
show ipv6 isis route	Zeigt die aktualisierte IPv6-ISIS-Routingtabelle an.
sh isis interface <vlan_name>	Zeigt IPv6-ISIS-Informationen für das angegebene VLAN an.

Beispiel:

```
NS# VTYSH
NS#  show ip isis route
NS#  show ipv6 isis route
NS# sh isis interface VLAN0
<!--NeedCopy-->
```

Installieren von Routen in die Citrix ADC Routingtabelle

October 5, 2021

Die Citrix ADC Appliance kann Routen verwenden, die von verschiedenen Routingprotokollen gelernt wurden, nachdem Sie die Routen in der Routingtabelle der Appliance installiert haben.

So installieren Sie verschiedene Routen in die interne Routingtabelle mithilfe der VTYSH Befehlszeile:

Geben Sie an der Befehlszeilenschnittstelle die folgenden Befehle für die zu installierenden Routen ein:

Befehle	Gibt an
VTYSH	Zeigt die VTYSH Eingabeaufforderung an.
configure terminal	Geben Sie den globalen Konfigurationsmodus ein.
ns Route-Installation Standard	Installieren Sie IPv4-Standardrouten in die interne Routingtabelle.
ns Route-Installations-RIP	Installieren Sie IPv4-RIP-spezifische Routen in der internen Routingtabelle.

Befehle	Gibt an
ns Route-Install BGP	Installieren Sie IPv4 BGP-spezifische Routen in der internen Routingtabelle.
ns Route-Installation OSPF	Installieren Sie IPv4-OSPF-spezifische Routen in der internen Routingtabelle.
ns Route-Installation IPv6-Standard	Installieren Sie IPv6-Standardrouten in die interne Routingtabelle.
ns Route-Installation von IPv6 RIP	Installieren Sie IPv6-RIP-spezifische Routen in der internen Routingtabelle.
ns Route-Installation von IPv6 BGP	Installieren Sie IPv6 BGP-spezifische Routen in die interne Routingtabelle.
ns Route-Installation von IPv6 OSPF	Installieren Sie IPv6-OSPF-spezifische Routen in die interne Routingtabelle.

Beispiel:

```
>VTYSH
NS# configure terminal
NS# ns route-install Default
NS(config)# ns route-install RIP
NS(config)# ns route-install BGP
NS(config)# ns route-install OSPF
NS# ns route-install IPv6 Default
NS(config)# ns route-install IPv6 RIP
NS(config)# ns route-install IPv6 BGP
NS(config)# ns route-install IPv6 OSPF
<!--NeedCopy-->
```

Werbung von SNIP und VIP Routen zu selektiven Gebieten

October 5, 2021

Um einige SNIP-Adressen in selektiven Bereichen anzukündigen, können die Aktivierung des DRADV-Modus oder die Weiterverteilung von Verbindungen ZEBOS-Operationen nicht verwendet werden. Dies liegt daran, dass diese Operationen alle verbundenen Routen an ZEBOs senden. Außerdem ist das Hinzufügen von statischen Dummy-Routen in ZEBOs für die erforderlichen Subnetze oder das

Hinzufügen von ACLs in ZEBOs, um unerwünschte verbundene Routen zu filtern, eine umständliche und mühsame Aufgabe.

Die Netzwerkroute und die Tag-Optionen beheben dieses Problem. Sie können die Option Netzwerkroute für nur eine SNIP-Adresse pro Subnetz aktivieren. Die verbundene Route für diese SNIP-Adresse wird als Kernelroute an ZebOS gesendet.

Für VIP- und SNIP-Adressen kann Tag eine ganze Zahl von 1 bis 4294967295 zugewiesen werden. Dieser Parameter kann nur festgelegt werden, wenn Hostroute oder Netzwerkroute für VIP- oder SNIP-Adressen aktiviert ist. Der Tag-Wert, der mit VIP- und SNIP-Adressen verknüpft ist, wird zusammen mit ihren Routen an ZEBOs gesendet. Tags mit unterschiedlichen Werten können für VIP- und SNIP-Routen eingestellt werden. Diese Tag-Werte können dann in Routenkarten in ZEBOs abgeglichen und in selektive Bereiche beworben werden.

SNIP-Routen in selektive Bereiche bewerben

So konfigurieren Sie die Netzwerk-Routen- und Tag-Parameter einer SNIP-Adresse mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- Wenn Sie eine neue SNIP-Adresse hinzufügen:
  - **add ns ip** <IPAddress>@ <netmask> -**type SNIP** -**networkroute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **ns ip anzeigen** <IPAddress>
- Wenn Sie eine vorhandene SNIP-Adresse neu konfigurieren:
  - **set ns ip** <IPAddress>@ <netmask> -**type SNIP** - **networkroute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **ns ip anzeigen** <IPAddress>

So konfigurieren Sie die Netzwerk-Routen- und Tag-Parameter einer SNIP-Adresse mit der GUI:

1. Navigieren Sie zu **System**> **Netzwerk**> **IPs**> **IPv4s**.
2. Legen Sie die Parameter **Netzwerkroute** und **Tag** fest, während Sie eine Subnetz-IP (SNIP) -Adresse hinzufügen oder eine vorhandene Subnetz-IP-Adresse ändern.

Bewerben Sie VIP-Routen in selektive Bereiche

So konfigurieren Sie die Host-Routen- und Tag-Parameter einer VIP-Adresse mit der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehlssätze ein.

- Wenn Sie eine neue VIP-Adresse hinzufügen:
  - **add ns ip** <IPAddress>@ <netmask> -**type VIP** -**hostRoute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>

  - **ns ip anzeigen** <IPAddress>

- Wenn Sie eine vorhandene VIP-Adresse neu konfigurieren:
  - **set ns ip** <IPAddress>@ <netmask> -**type VIP** -**hostRoute** (**ENABLED** | **DISABLED**) -**tag** <positive_integer>
  - **ns ip anzeigen** <IPAddress>

So konfigurieren Sie die Netzwerk-Routen- und Tag-Parameter einer VIP-Adresse mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs** > **IPv4s**.
2. Legen Sie die **Hostroute** und **Tag-Parameter** fest, während Sie eine VIP-Adresse hinzufügen oder eine vorhandene VIP-Adresse ändern.

Bidirektionale Weiterleitungserkennung konfigurieren

October 5, 2021

Das bidirektionale Forwarding Detection (BFD) -Protokoll ist ein Mechanismus zur schnellen Erkennung von Ausfällen von Weiterleitungspfaden. BFD erkennt Pfadfehler in Millisekunden. BFD wird mit dynamischen Routing-Protokollen verwendet.

Im BFD-Vorgang tauschen Routing-Peers BFD-Pakete in einem ausgehandelten Intervall aus. Wenn ein Paket innerhalb des ausgehandelten Intervalls plus Gnadenintervalls nicht von einem Peer empfangen wird, gilt der Peer als tot und eine Benachrichtigung wird an die Gruppe der registrierten Routing-Protokolle gesendet. Die Routingprotokolle wiederum berechnen den besten Pfad neu und programmieren die Routingtabelle neu. BFD unterstützt im Vergleich zu den Timern, die von den Routingprotokollen bereitgestellt werden, ein geringeres Zeitintervall, was zu einer schnelleren Erkennung von Fehlern führt.

Die Citrix ADC Appliance unterstützt BFD für die folgenden Routingprotokolle: BGP (IPv4 und IPv6), OSPFv2 (IPv4) und OSPFv3 (IPv6). Die BFD-Unterstützung in der Citrix ADC Appliance ist mit RFCs 5880, 5881 und 5883 kompatibel.

Zu berücksichtigende Punkte für die Konfiguration der bidirektionalen Weiterleitungserkennung

Bevor Sie mit der Konfiguration von BFD beginnen, sollten Sie die folgenden Punkte beachten:

- Stellen Sie sicher, dass Sie die verschiedenen Komponenten von BFD kennen, die in RFCs 5880, 5881 und 5883 beschrieben sind.
- BFD auf einer Citrix ADC Appliance wird für die folgenden Routingprotokolle unterstützt:
  - BGP (IPv4 und IPv6)

  - OSPFv2 (IPv4)
  - OSPFv3 (IPv6)
- BFD auf einer Citrix ADC Appliance wird für die folgenden Routingprotokolle nicht unterstützt:
  - ISIS
  - RIP (IPv4)
  - RipNG (IPv6)
- Die folgenden BFD-Funktionen werden auf einer Citrix ADC Appliance nicht unterstützt:
  - BFD-Echo-Modus
  - BFD-Authentifizierung
  - Asynchroner BFD-Bedarfsmodus
- Die Mindestwerte für BFD-Intervall und BFD Rx-Timer betragen 100 Millisekunden.
- Wenn BFD in einer Topologie mit gemeinsam genutzten IP-Adressen verwendet wird (z. B. ein Layer-2-Hochverfügbarkeitssetup mit SNIP-Adressen oder ein Cluster-Setup mit gestreiften IP-Adressen), bringt BFD die aktiven Sitzungen während eines Failovers herunter, da die BFD-Fehlererkennungszeit (die Reihenfolge der Millisekunden) geringer ist als die Failover-Erkennungsintervall (3-4 Sekunden). Daher empfiehlt Citrix die Verwendung von Graceful Neustart in Layer-2-HA-Topologien, da die Routen während des Failoverprozesses beibehalten werden.

Konfigurationsschritte

Die Konfiguration von BFD auf einer Citrix ADC Appliance umfasst die folgenden Aufgaben:

- Konfigurieren von BFD-Parametern
- Konfigurieren der BFD-Unterstützung für dynamische Routing-Protokolle

Konfigurieren von BFD-Parametern

Die Citrix ADC Appliance bietet separate BFD-Sitzungsparameter für Einzelhop-Sitzungen, IPv4-Mehrfachhop-Sitzungen und IPv6-Mehrfachhop-Sitzungen. Wenn Sie keine BFD-Parameter für einen Sitzungstyp konfigurieren, werden die Standardwerte für diese Sitzung angewendet.

Der Standardwert jedes BFD-Parameters ist für Einzelhop-Sitzungen, IPv4-Mehrfachhop-Sitzungen und IPv6-Mehrfachhop-Sitzungen gleich. In der folgenden Tabelle wird der Standardwert jedes BFD-Parameters angezeigt.

BFD-Parametername	Standardwert
Intervall	750 Millisekunden
Mindestens Rx	500 Millisekunden

BFD-Parametername	Standardwert
Multiplikator	3

> **Wichtig:**
>
> Mellanox-NICs in einer Citrix Appliance benötigen etwa 1500 ms, um zu initialisieren. Sie müssen die BFD-Timer für eine Citrix ADC Appliance mit Mellanox-NICs auf mehr als 1500 ms einstellen. Citrix empfiehlt, die BFD-Timer auf 3000 ms einzustellen:
>
> - Intervall Tx = 600 ms
> - Mindest Rx = 600 ms
> - Multipler = 5

Konfigurieren von BFD-Parametern für eine Single-Hop-Sitzung

Um BFD-Parameter für eine Single-Hop-Sitzung über die VTYSH Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Gibt an
`vtysh`	Zeigt die VTYSH Eingabeaufforderung an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`interface vlan ID>`	Geben Sie den Schnittstellenkonfigurationsmodus ein.
`bfd singlehop-peer interval <num> minrx <num> multiplier <num>`	Konfigurieren Sie die BFD-Parameter auf der angegebenen Schnittstelle.

Beispielkonfiguration:

```
> vtysh

ns# configure terminal

ns(config)# interface vlan3

ns(config-if)# bfd singlehop-peer interval 200 minrx 200 multiplier 5

```



```
9  ns(config-if)# exit
10 <!--NeedCopy-->
```

Konfigurieren von BFD-Parametern für IPv4-Mehrfachhop-Sitzungen

Um BFD-Parameter für IPv4-Multiple-Hop-Sitzungen über die VTYSH Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Gibt an
`vtysh`	Zeigt die VTYSH Eingabeaufforderung an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`bfd multihop-peer <ipv4addr> interval <num> minrx <num> multiplier <num>`	Konfigurieren Sie die BFD-Parameter für IPv4-Multiple-Hops-Sitzungen.

Beispielkonfiguration:

```
1      > vtysh
2
3      ns# configure terminal
4
5      ns(config)# bfd multihop-peer 20.20.20.138 interval 300 minrx 300
           multiplier 5
6
7      ns(config)# exit
8  <!--NeedCopy-->
```

Konfigurieren von BFD-Parametern für IPv6-Mehrfachhop-Sitzungen

Um BFD-Parameter für IPv6-Multiple-Hop-Sitzungen über die VTYSH Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Gibt an
`vtysh`	Zeigt die VTYSH Eingabeaufforderung an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.

Befehl	Gibt an
`bfd multihop-peer ipv6 <ipv6addr> interval <num> minrx <num> multiplier <num>`	Konfigurieren Sie die BFD-Parameter für IPv6-Multiple-Hops-Sitzungen.

Beispielkonfiguration:

```
1      > vtysh
2
3      ns(config)# bfd multihop-peer ipv6 20fe:125::138 interval 500 minrx
           500 multiplier 5
4
5      ns(config)# exit
6  <!--NeedCopy-->
```

Konfigurieren der BFD-Unterstützung für dynamische Routing-Protokolle

Sie können BFD für ein dynamisches Routingprotokoll für eine Art von Sitzung mit einem Peer aktivieren. Zum Beispiel Single Hop und Multiple Hops. Die Citrix ADC Appliance wendet die entsprechenden BFD-Parametereinstellungen auf die Sitzung an.

Konfigurieren von BFD für eine IPv4 BGP Single Hop Session

Um BFD für eine IPv4 BGP Single Hop-Sitzung über die `VTYSH` Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Gibt an
`vtysh`	Zeigt die `VTYSH` Eingabeaufforderung an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`router bgp <asnumber>`	Autonome BGP-Anlage. `asnumber` ist ein erforderlicher Parameter.
`neighbor <ipv4addr> remote-as <num>`	Aktualisieren Sie die IPv4 BGP-Tabelle mit der IPv4-Adresse des Nachbarn im angegebenen autonomen System.

Befehl	Gibt an
`neighbor <ipv4addr> fall-over bfd`	Aktivieren Sie BFD für den angegebenen Nachbarn.

Beispielkonfiguration:

```
1      > vtysh
2
3      ns# configure terminal
4
5      ns(config)#router bgp 1
6
7      ns(config-router)#neighbor 20.20.20.138 remote-as 1
8
9      ns(config-router)#neighbor 20.20.20.138 fall-over bfd
10
11     ns(config-router)#redistribute kernel
12
13     ns(config-router)#exit
14 <!--NeedCopy-->
```

Konfigurieren von BFD für eine IPv4 BGP Multiple Hop Session

Um BFD für eine IPv4 BGP Multiple-Hop-Sitzung über die VTYSH Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Gibt an
`vtysh`	Zeigt die VTYSH Eingabeaufforderung an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`router bgp <asnumber>`	Autonome BGP-Anlage. `asnumber` ist ein erforderlicher Parameter.
`neighbor <ipv4addr> remote-as <num>`	Aktualisieren Sie die IPv4 BGP-Tabelle mit der IPv4-Adresse des Nachbarn im angegebenen autonomen System.

Befehl	Gibt an
`neighbor <ipv4addr> fall-over bfd multihop`	Aktivieren Sie BFD für den angegebenen Nachbarn.

Beispielkonfiguration:

```
    > vtysh

    ns# configure terminal

    ns(config)#router bgp 1

    ns(config-router)#neighbor 20.20.20.138 remote-as 1

    ns(config-router)#neighbor 20.20.20.138 fall-over bfd multihop

    ns(config-router)#redistribute kernel

    ns(config-router)#exit
<!--NeedCopy-->
```

Konfigurieren von BFD für eine IPv6 BGP Single Hop Session

Um BFD für eine IPv6 BGP Single Hop-Sitzung über die VTYSH Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Gibt an
`vtysh`	Zeigt die VTYSH Eingabeaufforderung an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`router bgp <asnumber>`	Autonome BGP-Anlage. `asnumber` ist ein erforderlicher Parameter.
`neighbor <ipv6addr> remote-as <num>`	Aktualisieren Sie die IPv6-BGP-Tabelle mit der lokalen IPv6-Adresse des Nachbarn im angegebenen autonomen System.
`neighbor <ipv6addr> fall-over bfd`	Aktivieren Sie BFD für den angegebenen Nachbarn.

Befehl	Gibt an
`address-family ipv6`	Geben Sie den Konfigurationsmodus für die Adressfamilie ein.
`neighbor <ipv6addr> activate`	Exchange-Präfixe für die IPv6-Routerfamilie zwischen dem Peer und dem lokalen Knoten mithilfe der lokalen Linkadresse.

Beispielkonfiguration:

```
> vtysh

ns# configure terminal ns(config)#router bgp 1

ns(config-router)#neighbor 30fe:123::124 remote-as 1

ns(config-router)#neighbor 30fe:123::124 fall-over bfd

ns(config-router)#address-family ipv6

ns(config-router-af)#neighbor 30fe:123::124 activate

ns(config-router-af)#redistribute kernel

ns(config-router-af)#exit

<!--NeedCopy-->
```

Konfigurieren von BFD für eine IPv6 BGP-Sitzung mit mehreren Hop

Um BFD für eine IPv6 BGP Multi-Hop-Sitzung über die `VTYSH` Befehlszeile zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Gibt an
`vtysh`	Zeigt die `VTYSH` Eingabeaufforderung an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`router bgp <asnumber>`	Autonome BGP-Anlage. `asnumber` ist ein erforderlicher Parameter.

Befehl	Gibt an
`neighbor <ipv6addr> remote-as <num>`	Aktualisieren Sie die IPv6-BGP-Tabelle mit der lokalen IPv6-Adresse des Nachbarn im angegebenen autonomen System.
`neighbor <ipv6addr> fall-over bfd multihop`	Aktivieren Sie BFD für den angegebenen Nachbarn.
`address-family ipv6`	Geben Sie den Konfigurationsmodus für die Adressfamilie ein.
`neighbor <ipv6addr> activate`	Exchange-Präfixe für die IPv6-Routerfamilie zwischen dem Peer und dem lokalen Knoten mithilfe der link-lokalen Adresse.

Beispielkonfiguration:

```
> vtysh

ns# configure terminal

ns(config)# bfd multihop-peer ipv6 20fe:125::138 interval 500 minrx 500
    multiplier 5

ns(config)#router bgp 1

ns(config-router)#neighbor 20fe:125::138 remote-as 1

ns(config-router)#neighbor 20fe:125::138 fall-over bfd multihop

ns(config-router)#address-family ipv6

ns(config-router-af)#neighbor 20fe:125::138 activate

ns(config-router-af)#redistribute kernel

ns(config-router-af)#end

<!--NeedCopy-->
```


Konfigurieren von BFD für OSPFv2 (IPv4) auf Schnittstellen

Sie können BFD auf allen oder auf einer bestimmten Schnittstelle aktivieren, die das OSPFv2-Protokoll verwendet.

So konfigurieren Sie BFD für OSPfv2 auf allen Schnittstellen mit der VTYSH Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Gibt an
`vtysh`	Zeigt die VTYSH Eingabeaufforderung an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`router ospf <process tag>`	Geben Sie den OSPFv2-Konfigurationsmodus ein.
`bfd all-interfaces`	Aktivieren Sie BFD auf allen Schnittstellen, die OSPFv2 verwenden.

Beispielkonfiguration:

```
1      > vtysh
2
3      ns# configure terminal
4
5      ns(config)#router ospf 1
6
7      ns(config-router)#bfd all-interfaces
8
9      ns(config-router)#redistribute kernel
10
11     ns(config-router)#exit
12 <!--NeedCopy-->
```

So konfigurieren Sie BFD für OSPfv2 auf einer bestimmten Schnittstelle mit der VTYSH Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Gibt an
`vtysh`	Zeigt die VTYSH Eingabeaufforderung an.

Befehl	Gibt an
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`interface` `<vlan ID>`	Geben Sie den Schnittstellenkonfigurationsmodus ein.
`ip ospf bfd`	Aktivieren Sie BFD auf der angegebenen Schnittstelle, die OSPFv2 verwendet.

Beispielkonfiguration:

```
    > vtysh

    ns# configure terminal

    ns(config)# interface vlan5

    ns(config-if)# ip ospf bfd

    ns(config-if)# exit
<!--NeedCopy-->
```

Konfigurieren von BFD für OSPFv3 (IPv6) auf Schnittstellen

Sie können BFD auf allen oder auf einer bestimmten Schnittstelle aktivieren, die das OSPFv3-Protokoll verwendet.

So konfigurieren Sie BFD für OSPfv3 auf allen Schnittstellen mit der `VTYSH` Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Gibt an
`vtysh`	Zeigt die `VTYSH` Eingabeaufforderung an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`router ipv6 ospf <process tag>`	Rudern Sie den OSPFv3-Konfigurationsmodus ein.

Befehl	Gibt an
`bfd all-interfaces`	Aktivieren Sie BFD auf allen Schnittstellen, die OSPFv3 verwenden.

Beispielkonfiguration:

```
1      > vtysh
2
3      ns# configure terminal
4
5      ns(config)#router ipv6 ospf 10
6
7      ns(config-router)#bfd all-interfaces
8
9      ns(config-router)#redistribute kernel
10
11     ns(config-router)#exit
12 <!--NeedCopy-->
```

So konfigurieren Sie BFD für OSPFv3 auf einer bestimmten Schnittstelle mit der `VTYSH` Befehlszeile:

Geben Sie an der Eingabeaufforderung die folgenden Befehle in der angegebenen Reihenfolge ein:

Befehl	Gibt an
`vtysh`	Zeigt die `VTYSH` Eingabeaufforderung an.
`configure terminal`	Geben Sie den globalen Konfigurationsmodus ein.
`interface` `<vlan ID>`	Geben Sie den Schnittstellenkonfigurationsmodus ein.
`ipv6 ospf bfd`	Aktivieren Sie BFD auf der angegebenen Schnittstelle, die OSPFv3 verwendet.

Beispielkonfiguration:

```
1      > vtysh
```



```
2
3     ns# configure terminal
4
5     ns(config)# interface vlan15
6
7     ns(config-if)# ipv6 ospf bfd
8
9     ns(config-if)# exit
10 <!--NeedCopy-->
```

Statische Routen konfigurieren

October 5, 2021

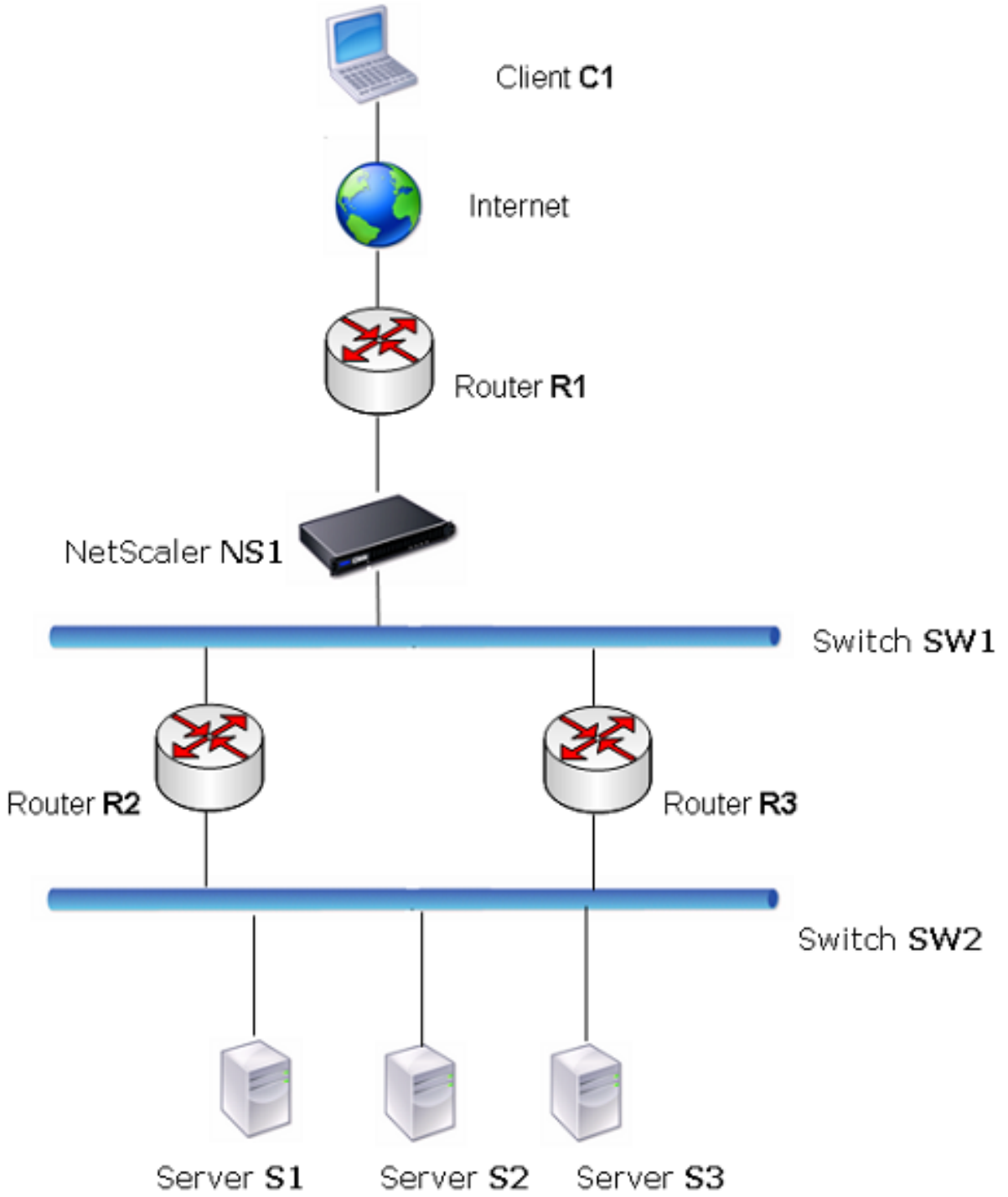
Statische Routen werden manuell erstellt, um die Leistung Ihres Netzwerks zu verbessern. Sie können statische Routen überwachen, um Serviceunterbrechungen zu vermeiden. Außerdem können Sie ECMP-Routen Gewichtungen zuweisen und Nullrouten erstellen, um Routingschleifen zu verhindern.

Überwachte statische Routen. Wenn eine manuell erstellte (statische) Route ausfällt, wird eine Backuproute nicht automatisch aktiviert. Sie müssen die inaktive primäre statische Route manuell löschen. Wenn Sie die statische Route jedoch als überwachte Route konfigurieren, kann die Citrix ADC Appliance automatisch eine Backuproute aktivieren.

Die statische Routenüberwachung kann auch auf der Zugänglichkeit des Subnetzes basieren. Ein Subnetz ist normalerweise mit einer einzigen Schnittstelle verbunden, kann aber logisch über andere Schnittstellen zugegriffen werden. Subnetze, die an ein VLAN gebunden sind, sind nur verfügbar, wenn das VLAN hochläuft. VLANs sind logische Schnittstellen, über die Pakete vom Citrix ADC übertragen und empfangen werden. Eine statische Route wird als DOWN markiert, wenn sich der nächste Hop in einem Subnetz befindet, das nicht erreichbar ist.

Hinweis: In einem Hochverfügbarkeitssetup (High Availability, HA) ist der Standardwert für Monitoring State Routes (MSRs) auf dem sekundären Knoten UP. Der Wert wird so festgelegt, dass beim Failover eine Statusübergangslücke vermieden wird, was dazu führen kann, dass Pakete auf diesen Routen entfernt werden.

Betrachten Sie die folgende einfache Topologie, bei der ein Citrix ADC den Lastenausgleich des Datenverkehrs zu einem Standort über mehrere Server hinweg führt.



Router R1 verschiebt den Datenverkehr zwischen dem Client und der Citrix ADC Appliance. Die Appliance kann Server S1 und S2 über Router R2 oder R3 erreichen. Es verfügt über zwei statische Routen,

durch die das Subnetz der Server erreicht werden kann, eine mit R2 als Gateway und eine andere mit R3 als Gateway. Beide Routen haben die Überwachung aktiviert. Die administrative Entfernung der statischen Route mit Gateway R2 ist geringer als die der statischen Route mit Gateway R3. Daher wird R2 gegenüber R3 bevorzugt, um Datenverkehr an die Server weiterzuleiten. Außerdem zeigt die Standardroute auf dem Citrix ADC auf R1, sodass der gesamte Internetverkehr ordnungsgemäß beendet wird.

Wenn R2 fehlschlägt, während die Überwachung auf der statischen Route aktiviert ist, die R2 als Gateway verwendet, markiert der Citrix ADC es als DOWN. Der Citrix ADC verwendet nun die statische Route mit R3 als Gateway und leitet den Datenverkehr über R3 an die Server weiter.

Das Citrix ADC unterstützt die Überwachung statischer IPv4- und IPv6-Routen. Sie können Citrix ADC so konfigurieren, dass eine statische IPv4-Route überwacht wird, indem Sie einen neuen ARP- oder PING-Monitor erstellen oder vorhandene ARP- oder PING-Monitore verwenden. Sie können Citrix ADC so konfigurieren, dass eine statische IPv6-Route überwacht wird, indem Sie entweder eine neue Neighbor Discovery für IPv6 (ND6) oder einen PING-Monitor erstellen oder die vorhandenen ND6- oder PING-Monitore verwenden.

Gewichtete statische Routen. Wenn die Citrix ADC Appliance Routing-Entscheidungen trifft, die Routen mit gleicher Entfernung und Kosten betreffen, d. h. ECMP-Routen (Equal Cost Multi-Path-Routen), wird die Last zwischen ihnen mithilfe eines Hashmechanismus auf der Grundlage der Quell- und Ziel-IP-Adressen ausgeglichen. Für eine ECMP-Route können Sie jedoch einen Gewichtungswert konfigurieren. Der Citrix ADC verwendet dann sowohl das Gewicht als auch den Hashwert für den Lastausgleich.

Null-Routen. Wenn die in einer Routingentscheidung gewählte Route inaktiv ist, wählt die Citrix ADC Appliance eine Backuproute aus. Wenn auf alle Backuprouten nicht zugegriffen werden kann, leitet die Appliance das Paket möglicherweise an den Absender um, was zu einer Routingschleife führen kann, die zu einer Netzwerküberlastung führt. Um diese Situation zu verhindern, können Sie eine Null-Route erstellen, die eine Null-Schnittstelle als Gateway hinzufügt. Die Null-Route ist nie die bevorzugte Route, da sie eine höhere administrative Entfernung als die anderen statischen Routen hat. Es wird jedoch ausgewählt, wenn die anderen statischen Routen nicht mehr zugänglich sind. In diesem Fall lässt die Appliance das Paket fallen und verhindert eine Routingschleife.

Konfigurieren statischer IPv4-Routen

Sie können eine einfache statische Route oder eine Null-Route hinzufügen, indem Sie einige Parameter festlegen, oder Sie können zusätzliche Parameter festlegen, um eine überwachte oder überwachte und gewichtete statische Route zu konfigurieren. Sie können die Parameter einer statischen Route ändern. Sie können beispielsweise einer nicht gewichteten Route eine Gewichtung zuweisen oder die Überwachung auf einer überwachten Route deaktivieren.

CLI-Verfahren

So erstellen Sie eine statische Route mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add route <network> <netmask> <gateway>[-cost <positive_integer>] [-advertise (DISABLED | ENABLED)]
- show route [<network> <netmask> [<gateway>]] [<routeType>] [-detail]

Beispiel:

```
> add route 10.102.29.0 255.255.255.0 10.102.29.2 -cost 2 -advertise
   ENABLED
 Done
<!--NeedCopy-->
```

So erstellen Sie eine überwachte statische Route mit der CLI:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine überwachte statische Route zu erstellen und die Konfiguration zu überprüfen:

- add route <network> <netmask> <gateway> [-distance <positive_integer>] [-weight <positive_integer>][-msr (ENABLED | DISABLED) [-monitor <string>]]
- show route [<network> <netmask> [<gateway>]] [<routeType>] [-detail]

Beispiel:

```
> add route 10.102.29.0 255.255.255.0 10.102.29.3 -distance 5 -weight 6
    -msr ENBLED -monitor PING
 Done
<!--NeedCopy-->
```

So erstellen Sie eine Null-Route mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add route <network> <netmask> null
- show route <network> <netmask>

Beispiel:

```
> add route 10.102.29.0 255.255.255.0 null
 Done
<!--NeedCopy-->
```


So entfernen Sie eine statische Route mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

rm route <network> <netmask> <gateway>

Beispiel:

```
1 > rm route 10.102.29.0 255.255.255.0 10.102.29.3
2  Done
3 <!--NeedCopy-->
```

GUI-Verfahren

So konfigurieren Sie eine statische Route mit der GUI:

Navigieren Sie zu System > Netzwerk > Routen, und fügen Sie auf der Registerkarte Basic eine neue statische Route hinzu, oder bearbeiten Sie eine vorhandene statische Route.

So entfernen Sie eine Route mit der GUI:

Navigieren Sie zu System > Netzwerk > Routen, und löschen Sie auf der Registerkarte Basic die statische Route.

Konfigurieren statischer IPv6-Routen

Sie können maximal sechs statische IPv6-Standardrouten konfigurieren. IPv6-Routen werden auf der Grundlage ausgewählt, ob die MAC-Adresse des Zielgeräts erreichbar ist. Dies kann mithilfe der IPv6-Neighbor Discovery-Funktion ermittelt werden. Routen sind Lastausgleich und nur Quellen-/Ziel-basierte Hash-Mechanismen werden verwendet. Daher werden Routenauswahlmechanismen wie Roundrobin nicht unterstützt. Die nächste Hop-Adresse in der Standardroute muss nicht zum NSIP-Subnetz gehören.

CLI-Verfahren

So erstellen Sie eine IPv6-Route mit der CLI:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine IPv6-Route zu erstellen und die Konfiguration zu überprüfen:

- add route6 <network> <gateway> [-vlan <positive_integer>]
- show route6 [<network> [<gateway>]

Beispiel:


```
> add route6 ::/0 FE80::67 -vlan 5
 Done
<!--NeedCopy-->
```

So erstellen Sie eine überwachte statische IPv6-Route mit der CLI:

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine überwachte statische IPv6-Route zu erstellen und die Konfiguration zu überprüfen:

- add route6 <network> <gateway> [-msr (ENABLED | DISABLED) [-monitor <string>]
- show route6 [<network> [<gateway>]

Beispiel:

```
> add route6 ::/0 2004::1 -msr ENABLED -monitor PING
 Done
<!--NeedCopy-->
```

So entfernen Sie eine IPv6-Route mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

rm route6 <network> <gateway>

Beispiel:

```
> rm route6 ::/0 FE80::67
 Done
<!--NeedCopy-->
```

GUI-Verfahren

So konfigurieren Sie eine IPv6-Route mit der GUI:

Navigieren Sie zu System > Netzwerk > Routen, und fügen Sie auf der Registerkarte IPv6 eine neue IPv6-Route hinzu, oder bearbeiten Sie eine vorhandene IPv6-Route.

So entfernen Sie eine IPv6-Route mit der GUI:

Navigieren Sie zu System > Netzwerk > Routen, und löschen Sie auf der Registerkarte IPv6 die IPv6-Route.

Routing Health Injection basierend auf Einstellungen des virtuellen Servers

December 7, 2021

Die folgende Option und der Parameter werden eingeführt, um die RHI-Funktionalität (Route Health Injection) der Citrix ADC Appliance für die Werbung für die Route einer VIP-Adresse zu steuern.

- **VSVR_CNTRLD**. Es ist eine Option für den Parameter (Vserver RHI Level) einer VIP-Adresse. Wenn diese Option auf den Parameter Vserver RHI Level gesetzt ist, hängt das RHI-Verhalten für die Werbung für die Route der VIP-Adresse von der Einstellung des RHI STATE-Parameters auf allen zugeordneten virtuellen Servern der VIP-Adresse zusammen mit ihrem Status ab.
- **RHI STATE**. Es ist ein Parameter des virtuellen Servers. Sie können den Parameter RHI STATE entweder auf PASSIVE oder ACTIVE einstellen. Standardmäßig ist der Parameter RHI STATE auf PASSIVE gesetzt.

Wenn für eine VIP-Adresse der Parameter RHI (Vserver RHI Level) auf VSVR_CNTRLD festgelegt ist, sind folgende unterschiedliche RHI-Verhaltensweisen für die VIP-Adresse auf der Grundlage der RHI STATE-Einstellungen auf den virtuellen Servern, die mit der VIP-Adresse verknüpft sind:

- Wenn Sie RHI STATE auf allen virtuellen Servern auf PASSIVE setzen, gibt der Citrix ADC immer die Route für die VIP-Adresse an.
- Wenn Sie RHI STATE auf allen virtuellen Servern auf ACTIVE festlegen, gibt Citrix ADC die Route für die VIP-Adresse an, wenn sich mindestens einer der zugeordneten virtuellen Server im Status UP befindet.
- Wenn Sie RHI STATE für einige auf ACTIVE und für andere PASSIVE festlegen, gibt Citrix ADC die Route für die VIP-Adresse an, wenn mindestens einer der zugeordneten virtuellen Server, deren RHI STATE auf ACTIVE festgelegt ist, den Status UP hat.

Die folgende Tabelle zeigt das Beispiel RHI-Verhalten für eine VIP-Adresse auf der Grundlage der RHI STATE-Einstellungen auf den virtuellen Servern mit der VIP-Adresse zugeordnet. Die Citrix ADC Appliance verfügt über zwei virtuelle Server V1 und V2, die der VIP-Adresse zugeordnet sind:

Zugehörige virtuelle Server für einen VIP	State 1	State 2	State 3	State 4
RHI-Status auf allen virtuellen Servern auf PASSIVE eingestellt				

Zugehörige virtuelle Server für einen VIP	State 1	State 2	State 3	State 4
V1	BEREIT	BEREIT	INAKTIV	INAKTIV
V2	BEREIT	INAKTIV	BEREIT	INAKTIV
Bewerben Sie die Route für diese VIP-Adresse?	Ja	Ja	Ja	Ja
RHI-Status auf allen virtuellen Servern auf ACTIVE festgelegt				
V1	BEREIT	BEREIT	INAKTIV	INAKTIV
V2	BEREIT	INAKTIV	BEREIT	INAKTIV
Bewerben Sie die Route für diese VIP-Adresse?	Ja	Ja	Ja	Nein
RHI-Status auf ACTIVE auf einem virtuellen Server und PASSIVE auf dem anderen				
V1 (RHI-Status = ACTIVE)	BEREIT	BEREIT	INAKTIV	INAKTIV
V2 (RHI-Zustand = PASSIVE)	BEREIT	INAKTIV	BEREIT	INAKTIV
Bewerben Sie die Route für diese VIP-Adresse?	Ja	Ja	Nein	Nein

So konfigurieren Sie RHI für eine VIP-Adresse, die auf der Parametereinstellung RHI (RHI State) der zugeordneten virtuellen Server basiert, gehen Sie wie folgt vor:

- Setzen Sie den Parameter RHI (Vserver RHI Level) für die VIP-Adresse auf VSVR_CNTRLD.
- Legen Sie den RHI-State-Parameter für jeden virtuellen Server fest, der der VIP-Adresse zugeordnet ist.

So legen Sie den vServer-RHI-Level für eine VIP-Adresse mit der Befehlszeilenschnittstelle fest:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **set ns ip** <IPAddress> [-**vserverRHILevel** <vserverRHILevel>]

So legen Sie den RHI-State-Parameter eines virtuellen Servers mit der CLI fest:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **set lb vserver** <name> [-**RHIstate** (**PASSIVE** | **ACTIVE**)]

So legen Sie den vServer RHI-Level für eine VIP-Adresse mit der GUI fest

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs**.
2. Wählen Sie eine VIP-Adresse aus, und klicken Sie dann auf **Bearbeiten**.
3. Legen Sie den Parameter **Vserver RHI Level auf VSVR_CNTRLD** fest, und klicken Sie dann auf **OK**.

So legen Sie den RHI-State-Parameter eines virtuellen Servers mit der GUI fest

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Wählen Sie einen virtuellen Lastausgleichsserver aus, und klicken Sie dann auf **Bearbeiten**.
3. Legen Sie den Parameter **RHI State** fest, und klicken Sie dann auf **OK** .

Konfigurieren von richtlinienbasierten Routen

October 5, 2021

Policy-basiertes Routingentscheidungen anhand von Kriterien, die Sie angeben. Eine richtlinienbasierte Route (PBR) gibt Kriterien für die Auswahl von Paketen und in der Regel einen nächsten Hop an, an den die ausgewählten Pakete gesendet werden sollen. Beispielsweise können Sie die Citrix ADC Appliance so konfigurieren, dass ausgehende Pakete von einer bestimmten IP-Adresse oder einem bestimmten Bereich an einen bestimmten Next Hop Router weitergeleitet werden. Jedes Paket wird mit jedem konfigurierten PBR in der durch die angegebenen Prioritäten festgelegten Reihenfolge abgeglichen, bis eine Übereinstimmung gefunden wird. Wenn keine Übereinstimmung gefunden wird oder wenn die passende PBR eine DENY-Aktion angibt, wendet Citrix ADC die Routingtabelle für normales zielbasiertes Routing an.

Ein PBR basiert Routing Entscheidungen für die Datenpakete auf Parametern wie Quell-IP-Adresse, Quellport, Ziel-IP-Adresse, Ziel-Port, Protokoll und Quell-MAC-Adresse. Ein PBR definiert die Bedingungen, die ein Paket erfüllen muss, damit der Citrix ADC das Paket weiterleiten kann. Diese Aktionen werden als Verarbeitungsmodi bezeichnet. Die Verarbeitungsmodi sind:

- **ALLOW.** Die Appliance sendet das Paket an den angegebenen Next-Hop-Router.
- **DENY.** Citrix ADC wendet die Routingtabelle für normales zielbasiertes Routing an.

Sie können PBRs für ausgehenden IPv4- und IPv6-Datenverkehr erstellen.

Viele Benutzer beginnen damit, PBRs zu erstellen und sie dann zu ändern. Um eine neue PBR zu aktivieren, müssen Sie sie anwenden. Um eine PBR zu deaktivieren, können Sie sie entweder entfernen oder deaktivieren. Sie können die Prioritätsnummer eines PBR ändern, um ihm eine höhere oder niedrigere Priorität zu geben.

Policy-Based Routes (PBR) für IPv4-Datenverkehr

October 5, 2021

Die Konfiguration von PBRs umfasst die folgenden Aufgaben:

- Erstellen Sie eine PBR.
- PBRs anwenden.
- (Optional) Deaktivieren oder aktivieren Sie eine PBR.
- (Optional) Nummerieren Sie die Priorität des PBR neu.

Erstellen oder Ändern einer PBR

Sie können nicht zwei PBRs mit denselben Parametern erstellen. Wenn Sie versuchen, ein Duplikat zu erstellen, wird eine Fehlermeldung angezeigt.

Sie können die Priorität eines PBR konfigurieren. Die Priorität (ein ganzzahliger Wert) definiert die Reihenfolge, in der die Citrix ADC Appliance PBRs auswertet. Wenn Sie eine PBR ohne Angabe einer Priorität erstellen, weist Citrix ADC automatisch eine Priorität zu, die ein Vielfaches von 10 ist.

Wenn ein Paket mit der vom PBR definierten Bedingung übereinstimmt, führt Citrix ADC eine Aktion aus. Wenn das Paket nicht mit der vom PBR definierten Bedingung übereinstimmt, vergleicht der Citrix ADC das Paket mit dem PBR mit der nächsthöheren Priorität.

Anstatt die ausgewählten Pakete an einen Next Hop Router zu senden, können Sie die PBR so konfigurieren, dass sie an einen virtuellen Link-Load Balancing Server gesendet werden, an den Sie mehrere nächste Hops gebunden haben. Diese Konfiguration kann ein Backup bereitstellen, wenn ein nächster Hop-Link fehlschlägt.

Betrachten Sie das folgende Beispiel. Zwei PBRs, p1 und p2, sind auf dem Citrix ADC konfiguriert und weisen automatisch Prioritäten 20 und 30 zu. Sie müssen eine dritte PBR, p3, hinzufügen, die unmittelbar nach dem ersten PBR, p1, ausgewertet werden soll. Die neue PBR, p3, muss eine Priorität zwischen 20 und 30 haben. In diesem Fall können Sie die Priorität als 25 angeben.

CLI-Verfahren

So erstellen Sie eine PBR mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add ns pbr <name> <action> [-srcIP [<operator>] <srcIPVal>] [-srcPort [<operator>] <srcPortVal>] [-destIP [<operator>] <destIPVal>] [-destPort [<operator>] <destPortVal>] [-nextHop <nextHopVal>] [-srcMac <mac_addr>] [-protocol <protocol> |-protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-msr (ENABLED | DISABLED) [-monitor <string>]] [-state (ENABLED | DISABLED)]
- show ns pbr

Beispiel:

```
> add ns pbr pbr1  allow -srcip 10.102.37.252 -destip 10.10.10.2 -
   nexthop 10.102.29.77
 Done
<!--NeedCopy-->
```

So ändern Sie die Priorität eines PBR mit der CLI:

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

- set ns pbr <name> [-action (ALLOW | DENY)] [-srcIP [<operator>] <srcIPVal>] [-srcPort [<operator>] <srcPortVal>] [-destIP [<operator>] <destIPVal>] [-destPort [<operator>] <destPortVal>] [-nextHop <nextHopVal>] [-srcMac <mac_addr>] [-protocol <protocol> | -protocolNumber <positive_integer>] [-vlan <positive_integer>] [-interface <interface_name>] [-priority <positive_integer>] [-msr (ENABLED | DISABLED) [-monitor <string>]] [-state (ENABLED | DISABLED)]
- show ns pbr [<name>]

Beispiel:

```
> set ns pbr pbr1 -priority 23
 Done
<!--NeedCopy-->
```


So entfernen Sie einen oder alle PBRs mit der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- rm ns pbr <name>
- clear ns pbrs

Beispiel:

```
> rm ns pbr pbr1
 Done

> clear ns PBRs
 Done
<!--NeedCopy-->
```

GUI-Verfahren

So erstellen Sie eine PBR mit der GUI:

Navigieren Sie zu System > Netzwerk > PBRs, fügen Sie auf der Registerkarte PBRs eine neue PBR hinzu, oder bearbeiten Sie eine vorhandene PBR.

So entfernen Sie einen oder alle PBRs mit der GUI:

Navigieren Sie zu System > Netzwerk > PBRs, löschen Sie auf der Registerkarte PBRs die PBR.

Anwenden einer PBR

Sie müssen eine PBR anwenden, um sie zu aktivieren. Das folgende Verfahren wendet alle PBRs erneut an, die Sie nicht deaktiviert haben. Die PBRs bilden eine Speicherstruktur (Nachschlagetabelle). Wenn Sie beispielsweise 10 PBRs (p1 - p10) erstellen und dann einen weiteren PBR (p11) erstellen und anwenden, werden alle PBRs (p1 - p11) neu angewendet und eine neue Nachschlagetabelle erstellt. Wenn eine Sitzung mit einem DENY-PBR zusammenhängt, wird die Sitzung zerstört.

Sie müssen dieses Verfahren nach jeder Änderung, die Sie an einem PBR vornehmen, anwenden. Sie müssen dieses Verfahren beispielsweise ausführen, nachdem Sie eine PBR deaktiviert haben.

Hinweis: Auf der Citrix ADC Appliance erstellte PBRs funktionieren erst dann, wenn sie angewendet werden.

So wenden Sie eine PBR mit der CLI an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

apply ns PBRs

So wenden Sie eine PBR mit der GUI an:

1. Navigieren Sie zu System > Netzwerk > PBRs.
2. Wählen Sie auf der Registerkarte PBRs den PBRaus, und wählen Sie in der Liste Aktiondie Option Übernehmenaus.

Aktivieren oder Deaktivieren von PBRs

Standardmäßig sind die PBRs aktiviert. Das bedeutet, dass die Citrix ADC Appliance bei der Anwendung von PBRs automatisch eingehende Pakete mit den konfigurierten PBRs verglichen. Wenn ein PBR in der Nachschlagetabelle nicht erforderlich ist, aber in der Konfiguration beibehalten werden muss, muss er deaktiviert werden, bevor die PBRs angewendet werden. Nachdem die PBRs angewendet wurden, gleicht der Citrix ADC keine eingehenden Pakete mit deaktivierten PBRs.

So aktivieren oder deaktivieren Sie einen PBR mit der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- enable ns pbr <name>
- disable ns pbr <name>

Beispiel:

```
> enable ns PBR pbr1
 Done
> show ns PBR pbr1
1)      Name: pbr1
        Action: ALLOW                           Hits: 0
        srcIP = 10.102.37.252
        destIP = 10.10.10.2
        srcMac:                                 Protocol:
        Vlan:                                   Interface:
        Active Status: ENABLED                  Applied Status: APPLIED
        Priority: 10
        NextHop: 10.102.29.77

 Done

> disable ns PBR pbr1
Warning: PBR modified, use 'apply pbrs' to commit this operation

> apply pbrs
 Done

> show ns PBR pbr1
```



```
1)      Name: pbr1
        Action: ALLOW                           Hits: 0
        srcIP = 10.102.37.252
        destIP = 10.10.10.2
        srcMac:                                 Protocol:
        Vlan:                                   Interface:
        Active Status: DISABLED                 Applied Status:
           NOTAPPLIED
        Priority: 10
        NextHop: 10.102.29.77
Done
<!--NeedCopy-->
```

So aktivieren oder deaktivieren Sie einen PBR mit der GUI:

1. Navigieren Sie zu System > Netzwerk > PBRs.
2. Wählen Sie auf der Registerkarte PBRs die PBR aus, wählen Sie in der Liste Aktion die Option Aktivieren oder Deaktivieren aus.

PBR6s neu nummerieren

Sie können die PBRs automatisch neu nummerieren, um ihre Prioritäten auf ein Vielfaches von 10 festzulegen.

So nummerieren Sie PBRs mit der CLI neu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- renumber ns pbrs

So nummerieren Sie PBRs mit der GUI neu:

Navigieren Sie zu System > Netzwerk > PBRs, wählen Sie auf der Registerkarte PBRs in der Liste Aktion die Option Priorität (n) neu nummerieren aus.

Anwendungsfall - PBR mit mehreren Hops

Betrachten Sie ein Szenario, in dem zwei PBRs, PBR1 und PBR2, auf der Citrix ADC Appliance NS1 konfiguriert sind. PBR1 leitet alle ausgehenden Pakete mit Quell-IP-Adresse als 10.102.29.30 an den nächsten Hop-Router R1 weiter. PBR2 leitet alle ausgehenden Pakete mit Quell-IP-Adresse als 10.102.29.90 an den Next Hop Router R2 weiter. R3 ist ein weiterer Next Hop-Router, der mit NS1 verbunden ist.

Wenn Router R1 ausfällt, werden alle ausgehenden Pakete, die mit PBR1 übereinstimmen, gelöscht. Um diese Situation zu vermeiden, können Sie beim Erstellen oder Ändern eines PBR im nächsten Hop-Feld einen virtuellen Link Load Balancing (LLB) angeben. Mehrere nächste Hops sind als Dienste an den virtuellen LLB-Server gebunden (z. B. R1, R2 und R3). Wenn R1 nun fehlschlägt, werden

alle Pakete, die mit PBR1 übereinstimmen, an R2 oder R3 weitergeleitet, wie von der LB-Methode bestimmt, die auf dem virtuellen LLB-Server konfiguriert ist.

Die Citrix ADC Appliance löst in folgenden Fällen einen Fehler aus, wenn Sie versuchen, eine PBR mit einem virtuellen LLB-Server als nächsten Hop zu erstellen:

- Hinzufügen eines weiteren PBR mit demselben virtuellen LLB-Server.
- Angeben eines nicht vorhandenen virtuellen LLB-Servers.
- Angeben eines virtuellen LLB-Servers, für den die gebundenen Dienste nicht als nächster Hops gelten.
- Angeben eines virtuellen LLB-Servers, für den die LB-Methode nicht auf eine der folgenden Werte festgelegt ist:
  - ROUNDROBIN
  - DESTINATIONIPHASH
  - SOURCEIPHASH
  - SRCIPDESTIPHASH
  - LEASTPACKETS
  - LEASTBANDWIDTH
  - LTRM
  - CALLIDHASH
  - CUSTOM LOAD
- Angeben eines virtuellen LLB-Servers, für den der LB-Persistenztyp nicht auf einen der folgenden Werte festgelegt ist:
  - DESTIP
  - SOURCEIP
  - SRCDSTIP

In der folgenden Tabelle sind die Namen und Werte der Entitäten aufgeführt, die auf der Citrix ADC Appliance konfiguriert sind:

Entitätstyp	Name	IP-Adresse
Link-Load Balancing virtueller Server	LLB1	Nicht verfügbar
Dienstleistungen (nächste Hops)	Router1	1.1.1.254
	Router2	2.2.2.254
	Router3	3.3.3.254
PBRs	PBR1	Nicht verfügbar
	PBR2	Nicht verfügbar

Tabelle 1. Beispielwerte für das Erstellen von Entitäten

Um die oben beschriebene Konfiguration zu implementieren, müssen Sie:

1. Erstellen Sie Dienste Router1, Router2 und Router3, die Next Hop Router R1, R2 und R3 darstellen.
2. Erstellen Sie den virtuellen Link-Load Balancing Server LLB1 und binden Sie die Dienste Router1, Router2 und Router3 an ihn.
3. Erstellen Sie PBRs PBR1 und PBR2, wobei Next Hop Felder als LLB1 bzw. 2.2.2.254 (IP-Adresse des Routers R2) festgelegt sind.

So erstellen Sie einen Dienst mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add service <name> <IP> <serviceType> <port>
- show service <name>

Beispiel:

```
> add service Router1 1.1.1.254 ANY *
 Done
> add service Router2 2.2.2.254 ANY *
 Done
> add service Router3 3.3.3.254 ANY *
 Done
<!--NeedCopy-->
```

So erstellen Sie einen Service mit der GUI:

Navigieren Sie zu Traffic Management > Load Balancing > Services, und erstellen Sie einen Dienst.

So erstellen Sie einen virtuellen Link-Load Balancing Server und binden einen Dienst mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add lb vserver <name> <serviceType>
- bind lb vserver < name> <serviceName>
- show lb vserver < name>

Beispiel:

```
> add lb vserver LLB1 ANY
 Done
> bind lb vserver LLB1 Router1 Router2 Router3
 Done
```



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

So erstellen Sie einen virtuellen Link-Load Balancing Server und binden einen Dienst mit der GUI:

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server, und erstellen Sie einen virtuellen Server für den Link-Load Balancing. Geben Sie **ANY** im Feld **Protokoll** an.
   Hinweis: Stellen Sie sicher, dass
   direkt adressierbar deaktiviert ist.
2. Aktivieren Sie auf der Registerkarte **Dienste** in der Spalte **Aktiv** das Kontrollkästchen für den Dienst, den Sie an den virtuellen Server binden möchten.

So erstellen Sie eine PBR mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add ns pbr <name> <action> [-srcIP [<operator>] <srcIPVal>] [-nextHop <nextHopVal>]
- show ns pbr

Beispiel:

```
> add pbr PBR1 ALLOW -srcIP 10.102.29.30 -nextHop LLB1
 Done
> add pbr PBR2 ALLOW -srcIP 10.102.29.90 -nextHop 2.2.2.254
 Done
<!--NeedCopy-->
```

So erstellen Sie eine PBR mit der GUI:

Navigieren Sie zu System > Netzwerk > PBRs, fügen Sie auf der Registerkarte PBRs eine neue PBR hinzu.

Policy-basierte Routen (PBR6) für IPv6-Datenverkehr

October 5, 2021

Die Konfiguration von PBR6s umfasst die folgenden Aufgaben:

- Erstellen Sie eine PBR6.
- PBR6s anwenden.
- (Optional) Deaktivieren oder aktivieren Sie ein PBR6.
- (Optional) Nummerieren Sie die Priorität des PBR6 neu.

Erstellen oder Ändern einer PBR6

Sie können nicht zwei PBR6s mit denselben Parametern erstellen. Wenn Sie versuchen, ein Duplikat zu erstellen, wird eine Fehlermeldung angezeigt.

Sie können die Priorität eines PBR6 konfigurieren. Die Priorität (ein ganzzahliger Wert) definiert die Reihenfolge, in der die Citrix ADC Appliance PBR6s auswertet. Wenn Sie eine PBR6 ohne Angabe einer Priorität erstellen, weist Citrix ADC automatisch eine Priorität zu, die ein Vielfaches von 10 ist.

Wenn ein Paket mit der vom PBR6 definierten Bedingung übereinstimmt, führt Citrix ADC eine Aktion aus. Wenn das Paket nicht mit der vom PBR6 definierten Bedingung übereinstimmt, vergleicht Citrix ADC das Paket mit dem PBR6 mit der nächsthöheren Priorität.

CLI-Verfahren

So erstellen Sie eine PBR6 mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add ns pbr6** <name><action>[-SrcIPv6 [] <operator><srcIPv6Val>] [-SrcPort [] <operator><srcPortVal>] [-destipv6 [] <operator><destIPv6Val>] [-DestPort [] <operator><destPortVal>] [-SrcMac <mac_addr>] [-protocol\ |-ProtocolNumber] <protocol><positive_integer>[-vlan\ -interface] <positive_integer>[-priority] <interface_name>[-state] <positive_integer>[(AKTIVIERT | DEAKTIVIERT)] [-msr (AKTIVIERT | DEAKTIVIERT) [- monitor]<string>] [-nextHop] <nextHopVal>[-NextHopVlan]<positive_integer>
- show ns pbr

So ändern oder entfernen Sie ein PBR6 mit der CLI:

Um eine PBR6 zu ändern, geben Sie den <name> Befehl **set pbr6** und die zu ändernden Parameter mit ihren neuen Werten ein.

So entfernen Sie eine oder alle PBR6s mit der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- **rm ns pbr6** <name>
- **clear ns pbr6**

GUI-Verfahren

So erstellen oder ändern Sie ein PBR6 mit der GUI:

Navigieren Sie zu System > Netzwerk > PBRs, und fügen Sie auf der Registerkarte PBR6s eine neue PBR6 hinzu, oder bearbeiten Sie eine vorhandene PBR6.

So entfernen Sie eine oder alle PBR6s mit der GUI:

Navigieren Sie zu System > Netzwerk > PBRs, und löschen Sie auf der Registerkarte PBR6s die PBR6.

PBR6s anwenden

Sie müssen ein PBR6 anwenden, um es zu aktivieren. Das folgende Verfahren wendet alle PBR6s erneut an, die Sie nicht deaktiviert haben. Die PBR6s bilden einen Speicherbaum (Nachschlagetabelle). Wenn Sie beispielsweise 10 PBR6s (p6_1 - p6_10) erstellen und dann ein weiteres PBR6 (p6_11) erstellen und anwenden, werden alle PBR6s (p6_1 - p6_11) neu angewendet und eine neue Nachschlagetabelle erstellt. Wenn eine Sitzung mit einem DENY PBR6 zusammenhängt, wird die Sitzung zerstört.

Sie müssen dieses Verfahren nach jeder Änderung, die Sie an einem beliebigen PBR6 vornehmen, anwenden. Sie müssen dieses Verfahren beispielsweise ausführen, nachdem Sie eine PBR6 deaktiviert haben.

Hinweis: PBR6s, die auf der Citrix ADC Appliance erstellt wurden, funktionieren erst, wenn sie angewendet wurden.

So wenden Sie PBR6s mit der CLI an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **anwenden ns PBR6**

So wenden Sie PBR6s mit der GUI an:

1. Navigieren Sie zu System > Netzwerk > PBRs.
2. Wählen Sie auf der Registerkarte PBR6s die PBR6 aus, wählen Sie in der Liste Aktion die Option Übernehmen aus.

Aktivieren oder Deaktivieren eines PBR6

Standardmäßig sind die PBR6s aktiviert. Wenn PBR6s angewendet werden, vergleicht die Citrix ADC Appliance automatisch ausgehende IPv6-Pakete mit den konfigurierten PBR6s. Wenn ein PBR6 in der Nachschlagetabelle nicht erforderlich ist, aber in der Konfiguration beibehalten werden muss, muss es deaktiviert werden, bevor die PBR6s angewendet werden. Nachdem die PBR6s angewendet wurden, gleicht der Citrix ADC keine eingehenden Pakete mit deaktivierten PBR6s.

So aktivieren oder deaktivieren Sie ein PBR6 mit der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- **aktivieren ns pbr** <name>
- **deaktivieren ns pbr** <name>

So aktivieren oder deaktivieren Sie ein PBR6 mit der GUI:

1. Navigieren Sie zu System > Netzwerk > PBRs.
2. Wählen Sie auf der Registerkarte PBR6s die Option PBR6, in der Liste Aktion die Option Aktivieren oder Deaktivieren aus.

PBR6s neu nummerieren

Sie können die PBR6s automatisch neu nummerieren, um ihre Prioritäten auf ein Vielfaches von 10 festzulegen.

So nummerieren Sie PBR6s mit der CLI neu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **nummerieren ns pbr6**

So nummerieren Sie PBR6s mit der GUI neu:

Navigieren Sie zu System > Netzwerk > PBRs, wählen Sie auf der Registerkarte PBR6s in der Liste Aktion die Option Priorität (n) neu nummerieren aus.

MAC-Adress-Platzhaltermaske für PBRs

October 5, 2021

Ein Platzhaltermasken-Parameter wurde für erweiterte PBRs und PBR6s eingeführt und wird zusammen mit dem Quell-MAC-Adressparameter verwendet, um einen Bereich von MAC-Adressen zu definieren, die mit der MAC-Quelladresse ausgehender Pakete übereinstimmen.

Platzhaltermasken geben an, welche Hexadezimalziffern der MAC-Adresse verwendet werden und welche Hexadezimalziffern ignoriert werden. Der Parameter Platzhaltermaske gibt eine Reihe von Einsen und Nullen an und hat eine Länge von 12 Ziffern. Jede Ziffer ist eine Maske für die entsprechende hexadezimale Ziffer der MAC-Adresse. Eine Nullziffer in der Platzhaltermaske gibt an, dass die entsprechende Hexadezimalziffer der MAC-Adresse berücksichtigt werden muss, und eine Ziffer gibt an, dass die entsprechende Hexadezimalziffer ignoriert werden soll.

Die Platzhaltermaske sollte die folgenden Bedingungen erfüllen:

- Hat nur eine Reihe von Nullen
- Hat nur eine Reihe von
- Beginnen Sie mit einer Reihe von Nullen

Im Folgenden finden Sie einige Beispiele für gültige Platzhaltermasken:

- 000000111111
- 000000011111
- 000011111111

Im Folgenden finden Sie einige Beispiele für ungültige Platzhaltermasken:

- 000000111100
- 111110000000

- 010101010101

Für eine PBR-Regel definiert eine Platzhaltermaske 000000111111 für MAC-Adresse 96:fa: 95:1 d: 67:4 a den MAC-Adressbereich 96:FA: 95:00:00:00 - 96:FA:95:FF:FF:FF. Dieser MAC-Adressbereich wird mit der Quell-MAC-Adresse der ausgehenden Pakete abgeglichen.

So geben Sie mit der CLI einen Bereich von Quell-MAC-Adressen in einer PBR-Regel an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add ns pbr** <name> <action> -**srcMac** <mac_addr> -**srcMacMask** <string>
- **show ns pbr** <pbrname>

Beispiel:

```
1 > add ns pbr PBR-1 ALLOW -srcip 192.0.2.34 -srcMac 96:fa:95:1d:67:4a
     - srcMacMask 000000111111 -nexthop 198.51.100.1
2
3  Done
```

So geben Sie mit der CLI einen Bereich von Quell-MAC-Adressen in einer PBR6-Regel an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add ns pbr6** <name> <action> -**srcMac** <mac_addr> -**srcMacMask** <string>
- **show pbr6** <pbr6name>

Beispiel:

```
1 > add ns pbr6 PBR6-1 ALLOW  - srcipv6 2001:db8:0::7 -srcMac 96:fa:95:1d
     :67:4a   - srcMacMask 000000001111 -nexthop 2001:db8:0::1
2  Done
```

Verwenden von NULL-Richtlinienbasierten Routen zum Löschen ausgehender Pakete

October 5, 2021

Einige Situationen erfordern möglicherweise, dass die Citrix ADC Appliance bestimmte ausgehende Pakete löscht, anstatt sie weiterzuleiten, z. B. in Testfällen und während der Bereitstellungsmigration.

NULL richtlinienbasierte Routen können verwendet werden, um bestimmte ausgehende Pakete zu löschen. Ein NULL-PBR ist ein Typ von PBR, für den der nexthop-Parameter auf NULL festgelegt ist. Die Citrix ADC Appliance löscht ausgehende Pakete, die mit einem NULL-PBR übereinstimmen.

Konfigurieren von NULL-PBRs für IPv4-Pakete

So erstellen Sie eine NULL-PBR mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add ns pbr** <name>ALlow [**-td**] <positive_integer>[-**srcIP** [] <operator><srcIPVal>] [-**srcPort** [] <operator><srcPortVal>] [-**DestIP** [<operator>] <destIPVal>] [-**destPort** [] <operator><destPortVal>] (-**NextHop NULL**) [**srcMac** \ [-**srcMacMask**]<mac_addr><string>] [-**Protokoll** <protocol>| -**ProtocolNumber**] <positive_integer>[-**vlan** \ | -**vxlan**] <positive_integer><positive_integer>[-**Schnittstelle**] <interface_name>[-**Priorität**] \ <positive_integer>[-**msr** (**ENABLED** | **DEAKTIVIERT**) [-**monitor**]<string>] [-**Status** (**ENABLED** | **DEAKTIVIERT**) [-**OwnerGroup**]<string>
- **apply ns pbrs**
- **show ns pbr**<id>

So konfigurieren Sie eine NULL-PBR mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **PBRs**, fügen Sie auf der Registerkarte **PBRs** eine **neue NULL-PBR** hinzu, oder bearbeiten Sie eine vorhandene NULL-PBR.

Beispielkonfiguration

In der folgenden Beispielkonfiguration ist NULL PBR6 PBR6-NULL-EXAMPLE-1 für das Löschen aller ausgehenden IPv6-Pakete von der Schnittstelle 1/5 konfiguriert.

```
1 > add ns pbr PBR6-NULL-EXAMPLE-1 ALLOW  - nextHop NULL -interface 1/5
2  Done
3
4 > apply ns pbr6
5  Done
```

Verkehrsverteilung auf mehreren Routen basierend auf fünf Tupel-Informationen

October 5, 2021

In einem Load Balancing-Setup kann eine Citrix ADC Appliance mehrere Routen haben, um ein Paket an ihr Ziel zu senden. Zum Beispiel: zu einem Server und zu einem Client.

Eine Citrix ADC Appliance verwendet einen Hashing-Algorithmus, um eine Route zum Senden des Pakets an sein Ziel auszuwählen.

Der Hashing-Algorithmus verwendet die folgenden zwei Tupel eines Pakets, um einen Hash zu berechnen, auf dessen Grundlage die Citrix ADC Appliance eine Route für das Paket auswählt.

- Quell-IP-Adresse
- Ziel-IP-Adresse

Die Auswahl der Routen basierend auf zwei Tupel-Informationen kann zu einer ungleichmäßigen Verteilung des Verkehrs auf den verfügbaren Routen führen. Diese ungleiche Verteilung des Verkehrs führt auf einigen Routen zu einer Überlastung des Verkehrs.

Um dieses Problem zu beheben, verwendet die Citrix ADC Appliance von Build 13.0 71.x die folgenden fünf Tupel-Informationen eines Pakets im Hashing-Algorithmus, um eine Route für das Paket auszuwählen:

- Quell-IP-Adresse (Client-IP)
- Quellport (Clientport)
- Ziel-IP-Adresse (Dienst-IP)
- Zielport (Serviceport)
- Protokollnummer

Die Auswahl der Routen basierend auf fünf Tupel-Informationen gewährleistet eine gleichmäßige Verteilung des Verkehrs auf den verfügbaren Routen. Diese gleichmäßige Verteilung des Verkehrs verhindert eine Überlastung des Verkehrs auf einer Route.

Betrachten Sie ein Beispiel für ein Load Balancing-Setup, bei dem ein Kunde eine Anfrage an die VIP-Adresse sendet. Die Citrix ADC Appliance verwendet die folgenden fünf Tupelinformationen, um eine Route zum Senden des Anforderungspakets an den Server mit Lastenausgleich auszuwählen:

- Quell-IP-Adresse (Client-IP-Adresse)
- Quellport (Clientport)
- Ziel-IP-Adresse (Service-IP-Adresse)
- Zielport (Service-Portnummer)
- Protokoll-Nummer

Vorrang hinsichtlich anderer Routenauswahl-basierter Citrix ADC Funktionen

In diesem Abschnitt wird der Vorrang der Routenauswahl basierend auf dem Fünf-Tupel-Feature und anderen Routenauswahl-Features in einer Citrix ADC Appliance beschrieben.

- **Richtlinienbasierte Routen (PBR)**. PBR-Regeln haben immer Vorrang vor der Routenauswahl basierend auf fünf Tupeln.

- **Mac-basierte Weiterleitung (MBF)**. In einer Load Balancing-Konfiguration hat MBF- oder Routenauswahl basierend auf fünf Tupeln in den folgenden Fällen Vorrang:
  - Für einen Client initiierten Datenverkehr an die VIP-Adresse der Load Balancing-Konfiguration in der Citrix ADC Appliance:
    * Fordern Sie Traffic an, der für einen Server mit Lastenaus Die Routenauswahl basierend auf fünf Tupeln hat den Vorzug vor MBF.
    * Antwort Traffic für den Kunden bestimmt. MBF bevorzugt die Routenauswahl basierend auf fünf Tupeln.
  - Für einen Server initiierten Datenverkehr an die SNIP-Adresse in der Citrix ADC Appliance:
    * Antwort Traffic für den Kunden bestimmt. Die Routenauswahl basierend auf fünf Tupeln hat den Vorzug vor MBF.
    * Fordern Sie Traffic an, der für einen Server mit Lastenaus MBF bevorzugt die Routenauswahl basierend auf fünf Tupeln.

Behebung von Routing-Problemen

October 5, 2021

Um die Fehlerbehebung so effizient wie möglich zu gestalten, sammeln Sie zunächst Informationen über Ihr Netzwerk. Sie müssen die folgenden Informationen über die Citrix ADC Appliance und andere Systeme im Netzwerk erhalten:

- Vollständiges Topologie-Diagramm, einschließlich Schnittstellenkonnektivität und Zwischen-Switch-Details.
- Konfiguration wird ausgeführt. Sie können den Befehl show running verwenden, um die laufende Konfiguration für ns.conf und zebos.conf abzurufen.
- Ausgabe des Befehls Historie, um zu bestimmen, ob Konfigurationsänderungen vorgenommen wurden, wenn das Problem aufgetreten ist.
- Ausgabe der Befehle Top und ps -ax, um zu bestimmen, ob ein Routing-Daemon die CPU überlastet oder sich falsch verhält.
- Alle Routing-bezogenen Kerndateien in /var/core - nsm, bgpd, ospfd oder ripd. Überprüfen Sie den Zeitstempel, um zu sehen, ob sie relevant sind.
- dr_error.log und dr_info.log Dateien aus /var/log.
- Ausgabe des Datumsbefehls und der Uhrzeitdetails für alle relevanten Systeme. Drucken Sie Datumsangaben auf allen Geräten nacheinander, so dass die Zeiten in den Protokollmeldungen mit verschiedenen Ereignissen korreliert werden können.
- Relevante ns.log, newnslog-Dateien.
- Konfigurationsdateien, Protokolldateien und Befehlsverlaufsdetails von Upstream- und Downstream-Routern.

Häufig gestellte Fragen zum Generischen Routing

October 5, 2021

Benutzer haben in der Regel die folgenden Fragen zur Behandlung von generischen Routingproblemen:

- Wie speichere ich die Konfigurationsdateien?

  Der Schreibbefehl von VTYSH speichert nur Zebos.conf. Führen Sie den Befehl save ns config von CLI aus, um sowohl ns.conf als auch zebos.conf Dateien zu speichern.

- Wenn ich sowohl eine statische Standardroute als auch eine dynamisch erlernte Standardroute konfiguriert habe, welche ist die bevorzugte Standardroute?

  Die dynamisch erlernte Route ist die bevorzugte Standardroute. Dieses Verhalten ist für Standardrouten eindeutig. Im Falle des Netzwerkdienstleistungsmoduls (Network Services Module, NSM) wird jedoch eine statisch konfigurierte Route im RIB gegenüber einer dynamischen Route bevorzugt. Die Route, die in die NSM FIB heruntergeladen wird, ist die statische Route.

- Wie kann ich die Werbung für Standardrouten blockieren?

  Die Standardroute wird nicht in ZEBOs injiziert.

- Wie kann ich die Debug-Ausgabe von Netzwerk-Daemons anzeigen?

  Sie können die Debugging-Ausgabe von Netzwerk-Daemons in eine Datei schreiben, indem Sie den folgenden Protokolldatei-Befehl aus der globalen Konfigurationsansicht in VTYSH eingeben:

  ```
  ns(config)# log file /var/ZebOS.log
  <!--NeedCopy-->
  ```

  Sie können die Debug-Ausgabe an die Konsole leiten, indem Sie den Terminalmonitor-Befehl aus der VTYSH Benutzeransicht eingeben:

  ```
  ns# terminal monitor
  <!--NeedCopy-->
  ```

- Wie sammle ich Kerne laufender Daemons?

  Sie können das gcore-Dienstprogramm verwenden, um Kerne von laufenden Daemons für die Verarbeitung durch gdb zu sammeln. Dies kann beim Debuggen von Daemons hilfreich sein, ohne den gesamten Routingvorgang zum Stillstand zu bringen.


```
gcore [-s] [-c core] [executable] pid
<!--NeedCopy-->
```

Die Option -s stoppt den Daemon vorübergehend, während das Core-Image gesammelt wird. Dies ist eine empfohlene Option, da sie garantiert, dass das resultierende Image den Kern in einem konsistenten Zustand zeigt.

```
root@ns#gcore -s -c nsm.core /netscaler/nsm 342
<!--NeedCopy-->
```

- Wie führe ich einen Stapel von ZeBOS-Befehlen aus?

  Sie können einen Stapel von ZeBOS-Befehlen aus einer Datei ausführen, indem Sie den Befehl VTYSH -f <file-name> eingeben. Dadurch wird die laufende Konfiguration nicht ersetzt, sondern an sie angehängt. Wenn Sie jedoch Befehle zum Löschen der vorhandenen Konfiguration in der Batchdatei einfügen und diese dann für die neue gewünschte Konfiguration hinzufügen, können Sie diesen Mechanismus verwenden, um eine bestimmte Konfiguration zu ersetzen:

```
!
router bgp 234
network 1.1.1.1 255.255.255.0
!
route-map bgp-out2 permit 10
 set metric 9900
 set community 8602:300
!
<!--NeedCopy-->
```

Behebung von OSPF-spezifischen Problemen

October 5, 2021

Bevor Sie mit dem Debuggen eines OSPF-spezifischen Problems beginnen, müssen Sie Informationen von der Citrix ADC Appliance und allen Systemen im betroffenen LAN sammeln, einschließlich Upstream- und Downstream-Routern. Geben Sie zunächst die folgenden Befehle ein:

1. show interface from both nscli and VTYSH

2. show ip ospf interface
3. show ip ospf neighbor detail
4. show ip route
5. show ip ospf route
6. show ip ospf database summary
   - Wenn es nur wenige LSAs in der Datenbank gibt, geben Sie show ip ospf database router, show ip ospf database A. network, show ip ospf database external und andere Befehle ein, um die vollständigen Details der LSAs zu erhalten.
   - Wenn eine große Anzahl von LSAs in der Datenbank vorhanden ist, geben Sie den Befehl show ip ospf database self-originated ein.
7. show ip ospf
8. show ns ip. Dadurch wird sichergestellt, dass die Details aller interessierenden VIPs berücksichtigt werden.
9. Rufen Sie die Protokolle von Peering-Geräten ab und führen Sie den folgenden Befehl aus:

```
gcore -s -c xyz.core /netscaler/ospfd <pid>
```

Hinweis: Der Befehl gcore ist unterbrechungsfrei.

Sammeln Sie zusätzliche Informationen aus dem Citrix ADC wie folgt:

1. Aktivieren Sie die Protokollierung von Fehlermeldungen, indem Sie den folgenden Befehl aus der globalen Konfigurationsansicht in VTYSH eingeben:

```
ns(config)# log file /var/ospf.log
<!--NeedCopy-->
```

2. Aktivieren Sie das Debuggen von ospf-Ereignissen und protokollieren Sie sie mit dem folgenden Befehl:

```
ns(config) #log file /var/ospf.log
<!--NeedCopy-->
```

Debug ospf lsa packet nur dann aktivieren, wenn die Anzahl der LSAs in der Datenbank relativ klein ist (< 500).

Internetprotokoll Version 6 (IPv6)

October 5, 2021

Eine Citrix ADC Appliance unterstützt sowohl serverseitige als auch clientseitige IPv6 und kann daher als IPv6-Knoten fungieren. Es kann Verbindungen von IPv6-Knoten (sowohl Hosts als auch Routern) und von IPv4-Knoten akzeptieren und Protokollübersetzung (RFC 2765) durchführen, bevor Datenverkehr an die Dienste gesendet wird.

In der folgenden Tabelle sind einige der IPv6-Funktionen aufgeführt, die von der Citrix ADC Appliance unterstützt werden.

Tabelle 1. Einige unterstützte IPv6-Funktionen

IPv6-Funktionen
IPv6-Adressen für SNIPs (NSIP6, VIP6 und SNIP6)
Nachbarerkennung (Adressenauflösung, Erkennung duplizierter Adressen, Erkennung von Nachbarn Unerreichbarkeit, Routererkennung)
Verwaltungsanwendungen (ping6, telnet6, ssh6)
Statisches Routing und dynamisches Routing (OSPF, BGP, RIPng und ISIS)
Port-basierte VLANs
Zugriffssteuerungslisten für IPv6-Adressen (ACL6)
IPv6-Protokolle (TCP6, UDP6, ICMP6)
Serverseitige Unterstützung (IPv6-Adressen für vServer, Dienste)
USIP (Quell-IP verwenden) und DSR (Direct Server Return) für IPv6
SNMP und CVPN für IPv6
HA mit nativer IPv6-Knotenadresse
IPv6-Adressen für MIPs
Path-MTU-Erkennung für IPv6

Implementieren von IPv6-Unterstützung

Sie müssen die IPv6-Funktion auf einer Citrix ADC Appliance aktivieren, bevor Sie sie verwenden oder konfigurieren können. Wenn IPv6 deaktiviert ist, verarbeitet Citrix ADC keine IPv6-Pakete. Beim Ausführen eines nicht unterstützten Befehls wird die folgende Warnung angezeigt:


```
”Warning: Feature(s) not enabled [IPv6PT]”
<!--NeedCopy-->
```

Verwenden Sie eines der folgenden Verfahren, um IPv6 zu aktivieren oder zu deaktivieren.

CLI-Verfahren

So aktivieren oder deaktivieren Sie IPv6 mit der CLI:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- ns-Funktion ipv6pt aktivieren
- ns-Funktion ipv6pt deaktivieren

GUI-Verfahren

So aktivieren oder deaktivieren Sie IPv6 mit der GUI:

1. Navigieren Sie zu **System** > **Einstellungen**, klicken Sie in der Gruppe **Modi und Features** auf **Erweiterte Funktionen konfigurieren** .
2. Aktivieren oder deaktivieren Sie die Option **IPv6-Protokollübersetzung** .

VLAN-Unterstützung

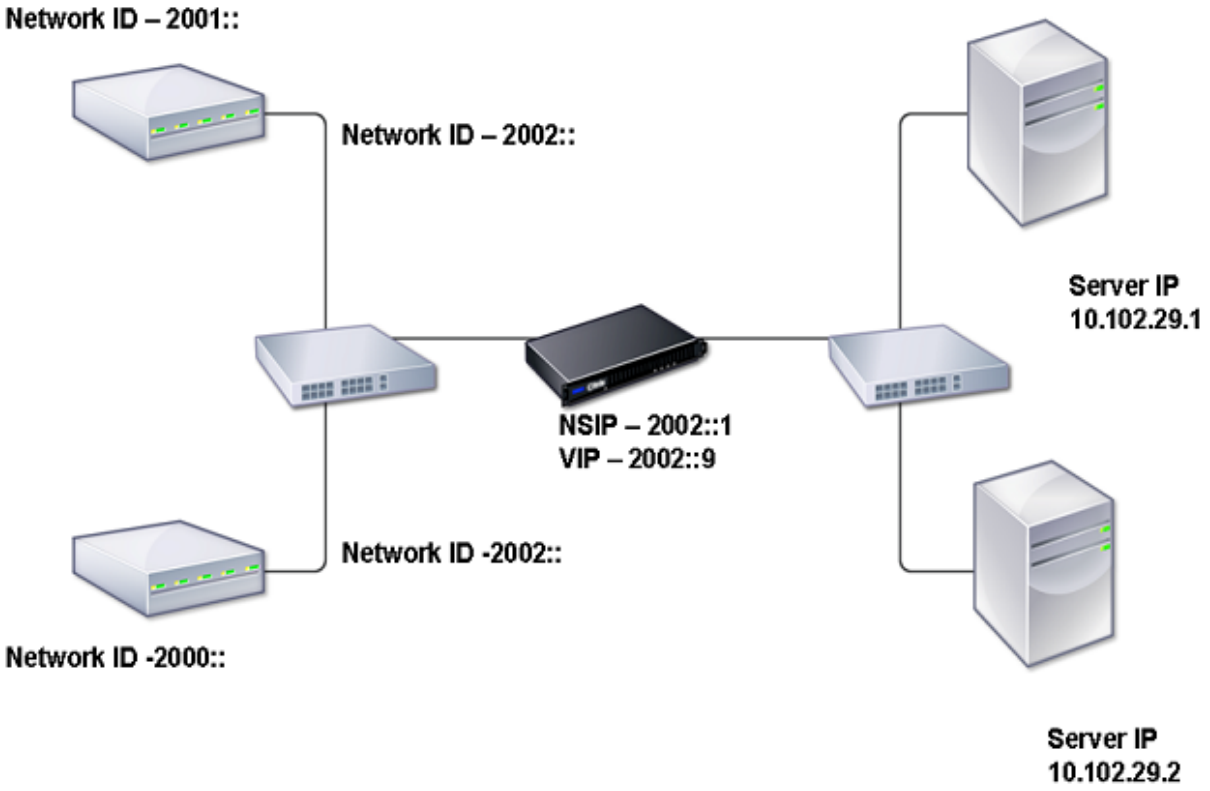
Wenn Sie Broadcast- oder Multicastpakete senden müssen, ohne das VLAN zu identifizieren (z. B. während DAD für NSIP oder ND6 für den nächsten Hop der Route), können Sie die Citrix ADC Appliance so konfigurieren, dass das Paket an allen Schnittstellen mit entsprechendem Tagging gesendet wird. Das VLAN wird durch ND6 identifiziert, und ein Datenpaket wird nur auf das VLAN gesendet. Weitere Informationen zu ND6 und VLANs finden Sie unter Konfigurieren von Neighbor Discovery.

Port-basierte VLANs sind für IPv4 und IPv6 üblich. Präfixbasierte VLANs werden für IPv6 unterstützt.

Einfaches Bereitstellungsszenario

Es folgt ein Beispiel für eine einfache Lastausgleichseinrichtung, die aus einem IPv6-vserver und IPv4-Dienste besteht, wie im folgenden Topologiediagramm dargestellt.

Abbildung 1. IPv6-Beispieltopologie



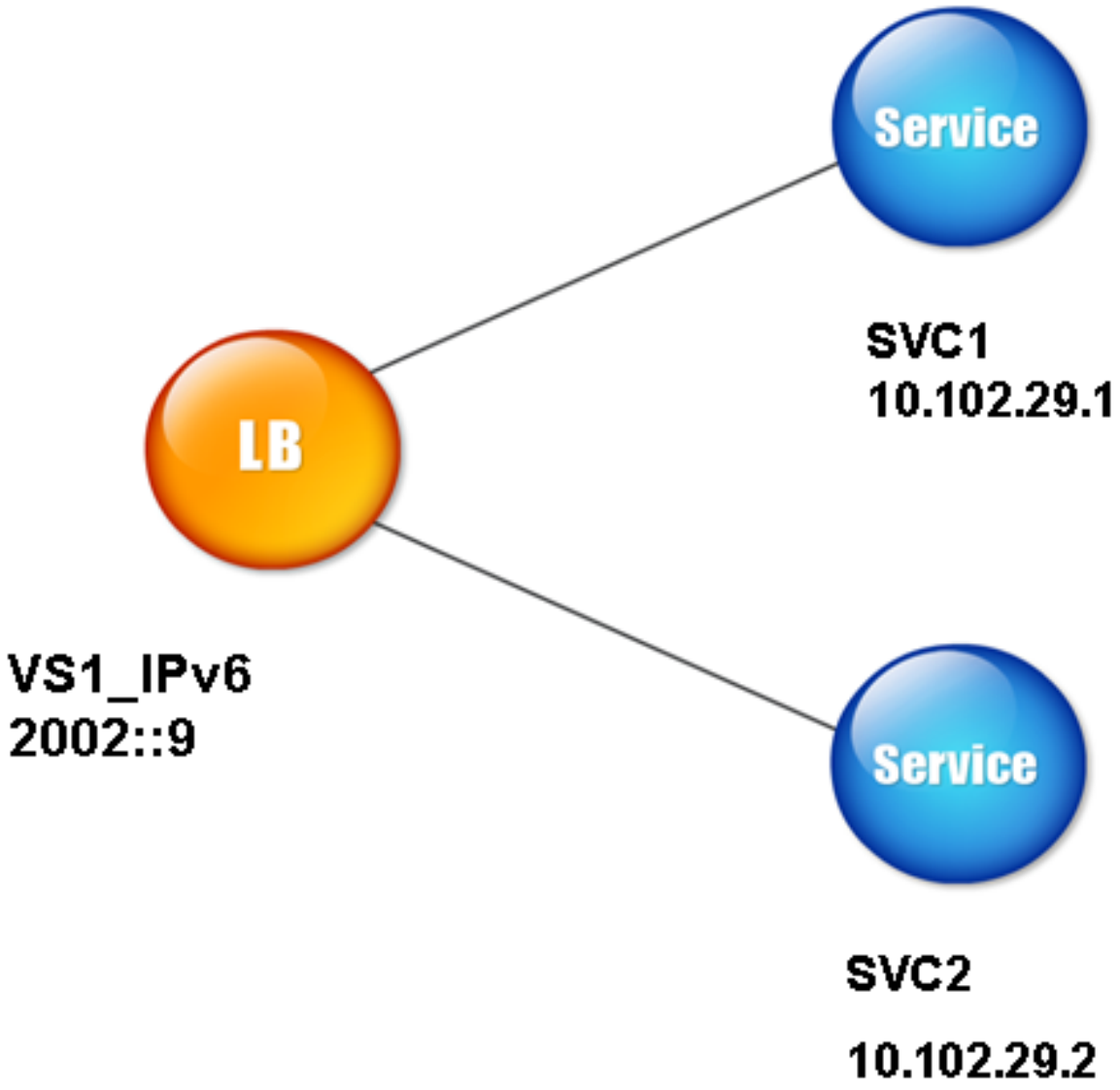
In der folgenden Tabelle werden die Namen und Werte der Entitäten zusammengefasst, die auf dem Citrix ADC konfiguriert werden müssen.

Tabelle 2. Beispielwerte für das Erstellen von Entitäten

Entitätstyp	Name	Wert
LB Vserver	VS1_IPv6	2002::9
Services	SVC1	10.102.29.1
	SVC2	10.102.29.2

Die folgende Abbildung zeigt die Entitäten und Werte der Parameter, die auf dem Citrix ADC konfiguriert werden sollen.

Abbildung 2. IPv6-Entitätsdiagramm



Um dieses Bereitstellungsszenario zu konfigurieren, müssen Sie Folgendes tun:

1. Erstellen Sie einen IPv6-Dienst.
2. Erstellen Sie einen IPv6-LB-vserver.
3. Binden Sie die Dienste an den vserver.

CLI-Verfahren

So erstellen Sie IPv4-Dienste mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add service** <Name> <IPAddress> <Protocol> <Port>
- **sh-Service** <Name>

Beispiel:

```
> add service SVC1 10.102.29.1 HTTP 80
Done

>add service SVC2 10.102.29.2 HTTP 80
Done
<!--NeedCopy-->
```

So erstellen Sie IPv6-vserver mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add lb vserver** <Name> <IPAddress> <Protocol> <Port>
- **sh lb vserver** <Name>

Beispiel:

```
> add lb vserver VS1_IPv6 2002::9 HTTP 80
Done
<!--NeedCopy-->
```

So binden Sie einen Dienst mit der CLI an einen LB-vserver:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **bind lb vserver** <name> <service>
- **sh lb vserver** <name>

Beispiel:

```
> bind lb vserver VS1_IPv6 SVC1
Done
<!--NeedCopy-->
```

GUI-Verfahren

So erstellen Sie IPv4-Dienste mit der GUI:

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**, klicken Sie auf **Hinzufügen**, und legen Sie die folgenden Parameter fest:

- Dienstname
- IP-Adresse
- Protokoll
- Port

So erstellen Sie IPv6-vserver mit der GUI:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, klicken Sie auf **Hinzufügen**, und aktivieren Sie das Kontrollkästchen **IPv6** .
2. Legen Sie die folgenden Parameter fest:
   - Name
   - Protokoll
   - IP-Adresstyp
   - IP-Adresse
   - Port

So binden Sie einen Dienst mit der GUI an einen LB-vserver:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Wählen Sie auf der Seite **Load Balancing Virtual** Servers den vserver aus, für den Sie den Dienst binden möchten (z. B. VS1_IPv6).
3. Klicken Sie auf **Öffnen**.
4. Aktivieren **Sie im Dialogfeld Virtuellen Server konfigurieren (Load Balancing)** auf der Registerkarte **Dienste** das Kontrollkästchen **Aktiv**, das dem Dienst entspricht, den Sie an den vserver binden möchten (z. B. SVC1).
5. Klicken Sie auf **OK**.
6. Wiederholen Sie die Schritte 1-4, um den Dienst zu binden (z. B. SVC2 an den vserver).

Änderung des Host-Headers

Wenn eine HTTP-Anforderung eine IPv6-Adresse im Host-Header enthält und der Server die IPv6-Adresse nicht versteht, müssen Sie die IPv6-Adresse einer IPv4-Adresse zuordnen. Die IPv4-Adresse wird dann im Host-Header der HTTP-Anforderung verwendet, die an den vserver gesendet wird.

CLI-Verfahren

So ändern Sie die IPv6-Adresse im Host-Header mit der Befehlszeilenschnittstelle in eine IPv4-Adresse:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **set ns ip6** <IPv6Address> -**map** <IPAddress>
- **sh ns ip6** <IPv6Address>

Beispiel:

```
> set ns ip6 2002::9 -map 200.200.200.200
Done
<!--NeedCopy-->
```

GUI-Verfahren

So ändern Sie die IPv6-Adresse im Host-Header mit der GUI in eine IPv4-Adresse:

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs**, und wählen Sie auf der Registerkarte **IPv6s** die IP-Adresse aus, für die Sie eine zugeordnete IP-Adresse konfigurieren möchten, z. B. 2002:0:0:0:0:0:0:9, und klicken Sie auf Bearbeiten.
2. Geben Sie im Textfeld **Zugeordnete IP** die zugeordnete IP-Adresse ein, die Sie konfigurieren möchten, z. B. 200.200.200.200.

VIP-Einlage

Wenn eine IPv6-Adresse an einen IPv4-basierten Server gesendet wird, kann der Server die IP-Adresse im HTTP-Header möglicherweise nicht verstehen und einen Fehler generieren. Um dies zu vermeiden, können Sie dem IPv6-VIP eine IPv4-Adresse zuordnen. Anschließend können Sie die VIP-Einfügung aktivieren, um das Einfügen der IPv4-VIP-Adresse und der Portnummer in die an die Server gesendeten HTTP-Anforderungen zu ermöglichen.

CLI-Verfahren

So konfigurieren Sie eine Zuordnungs-IPv6-Adresse mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

set ns ip6 <IPv6Address> -**map** <IPAddress>

Beispiel:

```
> set ns ip6 2002::9 -map 200.200.200.200
 Done
<!--NeedCopy-->
```

So aktivieren Sie die VIP-Einfügung mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **set lb vserver** <name> -**insertVserverIPPort** <Value>
- **sh lb vserver** <name>

Beispiel:

```
> set lb vserver VS1_IPv6 -insertVserverIPPort ON
 Done

<!--NeedCopy-->
```

GUI-Verfahren

So konfigurieren Sie eine Zuordnungs-IPv6-Adresse mit der GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **IPs**, wählen Sie auf der Registerkarte **IPv6s** die IP-Adresse aus, für die Sie eine Zuordnungs-IP-Adresse konfigurieren möchten, z. B. 2002:0:0:0:0:0:0:9, und klicken Sie auf **Bearbeiten** .
2. Geben Sie im Textfeld **Zugeordnete IP** die Zuordnungs-IP-Adresse ein, die Sie konfigurieren möchten, z. B. 200.200.200.200.

So aktivieren Sie die VIP-Einfügung mit der GUI:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, wählen Sie den virtuellen Server aus, den Sie die Porteinfügung aktivieren möchten, und klicken Sie auf **Bearbeiten** .
2. Wählen Sie auf der Registerkarte **Erweitert** unter **Verkehrseinstellungen** im Dropdownlistenfeld **Vserver IP-Port Insertion** die Option **VIPADDR** aus.
3. Geben Sie im Textfeld **Vserver IP Port Insertion** den VIP-Header ein.

Traffic-Domänen

October 5, 2021

> **Warnung**
>
> Citrix empfiehlt, Adminpartitionen anstelle von Traffic Domains zu verwenden. Weitere Informationen finden Sie auf der Seite Admin-Partitionierung .

Verkehrsdomänen sind eine Möglichkeit, den Netzwerkverkehr für verschiedene Anwendungen zu segmentieren. Sie können Datenverkehrsdomänen verwenden, um mehrere isolierte Umgebungen innerhalb einer Citrix ADC Appliance zu erstellen. Eine Anwendung, die zu einer bestimmten Datenverkehrsdomäne gehört, kommuniziert mit Entitäten und verarbeitet den Datenverkehr innerhalb

dieser Domäne. Der Datenverkehr, der zu einer Datenverkehrsdomäne gehört, kann die Grenze einer anderen Datenverkehrsdomäne nicht überschreiten.

Vorteile der Verwendung von Traffic Domains

Die Hauptvorteile der Verwendung von Verkehrsdomänen auf einer Citrix ADC Appliance sind die folgenden:

- **Verwendung von doppelten IP-Adressen in einem Netzwerk**. Verkehrsdomänen ermöglichen es Ihnen, doppelte IP-Adresse im Netzwerk zu verwenden. Sie können dieselbe IP-Adresse oder dieselbe Netzwerkadresse mehreren Geräten in einem Netzwerk oder mehreren Entitäten auf einer Citrix ADC Appliance zuweisen, sofern jede der doppelten Adressen zu einer anderen Verkehrsdomäne gehört.
- **Verwendung von duplizierten Entitäten auf der Citrix ADC Appliance**. Datenverkehrsdomänen ermöglichen es Ihnen auch, doppelte Citrix ADC Feature-Entitäten auf der Appliance zu verwenden. Sie können Entitäten mit denselben Einstellungen erstellen, solange jede Entität einer separaten Verkehrsdomäne zugewiesen ist.
  Hinweis: Doppelte Entitäten mit demselben Namen werden nicht unterstützt.
- **Mehrverhältnis**. Mithilfe von Traffic-Domänen können Sie Hostingdienste für mehrere Kunden bereitstellen, indem Sie den Anwendungsdatenverkehr jedes Kunden innerhalb eines definierten Adressraums im Netzwerk isolieren.

Eine Verkehrsdomäne wird eindeutig durch einen Bezeichner identifiziert, der ein ganzzahliger Wert ist. Jede Verkehrsdomäne benötigt ein VLAN oder eine Gruppe von VLANs. Die Isolationsfunktionalität der Datenverkehrsdomäne hängt von den VLANs ab, die an die Datenverkehrsdomäne gebunden sind. Mehrere VLAN können an eine Verkehrsdomäne gebunden werden, aber dasselbe VLAN kann nicht Teil mehrerer Verkehrsdomänen sein. Daher hängt die maximale Anzahl von Datenverkehrsdomänen, die erstellt werden können, von der Anzahl der auf der Appliance konfigurierten VLANS ab.

Standarddatenverkehrsdomäne

Eine Citrix ADC Appliance verfügt über eine vorkonfigurierte Datenverkehrsdomäne, die als *Standardverkehrsdomäne*bezeichnet wird, die die ID 0 aufweist. Alle Werkseinstellungen und Konfigurationen sind Teil der Standardverkehrsdomäne. Sie können andere Verkehrsdomänen erstellen und dann den Datenverkehr zwischen der Standardverkehrsdomäne und den anderen Verkehrsdomänen segmentieren. Sie können die Standarddatenverkehrsdomäne nicht von der Citrix ADC Appliance entfernen. Jede Feature-Entity, die Sie ohne Festlegen der Verkehrsdomänen-ID erstellen, wird automatisch der Standardverkehrsdomäne zugeordnet.

Hinweis: Einige Funktionen und Konfigurationen werden nur in der Standarddatenverkehrsdomäne unterstützt. Sie funktionieren nicht in nicht standardmäßigen Datenverkehrsdomänen. Eine Liste der

Funktionen, die in allen Verkehrsdomänen unterstützt werden, finden Sie unter Unterstützte Citrix ADC Features in Traffic-Domains.

Funktionsweise von Traffic-Domänen

Betrachten Sie als Veranschaulichung der Verkehrsdomänen ein Beispiel, in dem zwei Verkehrsdomänen mit IDs 1 und 2 auf der Citrix ADC Appliance NS1 konfiguriert sind.

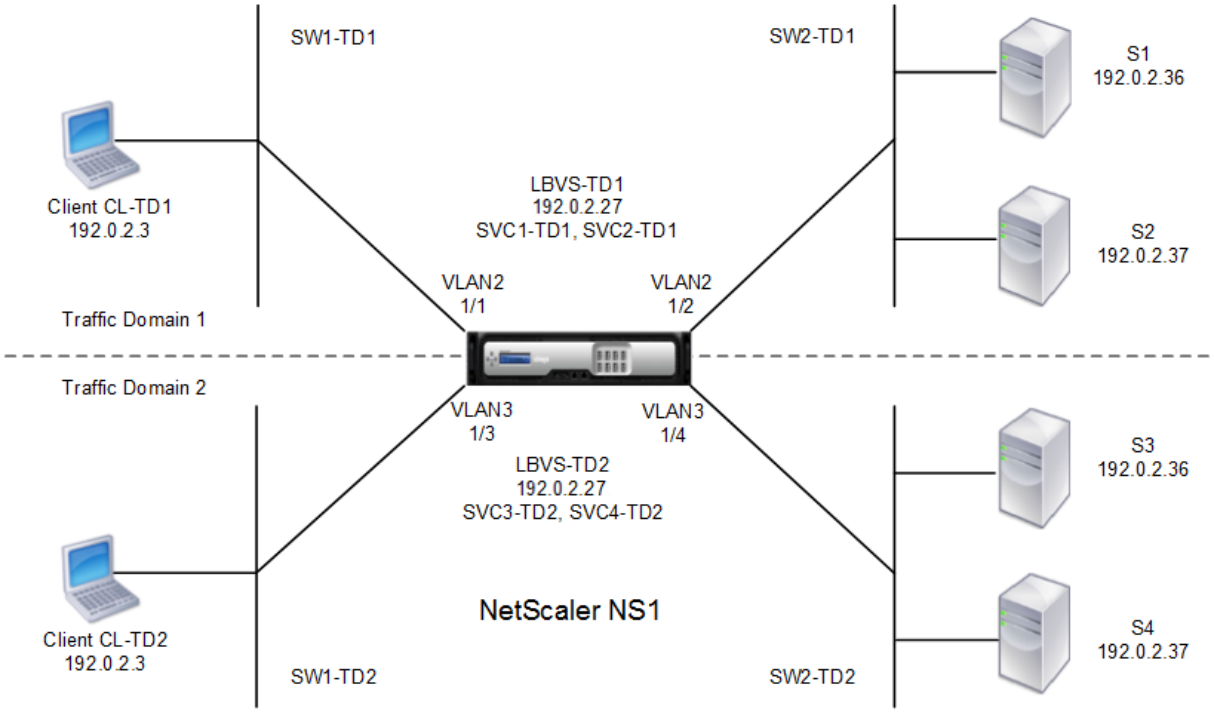
In der Verkehrsdomäne 1 ist der Lastenausgleichsserver LBVS-TD1 so konfiguriert, dass der Datenverkehr über die Server S1 und S2 verteilt wird. Auf der Citrix ADC Appliance werden Server S1 und S2 durch die Dienste SVC1-TD1 bzw. SVC2-TD1 dargestellt. Server S1 und S2 sind über den L2-Switch SW2-TD1 mit NS1 verbunden. Client CL-TD1 befindet sich in einem privaten Netzwerk, das über den L2-Switch SW1-TD1 mit NS1 verbunden ist. SW1-TD1 und SW2-TD1 sind mit VLAN 2 von NS1 verbunden. VLAN 2 ist an die Verkehrsdomäne 1 gebunden, was bedeutet, dass Client CL-TD1 und Server S1 und S2 Teil der Verkehrsdomäne 1 sind.

Ähnlich in der Verkehrsdomäne 2 ist der Lastenausgleichsserver LBVS-TD2 so konfiguriert, dass der Datenverkehr über S3 und S4 verteilt wird. Auf der Citrix ADC Appliance werden die Server S3 und S4 durch die Dienste SVC3-TD2 bzw. SVC4-TD2 dargestellt. Server S3 und S4 sind über den L2-Switch SW2-TD2 mit NS1 verbunden. Client CL-TD2 befindet sich in einem privaten Netzwerk, das über den L2-Switch SW1-TD2 mit NS1 verbunden ist. SW1-TD2 und SW2-TD2 sind mit VLAN 3 von NS1 verbunden. VLAN 3 ist an die Verkehrsdomäne 2 gebunden, was bedeutet, dass Client CL-TD2 und Server S3 und S4 Teil der Verkehrsdomäne 2 sind.

Auf der Citrix ADC Appliance verwenden die Entitäten LBVS-TD1 und LBVS-TD2 dieselben Einstellungen, einschließlich der IP-Adresse. Dasselbe gilt für SVC1-TD1 und SVC3-TD2 und für SVC2-TD1 und SVC4-TD2. Dies ist möglich, da sich diese Entitäten in verschiedenen Verkehrsdomänen befinden.

Ähnlich haben Server S1 und S3, S2 und S4 dieselbe IP-Adresse, und Clients CL-TD1 und CL-TD2 haben jeweils dieselbe IP-Adresse.

Abbildung 1. Funktionsweise von Verkehrsdomänen



In der folgenden Tabelle sind die im Beispiel verwendeten Einstellungen aufgeführt.

Entität	Name	Details
Einstellungen in der Verkehrsdomäne 1		
VLANs, die an die Datenverkehrsdomäne 1 gebunden sind	VLAN 2	VLAN-ID: 2 Schnittstellen gebunden: 1/1, 1/2
Client mit TD1 verbunden	CL-TD1 (nur zu Referenzzwecken)	IP-Adresse: 192.0.2.3
Lastenausgleich virtueller Server in TD1	LBVS-TD1	IP-Adresse: 192.0.2.27
Dienst gebunden an den virtuellen Server LBVS-TD1	SVC1-TD1	IP-Adresse: 192.0.2.36
Dienst gebunden an den virtuellen Server LBVS-TD1	SVC2-TD1	IP-Adresse: 192.0.2.37
SNIP	SNIP-TD1 (nur zu Referenzzwecken)	IP-Adresse: 192.0.2.27
Einstellungen in der Verkehrsdomäne 2		

Entität	Name	Details
VLAN gebunden an Verkehrsdomäne 2	VLAN 3	VLAN-ID: 3 Schnittstellen gebunden: 1/3, 1/4
Client mit TD2 verbunden	CL-TD2 (nur zu Referenzzwecken)	IP-Adresse: 192.0.2.3
Lastenausgleich virtueller Server in TD2	LBVS-TD2	IP-Adresse: 192.0.2.27
Dienst gebunden an den virtuellen Server LBVS-TD2	SVC3-TD2	IP-Adresse: 192.0.2.36
Dienst gebunden an den virtuellen Server LBVS-TD2	SVC4-TD2	IP-Adresse: 192.0.2.37
SNIP bei TD2	SNIP-TD2 (nur zu Referenzzwecken)	IP-Adresse: 192.0.2.29

Im Folgenden ist der Verkehrsfluss in Verkehrsdomäne 1:

1. Der Client CL-TD1 sendet eine ARP-Anforderung für die IP-Adresse von 192.0.2.27 über den L2-Switch SW1-TD1.
2. Die ARP-Anforderung erreicht NS1 auf Schnittstelle 1/1, die an VLAN 2 gebunden ist. Da VLAN 2 an die Verkehrsdomäne 1 gebunden ist, aktualisiert NS1 die ARP-Tabelle der Verkehrsdomäne 1 für die IP-Adresse des Clients CL-TD1.
3. Da die ARP-Anforderung auf Verkehrsdomäne 1 empfangen wird, sucht NS1 nach einer Entität, die in der Verkehrsdomäne 1 konfiguriert ist und eine IP-Adresse von 192.0.2.27 hat. NS1 stellt fest, dass ein virtueller Server mit Lastenausgleich LBVS-TD1 für Verkehrsdomäne 1 konfiguriert ist und die IP-Adresse 192.0.2.27 hat.
4. NS1 sendet eine ARP-Antwort mit der MAC-Adresse der Schnittstelle 1/1.
5. Die ARP-Antwort erreicht CL-TD1. CL-TD1 aktualisiert seine ARP-Tabelle für die IP-Adresse von LBVS-TD1 mit der MAC-Adresse der Schnittstelle 1/1 von NS1.
6. Client CL-TD1 sendet eine Anfrage an 192.0.2.27. Die Anforderung wird von LBVS-TD1 an Port 1/1 von NS1 empfangen.
7. Der Lastausgleichsalgorithmus von LBVS-TD1 wählt Server S2 aus, und NS1 öffnet eine Verbindung zwischen einem SNIP in der Verkehrsdomäne 1 (192.0.2.27) und S2.
8. S2 antwortet auf SNIP 192.0.2.27 auf NS1.
9. NS1 sendet die Antwort von S2 an Client CL-TD1.

Im Folgenden ist der Verkehrsfluss in Verkehrsdomäne 2:

1. Der Client CL-TD2 sendet eine ARP-Anforderung für die IP-Adresse von 192.0.2.27 über den L2-Switch SW1-TD2.

2. Die ARP-Anforderung erreicht NS1 auf Schnittstelle 1/3, die an VLAN 3 gebunden ist. Da VLAN 3 an die Verkehrsdomäne 2 gebunden ist, aktualisiert NS1 den ARP-Table-Eintrag für die IP-Adresse des Clients CL-TD2, obwohl bereits ein ARP-Eintrag für dieselbe IP-Adresse (CL-TD1) in der ARP-Tabelle der Verkehrsdomäne 1 vorhanden ist.
3. Da die ARP-Anfrage in Verkehrsdomäne 2 empfangen wird, durchsucht NS1 die Verkehrsdomäne 2 nach einer Entität mit einer IP-Adresse von 192.0.2.27. NS1 stellt fest, dass der virtuelle Lastausgleichsserver LBVS-TD2 in der Verkehrsdomäne 2 konfiguriert ist und die IP-Adresse 192.0.2.27 hat. NS1 ignoriert LBVS-TD1 in Verkehrsdomäne 1, obwohl es dieselbe IP-Adresse wie LBVS-TD2 hat.
4. NS1 sendet eine ARP-Antwort mit der MAC-Adresse der Schnittstelle 1/3.
5. Die ARP-Antwort erreicht CL-TD2. CL-TD2 aktualisiert seinen ARP-Tabelleneintrag für die IP-Adresse von LBVS-TD2 mit der MAC-Adresse der Schnittstelle 1/3 von NS1.
6. Client CL-TD2 sendet eine Anfrage an 192.0.2.27. Die Anforderung wird von LBVS-TD2 auf Schnittstelle 1/3 von NS1 empfangen.
7. Der Lastausgleichsalgorithmus von LBVS-TD2 wählt Server S3 aus, und NS1 öffnet eine Verbindung zwischen einem SNIP in der Verkehrsdomäne 2 (192.0.2.29) und S3.
8. S2 antwortet auf SNIP 192.0.2.29 auf NS1.
9. NS1 sendet die Antwort von S2 an Client CL-TD2.

Unterstützte Citrix ADC Funktionen in Verkehrsdomänen

Die Citrix ADC Funktionen in der folgenden Liste werden in allen Verkehrsdomänen unterstützt.

> **Wichtig**
>
> Alle Citrix ADC Funktionen, die nicht unten aufgeführt sind, werden nur in der Standardverkehrsdomäne unterstützt.

- ARP-Tisch
- ND6 Tisch
- Stegtisch
- Alle Arten von IPv4- und IPv6-Adressen
- IPv4- und IPv6-Routen
- ACL und ACL6
- PBR & PBR6
- INAT
- RNAT
- RNAT6
- MSR
- MSR6
- Netzprofile
- SNMP-MIBs

- Fragmentierung
- Monitore (Skriptfähige Monitore werden nicht unterstützt)
- Content Switching
- Cacheumleitung
- Persistency (Persistenzgruppen werden nicht unterstützt)
- Dienst (Domänenbasierte Dienste werden nicht unterstützt)
- Servicegruppe (Domänenbasierte Dienstgruppen werden nicht unterstützt)
- Richtlinien (*)
- PING
- TRACEROUTE
- PMTU
- Hohe Verfügbarkeit (Verbindungsspiegelung wird nicht unterstützt)
- Cluster (Unterstützt auf L2-Clustern. Nicht auf L3-Clustern unterstützt)
- Cookie-Persistenz
- MSS
- Protokollierung (Syslog wird nicht unterstützt)
- Priorität Queuing
- Überspannungsschutz
- HTTP-DOSP (**)
- Lastenausgleich (Die folgenden Typen werden nicht unterstützt:)
  - TFTP
  - RTSP
  - Diameter
  - SIP
  - SMPP
- NAT46
- NAT64
- DNS64
- Weiterleiten von Sitzungsregeln
- SNMP

Hinweis:

- *Richtlinien haben keine globalen Bindungspunkte für Traffic-Domains. Richtlinien können jedoch an einen bestimmten virtuellen Lastausgleichsserver einer Verkehrsdomäne gebunden werden.
- ** HTTP-DOSP-Richtlinien haben keine globalen Bindungspunkte für Verkehrsdomänen. HTTP-DOSP-Richtlinien können jedoch an einen bestimmten Lastenausgleichsdienst einer Verkehrsdomäne gebunden werden.

> - Global Server Loading Balancing (GSLB) und ADNS-Funktionen in Citrix ADC kennen keine Traffic Domains. Wenn die GSLB-Konfiguration über alle Datenverkehrsdomänen freigegeben werden muss, funktionieren die GSLB-Methoden Static Proximity und Round Trip Time (RTT) nicht. Als Workaround in diesem Szenario können Sie andere GSLB-Methoden als RTT und Static Proximity verwenden. Weitere Informationen finden Sie unter http://support.citrix.com/article/CTX202277.

Konfigurieren von Verkehrsdomänen

Die Konfiguration einer Verkehrsdomäne auf der Citrix ADC Appliance umfasst die folgenden Aufgaben:

- **Fügen Sie VLANs hinzu.** Erstellen Sie VLANs und binden Sie bestimmte Schnittstellen an sie.
- **Erstellen Sie eine Datenverkehrsdomänenentität und binden Sie VLANs daran.** Hierbei handelt es sich um die folgenden zwei Aufgaben:
  - Erstellen Sie eine Datenverkehrsdomänenentität, die eindeutig durch eine ID identifiziert wird, bei der es sich um einen Ganzzahlwert handelt.
  - Binden Sie die angegebenen VLANs an die Datenverkehrsdomänenentität. Alle Schnittstellen, die an die angegebenen VLANs gebunden sind, sind der Verkehrsdomäne zugeordnet. Mehrere VLAN können an eine Verkehrsdomäne gebunden werden, aber ein VLAN kann nicht Teil mehrerer Verkehrsdomänen sein.
- **Erstellen Sie Feature-Entitäten auf der Traff** Erstellen Sie die erforderlichen Feature-Entitäten in der Datenverkehrsdomäne. Die CLI-Befehle und Konfigurationsdialogfelder aller unterstützten Features in einer nicht standardmäßigen Verkehrsdomäne enthalten einen Parameter, der als *Traffic Domain Identifier* (td) bezeichnet wird. Wenn Sie eine Feature-Entity konfigurieren und die Entität einer bestimmten Verkehrsdomäne zugeordnet werden soll, müssen Sie den td angeben. Jede Feature-Entity, die Sie ohne Festlegen des td erstellen, wird automatisch der Standardverkehrsdomäne zugeordnet.

Um Ihnen eine Vorstellung davon zu geben, wie Feature-Entitäten einer Verkehrsdomäne zugeordnet sind, behandelt dieses Thema die Verfahren zum Konfigurieren aller Entitäten, die in der Abbildung mit dem Titel Wie Traffic-Domains funktionieren.

Die CLI verfügt über zwei Befehle für diese beiden Aufgaben, aber die GUI kombiniert sie in einem einzigen Dialogfeld.

CLI-Verfahren

So erstellen Sie ein VLAN und binden Schnittstellen mit der CLI daran:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add vlan** <id>

- **bind vlan** <id> -**ifnum** <slot/port>
- **vlan anzeigen** <id>

So erstellen Sie eine Datenverkehrsdomänenentität und binden VLANs mit der Befehlszeilenschnittstelle an sie:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add ns trafficdomain** <td>
- **binde ns Trafficdomain** <td> -**Vlan** <id>
- **ns Trafficdomain anzeigen** <td>

So erstellen Sie einen Dienst mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add service** <name> <IP> <serviceType> <port> -**td** <id>
- **show service** <name>

So erstellen Sie einen virtuellen Lastausgleichsserver und binden Dienste mithilfe der Befehlszeilenschnittstelle an diesen:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add lb vserver** <name> <serviceType> <IPAddress> <port> -**td** <id>
- **bind lb vserver** <name> <serviceName>
- **zeige lb vserver** <name>

GUI-Verfahren

So erstellen Sie ein VLAN mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **VLANs**, klicken Sie auf **Hinzufügen**, und legen Sie die Parameter fest.

So erstellen Sie eine Datenverkehrsdomänenentität mit der GUI:

Navigieren Sie zu **System** > **Netzwerk** > **Verkehrsdomänen**, klicken Sie auf **Hinzufügen**, und **legen Sie im Dialogfeld Datenverkehrsdomäne erstellen** die Parameter fest.

So erstellen Sie einen Service mit der GUI:

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**, klicken Sie auf **Hinzufügen**, und legen Sie die Parameter fest.

So erstellen Sie einen virtuellen Lastausgleichsserver mit der GUI:

Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, klicken Sie auf **Hinzufügen**, und legen Sie die Parameter fest.

Inter Traffic Domain Entity Bindings

October 5, 2021

Sie können Dienste in einer Verkehrsdomäne an einen virtuellen Server in einer anderen Verkehrsdomäne binden. Alle Dienste, die an einen virtuellen Server in einer anderen Verkehrsdomäne gebunden werden sollen, müssen sich in derselben Verkehrsdomäne befinden.

Sie konfigurieren diese Unterstützung mithilfe des vorhandenen Befehls bind lb vserver oder der zugehörigen GUI-Prozedur.

Diese Funktion kann die Interaktion zwischen verschiedenen Verkehrsdomänen erleichtern. In einem Unternehmen können Server in verschiedenen Verkehrsdomänen gruppiert werden. Virtuelle Server werden in einer Datenverkehrsdomäne erstellt, die mit dem Internet verbunden ist. Ein virtueller Server aus dieser Datenverkehrsdomäne kann so konfiguriert werden, dass er Server in einer anderen Verkehrsdomäne ausgleicht. Dieser virtuelle Server empfängt Verbindungsanforderungen aus dem Internet, die an die gebundenen Server weitergeleitet werden.

Wenn ein Citrix ADC in einer Cloud-Infrastruktur verwendet wird, kann jedem Mandanten eine separate Datenverkehrsdomäne zugewiesen werden, und alle Ressourcen (einschließlich Server) für einen Mandanten können in der Datenverkehrsdomäne des Mandanten gruppiert werden. Für jeden Mandanten wird ein virtueller Server für Lastausgleichsserver in seiner Verkehrsdomäne erstellt. Alle diese virtuellen Server sind in einer einzigen Datenverkehrsdomäne gruppiert, die dem Internet zugewandt ist.

Betrachten Sie ein Beispiel, in dem Clouddienstanbieter Example-Cloud-A drei Datenverkehrsdomänen mit IDs 10, 20 und 30 auf der Citrix ADC Appliance NS1 konfiguriert sind.

Beispiel-Org-A und Beispiel-Org-B sind Mandanten von Example-Cloud-A. Mandant A wird Verkehrsdomäne 20 zugewiesen, und Mandant B wird Domäne 30 zugewiesen. Die Server S1 und S2 befinden sich in der Verkehrsdomäne 20 und die Server S3 und S4 befinden sich in der Verkehrsdomäne 30.

Traffic Domain 10 steht im Internet. Virtuelle Server LBVS-1 und LBVS-2 werden in der Verkehrsdomäne 10 erstellt. LBVS-1 in der Verkehrsdomäne 10 ist für den Lastenausgleich der Server S1 und S2 konfiguriert, die sich in der Verkehrsdomäne 20 befinden. LBVS-2 in der Verkehrsdomäne 10 ist für den Lastenausgleich der Server S3 und S4 konfiguriert, die sich in der Verkehrsdomäne 30 befinden.

Daher akzeptieren diese virtuellen Server Internetverbindungsanforderungen für Server, die sich in einer anderen Datenverkehrsdomäne als die der virtuellen Server befinden.

virtuelle MAC-basierte Datenverkehrsdomänen

October 5, 2021

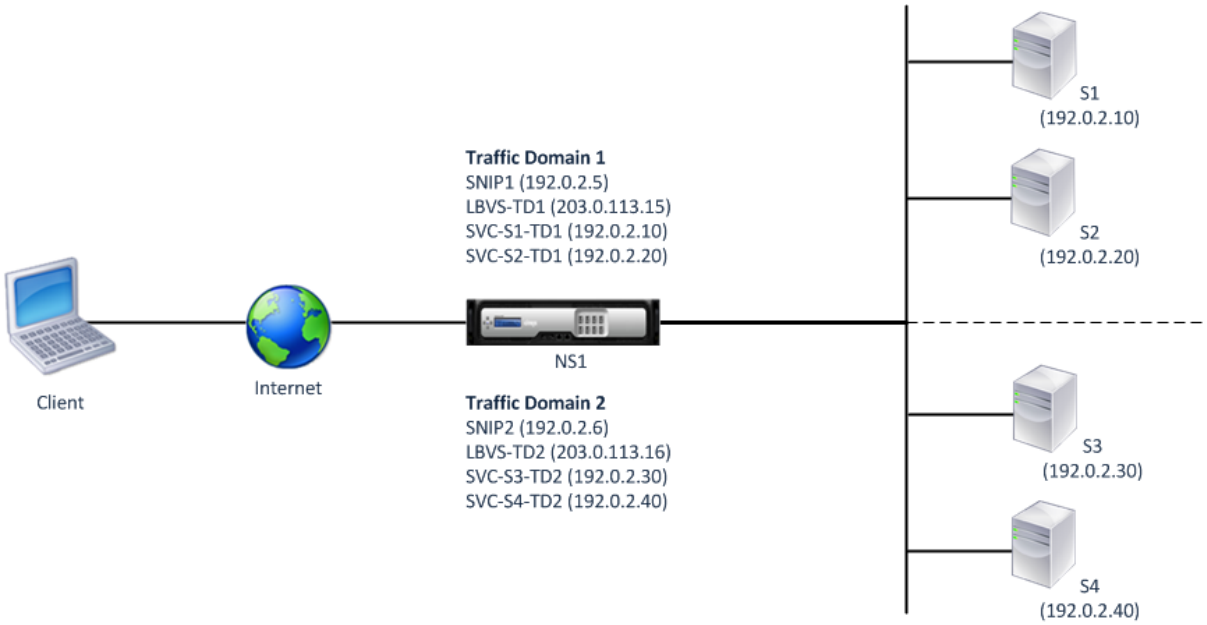
Sie können eine Verkehrsdomäne einer virtuellen MAC-Adresse anstelle von VLANs zuordnen. Der Citrix ADC sendet dann die virtuelle MAC-Adresse der Verkehrsdomäne in allen Antworten an ARP-Abfragen für Netzwerkentitäten in dieser Domäne. Dadurch kann der ADC nachfolgenden eingehenden Datenverkehr für verschiedene Verkehrsdomänen anhand der Ziel-MAC-Adresse trennen, da die Ziel-MAC-Adresse die virtuelle MAC-Adresse einer Verkehrsdomäne ist. Nachdem Sie Entitäten in einer Verkehrsdomäne erstellt haben, können Sie sie einfach verwalten und überwachen, indem Sie Vorgänge auf Domänenebene ausführen.

Betrachten Sie ein Beispiel, in dem zwei Datenverkehrsdomänen mit IDs 1 und 2 auf der Citrix ADC Appliance NS1 konfiguriert sind. Citrix ADC erstellt einen virtuellen MAC-Adressen-MAC1 und ordnet ihn der Verkehrsdomäne 1 zu. Ähnlich hat Citrix ADC eine weitere virtuelle MAC-Adresse erstellt, die virtuelle MAC2 und der Verkehrsdomäne 2 zugeordnet ist.

In der Verkehrsdomäne 1 ist der Lastenausgleichsserver LBVS-TD1 so konfiguriert, dass der Datenverkehr über die Server S1 und S2 verteilt wird. Auf der Citrix ADC Appliance werden Server S1 und S2 durch die Dienste SVC1-TD1 bzw. SVC2-TD1 dargestellt. Eine Subnetz-IP-Adresse (SNIP) SNIP1 ist so konfiguriert, dass Citrix ADC mit S1 und S2 kommunizieren kann. Da der virtuelle MAC1 der Verkehrsdomäne 1 zugeordnet ist, sendet die Appliance virtuellen MAC1 als MAC-Adresse in allen ARP-Ankündigungen und ARP-Antworten für LBVS-TD1 und SNIP1.

Ähnlich in der Verkehrsdomäne 2 ist der Lastenausgleichsserver LBVS-TD2 so konfiguriert, dass der Datenverkehr über S3 und S4 verteilt wird. Auf der Citrix ADC Appliance werden die Server S3 und S4 durch die Dienste SVC3-TD2 bzw. SVC4-TD2 dargestellt. Eine SNIP-Adresse SNIP2 ist so konfiguriert, dass Citrix ADC mit S3 und S4 kommunizieren kann. Da virtueller MAC2 mit Verkehrsdomäne 2 verknüpft ist, sendet die Appliance virtuellen MAC2 als MAC-Adresse in allen ARP-Ankündigungen und ARP-Antworten für LBVS-TD2 und SNIP2.

Der Citrix ADC trennt den nachfolgenden eingehenden Datenverkehr für Verkehrsdomänen 1 oder 2 auf Basis der Ziel-MAC-Adresse, wenn die Ziel-MAC-Adresse virtueller MAC1 oder virtueller MAC2 ist.



In der folgenden Tabelle sind die Einstellungen aufgeführt, die im Beispiel verwendet werden: Beispieleinstellungen für virtuelle MAC-basierte Datenverkehrsdomäne.

Bevor Sie beginnen

Im Folgenden sind Punkte zu beachten, bevor Sie virtuelle MAC-basierte Datenverkehrsdomäne konfigurieren:

1. virtuelle MAC-basierte Datenverkehrsdomänen sind der einfachste Weg, um die Trennung des Netzwerkverkehrs zu erreichen.
2. Da virtuelle MAC-basierte Datenverkehrsdomänen den Netzwerkverkehr basierend auf virtuellen MAC-Adressen und nicht auf VLANS trennen, können Sie keine doppelten IP-Adressen auf verschiedenen virtuellen MAC-basierten Datenverkehrsdomänen auf einem Citrix ADC erstellen.
3. virtuelle MAC-basierte Datenverkehrsdomänen funktionieren nicht, wenn Citrix ADC nur im L2-Modus bereitgestellt wird.
4. Sowohl VLAN- als auch virtuelle MAC-basierte Datenverkehrsdomänen können auf einem Citrix ADC koexistieren. Virtuelle MAC-basierte Datenverkehrsdomänen werden tatsächlich auf allen VLANs ausgeführt, die nicht an eine VLAN-basierte Datenverkehrsdomäne gebunden sind.

Konfigurationsschritte

Das Konfigurieren einer virtuellen MAC-basierten Datenverkehrsdomäne auf einer Citrix ADC Appliance umfasst die folgenden Aufgaben:

- Erstellen Sie eine Datenverkehrsdomänenentität und aktivieren Sie die virtuelle MAC-Option.

Erstellen Sie eine Datenverkehrsdomänenentität, die eindeutig durch eine ID identifiziert wird, bei der es sich um einen ganzzahligen Wert handelt, und aktivieren Sie dann die virtuelle MAC-Option. Nach dem Erstellen der Datenverkehrsdomänenentität erstellt Citrix ADC eine virtuelle MAC-Adresse und ordnet sie dann der Datenverkehrsdomänenentität zu.

- Erstellen Sie Feature-Entitäten auf der Traff Erstellen Sie die erforderlichen Feature-Entitäten in der Verkehrsdomäne, indem Sie beim Konfigurieren dieser Feature-Entitäten den Traffic-Domain-Identifier (td) angeben. Citrix ADC eigene Netzwerkeinheiten, die in einer virtuellen MAC-basierten Datenverkehrsdomäne erstellt wurden, sind mit der virtuellen MAC-Adresse verknüpft, die der Verkehrsdomäne zugeordnet ist. Der Citrix ADC sendet dann die virtuelle MAC-Adresse der Verkehrsdomäne in ARP-Ankündigungen und ARP-Antworten für diese Netzwerkentitäten.

CLI-Verfahren

So erstellen Sie eine virtuelle MAC-basierte Datenverkehrsdomäne mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
ns hinzufügen TrafficDomain <td> [-vmac (            DISABLED )]
ENABLED
```

-
- ns Trafficdomain anzeigen <td>

So konfigurieren Sie eine SNIP-Adresse mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add ns ip <IPAddress> <netmask> -type SNIP –td <id>
- show ns ip <IPAddress> -td <id>

So erstellen Sie einen Dienst mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add service <name> <IP> <serviceType> <port> -td <id>
- show service <name> -td <id>

So erstellen Sie einen virtuellen Lastausgleichsserver und binden Dienste mithilfe der Befehlszeilenschnittstelle an diesen:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add lb vserver <name> <serviceType> <IPAddress> <port> -td <id>
- bind lb vserver <name> <serviceName>

- show lb vserver <name> -td <id>

Beispiel:

```
> add ns trafficDomain 1 -vmac ENABLED
 Done
> add ns trafficDomain 2 -vmac ENABLED
 Done

> add ns ip 192.0.2.5 255.255.255.0 -type -SNIP -td 1
 Done
> add service  SVC-S1-TD1  192.0.2.10 HTTP 80 -td 1
 Done
> add service  SVC-S2-TD1  192.0.2.20 HTTP 80 -td 1
 Done
> add lb vserver  LBVS-TD1 HTTP   203.0.113.15 80 -td 1
 Done
> bind lb vserver  LBVS-TD1 SVC-S1-TD1
 Done
> bind lb vserver  LBVS-TD1 SVC-S2-TD1
 Done

> add ns ip 192.0.2.6 255.255.255.0 -type -SNIP -td 2
 Done
> add service  SVC-S3-TD2  192.0.2.30 HTTP 80 -td 2
 Done
> add service  SVC-S4-TD2  192.0.2.40 HTTP 80 -td 2
 Done
> add lb vserver  LBVS-TD1 HTTP   203.0.113.16 80 -td 1
 Done
> bind lb vserver  LBVS-TD2 SVC-S3-TD2
 Done
> bind lb vserver  LBVS-TD2 SVC-S3-TD2
 Done
<!--NeedCopy-->
```

GUI-Verfahren

So erstellen Sie eine virtuelle MAC-basierte Datenverkehrsdomäne mit der GUI:

1. Navigieren Sie zu System > Netzwerk > Interfaces.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Legen Sie auf der Seite Traffic-Domain erstellen die folgenden Parameter fest:

- Verkehrsdomänen-ID*
- Mac aktivieren

4. Klicken Sie auf Erstellen.

So konfigurieren Sie eine SNIP-Adresse mit der GUI:

1. Navigieren Sie zu System > Netzwerk > IPs > IPv4
2. Navigieren Sie zu Netzwerk > IPs > IPv4
3. Klicken Sie im Detailbereich auf Hinzufügen
4. Legen Sie auf der Seite IP erstellen die folgenden Parameter fest. Für eine Beschreibung eines Parameters bewegen Sie den Mauszeiger über das entsprechende Feld.
   - IP-Adresse
   - Netzmaske
   - IP-Typ
   - Traffic-Domain-ID
5. Klicken Sie auf Erstellen.

So erstellen Sie einen Service mit der GUI:

1. Navigieren Sie zu Traffic Management > Load Balancing > Services.
2. Klicken Sie im Detailbereich auf “Hinzufügen”.
3. Legen Sie auf der Seite Grundeinstellungen die folgenden Parameter fest. Für eine Beschreibung eines Parameters bewegen Sie den Mauszeiger über das entsprechende Feld.
   - Dienstname
   - Server
   - Protokoll
   - Port
   - Traffic-Domain-ID
4. Klicken Sie auf Weiter, und klicken Sie auf Fertig.
5. Wiederholen Sie die Schritte 2-4, um einen anderen Dienst zu erstellen.
6. Klicken Sie auf Schließen.

So erstellen Sie einen virtuellen Lastausgleichsserver und binden Dienste mit der GUI an ihn:

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Klicken Sie im Bereich Load Balancing Virtual Servers auf Hinzufügen.
3. Legen Sie im Dialogfeld Virtuelle Server erstellen (Load Balancing) die folgenden Parameter fest. Für eine Beschreibung eines Parameters bewegen Sie den Mauszeiger über das entsprechende Feld.
   - Name
   - IP-Adresse
   - Protokoll
   - Port
   - Traffic-Domain-ID

4. Klicken Sie auf Weiter, klicken Sie im Dienstbereich auf >.
5. Klicken Sie auf der Seite Dienst auf Einfügen, und aktivieren Sie dann das Kontrollkästchen für die Dienste, die Sie an den virtuellen Server binden möchten.
6. Klicken Sie auf Weiter, und klicken Sie auf Fertig.
7. Wiederholen Sie die Schritte 2-5, um einen anderen virtuellen Server zu erstellen

VXLAN

October 5, 2021

Citrix ADC Appliances unterstützen Virtual eXtensible Local Area Networks (VxLANs). Ein VXLAN überlagert Layer-2-Netzwerke auf eine Layer-3-Infrastruktur, indem Layer-2-Frames in UDP-Paketen gekapselt werden. Jedes Overlay-Netzwerk wird als VXLAN-Segment bezeichnet und wird durch einen eindeutigen 24-Bit-Kennzeichner namens VXLAN Network Identifier (VNI) identifiziert. Nur Netzwerkgeräte innerhalb desselben VXLAN können miteinander kommunizieren.

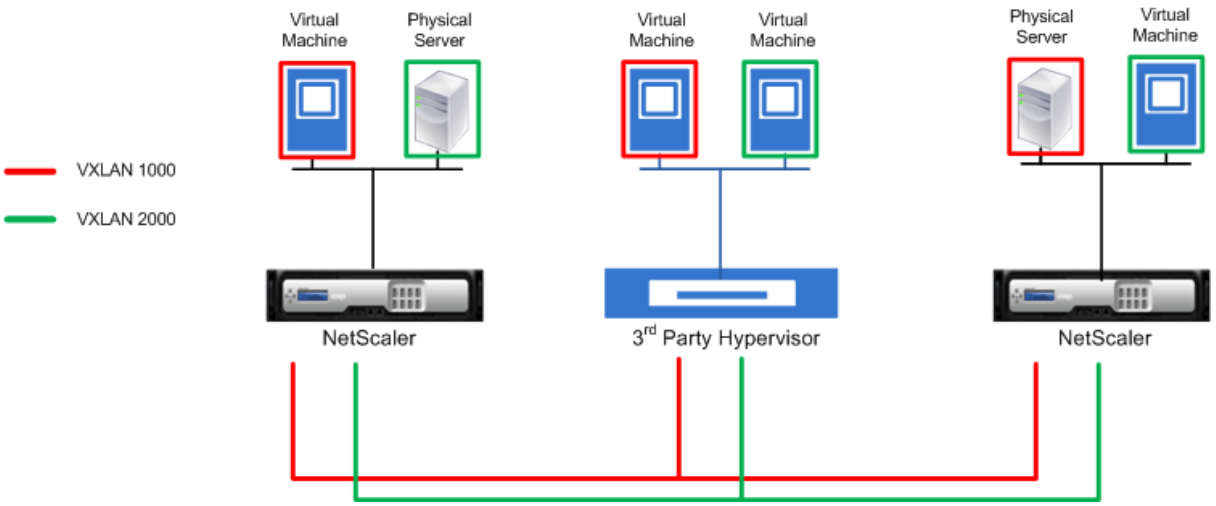
VxLANs bieten dieselben Ethernet-Layer-2-Netzwerkdienste wie VLANs, jedoch mit größerer Erweiterbarkeit und Flexibilität. Die beiden Hauptvorteile der Verwendung von VXLANs sind die folgenden:

- **Höhere Skalierbarkeit.** Servervirtualisierung und Cloud-Computing-Architekturen haben die Nachfrage nach isolierten Layer-2-Netzwerken in einem Rechenzentrum drastisch erhöht. Die VLAN-Spezifikation verwendet eine 12-Bit-VLAN-ID, um ein Layer-2-Netzwerk zu identifizieren, sodass Sie nicht über 4094 VLANs skalieren können. Diese Zahl kann unzureichend sein, wenn Tausende isolierter Layer-2-Netzwerke erforderlich sind. Der 24-Bit-VNI bietet Platz für bis zu 16 Millionen VXLAN-Segmente in derselben Administrationsdomäne.
- **Höhere Flexibilität.** Da VXLAN Layer-2-Datenrahmen über Layer-3-Pakete trägt, erweitern VXLANs L2-Netzwerke über verschiedene Teile eines Rechenzentrums und über geografisch getrennte Rechenzentren. Anwendungen, die in verschiedenen Teilen eines Rechenzentrums und in verschiedenen Rechenzentren gehostet werden, aber Teil desselben VXLAN sind, werden als ein zusammenhängender Netzwerk angezeigt.

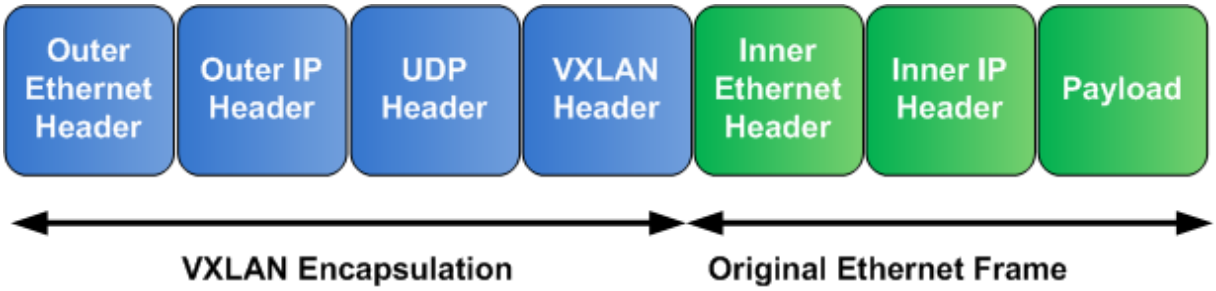
Funktionsweise von VxLANs

VXLAN-Segmente werden zwischen VXLAN-Tunnelendpunkten (VTEPs) erstellt. VTEPs unterstützen das VXLAN-Protokoll und führen VXLAN-Verkapselung und Entkapselung durch. Man kann sich ein VXLAN-Segment als Tunnel zwischen zwei VTEPs vorstellen, wobei ein VTEP einen Layer2-Frame mit einem UDP-Header und einem IP-Header kapselt und ihn durch den Tunnel sendet. Der andere VTEP empfängt und entkapselt das Paket, um den Layer 2-Frame zu erhalten. Ein Citrix ADC ist ein Beispiel für einen VTEP. Weitere Beispiele sind Hypervisoren von Drittanbietern, VXLAN-fähige virtuelle Maschinen und VXLAN-fähige Switches.

Die folgende Abbildung zeigt virtuelle Maschinen und physische Server, die über VXLAN-Tunnel verbunden sind.



In der folgenden Abbildung wird das Format eines VXLAN-Pakets angezeigt.



VXLANs auf einem Citrix ADC verwenden einen Layer 2-Mechanismus zum Senden von Broadcast-, Multicast- und unbekannten Unicast-Frames. Ein VXLAN unterstützt die folgenden Modi zum Senden dieser L2-Frames.

- **Unicast-Modus**: In diesem Modus geben Sie die IP-Adressen von VTEPs an, während Sie ein VXLAN auf einem Citrix ADC konfigurieren. Das Citrix ADC sendet Broadcast-, Multicast- und unbekannte Unicast-Frames über Layer 3 an alle VTEPs dieses VXLAN.
- **Multicastmodus**: In diesem Modus geben Sie beim Konfigurieren eines VXLAN auf einem Citrix ADC eine Multicastgruppen-IP-Adresse an. Citrix ADCs unterstützen kein IGMP-Protokoll (Internet Group Management Protocol). Citrix ADCs verlassen sich darauf, dass der Upstream-Router einer Multicastgruppe beitritt, die eine gemeinsame IP-Adresse der Multicastgruppe gemeinsam verwendet. Citrix ADC sendet Broadcast-, Multicast- und unbekannte Unicast-Frames über Layer 3 an die IP-Adresse der Multicastgruppe dieses VXLAN.

Ähnlich wie bei einer Layer-2-Bridge-Tabelle pflegen Citrix ADCs VXLAN-Zuordnungstabellen basierend auf dem inneren und äußeren Header der empfangenen VXLAN-Pakete. Diese Tabelle ordnet die Remote-Host-MAC-Adressen zu VTEP-IP-Adressen für ein bestimmtes VXLAN zu. Citrix ADC verwendet die VXLAN-Zuordnungstabelle, um die Ziel-MAC-Adresse eines Layer 2-Frames zu

suchen. Wenn ein Eintrag für diese MAC-Adresse in der VXLAN-Tabelle vorhanden ist, sendet Citrix ADC den Layer 2-Frame über Layer 3 unter Verwendung des VXLAN-Protokolls an die zugeordnete VTEP-IP-Adresse, die im Zuordnungseintrag für ein VXLAN angegeben ist.

Da VXLANs ähnlich wie VLANs funktionieren, unterstützen die meisten Citrix ADC Features, die VLAN als Klassifizierungsparameter unterstützen, VXLAN. Zu diesen Funktionen gehört eine optionale VXLAN-Parametereinstellung, die den VXLAN-VNI angibt.

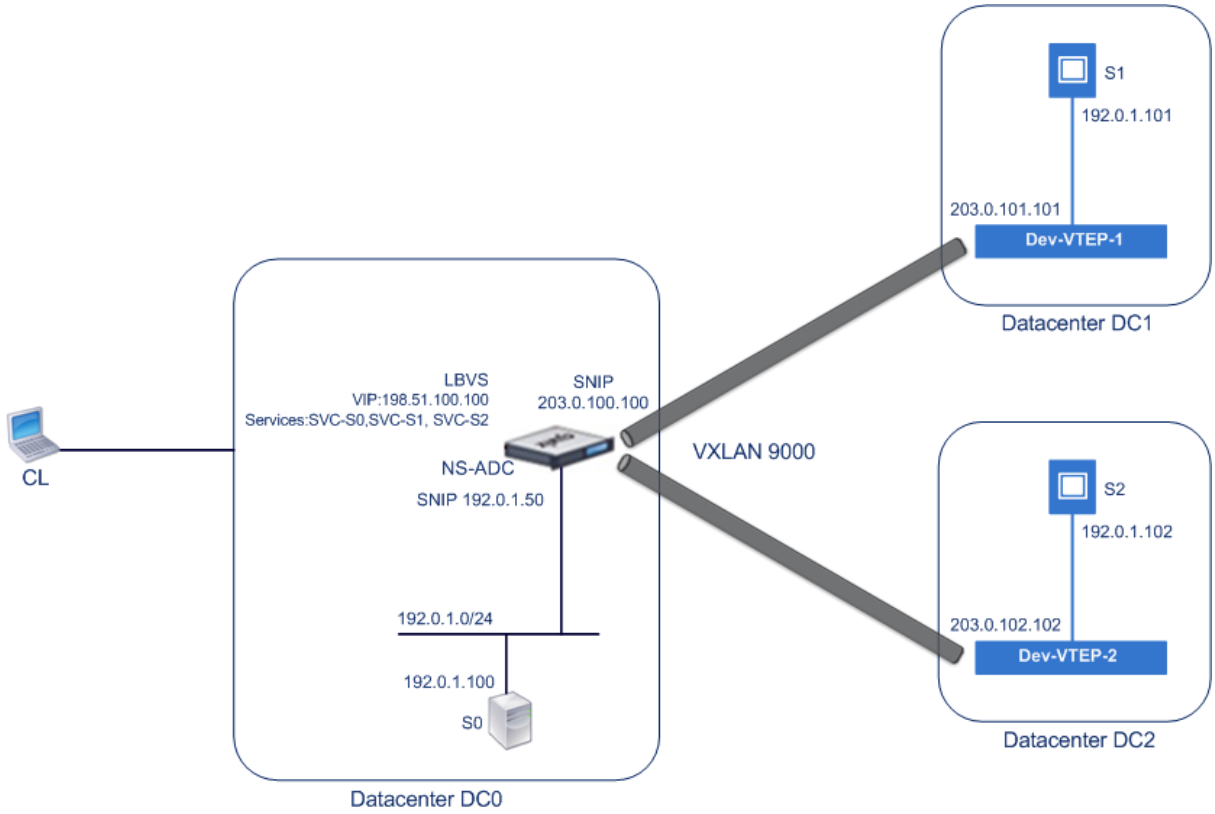
In einer High Availability (HA) -Konfiguration wird die VXLAN-Konfiguration weitergegeben oder mit dem sekundären Knoten synchronisiert.

VXLAN-Anwendungsfall: Lastenausgleich über Rechenzentren hinweg

Um die VXLAN-Funktionalität eines Citrix ADC zu verstehen, betrachten Sie ein Beispiel, in dem Example Corp eine Site unter www.example.com hostet. Um die Anwendungsverfügbarkeit zu gewährleisten, wird der Standort auf den drei Servern S0, S1 und S2 gehostet. Für den Lastenausgleich dieser Server wird ein virtueller Lastausgleichsserver, LBVS, auf Citrix ADC NS-ADC verwendet. S0, S1 und S2 befinden sich in Rechenzentren DC0, DC1 und DC2. In DC0 ist Server S0 mit NS-ADC verbunden.

S0 ist ein physischer Server und S1 und S2 sind virtuelle Maschinen (VMs). S1 wird auf dem Virtualisierungs-Hostgerät Dev-VTEP-1 im Rechenzentrum DC1 ausgeführt, und S2 wird auf dem Hostgerät Dev-VTEP-2 in DC2 ausgeführt. NS-ADC, Dev-VTEP-1 und Dev-VTEP-2 unterstützen das VXLAN-Protokoll.

S0, S1 und S2 sind Teil des gleichen privaten Subnetzes 192.0.1.0/24. S0, S1 und S2 sind Teil einer gemeinsamen Broadcastdomäne, VXLAN 9000 ist auf NS-ADC, Dev-VTEP-1 und Dev-VTEP-2 konfiguriert. Server S1 und S2 sind Teil von VXLAN9000 auf Dev-VTEP-1 bzw. Dev-VTEP-2.



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt: VXLAN-Einstellungen.

Die Dienste SVC-S0, SVC-S1 und SVC-S2 auf NS-ADC stellen S0, S1 und S2 dar. Sobald diese Dienste konfiguriert sind, sendet NS-ADC ARP-Anforderungen für S0, S1 und S2, um die IP-zu-Mac-Zuordnung aufzulösen. Diese ARP-Anfragen werden auch über VXLAN 9000 an Dev-VTEP-1 und Dev-VTEP-2 gesendet.

Im Folgenden ist der Verkehrsfluss zum Auflösen der ARP-Anforderung für S2:

1. NS-ADC sendet eine ARP-Anforderung für S2, um die IP-zu-Mac-Zuordnung aufzulösen. Dieses Paket hat:
   - Quell-IP-Adresse = Subnetz-IP-Adresse SNIP-für-Server (192.0.1.50)
   - Quell-MAC-Adresse = MAC-Adresse der Schnittstelle des NS-ADC, von der das Paket gesendet wird = NS-MAC-1
2. NS-ADC bereitet das ARP-Paket für den Versand über das VXLAN 9000 vor, indem es das Paket mit folgenden Headern kapselt:
   - VXLAN-Header mit ID (VNI) 9000
   - Standard-UDP-Header, UDP-Prüfsumme auf 0×0000 und Zielport auf 4789 festgelegt.
3. NS-ADC sendet das resultierende gekapselte Paket an Dev-VTEP-1 und Dev-VTEP-2 auf VXLAN-9000. Das gekapselte Paket hat:
   - Quell-IP-Adresse = SNIP-VTEP-0 (203.0.100.100).

4. Dev-VTEP-2 empfängt das UDP-Paket und entkapselt den UDP-Header, von dem Dev-VTEP-2 erfährt, dass das Paket ein VXLAN-bezogenes Paket ist. Dev-VTEP-2 entkapselt dann den VXLAN-Header und lernt die VXLAN-ID des Pakets. Das resultierende Paket ist das ARP-Anforderungspaket für S2, das gleiche wie in Schritt 1 ist.
5. Aus dem inneren und äußeren Header des VXLAN-Pakets macht Dev-VTEP-2 einen Eintrag in seine VXLAN-Zuordnungstabelle, der die Zuordnung von MAC-Adresse (NS-MAC-1) und SNIP-VTEP-0 (203.0.100.100) für VXLAN9000 anzeigt.
6. Dev-VTEP-2 sendet das ARP-Paket an S2. Das Antwortpaket von S2 erreicht Dev-VTEP-2. Dev-VTEP-2 führt eine Suche in seiner VXLAN-Zuordnungstabelle durch und erhält eine Übereinstimmung mit der Ziel-MAC-Adresse NS-MAC-1. Der Dev-VTEP-2 weiß nun, dass NS-MAC-1 über SNIP-VTEP-0 (203.0.100.100) über VXLAN 9000 erreichbar ist.
7. S2 antwortet mit seiner MAC-Adresse (MAC-S2). Das ARP-Antwortpaket hat:
    - Ziel-IP-Adresse = Subnetz-IP-Adresse SNIP-für-Server (192.0.1.50)
    - Ziel-MAC-Adresse = NS-MAC-1
8. Das Antwortpaket von S2 erreicht Dev-VTEP-2. Dev-VTEP-2 führt eine Suche in seiner VXLAN-Zuordnungstabelle durch und erhält eine Übereinstimmung mit der Ziel-MAC-Adresse NS-MAC-1. Der Dev-VTEP-2 weiß nun, dass NS-MAC-1 über SNIP-VTEP-0 (203.0.100.100) über VXLAN 9000 erreichbar ist. Dev-VTEP-2 kapselt die ARP-Antwort mit VXLAN- und UDP-Headern und sendet das resultierende Paket an SNIP-VTEP-0 (203.0.100.100) von NS-ADC.
9. NS-ADC beim Empfang des Pakets entkapselt das Paket, indem die VXLAN- und UDP-Header entfernt werden. Das resultierende Paket ist die ARP-Antwort von S2. NS-ADC aktualisiert die VXLAN-Zuordnungstabelle für S2 MAC-Adresse (MAC-S2) mit Dev-VTEP-2 IP-Adresse (203.0.102.102) für VXLAN 9000. NS-ADC aktualisiert auch die ARP-Tabelle für die IP-Adresse von S2 (192.0.1.102) mit der MAC-Adresse von S2 (MAC-S2).

Im Folgenden ist der Datenverkehr für den Lastenausgleich virtuellen Server LBVS in diesem Beispiel:

1. Client CL sendet ein Anforderungspaket an LBVS von NS-ADC. Das Anforderungspaket hat:
    - Quell-IP-Adresse = IP-Adresse des Client-CL (198.51.100.90)
    - Ziel-IP-Adresse = IP-Adresse (VIP) von LBVS = 198.51.110.100
2. LBVS von NS-ADC empfängt das Anforderungspaket, und sein Lastausgleichsalgorithmus wählt Server S2 des Rechenzentrums DC2 aus.
3. NS-ADC verarbeitet das Anforderungspaket und ändert seine Ziel-IP-Adresse in die IP-Adresse von S2 und seine Quell-IP-Adresse in eine der auf NS-ADC konfigurierten Subnetz-IP-Adressen (SNIP). Das Anforderungspaket hat:
    - Quell-IP-Adresse = Subnetz-IP-Adresse auf NS-ADC= SNIP-für-Server (192.0.1.50)
    - Ziel-IP-Adresse = IP-Adresse von S2 (192.0.1.102)
4. NS-ADC findet einen VXLAN-Zuordnungseintrag für S2 in seiner Bridge-Tabelle. Dieser Eintrag zeigt an, dass S2 über Dev-VTEP-2 über VXLAN 9000 erreichbar ist.
5. NS-ADC bereitet das Paket vor, das über das VXLAN 9000 gesendet werden soll, indem das Paket mit folgenden Headern kapselt wird:

    - VXLAN-Header mit ID (VNI) 9000
    - Standard-UDP-Header, UDP-Prüfsumme auf 0×0000 und Zielport auf 4789 festgelegt.
6. NS-ADC sendet das resultierende gekapselte Paket an Dev-VTEP-2. Das Anforderungspaket hat:
    - Quell-IP-Adresse = SNIP-Adresse = SNIP-VTEP-0 (203.0.100.100)
    - Ziel-IP-Adresse = IP-Adresse von Dev-VTEP-2 (203.0.102.102)
7. Dev-VTEP-2 empfängt das UDP-Paket und entkapselt den UDP-Header, von dem Dev-VTEP-2 erfährt, dass das Paket ein VXLAN-bezogenes Paket ist. Dev-VTEP-2 entkapselt dann den VXLAN-Header und lernt die VXLAN-ID des Pakets. Das resultierende Paket ist das gleiche Paket wie in Schritt 3.
8. Dev-VTEP-2 leitet das Paket dann an S2 weiter.
9. S2 verarbeitet das Anforderungspaket und sendet die Antwort an die SNIP-Adresse von NS-ADC. Das Antwortpaket hat:
    - Quell-IP-Adresse = IP-Adresse von S2 (192.0.1.102)
    - Ziel-IP-Adresse = Subnetz-IP-Adresse auf NS-ADC= SNIP-für-Server (192.0.1.50)
10. Dev-VTEP-2 kapselt das Antwortpaket auf die gleiche Weise, wie NS-ADC das Anforderungspaket in den Schritten 4 und 5 kapselte. Dev-VTEP-2 sendet dann das gekapselte UDP-Paket an SNIP-Adresse SNIP-for-Server (192.0.1.50) von NS-ADC.
11. NS-ADC entkapselt nach Erhalt des gekapselten UDP-Pakets das Paket, indem die UDP- und VXLAN-Header auf die gleiche Weise entfernt werden, wie Dev-VTEP-2 das Paket in Schritt 7 entkapselt hat. Das resultierende Paket ist das gleiche Antwortpaket wie in Schritt 9.
12. NS-ADC verwendet dann die Sitzungstabelle für den Lastenausgleich des virtuellen Servers LBVS und leitet das Antwortpaket an die Client-CL weiter. Das Antwortpaket hat:
    - Quell-IP-Adresse = IP-Adresse des Client-CL (198.51.100.90)
    - Ziel-IP-Adresse = IP-Adresse (VIP) von LBVS (198.51.110.100)

Zu berücksichtigende Punkte für die Konfiguration von VxLANs

Berücksichtigen Sie die folgenden Punkte, bevor Sie VxLANs auf einem Citrix ADC konfigurieren:

- Auf einem Citrix ADC können maximal 2048 VXLANs konfiguriert werden.
- VxLANs werden in einem Cluster nicht unterstützt.
- Link-lokale IPv6-Adressen können nicht für jedes VXLAN konfiguriert werden.
- Citrix ADCs unterstützen kein IGMP-Protokoll (Internet Group Management Protocol), um eine Multicastgruppe zu bilden. Citrix ADCs verlassen sich auf das IGMP-Protokoll des Upstream-Routers, um einer Multicastgruppe beizutreten, die eine gemeinsame IP-Adresse der Multicastgruppe gemeinsam nutzen. Sie können eine Multicastgruppen-IP-Adresse angeben, während Sie VXLAN-Bridge-Tabelleneinträge erstellen, die Multicastgruppe muss jedoch auf dem Upstream-Router konfiguriert werden. Citrix ADC sendet Broadcast-, Multicast- und unbekannte Unicast-Frames über Layer 3 an die IP-Adresse der Multicastgruppe dieses VXLAN.

Der Upstream-Router leitet das Paket dann an alle VTEPs weiter, die Teil der Multicastgruppe sind.

- Die VXLAN-Kapselung fügt jedem Paket einen Overhead von 50 Byte hinzu:

  Externer Ethernet-Header (14) + UDP-Header (8) + IP-Header (20) + VXLAN-Header (8) = 50 Bytes

  Um Fragmentierung und Leistungseinbußen zu vermeiden, müssen Sie die MTU-Einstellungen aller Netzwerkgeräte in einem VXLAN-Pfad, einschließlich der VXLAN-VTEP-Geräte, so anpassen, dass die 50 Bytes Overhead in den VXLAN-Paketen verarbeitet werden.

  Wichtig: Jumbo-Frames werden auf den virtuellen Citrix ADC VPX Appliances, Citrix ADC SDX-Appliances und Citrix ADC MPX 15000/17000 Appliances nicht unterstützt. Diese Appliances unterstützen eine MTU-Größe von nur 1500 Bytes und können nicht angepasst werden, um den 50-Byte-Overhead von VXLAN-Paketen zu verarbeiten. VXLAN-Datenverkehr ist möglicherweise fragmentiert oder beeinträchtigt die Leistung, wenn sich eine dieser Appliances im VXLAN-Pfad befindet oder als VXLAN-VTEP-Gerät fungiert.

- Bei Citrix ADC SDX-Appliances funktioniert die VLAN-Filterung nicht für VXLAN-Pakete.
- Sie können keinen MTU-Wert in einem VXLAN festlegen.
- Schnittstellen können nicht an ein VXLAN gebunden werden.

Konfigurationsschritte

Die Konfiguration eines VXLAN auf einer Citrix ADC Appliance umfasst die folgenden Aufgaben:

- **Fügen Sie eine VXLAN-Entität**hinzu. Erstellen Sie eine VXLAN-Entität, die eindeutig durch eine positive Ganzzahl identifiziert wird, die auch als VXLAN Network Identifier (VNI) bezeichnet wird. In diesem Schritt können Sie auch den Ziel-UDP-Port von Remote-VTEP angeben, auf dem das VXLAN-Protokoll ausgeführt wird. Standardmäßig ist der Ziel-UDP-Port-Parameter für die VXLAN-Entität auf 4789 festgelegt. Diese UDP-Port-Einstellung muss mit den Einstellungen auf allen Remote-VTEPs für dieses VXLAN übereinstimmen. Sie können VLANs auch an dieses VXLAN binden. Der Datenverkehr (einschließlich Broadcasts, Multicasts, unbekannte Unicasts) aller gebundenen VLANs ist über dieses VXLAN erlaubt. Wenn keine VLANs an das VXLAN gebunden sind, erlaubt das Citrix ADC den Datenverkehr aller VLANs auf diesem VXLAN, die nicht zu anderen VXLANs gehören.
- **Binden Sie die lokale VTEP-IP-Adresse und an die VXLAN-Entität**. Binden Sie eine der konfigurierten SNIP-Adresse an das VXLAN an ausgehende VXLAN-Pakete.
- **Fügen Sie einen überbrückbaren Eintrag**hinzu. Fügen Sie einen überbrückbaren Eintrag hinzu, der die VXLAN-ID und die entfernte VTEP-IP-Adresse für das zu erstellende VXLAN angibt.
- **(Optional) Binden Sie verschiedene Feature-Entitäten an das konfigurierte VXLAN**. VXLANs funktionieren ähnlich wie VLANs. Die meisten Citrix ADC Features, die VLAN als Klas-

sifizierungsparameter unterstützen, unterstützen auch VXLAN. Zu diesen Funktionen gehört eine optionale VXLAN-Parametereinstellung, die den VXLAN-VNI angibt.

- **(Optional) Zeigt die VXLAN-Zuordnungstabelle**an. Zeigen Sie die VXLAN-Zuordnungstabelle an, die Zuordnungseinträge für Remote-Host-MAC-Adresse zu VTEP-IP-Adresse für ein bestimmtes VXLAN enthält. Mit anderen Worten, eine VXLAN-Zuordnung besagt, dass ein Host über das VTEP auf einem bestimmten VXLAN erreichbar ist. Citrix ADC lernt VXLAN-Zuordnungen und aktualisiert seine Zuordnungstabelle von den empfangenen VXLAN-Paketen. Citrix ADC verwendet die VXLAN-Zuordnungstabelle, um nach der Ziel-MAC-Adresse eines Layer-2-Frames zu suchen. Wenn ein Eintrag für diese MAC-Adresse in der VXLAN-Tabelle vorhanden ist, sendet Citrix ADC den Layer 2-Frame über Layer 3 unter Verwendung des VXLAN-Protokolls an die zugeordnete VTEP-IP-Adresse, die im Zuordnungseintrag für ein VXLAN angegeben ist.

CLI-Verfahren

So fügen Sie eine VXLAN-Entität mit der CLI hinzu:

Geben Sie an der Eingabeaufforderung

- **add vxlan** <id>
- **show vxlan**<id>

So binden Sie die lokale VTEP-IP-Adresse mit der CLI an das VXLAN:

Geben Sie an der Eingabeaufforderung

- **bind vxlan** <id> -**SrcIP** <IPaddress>
- **show vxlan** <id>

So fügen Sie eine Bridgetable mit der CLI hinzu:

Geben Sie an der Eingabeaufforderung

- **add bridgetable** -**mac** <macaddress> -**vxlan** <ID> -**vtep** <IPaddress>
- **show bridgetable**

So zeigen Sie die VXLAN-Weiterleitungstabelle mithilfe der Befehlszeile an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **show bridgetable**

GUI-Verfahren

So fügen Sie eine VXLAN-Entität hinzu und binden eine lokale VTEP-IP-Adresse mit der GUI:

Navigieren Sie zu **System** > **Network** > **VxLans**, und fügen Sie eine neue VXLAN-Entität hinzu oder ändern Sie eine vorhandene VXLAN-Entität.

So fügen Sie eine Bridgetable mit der GUI hinzu:

Navigieren Sie zu **System** > **Netzwerk** > **Bridge Table**, und legen Sie die folgenden Parameter fest, während Sie einen Eintrag in der VXLAN-Brückentabelle hinzufügen oder ändern:

- MAC
- VTEP
- VXLAN-ID

So zeigen Sie die VXLAN-Weiterleitungstabelle mit der GUI an:

Navigieren Sie zu **System** > **Netzwerk** > **Bridge-Tabelle**.

```
Example
> add vxlan 9000
Done
> bind vxlan 9000 -srcIP 203.0.100.100

Done
> add bridgetable -mac 00:00:00:00:00:00 -vxlan 9000 -vtep
    203.0.101.101

Done
> add bridgetable -mac 00:00:00:00:00:00 -vxlan 9000 -vtep
    203.0.102.102

Done
```

Unterstützung von IPv6 Dynamic Routing-Protokollen auf VxLANs

Die Citrix ADC Appliance unterstützt dynamische IPv6-Routing-Protokolle für VXLANs. Sie können verschiedene IPv6 Dynamic Routing Protokolle (z. B. OSPFv3, RipNG, BGP) auf VXLANs über die VTYSH Befehlszeile konfigurieren. Zum VXLAN-Befehlssatz wurde eine Option IPv6 Dynamic Routing Protocol hinzugefügt, um dynamische IPv6-Routingprotokolle auf einem VXLAN zu aktivieren oder zu deaktivieren. Nach dem Aktivieren dynamischer IPv6-Routingprotokolle auf einem VXLAN müssen Prozesse im Zusammenhang mit den dynamischen IPv6-Routingprotokollen im VXLAN mithilfe der VTYSH Befehlszeile gestartet werden.

So aktivieren Sie dynamische IPv6-Routingprotokolle auf einem VXLAN mit der CLI:

- **add vxlan** <ID>[-**IPv6DynamicRouting** (**ENABLED** | **DEAKTIVIERT**)]
- **show vxlan**


```
In the following sample configuration, VXLAN-9000 is created and has
    IPv6 dynamic routing protocols enabled on it. Then, using the VTYSH
    command line, process for the IPv6 OSPF protocol is started on the
    VXLAN.

> add vxlan 9000 -ipv6DynamicRouting ENABLED

Done
> bind vxlan 9000 -srcIP 203.0.100.100

Done
> add bridgetable -mac 00:00:00:00:00:00 -vxlan 9000 -vtep
    203.0.101.101

Done
> VTYSH
NS# configure terminal
NS(config)# ns IPv6-routing
NS(config)# interface VXLAN-9000
NS(config-if)# ipv6 router OSPF area 3
```

Erweitern von VLANs von mehreren Unternehmen auf eine Cloud mithilfe von VXLAN-VLAN-Karten

CloudBridge Connector-Tunnel werden verwendet, um das VLAN eines Unternehmens auf eine Cloud zu erweitern. VLANs, die von mehreren Unternehmen ausgeweitet werden, können sich überlappende VLAN-IDs haben. Sie können die VLANs jedes Unternehmens isolieren, indem Sie sie einem eindeutigen VXLAN in der Cloud zuordnen. Auf einer Citrix ADC Appliance, dem CloudBridge-Connector-Endpunkt in der Cloud, können Sie eine VXLAN-VLAN-Karte konfigurieren, die die VLANs eines Unternehmens mit einem eindeutigen VXLAN in der Cloud verknüpft. VXLANs unterstützen VLAN-Tagging, um mehrere VLANs eines Unternehmens von CloudBridge Connector auf dasselbe VXLAN zu erweitern.

Führen Sie die folgenden Aufgaben aus, um VLANs mehrerer Unternehmen auf eine Cloud zu erweitern:

1. Erstellen Sie eine VXLAN-VLAN-Karte.
2. Binden Sie die VXLAN-VLAN-Karte an eine Netzwerkbrückenbasierte oder PBR-basierte CloudBridge Connector-Tunnelkonfiguration auf der Citrix ADC Appliance in der Cloud.
3. (Optional) Aktivieren Sie das VLAN-Tagging in einer VXLAN-Konfiguration.

CLI-Verfahren

So fügen Sie eine VXLAN-VLAN-Karte mit der CLI hinzu:

- **add vxlanVlanMap** <name>
- **show vxlanVlanMap** <name>

So binden Sie ein VXLAN und VLANS mit der CLI an eine VXLAN-VLAN-Karte:

- **bind vxlanVlanMap** <name> [-**vxlan** <positive_integer> -**vlan** <int[-int]> …]
- **show vxlanVlanMap** <name>

So binden Sie eine VXLAN-VLAN-Karte mit der CLI an einen auf Netzwerkbrücke basierenden Cloud-Bridge Connector-Tunnel:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehlssätze ein.

Wenn Sie eine neue Netzwerkbrücke hinzufügen:

- **add netbridge** <name> [-**vxlanVlanMap** <string>]
- **show netbridge** <name>

Wenn eine vorhandene Netzwerkbrücke neu konfiguriert wird:

- **set netbridge** <name> [-**vxlanVlanMap** <string>]
- **show netbridge** <name>

So binden Sie eine VXLAN-VLAN-Karte mit der CLI an einen PBR-basierten CloudBridge Connector-Tunnel:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehlssätze ein.

Wenn Sie eine neue PBR hinzufügen:

- **add pbr** <name> **ALLOW** (-**ipTunnel** <ipTunnelName> [-**vxlanVlanMap** <name>])
- **show pbr** <name>

Bei Neukonfiguration eines vorhandenen PBR:

- **set pbr** <name> **ALLOW** (-**ipTunnel** <ipTunnelName> [-**vxlanVlanMap** <name>])
- **show pbr** <name>

So schließen Sie VLAN-Tags in Paketen ein, die mit einem VXLAN verbunden sind, mit der CLI ein:

Geben Sie an der Eingabeaufforderung einen der folgenden Befehlssätze ein.

Wenn Sie ein neues VXLAN hinzufügen:

- **add vxlan** <vnid> -**vlanTag** (**ENABLED** | **DISABLED**)
- **show vxlan** <vnid>

bei Neukonfiguration eines vorhandenen VXLAN:

- **set vxlan** <vnid> -**vlanTag** (**ENABLED** | **DISABLED**)

- **show vxlan** <vnid>

GUI-Verfahren

So fügen Sie eine VXLAN-VLAN-Karte mit der GUI hinzu:

Navigieren Sie zu **System** > **Netzwerk** > **VXLAN-VLAN-Karte**, fügen Sie eine VXLAN-VLAN-Karte hinzu.

So binden Sie eine VXLAN-VLAN-Karte mit der GUI an einen Netbridge-basierten CloudBridge Connector-Tunnel:

Navigieren Sie zu **System** > **CloudBridge Connector** > **Network Bridge**, wählen Sie eine VXLAN-VLAN-Karte aus der Dropdownliste **VXLAN-VLAN** aus, während Sie eine neue Netzwerkbrücke hinzufügen oder eine vorhandene Netzwerkbrücke neu konfigurieren.

So binden Sie eine VXLAN-VLAN-Karte mit der GUI an einen PBR-basierten CloudBridge Connector-Tunnel:

Navigieren Sie zu **System** > **Netzwerk** > **PBRs**, wählen Sie auf der Registerkarte Policy Based Routing (PBRs) eine **VXLAN-VLAN-Karte** aus der Dropdownliste **VXLAN-VLAN** aus, während Sie eine neue PBR hinzufügen oder eine vorhandene PBR neu konfigurieren.

So schließen Sie VLAN-Tags in Paketen ein, die mit einem VXLAN verbunden sind, mit der GUI ein:

Navigieren Sie zu **System** > **Netzwerk** > **VXLANs**, aktivieren Sie die **innere VLAN-Tagging**, während Sie ein neues VXLAN hinzufügen oder ein vorhandenes VXLAN neu konfigurieren.

```
1  > add vxlanVlanMap VXLANVLAN-DC1
2
3  Done
4
5  > bind vxlanvlanmap VXLANVLAN-DC1 -vxlan 3000 -vlan 3
6
7  Done
8
9  > bind vxlanvlanmap VXLANVLAN-DC1 -vxlan 3500 -vlan 4
10
11 Done
12
13 >add vxlanVlanMap VXLANVLAN-DC2
14
15 Done
16
17 > bind vxlanvlanmap VXLANVLAN-DC1 -vxlan 8000 -vlan 3 4
18
```



```
19 Done
20
21 > set pbr PBR-CBC-DC-1-CLOUD ALLOW  -ipTunnel  CBC-DC-1-CLOUD -
      vxlanVlanMap VXLANVLAN-DC1
22
23 Done
24
25 > set pbr PBR-CBC-DC-2-CLOUD ALLOW  -ipTunnel  CBC-DC-2-CLOUD -
      vxlanVlanMap VXLANVLAN-DC2
26
27 Done
```

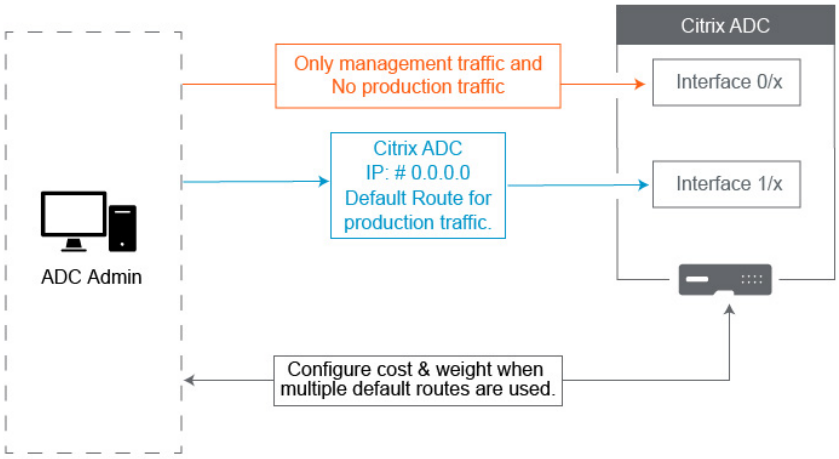
Best Practices für Netzwerkkonfigurationen

October 5, 2021

In den folgenden Abschnitten werden einige Best Practices zum Konfigurieren von Netzwerkfunktionen auf einer Citrix ADC Appliance erläutert.

Routing und Standardrouten

Im Folgenden finden Sie einige Best Practices zum Konfigurieren von Layer 3-Features auf einer Citrix ADC Appliance.



- **Die Schnittstelle `0/x` auf einer Citrix ADC Appliance oder einer Citrix SDX-Appliance darf nicht für den Produktionsdatenverkehr verwendet werden**. Auf einem MPX oder SDX werden die `0/x` benannten Schnittstellen auf die Verwaltungsschnittstellen verwiesen. Dies be-

deutet nicht, dass Sie diese Schnittstellen für die Verwaltung verwenden müssen. Was es bedeutet, ist, dass diese Schnittstellen NICHT für den Produktionsverkehr ausgelegt sind. Sie verfügen nicht über die erforderlichen Hardwarepuffer und -optimierungen, um einen dauerhaften Durchsatz von 1 Gbit/s zu erreichen. Wenn sich Ihre Standardroute im selben Subnetz wie Ihr NSIP befindet, müssen Sie entweder die Standardroute ändern oder eine `1/x`-Schnittstelle für Ihr Management-Netzwerk verwenden, da die `1/x`Schnittstellen vollständig für die Produktion optimiert sind 1 Gbit/s Datenverkehr.

> **Hinweis**:
>
> Dies gilt nicht für eine Citrix ADC VPX Appliance.

  - **Option 1.** Keine Verbindung mit Schnittstellen herstellen`0/x` — Trennen Sie das Kabel von der Schnittstelle`0/1` . NetScaler wartet auf das NSIP auf den anderen Schnittstellen. (HINWEIS: Dies ist keine Option für SDX, da SVM und XenServer nur mit`0/x` Schnittstellen sprechen können)
  - **Option 2.**Ändern Sie die Standardroute auf eine andere Schnittstelle, wie im nächsten Abschnitt beschrieben.

- **Das Standard-Gateway (Route 0.0.0.0) sollte sich in einem Produktionsnetzwerk und nicht auf einer`0/x` Schnittstelle befinden** . Beim ersten Einrichten eines NetScaler werden Sie nach der NSIP-, Subnetzmaske und Gateway-Adresse gefragt. Das Problem, das für Administratoren verursacht wird, besteht darin, dass sie gerade ihre Standardroute so konfiguriert haben, dass sie sich über die Schnittstelle 0/1 in ihrem Verwaltungsnetzwerk befinden.
  - Um zu überprüfen, was Ihre Routen sind, führen Sie in CLI aus`show route` und Ihr Standard-Gateway ist die IP in der Zeile, in der Netzwerk und Netzmaske 0.0.0.0 sind. Hier ist ein Beispiel, bei dem sich das Gateway in Zeile 1 befindet:

```
1  > sh route
2          Network          Netmask          Gateway/OwnedIP
               State   Traffic Domain  Type
3          -------          -------          ---------------
               -----   --------------  ----
4  1)      0.0.0.0          0.0.0.0          10.25.213.65     UP
            0               STATIC
5  2)      127.0.0.0        255.0.0.0        127.0.0.1        UP
            0               PERMANENT
6  3)      10.25.213.64     255.255.255.192  10.25.213.68     UP
            0               DIRECT
7  4)      172.16.0.0       255.255.255.0    172.16.0.1       UP
            0               DIRECT
8
```



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

- Um die Schnittstelle und das VLAN für Ihr Standard-Gateway zu überprüfen, überprüfen Sie die ARP-Tabelle`sh arp` in CLI. Sie können auch nach der spezifischen IP suchen`show arp | grep 10.25.213.65`. Hier ist ein Beispiel, in dem das Gateway 10.25.213.65 Interface 1/1 und VLAN 1 verwendet:

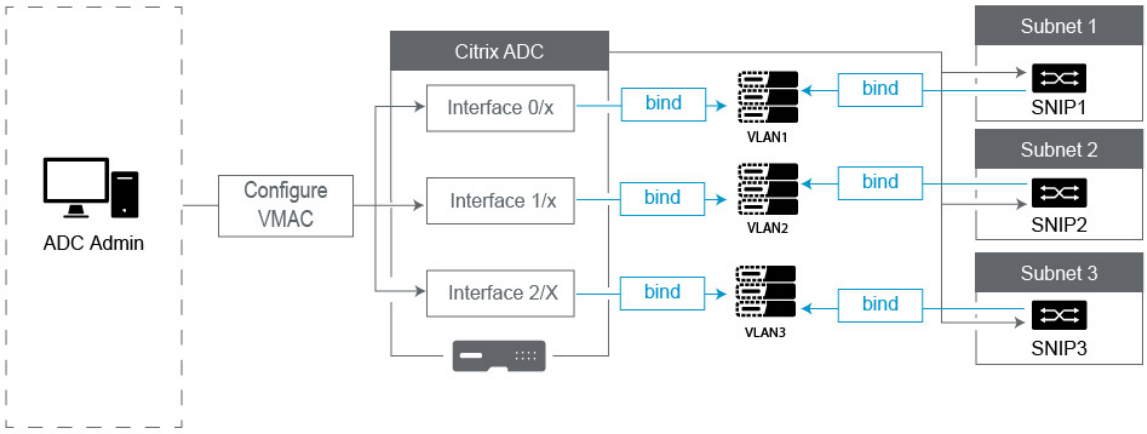
```
1   > sh arp
2           IP               MAC                Iface VLAN
               Origin     TTL     Traffic Domain
3           --               ---                ----- ----
               ------     ---     --------------
4   1)      127.0.0.1        02:00:18:a4:00:1e  LO/1  1
       PERMANENT  N/A    0
5   2)      10.25.213.70     02:00:0f:46:00:28  1/1   1
       DYNAMIC    967    0
6   3)      10.25.213.68     02:00:18:a4:00:1e  LO/1  1
       PERMANENT  N/A    0
7   4)      10.25.213.67     02:00:0f:46:00:28  1/1   1
       DYNAMIC    641    0
8   5)      10.25.213.65     00:08:e3:ff:fd:90  1/1   1
       DYNAMIC    483    0
9   <!--NeedCopy-->
```

- Ändern Sie die Standardroute, um ein Gateway im Produktionssubnetz und -schnittstelle zu verwenden. Angenommen, Ihr Verwaltungsnetzwerk ist 10.0.0.0/24 mit Gateway 10.0.0.1 und das Produktionsnetzwerk ist 10.1.1.0/24 mit Gateway 10.1.1.1. Richten Sie Ihre Konfiguration wie folgt ein:
  - SNIP: (Verwaltungszugriff deaktiviert) 10.1.1.2
  - NSIP: (Verwaltungszugriff aktiviert) 10.0.0.2
  - Standard-Route: 0.0.0.0 0.0.0.0 10.1.1.1 (System > Netzwerk > Routen). Dies verwendet einen Router im SNIP-Netzwerk anstelle des NSIP-Netzwerks.

    > **Hinweis**:
    >
    > Das Ändern des Standard-Gateway kann den Verwaltungsdatenverkehr unterbrechen, es sei denn, Sie konfigurieren statische Routen, eine richtlinienbasierte Route oder aktivieren die MAC-basierte Weiterleitung.

Schnittstellen, Kanäle und VLANs

Im Folgenden finden Sie einige Best Practices zum Konfigurieren von Layer 2-Features auf einer Citrix ADC Appliance.



- **Verbinden Sie nicht mehrere Schnittstellen/Kanäle mit demselben VLAN, einschließlich VLAN 1**:
  - Wenn Sie Ihre VLANs nicht richtig konfigurieren, kann dies zu unerwartetem Paketrouting in Ihrem Netzwerk und Layer 2-Looping führen, wenn mehr als eine aktive Schnittstelle mit demselben VLAN (entweder Native oder Tagged) vorhanden ist.
  - Standardmäßig befinden sich alle Schnittstellen und Kanäle auf nativem VLAN 1. Dies verursacht zwei mögliche Probleme:
    * Der NetScaler denkt, dass sich der gesamte empfangene Datenverkehr im selben Netzwerk befindet. Daher verwendet er eine beliebige Schnittstelle zum Senden des Datenverkehrs. Wenn Sie ein anderes natives VLAN auf der Schnittstelle haben, an der es Daten gesendet hat, wird der Datenverkehr nicht wie erwartet weitergeleitet.
    * Wenn der NetScaler Broadcast-Pakete an einem Port empfängt, kann er an einem anderen Port erneut übertragen. Wenn sich beide Switchports auf demselben VLAN befinden, haben Sie gerade eine Layer-2-Schleife erstellt.
  - So entfernen Sie eine Schnittstelle/einen Kanal aus VLAN 1:
    * Wenn Sie keine nativen VLANs auf Ihrer Switch-Schnittstelle/Portkanal verwenden. Ändern Sie das native VLAN auf der NetScaler Interface/Channel in eine nicht verwendete VLAN-Nummer wie 999. Sie sollten nicht dieselbe nicht verwendete VLAN-Nummer für mehrere Kanäle oder Schnittstellen verwenden, da sie eine Layer-2-Schleife erstellt.

        * Wenn Sie native VLANs auf Ihrer Switch-Schnittstelle/Portkanal verwenden. Ändern Sie das native VLAN auf der NetScaler Interface/Channel so, dass es übereinstimmt. Achten Sie jedoch darauf, dass nicht mehrere aktive Schnittstellen oder Kanäle auf demselben VLAN vorhanden sind, da dadurch Layer 2-Schleifen erstellt werden.
        * Sie können das native VLAN nicht entfernen. Stattdessen können Sie es ändern oder TagAll für die Schnittstelle oder den Kanal festlegen. Wenn der Switch-Port nicht mit einem nativen VLAN ohne Tags konfiguriert ist, aktivieren Sie tagall auf der Schnittstelle, damit Heartbeat-Pakete mit hoher Verfügbarkeit markiert werden.
    - Um das native VLAN auf einer Schnittstelle anzuzeigen, führen Sie`sh interface` in CLI aus. Dies informiert Sie auch, wenn die Schnittstelle die Option TAGALL verwendet.

- **Binden Sie eine Schnittstelle an Ihr VLAN** - Der NetScaler fügt standardmäßig kein neues VLAN an eine Schnittstelle an. Dies bedeutet, dass das VLAN erst verwendet wird, wenn Sie es an eine Schnittstelle binden. Wenn das neue VLAN nicht an eine Schnittstelle gebunden ist und dass VLAN Tagged ist, löscht der NetScaler den gesamten eingehenden Datenverkehr aus diesem VLAN. Binden Sie dasselbe VLAN auch nicht an mehrere Schnittstellen.
    - Binden Sie Subnetze an Ihre VLANs. Der NetScaler funktioniert nicht wie ein typischer Router. Die meisten Router verbinden IPs an Schnittstellen. Auf einem NetScaler schweben die IPs auf einer beliebigen Schnittstelle, sofern nicht anders konfiguriert. Daher müssen Sie jedes Subnetz, das Sie sicherstellen möchten, dass der NetScaler über ein bestimmtes VLAN sendet, insbesondere wenn der NetScaler diesen Datenverkehr initiiert, ein SNIP innerhalb dieses Subnetzes an das VLAN binden.
    - Ein häufiges Argument, das wir dagegen hören, ist, dass es früher gut funktioniert und jetzt nicht ohne Bindung des Subnetzes an das VLAN. Dies tritt häufig auf, weil NetScaler erfährt, welches VLAN Datenverkehr aussendet, aber dies kann Zeit in Anspruch nehmen, wenn es seine ARP-Tabellen erstellt. Wenn nach einem Neustart oder einem Firmware-Upgrade die ARP-Tabellen erneut erstellt werden, kann es zunächst lernen und daher einen anderen Pfad verwenden, als Sie möchten, z. B. Ihre Standardroute. Es empfiehlt sich, den Pfad anzuweisen, indem Sie das SNIP an das VLAN binden. Sobald ein SNIP an ein VLAN gebunden ist, wird das gesamte Subnetz für dieses SNIP an das VLAN gebunden.
    - Stellen Sie sicher, dass jedes SNIP an ein VLAN gebunden ist (außer in Fällen, in denen Sie mehr als 1 SNIP in einem Subnetz haben, dann müssen Sie nur eins binden) und dass das VLAN wiederum nur an eine Schnittstelle oder einen Kanal gebunden ist. Es ist auch oft am besten, ein SNIP in jedem Subnetz zu haben, aber das ist nicht erforderlich, da die spezifischste Route für jedes Zielsubnetz verwendet wird, das kein SNIP besitzt.
- So identifizieren Sie das von einem Subnetz verwendete VLAN und die Schnittstelle:
    1. Gehen Sie zu **System>Netzwerk > VLANs**.

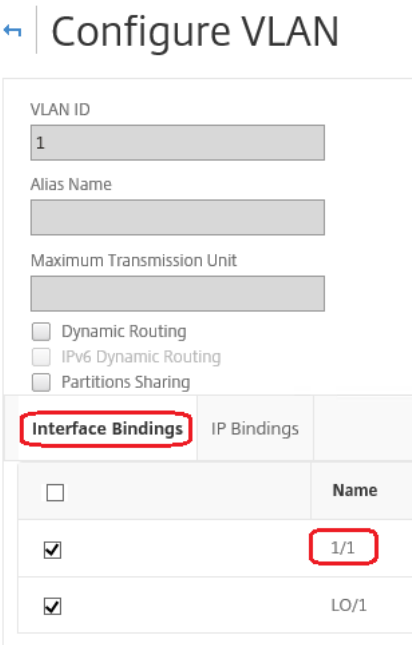
2. Bearbeiten Sie jedes konfigurierte VLAN wiederum, bis Sie die richtige IP-Adresse finden, wie im nächsten Schritt erläutert.
3. Klicken Sie auf die Registerkarte IP-Bindungen, um zu sehen, welche IP und damit welches Subnetz gebunden ist und somit dieses VLAN verwendet.
4. Sobald Sie das VLAN identifiziert haben, das eine IP gebunden ist, wobei sich diese IP innerhalb des Subnetzes der Standardroute befindet, klicken Sie auf die Schnittstellenbindungen. Jede Schnittstelle oder Kanal, die an dieses VLAN gebunden ist, wird verwendet.

Beispiel

Angenommen, die Standardroute ist`0.0.0.0 0.0.0.0 10.1.1.1`.

Angenommen, Sie haben zwei SNIPs von 10.0.0.5 und 10.1.1.69. Da sich 10.1.1.69 im Subnetz der Standardroute befindet, ist dies diejenige, die Sie suchen möchten. In den folgenden Screenshots überprüfen wir VLAN 1 und wir sehen, dass die IP 10.1.1.69 an dieses VLAN gebunden ist, so dass wir wissen, dass wir uns das richtige VLAN anschauen.

Klicken Sie nun auf Schnittstellenbindungen. In den VLAN-Schnittstellen-Bindungen sehen wir, dass Interface für dieses Subnetz verwendet`1/1` wird und daher für die Standardroute verwendet wird.



> **HINWEIS**:
>
> Wenn Sie keine IPs an Ihre VLANs gebunden haben, wird es standardmäßig aus VLAN 1 gesendet, also schauen Sie in diesem Fall, welche Schnittstellen an VLAN 1 gebunden sind. Dies bedeutet auch, dass NetScaler Ihre konfigurierten VLANs nicht für den initiierten Datenverkehr verwendet, es sei denn, Sie binden eine IP an das neue VLAN.

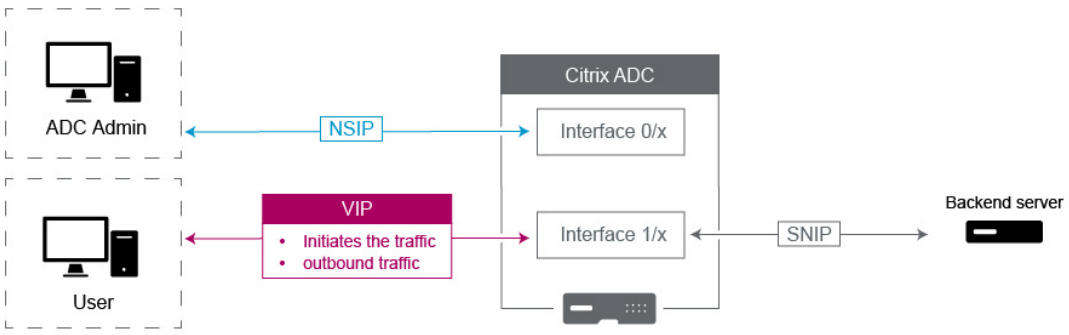
Unentgeltliche ARP

Wenn GARP nicht funktioniert, verwenden Sie VMAC - Standardmäßig verwendet NetScaler GARP, um seine IP-zu-MAC-Adressbindungen an andere Netzwerkgeräte anzukündigen. Dies funktioniert in der Regel ohne Probleme. Wenn Sie jedoch weitere Dienste im NetScaler erstellen, können Probleme auftreten, wenn ein Failover auf einem HA-Paar durchgeführt wird. Das häufigste Problem besteht darin, dass Dienste in dem NetScaler, auf den Sie ein Failover durchgeführt haben, ausfallen, da einige Netzwerkgeräte ihre ARP-Tabellen nicht mit der neuen MAC-Adresse aktualisiert haben. Sie können dies leicht überprüfen, indem Sie ihre ARP-Tabellen überprüfen, um zu sehen, ob die MAC-Adressen mit denen auf dem jetzt primären NetScaler übereinstimmen. In diesem Fall ist es sehr wahrscheinlich, dass einige Ihrer Netzwerkgeräte die Anzahl der GARP-Anzeigen einschränken, die sie berücksichtigen. In diesem Fall ist es notwendig, VMAC auf allen Ihren aktiven Schnittstellen und/oder Kanälen zu konfigurieren. Wenn Sie eine große Konfiguration auf Ihrem NetScaler erwarten, empfiehlt es sich, VMAC für alle Schnittstellen und Kanäle während der anfänglichen Bereitstellung zu konfigurieren.

> **HINWEIS**:
>
> Vergessen Sie nicht, VMAC für die Schnittstelle oder den Kanal zu konfigurieren, die von Ihrer Standardroute verwendet wird.

Citrix ADC eigene IP-Adressen

In diesem Abschnitt werden die bewährten Methoden zum Konfigurieren von IP-Adressen im Citrix ADC Besitz beschrieben:



- **Citrix ADC IP (NSIP)**: Im Allgemeinen wird diese IP für die Verwaltung verwendet, da sie die einzige IP ist, die für einen einzelnen NetScaler in einer HA- oder Clusterumgebung eindeutig ist. Wichtig ist auch, dass LDAP-, RADIUS- und Benutzerskriptdatenverkehr (wie der LDAP-Monitor

und StoreFront Monitor) aus dem NSIP quellt und somit über das VLAN und die Schnittstelle weitergeleitet werden, an die NSIP gebunden ist (Standard Native VLAN 1). Wenn der LDAP- und RADIUS-Datenverkehr aus dem SNIP stammen soll, erstellen Sie einen virtuellen LB-Server für Ihre Back-End-Server.

- **Subnetz-IP (SNIP)**: Diese IP-Adresse wird verwendet, um die Kommunikation mit Back-End-Servern zu initiieren und wird immer den Datenverkehr initiieren. Das heißt, es kann das Ziel für den Verkehr in diesen Fällen sein:
  - Es kann als Gateway-Adresse auf anderen Geräten verwendet werden, wenn Layer 3-Routing auf dem NetScaler durchgeführt wird.
  - Wenn diese Option aktiviert ist, kann sie Verwaltungsdienste akzeptieren, z. B. den Zugriff auf die GUI, SSH und SNMP.
- **Virtuelle IP (VIP)**: Der VIP ist einzigartig, da er niemals verwendet wird, um ausgehenden Datenverkehr zu initiieren. Es ist nur für den Empfang von Traffic vorgesehen. Sobald es Datenverkehr empfängt, antwortet es und sendet Datenverkehr ausgehend zurück an den Client. Mit anderen Worten, die VIP-Adresse initiiert den ausgehenden Datenverkehr nicht.

Beachten Sie, dass dies auch nicht als Quelle für die Kommunikation mit Back-End-Servern verwendet wird, die beispielsweise in einem virtuellen LB-Server verwendet werden.

Konfigurieration zum Beziehen von Citrix ADC FreeBSD-Datenverkehr von einer SNIP-Adresse

October 5, 2021

Einige Citrix ADC-Datenfunktionen werden auf dem zugrunde liegenden FreeBSD-Betriebssystem statt auf dem Citrix ADC OS ausgeführt. Aus diesem Grund senden diese Funktionen Datenverkehr, der von der Citrix ADC IP (NSIP) -Adresse bezogen wird, anstatt von einer SNIP-Adresse bezogen zu werden. Die Beschaffung des Datenverkehrs von der NSIP-Adresse ist nicht wünschenswert, wenn Ihr Setup Konfigurationen zur Trennung des gesamten Verwaltungs- und Datenverkehrs aufweist.

Die folgenden Citrix ADC-Datenfunktionen werden auf dem zugrunde liegenden FreeBSD-Betriebssystem ausgeführt und senden Datenverkehr aus der Citrix ADC IP (NSIP) -Adresse:

- Load Balancing skriptfähige Monitore
- GSLB Autosync

Um dieses Problem zu beheben, können Sie den globalen Layer-2-Parameter verwenden: `useNetprofileBSDtraffic`. Wenn Sie diesen Parameter aktivieren, senden die Citrix ADC Funktionen Datenverkehr, der von einer der SNIP-Adressen in einem mit der Funktion verknüpften Netzprofil stammt.

Voraussetzungen

Bevor Sie die Citrix ADC Appliance für die Beschaffung von Citrix ADC Funktionen bezogenen Datenverkehr von einer SNIP-Adresse konfigurieren, beachten Sie die folgenden Punkte:

- Derzeit `useNetprofileBSDtraffic` wird der globale Layer-2-Parameter nur für Scriptbilanz-Monitore mit Lastenausgleich unterstützt.

  Um die Citrix ADC Appliance so zu konfigurieren, dass sie GSLB-Autosync-Datenverkehr von einer SNIP-Adresse beziehen, können Sie erweiterte ACL-Regeln und RNAT-Regeln als Workaround verwenden.

- Die `useNetprofileBSDtraffic` Unterstützung für Scriptable Monitore für den Lastenausgleich gilt nur für Nettoprofile, die an die zugehörigen Dienste gebunden sind. Die `useNetprofileBSDtraffic` Unterstützung gilt nicht für Nettoprofile, die an die zugehörigen Dienstleistungsgruppen gebunden sind.

  Mit anderen Worten, die Citrix ADC Appliance verwendet keine SNIP-Adresse aus den Netzprofilen, die an die Dienstgruppen gebunden sind, um den Lastenausgleich skriptfähig zu beziehen, überwacht den Datenverkehr.

- Der `useNetprofileBSDtraffic` Support gilt nicht für SSL-Dienste.

  Mit anderen Worten, die Citrix ADC Appliance verwendet keine SNIP-Adresse aus den Netzprofilen, die an die SSL-Dienste gebunden sind, um den Datenverkehr für den Lastenausgleich für skriptfähige Monitore zu beschaffen.

Konfigurieren der Citrix ADC Appliance, um skriptfähig zu beziehen, überwacht den Datenverkehr von einer SNIP-Adresse

Das Konfigurieren der Citrix ADC Appliance für die skriptbasierte Quelle überwacht den Datenverkehr von einer SNIP-Adresse aus den folgenden Aufgaben:

- Aktivieren Sie den globalen Layer-2-Parameter `useNetprofileBSDtraffic`.
- Erstellen Sie ein Netzprofil und binden Sie mindestens eine SNIP-Adresse daran.
- Binden Sie das Nettoprofil an die Lastausgleichsdienste, die skriptfähige Monitore verwenden.

So aktivieren Sie den Layer-2-Parameter UsenetProfileBSDTraffic mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **set l2param** -**UsenetProfileBSDTraffic** (**AKTIVIERT** / **DEAKTIVIERT**)
- **show l2param**

So erstellen Sie ein Netzprofil und binden SNIP-Adressen mit der CLI an dieses:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **netProfile hinzufügen** <name> -**srcIP** <string>

- **NetProfile anzeigen**

So binden Sie ein Nettoprofil mit der CLI an einen Lastausgleichsdienst:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **Dienst festlegen** <name> -**NetProfile** <string>
- **show service** <name>

Beispielkonfiguration

Die folgende Beispielkonfiguration ermöglicht es einer Citrix ADC Appliance, skriptfähig den Datenverkehr von einer SNIP-Adresse zu beziehen. Ein Netzprofil NETPROFILE-1 ist mit der an ihn gebundenen SNIP-Adresse 198.51.100.20 konfiguriert. Ein Benutzer/skriptfähige Monitor USER-MONITOR-1 wird erstellt und ist an einen Lastausgleichsdienst SERVICE-1 gebunden. NETPROFILE-1 ist an SERVICE-1 gebunden. Die Citrix ADC Appliance bezieht alle skriptfähigen Überwachungspakete von USER-MONITOR-1 aus der SNIP-Adresse 198.51.100.20.

```
set l2param -useNetprofileBSDtraffic ENABLED

set netprofile NETPROFILE-1 -srcip 198.51.100.20

add lb monitor USER-MONITOR-1 USER -scriptName nsftp.pl -scriptArgs ”
   file=Index.png;user=nsroot;password=nsroot” -dispatcherIP 127.0.0.1
   -dispatcherPort 3013 -destIP 203.0.113.90 -destPort 21

bind service SERVICE-1 -monitorName USER-MONITOR-1

set service SERVICE-1 -netProfile NETPROFILE-1

<!--NeedCopy-->
```

Konfigurieren der Citrix ADC Appliance für die Beschaffung von GSLB-Autosync-Datenverkehr von einer SNIP-Adresse

Die Konfiguration der Citrix ADC Appliance für die Quelle des GSLB-Autosync-Datenverkehrs von einer SNIP-Adresse umfasst die folgenden Problemumgehungsaufgaben:

- **Erstellen Sie eine erweiterte ACL-Regel**. Eine erweiterte ACL-Regel identifiziert die GSLB-Autosync-Pakete. Diese Identifikation basiert auf der Quell-IP- und Ziel-IP-Adressen.
- **Wenden Sie ACLs**an Durch das Anwenden von ACLs wird die neu erstellte ACL-Regel aktiviert.
- **Erstellen Sie eine ACL-basierte RNAT-Regel**. Eine RNAT-Regel ändert die Quell-IP-Adresse dieser Pakete von der NSIP-Adresse in eine SNIP-Adresse.

> **Hinweis:**
>
> In einem Hochverfügbarkeits- oder Cluster-Setup müssen Sie ACL- und RNAT-Regeln für alle NSIP-Adressen des Setups hinzufügen.

So erstellen Sie eine erweiterte ACL über die CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add acl** <aclname> **ALLOW** -**srcIP** = <NSIP address> -**destIP** = <destination IP address of the packets>
- **show acl** <aclName>

So wenden Sie erweiterte ACLs mit der CLI an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **apply acls**

So erstellen Sie eine ACL-basierte RNAT-Regel über die CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **add rnat** <name> <aclname>
- **bind rnat** <name> -**natIP** <SNIP address - source IP address for the packets>
- **show rnat** <name>

Beispielkonfiguration

Die folgende Beispielkonfiguration ermöglicht es einer Citrix ADC Appliance, GSLB-Autosync-Verkehr von einer SNIP-Adresse zu beziehen. ACL-2 identifiziert GSLB-Autosync-Pakete, die von der NSIP-Adresse 192.0.1.20 stammen und für die GSLB-Standort-IP-Adresse 203.0.113.20 bestimmt sind. RNAT-2 ändert die Quell-IP-Adresse für diese identifizierten Pakete in die SNIP-Adresse 198.51.100.20.

```
add acl ACL-2 ALLOW -srcIP = 192.0.1.20  -destIP = 203.0.113.20

apply acls

add rnat RNAT-2 ACL-2

bind rnat RNAT-2 -natIP 198.51.100.20
<!--NeedCopy-->
```


Prioritäts-Lastenausgleich

October 5, 2021

Mit der Funktion für den Lastenausgleich können Sie jedem der Dienste oder Dienstgruppen, die an einen virtuellen Server mit Prioritätsausgleich gebunden sind, eine Prioritätsnummer zuweisen. Ein Dienst oder eine Servicegruppe mit der niedrigsten Nummer hat die höchste Priorität. Der Anwendungsdatenverkehr wird nur an diesen Dienst oder eine Dienstgruppe verteilt, solange dieser Dienst oder die Dienstgruppe UP ist. Der Dienst oder die Dienstgruppe, der die nächste Prioritätsnummer zugewiesen wird, werden nur dann betriebsbereit, wenn alle Dienste oder Mitglieder in der Dienstgruppe mit der höchsten Priorität DOWN sind. Wenn jedoch einer der Dienste oder ein Mitglied der Servicegruppe mit der höchsten Priorität wieder verfügbar ist, wird der Datenverkehr an diesen Dienst oder die Servicegruppe weitergeleitet.

Betrachten Sie beispielsweise die Dienstgruppen SVG1, SVG2 und SVG3, die an einen virtuellen Server für den Lastausgleich mit Priorität gebunden sind. Die maximale Anzahl von Prioritätsgruppen ist auf drei festgelegt. Für jede Gruppe weisen Sie die Priorität folgendermaßen zu:

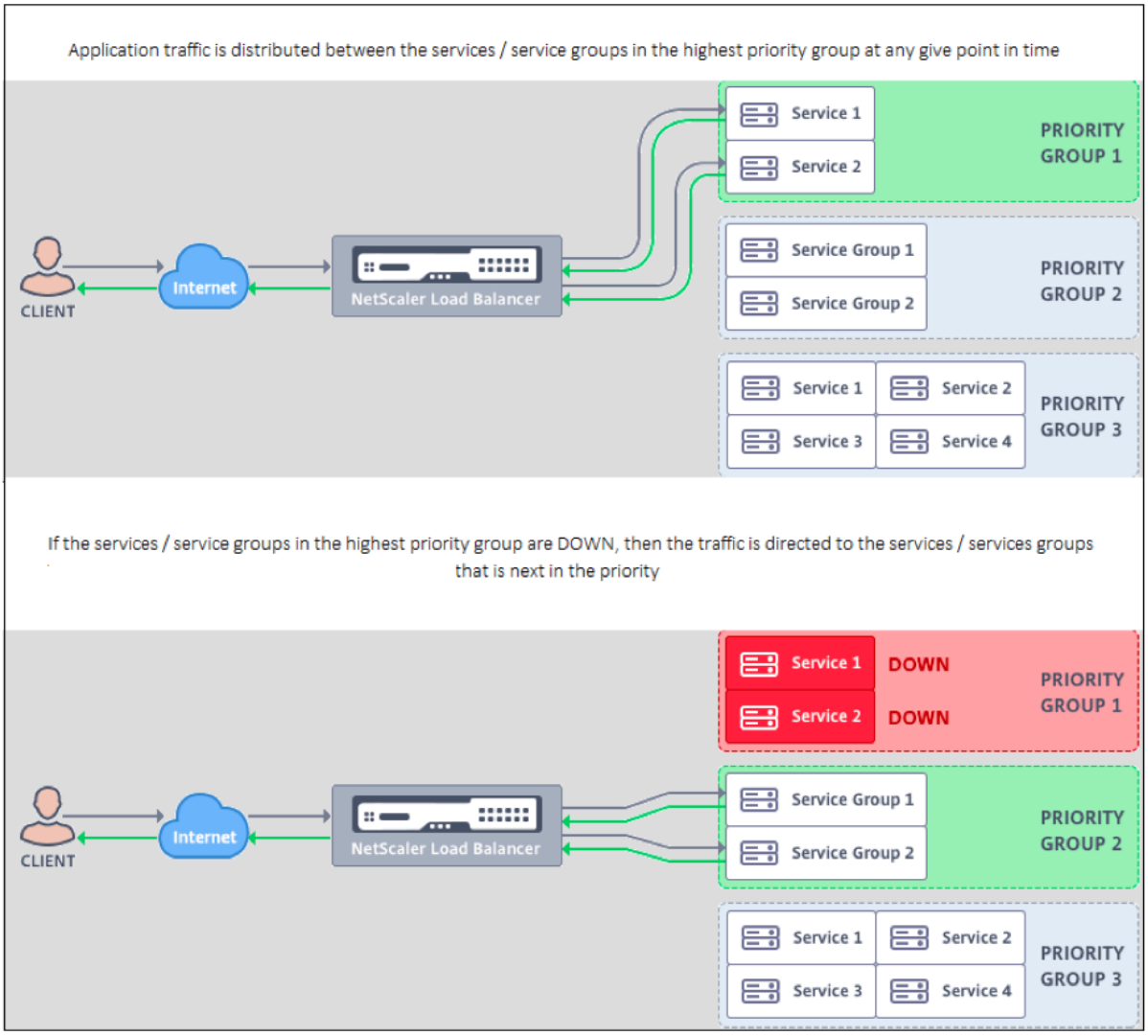
- SVG1 — Priorität 1
- SVG2 — Priorität 2
- SVG3 — Priorität 3

In diesem Szenario wird der Anwendungsdatenverkehr auf Dienstgruppe SVG1 geleitet, da dieser Gruppe die niedrigste Prioritätsnummer zugewiesen wird. Wenn alle Mitglieder in SVG1 DOWN sind, wird der Datenverkehr an die Dienstgruppe SVG2 verteilt, da dieser Gruppe die nächst niedrigere Prioritätsnummer zugewiesen wird. Wenn alle Mitglieder in SVG2 auch DOWN sind, wird der Datenverkehr an SVG3 verteilt. Wenn jedoch eines der Mitglieder in SVG1 UP ist, wird der Datenverkehr an SVG1 umgeleitet, da SVG1 die niedrigste Zahl zugewiesen wird und die höchste Priorität hat.

Sie können einer Dienstleistung oder einer Servicegruppe eine Priorität zuweisen, um die spezifische Dienst- oder Servicegruppe, die die höchste Priorität hat, bei Bedarf mit minimalen oder keinen Auswirkungen auf den Produktionsverkehr zu aktualisieren.

Wenn das Upgrade nicht erfolgreich ist, können Sie sicher zu dem Dienst oder der Servicegruppe wechseln, die als nächstes in der Priorität steht, mit minimalen oder keinen Einfluss auf den Produktionsdatenverkehr.

Die folgende Abbildung veranschaulicht die Funktion für den Lastausgleich mit Priorität.



Konfigurieren des Lastausgleichs mit Priorität

> **Hinweis:**
>
> Die Konfiguration des Lastenausgleichs mit Citrix ADC Priorität wird nur über die GUI unterstützt. Sie können den Prioritätslastenausgleich nicht über die CLI konfigurieren.

1. Navigieren Sie zu **Traffic Management** > **Priority Load Balancing**> **Virtuelle *Server** und geben Sie das Protokoll für den virtuellen Server, die IP-Adresse und die Portnummer des virtuellen Servers an.
2. Geben Sie im Feld **Maximale Prioritätsgruppen** die Anzahl der Prioritätsdienste oder die Dienstgruppen ein, die an diesen virtuellen Server gebunden werden können. Der Standardwert ist 2, und die maximale Priorität, die festgelegt werden kann, ist 10. Dieser Parameter kann nach der Konfiguration nicht bearbeitet werden.

Hinweis:

Nachdem Sie die maximale Anzahl von Prioritätsgruppen angegeben und auf **OK** geklickt haben, werden ein virtueller Content Switching-Server und die Anzahl der virtuellen Backup-Load Balancing erstellt. Das Alphabet “n” stellt die maximale Anzahl von Prioritätsgruppen dar.

Wenn Sie beispielsweise den Namen des virtuellen Servers als vs1 eingegeben und die maximale Prioritätsgruppe auf 5 festgelegt haben, wird ein virtueller Content Switching-Server mit dem Namen `_Pri.LB##vs1##MaxPri=5` und den folgenden 5 virtuellen Lastausgleichsservern erstellt.

- `_Pri.LB##vs1##MaxPri=5_LB1`
- `_Pri.LB##vs1##MaxPri=5_LB2`
- `_Pri.LB##vs1##MaxPri=5_LB3`
- `_Pri.LB##vs1##MaxPri=5_LB4`
- `_Pri.LB##vs1##MaxPri=5_LB5`

3. Nachdem Sie die maximale Anzahl von Prioritätsgruppen angegeben und auf **OK** geklickt haben, werden Sie aufgefordert, die Dienste oder Dienstgruppen auszuwählen, die an diesen virtuellen Content Switching-Server gebunden sein müssen.

   - Um Dienste an den virtuellen Server zu binden, klicken Sie im Abschnitt Dienste auf **Einfügen**. Wählen Sie als Nächstes entweder einen vorhandenen Dienst aus, oder erstellen Sie einen Dienst, und legen Sie die Priorität für diesen Dienst fest. Legen Sie außerdem die Prioritätsnummer fest, an die dieser Dienst gebunden sein muss.
   - Um Dienstgruppen an den virtuellen Server zu binden, klicken Sie im Abschnitt Dienstgruppen auf **Einfügen**. Wählen Sie als Nächstes entweder eine vorhandene Servicegruppe aus, oder erstellen Sie eine Servicegruppe, und legen Sie die Priorität für diese Dienstgruppe fest. Legen Sie außerdem die Prioritätsnummer fest, an die diese Dienstgruppe gebunden sein muss.

   Wiederholen Sie Schritt 3, abhängig von der maximalen Anzahl von Prioritätsgruppen, die Sie eingegeben haben.

   Hinweis:

   - Der Dienst oder die Dienstgruppe mit der höchsten Priorität ist an den virtuellen Lastausgleichsserver gebunden, der die höchste Priorität darstellt.

   Wenn Sie beispielsweise Servicegruppen die Priorität 1 und 2 zugewiesen `SG_App1 and SG_App2` haben, `SG_App1` ist an gebunden `virtual server _Pri.LB##vs1##MaxPri=5 _LB1 and SG_App2` ist verpflichtet `virtual server _Pri.LB##vs1##MaxPri=5_LB2` erstellt in Schritt 2.

   - Um die Priorität der Dienstgruppe oder des Dienstes zu ändern, klicken Sie auf der Seite

Virtueller Server für den Lastenausgleich auf das Symbol Bearbeiten, und ändern Sie die Priorität nach Bedarf.

- Sie können die Lastenausgleichsmethoden und die Persistenz für jeden virtuellen Server nicht explizit festlegen, da die Konfiguration aller virtuellen Server für den Lastenausgleich identisch ist.

4. Führen Sie in den Abschnitten Erweiterte Einstellungen die andere Konfiguration aus, die Ihren Anforderungen entspricht.

> **Wichtig:**
>
> Die Entitäten, die während der Priority-Load Balancing-Konfiguration erstellt wurden, dürfen nicht von anderen Registerkarten in der GUI und auch von der CLI geändert werden. Es wird empfohlen, die Prioritäts-Load Balancing-Entitäten nur über die Registerkarte Priority Load Balancing zu ändern.

Citrix ADC Erweiterungen

October 5, 2021

Citrix ADC Erweiterungen können verwendet werden, um eine Citrix ADC Appliance durch Schreiben von Erweiterungscode anzupassen. Derzeit werden Richtlinienerweiterungen und Protokollerweiterungen unterstützt. Richtlinienerweiterungen können verwendet werden, um die Richtliniensprache zu erweitern. Protokollerweiterungen können verwendet werden, um Unterstützung für benutzerdefinierte Protokolle auf einer Citrix ADC Appliance hinzuzufügen.

Citrix ADC-Erweiterungen werden auch von Citrix ADC CPX unterstützt.

Dieses Dokument enthält die folgenden Informationen:

- Citrix ADC Erweiterungen - Sprachübersicht
- Citrix ADC Erweiterungen - Bibliotheksreferenz
- Citrix ADC Erweiterungen API-Referenz
- Protokollerweiterungen
- Richtlinienerweiterungen

Citrix ADC Erweiterungen - Sprachübersicht

October 5, 2021

Die Erweiterungssprache basiert auf der Programmiersprache Lua 5.2. Lua bietet eine kompakte Ausführungs-Engine mit guter Leistung, die für die Einbettung in C-Programme wie Citrix ADC C-Software entwickelt wurde.

Die Erweiterungssprache wird dynamisch eingegeben, was bedeutet, dass jedes Objekt seine eigenen Typinformationen enthält. Jede Variable kann jederzeit während der Ausführung einen beliebigen Typ enthalten, so dass Variablentypen nicht deklariert werden.

Die Sprache ist auch freie Form, wobei Leerraum zwischen Token ignoriert wird. Anweisungen können durch Semikolons getrennt werden, aber das ist nicht erforderlich und in der Regel nicht getan. Anweisungsblöcke werden in der Regel durch Ende beendet. Es gibt keine Klammern um Blöcke wie {und} in C oder Java.

Bezeichner sind Sequenzen von Buchstaben (a bis z und A bis Z), Ziffern (0 bis 9) und Unterstriche (_), die nicht in einer Ziffer beginnen. Bei Bezeichnern wird zwischen Groß- und Kleinschreibung unterschieden, daher sind var, VAR und Var alle unterschiedliche Bezeichner.

Kommentare werden von — gestartet. Alles nach — wird bis zum Ende der Zeile ignoriert. Beispiel:

```
-- This is a comment.
```

Einfache Typen

October 5, 2021

Die Sprache erlaubt Werte der folgenden einfachen Typen:

- Ziffern
- Saiten
- Boolesch
- Nil
- Andere Typen

Ziffern

Alle Zahlen (gerade ganze Zahlen) werden durch IEEE 754-Gleitkommawerte dargestellt. Ganzzahlen bis zu 2^54 haben genaue Darstellungen. Numerische Werte können dargestellt werden durch:

- Ganzzahlen mit Vorzeichen und ohne Vorzeichen (Beispiele: 10, -5)
- Reelle Zahlen mit Dezimalstellen (10,5, 3,14159)
- Reelle Zahlen mit Exponenten (1.0e+10)
- Hexadezimale (0xffff0000)

Citrix ADC Richtlinienausdrücke haben drei numerische Typen:

- 32-Bit-Ganzzahlen (num_at)
- 64-Bit-Ganzzahlen (unsigned_long_at)
- 64-Bit-Gleitkommazahl (double_at)

Alle diese werden in den Zahlentyp konvertiert, wenn sie an eine Erweiterungsfunktion übergeben werden, und Zahlen werden in den erwarteten numerischen Richtlinientyp konvertiert, wenn sie zurückgegeben werden.

Saiten

Strings sind Byte-Sequenzen beliebiger Länge. Sie entsprechen dem Typ **text_at**. Strings können null (0x00) Bytes enthalten. Beliebige Binärdaten können in Strings gespeichert werden, einschließlich jeder Zeichencode-Darstellung (z. B. UTF-8 und vollständiger Unicode). String-Funktionen **wiestring.upper()** nehmen jedoch 8-Bit-ASCII an.

Strings werden automatisch zugewiesen, wenn sie verwendet werden. Es besteht keine Notwendigkeit (oder sogar Möglichkeit), Puffer für Strings explizit zuzuweisen. Zeichenfolgen werden auch automatisch von der Garbage Collection freigegeben, wenn sie nicht mehr verwendet werden. Es besteht keine Notwendigkeit (oder sogar Möglichkeit), Strings explizit freizumachen. Diese automatische Zuweisung und Freigabe vermeidet einige häufige Probleme in Sprachen wie C, wie Speicherlecks und baumelnde Zeiger.

Zeichenfolgenliterale sind Zeichenfolgen, die in doppelte oder einfache Anführungszeichen eingeschlossen sind. Es gibt keinen Unterschied zwischen den beiden Arten von Anführungszeichen: “ein Zeichenfolgenliteral” ist dasselbe wie ‘ein Zeichenfolgenliteral’. Das übliche Backslash Escaping ist verfügbar: \s (Glocke), \b (Rücktaste), \f (Seitenvorschub), \n (Zeilenvorschub), \t (horizontaler Tabulator), \\ (umgekehrter Schrägstrich), \” (doppeltes Anführungszeichen) und \’ (einfaches Anführungszeichen). Dezimalbyte-Werte können durch einen umgekehrten Schrägstrich und ein bis drei Ziffern (\d, \dd, \ddd) eingegeben werden. Hexadezimale Byte-Werte können durch einen umgekehrten Schrägstrich, ein \x und zwei Hexadezimalstellen (\xhh) eingegeben werden.

Ein spezieller Syntaxaufruf der Langklammernotation kann für lange, mehrzeilige Zeichenfolgenliterale verwendet werden. Diese Notation umschließt die Zeichenfolge in doppelten eckigen Klammern mit null oder mehr Gleichheitszeichen zwischen den Klammern — die Idee ist, eine Kombination von Klammern und Gleichen zu finden, die nicht in der Zeichenfolge ist. Es werden keine Escape-Sequenzen in der Zeichenfolge berücksichtigt. Beispiele:

[[Dies ist eine mehrzeilige Zeichenfolge mit langer Klammer Notation.]]

[= [Dies ist eine mehrzeilige Zeichenfolge, die eine lange Notation mit [[und] und einer nicht esaped darin verwendet].] =]

Langklammer Notation kann verwendet werden, um einen mehrzeiligen Kommentar zu machen. Beispiel:

—[[
Dies ist ein mehrzeiliger Kommentar.
–]]

Boolesch

Die üblichen booleschen Werte true und false werden bereitgestellt. Beachten Sie, dass boolesche Werte sich von Zahlenwerten unterscheiden, im Gegensatz zu C, wobei Null als falsch angenommen wird und jeder Wert ungleich Null true ist.

Nil

nil ist ein spezieller Wert, der “kein Wert” bedeutet. Es ist sein eigener Typ und entspricht keinem anderen Wert, im Gegensatz zu C, wo NULL als Null definiert ist.

Andere Typen

Es gibt zwei andere Typen, Benutzerdaten und Threads. Dies sind fortgeschrittene Themen und werden hier nicht behandelt.

Variablen

October 5, 2021

Variablen enthalten Werte, die sich während der Ausführung der Erweiterung ändern können. Aufgrund der dynamischen Eingabe kann jede Variable Werte jedes Typs enthalten. Es gibt keine Typdeklarationen für Variablen. Stattdessen wird der Typ einer Variablen zur Laufzeit bestimmt. Tatsächlich kann sich der Typ des Werts einer Variablen während der Ausführung ändern, obwohl dies keine empfohlene Vorgehensweise ist. Eine Variable hat anfänglich den Wert nil.

Variablennamen sind Bezeichner, also Zeichenfolgen aus Buchstaben, Ziffern und Unterstrichen, die nicht in einer Ziffer beginnen. Beispiele: Header, combined_headers.

Globale Variablen

In Lua sind Variablen, die nicht anderweitig deklariert werden, global innerhalb des Programms. Globale Variablen sind jedoch in Richtlinienerweiterungsfunktionen nicht zulässig, da es mehrere Paketmodule gibt, in denen eine Funktion ausgeführt werden kann und jede Packet Engine über einen eigenen Speicher verfügt.

Wenn Sie eine globale Variable in Ihrer Erweiterung verwenden, erhalten Sie einen Laufzeitfehler: Versuchen Sie, eine in **/var/log/ns.log**gemeldete globale Variable zu aktualisieren oder zu erstellen.

Tippfehler in Variablennamen sind ein potenzielles Problem, da die Variable mit dem Tippfehler als eine andere globale Variable interpretiert wird und keinen Syntaxfehler verursacht wie in Sprache wie C oder Java. Wie oben erwähnt, erhalten Sie stattdessen einen Laufzeitfehler.

Lokale Variablen

Eine Variable kann als lokal für einen Anweisungsblock deklariert werden, z. B. eine Funktion. Dies geschieht durch den lokalen Variablennamen. Die Variable wird auf den Block beschränkt, dh sie existiert nur innerhalb des Blocks. Die lokale Deklaration kann der Variablen optional einen Wert zuweisen.

Beispiele:

local headers = {}
local combined_headers = {}

Ausdrücke

October 5, 2021

Ausdrücke berechnen Werte aus Variablen- und Literalwerten.

- Arithmetische Operationen
- Relationale Vorgänge
- Logische Vorgänge
- Verkettung
- Testdauer
- Rangfolge

Arithmetische Operationen

Arithmetische Operationen werden für Zahlenwerte durchgeführt. Wenn ein Zeichenfolgenwert in einer arithmetischen Operation verwendet wird, wird er in eine Zahl konvertiert — wenn dies fehlschlägt, wird ein Fehler zurückgegeben.

a + b	a und b hinzufügen

a - b	subtrahieren b von a
a * b	multiplizieren a und b
a/b	dividieren a durch b
a% b	modulo = a - math.floor (a/b) *b
a ^ b	a auf die b Kraft erhöhen; b kann eine beliebige Zahl sein
-a	negieren Sie ein

Relationale Vorgänge

Relationale Operationen vergleichen zwei Werte und geben true zurück, wenn die Beziehung erfüllt ist, und false, wenn dies nicht der Fall ist. Relationale Operationen können zwischen Werten eines beliebigen Typs durchgeführt werden. Wenn die Werte nicht vom gleichen Typ sind, wird false zurückgegeben. Zahlen werden auf die übliche Weise verglichen. Strings werden mit der Sortiersequenz für das aktuelle Gebietsschema verglichen.

a == b	a ist gleich b
a ~= b	a ist nicht gleich b
a < b	a ist kleiner als b
a > b	a ist größer als b
a <= b	a ist kleiner oder gleich b
a >= b	a ist größer oder gleich b

Logische Operationen

Logische Operationen werden traditionell für boolesche Werte ausgeführt, aber in dieser Sprache können sie für zwei beliebige Werte ausgeführt werden. nil und false gilt als falsch und jeder andere Wert gilt als wahr. Logische Operationen verwenden eine Kurzschnittauswertung. Wenn der erste Wert das Ergebnis der Operation bestimmt, wird der zweite Wert nicht ausgewertet.

a und b	Wenn a falsch oder nil ist, geben Sie eine else zurück b
a oder b	Wenn a nicht falsch und nicht nil ist, geben Sie eine else zurück b
nicht ein	wenn a nicht falsch oder nil ist, gibt false zurück sonst true zurück

Die Operationen “und” und “oder” können für die bedingte Auswertung innerhalb eines Ausdrucks verwendet werden:

a oder b	kann verwendet werden, um einen Standardwert b bereitzustellen, wenn a nicht initialisiert ist (nil). Dies ist nützlich für optionale Parameter in Funktionen.
a und b oder c	kann verwendet werden, um nicht-nil b oder c basierend auf der Bedingung a zu wählen. Wenn a wahr ist, gibt a und b “b” zurück, und b oder c gibt b zurück. Wenn a falsch ist, dann a und b gibt false zurück oder c gibt c. Dies ist äquivalent zu einem? b: c in der Programmiersprache C.

Verkettung

String-Verkettung ist s1.. s2. Dadurch wird eine neue Zeichenfolge erstellt, die groß genug ist, um den Inhalt von s1 und s2 zu halten, und kopiert den Inhalt in die neue Zeichenfolge. Ein Fehler tritt auf, wenn s1 oder s2 keine Zeichenfolgen sind. Beachten Sie, dass wiederholte Verkettung einen erheblichen Kopieraufwand haben kann. Wenn Sie eine Zeichenfolge von n Bytes erstellen, indem Sie jeweils ein Byte verketten, kopiert dies n* (n+1) /2 Bytes. Für eine bessere Leistung können Sie Teile einer Zeichenfolge, die in eine Tabelle verkettet werden soll (später diskutiert) und dann die Funktion table.concat () verwenden. Ein Beispiel dafür wird im Beispiel COMBINE_HEADERS () gezeigt.

Testdauer

Die Länge eines Strings s wird von #s zurückgegeben. Der Operator # wird auch mit Array-Tabellen verwendet, wie später erläutert.

Rangfolge

Die Operatorpriorität bestimmt die Reihenfolge, in der Operationen in einem Ausdruck ausgeführt werden, wobei Operationen mit höherer Priorität vor denen mit niedrigerer Priorität ausgeführt werden. Die Prioritätsreihenfolge kann wie gewohnt durch Klammern überschrieben werden. Beispielsweise hat in`a + b \* c`, * eine höhere Priorität als +, daher wird der Ausdruck als ausgewertet`a + (b \* c)`.

höchste	^
-	nicht # - (unär)
-	* / %
-	..
-	= ~= < > <= >=
-	und
niedrigste	oder

Operationen mit der gleichen Priorität werden von links nach rechts (links assoziativ) ausgeführt, außer ^ und.., die von rechts nach links ausgeführt werden (rechts assoziativ). Daher wird a^b^c als a^ (b^c) ausgewertet.

Zuweisung

October 5, 2021

Die Zuweisungsanweisung wertet einen Ausdruck aus und weist den resultierenden Wert einer Variablen zu.

```
variable = expression
```

Wie bereits erwähnt, können Werte eines beliebigen Typs jeder Variablen zugewiesen werden, so dass Folgendes erlaubt ist:


```
local v1 = "a string literal"
v1 = 10
```

Eine Zuweisungsanweisung kann tatsächlich mehrere Variablen mit dem Formular

variable1, variable2, … = expression1, expression2, …

Wenn mehr Variablen als Ausdrücke vorhanden sind, werden den zusätzlichen Variablen nil zugewiesen. Wenn mehr Ausdrücke als Variablen vorhanden sind, werden die zusätzlichen Ausdruckswerte verworfen. Die Ausdrücke werden alle vor den Zuweisungen ausgewertet, so dass diese verwendet werden können, um die Werte zweier Variablen prägnant auszutauschen:

v1, v2 = v2, v1

entspricht

tmp = v1
v2 = v1
v1 = tmp

Tabellen

October 5, 2021

Tabellen sind Sammlungen von Einträgen mit Schlüsseln und Werten. Sie sind die einzige aggregierte Datenstruktur zur Verfügung gestellt. Alle anderen Datenstrukturen (Arrays, Listen, Sets usw.) werden aus Tabellen erstellt. Tabellenschlüssel und -werte können beliebig sein, einschließlich anderer Tabellen. Schlüssel und Werte innerhalb derselben Tabelle können Typen mischen.

- Tabellenkonstruktoren
- Tabellenverwendung
- Tabellen als Arrays
- Tabellen als Datensätze

Tabellenkonstruktoren

Mit Tabellenkonstruktoren können Sie eine Tabelle mit Schlüsseln und zugehörigen Werten angeben. Die Syntax lautet:

{[key1] = value1, [key2] = value2, …}

wobei die Schlüssel und Werte Ausdrücke sind. Wenn es sich bei den Schlüsseln um Zeichenfolgen handelt, die keine reservierten Wörter sind, können die Klammern und Anführungszeichen um die Schlüssel weggelassen werden. Beispiel:

{key1 = “value1”, key2 = “value2”, key3 = “value3”}

Eine leere Tabelle wird einfach durch {} angegeben.

Ein Tabellenkonstruktor kann in einer Zuweisung verwendet werden, um eine Variable auf eine Tabelle zu verweisen. Beispiele:

local t1 = {} – set t1 to an empty table
local t2 = {key1 = “value1”, key2 = “value2”, key3 = “value3”}

Beachten Sie, dass Tabellen selbst anonym sind. Mehr als eine Variable kann auf dieselbe Tabelle verweisen. Fortsetzung des obigen Beispiels:

local t3 = t2 — sowohl t2 als auch t3 beziehen sich auf dieselbe Tabelle

Tabellenverwendung

Wie erwartet, können Sie Schlüssel verwenden, um Werte in einer Tabelle zu finden. Die Syntax ist[Tabellenschlüssel], wobei Tabelle eine Tabellenreferenz ist (normalerweise eine Variable, der einer Tabelle zugewiesen wurde), und Schlüssel ist ein Ausdruck, der den Schlüssel bereitstellt. Wenn dies in einem Ausdruck verwendet wird und der Schlüssel in der Tabelle vorhanden ist, wird der Wert zurückgegeben, der dem Schlüssel zugeordnet ist. Wenn sich der Schlüssel nicht in der Tabelle befindet, gibt dies null zurück. Wenn dies als Variable in einer Zuweisung verwendet wird und der Schlüssel nicht in der Tabelle vorhanden ist, wird ein neuer Eintrag für den Schlüssel und den Wert erstellt. Wenn der Schlüssel bereits in der Tabelle vorhanden ist, wird der Wert des Schlüssels durch den neuen Wert ersetzt. Beispiele:

local t = {} — setzt t auf eine leere Tabelle
t[“k1”] = “v1” — erstellt einen Eintrag für den Schlüssel “k1” und den Wert “v1”
v1 = t[“k1”] — setzt v1 auf den Wert für Schlüssel “k1” = “v1”
t[“k1”] = “new_v1” — setzt den Wert für Schlüssel “k1” auf “new_v1”

Tabelle als Arrays

Das traditionelle Array kann mit einer Tabelle mit Integer-Schlüsseln als Indizes implementiert werden. Ein Array kann beliebige Indizes haben, einschließlich negativer, aber die Konvention besteht darin, Arrays am Index 1 zu starten (nicht 0, wie es bei Sprachen wie C und Java der Fall ist). Es gibt einen speziellen Tabellenkonstruktor für solche Arrays:

{value1, value2, value3, … }

Array-Referenzen sind dann[Array-Index].

Der Längenoperator # gibt die Anzahl der Elemente in einem Array mit aufeinanderfolgenden Indizes ab 1. Beispiel:

local a = {“value1”, “value2”, “value3”}
local length = #a – sets length to the length of array a = 3

Arrays können dünn sein, wobei nur die definierten Elemente zugewiesen werden. Aber # kann nicht für ein spärliches Array mit nicht aufeinanderfolgenden Indizes verwendet werden. Beispiel:

local sparse_array = {} — richte ein leeres Array ein
sparse_array[1] = “value1” — füge ein Element bei Index 1
sparse_array[99] = “value99” hinzu — füge ein Element bei Index 99 hinzu

Mehrdimensionale Arrays können als Tabellen von Tabellen eingerichtet werden. Zum Beispiel könnte eine 3x3-Matrix eingerichtet werden durch:

local m = {{1, 2, 3}, {4, 5, 6}, {7, 8, 9}}
lokal v22 = m[2][2] — setzt v22 auf 5

Tabellen als Datensätze

Datensätze mit Feldern können als Tabellen mit Feldnamenschlüsseln implementiert werden. Das Referenzformular table.field kann für die Tabelle[“field”]verwendet werden. Beispiele:

local person = {name = “John Smith”, phone = “777-777-7777”}
local name = person.name – sets name to “John Smith”

Ein Array von Tabellen kann für eine Sequenz von Datensätzen verwendet werden. Beispiel:

local people = {
{name = “John Smith”, phone = “777-777-7777”},
{name = “Jane Doe”, phone = “888-888-8888”}
…
}

name = people[2].name - setzt den Namen auf “Jane Doe”

Steuerungsstrukturen

October 5, 2021

Die Erweiterungsfunktionssprache stellt die üblichen Anweisungen zur Steuerung der Programmausführung bereit.

- Wenn dann sonst
- Während Do und Wiederholen bis
- Numerisch Für
- Pause/Untbr

- Gehe zu

Wenn dann sonst

Wenn Anweisungen wählen Sie Blöcke von Anweisungen, die auf einer oder mehreren Bedingungen ausgeführt werden sollen. Es gibt drei Formen:

Wenn dann Formular

```
if expression then
     statements to execute if expression is not false or nil
end
<!--NeedCopy-->
```

Wenn dann sonst Formular

```
if expression then
     statements to execute if expression is not false or nil
else
     statements to execute if expression is false or nil
end
<!--NeedCopy-->
```

Wenn dann andernfalls Formular

```
if expression1 then
     statements to execute if expression1 is not false or nil
     elseif expression2 then
          statements to execute if expression2 is not false or nil
. . .
else
     statements to execute if all expressions are false or nil
end
<!--NeedCopy-->
```

Beispiel:


```
if headers[name] then

     local next_value_index = #(headers[name]) + 1
     headers[name][next_value_index] = value

else

     headers[name] = {
 name .. ":" .. value }


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

Hinweis:

- Der Ausdruck ist nicht in Klammern eingeschlossen, wie es in C und Java der Fall ist.
- Es gibt kein Äquivalent zur C/Java switch-Anweisung. Sie müssen eine Reihe von if elseif-Anweisungen verwenden, um das Äquivalent zu tun.

Während Do und Wiederholen bis

Die **while-** und **repeat-Anweisungen** stellen Schleifen bereit, die von einem Ausdruck gesteuert werden.

```
while expression do
     statements to execute while expression is not false or nil
end

repeat

     statements to execute until expression is not false or nil

until expression
<!--NeedCopy-->
```

Beispiel für while:

```
local a = {
 1, 2, 3, 4 }

```



```
local sum, i = 0, 1 -- multiple assignment initializing sum and i
while i <= #a do -- check if at the end of the array
     sum = sum + a[i] -- add array element with index i to sum
     i = i + 1 -- move to the next element
end
<!--NeedCopy-->
```

Beispiel für Wiederholung:

```
sum, i = 0, 1 -- multiple assignment initializing sum and i
repeat
     sum = sum + a[i] -- add array element with index i to sum
     i = i + 1 -- move to the next element
until i > #a -- check if past the end of the array
<!--NeedCopy-->
```

Natürlich ist es möglich, eine Schleife zu schreiben, die nicht beendet, zum Beispiel, wenn Sie die i = i + 1 Anweisung in einem dieser Beispiele weglassen. Wenn eine solche Funktion ausgeführt wird, erkennt Citrix ADC, dass die Funktion nicht innerhalb eines angemessenen Zeitraums abgeschlossen wurde, und beendet sie mit einem Laufzeitfehler:

`Cpu limit reached. Terminating extension execution in [[string "function extension function..."]]: line line-number.`

wird in /var/log/ns.log gemeldet.

Numerisch Für

Es gibt zwei Arten von for-Schleifen. Die erste ist die numerische für, die der üblichen Verwendung der for -Anweisung in C und Java ähnelt. Die numerische for -Anweisung initialisiert eine Variable, testet, ob die Variable einen endgültigen Wert übergeben hat, und wenn nicht einen Block von Anweisungen, erhöht die Variable und wiederholt. Die Syntax für die numerische for-Schleife lautet:

```
for variable = initial, final, increment do

     statements in the loop body

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


wobei initiale, final und increment alle Ausdrücke sind, die Zahlen ergeben (oder in). Variable wird als lokal für den for-Schleifen-Anweisungsblock angesehen; sie kann nicht außerhalb der Schleife verwendet werden. Inkrement kann weggelassen werden; der Standardwert ist 1. Die Ausdrücke werden einmal am Anfang der Schleife ausgewertet. Die terminierende Bedingung ist variabel > final, wenn das Inkrement positiv ist, und variabel < final, wenn das Inkrement negativ ist. Die Schleife endet sofort, wenn das Inkrement 0 ist.

Beispiel (entspricht den while- und Wiederholungsschleifen im vorhergehenden Abschnitt):

```
sum = 0
for i = 1, #a do -- increment defaults to 1
     sum = sum + a[i]
end
<!--NeedCopy-->
```

Der zweite Typ von for-Schleife ist das generische für, das für flexiblere Arten von Schleifen verwendet werden kann. Es beinhaltet die Verwendung von Funktionen, so wird später diskutiert werden, nachdem Funktionen eingeführt wurden.

Pause/Untbr

Die break-Anweisung wird innerhalb einer while, repeat oder for-Schleife verwendet. Es wird die Schleife beenden und die Ausführung bei der ersten Anweisung nach der Schleife fortsetzen. Beispiel (auch äquivalent zu den vorherigen while, repeat, and for-Schleifen):

```
sum, i = 0, 1
while true do
     if i > #a then
          break
     end
     sum = sum + a[i]
     i = i + 1
end
<!--NeedCopy-->
```

Gehe zu

Die goto-Anweisung kann verwendet werden, um vorwärts oder rückwärts zu einer Beschriftung zu springen. Das Label ist ein Bezeichner und seine Syntax lautet:: label::. Die goto-Anweisung ist goto label. Beispiel (noch einmal äquivalent zu den vorherigen Schleifen):


```
sum, i = 0, 1
::start_loop::
     if i > #a then
          goto end_loop -- forward jump
     end
     sum = sum + a[i]
     i = i + 1
     goto start_loop -- backwards jump
::end_loop::
. . .
<!--NeedCopy-->
```

Es gab eine lange anhaltende Kontroverse über die Verwendung von gotos in der Programmierung. Im Allgemeinen sollten Sie versuchen, die anderen Steuerstrukturen zu verwenden, um Ihre Funktionen lesbarer und zuverlässiger zu machen. Aber gelegentlich vernünftige Verwendung von gotos kann zu besseren Programmen führen. Insbesondere kann gotos bei der Handhabung von Fehlern nützlich sein.

Funktionen

October 5, 2021

Funktionen sind ein grundlegender Baustein der Programmierung — sie sind eine bequeme und leistungsfähige Möglichkeit, Anweisungen zu gruppieren, die eine Aufgabe ausführen. Sie sind die Schnittstelle zwischen der Citrix ADC Appliance und dem Erweiterungscode. Für Richtlinien definieren Sie Richtlinienerweiterungsfunktionen. Bei Protokollen implementieren Sie Callback-Funktionen für das Protokollverhalten. Funktionen bestehen aus Funktionsdefinitionen, die angeben, welche Werte in und aus der Funktion übergeben werden und welche Anweisungen für die Funktion ausgeführt werden, und Funktionsaufrufe, die Funktionen mit bestimmten Eingabedaten ausführen und Ergebnisse aus der Funktion erhalten.

Callback-Funktionen des Protokollverhaltens

Das TCP-Clientverhalten besteht aus einer Callback-Funktion (on_data), die TCP-Client-Datenstream-Ereignisse verarbeitet. Um Message Based Load Balancing (MBLB) für ein TCP-basiertes Protokoll zu implementieren, können Sie Code für diese Callback-Funktion hinzufügen, um den TCP-Datenstrom vom Client zu verarbeiten und den Bytestream in Protokollmeldungen zu analysieren.

Die Callback-Funktionen in einem Verhalten werden mit einem Kontext aufgerufen, der der Verarbeitungsmodulstatus ist. Der Kontext ist die Instanz des Verarbeitungsmoduls. Beispielsweise werden die TCP-Clientverhalten Callbacks mit unterschiedlichen Kontexten für verschiedene Client-TCP-Verbindungen aufgerufen.

Zusätzlich zum Kontext können die Verhaltensrückrufe andere Argumente haben. Normalerweise werden die restlichen Argumente als Payload übergeben, was die Sammlung aller Argumente ist. So können die programmierbaren Verarbeitungsmodulinstanzen als eine Kombination aus Instanzstatus plus Ereignisrückruffunktionen gesehen werden, dh dem Kontext plus Verhalten. Und der Verkehr fließt durch die Pipeline als Ereignisnutzlast.

Prototyp der TCP-Client-Callback-Funktion:

```
1             Function                client on_data (ctxt, payload)
2
3                                             //.code
4
5             end
```

Wobei:

- ctxt - TCP-Clientverarbeitungskontext
- Nutzlast — Ereignisnutzlast
  - payload.data - Empfangene TCP-Daten, verfügbar als Bytestrom

Richtlinienerweiterungsfunktionen

Da die NetScaler Richtlinienausdruckssprache stark typisiert ist, muss die Definition einer Erweiterungsfunktion die Typen ihrer Eingaben und ihren Rückgabewert angeben. Die Lua-Funktionsdefinition wurde um folgende Typen erweitert:

```
1 function self-type:function-name(parameter1: parameter1-type, etc.):
     return-type
2      statements
3 end
4
5 where,
6
7 the types are NSTEXT, NSNUM, NSBOOL, or NSDOUBLE.
8 <!--NeedCopy-->
```


Selbsttyp ist der Typ des impliziten Selbstparameters, der an die Funktion übergeben wird. Wenn die Erweiterungsfunktion in einem Citrix ADC Richtlinienausdruck verwendet wird, ist dies der Wert, der vom Ausdruck links neben der Funktion generiert wird. Eine andere Möglichkeit, dies anzuzeigen, besteht darin, dass die Funktion diesen Typ in der Citrix ADC Richtliniensprache erweitert.

Die Parametertypen sind die Typen jedes Parameters, der im Aufruf der Erweiterungsfunktion im Richtlinienausdruck angegeben wird. Eine Erweiterungsfunktion kann null oder mehr Parameter haben.

return-type ist der Typ des Wertes, der durch den Aufruf der Erweiterungsfunktion zurückgegeben wird. Es ist die Eingabe für den Teil des Richtlinienausdrucks, falls vorhanden, rechts von der Funktion, oder andernfalls ist der Wert des Ausdrucksergebnisses.

Beispiel:

```
function NSTEXT:COMBINE_HEADERS(): NSTEXT
```

Verwendung der Erweiterungsfunktion in einer Richtlinienausdrücke:

```
HTTP.REQ.FULL_HEADER.AFTER_STR(”HTTP/1.1rn”).COMBINE_HEADERS()
```

Hier ist der self Parameter das Ergebnis von HTTP.REQ.FULL_HEADER.AFTER_STR (“HTTP/1.1rn”), was ein Textwert ist. Das Ergebnis des COMBINE_HEADERS () -Aufrufs ist Text, und da sich nichts rechts neben diesem Aufruf befindet, ist das Ergebnis des gesamten Ausdrucks Text.

Lokale Funktionsdefinition

Neben Erweiterungsfunktionen können keine globalen Funktionen in einer Erweiterungsdatei definiert werden. Aber lokale Funktionen können innerhalb von Erweiterungsfunktionen mit der normalen Lua-Funktionsanweisung definiert werden. Dies deklariert den Namen der Funktion und die Namen ihrer Parameter (auch als Argumente bezeichnet), und wie alle Deklarationen in Lua werden keine Typen angegeben. Die Syntax dafür ist:

```
local function function-name(parameter1-name, parameter2-name, etc.)
     statements
end
<!--NeedCopy-->
```

Die Funktions- und Parameternamen sind alle Bezeichner. (Der Funktionsname ist eigentlich eine Variable und die Funktionsanweisung ist Abkürzung für lokale Funktionsname = Funktion (Parameter1 usw.), aber Sie müssen diese Subtilität nicht verstehen, um Funktionen zu verwenden.)

Beachten Sie, dass usw. hier für die Fortsetzung des Musters von Parameternamen anstelle des üblichen… verwendet wird. Dies liegt daran, dass… selbst tatsächlich eine Variablen-Parameterliste bedeutet, die hier nicht diskutiert wird.

Funktionskörper und Rücklauf

Der Block von Anweisungen zwischen Funktion und End-Anweisung ist der Funktionskörper. Im Funktionskörper wirken die Funktionsparameter wie lokale Variablen, mit Werten, die von den Funktionsaufrufen bereitgestellt werden, wie zuvor beschrieben.

Die return-Anweisung liefert Werte an den Aufrufer der Funktion zurückgegeben werden. Es muss am Ende eines Blocks erscheinen (in einer Funktion, wenn dann, für Schleife, und so weiter; Es kann in seinem eigenen Block sein tun Rückkehr… Ende). Es kann keine, einen oder mehrere Rückgabewerte angeben:

```
return -- returns nil
return expression -- one return value
return expression1, expression2, ... -- multiple return values
<!--NeedCopy-->
```

Beispiele:

```
local function fsum(a)
     local sum = 0
     for i = 1, #a do
          sum = sum + a[i]
     end
     return sum
end

local function fsum_and_average(a)
     local sum = 0
     for i = 1, #a do
          sum = sum + a[i]
     end
     return sum, sum/#a
end
<!--NeedCopy-->
```

Funktionsaufrufe

Ein Funktionsaufruf führt den Körper einer Funktion aus, liefert Werte für ihre Parameter und empfängt Ergebnisse. Die Syntax für einen Funktionsaufruf ist Funktionsname (expression1, expression2 usw.), wobei die Funktionsparameter auf die entsprechenden Ausdrücke gesetzt werden. Die Anzahl der Ausdrücke und Parameter muss nicht gleich sein. Wenn weniger Ausdrücke als

Parameter vorhanden sind, werden die übrigen Parameter auf nil gesetzt. Sie können also einen oder mehrere Parameter am Ende des Aufrufs optional machen, und Ihre Funktion kann überprüfen, ob sie angegeben sind, indem Sie überprüfen, ob sie nicht Null sind. Eine übliche Möglichkeit, dies zu tun, ist mit der Operation oder:

```
function f(p1, p2) -- p2 is optional
     p2 = p2 or 0 -- if p2 is nil, set to a default of 0
     . . .
end
<!--NeedCopy-->
```

Wenn mehr Ausdrücke als Parameter vorhanden sind, werden die verbleibenden Ausdruckswerte ignoriert.

Wie bereits erwähnt, können Funktionen mehrere Werte zurückgeben. Diese Rückgaben können in einer Mehrfachzuweisungsanweisung verwendet werden. Beispiel:

```
local my_array = {
 1, 2, 3, 4 }

local my_sum, my_ave = sum_and_average(my_array)
<!--NeedCopy-->
```

Iterator-Funktionen und generische for-Schleifen

Jetzt, da wir Funktionen eingeführt haben, können wir über generische for-Schleifen sprechen. Die Syntax für die generische for-Schleife (mit einer Variablen) lautet:

```
for variable in iterator(parameter1, parameter2, etc.) do
     statements in the for loop body
end
<!--NeedCopy-->
```

wobei iterator () eine Funktion mit null oder mehr Parametern ist, die für jede Iteration des Schleifenkörpers einen Wert für Variable bereitstellt. Die Iteratorfunktion verfolgt, wo sie sich in der Iteration befindet, indem sie eine Technik namens Closure verwendet, über die Sie sich hier keine Sorgen machen müssen. Es signalisiert das Ende der Iteration, indem null zurückgegeben wird. Iterator-Funktionen können mehr als einen Wert für die Verwendung in einer Mehrfachzuweisung zurückgeben.

Das Schreiben einer Iteratorfunktion ist jenseits des Rahmens dieses Papiers, aber es gibt eine Reihe nützlicher integrierter Iteratoren, die das Konzept veranschaulichen. Eins ist der Paare () Iterator, der durch die Einträge in einer Tabelle iteriert und zwei Werte zurückgibt, den Schlüssel und den Wert des nächsten Eintrags.

Beispiel:

```
local t = {
 k1 = ”v1”, k2 = ”v2”, k3 = ”v3” }

local a = {
  }
  -- array to accumulate key-value pairs
local n = 0 -- number of key-value pairs
for key, value in pairs(t) do
     n = n + 1
     a[n] = key .. ” = ” .. value -- add key-value pair to the array
end
local s = table.concat(a, ”; ”) -- concatenate all key-value pairs into
    one string
<!--NeedCopy-->
```

Ein weiterer nützlicher Iterator ist die string.gmatch () Funktion, die im folgenden COMBINE_HEADERS () Beispiel verwendet wird.

Citrix ADC Erweiterungen - Bibliotheksreferenz

October 5, 2021

Die Liste der Bibliotheken, die in Richtlinienerweiterungen unterstützt werden.

- Basisbibliothek
- Zeichenfolgenbibliothek
- Muster für reguläre Ausdrücke - Zeichenklassen
- Muster für reguläre Ausdrücke - Pattern Items
- Tabellenbibliothek
- Mathematische Bibliothek
- Bitweise Bibliothek
- Betriebssystembibliothek
- Citrix ADC-Bibliothek

Basisbibliothek

assert (v[, message])	Ergibt einen Fehler mit einer optionalen Meldung, wenn v falsch ist.
Fehler (Meldung)	Beendet eine Funktion und meldet die Fehlermeldung.
ipairs (a)	Iterator für ein Array a Gibt einen Index und einen Wert für jede Iteration zurück.
Paare (t)	Iterator für eine Tabelle t. Gibt einen Schlüssel und einen Wert für jede Iteration zurück.
Tonumber (e[, Basis])	Konvertiert e in eine Zahl mit optionaler Basis.
tostring (v)	Konvertiert v in einen String
Typ (v)	Gibt den Typ von v: Zahl, String, boolean, Tabelle usw.
getmetatable (Objekt)	Gibt nil zurück, wenn das Objekt keine Metatable hat. Andernfalls wird der zugeordnete Wert zurückgegeben, wenn die Metatable des Objekts ein Feld __metatable hat. Andernfalls gibt die Metatable des angegebenen Objekts zurück.
setmetatable (Tabelle, Metatable)	Legt die Metatable für die angegebene Tabelle fest. (Sie können die Metatable anderer Typen nicht von Lua ändern, nur von C.) Wenn metatable nil ist, entfernt die Metatable der angegebenen Tabelle. Wenn die ursprüngliche Metatable ein Feld __metatable hat, wird ein Fehler ausgelöst.
wählen (Index, ··)	Gibt alle Argumente nach dem Argument Zahlenindex zurück. Wenn Index Zeichenfolge # ist, dann gibt es die Gesamtzahl der zusätzlichen Argumente, die er empfangen hat.

pcall (f [, arg1, ···])	Ruft Funktion f mit den angegebenen Argumenten im geschützten Modus auf. Es gibt Statuscode als erstes Ergebnis, das sagt, ob Aufruf erfolgreich oder nicht. Wenn der Aufruf erfolgreich war, gibt er zusammen mit dem Statuscode auch alle Ergebnisse des Aufrufs zurück, andernfalls wird eine Fehlermeldung zurückgegeben.
xpcall (f, msgh[, arg1, ···])	Diese Funktion ähnelt pcall, außer dass sie auch ein Argument für die Fehlerbehandlung benötigt.
_VERSION	Gibt die aktuelle Interpreterversion zurück.

Zeichenfolgenbibliothek

string.byte (s[, i [, j]])	Gibt die Bytewerte für s[i] bis s[j]zurück. Standard i = 1 und j = i
string.char (…)	Gibt einen String zurück, der aus den Integer-Parametern konstruiert wurde.
string.find (s, pattern[, init [, plain])	Sucht nach der ersten Übereinstimmung eines regulären Ausdrucksmusters in s. Gibt den ersten und letzten Indizes von Übereinstimmung oder nil zurück. init ist Index zu starten, Standard 1. plain = true bedeutet pattern ist kein Regex.
Zeichenfolgenformat (Form,…)	Gibt eine formatierte Version der Parameter zurück.
String.gmatch (s, Muster)	Iterator für die Suche nach s mit dem Regex-Muster. Gibt übereinstimmende Werte zurück.
string.gsub (s, muster, repl[, n])	Gibt eine Kopie von s zurück, in der alle (oder n) Vorkommen des Musters durch repl ersetzt wurden.

String.len (n)	Gibt die Zeichenfolgenlänge zurück.
String.untere (n)	Gibt eine Kopie der Zeichenfolge zurück, die in Kleinbuchstaben konvertiert wurde.
string.match (s, muster[, init])	Sucht nach der ersten Übereinstimmung des Regex-Musters in s und gibt die Captures oder das gesamte Muster zurück. init ist der zu startende Index, Standard 1.
string.rep (s, n[, sep])	Gibt einen String zurück, der n Kopien von s ist, mit Separator sep, Standard kein Trennzeichen
String.reverse (s)	Gibt eine Zeichenfolge zurück, die umgekehrt ist.
string.sub (s, i[, j])	Gibt die Teilzeichenfolge von s[i] bis s zurück[j], Standard j ist das Ende der Zeichenfolge.
String.oben (n)	Gibt eine Kopie der Zeichenfolge zurück, die in Großbuchstaben konvertiert wurde.
string.dump (Funktion)	Gibt einen String zurück, der eine binäre Darstellung der angegebenen Funktion enthält.

Muster für reguläre Ausdrücke - Zeichenklassen

x	das Zeichen x, mit Ausnahme von magischen Zeichen ^$ ()%.[]*+-?)
.	beliebiges Zeichen
%a	beliebiger Buchstabe
%c	beliebiges Steuerzeichen
%d	beliebige Ziffer
%g	beliebiges druckbares Zeichen außer Leerzeichen
%l	Kleinbuchstaben
%p	beliebiges Satzzeichen
%s	beliebiges Leerzeichen

%u	beliebiger Großbuchstabe
%w	beliebiges alphanumerisches Zeichen
%x	ein maskiertes magisches Zeichen x (z. B.%%)
[Set]	eine Reihe von Zeichen: Sequenz von einzelnen Zeichen, Bereiche x-y und% Klassen
[^set]	Zeichen, die nicht im Satz enthalten sind.

Muster für reguläre Ausdrücke - Musterelemente

X	eine Zeichenklasse
X*	0 oder mehr längste Wiederholungen von Zeichen in X
X+	1 oder mehr Wiederholungen von Zeichen in X
X-	0 oder mehr kürzeste Wiederholungen von Zeichen in X
X?	0 oder 1 Zeichen in X
%n	n=1 bis 9; entspricht der n-ten erfassten Zeichenfolge
%bxy	entspricht Teilzeichenfolge zwischen zwei symmetrischen Zeichen x und y. Beispiel %b() entspricht Teilzeichenfolge zwischen zwei ausbalancierten Klammern.
%f[Set]	eine leere Zeichenfolge an einer beliebigen Position entspricht, so dass das nächste Zeichen zum Satz gehört und das vorherige Zeichen nicht zu setzen gehört.

Ein Muster ist eine Folge von Musterelementen. ^pattern entspricht dem Anfang einer Zeichenfolge und pattern$ entspricht dem Ende der Zeichenfolge.

Übereinstimmende Teilzeichenfolgen können mit (Muster) erfasst werden. Klammern ohne Muster () erfassen die aktuelle Zeichenfolgenposition (eine Zahl).

Tabellenbibliothek

table.concat (list[, sep [, i [, j]]])	Gibt eine Stringliste zurück[i].. sep.. list[i+1].. sep. list[j]. Standard sep ist die leere Zeichenfolge. Der Standardwert i ist 1, j ist #list.
table.insert (Liste,[Pos,]Wert)	Fügt Wert in die Liste an Indexposen ein. Der Standardwert für pos ist #list (Ende der Liste).
table.pack(…)	Gibt ein Array mit den Parametern ab Index 1 und einen Schlüssel n mit der Gesamtzahl der Parameter.
table.remove (Liste[, Pos])	Entfernt aus der Liste das Element an Position pos, Verschieben Elemente, um die Position zu füllen. Gibt das entfernte Element zurück. Default for posis #list (end of the list.)
table.sort (list[, comp])	Sortieren Sie die Elemente der Liste an Ort und Stelle. comp ist die Vergleichsfunktion zu verwenden. Der Standardwert für comp ist <.
table.unpack(list[, i [, j]])	Gibt Liste[i] durch Liste zurück[j] . Der Standardwert für i ist 1 und j ist #list <c/ode>.

Mathematische Bibliothek

Verschiedene trigonometrische und logarithmische Funktionen werden nicht angezeigt.

math.abs(x)	Gibt den absoluten Wert von x zurück.
math.ceil(x)	Gibt die kleinste ganze Zahl >= x zurück.
math.floor(x)	Gibt die größte ganze Zahl <= x zurück.
math.fmod(x,y)	Gibt den Rest von x/y zurück, um den Quotienten auf Null zu runden.
math.huge	Ein Wert >= eine beliebige andere Zahl.
math.max(x,…)	Gibt das maximale Argument zurück.
math.min(x,…)	Gibt das minimale Argument zurück.
math.modf(x)	Gibt die Integral- und Bruchteile von x zurück.

math.random()	Gibt eine pseudo-zufällige Zahl zwischen 0 und 1.
math.random(m)	Gibt eine pseudo-zufällige Ganzzahl zwischen 1 und m zurück.
math.random(m, n)	Gibt eine pseudo-zufällige Ganzzahl zwischen m und n.
math.randomseed(x)	Setzt den Pseudo-Zufallszahlengenerator auf x gesetzt.
math.sqrt(x)	Gibt die Quadratwurzel von x (x^0.5)
math.acos(x)	Gibt den Bogenkosinus von x (im Bogenmaß) zurück.
math.asin(x)	Gibt den Bogensinus von x (im Bogenmaß) zurück.
math.atan(x)	Gibt den Bogen-Tangens von x (im Bogenmaß) zurück.
math.atan2(y, x)	Gibt den Bogen-Tangens von y/x (im Bogenmaß) zurück.
math.cos(x)	Gibt den Kosinus von x zurück.
math.cosh(x)	Gibt den hyperbolischen Kosinus von x zurück.
math.sin(x)	Gibt den Sinus von x zurück.
math.sinh(x)	Gibt den hyperbolischen Sinus von x zurück.
math.tan(x)	Gibt den Tangens von x zurück.
math.tanh(x)	Gibt den hyperbolischen Tangens von x zurück.
math.deg(x)	Gibt den Winkel x (in Bogenmaß angegeben) in Grad zurück.
math.exp(x)	Gibt den Wert e^x zurück.
math.frexp (x)	Gibt m und e so zurück, dass x = m2e, e eine ganze Zahl ist und der absolute Wert von m im Bereich [0.5, 1) liegt.
math.ldexp (m, e)	Gibt m2e zurück (e sollte eine ganze Zahl sein).
math.log (x [, Basis])	Gibt den Logarithmus von x in der angegebenen Basis zurück. Der Standardwert für base ist e.

math.pow (x, y)	Gibt x^y zurück.
math.rad (x)	Gibt den Winkel x (in Grad angegeben) im Bogenmaß zurück.
math.pi	Der Wert von π.

Bitweise Bibliothek

Sofern nicht anders angegeben:

- Alle Funktionen akzeptieren numerische Argumente im Bereich (-2^51, +2^51).
- Jedes Argument wird auf den Rest seiner Division um 2 ^ 32 normalisiert und (auf eine unbestimmte Weise) auf eine Ganzzahl abgeschnitten, so dass sein endgültiger Wert im Bereich von [0,2^32 - 1]liegt.
- Alle Ergebnisse liegen im Bereich[0,2^32 - 1].

bit32.arshift (x, disp)	Gibt x arithmetisch verschoben disp Bits nach rechts (+disp) oder links (-disp) zurück.
bit32.band (…)	Gibt das bitweise und der Argumente zurück.
Bit32.bnot (x)	Gibt die bitweise Negation von x zurück.
bit32.bor (…)	Gibt die bitweise oder der Argumente zurück.
bit32.btest(…)	Gibt true zurück, wenn die bitweise und der Argumente nicht Null ist.
bit32.bxor (…)	Gibt das bitweise Exklusiv oder der Argumente zurück.
bit32.extract(n,field[,width])	Gibt die Bits in n von Feld zu Feld + Breite - 1 (Bitzahl von den meisten zu den geringsten signifikanten). Der Standardwert für Breite ist 1.
bit32.replace(n,v,field[,width])	Gibt eine Kopie von n mit Bits von Feld zu Feld + Breite -1 durch v. Die Standardbreite ist 1.
bit32.lrotate(x,disp)	Gibt x gedrehte Disp Bits nach links (+disp) oder rechts (-disp) zurück.

bit32.lshift(x,disp)	Gibt x verschoben disp Bits nach links (+disp) oder rechts (-disp) zurück.
bit32.rrotate(x,disp)	Gibt x gedrehte Disp Bits nach rechts (+disp) oder links (-disp) zurück.
bit32.rshift(x,disp)	Gibt x verschoben disp Bits nach rechts (+disp) oder links (-disp) zurück.

Betriebssystembibliothek

os.clock ()	Gibt eine Näherung des Betrags in Sekunden der CPU-Zeit zurück.
os.date ([Format [, Uhrzeit]])	Gibt eine Zeichenfolge oder eine Tabelle mit Datum und Uhrzeit zurück, formatiert gemäß dem angegebenen Zeichenfolgenformat.
os.time ([Tabelle])	Gibt die aktuelle Zeit zurück, wenn sie ohne Argumente aufgerufen wird, oder eine Zeit, die das Datum und die Uhrzeit darstellt, die in der angegebenen Tabelle angegeben ist.
os.difftime (t2, t1)	Gibt die Anzahl der Sekunden von Zeit t1 zu Zeit t2 zurück.

Citrix ADC-Bibliothek

ns.logger:level(message)	Protokollieren von Nachrichten, bei denen die Stufe Notfall, Warnung, Warnung, Hinweis, Info oder Debuggen ist. Die Parameter sind die gleichen wie die C printf () -Funktion: eine Formatzeichenfolge und eine variable Anzahl von Argumenten, die Werte für die% -Bezeichner in der Formatzeichenfolge angeben.

Citrix ADC Erweiterungen API-Referenz

October 5, 2021

Verhaltensweisen sind eine Formalisierung gängiger programmierbarer Muster, die auf einer Citrix ADC Appliance verfügbar sind. Ein virtueller TCP-Server unterstützt beispielsweise ein TCP-Clientverhalten und ein TCP-Serververhalten. Ein Verhalten ist ein vordefinierter Satz von Callback-Funktionen. Sie können Verhaltensweisen implementieren, indem Sie Callback-Funktionen bereitstellen. Beispielsweise kann ein TCP-Clientverhalten aus der Funktion on_data bestehen, die den TCP-Datenstrom verarbeitet.

TCP-Clientverhalten

on_data - Funktion Callback für TCP-Client-Datenereignisse. Der Rückruf nimmt zwei Argumente an:

- **ctxt** - TCP-Clientverarbeitungskontext
- **Nutzlast** — Ereignisnutzlast
  - **payload.data** - Empfangene TCP-Daten, verfügbar als Bytestrom

Verhalten des TCP-Servers

on_data - Funktion Callback für TCP-Server-Datenereignisse, nimmt der Callback zwei Argumente:

- **ctxt** - TCP-Server Verarbeitungskontext
- **Nutzlast** — Ereignisnutzlast
  - **payload.data** - empfangene TCP-Daten, verfügbar als Bytestrom

TCP-Clientkontext

Der Kontext, der an die TCP-Clientereignisrückrufe übergeben wird:

- **ctxt.output** - Der nächste Verarbeitungskontext in der Pipeline. Extension-Callback-Handler können ns.tcp.stream-Typdaten an ctxt.output senden, indem sie die Ereignisse DATA verwenden, was Teilnachricht oder EOM bedeutet, was das Ende der Protokollnachricht bedeutet. Das EOM-Ereignis kann TCP-Daten enthalten oder nicht. Ein EOM-Ereignis mit TCP-Daten kann ohne vorheriges DATA-Ereignis gesendet werden, um eine ganze Protokollnachrichtsdaten zu senden und das Ende der Nachricht zu markieren. Die Entscheidung für den Lastausgleich wird nachgeschaltet vom virtuellen Lastausgleichsserver bei den ersten empfangenen Daten getroffen. Nach Erhalt der EOM-Nachricht wird eine neue Lastausgleichsentscheidung getroffen. Um Protokollnachrichtendaten zu streamen, senden Sie mehrere DATA Ereignisse mit dem letzten Ereignis als EOM. Alle zusammenhängenden DATA-Ereignisse und

die folgenden EOM-Ereignisse werden an dieselbe Serververbindung gesendet, die durch die Lastenausgleichsentscheidung für das erste DATA-Ereignis in der Sequenz ausgewählt wurde.

- **ctxt.input** - Der vorherige Verarbeitungskontext in der Pipeline, von dem die TCP-Streamdaten stammen.
- **ctxt:hold (data)** - Funktion, um die Daten für die zukünftige Verarbeitung zu speichern. Beim Aufruf von Hold mit Daten werden die Daten im Kontext gespeichert. Später, wenn mehr Daten im gleichen Kontext empfangen werden, werden neu empfangene Daten an die zuvor gespeicherten Daten angehängt und der kombinierte Datenstrom wird dann an die on_data Callback-Funktion übergeben. Nach dem Aufruf einer Haltefunktion ist die Datenreferenz nicht mehr verwendbar und gibt Fehler bei jeder Verwendung.
- **ctxt.vserver** - Der virtuelle Serverkontext.
- **ctxt.client** — Verarbeitungskontext der Clientverbindung. Dieser Verarbeitungskontext kann verwendet werden, um Daten an den Client zu senden und einige verbindungsbezogene Informationen wie IP-Adresse, Quell- und Zielports abzurufen.
- **ctxt:close ()** — Schließen Sie die Clientverbindung, indem Sie FIN an den Client senden. Nach dem Aufruf dieser API ist der Client Verarbeitungskontext nicht mehr verwendbar und gibt Fehler bei jeder Verwendung.

TCP-Serverkontext

Der Kontext, der an die TCP-Serverereignisrückrufe übergeben wird:

- **ctxt.output** — Der nächste Verarbeitungskontext in der Pipeline. Extension-Callback-Handler können ns.tcp.stream-Typdaten an ctxt.output senden, indem sie die Ereignisse DATA verwenden, was Teilnachricht oder EOM bedeutet, was das Ende der Protokollnachricht bedeutet.
- **ctxt.input** - Der vorherige Verarbeitungskontext in der Pipeline, von dem die TCP-Streamdaten stammen.
- **ctxt:hold (data)** - Funktion, um die Daten für die zukünftige Verarbeitung zu speichern. Beim Aufruf von Hold mit Daten werden die Daten im Kontext gespeichert. Später, wenn mehr Daten im gleichen Kontext empfangen werden, werden neu empfangene Daten an die zuvor gespeicherten Daten angehängt und der kombinierte Datenstrom wird dann an die on_data Callback-Funktion übergeben. Nach dem Aufruf einer Haltefunktion ist die Datenreferenz nicht mehr verwendbar und gibt Fehler bei jeder Verwendung.
- **ctxt.vserver** - Der virtuelle Serverkontext.
- **ctxt.server** - Serververbindungskontext. Dieser Verarbeitungskontext kann verwendet werden, um Daten an den Server zu senden und einige verbindungsbezogene Informationen wie IP-Adresse, Quell- und Zielports abzurufen.

- **ctxt:reuse_server_connection ()** - Diese API wird verwendet, um die Serververbindung nur für andere Clientverbindungen im Serverkontext wiederverwendet werden kann. Diese API kann nur verwendet werden, wenn ein EOM-Ereignis (in ns.send () API) verwendet wird, um die Daten im Client-Kontext zu senden. Andernfalls löst die ADC-Appliance einen Fehler aus.

  Damit eine Serververbindung von anderen Clients wiederverwendet werden kann, muss diese API am Ende jeder Antwortnachricht aufgerufen werden. Wenn nach dem Aufruf dieser API mehr Daten auf dieser Serververbindung empfangen werden, wird dies als Fehler behandelt und die Serververbindung wird geschlossen. Wenn diese API nicht verwendet wird, kann die Serververbindung nur für den Client verwendet werden, für den sie geöffnet wurde. Wenn derselbe Server für eine weitere Lastenausgleichsentscheidung für diesen Client ausgewählt ist, wird dieselbe Serververbindung zum Senden der Clientdaten verwendet. Nach der Verwendung dieser API wird die Serververbindung nicht mehr an die Clientverbindung gebunden, für die sie geöffnet wurde, und kann für eine neue Lastausgleichsentscheidung für jede andere Clientverbindung wiederverwendet werden. Nach dem Aufruf dieser API ist der Serverkontext nicht mehr verwendbar und löst bei jeder Verwendung einen Fehler aus.

  Hinweis: Diese API ist in Citrix ADC 12.1 Build 49.xx und höher verfügbar.

- **ctxt:close ()** — Schließen Sie die Serververbindung, indem Sie FIN an den Server senden. Nach dem Aufruf dieser API ist der Client-Verarbeitungskontext nicht mehr verwendbar und zeigt bei jeder Verwendung einen Fehler an.

  Hinweis: Diese API ist in Citrix ADC 12.1 Build 50.xx und höher verfügbar.

vServer-Kontext

Der virtuelle Benutzerserverkontext, der über die an Callbacks übergebenen Kontexte verfügbar ist:

- **vserver:counter_increment (counter_name)** - Erhöht den Wert eines virtuellen Server-Leistungsindikators, der als Argument übergeben wird. Derzeit werden die folgenden integrierten Leistungsindikatoren unterstützt.
  - **- invalid_messages** — Anzahl der ungültigen Anforderungen/Antworten auf diesem virtuellen Server.
  - **- invalid_messages_dropped** — Anzahl der ungültigen Anforderungen/Antworten, die von diesem virtuellen Server gelöscht wurden.
- **vserver.params** - Die konfigurierten Parameter für den virtuellen Benutzerserver. Parameter bieten Konfigurierbarkeit von Erweiterungen. Der Erweiterungscode kann auf Parameter zugreifen, die in der CLI angegeben sind, um einen virtuellen Benutzerserver hinzuzufügen.

Clientverbindungskontext

Client-Verbindungsverarbeitungskontext, um verbindungsbezogene Informationen zu erhalten.

- **client.ssl** — SSL-Kontext
- **client.tcp** — TCP-Kontext
- **client.is_ssl** — True, wenn die Clientverbindung SSL-basiert ist

Serververbindungskontext

Serververbindungskontext, um verbindungsbezogene Informationen abrufen zu können.

- **server.ssl** — SSL-Kontext
- **server.tcp** — TCP-Kontext
- **server.is_ssl** — True, wenn die Serververbindung SSL-basiert ist

TCP-Kontext

TCP-Kontext arbeitet mit TCP-Protokoll.

- **tcp.srcport** — Quellport als Zahl
- **tcp.dstport** - Zielport als Zahl

IP-Kontext

Der IP-Kontext funktioniert mit IP- oder IPv6-Protokolldaten.

- **ip.src** - Quell-IP-Adresskontext.
- **ip.dst** - Ziel-IP-Adresse Kontext.

Hinweis: Diese API ist in Citrix ADC 12.1 Build 51.xx und höher verfügbar.

IP-Adresskontext

Der IP-Adresskontext funktioniert mit IP- oder IPv6-Adressdaten.

- **<address>.to_s**- Die Adresszeichenfolge in der entsprechenden ASCII-Notation.
- **<address>.to_n**- Der numerische Wert der Adresse als Zeichenfolge von Bytes in Netzwerreihenfolge (4 Bytes für IPv4 und 16 Bytes für IPv6).
- **<address>.version**- Gibt 4 für IPv4 und 6 für IPv6 zurück.
- **<address>:subnet(<prefix value>)**- Gibt die Subnetzadressenzeichenfolge nach dem Anwenden der Präfixnummer zurück.
  - Für IPv4-Adresse muss der Wert zwischen 0 und 32 liegen.
  - Bei IPv6-Adresse muss der Wert zwischen 0 und 128 liegen.
- **<address>:apply_mask(<mask string>)** - Gibt die Adresszeichenfolge nach dem Anwenden der Maskenzeichenfolge zurück. API überprüft die Version des Arguments und führt entsprechende Fehlerüberprüfung durch.

- **address>:eq(<address string>)** - Gibt true oder false zurück, je nachdem, ob das Argument äquivalent zum Adressobjekt ist. API überprüft die Version der Argumente.

Hinweis: Diese API ist in Citrix ADC 12.1 Build 51.xx und höher verfügbar.

SSL-Kontext

Der SSL-Kontext stellt Informationen zur Frontend-SSL-Verbindung bereit.

- **ssl.cert** — SSL-Zertifikatskontext. Für die Clientverbindung stellt sie Clientzertifikatkontext bereit und stellt für die Serververbindung Serverzertifikatkontext bereit.
- **ssl.version** - Eine Zahl, die die SSL-Protokollversion der aktuellen Transaktion darstellt, wie folgt:
  - - 0: The transaction is not SSL-based
  - - 0x002: The transaction is SSLv2
  - - 0x300: The transaction is SSLv3
  - - 0x301: The transaction is TLSv1
  - - 0x302: The transaction is TLSv1.1
  - - 0x303: The transaction is TLSv1.2
- **ssl.cipher_name** - SSL-Chiffriername als Zeichenfolge, wenn von einer SSL-Verbindung aufgerufen wird, andernfalls gibt NULL-Zeichenfolge.
- **ssl.cipher_bits** — Anzahl der Bits im kryptografischen Schlüssel.

SSL-Zertifikatkontext

- **Cert.version** — Versionsnummer des Zertifikats. Wenn die Verbindung nicht SSL-basiert, gibt 0 zurück.
- **Cert.valid_not_before** — Datum im Zeichenfolgenformat, vor dem das Zertifikat ungültig ist.
- **Cert.valid_not_after** — Datum im Zeichenfolgenformat, nach dem das Zertifikat nicht mehr gültig ist.
- **Cert.days_to_expire** — Anzahl der Tage, vor denen das Zertifikat gültig ist. Gibt -1 für abgelaufenes Zertifikat zurück.
- **Cert.to_pem** — Zertifikat im Binärformat.
- **cert.issuer** - Distinguished Name (DN) des Ausstellers im Zertifikat als Name-Wert-Liste. Ein Gleichheitszeichen (“=”) ist das Trennzeichen für den Namen und den Wert, und der Schrägstrich (“/”) ist das Trennzeichen, das die Name-Wert-Paare trennt.

  Es folgt ein Beispiel für den zurückgegebenen DN:
  /C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@n

- **cert.auth_keyid** — Kontext der Erweiterung des Authority Key Identifier des X.509 V3 Zertifikats.
  - **auth_keyid.exists** - TRUE, wenn das Zertifikat eine Erweiterung des Authority Key Identifier enthält.
  - **auth_keyid.issuer_name** - Distinguished Name des Ausstellers im Zertifikat als Name-Wert-Liste.
    Ein Gleichheitszeichen (“=”) ist das Trennzeichen für den Namen und den Wert, und der Schrägstrich (“/”) ist das Trennzeichen, das die Name-Wert-Paare trennt.

  Es folgt ein Beispiel:
  /C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@n
  - **auth_keyid.keyid** - KeyIdentifier Feld des Authority Key Identifier als Blob
  - **auth_keyid.cert_serialnumber** - Feld SerialNumber des Autoritätsschlüssel-Identifikators als Blob.
- **cert.pk_algorithm** - Name des öffentlichen Schlüsselalgorithmus, der vom Zertifikat verwendet wird.
- **cert.pk_size** - Größe des öffentlichen Schlüssels, der im Zertifikat verwendet wird.
- **cert.serialnumber** - Seriennummer des Client-Zertifikats. Wenn es sich um eine Nicht-SSL-Transaktion handelt oder ein Fehler im Zertifikat vorliegt, wird eine leere Zeichenfolge ausgegeben.
- **cert.signature_algorithm** - Name des kryptografischen Algorithmus, der von der Zertifizierungsstelle zum Signieren dieses Zertifikats verwendet wird.
- **cert.subject_keyid** - Betreff KeyID des Client-Zertifikats. Wenn keine Subject KeyID vorhanden ist, gibt dies ein Null-Längen-Textobjekt.
- **cert.subject** - Distinguished Name des Subjekts als Name-Wert. Ein Gleichheitszeichen (=) trennt Namen und Werte und ein Schrägstrich (/) trennt Name-Wert-Paare.

Es folgt ein Beispiel:
/C=US/O=myCompany/OU=www.mycompany.com/CN=www.mycompany.com/emailAddress=myuserid@mycom

Citrix ADC-Bibliotheken

- **ns.tcp.stream** - String ähnliche Bibliothek für die Verarbeitung von TCP-Daten als Bytestrom. Die maximale Größe der TCP-Streamdaten, mit denen diese APIs arbeiten können, beträgt 128 KB. Die Bibliotheksfunktionen ns.tcp.stream können auch im üblichen Erweiterungsobjektorientierten Stil des Aufrufs aufgerufen werden. Zum Beispiel ist data:len () identisch mit ns.tcp.stream.len (data)

  - **ns.tcp.stream.len (data)** - Gibt die Länge der Daten in Bytes zurück, ähnlich wie Luas string.len
  - **ns.tcp.stream.find (data, pattern, [init])**- Funktion ähnlich wie Luas string.find. Darüber hinaus führt es auch einen Teilabgleich am Ende der Daten durch. Bei partieller Übereinstimmung wird der Startindex zurückgegeben und der Endindex wird null.
  - **ns.tcp.stream.split (data, length)** - Teilt die Daten in zwei Chunks, der erste Chunk ist von der angegebenen Länge. Nach einer erfolgreichen Aufteilung sind die ursprünglichen Daten nicht mehr als TCP-Datenstrom nutzbar. Jeder Versuch, es auf diese Weise zu verwenden, verursacht einen Fehler.
  - **ns.tcp.stream.byte (data[, i [, j]])**- Funktion ähnlich wie Luas string.byte. Gibt die internen numerischen Codes der Zeichendaten[i], data[i+1],..., data[j]zurück.
  - n**s.tcp.stream.sub (data, i, [j])**- Funktion ähnlich wie Luas string.sub. Gibt die Teilzeichenfolge von s zurück, die bei i beginnt und bis j fortgesetzt wird.
  - **ns.tcp.stream.match (data, pattern,[init])**- Funktion ähnlich wie Luas string.match. Sucht nach der ersten *Übereinstimmung* des Musters in String s.

- **ns.send (processing_ctxt, event_name, event_data)** - Generische Funktion, um Ereignisse an einen Verarbeitungskontext zu senden. Ereignisdaten sind eine Lua-Tabelle, die beliebige Inhalte haben kann. Der Inhalt hängt vom Ereignis ab. Nachdem die ns.send () API aufgerufen wurde, ist die Datenreferenz nicht mehr verwendbar. Jeder Versuch, es zu verwenden, verursacht einen Fehler.

- **ns.pipe (src_ctxt, dest_ctxt)** - Mit einem Aufruf von pipe () API kann Erweiterungscode Quellkontext mit einem Zielkontext verbinden. Nach einem Aufruf von Pipe gehen alle Ereignisse, die vom Quellkontext an das nächste Modul in der Pipeline gesendet werden, direkt in den Zielkontext. Diese API wird normalerweise vom Modul verwendet, das den pipe () aufruft, um sich selbst aus der Pipeline zu entfernen.

- **ns.inet** — Bibliothek für Internetadressen.

  - **ns.inet.apply_mask (address_str, mask_str)** - gibt die Adresszeichenfolge nach dem Anwenden der Maskenzeichenfolge zurück.
  - **ns.inet.aton (address_str)** - Gibt den numerischen Wert der Adresse als Zeichenfolge von Bytes in Netzwerreihenfolge zurück (4 Bytes für IPv4 und 16 für IPv6).
  - **ns.inet.ntoa (byte_str)** - Konvertiert numerischen Byte-Wert als eine Zeichenfolge von Bytes in Adresszeichenfolge.
  - **ns.inet.ntohs (number)** - Konvertieren Sie die angegebene Netzwerk-Byte-Reihenfolge in Host-Byte-Reihenfolge. Wenn die Eingabe größer als 2^16 - 1 ist, wird ein Fehler ausgegeben.
  - **ns.inet.htons (number)** - Konvertiert die angegebene Host-Byte-Reihenfolge in Netzwerk-Byte-Reihenfolge. Wenn die Eingabe größer als 2^16 - 1 ist, wird ein Fehler ausgegeben.
  - **ns.inet.ntohl (number)** - Konvertiert die angegebene Netzwerk-Byte-Reihenfolge in Host-

Byte-Reihenfolge. Wenn die Eingabe größer als 2^32 - 1 ist, wird ein Fehler ausgegeben.
- **ns.inet.htonl (number)** - Konvertiert die angegebene Host-Byte-Reihenfolge in Netzwerk-Byte-Reihenfolge. Wenn die Eingabe größer als 2^32 - 1 ist, wird ein Fehler ausgegeben.
- **ns.inet.subnet (address_str, subnet_value)** — Gibt die Subnetzadressenzeichenfolge nach Anwendung des angegebenen Subnetzes zurück.

Protokollerweiterungen

October 5, 2021

Die Citrix ADC Appliances verfügen über native Unterstützung für Protokolle wie HTTP. Darüber hinaus können Sie Protokollerweiterungen verwenden, um Unterstützung für benutzerdefinierte Protokolle hinzuzufügen. Derzeit werden nur TCP-basierte benutzerdefinierte Protokolle unterstützt, z. B. das MQTT-Protokoll (Message Queuing Telemetry Transport). Für sichere Transaktionen wird auch TCP über SSL unterstützt.

Die Protokollerweiterungen auf der Citrix ADC Appliance sind Teil der hochrangigen Skriptinfrastruktur, die auf der Citrix ADC-Appliance verfügbar ist. Die Skriptsprache basiert auf der Programmiersprache Lua 5.2. Um ein benutzerdefiniertes Protokoll zu einer Citrix ADC Appliance hinzuzufügen, muss der Benutzer Erweiterungscode schreiben, um die entsprechenden Verhaltensweisen zu implementieren. Beispielsweise sind die Verhaltensweisen ns.tcp.client und ns.tcp.server auf TCP-basierte Protokolle anwendbar. Um ein Verhalten zu implementieren, implementieren Sie nur die Callbacks, die Sie anpassen möchten. Wenn Callback nicht implementiert ist, wird der Standardwert wirksam. Weitere Informationen zur Skriptsprache finden Sie unter Citrix ADC Extensions - Sprachübersicht. Weitere Informationen zu Verhaltensweisen finden Sie unter API-Referenz für Citrix ADC Extensions.

Die Citrix ADC Protokollerweiterungen können für Folgendes verwendet werden:

- Hinzufügen neuer Protokollunterstützung auf der Citrix ADC Appliance mithilfe von Erweiterungen programmgesteuert.
- Analysieren Sie den Protokollverkehr und führen Sie protokollspezifische Message Based Load Balancing (MBLB) durch.
- Konfigurieren Sie die Persistenz für den Lastausgleich.

Protokollerweiterungen - Architektur

October 5, 2021

Um Erweiterbarkeit auf Traffic-Ebene zu erreichen, wird die Datenverkehrsverarbeitung auf einer Citrix ADC Appliance als Pipeline von separaten Verarbeitungsmodulen bereitgestellt. Der Verkehr fließt

durch sie, während er ihn vom Ein- bis zum Ausstieg verarbeitet. Diese Module in der Pipeline folgen einem Shared Nothing Modell. Die Nachrichtenübergabe wird verwendet, um die Verkehrsdaten von einem Modul in der Pipeline an das nächste Modul zu senden.

Bestimmte Punkte in der Datenverarbeitungspipeline werden erweiterbar, sodass Sie Code hinzufügen können, um das Verhalten von Citrix ADC anzupassen.

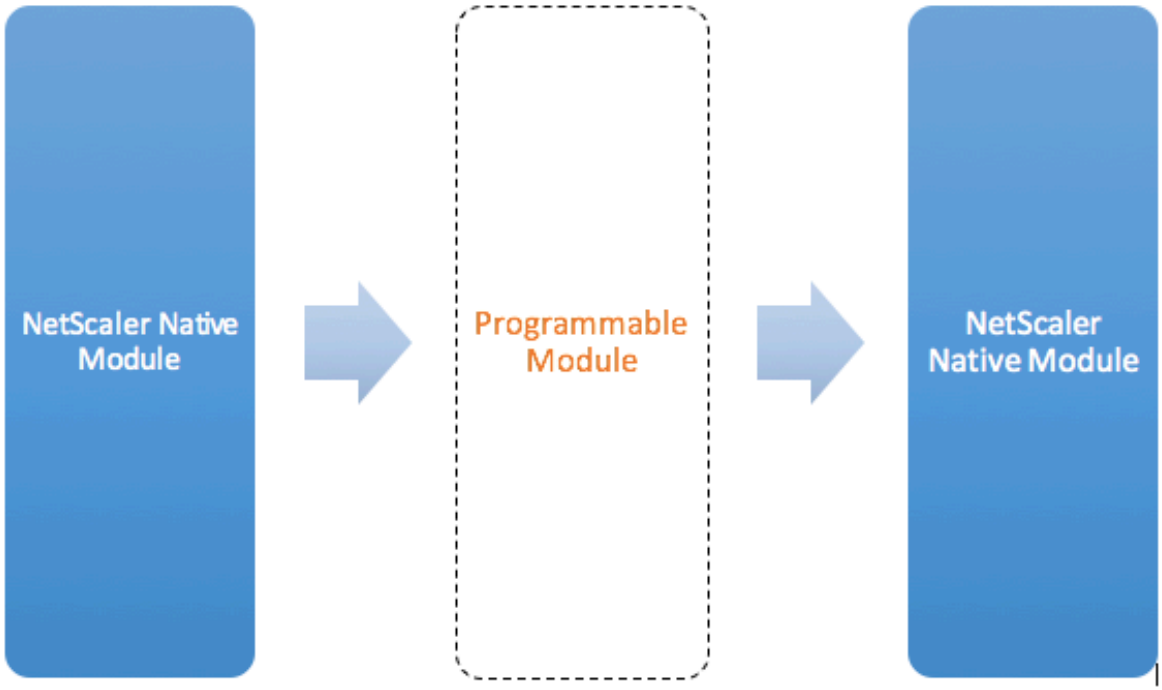


Figure: A Programmable Module In the Traffic Pipeline

Standardmäßig umgeht der Datenverkehr ein programmierbares Modul, dem Sie keinen Code hinzufügen.

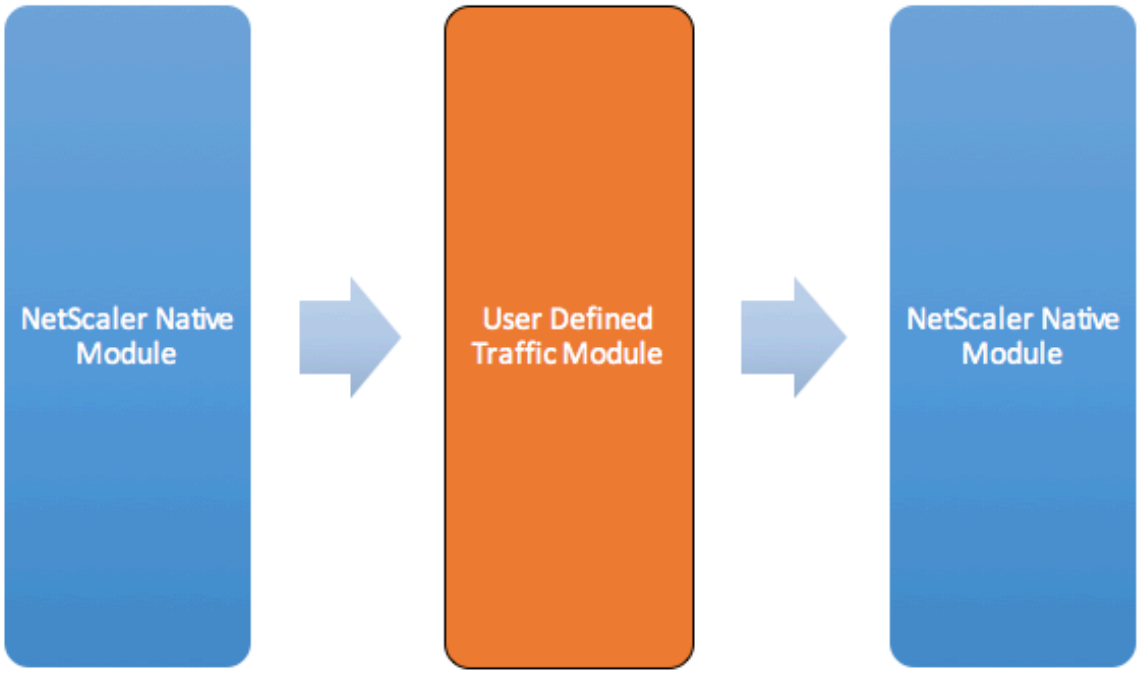


Figure: User Defined Traffic Module

Verhaltensweisen

Die programmierbaren Schnittstellen zur Anpassung der Traffic-Handling werden als Verhaltensweisen bezeichnet. Verhaltensweisen sind im Grunde eine Formalisierung gängiger programmierbarer Muster, die auf einer Citrix ADC Appliance verfügbar sind. Die Verhaltensweisen bestehen aus einem vordefinierten Satz von Ereignis-Callback-Funktionen. Sie können ein Verhalten implementieren, indem Sie Callback-Funktionen bereitstellen, die dem Verhalten entsprechen.

Das TCP-Clientverhalten besteht beispielsweise aus einer Callback-Funktion (on_data), die TCP-Client-Datenstream-Ereignisse verarbeitet. Um Message Based Load Balancing (MBLB) für ein TCP-basiertes Protokoll zu implementieren, können Sie Code für diese Callback-Funktion hinzufügen, um den TCP-Datenstrom vom Client zu verarbeiten und den Bytestream in Protokollmeldungen zu analysieren.

Kontext:

Die Callback-Funktionen in einem Verhalten werden mit einem Kontext aufgerufen, der der Verarbeitungsmodulstatus ist. Der Kontext ist die Instanz des Verarbeitungsmoduls. Beispielsweise werden die TCP-Clientverhalten Callbacks mit unterschiedlichen Kontexten für verschiedene Client-TCP-Verbindungen aufgerufen.

Nutzlast:

Zusätzlich zum Kontext können die Verhaltensrückrufe andere Argumente haben. Normalerweise werden die restlichen Argumente als Payload übergeben, was die Sammlung aller Argumente ist.

So können die programmierbaren Verarbeitungsmodulinstanzen als eine Kombination aus Instanzstatus plus Ereignisrückruffunktionen gesehen werden, dh dem Kontext plus Verhalten. Und der Verkehr fließt durch die Pipeline als Ereignisnutzlast.

Informationen zu Citrix ADC API-Erweiterungen finden Sie unter Referenz zur Citrix ADC-Erweiterung.

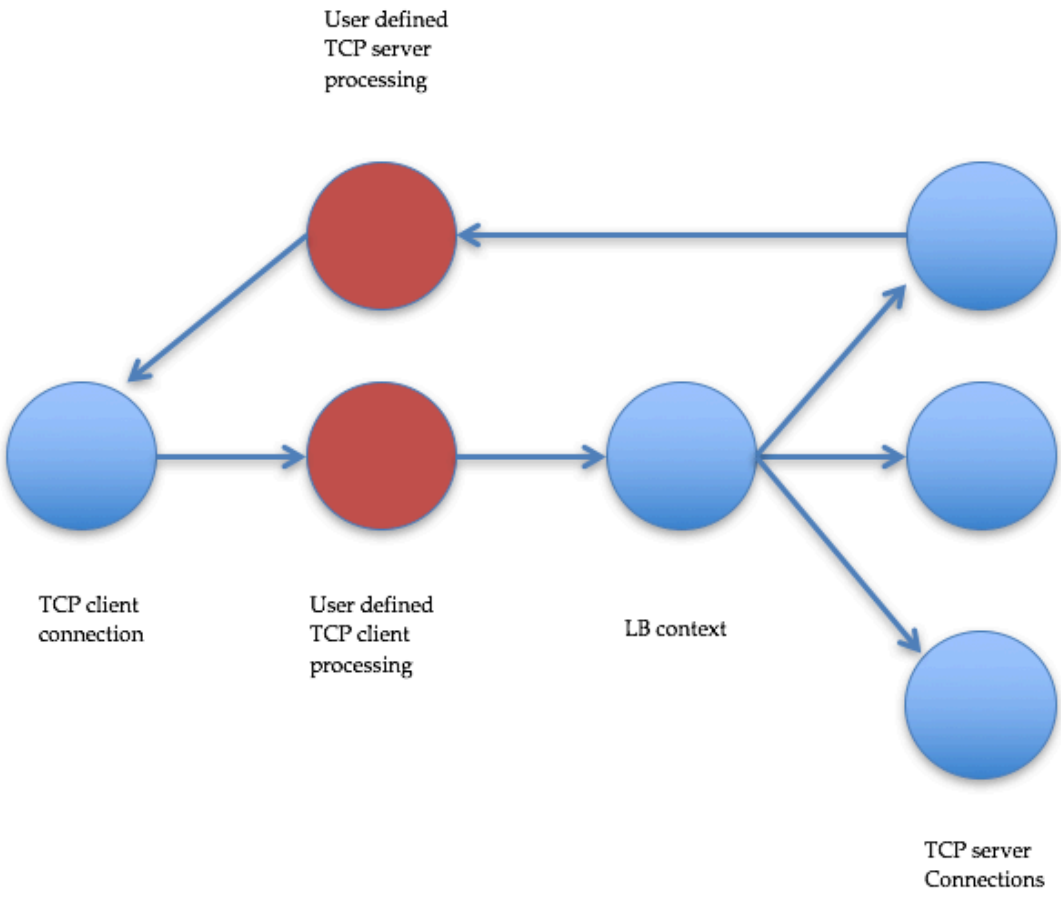
Das folgende Code-Snippet zeigt eine benutzerdefinierte Funktion zum Behandeln von TCP-Clientdatenstromereignissen. Der Kontext und die Nutzlast werden durch Citrix ADC Code an die Funktion übergeben. Dieser Code leitet die bei jedem Aufruf empfangenen TCP-Daten einfach an den nächsten Verarbeitungsmodulkontext in der Pipeline weiter. In diesem Fall ist das nächste Modul der Load Balancing (LB) -Kontext, bei dem es sich um ein natives Citrix ADC Modul handelt.

```
function client.on_data(ctxt, payload)
    ns.send(ctxt.output, "DATA", {
 data = payload.data }
 )
end
<!--NeedCopy-->
```

Protokollerweiterungen - Verkehrspipeline für benutzerdefinierte TCP-Client- und Serververhalten

October 5, 2021

Die folgende Abbildung zeigt die Beispielprotokollerweiterung - Verkehrspipeline für benutzerdefinierte TCP-Client- und Serververhalten



Traffic Pipeline For User Defined TCP Client And Server Behaviors

Hinzufügen eines benutzerdefinierten Protokolls mithilfe von Protokollerweiterungen

Die Befehlszeilenschnittstellenbefehle (CLI) für das benutzerdefinierte Protokoll verwenden das Schlüsselwort user, um die benutzerdefinierte Natur der zugrunde liegenden Konfigurationsobjekte zu signalisieren. Mit Hilfe von Erweiterungscode können Sie dem System ein neues Benutzerprotokoll hinzufügen und virtuelle Benutzerserver für benutzerdefinierte Protokolle hinzufügen. Die virtuellen Server des Benutzers sind wiederum durch Einstellen von Parametern konfigurierbar. Konfigurierte Werte für virtuelle Serverparameter sind im Erweiterungscode verfügbar.

Das folgende Beispiel veranschaulicht den Benutzerfluss zum Hinzufügen von Unterstützung für ein neues Protokoll. In diesem Beispiel wird dem System die Unterstützung des MQTT-Protokolls hinzugefügt. MQTT ist ein Internet of Things -Konnektivitätsprotokoll von Maschine zu Maschine. Es ist ein leichter Publish/Subscribe Messaging-Transport. Dieses Protokoll ist nützlich für Verbindungen mit Remotestandorten und verwendet Client- und Brokertools, um Nachrichten an Abonnenten zu veröffentlichen.

1. Importieren Sie die Implementierungsdatei für die MQTT-Protokollerweiterung in das Citrix ADC-System. Die Code-Auflistung für mqtt.lua ist unten angegeben. Im folgenden Beispiel wird die auf einem Webserver gehostete MQTT-Erweiterungsdatei importiert.

   ```
   import extension http://10.217.24.48/extensions/mqtt.lua mqtt_code
   ```

2. Fügen Sie dem System mithilfe der Erweiterung ein neues TCP-basiertes Benutzerprotokoll hinzu.

   ```
   add user protocol MQTT -transport TCP -extension mqtt_code
   ```

3. Fügen Sie einen Benutzer Load Balancing vserver hinzu und binden Sie Back-End-Dienste an ihn.

   ```
   add service mqtt_svr1 10.217.24.48 USER_TCP 1501
   add service mqtt_svr2 10.217.24.48 USER_TCP 1502
   add lb vserver mqtt_lb USER_TCP  - lbmethod USER_TOKEN
   bind lb vserver mqtt_lb mqtt_svr1
   bind lb vserver mqtt_lb mqtt_svr2
   <!--NeedCopy-->
   ```

4. Fügen Sie einen Benutzer vserver für das neu hinzugefügte Protokoll hinzu. Setzen Sie die defaultlb auf den oben konfigurierten LB-vserver.

   ```
   add user vserver mqtt_vs MQTT 10.217.24.28 8765 -defaultLb mqtt_lb
   ```

5. Aktivieren Sie optional die MQTT-Sitzungspersistenz basierend auf ClientID und legen Sie den Persistenztyp auf USERSESSION fest.

   ```
   set lb vserver mqtt_lb -persistenceType USERSESSION
   ```

Protokollerweiterungen - Anwendungsfälle

October 5, 2021

Protokollerweiterungen können für die folgenden Anwendungsfälle verwendet werden.

- Nachrichtenbasierter Lastausgleich (MBLB)
- Streaming
- Token basierter Lastausgleich
- Persistenz des Lastausgleichs
- TCP-Verbindung basierter Lastausgleich
- Inhaltsbasierter Lastausgleich
- SSL

- Datenverkehr ändern
- Datenverkehr zum Client oder Server ableiten
- Prozessdaten zum Verbindungsaufbau

Nachrichtenbasierter Lastausgleich

Protokollerweiterungen unterstützen Message Based Load Balancing (MBLB), mit dem jedes Protokoll auf einer Citrix ADC Appliance analysiert und die Protokollmeldungen, die auf einer Clientverbindung eingehen, Lastverteilung erfolgt, d. h. die Nachrichten über mehrere Serververbindungen. MBLB wird durch Benutzercode erreicht, der den Client-TCP-Datenstrom analysiert.

Der TCP-Datenstrom wird an die on_data Callbacks für Client- und Serververhalten übergeben. Der TCP-Datenstrom steht den Erweiterungsfunktionen über eine Lua-String-ähnliche Schnittstelle zur Verfügung. Sie können eine API ähnlich der Lua-String-API verwenden, um den TCP-Datenstrom zu analysieren.

Zu den nützlichen APIs gehören:

```
data:len()
```

```
data:find()
```

```
data:byte()
```

```
data:sub()
```

```
data:split()
```

Sobald der TCP-Datenstrom in eine Protokollnachricht analysiert wurde, erreicht der Benutzercode den Lastausgleich, indem er die Protokollnachricht einfach an den nächsten Kontext sendet, der aus dem Kontext verfügbar ist, der an den on_data Callback für den Client übergeben wird.

Die ns.send () API wird verwendet, um Nachrichten an andere Verarbeitungsmodule zu senden. Zusätzlich zum Zielkontext verwendet die send-API den Ereignisnamen und die optionale Nutzlast als Argumente. Es gibt Eins-zu-Eins-Korrespondenz zwischen dem Ereignisnamen und den Callback-Funktionsnamen für die Verhaltensweisen. Die Callbacks für Ereignisse werden mit on_<event_name> aufgerufen. Die Callback-Namen verwenden nur Kleinbuchstaben.

Beispielsweise sind der TCP-Client und der Server on_data Callbacks benutzerdefinierte Handler für Ereignisse mit dem Namen DATA. Für das Senden der gesamten Protokollnachricht in einem Sendeaufruf wird das EOM-Ereignis verwendet. EOM, die für Ende der Nachricht steht, bedeutet das Ende der Protokollnachricht an den LB-Kontext Downstream, so dass eine neue Lastausgleichsentscheidung für Daten getroffen wird, die dieser Nachricht folgen.

Der Erweiterungscode erhält manchmal nicht die gesamte Protokollnachricht im on_data Ereignis. In einem solchen Fall können die Daten mithilfe der ctxt:hold () API gespeichert werden. Die Hold-API ist sowohl für TCP-Client- als auch für Server-Callback-Kontexte verfügbar. Wenn hold with data

aufgerufen wird, werden die Daten im Kontext gespeichert. Wenn mehr Daten im selben Kontext empfangen werden, werden die neu empfangenen Daten an die zuvor gespeicherten Daten angehängt und die on_data Callback-Funktion mit den kombinierten Daten erneut aufgerufen.

Hinweis: Die verwendete Load Balancing-Methode hängt von der Konfiguration des virtuellen Lastausgleichsservers ab, der dem Lastenausgleichskontext entspricht.

Der folgende Codeausschnitt zeigt die Verwendung der Sende-API zum Senden der analysierten Protokollnachricht.

Beispiel:

```
    function client.on_data(ctxt, payload)
        --
        -- code to parse payload.data into protocol message comes here
        --
        -- sending the message to lb
        ns.send(ctxt.output, ”EOM”, {
 data = message }
 )
    end -- client.on_data

    function server.on_data(ctxt, payload)
        --
        -- code to parse payload.data into protocol message comes here
        --
        -- sending the message to client
        ns.send(ctxt.output, ”EOM”, {
 data = message }
 )

    end -- server.on_data
<!--NeedCopy-->
```

Streaming

In einigen Szenarien ist das Halten des TCP-Datenstroms möglicherweise nicht erforderlich, bis die gesamte Protokollnachricht erfasst wird. In der Tat wird es nicht empfohlen, es sei denn, es ist erforderlich. Das Halten der Daten erhöht die Speicherauslastung auf der Citrix ADC Appliance und kann die Appliance für DDoS-Angriffe anfällig machen, indem der Speicher auf der Citrix ADC-Appliance mit unvollständigen Protokollmeldungen an vielen Verbindungen belegt wird.

Benutzer können das Streaming von TCP-Daten in den Extension-Callback-Handlern mithilfe der Send-

API erreichen. Anstatt die Daten zu halten, bis die gesamte Nachricht erfasst ist, können Daten in Blöcken gesendet werden. Das Senden von Daten an ctxt.output mithilfe des DATA -Ereignisses sendet eine partielle Protokollmeldung. Es kann durch weitere DATA Ereignisse gefolgt werden. Ein EOM-Ereignis muss gesendet werden, um das Ende der Protokollnachricht zu markieren. Der Lastausgleichskontext nachgeschaltete Lastenausgleich entscheidet über die ersten empfangenen Daten. Nach Erhalt der EOM-Nachricht wird eine neue Lastausgleichsentscheidung getroffen.

Um Protokollnachrichtendaten zu streamen, senden Sie mehrere DATA Ereignisse gefolgt von einem EOM-Ereignis. Die zusammenhängenden DATA-Ereignisse und das folgende EOM-Ereignis werden an dieselbe Serververbindung gesendet, die durch Lastausgleichsentscheidung für das erste DATA-Ereignis in der Sequenz ausgewählt wurde.

Für einen Send to Client-Kontext sind EOM und DATA Ereignisse effektiv identisch, da es keine spezielle Behandlung durch den Clientkontext nachgeschaltet für EOM-Ereignisse gibt.

Token basierter Lastausgleich

Bei nativ unterstützten Protokollen unterstützt eine Citrix ADC Appliance eine tokenbasierte Load Balancing-Methode, die PI-Ausdrücke zum Erstellen des Token verwendet. Bei Erweiterungen ist das Protokoll nicht im Voraus bekannt, so dass PI-Ausdrücke nicht verwendet werden können. Für den token basierten Lastenausgleich müssen Sie den standardmäßigen virtuellen Lastausgleichsserver so festlegen, dass die USER_TOKEN Lastausgleichsmethode verwendet wird, und den Tokenwert aus dem Erweiterungscode angeben, indem Sie die Sende-API mit einem user_token Feld aufrufen. Wenn der Tokenwert von der Sende-API gesendet wird und die USER_TOKEN Lastausgleichsmethode auf dem virtuellen Standardserver für Lastausgleich konfiguriert ist, wird die Entscheidung für den Lastausgleich getroffen, indem ein Hash basierend auf dem Tokenwert berechnet wird. Die maximale Länge des Tokenwerts beträgt 64 Byte.

```
add lb vserver v\\_mqttlb USER\\_TCP -lbMethod USER\\_TOKEN
```

Der Codeausschnitt im folgenden Beispiel verwendet eine Sende-API, um einen LB-Tokenwert zu senden.

Beispiel:

```
1          -- send the message to lb
2
3
4
5
6          -- user_token is set to do LB based on clientID
7
8
```



```
9
10
11          ns.send(ctxt.output, ”EOM”, {
12   data = message,
13
14                                      user_token = token_info }
15   )
16  <!--NeedCopy-->
```

Persistenz des Lastausgleichs

Die Persistenz des Lastausgleichs hängt eng mit dem token basierten Lastausgleich zusammen. Benutzer müssen in der Lage sein, den Wert der Persistenzsitzung programmgesteuert zu berechnen und ihn für die Persistenz des Lastenausgleichs zu verwenden. Die Sende-API wird verwendet, um Persistenzparameter zu senden. Um die Persistenz des Lastenausgleichs zu verwenden, müssen Sie den Persistenztyp USERSESSION auf dem virtuellen Standardserver für Lastenausgleich festlegen und einen Persistenzparameter aus dem Erweiterungscode bereitstellen, indem Sie die Sende-API mit einem user_session Feld aufrufen. Die maximale Länge des Persistenz-Parameterwerts beträgt 64 Byte.

Wenn Sie mehrere Persistenzarten für ein benutzerdefiniertes Protokoll benötigen, müssen Sie Benutzerpersistenztypen definieren und konfigurieren. Die Namen der Parameter, die zum Konfigurieren der virtuellen Server verwendet werden, werden vom Protokollimplementierer festgelegt. Der konfigurierte Wert eines Parameters ist auch für den Erweiterungscode verfügbar.

Die folgende CLI und Codeausschnitt zeigen die Verwendung einer Sende-API zur Unterstützung der Persistenz des Lastenausgleichs. Die Codeauflistung im Abschnitt Codeauflistung für mqtt.lua veranschaulicht auch die Verwendung des Feldes user_session.

Für die Persistenz müssen Sie den Persistenztyp USERSESSION auf dem virtuellen Lastausgleichsserver angeben und den Wert user_session von der ns.send API übergeben.

```
add lb vserver v\\_mqttlb USER\\_TCP -persistencetype USERSESSION
```

Senden Sie die MQTT-Nachricht an den Load Balancer, wobei das Feld user_session in der Payload auf ClientID festgelegt ist.

Beispiel:

```
1  -- send the data so far to lb
2
3  -- user_session is set to clientID as well (it will be used to persist
       session)
4
```



```
ns.send(ctxt.output,  “DATA” , {
 data = data, user_session = clientID }
 )
<!--NeedCopy-->
```

TCP-Verbindung basierter Lastausgleich

Für einige Protokolle wird MBLB möglicherweise nicht benötigt. Stattdessen benötigen Sie möglicherweise auf TCP-Verbindung basierenden Lastenausgleich. Beispielsweise muss das MQTT-Protokoll den anfänglichen Teil des TCP-Streams analysieren, um das Token für den Lastenausgleich zu bestimmen. Und alle MQTT-Nachrichten auf derselben TCP-Verbindung müssen an dieselbe Serververbindung gesendet werden.

TCP-Verbindung basierter Lastausgleich kann erreicht werden, indem die Send-API nur mit DATA Ereignissen verwendet wird und keine EOM gesendet wird. Auf diese Weise basiert der nachgeschaltete Lastausgleichskontext die Lastenausgleichsentscheidung auf den zuerst empfangenen Daten und sendet alle nachfolgenden Daten an dieselbe Serververbindung, die durch die Lastausgleichsentscheidung ausgewählt wurde.

Außerdem erfordern einige Anwendungsfälle möglicherweise die Möglichkeit, die Erweiterungsbehandlung zu umgehen, nachdem die Entscheidung für den Lastausgleich getroffen wurde. Die Umgehung der Erweiterungsaufrufe führt zu einer besseren Leistung, da der Datenverkehr rein durch systemeigenen Code verarbeitet wird. Umgehung kann mit der ns.pipe () API erfolgen. Ein Aufruf des pipe-API-Erweiterungscodes kann den Eingabekontext mit einem Ausgabekontext verbinden. Nach dem Aufruf von pipe () gehen alle Ereignisse, die aus dem Eingabekontext kommen, direkt in den Ausgabekontext. Effektiv wird das Modul, von dem der pipe () -Aufruf ausgeführt wird, aus der Pipeline entfernt.

Das folgende Code-Snippet zeigt Streaming und die Verwendung der pipe () API, um ein Modul zu umgehen. Die Codeauflistung im Abschnitt Codeauflistung für mqtt.lua veranschaulicht auch, wie man Streaming und die Verwendung der pipe () API verwendet, um das Modul für den Rest des Datenverkehrs auf der Verbindung zu Bypass.

Beispiel:

```
        -- send the data so far to lb
        ns.send(ctxt.output, ”DATA”, {
 data = data,
                                      user_token = clientID }
 )
        -- pipe the subsequent traffic to the lb - to bypass the client
            on_data handler
```



```
7          ns.pipe(ctxt.input, ctxt.output)
8  <!--NeedCopy-->
```

Inhaltsbasierter Lastausgleich

Bei nativen Protokollen wird eine Funktion für Protokollerweiterungen unterstützt, die Content Switching ähnelt. Mit dieser Funktion können Sie die Daten nicht an den Standardlastausgleich senden, sondern an den ausgewählten Load Balancer senden.

Das Content Switching für Protokollerweiterungen wird mit der API ctxt:lb_connect (<lbname>) erreicht. Diese API ist für den TCP-Clientkontext verfügbar. Mit dieser API kann der Erweiterungscode einen Lastausgleichskontext abrufen, der einem bereits konfigurierten virtuellen Lastausgleichsserver entspricht. Sie können dann die Send-API mit dem so erhaltenen Load Balancing-Kontext verwenden.

Der lb-Kontext kann manchmal NULL sein:

- Virtueller Server ist nicht vorhanden
- Virtueller Server ist nicht vom Benutzerprotokolltyp
- Der Status des virtuellen Servers ist nicht UP
- Virtueller Server ist ein virtueller Benutzerserver, kein Lastenausgleich virtueller Server

Wenn Sie den virtuellen Zielserver für Lastenausgleich entfernen, wenn er verwendet wird, werden alle Verbindungen zurückgesetzt, die diesem virtuellen Lastausgleichsserver zugeordnet sind.

Das folgende Code-Snippet zeigt die Verwendung der lb_connect () API. Der Code ordnet die Client-ID zum Lastenausgleich virtueller Servernamen (lbname) mithilfe der Lua-Tabelle lb_map zu und ruft dann den LB-Kontext für lbname mit lb_connect () ab. Und schließlich sendet an den LB-Kontext mit Send-API.

```
1     local lb_map = {
2
3        ["client1*"] = "lb_1",
4        ["client2*"] = "lb_2",
5        ["client3*"] = "lb_3",
6        ["client4*"] = "lb_4"
7      }
8
9
10    -- map the clientID to the corresponding LB vserver and connect to
         it
11    for client_pattern, lbname in pairs(lb_map) do
12       local match_idx = string.find(clientID, client_pattern)
```



```
13         if (match_idx == 1) then
14        lb_ctxt = ctxt:lb_connect(lbname)
15        if (lb_ctxt == nil) then
16           error("Failed to connect to LB vserver: " .. lbname)
17        end
18        break
19         end
20     end
21     if (lb_ctxt == nil) then
22     -- If lb context is NULL, the user can raise an error or send data
          to default LB
23        error("Failed to map LB vserver for client: " .. clientID)
24     end
25 -- send the data so far to lb
26 ns.send(lb_ctxt, "DATA", {
27  data = data }
28
29 <!--NeedCopy-->
```

SSL

SSL für Protokolle, die Erweiterungen verwenden, wird ähnlich wie SSL für native Protokolle unterstützt. Mit demselben Parsing-Code zum Erstellen benutzerdefinierter Protokolle können Sie eine Protokollinstanz über TCP oder über SSL erstellen, die dann zur Konfiguration der virtuellen Server verwendet werden kann. Ebenso können Sie Benutzerdienste über TCP oder SSL hinzufügen.

Weitere Informationen finden Sie unter Konfigurieren von SSL-Offloading für MQTT und Konfigurieren von SSL-Offloading für MQTT mit End-to-End-Verschlüsselung.

Serververbindungs-Multiplexing

Manchmal sendet der Client jeweils eine Anforderung und sendet die nächste Anforderung erst, nachdem die Antwort für die erste Anforderung vom Server empfangen wurde. In einem solchen Fall kann die Serververbindung für andere Clientverbindungen und für die nächste Nachricht auf derselben Verbindung wiederverwendet werden, nachdem die Antwort an den Client gesendet wurde. Um die Wiederverwendung der Serververbindung durch andere Clientverbindungen zu ermöglichen, müssen Sie die API ctxt: reuse_server_connection () im serverseitigen Kontext verwenden.

Hinweis: Diese API ist in Citrix ADC 12.1 Build 49.xx und höher verfügbar.

Datenverkehr ändern

Um Daten in der Anforderung oder Antwort zu ändern, müssen Sie das native Rewrite-Feature verwenden, das einen erweiterten Richtlinien-PI-Ausdruck verwendet. Da Sie PI-Ausdrücke in Erweiterungen nicht verwenden können, können Sie die folgenden APIs verwenden, um TCP-Streamdaten zu ändern.

```
data:replace(offset, length, new_string)
data:insert(offset, new_string)
data:delete(offset, length)
data:gsub(pattern, replace [,n]))
```

Das folgende Code-Snippet zeigt die Verwendung von replace () API.

```
-- Get the offset of the pattern, we want to replace
   local old_pattern =  "pattern to repalace"
local old_pattern_length = old_pattern:len()
   local pat_off, pat_end = data:find(old_pattern)
   -- pattern is not present
if (not pat_off) then
    goto send_data
   end
  -- If the data we want to modify is not completely present, then
  -- wait for more data
  if (not pat_end) then
        ctxt:hold(data)
        data = nil
     goto done
  end
data:replace(pat_off, old_pattern_length,  "new pattern" )
::send_data::
ns.send(ctxt.output,  "EOM" , {
 data = data }
 )
::done::
```

Das folgende Code-Snippet zeigt die Verwendung von insert () API.

```
data:insert(5,  "pattern to insert" )
```

Das folgende Code-Snippet zeigt die Verwendung von insert () API, wenn wir nach oder vor einem Muster einfügen möchten:


```
-- Get the offset of the pattern, after or before which we want to
    insert
   local pattern =  “pattern after/before which we need to insert”
local pattern_length = pattern:len()
   local pat_off, pat_end = data:find(pattern)
-- pattern is not present
   if (not pat_off) then
    goto send_data
   end
  -- If the pattern after which we want to insert is not
  -- completely present, then wait for more data
  if (not pat_end) then
        ctxt:hold(data)
        data = nil
     goto done
  end
-- Insert after the pattern
data:insert(pat_end + 1,  “pattern to insert” )
   -- Insert before the pattern
data:insert(pat_off,  “pattern to insert” )
::send_data::
    ns.send(ctxt.output,  “EOM” , {
 data = data }
 )
::done::
```

Das folgende Code-Snippet zeigt die Verwendung von delete () API.

```
-- Get the offset of the pattern, we want to delete
   local delete_pattern =  “pattern to delete”
local delete_pattern_length = delete_pattern:len()
   local pat_off, pat_end = data:find(old_pattern)
   -- pattern is not present
if (not pat_off) then
          goto send_data
   end
  -- If the data we want to delete is not completely present,
  -- then wait for more data
  if (not pat_end) then
        ctxt:hold(data)
        data = nil
    goto done
```



```
  end
data:delete(pat_off, delete_pattern_length)
::send_data::
ns.send(ctxt.output,  “EOM” , {
 data = data }
 )
::done::
```

Das folgende Code-Snippet zeigt die Verwendung von gsub () API.

```
    -- Replace all the instances of the pattern with the new string
data:gsub( “old pattern” ,  “new string” )
-- Replace only 2 instances of  “old pattern”
data:gsub( “old pattern” ,  “new string” , 2)
-- Insert new_string before all instances of  “http”
data:gsub( “input data” ,  “(http)” ,  “new_string%1” )
-- Insert new_string after all instances of  “http”
data:gsub( “input data” ,  “(http)” ,  “%1new_string” )
-- Insert new_string before only 2 instances of  “http”
data:gsub( “input data” ,  “(http)” ,  “new_string%1” , 2)
```

Hinweis: Diese API ist in Citrix ADC 12.1 Build 50.xx und höher verfügbar.

Datenverkehr zum Client oder Server ableiten

Sie können die ns.send() API verwenden, um Daten, die aus dem Erweiterungscode stammen, an einen Client und einen Back-End-Server zu senden. Um eine Antwort direkt mit einem Client zu senden oder zu empfangen, müssen Sie ctxt.client als Ziel verwenden. Um eine Antwort direkt mit einem Back-End-Server aus dem Serverkontext zu senden oder zu empfangen, müssen Sie ctxt.server als Ziel verwenden. Die Daten in der Nutzlast können ein TCP-Stream-Daten oder eine Lua-Zeichenfolge sein.

Um die Datenverkehrsverarbeitung für eine Verbindung zu stoppen, können Sie die ctxt:close() -API entweder vom Client- oder vom Serverkontext aus verwenden. Diese API schließt die clientseitige Verbindung oder alle damit verknüpften Serververbindungen.

Wenn Sie die ctxt:close() API aufrufen, sendet der Erweiterungscode TCP-FIN-Paket an die Client- und Serververbindungen. Wenn mehr Daten vom Client oder Server auf dieser Verbindung empfangen werden, setzt die Appliance die Verbindung zurück.

Das folgende Codeausschnitt zeigt die Verwendung von ctxt.client und ctxt:close () APIs.


```
    -- If the input packet is not MQTT CONNECT type, then
-- send some error response to the client.
function client.on_data(ctxt, payload)
    local data = payload.data
    local offset = 1
    local msg_type = 0
    local error_response =  "Missing MQTT Connect packet."
    byte = data:byte(offset)
msg_type = bit32.rshift(byte, 4)
if (msg_type ~= 1) then
-- Send the error response
   ns.send(ctxt.client,  "DATA" , {
 data = error_response }
 )
-- Since error response has been sent, so now close the connection
    ctxt:close()
end
```

Der folgende Codeausschnitt zeigt das Beispiel, wenn der Benutzer die Daten in den normalen Verkehrsfluss injizieren kann.

```
-- After sending request, send some log message to the server.
function client.on_data(ctxt, payload)
local data = payload.data
local log_message =  "client id :  "..data:sub(3, 7).."  user name :  "
    data:sub(9, 15)
-- Send the request we get from the client to backend server
ns.send(ctxt.output,  "DATA" , {
 data = data }
 )
After sending the request, also send the log message
ns.send(ctxt.output,  "DATA" , {
 data = log_message"  }
 )
end
```

Der folgende Codeausschnitt zeigt die Verwendung der ctxt.to_server API.

```
-- If the HTTP response status message is  "Not Found" ,
-- then send another request to the server.
function server.on_data(ctxt, payload)
```



```
    local data = payload.data
    local request  "GET /default.html HTTP/1.1\r\n\r\n" ss
    local start, end = data:find( "Not Found" )
    if (start) then
    -- Send the another request to server
        ns.send(ctxt.server,  "DATA" , {
 data = request }
 )
end
```

Hinweis: Diese API ist in Citrix ADC 12.1 Build 50.xx und höher verfügbar.

Datenverarbeitung am Verbindungsaufbau

Es kann einen Anwendungsfall geben, in dem Sie einige Daten an die Verbindungseinrichtung senden möchten (wenn die endgültige ACK empfangen wird). Beispielsweise können Sie im Proxyprotokoll die Quell- und Ziel-IP-Adressen und -Ports des Clients an den Back-End-Server beim Verbindungsaufbau senden. In diesem Fall können Sie client.init () Callback-Handler verwenden, um die Daten über die Verbindungseinrichtung zu senden.

Der folgende Codeausschnitt zeigt die Verwendung von client.init() Callback:

```
-- Send a request to the next processing context
-- on the connection establishment.
function client.init(ctxt)
   local request  "PROXY TCP4"  + ctxt.client.ip.src.to_s +  "  " +
      ctxt.client.ip.dst.to_s +  "  " + ctxt.client.tcp.srcport +  "  "
       +     ctxt.client.tcp.dstport
-- Send the another request to server
   ns.send(ctxt.output,  "DATA" , {
 data = request }
 )
  end
```

Hinweis: Diese API ist in Citrix ADC 13.0 Build xx.xx und höher verfügbar.

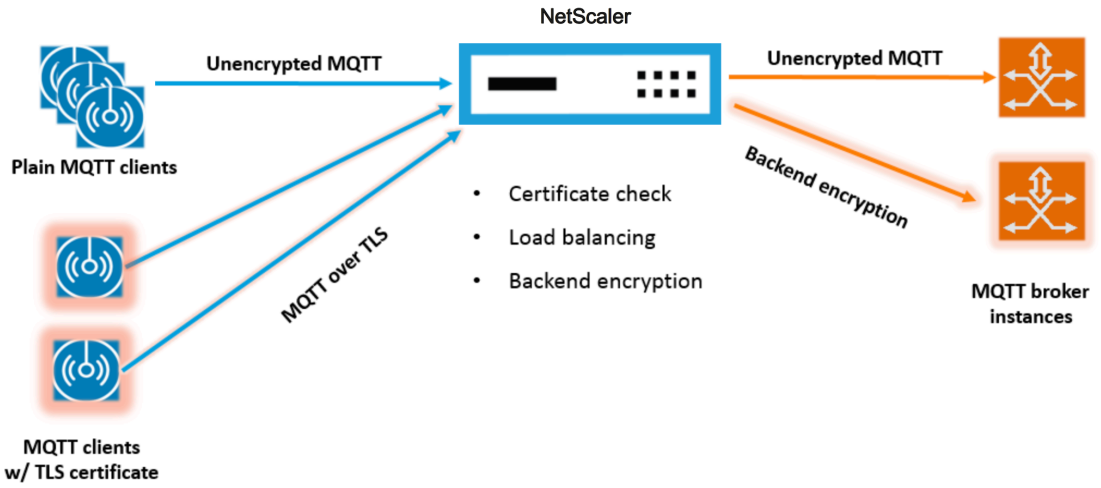
Lernprogramm — Hinzufügen des MQTT-Protokolls zur Citrix ADC Appliance mit Protokollerweiterungen

October 5, 2021

Die Befehlszeilenschnittstellenbefehle (CLI) für das benutzerdefinierte Protokoll verwenden das Schlüsselwort user, um die benutzerdefinierte Natur der zugrunde liegenden Konfigurationsobjekte zu signalisieren. Mit Hilfe von Erweiterungscode können Sie dem System ein neues Benutzerprotokoll hinzufügen und virtuelle Benutzerserver für benutzerdefinierte Protokolle hinzufügen. Die virtuellen Server des Benutzers sind wiederum durch Einstellen von Parametern konfigurierbar. Konfigurierte Werte für virtuelle Serverparameter sind im Erweiterungscode verfügbar.

Das MQTT-Protokoll wird zur Veranschaulichung verwendet.

Das folgende Diagramm veranschaulicht eine Citrix ADC Appliance sowie MQTT-Client- und Broker-tools.



Code-Auflistung für mqtt.lua

October 5, 2021

Die nachstehende Code-Auflistung, mqtt.lua, enthält den Code zum Implementieren des MQTT-Protokolls auf Citrix ADC unter Verwendung von Protokollerweiterungen. Der Code hat nur die TCP-Clientdaten-Callback-Funktion definiert - client.on_data (). Für Serverdaten wird keine Callback-Funktion hinzugefügt, und der Server zum Client nimmt den schnellen nativen Pfad. Bei Clientdaten analysiert der Code die CONNECT MQTT Protokollmeldung und extrahiert die ClientID. Es verwendet dann den ClientID für user_token Wert, der verwendet wird, um den gesamten Clientdatenverkehr für die Verbindung basierend auf der ClientID zu laden, indem die LB-Methode für den LB-vserver als USER_TOKEN festgelegt wird. Es verwendet die ClientID auch für user_session Wert, der für die LB-Persistenz verwendet werden kann, indem Persistenztyp für den LB-vserver als USERSESSION festgelegt wird. Der Code verwendet die ns.send (), um LB zu tun und die Anfangsdaten zu senden. Es verwendet die ns.pipe () API, um den Rest des Clientdatenverkehrs direkt an die Serververbindung zu senden, wobei Aufrufe an den Extension-Callback-Handler umgangen werden.


```
--[[

  MQTT event handler for TCP client data

    ctxt - TCP client side App processing context.

    data - TCP Data stream received.

    - parse the client ID from the connect message - the first message
       should be connect

    - send the data to LB with ClientID as user token and session

    - pipe the subsequent data to LB directly. This way the subsequent
       MQTT traffic will

      bypass the tcp client on_data handler

    - if a parse error is seen, throw an error so the connection is
       reset

--]]

function client.on_data(ctxt, payload)

    local data = payload.data

    local data_len = data:len()

    local offset = 1

    local byte = nil

    local utf8_str_len = 0

    local msg_type = 0

    local multiplier = 1

    local max_multiplier = 128 * 128 * 128

    local rem_length = 0

```



```
41      local clientID = nil
42
43      -- check if MQTT fixed header is present (fixed header length is
            atleast 2 bytes)
44
45      if (data_len < 2) then
46
47          goto need_more_data
48
49      end
50
51      byte = data:byte(offset)
52
53      offset = offset + 1
54
55         -- check for connect packet - type value 1
56
57      msg_type = bit32.rshift(byte, 4)
58
59      if (msg_type ~= 1) then
60
61          error("Missing MQTT Connect packet.")
62
63      end
64
65      -- parse the remaining length
66
67      repeat
68
69          if (multiplier > max_multiplier) then
70
71             error("MQTT CONNECT packet parse error - invalid Remaining
                   Length.")
72
73         end
74
75         if (data_len < offset) then
76
77            goto need_more_data
78
79         end
80
81         byte = data:byte(offset)
82
83         offset = offset + 1
```



```
84
85          rem_length = rem_length + (bit32.band(byte, 0x7F) * multiplier)
86
87          multiplier = multiplier * 128
88
89       until (bit32.band(byte, 0x80) == 0)
90
91       -- protocol name
92
93       -- check if protocol name length is present
94
95       if (data_len < offset + 1) then
96
97          goto need_more_data
98
99       end
100
101      -- protocol name length MSB
102
103      byte = data:byte(offset)
104
105      offset = offset + 1
106
107      utf8_str_len = byte * 256
108
109      -- length LSB
110
111      byte = data:byte(offset)
112
113      offset = offset + 1
114
115      utf8_str_len = utf8_str_len + byte
116
117         -- skip the variable header for connect message
118
119      -- the four required fields (protocol name, protocol level, connect
             flags, keep alive)
120
121      offset = offset + utf8_str_len + 4
122
123      -- parse the client ID
124
125      --
126
127      -- check if client ID len is present
```



```
128
129     if (data_len < offset + 1) then
130
131        goto need_more_data
132
133     end
134
135        -- client ID length MSB
136
137     byte = data:byte(offset)
138
139     offset = offset + 1
140
141     utf8_str_len = byte * 256
142
143     -- length LSB
144
145     byte = data:byte(offset)
146
147     offset = offset + 1
148
149     utf8_str_len = utf8_str_len + byte
150
151     if (data_len < (offset + utf8_str_len - 1)) then
152
153         goto need_more_data
154
155     end
156
157     clientID = data:sub(offset, offset + utf8_str_len - 1)
158
159     -- send the data so far to lb, user_token is set to do LB based on
           clientID
160
161     -- user_session is set to clientID as well (it will be used to
           persist session)
162
163     ns.send(ctxt.output, "DATA", {
164  data = data,
165
166                                 user_token = clientID,
167
168                                 user_session = clientID }
169  )
170
```



```
171         -- pipe the subsequent traffic to the lb - to bypass the
                extension handler
172
173     ns.pipe(ctxt.input, ctxt.output)
174
175     goto parse_done
176
177     ::need_more_data::
178
179     ctxt:hold(data)
180
181     ::parse_done::
182
183     return
184
185 end
186 <!--NeedCopy-->
```

Konfigurieren von MQTT über Protokollerweiterungen

October 5, 2021

Mit den folgenden Schritten fügen Sie der Citrix ADC Appliance ein MQTT-Protokoll hinzu.

Importieren Sie die Erweiterungsdatei von einem Webserver (über HTTP) oder Ihrer lokalen Workstation in die Citrix ADC Appliance. Weitere Informationen zum Importieren der Erweiterungsdatei finden Sie unter Importieren von Erweiterungen.

```
import ns extension local:mqtt_generic_fs.lua mqtt_code
```

Fügen Sie dem System mithilfe der Erweiterung ein neues TCP-basiertes Benutzerprotokoll hinzu.

```
add user protocol MQTT -transport TCP -extension mqtt_code
```

Fügen Sie einen Dienst vom Typ USER_TCP hinzu, um anzugeben, dass es sich um ein benutzerdefiniertes Protokoll handelt.

```
add service s1 10.102.90.112 USER_TCP 80
```

Fügen Sie einen Benutzer Load Balancing vserver hinzu und binden Sie Back-End-Dienste an ihn.

```
add lb vs mysv USER_TCP
```

```
bind lb vs mysv s1
```


Fügen Sie einen virtuellen Benutzerserver für das neu hinzugefügte Protokoll hinzu, und machen Sie den im vorherigen Schritt konfigurierten virtuellen Lastausgleichsserver zum Standardlastausgleichsserver.

```
add user vs v_mqtt MQTT 10.217.24.28 80 -defaultlb mysv
```

Aktivieren Sie optional die MQTT-Sitzungspersistenz basierend auf ClientID und legen Sie den Persistenztyp auf USERSESSION fest.

```
set lb vserver mqtt_lb -persistenceType USERSESSION
```

Konfigurieren von SSL-Abladung für MQTT

October 5, 2021

Sie können SSL-Abladung für Benutzerprotokolle implementieren, indem Sie eine SSL-Instanz für das Protokoll hinzufügen. Das folgende Beispiel zeigt, wie SSL-Abladung für ein Benutzerprotokoll durchgeführt wird. Der Datenverkehr zu Back-End-Diensten ist mit dieser Konfiguration unverschlüsselt.

Hinweis: Dieses Beispiel enthält keine Details zum Hinzufügen oder Aktualisieren eines Zertifikatschlüsselpaars und zum Binden an einen virtuellen Server. Weitere Informationen finden Sie unter SSL-Zertifikate.

Die folgenden Befehle fügen das MQTT_SSL-Protokoll hinzu, indem mqtt.lua mit dem Transportwert SSL eingefügt wird.

```
1 import extension http://10.217.24.48/extensions/mqtt.lua mqtt_code
2 add user protocol MQTT_SSL -transport SSL -extension mqtt_code
3 <!--NeedCopy-->
```

Mit den folgenden Befehlen wird ein virtueller Benutzerlastenausgleichsserver hinzugefügt und Backend-Services an ihn gebunden.

```
1 add service mqtt_svr1 10.217.24.48 USER_TCP 1501
2 add service mqtt_svr2 10.217.24.48 USER_TCP 1502
3 add lb vserver mqtt_lb USER_TCP  - lbMethod ROUNDROBIN
4 bind lb vserver mqtt_lb mqtt_svr1
5 bind lb vserver mqtt_lb mqtt_svr2
6 <!--NeedCopy-->
```


Mit dem folgenden Befehl wird ein virtueller Benutzerserver für das neu hinzugefügte Protokoll MQTT_SSL hinzugefügt. Die Verwendung von MQTT_SSL bedeutet, dass die Citrix ADC Appliance SSL-Abladung durchführen wird, da MQTT_SSL mit SSL-Transport konfiguriert wurde. Der Befehl legt außerdem den Standardwert auf den virtuellen Lastausgleichsserver fest, der im vorherigen Schritt konfiguriert wurde.

```
add user vserver mqtt_vs MQTT_SSL 10.217.24.28 8765 -defaultLb mqtt_lb
```

Für SSL-Abladung müssen Sie auch die SSL-Funktion aktivieren und einen Certkey an den virtuellen Server des Benutzers binden. Weitere Informationen finden Sie in den folgenden Themen:

Hinzufügen oder Aktualisieren eines Zertifikatschlüsselpaars

Binden Sie das Zertifikatschlüsselpaar an den virtuellen SSL-Server

Beispiel:

```
enable ns feature SSL

add SSL certKey mqtt_svr_cert_key -cert server1.cert -key server1.key

bind ssl vserver mqtt_vs  -certkeyName mqtt_svr_cert_key
<!--NeedCopy-->
```

Konfigurieren von SSL-Abladung mit End-to-End-Verschlüsselung für MQTT

October 5, 2021

Das folgende Beispiel zeigt, wie SSL-Verschiebung für MQTT mit End-to-End-Verschlüsselung durchgeführt wird.

Hinweis: Dieses Beispiel enthält keine Details zum Hinzufügen oder Aktualisieren eines Zertifikatschlüsselpaars und zum Binden an einen virtuellen Server. Weitere Informationen finden Sie unter SSL-Zertifikate.

Die folgenden Befehle importieren die Erweiterungsdatei und fügen Sie das MQTT_SSL-Protokoll mit SSL-Transport hinzu.

```
import extension http://10.217.24.48/extensions/mqtt.lua mqtt_code
add user protocol MQTT_SSL -transport SSL -extension mqtt_code
<!--NeedCopy-->
```


Mit den folgenden Befehlen wird ein virtueller Benutzerlastenausgleichsserver hinzugefügt und Backend-Services an ihn gebunden. Sowohl der virtuelle Lastausgleichsserver als auch die Dienste sind für den Diensttyp USER_SSL_TCP konfiguriert.

```
add service mqtt_svr1 10.217.24.48 USER_SSL_TCP 1501
add service mqtt_svr2 10.217.24.48 USER_SSL_TCP 1502
add lb vserver mqtt_lb USER_SSL_TCP  - lbmethod RR
bind lb vserver mqtt_lb mqtt_svr1
bind lb vserver mqtt_lb mqtt_svr2
<!--NeedCopy-->
```

Mit dem folgenden Befehl wird ein virtueller Benutzerserver für das neu hinzugefügte Protokoll MQTT_SSL hinzugefügt. Die Verwendung von MQTT_SSL bedeutet, dass die Citrix ADC Appliance SSL-Abladung durchführen wird, da MQTT_SSL mit SSL-Transport konfiguriert wurde. Der Befehl macht auch den im vorherigen Schritt konfigurierten virtuellen Lastausgleichsserver zum Standardlastausgleichsdienst.

```
add user vserver mqtt_vs MQTT_SSL 10.217.24.28 8765 -defaultLb mqtt_lb
```

Für die End-to-End-Verschlüsselung müssen Sie auch die SSL-Funktion aktivieren und einen Certkey an den Benutzer und die standardmäßigen virtuellen Server des Lastenausgleichs binden. Weitere Informationen finden Sie in den folgenden Themen:

Hinzufügen oder Aktualisieren eines Zertifikatschlüsselpaars

Binden Sie das Zertifikatschlüsselpaar an den virtuellen SSL-Server

```
enable ns feature SSL

add SSL certKey mqtt_svr_cert_key -cert server1.cert -key server1.key

bind ssl vserver mqtt_lb  -certkeyName mqtt_svr_cert_key

bind ssl vserver mqtt_vs  -certkeyName mqtt_svr_cert_key
<!--NeedCopy-->
```

Lernprogramm - Lastenausgleich von Syslog-Nachrichten mithilfe von Protokollerweiterungen

October 5, 2021

Das auf der Citrix ADC Appliance verfügbare Syslog-Protokoll funktioniert nur für die Nachrichten, die auf der Citrix ADC-Appliance generiert werden. Es wird kein Lastausgleich der Nachrichten, die von externen Knoten kommen. Um solche Meldungen zu laden, müssen Sie die Protokollerweiterungsfunktion verwenden und die Syslog-Message-Parsing-Logik schreiben, indem Sie die Lua 5.2 Programmiersprache verwenden.

Code zum Analysieren von Syslog-Nachricht

Der Code hat nur die TCP-Clientdaten-Callback-Funktion definiert - client.on_data (). Für Serverdaten wird keine Callback-Funktion hinzugefügt, und der Server zum Client nimmt den schnellen nativen Pfad. Der Code identifiziert die Nachrichtengrenze basierend auf dem nachfolgenden Zeichen. Wenn das TCP-Paket mehr als eine Syslog-Nachrichten enthält, teilen wir das Paket basierend auf dem nachfolgenden Zeichen und Lastverteilung jeder Nachricht.

```
--[[

  Syslog event handler for TCP client data

    ctxt - TCP client side App processing context.

    data - TCP Data stream received.

--]]

function client.on_data(ctxt, payload)

                  local message = nil

                  local data_len

                  local data = payload.data

                  local trailing_character = "\n"

                  ::split_message::

                                    -- Get the offset of trailing
                                       character

                                    local new_line_character_offset =
                                       data:find(trailing_character)

```



```
27                                  -- If trailing character is not
                                       found, then wait for more data.
28
29                                  if (not new_line_character_offset)
                                       then
30
31                                                      goto
                                                           need_more_data
32
33                                  end
34
35                                  -- Get the length of the current
                                       message
36
37                                  data_len = data:len()
38
39                                  -- Check whether we have more than
                                       one message
40
41                                  -- by comparing trailing character
                                       offset and
42
43                                  -- current data length
44
45                                  if (data_len >
                                       new_line_character_offset) then
46
47                                                      -- If we have
                                                           more than one
                                                           message, then
                                                           split
48
49                                                      -- the data into
                                                           two parts such
                                                            that first
                                                           part
50
51                                                      -- will contain
                                                           message upto
                                                           trailing
                                                           character
52
53                                                      -- offset and
                                                           second part
                                                           will contain
```



```
54
55                                                      -- remaining
                                                           message.
56
57                                                      message, data =
                                                           data:split(
                                                           new_line_character_offse
                                                           )
58
59                                      else
60
61                                                      message = data
62
63                                                      data = nil
64
65                                      end
66
67  -- Send the data to the backend server.
68
69                                      ns.send(ctxt.output, ”EOM”, {
70   data = message }
71   )
72
73                                      goto done
74
75                                      ::need_more_data::
76
77                                                      -- Wait for more
                                                           data
78
79                                                      ctxt:hold(data)
80
81                                                      data = nil
82
83                                                      goto done
84
85                                      ::done::
86
87                                                      -- If we have
                                                           more data to
                                                           parse,
88
89                                                      -- then do
                                                           parsing again.
90
```



```
91                                                          if (data) then
92
93                                                                          goto
                                                                                split_
94
95                                                          end
96
97  end
98  <!--NeedCopy-->
```

Konfigurieren des Syslog-Protokolls mithilfe von Protokollerweiterungen

October 5, 2021

Mit den folgenden Schritten fügen Sie der Citrix ADC Appliance ein SYSLOG-Benutzerprotokoll hinzu.

Importieren Sie die Erweiterungsdatei von einem Webserver (über HTTP) oder Ihrer lokalen Workstation in die Citrix ADC Appliance. Weitere Informationen zum Importieren der Erweiterungsdatei finden Sie unter Erweiterungen importieren.

```
import ns extension local:syslog_parser.lua syslog_parser_code
```

Fügen Sie dem System mithilfe der Erweiterung ein neues TCP-basiertes Benutzerprotokoll hinzu.

```
add user protocol USER_SYSLOG -transport TCP -extension syslog_parser_code
```

Fügen Sie einen Dienst vom Typ USER_TCP hinzu, um anzugeben, dass es sich um ein benutzerdefiniertes Protokoll handelt.

```
add service s1 10.102.90.112 USER_TCP 80
```

Fügen Sie einen Benutzer Load Balancing vserver hinzu und binden Sie Back-End-Dienste an ihn.

```
1  add lb vs mysv USER_TCP
2
3  bind lb vs mysv s1
4  <!--NeedCopy-->
```

Fügen Sie einen virtuellen Benutzerserver für das neu hinzugefügte Protokoll hinzu, und machen Sie den im vorherigen Schritt konfigurierten virtuellen Lastausgleichsserver zum Standardlastausgleichsserver.


```
add user vs v_syslog USER_SYSLOG 10.217.24.28 80 -defaultlb mysv
```

Protokollerweiterungen, Befehlsreferenz

October 5, 2021

In der folgenden Tabelle sind alle neuen Befehle aufgeführt, die für benutzerdefinierte Protokolle hinzugefügt wurden, sowie die vorhandenen Befehle, die für benutzerdefinierte Protokolle geändert wurden.

```
show lb persistentSessions [<vserv-name>]
```

- **CLI-Befehl:**

  ```
  add user protocol <name> -transport ( TCP | SSL )-extension <string> -
  comment <string>]>
  ```

- **Beschreibung:**

  Fügt der Citrix ADC Appliance mithilfe von Erweiterungen ein neues Benutzerprotokoll hinzu. Derzeit werden nur Benutzerprotokolle mit Transportwert TCP oder SSL unterstützt.

  > **Beispiel:**
  >
  > add user protocol MQTT -transport TCP -extension mqtt_code

- **CLI-Befehl:**

  ```
  rm user protocol <name>
  ```

- **Beschreibung:**

  Entfernt ein Benutzerprotokoll, das zuvor der Citrix ADC Appliance hinzugefügt wurde.

  > **Beispiel:**
  >
  > rm-Benutzerprotokoll mqtt

- **CLI-Befehl:**

  ```
  set user protocol <name> -comment <string>
  ```

- **Beschreibung:**

  Ändert die Einstellungen für ein Benutzerprotokoll, das zuvor der Citrix ADC Appliance hinzugefügt wurde.

  > **Beispiel:**
  >
  > setzen Sie das Benutzerprotokoll mqtt -comment “MQTT Protocol implementation”

- **CLI-Befehl:**

  ```
  unset user protocol <name> -comment
  ```

- **Beschreibung:**

  Entfernt Einstellungen für ein Benutzerprotokoll, das zuvor der Citrix ADC Appliance hinzugefügt wurde.

  > **Beispiel:**
  >
  > unset user protocol mqtt -comment MQTT protocol implementation

- **CLI-Befehl:**

  ```
  update ns extension <extension name>
  ```

- **Beschreibung:**

  Aktualisiert die Implementierung für ein zuvor hinzugefügtes Benutzerprotokoll mithilfe von Erweiterungen.

  Sie können die Protokollimplementierung nur aktualisieren, wenn das Protokoll nicht von einem virtuellen Benutzerserver verwendet wird.

  > **Beispiel:**ns-Erweiterung my-extension
  >
  > aktualisieren

- **CLI-Befehl:**

  ```
  add lb vserver <name> [USER_TCP | USER_SSL_TCP] [-lbmethod USER_TOKEN]
  [-persistencetype USERSESSION] [-timeout <value>]
  ```

- **Beschreibung:**

  Fügt der Citrix ADC Appliance einen virtuellen Lastausgleichsserver hinzu. Dies ist ein vorhandener CLI-Befehl.

  Bei virtuellen Servern des Lastenausgleichs lautet der zu verwendende Diensttyp USER_TCP oder USER_SSL_TCP. Die IP-Adresse und der Port sind bei virtuellen Servern mit Benutzerlastenausgleich nicht zulässig.

  Für virtuelle Server mit Benutzerlastenausgleich ist nur die ROUNDROBIN Lastausgleichsmethode zulässig, und der Tokenwert wird durch den Erweiterungscode bereitgestellt. Ebenso ist nur die Persistenz von USERSESSION zulässig, und die Persistenzeinstellung wird durch den Erweiterungscode bereitgestellt.

  > **Beispiel:**
  >
  > add lb vserver mysv USER_TCP —lbmethod ROUNDROBIN

- **CLI-Befehl:**

```
add user vserver <name> <userProtocol> <IPAddress> <port> -defaultLB <
string> [-params <string>] [-comment <string>]
```

- **Beschreibung:**

  Fügt mithilfe von Erweiterungen einen virtuellen Server für ein Benutzerprotokoll hinzu. Der konfigurierte virtuelle Standardserver für den Lastenausgleich des Benutzers ist für den TCP-Clientdaten-Erweiterungshandler als ctxt.output verfügbar. Für einen virtuellen Server können Erweiterungsparameter mithilfe der Option -params mit einem Namen und einem Wertepaar festgelegt werden. Der entsprechende Parameterwert steht den Erweiterungshandlern als ctxt.vserver.params zur Verfügung. <paramName>.

  > **Beispiel:**
  >
  > add user vs v_mqtt MQTT 10.217.24.28 80 -defaultlb mysv

- **CLI-Befehl:**

```
rm user vserver <name>
```

- **Beschreibung:**

  Entfernt einen virtuellen Benutzerserver, der der Citrix ADC Appliance zuvor hinzugefügt wurde.

  > **Beispiel:**
  >
  > rm-Benutzer vserver v_mqtt

- **CLI-Befehl:**

```
set user vserver <name> [-IPAddress <ip_addr|ipv6_addr|*>] [-defaultLB
<string>] [-params <string>] [-comment <string>]
```

- **Beschreibung:**

  Ändert die Einstellungen für einen virtuellen Benutzerserver, der zuvor der Citrix ADC Appliance hinzugefügt wurde. Wenn einem Erweiterungsparameter durch die Option -params ein neuer Wert zugewiesen wird, wird der alte Wert überschrieben.

  > **Beispiel:**
  >
  > set user vs v_mqtt MQTT 10.217.24.28 -defaultlb mysv -comment MQTT protocol implementation

- **CLI-Befehl:**

```
unset user vserver <name> [-params] [-comment]
```

- **Beschreibung:**

Entfernt die Einstellungen für einen virtuellen Benutzerserver, der zuvor der Citrix ADC Appliance hinzugefügt wurde. Wenn Sie die Option —params verwenden, um einen Erweiterungsparameter aufzuheben, wird der entsprechende Parameterwert, der für Erweiterungshandler verfügbar ist, in nil geändert.

> **Beispiel:**
>
> unset user vs v_mqtt MQTT 10.217.24.28 -defaultlb mysv -comment MQTT protocol implementation

- **CLI-Befehl:**

  `show user protocol [<name>]`

- **Beschreibung:**

  Zeigt Informationen zu einem Benutzerprotokoll an, z. B. Erweiterung und Rückrufe.

  > **Beispiel:**Benutzerprotokoll
  >
  > anzeigen mqtt

- **CLI-Befehl:**

  `show user vserver [<name>]`

- **Beschreibung:**

  Zeigt Informationen zu einem virtuellen Benutzerserver an.

  > **Beispiel:**Benutzer vserver vs_mqtt
  >
  > anzeigen

- **CLI-Befehl:**

  `stat user vserver [<name>]`

- **Beschreibung:**

  Zeigt Statistiken über einen virtuellen Benutzerserver an.

  > **Beispiel:**
  >
  > stat-Benutzer vserver vs_mqtt

- **CLI-Befehl:**

  `show lb persistentSessions [<vserv-name>]`

- **Beschreibung:**

  Zeigt Informationen zu persistenten Sitzungen an. Dies ist eine vorhandene CLI. Bei Benutzerprotokollen wird der Persistenztyp als USERSESSION angezeigt.

- **CLI-Befehl:**

  ```
  rm lb vserver <name>
  ```

- **Beschreibung:**

  Entfernt einen Benutzer LB vserver, der zuvor der Citrix ADC Appliance hinzugefügt wurde.

  > **Beispiel:**
  >
  > rm lb vserver mysv

- **CLI-Befehl:**

  ```
  add service <name> <IPAddr> (USER_TCP | USER_SSL_TCP)<Port>
  ```

- **Beschreibung:**

  Fügt einen Backend-Dienst hinzu, der für ein Benutzerprotokoll verwendet werden soll. Dies ist ein vorhandener CLI-Befehl mit den neuen Diensttypen USER_TCP und USER_SSL_TCP.

  > **Beispiel:**
  >
  > add service mqtt_svr1 10.217.24.48 USER_TCP 1501
  >
  > **Hinweis**: Die vorhandenen Befehle set service und unset service können verwendet werden, um die Einstellungen eines zuvor hinzugefügten Dienstes für ein Benutzerprotokoll zu entfernen oder zu ändern.

- **CLI-Befehl:**

  ```
  bind lb vserver <name> <serviceName>
  ```

- **Beschreibung:**

  Bindet einen Dienst an einen Benutzer LB vserver. Der Diensttyp sollte USER_TCP/USER_SSL_TCP sein, um an einen LB-vserver mit dem Typ USER_TCP/USER_SSL_TCP zu binden.

  > **Beispiel:**
  >
  > bind lb vserver mysv mqtt_svr1

- **CLI-Befehl:**

  ```
  unbind lb vserver <name> <serviceName>
  ```

- **Beschreibung:**

  Entbindet einen zuvor gebundenen Dienst an einen Benutzer LB vserver.

  > **Beispiel:**
  >
  > unbind lb vserver mysv mqtt_svr1

- **CLI-Befehl:**

  ```
  rm service <name>
  ```

- **Beschreibung:**

  Entfernt einen Dienst, der zuvor für ein Benutzerprotokoll hinzugefügt wurde.

  > **Beispiel:**
  >
  > rm-Dienst mqtt_svr1

Fehlerbehebung bei Protokollerweiterungen

October 5, 2021

Wenn sich Ihre Erweiterungsfunktion nicht wie erwartet verhält, können Sie die Erweiterungsprotokollierungsfunktion verwenden, um das Verhalten Ihrer Erweiterungsfunktion zu überprüfen. Sie können der Erweiterungsfunktion auch Protokollierung hinzufügen, indem Sie die benutzerdefinierte Protokollierungsfunktion verwenden, in der Sie die Protokollstufe definieren können, die auf der Citrix ADC Appliance erfasst werden soll.

Benutzerdefinierte Protokollierung

Sie können auch Ihre eigene Protokollierung zu Ihrer Erweiterungsfunktion hinzufügen. Verwenden Sie dazu die integrierte ns.logger:level() -Funktion, wobei levelist: emergency, alert, critical, error, warning, notice, info oder debug. Die Parameter sind die gleichen wie die C printf () -Funktion: eine Formatzeichenfolge und eine variable Anzahl von Argumenten, die Werte für die% angeben, die in der Formatzeichenfolge angegeben werden. Beispielsweise können Sie der COMBINE_HEADERS Funktion Folgendes hinzufügen, um das Ergebnis eines Aufrufs zu protokollieren:

```
local result_str = table.concat(combined_headers, ”\r\n”) .. ”\r\n\r\n”

ns.logger:info(”Result: %s”, result_str)

return result_str
<!--NeedCopy-->
```

Die obige Funktion würde die folgende Meldung nach/var/log/ns.log für die Beispieleingabe protokollieren, die in den abgekürzten Protokollnachrichtenbeispielen im Abschnitt Extension Tracing oben gezeigt wird.


```
... : default NSEXTENSION Message 143 0 : "Result: Host: 10.217.24.7:2000^M
 H1: abcd, 1234^M User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4)libcurl
/7.24.0 OpenSSL/0.9.8y zlib/1.2.3^M Accept: \*/\*^M H2: h2val1, h2val2,
h2val3^M ^M"
```

Richtlinienerweiterungen

October 5, 2021

Mit der Richtlinienerweiterung können Sie Erweiterungsfunktionen für integrierte Richtlinientypen schreiben. Die Erweiterungen können in Richtlinienausdrücken verwendet werden, genau wie integrierte Funktionen. Sie werden ausgeführt, wenn die entsprechenden Richtlinienausdrücke ausgewertet werden. Diese Funktion ist nützlich für:

- Hinzufügen benutzerdefinierter Funktionen zu vorhandenen Richtlinien.
- Implementierung von logischen Konstrukten für komplexe Kundenanforderungen.

Das Richtlinienerweiterungsfeature behebt diese Einschränkungen, indem es Benutzern ermöglicht wird, Erweiterungsfunktionen für integrierte Richtlinientypen zu schreiben. Die Erweiterungen können dann in den Richtlinienausdrücken verwendet werden, genau wie integrierte Funktionen. Sie werden ausgeführt, wenn die entsprechenden Richtlinienausdrücke ausgewertet werden.

In der folgenden Tabelle sind die Richtlinientypen aufgeführt, die beim Schreiben einer Erweiterung verwendet werden können, sowie die zugehörigen Zuordnungen.

Richtlinientyp	Zugeordneter Richtlinientyp	Ausgabe
TEXT_T	NSTEXT	Zeichenfolge
BOOL_AT	NSBOOL	Boolesch
NUM_AT	NSNUM	Zahl (Gleitkommazahl mit doppelter Genauigkeit)
DOUBLE_AT	NSDOUBLE	Zahl (Gleitkommazahl mit doppelter Genauigkeit)

Voraussetzungen für die Verwendung von Richtlinienerweiterungen

Die importierten Funktionen müssen den vorhandenen Richtlinienstandards entsprechen. Daher:

- Der Funktionsname muss mit einem Buchstaben beginnen und kann Zahlen oder Unterstriche enthalten.

- Der Funktionsname wird von Citrix ADC Richtlinien als Groß-/Kleinschreibung nicht beachtet.
- Die Funktion muss einen einzelnen Wert zurückgeben, auch wenn die Erweiterungssprache mehrere Werte zurückgibt.
- Funktionen mit einer variablen Anzahl von Argumenten werden nicht unterstützt.

Wie funktionieren Richtlinienerweiterungen?

Die vorhandenen Richtlinien auf einer Citrix ADC Appliance verwenden einen Interpreter, um die Funktionen auszuwerten, die in eine Richtlinienerweiterungsdatei importiert werden. Wenn ein Benutzer eine neue Funktion in eine Richtlinienerweiterungsdatei importiert:

1. Die Erweiterungsdatei wird auf Syntax und andere Bedingungen überprüft.
2. Wenn die Validierung fehlschlägt, wird der Fehler an den Benutzer gemeldet.
3. Wenn die Validierung erfolgreich ist, wird die Erweiterungsdatei in die Citrix ADC Appliance importiert und ihr Inhalt kann wie jede integrierte Richtlinienfunktion in Richtlinienausdrücken verwendet werden.
    a) Wenn die Auswertung des Richtlinienausdrucks während der Laufzeit einen Fehler zurückgibt, wird es als undef-Ereignis gemeldet und der zugehörige Fehlerindikator wird erhöht. **Hinweis:** Wenn ein Richtlinien undef-Ereignis eintritt und die Richtlinienregel eine oder mehrere Richtlinienerweiterungsfunktionen enthält, zeigt der `show ns extension <name>` Befehl die undef-Treffer an, wenn er auf diese Richtlinienerweiterungen angewendet wird. Wenn die Erweiterungsfunktion abgebrochen wird, wird der Abbruchzählerwert erhöht.
    b) Wenn die Auswertung des Richtlinienausdrucks erfolgreich ist, wird die Ausdrucksauswertung fortgesetzt, bis der gesamte Ausdruck ausgewertet wird oder bis er aufgrund eines Fehlers abgebrochen wird.

Wenn die Erweiterungsfunktion zu lange dauert, wird sie abgebrochen, und der Fehlerzähler für diese Erweiterungsfunktion wird erhöht. Die Erweiterungsfunktion ist sandboxed, was Folgendes verhindert:

- Übermäßige CPU-Auslastung auf der Citrix ADC Appliance.
- Übermäßige Speichernutzung auf der Citrix ADC Appliance.
- Verwendung schädlicher integrierter Bibliotheken oder Bibliotheken von Drittanbietern oder Binärdateien.
- Langfristige Skripts, die möglicherweise einen Neustart der Citrix ADC Appliance verursachen könnten.

Konfigurieren von Richtlinienerweiterungen

October 5, 2021

Wenn die Richtlinienerweiterungsdatei fertig ist, importieren Sie sie in die Citrix ADC Appliance. Der Importvorgang kopiert die Erweiterungsdatei in ein Verzeichnis auf der Citrix ADC Appliance und sucht nach Syntaxfehlern.

Nach dem Import müssen Sie die Erweiterungsdatei für die Verwendung in den Richtlinienausdrücken zur Verfügung stellen.

Hinweis: Der Importbefehl wird verwendet \<src\>, um den Dateiinhalt von einer externen Quelle oder einer internen Quelle auf das Citrix ADC-Dateisystem herunterzuladen. Um diesen Dateiinhalt zum ersten Mal in eine oder mehrere Paket-Engines zu laden, verwenden Sie den Befehl add. Wenn der Dateiinhalt aktualisiert wird, kann der aktualisierte Inhalt in das Citrix ADC-Dateisystem heruntergeladen werden, indem der Importbefehl mit dem Argument overwrite ausgegeben wird. Der Befehl aktualisiert den Inhalt im Dateisystem. Um den aktualisierten Inhalt in eine oder mehrere Paket-Engines zu laden, verwenden Sie den Befehl update.

Konfigurieren von Richtlinienerweiterungen mit der CLI

1. Importieren Sie die Richtlinienerweiterungsdatei von einem Webserver (über HTTP) oder Ihrer lokalen Workstation in die Citrix ADC Appliance.

   a) HTTP-Import

   Wenn Sie einen Webserver zur Verfügung haben, können Sie die Erweiterungsdatei im Webserververzeichnis speichern und in die Citrix ADC Appliance importieren.

```
import ns extension <src> <name> [-comment<string>] [-
   overwrite]
<!--NeedCopy-->
```

   Beispiel:

```
import ns extension http://myhost/path/to/extension
   myextension -comment  “Custom crc calculation
<!--NeedCopy-->
```

   b) Lokaler Import

Sie können den SSH-Client verwenden, um die Erweiterungsdatei von Ihrer Workstation in das /var/tmp-Verzeichnis der Citrix ADC Appliance zu kopieren

```
scp extension-file-name <ns-userid@ns-ip-addr>:/var/tmp
<!--NeedCopy-->
```

Wobei:

- `extension-file-name` ist der Name der Erweiterungsdatei auf Ihrem Client-Computer.
- `ns-userid` ist der Benutzer der Citrix ADC Appliance mit der Berechtigung, in /var/tmp zu schreiben.
- `ns-ip-addr` ist die Citrix ADC IP-Adresse.

Führen Sie nach dem Kopieren der Datei auf die Citrix ADC Appliance den Importbefehl auf der Citrix ADC Appliance aus.

```
import ns extension local:<extension-file-name extension-name>
<!--NeedCopy-->
```

Hinweis: Die CLI muss verwendet werden, um eine lokale Erweiterungsdatei zu importieren, indem der Befehl
import ausgeführt wird.

2. Fügen Sie der Paket-Engine die Richtlinienerweiterung zur Evaluierung hinzu.

```
add ns extension <name> [-comment <string>]
<!--NeedCopy-->
```

Beispiel:

```
add ns extension myextension
<!--NeedCopy-->
```

Nachdem eine Erweiterungsdatei importiert wurde, können Sie sie aktualisieren, wenn Sie den Parameter -overwrite in den Befehl import aufgenommen haben oder entfernen. Sie können auch die Details einer importierten Erweiterungsdatei anzeigen.

Aktualisieren einer Erweiterungsdatei auf der Citrix ADC Appliance von der Quelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
update ns extension <name>
<!--NeedCopy-->
```

Hinweis: Sie können die Erweiterungsdatei erst aktualisieren, nachdem Sie die angegebene Erweiterungsdatei mit dem Parameter -overwrite in die Citrix ADC Appliance importiert haben.

Beispiel:

```
update ns extension myextension
<!--NeedCopy-->
```

Entfernen einer Erweiterungsdatei aus der Citrix ADC Appliance

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm ns extension <name>
<!--NeedCopy-->
```

Beispiel:

```
rm ns extension myextension
<!--NeedCopy-->
```

Anzeigen der Details der angegebenen Erweiterungsfunktion auf der Citrix ADC Appliance

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show ns extension <name>
<!--NeedCopy-->
```

Beispiel:


```
show ns extension myextension
<!--NeedCopy-->
```

Konfigurieren von Richtlinienerweiterungen mit der GUI

1. Importieren Sie die Richtlinienerweiterungsdatei von einem Webserver (über HTTP) oder Ihrer lokalen Workstation in die Citrix ADC Appliance.
   a) Navigieren Sie zu **AppExpert** > **Richtlinienerweiterungen**, klicken Sie auf **Richtlinienerweiterung** . Wählen Sie in der Dropdownliste **Importieren von die URL für den Speicherort der Erweiterungsdatei aus**, die Sie importieren möchten.
   b) Navigieren Sie zu **AppExpert** > **Richtlinienerweiterungen**, **Richtlinienerweiterung**, und importieren Sie die Erweiterungsdatei, indem Sie in der Dropdownliste **Importieren** von Datei auswählen.
2. Fügen Sie der Paket-Engine die Richtlinienerweiterung zur Evaluierung hinzu.

   Navigieren Sie zu **AppExpert** > **Richtlinienerweiterungen**, und fügen Sie auf der Registerkarte**Richtlinienerweiterungen** die Erweiterungsdatei hinzu.

Aktualisieren einer Erweiterungsdatei auf der Citrix ADC Appliance von der Quelle

Navigieren Sie zu **AppExpert** > **Richtlinienerweiterungen**, und aktualisieren Sie auf der Registerkarte **Richtlinienerweiterungen** die Erweiterungsdatei.

Entfernen einer Erweiterungsdatei aus der Citrix ADC Appliance

Navigieren Sie zu **AppExpert** > **Richtlinienerweiterungen** und entfernen Sie auf der Registerkarte **Richtlinienerweiterungen** die Erweiterungsdatei.

Anzeigen der Details der angegebenen Erweiterungsfunktion auf der Citrix ADC Appliance

Navigieren Sie zu **AppExpert** > **Richtlinienerweiterungen**, und klicken Sie auf der Registerkarte **Funktionen für Richtlinienerweiterungen** auf den Pfeil auf die Dropdownliste der Erweiterungsfunktion, für die Sie die Details anzeigen möchten.

Richtlinienerweiterungen - Anwendungsfälle

October 5, 2021

Bestimmte Kundenanwendungen haben Anforderungen, die mit bestehenden Richtlinien und Ausdrücken nicht berücksichtigt werden können. Mit der Richtlinienerweiterung können Kunden benutzerdefinierte Funktionen zu ihren Anwendungen hinzufügen, um ihre Anforderungen zu erfüllen.

Die folgenden Anwendungsfälle veranschaulichen das Hinzufügen neuer Funktionen mithilfe der Richtlinienerweiterungsfunktion auf der Citrix ADC Appliance.

- Fall 1: Benutzerdefinierter Hash
- Fall 2: Doppelschrägstriche in URLs reduzieren
- Fall 3: Kopfzeilen kombinieren

Fall 1: Benutzerdefinierter Hash

Die CUSTOM_HASH Funktion bietet einen Mechanismus, um jede Art von Hash-Wert in die an den Client gesendeten Antworten einzufügen. In diesem Anwendungsfall wird die Hash-Funktion verwendet, um den Hash der Abfragezeichenfolge für eine Rewrite HTTP-Anforderung zu berechnen und einen HTTP-Header namens CUSTOM_HASH mit dem berechneten Wert einzufügen. Die CUSTOM_HASH Funktion implementiert den DJB2-Hash-Algorithmus.

Beispielverwendung von CUSTOM_HASH:

```
> add rewrite action test_custom_hash insert_http_header ”CUSTOM_HASH” ”HTTP.REQ.URL.QUERY.CUSTOM_HASH”
<!--NeedCopy-->
```

Beispieldefinition von CUSTOM_HASH ():

```
    -- Extension function to compute custom hash on the text

    -- Uses the djb2 string hash algorithm
    function NSTEXT:CUSTOM_HASH() : NSTEXT

        local hash = 5381

        local len = string.len(self)

        for i = 1, len do

            hash = bit32.bxor((hash * 33), string.byte(self, i))

        end
```



```
15
16         return tostring(hash)
17
18     end
19 <!--NeedCopy-->
```

Zeilenweise Beschreibung der obigen Probe:

```
1  function NSTEXT:CUSTOM_HASH() : NSTEXT
2
3  Defines the CUSTOM_HASH() function, with text input and a text return
       value.
4
5  local hash = 5381
6  local len = string.len(self)
7
8  Declares two local variables:
9
10  - hash. Accumulates the compute hash value and is seeded with the
       number 5381
11
12  - len. Sets to the length of the self input text string, using the
       built-in string.len() function.
13
14 for i = 1, len do
15       hash = bit32.bxor((hash * 33), string.byte(self, i))
16 end
17
18 Iterates through each byte of the input string and adds the byte to the
       hash. It uses the built-in string.byte() function to get the byte
      and the built-in bit32.bxor() function to compute the XOR of the
      existing hash value (multiplied by 33) and the byte.
19
20 return tostring(hash)
21
22 Calls the built-in tostring() function to convert the numeric hash
      value to a string and returns the string as the value of the
      function.
23 <!--NeedCopy-->
```


Fall 2: Doppelschrägstriche in URLs reduzieren

Durch das Reduzieren doppelter Schrägstriche in URLs wird die Rendering-Zeit der Website verbessert, da Browser die URLs mit einem Schrägstrich effizienter analysieren. Die einzelnen Schrägstriche URLs auch zur Aufrechterhaltung der Kompatibilität mit Anwendungen, die keine doppelten Schrägstriche akzeptieren. Mit der Richtlinienerweiterung können Kunden eine Funktion hinzufügen, die die doppelten Schrägstriche durch einzelne Schrägstriche in den URLs ersetzt. Das folgende Beispiel veranschaulicht das Hinzufügen einer Richtlinienerweiterungsfunktion, die Doppelschrägstriche in URLs reduziert.

Beispieldefinition von COLLAPSE_DOUBLE_SLASHES ():

```
1     -- Collapse double slashes in URL to a single slash and return the
          result
2     function NSTEXT:COLLAPSE_DOUBLE_SLASHES() : NSTEXT
3
4         local result = string.gsub(self, "//", "/")
5
6         return result
7
8     end
9 <!--NeedCopy-->
```

Zeilenweise Beschreibung der obigen Probe:

```
1  function NSTEXT:COLLAPSE_DOUBLE_SLASHES() : NSTEXT
2
3  Declares the COLLAPSE_DOUBLE_SLASHES() function with text input and
       return.
4
5  local result = string.gsub(self, "//", "/")
6
7  Declares a local variable named result and uses the built-in string.
       gsub() function to replace all double slashes with single slashes in
        the self input text.
8
9  The second parameter of string.gsub() is actually a regular expression
       pattern, although here a simple string is used for the pattern.
10
11 return result
12
13 Returns the resulting string.
```



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

Fall 3: Kopfzeilen kombinieren

Bestimmte Kundenanwendungen können nicht mehrere Header in einer Anforderung verarbeiten. Auch das Parsen von doppelten Headern mit gleichen Header-Werten oder mehreren Headern mit demselben Namen, aber unterschiedlichen Werten in einer Anforderung verbraucht Zeit und Netzwerkressourcen. Die Richtlinienerweiterungsfunktion ermöglicht es Kunden, eine Funktion hinzuzufügen, um diese Header zu einzelnen Headern zu kombinieren, wobei ein Wert, der die ursprünglichen Werte kombiniert. Beispiel: Kombinieren Sie die Werte der Header H1 und H2.

Ursprüngliche Anfrage:

```
GET /combine_headers HTTP/1.1
User-Agent: amigo unit test
Host: myhost
H2: h2val1
H1: abcd
Accept: \*/\*
H2: h2val2
Content-Length: 0
H2: h2val3
H1: 1234
<!--NeedCopy-->
```

Geänderte Anfrage:

```
GET /combine_headers HTTP/1.1
User-Agent: amigo unit test
Host: myhost
H2: h2val1, h2val2, h2val3
H1: abcd, 1234
Accept: \*/\*
Content-Length: 0
<!--NeedCopy-->
```

Im Allgemeinen wird diese Art von Anforderungsänderung mit der Funktion “Umschreiben” durchgeführt, wobei Richtlinienausdrücke verwendet werden, um den Teil der zu ändernden Anforderung (das Ziel) und die durchzuführende Änderung (der Zeichenfolgengenerator-Ausdruck) zu beschreiben. Richtlinienausdrücke können jedoch nicht über eine beliebige Anzahl von Headern iterieren.

Die Lösung dieses Problems erfordert eine Erweiterung der Richtlinienfazilität. Um dies zu tun, werden wir eine Erweiterungsfunktion definieren, genannt COMBINE_HEADERS. Mit dieser Funktion können wir die folgende Rewrite-Aktion einrichten:

```
> add rewrite action combine_headers_act replace 'HTTP.REQ.FULL_HEADER
.AFTER_STR(”HTTP/1.1rn”)''HTTP.REQ.FULL_HEADER.AFTER_STR(”HTTP/1.1rn”).
COMBINE_HEADERS'
```

Hier ist das Rewrite-Ziel HTTP.REQ.FULL_HEADER.AFTER_STR (“HTTP/1.1rn”). Die AFTER_STR (“HTTP/1.1rn”) ist erforderlich, da FULL_HEADER die erste Zeile der HTTP-Anfrage enthält (z.B. GET /combine_headers HTTP/1.1).

Der String-Builder-Ausdruck ist HTTP.REQ.FULL_HEADER.AFTER_STR(“HTTP/1.1rn”).COMBINE_HEADERS, wobei die Header (ohne die erste Zeile) in die Erweiterungsfunktion COMBINE_HEADERS eingespeist werden, die die Werte für Header kombiniert und zurückgibt.

Beispieldefinition von COMBINE_HEADERS ():

```
1     -- Extension function to combine multiple headers of the same name
         into one header.
2
3
4
5     function NSTEXT:COMBINE_HEADERS(): NSTEXT
6
7         local headers = {
8   }
9   -- headers
10
11        local combined_headers = {
12  }
13  -- headers with final combined values
14        -- Iterate over each header (format ”name:valuer\r\n”)
15
16        -- and build a list of values for each unique header name.
17
18        for name, value in string.gmatch(self, ”([^:]+):([^\r\n]*)\r\n”
             ) do
19
20            if headers[name] then
21
22                local next_value_index = #(headers[name]) + 1
23
24                headers[name][next_value_index] = value
```



```
25
26              else
27
28                  headers[name] = {
29   name .. ":" .. value }
30
31
32              end
33
34          end
35
36
37
38          -- iterate over the headers and concat the values with
                separator ","
39
40          for name, values in pairs(headers) do
41
42              local next_header_index = #combined_headers + 1
43
44              combined_headers[next_header_index] = table.concat(values,
                    ",")
45
46          end
47
48
49
50          -- Construct the result headers using table.concat()
51
52          local result_str = table.concat(combined_headers, "\r\n") .. "\
                r\n\r\n"
53
54          return result_str
55
56      end
57  <!--NeedCopy-->
```

Zeilenweise Beschreibung der obigen Probe:

```
1  function NSTEXT:COMBINE_HEADERS(): NSTEXT
2
3  Defines the COMBINE_HEADERS extension function, with the text input
       into the function from the policy expression and a text return type
```



```
      to the policy expression.
4
5  local headers = {
6    }
7    -- headers
8  local combined_headers = {
9    }
10   -- headers with final combined values
11
12 Declares local variables headers and combined_headers and initialize
      these variables to empty tables. headers will be a table of arrays
      of strings, where each array holds one or more values for a header.
      combined_headers will be an array of strings, where each array
      element is a header with its combined values.
13
14 for name, value in string.gmatch(self, "([^:]+):([^\r\n]*)\r\n") do
15 . . .
16 end
17 <!--NeedCopy-->
```

Diese generische for-Schleife analysiert jeden Header in der Eingabe. Der Iterator ist die integrierte String.gmatch () Funktion. Diese Funktion verwendet zwei Parameter: eine zu suchende Zeichenfolge und ein Muster, mit dem Teile der Zeichenfolge übereinstimmen. Die zu suchende Zeichenfolge wird durch den impliziten Selbstparameter bereitgestellt, der der Text für die Header ist, die in die Funktion eingegeben werden.

Das Muster wird mit einem regulären Ausdruck ausgedrückt (Regex für kurz). Diese Regex entspricht dem Headernamen und -wert für jeden Header, den der HTTP-Standard als *name*:*value*\r\n definiert. Die Klammern in der Regex geben die passenden Teile an, die extrahiert werden sollen. Daher lautet das Regex-Schema (*Match-Name*):(*Match-Wert*)\r\n. Das *Match-Name-Muster* muss mit allen Zeichen außer dem Doppelpunkt übereinstimmen. Dies ist geschrieben [^:]+ ([^:] ist ein beliebiges Zeichen außer: und + ist eine oder mehrere Wiederholungen). In ähnlicher Weise muss das *Match-Wert-Muster* mit allen Zeichen außer dem\ r\ n übereinstimmen, also wird es geschrieben [^\ r\ n]*([^\ r\ n] entspricht jedem Zeichen außer\ r und\ n und* ist Null oder mehr Wiederholungen). Dies macht die komplette Regex ([^:]+):([^\ r\ n]*)\r\n.

Die for -Anweisung verwendet eine Mehrfachzuweisung, um Namen und Wert auf die beiden Übereinstimmungen festzulegen, die vom string.gmatch () Iterator zurückgegeben werden. Diese werden implizit als lokale Variablen im Körper der for-Schleife deklariert.

```
1 if headers[name] then
2      local next_value_index = #(headers[name]) + 1
3      headers[name][next_value_index] = value
```



```
4  else
5       headers[name] = {
6   name .. ":" .. value }
7
8  end
9  <!--NeedCopy-->
```

Diese Anweisungen innerhalb der for-Schleife setzen die Headernamen und -werte in die Header-Tabelle. Wenn ein Header-Name zum ersten Mal analysiert wird (z. B. H2: h2val1 in der Beispieleingabe), gibt es keinen Headereintrag für den Namen und der[Headername] ist nil.

Da nil als falsch behandelt wird, wird die else-Klausel ausgeführt. Dies setzt den Header-Eintrag für name auf ein Array mit einem Zeichenfolgenwert *name*:*value*.

Hinweis: Der Array-Konstruktor in der else-Schleife entspricht {[1] = name.. ":".. value}, wodurch das erste Element des Arrays festgelegt wird.) Für den ersten H2-Header setzt es die Header["H2"] = {" H2:H2val1"}.

Bei nachfolgenden Instanzen eines Headers (z. B. H2: h2val2 in der Beispieleingabe). header[Headername] ist nicht nil, daher wird die then-Klausel ausgeführt. Dies bestimmt den nächsten verfügbaren Index im Array-Wert für headers[Headername]und setzt den Header-Wert in diesen Index. Für den zweiten H2-Header setzt er headers["H2"]= {"H2:h2val1", "h2val2"}.

```
1  for name, values in pairs(headers) do
2      local next_header_index = #combined_headers + 1
3      combined_headers[next_header_index] = table.concat(values, ",")
4  end
5  <!--NeedCopy-->
```

Nachdem die ursprünglichen Header analysiert und die Header-Tabelle ausgefüllt wurde, erstellt diese Schleife das kombined_headers-Array. Es verwendet die pairs() Funktion als for-Schleifen-Iterator.

Jeder Aufruf von pairs() gibt den Namen und den Wert des nächsten Eintrags in der Header-Tabelle zurück.

Die nächste Zeile bestimmt den nächsten verfügbaren Index im array combined_headers, und die nächste Zeile setzt dieses Array-Element auf den kombinierten Header. Es verwendet die integrierte Funktion table.concat(), die als Argumente ein Array von Strings und eine Zeichenfolge als Trennzeichen verwendet, und gibt eine Zeichenfolge zurück, die die Verkettung der Array-Strings ist, getrennt durch das Trennzeichen.

Für Werte = {"H2:h2val1", "h2val2"} ergibt dies beispielsweise "H2:h2val1, h2val2"


```
local result_str = table.concat(combined_headers, "\r\n") .. "\r\n\r\n"
<!--NeedCopy-->
```

Nachdem das Array combined_headers erstellt wurde, verkettet es die Elemente zu einer Zeichenfolge und fügt einen doppelten \r\n hinzu, der die HTTP-Header beendet.

```
return result_str
<!--NeedCopy-->
```

Gibt eine Zeichenfolge als Ergebnis der Erweiterungsfunktion COMBINE_HEADERS zurück.

Problembehandlung bei Richtlinienerweiterungen

October 5, 2021

Wenn sich Ihre Erweiterungsfunktion nicht wie erwartet verhält, können Sie die Erweiterungsprotokollierungsfunktion verwenden, um das Verhalten Ihrer Erweiterungsfunktion zu überprüfen. Sie können der Erweiterungsfunktion auch Protokollierung hinzufügen, indem Sie die benutzerdefinierte Protokollierungsfunktion verwenden, in der Sie die Protokollstufe definieren können, die auf der Citrix ADC Appliance erfasst werden soll.

Dieses Thema enthält Informationen zu:

- Erweiterungsprotokollierung
- Benutzerdefinierte Protokollierung

Erweiterungsprotokollierung

Um zu zeigen, was Ihre Erweiterungsfunktion tut, protokolliert die Erweiterungsprotokollierung die Ausführung der Funktion im Citrix ADC-Systemprotokoll (/var/log/ns.log). Die Ablaufverfolgungsprotokollierung verwendet die DEBUG-Protokollstufe, die normalerweise nicht aktiviert ist. Daher müssen Sie ALLE Log-Levels aktivieren. Anschließend können Sie die Ablaufverfolgung aktivieren, indem Sie die Option -trace des Befehls set ns extension setzen. Die verfügbaren Einstellungen sind:

- off turn off tracing (equivalent to unset ns extension -trace).
- calls trace function calls with arguments and function returns with the first return value.
- lines trace the above plus line numbers for executed lines.
- all trace the above plus local variables changed by executed lines.

Beispiel:

```
set audit syslogParams -loglevel ALL

set ns extension combine_headers -trace all
<!--NeedCopy-->
```

Jede Trace-Nachricht hat das Format

```
log-header : default NSEXTENSION Message message-number 0 : ”TRACE function
-name CALL call-number: event”
```

Hierbei gilt:

- log-header liefert Zeitstempel, die Citrix ADC IP-Adresse und die Packet Engine-ID.
- message-number ist eine fortlaufende Nummer, die die Protokollnachricht identifiziert.
- function-name ist der Name der Erweiterungsfunktion.
- call-number ist eine fortlaufende Nummer für jeden Aufruf der Erweiterungsfunktion. Es kann verwendet werden, um alle Trace-Meldungen für einen Erweiterungsfunktionsaufruf zu gruppieren.
- event ist Folgendes:
  - CALL function-name ; parameter-values gibt an, dass die Funktion mit den angegebenen Parametern aufgerufen wurde.
  - RETURN FROM function-name ; return = value gibt an, dass eine Funktion den angegebenen (ersten) Wert zurückgegeben hat. (Zusätzliche Rückgabewerte werden nicht gemeldet.)
  - LINE line-number ; variable-values gibt an, dass eine Zeile ausgeführt wurde und listet alle Variablen mit geänderten Werten auf.

Hierbei gilt:

- Wert oder Werte ist
  - eine Zahl, mit oder ohne Dezimalkomma,
  - eine Zeichenfolge, die in doppelte Anführungszeichen und mit Escape-Zeichen eingeschlossen ist, wie zuvor beschrieben
  - ein boolean true oder falsch,
  - nil,
  - ein Tabellenkonstruktor im Format {[key1]=value1,[key2]=value2,…}.
- parameter-values ist Parameter1 = Wert1; Parameter2 = Wert2,…
- Variablenwerte ist Variable1 = Wert1; Variable2 = Wert2,…

Ein Beispiel für abgekürzte Protokollmeldungen:


```
>shell tail -f /var/log/ns.log | grep TRACE | more

... NSEXTENSION Message 3035 0 : "TRACE combine_headers CALL 30 : CALL COMBINE_HEADERS; self = "User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r\nHost: 10.217.24.7\r\nAccept: \*/\*\r\nH2: h2val1\r\nH1: abcd\r\nH2: h2val2\r\nH2: h2val3\r\n\r\n""

... NSEXTENSION Message 3036 0 : "TRACE combine_headers CALL 30 : LINE 4; headers = {
 }
"

... NSEXTENSION Message 3037 0 : "TRACE combine_headers CALL 30 : LINE 5; combined_headers = {
 }
"

... NSEXTENSION Message 3038 0 : "TRACE combine_headers CALL 30 : CALL gmatch"

... NSEXTENSION Message 3039 0 : "TRACE combine_headers CALL 30 : RETURN FROM gmatch; return = function 0x2bee5a80"

... NSEXTENSION Message 3040 0 : "TRACE combine_headers CALL 30 : CALL for iterator"

... NSEXTENSION Message 3041 0 : "TRACE combine_headers CALL 30 : RETURN FROM for iterator; return = " curl/7.24.0 (amd64-portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3""

... NSEXTENSION Message 3042 0 : "TRACE combine_headers CALL 30 : LINE 9; name = "User-Agent"; value = " curl/7.24.0 (amd64-portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3""

... NSEXTENSION Message 3043 0 : "TRACE combine_headers CALL 30 : LINE 10"

... NSEXTENSION Message 3044 0 : "TRACE combine_headers CALL 30 : LINE 14; headers = {
["User-Agent"]={
[1]="User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3" }
 }
```



```
29  ”
30
31 . . .
32
33 ... NSEXTENSION Message 3117 0 : ”TRACE combine_headers CALL 30 : CALL
      for iterator”
34
35 ... NSEXTENSION Message 3118 0 : ”TRACE combine_headers CALL 30 :
      RETURN FROM for iterator; return = nil”
36
37 ... NSEXTENSION Message 3119 0 : ”TRACE combine_headers CALL 30 : LINE
      19”
38
39 ... NSEXTENSION Message 3120 0 : ”TRACE combine_headers CALL 30 : CALL
      concat”
40
41 ... NSEXTENSION Message 3121 0 : ”TRACE combine_headers CALL 30 :
      RETURN FROM concat; return = ”User-Agent: curl/7.24.0 (amd64-portbld
      -freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r\nH1: abcd\r\
      nAccept: \*/\*\r\nHost: 10.217.24.7\r\nH2: h2val1, h2val2, h2val3””
      ... NSEXTENSION Message 3122 0 : ”TRACE combine_headers CALL 30 :
      LINE 25; result_str = ”User-Agent: curl/7.24.0 (amd64-portbld-
      freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r\nH1: abcd\r\
      nAccept: \*/\*\r\nHost: 10.217.24.7\r\nH2: h2val1, h2val2, h2val3\r\
      n\r\n””
42
43 ... NSEXTENSION Message 3123 0 : ”TRACE combine_headers CALL 30 :
      RETURN FROM COMBINE_HEADERS; return = ”User-Agent: curl/7.24.0 (
      amd64-portbld-freebsd8.4) libcurl/7.24.0 OpenSSL/0.9.8y zlib/1.2.3\r
      \nH1: abcd\r\nAccept: \*/\*\r\nHost: 10.217.24.7\r\nH2: h2val1,
      h2val2, h2val3\r\n\r\n””
44 <!--NeedCopy-->
```

Benutzerdefinierte Protokollierung

Sie können auch Ihre eigene Protokollierung zu Ihrer Erweiterungsfunktion hinzufügen. Verwenden Sie dazu die integrierte ns.logger:*level*() -Funktion, wobei *level*ist: emergency, alert, critical, error, warning, notice, info oder debug. Die Parameter sind die gleichen wie die C printf () -Funktion: eine Formatzeichenfolge und eine variable Anzahl von Argumenten, die Werte für die% angeben, die in der Formatzeichenfolge angegeben werden. Beispielsweise können Sie der COMBINE_HEADERS Funktion Folgendes hinzufügen, um das Ergebnis eines Aufrufs zu protokollieren:


```
local result_str = table.concat(combined_headers, "\r\n") .. "\r\n\r\n"

ns.logger:info("Result: %s", result_str)

return result_str
<!--NeedCopy-->
```

Die obige Funktion würde die folgende Meldung nach/var/log/ns.log für die Beispieleingabe protokollieren, die in den abgekürzten Protokollnachrichtenbeispielen im Abschnitt Extension Tracing oben gezeigt wird.

```
... : default NSEXTENSION Message 143 0 : "Result: Host: 10.217.24.7:2000^M
 H1: abcd, 1234^M User-Agent: curl/7.24.0 (amd64-portbld-freebsd8.4)libcurl
/7.24.0 OpenSSL/0.9.8y zlib/1.2.3^M Accept: */*^M H2: h2val1, h2val2,
h2val3^M ^M"
```

Optimierung

October 5, 2021

Die Citrix ADC Optimierungsfunktionen reduzieren die Transaktionszeiten zwischen den Clients und den Servern und reduzieren den Bandbreitenverbrauch. Sie verbessern auch die Serverleistung, indem einige Aufgaben entlastet und andere effizienter gestaltet werden.

Feature	Beschreibung
Client Keep-Alive	Behandelt mehrere Anforderungen auf einer einzelnen Clientverbindung. Der Client muss nicht für jede Anforderung an den Server eine neue Verbindung aushandeln.
HTTP-Komprimierung	Komprimiert HTTP-Antworten, die von den Servern an komprimierungsfähige Browser gesendet werden. Die kleineren Antworten reduzieren die Download-Zeit und sparen Bandbreite.
Integriertes Caching	Speichert Antworten auf Clientanforderungen. Nachfolgende Anforderungen für denselben Inhalt werden aus dem Citrix ADC Cache bereitgestellt, anstatt an den Ursprungsserver weitergeleitet zu werden.

Feature	Beschreibung
Front-End-Optimierung	Reduziert die Lade- und Renderzeit von Webseiten durch Vereinfachung und Optimierung des an den Client-Browser bereitgestellten Inhalts. **Hinweis**: Unterstützt ab NetScaler 10.5.
Inhaltsbeschleuniger	Speichert Serverantworten auf einer Citrix ByteMobile T2100-Appliance. **Hinweis**: Unterstützt ab NetScaler 10.1.
SPDY (Speedy)	fungiert als SPDY-Gateway zwischen Clients und Ihren Servern und bietet SPDY-Unterstützung, ohne dass SPDY auf den Servern konfiguriert oder aktualisiert werden muss. **Hinweis**: Unterstützt ab NetScaler 10.1.

Kunde Keep-Alive

October 5, 2021

Die Client-Keepalive-Funktion ermöglicht das Senden von Anfragen mehrerer Clients über eine einzige Verbindung. Diese Funktion kommt dem Transaktionsmanagement zugute. Wenn der Client-Keep-Alive-Modus auf einer Appliance aktiviert ist und die Serverantwort auf die Clientanforderung die Verbindung enthält: Schließen Sie den HTTP-Header und führt die folgenden Aufgaben aus:

- Benennt den vorhandenen Connection Headernamen um, indem die Zeichen im Kopfzeilennamen gemischt werden.
- Fügt einen neuen Connection: Header mit Keep-Alive als Wert für den Header hinzu.

Der Client Keep-Alive-Modus ermöglicht es der Citrix ADC Appliance, mehrere Anfragen und Antworten über dieselbe Socket-Verbindung zu verarbeiten. Die Funktion hält die Verbindung zwischen dem Client und der Appliance (clientseitige Verbindung) auch dann geöffnet, nachdem der Server die Verbindung mit der Appliance geschlossen hat. Dies ermöglicht Anfragen mehrerer Clients über eine einzige Verbindung und speichert die beim Öffnen und Schließen einer Verbindung verbundenen Rundreisen. Client Keep-Alive ist in SSL-Sitzungen am vorteilhaftesten.

Client Keep-Alive ist für die folgenden Szenarien nützlich:

- Wenn der Server den Client Keep-Alive nicht unterstützt.

- Wenn der Server aber eine Anwendung auf dem Server unterstützt, unterstützt der Client Keep-Alive nicht.

> **Hinweis:**
> Client Keep-Alive gilt für HTTP- und SSL-Datenverkehr. Client-Keep Alive kann global konfiguriert werden, um den gesamten Datenverkehr zu bewältigen. Sie können es auch für bestimmte Dienste aktivieren.

In der Client-Keepalive-Umgebung fangen die konfigurierten Dienste den Clientdatenverkehr ab und die Clientanfrage wird an den Ursprungsserver weitergeleitet. Der Server sendet die Antwort und schließt die Verbindung zwischen dem Server und der Appliance. Wenn ein Header Verbindung: Schließen in der Serverantwort vorhanden ist, beschädigt die Appliance diesen Header in der clientseitigen Antwort und die clientseitige Verbindung bleibt offen. Daher muss der Client keine neue Verbindung für die nächste Anfrage eröffnen. Stattdessen wird die Verbindung zum Server wieder geöffnet.

> **Hinweis:**
> Wenn ein Server zwei Header "Verbindung: Schließen" zurücksendet, wird nur einer bearbeitet. Dies führt zu erheblichen Verzögerungen beim Rendern des Clients des Objekts, da ein Client nicht davon ausgeht, dass das Objekt vollständig geliefert wurde, bis die Verbindung geschlossen ist.

Konfigurieren der Client-Keepalive-Funktion

Client Keep-Alive ist standardmäßig auf dem Citrix ADC sowohl global als auch auf Service-Ebene deaktiviert. Daher müssen Sie das Feature im erforderlichen Bereich aktivieren.

> **Hinweis:**
> Wenn Sie den Client Keep-Alive global aktivieren, ist er für alle Services aktiviert, unabhängig davon, ob Sie ihn auf Service-Level aktivieren. Außerdem müssen Sie einige HTTP-Parameter konfigurieren, um Folgendes anzugeben:
>
> - die maximale Anzahl von HTTP-Verbindungen, die im Pool für die Verbindungswiederverwendung beibehalten werden.
> - aktivieren Sie das Multiplexing der Verbindung und aktivieren Sie die Persistenz `Etag`.
>
> **Hinweis:**
> Wenn Persistent aktiviert `ETag` ist, enthält der `ETag` Header Informationen über den Server, der den Inhalt bereitgestellt hat. Dadurch wird sichergestellt, dass bedingte Cache-Validierungsanforderungen oder Browseranforderungen für diesen Inhalt immer denselben Server erreichen.

Konfigurieren der Client-Keepalive-Funktion mithilfe der Citrix ADC Befehlszeilenschnittstelle

Führen Sie an der Eingabeaufforderung die folgenden Schritte aus:

1. Aktivieren Sie den Client Keep-Alive auf dem Citrix ADC.
   - Auf globaler Ebene - `enable ns mode cka`
   - Auf Service-Level - `set service <name> -CKA YES`

   > **Hinweis:**
   >
   > Client Keep-Alive kann nur für HTTP- und SSL-Dienste aktiviert werden.

2. Konfigurieren Sie HTTP-Parameter für das HTTP-Profil, das an einen oder mehrere Dienste gebunden ist.

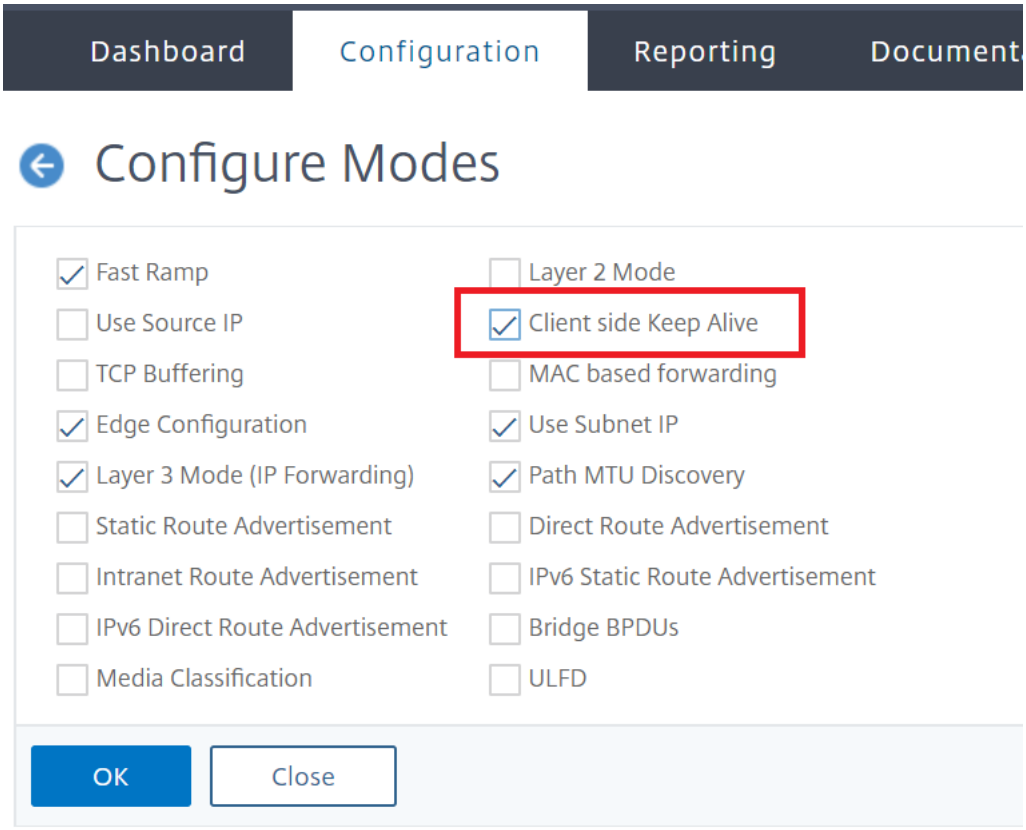
```
1 set ns httpProfile <name> -maxReusePool <value> -conMultiplex
     ENABLED -persistentETag ENABLED
2 <!--NeedCopy-->
```

> **Hinweis:**
>
> Konfigurieren Sie diese Parameter im`nshttp_default _profile HTTP`Profil, um sie global verfügbar zu machen.

Konfigurieren von Client-Keepalide mit Citrix ADC GUI

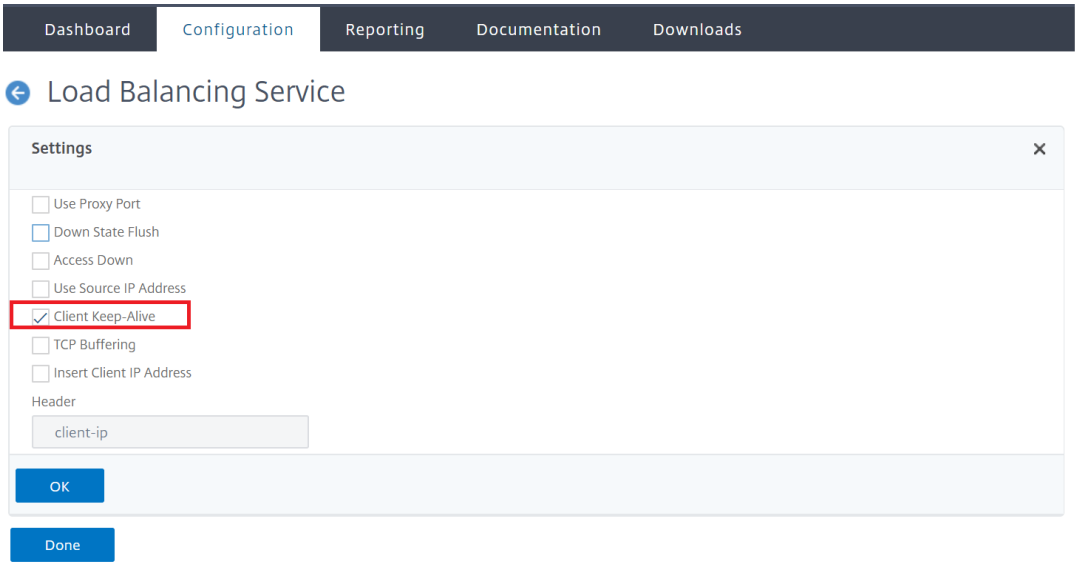
1. Aktivieren Sie den Client Keep-Alive auf dem Citrix ADC.
   - Auf globaler Ebene

     Navigieren Sie zu **System** > **Einstellungen**, klicken Sie auf **Modi konfigurieren** und wählen Sie **Client-Seite Keep Alive** aus.



- Auf Service-Ebene

  Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**, und wählen Sie den gewünschten Service aus. Aktivieren Sie im Bereich **Einstellungen** das Kontrollkästchen **Client Keep-Alive**.



2. Konfigurieren Sie die erforderlichen HTTP-Parameter für das HTTP-Profil, das an einen oder mehrere Dienste gebunden ist.
3. Navigieren Sie zu **System** > **Profile**, und wählen Sie auf der Registerkarte **HTTP-Profile** das gewünschte Profil aus, und aktualisieren Sie die erforderlichen HTTP-Parameter.

HTTP-Komprimierung

October 5, 2021

Bei Websites mit komprimierbarem Inhalt implementiert die HTTP-Komprimierungsfunktion verlustfreie Komprimierung, um Latenz, lange Downloadzeiten und andere Netzwerkleistungsprobleme zu verringern, indem die HTTP-Antworten komprimiert werden, die von Servern an komprimierungsfähige Browser gesendet werden. Sie können die Serverleistung verbessern, indem Sie die rechenintensive Komprimierungsaufgabe von Ihren Servern auf die Citrix ADC Appliance verlagern.

In der folgenden Tabelle werden die Funktionen der HTTP-Komprimierungsfunktion beschrieben:

Funktionalität	Beschreibung
Komprimierungsverhältnis	Das Komprimierungsverhältnis hängt von den Dateitypen in den Antworten ab, ist jedoch immer signifikant und reduziert die über das Netzwerk übertragene Datenmenge merklich.
Browser-Bewusstsein	Citrix ADC stellt komprimierte Daten nur für komprimierungsfähige Browser bereit, wodurch die Transaktionszeit zwischen Client und Server verkürzt wird. Die meisten modernen Webbrowser unterstützen HTTP-Komprimierung.
Komprimierungsblockierung	Sie können Inhaltsfilter definieren, um die Komprimierung selektiv zu blockieren, indem Sie integrierte Aktionen anwenden.
Komprimierungszwischenspeicherung	Wenn die integrierte Caching-Funktion aktiviert ist, werden nachfolgende Anforderungen für denselben Inhalt aus dem lokalen Cache bereitgestellt, wodurch die Anzahl der Roundtrips an den Server reduziert und die Transaktionszeiten verbessert werden.

Funktionalität	Beschreibung
HTTPS-Unterstützung	Die Komprimierung ist bei SSL-Verbindungen nützlich, da sie die Menge an Inhalten reduziert, die entweder auf dem Server oder von der Citrix ADC Appliance verschlüsselt und vom Client entschlüsselt werden müssen.
Intelligente Antwortfilterung	Die Citrix ADC Komprimierungs-Engine filtert auf intelligente Weise Serverreaktionen basierend auf definierten Komprimierungsparametern. Beispielsweise erkennt die Komprimierungs-Engine Antworten ohne Inhalt und komprimierte Antworten und komprimiert sie nicht. Die Erkennung komprimierter Antworten ermöglicht es Ursprungsstandorten, serverbasierte Komprimierung mit der Citrix ADC Komprimierungsfunktion zu verwenden.
Kompressionsschaltung	Die Citrix ADC Appliance leitet Anforderungen von komprimierungsfähigen Clients transparent an komprimierungsfähige Server weiter, sodass die Antworten auf diese Clients komprimiert werden und die Antworten auf andere Clients durch Komprimierungsverarbeitung nicht verzögert werden.

Funktionsweise der HTTP-Komprimierung

Ein Citrix ADC kann sowohl statische als auch dynamisch generierte Daten komprimieren. Es wendet den GZIP- oder den DEFLATE-Komprimierungsalgorithmus an, um fremde und sich wiederholende Informationen aus den Serverantworten zu entfernen und die ursprünglichen Informationen in einem kompakteren und effizienteren Format darzustellen. Diese komprimierten Daten werden an den Browser des Clients gesendet und nach dem vom Browser unterstützten Algorithmus oder Algorithmen (GZIP oder DEFLATE) des Browsers unkomprimiert.

Citrix ADC Komprimierung behandelt statische und dynamische Inhalte anders.

- Statische Dateien werden nur einmal komprimiert, und eine komprimierte Kopie wird im lokalen Speicher gespeichert. Nachfolgende Clientanforderungen für zwischengespeicherte

Dateien werden aus diesem Speicher gewartet.
- Dynamische Seiten werden jedes Mal dynamisch erstellt, wenn ein Client sie anfordert.

Wenn ein Client eine Anforderung an den Server sendet:

1. Die Clientanforderung kommt beim Citrix ADC an. Der ADC untersucht die Header und speichert Informationen darüber, welche Art von Komprimierung, falls vorhanden, der Browser unterstützt.
2. Der ADC leitet die Anforderung an den Server weiter und empfängt die Antwort.
3. Das Citrix ADC Komprimierungsmodul untersucht die Serverantwort auf Komprimierbarkeit, indem es mit Richtlinien übereinstimmt.
4. Wenn die Antwort einer Richtlinie entspricht, die einer Komprimierungsaktion zugeordnet ist und der Clientbrowser einen durch die Aktion angegebenen Komprimierungsalgorithmus unterstützt, wendet Citrix ADC den Algorithmus an und sendet die komprimierte Antwort an den Clientbrowser.
5. Der Client wendet den unterstützten Komprimierungsalgorithmus an, um die Antwort zu dekomprimieren.

Konfigurieren der HTTP-Komprimierung

Standardmäßig ist die Komprimierung auf dem Citrix ADC deaktiviert. Sie müssen das Feature aktivieren, bevor Sie es konfigurieren. Wenn das Feature aktiviert ist, komprimiert der ADC Serveranforderungen, die durch Komprimierungsrichtlinien angegeben werden.

So aktivieren Sie die HTTP-Komprimierung mit der CLI

Die Komprimierung kann nur für HTTP- und SSL-Dienste aktiviert werden. Sie können es global aktivieren, so dass es für alle HTTP- und SSL-Dienste gilt, oder Sie können es nur für bestimmte Dienste aktivieren.

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um die Komprimierung global oder für einen bestimmten Dienst zu aktivieren:

- `enable ns feature cmp`
  ODER
- `set service \<name\> -CMP YES`

So konfigurieren Sie die Komprimierung mit der GUI

Führen Sie einen der folgenden Schritte aus:

Um die Komprimierung global zu aktivieren, navigieren Sie zu System > Einstellungen, klicken Sie auf **Configure Basic Features**und wählen Sie HTTP-Komprimierung aus.

Um die Komprimierung für einen bestimmten Dienst zu aktivieren, navigieren Sie zu **Traffic Management > Load Balancing > Services**, wählen Sie den Dienst aus und klicken Sie auf Bearbeiten. Klicken Sie in der Gruppe Einstellungen auf das Bleistiftsymbol und aktivieren Sie die Komprimierung.

Konfigurieren einer Komprimierungsaktion

Eine Komprimierungsaktion gibt die Aktion an, die ausgeführt werden soll, wenn eine Anforderung oder Antwort mit der Regel (Ausdruck) in der Richtlinie übereinstimmt, der die Aktion zugeordnet ist. Sie können beispielsweise eine Komprimierungsrichtlinie konfigurieren, die Anforderungen identifiziert, die an einen bestimmten Server gesendet werden, und die Richtlinie einer Aktion zuordnen, die die Antwort des Servers komprimiert.

Es gibt vier integrierte Komprimierungsaktionen:

- COMPRESS: Verwendet den GZIP-Algorithmus, um Daten aus Browsern zu komprimieren, die entweder GZIP oder sowohl GZIP als auch DEFLATE unterstützen. Verwendet den DEFLATE Algorithmus, um Daten aus Browsern zu komprimieren, die nur den DEFLATE Algorithmus unterstützen. Wenn der Browser keinen Algorithmus unterstützt, wird die Antwort des Browsers nicht komprimiert.
- NOCOMPRESS: Komprimiert keine Daten.
- GZIP: Verwendet den GZIP-Algorithmus, um Daten für Browser zu komprimieren, die GZIP-Komprimierung unterstützen. Wenn der Browser den GZIP-Algorithmus nicht unterstützt, wird die Antwort des Browsers nicht komprimiert.
- DEFLATE: Verwendet den DEFLATE Algorithmus, um Daten für Browser zu komprimieren, die den DEFLATE Algorithmus unterstützen. Wenn der Browser den DEFLATE Algorithmus nicht unterstützt, wird die Antwort des Browsers nicht komprimiert.Nachdem Sie eine Aktion erstellt haben, ordnen Sie die Aktion einer oder mehreren Komprimierungsrichtlinien zu.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine Komprimierungsaktion zu erstellen:

```
add cmp action <name> <cmpType> [-addVaryHeader <addVaryHeader> -varyHeaderValue
<string>]
```

So konfigurieren Sie eine Komprimierungsrichtlinie mit der CLI

Eine Komprimierungsrichtlinie enthält eine Regel, bei der es sich um einen logischen Ausdruck handelt, der es der Citrix ADC Appliance ermöglicht, den zu komprimierenden Datenverkehr zu identifizieren.

Wenn Citrix ADC eine HTTP-Antwort von einem Server empfängt, werden die integrierten Komprimierungsrichtlinien und alle benutzerdefinierten Komprimierungsrichtlinien ausgewertet, um zu bestimmen, ob die Antwort komprimiert werden soll, und falls ja, der anzuwendende Komprimierungstyp. Die den Richtlinien zugewiesenen Prioritäten bestimmen die Reihenfolge, in der die Richtlinien mit den Anforderungen abgeglichen werden.

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine Komprimierungsrichtlinie zu erstellen:

```
add cmp policy <name> -rule <expression> -resAction <string>
```


So erstellen Sie eine Komprimierungsaktion mit der GUI

Navigieren Sie zu **Optimierung** > **HTTP-Komprimierung** > **Aktionen**, klicken Sie auf **Hinzufügen**, und erstellen Sie eine Komprimierungsaktion, um den Komprimierungstyp anzugeben, der für die HTTP-Antwort ausgeführt werden soll.

Konfigurieren einer Komprimierungsrichtlinie

Eine Komprimierungsrichtlinie enthält eine Regel, bei der es sich um einen logischen Ausdruck handelt, der es der Citrix ADC Appliance ermöglicht, den zu komprimierenden Datenverkehr zu identifizieren.

Wenn Citrix ADC eine HTTP-Antwort von einem Server empfängt, werden die integrierten Komprimierungsrichtlinien und alle benutzerdefinierten Komprimierungsrichtlinien ausgewertet, um zu bestimmen, ob die Antwort komprimiert werden soll, und falls ja, der anzuwendende Komprimierungstyp. Die den Richtlinien zugewiesenen Prioritäten bestimmen die Reihenfolge, in der die Richtlinien mit den Anforderungen abgeglichen werden.

In der folgenden Tabelle sind die integrierten HTTP-Komprimierungsrichtlinien aufgeführt. Diese Richtlinien werden global aktiviert, wenn Sie die Komprimierung aktivieren.

Integrierte Standard- oder Standard-Syntaxrichtlinie	Beschreibung
ns_nocmp_mozilla_47, ns_adv_nocmp_mozilla_	Verhindert die Komprimierung von CSS-Dateien, wenn eine Anforderung von einem Mozilla 4.7-Browser gesendet wird.
ns_cmp_mscss, ns_adv_cmp_mscss	Komprimiert CSS-Dateien, wenn die Anforderung von einem Microsoft Internet Explorer-Browser gesendet wird.
ns_cmp_msapp, ns_adv_cmp_msapp	Komprimiert Dateien, die von den folgenden Anwendungen generiert werden: Microsoft Office Word, Microsoft Office Excel, Microsoft Office PowerPoint.
ns_cmp_content_type, ns_adv_cmp_content_type	Komprimiert Daten, wenn die Antwort den Header Content-Typ enthält und Text enthält.
ns_nocmp_xml_ie, ns_adv_nocmp_xml_ie	Verhindert die Komprimierung, wenn eine Anforderung von einem Microsoft Internet Explorer-Browser gesendet wird und die Antwort einen Content-Type-Header enthält und Text oder XML enthält.

Binden einer Komprimierungsrichtlinie

Um eine Komprimierungsrichtlinie in Kraft zu setzen, müssen Sie sie entweder global binden, sodass sie für den gesamten Datenverkehr gilt, der über das Citrix ADC fließt, oder für einen bestimmten virtuellen Server, sodass die Richtlinie nur für Anforderungen gilt, deren Ziel die VIP-Adresse dieses virtuellen Servers ist.

Wenn Sie eine Richtlinie binden, weisen Sie ihr eine Priorität zu. Die Priorität bestimmt die Reihenfolge, in der die von Ihnen definierten Richtlinien ausgewertet werden. Sie können die Priorität auf eine beliebige positive Ganzzahl festlegen.

So binden Sie eine Komprimierungsrichtlinie mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um eine Komprimierungsrichtlinie global oder an einen bestimmten virtuellen Server zu binden:

- `bind cmp global <policyName> [-priority <positive_integer>] [-state ( ENABLED|DISABLED)]...`
- `bind lb vserver <vserverName> -policyName <policyName> -priority < positive_integer>.`

Wiederholen Sie diesen Befehl für jeden virtuellen Server, an den Sie die Komprimierungsrichtlinie binden möchten.

So binden Sie eine Komprimierungsrichtlinie mit der GUI

Führen Sie einen der folgenden Schritte aus:

Auf globaler Ebene Navigieren Sie zu **Optimierung** > **HTTP-Komprimierung** > **Richtlinien**, klicken Sie auf **Richtlinien-Manager**, und binden Sie die erforderlichen Richtlinien, indem Sie den entsprechenden Bindepunkt und den Verbindungstyp (Anforderung/Antwort) angeben.

Auf virtueller Serverebene

Navigieren Sie zum Lastenausgleichsserver zu **Verkehrsverwaltung** > **Lastenausgleich** > **Virtuelle Server**, wählen Sie den erforderlichen virtuellen Server aus, klicken Sie auf **Richtlinien**, und binden Sie die entsprechende Richtlinie.

Navigieren Sie für den virtuellen Server zum Content Switching zu **Traffic Management > Content Switching > Virtuelle Server**, wählen Sie den erforderlichen virtuellen Server aus, klicken Sie auf **Richtlinien**und binden Sie die entsprechende Richtlinie.

Festlegen der globalen Komprimierungsparameter für optimale Leistung

Viele Benutzer akzeptieren die Standardwerte für die globalen Komprimierungsparameter, aber Sie können möglicherweise eine effektivere Komprimierung bereitstellen, indem Sie diese Einstellungen anpassen.

> **Hinweis**
> Nachdem Sie die globalen Komprimierungsparameter konfiguriert haben, müssen Sie die Appliance nicht neu starten. Sie werden sofort auf die neuen Ströme angewendet.

In der folgenden Tabelle werden die Komprimierungsparameter beschrieben, die Sie im Citrix ADC festlegen können.

Komprimierungsparameter	Beschreibung
Quantengröße	Größe (in KB) des Puffers, der für die Akkumulation von Serverantworten verwaltet wird. Die Antworten werden komprimiert, wenn die Puffergröße diesen Wert überschreitet. Wenn Sie beispielsweise die Quantengröße auf 50 KB festlegen, komprimiert der Citrix ADC den Inhalt des Puffers, wenn seine Größe größer als 50 KB wird. Mindestwert: 1. Maximalwert: 63488 Standard: 57344.
Komprimierungsstufe	Komprimierungsebene, die auf Serverantworten angewendet wird. Mögliche Werte: Beste Geschwindigkeit, beste Kompression, optimal.
Minimale HTTP-Antwortgröße	Minimale Größe (in Byte) einer komprimierten HTTP-Antwort. Antworten, die kleiner als der von diesem Parameter angegebene Wert sind, werden gesendet, ohne komprimiert zu werden.
Umgehen der Komprimierung bei CPU-Auslastung	Citrix ADC CPU-Auslastung in Prozent, bei oder darüber, bei der keine Komprimierung durchgeführt wird. Standard: 100
Richtlinientyp*	Art der für die Komprimierung verwendeten Richtlinien. Mögliche Werte: Classic, Default Syntax. Standard: Klassisch.
Serverseitige Komprimierung zulassen	Erlauben Sie Servern, komprimierte Daten an den Citrix ADC zu senden.

Komprimierungsparameter	Beschreibung
Druckpaket komprimieren	Nach Erhalt eines Pakets mit einem TCP PUSH Flag komprimieren Sie die akkumulierten Pakete sofort, ohne darauf zu warten, dass der Quantenpuffer gefüllt wird.
Externer Cache	Ausgabe einer privaten Antwortrichtlinie, die angibt, dass die Antwortnachricht für einen einzelnen Benutzer gedacht ist und nicht von einem freigegebenen oder Proxy-Cache zwischengespeichert werden darf.

So konfigurieren Sie die HTTP-Komprimierung mit der GUI

Führen Sie einen der folgenden Schritte aus:

- Um die Komprimierung global zu aktivieren, navigieren Sie zu **System** > **Einstellungen** , klicken Sie auf **Grundfunktionen konfigurieren** und wählen Sie **HTTP-Komprimierung** aus.
- Um die Komprimierung für einen bestimmten Dienst zu aktivieren, navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services** , wählen Sie den Dienst aus, und klicken Sie auf **Bearbeiten** .
- Klicken Sie in der Gruppe **Einstellungen** auf das Bleistiftsymbol, und aktivieren Sie die **Komprimierung** .

So erstellen Sie eine Komprimierungsaktion mit der GUI

Navigieren Sie zu **Optimierung** > **HTTP-Komprimierung** > **Aktionen** , klicken Sie auf **Hinzufügen** , und erstellen Sie eine Komprimierungsaktion, um den Komprimierungstyp anzugeben, der für die HTTP-Antwort ausgeführt werden soll.

So erstellen Sie eine Komprimierungsrichtlinie über die GUI

Navigieren Sie zu**Optimierung**>**HTTP-Komprimierung**>**Richtlinien**, klicken Sie auf**Hinzufügen**und erstellen Sie eine Komprimierungsrichtlinie, indem Sie die Bedingung und die entsprechende auszuführenden Aktion angeben.

Komprimierungskonfiguration auswerten

Sie können die Komprimierungsstatistiken im Dashboard-Dienstprogramm oder in einem SNMP-Monitor anzeigen. Das Dashboard-Dienstprogramm zeigt zusammenfassende und detaillierte Statistiken in einem tabellarischen und grafischen Format an.

Optional können Sie auch Statistiken für eine Komprimierungsrichtlinie anzeigen, einschließlich der Anzahl der Anforderungen, die der Richtlinienzähler während der richtlinienbasierten Komprimierung erhöht.

> **Hinweis:**
>
> - Weitere Informationen zu den Statistiken und Diagrammen finden Sie in der Dashboard-Hilfe zur Citrix ADC Appliance.
> - Weitere Informationen zu SNMP finden Sie unterSNMP-Thema .

So zeigen Sie Komprimierungsstatistiken mit der CLI an

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Komprimierungsstatistik anzuzeigen:

1. So zeigen Sie die Zusammenfassung der Komprimierungsstatistiken an.

```
stat cmp
```

> **Hinweis:**
> Der Befehl stat cmp policy zeigt Statistiken nur für Standard-Syntaxkomprimierungsrichtlinien an.

2. So zeigen Sie Komprimierungsrichtlinientreffer und -details
show cmp policy \<name\>“an

3. So zeigen Sie detaillierte Komprimierungsstatistiken
stat cmp -detail“an

So zeigen Sie Komprimierungsstatistiken mithilfe des Dashboards an:

Im Dashboard-Dienstprogramm können Sie die folgenden Arten von Komprimierungsstatistiken anzeigen:

- Wählen Sie Komprimierung, um eine Zusammenfassung der Komprimierungsstatistiken anzuzeigen.
- Um detaillierte Komprimierungsstatistiken nach Protokolltyp anzuzeigen, klicken Sie auf Details
- Um die Rate der von der Komprimierungsfunktion verarbeiteten Anforderungen anzuzeigen, klicken Sie auf die Registerkarte Grafische Ansicht.

So zeigen Sie Komprimierungsstatistiken mithilfe von SNMP an

Sie können die folgenden Komprimierungsstatistiken mithilfe der SNMP-Netzwerkverwaltungsanwendung anzeigen.

- Anzahl der Komprimierungsanforderungen (OID: 1.3.6.1.4.1.5951.4.1.1.50.1)
- Anzahl der übertragenen komprimierten Bytes (OID: 1.3.6.1.4.1.5951.4.1.1.50.2)
- Anzahl der empfangenen komprimierbaren Bytes (OID: 1.3.6.1.4.1.5951.4.1.1.50.3)

- Anzahl der übertragenen komprimierbaren Pakete (OID: 1.3.6.1.4.1.5951.4.1.1.50.4)
- Anzahl der empfangenen komprimierbaren Pakete (OID: 1.3.6.1.4.1.5951.4.1.1.50.5)
- Verhältnis empfangener komprimierbarer Daten und übertragener komprimierter Daten (OID: 1.3.6.1.4.1.5951.4.1.1.50.6)
- Verhältnis der empfangenen Gesamtdaten zu den übermittelten Daten (OID: 1.3.6.1.4.1.5951.4.1.1.50.7)

So zeigen Sie weitere Komprimierungsstatistiken mit der GUI an

1. So zeigen Sie HTTP-Komprimierungsstatistiken an:

Navigieren Sie zu **Optimierung** > **HTTP-Komprimierung** , und klicken Sie auf **Statistiken** .

1. So zeigen Sie Statistiken einer Komprimierungsrichtlinie an.

Navigieren Sie zu **Optimierung** > **HTTP-Komprimierung** > **Richtlinien** > wählen Sie die Richtlinie aus, und klicken Sie auf **Statistiken** .

1. So zeigen Sie Statistiken einer Komprimierungsrichtlinienbezeichnung an
2. Navigieren Sie zu **Optimierung** > **HTTP-Komprimierung** > **Richtlinien** > wählen Sie eine Richtlinienbezeichnung aus, und klicken Sie auf **Statistiken** .

HTTP-Komprimierung entladen

Durch die Komprimierung auf einem Server kann sich die Leistung des Servers auswirken. Ein Citrix ADC, der sich vor Ihren Webservern befindet und für die HTTP-Komprimierung konfiguriert ist, wird die Komprimierung von statischen und dynamischen Inhalten entlastet, wodurch die CPU-Zyklen und Ressourcen des Servers gespart werden.

Sie können die Komprimierung von den Webservern auf zwei Arten entladen:

Deaktivieren Sie die Komprimierung auf den Webservern, aktivieren Sie die Citrix ADC Komprimierungsfunktion auf globaler Ebene und konfigurieren Sie Dienste für die Komprimierung.

Lassen Sie die Komprimierungsfunktion auf den Webservern aktiviert, und konfigurieren Sie die Citrix ADC Appliance, um den Header Accept Encoding aus allen HTTP-Clientanforderungen zu entfernen. Die Server senden dann unkomprimierte Antworten. Citrix ADC komprimiert die Serverantworten, bevor sie an die Clients gesendet werden.

> **Hinweis**
> Die zweite Option funktioniert nicht, wenn die Server automatisch alle Antworten komprimieren. Citrix ADC versucht nicht, eine bereits komprimierte Antwort zu komprimieren.

Der Parameter Servercmp ermöglicht es der Citrix ADC Appliance, die HTTP-Kompression zu entlasten. Dieser Parameter ist standardmäßig aktiviert, damit der Server komprimierte Daten an die Citrix ADC Appliance sendet. Um die HTTP-Komprimierung zu entlasten, müssen Sie den Parameter servercmp auf OFF setzen. Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:


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

Wiederholen Sie diesen Befehl für jeden Dienst, für den Sie die Komprimierung aktivieren möchten.

```
show service <service name>
```

Wiederholen Sie diesen Befehl für jeden Dienst, um zu überprüfen, ob die Komprimierung aktiviert ist.

```
Save config
```

```
set cmp parameter -serverCmp OFF
```

> **Hinweis:**
>
> Wenn der `Servercmp` Parameter aktiviert ist und die Appliance eine komprimierte Antwort vom Server erhält, komprimiert die Appliance die Daten nicht weiter. Stattdessen leitet es die komprimierte Antwort an den Client weiter.

Integriertes Caching

October 5, 2021

Der integrierte Cache bietet In-Memory-Speicher auf der Citrix ADC Appliance und stellt Webinhalte für Benutzer bereit, ohne dass ein Roundtrip zu einem Ursprungsserver erforderlich ist. Für statische Inhalte benötigt der integrierte Cache nur wenig anfänglich eingerichtet. Nachdem Sie die integrierte Cache-Funktion aktiviert und eine grundlegende Einrichtung durchgeführt haben (z. B. die Bestimmung der Menge des Citrix ADC Appliance-Speichers, den der Cache verwenden darf), verwendet der integrierte Cache integrierte Richtlinien zum Speichern und Bereitstellen bestimmter Arten von statischem Inhalt, einschließlich einfacher Webseiten und Bilddateien. Sie können den integrierten Cache auch so konfigurieren, dass dynamische Inhalte gespeichert und bereitgestellt werden, die von Web- und Anwendungsservern als nicht zwischenspeicherbar gekennzeichnet sind (z. B. Datenbankdatensätze und Aktienkurse).

> **Hinweis:**
>
> Der Begriff Integrated Cache kann austauschbar mit AppCache verwendet werden; beachten Sie, dass beide Begriffe aus funktionaler Sicht dasselbe bedeuten.

Wenn eine Anfrage oder Antwort mit der Regel (logischer Ausdruck) übereinstimmt, die in einer integrierten Richtlinie oder einer von Ihnen erstellten Richtlinie angegeben ist. Die Citrix ADC Appliance führt die mit der Richtlinie verknüpfte Aktion aus. Standardmäßig speichern alle Richtlinien zwischengespeicherte Objekte in der Standard-Content-Gruppe und rufen sie ab. Sie können Ihre eigenen Content-Gruppen für verschiedene Arten von Inhalten erstellen.

Damit die Appliance zwischengespeicherte Objekte in einer Content-Gruppe finden kann, können Sie Selektoren konfigurieren. Die Selektoren gleichen zwischengespeicherte Objekte mit Ausdrücken ab, oder Sie können Parameter zum Suchen von Objekten in der Content-Gruppe angeben. Wenn Sie Selektoren wie von Citrix empfohlen verwenden, konfigurieren Sie diese zuerst, damit Sie beim Konfigurieren von Content-Gruppen Selektoren angeben können. Richten Sie als Nächstes alle Inhaltsgruppen ein, die Sie hinzufügen möchten, damit sie verfügbar sind, wenn Sie die Richtlinien konfigurieren. Um die Erstkonfiguration abzuschließen, erstellen Sie Richtlinienbanken, indem Sie jede Richtlinie an einen globalen Bindepunkt oder einen virtuellen Server binden. Oder Sie können ein Label binden, das von anderen Policy-Banken aus aufgerufen werden kann.

Integriertes Caching kann mit der vorinstallierten Methode des zwischengespeicherten Objekts verbessert werden, bevor sie ablaufen. Um die Handhabung zwischengespeicherter Daten zu verwalten, können Sie in die Antworten eingefügte Caching-Header konfigurieren. Der integrierte Cache kann auch als Forward-Proxy für andere Cacheserver fungieren.

> **Hinweis:**
>
> Integriertes Caching erfordert etwas Vertrautheit mit HTTP-Anfragen und -Antworten.Informationen zur Struktur von HTTP-Daten finden Sie unter *Live HTTP-Headers* unter”<http://livehttpheaders.mozdev.org/>.”

Funktionsweise des Integrations-Cache

Der integrierte Cache überwacht HTTP- und SQL-Anforderungen, die durch die Citrix ADC Appliance fließen, und vergleicht die Anforderungen mit gespeicherten Richtlinien. Je nach Ergebnis durchsucht die integrierte Cache-Funktion entweder den Cache nach der Antwort oder leitet die Anforderung an den Ursprungsserver weiter. Bei HTTP-Anfragen dient das integrierte Caching als Teilinhalt aus dem Cache als Reaktion auf Anfragen mit einem einzelnen Bytebereich und mehreren Teilen Bytebereich.

Zwischengespeicherte Daten werden komprimiert, wenn der Client komprimierte Inhalte akzeptiert. Sie können Ablaufzeiten für eine Inhaltsgruppe konfigurieren und Einträge in einer Inhaltsgruppe selektiv ablaufen.

Daten, die aus dem integrierten Cache bereitgestellt werden, sind eine Anforderung, und Daten, die vom Ursprung bereitgestellt werden, sind ein Cache-Miss, wie in der folgenden Tabelle beschrieben.

Transaktionsart	Spezifikation
Cache-Treffer	Antworten, die die Citrix ADC Appliance aus dem Cache bereitstellt, einschließlich: Statische Objekte, zum Beispiel Bilddateien und statische Webseiten, 200 OK-Seiten, 203 Seiten ohne autorisierende Antwort, 300 Seiten mit mehreren Auswahlmöglichkeiten, 301 Seiten dauerhaft verschoben, 302 Seiten gefunden, 304 Seiten nicht geändert, Diese Antworten sind bekannt als positive Reaktionen. Die Citrix ADC Appliance speichert auch die folgenden negativen Antworten: 307 temporäre Weiterleitungsseiten, 403 Verbotene Seiten, 404 Nicht gefundene Seiten, 410 Vergessene Seiten. Um die Leistung weiter zu verbessern, können Sie die Citrix ADC Appliance so konfigurieren, dass weitere Arten von Inhalten zwischengespeichert werden.
Speicherbarer Cache Miss	Für einen speicherbaren Cache-Fehler ruft die Citrix ADC Appliance die Antwort vom Ursprungsserver ab und speichert die Antwort im Cache, bevor sie an den Client weitergeleitet wird.
Nicht speicherbarer Cache Miss	Ein nicht speicherbarer Cache-Fehler ist für das Caching ungeeignet. Standardmäßig ist jede Antwort, die die folgenden Statuscodes enthält, ein nicht speicherbares Cache-Fehlverhalten: 201, 202, 204, 205, 206 Statuscodes, Alle 4xx-Codes, außer 403, 404 und 410, 5xx Statuscodes

> **Hinweis:**
> Um dynamisches Caching in Ihre Anwendungsinfrastruktur zu integrieren, verwenden Sie die NITRO -API, um Cache-Befehle remote auszugeben. Sie können beispielsweise Trigger konfigurieren, die zwischengespeicherte Antworten ablaufen, wenn eine Datenbanktabelle aktualisiert wird.

Um die Synchronisierung zwischengespeicherter Antworten mit den Daten auf dem Ursprungsserver

sicherzustellen, konfigurieren Sie Ablaufmethoden. Wenn die Citrix ADC Appliance eine Anforderung empfängt, die einer abgelaufenen Antwort entspricht, aktualisiert sie die Antwort vom Ursprungsserver.

> **Hinweis:**
> Citrix empfiehlt, die Zeiten auf der Citrix ADC Appliance und einem oder mehreren Back-End-Servern zu synchronisieren.

Funktionsweise des dynamischen Cache

Dynamisches Caching wertet HTTP-Anforderungen und Antworten basierend auf Parameterwertpaaren, Strings, String-Mustern oder anderen Daten aus. Angenommen, ein Benutzer sucht nach Fehler 31231 in einer Fehlerberichterstattungsanwendung. Der Browser sendet die folgende Anfrage im Namen des Benutzers:

```
1     GET /mybugreportingsystem/mybugreport.dll?IssuePage&RecordId=31231&
          Template=view&TableId=1000
2
3     Host: mycompany.net
4
5     User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9)
          Gecko/2008052906 Firefox/3.0
6
7     Accept: text/html,application/xhtml+xml,application/xml;q
          =0.9,\*/\*;q=0.8
8
9     Accept-Language: en-us,en;q=0.5
10 <!--NeedCopy-->
```

In diesem Beispiel enthalten GET-Anfragen für diese Fehlerberichterstattungsanwendung immer die folgenden Parameter:

- IssuePage
- RecordID
- Vorlage
- TableId

GET-Anforderungen aktualisieren oder ändern die Daten nicht, sodass Sie diese Parameter im Caching von Richtlinien und Selektoren wie folgt konfigurieren können:

- Sie konfigurieren eine Caching-Richtlinie, die für die Zeichenfolge mybugreportingsystem und die GET-Methode in HTTP-Anforderungen sucht. Diese Richtlinie leitet Abgleichsanforderungen an eine Inhaltsgruppe für Fehler.

- In der Content-Gruppe für Bugs konfigurieren Sie einen `hit` Selektor, der verschiedenen Parameter-Wert-Paaren entspricht, einschließlich IssupEPage, RecordID usw.

> **Hinweis:**
>
> Ein Browser kann mehrere GET-Anfragen basierend auf einer Benutzeraktion senden. Im Folgenden finden Sie eine Reihe von drei separaten GET-Anfragen, die ein Browser ausgibt, wenn ein Benutzer nach einem Fehler basierend auf einer Fehler-ID sucht.

```
1     GET /mybugreportingsystem/mybugreport.dll?IssuePage&RecordId=31231&
          Template=view&TableId=1000
2
3     GET /mybugreportingsystem/mybugreport.dll?IssuePage&Template=
          viewbtns&RecordId=31231&TableId=1000
4
5     GET /mybugreportingsystem/mybugreport.dll?IssuePage&Template=
          viewbody&RecordId=31231&tableid=1000
6 <!--NeedCopy-->
```

Um diese Anfragen zu erfüllen, werden mehrere Antworten an den Browser des Benutzers gesendet, und die Webseite, die der Benutzer sieht, ist eine Zusammenstellung der Antworten.

Wenn ein Benutzer einen Fehlerbericht aktualisiert, müssen die entsprechenden Antworten im Cache mit Daten vom Original-Server aktualisiert werden. Die Fehlerberichterstattungsanwendung gibt HTTP POST-Anfragen aus, wenn ein Benutzer einen Fehlerbericht aktualisiert. In diesem Beispiel konfigurieren Sie Folgendes, um sicherzustellen, dass POST-Anforderungen die Invalidierung im Cache auslösen:

- Eine Richtlinie zur Invalidierung der Anforderung, die nach der Zeichenfolge mybugreportingsystem und der POST-HTTP-Anforderungsmethode sucht und übereinstimmende Anforderungen an die Inhaltsgruppe für Fehlerberichte leitet.
- Ein Invalidierungsselektor für die Content-Gruppe für Fehlerberichte, die zwischengespeicherten Inhalte basierend auf dem RecordID-Parameter ablaufen. Dieser Parameter wird in allen Antworten angezeigt, sodass der Invalidierungsselektor alle relevanten Elemente im Cache ablaufen kann.

Der folgende Auszug zeigt eine POST-Anforderung, die den Beispielfehlerbericht aktualisiert.

```
1     POST /mybugreportingsystem/mybugreport.dll?TransitionForm HTTP/1.1\
          r\n
2
3     User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
          Opera 7.23 [en]\r\n
```



```
4
5     Host: mybugreportingsystem\r\n
6
7     Cookie:ttSearch.134=%23options%3Afalse%23active%23owner%3Afalse%23
          unowned%3Afalse%23submitter%3Afalse%23incsub%3Atrue;
8
9     Cookie2: $Version=1\r\n
10
11    . . .
12
13    \r\n
14
15    ProjectId=2&RecordId=31231&TableId=1000&TransitionId=1&Action=
          Update&CopyProjectId=0&ReloadForm=0&State=&RecordLockId=49873+
          issues+in+HTTP&F43. . .
16 <!--NeedCopy-->
```

Wenn die Citrix ADC Appliance diese Anforderung empfängt, führt sie die folgenden Schritte aus:

- Vergleicht die Anforderung mit einer Invalidierungsrichtlinie.
- Sucht die Inhaltsgruppe, die in der Richtlinie benannt ist.
- Wendet die Invalidierungsauswahl für diese Inhaltsgruppe an und endet alle Antworten ab, die mit RecordID=31231 übereinstimmen.

Wenn ein Benutzer eine neue Anfrage für diesen Fehlerbericht ausgibt, geht die Citrix ADC Appliance an den Ursprungsserver, um aktualisierte Kopien aller Antworten zu erhalten, die mit der Berichtsinstanz verknüpft sind. Es speichert die Antworten in der Content-Gruppe und stellt sie dem Browser des Benutzers zur Verfügung, der den Bericht wieder zusammenstellt und anzeigt.

Integrierten Cache konfigurieren

Um den integrierten Cache zu verwenden, müssen Sie die Lizenz installieren und die Funktion aktivieren. Nachdem Sie den integrierten Cache aktiviert haben, speichert die Citrix ADC® -Appliance automatisch statische Objekte im Cache, wie in integrierten Richtlinien angegeben, und generiert Statistiken zum Cache-Verhalten. (Integrierte Richtlinien weisen einen Unterstrich in der Anfangsposition des Richtliniennamens auf.)

Selbst wenn die integrierten Richtlinien für Ihre Situation geeignet sind, sollten Sie die globalen Attribute ändern. Beispielsweise können Sie die Größe des Speichers der Citrix ADC Appliance ändern, der dem integrierten Cache zugewiesen ist.

Wenn Sie den Cache-Betrieb beobachten möchten, bevor Sie die Einstellungen ändern, lesen Sie “Zwischengespeicherte Objekte und Cache-Statistiken anzeigen. “

> **Hinweis:**
>
> Der Citrix ADC Cache ist ein speicherinterner Speicher, der beim Neustart der Appliance gelöscht wird.

So installieren Sie die integrierte Cache-Lizenz

- Eine integrierte Cache-Lizenz ist erforderlich.
- Rufen Sie einen Lizenzcode von Citrix ab, gehen Sie zur Befehlszeilenschnittstelle und melden Sie sich an.

Kopieren Sie an der Befehlszeilenschnittstelle die Lizenzdatei in den `/nsconfig/license` Ordner.

- Starten Sie die Citrix ADC Appliance mit folgendem Befehl neu:

```
reboot
```

So aktivieren Sie das integrierte Caching:
Wenn Sie das integrierte Caching aktivieren, beginnt die Citrix ADC Appliance mit dem Zwischenspeichern von Serverantworten. Wenn Sie keine Richtlinien oder Inhaltsgruppen konfiguriert haben, speichern die integrierten Richtlinien zwischengespeicherte Objekte in der Standardinhaltsgruppe.

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um das integrierte Caching zu aktivieren oder zu deaktivieren:

```
enable ns feature IC
```

Konfigurieren globaler Attribute für das Caching

Globale Attribute gelten für alle zwischengespeicherten Daten. Sie können die Menge des Citrix ADC Speichers angeben, die dem integrierten Cache Va Header-Einfügung zugewiesen ist. Ein Kriterium, um zu überprüfen, ob ein zwischengespeichertes Objekt bedient werden muss. Die maximale Länge eines POST-Texts, der im Cache zulässig ist, ob die Richtlinienbewertung für HTTP-GET-Anforderungen umgangen werden soll, und eine Aktion, die ergriffen werden muss, wenn eine Richtlinie nicht bewertet werden kann.

Die Cache-Speicherkapazität wird nur durch den Speicher der Hardware-Appliance begrenzt. Außerdem ist sich jede Paket-Engine (zentraler Distributions-Hub aller eingehenden TCP-Anforderungen) in der nCore Citrix ADC Appliance der Objekte bewusst, die von anderen Paket-Engines in der nCore Citrix ADC Appliance zwischengespeichert wurden.

> **Hinweis:**
>
> Wenn das globale Standardspeicherlimit auf 0 festgelegt ist und die Funktion Integriertes Caching (IC) aktiviert ist, zwischengespeichert die Appliance keine Objekte. Zum Zwischenspeichern müssen Sie explizit das globale Speicherlimit konfigurieren. Wenn Sie jedoch die Option "Festlegen von Authentifizierung, Autorisierung und Auditing-Parameter EnableStaticPage-

> Caching" aktivieren, wird in der Appliance ein Standardspeicher konfiguriert. Dieser Speicher reicht nicht aus, um große Objekte zwischenzuspeichern. Daher ist es notwendig, eine höhere Speichergrenze für IC zuzuweisen. Sie können dies ausführen, indem Sie den Befehl set cache parameter -memLimit konfigurieren. Die neue Einstellung wird erst angewendet, nachdem Sie die Konfiguration gespeichert und die Appliance neu gestartet haben.

Sie können das globale Speicherlimit ändern, das für das Caching von Objekten konfiguriert ist. Wenn Sie jedoch das globale Speicherlimit auf einen Wert aktualisieren, der unter dem vorhandenen Wert liegt (z. B. von 10 GB auf 4 GB), verwendet die Appliance weiterhin das Speicherlimit.

Dies bedeutet, dass das integrierte Caching-Limit zwar auf einen bestimmten Wert konfiguriert ist, das tatsächlich verwendete Limit höher sein kann. Dieser übermäßige Speicher wird jedoch freigegeben, wenn die Objekte aus dem Cache entfernt werden.

Die Ausgabe des Befehls show cache Parameter gibt den konfigurierten Wert (Speichernutzungslimit) und den tatsächlichen Wert an, der verwendet wird (Speichernutzungslimit (aktiver Wert)).

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1     set cache parameter [-memLimit <MBytes>] [-via <string>] [-
         verifyUsing <criterion>] [-maxPostLen <positiveInteger>] [-
         prefetchMaxPending <positiveInteger>] [-enableBypass(YES|NO)] [-
         undefAction (NOCACHE|RESET)]
2 <!--NeedCopy-->
```

Integriertes Caching durch Citrix ADC GUI aktivieren

Navigieren Sie zu **System** > **Einstellungen**, klicken Sie auf **Basisfunktionen konfigurieren**, und wählen Sie **Integriertes Caching** aus.

Konfigurieren Sie globale Einstellungen für das Caching mit der Citrix ADC GUI

Navigieren Sie zu **Optimierung** > **Integriertes Caching**, klicken Sie auf **Cache-Einstellungen ändern**, und konfigurieren Sie die globalen Einstellungen für das Caching.

Richten Sie eine integrierte Content-Gruppe, ein Musterset und Richtlinien für Integrated Cache ein

Die Citrix ADC Appliance verfügt über eine integrierte Caching-Konfiguration, die Sie zum Caching von Inhalten verwenden können. Die Konfiguration besteht aus einer Content-Gruppe namens ctx_cg_poc, einem Mustersatz namens ctx_file_extensions und einem Satz integrierter Cache-Richtlinien. In der Inhaltsgruppe ctx_cg_poc werden nur Objekte zwischengespeichert, die 500

KB oder kleiner sind. Der Inhalt wird für 86000 Sekunden zwischengespeichert, und die Speichergrenze für die Inhaltsgruppe beträgt 512 MB. Der Mustersatz ist ein indiziertes Array gemeinsamer Erweiterungen für den Dateitypabgleich.

In der folgenden Tabelle sind die mitgelieferten integrierten Caching-Richtlinien aufgeführt. Standardmäßig sind die Richtlinien an keinen Bindepunkt gebunden. Sie müssen die Richtlinien an einen Bindungspunkt binden, wenn Sie möchten, dass die Citrix ADC Appliance den Datenverkehr anhand der Richtlinien auswerten soll. Die Richtlinien speichern Objekte in der Inhaltsgruppe ctx_cg_poc.

Name der integrierten Caching-Richtlinie	Richtlinienregel
_cacheVPNStaticObjects	HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS_IN
_cacheTCPVPNStaticObjects	HTTP.REQ.URL.ENDSWITH(“.css”)
_cacheOCVPNStaticObjects	HTTP.REQ.URL.ENDSWITH(“.pdf”)
_cacheWFStaticObjects	HTTP.REQ.URL.ENDSWITH(“.js”)
_mayNoCacheReq	HTTP.RES.HEADER(“Content-Type”).CONTAINS(“application/x-javascript”)
_noCacheRest	TRUE

Cachekonfiguration leeren

Sie können eine Cache-Gruppe, Cache-Gruppen oder Cache-Objekt-Locator leeren. Im Folgenden finden Sie die Befehle zum Leeren von Cache-Objekten.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
flush cache contentgroup all
```

Beispiel

```
1          0x00000089bae000000004 DEFAULT GET  //1.1.1.1:80/html/index.
               html?name=hello
2          0x00000089bae000000005 DEFAULT GET  //1.1.1.1:80/html/index.
               html?name=hi
3
4          Flush cache contentGroup all
5          done
6
7  `flush cache contentgroup <content group name>`
8  <!--NeedCopy-->
```


Beispiel:

```
1          0x00000089bae000000004 DEFAULT GET  //1.1.1.1:80/html/index.
               html?name=hello
2          0x00000089bae000000005 DEFAULT GET  //1.1.1.1:80/html/index.
               html?name=hi
3
4          Flush cache ob -| 0x00000089bae000000004
5          done
6
7  `flush cache object (-locator <positive_integer> | (-url <URL> (-host <
       string> [-port <port>] [-groupName <string>] [-httpMethod ( GET |
       POST )]))))`
8  <!--NeedCopy-->
```

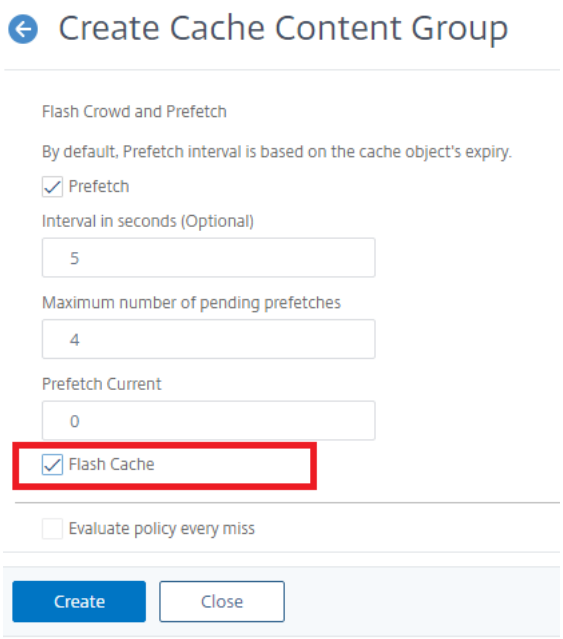
Beispiel:

```
1          0x00000089bae000000006 DEFAULT GET //1.1.1.1:80/html/index.html
2
3          flush cache ob -URL /html/index.html -host 1.1.1.1 -groupName
               DEFAULT
4          done
5  <!--NeedCopy-->
```

Leeren der Cachekonfiguration mit der Citrix ADC GUI

Führen Sie die Schritte zum Konfigurieren von Cache-Flushing mit der Citrix ADC GUI aus

1. Navigieren Sie zu **Optimierung** > **Contentgruppen**.
2. Klicken Sie im Detailbereich der **Inhaltsgruppen** auf **Hinzufügen**.
3. Legen Sie auf der Seite **Cache-Content-Gruppen erstellen** auf der Registerkarte **Sonstige** den folgenden Parameter fest:
   a) Cache leeren. Aktivieren Sie das Kontrollkästchen, um das Cache-Objekt zu leeren.
4. Klicken Sie auf **Erstellen** und **Schließen**.



Konfigurieren Sie integriertes Caching für verschiedene Szenarien

Im folgenden Abschnitt wird die Konfiguration des integrierten Cachings auf der NetScaler Appliance für verschiedene Szenarien beschrieben.

Ab der NetScaler 9.2 Version bietet das integrierte Caching mehr Speicher für das Caching. Der integrierte Caching-Speicher wird nur durch den auf der Hardware-Appliance verfügbaren Speicher begrenzt. Sie können der integrierten Caching-Funktion bis zu 50 Prozent des verfügbaren Speichers zuweisen.

So legen Sie die Speicherzuweisung für den Cache über die CLI fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cache parameter -memlimit <value>
```

> **Hinweis:**
>
> Das standardmäßige globale Speicherlimit für integriertes Caching ist Null. Selbst wenn Sie die integrierte Caching-Funktion aktivieren, speichert die NetScaler Appliance daher keine Objekte im Cache, bis das globale Speicherlimit explizit festgelegt ist.

Im folgenden Abschnitt werden Sie angewiesen, integriertes Caching für verschiedene Szenarien zu konfigurieren.

> **Hinweis:**
>
> Das Speicherlimit der NetScaler Appliance wird beim Start der Appliance identifiziert. Daher

> müssen bei Änderungen des Speicherlimits die Appliance neu gestartet werden, damit die Änderungen in den Paket-Engines anwendbar gemacht werden.

Integriertes Caching ist aktiviert und das Cache-Speicherlimit ist auf ungleich Null gesetzt

Stellen Sie sich ein Szenario vor, in dem Sie die Appliance starten, die integrierte Caching-Funktion aktiviert ist und das globale Speicherlimit auf eine positive Zahl festgelegt ist. Der Speicher, den Sie zuvor festgelegt hatten, wird während des Startvorgangs der integrierten Caching-Funktion zugewiesen. Möglicherweise möchten Sie das Speicherlimit je nach verfügbarem Speicher auf der Appliance auf einen anderen Wert ändern.

Konfigurieren über die Befehlszeile

1. Anzeigen des Cache-Parameters

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 500 MBytes
4                  Memory usage limit (active value): 500 MBytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3: 18
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
11                 Treat NOCACHE policies as BYPASS policies: YES
12                 Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```

1. Festlegen eines Speicherlimits ungleich Null

```
set cache parameter -memlimit 600
```

> **Hinweis:**
>
> Der vorangehende Befehl zeigt die folgende Warnmeldung an: **Warnung: Um ein neues Limit für den integrierten Cache zu verwenden, speichern Sie die Konfiguration und starten Sie die NetScaler Appliance neu.**

1. Speichern der Konfiguration

```
save config
```

1. Führen Sie an der Shell-Eingabeaufforderung den folgenden Befehl aus, um dies in der Konfigurationsdatei zu überprüfen.


```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Ändern Sie das Speicherlimit

```
set cache parameter -memLimit 600 -via NS-CACHE-9.3: 18 -verifyUsing
HOSTNAME_AND_IP -maxPostLen 0 -enableBypass YES -undefAction NOCACHE
```

1. Starten Sie die Appliance neu

```
root@ns## reboot
```

1. Überprüfen Sie den neuen Wert für das Speicherlimit

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 600 MBytes
4                  Memory usage limit (active value): 600 MBytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3: 18
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
11                 Treat NOCACHE policies as BYPASS policies: YES
12                 Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```

Nachdem alle Paketmodule erfolgreich gestartet wurden, verhandelt die integrierte Caching-Funktion den von Ihnen konfigurierten Speicher. Wenn die Appliance den konfigurierten Speicher nicht verwenden kann, wird der Speicher entsprechend zugewiesen. Wenn der verfügbare Speicher kleiner als der von Ihnen zugewiesene ist, empfiehlt die Appliance eine geringere Nummer. Die integrierte Caching-Funktion verwendet dasselbe wie der aktive Wert.

Integriertes Caching ist deaktiviert und das Cache-Speicherlimit ist auf ungleich Null gesetzt

In diesem Szenario ist beim Starten der Appliance die integrierte Caching-Funktion deaktiviert und das globale Speicherlimit auf eine positive Zahl festgelegt. Daher wird dem integrierten Caching während des Bootvorgangs kein Speicher zugewiesen.

Konfigurieren über die Befehlszeile

1. Anzeigen des Cache-Parameters


```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 600 MBytes
4                  Maximum value for Memory usage limit: 843 MBytes
5                  Via header: NS-CACHE-9.3: 18
6                  Verify cached object using: HOSTNAME_AND_IP
7                  Max POST body size to accumulate: 0 bytes
8                  Current outstanding prefetches: 0
9                  Max outstanding prefetches: 4294967295
10                 Treat NOCACHE policies as BYPASS policies: YES
11                 Global Undef Action: NOCACHE
12 <!--NeedCopy-->
```

1. Legen Sie ein neues Speicherlimit fest

```
set cache parameter -memlimit 500
```

> **Hinweis:**
>
> Der vorangehende Befehl zeigt die folgende Warnmeldung an: **Warnung: Funktion nicht aktiviert [IC]**.

1. Speichern der Konfiguration

```
save config
```

1. Führen Sie an der Shell-Eingabeaufforderung den folgenden Befehl aus, um dies in der Konfigurationsdatei zu überprüfen

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Ändern Sie das Speicherlimit

```
set cache parameter -memLimit 500 -via NS-CACHE-9.3: 18 -verifyUsing
HOSTNAME_AND_IP -maxPostLen 0 -enableBypass YES -undefAction NOCACHE
```

1. Überprüfen Sie den neuen Wert für das Speicherlimit

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 500 MBytes
4                  Maximum value for Memory usage limit: 843 MBytes
5                  Via header: NS-CACHE-9.3: 18
6                  Verify cached object using: HOSTNAME_AND_IP
7                  Max POST body size to accumulate: 0 bytes
8                  Current outstanding prefetches: 0
9                  Max outstanding prefetches: 4294967295
```



```
10                 Treat NOCACHE policies as BYPASS policies: YES
11                 Global Undef Action: NOCACHE
12 <!--NeedCopy-->
```

1. Aktivieren Sie die integrierte Caching-Funktion

```
enable ns feature IC
```

1. Überprüfen Sie den neuen Wert für das Speicherlimit

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 500 Mbytes
4                  Memory usage limit (active value): 500 Mbytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3: 18
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
11                 Treat NOCACHE policies as BYPASS policies: YES
12                 Global Undef Action: NOCACHE
13 <!--NeedCopy-->
```

> **Hinweis:**
>
> 500 MB Speicher werden der integrierten Caching-Funktion zugewiesen.

1. Speichern Sie die Konfiguration, um sicherzustellen, dass der Speicher beim Neustart der Appliance automatisch der Funktion zugewiesen wird.

Integriertes Caching ist aktiviert und der Cache-Speicher ist auf Null gesetzt

In diesem Szenario ist beim Starten der Appliance die integrierte Caching-Funktion aktiviert und das globale Speicherlimit auf Null festgelegt. Daher wird dem integrierten Caching während des Bootvorgangs kein Speicher zugewiesen.

Konfigurieren über die Befehlszeile

1. Überprüfen Sie die in der Datei ns.conf von der Shell-Eingabeaufforderung festgelegten Speicherlimits

```
root@ns## cat ns.conf | grep memLimit
```

1. Ändern Sie das Speicherlimit


```
set cache parameter -memLimit 0 -via NS-CACHE-9.3: 18 -verifyUsing HOSTNAME_AND_IP
 -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

1. Überprüfen Sie den Wert für das Speicherlimit

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 0 Mbytes
4                  Maximum value for Memory usage limit: 843 MBytes
5                  Via header: NS-CACHE-9.3: 18
6                  Verify cached object using: HOSTNAME_AND_IP
7                  Max POST body size to accumulate: 0 bytes
8                  Current outstanding prefetches: 0
9                  Max outstanding prefetches: 4294967295
10                 Treat NOCACHE policies as BYPASS policies: YES
11                 Global Undef Action: NOCACHE
12 <!--NeedCopy-->
```

> **Hinweis:**
>
> Das Speicherlimit ist auf 0 MB festgelegt und der integrierten Caching-Funktion wird kein Speicher zugewiesen.

1. Legen Sie die Speicherlimits fest, um sicherzustellen, dass die integrierte Caching-Funktion Objekte zwischenspeichert

```
set cache parameter -memLimit 600
```

Sobald Sie den vorhergehenden Befehl ausführen, handelt die Appliance Speicher für die integrierte Caching-Funktion aus, und der verfügbare Speicher wird der Funktion zugewiesen. Dies führt dazu, dass Appliance-Objekte zwischenspeichert, ohne die Appliance neu zu starten.

1. Überprüfen Sie den Wert für das Speicherlimit

```
1          > show cache parameter
2                  Integrated cache global configuration:
3                  Memory usage limit: 600 Mbytes
4                  Memory usage limit (active value): 600 Mbytes
5                  Maximum value for Memory usage limit: 843 MBytes
6                  Via header: NS-CACHE-9.3:
7                  Verify cached object using: HOSTNAME_AND_IP
8                  Max POST body size to accumulate: 0 bytes
9                  Current outstanding prefetches: 0
10                 Max outstanding prefetches: 4294967295
```



```
11                  Treat NOCACHE policies as BYPASS policies: YES
12                  Global Undef Action: NOCACHE
13  <!--NeedCopy-->
```

> **Hinweis:**
>
> 600 MB Arbeitsspeicher werden der integrierten Caching-Funktion zugewiesen.

1. Speichern Sie die Konfiguration. Stellen Sie sicher, dass der Speicher beim Neustart der Appliance automatisch der Funktion zugewiesen wird.
2. Überprüfen Sie die in der Datei ns.conf von der Shell-Eingabeaufforderung festgelegten Speicherlimits

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Ändern Sie das Speicherlimit

```
set cache parameter -memLimit 600 -via NS-CACHE-9.3: -verifyUsing HOSTNAME_AND_IP
 -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

Integriertes Caching ist deaktiviert und der Cache-Speicher ist auf Null gesetzt

In diesem Szenario ist beim Starten der Appliance die integrierte Caching-Funktion deaktiviert und das globale Speicherlimit auf Null festgelegt. Daher wird dem integrierten Caching während des Bootvorgangs kein Speicher zugewiesen.

Konfigurieren über die Befehlszeile

1. Überprüfen Sie die in der Datei ns.conf von der Shell-Eingabeaufforderung festgelegten Speicherlimits

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Ändern Sie das Speicherlimit

```
set cache parameter -memLimit 0 -via NS-CACHE-9.3: 18 -verifyUsing HOSTNAME_AND_IP
 -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

1. Überprüfen Sie den Wert für das Speicherlimit

```
1           > show cache parameter
2                   Integrated cache global configuration:
3                   Memory usage limit: 0 Mbytes
4                   Maximum value for Memory usage limit: 843 MBytes
5                   Via header: NS-CACHE-9.3: 18
```



```
6                   Verify cached object using: HOSTNAME_AND_IP
7                   Max POST body size to accumulate: 0 bytes
8                   Current outstanding prefetches: 0
9                   Max outstanding prefetches: 4294967295
10                  Treat NOCACHE policies as BYPASS policies: YES
11                  Global Undef Action: NOCACHE
12  <!--NeedCopy-->
```

> **Hinweis:**
>
> Das Speicherlimit ist auf 0 MB festgelegt und der integrierten Caching-Funktion wird kein Speicher zugewiesen. Wenn Sie einen Cachekonfigurationsbefehl ausführen, wird außerdem die folgende Warnmeldung angezeigt: **Warnung: Funktion nicht aktiviert [IC]**.

1. Aktivieren Sie die integrierte Caching-Funktion

```
enable ns feature IC
```

> **Hinweis:**
>
> In diesem Stadium, wenn Sie die integrierte Caching-Funktion aktivieren, weist die Appliance der Funktion keinen Speicher zu. Infolgedessen wird kein Objekt in den Speicher zwischengespeichert. Wenn Sie einen Cachekonfigurationsbefehl ausführen, wird außerdem die folgende Warnmeldung angezeigt: Für IC ist **kein Speicher konfiguriert. Verwenden Sie den Befehl set cache parameter, um das Speicherlimit festzulegen.**

1. Legen Sie die Speicherlimits fest, um sicherzustellen, dass die integrierte Caching-Funktion Objekte zwischenspeichert

```
set cache parameter -memLimit 500
```

Sobald Sie den vorhergehenden Befehl ausführen, handelt die Appliance Speicher für die integrierte Caching-Funktion aus, und der verfügbare Speicher wird der Funktion zugewiesen. Dies führt dazu, dass die Appliance Objekte zwischenspeichert, ohne die Appliance neu zu starten.

> **Hinweis:**
>
> Die Reihenfolge, in der Sie die Funktion aktivieren und die Speichergrenzen festlegen, ist wichtig. Wenn Sie die Speicherlimits festlegen, bevor Sie die Funktion aktivieren, wird die folgende Warnmeldung angezeigt: **Warnung: Funktion nicht aktiviert [IC]**.

1. Überprüfen Sie den Wert für das Speicherlimit

```
1           > show cache parameter
2                   Integrated cache global configuration:
3                   Memory usage limit: 500 Mbytes
4                   Memory usage limit (active value): 500 Mbytes
```



```
                Maximum value for Memory usage limit: 843 MBytes
                Via header: NS-CACHE-9.3:
                Verify cached object using: HOSTNAME_AND_IP
                Max POST body size to accumulate: 0 bytes
                Current outstanding prefetches: 0
                Max outstanding prefetches: 4294967295
                Treat NOCACHE policies as BYPASS policies: YES
                Global Undef Action: NOCACHE
<!--NeedCopy-->
```

> **Hinweis:**
>
> 500 MB Speicher werden der integrierten Caching-Funktion zugewiesen.

1. Speichern der Konfiguration

```
save config
```

1. Überprüfen Sie die in der Datei ns.conf von der Shell-Eingabeaufforderung festgelegten Speicherlimits

```
root@ns## cat /nsconfig/ns.conf | grep memLimit
```

1. Ändern Sie das Speicherlimit

```
set cache parameter -memLimit 500 -via NS-CACHE-9.3: 18 -verifyUsing
HOSTNAME_AND_IP -maxPostLen 4096 -enableBypass YES -undefAction NOCACHE
```

Konfigurieren von Selektoren und grundlegenden Inhaltsgruppen

October 5, 2021

Sie können Selektoren konfigurieren und auf Inhaltsgruppen anwenden. Wenn Sie einen Selektor zu einer oder mehreren Content-Gruppen hinzufügen, geben Sie an, ob der Selektor zur Identifizierung von Cache-Anfragen oder zur Identifizierung von zwischengespeicherten Objekten verwendet werden soll, die ungültig werden sollen (abgelaufen). Selektoren sind optional. Alternativ können Sie Content-Gruppen konfigurieren, um `hit` Parameter und Invalidierungsparameter zu verwenden. Citrix empfiehlt jedoch, Selektoren zu konfigurieren.

Nachdem Sie Selektoren konfiguriert haben oder sich dafür entschieden haben, stattdessen Parameter zu verwenden, können Sie eine grundlegende Content-Gruppe einrichten. Nachdem Sie die grundlegende Content-Gruppe erstellt haben, müssen Sie entscheiden, wie Objekte aus dem Cache abgelaufen werden sollen, und den Cache-Ablauf konfigurieren. Sie können den Cache weiter ändern, wie unter Verbesserung der Cache-Leistung und Konfigurieren von Cookies, Headern und Pollingbeschrieben, aber Sie möchten möglicherweise zuerst Caching-Richtlinien konfigurieren.

> **Hinweis:**
>
> Inhaltgruppenparameter und -selektoren werden nur zum Anforderungszeitpunkt verwendet, und Sie ordnen sie in der Regel Richtlinien zu, die MAY_CACHE oder MAY_NOCACHE Aktionen verwenden.

Vorteile von Selektoren

Ein Selektor ist ein Filter, der bestimmte Objekte in einer Inhaltsgruppe sucht. Wenn Sie keinen Selektor konfigurieren, sucht die Citrix® ADC-Appliance nach einer exakten Übereinstimmung in der Content-Gruppe. Dies kann dazu führen, dass sich mehrere Kopien desselben Objekts in einer Inhaltsgruppe befinden. Beispielsweise muss eine Inhaltsgruppe ohne Selektor URLs für host1.domain.commypage.htm, host2.domain.commypage.htm und host3.domain.commypage.htm speichern. Im Gegensatz dazu kann ein Selektor nur die URL (mypage.html, unter Verwendung des Ausdrucks http.req.url) und die Domäne (.com, unter Verwendung des Ausdrucks http.req.hostname.domain) übereinstimmen, sodass die Anfragen mit derselben URL erfüllt werden können.

Selektor-Ausdrücke können eine einfache Übereinstimmung von Parametern durchführen (z. B. um Objekte zu finden, die mit einigen Abfragezeichenfolgenparametern und ihren Werten übereinstimmen). Ein Selektorausdruck kann boolesche Logik, arithmetische Operationen und Kombinationen von Attributen verwenden, um Objekte zu identifizieren (z. B. Segmente eines URL-Stamms, eine Abfragezeichenfolge, eine Zeichenfolge in einem POST-Anforderungskörper, eine Zeichenfolge in einem HTTP-Header, ein Cookie). Selektoren können auch programmatische Funktionen ausführen, um Informationen in einer Anforderung zu analysieren. Beispielsweise kann ein Selektor Text in einem POST-Text extrahieren, den Text in eine Liste konvertieren und ein bestimmtes Element aus der Liste extrahieren.

Weitere Informationen zu Ausdrücken und was Sie in einem Ausdruck angeben können, finden Sie unter Richtlinien und Ausdrücke.

Parameter anstelle von Selektoren verwenden

Obwohl Citrix die Verwendung von Selektoren mit einer Content-Gruppe empfiehlt, können Sie stattdessen `hit` Parameter und Invalidierungsparameter konfigurieren. Angenommen, Sie konfigurieren drei `hit` Parameter in einer Content-Gruppe für Fehlerberichte: BugID, Issuer und Assignee. Wenn eine Anforderung BugID=456 mit Issuer=RoHitV und Assignee=Robert enthält, kann die Citrix ADC Appliance Antworten liefern, die diesen Parameterwertpaaren entsprechen.

Invalidierungsparameter in einer Content-Gruppe laufen zwischengespeicherte Einträge ab. Nehmen wir beispielsweise an, dass bugID ein Invalidierungsparameter ist und ein Benutzer eine POST-Anfrage ausgibt, um einen Fehlerbericht zu aktualisieren. Eine Invalidierungsrichtlinie leitet die Anforderung

an diese Content-Gruppe, und der Invalidierungsparameter für die Content-Gruppe läuft alle zwischengespeicherten Antworten ab, die dem BugID -Wert entsprechen. (Wenn ein Benutzer das nächste Mal eine GET-Anforderung für diesen Bericht ausgibt, kann eine Caching-Richtlinie die Citrix ADC Appliance ermöglichen, den zwischengespeicherten Eintrag für den Bericht vom Ursprungsserver zu aktualisieren.)

Beachten Sie, dass derselbe Parameter als `hit` Parameter oder Invalidationsparameter verwendet werden kann.

Inhaltsgruppen extrahieren Anforderungsparameter in der folgenden Reihenfolge:

- URL-Abfrage
- POST-Körper
- Cookie-Header

Nach dem ersten Auftreten eines Parameters, unabhängig davon, wo er in der Anforderung aufgetreten ist, werden alle nachfolgenden Vorkommen ignoriert. Wenn beispielsweise ein Parameter sowohl in der URL-Abfrage als auch im POST-Text vorhanden ist, wird nur der Parameter in der URL-Abfrage berücksichtigt.

Wenn Sie Treffer- und Invalidierungsparameter für eine Inhaltsgruppe verwenden, konfigurieren Sie die Parameter, wenn Sie die Inhaltsgruppe konfigurieren.

Hinweis: Citrix empfiehlt, Selektoren anstelle von parametrisierten Inhaltsgruppen zu verwenden, da Selektoren flexibler sind und an mehr Datentypen angepasst werden können.

Konfigurieren eines Selektors

Eine Inhaltsgruppe kann einen Trefferselektor verwenden, um Cache-Treffer abzurufen oder einen Invalidierungsselektor verwenden, um abgelaufene zwischengespeicherte Objekte zu verwenden und neue vom Ursprungsserver abzurufen.

Ein Selektor enthält einen Namen und einen logischen Ausdruck, der als *erweiterte Ausdruck* bezeichnet wird.

Weitere Informationen zu erweiterten Ausdrücken finden Sie unter Richtlinien und Ausdrücke.

Um einen Selektor zu konfigurieren, weisen Sie ihm einen Namen zu und geben einen oder mehrere Ausdrücke ein. Als bewährte Methode sollte ein Selektorausdruck den URL-Stamm und den Host enthalten, es sei denn, es gibt einen guten Grund, diese auszuschließen.

So konfigurieren Sie einen Selektor mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cache selector \<selectorName\> ( \<rule\> ... )
```


Informationen zum Konfigurieren des Ausdrucks oder der Ausdrücke finden Sie unter So konfigurieren Sie einen Selektorausdruck mithilfe der Befehlszeilenschnittstelle.

```
>add cache selector product_selector "http.req.url.query.value("
    ProductId")" "http.req.url.query.value("BatchNum")" "http.req.url.
    query.value("depotLocation")"

> add cache selector batch_selector "http.req.url.query.value("
    ProductId")" "http.req.url.query.value("BatchId")" "http.req.url.
    query.value("depotLocation")"

> add cache selector product_id_selector "http.req.url.query.value("
    ProductId")"

> add cache selector batchnum_selector "http.req.url.query.value("
    BatchNum")" "http.req.url.query.value("depotLocation")"

> add cache selector batchid_selector "http.req.url.query.value("
    depotLocation")" "http.req.url.query.value("BatchId")"

<!--NeedCopy-->
```

So konfigurieren Sie einen Selektor mit der GUI

Navigieren Sie zu **Optimierung > Integriertes Caching > Cache Selectors**, und fügen Sie den Cache-Selektor hinzu.

Inhaltsgruppen

Eine Content-Gruppe ist ein Container für zwischengespeicherte Objekte, die in einer Antwort bereitgestellt werden können. Wenn Sie den integrierten Cache zum ersten Mal aktivieren, werden zwischenspeicherbare Objekte in einer Inhaltsgruppe namens Standard gespeichert. Sie können Content-Gruppen erstellen, die über eindeutige Eigenschaften verfügen. Beispielsweise können Sie separate Inhaltsgruppen für Bilddaten, Fehlerberichte und Aktienkurse definieren, und Sie können die Inhaltsgruppe Aktienkurse so konfigurieren, dass sie häufiger aktualisiert wird als die anderen Gruppen.

Sie können den Ablauf einer gesamten Content-Gruppe oder ausgewählter Einträge in einer Content-Gruppe konfigurieren.

Die Daten in einer Content-Gruppe können wie folgt statisch oder dynamisch sein:

- **Statische Inhaltsgruppen**. Findet eine genaue Übereinstimmung zwischen dem URL-Stamm und dem Hostnamen in der Anforderung und dem URL-Stamm und dem Hostnamen der Antwort.

- **Dynamische Inhaltsgruppen**. Sucht nach Objekten, die bestimmte Parameter-Wert-Paare, beliebige Strings oder String-Muster enthalten. Dynamische Inhaltsgruppen sind nützlich, wenn Daten zwischengespeichert werden, die häufig aktualisiert werden (z. B. einen Fehlerbericht oder eine Aktienkurse).

Eine Anfrage von einer Content-Gruppe bereitstellen

1. Ein Benutzer gibt Suchkriterien für ein Element ein, z. B. einen Fehlerbericht, und klickt in einem HTML-Formular auf die Schaltfläche Suchen.
2. Der Browser gibt eine oder mehrere HTTP-GET-Anforderungen aus. Diese Anforderungen enthalten Parameter (z. B. den Fehlerbesitzer, die Fehler-ID usw.).
3. Wenn die Citrix ADC Appliance die Anforderungen empfängt, sucht sie nach einer übereinstimmenden Richtlinie. Wenn sie eine Caching-Richtlinie findet, die diesen Anforderungen entspricht, leitet sie die Anforderungen an eine Inhaltsgruppe weiter.
4. Die Content-Gruppe sucht nach geeigneten Objekten in der Content-Gruppe, basierend auf Kriterien, die Sie in einem Selektor konfigurieren.

Beispielsweise kann die Content-Gruppe übereinstimmende Antworten abrufen `NameField=username and BugID=ID`.

1. Wenn übereinstimmende Objekte gefunden werden, kann die Citrix ADC Appliance sie dem Browser des Benutzers bereitstellen, wo sie zu einer vollständigen Antwort zusammengefasst werden (z. B. einem Fehlerbericht).

Ein Objekt in einer Content-Gruppe ungültig machen

1. Ein Benutzer ändert Daten (z. B. ändert der Benutzer den Fehlerbericht und klickt auf die Schaltfläche Absenden).
2. Der Browser sendet diese Daten in Form einer oder mehrerer HTTP-Anfragen. Beispielsweise kann es einen Fehlerbericht in Form von mehreren HTTP POST-Anfragen senden, die Informationen über den Fehlerbesitzer und die Bug-ID enthalten.
3. Die Citrix ADC Appliance gleicht die Anforderungen mit Invalidierungsrichtlinien ab. In der Regel werden diese Richtlinien so konfiguriert, dass die HTTP POST-Methode erkannt wird.
4. Wenn die Anforderung mit einer Invalidierungsrichtlinie übereinstimmt, durchsucht die Citrix ADC Appliance die Inhaltsgruppe, die dieser Richtlinie zugeordnet ist, und beendet Antworten, die den konfigurierten Kriterien für die Invalidierung entsprechen.

Zum Beispiel kann ein Invaliden-Selektor die übereinstimmenden Antworten finden `NameField=username and BugID=ID`.

1. Wenn die Citrix ADC Appliance das nächste Mal eine GET-Anforderung für diese Antworten empfängt, ruft sie aktualisierte Versionen vom Ursprungsserver ab, speichert die aktualisierten Antworten und sendet diese Antworten an den Browser des Benutzers, wo sie zu einem vollständigen Fehlerbericht zusammengefasst werden.

Einrichten einer grundlegenden Content-Gruppe

Standardmäßig werden alle zwischengespeicherten Daten in der Standardinhaltsgruppe gespeichert. Sie können mehr Content-Gruppen konfigurieren und diese Content-Gruppen in einer oder mehreren Richtlinien angeben.

Sie können Inhaltsgruppen für statische Inhalte konfigurieren und Inhaltsgruppen für dynamischen Inhalt konfigurieren. Sie können die Konfiguration einer beliebigen Content-Gruppe, einschließlich der Standardgruppe, ändern.

So richten Sie eine grundlegende Inhaltsgruppe mit der Befehlszeilenschnittstelle ein

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cache contentgroup <name> (-hitSelector <hitSelectorName> -invalSelector
 <invalidationSelectorName> | -hitParams <hitParamName> -invalParams<
invalidationParamName>)-type <type> [-relExpiry <sec> | -relExpiryMilliSec
<msec>] [-heurExpiryParam <positiveInteger>]
```

```
add cache contentgroup Products_Details -hitSelector product_selector -
invalSelector id_selector
```

```
add cache contentgroup bugrep -hitParams IssuePage RecordID Template
TableId -invalParams RecordID -relExpiry 864000
```

So richten Sie eine grundlegende Content-Gruppe mit der GUI ein

Navigieren Sie zu **Optimierung > Integriertes Caching > Contentgruppen**und erstellen Sie die Content-Gruppe.

Ablaufen oder Leeren zwischengespeicherter Objekte

Wenn eine Antwort keinen Expires-Header oder einen Cache-Control-Header mit einer Ablaufzeit (Max-Age oder Smax-Age) hat, müssen Sie Objekte in einer Content-Gruppe mit einer der folgenden Methoden ablaufen:

- Konfigurieren Sie die Ablaufeinstellungen für Inhaltsgruppen, um zu bestimmen, ob und wie lange das Objekt beibehalten werden soll.
- Konfigurieren Sie eine Invalidierungsrichtlinie und -aktion für die Inhaltsgruppe. Weitere Informationen finden Sie unter Konfigurieren von Richtlinien für Caching und Invalidierung.
- Führen Sie die Content-Gruppe oder die darin enthaltenen Objekte manuell aus.

Nach Ablauf einer zwischengespeicherten Antwort aktualisiert die Citrix ADC Appliance sie, wenn der Client das nächste Mal eine Anforderung für die Antwort ausgibt. Wenn der Cache voll ist, ersetzt die Citrix ADC Appliance standardmäßig zuerst die zuletzt verwendete Antwort.

In der folgenden Liste werden Methoden zum Ablaufen zwischengespeicherter Antworten mithilfe von Einstellungen für eine Inhaltsgruppe beschrieben. In der Regel werden diese Methoden als Prozent oder in Sekunden angegeben:

- **Bedienungsanleitung** Alle Antworten in einer Inhaltsgruppe oder alle Antworten im Cache manuell ungültig machen.
- **Antwortbasiert**. Spezifische Ablaufintervalle für positive und negative Reaktionen. Der Antwortbasierte Ablauf wird nur berücksichtigt, wenn der Last-Modified Header in der Antwort fehlt.
- **Heuristisches Ablaufdatum**. Bei Antworten, die einen Last-Modifiedy-Header haben, gibt der heuristische Ablauf die Zeit an, die aus der Zeit genommen wurde, an der die Antwort geändert wurde (berechnet als die aktuelle Zeit abzüglich der zuletzt geänderten Zeit, multipliziert mit dem heuristischen Ablaufzeitwert). Wenn beispielsweise ein Last-Modified Header anzeigt, dass eine Antwort vor 2 Stunden aktualisiert wurde und die heuristische Ablaufeinstellung 10% beträgt, laufen zwischengespeicherte Objekte nach 0,2 Stunden ab. Bei dieser Methode wird davon ausgegangen, dass häufig aktualisierte Antworten häufiger abgelaufen sein müssen.
- **Absolut oder relativ**. Geben Sie eine genaue (absolute) Zeit an, zu der die Antwort jeden Tag abläuft, im HH:MM-Format, Ortszeit oder GMT. Lokale Zeit funktioniert möglicherweise nicht in allen Zeitzonen.

Der relative Ablauf gibt einige Sekunden oder Millisekunden ab dem Zeitpunkt an, zu dem ein Cache-Fehlschuss eine Reise zum Ursprungsserver bis zum Ablauf der Antwort führt. Wenn Sie den relativen Ablauf in Millisekunden angeben, geben Sie ein Vielfaches von 10 ein. Diese Form des Ablaufs funktioniert für alle positiven Antworten. Last-Modified, Expires und Cache-Control-Header in der Antwort werden ignoriert.

Absoluter und relativer Ablauf überschreibt alle Ablaufinformationen in der Antwort selbst.

- **Zum Download**. Die Option “Nach vollständiger Antwort erhalten abläuft eine Antwort ab, wenn sie heruntergeladen wird. Dies ist nützlich für häufig aktualisierte Antworten, z. B. Aktienkurse. Standardmäßig ist diese Option deaktiviert.

Durch Aktivieren von Flash Cache und Expire After Complete Response Received wird die Leistung dynamischer Anwendungen beschleunigt. Wenn Sie beide Optionen aktivieren, ruft die Citrix ADC Appliance nur eine Antwort für einen Block gleichzeitiger Anforderungen ab.

- **Geheftet**. Wenn der Cache voll ist, ersetzt die Citrix ADC Appliance standardmäßig zuerst die zuletzt verwendete Antwort. Die Citrix ADC Appliance wendet dieses Verhalten nicht auf Inhaltsgruppen an, die als angeheftet markiert sind.

Wenn Sie keine Ablaufeinstellungen für eine Content-Gruppe konfigurieren, finden Sie im Folgenden weitere Optionen für ablaufende Objekte in der Gruppe:

- Konfigurieren Sie eine Richtlinie mit einer INVAL-Aktion, die für die Inhaltsgruppe gilt.

- Geben Sie die Namen von Inhaltsgruppen ein, wenn Sie eine Richtlinie konfigurieren, die eine INVAL-Aktion verwendet.

Wie Ablaufmethoden angewendet werden

Das Ablaufdatum funktioniert anders für positive und negative Antworten. Positive und negative Antworten sind in der unten genannten Tabelle, *Ablauf positiver und negativer Antworten* beschrieben.

Im Folgenden finden Sie Faustregeln zum Verständnis der Ablaufmethode, die auf eine Inhaltsgruppe angewendet wird:

- Sie können steuern, ob die Citrix ADC Appliance Antwortheader auswertet, wenn Sie entscheiden, ob ein Objekt abläuft.
- Absoluter und relativer Ablauf führt dazu, dass die Citrix ADC Appliance die Antwortheader ignoriert (sie überschreiben alle Ablaufinformationen in der Antwort).
- Heuristische Ablaufeinstellungen und Schwache Positive und Schwache Negative (als **Standardwerte** im Konfigurationsprogramm bezeichnet) veranlassen die Citrix ADC Appliance, die Antwortheader zu untersuchen. Diese Einstellungen funktionieren wie folgt zusammen:
  - Der Wert in einem Expires- oder Cache-Control-Header überschreibt diese Inhaltsgruppeneinstellungen.
  - Für positive Antworten, die keinen Expire- oder Cache-Control-Header haben, aber einen Last-Modified Header haben, vergleicht die Citrix ADC Appliance heuristische Ablaufeinstellungen mit dem Headerwert.
  - Für positive Antworten, denen ein Expires-, Cache-Control- oder Last-Modified-Header fehlt, verwendet die Citrix ADC Appliance den “schwachen positiven” Wert.
  - Für negative Antworten, denen ein Expires- oder Cache-Control-Header fehlt, verwendet die Citrix ADC Appliance den “schwachen negativen” Wert.

In der folgenden Tabelle wird beschrieben, wie diese Methoden angewendet werden.

Typ der Antwort	Ablauf-Header-Typ	Inhaltsgruppeneinstellung	Zeitraum, in dem das Objekt im Cache verbleibt
Positiv	Beliebiger Header	Inhalte ablaufen nach (relExpiry) ohne andere Einstellungen	Verwenden Sie den Wert der Einstellung “ **Inhalt ablaufen nach** “.
Positiv	Beliebiger Header	Inhalt abläuft ab (absExpiry) ohne andere Einstellungen	Subtrahieren Sie das aktuelle Datum vom Wert der Einstellung **Inhalt ablaufen um**.

Typ der Antwort	Ablauf-Header-Typ	Inhaltsgruppeneinstellung	Zeitraum, in dem das Objekt im Cache verbleibt
Positiv	Beliebiger Header	Inhalt ablaufen nach (relExpiry) und Inhalt ab (absExpiry)	Verwenden Sie den kleineren der beiden Werte für die Inhaltsgruppeneinstellungen. Siehe die vorherigen Zeilen in dieser Tabelle.
Positiv	Zuletzt geändert (mit anderen Headern)	Heuristic (heurExpiry Param) mit jeder anderen Einstellung	Subtrahieren Sie das Datum Letzte Änderung vom aktuellen Datum, multiplizieren Sie das Ergebnis mit dem Wert der heuristischen Ablaufeinstellung und dividieren Sie dann durch 100.
Positiv	Zuletzt geändert (mit anderen Headern)	Standard (positiv) (weakPosRel Expiry) und keine andere Einstellung	Verwenden Sie den Wert der Standardeinstellung (positiv) Ablaufdatum.
Positiv	Läuft ab oder Cache-Control: Max-Age-Header vorhanden ist	Zuletzt geändert Header ist nicht vorhanden, Heuristisch (HeureXpiry Param), Default (positiv) (WeakPosRel Expiry) oder beides	Ziehen Sie das aktuelle Datum vom Ablauf oder dem `Cache-Control: Max-Age` Datum ab.
Positiv	no caching headers	Standard (positiv) (weakPosRel Expiry) und jede andere Ablaufeinstellung	Verwenden Sie den Wert der Standardeinstellung (positiv).

Typ der Antwort	Ablauf-Header-Typ	Inhaltsgruppeneinstellung	Zeitraum, in dem das Objekt im Cache verbleibt
Positiv	no caching headers	Heuristisch (heurExpiry Param) ist vorhanden, Standard (positiv) (weakPosRel Expiry)-Einstellung ist nicht vorhanden.	Wenn der Last-Modified Header nicht vorhanden ist, wird die Antwort nicht zwischengespeichert oder mit dem Status Bereits abgelaufen zwischengespeichert. Wenn der Last-Modified Header vorhanden ist, verwenden Sie den heuristischen Ablaufwert.
Negativ	Läuft ab oder `Cache-Control:Max-Age`	Inhalt ablaufen nach (relExpiry), Inhalt ab (absExpiry) oder beide Einstellungen	Subtrahieren Sie das aktuelle Datum vom Wert des Expires-Headers, oder verwenden Sie den Wert des Cache-Control:Max-Age-Headers.
Negativ	Läuft ab oder Cache-Control-Header fehlen	Inhalt ablaufen nach (relExpiry), Inhalt ab (absExpiry) oder beide Einstellungen	Antwort wird nicht zwischengespeichert oder mit dem Status Bereits abgelaufen zwischengespeichert.
Negativ	Läuft ab oder `Cache-Control:Max-Age`	Beliebige Einstellung	Ziehen Sie das aktuelle Datum vom Ablauf oder vom `Cache-Control:Max-Age` Datum ab.

Typ der Antwort	Ablauf-Header-Typ	Inhaltsgruppeneinstellung	Zeitraum, in dem das Objekt im Cache verbleibt
Negativ	Abläuft und Cache-Control:Max-Age-Header fehlen	Standard (negativ) (weakNegRel Expiry)	Verwenden Sie den Wert der Standardeinstellung (negativ).
Negativ	Abläuft und Cache-Control:Max-Age-Header fehlen	Jede andere Einstellung als Standard (negativ) (weakNegRel Expiry)	Das Objekt wird nicht zwischengespeichert oder mit dem Status Bereits abgelaufen zwischengespeichert.

Ablaufen einer Inhaltsgruppe nach manueller Methode

Sie können alle Einträge in einer Inhaltsgruppe manuell ablaufen.

So löschen Sie alle Antworten in einer Inhaltsgruppe mit der Befehlszeilenschnittstelle manuell ab

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
expire cache contentGroup <name>
```

So löschen Sie alle Antworten in einer Content-Gruppe mit der GUI manuell ab

Navigieren Sie zu **Optimierung > Integriertes Caching > Content-Gruppen**, wählen Sie die Content-Gruppe aus und klicken Sie auf Invalidate, um alle Antworten in einer Content-Gruppe abzulassen.

So laufen Sie alle Antworten im Cache mit der GUI manuell ab

Navigieren Sie zu **Optimierung > Integriertes Caching > Content-Gruppen**und klicken Sie auf Alle ungültig machen, um alle Antworten im Cache abzufliegend zu lösen.

Konfigurieren des periodischen Ablaufs einer Content-Gruppe

Sie können eine Inhaltsgruppe so konfigurieren, dass sie einen selektiven oder vollständigen Ablauf ihrer Einträge durchführt. Das Ablaufintervall kann festgelegt oder relativ sein.

So konfigurieren Sie den Ablauf der Inhaltsgruppe mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cache contentgroup \<name> (-relExpiry|-relExpiryMilliSec|-absExpiry
|-absExpiryGMT| -heurExpiryParam|-weakPosRelExpiry|-weakNegRelExpiry| -
expireAtLastBye)\<expirationValue>
```


So konfigurieren Sie den Ablauf der Inhaltsgruppe mit der GUI

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Inhaltsgruppen**, wählen Sie die Inhaltsgruppe aus, und geben Sie die Ablaufmethode an.

Einzelne Antworten ablaufen

Das Auslaufen einer Antwort zwingt die Citrix ADC Appliance, eine aktualisierte Kopie vom Ursprungsserver abzurufen. Antworten, die beispielsweise keine Validatoren `ETag` oder zuletzt geänderte Header haben, können nicht erneut validiert werden. Infolgedessen hat das Leeren dieser Antworten die gleiche Wirkung wie das Ablaufen dieser Antworten.

Um eine zwischengespeicherte Antwort in einer Inhaltsgruppe für statische Daten abzurufen, können Sie eine URL angeben, die mit der gespeicherten URL übereinstimmen muss. Wenn die zwischengespeicherte Antwort Teil einer parametrisierten Content-Gruppe ist, müssen Sie den Gruppennamen und den genauen URL-Stamm angeben. Der Hostname und die Portnummer müssen mit dem Host HTTP-Request-Header der zwischengespeicherten Antwort übereinstimmen. Wenn der Port nicht angegeben ist, wird Port 80 angenommen.

So löschen Sie einzelne Antworten in einer Inhaltsgruppe mit der Befehlszeilenschnittstelle ab

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
expire cache object -url <URL> -host <hostName> [-port <port>] [-groupName<
contentGroupName>] [-httpMethod GET|POST]
```

So löschen Sie einzelne Antworten in einer Content-Gruppe mit der CLI ab

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
expire cache object -locator <positiveInteger>
```

So laufen Sie eine zwischengespeicherte Antwort mit der GUI ab

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Cache-Objekte**, wählen Sie die zwischengespeicherte Antwort aus und laufen ab.

So laufen Sie eine Antwort mit der GUI ab

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Gecachte Objekte**, klicken Sie auf **Suchen**, und legen Sie die Suchkriterien fest, um die erforderliche zwischengespeicherte Antwort zu finden und abzurufen.

Leeren von Antworten in einer Content-Gruppe

Sie können alle Antworten in einer Inhaltsgruppe, einige Antworten in einer Gruppe oder alle Antworten im Cache entfernen oder löschen. Durch das Leeren einer zwischengespeicherten Antwort wird Speicher für neue zwischengespeicherte Antworten freigegeben.

> **Hinweis:**
>
> Um Antworten für mehr als ein Objekt gleichzeitig zu leeren, verwenden Sie die Konfigurationsdienstprogrammmethode. Die Befehlszeilenschnittstelle bietet diese Option nicht.

So leeren Sie Antworten aus einer Inhaltsgruppe mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
flush cache contentGroup <name> [-query <queryString> | [-selectorValue <
selectorExpressionIDList> -host <hostName>]]
```

So leeren Sie Antworten aus einer Inhaltsgruppe mit der GUI

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Contentgruppen**.
2. Lege die Antworten im Detailbereich wie folgt fest:
   - Um alle Antworten in allen Inhaltsgruppen zu leeren, klicken Sie auf Alle ungültig machen, und leeren Sie alle Antworten.
   - Um Antworten in einer bestimmten Inhaltsgruppe zu löschen, wählen Sie die Inhaltsgruppe aus, klicken Sie auf **ungültig**, und leeren Sie alle Antworten.

> **Hinweis**:
> Wenn diese Inhaltsgruppe einen Selektor verwendet, können Sie Antworten selektiv leeren, indem Sie eine Zeichenfolge in das Textfeld Selektor eingeben und einen Hostnamen in das Textfeld Host eingeben. Klicken Sie dann auf **Flush und OK**. Der Selector-Wert kann eine Abfragezeichenfolge mit bis zu 2319 Zeichen sein, die für die parametrisierte Invalidierung verwendet wird.

Wenn die Content-Gruppe einen Invalidierungsparameter verwendet, können Sie Antworten selektiv löschen, indem Sie eine Zeichenfolge in das Feld **Abfrage** eingeben.

Wenn die Content-Gruppe einen Invalidierungsparameter verwendet und Invalidate Objekte, die zum Ziel-Host gehören, konfiguriert ist, geben Sie Zeichenfolgen in die Felder **Abfrage und Host** ein.

So leeren Sie eine zwischengespeicherte Antwort mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
flush cache object -locator <positiveInteger> | -url <URL> -host <hostName>
 [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET|POST]
```

So leeren Sie eine zwischengespeicherte Antwort mit der GUI

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Gecachte Objekte**, wählen Sie das zwischengespeicherte Objekt aus und leeren Sie es.

Löschen einer Inhaltsgruppe

Sie können eine Inhaltsgruppe entfernen, wenn sie nicht von einer Richtlinie verwendet wird, die Antworten im Cache speichert. Wenn die Inhaltsgruppe an eine Richtlinie gebunden ist, müssen Sie die Richtlinie zuerst entfernen. Wenn Sie die Inhaltsgruppe entfernen, werden alle in dieser Gruppe gespeicherten Antworten entfernt.

Sie können die Gruppe Default, BASEFILE oder Deltas nicht entfernen. Die Standardgruppe speichert zwischengespeicherte Antworten, die keiner anderen Inhaltsgruppe angehören.

So löschen Sie eine Inhaltsgruppe mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm cache contentgroup <name>
```

So löschen Sie eine Inhaltsgruppe mit der GUI

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Inhaltsgruppen,** wählen Sie die Content-Gruppe aus, und löschen Sie sie.

Konfigurieren von Richtlinien für Caching und Invalidierung

October 5, 2021

Mithilfe von Richtlinien kann der integrierte Cache ermitteln, ob eine Antwort aus dem Cache oder dem Ursprung bereitgestellt werden soll. Die NetScaler Appliance bietet integrierte Richtlinien für integriertes Caching, und Sie können weitere Richtlinien konfigurieren. Wenn Sie eine Richtlinie konfigurieren, ordnen Sie sie einer Aktion zu. Eine Aktion speichert entweder die Objekte, auf die die Richtlinie angewendet wird, oder ungültig (läuft ab) die Objekte. In der Regel basieren Sie Caching-Richtlinien auf Informationen in GET und POST-Anforderungen. In der Regel basieren Sie Invalidierungsrichtlinien auf dem Vorhandensein der POST-Methode in Anforderungen zusammen mit anderen Informationen. Sie können alle Informationen in einer GET- oder POST-Anforderung in einer Caching- oder Invalidierungsrichtlinie verwenden.

Sie können einige der integrierten Richtlinien im Knoten Richtlinien des integrierten Caches im Konfigurationsdienstprogramm anzeigen. Die integrierten Richtliniennamen beginnen mit einem Unterstrich (_).

Aktionen bestimmen, was die NetScaler Appliance durchführt, wenn der Datenverkehr mit einer Richtlinie übereinstimmt. Folgende Aktionen sind verfügbar:

- **Caching-Aktionen**. Richtlinien, die Sie mit der CACHE-Aktion verknüpfen, speichern Antworten im Cache und dienen sie aus dem Cache.

- **Ungültigkeitsaktionen**. Richtlinien, die Sie der INVAL-Aktion zuordnen, laufen sofort zwischengespeicherte Antworten ab und aktualisieren sie vom Ursprungsserver. Bei webbasierten Anwendungen bewerten Invalidierungsrichtlinien häufig POST-Anfragen.
- **Aktionen "Kein Cache"**. Richtlinien, die Sie einer NOCACHE-Aktion zuordnen, speichern niemals Objekte im Cache.
- **Provisorische Zwischenspeicherung von Aktionen**. Richtlinien, die Sie mit einer MAYCACHE- oder MAYNOCACHE-Aktion verknüpfen, hängen vom Ergebnis weiterer Richtlinienbewertungen ab.

Obwohl der integrierte Cache keine durch die LOCK-Methode angegebenen Objekte speichert, können Sie zwischengespeicherte Objekte nach Erhalt einer `LOCK` Anforderung ungültig machen. Nur für Invalidierungsrichtlinien können Sie mithilfe des Ausdrucks `LOCK` als Methode angeben `http.req.method.eq( "lock" )`. Im Gegensatz zu Richtlinien für `GET` und `POST` Anfragen müssen Sie die LOCK-Methode in Anführungszeichen einschließen, da die NetScaler Appliance diesen Methodennamen nur als Zeichenfolge erkennt.

Nachdem Sie eine Richtlinie erstellt haben, binden Sie sie an einen bestimmten Punkt in der Gesamtverarbeitung von Anforderungen und Antworten. Obwohl Sie eine Richtlinie erstellen, bevor Sie sie binden, müssen Sie verstehen, wie sich die Bindepunkte auf die Reihenfolge der Verarbeitung auswirken, bevor Sie Ihre Richtlinien erstellen.

Die an einen bestimmten Bindepunkt gebundenen Richtlinien stellen eine Richtlinienbank dar. Sie können goto Ausdrücke verwenden, um die Reihenfolge der Ausführung in einer Richtlinienbank zu ändern. Sie können Richtlinien auch in anderen Richtlinienbanken aufrufen. Darüber hinaus können Sie Labels erstellen und Richtlinien an diese binden. Ein solches Label ist nicht mit einem Verarbeitungspunkt verknüpft, aber die an ihn gebundenen Richtlinien können von anderen Richtlinienbanken aufgerufen werden.

Aktionen, die mit integrierten Caching-Richtlinien verknüpft werden sollen

In der folgenden Tabelle werden Aktionen für integrierte Caching-Richtlinien beschrieben.

Aktion	Spezifikation
CACHE	Dient einer Antwort aus dem Cache, wenn die Antwort noch nicht abgelaufen ist. Wenn die Antwort vom Ursprungsserver abgerufen werden muss, speichert die NetScaler Appliance die Antwort, bevor sie bereitgestellt wird. Auch Daten, die aktualisiert und häufig aufgerufen werden, können zwischengespeichert werden. Beispielsweise werden Aktienkurse häufig aktualisiert, können aber zwischengespeichert werden, damit sie schnell mehreren Benutzern zugestellt werden können. Gegebenenfalls können zwischengespeicherte Daten unmittelbar nach dem Herunterladen aktualisiert werden. Eine CACHE-Aktion kann durch integrierte Richtlinien außer Kraft gesetzt werden.
NOCACHE	Ruft die Antwort immer vom Ursprungsserver ab und markiert die Antwort als nicht speicherbar. Normalerweise konfigurieren Sie NOCACHE-Richtlinien für vertrauliche oder personalisierte Daten.

Aktion	Spezifikation
MAY_CACHE	Wird in einer Anforderungszeitrichtlinie verwendet, ermöglicht diese Einstellung vorläufig, dass eine Antwort in einer Inhaltsgruppe gespeichert wird und die Auswertung der Antwortzeitrichtlinien aussteht. Folgende Möglichkeiten sind möglich: 1. Wenn eine übereinstimmende Antwortzeitrichtlinie über eine CACHE-Aktion verfügt, aber keine Inhaltsgruppe angibt, wird die Antwort in der Standardgruppe gespeichert, es sei denn, integrierte Richtlinien überschreiben diese Richtlinie. 2. Wenn eine übereinstimmende Antwortzeitrichtlinie über eine CACHE-Aktion verfügt und dieselbe Inhaltsgruppe wie die in der Anforderungszeitrichtlinie angibt, wird die Antwort in der benannten Inhaltsgruppe gespeichert, es sei denn, integrierte Richtlinien überschreiben diese Richtlinie. 3. Wenn eine übereinstimmende Antwortzeitrichtlinie über eine CACHE-Aktion verfügt, aber eine andere Inhaltsgruppe als die in der Anforderungszeitrichtlinie angibt, wird eine NOCACHE-Aktion angewendet. 4. Wenn eine übereinstimmende Antwortzeitrichtlinie über eine NOCACHE-Aktion verfügt, führen Sie eine NOCACHE-Aktion aus. 5. Wenn keine übereinstimmende Antwortzeitrichtlinie vorhanden ist, wird eine CACHE-Aktion angewendet, es sei denn, eine integrierte Richtlinie überschreibt diese Richtlinie.

Aktion	Spezifikation
MAY_NOCACHE	Bei einer Anforderungsrichtlinie verhindert diese Einstellung provisorisch das Zwischenspeichern der Antwort. Zur Reaktionszeit wird eine der folgenden Aktionen durchgeführt Wenn keine Reaktionszeitrichtlinie mit der Anfrage übereinstimmt, ist die letzte Aktion NOCACHE. - Wenn eine übereinstimmende Antwortzeitrichtlinie eine CACHE-Aktion enthält, ist die letzte Aktion CACHE, es sei denn, integrierte Richtlinien überschreiben diese Richtlinie. - Wenn eine übereinstimmende Antwortzeitrichtlinie eine NOCACHE-Aktion enthält, ist die letzte Aktion NOCACHE. -Wenn eine übereinstimmende Antwortzeitrichtlinie über eine CACHE-Aktion verfügt, aber keine Inhaltsgruppe angibt, besteht die letzte Aktion darin, die Antwort in der Standardinhaltsgruppe CACHE zu CACHE, es sei denn, integrierte Richtlinien überschreiben diese Richtlinie.
INVAL	Läuft zwischengespeicherte Antworten ab. Je nachdem, wie die Richtlinie und die Inhaltsgruppe konfiguriert sind, sind alle Antworten in einer oder mehreren Inhaltsgruppen abgelaufen, oder ausgewählte Objekte in der Inhaltsgruppe sind abgelaufen. Hinweis: Sie können INVAL-Aktionen nur in Anforderungszeitrichtlinien angeben.

Punkte für eine Richtlinie binden

Sie können die Richtlinie an einen der folgenden Bindungspunkte binden:

- **Eine globale Richtlinienbank**. Dies sind die Standardeinstellung für die Anforderungszeit, die Überschreibung der Anforderungszeit, der Ausfall der Reaktionszeit und die Policy-Banken zur Überschreibung der Antwortzeit, wie unter “Reihenfolge der Richtlinienbewer-

tungbeschrieben. “

- **Ein virtueller Server**. Richtlinien, die Sie an einen virtuellen Server binden, werden nach den globalen Überschreibungsrichtlinien und vor den globalen Standardrichtlinien verarbeitet, wie unter “Reihenfolge der Richtlinienbewertungbeschrieben. “ Wenn Sie eine Richtlinie an einen virtuellen Server binden, binden Sie sie entweder an die Anforderungszeit- oder Antwortzeitverarbeitung.
- **Ein Ad-hoc-Richtlinienlabel**. Ein Richtlinienlabel ist ein Name, der einer Richtlinienbank zugewiesen wird. Zusätzlich zu den globalen Labels verfügt der integrierte Cache über zwei integrierte benutzerdefinierte Richtlinienlabels:
  - _reqBuiltinDefaults. Diese Richtlinienbezeichnung wird standardmäßig von der Standardrichtlinienbank für die Anforderung aufgerufen.
  - _resBuiltinDefaults. Diese Richtlinienbezeichnung wird standardmäßig von der Standardrichtlinienbank für die Antwortzeit aufgerufen.

Sie können auch neue Richtlinienbeschriftungen definieren. Richtlinien, die an ein benutzerdefiniertes Richtlinienlabel gebunden sind, müssen innerhalb einer Richtlinienbank für einen der integrierten Bindungspunkte aufgerufen werden.

> **Wichtig:**
> Sie müssen eine Richtlinie mit einer INVAL-Aktion an eine Anforderungszeitüberschreibung oder einen Antwortzeit Override-Bindungspunkt binden. Um eine Richtlinie zu löschen, müssen Sie zuerst die Bindung aufheben.

Reihenfolge der Evaluierung der Richtlinie

Damit eine erweiterte Richtlinie wirksam wird, müssen Sie sicherstellen, dass die Richtlinie zu einem bestimmten Zeitpunkt während der Verarbeitung des Datenverkehrs durch die NetScaler Appliance aufgerufen wird. Um die Aufrufzeit anzugeben, ordnen Sie die Richtlinie einem Bindepunkt zu. Die folgenden Punkte sind in der Reihenfolge der Auswertung aufgeführt:

- **Überschreiben der Anforderungszeit**. Wenn eine Anforderung einer Richtlinie für die Überschreibung der Anforderungszeit entspricht, endet standardmäßig die Auswertung der Anforderungszeitrichtlinie, und die NetScaler Appliance speichert die Aktion, die mit der Vergleichsrichtlinie verknüpft ist.
- **Anforderungszeit-Lastausgleich virtueller Server**. Wenn die Richtlinienbewertung nicht abgeschlossen werden kann, nachdem alle Richtlinien für die Anforderungszeitüberschreibung ausgewertet wurden, verarbeitet die NetScaler Appliance Anforderungszeitrichtlinien, die an den Lastausgleich von virtuellen Servern gebunden sind. Wenn die Anforderung mit einer dieser Richtlinien übereinstimmt, endet die Bewertung, und die NetScaler Appliance speichert die Aktion, die mit der Vergleichsrichtlinie verknüpft ist.
- **Anforderungszeit virtueller Content Switching-Server**. Richtlinien, die an diesen

Bindungspunkt gebunden sind, werden nach den Richtlinien für die Anforderungszeit ausgewertet, die an den Lastausgleich virtueller Server gebunden sind.

- **Standardwert für Anforderungszeit**. Wenn die Richtlinienbewertung nicht abgeschlossen werden kann, nachdem alle anforderungszeitlichen Richtlinien ausgewertet wurden, verarbeitet die NetScaler Appliance die Standardrichtlinien für die Anforderungszeit. Wenn die Anforderung mit einer Standardrichtlinie zur Anforderungszeit übereinstimmt, endet die Auswertung der Anforderungszeitrichtlinie standardmäßig und die NetScaler Appliance speichert die Aktion, die mit der Vergleichsrichtlinie verknüpft ist.
- **Überschreiben der Reaktionszeit**. Ähnlich wie die Richtlinienbewertung für die Anforderungszeitüberschreibung.
- **Reaktionszeit-Lastenausgleich virtueller Server**. Ähnlich wie bei der Auswertung der virtuellen Serverrichtlinien für die Anforderung.
- **Anwortzeit virtueller Content Switching-Server**. Ähnlich wie bei der Auswertung der virtuellen Serverrichtlinien für die Anforderung.
- **Standardwert für die Reaktionszeit**. Ähnlich wie die Standardrichtlinienbewertung für die Anforderungszeit.

Sie können jedem Bindepunkt mehrere Richtlinien zuordnen. Um die Reihenfolge der Auswertung der Richtlinien zu steuern, die mit dem Bindepunkt verknüpft sind, konfigurieren Sie eine Prioritätsstufe. In Ermangelung anderer Flusssteuerungsinformationen werden Richtlinien entsprechend der Prioritätsstufe ausgewertet, beginnend mit dem niedrigsten numerischen Prioritätswert.

> **Hinweis:**
> Richtlinien zur Anforderungszeit für POST-Daten oder Cookie-Header müssen während der Auswertung zur Überschreibung der Anforderungszeit aufgerufen werden, da die integrierten Richtlinien zur Anforderungszeit im integrierten Cache eine `NOCACHE` Aktion für POST-Anfragen und eine `MAY_NOCACHE` Aktion für Anfragen mit Cookies zurückgeben. Sie verknüpfen `MAY_CACHE` oder `MAY_NOCACHE` Aktionen mit einer Richtlinie zur Anforderungszeit, die auf eine parametrisierte Content-Gruppe verweist. Die Antwortzeitrichtlinie bestimmt, ob die Transaktion im Cache gespeichert wird.

Konfigurieren einer Richtlinie für integriertes Caching

Sie konfigurieren neue Richtlinien, um Daten zu verarbeiten, die von den integrierten Richtlinien nicht verarbeitet werden können. Sie konfigurieren separate Richtlinien für das Caching, das Verhindern von Zwischenspeichern und das Invalidieren zwischengespeicherter Daten. Im Folgenden sind die Hauptkomponenten einer Richtlinie für integrierte Zwischenspeicherung:

- Regel: Ein logischer Ausdruck, der eine HTTP-Anforderung oder -Antwort auswertet.
- Aktion: Sie ordnen eine Richtlinie einer Aktion zu, um zu bestimmen, was mit einer Anforderung oder Antwort zu tun ist, die der Richtlinienregel entspricht.

Inhaltsgruppen: Sie ordnen die Richtlinie einer oder mehreren Inhaltsgruppen zu, um festzustellen, wo die Aktion ausgeführt werden soll.

So konfigurieren Sie eine Richtlinie für das Caching mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cache policy <policyName> -rule <expression> -actionCACHE|MAY_CACHE
|NOCACHE|MAY_NOCACHE [-storeInGroup <contentGroupName>] [-undefAction
NOCACHE|RESET]
> add cache policy image_cache -rule ”http.req.url.contains(\”jpg\”)|| http
.req.url.contains(\”jpeg\”)”-action CACHE -storeingroup myImages_group -
undefaction NOCACHE

> add cache policy bugReportPolicy -rule ”http.req.url.query.contains(\”
IssuePage\”)”-action CACHE -storeInGroup bugReportGroup

> add cache policy my_form_policy -rule ”http.req.header(\”Host\”)contains
(\”my.company.com\”)&& http.req.method.eq(\”GET\”)&& http.req.url.query.
contains(\”v=7\”)”-action CACHE -storeInGroup my_form_event

> add cache policy viewproducts_policy -rule ”http.req.url.contains(\”
viewproducts.aspx\”)”-action CACHE -storeInGroup Product_Details
```

So konfigurieren Sie eine Richtlinie für die Invalidierung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cache policy <policyName> -rule <expression> -action INVAL [-
    invalObjects ”<contentGroupName1>[,<selectorName1>”]. . .]] | [-
    invalGroup <contentGroupName1>[, <contentGroupName2>. . .]] [-
    undefAction NOCACHE|RESET]
<!--NeedCopy-->
```

```
> add cache policy invalidation_events_policy -rule ”http.req.header(”
    Host”)contains(”my.company.com”) && http.req.method.eq(”GET”) &&
    http.req.url.query.contains(”v=8”) -action INVAL -invalObjects
    my_form_event -undefaction NOCACHE
<!--NeedCopy-->
```

```
> add cache policy inval_all -rule ”http.req.method.eq(”POST”) && http.
    req.url.contains(”jpeg”)” -action INVAL -invalGroups myImages_group
    myApps_group PDF_group
```



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

```
> add cache policy bugReportInvalidationPolicy -rule ”http.req.url.
    query.contains(”TransitionForm”)” -action INVAL -invalObjects
    bugReport`
`> add cache policy editproducts_policy  - rule ”http.req.url.contains(”
    editproducts.aspx”)”  - action INVAL -invalObjects ”Product_Details,
    batchnum_sel” ”Products_In_Depots,batchid_sel”
<!--NeedCopy-->
```

So konfigurieren Sie eine Richtlinie für Caching oder Invalidierung mit der GUI

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Richtlinien**, und erstellen Sie die neue Richtlinie.

Globale Bindung einer integrierten Caching-Richtlinie

Wenn Sie eine Richtlinie global binden, steht sie allen virtuellen Servern auf der NetScaler Appliance zur Verfügung.

So binden Sie eine integrierte Caching-Richtlinie global über die Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind cache global <policy> -priority <positiveInteger> [-
    typeREQ_OVERRIDE|REQ_DEFAULT|RES_OVERRIDE|RES_DEFAULT] [-
    gotoPriorityExpression <expression>] [-invoke <labelType> <labelName
    >]
<!--NeedCopy-->
```

```
> bind cache global myCachePolicy -priority 100 -type req_default
<!--NeedCopy-->
```

> **Hinweis:**
>
> Das Argument type ist optional für global gebundene Richtlinien, um die Abwärtskompatibilität mit Richtlinien aufrechtzuerhalten, die Sie mit früheren Versionen der NetScaler Appliance definiert haben. Wenn Sie den Typ weglassen, ist die Richtlinie an REQ_DEFAULT oder RES_DEFAULT gebunden, je nachdem, ob es sich bei der Richtlinienregel um eine Antwortzeit oder einen Anforderungszeitausdruck handelt. Wenn die Regel sowohl Anforderungs- als auch

> Antwortzeitparameter enthält, ist sie an RES_DEFAULT gebunden. Es folgt ein Beispiel für eine Bindung, die den Typ

Es folgt ein Beispiel für eine Bindung, die den Typ auslässt.

```
> bind cache global myCache Policy 200
```

So binden Sie eine integrierte Caching-Richtlinie global mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu **Optimierung** > **Integriertes Caching**, klicken Sie auf **Cache-Richtlinien-Manager**, und binden Sie Richtlinien, indem Sie den relevanten Bindepunkt und den Verbindungstyp (Anforderung/Antwort) angeben.

Binden einer integrierten Caching-Richtlinie an einen virtuellen Server

Wenn Sie eine Richtlinie an einen virtuellen Server binden, ist sie nur für Anforderungen und Antworten verfügbar, die mit der Richtlinie übereinstimmen und die über den relevanten virtuellen Server fließen.

Wenn Sie die GUI verwenden, können Sie die Richtlinie über das Konfigurationsdialogfeld für den virtuellen Server binden. Auf diese Weise können Sie alle Richtlinien aller Citrix ADC-Module anzeigen, die an diesen virtuellen Server gebunden sind. Sie können auch das **Richtlinien-Manager-Konfigurationsdialogfeld** für den integrierten Cache verwenden. Auf diese Weise können Sie nur die integrierten Caching-Richtlinien anzeigen, die an den virtuellen Server gebunden sind.

So binden Sie eine integrierte Caching-Richtlinie über die Befehlszeilenschnittstelle an einen virtuellen Server:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name>@ -policyName <policyName> -priority <
    positiveInteger> -type(REQUEST|RESPONSE)
<!--NeedCopy-->
```

```
bind cs vserver <name>@ -policyName <policyName> -priority <
    positiveInteger> -type(REQUEST|RESPONSE)
<!--NeedCopy-->
```

So binden Sie eine integrierte Caching-Richtlinie mithilfe des Konfigurationsdienstprogramms an einen virtuellen Server (Methode des virtuellen Servers)

- CS Virtual Server - Navigieren Sie toTraffic **Management > Content Switching > Virtuelle Server**, wählen Sie den virtuellen Server aus und binden Sie relevante Cache-Richtlinien.

- LB Virtual Server - Navigieren Sie toTraffic **Management > Load Balancing > Virtuelle Server**, wählen Sie den virtuellen Server aus und binden Sie relevante Cache-Richtlinien.

So binden Sie eine integrierte Caching-Richtlinie mit der GUI (Policy Manager-Methode) an einen virtuellen Server.

Navigieren Sie zu **Optimierung** > **Integriertes Caching**, klicken Sie auf **Cache-Richtlinien-Manager**, und binden Sie Cache-Richtlinien, indem Sie den relevanten Bindepunkt und den Verbindungstyp angeben.

> **Hinweis:**
> Sie können Cache-Richtlinien sowohl an den virtuellen Lastausgleichsserver als auch an den virtuellen Server mit Content Switching binden, indem Sie den entsprechenden Bindepunkt auswählen.

Wie man komprimierte und unkomprimierte Versionen einer Datei zwischenspeichert

Standardmäßig kann ein Client, der die Komprimierung verarbeiten kann, unkomprimierte Antworten oder komprimierte Antworten im Format gzip, deflate, komprimieren und pack200-gzip bereitgestellt werden. Wenn der Client die Komprimierung übernimmt, wird ein `Accept-Encoding:compression` Format-Header in der Anfrage gesendet. Der vom Client akzeptierte Komprimierungstyp muss mit dem Komprimierungstyp des zwischengespeicherten Objekts übereinstimmen. Beispielsweise kann eine `cached.gzip` Datei nicht als Antwort auf eine Anfrage mit einem `Accept-Encoding:deflate` Header bereitgestellt werden.

Ein Client, der die Komprimierung nicht verarbeiten kann, wird eine Cache-Fehlmeldung bereitgestellt, wenn die zwischengespeicherte Antwort komprimiert ist.

Für das dynamische Caching müssen Sie zwei Inhaltsgruppen konfigurieren, eine für komprimierte Daten und eine für unkomprimierte Versionen derselben Daten. Im Folgenden finden Sie ein Beispiel für die Konfiguration der Selektoren, Inhaltsgruppen und Richtlinien für die Bereitstellung unkomprimierter Dateien aus dem Cache an Clients, die die Komprimierung nicht verarbeiten können, und komprimierte Versionen derselben Dateien an den Client bereitzustellen, der mit der Komprimierung umgehen kann.

```
add cache selector uncompressed_response_selector http.req.url "http.req.
header(\"Host\")"

add cache contentGroup uncompressed_group -hitSelector uncompressed_responst_selector
 -invalSelector uncomp_resp_sel

add cache policy cache_uncompressed -rule "HTTP.REQ.URL.CONTAINS(\"xyz\")&&
 !HTTP.REQ.HEADER(\"Accept-Encoding\").EXISTS"-action CACHE -storeInGroup
uncompressed_group
```



```
bind cache global cache_uncompressed -priority 100 -gotoPriorityExpression
END -type REQ_OVERRIDE

add cache selector compressed_response_selector HTTP.REQ.URL "HTTP.REQ.
HEADER(\"Host\")""HTTP.REQ.HEADER(\"Accept-Encoding\")"

add cache contentGroup compressed_group -hitSelector compressed_response_selector


add cache policy cache_compressed -rule "HTTP.REQ.URL.CONTAINS(\"xyz\")&&
 HTTP.REQ.HEADER(\"Accept-Encoding\").EXISTS"-action CACHE -storeInGroup
compressed_group

bind cache global cache_compressed -priority 200 -gotoPriorityExpression
END -type REQ_OVERRIDE
```

Konfigurieren einer Richtlinienbank für das Caching

Alle Richtlinien, die einem bestimmten Bindepunkt zugeordnet sind, werden gemeinsam als Richtlinienbank bezeichnet. Zusätzlich zur Konfiguration von Prioritätsstufen für Richtlinien in einer Bank können Sie die Reihenfolge der Auswertung in einer Bank ändern, indem Sie Goto-Ausdrücke konfigurieren. Sie können die Evaluierungsreihenfolge weiter ändern, indem Sie innerhalb der aktuellen Richtlinienbank eine externe Richtlinienbank aufrufen. Sie können auch neue Richtlinienbanken konfigurieren, denen Sie eigene Labels zuweisen. Da solche Richtlinienbanken an keinen Punkt im Verarbeitungszyklus gebunden sind, können sie nur innerhalb anderer Richtlinienbanken aufgerufen werden. Der Einfachheit halber werden Richtlinienbanken, deren Labels keinem integrierten Bindepunkt entsprechen, als Richtlinienlabels bezeichnet.

Zusätzlich zur Steuerung der Reihenfolge der Richtlinienbewertung durch Bindung der Richtlinie und Zuweisen einer Prioritätsstufe, wie unter "Binding Policys"beschrieben, können Sie den Ablauf innerhalb einer Bank von Richtlinien festlegen, indem Sie einen Goto-Ausdruck konfigurieren. Ein Goto-Ausdruck überschreibt den durch die Prioritätsstufen bestimmten Fluss. Sie können den Evaluierungsfluss auch steuern, indem Sie eine externe Richtlinienbank aufrufen, nachdem Sie einen Eintrag in der aktuellen Bank ausgewertet haben. Die Evaluierung kehrt nach Abschluss der Evaluierung immer an die aktuelle Bank zurück.

In der folgenden Tabelle werden die Einträge zur Kontrolle der Evaluierung in einer Richtlinienbank zusammengefasst.

Attribut	Gibt an
Name	Der Name einer Richtlinie oder, um eine andere Richtlinienbank aufzurufen, ohne die Richtlinie zu bewerten, das Schlüsselwort NOPOLICY. Sie können NOPOLICY mehrmals in einer Richtlinienbank angeben, aber Sie können eine benannte Richtlinie nur einmal angeben.
Priorität	Eine ganze Zahl. Je niedriger die ganze Zahl, desto höher die Priorität.
Gehe zu Ausdruck	Bestimmt die nächste Richtlinie oder Richtlinienbank, die ausgewertet werden soll. Sie können einen der folgenden Werte angeben: 1. NEXT: Gehen Sie zur Richtlinie mit der nächsthöheren Priorität. 2. END: Auswertung beenden. 3. USE_INVOCATION_RESULT: Gilt, wenn dieser Eintrag eine andere Richtlinienbank aufruft. Wenn der endgültige Gehe in der aufgerufenen Bank den Wert END aufweist, wird die Auswertung beendet. Wenn der endgültige Goto etwas anderes als END ist, führt die aktuelle Richtlinienbank eine NEXT durch. 4. Positive Zahl: Prioritätsnummer der nächsten zu bewertenden Richtlinie. 5. Numerischer Ausdruck: Ausdruck, der die Prioritätsnummer der nächsten auszuwertenden Richtlinie erzeugt. Der Gehe kann nur in einer Richtlinienbank vorwärts gehen. Das Auslassen des Goto-Ausdrucks entspricht der Angabe von END.

Attribut	Gibt an
Aufruftyp	Gibt einen Richtlinienbanktyp an. Der Wert kann einer der folgenden sein - 1. Virtueller Server anfordern: Ruft Richtlinien für die Anforderungszeit auf, die mit einem virtuellen Server verknüpft sind. 2. Reaktionsvirtueller Server: Ruft Reaktionszeit-Richtlinien auf, die mit einem virtuellen Server verknüpft sind. 3. Richtlinienbezeichnung: Ruft eine andere Richtlinienbank auf, die durch das Richtlinienbezeichnung für die Bank identifiziert wird.
Aufrufname	Name eines virtuellen Servers oder einer Richtlinienbezeichnung, abhängig vom Wert, den Sie für den Aufruftyp angegeben haben.

Der integrierte Cache verfügt über zwei integrierte Richtlinienbeschriftungen, und Sie können weitere Richtlinienlabels konfigurieren:

`_reqBuiltInDefaults`: Diese Policy Label wird vom Standardbindepunkt für die Anforderungszeit aus aufgerufen.
`_resBuiltInDefaults`: Diese Policy Label wird vom Standardbindepunkt für die Antwortzeit aus aufgerufen.

So rufen Sie eine Richtlinienbezeichnung in einer Caching-Richtlinienbank mit der Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind cache policylabel <labelName> -policname<policyName> -priority<
     priority> [-gotoPriorityExpression <gotoprioritыExpression>] [-
     invoke <labelType> <labelName>]
2 <!--NeedCopy-->
```

So rufen Sie ein Policy Label in einer Caching-Policy-Bank mit der GUI auf:

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching**, klicken Sie auf **Cache-Richtlinien-Manager**, und geben Sie den relevanten Bindpunkt (Override Global oder Standard Global) und den Verbindungstyp an, um die Liste der an diesen Bindungspunkt gebundenen Richtlinien anzuzeigen.

2. Wenn Sie eine Richtlinienbezeichnung aufrufen möchten, ohne eine Richtlinie zu evaluieren, klicken Sie auf **NOPOLICY**.

> **Hinweis:**
>
> Um eine externe Richtlinienbank aufzurufen, klicken Sie auf das Feld in der Spalte Invoke Type, und wählen Sie den Typ der Richtlinienbank aus, die Sie zu diesem Zeitpunkt in der Richtlinienbank aufrufen möchten. Dies kann ein globales Label oder eine virtuelle Serverbank sein. Geben Sie im Feld Name aufrufen die Bezeichnung oder den Namen des virtuellen Servers ein.

So rufen Sie eine Caching-Richtlinienbezeichnung in einer virtuellen Serverrichtlinienbank mit der Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name>@ -policyName <policyName>|<NOPOLICY-CACHE> -
    priority<positiveInteger> -gotoPriorityExpression <expression> -type
     REQUEST|RESPONSE -invoke<labelType> <labelName>
<!--NeedCopy-->
```

```
bind cs vserver <name> -policyName <policyName>|<NOPOLICY-CACHE> -
    priority<positiveInteger> -gotoPriorityExpression <expression> -type
     REQUEST|RESPONSE -invoke<labelType> <labelName>
<!--NeedCopy-->
```

So rufen Sie eine Caching-Richtlinienbezeichnung in einer virtuellen Serverrichtlinienbank mit der GUI auf

1. Navigieren Sie zu **Traffic Management** > **Load Balancing/Content Switching** > **Virtuelle Server**, wählen Sie den virtuellen Server aus, und klicken Sie auf **Richtlinien** .
2. Wenn Sie einen vorhandenen Eintrag in dieser Bank konfigurieren, überspringen Sie diesen Schritt. Wenn Sie dieser Richtlinienbank eine neue Richtlinie hinzufügen oder den Eintrag Dummy NOPOLICY verwenden möchten, klicken Sie auf **Hinzufügen** und führen Sie einen der folgenden Schritte aus:
   - Um eine neue Richtlinie zu konfigurieren, klicken Sie auf Cache und konfigurieren Sie die neue Richtlinie wie unter Richtlinie konfigurieren im integrierten Cachebeschrieben.
   - Um eine Richtlinienbank aufzurufen, ohne eine Richtlinie in einer Regel zu verarbeiten, wählen Sie die `NOPOLICY-CACHE` Option aus.

> **Hinweis:**
>
> Um eine externe Richtlinienbank aufzurufen, klicken Sie auf das Feld in der Spalte Invoke Type,

> und wählen Sie den Typ der Richtlinienbank aus, die Sie zu diesem Zeitpunkt in der Richtlinienbank aufrufen möchten. Dies kann ein globales Label oder eine virtuelle Serverbank sein. Geben Sie im Feld Name aufrufen die Bezeichnung oder den Namen des virtuellen Servers ein.

Konfigurieren einer Richtlinienbezeichnung in einem integrierten Cache

Zusätzlich zum Konfigurieren von Richtlinien in einer Richtlinienbank für einen der integrierten Bindpunkte oder einen virtuellen Server können Sie Caching-Richtlinienlabels erstellen und Richtlinienbänke für diese neuen Labels konfigurieren.

Eine Policy Label für den integrierten Cache kann nur von einem der Bindepunkte aus aufgerufen werden, die Sie im Richtlinien-Manager im Detailbereich für **integrierte Caching-Details** (Anforderungsüberschreibung, Anforderungsstandard, Antwortüberschreibung oder Antwortstandard) oder den integrierten Richtlinienbeschriftungen anzeigen können `\\_reqBuiltinDefaults` und `\\_resBuiltinDefaults`. Sie können eine Richtlinienbezeichnung beliebig oft aufrufen, anders als eine Richtlinie, die nur einmal aufgerufen werden kann.

Die Citrix ADC GUI bietet eine Option zum Umbenennen einer Richtlinienbezeichnung. Das Umbenennen einer Richtlinienbezeichnung hat keinen Einfluss auf den Prozess der Bewertung der an das Label gebundenen Richtlinien.

> **Hinweis**:
>
> Sie können die Richtlinie `NOPOLICY` “Dummy” verwenden, um jedes Policy Label von einer anderen Richtlinienbank aufzurufen. Der `NOPOLICY` Eintrag ist ein Platzhalter, der keine Regel verarbeitet.

So konfigurieren Sie eine Richtlinienbezeichnung für das Caching mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine Richtlinienbezeichnung zu erstellen und die Konfiguration zu überprüfen:

- `add cache policylabel <labelName> -evaluates (REQ|RES)`
- `show cache policylabel <labelName>`

Rufen Sie dieses Richtlinienlabel von einer Richtlinienbank auf.

So konfigurieren Sie eine Policy Label für das Caching mit der GUI:

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Richtlinienlabels**, fügen Sie eine Richtlinienbezeichnung hinzu, und binden Sie die zwischengespeicherten Richtlinien.

> **Hinweis:**
> Um sicherzustellen, dass der Citrix ADC das Policy Label zum richtigen Zeitpunkt verarbeitet, konfigurieren Sie einen Aufruf dieses Labels in einer der Richtlinienbanken, die mit den integrierten Bindepunkten verknüpft sind.

So benennen Sie ein Policy Label mit der GUI um:

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Richtlinienbezeichnungen**, wählen Sie die Richtlinienbezeichnung aus, und benennen Sie sie um.

Aufheben und Löschen einer integrierten Caching-Richtlinie und einer Richtlinienbezeichnung

Sie können die Bindung einer Richtlinienbank aufheben und sie löschen. Um die Richtlinie zu löschen, müssen Sie die Bindung zunächst aufheben. Sie können auch einen Richtlinienbezeichnungsaufruf entfernen und eine Richtlinienbezeichnung löschen. Um die Richtlinienbezeichnung zu löschen, müssen Sie zuerst alle Aufrufe entfernen, die Sie für die Bezeichnung konfiguriert haben.

Sie können die Beschriftungen für die integrierten Bindungspunkte (Anforderungsstandard, Anforderungsüberschreibung, Antwortstandard und Antwortüberschreibung) nicht aufheben oder löschen.

So heben Sie die Bindung einer globalen Caching-Richtlinie mit der Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
unbind cache global <policy>
```

So heben Sie die Bindung einer virtuellen serverspezifischen Caching-Richtlinie mit der Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
(unbind lb vserver|unbind cs vserver)<vserverName> -policyName <policyName>
 -type(REQUEST|RESPONSE)
```

So löschen Sie eine Caching-Richtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm cache policy <policyName>
```

So heben Sie die Bindung einer Caching-Richtlinie mit der GUI auf:

Navigieren Sie zu **Optimierung** > **Integriertes Caching**, klicken Sie auf **Cache-Richtlinien-Manager**, und heben Sie die Bindung von Richtlinien auf, indem Sie den relevanten Bindepunkt und den Verbindungstyp (Anforderung/Antwort) angeben.

So löschen Sie einen Richtlinienbeschriftungsaufruf mit der GUI:

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching**, klicken Sie auf **Cache-Richtlinien-Manager**und geben Sie den entsprechenden Verbindungspunkt (virtueller Lastausgleichsserver oder virtueller Content Switching-Server) und den Verbindungstyp an, um die Liste der an diesen virtuellen Server gebundenen Cache-Richtlinien anzuzeigen.
2. Deaktivieren Sie in der Spalte Invoke den Eintrag.

Cache-Unterstützung für Datenbankprotokolle

October 5, 2021

Die integrierte Cache-Funktion überwacht und speichert die Datenbankanforderung gemäß den Cache-Richtlinien. Benutzer müssen die Cache-Richtlinien für MYSQL- und MSSQL-Protokolle konfigurieren, da die Citrix ADC Appliance keine Standardrichtlinien bereitstellt. Denken Sie beim Konfigurieren der Standardprotokolle daran, dass die anforderungsbasierten Richtlinien nur CACHE- und INVAL-Aktionen unterstützen, während die antwortenbasierten Richtlinien nur die Aktion "NO-CACHE" unterstützen. Nachdem Sie die Richtlinien konfiguriert haben, müssen Sie sie an virtuelle Server binden. MYSQL- und MSSQL-Richtlinien, sowohl Anfrage als auch Antwort, sind nur an virtuelle Server gebunden.

Bevor Sie eine Cache-Richtlinie erstellen, müssen Sie eine Cache-Content-Gruppe vom Typ MYSQL oder MSSQL erstellen. Wenn Sie eine Cache-Content-Gruppe erstellen, verknüpfen Sie mindestens einen Auswahlselektor mit ihr. Weitere Informationen finden Sie unter Einrichten einer Basis-Content-Gruppe zum Einrichten einer Cache-Inhaltsgruppe.

Im folgenden Beispiel wird erläutert, wie Sie die Cache-Unterstützung für SQL-Protokolle konfigurieren und überprüfen.

```
1  > enable feature IC
2  > set cache parameter -memlimit 100
3  > add cache selector sel1 mssql.req.query.text
4
5  > add cache contentgroup cg1  -type "MSSQL" -hitselector "sel1" -
       invalselector "inval_sel" -relExpiry "500" -maxResSize
6   "100"
7  > add cache policy cp1  -rule "mssql.req.query.command.contains("select
       ")" -action "CACHE" -storeInGroup "cg1"
8  > add cache policy cp2  -invalObjects "cg1" -rule "mssql.req.query.text
       .contains("insert")" -action "INVAL"
9  > add db user user1  -password "Pass1"
10 > add service svc_sql_1 10.102.147.70 mssql 64834 -healthMonitor "NO" -
       downstateflush "ENABLED"
11 > add lb vserver lb_mssql1 mssql 10.102.147.77 1433  -lbmethod "
       roundrobin"
12 > bind lb vserver lb_mssql1 svc_sql_1
13 > bind lb vserver lb_mssql1 -policyName cp1  -type "REQUEST" -priority
       "2"
14 > bind lb vserver lb_mssql1 -policyName cp2  -type "REQUEST" -priority
       "1"
```



```
15
16 > show cache selector sel1
17      Name:sel1
18                      Expressions:
19                      1)mssql.req.query.text
20 > show cache policy cp1
21                      Name:cp1
22      Rule:mssql.req.query.command.contains(”select”)
23                      CacheAction:CACHE
24                      Stored in group: cg1
25                      UndefAction:Use Global
26                  Hits:2
27                      Undef Hits:0
28                      Policy is bound to following entities
29                      1) Bound to:
30                                  REQ VSERVER lb_mssql1
31                                  Priority:2
32                                  GotoPriorityExpression: END
33 <!--NeedCopy-->
```

> **Hinweis:**
>
> Die Methoden zur Reduzierung von Flash-Crowds, wie in Flash Crowds reduzierenerklärt, werden für MYSQL- und MSSQL-Protokolle nicht unterstützt.

Konfigurieren von Ausdrücken für Caching-Richtlinien und Selektoren

October 5, 2021

Ein Anforderungszeitausdruck untersucht Daten in der Anforderungszeit-Transaktion, und ein Reaktionszeitausdruck untersucht Daten in einer Response-Time-Transaktion. Wenn ein Ausdruck in einer Richtlinie zum Caching mit Daten in einer Anforderung oder Antwort übereinstimmt, führt die Citrix ADC-Appliance die mit der Richtlinie verknüpfte Aktion aus. In einem Selektor werden Anforderungszeitausdrücke verwendet, um übereinstimmende Antworten zu finden, die in einer Content-Gruppe gespeichert sind.

Bevor Sie Richtlinien und Selektoren für den integrierten Cache konfigurieren, müssen Sie mindestens die Hostnamen, Pfade und IP-Adressen kennen, die in HTTP-Anforderungs- und Antwort-URLs angezeigt werden. Und Sie müssen wahrscheinlich das Format ganzer HTTP-Anfragen und -Antworten kennen. Programme wie Live HTTP-Header http://livehttpheaders.mozdev.org/)or HTTPFox https://addons.mozilla.org/en-US/firefox/addon/6647 können Ihnen helfen, die Struktur der HTTP-Daten zu untersuchen, mit denen Ihre Organisation zusammenarbeitet.

Es folgt ein Beispiel für eine HTTP-GET-Anfrage für ein Aktienkursprogramm:

```
GET /quote.dll?page=dynamic&mode=data&mode=stock&symbol=CTXS&page=multi
    &selected=CTXS&random=0.00792039478975548 HTTP/1.1

Host: quotes.mystockquotes.com

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9)
    Gecko/2008052906 Firefox/3.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q
    =0.8

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate,compress,pack200-gzip

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300

Connection: keep-alive

Referer: http://quotes.mystockquotes.com/quote.dll?mode=stock&symbol=
    CTXS&page=multi&selected=CTXS

Cookie: __qca=1210021679-72161677-10297606
<!--NeedCopy-->
```

Beachten Sie beim Konfigurieren eines Ausdrucks die folgenden Einschränkungen:

Ausdruckstyp	Einschränkungen
Anfrage	Konfigurieren Sie keine Anforderungszeitausdrücke in einer Richtlinie mit einer CACHE- oder NOCACHE-Aktion. Verwenden Sie stattdessen MAY_CACHE oder MAY_NOCACHE.

Ausdruckstyp	Einschränkungen
Antwort	Konfigurieren Sie Ausdrücke zur Reaktionszeit nur in Caching-Richtlinien. Selektoren können nur Anforderungszeitausdrücke verwenden. Konfigurieren Sie keine Reaktionszeitausdrücke in einer Richtlinie mit einer INVAL-Aktion. Hinweis: Konfigurieren Sie keine Reaktionszeitausdrücke in einer Richtlinie mit einer CACHE-Aktion und einer parametrisierten Content-Gruppe. Verwenden Sie die MAY_CACHE -Aktion.

> **Hinweis:**
> Eine umfassende Diskussion erweiterter Ausdrücke finden Sie unter Richtlinien und Ausdruck.

Ausdruckssyntax

Im Folgenden sind die grundlegenden Komponenten der Syntax:

- Trennen Sie Schlüsselwörter wie folgt mit Punkten (.):

```
http.req.url
```

- Schließen Sie String-Werte wie folgt in Klammern und Anführungszeichen ein:

```
http.req.url.query.contains("this")
```

- Wenn Sie einen Ausdruck von der Befehlszeile aus konfigurieren, müssen Sie interne Anführungszeichen (die Anführungszeichen, die die Werte im Ausdruck begrenzen, im Gegensatz zu den Anführungszeichen, die den Ausdruck begrenzen) umgehen. Eine Methode besteht darin, einen Schrägstrich wie folgt zu verwenden:

```
\"abc\"
```

Selektorausdrücke werden in der Reihenfolge ihres Aussehens ausgewertet, und mehrere Ausdrücke in einer Selektordefinition werden durch ein logisches UND verbunden. Im Gegensatz zu Selektorausdrücken können Sie boolesche Operatoren angeben und die Priorität in einem erweiterten Ausdruck für eine Richtlinienregel ändern.

Konfigurieren eines Ausdrucks in einer Caching-Richtlinie oder einem Selektor

> **Hinweis:**
> Die Syntax für einen Richtlinienausdruck unterscheidet sich von einem Selektorausdruck. Eine umfassende Diskussion fortgeschrittener Ausdrücke finden Sie unter “Richtlinien und Ausdrücke. “

So konfigurieren Sie einen Richtlinienausdruck mit der Befehlszeilenschnittstelle

1. Starten Sie die Richtliniendefinition wie unter “Global Binden einer integrierten Caching-Richtlinie beschrieben. “
2. Um die Richtlinienregel zu konfigurieren, begrenzen Sie die gesamte Regel in Anführungszeichen und begrenzen Sie Zeichenfolgenwerte innerhalb der Regel in Escape-Anführungszeichen.

Ein Beispiel:

“http.req.url.contains(“jpg”)”

Um boolesche Werte hinzuzufügen, fügen Sie &&,	oder! Betreiber.

1.

Die folgenden Beispiele sind:

```
”http.req.url.contains(\”jpg\”)|| http.req.url.contains(\”jpeg\”)”
```

```
”http.req.url.query.contains(\”IssuePage\”)”
```

```
”http.req.header(\”Host\”)contains(\”my.company.com\”)&& http.req.method.eq(\”GET\”)&& http.req.url.query.contains(\”v=7\”)”
```

1. So konfigurieren Sie eine Evaluierungsreihenfolge für die Bestandteile einer Verbindung

```
”http.req.url.contains(\”jpg\”)|| (http.req.url.contains(\”jpeg\”)&& http.req.method.eq(\”GET\”))”
```

So konfigurieren Sie einen Selektorausdruck mit der Befehlszeilenschnittstelle:

1. Starten Sie die Selektordefinition wie unter Info zu Inhaltsgruppen beschrieben.
2. Um den Selektorausdruck zu konfigurieren, begrenzen Sie die gesamte Regel in Anführungszeichen und begrenzen Sie Zeichenfolgenwerte innerhalb der Regel in Escape-Anführungszeichen.

Ein Beispiel:

```
”http.req.url.contains(\”jpg\”)”
```


Sie können keine booleschen Werte hinzufügen, &&,	oder! Betreiber. Geben Sie jedes in Anführungszeichen getrennte Ausdruckselement ein. Mehrere Ausdrücke in der Definition werden als zusammengesetzter Ausdruck behandelt, der durch logische ANDs verbunden ist.

1.

Die folgenden Beispiele sind:

```
1 ”http.req.url.query.value(”ProductId”)” ”http.req.url.query.value(”
     BatchNum”)” ”http.req.url.query.value(”depotLocation”)”
2 <!--NeedCopy-->
```

So konfigurieren Sie einen Richtlinien- oder Selektorausdruck mit der GUI

1. Starten Sie die Richtlinie- oder Auswahldefinition wie unter “So konfigurieren Sie eine Richtlinie zum Caching oder Invalidierung mithilfe des Konfigurationsdienstprogramms” oder “So konfigurieren Sie einen Selektor mit dem Konfigurationsdienstprogramm. “
2. Im Feld **Ausdruck** können Sie die Standardsyntax entweder manuell eingeben, indem Sie auf Zur klassischen Syntax wechseln klicken oder mit dem **Ausdrucksеditor einen neuen Ausdruck**erstellen.

Um einen Operator zwischen zwei Teilen eines zusammengesetzten Ausdrucks einzufügen, klicken Sie auf die Schaltfläche Operatoren und wählen Sie den Operatortyp aus. Das Folgende ist ein Beispiel für einen konfigurierten Ausdruck mit einem booleschen ODER (signalisiert durch doppelte vertikale Balken,	):

3.

4. Klicken Sie auf die Dropdownliste **Häufig verwendete Ausdrücke**, um die häufig verwendeten Ausdrücke einzufügen.
5. Um den Ausdruck zu testen, klicken Sie auf **Auswerten**. Wählen Sie im Dialogfeld **Ausdrucks-Evaluator** den Flow-Typ aus, der dem Ausdruck entspricht. Fügen Sie in das Datenfeld die HTTP-Anfrage oder -Antwort ein, die Sie mit dem Ausdruck analysieren möchten, und klicken Sie auf **Auswerten**.

Zwischengespeicherte Objekte und Cache-Statistiken anzeigen

Sie können bestimmte zwischengespeicherte Objekte anzeigen und Zusammenfassungsstatistiken über Cache-Anfragen, Fehlschläge und Speicherauslastung anzeigen. Die Statistiken geben einen Einblick in die Datenmenge, die aus dem Cache bereitgestellt wird, welche Elemente für den größten Leistungsvorteil verantwortlich sind und was Sie optimieren können, um die Cache-Leistung zu verbessern.

Dieser Abschnitt enthält die folgenden Details:

- Zwischengespeicherte Objekte anzeigen
- Bestimmte gecachte Antworten finden
- Cache-Statistiken anzeigen

Zwischengespeicherte Objekte anzeigen

Nachdem Sie das Caching aktiviert haben, können Sie Details für zwischengespeicherte Objekte anzeigen. Sie können beispielsweise die folgenden Elemente anzeigen:

- Antwortgrößen und Header-Größen
- Statuscodes
- Content-Gruppen
- ETag, Letzte Änderung und Cache-Control-Header
- URLs anfordern
- Treffer-Parameter
- Ziel-IP-Adressen
- Anfragen- und Reaktionszeiten

So zeigen Sie eine Liste der zwischengespeicherten Objekte mithilfe der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show cache object
```

Eigenschaften	Beschreibung
Antwortgröße (Byte)	Die Größe des Antwortheaders und des Textkörpers.
Größe des Antwortheaders (Byte)	Die Größe des Header-Teils der Antwort.
Antwortstatuscode	Der Statuscode, der mit der Antwort gesendet wurde.
eTag	Der eTag-Header, der in die Antwort eingefügt wurde. In der Regel gibt dieser Header an, ob sich die Antwort kürzlich geändert hat.
Zuletzt geändert	Der Header “Letzte Änderung”, der in die Antwort eingefügt wurde. Dieser Header gibt das Datum an, an dem die Antwort zuletzt geändert wurde.
Cache-Steuerung	Der Cache-Control-Header, der in die Antwort eingefügt wurde.
Datum	Der Date-Header, der angibt, wann die Antwort gesendet wurde.
Contentgroup	Die Content-Gruppe, in der die Antwort gespeichert wird.

Eigenschaften	Beschreibung
Komplexes Spiel	Wenn dieses Objekt basierend auf parametrisierten Werten zwischengespeichert wurde, lautet dieser Feldwert JA.
Host	Der Host, der in der URL angegeben wurde, die diese Antwort angefordert hat.
Hostport	Der Listenport für den Host, der in der URL angegeben ist, die diese Antwort angefordert hat
URL	Die für die gespeicherte Antwort ausgegebene URL.
Ziel-IP	Die IP-Adresse des Servers, von dem diese Antwort abgerufen wurde.
Destination port	Der Listenport für den Zielserver.
Treffer-Parameter	Wenn die Inhaltsgruppe, die die Antwort speichert, Trefferparameter verwendet, werden sie in diesem Feld aufgeführt.
Auswahl treffen	Wenn diese Content-Gruppe einen Trefferauswahl verwendet, wird sie in diesem Feld aufgeführt.
Inval-Selektor	Wenn diese Content-Gruppe einen Selektor für die Invalidierung verwendet, wird sie in diesem Feld aufgeführt.
Selektor-Ausdrücke	Wenn diese Content-Gruppe einen Selektor verwendet, zeigt dieses Feld den Ausdruck an, der die Auswahlregel definiert.
Request time	Die Zeit in Millisekunden seit der Ausgabe der Anfrage.
Response time	Die Zeit in Millisekunden, seit der Cache begonnen hat, die Antwort zu erhalten.
Alter	Zeitspanne, in der sich das Objekt im Cache befindet.
Ablauf	Zeitspanne, nach der das Objekt als abgelaufen markiert wird.
Gespült	Ob die Antwort nach Ablauf gespült wurde.

Eigenschaften	Beschreibung
Prefetch	Wenn Prefetch für diese Content-Gruppe konfiguriert wurde, ist die Zeit vor Ablauf, während der das Objekt vom Ursprung abgerufen wird. Prefetch gilt nicht für negative Objekte (z. B. 404 “Objekt nicht gefunden” -Antworten).
Aktuelle Leser	Ungefähr die aktuelle Anzahl der Anfragen, die bearbeitet werden. Wenn eine Antwort mit einem Header-Objekt in Content-Length heruntergeladen wird, sind die aktuellen Fehlschläge und die aktuellen Leserwerte in der Regel jeweils 1. Wenn ein Chunked Response-Objekt heruntergeladen wird, ist der aktuelle Fehlschlagwert in der Regel 1, aber der aktuelle Leserwert ist normalerweise 0, da die Chunked Response, die an den Client bereitgestellt wird, nicht aus den integrierten Caching-Puffern stammt.
Aktuelle Fehlschläge	Die aktuelle Anzahl von Anfragen, die zu einem Cache-Verpassen und Abrufen vom Ursprungsserver geführt haben. Dieser Wert ist normalerweise 0 oder 1. Wenn Poll Every Time für eine Content-Gruppe aktiviert ist, kann die Anzahl größer als 1 sein.
Treffer	Die Anzahl der Cache-Treffer für dieses Objekt.
Fehlschläge	Die Anzahl der Cache-Fehlschläge für dieses Objekt
Komprimierungsformat	Die Art der Komprimierung, die auf dieses Objekt angewendet wird. Zu den Komprimierungsformaten gehören gzip, deflate, compress und pack200-gzip.
HTTP-Version als Antwort	Die Version von HTTP, die zum Senden der Antwort verwendet wurde.

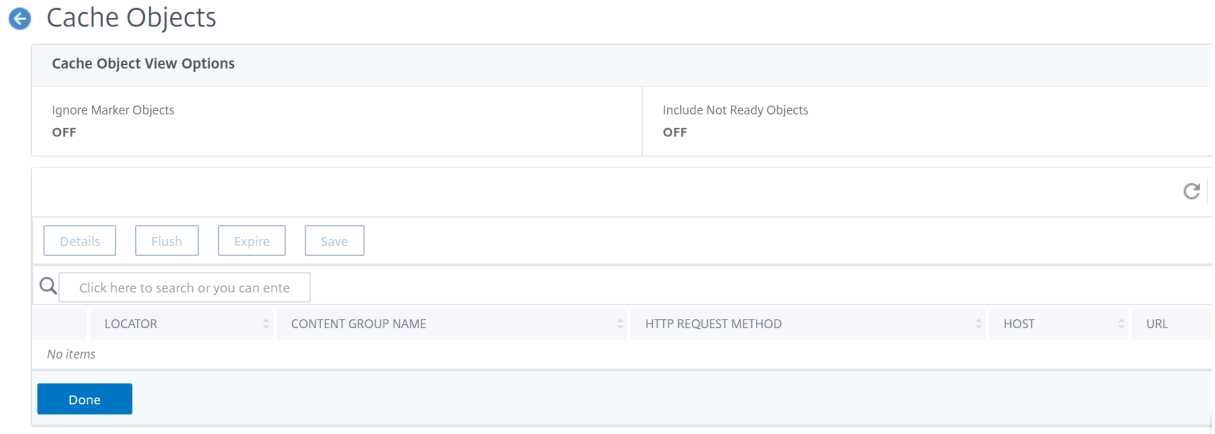
Eigenschaften	Beschreibung
Schwaches Etag als Antwort vorhanden	Starke Etag-Header ändern sich, wenn sich die Bits einer Entität ändern. Starke Header basieren auf den Oktettwerten eines Objekts. Schwache Etag-Header ändern sich, wenn sich die Bedeutung einer Entität ändert. Schwache Etag-Werte basieren auf semantischer Identität. Schwache Etags Werte beginnen mit einem “W.”
Negative Marker-Zelle	Ein Marker-Objekt ist zwischengespeichert, erfüllt aber noch nicht alle Kriterien für das Cache. Beispielsweise kann das Objekt die maximale Antwortgröße für die Content-Gruppe überschreiten. Für Objekte dieses Typs wird eine Markenzelle erstellt. Wenn ein Benutzer das nächste Mal eine Anfrage für dieses Objekt sendet, wird ein Cache-Fehler bereitgestellt.
Reason Marker erstellt	Der Grund, warum eine Marker-Zelle erstellt wurde (z. B. “Warten auf Minhit”, “Antwortdaten für Inhaltslänge sind nicht im Gruppengrößenlimit”).
Jedes Mal automatische Umfrage	Wenn der integrierte Cache eine bereits abgelaufene 200-OK-Antwort mit Validatoren (entweder die letzte Änderung oder die eTag-Antwortheader) erhält, speichert er die Antwort und markiert sie als Auto-PET (jedes Mal automatisch abfragen).
Citrix ADC Etag wurde als Antwort eingefügt	Eine Variation des eTag-Headers, der von der Citrix ADC-Appliance generiert wird. Der Wert YES wird angezeigt, wenn der Citrix ADC einen Etag in die Antwort einfügt.
Vollständige Antwort im Cache vorhanden	Zeigt an, ob dies eine vollständige Antwort ist.
Ziel-IP von DNS verifiziert	Gibt an, ob beim Speichern des Objekts eine DNS-Auflösung durchgeführt wurde.

Eigenschaften	Beschreibung
Objekt wird durch einen Cache-Forward-Proxy gespeichert	Gibt an, ob diese Antwort aufgrund eines Forward-Proxys gespeichert wurde, der im integrierten Cache konfiguriert ist.
Objekt ist ein Delta-Basisdatei	Eine Antwort, die delta-komprimiert ist.
Warten auf Minhits	Gibt an, ob diese Content-Gruppe eine Mindestanzahl von Original-Servern benötigt, die vor dem Zwischenspeichern einer Antwort getroffen werden.
Minhit zählen	Wenn diese Content-Gruppe vor dem Zwischenspeichern eines Objekts eine Mindestanzahl von Ursprungsserveranforderungen erfordert, wird in diesem Feld die Anzahl der bisher empfangenen Anforderungen angezeigt.
HTTP-Anforderungsmethode	Die Methode GET oder POST, die in der Anforderung verwendet wird, die dieses Objekt erhalten hat.
Gespeichert nach Richtlinie	Der Name der Caching-Richtlinie, die dazu geführt hat, dass dieses Objekt gespeichert wurde. Der Wert NICHT VERFÜGBAR gibt an, dass die Richtlinie deaktiviert oder gelöscht wurde. Der Wert NONE gibt an, dass das Objekt nicht mit einer sichtbaren Richtlinie übereinstimmte, sondern nach internen Kriterien für das Caching gespeichert wurde.
Metadaten der Anwendungs-Firewall vorhanden	Dieser Parameter wird verwendet, wenn die Anwendungs-Firewall und der integrierte Cache beide aktiviert sind. Die Anwendungs-Firewall analysiert den Inhalt einer Antwortseite, speichert ihre Metadaten (z. B. URLs und Formulare auf der Seite) und exportiert die Metadaten mit der Antwort in den Cache. Der Cache speichert die Seite und die Metadaten, und wenn der Cache die Seite bedient, sendet er die Metadaten zurück an die Sitzung der Anforderung.

Eigenschaften	Beschreibung
HTTP-Callout-Objekt, Name, Typ, Antwort	Diese Zellen geben an, ob diese Daten als Ergebnis eines HTTP-Callout-Ausdrucks gespeichert wurden, und liefern Informationen über verschiedene Aspekte des Callouts und die entsprechende Antwort. Weitere Informationen zu HTTP-Callouts finden Sie unter “HTTP-Callouts”.

So zeigen Sie zwischengespeicherte Objekte mit der GUI an

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Cache-Objekte**. Sie können alle zwischengespeicherten Objekte anzeigen und entsprechend nach Ihren Anforderungen sortieren.



Finde bestimmte zwischengespeicherte Antworten

Sie können einzelne Elemente im Cache basierend auf Suchkriterien finden. Es gibt verschiedene Methoden, um zwischengespeicherte Elemente zu finden, je nachdem, ob die Content-Gruppe, die die Daten enthält, Treffer- und Invalidierungsselektoren verwendet, wie folgt:

- Wenn die Content-Gruppe Selektoren verwendet, können Sie die Suche nur mit der Locator-ID für das zwischengespeicherte Element durchführen.
- Wenn die Content-Gruppe keine Selektoren verwendet, führen Sie die Suche mit Kriterien wie URL, Host, Name der Inhaltsgruppe durch.

Wenn Sie nach einer zwischengespeicherten Antwort suchen, können Sie einige Elemente nach URL und Host suchen. Wenn sich die Antwort in einer Content-Gruppe befindet, die einen Selektor verwendet, können Sie sie nur mit einer Locator-Nummer (z. B. 0x00000000ad7af00000050) finden.

Um eine Locator-Nummer zur späteren Verwendung zu speichern, klicken Sie mit der rechten Maustaste auf den Eintrag und wählen Sie **Kopieren**. Weitere Informationen zu Selektoren finden Sie unter "Konfigurieren von Selektoren und grundlegenden Inhaltsgruppen. "

So zeigen Sie zwischengespeicherte Antworten in Inhaltsgruppen an, die keinen Selektor haben, mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show cache object [-locator <positiveInteger>] | [(-url <URL> (-host <
hostName> [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET
 | POST ]))| [-httpStatus <positive integer>] | -group <contentGroupName> |
 -ignoreMarkerObjects (ON | OFF)| -includeNotReadyObjects (ON | OFF)]
```

So zeigen Sie zwischengespeicherte Antworten in Inhaltsgruppen mit einem Selektor über die Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show cache object -locator <locatorString> MarkerObjects ( ON | OFF )| -
includeNotReadyObjects ( ON | OFF )| [-httpStatus<positive integer>]
```

So zeigen Sie zwischengespeicherte Antworten in Inhaltsgruppen an, die keinen Selektor haben, mithilfe des Konfigurationsdienstprogramms

Navigieren Sie zu **Optimierung > Integriertes Caching > Cache-Objekte**, klicken Sie auf Suchen und legen Sie die Suchkriterien fest, um die erforderliche zwischengespeicherte Antwort anzuzeigen.

Wenn Sie noch keine Inhaltsgruppen konfiguriert haben, befinden sich alle Objekte in der Gruppe Standard.

Cache-Statistiken anzeigen

In der folgenden Tabelle werden die detaillierten Cache-Statistiken zusammengefasst, die Sie anzeigen können.

Zähler	Beschreibung
Treffer	Antworten, die im integrierten Cache gefunden und aus diesem bereitgestellt werden. Umfasst statische Objekte wie Bilddateien, Seiten mit den Statuscodes 200, 203, 300, 301, 302, 304, 307, 403, 404, 410 und Antworten, die einer benutzerdefinierten Richtlinie mit einer CACHE-Aktion entsprechen.

Zähler	Beschreibung
Fehlschläge	Es wurden HTTP-Anfragen abgefangen, bei denen die Antwort letztendlich vom Ursprungsserver abgerufen wurde.
Anfragen	Gesamtzahl der Cache-Anfragen plus Gesamtzahl der Cache-Fehler
Nicht-304 Treffer	Wenn der Benutzer ein Element mehrmals anfordert und das Element im Cache seit dem letzten Servieren der Citrix ADC-Appliance unverändert ist, gibt die Citrix ADC-Appliance anstelle des zwischengespeicherten Objekts eine 304-Antwort an.
This statistic indicates how many items the Citrix ADC appliance served from the cache, excluding 304 responses.	
304 hits	Number of 304 (object not modified) responses the Citrix ADC appliance served from the cache.
304 hit ratio (%)	Percentage of 304 responses that the Citrix ADC appliance served, relative to other responses.
Hit ratio (%)	Percentage of responses that the Citrix ADC appliance served from the cache (cache requests) relative to responses that could not be served from the cache.
Origin bandwidth saved (%)	An estimate of the processing capacity that the Citrix ADC appliance saved on the origin server due to serving responses from the cache.
Bytes served by the Citrix ADC	Total number of bytes that the Citrix ADC appliance served from the origin server and the cache.
Bytes served by cache	Total number of bytes that the Citrix ADC appliance served from the cache.
Byte hit ratio(%)	Percentage of data that the Citrix ADC appliance served from the cache, relative to all of the data in all served responses.
Compressed bytes from cache	Amount of data, in bytes, that the Citrix ADC appliance served in compressed form.

Zähler	Beschreibung
Storable misses	If the Citrix ADC appliance does not find a requested object in the cache, it fetches the object from the origin server. Dies wird als Cache-Miss bezeichnet. A storable cache miss can be stored in the cache.
Non-storable misses	A non-storable cache miss cannot be stored in the cache.
Misses	All cache misses.
Revalidations	Max-Age setting in a Cache-Control header determines, in number of seconds, when an intervening cache must revalidate the content with the integrated cache before serving it to the user.
For more information, see “Inserting a Cache-Control Header.”	
Successful revalidations	Number of revalidations that have been performed.
For more information, see “Inserting a Cache-Control Header.”	
Conversions to conditional req	A user-agent request for a cached PET object is always converted to a conditional request and sent to the origin server.
For more information, see “Polling the Origin Server Every Time a Request Is Received.”	
Storable miss ratio (%)	Storable cache misses as a percentage of non-storable cache misses.
Successful reval ratio (%)	Successful revalidations as a percentage of all revalidation attempts.
For more information, see “Inserting a Cache-Control Header.”	
Expire at last byte	Number of times that the cache expired content immediately after receiving the last body byte. Gilt nur für positive Antworten, wie in der Tabelle “Cache-Hits and Misses beschrieben. “

Zähler	Beschreibung
For more information, see “Example of Performance Optimization.”	
Flashcache misses	If you enable Flash Cache, the cache allows only one request to reach the server, eliminating flash crowds. Diese Statistik gibt die Anzahl der Flash Cache-Anfragen an, die Cache-Fehler waren.
For more information, “Queuing Requests to the Cache.”	
Flashcache hits	Number of Flash Cache requests that were cache hits.
For more information, see “Queuing Requests to the Cache.”	
Parameterized inval requests	Requests that match a policy with an invalidation (INVAL) action and a content group that uses an invalidation selector or parameters to selectively expire cached objects in the group.
Full inval requests	Requests that match an invalidation policy where the invalGroups parameter is configured and expires one or more content groups.
Inval requests	Requests that match an invalidation policy and result in expiration of specific cached responses or entire content groups.
Parameterized requests	Number of cache requests that were processed using a policy with a parameterized content group.
Parameterized non-304 hits	Number of cache requests that were processed using a policy with a parameterized content group, where full cached response was found, and the response was not a 304 (object not updated) response.

Zähler	Beschreibung
Parameterized 304 hits	Number of cache requests that were processed using a policy with a parameterized content group, where the cached object was found, and the object was a 304 (object not updated) response.
Total parameterized hits	Number of cache requests that were processed using a policy with a parameterized content group, where the cached object was found.
Parameterized 304 hit ratio (%)	Percentage of 304 (object not updated) responses that were found using a parameterized policy, relative to all cache hits.
Poll every time requests	If Poll Every Time is enabled, the Citrix ADC appliance always consults the origin server before serving a stored object.
For more information, see “Polling the Origin Server Every Time a Request Is Received.”	
Poll every time hits	Number of times a cache hit was found using the Poll Every Time method.
For more information, see “Polling the Origin Server Every Time a Request Is Received.”	
Poll every time hit ratio (%)	Percentage of cache hits using the Poll Every Time method, relative to all searches for cached objects using Poll Every Time. For more information, see “Polling the Origin Server Every Time a Request Is Received.”
Maximum memory (KB)	Maximum amount of memory in the Citrix ADC appliance that is allocated to the cache. For more information, see “Configuring Global Attributes for Caching.”
Maximum memory active value (KB)	Maximum amount of memory (active value) that will be set after the memory is allocated to the cache. For more information, see “How to Configure the Integrated Caching Feature of a Citrix ADC Appliance for various Scenarios.”
Utilized memory (KB)	Amount of memory that is actually being used.

Zähler	Beschreibung
Memory allocation failures	Number of failed attempts to utilize memory for the purpose of storing a response in the cache.
Largest response so far	Largest response in bytes found in either the cache or the origin server and sent to the client.
Cached objects	Number of objects in the cache, including responses that have not yet been fully downloaded and responses that have been expired but not yet flushed.
Marker objects	Marker objects are created when a response exceeds the maximum or minimum response size for the content group, or has not yet received the minimum number of hits for the content group.
Hits being served	Number of hits that have been served from the cache.
Misses being handled	Responses that were fetched from the origin server, stored in the cache, and then served. Sollte die Zahl für speicherbare Fehlschläge annähern. Beinhaltet keine nicht speicherbaren Fehlschläge.

So zeigen Sie Zusammenfassungs-Cache-Statistiken über die Befehlszeilenschnittstelle an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat cache
```

So zeigen Sie bestimmte Cache-Statistiken über die Befehlszeilenschnittstelle an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat cache -detail
```

```
1 > stat cache -detail
2
3 Integrated Cache Statistics - Detail
4 Integrated Cache Statistics - Summary
```



```
                                                Rate (/s)
                                                    Total

Hits                                                    0
                        0

Misses                                                  0
                        0

Requests                                                0
                        0

Hit ratio(%)                                           --
                        0

Origin bandwidth saved(%)                              --
                        0
Cached objects                                         --
                        0

Marker objects                                         --
                        0
                                                Rate (/s)
                                                    Total

Requests                                                0
                        0


Hit Statistics

                                                Rate (/s)
                                                    Total


Non-304 hits                                            0
                        0

304 hits                                                0
                        0


Sql hits                                                0
                        0
```



```
36
37
38 Hits                                                  0
                        0
39
40 304 hit ratio(%)                                     --
                        0
41
42 Hit ratio(%)                                         --
                        0
43
44 Origin bandwidth saved(%)                            --
                        0
45 Byte Statistics
46                                                Rate (/s)
                                                     Total
47
48
49 Bytes served by Citrix ADC                             648
    55379204
50
51 Bytes served by cache                                  0
                        0
52 Byte hit ratio(%)                                    --
                        0
53 Compressed bytes from cache                            0
                        0
54
55 Miss Statistics
56
57                                                Rate (/s)
                                                     Total
58
59
60 Storable misses                                        0
                        0
61
62 Non-storable misses                                    0
                        0
63
64 Misses                                                 0
                        0
65
66 Revalidations                                          0
                        0
```



```
67
68 Successful revalidations                          0
                        0
69
70 Conversions to conditional req                   0
                        0
71
72
73 Storable miss ratio(%)                           --
                        0
74 Successful reval ratio(%)                        --
                        0
75
76 Flashcache Statistics
77                                          Rate (/s)
                                               Total
78
79
80 Expire at last byte                              0
                        0
81
82 Flashcache misses                                0
                        0
83 Flashcache hits                                  0
                        0
84
85 Invalidation Statistics
86
87                                          Rate (/s)
                                               Total
88
89 Parameterized inval requests                     0
                        0
90
91
92 Full inval requests                              0
                        0
93
94
95
96 Inval requests                                   0
                        0
97
98 Parameterized Caching Statistics
99
```



```
100                                                Rate (/s)
                                                      Total
101
102
103 Parameterized requests                                 0
                          0
104
105 Parameterized non-304 hits                             0
                          0
106
107 Parameterized 304 hits                                 0
                          0
108
109
110 Total parameterized hits                               0
                          0
111
112 Parameterized 304 hit ratio(%)                        --
                          0
113
114 Poll Every Time (PET) Statistics
115
116                                                Rate (/s)
                                                      Total
117
118
119 Poll every time requests                               0
                          0
120
121 Poll every time hits                                   0
                          0
122
123 Poll every time hit ratio(%)                          --
                          0
124
125 Memory Usage Statistics
126                                                    Total
127
128 Maximum memory(KB)                                     0
129
130 Maximum memory active value(KB)                        0
131
132 Utilized memory(KB)                                    0
133
134 Memory allocation failures                             0
```



```
135
136 Largest response so far(B)                          0
137
138 Cached objects                                     0
139
140 Marker objects                                     0
141
142 Hits being served                                  0
143 Misses being handled                               0
144  Done
145 <!--NeedCopy-->
```

So zeigen Sie Zusammenfassungs-Cache-Statistiken mit der GUI an

1. Klicken Sie oben auf der Seite auf die Registerkarte **Dashboard**.
2. Scrollen Sie nach unten zum Abschnitt **Integriertes Caching** des Fensters.
3. Um detaillierte Statistiken anzuzeigen, klicken Sie unten in der Tabelle auf den Link Mehr…

So zeigen Sie bestimmte Cache-Statistiken mit der GUI an

1. Klicken Sie oben auf der Seite auf die Registerkarte **Reporting** .
2. Erweitern Sie unter Integrierte Berichte den Eintrag **Integrierter Cache**, und klicken Sie dann auf den Bericht mit den Statistiken, die Sie anzeigen möchten.
3. Um den Bericht als Vorlage zu speichern, klicken Sie auf **Speichern unter** und benennen Sie den Bericht. Der gespeicherte Bericht wird unter **Benutzerdefinierte** Berichte angezeigt.

Anzeigen zwischengespeicherter Objekte und Cache-Statistiken

October 5, 2021

Sie können bestimmte zwischengespeicherte Objekte anzeigen und Zusammenfassungsstatistiken zu Cache-Treffern, Fehlern und Speicherbelegung anzeigen. Die Statistiken geben Einblick in die Menge der Daten, die aus dem Cache bereitgestellt werden, welche Elemente für den größten Leistungsvorteil verantwortlich sind und was Sie optimieren können, um die Cache-Performance zu verbessern.

Dieser Abschnitt enthält die folgenden Details:

- Anzeigen zwischengespeicherter Objekte
- Bestimmte zwischengespeicherte Antworten finden
- Cache-Statistiken anzeigen

Anzeigen zwischengespeicherter Objekte

Nachdem Sie das Caching aktiviert haben, können Sie Details für zwischengespeicherte Objekte anzeigen. Beispielsweise können Sie die folgenden Elemente anzeigen:

- Antwortgrößen und Kopfzeilengrößen
- Statuscodes
- Inhaltsgruppen
- ETag, Zuletzt geändert und Cache-Control-Header
- URLs anfordern
- Hit parameters
- Ziel-IP-Adressen
- Anforderungs- und Antwortzeiten

So zeigen Sie eine Liste zwischengespeicherter Objekte mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show cache object
```

Eigenschaften	Spezifikation
Antwortgröße (Byte)	Die Größe des Antwort-Headers und des Hauptteils.
Größe des Antwort-Headers (Byte)	Die Größe des Kopfzeilenabschnitts der Antwort.
Response status code	Der Statuscode, der mit der Antwort gesendet wurde.
ETag	Der in der Antwort eingefügte ETag Header. In der Regel gibt dieser Header an, ob sich die Antwort kürzlich geändert hat.
Last-Modified	Der Last-Modified Header, der in die Antwort eingefügt wurde. Dieser Header gibt das Datum an, an dem die Antwort zuletzt geändert wurde.
Cache-Control	Der Cache-Control-Header, der in die Antwort eingefügt wurde.
Datum	Der Date-Header, der angibt, wann die Antwort gesendet wurde.
Contentgroup	Die Inhaltsgruppe, in der die Antwort gespeichert ist.

Eigenschaften	Spezifikation
Complex match	Wenn dieses Objekt basierend auf parametrisierten Werten zwischengespeichert wurde, lautet dieser Feldwert JA.
Host	Der in der URL angegebene Host, der diese Antwort angefordert hat.
Host port	Der Listenport für den Host, der in der URL angegeben ist, der diese Antwort angefordert hat
URL	Die URL, die für die gespeicherte Antwort ausgegeben wurde.
Ziel-IP	Die IP-Adresse des Servers, von dem diese Antwort abgerufen wurde.
Destination port	Der Listenport für den Zielserver.
Hit parameters	Wenn die Inhaltsgruppe, in der die Antwort gespeichert wird, Trefferparameter verwendet, werden diese in diesem Feld aufgeführt.
Hit selector	Wenn diese Inhaltsgruppe einen Trefferselektor verwendet, wird sie in diesem Feld aufgeführt.
Inval selector	Wenn diese Inhaltsgruppe einen Invalidierungsselektor verwendet, wird diese in diesem Feld aufgeführt.
Selector Expressions	Wenn diese Inhaltsgruppe einen Selektor verwendet, wird in diesem Feld der Ausdruck angezeigt, der die Auswahlregel definiert.
Request time	Die Zeit in Millisekunden seit der Anforderung.
Response time	Die Zeit in Millisekunden, seit der Cache begonnen hat, die Antwort zu empfangen.
Alter	Zeitraum, in dem sich das Objekt im Cache befindet.
Expiry	Zeitraum, nach der das Objekt als abgelaufen markiert wird.
Flushed	Gibt an, ob die Antwort nach Ablauf gelöscht wurde.

Eigenschaften	Spezifikation
Prefetch	Wenn Prefetch für diese Content-Gruppe konfiguriert wurde, ist die Zeit vor Ablauf, in der das Objekt vom Ursprung abgerufen wird. Prefetch gilt nicht für negative Objekte (z. B. 404 Objekt nicht gefunden -Antworten).
Current readers	Ungefähr die aktuelle Anzahl der Treffer, die serviert werden. Wenn eine Antwort mit einem Content-Length-Header-Objekt heruntergeladen wird, sind die aktuellen Fehlschläge und die aktuellen Leserwerte jeweils in der Regel 1. Wenn ein geteiltes Antwortobjekt heruntergeladen wird, ist der aktuelle Fehler-Wert in der Regel 1, aber der aktuelle Lese-Wert ist in der Regel 0, da die aufgeteilte Antwort, die dem Client bereitgestellt wird, nicht aus den integrierten Caching-Puffern stammt.
Current misses	Die aktuelle Anzahl von Anforderungen, die zu einem Cache-Fehlern und Abrufen vom Ursprungsserver geführt haben. Dieser Wert ist in der Regel 0 oder 1. Wenn Jedes Mal abfragen für eine Inhaltsgruppe aktiviert ist, kann die Anzahl größer als 1 sein.
Treffer	Die Anzahl der Cache-Treffer für dieses Objekt.
Misses	Die Anzahl der Cache-Fehlschläge für dieses Objekt.
Compression format	Der auf dieses Objekt angewendete Komprimierungstyp. Komprimierungsformate umfassen gzip, deflate, compress und pack200-gzip.
HTTP version in response	Die HTTP-Version, die zum Senden der Antwort verwendet wurde.

Eigenschaften	Spezifikation
Schwache `etag` Präsenz als Reaktion	Starke `etag` Header ändern sich, wenn sich die Bits einer Entity ändern. Starke Header basieren auf den Oktettwerten eines Objekts. Schwache `etag` Header ändern sich, wenn sich die Bedeutung einer Entität ändert. Schwache `etag` Werte beruhen auf semantischer Identität. Schwache `etags` Werte beginnen mit “W.”
Negative marker cell	Ein Markerobjekt kann zwischengespeichert werden, erfüllt aber noch nicht alle Kriterien für die Zwischenspeicherung. Beispielsweise kann das Objekt die maximale Antwortgröße für die Inhaltsgruppe überschreiten. Für Objekte dieses Typs wird eine Markierungszelle erstellt. Wenn ein Benutzer das nächste Mal eine Anforderung für dieses Objekt sendet, wird ein Cache-Fehler bereitgestellt.
Reason marker created	Der Grund, warum eine Markierungszelle erstellt wurde (z. B. Warten auf Minhit, Inhaltslängenantwortdaten sind nicht in der Gruppengrößenbeschränkung).
Auto poll every time	Wenn der integrierte Cache eine bereits abgelaufene 200-k-Acs-Antwort mit Validatoren erhält (entweder die Last-Modified- oder die `ETag` Antwortheader), speichert er die Antwort und markiert sie als Auto-Pet (jedes Mal automatisch abfragen).
Citrix ADC Etag inserted in response	Eine Variante des `ETag` Headers, der von der Citrix ADC Appliance generiert wird. Ein Wert von YES wird angezeigt, wenn der Citrix ADC eine `Etag` in die Antwort einfügt.
Full response present in cache	Gibt an, ob dies eine vollständige Antwort ist.
Destination IP verified by DNS	Gibt an, ob beim Speichern des Objekts die DNS-Auflösung durchgeführt wurde.

Eigenschaften	Spezifikation
Object stored through a cache forward proxy	Gibt an, ob diese Antwort aufgrund eines Forward-Proxy gespeichert wurde, der im integrierten Cache konfiguriert ist.
Object is a Delta basefile	Eine Antwort, die delta-komprimiert ist.
Waiting for minhits	Gibt an, ob diese Content-Gruppe eine Mindestanzahl von Original-Servern erfordert, die vor dem Caching einer Antwort getroffen werden.
Minhit count	Wenn diese Content-Gruppe eine Mindestanzahl von Ursprungsservern erfordert, die vor dem Caching eines Objekts getroffen wurden, zeigt dieses Feld eine Anzahl der bisher empfangenen Treffer an.
HTTP Request Method	Die Methode GET oder POST, die in der Anforderung verwendet wird, die dieses Objekt erhalten hat.
Stored by policy	Der Name der Caching-Richtlinie, die dazu führte, dass dieses Objekt gespeichert wurde. Der Wert NOT AVAILABLE gibt an, dass die Richtlinie deaktiviert oder gelöscht wurde. Der Wert NONE gibt an, dass das Objekt nicht mit einer sichtbaren Richtlinie übereinstimmte, sondern nach internen Kriterien für das Caching gespeichert wurde.
Application firewall metadata exists	Dieser Parameter wird verwendet, wenn die Anwendungsfirewall und der integrierte Cache aktiviert sind. Die Anwendungsfirewall analysiert den Inhalt einer Antwortseite, speichert ihre Metadaten (z. B. URLs und Formulare auf der Seite) und exportiert die Metadaten mit der Antwort in den Cache. Der Cache speichert die Seite und die Metadaten, und wenn der Cache die Seite bereitstellt, sendet er die Metadaten zurück an die Sitzung der Anforderung.

Eigenschaften	Spezifikation
HTTP callout object, name, type, response	Diese Zellen geben an, ob diese Daten als Ergebnis eines HTTP-Callout-Ausdrucks gespeichert wurden, und liefern Informationen über verschiedene Aspekte des Callouts und die entsprechende Antwort. Weitere Informationen zu HTTP-Callouts finden Sie unter “HTTP-Callouts”.

Bestimmte zwischengespeicherte Antworten finden

Sie können einzelne Elemente im Cache anhand von Suchkriterien finden. Es gibt verschiedene Methoden zum Suchen zwischengespeicherter Elemente, je nachdem, ob die Inhaltsgruppe, die die Daten enthält, Treffer- und Invalidierungsselektoren verwendet, wie folgt:

Wenn die Inhaltsgruppe Selektoren verwendet, können Sie die Suche nur mit der Locator-ID für das zwischengespeicherte Element durchführen.

Wenn die Content-Gruppe keine Selektoren verwendet, führen Sie die Suche nach Kriterien wie URL, Host, Name der Inhaltsgruppe durch.

Wenn Sie nach einer zwischengespeicherten Antwort suchen, können Sie einige Elemente nach URL und Host suchen. Wenn sich die Antwort in einer Inhaltsgruppe befindet, die einen Selektor verwendet, können Sie sie nur mithilfe einer Locator-Nummer finden (z. B. 0x00000000ad7af00000050). Um eine Locator-Nummer für die spätere Verwendung zu speichern, klicken Sie mit der rechten Maustaste auf den Eintrag undwählen Sie Weitere Informationen zu Selektoren finden Sie unter Konfigurieren von Selektoren und Basisinhaltsgruppen.

So zeigen Sie zwischengespeicherte Antworten in Inhaltsgruppen an, die keinen Selektor haben, mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show cache object [-locator <positiveInteger>] | [(-url <URL> (-host <
hostName> [-port <port>] [-groupName <contentGroupName>] [-httpMethod GET
 | POST ]))| [-httpStatus<positive integer>] | -group <contentGroupName> |
-ignoreMarkerObjects (ON | OFF)| -includeNotReadyObjects (ON | OFF)]
```

So zeigen Sie zwischengespeicherte Antworten in Inhaltsgruppen mit einem Selektor mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
show cache object -locator <locatorString> MarkerObjects ( ON | OFF )| -
includeNotReadyObjects ( ON | OFF )| [-httpStatus<positive integer>]
```

So zeigen Sie zwischengespeicherte Antworten in Inhaltsgruppen an, die keinen Selektor haben, mit der GUI an

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Cache-Objekte**, klicken Sie auf **Suchen**, und legen Sie die Suchkriterien fest, um die erforderliche zwischengespeicherte Antwort anzuzeigen.

Wenn Sie noch keine Inhaltsgruppen konfiguriert haben, befinden sich alle Objekte in der Gruppe Standard.

So zeigen Sie zwischengespeicherte Antworten in Inhaltsgruppen mit einem Selektor mit der GUI an

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Cache-Objekte**, klicken Sie auf **Suchen**, und legen Sie die Auswahlkriterien fest, um die erforderliche zwischengespeicherte Antwort anzuzeigen.

Cache-Statistiken anzeigen

In der folgenden Tabelle werden die Cache-Statistiken zusammengefasst.

Zähler

Spezifikation

Anzeigen von Cache-Statistiken

Aktualisierung: 28.10.2013

In der folgenden Tabelle werden die detaillierten Cache-Statistiken zusammengefasst, die Sie anzeigen können.

Zähler	Gibt an
Treffer	Antworten, die im integrierten Cache gefunden und aus diesem bereitgestellt werden. Enthält statische Objekte wie Bilddateien, Seiten mit Statuscodes 200, 203, 300, 301, 302, 304, 307, 403, 404, 410 und Antworten, die einer benutzerdefinierten Richtlinie mit einer CACHE-Aktion entsprechen.
Misses	Abgefangene HTTP-Anforderungen, bei denen die Antwort letztlich vom Ursprungsserver abgerufen wurde.

Zähler	Gibt an
Anforderungen	Gesamtanzahl der Cache-Treffer plus Gesamtanzahl der Cache-Fehler.
Non-304 hits	Wenn der Benutzer ein Element mehrmals anfordert und das Element im Cache seit dem letzten Servieren der Citrix ADC Appliance unverändert ist, gibt die Citrix ADC-Appliance anstelle des zwischengespeicherten Objekts eine 304-Antwort an. Diese Statistik gibt an, wie viele Elemente die Citrix ADC Appliance aus dem Cache bedient hat, ausgenommen 304 Antworten.
304 Aufrufe	Anzahl der 304 (Objekt nicht geändert) Antworten, die die Citrix ADC Appliance aus dem Cache bereitgestellt hat.
304 Trefferquote (%)	Prozentsatz der 304 Antworten, die von der Citrix ADC Appliance im Vergleich zu anderen Antworten bereitgestellt wurden.
Trefferquote (%)	Prozentsatz der Antworten, die die Citrix ADC Appliance aus dem Cache gedient hat (Cache-Treffer), relativ zu Antworten, die nicht aus dem Cache bereitgestellt werden konnten.
Original-Bandbreite gespart (%)	Eine Schätzung der Verarbeitungskapazität, die die Citrix ADC Appliance auf dem Ursprungsserver gespeichert hat, da Antworten aus dem Cache bereitgestellt wurden.
Bytes, die vom Citrix ADC bereitgestellt werden	Gesamtanzahl der Bytes, die die Citrix ADC Appliance vom Ursprungsserver und vom Cache bedient hat.
Bytes, die vom Cache bereitgestellt werden	Gesamtanzahl der Bytes, die die Citrix ADC Appliance aus dem Cache bereitgestellt hat.
Byte-Trefferquote (%)	Prozentsatz der Daten, die von der Citrix ADC Appliance aus dem Cache bereitgestellt werden, bezogen auf alle Daten in allen bereitgestellten Antworten.

Zähler	Gibt an
Komprimierte Bytes aus Cache	Datenmenge in Byte, die die Citrix ADC Appliance in komprimierter Form bereitgestellt hat.
Lagerbare Fehlschläge	Wenn die Citrix ADC Appliance kein angefordertes Objekt im Cache findet, ruft sie das Objekt vom Ursprungsserver ab. Dies ist als Cache-Miss bekannt. Ein speicherbarer Cache-Fehler kann im Cache gespeichert werden.
Nicht speicherbare Fehlschläge	Ein nicht speicherbarer Cache-Fehler kann nicht im Cache gespeichert werden.
Misses	Alle Cache-Fehlschläge.
Neuvalidierungen	Die Einstellung “Max-Age” in einem Cache-Control-Header bestimmt in Sekundenanzahl, wann ein zwischengreifender Cache den Inhalt mit dem integrierten Cache erneut validieren muss, bevor er dem Benutzer zugestellt wird. Weitere Informationen finden Sie unter “Einfügen eines Cache-Control-Headers”.
Erfolgreiche Neuvalidierungen	Anzahl der Revalidierungen, die durchgeführt wurden Weitere Informationen finden Sie unter “Einfügen eines Cache-Control-Headers”.
Konvertierungen in bedingte req	Eine User-Agent-Anforderung für ein zwischengespeichertes PET-Objekt wird immer in eine bedingte Anforderung konvertiert und an den Ursprungsserver gesendet. Weitere Informationen finden Sie unter “Polling des Origin Servers, wenn eine Anforderung empfangen wird”.
Speicherbare Fehlerrate (%)	Speicherbarer Cache fehlschlägt als Prozentsatz der nicht speicherbaren Cache-Fehlschläge.

Zähler	Gibt an
Erfolgreiche Revalquote (%)	Erfolgreiche Neuvalidierungen als Prozentsatz aller Neuvalidierungsversuche. Weitere Informationen finden Sie unter “Einfügen eines Cache-Control-Headers”.
Mit dem letzten Byte ablaufen	Anzahl der Male, dass der Cache Inhalt unmittelbar nach Erhalt des letzten Textbytes abgelaufen ist. Gilt nur für positive Antworten, wie in der Tabelle “Cache-Treffer und Fehlschläge” beschrieben. Weitere Informationen finden Sie unter “Beispiel für Leistungsoptimierung”.
Flashcache-Fehlschläge	Wenn Sie Flash Cache aktivieren, erlaubt der Cache nur eine Anforderung, den Server zu erreichen, wodurch Flash Crowds eliminiert werden. Diese Statistik gibt die Anzahl der Flash-Cache-Anforderungen an, bei denen Cache-Fehlschläge vorlagen. Weitere Informationen finden Sie unter “Queuing Requests to the Cache”.
`Flashcache` Hits	Anzahl der Flash-Cache-Anforderungen, bei denen es sich um Cache-Treffer handelte. Weitere Informationen finden Sie unter “Queuing Requests to the Cache”.
Parametrisierte Invas-Anforderungen	Anforderungen, die einer Richtlinie mit einer Invalidierungsaktion (INVAL) und einer Inhaltsgruppe entsprechen, die einen oder mehrere Parameter für die Invalidierung verwendet, um zwischengespeicherte Objekte in der Gruppe selektiv abzulaufen.
Vollständige Invas-Anfragen	Anforderungen, die einer Invalidierungsrichtlinie entsprechen, bei der der Parameter InvalGroups konfiguriert ist und eine oder mehrere Inhaltsgruppen abläuft.

Zähler	Gibt an
Invas-Anfragen	Anforderungen, die einer Invalidierungsrichtlinie entsprechen und zum Ablauf bestimmter zwischengespeicherter Antworten oder ganzer Inhaltsgruppen führen.
Parametrisierte Anforderungen	Anzahl der Cache-Anforderungen, die mit einer Richtlinie mit einer parametrisierten Inhaltsgruppe verarbeitet wurden.
Parametrisierte Nicht-304 Treffer	Anzahl der Cache-Anforderungen, die mit einer Richtlinie mit einer parametrisierten Inhaltsgruppe verarbeitet wurden, wobei eine vollständige zwischengespeicherte Antwort gefunden wurde und die Antwort keine 304 (Objekt nicht aktualisiert) Antwort war.
Parametrisierte 304 Aufrufe	Anzahl der Cache-Anforderungen, die mit einer Richtlinie mit einer parametrisierten Inhaltsgruppe verarbeitet wurden, wobei das zwischengespeicherte Objekt gefunden wurde und das Objekt eine 304-Antwort (Objekt nicht aktualisiert) war.
Gesamtzahl der parametrisierten Treffer	Anzahl der Cache-Anforderungen, die mit einer Richtlinie mit einer parametrisierten Inhaltsgruppe verarbeitet wurden, wobei das zwischengespeicherte Objekt gefunden wurde.
Parametrisierte 304-Trefferquote (%)	Prozentsatz der 304 (Objekt nicht aktualisiert) Antworten, die mithilfe einer parametrisierten Richtlinie gefunden wurden, relativ zu allen Cache-Treffern.
Abfrage jedes Mal Anfragen	Wenn “Jedes Mal abfragen” aktiviert ist, konsultiert die Citrix ADC Appliance immer den Ursprungsserver, bevor ein gespeichertes Objekt bereitgestellt wird. Weitere Informationen finden Sie unter “Polling des Origin Servers, wenn eine Anforderung empfangen wird”.

Zähler	Gibt an
Bei jedem Treffer abfragen	Anzahl, wie oft ein Cache-Treffer mit der Methode “Every Time” gefunden wurde. Weitere Informationen finden Sie unter “Polling des Origin Servers, wenn eine Anforderung empfangen wird”.
Befragung jedes Mal Trefferquote (%)	Prozentsatz der Cache-Treffer mit der Methode “Pol Every Time”, relativ zu allen Suchen nach zwischengespeicherten Objekten mit “Pol Every Time”. Weitere Informationen finden Sie unter “Polling des Origin Servers, wenn eine Anforderung empfangen wird”.
Maximaler Arbeitsspeicher (KB)	Maximale Speichermenge in der Citrix ADC Appliance, die dem Cache zugewiesen ist. Weitere Informationen finden Sie unter “Konfigurieren von globalen Attributen für Caching. “
Maximaler aktiver Arbeitsspeicherwert (KB)	Maximale Speichermenge (aktiver Wert), die festgelegt wird, nachdem der Speicher tatsächlich dem Cache zugewiesen wurde. Weitere Informationen finden Sie unter “Konfigurieren der integrierten Caching-Funktion einer Citrix ADC Appliance für verschiedene Szenarien. “
Ausgelasteter Speicher (KB)	Menge des Speichers, der tatsächlich verwendet wird.
Speicherzuordnungsfehler	Anzahl fehlgeschlagener Versuche, Speicher zum Speichern einer Antwort im Cache zu verwenden.
Bislang größte Antwort	Größte Antwort in Bytes, die entweder im Cache oder im Ursprungsserver gefunden und an den Client gesendet wird.
Gecachte Objekte	Anzahl der Objekte im Cache, einschließlich Antworten, die noch nicht vollständig heruntergeladen wurden und Antworten, die abgelaufen, aber noch nicht geleert wurden.

Zähler	Gibt an
Markierungsobjekte	Markerobjekte werden erstellt, wenn eine Antwort die maximale oder minimale Antwortgröße für die Inhaltsgruppe überschreitet oder die minimale Anzahl von Treffern für die Inhaltsgruppe noch nicht erhalten hat.
Treffer, die serviert werden	Anzahl der Treffer, die aus dem Cache bereitgestellt wurden.
Fehlschläge, die behandelt werden	Antworten, die vom Ursprungsserver abgerufen, im Cache gespeichert und dann gesendet wurden. Sollte die Nummer für lagerbare Fehlschläge annähernd sein. Enthält keine nicht speicherbaren Fehler.

So zeigen Sie zusammenfassende Cache-Statistiken mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat cache
```

So zeigen Sie bestimmte Cache-Statistiken mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1  stat cache -detail
2
3      > stat cache -detail
4      Integrated Cache Statistics - Detail
5      Integrated Cache Statistics - Summary
6                                                  Rate (/s)
                                                      Total
7      Hits                                               0
                            0
8      Misses                                             0
                            0
9      Requests                                           0
                            0
10     Hit ratio(%)                                      --
                            0
```



```
11      Origin bandwidth saved(%)                                --
                            0
12      Cached objects                                           --
                            0
13      Marker objects                                           --
                            0
14                                                    Rate (/s)
                                                         Total
15      Requests                                                  0
                            0
16      Hit Statistics
17                                                    Rate (/s)
                                                         Total
18      Non-304 hits                                              0
                            0
19      304 hits                                                  0
                            0
20      Sql hits                                                  0
                            0
21      Hits                                                      0
                            0
22      304 hit ratio(%)                                         --
                            0
23      Hit ratio(%)                                             --
                            0
24      Origin bandwidth saved(%)                                --
                            0
25
26      Byte Statistics
27                                                    Rate (/s)
                                                         Total
28      Bytes served by Citrix ADC                              648
           55379204
29      Bytes served by cache                                     0
                            0
30      Byte hit ratio(%)                                        --
                            0
31      Compressed bytes from cache                               0
                            0
32      Miss Statistics
33                                                    Rate (/s)
                                                         Total
34      Storable misses                                           0
                            0
35      Non-storable misses                                       0
```



```
                            0
36      Misses                                          0
                            0
37      Revalidations                                   0
                            0
38      Successful revalidations                        0
                            0
39      Conversions to conditional req                  0
                            0
40      Storable miss ratio(%)                         --
                            0
41      Successful reval ratio(%)                      --
                            0
42      Flashcache Statistics
43                                                Rate (/s)
                                                     Total
44      Expire at last byte                             0
                            0
45      Flashcache misses                               0
                            0
46      Flashcache hits                                 0
                            0
47
48      Invalidation Statistics
49                                                Rate (/s)
                                                     Total
50      Parameterized inval requests                    0
                            0
51      Full inval requests                             0
                            0
52      Inval requests                                  0
                            0
53
54      Parameterized Caching Statistics
55                                                Rate (/s)
                                                     Total
56      Parameterized requests                          0
                            0
57      Parameterized non-304 hits                      0
                            0
58      Parameterized 304 hits                          0
                            0
59      Total parameterized hits                        0
                            0
60      Parameterized 304 hit ratio(%)                 --
```



```
                              0
61
62      Poll Every Time (PET) Statistics
63                                                  Rate (/s)
                                                       Total
64      Poll every time requests                             0
                              0
65      Poll every time hits                                 0
                              0
66      Poll every time hit ratio(%)                        --
                              0
67      Memory Usage Statistics
68                                                    Total
69      Maximum memory(KB)                                   0
70      Maximum memory active value(KB)                      0
71      Utilized memory(KB)                                  0
72      Memory allocation failures                           0
73      Largest response so far(B)                           0
74      Cached objects                                       0
75      Marker objects                                       0
76      Hits being served                                    0
77      Misses being handled                                 0
78       Done
79  <!--NeedCopy-->
```

So zeigen Sie zusammenfassende Cache-Statistiken mit der GUI an

1. Klicken Sie oben auf der Seite auf die Registerkarte **Dashboard**.
2. Scrollen Sie nach unten zum Abschnitt Integriertes Caching des Fensters.
3. Um detaillierte Statistiken anzuzeigen, klicken Sie auf den Link Mehr… am unteren Rand der Tabelle.

So zeigen Sie bestimmte Cache-Statistiken mit der GUI an

1. Klicken Sie oben auf der Seite auf die Registerkarte Reporting.
2. Erweitern Sie unter Integrierte Berichte den Eintrag Integrierter Cache, und klicken Sie dann auf den Bericht mit den Statistiken, die Sie anzeigen möchten.
3. Um den Bericht als Vorlage zu speichern, klicken Sie auf Speichern unter, und benennen Sie den Bericht. Der gespeicherte Bericht wird unter Benutzerdefinierte Berichte angezeigt.

Verbesserung der Cache-Performance

October 5, 2021

Sie können die Leistung des integrierten Caches verbessern, einschließlich der gleichzeitigen Bearbeitung von Anfragen für dieselben zwischengespeicherten Daten, Vermeidungen vermeiden, die mit der Aktualisierung zwischengespeicherter Antworten vom Ursprungsserver verbunden sind, und sicherstellen, dass eine Antwort oft genug angefordert wird, um ein Zwischenspeichern zu ermöglichen.

Reduzieren Sie Flash-Massen

Flash-Crowds treten auf, wenn viele Benutzer gleichzeitig dieselben Daten anfordern. Die Anfragen in einer Flash-Crowd können zu Cache-Fehlern werden, wenn Sie den Cache so konfiguriert haben, dass er Treffer erst nach dem Herunterladen des gesamten Objekts bereitgestellt hat.

Die folgenden Techniken können Flash-Massen reduzieren oder beseitigen:

- **PREFETCH**: Aktualisiert eine positive Antwort, bevor sie abläuft, um sicherzustellen, dass sie nie veraltet oder inaktiv wird. Weitere Informationen finden Sie im Abschnitt Eine Antwort vor Ablauf aktualisieren.
- **Cache-Pufferung**: Beginnt mit der Bereitstellung einer Antwort an mehrere Clients, wenn er den Antwortheader vom Original-Server erhält, anstatt darauf zu warten, dass die gesamte Antwort heruntergeladen wird. Die einzige Grenze für die Anzahl der Clients, die eine Antwort gleichzeitig herunterladen können, sind die verfügbaren Systemressourcen. Die Citrix ADC Appliance lädt herunter und sendet Antworten, selbst wenn der Client, der den Download initiiert hat, angehalten wird, bevor der Download abgeschlossen ist. Wenn die Antwort die Cachegröße überschreitet oder wenn die Antwort unterbrochen ist, stoppt der Cache die Antwort, aber der Service für die Clients wird nicht unterbrochen.
- **Flash Cache:** Flash Cache stellt Anforderungen an den Cache in die Warteschlange und erlaubt nur eine Anforderung, den Server gleichzeitig zu erreichen.

Weitere Informationen finden Sie im Abschnitt Queuing Requests to the Cache.

Eine Antwort vor Ablauf aktualisieren

Um sicherzustellen, dass eine zwischengespeicherte Antwort immer neu ist, aktualisiert die Option PREFETCH eine Antwort vor der berechneten Ablaufzeit. Das Prefetch-Intervall wird nach Erhalt der ersten Clientanforderung berechnet. Ab diesem Zeitpunkt aktualisiert die Citrix ADC Appliance die zwischengespeicherte Antwort in einem Zeitintervall, das Sie im Parameter PREFETCH konfigurieren.

Diese Einstellung ist nützlich für Daten, die häufig zwischen Anforderungen aktualisiert werden. Sie gilt nicht für negative Antworten (z. B. 404 Nachrichten).

So konfigurieren Sie den Prefetch für eine Inhaltsgruppe mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set cache contentgroup <name> -prefetch YES [-prefetchPeriod <seconds> | -
prefetchPeriodMilliSec <milliseconds>] [-prefetchMaxPending <positiveInteger
>]
```

*So konfigurieren Sie Prefetch für eine Content-Gruppe mit der GUI

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Content-Gruppen**, und wählen Sie die **Content-Gruppe**aus.

Wählen Sie auf der Registerkarte **Andere** in der Gruppe Flash Crowd und Prefetch die Option **Prefetch** aus, und geben Sie die Werte in den Textfeldern Intervall und Maximale Anzahl der ausstehenden Prefetches an.

Warteschlange Anforderungen an den Cache

Mit der Option Flash Cache werden gleichzeitig ankommende Anforderungen (eine Flash-Crowd) in Warteschlange gestellt, die Antwort abgerufen und an alle Clients verteilt, deren Anforderungen sich in der Warteschlange befinden. Wenn die Antwort während dieses Prozesses nicht zwischengespeichert werden kann, stoppt die Citrix ADC Appliance die Antwort aus dem Cache und sendet stattdessen die Antwort des Ursprungsservers an die Clients in der Warteschlange. Wenn die Antwort nicht verfügbar ist, erhalten die Clients eine Fehlermeldung.

Flash Cache ist standardmäßig deaktiviert. Sie können Poll Every Time (PET) und Flash Cache nicht für dieselbe Content-Gruppe aktivieren.

Ein Nachteil von Flash Cache ist, wenn der Server mit einem Fehler antwortet (z. B. eine 404, die schnell behoben wird), wird der Fehler an die wartenden Clients gesendet.

> **Hinweis**:
> Wenn Flash Cache aktiviert ist, kann die Citrix ADC Appliance in einigen Situationen den Accept-Encoding-Header in der Clientanforderung nicht korrekt mit dem Content-Encoding-Header in der Antwort übereinstimmen. Die Citrix ADC Appliance kann davon ausgehen, dass diese Header übereinstimmen und fälschlicherweise einen Treffer liefern. Als Problemumgehung können Sie integrierte Caching-Richtlinien so konfigurieren, dass die Bereitstellung von Treffern für Clients, die über keinen geeigneten Accept-Encoding-Header verfügen, nicht zulässig ist.

So aktivieren Sie Flash Cache mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cache contentgroup <contentGroupName> -flashcache yes
```

So aktivieren Sie Flash Cache mit der GUI

Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Contentgruppen**, und wählen Sie die Content-Gruppe aus.

Wählen Sie auf der Registerkarte **Sonstiges** in der Gruppe Flash Crowd und Prefetch die Option **Prefetch** aus.

Cache einer Antwort, nachdem ein Client einen Download angehalten hat

Sie können den Parameter Quick Abort festlegen, um die Zwischenspeicherung einer Antwort fortzusetzen, selbst wenn der Client eine Anforderung angehalten hat, bevor sich die Antwort im Cache befindet.

Wenn die heruntergeladene Antwortgröße kleiner oder gleich der Quick Abort Größe ist, beendet die Citrix ADC Appliance das Herunterladen der Antwort. Wenn Sie den Parameter Quick Abort auf 0 setzen, werden alle Downloads angehalten.

So konfigurieren Sie die Größe des schnellen Abbruchs mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cache contentgroup <name> -quickAbortSize <integerInKBytes>
```

So konfigurieren Sie die Größe des schnellen Abbruchs mit der GUI

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Contentgruppen**, und wählen Sie die Content-Gruppe aus.
2. Legen Sie auf der Registerkarte **Speicher** den entsprechenden Wert in Quick Abort: Caching fortsetzen, wenn mehr als das Textfeld.

Erforderliche Mindestanzahl von Servertreffern vor dem Zwischenspeichern

Sie können konfigurieren, wie oft eine Antwort auf dem Ursprungsserver gefunden werden muss, bevor sie zwischengespeichert werden kann. Sie müssen erwägen, die minimalen Treffer zu erhöhen, wenn der Cache-Speicher schnell auffüllt und eine niedrigere als erwartete Trefferquote aufweist.

Der Standardwert für die Mindestanzahl von Treffern ist 0. Dieser Wert speichert die Antwort nach der ersten Anforderung.

So konfigurieren Sie die Mindestanzahl von Treffern, die vor dem Zwischenspeichern erforderlich sind, mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cache contentgroup <name> -minhits <positiveInteger>
```

So konfigurieren Sie die minimale Anzahl von Treffern, die vor dem Caching erforderlich sind, mit der GUI

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Contentgruppen**, und wählen Sie die Content-Gruppe aus.

2. Legen Sie auf der Registerkarte **Speicher** den relevanten Wert in Nicht zwischenspeichern fest, wenn die Treffer kleiner als das Textfeld sind.

Beispiel für die Leistungsoptimierung

In diesem Beispiel greift ein Kunde auf ein Aktienkurs zu. Aktienkurse sind hoch dynamisch. Sie konfigurieren den integrierten Cache so, dass dasselbe Aktienkurse für gleichzeitige Clients bereitgestellt wird, ohne mehrere Anforderungen an den Ursprungsserver zu senden. Der Aktienkurs läuft ab, nachdem er auf die Clients heruntergeladen wurde, und die nächste Anfrage wird vom Ursprungsserver abgerufen. Dadurch wird sichergestellt, dass das Angebot immer auf dem neuesten Stand ist.

In der folgenden Aufgabenübersicht werden die Schritte zum Konfigurieren des Caches für die Aktienanwendung beschrieben.

Caching für eine Aktienanwendung konfigurieren

Erstellen einer Content-Gruppe für Aktienkurse

Weitere Informationen finden Sie unter Inhaltsgruppen.

Konfigurieren Sie Folgendes für diese Content-Gruppe:

1. Aktivieren Sie auf der Registerkarte **Ablaufmethode** das Kontrollkästchen Nach vollständiger Antwort erhalten ablaufen.
2. Aktivieren Sie auf der Registerkarte **Andere** das Kontrollkästchen **Flash Cache**, und klicken Sie auf **Erstellen** .
3. Fügen Sie eine Cache-Richtlinie hinzu, um die Aktienkurse zwischenzuspeichern.

Weitere Informationen finden Sie unter Konfigurieren einer Richtlinie im integrierten Cache.

Konfigurieren Sie Folgendes für die Richtlinie

1. Wählen Sie in den **Listen Aktion und In Gruppe speichern**die Option **CACHE**, und wählen Sie die Gruppe aus, die Sie im vorherigen Schritt definiert haben.
2. Klicken Sie auf **Hinzufügen**, und konfigurieren **Sie im Dialogfeld Ausdruck hinzufügen**einen Ausdruck, der Aktienanfragen identifiziert, zum Beispiel: http.req.url.contains (cgi-bin/stockquote.pl)
3. Aktivieren Sie die Richtlinie.

Weitere Informationen finden Sie unter “Globale Bindung einer integrierten Caching-Richtlinie”. In diesem Beispiel binden Sie diese Richtlinie an die Verarbeitung von Anforderungszeitüberschreibungen und legen die Priorität auf einen niedrigen Wert fest.

Konfigurieren von Cookies, Header und Polling

December 3, 2021

In diesem Thema wird erläutert, wie die Cache-Verwaltung von Cookies, HTTP-Headern und Original-Serverabfragen konfiguriert wird. Dazu gehört das Ändern des Standardverhaltens, das dazu führt, dass der Cache von dokumentierten Standards abweicht, das Überschreiben von HTTP-Headern, die dazu führen könnten, dass cachbarer Inhalt nicht im Cache gespeichert wird, und das Konfigurieren des Caches so, dass immer der Ursprung nach aktualisierten Inhalten abgefragt wird.

Abweichung des Cache-Verhaltens von den Standards

Standardmäßig entspricht der integrierte Cache den folgenden RFC-Standards:

- RFC 2616, “HTTP HTTP/1.1”
- Das in RFC 2617, “HTTP-Authentifizierung: Basic and Digest Access Authentication” beschriebene Caching-Verhalten
- Das in RFC 2965, “HTTP State Management Mechanism” beschriebene Caching-Verhalten

Die integrierten Richtlinien und die Attribute der Standard-Inhaltsgruppe gewährleisten die Konformität mit den meisten dieser Standards.

Das standardmäßige integrierte Cache-Verhalten weicht wie folgt von der Spezifikation ab:

- Es gibt eine begrenzte Unterstützung für den Vari-Header. Standardmäßig wird jede Antwort, die einen Vari-Header enthält, als nicht cachbar angesehen, sofern sie nicht komprimiert ist. Eine komprimierte Antwort enthält Inhaltscodierung: gzip, Inhaltscodierung: deflate oder Inhaltscodierung: pack200-gzip und ist auch dann cachbar, wenn sie den Header Vary: Accept-Codierung enthält.
- Der integrierte Cache ignoriert die Werte der Header-Cache-Steuerung: kein Cache und Cache-Kontrolle: privat. Zum Beispiel wird eine Antwort, die Cache-Kontrolle enthält: NO-Cache=”set-Cookie” behandelt, als ob die Antwort Cache-Control: no-cache enthielt. Standardmäßig wird die Antwort nicht zwischengespeichert.
- Ein Bild (Content-Typ = image/*) wird immer als cachbar betrachtet, auch wenn eine Bild-Antwort Set-Cookie- oder set-cookie2-Header enthält oder wenn eine Bildanforderung einen Cookie-Header enthält. Der integrierte Cache entfernt Set-Cookie- und set-cookie2-Header aus einer Antwort, bevor er zwischengespeichert wird. Dies weicht von RFC 2965 ab. Sie können RFC-konformes Verhalten wie folgt konfigurieren:

```
1 add cache policy rfc_compliant_images_policy -rule ”http.res.header.set
     -cookie2.exists || http.res.header.set-cookie.exists” -action
     NOCACHE
```



```
2
3
4 bind cache global rfc_compliant_images_policy -priority 100 -type
     REQ_OVERRIDE
5 <!--NeedCopy-->
```

- Die folgenden Cache-Control-Header in einer Anforderung erzwingen einen RFC-kompatiblen Cache, eine zwischengespeicherte Antwort vom Original-Server neu zu laden:

```
Cache-control: max-age=0
```

```
Cache-control: no-cache
```

Zum Schutz vor Denial-of-Service-Angriffen ist dieses Verhalten nicht die Standardeinstellung.

- Standardmäßig betrachtet das Caching-Modul eine Antwort als cachbar, sofern nicht anders ein Response-Header-Status vorliegt. Um dieses Verhalten mit RFC 2616 konform zu machen, setzen Sie `-weakPosRelExpiry` und `-weakNegResExpiry` für alle Inhaltsgruppen auf 0.

Cookies aus einer Antwort entfernen

Cookies sind oft für einen Benutzer personalisiert und sollten in der Regel nicht zwischengespeichert werden. Der Parameter `Remove Response Cookies` entfernt die Header `Set-Cookie and Set-Cookie2`, bevor eine Antwort zwischenspeichert wird. Standardmäßig verhindert die Option `Remove Response Cookies` für eine Content-Gruppe das Zwischenspeichern von Antworten mit den Headern `Set-Cookie` oder `Set-Cookie2`.

> **Hinweis:**
> Wenn Bilder zwischengespeichert werden, besteht das integrierte Verhalten darin, die Header `Set-Cookie` und `Set-Cookie2` vor dem Zwischenspeichern zu entfernen, unabhängig davon, wie die Content-Gruppe konfiguriert ist.
>
> Citrix empfiehlt, dass Sie den Standard `Remove Response Cookies` für jede Content-Gruppe akzeptieren, die eingebettete Antworten speichert, z. B. Bilder.

Konfigurieren von `Remove Response Cookies` für eine Content-Gruppe über die Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cache contentgroup <name> -removeCookies YES
```

Konfigurieren von Response-Cookies für eine Inhaltsgruppe mithilfe der Citrix ADC GUI

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Inhaltsgruppen**, und wählen Sie die Content-Gruppe aus.

2. Wählen Sie auf der Registerkarte **Andere** in der Gruppe **Einstellungen** die Option Response-Cookies entfernen.

Einfügen von HTTP-Headern zur Reaktionszeit

Der integrierte Cache kann HTTP-Header in Antworten einfügen, die sich aus Cache-Anforderungen ergeben. Die Citrix ADC Appliance ändert keine Header in Antworten, die aus Cache-Fehlern resultieren.

In der folgenden Tabelle werden Kopfzeilen beschrieben, die Sie in eine Antwort einfügen können.

Überschrift	Spezifikation
Alter	Gibt das Alter der Antwort in Sekunden an, berechnet aus dem Zeitpunkt, zu dem die Antwort auf dem Original-Server generiert wurde. Standardmäßig fügt der Cache einen Age-Header für jede Antwort ein, die aus dem Cache bereitgestellt wird.
via	Listet Protokolle und Empfänger zwischen den Start- und Endpunkten für eine Anfrage oder eine Antwort auf. Die Citrix ADC Appliance fügt in jede Antwort, die sie aus dem Cache liefert, einen Via-Header ein. Der Standardwert des eingefügten Headers ist `NS-CACHE-10.0`: letztes Oktett der Citrix ADC IP-Adresse. “ Weitere Informationen finden Sie unter “Globale Attribute für das Caching konfigurieren.”

Überschrift	Spezifikation
Tag	Der Cache unterstützt die Response-Validierung mit Last-Modified und Tag Headern, um festzustellen, ob eine Antwort veraltet ist. Der Cache fügt nur dann eine Tag in eine Antwort ein, wenn er die Antwort zwischenspeichert und der Original-Server keinen eigenen Tag Header eingefügt hat. Der Tag Wert ist eine beliebige eindeutige Zahl. Der Tag Wert für eine Antwort ändert sich, wenn sie vom Original-Server aktualisiert wird, aber er bleibt unverändert, wenn der Server eine 304-Antwort (Objekt nicht aktualisiert) sendet. Original-Server generieren normalerweise keine Validatoren für dynamischen Inhalt, da dynamischer Inhalt als nicht cachbar angesehen wird. Sie können dieses Verhalten außer Kraft setzen. Beim Einfügen von Tag Header darf der Cache keine vollständigen Antworten liefern. Stattdessen muss der Benutzeragent die dynamische Antwort, die vom integrierten Cache zum ersten Mal gesendet wurde, zwischenspeichern. Um einen Benutzeragenten zum Zwischenspeichern einer Antwort zu zwingen, konfigurieren Sie den integrierten Cache so, dass er einen Tag Header einfügt und den vom Ursprung bereitgestellten Cache-Control-Header ersetzt.

Überschrift	**Spezifikation**
Cache-Steuerung	Die Citrix ADC Appliance ändert normalerweise keine Header zur Cachefähigkeit in Antworten, die vom Original-Server aus bereitgestellt werden. Wenn der Original-Server eine Antwort sendet, die als nicht cachbar gekennzeichnet ist, behandelt der Client die Antwort als nicht cachbar, auch wenn die Citrix ADC Appliance die Antwort im Cache speichert. Um dynamische Antworten in einem Benutzeragenten zwischenzuspeichern, können Sie Cache-Control-Header vom Original-Server ersetzen. Dies gilt nur für Benutzeragenten und andere dazwischenliegende Caches. Sie haben keinen Einfluss auf den integrierten Cache.

Überschrift	Spezifikation
Alter	Gibt das Alter der Antwort in Sekunden an, berechnet aus dem Zeitpunkt, zu dem die Antwort auf dem Original-Server generiert wurde. Standardmäßig fügt der Cache einen Age-Header für jede Antwort ein, die aus dem Cache bereitgestellt wird.
via	Listet Protokolle und Empfänger zwischen den Start- und Endpunkten für eine Anfrage oder eine Antwort auf. Die Citrix ADC Appliance fügt in jede Antwort, die sie aus dem Cache liefert, einen Via-Header ein. Der Standardwert des eingefügten Headers ist “NS-CACHE-9.2: letztes Oktett der Citrix ADC-IP-Adresse”. Weitere Informationen finden Sie unter “Globale Attribute für das Caching konfigurieren.”

Überschrift	Spezifikation
Tag	Der Cache unterstützt die Antwortvalidierung mithilfe der Header “Letzte Änderung” und “Tag”, um festzustellen, ob eine Antwort veraltet ist. Der Cache fügt nur dann eine Tag in eine Antwort ein, wenn er die Antwort zwischenspeichert und der Original-Server keinen eigenen Tag Header eingefügt hat. Der Tag Wert ist eine beliebige eindeutige Zahl. Der Tag Wert für eine Antwort ändert sich, wenn sie vom Original-Server aktualisiert wird, aber er bleibt unverändert, wenn der Server eine 304-Antwort (Objekt nicht aktualisiert) sendet. Original-Server generieren normalerweise keine Validatoren für dynamischen Inhalt, da dynamischer Inhalt als nicht cachbar angesehen wird. Sie können dieses Verhalten außer Kraft setzen. Beim Einfügen von Tag Header darf der Cache keine vollständigen Antworten liefern. Stattdessen muss der Benutzeragent die dynamische Antwort, die vom integrierten Cache zum ersten Mal gesendet wurde, zwischenspeichern. Um einen Benutzeragenten zum Zwischenspeichern einer Antwort zu zwingen, konfigurieren Sie den integrierten Cache so, dass er einen Tag Header einfügt und den vom Ursprung bereitgestellten Cache-Control-Header ersetzt.

Überschrift	Spezifikation
Cache-Steuerung	Die Citrix ADC Appliance ändert normalerweise keine Header zur Cachefähigkeit in Antworten, die vom Original-Server aus bereitgestellt werden. Wenn der Original-Server eine Antwort sendet, die als nicht cachbar gekennzeichnet ist, behandelt der Client die Antwort als nicht cachbar, auch wenn die Citrix ADC Appliance die Antwort im Cache speichert. Um dynamische Antworten in einem Benutzeragenten zwischenzuspeichern, können Sie Cache-Control-Header vom Original-Server ersetzen. Dies gilt nur für Benutzeragenten und andere dazwischenliegende Caches. Sie haben keinen Einfluss auf den integrierten Cache.

Fügen Sie einen Alter-, via- oder Tag-Header ein

In den folgenden Verfahren wird beschrieben, wie Age-, Via- und `ETag` Header eingefügt werden.

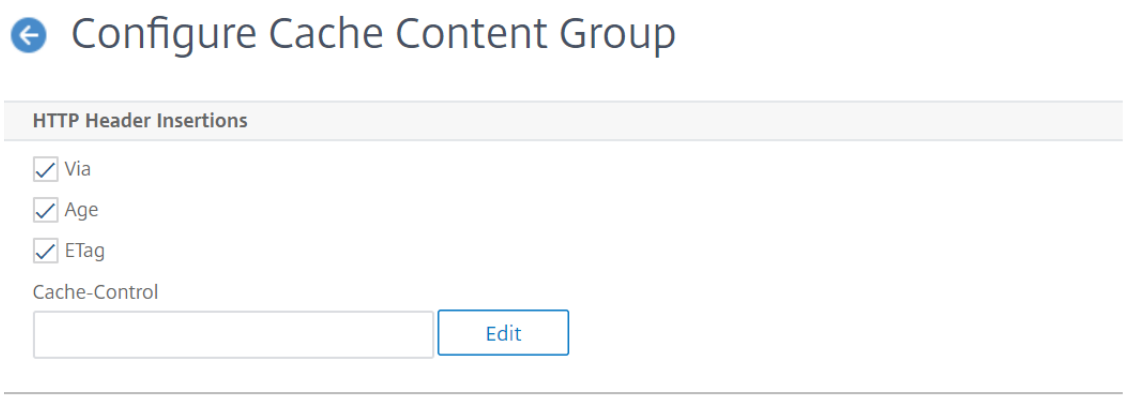
Fügen Sie mithilfe der Citrix ADC-Befehlsschnittstelle einen Age-, Via- oder ETAG-Headerein:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cache contentgroup <name> -insertVia YES -insertAge YES -insertETag YES
```

Konfigurieren Sie den Age-, Via- oder ETAG-Header mithilfe der Citrix ADC GUI

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Inhaltsgruppen,** und wählen Sie die **Content-Gruppe**aus.
2. Wählen Sie auf der Registerkarte **Andere** in der Gruppe HTTP-Header-Einfügungen nach Bedarf die Optionen **Via**, **Age**oder **ETag** aus.
3. Die Werte für die anderen Kopfzeilentypen werden automatisch berechnet. Den Via-Wert konfigurieren Sie in den Haupteinstellungen für den Cache.



Fügen Sie einen Cache-Control-Header ein

Wenn der integrierte Cache einen vom Originalserver eingefügten Cache-Control-Header ersetzt, ersetzt er auch den Expires-Header. Der neue Expires-Header enthält eine Ablaufzeit in der Vergangenheit. Dadurch wird sichergestellt, dass HTTP/1.0-Clients und -Caches (die den Cache-Control-Header nicht verstehen) den Inhalt nicht zwischenspeichern.

Fügen Sie mithilfe der Citrix ADC Befehlszeilenschnittstelle einen Cache-Control-Header ein

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cache contentgroup <name> -cacheControl <value>
```

Fügen Sie einen Cache-Control-Header mithilfe der Citrix ADC GUI ein

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Content-Gruppen**und
   a) Klicken Sie auf **Ablaufmethode**, um die Heuristik und die standardmäßigen Ablaufeinstellungen zu löschen und den entsprechenden Wert im Textfeld Inhalt ablaufen nach festzulegen.
   b) Klicken Sie auf die Registerkarte **Andere** und geben Sie den Header, den Sie einfügen möchten, in das Textfeld Cache-Control ein. Klicken Sie alternativ auf Konfigurieren, um die Cache-Control-Direktiven in zwischengespeicherten Antworten festzulegen.

Ignoriere Cache-Kontrolle und Pragma-Header in Anfragen

Standardmäßig verarbeitet das Caching-Modul Cache-Control- und Pragma-Header. Die folgenden Token in den Cache-Control-Headern werden wie in RFC 2616 beschrieben verarbeitet.

- max-age
- max-abgestanden
- nur-wenn-zwischengespeichert

- kein Cache

Ein Pragma: No-Cache-Header in einer Anforderung wird genauso behandelt wie ein Cache-Control: No-Cache-Header.

Wenn Sie das Caching-Modul so konfigurieren, dass es die Header Cache-Control und Pragma ignoriert, veranlasst eine Anforderung, die einen Cache-Control: No-Cache-Header enthält, die Citrix ADC Appliance, die Antwort vom Original-Server abzurufen, aber die zwischengespeicherte Antwort wird nicht aktualisiert. Wenn das Caching-Modul Cache-Control- und Pragma-Header verarbeitet, wird die zwischengespeicherte Antwort aktualisiert.

In der folgenden Tabelle sind die Auswirkungen verschiedener Einstellungen für diese Header und die Einstellung Neuladeanforderung des Browsers ignorieren zusammengefasst.

Einstellung für Ignorieren-Cache-Control und Pragma-Header	Einstellung für Neuladeanfrage des Browsers ignorieren	Ergebnis
Ja	Ja oder Nein	Ignorieren Sie die Cache-Control- und Pragma-Header des Clients, einschließlich der Cache-Control: no-Cache-Direktive.
Nein	Ja	Der Cache-Control: No-Cache-Header erzeugt einen Cache-Fehlschuss, aber eine Antwort, die sich bereits im Cache befindet, wird nicht aktualisiert.
Nein	Nein	Eine Anforderung, die einen Cache-Control: No-Cache-Header enthält, verursacht einen Cache-Fehlschlag und die gespeicherte Antwort wird aktualisiert.

So ignorieren Sie Cache-Control- und Pragma-Header in einer Anforderung mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set cache contentgroup <name> -ignoreReqCachingHdrs YES
```

So ignorieren Sie Anfragen zum Neuladen von Browsern mithilfe der Befehlszeilenschnittstelle

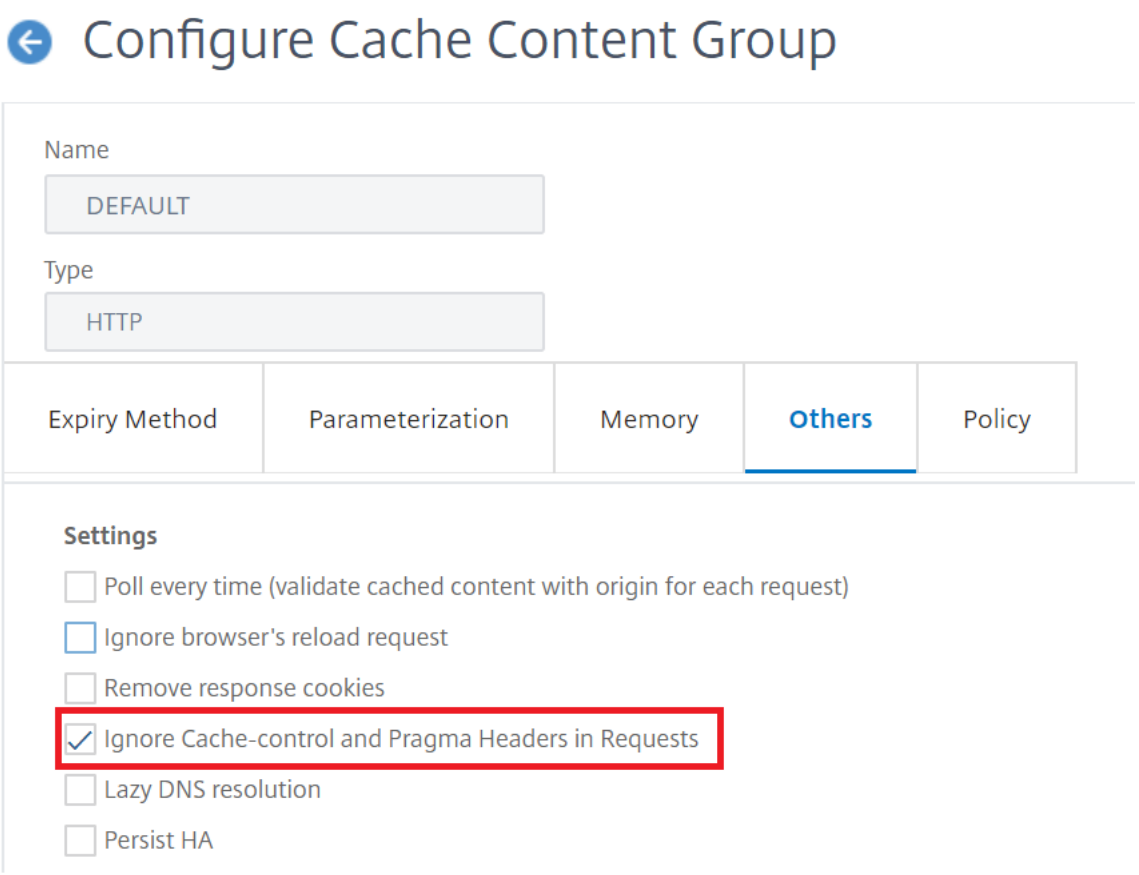
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cache contentgroup <name> -ignoreReloadReq NO
```

> **Hinweis:**
> Standardmäßig ist der Parameter -IgnoreReloadReq auf YES festgelegt.

Ignorieren Sie Cache-Control- und Pragma-Header in einer Anfrage mithilfe der GUI

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Inhaltsgruppen**, und wählen Sie die Content-Gruppe aus.
2. Wählen Sie auf der Registerkarte **Andere** in der Gruppe **Einstellungen** die Option **Cache-Control und Pragma-Header in**Anfragen**ignorieren** aus.



Beispiel für eine Richtlinie zum Ignorieren von Cache-Control-Headern:

Im folgenden Beispiel konfigurieren Sie eine Richtlinie zum Überschreiben der Anforderungszeit, um Antworten zu cachen, die Content-Typ enthalten: image/* unabhängig vom Cache-Control-Header in der Antwort.

Konfigurieren einer Richtlinie zum Überschreiben der Anforderungszeit, um alle Antworten mit image/* zu cachen

Leeren Sie den Cache mit der Option Alle ungültig machen.

Konfigurieren Sie eine neue Cache-Richtlinie und leiten Sie die Richtlinie an eine bestimmte Content-Gruppe weiter. Weitere Informationen finden Sie unter “Konfigurieren einer Richtlinie im integrierten Cache. “

Stellen Sie sicher, dass die von der Richtlinie verwendete Content-Gruppe so konfiguriert ist, dass sie Cache-Control-Header ignoriert, wie in “Cache-Control und Pragma-Header in Requests ignorieren” beschrieben ist.

Binden Sie die Richtlinie an die Richtlinienbank für die Anforderungszeitüberschreibung.

Weitere Informationen finden Sie unter Global Binden einer integrierten Caching-Richtlinie .

Poll-Original-Server jedes Mal, wenn eine Anfrage empfangen wird

Sie können die Citrix ADC Appliance so konfigurieren, dass sie immer den Original-Server konsultiert, bevor eine gespeicherte Antwort gesendet wird. Dies ist bekannt als Poll Every Time (PET). Wenn die Citrix ADC Appliance den Original-Server konsultiert und die PET-Antwort nicht abgelaufen ist, überschreibt eine vollständige Antwort des Original-Servers den zwischengespeicherten Inhalt nicht. Diese Eigenschaft ist nützlich, wenn Sie kundenspezifische Inhalte bereitstellen.

Nachdem eine PET-Antwort abgelaufen ist, aktualisiert die Citrix ADC Appliance sie, wenn die erste vollständige Antwort vom Original-Server eingeht.

Die Funktion “Poll Every Time” (PET) funktioniert wie folgt:

Bei einer zwischengespeicherten Antwort, die Validatoren in Form eines Tags oder eines Headers für die letzte Änderung enthält, wird die Antwort automatisch als PET gekennzeichnet und zwischengespeichert, wenn sie abläuft.

Sie können PET für eine Content-Gruppe konfigurieren.

Wenn Sie eine Content-Gruppe als PET konfigurieren, wird jede Antwort in der Content-Gruppe als PET gekennzeichnet. Die PET-Inhaltsgruppe kann Antworten speichern, die keine Validatoren haben. Antworten, die automatisch als PET gekennzeichnet sind, sind immer abgelaufen. Antworten, die zu einer PET-Inhaltsgruppe gehören, können nach einer Verzögerung ablaufen, je nachdem, wie Sie die Content-Gruppe konfigurieren.

Zwei Arten von Anfragen sind von Abfragen betroffen:

- Bedingte Anfragen: Ein Kunde stellt eine bedingte Anfrage aus, um sicherzustellen, dass die Antwort, die er hat, die neueste Kopie ist. Eine User-Agent-Anfrage für eine zwischengespeicherte PET-Antwort wird immer in eine bedingte Anforderung umgewandelt und an den

Original-Server gesendet. Eine bedingte Anforderung hat Validatoren in Headern If-Modified-Since oder If-None-Match. Der Header “Wenn-Modifiziert-Since” enthält die Zeit aus dem Header “Letzte Änderung”. Ein If-None-Match-Header enthält den Tag-Header-Wert der Antwort. Wenn die Kopie der Antwort des Clients neu ist, antwortet der Original-Server mit 304 Not Modified. Wenn die Kopie veraltet ist, generiert eine bedingte Antwort ein 200 OK, das die gesamte Antwort enthält.

- Unbedingte Anfragen: Eine bedingungslose Anforderung kann nur 200 OK generieren, die die gesamte Antwort enthält.

Antwort des Original-Servers	Aktion
Sende die vollständige Antwort	Der Original-Server sendet die Antwort unverändert an den Client. Wenn die zwischengespeicherte Antwort abgelaufen ist, wird sie aktualisiert.
304 nicht modifiziert	Die folgenden Header-Werte in der 304-Antwort werden mit der zwischengespeicherten Antwort zusammengeführt und die zwischengespeicherte Antwort wird dem Client zugestellt: Date, Expires, Age, Cache-Control-Header Max-Age und S-Maxage-Token
401 nicht autorisiert; 400 schlechte Anfrage; 405 Methode nicht zulässig; 406 nicht akzeptabel; 407 Proxy-Authentifizierung erforderlich	Die Antwort des Ursprungs wird dem Kunden so serviert, wie sie ist. Die zwischengespeicherte Antwort wird nicht geändert.
Jede andere Fehlerantwort, z. B. 404 Not Found	Die Antwort des Ursprungs wird dem Kunden so serviert, wie sie ist. Die zwischengespeicherte Antwort wird entfernt.

> **Hinweis:**
> Der Parameter “Umfrage jedes Mal” behandelt die betroffenen Antworten als nicht speicherbar.

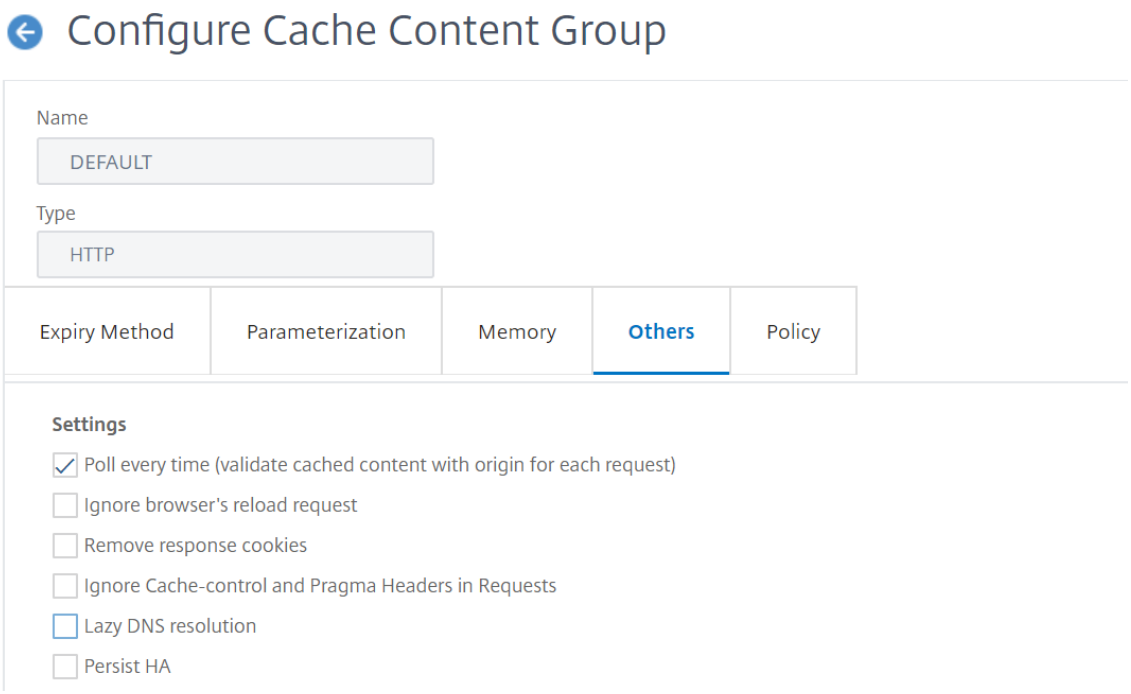
So konfigurieren Sie die Umfrage jedes Mal mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cache contentgroup <contentGroupName> -pollEveryTime YES
```


Umfrage mit der GUI

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Inhaltsgruppen**, und wählen Sie die Content-Gruppe aus.
2. Wählen Sie auf der Registerkarte **Andere** in der Gruppe Einstellungen die Option Jedes Mal abfragen (zwischengespeicherten Inhalt mit Ursprung für jede Anfrage überprüfen).



PET und kundenspezifische Inhalte

Die PET-Funktion kann sicherstellen, dass der Inhalt für einen Kunden angepasst wird. Beispielsweise untersucht eine Website, die Inhalte in mehreren Sprachen bereitstellt, den Accept-Language-Anforderungsheader, um die Sprache für den Inhalt auszuwählen, den sie bereitstellt. Bei einer mehrsprachigen Website, bei der Englisch die vorherrschende Sprache ist, können alle englischsprachigen Inhalte in einer PET-Inhaltsgruppe zwischengespeichert werden. Dadurch wird sichergestellt, dass jede Anfrage an den Original-Server geht, um die Sprache für die Antwort zu bestimmen. Wenn die Antwort englisch ist und sich der Inhalt nicht geändert hat, kann der Original-Server eine 304 Not Modified für den Cache bereitstellen.

Das folgende Beispiel zeigt Befehle zum Zwischenspeichern englischer Antworten in einer PET-Inhaltsgruppe, zum Konfigurieren eines benannten Ausdrucks, der englische Antworten im Cache identifiziert, und zum Konfigurieren einer Richtlinie, die diese Inhaltsgruppe und den benannten Ausdruck verwendet. Fett wird zur Betonung verwendet:


```
add cache contentgroup EnglishLanguageGroup -pollEveryTime YES
add expression containsENExpression  - rule ”http.res.header(\\”Content-
    Language\\”).contains(\\”en\\”)”
add cache policy englishPolicy -rule containsENExpression -action CACHE
     -storeInGroup englishLanguageGroup
bind cache policy englishPolicy -priority 100 -precedeDefRules NO
<!--NeedCopy-->
```

PET und Authentifizierung, Autorisierung und Prüfung

Outlook Web Access (OWA) ist ein gutes Beispiel für dynamisch generierte Inhalte, die von PET profitieren. Alle E-Mail-Antworten (*.EML-Objekte) haben einen `ETag` Validator, mit dem sie als PET-Antworten gespeichert werden können.

Jede Anfrage nach einer E-Mail-Antwort wird an den Original-Server weitergegeben, auch wenn die Antwort zwischengespeichert ist. Der Original-Server bestimmt, ob der Anforderer authentifiziert und autorisiert ist. Es überprüft auch, ob die Antwort im Original-Server vorhanden ist. Wenn alle Ergebnisse positiv sind, sendet der Ursprungsserver eine 304 Not Modified Antwort.

Integrierten Cache als Forward-Proxy konfigurieren

October 5, 2021

Der integrierte Cache kann als Forward-Proxygerät fungieren, das Anforderungen an andere Citrix ADC Appliances oder andere Typen von Cacheservern weiterleitet. Sie konfigurieren den integrierten Cache als Forward-Proxy, indem Sie die IP-Adressen des Cacheservers oder der Server identifizieren. Nach der Konfiguration des Forwardproxy sendet die Citrix ADC Appliance Anforderungen, die die konfigurierte IP-Adresse enthalten, an den Cacheserver, anstatt den integrierten Cache einzubeziehen.

So konfigurieren Sie Citrix ADC als Forward-Cache-Proxy mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cache forwardProxy <IPAddress> <port>
```

So konfigurieren Sie Citrix ADC als Forward-Cache-Proxy mit der GUI

1. Navigieren Sie zu **Optimierung** > **Integriertes Caching** > **Forward-Proxy**, und fügen Sie einen Forward-Proxy hinzu, indem Sie die IP-Adresse und die Portnummer angeben.

Standardeinstellungen für den integrierten Cache

October 5, 2021

Die integrierte Cache-Funktion von Citrix ADC bietet integrierte Richtlinien mit Standardeinstellungen und Anfangseinstellungen für die Standard-Content-Gruppe. Die Informationen in diesem Abschnitt definieren die Parameter für die integrierten Richtlinien und die Standardinhaltsgruppe.

Standard-Caching-Richtlinien

Der integrierte Cache verfügt über integrierte Richtlinien. Die Citrix ADC Appliance wertet die Richtlinien in einer bestimmten Reihenfolge aus, wie in den folgenden Abschnitten erläutert.

Sie können diese integrierten Richtlinien mit einer benutzerdefinierten Richtlinie überschreiben, die an eine Richtlinienbank für Anforderungszeitüberschreibung oder Antwortzeitüberschreibung gebunden ist.

> **Hinweis:**
> Wenn Sie Richtlinien vor Version 9.0 konfiguriert und beim Binden der Richtlinien den Parameter -precedeDefRules angegeben haben, werden diese während der Migration automatisch den Überschreibungszeit-Bindungspunkten zugewiesen.

Standardrichtlinien anzeigen

Die integrierten Richtliniennamen beginnen mit einem Unterstrich (_). Sie können die integrierten Richtlinien über die Befehlszeile und die Verwaltungskonsole mit dem Befehl show cache policy anzeigen.

Standardanforderungsrichtlinien

Sie können die folgenden integrierten Anforderungszeitrichtlinien überschreiben, indem Sie neue Richtlinien konfigurieren und sie an den Verarbeitungspunkt für die Anforderungszeitüberschreibung binden. Beachten Sie in den folgenden Richtlinien, dass die MAY_NOCACHE-Aktion vorschreibt, dass die Transaktion nur zwischengespeichert wird, wenn eine vom Benutzer konfigurierte oder integrierte CACHE-Direktive zur Antwortzeit vorhanden ist.

Die folgenden Richtlinien sind an die Richtlinienbeschriftung _reqBuiltinDefaults gebunden. Sie werden in der Prioritätsreihenfolge aufgeführt.

Cache keine Antwort für eine Anforderung, die eine andere Methode als GET verwendet.

Der Richtlinienname ist _nonGetReq. Die folgende Richtlinienregel ist:

```
!HTTP.REQ.METHOD.eq(GET)
```


Legen Sie eine NOCACHE-Aktion für eine Anforderung mit einem Header-Wert fest, der If-Match oder If-Unmodified-Since enthält.

Der Richtlinienname ist _advancedConditionalReq. Die folgende Richtlinienregel ist:

```
HTTP.REQ.HEADER("If-Match").EXISTS || HTTP.REQ.HEADER("If-Unmodified-Since"
).EXISTS
```

Legen Sie eine MAY_NOCACHE-Aktion für eine Anfrage mit den folgenden Header-Werten fest: Cookie, Autorisierung, Proxy-Autorisierung oder eine Anfrage, die den NTLM- oder Negotiate-Header enthält.

Der Richtlinienname ist _personalizedReq. Die folgende Richtlinienregel ist:

```
HTTP.REQ.HEADER("Cookie").EXISTS || HTTP.REQ.HEADER("Authorization").EXISTS
 || HTTP.REQ.HEADER("Proxy-Authorization").EXISTS || HTTP.REQ.IS_NTLM_OR_NEGOTIATE
```

Standardantwortrichtlinien

Sie können die folgenden Standardrichtlinien für die Antwortzeit außer Kraft setzen, indem Sie neue Richtlinien konfigurieren und sie an den Verarbeitungspunkt für die Antwortzeitüberschreibung binden.

Die folgenden Richtlinien sind an das Richtlinienlabel **_resBuiltinDefaults** gebunden und werden in der Reihenfolge ausgewertet, in der sie aufgeführt sind:

1. Cache HTTP-Antworten nur, wenn sie vom Typ 200, 304, 307, 203 sind oder wenn die Typen zwischen 400 und 499 oder zwischen 300 und 302 liegen.

   Der Richtlinienname ist **_uncacheableStatusRes**. Die folgende Richtlinienregel ist:

   ```
   !((HTTP.RES.STATUS.EQ(200))|| (HTTP.RES.STATUS.EQ(304))|| (HTTP.RES.
   STATUS.BETWEEN(400,499))|| (HTTP.RES.STATUS.BETWEEN(300, 302))|| (HTTP.
   RES.STATUS.EQ(307))|| (HTTP.RES.STATUS.EQ(203)))
   ```

2. Cache eine HTTP-Antwort nicht, wenn sie einen Variy-Header mit einem Wert von etwas anderem als Accept-Encoding hat.

   Das Komprimierungsmodul fügt den Header Vary: Accept_Encoding ein. Der Name dieses Ausdrucks ist **_uncacheableVaryRes**. Die folgende Richtlinienregel ist:

   ```
   ((HTTP.RES.HEADER("Vary").EXISTS)&& ((HTTP.RES.HEADER("Vary").INSTANCE
   (1).LENGTH > 0)|| (!HTTP.RES.HEADER("Vary").STRIP_END\\_WS.SET_TEXT_MODE
   (IGNORECASE).eq("Accept-Encoding"))))
   ```

3. Cache-Control-Header-Wert No-Cache, No-Store oder Privat lautet oder wenn der Cache-Control-Header ungültig ist.

   Der Richtlinienname ist **_uncacheableCacheControlRes**. Die folgende Richtlinienregel ist:


```
((HTTP.RES.CACHE\\_CONTROL.IS\\_PRIVATE)|| (HTTP.RES.CACHE\\_CONTROL.IS
\\_NO\\_CACHE)|| (HTTP.RES.CACHE\\_CONTROL.IS\\_NO\\_STORE)|| (HTTP.RES
.CACHE\\_CONTROL.IS\\_INVALID))
```

4. Cache-Control-Header hat einen der folgenden Werte: Public, Must-Revalidate, Proxy-Revalidate, Max-Age, S-Maxage.

   Der Richtlinienname ist **_cacheableCacheControlRes**. Die folgende Richtlinienregel ist:

   ```
   ((HTTP.RES.CACHE_CONTROL.IS_PUBLIC)|| (HTTP.RES.CACHE_CONTROL.IS_MAX_AGE
   )|| (HTTP.RES.CACHE_CONTROL.IS_MUST_REVALIDATE)|| (HTTP.RES.CACHE_CONTROL
   .IS_PROXY_REVALIDATE)|| (HTTP.RES.CACHE_CONTROL.IS_S_MAXAGE))
   ```

5. Cache keine Antworten, die einen Pragma-Header enthalten.

   Der Name der Richtlinie lautet **_uncacheablePragmaRes**. Die folgende Richtlinienregel ist:

   ```
   HTTP.RES.HEADER("Pragma").EXISTS
   ```

6. Cache-Antworten, die einen Expires-Header enthalten.

   Der Name der Richtlinie lautet **_cacheableExpiryRes**. Die folgende Richtlinienregel ist:

   ```
   HTTP.RES.HEADER("Expires").EXISTS
   ```

7. Wenn die Antwort einen Content-Type-Header mit dem Wert Image enthält, entfernen Sie alle Cookies im Header und speichern Sie sie.

   Der Name der Richtlinie lautet **_imageRes**. Die folgende Richtlinienregel ist:

   ```
   HTTP.RES.HEADER("Content-Type").SET_TEXT_MODE(IGNORECASE).STARTSWITH("
   image/")
   ```

   Sie können die folgende Content-Gruppe für die Arbeit mit dieser Richtlinie konfigurieren:

   ```
   add cache contentgroup nocookie -group -removeCookies YES
   ```

8. Cache keine Antwort, die einen Set-Cookie-Header enthält.

   Der Name der Richtlinie lautet **_ personalizedRes**. Die folgende Richtlinienregel ist:

HTTP.RES.HEADER("Set-Cookie").EXISTS	HTTP.RES.HEADER("Set-Cookie2").EXISTS

Einschränkungen für Standardrichtlinien

Sie können die folgenden integrierten Anforderungszeitrichtlinien nicht mit benutzerdefinierten Richtlinien überschreiben.

Diese Richtlinien werden in der Prioritätsreihenfolge aufgeführt.

1. Zwischenspeichern Sie keine Antworten, wenn die entsprechende HTTP-Anforderung keine GET- oder POST-Methode enthält.
2. Zwischenspeichern Sie keine Antworten für eine Anforderung, wenn die URL-Länge der HTTP-Anforderung plus Hostname 1744 Byes überschreitet.
3. Zwischenspeichern Sie keine Antwort für eine Anforderung, die einen If-Match-Header enthält.
4. Zwischenspeichern Sie keine Anforderung, die einen If-Unmodified-Since Header enthält.

> **Hinweis**
> Dies unterscheidet sich von der If-Modified-Since Header.

1. Keine Antwort zwischenspeichern, wenn der Server keinen Ablauf-Header festlegt.

Sie können die folgenden integrierten Richtlinien für die Antwortzeit nicht überschreiben. Diese Richtlinien werden in der Reihenfolge ausgewertet, in der sie aufgeführt sind:

1. Cache keine Antworten, die einen HTTP-Antwortstatuscode 201, 202, 204, 205 oder 206 haben.
2. Zwischenspeichern Sie keine Antworten mit einem HTTP-Antwortstatuscode 4xx, mit Ausnahme der Statuscodes 403, 404 und 410.
3. Cache keine Antworten, wenn der Antworttyp FIN beendet ist oder die Antwort kein der folgenden Attribute aufweist: Content-Length oder Transfer-Encoding: Chunked.
4. Cache die Antwort nicht, wenn das Cache-Control-Header nicht analysieren kann.

Anfangseinstellungen für die Standard-Content-Gruppe

Wenn Sie das integrierte Caching zum ersten Mal aktivieren, stellt die Citrix ADC Appliance eine vordefinierte Inhaltsgruppe mit der Bezeichnung Standardinhaltsgruppe zur Verfügung. Ausführliche Informationen finden Sie unter Tabelle mit Standardeinstellungen für Inhaltsgruppen .

Problembehandlung

October 5, 2021

Wenn das integrierte Cache-Feature nach der Konfiguration nicht wie erwartet funktioniert, können Sie einige gängige Tools verwenden, um auf Citrix ADC Ressourcen zuzugreifen und das Problem zu diagnostizieren.

Ressourcen für die Fehlerbehebung

Weitere Informationen zu den Ressourcen, die für die Fehlerbehebung und Beispielkonfigurationen verfügbar sind, finden Sie unter Ressource zur Fehlerbehebung bei PDF-Dateien.

Front-End-Optimierung

October 5, 2021

> **Hinweis:** Die Front-End-Optimierung ist verfügbar, wenn Sie über eine Advanced oder Premium Citrix ADC Lizenz verfügen und Citrix ADC Version 10.5 oder höher ausführen.

Die HTTP-Protokolle, die Webanwendungen zugrunde liegen, wurden ursprünglich entwickelt, um die Übertragung und das Rendern einfacher Webseiten zu unterstützen. Neue Technologien wie JavaScript und Cascading Stylesheets (CSS) sowie neue Medientypen wie Flash-Videos und grafikreiche Bilder stellen hohe Anforderungen an die Front-End-Performance, also an die Leistung auf Browserebene.

Die Citrix ADC Front-End-Optimierung (FEO) -Funktion behebt solche Probleme und reduziert die Ladezeit und die Rendering-Zeit von Webseiten durch:

- Reduzierung der Anzahl der Anforderungen.
- Erforderlich für das Rendern jeder Seite.
- Reduzieren der Anzahl von Bytes in Seitenantworten.

Vereinfachung und Optimierung der Inhalte, die dem Client-Browser bereitgestellt werden.

Sie können Ihre FEO-Konfiguration anpassen, um den Benutzern die besten Ergebnisse zu bieten. Citrix ADCs unterstützen zahlreiche Webinhaltsoptimierungen sowohl für Desktop- als auch für mobile Benutzer. In den folgenden Tabellen werden die Front-End-Optimierungen beschrieben, die von der FEO-Funktion bereitgestellt werden, und die Vorgänge, die für verschiedene Dateitypen ausgeführt werden.

Optimierungen durch die FEO-Funktion

Weboptimierung	Problem	Funktionen von Citrix ADC FEO	Vorteile
Inlining	Clientbrowser senden häufig mehrere Anfragen an Server, um externe CSS, Bilder und JavaScript zu laden, die mit der Webseite verknüpft sind.	CSS Inline, JavaScript Inline, CSS kombinieren	Das Laden von externen CSS, Bildern und JavaScript inline mit den HTML-Dateien verbessert die Seitenrendering-Zeit. Diese Optimierung ist vorteilhaft für Inhalte, die nur einmal angezeigt werden, und für Mobilgeräte mit begrenzten Cache-Größen.
Minimierung	Daten, die von Servern abgerufen werden, umfassen unwesentliche Zeichen wie Leerzeichen, Kommentare und Zeilenumbrüche. Die Zeit, die Browser mit der Verarbeitung solcher Daten verbringen, erzeugt Website-Latenz.	CSS-Minimierung, JavaScript-Minimierung, Entfernen von HTML-Kommentaren	Minimierte Dateien verbrauchen weniger Bandbreite und vermeiden die Latenz, die durch spezielle Verarbeitung verursacht wird.

Weboptimierung	Problem	Funktionen von Citrix ADC FEO	Vorteile
Bildoptimierung	Mobile Browser haben oft langsame Verbindungs-geschwindigkeiten und begrenzten Cache-Speicher. Das Herunterladen der Bilder auf mobile Clients verbraucht mehr Bandbreite, Verarbeitungszeit und Cache-Speicherplatz, was zu einer Website-Latenz führt.	JPEG-Optimierung, CSS-Bild-Inlining, **Bildschrumpfung** -Attribute, GIF zu PNG-Konvertierung, HTML-Bild-Inlining, WebP-Bildkonvertierung, JPEG, GIF, PNG zu JPEG-XR-Bildkonvertierung	Reduziert das Bild auf die Größe, die im Image-Tag von Citrix ADC angegeben wird, sodass Clientbrowser Bilder schneller laden können.
Neupositionierung	Die ineffiziente Verarbeitung von externen CSS, Bildern und JavaScript erhöht die Seitenladezeit.	Bild lazy loading, CSS move to Head, JavaScript move to end	Positioniert HTML-Elemente neu, um die Rendering-Zeit für Webseiten zu reduzieren und es Clientbrowsern zu ermöglichen, die Objekte schneller zu laden.

Weboptimierung	Problem	Funktionen von Citrix ADC FEO	Vorteile
Verbindungsverwaltung	Viele Browser legen Beschränkungen für die Anzahl gleichzeitiger Verbindungen fest, die mit einer einzelnen Domäne hergestellt werden können. Dies kann dazu führen, dass Browser Webseitenressourcen einzeln herunterladen, was zu einer höheren Browserzeit führt.	Domänenfreigabeverfa	Überwindet die Verbindungs-beschränkung, wodurch die Zeit für das Rendering von Seiten verbessert wird, da Client-Browsern mehr Ressourcen parallel herunterladen können.

Web-Optimierungen für verschiedene Dateitypen:

Citrix ADC kann Weboptimierungen für CSS, Bilder, Javascript und HTML durchführen. Weitere Informationen finden Sie unter PDF zur Weboptimierung .

> **Hinweis:**
> Die Front-End-Optimierungsfunktion unterstützt nur ASCII-Zeichen. Es unterstützt den Unicode-Zeichensatz nicht.

Funktionsweise der Front-End-Optimierung

Nachdem der Citrix ADC die Antwort vom Server empfängt:

1. Analysiert den Inhalt der Seite, erstellt einen Eintrag im Cache (wo immer zutreffend) und wendet die FEO-Richtlinie an.

   Beispielsweise kann ein Citrix ADC die folgenden Optimierungsregeln anwenden:

   - Entfernen Sie Leerzeichen oder Kommentare, die in einem CSS oder JavaScript vorhanden sind.
   - Kombinieren Sie eine oder mehrere CSS-Dateien zu einer Datei.
   - Konvertieren Sie GIF-Bildformat in PNG-Format.

2. Schreibt die eingebetteten Objekte neu und speichert den optimierten Inhalt im Cache mit einer anderen Signatur als die für den ursprünglichen Cache-Eintrag verwendete Signatur.
3. Ruft bei nachfolgenden Anforderungen die optimierten Objekte aus dem Cache ab, nicht vom Server, und leitet die Antworten an den Client weiter.

**

Entfernen Sie fremde Informationen wie Leerzeichen und Kommentare.

Der Zeitraum, in dem der Browser die zwischengespeicherte Ressource verwenden kann, ohne zu überprüfen, ob neue Inhalte auf dem Server verfügbar sind.

Konfigurieren der Front-End-Optimierung

Optional können Sie die Werte der globalen Einstellungen der Front-End-Optimierung ändern. Andernfalls erstellen Sie zunächst Aktionen, die die Optimierungsregeln angeben, die auf die eingebetteten Objekte angewendet werden sollen.

Erstellen Sie nach dem Konfigurieren von Aktionen Richtlinien mit jeweils einer Regel, die einen Anforderungstyp angibt, für den die Antwort optimiert werden soll, und ordnen Sie die Aktionen den Richtlinien zu.

> **Hinweis:** Der Citrix ADC wertet Richtlinien zur Front-End-Optimierung nur zur Anforderungszeit aus, nicht zur Reaktionszeit.

Um die Richtlinien in Kraft zu setzen, binden Sie sie an Punkte. Sie können eine Richtlinie global binden, sodass sie für den gesamten Datenverkehr gilt, der über den Citrix ADC fließt, oder Sie können die Richtlinie an einen virtuellen Lastausgleichs- oder Content Switching-Server vom Typ HTTP oder SSL binden. Wenn Sie eine Richtlinie binden, weisen Sie ihr eine Priorität zu. Eine niedrigere Prioritätszahl gibt einen höheren Wert an. Citrix ADC wendet die Richtlinien in der Reihenfolge ihrer Prioritäten an.

Voraussetzungen

Für die Front-End-Optimierung muss die integrierte Citrix ADC Caching-Funktion aktiviert sein. Außerdem müssen Sie die folgenden integrierten Caching-Konfigurationen durchführen:

- Weisen Sie Cache-Speicher zu.
- Legen Sie die maximale Antwortgröße und das Speicherlimit für eine Standard-Cache-Content-Gruppe fest.

Weitere Informationen zum Konfigurieren des integrierten Cachings finden Sie unter Integriertes Caching.

Hinweis: Der Begriff Integrated Cache kann austauschbar mit AppCache verwendet werden. Beachten Sie, dass beide Begriffe aus funktionaler Sicht dasselbe bedeuten.

Konfigurieren der Front-End-Optimierung mithilfe der Citrix ADC Befehlszeilenschnittstelle

Führen Sie an der Eingabeaufforderung die folgenden Schritte aus:

1. Aktivieren Sie die Frontend-Optimierungsfunktion.

```
enable ns feature FEO
```

1. Erstellen Sie eine oder mehrere Front-End-Optimierungsaktionen.

```
add feo action <name> [-imgShrinkToAttrib] [-imgGifToPng] ...
```

Beispiel: Sofügen Sie eine Front-End-Optimierungsaktion für die Konvertierung von Bildern im GIF-Format in das PNG-Format und die Verlängerung des Ablaufzeitraums des Caches hinzu:

```
add feo action allact -imgGifToPng -pageExtendCache
```

1. [Optional] Geben Sie nicht standardmäßige Werte für globale Einstellungen der Front-End-Optimierung an.

```
set feo parameter [-cacheMaxage <integer>] [-JpegQualityPercent <integer>]
[-cssInlineThresSize <integer>] [-inlineJsThresSize <integer> [-inlineImgThresSize
 <integer>]
```

Beispiel: So geben Sie den maximalen Cache-Ablaufzeitraum an:

```
set feo parameter -cacheMaxage 10
```

1. Erstellen Sie eine oder mehrere Frontend-Optimierungsrichtlinien.

```
add feo policy <name> <rule> <action>
```

Beispiel: So fügen Sie eine Front-End-Optimierungsrichtlinie hinzu und verknüpfen sie der oben angegebenen allact-Aktion:

```
1 >add feo policy pol1 TRUE all act
2 >add feo policy pol1 ”(HTTP.REQ.URL.CONTAINS(”testsite”))” allact1
3 <!--NeedCopy-->
```

1. Binden Sie die Richtlinie an einen virtuellen Lastausgleichs- oder Content Switching-Server oder binden Sie sie global.

```
bind lb vserver <name> -policyName <string> -priority <num>
```

```
bind cs vserver <name> -policyName <string> -priority <num>
```

```
bind feo global <policyName> <priority> -type <type> <gotoPriorityExpression
>
```


Beispiel: So wenden Sie die Front-End-Optimierungsrichtlinie auf einen virtuellen Server namens abc an:

```
> bind lb vserver abc -policyName pol1 -priority 1 -type NONE
```

Beispiel: So wenden Sie die Front-End-Optimierungsrichtlinie für den gesamten Datenverkehr an, der den ADC erreicht:

```
> bind feo global pol1 100 -type REQ_DEFAULT
```

1. Speichern Sie die Konfiguration. save ns config

Konfigurieren der Front-End-Optimierung mit der GUI

1. Navigieren Sie zu **Optimierung** > **Front-End-Optimierung** > **Aktionen**, und klicken Sie auf **Hinzufügen** und erstellen Sie eine Front-End-Optimierungsaktion, indem Sie die relevanten Details angeben.
2. [Optional] Geben Sie die globalen Einstellungen für die Front-End-Optimierung an.
3. Navigieren Sie zu **Optimierung** > **Front-End-Optimierung**, und klicken Sie im rechten Fensterbereich unter Einstellungen auf **Front-End-Optimierungseinstellungen ändern**, und geben Sie die globalen Einstellungen für die Front-End-Optimierung an.
4. Erstellen Sie eine Front-End-Optimierungsrichtlinie.
5. Navigieren Sie zu **Optimierung** > **Front-End-Optimierung** > **Richtlinien**, klicken Sie auf **Hinzufügen**, und erstellen Sie eine Front-End-Optimierungsrichtlinie, indem Sie die relevanten Details angeben.
6. Binden Sie die Richtlinie an einen virtuellen Lastausgleichs- oder Content Switching-Server.
   a) Navigieren Sie zu **Optimierung** > **Front-End-Optimierung** > **Richtlinien**.
   b) Wählen Sie eine Front-End-Optimierungsrichtlinie aus, und klicken Sie auf **Richtlinien-Manager**.
   c) Binden Sie unter **Front End Optimization Policy Manager**die Front-End-Optimierungsrichtlinie an einen virtuellen Load Balancing- oder Content Switching-Server.

Überprüfen der Konfiguration der Front-End-Optimierung

Das Dashboard-Dienstprogramm zeigt zusammenfassende und detaillierte Statistiken in tabellarischen und grafischen Formaten an. Sie können die FEO-Statistiken einsehen, um Ihre FEO-Konfiguration auszuwerten.

Optional können Sie auch Statistiken für eine FEO-Richtlinie anzeigen, einschließlich der Anzahl der Auswahl, die der Richtlinienzähler während der richtlinienbasierten FEO erhöht.

> **Hinweis:**
> Weitere Informationen zu Statistiken und Diagrammen finden Sie in der Dashboard-Hilfe zur Cit-

> rix ADC Appliance.

Anzeigen von FEO-Statistiken mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Zusammenfassung der FEO-Statistiken, FEO-Richtlinienauswahl und -details sowie detaillierte FEO-Statistiken anzuzeigen:

- `stat feo` Hinweis: Der Befehl stat feo policy zeigt Statistiken nur für erweiterte FEO-Richtlinien an.
- `show feo policy name`
- `stat feo -detail`

Anzeigen von FEO-Statistiken auf Citrix ADC Dashboard

In der Dashboard-GUI können Sie:

- Wählen Sie Front-End-Optimierung aus, um eine Zusammenfassung der `FEO` Statistiken anzuzeigen.
- Klicken Sie auf die Registerkarte **Grafische Ansicht**, um die Rate der von der FEO-Funktion verarbeiteten Anforderungen anzuzeigen.

Proben-Optimierung:

In der Beispiel-PDF-Datei finden Sie einige Beispiele für Aktionen zur Inhaltsoptimierung, die auf HTML-Inhalte und die eingebetteten Objekte im HTML-Inhalt angewendet werden.

Inhaltsbeschleuniger

October 5, 2021

> **Wichtig:**
>
> Die Inhaltsbeschleuniger-Funktion wird von der Citrix ADC Appliance nicht mehr unterstützt.

Inhaltsbeschleuniger ist eine Citrix ADC Funktion, die Sie in einer Citrix ByteMobile T1100 Bereitstellung verwenden können, um Daten auf einer Citrix ByteMobile T2100-Appliance zu speichern.

Das Speichern von Daten auf einer T2100-Appliance spart Bandbreite und bietet schnellere Reaktionszeiten, da Citrix ADC keine Verbindung zum Server für wiederholte Anforderungen derselben Daten herstellen muss.

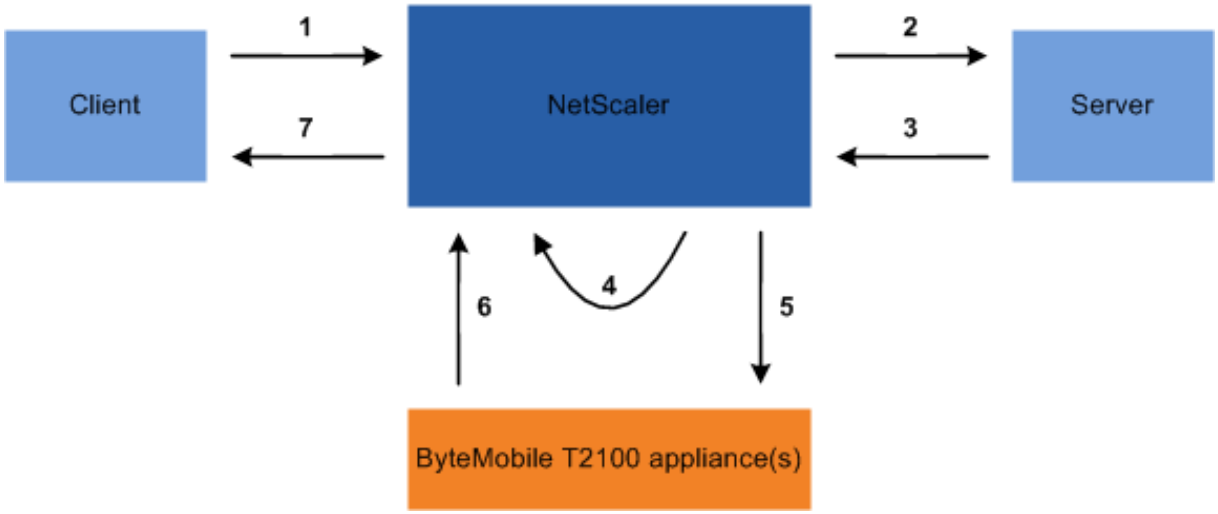
> **Hinweis:** Content Accelerator arbeitet mit einer Citrix ByteMobile Premium-Lizenz. Wenden Sie sich an den Kundendienst, um weitere Informationen zu erhalten und die Lizenz zu erhalten.

So funktioniert der Content Accelerator

Wenn ein virtuellen Lastausgleichs- oder Content Switching-Server eine Clientanforderung empfängt, wertet die Citrix ADC Appliance eine Inhaltsbeschleunigerrichtlinie aus, die Sie an den virtuellen Server gebunden haben. Die Richtlinie filtert die Anforderungen, um die Anforderungen zu identifizieren, auf die das Feature Inhaltsbeschleuniger angewendet werden soll.

> **Hinweis:**
>
> Bei HTTP-Anfragen kann die Content Accelerator-Funktion teilweise Inhalte als Reaktion auf Anfragen mit einem Bytebereich bereitstellen.

Die folgende Abbildung veranschaulicht die Vorgänge, die die Appliance ausführt, wenn eine Clientanforderung bei einem virtuellen Server eintrifft, der für die Verwendung der Inhaltsbeschleuniger-Funktion konfiguriert ist:



Der Prozessablauf ist wie folgt:

1. Der Client sendet eine Anfrage.
2. Citrix ADC leitet die Anforderung an den Server weiter.
3. Server antwortet mit der vordefinierten Größe der Antwort (angegeben durch den Parameter AccumresSize des Befehls add ca action).
4. Citrix ADC berechnet einen Hash der vom Server gesendeten Antwort.
5. Citrix ADC sucht den Hash auf der T2100-Appliance.
6. Eine erfolgreiche Suche zeigt an, dass die Daten verfügbar sind und die T2100-Appliance die Daten an den Citrix ADC sendet.

   > **Hinweis:**
   > Wenn die Datenbanksuche nicht erfolgreich ist, ruft die Appliance die angeforderten

> Daten vom Server ab, liefert die Daten an den Client und aktualisiert die Daten auf der T2100-Appliance.
> Die T2100-Appliance kann so konfiguriert werden, dass die Anzahl der Anforderungen angegeben wird, für die Daten zwischengespeichert werden sollen.

7. Citrix ADC sendet die Antwort an den Client.

Content-Beschleuniger konfigurieren

Bevor Sie das Content Accelerator-Feature konfigurieren, müssen Sie es auf der Citrix ADC Appliance aktivieren.

Sie müssen die Content Accelerator-Funktion konfigurieren, um eine oder mehrere T2100-Appliances verwenden zu können. Sie müssen jede T2100-Appliance als Dienst hinzufügen und diese Dienste an einen virtuellen Lastausgleichsserver binden, der für die Verteilung der Last auf die konfigurierten T2100-Appliances vorgesehen ist.

Sie müssen eine Content Accelerator-Aktion konfigurieren, um die Daten auf der T2100-Appliance nachschlagen zu können. Die Aktion muss den virtuellen Lastausgleichsserver T2100 und die Größe der Daten (in KB) angeben, die zum Berechnen des Hash vom Server abgerufen werden sollen.

Die Aktion muss an eine Inhaltsbeschleunigerrichtlinie gebunden sein, die den Datenverkehr definiert, für den die Inhaltsbeschleunigung ausgeführt werden soll. Die Inhaltsbeschleuniger-richtlinie muss an einen virtuellen Content Switching- oder Lastausgleichsserver gebunden sein, der Clientdatenverkehr empfängt. Alternativ können Sie die Richtlinie global an alle anwendbaren virtuellen Server binden.

So konfigurieren Sie den Content Accelerator mit der Befehlszeilenschnittstelle

Führen Sie an der Eingabeaufforderung die folgenden Schritte aus:

1. Aktivieren Sie die Inhaltsbeschleuniger-Funktion.

   ```
   enable ns feature ca
   ```

2. Identifizieren Sie die T2100-Appliances, und fügen Sie sie als Dienst auf der Citrix ADC Appliance hinzu.

   ```
   add service <name> <IPAddress> <serviceType> <port>
   ```

   Beispiel:

```
1 > add service T2100-A 10.102.29.61 HTTP 30
2 > add service T2100-B 10.102.29.62 HTTP 40
3 > add service T2100-C 10.102.29.63 HTTP 50
4 <!--NeedCopy-->
```


> **Hinweis:**
> Die Dienste dürfen nur vom Typ HTTP sein.

3. Erstellen Sie einen virtuellen Lastausgleichsserver für die T2100-Appliances. Geben Sie die Token Load Balancing-Methode und die Regel in der folgenden Syntax an.

```
1 add lb vserver <name> <serviceType> <IPAddress> <port> -lbMethod
     TOKEN -rule "http.req.url.after_str("/lookup/") alt http.req.
     url.path.SKIP(1).PREFIX(64)"
2 <!--NeedCopy-->
```

Beispiel:

```
1 add lb vserver T2100-lbvserver HTTP 10.102.29.64 99 -lbMethod
     TOKEN -rule "http.req.url.after_str("/lookup/") alt http.req.
     url.path.SKIP(1).PREFIX(64)"
2 <!--NeedCopy-->
```

4. Binden Sie die T2100-Dienste an den virtuellen Lastausgleichsserver, den Sie für sie erstellt haben.

```
bind lb vserver <name> <serviceName>
```

Beispiel:

```
1 > bind lb vserver T2100-lbvserver T2100-A
2 > bind lb vserver T2100-lbvserver T2100-B
3 > bind lb vserver T2100-lbvserver T2100-C
4 <!--NeedCopy-->
```

5. Definieren Sie eine Inhaltsbeschleunigeraktion.

```
add ca action <name> accumResSize <KBytes> -lbvserver <string> -type
lookup
```

Beispiel:

```
> add ca action ca_action1 -type lookup -lbvserver T2100-lbvserver -
accumResSize 60
```

6. Definieren Sie eine Inhaltsbeschleunigerrichtlinie.

```
add ca policy <name> -rule <expression> -action <name>
```


Beispiel:

Erstellen einer Richtlinie für den Inhaltsbeschleuniger, die alle Videoformate zwischenspeichert.

```
> add ca policy ca_mp4_pol -rule ns_video -action ca_action1
```

wobei ns_video ein integrierter Ausdruck ist.

7. Binden Sie die Inhaltsbeschleunigerrichtlinie entweder an einen virtuellen Server, der Datenverkehr empfängt, oder global an das Citrix ADC -System.

```
bind lb vserver <name> -policyName <string>
```

```
bind cs vserver <name> -policyName <string>
```

```
bind ca global -policyName <string> -priority <num> -type <type>
```

Beispiel: So wenden Sie die Inhaltsbeschleunigerrichtlinie auf einen virtuellen Server mit dem Namen traf_rec an

```
bind lb vserver traf_rec -policyName ca_mp4_pol
```

Beispiel: So wenden Sie die Inhaltsbeschleunigerrichtlinie für den gesamten Datenverkehr an, der den Citrix ADC erreicht.

```
bind ca global -policyName ca_mp4_pol -priority 100 -type RES_DEFAULT
```

8. Speichern Sie die Konfiguration.

```
save ns config
```

Konfigurieren des Inhaltsbeschleunigers mit der GUI

1. Navigieren Sie zu **System** > **Einstellungen** > **Erweiterte Funktionen konfigurieren**, und wählen Sie **Inhaltsbeschleuniger** aus.
2. Erstellen Sie einen Service für jede der T2100-Appliances.
   a) Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienste**.
   b) Klicken Sie auf **Hinzufügen**, und geben Sie die relevanten Details an. Stellen Sie im Feld **Server** sicher, dass Sie die IP-Adresse der T2100-Appliance angeben. Wählen Sie im Feld **Protokoll** die Option HTTP aus.
3. Erstellen Sie einen virtuellen Server und binden Sie die T2100-Dienste daran.
   a) Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
   b) Klicken Sie auf **Hinzufügen**, und geben Sie die relevanten Details an.
   c) Geben Sie auf der Registerkarte **Methode und Persistenz** die Methode als **Token** an.
   d) Geben Sie auf der Registerkarte **Richtlinien** die Regel als http.req.url.after_str("/lookup/") alt http.req.url.path.SKIP(1).PREFIX(64) an.
   e) Wählen Sie auf der Registerkarte **Dienste** die T2100-Dienste aus, die Sie an den virtuellen Server binden möchten.

4. Erstellen Sie eine Inhaltsbeschleunigeraktion.
   a) Navigieren Sie zu **Optimierung** > **Inhaltsbeschleuniger** > **Aktionen** .
   b) Geben Sie die relevanten Details an.
5. Erstellen Sie eine Inhaltsbeschleunigerrichtlinie.
   a) Navigieren Sie zu **Optimierung** > **Inhaltsbeschleuniger** > **Richtlinien** .
   b) Klicken Sie auf **Hinzufügen**, geben Sie die Richtlinienregel an, und ordnen Sie die Inhaltsbeschleunigeraktion zu.
6. Binden Sie die Inhaltsbeschleunigerrichtlinie global oder an einen virtuellen Server.
   a) Navigieren Sie zu **Optimierung** > **Inhaltsbeschleuniger** .
   b) Binden Sie die **Content Accelerator Policy [Manager-REQUEST]**[- oder Content Accelerator-Policy-Manager RESPONSE] die Content Accelerator-Richtlinie global oder an einen virtuellen Server.

Medienklassifizierung

October 5, 2021

Das Verständnis der Art des Datenverkehrs im Netzwerk hilft Netzwerkadministratoren, den Bandbreitenverbrauch für eine optimale Netzwerkleistung zu verwalten. Der Medienklassifizierungsmodus überwacht und zeigt die Statistiken des Medienverkehrs über die Citrix ADC Appliance an.

Wenn dieser Modus aktiviert ist, kann ein Netzwerkadministrator Statistiken sammeln, die die Menge der Daten, auf die zugegriffen wird, und die Arten von Geräten, von denen aus auf die Mediendateien zugegriffen wurde, abrufen. Die Citrix ADC Appliance unterstützt auch Bytebereichsanforderungen in diesem Modus.

Derzeit kann die Citrix ADC Appliance Statistiken für die folgenden Mediendateitypen überwachen und anzeigen:

Medien	Dateityp
Microsoft reibungsloses Streaming	Video
Apple-Livestreaming	Video
Audiodatentransport-Stream (ADTS)	Audio
Erweiterte Audiocodierung (AAC)	Audio
Flash-Video (FLV)	Audio und Video
3GP	Audio und Video

Die Appliance kann Statistiken für folgende Geräte anzeigen:

Geräteplattform	Gerätetyp
iOS	iPad und iPod
Android	Handys und Tablets
Laptop oder Desktop	Windows Laptop- und Desktop-Computer
Andere Probleme	Andere mobile Geräte (Handys und Tablets)

Die Netzwerkadministratoren können die folgenden Statistikindikatoren überprüfen, um die Datenmenge zu erfahren, auf die über die Citrix ADC Appliance für verschiedene Medienverkehrstypen zugegriffen wird.

Name der Mediendatei	Statistikzähler
Microsoft reibungsloses Streaming	`mcmssmthstrmvid`—Dieser Leistungsindikator zeichnet die Gesamtzahl der Microsoft Smooth Streaming-Videos auf, die von der Citrix ADC Appliance bereitgestellt werden.`Mcmssmthstrvidpl`—Dieser Leistungsindikator zeichnet die Gesamtzahl der Microsoft Smooth Streaming-Videowiedergabelisten auf, die von der Citrix ADC Appliance bereitgestellt werden;`Mcmssmthstrmvidbytes`—Dieser Zähler zeichnet die Gesamtzahl der Datenbytes, die für den Medienverkehr von Microsoft Smooth Streaming auf der Citrix ADC Appliance bereitgestellt werden;`Mcmssmthstrmplvidbytespl`—Dieser Leistungsindikator zeichnet die Gesamtzahl der Microsoft Smooth Streaming-Bytes auf, die von der Citrix ADC Appliance bereitgestellt werden.

Name der Mediendatei	Statistikzähler
Apple-Livestreaming	mccaplelivestrmngvid— Dieser Leistungsindikator zeichnet die Gesamtzahl der von der Citrix ADC Appliance bereitgestellten Apple Live Streaming-Videos auf.Mccapplelivestrmngvidpl—Dieser Leistungsindikator zeichnet die Gesamtzahl der von der Citrix ADC Appliance bereitgestellten Apple Live Streaming-Videowiedergabelisten auf.Mcapplelivestreamingvidbytes— Dieser Leistungsindikator zeichnet die Gesamtzahl der Datenbytes auf, die für den Medienverkehr von Apple Live Streaming auf der Citrix ADC Appliance bereitgestellt werden.Mcapplelivestreamingplaylistvidbytespl — Dieser Leistungsindikator zeichnet die Gesamtzahl der Apple Live Playlist-Bytes auf, die von der Citrix ADC Appliance bereitgestellt werden.
Audiodatentransport-Stream (ADTS)	mcadtsaudio— Dieser Leistungsindikator zeichnet die Gesamtzahl der ADTS-Audioclips auf, die von der Citrix ADC Appliance bereitgestellt werden.Mcadtsaudiobytes— Dieser Leistungsindikator zeichnet die Gesamtzahl der Datenbytes auf, die für den ADTS-Medienverkehr auf der Citrix ADC Appliance bereitgestellt werden.
Erweiterte Audiocodierung (AAC)	Mcaacaudio— Dieser Leistungsindikator zeichnet die Gesamtzahl der AAC-Audioclips auf, die von der Citrix ADC Appliance bereitgestellt werden.Mcaacaudiobytes— Dieser Leistungsindikator zeichnet die Gesamtzahl der Datenbytes auf, die für den AAC-Medienverkehr auf der Citrix ADC Appliance bereitgestellt werden.

Name der Mediendatei	Statistikzähler
Flash-Video (FLV)	`Mcflvvid`— Dieser Leistungsindikator zeichnet die Gesamtzahl der von der Citrix ADC Appliance bereitgestellten Flash-Videos auf.`Mcflvvidbytes`— Dieser Leistungsindikator zeichnet die Gesamtzahl der Datenbytes auf, die für Flash-Videos auf der Citrix ADC Appliance bereitgestellt werden.
3GP	`mc3gpvidbytes`— Dieser Leistungsindikator zeichnet die Gesamtzahl der Datenbytes auf, die für den 3GP-Medienverkehr auf der Citrix ADC Appliance bereitgestellt werden.

Die Citrix ADC Appliance erkennt Mediendateitypen anhand ihrer Signaturen in *den Anfangsbytes* der Antworten. Zum Beispiel haben die anfänglichen Body-Bytes für eine mp4-Datei die folgende Signatur in der Antwort:

```
**....ftypmp42** ....isommp42....moov...lmvhd.....c.\!.c.\!..
```

Die Citrix ADC Appliance erkennt den Clientgerätetyp anhand der *Benutzer-Agent-Zeichenfolge*, die das Clientgerät in die HTTP-GET-Anforderung enthält. Beispielsweise hat ein Fenstertelefon, das einen UC-Browser verwendet, die folgende Benutzeragentenzeichenfolge in der HTTP-GET-Anfrage:

```
User-Agent: **UCWEB**/2.0 (**Windows**; U; wds 8.10; en-US; HTC; 8X by HTC)
U2/1.0.0
```

Medienklassifizierung aktivieren

Standardmäßig ist die Medienklassifizierung auf der Citrix ADC Appliance deaktiviert. Sie müssen den Modus aktivieren, bevor Sie ihn verwenden.

So aktivieren Sie die Medienklassifizierung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns mode Mediaclassification
```

So aktivieren Sie die Medienklassifizierung mit der GUI

Medienklassifizierung auf der Citrix ADC Appliance aktivieren

Navigieren Sie zu **System** > **Einstellungen** > **Modi konfigurieren**, und wählen Sie **Medienklassifizierung** aus.

So zeigen Sie Statistiken zum Medienverkehr auf der Citrix ADC Appliance an

Navigieren Sie zu **Optimierung**, und klicken Sie auf **Medienklassifizierung**, um die Statistiken des Medienverkehrs anzuzeigen.

Statistiken zur Medienklassifizierung überprüfen

Sie können die Statistiken des Medienverkehrs im Dashboard-Dienstprogramm oder über die Befehlszeilenschnittstelle anzeigen. Das Dashboard-Dienstprogramm zeigt zusammenfassende und detaillierte Statistiken in einem tabellarischen und grafischen Format an.

> **Hinweis**
> Weitere Informationen zu Statistiken und Diagrammen finden Sie in der Dashboard-Hilfe zu Ihrer Citrix ADC Appliance.

So zeigen Sie Medienklassifizierungsstatistiken mit der Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um eine Zusammenfassung der Medienklassifizierungsstatistiken anzuzeigen, detaillierte Statistiken anzuzeigen oder die Anzeige zu deaktivieren:

```
stat Mediaclassification
```

```
stat Mediaclassification -detail
```

```
stat Mediaclassification -clearstats
```

So zeigen Sie Statistiken zur Medienklassifizierung auf dem Dashboard an

Im **Dashboard-Dienstprogramm** können Sie die folgenden Arten von Medienklassifizierungsstatistiken anzeigen:

1. Wählen Sie **Medienklassifizierung** aus, um eine Zusammenfassung der Statistiken des Medienverkehrs anzuzeigen.
2. Um detaillierte Statistiken zum Medienverkehr anzuzeigen, klicken Sie auf **Details**.
3. Klicken Sie auf Löschen, um die Statistiken des Medienverkehrs zu **löschen**.

Bewertung

October 5, 2021

Citrix bietet Reputationsbasierte Sicherheit. Mithilfe der Reputationsbewertung können Sie das Risiko der Verarbeitung von Anforderungen ermitteln, wie z. B. das Blockieren oder Löschen bestimmter Anforderungen, um die Leistung Ihrer Anwendung zu verbessern.

Die Citrix ADC IP-Reputationsfunktion verwendet IP-Reputationsprüfungen, um Zero-Day-Angriffe zu verhindern und vor bösartigen Quellen zu schützen, die mit Webangriffen, Phishing-Aktivitäten oder Web-Scans verbunden sind.

Weitere Informationen finden Sie unter IP-Reputation.

IP-Reputation

December 3, 2021

IP-Reputation ist ein Tool, das IP-Adressen identifiziert, die unerwünschte Anfragen senden. Mithilfe der IP-Reputationsliste können Sie Anfragen ablehnen, die von einer IP-Adresse mit schlechtem Ruf stammen. Optimieren Sie die Leistung der Web Application Firewall, indem Sie Anfragen filtern, die Sie nicht verarbeiten möchten. Setzen Sie eine Anfrage zurück, löschen Sie sie oder konfigurieren Sie sogar eine Responder Policy, um eine bestimmte Responder Action auszuführen.

Im Folgenden sind einige Angriffe aufgeführt, die Sie mithilfe von IP Reputation verhindern können:

- **Virus Infizierte PCs**. (Heim-PCs) sind die größte Spam-Quelle im Internet. IP Reputation kann die IP-Adresse identifizieren, die unerwünschte Anfragen sendet. Die IP-Reputation kann besonders nützlich sein, um große DDoS-, DoS- oder anomale SYN-Flood-Angriffe von bekannten infizierten Quellen zu blockieren.
- **Zentrales verwaltetes und automatisiertes Botnet**. Angreifer haben aufgrund des Diebstahls von Kennwörtern an Popularität gewonnen, da es nicht lange dauert, bis Hunderte von Computern zusammenarbeiten, um Ihr Kennwort zu knacken. Es ist einfach, Botnet-Angriffe zu starten, um Kennwörter herauszufinden, die häufig verwendete Wörterbuchwörter verwenden.
- **Kompromittierter Webserver**. Angriffe sind nicht so häufig, da das Bewusstsein und die Serversicherheit zugenommen haben, sodass Hacker und Spammer nach einfacheren Zielen suchen. Es gibt immer noch Webserver und Online-Formulare, die Hacker kompromittieren und zum Versenden von Spam verwenden können (wie Viren und Pornos). Solche Aktivitäten sind einfacher zu erkennen und schnell herunterzufahren oder mit einer Reputationsliste wie SpamRats zu blockieren.
- **Windows Exploits**. (wie Active IPs, die Malware, Shell-Code, Rootkits, Würmer oder Viren anbieten oder verbreiten).
- **Bekannte Spammer und Hacker**.
- **Massen-E-Mail-Marketingkampagnen**.
- **Phishing-Proxys** (IP-Adressen, die Phishing-Websites hosten, und andere Betrugsfälle wie Werbeklickbetrug oder Spielbetrug).
- **Anonyme Proxys** (IPs, die Proxy- und Anonymisierungsdienste bereitstellen, einschließlich The Onion Router alias TOR).

Eine Citrix ADC-Appliance verwendet **Webroot** als Dienstanbieter für eine dynamisch generierte bösartige IP-Datenbank und die Metadaten für diese IP-Adressen. Metadaten können Geolokationsdetails, Bedrohungskategorie, Bedrohungszahl usw. enthalten. Die Webroot Threat Intelligence-Engine erhält Echtzeitdaten von Millionen von Sensoren. Es erfasst, scannt, analysiert und bewertet die Daten automatisch und kontinuierlich mithilfe von fortschrittlichem maschinellem Lernen und Verhaltensanalysen. Die Informationen über eine Bedrohung werden ständig aktualisiert.

Die Citrix ADC Appliance validiert eine eingehende Anfrage auf ihren schlechten Ruf mithilfe der Webroot verwendet die IP-Reputationsdatenbank. Die Datenbank verfügt über eine riesige Sammlung von IP-Adressen klassifizierten IP-Bedrohungskategorien. Im Folgenden sind die Kategorien von IP-Bedrohungen und deren Beschreibung aufgeführt.

- Spam-Quellen. Spam-Quellen umfassen das Tunneln von Spam-Nachrichten über Proxy, anomale SMTP-Aktivitäten und Forum-Spam-Aktivitäten.
- Windows Exploits. Die Windows-Exploit-Kategorie umfasst aktive IP-Adressen, die Malware, Shellcode, Rootkits, Würmer oder Viren anbieten oder verteilen
- Internet-Angriffe. Die Kategorie der Webangriffe umfasst Cross-Site-Scripting, iFrame-Injection, SQL-Injection, domänenübergreifende Injection oder
- Botnetze. Botnet-Kategorie umfasst Botnet-C&C-Kanäle und infizierte Zombie-Maschinen, die vom Bot-Master gesteuert werden
- Scanner. Die Kategorie Scanner umfasst alle Aufklärungen wie Sonden, Host-Scan, Domain-Scan und Kennwort-Brute-Force-Angriff
- Diensteverweigerung. Die Kategorie "Denial of Services" umfasst DOS, DDOS, anomale Synchronisationsflut und Erkennung von anomalem Datenverkehr
- Ruf. Den Zugriff von IP-Adressen verweigern, von denen derzeit bekannt ist, dass sie mit Malware infiziert sind. Diese Kategorie umfasst auch IPs mit einem durchschnittlich niedrigen Webroot Reputation Index. Durch die Aktivierung dieser Kategorie wird der Zugriff von identifizierten Quellen verhindert, um Malware-Verteilungspunkte zu kontaktieren
- Phishing. Die Phishing-Kategorie umfasst IP-Adressen, die Phishing-Seiten hosten, andere Betrugsaktivitäten wie Ad-Click-Betrug oder Spielbetrug.
- Proxy. Die Proxykategorie umfasst IP-Adressen, die Proxy- und Def-Dienste bereitstellen.
- Mobile Bedrohungen. Die Kategorie Mobile Threat umfasst IP-Adressen bösartiger und unerwünschter mobiler Anwendungen. Diese Kategorie nutzt Daten des Webroot Forschungsteams für mobile Bedrohungen.
- Tor-Proxy. Die Tor-Proxykategorie umfasst IP-Adressen, die als Ausgangsknoten für das Tor-Netzwerk fungieren. Ausgangsknoten sind der letzte Punkt entlang der Proxykette und stellen eine direkte Verbindung zum beabsichtigten Ziel des Urhebers her.

Wenn irgendwo im Netzwerk eine Bedrohung erkannt wird, wird die IP-Adresse als bösartig gekennzeichnet und alle mit dem Netzwerk verbundenen Geräte sind sofort geschützt. Die dynamischen Änderungen der IP-Adressen werden mithilfe von fortschrittlichem maschinellem Lernen mit hoher Geschwindigkeit und Genauigkeit verarbeitet.

Wie im Datenblatt von Webroot angegeben, identifiziert das Sensornetzwerk des Webroot viele wichtige IP-Bedrohungsarten, darunter Spam-Quellen, Windows-Exploits, Botnetze, Scanner und andere. (Siehe das Flussdiagramm auf dem Datenblatt.)

Die Citrix ADC-Appliance verwendet einen `iprep` Clientprozess, um die Datenbank von Webroot abzurufen. Der `iprep` Client verwendet die Methode HTTP GET, um zum ersten Mal die absolute IP-Liste von Webroot abzurufen. Später werden alle 5 Minuten Delta-Änderungen überprüft.

> **Wichtig:**
>
> - Stellen Sie sicher, dass die Citrix ADC Appliance über Internetzugang verfügt und DNS konfiguriert ist, bevor Sie die IP-Reputationsfunktion verwenden.
> - Um auf die Webroot Datenbank zuzugreifen, muss die Citrix ADC-Appliance in der Lage sein, eine Verbindung zu **api.bcti.brightcloud.com** auf **Port 443**herzustellen. Jeder Knoten in der HA- oder Clusterbereitstellung erhält die Datenbank von Webroot und muss auf diesen vollqualifizierten Domänennamen (FQDN) zugreifen können.
> - Webroot hostet derzeit seine Reputationsdatenbank in AWS. Daher muss Citrix ADC in der Lage sein, AWS-Domänen für das Herunterladen der Reputationsdatenbank aufzulösen. Außerdem muss die Firewall für AWS-Domains offen sein.
>
> **Hinweis:**
>
> Jede Paket-Engine benötigt mindestens 4 GB, um ordnungsgemäß zu funktionieren, wenn die IP-Reputationsfunktion aktiviert ist.

Erweiterte Richtlinienausdrücke. Konfigurieren Sie die Funktion “IP-Reputation” mithilfe erweiterter Richtlinienausdrücke (Standardsyntaxausdrücke) in den Richtlinien, die an unterstützte Module wie Web Application Firewall und Responder gebunden sind. Im Folgenden finden Sie zwei Beispiele, die Ausdrücke zeigen, mit denen festgestellt werden kann, ob die Client-IP-Adresse bösartig ist.

1. **CLIENT.IP.SRC.IPREP_IS_MALICIOUS**: Dieser Ausdruck wird als TRUE ausgewertet, wenn der Client in die Liste der böswilligen IP-Adressen aufgenommen wurde.
2. **CLIENT.IP.SRC.IPREP_THREAT_CATEGORY (CATEGORY)**: Dieser Ausdruck wird als TRUE ausgewertet, wenn die Client-IP böswillige IP ist und zur angegebenen Bedrohungskategorie gehört.

Im Folgenden sind die möglichen Werte für die Bedrohungskategorie:

SPAM_SOURCES, WINDOWS_EXPLOITS, WEB_ATTACKS, BOTNETS, SCANNERS, DOS, REPUTATION, PHISHING, PROXY, NETWORK, CLOUD_PROVIDERS, MOBILE_THREATS, TOR_PROXY.

> **Hinweis:**
>
> Die IP-Reputationsfunktion prüft sowohl Quell- als auch Ziel-IP-Adressen. Es erkennt böswillige IPs im Header. Wenn der PI-Ausdruck in einer Richtlinie die IP-Adresse identifizieren kann, bes-

> timmt die IP-Reputationsprüfung, ob sie bösartig ist.

iPrep Protokollnachricht. Die `/var/log/iprep.log` Datei enthält nützliche Nachrichten, die Informationen über die Kommunikation mit der Webroot-Datenbank erfassen. Die Informationen können sich auf die während der Webrootkommunikation verwendeten Anmeldeinformationen beziehen, die fehlende Verbindung mit Webroot, Informationen, die in einem Update enthalten sind (z. B. die Anzahl der IP-Adressen in der Datenbank).

Erstellen einer Sperrliste oder einer Allowlist von IPs unter Verwendung eines Richtliniendatensatzes. Sie können eine Positivliste verwalten, um den Zugriff auf bestimmte IP-Adressen zu ermöglichen, die in der Webroot-Datenbank blockiert sind. Sie können auch eine angepasste Sperrliste von IP-Adressen erstellen, um die Reputationsprüfung von Webroot zu ergänzen. Diese Listen können mithilfe eines **Richtliniendatensatzes**erstellt werden. Ein Datensatz ist eine spezielle Form von Mustersatz, die sich ideal für den IPv4-Adressabgleich eignet. Um Datensätze zu verwenden, erstellen Sie zuerst den Datensatz und binden IPv4-Adressen an ihn. Verwenden Sie beim Konfigurieren einer Richtlinie zum Vergleichen einer Zeichenfolge in einem Paket einen entsprechenden Operator und übergeben Sie den Namen des Mustersatzes oder Datensatzes als Argument.

So erstellen Sie eine Positivliste von Adressen, die während der IP-Reputationsbewertung als Ausnahmen behandelt werden sollen:

- Konfigurieren Sie die Richtlinie so, dass der PI-Ausdruck auf False ausgewertet wird, selbst wenn eine Adresse in der Positivliste von Webroot (oder einem Dienstanbieter) als bösartig aufgeführt wird.

IP-Reputation aktivieren oder deaktivieren. Die IP-Reputation ist Teil der allgemeinen Reputationsfunktion, die lizenzbasiert ist. Wenn Sie die Reputationsfunktion aktivieren oder deaktivieren, wird die IP-Reputation aktiviert oder deaktiviert.

Allgemeines Verfahren. Die Bereitstellung von IP-Reputation umfasst die folgenden Aufgaben:

- Stellen Sie sicher, dass die auf der Citrix ADC-Appliance installierte Lizenz IP-Reputationsunterstützung bietet. Premium- und Standalone-Anwendungsfirewall-Lizenzen unterstützen die IP-Reputationsfunktion.
- Aktivieren Sie die Funktionen für IP-Reputation und Anwendungsfirewall.
- Fügen Sie ein Anwendungs-Firewall-Profil hinzu.
- Fügen Sie mithilfe der PI-Ausdrücke eine Anwendungsfirewall-Richtlinie hinzu, um die böswilligen IP-Adressen in der IP-Reputation-Datenbank zu identifizieren.
- Binden Sie die Anwendungsfirewall-Richtlinie an einen entsprechenden Bindepunkt.
- Stellen Sie sicher, dass jede Anfrage von einer böswilligen Adresse in der `ns.log` Datei protokolliert wird, um anzuzeigen, dass die Anforderung wie im Profil angegeben verarbeitet wurde.

Konfigurieren Sie die IP-Reputationsfunktion über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `enable feature reputation`
- `disable feature reputation`

Die folgenden Beispiele zeigen, wie Sie mithilfe des PI-Ausdrucks eine Anwendungsfirewall-Richtlinie hinzufügen können, um schädliche Adressen zu identifizieren. Sie können die integrierten Profile verwenden, ein Profil hinzufügen oder ein vorhandenes Profil konfigurieren, um die gewünschte Aktion aufzurufen, wenn eine Anforderung mit einer Richtlinienübereinstimmung übereinstimmt.

Beispiele 3 und 4 zeigen, wie ein Richtlinien-Dataset erstellt wird, um eine Sperrliste oder eine Positivliste von IP-Adressen zu generieren.

Beispiel 1:

Der folgende Befehl erstellt eine Richtlinie, die böswillige IP-Adressen identifiziert und die Anforderung blockiert, wenn eine Übereinstimmung ausgelöst wird:

```
add appfw policy pol1 CLIENT.IP.SRC.IPREP_IS_MALICIOUS APPFW_BLOCK
```

Beispiel 2:

Der folgende Befehl erstellt eine Richtlinie, die den Reputationsdienst verwendet, um die Client-IP-Adresse im `X-Forwarded-For` Header zu überprüfen und die Verbindung zurückzusetzen, wenn eine Übereinstimmung ausgelöst wird.

```
> add appfw policy pol1 ”HTTP.REQ.HEADER(\”X-Forwarded-For\”).TYPECAST_IP_ADDRESS_AT
.IPREP_IS_MALICIOUS”APPFW_RESET**
```

Beispiel 3:

Das folgende Beispiel zeigt, wie eine Liste hinzugefügt wird, um Ausnahmen hinzuzufügen, die bestimmte IP-Adressen zulassen:

```
> add policy dataset Allow_list1 ipv4
> bind policy dataset Allow_list1 10.217.25.17 -index 1
> bind policy dataset Allow_list1 10.217.25.18 -index 2
```

Beispiel 4:

Das folgende Beispiel zeigt, wie die angepasste Liste hinzugefügt wird, um bestimmte IP-Adressen als bösartig zu kennzeichnen:

```
> add policy dataset Block_list1 ipv4
> bind policy dataset Block_list1 10.217.31.48 -index 1
> bind policy dataset Block_list1 10.217.25.19 -index 2
```


Beispiel 5:

Das folgende Beispiel zeigt einen Richtlinienausdruck, um die Client-IP unter den folgenden Bedingungen zu blockieren:

- Es stimmt mit einer in der benutzerdefinierten Block_List1 konfigurierten IP-Adresse überein (Beispiel 4)
- Sie stimmt mit einer in der Webroot-Datenbank aufgelisteten IP-Adresse überein, es sei denn, sie wird durch die Aufnahme in die allow_List1 gelockert (Beispiel 3).

```
1 > add appfw policy ”Ip_Rep_Policy” ”((CLIENT.IP.SRC.IPREP_IS_MALICIOUS
     || CLIENT.IP.SRC.TYPECAST_TEXT_T.CONTAINS_ANY(”Block_list1”)) && ! (
     CLIENT.IP.SRC.TYPECAST_TEXT_T.CONTAINS_ANY(”Allow_list1”)))”
     APPFW_BLOCK
2 <!--NeedCopy-->
```

Verwenden des Proxyservers:

Wenn die Citrix ADC-Appliance keinen direkten Zugriff auf das Internet hat und mit einem Proxy verbunden ist, konfigurieren Sie den IP-Reputation-Client so, dass er Anfragen an den Proxy sendet.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set reputation settings -proxyServer <proxy server ip> -proxyPort <proxy
server port>
```

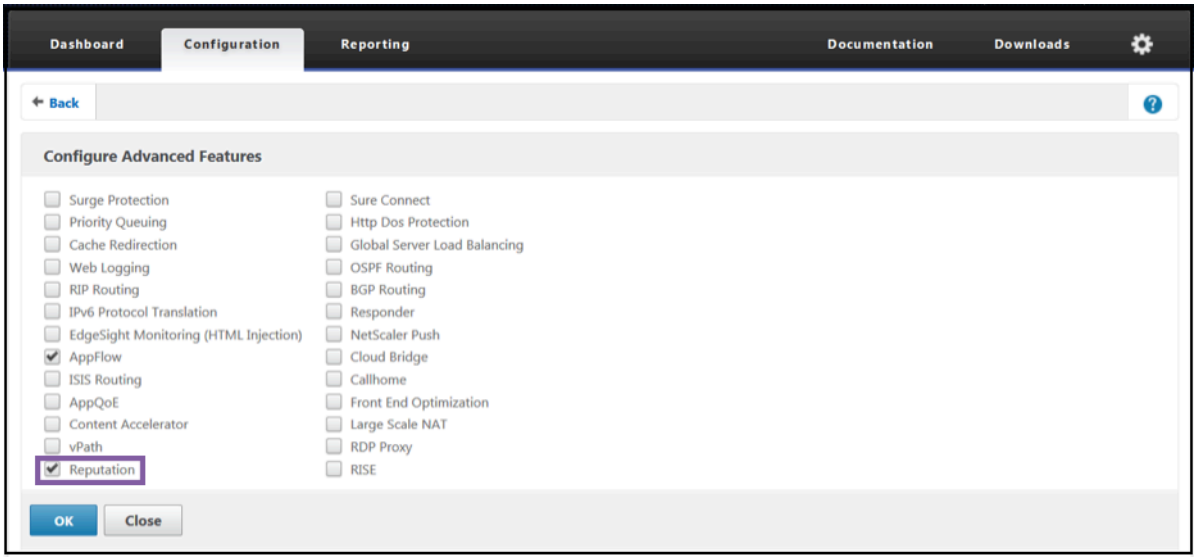
Beispiel:

```
> set reputation settings proxyServer 10.102.30.112 proxyPort 3128
> set reputation settings -proxyServer testproxy.citrite.net -proxyPort 3128
> unset reputation settings -proxyserver -proxyport
> sh reputation settings
```

> **Hinweis:**
>
> Die Proxy-Server-IP kann eine IP-Adresse oder ein vollqualifizierter Domänenname (FQDN) sein.

Konfigurieren Sie die IP-Reputation über die Citrix ADC GUI

1. Navigieren Sie zu **System > Einstellungen**. Klicken Sie im Abschnitt **Modi und Funktionen** auf den Link, um auf den Bereich **Erweiterte Funktionen konfigurieren** zuzugreifen und das Kontrollkästchen **Reputation** zu aktivieren.
2. Klicken Sie auf **OK**.

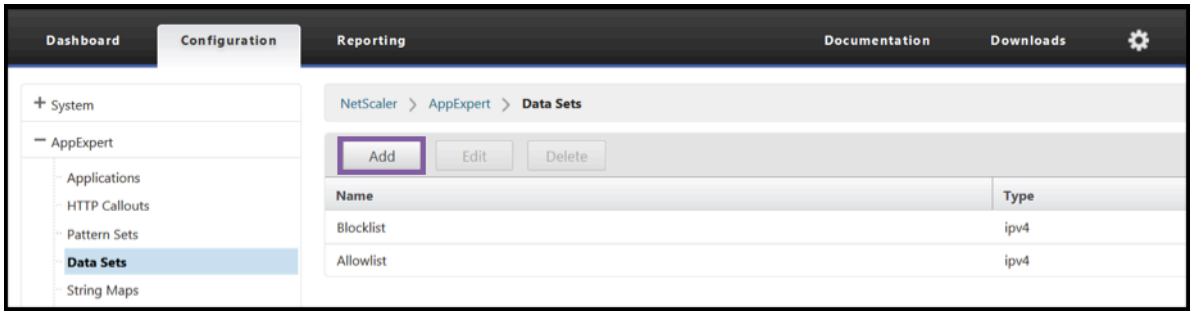


So konfigurieren Sie einen Proxyserver über die Citrix ADC GUI

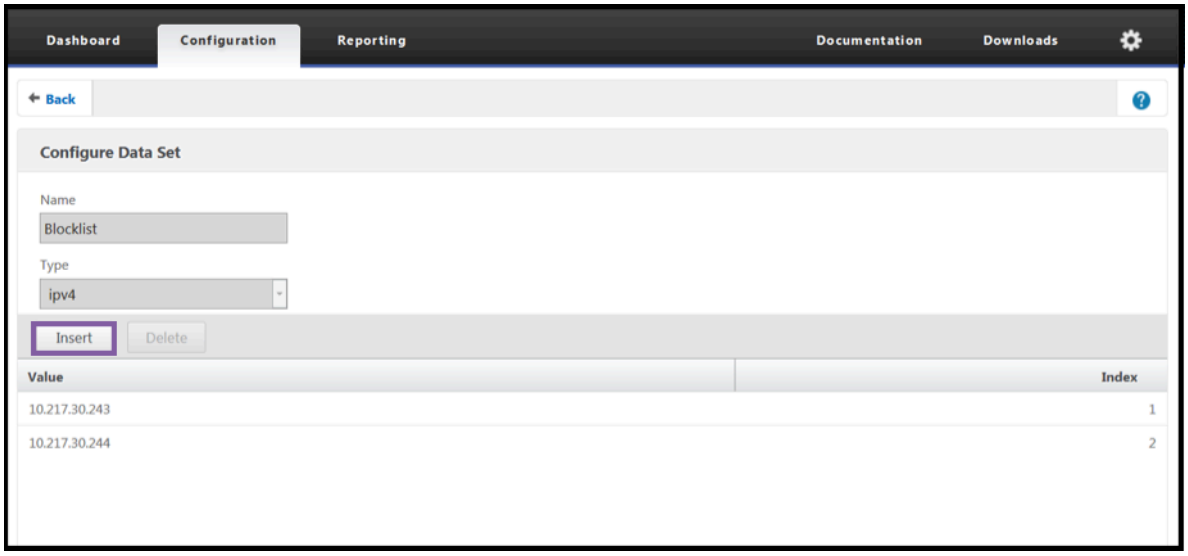
1. Navigieren Sie auf der Registerkarte Konfiguration zu **Sicherheit > Reputation**. Klicken Sie unter **Einstellungen**auf **Reputationseinstellungen ändern**, um einen Proxyserver zu konfigurieren. Sie können die Reputationsfunktion auch aktivieren oder deaktivieren. **Proxyserver** kann eine IP-Adresse oder ein vollqualifizierter Domänenname (FQDN) sein. Der**Proxy-Port** akzeptiert Werte zwischen [1 und 65535].

Erstellen Sie über die GUI eine Positivliste und eine Sperrliste von Client-IP-Adressen

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **AppExpert > Datensätze**.
2. Klicken Sie auf **Hinzufügen**.



- Geben **Sie im Bereich Datensatz erstellen** (oder **Datensatz konfigurieren**) einen aussagekräftigen Namen für die Liste der IP-Adressen an. Der Name muss den Zweck der Liste widerspiegeln.
- Wählen Sie **Typ** als **IPv4**aus.
- Klicken Sie auf **Einfügen**, um einen Eintrag hinzuzufügen.



- Fügen **Sie im Bereich Policy-Dataset-Bindung konfigurieren** eine IP-Adresse im IPv4-Format in das Eingabefeld Wert ein.
- Stellen Sie einen Index bereit.
- Fügen Sie einen Kommentar hinzu, der den Zweck der Liste erklärt. Dieser Schritt ist optional, wird jedoch empfohlen, da ein beschreibender Kommentar bei der Verwaltung der Liste hilfreich ist.

Auf ähnliche Weise können Sie eine Sperrliste erstellen und die IP-Adressen hinzufügen, die als bösartig angesehen werden sollen.

Weitere Informationen zur Verwendung von Datensätzen und Konfigurieren von Standardsyntaxrichtlinienausdrücken finden Sie unter Mustersätze und Datensätze.

Konfigurieren einer Anwendungs-Firewall-Richtlinie über die Citrix ADC GUI

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **Sicherheit > Anwendungsfirewall**

> Richtlinien > Firewall. Klicken Sie auf **Hinzufügen**, um mithilfe der PI-Ausdrücke eine Richtlinie hinzuzufügen, um die IP-Reputation zu verwenden.

Sie können auch den Ausdruckseditor verwenden, um Ihren eigenen Richtlinienausdruck zu erstellen. Die Liste zeigt vorkonfigurierte Optionen, die für die Konfiguration eines Ausdrucks mithilfe der Bedrohungskategorien nützlich sind.

Highlights

- Stoppen Sie schnell und genau schlechten Datenverkehr am Netzwerkrand von bekannten bösartigen IP-Adressen, die verschiedene Arten von Bedrohungen darstellen. Sie können die Anfrage blockieren, ohne den Text zu analysieren.
- Konfigurieren Sie dynamisch die IP-Reputationsfunktion für mehrere Anwendungen.
- Schützen Sie Ihr Netzwerk ohne Leistungseinbußen vor Datenverletzungen und konsolidieren Sie den Schutz mithilfe schneller und einfacher Bereitstellungen auf einer einzigen Services-Fabric.
- Sie können IP-Reputationsprüfungen für Quell- und Ziel-IPs durchführen.
- Sie können die Header auch überprüfen, um schädliche IPs zu erkennen.
- Die IP-Reputationsprüfung wird sowohl bei Forward-Proxy- als auch bei Reverse-Proxy-Bereitstellungen unterstützt.
- Der IP-Reputationsprozess stellt eine Verbindung zu Webroot her und aktualisiert die Datenbank alle 5 Minuten.
- Jeder Knoten in der High Availability (HA) oder Clusterbereitstellung erhält die Datenbank von Webroot.
- Die IP-Reputationsdaten werden von allen Partitionen in Admin-Partitions-Bereitstellungen gemeinsam genutzt.
- Sie können einen AppExpert-Datensatz verwenden, um Listen von IP-Adressen zu erstellen und Ausnahmen für IPs hinzuzufügen, die in der Webroot Datenbank blockiert sind. Sie können auch Ihre eigene angepasste Sperrliste erstellen, um bestimmte IPs als bösartig zu kennzeichnen.
- Die Datei iprep.db wird im `/var/nslog/iprep` Ordner erstellt. Nach der Erstellung wird es nicht gelöscht, auch wenn das Feature deaktiviert ist.
- Wenn die Reputationsfunktion aktiviert ist, wird die Citrix ADC Webroot Datenbank heruntergeladen. Danach wird es alle 5 Minuten aktualisiert.
- Die Webroot-Datenbankversion ist 1.
- Die Nebenversion wird jeden Tag aktualisiert. Die Update-Version wird alle 5 Minuten erhöht und auf 1 zurückgesetzt, wenn die Nebenversion erhöht wird.
- PI-Ausdrücke ermöglichen es Ihnen, die IP-Reputation mit anderen Funktionen wie Responder und Rewrite zu verwenden.
- Die IP-Adressen in der Datenbank sind in Dezimalschreibweise.

Tipps zum Debuggen

- Wenn Sie die Reputationsfunktion in der GUI nicht sehen können, überprüfen Sie, ob Sie über die richtige Lizenz verfügen.
- Überwachen Sie die Nachrichten `var/log/iprep.log` zum Debuggen.
- **Webrootkonnektivität**: Wenn die `ns iprep: Not able to connect/resolve WebRoot` Meldung angezeigt wird, stellen Sie sicher, dass die Appliance über einen Internetzugang verfügt und DNS konfiguriert ist.
- **Proxyserver**: Wenn die `ns iprep: iprep_curl_download: 88 curl_easy_perform failed. Error code: 5 Err msg:couldnt resolve proxy name` Meldung angezeigt wird, stellen Sie sicher, dass die Proxy-Serverkonfiguration korrekt ist.
- **IP-Reputationsfunktion funktioniert nicht**: Der IP-Reputationsprozess dauert etwa fünf Minuten, nachdem Sie die Reputationsfunktion aktiviert haben. Die IP-Reputationsfunktion funktioniert möglicherweise für diese Dauer nicht.
- **Datenbankdownload**: Wenn der Download von IP-DB-Daten nach dem Aktivieren der IP-Reputationsfunktion fehlschlägt, wird der folgende Fehler in den Protokollen angezeigt.

```
iprep: iprep_curl_download:86 curl_easy_perform failed. Error code:7 Err
msg:Couldn't connect to server
```

Lösung: Zulassen Sie den ausgehenden Datenverkehr zu den folgenden URLs, oder konfigurieren Sie einen Proxy, um das Problem zu beheben.

```
localdb-ip-daily.brightcloud.com:443
localdb-ip-rtu.brightcloud.com:443
api.bcti.brightcloud.com:443
<!--NeedCopy-->
```

SSL-Offload und Beschleunigung

October 5, 2021

Eine Citrix ADC Appliance, die für die SSL-Beschleunigung konfiguriert ist, beschleunigt SSL-Transaktionen transparent, indem SSL-Verarbeitung vom Server entfernt wird. Zum Konfigurieren von SSL-Offload konfigurieren Sie einen virtuellen Server zum Abfangen und Verarbeiten von SSL-Transaktionen und senden den entschlüsselten Datenverkehr an den Server (es sei denn, Sie konfigurieren die End-to-End-Verschlüsselung, in diesem Fall wird der Datenverkehr neu verschlüsselt). Nach Erhalt der Antwort vom Server schließt die Appliance die sichere Transaktion mit dem Client ab. Aus Sicht des Clients scheint die Transaktion direkt beim Server zu sein. Ein Citrix ADC,

der für die SSL-Beschleunigung konfiguriert ist, führt auch andere konfigurierte Funktionen aus, z. B. den Lastausgleich.

Für die Konfiguration von SSL-Offload sind ein SSL-Zertifikat und ein Schlüsselpaar erforderlich, das Sie erhalten müssen, wenn Sie noch kein SSL-Zertifikat besitzen. Weitere SSL-bezogene Aufgaben, die Sie möglicherweise ausführen müssen, umfassen das Verwalten von Zertifikatssperrlisten, das Konfigurieren der Clientauthentifizierung und das Verwalten von SSL-Aktionen und -Richtlinien.

Eine Nicht-FIPS-Citrix ADC Appliance speichert den privaten Schlüssel des Servers auf der Festplatte. Auf einer FIPS-Appliance wird der Schlüssel in einem kryptografischen Modul gespeichert, das als Hardwaresicherheitsmodul (HSM) bezeichnet wird.

Alle Citrix ADC Appliances, die keine FIPS-Karte unterstützen (einschließlich virtueller Appliances), unterstützen die externen Thales nShield® Connect und SafeNet HSMs. (MPX 9700/10500/12500/15500-Appliances unterstützen kein externes HSM.)

Hinweis: FIPS-bezogene Optionen für einige der in diesem Dokument beschriebenen SSL-Konfigurationsverfahren sind spezifisch für eine FIPS-fähige Citrix ADC Appliance.

SSL-Offload-Konfiguration

March 8, 2022

Um das SSL-Offloading zu konfigurieren, müssen Sie die SSL-Verarbeitung auf der Citrix ADC-Appliance aktivieren und einen SSL-basierten virtuellen Server konfigurieren. Der virtuelle Server fängt SSL-Verkehr ab, entschlüsselt den Datenverkehr und leitet ihn an einen Dienst weiter, der an den virtuellen Server gebunden ist. Um zeitkritischen Datenverkehr wie Medienstreaming zu sichern, können Sie einen virtuellen DTLS-Server konfigurieren. Um das SSL-Offloading zu aktivieren, müssen Sie ein gültiges Zertifikat und einen gültigen Schlüssel importieren und das Paar an den virtuellen Server binden.

SSL aktivieren

Um SSL-Verkehr zu verarbeiten, müssen Sie die SSL-Verarbeitung aktivieren. Sie können SSL-basierte Entitäten wie virtuelle Server und Dienste konfigurieren, ohne die SSL-Verarbeitung zu aktivieren. Sie funktionieren jedoch erst, wenn die SSL-Verarbeitung aktiviert ist.

SSL-Verarbeitung über die CLI aktivieren

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
enable ns feature ssl

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

Beispiel:

```
enable ns feature SSL
 Done
show ns feature

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

SSL-Verarbeitung über die GUI aktivieren

Navigieren Sie zu **System > Einstellungen**, und klicken Sie in der Gruppe **Modi und Funktionen** auf **Grundfunktionen konfigurieren**, und klicken Sie auf **SSL-Offloading**.

Konfigurieren von Diensten

Auf der Citrix ADC-Appliance stellt ein Dienst einen physischen Server oder eine Anwendung auf einem physischen Server dar. Nach der Konfiguration befinden sich Dienste im deaktivierten Zustand, bis die Appliance den physischen Server im Netzwerk erreichen und seinen Status überwachen kann.

Hinzufügen eines Dienstes über die CLI

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

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

Beispiel:

```
add service sslsvc 198.51.100.225 SSL 443

Done

sh ssl service sslsvc

            Advanced SSL configuration for Back-end SSL Service sslsvc:
            DH: DISABLED
            DH Private-Key Exponent Size Limit: DISABLED    Ephemeral
                RSA: DISABLED
            Session Reuse: ENABLED          Timeout: 300 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Server Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            OCSP Stapling: DISABLED
            SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1:
                ENABLED  TLSv1.2: ENABLED  TLSv1.3: DISABLED
            Send Close-Notify: YES
            Strict Sig-Digest Check: DISABLED
            Zero RTT Early Data: ???
            DHE Key Exchange With PSK: ???
            Tickets Per Authentication Context: ???

            ECC Curve: P_256, P_384, P_224, P_521

    1)      Cipher Name: DEFAULT_BACKEND
            Description: Default cipher list for Backend SSL session
```



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

Ändern oder entfernen Sie einen Dienst über die CLI

Um einen Dienst zu ändern, verwenden Sie den Befehl set service. Dies entspricht genau dem Befehl add service, außer dass Sie den Namen eines vorhandenen Dienstes eingeben.

Um einen Dienst zu entfernen, verwenden Sie den Befehl rm service, der nur das <name> -Argument akzeptiert.

```
1 rm service <servicename>
2 <!--NeedCopy-->
```

Beispiel:

```
1 rm service sslsvc
2 <!--NeedCopy-->
```

Um einen Dienst zu ändern, verwenden Sie den Befehl set service, wählen Sie einen beliebigen Parameter aus und ändern Sie seine Einstellung.

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

Beispiel:

```
1 set service sslsvc 198.51.100.225 SSL 443
2 <!--NeedCopy-->
```

Konfigurieren Sie einen Dienst über die GUI

Navigieren Sie zu **Traffic Management > Load Balancing > Dienste**, erstellen Sie einen Dienst und geben Sie das Protokoll als SSL an.

Virtuelle SSL-Serverkonfiguration

Für sichere Sitzungen muss eine Verbindung zwischen dem Client und einem SSL-basierten virtuellen Server auf der Citrix ADC-Appliance hergestellt werden. Der virtuelle SSL-Server fängt den SSL-Verkehr ab, entschlüsselt ihn und verarbeitet ihn, bevor er an Dienste gesendet wird, die an den virtuellen Server gebunden sind.

Hinweis: Der virtuelle SSL-Server wird auf der Citrix ADC-Appliance als heruntergefahren markiert, bis ein gültiges Zertifikat-/Schlüsselpaar und mindestens ein Dienst daran gebunden sind. Ein SSL-basierter virtueller Server ist ein virtueller Lastausgleichsserver vom Protokolltyp SSL oder SSL_TCP. Die Lastausgleichsfunktion muss auf der Citrix ADC-Appliance aktiviert sein.

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

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

```
add lb vserver <name> (serviceType) <IPAddress> <port>
show ssl vserver <name>
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver sslvs SSL 192.0.2.240 443
Done

sh ssl vserver sslvs

            Advanced SSL configuration for VServer sslvs:
            DH: DISABLED
            DH Private-Key Exponent Size Limit: DISABLED    Ephemeral
                RSA: ENABLED          Refresh Count: 0
            Session Reuse: ENABLED          Timeout: 120 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Client Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            OCSP Stapling: DISABLED
            HSTS: DISABLED
```



```
19              HSTS IncludeSubDomains: NO
20              HSTS Max-Age: 0
21              SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1:
                    ENABLED  TLSv1.2: ENABLED  TLSv1.3: DISABLED
22              Push Encryption Trigger: Always
23              Send Close-Notify: YES
24              Strict Sig-Digest Check: DISABLED
25              Zero RTT Early Data: DISABLED
26              DHE Key Exchange With PSK: NO
27              Tickets Per Authentication Context: 1
28              ECC Curve: P_256, P_384, P_224, P_521
29
30      1)      Cipher Name: DEFAULT
31              Description: Default cipher list with encryption strength
                   >= 128bit
32       Done
33  <!--NeedCopy-->
```

Ändern oder entfernen Sie einen SSL-basierten virtuellen Server über die CLI

Verwenden Sie den `set lb vserver` Befehl, um die Lastausgleichseigenschaften eines virtuellen SSL-Servers zu ändern. Der Befehl set ähnelt dem `add lb vserver` Befehl, außer dass Sie den Namen eines vorhandenen virtuellen Servers eingeben. Um die **SSL-Eigenschaften** eines SSL-basierten virtuellen Servers zu ändern, verwenden Sie den `set ssl vserver` Befehl. Weitere Informationen finden Sie im Abschnitt “Virtuelle SSL-Server-Parameter” weiter unten auf dieser Seite.

Um einen virtuellen SSL-Server zu entfernen, verwenden Sie den `rm lb vserver` Befehl, der nur das `<name>` Argument akzeptiert.

Konfigurieren eines SSL-basierten virtuellen Servers über die GUI

Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, erstellen Sie einen virtuellen Server und geben Sie das Protokoll als SSL an.

Binden Sie Dienste an den virtuellen SSL-Server

Die ADC-Appliance leitet entschlüsselte SSL-Daten an Server im Netzwerk weiter. Um Daten weiterzuleiten, müssen Dienste, die diese physischen Server darstellen, an den virtuellen Server gebunden sein, der die SSL-Daten empfängt.

In der Regel ist die Verbindung zwischen der ADC-Appliance und dem physischen Server sicher. Daher muss die Datenübertragung zwischen der Appliance und dem physischen Server nicht verschlüsselt

werden. Sie können jedoch End-to-Ende-Verschlüsselung bereitstellen, indem Sie die Datenübertragung zwischen der Appliance und dem Server verschlüsseln. Weitere Informationen finden Sie unter Konfigurieren des SSL-Offloading mit End-to-End-Verschlüsselung.

Hinweis: Aktivieren Sie die Lastenausgleichsfunktion auf der ADC-Appliance, bevor Sie Dienste an den SSL-basierten virtuellen Server binden.

Binden eines Dienstes an einen virtuellen Server mit der CLI

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

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

Beispiel:

```
bind lb vserver sslvs sslsvc
     Done

sh lb vserver sslvs

            sslvs (192.0.2.240:443) - SSL       Type: ADDRESS
            State: DOWN[Certkey not bound]
            Last state change was at Wed May  2 11:43:04 2018
            Time since last state change: 0 days, 00:13:21.150
            Effective State: DOWN
            Client Idle Timeout: 180 sec
            Down state flush: ENABLED
            Disable Primary Vserver On Down : DISABLED
            Appflow logging: ENABLED
            No. of Bound Services :  1 (Total)       0 (Active)
            Configured Method: LEASTCONNECTION      BackupMethod:
               ROUNDROBIN
            Mode: IP
            Persistence: NONE
            Vserver IP and Port insertion: OFF
            Push: DISABLED  Push VServer:
            Push Multi Clients: NO
            Push Label Rule: none
            L2Conn: OFF
```



```
            Skip Persistency: None
            Listen Policy: NONE
            IcmpResponse: PASSIVE
            RHIstate: PASSIVE
            New Service Startup Request Rate: 0 PER_SECOND, Increment
               Interval: 0
            Mac mode Retain Vlan: DISABLED
            DBS_LB: DISABLED
            Process Local: DISABLE
            Traffic Domain: 0
            TROFS Persistence honored: ENABLED
            Retain Connections on Cluster: NO
    1) sslsvc (198.51.100.225: 443) - SSL State: DOWN       Weight: 1
     Done
<!--NeedCopy-->
```

Trennen Sie einen Dienst über die CLI von einem virtuellen Server

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
unbind lb vserver <name> <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
unbind lb vserver sslvs sslsvc
     Done
<!--NeedCopy-->
```

Binden Sie einen Dienst über die GUI an einen virtuellen Server

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen Server und klicken Sie im Abschnitt **Dienste und Dienstgruppen auf die Kachel Load Balancing Virtual Server ServiceBindings** .
3. Klicken Sie auf der Seite **Load Balancing Virtual Server Service Binding** auf die Registerkarte **Bindungen hinzufügen**, **klicken Sie auf Klicken, um** unter **Dienst auswählen**auszuwählen, und aktivieren Sie das Kontrollkästchen neben dem zu bindenden Dienst.
4. Klicken Sie auf **Auswählen** und dann auf **Binden**

Konfigurieren eines virtuellen Servers mit Servernamenangabe (SNI) für das sichere Hosting mehrerer Sites

Virtuelles Hosting wird von Webservern verwendet, um mehr als einen Domainnamen mit derselben IP-Adresse zu hosten. Die Appliance unterstützt das Hosting mehrerer sicherer Domänen, indem sie die SSL-Verarbeitung mithilfe transparenter SSL-Dienste oder virtueller serverbasierter SSL-Offloading von den Webservern auslagert. Wenn jedoch mehrere Sites auf demselben virtuellen Server gehostet werden, ist der SSL-Handshake abgeschlossen, bevor der erwartete Hostname an den virtuellen Server gesendet wird. Daher kann die Appliance nicht ermitteln, welches Zertifikat dem Client nach dem Herstellen einer Verbindung vorgelegt werden soll. Dieses Problem wird gelöst, indem SNI auf dem virtuellen Server aktiviert wird. SNI ist eine Transport Layer Security (TLS) -Erweiterung, die vom Client verwendet wird, um den Hostnamen während der Handshake-Initiierung anzugeben. Die ADC-Appliance vergleicht diesen Hostnamen mit dem allgemeinen Namen und vergleicht ihn, falls er nicht übereinstimmt, mit dem alternativen Antragstellernamen (SAN). Wenn der Name übereinstimmt, legt die Appliance dem Client das entsprechende Zertifikat vor.

Ein Wildcard-SSL-Zertifikat ermöglicht die SSL-Verschlüsselung für mehrere Subdomänen, wenn dieselbe Organisation diese Domänen kontrolliert und der Domainname der zweiten Ebene derselbe ist. Beispielsweise kann ein Wildcard-Zertifikat, das an ein Sportnetzwerk mit dem allgemeinen Namen "*.sports.net" ausgestellt wurde, verwendet werden, um Domänen wie "login.sports.net" und "help.sports.net" zu sichern. Die Domäne "login.ftp.sports.net" kann nicht gesichert werden.

Hinweis:
Auf einer ADC-Appliance werden nur DNS-Einträge für Domänenname, URL und E-Mail-ID im Feld **SAN** verglichen.

Mit der Option -SNICert können Sie mehrere Serverzertifikate an einen einzelnen virtuellen SSL-Server oder transparenten Dienst binden. Der virtuelle Server oder Dienst stellt diese Zertifikate aus, wenn SNI auf dem virtuellen Server oder Dienst aktiviert ist. Sie können SNI jederzeit aktivieren.

Binden Sie mehrere Serverzertifikate über die CLI an einen einzelnen virtuellen SSL-Server

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

```
set ssl vserver <vServerName>@ [-SNIEnable ( ENABLED | DISABLED )]

bind ssl vserver <vServerName>@ -certkeyName <string> -SNICert

show ssl vserver <vServerName>
<!--NeedCopy-->
```


Um mehrere Serverzertifikate über die CLI an einen transparenten Dienst zu binden, `vserver` ersetzen Sie in den vorhergehenden Befehlen durch den Dienst und `vservername` durch den Dienstnamen.

Hinweis: Erstellen Sie den SSL-Dienst mit der `-clearTextPort 80` Option.

Binden Sie mehrere Serverzertifikate über die GUI an einen einzelnen virtuellen SSL-Server

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen SSL-Server und wählen Sie unter **CertificatesServerzertifikat**aus.
3. Fügen Sie ein Zertifikat hinzu oder wählen Sie ein Zertifikat aus der Liste aus, und klicken Sie auf **Serverzertifikat für SNI**.
4. Wählen Sie in **den erweiterten EinstellungenSSL-Parameter**aus.
5. Klicken Sie auf **SNI Enable**.

Unterstützung für SNI im Back-End-Dienst

> **Hinweis**: SNI wird in einem DTLS-Back-End-Dienst nicht unterstützt.

Die Citrix ADC-Appliance unterstützt Server Name Indication (SNI) im Backend. Das heißt, der allgemeine Name wird als Servername im Client-Hallo an den Back-End-Server gesendet, damit der Handshake erfolgreich abgeschlossen werden kann. Diese Unterstützung trägt dazu bei, die Sicherheitsanforderungen von Systemintegratoren des Bundes zu SNI bietet außerdem den Vorteil, dass nur ein Port verwendet wird, anstatt Hunderte verschiedener IP-Adressen und Ports in einer Firewall zu öffnen.

Zu den Sicherheitsanforderungen des föderalen Systemintegrators gehört die Unterstützung von Active Directory Federation Services (ADFS) 3.0 in 2012 R2 und WAP-Servern. Um diese Anforderung zu erfüllen, ist die Unterstützung für SNI im Backend einer Citrix ADC-Appliance erforderlich.

> **Hinweis:**
>
> Damit SNI funktioniert, muss der Servername im Client-Hello mit dem Hostnamen übereinstimmen, der im Back-End-Dienst konfiguriert ist, der an einen virtuellen SSL-Server gebunden ist. Wenn der Hostname des Backend-Servers beispielsweise www.mail.example.com lautet, muss der SNI-fähige Back-End-Dienst mit dem Servernamen als konfiguriert werden https://www.mail.example.com. Und dieser Hostname muss mit dem Servernamen im Client Hello übereinstimmen.

Unterstützung für dynamisches SNI im Back-End-Dienst

Die Citrix ADC-Appliance unterstützt dynamisches SNI auf den Back-End-TLS-Verbindungen. Das heißt, die Appliance lernt den SNI in der Clientverbindung und verwendet ihn in der serverseitigen

Verbindung. Sie müssen keinen allgemeinen Namen mehr im SSL-Dienst, in der Dienstgruppe oder im Profil angeben. Der in der SNI-Erweiterung der Client-Hello-Nachricht empfangene allgemeine Name wird an die Back-End-SSL-Verbindung weitergeleitet.

Zuvor mussten Sie statisches SNI für SSL-Dienste, Dienstgruppen und SSL-Profile konfigurieren. Daher wurde nur die konfigurierte statische SNI-Erweiterung an den Server gesendet. Wenn ein Client gleichzeitig auf mehrere Domänen zugreifen musste, konnte die ADC-Appliance das vom Client empfangene SNI nicht an den Back-End-Dienst senden. Stattdessen wurde der statische allgemeine Name gesendet, der konfiguriert wurde. Wenn der Back-End-Server jetzt für mehrere Domänen konfiguriert ist, kann der Server mit dem richtigen Zertifikat antworten, das auf dem SNI basiert, das in der Client-Hello-Nachricht von der Appliance empfangen wurde.

Zeigen Sie auf Hinweis:

- SNI muss auf dem Front-End aktiviert sein und das richtige SNI-Zertifikat muss an den virtuellen SSL-Server gebunden sein. Wenn Sie SNI im Front-End nicht aktivieren, werden die SNI-Informationen nicht an das Back-End weitergegeben.
- Wenn die Serverauthentifizierung aktiviert ist, wird das Serverzertifikat durch das CA-Zertifikat überprüft, und die allgemeinen Name/SAN-Einträge im Serverzertifikat werden mit dem SNI abgeglichen. Daher muss das CA-Zertifikat an den Dienst gebunden sein.
- Die Wiederverwendung der Back-End-Verbindung und der SSL-Sitzung basiert auf SNI, wenn dynamisches SNI aktiviert ist.

SSL-Monitore senden kein SNI, wenn dynamisches SNI aktiviert ist. Für SNI-basierte Sondierung fügen Sie ein Back-End-Profil an, auf dem statisches SNI für die SSL-Monitore konfiguriert ist. Der Monitor muss mit demselben benutzerdefinierten Header wie SNI konfiguriert werden.

Konfigurieren von SNI im Back-End-Dienst über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name>  <IP>  <serviceType>  <port>

add lb vserver <name>  <IPAddress> <serviceType>  <port>

bind lb vserver <name> <serviceName>

set ssl service <serviceName> -SNIEnable ENABLED -commonName <string>

set ssl profile <name> -SNIEnable ENABLED
<!--NeedCopy-->
```


Beispiel:

```
    add service service_ssl 198.51.100.100 SSL 443

    add lb vserver ssl-vs 203.0.113.200 SSL 443

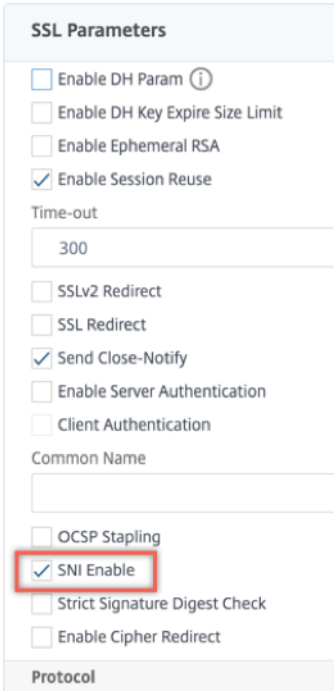
    bind lb vserver ssl-vs service_ssl

    set ssl service service_ssl -SNIEnable ENABLED  - commonName www.
       example.com

    set ssl profile sslprof -SNIEnable ENABLED
<!--NeedCopy-->
```

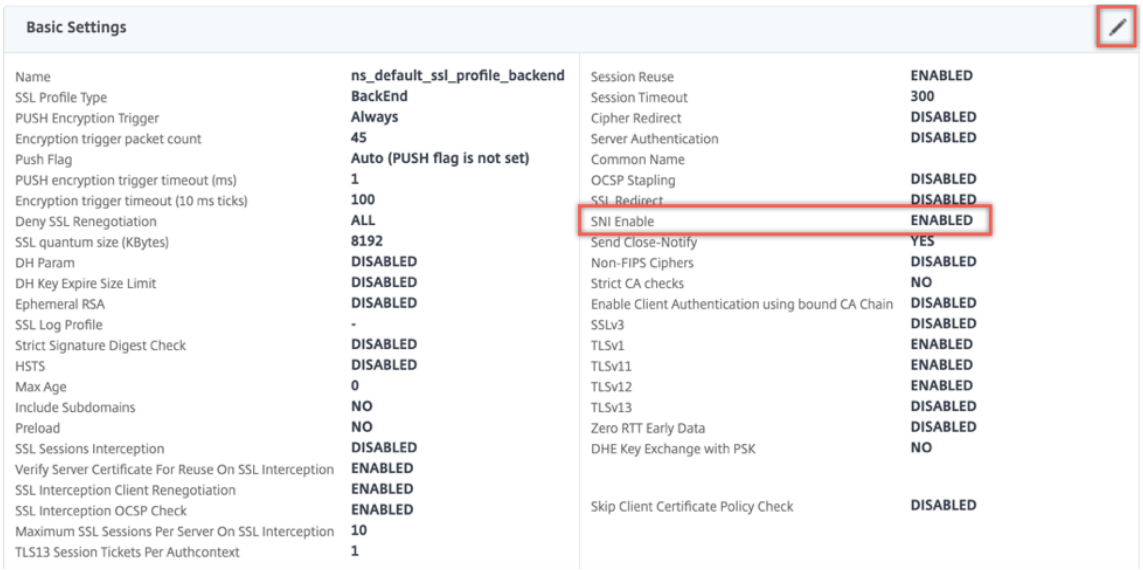
Konfigurieren Sie SNI im Back-End-Dienst über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Wählen Sie einen SSL-Dienst aus und klicken Sie in **Erweiterte Einstellungen**auf **SSL-Parameter**.
3. Klicken Sie auf **SNI Enable**.



Konfigurieren Sie SNI im SSL-Profil über die GUI

1. Navigieren Sie zu **System > Profile > SSL-Profil**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie in **den GrundeinstellungenSNI-Aktivierung**aus.



4. Klicken Sie auf **OK**.

Binden Sie einen sicheren Monitor an einen SNI-fähigen Back-End-Dienst

Sie können sichere Monitore vom Typ HTTP, HTTP-ECV, TCP oder TCP-ECV an die Back-End-Dienste und Dienstgruppen binden, die SNI unterstützen. Die Monitor-Prüfpunkte senden jedoch nicht die SNI-Erweiterung, wenn dynamisches SNI aktiviert ist. Um SNI-Prüfungen zu senden, aktivieren Sie statisches SNI im Back-End-SSL-Profil und binden Sie das Profil an den Monitor. Stellen Sie den benutzerdefinierten Header im Monitor auf den Servernamen ein, der als SNI-Erweiterung im Client-Hello der Monitorprobe gesendet wird.

Konfigurieren und binden Sie einen sicheren Monitor über die CLI an einen SNI-fähigen Back-End-Dienst

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb monitor <monitorName> <type> -secure YES
add ssl profile <name> -sslProfileType BackEnd
set lb monitor <monitorName> <type> -customHeaders <string> -sslprofile
    <backend ssl profile>
```



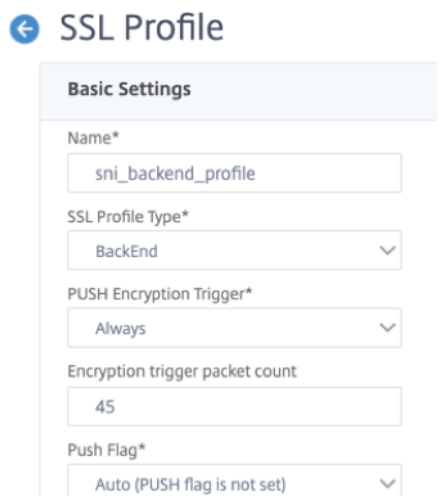
```
set ssl profile <name> -sniEnable ENABLED -commonName <string>
bind service <name> -monitorName <string>
<!--NeedCopy-->
```

Beispiel:

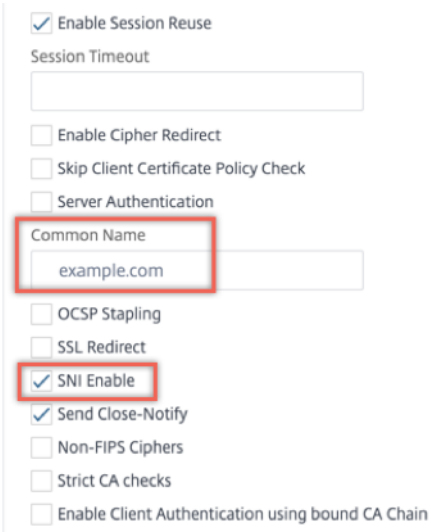
```
add ssl profile sni_backend_profile -sslProfileType BackEnd
set ssl profile sni_backend_profile -sniEnable ENABLED -commonName
   example.com
add lb monitor http-ecv-mon HTTP-ECV -secure YES
set monitor http-ecv-mon HTTP-ECV -customHeaders "Host: example.com\r\n
   " -sslprofile sni_backend_profile
bind service ssl_service  - monitorName http-ecv-mon
<!--NeedCopy-->
```

Konfigurieren und binden Sie einen sicheren Monitor über die GUI an einen SNI-fähigen Back-End-Dienst

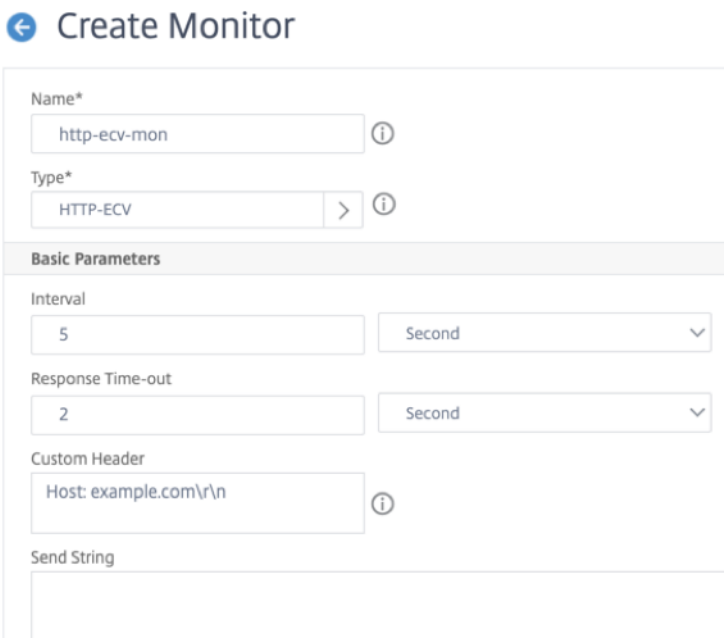
1. Navigieren Sie zu **System > Profile > SSL-Profile**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie einen Namen für das Profil an und wählen Sie **unter SSL-ProfiltypBackend**aus.



4. Geben Sie den allgemeinen Namen an (wie Host-Header) und wählen Sie **SNI-Aktivieren**.

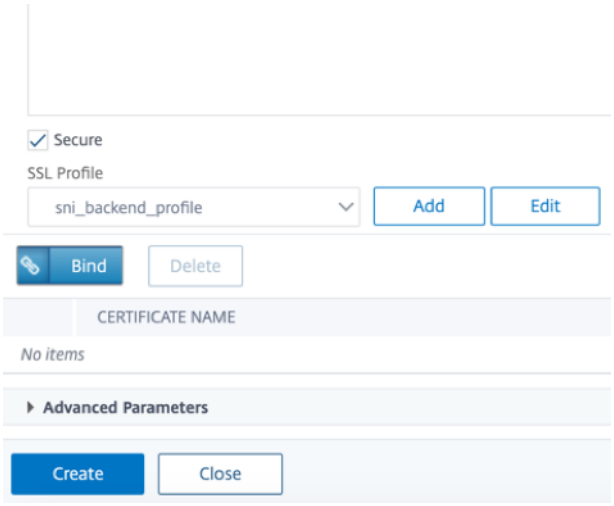


5. Klicken Sie auf **OK**.
6. Navigieren Sie zu **Traffic Management > Load Balancing > Überwachen**.
7. Klicken Sie auf **Hinzufügen**.
8. Geben Sie einen Namen für den Monitor an. Wählen Sie unter **Typ**die Option HTTP, HTTP-ECV, TCP oder TCP-ECV aus.
9. Geben Sie einen **benutzerdefinierten Header**an.

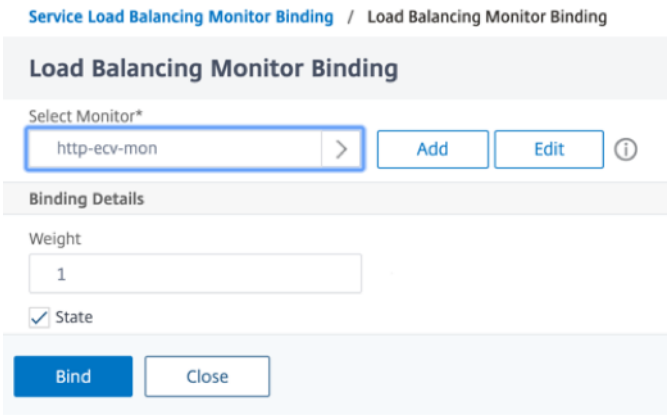


10. Wählen Sie **Sicher**aus.
11. Wählen Sie im **SSL-Profil**das Back-End-SSL-Profil aus, das in den vorherigen Schritten erstellt wurde.

12. Klicken Sie auf **Erstellen**.



13. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
14. Wählen Sie einen SSL-Dienst und klicken Sie auf **Bearbeiten**.
15. Klicken Sie **unter Monitore**auf **Bindung hinzufügen**, wählen Sie den in den vorherigen Schritten erstellten Monitor aus und klicken Sie auf **Binden**.



Konfigurieren und binden Sie einen sicheren Monitor über die GUI an einen SNI-fähigen Back-End-Dienst

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Monitor**.
2. Fügen Sie einen Monitor vom Typ **HTTP-ECV** oder **TCP-ECV**hinzu und geben Sie einen **benutzerdefinierten Header**an.
3. Klicken Sie auf **Erstellen**.
4. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienste**.
5. Wählen Sie einen SSL-Dienst und klicken Sie auf **Bearbeiten**.
6. Klicken Sie **unter Monitore**auf **Bindung hinzufügen**, wählen Sie den in Schritt 3 erstellten Monitor aus und klicken Sie auf **Binden**.

Hinzufügen oder Aktualisieren eines Zertifikatsschlüsselpaars

> **Hinweise:**
>
> Wenn Sie kein vorhandenes Zertifikat und keinen vorhandenen Schlüssel haben, lesen Sie ein Zertifikat erstellen.
>
> Um ein ECDSA-Zertifikatschlüsselpaar zu erstellen, klicken Sie auf Ein ECDSA-Zertifikatschlüsselpaarerstellen.
>
> Ab Build 41.x werden Zertifikatnamen mit bis zu 63 Zeichen unterstützt.
>
> Ab Version 13.0 build 79.x werden kennwortgeschützte Zertifikatschlüsselpaare immer erfolgreich hinzugefügt. Früher, wenn die Option für starkes Kennwort auf einer Citrix ADC-Appliance aktiviert war, wurden die kennwortgeschützten Zertifikatsschlüsselpaare manchmal nicht hinzugefügt. Die Zertifikatschlüsselkonfiguration geht jedoch verloren, wenn Sie auf einen früheren Build herunterstufen. In der NITRO-API-Antwort für Zertifikatschlüsselpaare wird die `passplain` Variable anstelle der `passcrypt` Variablen gesendet.

Für jede SSL-Transaktion benötigt der Server ein gültiges Zertifikat und das entsprechende private und öffentliche Schlüsselpaar. Die SSL-Daten werden mit dem öffentlichen Schlüssel des Servers verschlüsselt, der über das Zertifikat des Servers verfügbar ist. Für die Entschlüsselung ist der entsprechende private Schlüssel erforderlich. Das Kennwort des privaten Schlüssels, der beim Hinzufügen eines SSL-Zertifikatsschlüsselpaars verwendet wird, wird mit einem eindeutigen Verschlüsselungsschlüssel für jede Citrix ADC-Appliance gespeichert.

Die ADC-Appliance lagert SSL-Transaktionen vom Server aus. Daher müssen das Zertifikat und der private Schlüssel des Servers auf der Appliance vorhanden sein, und das Zertifikat muss mit dem entsprechenden privaten Schlüssel gekoppelt werden. Dieses Zertifikatsschlüsselpaar muss an den virtuellen Server gebunden sein, der die SSL-Transaktionen verarbeitet.

Hinweis: Das Standardzertifikat auf einer Citrix ADC-Appliance ist 2048 Bit. In früheren Builds war das Standardzertifikat 512 Bit oder 1024 Bit. Nach dem Upgrade auf Version 11.0 müssen Sie alle Ihre alten Zertifikatsschlüsselpaare löschen und dann die Appliance neu starten `"ns-"`, um automatisch ein 2048-Bit-Standardzertifikat zu generieren.

Sowohl das Zertifikat als auch der Schlüssel müssen sich im lokalen Speicher der Citrix ADC-Appliance befinden, bevor sie der Appliance hinzugefügt werden können. Wenn sich Ihr Zertifikat oder Ihre Schlüsseldatei nicht auf der Appliance befindet, laden Sie es auf die Appliance hoch, bevor Sie das Paar erstellen.

Wichtig: Zertifikate und Schlüssel werden standardmäßig im Verzeichnis /nsconfig/ssl gespeichert. Wenn Ihre Zertifikate oder Schlüssel an einem anderen Ort gespeichert sind, müssen Sie den absoluten Pfad zu den Dateien auf der Citrix ADC-Appliance angeben. Die Citrix ADC FIPS-Appliances unterstützen keine externen Schlüssel (Nicht-FIPS-Schlüssel). Auf einer FIPS-Appliance können Sie keine Schlüssel von einem lokalen Speichergerät wie einer Festplatte oder einem Flash-Speicher laden. Die FIPS-Schlüssel müssen im Hardware Security Module (HSM) der Appliance vorhanden sein.

Auf Citrix ADC-Appliances werden nur RSA-Schlüssel unterstützt.

Legen Sie den Benachrichtigungszeitraum fest und ermöglichen Sie dem Ablaufmonitor, vor Ablauf des Zertifikats eine Aufforderung auszustellen.

Die Citrix ADC-Appliance unterstützt die folgenden Eingabeformate des Zertifikats und der Privatschlüsseldateien:

- PEM — Datenschutz Enhanced Mail
- DER - Distinguished Encoding
- PFX - Austausch personenbezogener Daten

Die Software erkennt das Format automatisch. Daher müssen Sie das Format nicht mehr im inform-Parameter angeben. Wenn Sie das Format angeben (richtig oder falsch), ignoriert die Software es. Das Format des Zertifikats und der Schlüsseldatei müssen identisch sein.

Hinweis: Ein Zertifikat muss mit einem der folgenden Hash-Algorithmen signiert werden:

- MD5
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Eine MPX-Appliance unterstützt Zertifikate mit 512 oder mehr Bit bis zu den folgenden Größen:

- 4096-Bit-Serverzertifikat auf dem virtuellen Server
- 4096-Bit-Clientzertifikat im Dienst
- 4096-Bit-CA-Zertifikat (einschließlich Zwischen- und Stammzertifikaten)
- 4096-Bit-Zertifikat auf dem Back-End-Server
- 4096-Bit-Clientzertifikat (wenn die Clientauthentifizierung auf dem virtuellen Server aktiviert ist)

Eine virtuelle VPX-Appliance unterstützt Zertifikate mit 512 oder mehr Bit bis zu den folgenden Größen:

- 4096-Bit-Serverzertifikat auf dem virtuellen Server
- 4096-Bit-Clientzertifikat im Dienst
- 4096-Bit-CA-Zertifikat (einschließlich Zwischen- und Stammzertifikaten)
- 4096-Bit-Zertifikat auf dem Back-End-Server
- 4096-Bit-Clientzertifikat (wenn die Clientauthentifizierung auf dem virtuellen Server aktiviert ist)

> **Hinweis**
>
> Eine Citrix ADC SDX-Appliance unterstützt Zertifikate mit 512 oder mehr Bit. Jede Citrix ADC VPX-Instanz, die auf der Appliance gehostet wird, unterstützt die vorherigen Zertifikatsgrößen für

> eine virtuelle VPX-Appliance. Wenn jedoch einer Instanz ein SSL-Chip zugewiesen ist, unterstützt diese Instanz die von einer MPX-Appliance unterstützten Zertifikatsgrößen.

Hinzufügen eines Zertifikatschlüsselpaars mit der CLI

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

```
add ssl certKey <certkeyName> -cert <string>[(-key <string> [-password
   ]) | -fipsKey <string>] [-inform ( DER | PEM )] [<passplain>] [-
   expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod <
   positive_integer>]]

show ssl certKey [<certkeyName>]
<!--NeedCopy-->
```

Beispiel:

```
add ssl certKey sslckey -cert server_cert.pem -key server_key.pem -
   password ssl -expiryMonitor ENABLED -notificationPeriod 30
 Done
Note: For FIPS appliances, replace -key with -fipskey

show ssl certKey sslckey
        Name: sslckey           Status: Valid,   Days to expiration
           :8418
        Version: 3
        Serial Number: 01
        Signature Algorithm: md5WithRSAEncryption
        Issuer:  C=US,ST=SJ,L=SJ,O=NS,OU=NSSSL,CN=www.root.com
        Validity
                Not Before: Jul 15 02:25:01 2005 GMT
                Not After : Nov 30 02:25:01 2032 GMT
        Subject:  C=US,ST=SJ,L=SJ,O=NS,OU=NSSSL,CN=www.server.com
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048
 Done
<!--NeedCopy-->
```


Aktualisieren oder entfernen Sie ein Zertifikatsschlüsselpaar über die CLI

Um die Ablaufüberwachung oder den Benachrichtigungszeitraum in einem Zertifikat-Schlüsselpaar zu ändern, verwenden Sie den `set ssl certkey` Befehl. Um das Zertifikat oder den Schlüssel in einem Zertifikat-Schlüsselpaar zu ersetzen, verwenden Sie den `update ssl certkey` Befehl. Der `update ssl certkey` Befehl hat einen zusätzlichen Parameter zum Überschreiben der Domänenprüfung. Geben Sie für beide Befehle den Namen eines vorhandenen Zertifikat-Schlüssel-Paars ein. Um ein SSL-Zertifikat-Schlüsselpaar zu entfernen, verwenden Sie den `rm ssl certkey` Befehl, der nur das `<certkeyName>` Argument akzeptiert.

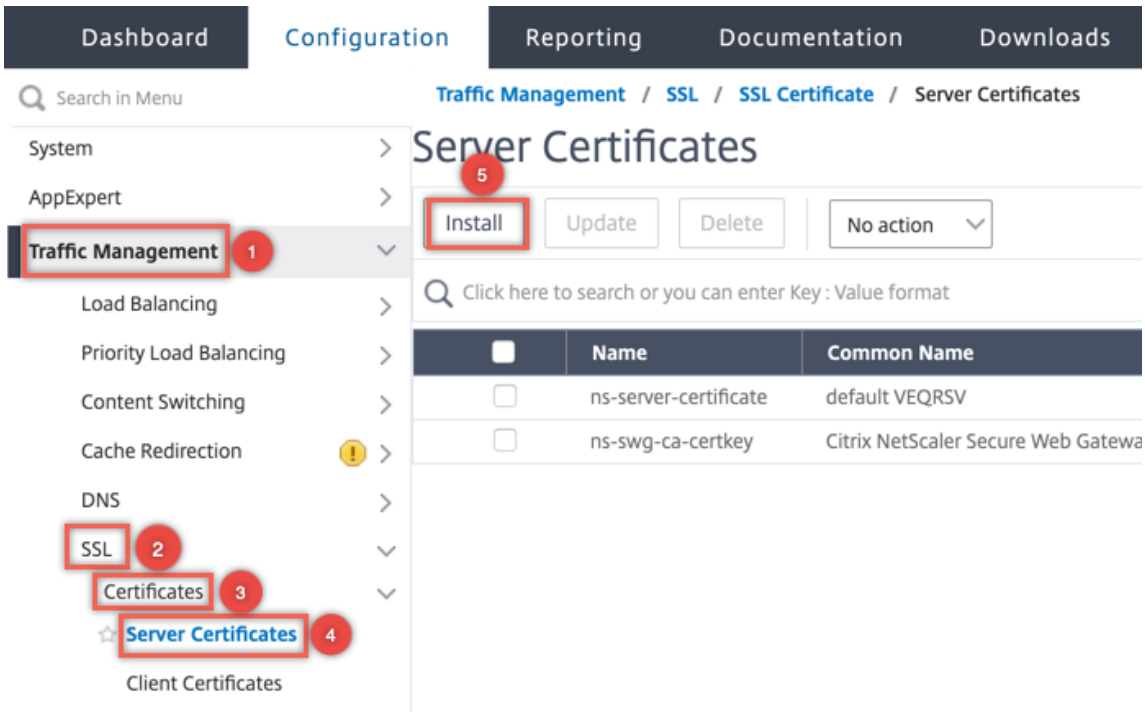
Beispiel:

```
set ssl certKey <certkeyName> [-expiryMonitor ( ENABLED | DISABLED )
       [-notificationPeriod <positive_integer>]]

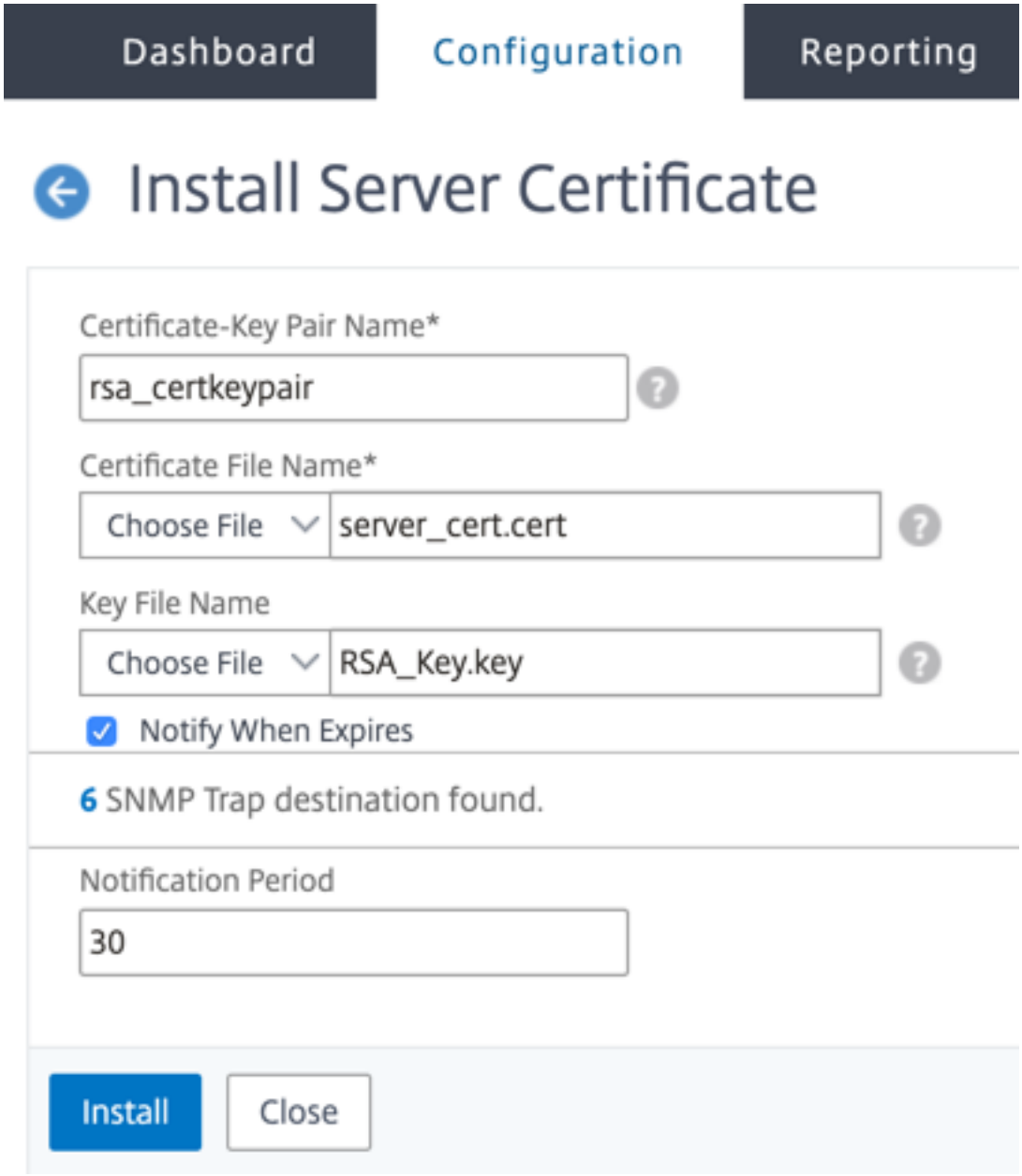
update ssl certKey <certkeyName> [-cert <string> [-password]] [-key
       <string> | -fipsKey <string>] [-inform <inform>] [-noDomainCheck
          ]
<!--NeedCopy-->
```

Hinzufügen oder Aktualisieren eines Zertifikatsschlüsselpaars über die GUI

1. Navigieren Sie zu **Traffic Management > SSL > Zertifikate > Server**.



2. Geben Sie die Werte für die folgenden Parameter ein und klicken Sie auf **Installieren**.
   - Name des Zertifikat-Schlüssel-Paars — Name für das Zertifikat und den privaten Schlüssel.
   - Zertifikatsdateiname — Signiertes Zertifikat, das von der Zertifizierungsstelle erhalten
   - Schlüsseldateiname — Name und optional Pfad der Datei mit privatem Schlüssel, die zum Bilden des Zertifikatsschlüsselpaars verwendet wird.



Binden Sie das Zertifikatschlüsselpaar an den virtuellen SSL-Server

Wichtig: Verknüpfen Sie alle Zwischenzertifikate mit diesem Zertifikat, bevor Sie das Zertifikat an einen virtuellen SSL-Server binden. Informationen zum Verknüpfen von Zertifikaten finden Sie unter Erstellen einer Zertifikatkette.

Das Zertifikat, das für die Verarbeitung von SSL-Transaktionen verwendet wird, muss an den virtuellen Server gebunden sein, der die SSL-Daten empfängt. Wenn Sie über mehrere virtuelle Server verfügen, die SSL-Daten empfangen, muss an jeden von ihnen ein gültiges Zertifikatsschlüsselpaar gebunden sein.

Verwenden Sie ein gültiges, vorhandenes SSL-Zertifikat, das Sie auf die Citrix ADC-Appliance hochgeladen haben. Erstellen Sie alternativ zu Testzwecken Ihr eigenes SSL-Zertifikat auf der Appliance. Zwischenzertifikate, die mit einem FIPS-Schlüssel auf der Appliance erstellt wurden, können nicht an einen virtuellen SSL-Server gebunden werden.

Während des SSL-Handshakes listet der Server in der Zertifikatsanforderungsnachricht während der Clientauthentifizierung die Distinguished Names (DN) aller an den Server gebundenen Zertifizierungsstellen (CA) auf. Der Server akzeptiert nur ein Clientzertifikat aus dieser Liste. Wenn Sie nicht möchten, dass der DN-Name eines bestimmten CA-Zertifikats an den SSL-Client gesendet wird, setzen Sie das `skipCA` Flag. Diese Einstellung gibt an, dass der definierte Name des bestimmten Zertifizierungsstellenzertifikats nicht an den SSL-Client gesendet werden darf.

Weitere Informationen zum Erstellen eines eigenen Zertifikats finden Sie unter Zertifikate verwalten.

Hinweis: Citrix empfiehlt, nur gültige SSL-Zertifikate zu verwenden, die von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurden.

Binden eines SSL-Zertifikatsschlüsselpaars über die CLI an einen virtuellen Server

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

```
1 -  bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName
     > -CA -skipCAName
2 -  show ssl vserver <vServerName>
3 <!--NeedCopy-->
```

Beispiel:

```
1 bind ssl vs vs1 -certkeyName cert2 -CA -skipCAName
2  Done
```



```
sh ssl vs vs1

 Advanced SSL configuration for VServer vs1:

 DH: DISABLED

 Ephemeral RSA: ENABLED Refresh Count: 0

 Session Reuse: ENABLED Timeout: 120 seconds

 Cipher Redirect: DISABLED

 SSLv2 Redirect: DISABLED

 ClearText Port: 0

 Client Auth: DISABLED

 SSL Redirect: DISABLED

 Non FIPS Ciphers: DISABLED

 SNI: DISABLED

 OCSP Stapling: DISABLED

 HSTS: DISABLED

 IncludeSubDomains: NO

 HSTS Max-Age: 0

 SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: DISABLED
    TLSv1.2: DISABLED

 Push Encryption Trigger: Always

 Send Close-Notify: YES

 Strict Sig-Digest Check: DISABLED

ECC Curve: P_256, P_384, P_224, P_521

 1) CertKey Name: cert1 CA Certificate OCSPCheck: Optional CA_Name Sent
 2) CertKey Name: cert2 CA Certificate OCSPCheck: Optional CA_Name
```



```
        Skipped
 1)  Cipher Name: DEFAULT

Description: Default cipher list with encryption strength >= 128bit
Done
<!--NeedCopy-->
```

Trennen eines SSL-Zertifikatsschlüsselpaars von einem virtuellen Server über die CLI

Wenn Sie versuchen, ein Zertifikatsschlüsselpaar mithilfe des `unbind ssl certKey <certkeyName>` Befehls von einem virtuellen Server zu trennen, wird eine Fehlermeldung angezeigt. Der Fehler tritt auf, weil sich die Syntax des Befehls geändert hat. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

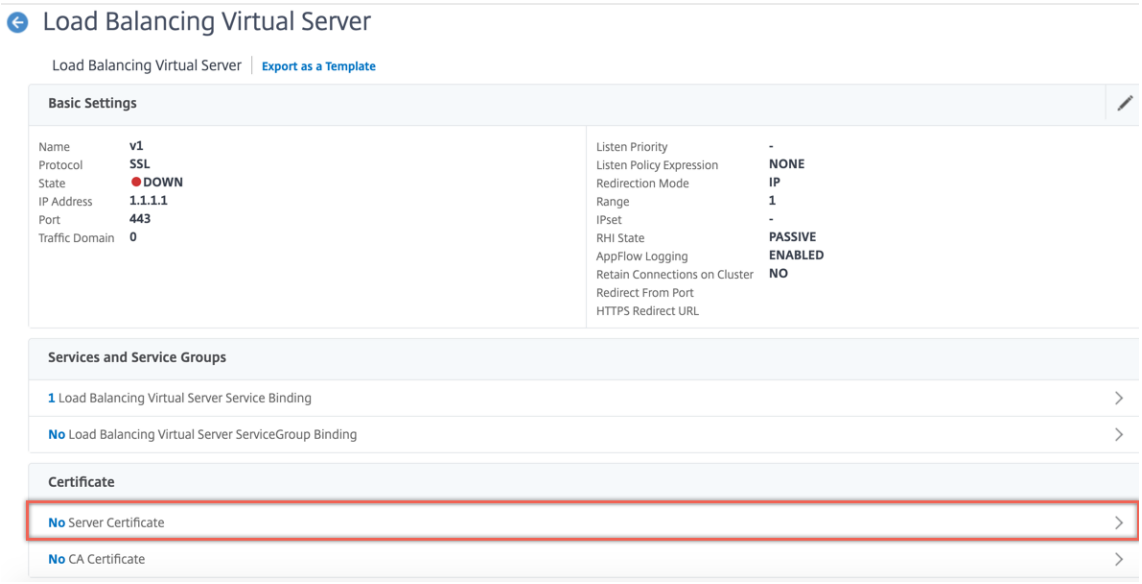
```
unbind ssl vserver <vServerName> -certkeyName <string>
<!--NeedCopy-->
```

Beispiel:

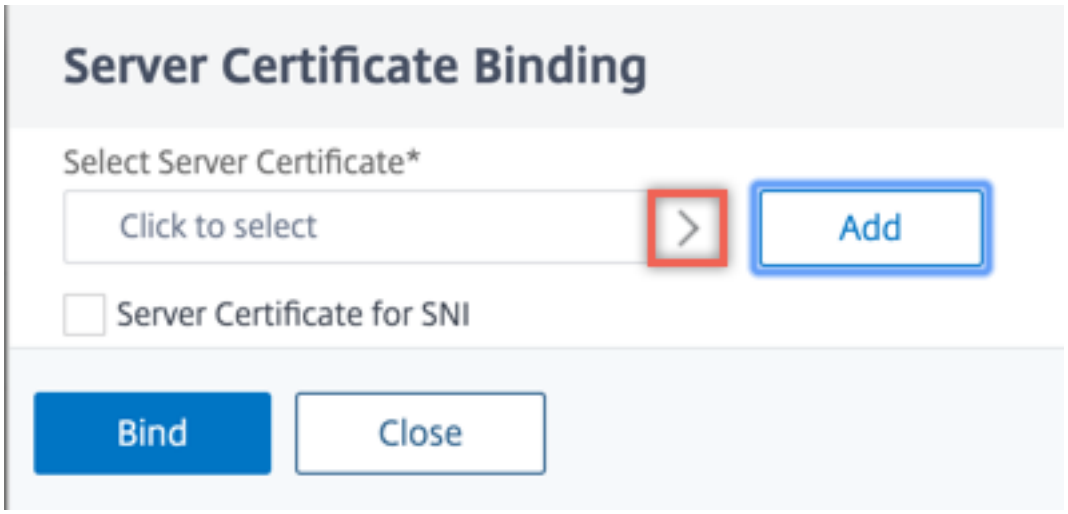
```
unbind ssl vserver vssl -certkeyName sslckey
<!--NeedCopy-->
```

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

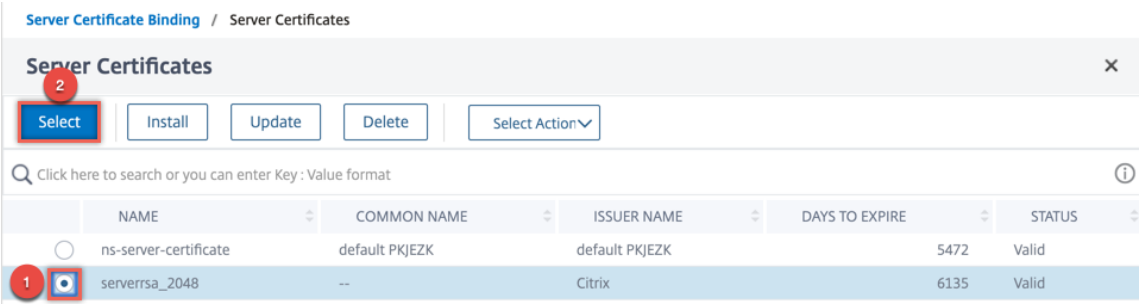
1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server** und öffnen Sie einen virtuellen SSL-Server. Klicken Sie in den Abschnitt **Zertifikat** .



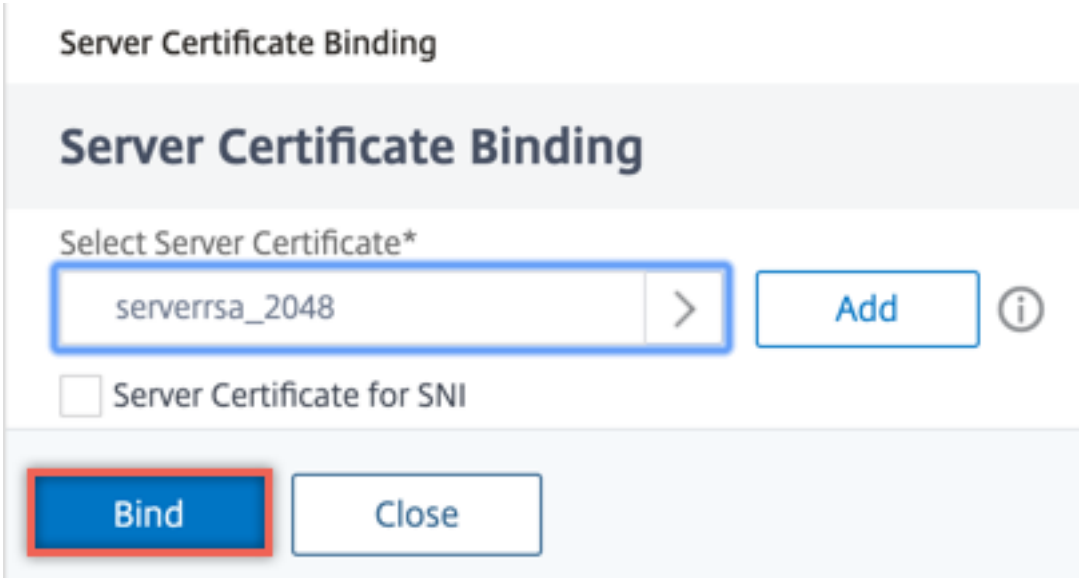
2. Klicken Sie auf den Pfeil, um das Zertifikatsschlüsselpaar auszuwählen.



3. Wählen Sie das Zertifikatsschlüsselpaar aus der Liste aus.



4. Binden Sie das Zertifikatsschlüsselpaar an den virtuellen Server. Um ein Serverzertifikat als SNI-Zertifikat hinzuzufügen, wählen Sie **Serverzertifikat für SNI**aus.



Virtuelle SSL-Serverparameter

Stellen Sie die erweiterte SSL-Konfiguration für einen virtuellen SSL-Server ein. Sie können viele dieser Parameter auch in einem SSL-Profil festlegen. Informationen zu den Parametern, die in einem SSL-Profil festgelegt werden können, finden Sie unter SSL-Profilparameter.

Festlegen von virtuellen SSL-Serverparametern mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl vserver <vServerName>@ [-clearTextPort <port>] [-dh ( ENABLED |
    DISABLED ) -dhFile <string>] [-dhCount <positive_integer>][-
    dhKeyExpSizeLimit ( ENABLED | DISABLED )] [-eRSA ( ENABLED |
    DISABLED) [-eRSACount <positive_integer>]] [-sessReuse ( ENABLED |
    DISABLED )[-sessTimeout <positive_integer>]] [-cipherRedirect (
    ENABLED | DISABLED ) [-cipherURL <URL>]] [-sslv2Redirect ( ENABLED |
     DISABLED )[-sslv2URL <URL>]] [-clientAuth ( ENABLED | DISABLED ) [-
    clientCert ( Mandatory | Optional )]] [-sslRedirect ( ENABLED |
    DISABLED )][-redirectPortRewrite ( ENABLED | DISABLED )] [-ssl2 (
    ENABLED | DISABLED )] [-ssl3 ( ENABLED | DISABLED )] [-tls1 (
    ENABLED | DISABLED )] [-tls11 ( ENABLED | DISABLED )] [-tls12 (
    ENABLED | DISABLED )][-tls13 ( ENABLED | DISABLED )] [-SNIEnable (
    ENABLED | DISABLED )][-ocspStapling ( ENABLED | DISABLED )] [-
    pushEncTrigger <pushEncTrigger>] [-sendCloseNotify ( YES | NO )] [-
    dtlsProfileName <string>] [-sslProfile <string>] [-HSTS ( ENABLED |
    DISABLED )][-maxage <positive_integer>] [-IncludeSubdomains ( YES |
```



```
    NO )][-strictSigDigestCheck ( ENABLED | DISABLED )] [-
    zeroRttEarlyData (ENABLED | DISABLED )] [-
    tls13SessionTicketsPerAuthContext <positive_integer>] [-
    dheKeyExchangeWithPsk ( YES | NO )]
<!--NeedCopy-->
```

Diffie-Hellman-Parameter (DH)

Um Verschlüsselungen auf der Appliance zu verwenden, die einen DH-Schlüsselaustausch zum Einrichten der SSL-Transaktion erfordern, aktivieren Sie den DH-Schlüsselaustausch auf der Appliance. Konfigurieren Sie andere Einstellungen basierend auf Ihrem Netzwerk.

Um die Verschlüsselungen aufzulisten, für die DH-Parameter über die CLI festgelegt werden müssen, geben Sie Folgendes ein: sh cipher DH.

Um die Chiffre aufzulisten, für die DH-Parameter mithilfe des Konfigurationsdienstprogramms festgelegt werden müssen, navigieren Sie zu **Verkehrsverwaltung > SSL > Verschlüsselungsgruppen**, und doppelklicken Sie auf **DH**.

Weitere Informationen zur Aktivierung des DH-Schlüsselaustauschs finden Sie unter Generieren eines Diffie-Hellman-Schlüssels (DH).

Konfigurieren von DH-Parametern mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um DH-Parameter zu konfigurieren und die Konfiguration zu überprüfen:

```
-  `set ssl vserver <vserverName> -dh <Option> -dhCount <
   RefreshCountValue> -filepath <string>
-  show ssl vserver <vServerName>`
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver vs-server -dh ENABLED  -dhFile /nsconfig/ssl/ns-server.
   cert -dhCount 1000
Done

show ssl vserver vs-server

            Advanced SSL configuration for VServer vs-server:
```



```
7               DH: ENABLED
8               Ephemeral RSA: ENABLED          Refresh Count: 1000
9               Session Reuse: ENABLED          Timeout: 120 seconds
10              Cipher Redirect: DISABLED
11              SSLv2 Redirect: DISABLED
12              ClearText Port: 0
13              Client Auth: DISABLED
14              SSL Redirect: DISABLED
15              Non FIPS Ciphers: DISABLED
16              SNI: DISABLED
17              OCSP Stapling: DISABLED
18              HSTS: DISABLED
19              HSTS IncludeSubDomains: NO
20              HSTS Max-Age: 0
21              SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2:
                    ENABLED  TLSv1.2: ENABLED
22
23      1)      Cipher Name: DEFAULT
24              Description: Predefined Cipher Alias
25  Done
26  <!--NeedCopy-->
```

Konfigurieren von DH-Parametern über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie im Abschnitt **SSL-Parameter** die Option **DH Param aktivieren**aus, und geben Sie einen Aktualisierungszähler und einen Dateipfad an.

Vergängliches RSA

Mit kurzlebigen RSA können Exportclients mit dem sicheren Server kommunizieren, auch wenn das Serverzertifikat keine Exportclients unterstützt (1024-Bit-Zertifikat). Wenn Sie verhindern möchten, dass Exportclients auf das sichere Webobjekt oder die sichere Ressource zugreifen, müssen Sie den kurzlebigen RSA-Schlüsselaustausch deaktivieren.

Standardmäßig ist diese Funktion auf der Citrix ADC-Appliance aktiviert, wobei der Aktualisierungszähler auf Null gesetzt ist (unendliche Verwendung).

Hinweis:

Der kurzlebige RSA-Schlüssel wird automatisch generiert, wenn Sie eine Exportverschlüsselung an einen SSL- oder TCP-basierten virtuellen SSL-Server oder -Dienst binden. Wenn Sie die Exportverschlüsselung entfernen, wird der eRSA-Schlüssel nicht gelöscht. Sie wird später wiederverwendet,

wenn eine andere Exportverschlüsselung an einen virtuellen SSL- oder TCP-basierten SSL-Server oder -Dienst gebunden ist. Der eRSA-Schlüssel wird beim Neustart des Systems gelöscht.

Konfigurieren Sie kurzlebigen RSA über die CLI

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

```
set ssl vserver <vServerName> -eRSA (enabled | disabled) -eRSACount <
   positive_integer>
show ssl vserver <vServerName>
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver vs-server -eRSA ENABLED -eRSACount 1000
 Done

show ssl vserver vs-server

        Advanced SSL configuration for VServer vs-server:
        DH: DISABLED
        Ephemeral RSA: ENABLED          Refresh Count: 1000
        Session Reuse: ENABLED          Timeout: 120 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SNI: DISABLED
        OCSP Stapling: DISABLED
        HSTS: DISABLED
        HSTS IncludeSubDomains: NO
        HSTS Max-Age: 0
        SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2:
           ENABLED  TLSv1.2: ENABLED

1)      Cipher Name: DEFAULT
        Description: Predefined Cipher Alias
 Done
<!--NeedCopy-->
```


Konfigurieren Sie kurzlebigen RSA über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie im Abschnitt **SSL-Parameter** die Option **Ephemere RSA aktivieren**aus, und geben Sie einen Aktualisierungszähler an.

Wiederverwendung der Sitzung

Für SSL-Transaktionen erfordert das Einrichten des ersten SSL-Handshakes CPU-intensive Verschlüsselungsvorgänge mit öffentlichen Schlüsseln. Die meisten Handshake-Vorgänge sind mit dem Austausch des SSL-Sitzungsschlüssels (Clientschlüsselaustauschnachricht) verbunden. Wenn eine Clientsitzung für einige Zeit im Leerlauf ist und dann wieder aufgenommen wird, wird der SSL-Handshake in der Regel erneut durchgeführt. Wenn die Sitzungswiederverwendung aktiviert ist, wird der Austausch von Sitzungsschlüsseln für vom Client empfangene Anfragen zur Sitzungswiederaufnahme vermieden.

Die Wiederverwendung von Sitzungen ist auf der Citrix ADC-Appliance standardmäßig aktiviert. Durch die Aktivierung dieser Funktion wird die Serverlast reduziert, die Reaktionszeit verbessert und die Anzahl der SSL-Transaktionen pro Sekunde (TPS) erhöht, die der Server unterstützen kann.

Konfigurieren der Wiederverwendung von Sitzungen über die CLI

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

```
set ssl vserver <vServerName> -sessReuse ( ENABLED | DISABLED ) -
   sessTimeout <positive_integer>
show ssl vserver <vServerName>
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver vs-ssl -sessreuse enabled -sesstimeout 600
 Done

show ssl vserver vs-ssl

```



```
6          Advanced SSL configuration for VServer vs-ssl:
7          DH: DISABLED
8          Ephemeral RSA: ENABLED          Refresh Count: 1000
9          Session Reuse: ENABLED          Timeout: 600 seconds
10         Cipher Redirect: DISABLED
11         SSLv2 Redirect: DISABLED
12         ClearText Port: 0
13         Client Auth: DISABLED
14         SSL Redirect: DISABLED
15         Non FIPS Ciphers: DISABLED
16         SNI: DISABLED
17         OCSP Stapling: DISABLED
18         HSTS: DISABLED
19         HSTS IncludeSubDomains: NO
20         HSTS Max-Age: 0
21         SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2:
               ENABLED  TLSv1.2: ENABLED
22
23 1)      CertKey Name: Auth-Cert-1       Server Certificate
24
25 1)      Cipher Name: DEFAULT
26         Description: Predefined Cipher Alias
27  Done
28 <!--NeedCopy-->
```

Konfigurieren der Wiederverwendung von Sitzungen über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie im Abschnitt **SSL-Parameter** die Option **Sitzungswiederverwendung aktivieren**aus, und geben Sie eine Zeit an, zu der die Sitzung aktiv bleiben soll.

SSL-Protokolleinstellungen

Die Citrix ADC-Appliance unterstützt die Protokolle SSLv3, TLSv1, TLSv1.1 und TLSv1.2. Jedes dieser Protokolle kann auf der Appliance festgelegt werden, wie es für Ihre Bereitstellung und die Art der Clients erforderlich ist, die eine Verbindung zur Appliance herstellen.

Die TLS-Protokollversionen 1.0, 1.1 und 1.2 sind sicherer als ältere Versionen des TLS/SSL-Protokolls. Um jedoch Legacy-Systeme zu unterstützen, behalten viele TLS-Implementierungen die Abwärtskompatibilität mit dem SSLv3-Protokoll bei. In einem SSL-Handshake wird die höchste Protokollversion verwendet, die dem Client und dem auf der Citrix ADC-Appliance konfigurierten virtuellen SSL-Server gemeinsam ist.

Beim ersten Handshake-Versuch bietet ein TLS-Client die höchste Protokollversion, die er unterstützt. Wenn der Handshake fehlschlägt, bietet der Client eine niedrigere Protokollversion an. Wenn beispielsweise ein Handshake mit TLS-Version 1.1 nicht erfolgreich ist, versucht der Client, neu zu verhandeln, indem er das TLSv1.0-Protokoll anbietet. Wenn dieser Versuch nicht erfolgreich ist, versucht der Client erneut mit dem SSLv3-Protokoll. Ein “Mann in der Mitte” (MITM) -Angreifer kann den anfänglichen Handshake brechen und eine Neuverhandlung mit dem SSLv3-Protokoll auslösen und dann eine Schwachstelle in SSLv3 auszunutzen. Um solche Angriffe zu mildern, können Sie SSLv3 deaktivieren oder Neuverhandlungen mit einem heruntergestuften Protokoll nicht zulassen. Dieser Ansatz ist jedoch möglicherweise nicht praktikabel, wenn Ihre Bereitstellung Legacy-Systeme umfasst. Eine Alternative besteht darin, einen Signalisierungs-Chiffre-Suite-Wert (TLS_FALLBACK_SCSV) in der Clientanforderung zu erkennen.

Ein TLS_FALLBACK_SCSV-Wert in einer Client-Hello-Nachricht zeigt dem virtuellen Server an, dass der Client zuvor versucht hat, eine Verbindung mit einer höheren Protokollversion herzustellen, und dass die aktuelle Anforderung ein Fallback ist. Wenn der virtuelle Server diesen Wert erkennt und eine höhere Version als die vom Client angegebene unterstützt, lehnt er die Verbindung mit einer schwerwiegenden Warnung ab. Der Handshake ist erfolgreich, wenn eine der folgenden Bedingungen erfüllt ist:

- Der TLS_FALLBACK_SCSV-Wert ist nicht in der Hello-Nachricht des Clients enthalten.
- Die Protokollversion im Client Hello ist die höchste Protokollversion, die vom virtuellen Server unterstützt wird.

Konfigurieren der SSL-Protokollunterstützung über die CLI

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

```
set ssl vserver <vServerName> -ssl2 ( ENABLED | DISABLED ) -ssl3 (
    ENABLED | DISABLED ) -tls1 ( ENABLED | DISABLED ) -tls11 ( ENABLED |
     DISABLED ) -tls12 ( ENABLED | DISABLED )

show ssl vserver <vServerName>
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver vs-ssl -tls11 ENABLED -tls12 ENABLED
Done

```



```
sh ssl vs vs-ssl

        Advanced SSL configuration for VServer vs-ssl:
            DH: DISABLED
            Ephemeral RSA: ENABLED                              Refresh
               Count: 0
            Session Reuse: ENABLED                                Timeout
               : 120 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Client Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            SSLv2: DISABLED        SSLv3: ENABLED    TLSv1.0: ENABLED
               TLSv1.1: ENABLED  TLSv1.2: ENABLED
            Push Encryption Trigger: Always
            Send Close-Notify: YES
            1 bound certificate:

    1)      CertKey Name: mycert  Server Certificate
            1 configured cipher:

    1)      Cipher Name: DEFAULT
            Description: Predefined Cipher Alias

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

Konfigurieren der SSL-Protokollunterstützung über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie im Abschnitt **SSL-Parameter** ein zu aktivierendes Protokoll aus.

nah-benachrichtigen

Eine Close-Notify ist eine sichere Nachricht, die das Ende der SSL-Datenübertragung anzeigt. Eine Einstellung für eine nahe Benachrichtigung ist auf globaler Ebene erforderlich. Diese Einstellung gilt für alle virtuellen Server, Dienste und Dienstgruppen. Informationen zur globalen Einstellung finden Sie im Abschnitt “Globale SSL-Parameter” weiter unten auf dieser Seite.

Zusätzlich zur globalen Einstellung können Sie den Close-Notify-Parameter auf der Ebene des virtuellen Servers, des Dienstes oder der Dienstgruppe festlegen. Sie haben daher die Flexibilität, den Parameter für eine Entität festzulegen und ihn für eine andere Entität aufzuheben. Stellen Sie jedoch sicher, dass Sie diesen Parameter auf globaler Ebene festlegen. Andernfalls gilt die Einstellung auf Entitätsebene nicht.

Konfigurieren von Close-Notify auf Entitätsebene über die CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um die Funktion zum Schließen der Benachrichtigung zu konfigurieren und die Konfiguration zu überprüfen:

1. Um auf der Ebene des virtuellen Servers zu konfigurieren, geben Sie Folgendes ein:

```
set ssl vserver <vServerName> -sendCloseNotify ( YES | NO )
show ssl vserver <vServerName>
<!--NeedCopy-->
```

1. Um auf Service-Ebene zu konfigurieren, geben Sie Folgendes ein:

```
set ssl service <serviceName> -sendCloseNotify ( YES | NO )
show ssl service <serviceName>
<!--NeedCopy-->
```

1. Um auf der Dienstgruppenebene zu konfigurieren, geben Sie Folgendes ein:

```
set ssl serviceGroup <serviceGroupName> -sendCloseNotify ( YES | NO )
show ssl serviceGroup <serviceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver sslvsvr -sendCloseNotify YES

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


Konfigurieren Sie die Funktion zum Schließen von Benachrichtigungen auf Entitätsebene über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie im Abschnitt **SSL-Parameter** die Option **Close-Notify senden**aus.

Globale SSL-Parameter

Die erweiterte Anpassung Ihrer SSL-Konfiguration behebt bestimmte Probleme. Sie können den `set ssl parameter` Befehl oder das Konfigurationsdienstprogramm verwenden, um Folgendes anzugeben:

- Für SSL-Transaktionen zu verwendende Quantengröße.
- CRL-Speichergröße.
- OCSP-Cachegröße.
- Verweigern Sie die SSL-Neuverhandlung.
- Setzen Sie das PUSH-Flag für entschlüsselte, verschlüsselte oder alle Datensätze.
- Löschen Sie Anfragen, wenn der Client den Handshake für eine Domäne initiiert und eine HTTP-Anforderung für eine andere Domäne sendet.
- Stellen Sie die Zeit ein, nach der die Verschlüsselung ausgelöst wird.
  Hinweis: Die von Ihnen angegebene Zeit gilt nur, wenn Sie den `set ssl vserver` Befehl oder das Konfigurationsdienstprogramm verwenden, um die timer-basierte Verschlüsselung festzulegen.
- NDCPP-Konformitätszertifikatprüfung — Gilt, wenn die Appliance als Client fungiert (Back-End-Verbindung). Ignorieren Sie bei der Zertifikatsüberprüfung den allgemeinen Namen, wenn SAN im SSL-Zertifikat vorhanden ist.
- Ermöglichen Sie einen heterogenen Cluster von Cavium-Chip-basierten Appliances wie MPX 14000 und Intel Coleto-Chip-basierten Appliances wie MPX 15000 Appliances mit einer anderen Anzahl von Paket-Engines. (Unterstützung in Release 13.0 Build 47.x hinzugefügt).
- Aktivieren Sie sichere Neuverhandlungen am Back-End (Unterstützung aus Release 1.0 Build 58.x hinzugefügt).
- Adaptive SSL-Datenverkehrskontrolle (Unterstützung in Release 13.0 Build 58.x hinzugefügt).

Konfigurieren globaler SSL-Parameter mit der CLI

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


```
set ssl parameter [-quantumSize <quantumSize>] [-crlMemorySizeMB <
    positive_integer>] [-strictCAChecks (YES | NO)] [-sslTriggerTimeout
    <positive_integer>] [-sendCloseNotify (YES | NO)] [-
    encryptTriggerPktCount <positive_integer>] [-denySSLReneg <
    denySSLReneg>] [-insertionEncoding (Unicode|UTF-8)] [-ocspCacheSize
    <positive_integer>][- pushFlag <positive_integer>] [-
    dropReqWithNoHostHeader (YES | NO)] [-pushEncTriggerTimeout <
    positive_integer>] [-ndcppComplianceCertCheck ( YES | NO)] [-
    heterogeneousSSLHW (ENABLED | DISABLED )]
show ssl parameter
<!--NeedCopy-->
```

Beispiel:

```
set ssl parameter -quantumSize 8 -crlMemorySizeMB 256 -strictCAChecks
    no -ssltriggerTimeout 100 -sendClosenotify no -
    encryptTriggerPktCount 45 -denySSLReneg NONSECURE -insertionEncoding
     unicode -ocspCacheSize 10 -pushFlag 3 -dropReqWithNoHostHeader YES
     -pushEncTriggerTimeout 100 ms -ndcppComplianceCertCheck YES
Done

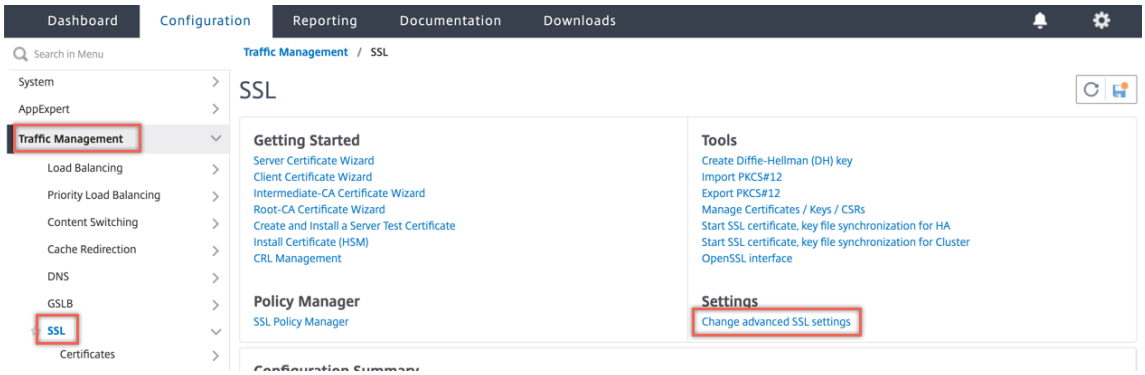
show ssl parameter
Advanced SSL Parameters
-----------------------
    SSL quantum size                                    : 8 KB
    Max CRL memory size                                 : 256 MB
    Strict CA checks                                    : NO
    Encryption trigger timeout                          : 100 ms
    Send Close-Notify                                   : NO
    Encryption trigger packet count                     : 45
    Deny SSL Renegotiation                              : NONSECURE
    Subject/Issuer Name Insertion Format                : Unicode
    OCSP cache size                                     : 10 MB
    Push flag                                           : 0x3 (On
        every decrypted and encrypted record)
    Strict Host Header check for SNI enabled SSL sessions : YES
    PUSH encryption trigger timeout                     : 100 ms
    Crypto Device Disable Limit                         : 0
    Global undef action for control policies            : CLIENTAUTH
    Global undef action for data policies               : NOOP
    Default profile                                     : DISABLED
    SSL Insert Space in Certificate Header              : YES
    Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors    : NO
```



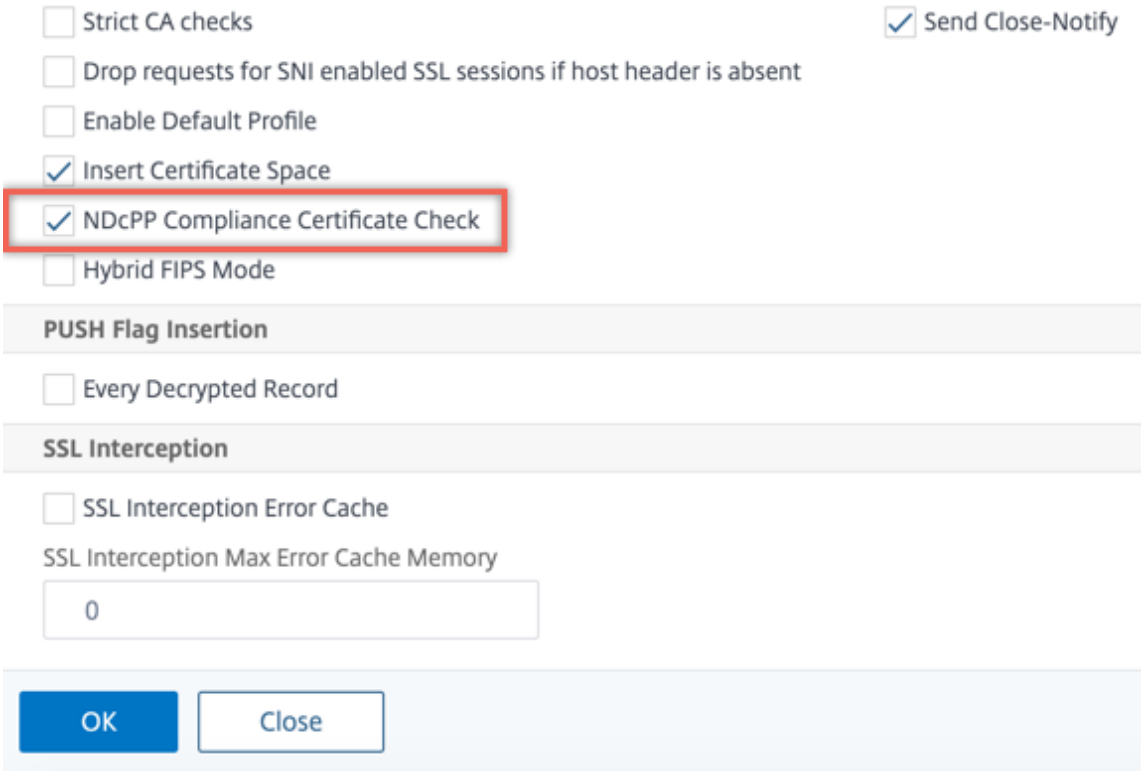
```
25      Disable TLS 1.1/1.2 for dynamic and VPN services       : NO
26      Software Crypto acceleration CPU Threshold             : 0
27      Hybrid FIPS Mode                                       : DISABLED
28      Signature and Hash Algorithms supported by TLS1.2      : ALL
29      SSL Interception Error Learning and Caching            : DISABLED
30      SSL Interception Maximum Error Cache Memory            : 0 Bytes
31      NDCPP Compliance Certificate Check                     : YES
32      Heterogeneous SSL HW (Cavium and Intel Based)          : ENABLED
33   Done
34  <!--NeedCopy-->
```

Konfigurieren der NdCPP-Konformitätszertifikatprüfung über die GUI

1. Navigieren Sie zu **Traffic Management > SSL** und wählen Sie in der Gruppe **Einstellungen** die Option **Erweiterte SSL-Einstellungen ändern**aus.



2. Wählen Sie **NDCPP-Konformitätszertifikatprüfung**aus. Klicken Sie auf **OK**.



Unterstützung für sichere Neuverhandlungen am Backend einer Citrix ADC-Appliance

Hinweis: Diese Funktion wird in Version 13.0 Build 58.x und höher unterstützt. In früheren Versionen und Builds wurde nur unsichere Neuverhandlungen im Backend unterstützt.

Die Funktion wird auf den folgenden Plattformen unterstützt:
• VPX
• MPX-Plattformen mit N2- oder N3-Chips
• Intel Coleto SSL-Chip-basierte Plattformen

Die Funktion wird auf der FIPS-Plattform noch nicht unterstützt.

Sichere Neuverhandlungen werden standardmäßig im Backend einer ADC-Appliance verweigert. Das heißt, der denySSLReneg Parameter ist auf ALL (Standard) festgelegt.

Um eine sichere Neuverhandlung im Backend zu ermöglichen, wählen Sie eine der folgenden Einstellungen für den denySSLReneg Parameter aus:

- NEIN
- FRONTEND_CLIENT
- FRONTEND_CLIENTSERVER
- NONSECURE

Ermöglichen Sie sichere Neuverhandlungen über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl parameter -denySSLReneg <denySSLReneg>
```

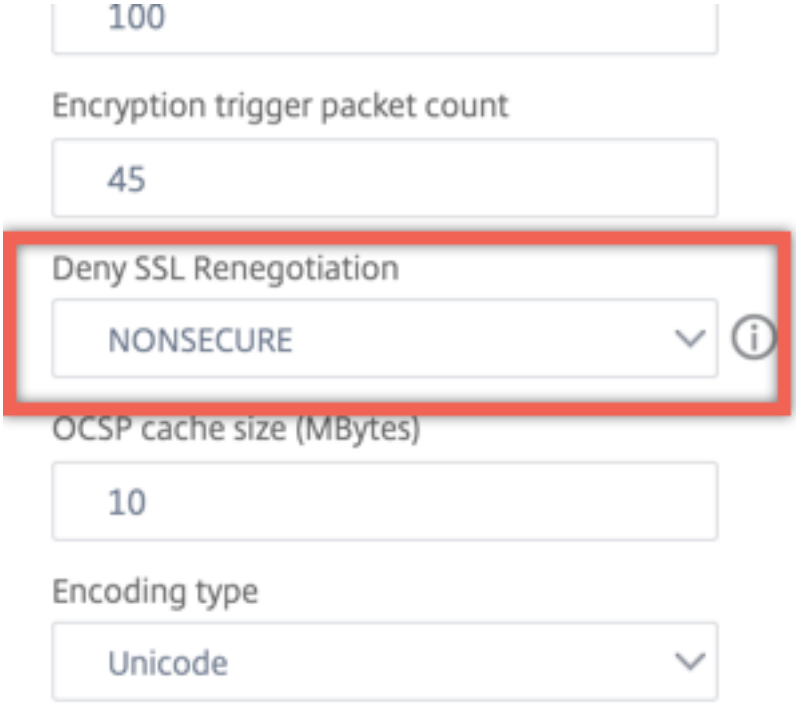
Beispiel:

```
set ssl parameter -denySSLReneg NONSECURE
 Done

sh ssl parameter
Advanced SSL Parameters
-----------------------
    SSL quantum size                                  : 8 KB
    Max CRL memory size                               : 256 MB
    Strict CA checks                                  : NO
    Encryption trigger timeout                        : 100 ms
    Send Close-Notify                                 : YES
    Encryption trigger packet count                   : 45
    Deny SSL Renegotiation                            : NONSECURE
    Subject/Issuer Name Insertion Format              : Unicode
    OCSP cache size                                   : 10 MB
    Push flag                                         : 0x0 (Auto)
    Strict Host Header check for SNI enabled SSL sessions : NO
    Match HTTP Host header with SNI                   : CERT
    PUSH encryption trigger timeout                   : 1 ms
    Crypto Device Disable Limit                       : 0
    Global undef action for control policies          : CLIENTAUTH
    Global undef action for data policies             : NOOP
    Default profile                                   : ENABLED
    SSL Insert Space in Certificate Header            : YES
    Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors    : NO
    Disable TLS 1.1/1.2 for dynamic and VPN services      : NO
    Software Crypto acceleration CPU Threshold        : 0
    Hybrid FIPS Mode                                  : DISABLED
    Signature and Hash Algorithms supported by TLS1.2     : ALL
    SSL Interception Error Learning and Caching       : DISABLED
    SSL Interception Maximum Error Cache Memory       : 0 Bytes
    NDCPP Compliance Certificate Check                : NO
    Heterogeneous SSL HW (Cavium and Intel Based)         : DISABLED
    Crypto Operation Queue Limit                      : 150%
 Done
<!--NeedCopy-->
```


Ermöglichen Sie sichere Neuverhandlungen mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL > Erweiterte SSL-Einstellungen ändern**.
2. Legen Sie “ **SSL-Neuverhandlung verweigern** “ auf einen anderen Wert als ALL fest.



Adaptive SSL-Verkehrssteuerung

Hinweis: Diese Funktion wird in Version 13.0 Build 58.x und höher unterstützt.

Wenn viel Verkehr auf der Appliance empfangen wird und die Krypto-Beschleunigungskapazität voll ist, beginnt die Appliance, Verbindungen in die Warteschlange zu stellen, um sie später zu verarbeiten. Derzeit ist die Größe dieser Warteschlange auf 64 K festgelegt und die Appliance beginnt, Verbindungen zu trennen, wenn dieser Wert überschritten wird.

Ab Version 13.0 Build 58.x kann der Benutzer einen Wert konfigurieren, der einen Prozentsatz der tatsächlichen Kapazität darstellt. Mit dieser Erweiterung trennt die Appliance neue Verbindungen, wenn die Anzahl der Elemente in der Warteschlange den Grenzwert überschreitet, der adaptiv und dynamisch berechnet wird. Dieser Ansatz steuert eingehende SSL-Verbindungen und verhindert übermäßigen Ressourcenverbrauch und andere Ausfälle, wie z. B. einen Ausfall der Lastenausgleichsüberwachung oder eine langsame Reaktion auf sichere Anwendungen auf der Appliance.

Wenn die Warteschlange leer ist, kann die Appliance weiterhin Verbindungen annehmen. Wenn die Warteschlange nicht leer ist, hat das Kryptosystem seine Kapazität erreicht und die Appliance beginnt, Verbindungen in die Warteschlange zu stellen.

Das Limit wird basierend auf folgenden Kriterien berechnet:

- Die tatsächliche Kapazität des Geräts.
- Vom Benutzer konfigurierter Wert als Prozentsatz der tatsächlichen Kapazität. Der Standardwert ist auf 150% festgelegt.

Wenn beispielsweise die tatsächliche Kapazität einer Appliance zu einem bestimmten Zeitpunkt 1000 Operationen/Sekunde beträgt und der Standardprozentsatz konfiguriert ist, beträgt der Grenzwert, nach dem die Appliance Verbindungen trennt, 1500 (150% von 1000).

So konfigurieren Sie das Limit für die Operationswarteschlange über die CLI

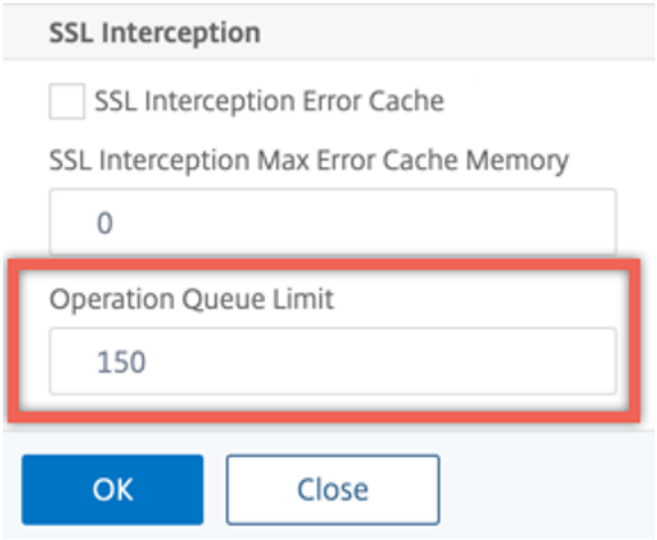
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl parameter -operationQueueLimit <positive_integer>
```

Limit der Warteschlange für Vorgänge - Begrenzung des Prozentsatzes der Kapazität der Warteschlange für Kryptovorgänge, ab der neue SSL-Verbindungen erst akzeptiert werden, wenn die Warteschlange reduziert wurde. Standardwert: 150. Mindestwert: 0. Maximaler Wert: 10000.

So konfigurieren Sie das Limit der Operationswarteschlange über die GUI

1. Navigieren Sie zu **Traffic Management > SSL**.
2. Klicken Sie in den **Einstellungen**auf **Erweiterte SSL-Einstellungen ändern**.
3. Geben Sie einen Wert in **Warteschlangenlimit für Vorgänge**ein. Die Standardeinstellung ist 150.
4. Klicken Sie auf **OK**.



Heterogene Clusterbereitstellungen

Ab Version 13.0 Build 47.x können Sie eine heterogene Clusterbereitstellung von Citrix ADC MPX-Appliances mit einer anderen Anzahl von Paket-Engines erstellen, indem Sie den SSL-Parameter "Heterogenes SSL HW" auf ENABLED setzen. Um beispielsweise einen Cluster von Cavium-Chip-basierten Appliances (MPX 14000 oder ähnlich) und Intel Coleto-Chip-basierten Appliances (MPX 15000 oder ähnlich) zu bilden, aktivieren Sie den SSL-Parameter "Heterogenes SSL HW. " Um einen Cluster von Plattformen mit demselben Chip zu bilden, behalten Sie den Standardwert (DISABLED) für diesen Parameter bei.

> **Hinweise:**
>
> Die folgenden Funktionen werden in einem heterogenen Cluster nicht unterstützt:
>
> - VPX-Instanzen werden auf Citrix ADC SDX-Appliances gehostet.
> - SSLv3-Protokoll auf SSL-Entitäten wie virtuellen Servern, Diensten, Dienstgruppen und internen Diensten.
> - CPU-Schwellenwert für Software-Krypto-Beschleunigung (Verwendung von Hardware und Software zur Verbesserung der Verschlüsselungsleistung von ECDSA und ECDHE).

Weitere Informationen zu den Plattformen, die in einem heterogenen Cluster unterstützt werden, finden Sie unter https://docs.citrix.com/en-us/citrix-adc/13/clustering/support-for-heterogeneous-cluster.html.

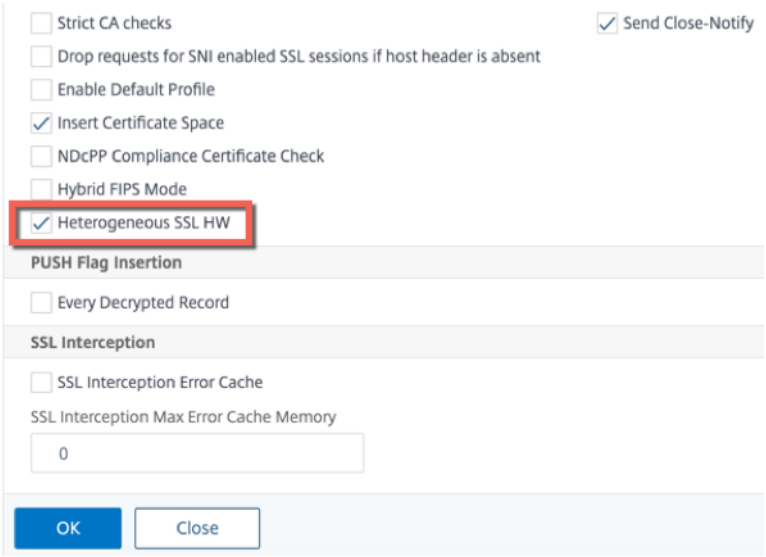
Aktivieren eines heterogenen Clusters mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl parameter -heterogeneousSSLHW ENABLED
```

Ermöglichen eines heterogenen Clusters über die GUI

1. Navigieren Sie zu **Traffic Management > SSL** und wählen Sie in der Gruppe **Einstellungen** die Option **Erweiterte SSL-Einstellungen ändern**aus.
2. Wählen Sie **Heterogene SSL HW**. Klicken Sie auf **OK**.



Push-Flag basierter Verschlüsselungsauslösemechanismus

Mit dem Verschlüsselungsauslösemechanismus, der auf dem PSH-TCP-Flag basiert, können Sie jetzt Folgendes tun:

- Führen Sie aufeinanderfolgende Pakete, in denen das PSH-Flag gesetzt ist, zu einem einzigen SSL-Datensatz zusammen oder ignorieren Sie das PSH-Flag.
- Führen Sie eine timerbasierte Verschlüsselung durch, bei der der Timeoutwert mithilfe des `set ssl parameter -pushEncTriggerTimeout <positive_integer>` Befehls global festgelegt wird.

Konfigurieren der PUSH-Flag-basierten Verschlüsselung über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Push-Flag-basierte Verschlüsselung zu konfigurieren und die Konfiguration zu überprüfen:

```
set ssl vserver <vServerName> [-pushEncTrigger <pushEncTrigger>]

show ssl vserver
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver vserver1 -pushEncTrigger always

```



```
Done

sh ssl vserver vserver1

            Advanced SSL configuration for VServer vserver1:
            DH: DISABLED
            DH Private-Key Exponent Size Limit: DISABLED    Ephemeral
                RSA: ENABLED

                Refresh Count: 0
            Session Reuse: ENABLED          Timeout: 120 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            ClearText Port: 0
            Client Auth: DISABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SNI: DISABLED
            OCSP Stapling: DISABLED
            HSTS: DISABLED
            HSTS IncludeSubDomains: NO
            HSTS Max-Age: 0
            SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1:
                ENABLED  TLSv1.2: ENABLED  TLSv1.3: DISABLED
            Push Encryption Trigger: Always
            Send Close-Notify: YES
            Strict Sig-Digest Check: DISABLED
            Zero RTT Early Data: DISABLED
            DHE Key Exchange With PSK: NO
            Tickets Per Authentication Context: 1
            ECC Curve: P_256, P_384, P_224, P_521

    1)      Cipher Name: DEFAULT
            Description: Default cipher list with encryption strength
                >= 128bit
Done
<!--NeedCopy-->
```

Konfigurieren der Push-Flag-basierten Verschlüsselung über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server** und öffnen Sie einen virtuellen SSL-Server.
2. Wählen Sie im Abschnitt **SSL-Parameter** in der Liste **PUSH-Verschlüsselungsauslöser** einen Wert aus.

Unterstützung für den TLS1.2 Signatur-Hash-Algorithmus

Die Citrix ADC-Appliance ist vollständig TLS1.2-Signatur-Hash-Erweiterung kompatibel.

In einem SSL-Handshake sendet ein Client eine Liste unterstützter Signatur-Hash-Algorithmen. Der Client teilt dem Server mit der Erweiterung “signature_algorithmus” mit, welche Signatur-Hash-Algorithmus-Paare in den SSL-Handshake-Nachrichten (SKE und CCV) verwendet werden könnten. Das Feld “extension_data” dieser Erweiterung enthält einen Wert “supported_signature_algorithms” in der Client-Hello Nachricht. Der SSL-Handshake wird fortgesetzt, wenn der Server einen dieser Signatur-Hash-Algorithmen unterstützt. Wenn der Server keinen dieser Algorithmen unterstützt, wird die Verbindung getrennt.

Wenn der Server ein Clientzertifikat für die Clientauthentifizierung anfordert, enthält die Zertifikatsanforderungsnachricht einen Wert “supported_signature_algorithms”. Das Clientzertifikat wird basierend auf diesem Signatur-Hash-Algorithmus ausgewählt.

> **Hinweis:**
>
> Die Citrix ADC-Appliance fungiert als Server für einen Client und als Client für den Backend-Server.

Die Appliance unterstützt nur RSA-SHA1 und RSA-SHA256 im Front-End und RSA-MD5, RSA-SHA1 und RSA-SHA256 im Backend.

Die MPX/SDX/VPX-Appliance unterstützt die folgenden Signatur-Hash-Kombinationen. Wenn auf einer SDX-Appliance ein SSL-Chip einer VPX-Instanz zugewiesen ist, gilt die Verschlüsselungsunterstützung einer MPX-Appliance. Andernfalls gilt die normale Verschlüsselungsunterstützung einer VPX-Instanz.

- Auf einer VPX-Instanz und auf einer MPX/SDX-Appliance ohne N3-Chips:
  - RSA-MD5
  - RSA-SHA1
  - RSA-SHA224
  - RSA-SHA256
  - RSA-SHA384
  - RSA-SHA512
- Auf einer MPX/SDX-Einheit mit N3-Chips:
  - RSA-MD5
  - RSA-SHA1
  - RSA-SHA224
  - RSA-SHA256
  - RSA-SHA384
  - RSA-SHA512
  - ECDSA-SHA1
  - ECDSA-SHA224

- ECDSA-SHA256
- ECDSA-SHA384
- ECDSA-SHA512

Standardmäßig sind alle Signatur-Hash-Algorithmen aktiviert. Sie können jedoch nur einige Signatur-Hash-Algorithmen aktivieren, indem Sie den folgenden Befehl verwenden:

```
set ssl parameter -sigDigestType <sigDigestType>

Parameters

sigDigestType

Signature digest algorithms supported by the appliance. The platform
   determines the list of algorithms supported by default.

             On VPX: RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384
                  RSA-

             SHA512

             On MPX with N3 cards: RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-

             SHA256 RSA-SHA384 RSA-SHA512 ECDSA-SHA1 ECDSA-SHA224
                ECDSA-

             SHA256 ECDSA-SHA384 ECDSA-SHA512

             Other MPX Platforms: RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-
                SHA256 RSA-SHA384 RSA-

             SHA512.

    set ssl parameter -sigDigestType RSA-SHA224 RSA-SHA256 RSA-SHA384
       RSA-SHA512
<!--NeedCopy-->
```

Validierung des Peer-Zertifikats

Gemäß RFC 5246 muss das Peer-Zertifikat mit einem der Signatur-Hash-Algorithmen signiert werden, die in der Client-Hello-Erweiterung enthalten sind. Sie können den `strictSigDigestCheck` Parameter verwenden. Abhängig von der vom Client gesendeten Signatur-Hash-Liste gibt die Appliance

bei Aktivierung ein Zertifikat zurück `strictSigDigestCheck`, das von einem der Signatur-Hash-Algorithmen signiert ist, die in der Client-Hello-Erweiterung erwähnt werden. Wenn der Peer kein ordnungsgemäßes Zertifikat besitzt, wird die Verbindung getrennt. Wenn dieser Parameter deaktiviert ist, wird der Signatur-Hash nicht im Peer-Zertifikat geprüft.

Sie können eine strikte Signaturüberprüfung auf einem virtuellen SSL-Server und -Dienst konfigurieren. Wenn Sie diesen Parameter auf einem virtuellen SSL-Server aktivieren, muss das vom Server gesendete Serverzertifikat von einem der Signatur-Hash-Algorithmen signiert sein, die in der Client-Hello-Erweiterung aufgeführt sind. Wenn die Clientauthentifizierung aktiviert ist, muss das vom Server empfangene Clientzertifikat mit einem der Signatur-Hash-Algorithmen signiert werden, die in der vom Server gesendeten Zertifikatsanforderung aufgeführt sind.

Wenn Sie diesen Parameter in einem SSL-Dienst aktivieren, muss das vom Client empfangene Serverzertifikat von einem der Signatur-Hash-Algorithmen signiert sein, die in der Client-Hello-Erweiterung aufgeführt sind. Das Clientzertifikat muss mit einem der Signatur-Hash-Algorithmen signiert werden, die in der Zertifikatsanforderungsnachricht aufgeführt sind.

Wenn das Standardprofil aktiviert ist, können Sie es verwenden, um eine strikte Signaturüberprüfung auf einem virtuellen SSL-Server, einem SSL-Dienst und einem SSL-Profil zu konfigurieren.

Konfigurieren einer strengen Signaturüberprüfung auf einem virtuellen SSL-Server, Dienst oder Profil über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl vserver <vServerName> -strictSigDigestCheck ( ENABLED |
    DISABLED )

set ssl service <serviceName> -strictSigDigestCheck ( ENABLED |
    DISABLED )

set ssl profile <name>-strictSigDigestCheck ( ENABLED | DISABLED )

Parameters

strictSigDigestCheck

              Check whether peer entity certificate is signed using one
                  of the signature-hash algorithms supported by the
                 Citrix ADC appliance.

              Possible values: ENABLED, DISABLED

```



```
15                Default: DISABLED
16 <!--NeedCopy-->
```

Beispiel:

```
1 set ssl vserver v1 -strictSigDigestCheck Enabled
2 set ssl service s1 -strictSigDigestCheck Enabled
3 set ssl profile p1 -strictSigDigestCheck Enabled
4 <!--NeedCopy-->
```

> **Wichtig:**
>
> Wenn DH-, ECDHE- oder ECDSA-Verschlüsselungen auf der Appliance konfiguriert sind, muss die SKE-Nachricht mit einem der Signatur-Hashes signiert werden, die in der Clientliste gemeinsam sind, und der auf der Appliance konfigurierten Liste. Wenn kein gemeinsamer Signaturhash vorhanden ist, wird die Verbindung unterbrochen.

Unterstützung des TLSv1.3-Protokolls wie in RFC 8446 definiert

January 25, 2022

Die Citrix ADC VPX- und Citrix ADC MPX-Appliances unterstützen jetzt das in RFC 8446 angegebene TLSv1.3-Protokoll.

> **Hinweise:**
>
> - Ab Release 13.0 Build 71.x und höher wird die Hardwarebeschleunigung TLS1.3 auf den folgenden Plattformen unterstützt:
>   - MPX 5900
>   - MPX/SDX 8900
>   - MPX/SDX 15000
>   - MPX/SDX 15000-50G
>   - MPX/SDX 26000
>   - MPX/SDX 26000-50S
>   - MPX/SDX 26000-100G
>
>   - Nur-Software-Unterstützung für das TLSv1.3-Protokoll ist auf allen anderen Citrix ADC MPX- und SDX-Appliances mit Ausnahme von Citrix ADC FIPS-Appliances verfügbar.
> - TLSv1.3 wird nur mit dem erweiterten Profil unterstützt. Informationen zum Aktivieren des erweiterten Profils finden Sie unter Aktivieren des erweiterten Profils.

> • Um TLS1.3 zu verwenden, müssen Sie einen Client verwenden, der der RFC 8446-Spezifikation entspricht.

Unterstützte Citrix ADC-Funktionen

Die folgenden SSL-Funktionen werden unterstützt:

1. TLSv1.3-Verschlüsselungssammlungen:
   - TLS1.3-AES256-GCM-SHA384 (0x1302)
   - TLS1.3_CHACHA20_POLY1305_SHA256 (0x1303)
   - TLS1.3-AES128_GCM-SHA256 (0x1301)
2. ECC-Kurven für kurzlebigen Diffie-Hellman-Schlüsselaustausch:
   - P_256
   - P_384
   - P_521
3. Verkürzte Handshakes, wenn die ticket-basierte Sitzungswiederaufnahme aktiviert ist
4. 0-RTT frühe Anwendungsdaten
5. Optionale oder verbindliche zertifikatsbasierte Clientauthentifizierung mit Unterstützung für OCSP- und CRL-Validierung von Clientzertifikaten
6. Servernamenerweiterung: Auswahl des Serverzertifikats mithilfe von SNI
7. Aushandlung des Anwendungsprotokolls (ALPN) mithilfe der Erweiterung application_level_protocol_negot
8. OCSP-Heftung
9. Protokollnachrichten und AppFlow-Datensätze werden für TLSv1.3-Handshakes erstellt.
10. Optionale Protokollierung von TLS 1.3-Verkehrsgeheimnissen durch das `nstrace` Paketerfassungsprogramm.
11. Interoperabilität mit TLS-Clients, die RFC 8446 implementieren. Zum Beispiel Mozilla Firefox, Google Chrome und OpenSSL.

Unterstützte Browser

Die folgenden Browserversionen werden unterstützt und sind mit der Citrix ADC-Implementierung des TLS 1.3-Protokolls kompatibel:

- Google Chrome — Version 72.0.3626.121 (offizielles Build) (64-bisschen)
- Mozilla Firefox — 65.0.2 (64 bisschen)
- Opera - Version:58.0.3135.79

Konfiguration

TLSv1.3 ist in einem SSL-Profil standardmäßig deaktiviert.

Hinzufügen eines SSL-Profils mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ssl profile <tls13-profile-name>
<!--NeedCopy-->
```

Beispiel:

```
add ssl profile tls13profile

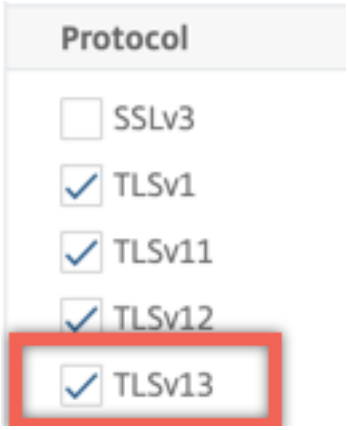
sh ssl profile tls13profile
1)  Name: tls13profile           (Front-End)
    SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1.1: ENABLED
       TLSv1.2: ENABLED  TLSv1.3: DISABLED
    Client Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:   NO
    Session Reuse: ENABLED                      Timeout: 120 seconds
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED   Ephemeral RSA:
       ENABLED                             Refresh Count: 0
    Deny SSL Renegotiation                              ALL
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:            1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions: NO
    Push flag:            0x0 (Auto)
    SSL quantum size:                           8 kB
```



```
28      Encryption trigger timeout           100 mS
29      Encryption trigger packet count:               45
30      Subject/Issuer Name Insertion Format: Unicode
31
32      SSL Interception: DISABLED
33      SSL Interception OCSP Check: ENABLED
34      SSL Interception End to End Renegotiation: ENABLED
35      SSL Interception Maximum Reuse Sessions per Server:  10
36      Session Ticket: DISABLED
37      HSTS: DISABLED
38      HSTS IncludeSubDomains: NO
39      HSTS Max-Age: 0
40
41      ECC Curve: P_256, P_384, P_224, P_521
42
43  1)  Cipher Name: DEFAULT Priority :1
44      Description: Predefined Cipher Alias
45  Done
46  <!--NeedCopy-->
```

Hinzufügen eines SSL-Profils mithilfe der GUI

1. Navigieren Sie zu **System > Profile**. Wählen Sie **SSL-Profile**.
2. Klicken Sie auf **Hinzufügen** und geben Sie einen Namen für das Profil an.
3. Wählen Sie **unter ProtokollTLSv13**aus.



4. Klicken Sie auf **OK**.

Binden Sie ein SSL-Profil mithilfe der CLI an einen virtuellen SSL-Server

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set ssl vserver <vServerName> -sslProfile <tls13-profile-name>
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver ssl-vs -sslProfile tls13profile
```

Binden Sie ein SSL-Profil mithilfe der GUI an einen virtuellen SSL-Server

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und wählen Sie einen virtuellen SSL-Server aus.
2. Klicken Sie **unter Erweiterte Einstellungen**auf **SSL-Profil**.
3. Wählen Sie das zuvor erstellte TLSv1.3-Profil aus.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Fertig**.

SSL-Profilparameter für das TLSv1.3-Protokoll

1. TLS1.3-Parameter in einem SSL-Profil aktivieren oder deaktivieren.

   tls13: Status der TLSv1.3-Protokollunterstützung für das SSL-Profil.

   Mögliche Werte: ENABLED, DISABLED

   Standardwert: DISABLED

   ```
   set ssl profile tls13profile -tls13 enable
   <!--NeedCopy-->
   ```

   ```
   set ssl profile tls13profile -tls13 disable
   <!--NeedCopy-->
   ```

2. Anzahl der ausgestellten Sitzungstickets festlegen.

   Tls13SessionTicketsPerAuthContext: Anzahl der Tickets, die der virtuelle SSL-Server ausgibt, wenn TLS1.3 ausgehandelt wird, die ticket-basierte Wiederaufnahme aktiviert ist und entweder (1) ein Handshake abgeschlossen ist oder (2) die Clientauthentifizierung nach dem Handshake abgeschlossen ist.

   Dieser Wert kann erhöht werden, damit Clients mehrere parallele Verbindungen mit einem neuen Ticket für jede Verbindung öffnen können.

Es werden keine Tickets gesendet, wenn die Wiederaufnahme deaktiviert ist.

Standardwert: 1

Mindestwert: 1

Maximaler Wert: 10

```
set ssl profile tls13profile -tls13sessionTicketsPerAuthContext 1

set ssl profile tls13profile -tls13sessionTicketsPerAuthContext 10
<!--NeedCopy-->
```

3. Festlegen des DH-Schlüsselaustausch

   `dheKeyExchangeWithPsk`: Gibt an, ob ein virtueller SSL-Server einen DHE-Schlüsselaustausch erfordert, wenn ein vorab freigegebener Schlüssel während eines Handshakes zur Wiederaufnahme einer TLS 1.3-Sitzung akzeptiert wird. Ein DHE-Schlüsselaustausch gewährleistet die Vorwärtsgeheimnis, auch wenn Ticketschlüssel kompromittiert sind, auf Kosten zusätzlicher Ressourcen, die für die Durchführung des **DHE-Schlüsselaustauschs** erforderlich sind.

   Die verfügbaren Einstellungen funktionieren wie folgt, wenn das Sitzungsticket aktiviert ist:

   JA: Ein DHE-Schlüsselaustausch ist erforderlich, wenn ein vorab freigegebener Schlüssel akzeptiert wird, unabhängig davon, ob der Kunde den Schlüsselaustausch unterstützt. Der Handshake wird mit einer schwerwiegenden Warnung abgebrochen, wenn der Client den DHE-Schlüsselaustausch nicht unterstützt, wenn er einen vorab freigegebenen Schlüssel anbietet.

   NEIN: Der DHE-Schlüsselaustausch wird durchgeführt, wenn ein vorab freigegebener Schlüssel akzeptiert wird, nur wenn dies vom Kunden angefordert wird.

   Mögliche Werte: JA, NEIN

   Standardwert: NEIN

```
set ssl profile tls13profile dheKeyExchangeWithPsk yes

set ssl profile tls13profile dheKeyExchangeWithPsk no
<!--NeedCopy-->
```

4. Frühe Datenakzeptanz von 0-RTT aktivieren oder deaktivieren

   `zeroRttEarlyData`: Stand der frühen Anwendungsdaten von TLS 1.3. Die zutreffenden Einstellungen funktionieren wie folgt:

ENABLED: Frühe Anwendungsdaten könnten verarbeitet werden, bevor der Handshake abgeschlossen ist.
DISABLED: Frühe Anwendungsdaten werden ignoriert.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

```
set ssl profile tls13profile -zeroRttEarlyData ENABLED

set ssl profile tls13profile -zeroRttEarlyData DISABLED
<!--NeedCopy-->
```

Standard-Verschlüsselungsgruppe

Die standardmäßige Verschlüsselungsgruppe umfasst TLS1.3-Verschlüsselungen.

```
sh cipher DEFAULT
1) Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035

2)  Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
...
...
27) Cipher Name: TLS1.3-AES256-GCM-SHA384         Priority : 27
    Description: TLSv1.3 Kx=any      Au=any  Enc=AES-GCM(256) Mac=AEAD
         HexCode=0x1302

28) Cipher Name: TLS1.3_CHACHA20_POLY1305_SHA256     Priority : 28
    Description: TLSv1.3 Kx=any      Au=any  Enc=CHACHA20/POLY1305(256)
        Mac=AEAD   HexCode=0x1303

29) Cipher Name: TLS1.3-AES128_GCM-SHA256        Priority : 29
    Description: TLSv1.3 Kx=any      Au=any  Enc=AES-GCM(128) Mac=AEAD
         HexCode=0x1301
Done
<!--NeedCopy-->
```


Einschränkungen

- TLSv1.3 wird im Backend nicht unterstützt.
- TLSv1.3 wird auf einer Citrix Secure Web Gateway-Anwendung und auf einer Citrix ADC FIPS-Appliance nicht unterstützt.

Beschränkungen der Sicherheit

TLSv1.3-Serverbetreiber müssen die folgenden Sicherheitsbeschränkungen für die Abwärtskompatibilität beachten, die in RFC 8446 beschrieben sind. Die Standardkonfiguration auf einer NetScaler-Appliance entspricht diesen Einschränkungen. Eine NetScaler-Appliance erzwingt jedoch nicht, dass diese Regeln eingehalten werden.

- Die Sicherheit von RC4-Verschlüsselungssammlungen wird als unzureichend angesehen, wie in RFC7465 beschrieben. Implementierungen dürfen keine RC4-Verschlüsselungssammlungen für irgendeine Version von TLS anbieten oder aushandeln.
- Alte Versionen von TLS ermöglichten die Verwendung von Chiffren mit geringer Stärke. Chiffren mit einer Stärke von weniger als 112 Bit dürfen für keine Version von TLS angeboten oder ausgehandelt werden.
- Die Sicherheit von SSL 3.0 [SSLv3] wird wie in RFC7568 beschrieben als unzureichend angesehen und darf nicht ausgehandelt werden. Deaktivieren Sie SSLv3, wenn TLSv1.3 aktiviert ist (SSLv3 ist standardmäßig deaktiviert).
- Die Sicherheit von SSL 2.0 [SSLv2] wird wie in RFC6176 beschrieben als unzureichend angesehen und darf nicht ausgehandelt werden. Deaktivieren Sie SSLv2, wenn TLS 1.3 aktiviert ist (SSLv2 ist standardmäßig deaktiviert).

> **Hinweis:**
>
> Informationen zur Fehlerbehebung von Protokollen, die über TLS1.3 laufen, finden Sie unter Entschlüsseln des TLS1.3-Datenverkehrs aus der Paketverfolgung.

Anleitungsartikel

October 5, 2021

Anleitungen sind einfach und einfach zu bedienende Artikel mit Konfigurationsschritten für allgemeine Bereitstellungen. Klicken Sie auf einen Link, um den Artikel aufzurufen.

Erstellen einer Zertifikatsignaturanforderung und Verwenden von SSL-Zertifikaten auf einer Citrix ADC Appliance

SSL-Zertifikate

October 5, 2021

Ein SSL-Zertifikat, das Teil einer SSL-Transaktion ist, ist ein digitales Datenformular (X509), das ein Unternehmen (eine Domain) oder eine Person identifiziert. Das Zertifikat verfügt über eine Public-Key-Komponente, die für jeden Client sichtbar ist, der eine sichere Transaktion mit dem Server initiieren möchte. Der entsprechende private Schlüssel, der sich sicher auf der Citrix ADC-Appliance befindet, wird verwendet, um die Verschlüsselung und Entschlüsselung asymmetrischer Schlüssel (oder öffentlicher Schlüssel) abzuschließen.

Sie können ein SSL-Zertifikat und einen Schlüssel auf eine der folgenden Arten beziehen:

- Von einer autorisierten Zertifizierungsstelle (CA) wie Verisign
- Durch Generieren eines neuen SSL-Zertifikats und eines neuen Schlüssels auf der Citrix ADC-Appliance

Alternativ können Sie ein vorhandenes SSL-Zertifikat auf der Appliance verwenden.

Zertifikate werden von der Citrix ADC Appliance in vier Typen eingeteilt:

- **Serverzertifikate:** Ein Serverzertifikat authentifiziert die Identität des Servers gegenüber dem Client. Im Front-End fungiert die ADC-Appliance als Server. Sie binden ein Serverzertifikat und einen privaten Schlüssel an einen virtuellen SSL-Server auf der ADC-Appliance.
- **Clientzertifikate:** Ein Clientzertifikat authentifiziert die Identität des Clients gegenüber dem Server. Im Back-End fungiert die ADC-Appliance als Client. Sie binden ein Clientzertifikat und einen privaten Schlüssel an den SSL-Dienst oder die Dienstgruppe auf der ADC-Appliance.
- **CA-Zertifikate:** CA-Zertifikate stellen die Endbenutzerzertifikate (Client- und Serverzertifikate) aus. Ein CA-Zertifikat kann eine vertrauenswürdige Stammzertifizierungsstelle (von der Zertifizierungsstelle selbst signiert) oder eine Zwischenzertifizierungsstelle (signiert von einer vertrauenswürdigen Stammzertifizierungsstelle) sein. In der Regel benötigen CA-Zertifikate keine privaten Schlüssel.
- **Unbekannte Zertifikate:** Alle anderen Zertifikate fallen in diese Kategorie.

Wichtig: Citrix empfiehlt, dass Sie Zertifikate von autorisierten Zertifizierungsstellen wie Verisign für alle Ihre SSL-Transaktionen verwenden. Verwenden Sie Zertifikate, die auf der Citrix ADC Appliance generiert werden, nur zu Testzwecken, nicht in einer Live-Bereitstellung.

- Wenn Sie beim Hinzufügen eines Zertifikatschlüsselpaars eine Zertifikatdatei mit dem gleichen Namen wie eine vorhandene Zertifikatsdatei hinzufügen, wird die ursprüngliche Zertifikatsdatei ohne Warnung überschrieben. Diese Aktion kann nach dem Neustart der Appliance zu Problemen führen, da die ursprüngliche Zertifikatsdatei nicht mehr im `/nsconfig/ssl` Verzeichnis verfügbar ist.
- Das Entfernen von Zertifikaten oder Schlüsseldateien in einer Clusterumgebung schränkt die weitere Konfiguration auf der ADC-Appliance ein. Fügen Sie die Dateien am selben Speicherort hinzu, um Konfigurationsänderungen vorzunehmen.

Hinweis: Sie können das ADM SSL-Dashboard verwenden, um die SSL-Zertifikatsverwaltung zu vereinfachen und Benachrichtigungen für Zertifikate festzulegen, die nicht verwendet werden oder bald ablaufen. Weitere Informationen finden Sie unter Verwaltung von SSL-Zertifikaten.

Erstellen eines Zertifikats

April 7, 2022

Eine Zertifizierungsstelle (CA) ist eine Stelle, die digitale Zertifikate für die Verwendung in der Kryptografie mit öffentlichen Schlüsseln ausstellt. Anwendungen wie Webbrowser, die SSL-Transaktionen durchführen, vertrauen Zertifikaten, die von einer Zertifizierungsstelle ausgestellt oder signiert wurden. Diese Anwendungen führen eine Liste der Zertifizierungsstellen, denen sie vertrauen. Wenn einer der vertrauenswürdigen Zertifizierungsstellen das für die sichere Transaktion verwendete Zertifikat signiert, setzt die Anwendung die Transaktion fort.

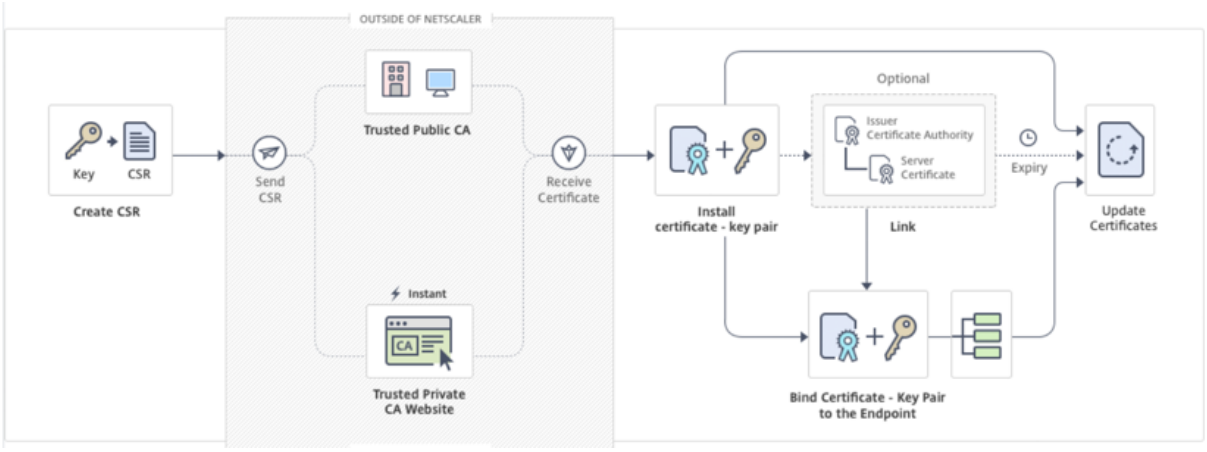
Vorsicht: Citrix empfiehlt, dass Sie für alle Ihre SSL-Transaktionen Zertifikate verwenden, die von autorisierten Zertifizierungsstellen wie Verisign bezogen wurden. Verwenden Sie Zertifikate, die auf der Citrix ADC-Appliance generiert werden, nur zu Testzwecken, nicht in einer Live-Bereitstellung.

Informationen zum Importieren eines vorhandenen Zertifikats und Schlüssels finden Sie unter Importieren eines Zertifikats.

Führen Sie die folgenden Schritte aus, um ein Zertifikat zu erstellen und es an einen virtuellen SSL-Server zu binden. Die einzigen Sonderzeichen, die in den Dateinamen zulässig sind, sind Unterstrich und Punkt.

- Erstellen Sie einen privaten Schlüssel.
- Erstellen Sie eine Zertifikatssignieranforderung (CSR).
- Reichen Sie die CSR bei einer Zertifizierungsstelle ein.
- Erstellen Sie ein Zertifikatsschlüsselpaar.
- Binden Sie das Zertifikatsschlüsselpaar an einen virtuellen SSL-Server

Das folgende Diagramm veranschaulicht den Arbeitsablauf.



Videolink zu Wie erstelle und installiere ich ein neues Zertifikat.

Erstellen eines privaten Schlüssels

> **Hinweise:**
>
> - Ab Version 12.1 Build 49.x können Sie den AES256-Algorithmus mit dem PEM-Schlüsselformat

> verwenden, um einen privaten Schlüssel auf der Appliance zu verschlüsseln. AES mit 256-Bit-Schlüssel ist mathematisch effizienter und sicherer als der 56-Bit-Schlüssel des Data Encryption Standard (DES).
>
> - Ab Version 12.1 Build 50.x können Sie einen RSA-Schlüssel im PKCS #8 -Format erstellen.

Der private Schlüssel ist der wichtigste Teil eines digitalen Zertifikats. Per Definition darf dieser Schlüssel nicht mit irgendjemandem geteilt werden und muss sicher auf der Citrix ADC Appliance aufbewahrt werden. Alle mit dem öffentlichen Schlüssel verschlüsselten Daten können nur mit dem privaten Schlüssel entschlüsselt werden.

Das Zertifikat, das Sie von der Zertifizierungsstelle erhalten, ist nur mit dem privaten Schlüssel gültig, der zum Erstellen der CSR verwendet wurde. Der Schlüssel ist erforderlich, um das Zertifikat zur Citrix ADC Appliance hinzuzufügen.

Die Appliance unterstützt nur die RSA-Verschlüsselungsalgorithmen zum Erstellen privater Schlüssel. Sie können beide Arten von privaten Schlüsseln an die Zertifizierungsstelle (CA) senden. Das Zertifikat, das Sie von der Zertifizierungsstelle erhalten, ist nur mit dem privaten Schlüssel gültig, der zum Erstellen der CSR verwendet wurde. Der Schlüssel ist erforderlich, um das Zertifikat zur Citrix ADC Appliance hinzuzufügen.

Wichtig:

> - Beschränken Sie unbedingt den Zugriff auf Ihren privaten Schlüssel. Jeder, der Zugriff auf Ihren privaten Schlüssel hat, kann Ihre SSL-Daten entschlüsseln.
> - Die Länge des zulässigen SSL-Schlüsselnamens umfasst die Länge des absoluten Pfadnamens, wenn der Pfad im Schlüsselnamen enthalten ist.

Alle SSL-Zertifikate und Schlüssel werden im Ordner `/nsconfig/ssl` auf der Appliance gespeichert. Für zusätzliche Sicherheit können Sie den DES- oder Triple DES (3DES) -Algorithmus verwenden, um den auf der Appliance gespeicherten privaten Schlüssel zu verschlüsseln.

Erstellen eines privaten RSA-Schlüssels mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

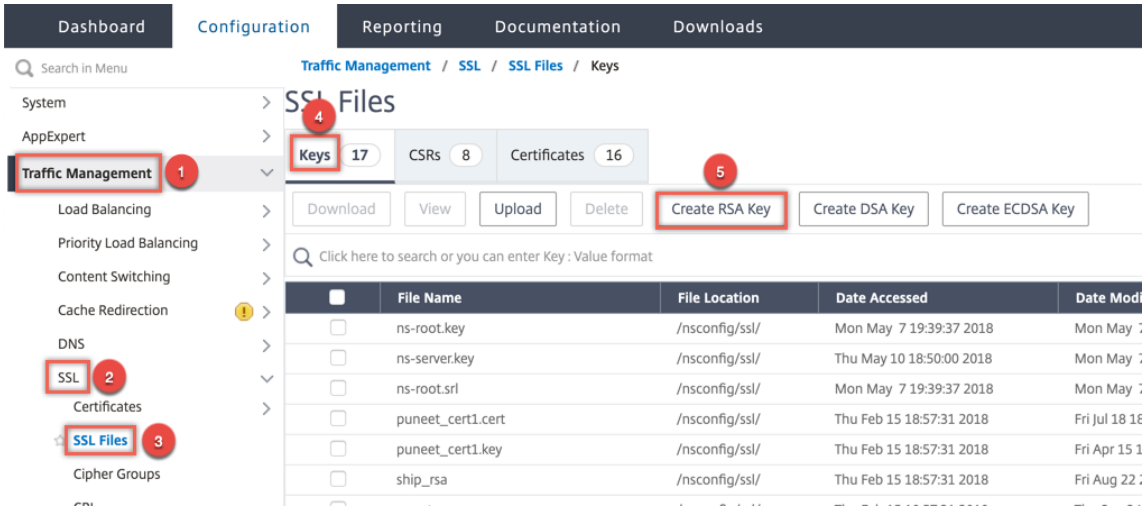
```
1 create ssl rsakey <keyFile> <bits> [-exponent ( 3 | F4 )] [-keyform (
     DER | PEM )] [-des | -des3 | -aes256] {
2  -password  }
3   [-pkcs8]
4 <!--NeedCopy-->
```

Beispiel:


```
create rsakey testkey 2048 -aes256 -password 123456 -pkcs8
<!--NeedCopy-->
```

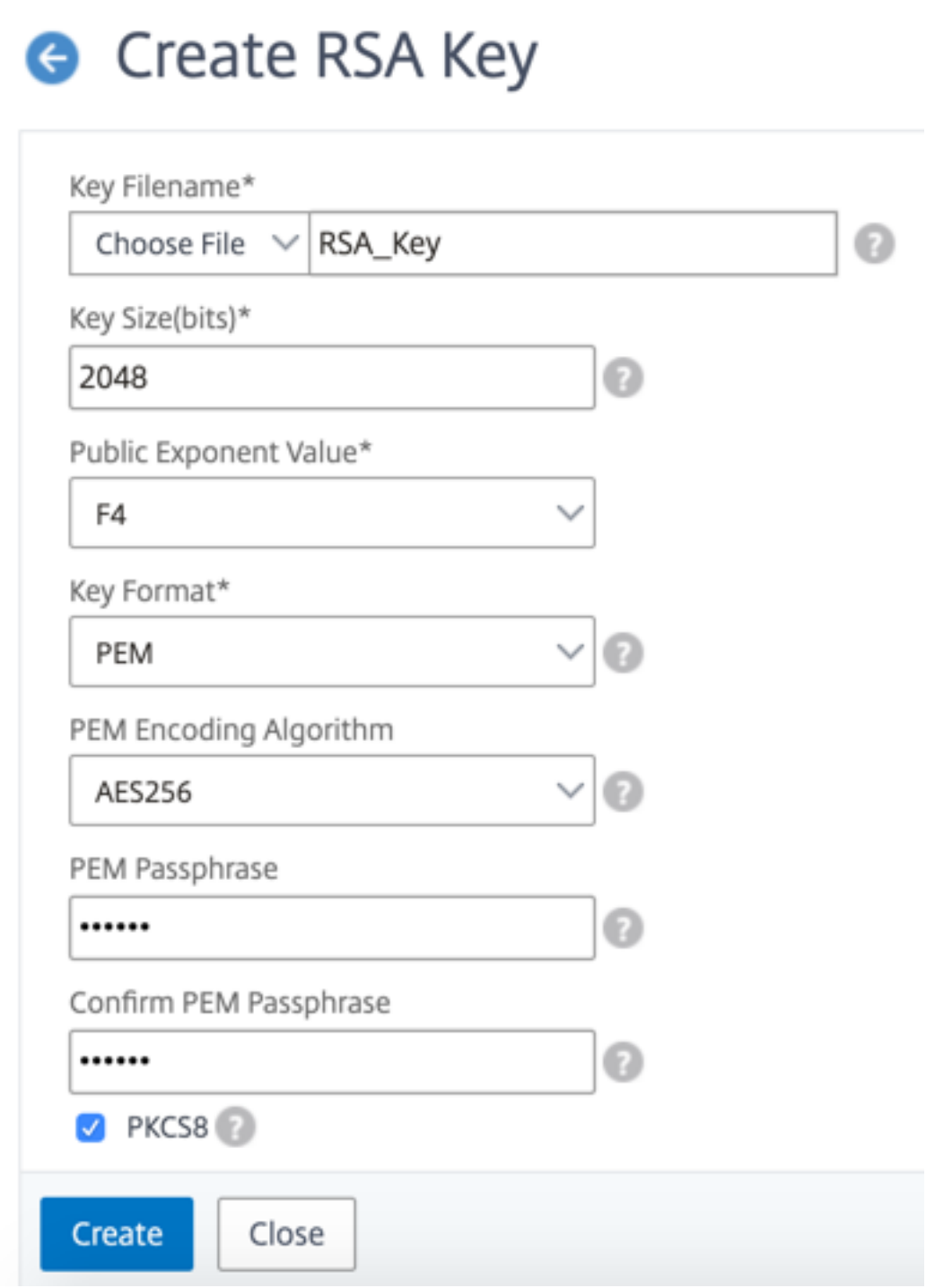
Erstellen eines privaten RSA-Schlüssels mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL > SSL-Dateien**.
2. Wählen Sie auf der Registerkarte **Keys** die Option **RSA-Schlüssel erstellen**aus.



3. Geben Sie Werte für die folgenden Parameter ein und klicken Sie auf **Erstellen**.

   - **Key Filename** — Name für und optional Pfad zur RSA-Schlüsseldatei. /nsconfig/ssl/ ist der Standardpfad.
   - **Schlüsselgröße** — Größe des RSA-Schlüssels in Bit. Kann von 512 Bit bis 4096 Bit reichen.
   - **Öffentlicher Exponentenwert** — Öffentlicher Exponent für den RSA-Schlüssel. Der Exponent ist Teil des Verschlüsselungsalgorithmus und wird zum Erstellen des RSA-Schlüssels benötigt.
   - **Schlüsselformat** — Das Format, in dem die RSA-Schlüsseldatei auf der Appliance gespeichert ist.
   - **PEM-Codierungsalgorithmus** - Verschlüsseln Sie den generierten RSA-Schlüssel mithilfe des AES 256-, DES- oder Triple-DES (DES3) -Algorithmus. Standardmäßig sind private Schlüssel unverschlüsselt.
   - **PEM-Passphrase — Wenn der private Schlüssel verschlüsselt ist, geben Sie eine Passphrase** für den Schlüssel ein.



Wählen Sie über die grafische Benutzeroberfläche einen AES256-Codierungsalgorithmus in einem RSA-Schlüssel

1. Navigieren Sie zu **Traffic Management > SSL > SSL-Dateien > RSA-Schlüssel erstellen**.

2. Wählen Sie **unter SchlüsselformatPEM**aus.
3. Wählen Sie im **PEM-KodierungsalgorithmusAES256**aus.
4. Wählen Sie **PKCS8**.

Erstellen einer Zertifikatsignaturanforderung mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

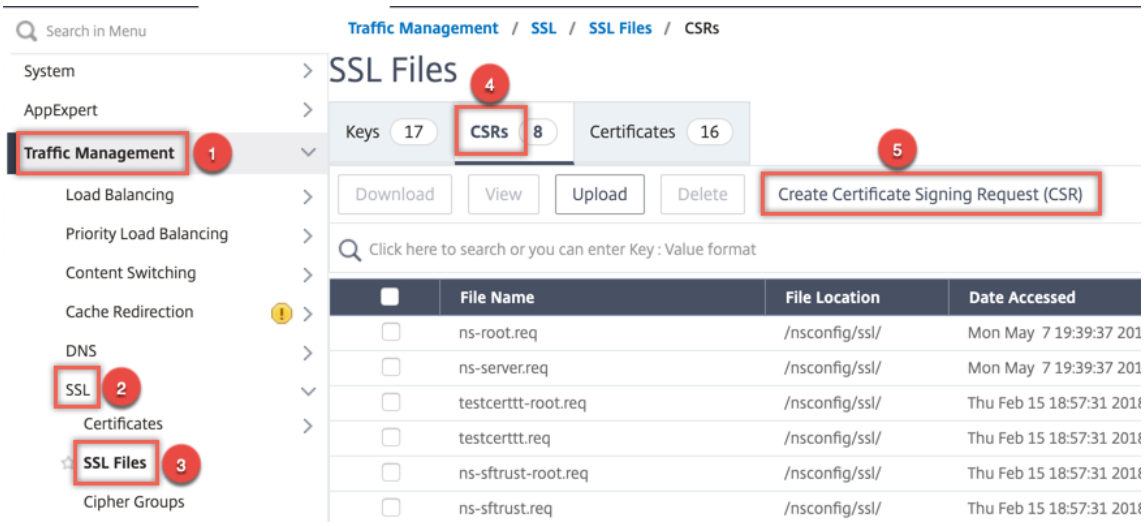
```
create ssl certreq <reqFile> -keyFile <input_filename> | -fipsKeyName <
   string>) [-keyForm (DER | PEM) {
 -PEMPassPhrase  }
 ] -countryName <string> -stateName <string> -organizationName <string>
     -organizationUnitName <string> -localityName <string> -commonName
    <string> -emailAddress <string> {
 -challengePassword  }
  -companyName <string> -digestMethod ( SHA1 | SHA256 )
<!--NeedCopy-->
```

Beispiel:

```
create ssl certreq priv_csr_sha256 -keyfile priv_2048_2 -keyform PEM -
   countryName IN -stateName Karnataka -localityName Bangalore -
   organizationName Citrix -organizationUnitName NS -digestMethod
   SHA256
<!--NeedCopy-->
```

Erstellen einer Zertifikatssignieranforderung über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > SSL**.
2. Klicken Sie in **SSL-Zertifikat** auf **Certificate Signing Request (CSR) erstellen**



3. Wählen Sie unter **Digest-Methode** die Option **SHA256** aus.

Weitere Informationen finden Sie unter Erstellen einer CSR .

Unterstützung für alternativen Antragstellernamen in einer Zertifikatsignieranforderung

Das Feld “Subject Alternative Name” (SAN) in einem Zertifikat ermöglicht es Ihnen, mehrere Werte, wie Domänennamen und IP-Adressen, einem einzigen Zertifikat zuzuordnen. Mit anderen Worten, Sie können mehrere Domänen wie www.example.com, www.example1.com, www.example2.com, mit einem einzigen Zertifikat sichern.

Einige Browser, wie Google Chrome, unterstützen keinen gebräuchlichen Namen in einer Zertifikatssignieranforderung (CSR) mehr. Sie setzen SAN in allen öffentlich vertrauenswürdigen Zertifikaten durch.

Die Citrix ADC Appliance unterstützt das Hinzufügen von SAN-Werten beim Erstellen einer CSR. Sie können eine CSR mit einem SAN-Eintrag an eine Zertifizierungsstelle senden, um ein signiertes Zertifikat mit diesem SAN-Eintrag zu erhalten. Wenn die Appliance eine Anforderung erhält, sucht sie in den SAN-Einträgen im Serverzertifikat nach einem übereinstimmenden Domänennamen. Wenn eine Übereinstimmung gefunden wird, sendet es das Zertifikat an den Client und schließt den SSL-Handshake ab. Sie können die CLI oder die GUI verwenden, um eine CSR mit SAN-Werten zu erstellen.

> **Hinweis:** Die Citrix ADC Appliance verarbeitet nur DNS-basierte SAN-Werte.

Erstellen einer CSR mit dem alternativen Antragstellernamen mithilfe der CLI

```
create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName
    <string>) [-subjectAltName <string>] [-keyform ( DER | PEM )  {
```



```
2   -PEMPassPhrase  }
3   ] -countryName <string> -stateName <string> -organizationName <string>
        [-organizationUnitName <string>] [-localityName <string>] [-
       commonName <string>] [-emailAddress <string>] {
4   -challengePassword  }
5    [-companyName <string>] [-digestMethod ( SHA1 | SHA256 )]
6   <!--NeedCopy-->
```

Parameter:

SubjectAltName: Der alternative Antragstellername (SAN) ist eine Erweiterung von X.509, mit der verschiedene Werte mithilfe eines SubjectAltName-Feldes mit einem Sicherheitszertifikat verknüpft werden können. Diese Werte werden als “Subject Alternative Names” (SAN) bezeichnet. Zu den Namen gehören:

1. IP-Adressen (Präfix mit “IP:” Beispiel: IP:198.51.10.5 IP:192.0.2.100)
2. DNS-Namen (Präfix mit “DNS:” Beispiel: DNS: www.example.com DNS: www.example.org DNS: www.example.net)

Geben Sie in der Befehlszeile Werte in Anführungszeichen ein. Trennen Sie zwei Werte durch ein Leerzeichen. Anführungszeichen sind in der GUI nicht erforderlich.
Maximale Länge: 127

Beispiel:

```
1   create certReq test1.csr -keyFile test1.ky -countryName IN -stateName
       Kar -organizationName citrix -commonName ctx.com -subjectAltName ”
       DNS:*.example.com DNS:www.example.org DNS:www.example.net”
2   <!--NeedCopy-->
```

> **Hinweis:**
>
> Auf einer FIPS-Appliance müssen Sie den Schlüsseldateinamen durch den FIPS-Schlüsselnamen ersetzen, wenn Sie den FIPS-Schlüssel direkt auf der Appliance erstellen.
>
> ```
> 1   create certReq <csrname> -fipsKeyName fipskey.ky -countryName IN -
>        stateName Kar -organizationName citrix -commonName ctx.com -
>        subjectAltName ”DNS:www.example.com DNS:www.example.org DNS:www.
>        example.net”
> 2   <!--NeedCopy-->
> ```


Erstellen einer CSR mit der GUI

1. Navigieren Sie zu **Traffic Management** > **SSL** > **SSL-Dateien**.
2. Klicken Sie auf der Registerkarte **CSR** auf **Certificate Signing Request (CSR) erstellen**.
3. Geben Sie die Werte ein und klicken Sie auf **Erstellen**.

Einschränkungen

Um SAN beim Erstellen eines SSL-Zertifikats zu verwenden, müssen Sie die SAN-Werte explizit angeben. Die Werte werden nicht automatisch aus der CSR-Datei gelesen.

Reichen Sie die CSR bei der Zertifizierungsstelle ein

Die meisten Zertifizierungsstellen (CA) akzeptieren die Einreichung von Zertifikaten per E-Mail. Die Zertifizierungsstelle gibt ein gültiges Zertifikat an die E-Mail-Adresse zurück, von der Sie die CSR übermitteln.

Die CSR ist im Ordner `/nsconfig/ssl` gespeichert.

Erstellen eines Testzertifikats

> **Hinweis:**
>
> Informationen zum Generieren eines Servertestzertifikats finden Sie unter Generieren eines Server-Testzertifikats.

Die Citrix ADC Appliance verfügt über eine integrierte Zertifizierungsstellen-Tools-Suite, mit der Sie selbstsignierte Zertifikate zu Testzwecken erstellen können.

Vorsicht: Da die Citrix ADC Appliance diese Zertifikate signiert und keine tatsächliche Zertifizierungsstelle, dürfen Sie sie nicht in einer Produktionsumgebung verwenden. Wenn Sie versuchen, ein selbstsigniertes Zertifikat in einer Produktionsumgebung zu verwenden, erhalten Benutzer bei jedem Zugriff auf den virtuellen Server eine Warnung “Zertifikat ungültig”.

Die Appliance unterstützt die Erstellung der folgenden Zertifikattypen:

- Root-CA-Zertifikate
- CA-Zertifikate für Fortgeschrittene
- Endbenutzer-Zertifikate
  - Server-Zertifikate
  - Client-Zertifikate

Erstellen Sie vor dem Generieren eines Zertifikats einen privaten Schlüssel und erstellen Sie damit eine Zertifikatssignierungsanforderung (CSR) auf der Appliance. Anstatt die CSR dann an eine Zertifizierungsstelle zu senden, verwenden Sie die Citrix ADC CA Tools, um ein Zertifikat zu generieren.

Erstellen eines Zertifikats mithilfe eines Assistenten

1. Navigieren Sie zu **Traffic Management > SSL**.
2. Wählen Sie im Detailbereich unter **Erste Schritte**den Assistenten für den zu erstellenden Zertifikattyp aus.
3. Befolgen Sie die Anweisungen auf dem Bildschirm.

Erstellen eines Root-CA-Zertifikats mithilfe der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM )] [-days <positive_integer>]
<!--NeedCopy-->
```

Im folgenden Beispiel ist csreq1 die CSR und rsa1 ist der private Schlüssel, der zuvor erstellt wurde.

Beispiel:

```
create ssl cert cert1 csreq1 ROOT_CERT -keyFile rsa1 -keyForm PEM -days
     365

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

Erstellen eines zwischengeschalteten CA-Zertifikats mithilfe der CLI

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM )] [-days <positive_integer>]
     [-certForm ( DER | PEM )] [-CAcert <input_filename>] [-CAcertForm (
     DER | PEM )] [-CAkey <input_filename>] [-CAkeyForm ( DER | PEM )]
    [-CAserial <output_filename>]
<!--NeedCopy-->
```

Im folgenden Beispiel ist csr1 die zuvor erstellte CSR. Cert1 und rsakey1 sind das Zertifikat und der entsprechende Schlüssel des selbstsignierten Zertifikats (Root-CA), und pvtkey1 ist der private Schlüssel des zwischengeschalteten CA-Zertifikats.

Beispiel:


```
create ssl cert certsy csr1 INTM_CERT -CAcert cert1 -CAkey rsakey1 -
    CAserial 23
Done

create ssl rsakey pvtkey1 2048 -exponent F4 -keyform PEM
Done
<!--NeedCopy-->
```

Erstellen eines Root-CA-Zertifikats mit der GUI

Navigieren Sie zu **Traffic Management > SSL**, und wählen Sie in der Gruppe Erste Schritte den **Assistenten für das Root-CA-Zertifikat**aus, und konfigurieren Sie ein Stammzertifikat der Zertifizierungsstelle.

Erstellen eines zwischengeschalteten CA-Zertifikats über die grafische Benutzeroberfläche

Navigieren Sie zu **Traffic Management > SSL**, und wählen Sie in der Gruppe Erste Schritte den **Assistenten für zwischengeschaltete CA-Zertifikate**aus, und konfigurieren Sie ein zwischengeschaltetes CA-Zertifikat.

Erstellen eines Endbenutzerzertifikats

Ein Endbenutzerzertifikat kann ein Clientzertifikat oder ein Serverzertifikat sein. Um ein Testendbenutzerzertifikat zu erstellen, geben Sie das Zwischenzertifikat der Zertifizierungsstelle oder das selbstsignierte Root-CA-Zertifikat an.

> **Hinweis:** Um ein Endbenutzerzertifikat für die Produktionsverwendung zu erstellen, geben Sie ein vertrauenswürdiges CA-Zertifikat an und senden Sie die CSR an eine Zertifizierungsstelle (CA).

Erstellen eines Test-Endbenutzerzertifikats mithilfe der Befehlszeilenschnittstelle

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM )] [-days<positive_integer>]
    [-certForm ( DER | PEM )] [-CAcert <input_filename>] [-CAcertForm (
    DER | PEM )] [-CAkey<input_filename>] [-CAkeyForm ( DER | PEM )] [-
    CAserial <output_filename>]
<!--NeedCopy-->
```

Wenn kein Zwischenzertifikat vorhanden ist, verwenden Sie die Werte für das Zertifikat (cert1) und den privaten Schlüssel (rsakey1) des Root-CA-Zertifikats in `CAcert` und `CAkey`.

Beispiel:

```
create ssl cert cert12 csr1 SRVR_CERT -CAcert cert1 -CAkey rsakey1 -
    CAserial 23

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

Wenn ein Zwischenzertifikat vorhanden ist, verwenden Sie die Werte für das Zertifikat (`certsy`) und den privaten Schlüssel (pvtkey1) des Zwischenzertifikats in `CAcert` und `CAkey`.

Beispiel:

```
create ssl cert cert12 csr1 SRVR_CERT -CAcert certsy -CAkey pvtkey1 -
    CAserial 23

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

Erstellen eines selbstsignierten SAN-Zertifikats mit OpenSSL

Um ein selbstsigniertes SAN-Zertifikat mit mehreren alternativen Antragstellernamen zu erstellen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie eine OpenSSL-Konfigurationsdatei auf Ihrem lokalen Computer, indem Sie die entsprechenden Felder gemäß den Unternehmensanforderungen bearbeiten.

   Hinweis: Im folgenden Beispiel ist die Konfigurationsdatei “req.conf”.

   ```
   [req]
   distinguished_name = req_distinguished_name
   x509_extensions = v3_req
   prompt = no
   [req_distinguished_name]
   C = US
   ST = VA
   L = SomeCity
   O = MyCompany
   OU = MyDivision
   CN = www.company.com
   [v3_req]
   ```



```
keyUsage = keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = www.company.net
DNS.2 = company.com
DNS.3 = company.net
<!--NeedCopy-->
```

2. Laden Sie die Datei in das Verzeichnis /nsconfig/ssl auf der Citrix ADC Appliance hoch.
3. Melden Sie sich als Benutzer `nsroot` bei der Citrix ADC CLI an und wechseln Sie zur Shell-Eingabeaufforderung.
4. Führen Sie den folgenden Befehl aus, um das Zertifikat zu erstellen:

```
cd /nsconfig/ssl
openssl req -x509 -nodes -days 730 -newkey rsa:2048 -keyout cert.
   pem -out cert.pem -config req.conf -extensions 'v3_req'
<!--NeedCopy-->
```

5. Führen Sie den folgenden Befehl aus, um das Zertifikat zu überprüfen:

```
openssl x509 -in cert.pem -noout  - text
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
ed:90:c5:f0:61:78:25:ab
Signature Algorithm: md5WithRSAEncryption
Issuer: C=US, ST=VA, L=SomeCity, O=MyCompany, OU=MyDivision, CN=
   www.company.com
Validity
Not Before: Nov 6 22:21:38 2012 GMT
Not After : Nov 6 22:21:38 2014 GMT
Subject: C=US, ST=VA, L=SomeCity, O=MyCompany, OU=MyDivision, CN=
   www.company.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
…
Exponent: 65537 (0x10001)
```



```
X509v3 extensions:
X509v3 Key Usage:
Key Encipherment, Data Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication
X509v3 Subject Alternative Name:
DNS:www.company.net, DNS:company.com, DNS:company.net
Signature Algorithm: md5WithRSAEncryption …
<!--NeedCopy-->
```

Installieren, Verknüpfen und Aktualisieren von Zertifikaten

April 7, 2022

Informationen zum Installieren eines Zertifikats finden Sie unter Hinzufügen oder Aktualisieren eines Zertifikatschlüsselpaares.

Verknüpfen von Zertifikaten

Viele Serverzertifikate sind von mehreren hierarchischen Zertifizierungsstellen (CA) signiert, was bedeutet, dass die Zertifikate eine Kette wie die folgende bilden:

```
Root CA
|
+---------- Intermediate CA
|
+---------------------- End-Entity (Server) Certificate
```

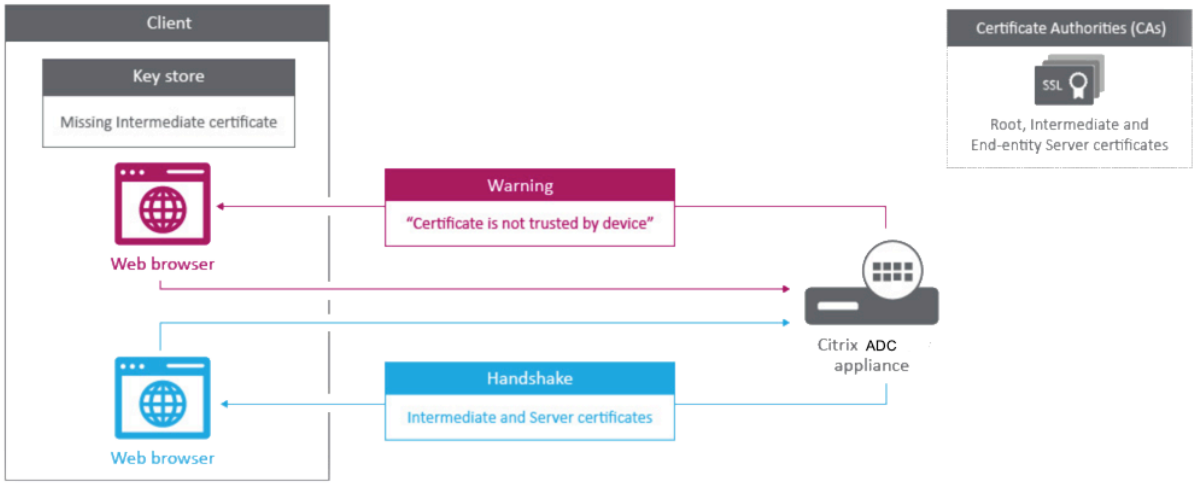
Manchmal wird die Zwischenzertifizierungsstelle in ein primäres und ein sekundäres Zwischenzertifikat der Zertifizierungsstelle aufgeteilt Dann bilden die Zertifikate eine Kette wie folgt:

```
Root CA
|
+------ Primary Intermediate CA
|+-------------- Secondary Intermediate CA
|
+---------------------- End-Entity (Server) Certificate
```

Clientcomputer enthalten normalerweise das Stammzertifizierungsstellenzertifikat in ihrem lokalen Zertifikatsspeicher, aber nicht ein oder mehrere zwischengeschaltete CA-Zertifikate. Die ADC-Appliance muss ein oder mehrere Zwischenzertifikate der Zertifizierungsstelle an die Clients senden.

Hinweis: Die Appliance darf das Stammzertifizierungsstellenzertifikat nicht an den Client senden. Für das Public Key Infrastructure (PKI) -Trust-Relationship-Modell müssen Root-CA-Zertifikate mithilfe einer Out-of-Band-Methode auf Clients installiert werden. Zum Beispiel sind die Zertifikate im Betriebssystem oder Webbrowser enthalten. Der Client ignoriert ein Stammzertifikat der Zertifizierungsstelle, das von der Appliance gesendet wurde.

Manchmal stellt eine zwischengeschaltete Zertifizierungsstelle, die Standardwebbrowser nicht als vertrauenswürdige Zertifizierungsstelle erkennen, das Serverzertifikat aus. In diesem Fall müssen ein oder mehrere CA-Zertifikate mit dem eigenen Zertifikat des Servers an den Client gesendet werden. Andernfalls beendet der Browser die SSL-Sitzung, da er das Serverzertifikat nicht authentifizieren kann.



Videolink zu Wie verbinde ich ein Zwischenautoritätszertifikat.

In den folgenden Abschnitten finden Sie Informationen zum Hinzufügen von Server- und Zwischenzertifikaten:

- Manuelle Zertifikatsverknüpfung
- Automatisiertes Verknüpfen von
- Erstellen Sie eine Kette von Zertifikaten

Manuelle Zertifikatsverknüpfung

Hinweis: Diese Funktion wird auf der Citrix ADC FIPS-Plattform und in einem Cluster-Setup nicht unterstützt.

Anstatt einzelne Zertifikate hinzuzufügen und zu verknüpfen, können Sie jetzt ein Serverzertifikat und bis zu neun Zwischenzertifikate in einer einzigen Datei gruppieren. Sie können den Namen der Datei angeben, wenn Sie ein Zertifikat-Schlüsselpaar hinzufügen. Bevor Sie dies tun, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind.

- Die Zertifikate in der Datei haben die folgende Reihenfolge:
  - Serverzertifikat (muss das erste Zertifikat in der Datei sein)
  - Optional ein Serverschlüssel
  - Zwischenprodukt Zertifikat 1 (ic1)
  - Zwischenprodukt Zertifikat 2 (ic2)

  - Zwischenzertifikat 3 (ic3) usw.
    Hinweis: Zwischenzertifikatsdateien werden für jedes Zwischenzertifikat mit dem Namen "<certificatebundlename>.pem_ic <
    n>" erstellt, wobei n zwischen 1 und 9 liegt. Beispiel: bundle.pem_ic1, wobei **Bundle** der Name des Zertifikatssatzes und ic1 das erste Zwischenzertifikat im Satz ist.
- Bundle-Option ist ausgewählt.
- Die Datei enthält nicht mehr als neun Zwischenzertifikate.

Die Datei wird analysiert und das Serverzertifikat, die Zwischenzertifikate und der Serverschlüssel (falls vorhanden) werden identifiziert. Zunächst werden das Serverzertifikat und der Schlüssel hinzugefügt. Anschließend werden die Zwischenzertifikate in der Reihenfolge hinzugefügt, in der sie der Datei hinzugefügt wurden, und entsprechend verknüpft.

Ein Fehler wird gemeldet, wenn eine der folgenden Bedingungen zutrifft:

- Eine Zertifikatsdatei für eines der Zwischenzertifikate ist auf der Appliance vorhanden.
- Der Schlüssel wird in der Datei vor dem Serverzertifikat platziert.
- Ein Zwischenzertifikat wird vor das Serverzertifikat gestellt.
- Zwischenzertifikate werden nicht in derselben Reihenfolge in die Datei aufgenommen, in der sie erstellt wurden.
- In der Datei sind keine Zertifikate enthalten.
- Ein Zertifikat hat nicht das richtige PEM-Format.
- Die Anzahl der Zwischenzertifikate in der Datei übersteigt neun.

Hinzufügen eines Zertifikatssatzes mithilfe der CLI

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

```
1 add ssl certKey <certkeyName> -cert <string> -key <string> -bundle (YES
      | NO)
2
3 show ssl
4
5 show ssl certlink
6 <!--NeedCopy-->
```

Im folgenden Beispiel enthält der Zertifikatssatz (bundle.pem) die folgenden Dateien:

Serverzertifikat (Bundle) ist mit bundle_ic1 verknüpft

Erstes Zwischenzertifikat (bundle_ic1), das mit bundle_ic2 verknüpft ist

Zweites Zwischenzertifikat (bundle_ic2) mit bundle_ic3 verknüpft

Drittes Zwischenzertifikat (bundle_ic3)

```
add ssl certKey bundletest -cert bundle9.pem -key bundle9.pem -bundle
    yes

sh ssl certkey

1)      Name: ns-server-certificate
        Cert Path: ns-server.cert
        Key Path: ns-server.key
        Format: PEM
        Status: Valid,   Days to expiration:5733
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Server Certificate
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS
           Internal,CN=default OULLFT
        Validity
                Not Before: Apr 21 15:56:16 2016 GMT
                Not After : Mar  3 06:30:56 2032 GMT
        Subject:  C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS
           Internal,CN=default OULLFT
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

2)      Name: servercert
        Cert Path: complete/server/server_rsa_1024.pem
        Key Path: complete/server/server_rsa_1024.ky
        Format: PEM
        Status: Valid,   Days to expiration:7150
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Server Certificate
        Version: 3
        Serial Number: 1F
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:  C=IN,ST=KAR,O=Citrix R&D Pvt Ltd,CN=Citrix
        Validity
                Not Before: Sep  2 09:54:07 2008 GMT
                Not After : Jan 19 09:54:07 2036 GMT
```



```
        Subject:  C=IN,ST=KAR,O=Citrix Pvt Ltd,CN=Citrix
        Public Key Algorithm: rsaEncryption
        Public Key size: 1024

3)      Name: bundletest
        Cert Path: bundle9.pem
        Key Path: bundle9.pem
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Server Certificate
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA9
        Validity
                Not Before: Nov 28 06:43:11 2014 GMT
                Not After : Nov 25 06:43:11 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=Server9
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

4)      Name: bundletest_ic1
        Cert Path: bundle9.pem_ic1
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA8
        Validity
                Not Before: Nov 28 06:42:56 2014 GMT
                Not After : Nov 25 06:42:56 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA9
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

5)      Name: bundletest_ic2
        Cert Path: bundle9.pem_ic2
        Format: PEM
        Status: Valid,   Days to expiration:3078
```



```
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA7
        Validity
                Not Before: Nov 28 06:42:55 2014 GMT
                Not After : Nov 25 06:42:55 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA8
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

6)      Name: bundletest_ic3
        Cert Path: bundle9.pem_ic3
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA6
        Validity
                Not Before: Nov 28 06:42:53 2014 GMT
                Not After : Nov 25 06:42:53 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA7
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

7)      Name: bundletest_ic4
        Cert Path: bundle9.pem_ic4
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA5
        Validity
                Not Before: Nov 28 06:42:51 2014 GMT
```



```
                Not After : Nov 25 06:42:51 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA6
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

8)      Name: bundletest_ic5
        Cert Path: bundle9.pem_ic5
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA4
        Validity
                Not Before: Nov 28 06:42:50 2014 GMT
                Not After : Nov 25 06:42:50 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA5
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

9)      Name: bundletest_ic6
        Cert Path: bundle9.pem_ic6
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA3
        Validity
                Not Before: Nov 28 06:42:48 2014 GMT
                Not After : Nov 25 06:42:48 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA4
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

10)     Name: bundletest_ic7
        Cert Path: bundle9.pem_ic7
        Format: PEM
        Status: Valid,   Days to expiration:3078
```



```
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA2
        Validity
                Not Before: Nov 28 06:42:46 2014 GMT
                Not After : Nov 25 06:42:46 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA3
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

11)     Name: bundletest_ic8
        Cert Path: bundle9.pem_ic8
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=ICA1
        Validity
                Not Before: Nov 28 06:42:45 2014 GMT
                Not After : Nov 25 06:42:45 2024 GMT
        Subject:  C=IN,ST=ka,O=sslteam,CN=ICA2
        Public Key Algorithm: rsaEncryption
        Public Key size: 2048

12)     Name: bundletest_ic9
        Cert Path: bundle9.pem_ic9
        Format: PEM
        Status: Valid,   Days to expiration:3078
        Certificate Expiry Monitor: ENABLED
        Expiry Notification period: 30 days
        Certificate Type: Intermediate CA
        Version: 3
        Serial Number: 01
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IN,ST=ka,O=sslteam,CN=RootCA4096
        Validity
                Not Before: Nov 28 06:42:43 2014 GMT
```



```
219                 Not After : Nov 25 06:42:43 2024 GMT
220         Subject:  C=IN,ST=ka,O=sslteam,CN=ICA1
221         Public Key Algorithm: rsaEncryption
222         Public Key size: 2048
223 Done
224
225 sh ssl certlink
226
227 1)      Cert Name: bundletest    CA Cert Name: bundletest_ic1
228 2)      Cert Name: bundletest_ic1        CA Cert Name: bundletest_ic2
229 3)      Cert Name: bundletest_ic2        CA Cert Name: bundletest_ic3
230 4)      Cert Name: bundletest_ic3        CA Cert Name: bundletest_ic4
231 5)      Cert Name: bundletest_ic4        CA Cert Name: bundletest_ic5
232 6)      Cert Name: bundletest_ic5        CA Cert Name: bundletest_ic6
233 7)      Cert Name: bundletest_ic6        CA Cert Name: bundletest_ic7
234 8)      Cert Name: bundletest_ic7        CA Cert Name: bundletest_ic8
235 9)      Cert Name: bundletest_ic8        CA Cert Name: bundletest_ic9
236 Done
237 <!--NeedCopy-->
```

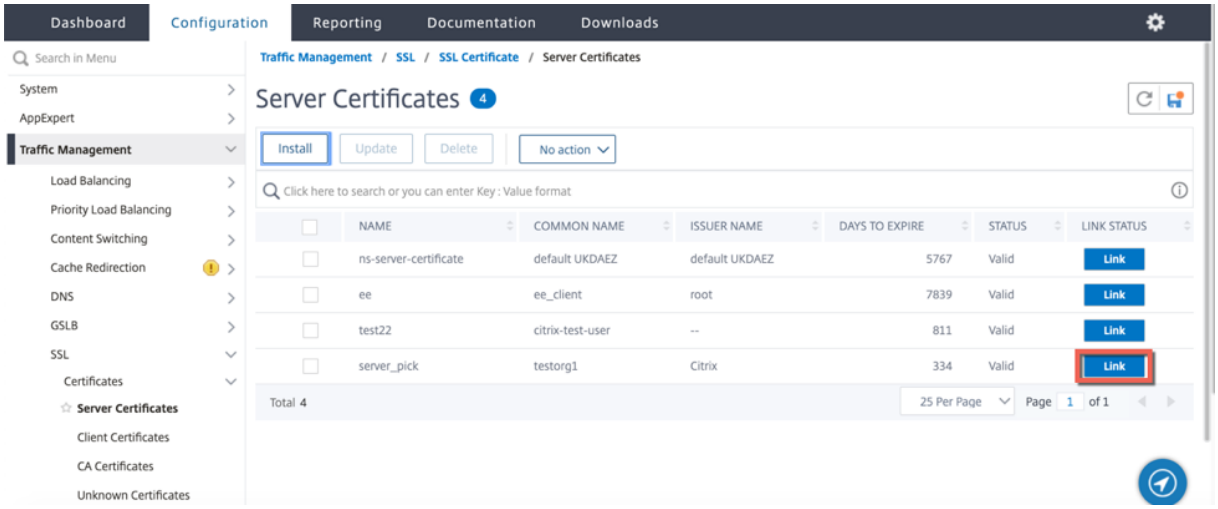
Hinzufügen eines Zertifikatssatzes über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management** > **SSL** > **Zertifikate** > **CA-Zertifikate**.
2. Klicken Sie im Detailbereich auf **Installieren**.
3. Geben **Sie im Dialogfeld Zertifikat installieren** die Details wie das Zertifikat und den Schlüsseldateinamen ein, und wählen Sie dann **Zertifikatpaket**aus.
4. Klicken Sie auf **Installieren**, und klicken Sie dann auf **Schließen**.

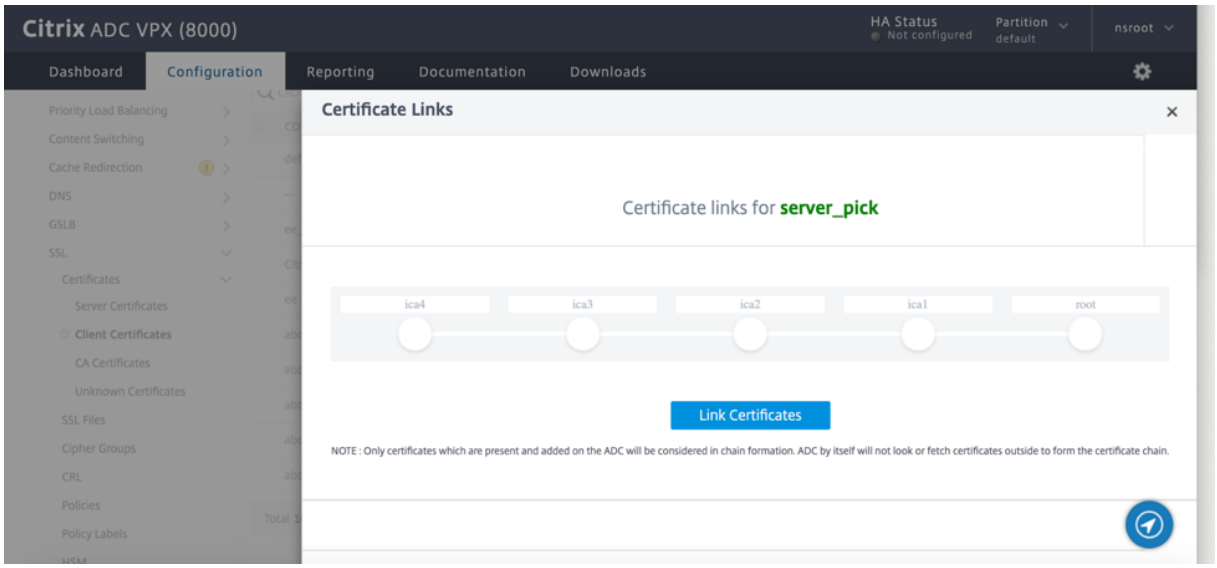
Automatisiertes Verknüpfen von

Hinweis: Diese Funktion ist ab Version 13.0 Build 47.x verfügbar.

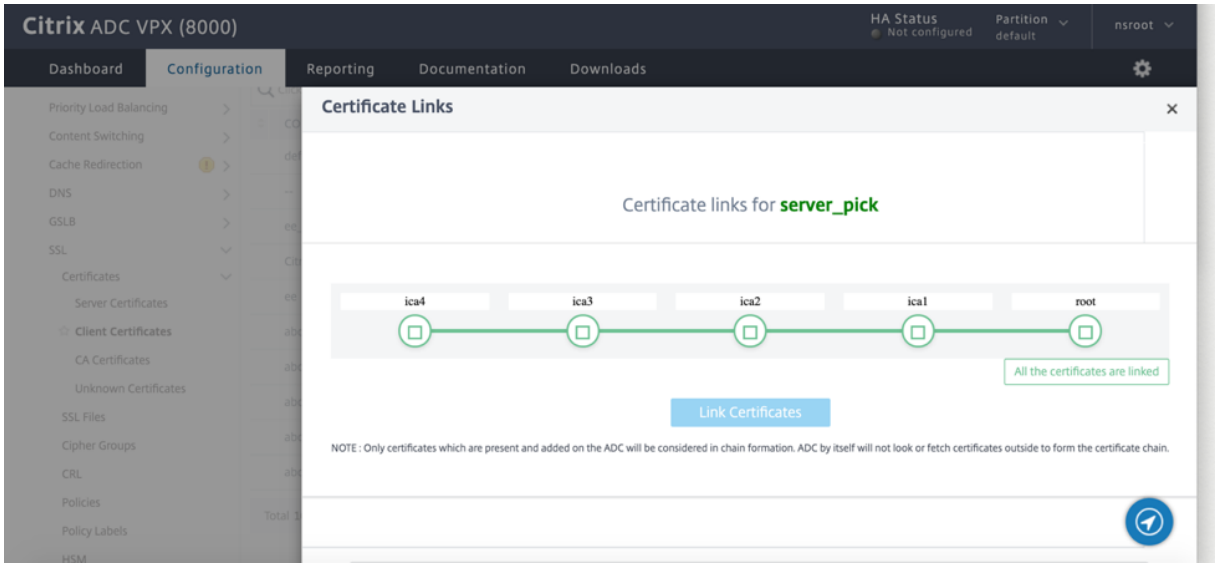
Sie müssen ein Zertifikat nicht mehr manuell mit seinem Aussteller bis zum Stammzertifikat verknüpfen. Wenn die Zwischenzertifikate der Zertifizierungsstelle und das Stammzertifikat auf der Appliance vorhanden sind, können Sie im Endbenutzerzertifikat auf die Schaltfläche **Verknüpfen** klicken.



Die potenzielle Kette erscheint.



Klicken Sie auf **Zertifikat verknüpfen**, um alle Zertifikate zu verknüpfen.



Erstellen Sie eine Kette von Zertifikaten

Anstatt eine Reihe von Zertifikaten (eine einzelne Datei) zu verwenden, können Sie eine Kette von Zertifikaten erstellen. Die Kette verknüpft das Serverzertifikat mit seinem Aussteller (der Zwischenzertifizierungsstelle). Dieser Ansatz erfordert, dass die Zwischenzertifikatsdatei der Zertifizierungsstelle auf der ADC-Appliance installiert ist und die Clientanwendung einem der Zertifikate in der Kette vertrauen muss. Verknüpfen Sie beispielsweise Cert-Intermediate-A mit Cert-Intermediate-B, wobei Cert-Intermediate-B mit Cert-Intermediate-C verknüpft ist, einem Zertifikat, dem die Clientanwendung vertraut.

Hinweis: Die Appliance unterstützt das Senden von maximal 10 Zertifikaten in der Kette der an den Client gesendeten Zertifikate (ein Serverzertifikat und neun CA-Zertifikate).

Erstellen einer Zertifikatkette mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Zertifikatkette zu erstellen und die Konfiguration zu überprüfen. (Wiederholen Sie den ersten Befehl für jedes neue Glied in der Kette.)

```
1 link ssl certkey <certKeyName> <linkCertKeyName>
2 show ssl certlink
3 <!--NeedCopy-->
```

Beispiel:


```
link ssl certkey siteAcertkey CAcertkey
Done

show ssl certlink

linked certificate:
       1) Cert Name: siteAcertkey CA Cert Name: CAcertkey
Done
<!--NeedCopy-->
```

Erstellen einer Zertifikatkette mit der GUI

1. Navigieren Sie zu **Traffic Management** > **SSL** > **Zertifikate**.
2. Wählen Sie ein Serverzertifikat aus, und wählen Sie in der Liste **Aktion** die Option **Verknüpfen**aus, und geben Sie einen CA-Zertifikatsnamen an.

Aktualisieren eines vorhandenen Serverzertifikats

Um ein vorhandenes Serverzertifikat manuell zu ändern, müssen Sie die folgenden Schritte ausführen:

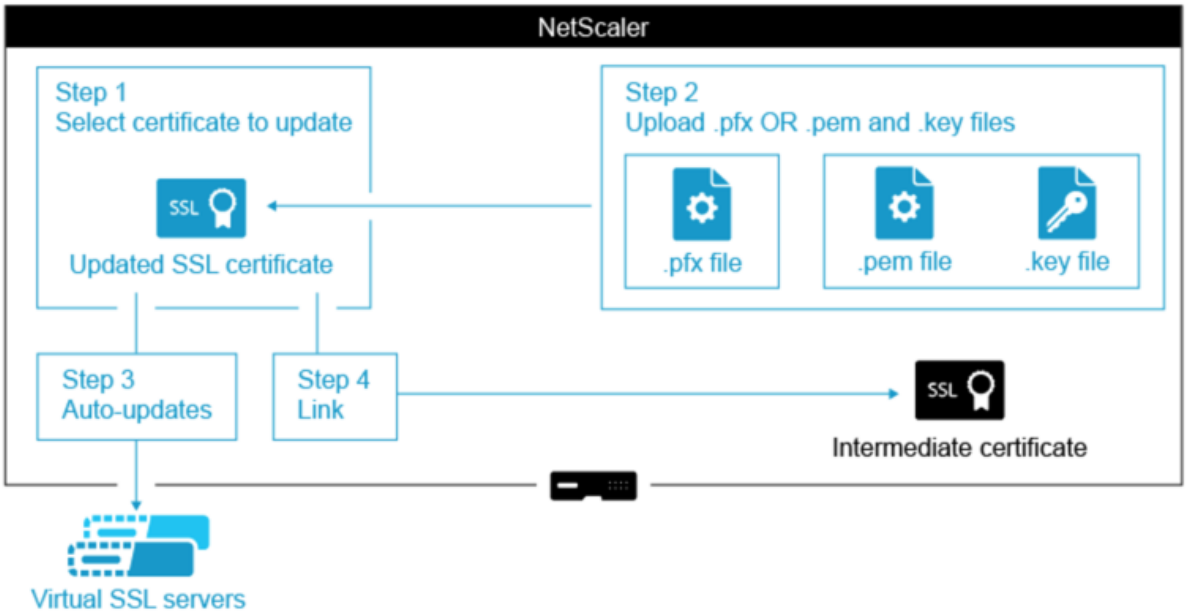
1. Trennen Sie das alte Zertifikat vom virtuellen Server.
2. Entfernen Sie das Zertifikat aus der Appliance.
3. Fügen Sie das neue Zertifikat der Appliance hinzu.
4. Binden Sie das neue Zertifikat an den virtuellen Server.

Um Ausfallzeiten beim Ersetzen eines Zertifikatsschlüsselpaars zu reduzieren, können Sie ein vorhandenes Zertifikat aktualisieren. Wenn Sie ein Zertifikat durch ein Zertifikat ersetzen möchten, das für eine andere Domäne ausgestellt wurde, müssen Sie Domänenprüfungen vor dem Aktualisieren des Zertifikats deaktivieren.

Um Benachrichtigungen über ablaufende Zertifikate zu erhalten, können Sie die Ablaufüberwachung aktivieren.

Wenn Sie ein Zertifikat von einem konfigurierten virtuellen SSL-Server oder -Dienst entfernen oder die Bindung aufheben, wird der virtuelle Server oder Dienst inaktiv. Sie sind aktiv, nachdem ein neues gültiges Zertifikat an sie gebunden wurde. Um Ausfallzeiten zu reduzieren, können Sie die Aktualisierungsfunktion verwenden, um ein Zertifikatsschlüsselpaar zu ersetzen, das an einen virtuellen SSL-Server oder einen SSL-Dienst gebunden ist.

Übersichtsdiagramm zum Aktualisieren eines SSL-Zertifikats auf der Citrix ADC-Appliance.



Videolink zu Wie aktualisiere ich ein vorhandenes Zertifikat.

Aktualisieren eines vorhandenen Zertifikatschlüsselpaars mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um ein vorhandenes Zertifikatsschlüsselpaar zu aktualisieren und die Konfiguration zu überprüfen:

```
update ssl certkey <certkeyName> -cert <string> -key <string>

show ssl certKey <certkeyName>
<!--NeedCopy-->
```

Beispiel:

```
update ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /
   nsconfig/ssl/pkey.pem

Done

show ssl certkey siteAcertkey

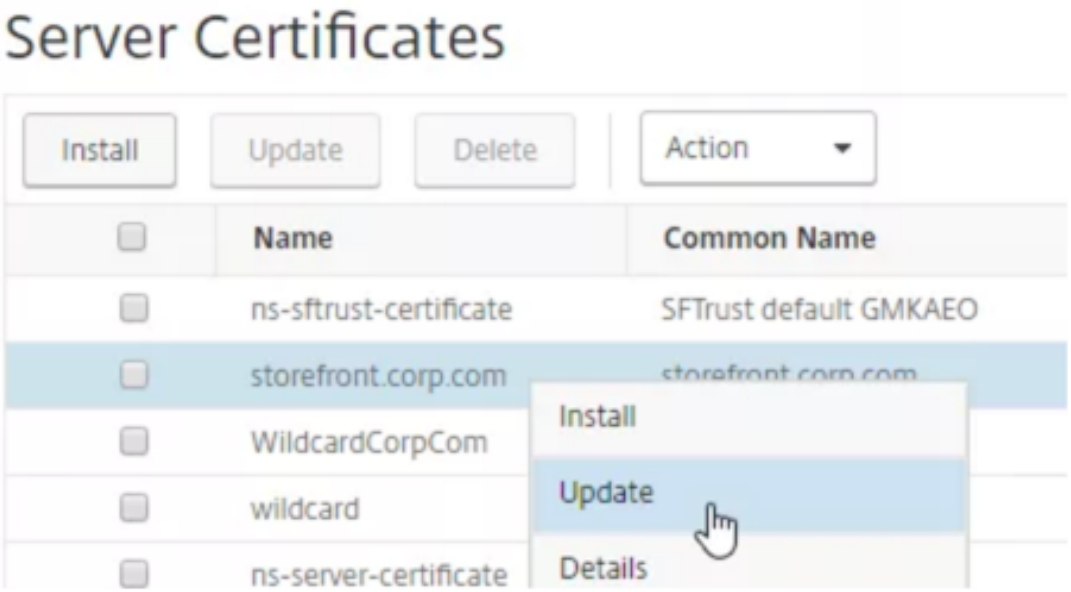
Name: siteAcertkey       Status: Valid
          Version: 3
          Serial Number: 02
          Signature Algorithm: md5WithRSAEncryption
```



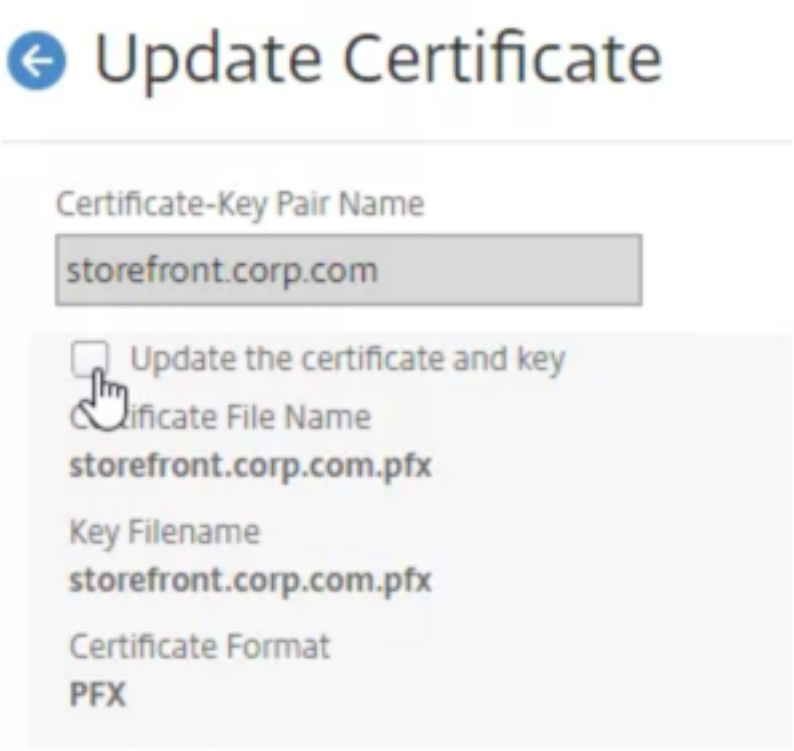
```
            Issuer: /C=US/ST=CA/L=Santa Clara/O=siteA/OU=Tech
            Validity
                 Not Before: Nov 11 14:58:18 2001 GMT
                 Not After: Aug 7 14:58:18 2004 GMT
            Subject: /C=US/ST-CA/L=San Jose/O=CA/OU=Security
            Public Key Algorithm: rsaEncryption
            Public Key size: 2048
Done
<!--NeedCopy-->
```

Aktualisieren eines vorhandenen Zertifikat-Schlüssel-Paars über die grafische Benutzeroberfläche

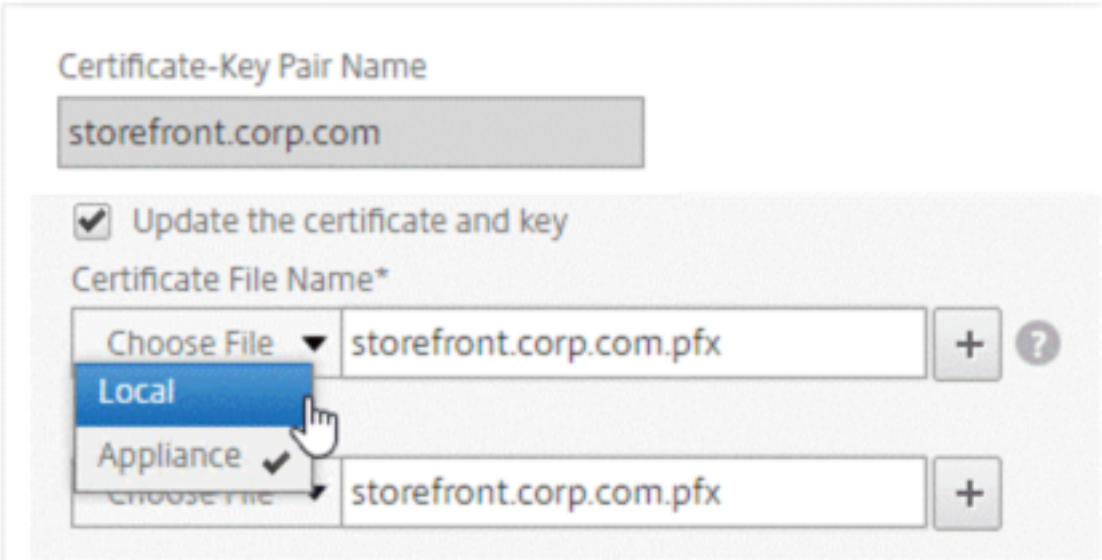
1. Navigieren Sie zu **Traffic Management** > **SSL** > **Zertifikate** > **Serverzertifikate**.
2. Wählen Sie das Zertifikat aus, das Sie aktualisieren möchten, und klicken Sie auf **Aktualisieren**.



3. Wählen Sie **Zertifikat und Schlüssel aktualisieren**aus.



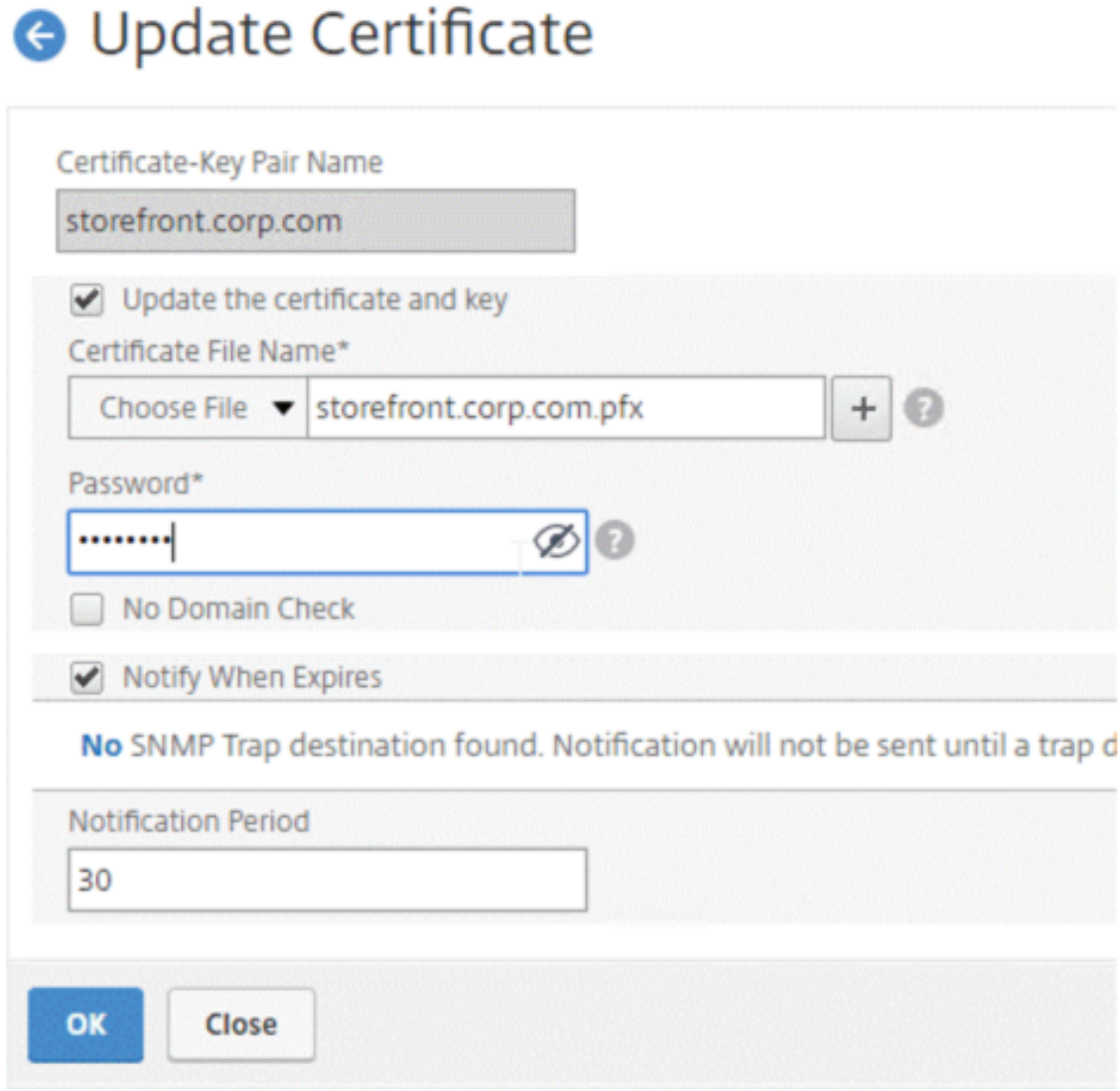
4. Klicken Sie **unter Zertifikatsdateiname**auf **Datei auswählen** > **Lokal**, und navigieren Sie zur aktualisierten PFX-Datei oder Zertifikats-PEM-Datei.



- Wenn Sie eine.pfx-Datei hochladen, werden Sie aufgefordert, das PFX-Dateikennwort anzugeben.
- Wenn Sie eine PEM-Datei für ein Zertifikat hochladen, müssen Sie auch eine Zertifikatsschlüsseldatei hochladen. Wenn der Schlüssel verschlüsselt ist, müssen Sie das Verschlüs-

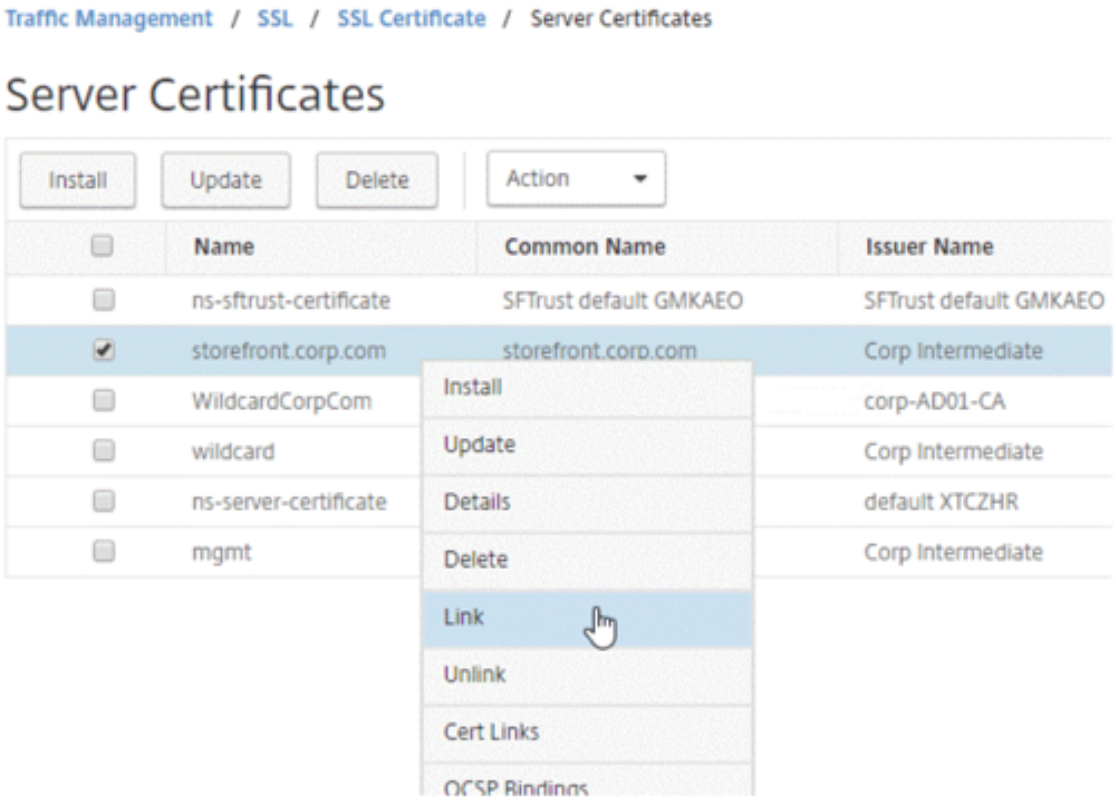
selungskennwort angeben.

5. Wenn der allgemeine Name des neuen Zertifikats nicht mit dem alten Zertifikat übereinstimmt, wählen Sie **Keine Domänenprüfung**aus.
6. Klicken Sie auf **OK**. Alle virtuellen SSL-Server, an die dieses Zertifikat gebunden ist, werden automatisch aktualisiert.



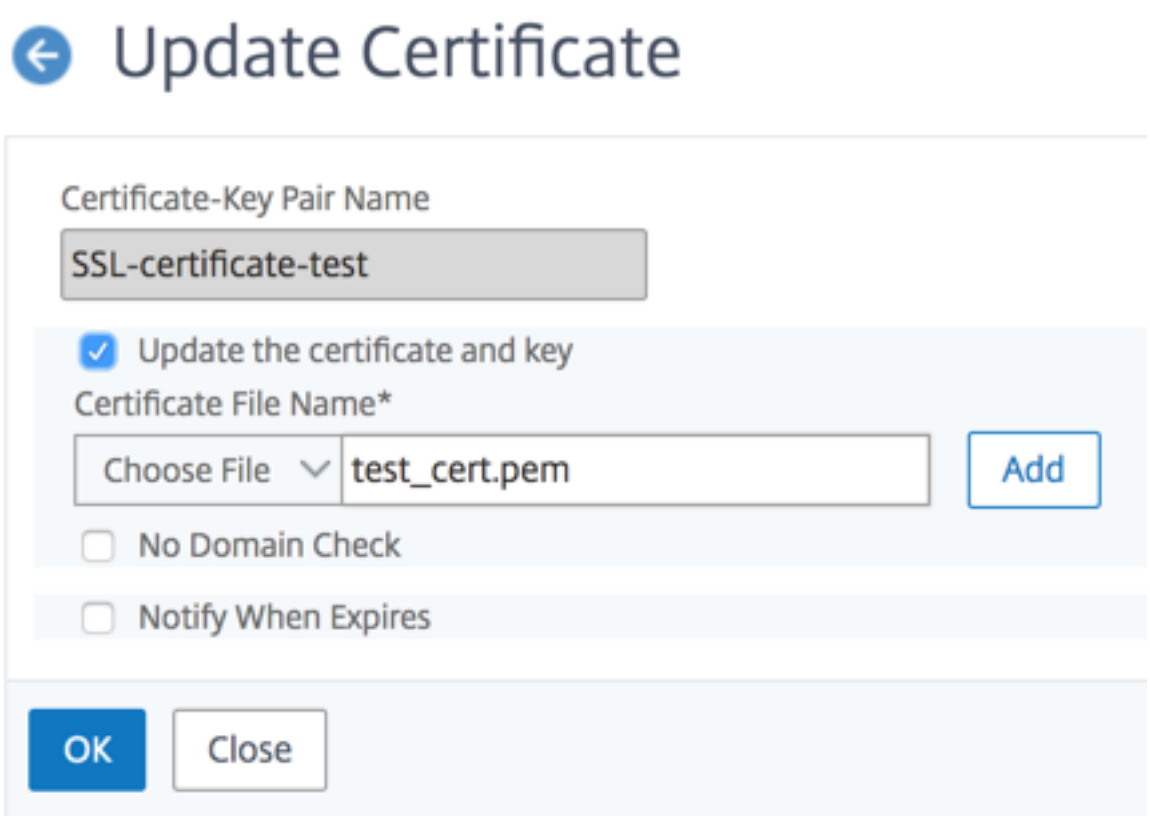
7. Nach dem Ersetzen des Zertifikats müssen Sie möglicherweise die Zertifikatverknüpfung auf ein neues Zwischenzertifikat aktualisieren. Weitere Informationen zum Aktualisieren eines Zwischenzertifikats ohne Unterbrechung der Links finden Sie unter Aktualisieren eines Zwischenzertifikats, ohne die Links zu unterbrechen.
   - Klicken Sie mit der rechten Maustaste auf das aktualisierte Zertifikat, und klicken Sie auf **Zertifikatverknüpfungen**, um festzustellen, ob es mit einem Zwischenzertifikat verknüpft ist.

- Wenn das Zertifikat nicht verknüpft ist, klicken Sie mit der rechten Maustaste auf das aktualisierte Zertifikat, und klicken Sie auf **Link**, um es mit einem Zwischenzertifikat zu verknüpfen. Wenn Sie keine Option zum Verknüpfen sehen, müssen Sie zuerst ein neues Zwischenzertifikat auf der Appliance unter dem Knoten **CA Certificates** installieren.



Aktualisieren eines vorhandenen CA-Zertifikats

Die Schritte zum Aktualisieren eines vorhandenen CA-Zertifikats entsprechen dem Aktualisieren eines vorhandenen Serverzertifikats. Der einzige Unterschied besteht darin, dass Sie bei CA-Zertifikaten keinen Schlüssel benötigen.



Deaktivieren Sie Domainprüfungen

Wenn ein SSL-Zertifikat auf der Appliance ersetzt wird, muss der auf dem neuen Zertifikat angegebene Domänenname mit dem Domänennamen des zu ersetzenden Zertifikats übereinstimmen. Wenn Sie beispielsweise ein Zertifikat für abc.com ausgestellt haben und es mit einem auf def.com ausgestellten Zertifikat aktualisieren, schlägt die Zertifikatsaktualisierung fehl.

Wenn Sie jedoch möchten, dass der Server, der eine bestimmte Domäne gehostet hat, eine neue Domäne hosten soll, deaktivieren Sie die Domänenprüfung, bevor Sie das Zertifikat aktualisieren.

Deaktivieren Sie die Domänenprüfung für ein Zertifikat mithilfe der CLI

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

```
update ssl certKey <certkeyName> -noDomainCheck

show ssl certKey <certkeyName>
<!--NeedCopy-->
```


Beispiel:

```
update ssl certKey sv -noDomainCheck

Done

show ssl certkey sv

Name: sv
Cert Path: /nsconfig/ssl/complete/server/server_rsa_512.pem
Key Path: /nsconfig/ssl/complete/server/server_rsa_512.ky
Format: PEM
Status: Valid,   Days to expiration:9349
Certificate Expiry Monitor: DISABLED
Done
<!--NeedCopy-->
```

Deaktivieren Sie die Domänenprüfung für ein Zertifikat über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > SSL > Zertifikate**, wählen Sie ein Zertifikat aus und klicken Sie auf **Aktualisieren**.
2. Wählen Sie **Keine Domainprüfung**aus.

Ersetzen Sie das Standardzertifikat einer ADC-Appliance durch ein vertrauenswürdiges CA-Zertifikat, das dem Hostnamen der Appliance entspricht

Das folgende Verfahren setzt voraus, dass das Standardzertifikat (`ns-server-certificate`) an die internen Dienste gebunden ist.

1. Navigieren Sie zu **Traffic Management > SSL > SSL-Zertifikate > Zertifikatsanforderung erstellen**.
2. Geben Sie im allgemeinen Namen ein `test.citrixadc.com`.
3. Reichen Sie die CSR an eine vertrauenswürdige Zertifizierungsstelle ein.
4. Nachdem Sie das Zertifikat von der vertrauenswürdigen Zertifizierungsstelle erhalten haben, kopieren Sie die Datei in das Verzeichnis `/nsconfig/ssl`.
5. Navigieren Sie zu **Traffic Management > SSL > Zertifikate > Serverzertifikate**.
6. Wählen Sie das Standard-Serverzertifikat (`ns-server-certificate`) aus und klicken Sie auf **Aktualisieren**.
7. Navigieren **Sie im Dialogfeld Zertifikat aktualisieren** unter **Certificate File Name zu dem Zertifikat**, das Sie nach dem Signieren von der Zertifizierungsstelle erhalten haben.

8. Geben Sie im Feld **Schlüsseldateiname** den standardmäßigen privaten Schlüsseldateinamen (`ns-server.key`) an.
9. Wählen Sie **Keine Domainprüfung**aus.
10. Klicken Sie auf **OK**.

Ablaufüberwachung aktivieren

Ein SSL-Zertifikat ist für einen bestimmten Zeitraum gültig. Eine typische Bereitstellung umfasst mehrere virtuelle Server, die SSL-Transaktionen verarbeiten, und die an sie gebundenen Zertifikate können zu unterschiedlichen Zeiten ablaufen. Ein auf der Appliance konfigurierter Ablaufmonitor erstellt Einträge in den Syslog- und NS-Überwachungsprotokollen der Appliance, wenn ein konfiguriertes Zertifikat abläuft.

Wenn Sie SNMP-Warnungen für den Ablauf des Zertifikats erstellen möchten, müssen Sie diese separat konfigurieren.

Aktivieren einer Ablaufüberwachung für ein Zertifikat mithilfe der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Ablaufüberwachung für ein Zertifikat zu aktivieren und die Konfiguration zu überprüfen:

```
set ssl certKey <certkeyName> [-expiryMonitor ( ENABLED | DISABLED ) [-
    notificationPeriod <positive_integer>]]

show ssl certKey <certkeyName>
<!--NeedCopy-->
```

Beispiel:

```
set ssl certKey sv -expiryMonitor ENABLED  - notificationPeriod 60
Done
<!--NeedCopy-->
```

Aktivieren einer Ablaufüberwachung für ein Zertifikat über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Traffic Management > SSL > Zertifikate**, wählen Sie ein Zertifikat aus und klicken Sie auf **Aktualisieren**.
2. Wählen Sie **Bei Ablauf benachrichtigen**aus, und geben Sie optional einen Benachrichtigungszeitraum an.

Aktualisieren Sie ein Zwischenzertifikat, ohne die Links zu unterbrechen

Sie können jetzt ein Zwischenzertifikat aktualisieren, ohne vorhandene Links zu trennen. Die Erweiterung “AuthorityKeyIdentifier” in dem verknüpften Zertifikat, das von dem zu ersetzenden Zertifikat ausgestellt wurde, darf kein Feld mit der Seriennummer des Autoritätszertifikats (“AuthorityCertSerialNumber”) enthalten. Wenn die Erweiterung ‘AuthorityKeyIdentifier’ ein Seriennummernfeld enthält, müssen die Seriennummern des alten und des neuen Zertifikats identisch sein. Sie können eine beliebige Anzahl von Zertifikaten im Link nacheinander aktualisieren, wenn die vorherige Bedingung erfüllt ist. Zuvor wurden die Links unterbrochen, wenn ein Zwischenzertifikat aktualisiert wurde.

Zum Beispiel gibt es vier Zertifikate: `CertACertB`, `CertC`, und `CertD`. Das Zertifikat `CertA` ist der Aussteller für `CertB`, `CertB` ist der Aussteller für `CertC`und so weiter. Wenn Sie ein Zwischenzertifikat `CertB` durch `CertB_new` ersetzen möchten, ohne die Verbindung zu unterbrechen, muss die folgende Bedingung erfüllt sein:

Die Seriennummer des Zertifikats von `CertB` muss mit der Seriennummer des Zertifikats von `CertB_new` übereinstimmen, wenn beide der folgenden Bedingungen erfüllt sind:

- Die Erweiterung `AuthorityKeyIdentifier` ist in `CertC` vorhanden.
- Diese Erweiterung enthält ein Seriennummernfeld.

Wenn sich der allgemeine Name in einem Zertifikat ändert, geben Sie beim Aktualisieren des Zertifikats an `nodomaincheck`.

Um im vorherigen Beispiel “www.example.com” in `CertD` zu “*.example.com” zu ändern, wählen Sie den Parameter “No Domain Check” aus.

Aktualisieren Sie das Zertifikat mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
update ssl certKey <certkeyName> -cert <string> [-password] -key <
    string>  [-noDomainCheck]
<!--NeedCopy-->
```

Beispiel:

```
update ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /
    nsconfig/ssl/pkey.pem -noDomainCheck
<!--NeedCopy-->
```


Eine Zertifikatkette anzeigen

Ein Zertifikat enthält den Namen der ausstellenden Behörde und den Antragsteller, für den das Zertifikat ausgestellt wurde. Um ein Zertifikat zu validieren, müssen Sie sich den Aussteller dieses Zertifikats ansehen und bestätigen, ob Sie dem Aussteller vertrauen. Wenn Sie dem Aussteller nicht vertrauen, müssen Sie sehen, wer das Ausstellerzertifikat ausgestellt hat. Gehen Sie die Kette hoch, bis Sie das Stammzertifizierungsstellenzertifikat oder einen Aussteller erreichen, dem Sie vertrauen.

Wenn ein Client im Rahmen des SSL-Handshakes ein Zertifikat anfordert, präsentiert die Appliance ein Zertifikat und die Kette der Ausstellerzertifikate, die auf der Appliance vorhanden sind. Ein Administrator kann die Zertifikatkette für die auf der Appliance vorhandenen Zertifikate anzeigen und fehlende Zertifikate installieren.

Zeigen Sie die Zertifikatkette für die auf der Appliance vorhandenen Zertifikate mithilfe der CLI an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show ssl certchain <cert_name>
<!--NeedCopy-->
```

Beispiele

Es gibt 3 Zertifikate: c1, c2 und c3. Zertifikat c3 ist das Stammzertifikat der Zertifizierungsstelle und signiert c2 und c2-Zeichen c1. Die folgenden Beispiele veranschaulichen die Ausgabe des `show ssl certchain c1` Befehls in verschiedenen Szenarien.

Szenario 1:

Das Zertifikat c2 ist mit c1 verknüpft, und c3 ist mit c2 verknüpft.

Das Zertifikat c3 ist ein Stammzertifikat der Zertifizierungsstelle.

Wenn Sie den folgenden Befehl ausführen, werden die Zertifikatsverknüpfungen zum Stammzertifikat der Zertifizierungsstelle angezeigt.

```
show ssl certchain c1

Certificate chain details of certificate name c1 are:
    1) Certificate name: c2              linked; not a root
       certificate
    2) Certificate name: c3              linked; root certificate
```



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

Szenario 2:

Das Zertifikat c2 ist mit c1 verknüpft.

Das Zertifikat c2 ist kein Stammzertifikat der Zertifizierungsstelle.

Wenn Sie den folgenden Befehl ausführen, werden die Informationen angezeigt, dass das Zertifikat c3 ein Stammzertifikat der Zertifizierungsstelle ist, aber nicht mit c2 verknüpft ist.

```
1 show ssl certchain c1
2
3 Certificate chain  details of certificate name c1 are:
4     1) Certificate Name: c2               linked; not a root
         certificate
5     2) Certificate Name: c3               not linked; root certificate
6     Done
7 <!--NeedCopy-->
```

Szenario 3:

Zertifikat c1, c2 und c3 sind nicht verknüpft, aber auf der Appliance vorhanden.

Wenn Sie den folgenden Befehl ausführen, werden Informationen zu allen Zertifikaten angezeigt, die mit dem Aussteller des Zertifikats c1 beginnen. Es wird auch angegeben, dass die Zertifikate nicht verknüpft sind.

```
1 show ssl certchain c1
2
3 Certificate chain details of certificate name c1 are:
4     1) Certificate Name: c2               not linked; not a root
         certificate
5     2) Certificate Name: c3               not linked; root certificate
6     Done
7 <!--NeedCopy-->
```

Szenario 4:

Das Zertifikat c2 ist mit c1 verknüpft.

Das Zertifikat c3 ist auf der Appliance nicht vorhanden.

Wenn Sie den folgenden Befehl ausführen, werden Informationen über das mit c1 verknüpfte Zertifikat angezeigt. Sie werden aufgefordert, ein Zertifikat mit dem in c2 angegebenen Antragstellernamen hinzuzufügen. In diesem Fall wird der Benutzer aufgefordert, das Stammzertifizierungsstellenzertifikat c3 hinzuzufügen.

```
show ssl certchain c1

Certificate chain details of certificate name c1 are:
    1) Certificate Name: c2                linked; not a root
       certificate
    2) Certificate Name: /C=IN/ST=ka/O=netscaler/CN=test
       Action: Add a certificate with this subject name.
Done
<!--NeedCopy-->
```

Szenario 5:

Ein Zertifikat ist nicht mit dem Zertifikat c1 verknüpft, und das Ausstellerzertifikat von c1 ist auf der Appliance nicht vorhanden.

Wenn Sie den folgenden Befehl ausführen, werden Sie aufgefordert, ein Zertifikat mit dem Antragstellernamen in Zertifikat c1 hinzuzufügen.

```
sh ssl certchain c1

Certificate chain details of certificate name c1 are:
    1) Certificate Name: /ST=KA/C=IN
       Action: Add a certificate with this subject name.
<!--NeedCopy-->
```

Erstellen eines Servertestzertifikats

December 7, 2021

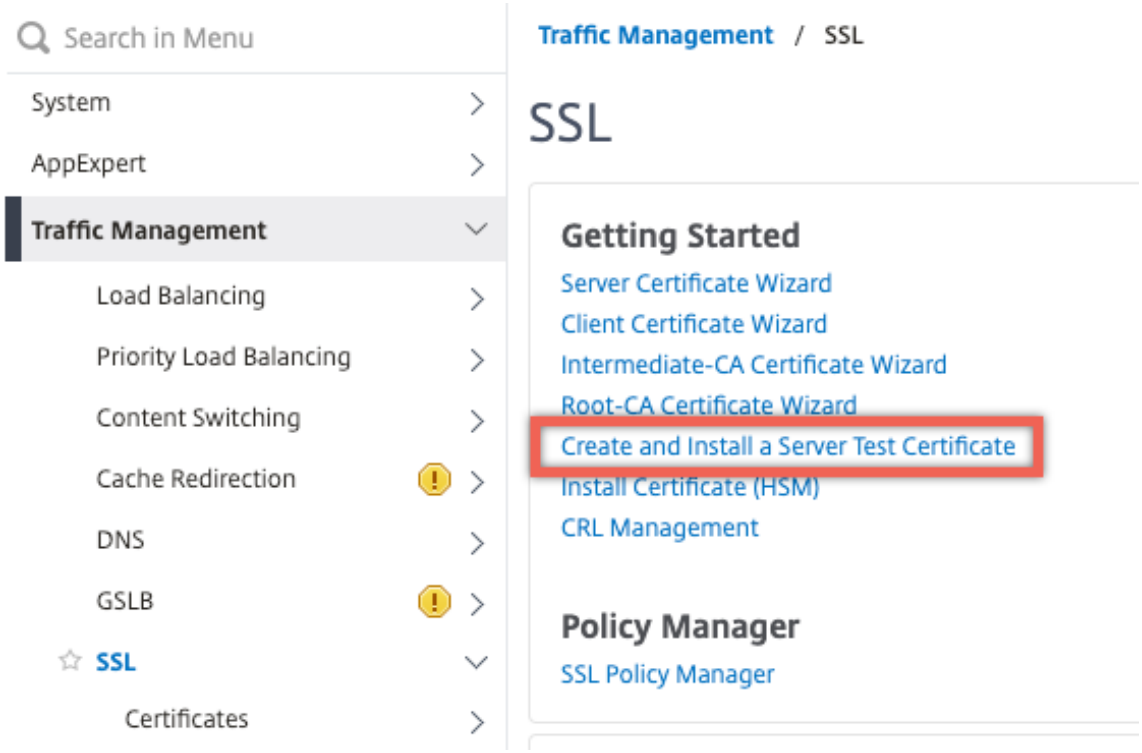
Mit der Citrix ADC Appliance können Sie mithilfe eines GUI-Assistenten im Konfigurationsdienstprogramm ein Testzertifikat für die Serverauthentifizierung erstellen. Ein Serverzertifikat wird verwendet, um einen Server in einem SSL-Handshake zu authentifizieren und zu identifizieren. Normalerweise gibt eine vertrauenswürdige Zertifizierungsstelle ein Serverzertifikat aus. Der Server sendet das Zertifikat an einen Client, der es zur Authentifizierung des Servers verwendet.

Für die Ausstellung eines Servertest-Zertifikats arbeitet die Appliance als Zertifizierungsstelle. Dieses Zertifikat kann zur Authentifizierung in einem SSL-Handshake mit einem Client an einen virtuellen SSL-Server gebunden werden. Dieses Zertifikat dient nur zu Testzwecken. Verwenden Sie nicht in einer Produktionsumgebung.

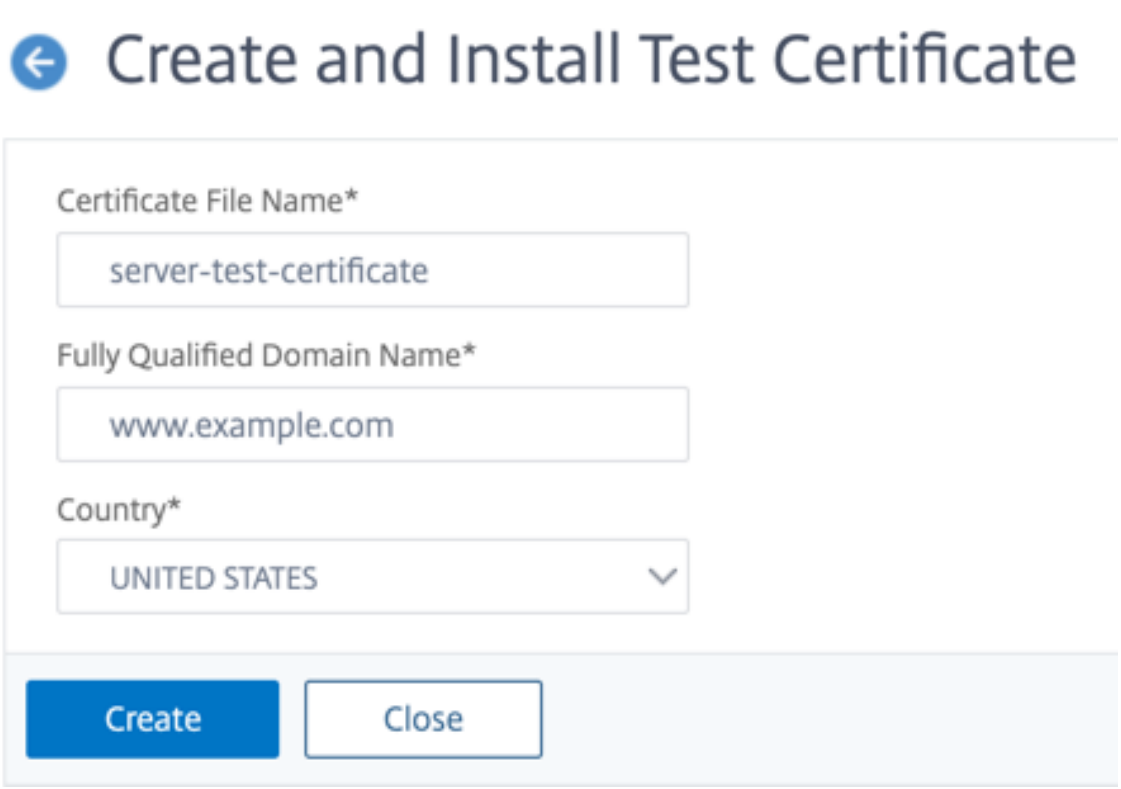
Sie können das Servertestzertifikat auf jedem virtuellen Server installieren, der das SSL- oder das SSL_TCP-Protokoll verwendet.

Generieren eines Servertestzertifikats mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL** und wählen Sie in der **Gruppe SSL Certificates Create and Install a Server Test Certificate**aus.



2. Geben Sie Details für die Parameter ein und klicken Sie auf **Erstellen**.



Importieren und Konvertieren von SSL-Dateien

October 5, 2021

Sie können jetzt SSL-Ressourcen wie Zertifikate, private Schlüssel, CRLs und DH-Schlüssel von Remote-Hosts importieren, selbst wenn der FTP-Zugriff auf diese Hosts nicht verfügbar ist. Diese Funktion ist besonders in Umgebungen hilfreich, in denen der Shell-Zugriff auf den Remote-Host eingeschränkt ist. Standardordner werden in /nsconfig/ssl wie folgt erstellt:

- Für Zertifikatdateien: /nsconfig/ssl/certfile
- Für private Schlüssel: die Datei /nsconfig/ssl/keyfile
- Für CRLs: /var/netscaler/ssl/crlfile
- Für DH-Tasten: /nsconfig/ssl/dhfile

Importe von HTTP- und HTTPS-Servern werden unterstützt. Der Import schlägt jedoch fehl, wenn sich die Datei auf einem HTTPS-Server befindet, der Clientzertifikatauthentifizierung für den Zugriff erfordert.

> **Hinweis:**

> Der Befehl import wird nicht in der Konfigurationsdatei (ns.conf) gespeichert, da das erneute Importieren der Datei nach einem Neustart einen Fehler verursachen kann.

Importieren einer Zertifikatdatei

Sie können CLI und GUI verwenden, um eine Datei (Ressource) von einem Remote-Host zu importieren.

Importieren einer Zertifikatdatei von einem Remote-Host mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import ssl certFile [<name>] [<src>]
<!--NeedCopy-->
```

Beispiel:

```
import ssl certfile my-certfile http://www.example.com/file_1
<!--NeedCopy-->
```

```
show ssl certfile
     Name : my-certfile
     URL : http://www.example.com/file_1
<!--NeedCopy-->
```

Um eine Zertifikatsdatei zu entfernen, verwenden Sie den `rm ssl certFile` Befehl, der nur das Argument “Name” akzeptiert.

Importieren einer Schlüsseldatei von einem Remote-Host mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import ssl keyFile [<name>] [<src>]
<!--NeedCopy-->
```

Beispiel:


```
import ssl keyfile my-keyfile http://www.example.com/key_file
<!--NeedCopy-->
```

```
show ssl keyfile
     Name : my-keyfile
     URL : http://www.example.com/key_file
<!--NeedCopy-->
```

Um eine Schlüsseldatei zu entfernen, verwenden Sie den `rm ssl keyFile` Befehl, der nur das Argument “Name” akzeptiert.

Importieren einer CRL-Datei von einem Remote-Host mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import ssl crlFile [<name>] [<src>]
<!--NeedCopy-->
```

Um eine CRL-Datei zu entfernen, verwenden Sie den `rm ssl crlFile` Befehl, der nur das <name> Argument akzeptiert.

Beispiel:

```
import ssl crlfile my-crlfile http://www.example.com/crl_file

show ssl crlfile

    Name : my-crlfile
    URL : http://www.example.com/crl_file
<!--NeedCopy-->
```

Importieren einer DH-Datei von einem Remote-Host mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import ssl dhFile [<name>] [<src>]
<!--NeedCopy-->
```


Beispiel:

```
import ssl dhfile my-dhfile http://www.example.com/dh_file
show ssl dhfile
     Name : my-dhfile
     URL : http://www.example.com/dh_file
<!--NeedCopy-->
```

Um eine DH-Datei zu entfernen, verwenden Sie den `rm ssl dhFile` Befehl, der nur das <name> Argument akzeptiert.

Importieren einer SSL-Ressource mit der GUI

Navigieren Sie zu **Traffic Management > SSL > Importe**, und wählen Sie dann die entsprechende Registerkarte aus.

Importieren von PKCS #8 und PKCS #12 Zertifikaten

Wenn Sie Zertifikate und Schlüssel verwenden möchten, die bereits auf anderen sicheren Servern oder Anwendungen im Netzwerk vorhanden sind, können Sie diese exportieren und anschließend in die Citrix ADC Appliance importieren. Möglicherweise müssen Sie exportierte Zertifikate und Schlüssel konvertieren, bevor Sie sie in die Citrix ADC Appliance importieren können.

Weitere Informationen zum Exportieren von Zertifikaten von sicheren Servern oder Anwendungen in Ihrem Netzwerk finden Sie in der Dokumentation des Servers oder der Anwendung, von dem Sie exportieren möchten.

> **Hinweis:**
>
> Für die Installation auf der Citrix ADC Appliance dürfen Schlüssel- und Zertifikatnamen keine Leerzeichen oder Sonderzeichen enthalten, außer den vom UNIX-Dateisystem unterstützten Zeichen. Befolgen Sie die entsprechende Namenskonvention, wenn Sie den exportierten Schlüssel und das Zertifikat speichern.

Ein Zertifikat und ein privates Schlüsselpaar werden üblicherweise im PKCS #12 Format gesendet. Die Appliance unterstützt PEM- und DER-Formate für Zertifikate und Schlüssel. Informationen zum Konvertieren von PKCS #12 in PEM oder DER oder PEM oder DER in PKCS #12 finden Sie im Abschnitt Konvertieren von SSL-Zertifikaten für den Import oder Export weiter unten auf dieser Seite.

Die Citrix ADC Appliance unterstützt keine PEM-Schlüssel im PKCS #8 -Format. Sie können diese Schlüssel jedoch in ein unterstütztes Format konvertieren, indem Sie die OpenSSL-Schnittstelle verwenden, auf die Sie über die Befehlszeilenschnittstelle oder das Konfigurationsdienstprogramm

zugreifen können. Bevor Sie den Schlüssel konvertieren, müssen Sie überprüfen, ob der private Schlüssel im PKCS #8 Format ist. Schlüssel im PKCS #8 Format beginnen in der Regel mit folgendem Text:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----


leuSSZQZKgrgUQ==


-----END ENCRYPTED PRIVATE KEY-----
<!--NeedCopy-->
```

Öffnen Sie die OpenSSL-Schnittstelle über die CLI

1. Öffnen Sie eine SSH-Verbindung zur Appliance mit einem SSH-Client, z. B. PuTTY.
2. Melden Sie sich mit den Administratoranmeldeinformationen bei der Appliance an.
3. Geben Sie an der Eingabeaufforderung shell ein.
4. Geben Sie an der `openssl`Shell-Eingabeaufforderung ein

Öffnen Sie die OpenSSL-Schnittstelle über die GUI

Navigieren Sie zu **Traffic Management > SSL** und wählen Sie in der Gruppe Tools die Option **OpenSSL interface**aus.

Konvertieren Sie ein nicht unterstütztes PKCS #8 Schlüsselformat mithilfe der OpenSSL-Schnittstelle in ein verschlüsseltes unterstütztes Schlüsselformat

Geben Sie an der OpenSSL-Eingabeaufforderung einen der folgenden Befehle ein, je nachdem, ob das nicht unterstützte Tastenformat vom Typ RSA oder ECDSA ist:

```
OpenSSL>rsa- in <PKCS#8 Key Filename> -des3 -out <encrypted Key
   Filename>

OpenSSL>ec -in <PKCS#8 Key Filename> -des3 -out <encrypted Key Filename
   >
<!--NeedCopy-->
```


Parameter zum Konvertieren eines nicht unterstützten Schlüsselformats in ein unterstütztes Schlüsselformat

- **PKCS #8 Schlüsseldateiname:** Der Name der Eingabedatei des inkompatiblen PKCS #8 privaten Schlüssels.
- **verschlüsselter Schlüsseldateiname:** Der Ausgabedateiname des kompatiblen verschlüsselten privaten Schlüssels im PEM-Format.
- **unverschlüsselter Schlüsseldateiname:** Der Ausgabedateiname des kompatiblen unverschlüsselten privaten Schlüssels im PEM-Format.

Konvertieren von SSL-Zertifikaten für den Import oder Export

Eine Citrix ADC Appliance unterstützt die PEM- und DER-Formate für SSL-Zertifikate. Andere Anwendungen, wie Client-Browser und einige externe sichere Server, erfordern verschiedene PKCS-Formate (Public Key Cryptography Standard). Die Appliance kann das PKCS #12 -Format in das PEM- oder DER-Format konvertieren, um ein Zertifikat in die Appliance zu importieren, und kann PEM oder DER zum Exportieren eines Zertifikats in PKCS #12 konvertieren. Für mehr Sicherheit kann die Konvertierung einer Datei für den Import die Verschlüsselung des privaten Schlüssels mit dem DES- oder DES3-Algorithmus umfassen.

> **Hinweis:**
>
> Wenn Sie die GUI verwenden, um ein PKCS #12 -Zertifikat zu importieren, und das Kennwort ein Dollarzeichen ($), ein Backquote (‘) oder ein Escape () -Zeichen enthält, schlägt der Import möglicherweise fehl. Wenn dies der Fall ist, wird die Meldung FEHLER: Ungültiges Kennwort angezeigt. Wenn Sie ein Sonderzeichen im Kennwort verwenden müssen, stellen Sie sicher, dass Sie ihm ein Escape-Zeichen () voranstellen, es sei denn, alle Importe werden mit der CLI ausgeführt.

Konvertieren des Formats eines Zertifikats mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
convert ssl pkcs12 <outfile> [-import [-pkcs12File <inputFilename>] [-
    des | -des3] [-export [-certFile <inputFilename>] [-keyFile <
    inputFilename>]]
<!--NeedCopy-->
```

Während des Vorgangs werden Sie aufgefordert, ein Importkennwort oder ein Exportkennwort einzugeben. Bei einer verschlüsselten Datei werden Sie außerdem aufgefordert, eine Passphrase einzugeben.

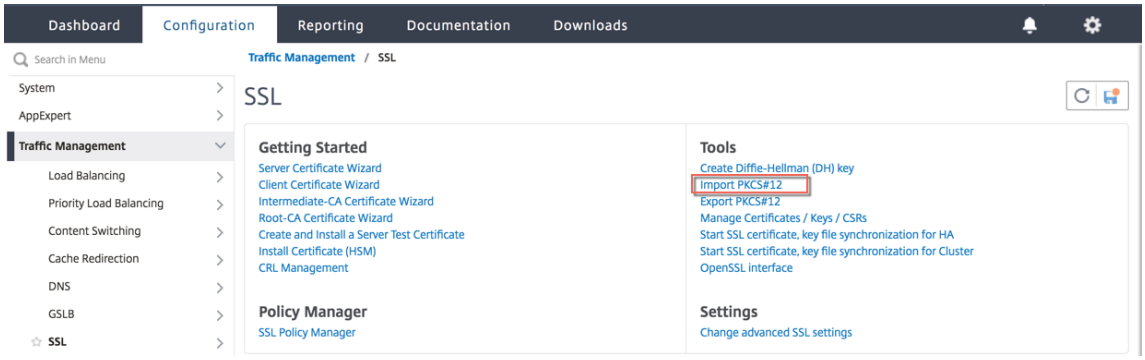
Beispiel:

```
convert ssl pkcs12 Cert-Import-1.pem -import -pkcs12File Cert-Import-1.pfx -des

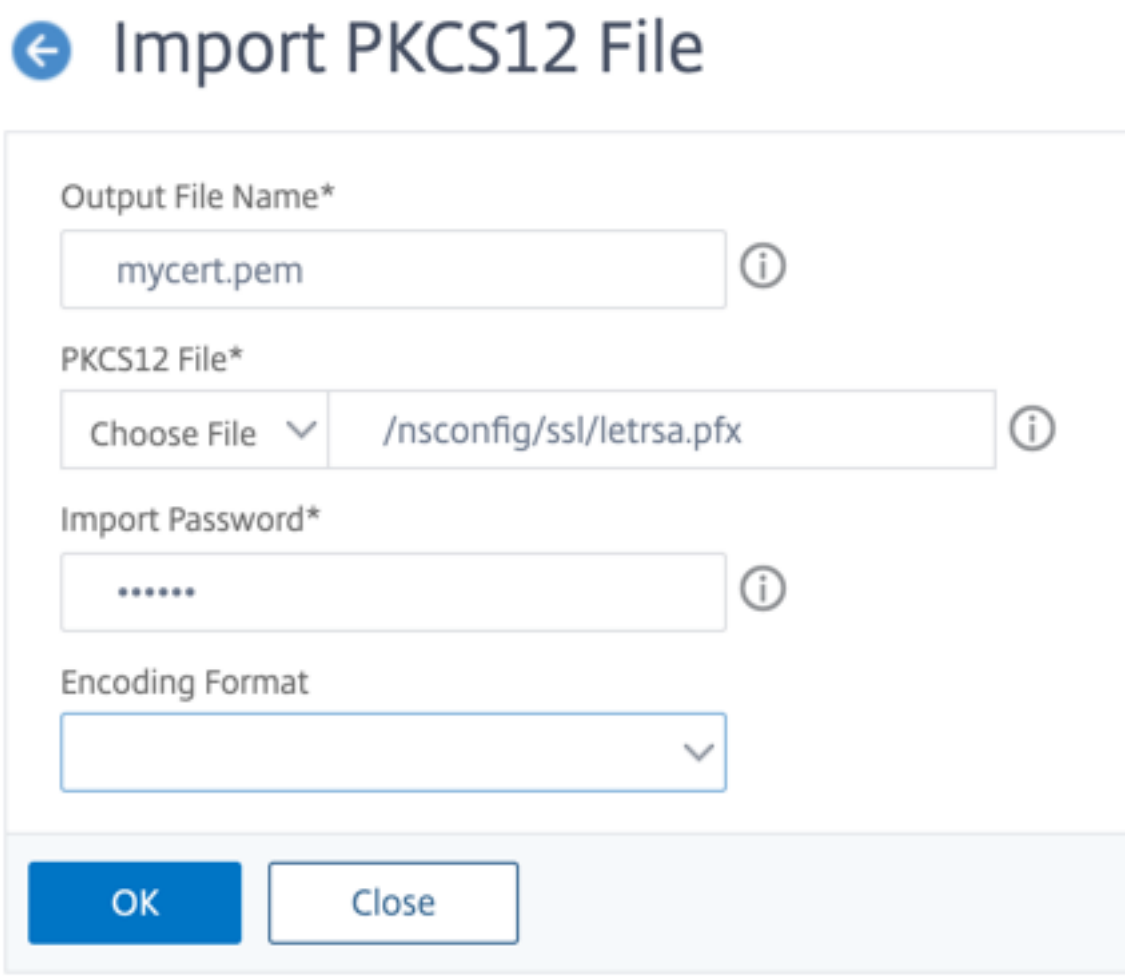
convert ssl pkcs12 Cert-Client-1.pfx -export -certFile Cert-Client-1 -keyFile Key-Client-1
<!--NeedCopy-->
```

Konvertieren des Formats eines Zertifikats mit der GUI

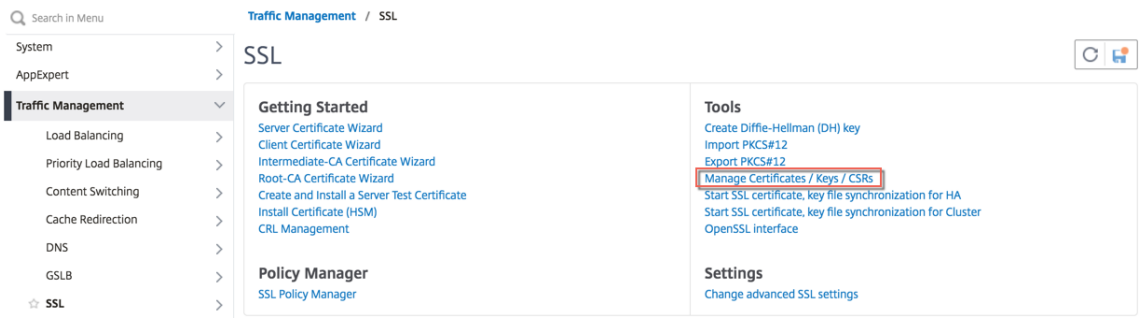
1. Navigieren Sie zu **Traffic Management > SSL** und wählen Sie in der Gruppe **Tools** die Option **PKCS #12 importieren**.



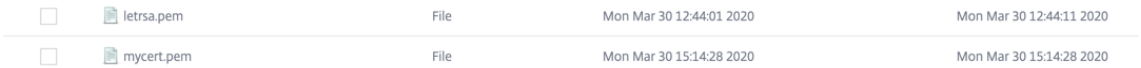
2. Geben Sie den Namen des PEM-Zertifikats im Feld **Ausgabedateiname** an.
3. Navigieren Sie zum Speicherort des PFX-Zertifikats auf Ihrem lokalen Computer oder der Appliance.



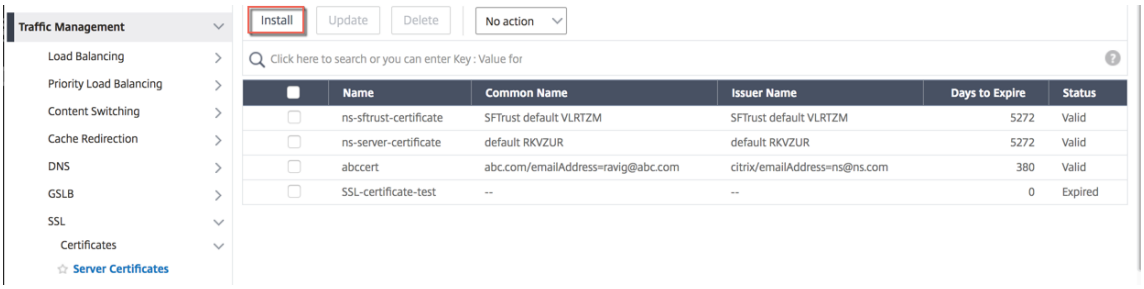
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Zertifikat/Schlüssel/CSRs verwalten**, um die konvertierte PEM-Datei anzuzeigen.



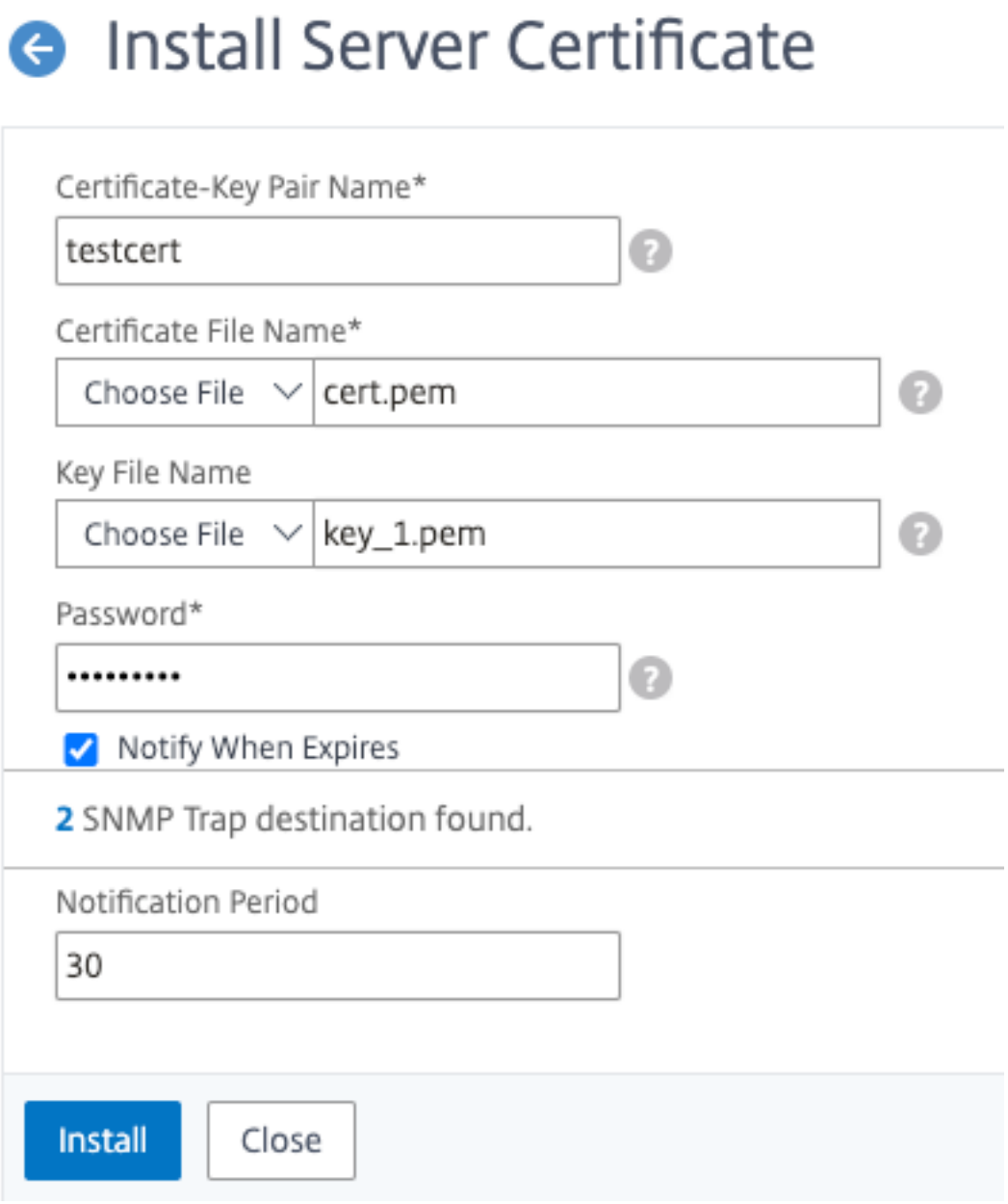
6. Sie können die hochgeladene PFX-Datei und die konvertierte PEM-Datei anzeigen.



7. Navigieren Sie zu **SSL** > **Zertifikate** > **Serverzertifikate**, und klicken Sie auf **Installieren** .



8. Geben Sie den **Namen eines Zertifikatschlüsselpaares**an.
9. Navigieren Sie zum Speicherort der PEM-Datei.
10. Geben Sie das Kennwort an, wenn Sie dazu aufgefordert werden.
11. Klicken Sie auf **Installieren**.



12. Binden Sie das Zertifikatschlüsselpaar an einen virtuellen SSL-Server.

Bind an SSL certificate to a virtual server on the Citrix ADC appliance

December 7, 2021

An SSL certificate is an essential part of SSL encryption and decryption processes. The certificate is used during an SSL handshake to establish the identity of the SSL server, which is the Citrix ADC appliance as it acts as the SSL termination point for the clients.

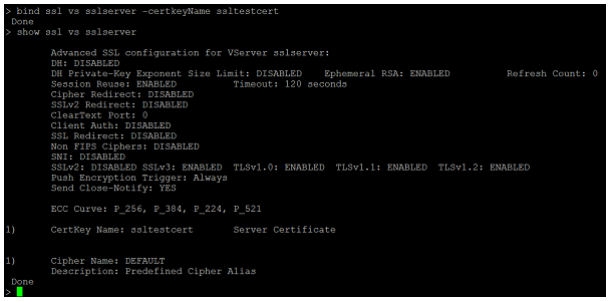
The certificate used for processing the SSL transactions must be bound to the virtual server (SSL) that receives the SSL data.

To bind an SSL certificate to an SSL virtual server using the command line interface

At the command prompt, type:

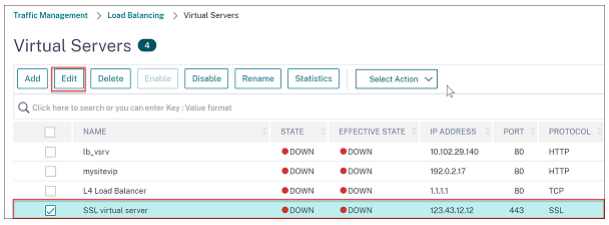
```
bind ssl vs <vServerName> -certkeyName <certificate-KeyPairName>
show ssl vs <vServerName>
<!--NeedCopy-->
```

Example:



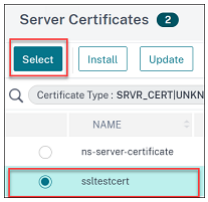
To bind an SSL certificate to an SSL virtual server using the GUI

1. Navigate to **Traffic Management > Load Balancing > Virtual Servers**.
2. Select a virtual server of type SSL and click **Edit**.



3. In the **Load Balancing Virtual Server** page, under the **Certificates** section, click **No Server Certificate**.

4. In the **Server Certificate Binding** page, click **Click to select**.
5. Select the SSL certificate and click **Select**.



6. Click **Bind** to bind the SSL certificate to the virtual server.
7. Click **Done**.

   You have completed binding the SSL certificate to the virtual server.

SSL-Profile

October 5, 2021

Ein SSL-Profil ist eine Sammlung von Einstellungen für SSL-Entitäten. Es bietet einfache Konfiguration und Flexibilität. Anstatt die Einstellungen für jede Entität zu konfigurieren, können Sie sie in einem Profil konfigurieren und das Profil an alle Entitäten binden, für die die Einstellungen gelten.

Die SSL-Profilinfrastruktur wurde erweitert, um die neuesten Verschlüsselungen und Protokolle zu verwenden. Unterschiede zwischen dem Legacy-Profil (altes Profil) und dem erweiterten SSL-Profil (neues Profil) werden hervorgehoben.

Unterschiede zwischen der alten und der neuen SSL-Profilinfrastruktur

Unterschiede	Altes Profil	Neues Profil
Chiffre und ECC-Kurven im Profil enthalten	Nein	Ja
Einfügen einer Chiffre- oder Chiffregruppe in der Mitte einer vorhandenen Liste	Heben Sie die Bindung aller Chiffre auf und binden Sie sie erneut in der Reihenfolge der erforderlichen Priorität.	Fügen Sie eine Chiffre hinzu und weisen Sie ihr eine Priorität zu. Wenn keine Priorität angegeben wird, wird der Chiffre die niedrigste Priorität in der Liste zugewiesen.

Unterschiede	Altes Profil	Neues Profil
Aufheben der Bindung aller Chiffre	`unbind ssl vserver \<name\> ciphername -ALL`	`unbind ssl profile -cipherName FlushAllCiphers` (Release 11.0 build 64.x oder höher enthält den Parameter FlushAllCiphers zum Aufheben der Bindung aller Chiffrier- oder Chiffriergruppen von einem Profil, da ALL wie eine Chiffriergruppe behandelt wird.)
Status von SSLv3	–	Deaktiviert im Standard-Front-End-Profil (ns_default_ssl_profile_frontend). Hinweis: Bevor Sie dieses Profil aktivieren, wird SSLv3 global aktiviert. Nach dem Aktivieren des Profils wird SSLv3 für das Front-End-Standardprofil deaktiviert.

SSL-Profilinfrastruktur

October 5, 2021

Sicherheitsanfälligkeiten in der SSLv3- und RC4-Implementierung haben betont, dass die neuesten Verschlüsselungen und Protokolle verwendet werden müssen, um die Sicherheitseinstellungen für eine Netzwerkverbindung auszuhandeln. Das Implementieren von Änderungen an der Konfiguration, wie das Deaktivieren von SSLv3 über Tausende von SSL-Endpunkten, ist ein umständlicher Prozess. Daher wurden Einstellungen, die Teil der SSL-Endpunktkonfiguration waren, zusammen mit den Standardverschlüsselungen in die SSL-Profile verschoben. Um Änderungen in der Konfiguration zu implementieren, einschließlich der Verschlüsselungsunterstützung, müssen Sie nur das Profil ändern, das an die Entitäten gebunden ist.

Die Standard-Front-End- und Standard-Back-End-SSL-Profile enthalten zusätzlich zu den Einstellun-

gen, die Teil der alten Profile waren, alle Standardchiffrier- und ECC-Kurven. Beispielausgaben für die Standardprofile sind im Anhang enthalten. Der Vorgang Standardprofil aktivieren bindet das Standard-Front-End-Profil automatisch an alle Front-End-Entitäten und das Standard-Back-End-Profil an alle Back-End-Entitäten. Sie können ein Standardprofil entsprechend Ihrer Bereitstellung ändern. Sie können auch benutzerdefinierte Profile erstellen und an SSL-Entitäten binden.

Das Front-End-Profil enthält Parameter, die für eine Front-End-Entität gelten. Das heißt, sie gelten für die Entität, die Anforderungen von einem Client empfängt. In der Regel handelt es sich bei dieser Entität um einen virtuellen SSL-Server oder einen transparenten SSL-Dienst auf der Citrix ADC Appliance. Das Back-End-Profil enthält Parameter, die für eine Backend-Entität gelten. Das heißt, sie gelten für die Entität auf der ADC-Appliance, die Client-Anfragen an einen Back-End-Server sendet. In der Regel ist diese Entität ein SSL-Dienst auf der Citrix ADC Appliance. Wenn Sie versuchen, einen nicht unterstützten Parameter zu konfigurieren, wird der Fehler `ERROR: Specified parameters are not applicable for this type of SSL profile` angezeigt.

> **Wichtig:**
>
> - Ein SSL-Profil hat Vorrang vor SSL-Parametern. Das heißt, wenn Sie SSL-Parameter mit dem `set ssl parameter` Befehl konfigurieren und später ein Profil an eine SSL-Entität binden, haben die Einstellungen im Profil Vorrang.
> - Wenn Sie nach dem Upgrade die Standardprofile aktivieren, können Sie die Änderungen nicht rückgängig machen. Das heißt, die Profile können nicht deaktiviert werden. Speichern Sie die Konfiguration und erstellen Sie eine Kopie der Konfigurationsdatei (ns.conf), bevor Sie die Profile aktivieren. Wenn Sie jedoch die Features im Standardprofil nicht verwenden möchten, können Sie weiterhin die alten SSL-Profile verwenden. Weitere Informationen zu diesen Profilen finden Sie unter Legacy-SSL-Profil.
> - Ab Release 11.1 51.x wird in der GUI und CLI eine Bestätigungsaufforderung hinzugefügt, wenn Sie das Standardprofil aktivieren, um zu verhindern, dass es versehentlich aktiviert wird.

Befehl:

```
1 set ssl parameter -defaultProfile ENABLED
2     Save your configuration before enabling the Default profile. You
         cannot undo the changes. Are you sure you want to enable the
         Default profile? [Y/N]Y
3 Done
4 <!--NeedCopy-->
```

Standardmäßig gelten einige SSL-Parameter, sogenannte *globale Parameter*, für alle SSL-Endpunkte. Wenn ein Profil jedoch an einen SSL-Endpunkt gebunden ist, gelten die globalen Parameter nicht.

Stattdessen gelten die im Profil angegebenen Einstellungen.

Punkte zu beachten

1. Ein Profil kann an mehrere virtuelle Server gebunden werden, aber ein virtueller Server kann nur über ein Profil gebunden sein.
2. Um ein Profil zu löschen, das an einen virtuellen Server gebunden ist, heben Sie zunächst die Bindung des Profils auf.
3. Eine Chiffre- oder Chiffriergruppe kann an mehrere Profile mit unterschiedlichen Prioritäten gebunden werden.
4. Ein Profil kann mehrere Chiffre und Verschlüsselungsgruppen an unterschiedliche Prioritäten gebunden sein.
5. Änderungen an einer Chiffregruppe werden sofort in allen Profilen und in allen virtuellen Servern widergespiegelt, an die eines der Profile gebunden ist.
6. Wenn eine Verschlüsselungssuite Teil einer Verschlüsselungsgruppe ist, bearbeiten Sie die Verschlüsselungsgruppe, um diese Verschlüsselungssuite zu entfernen, bevor Sie die Verschlüsselungssuite aus dem Profil entfernen.
7. Wenn Sie einer mit einem Profil verknüpften Verschlüsselungsgruppe oder einer Chiffriergruppe keine Priorität zuweisen, wird ihr die niedrigste Priorität innerhalb des Profils zugewiesen.
8. Sie können eine benutzerdefinierte Verschlüsselungsgruppe (auch als benutzerdefinierte Verschlüsselungsgruppe bezeichnet) aus vorhandenen Verschlüsselungsgruppen und Verschlüsselungssammlungen erstellen. Wenn Sie Chiffriergruppe A erstellen und vorhandene Chiffriergruppen X und Y hinzufügen, wird Y in dieser Reihenfolge mit einer niedrigeren Priorität als X zugewiesen. Das heißt, die zuerst hinzugefügte Gruppe hat eine höhere Priorität.
9. Wenn eine Cipher Suite Teil von zwei Verschlüsselungsgruppen ist, die an dasselbe Profil angehängt sind, wird die Cipher-Suite nicht als Teil der zweiten Verschlüsselungsgruppe hinzugefügt. Die Chiffre Suite mit der höheren Priorität ist wirksam, wenn Datenverkehr verarbeitet wird.
10. Verschlüsselungsgruppen werden im Profil nicht erweitert. Dadurch wird die Anzahl der Zeilen in der Konfigurationsdatei (ns.conf) stark reduziert. Wenn beispielsweise zwei Verschlüsselungsgruppen mit jeweils 15 Verschlüsselungen an tausend virtuelle SSL-Server gebunden sind, fügt die Erweiterung 30* 1000 verschlüsselungsbezogene Einträge in der Konfigurationsdatei hinzu. Mit dem neuen Profil hätte es nur zwei Einträge: einen für jede Verschlüsselungsgruppe, die an ein Profil gebunden ist.
11. Das Erstellen einer benutzerdefinierten Verschlüsselungsgruppe aus vorhandenen Verschlüsselungsgruppen und Chiffriergruppen ist eine Kopier- und Einfügeoperation. Änderungen in der ursprünglichen Gruppe werden nicht in der neuen Gruppe wiedergegeben.
12. Eine benutzerdefinierte Verschlüsselungsgruppe listet alle Profile auf, zu denen sie gehört.
13. Ein Profil listet alle virtuellen SSL-Server, -Dienste und -Dienstgruppen auf, an die es gebunden ist.
14. Wenn die standardmäßige SSL-Profilfunktion aktiviert ist, verwenden Sie das Profil, um eines

der Attribute einer SSL-Entität festzulegen oder zu ändern. Zum Beispiel virtueller Server, Dienst, Dienstgruppe oder ein interner Dienst.

Speichern der Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
save config

shell

root@ns# cd /nsconfig

root@ns# cp ns.conf ns.conf.NS<currentreleasenumber><currentbuildnumber
   >
<!--NeedCopy-->
```

Beispiel:

```
save config
shell
root@ns# cd /nsconfig
root@ns# cp ns.conf ns.conf.NS.11.0.jun.16
<!--NeedCopy-->
```

Aktivieren des Standardprofils

> **Wichtig:**
>
> Speichern Sie Ihre Konfiguration, bevor Sie die Software aktualisieren, und aktivieren Sie die Standardprofile.
>
> Ab Release 11.1 Build 51.x erscheint in der GUI und CLI eine Bestätigungsaufforderung, wenn Sie das Standardprofil aktivieren, um zu vermeiden, dass es versehentlich aktiviert wird.

Befehl: Der folgende Befehl aktiviert das Standardprofil und bindet dieses Profil an die SSL-Entitäten, an die ein Profil bereits gebunden ist. Das heißt, wenn ein Profil (zum Beispiel P1) bereits an eine SSL-Entität gebunden ist, ersetzt das Standard-Front-End-Profil oder das Standard-Back-End-Profil P1. Das ältere Profil (P1) wird nicht gelöscht. Es ist jetzt ein erweitertes SSL-Profil und enthält die früheren Einstellungen sowie die Chiffre und ECC-Kurven. Wenn Sie das Standardprofil nicht möchten, können Sie P1 explizit an die SSL-Entität binden.


```
set ssl parameter -defaultProfile ENABLED
    Save your configuration before enabling the Default profile. You
       cannot undo the changes. Are you sure you want to enable the
       Default profile? [Y/N]Y
Done
<!--NeedCopy-->
```

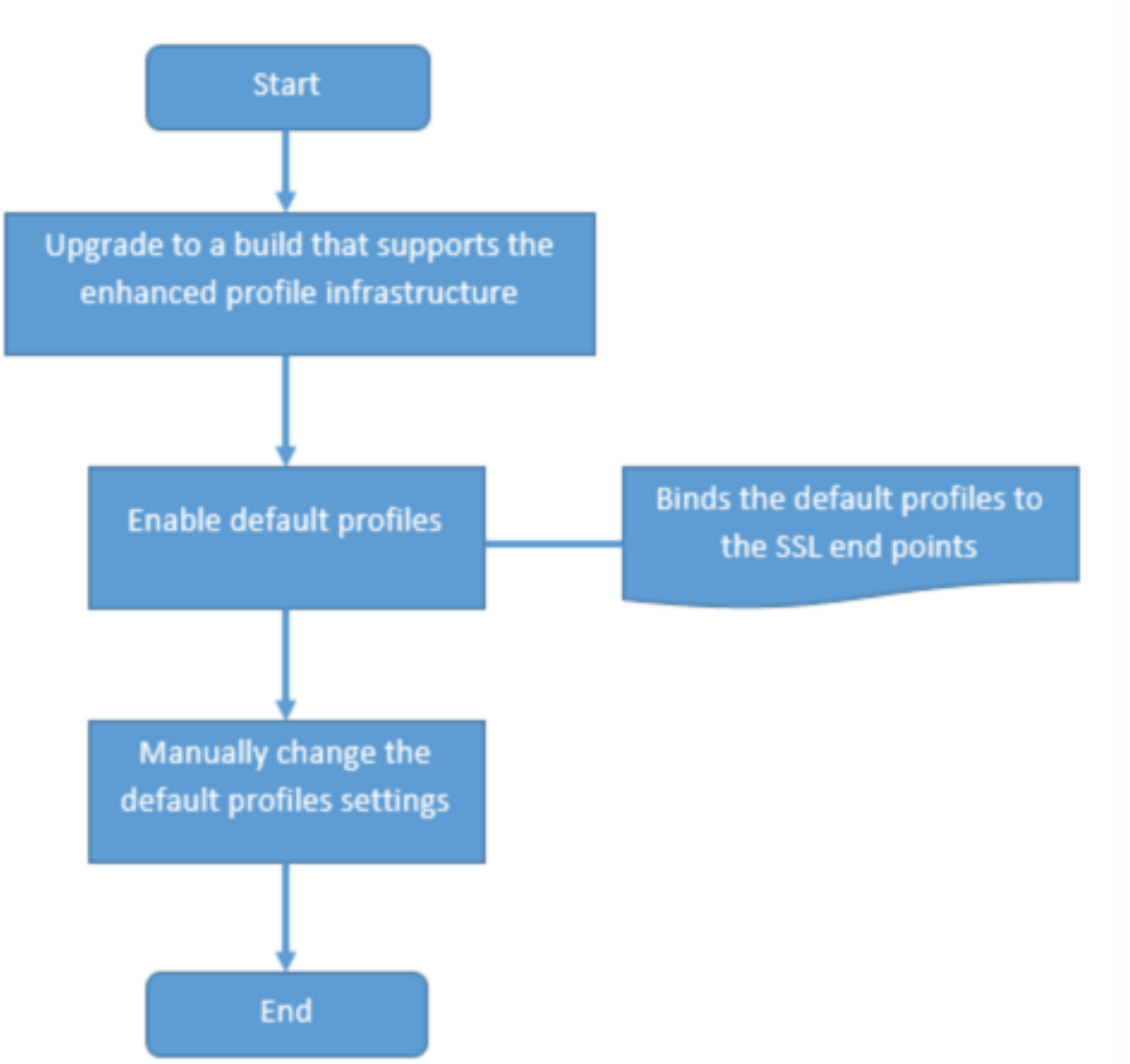
Aktualisieren Sie die Software auf einen Build, der die erweiterte Profilinfrastruktur unterstützt, und aktivieren Sie dann die Standardprofile.

> **Hinweise:**
>
> - Wenn ein Legacy-Profil (P1) bereits an eine SSL-Entität gebunden ist und Sie das Standardprofil aktivieren, überschreibt das Standardprofil die frühere Bindung. Das heißt, das Standardprofil ist an die SSL-Entitäten gebunden. Wenn das Standardprofil nicht gebunden werden soll, müssen Sie P1 erneut an die SSL-Entität binden.
> - Ein einzelner Vorgang (Standardprofil aktivieren oder`set ssl parameter -defaultProfile ENABLED`) aktiviert (bindet) sowohl das Standard-Front-End-Profil als auch das Standard-Back-End-Profil.

Anwendungsfall

Nachdem Sie die Standardprofile aktiviert haben, sind sie an alle SSL-Endpunkte gebunden. Die Standardprofile können bearbeitet werden. Wenn Ihre Bereitstellung die meisten Standardeinstellungen verwendet und nur wenige Parameter ändert, können Sie die Standardprofile bearbeiten. Die Änderungen werden sofort über alle Endpunkte reflektiert. Sie können auch benutzerdefinierte SSL-Profile mit einigen benutzerdefinierten und einigen Standardparametern erstellen und an die SSL-Entitäten binden.

Im folgenden Flussdiagramm werden die Schritte erläutert, die Sie ausführen müssen:



1. Informationen zum Upgrade der Software finden Sie unter Upgrade der Systemsoftware.
2. Aktivieren Sie die Standardprofile mit der CLI oder GUI.

- Geben Sie in der Befehlszeile Folgendes ein: `set ssl parameter -defaultProfile ENABLED`
- Wenn Sie die GUI bevorzugen, navigieren Sie zu **Traffic Management** > **SSL** > **Erweiterte SSL-Einstellungen ändern**, scrollen Sie nach unten, und wählen Sie **Standardprofil aktivieren** aus.

Wenn ein Profil vor dem Upgrade nicht an einen Endpunkt gebunden war, ist ein Standardprofil an den SSL-Endpunkt gebunden. Wenn ein Profil vor dem Upgrade an einen Endpunkt gebunden wurde, wird dasselbe Profil nach dem Upgrade gebunden, und Standardchiffre werden dem Profil hinzugefügt.

1. (Optional) Ändern Sie manuell alle Einstellungen im Standardprofil.

- Geben Sie in der Befehlszeile:`set ssl profile <name>` gefolgt von den zu ändernden Pa-

rametern ein.

- Wenn Sie die GUI lieber verwenden möchten, navigieren Sie zu **System** > **Profile**. Wählen Sie in **SSL Profiles**ein Profil aus und klicken Sie auf **Edit**.

SSL-Profilparameter

Sie können die folgenden SSL-Parameter in einem SSL-Profil festlegen. Sie können einige dieser Parameter in einem virtuellen SSL-Server festlegen. Weitere Informationen zu Parametern für virtuelle SSL-Server finden Sie unter Parameter für virtuelle SSL-Server.

Unterstützung für sichere Neuverhandlungen am Backend einer Citrix ADC Appliance

Hinweis: Dieser Parameter wird in Version 13.0 Build 58.x und höher eingeführt. In früheren Releases und Builds wurde im Back-End nur unsichere Neuverhandlungen unterstützt.

Die Funktion wird auf den folgenden Plattformen unterstützt:

- VPX
- MPX-Plattformen, die N2- oder N3-Chips enthalten
- Plattformen mit Intel Coleto SSL Chips

Die Funktion wird auf der FIPS-Plattform noch nicht unterstützt.

Eine sichere Neuverhandlung wird standardmäßig am Back-End einer ADC-Appliance verweigert. Das heißt, der `denySSLReneg` Parameter ist auf ALL (Standard) festgelegt.

Um eine sichere Neuverhandlung auf dem Back-End zu ermöglichen, wählen Sie eine der folgenden Einstellungen für den Parameter `denySSLReneg` aus:

- NEIN
- FRONTEND_CLIENT
- FRONTEND_CLIENTSERVER
- NONSECURE

Sichere Neuverhandlung über die CLI aktivieren

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile <name> -denySSLReneg <denySSLReneg>
```

Beispiel:

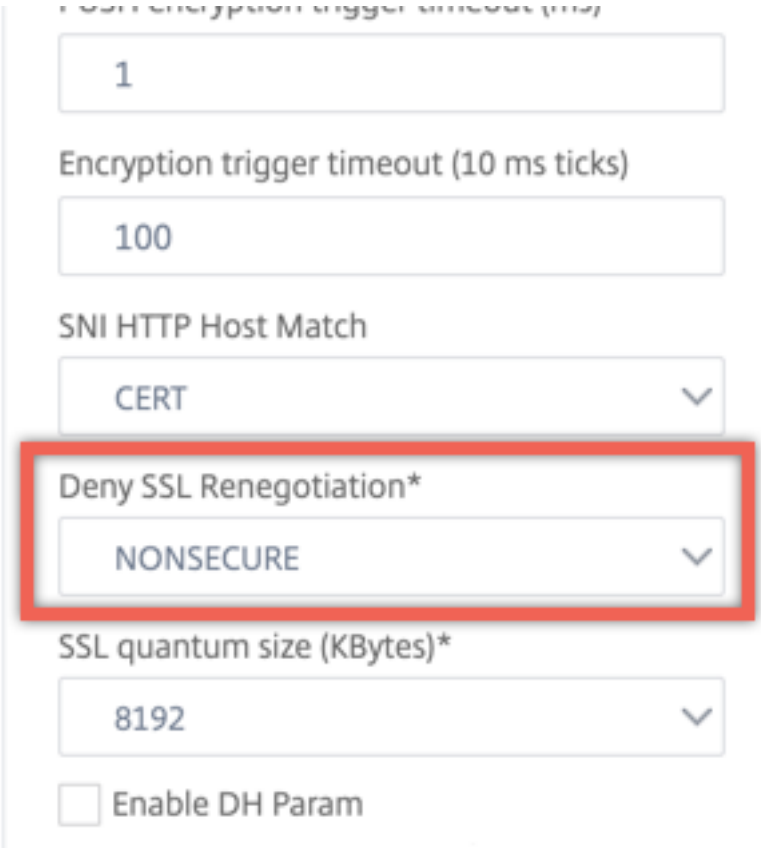
```
1 set ssl profile ns_default_ssl_profile_backend -denySSLReneg NONSECURE
2  Done
```



```
3
4  sh ssl profile ns_default_ssl_profile_backend
5  1)  Name: ns_default_ssl_profile_backend    (Back-End)
6      SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
          ENABLED  TLSv1.3: DISABLED
7      Server Auth: DISABLED
8      Use only bound CA certificates: DISABLED
9      Strict CA checks:       NO
10     Session Reuse: ENABLED      Timeout: 300 seconds
11     DH: DISABLED
12     Ephemeral RSA: DISABLED
13     Deny SSL Renegotiation      NONSECURE
14     Non FIPS Ciphers: DISABLED
15     Cipher Redirect: DISABLED
16     SSL Redirect: DISABLED
17     Send Close-Notify: YES
18     Strict Sig-Digest Check: DISABLED
19     Push Encryption Trigger: Always
20     PUSH encryption trigger timeout:    1 ms
21     SNI: DISABLED
22     OCSP Stapling: DISABLED
23     Strict Host Header check for SNI enabled SSL sessions:      NO
24     Push flag:  0x0 (Auto)
25     SSL quantum size:       8 kB
26     Encryption trigger timeout  100 mS
27     Encryption trigger packet count:    45
28
29     ECC Curve: P_256, P_384, P_224, P_521
30
31 1)  Cipher Name: DEFAULT_BACKEND        Priority :2
32     Description: Predefined Cipher Alias
33
34 1)  Service Name: s187
35  Done
36 <!--NeedCopy-->
```

Ermöglichen Sie sichere Neuverhandlungen mit der GUI

1. Navigieren Sie zu **System > Profile > SSL-Profil**.
2. Fügen Sie ein Profil hinzu oder bearbeiten Sie es.
3. Setzen Sie **Deny SSL Renegotiation** auf einen anderen Wert als ALL.



Validierung von Host-Head

Hinweis: Dieser Parameter wird in Version 13.0 build 52.x eingeführt.

Mit HTTP/1.1 mussten Clients mehrere Verbindungen verwenden, um mehrere Anfragen zu verarbeiten. Mit HTTP/2 können Clients Verbindungen zwischen Domänen wiederverwenden, die von demselben Zertifikat abgedeckt sind. Für eine SNI-aktivierte Sitzung muss die ADC-Appliance in der Lage sein zu steuern, wie der HTTP-Host-Header validiert wird, um dieser Änderung Rechnung zu tragen. In früheren Builds wurde die Anforderung gelöscht, wenn der Parameter aktiviert war (auf “Ja” gesetzt) und die Anfrage nicht den Host-Header für eine SNI-aktivierte Sitzung enthielt. Wenn der Parameter deaktiviert wurde (auf “Nein” gesetzt), hat die Appliance die Validierung nicht durchgeführt. Ein neuer Parameter `SNIHTTPHostMatch` wird zu einem SSL-Profil und globalen SSL-Parametern hinzugefügt, um diese Validierung besser kontrollieren zu können. Dieser Parameter kann drei Werte annehmen: CERT, STRICT und NONE. Diese Werte funktionieren nur für SNI-aktivierte Sitzungen wie folgt. SNI muss auf dem virtuellen SSL-Server oder dem an den virtuellen Server gebundenen Profil aktiviert sein, und die HTTP-Anfrage muss den Host-Header enthalten.

- CERT - Die Verbindung wird weitergeleitet, wenn der Host-Header-Wert in der Anfrage durch das Zertifikat abgedeckt wird, mit dem diese SSL-Sitzung eingerichtet wurde.
- STRICT - Die Verbindung wird nur weitergeleitet, wenn der Host-Header-Wert in der Anfrage mit

dem Servernamenwert übereinstimmt, der in der Client Hello Nachricht der SSL-Verbindung übergeben wurde.

- NO - Der Host-Headerwert wird nicht validiert.

Mögliche Werte: NO, CERT, STRICT
Standardwert: CERT

Mit der Einführung des neuen Parameters `SNIHTTPHostMatch` ändert sich das Verhalten des Parameters `dropReqWithNoHostHeader`. Die Einstellung des Parameters `dropReqWithNoHostHeader` wirkt sich nicht mehr darauf aus, wie der Host-Header mit dem SNI-Zertifikat validiert wird.

Festlegen von SSL-Profilparametern mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile <name> [-ssllogProfile <string>] [-dh ( ENABLED | DISABLED ) -dhFile <string>] [-dhCount <positive_integer>][-dhKeyExpSizeLimit ( ENABLED | DISABLED )] [-eRSA ( ENABLED | DISABLED) [-eRSACount <positive_integer>]] [-sessReuse ( ENABLED | DISABLED )
[-sessTimeout <positive_integer>]] [-cipherRedirect ( ENABLED | DISABLED ) [-cipherURL <URL>]] [-clientAuth ( ENABLED | DISABLED )[-clientCert ( Mandatory | Optional )]] [-sslRedirect ( ENABLED |
DISABLED )] [-redirectPortRewrite ( ENABLED | DISABLED )] [-ssl3 ( ENABLED | DISABLED )] [-tls1 ( ENABLED | DISABLED )] [-tls11 ( ENABLED| DISABLED )] [-tls12 ( ENABLED | DISABLED )] [-tls13 ( ENABLED |DISABLED )] [-SNIEnable ( ENABLED | DISABLED )] [-ocspStapling (ENABLED | DISABLED )] [-serverAuth ( ENABLED | DISABLED )] [-commonName <string>] [-pushEncTrigger <pushEncTrigger>] [-sendCloseNotify ( YES |
NO )] [-clearTextPort <port|*>] [-insertionEncoding ( Unicode | UTF-8)] [-denySSLReneg <denySSLReneg>] [-quantumSize <quantumSize>]
[-strictCAChecks ( YES | NO )] [-encryptTriggerPktCount <positive_integer>] [-pushFlag <positive_integer>][-dropReqWithNoHostHeader ( YES | NO )] [-SNIHTTPHostMatch <SNIHTTPHostMatch>] [-pushEncTriggerTimeout <positive_integer>]
[-sslTriggerTimeout <positive_integer>] [-clientAuthUseBoundCAChain ( ENABLED | DISABLED )] [-sslInterception ( ENABLED | DISABLED )][-ssliReneg ( ENABLED | DISABLED )] [-ssliOCSPCheck ( ENABLED | DISABLED )] [-ssliMaxSessPerServer <positive_integer>] [-HSTS ( ENABLED| DISABLED )] [-maxage <positive_integer>] [-IncludeSubdomains ( YES | NO )] [-preload ( YES | NO )] [-sessionTicket ( ENABLED | DISABLED )][-sessionTicketLifeTime <
```

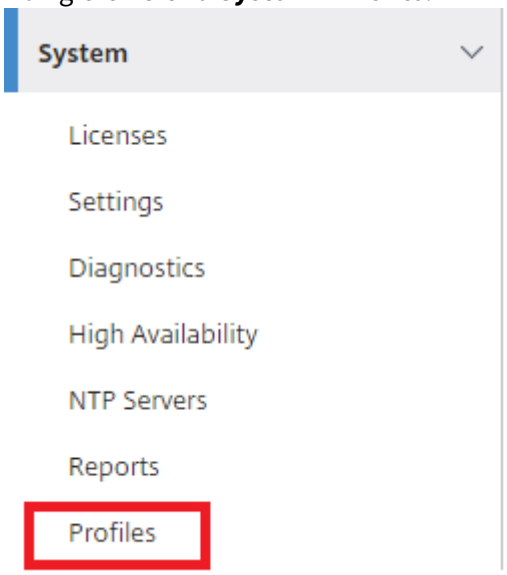


```
    positive_integer>] [-sessionTicketKeyRefresh (ENABLED | DISABLED )]
    {
 -sessionTicketKeyData  }
  [-sessionKeyLifeTime <positive_integer>] [-prevSessionKeyLifeTime <
     positive_integer>]
[-cipherName <string> -cipherPriority <positive_integer>][-
    strictSigDigestCheck ( ENABLED | DISABLED )]
[-skipClientCertPolicyCheck ( ENABLED | DISABLED )] [-zeroRttEarlyData
    ( ENABLED | DISABLED )] [-tls13SessionTicketsPerAuthContext
<positive_integer>] [-dheKeyExchangeWithPsk ( YES | NO )]
<!--NeedCopy-->
```

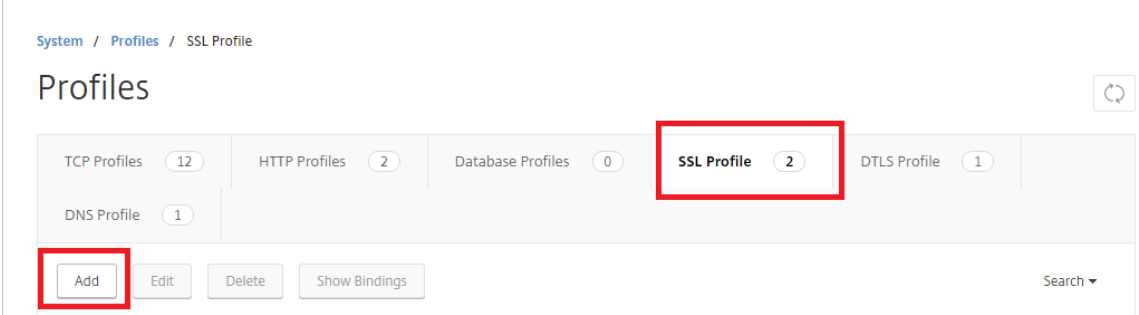
Festlegen von SSL-Profilparametern mit der GUI

So fügen Sie ein Profil hinzu:

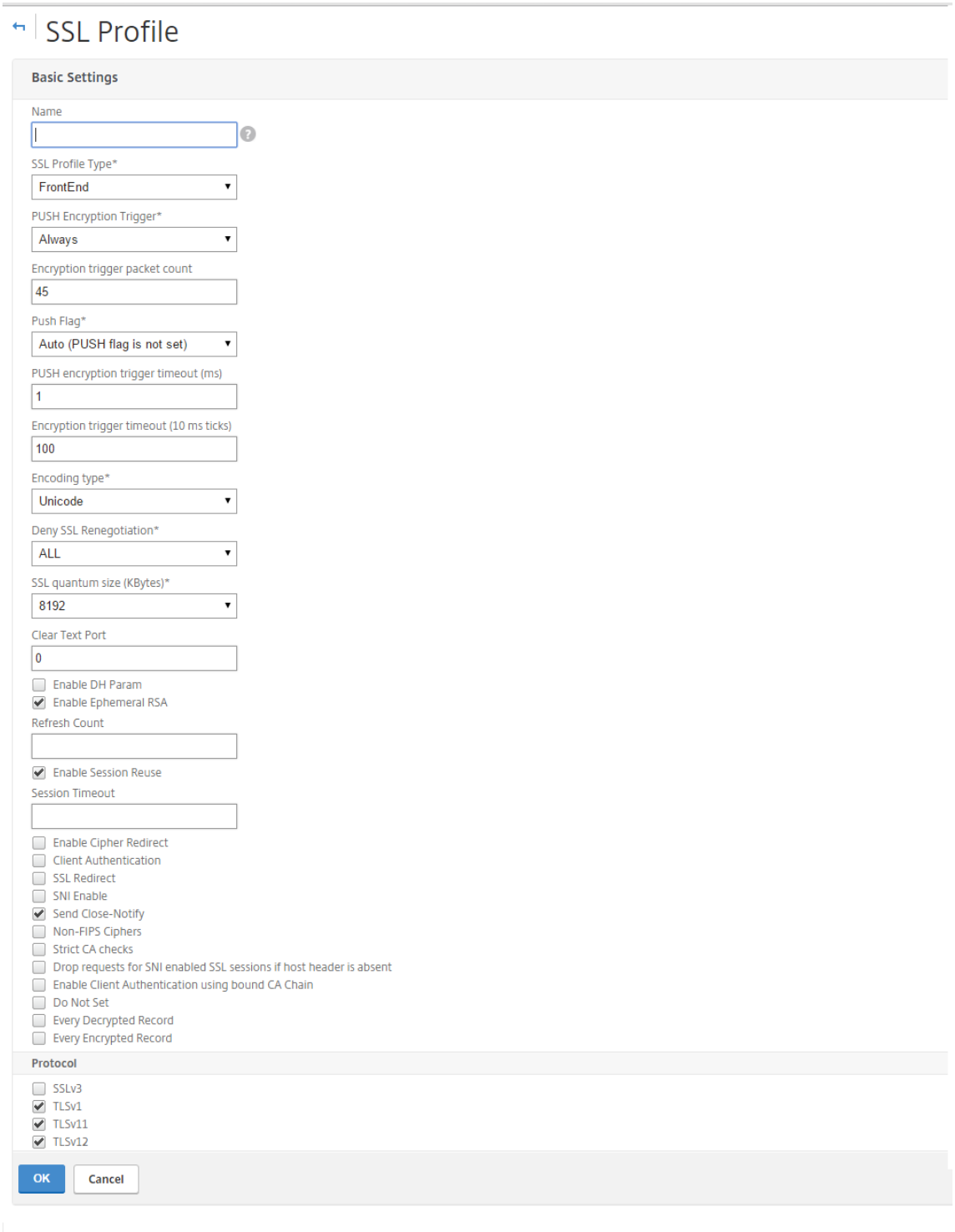
1. Navigieren Sie zu **System > Profile**.



2. Wählen Sie **SSL-Profile aus**. Klicken Sie auf **Hinzufügen**.



3. Geben Sie Werte für die verschiedenen Parameter an.



4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Fertig**.

So verwenden Sie ein vorhandenes SSL-Profil wieder:

1. Navigieren Sie zu **System > Profile**.
2. Wählen Sie ein vorhandenes Profil aus und klicken Sie auf **Hinzufügen**.

3. Geben Sie einen anderen Namen an, ändern Sie alle Parameter und klicken Sie auf **OK**.
4. Klicken Sie auf **Fertig**.

TLS-Sitzungsticketerweiterung

Ein SSL-Handshake ist ein CPU-intensiver Betrieb. Wenn die Sitzungswiederverwendung aktiviert ist, wird der Server-/Clientschlüsselaustauschvorgang für vorhandene Clients übersprungen. Sie dürfen ihre Sitzungen fortsetzen. Diese Aktion verbessert die Antwortzeit und erhöht die Anzahl der SSL-Transaktionen pro Sekunde, die ein Server unterstützen kann. Allerdings muss der Server Details zu jedem Sitzungsstatus speichern, der Speicher belegt und schwer auf mehreren Servern freigegeben werden kann, wenn Anforderungen über Server verteilt werden.

Citrix ADC Appliances unterstützen die SessionTicket TLS-Erweiterung. Die Verwendung dieser Erweiterung zeigt an, dass die Sitzungsdetails auf dem Client und nicht auf dem Server gespeichert werden. Der Client muss angeben, dass er diesen Mechanismus unterstützt, indem er die TLS-Erweiterung des Sitzungstickets in die Client-Hello -Nachricht einschließt. Für neue Clients ist diese Erweiterung leer. Der Server sendet ein neues Sitzungsticket in der NewsessionTicket-Handshake-Nachricht. Das Sitzungsticket wird verschlüsselt, indem ein Schlüsselpaar verwendet wird, das nur dem Server bekannt ist. Wenn ein Server jetzt kein neues Ticket ausstellen kann, wird ein normaler Handshake abgeschlossen.

Diese Funktion ist nur in Front-End-SSL-Profilen und nur am Frontend der Kommunikation verfügbar, bei der die Appliance als Server fungiert und Sitzungstickets generiert.

Einschränkungen

- Diese Funktion wird auf einer FIPS-Plattform nicht unterstützt.
- Diese Funktion wird nur mit TLS-Versionen 1.1 und 1.2 unterstützt.
- Die Persistenz der SSL-Sitzungs-ID wird bei Sitzungstickets nicht unterstützt.

Aktivieren der TLS-Sitzungsticketerweiterung mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile <name> -sessionTicket (ENABLED | DISABLED ) [-
    sessionTicketLifeTime <positive_integer>
<!--NeedCopy-->
```

Argumente:

SessionTicket: Status der TLS-Sitzungsticketerweiterung. Die Verwendung dieser Erweiterung zeigt an, dass die Sitzungsdetails auf dem Client und nicht auf dem Server gespeichert werden, wie in RFC 5077 definiert.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

SessionTicketLifetime: Geben Sie eine Zeit in Sekunden an, nach der das Sitzungsticket abläuft und ein neuer SSL-Handshake gestartet werden muss.

Standardwert: 300

Mindestwert: 0

Maximalwert: 172800

Beispiel:

```
1 add ssl profile profile1 -sessionTicket ENABLED -sessionTicketlifeTime
     300
2 Done
3 <!--NeedCopy-->
```

Aktivieren der TLS-Sitzungsticketerweiterung mit der GUI

1. Navigieren Sie zu **System** > **Profile**. Wählen Sie **SSL-Profile aus**.
2. Klicken Sie auf **Hinzufügen**, und geben Sie einen Namen für das Profil an.
3. Wählen Sie **Sitzungsticket**aus.
4. Geben Sie optional die **Gültigkeitsdauer des Sitzungstickets (Sekunden)**an.

Sichere Implementierung von Sitzungstickets

Mithilfe von TLS-Sitzungstickets können Clients abgekürzte Handshakes für eine schnellere Wiederherstellung der Verbindung zu Servern verwenden. Wenn Sitzungstickets jedoch nicht verschlüsselt oder über längere Zeit geändert werden, können sie ein Sicherheitsrisiko darstellen. Sie können Sitzungstickets sichern, indem Sie sie mit einem symmetrischen Schlüssel verschlüsseln. Um die Weiterleitungsgeheimnis zu erreichen, können Sie ein Zeitintervall angeben, in dem der Sitzungsticketschlüssel aktualisiert wird.

Die Appliance generiert standardmäßig die Sitzungsticket-Schlüssel. Wenn jedoch mehrere Appliances in einer Bereitstellung die Sitzungstickets des anderen entschlüsseln müssen, müssen sie

alle denselben Sitzungsticketschlüssel verwenden. Daher müssen Sie die gleichen Sitzungs-Ticket-Schlüsseldaten manuell auf allen Appliances festlegen (hinzufügen oder laden). Die Schlüsseldaten für das Session-Ticket umfassen folgende Informationen:

- Name des Sitzungstickets.
- Sitzungs-AES-Schlüssel, der zum Verschlüsseln oder Entschlüsseln des Tickets verwendet wird.
- Session-HMAC-Schlüssel verwendet, um den Digest des Tickets zu berechnen.

Sie können jetzt Sitzungsticketschlüsseldaten der Länge 64 Byte so konfigurieren, dass 256-Bit-HMAC-Schlüssel unterstützt werden, wie in RFC 5077 empfohlen. Aus Gründen der Abwärtskompatibilität werden auch Schlüssellängen von 48 Byte unterstützt.

> **Hinweis:**
>
> Stellen Sie beim manuellen Eingeben der Sitzungsticketschlüsseldaten sicher, dass die Konfiguration über alle Citrix ADC Appliances in einem HA-Setup oder in einem Cluster-Setup identisch ist.

Der`sessionTicketKeyLifeTime` Parameter gibt an, wie oft ein Sitzungsticketschlüssel aktualisiert wird. Sie können den`prevSessionTicketKeyLifeTime` Parameter festlegen, um festzulegen, wie lange der vorherige Sitzungsticketschlüssel für die Entschlüsselung von Tickets mit diesem Schlüssel beibehalten wird, nachdem ein neuer Schlüssel generiert wurde. Die`prevSessionTicketKeyLifeTime` Einstellung verlängert die Zeit, für die ein Client einen abgekürzten Handshake verwenden kann, um die Verbindung wiederherzustellen. Wenn beispielsweise auf 10 Minuten und`sessionTicketKeyLifeTime` auf 5 Minuten festgelegt`prevSessionTicketKeyLife` ist, wird nach 10 Minuten ein neuer Schlüssel generiert und für alle neuen Sitzungen verwendet. Allerdings haben zuvor verbundene Kunden weitere 5 Minuten, für die zuvor ausgestellte Tickets für einen abgekürzten Handshake geehrt werden.

Konfigurieren von SSL-Session-Ticket-Daten mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile <name> -sessionTicket ENABLED -sessionTicketLifeTime <
    positive_integer> -sessionTicketKeyRefresh ( ENABLED | DISABLED )] -
    sessionTicketKeyLifeTime <positive_integer> [-
    prevSessionTicketKeyLifeTime <positive_integer>]
<!--NeedCopy-->
```

Argumente:

SessionTicket: Verwenden Sie Session-Tickets wie in RFC 5077 beschrieben. Für die Einrichtung des ersten Handshakes sind CPU-intensive Verschlüsselungsvorgänge mit öffentlichen Schlüsseln er-

forderlich. Mit der **Einstellung** ENABLED gibt ein Server ein Sitzungsticket an einen Client aus, mit dem der Client einen abgekürzten Handshake ausführen kann.

Mögliche Werte: ENABLED, DISABLED. Standard: DISABLED

SessionTicketLifetime: Lebensdauer des Sitzungstickets in Sekunden. Nach Ablauf dieser Zeit können Clients dieses Ticket nicht verwenden, um ihre Sitzungen fortzusetzen.

Maximalwert: 172800 Mindestwert: 0. Standard: 300.

SessionTicketKeyRefresh: Wenn die Zeit abläuft, die durch den Parameter der Lebenszeit des Sitzungsticketschlüssels angegeben wird, generieren Sie den Sitzungsticketschlüssel, der zum Verschlüsseln oder Entschlüsseln der Sitzungstickets verwendet wird. Automatisch aktiviert, wenn SessionTicket aktiviert ist. Deaktiviert, wenn ein Administrator die Sitzungs-Ticket-Daten eingibt.

Mögliche Werte: ENABLED, DISABLED. Standard: ENABLED

SessionKeyLifetime: Die Lebensdauer eines symmetrischen Schlüssels, der zum Verschlüsseln der von einer Citrix ADC Appliance ausgestellten Sitzungstickets in Sekunden verwendet wird.

Maximalwert: 86400 Mindestwert: 600 Standard: 3000

PrevSessionKeyLifetime: Zeit in Sekunden, für die der vorherige symmetrische Schlüssel, der zum Verschlüsseln von Sitzungstickets verwendet wird, für bestehende Clients gültig bleibt, nachdem die Gültigkeitsdauer des Sitzungsticketschlüssels abgelaufen ist. Innerhalb dieser Zeit können vorhandene Clients ihre Sitzungen mit dem vorherigen Sitzungsticketschlüssel fortsetzen. Sitzungstickets für neue Clients werden mithilfe des neuen Schlüssels verschlüsselt.

Maximalwert: 172800 Mindestwert: 0. Standard: 0

Beispiel:

```
1  set ssl profile ns_default_ssl_profile_frontend -sessionTicket ENABLED
       -sessionTicketlifeTime 120 -sessionTicketKeyRefresh ENABLED -
       sessionTicketKeyLifeTime 100 -prevSessionTicketKeyLifeTime 60
2
3  Done
4
5  show ssl profile ns_default_ssl_profile_frontend
6
7      Session Ticket: ENABLED
8      Session Ticket Lifetime: 120 (secs)
9      Session Key Auto Refresh: ENABLED
10     Session Key Lifetime: 100 (secs)
11     Previous Session Key Lifetime: 60 (secs)
12 <!--NeedCopy-->
```


Konfigurieren von SSL-Session-Ticket-Daten mit der GUI

1. Navigieren Sie zu **System** > **Profile**und wählen Sie **SSL-Profil**aus.
2. Wählen Sie **ns_default_ssl_profile_frontend** und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Grundeinstellungen** auf das Stiftsymbol und legen Sie die folgenden Parameter fest:
   - Sitzungsticket
   - Sitzungs-Ticket-Lebensdauer (Sekunden)
   - Automatische Aktualisierung des Sitzungsticketschlüssels
   - Lebensdauer des Sitzungsticketschlüssels (Sekunden)
   - Lebensdauer des vorherigen Sitzungsticketschlüssels (Sekunden)
4. Klicken Sie auf **OK**.

Geben Sie SSL-Sitzungsticketdaten manuell mit der CLI ein

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile <name> -sessionTicket ENABLED

set ssl profile <name> -sessionTicketKeyData

show ssl profile ns_default_ssl_profile_frontend
<!--NeedCopy-->
```

Argumente:

SessionTicket: Verwendung von Session-Tickets wie in RFC 5077 beschrieben. Für die Einrichtung des ersten Handshakes sind CPU-intensive Verschlüsselungsvorgänge mit öffentlichen Schlüsseln erforderlich. Mit der **Einstellung** ENABLED gibt ein Server ein Sitzungsticket an einen Client aus, mit dem der Client einen abgekürzten Handshake ausführen kann.

Mögliche Werte: ENABLED, DISABLED. Standard: DISABLED

sessionTicketKeyData: Contains the session ticket name (0-15 bytes), the session AES key used to encrypt or decrypt the session ticket (16-31 bytes), and the session HMAC key used to compute the digest of the ticket (32-63 bytes). Externally generated by an administrator and added to a Citrix ADC appliance.

Maximale Länge: 64 Byte

Beispiel:


```
set ssl profile ns_default_ssl_profile_frontend -sessionTicket ENABLED

Done

set ssl profile ns_default_ssl_profile_frontend -sessionTicketKeyData
    1111111111111111111111111111111111111111111111111111

Done

show ssl profile ns_default_ssl_profile_frontend

    1) Name: ns_default_ssl_profile_frontend (Front-End)
    SSLv3: ENABLED TLSv1.0: ENABLED TLSv1.1: ENABLED TLSv1.2: ENABLED
    Client Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks: NO
    Session Reuse: ENABLED Timeout: 120 seconds
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED Ephemeral RSA: ENABLED
        Refresh Count: 0
    Deny SSL Renegotiation ALL
    Non FIPS Ciphers: DISABLED
    Cipher Redirect: DISABLED
    SSL Redirect: DISABLED
    Send Close-Notify: YES
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout: 1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions: NO
    Push flag: 0x0 (Auto)
    SSL quantum size: 8 kB
    Encryption trigger timeout 100 mS
    Encryption trigger packet count: 45
    Subject/Issuer Name Insertion Format: Unicode
    Session Ticket: ENABLED
    Session Ticket Lifetime: 300 (secs)
    Session Key Auto Refresh: DISABLED
    Session Key Lifetime: 3000 (secs)
    Previous Session Key Lifetime: 0 (secs)
    Session Key Data: 84
       dad1afc6d56b0deeb0a7fd7f299a207e8d8c15cdd087a5684a11a329fd732e87a0535d9088
```



```
40      47
           e8c181ba266f5c8838ae472cb3ab9255b683bf922fad32cee816c329989ef7cdeb278e93ac
41
42      ECC Curve: P_256, P_384, P_224, P_521
43
44      1) Cipher Name: DEFAULT Priority :4
45      Description: Predefined Cipher Alias
46
47      1) Internal Service Name (Front-End): nsrnatsip-127.0.0.1-5061
48      2) Internal Service Name (Front-End): nskrpcs-127.0.0.1-3009
49      3) Internal Service Name (Front-End): nshttps-::1l-443
50      4) Internal Service Name (Front-End): nsrpcs-::1l-3008
51      5) Internal Service Name (Front-End): nshttps-127.0.0.1-443
52      6) Internal Service Name (Front-End): nsrpcs-127.0.0.1-3008
53      7) Vserver Name: v1
54
55  Done
56  <!--NeedCopy-->
```

Geben Sie SSL-Sitzungsticketdaten manuell mit der GUI ein

1. Navigieren Sie zu **System > Profile**und wählen Sie **SSL-Profil**aus.
2. Wählen Sie **ns_default_ssl_profile_frontend** und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **Grundeinstellungen** auf das Stiftsymbol und legen Sie die folgenden Parameter fest:
   - Sitzungsticket
   - Schlüsseldaten des Sitzungstickets
   - Sitzungsticketschlüsseldaten bestätigen
4. Klicken Sie auf **OK**.

Unterstützung für Extended Master Secret in SSL-Handshake auf Citrix ADC Nicht-FIPS-Plattformen

Hinweis: Dieser Parameter wird in Version 13.0 build 61.x eingeführt.

Extended Master Secret (EMS) ist eine optionale Erweiterung des Transport Layer Security (TLS) -Protokolls. Es wird ein neuer Parameter hinzugefügt, der sowohl für Front-End- als auch Back-End-SSL-Profile gilt, um EMS auf der Citrix ADC Appliance zu unterstützen. Wenn der Parameter aktiviert ist und der Peer EMS unterstützt, verwendet die ADC-Appliance die EMS-Berechnung. Wenn der Peer

EMS nicht unterstützt, wird die EMS-Berechnung nicht für die Verbindung verwendet, obwohl der Parameter auf der Appliance aktiviert ist. Weitere Informationen zu EMS finden Sie unter RFC 7627.

Hinweis: EMS gilt nur für Handshakes, die das TLS-Protokoll Version 1.0, 1.1 oder 1.2 verwenden.

Plattformunterstützung für EMS

- MPX- und SDX-Plattformen, die entweder Cavium N3-Chips oder Crypto-Karten von Intel Coleto Creek enthalten. Die folgenden Plattformen werden mit Intel Coleto-Chips ausgeliefert:
- MPX 5900
- MPX/SDX 8900
- MPX/SDX 26000
- MPX/SDX 26000-50S
- MPS/SDX 26000-100 G
- MPX/SDX 15000-50 G

Sie können auch den Befehl “show hardware” verwenden, um festzustellen, ob Ihre Appliance über Coleto (COL) - oder N3-Chips verfügt.

- MPX- und SDX-Plattformen ohne Krypto-Karten (nur Software).
- Nur-Software-Plattformen: VPX, CPX und BLX.

EMS kann auf den folgenden Plattformen nicht aktiviert werden:

- MPX 9700 FIPS- und MPX 14000 FIPS-Plattformen.
- MPX- und SDX-Plattformen mit Cavium N2-Krypto-Chips.

Wenn der Parameter aktiviert ist, versucht die ADC-Appliance, EMS in Verbindungen mit TLS 1.2, TLS 1.1 und TLS 1.0 zu verwenden. Die Einstellung hat keine Auswirkungen auf TLS 1.3 oder SSLv3 Verbindungen.

Damit EMS mit dem Peer ausgehandelt werden kann, aktivieren Sie die Einstellung für das SSL-Profil, das an den virtuellen Server (Frontend) oder den Dienst (Backend) gebunden ist.

Aktivieren von EMS mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile <profile name> [-allowExtendedMasterSecret (YES | NO)]
```

Beispiele

```
1 set ssl profile ns_default_ssl_profile_frontend  -
     allowExtendedMasterSecret YES
```



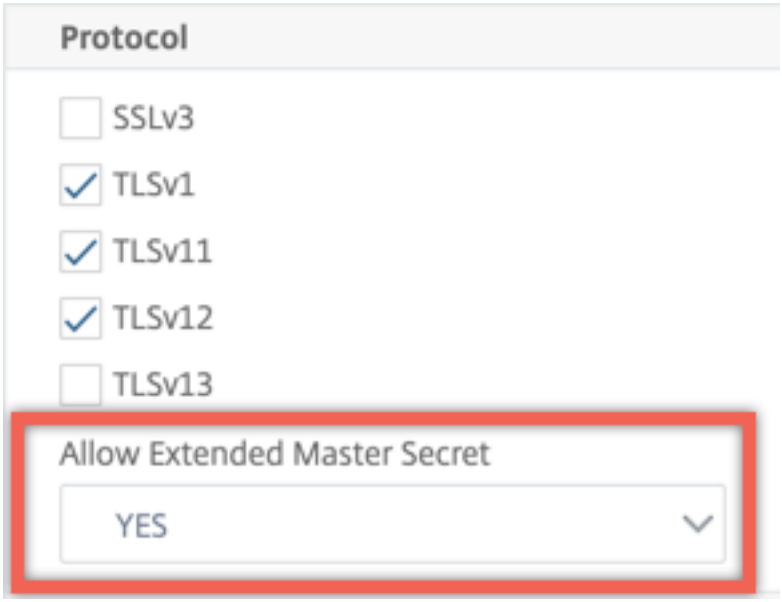
```
2
3 set ssl profile ns_default_ssl_profile_backend  -
     allowExtendedMasterSecret YES
4 <!--NeedCopy-->
```

Die folgende Tabelle zeigt den Standardwert des `allowExtendedMasterSecret` Parameters in verschiedenen Standard- und benutzerdefinierten Profilen.

Profil	Standardeinstellung
Standard-Front-End-Profil	NEIN
Standard-Sicheres Front-End-Profil	JA
Standard-Back-End-Profil	NEIN
Benutzerdefiniertes Profil	NEIN

Aktivieren von EMS mit der GUI

1. Navigieren Sie zu **System > Profile > SSL-Profil**.
2. Fügen Sie ein Profil hinzu oder bearbeiten Sie ein Profil.
3. Setzen Sie **Extended Master Secret zulassen** auf YES.



Unterstützung für die Verarbeitung der ALPN-Erweiterung in der Client-Hallo-Nachricht

Hinweis: Diese Funktion wird in Version 13.0 Build 61.x und höher unterstützt.

Den Front-End-SSL-Profilen `alpnProtocol` wird ein Parameter hinzugefügt, um das Anwendungsprotokoll in der ALPN-Erweiterung für die vom virtuellen SSL_TCP-Server bearbeiteten Verbindungen auszuhandeln. Nur das im SSL-Profil angegebene Protokoll wird ausgehandelt, wenn das gleiche Protokoll in der ALPN-Erweiterung der Client-Hallo-Nachricht empfangen wird.

Hinweis: Der Parameter `alpnProtocol` wird nur auf Front-End-SSL-Profilen unterstützt und gilt für SSL-Verbindungen, die von virtuellen Servern vom Typ SSL_TCP verarbeitet werden.

Festlegen des Protokolls im Front-End-SSL-Profil über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile ns_default_ssl_profile_frontend -alpnProtocol <protocol_name
>
```

Der Parameter `alpnProtocol` kann drei Werte annehmen. Maximale Länge: 4096 Byte.

- **NONE:** Die Verhandlung über das Anwendungsprotokoll findet nicht statt. Dies ist die Standardeinstellung.
- **HTTP1:** HTTP1 kann als das Anwendungsprotokoll ausgehandelt werden.
- **HTTP2:** HTTP2 kann als das Anwendungsprotokoll ausgehandelt werden.

Beispiel:

```
1  set ssl profile ns_default_ssl_profile_frontend -ALPNProtocol HTTP2
2  > sh ssl profile ns_default_ssl_profile_frontend
3  1)  Name: ns_default_ssl_profile_frontend   (Front-End)
4      SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
           ENABLED  TLSv1.3: DISABLED
5      Client Auth: DISABLED
6      Use only bound CA certificates: DISABLED
7      Strict CA checks:   NO
8      Session Reuse: ENABLED  Timeout: 120 seconds
9      DH: DISABLED
10     DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
           ENABLED  Refresh Count: 0
11     Deny SSL Renegotiation  ALL
12     Non FIPS Ciphers: DISABLED
13     Cipher Redirect: DISABLED
14     SSL Redirect: DISABLED
```



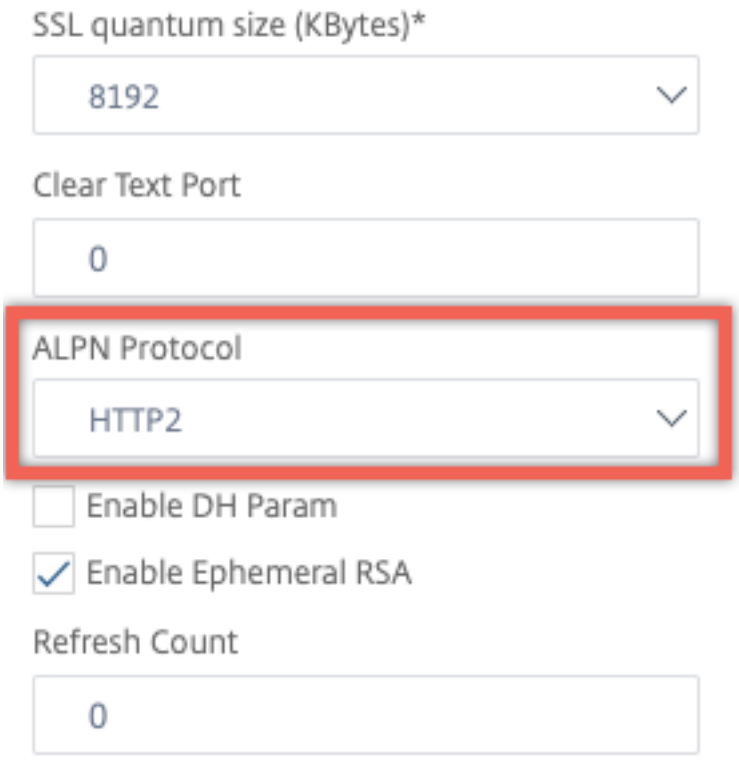
```
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1
    Push Encryption Trigger: Always
    PUSH encryption trigger timeout:    1 ms
    SNI: DISABLED
    OCSP Stapling: DISABLED
    Strict Host Header check for SNI enabled SSL sessions:  NO
    Match HTTP Host header with SNI:    CERT
    Push flag:  0x0 (Auto)
    SSL quantum size:   8 kB
    Encryption trigger timeout  100 mS
    Encryption trigger packet count:    45
    Subject/Issuer Name Insertion Format:   Unicode

    SSL Interception: DISABLED
    SSL Interception OCSP Check: ENABLED
    SSL Interception End to End Renegotiation: ENABLED
    SSL Interception Maximum Reuse Sessions per Server: 10
    Session Ticket: DISABLED
    HSTS: DISABLED
    HSTS IncludeSubDomains: NO
    HSTS Max-Age: 0
    HSTS Preload: NO
    Allow Extended Master Secret: NO
    Send ALPN Protocol: HTTP2

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

Legen Sie das Protokoll im Front-End-SSL-Profil mit der GUI fest

1. Navigieren Sie zu **System > Profile**und wählen Sie **SSL-Profil**aus.
2. Wählen Sie **ns_default_ssl_profile_frontend** und klicken Sie auf **Bearbeiten**.
3. Wählen Sie in der Liste **ALPN-Protokoll** die Option **HTTP2** aus.



Laden einer alten Konfiguration

Das Aktivieren der Standardprofile ist nicht reversibel. Wenn Sie jedoch entscheiden, dass für die Bereitstellung die Standardprofile nicht erforderlich sind, können Sie eine ältere Konfiguration laden, die Sie gespeichert haben, bevor Sie die Standardprofile aktivieren. Die Änderungen sind wirksam, nachdem Sie die Appliance neu gestartet haben.

Laden einer alten Konfiguration mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
shell

root@ns# clear config

root@ns# cd /nsconfig

root@ns# cp ns.conf.NS.11.0.jun.16 ns.conf

root@ns# reboot
<!--NeedCopy-->
```


Sicheres Front-End-Profil

October 5, 2021

Neben einem Standard-Front-End und einem Standard-Back-End-Profil ist ab Version 12.1 ein neues sicheres Standard-Front-End-Profil verfügbar. Die Einstellungen, die für eine A+ Bewertung (Stand Mai 2018) von Qualys SSL Labs erforderlich sind, sind in dieses Profil vorinstalliert. Früher mussten Sie jeden Parameter explizit festlegen, der für eine A+-Bewertung auf einem SSL-Front-End-Profil oder einem virtuellen SSL-Server erforderlich ist. Jetzt können Sie das ns_default_ssl_profile_secure_frontend-Profil an Ihren virtuellen SSL-Server binden und die erforderlichen Parameter werden automatisch auf Ihrem virtuellen SSL-Server festgelegt.

> **Hinweis:**
>
> Das sichere Front-End-Profil kann nicht bearbeitet werden.

Wenn Sie das Standardprofil aktivieren, wird das Standard-Front-End-Profil automatisch an alle virtuellen SSL-Server gebunden. Um eine A+-Bewertung zu erhalten, müssen Sie explizit das ns_default_ssl_profile_secure_frontend-Profil binden und auch ein SHA2/SHA256-Serverzertifikat an Ihren virtuellen SSL-Server binden.

Sichere Front-End-Profilparameter

Die Parameter mit ihren Standardeinstellungen sind hier aufgelistet:

```
SSLv3: DISABLED  TLSv1.0: DISABLED  TLSv1.1: DISABLED  TLSv1.2: ENABLED
     TLSv1.3: DISABLED

Deny SSL Renegotiation: NONSECURE

HSTS: ENABLED

HSTS IncludeSubDomains: YES

HSTS Max-Age: 15552000

Cipher Name: SECURE    Priority :1
<!--NeedCopy-->
```


Alias für sichere Verschlüsselungsverfahren

Ein neuer gesicherter Chiffrealias wird hinzugefügt und an das sichere Front-End-Profil gebunden. Um die Chiffre aufzulisten, die Teil dieses Alias sind, geben Sie an der Eingabeaufforderung Folgendes ein: show chiffre SECURE

```
show cipher SECURE

    1) Cipher Name: TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 Priority : 1
           Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(256)
              Mac=AEAD   HexCode=0xc030
    2) Cipher Name: TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 Priority : 2
           Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(128)
              Mac=AEAD   HexCode=0xc02f
    3) Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
       Priority : 3
           Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(256)
              Mac=AEAD   HexCode=0xc02c
    4) Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
       Priority : 4
           Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(128)
              Mac=AEAD   HexCode=0xc02b
Done
<!--NeedCopy-->
```

Konfiguration

Gehen Sie wie folgt vor:

1. Fügen Sie einen virtuellen Lastausgleichsserver vom Typ SSL hinzu.
2. Binden Sie ein SHA2/SHA256-Zertifikat.
3. Aktivieren Sie das Standardprofil.
4. Binden Sie das sichere Front-End-Profil an den virtuellen SSL-Server.

Abrufen einer A+-Bewertung für einen virtuellen SSL-Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <serviceType> <IPAddress> <port>
bind ssl vserver <vServerName> -certkeyName <string>
set ssl parameter -defaultProfile ENABLED
```



```
set ssl vserver <vServerName> -sslProfile
   ns_default_ssl_profile_secure_frontend
show ssl vserver [<vServerName>]
<!--NeedCopy-->
```

Beispiel:

```
add lb vserver ssl-vsvr SSL 192.0.2.240 443

bind ssl vserver ssl-vsvr -certkeyName letrsa

set ssl parameter -defaultProfile ENABLED

Save your configuration before enabling the Default profile. You cannot
    undo the changes. Are you sure you want to enable the Default
   profile? [Y/N]y

set ssl vserver ssl-vsvr -sslProfile
   ns_default_ssl_profile_secure_frontend
<!--NeedCopy-->
```

```
sh ssl vserver ssl-vsvr

    Advanced SSL configuration for VServer ssl-vsvr:
    Profile Name :ns_default_ssl_profile_secure_frontend
    1) CertKey Name: letrsa     Server Certificate
Done
<!--NeedCopy-->
```

```
sh ssl profile ns_default_ssl_profile_secure_frontend

    1) Name: ns_default_ssl_profile_secure_frontend (Front-End)
    SSLv3: DISABLED  TLSv1.0: DISABLED  TLSv1.1: DISABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Client Auth: DISABLED
    Use only bound CA certificates: DISABLED
    Strict CA checks:                  NO
    Session Reuse: ENABLED   Timeout: 120 seconds
    DH: DISABLED
```



```
10      DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
           ENABLED     Refresh Count: 0
11      Deny SSL Renegotiation                NONSECURE
12      Non FIPS Ciphers: DISABLED
13      Cipher Redirect: DISABLED
14      SSL Redirect: DISABLED
15      Send Close-Notify: YES
16      Strict Sig-Digest Check: DISABLED
17      Zero RTT Early Data: DISABLED
18      DHE Key Exchange With PSK: NO
19      Tickets Per Authentication Context: 1
20      Push Encryption Trigger: Always
21      PUSH encryption trigger timeout:  1 ms
22      SNI: DISABLED
23      OCSP Stapling: DISABLED
24      Strict Host Header check for SNI enabled SSL sessions:
                              NO
25      Push flag:             0x0 (Auto)
26      SSL quantum size:                8 kB
27      Encryption trigger timeout       100 mS
28      Encryption trigger packet count: 45
29      Subject/Issuer Name Insertion Format:  Unicode
30      SSL Interception: DISABLED
31      SSL Interception OCSP Check: ENABLED
32      SSL Interception End to End Renegotiation: ENABLED
33      SSL Interception Maximum Reuse Sessions per Server:   10
34      Session Ticket: DISABLED
35      HSTS: ENABLED
36      HSTS IncludeSubDomains: YES
37      HSTS Max-Age: 15552000
38      ECC Curve: P_256, P_384, P_224, P_521
39      1) Cipher Name: SECURE    Priority :1
40      Description: Predefined Cipher Alias
41      1) Vserver Name: v2
42  Done
43  <!--NeedCopy-->
```

Abrufen einer A+-Bewertung für einen virtuellen SSL-Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und wählen Sie einen virtuellen SSL-Server aus.
2. Klicken Sie unter Erweiterte Einstellungen auf SSL-Profil.
3. Wählen Sie ns_default_ssl_profile_secure_frontend aus.

4. Klicken Sie auf OK.
5. Klicken Sie auf Fertig.

Anhang A: Beispielmigration der SSL-Konfiguration nach dem Upgrade

October 5, 2021

Hinweis: Dieser Inhalt wurde entfernt, da das SSL-Migrationsskript für das neue Standardprofil nicht mehr unterstützt wird.

Anhang B: Standardeinstellungen für Front-End- und Back-End-SSL-Profile

October 5, 2021

Ein Standard-Front-End-Profil hat die folgenden Einstellungen:

```
sh ssl profile ns_default_ssl_profile_frontend

1)Name: ns_default_ssl_profile_frontend

      Configuration for Front-End SSL profile
      DH: DISABLED
      Ephemeral RSA: ENABLED          Refresh Count: 0
      Session Reuse: ENABLED          Timeout: 120 seconds
      Non FIPS Ciphers: DISABLED
      Cipher Redirect: ENABLED   Redirect URL: http://10.102.28.212/
         redirect.html
      Client Auth: DISABLED
      SSL Redirect: DISABLED
      SNI: DISABLED
      SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
         ENABLED
      Push Encryption Trigger: Always
      PUSH encryption trigger timeout:     1 ms
      Send Close-Notify: YES
      Push flag: 0x0 (Auto)
      Deny SSL Renegotiation          NO
      SSL quantum size:          8 kB
```



```
21      Strict CA checks:          NO
22      Encryption trigger timeout 100 mS
23      Encryption trigger packet count:     45
24      Use only bound CA certificates: DISABLED
25      Subject/Issuer Name Insertion Format: Unicode
26      Strict Host Header check for SNI enabled SSL sessions:          NO
27
28      ECC Curve: P_256, P_384, P_521
29
30  1)  Cipher Name: AES     Priority :2
31      Description: Predefined Cipher Alias
32
33  1)  Vserver Name: v1
34  2)  Vserver Name: nshttps-::1l-443
35  3)  Vserver Name: nsrpcs-::1l-3008
36  4)  Vserver Name: nskrpcs-127.0.0.1-3009
37  5)  Vserver Name: nshttps-127.0.0.1-443
38  6)  Vserver Name: nsrpcs-127.0.0.1-3008
39  Done
40  <!--NeedCopy-->
```

Ein Standard-Back-End-Profil hat die folgenden Einstellungen:

```
1  sh ssl profile ns_default_ssl_profile_backend
2
3  1)Name: ns_default_ssl_profile_backend
4
5       Configuration for Back-End SSL profile
6       Session Reuse: ENABLED          Timeout: 300 seconds
7       Non FIPS Ciphers: DISABLED
8       Server Auth: DISABLED
9       SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: DISABLED  TLSv1.2:
           DISABLED
10      Push Encryption Trigger: Always
11      PUSH encryption trigger timeout:     1 ms
12      Send Close-Notify: YES
13      Push flag: 0x0 (Auto)
14      Deny SSL Renegotiation          ALL
15      SSL quantum size:          8 kB
16      Strict CA checks:          NO
17      Encryption trigger timeout 100 mS
18      Encryption trigger packet count:     45
19      Use only bound CA certificates: DISABLED
```



```
20
21      ECC Curve: P_256, P_224, P_521
22
23 1)   Cipher Name: AES     Priority :1
24      Description: Predefined Cipher Alias
25
26 2)   Cipher Name: RC4     Priority :2
27      Description: Predefined Cipher Alias
28
29 1)   Service Name: s2
30 2)   Service Name: s1
31 Done
32 <!--NeedCopy-->
```

Legacy-SSL-Profil

October 5, 2021

> **Hinweis:**
>
> Citrix empfiehlt, die erweiterten Profile anstelle von Legacy-Profilen zu verwenden. Informationen zur erweiterten Profilinfrastruktur finden Sie unter SSL-Profilinfrastruktur.

Wichtig:

> Binden Sie ein SSL-Profil an einen virtuellen SSL-Server. Binden Sie ein DTLS-Profil nicht an einen virtuellen SSL-Server. Informationen zu DTLS-Profilen finden Sie unter DTLS-Profile.

Sie können ein SSL-Profil verwenden, um anzugeben, wie ein Citrix ADC SSL-Datenverkehr verarbeitet. Das Profil ist eine Sammlung von SSL-Parametereinstellungen für SSL-Entitäten, wie z. B. virtuelle Server, Dienste und Dienstgruppen, und bietet einfache Konfiguration und Flexibilität. Sie sind nicht darauf beschränkt, nur einen Satz globaler Parameter zu konfigurieren. Sie können mehrere Sets (Profile) globaler Parameter erstellen und verschiedenen SSL-Entitäten unterschiedliche Sets zuweisen. SSL-Profile werden in zwei Kategorien eingeteilt:

- Front-End-Profile, die Parameter enthalten, die für die Front-End-Entity gelten. Das heißt, sie gelten für die Entität, die Anforderungen von einem Client empfängt.
- Back-End-Profile, die Parameter enthalten, die für die Back-End-Entität gelten. Das heißt, sie gelten für die Entität, die Clientanforderungen an einen Server sendet.

Im Gegensatz zu einem TCP- oder HTTP-Profil ist ein SSL-Profil optional. Daher gibt es kein Standard-SSL-Profil. Das gleiche Profil kann über mehrere Elemente hinweg wiederverwendet werden. Wenn einer Entität kein Profil zugeordnet ist, gelten die auf globaler Ebene festgelegten Werte. Für dynamisch erlernte Dienste gelten aktuelle globale Werte.

In der folgenden Tabelle sind die Parameter aufgeführt, die Teil jedes Profils sind.

Frontprofil	Back-End-Profil
cipherRedirect, cipherURL	denySSLReneg
clearTextPort*	encryptTriggerPktCount
clientAuth, clientCert	nonFipsCiphers
denySSLReneg	pushEncTrigger
dh, dhFile, dhCount	pushEncTriggerTimeout
dropReqWithNoHostHeader	pushFlag
encryptTriggerPktCount	quantumSize
eRSA, eRSACount	serverAuth
insertionEncoding	commonName
nonFipsCiphers	sessReuse, sessTimeout
pushEncTrigger	`SNIEnable`
pushEncTriggerTimeout	ssl3
pushFlag	sslTriggerTimeout
quantumSize	strictCAChecks
redirectPortRewrite	tls1
sendCloseNotify	-
sessReuse, sessTimeout	-
`SNIEnable`	-
ssl3	-
sslRedirect	-
sslTriggerTimeout	-
strictCAChecks	-
tls1, tls11, tls12	-

* Der Parameter ClearTextPort gilt nur für einen virtuellen SSL-Server.

Eine Fehlermeldung wird angezeigt, wenn Sie versuchen, einen Parameter festzulegen, der nicht Teil des Profils ist. Zum Beispiel, wenn Sie versuchen, den ClientAuth -Parameter in einem Back-End-Profil festzulegen.

Einige SSL-Parameter wie CRL-Speichergröße, OCSP-Cachegröße, UndefAction Control und UndefAction Data sind nicht Teil eines der vorhergehenden Profile, da diese Parameter von Entitäten unabhängig sind.

Ein SSL-Profil unterstützt die folgenden Vorgänge:

- Add - Erstellt ein SSL-Profil auf dem Citrix ADC. Geben Sie an, ob das Profil Frontend oder Backend ist. Frontend ist die Standardeinstellung.
- Set - Ändert die Einstellungen eines vorhandenen Profils.
- Unset - Legt die angegebenen Parameter auf ihre Standardwerte fest. Wenn Sie keine Parameter angeben, wird eine Fehlermeldung angezeigt. Wenn Sie ein Profil für eine Entität aufheben, wird das Profil von der Entität nicht gebunden.
- Entfernen (Remove) - Löscht ein Profil. Ein Profil, das von einer Entität verwendet wird, kann nicht gelöscht werden. Wenn Sie die Konfiguration löschen, werden alle Entitäten gelöscht. Dadurch werden auch die Profile gelöscht.
- Anzeigen — Zeigt alle Profile an, die im Citrix ADC verfügbar sind. Wenn ein Profilname angegeben wird, werden die Details dieses Profils angezeigt. Wenn eine Entität angegeben wird, werden die mit dieser Entität verknüpften Profile angezeigt.

Erstellen eines SSL-Profils mit der CLI

- Um ein SSL-Profil hinzuzufügen, geben Sie Folgendes ein:

```
add ssl profile <name> [-sslProfileType ( BackEnd | FrontEnd )]
<!--NeedCopy-->
```

- Um ein vorhandenes Profil zu ändern, geben Sie Folgendes ein:

```
set ssl profile <name>
<!--NeedCopy-->
```

- Geben Sie Folgendes ein, um die Einstellung eines vorhandenen Profils aufzuheben:

```
unset ssl profile <name> [-dh] [-dhFile] [-dhCount] [-eRSA]…
<!--NeedCopy-->
```

- Geben Sie Folgendes ein, um ein vorhandenes Profil aus einer Entität aufzuheben:


```
unset ssl vserver <vServerName>  - sslProfile
<!--NeedCopy-->
```

- Um ein vorhandenes Profil zu entfernen, geben Sie Folgendes ein:

```
rm ssl profile <name>
<!--NeedCopy-->
```

- Um ein vorhandenes Profil anzuzeigen, geben Sie Folgendes ein:

```
sh ssl profile <name>
<!--NeedCopy-->
```

Erstellen eines SSL-Profils mit der GUI

Navigieren Sie zu **System** > **Profile**, wählen Sie die Registerkarte SSL-Profile und erstellen Sie ein SSL-Profil.

strengere Kontrolle bei der Validierung von Clientzertifikaten aktivieren

Die Citrix ADC Appliance akzeptiert gültige Intermediate-CA-Zertifikate, wenn eine einzelne Root-CA sie ausgestellt hat. Das heißt, wenn nur das Root-CA-Zertifikat an den virtuellen Server gebunden ist und Root-CA eines der mit dem Clientzertifikat gesendeten Zwischenzertifikate validiert, vertraut die Appliance der Zertifikatskette und der Handshake ist erfolgreich.

Wenn ein Client jedoch eine Kette von Zertifikaten im Handshake sendet, können die Zwischenzertifikate nur mit einem CRL- oder OCSP-Responder validiert werden, wenn dieses Zertifikat an den virtuellen SSL-Server gebunden ist. Daher, selbst wenn eines der Zwischenzertifikate widerrufen wird, ist der Handshake erfolgreich. Als Teil des Handshakes sendet der virtuelle SSL-Server die Liste der Zertifizierungsstellenzertifikate, die an ihn gebunden sind. Für eine strengere Kontrolle können Sie den virtuellen SSL-Server so konfigurieren, dass er nur ein Zertifikat akzeptiert, das eines der an diesen virtuellen Server gebundenen CA-Zertifikate signiert hat. Dazu müssen Sie die `ClientAuthUseBoundCAChain` Einstellung im SSL-Profil aktivieren, das an den virtuellen Server gebunden ist. Der Handshake schlägt fehl, wenn eines der an den virtuellen Server gebundenen CA-Zertifikate das Clientzertifikat nicht signiert hat.

Angenommen, zwei Clientzertifikate, clientcert1 und clientcert2, sind von den Zwischenzertifikaten int-ca-a bzw. int-ca-b signiert. Die Zwischenzertifikate werden vom Stammzertifikat Root-CA signiert.

INT-CA-A und Root-CA sind an den virtuellen SSL-Server gebunden. Im Standardfall (ClientAuthUseBoundCAChain deaktiviert) werden sowohl clientcert1 als auch clientcert2 akzeptiert. Wenn ClientAuthUseBoundCAChain jedoch aktiviert ist, akzeptiert die Citrix ADC Appliance nur clientcert1.

Aktivieren Sie strengere Kontrolle der Clientzertifikatvalidierung mit der CLI

Geben Sie an der Eingabeaufforderung ein: `set ssl profile <name> -ClientAuthUseBoundCAChain Enabled`

Aktivieren Sie strengere Kontrolle der Clientzertifikatvalidierung mit der GUI

1. Navigieren Sie zu **System** > **Profile**, wählen Sie die Registerkarte **SSL-Profile**, und erstellen Sie ein SSL-Profil, oder wählen Sie ein vorhandenes Profil aus.
2. Wählen Sie **Client-Authentifizierung mit gebundener Zertifizierungsstellenkette**aktivieren aus.

Zertifikatsperrlisten

October 5, 2021

Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat bleibt in der Regel bis zum Ablaufdatum gültig. Unter bestimmten Umständen kann die Zertifizierungsstelle das ausgestellte Zertifikat jedoch vor dem Ablaufdatum widerrufen. Wenn beispielsweise der private Schlüssel eines Eigentümers kompromittiert wird, ändert sich der Name eines Unternehmens oder einer Person oder die Verknüpfung zwischen dem Subjekt und der Zertifizierungsstelle.

Eine Zertifikatsperrliste (Certificate Revocation List, CRL) identifiziert ungültige Zertifikate anhand der Seriennummer und des Ausstellers.

Zertifizierungsstellen stellen regelmäßig Zertifikatsperrlisten aus. Sie können die Citrix ADC Appliance so konfigurieren, dass eine Zertifikatsperrliste verwendet wird, um Clientanforderungen zu blockieren, die ungültige Zertifikate enthalten.

Wenn Sie bereits eine CRL-Datei von einer Zertifizierungsstelle haben, fügen Sie diese der Citrix ADC Appliance hinzu. Sie können Aktualisierungsoptionen konfigurieren. Sie können Citrix ADC auch so konfigurieren, dass die CRL-Datei automatisch in einem bestimmten Intervall von einem Webspeicherort oder einem LDAP-Standort aus synchronisiert wird. Die Appliance unterstützt CRLs im PEM- oder DER-Dateiformat. Stellen Sie sicher, dass Sie das Dateiformat der CRL-Datei angeben, die der Citrix ADC Appliance hinzugefügt wird.

Wenn Sie den ADC als Zertifizierungsstelle verwendet haben, um Zertifikate zu erstellen, die in SSL-Bereitstellungen verwendet werden, können Sie auch eine CRL erstellen, um ein bestimmtes Zertifikat

zu widerrufen. Diese Funktion kann beispielsweise verwendet werden, um sicherzustellen, dass selbstsignierte Zertifikate, die auf dem Citrix ADC erstellt werden, weder in einer Produktionsumgebung noch über ein bestimmtes Datum hinaus verwendet werden.

Hinweis:

Standardmäßig werden Zertifikatsperrlisten im Verzeichnis /var/netscaler/ssl auf der Citrix ADC Appliance gespeichert.

Erstellen einer CRL auf der ADC-Appliance

Da Sie die ADC-Appliance verwenden können, um als Zertifizierungsstelle zu fungieren und selbstsignierte Zertifikate zu erstellen, können Sie auch die folgenden Zertifikate widerrufen:

- Zertifikate, die Sie erstellt haben.
- Zertifikate, deren CA-Zertifikat Sie besitzen.

Die Appliance muss ungültige Zertifikate widerrufen, bevor eine Zertifikatsperrliste für diese Zertifikate erstellt wird. Die Appliance speichert die Seriennummern der gesperrten Zertifikate in einer Indexdatei und aktualisiert die Datei jedes Mal, wenn sie ein Zertifikat widerruft. Die Indexdatei wird automatisch erstellt, wenn ein Zertifikat zum ersten Mal gesperrt wird.

Widerrufen eines Zertifikats oder Erstellen einer Zertifikatsperrliste mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
create ssl crl <CAcertFile> <CAkeyFile> <indexFile> (-revoke <
    input_filename> | -genCRL <output_filename>)
<!--NeedCopy-->
```

Beispiel:

```
create ssl crl Cert-CA-1 Key-CA-1 File-Index-1 -revoke Invalid-1

create ssl crl Cert-CA-1 Key-CA-1 File-Index-1 -genCRL CRL-1
<!--NeedCopy-->
```

Widerrufen eines Zertifikats oder Erstellen einer Zertifikatsperrliste mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL**, und wählen Sie in der Gruppe Erste Schritte die Option CRL-Verwaltung aus.

2. Geben Sie die Zertifikatsdetails ein und **wählen Sie in der Liste Operation** auswählen die Option **Zertifikat widerrufen**oder **CRL generieren**aus.

Hinzufügen einer vorhandenen Zertifikatsperrliste zum ADC

Bevor Sie die Zertifikatsperrliste auf der Citrix ADC Appliance konfigurieren, stellen Sie sicher, dass die CRL-Datei lokal auf der Citrix ADC-Appliance gespeichert ist. In einem HA-Setup muss die CRL-Datei auf beiden ADC-Appliances vorhanden sein, und der Verzeichnispfad zur Datei muss auf beiden Appliances identisch sein.

Hinzufügen einer Zertifikatsperrliste auf dem Citrix ADC mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Zertifikatsperrliste auf dem Citrix ADC hinzuzufügen und die Konfiguration zu überprüfen:

```
add ssl crl <crlName> <crlPath> [-inform (DER | PEM)]

show ssl crl [<crlName>]
<!--NeedCopy-->
```

Beispiel:

```
> add ssl crl crl-one /var/netscaler/ssl/CRL-one -inform PEM

Done

> show ssl crl crl-one

            Name: crl-one   Status: Valid,  Days to expiration: 29
            CRL Path: /var/netscaler/ssl/CRL-one
            Format: PEM     CAcert: samplecertkey
            Refresh: DISABLED
            Version: 1
            Signature Algorithm: sha1WithRSAEncryption
            Issuer:  C=US,ST=California,L=Santa Clara,O=NetScaler Inc.,
               OU=SSL Acceleration,CN=www.ns.com/emailAddress=
               support@Citrix ADC appliance.com
            Last_update:Jun 15 10:53:53 2010 GMT
            Next_update:Jul 15 10:53:53 2010 GMT

    1)      Serial Number: 00
```



```
18              Revocation Date:Jun 15 10:51:16 2010 GMT
19      Done
20  <!--NeedCopy-->
```

Hinzufügen einer Zertifikatsperrliste auf dem Citrix ADC mit der GUI

Navigieren Sie zu **Traffic Management** > **SSL** > **CRL**, und fügen Sie eine CRL hinzu.

Konfigurieren von CRL-Aktualisierungsparametern

Eine Zertifikatsperrliste wird von einer Zertifizierungsstelle in regelmäßigen Abständen oder manchmal unmittelbar nach dem Widerruf eines bestimmten Zertifikats generiert und veröffentlicht. Citrix empfiehlt, die Zertifikatsperrlisten auf der Citrix ADC Appliance regelmäßig zu aktualisieren, um den Schutz vor Clients zu gewährleisten, die eine Verbindung mit ungültigen Zertifikaten herstellen möchten.

Die Citrix ADC Appliance kann Zertifikatsperrlisten von einem Webspeicherort oder einem LDAP-Verzeichnis aktualisieren. Wenn Sie Aktualisierungsparameter und einen Webspeicherort oder einen LDAP-Server angeben, muss die Zertifikatsperrliste zum Zeitpunkt der Ausführung des Befehls nicht auf der lokalen Festplatte vorhanden sein. Bei der ersten Aktualisierung wird eine Kopie auf dem lokalen Festplattenlaufwerk in dem durch den Parameter CRL-Datei angegebenen Pfad gespeichert. Der Standardpfad zum Speichern der Zertifikatsperrliste lautet /var/netscaler/ssl.

Hinweis: In Version 10.0 und höher ist die Methode zum Aktualisieren einer Zertifikatsperrliste standardmäßig nicht enthalten. Geben Sie eine HTTP- oder LDAP-Methode an. Wenn Sie ein Upgrade von einer früheren Version auf Version 10.0 oder höher durchführen, müssen Sie eine Methode hinzufügen und den Befehl erneut ausführen.

Konfigurieren der automatischen CRL-Aktualisierung mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um CRL Auto Refresh zu konfigurieren und die Konfiguration zu überprüfen:

```
1 set ssl crl <crlName> [-refresh ( ENABLED | DISABLED )] [-CAcert <
     string>] [-server <ip_addr|ipv6_addr|*> | -url <URL>] [-method (
     HTTP | LDAP )] [-port <port>] [-baseDN <string>] [-scope ( Base |
     One )] [-interval <interval>] [-day <positive_integer>] [-time <HH:
     MM>][-bindDN <string>] {
2  -password  }
3   [-binary ( YES | NO )]
4
```



```
show ssl crl [<crlName>]
<!--NeedCopy-->
```

Beispiel:

```
    set CRL crl1  -refresh enabled -method ldap -inform DER -CAcert ca1
        -server 10.102.192.192 -port 389 -scope base -baseDN "cn=
       clnt_rsa4_multicert_der,ou=eng,o=ns,c=in" -time 00:01

    set ssl crl crl1 -refresh enabled -method http -cacert ca1 -port 80
        -time 00:10 -url http://10.102.192.192/crl/ca1.crl


    > sh crl

    1)         Name: crl1        Status: Valid,     Days to expiration:
        355
                CRL Path: /var/netscaler/ssl/crl1
                Format: PEM      CAcert: ca1
                Refresh: ENABLED          Method: HTTP
                URL: http://10.102.192.192/crl/ca1.crl
                   Port:80
                Refresh Time: 00:10
                Last Update: Successful, Date:Tue Jul  6 14:38:13 2010
    Done
<!--NeedCopy-->
```

Konfigurieren der automatischen CRL-Aktualisierung mit LDAP oder HTTP mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL > CRL**.
2. Öffnen Sie eine Zertifikatsperrliste, und wählen Sie **Automatische Zertifikatsperrliste aktivieren**.

> **Hinweis** Wenn die neue CRL vor der tatsächlichen Aktualisierungszeit im externen Repository aktualisiert wurde, wie im Feld **Letzte Aktualisierungszeit** der CRL angegeben, müssen Sie Folgendes tun: Aktualisieren Sie die CRL auf der Citrix ADC Appliance
>
> sofort.

Um die letzte Aktualisierungszeit anzuzeigen, wählen Sie die Zertifikatsperrliste aus, und klicken Sie auf **Details**.

Synchronisieren von Zertifikatsperrlisten

Die Citrix ADC Appliance verwendet die zuletzt verteilte Zertifikatsperrliste, um zu verhindern, dass Clients mit gesperrten Zertifikaten auf sichere Ressourcen zugreifen.

Wenn Zertifikatsperrlisten häufig aktualisiert werden, benötigt die Citrix ADC Appliance einen automatisierten Mechanismus, um die neuesten Zertifikatsperrlisten aus dem Repository abzurufen. Sie können die Appliance so konfigurieren, dass Zertifikatsperrlisten automatisch in einem angegebenen Aktualisierungsintervall aktualisiert werden.

Die Appliance verwaltet eine interne Liste der Zertifikatsperrlisten, die in regelmäßigen Abständen aktualisiert werden müssen. In diesen festgelegten Intervallen durchsucht die Appliance die Liste nach CRLs, die aktualisiert werden müssen. Es stellt dann eine Verbindung mit dem Remote-LDAP-Server oder HTTP-Server her, ruft die neuesten CRLs ab und aktualisiert dann die lokale CRL-Liste mit den neuen CRLs.

> **Hinweis:**
>
> Wenn die CRL-Prüfung auf obligatorisch gesetzt ist, wenn das CA-Zertifikat an den virtuellen Server gebunden ist und die anfängliche CRL-Aktualisierung fehlschlägt, wird die folgende Aktion für Verbindungen ergriffen:
>
> Alle Client-Authentifizierungsverbindungen mit demselben Aussteller wie die CRL werden bis zur CRL als REVOKED zurückgewiesen wird erfolgreich aktualisiert.

Sie können das Intervall angeben, in dem die CRL-Aktualisierung durchgeführt werden muss. Sie können auch die genaue Zeit angeben.

Synchronisieren der automatischen CRL-Aktualisierung mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
set ssl crl <crlName> [-interval <interval>] [-day <integer>] [-time <
    HH:MM>]
<!--NeedCopy-->
```

Beispiel:

```
set ssl crl CRL-1 -refresh ENABLE -interval MONTHLY -days 10 -time
    12:00
<!--NeedCopy-->
```


Synchronisieren der CRL-Aktualisierung mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL > CRL**.
2. Öffnen Sie eine Zertifikatsperrliste, wählen Sie **Automatische Zertifikatsperrliste aktivieren** und geben Sie das Intervall an.

Ausführen der Clientauthentifizierung mit einer Zertifikatsperrliste

Wenn eine Zertifikatsperrliste (Certificate Revocation List, CRL) auf einer Citrix ADC Appliance vorhanden ist, wird eine Zertifikatsperrlistenprüfung durchgeführt, unabhängig davon, ob die Zertifikatsperrlistenprüfung auf obligatorisch oder optional festgelegt ist.

Der Erfolg oder Misserfolg eines Handshake hängt von einer Kombination der folgenden Faktoren ab:

- Regel für die CRL-Prüfung
- Regel für die Clientzertifikatprüfung
- Status der für das Zertifizierungsstellenzertifikat konfigurierten Zertifikatsperrliste

In der folgenden Tabelle sind die Ergebnisse der möglichen Kombinationen für einen Handshake mit einem gesperrten Zertifikat aufgeführt.

Tabelle 1. Ergebnis eines Handshake mit einem Client unter Verwendung eines gesperrten Zertifikats

Regel für die CRL-Prüfung	Regel für die Clientzertifikatprüfung	Status der für das Zertifizierungsstellenzertifikat konfigurierten Zertifikatsperrliste	Ergebnis eines Handshake mit einem gesperrten Zertifikat
Optional	Optional	Fehlt	Erfolg
Optional	Erforderlich	Fehlt	Erfolg
Optional	Erforderlich	Vorhanden	Fehler
Erforderlich	Optional	Fehlt	Erfolg
Erforderlich	Erforderlich	Fehlt	Fehler
Erforderlich	Optional	Vorhanden	Erfolg
Erforderlich	Erforderlich	Vorhanden	Fehler
Optional/Obligatorisch	Optional	Abgelaufen	Erfolg
Optional/Obligatorisch	Erforderlich	Abgelaufen	Fehler

Hinweis:

- Die CRL-Prüfung ist standardmäßig optional. Um von optional zu obligatorisch oder umgekehrt zu wechseln, müssen Sie zuerst das Zertifikat vom virtuellen SSL-Server lösen und es dann nach dem Ändern der Option erneut binden.
- In der Ausgabe des Befehls `sh ssl vserver` bedeutet OCSP check: optional, dass eine CRL-Prüfung ebenfalls optional ist. Die CRL-Prüfungseinstellungen werden in der Ausgabe des `sh ssl vserver` Befehls nur angezeigt, wenn die CRL-Prüfung auf obligatorisch gesetzt ist. Wenn die CRL-Prüfung auf optional gesetzt ist, werden die Details der CRL-Prüfung nicht angezeigt.

So konfigurieren Sie die CRL-Prüfung mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
bind ssl vserver <vServerName> -certkeyName <string> [(-CA -crlCheck (
   Mandatory | Optional ))]
sh ssl vserver
<!--NeedCopy-->
```

Beispiel:

```
bind ssl vs v1 -certkeyName ca -CA -crlCheck mandatory
> sh ssl vs v1

Advanced SSL configuration for VServer v1:

DH: DISABLED
DH Private-Key Exponent Size Limit: DISABLED
Ephemeral RSA: ENABLED Refresh Count: 0
Session Reuse: ENABLED Timeout: 120 seconds
Cipher Redirect: DISABLED
SSLv2 Redirect: DISABLED
ClearText Port: 0
Client Auth: ENABLED Client Cert Required: Mandatory
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: DISABLED
OCSP Stapling: DISABLED
HSTS: DISABLED
```



```
19 HSTS IncludeSubDomains: NO
20 HSTS Max-Age: 0
21 SSLv2: DISABLED SSLv3: ENABLED TLSv1.0: ENABLED TLSv1.1: ENABLED TLSv1
       .2: ENABLED
22 Push Encryption Trigger: Always
23 Send Close-Notify: YES
24
25 ECC Curve: P_256, P_384, P_224, P_521
26
27 1) CertKey Name: ca CA Certificate CRLCheck: Mandatory CA_Name Sent
28
29 1) Cipher Name: DEFAULT
30 Description: Predefined Cipher Alias
31 Done
32 <!--NeedCopy-->
```

Konfigurieren der CRL-Prüfung mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie einen virtuellen SSL-Server.
2. Klicken Sie in den Abschnitt **Zertifikate**.
3. Wählen Sie ein Zertifikat aus, und wählen Sie in der Liste **OCSP und CRL Check** die Option **CRL Obligatorisch** aus.

Ergebnis eines Handshakes mit einem gesperrten oder gültigen Zertifikat

Regel für die CRL-Prüfung	Regel für die Clientzertifikat-prüfung	Status der für das Zerti-fizierungsstellen-zertifikat konfigurierten Zertifikatsper-rliste	Ergebnis eines Handshakes mit einem gesperrten Zertifikat	Ergebnis eines Handshakes mit gültigem Zertifikat
Erforderlich	Erforderlich	Vorhanden	Fehler	Erfolg
Erforderlich	Erforderlich	Abgelaufen	Fehler	Fehler
Erforderlich	Erforderlich	Fehlt	Fehler	Fehler
Erforderlich	Erforderlich	Nicht definiert	Fehler	Fehler
Optional	Erforderlich	Vorhanden	Fehler	Erfolg

Regel für die CRL-Prüfung	Regel für die Clientzertifikat-prüfung	Status der für das Zerti-fizierungsstellen-zertifikat konfigurierten Zertifikatsper-rliste	Ergebnis eines Handshakes mit einem gesperrten Zertifikat	Ergebnis eines Handshakes mit gültigem Zertifikat
Optional	Erforderlich	Abgelaufen	Erfolg	Erfolg
Optional	Erforderlich	Fehlt	Erfolg	Erfolg
Optional	Erforderlich	Nicht definiert	Erfolg	Erfolg
Erforderlich	Optional	Vorhanden	Erfolg	Erfolg
Erforderlich	Optional	Abgelaufen	Erfolg	Erfolg
Erforderlich	Optional	Fehlt	Erfolg	Erfolg
Erforderlich	Optional	Nicht definiert	Erfolg	Erfolg
Optional	Optional	Vorhanden	Erfolg	Erfolg
Optional	Optional	Abgelaufen	Erfolg	Erfolg
Optional	Optional	Fehlt	Erfolg	Erfolg
Optional	Optional	Nicht definiert	Erfolg	Erfolg

Überwachen des Zertifikatsstatus mit OCSP

October 5, 2021

Online Certificate Status Protocol (OCSP) ist ein Internetprotokoll, das verwendet wird, um den Status eines Client-SSL-Zertifikats zu bestimmen. Citrix ADC Appliances unterstützen OCSP gemäß RFC 2560. OCSP bietet erhebliche Vorteile gegenüber Zertifikatsperrlisten (Certificate Revocation Lists, CRLs) in Bezug auf zeitnahe Informationen. Der aktuelle Widerrufsstatus eines Kundenzertifikats ist besonders bei Transaktionen mit großen Geldsummen und wertvollen Aktiengeschäften nützlich. Außerdem werden weniger System- und Netzwerkressourcen benötigt. Die Citrix ADC Implementierung von OCSP umfasst Anforderungsbatching und Antwort-Caching.

OCSP-Implementierung

Die OCSP-Validierung auf einer Citrix ADC Appliance beginnt, wenn die Appliance während eines SSL-Handshakes ein Clientzertifikat erhält. Zur Validierung des Zertifikats erstellt die Appliance eine OCSP-

Anforderung und leitet sie an den OCSP-Responder weiter. Dazu verwendet die Appliance eine lokal konfigurierte URL. Die Transaktion befindet sich in einem angehaltenen Zustand, bis die Appliance die Antwort vom Server auswertet und festlegt, ob die Transaktion zugelassen oder abgelehnt werden soll. Wenn die Antwort des Servers über die konfigurierte Zeit hinaus verzögert wird und keine anderen Responder konfiguriert sind, lässt die Appliance die Transaktion zu oder zeigt einen Fehler an, je nachdem, ob die OCSP-Prüfung auf optional oder obligatorisch gesetzt wurde.

Die Appliance unterstützt das Stapeln von OCSP-Anforderungen und das Caching von OCSP-Antworten, um die Belastung des OCSP-Responders zu reduzieren und schnellere Antworten bereitzustellen.

OCSP-Anforderungsbatching

Jedes Mal, wenn die Appliance ein Clientzertifikat empfängt, sendet sie eine Anforderung an den OCSP-Responder. Um zu vermeiden, dass der OCSP-Responder überlastet wird, kann die Appliance den Status von mehr als einem Clientzertifikat in derselben Anforderung abfragen. Damit diese Funktion effizient funktioniert, muss ein Timeout definiert werden, damit die Verarbeitung eines einzelnen Zertifikats nicht übermäßig verzögert wird, während auf die Bildung eines Batches gewartet wird.

OCSP-Antwort-Zwischenspeicherung

Das Zwischenspeichern der vom OCSP-Responder empfangenen Antworten ermöglicht schnellere Antworten auf die Clients und reduziert die Belastung des OCSP-Responders. Nach Erhalt des Sperrstatus eines Clientzertifikats vom OCSP-Responder speichert die Appliance die Antwort lokal für einen vordefinierten Zeitraum. Wenn ein Clientzertifikat während eines SSL-Handshake empfangen wird, überprüft die Appliance zunächst ihren lokalen Cache auf einen Eintrag für dieses Zertifikat. Wenn ein Eintrag gefunden wird, der noch gültig ist (innerhalb des Cache-Timeoutlimits), wird er ausgewertet und das Clientzertifikat wird akzeptiert oder abgelehnt. Wenn kein Zertifikat gefunden wird, sendet die Appliance eine Anforderung an den OCSP-Responder und speichert die Antwort für eine konfigurierte Dauer im lokalen Cache.

> **Hinweis**: Ab Release 12.1 Build 49.x wird das Cache-Timeout-Limit jetzt auf maximal 43200 Minuten (30 Tage) erhöht. Früher war die Grenze 1440 Minuten (ein Tag). Das erhöhte Limit hilft, die Suchvorgänge auf dem OCSP-Server zu reduzieren und SSL/TLS-Verbindungsfehler zu vermeiden, falls der OCSP-Server aufgrund von Netzwerkproblemen oder anderen Problemen nicht erreichbar ist.

Konfiguration des OCSP-Responders

Die Konfiguration von OCSP beinhaltet das Hinzufügen eines OCSP-Responders, das Binden des OCSP-Responders an ein Zertifikat der Zertifizierungsstelle (Certification Authority, CA) und das Binden des

Zertifikats an einen virtuellen SSL-Server. Wenn Sie ein anderes Zertifikat an einen bereits konfigurierten OCSP-Responder binden müssen, müssen Sie zuerst den Responder aufheben und dann den Responder an ein anderes Zertifikat binden.

Hinzufügen eines OCSP-Responders mit der CLI

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

```
add ssl ocspResponder <name> -url <URL> [-cache ( ENABLED | DISABLED )
    [-cacheTimeout <positive_integer>]] [ -batchingDepth <
    positive_integer>][-batchingDelay <positive_integer>] [-resptimeout
    <positive_integer>] [-responderCert <string> | -trustResponder] [-
    producedAtTimeSkew <positive_integer>][-signingCert <string>][-
    useNonce ( YES | NO )][ -insertClientCert( YES | NO )]
<!--NeedCopy-->
```

```
bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
    positive_integer>]
<!--NeedCopy-->
```

```
bind ssl vserver <vServerName>@ (-certkeyName <string> ( CA [-ocspCheck
     ( Mandatory | Optional )]))
<!--NeedCopy-->
```

```
show ssl ocspResponder [<name>]
<!--NeedCopy-->
```

Beispiel:

```
add ssl ocspResponder ocsp_responder1 -url ”http:// www.myCA.org:80/
    ocsp/” -cache ENABLED -cacheTimeout 30 -batchingDepth 8 -
    batchingDelay 100 -resptimeout 100 -responderCert responder_cert -
    producedAtTimeSkew 300 -signingCert sign_cert  -insertClientCert YES
<!--NeedCopy-->
```



```
bind ssl certKey ca_cert -ocspResponder ocsp_responder1 -priority 1
<!--NeedCopy-->
```

```
bind ssl vserver vs1 -certkeyName ca_cert -CA -ocspCheck Mandatory
<!--NeedCopy-->
```

```
sh ocspResponder ocsp_responder1

    1)Name: ocsp_responder1
    URL: http://www.myCA.org:80/ocsp/, IP: 192.128.22.22
    Caching: Enabled        Timeout: 30 minutes
    Batching: 8 Timeout: 100 mS
    HTTP Request Timeout: 100mS
    Request Signing Certificate: sign_cert
    Response Verification: Full, Certificate: responder_cert
    ProducedAt Time Skew: 300 s
    Nonce Extension: Enabled
     Client Cert Insertion: Enabled
    Done
<!--NeedCopy-->
```

```
show certkey ca_cert

    Name: ca_cert     Status: Valid,   Days to expiration:8907
    Version: 3
    …

    1)  VServer name: vs1      CA Certificate
    1)  OCSP Responder name: ocsp_responder1     Priority: 1
Done
<!--NeedCopy-->
```

```
sh ssl vs vs1

    Advanced SSL configuration for VServer vs1:
    DH: DISABLED
```



```
5       ...
6
7       1) CertKey Name: ca_cert CA Certificate OCSPCheck: Mandatory
8       1) Cipher Name: DEFAULT
9         Description: Predefined Cipher Alias
10      Done
11  <!--NeedCopy-->
```

Ändern eines OCSP-Responders mit der CLI

Sie können den Respondernamen nicht ändern. Alle anderen Parameter können mit dem `set ssl ocspResponder` Befehl geändert werden.

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

```
1  set ssl ocspResponder <name> [-url <URL>] [-cache ( ENABLED | DISABLED)
       ] [-cacheTimeout <positive_integer>] [-batchingDepth <
       positive_integer>] [-batchingDelay <positive_integer>] [-resptimeout
        <positive_integer>] [ -responderCert <string> | -trustResponder][-
       producedAtTimeSkew <positive_integer>][-signingCert <string>] [-
       useNonce ( YES | NO )]
2
3  unbind ssl certKey [<certkeyName>] [-ocspResponder <string>]
4
5  bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
       positive_integer>]
6
7  show ssl ocspResponder [<name>]
8  <!--NeedCopy-->
```

Konfigurieren eines OCSP-Responders mit der GUI

1. Navigieren Sie zu **Traffic Management** > **SSL** > **OCSP-Responder**, und konfigurieren Sie einen OCSP-Responder.
2. Navigieren Sie zu **Traffic Management** > **SSL** > **Zertifikate**, wählen Sie ein Zertifikat aus, und wählen Sie in der Liste **Aktion** die Option **OCSP-Bindings** aus. Binden Sie einen OCSP-Responder.
3. Navigieren Sie zu **Datenverkehrsverwaltung** > **Lastenausgleich** > **Virtuelle Server**, öffnen Sie einen virtuellen Server, und klicken Sie im Abschnitt Zertifikate, um ein Zertifizierungsstellenzertifikat zu binden.

4. Wählen Sie optional **OCSP Obligatorisch**.

OCSP-Heftung

December 7, 2021

Die Citrix ADC Implementierung von CRL und OCSP meldet nur den Sperrstatus von Clientzertifikaten. Um den Sperrstatus eines Serverzertifikats zu überprüfen, das während eines SSL-Handshake empfangen wurde, muss ein Client eine Anforderung an eine Zertifizierungsstelle senden.

Bei Websites mit hohem Datenverkehr erhalten viele Clients das gleiche Serverzertifikat. Wenn jeder Client eine Abfrage für den Sperrstatus des Serverzertifikats gesendet hat, wird die Zertifizierungsstelle mit OCSP-Anforderungen überflutet, um die Gültigkeit des Zertifikats zu überprüfen.

OCSP-Heftlösung

Um unnötige Engpässe zu vermeiden, unterstützt die Citrix ADC Appliance nun das OCSP-Heften. Das heißt, die Appliance kann nun den Sperrstatus eines Serverzertifikats zum Zeitpunkt des SSL-Handshake an einen Client senden, nachdem der Zertifikatstatus von einem OCSP-Responder überprüft wurde. Der Sperrstatus eines Serverzertifikats wird auf die Antwort geheftet, die die Appliance als Teil des SSL-Handshake an den Client sendet. Um die OCSP-Heftfunktion verwenden zu können, müssen Sie sie auf einem virtuellen SSL-Server aktivieren und der Appliance einen OCSP-Responder hinzufügen.

Hinweis:

- Citrix ADC Appliances unterstützen die OCSP-Heftung gemäß RFC 6066.
- Das OCSP-Heften wird nur am Front-End von Citrix ADC Appliances unterstützt.

> **Wichtig:**
>
> Citrix ADC Unterstützung für OCSP-Heften ist auf Handshakes mit TLS-Protokoll Version 1.0 oder höher beschränkt.

OCSP-Antwort-Caching von Serverzertifikaten

Wenn ein Client während des SSL-Handshake den Sperrstatus des Serverzertifikats anfordert, überprüft die Appliance zunächst ihren lokalen Cache auf einen Eintrag für dieses Zertifikat. Wenn ein gültiger Eintrag gefunden wird, wird er ausgewertet und das Serverzertifikat und sein Status dem Client angezeigt. Wenn kein Sperrstatuseintrag gefunden wird, sendet die Appliance eine Anforderung für den Sperrstatus des Serverzertifikats an den OCSP-Responder. Wenn es eine

Antwort erhält, sendet es das Zertifikat und den Sperrstatus an den Client. Wenn das nächste Aktualisierungsfeld in der OCSP-Antwort vorhanden ist, wird die Antwort für die konfigurierte Zeitspanne zwischengespeichert (Wert, der im Timeout-Feld angegeben ist).

> **Hinweis**: Ab Release 12.1 Build 49.x können Sie die zwischengespeicherte Antwort des Serverzertifikats aus dem OCSP-Responder löschen, noch bevor das Timeout abläuft. Zuvor war es nicht möglich, den zwischengespeicherten Status im Zertifikatschlüsselpaar zu verwerfen, bis das konfigurierte Timeout vorbei war.

Um den zwischengespeicherten Status mit der CLI zu löschen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
clear ssl certKey <certkey name> -ocspstaplingCache
<!--NeedCopy-->
```

Beispiel:

```
clear ssl certKey s1 -ocspstaplingCache
<!--NeedCopy-->
```

So löschen Sie den zwischengespeicherten Status mit der GUI

1. Navigieren Sie in der Benutzeroberfläche zu **Traffic Management** > **SSL** > **Zertifikate** > **CA-Zertifikate** .
2. Wählen Sie im Detailbereich ein Zertifikat aus.
3. Wählen Sie in der Liste **Aktion auswählen** die Option **Löschen** aus. Wenn Sie zur Bestätigung aufgefordert werden, klicken Sie auf **Ja**.

OCSP-Heftkonfiguration

Beim Konfigurieren von OCSP-Heften müssen Sie das Feature aktivieren und OCSP konfigurieren. Um OCSP zu konfigurieren, müssen Sie einen OCSP-Responder hinzufügen, den OCSP-Responder an ein Zertifizierungsstellenzertifikat binden und das Zertifikat an einen virtuellen SSL-Server binden.

> **Hinweis:**
>
> OCSP-Responder mit nur HTTP-basierter URL werden unterstützt.

Aktivieren der OCSP-Heftung mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set ssl vserver <name> -ocspstapling [ENABLED | DISABLED]
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver vip1 -ocspStapling ENABLED
Done

sh ssl vserver vip1

      Advanced SSL configuration for VServer vip1:
      DH: DISABLED
      DH Private-Key Exponent Size Limit: DISABLED Ephemeral RSA:
         ENABLED Refresh Count: 0
      Session Reuse: ENABLED Timeout: 120 seconds
      Cipher Redirect: DISABLED
      SSLv2 Redirect: DISABLED
      ClearText Port: 0
      Client Auth: DISABLED
      SSL Redirect: DISABLED
      Non FIPS Ciphers: DISABLED
      SNI: ENABLED
      OCSP Stapling: ENABLED
      SSLv2: DISABLED SSLv3: DISABLED TLSv1.0: ENABLED  TLSv1.1: ENABLED
           TLSv1.2: ENABLED
      Push Encryption Trigger: Always
      Send Close-Notify: YES

      ECC Curve: P_256, P_384, P_224, P_521

     1) CertKey Name: server_certificate1 Server Certificate

     1) Cipher Name: DEFAULT
      Description: Default cipher list with encryption strength >= 128
         bit
Done
<!--NeedCopy-->
```

Hinweis: Wenn das standardmäßige (erweiterte) Profil aktiviert ist, verwenden Sie den `set ssl profile <profile name> -ocspStapling [ENABLED | DISABLED]` Befehl, um OCSP zu aktivieren oder zu deaktivieren.

Aktivieren der OCSP-Heftung mit der GUI

1. Navigieren Sie zu **Traffic Management** > **SSL** > **Virtueller Server** .
2. Öffnen Sie einen virtuellen Server, und wählen Sie unter **SSL-Parameter OCSP-Stapling**aus.

OCSP-Konfiguration

Ein OCSP-Responder wird dynamisch oder manuell hinzugefügt, um OCSP-Stapelanforderungen zu senden. Ein interner Responder wird dynamisch hinzugefügt, wenn Sie ein Serverzertifikat und dessen Ausstellerzertifikat basierend auf der OCSP-URL im Serverzertifikat hinzufügen. Ein manueller OCSP-Responder wird von der CLI oder GUI hinzugefügt. Um eine OCSP-Anforderung für ein Serverzertifikat zu senden, wählt die Citrix ADC Appliance einen OCSP-Responder basierend auf der Priorität aus, die ihm beim Binden an ein Ausstellerzertifikat zugewiesen wurde. Wenn ein Responder eine OCSP-Staplungsanforderung nicht sendet, wird der Responder mit der nächsthöheren Priorität zum Senden der Anforderung ausgewählt. Wenn beispielsweise nur ein Responder manuell konfiguriert und fehlschlägt und ein dynamisch gebundener Responder vorhanden ist, wird er zum Senden der OCSP-Anforderung ausgewählt.

Wenn die OCSP-URL nicht HTTP ist, wird kein interner OCSP-Responder erstellt.

> **Hinweis:**
>
> Ein manuell hinzugefügter OCSP-Responder hat Vorrang vor einem dynamisch hinzugefügten Responder.

Unterschied zwischen einem manuell erstellten OCSP-Responder und einem intern erstellten OCSP-Responder

Manuell erstellter OCSP-Responder	Intern (dynamisch) erstellter OCSP-Responder
Erstellt manuell und explizit an das Ausstellerzertifikat mit einer Priorität gebunden.	Beim Hinzufügen eines Serverzertifikats und seines Ausstellerzertifikats (CA-Zertifikat) wird standardmäßig erstellt und gebunden. Name beginnt mit ns_internal_.
Die Priorität zwischen 1 und 127 ist für einen konfigurierten Responder reserviert.	Priorität wird automatisch ab 128 zugewiesen.
URL und Batching-Tiefe können geändert werden.	URL und Batching-Tiefe können nicht geändert werden.

Direkt gelöscht.	Wird nur gelöscht, wenn Sie das Serverzertifikat oder das Zertifizierungsstellenzertifikat löschen.
Kann an jedes Zertifizierungsstellenzertifikat gebunden werden.	Standardmäßig an ein Zertifizierungsstellenzertifikat gebunden. Kann nicht an ein anderes Zertifizierungsstellenzertifikat gebunden werden.
In der Konfiguration gespeichert (ns.conf).	Befehle zum Hinzufügen werden nicht in der Konfiguration gespeichert. Es werden nur gesetzte Befehle gespeichert.
Wenn Sie drei OCSP-Responder an dasselbe Ausstellerzertifikat mit den Prioritäten 1, 2 und 3 binden und später die Bindung von Priorität 2 aufheben, sind die anderen Prioritäten nicht betroffen.	Drei OCSP-Responder sind automatisch an ein Emittentenzertifikat mit den Prioritäten 128, 129 und 130 gebunden. Wenn Sie das Serverzertifikat entfernen, das zum Erstellen eines Responders mit Priorität 129 verwendet wurde, wird dieser Responder gelöscht. Außerdem wird die Priorität für den nächsten Responder (Priorität 130) automatisch auf 129 geändert.

> **Beispiel für die Anforderungsbehandlung**:

1. Fügen Sie einen virtuellen Server (VIP1) hinzu.
2. Fügen Sie das Ausstellerzertifikat (CA1) hinzu und binden Sie es an VIP1.
3. Fügen Sie drei Zertifikate S1, S2 und S3 hinzu. Interne Responder bzw. Interne Responder bzw. Resp1, Resp2 und Resp3 werden standardmäßig erstellt.
4. Binden Sie S3 an VIP1.
5. Eine Anfrage kommt an VIP1. Responder bzw. 3 ist ausgewählt.

Um einen internen OCSP-Responder dynamisch zu erstellen, benötigt die Appliance Folgendes:

- Zertifikat des Ausstellers des Serverzertifikats (normalerweise das CA-Zertifikat).
- Zertifikatschlüsselpaar des Serverzertifikats. Dieses Zertifikat muss die von der Zertifizierungsstelle bereitgestellte OCSP-URL enthalten. Die URL wird als Name des dynamisch hinzugefügten internen Responders verwendet.

Ein interner OCSP-Responder hat dieselben Standardwerte wie ein manuell konfigurierter Responder.

> **Hinweis:**
>
> Caching ist bei einem internen Responder standardmäßig deaktiviert. Verwenden Sie den `set ssl ocspResponder` Befehl, um das Caching zu aktivieren.

Konfigurieren von OCSP mit der CLI

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

```
1 add ssl certKey <certkeyName> (-cert <string> [-password]) [-key <
      string> | -fipsKey <string> | -hsmKey <string>] [-inform <inform>]
      [-expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod <
      positive_integer>]] [-bundle ( YES | NO )]
2
3 add ssl ocspResponder <name> -url <URL> [-cache ( ENABLED | DISABLED )
      [-cacheTimeout <positive_integer>]] [-resptimeout <positive_integer
      >] [-responderCert <string> | -trustResponder] [-producedAtTimeSkew
      <positive_integer>][-signingCert <string>][-useNonce ( YES | NO )][
      -insertClientCert ( YES | NO )]
4
5 bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
      positive_integer>]
6
7 show ssl ocspResponder [<name>]
8 <!--NeedCopy-->
```

Die Parameter:

httpMethod:

HTTP-Methode verwendet, um OCSP-Anforderungen zu senden. Bei Anforderungen mit einer Länge von weniger als 255 Byte können Sie die HTTP-GET-Methode für Abfragen an einen OCSP-Server konfigurieren. Wenn Sie die GET-Methode angeben, die Länge jedoch größer als 255 Byte ist, verwendet die Appliance die Standardmethode (POST).

Mögliche Werte: GET, POST

Standardwert: POST

ocspUrlResolveTimeout:

Wartezeit in Millisekunden auf eine OCSP-URL-Auflösung. Nach Ablauf dieser Zeit wird der Responder mit der nächsthöheren Priorität ausgewählt. Wenn alle Responder fehlschlagen, wird je nach

den Einstellungen auf dem virtuellen Server eine Fehlermeldung angezeigt oder die Verbindung wird gelöscht.

Mindestwert: 100

Maximalwert: 2000

Beispiel:

```
add ssl certkey root_ca1  - cert root_cacert.pem
add ssl ocspResponder ocsp_responder1 -url ”http:// www.myCA.org:80/
    ocsp/” -cache ENABLED -cacheTimeout 30  -resptimeout 100 -
    responderCert responder_cert -producedAtTimeSkew 300 -signingCert
    sign_cert  -insertClientCert YES
bind ssl certKey root_ca1 -ocspResponder ocsp_responder1 -priority 1
sh ocspResponder ocsp_responder1
    1)Name: ocsp_responder1
    URL: http://www.myCA.org:80/ocsp/, IP: 192.128.22.22
    Caching: Enabled        Timeout: 30 minutes
    Batching: 8 Timeout: 100 mS
    HTTP Request Timeout: 100mS
    Request Signing Certificate: sign_cert
    Response Verification: Full, Certificate: responder_cert
    ProducedAt Time Skew: 300 s
    Nonce Extension: Enabled
     Client Cert Insertion: Enabled
    Done

show certkey root_ca1
    Name: root_ca1     Status: Valid,   Days to expiration:8907
    Version: 3
    …
    1)  OCSP Responder name: ocsp_responder1     Priority: 1
    Done
<!--NeedCopy-->
```

Ändern von OCSP mit der CLI

Sie können den Namen eines OCSP-Responders nicht ändern, aber Sie können den `set ssl ocspResponder` Befehl verwenden, um einen der anderen Parameter zu ändern.

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


```
set ssl ocspResponder <name> [-url <URL>] [-cache ( ENABLED | DISABLED)
    ] [-cacheTimeout <positive_integer>]  [-resptimeout <
    positive_integer>] [ -responderCert <string> | -trustResponder][-
    producedAtTimeSkew <positive_integer>][-signingCert <string>] [-
    useNonce ( YES | NO )]

unbind ssl certKey [<certkeyName>] [-ocspResponder <string>]

bind ssl certKey [<certkeyName>] [-ocspResponder <string>] [-priority <
    positive_integer>]

show ssl ocspResponder [<name>]
<!--NeedCopy-->
```

Konfigurieren von OCSP mit der GUI

1. Navigieren Sie zu **Traffic Management** > **SSL** > **OCSP-Responder**, und konfigurieren Sie einen OCSP-Responder.
2. Navigieren Sie zu **Traffic Management** > **SSL** > **Zertifikate**, wählen Sie ein Zertifikat aus, und wählen Sie in der Liste **Aktion** die Option **OCSP-Bindings** aus. **Binden Sie einen OCSP-Responder**.
3. Navigieren Sie zu **Datenverkehrsverwaltung** > **Lastenausgleich** > **Virtuelle Server**, öffnen Sie einen virtuellen Server, und klicken Sie im Abschnitt Zertifikate, um ein Zertifizierungsstellenzertifikat zu binden.
4. Wählen Sie optional **OCSP Obligatorisch**aus.

> **Hinweis:**
>
> Der Parameter “Clientzertifikat einfügen” in den `set ssl ocspResponder` Befehl `add ssl ocspResponder` und ist nicht mehr gültig. Das heißt, der Parameter wird während der Konfiguration ignoriert.

Verfügbare Verschlüsselungen auf Citrix ADC-Appliances

September 22, 2022

Ihre Citrix ADC-Appliance wird mit einem vordefinierten Satz von Verschlüsselungsgruppen geliefert. Um Verschlüsselungen zu verwenden, die nicht Teil der DEFAULT-Verschlüsselungsgruppe sind, müssen Sie sie explizit an einen virtuellen SSL-Server binden. Sie können auch eine benutzerdefinierte Verschlüsselungsgruppe erstellen, die an den virtuellen SSL-Server gebunden

werden soll. Weitere Informationen zum Erstellen einer benutzerdefinierten Chiffriergruppe finden Sie unter Konfigurieren benutzerdefinierter Chiffriergruppen auf der ADC-Appliance.

> **Hinweise**
>
> RC4-Chiffre ist nicht in der Standardchiffregruppe auf der Citrix ADC-Appliance enthalten. Es wird jedoch in der Software auf den N3-basierten Appliances unterstützt. Die RC4-Verschlüsselung, einschließlich des Handshakes, erfolgt in Software.
>
> Citrix empfiehlt, diese Verschlüsselung nicht zu verwenden, da sie von RFC 7465 als unsicher und veraltet eingestuft wird.
>
> Verwenden Sie den Befehl “Hardware anzeigen”, um festzustellen, ob Ihr Gerät über N3-Chips verfügt.

```
sh hardware

Platform: NSMPX-22000 16\*CPU+24\*IX+12\*E1K+2\*E1K+4*CVM N3 2200100

Manufactured on: 8/19/2013

CPU: 2900MHZ

Host Id: 1006665862

Serial no: ENUK6298FT

Encoded serial no: ENUK6298FT
<!--NeedCopy-->
```

- Um Informationen zu den Verschlüsselungssammlungen anzuzeigen, die standardmäßig am Front-End (an einen virtuellen Server) gebunden sind, geben Sie Folgendes ein: `sh cipher DEFAULT`
- Um Informationen zu den Verschlüsselungssammlungen anzuzeigen, die standardmäßig am Back-End (an einen Dienst) gebunden sind, geben Sie Folgendes ein: `sh cipher DEFAULT_BACKEND`
- Um Informationen zu allen auf der Appliance definierten Verschlüsselungsgruppen (Aliase) anzuzeigen, geben Sie Folgendes ein: `sh cipher`
- Um Informationen zu allen Verschlüsselungssammlungen anzuzeigen, die Teil einer bestimmten Verschlüsselungsgruppe sind, geben Sie Folgendes ein: `sh cipher <alias name>`. Zum Beispiel sh chiffre ECDHE.

Die folgenden Links führen die Verschlüsselungssammlungen auf, die auf verschiedenen Citrix ADC

Plattformen und auf externen Hardwaresicherheitsmodulen (HSMs) unterstützt werden:

- **Citrix ADC MPX/SDX (N3) -Appliance**: Verschlüsselungsunterstützung auf einer Citrix ADC MPX/SDX (N3) -Appliance
- **Citrix ADC MPX/SDX Intel Coleto-Appliance**: Verschlüsselungsunterstützung auf einer Citrix ADC MPX/SDX Intel Coleto SSL-Chip-basierten Appliance
- **Citrix ADC VPX Appliance**: Verschlüsselungsunterstützung auf einer Citrix ADC VPX Appliance
- **Citrix ADC MPX/SDX 14000 FIPS-Appliance**: Verschlüsselungsunterstützung auf einer Citrix ADC MPX/SDX 14000 FIPS-Appliance
- **Externes HSM (Thales/Safenet)**: Chiffre wird auf einem externen HSM unterstützt (Thales/Safenet)
- **Citrix ADC MPX/SDX (N2) -Appliance**: Verschlüsselungsunterstützung auf einer Citrix ADC MPX/SDX (N2) -Appliance
- **Citrix ADC MPX 9700 FIPS-Appliance**: Verschlüsselungsunterstützung auf einem Citrix ADC MPX 9700 FIPS mit Firmware 2.2
- **Citrix ADC VPX FIPS- und MPX FIPS-Appliances**: Verschlüsselungsunterstützung auf Citrix ADC VPX FIPS- und MPX FIPS-zertifizierten Appliances

> **Hinweis:**
>
> Informationen zur Unterstützung der DTLS-Verschlüsselung finden Sie unter Unterstützung der DTLS-Verschlüsselung auf Citrix ADC VPX-, MPX- und SDX-Appliances.

Tabelle1 - Unterstützung für virtuellen Server/Frontend-Service/interner Service:

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
TLS 1.3	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	Nicht unterstützt	13.0 alle Builds
	12.1—50.x (außer TLS1.3-CHACHA20-POLY1305-SHA256)	12.1—50.x (außer TLS1.3-CHACHA20-POLY1305-SHA256)	12.1–50.x	Nicht unterstützt	12.1–50.x
TLS 1.1/1.2	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G
	12.0 alle Builds	12.0 alle Builds	12.0 alle Builds	12.0 alle Builds	12.0 alle Builds für MPX 5900/8900, 12.0-57.x für MPX 15000-50G, 12,0-60.x für MPX 26000-100G
	11.1 alle Builds	11.1 alle Builds	11.1 alle Builds	11.1 alle Builds	11,1—56.x für MPX 5900/8900 und MPX 15000-50G, 11,1-60.x für MPX 26000-100 G
	11.0 alle Builds	11.0 alle Builds	11.0 alle Builds	11.0 alle Builds	11.0—70.x (nur bei MPX 5900/8900)

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	10.5 alle Builds	10.5 alle Builds	10.5–57.x	10.5–59.1359.e	10,5—67.x, 10,5-63,47 (nur auf MPX 5900/8900)
ECDHE/DHE (Beispiel TLS1-ECDHE-RSA-AES128-SHA)	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds
	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G
	12.0 alle Builds	12.0 alle Builds	12.0 alle Builds	12.0 alle Builds	12.0 alle Builds für MPX 5900/8900, 12.0-57.x für MPX 15000-50G, 12,0-60.x für MPX 26000-100G

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	11.1 alle Builds	11.1 alle Builds	11.1 alle Builds	11.1–51.x	11,1—56.x für MPX 5900/8900 und MPX 15000-50G, 11,1-60.x für MPX 26000-100 G
	11.0 alle Builds	11.0 alle Builds	11.0 alle Builds		11.0—70.114 (nur auf MPX 5900/8900)
	10.5–53.x	10.5–53.x	10.5 alle Builds		10,5—67.x, 10,5-63,47 (nur auf MPX 5900/8900)
AES-GCM (Beispiel TLS1.2-AES128-GCM-SHA256)	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds
	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.0 alle Builds	12.0 alle Builds	12.0 alle Builds	12.0 alle Builds	12.0 alle Builds für MPX 5900/8900, 12.0-57.x für MPX 15000-50G, 12,0-60.x für MPX 26000-100G
	11.1 alle Builds	11.1 alle Builds	11.1 alle Builds	11.1—51.x (siehe Hinweis)	11,1—56.x für MPX 5900/8900 und MPX 15000-50G, 11,1-60.x für MPX 26000-100 G
	11.0 alle Builds	11.0 alle Builds	11.0–66.x		11.0—70.114 (nur auf MPX 5900/8900)
	10.5–53.x	10.5–53.x			10,5—67.x, 10,5-63,47 (nur auf MPX 5900/8900)
SHA-2-Chiffren (Beispiel TLS1.2-AES-128-SHA256)	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G
	12.0 alle Builds	12.0 alle Builds	12.0 alle Builds	12.0 alle Builds	12.0 alle Builds für MPX 5900/8900, 12.0-57.x für MPX 15000-50G, 12,0-60.x für MPX 26000-100G
	11.1 alle Builds	11.1 alle Builds	11.1 alle Builds	11.1–52.x	11,1—56.x für MPX 5900/8900 und MPX 15000-50G, 11,1-60.x für MPX 26000-100 G
	11.0 alle Builds	11.0 alle Builds	11.0–66.x		11.0—72.x, 11,0-70,114 (nur auf MPX 5900/8900)

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	10.5–53.x	10.5–53.x			10,5—67.x, 10,5-63,47 (nur auf MPX 5900/8900)
ECDSA (Beispiel TLS1-ECDHE-ECDSA-AES256-SHA)	Nicht unterstützt	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds
	Nicht unterstützt	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G
	Nicht unterstützt	12.0 alle Builds	12.0-57.x	Nicht unterstützt	12.0 alle Builds für MPX 5900/8900, 12.0-57.x für MPX 15000-50G, 12,0-60.x für MPX 26000-100G

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
		11.1 alle Builds			11.1—56.x, 11.1-54,126 (Nur die ECC-Kurven P_256 und P_384 werden unterstützt.)
CHACHA20	Nicht unterstützt	13.0 alle Builds	13.0 alle Builds	Nicht unterstützt	13.0 alle Builds
	Nicht unterstützt	Nicht unterstützt	12.1 alle Builds	Nicht unterstützt	12,1—49.x (nur auf MPX 5900/8900)
	Nicht unterstützt	Nicht unterstützt	12.0–56.x	Nicht unterstützt	Nicht unterstützt

Tabelle 2 — Unterstützung von Backend-Diensten:

TLS 1.3 wird im Backend nicht unterstützt.

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
TLS 1.1/1.2	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G
	12.0 alle Builds	12.0 alle Builds	12.0 alle Builds	12.0 alle Builds	12.0 alle Builds für MPX 5900/8900, 12.0-57.x für MPX 15000-50G, 12,0-60.x für MPX 26000-100G
	11.1 alle Builds	11.1 alle Builds	11.1 alle Builds	11.1 alle Builds	11,1—56.x für MPX 5900/8900 und MPX 15000-50G, 11,1-60.x für MPX 26000-100 G
	11.0–50.x	11.0–50.x	11.0–66.x		11.0—70.119 (nur auf MPX 5900/8900)

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	10.5–59.x	10.5–59.x		10.5–59.1359.e	10,5—67.x, 10,5-63,47 (nur auf MPX 5900/8900)
ECDHE/DHE (Beispiel TLS1-ECDHE-RSA-AES128-SHA)	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds
	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G
	12.0 alle Builds	12.0 alle Builds	12.0–56.x	12.0 alle Builds	12.0 alle Builds für MPX 5900/8900, 12.0-57.x für MPX 15000-50G, 12,0-60.x für MPX 26000-100G

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	11.1 alle Builds	11.1 alle Builds		11.1–51.x	11,1—56.x für MPX 5900/8900 und MPX 15000-50G, 11,1-60.x für MPX 26000-100 G
	11.0–50.x	11.0–50.x			11.0—70.119 (nur auf MPX 5900/8900)
	10.5–58.x	10.5–58.x			10,5—67.x, 10,5-63,47 (nur auf MPX 5900/8900)
AES-GCM (Beispiel TLS1.2-AES128-GCM-SHA256)	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds
	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.0 alle Builds	12.0 alle Builds	Nicht unterstützt	12.0 alle Builds	12.0 alle Builds für MPX 5900/8900, 12.0-57.x für MPX 15000-50G, 12,0-60.x für MPX 26000-100G
	11.1 alle Builds	11.1 alle Builds		11.1–51.x	11,1—56.x für MPX 5900/8900 und MPX 15000-50G, 11,1-60.x für MPX 26000-100 G
SHA-2-Chiffren (Beispiel TLS1.2-AES-128-SHA256)	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds
	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	12.0 alle Builds	12.0 alle Builds	Nicht unterstützt	12.0 alle Builds	12.0 alle Builds für MPX 5900/8900, 12.0-57.x für MPX 15000-50G, 12,0-60.x für MPX 26000-100G
	11.1 alle Builds	11.1 alle Builds		11.1–52.x	11,1—56.x für MPX 5900/8900 und MPX 15000-50G, 11,1-60.x für MPX 26000-100 G
ECDSA (Beispiel TLS1-ECDHE-ECDSA-AES256-SHA)	Nicht unterstützt	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds	13.0 alle Builds
	Nicht unterstützt	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds	12.1 alle Builds für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100G

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	Nicht unterstützt	12.0 alle Builds	12.0–57.x	Nicht unterstützt	12.0 alle Builds für MPX 5900/8900, 12.0-57.x für MPX 15000-50G, 12,0-60.x für MPX 26000-100G
		11.1–51.x			11,1—56.x für MPX 5900/8900 und MPX 15000-50G, 11,1-60.x für MPX 26000-100G (nur die ECC-Kurven P_256 und P_384 werden unterstützt.)
CHACHA20	Nicht unterstützt	13.0 alle Builds	13.0 alle Builds	Nicht unterstützt	13.0 alle Builds

Protokoll/Plattform	MPX/SDX (N2)	MPX/SDX (N3)	VPX	MPX/SDX 14000** FIPS	MPX 5900/8900 MPX 15000-50G MPX 26000-100G
	Nicht unterstützt	Nicht unterstützt	12.1 alle Builds	Nicht unterstützt	12,1—49,x für MPX 5900/8900, 12,1-50.x für MPX 15000-50G und MPX 26000-100 G
	Nicht unterstützt	Nicht unterstützt	12.0–56.x	Nicht unterstützt	Nicht unterstützt

Eine detaillierte Liste der unterstützten ECDSA-Chiffren finden Sie unter Unterstützung von ECDSA Cipher Suites.

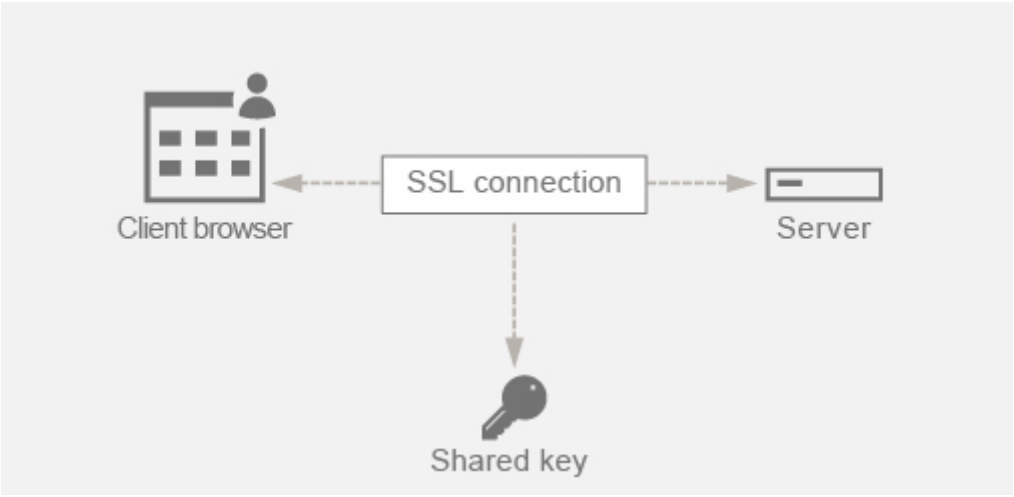
> Hinweis
>
> - Die TLS-Fallback_SCSV-Verschlüsselungssuite wird auf allen Appliances ab Version 10.5 Build 57.x unterstützt.
> - Die Unterstützung von HTTP Strict Transport Security (HSTS) ist richtlinienbasiert.
> - Alle signierten SHA-2-Zertifikate (SHA256, SHA384, SHA512) werden auf dem Front-End aller Appliances unterstützt. In Version 11.1 Build 54.x und höher werden diese Zertifikate auch im Back-End aller Appliances unterstützt. In Version 11.0 und früher werden nur signierte SHA256-Zertifikate im Backend aller Appliances unterstützt.
> - In Release 11.1 Build 52.x und früher werden die folgenden Chiffriergeräte nur am Frontend der MPX 9700 und MPX/SDX 14000 FIPS-Appliances unterstützt:
>   - TLS1.2-ECDHE-RSA-AES-256-SHA384
>   - TLS1.2-ECDHE-RSA-AES256-GCM-SHA384. From release 11.1 build 53.x, and in release 12.0, these ciphers are also supported on the back end.
> - Alle ChaCha20-Poly1035-Chiffren verwenden eine TLS-Pseudozufallsfunktion (PSF) mit der SHA-256-Hash-Funktion.

Perfect Forward Secrecy (PFS)

Perfect Forward Secrecy gewährleistet den Schutz der aktuellen SSL-Kommunikation, auch wenn der Sitzungsschlüssel eines Webservers zu einem späteren Zeitpunkt kompromittiert wird.

Warum brauchen Sie Perfect Forward Secrecy (PFS)?

Eine SSL-Verbindung wird verwendet, um die Daten zu sichern, die zwischen einem Client und einem Server übergeben werden. Diese Verbindung beginnt mit dem SSL-Handshake, der zwischen dem Browser eines Clients und dem kontaktierten Webserver stattfindet. Während dieses Handshakes tauschen der Browser und der Server bestimmte Informationen aus, um auf einen Sitzungsschlüssel zu gelangen, der als Mittel zur Verschlüsselung der Daten während des restlichen Kommunikationsweges dient.

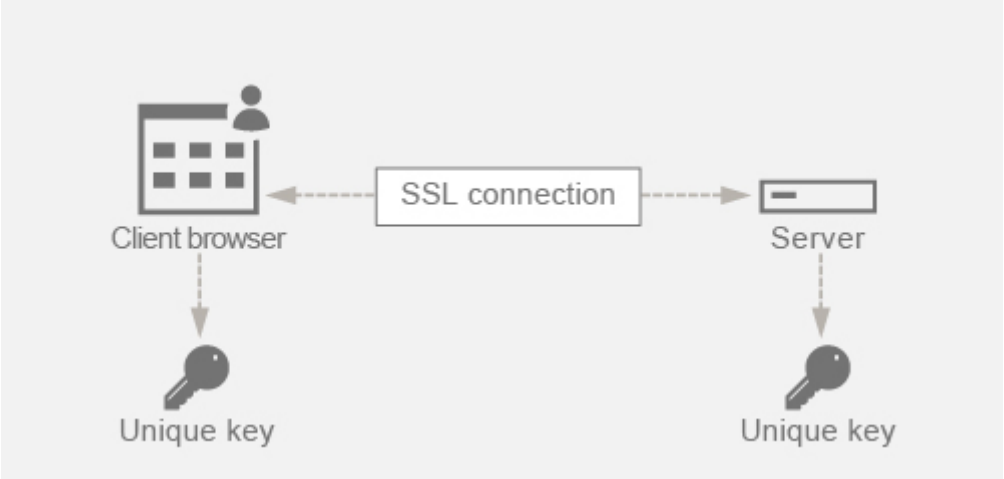


RSA ist der am häufigsten verwendete Algorithmus für den Schlüsselaustausch. Der Browser verwendet den öffentlichen Schlüssel des Servers, um das Pre-Master-Geheimnis zu verschlüsseln und an einen Server zu senden. Dieses Pre-Master-Geheimnis wird verwendet, um zum Sitzungsschlüssel zu gelangen. Das Problem beim RSA-Schlüsselaustauschansatz besteht darin, dass, wenn es einem Angreifer gelingt, den privaten Schlüssel des Servers zu irgendeinem Zeitpunkt in der Zukunft zu erhalten, der Angreifer das Vor-Master-Geheimnis erhält, mit dem der Sitzungsschlüssel abgerufen werden kann. Dieser Sitzungsschlüssel kann jetzt vom Angreifer verwendet werden, um alle SSL-Konversationen zu entschlüsseln. Dies bedeutet, dass Ihre historische SSL-Kommunikation früher sicher war, aber nicht mehr sicher ist, da der gestohlene private Schlüssel des Servers verwendet werden kann, um zum Sitzungsschlüssel zu gelangen und somit auch gespeicherte historische Konversationen zu entschlüsseln.

Die Notwendigkeit besteht darin, die vergangene SSL-Kommunikation auch dann schützen zu können, wenn der private Schlüssel des Servers gefährdet wurde. Hier kommt die Konfiguration von Perfect Forward Secrecy (PFS) zur Rettung.

Wie hilft PFS?

Perfect Forward Secrecy (PFS) schützt die vergangene SSL-Kommunikation, indem der Client und der Server für jede Sitzung einen neuen Schlüssel vereinbaren und die Berechnung dieses Sitzungsschlüssels geheim halten. Es funktioniert auf der Grundlage, dass ein Kompromiss eines Serverschlüssels nicht zu Kompromissen des Sitzungsschlüssels führen darf. Der Sitzungsschlüssel wird an beiden Enden separat abgeleitet und niemals über den Draht übertragen. Die Sitzungsschlüssel werden ebenfalls zerstört, sobald die Kommunikation abgeschlossen ist. Diese Fakten stellen sicher, dass selbst wenn jemand Zugriff auf den privaten Schlüssel des Servers erhält, nicht zum Sitzungsschlüssel gelangen kann und daher die Daten der Vergangenheit nicht entschlüsseln kann.



Erklärung mit Beispiel

Angenommen, wir verwenden DHE, um PFS zu erreichen. Der DH-Algorithmus stellt sicher, dass der Hacker, obwohl ein Hacker den privaten Schlüssel des Servers erhält, nicht zum Sitzungsschlüssel gelangen kann, da der Sitzungsschlüssel und die Zufallszahlen (die verwendet werden, um am Sitzungsschlüssel zu gelangen) an beiden Enden geheim gehalten und niemals über den Draht ausgetauscht werden.
PFS kann durch Verwendung des ephemeren Diffie-Hellman-Schlüsselaustauschs erreicht werden, der für jede SSL-Sitzung neue temporäre Schlüssel erstellt.

Die Kehrseite beim Erstellen eines Schlüssels für jede Sitzung ist, dass eine zusätzliche Berechnung erforderlich ist, dies kann jedoch durch die Verwendung der Elliptischen Kurve überwunden werden, die kleinere Schlüsselgrößen hat.

Konfigurieren von PFS auf Citrix ADC-Appliance

PFS kann auf einem Citrix ADC konfiguriert werden, indem DHE- oder ECDHE-Chiffern konfiguriert werden. Diese Chiffern stellen sicher, dass der erstellte geheime Sitzungsschlüssel nicht auf dem

Draht (DH-Algorithmus) geteilt wird und dass der Sitzungsschlüssel nur für kurze Zeit am Leben bleibt (Vergänglich). Beide Konfigurationen werden in den folgenden Abschnitten erläutert.

Hinweis: Die Verwendung von ECDHE-Chiffern anstelle von DHE macht die Kommunikation bei kleineren Schlüsselgrößen sicherer.

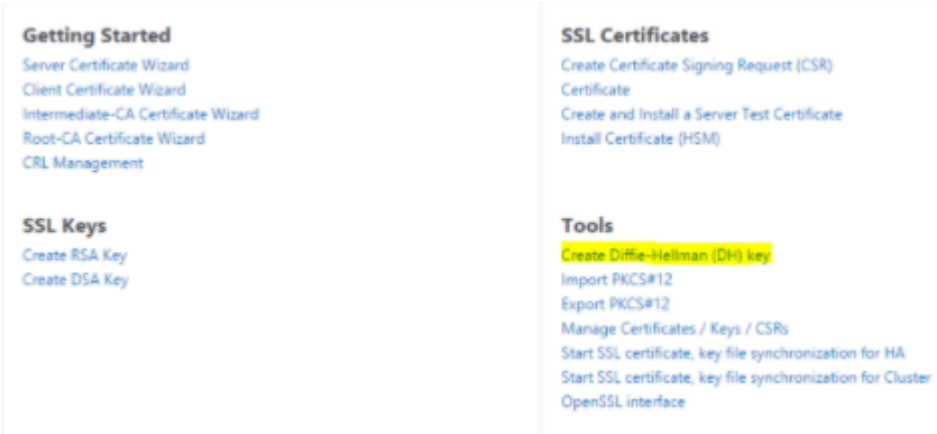
Konfigurieren Sie DHE mit der GUI

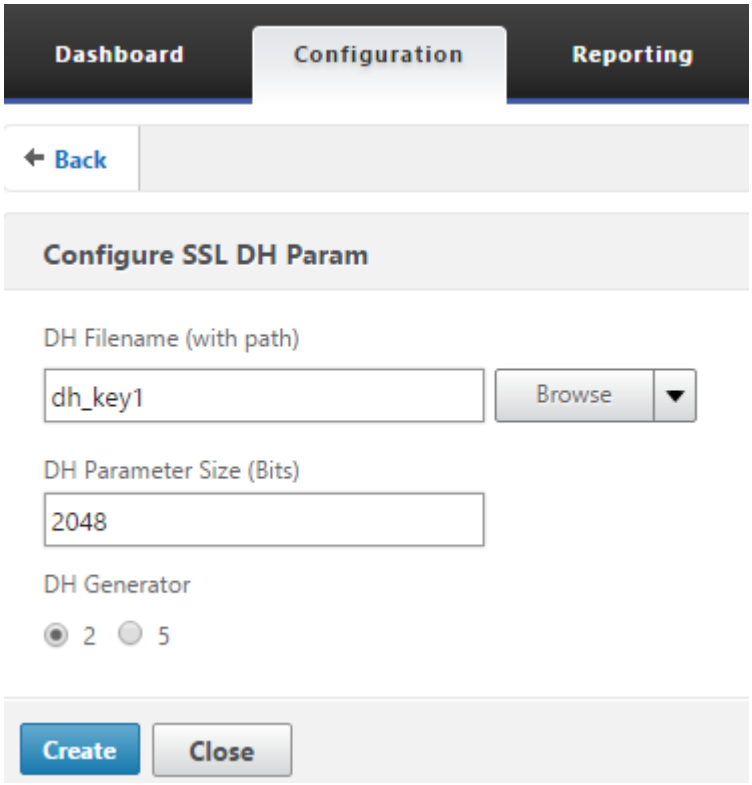
1. Generieren Sie einen DH-Schlüssel.

   a. Navigieren Sie zu **Traffic Management > SSL > Tools**.

   b. Klicken Sie auf **Diffie Helman (DH) Key erstellen**.

   Hinweis: Das Generieren eines 2048-Bit-DH-Schlüssels kann bis zu 30 Minuten dauern.



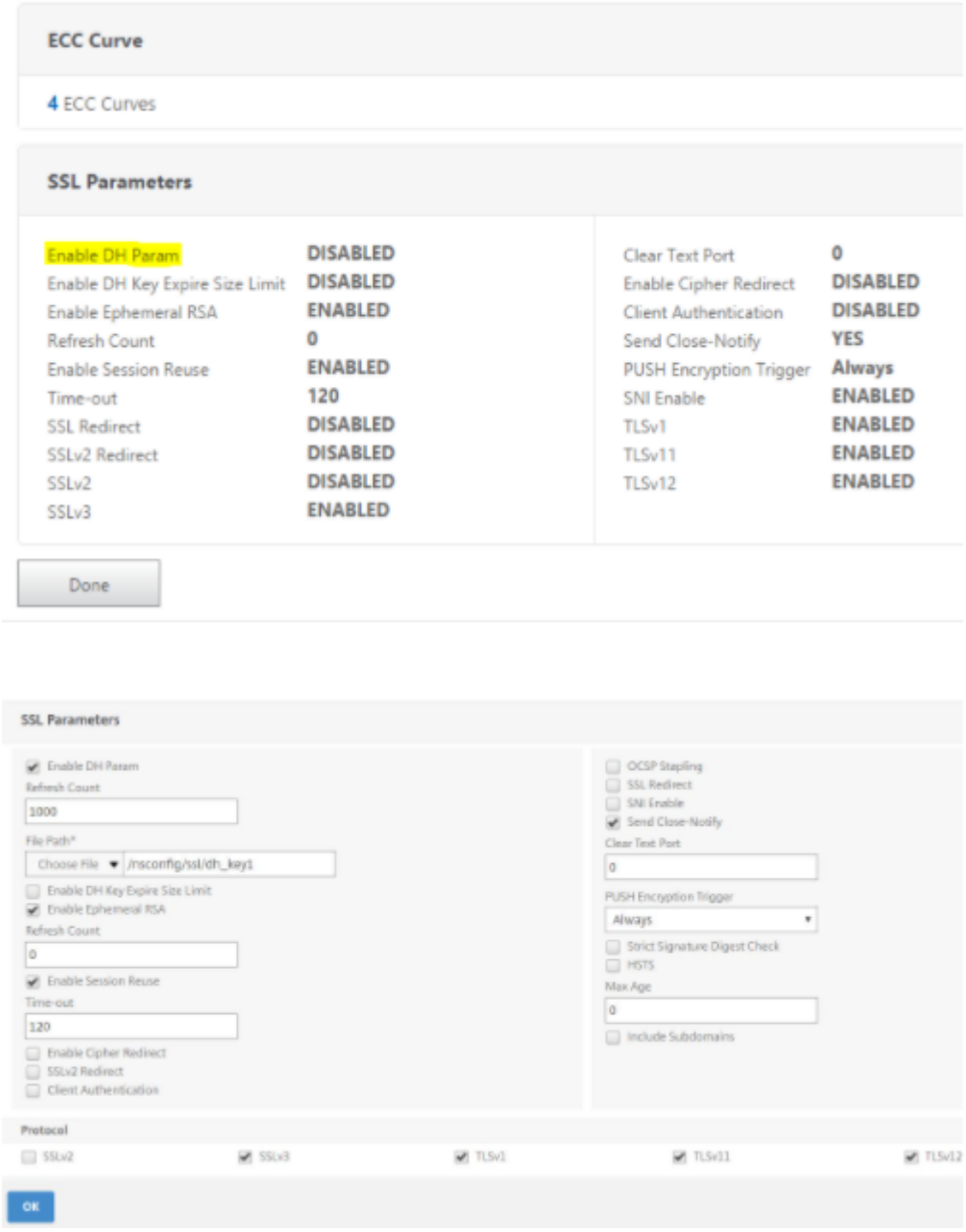


2. Aktivieren Sie DH Param für den virtuellen SSL-Server und fügen Sie den DH-Schlüssel an den virtuellen SSL-Server an.

   a. Navigieren Sie zu **Konfiguration > Traffic Management > Virtuelle Server**.

   b. Wählen Sie den virtuellen Server aus, auf dem Sie DH aktivieren möchten.

   c. Klicken Sie auf **Bearbeiten**, klicken Sie auf **SSL-Parameter**und dann auf **DH Param aktivieren**.



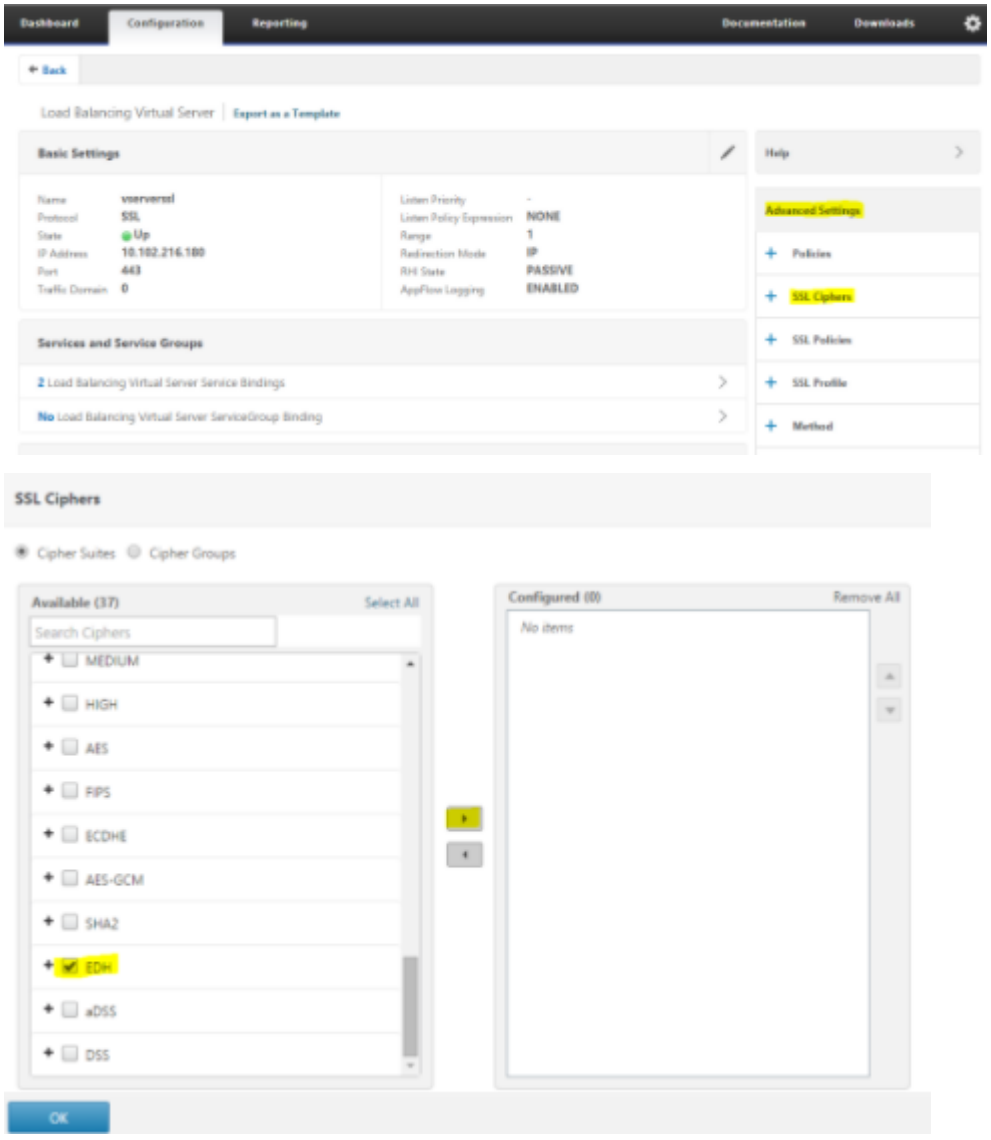
3. Binden Sie die DHE-Chiffern an den virtuellen Server.

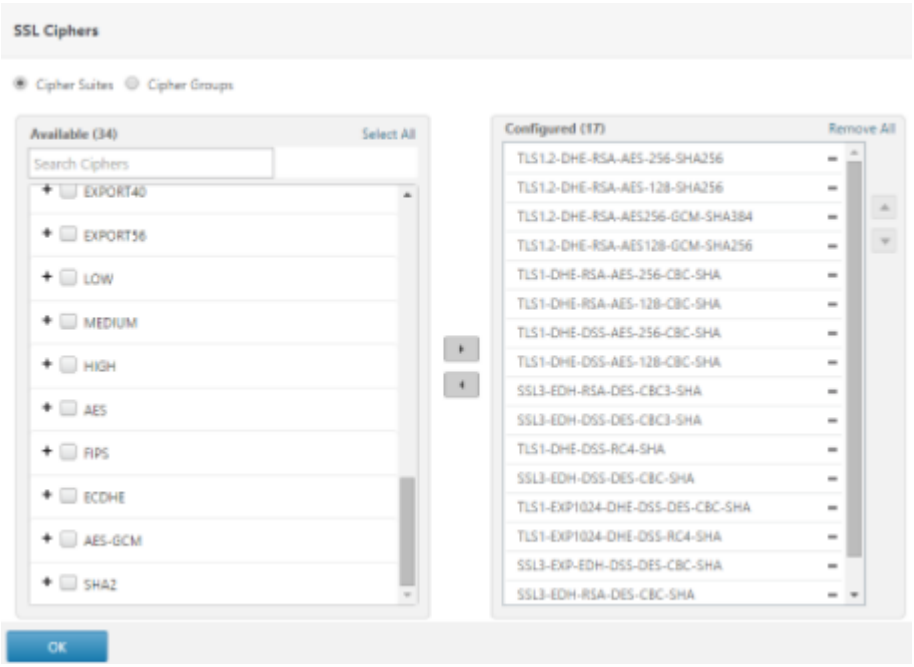
   a. Navigieren Sie zu **Konfiguration > Traffic Management > Virtuelle Server**.

   b. Wählen Sie den virtuellen Server aus, auf dem Sie DH aktivieren möchten, und klicken Sie auf das zu bearbeitende Bleistiftsymbol.

   c. Klicken Sie unter **Erweiterte Einstellungen**auf das Plus-Symbol neben **SSL-Chiffers**, wählen Sie die DHE-Chiffriergruppen aus und klicken Sie zum Binden auf **OK** .

   Hinweis: Stellen Sie sicher, dass die DHE-Chiffren ganz oben in der Chiffrierliste stehen, die an den virtuellen Server gebunden ist.





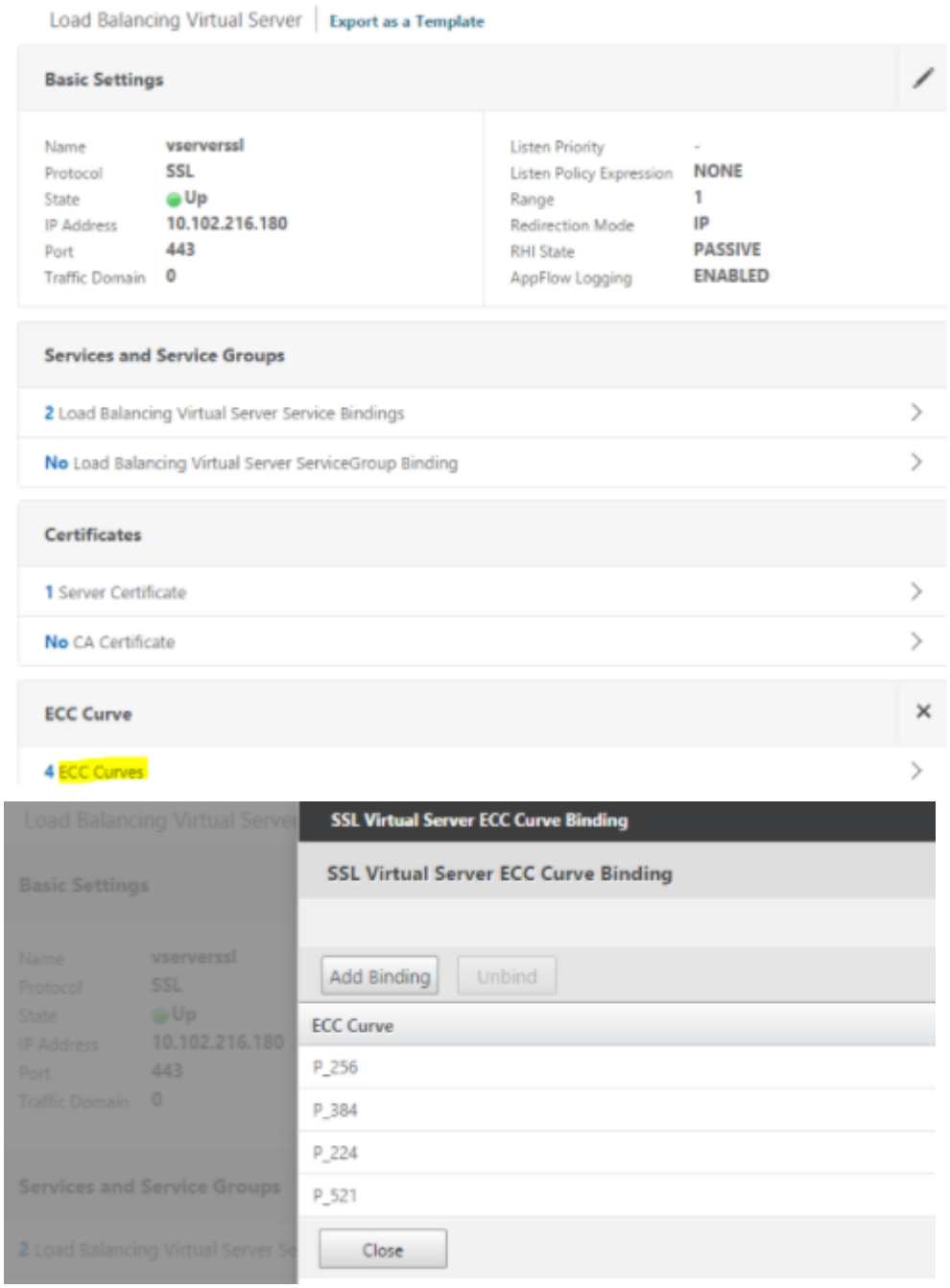
Konfigurieren Sie ECDHE mit der GUI

1. Binden Sie die ECC-Kurven an den virtuellen SSL-Server.

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

   b. Wählen Sie den virtuellen SSL-Server aus, den Sie bearbeiten möchten, klicken Sie auf **ECC-Kurve** und dann auf **Bindung hinzufügen**.

   c. Binden Sie die erforderliche ECC-Kurve an den virtuellen Server.

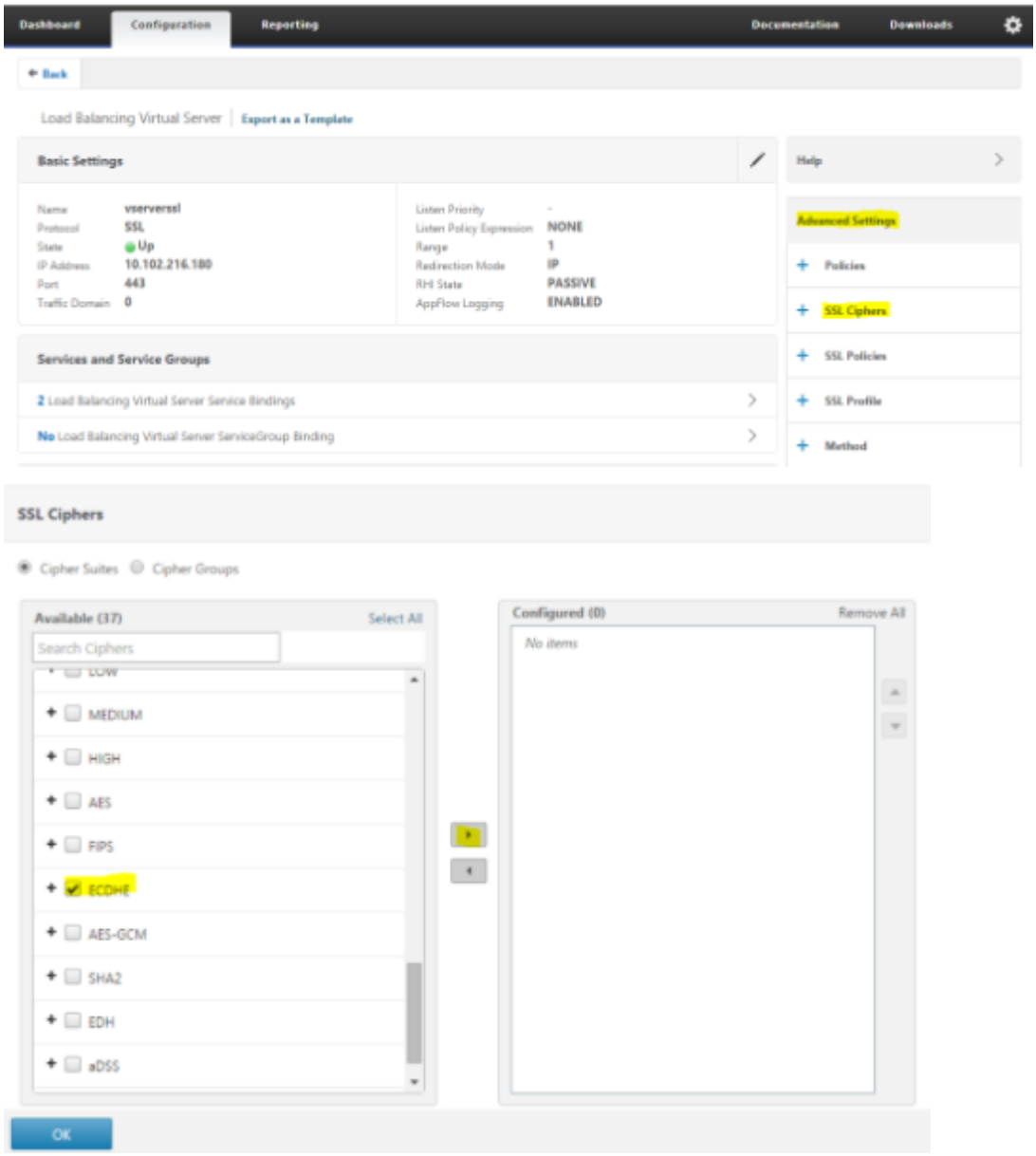


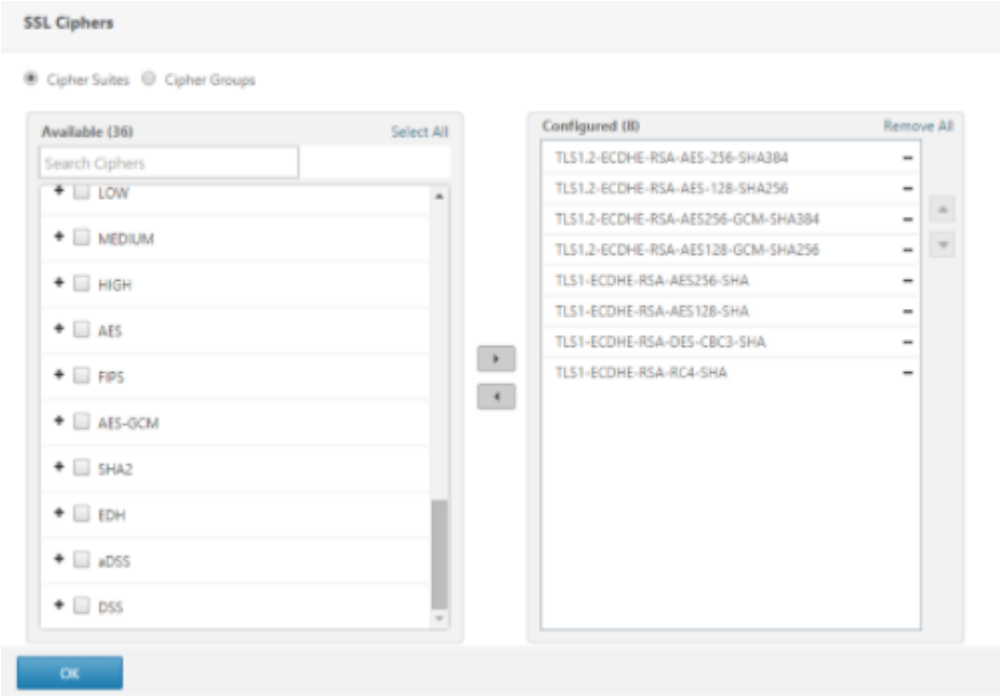
2. Binden Sie die ECDHE-Chiffern an den virtuellen Server.

   a. Navigieren Sie zu **Konfiguration > Traffic Management > Virtuelle Server** und wählen Sie den virtuellen Server aus, auf dem Sie DH aktivieren möchten.

   b. Klicken Sie auf **Edit > SSL Ciphers** und wählen Sie die ECDHE-Verschlüsselungsgruppen aus und klicken Sie auf **Binden**.

   Hinweis: Stellen Sie sicher, dass die ECDHE-Verschlüsselungen in der an den virtuellen Server gebundenen Verschlüsselungsliste ganz oben stehen.





Hinweis: Stellen Sie in jedem Fall sicher, dass die Citrix ADC-Appliance die Chiffern unterstützt, die Sie für die Kommunikation verwenden möchten.

Konfigurieren Sie PFS mit einem SSL-Profil

Hinweis: Die Option zur Konfiguration von PFS (Cipher oder ECC) mit einem SSL-Profil wird ab Version 11.0 64.x eingeführt. Ignorieren Sie den folgenden Abschnitt bei älteren Versionen.

Um PFS mit einem SSL-Profil zu aktivieren, muss eine ähnliche Konfiguration (wie in früheren Konfigurationsabschnitten beschrieben) durchgeführt werden, jedoch im SSL-Profil, anstatt direkt auf einem virtuellen Server zu konfigurieren.

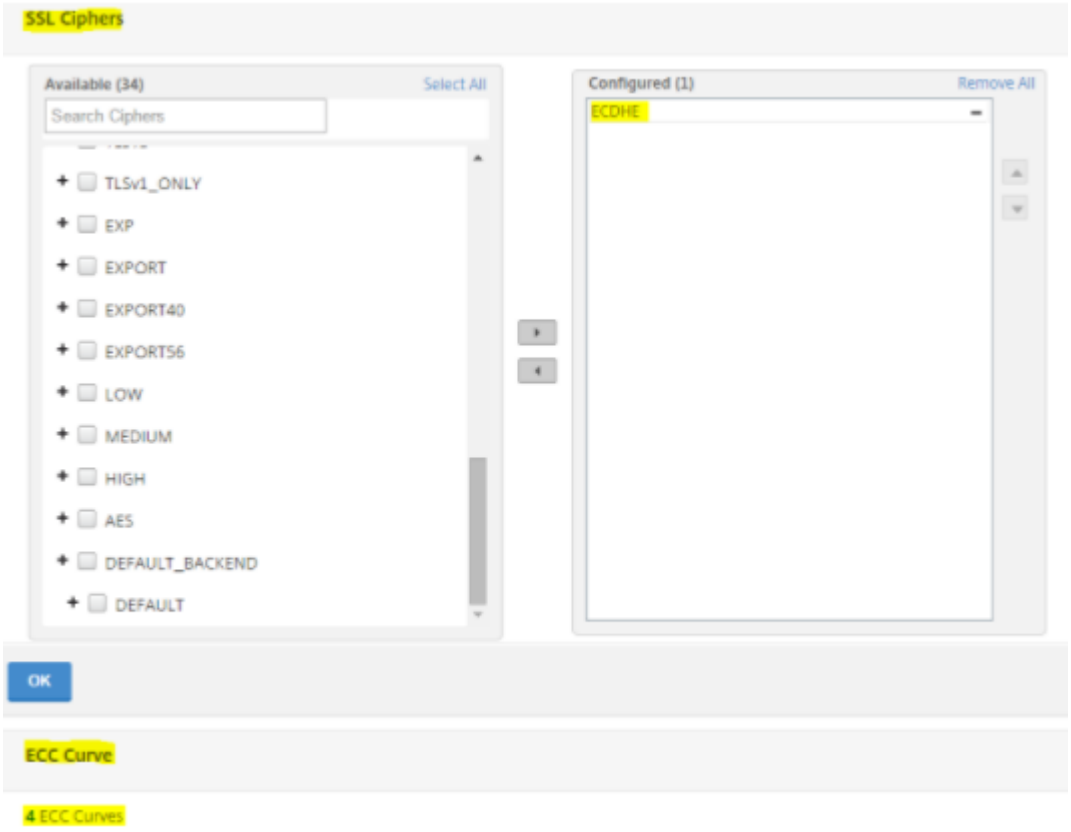
Konfigurieren Sie PFS mit einem SSL-Profil über die grafische Benutzeroberfläche

1. Binden Sie die ECC-Kurven und die ECDHE-Chiffre an das SSL-Profil.

   Hinweis: ECC-Kurven sind bereits standardmäßig an alle SSL-Profile gebunden.

   a. Navigieren Sie zu **System > Profile > SSL-Profile** und wählen Sie das Profil aus, für das Sie PFS aktivieren möchten.

   b. Binden Sie die ECDHE-Chiffern.



2. Binden Sie das SSL-Profil an den virtuellen Server.

   a. Gehen Sie zu **Konfiguration > Traffic Management > Virtuelle Server** und wählen Sie den virtuellen Server aus.

   b. Klicken Sie auf das Stiftsymbol, um das SSL-Profil zu bearbeiten.

   c. Klicken Sie auf **OK** und dann auf **Fertig**.

Konfigurieren Sie PFS mit SSL mit der CLI

Geben Sie in der Befehlszeile Folgendes ein:

1. Binden Sie ECC-Kurven an das SSL-Profil.


```
bind sslprofile <SSLProfileName> -eccCurveName <Name_of_curve>
<!--NeedCopy-->
```

2. Binden Sie die ECDHE-Chiffriergruppe.

```
bind sslprofile <SSLProfileName> cipherName <ciphergroupName>
<!--NeedCopy-->
```

3. Legen Sie die Priorität der ECDHE-Chiffre auf 1 fest.

```
set sslprofile <SSLProfileName> cipherName <ciphergroupName>
   cipherPriority <positive_integer>
<!--NeedCopy-->
```

4. Binden Sie das SSL-Profil an den virtuellen Server.

```
set SSL vserver <vservername> sslProfile <SSLProfileName>
<!--NeedCopy-->
```

ECDHE-Chiffre

October 5, 2021

Alle Citrix ADC Appliances unterstützen die ECDHE-Verschlüsselungsgruppe am Front-End und Back-End. Wenn auf einer SDX-Appliance ein SSL-Chip einer VPX-Instanz zugewiesen ist, gilt die Verschlüsselungsunterstützung einer MPX-Appliance. Andernfalls gilt die normale Verschlüsselung-sunterstützung einer VPX-Instanz.

Weitere Informationen zu den Builds und Plattformen, die diese Chiffren unterstützen, finden Sie unter Chiffren, die auf den Citrix ADC Appliances verfügbar sind.

ECDHE-Verschlüsselungssammlungen verwenden elliptische Kurvenkryptographie (ECC). Aufgrund seiner kleineren Schlüsselgröße ist ECC besonders nützlich in einer mobilen (drahtlosen) Umgebung oder einer interaktiven Sprachreaktionsumgebung, in der jede Millisekunde wichtig ist. Kleinere Schlüsselgrößen sparen Strom, Speicher, Bandbreite und Rechenkosten.

Eine Citrix ADC Appliance unterstützt die folgenden ECC-Kurven:

- P_256

- P_384
- P_224
- P_521

Hinweis: Wenn Sie ein Upgrade von einem Build vor Version 10.1 Build 121.10 durchführen, müssen Sie ECC-Kurven explizit an Ihre vorhandenen virtuellen SSL-Server und -Dienste binden. Die Kurven sind standardmäßig an alle virtuellen Server und Dienste gebunden, die Sie nach dem Upgrade erstellen.

Sie können eine ECC-Kurve an SSL-Frontend- und Back-End-Entitäten binden. Standardmäßig sind alle vier Kurven in der folgenden Reihenfolge gebunden: P_256, P_384, P_224, P_521. Um die Reihenfolge zu ändern, müssen Sie zuerst alle Kurven aufheben und sie dann in der gewünschten Reihenfolge binden.

Binden von ECC-Kurven an einen virtuellen SSL-Server über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind ssl vserver <vServerName > -eccCurveName <eccCurveName >
```

Beispiel:

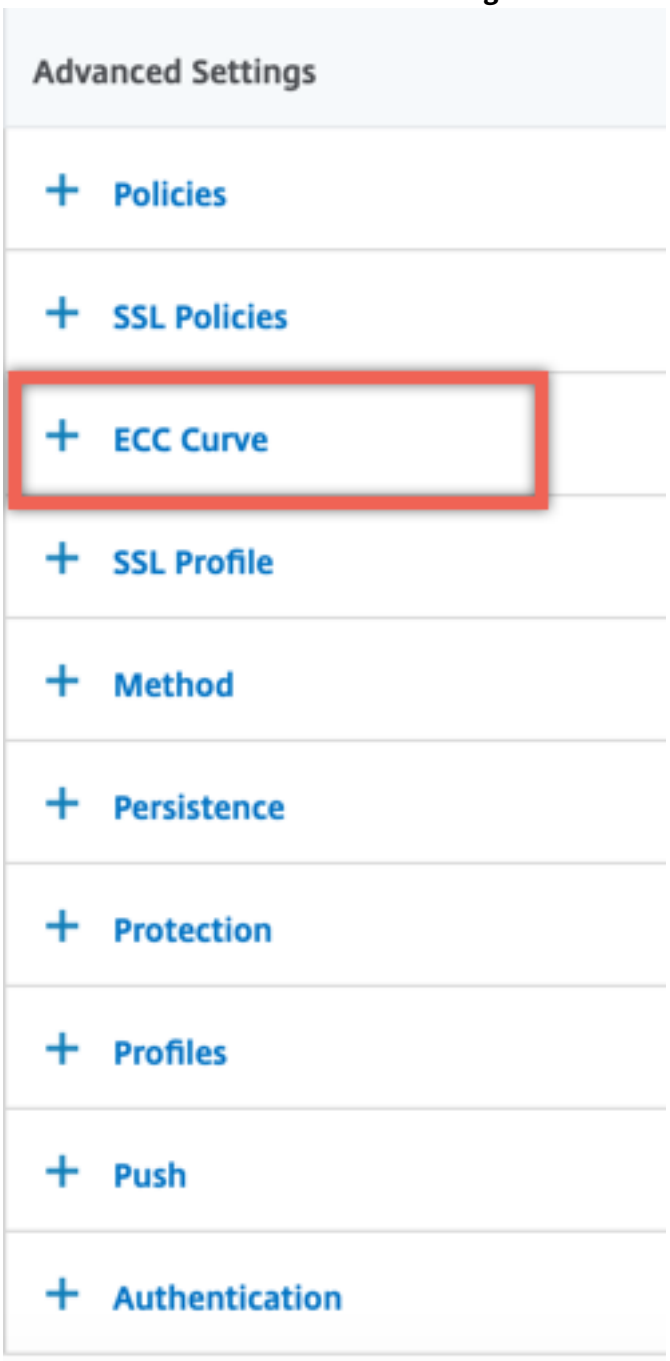
```
1  bind ssl vserver  v1 -eccCurveName P_224
2
3  sh ssl vserver v1
4
5  Advanced SSL configuration for VServer v1:
6  DH: DISABLED
7  Ephemeral RSA: ENABLED Refresh Count: 0
8  Session Reuse: ENABLED Timeout: 120 seconds
9  Cipher Redirect: DISABLED
10 SSLv2 Redirect: DISABLED
11 ClearText Port: 0
12 Client Auth: DISABLED
13 SSL Redirect: DISABLED
14 Non FIPS Ciphers: DISABLED
15 SNI: DISABLED
16 SSLv2: DISABLED SSLv3: ENABLED TLSv1.0: ENABLED  TLSv1.1: DISABLED
      TLSv1.2: DISABLED
17 Push Encryption Trigger: Always
18 Send Close-Notify: YES
19 ECC Curve: P_224
20
21 1) Cipher Name: DEFAULT
22 Description: Predefined Cipher Alias
```



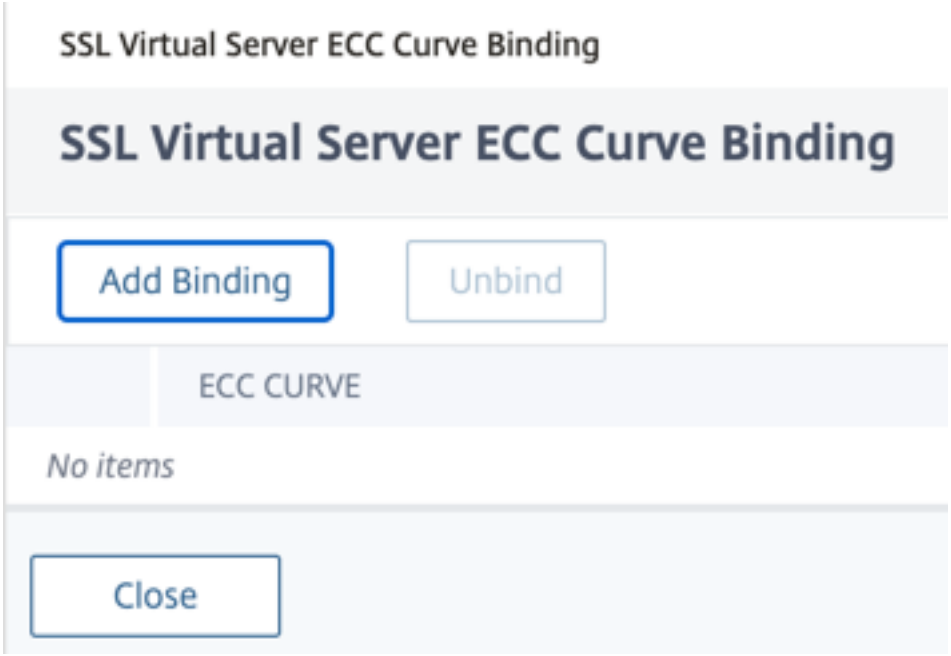
```
23 Done
24 <!--NeedCopy-->
```

Binden von ECC-Kurven an einen virtuellen SSL-Server mit der GUI

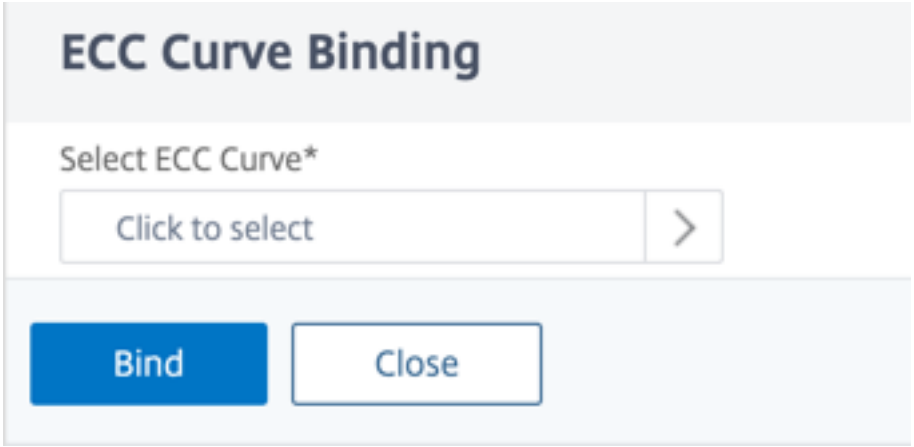
1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie einen virtuellen SSL-Server aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie unter **Erweiterte Einstellungen** auf **ECC-Kurve**.



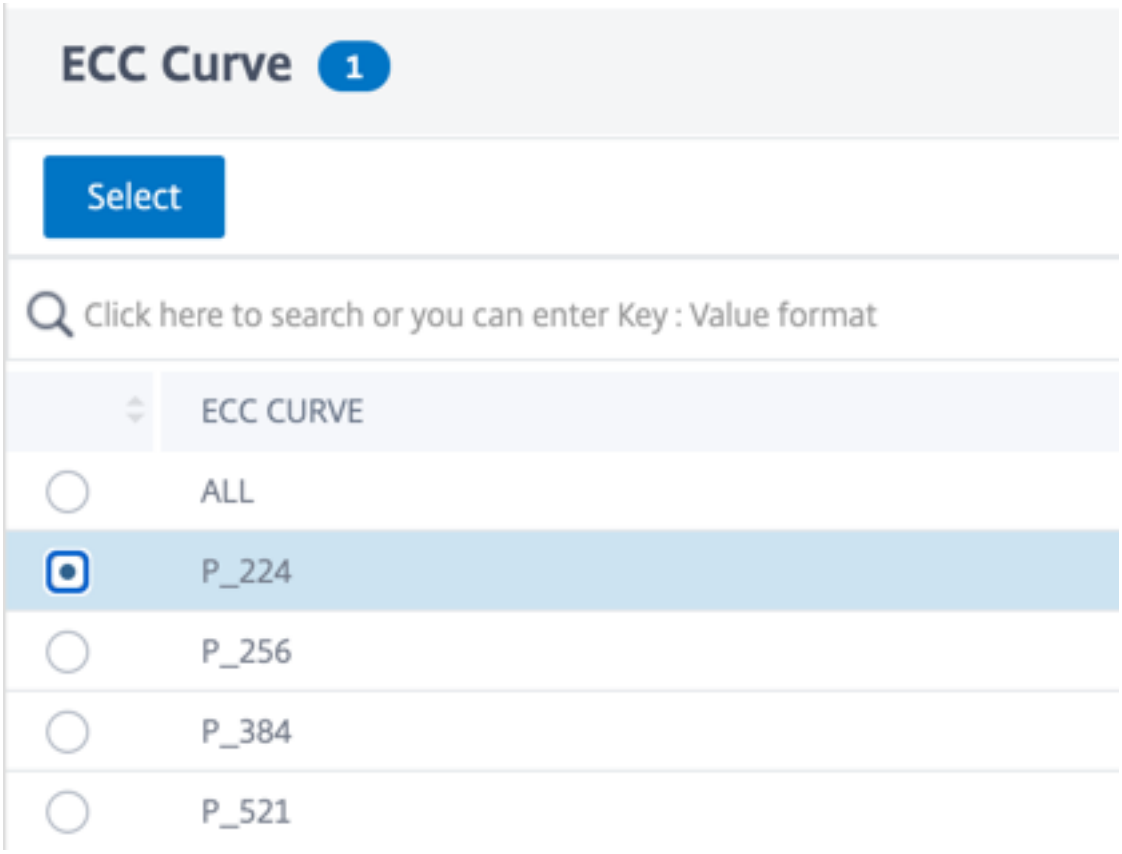
4. Klicken Sie in den ECC-Kurvenabschnitt.
5. Klicken Sie auf der Seite **SSL Virtual Server ECC Curve Binding** auf **Binding hinzufügen**.



6. Klicken Sie in **ECC-Kurvenbindung** auf **ECC-Kurve auswählen**.



7. Wählen Sie einen Wert aus, und klicken Sie dann auf **Auswählen**.



8. Klicken Sie auf **Bind**.
9. Klicken Sie auf **Schließen**.
10. Klicken Sie auf **Fertig**.

Binden von ECC-Kurven an einen SSL-Dienst über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind ssl service <vServerName > -eccCurveName <eccCurveName >
```

Beispiel:

```
1 > bind ssl service sslsvc -eccCurveName P_224
2  Done
3 > sh ssl service sslsvc
4
5     Advanced SSL configuration for Back-end SSL Service sslsvc:
6     DH: DISABLED
7     DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
          DISABLED
8     Session Reuse: ENABLED      Timeout: 300 seconds
```



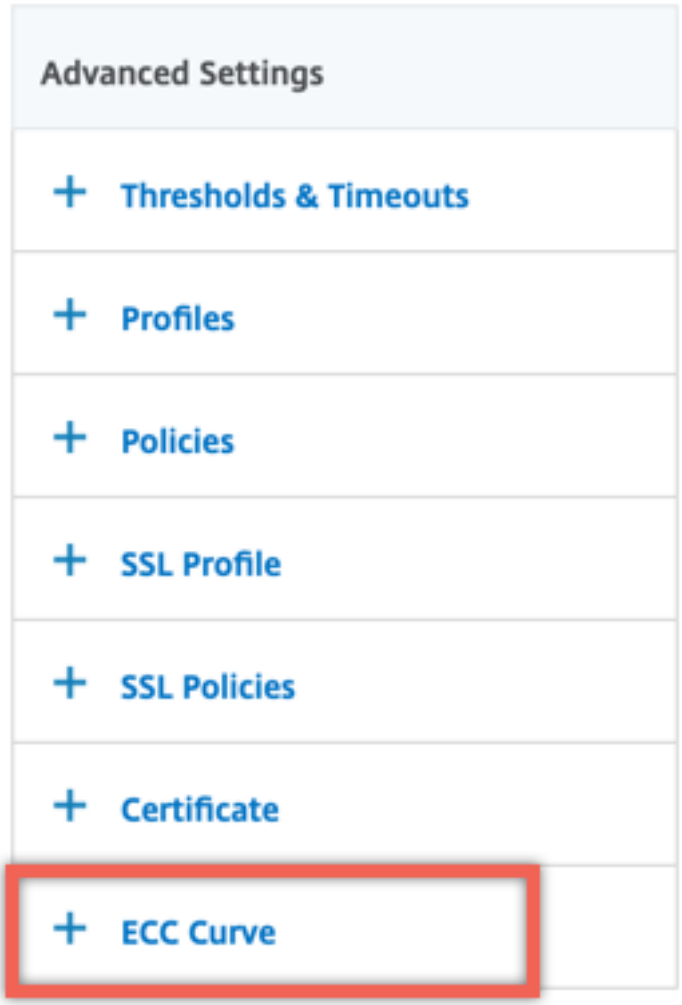
```
    Cipher Redirect: DISABLED
    ClearText Port: 0
    Server Auth: DISABLED
    SSL Redirect: DISABLED
    Non FIPS Ciphers: DISABLED
    SNI: DISABLED
    OCSP Stapling: DISABLED
    SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: ???
    DHE Key Exchange With PSK: ???
    Tickets Per Authentication Context: ???

    ECC Curve: P_224

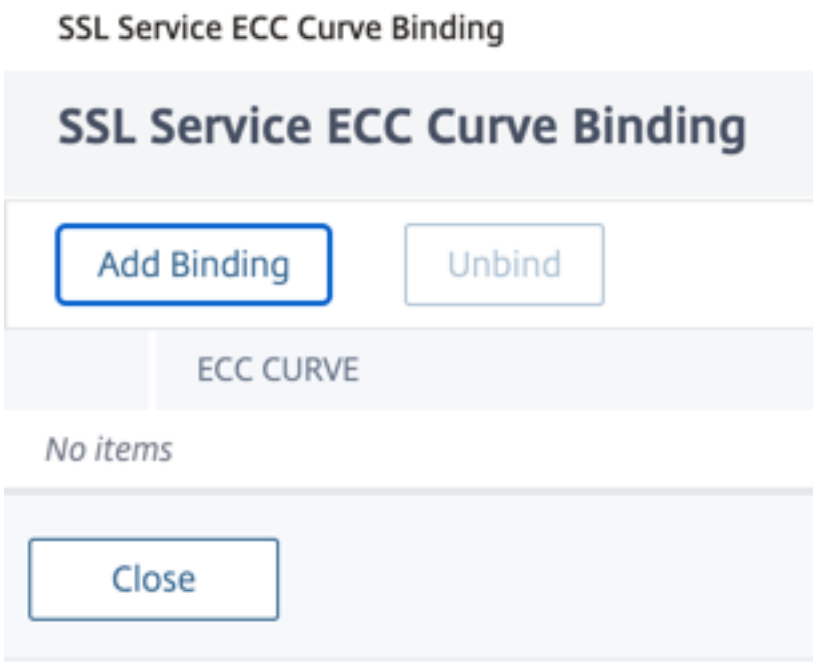

1)  Cipher Name: DEFAULT_BACKEND
    Description: Default cipher list for Backend SSL session
 Done
<!--NeedCopy-->
```

Binden von ECC-Kurven an einen SSL-Service mit der GUI

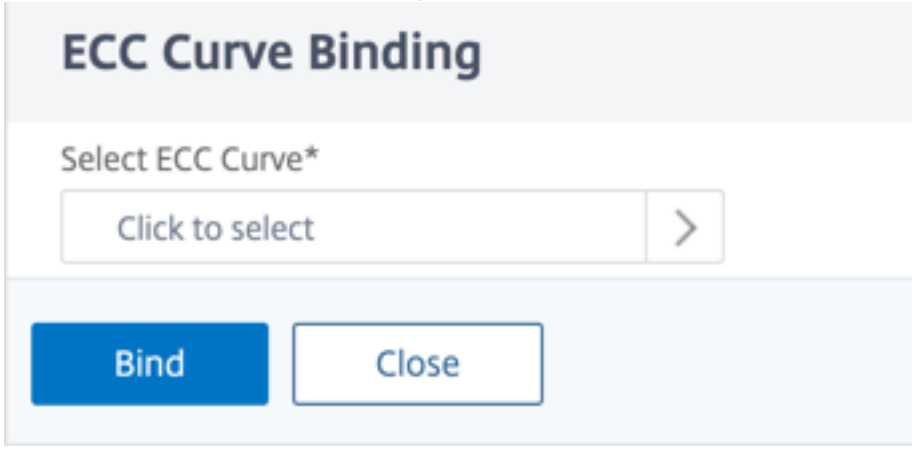
1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Wählen Sie einen SSL-Dienst aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie unter **Erweiterte Einstellungen** auf **ECC-Kurve**.



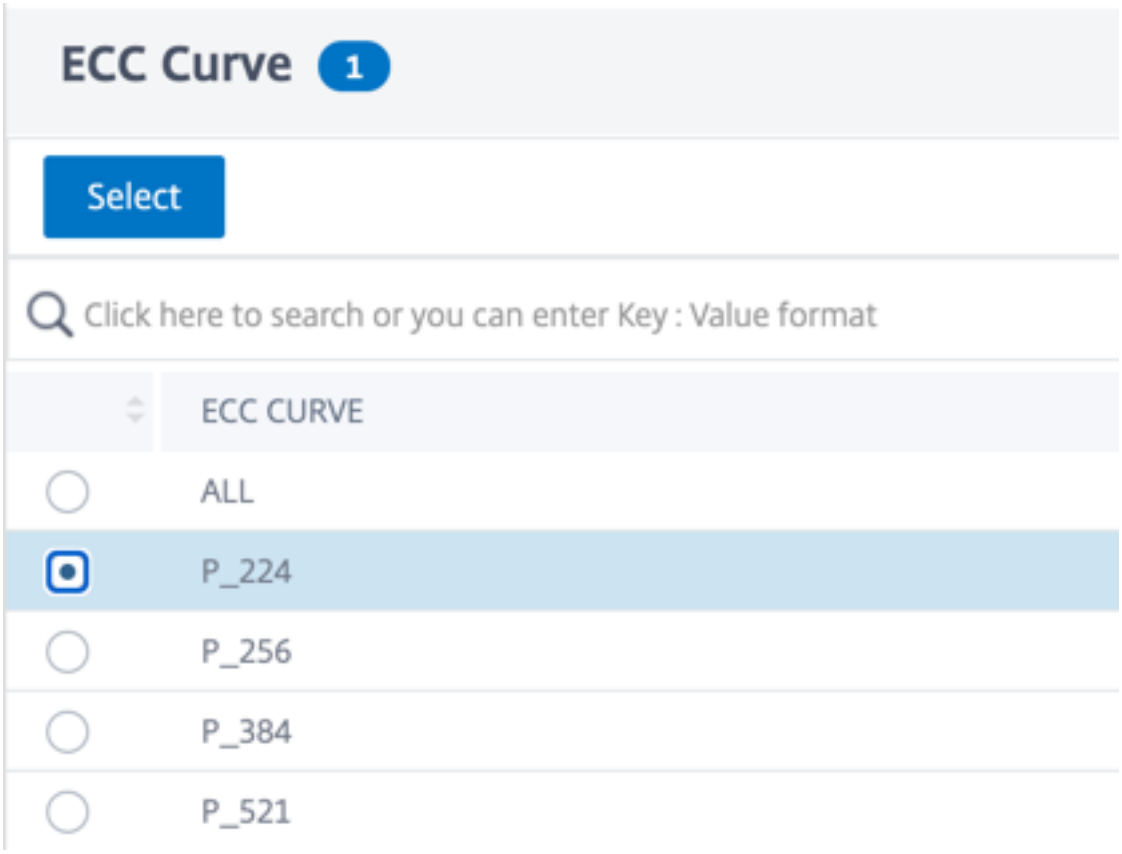
4. Klicken Sie in den ECC-Kurvenabschnitt.
5. Klicken Sie auf der Seite **SSL Service ECC Curve Binding** auf **Add Binding**.



6. Klicken Sie in **ECC-Kurvenbindung** auf **ECC-Kurve auswählen**.



7. Wählen Sie einen Wert aus, und klicken Sie dann auf **Auswählen**.



8. Klicken Sie auf **Bind**.
9. Klicken Sie auf **Schließen**.
10. Klicken Sie auf **Fertig**.

Diffie-Hellman-Parametergenerierung und Erreichen von PFS mit DHE

October 5, 2021

Der Diffie-Hellman (DH) Schlüsselaustausch ist eine Möglichkeit für zwei Parteien, die an einer SSL-Transaktion beteiligt sind, um ein gemeinsames Geheimnis über einen unsicheren Kanal zu vereinbaren. Diese Parteien haben keine Vorkenntnisse voneinander. Dieses Geheimnis kann in kryptografisches Schlüsselmaterial für symmetrische Schlüsselverschlüsselungsalgorithmen umgewandelt werden, die einen solchen Schlüsselaustausch erfordern.

Diese Funktion ist in der Standardeinstellung deaktiviert. Die Funktion wurde so konfiguriert, dass Verschlüsselungen unterstützt werden, die DH als Schlüsselaustauschalgorithmus verwenden.

> **Hinweis**:
>
> Das Generieren von 2048-Bit-DH-Parametern kann sehr lange dauern (bis zu 30 Minuten).

Generieren von DH-Parametern mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

```
create ssl dhparam <dhFile> [<bits>] [-gen (2 | 5)]
<!--NeedCopy-->
```

Beispiel:

```
create ssl dhparam Key-DH-1 512 -gen 2
<!--NeedCopy-->
```

Generieren von DH-Parametern mit der GUI

Navigieren Sie zu **Traffic Management** > **SSL**, und wählen Sie in der Gruppe **Extras** die Option **Diffie-Hellman (DH) Schlüssel erstellen** und **SSL DH Param konfigurieren** aus.

> **Hinweis:**
>
> Informationen zu DH-Parametern finden Sie unter Diffie-Hellman-Parametern.

Perfektes Vorwärtsgeheimnis mit DHE

Die Erzeugung von DH-Parametern ist ein CPU-intensiver Betrieb. In früheren Versionen hat die Parametergenerierung auf einer VPX-Appliance lange gedauert, da sie in der Software durchgeführt wurde. Die Parametergenerierung wird durch die Einstellung des`dhKeyExpSizeLimit` Parameters optimiert. Sie können diesen Parameter für einen virtuellen SSL-Server oder ein SSL-Profil festlegen und dann das Profil an einen virtuellen Server binden.

Sie können Perfect Forward Secrecy (PFS) auf Citrix ADC MPX-Appliances beibehalten, indem Sie die DH-Anzahl auf Null setzen. Daher werden DH-Parameter für jede Transaktion (Minimum`DHcount` ist 0) auf Citrix ADC MPX-Appliances generiert. Die Parameter werden ohne einen signifikanten Leistungsabfall generiert, da die Operation optimiert ist. Früher war die minimale DH-Zählung zulässig 500. Das heißt, Sie können den Schlüssel für bis zu 500 Transaktionen nicht regenerieren.

Auf einer Citrix ADC VPX Appliance können Sie DH-Parameter für jede 500-Transaktion mindestens (`DHcount` = 500) generieren. Wenn Sie 0`DHcount` setzen, werden die DH-Parameter nicht regeneriert.

> **Einschränkung:**
>
> Sie können PFS in VPX heute nicht mit DH-Chiffern erreichen.

Optimierung der DH-Parametergenerierung mit der CLI

Geben Sie an der Eingabeaufforderung die Befehle 1 und 2 ein, oder geben Sie Befehl 3 ein:

```
1. add ssl profile <name> [-sslProfileType ( BackEnd | FrontEnd )] [-dhCount <positive_integer>] [-dh ( ENABLED | DISABLED) -dhFile <string>] [-dhKeyExpSizeLimit ( ENABLED | DISABLED)]
2. set ssl vserver <vServerName> [-sslProfile <string>]
<!--NeedCopy-->
```

```
3. set ssl vserver <vServerName> [-dh ( ENABLED | DISABLED) -dhFile <string>] [-dhCount <positive_integer>] [-dhKeyExpSizeLimit ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

Optimieren Sie die Generierung von DH-Parametern mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie im Abschnitt **SSL-Parameter** die Option **Enable DH Key Expire Size Limit** aus.

Chiffreumleitung

October 5, 2021

Während des SSL-Handshakes kündigt der SSL-Client (normalerweise ein Webbrowser) die von ihm unterstützte Verschlüsselungssuite in der konfigurierten Reihenfolge an. Aus dieser Liste wählt der SSL-Server dann eine Chiffre aus, die mit seiner eigenen Liste konfigurierter Chiffren übereinstimmt.

Wenn die vom Client angekündigten Chiffre nicht mit den auf dem SSL-Server konfigurierten Chiffrieren übereinstimmen, schlägt der SSL-Handshake fehl. Der Fehler wird durch eine im Browser angezeigte kryptische Fehlermeldung angekündigt. Diese Meldungen erwähnen selten die genaue Ursache des Fehlers.

Mit der Chiffreumleitung können Sie einen virtuellen SSL-Server konfigurieren, um genaue, aussagekräftige Fehlermeldungen zu liefern, wenn ein SSL-Handshake ausfällt. Wenn ein SSL-Handshake fehlschlägt, leitet die ADC-Appliance den Benutzer auf eine zuvor konfigurierte URL um oder zeigt, wenn keine URL konfiguriert ist, eine intern generierte Fehlerseite an.

Konfigurieren der Chiffreumleitung mit der CLI

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

```
- set ssl vserver <vServerName> -cipherRedirect < ENABLED | DISABLED>
   -cipherURL < URL>
- show ssl vserver <vServerName>
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver vs-ssl -cipherRedirect ENABLED -cipherURL http://
   redirectURl

Done

show ssl vserver vs-ssl

Advanced SSL configuration for VServer vs-ssl:
DH: DISABLED
Ephemeral RSA: ENABLED          Refresh Count: 1000
Session Reuse: ENABLED          Timeout: 600 seconds
Cipher Redirect: ENABLED        Redirect URL: http://redirectURl
SSLv2 Redirect: DISABLED
ClearText Port: 0
Client Auth: DISABLED
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: DISABLED
OCSP Stapling: DISABLED
HSTS: DISABLED
HSTS IncludeSubDomains: NO
HSTS Max-Age: 0
SSLv2: DISABLED SSLv3: ENABLED  TLSv1.0: ENABLED TLSv1.2: ENABLED
   TLSv1.2: ENABLED
    1)      CertKey Name: Auth-Cert-1       Server Certificate
    1)      Cipher Name: DEFAULT
            Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```


Konfigurieren der Chiffreumleitung mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie im Abschnitt **SSL-Parameter** die Option **Chiffrier-Umleitung aktivieren** aus, und geben Sie eine Umleitungs-URL an.

Verwenden Sie Hardware und Software zur Verbesserung der ECDHE- und ECDSA-Verschlüsselungsleistung

October 5, 2021

> **Hinweis:**
>
> Diese Erweiterung gilt nur für die folgenden Plattformen:
>
> - MPX/SDX 11000
> - MPX/SDX 14000
> - MPX 22000, MPX 24000 und MPX 25000
> - MPX/SDX 14000 FIPS

Früher wurde die ECDHE und ECDSA-Berechnung auf einer Citrix ADC Appliance nur auf der Hardware (Cavium-Chips) durchgeführt, wodurch die Anzahl der SSL-Sitzungen zu einem bestimmten Zeitpunkt begrenzt wurde. Mit dieser Erweiterung werden auch einige Operationen in der Software durchgeführt. Das heißt, die Verarbeitung erfolgt sowohl auf den Cavium-Chips als auch auf den CPU-Kernen, um die ECDHE und ECDSA-Verschlüsselungsleistung zu verbessern.

Die Verarbeitung erfolgt zunächst in Software, bis zum konfigurierten Software-Kryptoschwellenwert. Nachdem dieser Schwellenwert erreicht ist, werden die Vorgänge auf die Hardware ausgelagert. Daher verwendet dieses Hybridmodell sowohl Hardware als auch Software, um die SSL-Leistung zu verbessern. Sie können das Hybridmodell aktivieren, indem Sie den Parameter “SoftwareCryptoThreshold” entsprechend Ihren Anforderungen festlegen. Um das Hybridmodell zu deaktivieren, setzen Sie diesen Parameter auf 0.

Die Vorteile sind am größten, wenn die aktuelle CPU-Auslastung nicht zu hoch ist, da der CPU-Schwellenwert nicht exklusiv für ECDHE und ECDSA-Berechnung ist. Wenn beispielsweise die aktuelle Arbeitslast auf der Appliance 50% der CPU-Zyklen verbraucht und der Schwellenwert auf 80% festgelegt ist, können ECDHE- und ECDSA-Berechnungen nur 30% verwenden. Nachdem der konfigurierte Software-Kryptoschwellenwert von 80% erreicht wurde, wird die weitere ECDHE und ECDSA-Berechnung auf die Hardware abgeladen. In diesem Fall kann die tatsächliche CPU-Auslastung 80% überschreiten, da die Durchführung von ECDHE und ECDSA-Berechnungen in der Hardware einige CPU-Zyklen verbraucht.

Aktivieren des Hybridmodells mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl parameter -softwareCryptoThreshold <positive_integer>

Synopsis:

softwareCryptoThreshold:

Citrix ADC CPU utilization threshold (as a percentage) beyond which
   crypto operations are not done in software. A value of zero implies
   that CPU is not utilized for doing crypto in software.

Default = 0

Min = 0

Max = 100
<!--NeedCopy-->
```

Beispiel:

```
set ssl parameter - softwareCryptoThreshold 80
Done

show ssl parameter
Advanced SSL Parameters

SSL quantum size                  : 8 KB
Max CRL memory size               : 256 MB
Strict CA checks                  : NO
Encryption trigger timeout        : 100 ms
Send Close-Notify                 : YES
Encryption trigger packet c       : 45
Deny SSL Renegotiation            : ALL
Subject/Issuer Name Insertion Format : Unicode
OCSP cache size                   : 10 MB
Push flag                         : 0x0 (Auto)
Strict Host Header check for SNI enabled SSL sessions : NO
PUSH encryption trigger timeout   : 1 ms
Crypto Device Disable Limit       : 0
Global undef action for control policies : CLIENTAUTH
```



```
Global undef action for data policies : NOOP
Default profile                   : DISABLED
Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors    : NO
Disable TLS 1.1/1.2 for dynamic and VPN services : NO
Software Crypto acceleration CPU Threshold : 80
Signature and Hash Algorithms supported by TLS1.2 : ALL
<!--NeedCopy-->
```

Aktivieren Sie das Hybridmodell mit der GUI

1. Navigieren Sie zu **Traffic Management** > **SSL** > **Erweiterte SSL-Einstellungen ändern**.
2. Geben Sie einen Wert für **Software-Krypto-Schwellenwert (%)**ein.

Legen Sie einen SNMP-Alarm für den ECDHE-Wechselkurs fest

Der ECDHE-basierte Schlüsselaustausch kann dazu führen, dass die Transaktionen pro Sekunde auf der Appliance sinken. Ab Release 13.0 Build 52.x können Sie einen SNMP-Alarm für ECDHE-basierte Transaktionen konfigurieren. In diesem Alarm können Sie den Schwellenwert und die normalen Grenzwerte für den ECDHE-Wechselkurs festlegen. Ein neuer Zähler `nsssl_tot_sslInfo_ECDHE_Tx` wird hinzugefügt. Dieser Leistungsindikator ist die Summe aller ECDHE-basierten Transaktionszähler im Front-End und Back-End der Appliance. Wenn der ECDHE-basierte Schlüsselaustausch die konfigurierten Grenzen überschreitet, wird ein SNMP-Trap gesendet. Eine weitere Trap-Funktion wird gesendet, wenn der Wert auf den konfigurierten Normalwert zurückgesetzt wird.

Einstellen eines SNMP-Alarms für den ECDHE-Wechselkurs über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set snmp alarm ECDHE-EXCHANGE-RATE -logging ( ENABLED | DISABLED ) -
    severity <severity>
 -state ( ENABLED | DISABLED ) -thresholdValue <positive_integer>  [-
     normalValue <positive_integer>] -time <secs>
<!--NeedCopy-->
```

Beispiel:

```
set snmp alarm ECDHE-EXCHANGE-RATE -logging eNABLED -severity critical
    -state eNABLED -thresholdValue 100 -normalValue 50
<!--NeedCopy-->
```


Unterstützung von ECDSA-Verschlüsselungssammlungen

October 5, 2021

ECDSA-Verschlüsselungssammlungen verwenden elliptische Kurvenkryptographie (ECC). Aufgrund seiner kleineren Größe ist es in Umgebungen hilfreich, in denen Verarbeitungsleistung, Speicherplatz, Bandbreite und Stromverbrauch eingeschränkt sind.

Wenn die ECDHE_ECDSA-Verschlüsselungsgruppe verwendet wird, muss das Zertifikat des Servers einen ECDSA-fähigen öffentlichen Schlüssel enthalten.

In der folgenden Tabelle sind die ECDSA-Verschlüsselungen aufgeführt, die von Citrix ADC MPX- und SDX-Appliances mit N3-Chips, Citrix ADC VPX Appliances, MPX 5900/26000 und MPX/SDX 8900/15000 unterstützt werden.

Chiffre Name	Priorität	Beschreibung	Schlüsselaustauschalgorithmus	Authentifizierungsalgorithmus	Verschlüsselungsalgorithmus (Schlüsselgröße)	MAC-Algorithmus (Message Authentication Code)	Hexcode
TLS1-ECDHE-ECDSA-AES128-SHA	1	SSLv3	ECC-DHE	ECDSA	AES(128)	SHA1	0xc009
TLS1-ECDHE-ECDSA-AES256-SHA	2	SSLv3	ECC-DHE	ECDSA	AES(256)	SHA1	0xc00a
TLS1.2-ECDHE-ECDSA-AES128-SHA256	3	TLSv1.2	ECC-DHE	ECDSA	AES(128)	SHA-256	0xc023

Chiffre Name	Priorität	Beschreibung	Schlüsselaustauschalgorithmus	Authentifizierungsalgorithmus	Verschlüsselungsalgorithmus (Schlüsselgröße)	MAC-Algorithmus (Message Authentication Code)	Hexcode
TLS1.2-ECDHE-ECDSA-AES256-SHA384	4	TLSv1.2	ECC-DHE	ECDSA	AES(256)	SHA-384	0xc024
TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256	5	TLSv1.2	ECC-DHE	ECDSA	AES-GCM(128)	SHA-256	0xc02b
TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384	6	TLSv1.2	ECC-DHE	ECDSA	AES-GCM(256)	SHA-384	0xc02c
TLS1-ECDHE-ECDSA-RC4-SHA	7	SSLv3	ECC-DHE	ECDSA	RC4(128)	SHA1	0xc007
TLS1-ECDHE-ECDSA-DES-CBC3-SHA	8	SSLv3	ECC-DHE	ECDSA	3DES(168)	SHA1	0xc008

Chiffre Name	Priorität	Beschreibung	Schlüsselaustausch-Algorithmus	Authentifizierungsalgorithmus	Verschlüsselungsalgorithmus (Schlüssellänge)	MAC-Algorithmus (Message Authentication Code)	Hexcode
TLS1.2-ECDHE-ECDSA-CHACHA20-POLY1305	9	TLSv1.2	ECC-DHE	ECDSA	CHACHA20/	AEAD	0xcca9

ECDSA/RSA-Verschlüsselung und Zertifikatauswahl

Sie können ECDSA- und RSA-Serverzertifikate gleichzeitig an einen virtuellen SSL-Server binden. Wenn ECDSA- und RSA-Zertifikate an den virtuellen Server gebunden sind, wird automatisch das entsprechende Serverzertifikat ausgewählt, das dem Client vorgelegt werden soll. Wenn die Client-Verschlüsselungsliste RSA-Chiffre enthält, aber keine ECDSA-Chiffre enthält, stellt der virtuelle Server das RSA-Serverzertifikat vor. Wenn beide Verschlüsselungen in der Clientliste vorhanden sind, hängt das dargestellte Serverzertifikat von der auf dem virtuellen Server festgelegten Verschlüsselungspriorität ab. Das heißt, wenn RSA eine höhere Priorität hat, wird das RSA-Zertifikat präsentiert. Wenn ECDSA eine höhere Priorität hat, wird das ECDSA-Zertifikat dem Client vorgelegt.

Clientauthentifizierung mithilfe eines ECDSA- oder RSA-Zertifikats

Für die Clientauthentifizierung kann das an den virtuellen Server gebundene Zertifizierungsstellenzertifikat ECDSA- oder RSA-signiert sein. Die Appliance unterstützt eine gemischte Zertifikatkette. Beispielsweise wird die folgende Zertifikatkette unterstützt.

Client-Zertifikat (ECDSA) <-> CA-Zertifikat (RSA) <-> Zwischenzertifikat (RSA) <-> Stammzertifikat (RSA)

Die folgende Tabelle zeigt die elliptischen Kurven, die auf den verschiedenen Citrix ADC Appliances mit ECDSA-Chiffriergruppen und ECDSA-Zertifikaten unterstützt werden:

Elliptische Kurven	Unterstützte Plattformen
prime256v1	Alle Plattformen, einschließlich FIPS.
secp384r1	Alle Plattformen, einschließlich FIPS.
secp521r1	MPX 5900, MPX/SDX 8900, MPX/SDX 15000, MPX/SDX 26000, VPX

Elliptische Kurven	Unterstützte Plattformen
secp224r1	MPX 5900, MPX/SDX 8900. MPX/SDX 15000, MPX/SDX 26000, VPX

Erstellen eines ECDSA-Zertifikatschlüsselpaars

Sie können ein ECDSA-Zertifikatschlüsselpaar direkt auf einer Citrix ADC Appliance mit der CLI oder der GUI erstellen. Zuvor konnten Sie ein ECC-Zertifikatschlüsselpaar auf der Appliance installieren und binden, aber Sie mussten OpenSSL verwenden, um ein Zertifikatschlüsselpaar zu erstellen.

Es werden nur P_256 und P_384 Kurven unterstützt.

> **Hinweis:**
>
> Diese Unterstützung ist auf allen Plattformen außer MPX 9700/1050/12500/15500 verfügbar.

So erstellen Sie ein ECDSA-Zertifikatschlüsselpaar mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
create ssl ecdsaKey <keyFile> -curve ( P_256 | P_384 ) [-keyform ( DER | PEM )] [-des | -des3] {
 -password  }
  [-pkcs8]
<!--NeedCopy-->
```

Beispiel:

```
create ecdsaKey ec_p256.ky -curve P_256 -pkcs8
Done
create ecdsaKey ec_p384.ky -curve P_384
Done
<!--NeedCopy-->
```

So erstellen Sie ein ECDSA-Zertifikatschlüsselpaar mit der GUI:

1. Navigieren Sie zu **Traffic Management > SSL > SSL-Dateien > Schlüssel** und klicken Sie auf **ECDSA-Schlüssel erstellen**.
2. Um einen Schlüssel im PKCS #8 Format zu erstellen, wählen Sie **PKCS8**aus.

Konfigurieren von benutzerdefinierten Verschlüsselungsgruppen auf der ADC-Appliance

December 7, 2021

Eine Verschlüsselungsgruppe ist eine Gruppe von Verschlüsselungssammlungen, die Sie an einen virtuellen SSL-Server, einen virtuellen Dienst oder eine Dienstgruppe auf der Citrix ADC Appliance binden. Eine Verschlüsselungssuite besteht aus einem Protokoll, einem Schlüsselaustauschalgorithmus (Kx), einem Authentifizierungsalgorithmus (Au), einem Verschlüsselungsalgorithmus (Enc) und einem Nachrichtenauthentifizierungscode (Mac) -Algorithmus. Ihre Appliance wird mit einem vordefinierten Satz von Chiffriergruppen ausgeliefert. Wenn Sie einen SSL-Dienst oder eine SSL-Dienstgruppe erstellen, wird die ALL-Verschlüsselungsgruppe automatisch an sie gebunden. Wenn Sie jedoch einen virtuellen SSL-Server oder einen transparenten SSL-Dienst erstellen, wird die DEFAULT-Verschlüsselungsgruppe automatisch an ihn gebunden. Darüber hinaus können Sie eine benutzerdefinierte Verschlüsselungsgruppe erstellen und sie an einen virtuellen SSL-Server, einen Dienst oder eine Dienstgruppe binden.

Hinweis: Wenn Ihre MPX-Appliance über keine Lizenzen verfügt, ist nur die EXPORT-Verschlüsselung an Ihren virtuellen SSL-Server, -Dienst oder -Dienstgruppe gebunden.

Um eine benutzerdefinierte Chiffregruppe zu erstellen, erstellen Sie zuerst eine Chiffregruppe und binden dann Chiffre- oder Chiffregruppen an diese Gruppe. Wenn Sie einen Chiffrealias oder eine Chiffregruppe angeben, werden alle Chiffrealias oder -gruppe zur benutzerdefinierten Chiffregruppe hinzugefügt. Sie können auch einzelne Chiffre (Chiffre Suites) zu einer benutzerdefinierten Gruppe hinzufügen. Eine vordefinierte Verschlüsselungsgruppe kann jedoch nicht geändert werden. Bevor Sie eine Verschlüsselungsgruppe entfernen, heben Sie die Bindung aller Verschlüsselungssammlungen in der Gruppe auf.

Wenn Sie eine Verschlüsselungsgruppe an einen virtuellen SSL-Server, einen Dienst oder eine Dienstgruppe binden, werden die Chiffre an die vorhandenen Verschlüsselungen angehängt, die an die Entität gebunden sind. Um eine bestimmte Chiffregruppe an die Entität zu binden, müssen Sie zunächst die an die Entität gebundenen Chiffre- oder Chiffregruppe aufheben. Binden Sie dann die bestimmte Verschlüsselungsgruppe an die Entität. Um beispielsweise nur die AES-Verschlüsselungsgruppe an einen SSL-Dienst zu binden, führen Sie die folgenden Schritte aus:

1. Heben Sie die Bindung der Standard-Verschlüsselungsgruppe ALL auf, die standardmäßig an den Dienst gebunden ist, wenn der Dienst erstellt wird.

```
unbind ssl service <service name> -cipherName ALL
<!--NeedCopy-->
```


2. Binden Sie die AES-Verschlüsselungsgruppe an den Dienst

```
bind ssl service <Service name> -cipherName AE
<!--NeedCopy-->
```

Wenn Sie die Verschlüsselungsgruppe DES zusätzlich zu AES binden möchten, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind ssl service <service name> -cipherName DES
<!--NeedCopy-->
```

Hinweis: Die freie virtuelle Citrix ADC Appliance unterstützt nur die DH-Verschlüsselungsgruppe.

Konfigurieren einer benutzerdefinierten Verschlüsselungsgruppe mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Verschlüsselungsgruppe hinzuzufügen oder Chiffre zu einer zuvor erstellten Gruppe hinzuzufügen, und überprüfen Sie die Einstellungen:

```
add ssl cipher <cipherGroupName>
bind ssl cipher <cipherGroupName> -cipherName <cipherGroup/cipherName>
show ssl cipher <cipherGroupName>
<!--NeedCopy-->
```

Beispiel:

```
add ssl cipher test

Done

bind ssl cipher test -cipherName ECDHE

Done

sh ssl cipher test

1)      Cipher Name: TLS1-ECDHE-RSA-AES256-SHA  Priority : 1
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1   HexCode
   =0xc014
```



```
2)      Cipher Name: TLS1-ECDHE-RSA-AES128-SHA  Priority : 2
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1   HexCode
   =0xc013
3)      Cipher Name: TLS1.2-ECDHE-RSA-AES-256-SHA384    Priority : 3
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA-384
   HexCode=0xc028
4)      Cipher Name: TLS1.2-ECDHE-RSA-AES-128-SHA256    Priority : 4
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA-256
   HexCode=0xc027
5)      Cipher Name: TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 Priority : 5
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(256) Mac=AEAD
   HexCode=0xc030
6)      Cipher Name: TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 Priority : 6
Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=AES-GCM(128) Mac=AEAD
   HexCode=0xc02f
7)      Cipher Name: TLS1-ECDHE-ECDSA-AES256-SHA        Priority : 7
Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=AES(256)  Mac=SHA1
   HexCode=0xc00a
8)      Cipher Name: TLS1-ECDHE-ECDSA-AES128-SHA        Priority : 8
Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=AES(128)  Mac=SHA1
   HexCode=0xc009
9)      Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-SHA384   Priority : 9
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES(256)  Mac=SHA-384
   HexCode=0xc024
10)     Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-SHA256   Priority : 10
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES(128)  Mac=SHA-256
   HexCode=0xc023
11)     Cipher Name: TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
   Priority : 11
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(256) Mac=AEAD
   HexCode=0xc02c
12)     Cipher Name: TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256
   Priority : 12
Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=AES-GCM(128) Mac=AEAD
   HexCode=0xc02b
13)     Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA        Priority : 13
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1   HexCode
   =0xc012
14)     Cipher Name: TLS1-ECDHE-ECDSA-DES-CBC3-SHA      Priority : 14
Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=3DES(168) Mac=SHA1
   HexCode=0xc008
15)     Cipher Name: TLS1-ECDHE-RSA-RC4-SHA     Priority : 15
Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=RC4(128)  Mac=SHA1   HexCode
   =0xc011
16)     Cipher Name: TLS1-ECDHE-ECDSA-RC4-SHA   Priority : 16
```



```
42 Description: SSLv3 Kx=ECC-DHE  Au=ECDSA Enc=RC4(128)  Mac=SHA1
      HexCode=0xc007
43 17)     Cipher Name: TLS1.2-ECDHE-RSA-CHACHA20-POLY1305 Priority : 17
44 Description: TLSv1.2 Kx=ECC-DHE  Au=RSA  Enc=CHACHA20/POLY1305(256) Mac
      =AEAD   HexCode=0xcca8
45 18)     Cipher Name: TLS1.2-ECDHE-ECDSA-CHACHA20-POLY1305
      Priority : 18
46 Description: TLSv1.2 Kx=ECC-DHE  Au=ECDSA Enc=CHACHA20/POLY1305(256)
      Mac=AEAD   HexCode=0xcca9
47 Done
48
49 bind ssl cipher test -cipherName TLS1-ECDHE-RSA-DES-CBC3-SHA
50 <!--NeedCopy-->
```

Entbinden von Verschlüsselungen aus einer Chiffregruppe mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Bindung von Verschlüsselungen aus einer benutzerdefinierten Verschlüsselungsgruppe aufzuheben, und überprüfen Sie die Einstellungen:

```
1 show ssl cipher <cipherGroupName>
2
3 unbind ssl cipher <cipherGroupName> -cipherName <string>
4
5 show ssl cipher <cipherGroupName>
6 <!--NeedCopy-->
```

Entfernen einer Verschlüsselungsgruppe mit der CLI

Hinweis: Eine integrierte Verschlüsselungsgruppe kann nicht entfernt werden. Bevor Sie eine benutzerdefinierte Verschlüsselungsgruppe entfernen, stellen Sie sicher, dass die Verschlüsselungsgruppe leer ist.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine benutzerdefinierte Verschlüsselungsgruppe zu entfernen, und überprüfen Sie die Konfiguration:

```
1 rm ssl cipher <userDefCipherGroupName> [<cipherName> ...]
2 show ssl cipher <cipherGroupName>
3
4 <!--NeedCopy-->
```


Beispiel:

```
rm ssl cipher test Done

sh ssl cipher test ERROR: No such resource [cipherGroupName, test]
<!--NeedCopy-->
```

Konfigurieren einer benutzerdefinierten Verschlüsselungsgruppe mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL > Cipher Groups**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie einen Namen für die Verschlüsselungsgruppe an.
4. Klicken Sie auf **Hinzufügen**, um die verfügbaren Chiffre und Verschlüsselungsgruppen anzuzeigen.
5. Wählen Sie eine Chiffre oder Verschlüsselungsgruppe aus und klicken Sie auf die Pfeilschaltfläche, um sie hinzuzufügen.
6. Klicken Sie auf **Erstellen**.
7. Klicken Sie auf **Schließen**.

So binden Sie eine Verschlüsselungsgruppe mit der CLI an einen virtuellen SSL-Server, einen Dienst oder eine Dienstgruppe:

Geben Sie an der Eingabeaufforderung einen der folgenden Schritte ein:

```
bind ssl vserver <vServerName> -cipherName <string>

bind ssl service <serviceName> -cipherName <string>

bind ssl serviceGroup <serviceGroupName> -cipherName <string>

<!--NeedCopy-->
```

Beispiel:

```
bind ssl vserver ssl_vserver_test -cipherName test
Done

bind ssl service  nshttps -cipherName test
Done

```



```
7 bind ssl servicegroup  ssl_svc  -cipherName test
8 Done
9 <!--NeedCopy-->
```

So binden Sie eine Verschlüsselungsgruppe mit der GUI an einen virtuellen SSL-Server, einen Dienst oder eine Dienstgruppe:

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

   Ersetzen Sie für den Dienst virtuelle Server durch Dienste. Ersetzen Sie bei Dienstgruppen virtuelle Server durch Dienstgruppen.

   Öffnen Sie den virtuellen Server, den Dienst oder die Dienstgruppe.

2. Wählen Sie unter **Erweiterte Einstellungen** die Option **SSL-Verschlüsselungen** aus.
3. Binden Sie eine Verschlüsselungsgruppe an den virtuellen Server, den Dienst oder die Dienstgruppe.

Binden einzelner Chiffre an einen virtuellen SSL-Server oder Dienst

Sie können auch einzelne Chiffre anstelle einer Chiffregruppe an einen virtuellen Server oder Dienst binden.

So binden Sie eine Verschlüsselung mit der CLI:
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind ssl vserver <vServerName> -cipherName <string>
2 bind ssl service <serviceName> -cipherName <string>
3 <!--NeedCopy-->
```

Beispiel:

```
1 bind ssl vserver v1 -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
2 Done
3
4 bind ssl service sslsvc -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
5 Done
6 <!--NeedCopy-->
```

So binden Sie eine Chiffre an einen virtuellen SSL-Server mit der GUI:

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie einen virtuellen SSL-Server aus, und klicken Sie auf **Bearbeiten**.

3. Wählen Sie unter **Erweiterte Einstellungen** die Option **SSL-Verschlüsselungen** aus.
4. Wählen Sie in **Cipher Suites Hinzufügen**aus.
5. Suchen Sie in der verfügbaren Liste nach der Verschlüsselung, und klicken Sie auf den Pfeil, um sie der konfigurierten Liste hinzuzufügen.
6. Klicken Sie auf **OK**.
7. Klicken Sie auf **Fertig**.

Um eine Verschlüsselung an einen SSL-Dienst zu binden, wiederholen Sie die vorherigen Schritte, nachdem Sie den virtuellen Server durch den Dienst ersetzt haben.

Unterstützungsmatrix für Serverzertifikate auf der ADC-Appliance

January 25, 2022

Ab Version 13.0 Build 41.x unterstützt die ADC-Appliance Serverzertifikatmeldungen, die in mehr als einen Datensatz fragmentiert sind, wenn die Gesamtgröße innerhalb von 32 KB liegt. Zuvor betrug die maximal unterstützte Größe 16 KB und die Fragmentierung wurde nicht unterstützt.

Die Citrix ADC-Appliance unterstützt die folgenden Serverzertifikate.

Tabelle 1: Unterstützung von Front-End- (FE) und Back-End-Diensten (BE)

Serverzertifikat/E	MPX/SDX (N2 CHIPS) FE Plattform	MPX/SDX (N2 CHIPS) BE	MPX/SDX (N3 CHIPS) FE	MPX/SDX (N3 CHIPS) BE	VPX FE	VPX BE
MD5	J	J	J	J	J	J
SHA1	J	J	J	J	J	J
SHA224	J	J	J	J	J	J
SHA256	J	J	J	J	J	J
SHA384	J	J	J	J	J	J
SHA512	J	J	J	J	J	J
RSA-Schlüssel	1024, 2048, 3072 und 4096 Bit	1024, 2048, 3072 und 4096 Bit	1024, 2048, 3072 und 4096 Bit	1024, 2048, 3072 und 4096 Bit	1024, 2048, 3072 und 4096 Bit	1024, 2048, 3072 und 4096 Bit
DH-Schlüssel	1024 Bit und 2048 Bit	1024 Bit und 2048 Bit	1024 Bit und 2048 Bit	1024 Bit und 2048 Bit	1024, 2048, 3072 und 4096 Bit	1024, 2048, 3072 und 4096 Bit

Serverzertifikat/Plattform	MPX 9700/10500/12500/15500 FIPS mit FW 2.2 FE	MPX 9700/10500/12500/15500 FIPS mit FW 2.2 BE	MPX/SDX 14030/14060/14080 FIPS FE	MPX/SDX 14030/14060/14080 FIPS BE
MD5	J	J	J	J
SHA1	J	J	J	J
SHA224	J	J	J	J
SHA256	J	J	J	J
SHA384	J	J	J	J
SHA512	J	J	J	J
RSA-Schlüssel	2048 Bit	2048 Bit	2048 Bit und 3072 Bit	2048 Bit und 3072 Bit
DH-Schlüssel	N	N	N	N

Hinweise

- 4k-Zertifikate erfordern höhere CPU-Zyklen und können die Leistung von Low-End-Appliances beeinträchtigen.
- In Version 11.1 und früher unterstützt eine Citrix ADC-Appliance die folgenden Erweiterungen für “Signaturalgorithmen” in der Hello-Nachricht des Back-End-Clients: RSA-MD5, RSA-SHA1 und RSA-SHA256.
  Die Citrix ADC-Appliance unterstützt keine Erweiterungen der Signaturalgorithmen SHA 384 und SHA 512. Daher setzen einige Server, z. B. Windows IIS-Server, die Verbindung zurück.
- Ab Release 12.0 unterstützt eine Citrix ADC-Appliance alle signature_algorithms Erweiterungen.

Clientauthentifizierung oder Mutual TLS (mTLS)

January 25, 2022

In einer typischen SSL-Transaktion prüft der Client, der über eine sichere Verbindung mit einem Server eine Verbindung herstellt, die Gültigkeit des Servers. Dazu prüft es das Zertifikat des Servers, bevor die SSL-Transaktion initiiert wird. Manchmal möchten Sie den Server jedoch so konfigurieren, dass er den Client authentifiziert, der eine Verbindung zu ihm herstellt.

Hinweis: Ab Version 13.0 Build 41.x unterstützt die Citrix ADC-Appliance Zertifikatsanforderungsnachrichten, die in mehr als einen Datensatz fragmentiert sind, sofern die Gesamtgröße 32 KB beträgt. Zuvor

betrug die maximal unterstützte Größe 16 KB und die Fragmentierung wurde nicht unterstützt.

Wenn die Clientauthentifizierung auf einem virtuellen SSL-Server aktiviert ist, fragt die Citrix ADC-Appliance während des SSL-Handshakes nach dem Clientzertifikat. Die Appliance prüft das vom Client vorgelegte Zertifikat auf normale Einschränkungen wie die Signatur des Ausstellers und das Ablaufdatum.

> **Hinweis Damit**
>
> die Appliance die Signaturen des Ausstellers überprüfen kann, muss das Zertifikat der Zertifizierungsstelle, die das Clientzertifikat ausgestellt hat, wie folgt lauten:
>
> - Auf dem Gerät installiert.
> - An den virtuellen Server gebunden, mit dem der Client Transaktionen durchführt.

Wenn das Zertifikat gültig ist, ermöglicht die Appliance dem Client den Zugriff auf alle sicheren Ressourcen. Wenn das Zertifikat jedoch ungültig ist, löscht die Appliance die Clientanforderung während des SSL-Handshakes.

Die Appliance überprüft das Clientzertifikat, indem sie zuerst eine Kette von Zertifikaten bildet, beginnend mit dem Clientzertifikat und endend mit dem Stammzertifizierungsstellenzertifikat für den Client (z. B. Verisign). Das Stammzertifizierungsstellenzertifikat kann ein oder mehrere zwischengeschaltete CA-Zertifikate enthalten (wenn die Stammzertifizierungsstelle das Clientzertifikat nicht direkt ausstellt).

Bevor Sie die Clientauthentifizierung auf der Citrix ADC-Appliance aktivieren, stellen Sie sicher, dass ein gültiges Clientzertifikat auf dem Client installiert ist. Aktivieren Sie dann die Clientauthentifizierung für den virtuellen Server, der die Transaktionen abwickelt. Binden Sie abschließend das Zertifikat der Zertifizierungsstelle, die das Clientzertifikat ausgestellt hat, an den virtuellen Server auf der Appliance.

Hinweis: Eine Citrix ADC MPX-Appliance unterstützt eine Zertifikatsschlüsselpaargröße von 512 Bit bis 4096 Bit. Das Zertifikat muss mit einem der folgenden Hash-Algorithmen signiert werden:

- MD5
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Wenn auf einer SDX-Appliance ein SSL-Chip einer VPX-Instanz zugewiesen ist, gilt die Unterstützung der Zertifikatsschlüsselpaargröße einer MPX-Appliance. Andernfalls gilt die normale Unterstützung der Zertifikat-Schlüssel-Paargröße einer VPX-Instanz.

Eine virtuelle Citrix ADC-Appliance (VPX-Instanz) unterstützt Zertifikate mit mindestens 512 Bit bis zu den folgenden Größen:

- 4096-Bit-Serverzertifikat auf dem virtuellen Server
- 4096-Bit-Clientzertifikat im Dienst
- 4096-Bit-CA-Zertifikat
- 4096-Bit-Zertifikat auf dem physischen Server

Hinweis: Ab Version 13.0 Build 79.x wird die Clientauthentifizierung mit einem 4096-Bit-RSA-Clientzertifikat während eines SSL-Handshakes auf der VPX-Plattform unterstützt.

Hinweise:

- Informationen zu MPX FIPS-Einschränkungen finden Sie unter Einschränkungen bei MPX FIPS.
- Informationen zu SDX FIPS-Einschränkungen finden Sie unter SDX FIPS-Einschränkungen.

Bereitstellen des Clientzertifikats

Bevor Sie die Clientauthentifizierung konfigurieren, muss ein gültiges Clientzertifikat auf dem Client installiert sein. Ein Clientzertifikat enthält Details zum spezifischen Clientsystem, das sichere Sitzungen mit der Citrix ADC-Appliance erstellt. Jedes Clientzertifikat ist eindeutig und darf nur von einem Clientsystem verwendet werden.

Unabhängig davon, ob Sie das Clientzertifikat von einer Zertifizierungsstelle erhalten, ein vorhandenes Clientzertifikat verwenden oder ein Clientzertifikat auf der Citrix ADC-Appliance generieren, müssen Sie das Zertifikat in das richtige Format konvertieren. Auf der Citrix ADC-Appliance werden Zertifikate entweder im PEM- oder DER-Format gespeichert und müssen in das PKCS #12 -Format konvertiert werden, bevor sie auf dem Clientsystem installiert werden. Nachdem Sie das Zertifikat konvertiert und auf das Clientsystem übertragen haben, stellen Sie sicher, dass es auf diesem System installiert und für die Clientanwendung konfiguriert ist. Die Anwendung, z. B. ein Webbrowser, muss Teil der SSL-Transaktionen sein.

Anweisungen zum Konvertieren eines Zertifikats aus dem PEM- oder DER-Format in das PKCS #12 -Format finden Sie unter Importieren und Konvertieren von SSL-Dateien.

Anweisungen zum Generieren eines Clientzertifikats finden Sie unter Erstellen eines Zertifikats.

Aktivieren der clientzertifikatbasierten Authentifizierung

Standardmäßig ist die Clientauthentifizierung auf der Citrix ADC-Appliance deaktiviert, und alle SSL-Transaktionen werden ohne Authentifizierung des Clients ausgeführt. Sie können die Clientauthentifizierung so konfigurieren, dass sie im Rahmen des SSL-Handshakes entweder optional oder obligatorisch ist.

Wenn die Clientauthentifizierung optional ist, fordert die Appliance das Clientzertifikat an, fährt jedoch mit der SSL-Transaktion fort, auch wenn der Client ein ungültiges Zertifikat vorlegt. Wenn die

Clientauthentifizierung erforderlich ist, beendet die Appliance den SSL-Handshake, wenn der SSL-Client kein gültiges Zertifikat bereitstellt.

Vorsicht: Citrix empfiehlt, dass Sie die richtigen Zugriffssteuerungsrichtlinien definieren, bevor Sie die clientzertifikatbasierte Authentifizierungsprüfung auf optional ändern.

Hinweis: Die Clientauthentifizierung ist für einzelne virtuelle SSL-Server konfiguriert, nicht global.

Clientzertifikatsbasierte Authentifizierung mithilfe der CLI aktivieren

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

```
set ssl vserver <vServerName> [-clientAuth (ENABLED | DISABLED)] [-
    clientCert (MANDATORY | OPTIONAL)]
show ssl vserver <vServerName>
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver vssl -clientAuth ENABLED -clientCert Mandatory
Done
show ssl vserver vssl

Advanced SSL configuration for VServer vssl:
DH: DISABLED
Ephemeral RSA: ENABLED Refresh Count: 0
Session Reuse: ENABLED Timeout: 120 seconds
Cipher Redirect: DISABLED
SSLv2 Redirect: DISABLED
ClearText Port: 0
Client Auth: ENABLED Client Cert Required: Mandatory
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
        SNI: DISABLED
        OCSP Stapling: DISABLED
        HSTS: DISABLED
        HSTS IncludeSubDomains: NO
        HSTS Max-Age: 0
SSLv2: DISABLED SSLv3: ENABLED TLSv1.0: ENABLED TLSv1.2: ENABLED TLSv1
    .2: ENABLED

```



```
1) CertKey Name: sslckey Server Certificate

1) Policy Name: client_cert_policy Priority: 0

1) Cipher Name: DEFAULT
Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

Clientzertifikatsbasierte Authentifizierung mithilfe der GUI aktivieren

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und öffnen Sie einen virtuellen Server.
2. Wählen Sie im Abschnitt SSL-Parameter die Option Clientauthentifizierung und in der Liste Clientzertifikat die Option Obligatorisch aus.

> **Hinweis:**
>
> Wenn die Clientauthentifizierung auf obligatorisch festgelegt ist und das Clientzertifikat Richtlinienerweiterungen enthält, schlägt die Zertifikatsüberprüfung fehl. Ab Version 12.0-56.x können Sie einen Parameter im Front-End-SSL-Profil festlegen, um diese Prüfung zu überspringen. Der Parameter ist standardmäßig deaktiviert. Das heißt, die Prüfung wird standardmäßig durchgeführt.

Überspringen Sie die Überprüfung der Richtlinienerweiterung während der Clientauthentifizierung mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile ns_default_ssl_profile_frontend -clientauth ENABLED -
    skipClientCertPolicyCheck ENABLED

Parameter

skipClientCertPolicyCheck

              Control policy extension check, if present inside the
                 X509 certificate chain. Applicable only if client
                 authentication is enabled and client certificate is
                 set to mandatory. Possible values functions as follows
                 :

```



```
- ENABLED: Skip the policy check during client authentication.

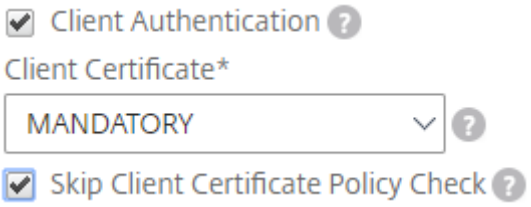
- DISABLED: Perform policy check during client authentication.

Possible values: ENABLED, DISABLED

Default: DISABLED
<!--NeedCopy-->
```

Überspringen Sie die Überprüfung der Richtlinienerweiterung während der Clientauthentifizierung mithilfe der GUI

1. Navigieren Sie zu **System** > **Profile** > **SSL-Profile**.
2. Erstellen Sie ein neues Front-End-Profil oder bearbeiten Sie ein vorhandenes Front-End-Profil.
3. Stellen Sie sicher, dass die Clientauthentifizierung aktiviert und das Clientzertifikat auf obligatorisch festgelegt ist
4. Wählen Sie **Überprüfung der Clientzertifikatrichtlinie überspringen**.



Binden von CA-Zertifikaten an den virtuellen Server

Eine Zertifizierungsstelle, deren Zertifikat auf der Citrix ADC-Appliance vorhanden ist, muss das für die Clientauthentifizierung verwendete Clientzertifikat ausstellen. Binden Sie dieses Zertifikat an den virtuellen Citrix ADC-Server, der die Clientauthentifizierung durchführt.

Binden Sie das CA-Zertifikat so an den virtuellen SSL-Server, dass die Appliance bei der Überprüfung des Clientzertifikats eine vollständige Zertifikatkette bilden kann. Andernfalls schlägt die Bildung der Zertifikatkette fehl und dem Client wird der Zugriff verweigert, auch wenn sein Zertifikat gültig ist.

Sie können CA-Zertifikate in beliebiger Reihenfolge an den virtuellen SSL-Server binden. Die Appliance bildet bei der Überprüfung des Clientzertifikats die richtige Reihenfolge.

Wenn der Client beispielsweise ein von **CA_A**ausgestelltes Zertifikat vorlegt, wobei **CA_A eine**Zwischenzertifizierungsstelle ist, deren Zertifikat von **CA_B**ausgestellt wird, dessen Zertifikat wiederum von einer vertrauenswürdigen Stammzertifizierungsstelle, **Root_CA**, einer Kette von Zertifikaten, die Alle drei Zertifikate müssen an den virtuellen Server der Citrix ADC-Appliance gebunden sein.

Anweisungen zum Binden eines oder mehrerer Zertifikate an den virtuellen Server finden Sie unter Binden des Zertifikatschlüsselpaars an den virtuellen SSL-Server.

Anweisungen zum Erstellen einer Zertifikatkette finden Sie unter Erstellen einer Zertifikatkette.

Strengere Kontrolle der Validierung von Clientzertifikaten

Die Citrix ADC-Appliance akzeptiert gültige Zwischen-CA-Zertifikate, wenn sie von einer einzigen Root-CA ausgestellt werden. Das heißt, wenn nur das Root-CA-Zertifikat an den virtuellen Server gebunden ist und diese Root-CA jedes mit dem Clientzertifikat gesendete Zwischenzertifikat validiert, vertraut die Appliance der Zertifikatkette und der Handshake ist erfolgreich.

Wenn ein Client jedoch eine Kette von Zertifikaten im Handshake sendet, kann keines der Zwischenzertifikate mithilfe eines CRL- oder OCSP-Responders validiert werden, es sei denn, dieses Zertifikat ist an den virtuellen SSL-Server gebunden. Selbst wenn eines der Zwischenzertifikate widerrufen wird, ist der Handshake daher erfolgreich. Im Rahmen des Handshakes sendet der virtuelle SSL-Server die Liste der an ihn gebundenen CA-Zertifikate. Für eine strengere Kontrolle können Sie den virtuellen SSL-Server so konfigurieren, dass er nur ein Zertifikat akzeptiert, das von einem der an diesen virtuellen Server gebundenen CA-Zertifikate signiert ist. Dazu müssen Sie die Einstellung **clientAuthuseBoundCachain** im an den virtuellen Server gebundenen SSL-Profil aktivieren. Der Handshake schlägt fehl, wenn eines der an den virtuellen Server gebundenen CA-Zertifikate das Clientzertifikat nicht signiert hat.

Beispiel: Zwei Clientzertifikate, clientcert1 und clientcert2, werden von den Zwischenzertifikaten Int-CA-A bzw. int-CA-B signiert. Die Zwischenzertifikate sind vom Stammzertifikat Root-CA signiert. Int-CA-A und Root-CA sind an den virtuellen SSL-Server gebunden. Im Standardfall (ClientAuthuseBoundCachain deaktiviert) werden sowohl clientcert1 als auch clientcert2 akzeptiert. Wenn ClientAuthuseBoundCachain jedoch aktiviert ist, akzeptiert die Citrix ADC-Appliance nur clientcert1.

Ermöglichen Sie eine strengere Kontrolle der Clientzertifikatvalidierung mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile <name> -ClientAuthUseBoundCAChain Enabled
<!--NeedCopy-->
```

Ermöglichen Sie eine strengere Kontrolle der Validierung von Clientzertifikaten mithilfe der GUI

1. Navigieren Sie zu **System** > **Profile**, wählen Sie die Registerkarte **SSL-Profile** und erstellen Sie ein SSL-Profil oder wählen Sie ein vorhandenes Profil aus.

2. Wählen Sie **Client-Authentifizierung mit gebundener Zertifizierungsstellenkette**aktivieren aus.

Serverauthentifizierung

October 5, 2021

Da die Citrix ADC Appliance SSL-Offload und -Beschleunigung im Auftrag eines Webservers durchführt, authentifiziert die Appliance das Zertifikat des Webservers normalerweise nicht. Sie können den Server jedoch in Bereitstellungen authentifizieren, die eine End-to-End-SSL-Verschlüsselung erfordern.

In einer solchen Situation wird die Appliance zum SSL-Client und führt eine sichere Transaktion mit dem SSL-Server durch. Es wird überprüft, ob eine CA, deren Zertifikat an den SSL-Dienst gebunden ist, das Serverzertifikat signiert hat, und prüft die Gültigkeit des Serverzertifikats.

Um den Server zu authentifizieren, aktivieren Sie die Serverauthentifizierung und binden Sie das Zertifikat der CA, die das Zertifikat des Servers signiert hat, an den SSL-Dienst auf der ADC-Appliance. Beim Binden des Zertifikats müssen Sie die Option “Bindung als CA” angeben.

Aktivieren (oder Deaktivieren) der Serverzertifikatsauthentifizierung

Sie können die CLI und die GUI verwenden, um die Serverzertifikatsauthentifizierung zu aktivieren und zu deaktivieren.

Aktivieren (oder deaktivieren) der Serverzertifikatsauthentifizierung mit der CLI

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

```
set ssl service <serviceName> -serverAuth ( ENABLED | DISABLED )
show ssl service <serviceName>
<!--NeedCopy-->
```

Beispiel:

```
set ssl service ssl-service-1 -serverAuth ENABLED
<!--NeedCopy-->
```



```
show ssl service ssl-service-1

            Advanced SSL configuration for Back-end SSL Service ssl-
               service-1:`
            DH: DISABLED
            Ephemeral RSA: DISABLED
            Session Reuse: ENABLED          Timeout: 300 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            Server Auth: ENABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED
    1)      Cipher Name: ALL
            Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

Aktivieren (oder deaktivieren) der Serverzertifikatsauthentifizierung mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, und öffnen Sie einen SSL-Dienst.
2. Wählen Sie im Abschnitt SSL-Parameter die Option Serverauthentifizierung aktivieren aus, und geben Sie einen allgemeinen Namen an.
3. Wählen Sie unter Erweiterte Einstellungen Zertifikate aus, und binden Sie ein Zertifizierungsstellenzertifikat an den Dienst.

Binden des Zertifizierungsstellenzertifikats an den Dienst mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um das Zertifizierungsstellenzertifikat an den Dienst zu binden und die Konfiguration zu überprüfen:

```
bind ssl service <serviceName> -certkeyName <string> -CA

show ssl service <serviceName>
<!--NeedCopy-->
```

Beispiel:


```
bind ssl service ssl-service-1 -certkeyName samplecertkey -CA
<!--NeedCopy-->
```

```
show ssl service ssl-service-1

            Advanced SSL configuration for Back-end SSL Service ssl-
               service-1:
            DH: DISABLED
            Ephemeral RSA: DISABLED
            Session Reuse: ENABLED          Timeout: 300 seconds
            Cipher Redirect: DISABLED
            SSLv2 Redirect: DISABLED
            Server Auth: ENABLED
            SSL Redirect: DISABLED
            Non FIPS Ciphers: DISABLED
            SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED
    1)      CertKey Name: samplecertkey     CA Certificate
       CRLCheck: Optional
    1)      Cipher Name: ALL
            Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

Konfigurieren eines allgemeinen Namens für die Serverzertifikatauthentifizierung

Bei der End-to-End-Verschlüsselung mit aktivierter Serverauthentifizierung können Sie einen gemeinsamen Namen in die Konfiguration eines SSL-Dienstes oder einer Dienstgruppe aufnehmen. Der angegebene Name wird während eines SSL-Handshakes mit dem allgemeinen Namen im Serverzertifikat verglichen. Wenn die beiden Namen übereinstimmen, ist der Handshake erfolgreich. Wenn die allgemeinen Namen nicht übereinstimmen, wird der für den Dienst oder die Dienstgruppe angegebene allgemeine Name mit den Werten im Feld Subject Alternative Name (SAN) im Zertifikat verglichen. Wenn er einem dieser Werte entspricht, ist der Handshake erfolgreich. Diese Konfiguration ist besonders nützlich, wenn sich beispielsweise zwei Server hinter einer Firewall befinden und einer der Server die Identität des anderen hinterlässt. Wenn der allgemeine Name nicht aktiviert ist, wird ein von beiden Servern vorgestelltes Zertifikat akzeptiert, wenn die IP-Adresse übereinstimmt.

Hinweis: Im SAN-Feld werden nur Domänenname, URL und E-Mail-ID DNS-Einträge verglichen.

Konfigurieren der Überprüfung gemeinsamem Namen für einen SSL-Dienst oder eine Dienstgruppe mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die Serverauthentifizierung mit der Überprüfung des gemeinsamen Namens anzugeben und die Konfiguration zu überprüfen:

1. Um einen allgemeinen Namen in einem Dienst zu konfigurieren, geben Sie Folgendes ein:

```
set ssl service <serviceName> -commonName <string> -serverAuth
    ENABLED
show ssl service <serviceName>
<!--NeedCopy-->
```

2. Um einen allgemeinen Namen in einer Dienstgruppe zu konfigurieren, geben Sie Folgendes ein:

```
set ssl serviceGroup <serviceGroupName> -commonName <string> -
    serverAuth ENABLED
show ssl serviceGroup <serviceGroupName>
<!--NeedCopy-->
```

Beispiel:

```
> set ssl service svc1 -commonName xyz.com -serverAuth ENABLED
<!--NeedCopy-->
```

```
show ssl service svc

     Advanced SSL configuration for Back-end SSL Service svc1:
     DH: DISABLED
     Ephemeral RSA: DISABLED
     Session Reuse: ENABLED Timeout: 300 seconds
     Cipher Redirect: DISABLED
     SSLv2 Redirect: DISABLED
     Server Auth: ENABLED Common Name: www.xyz.com
     SSL Redirect: DISABLED
     Non FIPS Ciphers: DISABLED
     SNI: DISABLED
     SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED
    1) CertKey Name: cacert CA Certificate OCSPCheck: Optional
```



```
    1) Cipher Name: ALL
     Description: Predefined Cipher Alias
Done
<!--NeedCopy-->
```

Konfigurieren der Überprüfung gemeinsamem Namen für einen SSL-Dienst oder eine Dienstgruppe mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**, oder navigieren Sie zu **Traffic Management > Load Balancing > Dienstgruppen**, und öffnen Sie einen Dienst oder eine Dienstgruppe.
2. Wählen Sie im Abschnitt SSL-Parameter die Option Serverauthentifizierung aktivieren aus, und geben Sie einen allgemeinen Namen an.

SSL-Aktionen und -Richtlinien

October 5, 2021

Eine SSL-Richtlinie wertet eingehenden Datenverkehr aus und wendet eine vordefinierte Aktion auf Anforderungen an, die einer Regel (Ausdruck) entsprechen. Konfigurieren Sie die Aktionen vor dem Erstellen der Richtlinien, damit Sie beim Erstellen einer Richtlinie eine Aktion angeben können. Um eine Richtlinie in Kraft zu setzen, führen Sie einen der folgenden Schritte aus:

- Binden Sie die Richtlinie an einen virtuellen Server auf der Appliance, sodass sie nur für den Datenverkehr gilt, der durch diesen virtuellen Server fließt.
- Binden Sie die Richtlinie global, damit sie für den gesamten Datenverkehr gilt, der durch die Appliance fließt.

SSL-Aktionen definieren SSL-Einstellungen, die Sie auf die ausgewählten Anforderungen anwenden können. Sie ordnen eine Aktion einer oder mehreren Richtlinien zu. Daten in Clientverbindungsanforderungen oder -antworten werden mit einer Regel verglichen, die in der Richtlinie angegeben ist, und die Aktion wird auf Verbindungen angewendet, die der Regel (Ausdruck) entsprechen.

Sie können klassische Richtlinien mit klassischen Ausdrücken und Standard-Syntaxrichtlinien mit Standardsyntaxausdrücken für SSL konfigurieren.

Hinweis: Benutzer, die keine Erfahrung mit der Konfiguration von Richtlinien an der CLI haben, finden in der Regel die Verwendung des Konfigurationsdienstprogramms erheblich einfacher.

Sie können einer Standard-Syntaxrichtlinie eine benutzerdefinierte Aktion oder eine integrierte Aktion zuordnen. Klassische Richtlinien erlauben nur benutzerdefinierte Aktionen. In der Standard-

Syntaxrichtlinie können Sie Richtlinien auch unter einer Richtlinienbezeichnung gruppieren. In diesem Fall werden sie nur angewendet, wenn sie von einer anderen Richtlinie aufgerufen werden.

Häufige Verwendung von SSL-Aktionen und -Richtlinien umfassen die Clientauthentifizierung pro Verzeichnis, Unterstützung für Outlook-Webzugriff und SSL-basierte Header-Einfügungen. SSL-basierte Header-Einfügungen enthalten SSL-Einstellungen, die von einem Server benötigt werden, dessen SSL-Verarbeitung an die Citrix ADC Appliance ausgelagert wurde.

SSL-Richtlinien

October 5, 2021

Richtlinien auf der Citrix ADC Appliance helfen, bestimmte Verbindungen zu identifizieren, die Sie verarbeiten möchten. Die Verarbeitung basiert auf den Aktionen, die für diese bestimmte Richtlinie konfiguriert sind. Nachdem Sie die Richtlinie erstellt und eine Aktion dafür konfiguriert haben, müssen Sie einen der folgenden Schritte ausführen:

- Binden Sie die Richtlinie an einen virtuellen Server auf der Appliance, sodass sie nur für den Datenverkehr gilt, der durch diesen virtuellen Server fließt.
- Binden Sie die Richtlinie global, damit sie für den gesamten Datenverkehr gilt, der durch einen virtuellen Server fließt, der auf der Citrix ADC Appliance konfiguriert ist.

Die SSL-Funktion der Citrix ADC Appliance unterstützt (erweiterte) Standard-Syntaxrichtlinien. Eine vollständige Beschreibung der Standardsyntaxausdrücke, wie sie funktionieren und wie sie manuell konfiguriert werden, finden Sie unter Richtlinien und Ausdrücke.

> **Hinweis:**
>
> Benutzer, die keine Erfahrung mit der Konfiguration von Richtlinien an der CLI haben, finden die Verwendung des Konfigurationsdienstprogramms normalerweise erheblich.

SSL-Richtlinien erfordern, dass Sie vor dem Erstellen einer Richtlinie eine Aktion erstellen, damit Sie die Aktionen beim Erstellen der Richtlinien angeben können.
In SSL-Standard-Syntaxrichtlinien können Sie auch die integrierten Aktionen verwenden. Weitere Informationen zu integrierten Aktionen finden Sie unter Integrierte SSL-Aktionen und benutzerdefinierte Aktionen.

SSL-Standard-Syntaxrichtlinien

Eine SSL-Standardsyntaxrichtlinie, auch als erweiterte Richtlinie bezeichnet, definiert ein Steuerelement oder eine Datenaktion, die bei Anforderungen ausgeführt werden soll. SSL-Richtlinien können daher als Steuerungsrichtlinien und Datenrichtlinien kategorisiert werden:

- **Kontrollrichtlinie**. Eine Steuerungsrichtlinie verwendet eine Steuerungsaktion, z. B. das Erzwingen der Clientauthentifizierung.
  Hinweis: In Version 10.5 oder höher ist die SSL-Neuverhandlung verweigern (denySSLReneg) standardmäßig auf ALL festgelegt. Steuerrichtlinien wie CLIENTAUTH lösen jedoch einen Neuverhandlungshandshake aus. Wenn Sie solche Richtlinien verwenden, müssen Sie denySSLReneg auf NO setzen.
- **Datenrichtlinie**. Eine Datenrichtlinie verwendet eine Datenaktion, z. B. das Einfügen einiger Daten in die Anforderung.

Die wesentlichen Bestandteile einer Richtlinie sind Ausdruck und Aktion. Der Ausdruck identifiziert die Anforderungen, für die die Aktion ausgeführt werden soll.

Sie können eine Standard-Syntaxrichtlinie mit einer integrierten Aktion oder einer benutzerdefinierten Aktion konfigurieren. Sie können eine Richtlinie mit einer integrierten Aktion konfigurieren, ohne eine separate Aktion zu erstellen. Um jedoch eine Richtlinie mit einer benutzerdefinierten Aktion zu konfigurieren, konfigurieren Sie zuerst die Aktion und dann die Richtlinie.

Sie können eine zusätzliche Aktion angeben, die als UNDEF-Aktion bezeichnet wird und ausgeführt wird, wenn das Anwenden des Ausdrucks auf eine Anforderung ein undefiniertes Ergebnis hat.

SSL-Richtlinienkonfiguration

Sie können eine SSL-Standard-Syntaxrichtlinie mit der CLI und der GUI konfigurieren.

Konfigurieren einer SSL-Richtlinie mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add ssl policy <name> -rule <expression> -Action <string> [-undefAction
      <string>] [-comment <string>]
2 <!--NeedCopy-->
```

Konfigurieren einer SSL-Richtlinie mit der GUI

Navigieren Sie zu **Traffic Management > SSL > Richtlinien** und klicken Sie auf der Registerkarte **Richtlinien** auf *Hinzufügen*.

Unterstützung für SSL-Richtlinien mit TLS1.3-Protokoll

Ab Release 13.0 Build 71.x und höher wird Unterstützung für SSL-Richtlinien mit dem TLS1.3-Protokoll hinzugefügt. Wenn das TLSv1.3-Protokoll für eine Verbindung ausgehandelt wird, lösen Richtlinien-

regeln, die TLS-Daten prüfen, die vom Client empfangen wurden, jetzt die konfigurierte Aktion aus.

Wenn die folgende Richtlinienregel beispielsweise “true” zurückgibt, wird der Datenverkehr an den in der Aktion definierten virtuellen Server weitergeleitet.

```
1 add ssl action action1 -forward vserver2
2 add ssl policy pol1 -rule client.ssl.client_hello.sni.contains( “xyz” )
      -action action1
3 <!--NeedCopy-->
```

Einschränkungen

- Kontrollrichtlinien werden nicht unterstützt.
- Die folgenden Aktionen werden nicht unterstützt:
  - DOCLIENTAUTH
  - NOCLIENTAUTH
  - CacertGrpName
  - ClientCertVerification
  - ssllogProfile

Integrierte SSL-Aktionen und benutzerdefinierte Aktionen

October 5, 2021

Wenn Sie nicht nur die integrierten Aktionen in Ihren Richtlinien benötigen, müssen Sie die Aktionen erstellen, bevor Sie die Richtlinien erstellen. Anschließend können Sie die Aktionen beim Erstellen der Richtlinien angeben. Die integrierten Aktionen sind von zwei Arten, Steueraktionen und Datenaktionen. Sie verwenden Steueraktionen in Steuerungsrichtlinien und Datenaktionen in Datenrichtlinien.

Die integrierten Steueraktionen sind:

- DOCLIENTAUTH - Führen Sie die Clientzertifikatauthentifizierung durch. (Nicht unterstützt für TLS1.3)
- NOCLIENTAUTH - Führen Sie keine Clientzertifikatauthentifizierung durch. (Nicht unterstützt für TLS1.3)

Die integrierten Datenaktionen sind:

- zurücksetzen — Schließen Sie die Verbindung, indem Sie ein RST-Paket an den Client senden.
- DROP - Alle Paket von dem Client fallen lassen. Die Verbindung bleibt offen, bis der Client sie schließt.

- NOOP - Leiten Sie das Paket ohne Operation weiter.

Hinweis: Alle abhängigen Aktionen zur Clientauthentifizierung, wie ClientCertVerification und SSLLogProfile, werden mit dem TLS 1.3-Protokoll nicht unterstützt.

Sie können benutzerdefinierte Datenaktionen erstellen. Wenn Sie die Clientauthentifizierung aktivieren, können Sie eine SSL-Aktion erstellen, um Clientzertifikatdaten in den Anforderungs-Header einzufügen, bevor Sie die Anforderung an den Webserver weiterleiten.

Wenn eine Richtlinienbewertung zu einem undefinierten Zustand führt, wird eine UNDEF-Aktion ausgeführt. Für eine Datenrichtlinie oder eine Steuerungsrichtlinie können Sie RESET, DROP oder NOOP als UNDEF -Aktion angeben. Für eine Steuerungsrichtlinie haben Sie auch die Möglichkeit, DOCLIENTAUTH oder NOCLIENTAUTH anzugeben.

Beispiele für integrierte Aktionen in einer Richtlinie

Wenn der Client im folgenden Beispiel eine andere Verschlüsselung als eine EXPORT-Kategorieverschlüsselung sendet, fordert die Citrix ADC Appliance die Clientauthentifizierung an. Der Client muss ein gültiges Zertifikat für eine erfolgreiche Transaktion bereitstellen.

```
1 add ssl policy pol1 -rule CLIENT.SSL.CIPHER_EXPORTABLE.NOT -reqAction
     DOCLIENTAUTH
2 <!--NeedCopy-->
```

In den folgenden Beispielen wird davon ausgegangen, dass die Clientauthentifizierung aktiviert ist.

Wenn die vom Benutzer bereitgestellte Version im Zertifikat mit der Version in der Richtlinie übereinstimmt, wird keine Aktion ausgeführt und das Paket wird weitergeleitet:

```
1 add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -
     reqAction NOOP
2 <!--NeedCopy-->
```

Wenn die Version im vom Benutzer bereitgestellten Zertifikat mit der Version in der Richtlinie übereinstimmt, wird die Verbindung gelöscht:

```
1 add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -
     reqAction DROP
2 <!--NeedCopy-->
```


Wenn die vom Benutzer bereitgestellte Version im Zertifikat mit der Version in der Richtlinie übereinstimmt, wird die Verbindung zurückgesetzt:

```
add ssl policy pol1 -rule CLIENT.SSL.CLIENT_CERT.VERSION.EQ(2) -
    reqAction RESET
<!--NeedCopy-->
```

Clientzertifikatüberprüfung mit richtlinienbasierter Clientauthentifizierung

Sie können die Clientzertifikatsüberprüfung auf obligatorisch oder Option festlegen, wenn Sie richtlinienbasierte Clientauthentifizierung konfiguriert haben. Der Standardwert ist obligatorisch.

Festlegen der Clientzertifikatüberprüfung mit der CLI auf optional

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ssl action <name> ((-clientAuth ( DOCLIENTAUTH | NOCLIENTAUTH ) [-
    clientCertVerification ( Mandatory | Optional )]
<!--NeedCopy-->
```

Beispiel:

```
add ssl action sslact -clientauth DOCLIENTAUTH -clientcertverification
    OPTIONAL
<!--NeedCopy-->
```

Festlegen der Clientzertifikatsüberprüfung auf optional mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL > Richtlinien**.
2. Klicken Sie auf der Registerkarte **SSL-Aktionen** auf **Hinzufügen**.
3. Geben Sie einen Namen an, und wählen Sie in der Liste **Clientzertifikatüberprüfung** die Option **Optional** aus.

Benutzerdefinierte SSL-Aktionen

Zusätzlich zu integrierten Aktionen können Sie je nach Bereitstellung auch andere SSL-Aktionen konfigurieren. Diese Aktionen werden als benutzerdefinierte Aktionen bezeichnet.

Konfigurieren einer benutzerdefinierten SSL-Aktion mit der CLI

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

```
add SSL action <name> -clientAuth(DOCLIENTAUTH | NOCLIENTAUTH) -
    clientCert (ENABLED | DISABLED) certHeader <string> -clientHeader <
    string> -clientCertSerialNumber (ENABLED | DISABLED) -
    certSerialHeader <string> -clientCertSubject (ENABLED | DISABLED) -
    certSubjectHeader <string> -clientCertHash (ENABLED | DISABLED) -
    certHashHeader <string> -clientCertIssuer (ENABLED | DISABLED) -
    certIssuerHeader <string> -sessionID (ENABLED | DISABLED) -
    sessionIDheader <string> -cipher (ENABLED | DISABLED) -cipherHeader
    <string> -clientCertNotBefore (ENABLED | DISABLED) -
    certNotBeforeHeader <string> -clientCertNotAfter (ENABLED | DISABLED
    ) -certNotAfterHeader <string> -OWASupport (ENABLED | DISABLED)
<!--NeedCopy-->
```

```
show ssl action [<name>]
<!--NeedCopy-->
```

Beispiel:

```
add ssl action Action-SSL-ClientCert -clientCert ENABLED -certHeader "X
    -Client-Cert"
<!--NeedCopy-->
```

```
show ssl action Action-SSL-ClientCert

1)      Name: Action-SSL-ClientCert
        Data Insertion Action:
        Cert Header: ENABLED            Cert Tag: X-Client-Cert
Done
<!--NeedCopy-->
```


Konfigurieren einer benutzerdefinierten SSL-Aktion mit der GUI

Navigieren Sie zu **Traffic Management > SSL > Richtlinien**, und klicken Sie auf der Registerkarte **Aktionen** auf **Hinzufügen**.

Konfigurieren einer SSL-Aktion zum Weiterleiten des Clientdatenverkehrs an einen anderen virtuellen Server

Administratoren können eine SSL-Aktion konfigurieren, um den auf einem virtuellen SSL-Server empfangenen Clientdatenverkehr an einen anderen virtuellen Server weiterzuleiten, um SSL-Abladung zu vermeiden. Oder zum Beenden der Verbindung auf der ADC-Appliance. Dieser virtuelle Server kann vom Typ: SSL, TCP oder SSL_BRIDGE sein. Beispielsweise können Administratoren wählen, die Anforderung an einen anderen virtuellen Server weiterzuleiten, anstatt die Verbindung zu beenden, wenn einer der folgenden Fälle:

- Die Appliance hat kein Zertifikat.
- Die Appliance unterstützt keine bestimmte Verschlüsselung.

Um dies zu erreichen, wird ein neuer Bindepunkt 'CLIENTHELLO_REQ' hinzugefügt, um den Client-Datenverkehr zu bewerten, wenn ein Client-Hallo empfangen wird. Wenn die Richtlinie, die an den virtuellen Server gebunden ist, der Clientdatenverkehr empfängt, nach der Analyse des Client-Hallo auf true ausgewertet wird, wird der Datenverkehr an einen anderen virtuellen Server weitergeleitet. Wenn dieser virtuelle Server vom Typ SSL ist, führt er den Handshake aus. Wenn dieser virtuelle Server vom Typ TCP oder SSL_BRIDGE ist, führt der Backend-Server den Handshake durch.

In Release 12.1-49.x werden nur die Vorwärts- und Rücksetzaktionen für den BIND-Punkt CLIENTHELLO_REQ unterstützt. Die folgenden Ausdruckspräfixe sind verfügbar:

- CLIENT.SSL.CLIENT_HELLO.CIPHERS.HAS_HEXCODE
- CLIENT.SSL.CLIENT_HELLO.CLIENT_VERSION
- CLIENT.SSL.CLIENT_HELLO.IS_RENEGOTIATE
- CLIENT.SSL.CLIENT_HELLO.IS_REUSE
- CLIENT.SSL.CLIENT_HELLO.IS_SCSV
- CLIENT.SSL.CLIENT_HELLO.IS_SESSION_TICKET
- CLIENT.SSL.CLIENT_HELLO.LENGTH
- CLIENT.SSL.CLIENT_HELLO.SNI
- CLIENT.SSL.CLIENT_HELLO.ALPN.HAS_NEXTPROTOCOL (from release 13.0 build 61.x)

Eine Beschreibung dieser Präfixe finden Sie unter Erweiterte Richtlinienausdrücke: Parsing SSL.

Dem Befehl `add SSL action` wird ein Parameter `forward` hinzugefügt, und dem Befehl `bind ssl vserver` wird ein neuer Bindpunkt `CLIENTHELLO_REQ` hinzugefügt.

Konfiguration über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ssl action <name> -forward <virtual server name>

add ssl policy <name> -rule <expression> -action <string>

bind ssl vserver <vServerName> -policyName <string> -priority <
   positive_integer> -type <type>
<!--NeedCopy-->
```

BEISPIEL:

```
add ssl action act1 -forward v2

add ssl policy pol1 -rule client.ssl.client_hello.ciphers.has_hexcode(0
   x002f) -action act1

bind ssl vserver v1 -policyName pol1 -priority 1 -type CLIENTHELLO_REQ
<!--NeedCopy-->
```

Konfiguration über die GUI

Navigieren Sie zu **Traffic Management > SSL > Richtlinien**.

SSL-Aktion erstellen:

1. Klicken Sie unter **SSL-Aktionen** auf **Hinzufügen**.
2. Geben Sie unter **SSL-Aktion erstellen** einen Namen für die Aktion an.
3. Wählen Sie unter **Virtueller Server Vorwärtsaktion** einen vorhandenen virtuellen Server aus, oder fügen Sie einen neuen virtuellen Server hinzu, an den der Datenverkehr weitergeleitet werden soll.
4. Legen Sie optional andere Parameter fest.
5. Klicken Sie auf **Erstellen**.

SSL-Richtlinie erstellen:

1. Klicken Sie in **SSL-Richtlinien** auf **Hinzufügen**.
2. Geben Sie unter **SSL-Richtlinie erstellen** einen Namen für die Richtlinie an.
3. Wählen Sie unter **Aktion**die Aktion aus, die Sie zuvor erstellt haben.
4. Geben Sie im **Ausdruckseditor** die auszuwertende Regel ein.

5. Klicken Sie auf **Erstellen**.

Erstellen oder Hinzufügen eines virtuellen Servers und Bind-Richtlinie:

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
2. Fügen Sie einen virtuellen Server hinzu oder wählen Sie diesen aus.
3. Klicken Sie unter **Erweiterte Einstellungen** auf **SSL-Richtlinien**.
4. Klicken Sie in den Abschnitt SSL-Richtlinie.
5. Wählen Sie unter **Richtlinie auswählen** die Richtlinie aus, die Sie zuvor erstellt haben.
6. Geben Sie unter **Richtlinienbindung** eine Priorität für die Richtlinie an.
7. Wählen Sie unter **Typ** die Option **CLIENTHELLO_REQ** aus.
8. Klicken Sie auf **Bind**.
9. Klicken Sie auf **Fertig**.

Die End-to-End-Konfiguration für die beliebtesten Anwendungsfälle finden Sie in den folgenden Themen:

- Konfigurieren Sie die SSL-Aktion, um den Clientdatenverkehr weiterzuleiten, wenn die Appliance kein domänenspezifisches (SNI-) Zertifikatbesitzt.
- Konfigurieren Sie eine SSL-Aktion, um den Clientdatenverkehr basierend auf dem Protokoll in der ALPN-Erweiterung der Client-Hallo Nachricht weiterzuleiten.
- Konfigurieren Sie die SSL-Aktion, um den Clientdatenverkehr weiterzuleiten, wenn eine Chiffre auf dem ADC nicht unterstützt wird.

SSL-Aktion zur selektiven Auswahl von Zertifizierungsstellen basierend auf SNI für die Clientauthentifizierung

Sie können nur die Liste der Zertifizierungsstellen basierend auf SNI (Domäne) in der Clientzertifikatanforderung senden und nicht die Liste aller Zertifizierungsstellen, die an einen virtuellen SSL-Server gebunden sind. Wenn beispielsweise ein Client-Hallo empfangen wird, werden nur die Zertifizierungsstellenzertifikate gesendet, die auf dem SSL-Richtlinienausdruck basieren (z. B. SNI). Um einen bestimmten Satz von Zertifikaten zu senden, müssen Sie eine Zertifizierungsstellenzertifikatsgruppe erstellen. Binden Sie diese Gruppe dann an eine SSL-Aktion, und binden Sie die Aktion an eine SSL-Richtlinie. Wenn die Richtlinie, die an den virtuellen Server gebunden ist, der den Clientdatenverkehr empfängt, nach der Analyse des Client-Hallo als true ausgewertet wird, wird im Clientanforderungszertifikat nur eine bestimmte Zertifizierungsstellengruppe gesendet.

Zuvor mussten Sie Zertifizierungsstellenzertifikate an einen virtuellen SSL-Server binden. Mit dieser Erweiterung können Sie CA-Zertifikatgruppen einfach hinzufügen und einer SSL-Aktion zuordnen.

Hinweis: Aktivieren Sie die Clientauthentifizierung und SNI auf dem virtuellen SSL-Server. Binden Sie die richtigen SNI-Zertifikate an den virtuellen Server.

Gehen Sie wie folgt vor:

1. Fügen Sie eine Zertifizierungsstellenzertifikatsgruppe hinzu.
2. Fügen Sie Zertifikatschlüsselpaare hinzu.
3. Binden Sie die Zertifikatschlüssel-Paare an diese Gruppe.
4. Fügen Sie eine SSL-Aktion hinzu.
5. Fügen Sie eine SSL-Richtlinie hinzu. Geben Sie die Aktion in der Richtlinie an.
6. Binden Sie die Richtlinie an einen virtuellen SSL-Server. Geben Sie den Bindepunkt als CLIENTHELLO_REQ an.

Konfiguration über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle in einer Sequenz ein:

```
add ssl caCertGroup <caCertGroupName>
add ssl certkey <certkey_name> -cert <cert> -key <key>
bind ssl caCertGroup <caCertGroupName> <certkey_name>
add ssl action <name> -caCertGrpName <string>
add ssl policy <name> -rule <expression> -action <string>
bind ssl vserver <vServerName> -policyName <string> -priority <
   positive_integer> -type CLIENTHELLO_REQ
<!--NeedCopy-->
```

Beispiel:

```
add ssl cacertGroup ca_cert_group

add ssl certkey ca_certkey1 -cert cacert1 -key cakey1
add ssl certkey ca_certkey2 -cert cacert2 -key cakey2
add ssl certkey snicert -cert snicert -key snikey

bind ssl cacertGroup ca_cert_group ca_certkey1
bind ssl caCertGroup ca_cert_group ca_certkey2
<!--NeedCopy-->
```

```
sh ssl caCertGroup ca_cert_group

CA GROUP NAME:     ca_cert_group
ACTIONS REFERRING: 1
```



```
5
6 1) CertKey Name: ca_certkey1   CA Certificate   CRLCheck: Optional
     CA_Name Sent
7 2) CertKey Name: ca_certkey2   CA Certificate   CRLCheck: Optional
     CA_Name Sent
8 <!--NeedCopy-->
```

```
1 add ssl action pick_ca_group -cacertGrpName ca_cert_group
2 <!--NeedCopy-->
```

```
1 sh ssl action pick_ca_group
2 1) Name: pick_ca_group
3    Type: Data Insertion
4    PickCaCertGroup: ca_cert_group
5    Hits: 0
6    Undef Hits: 0
7    Action Reference Count: 1
8 <!--NeedCopy-->
```

```
1 add ssl policy snipolicy -rule client.ssl.client_hello.sni.contains("
     abc") -action pick_ca_group
2 bind ssl vserver v_SSL -policyName snipolicy -type CLIENTHELLO_REQ -
     priority 10
3 <!--NeedCopy-->
```

```
1 sh ssl policy snipolicy
2     Name: snipolicy
3     Rule: client.ssl.client_hello.sni.contains("abc")
4     Action: pick_ca_group
5     UndefAction: Use Global
6     Hits: 0
7     Undef Hits: 0
8
9
10    Policy is bound to following entities
11 1)  Bound to: CLIENTHELLO_REQ VSERVER v_SSL
12    Priority: 10
```



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

```
set ssl vserver v_SSL -clientauth ENABLED -SNIEnable ENABLED
bind ssl vserver v_SSL -certkeyName snicert -sniCert
<!--NeedCopy-->
```

```
sh ssl vserver v_SSL

    Advanced SSL configuration for VServer v_SSL:
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED   Ephemeral RSA:
       ENABLED   Refresh Count: 0
    Session Reuse: ENABLED   Timeout: 120 seconds
    Cipher Redirect: DISABLED
    SSLv2 Redirect: DISABLED
    ClearText Port: 0
    Client Auth: ENABLED   Client Cert Required: Mandatory
    SSL Redirect: DISABLED
    Non FIPS Ciphers: DISABLED
    SNI: ENABLED
    OCSP Stapling: DISABLED
    HSTS: DISABLED
    HSTS IncludeSubDomains: NO
    HSTS Max-Age: 0
    SSLv2: DISABLED  SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: ENABLED
         TLSv1.2: ENABLED  TLSv1.3: DISABLED
    Push Encryption Trigger: Always
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1

    ECC Curve: P_256, P_384, P_224, P_521

1)  CertKey Name: snicert   Server Certificate for SNI


    Data policy
1)  Policy Name: snipolicy  Priority: 10

```



```
34
35
36 1)  Cipher Name: DEFAULT
37     Description: Default cipher list with encryption strength >= 128bit
38 <!--NeedCopy-->
```

Konfiguration über die GUI

Erstellen Sie Zertifizierungsstellenzertifikatsgruppe und binden Sie Zertifikate an die Gruppe:

1. Navigieren Sie zu **Traffic Management > SSL > CA Certificate Group**.
2. Klicken Sie auf **Hinzufügen**, und geben Sie einen Namen für die Gruppe an.
3. Klicken Sie auf **Erstellen**.
4. Wählen Sie die **Zertifizierungsstellenzertifikatsgruppe** aus, und klicken Sie dann auf **Bindungen anzeigen** .
5. Klicken Sie auf **Bind**.
6. Wählen Sie auf der Seite **CA-Zertifikatbindung** ein vorhandenes Zertifikat aus, oder klicken Sie auf Hinzufügen, um ein neues Zertifikat hinzuzufügen.
7. Klicken Sie auf **Auswählen** und dann auf **Binden**.
8. Wiederholen Sie die Schritte 5 bis 7, um ein anderes Zertifikat zu binden.
9. Klicken Sie auf **Schließen**.

Navigieren Sie zu **Traffic Management > SSL > Richtlinien**.

SSL-Aktion erstellen:

1. Klicken Sie unter **SSL-Aktionen** auf **Hinzufügen**.
2. Geben Sie unter **SSL-Aktion erstellen** einen Namen für die Aktion an.
3. Wählen Sie unter **Virtueller Server Vorwärtsaktion** einen vorhandenen virtuellen Server aus, oder fügen Sie einen virtuellen Server hinzu, an den der Datenverkehr weitergeleitet werden soll.
4. Legen Sie optional andere Parameter fest.
5. Klicken Sie auf **Erstellen**.

SSL-Richtlinie erstellen:

1. Klicken Sie in **SSL-Richtlinien** auf **Hinzufügen**.
2. Geben Sie unter **SSL-Richtlinie erstellen** einen Namen für die Richtlinie an.
3. Wählen Sie unter **Aktion**die zuvor erstellte Aktion aus.
4. Geben Sie im **Ausdruckseditor** die auszuwertende Regel ein.
5. Klicken Sie auf **Erstellen**.

Erstellen oder Hinzufügen eines virtuellen Servers und Bind-Richtlinie:

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

2. Fügen Sie einen virtuellen Server hinzu oder wählen Sie diesen aus.
3. Klicken Sie unter **Erweiterte Einstellungen** auf **SSL-Richtlinien**.
4. Klicken Sie in den Abschnitt SSL-Richtlinie.
5. Wählen Sie unter **Richtlinie auswählen** die Richtlinie aus, die Sie zuvor erstellt haben.
6. Geben Sie unter **Richtlinienbindung** eine Priorität für die Richtlinie an.
7. Wählen Sie unter **Typ** die Option **CLIENTHELLO_REQ** aus.
8. Klicken Sie auf **Bind**.
9. Klicken Sie auf **Fertig**.

Aufheben der Bindung einer Zertifizierungsstellenzertifikatsgruppe mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL > CA Certificate Group**.
2. Wählen Sie eine Zertifikatgruppe aus, und klicken Sie auf **Bindungen anzeigen**.
3. Wählen Sie das Zertifikat aus, das aus der Gruppe entfernt werden soll, und klicken Sie auf **Binden aufheben**.
4. Wenn Sie zur Bestätigung aufgefordert werden, klicken Sie auf **Ja••.
5. Klicken Sie auf **Schließen**.

Entfernen einer Zertifizierungsstellenzertifikatsgruppe mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL > CA Certificate Group**.
2. Wählen Sie eine Zertifikatgruppe aus, und klicken Sie auf **Löschen**.
3. Wenn Sie zur Bestätigung aufgefordert werden, klicken Sie auf **Ja**.

SSL-Richtlinienbindung

October 5, 2021

Sie können SSL-Richtlinien global oder nur an einen virtuellen SSL-Server binden. Globale Richtlinien werden ausgewertet, nachdem alle Richtlinien, die an Dienste, virtuelle Server oder andere Citrix ADC -Bindungspunkte gebunden sind. Wenn die eingehenden Daten mit einer der in der SSL-Richtlinie konfigurierten Regeln übereinstimmen, wird die Richtlinie ausgelöst, und die damit verbundene Aktion wird ausgeführt.

Wenn Sie eine SSL-Richtlinie an einen virtuellen Server binden, müssen Sie einen der folgenden Verbindungspunkte auswählen:

- REQUEST (Standardverbindungspunkt. Die Richtlinienbewertung erfolgt auf der HTTP-Ebene, nachdem der SSL-Handshake abgeschlossen ist.)

- INTERCEPT_REQ (Diese Option gilt für ein Citrix Secure Web Gateway -Setup. Weitere Informationen finden Sie unter SSL-Richtlinieninfrastruktur für SSL-Abfangen).
- CLIENTHELLO_REQ

Ebenso müssen Sie beim Aufheben der Bindung einer Richtlinie von einem virtuellen Server den Bindepunkt angeben.

Wenn Sie CLIENTHELLO_REQ als Bindepunkt angeben, wird die Richtlinie ausgewertet, wenn eine Client-Hallo Nachricht empfangen wird. Die zulässigen Aktionen sind RESET, FORWARD und `caCertGrpName`. Die Zurücksetzungsaktion beendet die Verbindung. Die Weiterleitungsaktion leitet die Anforderung zur Verarbeitung an einen virtuellen Lastausgleichsserver weiter. Die Aktion wählt `caCertGrpName` selektiv Zertifizierungsstellen basierend auf SNI für die Clientauthentifizierung aus. Weitere Informationen zu SSL-Aktionen finden Sie unter Integrierte SSL-Aktionen und benutzerdefinierte Aktionen.

Hinweis: Die Aktion CacertGrpName wird mit dem TLS 1.3-Protokoll nicht unterstützt.

Binden einer SSL-Richtlinie global mit der CLI

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um eine globale SSL-Richtlinie zu binden und die Konfiguration zu überprüfen:

```
bind ssl global - policyName <string> [- priority <positive_integer>]
show ssl global
<!--NeedCopy-->
```

Beispiel:

```
bind ssl global -policyName Policy-SSL-2 -priority 90
Done

sh ssl global

      1) Name: Policy-SSL-2 Priority: 90
      2) Name: Policy-SSL-1 Priority: 100
      Done
<!--NeedCopy-->
```

Binden Sie eine SSL-Richtlinie global mit der GUI

1. Navigieren Sie zu **Traffic Management** > **SSL** > **Richtlinien**.

2. Klicken Sie im Detailbereich auf **Globale Bindungen**.
3. Klicken Sie im Dialogfeld **SSL-Richtlinien an global binden/aufheben** auf **Richtlinie einfügen**.
4. Wählen Sie in der Liste **Richtlinienname** eine Richtlinie aus.
5. Ziehen Sie den Eintrag optional an eine neue Position in der Richtlinienbank, um die Prioritätsstufe automatisch zu aktualisieren.
6. Klicken Sie auf **OK**. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die Richtlinie erfolgreich gebunden wurde.

Binden oder Aufheben der Bindung einer SSL-Richtlinie an einen virtuellen Server mit der CLI

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

```
bind ssl vserver <vServerName> -policyName <string> -priority <
    positive_integer> -type <type>

unbind ssl vserver <vServerName> -policyName <string> -priority <
    positive_integer> -type <type>

<!--NeedCopy-->
```

Beispiel:

```
bind ssl vserver v1 -policyName pol1 -priority 1 -type CLIENTHELLO_REQ
<!--NeedCopy-->
```

```
unbind ssl vserver v1 -policyName pol1 -priority 1 -type
    CLIENTHELLO_REQ
<!--NeedCopy-->
```

```
show ssl vserver vs-server

Advanced SSL configuration for VServer vs-server:

DH: DISABLED

```



```
Ephemeral RSA: ENABLED          Refresh Count: 1000

Session Reuse: ENABLED          Timeout: 120 seconds

Cipher Redirect: DISABLED

SSLv2 Redirect: DISABLED

ClearText Port: 80

Client Auth: DISABLED

SSL Redirect: ENABLED

SSL-REDIRECT Port Rewrite: ENABLED

Non FIPS Ciphers: DISABLED

SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED

1)      Policy Name: ssl-policy-1        Priority: 10

1)      Cipher Name: DEFAULT

            Description: Predefined Cipher Alias

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

Binden einer SSL-Richtlinie an einen virtuellen Server mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie einen virtuellen SSL-Server.
2. Wählen Sie unter **Erweiterte Einstellungen** die Option **SSL-Richtlinie** aus. Klicken Sie im Abschnitt **SSL-Richtlinie**, um eine Richtlinie an den virtuellen Server zu binden.
3. Wählen Sie auf der Seite **Richtlinienbindung** eine vorhandene Richtlinie aus, oder fügen Sie eine neue Richtlinie hinzu.
4. Geben Sie Priorität und Typ (Bindepunkt) für die Richtlinie an.
5. Wählen Sie **Binden** aus.
6. Wählen Sie **Fertig** aus.

SSL-Richtlinienbeschriftungen

October 5, 2021

Richtlinienbezeichnungen sind Inhaber für Richtlinien. Ein Richtlinienlabel hilft bei der Verwaltung einer Gruppe von Richtlinien, die sogenannte Richtlinienbank, die von einer anderen Richtlinie aufgerufen werden kann. SSL-Richtlinienbeschriftungen können Steuerbeschriftungen oder Datenbeschriftungen sein, abhängig vom Typ der Richtlinien, die in der Richtlinienbeschriftung enthalten sind. Sie können nur Datenrichtlinien zu einer Datenrichtlinienbeschriftung und nur Steuerrichtlinien in einer Steuerrichtlinienbeschriftung hinzufügen. Um die Policenbank zu erstellen, binden Sie Richtlinien an das Label und geben Sie die Reihenfolge der Bewertung jeder Richtlinie im Verhältnis zu anderen in der Bank der Richtlinien für das Richtlinienlabel an. An der CLI geben Sie zwei Befehle ein, um eine Richtlinienbezeichnung zu erstellen und Richtlinien an die Richtlinienbezeichnung zu binden. Im Konfigurationsdienstprogramm wählen Sie Optionen aus einem Dialogfeld aus.

Hinweis: Richtlinienbeschriftungen der Typsteuerung werden mit dem TLS 1.3-Protokoll nicht unterstützt.

Erstellen eines SSL-Richtlinienbezeichners und Binden von Richtlinien an das Label mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ssl policylabel <labelName> -type ( CONTROL | DATA )

bind ssl policylabel <labelName> <policyName> <priority> [<
   gotoPriorityExpression>] [-invoke (<labelType> <labelName>) ]
<!--NeedCopy-->
```

Beispiel:

```
add ssl policylabel cpl1 -type CONTROL

add ssl policylabel dpl1 -type DATA

bind ssl policylabel cpl1 -policyName ctrlpol -priority 1

bind ssl policylabel dpl1 -policyName datapol -priority 1
<!--NeedCopy-->
```


Konfigurieren Sie ein SSL-Richtlinienlabel und binden Sie Richtlinien mit der GUI an das Label

Navigieren Sie zu **Traffic Management > SSL > Policy Labels**, und konfigurieren Sie ein SSL-Richtlinienlabel.

Selektive SSL-Protokollierung

October 5, 2021

In einer großen Bereitstellung, die Tausende virtueller Server umfasst, werden alle SSL-bezogenen Informationen protokolliert. Zuvor war das Filtern der Clientauthentifizierung und des SSL-Handshake Erfolge und Fehler für einige kritische virtuelle Server nicht einfach. Das Durchblättern des gesamten Protokolls, um diese Informationen zu erhalten, war eine zeitaufwändige und mühsame Aufgabe, da die Infrastruktur nicht die Kontrolle zum Filtern der Protokolle bot. Jetzt können Sie SSL-bezogene Informationen für einen bestimmten virtuellen Server oder für eine Gruppe virtueller Server protokollieren.ns.log“ Diese Informationen sind besonders hilfreich bei Debugging-Fehlern. Um diese Informationen zu protokollieren, müssen Sie ein SSL-Protokollprofil hinzufügen.

Siehe Beispiel ns.log-Ausgabe für eine erfolgreiche Clientauthentifizierung am Ende dieser Seite.

Wichtig: Setzen Sie die Syslog-Log-Ebene auf DEBUG. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set audit syslogParams -logLevel DEBUG
```

SSL-Protokollprofil

Ein SSL-Protokollprofil ermöglicht die Kontrolle über die Protokollierung der folgenden Ereignisse für einen virtuellen Server oder eine Gruppe virtueller Server:

- Erfolg und Fehler der Clientauthentifizierung oder nur Fehler.
- SSL-Handshake-Erfolg und -Fehler oder nur Fehler.

Standardmäßig sind alle Parameter deaktiviert.

Ein SSL-Protokollprofil kann für ein SSL-Profil oder für eine SSL-Aktion festgelegt werden. Wenn auf ein SSL-Profil festgelegt ist, können Sie sowohl die Clientauthentifizierung als auch die Erfolgs- und Fehlerinformationen des SSL-Handshakes protokollieren. Wenn auf eine SSL-Aktion festgelegt ist, können Sie nur Erfolgs- und Fehlerinformationen der Clientauthentifizierung protokollieren, da der Handshake abgeschlossen ist, bevor die Richtlinie ausgewertet wird.

Clientauthentifizierung und SSL-Handshake Erfolg und Fehler werden protokolliert, auch wenn Sie kein SSL-Protokollprofil konfigurieren. Eine selektive Protokollierung ist jedoch nur möglich, wenn ein SSL-Protokollprofil verwendet wird.

> **Hinweis:**
>
> SSL-Protokollprofil wird bei Hochverfügbarkeits- und Cluster-Setups unterstützt.

Hinzufügen eines SSL-Protokollprofils mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add ssl logprofile <name> [-sslLogClAuth ( ENABLED | DISABLED )] [-
     ssllogClAuthFailures ( ENABLED | DISABLED )] [-sslLogHS ( ENABLED |
     DISABLED )] [-sslLogHSfailures ( ENABLED | DISABLED )]
2 <!--NeedCopy-->
```

Die Parameter:

Name:

Name für das SSL-Protokollprofil. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Nach der Erstellung des Profils kann nicht geändert werden.

Name ist ein obligatorisches Argument. Maximale Länge: 127

`sslLogClAuth`:

Protokollieren Sie alle Clientauthentifizierungsereignisse. Enthält sowohl Erfolgs- als auch Fehlerereignisse.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

`ssllogClAuthFailures`:

Protokollieren Sie alle Ereignisse des Clientauthentifizierungsfehlers.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

`sslLogHS`:

Protokollieren Sie alle Ereignisse im Zusammenhang mit SSL-Handshake. Enthält sowohl Erfolgs- als auch Fehlerereignisse.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

sslLogHSfailures:

Protokollieren Sie alle SSL-Handshake-bezogenen Fehlerereignisse.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

Beispiel:

```
> add ssl logprofile ssllog10 -sslLogClAuth ENABLED -sslLogHS ENABLED

 Done

sh ssllogprofile ssllog10

1)      Name: ssllog10

        SSL log ClientAuth [Success/Failures] : ENABLED

        SSL log ClientAuth [Failures] : DISABLED

        SSL log Handshake [Success/Failures] : ENABLED

        SSL log Handshake [Failures] : DISABLED

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

Hinzufügen eines SSL-Protokollprofils mit der GUI

Navigieren Sie zu **System > Profile > SSL-Protokollprofil**, und fügen Sie ein Profil hinzu.

Ändern eines SSL-Protokollprofils mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl logprofile <name> [-sslLogClAuth ( ENABLED | DISABLED )][-
    ssllogClAuthFailures ( ENABLED | DISABLED )] [-sslLogHS ( ENABLED |
    DISABLED )] [-sslLogHSfailures ( ENABLED | DISABLED )]
```



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

Beispiel:

```
set ssllogprofile ssllog10 -ssllogClAuth en -ssllogClAuthFailures en -
    ssllogHS en -ssllogHSfailures en

Done

sh ssllogprofile ssllog10

    1)            Name: ssllog10

                    SSL log ClientAuth [Success/Failures] : ENABLED
                    SSL log ClientAuth [Failures] : ENABLED
                    SSL log Handshake [Success/Failures] : ENABLED
                    SSL log Handshake [Failures] : ENABLED
     Done
<!--NeedCopy-->
```

Ändern eines SSL-Protokollprofils mit der GUI

1. Navigieren Sie zu **System > Profile > SSL-Protokollprofil**, wählen Sie ein Profil aus, und klicken Sie auf **Bearbeiten**.
2. Nehmen Sie Änderungen vor, und klicken Sie auf **OK**.

Anzeigen aller SSL-Protokollprofile mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
sh ssl logprofile
<!--NeedCopy-->
```

Beispiel:

```
sh ssl logprofile

    1)            Name: ssllogp1
                    SSL log ClientAuth [Success/Failures] : ENABLED
```



```
                    SSL log ClientAuth [Failures] : ENABLED
                    SSL log Handshake [Success/Failures] : DISABLED
                    SSL log Handshake [Failures] : ENABLED

    2)            Name: ssllogp2
                    SSL log ClientAuth [Success/Failures] : DISABLED
                    SSL log ClientAuth [Failures] : DISABLED
                    SSL log Handshake [Success/Failures] : DISABLED
                    SSL log Handshake [Failures] : DISABLED

    3)            Name: ssllogp3
                    SSL log ClientAuth [Success/Failures] : DISABLED
                    SSL log ClientAuth [Failures] : DISABLED
                    SSL log Handshake [Success/Failures] : DISABLED
                    SSL log Handshake [Failures] : DISABLED

    4)            Name: ssllog10
                    SSL log ClientAuth [Success/Failures] : ENABLED
                    SSL log ClientAuth [Failures] : ENABLED
                    SSL log Handshake [Success/Failures] : ENABLED
                    SSL log Handshake [Failures] : ENABLED
Done
<!--NeedCopy-->
```

Anzeigen aller SSL-Protokollprofile mit der GUI

Navigieren Sie zu **System > Profile > SSL-Protokollprofil**. Alle Profile sind aufgelistet.

Anfügen eines SSL-Protokollprofils an ein SSL-Profil

Sie können ein SSL-Protokollprofil an ein SSL-Profil anhängen (festlegen), wenn Sie ein SSL-Profil erstellen, oder später, indem Sie das SSL-Profil bearbeiten. Sie können sowohl Clientauthentifizierung als auch Handshake-Erfolge und -Fehler protokollieren.

> **Wichtig:**
>
> Das Standard-SSL-Profil muss aktiviert sein, bevor Sie ein SSL-Protokollprofil anhängen können.

Anfügen eines SSL-Protokollprofils an ein SSL-Profil mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set ssl profile <name> [-ssllogProfile <string>]
<!--NeedCopy-->
```

Beispiel:

```
set ssl profile fron_1 -ssllogProfile ssllog10
<!--NeedCopy-->
```

Anfügen eines SSL-Protokollprofils an ein SSL-Profil mit der GUI

1. Navigieren Sie zu **System > Profile > SSL-Profil**.
2. Klicken Sie auf **Bearbeiten** und geben Sie im **SSL-Protokollprofil**ein Profil an.

Anfügen eines SSL-Protokollprofils an eine SSL-Aktion

Sie können ein SSL-Protokollprofil nur beim Erstellen einer SSL-Aktion festlegen. Sie können eine SSL-Aktion nicht ändern, um das Protokollprofil festzulegen. Ordnen Sie die Aktion einer Richtlinie zu. Sie können nur Erfolge und Fehler der Clientauthentifizierung protokollieren.

Anfügen eines SSL-Protokollprofils an eine SSL-Aktion mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ssl action <name> -clientAuth ( DOCLIENTAUTH | NOCLIENTAUTH ) -
   ssllogProfile <string>
<!--NeedCopy-->
```

Beispiel:

```
> add ssl action act1 -clientAuth DoCLIENTAUTH -ssllogProfile ssllog10

Done

> sh ssl action act1

    1)            Name: act1
                    Type: Client Authentication (DOCLIENTAUTH)
                    Hits: 0
```



```
                    Undef Hits: 0
                    Action Reference Count: 0
                    SSLlogProfile: ssllog10
Done
<!--NeedCopy-->
```

Anfügen eines SSL-Protokollprofils an eine SSL-Aktion mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL > Richtlinien**, und klicken Sie auf **SSL-Aktionen** .
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie unter Clientauthentifizierung die **Option ENABLED**aus.
4. Wählen Sie im SSL-Protokollprofil ein Profil aus der Liste aus, oder klicken Sie auf +, um ein Profil zu erstellen.
5. Klicken Sie auf **Erstellen**.

Beispielausgabe aus der Protokolldatei

Im Folgenden finden Sie eine Beispielprotokollausgabe von`ns.log` für eine erfolgreiche Clientauthentifizierung.

```
Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUCCESS 158 0 :  SPCBId 671 - ClientIP 10.102.1.98 - ClientPort 49451 - VserverServiceIP 10.102.57.82 - VserverServicePort 443 - ClientVersion TLSv1.2 - CipherSuite ”AES-256-CBC-SHA TLSv1.2 Non-Export 256-bit” - Session New - CLIENT_AUTHENTICATED -SerialNumber ”2A” - SignatureAlgorithm ”sha1WithRSAEncryption” - ValidFrom ”Sep 22 09:15:20 2008 GMT” - ValidTo ”Feb  8 09:15:20 2036 GMT” - HandshakeTime 10 ms
Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-PPE-0 : default SSLLOG SSL_HANDSHAKE_ISSUERNAME 159 0 :  SPCBId 671 - IssuerName ” C=IN,ST=KAR,O=Citrix R&D Pvt Ltd,CN=Citrix”
Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUBJECTNAME 160 0 :  SPCBId 671 - SubjectName ” C=IN,ST=KAR,O=Citrix Pvt Ltd,OU=A,CN=B”
Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUCCESS 161 0 :  Backend SPCBId 674 - ServerIP 10.102.57.85 - ServerPort 443 - ProtocolVersion TLSv1.2 - CipherSuite ”AES-256-CBC-SHA TLSv1.2 Non-Export 256-bit” - Session Reuse - SERVER_AUTHENTICATED -SerialNumber ”3E” - SignatureAlgorithm ”sha1WithRSAEncryption” - ValidFrom ”Sep 24
```



```
    06:40:37 2008 GMT" - ValidTo "Feb 10 06:40:37 2036 GMT" -
    HandshakeTime 1 ms
5 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_ISSUERNAME 162 0 :  SPCBId 674
    - IssuerName " C=IN,ST=KAR,O=Citrix Pvt Ltd"
6 Jan 24 16:24:25 <local0.debug> 10.102.57.80 01/24/2019:10:54:25 GMT  0-
    PPE-0 : default SSLLOG SSL_HANDSHAKE_SUBJECTNAME 163 0 :  SPCBId 674
     - SubjectName " C=IN,ST=P,L=Q,O=R"
7 <!--NeedCopy-->
```

Unterstützung des DTLS-Protokolls

February 24, 2022

Hinweise:

- Das DTLSv1.0-Protokoll wird auf Citrix ADC MPX/SDX (N2- und N3-basiert), VPX und MPX 14000 FIPS-Appliances unterstützt. Es wird auf externen HSMs nicht unterstützt.
- Das DTLS 1.0-Protokoll wird auf Citrix ADC-Appliances unterstützt, die Intel Coleto SSL-Chips enthalten (ab Version 12.1 Build 50.x).
- Das DTLSv1.2-Protokoll wird im Front-End von Citrix ADC VPX-Appliances unterstützt (ab Version 13.0 Build 47.x).
- Das DTLS 1.2-Protokoll wird im Front-End von Citrix ADC-Appliances unterstützt, die Intel Coleto SSL-Chips enthalten (ab Release 13.0 Build 52.x). Weitere Informationen zu den Plattformen, die Intel Coleto SSL-Chips enthalten, finden Sie unter Unterstützung für Intel Coleto SSL-Chip-basierte Plattformen.
- Dienstgruppen vom Typ DTLS werden nicht unterstützt.
- Das DTLSv1.2-Protokoll wird im Front-End von Citrix ADC MPX (N3-basiert) Appliances unterstützt (ab Release 13.0 Build 58.x).
- Informationen zur Unterstützung von Enlightened Data Transport (EDT) für Citrix Gateway finden Sie unter Unterstützung von HDX Enlightened Data Transport.
- Es wurden Änderungen am DTLS-Profil ab Version 13.0 build 79.x vorgenommen. Weitere Informationen finden Sie unter DTLS-Profil.
- Ab Version 13.0 build 82.x `maxBadmacIgnorecount` wird ein neuer Parameter im DTLS-Profil eingeführt, um fehlerhafte MAC-Datensätze zu ignorieren, die in einer DTLS-Sitzung empfangen wurden. Weitere Informationen finden Sie unter DTLS-Profil.
- Informationen zu den unterstützten Plattformen und Builds finden Sie unter Citrix ADC MPX-Hardware-Software-Kompatibilitätsmatrix.

Die SSL- und TLS-Protokolle wurden traditionell verwendet, um Streaming-Datenverkehr zu sichern.

Beide Protokolle basieren auf TCP, das langsam ist. Außerdem kann TLS keine verlorenen oder neu geordneten Pakete verarbeiten.

UDP ist das bevorzugte Protokoll für Audio- und Videoanwendungen wie Lync, Skype, iTunes, YouTube, Schulungsvideos und Flash. UDP ist jedoch nicht sicher oder zuverlässig. Das DTLS-Protokoll wurde entwickelt, um Daten über UDP zu sichern, und wird für Anwendungen wie Medienstreaming, VOIP und Online-Gaming für die Kommunikation verwendet. In DTLS wird jeder Handshake-Nachricht innerhalb dieses Handshakes eine bestimmte Sequenznummer zugewiesen. Wenn ein Peer eine Handshake-Nachricht erhält, kann er schnell feststellen, ob diese Nachricht die nächste erwartete ist. Wenn dies der Fall ist, verarbeitet der Peer die Nachricht. Wenn nicht, wird die Nachricht zur Bearbeitung in die Warteschlange gestellt, nachdem alle vorherigen Nachrichten empfangen wurden.

Erstellen Sie einen virtuellen DTLS-Server und einen Dienst vom Typ UDP. Standardmäßig ist ein DTLS-Profil (nsdtls_default_profile) an den virtuellen Server gebunden. Optional können Sie ein benutzerdefiniertes DTLS-Profil erstellen und an den virtuellen Server binden.

Hinweis: RC4-Chiffrern werden auf einem virtuellen DTLS-Server nicht unterstützt.

DTLS-Konfiguration

Sie können die Befehlszeile (CLI) oder das Konfigurationsdienstprogramm (GUI) verwenden, um DTLS auf Ihrer ADC-Appliance zu konfigurieren.

Hinweis: Ab Version 13.0 Build 47.x wird das DTLS 1.2-Protokoll im Frontend einer Citrix ADC VPX-Appliance unterstützt. Geben Sie bei der Konfiguration eines virtuellen DTLSv1.2-Servers DTLS12 an. Die Standardeinstellung ist DTLS1.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl vserver DTLS [-dtls1 ( ENABLED | DISABLED )] [-dtls12 ( ENABLED |
DISABLED )]
```

Erstellen einer DTLS-Konfiguration über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb vserver <vserver_name> DTLS <IPAddress>  <port>
2 add service  <service_name>  <IPAddress> UDP 443
3 bind lb vserver  <vserver_name>  <udp_service_name>
4 <!--NeedCopy-->
```

Die folgenden Schritte sind optional:


```
add dtlsProfile dtls-profile -maxretryTime <positive_integer>
set ssl vserver <vserver_name> -dtlsProfileName <dtls_profile_name>
<!--NeedCopy-->
```

Erstellen einer DTLS-Konfiguration über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Erstellen Sie einen virtuellen Server vom Typ DTLS und binden Sie einen UDP-Dienst an den virtuellen Server.
3. Ein Standard-DTLS-Profil ist an den virtuellen DTLS-Server gebunden. Um ein anderes Profil zu binden, wählen Sie in SSL-Parametern ein anderes DTLS-Profil aus. Um ein Profil zu erstellen, klicken Sie auf das Plus (+) neben DTLS-Profil.

Unterstützung für SNI auf einem virtuellen DTLS-Server

Informationen zu SNI finden Sie unter Konfigurieren eines virtuellen SNI-Servers für das sichere Hosting mehrerer Websites.

Konfigurieren von SNI auf einem virtuellen DTLS-Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl vserver <vServerName> -SNIEnable ENABLED
bind ssl vserver <vServerName> -certkeyName <string> -SNICert
show ssl vserver <vServerName>
<!--NeedCopy-->
```

Beispiel:

```
set ssl vserver v1 -sniEnable ENABLED
bind ssl vserver  v1 -certkeyName san2 -sniCert
bind ssl vserver  v1 -certkeyName san13  - sniCert
bind ssl vserver  v1 -certkeyName san17  - sniCert
<!--NeedCopy-->
```



```
sh ssl vserver v1

Advanced SSL configuration for VServer v1:
DH: DISABLED
DH Private-Key Exponent Size Limit: DISABLED
Ephemeral RSA: ENABLED
Refresh Count: 0
Session Reuse: ENABLED
Timeout: 1800 seconds
Cipher Redirect: DISABLED

ClearText Port: 0
Client Auth: DISABLED
SSL Redirect: DISABLED
Non FIPS Ciphers: DISABLED
SNI: ENABLED
OCSP Stapling: DISABLED
HSTS: DISABLED
HSTS IncludeSubDomains: NO
HSTS Max-Age: 0
DTLSv1: ENABLED
Send Close-Notify: YES
Strict Sig-Digest Check: DISABLED
Zero RTT Early Data: DISABLED
DHE Key Exchange With PSK: NO
Tickets Per Authentication Context: 1

DTLS profile name: nsdtls_default_profile

ECC Curve: P_256, P_384, P_224, P_521

1) CertKey Name: ca
CA Certificate  OCSPCheck: OptionalCA_Name Sent
2) CertKey Name: san2 Server Certificate for SNI
3) CertKey Name: san17 Server Certificate for SNI
4) CertKey Name: san13 Server Certificate for SNI


1) Cipher Name: DEFAULT
Description: Default cipher list with encryption strength >= 128bit
Done
<!--NeedCopy-->
```


Konfigurieren von SNI auf einem virtuellen DTLS-Server über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen DTLS-Server und klicken Sie unter Zertifikate auf **Serverzertifikat**.
3. Fügen Sie ein Zertifikat hinzu oder wählen Sie ein Zertifikat aus der Liste aus und wählen Sie **Serverzertifikat für SNI**aus.
4. Klicken Sie in **Erweiterte Einstellungen**auf **SSL-Parameter**.
5. Wählen Sie **SNI Enable**.

Funktionen, die von einem virtuellen DTLS-Server nicht unterstützt werden

Die folgenden Optionen können auf einem virtuellen DTLS-Server nicht aktiviert werden:

- SSLv2
- SSLv3
- TLSv1
- TLSv1.1
- TLSv1.2
- Push verschlüsseln Trigger
- SSLv2Redirect
- SSLv2URL

Parameter, die nicht von einem virtuellen DTLS-Server verwendet werden

Ein virtueller DTLS-Server ignoriert die folgenden SSL-Parameter, auch wenn diese gesetzt sind:

- Verschlüsselung löst Paketanzahl aus
- PUSH-Verschlüsselung Trigger
- SSL-Quantengröße
- Verschlüsselung löst Timeout
- Format für das Einfügen von Betreff-/Ausstellernamen

Konfigurieren Sie Neuverhandlungen für einen DTLS-Dienst

Nicht sichere Neuverhandlungen werden auf einem DTLS-Dienst unterstützt. Sie können die CLI oder die GUI verwenden, um diese Einstellung zu konfigurieren.

Konfigurieren Sie die Neuverhandlung auf einem DTLS-Dienst über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
set ssl parameter -denysslreneg NONSECURE
<!--NeedCopy-->
```

Beispiel:

```
set ssl parameter -denysslreneg NONSECURE


sh ssl parameter
Advanced SSL Parameters
-----------------------
SSL quantum size                                  : 8 KB
Max CRL memory size                               : 256 MB
Strict CA checks                                  : NO
Encryption trigger timeout                        : 100 ms
Send Close-Notify                                 : YES
Encryption trigger packet count                   : 45
Deny SSL Renegotiation                            : NONSECURE
Subject/Issuer Name Insertion Format              : Unicode
OCSP cache size                                   : 10 MB
Push flag                                         : 0x0 (Auto)
Strict Host Header check for SNI enabled SSL sessions : NO
PUSH encryption trigger timeout                   : 1 ms
Crypto Device Disable Limit                       : 0
Global undef action for control policies          : CLIENTAUTH
Global undef action for data policies             : NOOP
Default profile                                   : DISABLED
SSL Insert Space in Certificate Header            : YES
Disable TLS 1.1/1.2 for SSL_BRIDGE secure monitors    : NO
Disable TLS 1.1/1.2 for dynamic and VPN services      : NO
Software Crypto acceleration CPU Threshold        : 0
Hybrid FIPS Mode                                  : DISABLED
Signature and Hash Algorithms supported by TLS1.2     : ALL
SSL Interception Error Learning and Caching       : DISABLED
SSL Interception Maximum Error Cache Memory       : 0 Bytes
Done
<!--NeedCopy-->
```

Konfigurieren Sie die Neuverhandlung auf einem DTLS-Dienst über die GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Wählen Sie einen DTLS-Dienst aus und klicken Sie auf **Bearbeiten**.

3. Navigieren Sie zu **SSL** > **Erweiterte Einstellungen**.
4. Wählen Sie **SSL-Neuverhandlung verweigern**.

Funktionen, die von einem DTLS-Dienst nicht unterstützt werden

Die folgenden Optionen können für einen DTLS-Dienst nicht aktiviert werden:

- SSLv2
- SSLv3
- TLSv1
- TLSv1.1
- TLSv1.2
- Push verschlüsseln Trigger
- SSLv2Redirect
- SSLv2URL
- SNI
- Sichere Neuverhandlung

Parameter, die nicht von einem DTLS-Dienst verwendet werden

Ein DTLS-Dienst ignoriert die folgenden SSL-Parameter, auch wenn diese gesetzt sind:

- Verschlüsselung löst Paketanzahl aus
- PUSH-Verschlüsselung Trigger
- SSL-Quantengröße
- Verschlüsselung löst Timeout
- Format für das Einfügen von Betreff-/Ausstellernamen

> **Hinweis:**
>
> Der Handshake zur Wiederverwendung von SSL-Sitzungen schlägt bei einem DTLS-Dienst fehl, da die Wiederverwendung von Sitzungen derzeit auf DTLS-Diensten nicht unterstützt wird.
>
> **Problemumgehung:** Deaktivieren Sie manuell die Wiederverwendung von Sitzungen für einen DTLS-Dienst. Geben Sie bei der CLI Folgendes ein:
>
> ```
> set ssl service <dtls-service-name> -sessReuse DISABLED
> ```

DTLS-Profil

Ein DTLS-Profil mit den Standardeinstellungen wird automatisch an einen virtuellen DTLS-Server gebunden. Sie können jedoch ein DTLS-Profil mit bestimmten Einstellungen erstellen, die Ihren Anforderungen entsprechen.

Verwenden Sie ein DTLS-Profil mit einem virtuellen DTLS-Server oder einem virtuellen VPN-DTLS-Server. Sie können kein SSL-Profil mit einem virtuellen DTLS-Server verwenden.

> **Hinweis:**
>
> Ändern Sie die Einstellung für die maximale Datensatzgröße im DTLS-Profil basierend auf den Änderungen der MTU und der Paketgröße. Beispielsweise wird die standardmäßige maximale Datensatzgröße von 1459 Byte basierend auf einer IPv4-Adresskopfgröße berechnet. Bei IPv6-Datensätzen ist die Header-Größe größer und daher muss die maximale Datensatzgröße reduziert werden, um die folgenden Kriterien zu erfüllen.

```
max record size + UDP header(8bytes)+ IP header size < MTU
```

Beispiel:

```
Default DTLS profile
    1) Name: nsdtls_default_profile
    PMTU Discovery: DISABLED
    Max Record Size: 1459 bytes
    Max Retry Time: 3 sec
    Hello Verify Request: ENABLED
    Terminate Session: DISABLED
    Max Packet Count: 120 bytes

Custom DTLS profile
    1) Name: ns_dtls_profile_ipv6_1
    PMTU Discovery: DISABLED
    Max Record Size: 1450 bytes
    Max Retry Time: 3 sec
    Hello Verify Request: ENABLED
    Terminate Session: DISABLED
    Max Packet Count: 120 bytes
<!--NeedCopy-->
```

Erstellen eines DTLS-Profils mit der CLI

> **Hinweise:**
>
> Ab Version 13.0 build 79.x lauten die Änderungen am DTLS-Profil wie folgt:
>
> - Der `helloverifyrequest` Parameter ist standardmäßig aktiviert. Die Aktivierung dieses Parameters hilft, das Risiko zu mindern, dass ein Angreifer oder Bots den Netzwerkdurchsatz überfordert, was möglicherweise zu einer Erschöpfung der ausgehenden Bandbreite führt. Das heißt, es hilft, den DTLS DDoS-Verstärkungsangriff zu mildern.

- Der `maxHoldQlen` Parameter wird hinzugefügt. Dieser Parameter definiert die Anzahl der Datagramme, die auf der DTLS-Schicht zur Verarbeitung in die Warteschlange gestellt werden können. Ein hoher Wert des `maxHoldQlen` Parameters kann zu Speicheransammlungen auf der DTLS-Schicht führen, wenn das UDP-Multiplexing hohen UDP-Datenverkehr überträgt. Daher wird empfohlen, einen niedrigeren Wert zu konfigurieren. Der Mindestwert ist 32, der Maximalwert beträgt 65535 und der Standardwert 32.

Ab Version 13.0 build 82.x `maxBadmacIgnorecount` wird ein neuer Parameter im DTLS-Profil eingeführt, um fehlerhafte MAC-Datensätze zu ignorieren, die in einer DTLS-Sitzung empfangen wurden. Mit diesem Parameter werden fehlerhafte Datensätze bis zu dem im Parameter festgelegten Wert ignoriert. Die Appliance beendet die Sitzung erst, nachdem das Limit erreicht ist, und sendet eine Warnung.
Diese Parametereinstellung ist nur wirksam, wenn der `terminateSession` Parameter aktiviert ist.

```
ssl dtlsProfile <name> -maxRetryTime <positive_integer> -
    helloVerifyRequest ( ENABLED | DISABLED ) -terminateSession (ENABLED
     | DISABLED ) -maxHoldQLen <positive_integer> -maxBadmacIgnorecount
    <positive_integer>

helloVerifyRequest
               Send a Hello Verify request to validate the client.
               Possible values: ENABLED, DISABLED
               Default value: ENABLED

terminateSession
               Terminate the session if the message authentication code
                   (MAC)
               of the client and server do not match.
               Possible values: ENABLED, DISABLED
               Default value: DISABLED

maxHoldQLen
               Maximum number of datagrams that can be queued at DTLS
                   layer for
               processing
               Default value: 32
               Minimum value: 32
               Maximum value: 65535

maxBadmacIgnorecount
               Maximum number of bad MAC errors to ignore for a
                   connection prior disconnect. Disabling parameter
```



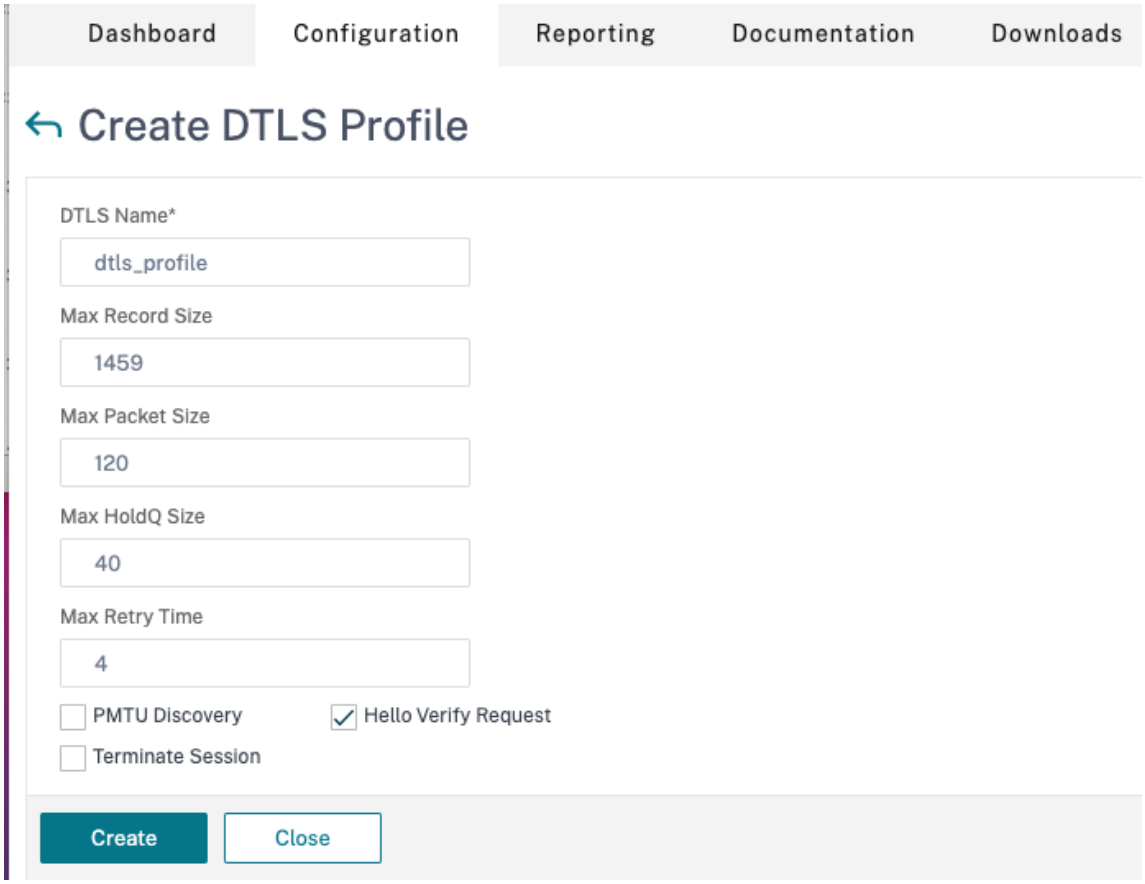
```
                    terminateSession
23 terminates session immediately when bad MAC is detected in the
      connection.
24                Default value: 100
25                Minimum value: 1
26                Maximum value: 65535
27 <!--NeedCopy-->
```

Beispiel:

```
1  > add ssl dtlsprofile dtls_profile -maxRetryTime 4 -helloVerifyRequest
      ENABLED -terminateSession ENABLED -maxHoldQLen 40 -
      maxBadmacIgnorecount 150
2   Done
3  > sh dtlsprofile dtls_profile
4  1)  Name: dtls_profile
5      PMTU Discovery: DISABLED
6      Max Record Size: 1459 bytes
7      Max Retry Time: 4 sec
8      Hello Verify Request: ENABLED
9      Terminate Session: ENABLED
10     Max Packet Count: 120 bytes
11     Max HoldQ Size: 40 datagrams
12     Max bad-MAC Ignore Count: 150
13
14  Done
15 <!--NeedCopy-->
```

Erstellen eines DTLS-Profils mit der GUI

1. Navigieren Sie zu **System > Profile > DTLS-Profile** und klicken Sie auf **Hinzufügen**.
2. Geben **Sie auf der Seite DTLS-Profil erstellen** Werte für die verschiedenen Parameter ein.



3. Klicken Sie auf **Erstellen**.

Beispiel für eine End-to-End-DTLS-Konfiguration

```
enable ns feature SSL LB

add server s1 198.51.100.2

en ns mode usnip

add service svc_dtls s1 DTLS 443

add lb vserver v1 DTLS 10.102.59.244 443

bind ssl vserver v1 -ciphername ALL

add ssl certkey servercert -cert servercert_aia_valid.pem -key
   serverkey_aia.pem

bind ssl vserver v1 -certkeyname servercert
```



```
16
17 bind lb vserver lb1 svc_dtls
18
19 sh lb vserver v1
20
21                     v1 (10.102.59.244:4433) - DTLS     Type: ADDRESS
22                     State: UP
23                     Last state change was at Fri Apr 27 07:00:27 2018
24                     Time since last state change: 0 days, 00:00:04.810
25                     Effective State: UP
26                     Client Idle Timeout: 120 sec
27                     Down state flush: ENABLED
28                     Disable Primary Vserver On Down : DISABLED
29                     Appflow logging: ENABLED
30                     No. of Bound Services :  1 (Total) 0 (Active)
31                     Configured Method: LEASTCONNECTION
32                     Current Method: Round Robin, Reason: A new service
                          is bound         BackupMethod: ROUNDROBIN
33                     Mode: IP
34                     Persistence: NONE
35                     L2Conn: OFF
36                     Skip Persistency: None
37                     Listen Policy: NONE
38                     IcmpResponse: PASSIVE
39                     RHIstate: PASSIVE
40                     New Service Startup Request Rate: 0 PER_SECOND,
                          Increment Interval: 0
41                     Mac mode Retain Vlan: DISABLED
42                     DBS_LB: DISABLED
43                     Process Local: DISABLED
44                     Traffic Domain: 0
45                     TROFS Persistence honored: ENABLED
46                     Retain Connections on Cluster: NO
47
48     1) svc_dtls (10.102.59.190: 4433) - DTLS State: UP  Weight: 1
49 Done
50
51
52 sh ssl vserver v1
53
54                     Advanced SSL configuration for VServer v1:
55                     DH: DISABLED
56                     DH Private-Key Exponent Size Limit: DISABLED
                                  Ephemeral RSA: ENABLED
                                                        Refresh Count: 0
```



```
                      Session Reuse: ENABLED                  Timeout:
                         1800 seconds
                      Cipher Redirect: DISABLED
                      ClearText Port: 0
                      Client Auth: DISABLED
                      SSL Redirect: DISABLED
                      Non FIPS Ciphers: DISABLED
                      SNI: DISABLED
                      OCSP Stapling: DISABLED
                      HSTS: DISABLED
                      HSTS IncludeSubDomains: NO
                      HSTS Max-Age: 0
                      DTLSv1: ENABLED
                      Send Close-Notify: YES
                      Strict Sig-Digest Check: DISABLED
                      Zero RTT Early Data: DISABLED
                      DHE Key Exchange With PSK: NO
                      Tickets Per Authentication Context: 1
                      DTLS profile name: nsdtls_default_profile

                      ECC Curve: P_256, P_384, P_224, P_521

    1)            CertKey Name: servercert               Server
       Certificate

    1)            Cipher Name: DEFAULT
                    Description: Default cipher list with encryption
                       strength >= 128bit

    2)            Cipher Name: ALL
                    Description: All ciphers supported by NetScaler,
                       excluding NULL ciphers
     Done

sh service svc_dtls

                      svc_dtls (10.102.59.190:4433) - DTLS
                      State: UP
                      Last state change was at Fri Apr 27 07:00:26 2018
                      Time since last state change: 0 days, 00:00:22.790
                      Server Name: s1
                      Server ID : None                  Monitor Threshold
                         : 0
                      Max Conn: 0        Max Req: 0           Max
                         Bandwidth: 0 kbits
```



```
                        Use Source IP: NO
                        Client Keepalive(CKA): NO
                        Access Down Service: NO
                        TCP Buffering(TCPB): NO
                        HTTP Compression(CMP): NO
                        Idle timeout: Client: 120 sec           Server: 120
                             sec
                        Client IP: DISABLED
                        Cacheable: NO
                        SC: OFF
                        SP: OFF
                        Down state flush: ENABLED
                        Monitor Connection Close : NONE
                        Appflow logging: ENABLED
                        Process Local: DISABLED
                        Traffic Domain: 0

     1)             Monitor Name: ping-default
                                      State: UP               Weight: 1
                                                          Passive: 0
                                    Probes: 5               Failed [Total
                                       : 0 Current: 0]
                                     Last response: Success - ICMP echo
                                        reply received.
                           Response Time: 2.77 millisec
      Done

sh ssl service svc_dtls

                        Advanced SSL configuration for Back-end SSL Service
                             svc_dtls:
                        DH: DISABLED
                        DH Private-Key Exponent Size Limit: DISABLED
                                  Ephemeral RSA: DISABLED
                        Session Reuse: ENABLED                  Timeout:
                           1800 seconds
                        Cipher Redirect: DISABLED
                        ClearText Port: 0
                        Server Auth: DISABLED
                        SSL Redirect: DISABLED
                        Non FIPS Ciphers: DISABLED
                        SNI: DISABLED
                        OCSP Stapling: DISABLED
                        DTLSv1: ENABLED
                        Send Close-Notify: YES
```



```
                      Strict Sig-Digest Check: DISABLED
                      Zero RTT Early Data: ???
                      DHE Key Exchange With PSK: ???
                      Tickets Per Authentication Context: ???
                      DTLS profile name: nsdtls_default_profile
                      ECC Curve: P_256, P_384, P_224, P_521
     1)            Cipher Name: DEFAULT_BACKEND
                      Description: Default cipher list for Backend SSL
                         session
      Done


> sh dtlsProfile nsdtls_default_profile
1)  Name: nsdtls_default_profile
     PMTU Discovery: DISABLED
     Max Record Size: 1459 bytes
     Max Retry Time: 3 sec
     Hello Verify Request: DISABLED
     Terminate Session: ENABLED
     Max Packet Count: 120 bytes
     Max HoldQ Size: 32 datagrams
     Max bad-MAC Ignore Count: 10

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

DTLS-Unterstützung für IPv6-Adresse

DTLS wird auch mit IPv6-Adressen unterstützt. Um jedoch DTLS mit IPv6-Adressen zu verwenden, muss die maximale Datensatzgröße im DTLS-Profil angepasst werden.

Wenn der Standardwert für die maximale Datensatzgröße verwendet wird, schlägt die anfängliche DTLS-Verbindung möglicherweise fehl. Passen Sie die maximale Datensatzgröße mithilfe eines DTLS-Profils an.

DTLS cipher support

Standardmäßig ist eine DTLS-Verschlüsselungsgruppe gebunden, wenn Sie einen virtuellen DTLS-Server oder -Dienst erstellen. DEFAULT_DTLS enthält die Chiffreen, die eine Front-End-DTLS-Entität unterstützt. Diese Gruppe ist standardmäßig gebunden, wenn Sie einen virtuellen DTLS-Server erstellen. DEFAULT_DTLS_BACKEND enthält die Chiffreen, die für eine Back-End-DTLS-Entität unterstützt werden. Diese Gruppe ist standardmäßig an einen DTLS-Back-End-Dienst gebunden. DTLS_FIPS enthält die Chiffreen, die auf der Citrix ADC FIPS-Plattform unterstützt werden. Diese

Gruppe ist standardmäßig an einen virtuellen DTLS-Server oder -Dienst gebunden, der auf einer FIPS-Plattform erstellt wurde.

Unterstützung von DTLS-Verschlüsselungen auf Citrix ADC VPX-, MPX/SDX- (N2- und N3-basierten) Appliances

Wie liest man die Tabellen:

Sofern keine Build-Nummer angegeben wird, wird eine Verschlüsselungssammlung für alle Builds in einer Version unterstützt.

Beispiel:

- **10.5, 11,0, 11,1, 12,0, 12,1, 13,0**: Alle Builds von 10.5, 11.0, 11.1, 12.0, 12.1, 13.0-Releases.
- **-NA-**: nicht zutreffend.

Unterstützung von DTLS-Verschlüsselungen auf Citrix ADC VPX-, MPX/SDX- (N2- und N3-basierten) Appliances

Name der Verschlüs-selungssuite	Hex-Code	Name der Wireshark Cipher Suite	Unterstützte Builds (Frontend)	Unterstützte Builds (Backend)
TLS1-AES-256-CBC-SHA	0x0035	TLS_RSA_WITH_AI	11.0, 11.1, 12.0, 12.1, 13.0	12.0, 12.1, 13.0
TLS1-AES-128-CBC-SHA	0x002f	TLS_RSA_WITH_AES	11,0, 11,1, 12,0, 12,1, 13,0	12,0, 12,1, 13,0
SSL3-DES-CBC-SHA	0x0009	TLS_RSA_WITH_DI	11,0, 11,1, 12,0, 12,1, 13,0	Nicht zutreffend
SSL3-DES-CBC3-SHA	0x000a	TLS_RSA_WITH_3DE	11,0, 11,1, 12,0, 12,1, 13,0	12,0, 12,1, 13,0
SSL3-EDH-RSA-DES-CBC3-SHA	0x0016	TLS_DHE_RSA_WI	11,0, 11,1, 12,0, 12,1, 13,0	Nicht zutreffend
SSL3-EDH-RSA-DES-CBC-SHA	0x0015	TLS_DHE_RSA_WITH	11,0, 11,1, 12,0, 12,1, 13,0	Nicht zutreffend
TLS1-ECDHE-RSA-AES256-SHA	0xc014	TLS_ECDHE_RSA_	12.1, 13.0	12.1, 13.0
TLS1-ECDHE-RSA-AES128-SHA	0xc013	TLS_ECDHE_RSA_WITH_AES	12.1, 13.0	12.1, 13.0

Name der Verschlüs-selungssuite	Hex-Code	Name der Wireshark Cipher Suite	Unterstützte Builds (Frontend)	Unterstützte Builds (Backend)
TLS1-ECDHE-RSA-DES-CBC3-SHA	0xc012	TLS_ECDHE_RSA_	12.1, 13.0	Nicht zutreffend
TLS1-DHE-RSA-AES-128-CBC-SHA	0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	12.1, 13.0	12.1, 13.0
TLS1-DHE-RSA-AES-256-CBC-SHA	0x0039	TLS_DHE_RSA_WI	12.1, 13.0	12.1, 13.0

Um die Liste der im Front-End unterstützten Standardchiffren anzuzeigen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
show ssl cipher DEFAULT_DTLS
1)    Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035
2)    Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
3)    Cipher Name: TLS1-ECDHE-RSA-AES256-SHA    Priority : 3
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0xc014
4)    Cipher Name: TLS1-ECDHE-RSA-AES128-SHA    Priority : 4
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0xc013
5)    Cipher Name: TLS1-DHE-RSA-AES-256-CBC-SHA    Priority : 5
    Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0039
6)    Cipher Name: TLS1-DHE-RSA-AES-128-CBC-SHA    Priority : 6
    Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x0033
7)    Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA Priority : 7
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0xc012
8)    Cipher Name: SSL3-DES-CBC3-SHA    Priority : 8
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
```



```
          HexCode=0x000a
<!--NeedCopy-->
```

Um die Liste der im Back-End unterstützten Standardchiffren anzuzeigen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
show ssl cipher DEFAULT_DTLS_BACKEND
1)  Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035
2)    Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
3)    Cipher Name: TLS1-ECDHE-RSA-AES256-SHA    Priority : 3
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0xc014
4)    Cipher Name: TLS1-ECDHE-RSA-AES128-SHA    Priority : 4
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0xc013
5)    Cipher Name: TLS1-DHE-RSA-AES-256-CBC-SHA    Priority : 5
    Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0039
6)    Cipher Name: TLS1-DHE-RSA-AES-128-CBC-SHA    Priority : 6
    Description: SSLv3 Kx=DH       Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x0033
7)    Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA Priority : 7
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0xc012
8)    Cipher Name: SSL3-DES-CBC3-SHA    Priority : 8
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0x000a
<!--NeedCopy-->
```

Unterstützung von DTLS-Verschlüsselungen auf der Citrix ADC MPX 14000 FIPS-Plattform

Hinweis: Enlightened Data Support (EDT) wird auf der FIPS-Plattform unterstützt, wenn die folgenden Bedingungen erfüllt sind:

- Der in StoreFront festgelegte UDT-MSS-Wert beträgt 900.
- Die Windows-Clientversion ist 4.12 oder höher.
- DTLS-fähige VDA-Version ist 7.17 oder höher.

- Nicht-DTLS-VDA-Version ist 7.15 LTSR CU3 oder höher.

Wie liest man die Tabellen:

Sofern keine Build-Nummer angegeben wird, wird eine Verschlüsselungssammlung für alle Builds in einer Version unterstützt.

Beispiel:

- **10.5, 11,0, 11,1, 12,0, 12,1, 13,0**: Alle Builds von 10.5, 11.0, 11.1, 12.0, 12.1, 13.0-Releases.
- **-NA-**: nicht zutreffend.

Name der Verschlüsselungssammlung	Hex-Code	Name der Wireshark Cipher Suite	Unterstützte Builds (Frontend)	Unterstützte Builds (Backend)
TLS1-AES-256-CBC-SHA	0x0035	TLS_RSA_WITH_AI	11.0, 11.1, 12.0, 12.1–49.x, 13.0	12.0, 12.1–49.x, 13.0
TLS1-AES-128-CBC-SHA	0x002f	TLS_RSA_WITH_AES	11,0, 11,1, 12,0, 12,1—49,x, 13,0	12,0, 12,1—49,x, 13,0
SSL3-DES-CBC-SHA	0x0009	TLS_RSA_WITH_DI	11,0, 11,1, 12,0, 12,1—49,x, 13,0	Nicht zutreffend
SSL3-DES-CBC3-SHA	0x000a	TLS_RSA_WITH_3DE	11,0, 11,1, 12,0, 12,1—49,x, 13,0	12,0, 12,1—49,x, 13,0
SSL3-EDH-RSA-DES-CBC3-SHA	0x0016	TLS_DHE_RSA_WI	11,0, 11,1, 12,0, 12,1—49,x, 13,0	Nicht zutreffend
SSL3-EDH-RSA-DES-CBC-SHA	0x0015	TLS_DHE_RSA_WITH	11,0, 11,1, 12,0, 12,1—49,x, 13,0	Nicht zutreffend
TLS1-ECDHE-RSA-AES256-SHA	0xc014	TLS_ECDHE_RSA_	12.1–49.x, 13.0	12,1—49,x, 13,0
TLS1-ECDHE-RSA-AES128-SHA	0xc013	TLS_ECDHE_RSA_WI	12,1—49,x, 13,0	12,1—49,x, 13,0
TLS1-ECDHE-RSA-DES-CBC3-SHA	0xc012	TLS_ECDHE_RSA_	12,1—49,x, 13,0	Nicht zutreffend
TLS1-DHE-RSA-AES-128-CBC-SHA	0x0033	TLS_DHE_RSA_WITH	12,1—49,x, 13,0	12,1—49,x, 13,0

Name der Verschlüs-selungssamm-lung	Hex-Code	Name der Wireshark Cipher Suite	Unterstützte Builds (Frontend)	Unterstützte Builds (Backend)
TLS1-DHE-RSA-AES-256-CBC-SHA	0x0039	TLS_DHE_RSA_WI	12,1—49,x, 13,0	12,1—49,x, 13,0

Um die Liste der auf einer Citrix ADC FIPS-Appliance unterstützten Standardverschlüsse anzuzeigen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
show ssl cipher DTLS_FIPS
1)    Cipher Name: TLS1-AES-256-CBC-SHA    Priority : 1
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0x0035
2)    Cipher Name: TLS1-AES-128-CBC-SHA    Priority : 2
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0x002f
3)    Cipher Name: TLS1-ECDHE-RSA-AES256-SHA    Priority : 3
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(256)  Mac=SHA1
       HexCode=0xc014
4)    Cipher Name: TLS1-ECDHE-RSA-AES128-SHA    Priority : 4
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=AES(128)  Mac=SHA1
       HexCode=0xc013
5)    Cipher Name: TLS1-ECDHE-RSA-DES-CBC3-SHA  Priority : 5
    Description: SSLv3 Kx=ECC-DHE  Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0xc012
6)    Cipher Name: SSL3-DES-CBC3-SHA    Priority : 6
    Description: SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
       HexCode=0x000a
<!--NeedCopy-->
```

DTLSv1.2-Verschlüsselungsunterstützung auf den Front-End-VPX-Appliances, MPX/SDX-Appliances (Coleto und N3-basiert)

In der folgenden Tabelle sind die zusätzlichen Verschlüsselungen aufgeführt, die für das DTLSv1.2-Protokoll unterstützt werden.

Name der Verschlüsselungssammlung	Hex-Code	Name der Wireshark Cipher Suite	Unterstützte Builds (VPX-Frontend)	Unterstützte Builds (Coleto-basiert)	Unterstützte Builds (N3-basiert)
TLS1.2-AES256-GCM-SHA384	0x009d	TLS_RSA_WITH	13.0-47.x	13.0–52.x	13.0–58.x
TLS1.2-AES128-GCM-SHA256	0x009c	TLS_RSA_WITH_AES_128_GCM_SHA256	13.0-47.x	13.0–52.x	13.0–58.x
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384	0xc030	TLS_ECDHE_RS	13.0-47.x	13.0–52.x	13.0–58.x
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	0xc02f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	13.0-47.x	13.0–52.x	13.0–58.x
TLS1.2-DHE-RSA-AES256-GCM-SHA384	0x009f	TLS_DHE_RSA_	13.0-47.x	13.0–52.x	13.0–58.x
TLS1.2-DHE-RSA-AES128-GCM-SHA256	0x009e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	13.0-47.x	13.0–52.x	13.0–58.x
TLS1.2-AES-256-SHA256	0x003d	TLS_RSA_WITH	13.0-47.x	13.0–52.x	13.0–58.x
TLS1.2-AES-128-SHA256	0x003c	TLS_RSA_WITH_AES_128_CBC_SHA256	13.0-47.x	13.0–52.x	13.0–58.x
TLS1.2-ECDHE-RSA-AES-256-SHA384	0xc028	TLS_ECDHE_RS	13.0-47.x	13.0–52.x	13.0–58.x
TLS1.2-ECDHE-RSA-AES-128-SHA256	0xc027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	13.0-47.x	13.0–52.x	13.0–58.x

Name der Verschlüsselungssammlung	Hex-Code	Name der Wireshark Cipher Suite	Unterstützte Builds (VPX-Frontend)	Unterstützte Builds (Coleto-basiert)	Unterstützte Builds (N3-basiert)
TLS1.2-DHE-RSA-AES-256-SHA256	0x006b	TLS_DHE_RSA_	13.0-47.x	13.0–52.x	13.0–58.x
TLS1.2-DHE-RSA-AES-128-SHA256	0x0067	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	13.0-47.x	13.0–52.x	13.0–58.x

Unterstützung für Intel Coleto SSL-Chip-basierte Plattformen

October 5, 2021

Die folgenden Geräte werden mit Intel Coleto Chips geliefert:

- MPX 5900
- MPX/SDX 8900
- MPX/SDX 15000
- MPX/SDX 15000-50 G
- MPX/SDX 26000
- MPX/SDX 26000-50S
- MPX/SDX 26000-100 G

Verwenden Sie den Befehl Hardware anzeigen, um festzustellen, ob Ihre Appliance über Coleto (COL) -Chips verfügt.

```
> sh hardware

    Platform: NSMPX-8900 8\*CPU+4\*F1X+6\*E1K+1\*E1K+1*COL 8955 30010
    Manufactured on: 10/18/2016
    CPU: 2100MHZ
    Host Id: 0
    Serial no: CRAC5CR8UA
    Encoded serial no: CRAC5CR8UA
 Done
<!--NeedCopy-->
```


Hinweis: Sichere Neuverhandlungen werden im Back-End für diese Plattformen unterstützt.

Einschränkungen:

- DH 512-Verschlüsselung wird nicht unterstützt.
- SSLv3-Protokoll wird nicht unterstützt.
- Hardwaresicherheitsmodul (HSM) wird nicht unterstützt.
- GnuTLS wird nicht unterstützt.
- ECDSA-Zertifikate mit ECC-Kurven P_224 und P521 werden nicht unterstützt (Nicht unterstützt auf Plattformen mit Cavium-Chips auch.)
- DNSSEC-Abladung wird nicht unterstützt. (DNSSEC wird in Software unterstützt, aber das Auslagern auf Hardware wird nicht unterstützt.)

Anzeigen der SSL-Chip-Auslastung auf Citrix ADC MPX-Plattformen

Ab Release 13.0 Build 47.x können Sie die SSL-Chip-Auslastung auf MPX-Plattformen anzeigen, die mit Intel Coleto-Chips ausgeliefert werden. Diese Funktion wird auf der SDX-Plattform und in einem MPX-Cluster nicht unterstützt.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
> stat ssl


SSL Summary


# SSL cards present                              4

# SSL cards UP                                   4

SSL engine status                                1

SSL sessions (Rate)                            0

SSL Crypto Utilization Asym (%)                  67

SSL Crypto Utilization Symm (%)                  19
<!--NeedCopy-->
```


MPX 14000 FIPS-Geräte

April 25, 2022

> **Wichtig:**
>
> - Die FIPS-Plattform MPX 9700/10500/12500/15500 hat das Lebensende erreicht.
> - Die Konfigurationsschritte für NetScaler MPX 14000 FIPS und NetScaler MPX 9700/10500/12500/15500 FIPS-Appliances sind unterschiedlich. MPX 14000 FIPS-Appliances verwenden keine Firmware v2.2. Ein FIPS-Schlüssel, der auf dem Hardware Security Module (HSM) der MPX 9700-Plattform erstellt wurde, kann nicht an das HSM der MPX 14000-Plattform übertragen werden. Umgekehrt wird auch nicht unterstützt. Wenn Sie jedoch einen RSA-Schlüssel als FIPS-Schlüssel importiert haben, können Sie den RSA-Schlüssel auf die MPX 14000-Plattform kopieren. Importiere es dann als FIPS-Schlüssel. Es werden nur 2048-Bit- und 3072-Bit-Schlüssel unterstützt.
> - Die Firmware-Versionen, die auf der Citrix ADC-Downloadseite unter “Citrix ADC Release 12.1-FIPS” und “Citrix ADC Release 12.1-ndcpp” aufgeführt sind, werden auf den MPX 14000 FIPS- oder SDX 14000 FIPS-Plattformen nicht unterstützt. Diese Plattformen können andere neueste Citrix ADC-Firmware-Versionen verwenden, die auf der Downloadseite verfügbar sind.

Eine FIPS-Appliance ist mit einem manipulationssicheren (manipulationssicheren) kryptografischen Modul - einem Cavium CNN3560-NFBE-G - ausgestattet, das den FIPS 140-2 Level-3-Spezifikationen entspricht (ab Release 12.0 Build 56.x). Die kritischen Sicherheitsparameter (CSPs), hauptsächlich der private Schlüssel des Servers, werden sicher gespeichert und innerhalb des kryptografischen Moduls, auch HSM genannt, gespeichert und generiert. Auf die CSPs wird niemals außerhalb der Grenzen des HSM zugegriffen. Nur der Superuser (`nsroot`) kann Operationen an den im HSM gespeicherten Schlüsseln ausführen.

Bevor Sie eine FIPS-Appliance konfigurieren, müssen Sie den Status der FIPS-Karte überprüfen und dann die Karte initialisieren. Erstellen Sie einen FIPS-Schlüssel und ein Serverzertifikat, und fügen Sie zusätzliche SSL-Konfiguration hinzu.

Informationen zu den unterstützten FIPS-Chiffern finden Sie unter FIPS-zugelassene Algorithmen und Chiffern.

Informationen zum Konfigurieren von FIPS-Appliances in einem HA-Setup finden Sie unter Konfigurieren von FIPS auf Appliances in einem HA-Setup.

Einschränkungen

1. SSL-Neuverhandlungen mit dem SSLv3-Protokoll werden im Backend einer MPX-FIPS-Appliance nicht unterstützt.
2. 1024-Bit- und 4096-Bit-Schlüssel und der Exponentwert von 3 werden nicht unterstützt.
3. Das 4096-Bit-Serverzertifikat wird nicht unterstützt.
4. Das 4096-Bit-Clientzertifikat wird nicht unterstützt (wenn die Clientauthentifizierung auf dem Back-End-Server aktiviert ist).

Konfigurieren des HSM

Bevor Sie das HSM auf einer MPX 14000 FIPS-Appliance konfigurieren, überprüfen Sie den Status Ihrer FIPS-Karte, um sicherzustellen, dass der Treiber korrekt geladen wurde. Initialisieren Sie dann die Karte.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 show fips
2
3 FIPS Card is not configured
4
5 <!--NeedCopy-->
```

Die Meldung “FEHLER: Betrieb nicht zulässig - keine FIPS-Karte im System vorhanden” wird angezeigt, wenn der Treiber nicht korrekt geladen wurde.

Initialisieren der FIPS-Karte

Die Appliance muss dreimal neu gestartet werden, um die FIPS-Karte ordnungsgemäß zu initialisieren.

> **Wichtig**
>
> - Stellen Sie sicher, dass das Verzeichnis `/nsconfig/fips` erfolgreich auf der Appliance erstellt wurde.
> - Speichern Sie die Konfiguration nicht, bevor Sie die Appliance zum dritten Mal neu starten.

Führen Sie die folgenden Schritte aus, um die FIPS-Karte zu initialisieren:

1. Setzen Sie die FIPS-Karte zurück (`reset fips`).
2. Starten Sie das Gerät neu (`reboot`).

3. Legen Sie das Kennwort für den Sicherheitsbeauftragten für die Partitionen 0 und 1 und das Benutzerkennwort für die Partition (`set fips -initHSM Level-2 <soPassword> <oldsoPassword> <userPassword> -hsmLabel NSFIPS`) fest.)

   Note: The set or reset command takes more than 60 seconds to run.

4. Speichern Sie die Konfiguration (`saveconfig`).
5. Stellen Sie sicher, dass der kennwortverschlüsselte Schlüssel für die Hauptpartition (master_pek.key) im Verzeichnis `/nsconfig/fips/` erstellt wurde.
6. Starten Sie das Gerät neu (`reboot`).
7. Stellen Sie sicher, dass der kennwortverschlüsselte Schlüssel für die Standardpartition (default_pek.key) im Verzeichnis `/nsconfig/fips/` erstellt wurde.
8. Starten Sie das Gerät neu (`reboot`).
9. Stellen Sie sicher, dass die FIPS-Karte UP (`show fips`) ist.

Initialisieren Sie die FIPS-Karte über die CLI

Der Befehl `set fips` initialisiert das Hardware Security Module (HSM) auf der FIPS-Karte und legt ein neues Kennwort und ein neues Benutzerkennwort für den Sicherheitsbeauftragten fest.

Vorsicht: Dieser Befehl löscht alle Daten auf der FIPS-Karte. Sie werden aufgefordert, bevor Sie mit der Befehlsausführung fortfahren. Vor und nach dem Ausführen dieses Befehls ist ein Neustart erforderlich, damit die Änderungen übernommen werden. Speichern Sie die Konfiguration, nachdem Sie diesen Befehl ausgeführt haben und bevor Sie die Appliance neu starten.

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
1  reset fips
2
3
4  reboot
5
6  set fips -initHSM Level-2 so12345 so12345 user123 -hsmLabel NSFIPS
7
8  This command will erase all data on the FIPS card. You must save the
       configuration (saveconfig) after executing this command. Do you want
        to continue?(Y/N)y
9
10 <!--NeedCopy-->
```


Hinweis: Die folgende Meldung wird angezeigt, wenn Sie den Befehl `set fips`ausführen:

```
This command will erase all data on the FIPS card. You must save the
   configuration (saveconfig) after executing this command. [Note: On
   MPX/SDX 14xxx FIPS platform, the FIPS security is at Level-3 by
   default, and the -initHSM Level-2 option is internally converted to
   Level-3]  Do you want to continue?(Y/N)y

saveconfig

reboot

reboot

show fips

        FIPS HSM Info:
                 HSM Label              : NetScaler FIPS
                 Initialization         : FIPS-140-2 Level-3
                 HSM Serial Number      : 3.1G1836-ICM000136
                 HSM State              : 2
                 HSM Model              : NITROX-III CNN35XX-NFBE
                 Hardware Version       : 0.0-G
                 Firmware Version       : 1.0
                 Firmware Build         : NFBE-FW-1.0-48
                 Max FIPS Key Memory    : 102235
                 Free FIPS Key Memory   : 102231
                 Total SRAM Memory      : 557396
                 Free SRAM Memory       : 262780
                 Total Crypto Cores     : 63
                 Enabled Crypto Cores   : 63

<!--NeedCopy-->
```

Erstellen eines FIPS-Schlüssels

Sie können einen FIPS-Schlüssel auf Ihrer MPX 14000 FIPS-Einheit erstellen oder einen vorhandenen FIPS-Schlüssel in die Appliance importieren. Die MPX 14000 FIPS-Appliance unterstützt nur 2048-Bit- und 3072-Bit-Schlüssel und einen Exponentenwert von F4 (dessen Wert 65537 ist). Für PEM-Schlüssel ist kein Exponent erforderlich. Stellen Sie sicher, dass der FIPS-Schlüssel korrekt erstellt wurde. Erstellen Sie eine Zertifikatsignieranforderung und ein Serverzertifikat. Fügen Sie abschließend das Zertifikatschlüsselpaar zu Ihrer Appliance hinzu.

Geben Sie den Schlüsseltyp an (RSA oder ECDSA). Geben Sie für ECDSA-Schlüssel nur die Kurve an. Die ECDSA-Schlüsselerstellung mit Kurve P_256 und P_384 wird unterstützt.

> **Hinweis:**
>
> 1024-Bit- und 4096-Bit-Schlüssel und ein Exponentenwert von 3 werden nicht unterstützt.

Erstellen Sie über die CLI einen FIPS-Schlüssel

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
create ssl fipsKey <fipsKeyName> -keytype ( RSA | ECDSA ) [-exponent ( 3 | F4 )] [-modulus <positive_integer>] [-curve ( P_256 | P_384 )]
<!--NeedCopy-->
```

Example1:

```
create fipsKey f1 -keytype RSA -modulus 2048 -exponent F4

show ssl fipskey f1

FIPS Key Name: f1  Key Type: RSA Modulus: 2048   Public Exponent: F4 (Hex: 0x10001)

<!--NeedCopy-->
```

Example2:

```
> create fipskey f2 -keytype ECDSA -curve P_256

> sh fipskey f2
    FIPS Key Name: f2   Key Type: ECDSA Curve: P_256

<!--NeedCopy-->
```

Erstellen eines FIPS-Schlüssels mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL > FIPS**.
2. Klicken Sie im Detailbereich auf der Registerkarte FIPS-Schlüssel auf **Hinzufügen**.

3. Geben Sie im Dialogfeld FIPS-Schlüssel erstellen Werte für die folgenden Parameter an:

   - FIPS-Schlüsselname*—FIPSKeyname
   - Modul*—Modul
   - Exponent*—Exponent

   * Ein erforderlicher Parameter

4. Klicken Sie auf **Erstellen**, und klicken Sie dann auf **Schließen**.
5. Vergewissern Sie sich auf der Registerkarte FIPS-Tasten, dass die für den von Ihnen erstellten FIPS-Schlüssel angezeigten Einstellungen korrekt sind.

Importieren eines FIPS-Schlüssels

Um einen vorhandenen FIPS-Schlüssel mit Ihrer FIPS-Appliance zu verwenden, müssen Sie den FIPS-Schlüssel von der Festplatte der Appliance in das HSM übertragen.

Hinweis: Um Fehler beim Importieren eines FIPS-Schlüssels zu vermeiden, stellen Sie sicher, dass der Name des importierten Schlüssels mit dem ursprünglichen Schlüsselnamen übereinstimmt, als er erstellt wurde.

Importieren eines FIPS-Schlüssels mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import ssl fipsKey <fipsKeyName> -key <string> [-inform <inform>] [-
   wrapKeyName <string>] [-iv<string>] -exponent  F4 ]
<!--NeedCopy-->
```

Beispiel:

```
import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform SIM -exponent F4

import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform PEM

<!--NeedCopy-->
```

Stellen Sie sicher, dass der FIPS-Schlüssel korrekt erstellt oder importiert wurde, indem Sie den`show fipskey` Befehl ausführen.


```
show fipskey
1)      FIPS Key Name: Key-FIPS-2

<!--NeedCopy-->
```

Importieren eines FIPS-Schlüssels mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL > FIPS**.
2. Klicken Sie im Detailbereich auf der Registerkarte FIPS-Schlüssel auf **Importieren**.
3. Wählen Sie im Dialogfeld Als FIPS-Schlüssel importieren die FIPS-Schlüsseldatei aus und legen Sie Werte für die folgenden Parameter fest:
   - FIPS-Schlüsselname*
   - Schlüsseldateiname* — Um die Datei an einem anderen Speicherort als dem Standardwert zu platzieren, geben Sie den vollständigen Pfad an oder klicken Sie auf **Durchsuchen** und navigieren Sie zu einem Speicherort.
   - Exponent*

   * Ein erforderlicher Parameter
4. Klicken Sie auf **Importieren**und dann auf **Schließen**.
5. Vergewissern Sie sich auf der Registerkarte FIPS-Tasten, dass die für den importierten FIPS-Schlüssel angezeigten Einstellungen korrekt sind.

Exportieren eines FIPS-Schlüssels

Citrix empfiehlt, ein Backup eines Schlüssels zu erstellen, der im FIPS HSM erstellt wurde. Wenn ein Schlüssel im HSM gelöscht wird, können Sie den gleichen Schlüssel nicht erneut erstellen, und alle damit verbundenen Zertifikate werden nutzlos gemacht.

Zusätzlich zum Exportieren eines Schlüssels als Backup müssen Sie möglicherweise einen Schlüssel für die Übertragung auf eine andere Appliance exportieren.

Das folgende Verfahren enthält Anweisungen zum Exportieren eines FIPS-Schlüssels in den Ordner `/nsconfig/ssl` auf dem CompactFlash der Appliance und zum Sichern des exportierten Schlüssels mithilfe einer starken asymmetrischen Schlüsselverschlüsselungsmethode.

Exportieren Sie einen FIPS-Schlüssel über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
export ssl fipsKey <fipsKeyName> -key <string>
<!--NeedCopy-->
```

Beispiel:

```
export fipskey Key-FIPS-1 -key Key-FIPS-1.key
<!--NeedCopy-->
```

Exportieren Sie einen FIPS-Schlüssel über die GUI

1. Navigieren Sie zu **Traffic Management > SSL > FIPS**.
2. Klicken Sie im Detailbereich auf der Registerkarte FIPS-Schlüssel auf **Exportieren**.
3. Geben Sie im Dialogfeld FIPS-Schlüssel in eine Datei exportieren Werte für die folgenden Parameter an:
   - FIPS-Schlüsselname*—FIPSKeyname
   - Dateiname* — Schlüssel (Um die Datei an einem anderen als dem Standardspeicherort abzulegen, können Sie entweder den vollständigen Pfad angeben oder auf die Schaltfläche Durchsuchen klicken und zu einem Speicherort navigieren.)

   * Ein erforderlicher Parameter
4. Klicken Sie auf **Exportieren**und dann auf **Schließen**.

Importieren eines externen Schlüssels

Sie können FIPS-Schlüssel übertragen, die im HSM der Citrix ADC-Appliance erstellt wurden. Sie können auch externe private Schlüssel (wie Schlüssel, die mit einem Standard-Citrix ADC, Apache oder IIS erstellt wurden) auf eine Citrix ADC FIPS-Appliance übertragen. Externe Schlüssel werden außerhalb des HSM mithilfe eines Tools wie OpenSSL erstellt. Bevor Sie einen externen Schlüssel in das HSM importieren, kopieren Sie ihn auf das Flash-Laufwerk der Appliance unter `/nsconfig/ssl`.

Auf den MPX 14000 FIPS-Appliances ist der Parameter -exponent im Befehl **`import`** `ssl fipskey` beim Importieren eines externen Schlüssels nicht erforderlich. Der richtige öffentliche Exponent wird automatisch erkannt, wenn der Schlüssel importiert wird, und der Wert des -exponent-Parameters wird ignoriert.

Die Citrix ADC FIPS-Appliance unterstützt keine externen Schlüssel mit einem anderen öffentlichen Exponenten als 3 oder F4.

Sie benötigen keinen Wrap Key auf den MPX 14000 FIPS-Appliances.

Sie können einen externen, verschlüsselten FIPS-Schlüssel nicht direkt in eine MPX 14000 FIPS-Appliance importieren. Um den Schlüssel zu importieren, müssen Sie zuerst den Schlüssel entschlüsseln und dann importieren. Um den Schlüssel zu entschlüsseln, geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
openssl rsa -in <EncryptedKey.key> > <DecryptedKey.out>
<!--NeedCopy-->
```

Hinweis: Wenn Sie einen RSA-Schlüssel als FIPS-Schlüssel importieren, empfiehlt Citrix, den RSA-Schlüssel aus Sicherheitsgründen aus der Appliance zu löschen.

Importieren Sie einen externen Schlüssel als FIPS-Schlüssel über die Befehlszeilenschnittstelle

1. Kopieren Sie den externen Schlüssel auf das Flash-Laufwerk der Appliance.
2. Wenn der Schlüssel im PFX-Format ist, müssen Sie ihn zuerst in das PEM-Format konvertieren. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
convert ssl pkcs12 <output file> -import -pkcs12File <input .pfx
   file name> -password <password>
<!--NeedCopy-->
```

3. Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den externen Schlüssel als FIPS-Schlüssel zu importieren und die Einstellungen zu überprüfen:

```
import ssl fipsKey <fipsKeyName> -key <string> -informPEM
show ssl fipskey<fipsKeyName>
<!--NeedCopy-->
```

Beispiel:

```
convert ssl pkcs12 iis.pem -password 123456 -import -pkcs12File iis.pfx

import fipskey Key-FIPS-2 -key iis.pem -inform PEM

show ssl fipskey key-FIPS-2

```



```
7 FIPS Key Name: Key-FIPS-2 Modulus: 0   Public Exponent: F4 (Hex value 0
     x10001)
8 <!--NeedCopy-->
```

Importieren Sie einen externen Schlüssel als FIPS-Schlüssel über die grafische Benutzeroberfläche

1. Wenn der Schlüssel im PFX-Format ist, müssen Sie ihn zuerst in das PEM-Format konvertieren.
   a) Navigieren Sie zu **Traffic Management > SSL**.
   b) Klicken Sie im Detailbereich unter Tools auf **PKCS importieren #12**.
   c) Stellen Sie im Dialogfeld PKCS12-Datei importieren die folgenden Parameter ein:
      - Name der Ausgabedatei*
      - PKCS12-Dateiname* — Geben Sie den Pfx-Dateinamen an.
      - Kennwort importieren*
      - Kodierungsformat

      *Ein erforderlicher Parameter
2. Navigieren Sie zu **Traffic Management > SSL > FIPS**.
3. Klicken Sie im Detailbereich auf der Registerkarte FIPS-Schlüssel auf **Importieren**.
4. Wählen Sie im Dialogfeld Als FIPS-Schlüssel importieren die PEM-Datei aus und legen Sie Werte für die folgenden Parameter fest:
   - FIPS-Schlüsselname*
   - Schlüsseldateiname* — Um die Datei an einem anderen als dem Standardspeicherort abzulegen, können Sie entweder den vollständigen Pfad angeben oder auf Durchsuchen klicken und zu einem Speicherort navigieren.

   * Ein erforderlicher Parameter
5. Klicken Sie auf **Importieren**und dann auf **Schließen**.
6. Vergewissern Sie sich auf der Registerkarte FIPS-Tasten, dass die für den importierten FIPS-Schlüssel angezeigten Einstellungen korrekt sind.

Konfigurieren von FIPS auf Appliances in einem HA-Setup

Sie können zwei Appliances in einem HA-Paar als FIPS-Appliances konfigurieren.

Voraussetzungen

- Das Hardware Security Module (HSM) muss auf beiden Appliances konfiguriert sein. Weitere Informationen finden Sie unter Konfigurieren des HSM.

- Stellen Sie bei Verwendung der GUI sicher, dass sich die Appliances bereits in einem HA-Setup befinden. Weitere Informationen zum Konfigurieren eines HA-Setups finden Sie unter Hochverfügbarkeit.

> **Hinweis:**
>
> Citrix empfiehlt, das Konfigurationsdienstprogramm (GUI) für dieses Verfahren zu verwenden. Wenn Sie die Befehlszeile (CLI) verwenden, stellen Sie sicher, dass Sie die im Verfahren aufgeführten Schritte sorgfältig ausführen. Das Ändern der Reihenfolge der Schritte oder das Angeben einer falschen Eingabedatei kann zu Inkonsistenzen führen, die einen Neustart der Appliance erfordert. Wenn Sie die CLI verwenden, wird der Befehl `create ssl fipskey` außerdem nicht an den sekundären Knoten weitergegeben. Wenn Sie den Befehl mit denselben Eingabewerten für Modulgröße und Exponent auf zwei verschiedenen FIPS-Appliances ausführen, sind die generierten Schlüssel nicht dieselben. Erstellen Sie den FIPS-Schlüssel auf einem der Knoten und übertragen Sie ihn dann auf den anderen Knoten. Wenn Sie jedoch das Konfigurationsdienstprogramm verwenden, um FIPS-Appliances in einem HA-Setup zu konfigurieren, wird der von Ihnen erstellte FIPS-Schlüssel automatisch an den sekundären Knoten übertragen. Das Verwalten und Übertragen der FIPS-Schlüssel wird als sicheres Informationsmanagement (SIM) bezeichnet.

Wichtig: Das HA-Setup muss innerhalb von sechs Minuten abgeschlossen sein. Wenn das Verfahren bei irgendeinem Schritt fehlschlägt, gehen Sie wie folgt vor:

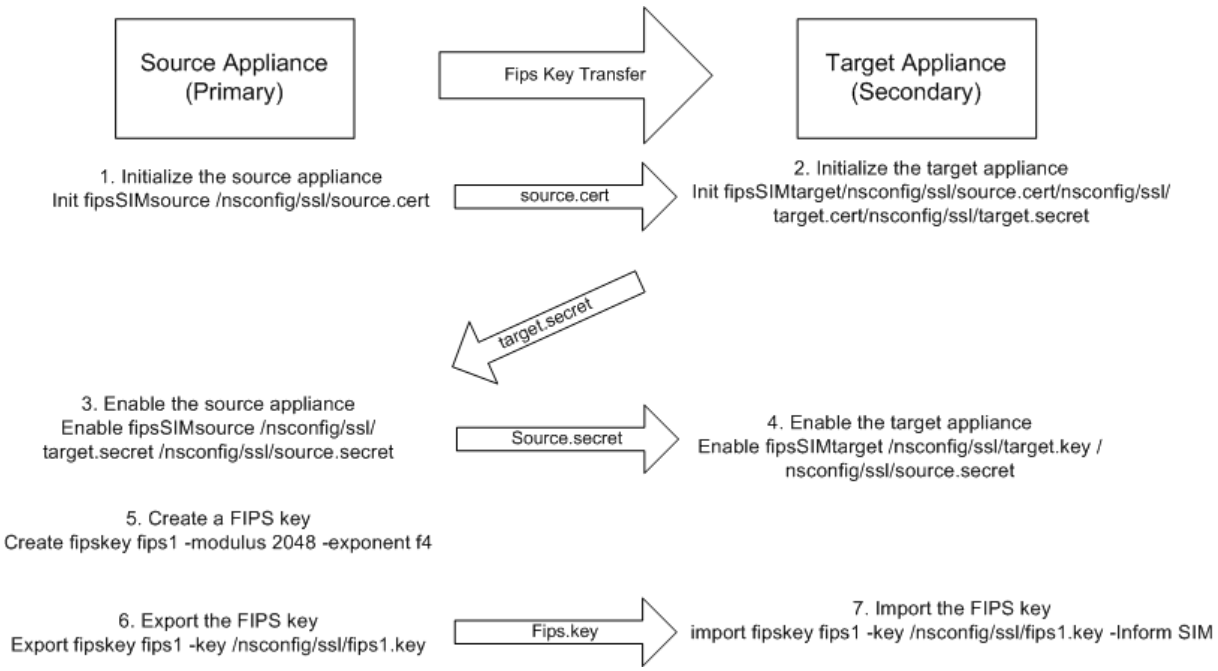
> 1. Starten Sie das Gerät neu oder warten Sie 10 Minuten.
> 2. Entfernen Sie alle durch das Verfahren erstellten Dateien.
> 3. Wiederholen Sie den HA-Setup-Vorgang.
>
> Verwenden Sie keine vorhandenen Dateinamen wieder.

Im folgenden Verfahren ist Appliance A der primäre Knoten und Appliance B der sekundäre Knoten.

Konfigurieren Sie FIPS auf Appliances in einem HA-Setup über die Befehlszeilenschnittstelle

Das folgende Diagramm fasst den Übertragungsprozess auf der CLI zusammen.

Abbildung 1. Übertragen Sie die FIPS-Schlüsselzusammenfassung



1. Öffnen Sie auf **Appliance A** eine SSH-Verbindung zur Appliance mithilfe eines SSH-Clients, z. B. PuTTY.
2. Melden Sie sich mit den Administratoranmeldeinformationen bei der Appliance an.
3. Initialisieren Sie Appliance A als Quell-Appliance. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 init ssl fipsSIMsource <certFile>
2 <!--NeedCopy-->
```

Beispiel:

```
init fipsSIMsource /nsconfig/ssl/nodeA.cert
```

4. Kopieren Sie diese Datei <certFile> auf Appliance B im Ordner /nconfig/ssl.

Beispiel:

```
scp /nsconfig/ssl/nodeA.cert nsroot@198.51.100.10:/nsconfig/ssl
```

5. Öffnen Sie**auf Appliance B**mithilfe eines SSH-Clients wie PuTTY eine SSH-Verbindung zur Appliance.
6. Melden Sie sich mit den Administratoranmeldeinformationen bei der Appliance an.
7. Initialisieren Sie Appliance B als Ziel-Appliance. Geben Sie an der Eingabeaufforderung Folgendes ein:


```
1 init ssl fipsSIMtarget <certFile> <keyVector> <targetSecret>
2 <!--NeedCopy-->
```

Beispiel:

```
init fipsSIMtarget /nsconfig/ssl/nodeA.cert /nsconfig/ssl/nodeB.key /
nsconfig/ssl/nodeB.secret
```

8. Kopieren Sie diese Datei <targetSecret> auf Appliance A.

   Beispiel:

   ```
   scp /nsconfig/ssl/fipslbdal0801b.secret nsroot@198.51.100.20:/nsconfig/
   ssl
   ```

9. Aktivieren Sie**auf Appliance**A Appliance A als Quell-Appliance. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   1 enable ssl fipsSIMSource <targetSecret> <sourceSecret>
   2 <!--NeedCopy-->
   ```

   Beispiel:

   ```
   enable fipsSIMsource /nsconfig/ssl/nodeB.secret /nsconfig/ssl/nodeA.
   secret
   ```

10. Kopieren Sie diese Datei <sourceSecret> auf Appliance B.

    Beispiel:

    ```
    scp /nsconfig/ssl/fipslbdal0801b.secret nsroot@198.51.100.10:/nsconfig/
    ssl
    ```

11. Aktivieren Sie**auf Einheit B**Einheit B als Ziel-Appliance. Geben Sie an der Eingabeaufforderung Folgendes ein:

    ```
    1 enable ssl fipsSIMtarget <keyVector> <sourceSecret>
    2 <!--NeedCopy-->
    ```

    Beispiel:

    ```
    enable fipsSIMtarget /nsconfig/ssl/nodeB.key /nsconfig/ssl/nodeA.secret
    ```

12. Erstellen Sie**auf Appliance A**einen FIPS-Schlüssel, wie unter Erstellen eines FIPS-Schlüsselsbeschrieben.
13. Exportieren Sie den FIPS-Schlüssel auf die Festplatte der Appliance, wie unter Einen FIPS-Schlüssel exportierenbeschrieben.

14. Kopieren Sie den FIPS-Schlüssel auf die Festplatte der sekundären Appliance mithilfe eines sicheren Dateiübertragungsdienstprogramms, z. B. SCP.
15. Importieren Sie**auf Appliance B**den FIPS-Schlüssel von der Festplatte in das HSM der Appliance, wie unter Einen FIPS-Schlüssel importierenbeschrieben.

Konfigurieren Sie FIPS auf Appliances in einem HA-Setup über die grafische Benutzeroberfläche

1. Navigieren Sie auf der Appliance, die als primäre Quell-Appliance konfiguriert werden soll, zu **Traffic Management > SSL > FIPS**.
2. Klicken Sie im Detailbereich auf der Registerkarte FIPS-Info auf **SIM aktivieren**.
3. Geben **Sie im Dialogfeld SIM für HA-Paar aktivieren** im Textfeld **Zertifikatsdateiname** den Dateinamen ein. Der Dateiname muss den Pfad zu dem Speicherort enthalten, an dem das FIPS-Zertifikat auf der Quell-Appliance gespeichert werden muss.
4. Geben Sie im Textfeld **Key Vector Dateiname** den Dateinamen ein. Der Dateiname muss den Pfad zu dem Speicherort enthalten, an dem der FIPS-Schlüsselvektor auf der Quell-Appliance gespeichert werden muss.
5. Geben Sie im Textfeld **Target Secret File Name** den Speicherort für die Speicherung der geheimen Daten auf der Ziel-Appliance ein.
6. Geben Sie im Textfeld **Source Secret File Name** den Speicherort für die Speicherung der geheimen Daten auf der Quell-Appliance ein.
7. Geben Sie unter **Secondary System Login Credential**die Werte für **Benutzername** und **Kennwort ein**.
8. Klicken Sie auf **OK**. Die FIPS-Appliances sind jetzt im HA-Modus konfiguriert.

Hinweis: Erstellen Sie nach der Konfiguration der Appliances in HA einen FIPS-Schlüssel, wie unter Erstellen eines FIPS-Schlüsselsbeschrieben. Der FIPS-Schlüssel wird automatisch von der primären auf die sekundäre Appliance übertragen.

Erstellen einer Zertifikatsignaturanforderung mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName
   <string>) [-keyform ( DER | PEM )  {
 -PEMPassPhrase  }
 ] -countryName <string> -stateName <string> -organizationName<string>
    [-organizationUnitName <string>] [-localityName <string>] [-
    commonName <string>] [-emailAddress <string>] {
 -challengePassword  }
  [-companyName <string>] [-digestMethod ( SHA1 | SHA256 )]
```



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

Beispiel:

```
>create certreq f1.req  - fipsKeyName  f1 -countryName US  -stateName CA
     -organizationName Citrix -companyName Citrix -commonName ctx -
    emailAddress test@example.com

<!--NeedCopy-->
```

Erstellen eines Serverzertifikats über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
    input_filename>] [-keyform ( DER | PEM ) {
 -PEMPassPhrase  }
 ] [-days <positive_integer>] [-certForm ( DER | PEM )] [-CAcert <
     input_filename>] [-CAcertForm ( DER | PEM )] [-CAkey <
     input_filename>][-CAkeyForm ( DER | PEM )] [-CAserial <
     output_filename>]
<!--NeedCopy-->
```

Beispiel:

```
create cert f1.cert f1.req SRVR_CERT -CAcert ns-root.cert -CAkey ns-
    root.key -CAserial ns-root.srl -days 1000

<!--NeedCopy-->
```

Im vorangegangenen Beispiel wird ein Serverzertifikat mithilfe einer lokalen Stammzertifizierungsstelle auf der Appliance erstellt.

Hinzufügen eines Zertifikatschlüsselpaars mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add ssl certKey <certkeyName> (-cert <string> [-password]) [-key <
    string> | -fipsKey <string> | -hsmKey <string>] [-inform <inform>][-
    expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod <
    positive_integer>]] [-bundle ( YES | NO )]
<!--NeedCopy-->
```

Beispiel:

```
add certkey cert1 -cert f1.cert -fipsKey f1

<!--NeedCopy-->
```

Nachdem Sie den FIPS-Schlüssel und das Serverzertifikat erstellt haben, können Sie die generische SSL-Konfiguration hinzufügen. Aktivieren Sie die Funktionen, die für Ihre Bereitstellung erforderlich sind. Fügen Sie Server, Dienste und virtuelle SSL-Server hinzu. Binden Sie das Zertifikatschlüsselpaar und den Dienst an den virtuellen SSL-Server. Speichern Sie die Konfiguration.

```
enable ns feature SSL LB

add server s1 10.217.2.5

add service sr1 s1 HTTP 80

add lb vserver v1 SSL 10.217.2.172 443

bind ssl vserver v1  -certkeyName cert1

bind lb vserver v1 sr1

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

Die Grundkonfiguration Ihrer MPX 14000 FIPS Appliance ist nun abgeschlossen.

Weitere Informationen zum Konfigurieren von sicherem HTTPS erhalten Sie, indem Sie auf FIPS konfigurierenklicken.

Weitere Informationen zum Konfigurieren von sicherem RPC erhalten Sie, wenn Sie zum ersten Mal auf FIPS konfigurierenklicken.

Aktualisieren der Lizenz auf einer MPX 14000 FIPS-Appliance

Jedes Update der Lizenz auf dieser Plattform erfordert zwei Neustarts.

1. Aktualisieren Sie die Lizenz im Ordner `/nsconfig/license`.
2. Starten Sie die Appliance neu.
3. Melden Sie sich bei der Einheit an.
4. Starten Sie das Gerät erneut neu.
   Hinweis: Fügen Sie vor dem zweiten Neustart keine neuen Befehle hinzu, speichern Sie die Konfiguration oder überprüfen Sie den Systemstatus.
5. Melden Sie sich bei der Appliance an und stellen Sie sicher, dass FIPS durch Ausführen des Befehls `show ssl fips` initialisiert wird.

Unterstützung für den Hybrid-FIPS-Modus auf den Plattformen MPX 14000 FIPS und SDX 14000 FIPS

> **Hinweis:**
>
> Diese Funktion wird nur auf der neuen MPX/SDX 14000 FIPS-Plattform unterstützt, die eine primäre FIPS-Karte und eine oder mehrere Sekundärkarten enthält. Es wird nicht auf einer VPX-Plattform oder einer Plattform unterstützt, die nur einen Hardwarekartentyp enthält.

Auf einer FIPS-Plattform erfolgt die asymmetrische und symmetrische Verschlüsselung und Entschlüsselung aus Sicherheitsgründen auf der FIPS-Karte. Sie können jedoch einen Teil dieser Aktivität (asymmetrisch) auf einer FIPS-Karte ausführen und die Massenverschlüsselung und -entschlüsselung (symmetrisch) auf eine andere Karte übertragen, ohne die Sicherheit Ihrer Schlüssel zu beeinträchtigen.

Die neue MPX/SDX 14000 FIPS-Plattform enthält eine Primärkarte und eine oder mehrere Sekundärkarten. Wenn Sie den Hybrid-FIPS-Modus aktivieren, werden die geheimen Entschlüsselungsbefehle vor dem Master auf der Primärkarte ausgeführt, da der private Schlüssel auf dieser Karte gespeichert ist. Die Massenverschlüsselung und -entschlüsselung wird jedoch auf die Sekundärkarte abgeladen. Dieser Offload erhöht den Massenverschlüsselungsdurchsatz auf einer MPX/SDX 14000 FIPS-Plattform im Vergleich zum Nicht-Hybrid-FIPS-Modus und der vorhandenen MPX 9700/10500/12500/15000 FIPS-Plattform erheblich. Durch die Aktivierung des Hybrid-FIPS-Modus wird auch die SSL-Transaktion pro Sekunde auf dieser Plattform verbessert.

> **Hinweise:**
>
> - Der hybride FIPS-Modus ist standardmäßig deaktiviert, um die strengen Zertifizierungsanforderungen zu erfüllen, bei denen die gesamte Kryptoberechnungen in einem FIPS-zertifizierten Modul durchgeführt werden müssen. Aktivieren Sie den Hybridmodus, um die Massenverschlüsselung und -entschlüsselung auf die sekundäre Karte zu übertragen.
> - Auf einer SDX 14000 FIPS-Plattform müssen Sie zuerst der VPX-Instanz einen SSL-Chip

> zuweisen, bevor Sie den Hybridmodus aktivieren.

Aktivieren Sie den Hybrid-FIPS-Modus über die CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set SSL parameter -hybridFIPSMode {
 ENABLED|DISABLED }


Arguments

hybridFIPSMode

When this mode is enabled, system will use additional crypto hardware
   to accelerate symmetric crypto operations.

Possible values: ENABLED, DISABLED

Default value: DISABLED
<!--NeedCopy-->
```

Beispiel:

```
    set SSL parameter -hybridFIPSMode ENABLED
    show SSL parameter
    Advanced SSL Parameters
    -----------------------
    . . . . . .
    Hybrid FIPS Mode    : ENABLED
    . . . . . .

<!--NeedCopy-->
```

Aktivieren Sie den Hybrid-FIPS-Modus über die GUI

1. Navigieren Sie zu **Traffic Management > SSL**.
2. Klicken Sie im Detailbereich unter **Einstellungen**auf **Erweiterte SSL-Einstellungen ändern**.
3. Wählen **Sie im Dialogfeld Erweiterte SSL-Einstellungen ändern** die Option **Hybrid FIPS-Modus**aus.

Einschränkungen:

1. Neuverhandlungen werden nicht unterstützt.
2. Der Befehl `stat ssl parameter` auf einer SDX 14000-Plattform zeigt nicht den korrekten Prozentsatz der sekundären Kartenauslastung an. Es zeigt immer 0,00% Auslastung an.

```
stat ssl

SSL Summary
# SSL cards present 1
# SSL cards UP  1
# Secondary SSL cards present   4
# Secondary SSL cards UP    4
SSL engine status      1
SSL sessions (Rate)     963
Secondary card utilization (%)     0.00
<!--NeedCopy-->
```

SDX 14000 FIPS-Appliances

April 25, 2022

> **Hinweis**
>
> Die Firmware-Versionen, die auf der Citrix ADC-Downloadseite unter “Citrix ADC Release 12.1-FIPS” und “Citrix ADC Release 12.1-NdCPP” aufgeführt sind, werden auf den MPX 14000 FIPS- oder SDX 14000 FIPS-Plattformen nicht unterstützt. Diese Plattformen können andere neueste Citrix ADC-Firmware-Versionen verwenden, die auf der Downloadseite verfügbar sind.

Eine Citrix ADC SDX-Appliance ist eine Multitenant-Plattform, auf der Sie mehrere virtuelle Citrix ADC-Instanzen bereitstellen und verwalten können. Die SDX-Appliance erfüllt Cloud-Computing- und Multitenancy-Anforderungen, indem sie es einem einzelnen Administrator ermöglicht, die Appliance zu konfigurieren und zu verwalten und die Verwaltung jeder gehosteten Instanz an Mandanten zu delegieren.

Eine Citrix ADC SDX 14030/14060/14080 FIPS-Appliance bietet die Funktionen einer SDX-Appliance mit FIPS-Funktionalität. Es ist mit einem manipulationssicheren (manipulationssicheren) kryptographischen Modul — einem Cavium CNN3560-NFBE-G — ausgestattet, das den FIPS 140-2 Level-3-Spezifikationen (ab Version 12.0 Build 56.x) entspricht. Die Critical Security Parameters (CSPs), hauptsächlich der private Schlüssel des Servers, werden sicher gespeichert und innerhalb

des kryptographischen Moduls generiert. Dieses Modul wird auch als das Hardware Security Module (HSM) bezeichnet. Auf die CSPs wird niemals außerhalb der Grenzen des HSM zugegriffen. Nur der Superuser (`nsroot`) kann Operationen an den im HSM gespeicherten Schlüsseln ausführen.

Eine Citrix ADC SDX 14030/14060/14080 FIPS-Appliance enthält ein FIPS HSM-Modul mit 63 Kernen. Das FIPS HSM-Modul kann auf bis zu maximal 32 Partitionen partitioniert werden. Der SDX-Administrator kann jeder Partition dedizierten Schlüsselspeicher, kryptografische Ressourcen und die Anzahl der Krypto-SSL-FIPS-Kerne zuweisen. Schlüssel und Ressourcen, die einer Partition zugewiesen sind, sind dediziert und sicher, und jede andere Partition kann nicht auf sie zugreifen oder sie gemeinsam nutzen.

Die von Ihnen erstellte FIPS-HSM-Partition kann zum Zeitpunkt der Bereitstellung der Instanz oder später durch Bearbeiten der Instanz einer VPX-Instanz zugewiesen oder angehängt werden. Die erstellte und an eine Instanz angehängte FIPS-Partition verhält sich für diese Instanz wie ein virtuelles HSM-Modul.

Den VPX-Instanzen auf einer SDX 14030/14060/14080 FIPS-Einheit wird eine Partition für virtuelle FIPS-Funktionen (VF) zugewiesen, die als isolierte virtuelle FIPS-Karte oder HSM behandelt wird. Daher ähneln die Schritte zum Konfigurieren einer FIPS-Partition innerhalb einer VPX-Instanz den Schritten zum Konfigurieren einer MPX-FIPS-Appliance. Einzelheiten zur Einhaltung der Vorschriften finden Sie in den Sicherheitsrichtlinien auf der Website des U.S. National Institute of Standards and Technology (NIST).

Informationen zum Konfigurieren von FIPS-Appliances in einem Hochverfügbarkeits-Setup finden Sie unter FIPS Appliances in einem Hochverfügbarkeits-Setup

> **Wichtig**
>
> Jeder Schlüssel enthält einen privaten und einen öffentlichen Schlüssel. Infolgedessen nimmt es zwei Schlüsselbereiche ein. Daher ist die maximale Anzahl von Schlüsseln auf einen unter der halben Schlüsselspeichergröße begrenzt.

Die SDX 14000 FIPS-Plattform unterstützt einen hybriden FIPS-Modus. In diesem Modus können Sie einen Teil der Verschlüsselungs- und Entschlüsselungsaktivität auf eine Nicht-FIPS-Karte auslagern. Weitere Informationen finden Sie unter Hybrid-FIPS-Modus.

Einschränkungen

October 5, 2021

1. SSL-Neuverhandlungen mit dem SSLv3-Protokoll werden im Backend einer SDX FIPS-Appliance nicht unterstützt.
2. 1024-Bit- und 4096-Bit-Schlüssel und ein Exponentenwert von 3 werden nicht unterstützt.

3. Backup und Wiederherstellung werden nicht unterstützt.
4. Cluster- und Verwaltungsdomänen werden nicht unterstützt.
5. Sie können nur eine FIPS-Partition an eine Instanz anhängen.
6. Einer Instanz mit einer FIPS-Partition kann nur ein CPU-Kern zugewiesen werden.
7. Sie können einer Instanz entweder eine FIPS-Partition oder einen SSL-Kern zuweisen, aber nicht beides.
8. Das 4096-Bit-Serverzertifikat wird nicht unterstützt.
9. Das 4096-Bit-Clientzertifikat wird nicht unterstützt (wenn die Clientauthentifizierung auf dem Back-End-Server aktiviert ist).

Terminologie

October 5, 2021

Nullstellen: HSM zurücksetzen. Alle Daten auf dem HSM werden gelöscht. Dieser Schritt ist obligatorisch, bevor das HSM initialisiert wird.

Initialisieren: Legen Sie die HSM-Funktionen fest. Die Citrix ADC SDX FIPS-Appliance erfüllt die FIPS-140-2 Level 2. Sie können Partitionen erstellen, nachdem Sie den Chip initialisiert haben.

Größe des Schlüsselspeichers: Anzahl der Schlüssel, die auf einer Partition gespeichert werden können. Es können maximal 102235 Schlüssel angegeben werden. Die maximale Anzahl von Schlüsseln, die gespeichert werden können, ist weniger als die Hälfte der angegebenen Anzahl. Wenn Sie beispielsweise 100 angeben, können Sie nur 49 Schlüssel erstellen, da einer der Schlüssel das RSA-Schlüsselpaar ist, das 2 Schlüsselspeicher verbraucht.

Crypto Core Capacity: Anzahl der Kryptokerne, die einer Partition zugewiesen sind. Es stehen maximal 63 Kerne zur Verfügung.

SSL-Kontext: Anzahl gleichzeitiger SSL-Verbindungen, die auf einer Partition erstellt werden können.

HSM initialisieren

October 5, 2021

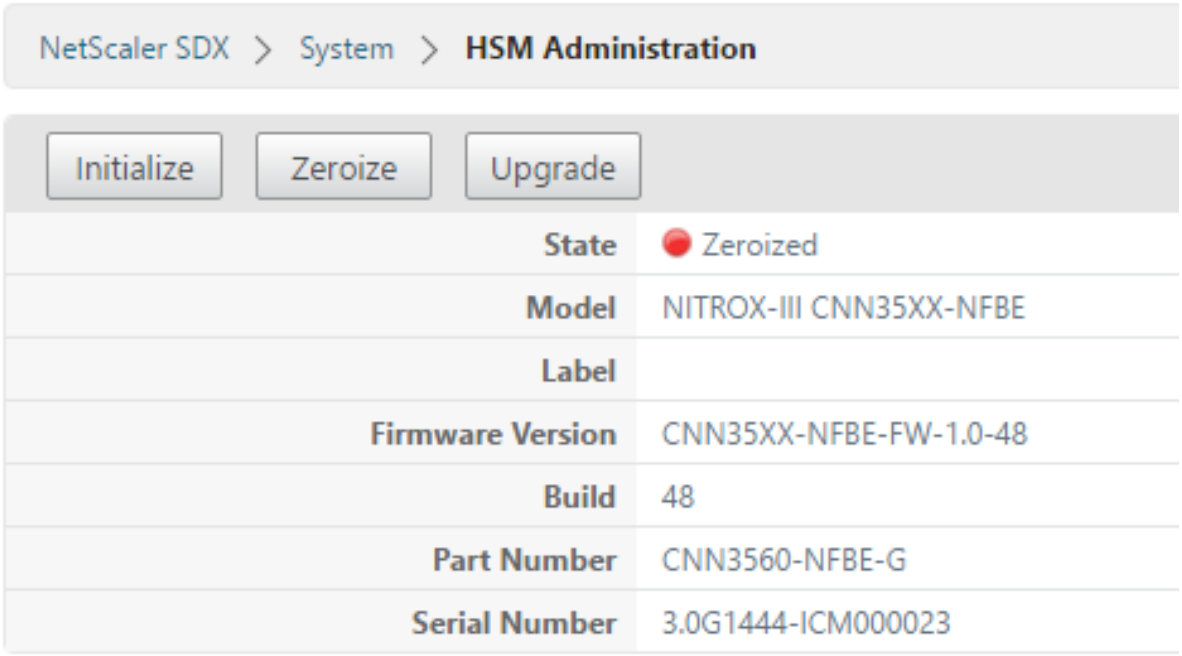
Bevor Sie das HSM initialisieren, müssen Sie es zunächst auf Null setzen.

Nullstellen des HSM mithilfe des Verwaltungsdienstes

1. Öffnen Sie einen Browser, und melden Sie sich bei der Appliance an.

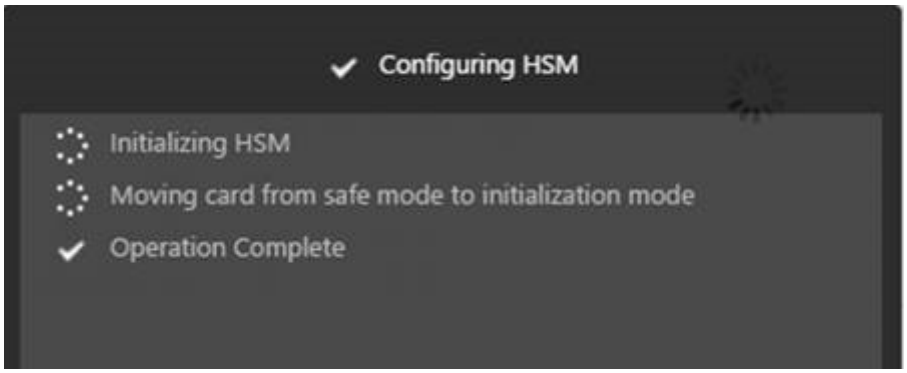
2. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System > HSM-Administration**, und klicken Sie in der Detailebene auf **Zeroize**.

Alle Daten werden vom FIPS-Chip gelöscht und der Status wird als “Zeroized” angezeigt. Alle zuvor erstellten HSM-Partitionen werden gelöscht.

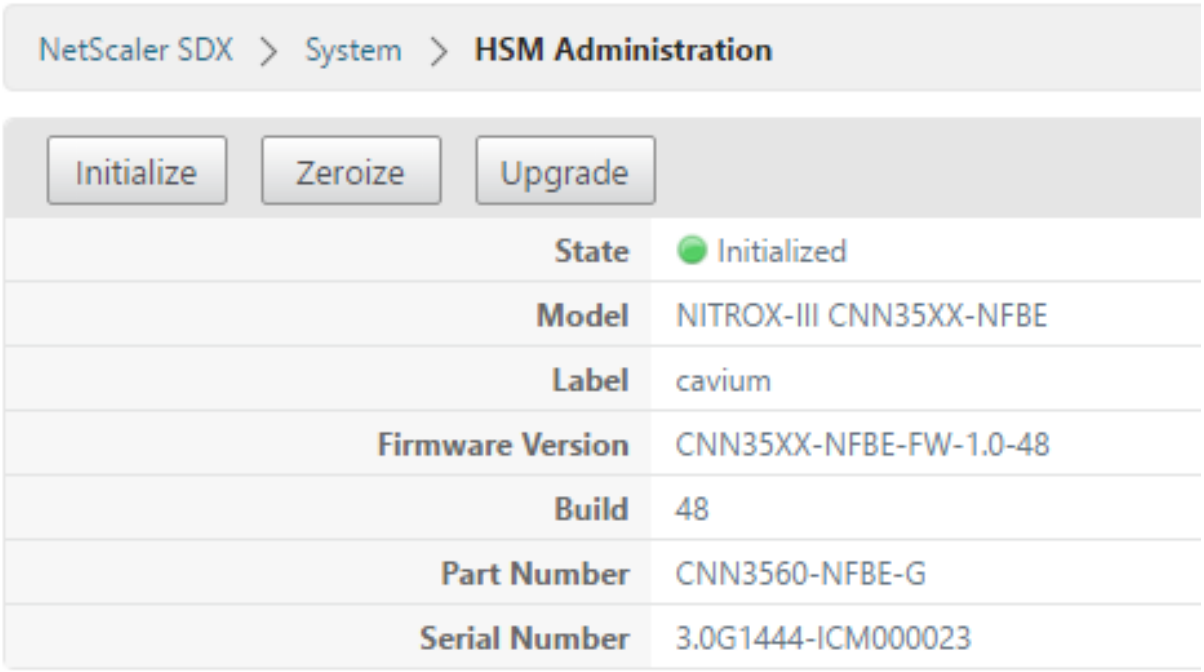


Initialisieren des HSM mit dem Verwaltungsdienst

1. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System > HSM-Administration**, und klicken Sie in der Detailebene auf **Initialisieren**.
2. Geben Sie einen neuen Benutzernamen ein, geben Sie ein Kennwort an, und klicken Sie auf **OK**.



Der Kartenstatus wird als Initialisiert angezeigt.



Partitionen erstellen

October 5, 2021

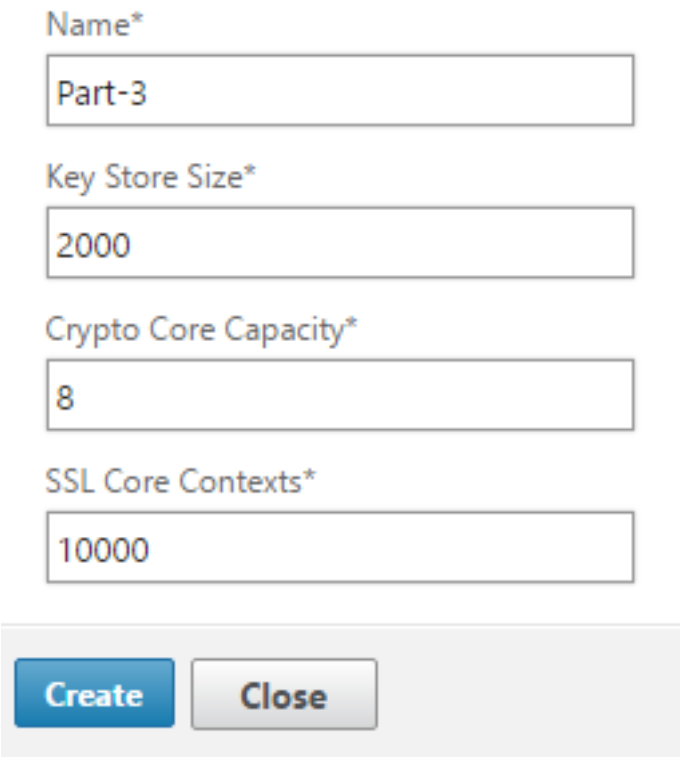
Erstellen Sie Partitionen für verschiedene Mandanten und geben Sie die kryptografischen Ressourcen für jede Partition an. Jeder Instanz wird eine Partition zugewiesen, und eine Partition kann nur einer Instanz zugewiesen werden. Beim Löschen einer Instanz wird die Partition gelöscht, die der Instanz zugewiesen ist. Dadurch werden auch die Partitionsdaten gelöscht und nicht ungesichert oder später zugänglich gelassen. Die Anzahl der Schlüssel und die SSL-Kontextzuweisung hängt von Ihrer Anwendung ab. Informationen zur Anzahl der zuzuweisenden Kerne finden Sie im Citrix ADC Datenblatt.

> **Wichtig**
>
> Nachdem Sie einer HSM-Partition eine Schlüsselspeichergröße und Kerne zugewiesen haben, können Sie sie zur Laufzeit nicht ändern. Trennen Sie zuerst die Partition von der Instanz.

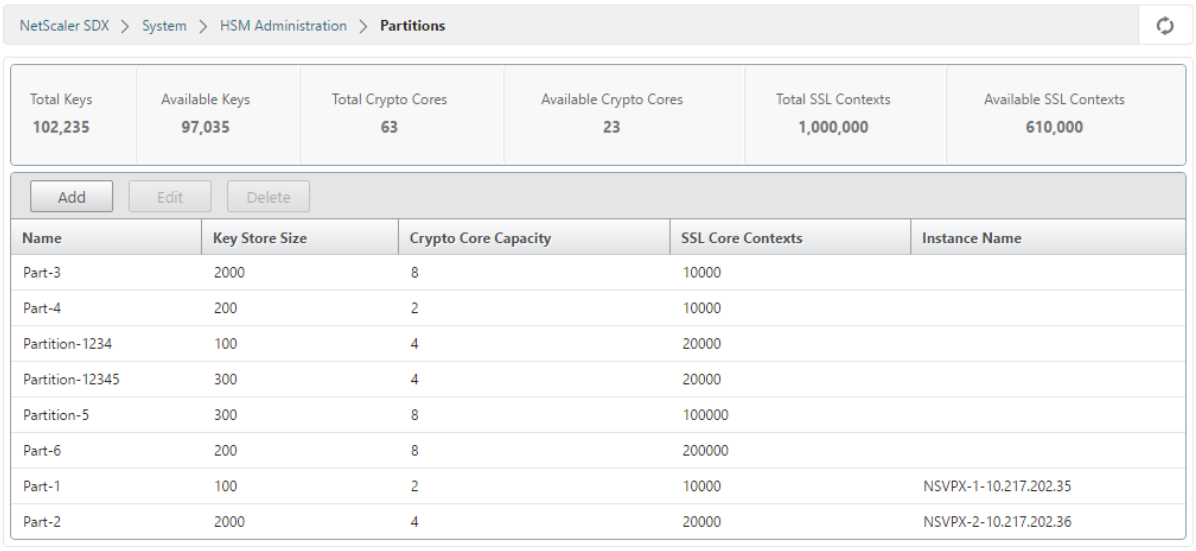
Erstellen einer Partition mithilfe des Verwaltungsdienstes

1. Navigieren Sie auf der Registerkarte Konfiguration zu **System** > **HSM-Verwaltung** > **Partitionen**, und klicken Sie auf der Detailebene auf **Hinzufügen** .

2. Geben Sie einen Namen für die Partition und die Ressourcen an, die dieser Partition zugewiesen werden sollen.
3. Klicken Sie auf **OK**.



Auf der Übersichtsseite werden alle Partitionen angezeigt, die erstellt wurden. Einige Partitionen werden eine Instanz zugewiesen, während einige freie Partitionen sind.



Name	Key Store Size	Crypto Core Capacity	SSL Core Contexts	Instance Name
Part-3	2000	8	10000	
Part-4	200	2	10000	
Partition-1234	100	4	20000	
Partition-12345	300	4	20000	
Partition-5	300	8	100000	
Part-6	200	8	200000	
Part-1	100	2	10000	NSVPX-1-10.217.202.35
Part-2	2000	4	20000	NSVPX-2-10.217.202.36

Bereitstellen einer neuen Instanz oder Ändern einer vorhandenen Instanz und Zuweisen einer Partition

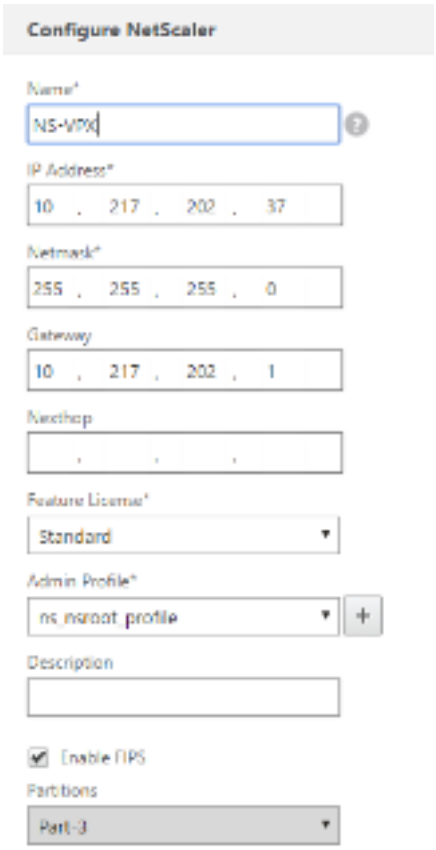
October 5, 2021

Nachdem Sie die Partitionen erstellt haben, müssen Sie sie Instanzen zuweisen.

> **Wichtig:**
>
> - Sie können nur eine FIPS-Partition an eine Instanz anhängen.
> - Einer Instanz mit einer FIPS-Partition kann nur ein CPU-Kern zugewiesen werden.

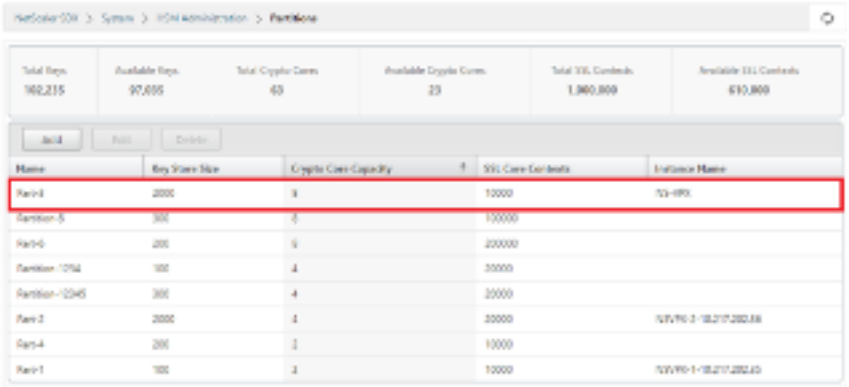
Bereitstellen einer neuen Instanz oder Ändern einer vorhandenen Instanz

1. Navigieren Sie auf der Registerkarte Konfiguration zu **NetScaler** > **Instances**, und fügen Sie eine Instanz hinzu oder ändern Sie sie.
2. Wählen Sie **FIPS aktivieren**, und wählen Sie in der Liste **Partitionen**eine Partition aus, die an diese Instanz angefügt werden soll.



Sie können überprüfen, ob die Partition mit einer Instanz verbunden ist, indem Sie entweder die GUI oder die CLI verwenden.

Navigieren Sie in der GUI zu **System** > **HSM Administration** > **Partitionen**. Der Instanzname, der der Partition zugeordnet ist, wird angezeigt.



Um die Zuweisung einer FIPS-Partition aufzuheben, navigieren Sie zu **NetScaler** > **Instanzen**. Bearbeiten Sie die Instanz, und deaktivieren Sie das Kontrollkästchen **FIPS aktivieren**.

Geben Sie in der Befehlszeile an der Eingabeaufforderung die folgenden Befehle ein:

```
show fips

FIPS Card is not configured
 Done
<!--NeedCopy-->
```

Wenn die folgende Ausgabe angezeigt wird, lesen Sie den Abschnitt zur Fehlerbehebung für das Debuggen.

FEHLER: Betrieb nicht erlaubt - keine FIPS-Karte im System vorhanden

Konfigurieren von HSM für eine Instanz auf einer SDX 14030/14060/14080 FIPS-Appliance

December 3, 2021

Überprüfen Sie zunächst den Status Ihrer FIPS-Karte, um sicherzustellen, dass der Treiber korrekt geladen wurde, und initialisieren Sie dann die Karte.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show fips
```



```
2
3 FIPS Card is not configured
4
5 Done
6 <!--NeedCopy-->
```

Wenn der Treiber nicht korrekt geladen wurde, erscheint die Meldung “FEHLER: Betrieb nicht zulässig - keine FIPS-Karte im System vorhanden”.

Initialisieren der FIPS-Karte

> **Wichtig:**
>
> Stellen Sie sicher, dass das `/nsconfig/fips` Verzeichnis erfolgreich auf der Appliance erstellt wurde.

Speichern Sie die Konfiguration nicht, bevor Sie die Appliance zum dritten Mal neu starten.

Führen Sie die folgenden Schritte aus, um die FIPS-Karte zu initialisieren:

1. Setzen Sie die FIPS-Karte zurück (`reset fips`).
2. Starten Sie das Gerät neu (`reboot`).
3. Legen Sie das Kennwort für den Sicherheitsbeauftragten für die Partitionen 0 und 1 und das Benutzerkennwort für die Partition (`set fips -initHSM Level-2 <soPassword> <oldsoPassword> <userPassword> -hsmLabel NSFIPS`) fest.

   Hinweis: Die Ausführung des Befehls set oder reset dauert mehr als 60 Sekunden.
4. Speichern Sie die Konfiguration (`saveconfig`).
5. Stellen Sie sicher, dass der kennwortverschlüsselte Schlüssel für die Hauptpartition (master_pek.key) im Verzeichnis /nsconfig/fips/ erstellt wurde.
6. Starten Sie das Gerät neu (`reboot`).
7. Stellen Sie sicher, dass die FIPS-Karte UP (`show fips`) ist.

Initialisieren Sie die FIPS-Karte über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

```
1 reset fips
2
3 reboot
4
```



```
set fips -initHSM Level-2 <soPassword> <oldsoPassword> <userPassword> -
    hsmLabel <string>
<!--NeedCopy-->
```

> **Hinweis**: Die folgende Meldung wird angezeigt, wenn Sie den Befehl **set fips** ausführen:

```
This command will erase all data on the FIPS card. You must save the
    configuration (saveconfig) after executing this command. [Note: On
    MPX/SDX 14xxx FIPS platform, the FIPS security is at Level-3 by
    default, and the -initHSM Level-2 option is internally converted to
    Level-3]  Do you want to continue?(Y/N)y

saveconfig

reboot

show fips
<!--NeedCopy-->
```

Beispiel:

```
reset fips

Done

reboot

set fips -initHSM Level-2 so12345 so12345 user123 -hsmLabel NSFIPS

This command will erase all data on the FIPS card. You must save the
    configuration (saveconfig) after executing this command. [Note: On
    MPX/SDX 14xxx FIPS platform, the FIPS security is at Level-3 by
    default, and the -initHSM Level-2 option is internally converted to
    Level-3]  Do you want to continue?(Y/N)y

Done

saveconfig

Done

reboot
```



```
18
19 show fips
20
21     FIPS HSM Info:
22     HSM Label : NSFIPS
23     Initialization : FIPS-140-2 Level-2
24     HSM Serial Number : 3.0G1532-ICM000228
25     HSM State : 2
26     HSM Model : NITROX-III CNN35XX-NFBE
27     Hardware Version : 0.0-G
28     Firmware Version : 1.0
29     Firmware Build : NFBE-FW-1.0-48
30     Max FIPS Key Memory : 1000
31     Free FIPS Key Memory : 1000
32     Total SRAM Memory : 557396
33     Free SRAM Memory : 238088
34     Total Crypto Cores : 4
35     Enabled Crypto Cores : 4
36 Done
37 <!--NeedCopy-->
```

Erstellen eines FIPS-Schlüssels für eine Instanz auf einer SDX 14030/14060/14080 FIPS-Einheit

October 5, 2021

Sie können einen FIPS-Schlüssel auf Ihrer Instanz erstellen oder einen vorhandenen FIPS-Schlüssel in die Instanz importieren. Eine SDX 14030/14060/14080 FIPS-Einheit unterstützt nur 2048-Bit- und 3072-Bit-Schlüssel und einen Exponentenwert von F4. Für PEM-Schlüssel ist kein Exponent erforderlich. Stellen Sie sicher, dass der FIPS-Schlüssel korrekt erstellt wurde. Erstellen Sie eine Zertifikatsignaturanforderung und ein Serverzertifikat. Fügen Sie schließlich der Instanz das Zertifikatschlüsselpaar hinzu.

> **Hinweis:**
>
> 1024-Bit- und 4096-Bit-Schlüssel und ein Exponentenwert von 3 werden nicht unterstützt.

Erstellen eines FIPS-Schlüssels mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
create ssl fipsKey <fipsKeyName> -keytype ( RSA | ECDSA ) [-exponent (3 | F4 )] [-modulus <positive_integer>] [-curve ( P_256 | P_384 )]
<!--NeedCopy-->
```

Beispiel:

```
create fipsKey f1 -keytype RSA -modulus 2048 -exponent F4

Done

show ssl fipskey ddvws

FIPS Key Name: f1  Key Type: RSA Modulus: 2048   Public Exponent: F4 (Hex: 0x10001)

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

Importieren eines FIPS-Schlüssels mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import ssl fipsKey <fipsKeyName> -key <string> [-inform <inform>] [-wrapKeyName <string>] [-iv<string>] [-exponent F4 ]
<!--NeedCopy-->
```

Beispiel:

```
import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform SIM -exponent F4
Done
import fipskey Key-FIPS-2 -key Key-FIPS-2.key -inform PEM
Done
<!--NeedCopy-->
```

Überprüfen Sie, ob der FIPS-Schlüssel korrekt erstellt oder importiert wurde, indem Sie den Befehl **show fipskey** ausführen.


```
show fipskey
1)      FIPS Key Name: Key-FIPS-2
Done
<!--NeedCopy-->
```

Erstellen einer Zertifikatsignaturanforderung mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName
   <string>) [-keyform ( DER | PEM )  {
 -PEMPassPhrase  }
 ] -countryName <string> -stateName <string> -organizationName<string>
    [-organizationUnitName <string>] [-localityName <string>] [-
    commonName <string>] [-emailAddress <string>] {
 -challengePassword  }
  [-companyName <string>] [-digestMethod ( SHA1 | SHA256 )]
<!--NeedCopy-->
```

Beispiel:

```
create certreq f1.req  - fipsKeyName f1 -countryName US -stateName CA -
   organizationName Citrix -companyName Citrix -commonName ctx -
   emailAddress test@example.com`
`Done
<!--NeedCopy-->
```

Erstellen eines Serverzertifikats mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
create ssl cert <certFile> <reqFile> <certType> [-keyFile <
   input_filename>] [-keyform ( DER | PEM ) {
 -PEMPassPhrase  }
 ] [-days <positive_integer>] [-certForm ( DER | PEM )] [-CAcert <
    input_filename>] [-CAcertForm ( DER | PEM )] [-CAkey <
    input_filename>] [-CAkeyForm ( DER | PEM )] [-CAserial <
    output_filename>]
```



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

Beispiel:

```
create cert f1.cert f1.req SRVR_CERT -CAcert ns-root.cert -CAkey ns-
    root.key -CAserial ns-root.srl -days 1000
Done
<!--NeedCopy-->
```

Im vorangegangenen Beispiel wird ein Serverzertifikat mit einer lokalen Stammzertifizierungsstelle auf der Appliance erstellt.

Hinzufügen eines Zertifikatschlüsselpaars mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ssl certKey <certkeyName> (-cert <string> [-password]) [-key <
    string> | -fipsKey <string> | -hsmKey <string>] [-inform <inform>]
    [-expiryMonitor ( ENABLED | DISABLED ) [-notificationPeriod   <
    positive_integer>]] [-bundle ( YES | NO )]
<!--NeedCopy-->
```

Beispiel:

```
add certkey cert1 -cert f1.cert -fipsKey f1
Done
<!--NeedCopy-->
```

Nach dem Erstellen des FIPS-Schlüssels und des Serverzertifikats können Sie die generische SSL-Konfiguration hinzufügen. Aktivieren Sie die Funktionen, die für Ihre Bereitstellung erforderlich sind. Fügen Sie Server, Dienste und virtuelle SSL-Server hinzu. Binden Sie das Zertifikatschlüsselpaar und den Dienst an den virtuellen SSL-Server, und speichern Sie die Konfiguration.

```
enable ns feature SSL LB
Done
add server s1 10.217.2.5
Done
add service sr1 s1 HTTP 80
```



```
Done
add lb vserver v1 SSL 10.217.2.172 443
Done
bind ssl vserver v1  -certkeyName cert1
Done
bind lb vserver v1 sr1
Done
saveconfig
Done
<!--NeedCopy-->
```

Weitere Informationen zum Konfigurieren von sicherem HTTPS und sicherem RPC finden Sie hier.

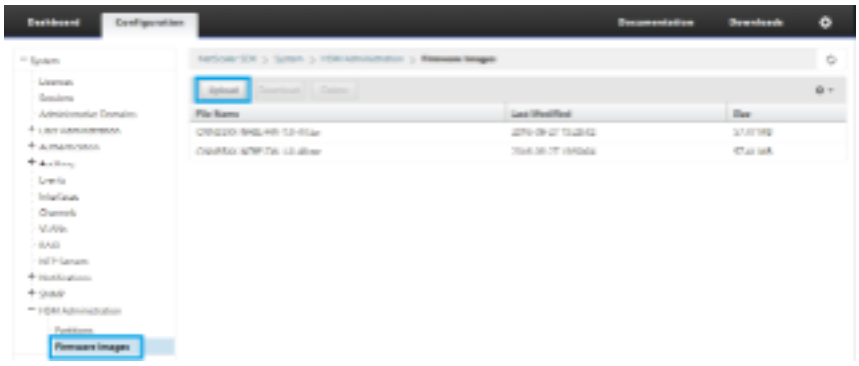
Aktualisieren der FIPS-Firmware auf einer VPX-Instanz

October 5, 2021

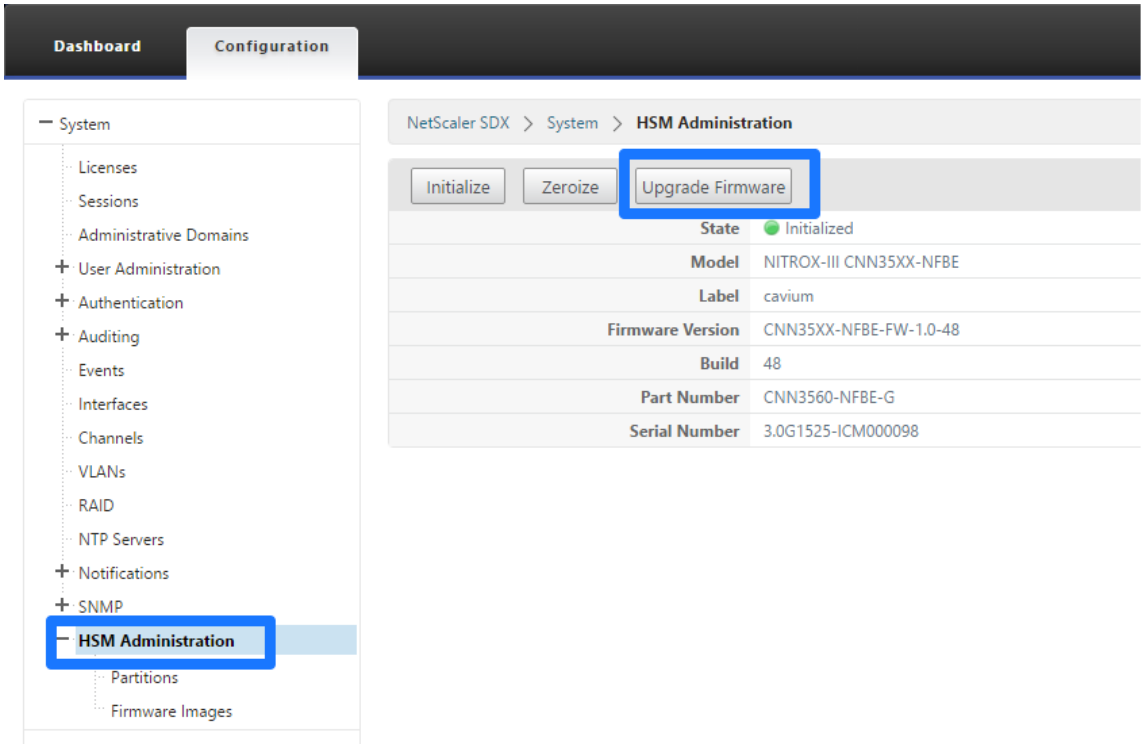
FIPS-Firmware-Updates werden von Zeit zu Zeit veröffentlicht. Laden Sie die neueste Firmware von der Citrix Downloadseite herunter und laden Sie sie auf die Appliance hoch. Der Upgrade-Vorgang kann bis zu 10 Minuten dauern. Die Instanz wird nach dem Upgrade neu gestartet.

Aktualisieren der FIPS-Firmware

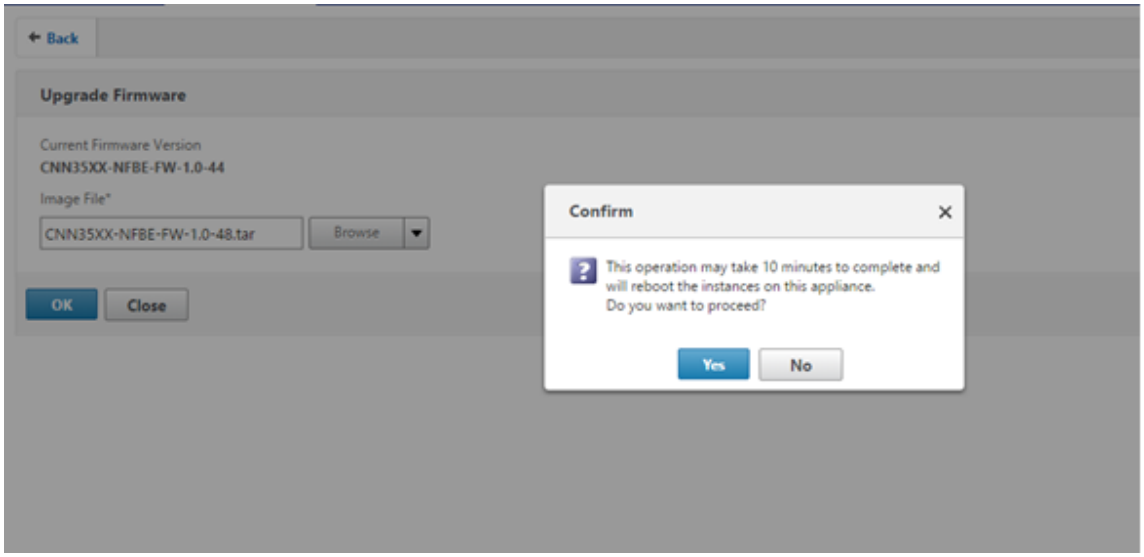
1. Navigieren Sie zu **System > HSM Administration > Firmware-Images**.
2. Wählen Sie **Hochladen** aus.

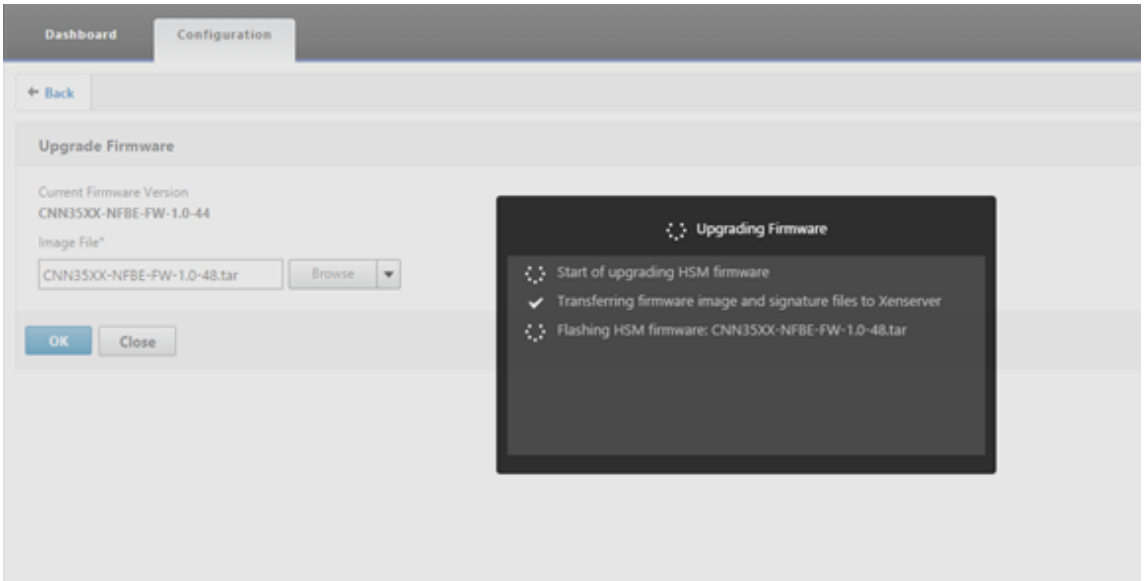


3. Navigieren Sie zu dem Ordner, der das Firmware-Image enthält, und wählen Sie die Datei aus.
4. Navigieren Sie zu **System > HSM Administration** und wählen Sie **Firmware aktualisieren**.



5. Wählen Sie das Firmware-Image aus, auf das Sie aktualisieren möchten, und klicken Sie auf **OK**.





Unterstützung für das NShield Connect Hardwaresicherheitsmodul (HSM)

October 5, 2021

Eine Nicht-FIPS-Citrix ADC Appliance speichert den privaten Schlüssel des Servers auf der Festplatte. Auf einer FIPS-Appliance wird der Schlüssel in einem kryptografischen Modul gespeichert, das als HSM bekannt ist. Das Speichern eines Schlüssels im HSM schützt ihn vor physischen und Software-Angriffen. Darüber hinaus werden die Schlüssel mithilfe spezieller FIPS-zugelassener Chiffre verschlüsselt.

Nur die Citrix ADC MPX 9700/10500/12500/15500 FIPS-Appliances unterstützen eine FIPS-Karte. Unterstützung für FIPS ist nicht auf anderen MPX-Appliances oder auf den SDX- und VPX-Appliances verfügbar. Diese Einschränkung wird durch die Unterstützung eines externen NSM von nShield Connect auf allen Citrix ADC MPX, SDX und VPX Appliances mit Ausnahme der MPX 9700/10500/12500/15500 FIPS-Appliances behoben.

nShield® Connect ist ein externes FIPS-zertifiziertes Network-Attached HSM. Bei einem NShield HSM werden die Schlüssel sicher als Anwendungsschlüssel-Token auf einem Remote-Dateiserver (RFS) gespeichert und können nur innerhalb des nShield HSM rekonstituiert werden.

Wenn Sie bereits ein nShield HSM verwenden, können Sie jetzt einen Citrix ADC verwenden, um die Bereitstellung aller Unternehmens- und Cloud-Services zu optimieren, zu sichern und zu kontrollieren.

Hinweis:

- nShield HSMs entsprechen den FIPS 140-2 Level 3-Spezifikationen, während die MPX FIPS-Geräte den Level-2-Spezifikationen entsprechen.
- Sie können den Trace nicht entschlüsseln, während Sie das nShield HSM verwenden. Nur der `hardserver` kann die Antwort des HSM an die Citrix ADC Appliance lesen, da sie verschlüsselt ist.

Unterstützte Versionen Matrix

Citrix ADC Version	NShield Client-Version	`Hardserver` Version	NShield Firmwareversion
10.5e, 11.0, 11.1, 12.0, 12.1	11.70, 11.72	2.71.2	2.50.16, 2.51.10

Architektur im Überblick

October 5, 2021

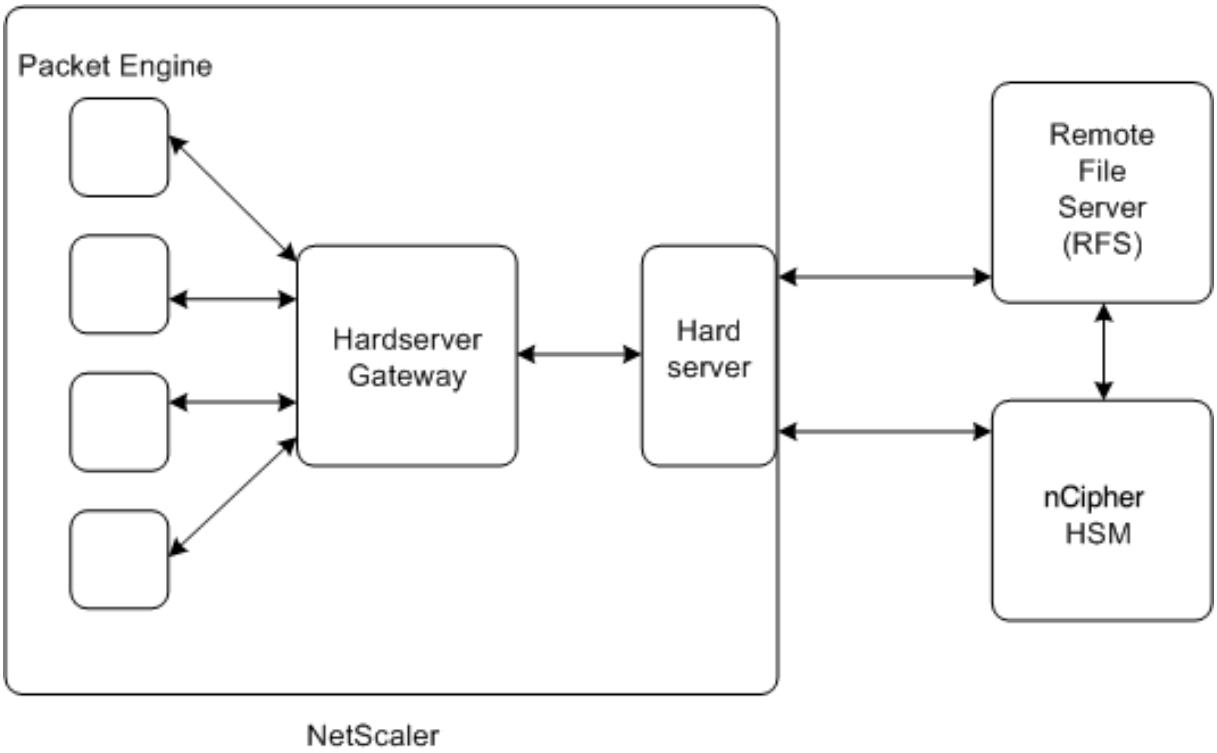
Die drei Entitäten, die Teil einer Citrix ADC-entrust Bereitstellung sind, sind ein Entrust NShield Connect-Modul, ein Remote-Dateiserver (RFS) und ein Citrix ADC.

Das Entrust nShield Connect ist ein an das Netzwerk angeschlossenes Hardwaresicherheitsmodul. Das RFS dient zur Konfiguration des HSM und zum Speichern der verschlüsselten Schlüsseldateien.

`Hardserver`, ein von Entrust bereitgestellter proprietärer Daemon, wird für die Kommunikation zwischen dem Client (ADC), dem Entrust HSM und der RFS verwendet. Es verwendet das IMPATH sichere Kommunikationsprotokoll. Ein Gateway-Daemon, genannt der `Hardserver Gateway`, wird verwendet, um zwischen der Citrix ADC Packet Engine und dem zu kommunizieren `Hardserver`.

Hinweis: Die Begriffe Entrust nShield Connect, Entrust HSM und HSM werden in dieser Dokumentation austauschbar verwendet.

Die folgende Abbildung veranschaulicht die Wechselwirkung zwischen den verschiedenen Komponenten.

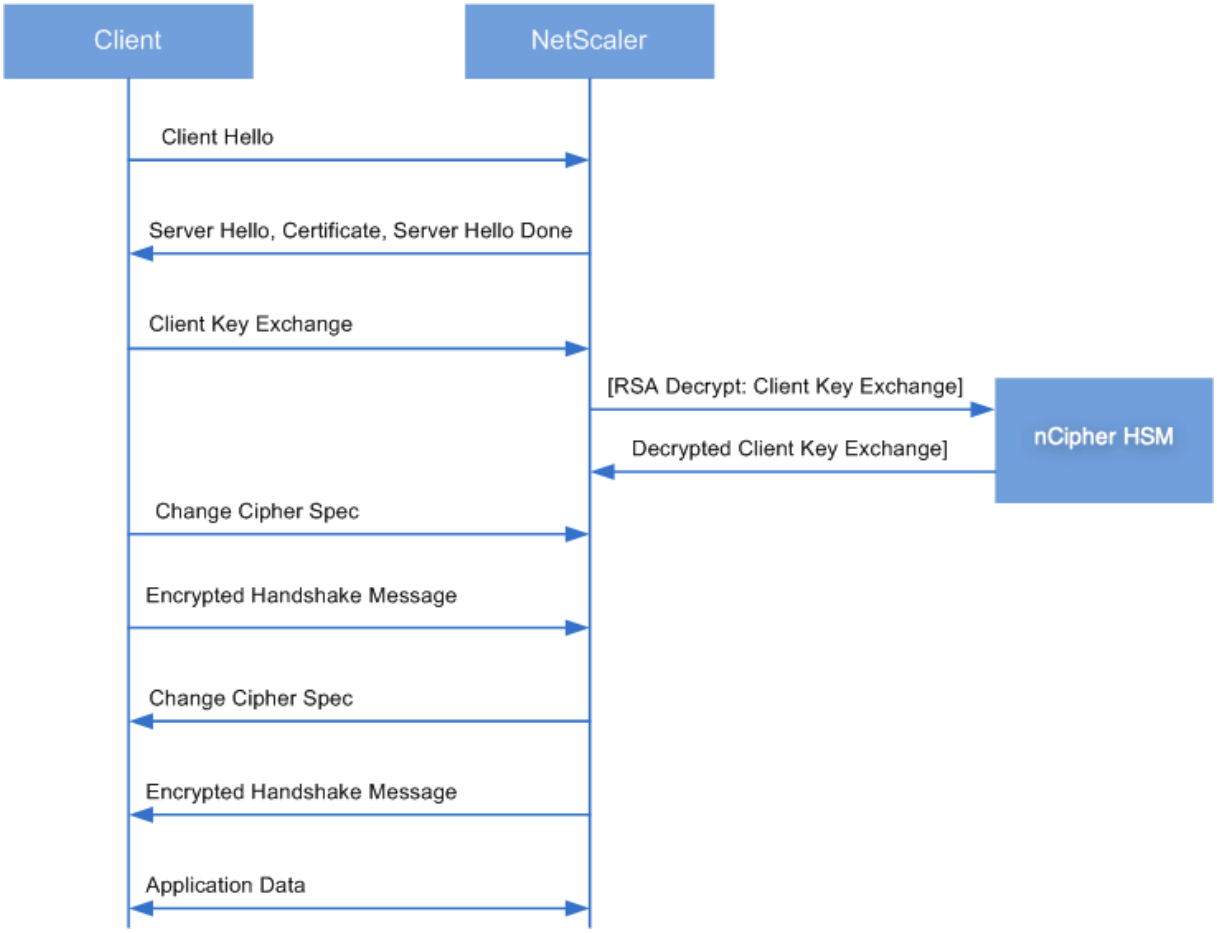


In einer typischen Bereitstellung wird der RFS verwendet, um Schlüssel, die vom HSM generiert werden, sicher zu speichern. Nachdem die Schlüssel generiert wurden, können Sie sie sicher an den ADC übertragen und dann die GUI oder die Befehlszeile verwenden, um die Schlüssel in das HSM zu laden. Ein virtueller Server im ADC entschlüsselt mit Entrust den Clientschlüsselaustausch, um den SSL-Handshake abzuschließen. Danach werden alle SSL-Operationen auf dem ADC durchgeführt.

Hinweis: Die Begriffsschlüssel und Anwendungsschlüssel-Token werden in dieser Dokumentation austauschbar verwendet.

Die folgende Abbildung veranschaulicht den Paketfluss im SSL-Handshake mit dem Entrust HSM.

Abbildung 1. SSL-Handshake-Paket-Flow-Diagramm mit Citrix ADC unter Verwendung von Entrust HSM



Hinweis: Die Kommunikation zwischen dem ADC und dem HSM verwendet ein proprietäres Kommunikationsprotokoll von Entrust, das als IMPATH bezeichnet wird.

Voraussetzungen

October 5, 2021

Bevor Sie ein Entrust nShield Connect mit einem Citrix ADC verwenden können, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Ein Entrust NShield Connect-Gerät ist im Netzwerk installiert, einsatzbereit und für den Citrix ADC zugänglich. Das heißt, die NSIP-Adresse wird als autorisierter Client auf dem HSM hinzugefügt.
- Eine nutzbare Sicherheitswelt existiert. Security World ist eine einzigartige Schlüsselmanagement-Architektur, die von der HSMs Entrust nShield verwendet wird. Es schützt und verwaltet Schlüssel als Anwendungsschlüssel-Token, ermöglicht unbegrenzte Schlüsselkapazität und automatisches Backup und Wiederherstellung von Schlüsseln. Weitere Informationen zum

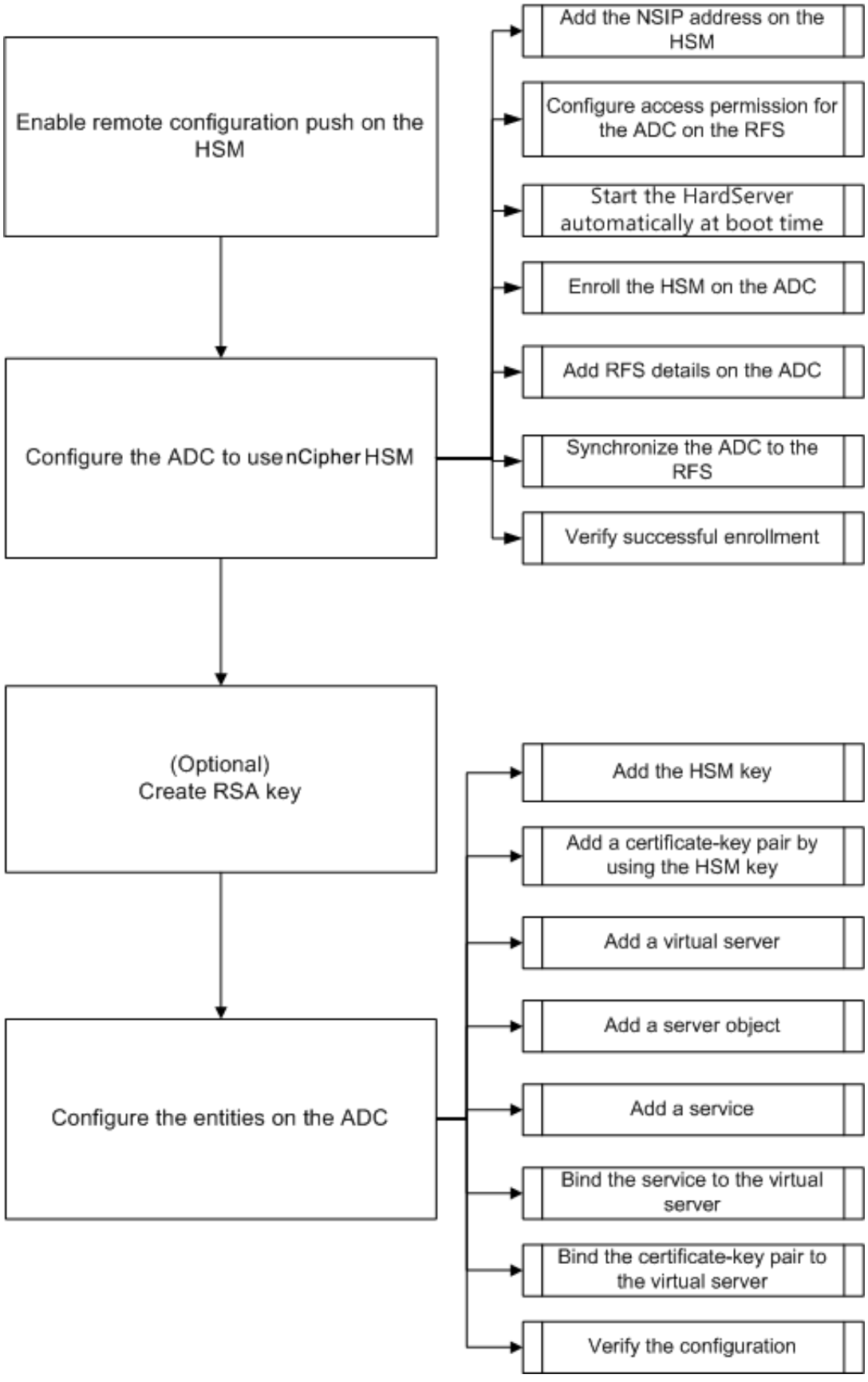
Erstellen einer Security World finden Sie im NShield Connect Quick Start Guide von Entrust. Sie finden den Leitfaden auch in der CD, die mit dem Entrust HSM-Modul geliefert wird, unter CipherTools-Linux-Dev-XX.xx.xx/Document/NShield_Connect_Quick_Start_Guide.pdf.
Hinweis: `Softcard` oder Token/OCS-geschützte Schlüssel werden derzeit auf dem Citrix ADC nicht unterstützt.

- Es stehen Lizenzen zur Verfügung, um die Anzahl der Clients zu unterstützen, die mit dem Entrust HSM verbunden sind. Der ADC und der Remote File Server (RFS) sind Clients des HSM.
- Ein RFS ist im Netzwerk installiert und ist für den Citrix ADC zugänglich.
- Das Entrust NShield Connect-Gerät, der RFS und der Citrix ADC können Verbindungen miteinander über Port 9004 initiieren.
- Sie verwenden NetScaler Version 10.5 Build 52.1115.e oder höher.
- Die Citrix ADC Appliance enthält keine FIPS Cavium-Karte.
  Wichtig: Entrust HSM wird auf den MPX 9700/10500/12500/15500 FIPS-Appliances nicht unterstützt.

Konfigurieren der ADC-Enrust-Integration

October 5, 2021

Das folgende Flussdiagramm zeigt die Aufgaben, die Sie ausführen müssen, um Entrust HSM mit einem Citrix ADC zu verwenden:



Wie im vorherigen Flussdiagramm gezeigt, führen Sie die folgenden Aufgaben aus:

1. Aktivieren Sie Remote Configuration Push auf dem HSM.
2. Konfigurieren Sie den ADC für die Verwendung des Entrust HSM.
    - Fügen Sie die NSIP-Adresse im HSM hinzu.
    - Konfigurieren Sie die Zugriffsberechtigung für den ADC auf dem RFS.
    - Konfigurieren Sie den automatischen Start des `Hardserver` beim Booten.
    - Registrieren Sie den HSM auf dem ADC.
    - Fügen Sie RFS-Details zum ADC hinzu.
    - Synchronisieren Sie den ADC mit dem RFS.
    - Stellen Sie sicher, dass Entrust HSM erfolgreich beim ADC registriert ist.
3. (Optional) Erstellen Sie einen HSM-RSA-Schlüssel.
4. Konfigurieren Sie die Entitäten auf dem Citrix ADC.
    - Fügen Sie den HSM-Schlüssel hinzu.
    - Fügen Sie mit dem HSM-Schlüssel ein Zertifikatschlüsselpaar hinzu.
    - Fügen Sie einen virtuellen Server hinzu.
    - Fügen Sie ein Serverobjekt hinzu.
    - Fügen Sie einen Dienst hinzu.
    - Binden Sie den Dienst an den virtuellen Server.
    - Binden Sie das Zertifikatschlüsselpaar an den virtuellen Server.
    - Überprüfen Sie die Konfiguration.

Konfigurieren Sie das Entrust HSM

Geben Sie die IP-Adresse des RFS im Entrust HSM an, damit es die Konfiguration akzeptiert, die der RFS an ihn schiebt. Verwenden Sie die NShield Connect-Frontplatte des Entrust HSM, um das folgende Verfahren auszuführen.

Geben Sie die IP-Adresse eines Remote-Computers auf dem Entrust HSM an

1. Navigieren Sie zu **Systemkonfiguration > Konfigurationsdateioptionen > Automatisches Push zulassen**.
2. Wählen Sie **ON** aus und geben Sie die IP-Adresse des Computers (RFS) an, von dem die Konfiguration akzeptiert werden soll.

Aktivieren Sie das Pushen der Remotekonfiguration auf dem HSM

Geben Sie die IP-Adresse des RFS im Entrust HSM an, damit es die Konfiguration akzeptiert, die der RFS an ihn schiebt. Verwenden Sie die NShield Connect-Frontplatte des Entrust HSM, um das folgende Verfahren auszuführen.

Geben Sie die IP-Adresse eines Remote-Computers auf dem Entrust HSM an

1. Navigieren Sie zu **Systemkonfiguration > Konfigurationsdateioptionen > Automatisches Push zulassen**.
2. Wählen Sie **ON** aus und geben Sie die IP-Adresse des Computers (RFS) an, von dem die Konfiguration akzeptiert werden soll.

Konfigurieren Sie den ADC für die Verwendung des Entrust HSM

Beispielwerte, die in dieser Dokumentation verwendet werden:

NSIP-Adresse=10.217.2.43

Vertrauen Sie HSM IP-Adresse=10.217.2.112 an

RFS-IP-Adresse=10.217.2.6

Fügen Sie die NSIP-Adresse auf dem HSM hinzu

Normalerweise verwenden Sie die NShield Connect-Frontplatte, um Clients zum HSM hinzuzufügen. Weitere Informationen finden Sie in der NShield Connect Quick Start Guide.

Alternativ können Sie mit dem RFS den ADC als Client zum HSM hinzufügen. Um den ADC hinzuzufügen, müssen Sie die NSIP-Adresse in der HSM-Konfiguration auf dem RFS hinzufügen und die Konfiguration dann an das HSM übertragen. Bevor Sie die Konfiguration pushen können, müssen Sie die elektronische Seriennummer (ESN) des HSM kennen.

Um den ESN Ihres HSM abzurufen, führen Sie den folgenden Befehl auf dem RFS aus:

```
root@ns# /opt/nfast/bin/anonkneti <Entrust HSM IP address>
<!--NeedCopy-->
```

Beispiel:

```
root@ns# /opt/nfast/bin/anonkneti 10.217.2.112
BD17-C807-58D9 5e30a698f7bab3b2068ca90a9488dc4e6c78d822
<!--NeedCopy-->
```

Die ESN-Nummer ist BD17-C807-58D9.

Nachdem Sie die ESN-Nummer haben, verwenden Sie einen Editor wie vi, um die HSM-Konfigurationsdatei auf dem RFS zu bearbeiten.


```
vi /opt/nfast/kmdata/hsm-BD17-C807-58D9/config/config
<!--NeedCopy-->
```

Fügen Sie in `hs_clients` diesem Abschnitt die folgenden Einträge hinzu:

```
# Amount of data in bytes to encrypt with a session key before session
   key# renegotiation, or 0 for unlimitied. (default=1024\*1024\*8b=8Mb
   ).
#  datalimit=INT
addr=10.217.2.43
clientperm=unpriv
keyhash=0000000000000000000000000000000000000000
esn=
timelimit=86400
datalimit=8388608
-----
<!--NeedCopy-->
```

Hinweis: Fügen Sie einen oder mehrere Bindestriche als Trennzeichen ein, um mehrere Einträge im selben Abschnitt hinzuzufügen.

Führen Sie den folgenden Befehl auf dem RFS aus, um die Konfiguration an den HSM zu übertragen:

```
/opt/nfast/bin/cfg-pushnethsm --address=<Entrust HSM IP address> --
   force /opt/nfast/kmdata/hsm-BD17-C807-58D9/config/config
<!--NeedCopy-->
```

Beispiel:

```
/opt/nfast/bin/cfg-pushnethsm --address=10.217.2.112 --force
                /opt/nfast/kmdata/hsm-BD17-C807-58D9/config/config
<!--NeedCopy-->
```

Konfigurieren der Zugriffsberechtigung für den ADC auf dem RFS

Um die Zugriffsberechtigung für den ADC auf dem RFS zu konfigurieren, führen Sie den folgenden Befehl auf dem RFS aus:


```
/opt/nfast/bin/rfs-setup --force -g --write-noauth <NetScaler IP
   address>
<!--NeedCopy-->
```

Beispiel:

```
[root@localhost bin]# /opt/nfast/bin/rfs-setup --force -g --write-
   noauth 10.217.2.43
Adding read-only remote_file_system entries
Ensuring the directory /opt/nfast/kmdata/local exists
Adding new writable remote_file_system entries
Ensuring the directory /opt/nfast/kmdata/local/sync-store exists
Saving the new config file and configuring the hardserver
Done
<!--NeedCopy-->
```

Stellen Sie sicher, dass der ADC sowohl den RFS als auch den Entrust HSM erreichen kann, indem Sie Port 9004 verwenden.

Konfigurieren Sie den automatischen Start des `hardserver` beim Booten

Erstellen Sie eine Datei, und starten Sie die Appliance neu. Wenn Sie jetzt die Appliance neu starten und diese Datei gefunden wird, `Hardserver` wird die automatisch gestartet.

Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
touch /var/opt/nfast/bin/thales_hsm_is_enrolled
<!--NeedCopy-->
```

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

HSM im ADC registrieren

Ändern Sie das Verzeichnis in /var/opt/nfast/bin.

Um HSM-Details zur ADC-Konfiguration hinzuzufügen, führen Sie den folgenden Befehl auf dem ADC aus:

```
nethsmenroll --force <Thales_nShield_Connect_ip_address> $(anonkneti <
Thales_nShield_Connect_ip_address>)
```

Beispiel:

```
root@ns# ./nethsmenroll --force 10.217.2.112 $(anonkneti 10.217.2.112)
OK configuring hardserver's nethsm imports
<!--NeedCopy-->
```

Dieser Schritt fügt die folgenden Einträge nach der Zeile # ntoken_esn=ESN im `nethsm_imports` Abschnitt der Datei /var/opt/nfast/kmdata/config/config hinzu.

```
...
local_module=0
remote_ip=10.217.2.112
remote_port=9004
remote_esn=BD17-C807-58D9
keyhash=5e30a698f7bab3b2068ca90a9488dc4e6c78d822
timelimit=86400
datalimit=8388608
privileged=0
privileged_use_high_port=0
ntoken_esn=
<!--NeedCopy-->
```

Ändern Sie das Verzeichnis in /var/opt/nfast/bin und führen Sie den folgenden Befehl auf dem ADC aus:

```
touch ”thales_hsm_is_enrolled”
<!--NeedCopy-->
```

Hinweis: Um einen HSM zu entfernen, der für den ADC registriert ist, geben Sie Folgendes ein:

```
./nethsmenroll - -remove <NETHSM-IP>
<!--NeedCopy-->
```


Hinzufügen von RFS-Details zum ADC

Um RFS-Details hinzuzufügen, ändern Sie das Verzeichnis in /var/opt/nfast/bin/ und führen Sie dann den folgenden Befehl aus:

```
./rfs-sync --no-authenticate --setup <rfs_ip_address>
<!--NeedCopy-->
```

Beispiel:

```
./rfs-sync --no-authenticate --setup 10.217.2.6
No current RFS synchronization configuration.
Configuration successfully written; new config details:
Using RFS at 10.217.2.6:9004: not authenticating.
<!--NeedCopy-->
```

Dieser Schritt fügt die folgenden Einträge nach der Zeile # local_esn=ESN im `rfs_sync_client` Abschnitt der Datei /var/opt/nfast/kmdata/config/config hinzu.

```
... ...
remote_ip=10.217.2.6
remote_port=9004
use_kneti=no
local_esn=
<!--NeedCopy-->
```

Hinweis: Um einen RFS zu entfernen, der für den ADC registriert ist, geben Sie Folgendes ein:

```
./rfs_sync  - remove
<!--NeedCopy-->
```

Synchronisieren des ADC mit dem RFS

Um alle Dateien zu synchronisieren, ändern Sie das Verzeichnis in /var/opt/nfast/bin und führen Sie dann den folgenden Befehl auf dem ADC aus:


```
./rfs-sync - -update
<!--NeedCopy-->
```

Dieser Befehl ruft alle World-Dateien, Moduldateien und Schlüsseldateien aus dem Verzeichnis /opt/nfast/kmdata/local auf dem RFS ab und legt sie in das Verzeichnis /var/opt/nfast/kmdata/local auf dem ADC. Citrix empfiehlt, die World-Dateien, die Module_xx_xx_xxxx-Dateien, wobei XXXX_XXXX_XXXX der ESN des registrierten HSM ist, und nur die erforderlichen RSA-Schlüssel und Zertifikatdateien manuell zu kopieren.

Stellen Sie sicher, dass der Entrust HSM erfolgreich beim ADC registriert ist

Nachdem Sie den ADC mit dem RFS synchronisiert haben, gehen Sie folgendermaßen vor:

- Stellen Sie sicher, dass der lokale `Hardserver` Betrieb läuft. (Entvertrauen Sie Server läuft).
- Rufen Sie den Status der konfigurierten HSMs ab, und überprüfen Sie, ob die Werte für das Feld n_modules (Anzahl der Module) und die Felder km Info ungleich Null sind.
- Stellen Sie sicher, dass der HSM korrekt registriert ist und vom ADC verwendbar ist (Status 0x2 Useable).
- Laden Sie Tests mit ordnungsgemäß `sigtest` ausführen.

Ändern Sie das Verzeichnis in /var/opt/nfast/bin, und führen Sie an der Shell-Eingabeaufforderung die folgenden Befehle aus:

```
root@ns# ./chkserv root@ns# ./nfkminfo root@ns# ./sigtest
<!--NeedCopy-->
```

Ein Beispiel finden Sie in Anhang .

Erstellen eines HSM-RSA-Schlüssels

Nur RSA-Schlüssel werden als HSM-Schlüssel unterstützt.

Hinweis: Überspringen Sie diesen Schritt, wenn Schlüssel bereits im `/opt/nfast/kmdata/local` Ordner auf dem RFS vorhanden sind.

Erstellen Sie einen RSA-Schlüssel, ein selbstsigniertes Zertifikat und eine Zertifikatsignieranforderung (Certificate Signing Request, CSR). Senden Sie die CSR an eine Zertifizierungsstelle, um ein Serverzertifikat abrufen zu können.

Die folgenden Dateien werden im folgenden Beispiel erstellt:

- RSA-Schlüssel einbetten: key_embed_2ed5428aaeae1e159bdbd63f25292c7113ec2c78

- Selbstsigniertes Zertifikat: beispiel_selfcert
- Zertifikatsignaturanforderung: beispiel_req

Hinweis: Der `generatekey` Befehl wird in der strikten FIPS 140-2 Level 3 Security World unterstützt. Ein Administratorkartenset (ACS) oder ein Operatorkarten-Set (OCS) wird benötigt, um viele Vorgänge zu steuern, einschließlich der Erstellung von Schlüsseln und OCSs. Wenn Sie den `generatekey` Befehl ausführen, werden Sie aufgefordert, eine ACS- oder OCS-Karte einzulegen. Weitere Informationen zur strikten FIPS 140-2 Level 3 Security World finden Sie im NShield Connect Benutzerhandbuch.

Im folgenden Beispiel wird Level 2 Security World verwendet. Im Beispiel sind die Befehle in Fettdruck dargestellt.

Beispiel:

```
[root@localhost bin]# ./generatekey embed
size: Key size? (bits, minimum 1024) [1024] > 2048
OPTIONAL: pubexp: Public exponent for RSA key (hex)? []
>
embedsavefile: Filename to write key to? []
> example
plainname: Key name? [] > example
x509country: Country code? [] > US
x509province: State or province? [] > CA
x509locality: City or locality? [] > Santa Clara
x509org: Organisation? [] > Citrix
x509orgunit: Organisation unit? [] > NS
x509dnscommon: Domain name? [] > www.citrix.com
x509email: Email address? [] > example@citrix.com
nvram: Blob in NVRAM (needs ACS)? (yes/no) [no] >
digest: Digest to sign cert req with? (md5, sha1, sha256, sha384,
   sha512)
  [default sha1] > sha512
key generation parameters:
 operation      Operation to perform              generate
 application    Application                       embed
 verify         Verify security of key            yes
 type           Key type                          RSA
 size           Key size                          2048
 pubexp         Public exponent for RSA key (hex)
 embedsavefile  Filename to write key to          example
 plainname      Key name                          example
 x509country    Country code                      US
 x509province   State or province                 CA
 x509locality   City or locality                  Santa Clara
```



```
 x509org        Organisation                        Citrix
 x509orgunit    Organisation unit                   NS
 x509dnscommon  Domain name                         www.citrix.com
 x509email      Email address                       example@citrix.com
 nvram          Blob in NVRAM (needs ACS)           no
 digest         Digest to sign cert req with        sha512
Key successfully generated.
Path to key: /opt/nfast/kmdata/local/
   key_embed_2ed5428aaeae1e159bdbd63f25292c7113ec2c78
You have new mail in /var/spool/mail/root
<!--NeedCopy-->
```

Ergebnis:

Sie haben eine CSR (example_req), ein selbstsigniertes Zertifikat (example_selfcert) und eine Anwendungsschlüssel-Token im Einbettungsformat (/opt/nfast/kmdata/local/key_embed_2ed5428aaeae1e159bd erstellt.

Da der ADC Schlüssel nur im einfachen Format unterstützt, müssen Sie den Einbettungsschlüssel in einen einfachen Schlüssel konvertieren.

Um den Einbettungsschlüssel in einen einfachen Schlüssel zu konvertieren, führen Sie den folgenden Befehl auf dem RFS aus:

```
[root@localhost bin]# ./generatekey -r simple
from-application: Source application? (embed, simple) [embed] > embed
from-ident: Source key identifier? (
   c6410ca00af7e394157518cb53b2db46ff18ce29,
                                    2
                                       ed5428aaeae1e159bdbd63f25292c7113ec2c78
                                       )
  [default c6410ca00af7e394157518cb53b2db46ff18ce29]
> 2ed5428aaeae1e159bdbd63f25292c7113ec2c78
ident: Key identifier? [] > examplersa2048key
plainname: Key name? [] > examplersa2048key
key generation parameters:
 operation         Operation to perform    retarget
 application       Application             simple
 verify            Verify security of key  yes
 from-application  Source application      embed
 from-ident        Source key identifier   2
    ed5428aaeae1e159bdbd63f25292c7113ec2c78
 ident             Key identifier          examplersa2048key
 plainname         Key name                examplersa2048key
```



```
Key successfully retargetted.
Path to key: /opt/nfast/kmdata/local/key_simple_examplersa2048key
<!--NeedCopy-->
```

> **Wichtig:**
>
> Wenn Sie zur Eingabe der Quellschlüsselkennung aufgefordert werden, geben Sie **2ed5428aaeae1e159bdbd63f** als Einbettungsschlüssel ein.

Ergebnis:

Ein Schlüssel mit dem Präfix key_simple (z.B. key_simple_examplersa2048key) wird erstellt.

Hinweis: examplersa2048key ist der Schlüsselbezeichner (Ident) und wird im ADC als HSM-Schlüsselname bezeichnet. Eine Schlüsselkennung ist eindeutig. Alle einfachen Dateien haben das Präfix key_simple.

Konfigurieren Sie die Entitäten im ADC

Bevor der ADC Datenverkehr verarbeiten kann, müssen Sie Folgendes tun:

1. Funktionen aktivieren.
2. Fügen Sie eine Subnetz-IP (SNIP) -Adresse hinzu.
3. Fügen Sie dem ADC den HSM-Schlüssel hinzu.
4. Fügen Sie mit dem HSM-Schlüssel ein Zertifikatschlüsselpaar hinzu.
5. Fügen Sie einen virtuellen Server hinzu.
6. Fügen Sie ein Serverobjekt hinzu.
7. Fügen Sie einen Dienst hinzu.
8. Binden Sie den Dienst an den virtuellen Server.
9. Binden Sie das Zertifikatschlüsselpaar an den virtuellen Server.
10. Überprüfen Sie die Konfiguration.

Aktivieren von Funktionen auf dem ADC

Lizenzen müssen auf dem ADC vorhanden sein, bevor Sie ein Feature aktivieren können.

Aktivieren eines Features mit der CLI

Führen Sie an der Eingabeaufforderung die folgenden Befehle aus:

```
enable feature lb
enable feature ssl
<!--NeedCopy-->
```


Aktivieren eines Features mit der GUI

Navigieren Sie zu **System** > **Einstellungen** und wählen Sie in der Gruppe **Modi und Funktionen** die Option **Basisfunktionen konfigurieren**aus und wählen Sie dann **SSL-Offloading**aus.

Hinzufügen einer Subnetz-IP-Adresse

Weitere Informationen zu Subnetz-IP-Adressen finden Sie unter Konfigurieren von Subnetz-IP-Adressen.

Fügen Sie eine SNIP-Adresse hinzu und überprüfen Sie die Konfiguration mit der CLI

Führen Sie an der Eingabeaufforderung die folgenden Befehle aus:

```
add ns ip <IPAddress> <netmask> -type SNIP
show ns ip
<!--NeedCopy-->
```

Beispiel:

```
add ns ip 192.168.17.253 255.255.248.0 -type SNIP
Done
show ns ip
        Ipaddress        Traffic Domain  Type             Mode     Arp
                 Icmp     Vserver  State
        ---------        --------------  ----             ----     ---
                 ----     -------  ------
1)      192.168.17.251   0               NetScaler IP     Active
   Enabled  Enabled  NA       Enabled
2)      192.168.17.252   0               VIP              Active
   Enabled  Enabled  Enabled  Enabled
3)      192.168.17.253   0               SNIP              Active
   Enabled  Enabled  NA       Enabled
 Done
<!--NeedCopy-->
```

Fügen Sie eine SNIP-Adresse hinzu und überprüfen Sie die Konfiguration mit der GUI

Navigieren Sie zu **System > Netzwerk > IPs**, fügen Sie eine IP-Adresse hinzu und wählen Sie den **IP-Typ als Subnetz-IP**aus.

HSM-Schlüssel und -Zertifikat in den ADC kopieren

Verwenden Sie ein Dienstprogramm zur sicheren Dateiübertragung, um den Schlüssel (key_simple_examplersa204
sicher in den `/var/opt/nfast/kmdata/local` Ordner und das Zertifikat (example_selfcert) in den
`/nsconfig/ssl` Ordner auf dem ADC zu kopieren.

Fügen Sie den Schlüssel auf dem ADC hinzu

Alle Schlüssel haben ein Schlüssel-einfaches Präfix. Wenn Sie den Schlüssel zum ADC hinzufügen, verwenden Sie die Ident als HSM-Schlüsselname. Wenn der hinzugefügte Schlüssel beispielsweise KEY_Simple_XXXX lautet, lautet der HSM-Schlüsselname XXXX.

Wichtig:

- Der HSM-Schlüsselname muss mit der Ident übereinstimmen, die Sie beim Konvertieren eines Einbettungsschlüssels in ein einfaches Schlüsselformat angegeben haben.
- Die Schlüssel müssen im `/var/opt/nfast/kmdata/local/` Verzeichnis des ADC vorhanden sein.

Hinzufügen eines HSM-Schlüssels mit der CLI

Führen Sie an der Shell-Eingabeaufforderung den folgenden Befehl aus:

```
1 add ssl hsmKey <hsmKeyName> -key <string>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add ssl hsmKey examplersa2048key  - key key_simple_examplersa2048key
2 Done
3 <!--NeedCopy-->
```

Hinzufügen eines HSM-Schlüssels mit der GUI

Navigieren Sie zu **Traffic Management > SSL > HSM**und fügen Sie einen HSM-Schlüssel hinzu.

Hinzufügen eines Zertifikatschlüsselpaars auf dem ADC

Informationen zu Zertifikatschlüsselpaaren finden Sie unter Hinzufügen oder Aktualisieren eines Zertifikatschlüsselpaares.

Hinzufügen eines Zertifikatschlüsselpaars mit der CLI

Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

```
add ssl certKey <certkeyName> -cert <string> -hsmKey <string>
<!--NeedCopy-->
```

Beispiel:

```
add ssl certKey key22 -cert example_selfcert -hsmKey examplersa2048key
Done
<!--NeedCopy-->
```

Hinzufügen eines Zertifikatschlüsselpaars mit der GUI

Navigieren Sie zu **Traffic Management > SSL > Certificates**, und fügen Sie ein Zertifikatschlüsselpaar hinzu.

Hinzufügen eines virtuellen Servers

Informationen zu einem virtuellen Server finden Sie unter Konfiguration des virtuellen SSL-Servers.

Konfigurieren eines SSL-basierten virtuellen Servers mit der CLI

Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

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

Beispiel:

```
add lb vserver v1 SSL 192.168.17.252 443
<!--NeedCopy-->
```

Konfigurieren eines SSL-basierten virtuellen Servers mit der GUI

Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, erstellen Sie einen virtuellen Server und geben Sie das Protokoll als SSL an.

Hinzufügen eines Serverobjekts

Bevor Sie ein Serverobjekt zum ADC hinzufügen können, vergewissern Sie sich, dass Sie einen Backend-Server erstellt haben. Im folgenden Beispiel wird das integrierte Python-HTTP-Server-Modul auf einem Linux-System verwendet.

Beispiel:

```
%python  -m SimpleHTTPServer 80
<!--NeedCopy-->
```

Hinzufügen eines Serverobjekts mit der CLI

Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

```
add server <name> <IPAddress>
<!--NeedCopy-->
```

Beispiel:

```
add server s1 192.168.17.246
<!--NeedCopy-->
```

Hinzufügen eines Serverobjekts mit der GUI

Navigieren Sie zu **Traffic Management > Load Balancing > Server**, und fügen Sie einen Server hinzu.

Hinzufügen eines Dienstes

Weitere Informationen finden Sie unter Konfigurieren von Diensten.

Konfigurieren eines Dienstes mit der CLI

Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

```
add service <name> <serverName> <serviceType> <port>
<!--NeedCopy-->
```


Beispiel:

```
add service sr1 s1 HTTP 80
<!--NeedCopy-->
```

Konfigurieren eines Dienstes mit der GUI

Navigieren Sie zu **Traffic Management > Load Balancing > Dienste**, und erstellen Sie einen Dienst.

Binden Sie den Dienst an den virtuellen Server

Weitere Informationen finden Sie unter Binden von Diensten an den virtuellen SSL-Server.

Binden eines Dienstes an einen virtuellen Server mit der CLI

Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

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

Beispiel:

```
bind lb vserver v1 sr1
<!--NeedCopy-->
```

Binden eines Dienstes an einen virtuellen Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen Server, und klicken Sie im Bereich Dienste auf, um einen Dienst an den virtuellen Server zu binden.

Binden Sie das Zertifikatschlüsselpaar an den virtuellen Server auf dem ADC

Weitere Informationen finden Sie unter Binden des Zertifikatschlüsselpaars an den virtuellen SSL-Server.

Binden Sie ein Zertifikatschlüsselpaar an einen virtuellen Server mit der CLI

Führen Sie an der Eingabeaufforderung den folgenden Befehl aus:

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

Beispiel:

```
bind ssl vserver v1 -certkeyName key22
Warning: Current certificate replaces the previous binding
<!--NeedCopy-->
```

Binden Sie ein Zertifikatschlüsselpaar an einen virtuellen Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Öffnen Sie einen virtuellen SSL-Server, und klicken Sie unter **Erweiterte Einstellungen** auf **SSL-Zertifikat**.
3. Binden Sie ein Serverzertifikat an den virtuellen Server.

Überprüfen der Konfiguration

So zeigen Sie die Konfiguration mit der CLI an:

Führen Sie an der Eingabeaufforderung die folgenden Befehle aus:

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

Beispiel:

```
show lb vserver v1
        v1 (192.168.17.252:443) - SSL   Type: ADDRESS
        State: UP
        Last state change was at Wed Oct 29 03:11:11 2014
        Time since last state change: 0 days, 00:01:25.220
        Effective State: UP
        Client Idle Timeout: 180 sec
```



```
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Appflow logging: ENABLED
        No. of Bound Services :  1 (Total)       1 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: Bound service's state
           changed to UP
        Mode: IP
        Persistence: NONE
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none
        L2Conn: OFF
        Skip Persistency: None
        IcmpResponse: PASSIVE
        RHIstate: PASSIVE
        New Service Startup Request Rate: 0 PER_SECOND, Increment
           Interval: 0
        Mac mode Retain Vlan: DISABLED
        DBS_LB: DISABLED
        Process Local: DISABLED
        Traffic Domain: 0

1) sr1 (192.168.17.246: 80) - HTTP State: UP    Weight: 1
Done
<!--NeedCopy-->
```

```
sh ssl vserver v1
        Advanced SSL configuration for VServer v1:
        DH: DISABLED
        Ephemeral RSA: ENABLED          Refresh Count: 0
        Session Reuse: ENABLED          Timeout: 120 seconds
        Cipher Redirect: DISABLED
        SSLv2 Redirect: DISABLED
        ClearText Port: 0
        Client Auth: DISABLED
        SSL Redirect: DISABLED
        Non FIPS Ciphers: DISABLED
        SNI: DISABLED
        SSLv2: DISABLED  SSLv3: DISABLED  TLSv1.0: ENABLED  TLSv1.1:
           DISABLED  TLSv1.2: DISABLED
        Push Encryption Trigger: Always
```



```
15          Send Close-Notify: YES
16
17          ECC Curve: P_256, P_384, P_224, P_521
18
19  1)      CertKey Name: key22       Server Certificate
20
21  1)      Cipher Name: DEFAULT
22          Description: Predefined Cipher Alias
23   Done
24  <!--NeedCopy-->
```

So zeigen Sie die Konfiguration mit der GUI an:

Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**, und doppelklicken Sie auf einen virtuellen SSL-Server, um ihn zu öffnen und die Konfiguration anzuzeigen.

Einschränkungen

October 5, 2021

- SSL Version 3 (SSLv3) wird auf einer MPX-Appliance nicht unterstützt, wird aber von einer virtuellen VPX-Appliance unterstützt. Eine VPX-Instanz, die auf einer SDX-Appliance bereitgestellt wird, unterstützt SSLv3 nur, wenn der Instanz kein SSL-Chip zugewiesen ist.
- Export-Chiffre werden nicht unterstützt.
- SSL-Serverschlüsselaustausch mit HSM-Schlüsseln wird nicht unterstützt.
- Wenn Sie Schlüssel hinzugefügt oder entfernt haben, nachdem Sie die Konfiguration zuletzt gespeichert haben, müssen Sie die Konfiguration speichern, bevor Sie einen Warmstart durchführen. Wenn Sie die Konfiguration nicht speichern, besteht ein Schlüsselkonflikt zwischen dem ADC und dem HSM.
- Sie können einen HSM-Schlüssel nicht an einen virtuellen DTLS-Server binden.
- Sie können kein Zertifikatschlüsselpaar binden, das mithilfe eines HSM-Schlüssels an einen SSL-Dienst erstellt wird.
- Sie können die GUI nicht verwenden, um den ADC als Client des HSM zu registrieren oder den Status des HSM über das Konfigurationsdienstprogramm zu überprüfen.
- Ab Release 11 Build 62.x wird SSL-Neuverhandlung unterstützt.
- Sie können OCSP-Anforderungen nicht signieren, indem Sie ein Zertifikatschlüsselpaar verwenden, das mithilfe eines HSM-Schlüssels erstellt wird.
- Ein Zertifikatbündel mit HSM-Schlüsseln wird nicht unterstützt.
- Ein Fehler wird nicht angezeigt, wenn der HSM-Schlüssel und das Zertifikat nicht übereinstimmen. Daher müssen Sie beim Hinzufügen eines Zertifikatschlüsselpaars sicherstellen, dass der HSM-Schlüssel und das Zertifikat übereinstimmen.

- Clustering und Adminpartitionen werden nicht unterstützt.

Anhang

October 5, 2021

Beispiel:

Hinweis: Im folgenden Beispiel sind die Befehle in Fettschrift dargestellt.

```
root@ns# ./chkserv
nCipher server running
root@ns# ./nfkminfo
World
 generation  2
 state       0x17a70000 Initialised Usable Recovery PINRecovery !
    ExistingClient RTC NVRAM FTO !AlwaysUseStrongPrimes SEEDebug
 n_modules   1
 hknso       cbec8c0c56c6b5e76b73147ef02d34a661eaa044
 hkm     bbb8d4839da5782be4d092735a7535538834dc91 (type Rijndael)
 hkmwk       1d572201be533ebc89f30fdd8f3fac6ca3395bf0
 hkre        01f21ecf43933ffdd45e74c3883525176c5c439c
 hkra        ac8ec5ee6bce00991bd97adce2091d9739b9b452
 hkmc        cf1b509abaad91995ed202d8f36613fc99433155
 hkp         c20910b2ed1ca62d6a2b0db67052a05f7bbfeb43
 hkrtc       bd811020a7c2f8df435a481c3767a89c2e13bc4f
 hknv        278b8012e48910d518a9ee91cff57233fb0c9093
 hkdsee      12230b0e31e3cec66324c0815f782cfb9249edd5
 hkfto       89dd6250b3d6149bcd15606f4553085e2fd6271a
 hkmnull     0100000000000000000000000000000000000000
 ex.client   none
 k-out-of-n  1/2
 other quora m=1 r=1 p=1 nv=1 rtc=1 dsee=1 fto=1
 createtime  2014-02-28 21:05:32
 nso timeout 10 min
 ciphersuite DLf1024s160mRijndael

Module #1
 generation 2
 state      0x2 Usable
 flags      0x10000 ShareTarget
 n_slots    2
```



```
 esn         BD17-C807-58D9
 hkml        70289a6edba00ddc7e3f6d6f5a49edc963e822f2

Module #1 Slot #0 IC 0
 generation    1
 phystype      SmartCard
 slotlistflags 0x2 SupportsAuthentication
 state         0x2 Empty
 flags         0x0
 shareno       0
 shares
 error         OK
No Cardset

Module #1 Slot #1 IC 0
 generation    1
 phystype      SoftToken
 slotlistflags 0x0
 state         0x2 Empty
 flags         0x0
 shareno       0
 shares
 error         OK
No Cardset

No Pre-Loaded Objects

root@ns# ./sigtest
 Hardware module #1 speed index 5792 recommended minimum queue 19
Found 1 module; using 19 jobs
Making 1024-bit RSAPrivate key on module #1;
  using Mech_RSApPKCS1 and PlainTextType_Bignum.
Generated and exported key from module #1.
Imported keys on module #1
 1,       3059 1223.6, 3059 overall
 2,       8698 2989.76, 4349 overall
 3,      14396 4073.06, 4798.67 overall
 4,      20091 4721.83, 5022.75 overall
 5,      25799 5116.3, 5159.8 overall
 6,      31496 5348.58, 5249.33 overall
 7,      37192 5487.55, 5313.14 overall
 8,      42780 5527.73, 5347.5 overall
 9,      45777 4515.44, 5086.33 overall
 10,      51457 4981.26, 5145.7 overall
 11,      57151 5266.36, 5195.55 overall
```



```
 12,      62813 5424.61, 5234.42 overall
 13,      68496 5527.97, 5268.92 overall
 14,      74182 5591.18, 5298.71 overall
 15,      79832 5614.71, 5322.13 overall
 16,      85518 5643.23, 5344.88 overall
 17,      88412 4543.54, 5200.71 overall
 18,      94086 4995.72, 5227 overall
 19,      99778 5274.23, 5251.47 overall
 20,     105469 5440.94, 5273.45 overall
 21,     111133 5530.16, 5292.05 overall
 22,     116838 5600.1, 5310.82 overall
 23,     122522 5633.66, 5327.04 overall
 24,     128175 5641.4, 5340.62 overall
 25,     131072 4543.64, 5242.88 overall
 26,     136762 5002.18, 5260.08 overall
 27,     142415 5262.51, 5274.63 overall
 28,     148125 5441.51, 5290.18 overall
 29,     153816 5541.3, 5304 overall
 30,     159414 5563.98, 5313.8 overall
<!--NeedCopy-->
```

Unterstützung für Thales Luna Network Hardwaresicherheitsmodul

May 10, 2022

Eine Citrix ADC-Appliance ohne FIPS speichert den privaten Schlüssel des Servers auf der Festplatte. Auf einer FIPS-Appliance wird der Schlüssel in einem kryptografischen Modul gespeichert, das als Hardware-Sicherheitsmodul (HSM) bekannt ist. Das Speichern eines Schlüssels im HSM schützt ihn vor physischen und Software-Angriffen. Darüber hinaus sind die Schlüssel mit speziellen FIPS-zugelassenen Verschlüsselungen verschlüsselt.

Nur die Citrix ADC MPX/SDX 14000 FIPS-Appliances unterstützen eine FIPS-Karte. Unterstützung für FIPS ist nicht auf anderen MPX/SDX-Appliances oder auf Citrix ADC VPX Appliances verfügbar. Diese Einschränkung wird durch die Unterstützung eines Thales Luna-Netzwerk-HSM auf allen Citrix ADC MPX-, SDX- und VPX-Appliances mit Ausnahme der MPX/SDX 14000 FIPS-Appliances und den unter Unterstützung für Intel Coleto SSL-Chip-basierten Plattformenaufgeführten Appliances behoben.

Ein Thales Luna-Netzwerk HSM wurde entwickelt, um kritische kryptografische Schlüssel zu schützen und sensible kryptografische Operationen in einer Vielzahl von Sicherheitsanwendungen zu beschleunigen.

Unterstützte Versionen Matrix

Citrix ADC-Version	Version der Software-Appliance	Firmware-Version	Clientversion
11.1, 12.0, 12.1	5.2.3-1	6.2.1	6.0.0
11.1, 12.0, 12.1	6.2.2-5	6.10.9	6.2.2
13.0	7.2.0-220	7.0.3	7.2.2 (7.2.0-220)

Voraussetzungen

October 5, 2021

Bevor Sie ein Thales Luna-Netzwerk HSM mit einem Citrix ADC verwenden können, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Ein HSM des Thales Luna-Netzwerks ist im Netzwerk installiert, einsatzbereit und für den Citrix ADC zugänglich. Das heißt, die NSIP-Adresse oder die SNIP-Adresse wird als autorisierter Kunde auf dem HSM hinzugefügt.
- Es stehen Lizenzen zur Unterstützung der erforderlichen Anzahl von Partitionen auf dem HSM zur Verfügung.
- Das Thales Luna-Netzwerk HSM und der Citrix ADC können Verbindungen untereinander über Port 1792 initiieren.
- Sie verwenden NetScaler Version 11.1 oder höher.
- Die Citrix ADC Appliance enthält keine FIPS Cavium-Karte.

> **Wichtig**
>
> HSMs des Thales Luna-Netzwerks werden auf den MPX 9700/10500/12500/15500 FIPS-Appliances nicht unterstützt.

Konfigurieren eines Thales Luna-Clients auf ADC

June 21, 2022

Nachdem Sie das Thales Luna HSM konfiguriert und die erforderlichen Partitionen erstellt haben, müssen Sie Clients erstellen und sie Partitionen zuweisen. Konfigurieren Sie zunächst die Thales Luna-Clients auf dem Citrix ADC und richten Sie die Netzwerkvertrauensverbindungen (NTLs) zwischen den Thales Luna-Clients und dem Thales Luna HSM ein. Eine Beispielkonfiguration ist im Anhangangegeben.

1. Wechseln Sie das Verzeichnis in /var/safenet und installieren Sie den Thales Luna Client. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
cd /var/safenet
<!--NeedCopy-->
```

Um den Thales Luna-Client Version 6.0.0 zu installieren, geben Sie Folgendes ein:

```
install_client.sh -v 600
<!--NeedCopy-->
```

Um den Thales Luna Client Version 6.2.2 zu installieren, geben Sie Folgendes ein:

```
install_client.sh -v 622
<!--NeedCopy-->
```

Um den Thales Luna Client Version 7.2.2 zu installieren, geben Sie Folgendes ein:

```
install_client.sh -v 722
<!--NeedCopy-->
```

2. Konfigurieren Sie die NTLs zwischen Thales Luna Client (ADC) und HSM.

   Nachdem das Verzeichnis '/var/safenet/' erstellt wurde, führen Sie die folgenden Aufgaben auf dem ADC aus.

   a) Ändern Sie das Verzeichnis in '/var/safenet/config/' und führen Sie das 'safenet_config'-Skript aus. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
cd /var/safenet/config

sh safenet_config
<!--NeedCopy-->
```

   Dieses Skript kopiert die Datei "Chrystoki.conf" in das Verzeichnis /etc/. Es erzeugt auch einen symbolischen Link 'libCryptoki2_64.so' im Verzeichnis '/usr/lib/'.

   b) Erstellen und übertragen Sie ein Zertifikat und einen Schlüssel zwischen dem ADC und dem Thales Luna HSM.

Um sicher kommunizieren zu können, müssen der ADC und HSM Zertifikate austauschen. Erstellen Sie ein Zertifikat und einen Schlüssel auf dem ADC und übertragen Sie es dann an das HSM. Kopieren Sie das HSM-Zertifikat in den ADC.

i) Wechseln Sie in das Verzeichnis /var/safenet/safenet/lunaclient/bin.

ii) Erstellen Sie ein Zertifikat auf dem ADC. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
./vtl createCert -n <ip address of Citrix ADC>
<!--NeedCopy-->
```

Dieser Befehl fügt auch das Zertifikat und den Schlüsselpfad zur Datei "/etc/Chrystoki.conf" hinzu.

iii) Kopieren Sie dieses Zertifikat in das HSM. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
scp /var/safenet/safenet/lunaclient/cert/client/<ip address of NS
   >.pem <LunaSA_HSM account>@<IP address of Luna SA>
<!--NeedCopy-->
```

iv) Kopieren Sie das HSM-Zertifikat in den Citrix ADC. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
scp <HSM account>@<HSM IP>:server.pem  /var/safenet/safenet/
   lunaclient/server_<HSM ip>.pem
<!--NeedCopy-->
```

3. Registrieren Sie den Citrix ADC als Client und weisen Sie ihm eine Partition auf dem Thales Luna HSM zu.

   Melden Sie sich beim HSM an und erstellen Sie einen Client. Geben Sie das NSIP als Client-IP ein. Diese Adresse muss die IP-Adresse des ADC sein, von dem Sie das Zertifikat an das HSM übertragen haben. Nachdem der Client erfolgreich registriert wurde, weisen Sie ihm eine Partition zu. Führen Sie die folgenden Befehle auf dem HSM aus.

   a) Verwenden Sie SSH, um eine Verbindung zum Thales Luna HSM herzustellen und geben Sie das Kennwort ein.

   b) Registrieren Sie den Citrix ADC im Thales Luna HSM. Der Client wird auf dem HSM angelegt. Die IP-Adresse ist die IP-Adresse des Clients. Das heißt, die NSIP-Adresse.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
client register  - client <client name> -ip <Citrix ADC ip>
<!--NeedCopy-->
```

c) Weisen Sie dem Client eine Partition aus der Partitionsliste zu. Geben Sie Folgendes ein, um die verfügbaren Partitionen anzuzeigen:

```
<luna_sh> partition list
<!--NeedCopy-->
```

Weisen Sie eine Partition aus dieser Liste zu. Typ:

```
<lunash:> client assignPartition -client <Client Name> -par <
   Partition Name>
<!--NeedCopy-->
```

4. Registrieren Sie das HSM mit seinem Zertifikat auf dem Citrix ADC.

   Ändern Sie auf dem ADC das Verzeichnis in “/var/safenet/safenet/lunaclient/bin” und geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
./vtl addserver -n <IP addr of HSM> -c /var/safenet/safenet/
   lunaclient/server_<HSM_IP>.pem
<!--NeedCopy-->
```

   Geben Sie Folgendes ein, um das HSM zu entfernen, das am ADC registriert ist:

```
./vtl deleteServer -n <HSM IP> -c <cert path>
<!--NeedCopy-->
```

   Geben Sie Folgendes ein, um die auf dem ADC konfigurierten HSM-Server aufzulisten:

```
./vtl listServer
<!--NeedCopy-->
```


> **Hinweis:**
>
> Stellen Sie vor dem Entfernen des HSM mithilfe von sicher `vtl`, dass alle Schlüssel für dieses HSM manuell von der Appliance entfernt wurden. HSM-Schlüssel können nicht gelöscht werden, nachdem der HSM-Server entfernt wurde.

5. Überprüfen Sie die Netzwerk-Trustlinks (NTLs) -Konnektivität zwischen ADC und HSM. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
./vtl verify
<!--NeedCopy-->
```

Wenn die Überprüfung fehlschlägt, überprüfen Sie alle Schritte. Fehler sind auf eine falsche IP-Adresse in den Client-Zertifikaten zurückzuführen.

6. Speichern Sie die Konfiguration.

Die vorherigen Schritte aktualisieren die "/etc/Chrystoki.conf" -Konfigurationsdatei. Diese Datei wird gelöscht, wenn der ADC gestartet wird. Kopieren Sie die Konfiguration in die Standardkonfigurationsdatei, die beim Neustart eines ADC verwendet wird.

Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
root@ns# cp /etc/Chrystoki.conf /var/safenet/config/
<!--NeedCopy-->
```

Es wird empfohlen, diesen Befehl jedes Mal auszuführen, wenn die Konfiguration im Zusammenhang mit Thales Luna geändert wird.

7. Starten Sie den Thales Luna Gateway-Prozess.

Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

```
sh /var/safenet/gateway/start_safenet_gw
<!--NeedCopy-->
```

8. Konfigurieren Sie den automatischen Start des Gateway Daemons beim Booten.

Erstellen Sie die Datei "safenet_is_enrolled", die angibt, dass Thales Luna HSM auf diesem ADC konfiguriert ist. Wenn der ADC neu gestartet wird und diese Datei gefunden wird, wird das Gateway automatisch gestartet.

Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:


```
touch /var/safenet/safenet_is_enrolled
<!--NeedCopy-->
```

9. Starten Sie die Citrix ADC-Appliance neu. Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Konfigurieren Sie Thales Luna HSMs in einem Hochverfügbarkeits-Setup auf dem ADC

December 7, 2021

Die Konfiguration von Thales Luna HSMs in einer Hochverfügbarkeit (HA) gewährleistet einen unterbrechungsfreien Service, auch wenn alle, außer eines der Geräte, nicht verfügbar sind. In einem HA-Setup schließt sich jeder HSM im Aktiv-Aktiv-Modus einer HA-Gruppe an. Thales Luna HSMs in einem HA-Setup bieten einen Lastenausgleich aller Gruppenmitglieder, um die Leistung und Reaktionszeit zu erhöhen und gleichzeitig die Gewährleistung eines Hochverfügbarkeitsdienstes zu gewährleisten. Für weitere Informationen wenden Sie sich an den Verkauf und Support von Thales Luna.

Voraussetzungen:

- Mindestens zwei Thales Luna HSM-Geräte. Alle Geräte in einer HA-Gruppe müssen entweder eine PED-Authentifizierung (vertrauenswürdiger Pfad) oder eine Kennwortauthentifizierung aufweisen. Eine Kombination aus vertrauenswürdiger Pfadauthentifizierung und Kennwortauthentifizierung in einer HA-Gruppe wird nicht unterstützt.
- Partitionen auf jedem HSM-Gerät müssen dasselbe Kennwort haben, auch wenn das Label (Name) anders ist.
- Alle Partitionen in HA müssen dem Client zugewiesen werden (Citrix ADC Appliance).

Nachdem Sie einen Thales Luna-Client auf dem ADC konfiguriert haben, wie unter Konfigurieren eines Thales Luna-Clients auf dem ADCbeschrieben, führen Sie die folgenden Schritte aus, um Thales Luna HSMs in HA zu konfigurieren:

1. Starten Sie an der Citrix ADC Shell-Eingabeaufforderung `lunacm` (/usr/safenet/lunaclient/bin)

   Beispiel:


```
root@ns# cd /var/safenet/safenet/lunaclient/bin/

root@ns# ./lunacm
<!--NeedCopy-->
```

2. Identifizieren Sie die Slot-IDs der Partitionen. Geben Sie Folgendes ein, um die verfügbaren Slots (Partitionen) aufzulisten:

```
lunacm:> slot list
<!--NeedCopy-->
```

Beispiel:

```
    Slot Id ->              0
    HSM Label ->            trinity-p1
    HSM Serial Number ->    481681014
    HSM Model ->            LunaSA 6.2.1
    HSM Firmware Version -> 6.10.9
    HSM Configuration ->    Luna SA Slot (PED) Signing With
       Cloning Mode
    HSM Status ->           OK

    Slot Id ->              1
    HSM Label ->            trinity-p2
    HSM Serial Number ->    481681018
    HSM Model ->            LunaSA 6.2.1
    HSM Firmware Version -> 6.10.9
    HSM Configuration ->    Luna SA Slot (PED) Signing With
       Cloning Mode
    HSM Status ->           OK

     Slot Id ->              2
     HSM Label ->            neo-p1
     HSM Serial Number ->    487298014
     HSM Model ->            LunaSA 6.2.1
     HSM Firmware Version -> 6.10.9
     HSM Configuration ->    Luna SA Slot (PED) Signing With
        Cloning Mode
    HSM Status ->           OK

    Slot Id ->              3
```



```
26      HSM Label ->             neo-p2
27      HSM Serial Number ->     487298018
28      HSM Model ->             LunaSA 6.2.1
29      HSM Firmware Version -> 6.10.9
30      HSM Configuration ->     Luna SA Slot (PED) Signing With
           Cloning Mode
31      HSM Status ->            OK
32
33      Slot Id ->               7
34      HSM Label ->             hsmha
35      HSM Serial Number ->     1481681014
36      HSM Model ->             LunaVirtual
37      HSM Firmware Version -> 6.10.9
38      HSM Configuration ->     Luna Virtual HSM (PED) Signing With
           Cloning Mode
39      HSM Status ->            N/A - HA Group
40
41      Slot Id ->               8
42      HSM Label ->             newha
43      HSM Serial Number ->     1481681018
44      HSM Model ->             LunaVirtual
45      HSM Firmware Version -> 6.10.9
46      HSM Configuration ->     Luna Virtual HSM (PED) Signing With
           Cloning Mode
47      HSM Status ->            N/A - HA Group
48
49      Current Slot Id: 0
50  <!--NeedCopy-->
```

3. Erstellen Sie die HA-Gruppe. Die erste Partition wird als primäre Partition bezeichnet. Sie können mehrere sekundäre Partitionen hinzufügen.

```
1  lunacm:> hagroup createGroup -slot <slot number of primary
       partition> -label <group name> -password <partition password >
2
3  lunacm:> hagroup createGroup -slot 1 -label gp12 -password ** ****
4  <!--NeedCopy-->
```

4. Fügen Sie die sekundären Elemente (HSM-Partitionen) hinzu. Wiederholen Sie diesen Schritt für alle Partitionen, die der HA-Gruppe hinzugefügt werden sollen.


```
lunacm:> hagroup addMember -slot <slot number of secondary
    partition to be added> -group <group name> -password <partition
     password>
<!--NeedCopy-->
```

Code:

```
lunacm:> hagroup addMember -slot 2 -group gp12 -password ** ****
<!--NeedCopy-->
```

5. Nur HA-Modus aktivieren.

```
lunacm:> hagroup HAOnly  - enable
<!--NeedCopy-->
```

6. Aktiven Wiederherstellungsmodus aktivieren.

```
lunacm:.>hagroup recoveryMode  - mode active
<!--NeedCopy-->
```

7. Einstellen der automatischen Wiederherstellungsintervall (in Sekunden). Die Standardeinstellung ist 60 Sekunden.

```
lunacm:.>hagroup interval  - interval <value in seconds>
<!--NeedCopy-->
```

Beispiel:

```
lunacm:.>hagroup interval  - interval 120
<!--NeedCopy-->
```

8. Festlegen der Anzahl der Wiederherstellungswiederholungen. Ein Wert von -1 erlaubt eine unendliche Anzahl von Wiederholungen.

```
lunacm:> hagroup retry -count <xxx>
<!--NeedCopy-->
```


Beispiel:

```
lunacm:> hagroup retry -count 2
<!--NeedCopy-->
```

9. Kopieren Sie die Konfiguration von `Chrystoki.conf` in das SafeNet-Konfigurationsverzeichnis.

```
cp /etc/Chrystoki.conf /var/safenet/config/
<!--NeedCopy-->
```

10. Starten Sie die ADC-Appliance neu.

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

Nach der Konfiguration von Thales Luna HSM in HA finden Sie unter Andere ADC-Konfiguration für weitere Konfiguration auf dem ADC.

Andere ADC-Konfiguration

October 5, 2021

1. Generieren Sie einen Schlüssel auf dem HSM.

   Verwenden Sie Tools von Drittanbietern, um Schlüssel auf dem HSM zu erstellen.

2. Fügen Sie einen HSM-Schlüssel auf dem ADC hinzu.

   Wichtig! Das #-Zeichen wird in einem Schlüsselnamen nicht unterstützt. Wenn der Schlüsselname dieses Zeichen enthält, schlägt der Ladeschlüsselvorgang fehl.

   So fügen Sie mit der CLI einen Thales Luna HSM-Schlüssel hinzu:

   Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ssl hsmkey <KeyName> -hsmType SAFENET -serialNum <serial #> -
    password
<!--NeedCopy-->
```


Wobei:

-keyName ist der Schlüssel, der auf dem HSM mithilfe von Tools von Drittanbietern erstellt wird.

-serialNum ist die Seriennummer der Partition auf dem HSM, auf der die Schlüssel generiert werden.

Hinweis: Verwenden Sie für HSM in einem Hochverfügbarkeitssetup die Seriennummer der Hochverfügbarkeitsgruppe.

-password ist das Kennwort der Partition, auf der die Schlüssel vorhanden sind.

So fügen Sie mit der GUI einen Thales Luna HSM-Schlüssel hinzu:

Navigieren Sie zu **Traffic Management** > **SSL** > **HSM**, und fügen Sie einen HSM-Schlüssel hinzu. Sie müssen den HSM Typ als **SAFENET**angeben.

3. Fügen Sie dem ADC ein Zertifikatschlüsselpaar hinzu. Verwenden Sie zuerst ein Drittanbieter-Tool, um ein mit dem Schlüssel verknüpftes Zertifikat zu generieren. Kopieren Sie dann das Zertifikat in das Verzeichnis /nsconfig/ssl/ auf dem ADC.

   Hinweis: Der Schlüssel muss ein HSM-Schlüssel sein.

   So fügen Sie dem ADC mit der CLI ein Certkey-Paar hinzu:

   Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   add ssl certkey <CertkeyName> -cert <cert name> -hsmkey <KeyName>
   <!--NeedCopy-->
   ```

   So fügen Sie ein Certkey-Paar auf dem ADC mit der GUI hinzu:

   a) Navigieren Sie zu **Traffic Management** > **SSL**.
   b) Wählen Sie unter **Erste Schritte**die Option **Zertifikat (HSM) installieren**aus, und erstellen Sie ein Zertifikatschlüsselpaar mit einem HSM-Schlüssel.

4. Erstellen Sie einen virtuellen Server, und binden Sie das Zertifikatschlüsselpaar an diesen virtuellen Server.

Weitere Informationen zum Erstellen eines virtuellen Servers erhalten Sie, indem Sie auf Konfiguration des virtuellen SSL-Serversklicken.

Um Informationen zum Hinzufügen eines Zertifikatschlüsselpaars zu erhalten, klicken Sie auf Hinzufügen oder Aktualisieren eines Zertifikatschlüsselpaars.

Informationen zum Binden eines Zertifikatschlüsselpaars an einen virtuellen SSL-Server erhalten Sie, um Informationen zum Binden eines Zertifikatschlüsselpaars an den virtuellen SSL-Serverzu erhalten.

Citrix ADC Appliances in einem Hochverfügbarkeitssetup

October 5, 2021

Sie können ein Hochverfügbarkeits-Setup (HA) auf den Citrix ADC Appliances mit einer Thales Luna HSM-Konfiguration auf eine der folgenden zwei Arten konfigurieren:

- Konfigurieren Sie zunächst ein Thales Luna HSM auf den beiden Knoten mit demselben HSM und derselben Partition. Erstellen Sie dann ein HA-Paar. Fügen Sie schließlich die Citrix ADC Konfiguration wie Schlüssel, Zertifikatschlüsselpaare und virtuelle Server auf dem primären Knoten hinzu.
- Wenn ein Thales Luna HSM bereits auf einem Knoten mit der Citrix ADC-Konfiguration konfiguriert ist, fügen Sie eine ähnliche Konfiguration auf dem anderen Knoten hinzu. Kopieren Sie /var/safenet/sfgw_ident_file vom ersten Knoten auf den anderen und starten Sie die safenet_gw-Binärdatei neu. Nachdem das Gateway gestartet ist und ausgeführt wurde, fügen Sie die Knoten in einem HA-Setup hinzu.

Einschränkungen

October 5, 2021

1. Bei Änderungen an der HSM-bezogenen Konfiguration in einem vorhandenen Setup, z. B. Hinzufügen oder Entfernen eines HSM oder Erstellen eines Hochverfügbarkeitssetups, müssen Sie '/etc/chrystoki.conf' in '/var/safenet/config' kopieren.
2. Nach dem Hinzufügen, Entfernen oder Neustart eines HSM müssen Sie die Binärdatei '/var/safenet/gateway/safenet_gw' neu starten. Wenn Sie die Gateway -Binärdatei nicht neu starten, wird der HSM nach dem Hinzufügen oder nach dem Neustart keinen Datenverkehr bereitstellen.
3. Um die aktuelle Binärdatei '/var/safenet/gateway/safenet_gw' neu zu starten oder zu stoppen, verwenden Sie

   ```
   kill  - SIGTERM <PID>
   kill  - SIGINT <PID>
   <!--NeedCopy-->
   ```

   Wichtig! Verwenden Sie nicht`kill -9 <PID>` oder`kill -6 <PID>`
4. Entfernen Sie vor dem Entfernen eines vorhandenen HSM aus dem ADC alle Schlüssel und Zertifikatschlüsselpaare, die diesem HSM zugeordnet sind. Sie können diese Dateien nicht aus dem

ADC löschen, nachdem Sie das HSM entfernt haben.

5. Auf einer eigenständigen Citrix ADC Appliance werden Thales Luna HSMs in HA für Luna Version 6.2 und höher unterstützt.
6. EXPORT-Chiffren werden nicht unterstützt.
7. Update-Zertifikatschlüssel-Paar wird nicht unterstützt.
8. Wenn Sie einen HSM-Schlüssel auf einem Drittanbieter-Tool generieren, müssen die Namen für private und öffentliche Schlüssel identisch sein. Wenn Sie den HSM-Schlüssel der Appliance hinzufügen, geben Sie diesen Namen als Schlüsselnamen an.
9. Das ## Zeichen wird in einem Schlüsselnamen nicht unterstützt.
10. Cluster- und Adminpartitionen werden nicht unterstützt.

Anhang

December 7, 2021

Beispielbefehle mit ihren Ausgaben:

Führen Sie das Skript aus

```
1      root@ns# pwd
2     /var/safenet/config
3     root@ns# sh safenet_config
4 <!--NeedCopy-->
```

Erstellen eines Zertifikats

```
1     root@ns# cd /var/safenet/safenet/lunaclient/bin
2     root@ns# ./vtl createcert -n 10.102.59.175
3     Private Key created and written to: /var/safenet/safenet/lunaclient
         /cert/client/10.102.59.175Key.pem
4     Certificate created and written to: /var/safenet/safenet/lunaclient
         /cert/client/10.102.59.175.pem
5 <!--NeedCopy-->
```


Kopieren Sie das Zertifikat in das HSM

```
root@ns# scp /var/safenet/safenet/lunaclient/cert/client
   /10.102.59.175.pem admin@10.217.2.7:
admin@10.217.2.7's password:

10.102.59.175.pem          100%  818     0.8KB/s   00:00
<!--NeedCopy-->
```

Kopieren des Zertifikats und des Schlüssels aus dem HSM in die Citrix ADC Appliance

```
root@ns# scp admin@10.217.2.7:server.pem /var/Thales Luna/safenet/
   lunaclient/server.2.7.pem
admin@10.217.2.7's password:

server.pem            100% 1164     1.1KB/s   00:01
<!--NeedCopy-->
```

Verwenden Sie SSH, um eine Verbindung zum Thales Luna HSM herzustellen

```
ssh admin@10.217.2.7
Connecting to 10.217.2.7:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.

Last login: Thu Jun 23 02:20:29 2016 from 10.252.243.11

Luna SA 5.2.3-1 Command Line Shell - Copyright (c) 2001-2014
   SafeNet, Inc. All rights reserved.

[Safenet1] lunash:>hsm login


  Please enter the HSM Administrators' password:
  > ** *****

'hsm login' successful.


Command Result : 0 (Success)
[Safenet1] lunash:>
```



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

Registrieren Sie den Citrix ADC im Thales Luna HSM

```
    [Safenet1] lunash:>client register -client ns175 -ip 10.102.59.175

    'client register' successful.


    Command Result : 0 (Success)
    [Safenet1] lunash:>
<!--NeedCopy-->
```

Weisen Sie dem Client eine Partition aus der Partitionsliste zu

```
    [Safenet1] lunash:>client assignPartition -client ns175 -partition
       p2

    'client assignPartition' successful.


    Command Result : 0 (Success)
    [Safenet1] lunash:>
<!--NeedCopy-->
```

Registrieren des HSM mit seinem Zertifikat auf dem Citrix ADC

```
    root@ns# ./vtl addserver -n 10.217.2.7 -c /var/safenet/safenet/
       lunaclient/server.2.7.pem

    New server 10.217.2.7 successfully added to server list.
<!--NeedCopy-->
```

Überprüfen der NTL-Verbindung (Network Trust Links) zwischen ADC und HSM

```
    root@ns# ./vtl verify

    The following Luna SA Slots/Partitions were found:
```



```
4
5     Slot        Serial #                  Label
6     ====      ================          =====
7        0              477877010          p2
8  <!--NeedCopy-->
```

Speichern der Konfiguration

```
1     root@ns# cp /etc/Chrystoki.conf /var/safenet/config/
2  <!--NeedCopy-->
```

Konfigurieren Sie den automatischen Start des Gateway Daemons beim Booten

```
1     touch /var/safenet/safenet_is_enrolled
2  <!--NeedCopy-->
```

Häufig gestellte Fragen

October 5, 2021

- **Wie überprüfe ich, ob der Thales Luna-Prozess läuft?**

  Geben Sie an der Citrix ADC -Shell Eingabeaufforderung Folgendes ein:

  ```
  1  ps  - aux | grep safenet_gw
  2  <!--NeedCopy-->
  ```

- **Wie kann ich die Netzwerkvertrauens-Links (Network Trust Links, NTLs) -Konnektivität zwischen ADC und HSM überprüfen?**

  Ändern Sie nach der Konfiguration von Thales Luna das Verzeichnis in “/var/safenet/safenet/lunaclient/bin” und geben Sie ein:

  ```
  1  ./vtl verify
  2  <!--NeedCopy-->
  ```


Unterstützung für Azure Key Vault

December 3, 2021

Die Citrix ADC Appliance lässt sich in externe HSMs (SafeNet und Thales) für on-premises Bereitstellungen integrieren. Bei Cloud-Bereitstellungen lässt sich die ADC-Appliance in Azure Key Vault integrieren. Die Appliance speichert ihre privaten Schlüssel im Schlüsseltresor, um die Verwaltung und Sicherheit des privaten Schlüssels in der Public Cloud-Domäne zu vereinfachen. Sie müssen keine Schlüssel mehr an verschiedenen Orten für ADC-Appliances speichern und verwalten, die in mehreren Rechenzentren und Cloud-Anbietern bereitgestellt werden.

Die Verwendung von ADC mit der Preisstufe Azure Key Vault Premium, die HSM-gestützte Schlüssel bereitstellte, bietet FIPS 140-2 Level 2-Konformität.

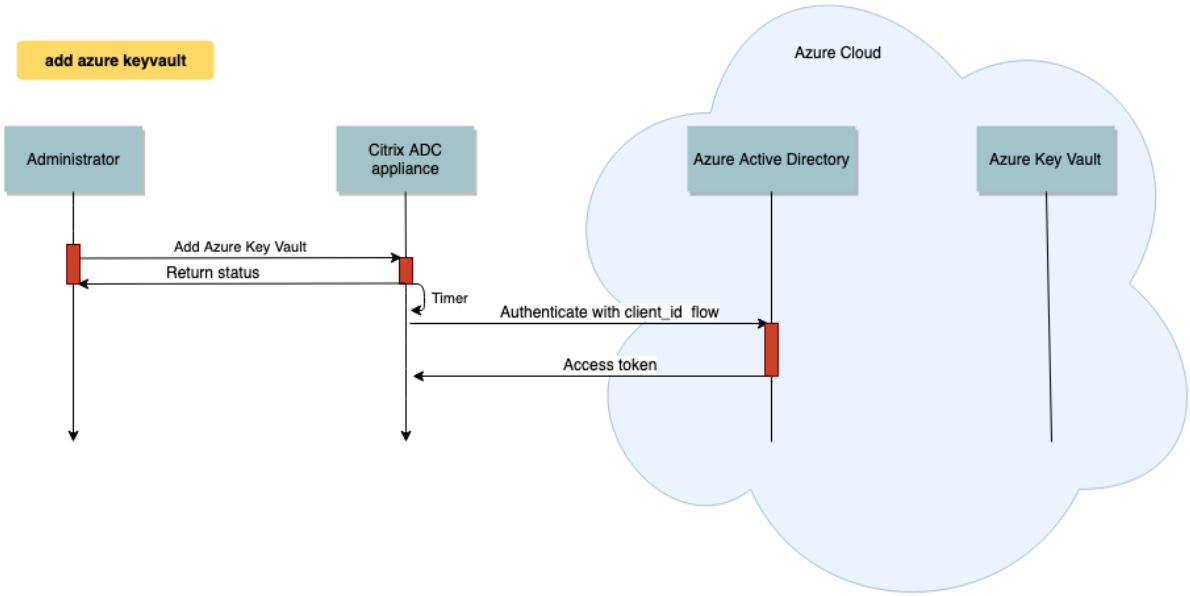
Azure Key Vault ist ein Standardangebot von Microsoft. Weitere Informationen zu Azure Key Vault finden Sie in der Microsoft Azure-Dokumentation.

Hinweis: Die Citrix ADC-Integration mit Azure Key Vault wird mit dem TLS 1.3-Protokoll unterstützt.

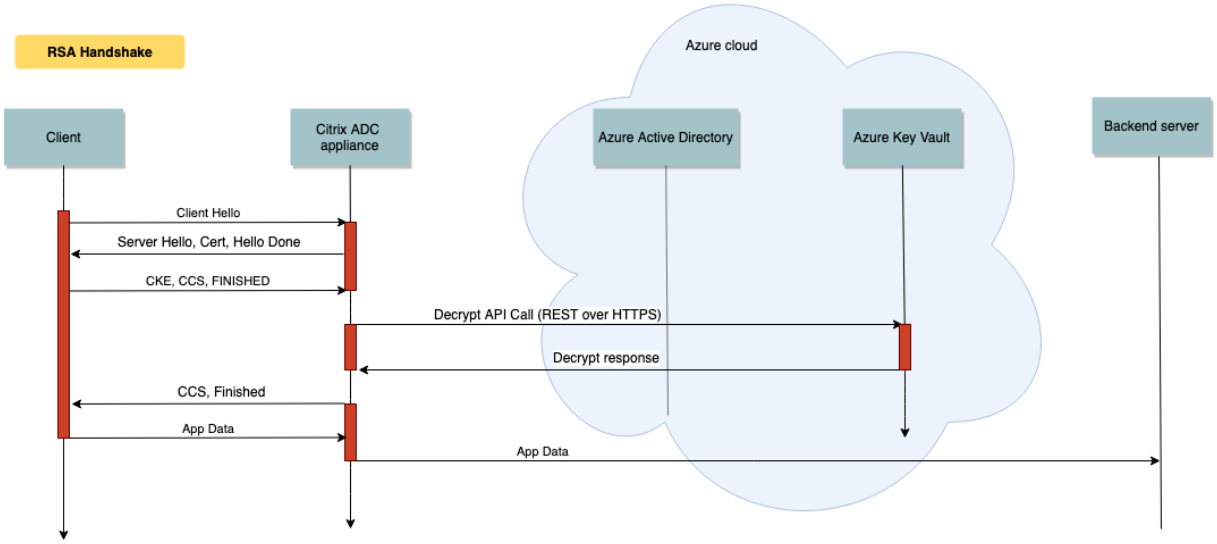
Architektur im Überblick

Azure Key Vault ist ein Dienst zum sicheren Speichern von Geheimnissen in der Azure Cloud. Indem Sie Ihre Schlüssel im Azure Key Vault aufbewahren, verringern Sie die Wahrscheinlichkeit, dass Schlüssel gestohlen werden. Sobald der Schlüsseltresor eingerichtet ist, können Sie Ihre Schlüssel darin aufbewahren. Konfigurieren Sie virtuelle Server auf der ADC-Appliance für private Schlüsselvorgänge im Schlüsseltresor. Die ADC-Appliance greift für jeden SSL-Handshake auf den Schlüssel zu.

Das folgende Diagramm veranschaulicht den Vorgang zum Abrufen eines Zugriffstokens aus Azure Active Directory nach der Authentifizierung. Dieses Token wird mit REST-API-Aufrufen für Kryptooperationen mit privaten Schlüsseln verwendet.



Das folgende Diagramm zeigt einen typischen RSA-Handshake. Die Clientschlüsselungsnachricht (CKE), die mit dem öffentlichen Schlüssel verschlüsselt wird, wird mit dem im Schlüsselspeicher gespeicherten privaten Schlüssel entschlüsselt.



In einem ECDHE-Handshake wird die von der Citrix ADC Appliance gesendete Serverschlüsselaustauschnachricht (SKE) mithilfe des im Schlüsseltresor gespeicherten privaten Schlüssels signiert.

Voraussetzungen

1. Sie müssen ein Azure-Abonnement haben.

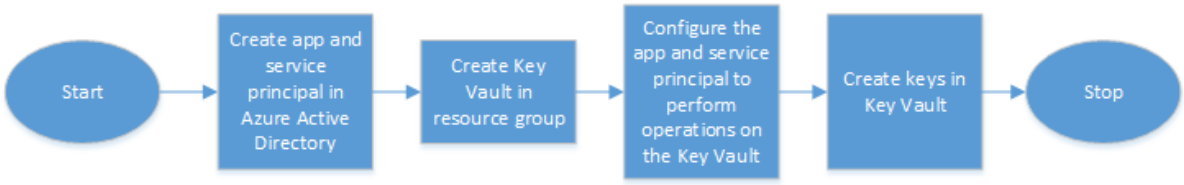
2. (Optional) Installieren Sie Azure CLI auf einem Linux-Computer. Anweisungen finden Sie in der Azure-Dokumentation https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-apt?view=azure-cli-latest.
3. Schließen Sie die Konfiguration auf dem Azure-Portal ab, bevor Sie Entitäten auf der ADC Appliance

Konfigurieren der ADC Azure Key Vault-Integration

Führen Sie zuerst die Konfiguration im Azure-Portal durch, gefolgt von der Konfiguration auf der ADC-Appliance.

Führen Sie die folgenden Schritte im Azure-Portal aus

Das folgende Flussdiagramm zeigt den übergeordneten Fluss für die Konfiguration, die für das Azure-Portal erforderlich ist.

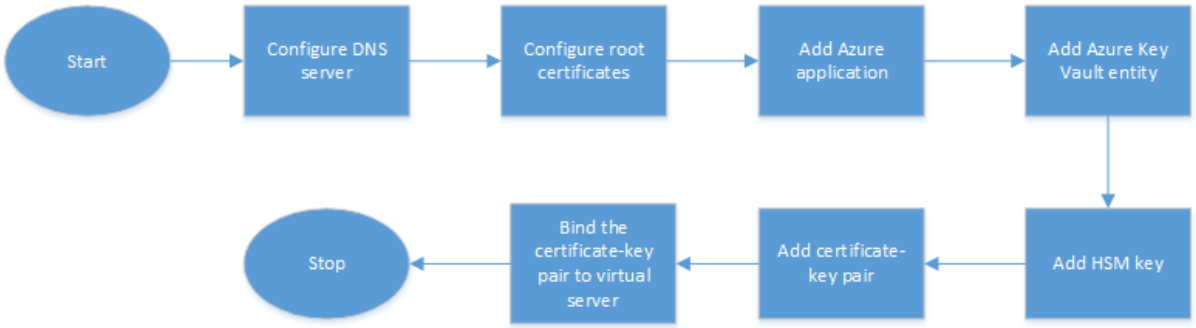


1. Erstellen Sie App und Service Principal in Azure Active Directory.
2. Erstellen Sie einen Schlüsseltresor in einer Ressourcengruppe.
3. Konfigurieren Sie die App und den Service Principal für Signierungs- und Entschlüsselungsvorgänge im Schlüsseltresor.
4. Erstellen Sie Schlüssel im Schlüsseltresor auf eine der folgenden Arten:
    a) Indem Sie eine Schlüsseldatei importieren.
    b) Durch Generieren eines Zertifikats.

Informationen zu den Befehlen zum Konfigurieren der vorangegangenen Schritte finden Sie in der Azure-Dokumentation unter https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals.

Führen Sie die folgenden Schritte auf der ADC-Appliance aus

Das folgende Flussdiagramm zeigt den High-Level-Fluss für die Konfiguration, die auf der ADC-Appliance erforderlich ist.



1. Konfigurieren Sie einen DNS-Server.
2. Konfigurieren Sie Stammzertifikate zur Überprüfung der von Azure präsentierten Zertifikate.
3. Erstellen Sie eine Azure-Anwendung.
4. Erstellen Sie eine Azure Key Vault-Entität.
5. Erstellen Sie einen HSM-Schlüssel.
6. Erstellen Sie ein Zertifikatsschlüsselpaar.
7. Binden Sie das Zertifikatsschlüsselpaar an einen virtuellen Server.

Konfigurieren Sie einen DNS-Server

Für die Namensauflösung des Key Vault-Hosts und des Azure Active Directory-Endpunkts ist ein DNS-Server erforderlich.

So konfigurieren Sie einen DNS-Server mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

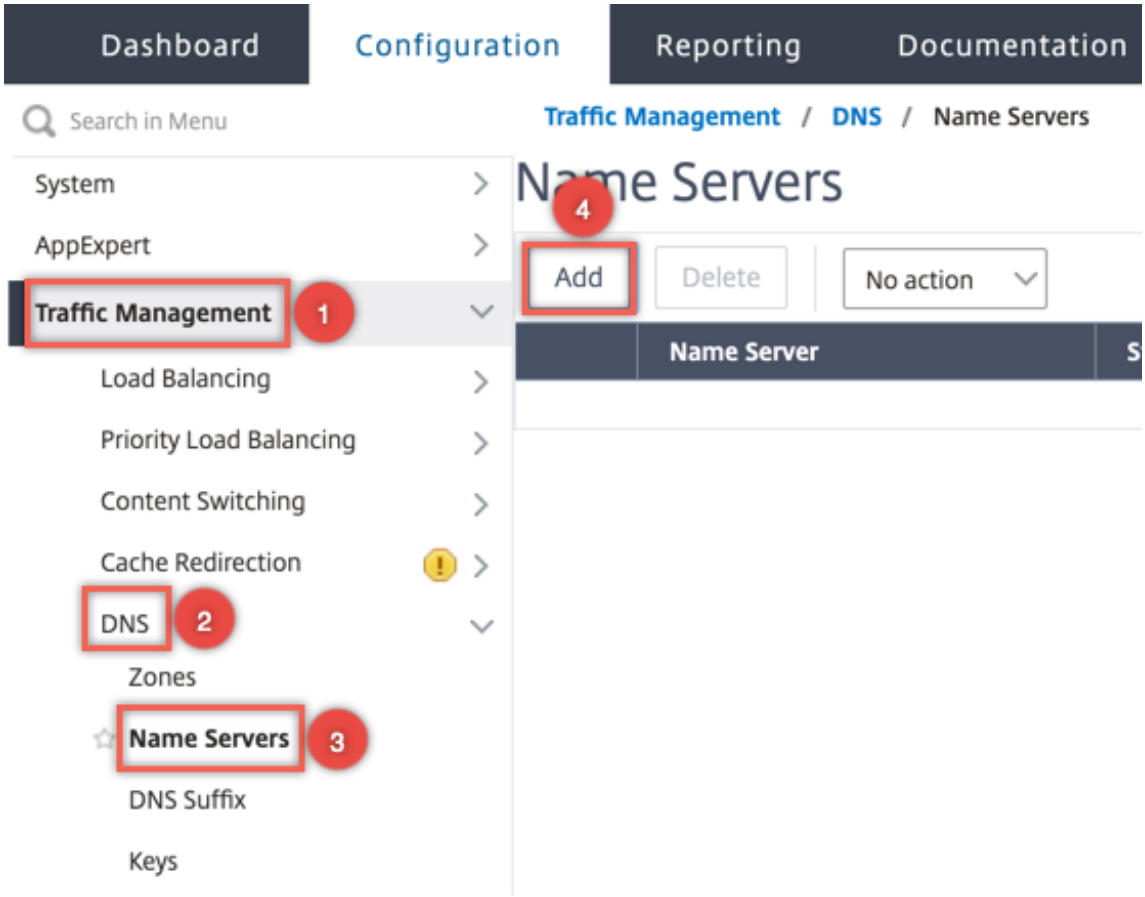
```
add dns nameserver <IP address>
<!--NeedCopy-->
```

Beispiel:

```
add dns nameserver 192.0.2.150
<!--NeedCopy-->
```

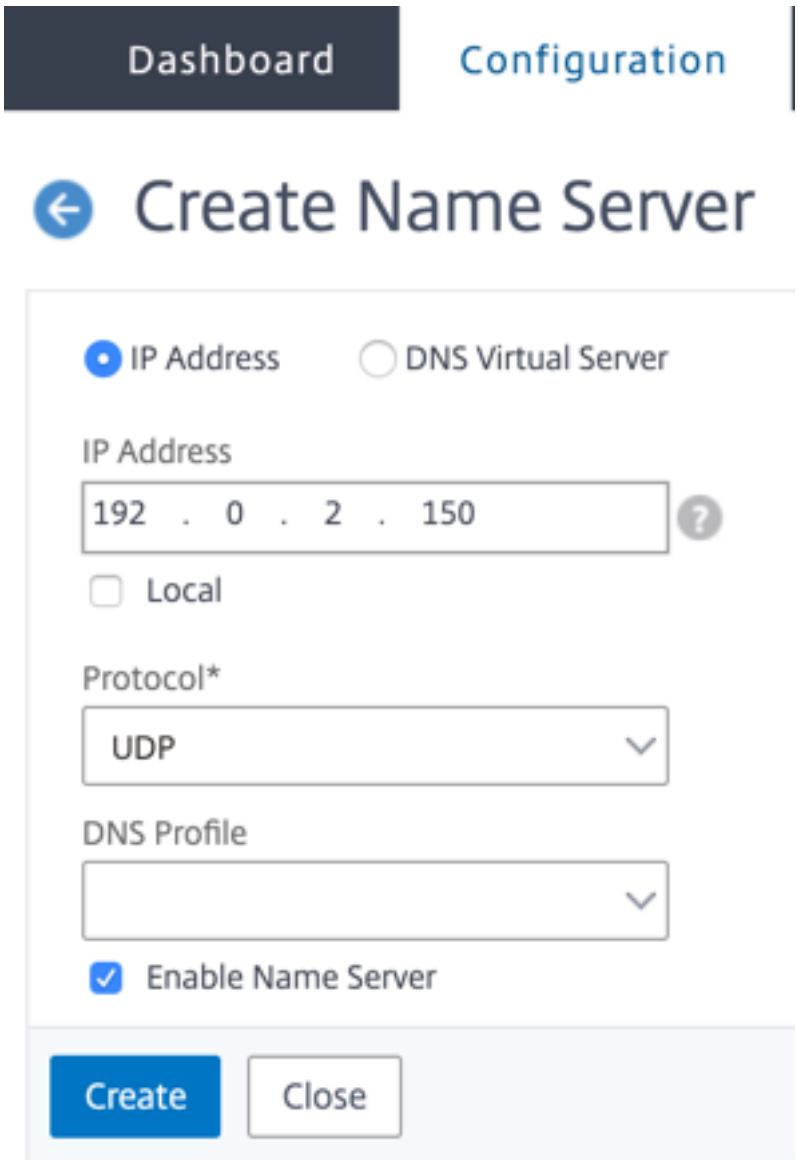
So konfigurieren Sie einen DNS-Server mit der GUI

1. Navigieren Sie zu **Traffic Management > DNS > Nameserver**. Klicken Sie auf **Hinzufügen**.



2. Geben Sie Werte für die folgenden Parameter ein:

   - IP-Adresse — Die IP-Adresse eines externen Nameservers oder, falls der lokale Parameter festgelegt ist, die IP-Adresse eines lokalen DNS-Servers (LDNS).
   - Protokoll — vom Nameserver verwendetes Protokoll. UDP_TCP ist nicht gültig, wenn der Nameserver ein virtueller DNS-Server ist, der auf der Appliance konfiguriert ist.



3. Klicken Sie auf **Erstellen**.

Hinzufügen und Binden eines Stammzertifikats

Laden Sie die Stammzertifikate des von Azure Key Vault `https://<vault_name>.vault.azure.net` und Azure Active Directory (AAD) vorgestellten Zertifikats herunter https://login.microsoftonline.com und laden Sie es auf die ADC Appliance. Diese Zertifikate sind erforderlich, um das von Azure Key Vault und AAD vorgelegte Zertifikat zu validieren. Binden Sie ein oder mehrere Zertifikate an die CA-Zertifikatsgruppe `ns_callout_certs`.

So fügen Sie mithilfe der CLI ein Stammzertifikat hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

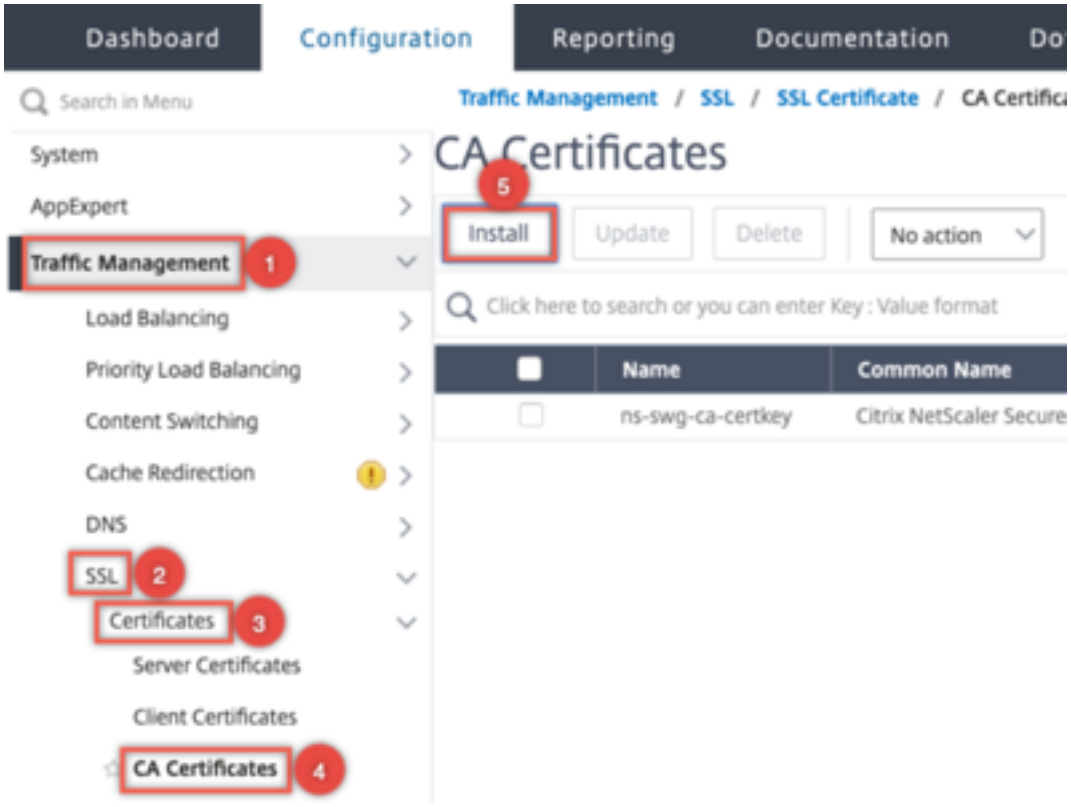

```
add ssl certkey <certkeyname> -cert <certname>
bind ssl caCertGroup <caCertGroupName> <certkeyName>
<!--NeedCopy-->
```

Beispiel:
Im folgenden Beispiel ist das von Azure Key Vault und AAD präsentierte Stammzertifikat dasselbe.

```
add ssl certKey rootcert -cert RootCyberTrustRoot.crt
bind ssl cacertGroup ns_callout_certs  rootcert
<!--NeedCopy-->
```

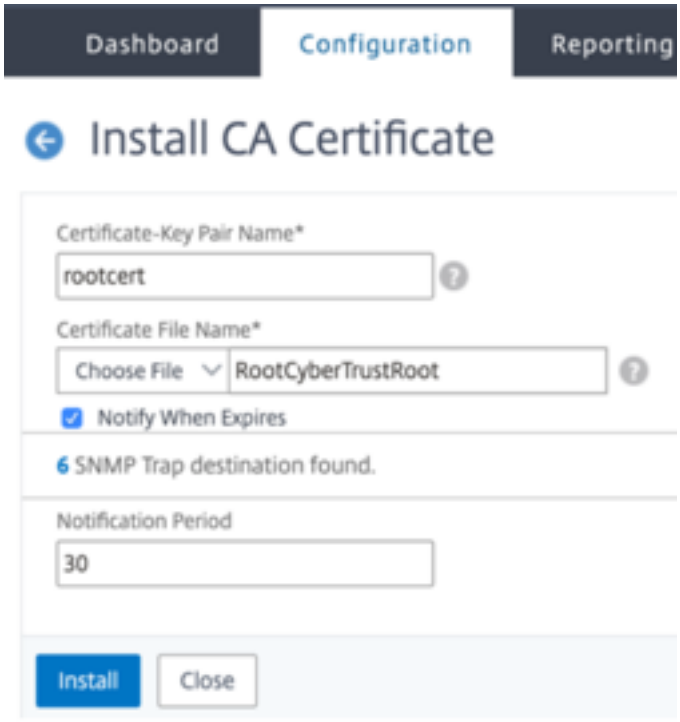
So fügen Sie mithilfe der GUI ein Stammzertifikat hinzu

1. Navigieren Sie zu **Traffic Management > SSL > Zertifikate > CA-Zertifikate**.

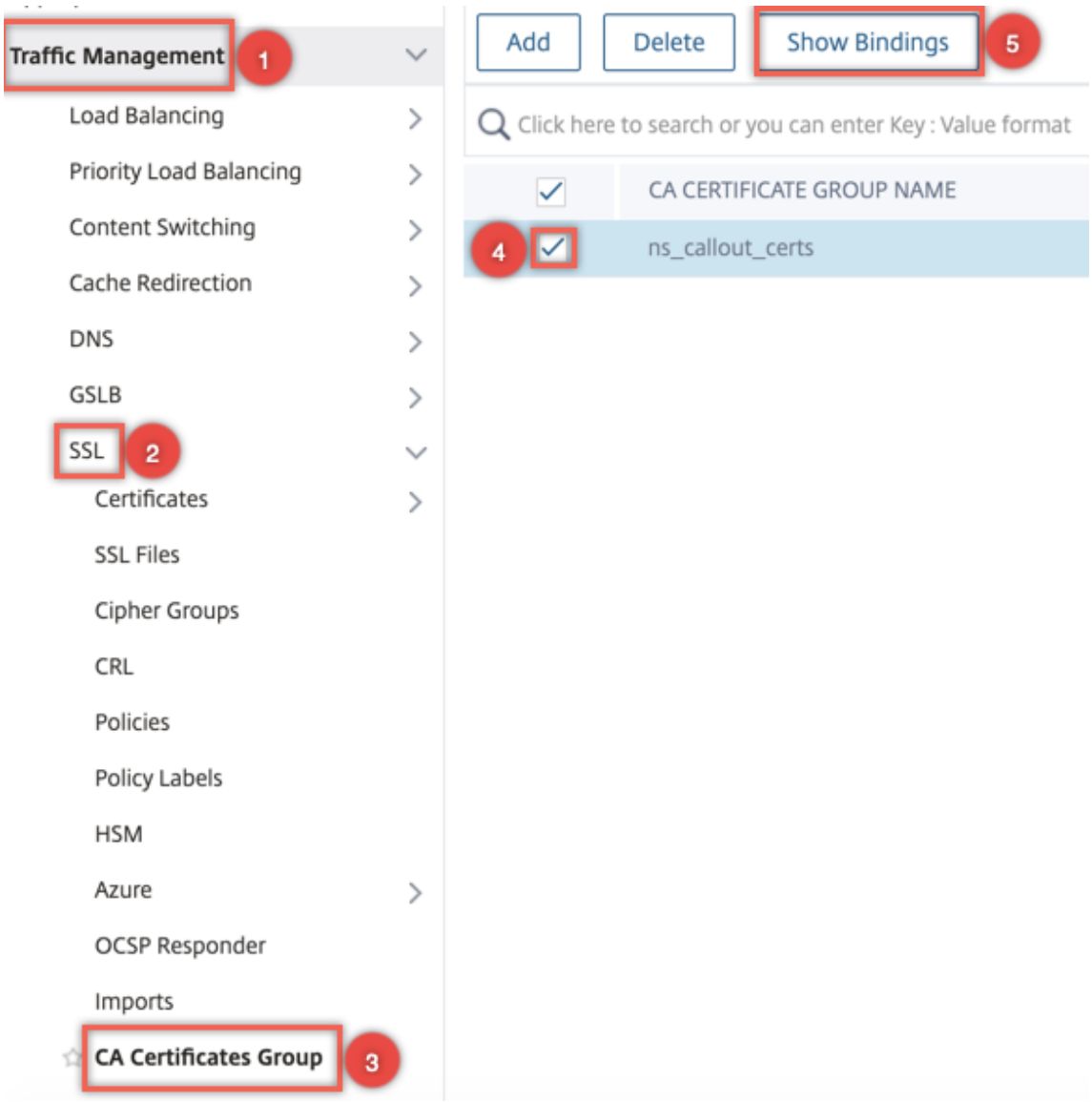


2. Geben Sie Werte für die folgenden Parameter ein:

   - Name des Zertifikatsschlüssel-Paars
   - Name der Zertifikatsdatei



3. Klicken Sie auf **Installieren**.
4. Navigieren Sie zu **Verkehrsmanagement > SSL > CA Certificates Group**.
5. Wählen Sie **ns_callout_certs** aus und klicken Sie auf **Bindungen anzeigen**.



6. Klicken Sie auf **Bind**.
7. Wählen Sie das zuvor erstellte CA Zertifikat aus und klicken Sie auf **Auswählen**
8. Klicken Sie auf **Binden**, und klicken Sie dann auf **Schließen**.

Konfigurieren einer Azure-Anwendung

Die Azure-Anwendungsentität enthält die erforderlichen Anmeldeinformationen, um sich bei Azure Active Directory zu authentifizieren und das Zugriffstoken abzurufen. Das heißt, um Autorisierungszugriff auf Key Vault-Ressourcen und APIs zu erhalten, fügen Sie die Azure Application ID, das geheime (Kennwort) und die Mandanten-ID auf der ADC-Appliance hinzu.
Wenn Sie die Azure Application Entity mithilfe der CLI konfigurieren, müssen Sie das Kennwort eingeben. Wenn Sie die GUI verwenden, enthält die Azure-Anwendungseinheit die erforderlichen

Anmeldeinformationen, um sich bei Azure Active Directory zu authentifizieren und das Zugriffstoken abzurufen.

So konfigurieren Sie eine Azure-Anwendung mithilfe der CLI

Ab Version 13.0-61.x wird dem `add azure application` Befehl ein Parameter, VaultResource, hinzugefügt, um die Domäne der Ressourcengruppe abzurufen, bevor das Zugriffstoken der Anwendung gewährt wird. Dieser Parameter wird hinzugefügt, da der Domainname für verschiedene Regionen unterschiedlich sein kann. Zum Beispiel könnte die Domäne `vault.azure.net` oder sein `vault.usgov.net`.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add azure application <name> -clientID <string> -clientSecret -tenantID
    <string> -vaultResource <string> [-tokenEndpoint <URL>]
show azure application
<!--NeedCopy-->
```

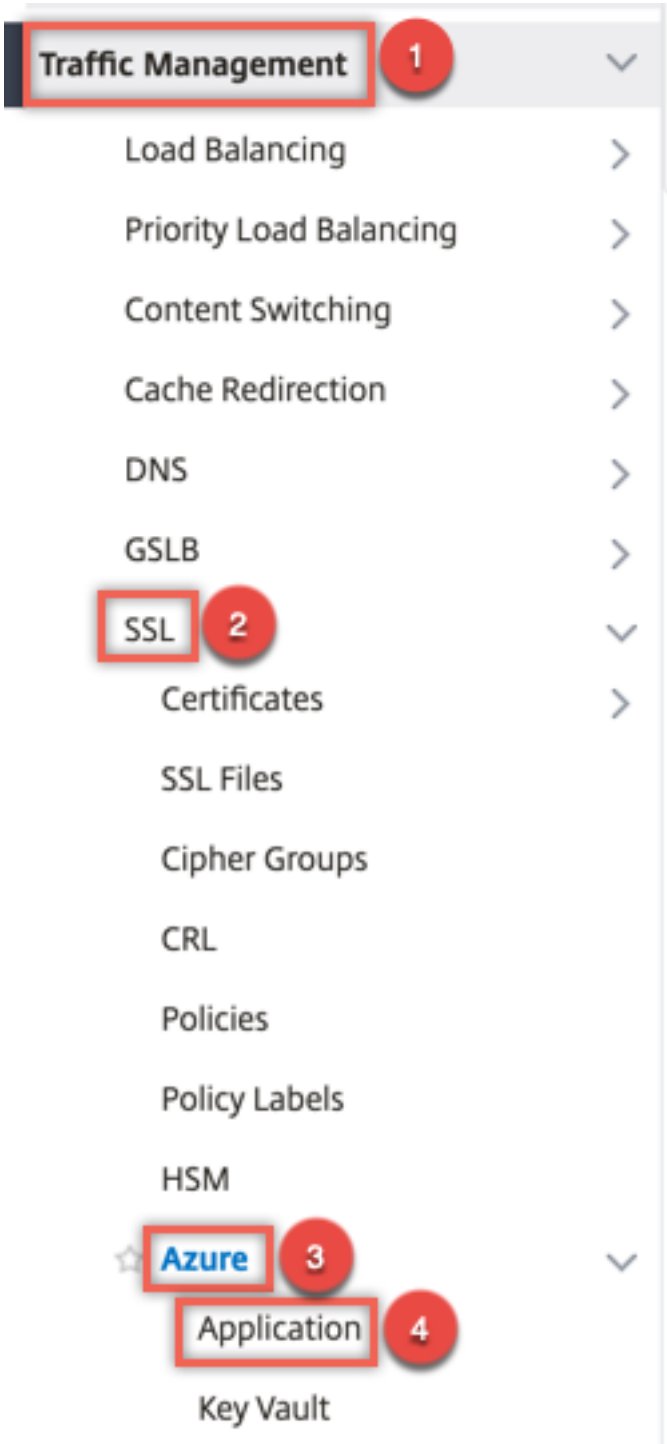
Beispiel:

```
add azure application app10 -clientiD 12345t23aaa5 -clientsecret
   csHzOoEzmuY= -vaultResource example.vault.azure.net -tenantID 33583
   ee9ca5b
 Done
> sh azure application app10
1)  Name:  app10            ClientID:  12345t23aaa5
    TokenEndpoint:  ”https://login.microsoftonline.com/33583ee9ca5b/”
    TenantID:  33583ee9ca5b  VaultResource:  example.vault.azure.net
 Done

<!--NeedCopy-->
```

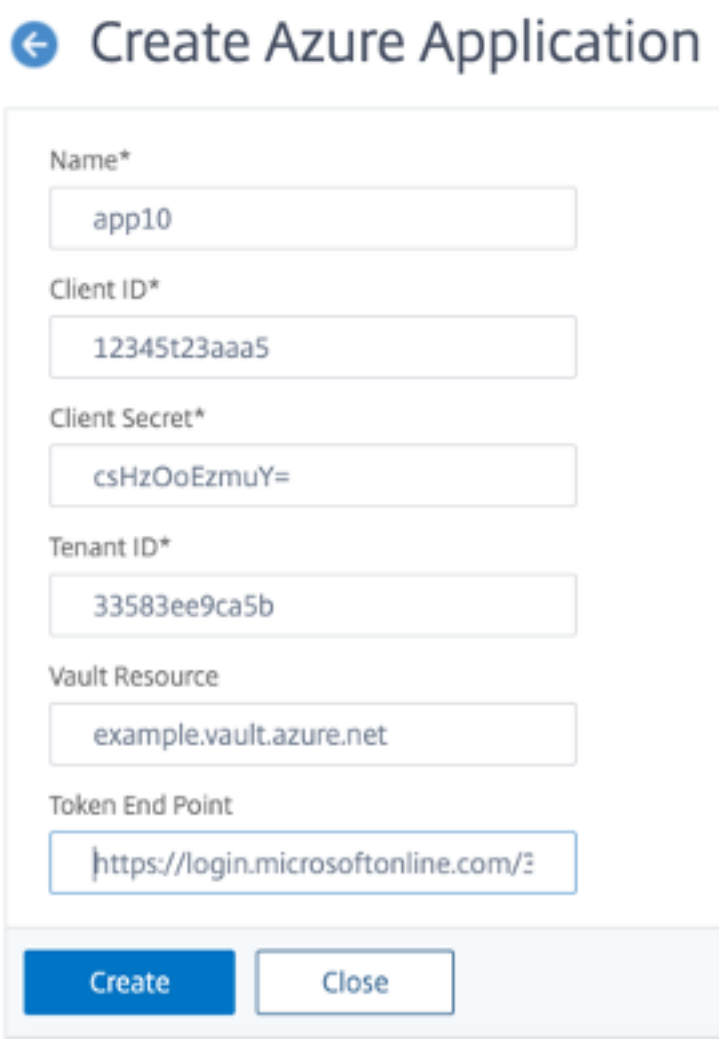
So konfigurieren Sie eine Azure-Anwendung mithilfe der GUI

1. Navigieren Sie zu **Traffic Management > SSL > Azure > Anwendung**.



2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie Werte für die folgenden Parameter ein:
   - Name — Name für das Anwendungsobjekt auf der Citrix ADC Appliance.
   - Client-ID — Anwendungs-ID, die generiert wird, wenn eine Anwendung in Azure Active Directory mithilfe der Azure CLI oder des Azure-Portals (GUI) erstellt wird.

- Clientgeheimnis — Kennwort für die in Azure Active Directory konfigurierte Anwendung. Das Kennwort wird in der Azure CLI angegeben oder im Azure-Portal (GUI) generiert.
- Mandanten-ID — ID des Verzeichnisses in Azure Active Directory, in dem die Anwendung erstellt wurde.
- Tresorressource — Tresorresorressource, für die Zugriffstoken gewährt wird Beispiel `vault.azure.net`.
- Token-Endpunkt — URL, von der aus das Zugriffstoken abgerufen werden kann. Wenn der Token-Endpunkt nicht angegeben ist, ist der Standardwert `https://login.microsoftonline.com/<tenant id>`.



Konfigurieren von Azure Key Vault

Erstellen Sie ein Azure Key Vault-Objekt auf der ADC-Appliance.

So konfigurieren Sie Azure Key Vault mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add azure keyVault <name> -azureVaultName <string> -azureApplication
       <string>
show azure keyvault
<!--NeedCopy-->
```

Beispiel:

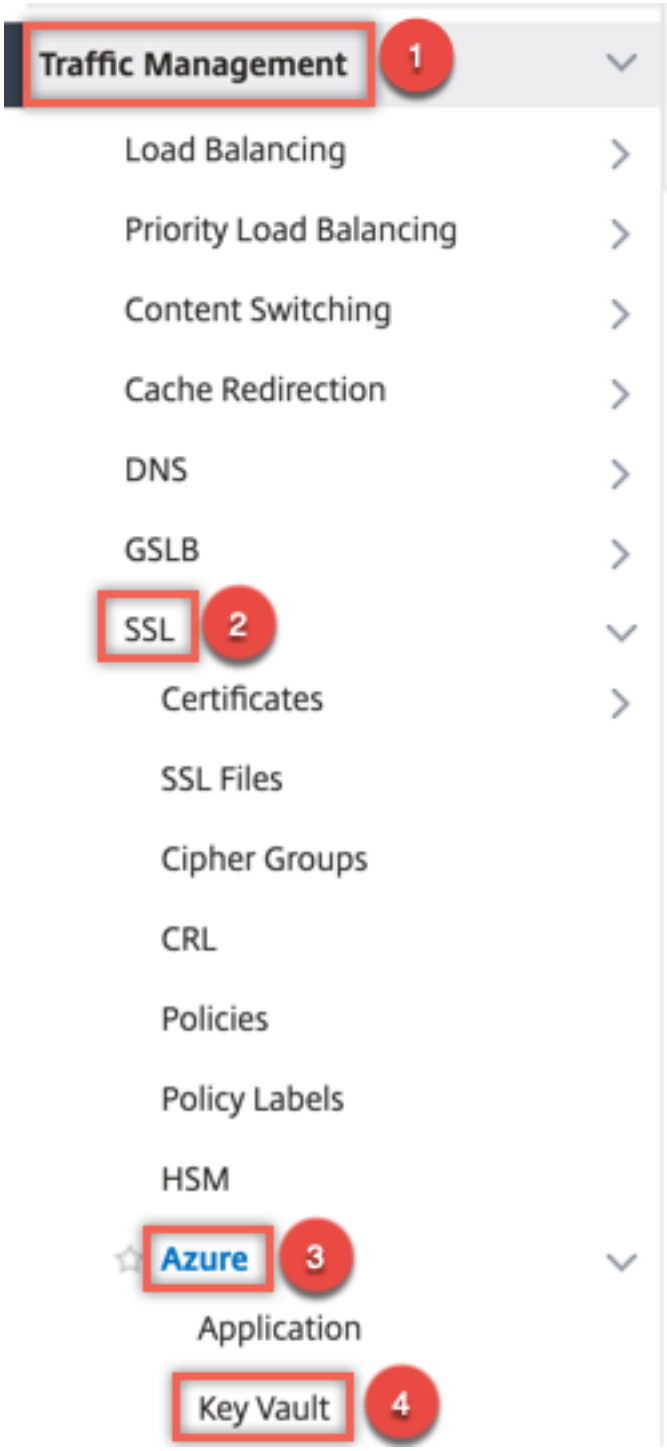
```
add azure keyvault kv1 -azureapplication app10 -azurevaultName pctest.
   vault.azure.net
> sh azure keyVault
1)  Name:  kv1              AzureVaultName:  pctest.vault.azure.net
  AzureApplication:  app10  State:  "Access token obtained"
 Done
<!--NeedCopy-->
```

In der folgenden Tabelle sind die verschiedenen Werte aufgeführt, die der Status des Azure Key Vault annehmen kann, zusammen mit einer kurzen Beschreibung der einzelnen Status.

Status	Beschreibung
`Created`	Anfangszustand des Key Vault-Objekts. Die Authentifizierung wurde nicht versucht.
`Could not reach token end point`	Weist auf einen der folgenden Punkte hin: DNS-Server nicht konfiguriert, Ausstellerzertifikat, das nicht an eine CA-Zertifikatsgruppe gebunden ist, oder Netzwerkprobleme.
`Authorization failed`	Falsche Anmeldeinformationen für die Anwendung.
`Token parse error`	Die Antwort von Azure Active Directory hat nicht das erwartete Format.
`Access token obtained`	Erfolgreich von Azure Active Directory authentifiziert.

So konfigurieren Sie den Azure Key Vault mithilfe der GUI

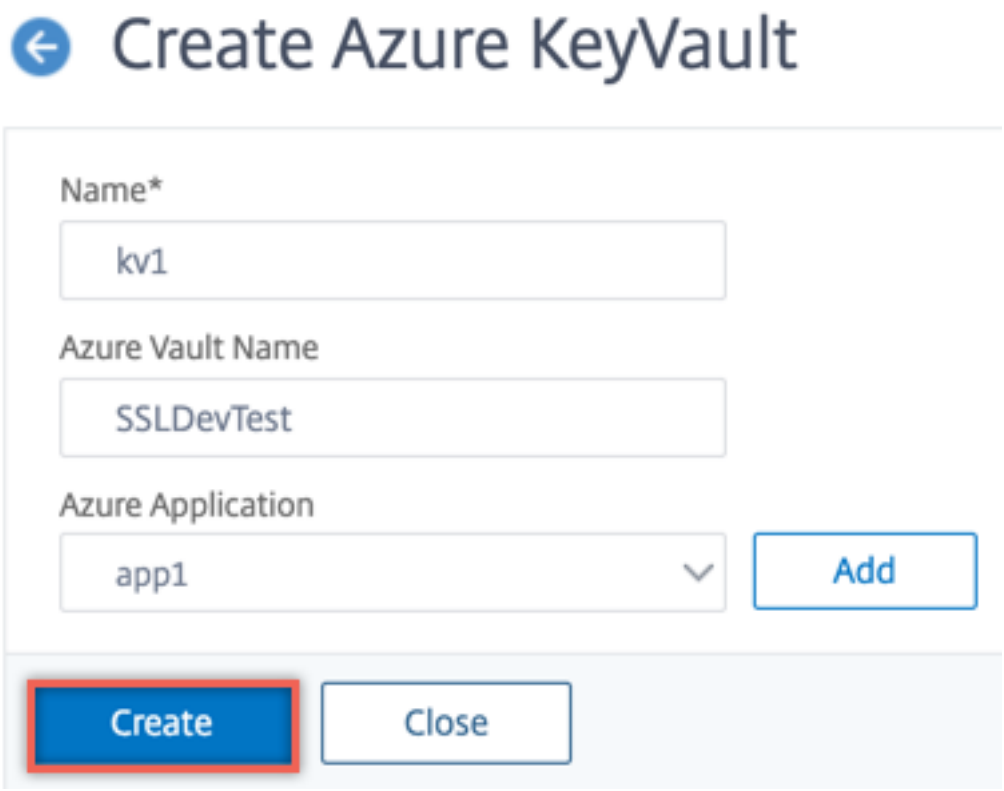
1. Navigieren Sie zu **Traffic Management > SSL > Azure > Schlüsseltresor**.



2. Geben Sie Werte für die folgenden Parameter ein:

   - Name — Name für den Schlüsseltresor.
   - Azure Key Vault Name — Name des Schlüsseltresors, der in Azure Cloud mithilfe der Azure CLI oder des Azure-Portals (GUI) mit Domänennamen konfiguriert wurde.
   - Azure Application Name — Name des Azure Application-Objekts, das auf der ADC Appli-

ance erstellt wurde. Das Azure Application-Objekt mit diesem Namen wird für die Authentifizierung mit Azure Active Directory verwendet.



HSM-Schlüssel hinzufügen

Das Speichern Ihres privaten Schlüssels im HSM gewährleistet die Konformität mit FIPS 140-2 Level 2.

So fügen Sie einen HSM-Schlüssel mit der CLI hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ssl hsmKey <hsmKeyName> [-hsmType <hsmType>] [-key <string> |
       -serialNum <string>] {
 -password  }
  [-keystore <string>]
<!--NeedCopy-->
```

Beispiel:

```
add ssl hsmKey h1 -keystore kv1 -key san15key -hsmType KEYVAULT
```



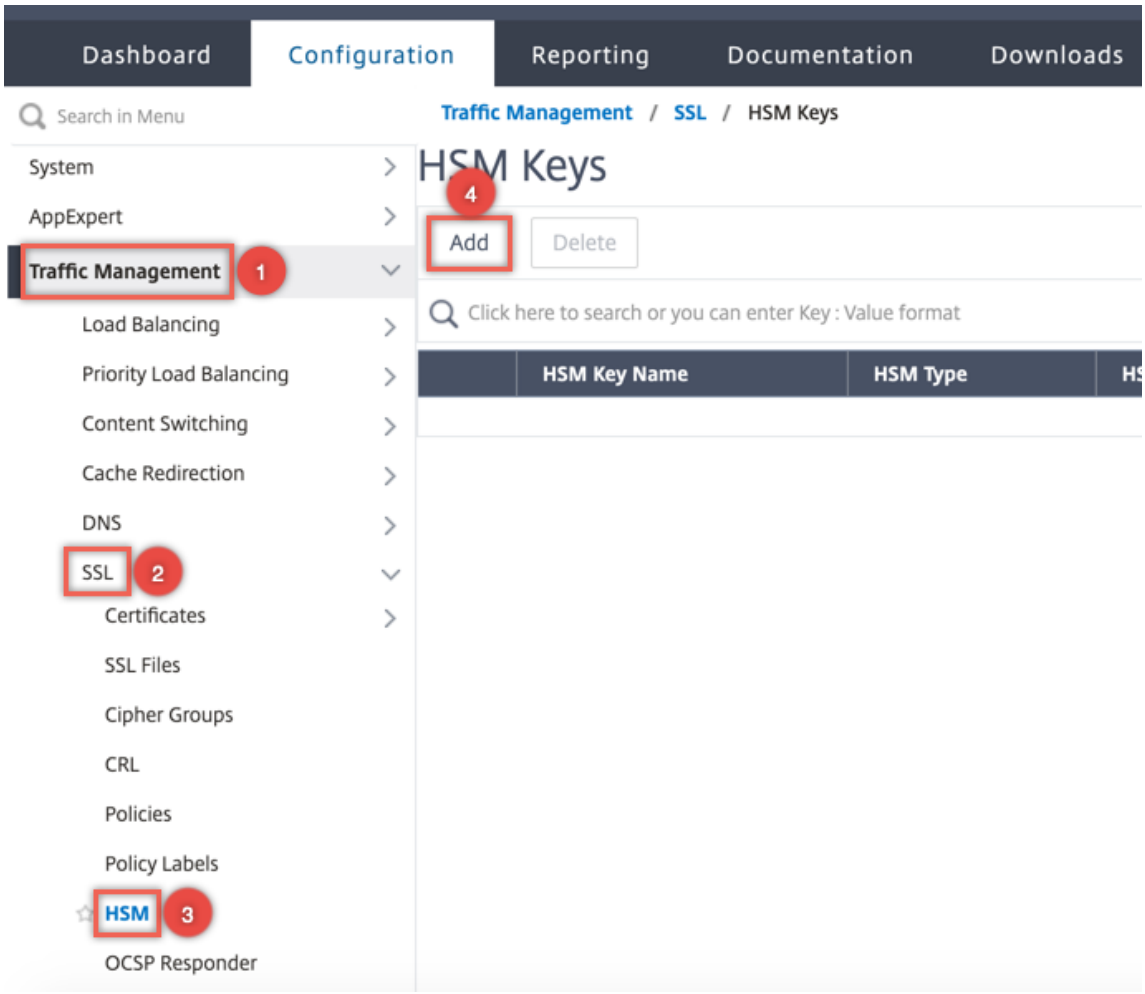
```
2
3
4  > sh ssl hsmKey h1
5      HSM Key Name: h1       Type: KEYVAULT
6      Key: san15key
7      Key store: kv1
8      State:  “Created”
9   Done
10 <!--NeedCopy-->
```

In der folgenden Tabelle sind die verschiedenen Werte aufgeführt, die der Status eines HSM-Schlüssels annehmen kann, zusammen mit einer kurzen Beschreibung der einzelnen Status.

Status	Beschreibung
Created	Der HSM-Schlüssel wird auf der ADC-Appliance hinzugefügt. Eine Schlüsseloperation wird noch nicht versucht.
Zugriffstoken nicht verfügbar	Zugriffstoken ist nicht verfügbar, als eine Schlüsseloperation versucht wurde.
Nicht autorisiert	Die konfigurierte Azure-Anwendung ist nicht berechtigt, den Schlüsselvorgang auszuführen.
Existiert nicht	Der Schlüssel ist im Azure Key Vault nicht vorhanden.
Unerreichbar	Der Key Vault-Host ist im Netzwerk nicht erreichbar.
Markiert	Die HSM-Taste ist auf der ADC-Appliance aufgrund von Schwellenwertfehlern während des Schlüsselbetriebs mit DOWN gekennzeichnet.
Wichtige Vorgänge waren erfolgreich	Antwort auf Erfolg vom Schlüsseltresor für den Schlüsselbetrieb erhalten.
Wichtige Operationen sind fehlgeschlagen	Fehlerantwort von Key Vault für den Schlüsselbetrieb erhalten.
Tastenbetrieb gedrosselt	Die Anforderung der Schlüsseloperation wird durch den Schlüsseltresor gedrosselt.

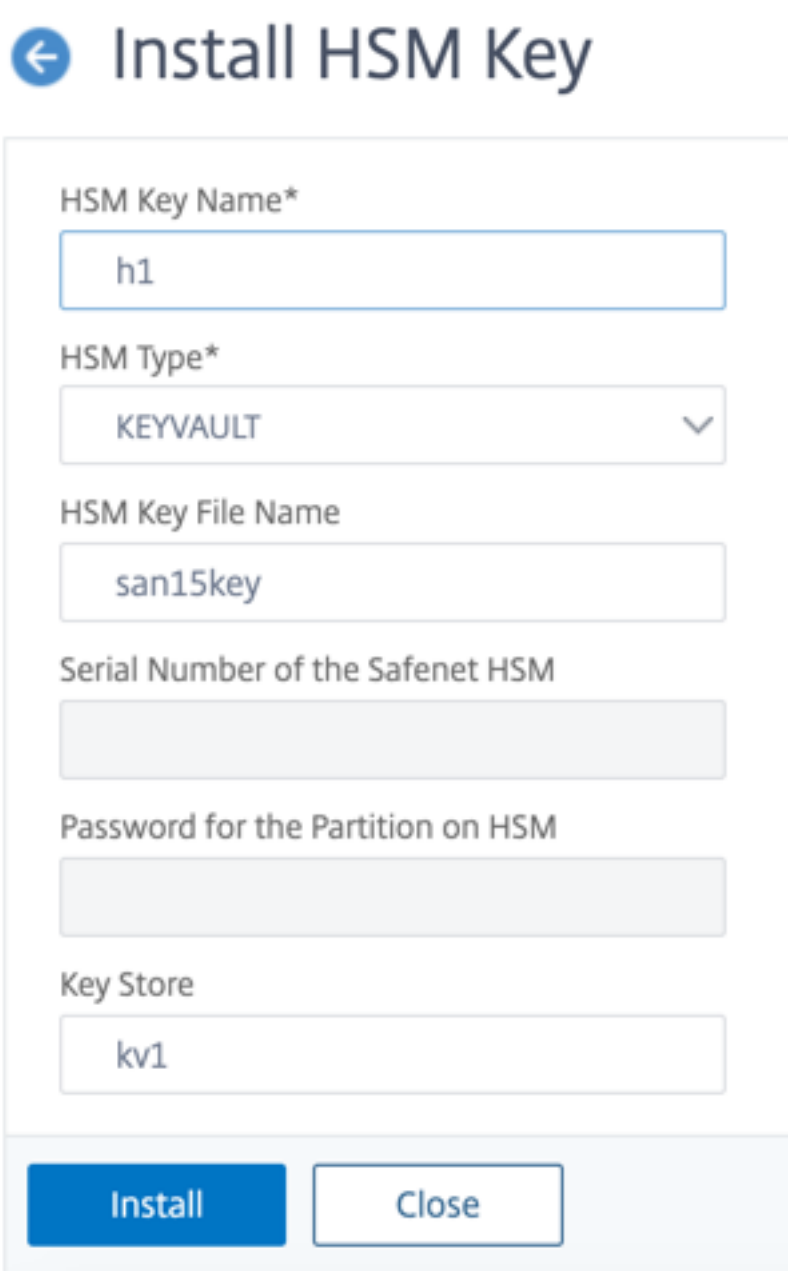
So fügen Sie einen HSM-Schlüssel mithilfe der GUI hinzu

1. Navigieren Sie zu **Traffic Management > SSL > HSM**.



2. Geben Sie Werte für die folgenden Parameter ein.

   - HSM-Schlüsselname — Name des Schlüssels.
   - HSM-Typ — Typ des HSM.
   - Schlüsselspeicher — Name des Schlüsselspeicherobjekts, das HSM darstellt, in dem der Schlüssel gespeichert ist. Beispiel: Name des Key Vault-Objekts oder Azure Key Vault-Authentifizierungsobjekts. Gilt nur für den KEYVAULT Typ HSM.



3. Klicken Sie auf **Hinzufügen**.

Fügen Sie ein Zertifikatschlüsselpaar hinzu

Fügen Sie ein Zertifikatsschlüsselpaar mit dem zuvor erstellten HSM-Schlüssel hinzu.

So fügen Sie ein Zertifikatsschlüsselpaar mit der CLI hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

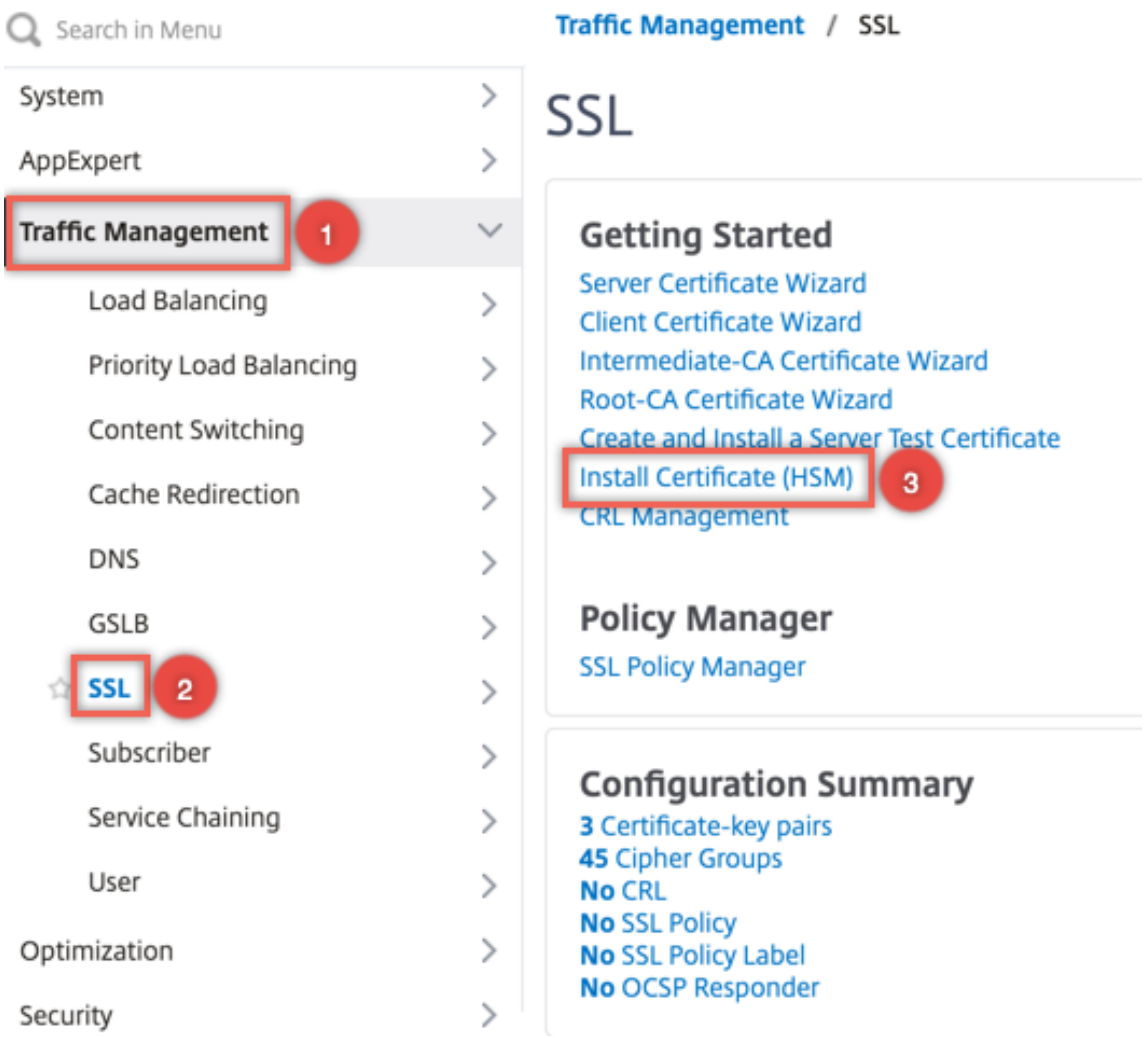

```
add ssl certKey <certkeyName> (-cert <string> [-password]) -hsmKey <
    string>]
show ssl certkey
<!--NeedCopy-->
```

Beispiel:

```
add ssl certKey serverrsa_2048 -cert /nsconfig/ssl/san_certs/san15.pem
    -hsmKey h1
> sh ssl certkey serverrsa_2048
     Name: serverrsa_2048        Status: Valid,   Days to expiration
        :9483
     Version: 3
     Serial Number: F5CFF9EF1E246022
     Signature Algorithm: sha256WithRSAEncryption
     Issuer:  C=in,O=citrix,CN=ca
     Validity
         Not Before: Mar 20 05:42:57 2015 GMT
         Not After : Mar 12 05:42:57 2045 GMT
     Certificate Type:   "Server Certificate"
     Subject:  C=in,O=citrix
     Public Key Algorithm: rsaEncryption
     Public Key size: 2048
     Ocsp Response Status: NONE
 Done
<!--NeedCopy-->
```

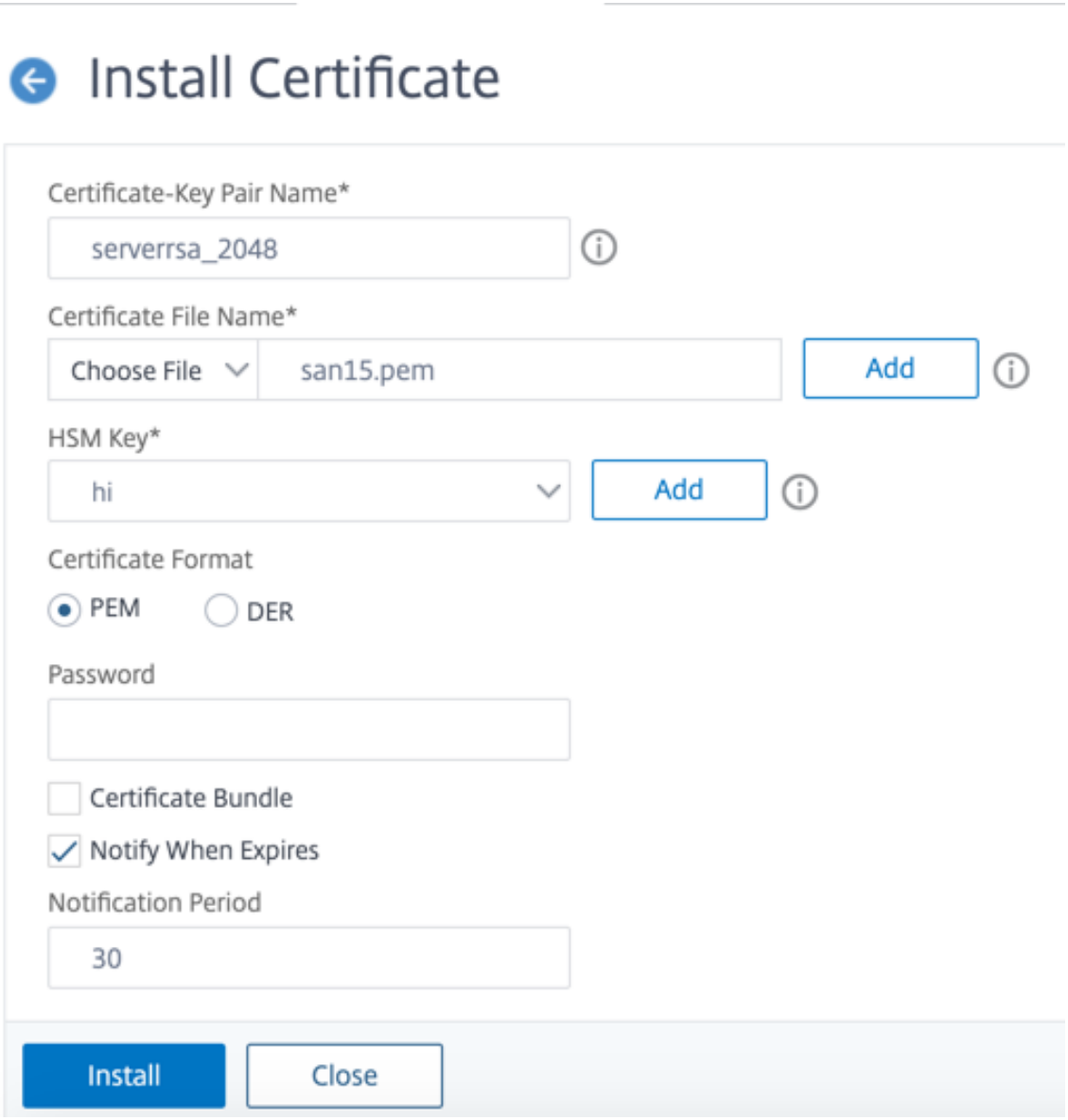
So fügen Sie ein Zertifikatsschlüsselpaar mithilfe der GUI hinzu

1. Navigieren Sie zu **Traffic Management > SSL > Zertifikat (HSM) installieren**.



2. Geben Sie Werte für die folgenden Parameter ein:

   - Name des Zertifikatschlüssel-Paars
   - Name der Zertifikatsdatei
   - HSM-Schlüssel



3. Klicken Sie auf **Installieren**.

Binden Sie das Zertifikatsschlüsselpaar an einen virtuellen Server

Das für die Verarbeitung von SSL-Transaktionen verwendete Zertifikat muss an den virtuellen Server gebunden sein, der die SSL-Daten empfängt.

So binden Sie das SSL-Zertifikatsschlüsselpaar mithilfe der CLI an einen virtuellen Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>
show ssl vserver <vServerName>
```



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

Beispiel:

```
bind ssl vserver v1 -certkeyName serverrsa_2048

sh ssl vserver v1

    Advanced SSL configuration for VServer v1:
    DH: DISABLED
    DH Private-Key Exponent Size Limit: DISABLED    Ephemeral RSA:
       ENABLED      Refresh Count: 0
    Session Reuse: ENABLED      Timeout: 120 seconds
    Cipher Redirect: DISABLED
    ClearText Port: 0
    Client Auth: DISABLED
    SSL Redirect: DISABLED
    Non FIPS Ciphers: DISABLED
    SNI: DISABLED
    OCSP Stapling: DISABLED
    HSTS: DISABLED
    HSTS IncludeSubDomains: NO
    HSTS Max-Age: 0
    HSTS Preload: NO
    SSLv3: ENABLED  TLSv1.0: ENABLED  TLSv1.1: ENABLED  TLSv1.2:
       ENABLED  TLSv1.3: DISABLED
    Push Encryption Trigger: Always
    Send Close-Notify: YES
    Strict Sig-Digest Check: DISABLED
    Zero RTT Early Data: DISABLED
    DHE Key Exchange With PSK: NO
    Tickets Per Authentication Context: 1

    ECC Curve: P_256, P_384, P_224, P_521

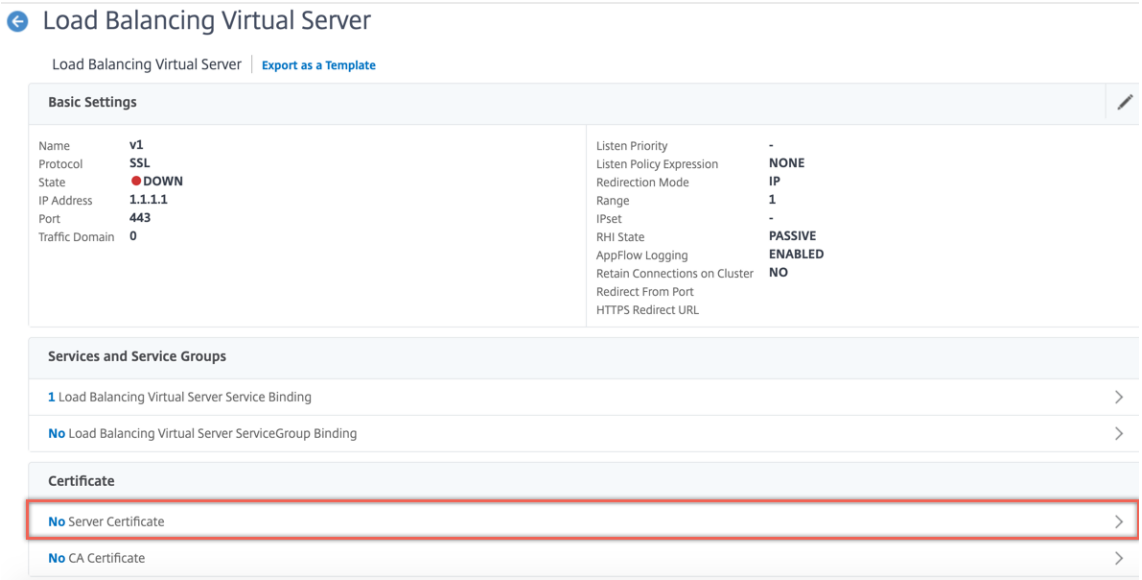
1)  CertKey Name: serverrsa_2048    Server Certificate



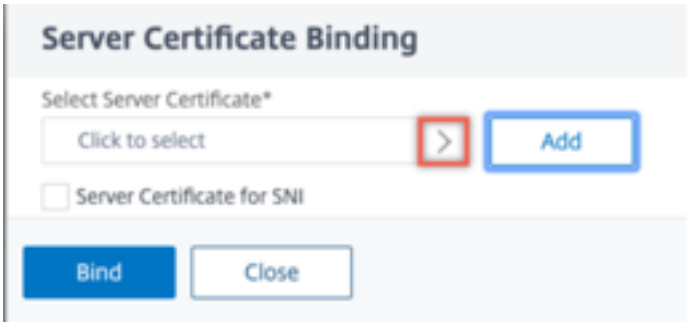
1)  Cipher Name: DEFAULT
    Description: Default cipher list with encryption strength >= 128bit
 Done
<!--NeedCopy-->
```


So binden Sie ein SSL-Zertifikatsschlüsselpaar mithilfe der GUI an einen virtuellen Server

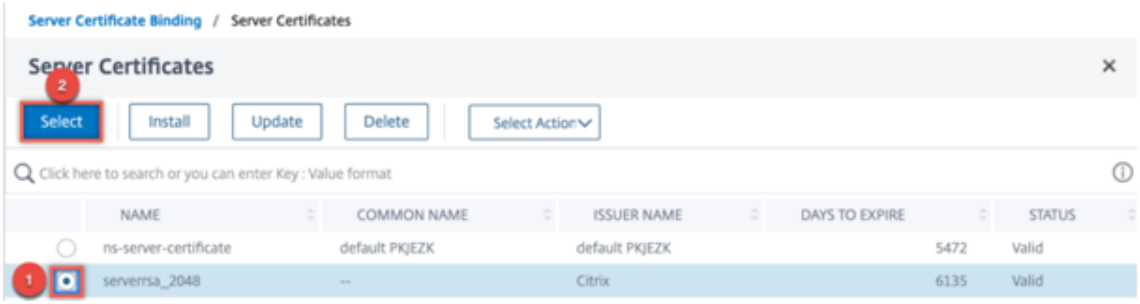
1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server** und öffnen Sie einen virtuellen SSL-Server. Klicken Sie in den Abschnitt Zertifikat.



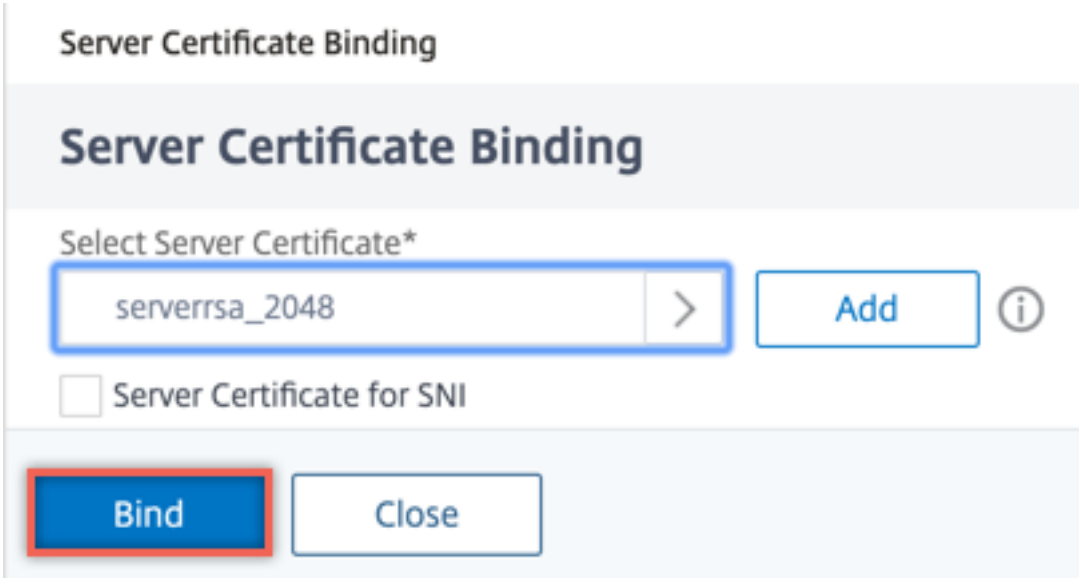
2. Klicken Sie auf den Pfeil, um das Zertifikatsschlüsselpaar auszuwählen.



3. Wählen Sie das Zertifikatsschlüsselpaar aus der Liste aus.



4. Binden Sie das Zertifikatsschlüsselpaar an den virtuellen Server.



Einschränkungen

- Die Anzahl der gleichzeitigen Aufrufe des Azure Key Vault für wichtige Vorgänge ist begrenzt. Die Leistung der ADC-Appliance hängt von den Grenzwerten für Key Vault ab. Weitere Informationen finden Sie unter Microsoft Azure Key Vault-Dokumentation.
- EC-Schlüssel werden nicht unterstützt.
- EDT- und DTLS-Protokolle werden nicht unterstützt.
- ADC-Geräte mit Intel Coleto SSL-Chips werden nicht unterstützt.
- Clustering und Adminpartitionen werden nicht unterstützt.
- Sie können die Azure Application Entity, das Azure Key Vault-Objekt und das HSM-Zertifikatsschlüsselpaar nicht aktualisieren, nachdem Sie sie der ADC-Appliance hinzugefügt haben.
- Ein Zertifikatspaket mit HSM-Schlüsseln wird nicht unterstützt.
- Ein Fehler tritt nicht auf, wenn der HSM-Schlüssel und das Zertifikat nicht übereinstimmen. Stellen Sie beim Hinzufügen eines Zertifikatsschlüsselpaars sicher, dass der HSM-Schlüssel und das Zertifikat übereinstimmen.
- Sie können keinen HSM-Schlüssel an einen virtuellen DTLS-Server binden.
- Sie können OCSP-Anfragen nicht mit einem Zertifikatsschlüsselpaar signieren, das mit einem HSM-Schlüssel erstellt wurde.
- Sie können kein Zertifikatsschlüsselpaar an einen SSL-Dienst binden, wenn das Zertifikatsschlüsselpaar mit einem HSM-Schlüssel erstellt wird.

Häufig gestellte Fragen

Werden bei der Integration in Azure Key Vault private Schlüssel im Speicher der ADC Appliance gespeichert?

Nein, private Schlüssel werden nicht im Speicher der ADC Appliance gespeichert. Für jede SSL-Transaktion sendet die Appliance eine Anfrage an Key Vault.

Ist die Integration FIPS 140-2 Level 2 konform?

Ja, die integrierte Lösung bietet FIPS 140-2 Level 2-Unterstützung.

Welche Schlüsseltypen werden unterstützt?

Es werden nur RSA-Schlüsseltypen unterstützt.

Welche Schlüsselgrößen werden unterstützt?

1024-Bit-, 2048-Bit- und 4096-Bit-RSA-Schlüssel werden unterstützt.

Welche Chiffern werden unterstützt?

Alle auf der ADC-Appliance unterstützten Verschlüsselungen, einschließlich TLSv1.3-Verschlüsselungen mit ECDHE und SHA256, werden unterstützt.

Werden Transaktionen protokolliert?

Die ADC-Appliance protokolliert jede Transaktion, die sie mit dem Schlüsseltresor tätigt. Details wie Uhrzeit, Tresor-IP-Adresse, Port, Erfolg oder Misserfolg der Verbindung und Fehler werden protokolliert.
Im Folgenden finden Sie eine SSL-Protokollausgabe.

```
Apr  9 16:35:30 <local0.debug> 10.102.57.30 04/09/2019:16:35:30 GMT
      0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUCCESS 896 0 :
     Backend SPCBId 30894 - ServerIP 104.211.224.186 - ServerPort 443
      - ProtocolVersion TLSv1.2 - CipherSuite "ECDHE-RSA-AES256-GCM-
     SHA384 TLSv1.2 Non-Export 256-bit" - Session New -
     SERVER_AUTHENTICATED -SerialNumber "200005
     A75B04365827852D630000000005A75B" - SignatureAlgorithm "
     sha256WithRSAEncryption" - ValidFrom "Mar 17 03:28:42 2019 GMT"
     - ValidTo "Mar 17 03:28:42 2021 GMT" - HandshakeTime 40 ms
```



```
2 Apr  9 16:35:30 <local0.debug> 10.102.57.30 04/09/2019:16:35:30 GMT
      0-PPE-0 : default SSLLOG SSL_HANDSHAKE_ISSUERNAME 897 0 :
    SPCBId 30894 - IssuerName " C=US,ST=Washington,L=Redmond,O=
    Microsoft Corporation,OU=Microsoft IT,CN=Microsoft IT TLS CA 2"
3 Apr  9 16:35:30 <local0.debug> 10.102.57.30 04/09/2019:16:35:30 GMT
      0-PPE-0 : default SSLLOG SSL_HANDSHAKE_SUBJECTNAME 898 0 :
    SPCBId 30894 - SubjectName " CN=vault.azure.net"
4 <!--NeedCopy-->
```

Problembehandlung

October 5, 2021

Wenn die SSL-Funktion nach der Konfiguration nicht wie erwartet funktioniert, können Sie einige gängige Tools verwenden, um auf Citrix ADC Ressourcen zuzugreifen und das Problem zu diagnostizieren.

Ressourcen für die Fehlerbehebung

Verwenden Sie die folgenden Ressourcen, um ein SSL-Problem auf einer Citrix ADC Appliance zu beheben, um optimale Ergebnisse zu erzielen:

- Die relevante ns.log-Datei
- Die neueste ns.conf-Datei
- Die Meldungsdatei
- Die relevante`newnslog` Datei
- Trace-Dateien
- Eine Kopie der Zertifikatdateien, wenn möglich
- Eine Kopie der Schlüsseldatei, wenn möglich
- Die Fehlermeldung, falls vorhanden

Zusätzlich zu diesen Ressourcen können Sie die Wireshark-Anwendung verwenden, die für die Citrix ADC Ablaufverfolgungsdateien angepasst ist, um die Fehlerbehebung zu beschleunigen.

Beheben von SSL-Problemen

Gehen Sie wie folgt vor, um ein SSL-Problem zu beheben:

- Stellen Sie sicher, dass die Citrix ADC Appliance für SSL-Abladung und Lastausgleich lizenziert ist.

- Stellen Sie sicher, dass SSL-Offloading- und Lastausgleichsfunktionen auf der Appliance aktiviert sind.
- Stellen Sie sicher, dass der Status des virtuellen SSL-Servers nicht als DOWN angezeigt wird.
- Stellen Sie sicher, dass der Status des an den virtuellen Server gebundenen Dienstes nicht als DOWN angezeigt wird.
- Stellen Sie sicher, dass ein gültiges Zertifikat an den virtuellen Server gebunden ist.
- Stellen Sie sicher, dass der Dienst einen geeigneten Port verwendet, vorzugsweise Port 443.

Entschlüsseln des TLS1.3-Datenverkehrs aus der Paketverfolgung

Um Protokolle zu beheben, die über TLS1.3 ausgeführt werden, müssen Sie zuerst den TLS1.3-Datenverkehr entschlüsseln. Um TLS 1.3 in Wireshark zu entschlüsseln, müssen die Geheimnisse imNSS Schlüsselprotokollformat exportiert werden. Weitere Informationen zum Schlüsselprotokollformat finden Sie unter NSS Key Log Format.

Informationen zum Erfassen einer Paketverfolgung finden Sie unter Erfassen von SSL-Sitzungsschlüsseln während einer Ablaufverfolgung.

Hinweis: Citrix ADC protokolliert automatisch die Geheimnisse jeder Verbindung im entsprechenden Format für die verwendete TLS/SSL-Protokollversion.

CRL-Aktualisierung erfolgt nicht auf dem sekundären Knoten in einem HA-Setup

Die Aktualisierung erfolgt nicht, da der CRL-Server nur für den primären Knoten über ein privates Netzwerk zugänglich ist.

Problemumgehung: Fügen Sie einen Dienst auf dem primären Knoten mit der IP-Adresse des CRL-Servers hinzu. Dieser Dienst fungiert als Proxy für den CRL-Server. Wenn die Konfiguration zwischen den Knoten synchronisiert wird, funktioniert die CRL-Aktualisierung sowohl für primäre als auch für sekundäre Knoten über den Dienst, der auf dem primären Knoten konfiguriert ist.

Häufig gestellte Fragen zu SSL

October 5, 2021

Grundlegende Fragen

Der HTTPS-Zugriff auf die GUI schlägt auf einer VPX-Instanz fehl. Wie erhalte ich Zugang?

Für den HTTPS-Zugriff auf die GUI ist ein Zertifikatschlüsselpaar erforderlich. Auf einer Citrix ADC-Appliance wird ein Zertifikatschlüsselpaar automatisch an die internen Dienste gebunden.

Auf einer MPX- oder SDX-Appliance beträgt die Standardschlüsselgröße 1024 Byte, und bei einer VPX-Instanz beträgt die Standardschlüsselgröße 512 Byte. Die meisten Browser akzeptieren heute jedoch keinen Schlüssel mit weniger als 1024 Bytes. Infolgedessen wird der HTTPS-Zugriff auf das VPX-Konfigurationsdienstprogramm blockiert.

Citrix empfiehlt, ein Zertifikatschlüsselpaar von mindestens 1024 Byte zu installieren und es an den internen Dienst für den HTTPS-Zugriff auf das Konfigurationsdienstprogramm zu binden. Aktualisieren Sie alternativ den `ns-server-certificate` auf 1024 Bytes. Sie können den HTTP-Zugriff auf das Konfigurationsdienstprogramm oder die CLI verwenden, um das Zertifikat zu installieren.

Wenn ich einer MPX-Appliance eine Lizenz hinzufüge, geht die Bindung des Zertifikatschlüsselpaars verloren. Wie löse ich dieses Problem?

Wenn beim Start keine Lizenz auf einer MPX-Appliance vorhanden ist und Sie später eine Lizenz hinzufügen und die Appliance neu starten, verlieren Sie möglicherweise die Zertifikatbindung. Installieren Sie das Zertifikat neu und binden Sie es an den internen Dienst

Citrix empfiehlt, vor dem Starten der Appliance eine entsprechende Lizenz zu installieren.

Was sind die verschiedenen Schritte beim Einrichten eines sicheren Kanals für eine SSL-Transaktion?

Das Einrichten eines sicheren Kanals für eine SSL-Transaktion umfasst die folgenden Schritte:

1. Der Client sendet eine HTTPS-Anfrage für einen sicheren Kanal an den Server.
2. Nach Auswahl des Protokolls und der Verschlüsselung sendet der Server sein Zertifikat an den Client.
3. Der Client überprüft die Authentizität des Serverzertifikats.
4. Wenn eine der Prüfungen fehlschlägt, zeigt der Client das entsprechende Feedback an.
5. Wenn die Schecks bestehen oder der Kunde sich entscheidet, fortzufahren, auch wenn eine Überprüfung fehlschlägt, erstellt der Kunde einen temporären, wegwerfbaren Schlüssel. Dieser Schlüssel wird als *Pre-Master-Geheimnis* bezeichnet und der Client verschlüsselt diesen Schlüssel mithilfe des öffentlichen Schlüssels des Serverzertifikats.
6. Der Server entschlüsselt es nach Erhalt des Pre-Master-Geheimnisses mit dem privaten Schlüssel des Servers und generiert die Sitzungsschlüssel. Der Client generiert auch die Sitzungsschlüssel aus dem Pre-Master-Geheimnis. Daher haben sowohl Client als auch Server jetzt einen gemeinsamen Sitzungsschlüssel, der zur Verschlüsselung und Entschlüsselung von Anwendungsdaten verwendet wird.

Ich verstehe, dass SSL ein CPU-intensiver Prozess ist. Wie hoch sind die CPU-Kosten im Zusammenhang mit dem SSL-Prozess?

Die folgenden beiden Phasen sind mit dem SSL-Prozess verbunden:

- Der erste Handshake und die sichere Kanaleinrichtung unter Verwendung der öffentlichen und privaten Schlüsseltechnologie.
- Massendatenverschlüsselung unter Verwendung der symmetrischen Schlüsseltechnologie.

Beide vorangegangenen Phasen können sich auf die Serverleistung auswirken und erfordern aus folgenden Gründen eine intensive CPU-Verarbeitung:

1. Der erste Handshake beinhaltet Kryptographie mit öffentlich-privaten Schlüsseln, die aufgrund großer Schlüsselgrößen (1024 Bit, 2048 Bit, 4096 Bit) sehr CPU-intensiv ist.
2. Die Verschlüsselung/Entschlüsselung von Daten ist ebenfalls rechnerisch teuer, abhängig von der Datenmenge, die verschlüsselt oder entschlüsselt werden muss.

Was sind die verschiedenen Entitäten einer SSL-Konfiguration?

Eine SSL-Konfiguration hat die folgenden Entitäten:

- Serverzertifikat
- Zertifikat der Zertifizierungsstelle (CA)
- Cipher Suite, die die Protokolle für die folgenden Aufgaben angibt:
  - Anfänglicher Schlüsselaustausch
  - Server- und Clientauthentifizierung
  - Algorithmus zur Massenverschlüsselung
  - Nachrichten-Authentifizierung
- Clientauthentifizierung
- CRL
- SSL Certificate Key Generierung Tool, mit dem Sie die folgenden Dateien erstellen können:
  - Anforderung des Zertifikats
  - Selbstsigniertes Zertifikat
  - RSA-Schlüssel
  - DH-Parameter

Ich möchte die SSL-Entladungsfunktion der Citrix ADC-Appliance verwenden. Welche Möglichkeiten gibt es, ein SSL-Zertifikat zu erhalten?

Sie müssen ein SSL-Zertifikat erhalten, bevor Sie das SSL-Setup auf der Citrix ADC-Appliance konfigurieren können. Sie können eine der folgenden Methoden verwenden, um ein SSL-Zertifikat zu erhalten:

- Fordern Sie ein Zertifikat von einer autorisierten Zertifizierungsstelle (CA) an.

- Verwenden Sie das vorhandene Serverzertifikat.
- Erstellen Sie ein Zertifikatschlüsselpaar auf der Citrix ADC-Appliance.

Hinweis: Dieses Zertifikat ist ein Testzertifikat, das von der Citrix ADC-Appliance generiert wurde, signiert von der Test-Root-CA. Von der Test-Root-CA signierte Testzertifikate werden von Browsern nicht akzeptiert. Der Browser löst eine Warnmeldung aus, die besagt, dass das Zertifikat des Servers nicht authentifiziert werden kann.

- Für andere Zwecke als Testzwecke müssen Sie ein gültiges CA-Zertifikat und einen CA-Schlüssel angeben, um das Serverzertifikat zu signieren.

Was sind die Mindestanforderungen für ein SSL-Setup?

Die Mindestanforderungen für die Konfiguration eines SSL-Setups lauten wie folgt:

- Besorgen Sie sich die Zertifikate und Schlüssel.
- Erstellen Sie einen virtuellen Lastenausgleich SSL-Server.
- Binden Sie HTTP- oder SSL-Dienste an den virtuellen SSL-Server.
- Binden Sie ein Zertifikatschlüsselpaar an den virtuellen SSL-Server.

Was sind die Grenzen für die verschiedenen Komponenten von SSL?

SSL-Komponenten haben folgende Grenzwerte:

- Bitgröße von SSL-Zertifikaten: 4096
- Anzahl der SSL-Zertifikate: Hängt vom verfügbaren Speicher auf der Appliance ab.
- Maximal verknüpfte Zwischenzertifikate CA SSL: 9 pro Kette.
- CRL-Widerrufe: Hängt vom verfügbaren Speicher auf der Appliance ab.

Was sind die verschiedenen Schritte bei der End-to-End-Datenverschlüsselung auf einer Citrix ADC-Appliance?

Die Schritte für den serverseitigen Verschlüsselungsprozess auf einer Citrix ADC-Appliance lauten wie folgt:

1. Der Client stellt eine Verbindung mit dem SSL-VIP her, der auf der Citrix ADC-Appliance am sicheren Standort konfiguriert ist.
2. Nach Erhalt der sicheren Anforderung entschlüsselt die Appliance die Anforderung und wendet Content Switching-Techniken der Layer 4 bis 7 und Load Balancing-Richtlinien an. Anschließend wählt es den besten verfügbaren Back-End-Webserver für die Anforderung aus.
3. Die Citrix ADC-Appliance erstellt eine SSL-Sitzung mit dem ausgewählten Server.

4. Nach dem Einrichten der SSL-Sitzung verschlüsselt die Appliance die Clientanforderung und sendet sie mithilfe der sicheren SSL-Sitzung an den Webserver.
5. Wenn die Appliance die verschlüsselte Antwort vom Server erhält, entschlüsselt und verschlüsselt sie die Daten erneut. Anschließend sendet es die Daten mithilfe der clientseitigen SSL-Sitzung an den Client.

Die Multiplexing-Technik der Citrix ADC-Appliance ermöglicht es der Appliance, SSL-Sitzungen wiederzuverwenden, die mit den Webservern eingerichtet wurden. Daher vermeidet die Appliance den CPU-intensiven Schlüsselaustausch, der als *Full Handshake*bezeichnet wird. Dieser Prozess reduziert die Gesamtzahl der SSL-Sitzungen auf dem Server und gewährleistet die End-to-End-Sicherheit.

Zertifikate und Schlüssel

Kann ich das Zertifikat und die Schlüsseldateien an einem beliebigen Ort ablegen? Gibt es einen empfohlenen Speicherort zum Speichern dieser Dateien?

Sie können das Zertifikat und die Schlüsseldateien auf der Citrix ADC-Appliance oder einem lokalen Computer speichern. Citrix empfiehlt jedoch, das Zertifikat und die Schlüsseldateien im `/nsconfig/ssl` Verzeichnis der Citrix ADC-Appliance zu speichern. Das `/etc` Verzeichnis befindet sich im Flash-Speicher der Citrix ADC-Appliance. Diese Aktion bietet Portabilität und erleichtert die Backup und Wiederherstellung der Zertifikatsdateien auf der Appliance.

Hinweis: Stellen Sie sicher, dass das Zertifikat und die Schlüsseldateien im selben Verzeichnis gespeichert sind.

Wie groß ist die maximale Größe des Zertifikatsschlüssels, der auf der Citrix ADC-Appliance unterstützt wird?

Eine Citrix ADC-Appliance, auf der eine Softwareversion vor Version 9.0 ausgeführt wird, unterstützt eine maximale Zertifikatschlüsselgröße von 2048 Bit. Version 9.0 und höher unterstützt eine maximale Zertifikatschlüsselgröße von 4096 Bit. Diese Grenze gilt für RSA-Zertifikate.

Eine MPX-Appliance unterstützt Zertifikate von 512 Bit bis zu den folgenden Größen:

- 4096-Bit-Serverzertifikat auf dem virtuellen Server
- 4096-Bit-Clientzertifikat im Dienst
- 4096-Bit-CA-Zertifikat (einschließlich Zwischen- und Stammzertifikaten)
- 4096-Bit-Zertifikat auf dem Back-End-Server
- 4096-Bit-Clientzertifikat (wenn die Clientauthentifizierung auf dem virtuellen Server aktiviert ist)

Eine virtuelle Appliance unterstützt Zertifikate von 512 Bit bis zu den folgenden Größen:

- 4096-Bit-Serverzertifikat auf dem virtuellen Server
- 4096-Bit-Clientzertifikat im Dienst
- 4096-Bit-CA-Zertifikat (einschließlich Zwischen- und Stammzertifikaten)
- 4096-Bit-Zertifikat auf dem Back-End-Server von Release 12.0-56.x. Ältere Versionen unterstützen 2048-Bit-Zertifikate.
- 2048-Bit-Clientzertifikat (wenn die Clientauthentifizierung auf dem virtuellen Server aktiviert ist) ab Version 12.0-56.x.

Wie groß ist die maximale Größe des DH-Parameters, der auf der Citrix ADC-Appliance unterstützt wird?

Die Citrix ADC-Appliance unterstützt einen DH-Parameter von maximal 2048 Bit.

Wie hoch ist die maximale Länge der Zertifikatkette, dh die maximale Anzahl von Zertifikaten in einer Kette, die auf einer Citrix ADC-Appliance unterstützt wird?

Eine Citrix ADC-Appliance kann beim Senden einer Serverzertifikatnachricht maximal 10 Zertifikate in einer Kette senden. Eine Kette mit maximaler Länge umfasst das Serverzertifikat und neun Zwischenzertifikate der Zertifizierungsstelle.

Welche Zertifikate und Schlüsselformate werden auf der Citrix ADC-Appliance unterstützt?

Die Citrix ADC-Appliance unterstützt die folgenden Zertifikat- und Schlüsselformate:

- Datenschutz Verbesserte E-Mails (PEM)
- Distinguished Coding Regel (DER)

Gibt es ein Limit für die Anzahl der Zertifikate und Schlüssel, die ich auf der Citrix ADC-Appliance installieren kann?

Nein. Die Anzahl der Zertifikate und Schlüssel, die installiert werden können, ist nur durch den verfügbaren Speicher auf der Citrix ADC-Appliance begrenzt.

Ich habe das Zertifikat und die Schlüsseldateien auf dem lokalen Computer gespeichert. Ich möchte diese Dateien mithilfe des FTP-Protokolls auf die Citrix ADC-Appliance übertragen. Gibt es einen bevorzugten Modus zum Übertragen dieser Dateien auf die Citrix ADC-Appliance?

Ja. Wenn Sie das FTP-Protokoll verwenden, müssen Sie das Zertifikat und die Schlüsseldateien im Binärmodus an die Citrix ADC-Appliance übertragen.

Hinweis: Standardmäßig ist FTP deaktiviert. Citrix empfiehlt, das SCP-Protokoll für die Übertragung von Zertifikats- und Schlüsseldateien zu verwenden. Das Konfigurationsdienstprogramm verwendet implizit SCP, um eine Verbindung mit der Appliance herzustellen.

Was ist der Standardverzeichnispfad für das Zertifikat und den Schlüssel?

Der Standardverzeichnispfad für das Zertifikat und den Schlüssel ist '/nsconfig/ssl'.

Was passiert beim Hinzufügen eines Zertifikats und eines Schlüsselpaars, wenn ich keinen absoluten Pfad zu den Zertifikats- und Schlüsseldateien angebe?

Geben Sie beim Hinzufügen eines Zertifikatschlüsselpaars einen absoluten Pfad zu den Zertifikats- und Schlüsseldateien an. Wenn Sie dies nicht angeben, durchsucht die ADC-Appliance das Standardverzeichnis nach diesen Dateien und versucht, sie in den Kernel zu laden. Das Standardverzeichnis ist `/nsconfig/ssl`. Wenn beispielsweise die cert1024.pem- und rsa1024.pem-Dateien im `/nsconfig/ssl` Verzeichnis der Appliance verfügbar sind, sind beide der folgenden Befehle erfolgreich:

```
1 add ssl certKey cert1 -cert cert1204.pem -key rsa1024.pem
2 <!--NeedCopy-->
```

```
1 add ssl certKey cert1 -cert /nsconfig/ssl/cert1204.pem -key /nsconfig/
     ssl/rsa1024.pem
2 <!--NeedCopy-->
```

Ich habe ein Hochverfügbarkeits-Setup konfiguriert. Ich möchte die SSL-Funktion im Setup implementieren. Wie muss ich mit dem Zertifikat und den Schlüsseldateien in einem Hochverfügbarkeits-Setup umgehen?

In einem Hochverfügbarkeits-Setup müssen Sie das Zertifikat und die Schlüsseldateien sowohl auf der primären als auch auf der sekundären Citrix ADC-Appliance speichern. Der Verzeichnispfad für das Zertifikat und die Schlüsseldateien muss auf beiden Appliances identisch sein, bevor Sie ein SSL-Zertifikatschlüsselpaar auf der primären Appliance hinzufügen.

nCipher nShield® HSM

Müssen wir bei der Integration mit NCipher nShield® HSM eine bestimmte Konfiguration berücksichtigen, wenn wir die Citrix ADC-Appliance zu HA hinzufügen?

Konfigurieren Sie dieselben NCipher-Geräte auf beiden Knoten in HA. nCipher Konfigurationsbefehle werden nicht in HA synchronisiert. Informationen zu den Voraussetzungen für NCipher nShield® HSM finden Sie unter Voraussetzungen.

Müssen wir beide Appliances individuell mit nCipher nShield® HSM und RFS integrieren? Müssen wir diese Aktion vor oder nach dem HA-Setup abschließen?

Sie können die Integration vor oder nach dem HA-Setup abschließen. Wenn die Integration nach dem HA-Setup erfolgt, werden die Schlüssel, die vor der Konfiguration des sekundären Knotens auf den primären Knoten importiert wurden, nicht mit dem sekundären Knoten synchronisiert. Daher empfiehlt Citrix die NCipher Integration vor dem HA-Setup.

Müssen wir den Schlüssel sowohl in die primäre als auch in die sekundären Citrix ADC-Appliances importieren oder werden die Schlüssel vom primären Knoten mit dem sekundären Knoten synchronisiert?

Wenn NCipher vor der Bildung des HA auf beiden Geräten integriert ist, werden die Schlüssel während der Integration automatisch von RFS synchronisiert.

Angesichts der Tatsache, dass sich das HSM nicht auf der Citrix ADC-Appliance, sondern auf nCipher befindet, was passiert mit den Schlüsseln und Zertifikaten, wenn ein Knoten ausfällt und ersetzt wird?

Wenn ein Knoten ausfällt, können Sie die Schlüssel und Zertifikate mit dem neuen Knoten synchronisieren, indem Sie nCipher auf den neuen Knoten integrieren. Führen Sie dann die folgenden Befehle aus:

```
1 sync ha files ssl
2 force ha sync
3 <!--NeedCopy-->
```

Die Zertifikate werden synchronisiert und hinzugefügt, wenn die Schlüssel bei der Integration von nCipher synchronisiert werden.

Chiffern

Was ist eine Null-Chiffre?

Chiffern ohne Verschlüsselung werden als Null-Chiffers bezeichnet. Zum Beispiel ist NULL-MD5 eine Null-Chiffre.

Sind die Null-Chiffern standardmäßig für einen SSL-VIP oder einen SSL-Dienst aktiviert?

Nein. Null-Chiffern sind für einen SSL-VIP oder einen SSL-Dienst standardmäßig nicht aktiviert.

Wie ist das Verfahren zum Entfernen von Null-Chiffern?

Um die Null-Chiffern aus einem SSL-VIP zu entfernen, führen Sie den folgenden Befehl aus:

```
bind ssl cipher <SSL_VIP> REM NULL
<!--NeedCopy-->
```

Um die Null-Chiffern aus einem SSL-Dienst zu entfernen, führen Sie den folgenden Befehl aus:

```
bind ssl cipher <SSL_Service> REM NULL -service
<!--NeedCopy-->
```

Welche verschiedenen Chiffrieraliase werden auf der Citrix ADC-Appliance unterstützt?

Um die auf der Appliance unterstützten Verschlüsselungsaliase aufzulisten, geben Sie an der Eingabeaufforderung Folgendes ein:

```
sh cipher
<!--NeedCopy-->
```

Wie lautet der Befehl zum Anzeigen aller vordefinierten Chiffuren der Citrix ADC-Appliance?

Um alle vordefinierten Chiffuren der Citrix ADC-Appliance anzuzeigen, geben Sie an der CLI Folgendes ein:


```
show ssl cipher
<!--NeedCopy-->
```

Wie lautet der Befehl, um die Details einer einzelnen Chiffre der Citrix ADC-Appliance anzuzeigen?

Um die Details einer einzelnen Chiffre der Citrix ADC-Appliance anzuzeigen, geben Sie an der CLI Folgendes ein:

```
show ssl cipher <Cipher_Name/Cipher_Alias_Name/Cipher_Group_Name>
<!--NeedCopy-->
```

Beispiel:

```
show cipher SSL3-RC4-SHA
     1) Cipher Name: SSL3-RC4-SHA
     Description: SSLv3 Kx=RSA Au=RSA Enc=RC4(128)
    Mac=SHA1
     Done
<!--NeedCopy-->
```

Welche Bedeutung hat das Hinzufügen der vordefinierten Chiffuren der Citrix ADC-Appliance?

Durch das Hinzufügen der vordefinierten Verschlüsselungen der Citrix ADC-Appliance werden die NULL-Ciphers zu einem SSL-VIP oder einem SSL-Dienst hinzugefügt.

Ist es möglich, die Reihenfolge der Chiffre zu ändern, ohne sie von einer Chiffriergruppe auf einer Citrix ADC-Appliance abzubinden?

Ja. Es ist möglich, die Reihenfolge der Chiffre zu ändern, ohne die Chiffren von einer benutzerdefinierten Chiffriergruppe aufzuheben. Sie können die Priorität in eingebauten Chiffriergruppen jedoch nicht ändern. Um die Priorität einer an eine SSL-Entität gebundenen Chiffre zu ändern, heben Sie zuerst die Bindung des virtuellen Servers, des Dienstes oder der Servicegruppe auf.

Hinweis: Wenn die an eine SSL-Entität gebundene Chiffriergruppe leer ist, schlägt der SSL-Handshake fehl, da keine ausgehandelte Chiffre vorhanden ist. Die Chiffriergruppe muss mindestens eine Chiffre enthalten.

Wird ECDSA auf der Citrix ADC-Appliance unterstützt?

ECDSA wird auf den folgenden Citrix ADC Plattformen unterstützt. Weitere Informationen zu unterstützten Builds finden Sie in Tabelle 1 und Tabelle 2 in Chiffren, die auf den Citrix ADC-Appliances verfügbar sind.

- Citrix ADC MPX- und SDX-Appliances mit N3-Chips
- Citrix ADC MPX 5900/8900/15000/26000
- Citrix ADC SDX 8900/15000
- Citrix ADC VPX Appliances

Unterstützt die Citrix ADC VPX Appliance AES-GCM/SHA2-Chiffern im Front-End?

Ja, AES-GCM/SHA2-Chiffre werden auf der Citrix ADC VPX Appliance unterstützt. Weitere Informationen zu den unterstützten Builds finden Sie unter Chiffren, die auf den Citrix ADC-Appliances verfügbar sind.

Zertifikate

Ist der Distinguished Name in einem Clientzertifikat für die Dauer der Benutzersitzung verfügbar?

Ja. Während der Dauer der Benutzersitzung können Sie in nachfolgenden Anfragen auf den Distinguished Name des Clientzertifikats zugreifen. Das heißt, selbst nachdem der SSL-Handshake abgeschlossen ist und das Zertifikat vom Browser nicht erneut gesendet wird. Verwenden Sie eine Variable und eine Zuweisung, wie in der folgenden Beispielkonfiguration beschrieben:

Beispiel:

```
add ns variable v2 -type ”text(100)”

add ns assignment a1 -variable ”$v2” -set       ”CLIENT.SSL.CLIENT_CERT
    .SUBJECT.TYPECAST_NVLIST_T('=','/').VALUE(”CN”)”

add rewrite action act1 insert_http_header subject ”$v2”  // example:
    to insert the distinguished name in the header

add rewrite policy pol1 true a1

add rewrite policy pol2 true act1

bind rewrite global pol1 1 next -type RES_DEFAULT

```



```
bind rewrite global pol2 2 next -type RES_DEFAULT

set rewrite param -undefAction RESET
<!--NeedCopy-->
```

Warum muss ich das Serverzertifikat binden?

Die Bindung der Serverzertifikate ist die Grundvoraussetzung dafür, dass die SSL-Konfiguration SSL-Transaktionen verarbeiten kann.

Um das Serverzertifikat an einen SSL-VIP zu binden, geben Sie an der CLI Folgendes ein:

```
bind ssl vserver <vServerName> -certkeyName <cert_name>
<!--NeedCopy-->
```

Um das Serverzertifikat an einen SSL-Dienst zu binden, geben Sie an der CLI Folgendes ein:

```
bind ssl service <serviceName> -certkeyName <cert_name>
<!--NeedCopy-->
```

Wie viele Zertifikate kann ich an einen SSL-VIP oder einen SSL-Dienst binden?

Auf einer Citrix ADC VPX-, MPX/SDX (N3)- und MPX/SDX 14000 FIPS-Appliance können Sie zwei Zertifikate an einen virtuellen SSL-Server oder einen SSL-Dienst binden, wenn SNI deaktiviert ist. Die Zertifikate müssen jeweils eins vom Typ RSA und ECDSA sein. Wenn SNI aktiviert ist, können Sie mehrere Serverzertifikate vom Typ RSA oder ECDSA binden. Wenn SNI deaktiviert ist, können Sie auf einer Citrix ADC MPX (N2) oder MPX 9700 FIPS-Appliance nur ein Zertifikat vom Typ RSA binden. Wenn SNI aktiviert ist, können Sie nur mehrere Serverzertifikate vom Typ RSA binden.

Was passiert, wenn ich ein Serverzertifikat aufhebe oder überschreibe?

Wenn Sie das Binden oder Überschreiben eines Serverzertifikats aufheben oder überschreiben, werden alle Verbindungen und SSL-Sitzungen beendet, die mit dem vorhandenen Zertifikat erstellt wurden. Wenn Sie ein vorhandenes Zertifikat überschreiben, wird die folgende Meldung angezeigt:

```
ERROR:

Warning: Current certificate replaces the previous binding.
```



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

Wie installiere ich ein Zwischenzertifikat auf einer Citrix ADC-Appliance und verbinde mich mit einem Serverzertifikat?

Weitere Informationen http://support.citrix.com/article/ctx114146 zur Installation eines Zwischenzertifikats finden Sie im Artikel unter.

Warum erhalte ich einen Fehler "Ressource existiert bereits", wenn ich versuche, ein Zertifikat auf dem Citrix ADC zu installieren?

Anweisungen http://support.citrix.com/article/CTX117284 zum Beheben des Fehlers "Ressource existiert bereits" finden Sie im Artikel unter.

Ich möchte ein Serverzertifikat auf einer Citrix ADC-Appliance erstellen, um das Produkt zu testen und auszuwerten. Wie ist das Verfahren zum Erstellen eines Serverzertifikats?

Führen Sie das folgende Verfahren aus, um ein Testzertifikat zu erstellen.

Hinweis: Ein mit diesem Verfahren erstelltes Zertifikat kann nicht zur Authentifizierung aller Benutzer und Browser verwendet werden. Nachdem Sie das Zertifikat zum Testen verwendet haben, müssen Sie ein Serverzertifikat erhalten, das von einer autorisierten Root-Zertifizierungsstelle signiert wurde.

So erstellen Sie ein selbstsigniertes Serverzertifikat:

1. Um ein Root-CA-Zertifikat zu erstellen, geben Sie an der CLI Folgendes ein:

```
create ssl rsakey /nsconfig/ssl/test-ca.key 1024

create ssl certreq /nsconfig/ssl/test-ca.csr -keyfile /nsconfig/
   ssl/test-ca.key

Enter the required information when prompted, and then type the
   following command:

create ssl cert /nsconfig/ssl/test-ca.cer /nsconfig/ssl/test-ca.
   csr ROOT_CERT -keyfile /nsconfig/ssl/test-ca.key
<!--NeedCopy-->
```

2. Führen Sie das folgende Verfahren aus, um ein Serverzertifikat zu erstellen und es mit dem soeben erstellten Stammzertifikat zu signieren

a) Um die Anforderung und den Schlüssel zu erstellen, geben Sie an der CLI Folgendes ein:

```
create ssl rsakey /nsconfig/ssl/test-server.key 1024

    create ssl certreq /nsconfig/ssl/test-server.csr -keyfile
       /nsconfig/ssl/test-server.key
<!--NeedCopy-->
```

b) Geben Sie bei Aufforderung die erforderlichen Informationen ein.

c) Um eine Seriennummerndatei zu erstellen, geben Sie an der CLI Folgendes ein:

```
shell
 # echo '01' >
/nsconfig/ssl/serial.txt
 # exit
<!--NeedCopy-->
```

d) Um ein Serverzertifikat zu erstellen, das von dem in Schritt 1 erstellten Stammzertifikat signiert wurde, geben Sie an der CLI Folgendes ein:

```
create ssl cert /nsconfig/ssl/test-server.cer /nsconfig/ssl/
   test-server.csr SRVR_CERT -CAcert /nsconfig/ssl/test-ca.cer
    -CAkey /nsconfig/ssl/test-ca.key -CAserial /nsconfig/ssl/
   serial.txt
<!--NeedCopy-->
```

e) Um ein Citrix ADC Cert-Schlüsselpaar, das das In-Memory-Objekt ist, das die Serverzertifikatsinformationen für SSL-Handshakes und Massenverschlüsselung enthält, an der CLI zu erstellen, geben Sie Folgendes ein:

```
add ssl certkey test-certkey -cert /nsconfig/ssl/test-server.
   cer -key /nsconfig/ssl/test-server.key
<!--NeedCopy-->
```

f) Um das Cert-Schlüsselpaar an den virtuellen SSL-Server zu binden, geben Sie an der CLI Folgendes ein:


```
bind ssl vserver <vServerName> -certkeyName <cert_name>
<!--NeedCopy-->
```

Ich habe eine Citrix ADC-Appliance erhalten, auf der NetScaler Software-Release 9.0 installiert ist. Mir ist eine zusätzliche Lizenzdatei auf der Appliance aufgefallen. Gibt es eine Änderung der Lizenzrichtlinie, beginnend mit NetScaler Software Release 9.0?

Ja. Ab Citrix NetScaler Software-Release 9.0 verfügt die Appliance möglicherweise über keine einzige Lizenzdatei. Die Anzahl der Lizenzdateien hängt von der Citrix ADC Software Release-Edition ab. Wenn Sie beispielsweise die Advanced Edition installiert haben, benötigen Sie möglicherweise zusätzliche Lizenzdateien, um die verschiedenen Funktionen voll funktionsfähig zu machen. Wenn Sie jedoch die Premium Edition installiert haben, verfügt die Appliance über nur eine Lizenzdatei.

Wie exportiere ich das Zertifikat aus dem Internetinformationsdienst (IIS)?

Es gibt viele Möglichkeiten, aber mit der folgenden Methode werden das entsprechende Zertifikat und der private Schlüssel für die Website exportiert. Dieser Vorgang muss auf dem eigentlichen IIS-Server durchgeführt werden.

1. Öffnen Sie das Verwaltungstool für Internetinformationsdienste (IIS) Manager.
2. Erweitern Sie den Website-Knoten und suchen Sie die SSL-fähige Website, die Sie über die Citrix ADC-Appliance bereitstellen möchten.
3. Klicken Sie mit der rechten Maustaste auf diese Website und klicken Sie
4. Klicken Sie auf die Registerkarte Verzeichnissicherheit, und wählen Sie im Abschnitt Sichere Kommunikation des Fensters das Feld Zertifikat anzeigen aus.
5. Klicken Sie auf die Registerkarte Details und dann auf In Datei kopieren.
6. Klicken Sie auf der Seite Willkommen beim Zertifikatexport-Assistenten auf Weiter.
7. Wählen Sie Ja aus, exportieren Sie den privaten Schlüssel und klicken Sie auf Weiter.

   Hinweis: Der private Schlüssel MUSS exportiert werden, damit SSL Offload am Citrix ADC arbeitet.
8. Stellen Sie sicher, dass das Optionsfeld Persönlicher Informationsaustausch -PKCS #12 aktiviert ist, und aktivieren Sie nach Möglichkeit *nur* das Kontrollkästchen Alle Zertifikate in den Zertifizierungspfad einbeziehen. Klicken Sie auf Weiter.
9. Geben Sie ein Kennwort ein und klicken Sie auf Weiter.
10. Geben Sie einen Dateinamen und einen Speicherort ein, und klicken Sie dann auf Weiter. Geben Sie der Datei eine Erweiterung von .PFX.

11. Klicken Sie auf Fertig stellen.

Wie konvertiere ich das PKCS #12 -Zertifikat und installiere es auf dem Citrix ADC?

1. Verschieben Sie die exportierte PFX-Zertifikatdatei an einen Speicherort, von dem aus sie auf die Citrix ADC-Appliance kopiert werden kann. Das heißt, auf einen Computer, der SSH-Zugriff auf die Verwaltungsschnittstelle einer Citrix ADC-Appliance ermöglicht. Kopieren Sie das Zertifikat mithilfe eines sicheren Kopierdienstprogramms wie SCP auf die Appliance.
2. Greifen Sie auf die BSD-Shell zu und konvertieren Sie das Zertifikat (z. B. Cert.PFX) in das PEM-Format:

```
root@ns# openssl pkcs12 -in cert.PFX -out cert.PEM
<!--NeedCopy-->
```

3. Um sicherzustellen, dass das konvertierte Zertifikat das richtige x509-Format hat, stellen Sie sicher, dass der folgende Befehl keinen Fehler verursacht:

```
root@ns# openssl x509 -in cert.PEM -text
<!--NeedCopy-->
```

4. Stellen Sie sicher, dass die Zertifikatsdatei einen privaten Schlüssel enthält. Geben Sie zunächst den folgenden Befehl aus:

```
root@ns# cat cert.PEM

Verify that the output file includes an RSA PRIVATE KEY section.

-----BEGIN RSA PRIVATE KEY-----
Mkm^s9KMs9023pz/s...
-----END RSA PRIVATE KEY-----
<!--NeedCopy-->
```

   Im Folgenden finden Sie ein weiteres Beispiel für einen Abschnitt mit RSA PRIVATE KEY:

```
    Bag Attributes
    1.3.6.1.4.1.311.17.2: <No Values>
    localKeyID: 01 00 00 00
```



```
    Microsoft CSP Name: Microsoft RSA SChannel Cryptographic
    Provider
    friendlyName:
    4b9cef4cc8c9b849ff5c662fd3e0ef7e_76267e3e-6183-4d45-886e-6
       e067297b38f

    Key Attributes
    X509v3 Key Usage: 10
    -----BEGIN RSA PRIVATE KEY-----
    Proc-Type: 4,ENCRYPTED
    DEK-Info: DES-EDE3-CBC,43E7ACA5F4423968
    pZJ2SfsSVqMbRRf6ug37Clua5gY0Wld4frPIxFXyJquUHr31dilW5ta3hbIaQ+
       Rg

    ... (more random characters)
    v8dMugeRplkaH2Uwt/mWBk4t71Yv7GeHmcmjafK8H8iW80ooPO3D/ENV8X4U/
       tlh

    5eU6ky3WYZ1BTy6thxxLlwAullynVXZEflNLxq1oX+ZYl6djgjE3qg==
    -----END RSA PRIVATE KEY-----
<!--NeedCopy-->
```

Im Folgenden finden Sie einen Abschnitt SERVERZERTIFIKAT

```
    Bag Attributes
    localKeyID: 01 00 00 00
    friendlyName: AG Certificate
    subject=/C=AU/ST=NSW/L=Wanniassa/O=Dave Mother
    Asiapacific/OU=Support/CN=davemother.food.lan
    issuer=/DC=lan/DC=food/CN=hotdog
    -----BEGIN CERTIFICATE-----
    MIIFiTCCBHGgAwIBAgIKCGryDgAAAAAHzANBgkqhkiG9w0BAQUFADA8MRMwEQYK


    ... (more random characters) 5
       pLDWYVHhLkA1pSxvFjNJHRSIydWHc5ltGyKqIUcBezVaXyel94pNSUYx07NpPV
       /

    MY2ovQyQZM8gGe3+lGFum0VHbv/y/gB9HhFesog=
    -----END CERTIFICATE-----
<!--NeedCopy-->
```

Im Folgenden finden Sie einen Abschnitt INTERMEDIATE CA CERTIFICATE:


```
    Bag Attributes: <Empty Attributes>
    subject=/DC=lan/DC=food/CN=hotdog
    issuer=/DC=lan/DC=food/CN=hotdog
    -----BEGIN CERTIFICATE-----
    MIIESDCCAzCgAwIBAgIQah20fCRYTY9LRXYMIRaKGjANBgkqhkiG9w0BAQUFADA8


    ... (more random characters)
       Nt0nksawDnbKo86rQcNnY5xUs7c7pj2zxj/IOsgNHUp5W6dDI9pQoqFFaDk
       =

    -----END CERTIFICATE-----
<!--NeedCopy-->
```

Je nach Zertifizierungspfad des exportierten Zertifikats können weitere Zwischenzertifikate folgen.

5. Öffnen Sie die PEM-Datei in einem Texteditor
6. Suchen Sie die erste Zeile der PEM-Datei und die erste Instanz der folgenden Zeile und kopieren Sie diese beiden Zeilen und alle Zeilen dazwischen:

```
-----END CERTIFICATE-----

Note: Make sure that last copied line is the first
-----END CERTIFICATE----- line in the .PEM file.

<!--NeedCopy-->
```

7. Fügen Sie die kopierten Zeilen in eine neue Datei ein. Nennen Sie die neue Datei etwas Intuitives wie cert-key.pem. Dieses Zertifikatschlüsselpaar ist für den Server, der den HTTPS-Dienst hostet. Diese Datei muss sowohl den Abschnitt mit der Bezeichnung RSA PRIVATE KEY als auch den Abschnitt mit der Bezeichnung SERVERZERTIFIKAT im vorherigen Beispiel enthalten.

   Hinweis: Die Zertifikatschlüsselpaardatei enthält den privaten Schlüssel und muss sicher aufbewahrt werden.

8. Suchen Sie alle nachfolgenden Abschnitte, die mit —BEGIN CERTIFICATE— beginnen und mit —END CERTIFICATE— enden, und kopieren Sie jeden dieser Abschnitt in eine separate neue Datei.

   Diese Abschnitte entsprechen Zertifikaten vertrauenswürdiger Zertifizierungsstellen, die in den Zertifizierungspfad aufgenommen wurden. Diese Abschnitte müssen kopiert und in neue einzelne Dateien für diese Zertifikate eingefügt werden. Beispielsweise muss der Abschnitt

INTERMEDIATE CA CERTIFICATE des vorherigen Beispiels kopiert und in eine neue Datei eingefügt werden).

Erstellen Sie für mehrere Zwischenzertifizierungsstellenzertifikate in der Originaldatei Dateien für jedes Zwischenzertifikat in der Reihenfolge, in der sie in der Datei erscheinen. Behalten Sie (unter Verwendung entsprechender Dateinamen) die Reihenfolge, in der die Zertifikate erscheinen, im Auge, da sie in einem späteren Schritt in der richtigen Reihenfolge miteinander verknüpft werden müssen.

9. Kopieren Sie die Zertifikatschlüsseldatei (cert-key.pem) und alle zusätzlichen Zertifizierungsstellen-Zertifikatdateien in das Verzeichnis /nsconfig/ssl auf der Citrix ADC-Appliance.
10. Beenden Sie die BSD-Shell und greifen Sie auf die Citrix ADC-Eingabeaufforderung zu.
11. Folgen Sie den Schritten unter "Installieren Sie die Zertifikatschlüsseldateien auf der Appliance", um den Schlüssel/das Zertifikat nach dem Hochladen auf das Gerät zu installieren.

Wie konvertiere ich das PKCS #7 -Zertifikat und installiere es auf der Citrix ADC-Appliance?

Sie können OpenSSL verwenden, um ein PKCS #7 -Zertifikat in ein Format zu konvertieren, das von der Citrix ADC-Appliance erkennbar ist. Die Prozedur ist identisch mit der Prozedur für PKCS #12 -Zertifikate, außer dass Sie OpenSSL mit verschiedenen Parametern aufrufen. Die Schritte zum Konvertieren von PKCS #7 -Zertifikaten lauten wie folgt:

1. Kopieren Sie das Zertifikat mithilfe eines sicheren Kopierdienstprogramms wie SCP auf die Appliance.
2. Konvertieren Sie das Zertifikat (z. B. Cert.P7b) in das PEM-Format:

```
openssl pkcs7 -inform DER -in cert.p7b -print_certs -text -out
   cert.pem
<!--NeedCopy-->
```

3. Befolgen Sie die Schritte 3 bis 7, wie in der Antwort für PKCS #12 -Zertifikate beschrieben.
   Hinweis: Bevor Sie das konvertierte PKCS #7 -Zertifikat auf die Appliance laden, überprüfen Sie, ob es einen privaten Schlüssel enthält, genau wie in Schritt 3 für die PKCS #12 -Prozedur beschrieben. PKCS #7 -Zertifikate, insbesondere die aus IIS exportierten Zertifikate, enthalten normalerweise keinen privaten Schlüssel.

Wenn ich eine Chiffre mithilfe des Befehls bind cipher an einen virtuellen Server oder Dienst binde, sehe ich die Fehlermeldung "Befehl veraltet. "?

Der Befehl zum Binden einer Chiffre an einen virtuellen Server oder Dienst hat sich geändert.

Binden Sie eine SSL-Chiffre mit dem `bind ssl vserver <vsername> -ciphername <ciphername>` Befehl an einen virtuellen SSL-Server.

Verwenden Sie den `bind ssl service <serviceName> -ciphername <ciphername>` Befehl, um eine SSL-Chiffre an einen SSL-Dienst zu binden.

Hinweis: Neue Chiffren und Chiffriergruppen werden zur vorhandenen Liste hinzugefügt und nicht ersetzt.

Warum kann ich keine Chiffriergruppe erstellen und Chiffren mithilfe des Befehls add cipher daran binden?

Die Funktionalität des Befehls “chiffre hinzufügen” hat sich in Release 10 geändert. Der Befehl erstellt nur eine Chiffriergruppe. Um der Gruppe Chiffren hinzuzufügen, verwenden Sie den Befehl bind cipher.

OpenSSL

Wie verwende ich OpenSSL, um Zertifikate zwischen PEM und DER zu konvertieren?

Um OpenSSL verwenden zu können, müssen Sie eine funktionierende Installation der OpenSSL-Software haben und OpenSSL von der Befehlszeile aus ausführen können.

x509-Zertifikate und RSA-Schlüssel können in verschiedenen Formaten gespeichert werden.

Zwei gängige Formate sind:

- DER (ein Binärformat, das hauptsächlich von Java- und Macintosh-Plattformen verwendet wird)
- PEM (eine base64-Darstellung von DER mit Kopf- und Fußzeileninformationen, die hauptsächlich von UNIX- und Linux-Plattformen verwendet wird).

Ein Schlüssel und das entsprechende Zertifikat können zusätzlich zum Root- und Zwischenzertifikaten auch in einer einzigen PKCS #12 (.P12, .PFX) -Datei gespeichert werden.

Prozedur

Verwenden Sie den **OpenSSL-Befehl**, um wie folgt zwischen Formaten zu konvertieren:

1. So konvertieren Sie ein Zertifikat von PEM in DER:

```
x509 -in input.crt -inform PEM -out output.crt -outform DER
<!--NeedCopy-->
```

2. So konvertieren Sie ein Zertifikat von DER in PEM:


```
x509 -in input.crt -inform DER -out output.crt -outform PEM
<!--NeedCopy-->
```

3. So konvertieren Sie einen Schlüssel von PEM in DER:

```
rsa -in input.key -inform PEM -out output.key -outform DER
<!--NeedCopy-->
```

4. So konvertieren Sie einen Schlüssel von DER in PEM:

```
rsa -in input.key -inform DER -out output.key -outform PEM
<!--NeedCopy-->
```

Hinweis: Wenn der Schlüssel, den Sie importieren, mit einer unterstützten symmetrischen Chiffre verschlüsselt ist, werden Sie aufgefordert, den Pass-Phrase einzugeben.

Hinweis: Um einen Schlüssel in oder aus dem veralteten NET-Format (Netscape-Server) zu konvertieren, ersetzen Sie NET gegebenenfalls durch PEM oder DER. Der gespeicherte Schlüssel wird in einer schwach ungesalzenen symmetrischen RC4-Chiffre verschlüsselt, daher wird eine Passphrase angefordert. Ein leerer Pass-Phrase ist akzeptabel.

Grenzwerte des Systems

Welche wichtigen Zahlen sollten Sie sich merken?

1. Zertifikatanforderung erstellen:
   - Dateiname anfordern: Maximal 63 Zeichen
   - Name der Schlüsseldatei: Maximal 63 Zeichen
   - PEM-Passphrase (für verschlüsselten Schlüssel): Maximal 31 Zeichen
   - Allgemeiner Name: Maximal 63 Zeichen
   - Stadt: Maximal 127 Zeichen
   - Name der Organisation: Maximal 63 Zeichen
   - Bundesland/Provinz Name: Maximal 63 Zeichen
   - E-Mail-Adresse: Maximal 39 Zeichen
   - Organisationseinheit: Maximal 63 Zeichen
   - Challenge Password: Maximal 20 Zeichen
   - Firmenname: Maximal 127 Zeichen
2. Zertifikat erstellen:

- Dateiname des Zertifikats: Maximal 63 Zeichen
- Dateiname der Zertifikatanforderung: Maximal 63 Zeichen
- Name der Schlüsseldatei: Maximal 63 Zeichen
- PEM-Passphrase: Maximal 31 Zeichen
- Gültigkeitszeitraum: Maximal 3650 Tage
- Dateiname des CA-Zertifikats: Maximal 63 Zeichen
- Name der CA-Schlüsseldatei: Maximal 63 Zeichen
- PEM-Passphrase: Maximal 31 Zeichen
- CA-Seriennummerndatei: Maximal 63 Zeichen

3. Erstellen und installieren Sie ein Server-Testzertifikat:

   - Dateiname des Zertifikats: Maximal 31 Zeichen
   - Vollqualifizierter Domainname: Maximal 63 Zeichen

4. Erstellen Sie Diffie-Hellman (DH) Schlüssel:

   - DH-Dateiname (mit Pfad): Maximal 63 Zeichen
   - DH-Parametergröße: Maximal 2048 Bit

5. PKCS12-Schlüssel importieren:

   - Ausgabedateiname: Maximal 63 Zeichen
   - PKCS12 Dateiname: Maximal 63 Zeichen
   - Kennwort importieren: Maximal 31 Zeichen
   - PEM-Passphrase: Maximal 31 Zeichen
   - Überprüfen der PEM-Passphrase: Maximal 31 Zeichen

6. Exportieren PKCS12

   - PKCS12 Dateiname: Maximal 63 Zeichen
   - Dateiname des Zertifikats: Maximal 63 Zeichen
   - Name der Schlüsseldatei: Maximal 63 Zeichen
   - Kennwort exportieren: Maximal 31 Zeichen
   - PEM-Passphrase: Maximal 31 Zeichen

7. CRL-Verwaltung:

   - Dateiname des CA-Zertifikats: Maximal 63 Zeichen
   - Name der CA-Schlüsseldatei: Maximal 63 Zeichen
   - CA-Schlüsseldatei-Kennwort: Maximal 31 Zeichen
   - Indexdateiname: Maximal 63 Zeichen
   - Dateiname des Zertifikats: Maximal 63 Zeichen

8. RSA-Schlüssel erstellen:

   - Name der Schlüsseldatei: Maximal 63 Zeichen

- Schlüsselgröße: Maximal 4096 Bit
- PEM-Passphrase: Maximal 31 Zeichen
- Passphrase überprüfen: Maximal 31 Zeichen

9. Ändern Sie erweiterte SSL-Einstellungen:

   - Maximale CRL-Speichergröße: Maximal 1024 Mbyte
   - Timeout für Verschlüsselungsauslöser (10 mS-Ticks): Maximal 200
   - Paketanzahl der Verschlüsselung: Maximal 50
   - OCSP-Cachegröße: Maximal 512 Mbyte

10. Zertifikat installieren:

    - Name des Zertifikatschlüsselpaars: Maximal 31 Zeichen
    - Dateiname des Zertifikats: Maximal 63 Zeichen
    - Dateiname des privaten Schlüssels: Maximal 63 Zeichen
    - Kennwort: Maximal 31 Zeichen
    - Benachrichtigungszeitraum: Maximal 100

11. Chiffriergruppe erstellen:

    - Name der Chiffriergruppe: Maximal 39 Zeichen

12. CRL erstellen:

    - CRL-Name: Maximal 31 Zeichen
    - CRL-Datei: Maximal 63 Zeichen
    - URL: Maximal 127 Zeichen
    - Basis-DN: Maximal 127 Zeichen
    - Bind DN: Maximal 127 Zeichen
    - Kennwort: Maximal 31 Zeichen
    - Tage: Maximal 31

13. Erstellen Sie SSL-Richtlinie:

    - Name: Maximal 127 Zeichen

14. SSL-Aktion erstellen:

    - Name: Maximal 127 Zeichen

15. Erstellen Sie OCSP-Responder:

    - Name: Maximal 32 Zeichen
    - URL: Maximal 128 Zeichen
    - Batchtiefe: Maximal 8
    - Batching-Verzögerung: Maximal 10000
    - Produziert bei Time Skew: Maximal 86400
    - Timeout anfordern: Maximum120000

16. Virtuellen Server erstellen:
    - Name: Maximal 127 Zeichen
    - Umleitungs-URL: Maximal 127 Zeichen
    - Client-Timeout: Maximal 31536000 Sekunden
17. Service erstellen:
    - Name: Maximal 127 Zeichen
    - Timeout im Leerlauf (Sekunden):
      Client: Maximal 31536000
      Server: Maximal 31536000
18. Dienstgruppe erstellen:
    - Dienstgruppenname: Maximal 127 Zeichen
    - Server-ID: Maximal 4294967295
    - Timeout im Leerlauf (Sekunden):
      Client: Maximalwert 31536000
      Server: Maximal 31536000
19. Monitor erstellen:
    - Name: Maximal 31 Zeichen
20. Server erstellen:
    - Servername: Maximal 127 Zeichen
    - Domainname: Maximal 255 Zeichen
    - Wiederholung auflösen: Maximal 20939 Sekunden

Inhaltsprüfung

October 5, 2021

In letzter Zeit wurden die Gerätetypen erweitert, um verschiedene Multimedia-Inhalte anzuzeigen. Die Gerätetypen können von Mobiltelefonen für Tablets und Desktops sein. Anbieter von Intermediate-Infrastrukturen müssen den ursprünglichen Inhalt von einem Webserver in ein Format umwandeln, das für das Gerät geeignet ist, das nach den Inhalten fragt. Die externen Geräte prüfen den transkodierenden Inhalt und senden ihn an den Client zurück. Häufig verwendete Protokoll, um dies zu erreichen, ist ICAP. ICAP ermöglicht die Implementierung der Citrix ADC Appliance in verschiedene Bereitstellungen. ICAP verwendet die Content-Inspektionstechnik, die Daten auf Malware und Sicherheitsprobleme untersucht.

> **Hinweis:**
>
> HTTP/2 ist nicht mit der Inhaltsüberprüfung kompatibel. Die Anwendungen, die den HTTP/2 verwenden, funktionieren möglicherweise nicht ordnungsgemäß, wenn der Datenverkehr durch die Inhaltsüberprüfung gesendet wird.

ICAP für Remote-Content-Inspektion

October 5, 2021

Das Internet Content Adaptation Protocol (ICAP) ist ein einfaches, leichtgewichtiges Protokoll zum Ausführen des Mehrwerttransformationsdienstes auf HTTP-Nachrichten. In einem typischen Szenario leitet ein ICAP-Client HTTP-Anforderungen und Antworten zur Verarbeitung an einen oder mehrere ICAP-Server weiter. Die ICAP-Server führen die Inhaltstransformation für die Anforderungen durch und senden Antworten mit geeigneten Maßnahmen für die Anforderung oder Antwort zurück.

ICAP auf einer Citrix ADC Appliance

In einem Citrix ADC -Setup fungiert die Appliance als ICAP-Client, der mit ICAP-Servern von Drittanbietern (wie Antimalware und Data Loss Protection (DLP)) zusammenarbeitet. Wenn die Appliance einen eingehenden Webverkehr empfängt, fängt die Appliance den Datenverkehr ab und verwendet eine Inhaltsinspektionsrichtlinie, um zu bewerten, ob die HTTP-Anforderung eine ICAP-Verarbeitung erfordert. Wenn ja, entschlüsselt die Appliance die Nachricht und sendet sie als Klartext an die ICAP-Server. Die ICAP-Server führen den Content-Transformationsdienst für die Anforderungsnachricht aus und senden eine Antwort an die Appliance zurück. Die angepassten Nachrichten können entweder eine HTTP-Anforderung oder eine HTTP-Antwort sein. Wenn die Appliance mit mehreren ICAP-Servern interagiert, führt die Appliance den Lastenausgleich von ICAP-Servern durch. Dieses Szenario tritt auf, wenn ein ICAP-Server nicht ausreicht, um den gesamten Datenverkehr zu verarbeiten. Sobald die ICAP-Server eine geänderte Nachricht zurückgeben, leitet die Appliance die geänderte Nachricht an den Back-End-Ursprungsserver weiter.

Die Citrix ADC Appliance stellt auch einen gesicherten ICAP-Dienst bereit, wenn der eingehende Datenverkehr ein HTTPS-Typ ist. Die Appliance verwendet einen SSL-basierten TCP-Dienst, um eine gesicherte Verbindung zwischen der Appliance und den ICAP-Servern herzustellen.

Funktionsweise der ICAP-Anforderungsänderung (REQMOD)

Im Modus Anforderungsänderung (REQMOD) leitet die Citrix ADC Appliance die vom Client empfangene HTTP-Anfrage an den ICAP-Server weiter. Der ICAP-Server führt dann eine der folgenden Aktionen aus:

1. Sendet eine geänderte Version der Anforderung zurück und die Appliance sendet die geänderte Anforderung wiederum an den Back-End-Ursprungsserver oder leitet die geänderte Anforderung an einen anderen ICAP-Server weiter.
2. Antwortet mit einer Meldung, die darauf hinweist, dass keine Anpassung erforderlich ist.
3. Gibt einen Fehler zurück und die Appliance sendet die Fehlermeldung wiederum an den Benutzer zurück.

Funktionsweise der ICAP-Antwortmodifikation (RESPMOD)

Im Response Modification (RESPMOD) -Modus sendet die Citrix ADC Appliance eine HTTP-Antwort an den ICAP-Server (die von der Appliance gesendete Antwort ist in der Regel die vom Ursprungsserver gesendete Antwort). Der ICAP-Server führt dann eine der folgenden Aktionen aus:

1. Sendet eine geänderte Version der Antwort, und die Appliance wiederum sendet die Antwort an den Benutzer oder leitet die Antwort an einen anderen ICAP-Server weiter.
2. Antwortet mit einer Meldung, die darauf hinweist, dass keine Anpassung erforderlich ist.
3. Gibt einen Fehler zurück und die Appliance sendet die Fehlermeldung wiederum an den Benutzer.

ICAP-Lizenz

Die ICAP-Funktion funktioniert auf einem eigenständigen oder hochverfügbaren Citrix ADC Setup mit Citrix ADC Premium oder Advanced Lizenz Edition.

Konfigurieren von ICAP für Content-Transformationsdienst

Um ICAP für den Content-Transformationsdienst zu verwenden, müssen Sie zunächst die Funktionen Inhaltsprüfung und Lastausgleich aktivieren. Nachdem Sie die Features aktiviert haben, können Sie die folgenden Aufgaben ausführen.

So aktivieren Sie die Inhaltsüberprüfung

Wenn Sie möchten, dass die Citrix ADC Appliance als ICAP-Client fungiert, müssen Sie zunächst die Funktionen Content Inspection und Load Balancing aktivieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns feature contentInspection LoadBalancing
<!--NeedCopy-->
```


ICAP-Profil hinzufügen

ICAP-Konfigurationen für eine Citrix ADC Appliance werden in einer Entität namens ICAP-Profil angegeben. Das Profil verfügt über eine Sammlung der ICAP-Einstellungen. Die Einstellungen umfassen Parameter, um dynamisch eine ICAP-Anfrage zu generieren, die ICAP-Antwort zu erhalten und Inhaltsüberprüfungsdaten zu protokollieren.

Um eine ICAP-Anfrage dynamisch an den ICAP-Server zu generieren, wird dem ICAP-Profil ein neuer Parameter "inserthttpRequest" hinzugefügt. Wenn dieser Parameter konfiguriert ist, übernimmt die Appliance den konfigurierten Wert als Richtlinienausdruck und wertet den Ausdruck aus und schließt das Ergebnis als gekapselte HTTP-Anforderung oder -Antwort ein und sendet ihn dann an den ICAP-Server. Außerdem ist ein neuer Parameter InsertiCapHeaders konfigurierbar, um die ICAP-Header dynamisch auszuwerten und einzubeziehen.

Wenn die Appliance eine ICAP-Anforderung sendet und keine Antwort auf den ICAP-Server erhält, reagiert die Verbindung nicht mehr. Es tritt auf, bis der ICAP-Server eine Antwort sendet oder eine Sitzung freigegeben wird. Das Verhalten kann durch Konfigurieren der ICAP-Antworttimeout-Option behandelt werden. Sie können einen Anforderungs-Timeout-Parameter für Aktionen festlegen, wenn eine verzögerte ICAP-Antwort vorliegt. Wenn die Citrix ADC Appliance innerhalb des konfigurierten Anforderungstimeouts keine Antwort erhält, wird die Anforderungstimeout-Aktion ausgeführt.

ReqTimeoutAction: Mögliche Werte sind BYPASS, RESET, DROP.
BYPASS: Dies ignoriert die Antwort des entfernten ICAP-Servers und sendet die Anforderung/Antwort an Client/Server.
RESET (Standard): Setzen Sie die Clientverbindung zurück, indem Sie sie schließen.
DROP: Lösen Sie die Anfrage, ohne eine Antwort an den Benutzer zu senden

Um eine ICAP-Antwort auszuwerten, `ICAP.RES` wird ein neuer Richtlinienausdruck im Rückgabeausdruck der Inhaltsübersicht verwendet. Dieser Ausdruck wertet die ICAP-Antwort ähnlich dem `HTTP.RES` Ausdruck in einem aus `HTTP_CALLOUT`.

Wenn beispielsweise eine Citrix ADC Appliance eine HTTP-Anforderung für einen Dienst empfängt, der hinter der virtuellen IP-Adresse des Citrix ADC gehostet wird, muss die Appliance möglicherweise die Authentifizierung des Clients mit einem externen Server überprüfen und eine Aktion ausführen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns icapProfile <name> [-preview ( ENABLED | DISABLED )][-previewLength
 <positive_integer>] -uri <string> [-hostHeader <string>] [-userAgent <
string>] -Mode ( REQMOD | RESPMOD )[-queryParams <string>] [-connectionKeepAlive
 ( ENABLED | DISABLED )][-allow204 ( ENABLED | DISABLED )] [-insertICAPHeaders
 <string>][-insertHTTPRequest <string>] [-reqTimeout <positive_integer>][-
reqTimeoutAction <reqTimeoutAction>] [-logAction <string>]
```

Beispiel:


```
add icapprofile reqmod-profile -mode RESPMOD -uri “/req_scan” -hostHeader “Webroot.reqsca” -useragent “NS_SWG-Proxy”

add ns icapProfile icap_prof1 -uri ”/example”-Mode REQMOD -reqtimeout 4 -reqtimeoutaction BYPASS

> add icapProfile reqmode-profile -uri '/example'-mode REQMOD -insertHTTPRequest q{ HTTP.REQ.METHOD + ””+ HTTP.REQ.URL + ”HTTP/1.1\r\n”+ ”Host: ”+ HTTP.REQ.HOSTNAME + ”\r\n\r\n”}
```

Aktion zur Überprüfung des ICAP-Inhalts protokollieren

Um dynamisch Content-Inspection-Protokolldatensätze oder SYSLOG-Protokolle zu generieren, können Sie den ICAP.RES-basierten Richtlinienausdruck für die ICAP-Antwort verwenden. Dieser Parameter kann im ICAP-Profil konfiguriert werden, um den Richtlinienausdruck zum Generieren der dynamischen Protokolldatensätze zu konfigurieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add audit messageaction icap_log_expr INFORMATIONAL icap.res.full_header

set icapProfile reqmode-profile -logAction messageaction
```

Hinzufügen des ICAP-Dienstes als TCP- oder SSL_TCP-Dienst

Nachdem Sie die Inhaltsinspektion aktiviert haben, müssen Sie einen ICAP-Dienst für die ICAP-Server hinzufügen, die Teil des Lastausgleichs-Setups sind. Der hinzugefügte Dienst stellt die ICAP-Verbindung zwischen der Citrix ADC Appliance und den virtuellen Lastausgleichsservern bereit.

Hinweis: Als Administrator können Sie einen ICAP-Dienst hinzufügen und die IP-Adresse des ICAP-Servers direkt in der Inhaltsprüfung konfigurieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add service <name> <IP> <serviceType> <port>
2 <!--NeedCopy-->
```

Beispiel:

```
add service icapsv1 10.10.10.10 SSL_TCP 1345

add service icapsv2 10.10.10.11 SSL_TCP 1345
```


Hinzufügen eines TCP- oder SSL_TCP-basierten Lastausgleichsservers

Nachdem Sie einen ICAP-Dienst erstellt haben, müssen Sie einen virtuellen Server erstellen, um den ICAP-Datenverkehr zu akzeptieren und den Lastausgleich der ICAP-Server zu erhalten.

> **Hinweis:**
>
> Sie können auch einen SSL-basierten TCP-Dienst über einen gesicherten Kanal verwenden. Sie verwenden einen SSL_TCP-Dienst und binden an die Aktion Content Inspection.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb vserver <name> <serviceType> <port>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add lb vserver vicap TCP 0.0.0.0 - persistenceType NONE -cltTimeout
     9000
2
3 add lb vserver vicap SSL_TCP 0.0.0.0 0 - persistenceType NONE -
     cltTimeout 9000
4 <!--NeedCopy-->
```

Binden des ICAP-Dienstes an den virtuellen Lastausgleichsserver

Nachdem Sie einen ICAP-Dienst und einen virtuellen Server erstellt haben, müssen Sie den ICAP-Dienst an den virtuellen Server binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind lb vserver <name> <serviceName>
2 <!--NeedCopy-->
```

Beispiel:

```
1 bind lb vserver vicap icapsv1
2 <!--NeedCopy-->
```


Aktion zur Inhaltsüberprüfung hinzufügen

Nachdem Sie die Inhaltsinspektion aktiviert haben, müssen Sie eine ICAP-Aktion für die Verarbeitung der ICAP-Anforderungsinformationen hinzufügen. Das erstellte ICAP-Profil und die erstellten Dienste oder der Lastenausgleichsserver sind an die ICAP-Aktion gebunden. Wenn der ICAP-Server ausgefallen ist, können Sie den `ifserverdown` Parameter konfigurieren, mit dem die Appliance eine der folgenden Aktionen ausführen soll.

CONTINUE: Wenn der Benutzer die Inhaltsüberprüfung umgehen möchte, wenn der Remoteserver ausfällt, können Sie standardmäßig die Aktion “CONTINUE” wählen.
RESET (Standard): Diese Aktion reagiert auf den Client, indem die Verbindung mit RST geschlossen wird.
DROP: Diese Aktion löscht automatisch die Pakete, ohne eine Antwort an den Benutzer zu senden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add contentInspection action <name> -type ICAP -serverName <string> -
     icapProfileName <string>
2
3 add ContentInspection action <name> -type ICAP -serverip <ip> -
     serverport <port> -icapProfileName <string>
4 <!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn Sie den ICAP-Dienst anstelle eines virtuellen Lastausgleichsservers konfigurieren können, können Sie den Dienstnamen in der `\<-serverip>` Option angeben. Beim Hinzufügen der Content-Inspection-Aktion wird der TCP-Dienst automatisch für die angegebene IP-Adresse mit Port 1344 erstellt und für die ICAP-Kommunikation verwendet.

Beispiel:

```
1 add ContentInspection action ci_act_lb -type ICAP -serverName vicap -
     icapProfileName icap_reqmod
2
3 add ContentInspection action ci_act_svc -type ICAP -serverName icapsv1
     -icapProfileName icap_reqmod
4
5 add ContentInspection action ci_act_svc -type ICAP -serverip 1.1.1.1 -
     serverport 1344 -icapProfileName icap_reqmod
6 <!--NeedCopy-->
```


Richtlinien zur Inhaltsüberprüfung hinzufügen

Nachdem Sie eine Inhaltsprüfung Aktion erstellt haben, müssen Sie Richtlinien zur Inhaltsüberprüfung erstellen, um Anforderungen für die ICAP-Verarbeitung und die Überwachungsprotokollierung auszuwerten. Die Richtlinie basiert auf einer Regel, die aus einem oder mehreren Ausdrücken besteht. Die Regel ist der Inhaltsüberprüfungsaktion zugeordnet, die zugeordnet ist, wenn eine Anforderung mit der Regel übereinstimmt.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection policy <name> -rule <expression> -action <string>
<!--NeedCopy-->
```

Beispiel:

```
add ContentInspection policy ci_pol_basic - rule true - action
    ci_act_svc

add ContentInspection policy ci_pol_HTTP - rule HTTP.REQ.URL.CONTAINS(
    "html" ) - action ci_act_svc
<!--NeedCopy-->
```

Binden von Richtlinien zur Inhaltsüberprüfung an den virtuellen Content Switching- oder Lastausgleichsserver

Um eine ICAP-Richtlinie in Kraft zu setzen, müssen Sie sie global binden oder an einen virtuellen Content Switching- oder Lastausgleichsserver binden, der die Anwendung Frontend macht. Wenn Sie die Richtlinie binden, müssen Sie ihr eine Priorität zuweisen. Die Priorität bestimmt die Reihenfolge, in der die von Ihnen definierten Richtlinien ausgewertet werden.

> **Hinweis:**
>
> Der virtuelle Anwendungsserver muss vom Typ HTTP/SSL/CS-PROXY sein.

Informationen zum Konfigurieren eines Load Balancing-Setups für die Weiterleitung des Datenverkehrs an den Back-End-Ursprungsserver nach der Inhaltstransformation finden Sie unter Load Balancing.

Konfigurieren des sicheren ICAP-Dienstes

Um eine sichere Verbindung zwischen der Citrix ADC Appliance und den ICAP-Webservern herzustellen, verwendet die Appliance einen SSL-basierten TCP-Dienst oder einen virtuellen

Lastausgleichsserver, der an eine ICAP-Aktion gebunden ist.

Führen Sie die folgenden Aufgaben aus, um eine sichere ICAP-Verbindung herzustellen:

1. Fügen Sie SSL-basierten TCP-Dienst hinzu.
2. Binden Sie den SSL-basierten TCP-Dienst an den Lastenausgleich virtuellen Server vom Typ TCP oder SSL_TCP.
3. Binden Sie SSL-basierten TCP-Dienst oder einen virtuellen Lastenausgleichsserver an die Inhaltsprüfung Aktion.

Hinzufügen eines SSL-basierten TCP-Dienstes zum Lastenausgleich eines virtuellen Servers

Um eine sichere Verbindung zwischen der Citrix ADC Appliance und den ICAP-Webservern herzustellen, verwendet die Appliance einen SSL-basierten TCP-Dienst oder einen virtuellen Lastausgleichsserver, der an eine ICAP-Aktion gebunden ist.

Führen Sie die folgenden Aufgaben aus, um eine sichere ICAP-Verbindung herzustellen:

1. Fügen Sie SSL-basierten TCP-Dienst hinzu.
2. Binden Sie den SSL-basierten TCP-Dienst an den Lastenausgleich virtuellen Server vom Typ TCP oder SSL_TCP.

Binden Sie SSL-basierten TCP-Dienst oder den Lastenausgleich virtueller Server an Content Inspection Aktion

Hinzufügen eines SSL-basierten TCP-Dienstes zum Lastenausgleich eines virtuellen Servers

Nachdem Sie die Inhaltsinspektion aktiviert haben, müssen Sie einen sicheren ICAP-Dienst hinzufügen, der Teil des Lastausgleichs ist. Der hinzugefügte Dienst stellt eine sichere ICAP-Verbindung zwischen der Citrix ADC Appliance und den virtuellen Lastenausgleichs-Servern bereit.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name> <IP> <serviceType> <port>
<!--NeedCopy-->
```

Beispiel:

```
add service icapsv2 10.102.29.200 SSL_TCP 1344 -gslb NONE -maxclient
    0 -maxReq 0 -cip DISABLED -usip NO -useproxport YES -sp ON -
    cltTimeout 9000 -svrTimeout 9000 -CKA NO -TCPB NO -CMP NO
<!--NeedCopy-->
```


Binden Sie SSL-basierten TCP-Dienst an den virtuellen SSL_TCP oder TCP-Lastenausgleichsserver

Nachdem Sie einen gesicherten ICAP-Dienst erstellt haben, müssen Sie den Dienst an den virtuellen Lastausgleichsserver binden. Dies ist erforderlich, wenn Sie einen virtuellen Lastausgleichsserver verwenden, um den Lastausgleich der ICAP-Server zu verwenden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind lb vserver <name> <serviceName>
2 <!--NeedCopy-->
```

Beispiel:

```
1 bind lb vserver vicap icapsv2
2 <!--NeedCopy-->
```

Binden Sie SSL-basierten TCP-Dienst oder einen virtuellen Lastenausgleichsserver an die Inhaltsinspektion Aktion

Sie fügen eine ICAP-Aktion zur Behandlung der ICAP-Anforderungsinformationen hinzu und binden den SSL-basierten TCP-Dienst auch an die Aktion.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add contentInspection action <name> -type ICAP -serverName <string> -
     icapProfileName <string>
2 <!--NeedCopy-->
```

Beispiel:

```
1 add ContentInspection action ci_act_svc -type ICAP -serverName icapsv2
     -icapProfileName icap_reqmod
2
3 add ContentInspection action ci_act_svc -type ICAP -serverName vicap -
     icapProfileName icap_reqmod
4 <!--NeedCopy-->
```


Konfigurieren des ICAP-Protokolls mit der GUI

1. Navigieren Sie zu **Load Balancing** > **Services**, und klicken Sie auf **Hinzufügen**.
2. Geben Sie auf der Seite **Dienste** die Service-Details ein.
3. Navigieren Sie zu **Lastenausgleich** > **Virtuelle Server**. Fügen Sie einen virtuellen Lastausgleichsserver vom Typ HTTP/SSL hinzu. Sie können auch einen virtuellen Server auswählen und auf **Bearbeiten**klicken.
4. Nachdem Sie die grundlegenden Details des Servers eingegeben haben, klicken Sie auf **Weiter**.
5. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.
6. Gehen Sie in den Abschnitt **Richtlinien** und klicken Sie auf das **Bleistift-Symbol**, um die Richtlinie zur Inhaltsüberwachung zu konfigurieren.
7. Wählen Sie auf der Seite **Richtlinie auswählen** die Option **Inhaltsübersicht** aus. Klicken Sie auf **Weiter**.
8. Klicken Sie im Abschnitt **Richtlinienbindung** auf **+**, um eine Richtlinie zur Inhaltsüberwachung hinzuzufügen.
9. Geben **Sie auf der Seite ICAP-Richtlinie erstellen** einen Namen für die Richtlinie ein.
10. Klicken Sie im Feld **Aktion** auf das Zeichen "+", um eine ICAP-Aktion hinzuzufügen.
11. Geben **Sie auf der Seite ICAP-Aktion erstellen** einen Namen für die Aktion ein.
12. Geben Sie einen Namen für die Aktion ein.
13. Geben Sie im Feld **Servername** den Namen des bereits erstellten TCP-Dienstes ein.
14. Klicken Sie im Feld **ICAP-Profil** auf das Zeichen "+", um ein ICAP-Profil hinzuzufügen.
15. Geben **Sie auf der Seite ICAP-Profil erstellen** einen Profilnamen, einen URI und MODE ein.
16. Klicken Sie auf **Erstellen**.
17. Klicken Sie auf der Seite **ICAP-Aktion erstellen** auf **Erstellen**.
18. Geben Sie auf der Seite **ICAP-Richtlinie erstellen** im **Ausdruckseditor** "true" ein, und klicken Sie dann auf **Erstellen**.
19. Klicken Sie auf **Bind**.
20. Wenn Sie aufgefordert werden, die Inhaltsüberprüfung zu aktivieren, klicken Sie auf **Ja**.
21. Klicken Sie auf **Fertig**.

Informationen zur Citrix ADC GUI-Konfiguration für den Lastenausgleich und das Weiterleiten des Datenverkehrs nach der Inhaltstransformation an den Back-End-Ursprungsserver finden Sie unter Load Balancing.

Konfigurieren des gesicherten ICAP-Protokolls mit der GUI

1. Navigieren Sie zu **Load Balancing** > **Services**, und klicken Sie auf **Hinzufügen**.
2. Geben Sie auf der Seite **Dienste** die Service-Details ein.
3. Navigieren Sie zu **Lastenausgleich** > **Virtuelle Server**. Fügen Sie einen virtuellen Server vom Typ HTTP/SSL hinzu. Sie können auch einen virtuellen Server auswählen und auf **Bearbeiten**klicken.

4. Nachdem Sie die grundlegenden Details des Servers eingegeben haben, klicken Sie auf **Weiter**.
5. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.
6. Gehen Sie in den Abschnitt **Richtlinien** und klicken Sie auf das **Bleistift-Symbol**, um die Richtlinie zur Inhaltsüberwachung zu konfigurieren.
7. Wählen Sie auf der Seite **Richtlinie auswählen** die Option **Inhaltsübersicht** aus. Klicken Sie auf **Weiter**.
8. Klicken Sie im Abschnitt **Richtlinienbindung** auf **+**, um eine Richtlinie zur Inhaltsüberwachung hinzuzufügen.
9. Geben **Sie auf der Seite ICAP-Richtlinie erstellen** einen Namen für die Richtlinie ein.
10. Klicken Sie im Feld **Aktion** auf das Zeichen "+", um eine ICAP-Aktion hinzuzufügen.
11. Geben **Sie auf der Seite ICAP-Aktion erstellen** einen Namen für die Aktion ein.
12. Geben Sie einen Namen für die Aktion ein.
13. Geben Sie im Feld **Servername** den Namen des bereits erstellten TCP_SSL-Dienstes ein.
14. Klicken Sie im Feld **ICAP-Profil** auf das Zeichen "+", um ein ICAP-Profil hinzuzufügen.
15. Geben **Sie auf der Seite ICAP-Profil erstellen** einen Profilnamen, einen URI und MODE ein.
16. Klicken Sie auf **Erstellen**.
17. Klicken Sie auf der Seite **ICAP-Aktion erstellen** auf **Erstellen**.
18. Geben Sie auf der Seite **ICAP-Richtlinie erstellen** im **Ausdrucksеditor** "true" ein, und klicken Sie dann auf **Erstellen**.
19. Klicken Sie auf **Bind**.
20. Wenn Sie aufgefordert werden, die Inhaltsüberprüfung zu aktivieren, klicken Sie auf **Ja**.
21. Klicken Sie auf **Fertig**.

Unterstützung von Audit-Logs für Remote-Inhaltsüberwachung

Wenn eine eingehende Anforderung oder ausgehende Antwort Inhalt überprüft wird, protokolliert die Citrix ADC Appliance die ICAP-Details. Die Appliance speichert die Details als Protokollmeldung in der Datei ns.log.

Jede Protokollnachricht enthält in der Regel die folgenden Details:

```
1 <Source IP> <Destination IP> <Domain> <ICAP server IP><ICAP Mode> <
     Service URI> <ICAP response> <Policy action>
2 <!--NeedCopy-->
```

Beispiel für Content-inspizierte Anforderungsprotokollmeldung:

```
1 Apr 18 14:45:41 <local0.info> 10.106.97.104 04/18/2018:14:45:41 GMT 0-
     PPE-0 : default CI ICAP_LOG 788 0 : Source 10.102.1.98:39048 -
```



```
    Destination 10.106.97.89:8011 - Domain 10.106.97.89 - Content-Type
    application/x-www-form-urlencoded - ICAP Server 10.106.97.99:1344 -
    Mode REQMOD - Service /example - Response 204 - Action FORWARD
<!--NeedCopy-->
```

Beispiel für Content-inspizierte Antwortprotokollmeldung:

```
Apr 18 12:34:08 <local0.info> 10.106.97.104 04/18/2018:12:34:08 GMT 0-
    PPE-0 : default CI ICAP_LOG 71 0 : Source 10.106.97.105:18552 -
    Destination 10.106.97.99:80 - Domain NA - Content-Type NA - ICAP
    Server 10.106.97.99:1344 - Mode RESPMOD - Service /example -
    Response 400 - Action Internal Error
<!--NeedCopy-->
```

Inline-Geräteintegration mit Citrix ADC

October 5, 2021

Sicherheitsgeräte wie Intrusion Prevention System (IPS) und Next Generation Firewall (NGFW) schützen Server vor Netzwerkangriffen. Diese Geräte werden im Layer-2-Inline-Modus bereitgestellt. Ihre primäre Funktion besteht darin, Server vor Netzwerkangriffen zu schützen und Sicherheitsbedrohungen im Netzwerk zu melden.

Um anfällige Bedrohungen zu vermeiden und erweiterten Sicherheitsschutz zu bieten, ist eine Citrix ADC Appliance mit einem oder mehreren Inline-Geräten integriert. Die Inline-Geräte können jedes Sicherheitsgerät wie IPS, NGFW sein.

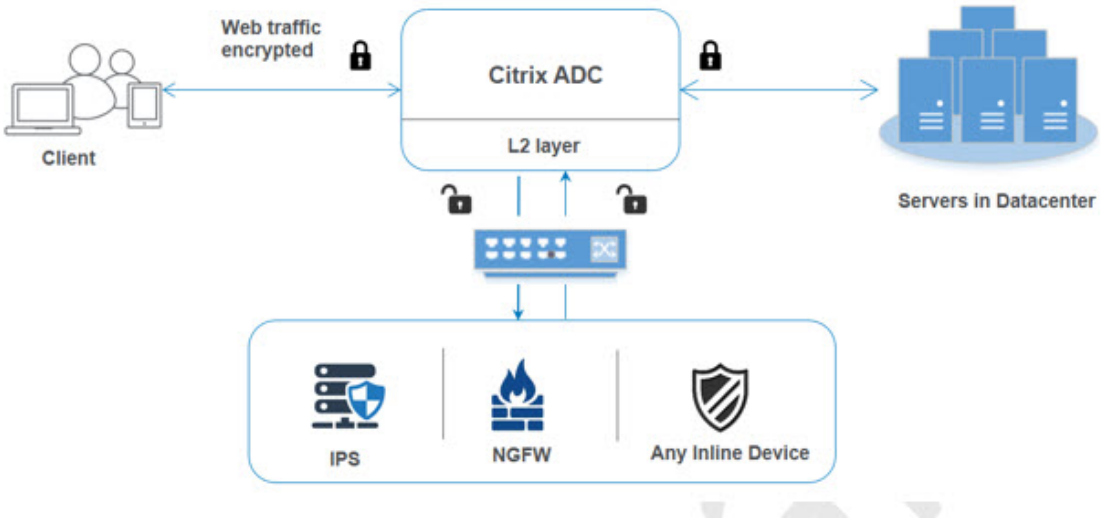
Im Folgenden sind einige der Anwendungsfälle aufgeführt, die bei der Verwendung der Inline-Geräteintegration mit der Citrix ADC Appliance profitieren:

- **Verschlüsselten Datenverkehr wird überprüft**. Die meisten IPS- und NGFW-Appliances umgehen verschlüsselten Datenverkehr, wodurch Server anfällig für Angriffe bleiben. Eine Citrix ADC Appliance kann Datenverkehr entschlüsseln und zur Inspektion an Inline-Geräte senden. Es erhöht die Netzwerksicherheit des Kunden.
- **Entladen von Inline-Geräten aus der TLS/SSL-Verarbeitung**. Die TLS/SSL-Verarbeitung ist teuer und das Problem kann zu einer hohen System-CPU in IPS- oder NGFW-Appliances führen, wenn sie den Datenverkehr entschlüsseln. Da der verschlüsselte Datenverkehr in einem rasanten Tempo wächst, können diese Systeme verschlüsselten Datenverkehr nicht entschlüsseln und untersuchen. Citrix ADC hilft beim Abladen von Inline-Geräten aus der TLS/SSL-Verarbeitung. Dies führt dazu, dass das Inline-Gerät ein hohes Maß an Verkehrsinspektion unterstützt.

- **Laden von Balancing-Inline-Geräten**. Die Citrix ADC Appliance gleicht bei hohem Datenverkehr mehrere Inline-Geräte aus.
- **Intelligente Auswahl des Datenverkehrs**. Jedes Paket, das in die Appliance fließt, kann Inhalt inspiziert werden, zum Beispiel das Herunterladen von Textdateien. Benutzer können die Citrix ADC Appliance so konfigurieren, dass sie bestimmten Datenverkehr (z. B. EXE-Dateien) zur Überprüfung auswählen und den Datenverkehr an Inline-Geräte zur Verarbeitung der Daten senden

Wie der Citrix ADC in Inline-Geräte integriert ist

Das folgende Diagramm zeigt, wie ein Citrix ADC in Inline-Sicherheitsgeräte integriert ist.



Wenn Sie Inline-Geräte in die Citrix ADC Appliance integrieren, interagiert die Komponente wie folgt:

1. Ein Client sendet eine Anforderung an die Citrix ADC Appliance.
2. Die Appliance empfängt die Anforderung und sendet sie basierend auf der Richtlinienbewertung an ein Inline-Gerät.
   Hinweis: Wenn zwei oder mehr Inline-Geräte vorhanden sind, gleicht die Appliance die Geräte aus und sendet den Datenverkehr.
   Wenn der eingehende Datenverkehr verschlüsselt ist, entschlüsselt die Appliance die Daten und sendet sie als Klartext an das Inline-Gerät zur Inhaltsüberprüfung.
3. Das Inline-Gerät prüft die Daten auf Bedrohungen und entscheidet, ob die Daten gelöscht, zurückgesetzt oder an die Appliance gesendet werden sollen.
4. Wenn Sicherheitsbedrohungen vorliegen, ändert das Gerät die Daten und sendet sie an die Appliance.
5. Der Citrix ADC wiederum verschlüsselt die Daten erneut und leitet die Anforderung an den Back-End-Server weiter.
6. Der Back-End-Server sendet die Antwort an die Citrix ADC Appliance.

7. Die Appliance entschlüsselt die Daten erneut und sendet sie zur Überprüfung an das Inline-Gerät.
8. Appliance verschlüsselt die Daten erneut und sendet die Antwort an den Client

Softwarelizenzierung

Um die Inline-Geräteintegration bereitzustellen, muss Ihre Citrix ADC Appliance mit einer der folgenden Lizenzen bereitgestellt werden:

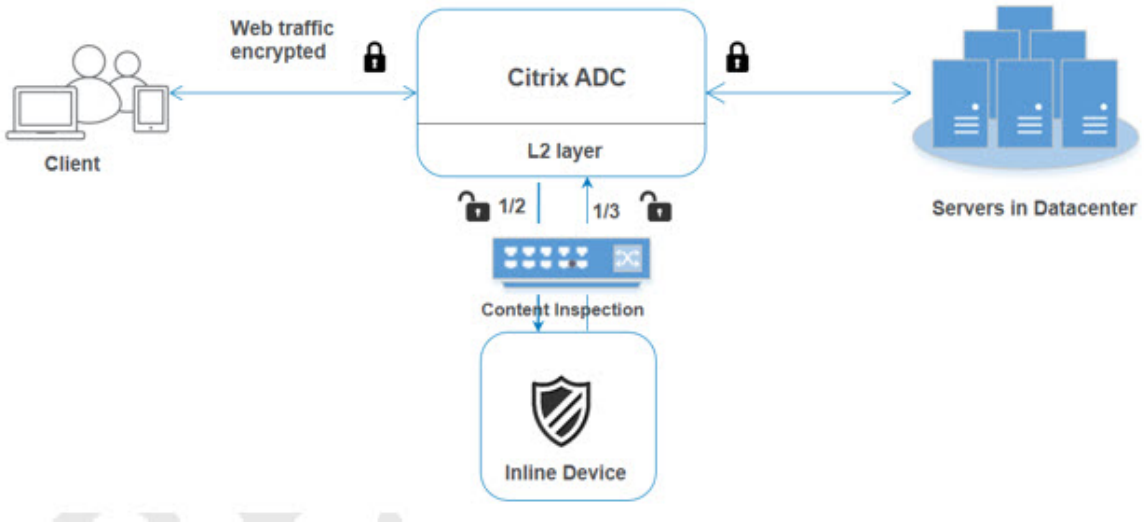
1. ADC Premium
2. ADC Advanced
3. Telco Fortgeschrittene
4. Telco Premium
5. SWG-Lizenz

Konfigurieren der Inline-Geräteintegration

Sie können eine Citrix ADC Appliance mit einem Inline-Gerät auf drei verschiedene Arten konfigurieren. Die Konfigurationsszenarien sind wie folgt.

Szenario 1 für die Verwendung eines einzelnen Inline-Geräts

Wenn Sie ein Sicherheitsgerät (IPS oder NGFW) im Inlinemodus integrieren möchten, müssen Sie zunächst die Content Inspection-Funktion aktivieren und den Citrix ADC in MBF (Mac-basierte Weiterleitung) im globalen Modus aktivieren. Nachdem Sie die Funktionen aktiviert haben, müssen Sie das Content Inspection-Profil hinzufügen und die Aktion zur Inhaltsüberprüfung hinzufügen, damit Inline-Geräte den Datenverkehr basierend auf der Inspektion zurücksetzen, blockieren oder löschen können. Fügen Sie dann die Inhaltsinspektionsrichtlinie für die Appliance hinzu, um zu entscheiden, welche Teilmenge des Datenverkehrs an die Inline-Geräte gesendet werden soll. Konfigurieren Sie dann den virtuellen Lastausgleichsserver mit aktivierter Layer-2-Verbindung auf dem Server. Schließlich binden Sie die Inhaltsüberprüfungsrichtlinie an den virtuellen Lastenausgleichsserver.



MBF-Modus (MAC-basierte Weiterleitung) aktivieren

Wenn die Citrix ADC Appliance in Inline-Geräte wie IPS oder Firewalls integriert werden soll, müssen Sie diesen Modus aktivieren. Weitere Informationen zu MBF finden Sie unter Konfigurieren der MAC-basierten Weiterleitung.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns mode mbf
```

Inhaltsprüfung aktivieren

Wenn Sie möchten, dass die Citrix ADC Appliance den Inhalt zur Inspektion entschlüsselt und dann an die Inline-Geräte sendet, müssen Sie die Funktionen Content Inspection und Load Balancing aktivieren.

```
enable ns feature contentInspection LoadBalancing
```

Add Layer 2-Verbindungsmethode

Um die von Inline-Geräten generierte Reaktion zu verarbeiten, verwendet die Appliance den VLAN-Kanal als Layer-2-Methode (L2ConnMethod) für die Kommunikation mit Inline-Geräten.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set l4param -l2ConnMethod <l2ConnMethod>
```

Beispiel

```
set l4param -l2ConnMethod VlanChannel
```


Content-Inspection-Profil für Service hinzufügen

Die Inline-Gerätekonfiguration für eine Citrix ADC Appliance kann in einer Entität namens Content Inspection Profile angegeben werden. Das Profil verfügt über eine Sammlung von Einstellungen, die die Integration mit einem Inline-Gerät erklären.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile Inline_profile1 -type InlineInspection -
ingressinterface "1/2" -egressInterface "1/3"
```

IPS-TCP-Monitor hinzufügen

Wenn Sie Monitore konfigurieren möchten, fügen Sie einen benutzerdefinierten Monitor hinzu.
Hinweis: Wenn Sie Monitore konfigurieren möchten, müssen Sie einen benutzerdefinierten Monitor verwenden. Wenn Sie einen Monitor hinzufügen, müssen Sie den transparenten Parameter aktivieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb monitor <monitorName> <type> [-destIP <ip_addr|ipv6_addr>] [-destPort
 <port>] [-transparent ( YES | NO )]
```

Beispiel:

```
add lb monitor ips_tcp TCP -destIP 192.168.10.2 -destPort 80 -transparent
YES
```

Hinzufügen eines Dienstes

Fügen Sie einen Dienst hinzu. Geben Sie eine Dummy-IP-Adresse an, die keinem der Geräte gehört, einschließlich der Inline-Geräte. Setzen Sie `use source IP address` (USIP) auf YES. Setzen Sie `useproxyport` auf NO. Standardmäßig ist die Systemüberwachung ON, binden Sie den Dienst an einen Integritätsmonitor und legen Sie auch die Option TRANSPARENT im Monitor ON fest. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <Service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor YES -usip ON -useproxyport OFF
```

Beispiel:

```
add service ips_service 192.168.10.2 TCP * -healthMonitor YES -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof
```


Hinzufügen eines Integritätsmonitors

Standardmäßig ist der Integritätsmonitor aktiviert und Sie haben auch die Möglichkeit, ihn bei Bedarf zu deaktivieren. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb monitor <name> TCP -destIP <ip address> -destPort 80 -transparent <
YES, NO>
```

Beispiel:

```
add lb monitor ips_tcp TCP -destIP 192.168.10.2 -destPort 80 -transparent
YES
```

Binden Sie den Dienst an den Integritätsmonitor

Nachdem Sie den Integritätsmonitor konfiguriert haben, müssen Sie den Dienst an den Integritätsmonitor binden. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind service <name> -monitorName <name>
```

Beispiel:

```
bind service ips_svc -monitorName ips_tcp
```

Aktion zur Inhaltsprüfung für Service hinzufügen

Nachdem Sie die Funktion zur Inhaltsüberwachung aktiviert haben und nachdem Sie das Inline-Profil und den Service hinzugefügt haben, müssen Sie die Aktion Inhaltsüberwachung für die Bearbeitung der Anfrage hinzufügen. Basierend auf der Inhaltsüberprüfungsaktion kann das Inline-Gerät Aktionen nach Überprüfung der Daten löschen, zurücksetzen oder blockieren.

Wenn der Inline-Server oder -Dienst nicht verfügbar ist, können Sie den Parameter `ifserverdown` in der Appliance so konfigurieren, dass eine der folgenden Aktionen ausgeführt wird.

CONTINUE: Wenn der Benutzer die Inhaltsüberprüfung umgehen möchte, wenn der Remoteserver ausfällt, können Sie standardmäßig die Aktion “CONTINUE” wählen.
RESET (Standard): Diese Aktion reagiert auf den Client, indem die Verbindung mit RST geschlossen wird.
DROP: Diese Aktion löscht automatisch die Pakete, ohne eine Antwort an den Benutzer zu senden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>] [-reqTimeout <positive_integer>] [-reqTimeoutAction
 <reqTimeoutAction>]
```

```
add ContentInspection action <action_name> -type InlineINSPECTION -serverName
 Service_name/Vserver_name>
```


Beispiel:

```
add ContentInspection action <Inline_action> -type InlineSPECTION -serverName
 Inline_service1
```

Inhaltsüberprüfungsrichtlinie für die Inspektion hinzufügen

Nachdem Sie eine Inhaltsprüfungsaktion erstellt haben, müssen Sie Inhaltsprüfungsrichtlinien hinzufügen, um Prüfungsanforderungen auszuwerten. Die Richtlinie basiert auf einer Regel, die aus einem oder mehreren Ausdrücken besteht. Die Richtlinie bewertet und wählt den Datenverkehr für die Inspektion basierend auf der Regel aus.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Beispiel

```
add contentInspection policy Inline_pol1 -rule true -action Inline_action
```

Hinzufügen von virtuellem Content Switching- oder Lastausgleichsserver vom Typ HTTP/SSL

Um den Webdatenverkehr zu empfangen, müssen Sie einen virtuellen Lastausgleichsserver hinzufügen. Außerdem müssen Sie die Layer2-Verbindung auf dem virtuellen Server aktivieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <vserver name> -l2Conn ON
```

Beispiel:

```
add lb vserver HTTP_vserver HTTP 10.102.29.200 8080 -l2Conn ON
```

Content Inspection Policy an virtuellen Content Switching- oder Load Balancing-Server vom Typ HTTP/SSL binden

Sie binden den virtuellen Lastenausgleichsserver oder den virtuellen Content Switching-Server vom Typ HTTP/SSL an die Inhaltsinspektionsrichtlinie.
Geben Sie an der Eingabeaufforderung Folgendes ein:

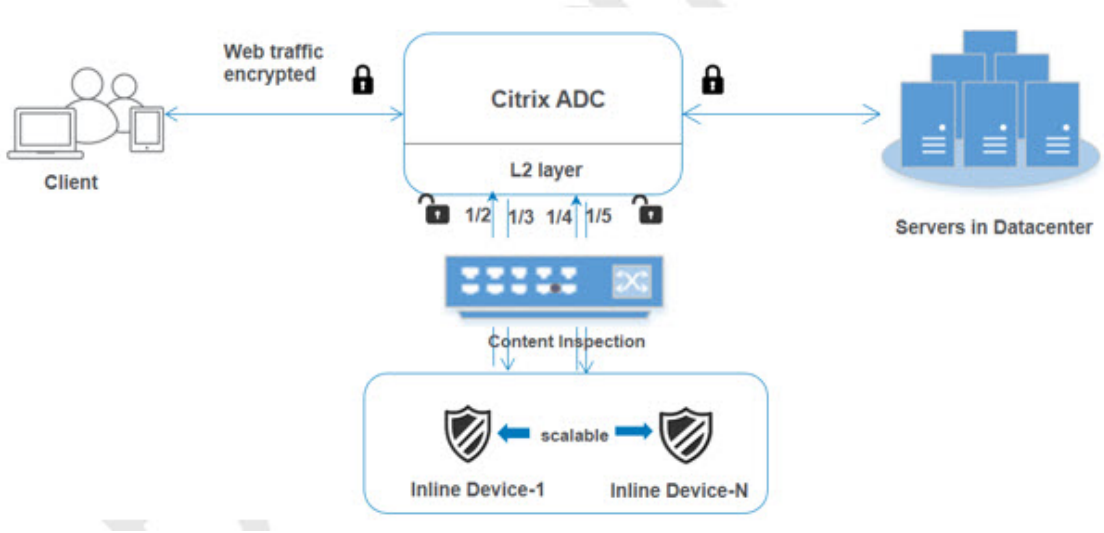
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <
priority > -type <REQUEST>
```

Beispiel:

```
bind lb vserver HTTP_vserver -policyName Inline_pol1 -priority 100 -type
REQUEST
```


Szenario 2: Lastenausgleich mehrerer Inline-Geräte mit dedizierten Schnittstellen

Wenn Sie zwei oder mehr Inline-Geräte verwenden, müssen Sie die Geräte mit verschiedenen Content-Inspektionsdiensten in einem dedizierten VLAN-Setup ausgleichen. In diesem Fall gleicht die Citrix ADC Appliance die Geräte so aus, dass eine Teilmenge des Datenverkehrs an jedes Gerät über eine dedizierte Schnittstelle gesendet wird.
Grundlegende Konfigurationsschritte finden Sie unter Szenario 1.



Inhaltsprüfprofil1 hinzufügen für Service1

Inline-Konfigurationen für eine Citrix ADC Appliance können in einer Entität namens Content Inspection Profile angegeben werden. Das Profil verfügt über eine Sammlung von Geräteeinstellungen. Das Content Inspection Profile1 wird für Inline Service 1 erstellt und die Kommunikation erfolgt über 1/2 und 1/3 dedizierte Schnittstellen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile Inline_profile1 -type InlineInspection -
ingressinterface “1/2” -egressInterface “1/3”
```

Add content inspection profile2 for service2

Das Content Inspection Profile2 wird für service2 hinzugefügt und das Inline-Gerät kommuniziert über `1/41/5` dedizierte Schnittstellen mit der Appliance.
Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile Inline_profile2 -type InlineInspection -
ingressinterface "1/4" -egressInterface "1/5"
```

Service 1 für Inline-Gerät 1 hinzufügen

Nachdem Sie die Inhaltsinspektion aktiviert und das Inline-Profil hinzugefügt haben, müssen Sie einen Inline-Dienst 1 für Inline-Gerät 1 hinzufügen, um Teil des Lastausgleichs zu sein. Der Dienst, den Sie hinzufügen, enthält alle Inline-Konfigurationsdetails.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <Service_name_1> <Pvt_IP1> TCP * -contentInspectionProfileName
<Inline_Profile_1> -healthmonitor OFF -usip ON -useproxyport OFF
```

Beispiel:

```
add service Inline_service1 10.102.29.200 TCP 80 -contentInspectionProfileName
 Inline_profile1 -healthmonitor OFF -usip ON -useproxyport OFF
```

Service 2 für Inline-Gerät 2 hinzufügen

Nachdem Sie die Inhaltsinspektion aktiviert und das Inline-Profil hinzugefügt haben, müssen Sie einen Inline-Dienst 2 für Inline-Gerät 2 hinzufügen. Der Dienst, den Sie hinzufügen, enthält alle Inline-Konfigurationsdetails.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <Service_name_1> <Pvt_IP1> TCP * -contentInspectionProfileName
<Inline_Profile_2> -healthmonitor OFF -usip ON -useproxyport OFF
```

Beispiel:

```
add service Inline_service1 10.29.20.205 TCP 80 -contentInspectionProfileName
 Inline_profile2 -healthmonitor OFF -usip ON -useproxyport OFF
```

Hinzufügen eines virtuellen Lastausgleichsservers

Nachdem Sie das Inline-Profil und die Dienste hinzugefügt haben, müssen Sie einen virtuellen Lastausgleichsserver für den Lastenausgleich der Dienste hinzufügen.

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add lb vserver <vserver_name> TCP <Pvt_IP3> <port>
```

Beispiel:

```
add lb vserver lb-Inline_vserver TCP *
```

Binden Sie Dienst 1 an den virtuellen Lastausgleichsserver

Nachdem Sie den virtuellen Lastausgleichsserver hinzugefügt haben, binden Sie nun den virtuellen Lastausgleichsserver an den ersten Dienst.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Beispiel:

```
bind lb vserver lb-Inline_vserver Inline_service1
```

Binden Sie Dienst 2 an den virtuellen Lastausgleichsserver

Nachdem Sie den virtuellen Lastausgleichsserver hinzugefügt haben, binden Sie den Server nun an den zweiten Dienst.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Beispiel:

```
bind lb vserver lb-Inline_vserver Inline_service2
```

Hinzufügen von Inhaltsprüfungsmaßnahmen für den Service

Nachdem Sie die Funktion Inhaltsüberprüfung aktiviert haben, müssen Sie die Aktion Inhaltsüberprüfung für die Verarbeitung der Inline-Anforderungsinformationen hinzufügen. Basierend auf der ausgewählten Aktion wird das Inline-Gerät abgesetzt, zurückgesetzt oder blockiert, nachdem es die angegebene Teilmenge des Datenverkehrs untersucht hat.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>] [-reqTimeout <positive_integer>] [-reqTimeoutAction
 <reqTimeoutAction>]
```

```
add ContentInspection action < action_name > -type InlineINSPECTION -
serverName Service_name/Vserver_name>
```

Beispiel:


```
add ContentInspection action Inline_action -type InlineINSPECTION -serverName
 lb-Inline_vserver
```

Inhaltsüberprüfungsrichtlinie für die Inspektion hinzufügen

Nachdem Sie eine Aktion zur Inhaltsüberwachung erstellt haben, müssen Sie die Inhaltsinspektionsrichtlinie hinzufügen, um Serviceanfragen zu bewerten. Die Richtlinie basiert auf einer Regel, die aus einem oder mehreren Ausdrücken besteht. Die Regel ist der Inhaltsprüfung Aktion zugeordnet, die zugeordnet ist, wenn eine Anforderung mit der Regel übereinstimmt.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Beispiel:

```
add contentInspection policy Inline_pol1 -rule true -action Inline_action
```

Hinzufügen von virtuellem Content Switching- oder Lastausgleichsserver vom Typ HTTP/SSL

Fügen Sie einen virtuellen Content Switching-Server oder zum Lastenausgleich hinzu, um Webdatenverkehr zu akzeptieren. Außerdem müssen Sie die Layer2-Verbindung auf dem virtuellen Server aktivieren.
Weitere Informationen zum Lastenausgleich finden Sie unter Funktionsweise des Lastenausgleichs .

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <vserver name> -l2Conn ON
```

Beispiel:

```
add lb vserver http_vserver HTTP 10.102.29.200 8080 -l2Conn ON
```

Bind Content Inspection Policy für den Lastenausgleich virtueller Server vom Typ HTTP/SSL

Sie müssen den virtuellen Content Switching- oder Lastausgleichsserver des Typs HTTP/SSL an die Inhaltsüberprüfungsrichtlinie binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

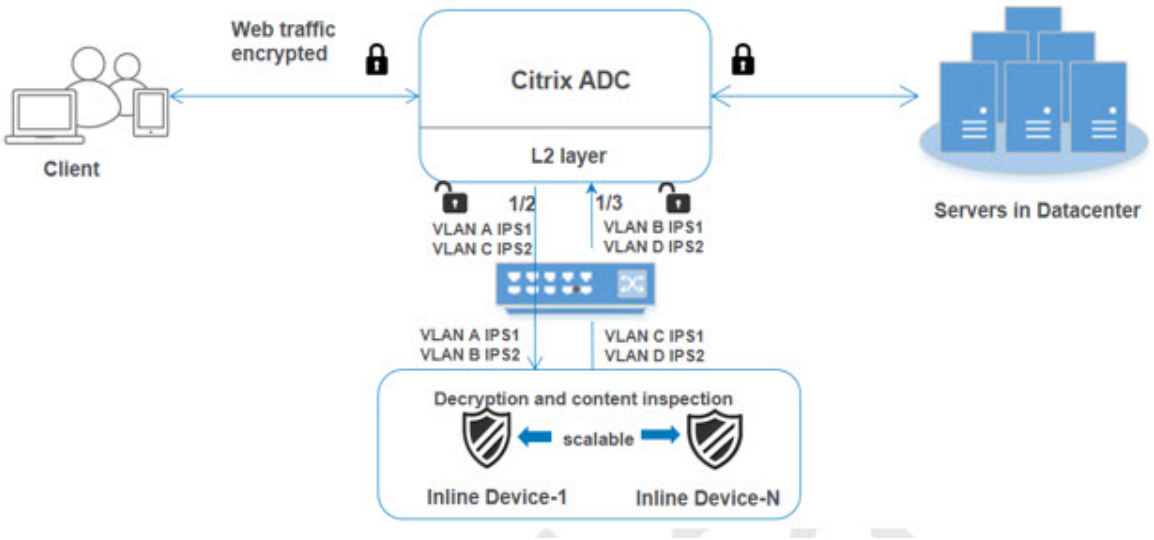
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <> -
type <L7InlineREQUEST | L4Inline-REQUEST>
```

Beispiel:

```
bind lb vserver http_vserver -policyName Inline_pol1 -priority 100 -type
REQUEST
```


Szenario 3: Lastenausgleich mehrerer Inline-Geräte über gemeinsame Schnittstellen

Sie können auf diese Konfiguration verweisen, wenn Sie mehrere Inline-Geräte verwenden und wenn Sie die Geräte über verschiedene Dienste in einer gemeinsam genutzten VLAN-Schnittstelle laden möchten. Diese Konfiguration mit gemeinsam genutzten VLAN-Schnittstellen ähnelt dem Anwendungsfall 2. Informationen zur Grundkonfiguration finden Sie unter Szenario 2.



Binden Sie VLAN A mit aktivierter Freigabeoption

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind vlan <id> -ifnum <interface> -tagged
```

Beispiel:

```
bind vlan 100 -ifnum 1/2 tagged
```

Binden Sie VLAN B mit aktivierter Freigabeoption

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind vlan <id> -ifnum <interface> -tagged
```

Beispiel:

```
bind vlan 200 -ifnum 1/3 tagged
```

Binden Sie VLAN C mit aktivierter Freigabeoption

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind vlan <id> -ifnum <interface> -tagged
```


Beispiel:

```
bind vlan 300 -ifnum 1/2 tagged
```

Binden Sie VLAN D mit aktivierter Freigabeoption

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind vlan <id> -ifnum <interface> -tagged
```

Beispiel:

```
bind vlan 400 -ifnum 1/3 tagged
```

Inhaltsprüfprofil1 hinzufügen für Service1

Inline-Konfigurationen für eine Citrix ADC Appliance können in einer Entität namens Content Inspection Profile angegeben werden. Das Profil verfügt über eine Sammlung von Geräteeinstellungen. Das Content Inspection-Profil wird für den Inline-Service 1 erstellt und die Kommunikation erfolgt über dedizierte 1/2- und 1/3-Schnittstellen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile Inline_profile1 -type InlineInspection -
ingressinterface “1/2” -egressInterface “1/3” -egressVlan 100 -ingressVlan
 300
```

Add content inspection profile2 for service2

Das Content Inspection Profile2 wird für service2 hinzugefügt und das Inline-Gerät kommuniziert über `1/21/3` dedizierte Schnittstellen mit der Appliance.

Geben Sie an der Eingabeaufforderung Folgendes ein:

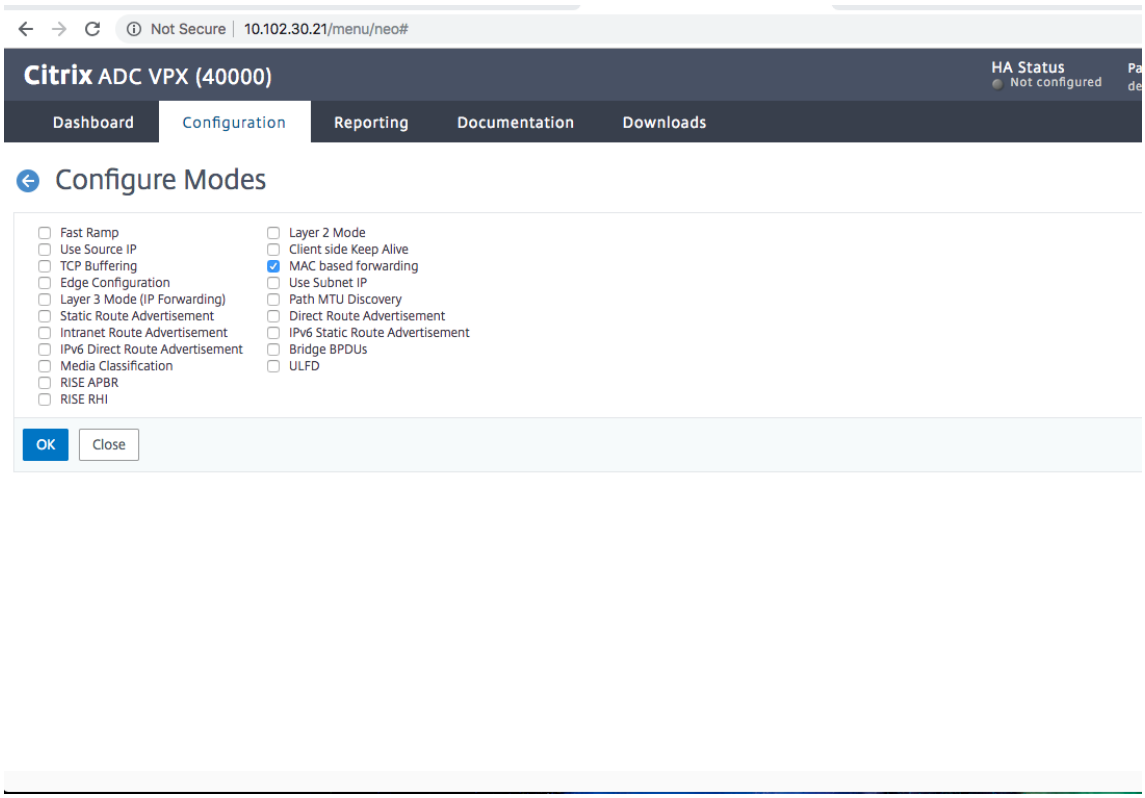
```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

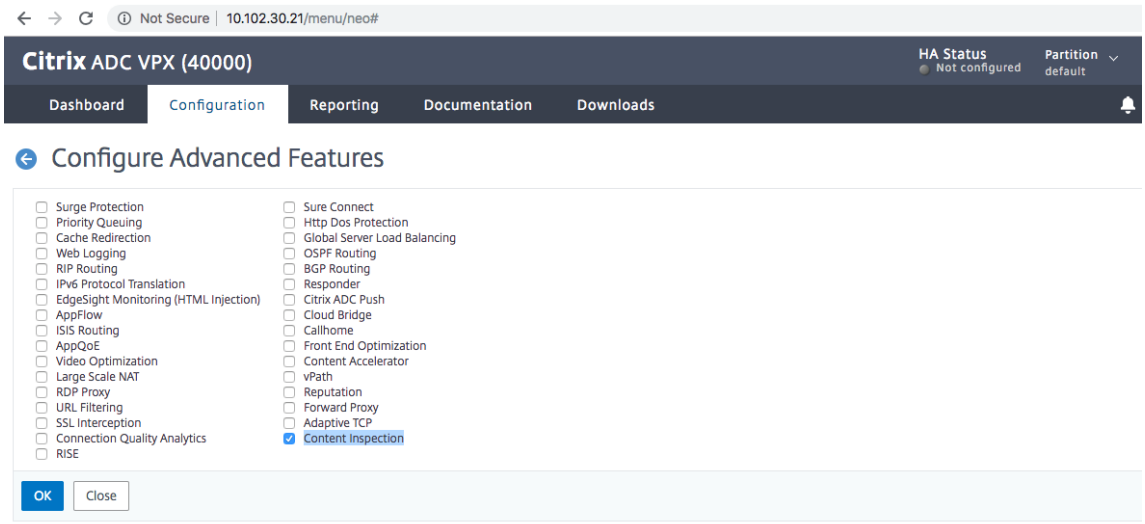
```
add contentInspection profile Inline_profile2 -type InlineInspection -
ingressinterface “1/2” -egressInterface “1/3” -egressVlan 200 -ingressVlan
 400
```


Konfigurieren der Inline-Dienstintegration über die Citrix ADC GUI

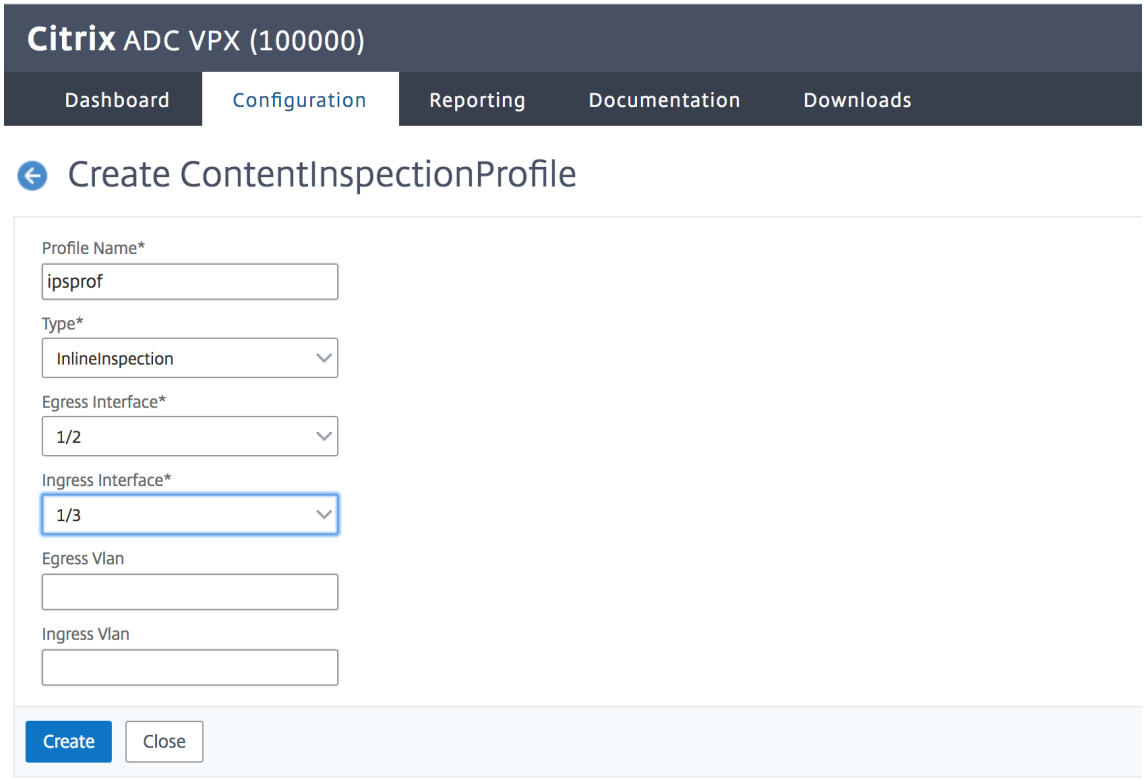
1. Melden Sie sich bei der Citrix ADC Appliance an, und navigieren Sie zur Registerkarte **Konfiguration** .
2. Navigieren Sie zu **System** > **Einstellungen** > **Modi konfigurieren** .
3. Wählen **Sie auf der Seite Modi konfigurieren** die Option **Mac Based Forwarding** aus.
4. Klicken Sie auf **OK** und **schließen**.



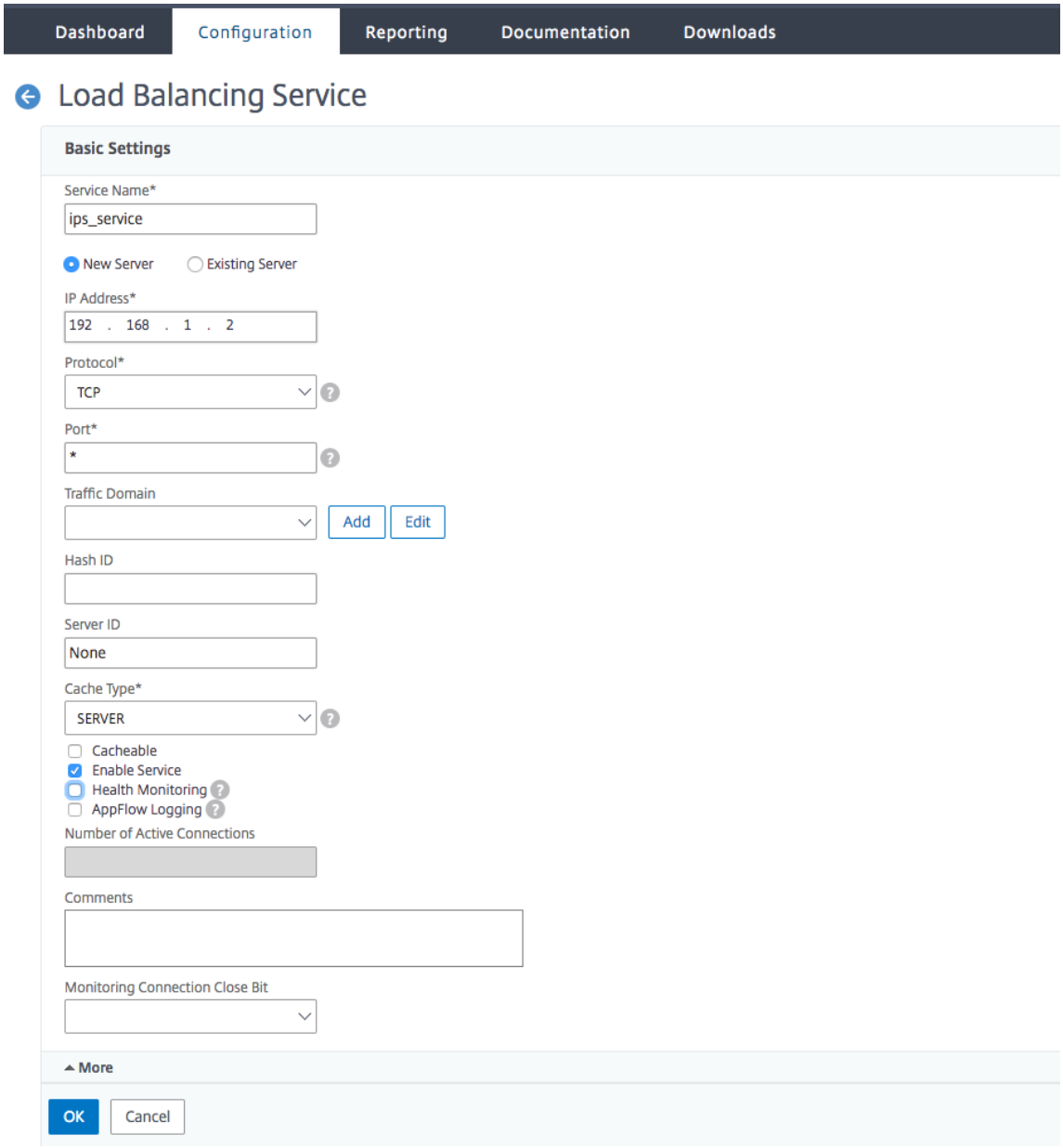
5. Navigieren Sie zu **System** > **Einstellungen** > **Erweiterte Funktionen konfigurieren**.
6. Wählen **Sie auf der Seite Erweiterte Funktion konfigurieren** die Option **Inhaltsinspektion** aus.
7. Klicken Sie auf **OK** und **schließen**.



8. Navigieren Sie zu **Sicherheit** > **Inhaltsinspektion** > **ContentInspection-Profile** .
9. Klicken Sie auf der Seite **ContentInspection-Profile** auf **Hinzufügen** .
10. **Legen Sie auf der Seite ContentInspection-Profile erstellen** die folgenden Parameter fest.
    a) Profilname Name des Content-Inspektionsprofils.
    b) Geben Sie ein. Wählen Sie den Profiltyp als InlineInspection aus.
    c) Schnittstelle ausziehen. Schnittstelle, über die die Appliance Datenverkehr vom Citrix ADC an das Inline-Gerät sendet.
    d) Eingangs-Schnittstelle. Schnittstelle, über die die Appliance Datenverkehr vom Inline-Gerät zum Citrix ADC empfängt.
    e) VLAN auslassen. Schnittstellen-VLAN-ID, über die der Datenverkehr an das Inline-Gerät gesendet wird.
    f) Eindringendes VLAN. Schnittstellen-VLAN-ID, über die die Appliance Datenverkehr von Inline zu Citrix ADC empfängt (falls konfiguriert).

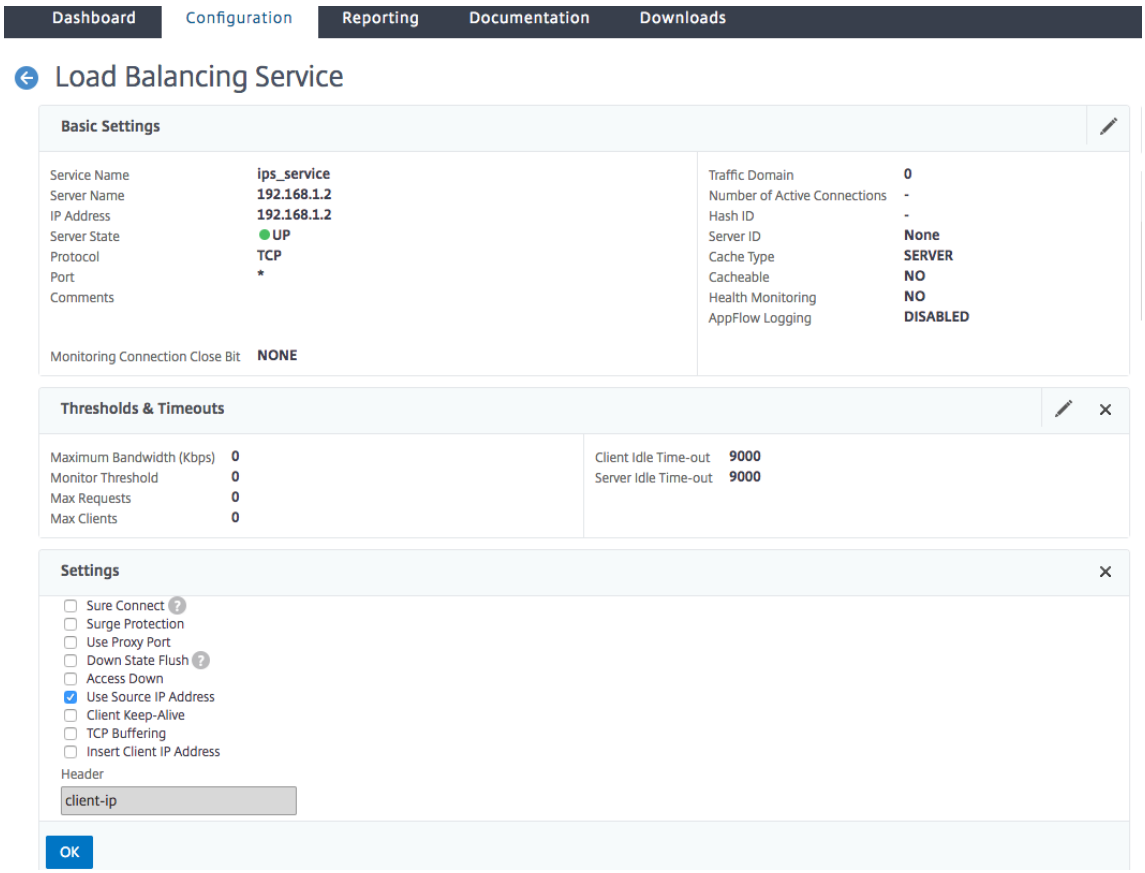


11. Klicken Sie auf **Erstellen** und **Schließen**.
12. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**, und klicken Sie auf **Hinzufügen**.
13. Legen Sie auf der Seite **Dienste** die folgenden Parameter fest:
    a) Dienstname. Name des Lastenausgleichsdiensts.
    b) IP-Adresse. Verwenden Sie eine Dummy-IP-Adresse. Hinweis: Kein Gerät darf die IP-Adresse besitzen.
    c) -Protokoll. Wählen Sie den Protokolltyp als TCP aus.
    d) Port. Geben Sie ein *
    e) Gesundheitsüberwachung. Deaktivieren Sie diese Option und aktivieren Sie sie nur, wenn Sie den Dienst an den TCP-Typmonitor binden möchten. Wenn Sie einen Monitor an den Dienst binden möchten, muss die TRANSPARENT Option im Monitor eingeschaltet sein. Siehe Schritt 14 zum Hinzufügen eines Monitors und zum Binden des Monitors an den Dienst.
    f) Klicken Sie auf **OK**.

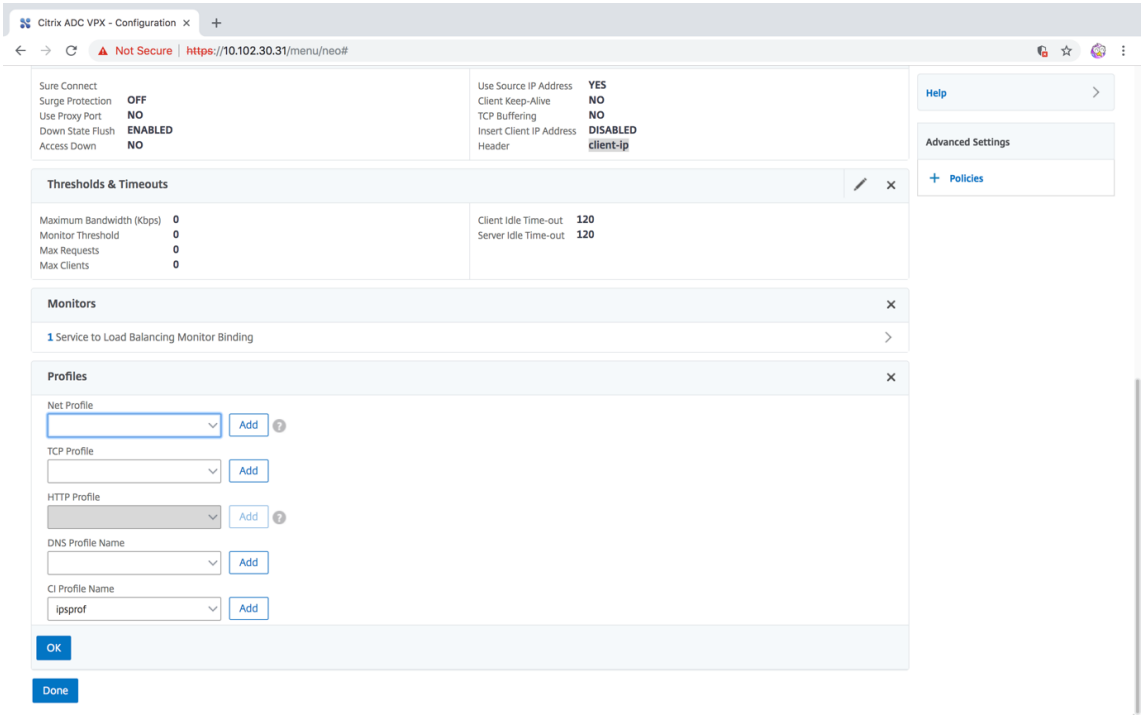


14. Bearbeiten **Sie im Abschnitt Einstellungen** Folgendes, und klicken Sie auf **OK** .

    a) Proxy-Port verwenden: Ausschalten
    b) Quell-IP-Adresse verwenden: Einschalten



15. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Profile**.
16. Gehen Sie zum Abschnitt **Profile**, fügen Sie das Inline-Content-Inspektionsprofil hinzu, und klicken Sie auf **OK** .

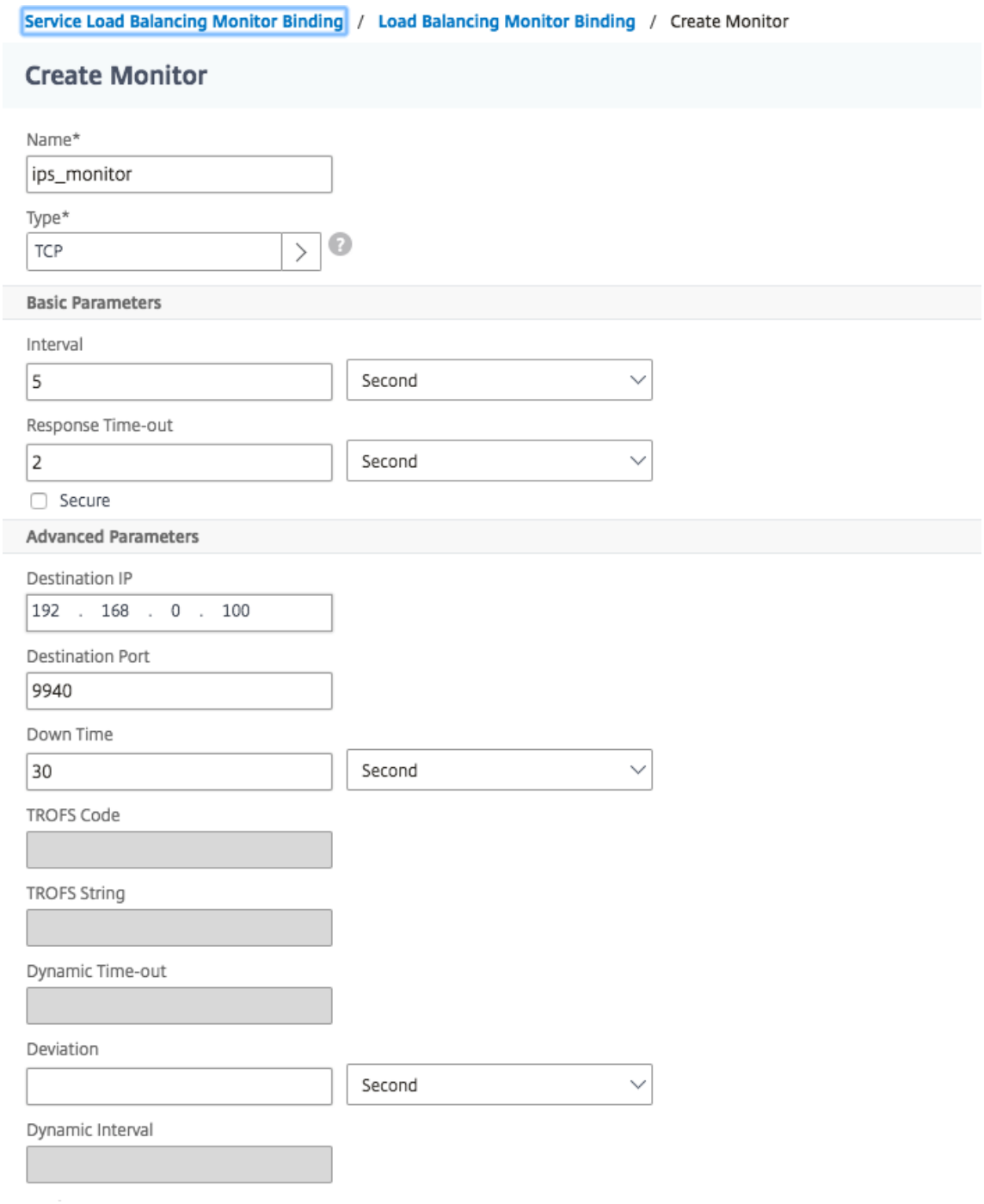


17. Gehen Sie zum Abschnitt **Monitore**, **Bindungen hinzufügen** > **Wählen Sie Monitor** > **Hinzufügen** .

    a) Name: Name des Monitors
    b) Typ: Wählen Sie TCP Typ
    c) Ziel-IP, PORT: Ziel-IP-Adresse und -Port.
    d) Transparent: Einschalten

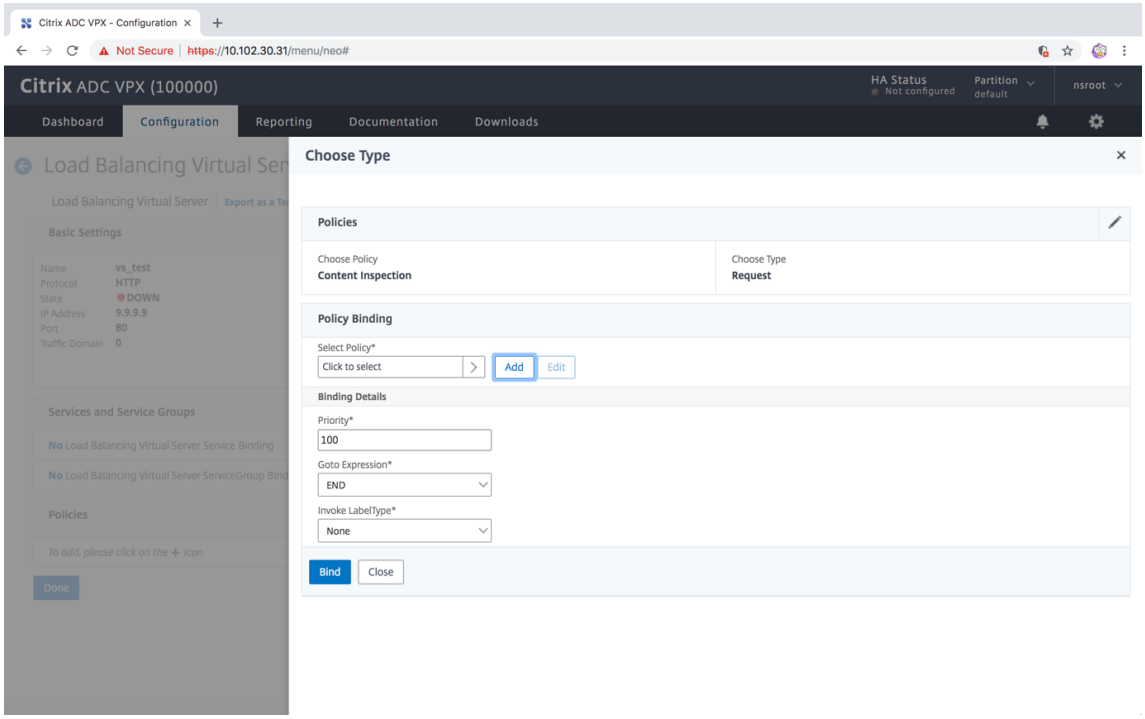
    Hinweis: Monitorpakete müssen durch das Inline-Gerät fließen, um den Status des Inline-Geräts zu überwachen.

18. Klicken Sie auf **Erstellen**.



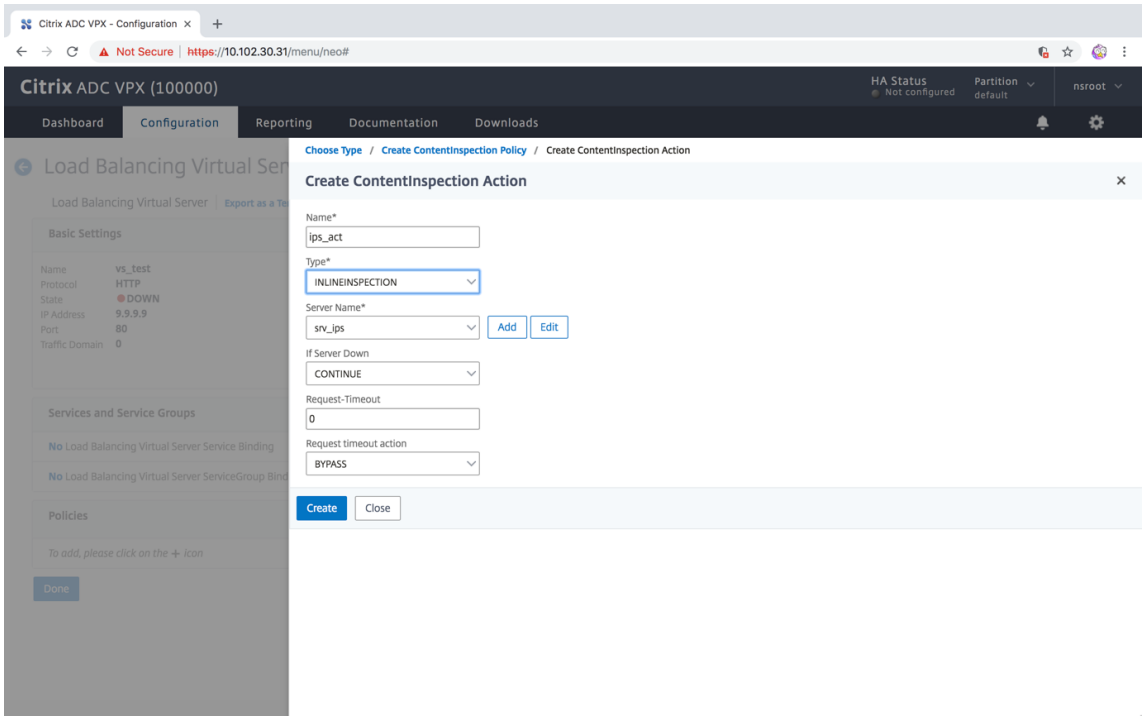
19. Klicken Sie auf **Fertig**.
20. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**. Fügen Sie einen virtuellen Server vom Typ HTTP oder SSL hinzu.
21. Nachdem Sie die Serverdetails eingegeben haben, klicken Sie auf **OK** und erneut auf **OK**.
22. Aktivieren Sie im Abschnitt **Datenverkehrseinstellungen** des virtuellen Lastenausgleichsservers Layer-2-Parameter.

23. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.
24. Gehen Sie in den Abschnitt **Richtlinien** und klicken Sie auf das “+” -Symbol, um die Inhaltsüberprüfungsrichtlinie zu konfigurieren.
25. Wählen Sie auf der Seite **“Richtlinie** auswählen” die Option Inhaltsüberprüfung aus. Klicken Sie auf **Weiter**.
26. Klicken Sie im Abschnitt **Richtlinienbindung** auf **Hinzufügen**, um eine Richtlinie zur Inhaltsüberwachung hinzuzufügen.



27. Geben **Sie auf der Seite ContentInspection-Richtlinie erstellen** einen Namen für die Inline-Inhaltsüberprüfungsrichtlinie ein.
28. Klicken Sie im Feld **Aktion** auf **Hinzufügen**, um eine Inline-Inhaltsprüfung zu erstellen.
29. **Legen Sie auf der Seite CI-Aktion erstellen** die folgenden Parameter fest:
    a) Name. Name der Inhaltsüberprüfung Inline-Richtlinie.
    b) Geben Sie ein. Wählen Sie den Typ als InlineInspection aus.
    c) Server. Wählen Sie den Server/Dienst als Inline-Geräte aus.
    d) Wenn Server heruntergefahren ist. Wählen Sie einen Vorgang aus, wenn der Server ausfällt.
    e) Zeitüberschreitung der Anforderung. Wählen Sie einen Zeitüberschreitungswert aus. Sie können Standardwerte verwenden.
    f) Zeitüberschreitungsaktion anfordern. Wählen Sie eine Zeitüberschreitungsaktion aus. Sie können Standardwerte verwenden.

30. Klicken Sie auf **Erstellen**.



31. Klicken Sie auf **Erstellen**.
32. Geben **Sie auf der Seite CI-Richtlinie erstellen** weitere Details ein:
33. Klicken Sie auf **OK** und **schließen**.

Integration mit IPS oder NGFW als Inline-Geräte mit SSL-Forward-Proxy

October 5, 2021

Sicherheitsgeräte wie Intrusion Prevention System (IPS) und Next Generation Firewall (NGFW) schützen Server vor Netzwerkangriffen. Diese Geräte können den Live-Datenverkehr überprüfen und werden in der Regel im Layer 2-Inline-Modus bereitgestellt. Die SSL-Forward-Proxy-Appliance bietet Sicherheit für Benutzer und das Unternehmensnetzwerk beim Zugriff auf Ressourcen im Internet.

Eine SSL-Forward-Proxy-Appliance kann mit einem oder mehreren Inline-Geräten integriert werden, um Bedrohungen zu verhindern und erweiterten Sicherheitsschutz zu bieten. Bei den Inline-Geräten kann es sich um ein beliebiges Sicherheitsgerät wie IPS und NGFW handeln.

Einige Anwendungsfälle, in denen Sie von der SSL-Forward-Proxy-Appliance und der Inline-Geräteintegration profitieren können, sind:

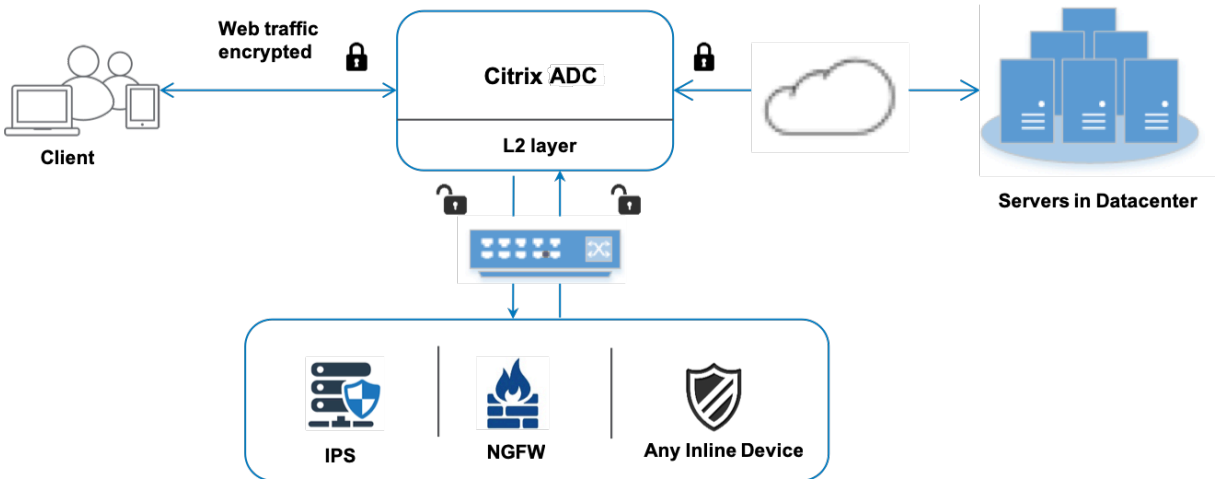
- **Überprüfen des verschlüsselten Datenverkehrs:** Die meisten IPS- und NGFW-Appliances umgehen verschlüsselten Datenverkehr, wodurch Server anfällig für Angriffe werden können.

Eine SSL-Forward-Proxy-Appliance kann den Datenverkehr entschlüsseln und ihn zur Überprüfung an die Inline-Geräte senden. Diese Integration erhöht die Netzwerksicherheit des Kunden.

- **Entladen von Inline-Geräten aus der TLS/SSL -Verarbeitung:** Die TLS/SSL -Verarbeitung ist teuer, was zu einer hohen CPU-Auslastung in IPS- oder NGFW-Appliances führen kann, wenn sie auch den Datenverkehr entschlüsseln. Eine SSL-Forward-Proxy-Appliance hilft beim Auslagern von TLS/SSL-Verarbeitung von Inline-Geräten. Inline-Geräte können daher ein höheres Verkehrsaufkommen untersuchen.
- **Inline-Geräte für den Ladeausgleich:** Wenn Sie mehrere Inline-Geräte für die Verwaltung des hohen Datenverkehrs konfiguriert haben, kann eine SSL-Forward-Proxy-Appliance einen Lastausgleich durchführen und den Datenverkehr gleichmäßig auf diese Geräte verteilen.
- **Intelligente Auswahl des Datenverkehrs:** Statt den gesamten Datenverkehr zur Inspektion an das Inline-Gerät zu senden, führt die Appliance eine intelligente Auswahl des Datenverkehrs durch. Beispielsweise wird das Senden von Textdateien zur Überprüfung an die Inline-Geräte übersprungen.

SSL-Forward-Proxy-Integration mit Inline-Geräten

Das folgende Diagramm zeigt, wie ein SSL-Forward-Proxy in Inline-Sicherheitsgeräte integriert ist.



Wenn Sie Inline-Geräte mit der SSL Forward-Proxy-Appliance integrieren, interagieren die Komponenten wie folgt:

1. Ein Client sendet eine Anforderung an eine SSL-Forward-Proxy-Appliance.
2. Die Appliance sendet die Daten an das Inline-Gerät zur Inhaltsüberprüfung basierend auf der Richtlinienbewertung. Bei HTTPS-Datenverkehr entschlüsselt die Appliance die Daten und sendet sie zur Inhaltsüberprüfung im Klartext an das Inline-Gerät.

> **Hinweis:**
>
> Wenn zwei oder mehr Inline-Geräte vorhanden sind, gleicht die Appliance die Geräte aus und sendet den Datenverkehr.

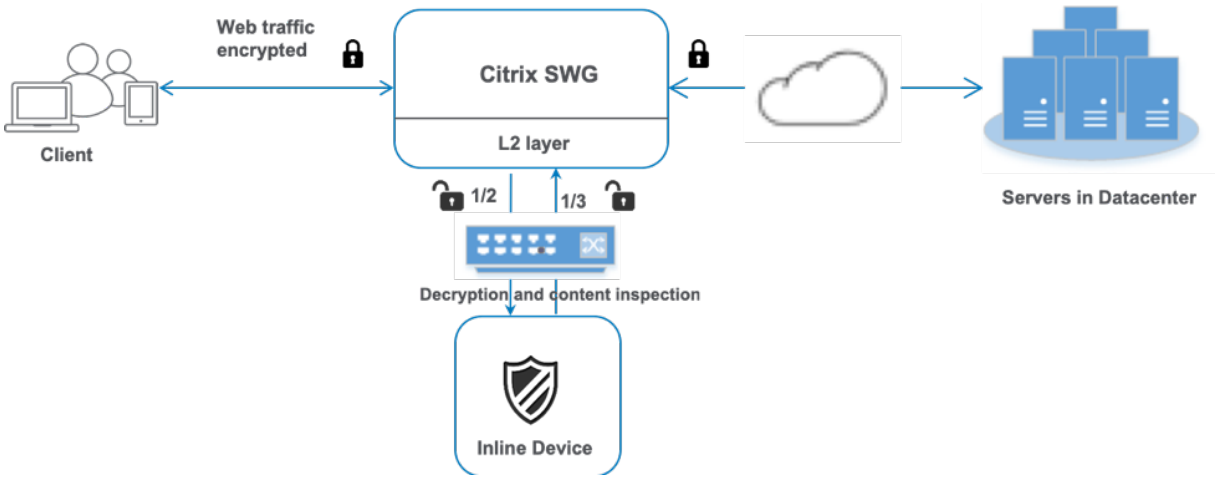
3. Fügen Sie einen virtuellen Content Switching- oder HTTP/HTTPS-Load Balancing-Server hinzu.
4. Das Inline-Gerät prüft die Daten auf Bedrohungen und entscheidet, ob die Daten gelöscht, zurückgesetzt oder an die Appliance gesendet werden sollen.
5. Wenn Sicherheitsbedrohungen vorliegen, ändert das Gerät die Daten und sendet sie an die Appliance.
6. Bei HTTPS-Datenverkehr verschlüsselt die Appliance die Daten erneut und leitet die Anforderung an den Back-End-Server weiter.
7. Der Back-End-Server sendet die Antwort an die Appliance.
8. Die Appliance entschlüsselt die Daten erneut und sendet sie zur Überprüfung an das Inline-Gerät.
9. Das Inline-Gerät prüft die Daten. Wenn Sicherheitsbedrohungen vorliegen, ändert das Gerät die Daten und sendet sie an die Appliance.
10. Die Appliance verschlüsselt die Daten erneut und sendet die Antwort an den Client.

Konfigurieren der Inline-Geräteintegration

Sie können eine SSL-Forward-Proxy-Appliance mit einem Inline-Gerät auf drei verschiedene Arten konfigurieren:

Szenario 1: Verwenden eines einzelnen Inline-Geräts

Um ein Sicherheitsgerät (IPS oder NGFW) in den Inline-Modus zu integrieren, müssen Sie die Inhaltsinspektion und die MAC-basierte Weiterleitung (MBF) im globalen Modus auf der SSL-Forward-Proxy-Appliance aktivieren. Fügen Sie anschließend ein Inhaltsinspektionsprofil, einen TCP-Dienst, eine Inhaltsüberprüfungsaktion für Inline-Geräte hinzu, um den Datenverkehr basierend auf der Inspektion zurückzusetzen, zu blockieren oder zu löschen. Fügen Sie außerdem eine Richtlinie zur Inhaltsüberprüfung hinzu, die von der Appliance verwendet wird, um die Teilmenge des Datenverkehrs zu bestimmen, die an die Inline-Geräte gesendet werden soll. Konfigurieren Sie schließlich den virtuellen Proxyserver mit aktivierter Layer-2-Verbindung auf dem Server und binden Sie die Inhaltsüberprüfungsrichtlinie an diesen virtuellen Proxyserver.



Gehen Sie wie folgt vor:

1. Aktivieren Sie den MAC-basierten Weiterleitungsmodus (MPF).
2. Aktivieren Sie die Funktion zur Inhaltsüberprüfung.
3. Fügen Sie ein Inhaltsinspektionsprofil für den Service hinzu. Das Content-Inspektionsprofil enthält die Inline-Geräteeinstellungen, die die SSL-Forward-Proxy-Appliance mit einem Inline-Gerät integrieren.
4. (Optional) Fügen Sie einen TCP-Monitor hinzu.

   > **Hinweis:**
   >
   > Transparente Geräte haben keine IP-Adresse. Um Integritätsprüfungen durchzuführen, müssen Sie daher einen Monitor explizit binden.

5. Fügen Sie einen Dienst hinzu. Ein Dienst stellt ein Inline-Gerät dar.
6. (Optional) Binden Sie den Dienst an den TCP-Monitor.
7. Fügen Sie eine Inhaltsinspektionsaktion für den Service hinzu.
8. Fügen Sie eine Richtlinie zur Inhaltsüberprüfung hinzu, und geben Sie die Aktion an.
9. Fügen Sie einen virtuellen HTTP- oder HTTPS-Proxyserver (Content Switching) hinzu.
10. Binden Sie die Richtlinie zur Inhaltsüberprüfung an den virtuellen Server.

Konfiguration mit der CLI

Geben Sie die folgenden Befehle an der Eingabeaufforderung ein. Beispiele werden nach den meisten Befehlen angegeben.

1. MBF aktivieren.

```
enable ns mode mbf
```


1. Aktivieren Sie das Feature.

```
enable ns feature contentInspection
```

1. Fügen Sie ein Inhaltsinspektionsprofil hinzu.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile ipsprof -type InlineInspection -ingressinterface
 “1/2” -egressInterface “1/3”
```

1. Fügen Sie einen Dienst hinzu. Geben Sie eine Dummy-IP-Adresse an, die keinem der Geräte gehört, einschließlich der Inline-Geräte. Setzen Sie `use source IP address` (USIP) auf YES. Setzen Sie `useproxyport` auf NO. Standardmäßig ist die Systemüberwachung ON, binden Sie den Dienst an einen Integritätsmonitor und legen Sie auch die Option TRANSPARENT im Monitor ON fest.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor YES -usip YES -useproxyport NO
```

Beispiel:

```
add service ips_service 198.51.100.2 TCP * -healthMonitor YES -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof
```

1. Fügen Sie einen Integritätsmonitor hinzu. Standardmäßig ist der Integritätsmonitor aktiviert und Sie haben auch die Möglichkeit, ihn bei Bedarf zu deaktivieren. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   add lb monitor <name> TCP -destIP <ip address> -destPort 80 -transparent
    <YES, NO>
   ```

Beispiel:

```
add lb monitor ips_tcp TCP -destIP 192.168.10.2 -destPort 80 -transparent
YES
```

1. Binden Sie den Dienst an den Integritätsmonitor

Nachdem Sie den Integritätsmonitor konfiguriert haben, müssen Sie den Dienst an den Integritätsmonitor binden. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind service <name> -monitorName <name>
```

Beispiel:

```
bind service ips_svc -monitorName ips_tcp
```


1. Fügen Sie eine Inhaltsüberprüfungsaktion hinzu.

```
add contentInspection action <name> -type INLINEINSPECTION -serverName <
string>
```

Beispiel:

```
add contentInspection action ips_action -type INLINEINSPECTION -serverName
ips_service
```

1. Fügen Sie eine Richtlinie zur Inhaltsüberprüfung hinzu.

```
add contentInspection policy <name> -rule <expression> -action <string>
```

Beispiel:

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE(\"CONNECT\")
"-action ips_action
```

1. Fügen Sie einen virtuellen Proxyserver hinzu.

```
add cs vserver <name> PROXY <IPAddress> <port> -cltTimeout <secs> -Listenpolicy
 <expression> -authn401 ( ON | OFF )-authnVsName <string> -l2Conn ON
```

> **Hinweis:**
>
> Der Lastausgleich virtueller Server vom Typ HTTP/SSL wird ebenfalls unterstützt.

Beispiel:

```
add cs vserver transparentcs PROXY * * -cltTimeout 180 -Listenpolicy exp1 -
authn401 on -authnVsName swg-auth-vs-trans-http -l2Conn ON
```

1. Binden Sie die Richtlinie an den virtuellen Server.

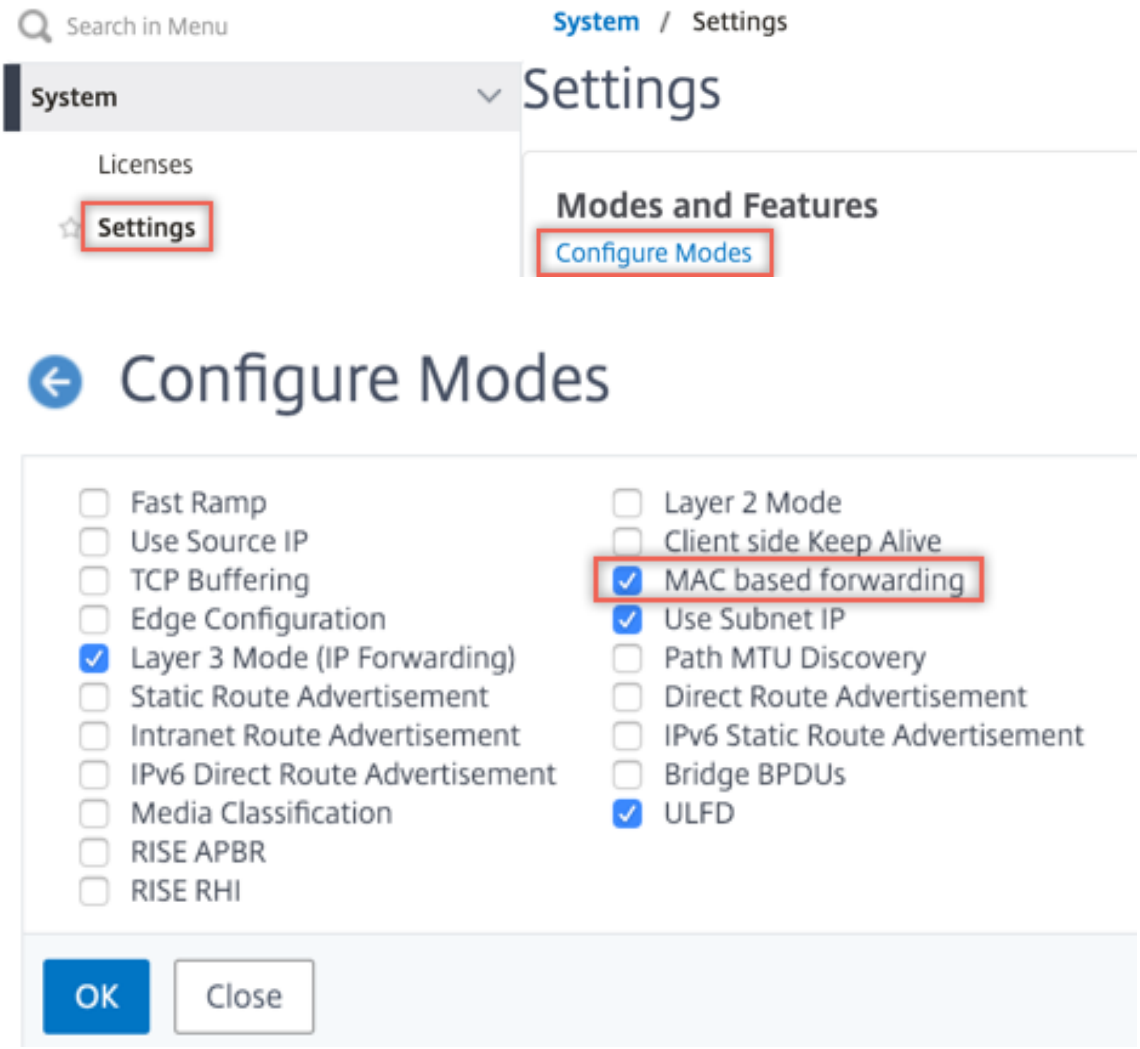
```
bind cs vserver <name> -policyName <string> -priority <positive_integer> -
gotoPriorityExpression <expression> -type REQUEST
```

Beispiel:

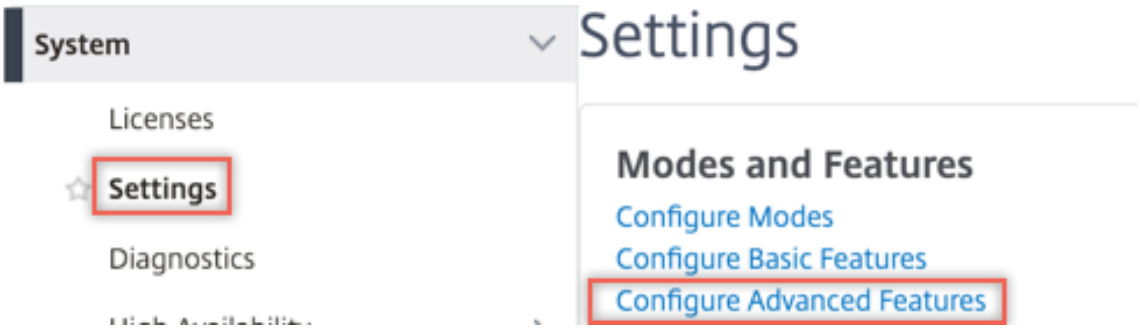
```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -gotoPriorityExpression
 END -type REQUEST
```

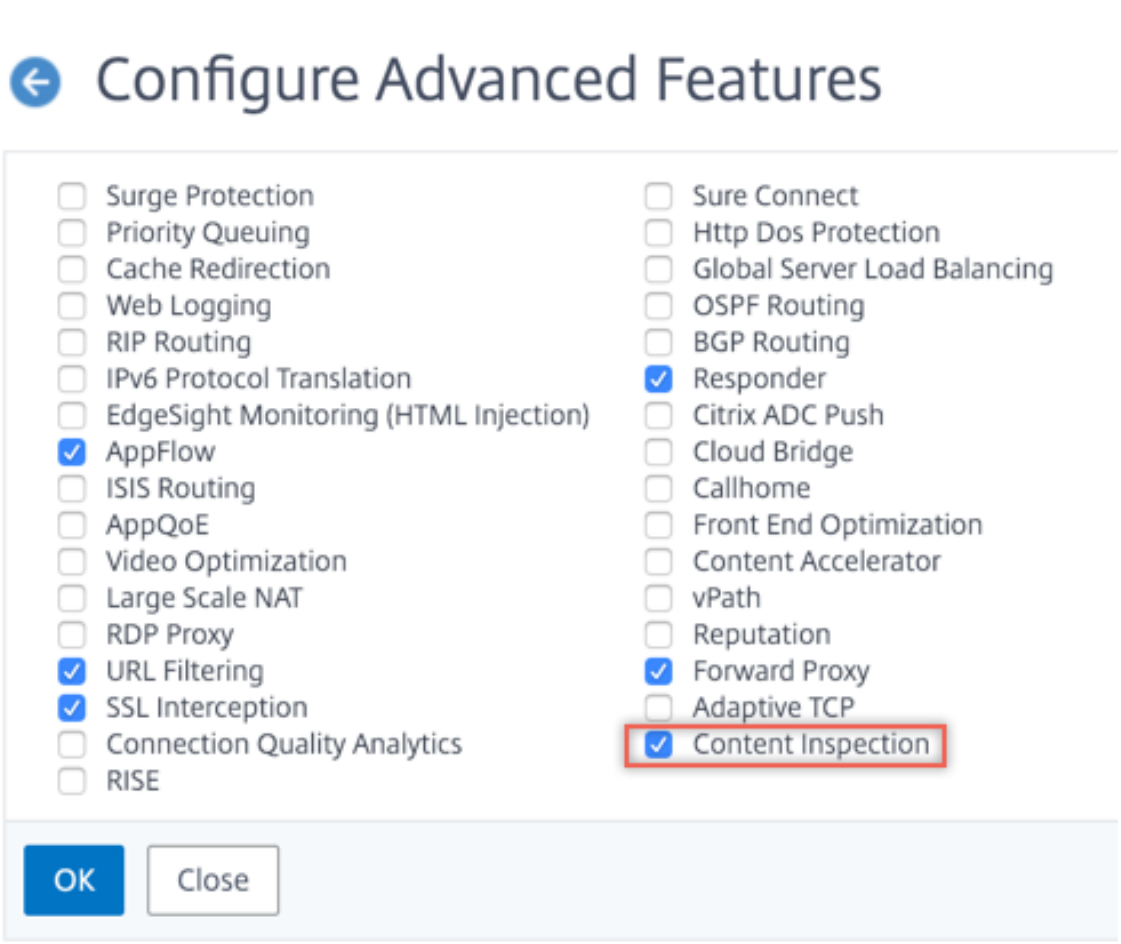
Konfigurieren Sie mit der GUI

1. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Modi konfigurieren**.

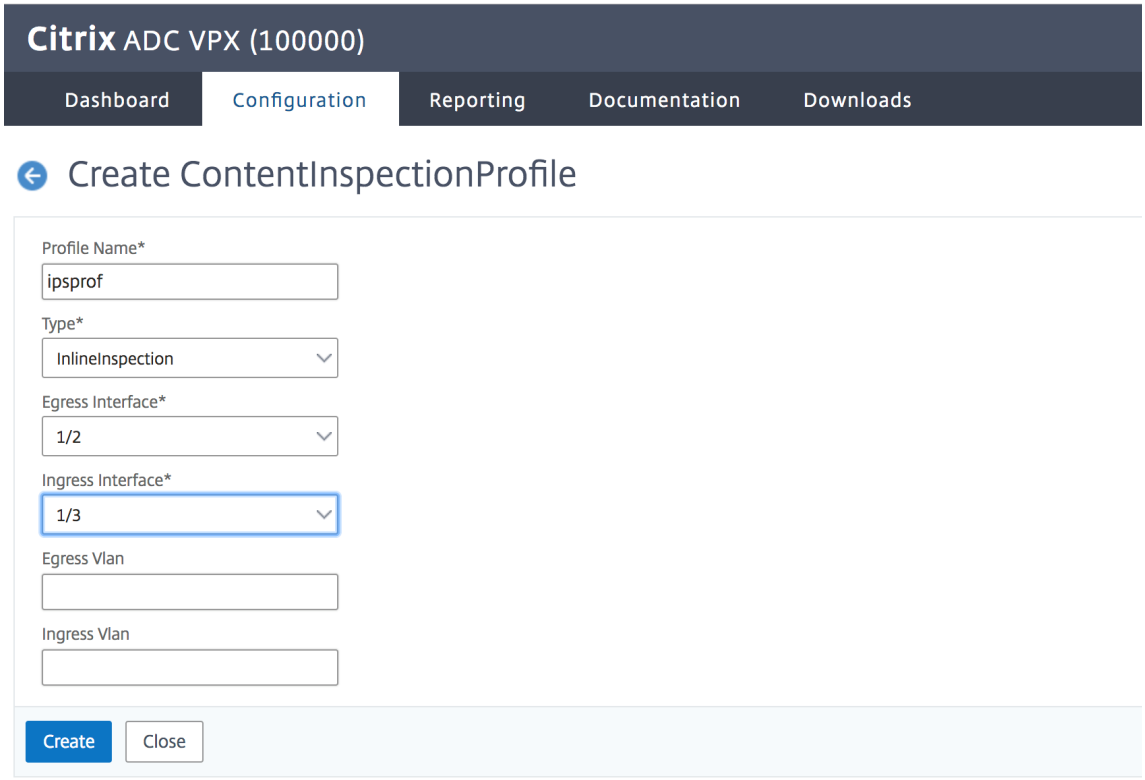


2. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Erweiterte Funktionen konfigurieren**.

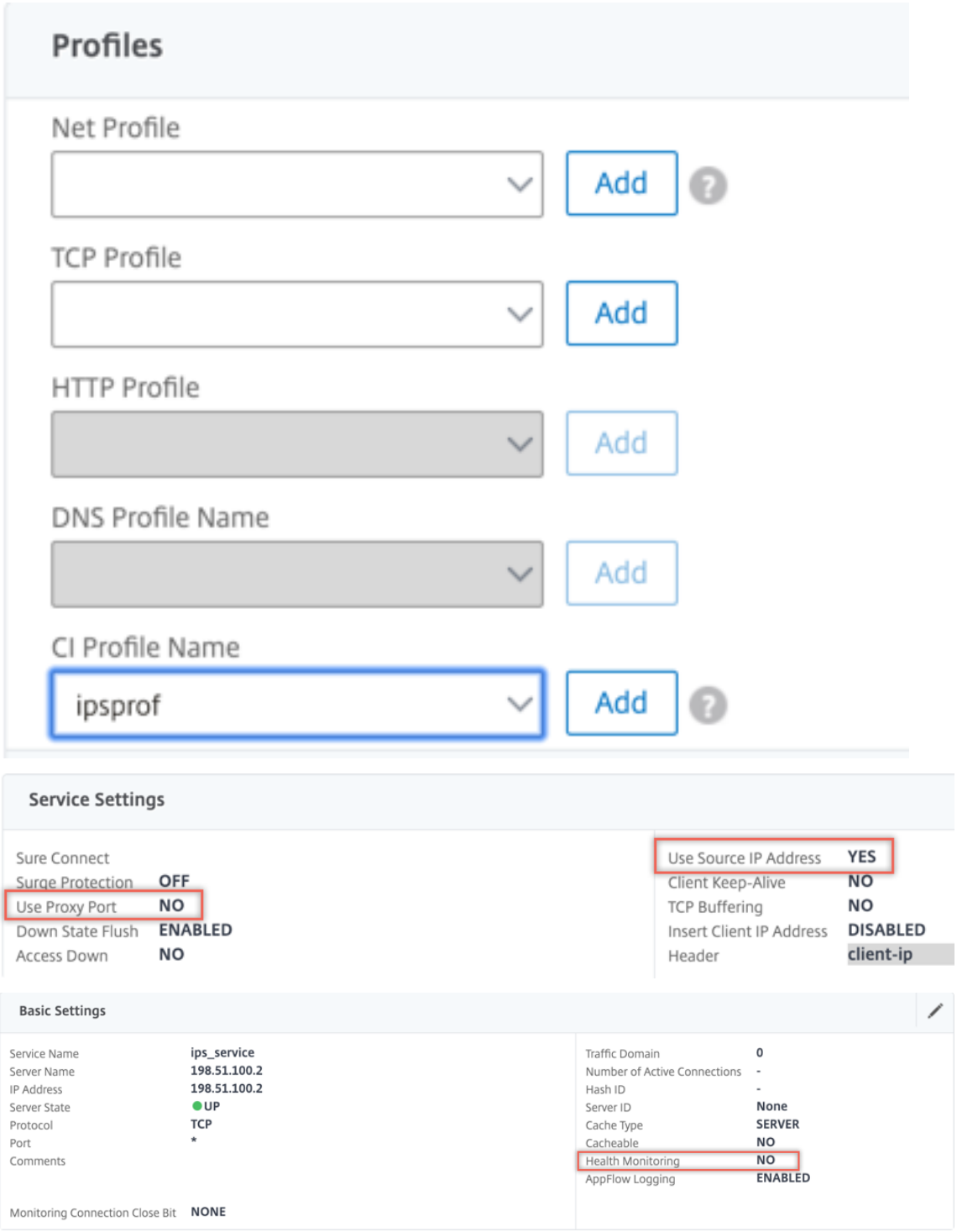




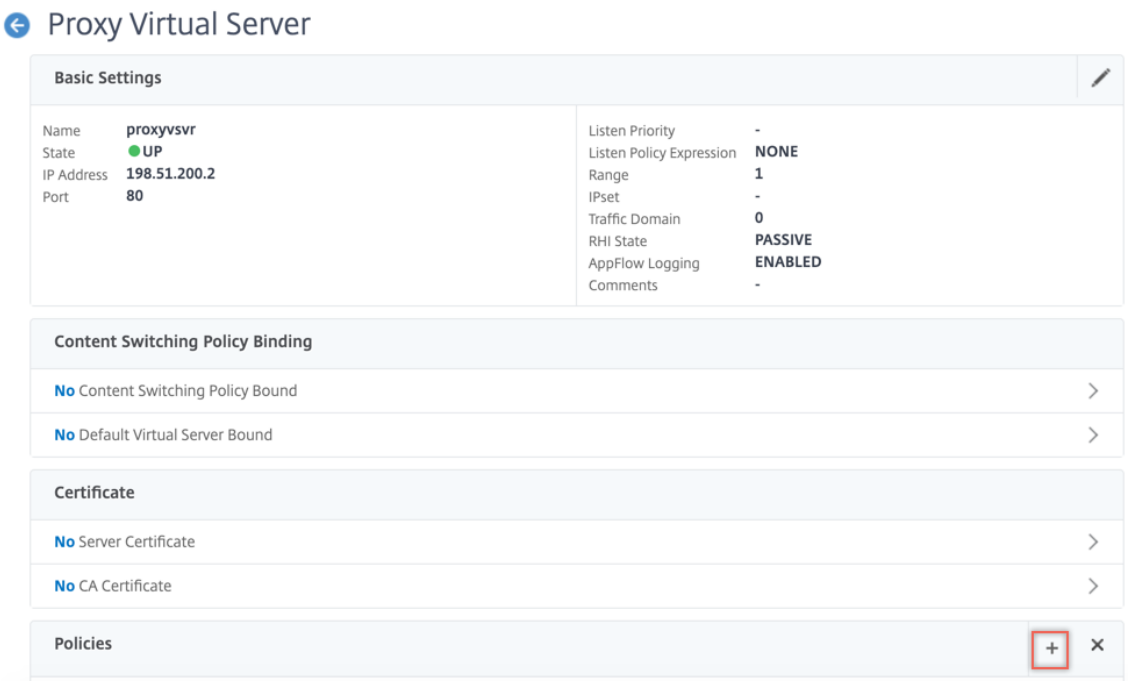
3. Navigieren Sie zu **Secure Web Gateway > Content Inspection > Content Inspection Profile**. Klicken Sie auf **Hinzufügen**.



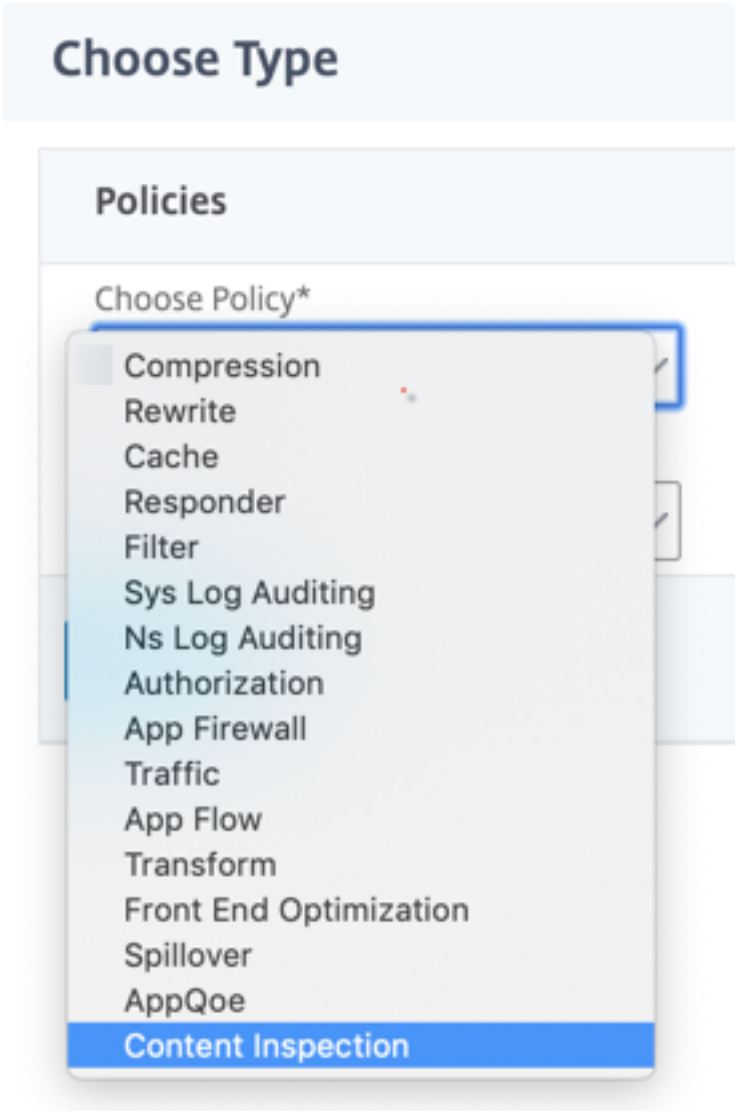
4. Navigieren Sie zu **Load Balancing > Services > Hinzufügen** und fügen Sie einen Service hinzu. Klicken Sie unter **Erweiterte Einstellungen** auf **Profile**. Wählen Sie in der Liste **CI-Profilname** das zuvor erstellte Content-Inspektionsprofil aus. Legen Sie unter **Diensteinstellungen** die Option **Quell-IP-Adresse verwenden** auf Ja und **Proxyport verwenden** auf Nein fest. Legen Sie in den **Grundeinstellungen** die **Integritätsüberwachung** auf Nein fest. Aktivieren Sie die Integritätsüberwachung nur, wenn Sie diesen Dienst an einen TCP-Monitor binden. Wenn Sie einen Monitor an einen Dienst binden, setzen Sie die Option TRANSPARENT im Monitor auf ON.



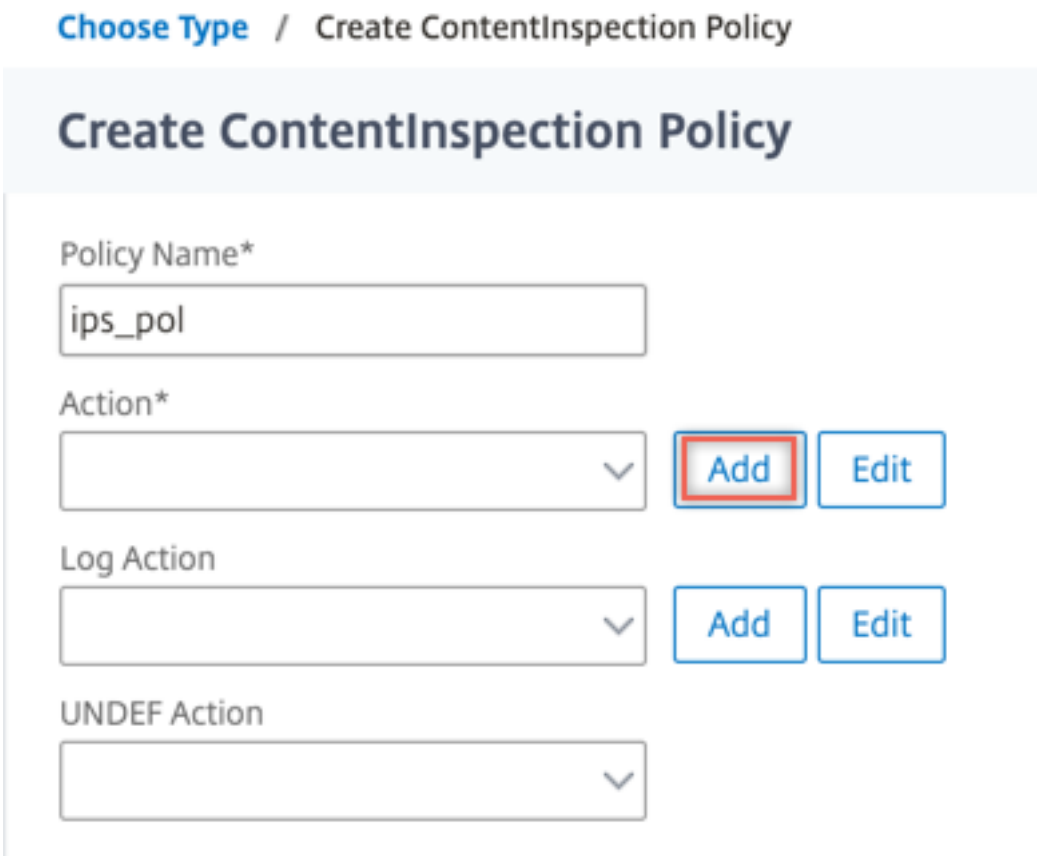
5. Navigieren Sie zu **Secure Web Gateway > Virtuelle Proxyserver > Hinzufügen**. Geben Sie einen Namen, eine IP-Adresse und einen Port an. Wählen Sie unter **Erweiterte Einstellungen** die Option **Richtlinien**aus. Klicken Sie auf das +-Zeichen.



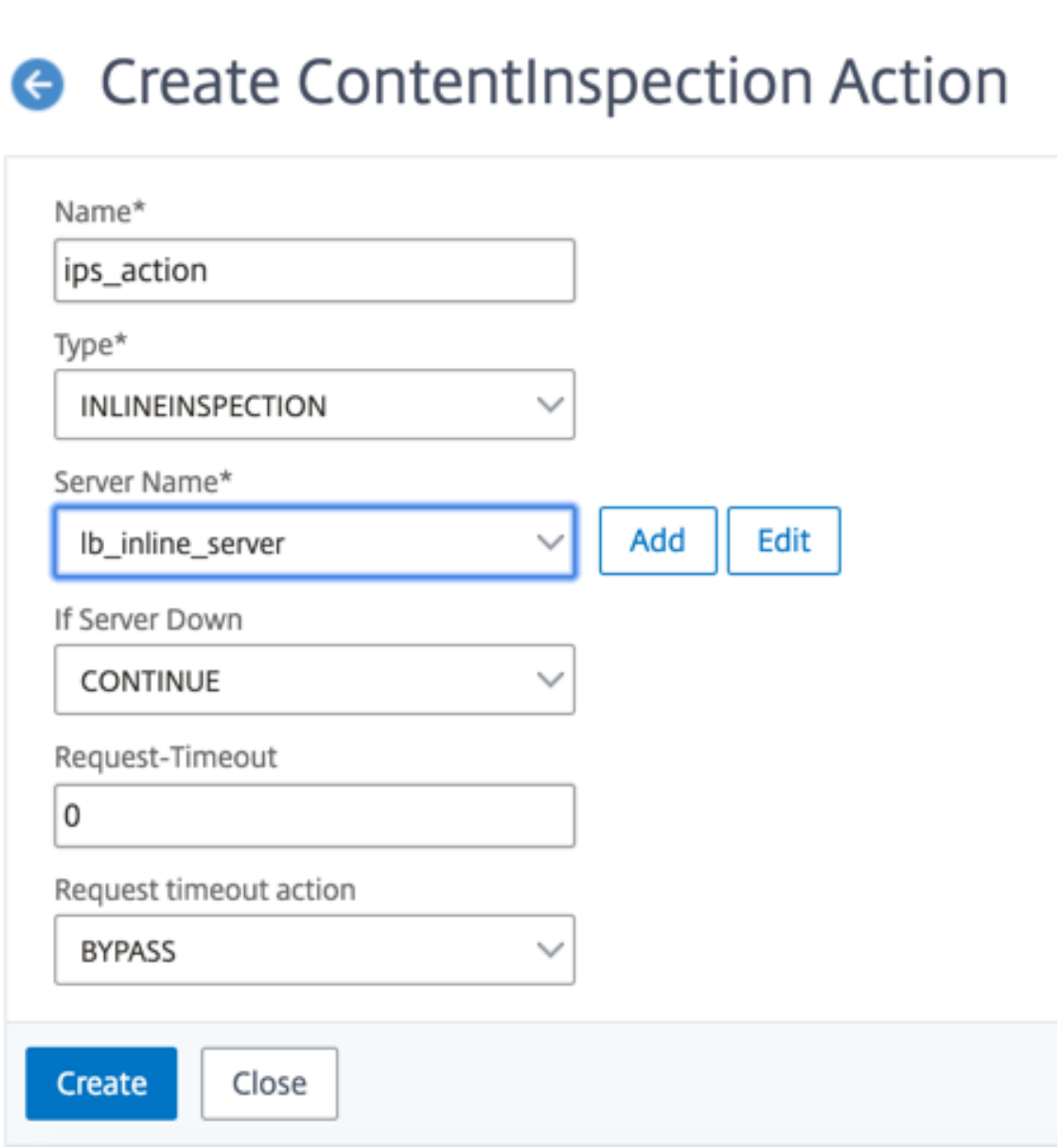
6. Wählen Sie unter **Richtlinie auswählen** die Option **Inhaltsüberprüfung** aus. Klicken Sie auf **Weiter**.



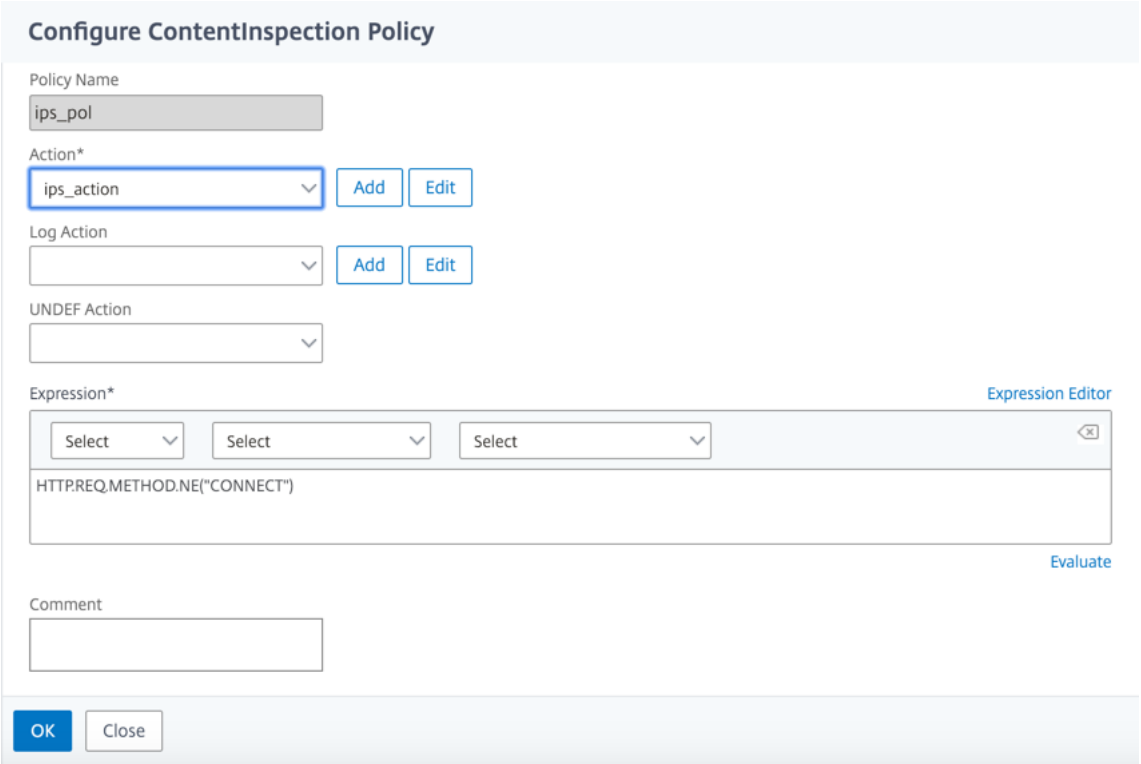
7. Klicken Sie auf **Hinzufügen**. Geben Sie einen Namen an. Klicken Sie unter **Aktion** auf **Hinzufügen**.



8. Geben Sie einen Namen an. Wählen Sie unter **Typ** die Option **INLINEINSPECTION** aus. Wählen Sie **unter Servername**den zuvor erstellten TCP-Dienst aus.



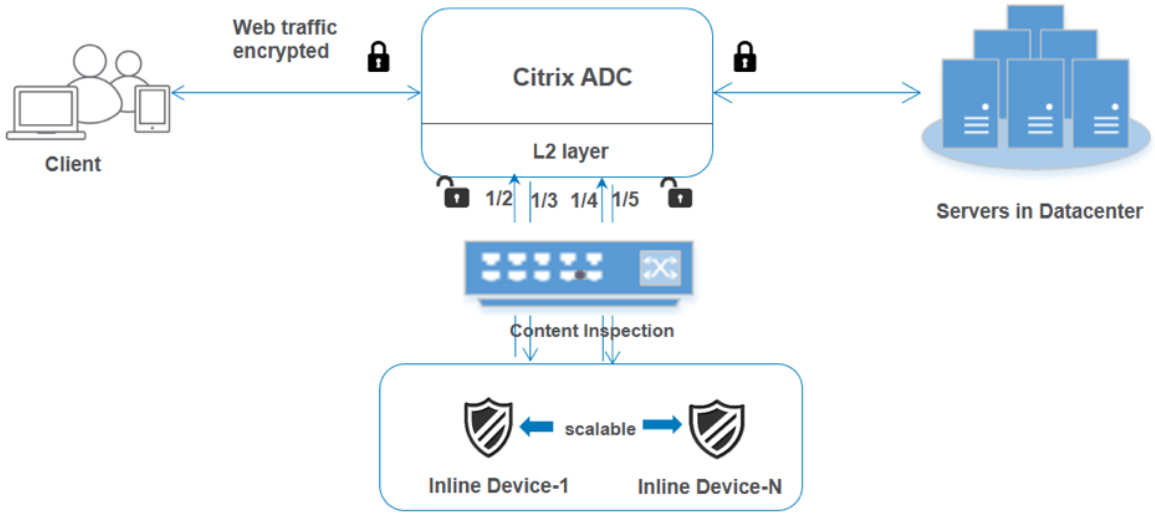
9. Klicken Sie auf **Erstellen**. Geben Sie die Regel an, und klicken Sie auf **Erstellen**.



10. Klicken Sie auf **Bind**.
11. Klicken Sie auf **Fertig**.

Szenario 2: Lastausgleich mehrerer Inline-Geräte mit dedizierten Schnittstellen

Wenn Sie zwei oder mehr Inline-Geräte verwenden, können Sie die Geräte mit verschiedenen Contentinspektionsdiensten mit dedizierten Schnittstellen ausgleichen. In diesem Fall gleicht die SSL-Forward-Proxy-Appliance die Teilmenge des Datenverkehrs aus, der über eine dedizierte Schnittstelle an jedes Gerät gesendet wird. Die Teilmenge wird basierend auf den konfigurierten Richtlinien festgelegt. Beispielsweise werden TXT- oder Bilddateien möglicherweise nicht zur Überprüfung an die Inline-Geräte gesendet.



Die Basiskonfiguration bleibt dieselbe wie in Szenario 1. Sie müssen jedoch für jedes Inline-Gerät ein Inhaltsinspektionsprofil erstellen und die Eingangs- und Ausgangsschnittstelle in jedem Profil angeben. Fügen Sie einen Dienst für jedes Inline-Gerät hinzu. Fügen Sie einen virtuellen Lastausgleichsserver hinzu, und geben Sie ihn in der Inhaltsüberprüfungsaktion an. Führen Sie die folgenden zusätzlichen Schritte aus:

1. Fügen Sie Content-Inspektionsprofile für jeden Service hinzu.
2. Fügen Sie einen Dienst für jedes Gerät hinzu.
3. Fügen Sie einen virtuellen Lastenausgleichsserver hinzu.
4. Geben Sie den virtuellen Lastausgleichsserver in der Inhaltsüberprüfungsaktion an.

Konfiguration mit der CLI

Geben Sie die folgenden Befehle an der Eingabeaufforderung ein. Beispiele werden nach jedem Befehl angegeben.

1. MBF aktivieren.

```
enable ns mode mbf
```

1. Aktivieren Sie das Feature.

```
enable ns feature contentInspection
```

1. Profil 1 für Service 1 hinzufügen.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:


```
add contentInspection profile ipsprof1 -type InlineInspection -ingressInterface
 ”1/2”-egressInterface ”1/3”
```

1. Profil 2 für Service 2 hinzufügen.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile ipsprof2 -type InlineInspection -ingressInterface
 ”1/4”-egressInterface ”1/5”
```

1. Service 1 hinzufügen. Geben Sie eine Dummy-IP-Adresse an, die keinem der Geräte gehört, einschließlich der Inline-Geräte. Setzen Sie `use source IP address` (USIP) auf YES. Setzen Sie `useproxyport` auf NO. Schalten Sie die Zustandsüberwachung mit dem TCP-Monitor mit der Option TRANSPARENT ein.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Beispiel:

```
add service ips_service1 192.168.10.2 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof1
```

1. Service 2 hinzufügen. Geben Sie eine Dummy-IP-Adresse an, die keinem der Geräte gehört, einschließlich der Inline-Geräte. Setzen Sie `use source IP address` (USIP) auf YES. Setzen Sie `useproxyport` auf NO. Schalten Sie die Zustandsüberwachung mit der Option TRANSPARENT ein.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Beispiel:

```
add service ips_service2 192.168.10.3 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof2
```

1. Fügen Sie einen virtuellen Lastenausgleichsserver hinzu.

```
add lb vserver <LB_VSERVER_NAME> TCP <IP> <port>
```

Beispiel:

```
add lb vserver lb_inline_vserver TCP 192.0.2.100 *
```

1. Binden Sie die Dienste an den virtuellen Lastenausgleichsserver.


```
bind lb vserver <LB_VSERVER_NAME> <service_name>
bind lb vserver <LB_VSERVER_NAME> <service_name>
```

Beispiel:

```
bind lb vserver lb_inline_vserver ips_service1
bind lb vserver lb_inline_vserver ips_service2
```

1. Geben Sie den virtuellen Lastausgleichsserver in der Inhaltsüberprüfungsaktion an.

```
add contentInspection action <name> -type INLINEINSPECTION -serverName <
string>
```

Beispiel:

```
add contentInspection action ips_action -type INLINEINSPECTION -serverName
lb_inline_vserver
```

1. Fügen Sie eine Richtlinie zur Inhaltsüberprüfung hinzu. Geben Sie die Inhaltsinspektionsaktion in der Richtlinie an.

```
add contentInspection policy <name> -rule <expression> -action <string>
```

Beispiel:

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE(\"CONNECT\")
"-action ips_action
```

1. Fügen Sie einen virtuellen Proxyserver hinzu.

```
add cs vserver <name> PROXY <IPAddress> <port> -l2Conn ON
```

Beispiel:

```
add cs vserver transparentcs PROXY * * -l2Conn ON
```

1. Binden Sie die Richtlinie zur Inhaltsüberprüfung an den virtuellen Server.

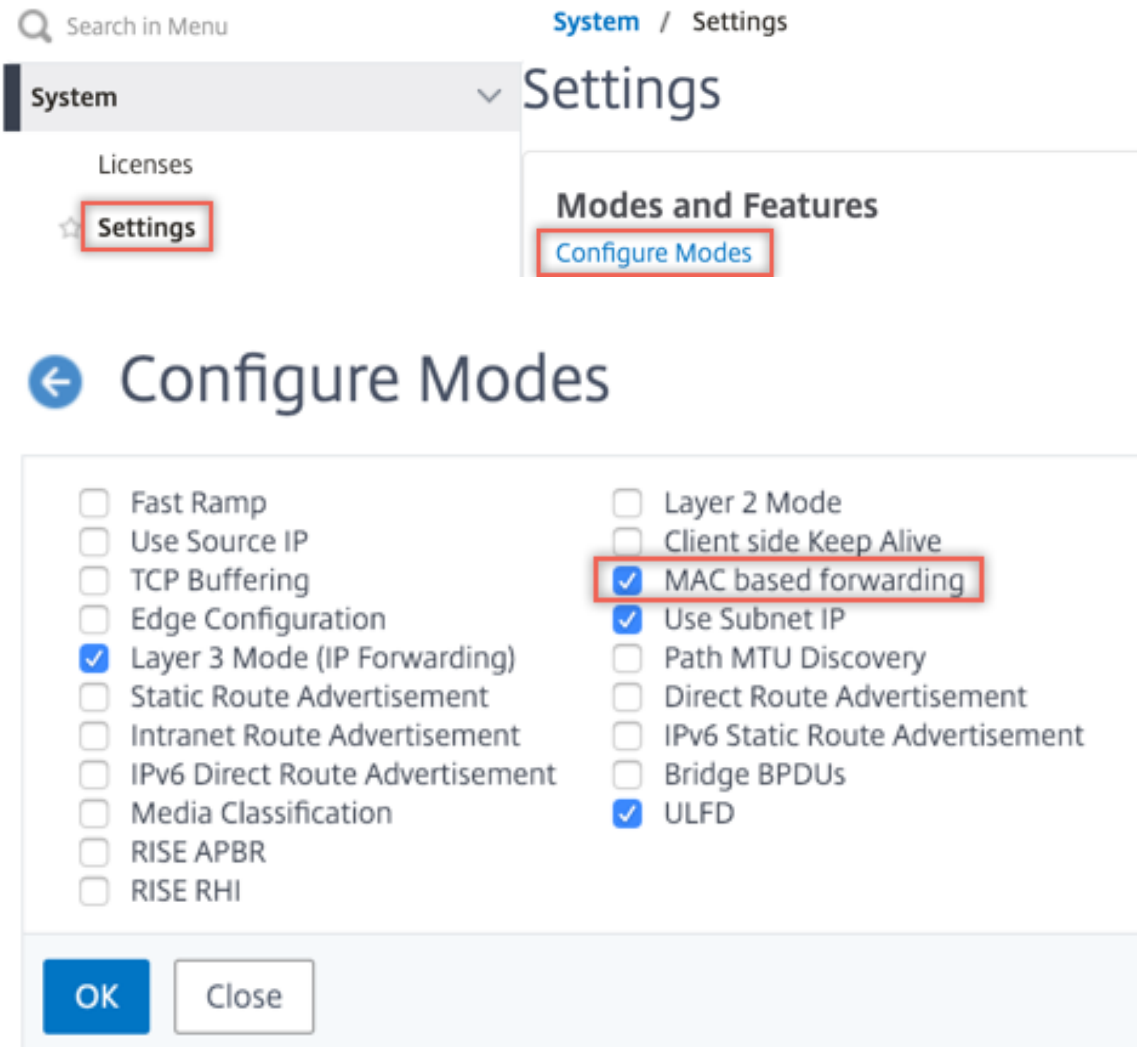
```
bind cs vserver <name> -policyName <string> -priority <positive_integer> -
gotoPriorityExpression <expression> -type REQUEST
```

Beispiel:

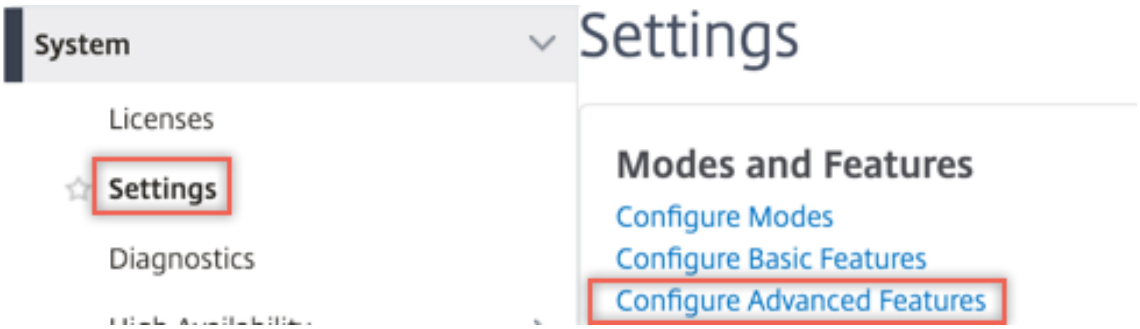
```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -gotoPriorityExpression
 END -type REQUEST
```

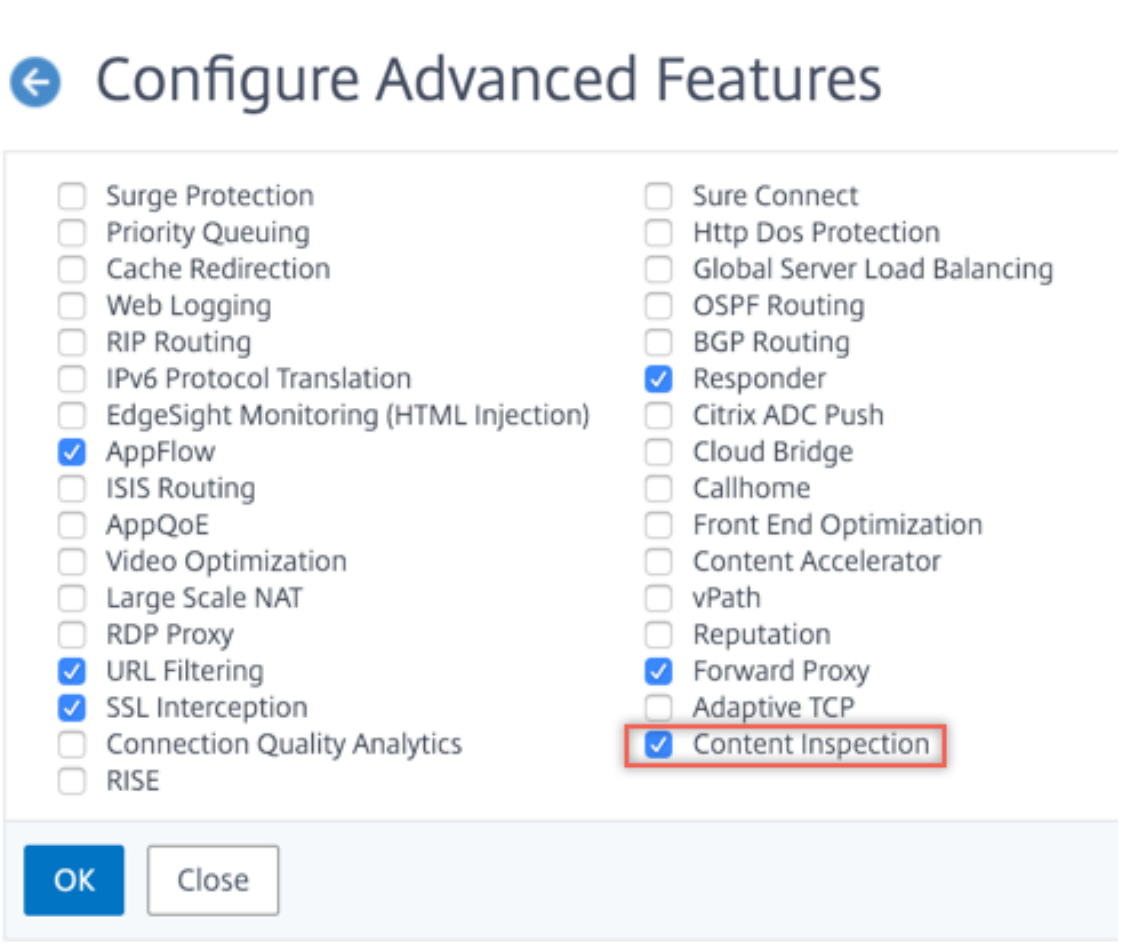
Konfiguration über die GUI

1. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Modi konfigurieren**.

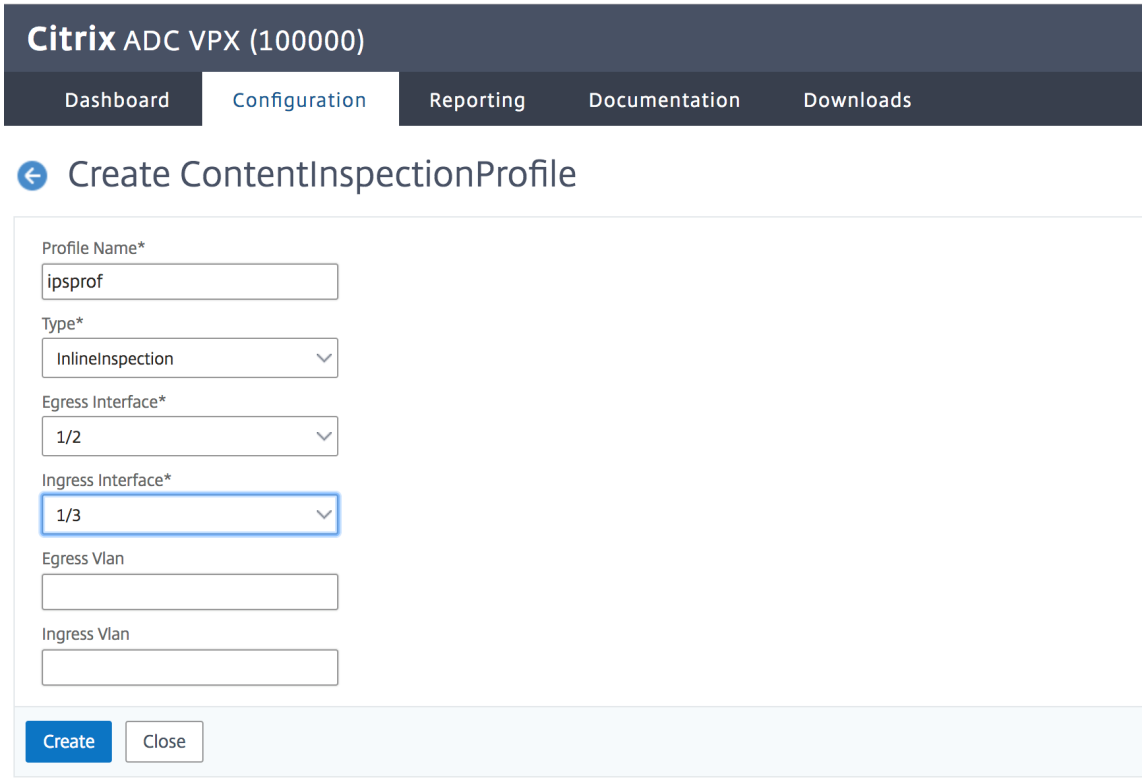


2. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Erweiterte Funktionen konfigurieren**.

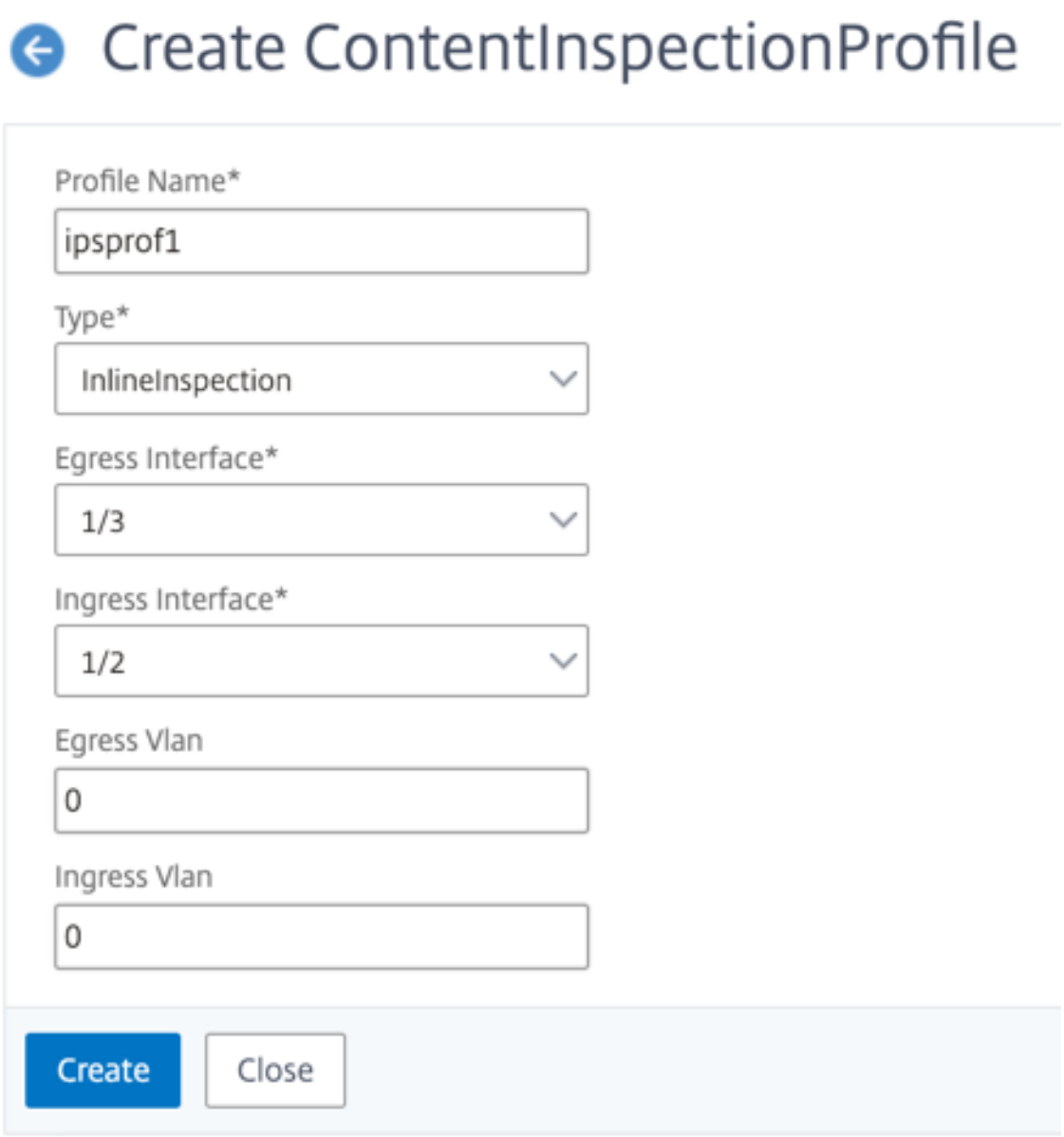




3. Navigieren Sie zu **Secure Web Gateway > Content Inspection > Content Inspection Profile**. Klicken Sie auf **Hinzufügen**.

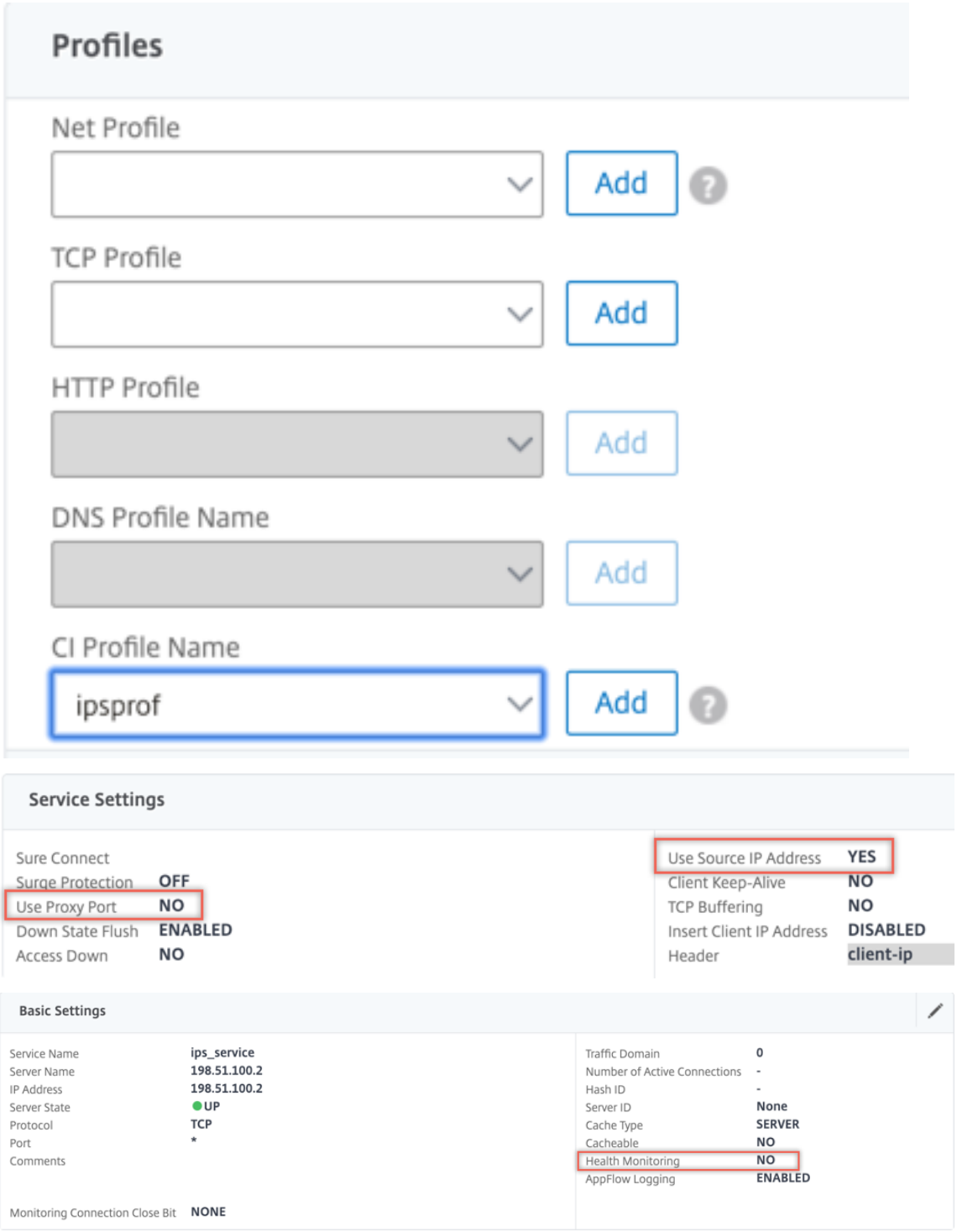


Geben Sie die Eingangs- und Ausgangsschnittstellen an.



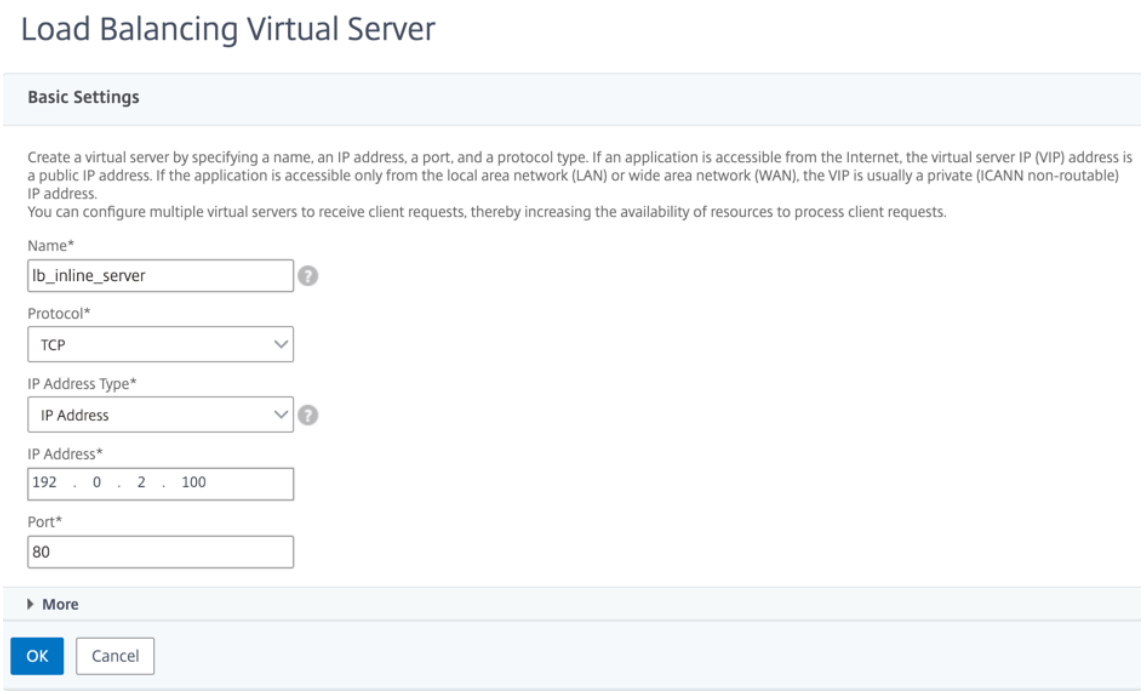
Erstellen Sie zwei Profile. Geben Sie im zweiten Profil eine andere Eingangs- und Ausgangsschnittstelle an.

4. Navigieren Sie zu **Load Balancing > Services > Hinzufügen** und fügen Sie einen Service hinzu. Klicken Sie unter **Erweiterte Einstellungen** auf **Profile**. Wählen Sie in der Liste **CI-Profilname** das zuvor erstellte Content-Inspektionsprofil aus. Legen Sie unter **Diensteinstellungen** die Option **Quell-IP-Adresse verwenden** auf Ja und **Proxyport verwenden** auf Nein fest. Legen Sie in den **Grundeinstellungen** die **Integritätsüberwachung** auf Nein fest. Aktivieren Sie die Integritätsüberwachung nur, wenn Sie diesen Dienst an einen TCP-Monitor binden. Wenn Sie einen Monitor an einen Dienst binden, setzen Sie die Option TRANSPARENT im Monitor auf ON.



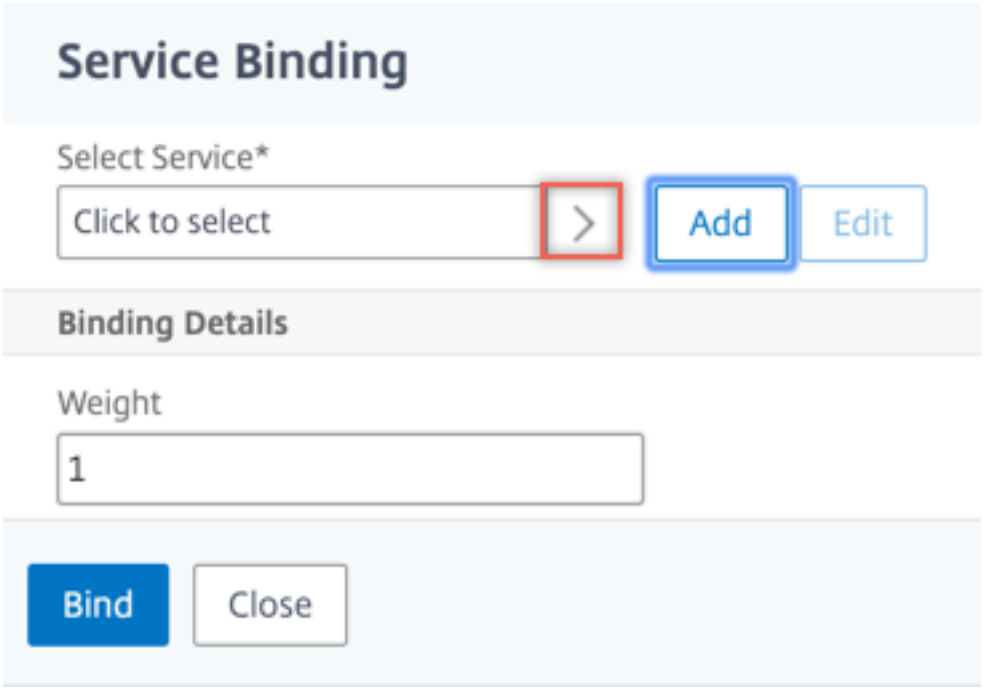
Erstellen Sie zwei Dienste. Geben Sie Dummy-IP-Adressen an, die keinem der Geräte gehören, einschließlich der Inline-Geräte.

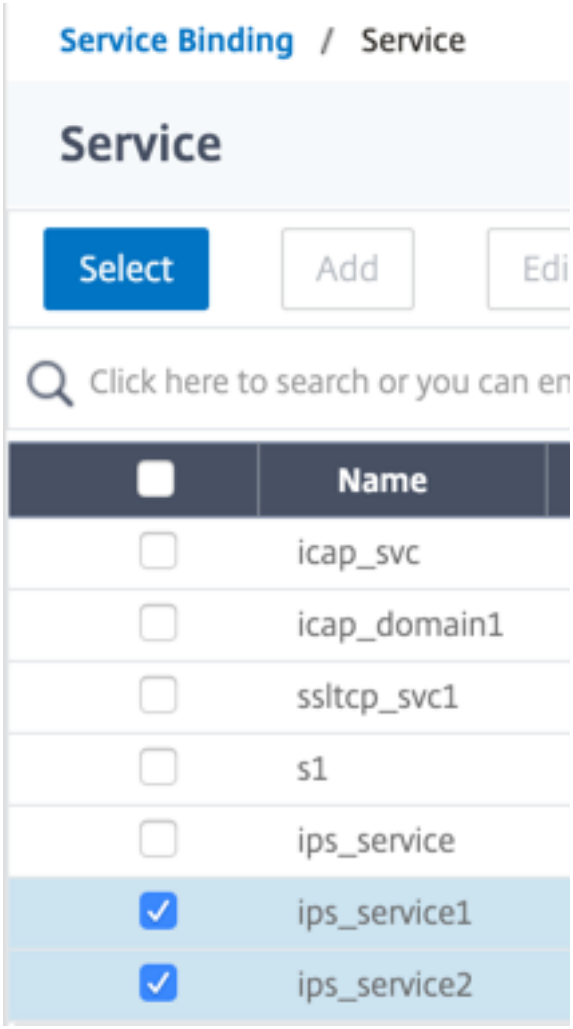
5. Navigieren Sie zu **Lastenausgleich > Virtuelle Server > Hinzufügen**. Erstellen Sie einen virtuellen TCP-Load Balancing Server.

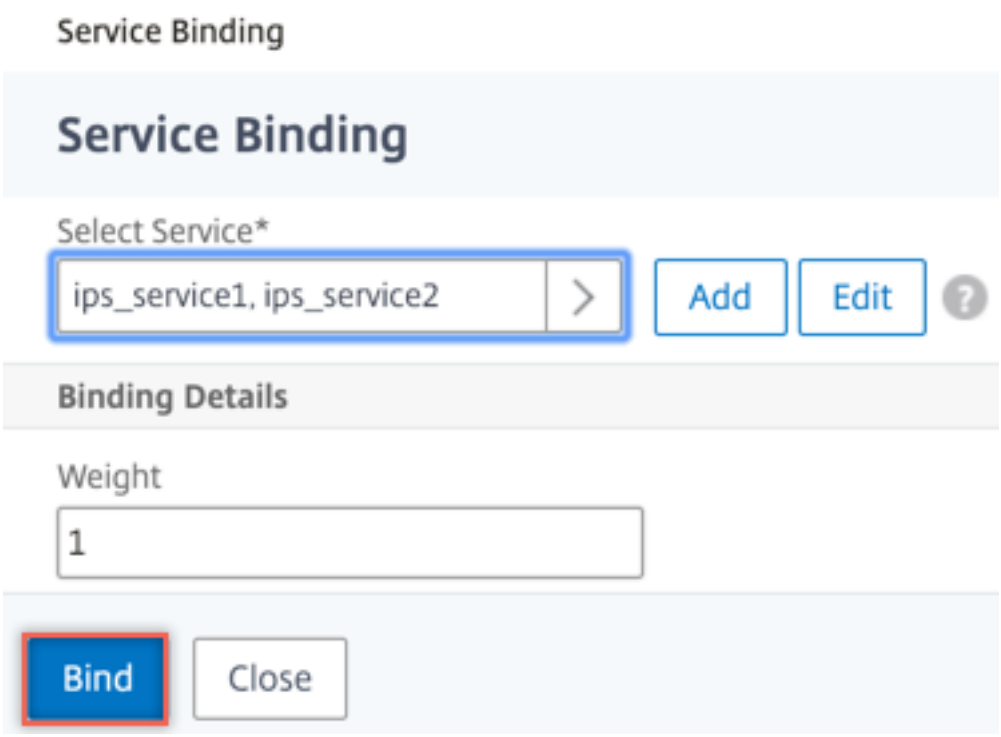


Klicken Sie auf **OK**.

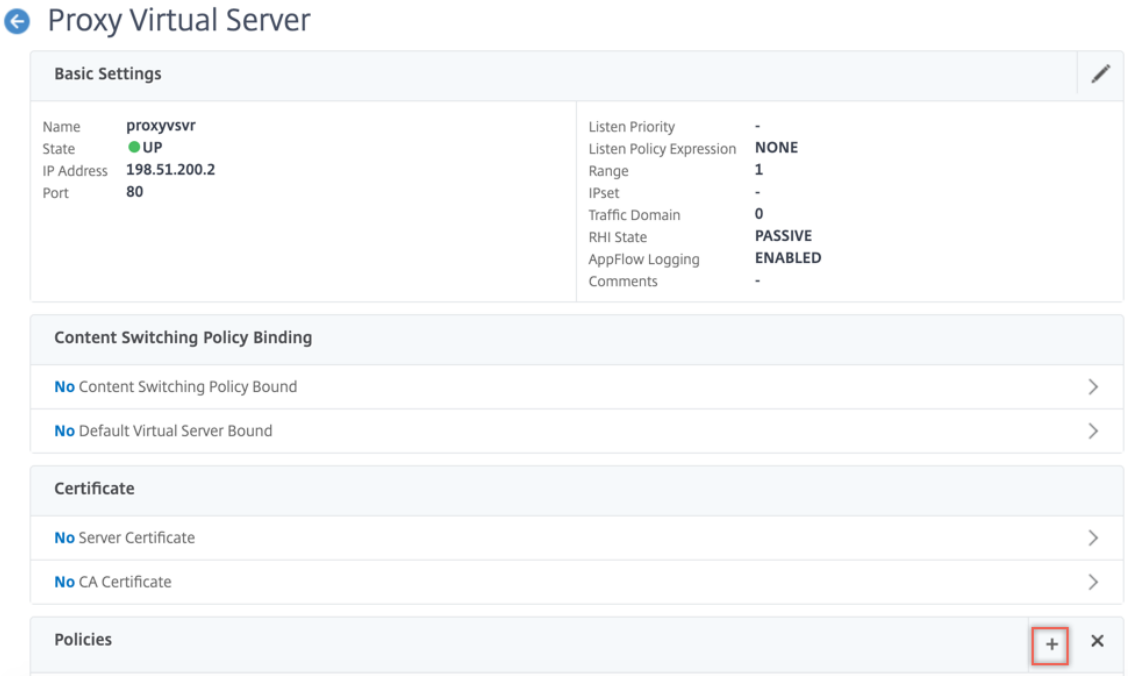
6. Klicken Sie in den Abschnitt **Load Balancing Virtual Server Service Binding**. Klicken Sie unter **Dienstbindung** auf den Pfeil unter **Dienst auswählen**. Wählen Sie die beiden zuvor erstellten Dienste aus, und klicken Sie auf **Auswählen**. Klicken Sie auf **Bind**.



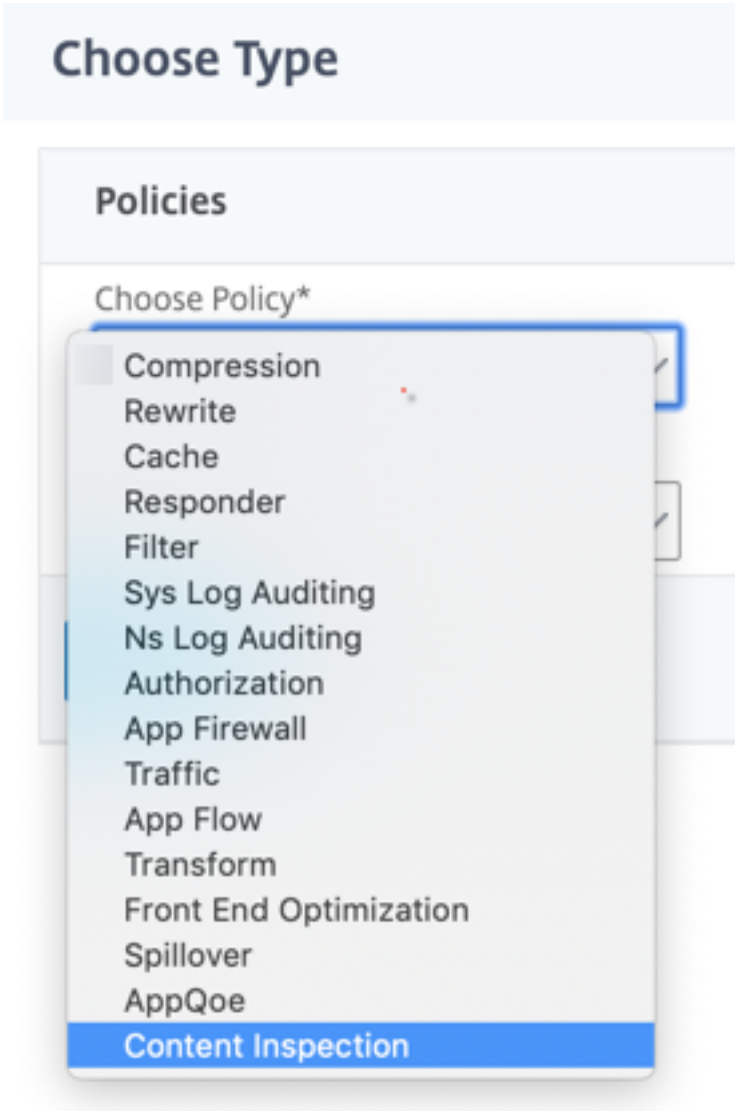




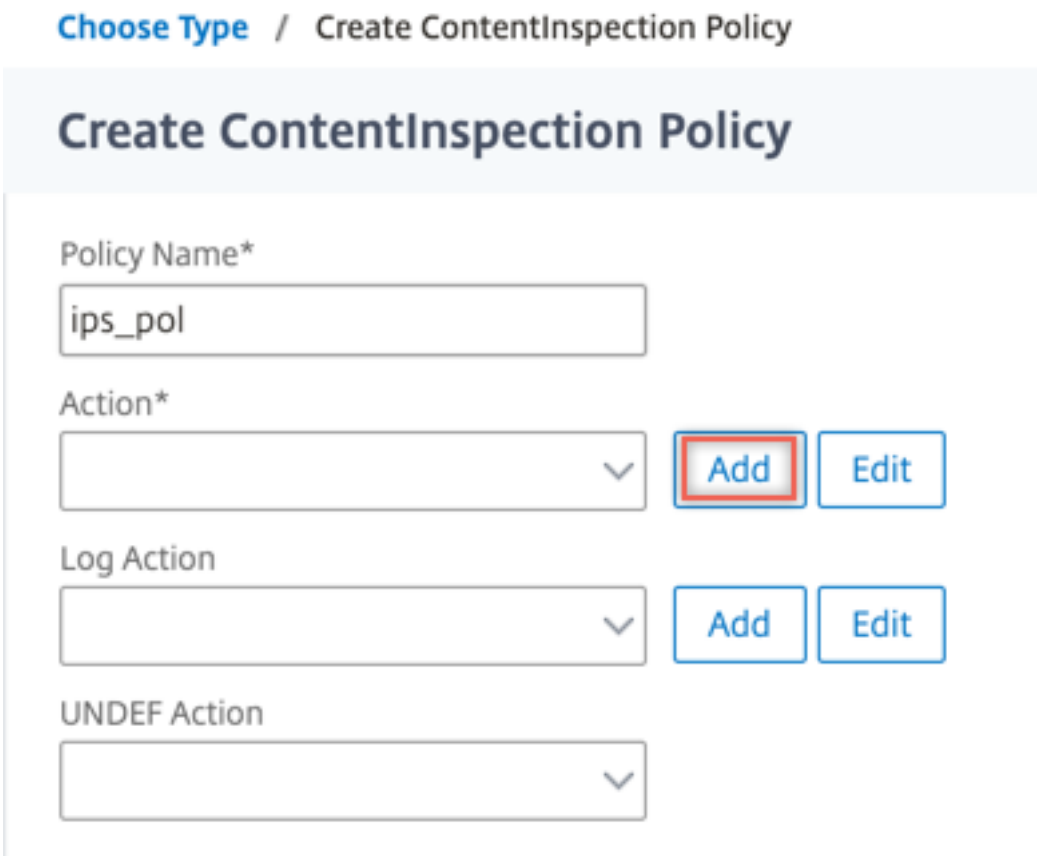
7. Navigieren Sie zu **Secure Web Gateway > Virtuelle Proxyserver > Hinzufügen**. Geben Sie einen Namen, eine IP-Adresse und einen Port an. Wählen Sie unter **Erweiterte Einstellungen** die Option **Richtlinien**aus. Klicken Sie auf das +-Zeichen.



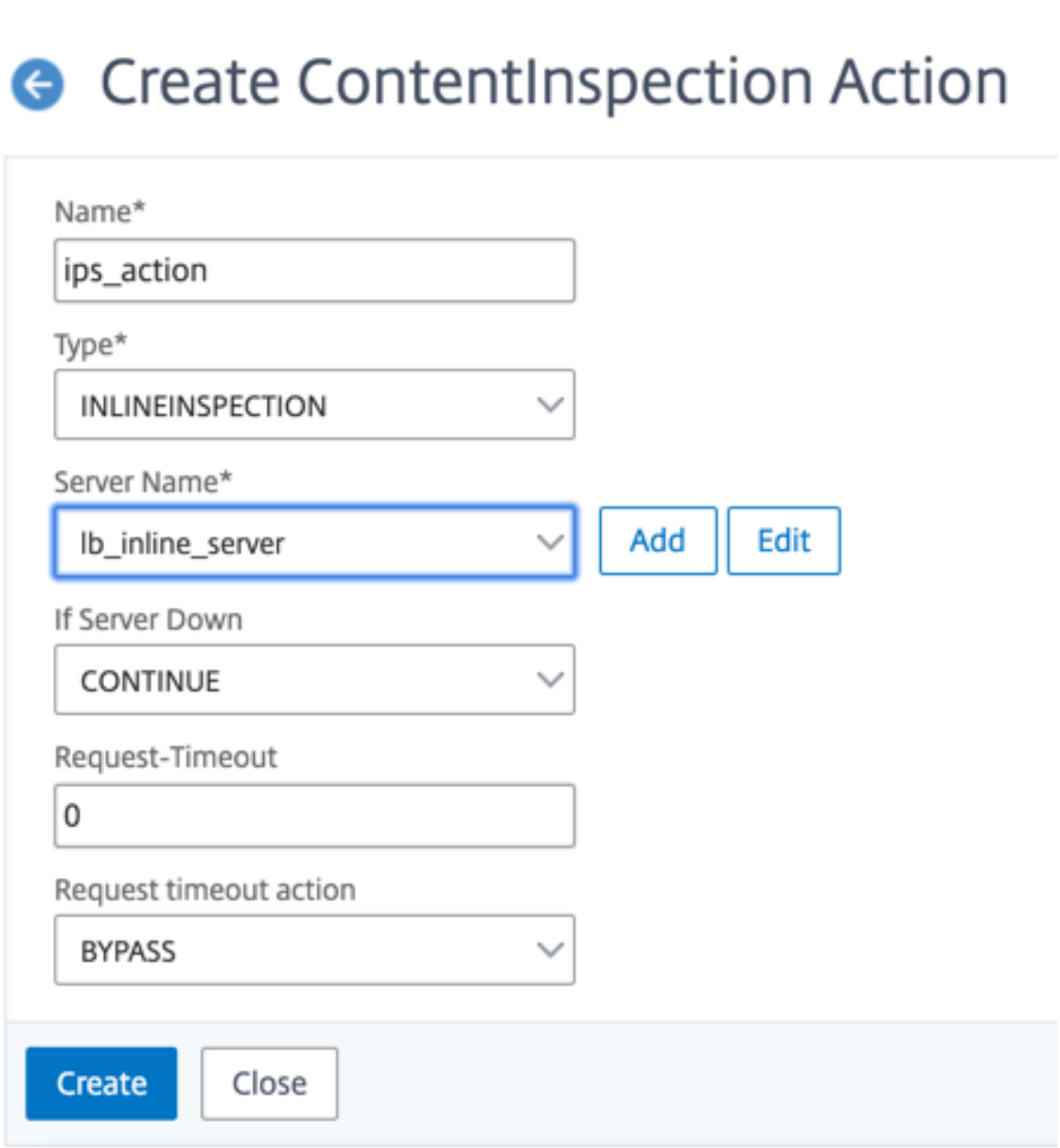
8. Wählen Sie unter **Richtlinie auswählen** die Option **Inhaltsüberprüfung** aus. Klicken Sie auf **Weiter**.



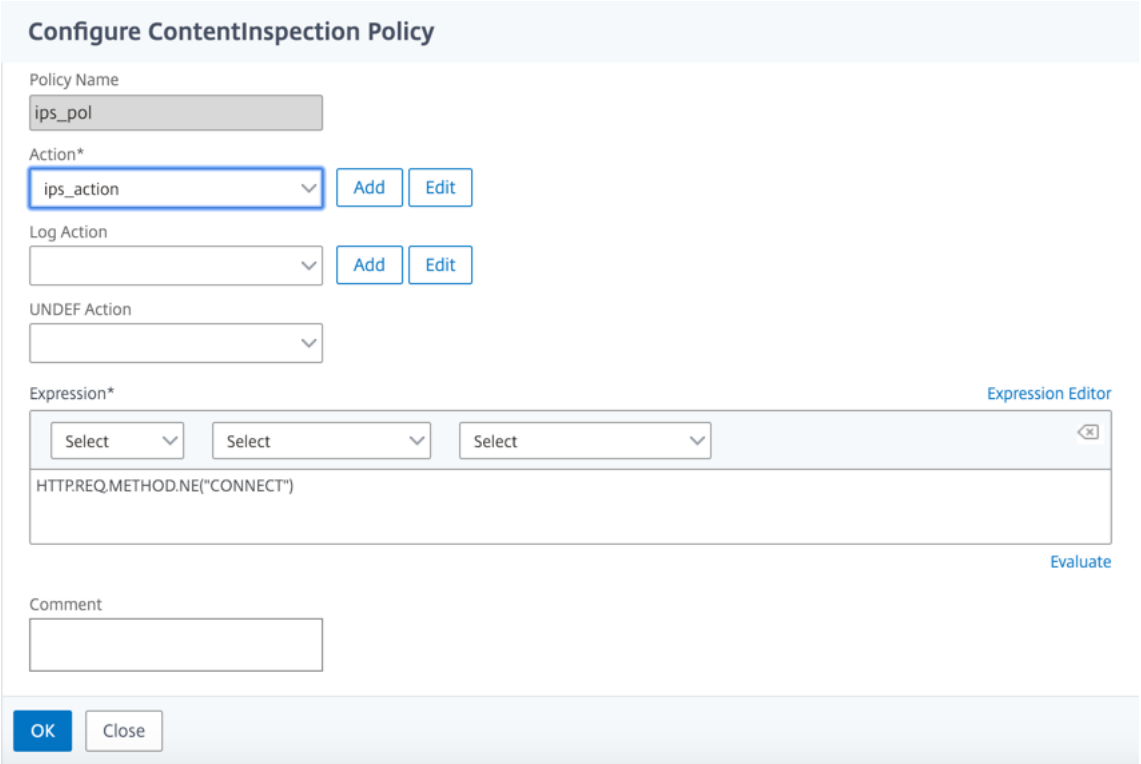
9. Klicken Sie auf **Hinzufügen**. Geben Sie einen Namen an. Klicken Sie unter **Aktion** auf **Hinzufügen**.



10. Geben Sie einen Namen an. Wählen Sie unter **Typ** die Option **INLINEINSPECTION** aus. Wählen Sie unter **Servername** den zuvor erstellten virtuellen Lastenausgleichsserver aus.



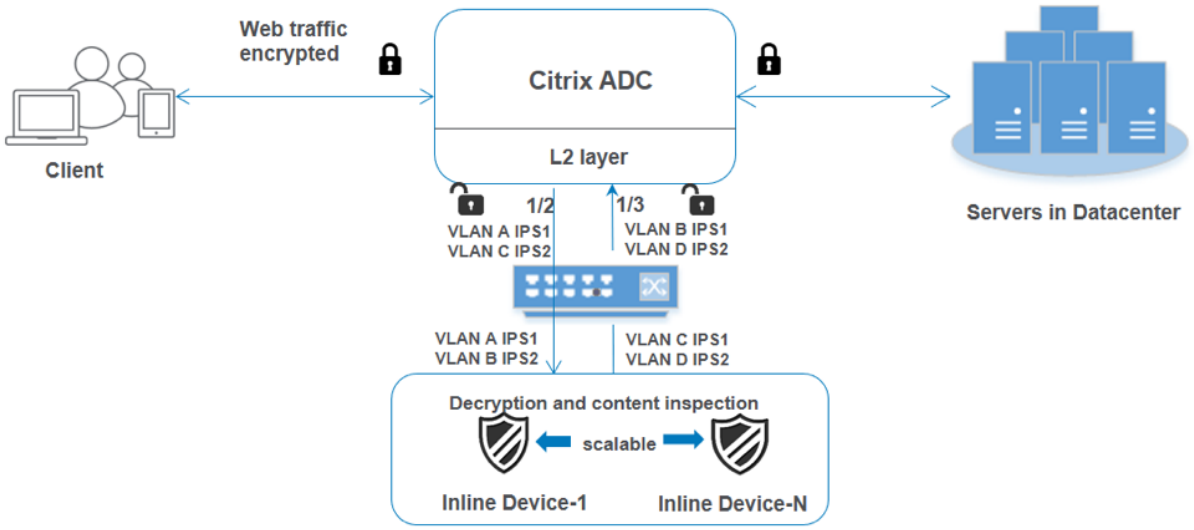
11. Klicken Sie auf **Erstellen**. Geben Sie die Regel an, und klicken Sie auf **Erstellen**.



12. Klicken Sie auf **Bind**.
13. Klicken Sie auf **Fertig**.

Szenario 3: Lastausgleich mehrerer Inline-Geräte mit gemeinsamen Schnittstellen

Wenn Sie zwei oder mehr Inline-Geräte verwenden, können Sie die Geräte mit verschiedenen Contentinspektionsdiensten mit gemeinsam genutzten Schnittstellen ausgleichen. In diesem Fall gleicht die SSL-Forward-Proxy-Appliance die Teilmenge des Datenverkehrs aus, der über eine gemeinsame Schnittstelle an jedes Gerät gesendet wird. Die Teilmenge wird basierend auf den konfigurierten Richtlinien festgelegt. Beispielsweise werden TXT- oder Bilddateien möglicherweise nicht zur Überprüfung an die Inline-Geräte gesendet.



Die Basiskonfiguration bleibt dieselbe wie in Szenario 2. Binden Sie für dieses Szenario die Schnittstellen an verschiedene VLANs, um den Datenverkehr für jedes Inline-Gerät zu trennen. Geben Sie die VLANs in den Content-Inspektionsprofilen an. Führen Sie die folgenden zusätzlichen Schritte aus:

1. Binden Sie die freigegebenen Schnittstellen an verschiedene VLANs.
2. Geben Sie die Ein- und Ausgangs-VLANs in den Content-Inspektionsprofilen an.

Konfiguration über die CLI

Geben Sie die folgenden Befehle an der Eingabeaufforderung ein. Beispiele werden nach jedem Befehl angegeben.

1. MBF aktivieren.

```
enable ns mode mbf
```

1. Aktivieren Sie das Feature.

```
enable ns feature contentInspection
```

1. Binden Sie die freigegebenen Schnittstellen an verschiedene VLANs.

```
bind vlan <id> -ifnum <interface> -tagged
```

Beispiel:

```
1 bind vlan 100  - ifnum 1/2 tagged
2 bind vlan 200  - ifnum 1/3 tagged
```



```
3 bind vlan 300 -ifnum 1/2 tagged
4 bind vlan 400 -ifnum 1/3 tagged
5 <!--NeedCopy-->
```

1. Profil 1 für Service 1 hinzufügen. Geben Sie die Ein- und Aus-VLANs im Profil an.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile ipsprof1 -type InlineInspection -egressInterface
 "1/3" -ingressinterface "1/2" -egressVlan 100 -ingressVlan 300
```

1. Profil 2 für Service 2 hinzufügen. Geben Sie die Ein- und Aus-VLANs im Profil an.

```
add contentInspection profile <name> -type InlineInspection -egressInterface
 <interface_name> -ingressInterface <interface_name>[-egressVlan <positive_integer
>] [-ingressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile ipsprof2 -type InlineInspection -egressInterface
 "1/3" -ingressinterface "1/2" -egressVlan 200 -ingressVlan 400
```

1. Service 1 hinzufügen.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Beispiel:

```
add service ips_service1 192.168.10.2 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof1
```

1. Service 2 hinzufügen.

```
add service <service_name> <IP> TCP * - contentinspectionProfileName <Name>
 -healthMonitor NO -usip YES -useproxyport NO
```

Beispiel:

```
add service ips_service2 192.168.10.3 TCP * -healthMonitor NO -usip YES -
useproxyport NO -contentInspectionProfileName ipsprof2
```

1. Fügen Sie einen virtuellen Lastenausgleichsserver hinzu.

```
add lb vserver <LB_VSERVER_NAME> TCP <IP> <port>
```

Beispiel:

```
add lb vserver lb_inline_vserver TCP 192.0.2.100 *
```


1. Binden Sie die Dienste an den virtuellen Lastenausgleichsserver.

```
bind lb vserver <LB_VSERVER_NAME> <service_name>
bind lb vserver <LB_VSERVER_NAME> <service_name>
```

Beispiel:

```
bind lb vserver lb_inline_vserver ips_service1
bind lb vserver lb_inline_vserver ips_service2
```

1. Geben Sie den virtuellen Lastausgleichsserver in der Inhaltsüberprüfungsaktion an.

```
add contentInspection action <name> -type INLINEINSPECTION -serverName <
string>
```

Beispiel:

```
add contentInspection action ips_action -type INLINEINSPECTION -serverName
lb_inline_vserver
```

1. Fügen Sie eine Richtlinie zur Inhaltsüberprüfung hinzu. Geben Sie die Inhaltsinspektionsaktion in der Richtlinie an.

```
add contentInspection policy <name> -rule <expression> -action <string>
```

Beispiel:

```
add contentInspection policy ips_pol -rule "HTTP.REQ.METHOD.NE(\"CONNECT\")
"-action ips_action
```

1. Fügen Sie einen virtuellen Proxyserver hinzu.

```
add cs vserver <name> PROXY <IPAddress> <port> -l2Conn ON
```

Beispiel:

```
add cs vserver transparentcs PROXY * * -l2Conn ON
```

1. Binden Sie die Richtlinie zur Inhaltsüberprüfung an den virtuellen Server.

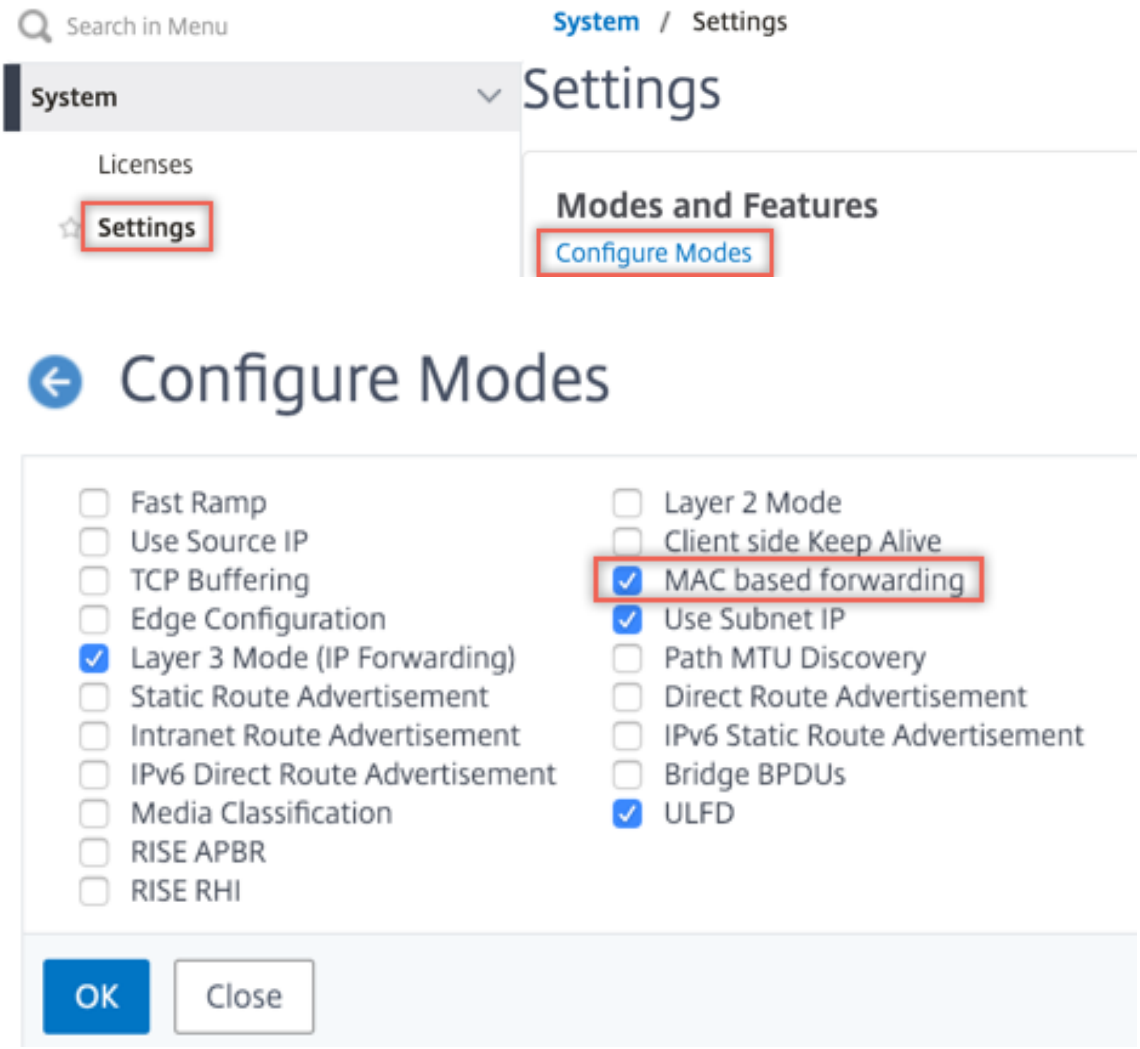
```
bind cs vserver <name> -policyName <string> -priority <positive_integer> -
gotoPriorityExpression <expression> -type REQUEST
```

Beispiel:

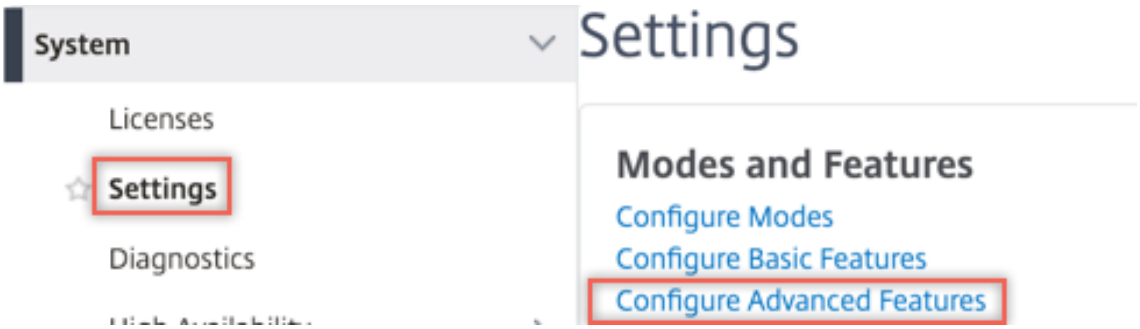
```
bind cs vserver explicitcs -policyName ips_pol -priority 1 -gotoPriorityExpression
 END -type REQUEST
```

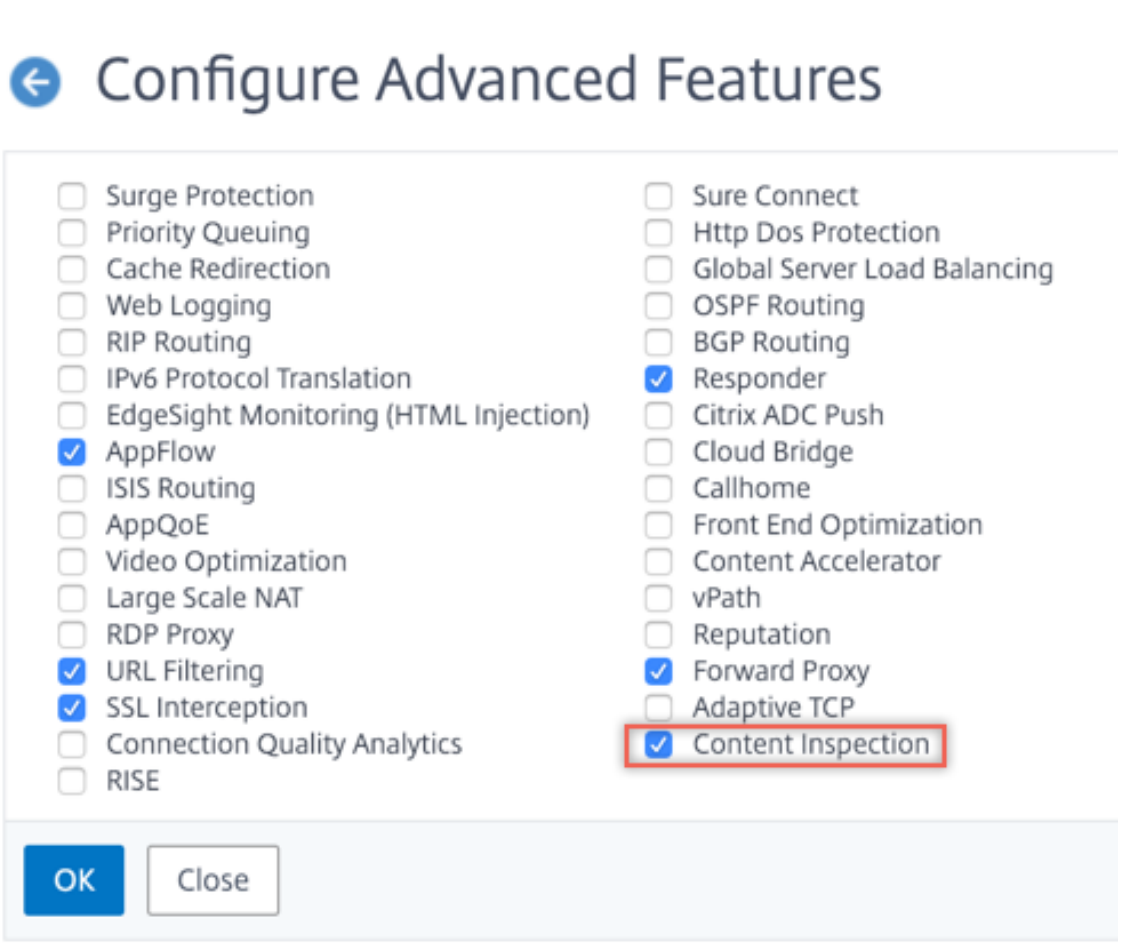
Konfiguration über die GUI

1. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Modi konfigurieren**.

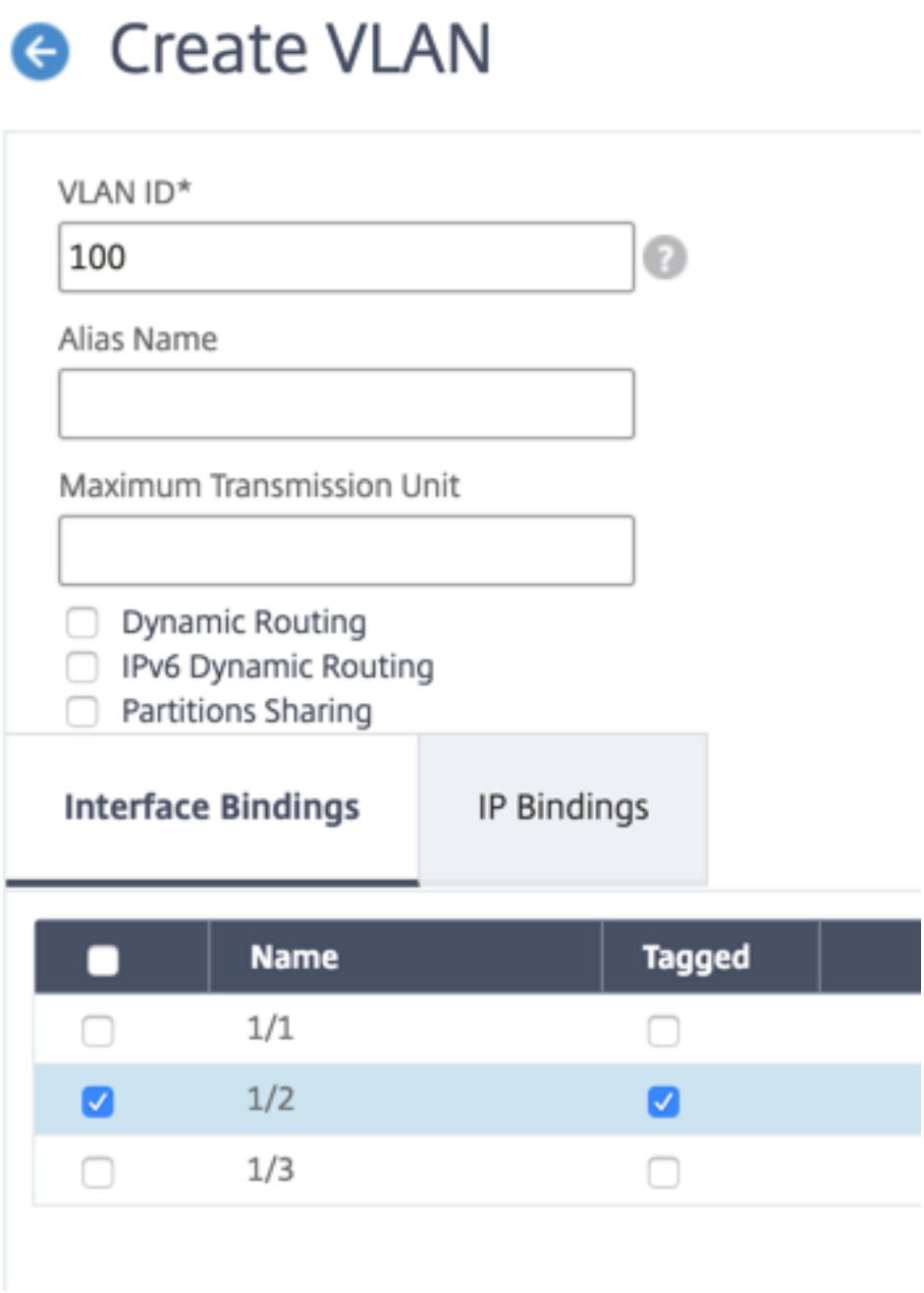


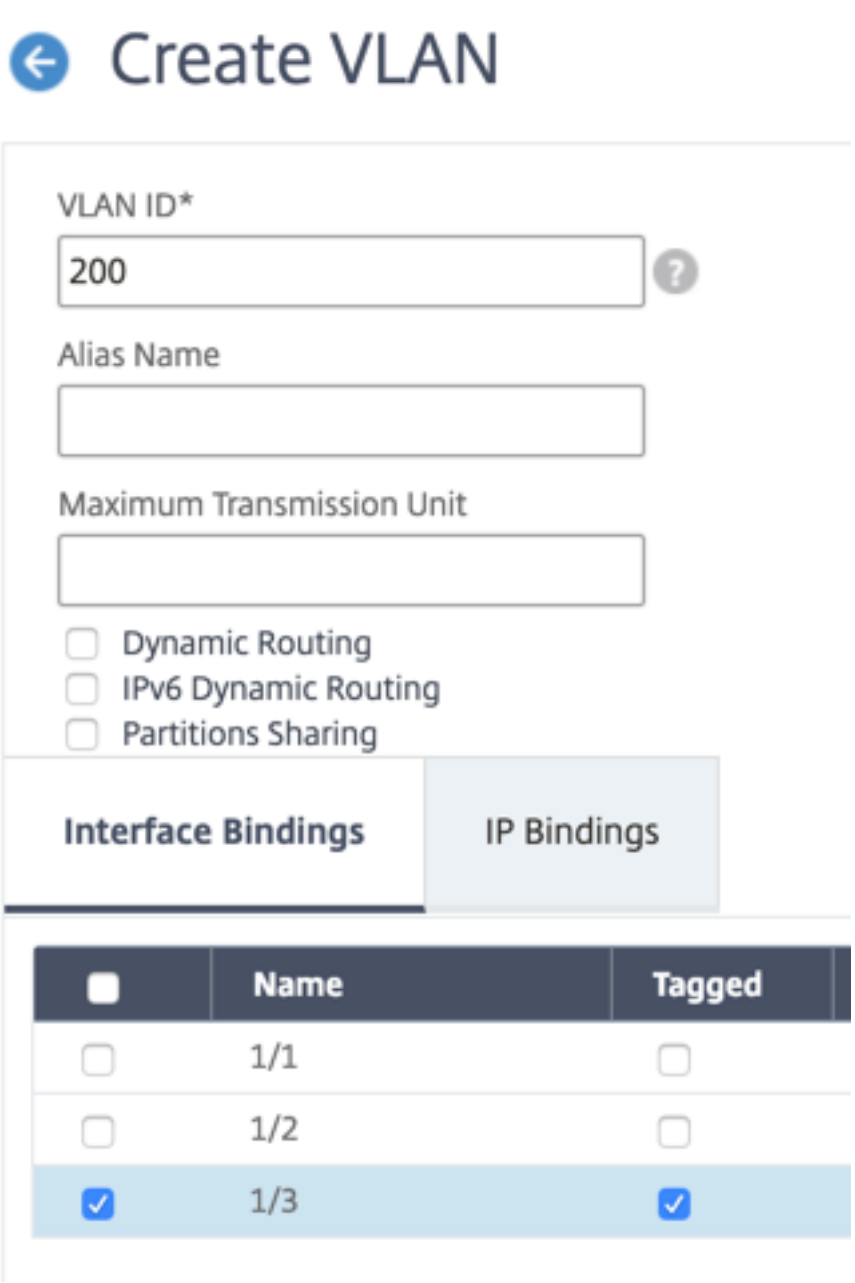
2. Navigieren Sie zu **System > Einstellungen**. Klicken Sie unter **Modi und Features** auf **Erweiterte Funktionen konfigurieren**.

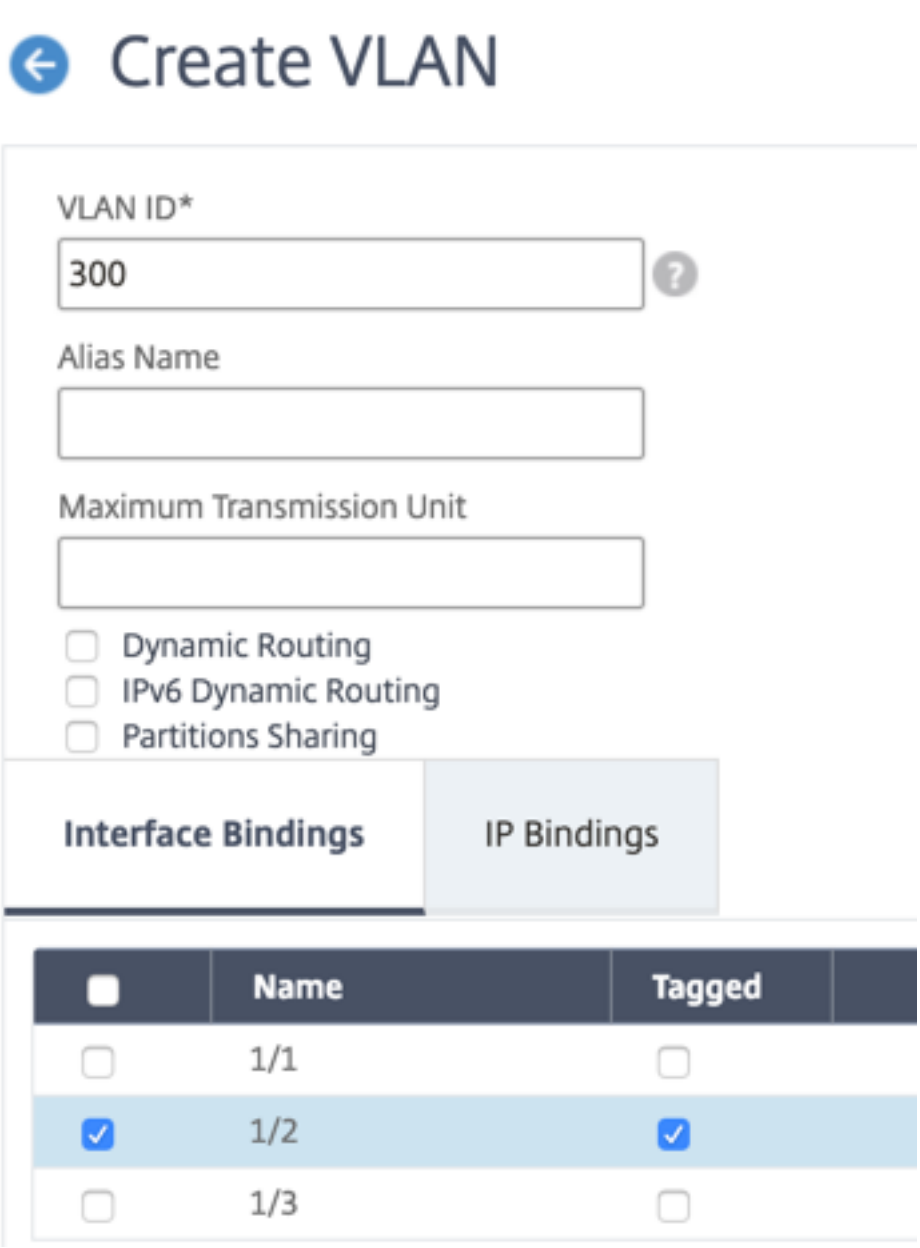


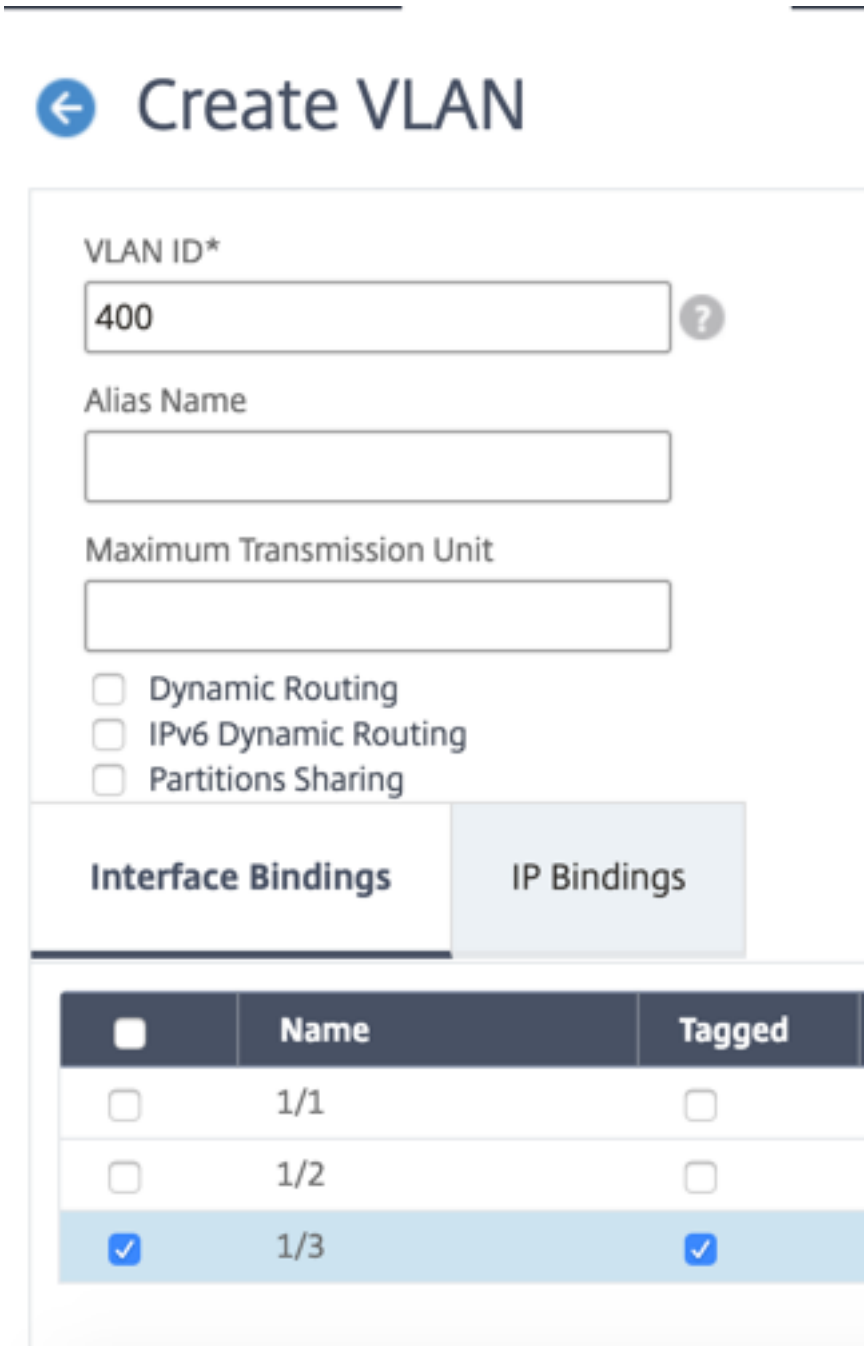


3. Navigieren Sie zu **System > Netzwerk > VLANs > Hinzufügen**. Fügen Sie vier VLANs hinzu und markieren Sie sie den Schnittstellen.

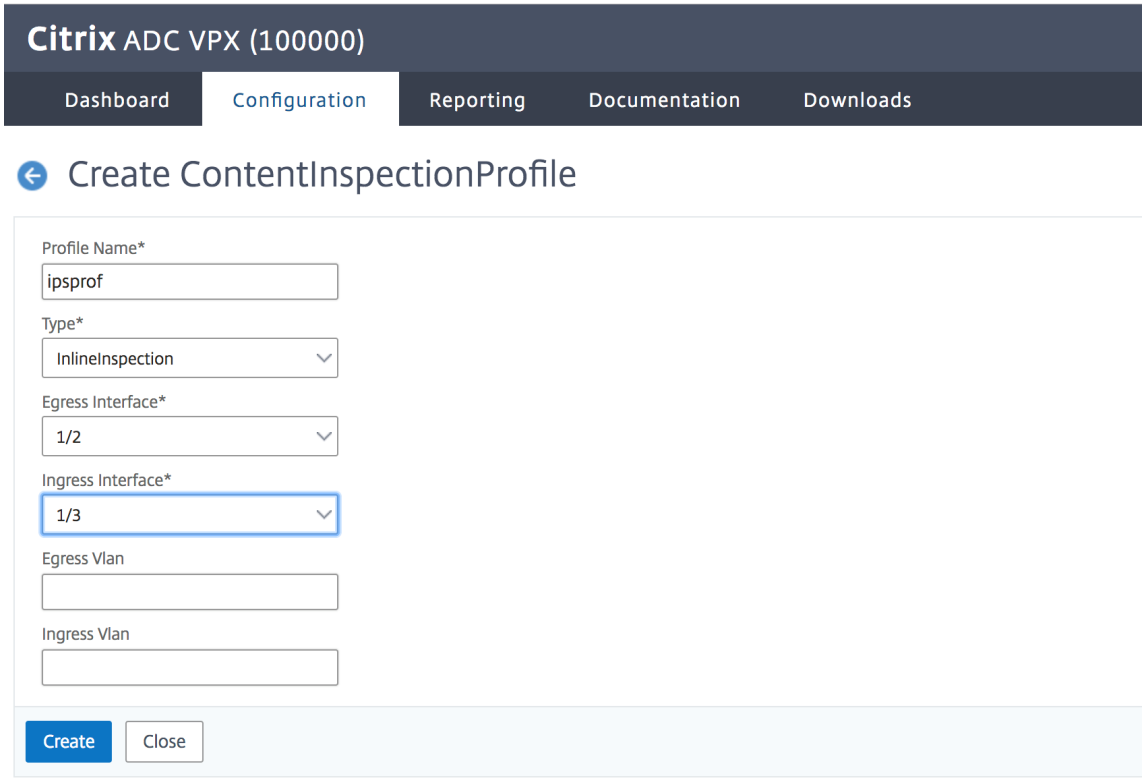




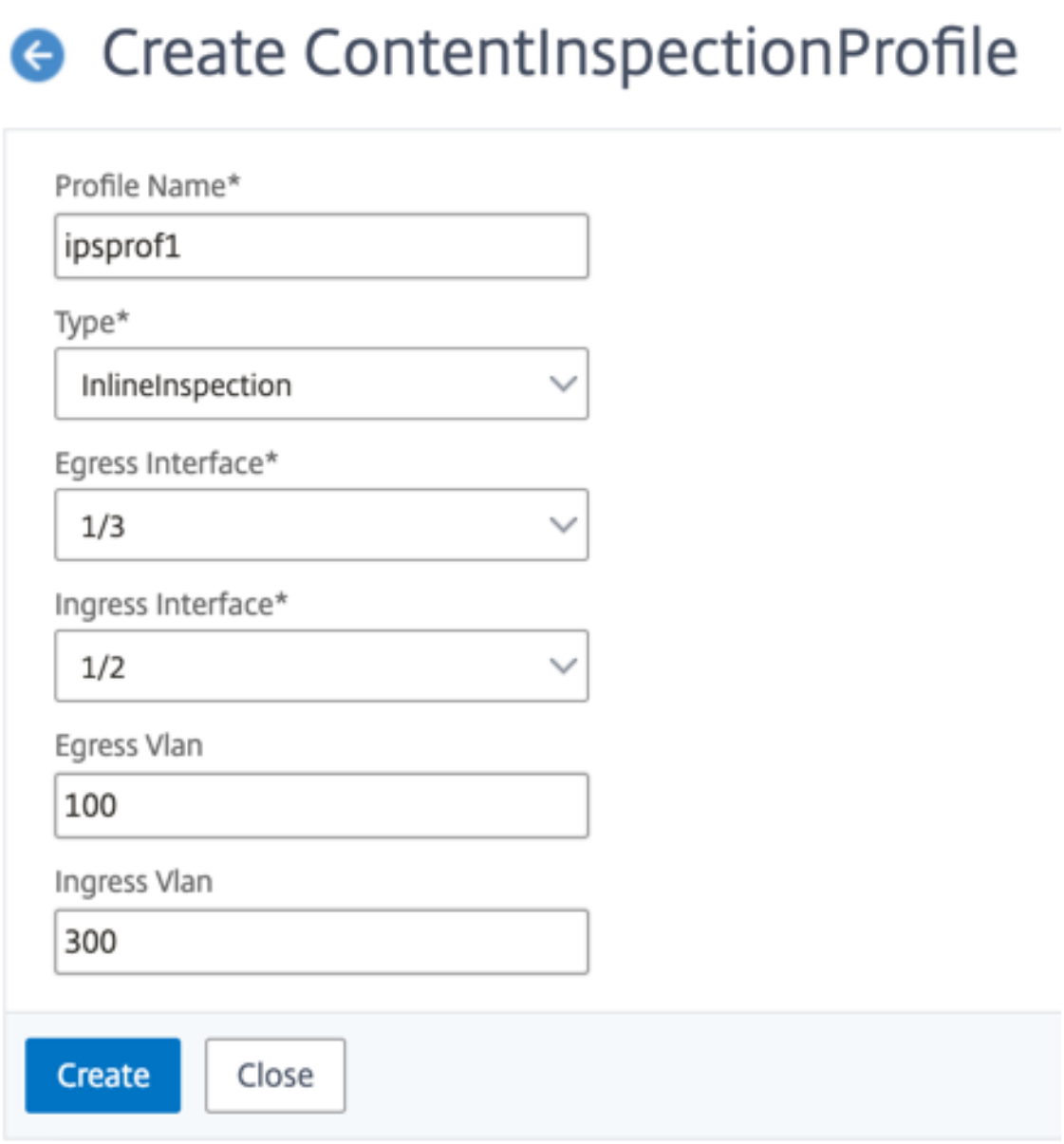




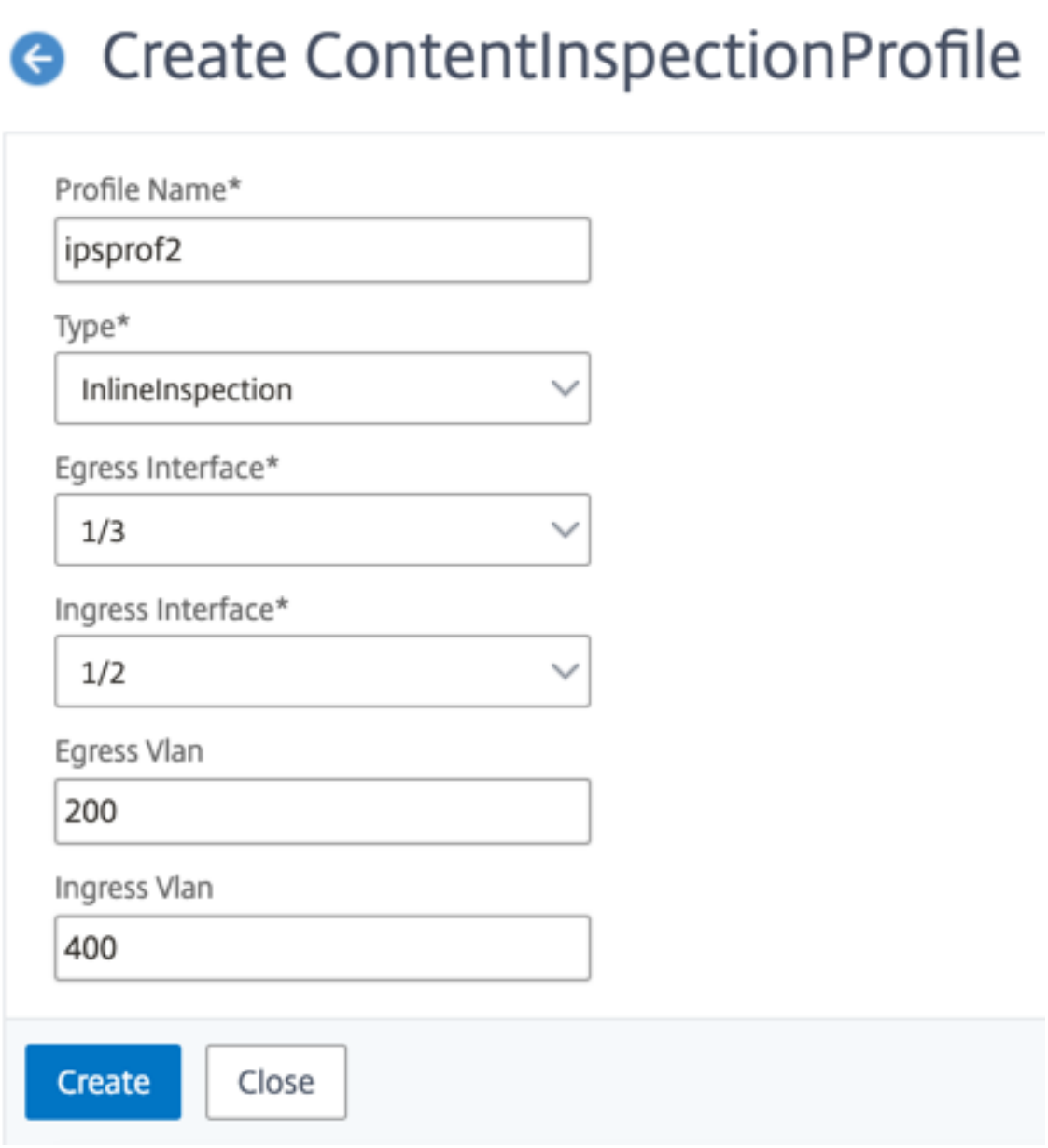
4. Navigieren Sie zu **Secure Web Gateway > Content Inspection > Content Inspection Profile**. Klicken Sie auf **Hinzufügen**.



Geben Sie die Ein- und Aus-VLANs an.

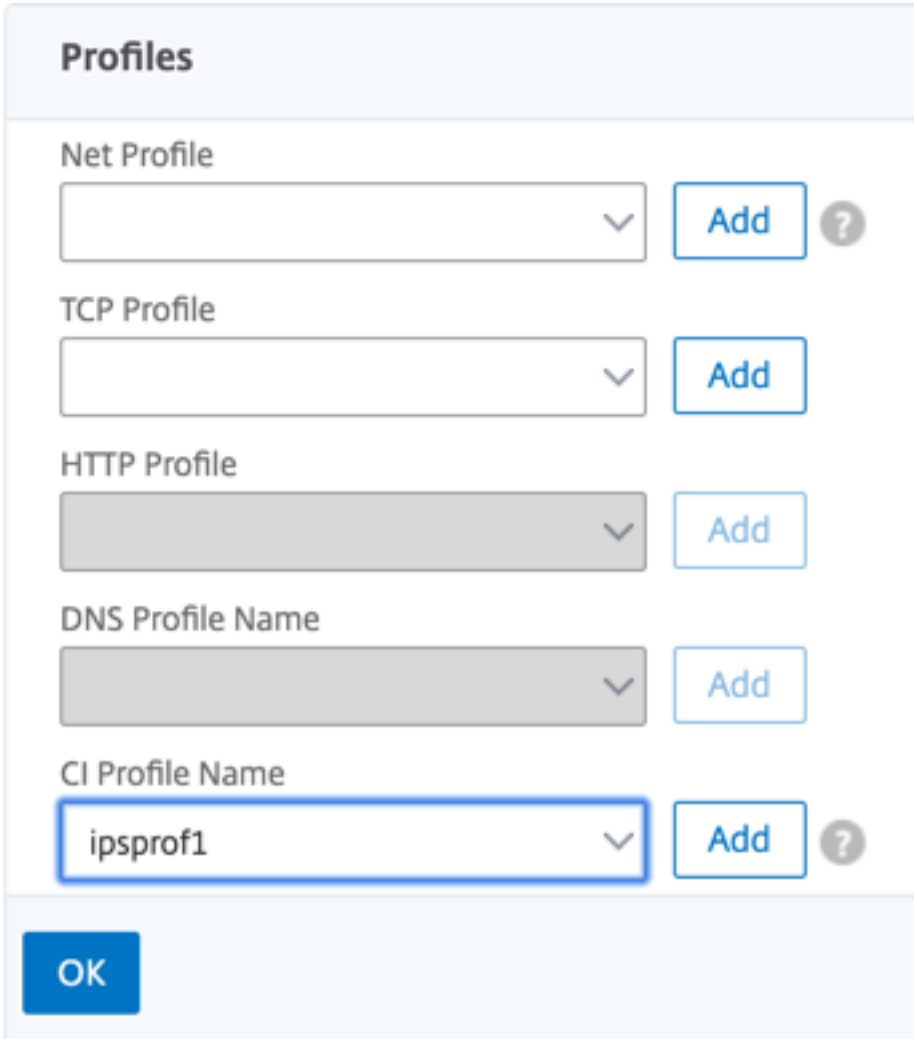


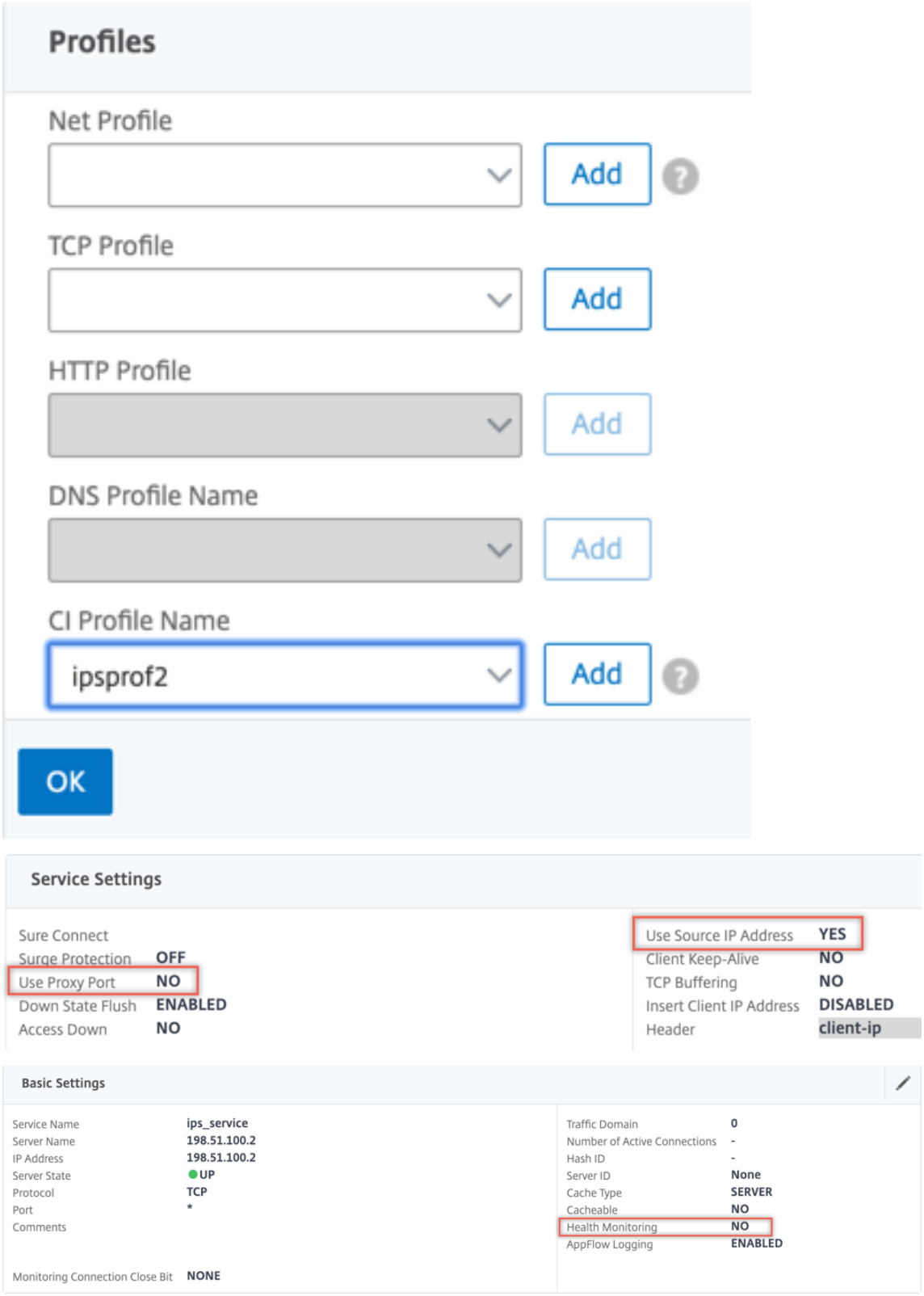
Erstellen Sie weitere Profile. Geben Sie im zweiten Profil ein anderes Ingress- und Egress-VLAN an.



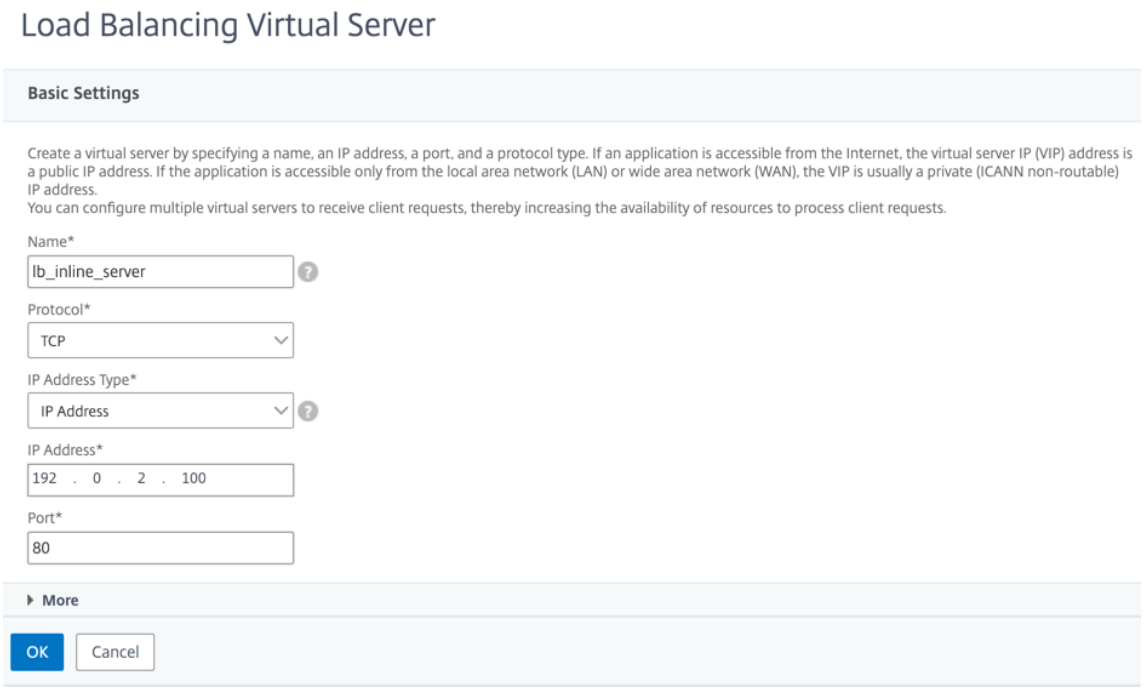
5. Navigieren Sie zu **Load Balancing > Services > Hinzufügen** und fügen Sie einen Service hinzu. Klicken Sie unter **Erweiterte Einstellungen** auf **Profile**. Wählen Sie in der Liste **CI-Profilname** das zuvor erstellte Content-Inspektionsprofil aus. Legen Sie unter **Diensteinstellungen** die Option **Quell-IP-Adresse verwenden** auf Ja und **Proxyport verwenden** auf Nein fest. Legen Sie in den **Grundeinstellungen** die **Integritätsüberwachung** auf Nein fest.

   Erstellen Sie zwei Dienste. Geben Sie Dummy-IP-Adressen an, die keinem der Geräte gehören, einschließlich der Inline-Geräte. Geben Sie Profil 1 in Dienst 1 und Profil 2 in Dienst 2 an.

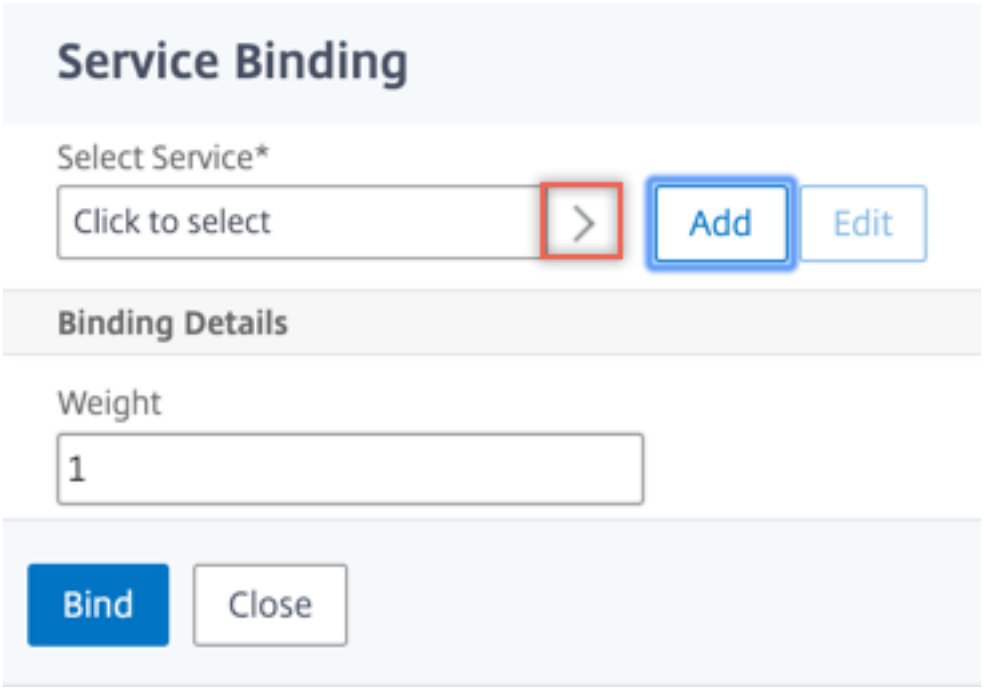


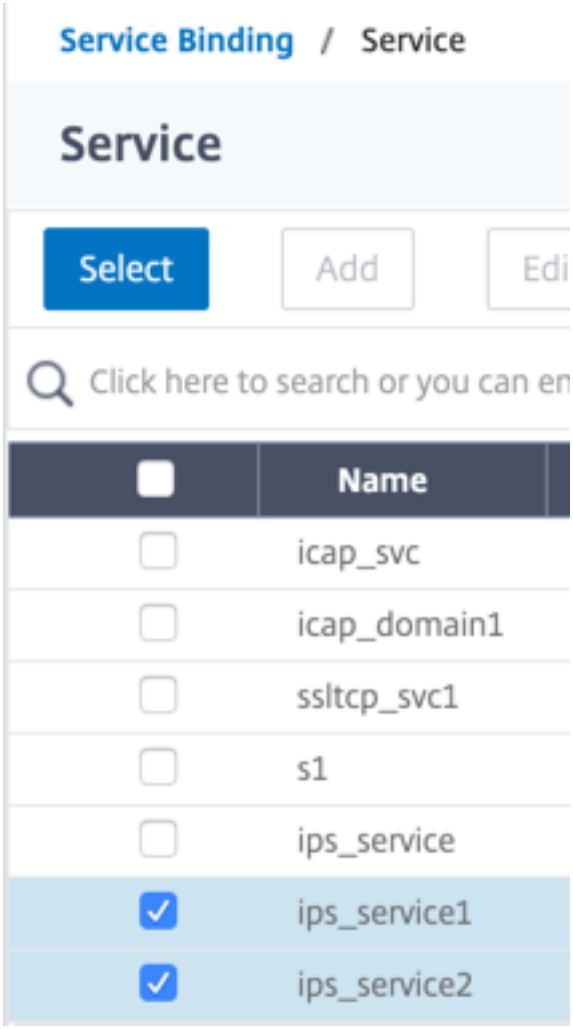


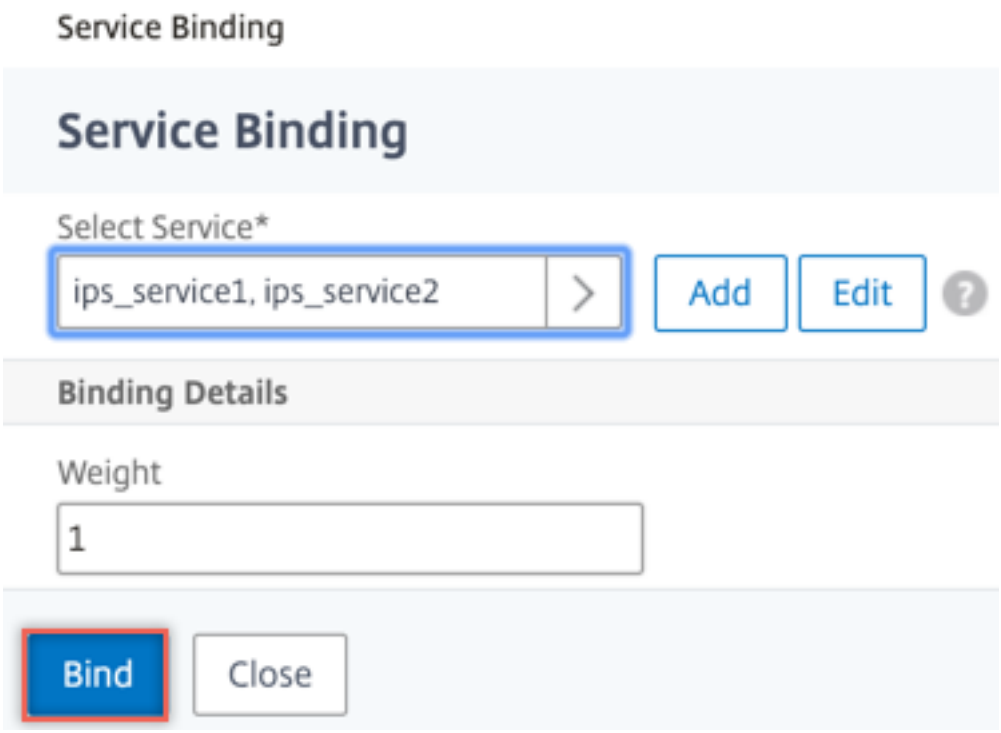
6. Navigieren Sie zu **Lastenausgleich > Virtuelle Server > Hinzufügen**. Erstellen Sie einen virtuellen TCP-Load Balancing Server.



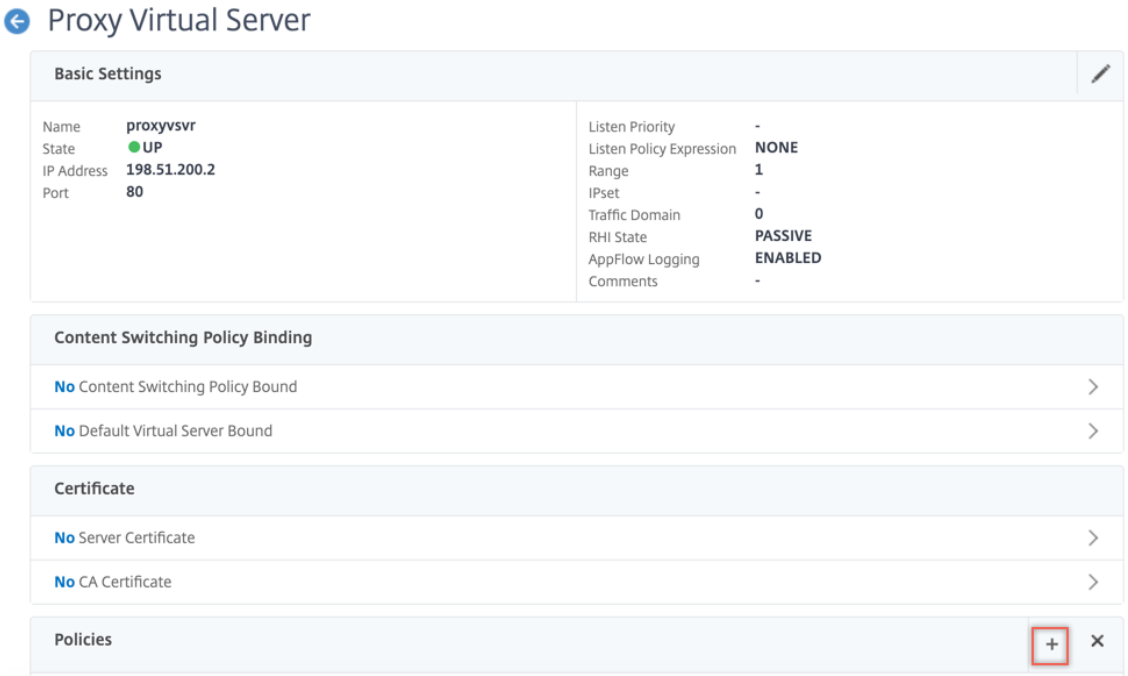
7. Klicken Sie auf **OK**.
8. Klicken Sie in den Abschnitt **Load Balancing Virtual Server Service Binding**. Klicken Sie unter **Dienstbindung** auf den Pfeil unter **Dienst auswählen**. Wählen Sie die beiden zuvor erstellten Dienste aus, und klicken Sie auf **Auswählen**. Klicken Sie auf **Bind**.



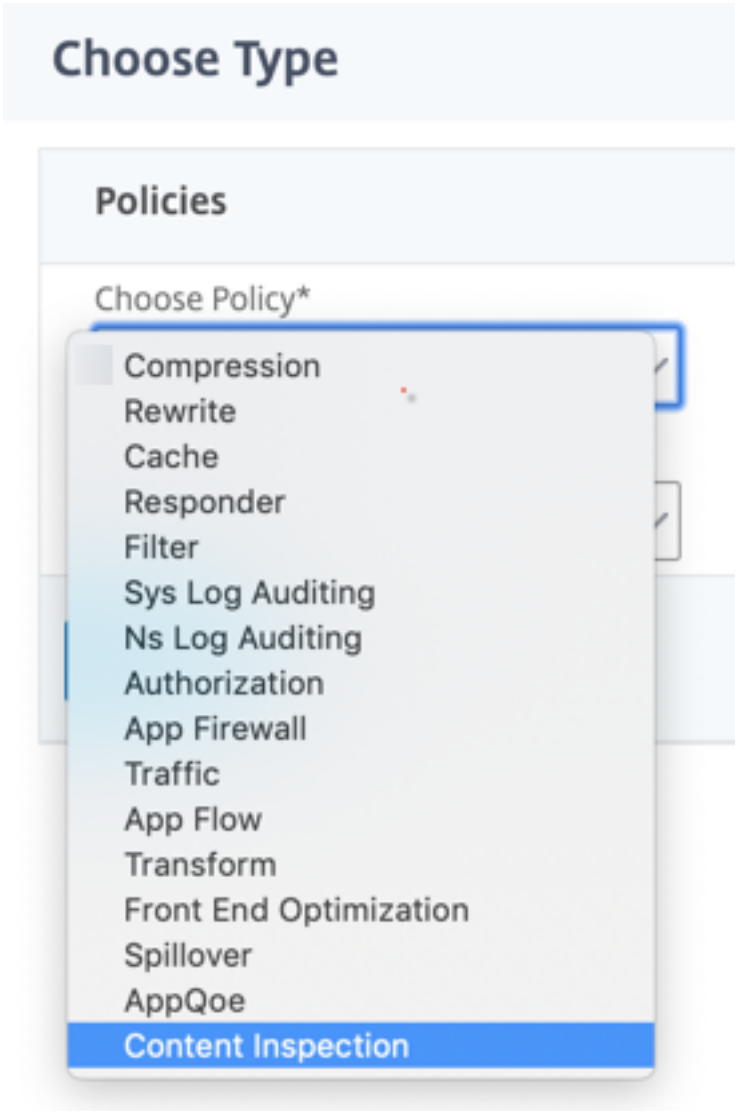




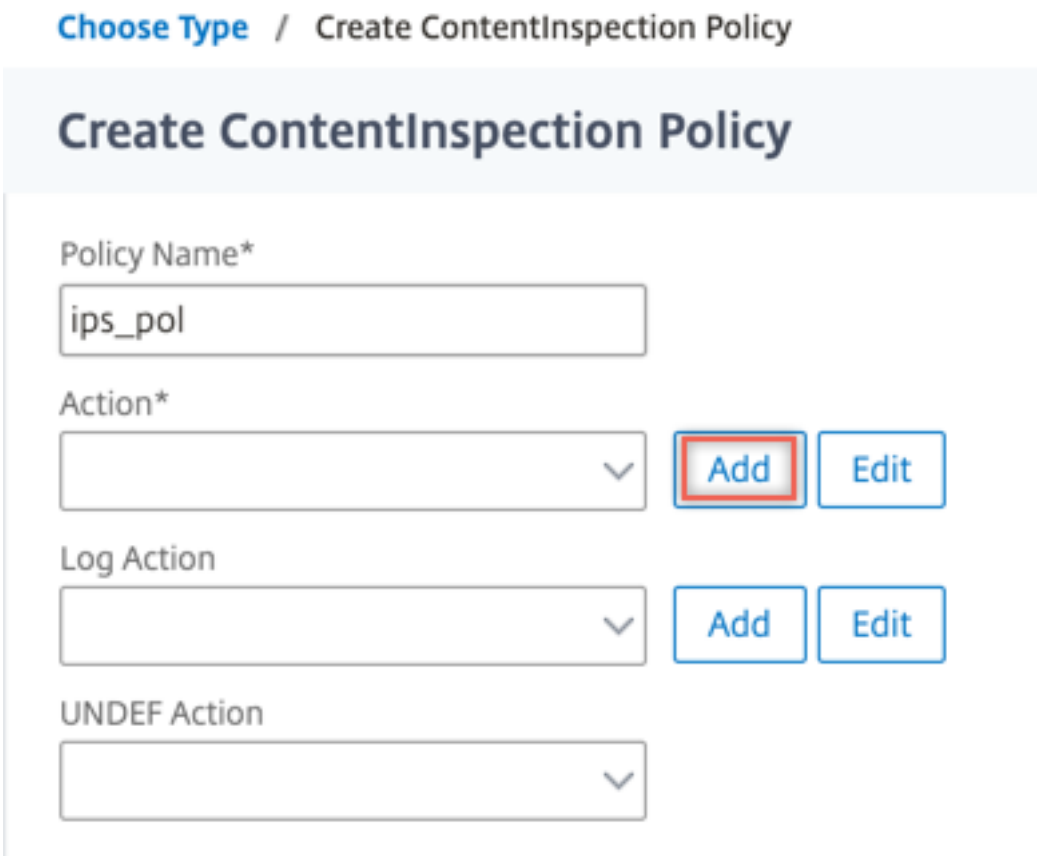
9. Navigieren Sie zu **Secure Web Gateway > Virtuelle Proxyserver > Hinzufügen**. Geben Sie einen Namen, eine IP-Adresse und einen Port an. Wählen Sie unter **Erweiterte Einstellungen** die Option **Richtlinien**aus. Klicken Sie auf das +-Zeichen.



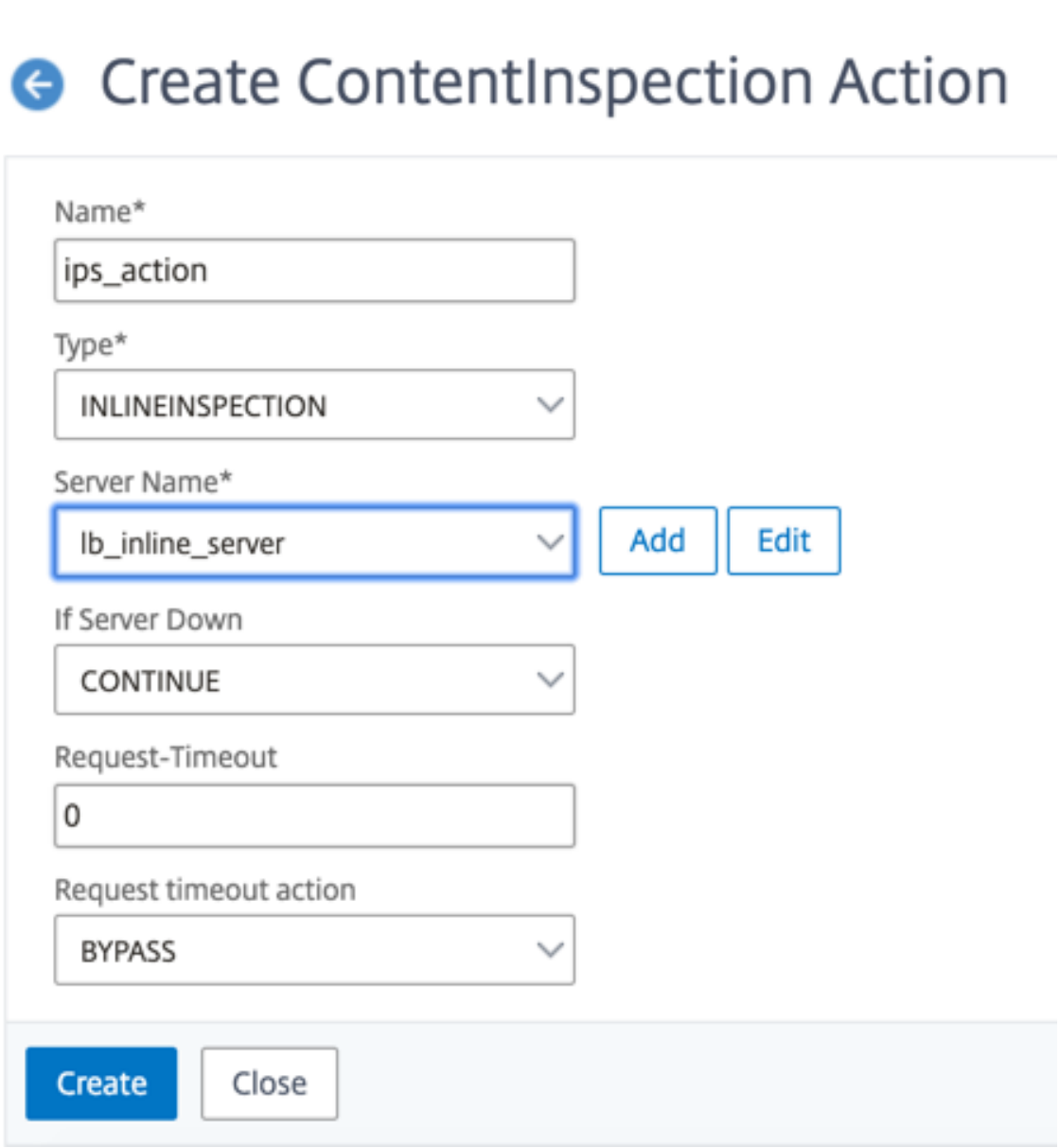
10. Wählen Sie unter **Richtlinie auswählen** die Option **Inhaltsüberprüfung** aus. Klicken Sie auf **Weiter**.



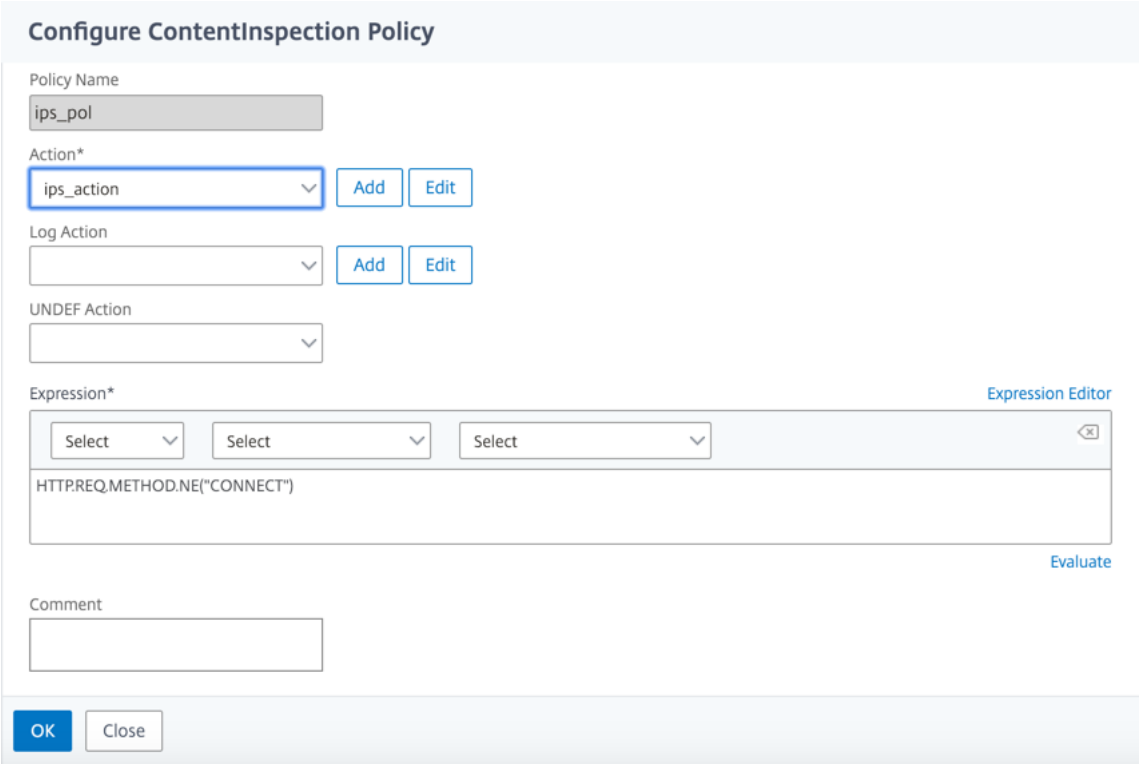
11. Klicken Sie auf **Hinzufügen**. Geben Sie einen Namen an. Klicken Sie unter **Aktion** auf **Hinzufügen**.



12. Geben Sie einen Namen an. Wählen Sie unter **Typ** die Option **INLINEINSPECTION** aus. Wählen Sie unter **Servername** den zuvor erstellten virtuellen Lastenausgleichsserver aus.



13. Klicken Sie auf **Erstellen**. Geben Sie die Regel an, und klicken Sie auf **Erstellen**.



14. Klicken Sie auf **Bind**.
15. Klicken Sie auf **Fertig**.

Integrieren von Citrix ADC mit passiven Sicherheitsgeräten (Intrusion Detection System)

January 25, 2022

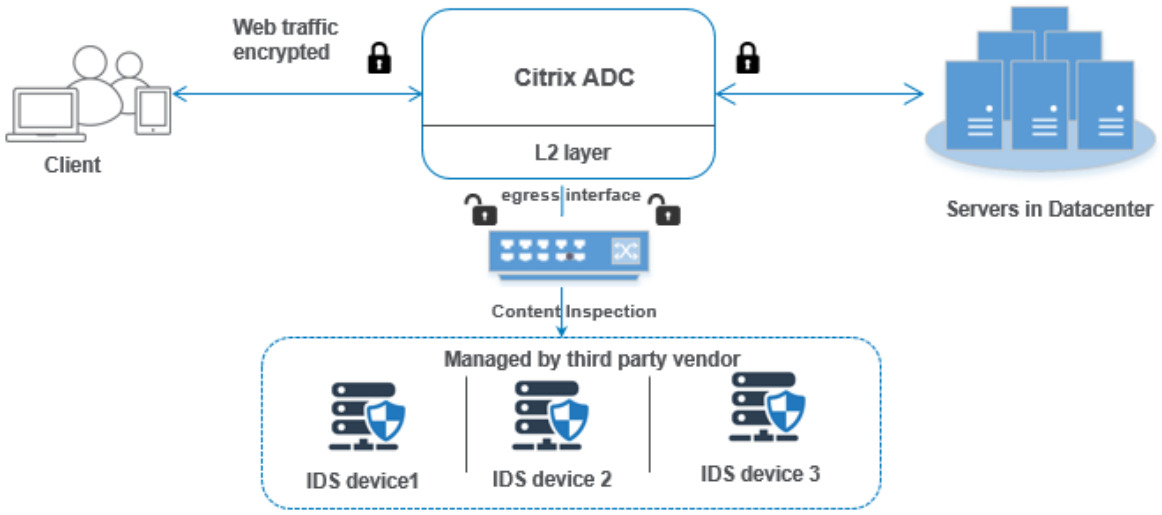
Eine Citrix ADC-Appliance ist jetzt in passive Sicherheitsgeräte wie das Intrusion Detection System (IDS) integriert. Diese passiven Geräte speichern Protokolle und lösen Warnungen aus, wenn sie einen schlechten oder nicht konformen Datenverkehr erkennen. Es generiert auch Berichte für den Compliance-Zweck. Wenn die Citrix ADC-Appliance in zwei oder mehr IDS-Geräte integriert ist und wenn ein hohes Verkehrsaufkommen vorhanden ist, kann die Appliance die Geräte ausgleichen, indem der Datenverkehr auf virtueller Serverebene geklont wird.

Für erweiterten Sicherheitsschutz ist eine Citrix ADC-Appliance in passive Sicherheitsgeräte wie IDS integriert, die im Nur-Erkennungsmodus bereitgestellt werden. Diese Geräte speichern Protokolle und lösen Warnungen aus, wenn ein schlechter oder nicht konformer Datenverkehr festgestellt wird. Es generiert auch Berichte für den Compliance-Zweck. Im Folgenden sind einige der Vorteile der Integration des Citrix ADC in ein IDS-Gerät aufgeführt.

- **Überprüfung des verschlüsselten Datenverkehrs**. Die meisten Sicherheitsgeräte Bypass den verschlüsselten Datenverkehr, wodurch Server anfällig für Angriffe sind. Eine Citrix ADC-Appliance kann den Datenverkehr entschlüsseln und an IDS-Geräte senden, um die Netzwerksicherheit des Kunden zu verbessern.
- **Entladen von Inline-Geräten von der TLS/SSL-Verarbeitung**. Die TLS/SSL-Verarbeitung ist teuer und führt zu einer hohen System-CPU in Intrusion-Detection-Geräten, wenn sie den Datenverkehr entschlüsseln. Da der verschlüsselte Datenverkehr schnell zunimmt, können diese Systeme den verschlüsselten Datenverkehr nicht entschlüsseln und überprüfen. Citrix ADC hilft beim Auslagern des Datenverkehrs von der TLS/SSL-Verarbeitung auf IDS-Geräte. Diese Art der Datenauslagerung führt dazu, dass ein IDS-Gerät ein hohes Verkehrsaufkommen unterstützt.
- **Laden ausgleichender IDS-Geräte**. Die Citrix ADC-Appliance gleicht mehrere IDS-Geräte aus, wenn ein hohes Verkehrsaufkommen besteht, indem der Datenverkehr auf virtueller Serverebene geklont wird.
- **Replikation des Datenverkehrs auf passive Geräte**. Der in die Appliance fließende Datenverkehr kann auf andere passive Geräte repliziert werden, um Konformitätsberichte zu erstellen. Zum Beispiel schreiben nur wenige Regierungsbehörden vor, dass jede Transaktion in einigen passiven Geräten protokolliert wird.
- **Fächern des Datenverkehrs zu mehreren passiven Geräten**. Einige Kunden ziehen es vor, eingehenden Datenverkehr auf mehrere passive Geräte aufzufächern oder zu replizieren.
- **Intelligente Auswahl des Verkehrs**. Jedes Paket, das in die Appliance fließt, muss möglicherweise nicht inhaltlich geprüft werden, z. B. Der Benutzer kann die Citrix ADC-Appliance so konfigurieren, dass ein bestimmter Datenverkehr (z. B. EXE-Dateien) zur Überprüfung ausgewählt und der Datenverkehr zur Datenverarbeitung an IDS-Geräte gesendet wird.

Wie Citrix ADC in ein IDS-Gerät mit L2-Konnektivität integriert ist

Das folgende Diagramm zeigt, wie IDS in eine Citrix ADC-Appliance integriert ist.



Die Wechselwirkung der Komponenten ist wie folgt gegeben:

1. Ein Client sendet eine HTTP/HTTPS-Anforderung an die Citrix ADC-Appliance.
2. Die Appliance fängt den Datenverkehr ab und repliziert ihn auf ein IDS-Gerät basierend auf der Bewertung der Inhaltsüberprüfungsrichtlinie.
3. Wenn der Datenverkehr verschlüsselt ist, entschlüsselt die Appliance die Daten und sendet sie als Nur-Text.
4. Basierend auf der Bewertung der Richtlinien wendet die Appliance eine Inhaltsinspektionsaktion vom Typ “MIRROR” an
5. In der Aktion ist der IDS-Dienst oder der Lastausgleichsdienst (für mehrere IDS-Geräteintegrationen) konfiguriert.
6. Das IDS-Gerät ist auf der Appliance als Content-Inspection-Diensttyp “Beliebig” konfiguriert. Der Inhaltsinspektionsdienst wird dann dem Inhaltsinspektionsprofil vom Typ “MIRROR” zugeordnet, das die Ausgangsschnittstelle angibt, über die die Daten an das IDS-Gerät weitergeleitet werden müssen. Optional können Sie auch ein VLAN-Tag im Inhaltsüberprüfungsprofil konfigurieren.

   > **Hinweis:**
   >
   > - Die für den IDS-Dienst oder -Server verwendete IP-Adresse ist eine Dummy-Adresse.
   > - Die Citrix ADC-Appliance unterstützt keinen LA-Kanal für die Ausgangsschnittstelle.

7. Die Appliance repliziert dann die Daten über die Ausgangsschnittstelle auf ein oder mehrere IDS-Geräte.
8. Wenn der Back-End-Server eine Antwort an den Citrix ADC sendet, repliziert die Appliance die Daten und leitet sie an das IDS-Gerät weiter.

9. Wenn Ihre Appliance in ein oder mehrere IDS-Geräte integriert ist und Sie den Lastausgleich der Geräte bevorzugen, können Sie den virtuellen Lastausgleichsserver verwenden.

Softwarelizenzierung

Um die Inline-Gerätintegration bereitzustellen, muss Ihre Citrix ADC-Appliance mit einer der folgenden Lizenzen ausgestattet sein:

1. ADC Premium
2. ADC Advanced
3. Telco Fortgeschrittene
4. Telco Premium

Konfigurieren der Einbruchmelde-Systemintegration

Sie können das IDS-Gerät auf zwei verschiedene Arten in den Citrix ADC integrieren.

Szenario 1: Integration mit einem einzigen IDS-Gerät

Im Folgenden sind die Schritte aufgeführt, die Sie mithilfe der Befehlszeilenschnittstelle konfigurieren müssen.

1. Inhaltsüberprüfung aktivieren
2. Inhaltsüberprüfungsprofil vom Typ MIRROR für den Dienst, der das IDS-Gerät
3. IDS-Dienst vom Typ “ANY” hinzufügen
4. Inhaltsüberprüfungsaktion vom Typ “MIRROR” hinzugefügt
5. Inhaltsüberprüfungsrichtlinie für die IDS-Überprüfung hinzufügen
6. Binden Sie die Inhaltsüberprüfungsrichtlinie an den virtuellen Content Switching- oder Lastausgleichsdienst des Typs HTTP/SSL

Inhaltsüberprüfung aktivieren

Wenn Sie möchten, dass die Citrix ADC-Appliance den Inhalt zur Überprüfung an die IDS-Geräte sendet, müssen Sie die Funktionen Inhaltsüberprüfung und den Lastausgleich unabhängig von der Entschlüsselung aktivieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns feature contentInspection LoadBalancing
```

Inhaltsüberprüfungsprofil vom Typ “MIRROR”

Das Inhaltsüberprüfungsprofil vom Typ “MIRROR” erklärt, wie Sie eine Verbindung zum IDS-Gerät herstellen können.
Geben Sie an der Eingabeaufforderung ein.

```
add contentInspection profile <name> -type MIRROR -egressInterface <interface_name
> [-egressVlan <positive_integer>]
```

Beispiel:

```
add contentInspection profile IDS_profile1 -type MIRROR -egressInterface
1/1 -egressVLAN 10
```

IDS-Dienst hinzufügen

Sie müssen einen Dienst vom Typ “ANY” für jedes IDS-Gerät konfigurieren, das in die Appliance integriert ist. Der Dienst hat die IDS-Gerätekonfigurationsdetails. Der Dienst stellt das IDS-Gerät dar.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <Service_name> <IP> ANY <Port> - contentinspectionProfileName <
Name> -healthMonitor OFF -usip ON -useproxyport OFF
```

Beispiel:

```
add service IDS_service 1.1.1.1 ANY 8080 -contentInspectionProfileName
IDS_profile1 -healthMonitor OFF
```

Inhaltsüberprüfungsaktion vom Typ MIRROR für IDS-Dienst hinzufügen

Nachdem Sie die Funktion Inhaltsüberprüfung aktiviert und anschließend das IDS-Profil und den Dienst hinzugefügt haben, müssen Sie die Aktion Inhaltsüberprüfung für die Bearbeitung der Anforderung hinzufügen. Basierend auf der Inhaltsüberprüfungsaktion kann die Appliance Daten löschen, zurücksetzen, blockieren oder an das IDS-Gerät senden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ContentInspection action < action_name > -type MIRROR -serverName
Service_name/Vserver_name>
```

Beispiel:

```
add ContentInspection action IDS_action -type MIRROR -serverName IDS_service
```

Inhaltsüberprüfungsrichtlinie für die IDS-Überprüfung hinzufügen

Nachdem Sie eine Inhaltsüberprüfungsaktion erstellt haben, müssen Sie Richtlinien für die Inhaltsüberprüfung hinzufügen, um Überprüfungsanfragen zu bewerten. Die Richtlinie basiert auf einer

Regel, die aus einem oder mehreren Ausdrücken besteht. Die Richtlinie bewertet und wählt den zu überprüfenden Verkehr basierend auf der Regel aus.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection policy < policy_name > -rule <Rule> -action <action_name
>
```

Beispiel:

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Binden Sie die Inhaltsüberprüfungsrichtlinie an den virtuellen Content Switching- oder Lastausgleichsdienst des Typs HTTP/SSL

Um den Webverkehr zu empfangen, müssen Sie einen virtuellen Lastausgleichsserver hinzufügen. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <vserver name>
```

Beispiel:

```
add lb vserver HTTP_vserver HTTP 1.1.1.3 8080
```

Binden der Richtlinie zur Inhaltsüberprüfung an den virtuellen Server mit Content Switching oder den virtuellen Lastausgleichsserver vom Typ

Sie müssen den virtuellen Load Balancing-Server oder den virtuellen Content Switching-Server vom Typ HTTP/SSL an die Inhaltsüberprüfungsrichtlinie binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

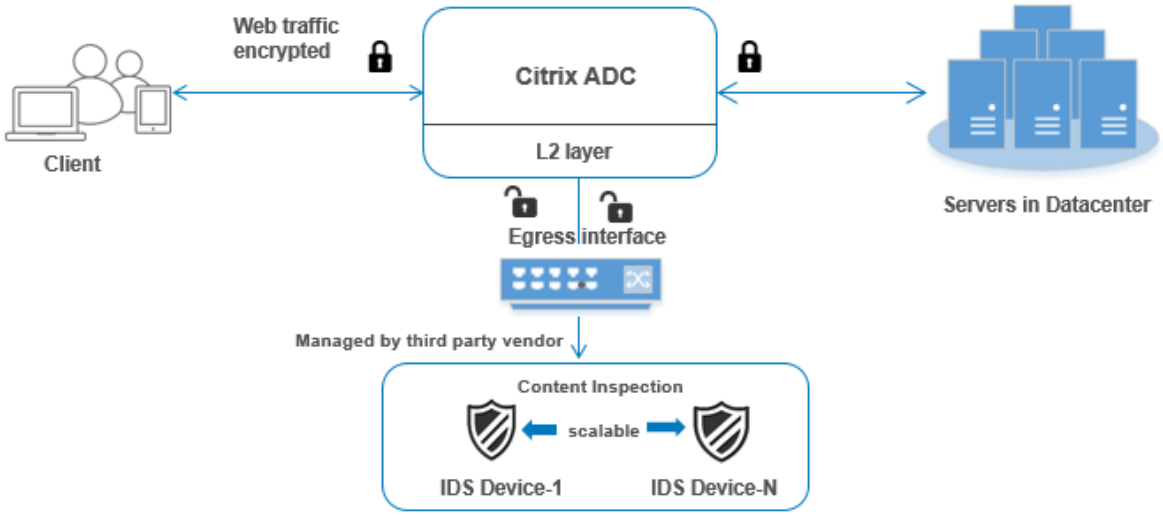
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <
priority > -type <REQUEST>
```

Beispiel:

```
bind lb vserver HTTP_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

Szenario 2: Lastenausgleich für mehrere IDS-Geräte

Wenn Sie zwei oder mehr IDS-Geräte verwenden, müssen Sie die Last der Geräte mithilfe verschiedener Inhaltsüberprüfungsdienste ausgleichen. In diesem Fall gleicht die Citrix ADC-Appliance die Geräte aus, zusätzlich zum Senden einer Teilmenge des Datenverkehrs an jedes Gerät. Grundlegende Konfigurationsschritte finden Sie in Szenario 1.



Im Folgenden sind die Schritte aufgeführt, die Sie mithilfe der Befehlszeilenschnittstelle konfigurieren müssen.

1. Inhaltsüberprüfungsprofil 1 vom Typ MIRROR für IDS-Dienst 1 hinzufügen
2. Inhaltsüberprüfungsprofil 2 vom Typ MIRROR für IDS-Dienst 2 hinzufügen
3. IDS-Dienst 1 vom Typ ANY für IDS-Gerät 1 hinzufügen
4. IDS-Dienst 2 vom Typ ANY für IDS-Gerät 2 hinzufügen
5. Hinzufügen eines virtuellen Lastausgleichsservers vom Typ ANY
6. IDS-Dienst 1 an den virtuellen Lastausgleichsserver binden
7. IDS-Dienst 2 an den virtuellen Lastausgleichsserver binden
8. Fügen Sie eine Inhaltsüberprüfungsaktion für den Lastausgleich von IDS-Geräten hinzu.
9. Inhaltsüberprüfungsrichtlinie zur Überprüfung hinzufügen
10. Hinzufügen eines virtuellen Content Switching- oder Lastausgleichsservers vom Typ HTTP/SSL
11. Richtlinie zur Inhaltsüberprüfung an einen virtuellen Lastausgleichsserver vom Typ HTTP/SSL binden

Inhaltsüberprüfungsprofil 1 vom Typ MIRROR für IDS-Dienst 1 hinzufügen

Die IDS-Konfiguration kann in einer Entität angegeben werden, die als Inhaltsprüfprofil bezeichnet wird. Das Profil hat eine Sammlung von Geräteeinstellungen. Das Inhaltsüberprüfungsprofil1 wird für den IDS-Dienst 1 erstellt.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection profile <name> -type ANY -egressInterface <interface_name
> [-egressVlan <positive_integer>]
```

Beispiel:


```
add contentInspection profile IDS_profile1 -type MIRROR -egressInterface
1/1 -egressVLAN 1
```

Inhaltsüberprüfungsprofil 2 für den Typ MIRROR für IDS-Dienst 2

Das Inhaltsinspektionsprofil 2 wird für Dienst 2 hinzugefügt, und das Inline-Gerät kommuniziert mit der Appliance über die Ausgangsschnittstelle 1/1.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection profile <name> -type MIRROR -egressInterface -egressVlan
 <positive_integer>]
```

Beispiel:

```
add contentInspection profile IDS_profile1 -type MIRROR -egressInterface
1/1 -egressVLAN 1
```

IDS-Dienst 1 vom Typ ANY für IDS-Gerät 1 hinzufügen

Nachdem Sie die Funktion Inhaltsüberprüfung aktiviert und das Inline-Profil hinzugefügt haben, müssen Sie einen Inline-Dienst 1 für das Inline-Gerät 1 hinzufügen, um Teil des Lastausgleichs-Setups zu sein. Der Dienst, den Sie hinzufügen, enthält alle Inline-Konfigurationsdetails.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <Service_name_1> <Pvt_IP1> ANY <Port> -contentInspectionProfileName
 <IDS_Profile_1> -usip ON -useproxyport OFF
```

Beispiel:

```
add service IDS_service1 1.1.1.1 ANY 80 -contentInspectionProfileName
IDS_profile1 -usip ON -useproxyport OFF
```

> **Hinweis**
>
> Bei der im Beispiel genannten IP-Adresse handelt es sich um eine Scheinadresse.

IDS-Dienst 2 vom Typ ANY für IDS-Gerät 2 hinzufügen

Nachdem Sie die Inhaltsinspektionsfunktion aktiviert und das Inline-Profil hinzugefügt haben, müssen Sie einen Inline-Dienst 2 für das Inline-Gerät 2 hinzufügen. Der Dienst, den Sie hinzufügen, enthält alle Inline-Konfigurationsdetails.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <Service_name_1> <Pvt_IP1> ANY -contentInspectionProfileName <
Inline_Profile_2> -healthmonitor OFF -usip ON -useproxyport OFF
```


Beispiel:

```
add service IDS_service 1 1.1.2 ANY 80 -contentInspectionProfileName
IDS_profile2
```

> **Hinweis**
>
> Bei der im Beispiel genannten IP-Adresse handelt es sich um eine Scheinadresse.

Virtuellen Lastausgleichsserver hinzufügen

Nachdem Sie das Inline-Profil und die Dienste hinzugefügt haben, müssen Sie einen virtuellen Lastausgleichsserver für den Lastenausgleich der Dienste hinzufügen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <vserver_name> ANY <Pvt_IP3> <port>
```

Beispiel:

```
add lb vserver lb-IDS_vserver ANY 1.1.1.2
```

IDS-Dienst 1 an den virtuellen Lastausgleichsserver binden

Nachdem Sie den virtuellen Lastausgleichsserver hinzugefügt haben, binden Sie nun den virtuellen Lastausgleichsserver an den ersten Dienst.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Beispiel:

```
bind lb vserver lb-IDS_vserver IDS_service1
```

IDS-Dienst 2 an den virtuellen Lastausgleichsserver binden

Nachdem Sie den virtuellen Lastausgleichsserver hinzugefügt haben, binden Sie den Server nun an den zweiten Dienst.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Beispiel:

```
bind lb vserver lb-IDS_vserver IDS_service2
```


Inhaltsüberprüfungsaktion für den IDS-Dienst hinzufügen

Nachdem Sie die Funktion Inhaltsüberprüfung aktiviert haben, müssen Sie die Aktion Inhaltsüberprüfung für die Verarbeitung der Inline-Anforderungsinformationen hinzufügen. Basierend auf der ausgewählten Aktion verwirft, setzt die Appliance den Datenverkehr zurück, blockiert oder sendet ihn an das IDS-Gerät.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>]
```

Beispiel:

```
add ContentInspection action IDS_action -type MIRROR -serverName lb-IDS_vserver
```

Inhaltsüberprüfungsrichtlinie zur Überprüfung hinzufügen

Nachdem Sie eine Inhaltsüberprüfungsaktion erstellt haben, müssen Sie eine Inhaltsüberprüfungsrichtlinie hinzufügen, um Serviceanfragen zu bewerten.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Beispiel:

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Hinzufügen eines virtuellen Content Switching- oder Lastausgleichsservers vom Typ HTTP/SSL

Fügen Sie einen virtuellen Content Switching- oder Lastausgleichsserver hinzu, um Webverkehr zu akzeptieren Außerdem müssen Sie die Layer2-Verbindung auf dem virtuellen Server aktivieren.

Weitere Informationen zum Lastenausgleich finden Sie unter Funktionsweise des Lastenausgleichs .

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <vserver name>
```

Beispiel:

```
add lb vserver http_vserver HTTP 1.1.1.1 8080
```


Richtlinie zur Inhaltsüberprüfung an einen virtuellen Lastausgleichsserver vom Typ HTTP/SSL binden

Sie müssen den virtuellen Content Switching- oder Load Balancing-Server vom Typ HTTP/SSL an die Richtlinie zur Inhaltsüberprüfung binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

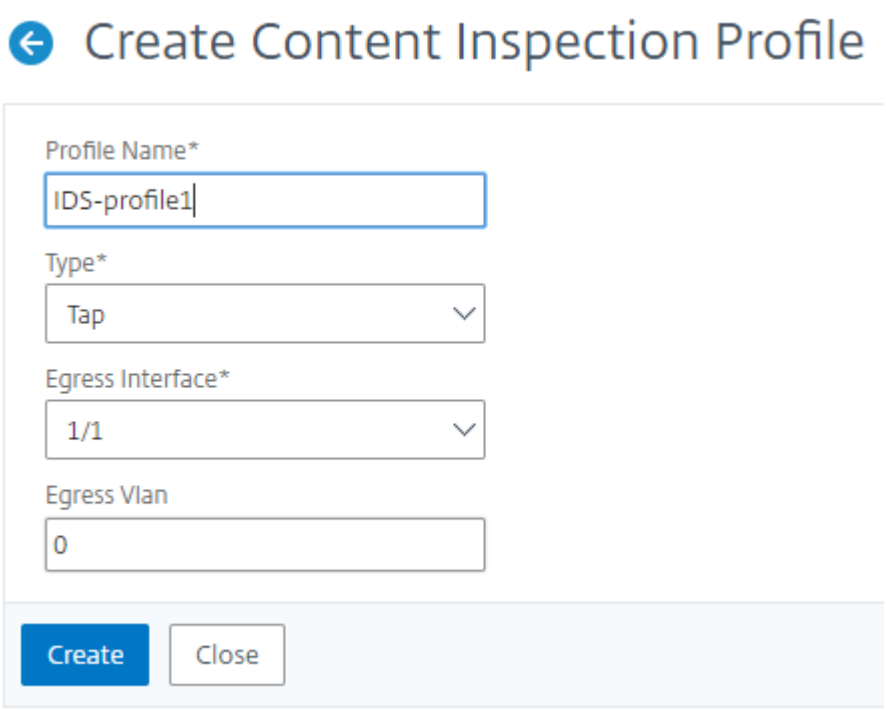
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <> -
type <REQUEST>
```

Beispiel:

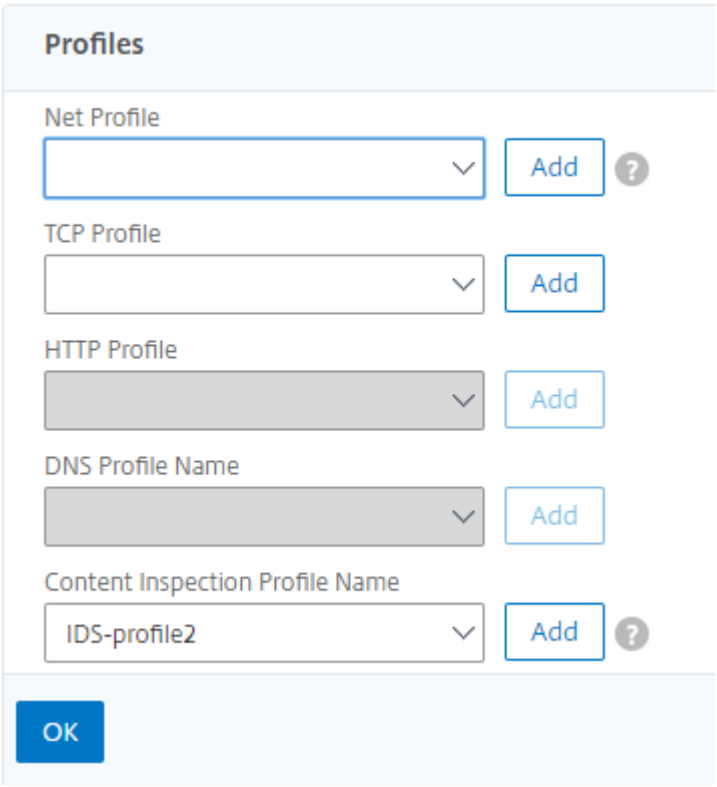
```
bind lb vserver http_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

Konfigurieren der Inline-Serviceintegration mithilfe der Citrix ADC GUI

1. Navigieren Sie zu **Sicherheit** > **Inhaltsüberprüfung** > **Inhaltsüberprüfungsprofile**.
2. Klicken Sie auf der **Seite Inhaltsüberprüfungsprofil** auf **Hinzufügen**.
3. Legen Sie auf der Seite **Inhaltsüberprüfungsprofil erstellen** die folgenden Parameter fest.
   a) Profilname Name des Inhaltsinspektionsprofils für IDS.
   b) Typ. Wählen Sie die Profiltypen als MIRROR aus.
   c) Ausgangsschnittstelle. Die Schnittstelle, über die der Datenverkehr vom Citrix ADC zum IDS-Gerät gesendet wird.
   d) Ausgang-VLAN (optional). Die Schnittstellen-VLAN-ID, über die der Datenverkehr an das IDS-Gerät gesendet wird.
4. Klicken Sie auf **Erstellen**.



5. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services** und klicken Sie auf **Hinzufügen**
6. Geben Sie auf der Seite **Load Balancing Service** die Details des Inhaltsüberprüfungsdienstes ein.
7. Klicken Sie im Abschnitt **“Erweiterte Einstellungen** “ auf “ **Profile**”.
8. Gehen Sie zum Abschnitt **Profile** und klicken Sie auf das **Bleistiftsymbol**, um das Inhaltsüberprüfungsprofil hinzuzufügen.
9. Klicken Sie auf **OK**.



10. Navigieren Sie zu **Load Balancing** > **Server**. Fügen Sie einen virtuellen Server vom Typ HTTP oder SSL hinzu.
11. Nachdem Sie die Serverdetails eingegeben haben, klicken Sie auf **OK** und erneut auf **OK**.
12. Klicken Sie im Abschnitt **“Erweiterte Einstellungen** “ auf **Richtlinien**.
13. Gehen Sie zum Abschnitt **Richtlinien** und klicken Sie auf das **Stiftsymbol**, um die Inhaltsüberprüfungsrichtlinie zu konfigurieren.
14. Wählen Sie auf der Seite **Richtlinie auswählen** die Option **Inhaltsübersicht** aus. Klicken Sie auf **Weiter**.
15. Klicken Sie im Abschnitt **Richtlinienbindung** auf “+”, um eine Richtlinie zur Inhaltsüberprüfung hinzuzufügen.
16. Geben Sie auf der Seite **CI-Richtlinie erstellen** einen Namen für die Richtlinie zur Inline-Inhaltsüberprüfung ein.
17. Klicken Sie im Feld **Aktion** auf das “+” -Zeichen, um eine IDS-Inhaltsüberprüfungsaktion vom Typ MIRROR zu erstellen.
18. Stellen Sie auf der Seite **CI-Aktion erstellen** die folgenden Parameter ein.

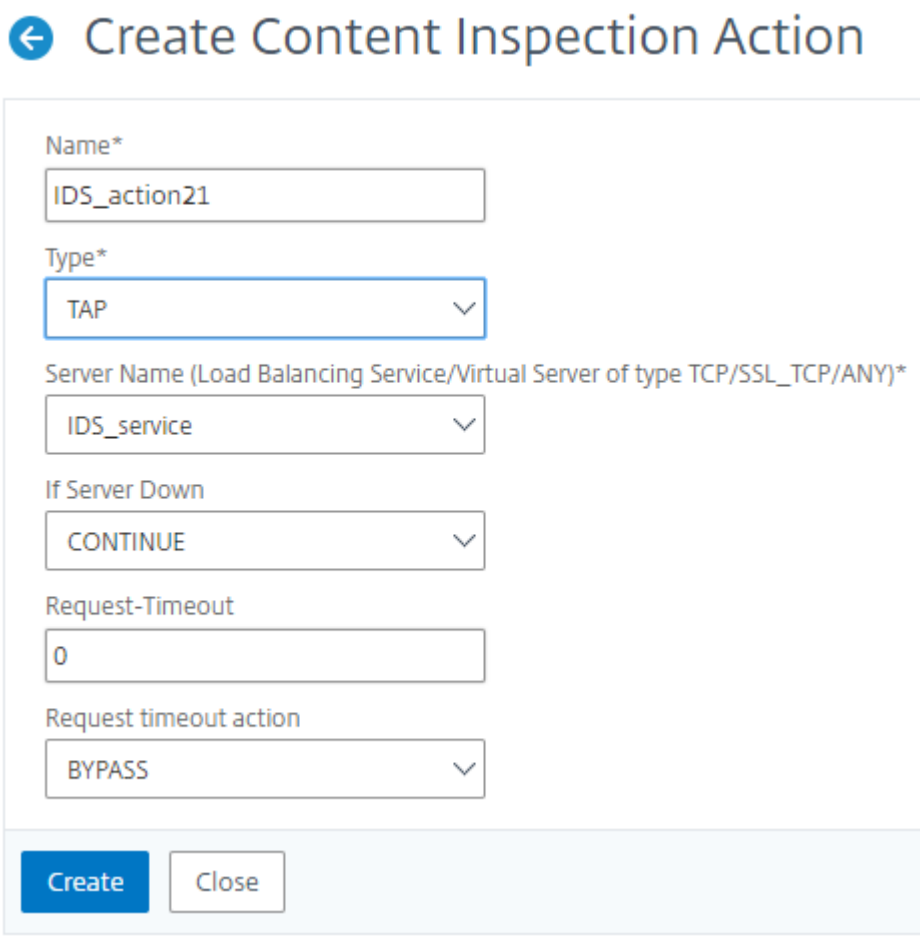
    a. Name. Name der Inline-Richtlinie zur Inhaltsüberprüfung.

b. Typ. Wählen Sie den Typ als MIRROR.
c. Servername. Wählen Sie den Server-/Dienstnamen als Inline-Geräte aus.

d. Wenn der Server ausgefallen ist. Wählen Sie einen Vorgang aus, wenn der Server ausfällt.
e. Zeitüberschreitung anfragen. Wählen Sie einen Timeoutwert aus. Standardwerte können verwendet werden.

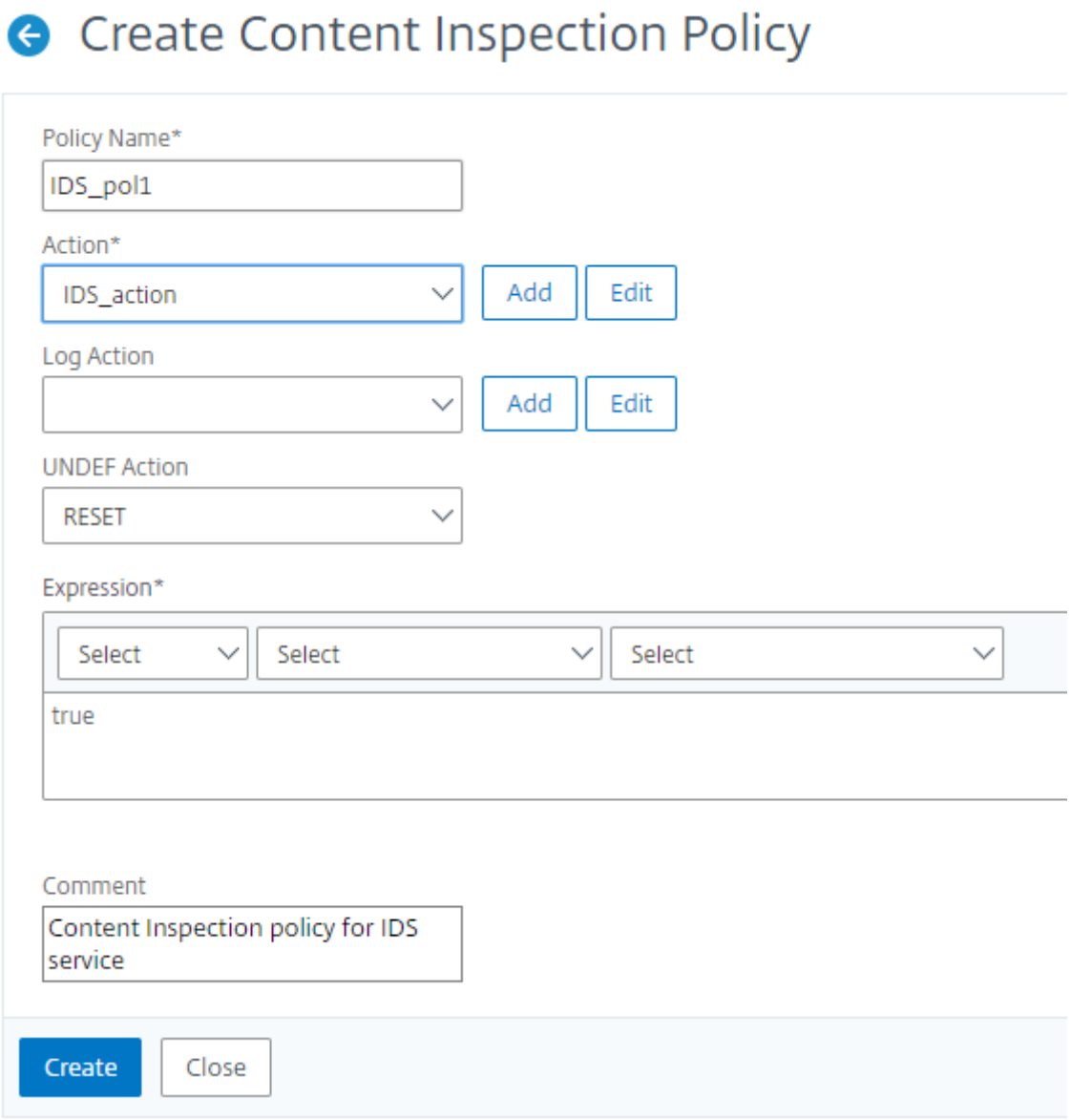
f. Timeout-Aktion anfordern. Wählen Sie eine Zeitüberschreitungsaktion aus. Standardwerte können verwendet werden.

19. Klicken Sie auf **Erstellen**.



20. Geben **Sie auf der Seite CI-Richtlinie erstellen** weitere Details ein.
21. Klicken Sie auf **OK** und **Schließen**.

Informationen zur Citrix ADC GUI-Konfiguration für den Lastenausgleich und das Replizieren des Datenverkehrs auf IDS-Geräte finden Sie unter Load Balancing.



Informationen zur Citrix ADC GUI-Konfiguration für den Lastenausgleich und das Weiterleiten des Datenverkehrs nach der Inhaltstransformation an den Back-End-Ursprungsserver finden Sie unter Thema Load Balancing .

Integration von Citrix ADC Layer 3 mit passiven Sicherheitsgeräten (Intrusion Detection System)

October 5, 2021

Eine Citrix ADC Appliance ist jetzt mit passiven Sicherheitsgeräten wie dem Intrusion Detection System

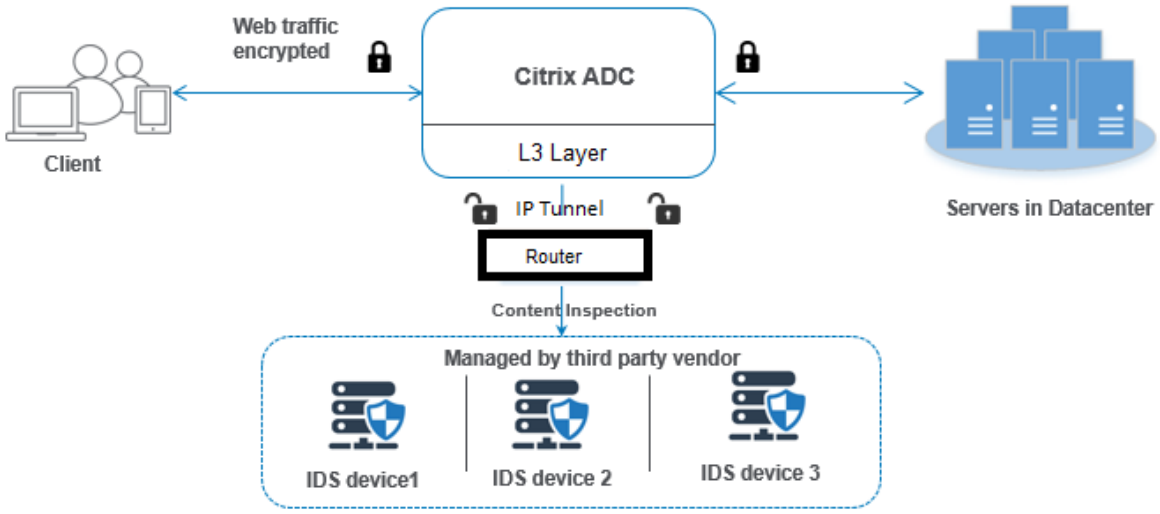
(IDS) integriert. In diesem Setup sendet die Appliance eine Kopie des ursprünglichen Datenverkehrs sicher an entfernte IDS-Geräte. Diese passiven Geräte speichern Protokolle und lösen Warnungen aus, wenn ein schlechter oder nicht konformer Datenverkehr erkannt wird. Es erstellt auch Berichte für den Compliance-Zweck. Wenn eine Citrix ADC Appliance in zwei oder mehr IDS-Geräte integriert ist und bei hohem Datenverkehr ein hohes Verkehrsaufkommen besteht, kann die Appliance die Geräte ausgleichen, indem sie Datenverkehr auf der Ebene des virtuellen Servers klont.

Für erweiterten Sicherheitsschutz ist eine Citrix ADC-Appliance mit passiven Sicherheitsgeräten wie IDS integriert, die im Nur-Erkennungsmodus bereitgestellt werden. Diese Geräte speichern Protokolle und lösen Warnungen aus, wenn ein schlechter oder nicht konformer Datenverkehr angezeigt wird. Es erstellt auch Berichte für den Compliance-Zweck. Im Folgenden sind einige der Vorteile der Integration des Citrix ADC mit einem IDS-Gerät aufgeführt.

- **Verschlüsselten Datenverkehr wird überprüft**. Die meisten Sicherheitsgeräte umgehen verschlüsselten Datenverkehr, wodurch Server anfällig für Angriffe bleiben. Eine Citrix ADC Appliance kann Datenverkehr entschlüsseln und an IDS-Geräte senden, um die Netzwerksicherheit des Kunden zu verbessern.
- **Entladen von Inline-Geräten aus der TLS/SSL-Verarbeitung**. TLS/SSL-Verarbeitung ist teuer und führt zu einer hohen System-CPU in Intrusion Detection Geräten, wenn sie den Datenverkehr entschlüsseln. Da der verschlüsselte Datenverkehr in einem rasanten Tempo wächst, können diese Systeme verschlüsselten Datenverkehr nicht entschlüsseln und untersuchen. Citrix ADC hilft beim Verschieben von Datenverkehr auf IDS-Geräte aus der TLS/SSL-Verarbeitung. Diese Art des Abladens von Daten führt dazu, dass ein IDS-Gerät ein hohes Volumen an Verkehrsinspektion unterstützt.
- **Laden von ausgleichenden IDS-Geräten**. Die Citrix ADC Appliance gleicht mehrere IDS-Geräte aus, wenn ein hohes Datenvolumen besteht, indem Datenverkehr auf der Ebene des virtuellen Servers geklont wird.
- **Datenverkehr auf passive Geräte replizieren**. Der Datenverkehr, der in die Appliance fließt, kann zur Erstellung von Compliance-Berichten auf andere passive Geräte repliziert werden. Zum Beispiel, nur wenige Behörden beauftragen jede Transaktion, in einigen passiven Geräten protokolliert zu werden.
- **Fanning des Datenverkehrs an mehrere passive Geräte**. Einige Kunden bevorzugen es, eingehenden Datenverkehr auf mehrere passive Geräte zu übertragen oder zu replizieren.
- **Intelligente Auswahl des Datenverkehrs**. Jedes Paket, das in die Appliance fließt, muss möglicherweise nicht inhaltlich geprüft werden, zum Beispiel das Herunterladen von Textdateien. Benutzer können die Citrix ADC Appliance so konfigurieren, dass sie bestimmten Datenverkehr (z. B. EXE-Dateien) zur Überprüfung auswählen und den Datenverkehr an IDS-Geräte zur Datenverarbeitung senden.

Integration von Citrix ADC in IDS-Gerät mit L3-Konnektivität

Das folgende Diagramm zeigt, wie die IDS in eine Citrix ADC Appliance integriert ist.



Die Komponenteninteraktion wird wie folgt angegeben:

1. Ein Client sendet eine HTTP/HTTPS-Anfrage an die Citrix ADC Appliance.
2. Die Appliance fängt den Datenverkehr ab und sendet die Daten an entfernte IDS-Geräte über verschiedene Rechenzentren oder sogar in einer Cloud. Diese Integration erfolgt über IP tunneled Layer 3. Weitere Informationen zum IP-Tunneling in einer Citrix ADC Appliance finden Sie unter IP-Tunnel Thema.
3. Wenn der Datenverkehr verschlüsselt ist, entschlüsselt die Appliance die Daten und sendet sie als Nur-Text.
4. Basierend auf der Richtlinienbewertung wendet die Appliance eine Inhaltsprüfung vom Typ MIRROR an.
5. Für die Aktion ist ein IDS-Dienst oder Lastausgleichsdienst (für mehrere IDS-Geräteintegrationen) darin konfiguriert.
6. Das IDS-Gerät ist auf der Appliance als Content-Inspection-Diensttyp Beliebig konfiguriert. Der Content Inspection Service wird dann dem Inhaltsinspektionsprofil vom Typ “MIRROR” und dem Tunnelparameter zugeordnet, der die getunnelte IP-Schicht-3-Schnittstelle angibt, über die die Daten an das IDS-Gerät weitergeleitet werden.

> **Hinweis** Optional können Sie auch ein VLAN-Tag im Content Inspection Profil konfigurieren.

1. Wenn der Back-End-Server eine Antwort an den Citrix ADC sendet, repliziert die Appliance die Daten und leitet sie an das IDS-Gerät weiter.
2. Wenn Ihre Appliance in ein oder mehrere IDS-Geräte integriert ist und Sie den Lastausgleich der Geräte bevorzugen, können Sie den virtuellen Lastausgleichsserver verwenden.

Softwarelizenzierung

Um die IDS-Integration bereitstellen zu können, muss Ihre Citrix ADC Appliance mit einer der folgenden Lizenzen bereitgestellt werden:

1. ADC Premium
2. ADC Advanced

Konfigurieren der Systemintegration von Intrusion Detection

Sie können IDS Device auf zwei verschiedene Arten in einen Citrix ADC integrieren.

Szenario 1: Integration mit einem einzelnen IDS-Gerät

Im Folgenden sind die Schritte, die Sie über die Befehlszeilenschnittstelle konfigurieren müssen.

1. Inhaltsüberprüfung aktivieren
2. Fügen Sie das Content-Inspektionsprofil vom Typ MIRROR für den Dienst hinzu, der IDS-Gerät darstellt.
3. Add IDS service of type “ANY”
4. Inhaltsprüfung vom Typ MIRROR hinzufügen
5. Richtlinie zur Inhaltsüberprüfung für IDS-Inspektion hinzufügen
6. Binden Sie die Inhaltsüberprüfungsrichtlinie an Content Switching oder den virtuellen Lastenausgleichsdienst vom Typ HTTP/SSL

Inhaltsprüfung aktivieren

Wenn Sie möchten, dass die Citrix ADC Appliance den Inhalt zur Überprüfung an die IDS-Geräte sendet, müssen Sie die Funktionen zur Inhaltsüberwachung und zum Lastenausgleich unabhängig von der Durchführung der Entschlüsselung aktivieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns feature contentInspection LoadBalancing
```

Content-Inspektionsprofil vom Typ MIRROR hinzufügen

Das Content-Inspection-Profil vom Typ MIRROR erklärt, wie Sie eine Verbindung mit dem IDS-Gerät herstellen können.
Geben Sie an der Eingabeaufforderung ein.

> **Hinweis**

> Der IP-Tunnel-Parameter darf nur für die IDS der Schicht 3 verwendet werden. Andernfalls müssen Sie die Egress-Schnittstelle mit der Option Egress VLAN verwenden.

```
add contentInspection profile <name> -type MIRROR -ipTunnel <iptunnel_name>
```

Beispiel:

```
add contentInspection profile IDS_profile1 -type MIRROR -ipTunnel ipsect-
tunnel1
```

IDS-Dienst hinzufügen

Sie müssen für jedes IDS-Gerät, das in die Appliance integriert ist, einen Dienst vom Typ ANY konfigurieren. Der Dienst enthält die IDS-Gerätekonfigurationsdetails. Der Dienst stellt das IDS-Gerät dar.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <Service_name> <IP> ANY <Port> - contentinspectionProfileName <
Name> -healthMonitor OFF -usip ON -useproxyport OFF
```

Beispiel:

```
add service IDS_service 1.1.1.1 ANY 8080 -contentInspectionProfileName
IDS_profile1 -healthMonitor OFF
```

Inhaltsprüfung vom Typ MIRROR für IDS-Dienst hinzufügen

Nachdem Sie die Inhaltsinspektion aktiviert und dann das IDS-Profil und den Dienst hinzugefügt haben, müssen Sie die Inhaltsprüfung Aktion für die Verarbeitung der Anforderung hinzufügen. Basierend auf der Inhaltsüberprüfungsaktion kann die Appliance Daten an das IDS -Gerät löschen, zurücksetzen, blockieren oder senden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ContentInspection action < action_name > -type MIRROR -serverName
Service_name/Vserver_name>
```

Beispiel:

```
add ContentInspection action IDS_action -type MIRROR -serverName IDS_service
```

Richtlinie zur Inhaltsüberprüfung für IDS-Inspektion hinzufügen

Nachdem Sie eine Inhaltsprüfungsaktion erstellt haben, müssen Sie Inhaltsprüfungsrichtlinien hinzufügen, um Prüfungsanforderungen auszuwerten. Die Richtlinie basiert auf einer Regel, die aus einem oder mehreren Ausdrücken besteht. Die Richtlinie bewertet und wählt den Datenverkehr für die Inspektion basierend auf der Regel aus.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection policy < policy_name > -rule <Rule> -action <action_name
>
```

Beispiel:

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Binden Sie die Inhaltsüberprüfungsrichtlinie an Content Switching oder den virtuellen Lastenausgleichsdienst vom Typ HTTP/SSL

Um den Webdatenverkehr zu empfangen, müssen Sie einen virtuellen Lastausgleichsserver hinzufügen.
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <vserver name>
```

Beispiel:

```
add lb vserver HTTP_vserver HTTP 1.1.1.3 8080
```

Content Inspection Policy an virtuellen Content Switching- oder Load Balancing-Server vom Typ HTTP/SSL binden

Sie müssen den virtuellen Lastausgleichsserver oder den virtuellen Content Switching-Server vom Typ HTTP/SSL an die Inhaltsinspektionsrichtlinie binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

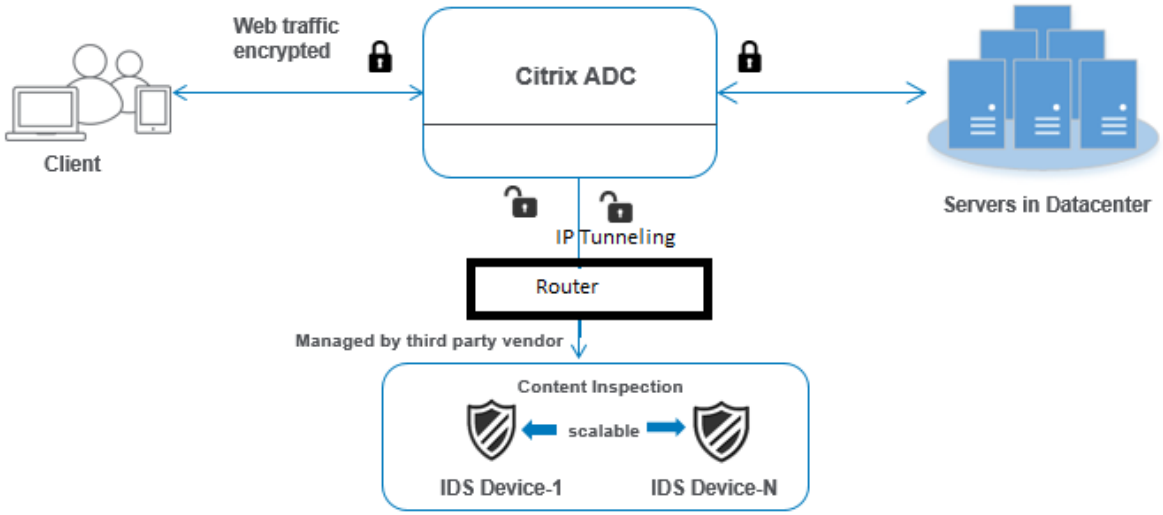
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <
priority > -type <REQUEST>
```

Beispiel:

```
bind lb vserver HTTP_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

Szenario 2: Lastenausgleich mehrerer IDS-Geräte

Wenn Sie zwei oder mehr IDS-Geräte verwenden, müssen Sie den Lastausgleich der IDS-Geräte über verschiedene Content-Inspektionsdienste verwenden. In diesem Fall gleicht das Lastenausgleich der Citrix ADC Appliance die Geräte zusätzlich zum Senden einer Teilmenge des Datenverkehrs an jedes Gerät aus.
Grundlegende Konfigurationsschritte finden Sie unter Szenario 1.



Im Folgenden sind die Schritte, die Sie über die Befehlszeilenschnittstelle konfigurieren müssen.

1. Inhaltsinspektionsprofil 1 vom Typ MIRROR für IDS Service 1 hinzufügen
2. Hinzufügen des Content-Inspektionsprofils 2 vom Typ MIRROR für IDS Service 2
3. Add IDS service 1 of type ANY for IDS device 1
4. Add IDS service 2 of type ANY for IDS device 2
5. Hinzufügen eines virtuellen Lastausgleichsservers vom Typ ANY
6. IDS-Dienst 1 zum Lastenausgleich eines virtuellen Servers binden
7. IDS-Dienst 2 zum Lastenausgleich eines virtuellen Servers binden
8. Hinzufügen von Inhaltsprüfungsaktion für den Lastausgleich von IDS-Geräten.
9. Inhaltsüberprüfungsrichtlinie für die Inspektion hinzufügen
10. Hinzufügen von virtuellem Content Switching- oder Lastausgleichsserver vom Typ HTTP/SSL
11. Richtlinie zur Inhaltsüberprüfung zum Lastenausgleich virtueller Server vom Typ HTTP/SSL binden

Inhaltsinspektionsprofil 1 vom Typ MIRROR für IDS Service 1 hinzufügen

Die IDS Konfiguration kann in einer Entität namens Content Inspection Profile angegeben werden. Das Profil verfügt über eine Sammlung von Geräteeinstellungen. Das Content-Inspection-Profile1 wird für den IDS-Dienst 1 erstellt.

> **Hinweis**: Der
> IP-Tunnelparameter darf nur für Layer 3 IDS-Topologie verwendet werden. Andernfalls müssen Sie die Egress-Schnittstelle mit der Option Egress VLAN verwenden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection profile <name> -type ANY - ipTunnel <iptunnel_name>
```


Beispiel:

```
add contentInspection profile IDS_profile1 -type MIRROR - ipTunnel ipsect_tunnel1
```

Inhaltsinspektionsprofil 2 für Typ MIRROR für IDS Service 2 hinzufügen

Das Content Inspection Profile 2 wird für Service 2 hinzugefügt, und das Inline-Gerät kommuniziert über die Egress-1/1-Schnittstelle mit der Appliance.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection profile <name> -type ANY - ipTunnel <iptunnel_name>
```

Beispiel:

```
add contentInspection profile IDS_profile2 -type ANY - ipTunnel ipsect_tunnel2
```

Add IDS service 1 of type ANY for IDS device 1

Nachdem Sie die Inhaltsinspektion aktiviert und das Inline-Profil hinzugefügt haben, müssen Sie einen Inline-Dienst 1 für Inline-Gerät 1 hinzufügen, um Teil des Lastausgleichs zu sein. Der Dienst, den Sie hinzufügen, enthält alle Inline-Konfigurationsdetails.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <Service_name_1> <Pvt_IP1> ANY <Port> -contentInspectionProfileName
 <IDS_Profile_1> -usip ON -useproxyport OFF
```

Beispiel:

```
add service IDS_service1 1.1.1.1 ANY 80 -contentInspectionProfileName
IDS_profile1 -usip ON -useproxyport OFF
```

> **Hinweis**:
>
> Die im Beispiel erwähnte IP-Adresse ist eine Dummy-Adresse.

Add IDS service 2 of type ANY for IDS device 2

Nachdem Sie die Inhaltsinspektion aktiviert und das Inline-Profil hinzugefügt haben, müssen Sie einen Inline-Dienst 2 für Inline-Gerät 2 hinzufügen. Der Dienst, den Sie hinzufügen, enthält alle Inline-Konfigurationsdetails.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <Service_name_1> <Pvt_IP1> ANY -contentInspectionProfileName <
Inline_Profile_2> -healthmonitor OFF -usip ON -useproxyport OFF
```


Beispiel:

```
add service IDS_service 1 1.1.2 ANY 80 -contentInspectionProfileName
IDS_profile2
```

> **Hinweis**:
>
> Die im Beispiel erwähnte IP-Adresse ist eine Dummy-Adresse.

Hinzufügen eines virtuellen Lastausgleichsservers

Nachdem Sie das Inline-Profil und die Dienste hinzugefügt haben, müssen Sie einen virtuellen Lastausgleichsserver für den Lastenausgleich der Dienste hinzufügen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <vserver_name> ANY <Pvt_IP3> <port>
```

Beispiel:

```
add lb vserver lb-IDS_vserver ANY 1.1.1.2
```

IDS-Dienst 1 zum Lastenausgleich eines virtuellen Servers binden

Nachdem Sie den virtuellen Lastausgleichsserver hinzugefügt haben, binden Sie nun den virtuellen Lastausgleichsserver an den ersten Dienst.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Beispiel:

```
bind lb vserver lb-IDS_vserver IDS_service1
```

IDS-Dienst 2 zum Lastenausgleich eines virtuellen Servers binden

Nachdem Sie den virtuellen Lastausgleichsserver hinzugefügt haben, binden Sie den Server nun an den zweiten Dienst.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <Vserver_name> <Service_name_1>
```

Beispiel:

```
bind lb vserver lb-IDS_vserver IDS_service2
```


Hinzufügen von Inhaltsüberprüfungsaktion für den IDS-Dienst

Nachdem Sie die Funktion Inhaltsüberprüfung aktiviert haben, müssen Sie die Aktion Inhaltsüberprüfung für die Verarbeitung der Inline-Anforderungsinformationen hinzufügen. Basierend auf der ausgewählten Aktion lässt die Appliance den Datenverkehr senkt, zurücksetzt, blockiert oder sendet ihn an das IDS-Gerät.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection action <name> -type <type> (-serverName <string> [-
ifserverdown <ifserverdown>]
```

Beispiel:

```
add ContentInspection action IDS_action -type MIRROR -serverName lb-IDS_vserver
```

Inhaltsüberprüfungsrichtlinie für die Inspektion hinzufügen

Nachdem Sie eine Aktion zur Inhaltsüberwachung erstellt haben, müssen Sie die Inhaltsinspektionsrichtlinie hinzufügen, um Serviceanfragen zu bewerten.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add contentInspection policy <policy_name> -rule <Rule> -action <action_name
>
```

Beispiel:

```
add contentInspection policy IDS_pol1 -rule true -action IDS_action
```

Hinzufügen von virtuellem Content Switching- oder Lastausgleichsserver vom Typ HTTP/SSL

Fügen Sie einen virtuellen Content Switching-Server oder zum Lastenausgleich hinzu, um Webdatenverkehr zu akzeptieren. Außerdem müssen Sie die Layer2-Verbindung auf dem virtuellen Server aktivieren.

Weitere Informationen zum Lastenausgleich finden Sie unter Funktionsweise des Lastenausgleichs .

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <vserver name>
```

Beispiel:

```
add lb vserver http_vserver HTTP 1.1.1.1 8080
```


Bind Content Inspection Policy für den Lastenausgleich virtueller Server vom Typ HTTP/SSL

Sie müssen den virtuellen Content Switching- oder Lastausgleichsserver des Typs HTTP/SSL an die Inhaltsüberprüfungsrichtlinie binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

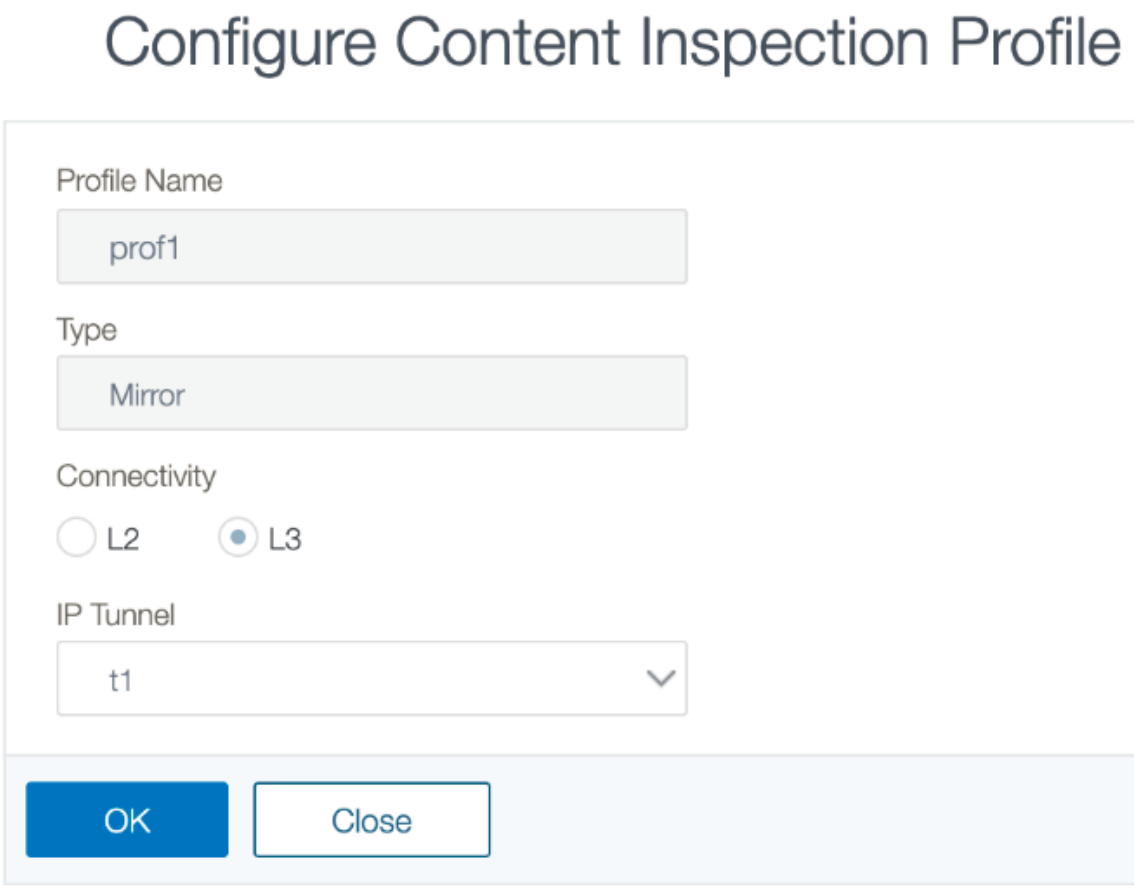
```
bind lb vserver <vserver name> -policyName < policy_name > -priority <> -
type <REQUEST>
```

Beispiel:

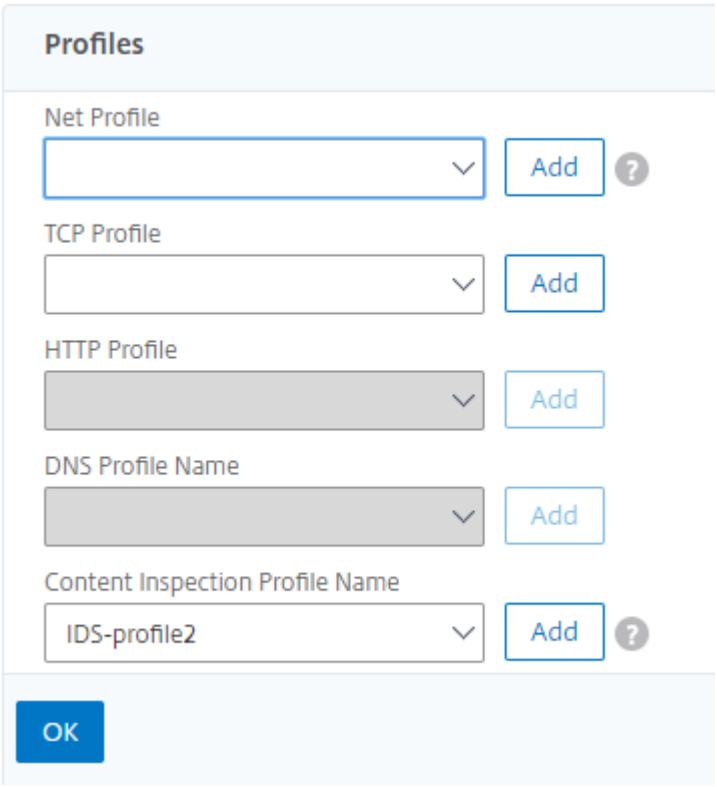
```
bind lb vserver http_vserver -policyName IDS_pol1 -priority 100 -type
REQUEST
```

Konfigurieren der Inline-Dienstintegration über die Citrix ADC GUI

1. Navigieren Sie zu **Sicherheit** > **Inhaltsinspektion** > **ContentInspection-Profile** .
2. Klicken Sie auf der Seite **ContentInspection-Profil** auf **Hinzufügen** .
3. **Legen Sie auf der Seite ContentInspectionProfile erstellen** die folgenden Parameter fest.
   a) Profilname Name des Content-Inspektionsprofils für IDS.
   b) Geben Sie ein. Wählen Sie die Profiltypen als MIRROR aus.
   c) Konnektivität. Layer-2- oder Layer-3-Schnittstelle.
   d) IP-Tunnel. Wählen Sie den Netzwerkkommunikationskanal zwischen den beiden Netzwerken aus.
4. Klicken Sie auf **Erstellen**.



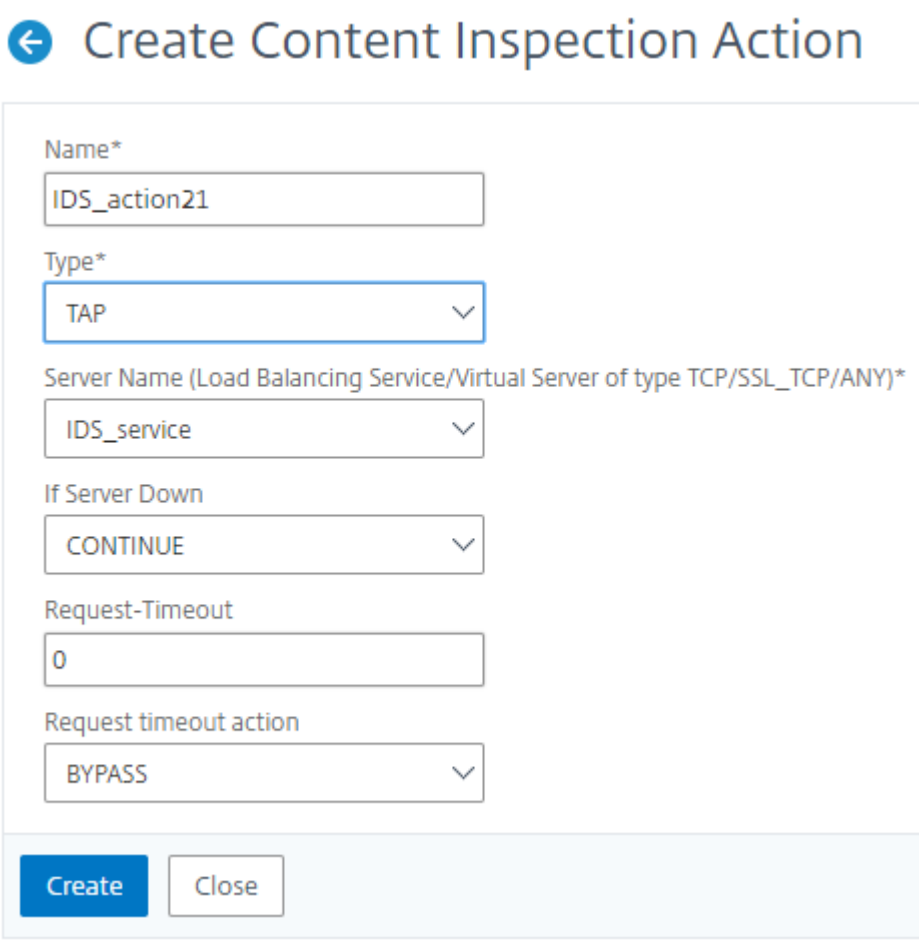
5. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**, und klicken Sie auf **Hinzufügen**.
6. Geben Sie auf der Seite **Load Balancing Service** die Details des Content-Inspektionsdienstes ein.
7. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Profile**.
8. Gehen Sie zum Abschnitt **Profile** und klicken Sie auf das **Bleistiftsymbol**, um das Content-Inspektionsprofil hinzuzufügen.
9. Klicken Sie auf **OK**.



10. Navigieren Sie zu **Lastenausgleich** > **Server** . Fügen Sie einen virtuellen Server vom Typ HTTP oder SSL hinzu.
11. Nachdem Sie die Serverdetails eingegeben haben, klicken Sie auf **OK** und erneut auf **OK**.
12. Klicken Sie im Abschnitt **Erweiterte Einstellungen** auf **Richtlinien**.
13. Gehen Sie in den Abschnitt **Richtlinien** und klicken Sie auf das **Bleistift-Symbol**, um die Richtlinie zur Inhaltsüberprüfung zu konfigurieren
14. Wählen Sie auf der Seite **Richtlinie auswählen** die Option **Inhaltsübersicht** aus. Klicken Sie auf **Weiter**.
15. Klicken Sie im Abschnitt **Richtlinienbindung** auf +, um eine Richtlinie zur Inhaltsüberwachung hinzuzufügen.
16. Geben **Sie auf der Seite CI-Richtlinie erstellen** einen Namen für die Inline-Inhaltsüberprüfungsrichtlinie ein.
17. Klicken Sie im Feld **Aktion** auf das Zeichen +, um eine IDS-Inhaltsprüfung vom Typ MIRROR zu erstellen.
18. **Legen Sie auf der Seite CI-Aktion erstellen** die folgenden Parameter fest.
    a) Name. Name der Inhaltsüberprüfung Inline-Richtlinie.
    b) Geben Sie ein. Wählen Sie den Typ als MIRROR aus.

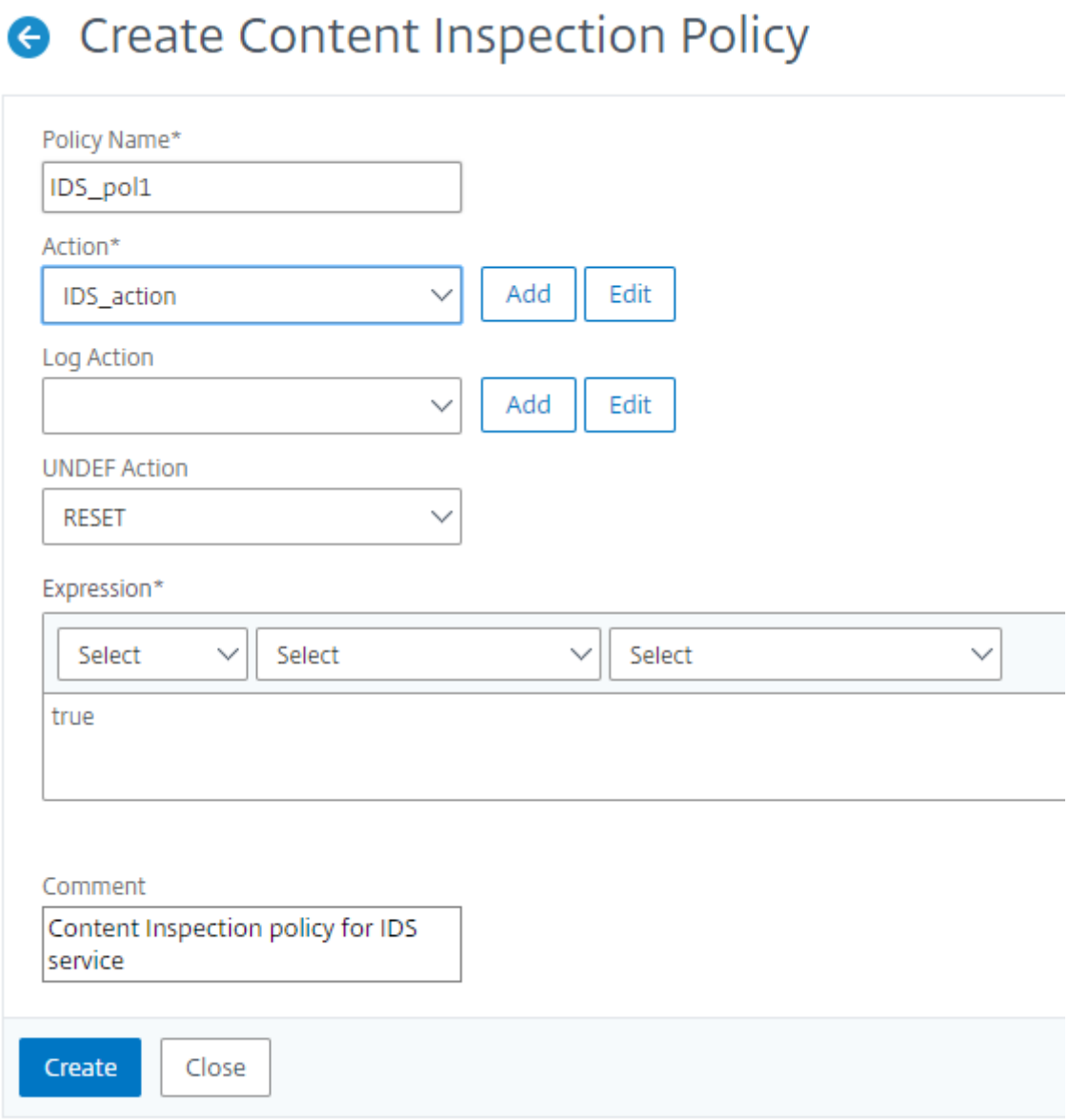
c) Servername: Wählen Sie den Server-/Dienstnamen als Inline-Geräte aus.
d) Wenn Server heruntergefahren ist. Wählen Sie einen Vorgang aus, wenn der Server ausfällt.
e) Zeitüberschreitung der Anforderung. Wählen Sie einen Zeitüberschreitungswert aus. Standardwerte können verwendet werden.
f) Zeitüberschreitungsaktion anfordern. Wählen Sie eine Zeitüberschreitungsaktion aus. Standardwerte können verwendet werden.

19. Klicken Sie auf **Erstellen**.



20. Geben **Sie auf der Seite CI-Richtlinie erstellen** weitere Details ein.
21. Klicken Sie auf **OK** und **schließen**.

Informationen zur Citrix ADC GUI-Konfiguration für den Lastenausgleich und das Replizieren des Datenverkehrs auf IDS-Geräte finden Sie unter Load Balancing.



Informationen zur Citrix ADC GUI-Konfiguration für den Lastenausgleich und Weiterleiten des Datenverkehrs an den Back-End-Ursprungsserver nach der Content-Transformation finden Sie unter Load Balancing.

Statistiken zur Inhaltsprüfung für ICAP, IPS und IDS

October 5, 2021

Die Statistiken zur Inhaltsinspektion für ICAP, Inline-Geräteintegration (IDS) und Intrusion Prevention System (IPS) sind eine detaillierte Ausgabe (Zusammenfassung) der Details zu Anfragen, Antworten und Serveraktionen.

Die Statistiken zur Inhaltsinspektion sind eine Sammlung statistischer Daten, die die zur Inhaltsüberprüfung gesendete HTTP/HTTPS-Anfrage enthält. HTTP-/HTTPS-Antwort von IPS-, IDS- und ICAP-Geräten sowie Back-End-Serveraktionen.

So zeigen Sie Statistiken zur Inhaltsüberwachung mit der CLI an:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
stat contentInspection
```

```
ContentInspection Stats

Inline Statistics
                                    Total
Requests                             10
Responses                             6
Request Bytes Sent                   3235
Request Bytes Received               2977
Response Bytes Sent                  17302
Response Bytes Received              19681
Serverdown Reset Action taken         1
Serverdown Drop Action taken          0
Serverdown BYPASS Action taken        0
Inline device Generated Response      3

Mirror Statistics
                                    Total
Requests                             4
Responses                            4
Requests Bytes Sent                 2763
Responses Bytes Sent                16732
Serverdown Reset Action taken        0
Serverdown Drop Action taken         0
Serverdown BYPASS Action taken       1

ICAP Statistics
                                    Total
REQMOD requests Sent                   6
RESPMOD requests Sent                  4
Preview requests                       1
204 Responses Received                 6
100 Continue Responses Received        1
204 NO content Received                5
Adaptive Requests                      0
Adaptive Responses                     4
```



```
Callout requests Initiated          1
Callout requests completed          1
ICAP Req/Resp Errors handled        1
Serverdown Reset Action taken       1
Serverdown Drop Action taken        0
Serverdown BYPASS Action taken      1

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

SSL-Forward-Proxy

October 5, 2021

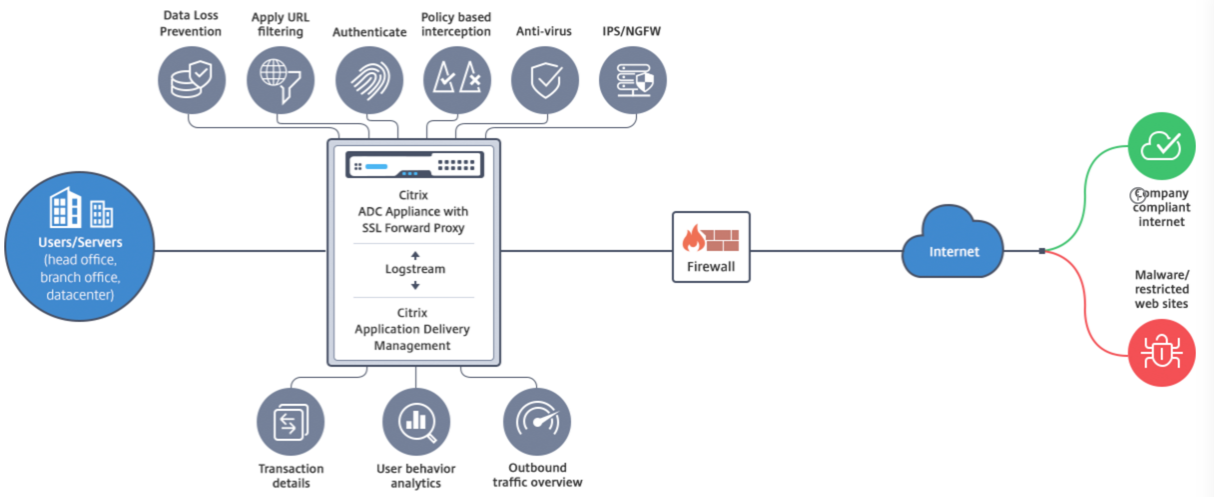
Hinweis: Die SSL-Forward-Proxy-Funktion ist mit der ADC Premium-Lizenz verfügbar.

Der Webverkehr hat in den letzten Jahren exponentiell zugenommen, und Unternehmen verlassen sich zunehmend auf das Internet für ihren täglichen Betrieb. Dies, kombiniert mit der Entstehung von vielfältigeren Endpunkten, Mobilität und BYOD, zusammen mit einer wachsenden Angreiferbasis, macht Benutzern einfache Ziele moderner Malware. Sie sind zunehmend anfällig für Identitätsdiebstahl und ihre Daten gefährden. Traditionell haben Unternehmen den HTTP-Datenverkehr auf Malware und Viren überprüft. Sie haben HTTPS/TLS -Verkehr umgangen, weil es nicht so prominent war. Es wurde sparsam für Inhalte verwendet, die sensibel und vertrauenswürdig waren. Aber das hat sich schnell geändert, da die meisten öffentlichen Internetseiten jetzt lieber HTTPS verwenden, um die Privatsphäre der Nutzer zu schützen. Infolgedessen ermöglicht die Unmöglichkeit, verschlüsselte Pakete zu überprüfen, Malware oder Eindringlinge in das Unternehmensnetzwerk. Die SSL-Forward-Proxy-Lösung bietet Tools, mit denen Unternehmen vor Internet-Bedrohungen schützen können.

Ein Proxy ist ein Server, der den gesamten Datenverkehr zwischen Benutzern und dem Internet oder SaaS-Anwendungen steuert. Da der gesamte Datenverkehr diesen Proxy durchläuft, führt er sicherheitsbezogene Funktionen wie Benutzerauthentifizierung und URL-Kategorisierung aus.

Die folgende Abbildung gibt einen Überblick über die SSL Forward-Proxy-Implementierung. Der Datenverkehr fließt über das Unternehmensnetzwerk von der Zentrale, Zweigstellen, Rechenzentren und Remote-Mitarbeitern aus. Eine Citrix ADC-Appliance am Rande des Netzwerks fungiert als Proxy. Die Appliance kann im transparenten Proxy-Modus oder im expliziten Proxymodus betrieben werden und bietet Steuerelemente zum Abfangen des Internetverkehrs, einschließlich HTTPS. Auf der Appliance konfigurierte Richtlinien bestimmen, ob eine bestimmte Anforderung abfängt, umgeht oder blockiert wird. Der Zugriff auf eingeschränkte Websites kann mithilfe von URL-Filtern blockiert werden. Ein Benutzer wird authentifiziert, bevor er sich am Unternehmensnetzwerk anmeldet. Alle Anfragen und Antworten werden markiert, um den Benutzer zu identifizieren, und der Zugriff auf

die Internet-Site wird kategorisiert. Benutzeraktivitäten werden protokolliert und zum Generieren von Berichten verwendet. Wenn ein Verstoß auftritt, können Administratoren das infizierte System isolieren, feststellen, ob die Geräte anderer Benutzer, die diese Website besucht haben, gefährdet sind, und geeignete Maßnahmen ergreifen. Wenn Sie Citrix Application Delivery Management (ADM) in SSL-Forward-Proxy integrieren, werden die protokollierten Benutzeraktivitäten und die nachfolgenden Datensätze in der Appliance mithilfe von Citrix ADM exportiert `logstream`. Citrix ADM stellt Informationen über die Aktivitäten der Nutzer zusammen, von besuchten Websites bis hin zu der online verbrachten Zeit. Außerdem werden Informationen über die Bandbreitennutzung und erkannte Bedrohungen wie Malware und Phishing-Sites bereitgestellt. Sie können diese wichtigen Metriken verwenden, um Ihr Netzwerk zu überwachen, und die SSL-Forward-Proxy-Funktion verwenden, um Korrekturmaßnahmen zu ergreifen.



SSL-Forward-Proxy ermöglicht IT-Direktoren Folgendes:

- Erhalten Sie Einblick in den sonst umgangenen sicheren Datenverkehr.
- Blockieren Sie den Zugriff auf bösartige oder unbekannte Websites und vermeiden Sie, dass Benutzer innerhalb des Unternehmens infiziert werden.
- Steuern Sie den Zugriff auf bestimmte Websites, z. B. persönliche E-Mails, soziale Netzwerke und Websites für die Jobsuche, über das Unternehmensnetzwerk.
- Wenden Sie intelligente Content-Control-Richtlinien an, um maximale Benutzerproduktivität zu gewährleisten.

Erste Schritte mit der SSL Forward-Proxy-Funktion

October 5, 2021

Wichtig:

- OCSP-Prüfung erfordert eine Internetverbindung, um die Gültigkeit von Zertifikaten zu überprüfen. Wenn die Appliance über die NSIP-Adresse nicht über das Internet zugegriffen werden kann, fügen Sie Zugriffssteuerungslisten (ACLs) hinzu, um NAT von der NSIP-Adresse zur Subnetz-IP-Adresse (SNIP) auszuführen. Der SNIP muss auf das Internet zugreifen können. Zum Beispiel:

```
add ns acl a1 ALLOW -srcIP = <NSIP> -destIP  “!=”
    10.0.0.0-10.255.255.255

add rnat RNAT-1 a1

bind rnat RNAT-1 -<SNIP>

apply acls
<!--NeedCopy-->
```

- Geben Sie einen DNS-Namensserver an, um Domänennamen aufzulösen.
- Stellen Sie sicher, dass das Datum auf der Appliance mit den NTP-Servern synchronisiert ist. Wenn das Datum nicht synchronisiert wird, kann die Appliance nicht effektiv überprüfen, ob es sich bei einem Ursprungsserverzertifikat um ein abgelaufenes Zertifikat handelt.

Um das SSL-Forward-Proxy-Feature zu verwenden, müssen Sie die folgenden Aufgaben ausführen:

- Fügen Sie einen Proxyserver im expliziten oder transparenten Modus hinzu.
- Aktivieren Sie SSL-Interception.
  - Konfigurieren Sie ein SSL-Profil.
  - Fügen Sie SSL-Richtlinien hinzu und binden Sie sie an den Proxyserver.
  - Fügen Sie ein Zertifizierungsstellen-Zertifikatschlüsselpaar für SSL-Interception hinzu und binden Sie sie.

Hinweis:

Eine im transparenten Proxy-Modus konfigurierte ADC-Appliance kann nur HTTP- und HTTPS-Protokolle abfangen. Um andere Protokolle wie Telnet zu umgehen, müssen Sie die folgende Abhörrichtlinie auf dem virtuellen Proxyserver hinzufügen.

Der virtuelle Server akzeptiert jetzt nur den eingehenden HTTP- und HTTPS-Datenverkehr.

```
set cs vserver transparent-pxy1 PROXY * * -cltTimeout 180 -Listenpolicy
    ”CLIENT.TCP.DSTPORT.EQ(80) || CLIENT.TCP.DSTPORT.EQ(443)”`
<!--NeedCopy-->
```


Je nach Bereitstellung müssen Sie möglicherweise die folgenden Funktionen konfigurieren:

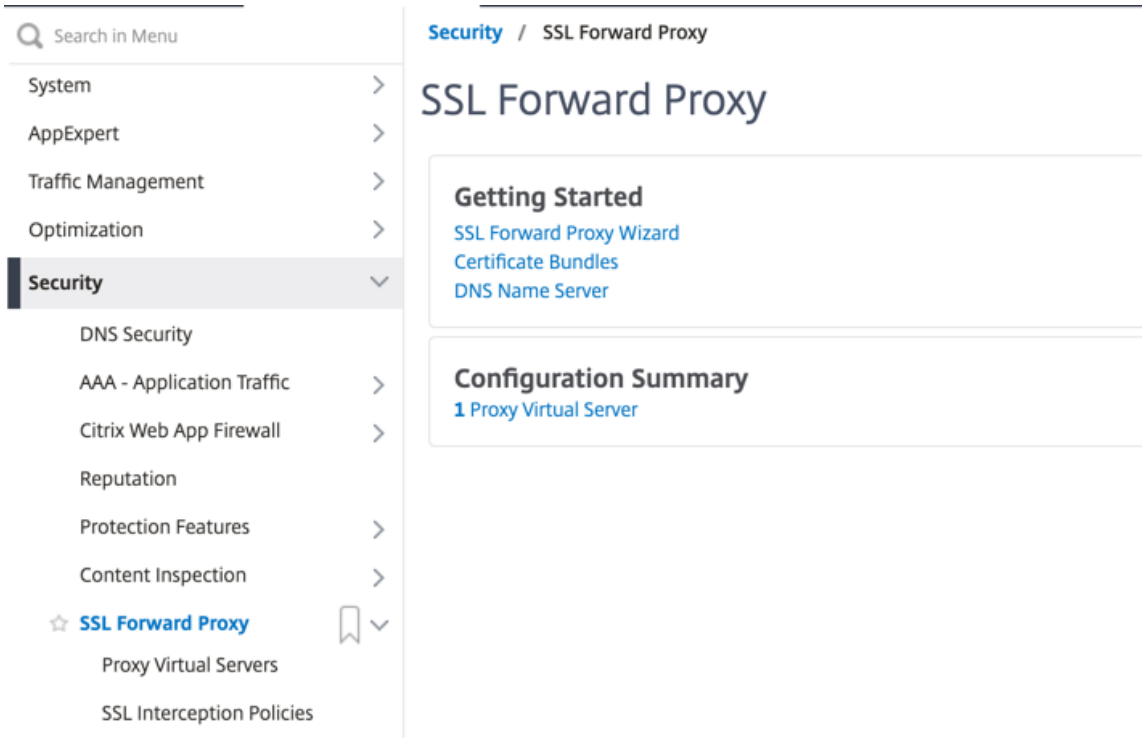
- Authentifizierungsdienst (empfohlen) — zur Authentifizierung von Benutzern. Ohne den Authentifizierungsdienst basiert die Benutzeraktivität auf der Client-IP-Adresse.
- URL-Filter — zum Filtern von URLs nach Kategorien, Reputationsbewertung und URL-Listen.
- Analytics: Zum Anzeigen von Benutzeraktivitäten, Benutzerrisikoindikatoren, Bandbreitenverbrauch und Transaktionen in Citrix Application Delivery Management (ADM).

Hinweis: SSL Forward Proxy implementiert die meisten typischen HTTP- und HTTPS-Standards, gefolgt von ähnlichen Produkten. Diese Implementierung wird ohne einen bestimmten Browser durchgeführt und ist mit den meisten gängigen Browsern kompatibel. SSL Forward Proxy wurde mit gängigen Browsern und aktuellen Versionen von Google Chrome, Internet Explorer und Mozilla Firefox getestet.

SSL-Weiterleitungs-Proxy-Assistent

Der SSL-Forward-Proxyassistent stellt Administratoren ein Tool zur Verfügung, mit dem die gesamte SSL-Forward-Proxybereitstellung mithilfe eines Webbrowsers verwaltet werden kann. Es hilft den Kunden dabei, einen SSL-Forward-Proxydienst schnell einzurichten, und vereinfacht die Konfiguration durch eine Reihe von klar definierten Schritten.

1. Navigieren Sie zu **Sicherheit > SSL Forward Proxy**. Klicken Sie unter **Erste Schritte** auf **SSL-Forward-Proxy-Assistent**.



2. Führen Sie die Schritte im Assistenten aus, um Ihre Bereitstellung zu konfigurieren.

Hinzufügen einer Listenrichtlinie zum transparenten Proxyserver

1. Navigieren Sie zu **Sicherheit > SSL-Forward-Proxy**> **Virtual Proxy Server**. Wählen Sie den transparenten Proxyserver aus, und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie die **Grundeinstellungen**, und klicken Sie auf **Mehr**.
3. Geben Sie unter **Listenpriorität** 1 ein.
4. Geben Sie unter **Listen-Richtlinienausdruck** den folgenden Ausdruck ein:

```
(CLIENT.TCP.DSTPORT.EQ(80)||CLIENT.TCP.DSTPORT.EQ(443))
<!--NeedCopy-->
```

Dieser Ausdruck setzt Standardports für HTTP- und HTTPS-Datenverkehr voraus. Wenn Sie verschiedene Ports konfiguriert haben, z. B. 8080 für HTTP oder 8443 für HTTPS, ändern Sie den Ausdruck so, dass er diese Ports widerspiegelt.

Einschränkungen

SSL-Forwardproxy wird in einem Cluster-Setup, in Adminpartitionen und auf einer Citrix ADC FIPS-Appliance nicht unterstützt.

Proxy-Modi

October 5, 2021

Die Citrix ADC Appliance fungiert als Client-Proxy für die Verbindung mit dem Internet und SaaS-Anwendungen. Als Proxy akzeptiert es den gesamten Datenverkehr und bestimmt das Protokoll des Datenverkehrs. Sofern der Datenverkehr nicht HTTP oder SSL ist, wird er so wie er ist an das Ziel weitergeleitet. Wenn die Appliance eine Anforderung von einem Client empfängt, fängt sie die Anforderung ab und führt einige Aktionen aus, z. B. Benutzerauthentifizierung, Sitekategorisierung und Umleitung. Es verwendet Richtlinien, um zu bestimmen, welcher Datenverkehr zugelassen und welcher Datenverkehr gesperrt werden soll.

Die Appliance verwaltet zwei verschiedene Sitzungen, eine zwischen dem Client und dem Proxy und die andere zwischen dem Proxy und dem Ursprungsserver. Der Proxy stützt sich auf kundendefinierte Richtlinien, um HTTP- und HTTPS-Datenverkehr zuzulassen oder zu blockieren. Daher ist es wichtig, dass Sie Richtlinien definieren, um vertrauliche Daten, z. B. Finanzinformationen, zu umgehen. Die Appliance bietet eine Reihe von Layer-4-zu-Layer-7-Datenverkehrsattributen und Benutzeridentitätsattributen zum Erstellen von Datenverkehrsmanagementrichtlinien.

Bei SSL-Datenverkehr überprüft der Proxy das Zertifikat des Ursprungsservers und stellt eine legitime Verbindung mit dem Server her. Anschließend emuliert es das Serverzertifikat, signiert es mit einem Zertifizierungsstellenzertifikat, das auf Citrix ADC installiert ist, und präsentiert dem Client das erstellte Serverzertifikat. Sie müssen das CA-Zertifikat als vertrauenswürdiges Zertifikat zum Browser des Clients hinzufügen, damit die SSL-Sitzung erfolgreich eingerichtet werden kann.

Die Appliance unterstützt transparente und explizite Proxy-Modi. Im expliziten Proxymodus muss der Client eine IP-Adresse in seinem Browser angeben, es sei denn, die Organisation verschiebt die Einstellung auf das Gerät des Clients. Diese Adresse ist die IP-Adresse eines Proxyservers, der auf der ADC-Appliance konfiguriert ist. Alle Client-Anfragen werden an diese IP-Adresse gesendet. Für einen expliziten Proxy müssen Sie einen virtuellen Content Switching-Server vom Typ PROXY konfigurieren und eine IP-Adresse und eine gültige Portnummer angeben.

Transparenter Proxy ist, wie der Name schon sagt, für den Client transparent. Das heißt, die Clients wissen möglicherweise nicht, dass ein Proxyserver ihre Anforderungen vermittelt. Die ADC-Appliance ist in einer Inline-Bereitstellung konfiguriert und akzeptiert transparent den gesamten HTTP- und HTTPS-Verkehr. Für transparenten Proxy müssen Sie einen virtuellen Content Switching-Server vom Typ PROXY mit Sternchen (* *) als IP-Adresse und Port konfigurieren. Wenn Sie den **SSL Forward Proxy Wizard** in der GUI verwenden, müssen Sie keine IP-Adresse und keinen Port angeben.

> **Hinweis:**
>
> Wenn Sie andere Protokolle als HTTP und HTTPS im transparenten Proxymodus abfangen möchten, müssen Sie eine Abhörrichtlinie hinzufügen und an den Proxyserver binden.

Konfigurieren des SSL-Forward-Proxy mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cs vserver <name> PROXY <ipaddress> <port>
<!--NeedCopy-->
```

Argumente:

Name:

Name für den Proxyserver. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Kann nicht geändert werden, nachdem der virtuelle CS Server erstellt wurde.

Die folgende Anforderung gilt nur für die CLI:

Wenn der Name ein oder mehrere Leerzeichen enthält, setzen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “mein Server” oder “mein Server”).

Dieses Argument ist obligatorisch. Maximale Länge: 127

IPAddress:

IP-Adresse des Proxyservers.

Port:

Portnummer für den Proxyserver Mindestwert: 1

Beispiel für expliziten Proxy:

```
add cs vserver swgVS PROXY 192.0.2.100 80
<!--NeedCopy-->
```

Beispiel für transparenten Proxy:

```
add cs vserver swgVS PROXY * *
<!--NeedCopy-->
```

Hinzufügen einer Listenrichtlinie zum transparenten Proxyserver mit der GUI

1. Navigieren Sie zu **Sicherheit** > **SSL Forward Proxy** > **Virtuelle Proxy-Server**. Wählen Sie den transparenten Proxyserver aus, und klicken Sie auf **Bearbeiten**.
2. Bearbeiten Sie die **Grundeinstellungen**, und klicken Sie auf **Mehr**.
3. Geben Sie unter **Listenpriorität** 1 ein.
4. Geben Sie unter **Listen-Richtlinienausdruck** den folgenden Ausdruck ein:

```
(CLIENT.TCP.DSTPORT.EQ(80)||CLIENT.TCP.DSTPORT.EQ(443))
<!--NeedCopy-->
```

> **Hinweis:**
>
> Dieser Ausdruck setzt Standardports für HTTP- und HTTPS-Datenverkehr voraus. Wenn Sie verschiedene Ports konfiguriert haben, z. B. 8080 für HTTP oder 8443 für HTTPS, ändern Sie den vorherigen Ausdruck, um diese Ports anzugeben.

SSL-Interception

October 5, 2021

Eine Citrix ADC Appliance, die für die SSL-Interception konfiguriert ist, fungiert als Proxy. Es kann SSL/TLS -Datenverkehr abfangen und entschlüsseln, die unverschlüsselte Anforderung überprüfen und einen Administrator ermöglichen, Compliance-Regeln und Sicherheitsprüfungen durchzusetzen. SSL-Interception verwendet eine Richtlinie, die angibt, welcher Datenverkehr abgefangen, blockiert oder zugelassen werden soll. Beispielsweise darf der Datenverkehr zu und von Finanzwebsites, wie Banken, nicht abgefangen werden, aber anderer Datenverkehr kann abgefangen werden, und Websites auf der Sperrliste können identifiziert und blockiert werden. Citrix empfiehlt, dass Sie eine allgemeine Richtlinie zum Abfangen des Datenverkehrs und spezifischere Richtlinien konfigurieren, um einen bestimmten Datenverkehr zu umgehen.

Der Client und der Proxy stellen einen HTTPS/TLS-Handshake her. Der Proxy erstellt einen weiteren HTTPS/TLS-Handshake mit dem Server und empfängt das Serverzertifikat. Der Proxy überprüft das Serverzertifikat im Namen des Clients und überprüft auch die Gültigkeit des Serverzertifikats mit dem Online Certificate Status Protocol (OCSP). Es generiert das Serverzertifikat neu, signiert es mit dem Schlüssel des auf der Appliance installierten Zertifizierungsstellenzertifikats und stellt es dem Client zur Verfügung. Daher wird ein Zertifikat zwischen dem Client und der Citrix ADC-Appliance und ein anderes Zertifikat zwischen der Appliance und dem Back-End-Server verwendet.

> **Wichtig**
>
> Das Zertifizierungsstellenzertifikat, das zum Signieren des Serverzertifikats verwendet wird, muss auf allen Clientgeräten vorinstalliert sein, damit das regenerierte Serverzertifikat vom Client als vertrauenswürdig eingestuft wird.

Bei abgefangenem HTTPS-Datenverkehr entschlüsselt der Proxyserver den ausgehenden Datenverkehr, greift auf die HTTP-Klartextanforderung zu und kann jede beliebige Layer-7-Anwendung verwenden, um den Datenverkehr zu verarbeiten, z. B. indem er die Nur-Text-URL durchsucht und den Zugriff basierend auf der Unternehmensrichtlinie und der URL-Reputation zulässt oder blockiert. Wenn die Richtlinienentscheidung den Zugriff auf den Ursprungsserver zulässt, leitet der Proxyserver die neu verschlüsselte Anforderung an den Zieldienst (auf dem Ursprungsserver) weiter. Der Proxy entschlüsselt die Antwort vom Ursprungsserver, greift auf die HTTP-Antwort im Klartext zu und wendet optional alle Richtlinien auf die Antwort an. Der Proxy verschlüsselt dann die Antwort erneut und leitet sie an den Client weiter. Wenn die Richtlinienentscheidung darin besteht, die Anforderung an den Ursprungsserver zu blockieren, kann der Proxy eine Fehlerantwort, z. B. HTTP 403, an den Client senden.

Um SSL-Interception durchzuführen, müssen Sie zusätzlich zum zuvor konfigurierten Proxyserver Folgendes auf der ADC-Appliance konfigurieren:

- SSL-Profil
- SSL-Richtlinie
- Zertifizierungsstellenzertifikatspeicher
- SSL-Fehler Autolearning und Caching

> **Hinweis:**
>
> HTTP/2-Verkehr wird von der SSL-Interception-Funktion nicht abgefangen.

Zertifikatspeicher für SSL-Interception

Ein SSL-Zertifikat, das Teil einer SSL-Transaktion ist, ist ein digitales Datenformular (X509), das ein Unternehmen (eine Domain) oder eine Person identifiziert. Ein SSL-Zertifikat wird von einer Zertifizierungsstelle ausgestellt. Eine Zertifizierungsstelle kann privat oder öffentlich sein. Zertifikate, die von öffentlichen Zertifizierungsstellen ausgestellt werden, wie z. B. Verisign, werden von Anwendungen, die SSL-Transaktionen durchführen, vertrauenswürdig. Diese Anwendungen verwalten eine Liste der Zertifizierungsstellen, denen sie vertrauen.

Als Forward-Proxy führt die ADC-Appliance die Verschlüsselung und Entschlüsselung des Datenverkehrs zwischen einem Client und einem Server durch. Es fungiert als Server für den Client (Benutzer) und als Client für den Server. Bevor eine Appliance HTTPS-Datenverkehr verarbeiten kann, muss sie die Identität eines Servers überprüfen, um betrügerische Transaktionen zu verhindern. Daher muss die Appliance als Client für den Ursprungsserver das Ursprungsserverzertifikat überprüfen, bevor sie es akzeptiert. Um ein Serverzertifikat zu überprüfen, müssen alle Zertifikate (z. B. Root- und Zwischenzertifikate), die zum Signieren und Ausstellen des Serverzertifikats verwendet werden, auf der Appliance vorhanden sein. Ein Standardsatz von Zertifizierungsstellenzertifikaten ist auf einer Appliance vorinstalliert. Die Appliance kann diese Zertifikate verwenden, um fast alle gängigen Ursprungs-Serverzertifikate zu überprüfen. Dieser Standardsatz kann nicht geändert werden. Wenn Ihre Bereitstellung jedoch mehr Zertifizierungsstellenzertifikate erfordert, können Sie ein Bündel solcher Zertifikate erstellen und das Paket in die Appliance importieren. Ein Bundle kann auch ein einzelnes Zertifikat enthalten.

Wenn Sie ein Zertifikatpaket in die Appliance importieren, lädt die Appliance das Paket vom Remotestandort herunter und installiert es nach der Überprüfung, ob das Paket nur Zertifikate enthält, auf der Appliance. Sie müssen ein Zertifikatpaket anwenden, bevor Sie es zum Überprüfen eines Serverzertifikats verwenden können. Sie können ein Zertifikatpaket auch exportieren, um es zu bearbeiten oder als Backup an einem Offline-Speicherort zu speichern.

Importieren und Anwenden eines CA-Zertifikatpakets auf der Appliance mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
import ssl certBundle <name> <src>
apply ssl certBundle <name>
<!--NeedCopy-->
```

```
show ssl certBundle
<!--NeedCopy-->
```

ARGUMENTS:

Name:

Name, der dem importierten Zertifikatspaket zugewiesen werden soll. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Die folgende Anforderung gilt nur für die CLI:

Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “meine Datei” oder ‘meine Datei’).

Maximale Länge: 31

src:

URL zur Angabe des Protokolls, des Hosts und des Pfads, einschließlich des Dateinamens, zum Zertifikatpaket, das importiert oder exportiert werden soll. Beispiel: `http://www.example.com/cert_bundle_file`.

HINWEIS: Der Import schlägt fehl, wenn sich das zu importierende Objekt auf einem HTTPS-Server befindet, der Clientzertifikatauthentifizierung für den Zugriff erfordert.

Maximale Länge: 2047

Beispiel:

```
import ssl certbundle swg-certbundle http://www.example.com/cert_bundle
apply ssl certBundle swg-certbundle
<!--NeedCopy-->
```

```
show ssl certbundle

            Name : swg-certbundle(Inuse)

```



```
5              URL : http://www.example.com/cert_bundle
6
7      Done
8  <!--NeedCopy-->
```

Importieren und Anwenden eines CA-Zertifikatpakets auf der Appliance mit der GUI

1. Navigieren Sie zu **Sicherheit > SSL Forward Proxy > Erste Schritte > Zertifikatpakete**.
2. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie ein Zertifikatspaket aus der Liste aus.
   - Um ein Zertifikatpaket hinzuzufügen, klicken Sie auf “+” und geben Sie einen Namen und eine Quell-URL an. Klicken Sie auf **OK**.
3. Klicken Sie auf **OK**.

Entfernen eines Zertifizierungsstellenzertifikatpakets aus der Appliance mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1  remove certBundle <cert bundle name>
2  <!--NeedCopy-->
```

Beispiel:

```
1  remove certBundle mytest-cacert
2  <!--NeedCopy-->
```

Exportieren eines Zertifizierungsstellen-Zertifikatpakets aus der Appliance mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1  export certBundle <cert bundle name> <Path to export>
2  <!--NeedCopy-->
```

ARGUMENTS:

Name:

Name, der dem importierten Zertifikatspaket zugewiesen werden soll. Muss mit einem alphanumerischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstriche, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestrich (-) enthalten. Die folgende Anforderung gilt nur für die CLI:

Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “meine Datei” oder ‘meine Datei’).

Maximale Länge: 31

src:

URL zur Angabe des Protokolls, des Hosts und des Pfads, einschließlich des Dateinamens, zum Zertifikatpaket, das importiert oder exportiert werden soll. Beispiel: `http://www.example.com/cert_bundle_file`.

HINWEIS: Der Import schlägt fehl, wenn sich das zu importierende Objekt auf einem HTTPS-Server befindet, der Clientzertifikatauthentifizierung für den Zugriff erfordert.

Maximale Länge: 2047

Beispiel:

```
export certBundle mytest-cacert http://192.0.2.20/
<!--NeedCopy-->
```

Importieren, Anwenden und Überprüfen eines CA-Zertifikatpakets aus dem Mozilla CA-Zertifikatspeicher

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
> import certbundle mozilla_public_ca https://curl.haxx.se/ca/cacert.
   pem
Done
<!--NeedCopy-->
```

Geben Sie Folgendes ein, um das Bündel anzuwenden:

```
> apply certbundle mozilla_public_ca
Done
<!--NeedCopy-->
```


Geben Sie Folgendes ein, um das verwendete Zertifikatbündel zu überprüfen:

```
> sh certbundle | grep mozilla
                Name : mozilla_public_ca (Inuse)
<!--NeedCopy-->
```

Einschränkungen

- Zertifikatpakete werden in einem Cluster-Setup oder auf einer partitionierten Appliance nicht unterstützt.
- Das TLSv1.3-Protokoll wird mit SSL-Forward-Proxy nicht unterstützt.

SSL-Richtlinieninfrastruktur für SSL-Interception

Eine Richtlinie verhält sich wie ein Filter für eingehenden Datenverkehr. Richtlinien auf der ADC-Appliance definieren, wie Proxy-Verbindungen und -Anforderungen verwaltet werden. Die Verarbeitung basiert auf den Aktionen, die für diese Richtlinie konfiguriert sind. Das heißt, Daten in Verbindungsanforderungen werden mit einer Regel verglichen, die in der Richtlinie angegeben ist, und die Aktion wird auf Verbindungen angewendet, die der Regel (Ausdruck) entsprechen. Nachdem Sie eine der Richtlinie zuweisende Aktion definiert und die Richtlinie erstellt haben, müssen Sie sie an einen Proxyserver binden, sodass sie für den Datenverkehr gilt, der durch diesen Proxyserver fließt.

Eine SSL-Richtlinie für das SSL-Interception wertet eingehenden Datenverkehr aus und wendet eine vordefinierte Aktion auf Anforderungen an, die einer Regel (Ausdruck) entsprechen. Eine Entscheidung zum Abfangen, Umgehen oder Zurücksetzen einer Verbindung wird basierend auf der definierten SSL-Richtlinie getroffen. Sie können eine von drei Aktionen für eine Richtlinie konfigurieren: INTERCEPT, BYPASS oder RESET. Sie müssen beim Erstellen einer Richtlinie eine Aktion angeben. Um eine Richtlinie in Kraft zu setzen, müssen Sie sie an einen Proxyserver auf der Appliance binden. Um anzugeben, dass eine Richtlinie für das SSL-Interception vorgesehen ist, müssen Sie den Typ (Bindpunkt) als INTERCEPT_REQ angeben, wenn Sie die Richtlinie an einen Proxyserver binden. Wenn Sie die Bindung einer Richtlinie aufheben, müssen Sie den Typ als INTERCEPT_REQ angeben.

> **Hinweis**:
>
> Der Proxyserver kann keine Entscheidung für Interception treffen, es sei denn, Sie geben eine Richtlinie an.

Interception des Datenverkehrs kann auf jedem SSL-Handshake-Attribut basieren. Am häufigsten wird die SSL-Domäne verwendet. Die SSL-Domäne wird normalerweise durch die Attribute des SSL-Handshake angezeigt. Hierbei kann es sich um den Wert Server Name Indicator handeln, der

aus der SSL-Client-Hallo (falls vorhanden) extrahiert wurde, oder um den aus dem Ursprungsserverzertifikat extrahierten Wert (Server Alternate Name, SAN) handeln. Die SSL-Abhörrichtlinie enthält ein spezielles Attribut, DETECTED_DOMAIN. Dieses Attribut erleichtert es den Kunden, Abhörrichtlinien basierend auf der SSL-Domäne aus dem Ursprungsserverzertifikat zu erstellen. Der Kunde kann den Domänennamen mit einer Zeichenfolge, einer URL-Liste (URL-Gruppe oder`patset`) oder einer von der Domäne abgeleiteten URL-Kategorie abgleichen.

Erstellen einer SSL-Richtlinie mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

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

Beispiele:

Die folgenden Beispiele beziehen sich auf Richtlinien mit Ausdrücken, die das`detected_domain` Attribut verwenden, um nach einem Domänennamen zu suchen.

Traffic zu einem Finanzinstitut wie XYZBANK nicht abfangen

```
add ssl policy pol1 -rule client.ssl.detected_domain.contains("XYZBANK")
   ) -action BYPASS
<!--NeedCopy-->
```

Erlauben Sie einem Benutzer nicht, sich über das Unternehmensnetzwerk mit YouTube zu verbinden

```
add ssl policy pol2 -rule client.ssl.client.ssl.detected_domain.
   url_categorize(0,0).category.eq ("YouTube") -action RESET
<!--NeedCopy-->
```

Abfangen des gesamten Benutzerverkehrs

```
add ssl policy pol3  - rule true  - action INTERCEPT
<!--NeedCopy-->
```

Wenn der Kunde die detected_domain nicht verwenden möchte, kann er jedes der SSL-Handshake-Attribute verwenden, um die Domäne zu extrahieren und abzuleiten.

Beispielsweise wird kein Domänenname in der SNI-Erweiterung der Client-Hello Message gefunden. Der Domänenname muss dem Ursprungsserverzertifikat entnommen werden. Die folgenden Beispiele beziehen sich auf Richtlinien mit Ausdrücken, die im Antragstellernamen des Ursprungsserverzertifikats nach einem Domänennamen suchen.

Abfangen des gesamten Benutzerverkehrs zu jeder Yahoo-Domain

```
1 add ssl policy pol4 -rule client.ssl.origin_server_cert.subject.
     contains("yahoo")  - action INTERCEPT
2 <!--NeedCopy-->
```

Den gesamten Benutzerverkehr für die Kategorie Shopping/Retail abfangen

```
1 add ssl policy pol_url_category -rule client.ssl.origin_server_cert.
     subject.URL_CATEGORIZE(0,0).CATEGORY.eq("Shopping/Retail") -action
     INTERCEPT
2 <!--NeedCopy-->
```

Abfangen des gesamten Benutzerverkehrs an eine nicht kategorisierte URL

```
1 add ssl policy pol_url_category -rule client.ssl.origin_server_cert.
     subject.url_categorize(0,0).category.eq("Uncategorized") -action
     INTERCEPT
2 <!--NeedCopy-->
```

Die folgenden Beispiele beziehen sich auf Richtlinien, die der Domäne mit einem Eintrag in einem URL-Satz entsprechen.

Den gesamten Benutzerverkehr abfangen, wenn der Domänenname in SNI mit einem Eintrag im URL-Satz “top100 übereinstimmt

```
1 add ssl policy pol_url_set  -rule client.ssl.client_hello.SNI.
     URLSET_MATCHES_ANY("top100") -action INTERCEPT
2 <!--NeedCopy-->
```

Abfangen des gesamten Benutzerdatenverkehrs des Domänennamens, wenn das Ursprungsserverzertifikat mit einem Eintrag im URL-Satz top100 übereinstimmt


```
add ssl policy pol_url_set  -rule client.ssl.origin_server_cert.subject
    .URLSET_MATCHES_ANY("top100") -action INTERCEPT
<!--NeedCopy-->
```

Erstellen einer SSL-Richtlinie für einen Proxyserver mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL > Richtlinien**.
2. Klicken Sie auf der Registerkarte **SSL-Richtlinien** auf **Hinzufügen**, und geben Sie die folgenden Parameter an:
   - Richtlinienname
   - Richtlinienaktion — Wählen Sie zwischen Abfangen, Umgehen oder Zurücksetzen aus.
   - Ausdruck
3. Klicken Sie auf **Erstellen**.

Binden einer SSL-Richtlinie an einen Proxyserver mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind ssl vserver <vServerName> -policyName <string> -priority <
    positive_integer> -type  INTERCEPT_REQ
<!--NeedCopy-->
```

Beispiel:

```
bind ssl vserver <name> -policyName pol1 -priority 10 -type
    INTERCEPT_REQ
<!--NeedCopy-->
```

Binden einer SSL-Richtlinie an einen Proxyserver mit der GUI

1. Navigieren Sie zu **Sicherheit > SSL Forward Proxy > Proxy Virtual Servers**.
2. Wählen Sie einen virtuellen Server aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie unter **Erweiterte Einstellungen** auf **SSL-Richtlinien**.
4. Klicken Sie in das Feld **SSL-Richtlinie** .
5. **Wählen Sie unter Richtlinie**auswählen eine zu bindende Richtlinie aus.
6. Wählen Sie unter **Typ**die Option **INTERCEPT_REQ**aus.
7. Klicken Sie auf **Bin** den und dann auf **OK** .

Aufheben der Bindung einer SSL-Richtlinie an einen Proxyserver über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
unbind ssl vserver <vServerName> -policyName <string> -type
   INTERCEPT_REQ
<!--NeedCopy-->
```

SSL-Ausdrücke, die in SSL-Richtlinien verwendet werden

Ausdruck	Beschreibung
`CLIENT.SSL.CLIENT_HELLO.SNI.*`	Gibt die SNI-Erweiterung in einem Zeichenfolgenformat zurück. Bewerten Sie die Zeichenfolge, um zu sehen, ob sie den angegebenen Text enthält. Beispiel: client.ssl.client_hello.sni.contains (`"xyz.com"`)
`CLIENT.SSL.ORIGIN_SERVER_CERT.*`	Gibt ein Zertifikat zurück, das von einem Back-End-Server empfangen wird, in einem Zeichenfolgenformat. Bewerten Sie die Zeichenfolge, um zu sehen, ob sie den angegebenen Text enthält. Beispiel: client.ssl.origin_server_cert.subject.contains(`"xyz.com"`)
`CLIENT.SSL.DETECTED_DOMAIN.*`	Gibt eine Domäne entweder aus der SNI-Erweiterung oder aus dem Ursprungsserverzertifikat in einem Zeichenfolgenformat zurück. Bewerten Sie die Zeichenfolge, um zu sehen, ob sie den angegebenen Text enthält. Beispiel: client.ssl.detected_domain.contains(`"xyz.com"`)

SSL-Fehler beim automatischen Lernen

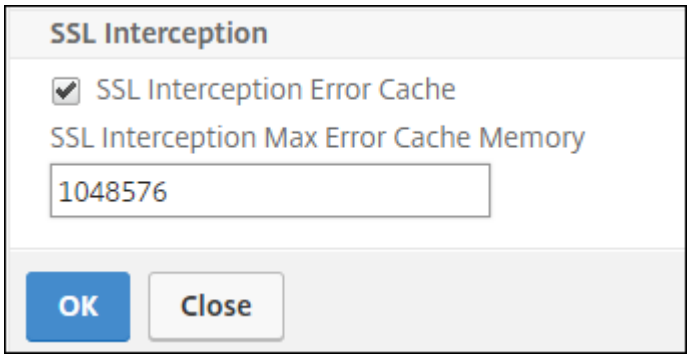
Die Appliance fügt der SSL-Umgehungsliste eine Domäne hinzu, wenn der Lernmodus aktiviert ist. Der Lernmodus basiert auf der SSL-Warnmeldung, die von einem Client oder einem Ursprungsserver empfangen wird. Das heißt, das Lernen hängt vom Client oder Server ab, der eine Warnmeldung sendet. Es gibt keine Erkenntnisse, wenn keine Warnmeldung gesendet wird. Die Appliance lernt, ob eine der folgenden Bedingungen erfüllt ist:

1. Eine Anforderung für ein Clientzertifikat wird vom Server empfangen.
2. Jede der folgenden Warnungen wird im Rahmen des Handshakes empfangen:
   - BAD_CERTIFICATE
   - UNSUPPORTED_CERTIFICATE
   - CERTIFICATE_REVOKED
   - CERTIFICATE_EXPIRED
   - CERTIFICATE_UNKNOWN
   - UNKNOWN_CA (Wenn ein Client das Anheften verwendet, sendet er diese Warnmeldung, wenn er ein Serverzertifikat erhält.)
   - HANDSHAKE_FAILURE

Um das Lernen zu aktivieren, müssen Sie den Fehler-Cache aktivieren und den für das Lernen reservierten Speicher angeben.

Aktivieren des Lernens mit der GUI

1. Navigieren Sie zu **Traffic Management > SSL**.
2. Klicken Sie in den **Einstellungen**auf **Erweiterte SSL-Einstellungen ändern**.
3. Wählen Sie in **SSL-Interception** die Option **SSL-Interception-Fehlercache** aus.
4. Geben Sie in **SSL Interception Max Error Cache Memory** den Speicher (in Byte) an, der reserviert werden soll.



5. Klicken Sie auf **OK**.

Aktivieren des Lernens mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl parameter -ssliErrorCache ( ENABLED | DISABLED ) -
    ssliMaxErrorCacheMem <positive_integer>
<!--NeedCopy-->
```

Argumente:

ssliErrorCache:

Aktivieren oder deaktivieren Sie dynamisches Lernen, und speichern Sie die erlernten Informationen, um nachfolgende Entscheidungen zu treffen, um Anforderungen abzufangen oder zu umgehen. Wenn diese Option aktiviert ist, führt die Appliance eine Cache-Suche durch, um zu entscheiden, ob die Anforderung umgangen werden soll.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

ssliMaxErrorCacheMem:

Geben Sie den maximalen Speicher in Byte an, mit dem die gelernten Daten zwischengespeichert werden können. Dieser Speicher wird als LRU-Cache verwendet, so dass die alten Einträge durch neue Einträge ersetzt werden, nachdem das eingestellte Speicherlimit erschöpft ist. Der Wert 0 entscheidet automatisch über den Grenzwert.

Standardwert: 0

Mindestwert: 0

maximaler Wert: 4294967294

SSL-Profil

Ein SSL-Profil ist eine Sammlung von SSL-Einstellungen, wie Verschlüsselungen und Protokolle. Ein Profil ist hilfreich, wenn Sie gemeinsame Einstellungen für verschiedene Server haben. Anstatt für jeden Server dieselben Einstellungen anzugeben, können Sie ein Profil erstellen, die Einstellungen im Profil angeben und das Profil dann an verschiedene Server binden. Wenn kein benutzerdefiniertes Front-End-SSL-Profil erstellt wird, ist das Standard-Front-End-Profil an clientseitige Entitäten gebunden. Mit diesem Profil können Sie Einstellungen für die Verwaltung der clientseitigen Verbindungen konfigurieren.

Für SSL-Interception müssen Sie ein SSL-Profil erstellen und SSL-Interception im Profil aktivieren. Eine Standardverschlüsselungsgruppe ist an dieses Profil gebunden, Sie können jedoch weitere

Verschlüsselungen entsprechend Ihrer Bereitstellung konfigurieren. Binden Sie ein SSL-Interception-CA-Zertifikat an dieses Profil und binden Sie das Profil dann an einen Proxyserver. Für das SSL-Interception sind die wesentlichen Parameter in einem Profil diejenigen, die für die folgenden Aktionen verwendet werden:

- Überprüfen Sie den OCSP-Status des Original-Serverzertifikats.
- Lösen Sie eine Neuverhandlung von Clients aus, wenn der Original-Server eine Neuverhandlung verlangt.
- Überprüfen Sie das Original-Serverzertifikat, bevor Sie die Front-End-SSL-Sitzung wiederverwenden.

Verwenden Sie das standardmäßige Backend-Profil bei der Kommunikation mit den Original-Servern. Legen Sie alle serverseitigen Parameter, z. B. Verschlüsselungssammlungen, im Standard-Back-End-Profil fest. Ein benutzerdefiniertes Back-End-Profil wird nicht unterstützt.

Beispiele für die am häufigsten verwendeten SSL-Einstellungen finden Sie unter Beispielprofil am Ende dieses Abschnitts.

Die Verschlüsselungs-/Protokollunterstützung unterscheidet sich vom internen und externen Netzwerk. In den folgenden Tabellen ist die Verbindung zwischen den Benutzern und einer ADC-Appliance das interne Netzwerk. Das externe Netzwerk befindet sich zwischen der Appliance und dem Internet.

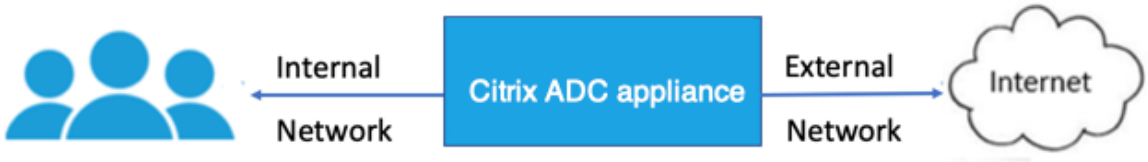


Tabelle 1: Verschlüsselungs-/Protokoll -Unterstützungsmatrix für das interne Netzwerk

Siehe Tabelle 1-Support für virtuelle Server/Frontend-Service/internen Dienst in Ciphers, die auf den Citrix ADC Appliances verfügbar sind.

Tabelle 2: Verschlüsselung/Protokoll-Unterstützungsmatrix für das externe Netzwerk

Siehe Tabelle 2-Unterstützung für Back-End-Dienste in Ciphers, die auf den Citrix ADC Appliances verfügbar sind.

Hinzufügen eines SSL-Profils und Aktivieren der SSL-Interception mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ssl profile <name> -sslinterception ENABLED -ssliReneg ( ENABLED |
 DISABLED )-ssliOCSPCheck ( ENABLED | DISABLED )-ssliMaxSessPerServer <
positive_integer>
```


Argumente:

sslInterception:

Aktivieren oder deaktivieren Sie SSL-Interception für Sitzungen.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

ssliReneg:

Aktivieren oder deaktivieren Sie die auslösende Clientneuverhandlung, wenn eine Neuverhandlungsanforderung vom Ursprungsserver empfangen wird.

Mögliche Werte: ENABLED, DISABLED

Standardwert: ENABLED

ssliOCSPCheck:

Aktivieren oder Deaktivieren der OCSP-Prüfung für ein Ursprungsserver-Zertifikat.

Mögliche Werte: ENABLED, DISABLED

Standardwert: ENABLED

ssliMaxSessPerServer:

Maximale Anzahl von SSL-Sitzungen, die pro dynamischem Ursprungsserver zwischengespeichert werden sollen. Für jede vom Client empfangene SNI-Erweiterung wird eine eindeutige SSL-Sitzung erstellt. Die übereinstimmende Sitzung wird für die Wiederverwendung von Serversitzungen verwendet.

Standardwert: 10

Mindestwert: 1

Maximalwert: 1000

Beispiel:

```
1 add ssl profile swg_ssl_profile  -sslinterception ENABLED
2
3 Done
4
5 sh ssl profile swg_ssl_profile
6
7 1)    Name: swg_ssl_profile (Front-End)
8
9                 SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1
                      .1: ENABLED  TLSv1.2: ENABLED
```



```
10
11                  Client Auth: DISABLED
12
13                  Use only bound CA certificates: DISABLED
14
15                  Strict CA checks:                                   NO
16
17                  Session Reuse: ENABLED
                        Timeout: 120 seconds
18
19                  DH: DISABLED
20
21                  DH Private-Key Exponent Size Limit: DISABLED
                        Ephemeral RSA: ENABLED
                        Refresh Count: 0
22
23                  Deny SSL Renegotiation
                        ALL
24
25                  Non FIPS Ciphers: DISABLED
26
27                  Cipher Redirect: DISABLED
28
29                  SSL Redirect: DISABLED
30
31                  Send Close-Notify: YES
32
33                  Strict Sig-Digest Check: DISABLED
34
35                  Push Encryption Trigger: Always
36
37                  PUSH encryption trigger timeout:              1 ms
38
39                  SNI: DISABLED
40
41                  OCSP Stapling: DISABLED
42
43                  Strict Host Header check for SNI enabled SSL sessions:
                                          NO
44
45                  Push flag:             0x0 (Auto)
46
47                  SSL quantum size:                               8 kB
48
49                  Encryption trigger timeout           100 mS
```



```
50
51                 Encryption trigger packet count:                45
52
53                 Subject/Issuer Name Insertion Format: Unicode
54
55                 SSL Interception: ENABLED
56
57                 SSL Interception OCSP Check: ENABLED
58
59                 SSL Interception End to End Renegotiation: ENABLED
60
61                 SSL Interception Server Cert Verification for Client
                      Reuse: ENABLED
62
63                 SSL Interception Maximum Reuse Sessions per Server:  10
64
65                 Session Ticket: DISABLED              Session Ticket
                      Lifetime: 300 (secs)
66
67                 HSTS: DISABLED
68
69                 HSTS IncludeSubDomains: NO
70
71                 HSTS Max-Age: 0
72
73                 ECC Curve: P_256, P_384, P_224, P_521
74
75 1)             Cipher Name: DEFAULT Priority :1
76
77                   Description: Predefined Cipher Alias
78
79 Done
80 <!--NeedCopy-->
```

Binden Sie ein SSL-Interception-CA-Zertifikat an ein SSL-Profil mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind ssl profile <name> -ssliCACertkey <ssli-ca-cert>
```

Beispiel:

```
1 bind ssl profile swg_ssl_profile -ssliCACertkey swg_ca_cert
```



```
2
3  Done
4
5  sh ssl profile swg_ssl_profile
6
7  1)            Name: swg_ssl_profile (Front-End)
8
9                  SSLv3: DISABLED               TLSv1.0: ENABLED  TLSv1
                       .1: ENABLED  TLSv1.2: ENABLED
10
11                 Client Auth: DISABLED
12
13                 Use only bound CA certificates: DISABLED
14
15                 Strict CA checks:                                NO
16
17                 Session Reuse: ENABLED
                       Timeout: 120 seconds
18
19                 DH: DISABLED
20
21                 DH Private-Key Exponent Size Limit: DISABLED
                       Ephemeral RSA: ENABLED
                       Refresh Count: 0
22
23                 Deny SSL Renegotiation
                       ALL
24
25                 Non FIPS Ciphers: DISABLED
26
27                 Cipher Redirect: DISABLED
28
29                 SSL Redirect: DISABLED
30
31                 Send Close-Notify: YES
32
33                 Strict Sig-Digest Check: DISABLED
34
35                 Push Encryption Trigger: Always
36
37                 PUSH encryption trigger timeout:             1 ms
38
39                 SNI: DISABLED
40
41                 OCSP Stapling: DISABLED
```



```
42
43                  Strict Host Header check for SNI enabled SSL sessions:
                                NO
44
45                  Push flag:            0x0 (Auto)
46
47                  SSL quantum size:                              8 kB
48
49                  Encryption trigger timeout           100 mS
50
51                  Encryption trigger packet count:                45
52
53                  Subject/Issuer Name Insertion Format: Unicode
54
55                  SSL Interception: ENABLED
56
57                  SSL Interception OCSP Check: ENABLED
58
59                  SSL Interception End to End Renegotiation: ENABLED
60
61                  SSL Interception Server Cert Verification for Client
                       Reuse: ENABLED
62
63                  SSL Interception Maximum Reuse Sessions per Server:  10
64
65                  Session Ticket: DISABLED              Session Ticket
                       Lifetime: 300 (secs)
66
67                  HSTS: DISABLED
68
69                  HSTS IncludeSubDomains: NO
70
71                  HSTS Max-Age: 0
72
73                  ECC Curve: P_256, P_384, P_224, P_521
74
75  1)            Cipher Name: DEFAULT Priority :1
76
77                  Description: Predefined Cipher Alias
78
79  1)            SSL Interception CA CertKey Name: swg_ca_cert
80
81  Done
82  <!--NeedCopy-->
```


Binden Sie ein SSL-Interception-CA-Zertifikat an ein SSL-Profil mit der GUI

1. Navigieren Sie zu **System** > **Profile** > **SSL-Profil**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie einen Namen für das Profil an.
4. Aktivieren Sie **SSL-Interception für Sitzungen**.
5. Klicken Sie auf **OK**.
6. Klicken Sie unter **Erweiterte Einstellungen** auf **Zertifikatschlüssel**.
7. Geben Sie einen SSL-Interception-CA-Zertifikatschlüssel für die Bindung an das Profil an.
8. Klicken Sie auf **Auswählen** und dann auf **Binden**.
9. Optional können Sie Verschlüsselungen entsprechend Ihrer Bereitstellung konfigurieren.
   - Klicken Sie auf das Symbol Bearbeiten, und klicken Sie dann auf **Hinzufügen**.
   - Wählen Sie eine oder mehrere Verschlüsselungsgruppen aus, und klicken Sie auf den Pfeil nach rechts.
   - Klicken Sie auf **OK**.
10. Klicken Sie auf **Fertig**.

Binden eines SSL-Profils an einen Proxyserver mit der GUI

1. Navigieren Sie zu **Sicherheit** > **SSL Forward Proxy** > **Virtual Proxy Server**, und fügen Sie einen Server hinzu, oder wählen Sie einen Server aus, der geändert werden soll
2. Klicken Sie im **SSL-Profil**auf das Symbol Bearbeiten.
3. Wählen Sie in der Liste **SSL-Profil** das SSL-Profil aus, das Sie zuvor erstellt haben.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Fertig**.

Beispielprofil:

```
Name: swg_ssl_profile (Front-End)

                SSLv3: DISABLED              TLSv1.0: ENABLED  TLSv1
                    .1: ENABLED  TLSv1.2: ENABLED

                Client Auth: DISABLED

                Use only bound CA certificates: DISABLED

```



```
                Strict CA checks:                                   NO

                Session Reuse: ENABLED
                    Timeout: 120 seconds

                DH: DISABLED

                DH Private-Key Exponent Size Limit: DISABLED
                    Ephemeral RSA: ENABLED
                    Refresh Count: 0

                Deny SSL Renegotiation
                    ALL

                Non FIPS Ciphers: DISABLED

                Cipher Redirect: DISABLED

                SSL Redirect: DISABLED

                Send Close-Notify: YES

                Strict Sig-Digest Check: DISABLED

                Push Encryption Trigger: Always

                PUSH encryption trigger timeout:              1 ms

                SNI: DISABLED

                OCSP Stapling: DISABLED

                Strict Host Header check for SNI enabled SSL sessions:
                                        NO

                Push flag:             0x0 (Auto)

                SSL quantum size:                              8 kB

                Encryption trigger timeout           100 mS

                Encryption trigger packet count:                45

                Subject/Issuer Name Insertion Format: Unicode

```



```
49                  SSL Interception: ENABLED
50
51                  SSL Interception OCSP Check: ENABLED
52
53                  SSL Interception End to End Renegotiation: ENABLED
54
55                  SSL Interception Maximum Reuse Sessions per Server:  10
56
57                  Session Ticket: DISABLED              Session Ticket
                       Lifetime: 300 (secs)
58
59                  HSTS: DISABLED
60
61                  HSTS IncludeSubDomains: NO
62
63                  HSTS Max-Age: 0
64
65                  ECC Curve: P_256, P_384, P_224, P_521
66
67 1)             Cipher Name: DEFAULT Priority :1
68
69                  Description: Predefined Cipher Alias
70
71 1)             SSL Interception CA CertKey Name: swg_ca_cert
72 <!--NeedCopy-->
```

Benutzeridentitätsverwaltung

February 24, 2022

Eine zunehmende Anzahl von Sicherheitsverletzungen und die wachsende Beliebtheit mobiler Geräte haben betont, dass sichergestellt werden muss, dass die Nutzung des externen Internets den Unternehmensrichtlinien entspricht. Nur autorisierten Benutzern muss der Zugriff auf externe Ressourcen gewährt werden, die vom Unternehmenspersonal bereitgestellt werden. Identity Management macht es möglich, indem es die Identität einer Person oder eines Geräts überprüft. Es bestimmt nicht, welche Aufgaben der Einzelne übernehmen kann oder welche Dateien der Einzelne sehen kann.

Eine SSL-Forward-Proxybereitstellung identifiziert den Benutzer, bevor der Zugriff auf das Internet gewährt wird. Alle Anfragen und Antworten des Benutzers werden überprüft. Benutzeraktivität wird protokolliert, und Datensätze werden zur Berichterstellung in das Citrix Application Delivery Management (ADM) exportiert. In Citrix ADM können Sie die Statistiken zu Benutzeraktivitäten, Transaktionen

und Bandbreitenverbrauch anzeigen.

Standardmäßig wird nur die IP-Adresse des Benutzers gespeichert, aber Sie können die Funktion so konfigurieren, dass weitere Details über den Benutzer aufgezeichnet werden. Sie können diese Identitätsinformationen verwenden, um umfangreichere Richtlinien zur Internetnutzung für bestimmte Benutzer zu erstellen.

Die Citrix ADC-Appliance unterstützt die folgenden Authentifizierungsmodi für eine explizite Proxy-Konfiguration.

- **Lightweight Directory Access Protocol (LDAP)**. Authentifiziert den Benutzer über einen externen LDAP-Authentifizierungsserver. Weitere Informationen finden Sie unter LDAP-Authentifizierungsrichtlinien.
- **RADIUS**. Authentifiziert den Benutzer über einen externen RADIUS-Server. Weitere Informationen finden Sie unter RADIUS-Authentifizierungsrichtlinien.
- **TACACS +**. Authentifiziert den Benutzer über einen externen TACACS-Authentifizierungsserver (Terminal Access Controller Access-Control System). Weitere Informationen finden Sie unter Authentifizierungsrichtlinien.
- **Verhandeln**. Authentifiziert den Benutzer über einen Kerberos-Authentifizierungsserver. Wenn bei der Kerberos-Authentifizierung ein Fehler auftritt, verwendet die Appliance die NTLM-Authentifizierung. Weitere Informationen finden Sie unter Authentifizierungsrichtlinien aushandeln.

Bei transparentem Proxy wird nur IP-basierte LDAP-Authentifizierung unterstützt. Wenn eine Clientanfrage empfangen wird, authentifiziert der Proxy den Benutzer, indem er einen Eintrag für die Client-IP-Adresse im Active Directory überprüft. Es erstellt dann eine Sitzung basierend auf der IP-Adresse des Benutzers. Wenn Sie das ssonameAttribute jedoch in einer LDAP-Aktion konfigurieren, wird eine Sitzung unter Verwendung des Benutzernamens anstelle der IP-Adresse erstellt. Klassische Richtlinien werden für die Authentifizierung in einem transparenten Proxy-Setup nicht unterstützt.

> **Hinweis:**
>
> Für expliziten Proxy müssen Sie den LDAP-Anmeldenamen auf **sAMAccountName**festlegen. Für transparenten Proxy müssen Sie den LDAP-Anmeldenamen auf **NetworkAddress** und attribute1 auf **sAMAccountName** festlegen.

Beispiel für expliziten Proxy:

```
1 add authentication ldapAction swg-auth-action-explicit -serverIP
     10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
     CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
     freebsd123$ -ldapLoginName sAMAccountName
2 <!--NeedCopy-->
```


Beispiel für transparenten Proxy:

```
add authentication ldapAction swg-auth-action-explicit -serverIP
    10.105.157.116 -ldapBase "CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDn "
    CN=Administrator,CN=Users,DC=CTXNSSFB,DC=COM" -ldapBindDnPassword
    freebsd123$ -ldapLoginName networkAddress -authentication disable -
    Attribute1 sAMAccountName
<!--NeedCopy-->
```

Einrichten der Benutzerauthentifizierung mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication vserver <vserver name> SSL

bind ssl vserver <vserver name> -certkeyName <certkey name>

add authentication ldapAction <action name> -serverIP <ip_addr> -
    ldapBase <string> -ldapBindDn <string> -ldapBindDnPassword -
    ldapLoginName <string>

add authentication Policy <policy name> -rule <expression> -action <
    string>

bind authentication vserver <vserver name> -policy <string> -priority <
    positive_integer>

set cs vserver <name> -authn401 ON -authnVsName <string>
<!--NeedCopy-->
```

Argumente:

Servername:

Name des virtuellen Authentifizierungsservers, an den die Richtlinie gebunden werden soll.

Maximale Länge: 127

serviceType:

Protokolltyp des virtuellen Authentifizierungsservers. Immer SSL.

Mögliche Werte: SSL

Standardwert: SSL

Name der Aktion:

Name für die neue LDAP-Aktion. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und nur Buchstaben, Zahlen und Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), at (@), Gleich (=), Doppelpunkt (:) und Unterstrich enthalten. Kann nicht geändert werden, nachdem die LDAP-Aktion hinzugefügt wurde. Die folgende Anforderung gilt nur für die CLI:

Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “Meine Authentifizierungsaktion” oder ‘Meine Authentifizierungsaktion’).

Maximale Länge: 127

serverIP:

IP-Adresse, die dem LDAP-Server zugewiesen ist.

ldapBase:

Basis (Knoten), von dem aus LDAP-Suchen gestartet werden sollen. Wenn der LDAP-Server lokal läuft, ist der Standardwert von base dc=netscaler, dc=com. Maximale Länge: 127

ldapBindDn:

Vollständiger Distinguished Name (DN), der zum Binden an den LDAP-Server verwendet wird.

Standard: cn=Manager, dc=netscaler, dc=com

Maximale Länge: 127

ldapBindDnPassword:

Kennwort für die Bindung an den LDAP-Server.

Maximale Länge: 127

ldapLoginName:

LDAP-Anmeldenamen-Attribut. Die Citrix ADC-Appliance verwendet den LDAP-Anmeldenamen, um externe LDAP-Server oder Active Directories abzufragen. Maximale Länge: 127

Richtlinienname:

Name für die erweiterte Authentifizierungsrichtlinie. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (_) beginnen und nur Buchstaben, Zahlen und Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), at (@), Gleich (=), Doppelpunkt (:) und Unterstrich enthalten. Kann nicht geändert werden, nachdem eine AUTHENTIFIZIERUNGSrichtlinie erstellt wurde. Die folgende Anforderung gilt nur für die CLI:

Wenn der Name ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in doppelte oder einfache Anführungszeichen ein (z. B. “meine Authentifizierungsrichtlinie” oder ‘meine Authentifizierungsrichtlinie’).

Maximale Länge: 127

rule:

Name der Regel oder eines Standardsyntaxausdrucks, mit dem die Richtlinie bestimmt, ob versucht wird, den Benutzer beim AUTHENTICATION-Server zu authentifizieren.

Maximale Länge: 1499

action:

Name der Authentifizierungsaktion, die ausgeführt werden soll, wenn die Richtlinie übereinstimmt.

Maximale Länge: 127

priority:

Positive Ganzzahl, die die Priorität der Richtlinie angibt. Eine niedrigere Zahl gibt eine höhere Priorität an. Richtlinien werden in der Reihenfolge ihrer Prioritäten ausgewertet, und die erste Richtlinie, die der Anforderung entspricht, wird angewendet. Muss innerhalb der Liste der Richtlinien eindeutig sein, die an den virtuellen Authentifizierungsserver gebunden sind.

Mindestwert: 0

Maximalwert: 4294967295

Beispiel:

```
1  add authentication vserver swg-auth-vs SSL
2
3  Done
4
5  bind ssl vserver explicit-auth-vs -certkeyName ns-swg-ca-certkey
6
7  Done
8
9  add authentication ldapAction swg-auth-action-explicit -serverIP
       192.0.2.116 -ldapBase ”CN=Users,DC=CTXNSSFB,DC=COM” -ldapBindDn ”CN=
       Administrator,CN=Users,DC=CTXNSSFB,DC=COM” -ldapBindDnPassword zzzzz
        -ldapLoginName sAMAccountName
10
11 Done
12
13 add authenticationpolicy swg-auth-policy -rule true -action swg-auth-
       action-explicit
```



```
14 Done
15
16 bind authentication vserver swg-auth-vs -policy swg-auth-policy -
      priority 1
17
18 Done
19
20 set cs vserver testswg -authn401 ON -authnVsName swg-auth-vs
21
22 Done
23 <!--NeedCopy-->
```

Aktivieren der Benutzernamenprotokollierung mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set appflow param -AAAUserName ENABLED
2 <!--NeedCopy-->
```

Argumente:

AAAUserName

Aktivieren Sie die AppFlow Authentifizierung, Autorisierung und Auditing-Benutzernamenprotokollierung.

Mögliche Werte: ENABLED, DISABLED

Standardwert: DISABLED

Beispiel:

```
1 set appflow param -AAAUserName ENABLED
2 <!--NeedCopy-->
```

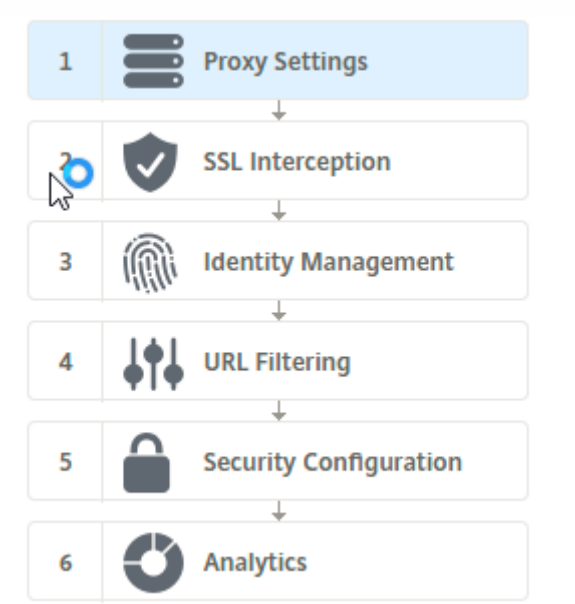
URL-Filterung

October 5, 2021

Die URL-Filterung ermöglicht die richtlinienbasierte Steuerung von Websites mit der in URLs enthaltenen Informationen. Mit dieser Funktion können Netzwerkadministratoren den Benutzerzugriff auf bösartige Websites im Netzwerk überwachen und kontrollieren.

Erste Schritte

Wenn Sie ein neuer Benutzer sind und die URL-Filterung konfigurieren möchten, müssen Sie die anfängliche SSL-Forward-Proxy-Setup abschließen. Um mit der URL-Filterung zu beginnen, müssen Sie sich zuerst beim SSL-Forward-Proxy-Assistenten anmelden. Der Assistent führt Sie durch eine Reihe von Konfigurationsschritten, bevor Sie die URL-Filterrichtlinien anwenden.



> **Hinweis:**
>
> Bevor Sie beginnen, stellen Sie sicher, dass auf Ihrer Appliance eine gültige URL Threat Intelligence Feature-Lizenz installiert ist. Wenn Sie eine Testversion verwenden, stellen Sie sicher, dass Sie eine gültige Lizenz erwerben, um diese Funktion weiterhin auf der ADC-Appliance nutzen zu können.

Anmelden beim SSL-Forward-Proxyassistenten

Der SSL-Forward-Proxy-Assistent führt Sie durch eine Reihe vereinfachter Konfigurationsaufgaben, und im rechten Fensterbereich wird die entsprechende Flow-Sequenz angezeigt. Mit diesem Assistenten können Sie URL-Filterrichtlinien auf eine URL-Liste oder eine vordefinierte Liste von Kategorien anwenden.

Schritt 1: Konfigurieren von Proxy-Einstellungen

Konfigurieren Sie zuerst einen Proxyserver, über den der Client auf das Gateway zugreift. Dieser Server ist vom Typ SSL und arbeitet im expliziten oder transparenten Modus. Weitere Informationen zur Proxy-Serverkonfiguration finden Sie unter Proxy-Modi.

Schritt 2: Konfigurieren von SSL-Interception

Nach der Konfiguration des Proxyservers müssen Sie den SSL-Interceptionproxy so konfigurieren, dass er verschlüsselten Datenverkehr an der Citrix ADC Appliance abfängt. Im Falle der URL-Filterung fängt der SSL-Proxy den Datenverkehr ab und lässt keine blockierten URLs zu, während der gesamte andere Datenverkehr umgangen werden kann. Weitere Informationen zum Konfigurieren von SSL-Interception finden Sie unter SSL-Interception.

Schritt 3: Konfigurieren der Identitätsverwaltung

Ein Benutzer wird authentifiziert, bevor er sich am Unternehmensnetzwerk anmelden darf. Die Authentifizierung bietet die Flexibilität, spezifische Richtlinien für einen Benutzer oder eine Gruppe von Benutzern basierend auf ihren Rollen zu definieren. Weitere Informationen zur Benutzerauthentifizierung finden Sie unter Verwaltung der Benutzeridentifizierung.

Schritt 4: URL-Filterung konfigurieren

Der Administrator kann eine URL-Filterrichtlinie entweder mit der URL-Kategorisierungsfunktion oder mit der URL-Listenfunktion anwenden.

URL-Kategorisierung. Steuert den Zugriff auf Websites und Webseiten, indem der Datenverkehr basierend auf einer vordefinierten Liste von Kategorien gefiltert wird.

URL-Liste. Steuert den Zugriff auf Websites und Webseiten auf der Sperrliste, indem der Zugriff auf URLs verweigert wird, die in einen in die Appliance importierten URLs enthalten sind.

Schritt 5: Konfigurieren der Sicherheitskonfiguration

Mit diesem Schritt können Sie eine Reputationsbewertung konfigurieren und Benutzern erlauben, den Zugriff auf die Websites zu steuern, indem Sie den Zugriff verweigern, wenn die Bewertung zu niedrig ist. Ihre Reputationsbewertung kann zwischen 1 und 4 liegen, und Sie können den Schwellenwert konfigurieren, bei dem die Punktzahl inakzeptabel wird. Bei Bewertungen, die den Schwellenwert überschreiten, können Sie eine Richtlinienaktion auswählen, um Datenverkehr zuzulassen, zu blockieren oder umzuleiten. Weitere Informationen finden Sie unter URL Reputation Score.

Schritt 6: Konfigurieren der SSL-Forward-Proxyanalyse

Mit diesem Schritt können Sie SSL-Proxyanalysen für die Kategorisierung des Webverkehrs aktivieren, URL-Kategorie in den Benutzertransaktionsprotokollen protokollieren und Datenverkehrsanalysen anzeigen. Weitere Informationen zu SSL-Forward-Proxy-Analysen finden Sie unter Analytics.

Schritt 7: Klicken Sie auf “Fertig”, um die Erstkonfiguration abzuschließen und die URL-Filterkonfiguration fortzusetzen

URL-Liste

October 5, 2021

Mit der URL-Listenfunktion können Unternehmenskunden den Zugriff auf bestimmte Websites und Websitekategorien steuern. Das Feature filtert Websites, indem eine Responder-Richtlinie angewendet wird, die an einen URL-Abgleichsalgorithmus gebunden ist. Der Algorithmus gleicht die eingehende URL mit einem URL-Satz ab, der aus bis zu einer Million (1.000.000) Einträgen besteht. Wenn die eingehende URL-Anforderung mit einem Eintrag in der Gruppe übereinstimmt, verwendet die Appliance die Responderrichtlinie, um die Anforderung (HTTP/HTTPS) auszuwerten und den Zugriff darauf zu steuern.

URL-Set-Typen

Jeder Eintrag in einem URL-Satz kann eine URL und optional deren Metadaten (URL-Kategorie, Kategoriegruppen oder andere verwandte Daten) enthalten. Bei URLs mit Metadaten verwendet die Appliance einen Richtlinienausdruck, der die Metadaten auswertet. Weitere Informationen finden Sie unter URL-Set.

SSL Forward-Proxy unterstützt benutzerdefinierte URL-Sets. Sie können auch Mustersätze verwenden, um URLs zu filtern.

Benutzerdefinierter URL-Satz. Sie können einen benutzerdefinierten URL-Satz mit bis zu 1.000.000 URL-Einträgen erstellen und als Textdatei in Ihre Appliance importieren.

Musterset Eine ADC-Appliance kann Pattern-Sets verwenden, um URLs zu filtern, bevor sie Zugriff auf Websites gewähren. Ein Mustersatz ist ein Zeichenfolge-Matching-Algorithmus, der nach einer genauen Übereinstimmung zwischen einer eingehenden URL und bis zu 5000 Einträgen sucht. Weitere Informationen finden Sie unter Musterset.

Jede URL in einem importierten URL-Satz kann eine benutzerdefinierte Kategorie in Form von URL-Metadaten aufweisen. Ihre Organisation kann das Set hosten und die ADC-Appliance so konfigurieren, dass das Set regelmäßig aktualisiert wird, ohne dass ein manueller Eingriff erforderlich ist.

Nach der Aktualisierung des Satzes erkennt die Citrix ADC Appliance automatisch die Metadaten. Die Kategorie ist jetzt als Richtlinienausdruck verfügbar, um die URL auszuwerten und eine Aktion wie Zulassen, Blockieren, Umleiten oder Benachrichtigen des Benutzers zu verwenden.

Erweiterte Richtlinienausdrücke, die mit URL-Sets verwendet werden

In der folgenden Tabelle werden die grundlegenden Ausdrücke beschrieben, die Sie zum Auswerten des eingehenden Datenverkehrs verwenden können.

1. .URLSET_MATCHES_ANY - Wertet TRUE aus, wenn die URL genau mit einem Eintrag im URL-Set übereinstimmt.
2. .GET_URLSET_METADATA () - Der Ausdruck GET_URLSET_METADATA () gibt die zugeordneten Metadaten zurück, wenn die URL genau einem Muster innerhalb des URL-Sets entspricht. Eine leere Zeichenfolge wird zurückgegeben, wenn keine Übereinstimmung vorhanden ist.
3. `.GET_ URLSET_METADATA().EQ(<METADATA)- .GET_ URLSET_METADATA().EQ(<METADATA)`
4. .GET_URLSET_METADATA ().TYPECAST_LIST_T(‘,’).GET(0).EQ() - Ist TRUE, wenn sich die übereinstimmenden Metadaten am Anfang der Kategorie befindet. Dieses Muster kann verwendet werden, um separate Felder innerhalb von Metadaten zu codieren, aber nur mit dem ersten Feld übereinstimmen.
5. HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL) - Verbindet sich mit den Host- und URL-Parametern, die dann für den Abgleich verwendet werden können.

Responder-Aktionstypen

> **Hinweis:** In der Tabelle wird HTTP.REQ.URL als `<URL expression>` verallgemeinert.

In der folgenden Tabelle werden die Aktionen beschrieben, die auf eingehenden Internetverkehr angewendet werden können.

Responderaktion	Beschreibung
Zulassen	Erlauben Sie der Anforderung, auf die Ziel-URL zuzugreifen.
Umleiten	Leiten Sie die Anforderung an die URL um, die als Ziel angegeben ist.
Blockieren	Verweigern Sie die Anfrage.

Voraussetzungen

Konfigurieren Sie einen DNS-Server, wenn Sie einen URL-Set von einer Hostnamen-URL importieren. Diese Konfiguration ist nicht erforderlich, wenn Sie eine IP-Adresse verwenden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add dns nameServer ((<IP> [-local])| <dnsVserverName>)[-state (ENABLED |
```



```
DISABLED )] [-type <type>] [-dnsProfileName <string>]
```

Beispiel:

```
add dns nameServer 10.140.50.5
```

Konfigurieren einer URL-Liste

Zum Konfigurieren einer URL-Liste können Sie den Citrix SSL-Forward-Proxyassistenten oder die Citrix ADC Befehlszeilenschnittstelle (CLI) verwenden. Auf der Citrix ADC Appliance müssen Sie zuerst die Responder-Richtlinie konfigurieren und dann die Richtlinie an einen URL-Satz binden.

Citrix empfiehlt, den Citrix SSL-Forward-Proxyassistenten als bevorzugte Option zum Konfigurieren einer URL-Liste zu verwenden. Verwenden Sie den Assistenten, um eine Responder-Richtlinie an einen URL-Satz zu binden. Alternativ können Sie die Richtlinie an einen Mustersatz binden.

Konfigurieren einer URL-Liste mithilfe des SSL-Forward-Proxy-Assistenten

So konfigurieren Sie die URL-Liste für HTTPS-Datenverkehr mit der GUI:

1. Navigieren Sie zur Seite **Sicherheit** > **SSL Forward Proxy**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   a) Klicken Sie auf **SSL-Forward-Proxy-Assistent**.
   b) Wählen Sie eine vorhandene Konfiguration aus, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt **URL-Filterung** auf **Bearbeiten**.
4. Aktivieren Sie das Kontrollkästchen **URL-Liste**, um die Funktion zu aktivieren.
5. Wählen Sie eine **URL-Listenrichtlinie** aus, und klicken Sie auf **Binden**.
6. Klicken Sie auf **Weiter** und dann **Fertig**.

Weitere Informationen finden Sie unter Erstellen einer URL-Listenrichtlinie.

Konfigurieren einer URL-Liste mit der CLI

Gehen Sie folgendermaßen vor, um eine URL-Liste zu konfigurieren.

1. Konfigurieren Sie einen virtuellen Proxyserver für HTTP- und HTTPS-Datenverkehr.
2. Konfigurieren Sie SSL-Interception zum Abfangen des HTTPS-Datenverkehrs.
3. Konfigurieren Sie eine URL-Liste, die einen URL-Satz für HTTP-Datenverkehr enthält.
4. Konfigurieren Sie die URL-Liste mit URL-Satz für HTTPS-Datenverkehr.
5. Konfigurieren Sie einen privaten URL-Satz.

> **Hinweis:**

> Wenn Sie bereits eine ADC-Appliance konfiguriert haben, können Sie die Schritte 1 und 2 überspringen und mit Schritt 3 konfigurieren.

Konfigurieren eines virtuellen Proxyservers für den Internetverkehr

Die Citrix ADC Appliance unterstützt transparente und explizite Proxyserver. Gehen Sie folgendermaßen vor, um einen virtuellen Proxyserver für den Internetverkehr im expliziten Modus zu konfigurieren:

1. Fügen Sie einen virtuellen SSL-Proxyserver hinzu.
2. Binden Sie eine Responderrichtlinie an den virtuellen Proxyserver.

So fügen Sie einen virtuellen Proxyserver mit der CLI hinzu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cs vserver <name> <serviceType> <IPAddress> <port>
<!--NeedCopy-->
```

Beispiel:

```
add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
<!--NeedCopy-->
```

So binden Sie eine Responder-Richtlinie mit der CLI an einen virtuellen Proxyserver:

```
bind ssl vserver <vServerName> -policyName <string> [-priority <
   positive_integer>]
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn Sie den SSL-Interzeptor bereits als Teil der Citrix ADC Konfiguration konfiguriert haben, können Sie das folgende Verfahren überspringen.

Konfigurieren der SSL-Interception für HTTPS-Datenverkehr

Gehen Sie folgendermaßen vor, um SSL-Interception für HTTPS-Datenverkehr zu konfigurieren:

1. Binden Sie ein Zertifizierungsstellen-Schlüsselpaar an den virtuellen Proxyserver.
2. Aktivieren Sie das standardmäßige SSL-Profil.

3. Erstellen Sie ein Front-End-SSL-Profil, binden Sie es an den virtuellen Proxyserver und aktivieren Sie SSL-Interception im Front-End-SSL-Profil.

So binden Sie ein Zertifizierungsstellen-Schlüsselpaar mit der Befehlszeilenschnittstelle an den virtuellen Proxyserver:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>
<!--NeedCopy-->
```

So konfigurieren Sie ein Front-End-SSL-Profil mit der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl parameter -defaultProfile ENABLED

add ssl profile <name> -sslInterception ENABLED -ssliMaxSessPerServer <
   positive_integer>
<!--NeedCopy-->
```

So binden Sie ein Front-End-SSL-Profil mit der Befehlszeilenschnittstelle an einen virtuellen Proxyserver

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl vserver <vServer name>  -sslProfile <name>
<!--NeedCopy-->
```

Konfigurieren einer URL-Liste durch Importieren eines URL-Sets für HTTP-Datenverkehr

Informationen zum Konfigurieren eines URL-Sets für HTTP-Datenverkehr finden Sie unter URL-Set.

Explizite Subdomain-Übereinstimmung durchführen

Sie können jetzt eine explizite Subdomain-Übereinstimmung für einen importierten URL-Satz durchführen. Dem **`import`** `policy URLset` Befehl wird ein neuer Parameter, “SubDomainExactMatch”, hinzugefügt.

Wenn Sie den Parameter aktivieren, führt der URL-Filteralgorithmus eine explizite Subdomain-Übereinstimmung aus. Wenn beispielsweise die eingehende URL `news.example.com` ist und der Eintrag im URL-Satz, `example.com`erkennt der Algorithmus die URLs nicht als übereinstimmend.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import policy urlset <name> [-overwrite] [-delimiter <character>][-rowSeparator
 <character>] -url [-interval <secs>] [-privateSet][-subdomainExactMatch]
[-canaryUrl <URL>]
```

Beispiel

```
import policy urlset test -url http://10.78.79.80/top-1k.csv -privateSet -
subdomainExactMatch -interval 900
```

Konfigurieren eines URL-Sets für HTTPS-Datenverkehr

So konfigurieren Sie einen URL-Satz für HTTPS-Datenverkehr mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add ssl policy <name> -rule <expression> -action <string> [-undefAction
      <string>] [-comment <string>]
2 <!--NeedCopy-->
```

Beispiel:

```
1 add ssl policy pol1 -rule "client.ssl.client_hello.SNI.
     URLSET_MATCHES_ANY("top1m") -action INTERCEPT
2 <!--NeedCopy-->
```

So konfigurieren Sie einen URL-Satz für HTTPS-Datenverkehr mithilfe des SSL-Forward-Proxy-Assistenten

Citrix empfiehlt, den SSL-Forward-Proxyassistenten als bevorzugte Option zum Konfigurieren einer URL-Liste zu verwenden. Verwenden Sie den Assistenten, um einen benutzerdefinierten URL-Satz zu importieren und an eine Responderrichtlinie zu binden.

1. Navigieren Sie zu **Sicherheit > SSL-Forward-Proxy > URL-Filter > URL-Listen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie auf der Seite **URL-Listenrichtlinie** den Richtliniennamen an.
4. Wählen Sie eine Option aus, um einen URL-Satz zu importieren.
5. Aktivieren Sie auf der Registerkarte **URL-Listenrichtlinie** das Kontrollkästchen **URL-Satz importieren**, und geben Sie die folgenden URL-Set-Parameter an.
   a) URL-Set-Name — Name des benutzerdefinierten URL-Sets.
   b) URL: Die Webadresse des Standorts, an dem auf den URL-Satz zugegriffen werden soll.

c) Überschreiben — Überschreiben Sie einen zuvor importierten URL-Satz.
d) Trennzeichen: Eine Zeichenfolge, die einen CSV-Dateidatensatz begrenzt.
e) Zeilentrenner — In der CSV-Datei verwendetes Zeilentrenner.
f) Intervall — Intervall in Sekunden, abgerundet auf die nächste Anzahl von Sekunden, die 15 Minuten entspricht, bei der der URL-Satz aktualisiert wird.
g) Private Set: Option, um das Exportieren des URL-Sets zu verhindern.
h) Kanarische URL — Interne URL zum Testen, ob der Inhalt des URL-Sets vertraulich behandelt werden soll. Die maximale Länge der URL beträgt 2047 Zeichen.

6. Wählen Sie eine Responder-Aktion aus der Dropdownliste aus.
7. Klicken Sie auf **Erstellen** und **Schließen**.

Konfigurieren eines privaten URL-Sets

Wenn Sie einen privaten URL-Satz konfigurieren und den Inhalt vertraulich behandeln, kennt der Netzwerkadministrator möglicherweise die in der Sperrliste enthaltenen URLs nicht. In solchen Fällen können Sie eine Canary-URL konfigurieren und sie dem URL-Satz hinzufügen. Mit der Canary-URL kann der Administrator den privaten URL-Satz für jede Lookup-Anfrage anfordern. Beschreibungen der einzelnen Parameter finden Sie im Assistentenabschnitt.

So importieren Sie einen URL-Satz mit der CLI:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import policy urlset <name> [-overwrite] [-delimiter <character>] [-
    rowSeparator <character>] -url <URL> [-interval <secs>] [-privateSet
    ] [-canaryUrl <URL>]
<!--NeedCopy-->
```

Beispiel:

```
import policy urlset test1  -url http://10.78.79.80/alytra/top-1k.csv -
    private -canaryUrl http://www.in.gr
<!--NeedCopy-->
```

Importierte URL-Satz anzeigen

Sie können nun zusätzlich zu den hinzugefügten URL-Sets importierte URL-Sets anzeigen. Dem `show urlset` Befehl wird ein neuer Parameter “importiert” hinzugefügt. Wenn Sie diese Option aktivieren, zeigt die Appliance alle importierten URL-Sets an und unterscheidet die importierten URL-Sets von den hinzugefügten URL-Sets.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show policy urlset [<name>] [-imported]
```

Beispiel

```
show policy urlset -imported
```

Auditprotokoll-Messaging konfigurieren

Die Audit-Protokollierung ermöglicht es Ihnen, eine Bedingung oder eine Situation in einer beliebigen Phase eines URL-Listenprozesses zu überprüfen. Wenn eine Citrix ADC Appliance eine eingehende URL erhält und die Responder-Richtlinie über einen erweiterten Richtlinienausdruck zum Setzen von URL verfügt, sammelt die Überwachungsprotokollfunktion URL-Set-Informationen in der URL. Es speichert die Details als Protokollmeldung für jedes Ziel, das durch die Audit-Protokollierung zulässig ist.

Die Protokollmeldung enthält die folgenden Informationen:

1. Zeitstempel.
2. Protokollnachrichtentyp.
3. Die vordefinierten Protokollstufen (Critical, Error, Notice, Warning, Informational, Debug, Alert und Emergency).
4. Meldungsinformationen wie URL-Setname, Richtlinienaktion, URL protokollieren.

Um die Überwachungsprotokollierung für die URL-Liste zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

1. Überwachungsprotokoll aktivieren.
2. Aktion “Auditprotokoll erstellen”
3. Legen Sie die Richtlinie für URL-Listen-Responder mit Auditprotokoll-Nachrichtenaktion fest.

Weitere Informationen finden Sie unter Thema Überwachungsprotokollierung .

URL-Mustersemantik

October 5, 2021

Die folgende Tabelle zeigt die URL-Muster, die zum Angeben der Liste der Seiten verwendet werden sollen, die gefiltert werden sollen. Beispielsweise entspricht das Muster www.example.com/bar nur einer Seite unter www.example.com/bar. Um alle Seiten zu vergleichen, deren URL mit ‘www.example.com/bar’ beginnt, fügen Sie am Ende der URL ein Sternchen (*) hinzu.

Semantik für URL-Muster, um Metadatenzuordnung anzupassen

Die Musterübereinstimmende Semantik ist in einem Tabellenformat verfügbar. Weitere Informationen finden Sie auf der PDF-Seite Pattern Semantik .

Zuordnen von URL-Kategorien

October 5, 2021

Eine Liste von Drittanbieterkategorien und Kategoriegruppen. Weitere Informationen finden Sie auf der Seite URL-Kategorie-Zuordnung .

Anwendungsfall: URL-Filterung mithilfe eines benutzerdefinierten URL-Sets

April 25, 2022

Wenn Sie ein Unternehmenskunde sind, der den Zugriff auf bestimmte Websites und Website-Kategorien steuern möchte, verwenden Sie einen benutzerdefinierten URL-Satz, der an eine Responder-Richtlinie gebunden ist. Die Netzwerkinfrastruktur Ihres Unternehmens kann einen URL-Filter verwenden, um den Zugriff auf schädliche oder gefährliche Websites zu blockieren. Zum Beispiel Websites mit Erwachsenen-, Gewalt-, Spiel-, Drogen-, Politik- oder Jobportalen. Sie können nicht nur die URLs filtern, sondern auch eine benutzerdefinierte Liste von URLs erstellen und in die ADC-Appliance importieren. Die Richtlinien Ihres Unternehmens könnten beispielsweise die Sperrung des Zugriffs auf bestimmte Websites wie soziale Netzwerke, Einkaufsportale und Jobportale vorsehen.

Jede URL in der Liste kann eine benutzerdefinierte Kategorie in Form von Metadaten haben. Die Organisation kann die Liste der URLs als URL hosten, die auf der Citrix ADC Appliance festgelegt ist. Konfigurieren Sie das Gerät so, dass das Gerät regelmäßig aktualisiert wird, ohne dass ein manueller Eingriff

Nachdem das Set aktualisiert wurde, erkennt die Citrix ADC Appliance die Metadaten automatisch. Die Responder-Richtlinie verwendet die URL-Metadaten (Kategoriedetails), um die eingehende URL auszuwerten und eine Aktion wie Zulassen, Blockieren, Umleiten oder Benachrichtigen des Benutzers anzuwenden.

Konfigurieren Sie dazu in Ihrem Netzwerk die folgenden Aufgaben:

1. Importieren eines benutzerdefinierten URL-Sets
2. Fügen Sie einen benutzerdefinierten URL-Satz hinzu
3. Konfigurieren Sie eine benutzerdefinierte URL-Liste im SSL-Forward-Proxy-Assistenten.

Importieren einer benutzerdefinierten URL, die über die CLI festgelegt wurde

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
import policy urlset <name> [-overwrite] [-delimiter <character>] [-
   rowSeparator <character>] -url <URL> [-interval <secs>] [-privateSet
   ] [-canaryUrl <URL>]

import policy urlset test1  -url http://10.78.79.80/alytra/top-1k.csv
<!--NeedCopy-->
```

Fügen Sie eine benutzerdefinierte URL hinzu, die über die CLI festgelegt wurde

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add urlset <urlset_name>
```

Beispiel:

```
add urlset test1
```

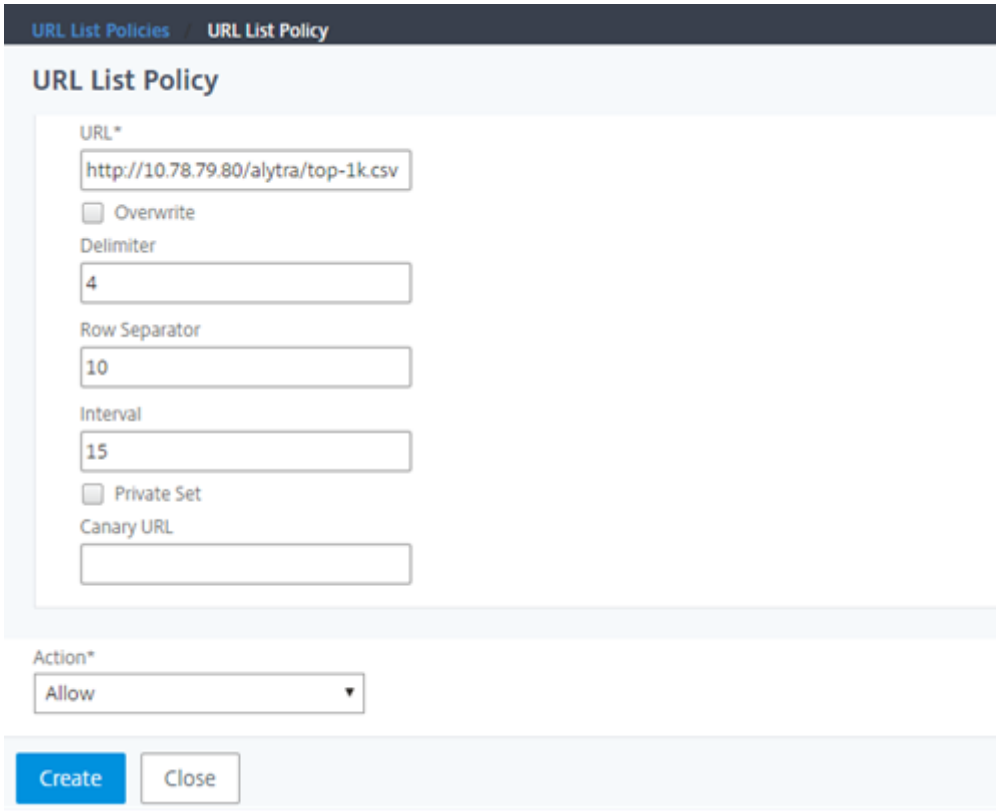
Konfigurieren einer URL-Liste mithilfe des SSL-Forward-Proxy-Assistenten

Citrix empfiehlt, den SSL-Forward-Proxy-Assistenten als bevorzugte Option zum Konfigurieren einer URL-Liste zu verwenden. Verwenden Sie den Assistenten, um einen benutzerdefinierten URL-Satz zu importieren und ihn an eine Responder-Richtlinie zu binden.

1. Navigieren Sie zu **Sicherheit > SSL-Weiterleitungsproxy > URL-Filter > URL-Listen**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Geben Sie auf der Seite “ **Richtlinie für URL-Liste** “ den Richtliniennamen an.
4. Wählen Sie eine Option aus, um entweder einen URL-Satz zu importieren.
5. Aktivieren Sie auf der Registerkarte “ **URL-Listenrichtlinie** “ das Kontrollkästchen **URL-Satz importieren** und geben Sie die folgenden URL-Set-Parameter an.
   a) URL-Set-Name — Name des benutzerdefinierten URL-Sets.
   b) URL—Webadresse des Standorts, an dem auf den URL-Set zugegriffen werden soll.
   c) Überschreiben — Überschreibt einen zuvor importierten URL-Satz.
   d) Trennzeichen—Zeichensequenz, die einen CSV-Dateidatensatz begrenzt.
   e) Zeilentrenner— In der CSV-Datei verwendetes Zeilentrennzeichen.
   f) Intervall — Intervall in Sekunden, abgerundet auf die nächsten 15 Minuten, in denen der URL-Satz aktualisiert wird.
   g) Private Set—Option, um das Exportieren des URL-Sets zu verhindern.

h) Canary URL — Interne URL zum Testen, ob der Inhalt des URL-Sets vertraulich behandelt werden soll. Die maximale Länge der URL beträgt 2047 Zeichen.

6. Wählen Sie eine Responder Action aus der Dropdownliste aus.
7. Klicken Sie auf **Erstellen** und **Schließen**.



Metadaten-Semantik für benutzerdefinierte URL-Sets

Um einen benutzerdefinierten URL-Satz zu importieren, fügen Sie die URLs zu einer Textdatei hinzu und binden Sie sie an eine Responder-Richtlinie, um URLs für soziale Netzwerke zu blockieren.

Im Folgenden finden Sie Beispiele für URLs, die Sie der Textdatei hinzufügen könnten:

cnn.com, Nachrichten

bbc.com, Nachrichten

google.com, Suchmaschine

yahoo.com, Suchmaschine

facebook.com, Soziale Netzwerke

twitter.com, Soziale Netzwerke

Konfigurieren einer Responder-Richtlinie zum Blockieren von Social-Media-URLs mit der CLI

```
add responder action act_url_unauthorized respondwith '"HTTP/1.1 451
    Unavailable For Legal Reasons\r\n\r\nURL is NOT authorized\n"'

add responder policy pol_url_meta_match 'HTTP.REQ.HOSTNAME.APPEND(HTTP.
    REQ.URL).GET_URLSET_METADATA("u1").EQ("Social Media")'
    act_url_unauthorized
<!--NeedCopy-->
```

URL-Kategorisierung

May 10, 2022

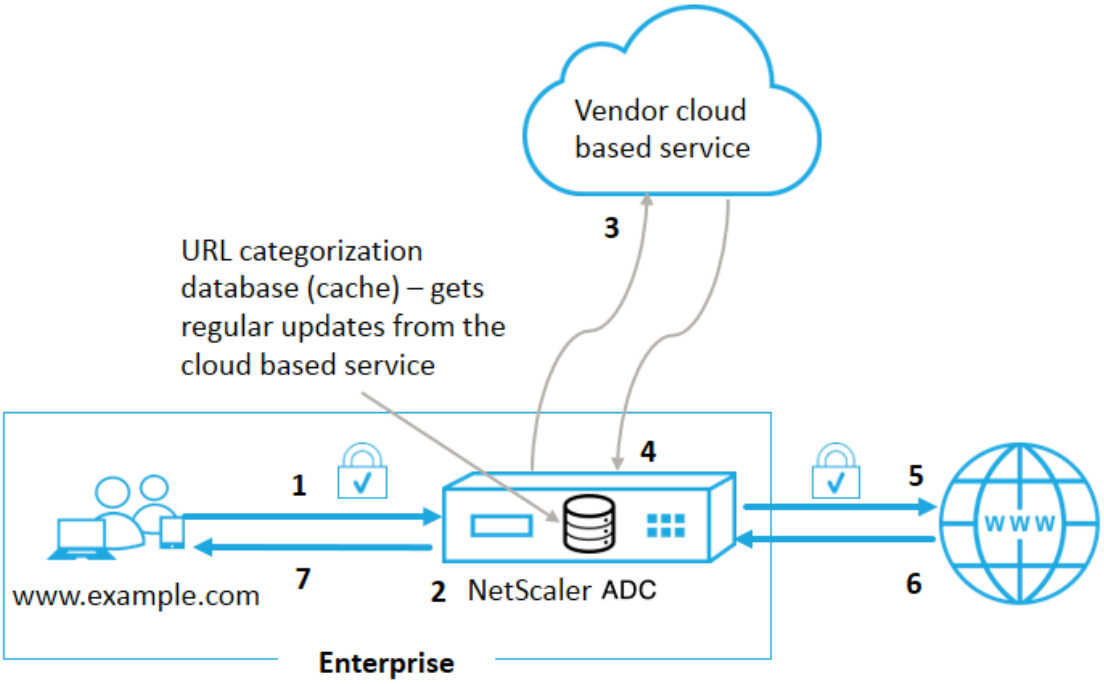
Die URL-Kategorisierung beschränkt den Benutzerzugriff auf bestimmte Websites und Website-Kategorien. Als abonnierter Dienst in Zusammenarbeit mit ermöglicht die Funktion Unternehmen-skunden NetSTAR, den Webverkehr mithilfe einer kommerziellen Kategorisierungsdatenbank zu filtern. Die NetSTAR-Datenbank enthält eine große Anzahl (Milliarden) von URLs, die in verschiedene Kategorien eingeteilt sind, z. B. soziale Netzwerke, Glücksspiele, Inhalte für Erwachsene, neue Medien und Shopping. Zusätzlich zur Kategorisierung hat jede URL eine Reputationsbewertung, die basierend auf dem historischen Risikoprofil der Website auf dem neuesten Stand gehalten wird. Wir können NetSTAR-Daten verwenden, um den Datenverkehr zu filtern, indem wir erweiterte Richtlinien basierend auf Kategorien, Kategoriegruppen (wie Terrorismus, illegale Drogen) oder Reputationsbewertungen für Websites konfigurieren.

Sie könnten beispielsweise den Zugriff auf gefährliche Websites blockieren, z. B. Websites, von denen bekannt ist, dass sie mit Malware infiziert sind. Sie können auch selektiv den Zugriff auf Inhalte wie Inhalte für Erwachsene oder Unterhaltungsstreaming-Medien für Unternehmensbenutzer einschränken. Sie können auch die Transaktionsdetails des Benutzers und die Details des ausgehenden Datenverkehrs erfassen, um die Analyse des Webverkehrs auf dem Citrix ADM-Server zu überwachen.

Citrix ADC lädt Daten vom vorkonfigurierten NetSTAR-Gerät nsv10.netstar-inc.com hoch oder lädt sie herunter und incompasshybridpc.netstar-inc.com wird standardmäßig als Cloudhost für Cloudkategorisierungsanfragen verwendet. Diese URLs müssen über die Firewall zugänglich sein, damit die URL-Filterung ordnungsgemäß funktioniert. Die Appliance verwendet ihre NSIP-Adresse als Quell-IP-Adresse und 443 als Zielport für die Kommunikation.

Funktionsweise der URL-Kategorisierung

Die folgende Abbildung zeigt, wie ein Citrix ADC URL-Kategorisierungsdienst in eine kommerzielle URL-Kategorisierungsdatenbank und Cloud-Dienste für häufige Updates integriert ist.



Die Komponenten interagieren wie folgt:

1. Ein Client sendet eine internetgebundene URL-Anfrage.
2. Der SSL-Forward-Proxy wendet eine Richtliniendurchsetzung auf die Anforderung an, die auf den Kategoriedetails wie Kategorie, Kategoriegruppe und Site-Reputationsbewertung basiert. Die Kategoriedetails werden aus der Datenbank zur URL-Kategorisierung abgerufen. Wenn die Datenbank die Kategoriedetails zurückgibt, springt der Prozess zu Schritt 5.
3. Wenn in der Datenbank die Kategorisierungsdetails fehlen, wird die Anforderung an einen Cloud-basierten Suchdienst gesendet, der von einem Anbieter der URL-Kategorisierung verwaltet wird. Die Appliance wartet jedoch nicht auf eine Antwort, stattdessen wird die URL als nicht kategorisiert gekennzeichnet und eine Richtliniendurchsetzung wird durchgeführt (weiter zu Schritt 5). Die Appliance überwacht weiterhin das Feedback der Cloud-Abfrage und aktualisiert den Cache, sodass zukünftige Anfragen vom Cloud-Lookup profitieren können.
4. Die ADC-Appliance erhält die URL-Kategoriedetails (Kategorie, Kategoriegruppe und Reputationsbewertung) vom Cloud-basierten Dienst und speichert sie in der Kategorisierungsdatenbank.
5. Die Richtlinie erlaubt die URL und die Anfrage wird an den Original-Server gesendet. Andernfalls verwirft die Appliance, leitet sie um oder antwortet mit einer benutzerdefinierten HTML-Seite.

6. Der Original-Server antwortet mit den angeforderten Daten an die ADC-Appliance.
7. Die Appliance sendet die Antwort an den Client.

Anwendungsfall: Internetnutzung unter Einhaltung von Unternehmensrichtlinien für Unternehmen

Sie können die URL-Filter-Funktion verwenden, um Compliance-Richtlinien zu erkennen und zu implementieren, um Websites zu blockieren, die gegen die Unternehmenskonformität verstoßen. Zum Beispiel Websites wie Erwachsene, Streaming-Medien und soziale Netzwerke, die als nicht produktiv angesehen werden können oder in einem Unternehmensnetzwerk überschüssige Internetbandbreite verbrauchen. Die Sperrung des Zugriffs auf diese Websites kann die Produktivität der Mitarbeiter verbessern, die Betriebskosten für die Bandbreitennutzung senken und den Gemeinkosten des Netzwerkverbrauchs reduzieren.

Voraussetzungen

Die Funktion zur URL-Kategorisierung funktioniert auf einer Citrix ADC-Plattform nur, wenn sie über einen optionalen Abonnementdienst mit URL-Filterfunktionen und Bedrohungsinformationen für SSL-Forward-Proxy verfügt Mit dem Abonnement können Kunden die neuesten Bedrohungskategorisierungen für Websites herunterladen und diese Kategorien dann für den SSL-Forward-Proxy durchsetzen. Bevor Sie die Funktion aktivieren und konfigurieren, müssen Sie die folgenden Lizenzen installieren:

- CNS_WEBF_SSERVER_Retail.lic
- CNS_XXXX_SERVER_PLT_Retail.lic

Wobei XXXXX der Plattformtyp ist, zum Beispiel: V25000

Richtlinienausdrücke für Resp

In der folgenden Tabelle sind die verschiedenen Richtlinienausdrücke aufgeführt, mit denen Sie überprüfen können, ob eine eingehende URL zulässig, umgeleitet oder gesperrt sein muss.

1. `<text>. URL_CATEGORIZE (<min_reputation>, <max_reputation>)` - Gibt ein URL_CATEGORY-Objekt zurück. Wenn `<min_reputation>` größer als 0 ist, enthält das zurückgegebene Objekt keine Kategorie mit einer niedrigeren Reputation als `<min_reputation>`. Wenn `<max_reputation>` größer als 0 ist, enthält das zurückgegebene Objekt keine Kategorie mit einer höheren Reputation als `<max_reputation>`. Wenn die Kategorie nicht rechtzeitig aufgelöst wird, wird der undef-Wert zurückgegeben.
2. `<url_category>. CATEGORY()` - Gibt die Kategorie für dieses Objekt zurück. Wenn die URL keine Kategorie hat oder wenn die URL fehlerhaft ist, ist der zurückgegebene Wert “Unbekannt”.

3. <url_category>. CATEGORY_GROUP() - Gibt eine Zeichenfolge zurück, die die Kategoriegruppe des Objekts identifiziert. Bei dieser Gruppierung handelt es sich um eine übergeordnete Gruppierung von Kategorien, die bei Vorgängen nützlich ist, die weniger detaillierte Informationen über die URL-Kategorie benötigen. Wenn die URL keine Kategorie hat oder wenn die URL fehlerhaft ist, ist der zurückgegebene Wert "Unbekannt".
4. <url_category>. REPUTATION() - Gibt den Reputationswert als Zahl von 0 bis 5 zurück, wobei 5 den riskantesten Ruf angibt. Wenn es die Kategorie "Unbekannt" gibt, ist der Reputationswert 1.

Policy-Typen:

1. Richtlinie zum Auswählen von Anfragen für URLs, die in der Suchmaschinenkategorie enthalten sind - add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY().EQ("Search Engine")
2. Richtlinie zur Auswahl von Anfragen für URLs, die in der Kategorie "Erwachsene" enthalten sind - add responder policy p1 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY_GROUP().EQ("Adult")'
3. Richtlinie zur Auswahl von Anfragen für Suchmaschinen-URLs mit einem Reputationswert von weniger als 4 — add responder policy p2 'HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL).URL_CATEGORIZE(4,0).HAS_CATEGORY("Search Engine")
4. Richtlinie zur Auswahl von Anfragen für Suchmaschinen und Einkaufs-URLs - add responder policy p3 'HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URL_CATEGORIZE(0,0).CATEGORY().EQ ("good_categories")
5. Richtlinie zur Auswahl von Anfragen für Suchmaschinen-URLs mit einer Reputationsbewertung von mindestens 4 - add responder policy p5 'CLIENT.SSL.DETECTED_DOMAIN.URL_CATEGORIZE(4,0). CATEGORY().EQ("Search Engines")
6. Richtlinie, um Anfragen für URLs auszuwählen, die sich in der Suchmaschinenkategorie befinden, und diese mit einem URL-Satz zu vergleichen - 'HTTP.REQ.HOSTNAME.APPEND (HTTP.REQ.URL).URL_CATEGORIZE(0,0). CATEGORY().EQ("Search Engine")&& HTTP.REQ.HOSTNAME.APPEND(HTTP.REQ.URL).URLSET_MATCHES_ANY("u1")'

Responder-Richtlinientypen

In einer Funktion zur URL-Kategorisierung werden zwei Arten von Richtlinien verwendet, und jeder dieser Richtlinientypen wird in der folgenden Tabelle erläutert:

Richtlinientyp	Beschreibung
URL-Kategorie	Kategorisieren Sie den Webverkehr und blockieren, erlauben oder leiten Sie den Datenverkehr basierend auf den Bewertungsergebnissen

Richtlinientyp	Beschreibung
URL-Reputationsbewertung	Bestimmt den Reputationswert der Website und ermöglicht Ihnen, den Zugriff basierend auf dem vom Administrator festgelegten Schwellenwert für die Reputationsbewertung zu steuern.

Konfigurieren der URL Kategorisierung

Gehen Sie wie folgt vor, um die URL-Kategorisierung auf einer Citrix ADC-Appliance zu konfigurieren:

1. URL-Filterung aktivieren.
2. Konfigurieren Sie einen Proxyserver für den Webverkehr.
3. Konfigurieren Sie das SSL-Abfangen für den Webverkehr im expliziten Modus.
4. Konfigurieren Sie gemeinsamen Speicher, um den Cache-Speicher zu begrenzen
5. Konfigurieren der URL-Kategorisierungsparameter
6. Konfigurieren der URL-Kategorisierung mithilfe des Citrix SSL-Forward-Proxy-Assistenten.
7. Konfigurieren Sie die URL-Kategorisierungsparameter mithilfe des SSL-Weiterleitungsproxy-Assistenten
8. Konfigurieren des Seeddatenbankpfads und des Cloud-Servernamens

Schritt 1: URL-Filterung aktivieren

Um die URL-Kategorisierung zu aktivieren, aktivieren Sie die URL-Filterfunktion und Modi für die URL-Kategorisierung.

So aktivieren Sie die URL-Kategorisierung mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns feature URLFiltering

disable ns feature URLFiltering
```

Schritt 2: Konfigurieren eines Proxyservers für den Webverkehr im expliziten Modus

Die Citrix ADC-Appliance unterstützt transparente und explizite virtuelle Proxyserver. Gehen Sie wie folgt vor, um einen virtuellen Proxyserver für SSL-Datenverkehr im expliziten Modus zu konfigurieren:

1. Fügen Sie einen Proxyserver hinzu.
2. Binden einer SSL-Richtlinie an den Proxyserver.

So fügen Sie einen Proxyserver mit der CLI hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add cs vserver <name> [-td <positive_integer>] <serviceType> [-cltTimeout <
secs>]
```

Beispiel:

```
add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180
```

Binden einer SSL-Richtlinie mithilfe der CLI an einen virtuellen Proxyserver

```
bind ssl vserver <vServerName> -policyName <string> [-priority <positive_integer
>]
```

Schritt 3: SSL-Abfangen für den HTTPS-Verkehr konfigurieren

Gehen Sie wie folgt vor, um das SSL-Abfangen für den HTTPS-Verkehr zu konfigurieren:

1. Binden Sie ein CA-Zertifikatsschlüsselpaar an den virtuellen Proxyserver.
2. Konfigurieren Sie das standardmäßige SSL-Profil mit SSL-Parametern.
3. Binden Sie ein Front-End-SSL-Profil an den virtuellen Proxyserver und aktivieren Sie das SSL-Abfangen im Front-End-SSL-Profil.

So binden Sie ein CA-Zertifikatsschlüsselpaar mithilfe der CLI an den virtuellen Proxyserver

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName> -CA -
skipCAName
```

So konfigurieren Sie das Standard-SSL-Profil mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl profile <name> -denySSLReneg <denySSLReneg> -sslInterception (
ENABLED | DISABLED)-ssliMaxSessPerServer positive_integer>
```

Binden Sie ein Front-End-SSL-Profil mithilfe der CLI an einen virtuellen Proxyserver

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ssl vserver <vServer name> -sslProfile ssl_profile_interception
```


Schritt 4: Konfigurieren Sie Shared Memory, um den Cache-Speicher

So konfigurieren Sie Shared Memory zur Begrenzung des Cache-Speichers mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set cache parameter [-memLimit <megaBytes>]
```

Wobei das für das Caching konfigurierte Speicherlimit auf 10 MB festgelegt ist.

Schritt 5: Konfigurieren der URL-Kategorisierungsparameter

So konfigurieren Sie die URL-Kategorisierungsparameter mithilfe der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>] [-
TimeOfDayToUpdateDB <HH:MM>]
```

Beispiel:

```
set urlfiltering parameter -urlfilt_hours_betweenDB_updates 20
```

Schritt 6: Konfigurieren der URL-Kategorisierung mithilfe des Citrix SSL-Forward-Proxy-Assistenten

1. Melden Sie sich bei der Citrix ADC-Appliance an und navigieren Sie zur Seite **Sicherheit** > **SSL Forward Proxy** .
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   a) Klicken Sie auf **SSL Forward Proxy Wizard**, um eine neue Konfiguration
   b) Wählen Sie eine vorhandene Konfiguration aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie im Abschnitt “ **URL-Filter** “ auf **Bearbeiten**.
4. Wählen Sie das Kontrollkästchen **URL-Kategorisierung**, um die Funktion zu aktivieren
5. Wählen Sie eine **URL-Kategorisierungsrichtlinie** aus und **klicken**Sie auf
6. Klicken Sie auf **Weiter** und dann **Fertig**.

Weitere Informationen zur URL-Kategorisierungsrichtlinie finden Sie unter Erstellen einer URL-Kategorisierungsrichtlinie.

Schritt 7: Konfigurieren von URL-Kategorisierungsparametern mit einem SSL-Forward-Proxy-Assistenten

1. Melden Sie sich bei der **Citrix ADC-Appliance** an und navigieren Sie zu **Sicherheit > URL-Filter**.
2. Klicken Sie auf der Seite “ **URL-Filter** “ auf den Link **URL-Filtereinstellungen ändern** .
3. Geben **Sie auf der Seite Konfigurieren von URL-Filterparametern** die folgenden Parameter an.

a) Stunden zwischen DB-Aktualisierungen. Stunden des URL-Filters zwischen Datenbankaktualisierungen Minimalwert: 0 und Maximalwert: 720.
b) Tageszeit zur Aktualisierung der DB. Uhrzeit des URL-Filters zum Aktualisieren der Datenbank.
c) Cloud-Host. Der URL-Pfad des Cloud-Servers.
d) Seed-DB-Pfad. Der URL-Pfad des Seed-Datenbank-Suchservers.

4. Klicken Sie auf **OK** und **Schließen**.

Beispiel-Konfiguration:

```
enable ns feature LB CS SSL IC RESPONDER AppFlow URLFiltering

enable ns mode FR L3 Edge USNIP PMTUD

set ssl profile ns_default_ssl_profile_frontend -denySSLReneg NONSECURE
    -sslInterception ENABLED -ssliMaxSessPerServer 100

add ssl certKey swg_ca_cert -cert ns_swg_ca.crt -key ns_swg_ca.key

set cache parameter -memLimit 100

add cs vserver starcs PROXY 10.102.107.121 80 -cltTimeout 180

add responder action act1 respondwith ""HTTP/1.1 200 OK\r\n\r\n" + http
   .req.url.url_categorize(0,0).reputation + "\n""

add responder policy p1 "HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
   Shopping/Retail") || HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.eq("
   Search Engines & Portals

")" act1

bind cs vserver starcs_PROXY -policyName p1 -priority 10 -
   gotoPriorityExpression END -type REQUEST

add dns nameServer 10.140.50.5

set ssl parameter -denySSLReneg NONSECURE -defaultProfile ENABLED -
   sigDigestType RSA-MD5 RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-
   SHA512 -ssliErrorCache ENABLED

-ssliMaxErrorCacheMem 100000000

```



```
27 add ssl policy pol1 -rule "client.ssl.origin_server_cert.subject.
      URL_CATEGORIZE(0,0).CATEGORY.eq("Search Engines & Portals")"" -
      action INTERCEPT
28
29 add ssl policy pol3 -rule "client.ssl.origin_server_cert.subject.ne("
      citrix")" -action INTERCEPT
30
31 add ssl policy swg_pol -rule "client.ssl.client_hello.SNI.
      URL_CATEGORIZE(0,0).CATEGORY.ne("Uncategorized")" -action INTERCEPT
32
33 set urlfiltering parameter -HoursBetweenDBUpdates 3 -
      TimeOfDayToUpdateDB 03:00
34 <!--NeedCopy-->
```

Konfigurieren des Seeddatenbankpfads und des Cloud-Servernamens

Sie können jetzt den Seed-Datenbankpfad und den Namen des Cloud-Lookup-Servers für die manuelle Einstellung des Cloud-Lookup-Servernamens und des Seed-Datenbankpfads konfigurieren. Zu diesem Zweck werden zwei neue Parameter, "CloudHost" und "SeedDBPath", zum URL-Filterparameter hinzugefügt.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set urlfiltering parameter [-HoursBetweenDBUpdates <positive_integer>] [-
TimeOfDayToUpdateDB <HH:MM>] [-LocalDatabaseThreads <positive_integer>] [-
CloudHost <string>] [-SeedDBPath <string>]
```

Beispiel:

```
set urlfiltering parameter -HoursBetweenDBUpdates 3 -TimeOfDayToUpdateDB
03:00 -CloudHost localhost -SeedDBPath /mypath
```

Die Kommunikation zwischen einer Citrix ADC-Appliance und `NetSTAR` erfordert möglicherweise einen Domänennamenserver. Sie können mit einer einfachen Konsolen- oder Telnet-Verbindung von der Appliance aus testen.

Beispiel:

```
1 root@ns# telnet nsv10.netstar-inc.com 443
2 Trying 1.1.1.1...
3 Connected to nsv10.netstar-inc.com.
4 Escape character is '^]'.
5
6 root@ns# telnet incompasshybridpc.netstar-inc.com 443
```



```
Trying 10.10.10.10...
Connected to incompasshybridpc.netstar-inc.com.
Escape character is '^]'.
<!--NeedCopy-->
```

Konfigurieren des Überwachungsprotokolls

Mit der Überwachungsprotokollierung können Sie einen Zustand oder eine Situation in jeder Phase des URL-Kategorisierungsprozesses überprüfen. Wenn eine Citrix ADC-Appliance eine eingehende URL empfängt und die Responder Policy über einen URL-Filterausdruck verfügt, sammelt die Überwachungsprotokollfunktion URL-Set-Informationen in der URL. Es speichert die Informationen als Protokollmeldungen für jedes Ziel, das von der Überwachungsprotokollierung zugelassen ist.

- Quell-IP-Adresse (die IP-Adresse des Clients, der die Anfrage gestellt hat).
- Ziel-IP-Adresse (die IP-Adresse des angeforderten Servers).
- Angeforderte URL mit dem Schema, dem Host und dem Domainnamen (http://www.example.com).
- URL-Kategorie, die das URL-Filterframework zurückgibt.
- URL-Kategoriegruppe, die vom URL-Filterframework zurückgegeben wurde
- Die vom URL-Filter-Framework zurückgegebene URL-Reputationsnummer
- Von der Richtlinie durchgeführte Auditprotokollaktion.

Um die Überwachungsprotokollierung für eine Funktion der URL-Liste zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

1. Überwachungsprotokoll aktivieren.
2. Aktion “Überwachungsprotokollmeldung erstellen”
3. Legen Sie die Richtlinie für URL-Listen-Responder mit Auditprotokoll-Nachrichtenaktion fest.

Weitere Informationen finden Sie unter Thema Überwachungsprotokollierung .

Speichern von Fehler mit SYSLOG-Messaging

In jeder Phase des URL-Filtervorgangs verwendet die ADC-Appliance bei einem Fehler auf Systemebene den Überwachungsprotokollmechanismus, um Protokolle in der Datei ns.log zu speichern. Die Fehler werden als Textnachrichten im SYSLOG-Format gespeichert, sodass ein Administrator sie später in einer chronologischen Reihenfolge des Ereignisses anzeigen kann. Diese Protokolle werden auch zur Archivierung an einen externen SYSLOG-Server gesendet. Weitere Informationen finden Sie im Artikel CTX229399.

Wenn beispielsweise ein Fehler auftritt, wenn Sie das URL-Filter-SDK initialisieren, wird die Fehlermeldung im folgenden Nachrichtenformat gespeichert.


```
Oct 3 15:43:40 <local0.err> ns URLFiltering[1349]: Error initializing
NetStar SDK (SDK error=-1). (status=1).
```

Die Citrix ADC-Appliance speichert die Fehlermeldungen in vier verschiedenen Fehlerkategorien:

- **Fehler beim Herunterladen**. Wenn beim Versuch, die Kategorisierungsdatenbank herunterzuladen, ein Fehler auftritt.
- **Scheitern der Integration**. Wenn ein Fehler auftritt, wenn Sie ein Update in die vorhandene Kategorisierungsdatenbank integrieren.
- **Fehler bei der Initialisierung**. Wenn bei der Initialisierung der Funktion zur URL-Kategorisierung ein Fehler auftritt, legen Sie Kategorisierungsparameter fest oder beenden Sie einen Kategorisierungsdienst.
- **Fehler beim Abrufen**. Wenn ein Fehler auftritt, wenn die Appliance die Kategorisierungsdetails der Anforderung abruft.

Konfigurieren von SNMP-Traps für NetStar-Ereignisse

Die Funktion “URL-Filter” generiert SNMP-Traps, wenn die folgenden Bedingungen eintreten:

- NetStar-Datenbank-Update schlägt fehl oder ist erfolgreich.
- Die NetStar SDK-Initialisierung schlägt fehl oder ist erfolgreich.

Die Appliance verfügt über eine Reihe von bedingten Einheiten, die als SNMP-Alarme bezeichnet werden Wenn eine Bedingung im SNMP-Alarm erfüllt ist, generiert die Appliance Traps und sendet sie an ein bestimmtes Trap-Ziel. Wenn beispielsweise die NetStar SDK-Initialisierung fehlschlägt, wird eine SNMP-OID 1.3.6.1.4.1.5951.1.1.0.183 generiert und an das Trap-Ziel gesendet.

Damit die Appliance Traps generiert, müssen Sie zunächst SNMP-Alarme aktivieren und konfigurieren. Anschließend geben Sie das Trap-Ziel an, an das die Appliance die generierten Trap-Nachrichten sendet.

Aktivieren eines SNMP-Alarms

Die Citrix ADC-Appliance generiert Traps nur für aktivierte SNMP-Alarme. Einige Alarme sind standardmäßig aktiviert, aber Sie können sie deaktivieren.

Wenn Sie einen SNMP-Alarm aktivieren, generiert die URL-Filterfunktion Trap-Meldungen, wenn ein Erfolgs- oder Miserfolgsereignis eintritt. Einige Alarme sind standardmäßig aktiviert.

So aktivieren Sie einen SNMP-Alarm mit der Befehlszeilenschnittstelle:

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


```
enable snmp alarm <trapName>
show snmp alarm <trapName>
```

So aktivieren Sie einen SNMP-Alarm mithilfe der Citrix ADC GUI

1. Navigieren Sie zu **System** > **SNMP** > **Alarme**, und wählen Sie den Alarm aus.
2. Klicken Sie auf **Aktionen** und wählen Sie **Aktivieren**

Konfigurieren des SNMP-Alarms mithilfe der CLI

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

```
set snmp alarm <trapName> [-thresholdValue <positive_integer> [-normalValue
 <positive_integer>]] [-time <secs>] [-state ( ENABLED | DISABLED )] [-
severity <severity>] [-logging ( ENABLED | DISABLED )]
```

Beispiel:

```
set snmp alarm URL-FIL-DB-UPDATE-STATUS -state ENABLED
set snmp alarm URL-FIL-INIT-SDK -state ENABLED
```

Konfigurieren von SNMP-Alarmen mit der GUI

Navigieren Sie zu **System** > **SNMP** > **Alarme**, wählen Sie einen Alarm aus und konfigurieren Sie die Alarmparameter.

Weitere Informationen zu SNMP-Traps finden Sie unter SNMP

URL-Reputationsbewertung

October 5, 2021

Die URL-Kategorisierungsfunktion bietet richtlinienbasierte Steuerung, um URLs in der Sperrliste einzuschränken. Sie können den Zugriff auf Websites basierend auf URL-Kategorie, Reputationsbewertung oder URL-Kategorie und Reputationsbewertung steuern. Wenn Netzwerkadministratoren einen Benutzer überwachen, der auf hochriskante Websites zugreift, können sie eine an den URL-Reputationswert gebundene Responder-Richtlinie verwenden, um solche riskanten Websites zu blockieren.

Nach Erhalt einer eingehenden URL-Anforderung ruft die Appliance die Kategorie- und Reputationsbewertung aus der URL-Kategorisierungsdatenbank ab. Basierend auf der von der Datenbank zurückgegebenen Reputationsbewertung weist die Appliance Websites eine Reputationsbewertung zu. Der Wert kann zwischen 1 und 4 liegen, wobei 4 der risikoreichste Typ von Websites ist, wie in der folgenden Tabelle dargestellt.

URL-Reputationsbewertung	Reputationskommentar
1	Saubere Website
2	Unbekannte Website
3	Potenziell gefährlich oder mit einer gefährlichen Site verbunden
4	Bösartige Website

Anwendungsfall: Filtern nach URL-Reputationsbewertung

Betrachten Sie eine Unternehmensorganisation mit einem Netzwerkadministrator, der Benutzertransaktionen und Netzwerkbandbreitenverbrauch überwacht. Wenn Malware in das Netzwerk gelangen kann, muss der Administrator die Datensicherheit verbessern und den Zugriff auf bösartige und gefährliche Websites kontrollieren, die auf das Netzwerk zugreifen. Um das Netzwerk vor solchen Bedrohungen zu schützen, kann der Administrator die URL-Filterfunktion so konfigurieren, dass der Zugriff nach URL-Reputationsbewertung zugelassen oder verweigert wird.

Weitere Informationen zur Überwachung des ausgehenden Datenverkehrs und der Benutzeraktivitäten im Netzwerk finden Sie unter Analytics.

Wenn ein Mitarbeiter der Organisation versucht, auf eine Social-Networking-Website zuzugreifen, erhält die ADC-Appliance eine URL-Anfrage. Es fragt die URL-Kategorisierungsdatenbank ab, um die URL-Kategorie als soziales Netzwerk und eine Reputationsbewertung 3 abzurufen, was auf eine potenziell gefährliche Website hinweist. Die Appliance überprüft dann die vom Administrator konfigurierte Sicherheitsrichtlinie, z. B. den Zugriff auf Websites mit einer Reputationsbewertung von 3 oder mehr. Anschließend wendet er die Richtlinienaktion an, um den Zugriff auf die Website zu kontrollieren.

Um dieses Feature zu implementieren, müssen Sie mithilfe des SSL-Forward-Proxy-Assistenten die URL-Reputationsbewertung und die Sicherheitsschwellenstufen konfigurieren.

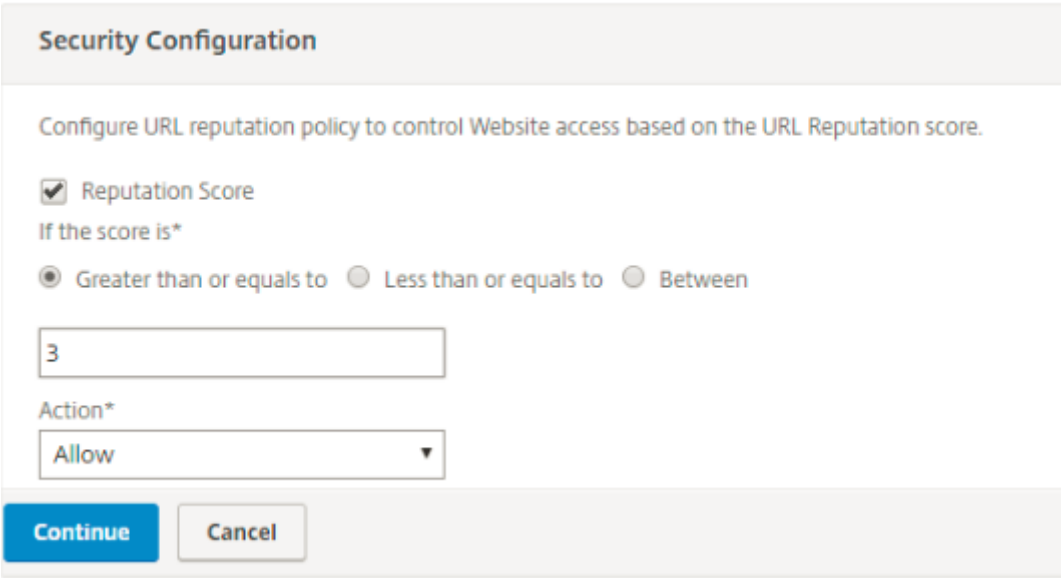
Konfigurieren der Reputationsbewertung mit der GUI

Citrix empfiehlt, den SSL-Forward-Proxyassistenten zum Konfigurieren der Reputationsbewertung und der Sicherheitsstufen zu verwenden. Basierend auf dem konfigurierten Schwellenwert können Sie eine Richtlinienaktion auswählen, um den Datenverkehr zuzulassen, zu blockieren oder umzuleiten.

1. Navigieren Sie zu **Sicherheit** > **SSL Forward Proxy**.
2. Klicken Sie im Detailbereich auf **SSL-Forward-Proxy-Assistent**.
3. Geben Sie auf der Detailseite die Proxyserver-Einstellungen an.

4. Klicken Sie auf **Weiter**, um andere Einstellungen wie SSL-Interception und Identifizieren der Verwaltung anzugeben.
5. Klicken Sie auf **Weiter**, um den Abschnitt **Sicherheitskonfiguration** aufzurufen.
6. Aktivieren Sie im Abschnitt **Sicherheitskonfiguration** das Kontrollkästchen **Reputation Score**, um den Zugriff basierend auf dem URL-Reputationswert zu steuern.
7. Wählen Sie die Sicherheitsstufe aus, und geben Sie den Schwellenwert für die Reputationsbewertung an:
   a) Größer als oder gleich — Zulassen oder Blockieren einer Website, wenn der Schwellenwert größer oder gleich N ist, wobei N zwischen 1 und 4 liegt.
   b) Kleiner als oder gleich — Zulassen oder Blockieren einer Website, wenn der Schwellenwert kleiner oder gleich N ist, wobei N zwischen 1 und 4 liegt.
   c) Zwischen — Erlaubt oder blockiert eine Website, wenn der Schwellenwert zwischen N1 und N2 liegt und der Bereich zwischen 1 und 4 liegt.
8. Wählen Sie eine Responder-Aktion aus der Dropdownliste aus.
9. Klicken Sie auf **Weiter** und **schließen**.

Die folgende Abbildung zeigt den Abschnitt " **Sicherheitskonfiguration** " des SSL Forward Proxy-Assistenten. Aktivieren Sie die Option URL Reputation Score, um die Richtlinieneinstellungen zu konfigurieren.



Analytics

October 5, 2021

In der Citrix ADC Appliance werden alle Benutzerdatensätze und nachfolgende Datensätze protokol-

liert. Wenn Sie Citrix Application Delivery Management (ADM) in die Citrix ADC Appliance integrieren, werden die protokollierten Benutzeraktivitäten und die nachfolgenden Datensätze in der Appliance mithilfe der `logstream` Funktion nach Citrix ADM exportiert.

Citrix ADM stellt Informationen über die Aktivitäten der Nutzer zusammen, z. B. besuchte Websites und die verbrauchte Bandbreite. Außerdem werden Bandbreitennutzung und erkannte Bedrohungen wie Malware und Phishing-Sites gemeldet. Mit diesen Schlüsselmetriken können Sie Ihr Netzwerk überwachen und Korrekturmaßnahmen mit der Citrix SWG-Appliance durchführen. Weitere Informationen finden Sie unter Citrix SSL Forward Proxy Analytics.

So integrieren Sie die Citrix ADC Appliance in Citrix ADM:

1. Aktivieren Sie in der Citrix ADC Appliance während der Konfiguration der SSL-Forward-Proxy-Funktion Analytics und geben Sie die Details der Citrix ADM Instanz an, die Sie für Analysen verwenden möchten.
2. Fügen Sie in Citrix ADM die Citrix ADC Appliance als Instanz zu Citrix ADM hinzu. Weitere Informationen finden Sie unter Instanzen zu Citrix ADM hinzufügen.

Anwendungsfall: Sichere Gestaltung eines Unternehmensnetzwerks durch Verwendung von ICAP für Remote-Malware-Inspektion

December 7, 2021

Die Citrix ADC Appliance fungiert als Proxy und fängt den gesamten Clientdatenverkehr ab. Die Appliance verwendet Richtlinien, um den Datenverkehr auszuwerten und leitet Clientanforderungen an den Ursprungsserver weiter, auf dem sich die Ressource befindet. Die Appliance entschlüsselt die Antwort vom Ursprungsserver und leitet den Nur-Text-Inhalt für eine Antischadwareprüfung an den ICAP-Server weiter. Der ICAP-Server antwortet mit einer Meldung mit der Meldung Keine Anpassung erforderlich oder Fehler oder geänderte Anforderung. Abhängig von der Antwort des ICAP-Servers wird der angeforderte Inhalt entweder an den Client weitergeleitet oder eine entsprechende Nachricht gesendet.

Für diesen Anwendungsfall müssen Sie eine allgemeine Konfiguration, eine Proxy- und SSL-Interceptionkonfiguration sowie eine ICAP-Konfiguration auf der Citrix ADC Appliance durchführen.

Allgemeine Konfiguration

Konfigurieren Sie die folgenden Entitäten:

- NSIP-Adresse
- Subnetz-IP-Adresse (SNIP)

- DNS-Namensserver
- Zertifizierungsstellenschlüsselpaar zum Signieren des Serverzertifikats für SSL-Interception

Proxyserver- und SSL-Interceptionkonfiguration

Konfigurieren Sie die folgenden Entitäten:

- Proxyserver im expliziten Modus, um den gesamten ausgehenden HTTP- und HTTPS-Datenverkehr abzufangen.
- SSL-Profil zum Definieren von SSL-Einstellungen, wie Verschlüsselungen und Parameter, für Verbindungen.
- SSL-Richtlinie zum Definieren von Regeln zum Abfangen von Datenverkehr. Auf true gesetzt, um alle Clientanforderungen abzufangen.

Weitere Informationen finden Sie in den folgenden Artikeln:

- Proxy-Modi
- SSL-Interception

In der folgenden Beispielkonfiguration befindet sich der Antischadsoftware-Erkennungsdienst unter `www.example.com`.

Allgemeine Beispielkonfiguration:

```
1 add dns nameServer 203.0.113.2
2
3 add ssl certKey ns-swg-ca-certkey -cert ns_swg_ca.crt -key ns_swg_ca.
     key
4 <!--NeedCopy-->
```

Beispiel-Proxyserver und SSL-Interceptionkonfiguration:

```
1 add cs vserver explicitswg PROXY 192.0.2.100 80 -Authn401 ENABLED -
     authnVsName explicit-auth-vs
2
3 set ssl parameter -defaultProfile ENABLED
4
5 add ssl profile swg_profile -sslInterception ENABLED
6
7 bind ssl profile swg_profile -ssliCACertkey ns-swg-ca-certkey
8
9 set ssl vserver explicitswg -sslProfile swg_profile
10
```



```
add ssl policy ssli-pol_ssli -rule true -action INTERCEPT

bind ssl vserver explicitswg -policyName ssli-pol_ssli -priority 100 -
    type INTERCEPT_REQ
<!--NeedCopy-->
```

Beispiel-ICAP-Konfiguration:

```
add service icap_svc 203.0.113.225 TCP 1344

enable ns feature contentinspection

add icapprofile icapprofile1 -uri /example.com -Mode RESMOD

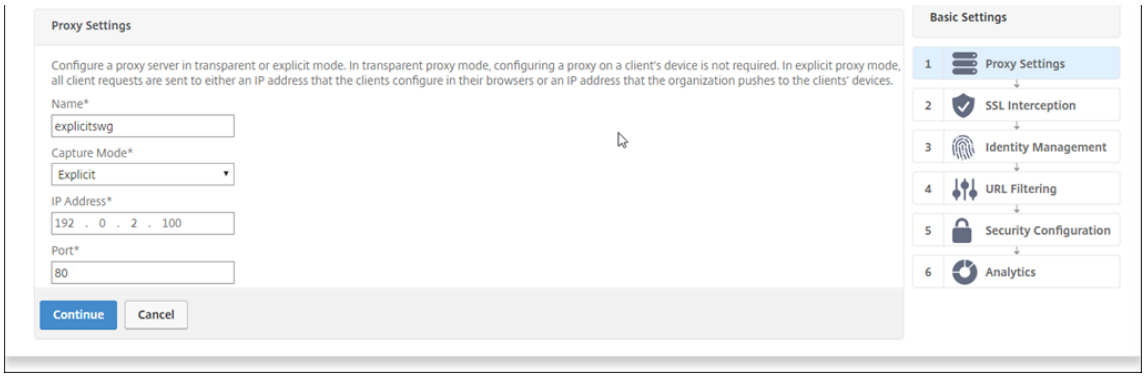
add contentInspection action CiRemoteAction -type ICAP -serverName
    icap_svc -icapProfileName icapprofile1

add contentInspection policy CiPolicy -rule ”HTTP.REQ.METHOD.NE(”
    CONNECT”)” -action CiRemoteAction

bind cs vserver explicitswg -policyName  CiPolicy -priority 200 -type
    response
<!--NeedCopy-->
```

Konfigurieren der Proxy-Einstellungen

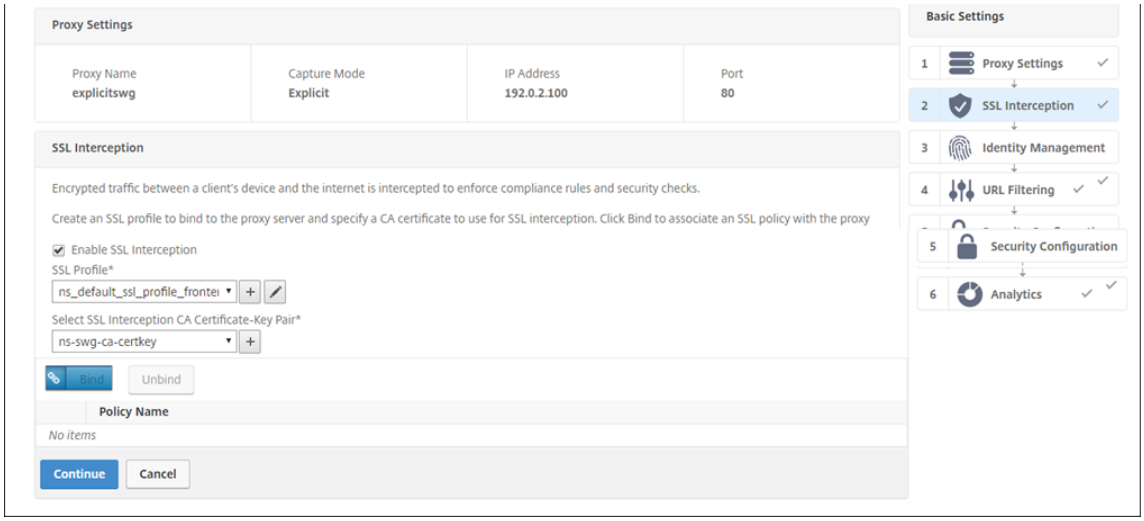
1. Navigieren Sie zu **Sicherheit** > **SSL-Forward-Proxy** > **SSL-Forward-Proxy-Assistent**.
2. Klicken Sie auf **Erste Schritte** und dann auf **Weiter**.
3. Geben Sie im Dialogfeld **Proxyeinstellungen** einen Namen für den expliziten Proxyserver ein.
4. Wählen Sie für **den Aufnahmemodus Explizit**aus
5. Geben Sie eine IP-Adresse und Portnummer ein.



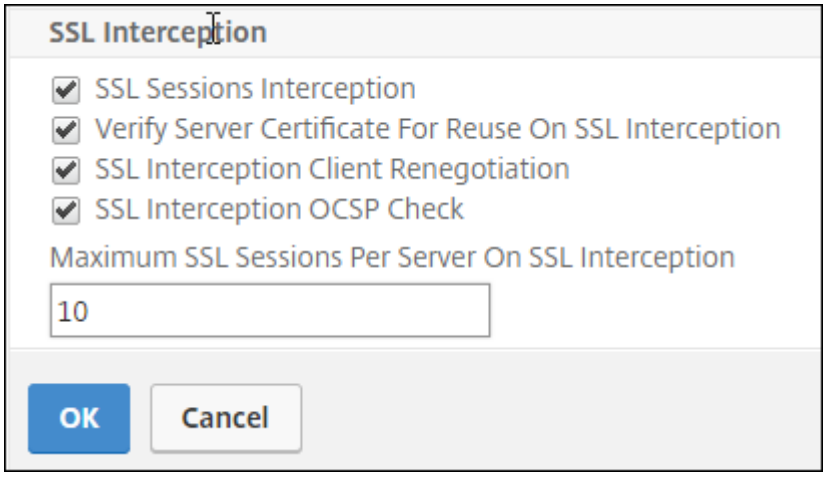
6. Klicken Sie auf **Weiter**.

Konfigurieren der Einstellungen für SSL-Interception

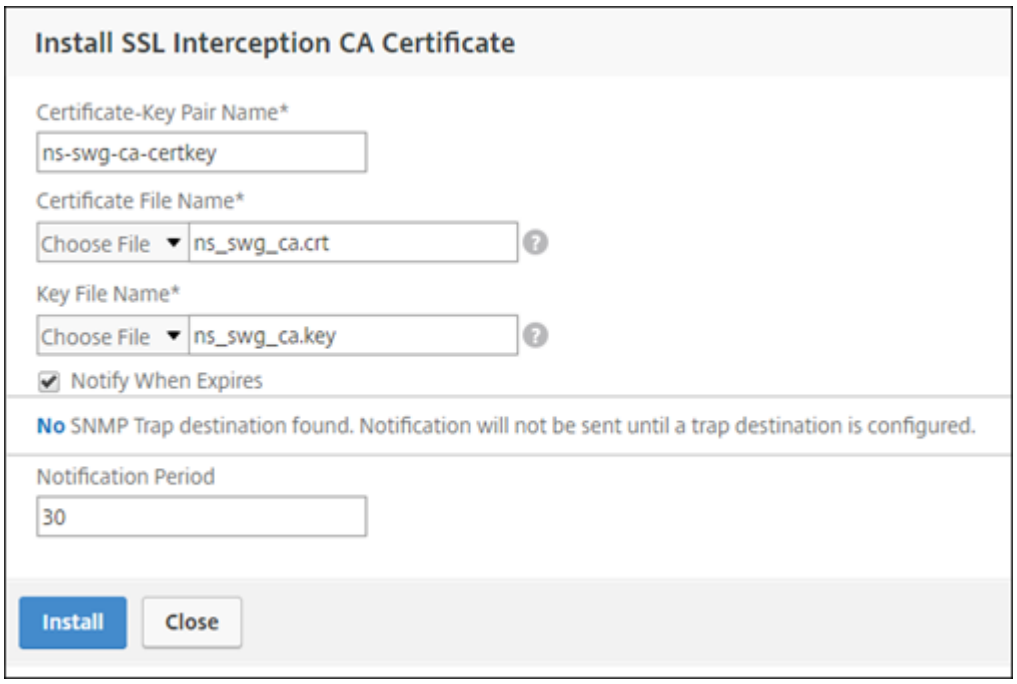
1. Wählen Sie **SSL-Abfangen aktivieren**aus.



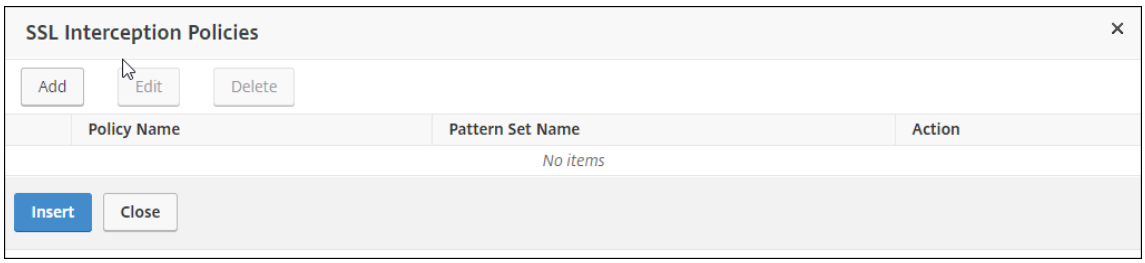
2. Wählen Sie in **SSL-Profil**ein vorhandenes Profil aus oder klicken Sie auf "+", um ein neues Front-End-SSL-Profil hinzuzufügen. Aktivieren Sie **SSL Sessions Interception** in diesem Profil. Wenn Sie ein vorhandenes Profil auswählen, überspringen Sie den nächsten Schritt.



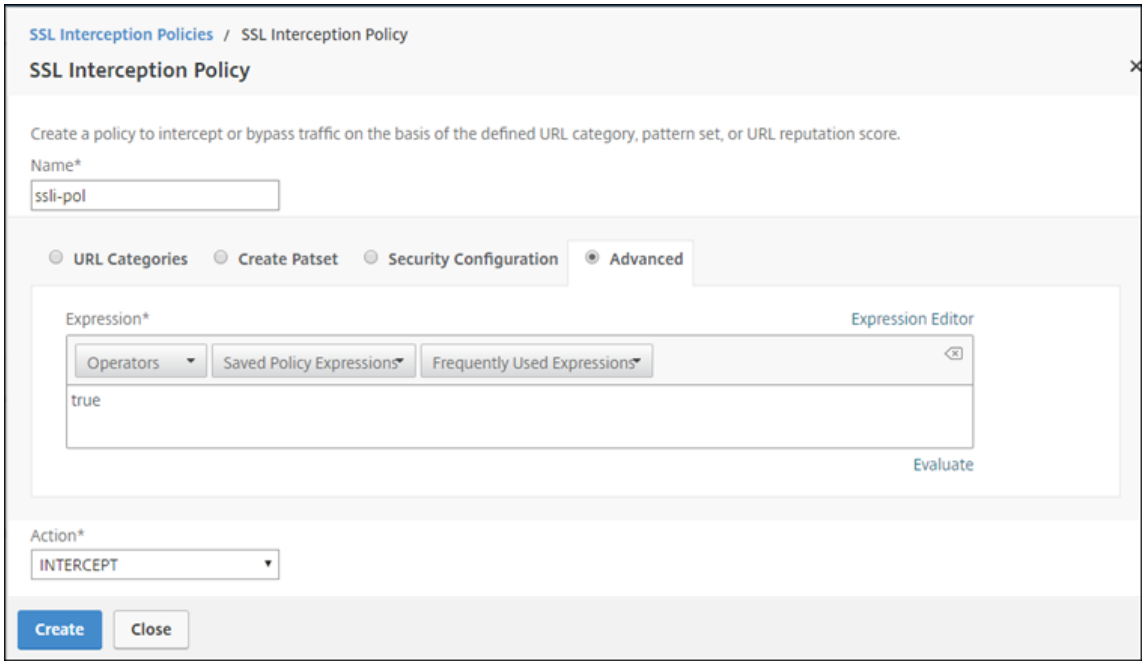
3. Klicken Sie auf **OK** und dann auf **Fertig**.
4. Wählen Sie unter **Select SSL Interception CA Certificate-Key Pair**ein vorhandenes Zertifikat aus, oder klicken Sie auf +, um ein CA-Zertifikatschlüsselpaar für die SSL-Abhörung zu installieren. Wenn Sie ein vorhandenes Zertifikat auswählen, überspringen Sie den nächsten Schritt.



5. Klicken Sie auf **Installieren** und dann auf **Schließen**.
6. Fügen Sie eine Richtlinie hinzu, um den gesamten Datenverkehr abzufangen. Klicken Sie auf **Bind**. Klicken Sie auf **Hinzufügen**, um eine neue Richtlinie hinzuzufügen oder eine vorhandene Richtlinie auszuwählen. Wenn Sie eine vorhandene Richtlinie auswählen, klicken Sie auf **Einfügen**, und überspringen Sie die nächsten drei Schritte.



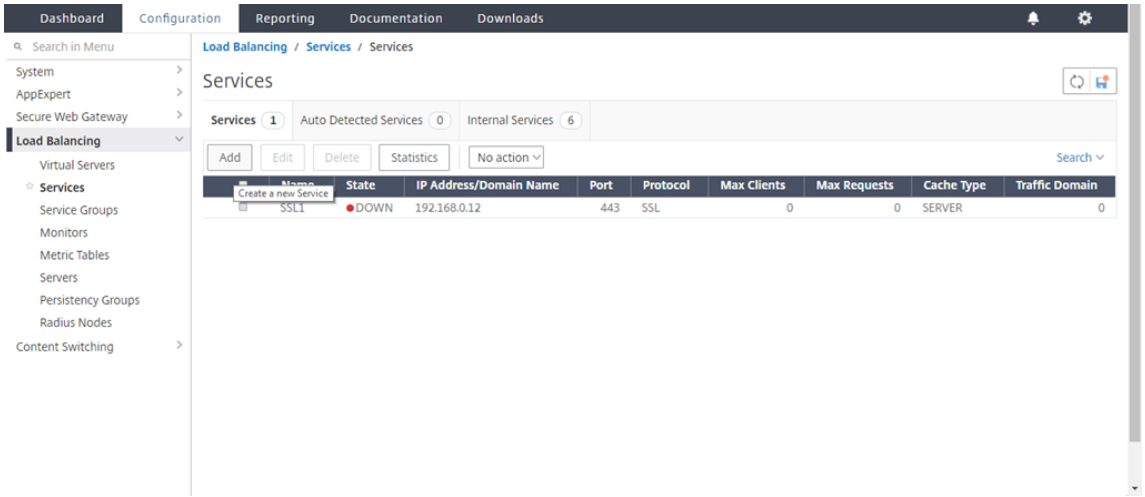
7. Geben Sie einen Namen für die Richtlinie ein, und wählen Sie **Erweitert** aus. Geben Sie im Ausdruckseditor true ein.
8. Wählen Sie unter **Aktion** die Option **INTERCEPT** aus.



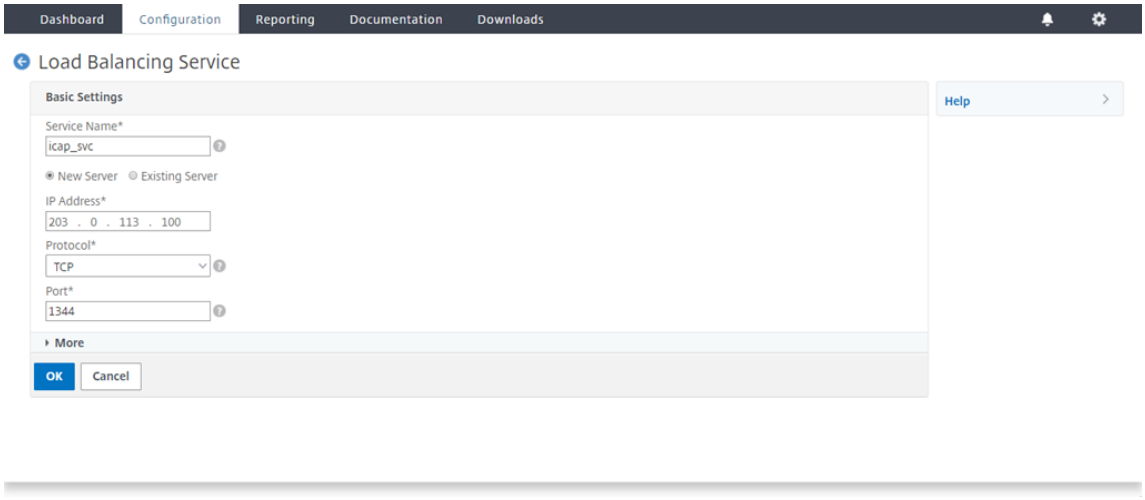
9. Klicken Sie auf **Erstellen**.
10. Klicken Sie viermal auf **Fortfahren**, und klicken Sie dann auf **Fertig**.

Konfigurieren der ICAP-Einstellungen

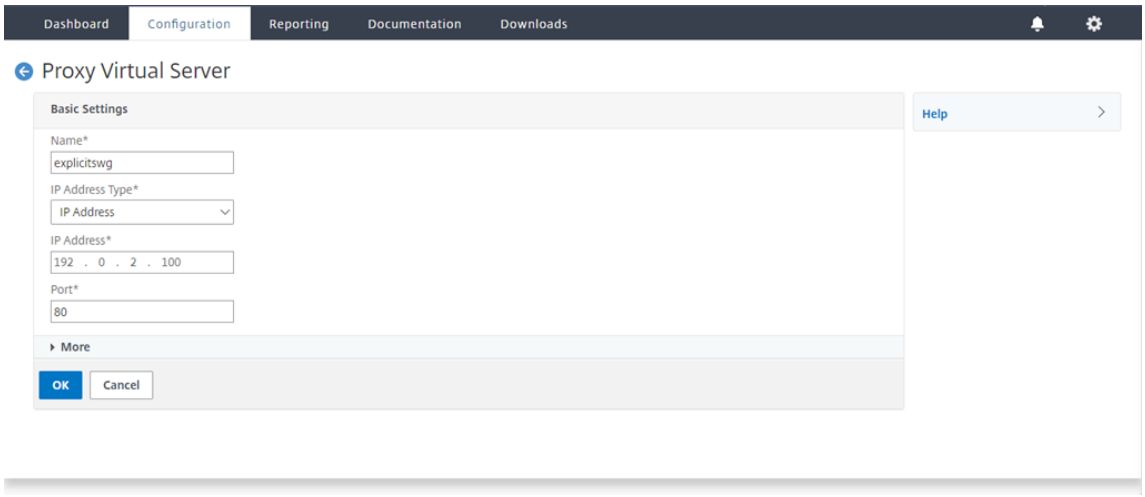
1. Navigieren Sie zu **Load Balancing** > **Services**, und klicken Sie auf **Hinzufügen**.



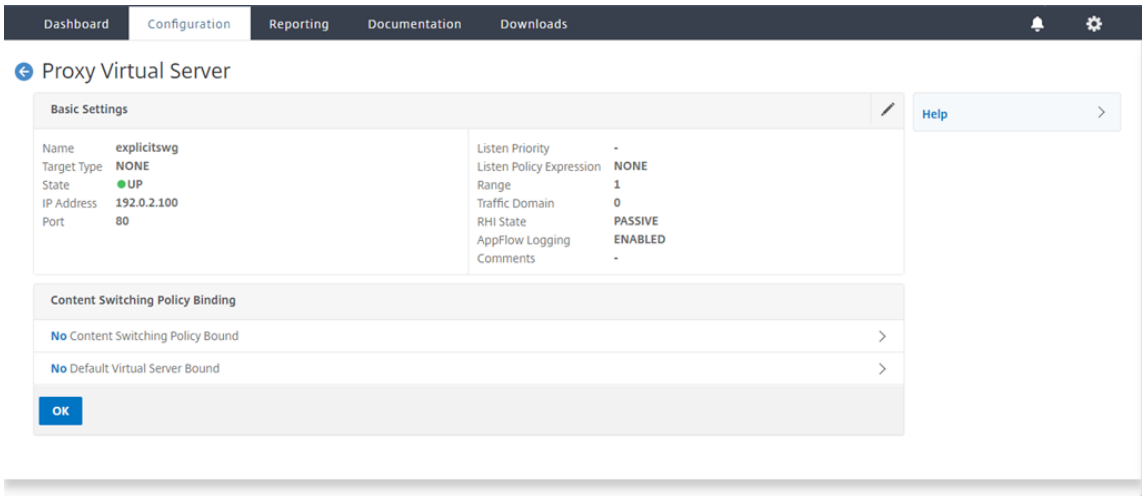
2. Geben Sie einen Namen und eine IP-Adresse ein. Wählen Sie unter **Protokoll** die Option **TCP**aus. Geben Sie in **Port** den Wert **1344**ein. Klicken Sie auf **OK**.



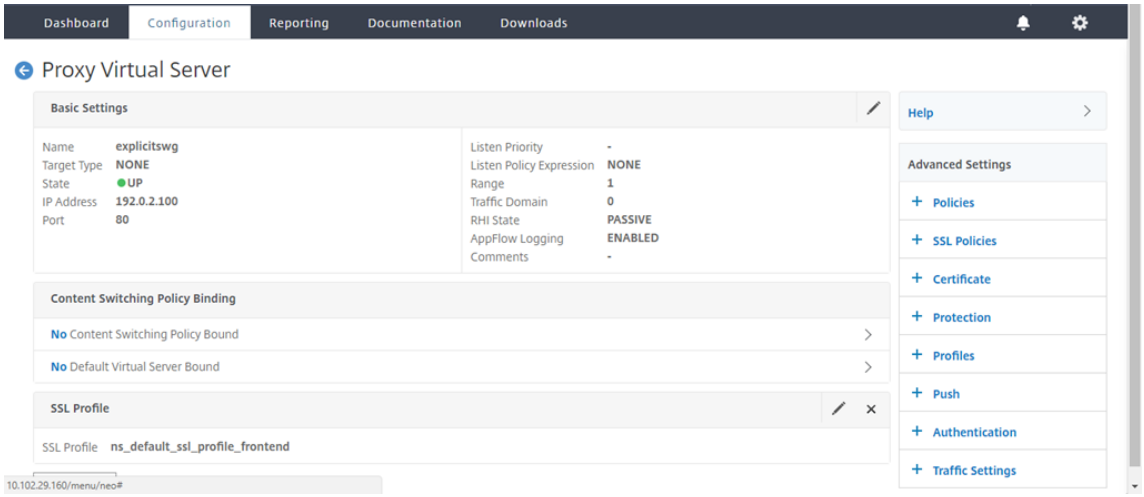
3. Navigieren Sie zu **SSL Forward Proxy**> **Virtual Proxy Server**. Fügen Sie einen virtuellen Proxyserver hinzu, oder wählen Sie einen virtuellen Server aus, und klicken Sie auf **Bearbeiten**. Klicken Sie nach der Eingabe von Details auf **OK**.



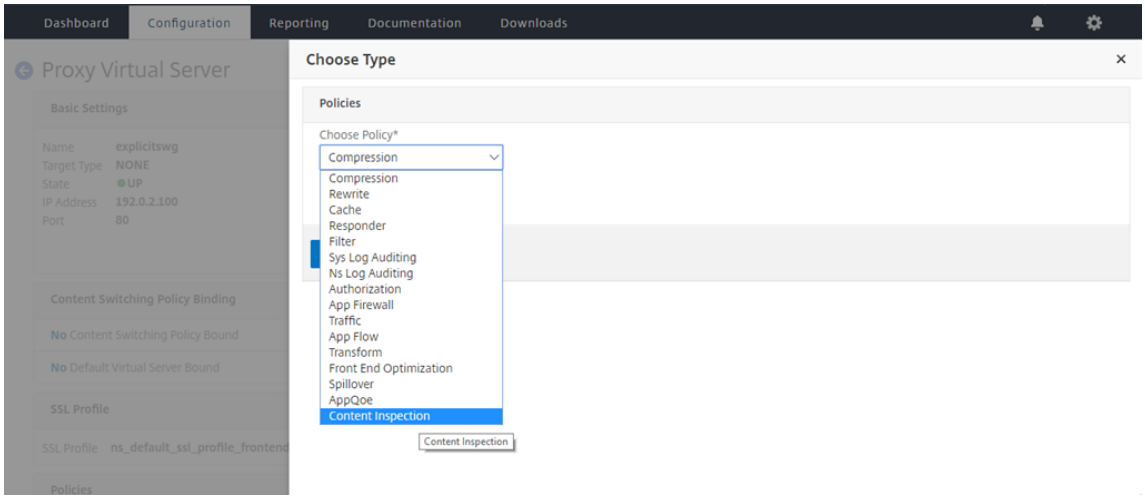
Klicken Sie erneut auf **OK**.



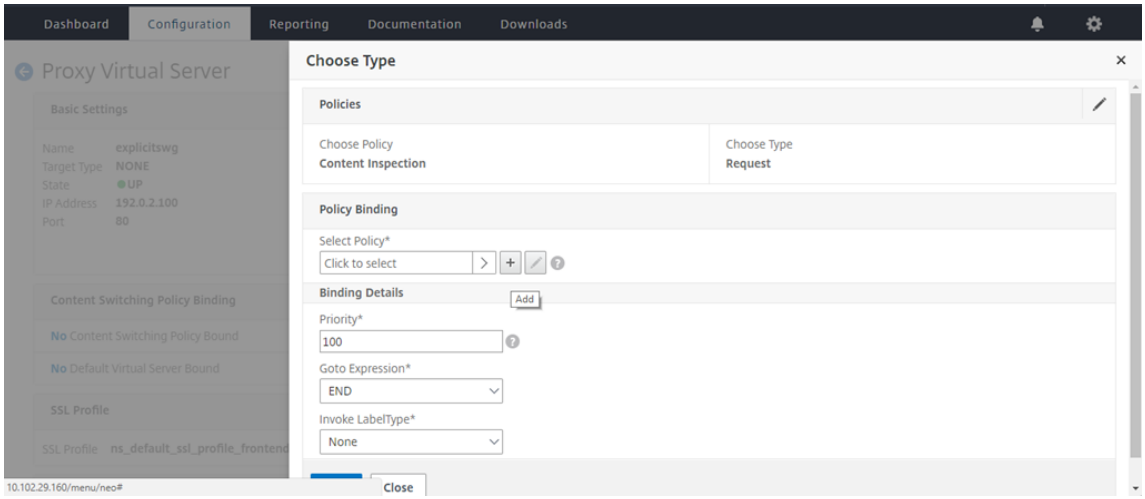
4. Klicken Sie unter **Erweiterte Einstellungen** auf **Richtlinien**.



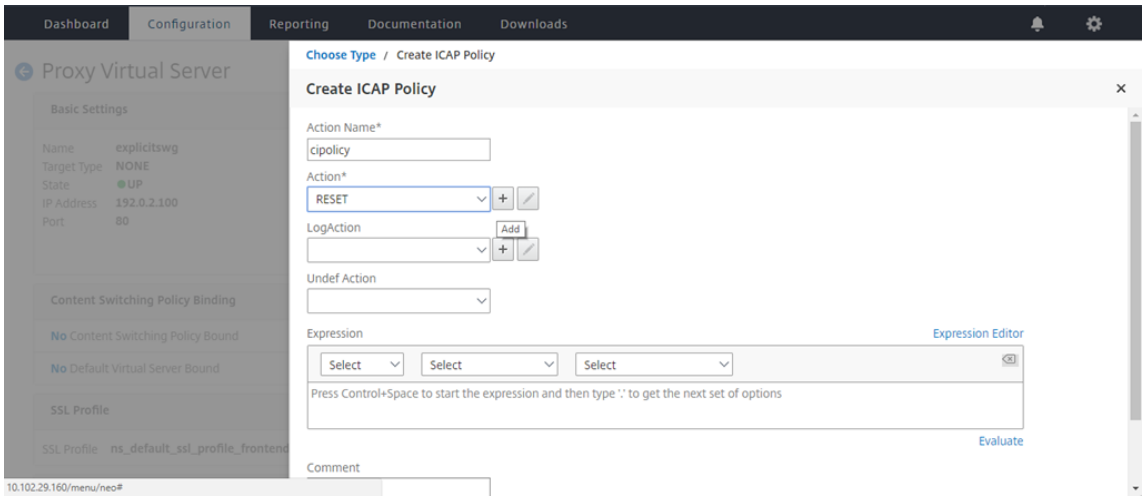
5. Wählen Sie unter **Richtlinie auswählen** die Option **Inhaltsüberprüfung** aus. Klicken Sie auf **Weiter**.



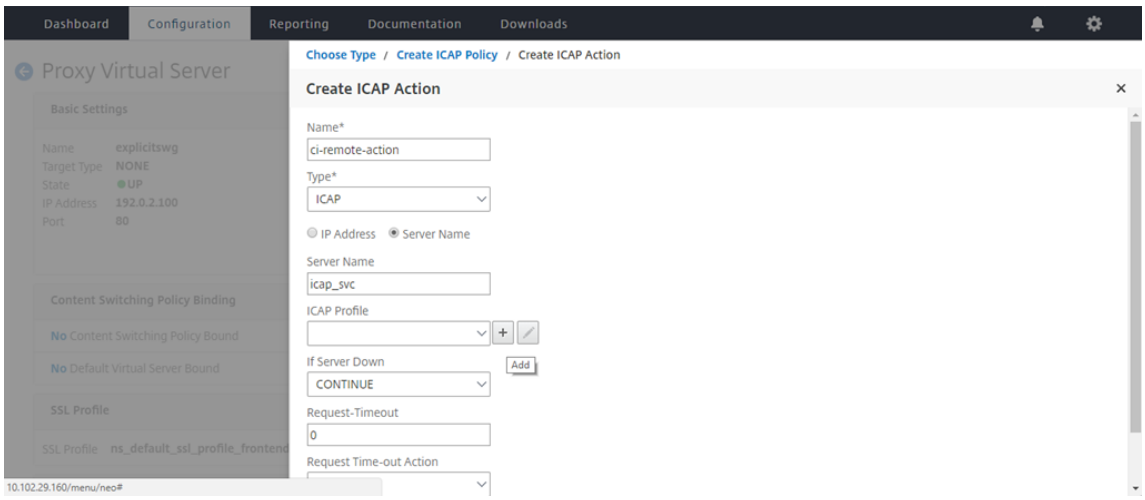
6. Klicken Sie unter **Richtlinie auswählen** auf das +-Zeichen, um eine Richtlinie hinzuzufügen.



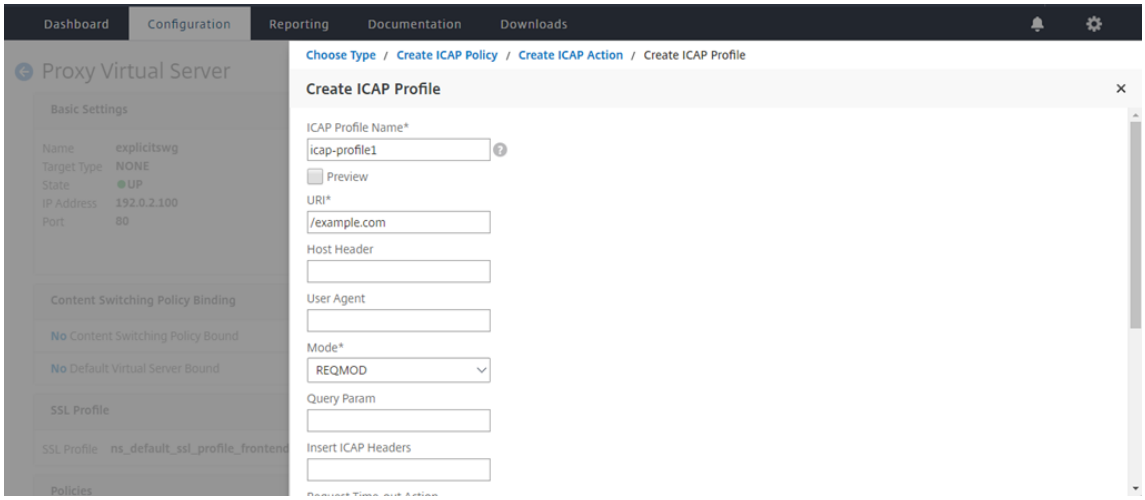
7. Geben Sie einen Namen für die Richtlinie ein. Klicken Sie in **Aktion** auf das +-Zeichen, um eine Aktion hinzuzufügen.



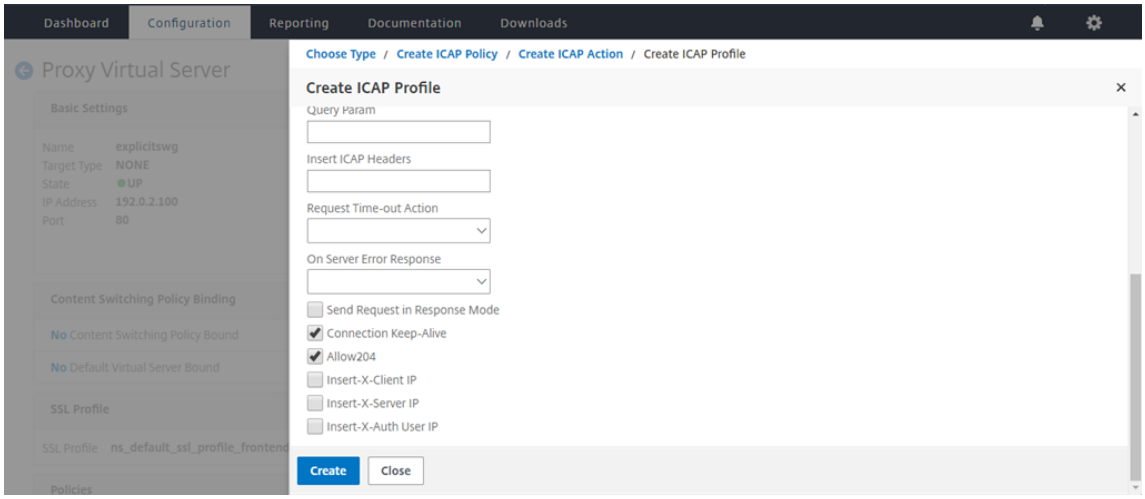
8. Geben Sie einen Namen für die Aktion ein. Geben Sie unter **Servername** den Namen des zuvor erstellten TCP-Dienstes ein. Klicken Sie im **ICAP-Profil** auf das +-Zeichen, um ein ICAP-Profil hinzuzufügen.



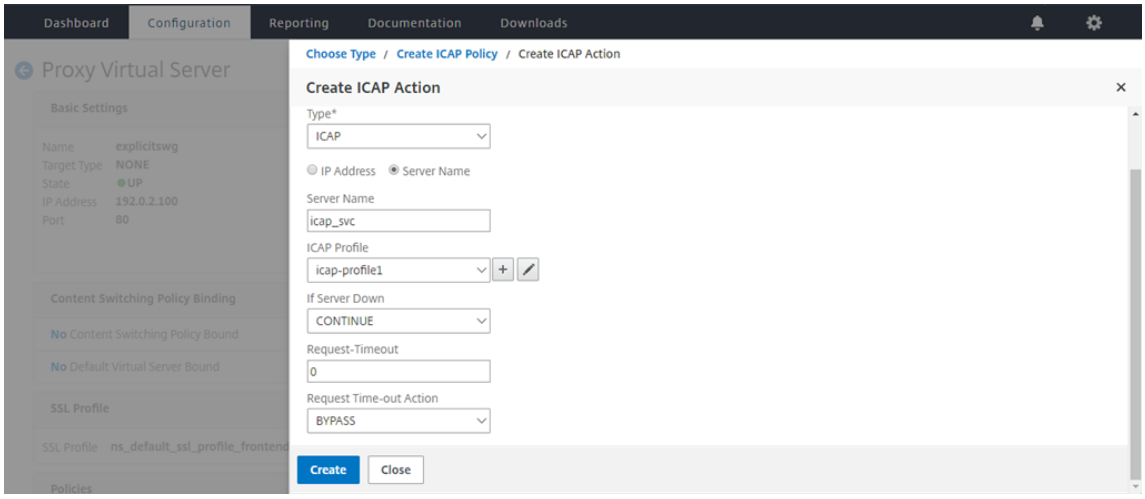
9. Geben Sie einen Profilnamen ein, URI. Wählen Sie unter **Modus** die Option **REQMOD** aus.



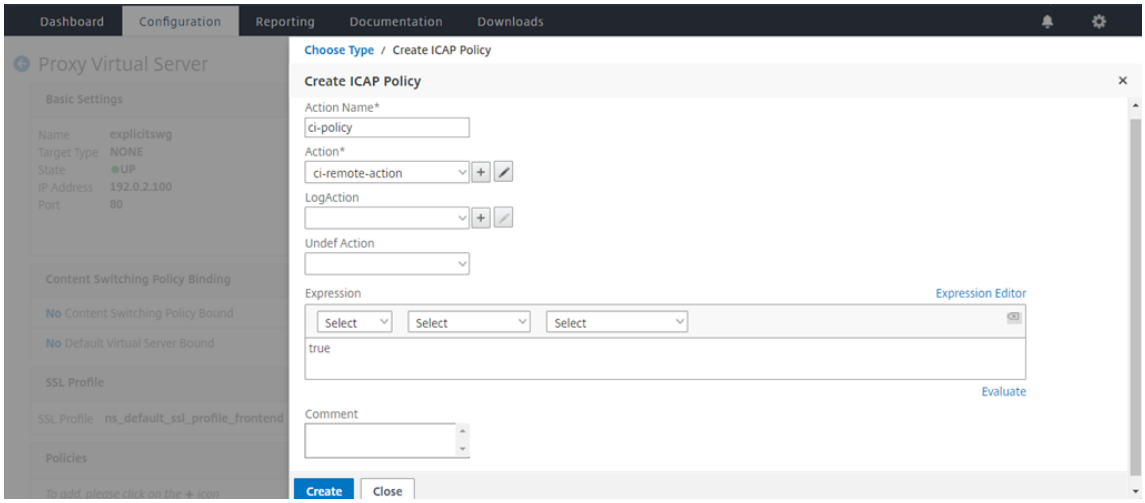
10. Klicken Sie auf **Erstellen**.



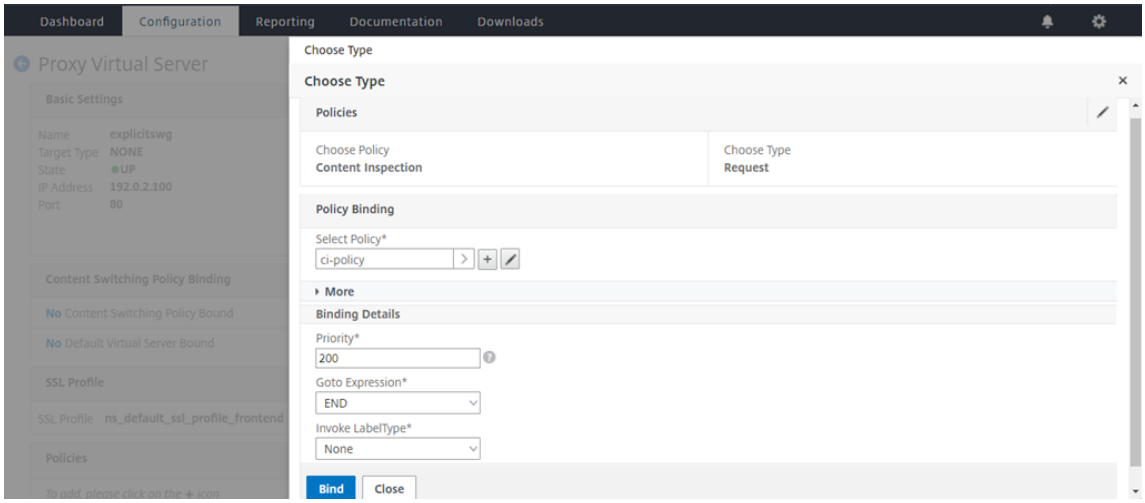
11. Klicken Sie auf der Seite **ICAP-Aktion erstellen** auf **Erstellen**.



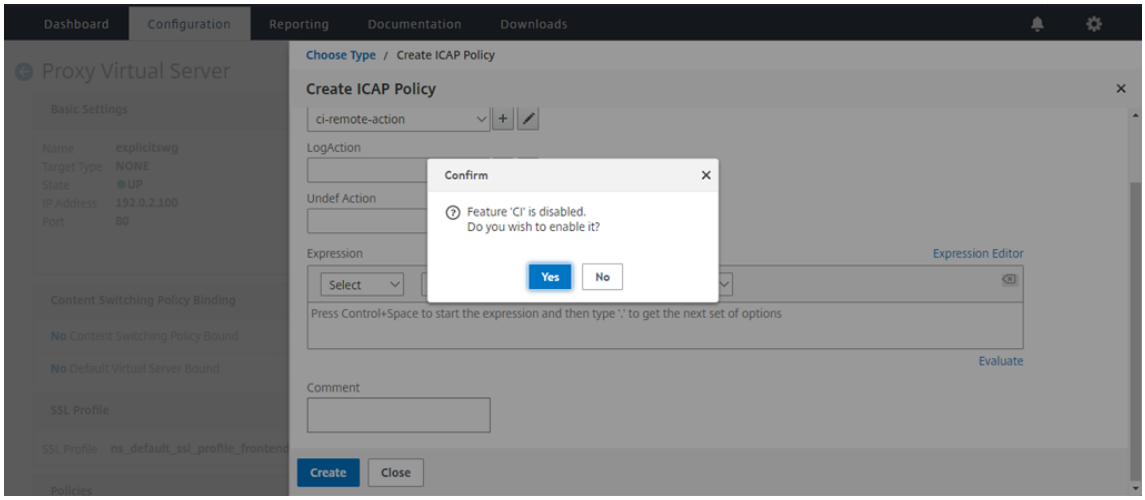
12. Geben Sie auf der Seite **ICAP-Richtlinie erstellen** im **Ausdrucksеditor** “true” ein. Klicken Sie dann auf **Erstellen**.



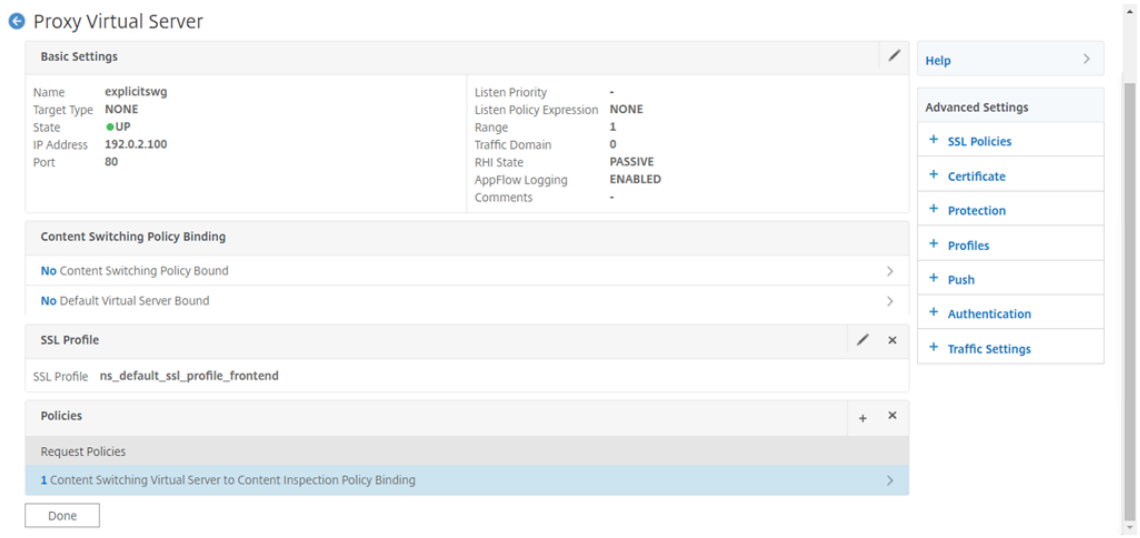
13. Klicken Sie auf **Bind**.



14. Wählen Sie **Ja**aus, wenn Sie dazu aufgefordert werden, die Inhaltsüberprüfungsfunktion zu aktivieren.



15. Klicken Sie auf **Fertig**.



Beispiel für ICAP-Transaktionen zwischen der Citrix ADC Appliance und dem ICAP-Server in RESPMOD

Anforderung von der Citrix ADC Appliance an den ICAP-Server:

```
RESPMOD icap://10.106.137.15:1344/resp ICAP/1.0

Host: 10.106.137.15

Connection: Keep-Alive

Encapsulated: res-hdr=0, res-body=282

HTTP/1.1 200 OK

Date: Fri, 01 Dec 2017 11:55:18 GMT

Server: Apache/2.2.21 (Fedora)

Last-Modified: Fri, 01 Dec 2017 11:16:16 GMT

ETag: ”20169-45-55f457f42aee4”

Accept-Ranges: bytes

Content-Length: 69

```



```
Keep-Alive: timeout=15, max=100

Content-Type: text/plain; charset=UTF-8

X5O!P%@AP[4PZX54(P^)7CC)7 }
 $EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
<!--NeedCopy-->
```

Antwort vom ICAP-Server auf die Citrix ADC Appliance:

```
ICAP/1.0 200 OK

Connection: keep-alive

Date: Fri, 01 Dec, 2017 11:40:42 GMT

Encapsulated: res-hdr=0, res-body=224

Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$

ISTag: ”9.8-13.815.00-3.100.1027-1.0”

X-Virus-ID: Eicar_test_file

X-Infection-Found: Type=0; Resolution=2; Threat=Eicar_test_file;

HTTP/1.1 403 Forbidden

Date: Fri, 01 Dec, 2017 11:40:42 GMT

Cache-Control: no-cache

Content-Type: text/html; charset=UTF-8

Server: IWSVA 6.5-SP1_Build_Linux_1080 $Date: 04/09/2015 01:19:26 AM$

Content-Length: 5688

<html><head><META HTTP-EQUIV=”Content-Type” CONTENT=”text/html; charset
   =UTF-8”/>

…

```



```
33  ...
34
35  </body></html>
36  <!--NeedCopy-->
```

Anleitungsartikel

October 5, 2021

Im Folgenden finden Sie einige Konfigurationsanweisungen oder funktionale Anwendungsfälle, die als How to -Artikel verfügbar sind, mit denen Sie Ihre SSL-Forward-Proxybereitstellung verwalten können.

URL-Filterung

Erstellen einer URL-Kategorisierungsrichtlinie

Erstellen einer URL-Listenrichtlinie

So lassen Sie eine außergewöhnliche URL zu

So blockieren Sie Websites für Erwachsene

Sicherheit

October 5, 2021

Die folgenden Themen behandeln Konfigurations- und Installationsinformationen für Citrix ADC -Sicherheitsfeatures. Die meisten dieser Funktionen sind richtlinienbasiert.

Inhaltsfilterung	Blockiert unangemessene HTML-Anforderungen und verhindert, dass die Anforderungen an die Webserver gelangen.
Überspannungsschutz	Erkennt einen schnellen Anstieg der Verbindungsversuche und passt die Geschwindigkeit an, mit der Verbindungen zum Server fortgesetzt werden dürfen, um Serverüberlastung zu verhindern.

DNS-Sicherheitsoptionen	Vereinfachter UI-Assistent zum Erstellen von Richtlinien zum Schutz vor DNS-Angriffen

Inhaltsfilterung

October 5, 2021

Die Inhaltsfilterung kann einige der gleichen Aufgaben wie die Citrix Web App Firewall ausführen und ist ein weniger CPU-intensives Tool. Es ist jedoch darauf beschränkt, den Header-Teil der HTTP-Anforderung oder -Antwort zu untersuchen und einige einfache Aktionen für Verbindungen auszuführen, die übereinstimmen. Wenn Sie über eine komplexe Website verfügen, die Skripts umfassend nutzt und auf Back-End-Datenbanken zugreift, ist die Application Firewall möglicherweise das bessere Werkzeug zum Schutz dieser Website. Weitere Informationen zur Citrix Web App Firewall finden Sie unter Application Firewall.

Die Inhaltsfilterung basiert auf regulären Ausdrücken, die Sie entweder auf HTTP-Anforderungen oder auf HTTP-Antworten anwenden können. Um beispielsweise Anfragen von einer bestimmten Site zu blockieren, können Sie einen Ausdruck verwenden, der die URL jeder Anforderung mit der im Ausdruck angegebenen URL vergleicht. Der Ausdruck ist Teil einer Richtlinie, die auch eine Aktion angibt, die für Anforderungen oder Antworten ausgeführt werden soll, die mit dem Ausdruck übereinstimmen. Beispielsweise kann eine Aktion eine Anforderung löschen oder die Verbindung zurücksetzen.

Im Folgenden finden Sie einige Beispiele für Dinge, die Sie mit Inhaltsfilterrichtlinien tun können:

- Verhindern Sie, dass Benutzer auf bestimmte Teile Ihrer Websites zugreifen, es sei denn, sie verbinden sich von autorisierten Standorten aus.
- Verhindern Sie, dass unangemessene HTTP-Header an Ihren Webserver gesendet werden, wodurch möglicherweise die Sicherheit verletzt wird.
- Leiten Sie angegebene Anforderungen an einen anderen Server oder Dienst um.

Um die Inhaltsfilterung zu konfigurieren, konfigurieren Sie, nachdem Sie sichergestellt haben, dass das Feature aktiviert ist, Filteraktionen für Ihre Server für ausgewählte Verbindungen (es sei denn, die vordefinierten Aktionen sind für Ihre Zwecke geeignet). Anschließend können Sie Richtlinien konfigurieren, um die Aktionen auf ausgewählte Verbindungen anzuwenden. Ihre Richtlinien können vordefinierte Ausdrücke verwenden, oder Sie können eigene erstellen. Um die von Ihnen konfigurierten Richtlinien zu aktivieren, binden Sie sie entweder global oder an bestimmte virtuelle Server.

Aktivieren der Inhaltsfilterung

October 5, 2021

Standardmäßig ist die Inhaltsfilterung auf Citrix ADC Appliances aktiviert, auf denen das Citrix ADC-Betriebssystem 8.0 oder höher ausgeführt wird. Wenn Sie eine vorhandene Appliance von einer Betriebssystemversion vor 8.0 aktualisieren, müssen Sie die Lizenzen aktualisieren, bevor Sie die Inhaltsfilterung verwenden können, und Sie müssen möglicherweise die Funktion zur Inhaltsfilterung selbst manuell aktivieren.

Aktivieren der Inhaltsfilterung über die CLI

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

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

Beispiel:

```
> enable ns feature ContentFiltering
 Done
> show ns feature

        Feature                         Acronym              Status
        -------                         -------              ------
 1)     Web Logging                     WL                   ON
 2)     Surge Protection                SP                   OFF
 .
 .
 .
 .
 11)    Http DoS Protection             HDOSP                OFF
 12)    Content Filtering               CF                   ON
 .
 .
 23)    HTML Injection                  HTMLInjection        ON
 24)    Citrix ADC Push                  push                 OFF
 Done
```



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

Aktivieren von Inhalten durch Filtern über die GUI

1. Erweitern Sie im Navigationsbereich System, und wählen Sie dann Einstellungen aus.
2. Klicken Sie im Detailbereich auf Grundfunktionen konfigurieren.
3. Aktivieren Sie im Bereich Grundfunktionen konfigurieren das Kontrollkästchen Inhaltsfilter, und klicken Sie dann auf OK.

Konfigurieren einer Inhaltsfilteraktion

October 5, 2021

Nachdem Sie die Inhaltsfilterfunktion aktiviert haben, erstellen Sie eine oder mehrere Aktionen, um der Citrix ADC Appliance mitzuteilen, wie die empfangenen Verbindungen verarbeitet werden sollen.

Die Inhaltsfilterung unterstützt die folgenden Aktionen für HTTP-Anforderungen:

- **Add:** Fügt den angegebenen HTTP-Header hinzu, bevor die Anforderung an den Webserver gesendet wird.
- **Zurücksetzen:** Beendet die Verbindung und sendet die entsprechende Kündigung an den Browser des Benutzers.
- **Weiterleiten:** leitet die Anforderung an den angegebenen Dienst weiter.
- **Drop:** Löscht die Anfrage im Hintergrund, ohne eine Antwort an den Browser des Benutzers zu senden.
- **Beschädigt:** Ändert den angegebenen HTTP-Header in einer Weise, die verhindert, dass er die Funktion ausführt, die er ausführen sollte, und sendet dann die Anforderung an den Server.

Die Inhaltsfilterung unterstützt die folgenden Aktionen für HTTP-Antworten:

- **Add:** Fügt den angegebenen HTTP-Header hinzu, bevor die Antwort an den Browser des Benutzers gesendet wird.
- **ErrorCode:** Gibt den angegebenen HTTP-Fehlercode an den Browser des Benutzers zurück.
- **Beschädigt:** Ändert den angegebenen HTTP-Header in einer Weise, die verhindert, dass er die Funktion ausführt, die er ausführen sollte, und sendet dann die Antwort an den Browser des Benutzers.

Konfigurieren einer Inhaltsfilter-Aktion über die CLI

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

```
1 -  add filter action <name> <qualifier> [<serviceName>] [<value>] [<
     respCode>] [<page>]
2 -  show filter action <name>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add filter action act_drop Drop
2  Done
3 > show filter action act_drop
4 1)      Name: act_drop   Filter Type: drop
5  Done
6 <!--NeedCopy-->
```

Konfigurieren einer Inhaltsfilter-Aktion über die GUI

1. Navigieren Sie zu **Sicherheit > Schutzfunktionen > Filter**.
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
   - Um eine neue Aktion zu erstellen, klicken Sie auf **Hinzufügen**.
   - Um eine vorhandene Aktion zu ändern, wählen Sie die Aktion aus, und klicken Sie dann auf **Öffnen**.
3. Geben **Sie im Dialogfeld Filteraktion hinzufügen** oder **Filteraktion konfigurieren** Werte für die Parameter an:
   - Aktionsname* — name
   - Qualifier* — Qualifier (Bestimmt, welchen der folgenden Parameter Sie konfigurieren können)
   - Dienstname — Dienstname
   - HeaderName:Value—value
   - Antwortcode—`respcode`
   - Response Page—page
4. Geben Sie alle anderen erforderlichen Informationen ein. Wenn Sie beispielsweise eine Aktion zum Senden eines HTTP-Fehlercodes konfigurieren, müssen Sie den entsprechenden Fehlercode aus einer Dropdownliste auswählen. Bei Bedarf können Sie dann den Text der Fehlermeldung ändern, die unter der Dropdownliste angezeigt wird.

5. Klicken Sie auf Erstellen oder OK und dann auf Schließen. In der Liste Aktionen wird die von Ihnen konfigurierte Aktion angezeigt, und eine Meldung in der Statusleiste zeigt an, dass Ihre Aktion erstellt wurde.

Konfigurieren einer Inhaltsfilterrichtlinie

October 5, 2021

Um die Inhaltsfilterung zu implementieren, müssen Sie mindestens eine Richtlinie konfigurieren, um der Citrix ADC Appliance mitzuteilen, wie die Verbindungen unterschieden werden, die Sie filtern möchten. Sie müssen zunächst mindestens eine Filteraktion konfiguriert haben, da Sie sie beim Konfigurieren einer Richtlinie einer Aktion zuordnen.

Inhaltsfilterrichtlinien prüfen eine Kombination aus einem oder mehreren der folgenden Elemente, um Anforderungen oder Antworten für die Filterung auszuwählen:

- **URL:** Die URL in der HTTP-Anforderung.
- **URL-Abfrage:** Nur der Abfrageteil der URL, der der Teil nach der Abfrage (?) ist -Symbol.
- **URL-Token:** Nur die Token in der URL, falls vorhanden, sind die Teile, die mit einem kaufmännischen Und-Zeichen (&) beginnen und aus dem Token-Namen bestehen, gefolgt von einem Gleichheitszeichen (=), gefolgt vom Token-Wert.
- **HTTP-Methode:** Die in der Anforderung verwendete HTTP-Methode, die normalerweise GET oder POST ist, kann aber eine der acht definierten HTTP-Methoden sein.
- **HTTP-Version:** Die HTTP-Version in der Anforderung, die normalerweise HTTP 1.1 ist.
- **Standard-HTTP-Header:** Alle Standard-HTTP-Header, die in der HTTP 1.1-Spezifikation definiert sind.
- **Standard-HTTP-Header-Wert:** Der Werteteil des HTTP-Headers, der der Teil nach dem Doppelpunkt und Leerzeichen (:) ist.
- **Benutzerdefinierter HTTP-Header:** Ein nicht standardmäßiger HTTP-Header, der von Ihrer Website ausgegeben wird oder der in einer Benutzeranfrage angezeigt wird.
- **Benutzerdefinierter Header-Wert:** Der Werteteil des benutzerdefinierten HTTP-Headers, der (wie beim Standard-HTTP-Header) der Teil hinter dem Doppelpunkt und Leerzeichen (:) ist.
- **Client-Quell-IP:** Die IP, von der die Clientanforderung gesendet wurde.

Inhaltsfilterrichtlinien verwenden die einfacheren von zwei Citrix ADC Ausdruckssprachen, die sogenannten klassischen Ausdrücke. Eine vollständige Beschreibung klassischer Ausdrücke, wie sie funktionieren und wie sie manuell konfiguriert werden, finden Sie unter “Richtlinien und Ausdrücke. “

Hinweis: Benutzer, die nicht mit der Konfiguration von Richtlinien in der Citrix ADC Befehlszeile vertraut sind, finden in der Regel die Verwendung des Konfigurationsdienstprogramms erheblich einfacher.

Konfigurieren einer Inhaltsfilterrichtlinie über die CLI

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

```
1 -  add filter policy <name> -rule <expression> (-reqAction <action> | -
     resAction <string>
2 -  show filter policy <name>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > add filter policy cf-pol -rule "REQ.HTTP.URL CONTAINS http://abc.com"
      -reqaction DROP
2  Done
3 > show filter policy cf-pol
4 1)      Name: cf-pol    Rule: REQ.HTTP.URL CONTAINS http://abc.com
5         Request action: DROP
6         Response action:
7         Hits: 0
8  Done
9 <!--NeedCopy-->
```

Konfigurieren einer Inhaltsfilterrichtlinie über die GUI

1. Navigieren Sie zu Sicherheit > Schutzfunktionen > Filter.
2. Navigieren Sie zu Schutzfunktionen > Filter.
3. Klicken Sie im Detailbereich auf Hinzufügen, um eine neue Richtlinie zu erstellen.
4. Wenn Sie eine neue Richtlinie erstellen, geben Sie im Dialogfeld Filterrichtlinie erstellen im Textfeld Filtername einen Namen für die neue Richtlinie ein.
5. Wählen Sie entweder Aktion anfordern oder Antwortaktion aus, um die Dropdownliste rechts neben dem Element zu aktivieren.
6. Klicken Sie auf den Pfeil nach unten rechts neben der Dropdownliste, und wählen Sie die Aktion aus, die für die Anforderung oder Antwort ausgeführt werden soll. Die Standardoptionen sind RESET und DROP. Alle anderen Aktionen, die Sie erstellt haben, werden ebenfalls in dieser Liste

angezeigt.

Hinweis: Sie können auch auf Neu klicken, um eine neue Inhaltsfilteraktion zu erstellen, oder auf Ändern, um eine vorhandene Inhaltsfilterungsaktion zu ändern. Sie können nur Aktionen ändern, die Sie erstellt haben. Die Standardaktionen sind schreibgeschützt.

7. Wenn Sie zum Definieren der Richtlinie einen vordefinierten Ausdruck (oder benannten Ausdruck) verwenden möchten, wählen Sie einen aus der Liste Benannte Ausdrücke aus.
   a) Klicken Sie auf den Pfeil nach unten rechts neben der ersten Dropdownliste Named Expressions, und wählen Sie die Kategorie der benannten Ausdrücke aus, die den benannten Ausdruck enthält, den Sie verwenden möchten.
   b) Klicken Sie auf den Pfeil nach unten rechts neben der zweiten Dropdownliste Named Expressions, und wählen Sie den gewünschten benannten Ausdruck aus. Wenn Sie einen benannten Ausdruck auswählen, wird die Definition des regulären Ausdrucks des benannten Ausdrucks im Bereich Vorschauausdruck unterhalb der Listenfelder benannter Ausdruck angezeigt.
   c) Klicken Sie auf Ausdruck hinzufügen, um den benannten Ausdruck der Liste Ausdruck hinzuzufügen.
   Hinweis: Sie müssen entweder diesen Schritt oder Schritt 7 ausführen, aber nicht beides.
8. Wenn Sie einen neuen Ausdruck zum Definieren Ihrer Richtlinie erstellen möchten, verwenden Sie den Ausdrucksеditor.
   a) Klicken Sie auf die Schaltfläche Add. Das Dialogfeld Ausdruck hinzufügen wird angezeigt.
   b) Wählen Sie im Dialogfeld Ausdruck hinzufügen den Verbindungstyp aus, den Sie filtern möchten. Der Flow Type ist standardmäßig auf REQ festgelegt, der die Citrix ADC Appliance anweist, eingehende Verbindungen oder Anforderungen zu betrachten. Wenn Sie ausgehende Verbindungen (Antworten) filtern möchten, klicken Sie neben der Dropdownliste auf den Pfeil nach rechts und wählen Sie RES.
   c) Wenn das Protokoll noch nicht auf HTTP festgelegt ist, klicken Sie auf den Pfeil nach unten rechts neben der Dropdownliste Protokoll, und wählen Sie HTTP.
   Hinweis: In der Sprache der klassischen Citrix ADC Ausdrücke enthält HTTP auch HTTPS-Anforderungen.
   d) Klicken Sie auf den Pfeil nach unten rechts neben der Dropdownliste Qualifier, und wählen Sie dann einen Qualifier für Ihren Ausdruck aus. Ihre Auswahlmöglichkeiten:
      - **METHOD:** Die HTTP-Methode, die in der Anforderung verwendet wird.
      - **URL:** Der Inhalt des URL-Headers.
      - **URLTOKENS:** Die URL-Tokens im HTTP-Header.
      - **VERSION:** Die HTTP-Version der Verbindung.
      - **HEADER:** Der Header-Teil der HTTP-Anforderung.
      - **URLLEN:** Die Länge des Inhalts des URL-Headers.
      - **URLQUERY:** Der Abfrageteil des Inhalts des URL-Headers.
      - **URLQUERYLEN:** Die Länge des Abfrageabschnitts des URL-Headers.

Der Inhalt der verbleibenden Listenfelder ändert sich zu den Optionen, die dem ausgewählten Qualifier entsprechen. Wenn Sie z. B. HEADER wählen, wird unter dem Listenfeld Flow-Typ ein Textfeld mit der Bezeichnung Kopfzeilenname* angezeigt.

e) Klicken Sie auf den Pfeil nach unten rechts neben der Dropdownliste Operator, und wählen Sie einen Operator für Ihren Ausdruck aus. Ihre Auswahl hängt vom Protokoll ab, das Sie im vorherigen Schritt ausgewählt haben. Die folgende Liste enthält alle Operatoren:
   - **==:** Entspricht exakt der folgenden Textzeichenfolge.
   - **!=:** Entspricht nicht exakt der folgenden Textzeichenfolge.
   - **>:** Ist größer als die folgende ganze Zahl.
   - **CONTAINS:** Enthält die folgende Textzeichenfolge.
   - **CONTENTS:** Der Inhalt der angegebenen Header-, URL- oder URL-Abfrage.
   - **EXISTS:** Der angegebene Header oder die angegebene Abfrage existiert.
   - **NOTCONTAINS:** Enthält nicht die folgende Textzeichenfolge.
   - **NOTEXISTS:** Der angegebene Header oder Abfrage existiert nicht.

f) Wenn das Textfeld Wert sichtbar ist, geben Sie die entsprechende Zeichenfolge oder Zahl ein. Wenn Sie eine Zeichenfolge in irgendeiner Weise testen, geben Sie die Zeichenfolge in das Textfeld Wert ein. Wenn Sie eine ganze Zahl auf irgendeine Weise testen, geben Sie die ganze Zahl in das Textfeld Wert ein.

g) Wenn Sie HEADER als Protokoll gewählt haben, geben Sie die gewünschte Kopfzeile in das Textfeld Kopfzeilenname* ein.

h) Klicken Sie auf OK, um den Ausdruck der Liste Ausdrücke hinzuzufügen.

i) Wiederholen Sie die Schritte B bis H, um weitere Ausdrücke für Ihr Profil zu erstellen.

j) Klicken Sie auf Schließen, um den Ausdrucksеditor zu schließen.

9. Wenn Sie einen neuen Ausdruck erstellt haben, wählen Sie im Rahmen Ausdruck eine Option aus der Dropdownliste Beliebiger Ausdruck aus. Ihre Auswahlmöglichkeiten:
   - Entsprechen Sie mit jedem Ausdruck. Wenn eine Anforderung mit einem Ausdruck in der Liste Ausdrücke übereinstimmt, stimmt die Anforderung mit dieser Richtlinie überein.
   - Alle Ausdrücke übereinstimmen Wenn eine Anforderung mit allen Ausdrücken in der Liste Ausdrücke übereinstimmt, stimmt die Anforderung mit dieser Richtlinie überein. Wenn es nicht mit allen übereinstimmt, stimmt es nicht mit dieser Richtlinie überein.
   - Tabellarischer Ausdruck Schaltet die Liste Ausdrücke in ein tabellarisches Format mit drei Spalten um. In der ersten Spalte können Sie einen BEGIN-Operator [(] platzieren. Die zweite Spalte enthält die Ausdrücke, die Sie ausgewählt oder erstellt haben. In der dritten Spalte können Sie einen der anderen Operatoren in der folgenden Liste platzieren, um komplexe Richtliniengruppen zu erstellen, in denen jede Gruppe für die Übereinstimmung mit einem beliebigen Ausdruck oder für die Übereinstimmung mit allen Ausdrücken konfiguriert werden kann.
   - Der Operator AND [&&] weist die Appliance an, dass eine Anforderung sowohl mit dem aktuellen Ausdruck als auch dem folgenden Ausdruck übereinstimmt.

Der Operator ODER [\ \		] weist die Appliance an, dass eine Anforderung entweder mit dem aktuellen Ausdruck oder dem folgenden Ausdruck oder beidem übereinstimmt. Nur wenn die Anforderung nicht mit einem Ausdruck übereinstimmt, stimmt sie nicht mit der Richtlinie überein.

-
- Der Operator END [)] teilt der Appliance mit, dass dies der letzte Ausdruck in dieser Ausdrucksgruppe oder Richtlinie ist.
  Hinweis: Das tabellarische Format ermöglicht es Ihnen, eine komplexe Richtlinie zu erstellen, die sowohl Beliebigen Ausdruck zuordnen als auch Alle Ausdrücke abgleichen enthält. Sie sind nicht nur auf das eine oder andere beschränkt.
- Erweiterte Freiform Schaltet den Ausdruckseditor vollständig aus und ändert die Ausdrucksliste in einen Textbereich. Im Textbereich können Sie den regulären Ausdruck des PCRE-Formats Ihrer Wahl eingeben, um diese Richtlinie zu definieren. Dies ist sowohl die leistungsstärkste als auch die schwierigste Methode zum Erstellen einer Richtlinie und wird nur für diejenigen empfohlen, die mit der regulären Ausdrücken im Citrix ADC Appliance- und PCRE-Format vertraut sind.
  Achtung: Wenn Sie in den erweiterten Bearbeitungsmodus für Freiformausdrücke wechseln, können Sie nicht zu einem der anderen Modi zurückkehren. Wählen Sie diesen Ausdruckbearbeitungsmodus nur dann aus, wenn Sie sicher sind, dass dies das ist, was Sie wollen.

10. Wiederholen Sie die Schritte 6 bis 8, um der Liste Ausdrücke weitere Ausdrücke hinzuzufügen. Sie können benannte Ausdrücke und Ausdrücke mischen, die im Ausdruckseditor erstellt wurden. Für die Citrix ADC Appliance sind sie alle gleich.
11. Klicken Sie auf Erstellen, um Ihre neue Richtlinie zu erstellen. Die neue Richtlinie wird in der Liste Richtlinien angezeigt.
12. Klicken Sie auf **Schließen**. Wiederholen Sie den vorherigen Vorgang, um zusätzliche Inhaltsfilterrichtlinien zu erstellen. Um eine Inhaltsfilterrichtlinie zu entfernen, wählen Sie die Richtlinie auf der Registerkarte **Richtlinien** aus, und klicken Sie auf **Entfernen**.

Binden einer Inhaltsfilterrichtlinie

October 5, 2021

Sie müssen jede Inhaltsfilterrichtlinie binden, um sie in Kraft zu setzen. Sie können Richtlinien global oder an einen bestimmten virtuellen Server binden. Globale Richtlinien werden jedes Mal ausgewertet, wenn der an einen virtuellen Server gerichtete Datenverkehr mit der Richtlinie übereinstimmt. Richtlinien, die an einen bestimmten virtuellen Server gebunden sind, werden nur ausgewertet, wenn dieser virtuelle Server Datenverkehr erhält, der der Richtlinie entspricht.

Binden einer Richtlinie an einen virtuellen Server über die CLI

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

```
1 -  bind lb vserver <name>@ -policyName <string> -priority <
     positive_integer>
2 -  show lb vserver <name>
3 <!--NeedCopy-->
```

Beispiel:

```
1 > bind lb vserver vs-loadbal -policyName policyTwo -priority 100
2  Done
3 > show lb vserver vs-loadbal
4 1)      vs-loadbal (10.102.29.20:80) - HTTP     Type: ADDRESS
5         State: OUT OF SERVICE
6         Last state change was at Wed Aug 19 09:05:47 2009 (+211 ms)
7         Time since last state change: 2 days, 00:58:03.260
8         Effective State: DOWN
9         Client Idle Timeout: 180 sec
10        Down state flush: ENABLED
11        Disable Primary Vserver On Down : DISABLED
12        Port Rewrite : DISABLED
13        No. of Bound Services :  0 (Total)       0 (Active)
14        Configured Method: LEASTCONNECTION
15        Mode: IP
16        Persistence: NONE
17        Vserver IP and Port insertion: OFF
18        Push: DISABLED  Push VServer:
```



```
19          Push Multi Clients: NO
20          Push Label Rule: none
21
22  Done
23 <!--NeedCopy-->
```

Globale Bindung einer Richtlinie über die CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Richtlinie global zu binden und die Konfiguration zu überprüfen:

```
1 - bind filter global (<policyName> [-priority <positive_integer>]) [-
     state ( ENABLED | DISABLED )]
2 - show filter global
3 <!--NeedCopy-->
```

Beispiel:

```
1  bind filter global cf-pol -priority 1
2  Done show filter global
3 1)      Policy Name: cf-pol     Priority: 1
4  Done
5 <!--NeedCopy-->
```

Binden einer Richtlinie an einen virtuellen Server mit der GUI

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Wählen Sie im Detailbereich den virtuellen Server aus, an den Sie die Inhaltsfilterrichtlinie binden möchten, aus der Liste aus, und klicken Sie auf **Öffnen**.
3. Aktivieren **Sie im Dialogfeld Virtuellen Server konfigurieren** (Load Balancing) die Registerkarte **Richtlinien**, und aktivieren Sie dann das Kontrollkästchen in der Spalte Aktiv der Filterrichtlinie, die Sie an den virtuellen Server binden möchten.
4. Klicken Sie auf **OK**. Die Richtlinien, die Sie gebunden haben, zeigen ein Häkchen und das Wort Ja in der Spalte Richtlinien gebunden auf der Registerkarte Richtlinien an.

Globale Bindung einer Richtlinie über die GUI

1. Navigieren Sie zu **Sicherheit > Schutzfunktionen > Filter**.

2. Wählen Sie im Detailbereich auf der Registerkarte **Richtlinien** die Richtlinie aus, die Sie binden möchten, und klicken Sie dann auf **Globale Bindungen**.
3. Wählen Sie im Dialogfeld Filterrichtlinien binden/aufheben in der Dropdownliste **Richtliniennamen** eine Richtlinie aus, und klicken Sie dann auf **Hinzufügen**. Die Richtlinie wird der Liste Konfiguriert hinzugefügt.

   > **Hinweis:**
   >
   > Um mehrere Richtlinien aus der Liste auszuwählen, ziehen Sie die Strg-Taste und klicken Sie dann auf jede gewünschte Richtlinie.

4. Klicken Sie auf **OK**und dann auf **Schließen**. Die Richtlinien, die Sie gebunden haben, werden in der Spalte Globally Bound auf der Registerkarte Richtlinien ein Häkchen und das Wort Ja angezeigt.

Konfigurieren der Inhaltsfilterung für ein häufig verwendetes Bereitstellungsszenario

October 5, 2021

Dieses Beispiel enthält Anweisungen zur Verwendung des Konfigurationsdienstprogramms zur Implementierung einer Inhaltsfilterrichtlinie, in der, wenn eine angeforderte URL root.exe oder cmd.exe enthält, die Richtlinie zur `filter-CF-nimda` Inhaltsfilterung ausgewertet und die Verbindung zurückgesetzt wird.

Um diese Inhaltsfilterrichtlinie zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

- Inhaltsfilterung aktivieren
- Konfigurieren der Inhaltsfilterrichtlinie
- Inhaltsfilterrichtlinie global oder an einen virtuellen Server binden
- Überprüfen der Konfiguration

Hinweis: Da in diesem Beispiel eine standardmäßige Inhaltsfilteraktion verwendet wird, müssen Sie keine separate Inhaltsfilteraktion erstellen.

Inhaltsfilterung aktivieren

1. Erweitern Sie im Navigationsbereich System, und klicken Sie auf Einstellungen.
2. Klicken Sie im Detailbereich unter Modi & Features auf Grundfunktionen ändern.
3. Aktivieren Sie im Dialogfeld Grundfunktionen konfigurieren das Kontrollkästchen Inhaltsfilterung, und klicken Sie dann auf OK.

4. Klicken Sie im Dialogfeld Feature (en) aktivieren/deaktivieren auf Ja. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das ausgewählte Feature aktiviert ist.

Konfigurieren der Richtlinie zur Inhaltsfilterung `filter-CF-nimda`

1. Navigieren Sie zu Sicherheit > Schutzfunktionen > Filter.
2. Klicken Sie im Detailbereich auf "Hinzufügen". Das Dialogfeld Filterrichtlinie erstellen wird angezeigt.
3. Geben Sie im Dialogfeld Filterrichtlinie erstellen im Textfeld Filtername den Namen ein `filter-CF-nimda`.
4. Wählen Sie die Option Aktion anfordern, und wählen Sie in der Dropdownliste die Option RESET aus.
5. Wählen Sie im Rahmen Ausdruck die Option Beliebiger Ausdruck aus der Dropdownliste aus, und klicken Sie dann auf Hinzufügen.
6. Wählen Sie im Dialogfeld Ausdruck hinzufügen in der Dropdownliste Ausdruckstyp die Option Allgemein aus.
7. Wählen Sie in der Dropdownliste Flow Type die Option REQ aus.
8. Wählen Sie in der Dropdownliste Protokoll die Option HTTP aus.
9. Wählen Sie in der Dropdownliste Qualifier die Option URL aus.
10. Wählen Sie in der Dropdownliste Operator die Option CONTAINS aus.
11. Geben Sie im Textfeld Wert cmd.exe ein, und klicken Sie dann auf OK. Der Ausdruck wird im Textfeld Ausdruck hinzugefügt.
12. Um einen anderen Ausdruck zu erstellen, wiederholen Sie die Schritte 7 bis 11, geben Sie jedoch im Textfeld Wert root.exe ein. Klicken Sie dann auf OK und schließlich auf Schließen.
13. Klicken Sie im Dialogfeld Filterrichtlinie erstellen auf Erstellen. Die Filterrichtlinie `filter-CF-nimda` wird in der Filterliste angezeigt.
14. Klicken Sie auf Schließen.

Globale Bindung der Inhaltsfilterrichtlinie

1. Navigieren Sie zu Sicherheit > Schutzfunktionen > Filter. Die Seite Filter wird im rechten Fensterbereich angezeigt.
2. Wählen Sie im Detailbereich auf der Registerkarte Richtlinien die Richtlinie aus, die Sie binden möchten, und klicken Sie auf Globale Bindungen. Das Dialogfeld Filterrichtlinien binden/aufheben wird angezeigt.
3. Wählen Sie im Dialogfeld Filterrichtlinien binden/aufheben in der Dropdownliste Richtliniennamen die Richtlinie aus `filter-CF-nimda`, und klicken Sie auf Hinzufügen. Die Richtlinie wird der Liste Konfiguriert hinzugefügt.
4. Klicken Sie auf OKund dann auf Schließen. Die Richtlinie, die Sie gebunden haben, zeigt ein Häkchen und Ja in der Spalte Globally Bound der Registerkarte Richtlinien an.

Binden der Inhaltsfilterrichtlinie an einen virtuellen Server

1. Navigieren Sie zu Traffic Management > Load Balancing > Virtuelle Server.
2. Wählen Sie in der Liste der virtuellen Server im Detailbereich vServer-CF-1 aus, an den Sie die Inhaltsfilterrichtlinie binden möchten, und klicken Sie auf Öffnen.
3. Wählen Sie im Dialogfeld Virtuellen Server konfigurieren (Load Balancing) die Registerkarte Richtlinien aus.
4. Aktivieren Sie in der Spalte Aktiv das Kontrollkästchen für die Richtlinie `filter-CF-nimda`, und klicken Sie dann auf OK. Ihre Richtlinie zur Inhaltsfilterung ist jetzt aktiv und muss Anfragen filtern. Wenn es ordnungsgemäß funktioniert, wird der Auswahlzähler jedes Mal erhöht, wenn eine Anfrage nach einer URL besteht, die entweder root.exe oder cmd.exe enthält. Auf diese Weise können Sie bestätigen, dass Ihre Inhaltsfilterrichtlinie funktioniert. Die Inhaltsfilterrichtlinie ist an den virtuellen Server gebunden.

Überprüfen der Content-Filterkonfiguration über die Befehlszeile

Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, um die Konfiguration der Inhaltsfilterung zu überprüfen:

```
show filter policy filter-CF-nimda
```

Beispiel:

```
1 sh filter policy filter-CF-nimda
2         Name: filter-CF-nimda   Rule: REQ.HTTP.URL CONTAINS cmd.exe ||
             REQ.HTTP.URL CONTAINS root.exe
3         Request action: RESET
4         Response action:
5         Hits: 0
6 Done
7 <!--NeedCopy-->
```

> **Hinweis:**
>
> Der Auswahlzähler zeigt eine Ganzzahl an, die angibt, wie oft die `filter-CF-nimda` Richtlinie ausgewertet wird. In den vorhergehenden Schritten wird der Auswahlzähler auf Null gesetzt, da noch keine Anfragen für eine URL gestellt wurden, die entweder cmd.exe oder root.exe enthält. Wenn Sie das Zählerinkrement in Echtzeit sehen möchten, können Sie einfach eine URL anfordern, die eine dieser Zeichenfolgen enthält.

Überprüfen der Content-Filterkonfiguration über die GUI

1. Navigieren Sie zu **Sicherheit > Schutzfunktionen > Filter**.
2. Wählen Sie im Detailbereich die Filterrichtlinie aus `filter-CF-nimda`. Am unteren Rand des Bereichs muss Folgendes angezeigt werden:

```
    \*\*Request Action:\*\*

    RESET

    \*\*Rule:\*\*

    REQ.HTTP.URL CONTAINS cmd.exe || REQ.HTTP.URL CONTAINS root.exe

    \*\*Hits:\*\*

    0
<!--NeedCopy-->
```

Problembehandlung

October 5, 2021

Wenn die Inhaltsfilterfunktion nach der Konfiguration nicht wie erwartet funktioniert, können Sie einige gängige Tools verwenden, um auf Citrix ADC Ressourcen zuzugreifen und das Problem zu diagnostizieren.

Ressourcen für die Fehlerbehebung

Sie können die folgenden Tools und Ressourcen verwenden, um die meisten Content-Filterprobleme auf einer Citrix ADC Appliance zu beheben:

- Die für Citrix ADC C-Trace-Dateien angepasste Wireshark-Anwendung
- Beim Zugriff auf die Ressource aufgezeichnete Trace-Dateien
- Die Konfigurationsdateien
- Die Datei ns.log
- Der `iehttpheaders`oder ein Fiddler-Trace oder ein ähnliches Dienstprogramm

Beheben von Problemen mit der Inhaltsfilterung

Gehen Sie wie folgt vor, um ein Problem mit der Inhaltsfilterung zu beheben:

- Stellen Sie sicher, dass das Feature aktiviert ist.
- Stellen Sie sicher, dass die Inhaltsfilterrichtlinie korrekt konfiguriert ist. Achten Sie besonders auf den Ausdruck, der die eingehenden Anfragen auswertet.

  > **Hinweis:**
  >
  > Die meisten Probleme mit der Inhaltsfilterung werden durch eine falsche Konfiguration verursacht, und der Fehler liegt am häufigsten in der Richtlinienkonfiguration.

- Überprüfen Sie den Auswahlzähler der Richtlinie, um sicherzustellen, dass sie inkrementiert wird. Ist dies nicht der Fall, wird die Richtlinie nicht ausgewertet.
- Wenn die Richtlinie ausgewertet wird und die erforderliche Filterung immer noch nicht durchgeführt wird, müssen Sie sich die Richtlinienausdrücke und -aktion ansehen.
- Wenn der Ausdruck der Richtlinie gültig erscheint, testen Sie ihn, indem Sie einen einfachen NSTRUE-Wert zuweisen, um festzustellen, ob die Auswertung des Ausdrucks ein Problem verursacht.
- Bewerten Sie erneut, ob die Filterung auf der Anfrage oder der Antwort basieren muss.
- Stellen Sie sicher, dass die Aktion korrekt konfiguriert ist. Wenn beispielsweise eine benutzerdefinierte Aktion verwendet wird, um einen Header in der Anforderung zu beschädigen, stellen Sie sicher, dass der Headername in der Aktion korrekt ist. Wenn Sie sich über den Header-Namen nicht sicher sind, starten Sie einen Browser mit `iehttpheaders` oder einem ähnlichen Dienstprogramm und überprüfen Sie dann die Header in der Anforderung. Wenn diese Funktion verwendet wird, können Sie mit ns trace herausfinden, ob eine entsprechende Aktion ausgeführt wird, wenn die Pakete die Citrix ADC Appliance verlassen.
- Ein `iehttpheaders` oder Fiddler-Trace kann Ihnen helfen, Header-Optionen und -Namen, clientseitige Anforderungsheader und Antwort-Header zu finden, die auf dem Client aufgezeichnet wurden.
- Um die am Anforderungsheader vorgenommenen Änderungen zu überprüfen, zeichnen Sie eine NS-Ablaufverfolgung auf der Citrix ADC Appliance oder eine Wireshark-Trace auf dem Server auf.
- Wenn keine der oben genannten Maßnahmen das Problem behebt, stellen Sie sicher, dass die Verbindung nicht mehr verfolgt werden kann, was unter bestimmten Umständen auftreten kann. Wenn eine Verbindung nicht mehr verfolgt werden kann, führt die Appliance keine Verarbeitung der Anforderungen auf Anwendungsebene durch. Wenden Sie sich in diesem Fall an den technischen Support von Citrix.

Überlastungsschutz

January 25, 2022

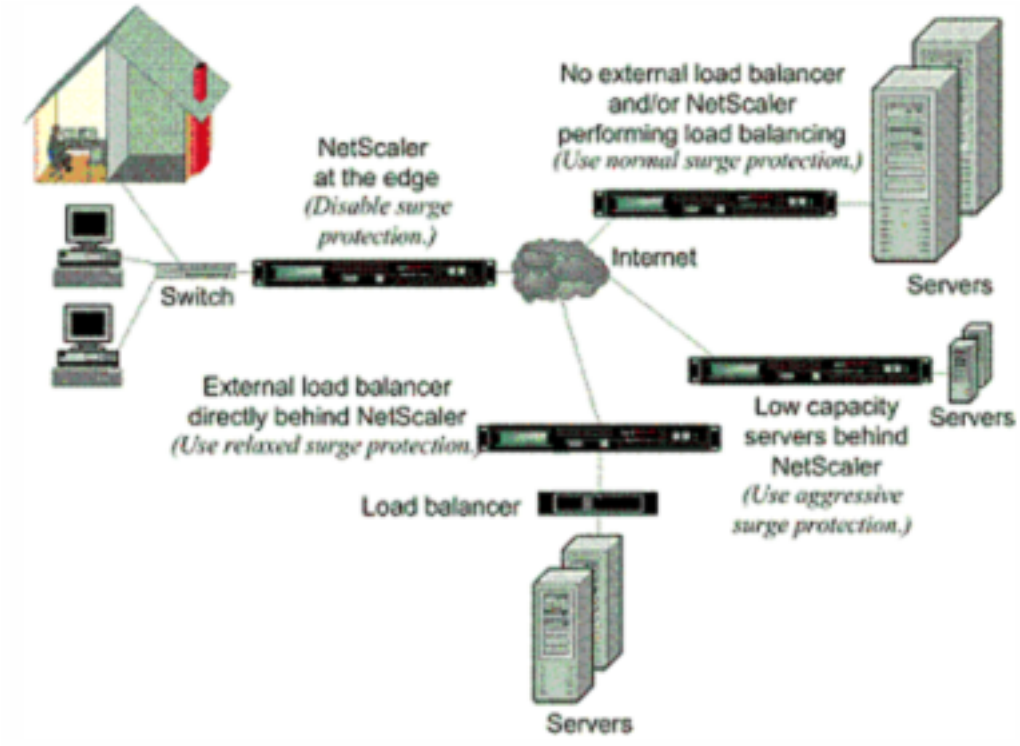
Wenn ein Anstieg der Clientanforderungen einen Server überlastet, wird die Serverantwort langsam und der Server kann nicht auf neue Anfragen reagieren. Die Überlastungsschutzfunktion stellt sicher, dass Verbindungen zum Server mit einer Geschwindigkeit hergestellt werden, die der Server verarbeiten kann. Die Rücklaufquote hängt davon ab, wie der Überlastungsschutz konfiguriert ist. Die Citrix ADC-Appliance verfolgt auch die Anzahl der Verbindungen zum Server und verwendet diese Informationen, um die Geschwindigkeit anzupassen, mit der neue Serververbindungen geöffnet werden.

Der Überlastungsschutz ist standardmäßig aktiviert. Wenn Sie keinen Überlastungsschutz verwenden möchten, wie es bei einigen speziellen Konfigurationen der Fall ist, müssen Sie ihn deaktivieren.

Die Standardeinstellungen für den Überlastungsschutz sind für die meisten Anwendungen ausreichend. Sie können den Überlastungsschutz jedoch so konfigurieren, dass er Ihren Anforderungen entspricht. Zuerst können Sie den Drosselungswert festlegen, um ihm mitzuteilen, wie aggressiv Verbindungsversuche verwaltet werden sollen. Zweitens können Sie den Basisschwellenwert festlegen, um die maximale Anzahl gleichzeitiger Verbindungen zu steuern, die die Citrix ADC-Appliance zulässt, bevor der Überlastungsschutz ausgelöst wird. (Der Standard-Basisschwellenwert wird durch den Drosselungswert festgelegt, aber nachdem Sie den Drosselungswert festgelegt haben, können Sie ihn in eine beliebige Zahl ändern.)

Die folgende Abbildung zeigt, wie der Überlastungsschutz so konfiguriert ist, dass der Datenverkehr auf eine Website verarbeitet wird.

Abbildung 1. Eine funktionale Illustration des Citrix ADC Überlastungsschutzes



Hinweis

Wenn die Citrix ADC-Appliance am Rand des Netzwerks installiert ist und wo sie mit Netzwerkgeräten auf der Clientseite des Internets interagiert, muss die Überlastungsschutzfunktion deaktiviert sein. Überlastungsschutz muss auch deaktiviert werden, wenn Sie den USIP-Modus (Using Source IP) auf Ihrer Appliance aktivieren.

Das folgende Beispiel und die folgende Abbildung zeigen die Anfrage- und Rücklaufquoten für zwei Fälle. In einem Fall ist der Überlastungsschutz deaktiviert und in dem anderen Fall ist er aktiviert.

Wenn der Überlastungsschutz deaktiviert ist und ein Anstieg der Anforderungen auftritt, akzeptiert der Server so viele Anforderungen, wie er gleichzeitig verarbeiten kann, und beginnt dann, Anforderungen zu verwerfen. Wenn der Server mehr überlastet wird, sinkt er und die Antwortrate wird auf Null reduziert. Wenn sich der Server einige Minuten später vom Absturz erholt, sendet er Resets für alle ausstehenden Anfragen, bei denen es sich um ein abnormales Verhalten handelt, und reagiert auch auf neue Anfragen mit Resets. Der Prozess wiederholt sich für jede Überspannung in Anforderungen. Daher kann ein Server, der unter DDoS-Angriff steht und mehrere Anfragen erhält, für legitime Benutzer nicht verfügbar sein.

Wenn der Überlastungsschutz aktiviert ist und ein Anstieg der Anforderungen auftritt, verwaltet der Überlastungsschutz die Rate der Anfragen an den Server und sendet Anfragen nur so schnell an den Server, wie der Server diese Anforderungen verarbeiten kann. Auf diese Weise kann der Server auf jede Anfrage korrekt in der Reihenfolge antworten, in der sie empfangen wurde. Wenn der Anstieg vorbei ist, werden die rückgestellten Anforderungen so schnell gelöscht, wie der Server sie verarbeiten kann,

bis die Anforderungsrate mit der Rücklaufquote übereinstimmt.

Überspannungsschutz deaktivieren und wieder aktivieren

October 5, 2021

Die Überspannungsschutzfunktion ist standardmäßig aktiviert. Wenn der Überspannungsschutz aktiviert ist, ist er für jeden von Ihnen hinzugefügten Dienst aktiv.

Deaktivieren oder erneutes Aktivieren des Überspannungsschutzes über die CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um den Überspannungsschutz zu deaktivieren oder erneut zu aktivieren und die Konfiguration zu überprüfen:

```
- disable ns feature SurgeProtection
- show ns feature
- enable ns feature SurgeProtection
- show ns feature
<!--NeedCopy-->
```

Beispiel:

```
disable ns feature SurgeProtection
 Done show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  ON
 2)     Surge Protection                SP                  OFF
 .
 .
 .
 23)    HTML Injection                  HTMLInjection       ON
 24)    Citrix ADC Push                  push                OFF
 Done
<!--NeedCopy-->
```



```
 enable ns feature SurgeProtection
 Done
> show ns feature

        Feature                         Acronym             Status
        -------                         -------             ------
 1)     Web Logging                     WL                  ON
 2)     Surge Protection                SP                  ON
 .
 .
 .

 23)    HTML Injection                  HTMLInjection       ON
 24)    Citrix ADC Push                  push                OFF
 Done
>
<!--NeedCopy-->
```

Deaktivieren oder erneutes Aktivieren des Überspannungsschutzes über die GUI

1. Erweitern Sie im Navigationsbereich **System**, und wählen Sie dann **Einstellungen**aus.
2. Klicken Sie im Detailbereich auf **Erweiterte Funktionen ändern**.
3. Deaktivieren **Sie im Dialogfeld Erweiterte Funktionen konfigurieren** die Auswahl aus dem Kontrollkästchen **Überspannungsschutz**, um die Überspannungsschutzfunktion zu deaktivieren, oder aktivieren Sie das Kontrollkästchen, um das Feature zu aktivieren.
4. Klicken Sie auf **OK**.
5. Klicken Sie im Dialogfeld Features aktivieren/deaktivieren auf Ja. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das Feature aktiviert oder deaktiviert wurde.

Deaktivieren oder erneutes Aktivieren des Überspannungsschutzes für einen bestimmten Dienst über die GUI

1. Navigieren Sie zu Traffic Management > Load Balancing > Services. Die Liste der konfigurierten Dienste wird im Detailbereich angezeigt.
2. Wählen Sie im Detailbereich den Dienst aus, für den Sie die Überspannungsschutzfunktion deaktivieren oder erneut aktivieren möchten, und klicken Sie dann auf Öffnen.
3. Klicken Sie im Dialogfeld Dienst konfigurieren auf die Registerkarte Erweitert, und führen Sie einen Bildlauf nach unten durch.
4. Deaktivieren Sie im Rahmen Sonstiges die Auswahl des Kontrollkästchens Überspannungsschutz, um das Überspannungsschutz-Feature zu deaktivieren, oder aktivieren Sie das Kontrollkästchen, um das Feature zu aktivieren.

5. Klicken Sie auf OK. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass das Feature aktiviert oder deaktiviert wurde.
   Hinweis: Der Überspannungsschutz funktioniert nur, wenn sowohl das Feature als auch die Service-Einstellung aktiviert sind.

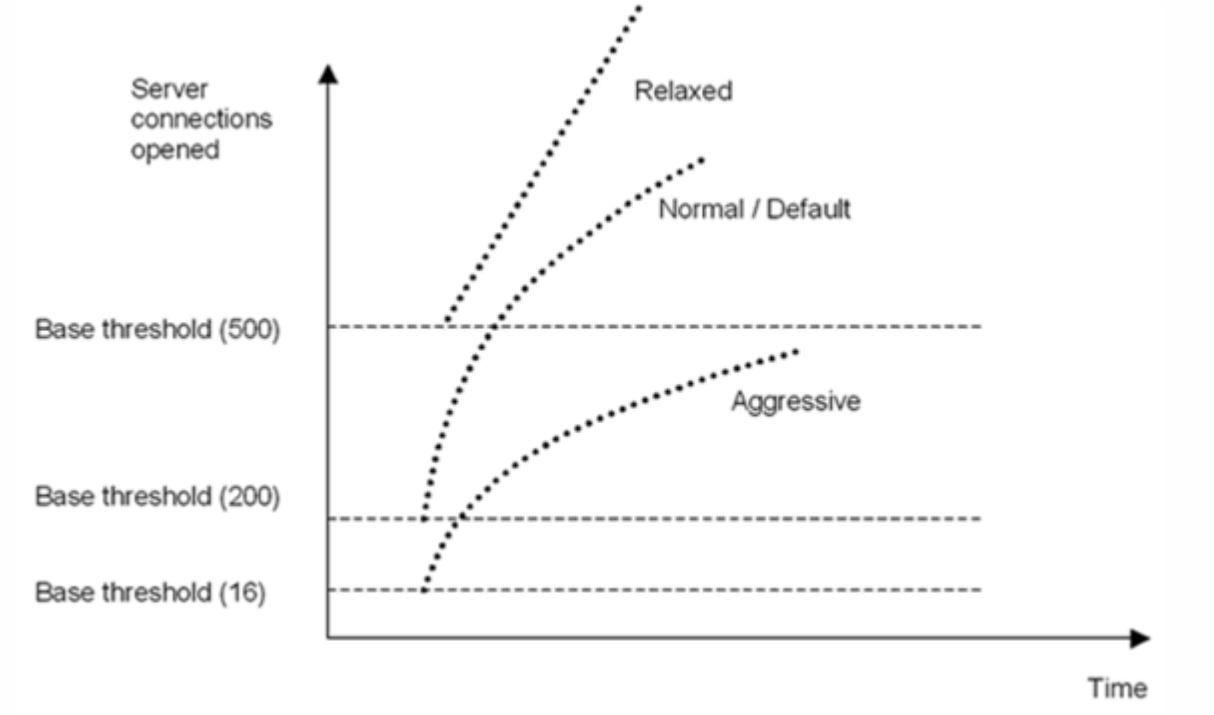
Grenzwerte für Überspannungsschutz festlegen

October 5, 2021

Um die Geschwindigkeit festzulegen, mit der die Citrix ADC Appliance Verbindungen zum Server öffnet, müssen Sie den Schwellenwert und die Drosselklappe für den Überspannungsschutz konfigurieren.

Die folgende Abbildung zeigt die Überspannungsschutzkurven, die sich aus der Einstellung der Drosselklappe auf entspannt, normal oder aggressiv ergeben. Abhängig von der Konfiguration der Serverkapazität können Sie Basisschwellenwerte festlegen, um geeignete Überspannungsschutzkurven zu generieren.

Abbildung 1. Überspannungsschutzkurven

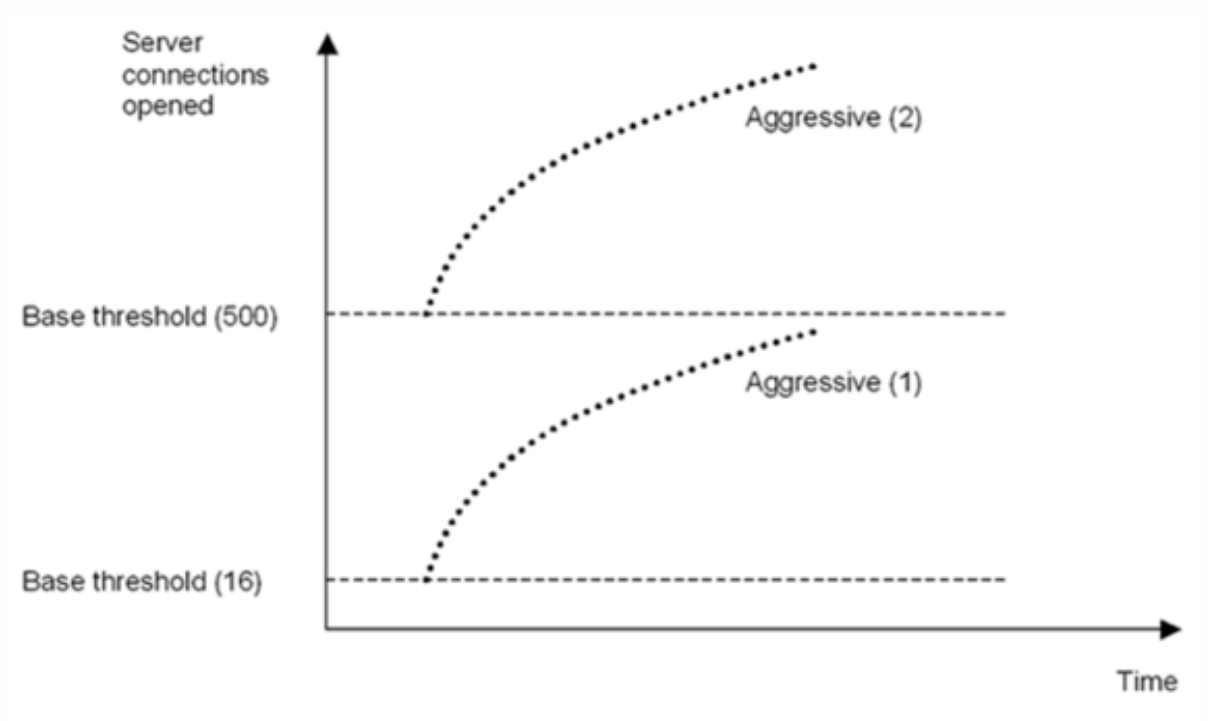


Die Konfigurationseinstellungen beeinflussen das Verhalten des Überspannungsschutzes folgendermaßen:

- Wenn Sie keine Drosselungsrate angeben, wird sie auf normal (Standardwert) und der Basisschwellenwert auf 200 gesetzt, wie in der vorhergehenden Abbildung gezeigt.
- Wenn Sie eine Drosselungsrate (aggressiv, normal oder entspannt) angeben, ohne einen Basisschwellenwert anzugeben, spiegelt die Kurve die Standardwerte des Basisschwellenwerts für diese Drosselungsrate wider. Wenn Sie beispielsweise die Drosselungsrate auf entspannt festlegen, hat die resultierende Kurve den Basisschwellenwert von 500.
- Wenn Sie nur den Basisschwellenwert angeben, wird die gesamte Überspannungsschutzkurve je nach dem angegebenen Wert nach oben oder unten verschoben, wie in der folgenden Abbildung dargestellt.
- Wenn Sie sowohl einen Basisschwellen- als auch eine Drosselungsrate angeben, wird die resultierende Überspannungsschutzkurve auf der eingestellten Drosselungsrate basiert und entsprechend dem für den Basisschwellenwert eingestellten Wert angepasst.

In der folgenden Abbildung ergibt sich die untere Kurve (Aggressive 1), wenn die Drosselungsrate auf aggressiv eingestellt ist, aber der Basisschwellenwert nicht festgelegt ist. Die obere Kurve (Aggressive 2) ergibt sich, wenn der Basisschwellenwert auf 500 gesetzt ist, die Drosselungsrate jedoch nicht festgelegt ist. Die zweite obere Kurve (Aggressive 2) ergibt auch, wenn die Basisschwelle auf 500 gesetzt ist und die Drosselklappe auf aggressiv eingestellt ist.

Abbildung 2. Aggressive Rate mit dem Standardwert oder einem festgelegten Basisschwellenwert



Stellen Sie den Schwellenwert für den Überspannungsschutz über die GUI ein

1. Erweitern Sie im Navigationsbereich System, und wählen Sie dann Einstellungen aus.
2. Klicken Sie im Detailbereich auf Globale Systemeinstellungen.
3. Wenn Sie einen anderen Basisschwellenwert als der Standardwert für die Drosselungsrate festlegen möchten, geben Sie im Dialogfeld Globale Einstellungen konfigurieren im Textfeld Basisschwellenwert die maximale Anzahl gleichzeitiger Serververbindungen ein, die zulässig sind, bevor Überspannungsschutz ausgelöst wird. Der Basis-Schwellenwert ist die maximale Anzahl von Serververbindungen, die geöffnet werden können, bevor der Überspannungsschutz aktiviert wird. Der maximale Wert für diese Einstellung beträgt 32.767 Serververbindungen. Die Standardeinstellung für diesen Wert wird durch die Drosselungsrate gesteuert, die Sie im nächsten Schritt auswählen.

   Hinweis: Wenn Sie hier keinen expliziten Wert festlegen, wird der Standardwert verwendet.
4. Wählen Sie in der Dropdownliste Drosselklappe eine Drosselungsrate aus. Die Drosselklappe ist die Geschwindigkeit, mit der die Citrix ADC Appliance das Öffnen von Verbindungen zum Server zulässt. Die Drosselklappe kann auf folgende Werte eingestellt werden:
   - **Aggressiv:** Wählen Sie diese Option, wenn die Verbindungs- und Überspannungskapazität des Servers gering ist und die Verbindung sorgfältig verwaltet werden muss. Wenn Sie die Drosselklappe auf aggressiv einstellen, wird der Basisschwellenwert auf den Standardwert 16 festgelegt. Dies bedeutet, dass Überspannungsschutz ausgelöst wird, wenn 17 oder mehr gleichzeitige Verbindungen zum Server vorhanden sind.
   - **Normal:** Wählen Sie diese Option, wenn hinter der Citrix ADC Appliance oder Downstream kein externer Load Balancer vorhanden ist. Der Basisschwellenwert ist auf den Wert 200 festgelegt, was bedeutet, dass Überspannungsschutz ausgelöst wird, wenn 201 oder mehr gleichzeitige Verbindungen zum Server vorhanden sind. Normal ist die Standarddrosseloption.
   - **Entspannt:** Wählen Sie diese Option, wenn die Citrix ADC Appliance Lastenausgleich zwischen einer großen Anzahl von Webservern durchführt und daher eine hohe Anzahl gleichzeitiger Verbindungen verarbeiten kann. Der Basisschwellenwert ist auf den Wert 500 festgelegt, was bedeutet, dass Überspannungsschutz nur ausgelöst wird, wenn 501 oder mehr gleichzeitige Verbindungen zum Server vorhanden sind.
5. Klicken Sie auf OK. In der Statusleiste wird eine Meldung angezeigt, die besagt, dass die globalen Einstellungen konfiguriert sind.

Überspannungswarteschlange leeren

October 5, 2021

Wenn ein physischer Server eine Welle von Anforderungen empfängt, wird es langsam, auf die Clients zu reagieren, die derzeit mit ihm verbunden sind, was die Benutzer unzufrieden und verärgert lässt. Oft führt die Überlastung auch dazu, dass Clients Fehlerseiten erhalten. Um solche Überlastungen zu vermeiden, bietet die Citrix ADC Appliance Funktionen wie Überspannungsschutz, die die Geschwindigkeit steuert, mit der neue Verbindungen zu einem Dienst hergestellt werden können.

Die Appliance verbindet Multiplexing zwischen Clients und physischen Servern. Wenn es eine Clientanforderung für den Zugriff auf einen Dienst auf einem Server erhält, sucht die Appliance nach einer bereits eingerichteten Verbindung mit dem Server, die frei ist. Wenn eine freie Verbindung gefunden wird, wird diese Verbindung verwendet, um eine virtuelle Verbindung zwischen dem Client und dem Server herzustellen. Wenn keine vorhandene freie Verbindung gefunden wird, stellt die Appliance eine neue Verbindung mit dem Server her und stellt eine virtuelle Verbindung zwischen einem Client und dem Server her. Wenn die Appliance jedoch keine neue Verbindung mit dem Server herstellen kann, sendet sie die Clientanforderung an eine Überspannungswarteschlange. Wenn alle physischen Server, die an den virtuellen Lastausgleichs- oder Content Switching-Server gebunden sind, die obere Grenze für Clientverbindungen erreichen (maximaler Clientwert, Überspannungsschutzschwelle oder maximale Kapazität des Dienstes), kann die Appliance keine Verbindung zu einem Server herstellen. Die Überspannungsschutzfunktion verwendet die Überspannungswarteschlange, um die Geschwindigkeit zu regulieren, mit der Verbindungen mit den physischen Servern geöffnet werden. Die Appliance verwaltet eine andere Überspannungswarteschlange für jeden Dienst, der an den virtuellen Server gebunden ist.

Die Länge einer Überspannungswarteschlange erhöht sich, wenn eine Anforderung eingeht, für die die Appliance keine Verbindung herstellen kann, und die Länge nimmt ab, wenn eine Anforderung in der Warteschlange an den Server gesendet wird oder eine Anforderung ein Timeout erreicht und aus der Warteschlange entfernt wird.

Wenn die Überspannungswarteschlange für einen Dienst oder eine Dienstgruppe zu lang wird, können Sie sie löschen. Sie können die Überspannungswarteschlange eines bestimmten Dienstes oder einer bestimmten Dienstgruppe oder aller Dienste und Dienstgruppen, die an einen virtuellen Lastausgleichsserver gebunden sind, leeren. Das Leeren einer Überspannungswarteschlange wirkt sich nicht auf die vorhandenen Verbindungen aus. Nur die Anforderungen, die in der Überspannungswarteschlange vorhanden sind, werden gelöscht. Für diese Anfragen muss der Kunde eine neue Anfrage stellen.

Sie können auch die Überspannungswarteschlange eines virtuellen Content Switching-Servers löschen. Wenn ein virtueller Content Switching-Server einige Anfragen an einen bestimmten virtuellen Lastausgleichsserver weiterleitet und der virtuelle Lastausgleichsserver auch einige andere Anfragen empfängt, wenn Sie die Überspannungswarteschlange des virtuellen Content Switching-Servers leeren, nur die Anfragen, die von diesem Content Switching empfangen wurden virtuelle Server werden geleert. Die anderen Anforderungen in der Überspannungswarteschlange des virtuellen Lastausgleichsservers werden nicht geleert.

Hinweis:

> - Sie können die Anstiegswarteschlangen von Cache-Umleitungen, Authentifizierung, VPN oder virtuellen GSLB-Servern oder GSLB-Diensten nicht leeren.
> - Verwenden Sie die Überspannungsschutzfunktion nicht, wenn die Option “Quell-IP (USIP) verwenden” aktiviert ist.

Leere eine Überspannungswarteschlange über die CLI

Der Befehl flush ns SurgeQ funktioniert wie folgt:

- Sie können den Namen eines Dienstes, einer Dienstgruppe oder eines virtuellen Servers angeben, dessen Überspannungswarteschlange geleert werden muss.
- Wenn Sie während der Ausführung des Befehls einen Namen angeben, wird die Überspannungswarteschlange der angegebenen Entität geleert. Wenn mehrere Entitäten denselben Namen haben, leert die Appliance Überspannungswarteschlangen aller dieser Entitäten.
- Wenn Sie den Namen einer Dienstgruppe und einen Servernamen und einen Port angeben, während der Befehl ausgeführt wird, löscht die Appliance die Überspannungswarteschlange nur des angegebenen Dienstgruppenmitglieds.
- Sie können ein Dienstgruppenmitglied `<serverName> and <port>` nicht direkt angeben, ohne den Namen der Dienstgruppe anzugeben,`<name>` und Sie können nicht `<port>` ohne `<serverName>` angeben Geben Sie `<serverName>` und `<port>` an, wenn Sie die Überspannungswarteschlange für ein bestimmtes Dienstgruppenmitglied leeren möchten.
- Wenn Sie den Befehl ausführen, ohne Namen anzugeben, legt die Appliance die Überspannungswarteschlangen aller auf der Appliance vorhandenen Entitäten.
- Wenn ein Dienstgruppenmitglied mit einem Servernamen identifiziert wird, müssen Sie den Servernamen in diesem Befehl angeben. Sie können die IP-Adresse nicht angeben.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
flush ns surgeQ [-name <name>] [-serverName <serverName> <port>]
```

Beispiele

1. `flush ns surgeQ -name SVC1ANZGB -serverName 10.10.10.1 80`

   Der vorhergehende Befehl spült die Überspannungswarteschlange des Dienstes oder virtuellen Servers, der SVC1ANZGB genannt wird und die IP-Adresse als 10.10.10 hat

2. `flush ns surgeQ`

   Der vorhergehende Befehl spült alle Überspannungswarteschlangen auf der Appliance.

Leere eine Überspannungswarteschlange über die GUI

Navigieren Sie zu Traffic Management > Content Switching > Virtuelle Server, wählen Sie einen virtuellen Server aus und wählen Sie in der Liste Aktion die Option Flush Surge Queue löschen aus.

DNS-Sicherheitsoptionen

December 7, 2021

Sie können die DNS-Sicherheitsoptionen jetzt auf der Seite DNS-Sicherheitsprofil hinzufügen in der Citrix ADC GUI konfigurieren. Verwenden Sie die AppExpert t-Komponenten, um die DNS-Sicherheitsoptionen über die Citrix ADC CLI oder die NITRO-API zu konfigurieren. Anweisungen finden Sie in der NITRO API-Dokumentation und im Citrix ADC Command Reference Guide.

Eine Option, Cache-Vergiftungsschutz, ist standardmäßig aktiviert und kann nicht deaktiviert werden. Sie können die anderen Optionen auf alle DNS-Endpunkte oder auf bestimmte virtuelle DNS-Server in Ihrer Bereitstellung anwenden, wie in der folgenden Tabelle dargestellt:

Sicherheitsoption	Kann auf alle DNS-Endpunkte angewendet werden?	Kann auf bestimmte virtuelle DNS-Server angewendet werden?
DNS-DDoS-Schutz	Ja	Ja
Verwalten von Ausnahmen — Server für Positivliste/Sperrliste	Ja	Ja
Verhindern von zufälligen Subdomain-Angriffen	Ja	Ja
Cache umgehen	Ja	Nein
DNS-Transaktionen über TCP erzwingen	Ja	Ja
Geben Sie Stammdetails in der DNS-Antwort an	Ja	Nein

Cache-Vergiftungsschutz

Ein Cache-Vergiftungsangriff leitet Benutzer von legitimen Websites auf bösartige Websites um.

Beispielsweise ersetzt der Angreifer eine echte IP-Adresse im DNS-Cache durch eine gefälschte IP-

Adresse, die er kontrolliert. Wenn der Server auf Anfragen von diesen IP-Adressen reagiert, wird der Cache vergiftet. Nachfolgende Anfragen nach den Adressen der Domain werden an die Website des Angreifers weitergeleitet.

Die Option Cache-Vergiftungsschutz verhindert das Einfügen von beschädigten Daten in die Datenbank, die DNS-Server-Anforderungen und -Antworten zwischenspeichert. Diese Funktion ist in die Citrix ADC Appliances integriert und ist immer aktiviert.

DNS-DDoS-Schutz

Sie können die Option DNS-DDoS-Schutz für jeden Anforderungstyp konfigurieren, der bei einem DDoS-Angriff verwendet wird. Für jeden Typ lässt die Appliance alle Anfragen fallen, die empfangen werden, nachdem ein Schwellenwert für die Anzahl der Anfragen, die in einem bestimmten Zeitraum (Zeitscheibe) empfangen wurden, überschritten wurde. Sie können diese Option auch so konfigurieren, dass eine Warnung auf dem SYSLOG-Server protokolliert wird. Beispiel:

- **DROP:** - Wählen Sie diese Option aus, um Anfragen ohne Protokollierung abzulegen. Angenommen, Sie haben einen Datensatzschutz mit Schwellenwert 15, Zeitscheibe als 1 Sekunde aktiviert und DROP gewählt. Wenn die eingehenden Anfragen 15 Abfragen in 1 Sekunde überschreiten, werden die Pakete gelöscht.
- **WARN:** - Wählen Sie diese Option aus, um Anfragen zu PROTOKOLLIEREN und ABZULEGEN. Angenommen, Sie haben einen Datensatzschutz mit Schwellenwert 15, Zeitscheibe als 1 Sekunde aktiviert und WARN gewählt. Wenn die eingehenden Anfragen 15 Abfragen in einer Sekunde überschreiten, wird eine Warnmeldung protokolliert, die auf eine Bedrohung hinweist, und dann werden die Pakete gelöscht. Citrix empfiehlt Ihnen, Schwellenwerte für WARN festzulegen, die kleiner als den Schwellenwert von DROP für einen Datensatztyp sind. Eine solche Einstellung hilft Administratoren, einen Angriff zu identifizieren, indem sie eine Warnmeldung protokollieren, bevor der eigentliche Angriff stattfindet und Citrix ADC eingehende Anfragen fallen lässt.

Legen Sie über die grafische Benutzeroberfläche einen Schwellenwert für eingehenden Datenverkehr fest

1. Navigieren Sie zu **Konfiguration** > **Sicherheit** > **DNS-Sicherheit**.
2. Klicken Sie auf der Seite **DNS-Sicherheitsprofil** auf **Hinzufügen**.
3. Gehen Sie auf der Seite **DNS-Sicherheitsprofil hinzufügen** folgendermaßen vor:
4. Erweitern Sie **DNS-DDoS-Schutz**.
    a) Wählen Sie den Datensatztyp aus, und geben Sie den Schwellenwert und den Zeitschnitt-Wert ein.
    b) Wählen Sie **DROP** oder **WARN** .

c) Wiederholen Sie die Schritte a und b für alle anderen Datensatztypen, gegen die Sie schützen möchten.

5. Klicken Sie auf **Absenden**.

Ausnahmen verwalten — allowlist/blocklist-Server

Ausnahmen verwalten ermöglicht es Ihnen, Ausnahmen hinzuzufügen, um die Liste zu blockieren oder Listendomänennamen und IP-Adressen zuzulassen. Beispiel:

- Wenn eine bestimmte IP-Adresse beim Posten eines Angriffs identifiziert wird, kann eine solche IP-Adresse zur Sperrliste hinzugefügt werden.
- Wenn Administratoren feststellen, dass eine unerwartet hohe Anzahl von Anfragen für einen bestimmten Domänennamen vorliegt, kann dieser Domänenname zur Sperrliste hinzugefügt werden.
- `NXDomains` und einige der vorhandenen Domänen, die die Serverressourcen verbrauchen können, können auf die Sperrliste gesetzt werden.
- Wenn Administratoren Listendomänennamen oder IP-Adressen zulassen, werden Anfragen oder Anfragen nur von diesen Domänen oder IP-Adressen beantwortet und alle anderen werden gelöscht.

Erstellen Sie eine Zulassungsliste oder eine Sperrliste mit der GUI

1. Navigieren Sie zu **Konfiguration > Sicherheit > DNS-Sicherheit**.
2. Klicken Sie auf der Seite **DNS-Sicherheitsprofile** auf **Hinzufügen**.
3. Gehen Sie auf der Seite **DNS-Sicherheitsprofil hinzufügen** folgendermaßen vor:
   a) Erweitern Sie **Ausnahmen verwalten — Server der Positivliste/Sperrliste**.
   b) Wählen Sie **Blockieren** aus, um Abfragen von Domäne/Adressen aus der Sperrliste zu blockieren, oder wählen Sie **Zulassen** nur, um Abfragen von Domäne/Adressen aus der Positivliste zuzulassen.
   c) Geben Sie im Feld **Domänenname/IP-Adresse** die Domänennamen, IP-Adressen oder IP-Adressbereiche ein. Verwenden Sie Kommas, um die Einträge zu trennen.
   Hinweis: Wenn Sie **Erweiterte Option**auswählen, können Sie die Optionen “Start mit”, “enthält” und “endet mit” verwenden, um die Kriterien festzulegen.
   Sie können beispielsweise Kriterien festlegen, um eine DNS-Abfrage zu blockieren, die mit “image” beginnt oder mit “.co.ru” endet oder “mobile Websites enthält. “
4. Klicken Sie auf **Absenden**.

Verhindern von zufälligen Subdomain-Angriffen

Bei zufälligen Subdomain-Angriffen werden Abfragen an zufällige, nicht vorhandene Subdomänen legitimer Domänen gesendet. Diese Aktion erhöht die Belastung der DNS-Resolver und Server. In-

folgedessen können sie überlastet werden und sich verlangsamen.

Die Option Zufällige Subdomain-Angriffe verhindern weist den DNS-Responder an, DNS-Abfragen zu löschen, die eine angegebene Länge überschreiten.

Angenommen, example.com ist ein Domänenname, der Ihnen gehört, und daher kommt die Auflösungsanforderung an Ihren DNS-Server. Der Angreifer kann eine zufällige Subdomain an example.com anhängen und eine Anfrage senden. Basierend auf der angegebenen Abfragelänge und des FQDN werden die Zufallsabfragen gelöscht.

Wenn die Abfrage beispielsweise www.image987trending.example.com lautet, wird sie gelöscht, wenn die Abfragelänge auf 20 festgelegt ist.

Angeben einer DNS-Abfragelänge über die GUI

1. Navigieren Sie zu **Konfiguration > Sicherheit > DNS-Sicherheit**.
2. Klicken Sie auf der Seite **DNS-Sicherheitsprofile** auf **Hinzufügen**.
3. Gehen Sie auf der Seite **DNS-Sicherheitsprofil hinzufügen** folgendermaßen vor:
   a) Erweitern Sie **Zufällige Subdomain-Angriffe verhindern**.
   b) Geben Sie den numerischen Wert für die Abfragelänge ein.
4. Klicken Sie auf **Absenden**.

Umgehen des Caches

Während eines Angriffs müssen die Daten, die bereits zwischengespeichert sind, geschützt werden. Um den Cache zu schützen, können neue Anforderungen für bestimmte Domänen oder Datensatztypen oder Antwortcodes an die Ursprungsserver anstatt zwischengespeichert gesendet werden.

Die Option Cache umgehen weist die Citrix ADC Appliance an, den Cache für bestimmte Domänen, Datensatztypen oder Antwortcodes zu umgehen, wenn ein Angriff erkannt wird.

Umgehen des Cache für bestimmte Domänen oder Datensatztypen oder Antworttypen über die GUI

1. Navigieren Sie zu **Konfiguration > Sicherheit > DNS-Sicherheit**.
2. Klicken Sie auf der Seite **DNS-Sicherheitsprofile** auf **Hinzufügen**.
3. Erweitern Sie auf der Seite **DNS-Sicherheitsprofil hinzufügen den Cache umgehen** und geben Sie die Domainnamen ein. Wählen Sie optional die Datensatztypen oder die Antworttypen aus, für die der Cache umgangen werden muss.
   - Klicken Sie auf **Domänen**, und geben Sie die Domänennamen ein. Verwenden Sie Kommas, um die Einträge zu trennen.
   - Klicken Sie auf **Record-Typen** und wählen Sie die Record-Typen aus

- Klicken Sie auf **Antworttypen**, und wählen Sie den Antworttyp aus.

4. Klicken Sie auf **Absenden**.

DNS-Transaktionen über TCP erzwingen

Einige DNS-Angriffe können verhindert werden, wenn die Transaktionen TCP anstelle von UDP verwenden müssen. Beispielsweise sendet der Client während eines Bot-Angriffs eine Flut von Abfragen, kann aber keine Antworten verarbeiten. Wenn die Verwendung von TCP für diese Transaktionen erzwungen wird, dann können die Bots die Antworten nicht verstehen und daher keine Anfragen über TCP senden.

Erzwingen Sie den Betrieb von Domänen oder Datensatztypen auf TCP-Ebene über die GUI

1. Navigieren Sie zu **Konfiguration > Sicherheit > DNS-Sicherheit**.
2. Klicken Sie auf der Seite **DNS-Sicherheitsprofile** auf **Hinzufügen**.
3. Erweitern Sie auf der Seite **DNS-Sicherheitsprofil hinzufügen DNS-Transaktionen über TCP erzwingen**, und geben Sie die Domänennamen ein und/oder wählen Sie die Datensatztypen aus, für die die DNS-Transaktionen über TCP erzwungen werden müssen.
   - Klicken Sie auf **Domänen**, und geben Sie die Domänennamen ein. Verwenden Sie Kommas, um die Einträge zu trennen.
   - Klicken Sie auf **Datensatztypen** und wählen Sie die Datensatztypen aus.
4. Klicken Sie auf **Absenden**.

Geben Sie Stammdetails in der DNS-Antwort an

Bei einigen Angriffen sendet der Angreifer eine Flut von Abfragen für nicht verwandte Domänen, die nicht auf der Citrix ADC Appliance konfiguriert oder zwischengespeichert sind. Wenn der `dnsRootReferral` Parameter ENABLED ist, werden alle Root-Server verfügbar.

Die Option Stammdetails in der DNS-Antwort bereitstellen weist die Citrix ADC Appliance an, den Zugriff auf Stammverweise für eine Abfrage zu beschränken, die nicht konfiguriert oder zwischengespeichert ist. Die Appliance sendet eine leere Antwort.

Die Option Stammdetails in der DNS-Antwort bereitstellen kann auch Amplifikationsangriffe mildern oder blockieren. Wenn der DnsRootReferral-Parameter DEAKTIVIERT ist, gibt es keine Root-Verweise in den Citrix ADC-Antworten und werden daher nicht verstärkt.

Aktivieren oder Deaktivieren des Zugriffs auf den Stammserver über die GUI

1. Navigieren Sie zu **Konfiguration > Sicherheit > DNS-Sicherheit**.
2. Klicken Sie auf der Seite **DNS-Sicherheitsprofile** auf **Hinzufügen**.

3. Gehen Sie auf der Seite **DNS-Sicherheitsprofil hinzufügen** folgendermaßen vor:
   a) Erweitern Sie in der **DNS-Antwort** die Option **Stammdetails bereitstellen**.
   b) Klicken Sie auf **ON** oder **OFF**, um den Zugriff auf den Stammserver zu erlauben oder zu beschränken.
4. Klicken Sie auf **Absenden**.

System

October 5, 2021

Dieser Abschnitt enthält Informationen auf Systemebene des Citrix ADC. Dazu gehören eine detaillierte Erläuterung der Features auf Systemebene, die Szenarien, in denen die Features verwendet werden können, die Konfigurationsschritte und Beispiele, die Ihnen helfen, die Features besser zu verstehen.

- Grundlegende Operationen
- Authentifizierung und Autorisierung
- TCP-Konfigurationen
- HTTP-Konfigurationen
- SNMP
- Auditprotokollierung
- Webserver-Protokollierung
- Call Home
- Reporting-Tool
- CloudBridge-Connector
- Hohe Verfügbarkeit
- TCP-Optimierung

Systembasisbetrieb

February 24, 2022

Mit den folgenden Konfigurationen können Sie Systembasisvorgänge auf einer Citrix ADC-Appliance ausführen.

So zeigen Sie die Citrix ADC-Konfiguration an, speichern und löschen

Citrix ADC-Konfigurationen werden in der gespeichert `/nsconfig/ns.conf directory`. Damit Konfigurationen sitzungsübergreifend verfügbar sind, müssen Sie die Konfiguration nach jeder

Konfigurationsänderung speichern.

Anzeigen der laufenden Konfiguration mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show ns runningConfig
```

Zeigen Sie die laufende Konfiguration über die GUI an

1. Navigieren Sie zu **System** > **Diagnose**, und klicken Sie in der Gruppe **Konfiguration anzeigen** auf **Konfiguration ausführen**.

Zeigen Sie den Unterschied zwischen den beiden Konfigurationsdateien über die Befehlszeilenschnittstelle an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
diff ns config <configfile> <configfile2>
```

Zeigen Sie den Unterschied zwischen den beiden Konfigurationsdateien über die GUI an

1. Navigieren Sie zu **System** > **Diagnose**, und klicken Sie in der **Gruppe Konfiguration anzeigen** auf **Konfigurationsdifferenz** .

Speichern von Citrix ADC Konfigurationen mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
save ns config
```

Speichern Sie Citrix ADC-Konfigurationen über die GUI

1. Klicken Sie auf der Registerkarte **Konfiguration** in der oberen rechten Ecke auf das Symbol **Speichern** .

Anzeigen gespeicherter Konfigurationen mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show ns ns.conf
```


Gespeicherte Konfigurationen über die GUI anzeigen

Navigieren Sie zu **System** > **Diagnose** und klicken Sie in der Gruppe **Konfiguration anzeigen** auf **Gespeicherte Konfiguration**.

Löschen der Citrix ADC Konfiguration mit der Befehlszeilenschnittstelle

Sie haben die folgenden drei Möglichkeiten, die Citrix ADC-Konfiguration zu löschen.

Grundstufe. Wenn Sie Ihre Konfiguration auf der Basis-Ebene löschen, werden alle Einstellungen außer den folgenden gelöscht:

- `Nsroot` password
- Zeitzone
- NTP-Server
- ADM-Server verbinden
- Lizenz-Fie-Informationen
- NSIP, MIP (s) und SNIP (s)
- Netzwerkeinstellungen (Standardeinstellungen für Gateway, VLAN, RHI, NTP und DNS-Einstellungen)
- Definitionen von HA-Knoten
- Feature- und Moduseinstellungen
- Standardadministratorkennwort (`nsroot`)

Erweiterte Ebene. Wenn Sie Ihre Konfiguration auf der erweiterten Ebene löschen, werden alle Einstellungen außer den folgenden gelöscht:

- `NSIP, MIP(s), and SNIP(s)`
- `Network settings (Default Gateway, VLAN, RHI, NTP, and DNS settings)`
- `HA node definitions`

Feature- und Moduseinstellungen werden auf ihre Standardwerte zurückgesetzt.

Volles Level. Wenn Sie Ihre Konfiguration auf der vollen Ebene löschen, werden alle Einstellungen auf die werkseitigen Standardwerte zurückgesetzt. Das NSIP und das Standard-Gateway werden jedoch nicht geändert, da eine Änderung dazu führen kann, dass die Appliance die Netzwerkkonnektivität verliert.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
clear ns config -force
```

Beispiel: Um die Grundkonfigurationen auf einer Appliance zwangsweise zu löschen.

```
clear ns config -force basic
```


Löschen Sie die Citrix ADC-Konfiguration über die GUI

Navigieren Sie zu **System** > **Diagnose**, klicken Sie in der Gruppe Wartung auf **Konfiguration löschen, und wählen Sie die Konfigurationsebene** aus, die von der Appliance gelöscht werden soll.

So starten oder fahren Sie die Appliance für nicht gespeicherte Citrix ADC-Konfigurationen neu

Die Citrix ADC-Appliance kann von den verfügbaren Benutzeroberflächen aus der Ferne neu gestartet oder heruntergefahren werden. Wenn Sie eine eigenständige Citrix ADC-Appliance neu starten oder herunterfahren, gehen die nicht gespeicherten Konfigurationen (Konfigurationen, die seit der letzten Ausgabe des Befehls
save ns config ausgeführt wurden) verloren.

In einem Hochverfügbarkeitssetup, wenn die primäre Appliance neu gestartet oder heruntergefahren wird, übernimmt die sekundäre Appliance die Kontrolle und wird zur primären Appliance. Die ungespeicherten Konfigurationen aus dem alten Primärgerät sind auf dem neuen primären Gerät verfügbar.

Sie können die Appliance auch neu starten, indem Sie nur die Citrix ADC-Software neu starten und das zugrunde liegende Betriebssystem nicht neu starten. Dies wird als warmer Neustart bezeichnet. Wenn Sie beispielsweise eine neue Lizenz hinzufügen oder die IP-Adresse ändern, können Sie die Citrix ADC-Appliance neu starten, damit diese Änderungen vorgenommen werden.

> **Hinweis:**
>
> Sie können einen Warm-Neustart nur auf einer eigenständigen Citrix ADC-Appliance durchführen.

Starten Sie die Appliance über die Befehlszeile neu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
reboot [-warm]
```

Starten Sie eine Citrix ADC-Appliance über die GUI neu

1. Klicken Sie auf der Konfigurationsseite auf **Reboot**.
2. Wenn Sie zum Neustart aufgefordert werden, wählen Sie **Konfiguration speichern** aus, um sicherzustellen, dass Sie keine Konfigurationen verlieren.

> **Hinweis:**
>
> Sie können einen warmen Neustart durchführen, indem Sie Warm reboot wählen.

Fahren Sie eine Appliance mit der Befehlszeilenschnittstelle herunter

Geben Sie an der Shell-Eingabeaufforderung Folgendes ein:

- `shutdown -p now`: Schaltet die Software herunter und schaltet den Citrix ADC aus. Um Citrix ADC MPX neu zu starten, drücken Sie den Wechselstromschalter. Um Citrix ADC VPX neu zu starten, starten Sie die VPX-Instanz neu.
- `shutdown -h now`: Schaltet die Software herunter und lässt den Citrix ADC eingeschaltet. Drücken Sie eine beliebige Taste, um Citrix ADC neu zu starten. Dieser Befehl schaltet den Citrix ADC nicht aus. Schalten Sie daher die Wechselstromversorgung nicht aus oder entfernen Sie die Wechselstromkabel.

> **Hinweis:**
>
> Sie können eine Appliance nicht über die Citrix ADC GUI herunterfahren.

So synchronisieren Sie die Systemuhr mit Servern im Netzwerk

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

Sie können die Uhrsynchronisierung auf Ihrer Appliance konfigurieren, indem Sie NTP-Servereinträge entweder über die GUI oder die Befehlszeilenschnittstelle zur Datei ntp.conf hinzufügen oder die Datei ntp.conf manuell ändern und dann den NTP-Daemon (NTPD) starten. Die Konfiguration der Uhrsynchronisierung ändert sich nicht, wenn die Appliance neu gestartet, aktualisiert oder heruntergestuft wird. Die Konfiguration wird jedoch in einem Hochverfügbarkeitssetup nicht an den sekundären Citrix ADC weitergegeben.

Mit der Citrix ADC GUI können Sie die Zeitzone und die IP-Adresse des NTP-Servers konfigurieren, die für die Uhrsynchronisierung auf dem Bildschirm für den Erstbenutzer (FTU) erforderlich sind.

> **Hinweis:**
>
> Wenn Sie keinen lokalen NTP-Server haben, finden Sie eine Liste öffentlicher Open-Access-NTP-Server auf der offiziellen NTP-Site unter Public Time Server List. <http://www.ntp.org> Bevor Sie Ihren Citrix ADC für die Verwendung eines öffentlichen NTP-Servers konfigurieren, lesen Sie unbedingt die Seite “Einsatzregeln” (Link auf allen Seiten von Public Time Server enthalten).
>
> In Citrix ADC Version 11 wurde die NTP-Version von 4.2.6p3 auf 4.2.8p2 aktualisiert.

Voraussetzung

Um die Uhrsynchronisierung zu konfigurieren, müssen Sie die folgenden Entitäten konfigurieren:

1. NTP-Server
2. NTP-Synchronisierung.

Fügen Sie einen NTP-Server mit der Befehlszeilenschnittstelle hinzu

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

- `add ntp server (<serverIP> | <serverName>)[-minpoll <positive_integer>] [-maxpoll <positive_integer>]`
- `show ntp server`

Beispiel:

```
add ntp server 10.102.29.30 -minpoll 6 -maxpoll 11
```

Hinzufügen eines NTP-Servers über die GUI

Navigieren Sie zu **System** > **NTP-Server**, und erstellen Sie den NTP-Server.

Aktivieren der NTP-Synchronisierung mit der Befehlszeilenschnittstelle

Wenn Sie die NTP-Synchronisierung aktivieren, startet Citrix ADC den NTP-Daemon und verwendet die NTP-Servereinträge in der Datei ntp.conf, um seine Ortszeit zu synchronisieren. Wenn Sie die Appliance-Zeit nicht mit den anderen Servern im Netzwerk synchronisieren möchten, können Sie die NTP-Synchronisierung deaktivieren, wodurch der NTP-Daemon (NTPD) gestoppt wird.

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

```
enable ntp sync
```

Aktivieren Sie die NTP-Synchronisierung über die GUI

Navigieren Sie zu **System** > **NTP-Server**, klicken Sie auf **Aktion** und wählen Sie **NTP-Synchronisierung**aus.

Konfigurieren Sie die Uhrsynchronisierung, um eine ntp.conf-Datei über die GUI zu bearbeiten

1. Melden Sie sich an der Befehlszeilenoberfläche an.
2. Wechselt zur Shell-Eingabeaufforderung
3. Kopieren Sie die `/etc/ntp.conf` Datei nach `/nsconfig/ntp.conf`, es sei denn, die enthält `/nsconfig directory` bereits eine `ntp.conf` Datei.
4. Für jeden NTP-Server, den Sie hinzufügen möchten, müssen Sie der`/nsconfig/ntp.conf` Datei die folgenden zwei Zeilen hinzufügen:


```
server <IP address for NTP server> iburst

restrict <IP address for NTP server> mask <netmask> nomodify notrap nopeer
noquery
```

```
> Note:
>
> For security reasons, there should be a corresponding restrict entry
   for each server entry.

Example

In the following example, an administrator has inserted # characters to
     “comment out” an existing NTP entry, and then added an entry:

`#server 1.2.3.4 iburst`

`#restrict 1.2.3.4 mask 55.255.255.255 nomodify notrap nopeer noquery`

`server 10.102.29.160 iburst`

`restrict 10.102.29.160 mask 255.255.255.255 nomodify notrap nopeer
   noquery`
```

1. Wenn das /nsconfig Verzeichnis keine Datei mit dem Namen enthält rc.netscaler, erstellen Sie die Datei.
2. Fügen Sie den folgenden Eintrag hinzu /nsconfig/rc.netscaler: /bin/sh /etc/ntpd_ctl full_start

   Dieser Eintrag startet den ntpd Dienst, prüft die Datei ntp.conf und protokolliert Meldungen im Verzeichnis /var/log.

   Dieser Prozess wird jedes Mal ausgeführt, wenn der Citrix ADC neu gestartet wird.
3. Starten Sie die Citrix ADC-Appliance neu, um die Uhrsynchronisierung zu aktivieren. Oder geben Sie an der Shell-Eingabeaufforderung die folgenden Befehle ein, um die Uhrzeitsynchronisierung zu starten, ohne die Appliance neu zu starten:

- rm /etc/ntp.conf
- ln -s /nsconfig/ntp.conf /etc/ntp.conf
- /bin/sh /etc/ntpd_ctl full_start

So konfigurieren Sie das Sitzungstimeout für Clientverbindungen im Leerlauf

Ein Sitzungstimeout-Intervall wird bereitgestellt, um die Zeitdauer einzuschränken, für die eine Sitzung (GUI, CLI oder API) aktiv bleibt, wenn sie nicht verwendet wird. Für den Citrix ADC kann das Systemsitzungs-Timeout auf den folgenden Ebenen konfiguriert werden:

- **Timeout auf Benutzerebene.** Gilt für den jeweiligen Benutzer.

Interface-Typ	Time-out-Konfiguration
Grafische Benutzeroberfläche (GUI)	Navigieren Sie zu **System > Benutzerverwaltung > Benutzer**, wählen Sie einen Benutzer aus und bearbeiten Sie die Timeout-Einstellung des Benutzers.
CLI	Geben Sie an der Eingabeaufforderung den folgenden Befehl ein: `set system user <name> -timeout <secs>`

- **Timeout auf Benutzergruppenebene.** Gilt für alle Benutzer in der Gruppe.

Interface-Typ	Time-out-Konfiguration
Grafische Benutzeroberfläche (GUI)	Navigieren Sie zu **System > Benutzerverwaltung > Gruppen**, wählen Sie eine Gruppe aus und bearbeiten Sie die Timeout-Einstellung der Gruppe.
CLI	Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:`set system group <groupName> -timeout <secs>`

- **Globales System-Timeout.** Gilt für alle Benutzer und Benutzer aus Gruppen, für die kein Time-out konfiguriert ist.

Interface-Typ	Time-out-Konfiguration
Grafische Benutzeroberfläche (GUI)	Navigieren Sie zu **System > Einstellungen**, klicken Sie auf Globale Systemeinstellungen ändern und aktualisieren Sie den Timeout-Wert nach Bedarf.

Interface-Typ	Time-out-Konfiguration
CLI	Geben Sie an der Eingabeaufforderung den folgenden Befehl ein: `set system parameter -timeout <secs>`

```
The timeout value specified for a user has the highest priority. If timeout is not configured for the user, the timeout configured for a member group is considered. If timeout is not specified for a group (or the user does not belong to a group), the globally configured timeout value is considered. If timeout is not configured at any level, the default value of 900 seconds is set as the system session timeout.

Additionally, you can specify timeout durations for each of the interfaces you are accessing. However, the timeout value specified for a specific interface is restricted to the timeout value configured for the user that is accessing the interface. For example, let us consider an user "publicadmin" who has a timeout value of 20 minutes. Now, when accessing an interface, the user must specify a timeout value that is within 20 minutes.

> **Note:**
>
> You can choose to keep a check on the minimum and maximum timeout values by specifying the timeout as restricted (in CLI by specifying the *restrictedTimeout* parameter). This parameter is provided to account for previous Citrix ADC versions where the timeout value was not restricted.
```

- Wenn diese Option aktiviert ist, beträgt der minimale konfigurierbare Zeitüberschreitungswert 5 Minuten (300 Sekunden) und der maximale Wert 1 Tag (86400 Sekunden). Wenn der Timeout-Wert bereits auf einen Wert von mehr als 1 Tag konfiguriert ist und dieser Parameter aktiviert ist, werden Sie aufgefordert, ihn zu ändern. Wenn Sie den Wert nicht ändern, wird der Timeout-Wert beim nächsten Neustart automatisch auf die Standard-Timeout-Dauer von 15 Minuten (900 Sekunden) neu konfiguriert. Das Gleiche passiert, wenn der konfigurierte Timeout-Wert weniger als 5 Minuten beträgt.
- Wenn diese Option deaktiviert ist, werden die konfigurierten Timeout-Dauern berücksichtigt.
- **Timeout-Dauer an jeder Schnittstelle:**

Interface-Typ	Time-out-Konfiguration
CLI	Geben Sie den Timeout-Wert an der Eingabeaufforderung mithilfe des folgenden Befehls an: `set cli mode -timeout <secs>`
API	Geben Sie den Timeout-Wert in der Login-Nutzlast an.

So stellen Sie Systemdatum und -uhrzeit ein, um die Uhr mit einem Zeitserver zu synchronisieren

Um das Systemdatum und die Uhrzeit zu ändern, müssen Sie die Shell-Schnittstelle zum zugrunde liegenden FreeBSD-Betriebssystem verwenden. Um jedoch Datum und Uhrzeit des Systems anzuzeigen, können Sie die Befehlszeilenschnittstelle oder die GUI verwenden.

Zeigen Sie Systemdatum und -zeit über die Befehlszeile an

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show ns config
```

Anzeigen von Systemdatum und -uhrzeit über die GUI

Navigieren Sie zu **System** und wählen Sie die Registerkarte **Systeminformationen** aus, um das Systemdatum anzuzeigen.

So konfigurieren Sie HTTP- und HTTPS-Management-Ports für interne Dienste

In einer Bereitstellung im Single-IP-Modus einer Citrix ADC-Appliance wird eine einzelne IP-Adresse als NSIP-, SNIP- und VIP-Adressen verwendet. Diese einzelne IP-Adresse verwendet unterschiedliche Portnummern, um als NSIP-, SNIP- und VIP-Adressen zu fungieren.

Die Portnummern 80 und 443 sind bekannte Ports für HTTP- und HTTPS-Dienste. Früher waren Port 80 und 443 der Citrix ADC IP-Adresse (NSIP) dedizierte Ports für interne HTTP- und HTTPS-Verwaltungsdienste. Da diese Ports für interne Dienste reserviert waren, können Sie diese bekannten Ports nicht für die Bereitstellung von HTTP- und HTTPS-Datendiensten von einer VIP-Adresse aus verwenden, die dieselbe Adresse wie die NSIP-Adresse in einer Bereitstellung im Einzel-IP-Modus hat.

Um diese Anforderung zu erfüllen, können Sie jetzt Ports für interne HTTP- und HTTPS-Verwaltungsdienste (der NSIP-Adresse) außer Port 80 und 443 konfigurieren.

Im Folgenden sind die Standardportnummern für interne HTTP- und HTTPS-Verwaltungsdienste in Citrix ADC MPX-, VPX- und CPX-Appliances aufgeführt:

- Citrix ADC MPX- und VPX-Appliances: 80 (HTTP) und 443 (HTTPS)
- Citrix ADC CPX-Appliances: 9080 (HTTP) und 9443 (HTTPS)

Konfigurieren von HTTP- und HTTPS-Verwaltungs-Ports mithilfe der Befehlsschnittstelle

Sie können einen HTTP- und einen HTTPS-Port auf einen beliebigen Wert auf der Citrix ADC-Appliance konfigurieren, um den HTTP- und HTTPS-Verwaltungsdienst zu unterstützen. Standardmäßig verwendet die Citrix ADC-Appliance jedoch 80 und 443 Ports für die HTTP- und HTTPS-Verbindung.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns param -mgmtHttpPort<port>
```

Beispiel:

```
set ns param –mgmtHttpPort 2000
```

So konfigurieren Sie einen HTTPS-Port mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns param -mgmtHttpsPort<port>
```

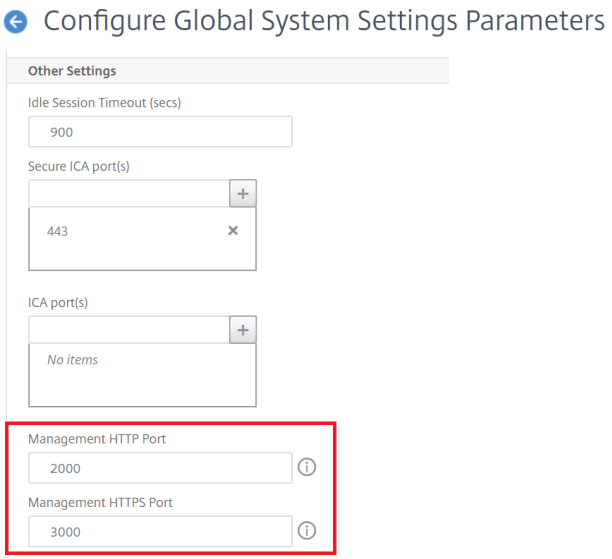
Beispiel:

```
set ns param –mgmtHttpsPort 3000
```

Konfigurieren von HTTP- und HTTPS-Management-Ports über die GUI

Befolgen Sie die unten angegebenen Schritte, um HTTP- und HTTPS-Portwerte zu konfigurieren:

1. Navigieren Sie zu **System** > **Einstellungen** > **Globale Systemeinstellungen ändern**.
2. Legen Sie auf der Seite **Globale Systemeinstellungen konfigurieren** im Abschnitt **Andere** Einstellungen die folgenden Parameter fest.
    a) Management-HTTP-Port. Setzen Sie den Portwert auf 2000. Standardwert = 80, Min = 1, Max = 65534.
    b) Verwaltung HTTPS-Port. Setzen Sie den Portwert auf 3000. Standardwert = 443, Min = 1, Max = 65534.



So weisen Sie zusätzliche Management-CPU für die Datenverarbeitung und -überwachung zu

Wenn Sie eine bessere Leistung für die Konfiguration und Überwachung einer Citrix ADC MPX-Appliance benötigen, können Sie eine zusätzliche Verwaltungs-CPU aus dem Paket-Engine-Pool der Appliance zuweisen. Diese Funktion wird bei bestimmten Citrix ADC MPX-Modellen und allen VPX-Modellen mit Ausnahme der VPX-Instanzen unterstützt, die auf Citrix ADC SDX-Appliances ausgeführt werden. Dies wirkt sich auf die Ausgabe der CPU- und Stat-Systembefehle des Statistiksystems aus.

Unterstützte Citrix ADC MPX-Modelle:

- 25xxx
- 22xxx
- 14xxx
- 115xx
- 15xxx
- 26xxx

> **Hinweis:**
>
> Für Citrix ADC MPX 26xxx Modelle mit mehr als 20 Kernen ist die obligatorische zusätzliche Management-CPU-Funktion standardmäßig aktiviert. Für Citrix ADC VPX-Modelle ist eine Lizenz erforderlich, die mindestens 12 vCPUs unterstützt, um diese Funktion zu aktivieren.

Weisen Sie eine zusätzliche Verwaltungs-CPU mit der Befehlszeilenschnittstelle zu

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- `enable extramgmtcpu`

- `disable extramgmtcpu`

> **Hinweis:**
>
> Nachdem Sie diese Funktion aktiviert und deaktiviert haben, zeigt die Citrix ADC-Appliance eine Warnung an, um die Appliance neu zu starten, damit die Änderungen wirksam werden.

Um den konfigurierten und effektiven Status einer zusätzlichen Management-CPU anzuzeigen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 `show extramgmtcpu`
```

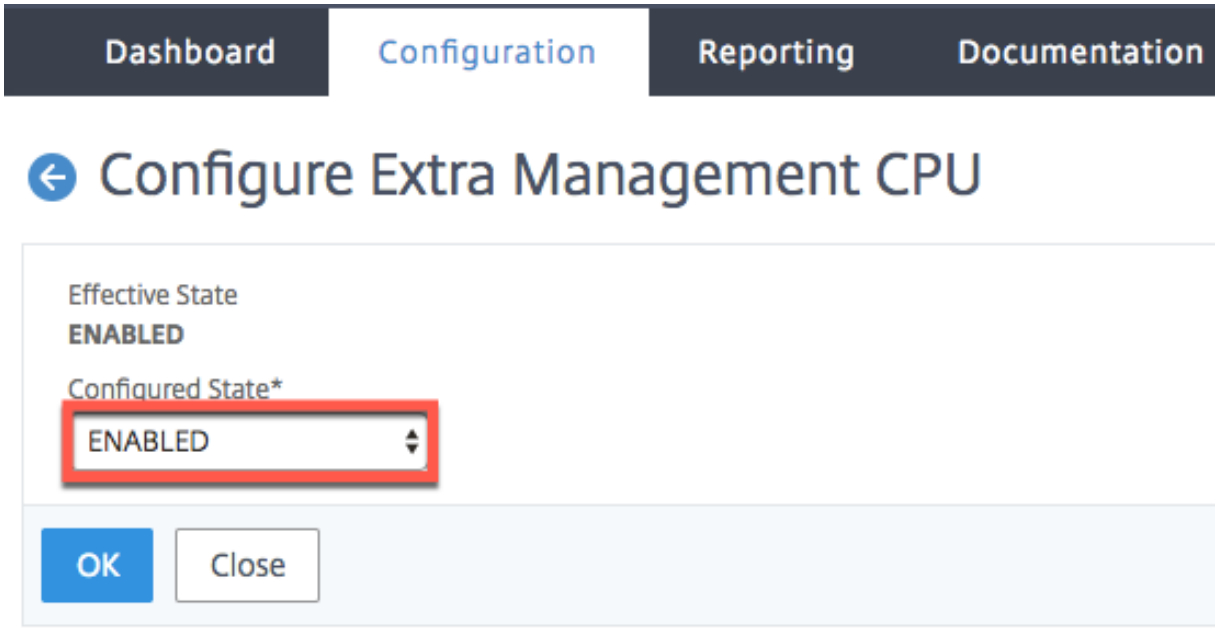
Beispiel:

```
> show extramgmtcpu ConfiguredState: ENABLED EffectiveState: ENABLED
```

> **Hinweis:**
>
> In diesem Beispiel wird der Befehl show vor dem Neustart der Appliance eingegeben.

Weisen Sie über die GUI eine zusätzliche Management-CPU zu

Um über die GUI eine zusätzliche Management-CPU zuzuweisen, navigieren Sie zu **System** > **Einstellungen** und klicken Sie auf **Zusätzliche Management-CPU konfigurieren**. Wählen Sie im Dropdown-Menü **Konfigurierter Status** die Option **Aktiviert** aus und wählen Sie dann **OK**aus.



Um die CPU-Auslastung zu überprüfen, gehen Sie zu **System** > **Einstellungen** > **Dashboard**.

Konfigurieren Sie eine zusätzliche Management-CPU mithilfe der NITRO-API

Verwenden Sie die folgenden NITRO-Methoden und -Formate, um eine zusätzliche Verwaltungs-CPU zu aktivieren, zu deaktivieren und anzuzeigen.

So aktivieren Sie eine zusätzliche Management-CPU:

```
HTTP Method: POST
```

```
URL: http://<NSIP>/nitro/v1/config/systemextramgmtcpu?action=enable
```

```
Payload: { "systemextramgmtcpu":{ } }
```

```
curl -v -X POST -H "Content-Type: application/json"-u nsroot:nsroot http://10.102.201.92/nitro/v1/config/systemextramgmtcpu?action=enable -d '{ "systemextramgmtcpu":{ } } '
```

Deaktivieren einer zusätzlichen Management-CPU

```
HTTP Method: POST
```

```
URL: http://<NSIP>/nitro/v1/config/systemextramgmtcpu?action=disable
```

```
Payload: { "systemextramgmtcpu":{ } }
```

```
curl -v -X POST -H "Content-Type: application/json"-u nsroot:nsroot http://10.102.201.92/nitro/v1/config/systemextramgmtcpu?action=disable -d '{ "systemextramgmtcpu":{ } } '
```

So zeigen Sie eine zusätzliche Verwaltungs-CPU an

```
HTTP Method: GET
```

```
URL: http://<NSIP>/nitro/v1/config/systemextramgmtcpu
```

Beispiel:

```
curl -v -X GET -H "Content-Type: application/json"-u nsroot:nsroot http://10.102.201.92/nitro/v1/config/systemextramgmtcpu
```

Statistik und Überwachung vor und nach dem Hinzufügen zusätzlicher Management-CPU

Die folgenden Beispiele zeigen die Unterschiede in der Ausgabe der CPU- und Stat-Systembefehle des Statistiksystems vor und nach dem Hinzufügen einer zusätzlichen Management-CPU.

```
stat system cpu
```

Dieser Befehl zeigt Statistiken von CPUs an.

Hier ist eine Beispielausgabe, bevor eine zusätzliche Management-CPU für eines der unterstützten Modelle hinzugefügt wird.

Beispiel

```
```
> stat system cpu

CPU statistics

ID   Usage

8   1

7   1

11   2

1   1

6   1

9   1

3   1

5   1

4   1

10   1

2   1
<!--NeedCopy--> ```
```

Hier ist die Ausgabe nach dem Hinzufügen einer zusätzlichen Verwaltungs-CPU auf derselben MPX-Appliance.

```
```
> stat system cpu

CPU statistics

ID         Usage

```



```
9               1

7               1

5               1

8               1

11              2

10              1

6               1

4               1

3               1

2               1
<!--NeedCopy--> ```
```

`stat system`

Dieser Befehl zeigt die CPU-Nutzung an. Im folgenden Beispiel lautet die Ausgabe vor dem Hinzufügen einer zusätzlichen Verwaltungs-CPU für eines der unterstützten Modelle:

Mgmt zusätzliche CPU-Auslastung (%) 0.00

Beispiel

```
```
> stat system

Citrix ADC Executive View

System Information:

Up since   Wed Oct 11 11:17:54 2017

/flash Used (%)   0

Packet CPU usage (%)   1.30

Management CPU usage (%)   4.00

```

 
```

```
Mgmt CPU0 usage (%)                  4.00

Mgmt Additional-CPU  usage (%)       0.00

Memory usage (MB)                    2167

InUse Memory (%)                     5.76

/var Used (%)                           0
<!--NeedCopy--> ```
```

Im folgenden Beispiel lautet die Ausgabe nach dem Hinzufügen einer zusätzlichen Verwaltungs-CPU auf derselben MPX-Appliance:

Mgmt zusätzliche CPU-Auslastung (%) 0.80

```
```     > stat system

Citrix ADC Executive View

System Information:

Up since   Wed Oct 11 11:55:56 2017

/flash Used (%)   0

Packet CPU usage (%)   1.20

Management CPU usage (%)   5.70

Mgmt CPU0 usage (%)   10.60

Mgmt Additional-CPU usage (%)   0.80

Memory usage (MB)   1970

InUse Memory (%)   5.75

/var Used (%)   0

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

 
```

Backup und Wiederherstellen der Appliance, um verlorene Konfigurationen wiederherzustellen

Wenn Ihre Appliance beschädigt wird oder ein Upgrade benötigt, können Sie Ihre Systemkonfiguration sichern. Der Backupvorgang erfolgt entweder über die Citrix CLI- oder GUI-Schnittstelle. Mit der Appliance können Sie auch die Backupdatei von einer externen Quelle importieren. Sie können dies jedoch nur über die GUI-Schnittstelle tun und es gibt keine Unterstützung über die CLI-Schnittstelle.

Wichtige Punkte

Sie müssen sich an die folgenden Punkte erinnern, wenn Sie Ihre Appliance Backup und wiederherstellen.

- Es muss eine Unterstützung für die Netzwerkkonfiguration auf einer neuen Plattform geben.
- Der neue Plattform-Build muss mit der Backupdatei oder einer späteren Version identisch sein.

Sichern einer Citrix ADC-Appliance

Abhängig von den Daten- und Sicherungsanforderungen können Sie ein “einfaches” Backup oder ein “vollständiges” Backup erstellen.

- **Grundlegende Backup.** Sie können diese Art der Backup durchführen, wenn Sie Dateien sichern möchten, die sich ständig ändern. Die Dateien, die Sie sichern können, finden Sie in der folgenden Tabelle.

Informationen zu den grundlegenden Backup-Details finden Sie im Thema Tabelle .

- **Vollständiges Backup.** Zusätzlich zu den Dateien, die durch eine Basissicherung gesichert werden, enthält eine vollständige Backup seltener aktualisierte Dateien. Die Dateien, die gesichert werden, wenn Sie die “vollständige” Backupoption verwenden, sind:

Verzeichnis	Unterverzeichnis oder Dateien
nsconfig	ssl*, license*, fips*
/var/	netscaler/ssl/*, wi/java_home/jre/lib/security/cacerts/*, wi/java_home/lib/security/cacerts/*

Die Backupdaten werden als komprimierte TAR-Datei im `/var/ns_sys_backup/` Verzeichnis gespeichert. Um Probleme aufgrund der Nichtverfügbarkeit von Speicherplatz zu vermeiden, können Sie bis zu 50 Backupdateien in diesem Verzeichnis speichern. Mit dem `rm system backup` Befehl können Sie vorhandene Backupdateien löschen und weitere Backups erstellen.

> **Hinweis:**
>
> Führen Sie bei laufendem Backupvorgang keine Befehle aus, die sich auf die Konfiguration auswirken.
>
> Wenn eine Datei, die gesichert werden muss, nicht verfügbar ist, überspringt der Vorgang diese Datei.

Sichern einer Citrix ADC-Appliance über die Befehlszeilenschnittstelle

Befolgen Sie die nachstehenden Schritte, um eine Citrix ADC-Appliance mithilfe der Citrix ADC-Befehlszeilenschnittstelle zu sichern.

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Speichern Sie die Citrix ADC-Konfigurationen.

```
save ns config
```

1. Erstellen Sie die Backupdatei.

```
create system backup [<fileName>] -level <basic ¦ full> -comment <string>
```

> **Hinweis:**
>
> Wenn der Dateiname nicht angegeben wird, erstellt die Appliance eine TAR-Datei mit der folgenden Namenskonvention:`backup_<level>_<nsip_address>_<date-timestamp>.tgz`.

Beispiel: Sichern der vollständigen Appliance mithilfe der Standardbenennungskonvention für die Backupdatei.

```
> create system backup -level full
```

1. Stellen Sie sicher, dass die Backupdatei erstellt wurde.

```
show system backup
```

Mithilfe des `fileName` Parameters können Sie die Eigenschaften einer bestimmten Backupdatei anzeigen.

Wiederherstellen einer Citrix ADC-Appliance mit der Befehlszeilenschnittstelle

> **Wichtig:**
>
> Sie können Ihre Appliance nicht erfolgreich wiederherstellen, wenn Sie Ihre Backupdatei umbenennen oder ändern.

Wenn Sie Ihre Appliance wiederherstellen, entfernt der Wiederherstellungsvorgang die Backupdatei aus dem `/var/ns_sys_backup/` Verzeichnis. Sobald die Dateien entkomprimiert sind, werden die Dateien in die jeweiligen Verzeichnisse kopiert.

Stellen Sie den Citrix ADC aus einer lokalen Backupdatei über die Befehlszeile wieder her

> **Hinweis:**
>
> Citrix empfiehlt Ihnen, die aktuelle Konfiguration zu sichern, bevor Sie eine vorherige Konfiguration wiederherstellen. Wenn Sie jedoch nicht möchten, dass der Wiederherstellungsbefehl automatisch ein Backup der aktuellen Konfiguration erstellt, verwenden Sie den `-skipBackup` Parameter.

Führen Sie an der Eingabeaufforderung Folgendes aus:

1. Rufen Sie eine Liste der auf der Appliance verfügbaren Backupdateien ab.

   ```
   show system backup
   ```

2. Stellen Sie die Appliance wieder her, indem Sie eine der Backupdateien angeben.

   ```
   restore system backup <filename> [-skipBackup]
   ```

   Beispiel: Wiederherstellen mit einem vollständigen Backup einer Appliance

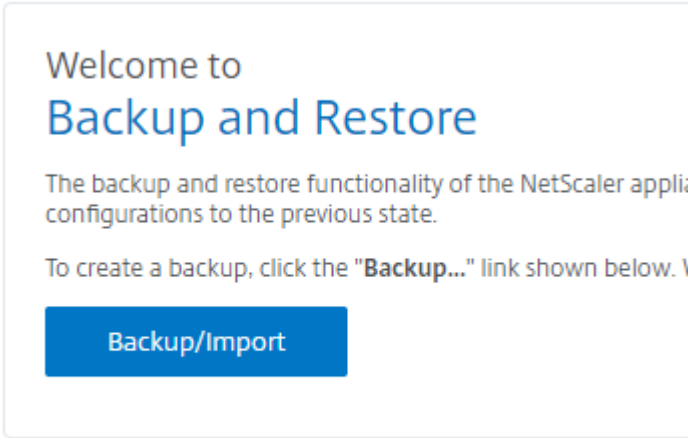
   ```
   > restore system backup backup_full_<nsip_address>_<date-timestamp>.tgz
   ```

3. Starten Sie die Appliance neu.

   ```
   reboot
   ```

Backup und Wiederherstellen einer Citrix ADC-Appliance über die GUI

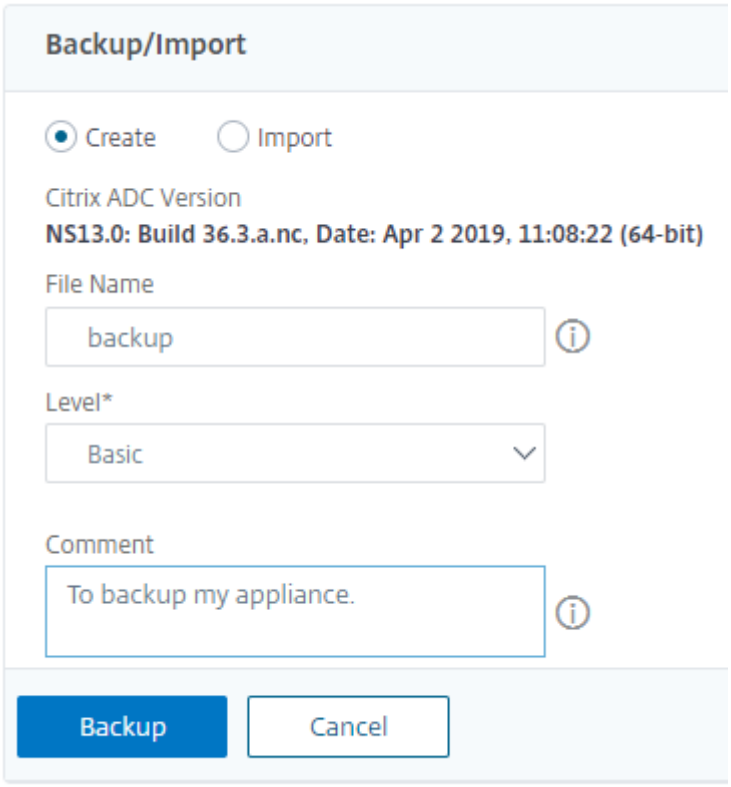
1. Navigieren Sie zu **System** > **Backup und Wiederherstellen**.



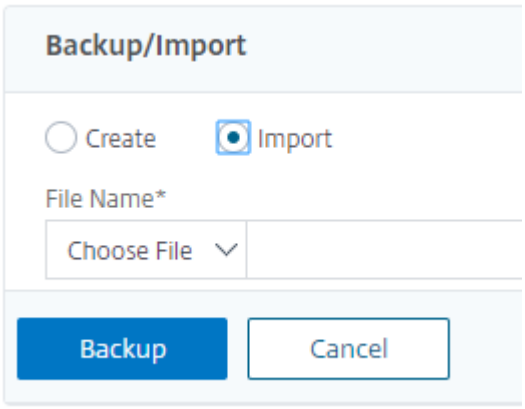
2. Klicken Sie auf **Backup/Import**, um den Vorgang zu starten.
3. Wählen Sie auf der Seite **Backup/Import** die Option **Erstellen** aus und legen Sie die folgenden Parameter fest.

a) Dateiname. Name der Appliance-Backup-Datei.
b) Niveau. Wählen Sie ein Backup-Level als Basic oder Full.
c) Kommentar. Geben Sie eine kurze Beschreibung für das Backup an.

4. Klicken Sie auf **Backup**.

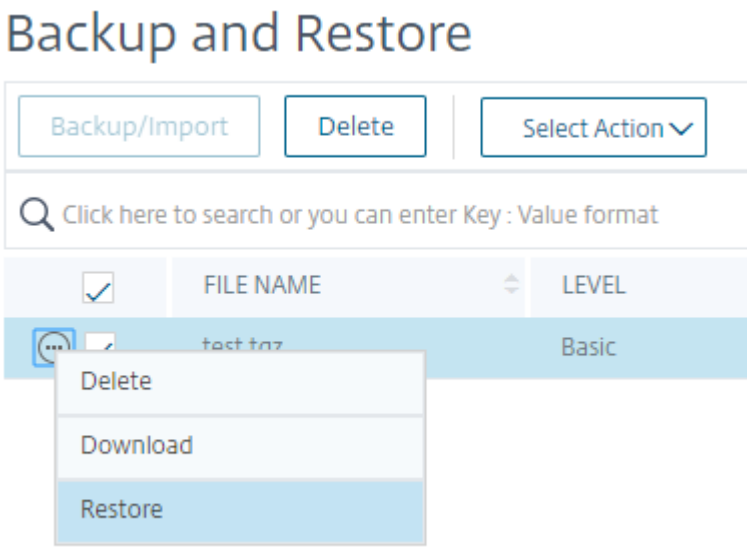


5. Wenn Sie ein Backup importieren möchten, müssen Sie **Importieren** auswählen.

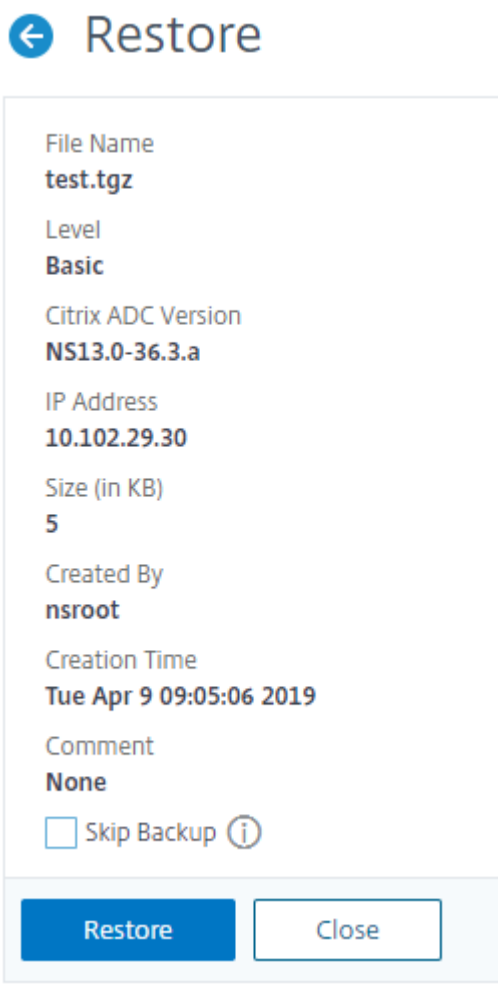


6. Sobald die Backup abgeschlossen ist, können Sie die Datei auswählen und auf **Herunterladen** klicken.

7. Zum Wiederherstellen wählen Sie die Backupdatei aus und klicken Sie auf **Wiederherstellen**.



8. Überprüfen Sie auf der Seite **Wiederherstellen** die Details der Backupdatei und klicken Sie auf **Wiederherstellen**.



9. Nach dem Wiederherstellen müssen Sie die Appliance neu starten.

Weitere Informationen zum Backup und Wiederherstellen von Citrix ADC-Instanzen finden Sie unter Backup und Wiederherstellen mit Citrix ADM.

Weitere Informationen zum Backup und Wiederherstellen einer SDX-Appliance finden Sie unter Sichern und Wiederherstellen der SDX-Appliance

Informationen zu Vorgängen, die bei dem Systembackup ausgeführt werden, finden Sie unter Systembackup.

So erstellen Sie ein Paket für den technischen Support zur Lösung von Appliance-Problemen

Wenn Sie Hilfe bei der Analyse und Behebung von Problemen mit einer Citrix ADC-Appliance benötigen, können Sie ein technisches Support-Paket auf der Appliance generieren und das Paket an den technischen Support von Citrix senden. Das Paket für den technischen Support von Citrix ADC ist

ein gezipptes TAR-Archiv mit Systemkonfigurationsdaten und -statistiken. Es sammelt die folgenden Daten von der Citrix ADC-Appliance, auf der Sie das Bundle generieren:

- **Konfigurationsdateien**. Alle Dateien im Verzeichnis /flash/nsconfig.
- **Newslog-Dateien**. Der aktuell laufende newnslog und einige vorherige Dateien. Um die Größe der Archivdatei zu minimieren, ist die `newnslog` Sammlung auf 500 MB, 6 Dateien oder 7 Tage beschränkt, je nachdem, was zuerst eintritt. Wenn ältere Daten benötigt werden, ist möglicherweise eine manuelle Erfassung erforderlich.
- **Protokolldateien**. Dateien in /var/log/messages *, /var/log/ns.log* und anderen Dateien unter /var/log und /var/nslog.
- **Anwendungs-Kerndateien**. Dateien, die in der letzten Woche im Verzeichnis /var/core erstellt wurden, falls vorhanden.
- **Ausgabe einiger CLI-Show-Befehle**.
- **Ausgabe einiger CLI-Statbefehle**.
- **Ausgabe von BSD-Shell-Befehlen**.

Sie können einen einzigen Befehl verwenden, um das technische Support-Paket zu generieren und sicher auf den Citrix Technical Support-Server hochzuladen. Zum Hochladen müssen Sie Ihre Citrix Anmeldeinformationen angeben. Wenn Sie das Bundle generieren, können Sie die Fall- oder Serviceanforderungsnummer angeben, die Ihnen vom Citrix Technical Support zugewiesen wurde. Wenn Sie bereits ein Paket für technischen Support generiert haben, können Sie die vorhandene Archivdatei auf den Citrix Technical Support Server hochladen, indem Sie den Dateinamen mit dem vollständigen Pfad angeben.

Das technische Support-Paket wird auf der Citrix ADC-Appliance in einem Archiv an folgendem Speicherort gespeichert:

`/var/tmp/support/support.tgz`

Der Pfad ist ein Symlink zum neuesten Collector für einfachen Zugriff. Der vollständige Dateiname variiert je nach Bereitstellungstopologie, folgt jedoch im Allgemeinen einem ähnlichen Format wie:

`collector_<P/S>_<NS IP>_<DateTime>.tgz.`

Wenn Ihre Citrix ADC-Appliance keine direkte Internetverbindung hat, können Sie einen Proxyserver verwenden, um das technische Supportpaket direkt auf den Citrix Technical Support Server hochzuladen. Das Grundformat der Proxy-Zeichenfolge lautet:

`proxy_IP:<proxy_port>`

Wenn der Proxyserver eine Authentifizierung erfordert, lautet das Format:

`username:password@proxsy_IP:<proxy_port>`

> **Hinweis:**
>
> Für Citrix ADC-Appliances in einem Hochverfügbarkeitspaar müssen Sie das technische Support-

> Paket auf jedem der beiden Knoten generieren.
>
> Für Citrix ADC-Appliances in einem Clustersetup können Sie das technische Support-Paket auf jedem Knoten einzeln generieren oder mithilfe der Cluster-IP-Adresse kleinere abgekürzte Archive für alle Knoten generieren.
>
> Für Citrix ADC-Administratorpartitionen müssen Sie das technische Support-Paket aus der Standard-Admin-Partition generieren. Um das technische Support-Paket für eine bestimmte Partition zu erhalten, müssen Sie den Namen der Partition angeben, für die Sie das technische Support-Paket generieren möchten. Wenn Sie den Namen der Partition nicht angeben, werden Daten aus allen Adminpartitionen gesammelt.

Generieren Sie das Paket für technischen Support von Citrix ADC über die Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
show techsupport [-scope <scope> <partitionName>] [-upload [-proxy <string
>] [-casenumber <string>] [-file <string>] [-description <string>] [-
userName <string> -password ]]
```

Sr. Nein	Aufgabe	Befehl
1	Generieren Sie das technische Support-Paket und laden Sie es auf den Citrix Technical Support Server hoch.	show techsupport –upload –userName account1 –password xxxxxxx
2	Generieren Sie das technische Support-Paket und laden Sie es über einen Proxyserver auf den Citrix Technical Support Server hoch	show techsupport –upload –proxy 1.1.1.1:80 –userName account1 –password xxxxxxx
3	Laden Sie ein vorhandenes Paket für technischen Support auf den Citrix Technical Support Server hoch.	show techsupport –upload -file,/var/tmp/support/collector_P_10.102.29.1 –userName account1 –password xxxxxxx
4	Generieren Sie kleine, abgekürzte Archive für alle Knoten in einem Clustersetup. Führen Sie diesen Befehl mit der Cluster-IP-Adresse aus	show techsupport –scope CLUSTER

Sr. Nein	Aufgabe	Befehl
5	Generieren Sie ein technisches Support-Paket für eine Admin-Partition. Führen Sie diesen Befehl auf der Standard-Admin-Partition aus.	show techsupport –scope PARTITION partition1

So sammeln Sie das technische Support-Paket von SDX- und VPX-Appliances für die Insight-Analyse

Eine Citrix ADC-Appliance verfügt über einen integrierten Mechanismus zum Sammeln von Protokolldateien. Die Protokolldateien werden wiederum zur Analyse an Citrix Insight Services gesendet.

> **Hinweis:**
>
> Alle Verfahren gelten für die Softwareversion 9.2 oder höher.

Laden Sie das technische Support-Paket von Citrix ADC MPX- und VPX-Appliances herunter

Um eine Collector-Datei über die Citrix ADC GUI auszuführen, müssen Sie das folgende Verfahren ausführen:

> **Hinweis:**
>
> Das Verfahren ist für Softwareversion 9.2 oder höher anwendbar.

1. Navigieren Sie zu **System** > **Diagnose**.
2. Klicken Sie im Abschnitt **Tools für den Technischen Support** auf den Link **Support-Datei generieren** .
3. Stellen Sie auf der Seite **Tech Support** die folgenden Parameter ein:
   a) Scope. Um Daten von einem oder mehreren Knoten zu sammeln.
   b) Partition. Name der Partition.
   c) Ladeoptionen für den technischen Support von Citrix. Stellen Sie alle Optionen wie Proxyserver, Servicefallnummer, Collector-Archivdateiname und eine kurze Beschreibung der Archivdatei zum Hochladen des technischen Support-Pakets ein.
   d) Citrix Konto. Geben Sie Ihre Citrix Anmeldeinformationen ein.
4. Klicken Sie auf **Ausführen**.
5. Das technische Support-Paket wird generiert.

6. Klicken Sie auf **Ja**, um das Technical Support Bundle auf Ihren lokalen Desktop herunterzuladen.

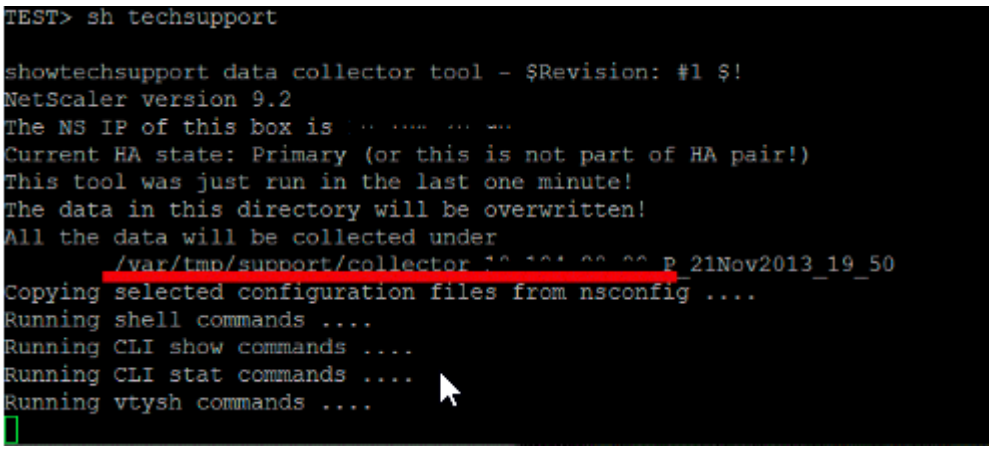
Beziehen Sie das technische Support-Paket über die Befehlszeilenschnittstelle

1. Laden Sie die Datei mit einem Dienstprogramm Secure FTP (SFTP) oder Secure Copy (SCP) von der Appliance herunter, z. B. `WinSCP`, und laden Sie sie zur Analyse in Citrix Insight Services hoch.

> **Hinweis:**
>
> In der Citrix ADC-Softwareversion vor 9.0 muss das Collector-Skript separat heruntergeladen und ausgeführt werden.

```
> show techsupport -scope CLUSTER
```

1. Dadurch werden Informationen zum technischen Support von allen Knoten im Cluster gesammelt und die Dateien in einem einzigen Archiv komprimiert.
2. Nachdem die Appliance das Collector-Archiv generiert hat, wird der Speicherort der Datei angezeigt, wie im folgenden Screenshot gezeigt.



Die Datei wird in gespeichert `/var/tmp/support` und Sie können sie überprüfen, indem Sie sich bei einer Citrix ADC-Appliance anmelden und den folgenden Befehl über eine Shell-Eingabeaufforderung ausführen.

```
root@NS## cd /var/tmp/support/
root@NS## ls -l
```

Beziehen Sie das Diagnose-Paket von Citrix ADC SDX über die GUI

1. Öffnen Sie die Citrix SDX GUI.
2. Erweitern Sie den Knoten **Diagnose** .
3. Wählen Sie den Knoten **Technischer Support** .

4. Klicken Sie auf Technical Support Datei generieren.
5. Wählen Sie im Dropdown-Menü **Appliance** (einschließlich Instanzen) aus.
6. Klicken Sie auf **Hinzufügen**.
7. Wählen Sie eine oder mehrere Instanzen aus, die hinzugefügt werden sollen.
8. Klicken Sie auf **OK**. Warten Sie, bis der Vorgang abgeschlossen ist.
9. Wählen Sie den generierten Bundlenamen aus, und klicken Sie dann auf **Herunterladen**.
10. Laden Sie die Paketdatei in Citrix Insight Serviceshoch.

Weitere Ressourcen

Sehen Sie sich ein Video an

Lies ein anderes Thema

Befehlsreferenzdokument

Authentifizierung und Autorisierung von Systembenutzern

October 5, 2021

Um die Citrix ADC-Benutzerauthentifizierung und -Autorisierung zu konfigurieren, müssen Sie zuerst die Benutzer definieren, die Zugriff auf die Citrix ADC Appliance haben, und dann können Sie diese Benutzer in Gruppen organisieren. Nachdem Sie Benutzer und Gruppen konfiguriert haben, müssen Sie Befehlsrichtlinien zum Definieren von Zugriffstypen konfigurieren und die Richtlinien Benutzern und/oder Gruppen zuweisen.

Sie müssen sich als Administrator anmelden, um Benutzer, Gruppen und Befehlsrichtlinien zu konfigurieren. Der standardmäßige Citrix ADC Administratorbenutzername lautet *nsroot*. Nachdem Sie sich als Standardadministrator angemeldet haben, sollten Sie das Kennwort für das Konto nsroot ändern. Nachdem Sie das Kennwort geändert haben, kann kein Benutzer auf die Citrix ADC Appliance zugreifen, bis Sie ein Konto für diesen Benutzer erstellt haben. Wenn Sie das Administratorkennwort vergessen haben, nachdem Sie es vom Standardwert geändert haben, können Sie es auf nsroot zurücksetzen.

> **Hinweis:**
>
> - Lokale Benutzer können sich beim Citrix ADC authentifizieren, selbst wenn externe Authentifizierungsserver konfiguriert sind. Sie können dies einschränken, indem Sie den Parameter LocalAuth des Befehls set system parameter deaktivieren.
> - Zur Verbesserung der Sicherheit empfiehlt Citrix, das nsroot-Kennwort zu ändern. Häufig ist es ratsam, das Kennwort zu ändern. Informationen zum Ändern des nsroot-Kennworts finden Sie unter Zurücksetzen des Kennworts des Standardadministrators (nsroot) .

Benutzer-, Benutzergruppen- und Befehlsrichtlinien

October 8, 2021

Sie müssen zuerst einen Benutzer mit einem Konto definieren und dann alle Benutzer in Gruppen organisieren. Sie können Befehlsrichtlinien erstellen oder integrierte Befehlsrichtlinien verwenden, um den Benutzerzugriff auf Befehle zu regulieren.

> **Hinweis:**
>
> Wenn Sie mehr über das Konfigurieren von Benutzer- und Benutzergruppen im Rahmen des Citrix ADC-Authentifizierungs- und Autorisierungs-Setups für das Verkehrsmanagement erfahren möchten, lesen Sie das Thema Konfigurieren von Benutzern und Gruppen .

Sie können auch die Eingabeaufforderung für einen Benutzer anpassen. Prompts können in der Konfiguration eines Benutzers, in einer Benutzergruppenkonfiguration und in den globalen Systemkonfigurationseinstellungen definiert werden. Die für einen Benutzer angezeigte Aufforderung befindet sich in der folgenden Rangfolge:

1. Zeigen Sie die Eingabeaufforderung an, wie sie in der Benutzerkonfiguration definiert ist.
2. Zeigen Sie die Eingabeaufforderung an, wie sie in der Gruppenkonfiguration für die Gruppe des Benutzers definiert ist.
3. Zeigen Sie die Eingabeaufforderung an, wie sie in den globalen Systemkonfigurationseinstellungen definiert ist.

Sie können nun einen Timeoutwert für inaktive CLI-Sitzungen für einen Systembenutzer angeben. Wenn die CLI-Sitzung eines Benutzers für einen Zeitraum im Leerlauf ist, der den Zeitüberschreitungswert überschreitet, beendet die Citrix ADC Appliance die Verbindung. Das Timeout kann in einer Benutzerkonfiguration, in einer Benutzergruppenkonfiguration oder in den globalen Systemkonfigurationseinstellungen definiert werden. Der Timeout für inaktive CLI-Sitzungen für einen Benutzer wird in der folgenden Rangfolge festgelegt:

1. Benutzerkonfiguration:
2. Gruppenkonfiguration für die Gruppe des Benutzers.
3. Globale Systemkonfigurationseinstellungen

Ein Citrix ADC Stammadministrator kann die maximale gleichzeitige Sitzungsgrenze für Systembenutzer konfigurieren. Indem Sie das Limit einschränken, können Sie die Anzahl der offenen Verbindungen reduzieren und die Serverleistung verbessern. Solange die CLI-Anzahl innerhalb des konfigurierten Grenzwerts liegt, können sich gleichzeitige Benutzer beliebig oft an der GUI anmelden. Wenn jedoch die Anzahl der CLI-Sitzungen das konfigurierte Limit erreicht, können sich Benutzer nicht mehr an der GUI anmelden. Wenn beispielsweise die Anzahl der gleichzeitigen Sitzungen auf 20 konfiguriert ist, können sich gleichzeitige Benutzer bei 19 CLI-Sitzungen anmelden. Wenn der Benutzer jedoch

bei der 20th CLI-Sitzung angemeldet ist, führt jeder Versuch, sich an der GUI, CLI oder NITRO anzumelden, zu einer Fehlermeldung (ERROR: Verbindungslimit für CFE wurde überschritten).

> **Hinweis:**
>
> Standardmäßig ist die Anzahl der gleichzeitigen Sitzungen auf 20 und die maximale Anzahl gleichzeitiger Sitzungen auf 40 konfiguriert.

Konfigurieren von Benutzerkonten

Um Benutzerkonten zu konfigurieren, geben Sie einfach Benutzernamen und Kennwörter an. Sie können Kennwörter ändern und Benutzerkonten jederzeit entfernen.

> **Hinweis:**
>
> Alle Zeichen in einem Kennwort werden nicht akzeptiert. Es funktioniert jedoch, wenn Sie die Zeichen in Anführungszeichen eingeben.
>
> Außerdem darf die Zeichenfolge eine maximale Länge von 127 Zeichen nicht überschreiten.

So erstellen Sie ein Benutzerkonto mit der Befehlszeilenschnittstelle

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

- `add system user <username> [-externalAuth ( ENABLED | DISABLED )] [-promptString <string>] [-timeout \<secs>] [-logging ( ENABLED | DISABLED )] [-maxsession <positive_integer>]`
- `show system user <userName>`

Externe Benutzer können den Parameter “Protokollierung” konfigurieren, um externe Protokolle mithilfe von Webprotokollierungs- oder Überwachungsprotokollierungsmechanismus zu sammeln. Wenn der Parameter aktiviert ist, authentifiziert sich der Überwachungsclient bei der Citrix ADC Appliance, um Protokolle zu sammeln.

Beispiel:

```
> add system user johnd -promptString user-%u-at-%T
```

```
1 Enter password:
2 Confirm password:
3 > show system user johnd
4 user name: john
5       Timeout:900 Timeout Inherited From: Global
6       External Authentication: ENABLED
7       Logging: DISABLED
```

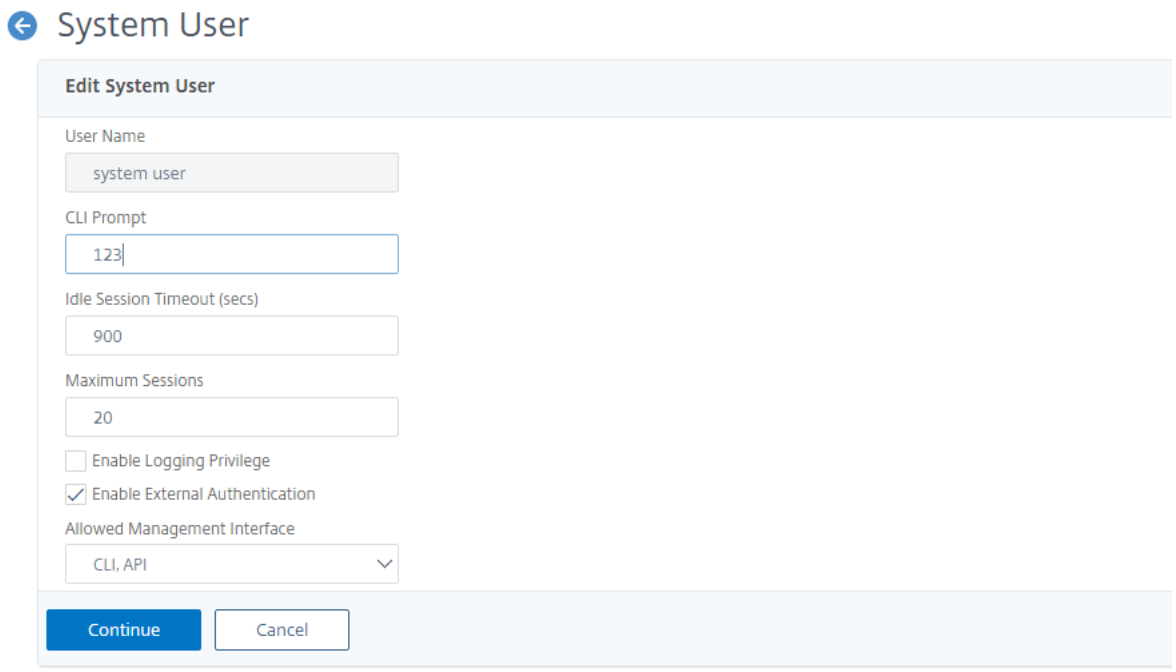


```
8       Maximum Client Sessions: 20
9  <!--NeedCopy-->
```

Informationen zur Parameterbeschreibung finden Sie unter Referenz zu Authentifizierung und Autorisierung für Benutzerbefehle .

Konfigurieren eines Benutzerkontos mit der Citrix ADC GUI

1. Navigieren Sie zu **System** > **Benutzeradministration** > **Benutzer**und erstellen Sie den Benutzer.
2. Klicken Sie im Detailbereich auf **Hinzufügen**, um einen Systembenutzer zu erstellen.
3. Legen Sie auf der Seite " **Systemgruppe erstellen** " die folgenden Parameter fest:
   a) Benutzername Name der Benutzergruppe
   b) CLI-Aufforderung. Die Aufforderung, die Sie für den Zugriff auf die CLI-Schnittstelle festlegen möchten.
   c) Timeout für Sitzungen im Leerlauf (Sekunden). Legen Sie fest, wie lange ein Benutzer inaktiv sein kann, bevor die Sitzung abläuft und geschlossen wird.
   d) Maximale Sitzungen. Legen Sie das Maximum an Sitzungen fest, die ein Benutzer versuchen kann.
   e) Aktivieren Sie Protokollierungsberechtigung Aktivieren Sie die Protokollierungsberechtigung für den Benutzer.
   f) Aktivieren Sie externe Authentifizierung. Wählen Sie die Option aus, wenn Sie einen externen Authentifizierungsserver zur Authentifizierung des Benutzers verwenden möchten.
   g) Erlaubte Verwaltungsoberfläche. Wählen Sie die Citrix ADC Schnittstellen aus, für die der Benutzergruppe Zugriffsberechtigung erteilt wird.
   h) Richtlinien für Befehle. Binden Sie Befehlsrichtlinien an die Benutzergruppe.
   i) Partitionen. Binden Sie Partitionen an die Benutzergruppe.
4. Klicken Sie auf **Erstellen** und **Schließen**.



Konfigurieren von Benutzergruppen

Nachdem Sie eine Benutzergruppe konfiguriert haben, können Sie ganz einfach jedem in der Gruppe dieselben Zugriffsrechte erteilen. Um eine Gruppe zu konfigurieren, erstellen Sie die Gruppe und binden Benutzer an die Gruppe. Sie können jedes Benutzerkonto an mehrere Gruppen binden. Das Binden von Benutzerkonten an mehrere Gruppen ermöglicht möglicherweise mehr Flexibilität beim Anwenden von Befehlsrichtlinien.

So erstellen Sie eine Benutzergruppe mit der Befehlszeilenschnittstelle

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

- `add system group <groupName> [-promptString <string>] [-timeout <secs>]`
- `show system group <groupName>`

Beispiel:

```
> add system group Managers -promptString Group-Managers-at-%h
```

Binden eines Benutzerkontos an eine Gruppe über die Befehlszeile

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um ein Benutzerkonto an eine Gruppe zu binden und die Konfiguration zu überprüfen:

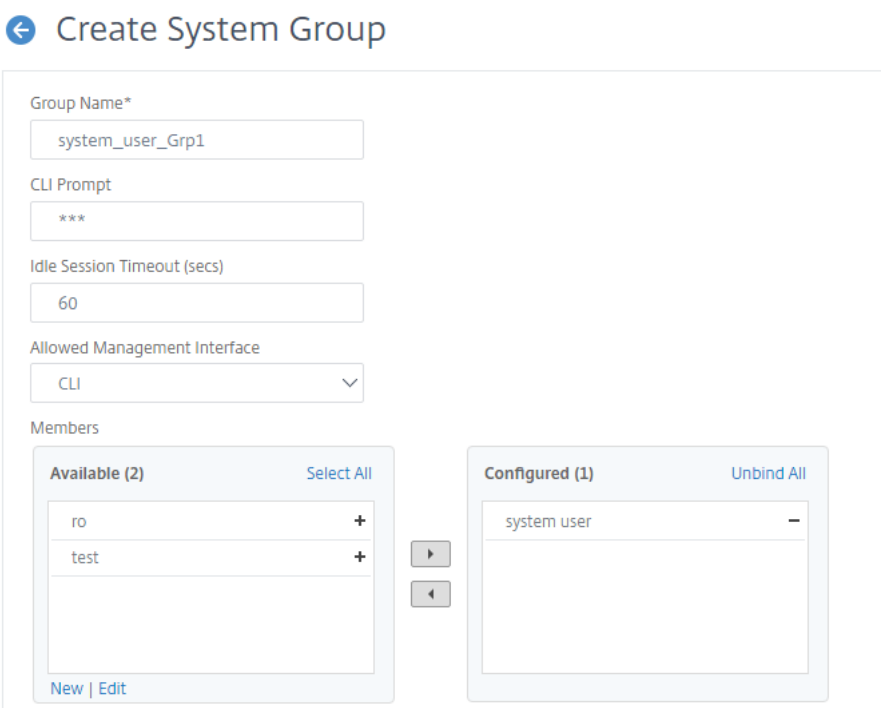
- `bind system group <groupName> -userName <userName>`
- `show system group <groupName>`

Beispiel:

```
> bind system group Managers -userName user1
```

Konfigurieren einer Benutzergruppe mit der Citrix ADC GUI

1. Navigieren Sie zu **System** > **User Administration** > **Groups**, und erstellen Sie die Benutzergruppe.
2. Klicken Sie im Detailbereich auf **Hinzufügen**, um eine Systembenutzergruppe zu erstellen.
3. Legen Sie auf der Seite " **Systemgruppe erstellen** " die folgenden Parameter fest:
   a) Gruppenname. Name der Benutzergruppe
   b) CLI-Aufforderung. Die Aufforderung, die Sie für den Zugriff auf die CLI-Schnittstelle festlegen möchten.
   c) Timeout für Sitzungen im Leerlauf (Sekunden). Legen Sie fest, wie lange ein Benutzer inaktiv sein kann, bevor die Sitzung abläuft und geschlossen wird.
   d) Erlaubte Verwaltungsoberfläche. Wählen Sie die Citrix ADC Schnittstellen aus, für die der Benutzergruppe Zugriffsberechtigung erteilt wird.
   e) Mitglieder. Fügen Sie der Gruppe Benutzerkonten hinzu.
   f) Richtlinien für Befehle. Binden Sie Befehlsrichtlinien an die Benutzergruppe.
   g) Partitionen. Binden Sie Partitionen an die Benutzergruppe.
4. Klicken Sie auf **Erstellen** und **Schließen**.



Hinweis:

Um der Gruppe Mitglieder hinzuzufügen, klicken Sie im Abschnitt Mitglieder auf **Hinzufügen**. Wählen Sie Benutzer aus der Liste Verfügbar aus und fügen Sie sie der Liste Konfiguriert hinzu.

Konfigurieren von Befehlsrichtlinien

Befehlsrichtlinien regeln, welche Befehle, Befehlsgruppen, virtuelle Server und andere Entitäten Benutzer und Benutzergruppen verwenden dürfen.

Die Appliance stellt eine Reihe integrierter Befehlsrichtlinien bereit, und Sie können benutzerdefinierte Richtlinien konfigurieren. Um die Richtlinien anzuwenden, binden Sie sie entweder an Benutzer oder an Gruppen.

Hier sind die wichtigsten Punkte, die Sie beim Definieren und Anwenden von Befehlsrichtlinien beachten müssen.

- Globale Befehlsrichtlinien können nicht erstellt werden. Befehlsrichtlinien müssen direkt an die Benutzer und Gruppen auf der Appliance gebunden sein.
- Benutzer oder Gruppen ohne zugehörige Befehlsrichtlinien unterliegen der Standardbefehlsrichtlinie (DENY-ALL) und können daher keine Konfigurationsbefehle ausführen, bis die richtigen Befehlsrichtlinien an ihre Konten gebunden sind.
- Alle Benutzer erben die Richtlinien der Gruppen, zu denen sie gehören.
- Sie müssen einer Befehlsrichtlinie eine Priorität zuweisen, wenn Sie sie an ein Benutzerkonto oder ein Gruppenkonto binden. Auf diese Weise kann die Appliance bestimmen, welche

Richtlinie Priorität hat, wenn zwei oder mehr widersprüchliche Richtlinien für denselben Benutzer oder dieselbe Gruppe gelten.

- Die folgenden Befehle sind standardmäßig für jeden Benutzer verfügbar und sind von einem von Ihnen angegebenen Befehl nicht betroffen:
- Hilfe, zeige CLI-Attribut an, setze CLI-Eingabeaufforderung, lösche CLI-Eingabeaufforderung, Alias, Unalias, Verlauf, Beenden, Beenden, Whoami, Config, Config, CLI-Modus festlege, lösche CLI-Modus und zeige den CLI-Modus an und zeige den CLI-Modus an.

In der folgenden Tabelle werden die integrierten Richtlinien beschrieben.

Richtlinienname	**Erlaubt**
read-only	Schreibgeschützter Zugriff auf alle Show-Befehle außer show ns RunningConfig, show ns ns.conf und den show-Befehlen für die Citrix ADC Befehlsgruppe.
operator	Schreibgeschützter Zugriff und Zugriff auf Befehle zum Aktivieren und Deaktivieren von Diensten und Servern.
Netzwerk	Voller Zugriff, mit Ausnahme der set- und unset-SSL-Befehle, zeigt ns ns.conf, show ns runningConfig und zeigt die Befehle gslb runningConfig an.
sysadmin	[In Citrix ADC 12.0 und höher enthalten] Ein Sysadmin ist niedriger als ein Superuser ist die Zugriffsbedingungen für die Appliance zulässig. Ein sysadmin-Benutzer kann alle Citrix ADC Vorgänge mit folgenden Ausnahmen ausführen: Kein Zugriff auf die Citrix ADC-Shell, keine Benutzerkonfigurationen ausführen, keine Partitionskonfigurationen ausführen und einige andere Konfigurationen, wie in der Sysadmin-Befehlsrichtlinie angegeben.
superuser	Vollzugriff: Dieselben Berechtigungen wie der Benutzer nsroot.

Erstellen benutzerdefinierter Befehlsrichtlinien

Für Benutzer mit den Ressourcen, um benutzerdefinierte Ausdrücke zu verwalten, und für Bereitstellungen, die die Flexibilität, die reguläre Ausdrücke bieten, wird Unterstützung für reguläre Ausdrücke angeboten. Für die meisten Benutzer sind die integrierten Befehlsrichtlinien ausreichend. Benutzer, die mehr Steuerungsebenen benötigen, aber mit regulären Ausdrücken nicht vertraut sind, möchten möglicherweise nur einfache Ausdrücke verwenden, wie die in den Beispielen in diesem Abschnitt, um die Lesbarkeit von Richtlinien zu erhalten.

Wenn Sie einen regulären Ausdruck zum Erstellen einer Befehlsrichtlinie verwenden, beachten Sie Folgendes:

- Wenn Sie reguläre Ausdrücke verwenden, um Befehle zu definieren, die von einer Befehlsrichtlinie betroffen sind, müssen Sie die Befehle in doppelte Anführungszeichen setzen. Um beispielsweise eine Befehlsrichtlinie zu erstellen, die alle Befehle enthält, die mit show beginnen, geben Sie Folgendes ein:
- “^show .*$”
- Um eine Befehlsrichtlinie zu erstellen, die alle Befehle enthält, die mit rm beginnen, geben Sie Folgendes ein:
- “^rm .*$”
- Reguläre Ausdrücke, die in Befehlsrichtlinien verwendet werden, werden nicht zwischen Groß- und Kleinschreibung unterschieden.

Die folgende Tabelle enthält Beispiele für reguläre Ausdrücke für Befehlsrichtlinien:

Befehlsspezifikation	Entspricht diesen Befehlen
“^rm\s+.*$”	Alle Entfernungsaktionen, da alle Entfernungsaktionen mit der rm-Zeichenfolge beginnen, gefolgt von einem Leerzeichen und weiteren Parametern wie Befehlsgruppen, Befehlsobjekttypen und Argumenten.
“^show\s+.*$”	Alle Show-Befehle, da alle Show-Aktionen mit der Show-String beginnen, gefolgt von einem Leerzeichen und weiteren Parametern wie Befehlsgruppen, Befehlsobjekttypen und Argumenten.
“^shell$”	Der Shell-Befehl allein, jedoch nicht mit zusätzlichen Parametern wie Befehlsgruppen, Befehlsobjekttypen und Argumenten kombiniert.

Befehlsspezifikation	Entspricht diesen Befehlen
“^add\s+vserver\s+.*$”	Alle erstellen virtuelle Serveraktionen, die aus dem Befehl “virtuellen Server hinzufügen”, gefolgt von einem Leerzeichen und weiteren Parametern wie Befehlsgruppen, Befehlsobjekttypen und Argumenten bestehen.
“^add\s+(lb\s+vserver)\s+.*”	Alle erstellen virtuelle Serveraktionen von lb, die aus dem Befehl add lb virtual server bestehen, gefolgt von einem Leerzeichen und weiteren Parametern wie Befehlsgruppen, Befehlsobjekttypen und Argumenten.

Informationen zu integrierten Befehlsrichtlinien finden Sie in Tabelle Integrierte Befehlsrichtlinientabelle .

So erstellen Sie eine Befehlsrichtlinie mit der Befehlszeilenschnittstelle

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

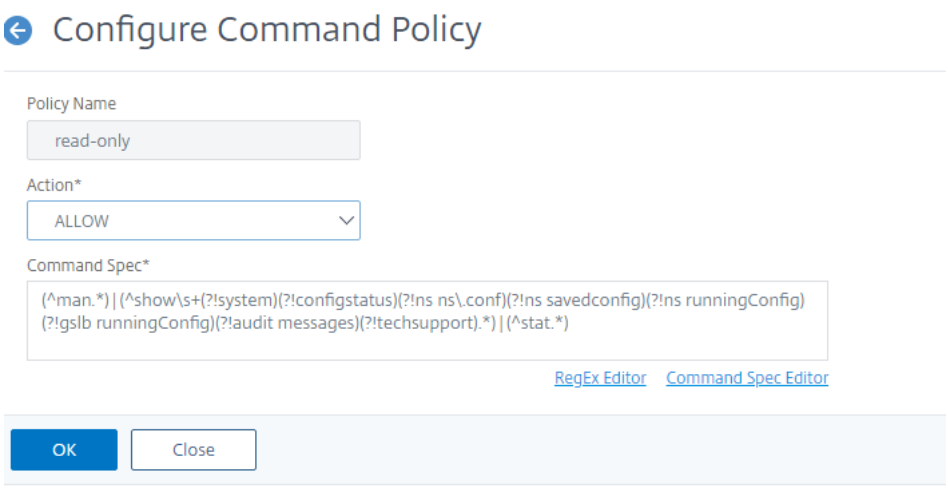
- `add system cmdPolicy <policyname> <action> <cmdspec>`
- `show system cmdPolicy <policyName>`

Beispiel:

```
add system cmdPolicy USER-POLICY ALLOW (\ server\ )|(\ service(Group)*\ )
|(\ vserver\ )|(\ policy\ )|(\ policylabel\ )|(\ limitIdentifier\ )|(^show\
 (?!(system|ns\ (ns.conf|runningConfig)))|(save)|(stat\ .*serv)
```

Konfigurieren einer Befehlsrichtlinie mit der Citrix ADC GUI

1. Navigieren Sie zu **System** > **Benutzerverwaltung** > **Befehlsrichtlinien**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**, um eine neue Befehlsrichtlinie zu erstellen.
3. Legen Sie auf der Seite **Command Policy konfigurieren** die folgenden Parameter fest:
   a) Richtlinienname
   b) Aktion
   c) Befehlsdetails
4. Klicken Sie auf **OK**.



Binden von Befehlsrichtlinien an Benutzerkonten und Benutzergruppen

Nachdem Sie die Befehlsrichtlinien definiert haben, müssen Sie sie an die entsprechenden Benutzerkonten und Gruppen binden. Wenn Sie eine Richtlinie binden, müssen Sie ihr eine Priorität zuweisen, damit die Appliance bestimmen kann, welche Befehlsrichtlinie befolgt werden soll, wenn zwei oder mehr anwendbare Befehlsrichtlinien in Konflikt stehen.

Befehlsrichtlinien werden in der folgenden Reihenfolge ausgewertet:

- Befehlsrichtlinien, die direkt an Benutzer und die entsprechenden Gruppen gebunden sind, werden anhand einer Prioritätsnummer ausgewertet. Eine Befehlsrichtlinie mit einer niedrigeren Prioritätsnummer wird vor einer mit einer höheren Prioritätsnummer ausgewertet. Daher werden alle Berechtigungen, die die untergeordnete Befehlsrichtlinie explizit gewährt oder verweigert, nicht durch eine höhere Befehlsrichtlinie außer Kraft gesetzt.
- Wenn zwei Befehlsrichtlinien, eine an ein Benutzerkonto und eine andere an eine Gruppe gebunden, dieselbe Prioritätsnummer haben, wird zuerst die direkt an das Benutzerkonto gebundene Befehlsrichtlinie ausgewertet.

So binden Sie Befehlsrichtlinien mit der Befehlszeilenschnittstelle an einen Benutzer

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Befehlsrichtlinie an einen Benutzer zu binden und die Konfiguration zu überprüfen:

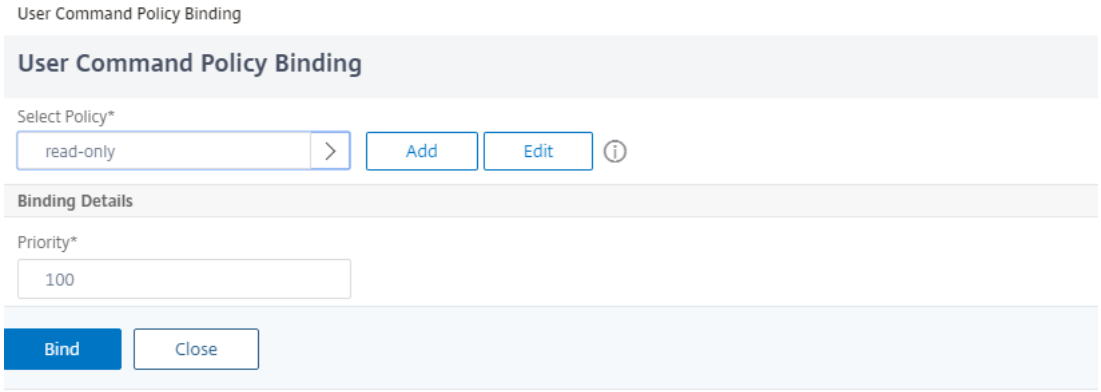
- `bind system user <userName> -policyName <policyName> <priority>`
- `show system user <userName>`

Beispiel:

```
> bind system user user1 -policyName read_all 1
```


Binden von Befehlsrichtlinien an ein Benutzerkonto mithilfe der Citrix ADC GUI

Navigieren Sie zu **System** > **Benutzeradministration** > **Benutzer**, wählen Sie den Benutzer und die Bind-Befehlsrichtlinien aus.



Optional können Sie die Standardpriorität ändern, um sicherzustellen, dass die Richtlinie in der richtigen Reihenfolge ausgewertet wird.

So binden Sie Befehlsrichtlinien mit der Befehlszeilenschnittstelle an eine Gruppe

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um eine Befehlsrichtlinie an eine Benutzergruppe zu binden, und überprüfen Sie die Konfiguration:

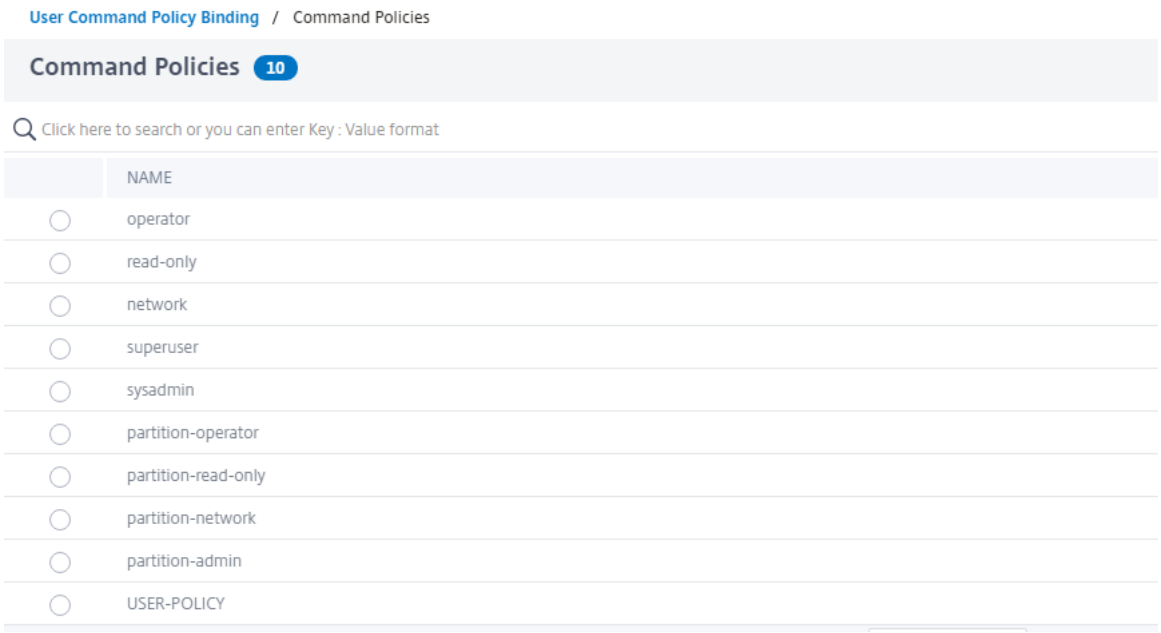
- `bind system group <groupName> -policyName <policyName> <priority>`
- `show system group <groupName>`

Beispiel:

```
> bind system group Managers -policyName read_all 1
```

Binden von Befehlsrichtlinien an eine Benutzergruppe mithilfe der Citrix ADC GUI

Navigieren Sie zu **System** > **Benutzeradministration** > **Gruppen**, wählen Sie die Gruppen- und Bind-Befehlsrichtlinien aus.



Optional können Sie die Standardpriorität ändern, um sicherzustellen, dass die Richtlinie in der richtigen Reihenfolge ausgewertet wird.

Anwendungsbeispiel: Verwalten von Benutzerkonten, Benutzergruppen und Befehlsrichtlinien in einer Fertigungsorganisation

Das folgende Beispiel zeigt, wie Sie einen vollständigen Satz von Benutzerkonten, Gruppen und Befehlsrichtlinien erstellen und jede Richtlinie an die entsprechenden Gruppen und Benutzer binden. Das Unternehmen, Example Manufacturing, Inc., verfügt über drei Benutzer, die auf die Citrix ADC Appliance zugreifen können:

- **John Doe.** Der IT-Manager. John muss in der Lage sein, alle Teile der Citrix ADC Konfiguration zu sehen, muss aber nichts ändern.
- **Maria Ramiez.** Die leitende IT-Administratorin. Maria muss in der Lage sein, alle Teile der Citrix ADC Konfiguration zu sehen und zu ändern, mit Ausnahme von Citrix ADC-Befehlen (welche lokalen Richtlinien diktiert, muss ausgeführt werden, während sie als NSroot angemeldet ist).
- **Michael Baldrock.** Der für den Lastausgleich zuständige IT-Administrator. Michael muss in der Lage sein, alle Teile der Citrix ADC Konfiguration zu sehen, muss jedoch nur die Load Balancing-Funktionen ändern.

Die folgende Tabelle zeigt die Aufschlüsselung der Netzwerkinformationen, Benutzerkontonamen, Gruppennamen und Befehlsrichtlinien für das Beispielunternehmen.

Feld	Wert	Hinweis:
Citrix ADC Hostname	ns01.beispiel.net	Nicht zutreffend

Feld	Wert	Hinweis:
Benutzerkonten	johnd, mariar und michaelb	John Doe, IT-Manager, Maria Ramirez, IT-Administrator und Michael Baldrock, IT-Administrator.
Gruppen	Manager und SysOps	Alle Manager und alle IT-Administratoren.
Befehlsrichtlinien	read_all, modify_lb und modify_all	Vollständigen schreibgeschützten Zugriff zulassen, Änderungszugriff für Lastenausgleich zulassen und Vollständigen Änderungszugriff zulassen.

Die folgende Beschreibung führt Sie durch das Erstellen eines vollständigen Satzes von Benutzerkonten, Gruppen und Befehlsrichtlinien auf der Citrix ADC Appliance namens ns01.example.net.

Die Beschreibung enthält Verfahren zum Binden der entsprechenden Benutzerkonten und -gruppen sowie zum Binden geeigneter Befehlsrichtlinien an die Benutzerkonten und -gruppen.

In diesem Beispiel wird veranschaulicht, wie Sie die Priorisierung verwenden können, um jedem Benutzer in der IT-Abteilung präzisen Zugriff und Berechtigungen zu gewähren.

Im Beispiel wird davon ausgegangen, dass die Erstinstallation und Konfiguration bereits auf dem Citrix ADC durchgeführt wurden.

Konfigurieren von Benutzerkonten, Gruppen und Befehlsrichtlinien für eine Beispielorganisation

1. Verwenden Sie das unter Abschnitt Konfigurieren von Benutzerkonten beschriebenen Verfahren, um **Benutzerkonten Jong**, **Mariar**und **michaelb**zu erstellen.
2. Verwenden Sie das unter Konfigurieren von Benutzergruppen beschriebene Verfahren, um Benutzergruppen **Manager** und **SysOps** zu erstellen, und binden Sie dann die Benutzer **mariar** und **michaelb** an die **SysOps-Gruppe** und den Benutzer **johnd** an die **Manager-Gruppe**.
3. Verwenden Sie das unter Erstellen von benutzerdefinierten Befehlsrichtlinien beschriebene Verfahren, um die folgenden Befehlsrichtlinien zu erstellen:
   - **read_all** mit Aktion **Zulassen** und Befehlsspezifikation `"(^show\s+(?!system)(?!ns ns.conf)(?!ns runningConfig).*)|(^stat.*)"`

- **modify_lb** mit Aktion **Zulassen** und der Befehlsspezifikation "^set\s+lb\s+.*$"
- modify_all mit Aktion Zulassen und der Befehlsspezifikation "^\S+\s+(?!system).*"

4. Verwenden Sie das unter "Binden von Befehlsrichtlinien an Benutzer und Gruppen" beschriebene Verfahren, um die **read_all-Befehlsrichtlinie** mit dem Prioritätswert **1** an die **SysOps-Gruppe**zu binden.

5. Verwenden Sie das unter "Binden von Befehlsrichtlinien an Benutzer und Gruppen" beschriebene Verfahren, um die **modify_lb-Befehlsrichtlinie** mit dem Prioritätswert **5**an Benutzer **michaelb**zu binden.

Die soeben erstellte Konfiguration führt zu folgendem Ergebnis:

- Der IT-Manager John Doe hat schreibgeschützten Zugriff auf die gesamte Citrix ADC Konfiguration, aber er kann keine Änderungen vornehmen.
- Maria Ramirez, IT-Lead, hat nahezu vollständigen Zugriff auf alle Bereiche der Citrix ADC Konfiguration und muss sich nur anmelden, um Befehle auf Citrix ADC-Ebene auszuführen.
- Michael Baldrock, der für den Lastausgleich zuständige IT-Administrator, hat schreibgeschützten Zugriff auf die Citrix ADC Konfiguration und kann die Konfigurationsoptionen für den Lastausgleich ändern.

Die Gruppe von Befehlsrichtlinien, die für einen bestimmten Benutzer gelten, ist eine Kombination von Befehlsrichtlinien, die direkt auf das Konto des Benutzers angewendet werden, und Befehlsrichtlinien, die auf eine oder mehrere Gruppen angewendet werden, in denen der Benutzer Mitglied ist.

Jedes Mal, wenn ein Benutzer einen Befehl eingibt, durchsucht das Betriebssystem die Befehlsrichtlinien für diesen Benutzer, bis eine Richtlinie mit der Aktion Zulassen oder DENY gefunden wird, die dem Befehl entspricht. Wenn es eine Übereinstimmung findet, stoppt das Betriebssystem seine Befehlsrichtliniensuche und erlaubt oder verweigert den Zugriff auf den Befehl.

Wenn das Betriebssystem keine übereinstimmende Befehlsrichtlinie findet, verweigert es dem Benutzer den Zugriff auf den Befehl gemäß der standardmäßigen Verweigerungsrichtlinie der Citrix ADC Appliance.

> **Hinweis:**
>
> Wenn Sie einen Benutzer in mehrere Gruppen platzieren, achten Sie darauf, keine unbeabsichtigten Benutzerbefehlsbeschränkungen oder -berechtigungen zu verursachen. Um diese Konflikte zu vermeiden, sollten Sie beim Organisieren der Benutzer in Gruppen die Citrix ADC Befehlsrichtlinien-Suchprozedur und die Regeln für die Richtlinienanordnung berücksichtigen.

Benutzerkonto und Kennwortverwaltung

October 5, 2021

Citrix ADC ermöglicht Ihnen die Verwaltung von Benutzerkonten und Kennwortkonfiguration. Nachfolgend sind einige der Aktivitäten aufgeführt, die Sie für ein Systembenutzerkonto oder ein `nsroot` Administratorbenutzerkonto auf der Appliance durchführen können.

- Systemnutzer-Kontosperrung
- Sperren des Systembenutzerkontos für Verwaltungszugriff
- Entsperren eines gesperrten Systembenutzerkontos für den
- Deaktivieren des Verwaltungszugriffs für Systembenutzerkonto
- Kennwortänderung für `nsroot` administrative Benutzer erz
- Entfernen vertraulicher Dateien in einem Systembenutzerkonto
- Starke Kennwortkonfiguration für Systembenutz

Systemnutzer-Kontosperrung

Um Brute-Force-Sicherheitsangriffe zu verhindern, können Sie die Benutzersperrenkonfiguration konfigurieren. Die Konfiguration ermöglicht es einem Netzwerkadministrator, zu verhindern, dass sich ein Systembenutzer bei einer Citrix ADC Appliance anmeldet. Entsperren Sie auch das Benutzerkonto, bevor der Sperrzeitraum abläuft.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set aaa parameter -maxloginAttempts <value> -failedLoginTimeout <value> -
persistentLoginAttempts (ENABLED | DISABLED)
```

> **Hinweis:**
>
> Der Parameter “PersistentLoginAttempts” muss ENABLED sein, um die Details der persistenten Speicherung von erfolglosen Anmeldeversuchen der Benutzer abzurufen.

Beispiel:

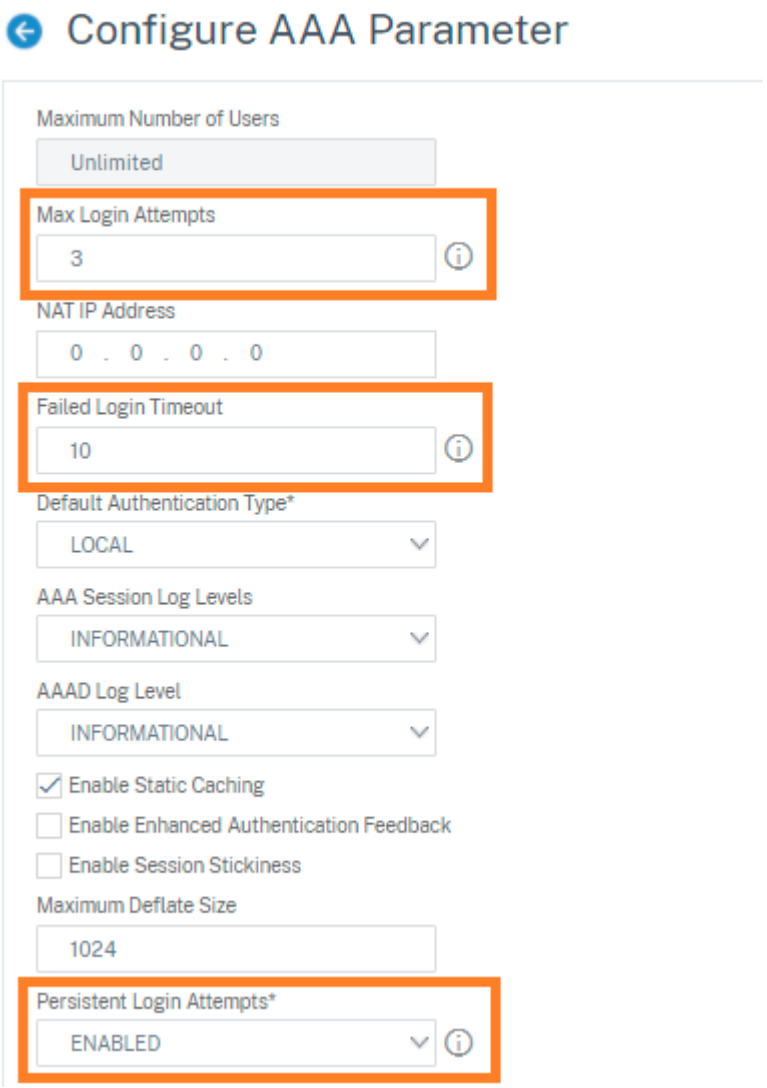
```
set aaa parameter -maxloginAttempts 3 -failedLoginTimeout 10 -persistentLoginAttempts
 ENABLED
```

Konfigurieren der Systembenutzerkontosperrung mit der GUI

1. Navigieren Sie zu **Konfiguration > Sicherheit > AAA-Anwendungsdatenverkehr > Authentifizierungseinstellungen > AAA-Authentifizierungseinstellungen ändern**.
2. Legen Sie auf der Seite **AAA-Parameter konfigurieren** die folgenden Parameter fest:

a) Max Login-Versuche. Die maximale Anzahl von Anmeldeversuchen, die der Benutzer ausprobieren konnte.
b) Timeout bei fehlgeschlagenem Die maximale Anzahl von ungültigen Anmeldeversuchen des Benutzers.
c) Dauerhafte Anmeldeversuche. Dauerhafte Speicherung von erfolglosen Anmeldeversuchen von Benutzern.

3. Klicken Sie auf **OK**.



Wenn Sie die Parameter festlegen, wird das Benutzerkonto für 10 Minuten für drei oder mehr ungültige Anmeldeversuche gesperrt. Außerdem kann sich der Benutzer nicht einmal mit gültigen Anmeldeinformationen für 10 Minuten anmelden.

> **Hinweis:**
>
> Wenn ein gesperrter Benutzer versucht, sich bei der Appliance anzumelden, wird eine Fehler-

> meldung `RBA Authentication Failure: maxlogin attempt reached for test.` angezeigt.

Sperren des Systembenutzerkontos für Verwaltungszugriff

Mit der Citrix ADC Appliance können Sie einen Systembenutzer 24 Stunden lang sperren und dem Benutzer den Zugriff verweigern.

Die Citrix ADC Appliance unterstützt die Konfiguration für Systembenutzer und externe Benutzer.

> **Hinweis:**
>
> Die Funktion wird nur unterstützt, wenn Sie die `persistentLoginAttempts` Option im `aaa` Parameter deaktivieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

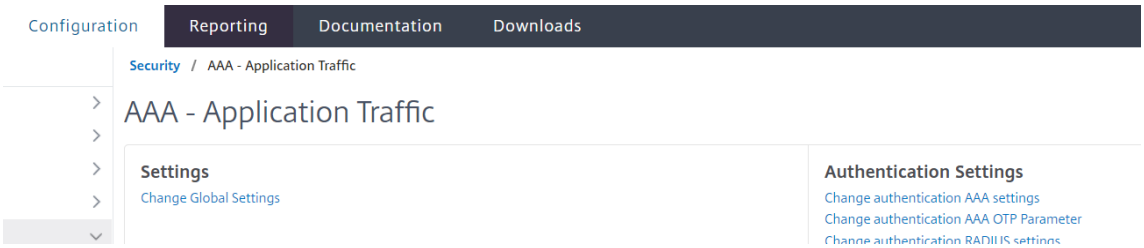
```
set aaa parameter -persistentLoginAttempts DISABLED
```

Um ein Benutzerkonto zu sperren, geben Sie an der Eingabeaufforderung Folgendes ein:

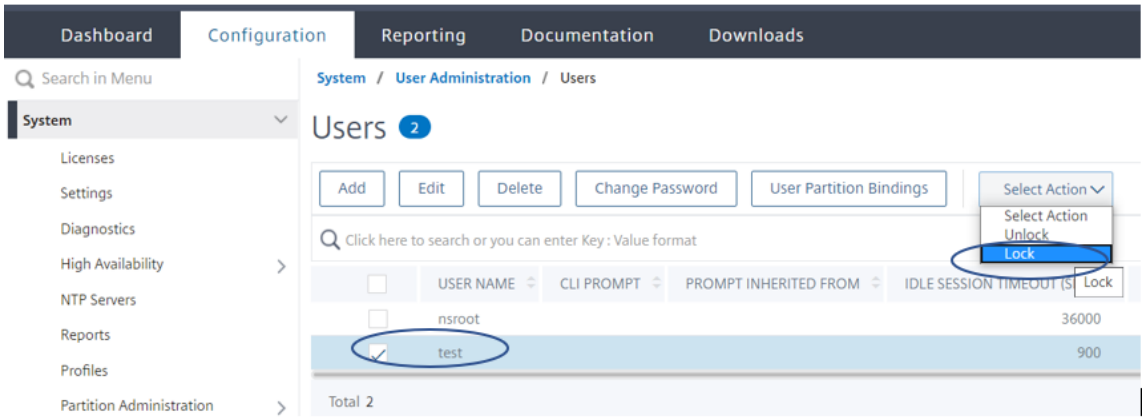
```
lock aaa user test
```

Sperren eines Systembenutzerkontos mit der GUI

1. Navigieren Sie zu **Konfiguration > Sicherheit > AAA-Anwendungsdatenverkehr > Authentifizierungseinstellungen > AAA-Authentifizierungseinstellungen ändern**.



2. Wählen Sie unter **AAA-Parameter konfigurieren**in der Liste **Persistente Anmeldeversuche** die Option **DEAKTIVIERT**aus.
3. Navigieren Sie zu **System > Benutzeradministration > Benutzer**.
4. Wählen Sie einen Benutzer aus.
5. Wählen Sie in der Liste Aktion auswählen die Option **Sperren**aus.



> **Hinweis:**
>
> Die Citrix ADC GUI hat keine Möglichkeit, externe Benutzer zu sperren. Um einen externen Benutzer zu sperren, muss der ADC-Administrator die CLI verwenden.
> Wenn ein gesperrter Systembenutzer (gesperrter Benutzer mit Sperrauthentifizierung, Autorisierung und Überwachungsbenutzer) versucht, sich bei Citrix ADC anzumelden, zeigt die Appliance eine Fehlermeldung "RBA-Authentifizierungsfehler: Benutzertest ist für 24 Stunden gesperrt" an.
>
> Wenn ein Benutzer für die Anmeldung beim Verwaltungszugriff gesperrt ist, ist der Konsolenzugriff ausgenommen. Der gesperrte Benutzer kann sich bei der Konsole anmelden.

Entsperren eines gesperrten Systembenutzerkontos für den

Systembenutzer und externe Benutzer können mit dem Befehl sperren Authentifizierung, Autorisierung und Überwachungsbenutzer für 24 Stunden gesperrt werden.

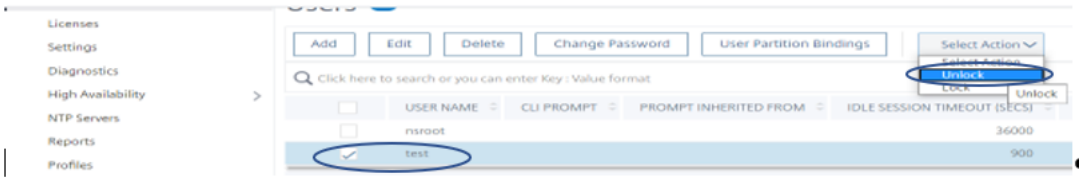
> **Hinweis:**
>
> Die ADC-Appliance ermöglicht es Administratoren, den gesperrten Benutzer zu entsperren, und die Funktion erfordert keine Einstellungen im Befehl "PersistentLoginAttempts".

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
unlock aaa user test
```

Konfigurieren Sie die Entsperrung von Systembenutzern über die GUI

1. Navigieren Sie zu **System > Benutzeradministration > Benutzer**.
2. Wählen Sie einen Benutzer aus.
3. Klicke auf **entsperr**



Die Citrix ADC GUI listet nur Systembenutzer auf, die im ADC erstellt wurden, sodass es in der GUI keine Möglichkeit gibt, externe Benutzer zu entsperren. Um einen externen Benutzer freizuschalten, muss der `nsroot` Administrator die CLI verwenden.

Deaktivieren des Verwaltungszugriffs für Systembenutzerkonto

Wenn die externe Authentifizierung auf der Appliance konfiguriert ist und Sie als Administrator es vorziehen, Systembenutzern den Zugriff zu verweigern, um sich beim Verwaltungszugriff anzumelden, müssen Sie die Option LocalAuth im Systemparameter deaktivieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

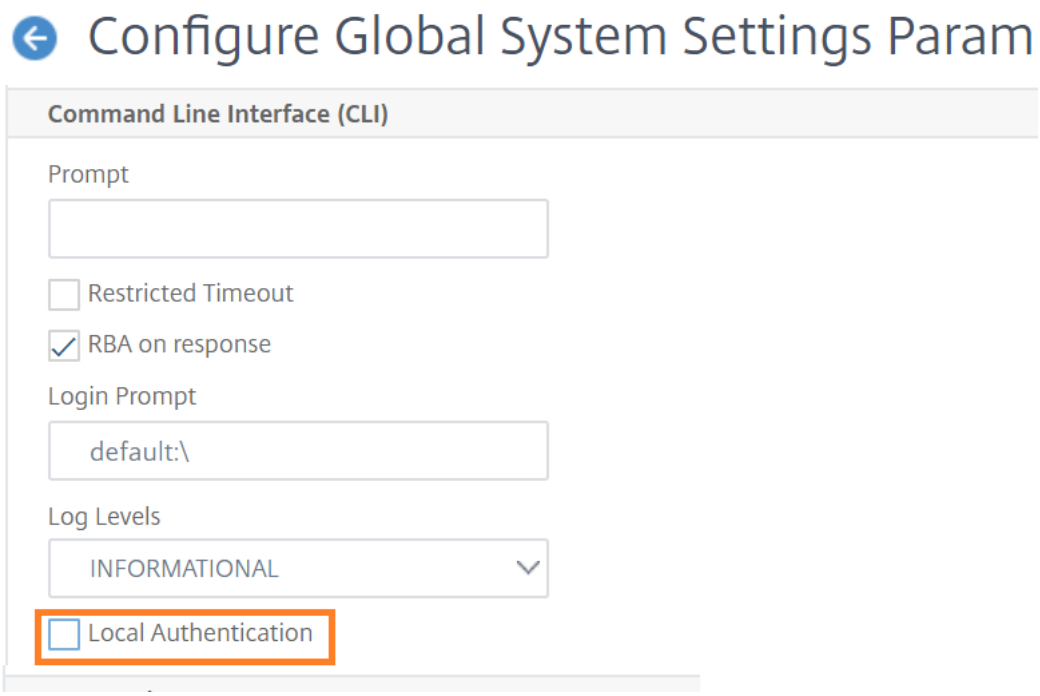
```
set system parameter localAuth <ENABLED|DISABLED>
```

Beispiel:

```
set system parameter localAuth DISABLED
```

Deaktivieren des Verwaltungszugriffs auf Systembenutzer über die GUI

1. Navigieren Sie zu **Konfiguration > System > Einstellungen > Globale Systemeinstellungen ändern**.
2. Deaktivieren Sie im Abschnitt **Command Line Interface (CLI)** das Kontrollkästchen **Lokale Authentifizierung**.



Durch Deaktivieren der Option können sich lokale Systembenutzer nicht bei ADC-Verwaltungszugriff anmelden.

> **Hinweis:**
>
> Externer Authentifizierungsserver muss konfiguriert und erreichbar sein, um die Benutzerauthentifizierung des lokalen Systems im Systemparameter zu unterlassen. Wenn ein externer Server, der in ADC für den Verwaltungszugriff konfiguriert ist, nicht erreichbar ist, können sich lokale Systembenutzer bei der Appliance anmelden. Das Verhalten ist für Wiederherstellungszwecke eingerichtet.

Kennwortänderung für administrative Benutzer erz

Zur `nsroot` sicheren Authentifizierung fordert die Citrix ADC Appliance den Benutzer auf, das Standardkennwort in ein neues zu ändern, wenn die `forcePasswordChange` Option im Systemparameter aktiviert ist. Sie können Ihr `nsroot` Kennwort entweder über CLI oder GUI ändern, bei Ihrer ersten Anmeldung mit den Standardanmeldeinformationen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set system parameter -forcePasswordChange ( ENABLED | DISABLED )
```

Beispiel für eine SSH-Sitzung für NSIP:

```
1 ssh nsroot@1.1.1.1
```



```
Connecting to 1.1.1.1:22...
Connection established.
To escape to local shell, press Ctrl+Alt+].
###############################################################################

WARNING: Access to this system is for authorized users only #
Disconnect IMMEDIATELY if you are not an authorized user! #

###############################################################################

Please change the default NSROOT password.
Enter new password:
Please re-enter your password:
Done
<!--NeedCopy-->
```

Entfernen vertraulicher Dateien in einem Systembenutzerkonto

Um sensible Daten wie autorisierte Schlüssel und öffentliche Schlüssel für ein Systembenutzerkonto zu verwalten, müssen Sie die `removeSensitiveFiles` Option aktivieren. Die Befehle, die vertrauliche Dateien entfernen, wenn der Systemparameter aktiviert ist, sind:

- rm-Clusterinstanz
- rm-Clusterknoten
- rm Knoten für hohe Verfügbarkeit
- klar Config voll
- beitreten Cluster
- Clusterinstanz hinzufügen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set system parameter removeSensitiveFiles ( ENABLED | DISABLED )
```

Beispiel:

```
set system parameter -removeSensitiveFiles ENABLED
```

Starke Kennwortkonfiguration für Systembenutz

Für eine sichere Authentifizierung fordert die Citrix ADC Appliance Systembenutzer und Administratoren auf, sichere Kennwörter festzulegen, um sich bei der Appliance anzumelden. Das Kennwort muss lang sein und muss eine Kombination aus folgenden Elementen sein:

- Ein Kleinbuchstaben
- Ein Großbuchstaben

- Ein numerisches Zeichen
- Ein Sonderzeichen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set system parameter -strongpassword <value> -minpasswordlen <value>
```

Hierbei gilt:

`Strongpassword`. Nach dem Aktivieren des starken Kennworts (`enable all` / `enablelocal`) müssen alle Kennwörter oder vertraulichen Informationen Folgendes enthalten:

- Mindestens ein Kleinbuchstaben
- Mindestens ein Großbuchstaben
- Mindestens ein numerisches Zeichen
- Mindestens ein Sonderzeichen

Exclude the list in `enablelocal` is - `NS_FIPS`, `NS_CRL`, `NS_RSAKEY`, `NS_PKCS12`, NS_PKCS8, NS_LDAP, `NS_TACACS`, `NS_TACACSACTION`, `NS_RADIUS`, `NS_RADIUSACTION`, `NS_ENCRYPTION_PARAMS`. Daher werden keine Strong Password-Überprüfungen für diese ObjectType-Befehle für den Systembenutzer durchgeführt.

Mögliche Werte: `enableall`, `enablelocal`, disabled
Standardwert: disabled

`minpasswordlen`. Mindestlänge des Kennworts des Systembenutzers. Wenn das starke Kennwort standardmäßig aktiviert ist, beträgt die Mindestlänge 4. Der vom Benutzer eingegebene Wert kann größer oder gleich 4 sein. Der Standardminimalwert ist 1, wenn das starke Kennwort deaktiviert ist. Der Höchstwert liegt in beiden Fällen bei 127.

Mindestwert: 1
Maximaler Wert: 127

Beispiel:

```
set system parameter -strongpassword enablelocal -minpasswordlen 6
```

Standardbenutzerkonto

Das `nsrecover`-Benutzerkonto kann vom Administrator zur Wiederherstellung der Citrix ADC Appliance verwendet werden. Sie können sich per `nsrecover` bei der ADC-Appliance anmelden, wenn sich die Standardsystembenutzer (`nsroot`) aufgrund unvorhergesehener Probleme nicht anmelden können. Die `nsrecover`-Anmeldung ist unabhängig von Benutzerkonfigurationen und ermöglicht Ihnen den direkten Zugriff auf die Shell-Eingabeaufforderung. Sie können sich immer über `nsrecover` einloggen, unabhängig davon, ob das maximale Konfigurationslimit erreicht ist.

So setzen Sie das root-Administrator (nsroot) -Kennwort zurück

June 1, 2022

Das Citrix ADC root-Administrator (`nsroot`) -Konto bietet vollständigen Zugriff auf alle ADC-Funktionen. Um die Sicherheit zu gewährleisten, darf das Administratorkonto nur bei Bedarf verwendet werden.

Als Admin empfiehlt es sich, Ihr Kennwort zu ändern. Wenn Sie Ihr Kennwort vergessen, müssen Sie zuerst auf das Standardkennwort zurücksetzen und es dann in ein neues Kennwort ändern.

Um Ihr Kennwort zurückzusetzen, müssen Sie sich als `nsroot`-Administrator bei Ihrer Appliance anmelden und das Kennwort ändern. Wenn Sie sich jedoch nicht an das Kennwort erinnern, können Sie die Appliance im Einzelbenutzermodus neu starten. Hängen Sie das Dateisystem im Lese-/Schreibmodus ein und entfernen Sie dann den **Citrix ADC-Eintrag** aus der Datei ns.conf. Starten Sie als letzten Schritt neu und melden Sie sich mit dem Standardgerät bei Ihrer Appliance an und legen Sie ein neues Kennwort fest.

Führen Sie die folgenden Schritte aus, um Ihr Root-Administratorkennwort zurückzusetzen

1. Verbinden Sie einen Computer mit dem Konsolenport des Citrix ADC und melden Sie sich an.

   > **Hinweis**
   >
   > Sie können sich nicht mit SSH anmelden, um dieses Verfahren durchzuführen. Sie müssen sich direkt mit der Appliance verbinden.

2. Starten Sie den Citrix ADC neu.
3. Drücken Sie STRG+C, wenn die folgende Meldung angezeigt wird:

   ```
   Press [Ctrl-C] for command prompt, or any other key to boot immediately
   .
   Booting [kernel] in ## seconds.
   ```

   > **Hinweis**
   >
   > In einer seriellen Azure-Konsole unterstützt die Citrix ADC Appliance keinen Einzelstart, bis die ADC-Appliance gestartet wurde.

4. Führen Sie den folgenden Befehl aus, um den Citrix ADC in einem einzigen Benutzermodus zu starten:

   ```
   boot -s
   ```

   Nach dem Booten der Appliance wird die folgende Meldung angezeigt:

   Geben Sie den vollständigen Pfadnamen der Shell ein oder `RETURN for /bin/sh:`

5. Drücken Sie die EINGABETASTE, um die Eingabeaufforderung # anzuzeigen, und geben Sie die folgenden Befehle ein, um die Dateisysteme

   a) Führen Sie den folgenden Befehl aus, um die Datenträgerkonsistenz zu überprüfen:

   ```
   fsck_ufs /dev/ad0s1a
   ```

   > **Hinweis**
   >
   > Ihr Flash-Laufwerk hat je nach Citrix ADC einen bestimmten Gerätenamen. Sie müssen also ad0s1a im vorherigen Befehl durch den entsprechenden Gerätenamen ersetzen.

   b) Greifen Sie auf das Dev-Verzeichnis zu und geben Sie 'ls' ein, um die Laufwerksdetails zu überprüfen.

   c) Führen Sie den folgenden Befehl aus, um die bereitgestellten Partitionen anzuzeigen:

   ```
   df
   ```

   > **Hinweis**
   >
   > Wenn die Flash-Partition nicht aufgeführt ist, müssen Sie sie manuell einhängen.

   d) Führen Sie den folgenden Befehl aus, um das Flash-Laufwerk einzubinden:

   ```
   mount dev/ad0s1a/flash
   ```

6. Führen Sie den folgenden Befehl aus, um in das Verzeichnis `nsconfig` zu wechseln:

   ```
   cd /flash/nsconfig
   ```

7. Führen Sie die folgenden Befehle aus, um die Datei ns.conf neu zu schreiben und den Satz von Systembefehlen zu entfernen, die standardmäßig auf den Administrator gesetzt sind:

   a) Führen Sie den folgenden Befehl aus, um eine Konfigurationsdatei zu erstellen, die keine Befehle enthält, die standardmäßig vom Administrator verwendet werden:

   ```
   grep -v "set system user nsroot" ns.conf > new.conf
   ```

   b) Führen Sie den folgenden Befehl aus, um eine Backup der vorhandenen Konfigurationsdatei zu erstellen:

   ```
   mv ns.conf old.ns.conf
   ```

   c) Führen Sie den folgenden Befehl aus, um die neue.conf-Datei in ns.conf umzubenennen:

   ```
   mv new.conf ns.conf
   ```

8. Führen Sie den folgenden Befehl aus, um den Citrix ADC neu zu starten:

   ```
   reboot
   ```

9. Melden Sie sich mit den Standard-Administratoranmeldeinformationen an.

10. Führen Sie den folgenden Befehl aus, um das Administratorkennwort zurückzusetzen:

    ```
    set system user nsroot <New_Password>
    ```

    > **Hinweis**
    >
    > Um das "?"-Zeichen in einer Kennwortzeichenfolge zu benutzen, stellen Sie diesem Zeichen ein \-Zeichen voraus.

    Zum Beispiel wird `yourexamplepasswd\?` für das Administratorkonto festgelegt, nachdem Sie den folgenden Vorgang ausgeführt haben:

    ```
    > set system user nsroot yourexamplepasswd\?
    ```

> **Hinweis**
>
> Um ein vergessenes (`nsroot`) Kennwort in einem Hochverfügbarkeits-Setup zurückzusetzen, empfiehlt Citrix, den Peer-Knoten herunterzufahren. Wenn der Peer-Knoten aktiv ist, wird das Kennwort überschrieben, da die Konfigurationssynchronisierung ausgelöst wird, wenn der Knoten nach dem Neustart hochfährt.

Lesen Sie auch den Citrix Artikel CTX224027, um zu erfahren, wie sicherer SSH-Zugriff auf Citrix ADC Appliance funktioniert.

Externe Benutzerauthentifizierung

February 24, 2022

Der Authentifizierungsdienst in einer Citrix ADC Appliance kann lokal oder extern sein. Bei der Authentifizierung externer Benutzer verwendet die Appliance einen externen Server wie LDAP, RADIUS oder TACACS+, um den Benutzer zu authentifizieren. Um einen externen Benutzer zu authentifizieren und dem Benutzer Zugriff auf die Appliance zu gewähren, müssen Sie eine Authentifizierungsrichtlinie anwenden. Die Citrix ADC -Systemauthentifizierung verwendet erweiterte Authentifizierungsrichtlinien mit erweiterten Richtlinienausdrücken. Die erweiterten Authentifizierungsrichtlinien werden auch für die Systembenutzerverwaltung in einer partitionierten Citrix ADC Appliance verwendet.

> **Hinweis:**
>
> Wenn Ihre Appliance weiterhin Classic-Richtlinien und ihre Ausdrücke verwendet, müssen Sie sie nicht mehr verwenden und die Verwendung der Classic-Richtlinie in die Advanced-Richtlinieninfrastruktur migrieren.

Sobald Sie eine Authentifizierungsrichtlinie erstellt haben, müssen Sie sie an die globale Systemeinheit binden. Sie können einen externen Authentifizierungsserver (z. B. TACACS) konfigurieren, indem Sie eine einzige Authentifizierungsrichtlinie an die globale Entität des Systems binden. Sie können

auch eine Kaskade von Authentifizierungsservern konfigurieren, indem Sie mehrere Richtlinien an die globale Entität des Systems binden.

> **Hinweis:**
>
> Wenn sich ein externer Benutzer bei der Appliance anmeldet, generiert das System eine Fehlermeldung “Benutzer existiert nicht” in der `ns.log` Datei. Das Vorkommen liegt daran, dass das System den Befehl systemuser_systemcmdpolicy_binding ausführt, um die GUI für den Benutzer zu initialisieren.

LDAP-Authentifizierung (mit externen LDAP-Servern)

Sie können die Citrix ADC Appliance so konfigurieren, dass der Benutzerzugriff mit einem oder mehreren LDAP-Servern authentifiziert wird. Die LDAP-Autorisierung erfordert identische Gruppennamen im Active Directory, auf dem LDAP-Server und auf der Appliance. Die Zeichen und die Groß- und Kleinschreibung müssen ebenfalls identisch sein.

Weitere Informationen zu LDAP-Authentifizierungsrichtlinien finden Sie unter Thema LDAP-Authentifizierungsrichtlinien .

Standardmäßig ist die LDAP-Authentifizierung durch das SSL/TLS-Protokoll gesichert. Es gibt zwei Arten von sicheren LDAP-Verbindungen. Beim ersten Typ akzeptiert der LDAP-Server die SSL/TLS-Verbindung an einem Port, der von dem Port getrennt ist, der für die Annahme klarer LDAP-Verbindungen verwendet wird. Nachdem Benutzer die SSL/TLS-Verbindung hergestellt haben, kann LDAP-Datenverkehr über die Verbindung gesendet werden. Der zweite Typ erlaubt sowohl unsichere als auch sichere LDAP-Verbindungen, und der einzelne Port verarbeitet es auf dem Server. In diesem Szenario erstellt der Client zunächst eine klare LDAP-Verbindung, um eine sichere Verbindung zu erstellen. Anschließend wird der **LDAP-Befehl** StartTLS über die Verbindung an den Server gesendet. Wenn der LDAP-Server StartTLS unterstützt, wird die Verbindung mithilfe von TLS in eine sichere LDAP-Verbindung konvertiert.

Die Portnummern für LDAP-Verbindungen lauten:

- 389 für ungesicherte LDAP-Verbindungen
- 636 für sichere LDAP-Verbindungen
- 3268 für Microsoft unsichere LDAP-Verbindungen
- 3269 für sichere Microsoft-LDAP-Verbindungen

LDAP-Verbindungen, die den Befehl startTLS verwenden, verwenden die Portnummer 389. Wenn die Portnummern 389 oder 3268 auf der Appliance konfiguriert sind, versucht sie, StartTLS zum Herstellen der Verbindung zu verwenden. Wenn eine andere Portnummer verwendet wird, verwenden Verbindungsversuche SSL/TLS. Wenn StartTLS oder SSL/TLS nicht verwendet werden können, schlägt die Verbindung fehl.

Bei der Konfiguration des LDAP-Servers muss die Groß-/Kleinschreibung der Buchstaben auf dem Server und auf der Appliance übereinstimmen. Wenn das Stammverzeichnis des LDAP-Servers angegeben wird, werden auch alle Unterverzeichnisse durchsucht, um das Benutzerattribut zu finden. In großen Verzeichnissen kann dies die Leistung beeinträchtigen. Aus diesem Grund empfiehlt Citrix, eine bestimmte Organisationseinheit (OU) zu verwenden.

In der folgenden Tabelle sind Beispiele für den definierten Basisnamen (DN) aufgeführt.

LDAP-Server	Basis-DN
Microsoft Active Directory	DC=Citrix, DC=local
Novell eDirectory	dc=Citrix, dc=net
IBM Directory Server	cn=users
Lotus Domino	OU=City, O=Citrix, C=US
Sun ONE Verzeichnis (ehemals iPlanet)	ou=People, dc=Citrix, dc=com

In der folgenden Tabelle sind Beispiele für den definierten Bind Name (DN) aufgeführt.

LDAP-Server	Binden DN
Microsoft Active Directory	CN=Administrator, CN=Users, DC=Citrix, DC=local
Novell eDirectory	cn=admin, dc=Citrix, dc=net
IBM Directory Server	LDAP_dn
Lotus Domino	CN=Notes Administrator, O=Citrix, C=US
Sun ONE Verzeichnis (ehemals iPlanet)	uid=admin, ou=Administrators, ou=TopologyManagement, o=NetscapeRoot

LDAP-Server	Binden DN
Microsoft Active Directory	CN=Administrator, CN=Users, DC=Citrix, DC=local
Novell eDirectory	cn=admin, dc=Citrix, dc=net
IBM Directory Server	LDAP_dn
Lotus Domino	CN=Notes Administrator, O=Citrix, C=US

LDAP-Server	Binden DN
Sun ONE Verzeichnis (ehemals iPlanet)	uid=admin, ou=Administrators, ou=TopologyManagement, o=NetscapeRoot

Konfigurieren der LDAP-Benutzerauthentifizierung über die CLI

Führen Sie die folgenden Schritte aus, um die LDAP-Authentifizierung für externe Benutzer zu konfigurieren

Konfigurieren der LDAP-Richtlinie

Führen Sie an der Eingabeaufforderung die folgenden Schritte aus:

Schritt 1: Erstellen Sie eine LDAP-Aktion.

```
add authentication ldapAction <name> { -serverIP <ip_addr|ipv6_addr|*> | {
 -serverName <string> } } >] [-authTimeout <positive_integer>] [-ldapBase
<string>] [-ldapBindDn <string>] { -ldapBindDnPassword } [-ldapLoginName <
string>] [-groupAttrName <string>] [-subAttributeName <string>]
```

Beispiel:

```
add authentication ldapAction ldap_act -serverIP <IP> -authTimeout 30 -
ldapBase ”CN=xxxxx,DC=xxxx,DC=xxx”-ldapBindDn ”CN=xxxxx,CN=xxxxx,DC=xxxx,DC
=xxx”-ldapBindDnPassword abcd -ldapLoginName sAMAccountName -groupattrName
memberOf -subAttributeName CN
```

Informationen zur Parameterbeschreibung finden Sie unter Referenz zu Authentifizierungs- und Berechtigungsbefehlen .

Schritt 2: Erstellen einer klassischen LDAP-Richtlinie.

```
add authentication ldapPolicy <name> <rule> [<reqAction>]
```

Beispiel:

```
add authentication ldappolicy ldap_pol_classic ns_true ldap_act
```

> **Hinweis:**
>
> Sie können mit einer klassischen oder einer erweiterten LDAP-Richtlinie konfigurieren, Citrix empfiehlt jedoch, eine erweiterte Authentifizierungsrichtlinie zu verwenden, da klassische Richtlinien ab der Version Citrix ADC 13.0 veraltet sind.

Schritt 3: Erstellen einer erweiterten LDAP-Richtlinie

```
add authentication Policy <name> <rule> [<reqAction>]
```


Beispiel:

```
add authentication policy ldap_pol_advance -rule true -action ldap_act
```

Schritt 4: Binden Sie die LDAP-Richtlinie an Systemglobal

Führen Sie an der Eingabeaufforderung die folgenden Schritte aus:

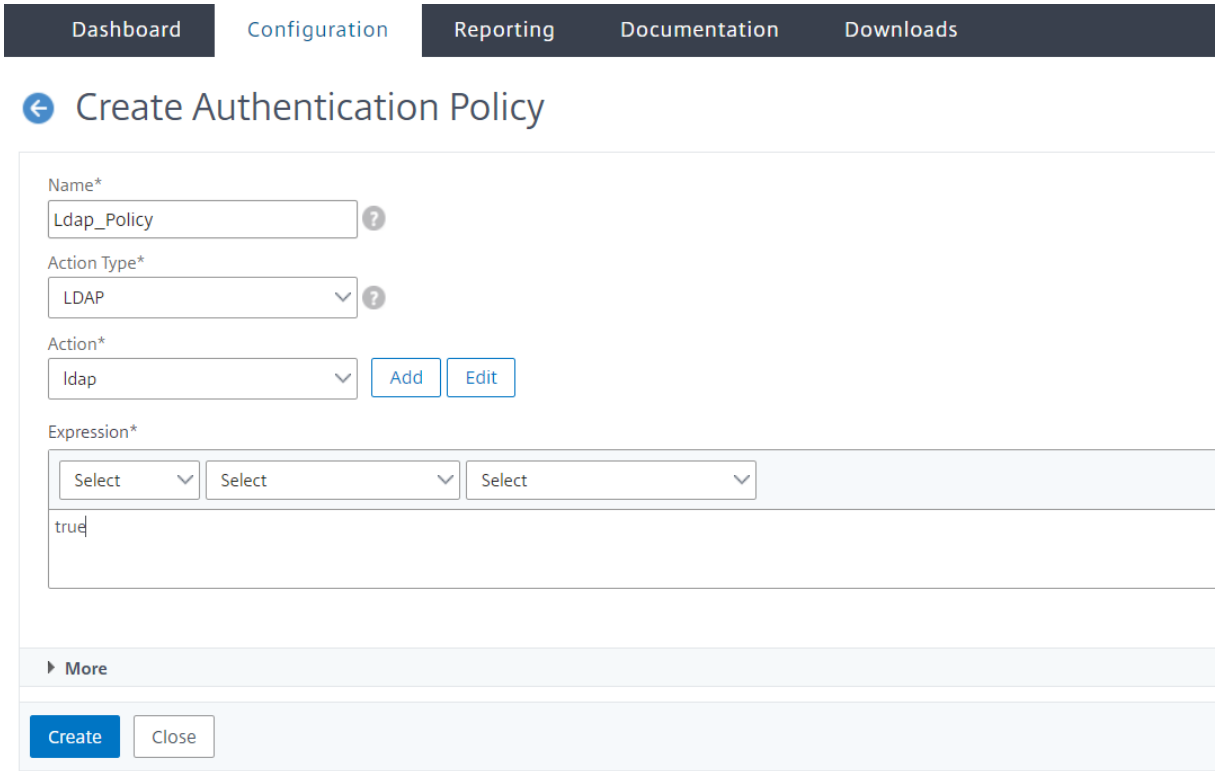
```
bind system global <policyName> [-priority <positive_integer]
```

Beispiel:

```
bind system global ldap_pol_advanced -priority 10
```

Konfigurieren der LDAP-Benutzerauthentifizierung mithilfe der Citrix ADC Benutzeroberfläche

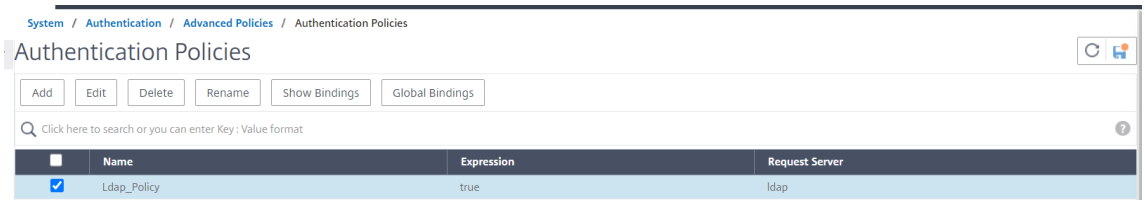
1. Navigieren Sie zu **System** > **Authentifizierung** > **Erweiterte Richtlinien** > **Richtlinie**.
2. Klicken Sie auf **Hinzufügen**, um eine Authentifizierungsrichtlinie vom Typ LDAP zu erstellen.
3. Klicken Sie auf **Erstellen** und **Schließen**.



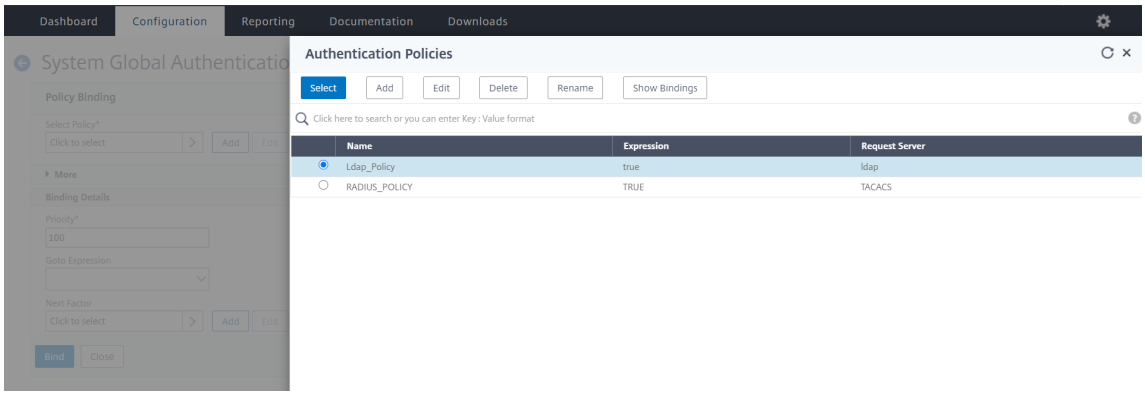
Binden einer Authentifizierungsrichtlinie an das System Global für die LDAP-Authentifizierung über die Citrix ADC GUI

1. Navigieren Sie zu **System** > **Authentifizierung** > **Erweiterte Richtlinien** > **Authentication PoliciesPolicy**.

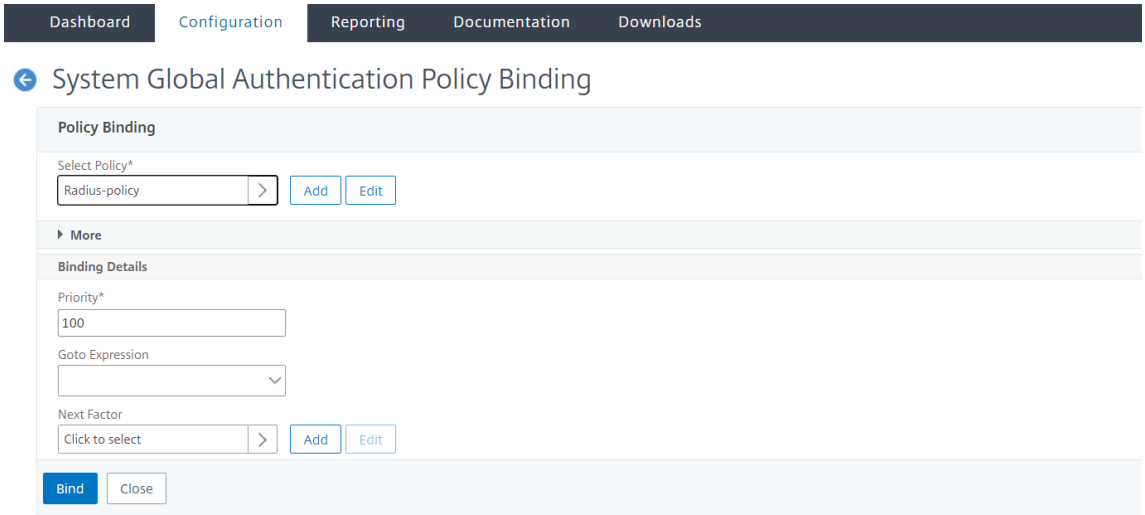
2. Klicken Sie im Detailbereich auf **Globale Bindungen**, um eine globale Systemauthentifizierungsrichtlinienbindung zu erstellen.
3. Klicken Sie auf **Globale Bindungen**.



4. Wählen Sie ein Authentifizierungsprofil aus.

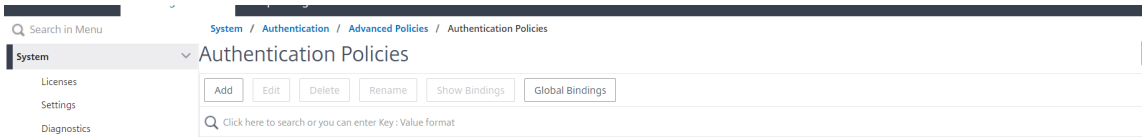


5. Wählen Sie die LDAP-Richtlinie aus.
6. Legen Sie auf der Seite **Bindung von System Global Authentication Policy** die folgenden Parameter fest:
   a) Wählen Sie Richtlinie aus.
   b) Verbindliche Angaben



7. Klicken Sie auf **Binden** und **Fertig**.

8. Klicken Sie auf **Globale Bindungen**, um die Richtlinie zu bestätigen, die an das globale System gebunden ist.



Bestimmen von Attributen im LDAP-Verzeichnis

Wenn Sie Hilfe bei der Bestimmung Ihrer LDAP-Verzeichnisattribute benötigen, können Sie diese einfach mit dem kostenlosen LDAP-Browser von Softerra nachschlagen.

Sie können den LDAP-Browser von der Softerra LDAP Administrator-Website unter herunterladen< `http://www.ldapbrowser.com`>. Legen Sie nach der Installation des Browsers die folgenden Attribute fest:

- Der Hostname oder die IP-Adresse Ihres LDAP-Servers.
- Der Port Ihres LDAP-Servers. Der Standardwert ist 389.
- Das Basis-DN-Feld kann leer gelassen werden.
- mit der vom LDAP-Browser bereitgestellten Informationen können Sie den Basis-DN ermitteln, der für die Registerkarte Authentifizierung erforderlich ist.
- Die Anonyme Bindung prüft, ob der LDAP-Server Benutzeranmeldeinformationen benötigt, damit der Browser eine Verbindung herstellen kann. Wenn der LDAP-Server Anmeldeinformationen benötigt, lassen Sie das Kontrollkästchen deaktiviert.

Nach Abschluss der Einstellungen zeigt der LDAP-Browser den Profilnamen im linken Fensterbereich an und stellt eine Verbindung zum LDAP-Server her.

Weitere Informationen finden Sie unter LDAP-Thema .

Schlüsselbasierte Authentifizierungsunterstützung für LDAP-Benutzer

Mit der schlüsselbasierten Authentifizierung können Sie jetzt die Liste der öffentlichen Schlüssel abrufen, die auf dem Benutzerobjekt im LDAP-Server über SSH gespeichert sind. Die Citrix ADC Appliance muss während des rollenbasierten Authentifizierungsprozesses (RBA) öffentliche SSH-Schlüssel vom LDAP-Server extrahieren. Der abgerufene öffentliche Schlüssel, der mit SSH kompatibel ist, muss es Ihnen ermöglichen, sich über die RBA-Methode anzumelden.

Ein neues Attribut “sshPublicKey” wird in den Befehlen “add authentication ldapAction” und “set authentication ldapAction” eingeführt. Wenn Sie dieses Attribut verwenden, können Sie die folgenden Vorteile erhalten:

- Kann den abgerufenen öffentlichen Schlüssel speichern, und die LDAP-Aktion verwendet dieses Attribut, um SSH-Schlüsselinformationen vom LDAP-Server abzurufen.

- Kann Attributnamen von bis zu 24 KB extrahieren.

> **Hinweis:**
>
> Der externe Authentifizierungsserver, wie LDAP, wird nur zum Abrufen von SSH-Schlüsselinformationen verwendet. Es wird nicht für Authentifizierungszwecke verwendet.

Es folgt ein Beispiel für den Ablauf von Ereignissen durch SSH:

- Der SSH-Daemon sendet eine AAA_AUTHENTICATE-Anforderung mit leerem Kennwortfeld an den Authentifizierungs-, Autorisierungs- und Überwachungsdaemon-Port.
- Wenn LDAP so konfiguriert ist, dass der öffentliche SSH-Schlüssel gespeichert wird, antwortet Authentifizierung, Autorisierung und Überwachung mit dem Attribut “SSHPublicKey” zusammen mit anderen Attributen.
- Der SSH-Daemon überprüft diese Schlüssel mit den Client-Schlüsseln.
- Der SSH-Daemon übergibt den Benutzernamen in der Anforderungsnutzlast, und Authentifizierung, Autorisierung und Überwachung gibt die für diesen Benutzer spezifischen Schlüssel zusammen mit generischen Schlüsseln zurück.

Um das Attribut sshPublicKey zu konfigurieren, geben Sie an der Eingabeaufforderung die folgenden Befehle ein:

- Mit Add-Operation können Sie SSHPublicKey Attribut hinzufügen, während LDAPAction Befehl konfigurieren.

```
add authentication ldapAction <name> { -serverIP <ip_addr|ipv6_addr
|*> | { -serverName <string> } } [-serverPort <port>] … [-Attribute1 <
string>] … [-Attribute16 <string>][-sshPublicKey <string>][-authentication
 off]<!--NeedCopy-->
```

- Mit set operation können Sie das Attribut SSHPublicKey zu einem bereits hinzugefügten LDAPAction Befehl konfigurieren.

```
set authentication ldapAction <name> [-sshPublicKey <string>][-authentication
 off]<!--NeedCopy-->
```

RADIUS-Authentifizierung (mit externen RADIUS-Servern)

Sie können die Citrix ADC Appliance so konfigurieren, dass der Benutzerzugriff mit einem oder mehreren RADIUS-Servern authentifiziert wird. Wenn Sie RSA SecurID-, SafeWord- oder Gemalto Protiva-Produkte verwenden, verwenden Sie einen RADIUS-Server.

Weitere Informationen zu RADIUS-Authentifizierungsrichtlinien finden Sie unter Thema RADIUS-Authentifizierungsrichtlinien .

Ihre Konfiguration erfordert möglicherweise die Verwendung einer Netzwerkzugriffsserver-IP-Adresse (NAS-IP) oder einer Netzwerkzugriffsserver-ID (NAS-ID). Wenn Sie die Appliance für die Verwendung

eines RADIUS-Authentifizierungsservers konfigurieren, verwenden Sie die folgenden Richtlinien:

- Wenn Sie die Verwendung der NAS-IP aktivieren, sendet die Appliance ihre konfigurierte IP-Adresse an den RADIUS-Server und nicht an die Quell-IP-Adresse, die beim Herstellen der RADIUS-Verbindung verwendet wird.
- Wenn Sie die NAS-ID konfigurieren, sendet die Appliance den Bezeichner an den RADIUS-Server. Wenn Sie die NAS-ID nicht konfigurieren, sendet die Appliance ihren Hostnamen an den RADIUS-Server.
- Wenn die NAS-IP-Adresse aktiviert ist, ignoriert die Appliance jede NAS-ID, die sie für die Kommunikation mit dem RADIUS-Server verwendet hat.

Konfigurieren Sie die RADIUS-Benutzerauthentifizierung mit der CLI

Führen Sie an der Eingabeaufforderung die folgenden Schritte aus:

Schritt 1: Erstellen Sie eine RADIUS-Aktion

```
add authentication radiusaction <name> -serverip <ip> -radkey <key> -
radVendorID <id> -radattributetype <value>
```

Wo, das Attribut “
`radVendorID` RADIUS-Händler-ID”, das für die Extraktion von RADIUS-
`radAttributeType` Attributtyp RADIUS, verwendet für die Extraktion von RADIUS-Gruppen.

Beispiel:

```
add authentication radiusaction RADserver531 rad_action -serverip 1.1.1.1 -
radkey key123 -radVendorID 66 -radattributetype 6
```

Schritt 2: Erstellen Sie eine klassische RADIUS-Richtlinie.

```
add authentication radiusPolicy <name> <rule> [<reqAction>]
```

Beispiel:

```
add authentication radiuspolicy radius_pol_classic ns_true radius_act
```

> **Hinweis:**
>
> Sie können mit einer klassischen oder einer erweiterten RADIUS-Richtlinie konfigurieren. Citrix empfiehlt Ihnen, die erweiterte Authentifizierungsrichtlinie zu verwenden, da klassische Richtlinien ab dem Release Citrix ADC 13.0 veraltet sind.

Schritt 3: Erstellen Sie eine erweiterte RADIUS-Richtlinie

```
add authentication policy <policyname> -rule true -action <radius action
name>
```

Beispiel:


```
add authentication policy rad_pol_advanced -rule true -action radserver531rad_action
```

Schritt 4: Binden Sie die RADIUS-Richtlinie an das globale System.

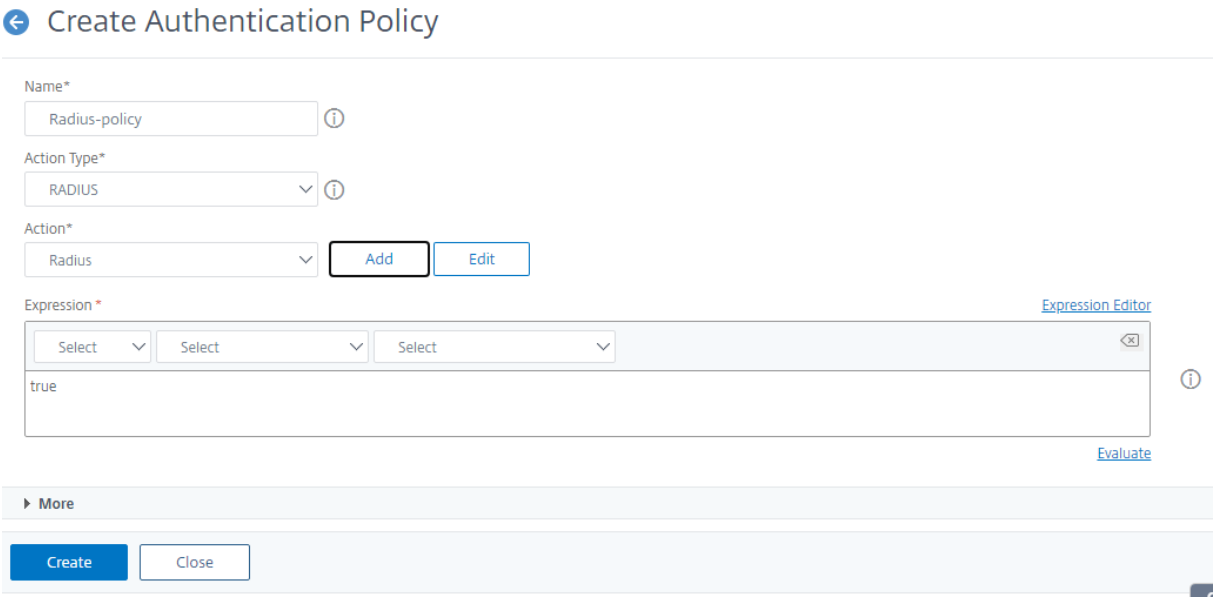
```
bind system global <policyName> -priority <positive_integer
```

Beispiel:

```
bind system global radius_pol_advanced -priority 10
```

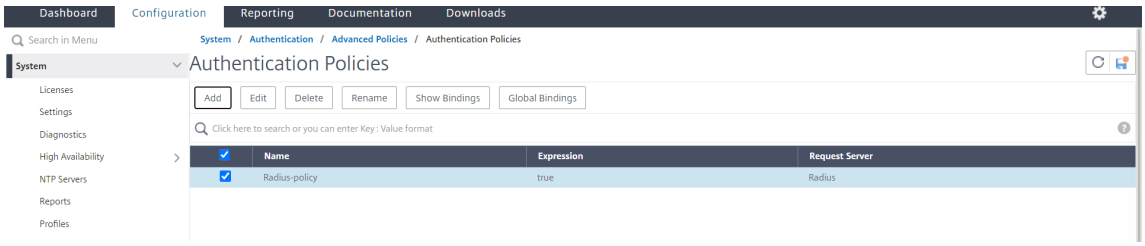
Konfigurieren Sie die RADIUS-Benutzerauthentifizierung mit der GUI

1. Navigieren Sie zu **System** > **Authentifizierung** > **Erweiterte Richtlinien** > **Richtlinie**.
2. Klicken Sie auf **Hinzufügen**, um eine Authentifizierungsrichtlinie vom Typ RADIUS zu erstellen.
3. Klicken Sie auf **Erstellen** und **Schließen**.



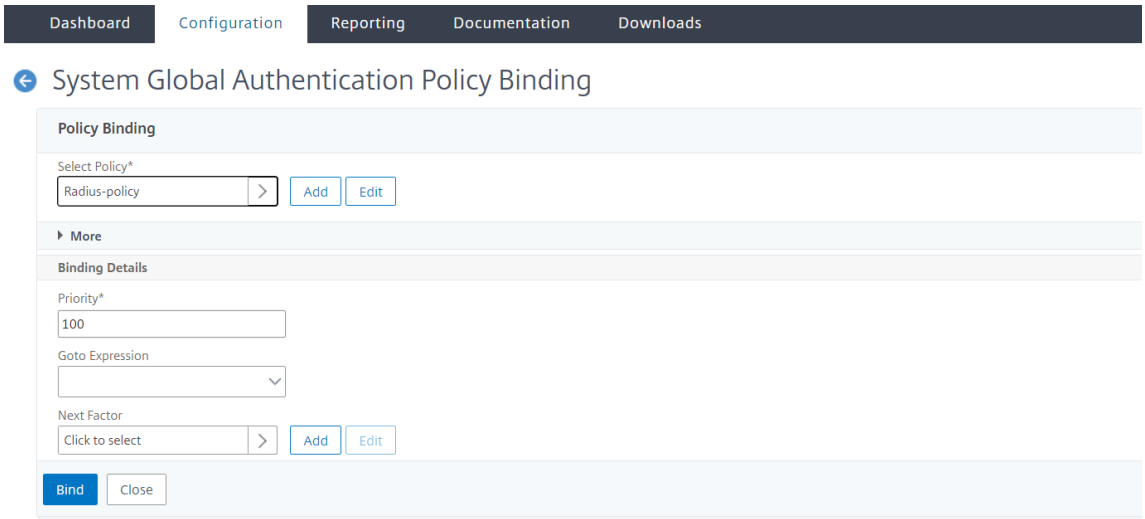
Binden Sie die Authentifizierungsrichtlinie für die RADIUS-Authentifizierung mit der GUI an das globale System

1. Navigieren Sie zu **System** > **Authentifizierung** > **Erweiterte Richtlinien** > **Richtlinie**.
2. Klicken Sie im Detailbereich auf **Globale Bindungen**, um eine globale Systemauthentifizierungsrichtlinienbindung zu erstellen.
3. Klicken Sie auf **Globale Bindungen**.

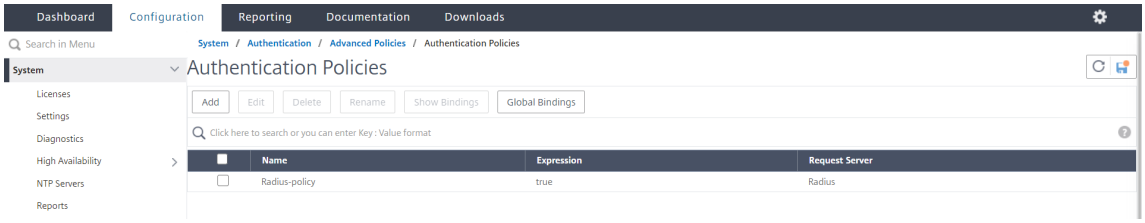


4. Wählen Sie RADIUS.
5. Legen Sie auf der Seite **Bindung von System Global Authentication Policy** die folgenden Parameter fest:

   a) Wählen Sie Richtlinie aus.
   b) Verbindliche Angaben.



6. Klicken Sie auf **Binden** und **Schließen** .
7. Klicken Sie auf **Globale Bindungen**, um die Richtlinie zu bestätigen, die an das globale System gebunden ist.



RADIUS-Benutzerauthentifizierungsprotokolle auswählen

Die Citrix ADC Appliance unterstützt RADIUS-Implementierungen, die für die Verwendung mehrerer Protokolle für die Benutzerauthentifizierung konfiguriert sind, einschließlich:

- Kennwortauthentifizierungsprotokoll
- Challenge-Handshake-Authentifizierungsprotokoll (CHAP)
- Microsoft Challenge-Handshake-Authentifizierungsprotokoll (MS-CHAP Version 1 und Version 2)

Wenn Ihre Bereitstellung für die Verwendung der RADIUS-Authentifizierung konfiguriert ist und Ihr RADIUS-Server mit einem Kennwortauthentifizierungsprotokoll konfiguriert ist. Sie können die Benutzerauthentifizierung verstärken, indem Sie dem RADIUS-Server ein starkes gemeinsames Geheimnis zuweisen. Starke gemeinsame Geheimnisse von RADIUS bestehen aus zufälligen Sequenzen von Groß- und Kleinbuchstaben, Zahlen und Satzzeichen und sind mindestens 22 Zeichen lang. Verwenden Sie nach Möglichkeit ein Programm zur Erzeugung von zufälligen Zeichen, um gemeinsam genutzte RADIUS-Geheimnisse zu ermitteln.

Um den RADIUS-Datenverkehr weiter zu schützen, weisen Sie jeder Appliance oder jedem virtuellen Server einen anderen gemeinsamen Schlüssel zu. Wenn Sie Clients auf dem RADIUS-Server definieren, können Sie jedem Client auch einen separaten gemeinsamen Schlüssel zuweisen. Außerdem müssen Sie jede Richtlinie, die die RADIUS-Authentifizierung verwendet, separat konfigurieren.

Konfigurieren der Extraktion von IP-Adres

Sie können die Appliance so konfigurieren, dass die IP-Adresse von einem RADIUS-Server extrahiert wird. Wenn sich ein Benutzer beim RADIUS-Server authentifiziert, gibt der Server eine eingerahmte IP-Adresse zurück, die dem Benutzer zugewiesen ist. Folgende Attribute sind für die IP-Adresseextraktion:

- Ermöglicht einem Remote-RADIUS-Server, eine IP-Adresse aus dem internen Netzwerk für einen an der Appliance angemeldeten Benutzer bereitzustellen.
- Ermöglicht die Konfiguration für jedes RADIUS-Attribut mit dem Typ IP-Adresse, einschließlich der Anbieter codiert.

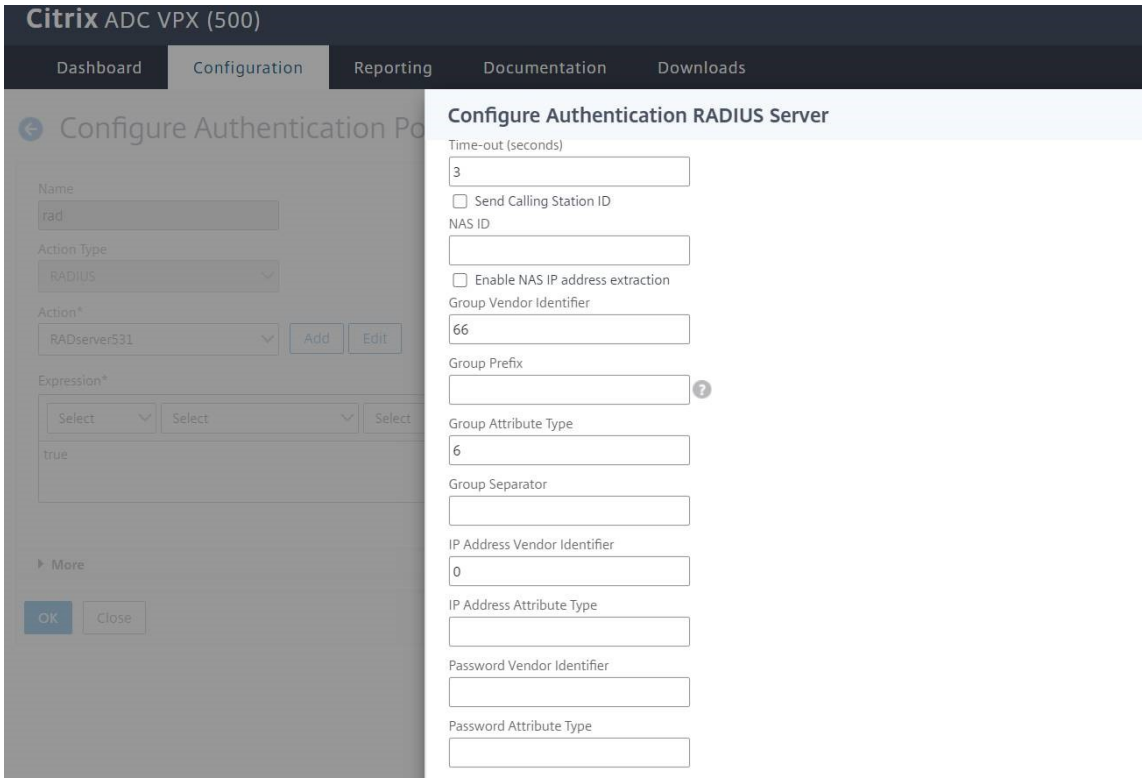
Wenn Sie den RADIUS-Server für die IP-Adressenextraktion konfigurieren, konfigurieren Sie die Hersteller-ID und den Attributtyp.

Die Herstellerbezeichnung ermöglicht es dem RADIUS-Server, dem Client eine IP-Adresse aus einem Pool von IP-Adressen zuzuweisen, die auf dem RADIUS-Server konfiguriert sind. Die Hersteller-ID und die Attribute werden verwendet, um die Zuordnung zwischen dem RADIUS-Client und dem RADIUS-Server herzustellen. Die Hersteller-ID ist das Attribut in der RADIUS-Antwort, das die IP-Adresse des internen Netzwerks bereitstellt. Der Wert Null gibt an, dass das Attribut nicht herstellercodiert ist. Der Attributtyp ist das Remote-IP-Adressattribut in einer RADIUS-Antwort. Der Mindestwert ist eins und der Maximalwert 255.

Eine übliche Konfiguration besteht darin, die *gerahmte IP-Adresse* des **RADIUS-Attributs** Die Lieferanten-ID ist auf Null oder wird nicht angegeben. Der Attributtyp ist auf acht festgelegt.

Gruppenextraktion für RADIUS mit der GUI

1. Navigieren Sie zu **System** > **Authentifizierung** > **Erweiterte Richtlinien** > **Radius**, und wählen Sie eine Richtlinie aus.
2. Wählen oder erstellen Sie eine RADIUS-Richtlinie.
3. Legen Sie auf der Seite **“Authentication RADIUS-Server konfigurieren** “ die folgenden Parameter fest.
   a) **Gruppen-Anbieter-ID**
   b) **Attributtyp der Gruppe**
4. Klicken Sie auf **OK** und **schließen**.



TACACS+-Authentifizierung (mit externen TACACS+ Servern)

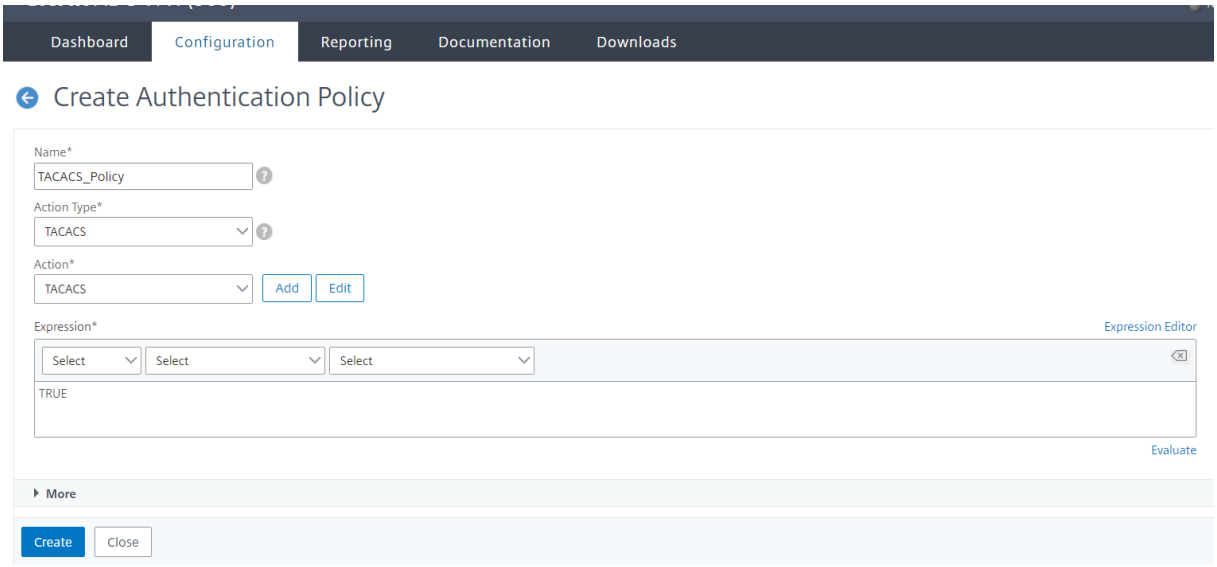
> **Wichtig**
>
> - Citrix empfiehlt, keine TACACS-bezogenen Konfigurationen zu ändern, wenn Sie einen Befehl “clear ns config” ausführen.
> - Die TACACS-bezogene Konfiguration im Zusammenhang mit erweiterten Richtlinien wird gelöscht und erneut angewendet, wenn der `RBAconfig` Parameter im Befehl “clear ns config” für erweiterte Richtlinien auf NEIN gesetzt ist.

Sie können einen TACACS+-Server für die Authentifizierung konfigurieren. Ähnlich wie die RADIUS-Authentifizierung verwendet TACACS+ einen geheimen Schlüssel, eine IP-Adresse und die Portnummer. Die Standardportnummer ist 49. Um die Appliance für die Verwendung eines TACACS+-Servers zu konfigurieren, geben Sie die Server-IP-Adresse und den TACACS+-Schlüssel ein. Sie müssen den Port nur angeben, wenn die verwendete Serverportnummer etwas anderes als die Standardportnummer 49 ist.

Weitere Informationen finden Sie unter TACACS-Authentifizierung.

Konfigurieren Sie die TACACS+-Authentifizierung mit der GUI

1. Navigieren Sie zu **System** > **Authentifizierung** > **Erweiterte Richtlinien** > **Richtlinie**.
2. Klicken Sie auf **Hinzufügen**, um eine Authentifizierungsrichtlinie des Typs TACACS zu erstellen.
3. Klicken Sie auf **Erstellen** und **Schließen**.



Nachdem die TACACS+-Servereinstellungen auf der Appliance konfiguriert wurden, binden Sie die Richtlinie an die globale Systemeinheit.

Binden von Authentifizierungsrichtlinien an die globale Systementität über die CLI

Wenn die Authentifizierungsrichtlinien konfiguriert sind, binden Sie die Richtlinien an die globale Systemeinheit.

Führen Sie an der Eingabeaufforderung die folgenden Schritte aus:

```
bind system global <policyName> [-priority <positive_integer>]
```

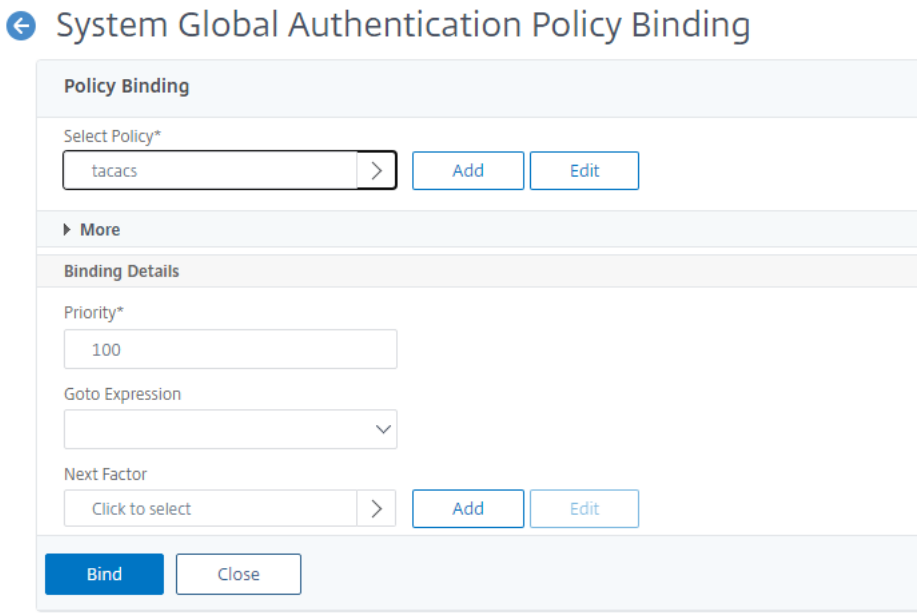
Beispiel:

```
bind system global pol_classic -priority 10
```


Lesen Sie auch den Citrix-Artikel CTX113820, um mehr über externe Authentifizierung mit TACACS zu erfahren.

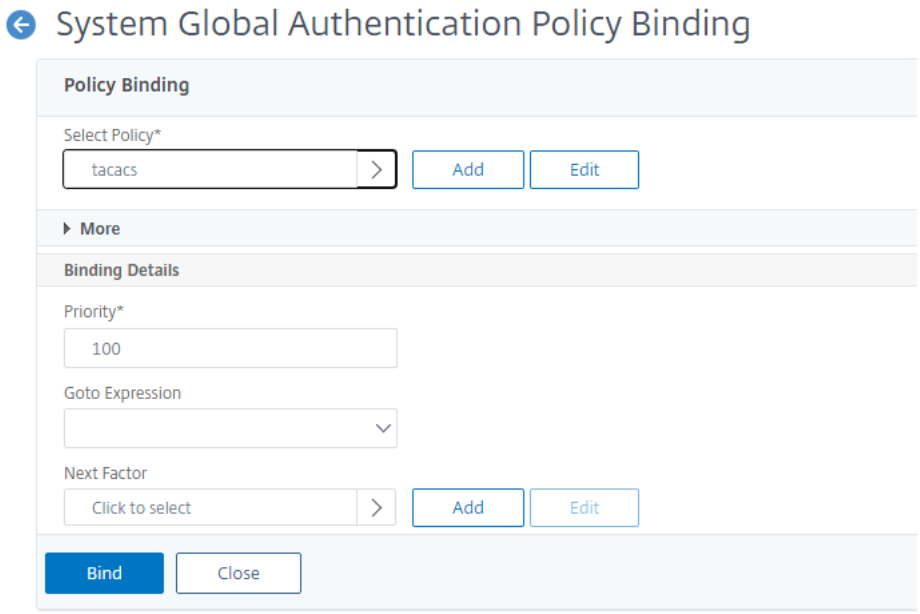
Binden Sie Authentifizierungsrichtlinien an die globale Systemeinheit über die GUI

1. Navigieren Sie zu **System** > **Authentifizierung** > **Erweiterte Richtlinien** > **Authentifizierungsrichtlinien > Richtlinie**.
2. Klicken Sie im Detailbereich auf **Globale Bindungen**, um eine globale Systemauthentifizierungsrichtlinienbindung zu erstellen.
3. Klicken Sie auf **Globale Bindungen**.

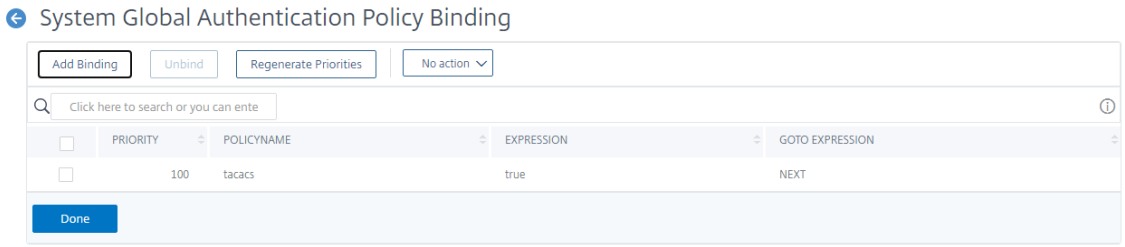


4. Wählen Sie die TACACS-Richtlinie aus.
5. Legen Sie auf der Seite System Global Authentication Policy Binding die folgenden Parameter fest:

   a) Wählen Sie Richtlinie aus.
   b) Verbindliche Angaben



6. Klicken Sie auf **Binden** und **Schließen** .
7. Klicken Sie auf **Globale Bindungen**, um die Richtlinie zu bestätigen, die an das globale System gebunden ist.



Weitere Informationen zur Extraktion der TACACS-Gruppe finden Sie im Citrix Artikel CTX220024.

Anzahl der erfolglosen Anmeldeversuche für externe Benutzer anzeigen

Die Citrix ADC Appliance zeigt dem externen Benutzer die Anzahl der ungültigen Anmeldeversuche an, wenn Sie mindestens eine nicht erfolgreiche Anmeldung versuchen, bevor Sie sich erfolgreich bei der Citrix ADC Verwaltungskonsole anmelden.

> **Hinweis:**
>
> Derzeit unterstützt Citrix nur die interaktive Tastaturauthentifizierung für externe Benutzer, wobei der Parameter “PersistentLoginAttempts” im Systemparameter aktiviert ist.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set aaa parameter -maxloginAttempts <value> -failedLoginTimeout <value> -
```



```
persistentLoginAttempts (ENABLED | DISABLED )]
```

Beispiel:

```
set aaa parameter -maxloginAttempts 5 -failedLoginTimeout 4 -persistentLoginAttempts
 ENABLED
```

```
Following msg will be seen to external user when he tries 1 invalid
    login attempt before successfully login to the ADC management access
    .

Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.
###############################################################################

#

    #
#        WARNING: Access to this system is for authorized users only
            #
#         Disconnect IMMEDIATELY if you are not an authorized user!
             #
#

    #
###############################################################################


WARNING! The remote SSH server rejected X11 forwarding request.
Last login: Mon Aug 24 17:09:00 2020 from 10.10.10.10

The number of unsuccessful login attempts since the last successful
    login : 1
Done
>
The number of unsuccessful login attempts since the last successful
    login : 1
Done
>
<!--NeedCopy-->
```


Schlüsselbasierte SSH-Authentifizierung für lokale Systembenutzer

October 5, 2021

Um einen sicheren Benutzerzugriff für die Citrix ADC Appliance zu haben, können Sie die Public Key-Authentifizierung des SSH-Servers haben. Die schlüsselbasierte SSH-Authentifizierung wird aus folgenden Gründen gegenüber der herkömmlichen Benutzernamen- oder kennwortbasierten Authentifizierung bevorzugt:

- Bietet eine bessere kryptografische Stärke als Benutzerpasswörter.
- Eliminiert die Notwendigkeit, sich an komplizierte Kennwörter zu erinnern, und verhindert Schulter-Surf-Angriffe, die bei Verwendung von Kennwörtern möglich sind.
- Bietet eine kennwortlose Anmeldung, um Automatisierungsszenarien sicherer zu machen.

Citrix ADC unterstützt die schlüsselbasierte SSH-Authentifizierung durch Anwendung des Public und Private Key-Konzepts. Die schlüsselbasierte SSH-Authentifizierung in Citrix ADC kann entweder für einen bestimmten Benutzer oder für alle lokalen Benutzer aktiviert werden.

> **Hinweis:**
>
> Die Funktion wird nur für lokale Benutzer von Citrix ADC unterstützt und wird nicht für externe Benutzer unterstützt.

Schlüsselbasierte SSH-Authentifizierung für lokale Systembenutzer

In einer Citrix ADC Appliance kann ein Administrator die schlüsselbasierte SSH-Authentifizierung für einen sicheren Systemzugriff einrichten. Wenn sich ein Benutzer mit einem privaten Schlüssel beim Citrix ADC anmeldet, authentifiziert das System den Benutzer mit dem auf der Appliance konfigurierten öffentlichen Schlüssel.

Konfigurieren der SSH-Schlüsselauthentifizierung für die Benutzer des lokalen Citrix ADC -Systems mithilfe von CLI

Die folgende Konfiguration hilft Ihnen bei der Konfiguration der schlüsselbasierten Authentifizierung für Benutzer des lokalen Citrix ADC-Systems.

1. Melden Sie sich mit Administratoranmeldeinformationen bei einer Citrix ADC Appliance an.
2. Standardmäßig greift Ihre `sshd_config` Datei auf diesen Pfad zu: **authorizedKeysFile /nsconfig/ssh/authorized_keys**.
3. Hängen Sie den öffentlichen Schlüssel an die authorized_keys-Datei an: **/nsconfig/ssh/authorized_keys**. Der Dateipfad für `sshd_config` ist `/etc/sshd_config`.
4. Kopieren Sie die `sshd_config` Datei in, `/nsconfig` um sicherzustellen, dass die Änderungen auch nach dem Neustart der Appliance bestehen bleiben.

5. Sie können den folgenden Befehl verwenden, um den `sshd` Prozess neu zu starten.

```
    kill -HUP `cat /var/run/sshd.pid`
<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn die Datei authorized_keys nicht verfügbar ist, müssen Sie zuerst eine erstellen und dann den öffentlichen Schlüssel anhängen. **Stellen Sie sicher, dass die Datei die folgenden Berechtigungen für die autorisierten_keys hat**.
>
> `root@Citrix ADC## chmod 0644 authorized_keys`

```
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993,
    1994
The Regents of the University of California. All rights reserved.
root@ns# cd /nsconfig/ssh
root@ns# vi authorized_keys
### Add public keys in authorized_keys file
<!--NeedCopy-->
```

Benutzerspezifische SSH-Schlüssel-basierte Authentifizierung für lokale Systembenutzer

In einer Citrix ADC Appliance kann ein Administrator jetzt eine benutzerspezifische SSH-Schlüssel-basierte Authentifizierung für einen gesicherten Systemzugriff einrichten. Der Administrator muss zuerst die `Authorizedkeysfile` Option in der `sshd_config` Datei konfigurieren und dann den öffentlichen Schlüssel für einen Systembenutzer in der `authorized_keys` Datei hinzufügen.

> **Hinweis:**
>
> Wenn die Datei authorized_keys für einen Benutzer nicht verfügbar ist, muss der Administrator zuerst einen erstellen und dann den öffentlichen Schlüssel hinzufügen.

Konfigurieren Sie die benutzerspezifische SSH-Schlüssel-basierte Authentifizierung mit der CLI

Das folgende Verfahren hilft Ihnen bei der Konfiguration der benutzerspezifischen SSH-Schlüsselauthentifizierung für Benutzer des lokalen Citrix ADC-Systems.

1. Melden Sie sich mit Administratoranmeldeinformationen bei einer Citrix ADC Appliance an.

2. Greifen Sie an der Shell-Eingabeaufforderung auf die `sshd_config` Datei zu und fügen Sie die folgende Konfigurationszeile hinzu:

   `AuthorizedKeysFile ~/.ssh/authorized_keys`

   > **Hinweis:**
   >
   > Das ~ ist das Home-Verzeichnis und unterscheidet sich für verschiedene Benutzer. Es erweitert sich auf das andere Home-Verzeichnis.

3. Ändern Sie das Verzeichnis in den Systembenutzerordner und fügen Sie die öffentlichen Schlüssel in der `authorized_keys` Datei hinzu.

   `/var/pubkey/<username>/.ssh/authorized_keys`

Wenn Sie die früheren Schritte abgeschlossen haben, starten Sie den `sshd` Prozess auf Ihrer Appliance mit dem folgenden Befehl neu:

```
    kill -HUP `cat /var/run/sshd.pid`

<!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn die Datei authorized_keys nicht verfügbar ist, müssen Sie zuerst eine erstellen und dann den öffentlichen Schlüssel hinzufügen.

```
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993,
    1994
The Regents of the University of California. All rights reserved.
root@ns# cd /var/pubkey/<username>/
root@ns# ls
.ssh
root@ns# cd .ssh
root@ns# vi authorized_keys
### Add public keys in authorized_keys file

<!--NeedCopy-->
```

Lesen Sie auch den Citrix Artikel CTX109011, um zu erfahren, wie sicherer SSH-Zugriff auf Citrix ADC Appliance funktioniert.

Zwei-Faktor-Authentifizierung für Systembenutzer und externe Benutzer

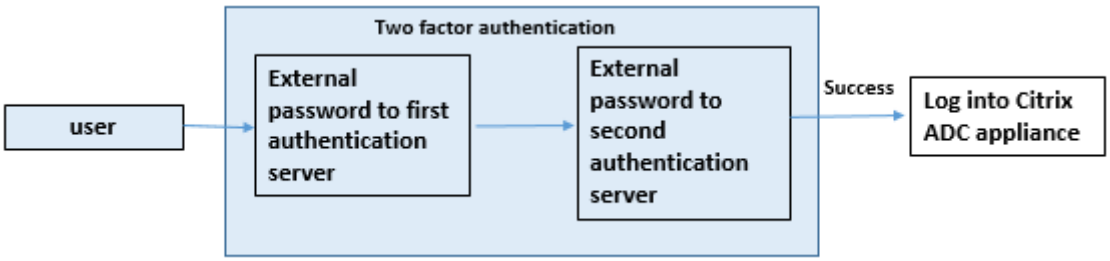
February 24, 2022

Die Zwei-Faktor-Authentifizierung ist ein Sicherheitsmechanismus, bei dem eine Citrix ADC Appliance einen Systembenutzer auf zwei Authentifikatorstufen authentifiziert. Die Appliance gewährt dem Benutzer erst nach erfolgreicher Validierung von Kennwörtern durch beide Authentifizierungsstufen Zugriff. Wenn ein Benutzer lokal authentifiziert wird, muss das Benutzerprofil in der Citrix ADC Datenbank erstellt werden. Wenn der Benutzer extern authentifiziert wird, müssen der Benutzername und das Kennwort mit der Benutzeridentität übereinstimmen, die auf dem externen Authentifizierungsserver registriert ist.

> **Hinweis**
>
> Die Zwei-Faktor-Authentifizierungsfunktion funktioniert nur ab Citrix ADC 12.1 Build 51.16.

So funktioniert Zwei-Faktor-Authentifizierung

Betrachten Sie einen Benutzer, der versucht, sich bei einer Citrix ADC Appliance anzumelden. Der angeforderte Anwendungsserver sendet den Benutzernamen und das Kennwort an den ersten externen Authentifizierungsserver (RADIUS, TACACS, LDAP oder AD). Sobald der Benutzername und das Kennwort überprüft wurden, wird der Benutzer zur Eingabe einer zweiten Authentifizierungsebene aufgefordert. Der Benutzer kann nun das zweite Kennwort angeben. Nur wenn beide Kennwörter korrekt sind, darf der Benutzer auf die Citrix ADC Appliance zugreifen. Das folgende Diagramm veranschaulicht, wie die Zwei-Faktor-Authentifizierung für eine Citrix ADC Appliance funktioniert.



Im Folgenden sind die verschiedenen Anwendungsfälle für die Konfiguration der Zwei-Faktor-Authentifizierung für externe und Systembenutzer.

Sie können die Zwei-Faktor-Authentifizierung auf einer Citrix ADC Appliance auf verschiedene Arten konfigurieren. Im Folgenden finden Sie die verschiedenen Konfigurationsszenarien für die Zwei-Faktor-Authentifizierung auf einer Citrix ADC Appliance.

1. Zwei-Faktor-Authentifizierung (2FA) für Citrix ADC, GUI, CLI, API und SSH.

2. Externe Authentifizierung aktiviert und lokale Authentifizierung für Systembenutzer deaktiviert.
3. Externe Authentifizierung mit richtlinienbasierter lokaler Authentifizierung für Systembenutzer aktiviert.
4. Externe Authentifizierung deaktiviert für Systembenutzer mit aktivierter lokaler Authentifizierung.
5. Externe Authentifizierung aktiviert und lokale Authentifizierung für Systembenutzer aktiviert.
6. Externe Authentifizierung für ausgewählte LDAP-Benutzer aktiviert

Anwendungsfall 1: Zwei-Faktor-Authentifizierung (2FA) über Citrix ADC -, GUI-, CLI-, API- und SSH-Schnittstellen

Die Zwei-Faktor-Authentifizierung ist für alle Citrix ADC Verwaltungszugriffe für GUI, API und SSH aktiviert und verfügbar.

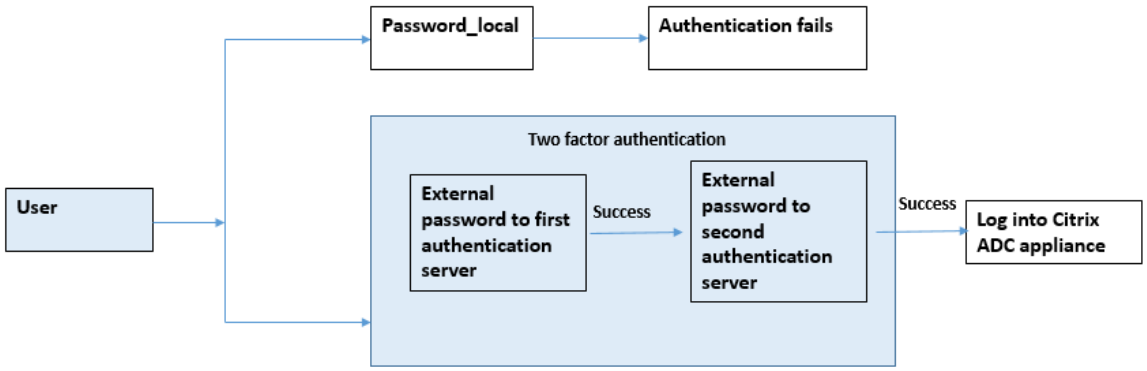
Anwendungsfall 2: Zwei-Faktor-Authentifizierung wird auf externen Authentifizierungsservern wie LDAP, RADIUS, Active Directory und TACACS unterstützt

Sie können die Zwei-Faktor-Authentifizierung auf den folgenden externen Authentifizierungsservern für die Benutzerauthentifizierung der ersten und zweiten Ebene konfigurieren.

- RADIUS
- LDAP
- Active Directory
- TACACS

Anwendungsfall 3: Externe Authentifizierung aktiviert und lokale Authentifizierung für Systembenutzer deaktiviert

Sie beginnen den Authentifizierungsprozess, indem Sie die Option für die externe Authentifizierung aktivieren und die lokale Authentifizierung für Systembenutzer deaktivieren.



Führen Sie die folgenden Schritte durch, indem Sie die Befehlszeilenschnittstelle verwenden:

1. Hinzufügen von Authentifizierungsaktion für LDAP-Richtlinie
2. Hinzufügen der Authentifizierungsrichtlinie für LDAP-Richtlinie
3. Hinzufügen der Authentifizierungsaktion für die RADIUS-Richtlinie
4. Hinzufügen der Authentifizierungsrichtlinie für die RADIUS-Richtlinie
5. Authentifizierungsanmeldeschema hinzufügen
6. Hinzufügen und Binden der Authentifizierungsrichtlinienbezeichnung zum RADIUS-Server
7. Globale Systemauthentifizierung für LDAP-Richtlinie binden
8. Deaktivieren der lokalen Authentifizierung im Systemparameter

Authentifizierungsaktion für LDAP-Server hinzufügen (Authentifizierung der ersten Ebene)

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname <
loginname> -groupattrname <grp attribute name> -subAttributename <string>-
ssoNameAttribute <string>
```

Beispiel:

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Hinzufügen der Authentifizierungsrichtlinie für LDAP-Server (Authentifizierung der ersten Ebene)

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication policy <ldap policy name> -rule true -action <ldap
action name>
```

Beispiel:

```
add authentication policy pol1 -rule true -action ldapact1
```

Authentifizierungsaktion für RADIUS-Server hinzufügen (Authentifizierung auf der zweiten Ebene)

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type>
```

Beispiel:


```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```

Hinzufügen der Authentifizierungsrichtlinie für RADIUS-Server (Authentifizierung auf der zweiten Ebene)

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication policy <radius policy name> -rule true -action <rad
action name>
```

Beispiel:

```
add authentication policy radpol11 -rule true -action radact1
```

Authentifizierungsanmeldeschema hinzufügen

Sie können das Anmeldeschema SingleAuth.xml für Systembenutzer verwenden, um das zweite Kennwort für die Citrix ADC Appliance anzugeben. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication loginSchema <login schema name> -authenticationSchema
LoginSchema/SingleAuth.xml
```

Beispiel:

```
add authentication loginSchema radschema -authenticationSchema LoginSchema/
SingleAuth.xml
```

Hinzufügen und Binden der Authentifizierungsrichtlinienbezeichnung zum RADIUS-Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
```

```
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Beispiel:

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
```

```
bind authentication policylabel label1 -policyName radpol11 -priority 1
```


Bind Authentication System global für LDAP-Richtlinie

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind system global ldappolicy -priority <priority> -nextFactor <policy
label name>
```

Beispiel:

```
bind system global pol11 -priority 1 -nextFactor label1
```

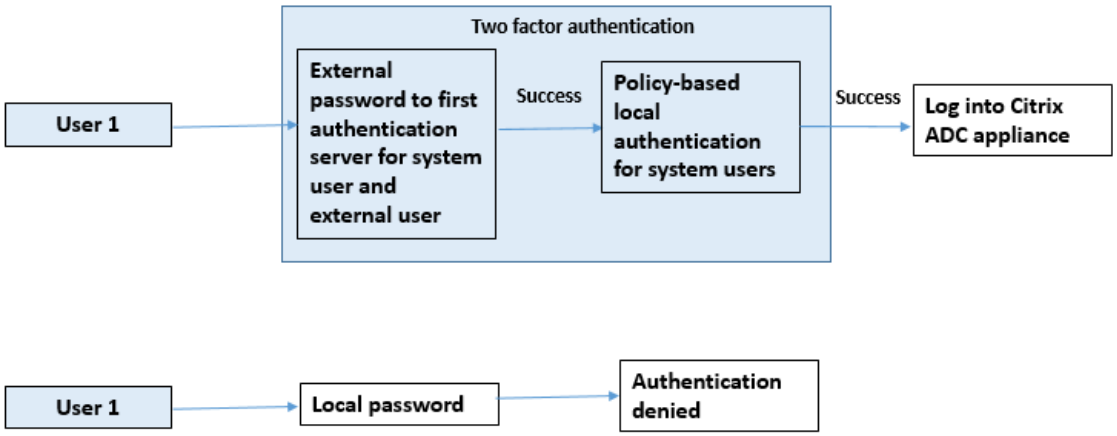
Deaktivieren der lokalen Authentifizierung im Systemparameter

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set system parameter -localauth disabled
```

Anwendungsfall 4: Externe Authentifizierung für Systembenutzer mit angehängter lokaler Authentifizierungsrichtlinie aktiviert

In diesem Szenario ist der Benutzer berechtigt, sich bei der Appliance mit Zwei-Faktor-Authentifizierung mit Auswertung der lokalen Authentifizierungsrichtlinie auf der zweiten Ebene der Benutzeridentifikation anzumelden.



Führen Sie die folgenden Schritte mit der Befehlszeilenschnittstelle aus.

1. Authentifizierungsaktion für LDAP-Server hinzufügen
2. Hinzufügen der Authentifizierungsrichtlinie für LDAP-Richtlinie
3. Lokale Authentifizierungsrichtlinie hinzufügen
4. Authentifizierungsrichtlinienlabel hinzufügen
5. LDAP-Richtlinie als systemglobal binden
6. Deaktivieren der lokalen Authentifizierung im Systemparameter

Authentifizierungsaktion für LDAP-Server hinzufügen (Authentifizierung der ersten Ebene)

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname <
loginname> -groupattrname <grp attribute name> -subAttributename <string>-
ssoNameAttribute <string>
```

Beispiel:

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name -ssoNameAttribute name
```

Hinzufügen der Authentifizierungsrichtlinie für LDAP-Server (Authentifizierung der ersten Ebene)

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication policy <ldap policy name> -rule true -action <ldap
action name>
```

Beispiel:

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Lokale Authentifizierungsrichtlinie für Systembenutzer hinzufügen (Authentifizierung auf der zweiten Ebene)

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type
```

Beispiel:

```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```

Hinzufügen und Binden der Authentifizierungsrichtlinienbezeichnung

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Beispiel:

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
bind authentication policylabel label1 -policyName radpol11 -priority 1 -
gotoPriorityExpression NEXT
```

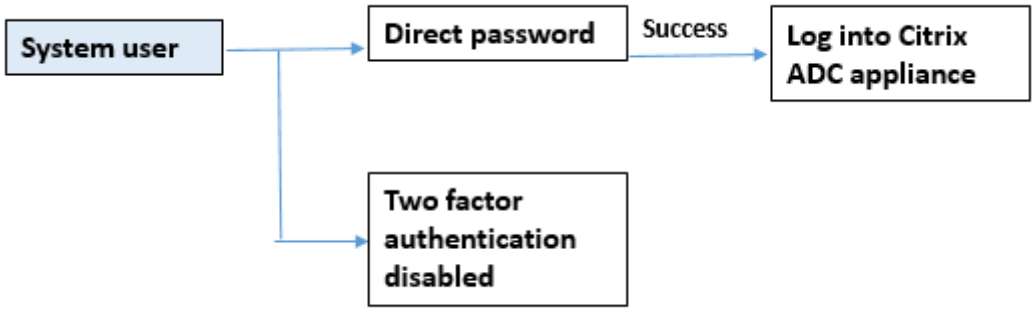
Deaktivieren der lokalen Authentifizierung im Systemparameter

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set system parameter -localauth disabled
```

Anwendungsfall 5: Externe Authentifizierung deaktiviert und lokale Authentifizierung für Systembenutzer aktiviert

Wenn der Benutzer ExternalAuth deaktiviert hat, zeigt dies an, dass der Benutzer nicht auf dem Authentifizierungsserver vorhanden ist. Der Benutzer wird nicht beim externen Authentifizierungsserver authentifiziert, selbst wenn ein Benutzer mit demselben Benutzernamen auf dem externen authentifizierten Server vorhanden ist. Der Benutzer wird lokal authentifiziert.



So aktivieren Sie das Kennwort des Systembenutzers und deaktivieren die externe Authentifizierung

Geben Sie an der Eingabeaufforderung Folgendes ein:

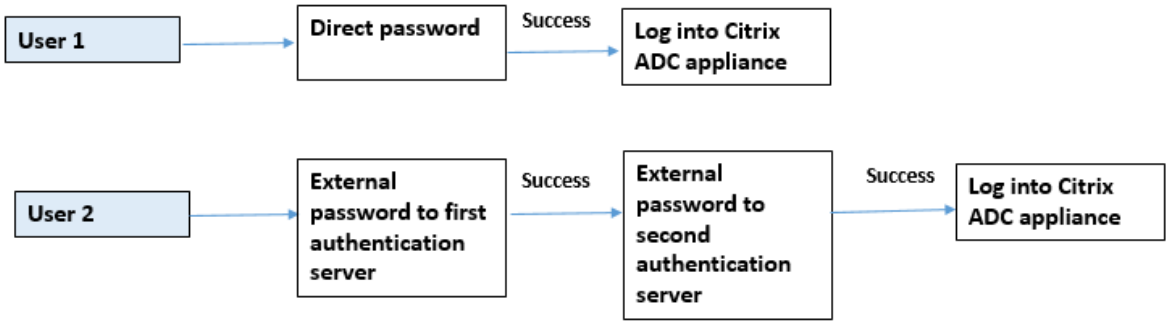
```
add system user <name> <password> -externalAuth DISABLED
```

Beispiel:


```
add system user user1 password1 -externalAuth DISABLED
```

Anwendungsfall 6: Externe Authentifizierung aktiviert und lokale Authentifizierung für Systembenutzer aktiviert

So konfigurieren Sie die Appliance für die Authentifizierung von Systembenutzern mithilfe eines lokalen Kennworts. Wenn diese Authentifizierung fehlschlägt, wird der Benutzer mit einem externen Authentifizierungskennwort auf den externen Authentifizierungsservern auf zwei Ebenen authentifiziert.



Konfigurieren Sie die folgenden Schritte mit der CLI.

1. Authentifizierungsaktion für LDAP-Server hinzufügen
2. Hinzufügen der Authentifizierungsrichtlinie für LDAP-Richtlinie
3. Hinzufügen der Authentifizierungsaktion für die RADIUS-Richtlinie
4. Hinzufügen der Authentifizierungsrichtlinie für die RADIUS-Richtlinie
5. Authentifizierungsanmeldeschema hinzufügen
6. Authentifizierungsrichtlinienlabel hinzufügen
7. Authentifizierungsrichtlinienlabel für Anmeldeschema binden
8. Globales Authentifizierungssystem für RADIUS-Richtlinie binden
9. Bind Authentication System global für LDAP-Richtlinie

Authentifizierungsaktion für LDAP-Server hinzufügen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname
 <loginname> -groupattrname <grp attribute name> -subAttributename <>-
ssoNameAttribute <>
```

Beispiel:


```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Hinzufügen der Authentifizierungsrichtlinie für LDAP-Richtlinie

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication policy <policy name> --rule true -action <ldap action
name>
```

Beispiel:

```
add authentication policy pol1 -rule true -action ldapact1
```

Hinzufügen von Authentifizierungsaktion für RADIUS-Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type>
```

Beispiel:

```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```

Erweiterte Authentifizierungsrichtlinie für RADIUS-Server hinzufügen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication policy <policy name> -rule true -action <rad action name
>
```

Beispiel:

```
add authentication policy radpol11 -rule true -action radact1
```

Authentifizierungsanmeldeschema hinzufügen

Sie können das Anmeldeschema SingleAuth.xml verwenden, um die Anmeldeseite anzuzeigen und den Systembenutzer bei der Authentifizierung der zweiten Ebene zu authentifizieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication loginSchema <name> -authenticationSchema <string>
```

Beispiel:


```
add authentication loginSchema radschema -authenticationSchema LoginSchema/
SingleAuth.xml
```

Hinzufügen und Binden der Authentifizierungsrichtlinie zur RADIUS-Authentifizierungsrichtlinie für die Benutzeranmeldung

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
```

Beispiel:

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Beispiel:

```
bind authentication policylabel label1 -policyName rad pol11 -priority 1
```

Authentifizierungsrichtlinie global binden

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind system global [<policyName> [-priority <positive_integer>] [-nextFactor
 <string>] [-gotoPriorityExpression <expression>]]
```

Beispiel:

```
bind system global radpol11 -priority 1 -nextFactor label11
```

Anwendungsfall 7: Externe Authentifizierung ist nur für ausgewählte externe Benutzer aktiviert

Konfiguration selektiver externer Benutzer mit Zwei-Faktor-Authentifizierung gemäß dem in der LDAP-Aktion konfigurierten Suchfilter, während andere Systembenutzer mit Einzelfaktorauthentifizierung authentifiziert werden.

Konfigurieren Sie die folgenden Schritte mit der CLI.

1. Authentifizierungsaktion für LDAP-Server hinzufügen
2. Hinzufügen der Authentifizierungsrichtlinie für LDAP-Richtlinie
3. Hinzufügen der Authentifizierungsaktion für die RADIUS-Richtlinie
4. Hinzufügen der Authentifizierungsrichtlinie für die RADIUS-Richtlinie

5. Authentifizierungsanmeldeschema hinzufügen
6. Authentifizierungsrichtlinienlabel hinzufügen
7. Authentifizierungsrichtlinienlabel für Anmeldeschema binden
8. Globales Authentifizierungssystem für RADIUS-Richtlinie binden

Authentifizierungsaktion für LDAP-Server hinzufügen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname
 <loginname> -groupattrname <grp attribute name> -subAttributename <>-
ssoNameAttribute <>
```

Beispiel:

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name -ssoNameAttribute name
```

Hinzufügen der Authentifizierungsrichtlinie für LDAP-Richtlinie

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication policy <policy name> --rule true -action <ldap action
name>
```

Beispiel:

```
add authentication policy pol1 -rule true -action ldapact1
```

Hinzufügen von Authentifizierungsaktion für RADIUS-Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication radiusaction <rad action name> -serverip <rad server ip>
 -radkey <key> -radVendorID <ID >-radattributetype <rad attribute type>
```

Beispiel:

```
add authentication radiusaction radact1 -serverip 1.1.1.1 -radkey 123 -
radVendorID 1234 -radAttributeType 2
```

Erweiterte Authentifizierungsrichtlinie für RADIUS-Server hinzufügen

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add authentication policy <policy name> -rule true -action <rad action name
>
```

Beispiel:

```
add authentication policy radpol11 -rule true -action radact1
```

Authentifizierungsanmeldeschema hinzufügen

Sie können das Anmeldeschema von SingleAuth.xml verwenden, um die Anmeldeseite bereitzustellen, auf der die Appliance einen Systembenutzer auf einer zweiten Authentifizierungsebene authentifizieren kann.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication loginSchema <name> -authenticationSchema <string>
```

Beispiel:

```
add authentication loginSchema radschema -authenticationSchema LoginSchema/
SingleAuth.xml
```

Hinzufügen und Binden der Authentifizierungsrichtlinie zur RADIUS-Authentifizierungsrichtlinie für die Benutzeranmeldung

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication policylabel <labelName> [-type ( AAATM_REQ | RBA_REQ )]
[-comment <string>][-loginSchema <string>]
```

Beispiel:

```
add authentication policylabel label1 -type RBA_REQ -loginSchema radschema
bind authentication policylabel <labelName> -policyName <string> -priority
 <positive_integer> [-gotoPriorityExpression <expression>][-nextFactor <
string>]
```

Beispiel:

```
bind authentication policylabel label1 -policyName radpol11 -priority
```

Authentifizierungsrichtlinie global binden

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind system global [<policyName> [-priority <positive_integer>] [-nextFactor
 <string>] [-gotoPriorityExpression <expression>]]
```


Beispiel:

```
bind system global radpol11 -priority 1 -nextFactor label11
```

So konfigurieren Sie ohne Zwei-Faktor-Authentifizierung für Gruppenbenutzer mit dem Suchfilter:

1. Authentifizierungsaktion für LDAP-Server hinzufügen
2. Hinzufügen der Authentifizierungsrichtlinie für LDAP-Server
3. Bind Authentication System global für LDAP-Server

Authentifizierungsaktion für LDAP-Server hinzufügen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication ldapaction <ldap action name> -serverip <IP> -ldapbase
<> -ldapbinddn <binddn name> -ldapbinddnpassword <password>-ldaploginname
 <loginname> -groupattrname <grp attribute name> -subAttributename <>-
searchFilter<>
```

Beispiel:

```
add authentication ldapaction ldapact1 -serverip 1.1.1.1 -ldapbase base -
ldapbindDn name -ldapbindDNpassword password -ldapLoginName name -groupAttrName
 name -subAttributeName name - searchFilter "memberOf=CN=grp4,CN=Users,DC=
aaatm-test,DC=com"
```

Hinzufügen der Authentifizierungsrichtlinie für LDAP-Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add authentication policy <policy name> --rule true -action <ldap action
name>
```

Beispiel:

```
add authentication policy pol1 -rule true -action ldapact1
```

Bind Authentication System global für LDAP-Richtlinie

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind system global ldappolicy -priority <priority> -nextFactor <policy
label name>
```

Beispiel:

```
bind system global pol11 -priority 1 -nextFactor label11
```


Angepasste Eingabeaufforderung für Zwei-Faktor-Authentifizierung anzeigen

Wenn Sie zwei Faktor-Kennwort-Feld mit der Datei SingleAuth.xml unter/flash/nsconfig/loginschema/LoginSchema

Es folgt das Snippet einer Datei SingleAuth.xml, in der ‘SecondPassword: ‘der zweite Kennwortfeldname ist, der an den Benutzer aufgefordert wird, ein zweites Kennwort einzugeben.

```
<?xml version=”1.0” encoding=”UTF-8”?>
<AuthenticateResponse xmlns=”http://citrix.com/authentication/response/1”>
<Status>success</Status>
<Result>more-info</Result>
<StateContext/>
<AuthenticationRequirements>
<PostBack>/nf/auth/doAuthentication.do</PostBack>
<CancelPostBack>/nf/auth/doLogoff.do</CancelPostBack>
<CancelButtonText>Cancel</CancelButtonText>
<Requirements>
<Requirement><Credential><ID>login</ID><SaveID>ExplicitForms-Username</SaveID><Type>username</Type></Credential><Label><Text>singleauth_user_name</Text><Type>nsg-login-label</Type></Label><Input><AssistiveText>singleauth_please_supply_either_domain\username_or_user@fully.qualified.domain</AssistiveText><Text><Secret>false</Secret><ReadOnly>false</ReadOnly><InitialValue/><Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><ID>passwd</ID><SaveID>ExplicitForms-Password</SaveID><Type>password</Type></Credential><Label><Text>SecondPassword:</Text><Type>nsg-login-label</Type></Label><Input><Text><Secret>true</Secret><ReadOnly>false</ReadOnly><InitialValue/><Constraint>.+</Constraint></Text></Input></Requirement>
<Requirement><Credential><Type>none</Type></Credential><Label><Text>singleauth_first_factor</Text><Type>nsg_confirmation</Type></Label><Input/></Requirement>
<Requirement><Credential><ID>saveCredentials</ID><Type>savecredentials</Type></Credential><Label><Text>singleauth_remember_my_password</Text><Type>nsg-login-label</Type></Label><Input><CheckBox><InitialValue>false</InitialValue></CheckBox></Input></Requirement>
<Requirement><Credential><ID>loginBtn</ID><Type>none</Type></Credential><Label><Type>none</Type></Label><Input><Button>singleauth_log_on</Button></Input></Requirement>
</Requirements>
</AuthenticationRequirements>
</AuthenticateResponse>
```



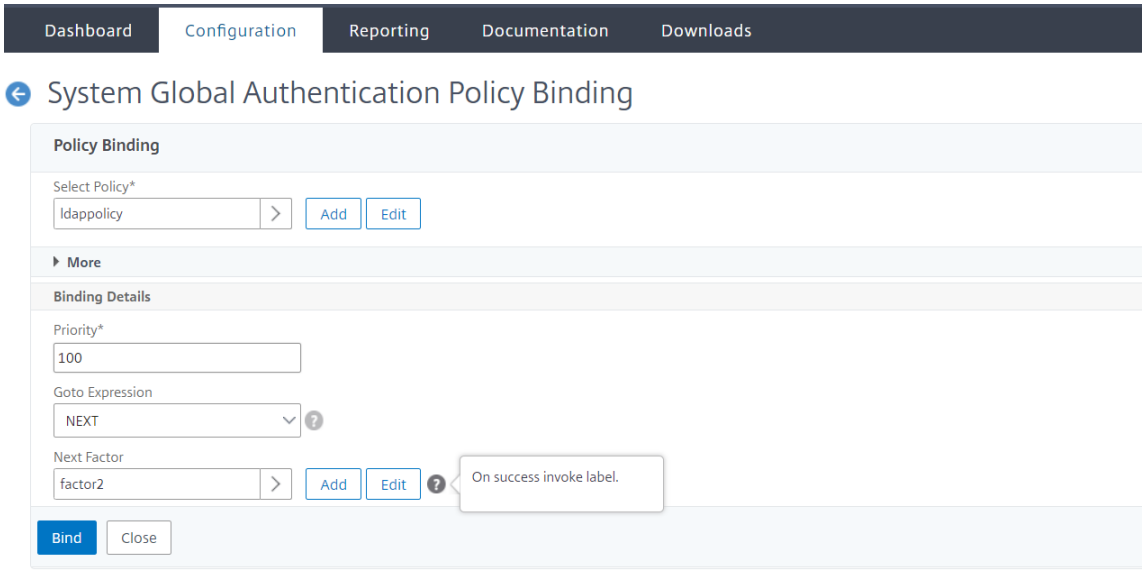
```
19 <!--NeedCopy-->
```

Konfigurieren der Zwei-Faktor-Authentifizierung mit der Citrix ADC GUI

1. Melden Sie sich bei der Citrix ADC Appliance an.
2. Gehen Sie zu **System** > **Authentifizierung** > **Erweiterte Richtlinien** > **Richtlinie** .
3. Klicken Sie auf Hinzufügen, um die Authentifizierungsrichtlinie der ersten Ebene zu erstellen.
4. Legen Sie auf der Seite **Authentifizierungsrichtlinie erstellen** die folgenden Parameter fest.
    a) Name. Name der Richtlinie
    b) Aktionstyp. Wählen Sie den Aktionstyp als LDAP, Active Directory, RADIUS, TACACS usw.
    c) Aktion: Die Authentifizierungsaktion (Profil), die der Richtlinie zugeordnet werden soll. Sie können eine vorhandene Authentifizierungsaktion auswählen oder auf das Pluszeichen klicken und eine Aktion des richtigen Typs erstellen.
    d) Ausdruck. Geben Sie einen erweiterten Richtlinienausdruck an.
5. Klicken Sie auf **Erstellen** und dann auf **Schließen**.
    a) Ausdruck. Geben Sie einen erweiterten Richtlinienausdruck an.
6. Klicken Sie auf **Erstellen**.
7. Klicken Sie auf **Hinzufügen**, um die Authentifizierungsrichtlinie der zweiten Ebene zu erstellen.
8. **Legen Sie auf der Seite Authentifizierungsrichtlinie erstellen** die folgenden Parameter fest
    a) Name. Name der Richtlinie
    b) Aktionstyp. Wählen Sie den Aktionstyp als LDAP, Active Directory, RADIUS, TACACS usw.
    c) Aktion: Die Authentifizierungsaktion (Profil), die der Richtlinie zugeordnet werden soll. Sie können eine vorhandene Authentifizierungsaktion auswählen oder auf das Symbol + klicken, um eine Aktion des richtigen Typs zu erstellen.
    d) Ausdruck. Bereitstellen eines erweiterten Richtlinienausdrucks
9. Klicken Sie auf **Erstellen** und dann auf **Schließen**.
    a) Ausdruck. Geben Sie einen erweiterten Richtlinienausdruck an.
10. Klicken Sie auf **Erstellen**.
11. Klicken Sie auf der Seite **Authentifizierungsrichtlinien** auf **Globale Bindung** .
12. Wählen Sie auf der Seite **Globale Authentifizierungsrichtlinien-Bindung erstellen** die Authentifizierungsrichtlinie der ersten Ebene aus und klicken Sie auf **Bindung hinzufügen**.
13. Wählen Sie auf der Seite **Richtlinienbindung** die Authentifizierungsrichtlinie aus, und legen Sie den folgenden Richtlinienbindungsparameter fest.

a) Nächster Faktor. Wählen Sie die Bezeichnung der Authentifizierungsrichtlinie der zweiten Ebene aus.

14. Klicken Sie auf **Binden** und **Schließen** .



15. Klicken Sie auf **Fertig**.

16. Melden Sie sich bei der Citrix ADC Appliance für die Authentifizierung der zweiten Ebene an. Der Benutzer kann nun das zweite Kennwort angeben. Nur wenn beide Kennwörter korrekt sind, darf der Benutzer auf die Citrix ADC Appliance zugreifen.

> **Hinweis**
>
> Die für eine zweite Faktorauthentifizierung konfigurierte TACACS unterstützt keine Autorisierung und Buchhaltung, selbst wenn Sie sie für den Befehl “tacacsAction” aktivieren. Der zweite Faktor wird nur für den Zweck der Authentifizierung verwendet.

Siehe auch das Thema Zwei-Faktor-Authentifizierung in Citrix ADC nFactor-Authentifizierung .

Eingeschränkte Systembenutzerauthentifizierung für Citrix ADC Managementschnittstellen

October 5, 2021

Sie können den Zugriff von Systembenutzern auf bestimmte Citrix ADC Verwaltungsschnittstellen wie CLI oder API einschränken. Der `allowedManagementInterface` Parameter definiert die Liste der erlaubten Verwaltungsschnittstellen. Wenn beispielsweise die Verwaltungsschnittstelle für einen Benutzer oder eine Gruppe auf API festgelegt ist, können alle Benutzer in der Gruppe über API und nicht

über CLI auf Citrix ADC zugreifen. Die Citrix ADC GUI ist jedoch Teil der API-Schnittstelle, und Benutzer mit API-Berechtigung können auch auf die GUI-Schnittstelle zugreifen.

> **Hinweis:**
>
> Standardmäßig haben Benutzer und Gruppen Zugriff auf alle Schnittstellen (CLI, API und die GUI).

Sie können den Parameter entweder auf Benutzerebene oder auf Benutzergruppenebene konfigurieren. Wenn Sie auf Gruppenebene konfigurieren, wird die Konfiguration auf alle Benutzerkonten in der Gruppe angewendet. Wenn ein Benutzer an mehrere Gruppen gebunden ist, ermöglicht die Appliance den Zugriff auf eine aggregierte Gruppe von Verwaltungsschnittstellen. Sie können Einstellungen für einen Benutzer in einer Gruppe festlegen, indem Sie den Parameter auf Benutzerebene konfigurieren. In diesem Fall ist die Einstellung auf Benutzerebene für eine Gruppe konfiguriert.
In bestimmten Szenarien werden die Serverdetails auf der Appliance konfiguriert, wenn der Kunde einen externen Authentifizierungsserver für die Verwaltung von Benutzerkonten verwendet. In diesem Fall kann der Administrator eine Benutzergruppe in der Citrix ADC Appliance erstellen und alle Benutzer (gruppiert auf dem externen Server) zur Gruppe hinzufügen. Beispielsweise werden alle auf dem externen Server verwalteten Benutzer der Gruppe API_Users hinzugefügt, und der Administrator kann die Gruppe lokal auf der Appliance konfigurieren.

> **Hinweis:**
>
> Die Citrix ADC Appliance erlaubt nur dem `nsroot` Administrator (Superuser) die Konfiguration des Parameters und erlaubt keinem Systembenutzer, die Parametereinstellung zu ändern.

Konfigurieren des Benutzerzugriffs auf Citrix ADC Verwaltungsschnittstellen über die CLI

Um Benutzern den Zugriff auf eine bestimmte Verwaltungsschnittstelle zu ermöglichen, müssen Sie den zulässigen Management-Interface-Parameter festlegen. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set system group <groupName> [-allowedManagementInterface ( CLI | API )]
```

Beispiel:

```
set system group network_usergroup -allowedManagementInterface CLI
```

Informationen zur Parameterbeschreibung finden Sie unter Referenz zu Authentifizierungs- und Berechtigungsbefehlen .

Informationen zu Citrix GUI- und CLI-Schnittstellen finden Sie unter Access Citrix ADC Thema.

TCP-Konfigurationen

June 21, 2022

TCP-Konfigurationen für eine Citrix ADC-Appliance können in einer Entität angegeben werden, die als TCP-Profil bezeichnet wird, bei der es sich um eine Sammlung von TCP-Einstellungen handelt. Das TCP-Profil kann dann mit Diensten oder virtuellen Servern verknüpft werden, die diese TCP-Konfigurationen verwenden möchten.

Ein Standard-TCP-Profil kann so konfiguriert werden, dass die TCP-Konfigurationen festgelegt werden, die standardmäßig global auf alle Dienste und virtuellen Server angewendet werden.

> **Hinweis:**
>
> Wenn ein TCP-Parameter unterschiedliche Werte für den Dienst, den virtuellen Server und global aufweist, erhält der Wert der am meisten spezifischen Entität (den Dienst) die höchste Priorität. Die Citrix ADC-Appliance bietet auch andere Ansätze zur Konfiguration von TCP. Lesen Sie weiter für weitere Informationen.

Unterstützte TCP-Konfiguration

Die Citrix ADC-Appliance unterstützt die folgenden TCP-Funktionen:

TCP gegen Spoofing-Angriffe verteidigen

Die **Citrix ADC-Implementierung der** Fensterdämpfung ist RFC 4953-konform.

Explicit Congestion Notification (ECN)

Die Appliance sendet eine Benachrichtigung über den Netzwerküberlastungsstatus an den Absender der Daten und ergreift Korrekturmaßnahmen für Datenüberlastung oder Datenbeschädigung. Die Citrix ADC-Implementierung von ECN ist RFC 3168-konform.

Roundtrip-Zeitmessung (RTTM) mit der Zeitstempeloption

Damit die TimeStamp-Option funktioniert, muss sie mindestens eine Seite der Verbindung (Client oder Server) unterstützen. Die Citrix ADC-Implementierung der Option `TimeStamp` ist RFC 1323-konform.

Erkennung von unvorsichtigen Wiederübertragungen

Dies kann mit doppelter selektiver TCP-Bestätigung (D-SACK) und Forward-RTO-Recovery (F-RTO) erfolgen. Wenn es unechte Wiederübertragungen gibt, werden die Konfigurationen der Überlastungssteuerung in ihren ursprünglichen Zustand versetzt. Die Citrix ADC Implementierung von D-SACK ist RFC 2883-konform und F-RTO ist RFC 5682-konform.

Überlastungskontrolle

Diese Funktionalität verwendet New-Reno-, BIC-, CUBIC-, Nile- und TCP-Westwood-Algorithmen.

Skalierung von Fenstern

Dies erhöht die Größe des **TCP-Empfangsfensters** über den Maximalwert von 65.535 Byte hinaus.

Punkte, die Sie beachten sollten, bevor Sie die Fensterskalierung konfigurieren

- Sie legen keinen hohen Wert für den Skalierungsfaktor fest, da dies negative Auswirkungen auf die Appliance und das Netzwerk haben kann.
- Sie konfigurieren keine Fensterskalierung, es sei denn, Sie wissen genau, warum Sie die Fenstergröße ändern möchten.
- Beide Hosts in der TCP-Verbindung senden beim Verbindungsaufbau eine Fensterskalierungsoption. Wenn nur eine Seite einer Verbindung diese Option setzt, wird für die Verbindung keine Fensterskalierung verwendet.
- Jede Verbindung für dieselbe Sitzung ist eine unabhängige Fensterskalierungssitzung. Wenn beispielsweise die Anforderung eines Clients und die Antwort des Servers durch die Appliance fließt, kann eine Fensterskalierung zwischen dem Client und der Appliance ohne Fensterskalierung zwischen der Appliance und dem Server erfolgen.

Fenster mit maximaler Überlastung von TCP

Die Fenstergröße ist vom Benutzer konfigurierbar. Der Standardwert ist 8190 Byte.

Selektive Bestätigung (SACK)

Dies verwendet den Datenempfänger (entweder eine Citrix ADC-Appliance oder ein Client), der den Absender über alle Segmente informiert, die erfolgreich empfangen wurden.

Bestätigung vorwärts (FACK)

Diese Funktion vermeidet TCP-Überlastung, indem sie die Gesamtzahl der im Netzwerk ausstehenden Datenbytes explizit misst und dem Absender (entweder einem Citrix ADC oder einem Client) hilft, die

Menge der Daten zu kontrollieren, die während der Zeitüberschreitung der erneuten Übertragung in das Netzwerk injiziert werden.

TCP-Verbindungs-Multiplexen

Diese Funktion ermöglicht die Wiederverwendung bestehender TCP-Verbindungen. Die Citrix ADC-Appliance speichert etablierte TCP-Verbindungen zum Wiederverwendungspool. Wenn eine Clientanforderung empfangen wird, sucht die Appliance nach einer verfügbaren Verbindung im Wiederverwendungspool und bedient den neuen Client, wenn die Verbindung verfügbar ist. Wenn sie nicht verfügbar ist, erstellt die Appliance eine Verbindung für die Client-Anfrage und speichert die Verbindung zum Wiederverwendungspool. Der Citrix ADC unterstützt das Verbindungsmultiplexing für HTTP-, SSL- und DataStream-Verbindungstypen.

Dynamische Empfangspufferung

Auf diese Weise kann der Empfangspuffer basierend auf Speicher- und Netzwerkbedingungen dynamisch angepasst werden.

Mehrwege-TCP-Verbindung

Multipath-TCP-Verbindungen (MPTCP) zwischen dem Client und der Citrix ADC-Appliance. MPTCP-Verbindungen werden zwischen der Citrix ADC Appliace und dem Back-End nicht unterstützt. Die Citrix ADC-Implementierung von MPTCP ist RFC 6824- und RFC 8684-konform und unterstützt sowohl MPTCP-Version 0 als auch 1.

Über die Befehlszeilenschnittstelle können Sie MPTCP-Statistiken wie aktive MPTCP-Verbindungen und aktive Subflow-Verbindungen anzeigen.

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um eine Zusammenfassung oder detaillierte Zusammenfassung der MPTCP-Statistiken anzuzeigen oder die Statistikanzeige zu löschen:

1. `Stat MPTCP`
2. `Stat mptcp -detail`
3. `Clearstats basic`

> **Hinweis:**
>
> Um eine MPTCP-Verbindung herzustellen, müssen sowohl der Client als auch die Citrix ADC-Appliance dieselbe MPTCP-Version unterstützen. Wenn Sie die Citrix ADC-Appliance als MPTCP-Gateway für Ihre Server verwenden, müssen die Server MPTCP nicht unterstützen. Wenn der Client eine neue MPTCP-Verbindung startet, identifiziert die Appliance die MPTPC-Version des Clients anhand der MP_CAPABALE-Option im SYN-Paket. Wenn die Version des Clients höher

> ist als die auf der Appliance unterstützte Version, gibt die Appliance ihre höchste Version in der MP_CAPABALE-Option des SYN-ACK-Pakets an. Der Client greift dann auf eine niedrigere Version zurück und sendet die Versionsnummer in der MP_CAPABALE-Option des ACK-Pakets. Wenn diese Version unterstützbar ist, setzt die Appliance die MPTCP-Verbindung fort. Andernfalls fällt die Appliance auf einen normalen TCP zurück. Die Citrix ADC-Appliance initiiert keine Subflows (MP_JOINs). Die Appliance erwartet, dass der Client Subflows initiiert.

Unterstützung für zusätzliche Adressenwerbung (ADD_ADDR) in MPTCP

Wenn Sie in einer MPTCP-Bereitstellung einen virtuellen Server haben, der an einen IP-Satz gebunden ist, der zusätzliche IP-Adressen des virtuellen Servers enthält, gibt die Funktion für zusätzliche Adressenankündigung (ADD_ADDR) die IP-Adresse der virtuellen Server an, die an den IP-Satz gebunden sind. Clients können mehr `MP-JOIN`-Subflows zu den angekündigten IP-Adressen initiieren.

Punkte, die Sie über die MPTCP ADD_ADDR-Funktionalität erinnern

- Sie können im Rahmen der Option `ADD_ADDR` maximal 10 IP-Adressen senden. Wenn mehr als 10 IP-Adressen mit aktiviertem Parameter `mptcpAdvertise` vorhanden sind, ignoriert die Appliance nach der Werbung für die 10-IP-Adresse den Rest der IP-Adressen.
- Wenn der MP-FÄHIGE Subflow an eine der IP-Adressen im IP-Satz anstelle der IP-Adresse des primären virtuellen Servers übertragen wird, wird die IP-Adresse des virtuellen Servers angekündigt, wenn der Parameter `mptcpAdvertise` für die IP-Adresse des virtuellen Servers aktiviert ist

Konfigurieren Sie die Funktion für weitere Adressenankündigungen (ADD_ADDR), um mithilfe der CLI mehr VIP-Adressen anzukündigen

Sie können die Funktionalität `MPTCP ADD_ADDR` sowohl für IPv4- als auch für IPv6-Adresstypen konfigurieren. Im Allgemeinen können mehrere IPv4- und IPv6-IPs an einen einzelnen IP-Satz angeschlossen werden, und der Parameter kann für jede Teilmenge von IP-Adressen aktiviert werden. In der ADD_ADDR-Funktion werden nur die IP-Adressen angekündigt, bei denen die Option “mptcpAdvertise” aktiviert ist, und die verbleibenden IP-Adressen aus dem IP-Satz werden ignoriert. Führen Sie die folgenden Schritte aus, um das Feature `ADD_ADDR` zu konfigurieren:

1. Fügen Sie einen IP-Satz hinzu.
2. Fügen Sie eine IP-Adresse vom Typ Virtual Server IP (VIP) hinzu, wobei MPTCP Advertise aktiviert ist.
3. Binden Sie die IP-Adresse an die IP gesetzt.
4. Konfigurieren Sie die IP-Satz mit dem virtuellen Lastenausgleichsserver.

Fügen Sie einen IP-Satz hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add ipset <name> [-td <positive_integer>]
2 <!--NeedCopy-->
```

Beispiel:

```
1 add ipset ipset_1
2 <!--NeedCopy-->
```

Fügen Sie eine IP-Adresse vom Typ Virtual Server IP (VIP) hinzu, wobei MPTCP Advertise aktiviert ist

Geben Sie beim Befehl ein:

```
1 add ns ip <IPAddress>@ <netmask> [-mptcpAdvertise ( YES | NO )] -type <
     type>
2 <!--NeedCopy-->
```

Beispiel:

```
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP
```

Binden Sie IP-Adressen an den IP-Satz

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind ipset <name> <IPAddress>
2 <!--NeedCopy-->
```

Beispiel:

```
bind ipset ipset_1 10.10.10.10
```


Konfigurieren der IP, die auf den virtuellen Lastenausgleich eingestellt ist

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> [-ipset  <string>]
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver lb1 -ipset ipset_1
<!--NeedCopy-->
```

Beispiel-Konfiguration:

```
Add ipset ipset_1
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP
bind ipset ipset_1 10.10.10.10
set lb vserver lb1 -ipset ipset_1
<!--NeedCopy-->
```

Konfigurieren Sie die externe IP-Adresse der Werbung mithilfe der ADD_ADDR-Funktionalität

Wenn die angekündigte IP-Adresse im Besitz der externen Entität ist und die Citrix ADC-Appliance die IP-Adresse bekannt geben muss, muss der Parameter “mptcpAdvertise” mit deaktivierten Status- und ARP-Parametern aktiviert sein.

Führen Sie die folgenden Schritte aus, um `ADD_ADDR` für die Ankündigung der externe IP-Adresse zu konfigurieren.

1. Fügen Sie eine IP-Adresse vom Typ Virtual Server IP (VIP) hinzu, wobei MPTCP Advertise aktiviert ist.
2. Binden Sie die IP-Adresse an die IP gesetzt.
3. Binden Sie IP mit dem virtuellen Lastenausgleichsserver

Fügen Sie eine externe IP-Adresse vom Typ Virtual Server IP (VIP) hinzu, wobei MPTCP Advertise aktiviert ist

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
add ns ip <IPAddress>@ <External-IP-mask -type VIP> [-mptcpAdvertise (
    YES | NO )] -type <type> -state DISABLED -arp DISABLED
<!--NeedCopy-->
```

Beispiel:

```
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP -state
DISABLED -arp DISABLED
```

Binden Sie IP-Adressen an den IP-Satz

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind ipset <name> <IPAddress>
<!--NeedCopy-->
```

Beispiel:

```
bind ipset ipset_1 10.10.10.10
```

Konfigurieren der IP, die auf den virtuellen Lastenausgleich eingestellt ist

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> [-ipset  <string>]
<!--NeedCopy-->
```

Beispiel:

```
set lb vserver lb1 -ipset ipset_1
```

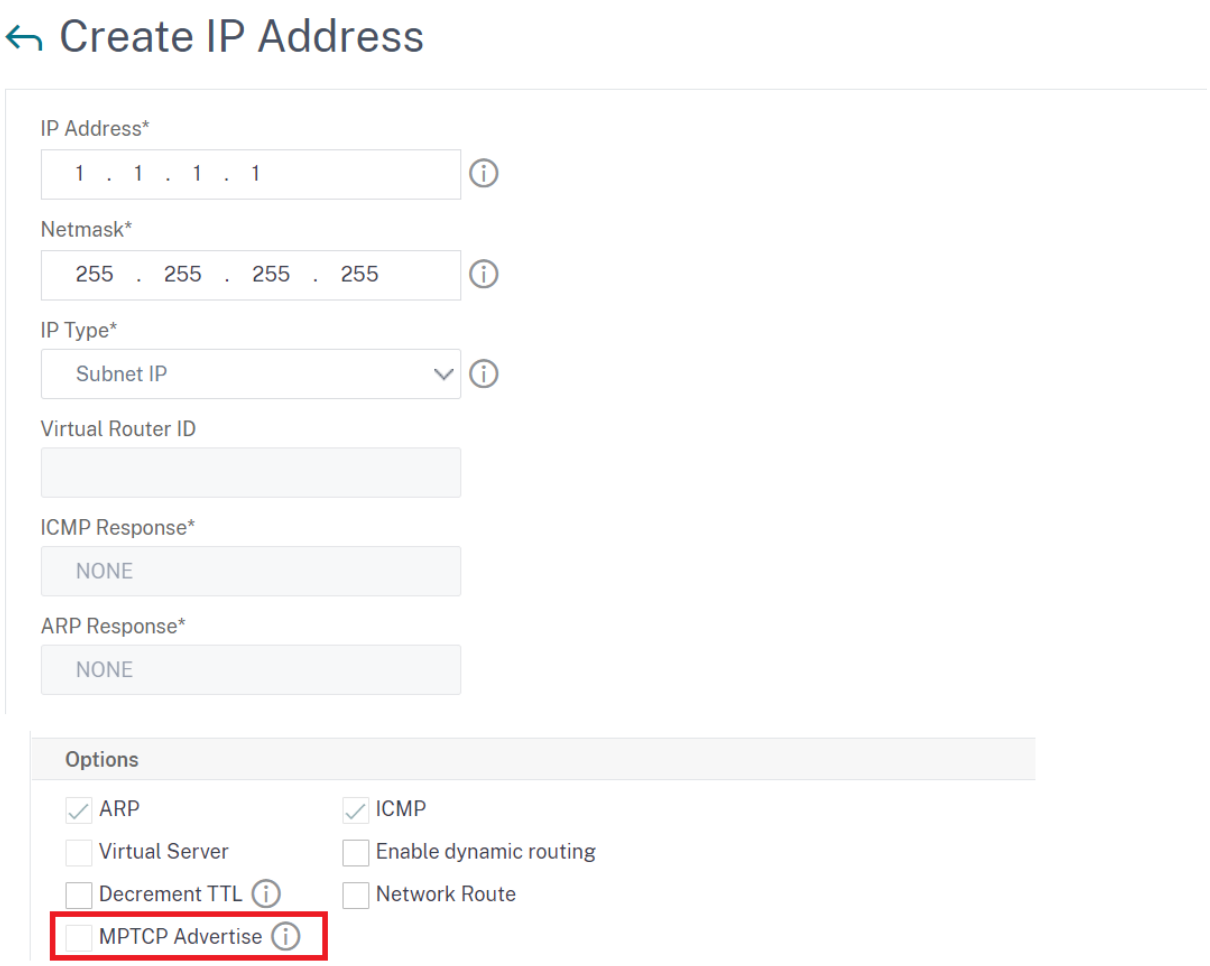
Beispiel-Konfiguration:

```
add ns ip 10.10.10.10 255.255.255.255 -mptcpAdvertise YES -type VIP
    state DISABLED -arp DISABLED
bind ipset ipset_1 10.10.10.10
set lb vserver lb1 -ipset ipset_1
<!--NeedCopy-->
```


Werben Sie die IP-Adresse für MPTCP-fähige Clients über die Citrix ADC GUI an

Führen Sie den folgenden Schritt aus, um die IP-Adresse an die MPTCP-fähigen Clients anzukündigen:

1. Navigieren Sie zu **System > Netzwerk > IPs**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Aktivieren Sie auf der Seite **IP-Adresse erstellen** das Kontrollkästchen **MPTCP Advertise**, um den Parameter festzulegen. Standardmäßig ist es deaktiviert.



Extrahieren der TCP/IP-Pfad-Overlay-Option und Einfügen des Client-IP-HTTP-Headers

Extrahieren von TCP/IP-Pfadüberlagerung und Einfügen von HTTP-Header von Client-IP. Der Datentransport durch Overlay-Netzwerke verwendet häufig Verbindungsabbruch oder Network Address Translation (NAT), bei der die IP-Adresse des Quell-Clients verloren geht. Um dies zu vermeiden, extrahiert die Citrix ADC-Appliance die TCP/IP-Pfad-Overlay Option und fügt die IP-Adresse des Quell-Clients in den HTTP-Header ein. Mit der IP-Adresse im Header kann der Webserver den Quellclient identifizieren, der die Verbindung hergestellt hat. Die extrahierten Daten sind für eine Lebensdauer

der TCP-Verbindung gültig und dies verhindert daher, dass der nächste Hop-Host die Option erneut interpretieren muss. Diese Option ist nur für Webdienste anwendbar, für die die Einfügeoption Client-IP aktiviert ist.

TCP-Segmentierungsabladung

Lädt die TCP-Segmentierung auf die NIC aus. Wenn Sie die Option auf "AUTOMATIC" festlegen, wird die TCP-Segmentierung auf die NIC verlagert, wenn die NIC unterstützt wird.

Cookie für TCP-Handshake mit Clients synchronisieren

Dies wird verwendet, um SYN-Überschwemmungen zu widerstehen. Sie können den `SYNCOOKIE` -Mechanismus für TCP-Handshake mit Clients aktivieren oder deaktivieren. Deaktivieren von `SYNCOOKIE` verhindert den `SYN`-Angriffsschutz auf der Citrix ADC-Appliance.

MSS lernen, um MSS Learning für alle virtuellen Server zu aktivieren, die auf der Appliance konfiguriert sind

Unterstützte TCP-Parameter

Die folgende Tabelle enthält eine Liste der TCP-Parameter und ihres Standardwerts, der auf einer Citrix ADC-Appliance konfiguriert ist.

Parameter	Standardwert	Beschreibung
Fenster-Verwaltung		
TCP-Verzögerter Ack Timer	100 Millisec	Timeout für TCP-verzögerte ACK in Millisekunden.
TCP-Mindestzeitlimit für die Weiterübertragung (RTO) in Milli Sek	1000 Milli Sek	Minimale Zeitüberschreitung für die erneute Übertragung in Millisekunden, angegeben in 10-Millisekunden-Schritten (Wert muss eine ganze Zahl ergeben, wenn sie durch 10 geteilt wird)

Parameter	Standardwert	Beschreibung
Leerlaufzeit der Verbindung vor dem Starten von Keep-Alive-Sonden	900 Sekunden	Löschen Sie im Stille TCP-etablierte Verbindungen bei Leerlauf-Timeouts, die Verbindungen im Leerlauf-Timeout hergestellt haben
TCP-Zeitstempeloption	DEAKTIVIERT	Die Zeitstempeloption ermöglicht eine genaue RTT-Messung. Aktivieren oder Deaktivieren Sie die Option TCP-Zeitstempel.
Timeout für Multipath TCP-Session	0 Sekunden	Zeitüberschreitung für die MPTCP Sitzung in Sekunden. Wenn dieser Wert nicht gesetzt ist, Leerlauf. MPTCP-Sitzungen werden nach dem Client-Leerlauf-Timeout des virtuellen Servers geleert.
Stillschweigendes Löschen von Halbgeschlossenen Verbindungen bei Leerlaufzeitüberschreitung	0 Sekunden	Lassen Sie die halbgeschlossenen TCP-Verbindungen im Leerlauf stillschweigend fallen.
Lege etablierte Verbindungen im Leerlauf-Timeout still ab	DEAKTIVIERT	Lassen Sie TCP-etablierte Verbindungen im Leerlauf-Timeout still fallen
Speicherverwaltung		

Parameter	Standardwert	Beschreibung
TCP-Puffergröße	131072 Bytes	Die Größe des TCP-Puffers ist die Größe des Empfangspuffers im Citrix ADC. Diese Puffergröße wird Clients und Servern von Citrix ADC angekündigt und steuert deren Fähigkeit, Daten an Citrix ADC zu senden. Die Standardpuffergröße beträgt 8K, und normalerweise ist es sicher, dies zu erhöhen, wenn Sie mit internen Serverfarmen sprechen. Die Puffergröße wirkt sich auch auf die tatsächliche Anwendungslayer in Citrix ADC aus, wie bei SSL-Endpunktfällen ist sie auf 40 K festgelegt und für die Komprimierung auf 96 K festgelegt. **Hinweis:** Das Argument für die Puffergröße muss festgelegt werden, damit dynamische Anpassungen stattfinden können.
TCP-Sendpuffergröße	8190 Bytes	TCP-Sendpuffergröße

Parameter	Standardwert	Beschreibung
Dynamische Empfangspufferung von TCP	DEAKTIVIERT	Aktivieren oder deaktivieren Sie die dynamische Empfangspufferung. Wenn diese Option aktiviert ist, kann der Empfangspuffer basierend auf Speicher- und Netzwerkbedingungen dynamisch angepasst werden. **Hinweis:** Das Argument Puffergröße muss festgelegt werden, damit dynamische Anpassungen stattfinden können
TCP-Max-Überlastungsfenster (CWND)	524288 Bytes	Fenster “Maximale Überlastung” von TCP
Status der Fensterskalierung	ENALBED	Aktivieren oder deaktivieren Sie die Fensterskalierung.
Skalierungsfaktor für Fenster	8	Faktor, der zur Berechnung der neuen Fenstergröße verwendet wird. Dieses Argument ist nur erforderlich, wenn die Fensterskalierung aktiviert ist.
Verbindungs-Setup		
Keep-Alive-Sonden	DEAKTIVIERT	Senden Sie periodische TCP-Keep-Alive-Sonden (KA), um zu überprüfen, ob der Peer noch aktiv ist.
Leerlaufzeit der Verbindung vor dem Starten von Keep-Alive-Sonden	900 Sekunden	Dauer in Sekunden, damit die Verbindung im Leerlauf ist, bevor eine Keep-Alive-Sonde (KA) gesendet wird.
Keep-Alive-Sondenintervall	75 Sekunden	Zeitintervall in Sekunden vor der nächsten Keep-Alive-Sonde (KA), wenn der Peer nicht reagiert.

Parameter	Standardwert	Beschreibung
Maximale Keep-Alive-Sonden, die verpasst werden müssen, bevor die Verbindung unterbrochen wird.	3	Anzahl der Keep-Alive-Sonden (KA), die gesendet werden sollen, wenn sie nicht bestätigt werden, bevor angenommen wird, dass der Peer ausgefallen ist.
RST-Fensterdämpfung (Spoofschutz)	DEAKTIVIERT	Aktivieren oder deaktivieren Sie RST-Fensterdämpfung, um vor Spoofing zu schützen. Wenn diese Option aktiviert ist, erfolgt die Antwort mit korrigierendem ACK, wenn eine Sequenznummer ungültig ist.
Akzeptieren Sie RST mit der letzten quittierten Sequenznummer.	AKTIVIERT	
Datenübertragung		
Sofortiges ACK auf PUSH-Paket	AKTIVIERT	Senden Sie sofort eine positive Bestätigung (ACK) nach Erhalt von TCP-Paketen mit PUSH-Flag.
Maximale Pakete pro MSS	0	Maximale Anzahl von Oktetten, die in einem TCP-Datensegment zugelassen werden sollen

Parameter	Standardwert	Beschreibung
Nagles Algorithmus	DEAKTIVIERT	Nagles Algorithmus kämpft mit dem Problem kleiner Pakete bei der TCP-Übertragung. Anwendungen wie Telnet und andere Echtzeit-Engines, bei denen jeder Tastendruck an die andere Seite weitergegeben werden muss, erzeugen oft kleine Pakete. Mit Nagle's Algorithmus kann Citrix ADC solche kleinen Pakete puffern und sendet sie zusammen, um die Verbindungseffizienz zu erhöhen. Dieser Algorithmus muss mit anderen TCP-Optimierungstechniken im Citrix ADC zusammenarbeiten.
Maximale zulässige TCP-Segmente in einem Burst	10 MSS	Maximale Anzahl von TCP-Segmenten in einem Burst zulässig
Maximale Pakete, die in die Warteschlange gestellt werden sollen	300	Maximale Größe der Warteschlange außerhalb der Ordnung Pakete. Ein Wert von 0 bedeutet kein Limit
Überlastungskontrolle		
TCP Flavor	CUBIC	
Einstellung des ersten Überlastungsfensters (cwnd)	4 MSS	Anfängliche maximale Obergrenze für die Anzahl der TCP-Pakete, die bei der TCP-Verbindung zum Server ausstehen können

Parameter	Standardwert	Beschreibung
Explizite TCP-Überlastungsbenachrichtigung (ECN)	DEAKTIVIERT	Die explizite Congestion Notification (ECN) ermöglicht eine End-zu-End-Benachrichtigung über Netzwerküberlastung, ohne Pakete zu verwerfen.
TCP-Max-Überlastungsfenster (CWND)	524288 Bytes	TCP unterhält ein Überlastungsfenster (CWND), das die Gesamtzahl der nicht bestätigten Pakete begrenzt, die möglicherweise End-to-End übertragen werden. In TCP ist das Überlastungsfenster einer der Faktoren, die die Anzahl der Bytes bestimmen, die jederzeit ausstehen können. Das Überlastungsfenster verhindert, dass eine Verbindung zwischen dem Absender und dem Empfänger mit zu viel Verkehr überlastet wird. Es wird berechnet, indem geschätzt wird, wie viel Staus auf der Verbindung vorhanden ist.
TCP-Hybrid-Start (HyStart)	8 Byte	
TCP-Mindestzeitlimit für die Weiterübertragung (RTO) in Milli Sek	1000	Minimales Zeitlimit für die Weiterübertragung in Millisekunden, angegeben in Schritten von 10 Millisekunden (der Wert muss eine ganze Zahl ergeben, wenn er durch 10 geteilt wird).
TCP-Dupack-Schwellenwert	DEAKTIVIERT	

Parameter	Standardwert	Beschreibung
Burst-Rate Steuerung	3	TCP-Burst-Rate Control DISABLED/FIXED/DYNAMIC. FIXED erfordert, dass eine TCP-Rate festgelegt wird
TCP-Rate	DEAKTIVIERT	Senderate der TCP-Verbindung Payload in KB/s
Höchstwarteschlange für TCP-Rate	0	Maximale Größe der Verbindungswarteschlange in Byte, wenn BurstrateControl verwendet wird.
MPTCP		
Mehrweg-TCP	DEAKTIVIERT	Multipath TCP (MPTCP) ist eine Reihe von Erweiterungen für reguläres TCP, um einen Multipath-TCP-Dienst bereitzustellen, der es ermöglicht, dass eine Transportverbindung über mehrere Pfade gleichzeitig funktioniert.
Multipath-TCP-Drop-Daten für vorab festgelegten Subflow	DEAKTIVIERT	Aktivieren oder deaktivieren Sie das stillschweigende Löschen der Daten im vorab etablierten Subflow. Wenn diese Option aktiviert ist, werden DSS-Datenpakete im Hintergrund gelöscht, anstatt die Verbindung zu löschen, wenn Daten im vorab festgelegten Subflow empfangen werden.

Parameter	Standardwert	Beschreibung
Multipath-TCP-fastopen	DEAKTIVIERT	Aktivieren oder deaktivieren Sie Multipath TCP fastopen. Wenn diese Option aktiviert ist, werden DSS-Datenpakete akzeptiert, bevor die dritte Packung SYN-Handshake empfangen wird.
Timeout für Multipath TCP-Session	0 Sekunden	Zeitüberschreitung für die MPTCP Sitzung in Sekunden. Wenn dieser Wert nicht festgelegt ist, werden ungenutzte MPTCP-Sitzungen nach dem Client-Leerlauf-Timeout des virtuellen Servers geleert.
Sicherheit		
SYN Spoof Schutz	DEAKTIVIERT	Aktivieren oder deaktivieren Sie das Löschen ungültiger SYN-Pakete zum Schutz vor Spoofing. Wenn diese Option deaktiviert ist, werden die etablierten Verbindungen zurückgesetzt, wenn ein SYN-Paket empfangen wird.
TCP Syncookie	DEAKTIVIERT	Dies wird verwendet, um SYN-Überschwemmungen zu widerstehen. Aktivieren oder deaktivieren Sie den SYNCOOKIE-Mechanismus für TCP-Handshake mit Clients. Das Deaktivieren von SYNCOOKIE verhindert den SYN-Angriffsschutz auf der Citrix ADC-Appliance.
Verlusterkennung und Erholung		

Parameter	Standardwert	Beschreibung
Doppelte selektive Bestätigung (DSACK)	AKTIVIERT	Eine Citrix ADC-Appliance verwendet Duplicate Selective Acknowledgment (DSACK), um festzustellen, ob eine erneute Übertragung fälschlicherweise gesendet wurde.
Forward RTO Erholung (FRTO)	AKTIVIERT	Erkennt unechte Timeouts für die TCP-Weiterübertragung. Nach der erneuten Übertragung des ersten nicht bestätigten Segments, das durch ein Timeout ausgelöst wird, überwacht der Algorithmus des TCP-Absenders die eingehenden Bestätigungen, um festzustellen, ob das Timeout falsch war. Anschließend entscheidet er, ob neue Segmente gesendet oder nicht bestätigte Segmente erneut übertragen werden sollen. Der Algorithmus hilft effektiv, weitere unnötige Neuübertragungen zu vermeiden und verbessert dadurch die TCP-Leistung im Falle eines unechten Timeouts.
TCP-Vorwärtsbestätigung (FACK)	AKTIVIERT	Aktivieren oder deaktivieren Sie FACK (Forward ACK).

Parameter	Standardwert	Beschreibung
Status der selektiven Bestätigung (SACK)	AKTIVIERT	TCP SACK befasst sich mit dem Problem der Mehrfachpaketverluste, wodurch die Gesamtdurchsatzkapazität reduziert wird. Mit selektiver Bestätigung kann der Empfänger den Absender über alle Segmente informieren, die erfolgreich empfangen wurden, sodass der Absender nur die verlorenen Segmente erneut übermitteln kann. Diese Technik hilft Citrix ADC, den Gesamtdurchsatz zu verbessern und die Verbindungslatenz zu reduzieren.
Maximale Pakete pro Weiterübertragung	1	Ermöglicht Citrix ADC zu steuern, wie viele Pakete in einem Versuch erneut übertragen werden sollen. Wenn Citrix ADC ein partielles ACK erhält und eine erneute Übertragung durchführen muss, wird diese Einstellung berücksichtigt. Dies wirkt sich nicht auf die RTO basierten Wiederübertragungen aus.
TCP-Verzögerter Ack Timer	100 Millisec	Timeout für TCP verzögertes ACK in Millisekunden
TCO-Optimierung		
TCP-Optimierungsmodus	TRANSPARENT	TCP-Optimierungsmodi TRANSPARENT/ENDPOINT

Parameter	Standardwert	Beschreibung
Wenden Sie adaptive TCP-Optimierungen an	DEAKTIVIERT	Wenden Sie adaptive TCP-Optimierungen an
TCP-Segmentierungs Offload	AUTOMATIC	Verlagern Sie die TCP-Segmentierung auf die NIC. Wenn diese Option auf AUTOMATIC eingestellt ist, wird die TCP-Segmentierung auf die NIC ausgelagert, wenn die NIC dies unterstützt.
ACK-Aggregation	DEAKTIVIERT	Aktivieren oder Deaktivieren von ACK Aggregation
TCP-Zeit-Warten (oder Time_Wait)	40 Sekunden	Zeit zu vergehen, bevor eine geschlossene TCP-Verbindung freigegeben wird
Delink Client und Server auf RST	DEAKTIVIERT	Delink Client- und Serververbindung, wenn ausstehende Daten vorhanden sind, die an die andere Seite gesendet werden.

Einstellen globaler TCP-Parameter

Mit der Citrix ADC-Appliance können Sie Werte für TCP-Parameter angeben, die für alle Citrix ADC-Dienste und virtuellen Server gelten. Dies kann geschehen mit:

- Standard-TCP-Profil
- Globaler TCP-Befehl
- TCP-Pufferungsfunktion

> **Hinweis**:
>
> Der Parameter `recvBuffSize` des Befehls set ns tcpParam ist ab Version 9.2 veraltet. Legen Sie in späteren Versionen die Puffergröße mithilfe des Parameters `bufferSize` des Befehls set ns tcpProfile fest. Wenn Sie auf eine Version aktualisieren, in der der Parameter `recvBuffSize` veraltet ist, wird der Parameter `bufferSize` auf den Standardwert festgelegt.

Standard-TCP-Profil

Ein TCP-Profil mit dem Namen `nstcp_default_profile` wird verwendet, um TCP-Konfigurationen anzugeben, die verwendet werden, wenn auf Service- oder virtuelle Serverebene keine TCP-Konfigurationen bereitgestellt werden.

> **Hinweise:**
>
> - Nicht alle TCP-Parameter können über das Standard-TCP-Profil konfiguriert werden. Einige Einstellungen müssen mit dem globalen TCP-Befehl vorgenommen werden (siehe Abschnitt unten).
> - Das Standardprofil muss nicht explizit an einen Dienst oder einen virtuellen Server gebunden sein.

So konfigurieren Sie das Standard-TCP-Profil

- Geben Sie über die Befehlszeilenschnittstelle an der Eingabeaufforderung Folgendes ein:

```
set ns tcpProfile nstcp_default_profile...
<!--NeedCopy-->
```

- Navigieren Sie auf der Benutzeroberfläche zu **System** > **Profile**, klicken Sie auf **TCP-Profile** und aktualisieren Sie nstcp_default_profile.

Globaler TCP-Befehl

Ein anderer Ansatz, mit dem Sie globale TCP-Parameter konfigurieren können, ist der globale TCP-Befehl. Zusätzlich zu einigen eindeutigen Parametern dupliziert dieser Befehl einige Parameter, die mithilfe eines TCP-Profils festgelegt werden können. Jede Aktualisierung dieser doppelten Parameter spiegelt sich im entsprechenden Parameter im Standard-TCP-Profil wider.

Wenn beispielsweise der SACK-Parameter mit diesem Ansatz aktualisiert wird, wird der Wert im SACK-Parameter des Standard-TCP-Profils (nstcp_default_profile) widergespiegelt.

> **Hinweis:**
>
> Citrix empfiehlt, diesen Ansatz nur für TCP-Parameter zu verwenden, die im Standard-TCP-Profil nicht verfügbar sind.

So konfigurieren Sie den globalen TCP-Befehl

- Geben Sie über die Befehlszeilenschnittstelle an der Eingabeaufforderung Folgendes ein:


```
set ns tcpParam …
<!--NeedCopy-->
```

- Navigieren Sie auf der GUI zu **System > Einstellungen**. Klicken Sie auf **TCP-Parameter ändern**, und aktualisieren Sie die erforderlichen TCP-Parameter.

TCP-Pufferungsfunktion

Citrix ADC bietet eine Funktion namens TCP-Pufferung, mit der Sie die TCP-Puffergröße angeben können. Die Funktion kann global oder auf Service-Ebene aktiviert werden.

> **Hinweis:**
>
> Die Puffergröße kann auch im Standard-TCP-Profil konfiguriert werden. Wenn die Puffergröße im TCP-Puffer-Feature und im Standard-TCP-Profil unterschiedliche Werte aufweist, wird der größere Wert angewendet.

So konfigurieren Sie die TCP-Pufferfunktion global

- Geben Sie in der Befehlszeile ein:

  enable ns mode TCPB

  ```
  set ns tcpbufParam -size <positiveInteger> -memLimit <positiveInteger>
  ```

- Navigieren Sie auf der GUI zu **System** > **Einstellungen**, klicken Sie auf **Modi konfigurieren** und wählen Sie **TCP-Pufferung**aus.

  Navigieren Sie zu **System** > **Einstellungen**, klicken Sie auf **TCP-Parameter ändern**, geben Sie Werte für **Puffergröße** und **Speicherauslastung** an.

Festlegen von Dienst- oder Virtual Server-spezifischen TCP-Parametern

Mithilfe von TCP-Profilen können Sie TCP-Parameter für Dienste und virtuelle Server angeben. Sie müssen ein TCP-Profil definieren (oder ein integriertes TCP-Profil verwenden) und das Profil mit dem entsprechenden Dienst und dem entsprechenden virtuellen Server verknüpfen.

> **Hinweis:**
>
> Sie können auch die TCP-Parameter von Standardprofilen gemäß Ihren Anforderungen ändern.

Sie können die TCP-Puffergröße auf Service-Ebene mit den durch die TCP-Pufferfunktion angegebenen Parametern angeben.

So geben Sie TCP-Konfigurationen auf Service- oder virtuelle Serverebene mit der Befehlszeilenschnittstelle an

Führen Sie an der Eingabeaufforderung folgende Schritte aus:

1. Konfigurieren Sie das TCP-Profil.

```
set ns tcpProfile <profile-name>...
<!--NeedCopy-->
```

2. Binden Sie das TCP-Profil an den Dienst oder den virtuellen Server.

```
    set service <name> ....
    <!--NeedCopy-->
```

Beispiel:

```
> set service service1 -tcpProfileName profile1
```

So binden Sie das TCP-Profil an den virtuellen Server:

```
set lb vserver <name> ....
<!--NeedCopy-->
```

Beispiel:

```
> set lb vserver lbvserver1 -tcpProfileName profile1
<!--NeedCopy-->
```

So geben Sie TCP-Konfigurationen auf Dienst- oder virtueller Serverebene mit der GUI an

Führen Sie an der GUI Folgendes aus:

1. Konfigurieren Sie das TCP-Profil.

   Navigieren Sie zu **System** > **Profile** > **TCP-Profile**und erstellen Sie das TCP-Profil.

2. Binden Sie das TCP-Profil an den Dienst oder den virtuellen Server.

   Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienste/Virtuelle Server**, und erstellen Sie das TCP-Profil, das an den Dienst oder den virtuellen Server gebunden sein sollte.

Integrierte TCP-Profile

Zur einfacheren Konfiguration bietet Citrix ADC einige integrierte TCP-Profile. Überprüfen Sie die im Folgenden aufgeführten integrierten Profile und wählen Sie ein Profil aus und verwenden Sie es so,

wie es ist, oder ändern Sie es so, dass es Ihren Anforderungen entspricht. Sie können diese Profile an Ihre erforderlichen Dienste oder virtuelle Server binden.

Eingebautes Profil	Beschreibung
nstcp_default_profile	Stellt die standardmäßigen globalen TCP-Einstellungen auf der Appliance dar.
nstcp_default_tcp_lan	Nützlich für Back-End-Serververbindungen, bei denen sich diese Server im selben LAN wie die Appliance befinden.
nstcp_default_WAN	nützlich für WAN-Bereitstellungen.
nstcp_default_tcp_lan_thin_stream	Ähnlich wie nstcp_default_tcp_lan profile. Die Einstellungen sind jedoch auf Paketflüsse kleiner Größe abgestimmt.
nstcp_default_tcp_interactive_stream	Ähnlich wie nstcp_default_tcp_lan profile. Es hat jedoch einen reduzierten verzögerten ACK-Timer und ACK bei **PUSH-Paketeinstellungen** .
nstcp_default_tcp_lfp	Nützlich für lange Fatpipe-Netzwerke (WAN) auf der Clientseite. Lange Fatpipe-Netzwerke haben lange Verzögerungen, Leitungen mit hoher Bandbreite mit minimalem Paketabfall.
nstcp_default_tcp_lfp_thin_stream	Ähnlich wie nstcp_default_tcp_lfp profile. Die Einstellungen sind jedoch auf Paketflüsse kleiner Größe abgestimmt.
nstcp_default_tcp_lnp	Nützlich für lange schmale Kanalnetze (WAN) auf der Clientseite. Lange schmale Kanalnetze weisen gelegentlich einen erheblichen Paketverlust auf.
nstcp_default_tcp_lnp_thin_stream	Ähnlich wie nstcp_default_tcp_lnp profile. Die Einstellungen sind jedoch auf Paketflüsse kleiner Größe abgestimmt.

Eingebautes Profil	Beschreibung
nstcp_internal_apps	Nützlich für interne Anwendungen auf der Appliance (z. B. GSLB-Sitesynchronisierung). Dies enthält abgestimmte Fensterskalierung und SACK-Optionen für die gewünschten Anwendungen. Dieses Profil sollte nicht an andere Anwendungen als interne Anwendungen gebunden sein.
nstcp_default_Mobile_profile	Nützlich für mobile Geräte.
nstcp_default_XA_XD_profile	Nützlich für die Bereitstellung von Citrix Virtual Apps and Desktops.

Beispiel für TCP-Konfigurationen

Beispiele für Beispielbeispiele für die Befehlszeilenschnittstelle zum Konfigurieren von folgenden

TCP gegen Spoofing-Angriffe verteidigen

Ermöglichen Sie dem Citrix ADC, TCP gegen Spoof-Angriffe zu verteidigen. Standardmäßig ist der Parameter "rstWindowtenuation" deaktiviert. Dieser Parameter ist aktiviert, um die Appliance vor Spoofing zu schützen. Wenn Sie aktivieren, antwortet es mit Korrekturbestätigung (ACK) auf eine ungültige Sequenznummer. Mögliche Werte sind Aktiviert, Deaktiviert.

Wo schützt der Parameter `RST` Fensterdämpfung das Gerät vor Spoofing. Wenn diese Option aktiviert ist, antworten Sie mit korrektiver ACK, wenn eine Sequenznummer ungültig ist

```
1      > set ns tcpProfile profile1 -rstWindowAttenuate ENABLED -
          spoofSynDrop ENABLED
2      Done
3      > set lb vserver lbvserver1 -tcpProfileName profile1
4      Done
5  <!--NeedCopy-->
```

Explicit Congestion Notification (ECN)

`Enable ECN on the required TCP profile`


```
    > set ns tcpProfile profile1 -ECN ENABLED
    Done
    > set lb vserver lbvserver1 -tcpProfileName profile1
    Done
<!--NeedCopy-->
```

Selektive Danksagung (SACK)

Aktivieren Sie SACK für das erforderliche TCP-Profil.

```
    > set ns tcpProfile profile1 -SACK ENABLED
    Done
    > set lb vserver lbvserver1 -tcpProfileName profile1
    Done
<!--NeedCopy-->
```

Bestätigung vorwärts (FACK)

Aktivieren Sie FACK für das erforderliche TCP-Profil.

```
> set ns tcpProfile profile1 -FACK ENABLED
> set lb vserver lbvserver1 -tcpProfileName profile1
<!--NeedCopy-->
```

Fensterskalierung (WS)

Aktivieren Sie die Fensterskalierung und legen Sie den Skalierungsfaktor für das gewünschte TCP-Profil fest.

```
set ns tcpProfile profile1  - WS ENABLED  - WSVal 9
Done
set lb vserver lbvserver1 -tcpProfileName profile1
Done
<!--NeedCopy-->
```


Maximale Segmentgröße (MSS)

Aktualisieren Sie die MSS-bezogenen Konfigurationen.

```
1 > set ns tcpProfile profile1  - mss 1460 - maxPktPerMss 512
2 Done
3 > set lb vserver lbvserver1 -tcpProfileName profile1
4 Done
5 <!--NeedCopy-->
```

Citrix ADC lernt das MSS eines virtuellen Servers

Aktivieren Sie Citrix ADC, um das VSS zu lernen und andere verwandte Konfigurationen zu aktualisieren.

```
1 > set ns tcpParam -learnVsvrMSS ENABLED  - mssLearnInterval 180 -
     mssLearnDelay 3600
2 Done
3 <!--NeedCopy-->
```

TCP Keep-Alive

Aktivieren Sie TCP Keep-Alive und aktualisieren Sie andere verwandte Konfigurationen.

```
> set ns tcpProfile profile1 -KA ENABLED -KaprobeUpdateLastactivity ENABLED
-KAconnIdleTime 900 -KAmaxProbes 3 -KaprobeInterval 75
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```

Puffergröße - mit TCP-Profil

Geben Sie die Puffergröße an.

```
> set ns tcpProfile profile1 -bufferSize 8190
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```


Puffergröße - Verwenden der TCP-Pufferfunktion

Aktivieren Sie die TCP-Pufferfunktion (global oder für einen Dienst) und geben Sie dann die Puffergröße und das Speicherlimit an.

```
> enable ns feature TCPB
Done
> set ns tcpbufParam -size 64 -memLimit 64
Done
```

MPTCP

Aktivieren Sie MPTCP und legen Sie dann die optionalen MPTCP-Konfigurationen fest.

```
> set ns tcpProfile profile1 -mptcp ENABLED
Done
> set ns tcpProfile profile1 -mptcpDropDataOnPreEstSF ENABLED -mptcpFastOpen
 ENABLED -mptcpSessionTimeout 7200
Done
> set ns tcpparam -mptcpConCloseOnPassiveSF ENABLED -mptcpChecksum ENABLED
-mptcpSFtimeout 0 -mptcpSFReplaceTimeout 10
-mptcpMaxSF 4 -mptcpMaxPendingSF 4 -mptcpPendingJoinThreshold 0 -mptcpRTOsToSwitchSF
 2 -mptcpUseBackupOnDSS ENABLED
Done
```

Überlastungskontrolle

Stellen Sie den erforderlichen Algorithmus zur TCP-Überlastungssteuerung ein.

```
set ns tcpProfile profile1 -flavor Westwood
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```

Dynamische Empfangspufferung

Aktivieren Sie die dynamische Empfangspufferung für das erforderliche TCP-Profil.

```
> set ns tcpProfile profile1 -dynamicReceiveBuffering ENABLED
Done
> set lb vserver lbvserver1 -tcpProfileName profile1
Done
```


Unterstützung für TCP Fast Open (TFO) in Multipath TCP (MPTCP)

Eine Citrix ADC-Appliance unterstützt jetzt den TCP Fast Open (TFO) -Mechanismus zum Herstellen von Multipath-TCP-Verbindungen (MPTCP) und zur Beschleunigung von Datenübertragungen. Der Mechanismus ermöglicht die Übertragung von Subflow-Daten während des anfänglichen MPTCP-Verbindungshandshake in SYN- und SYN-ACK-Paketen und ermöglicht auch die Verwendung von Daten durch den empfangenden Knoten während des Verbindungsaufbaus der MPTCP-Verbindung.

Weitere Informationen finden Sie unter Thema TCP Fast Open .

Unterstützung für variable TFO-Cookiegröße für MPTCP

Mit einer Citrix ADC-Appliance können Sie jetzt ein TCP-Fast Open (TFO) Cookie mit einer Mindestgröße von 4 Byte und einer maximalen Größe von 16 Byte in einem TCP-Profil konfigurieren. Auf diese Weise kann die Appliance mit der konfigurierten TFO-Cookie-Größe im SYN-ACK-Paket auf den Client reagieren.

So konfigurieren Sie das TCP-Fast Open (TFO) Cookie in einem TCP-Profil über die Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set tcpProfile nstcp_default_profile -tcpFastOpenCookieSize <positive_integer
>
```

Beispiel

```
set tcpProfile nstcp_default_profile -tcpFastOpenCookieSize 8
```

So konfigurieren Sie das TCP-Fast Open (TFO) Cookie in einem TCP-Profil über die grafische Benutzeroberfläche

1. Navigieren Sie zu **Konfiguration** > **System** > Profile.
2. Wechseln Sie im Detailbereich zur Registerkarte **TCP-Profile** und wählen Sie ein TCP-Profil aus.
3. Legen Sie auf der Seite **TCP-Profil konfigurieren** die Größe des **TCP-Fast Open-Cookies** fest.
4. Klicken Sie auf **OK** und **Fertig**.

Syn-Cookie-Zeitüberschreitungsintervall

Der Parameter `TCPSyncookie` ist in TCP-Profilen standardmäßig aktiviert, um einen robusten (RFC 4987) basierten Schutz vor SYN-Angriffen zu bieten. Wenn Sie benutzerdefinierte TCP-Clients aufnehmen müssen, die mit diesem Schutz nicht kompatibel sind, aber dennoch einen Fallback im Falle eines Angriffs sicherstellen möchten, wird dies für Sie von `synAttackDetection` erledigt, indem das `SYNCookie`-Verhalten automatisch intern für die vom Parameter `autosyncookietimeout` bestimmte Zeit aktiviert wird.

So konfigurieren Sie den maximalen Schwellenwert für SYN ACK-Neuübertragungen über die Befehlszeile:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1     set ns tcpparam [-maxSynAckRetx <positive_integer>]
2
3     Set ns tcpparam [-maxSynAckRetx 150]
4 <!--NeedCopy-->
```

So konfigurieren Sie das Timeout-Intervall des automatischen SYN-Cookies über die Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns tcpparam [-autosyncookietimeout <positive_integer>]
```

```
Set ns tcpparam [-autosyncookietimeout 90]
```

Delink Client- und Serververbindung

Wenn diese Option aktiviert ist, löscht der Parameter die Client- und Serververbindung, wenn noch ausstehende Daten an die andere Seite gesendet werden sollen. Standardmäßig ist der Parameter deaktiviert.

```
1 set ns tcpparam -delinkClientServerOnRST ENABLED
2 Done
3
4 <!--NeedCopy-->
```

HTTP-Konfigurationen

January 28, 2022

> **Wichtig:**
>
> Ab Citrix ADC Release 13.0 Build 71.x kann eine Citrix ADC-Appliance HTTP-Anfragen mit großen Header-Größen verarbeiten, um die L7-Anwendungsanforderungen zu erfüllen. Die Header-Größe kann bis zu 128 KB konfigurierbar sein.

HTTP-Konfigurationen für eine Citrix ADC-Appliance können in einer Entität angegeben werden, die als HTTP-Profil bezeichnet wird, bei der es sich um eine Sammlung von HTTP-Einstellungen handelt.

Das HTTP-Profil kann dann mit Diensten oder virtuellen Servern verknüpft werden, die diese HTTP-Konfigurationen verwenden möchten.

Ein Standard-HTTP-Profil kann konfiguriert werden, um die standardmäßig angewendeten HTTP-Konfigurationen global auf alle Dienste und virtuellen Server festzulegen.

> **Hinweis:**
>
> Wenn ein HTTP-Parameter unterschiedliche Werte für Service, virtuellen Server und global aufweist, erhält der Wert der spezifischsten Entität (des Dienstes) die höchste Priorität.

Die Citrix ADC-Appliance bietet auch andere Ansätze zur Konfiguration von HTTP. Lesen Sie weiter für weitere Informationen.

Der Citrix ADC unterstützt ein WebSocket-Protokoll, das es Browsern und anderen Clients ermöglicht, eine bidirektionale Vollduplex-TCP-Verbindung zu den Servern herzustellen. Die Citrix ADC-Implementierung von WebSocket ist RFC 6455 konform.

> **Hinweis:**
>
> Eine Citrix ADC-Appliance unterstützt jetzt die Adresskonfiguration der USIP (USIP) für HTTP/1.1- und HTTP/2-Protokolle.

Einstellen globaler HTTP-Parameter

Mit der Citrix ADC-Appliance können Sie Werte für HTTP-Parameter angeben, die für alle Citrix ADC-Dienste und virtuellen Server gelten. Dies kann geschehen mit:

- Standard-HTTP-Profil
- Globaler HTTP-Befehl

Standard-HTTP-Profil

Ein HTTP-Profil, das als nshttp_default_profile bezeichnet wird, wird verwendet, um HTTP-Konfigurationen anzugeben, die verwendet werden, wenn keine HTTP-Konfigurationen auf Service- oder virtuelle Serverebene bereitgestellt werden.

> **Hinweise:**
>
> - Nicht alle HTTP-Parameter können über das Standard-HTTP-Profil konfiguriert werden. Einige Einstellungen werden mit dem globalen HTTP-Befehl vorgenommen (siehe folgenden Abschnitt).
> - Das Standardprofil muss nicht explizit an einen Dienst oder einen virtuellen Server gebunden sein.

So konfigurieren Sie das Standard-HTTP-Profil

- Geben Sie über die Befehlszeilenschnittstelle an der Eingabeaufforderung Folgendes ein:

  ```
  set ns httpProfile nshttp_default_profile …
  ```

- Navigieren Sie auf der GUI zu **System** > **Profile**, klicken Sie auf **HTTP-Profile** und aktualisieren Sie nshttp_default_profile.

Globaler HTTP-Befehl

Ein anderer Ansatz, mit dem Sie globale HTTP-Parameter konfigurieren können, ist der globale HTTP-Befehl. Zusätzlich zu einigen eindeutigen Parametern dupliziert dieser Befehl einige Parameter, die mithilfe eines HTTP-Profils festgelegt werden können. Jede Aktualisierung dieser doppelten Parameter spiegelt sich im entsprechenden Parameter im Standard-HTTP-Profil wider.

Wenn beispielsweise der MaxReusePool-Parameter mit diesem Ansatz aktualisiert wird, wird der Wert im MaxReusePool-Parameter des Standard-HTTP-Profils (nshttp_default_profile) widergespiegelt.

> **Hinweis:**
>
> Citrix empfiehlt, diesen Ansatz nur für HTTP-Parameter zu verwenden, die im Standard-HTTP-Profil nicht verfügbar sind.

So konfigurieren Sie den globalen HTTP-Befehl

- Geben Sie über die Befehlszeilenschnittstelle an der Eingabeaufforderung Folgendes ein:

  ```
  set ns httpParam …
  ```

- Navigieren Sie auf der GUI zu **System > Einstellungen**, klicken Sie auf **HTTP-Parameter ändern** und aktualisieren Sie die erforderlichen HTTP-Parameter.

So konfigurieren Sie ein Ignorieren-Codierungsschema für Connect-Anfrage

Um HTTP/2 zu aktivieren und HTTP/2-Parameter so festzulegen, dass das Codierungsschema in der Verbindungsanforderung ignoriert wird, geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns httpParam [-ignoreConnectCodingScheme ( ENABLED | DISABLED )]
```

Beispiel:

```
set ns httpParam -ignoreConnectCodingScheme ENABLED
```

So binden Sie das HTTP-Profil mithilfe der Citrix ADC-Befehlszeile an einen virtuellen Server

Konfigurieren Sie das HTTP-Profil zum Löschen von ungültigen TRACE- oder TRACK-Anfragen

Sie können den markTraceReqInval-Parameter aktivieren, um TRACK- und TRACK-Anfragen als ungültig zu markieren. Wenn Sie diese Option zusammen mit der Option dropInvalidReqs für

die virtuelle IP-Adresse aktivieren, können Sie einen Client zurücksetzen, der TRACE- oder TRACK-Anfragen an eine Citrix ADC-Appliance sendet.

So konfigurieren Sie das HTTP-Profil mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns httpProfile <profile name> [-markTraceReqInval ENABLED | DISABLED ]
```

Beispiel:

```
set ns httpProfile profile1 -markTraceReqInval ENABLED
```

Konfigurieren des HTTP-Profils für eine Dienstgruppe

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add serviceGroup <serviceGroupName>@ <serviceType> [-cacheType <
     cacheType>] [-td <positive_integer>] [-maxClient <positive_integer>]
      [-maxReq <positive_integer>] [-cacheable ( YES | NO )] [-cip (
     ENABLED | DISABLED ) [<cipHeader>]] [-usip ( YES | NO )] [-
     pathMonitor ( YES | NO )] [-pathMonitorIndv ( YES | NO )] [-
     useproxyport ( YES | NO )] [-healthMonitor ( YES | NO )] [-sp ( ON |
      OFF )] [-rtspSessionidRemap ( ON | OFF )] [-cltTimeout <secs>] [-
     svrTimeout <secs>] [-CKA ( YES | NO )] [-TCPB ( YES | NO )] [-CMP (
     YES | NO )] [-maxBandwidth
2 <positive_integer>] [-monThreshold <positive_integer>] [-state ENABLED
     DISABLED )][-downStateFlush ( ENABLED | DISABLED )] [-tcpProfileName
      <string>] [-httpProfileName <string>] [-comment <string>] [-
     appflowLog ( ENABLED | DISABLED )] [-netProfile <string>] [-
     autoScale <autoScale> -memberPort <port> [-autoDisablegraceful ( YES
      | NO )] [-autoDisabledelay <secs>] ] [-monConnectionClose ( RESET |
      FIN )]
3
4 <!--NeedCopy-->
```

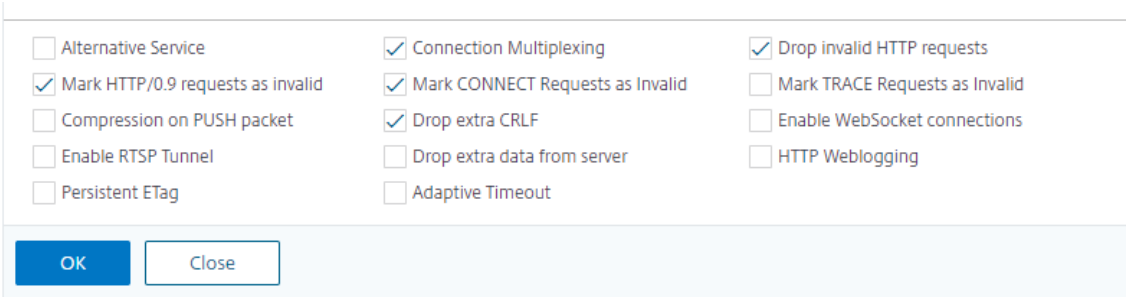
Beispiel:

```
add serviceGroup Service-Group-1 HTTP -maxClient 0 -maxReq 0 -cip ENABLED -
usip NO -useproxyport YES -cltTimeout 200 -svrTimeout 300 -CKA NO -TCPB NO
-CMP NO -httpProfileName profile1
```

Konfigurieren Sie das HTTP-Profil mit der Citrix ADC GUI

Führen Sie das folgende Verfahren aus, um TRACE oder TRACK ungültige Anfragen zu markieren.

1. Melden Sie sich bei der Citrix ADC-Appliance an und navigieren Sie zu **Konfiguration** > **System** > **Profile**.
2. Klicken Sie auf der Registerkarte **HTTP-Profile** auf **Hinzufügen**.
3. Wählen Sie auf der Seite **HTTP-Profil erstellen** die Option **TRACE-Anfragen als ungültig markieren** aus.
4. Klicken Sie auf **Erstellen**.



Festlegen von dienst- oder virtuellen serverspezifischen HTTP-Parametern

Mithilfe von HTTP-Profilen können Sie HTTP-Parameter für Dienste und virtuelle Server angeben. Sie müssen ein HTTP-Profil definieren (oder ein integriertes HTTP-Profil verwenden) und das Profil mit dem entsprechenden Dienst und dem entsprechenden virtuellen Server verknüpfen.

> **Hinweis:**
>
> Sie können auch die HTTP-Parameter von Standardprofilen gemäß Ihren Anforderungen ändern.

So geben Sie HTTP-Konfigurationen auf Service- oder virtuelle Serverebene mit der Befehlszeilenschnittstelle an

Führen Sie an der Eingabeaufforderung folgende Schritte aus:

1. Konfigurieren Sie das HTTP-Profil.

   ```
   set ns httpProfile <profile-name>...
   ```

2. Binden Sie das HTTP-Profil an den Dienst oder den virtuellen Server.

   So binden Sie das HTTP-Profil an den Dienst:

```
set service <name> .....
```

Beispiel:

```
1 > set service service1 -httpProfileName profile1
2 <!--NeedCopy-->
```


So binden Sie das HTTP-Profil an den virtuellen Server:

```
set lb vserver <name> .....
```

Beispiel:

```
1 > set lb vserver lbvserver1 -httpProfileName profile1
2 <!--NeedCopy-->
```

So geben Sie HTTP-Konfigurationen auf Dienstebene oder virtuelle Serverebene mit der GUI an

Führen Sie an der GUI Folgendes aus:

1. Konfigurieren Sie das HTTP-Profil.

   Navigieren Sie zu **System** > **Profile** > **HTTP-Profile** und erstellen Sie das HTTP-Profil.

2. Binden Sie das HTTP-Profil an den Dienst oder den virtuellen Server.

   Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Dienste/Virtuelle Server** und erstellen Sie das HTTP-Profil, das an den Service/virtuellen Server gebunden sein muss.

Integrierte HTTP-Profile

Zur Vereinfachung der Konfiguration bietet der Citrix ADC einige integrierte HTTP-Profile. Überprüfen Sie die aufgelisteten Profile und verwenden Sie sie so, wie es ist, oder ändern Sie sie an Ihre Anforderungen. Sie können diese Profile an die erforderlichen Dienste oder virtuellen Server binden.

Eingebautes Profil	Beschreibung
nshttp_default_profile	Stellt die standardmäßigen globalen HTTP-Einstellungen auf der Appliance dar.
nshttp_default_strict_validation	Einstellungen für Bereitstellungen, die eine strikte Validierung von HTTP-Anfragen und -Antworten erfordern.

Beispiel für HTTP-Konfigurationen

Beispiele für Beispiele für eine Befehlszeilenschnittstelle, um Folgendes zu konfigurieren:

- HTTP-Band-Statistiken
- WebSocket-Verbindungen

HTTP-Band-Statistiken

Geben Sie die Bandgröße für HTTP-Anfragen und -Antworten an.

```
> set protocol httpBand reqBandSize 300 respBandSize 2048
Done
> show protocol httpband -type REQUEST
<!--NeedCopy-->
```

WebSocket-Verbindungen

Aktivieren Sie WebSocket für das erforderliche HTTP-Profil.

```
> set ns httpProfile http_profile1 -webSocket ENABLED
Done
> set lb vserver lbvserver1 -httpProfileName profile1
Done
<!--NeedCopy-->
```

HTTP/2-Konfiguration

January 25, 2022

Hinweis: Die HTTP/2-Funktionalität wird von den Citrix ADC MPX-, VPX- und SDX-Modellen unterstützt. In einer Citrix ADC VPX-Appliance wird die HTTP/2-Funktionalität ab Citrix ADC Version 11.0 unterstützt.

Das Problem mit der Leistung von Webanwendungen hängt direkt mit dem Trend zur Erhöhung der Seitengröße und der Anzahl der Objekte auf den Webseiten zusammen. HTTP/1.1 wurde entwickelt, um kleinere Webseiten, langsamere Internetverbindungen und eingeschränktere Serverhardware als heute üblich zu unterstützen. Es ist nicht für neue Technologien wie JavaScript und Cascading Stylesheets (CSS) oder neue Medientypen wie Flash-Videos und grafikreiche Bilder geeignet. Dies liegt daran, dass nur eine Ressource pro Verbindung zum Server angefordert werden kann. Die Einschränkung erhöht die Anzahl der Roundtrips erheblich, was zu einem längeren Seitenrendern und einer verringerten Netzwerkleistung führt.

Das HTTP/2-Protokoll behebt diese Einschränkungen, indem es die Kommunikation mit weniger über das Netzwerk übertragenen Daten ermöglicht und die Möglichkeit bietet, mehrere Anfragen und Antworten über eine einzige Verbindung zu senden. Im Kern behebt HTTP/2 die wichtigsten

Einschränkungen von HTTP/1.1, indem die zugrunde liegenden Netzwerkverbindungen effizienter genutzt werden. Es verändert die Art und Weise, wie Anfragen und Antworten über das Netzwerk übertragen werden.

HTTP/2 ist ein binäres Protokoll. Es ist effizienter zu analysieren, kompakter auf dem Kabel und vor allem weniger fehleranfällig im Vergleich zu Textprotokollen wie HTTP/1.1. Das HTTP/2-Protokoll verwendet eine binäre Framing-Schicht, die den Frame-Typ und die Art und Weise definiert, wie HTTP-Nachrichten eingekapselt und zwischen Client und Server übertragen werden. Die HTTP/2-Funktionalität unterstützt die Verwendung der CONNECT-Methode zum Herstellen einer Tunnelverbindung über einen einzelnen HTTP/2-Stream zu einem Remote-Host.

Das HTTP/2-Protokoll enthält viele leistungssteigernde Änderungen, die die Leistung erheblich verbessern, insbesondere für Clients, die sich über ein Mobilfunknetz verbinden.

In der folgenden Tabelle sind die wichtigsten Verbesserungen in HTTP/2 gegenüber HTTP/1.1 aufgeführt:

HTTP/2-Funktionen	Beschreibung
Kopfzeilenkomprimierung	HTTP-Header haben viele sich wiederholende Informationen und verbrauchen daher unnötige Bandbreite während der Datenübertragung. HTTP/2 reduziert die Bandbreitenanforderungen, indem der Header komprimiert und die Anforderung minimiert wird, HTTP-Header mit jeder Anforderung und Antwort zu transportieren.
Verbindungs-Multiplexing	Die Latenz kann einen enormen Einfluss auf die Ladezeiten der Seite und die Benutzererfahrung haben. Das Verbindungsmultiplexing überwindet dieses Problem, indem mehrere Anfragen und Antworten über eine einzige Verbindung gesendet werden.

HTTP/2-Funktionen	Beschreibung
Server-Push	Server-Push ermöglicht es dem Server, Inhalte proaktiv an den Client-Browser zu übertragen, wodurch Roundtrip-Verzögerungen vermieden werden. Diese Funktion speichert die Antworten, die der Kunde benötigt, im Cache, reduziert die Anzahl von Roundtrips und verbessert die Seitenrendering-Zeit. Wichtig: Die Citrix ADC-Appliance unterstützt die Server-Push-Funktionalität nicht.
Keine Kopf-of-Line-Blockierung	Unter HTTP 1.1 können Browser pro Verbindung jeweils eine Ressource herunterladen. Wenn ein Browser eine große Ressource herunterladen muss, blockiert er alle anderen Ressourcen, bis der erste Download abgeschlossen ist. HTTP/2 überwindet dieses Problem mit einem Multiplexing-Ansatz. Es ermöglicht dem Client-Browser, andere Webkomponenten parallel über dieselbe Verbindung herunterzuladen und anzuzeigen, sobald sie verfügbar sind.

HTTP/2-Funktionen	Beschreibung
Priorisierung anfordern	Nicht alle Ressourcen haben die gleiche Priorität, wenn der Browser eine Webseite rendert. Um die Ladezeit zu beschleunigen, priorisieren alle modernen Browser Anfragen nach Art des Assets, ihrem Standort auf der Seite und sogar nach erlernter Priorität aus früheren Besuchen. Mit HTTP/1.1 kann der Browser die Prioritätsdaten nur eingeschränkt verwenden, da dieses Protokoll kein Multiplexing unterstützt und es keine Möglichkeit gibt, die Anforderungspriorisierung durch den Server zu kommunizieren. Das Ergebnis ist eine unnötige Netzwerklatenz. HTTP/2 überwindet dieses Problem, indem es dem Browser erlaubt, alle Anfragen zu versenden. Der Browser kann seine Präferenz für die Stream-Priorisierung über Stream-Abhängigkeiten und Gewichte kommunizieren, wodurch die Server die Antwortbereitstellung optimieren können. Wichtig: Die Citrix ADC-Appliance unterstützt die Funktion zur Anforderungspriorisierung nicht.

So funktioniert HTTP/2

Eine Citrix ADC-Appliance unterstützt HTTP/2 sowohl clientseitig als auch serverseitig. Auf der Clientseite fungiert die Citrix ADC-Appliance als Server, der einen virtuellen HTTP/HTTPS-Server für HTTP/2 hostet. Auf der Back-End-Seite fungiert der Citrix ADC als Client für die Server, die an den virtuellen Server gebunden sind.

Daher unterhält die Citrix ADC-Appliance separate Verbindungen sowohl auf der Clientseite als auch auf der Serverseite. Die Citrix ADC-Appliance verfügt über separate HTTP/2-Konfigurationen für die Client- und Serverseite.

HTTP/2 für HTTPS (SSL) -Lastausgleichskonfiguration

Für eine HTTPS-Lastausgleichskonfiguration verwendet die Citrix ADC-Appliance die TLS ALPN-Erweiterung (RFC 7301), um festzustellen, ob der Client/Server HTTP/2 unterstützt. Wenn dies der Fall ist, wählt die Appliance HTTP/2 als Protokoll der Anwendungsschicht, um Daten (wie in RFC 7540 - Abschnitt 3.3 beschrieben) auf der Client-/Serverseite zu übertragen.
Die Appliance verwendet bei der Auswahl des Anwendungsschicht-Protokolls über die TLS-ALPN-Erweiterung die folgende Präferenzreihenfolge:

- HTTP/2 (falls im HTTP-Profil aktiviert)
- SPDY (falls im HTTP-Profil aktiviert)
- HTTP/1.1

HTTP/2 für die Konfiguration des HTTP-Lastausgleichs

Für eine HTTP-Lastausgleichskonfiguration verwendet die Citrix ADC-Appliance eine der folgenden Methoden, um mit dem Client/Server über HTTP/2 zu kommunizieren.

> **Hinweis:**
>
> In den folgenden Methodenbeschreibungen sind Client und Server allgemeine Begriffe für eine HTTP/2-Verbindung. Beispielsweise fungiert die Citrix ADC-Appliance für ein Lastausgleichs-Setup einer Citrix ADC-Appliance mit HTTP/2 als Server auf der Clientseite und fungiert als Client für die Serverseite.

- **HTTP/2-Upgrade**. Ein Client sendet eine HTTP/1.1-Anfrage an einen Server. Die Anforderung enthält einen Upgrade-Header, der den Server auffordert, die Verbindung auf HTTP/2 zu aktualisieren. Wenn der Server HTTP/2 unterstützt, akzeptiert der Server die Upgrade-Anforderung und benachrichtigt ihn in seiner Antwort. Der Client und der Server beginnen mit der Kommunikation über HTTP/2, nachdem der Client die Upgrade-Bestätigungsantwort erhalten hat.
- **Direkt HTTP/2**. Ein Client beginnt direkt mit einem Server in HTTP/2 zu kommunizieren, anstatt die HTTP/2-Upgrade-Methode zu verwenden. Wenn der Server HTTP/2 nicht unterstützt oder nicht für die direkte Annahme von HTTP/2-Anfragen konfiguriert ist, löscht er die HTTP/2-Pakete vom Client. Diese Methode ist hilfreich, wenn der Administrator des Clientgeräts bereits weiß, dass der Server HTTP/2 unterstützt.
- **Direkte HTTP/2 mithilfe des alternativen Dienstes (ALT-SVC).** Ein Server kündigt an, dass er HTTP/2 für einen Client unterstützt, indem er ein Feld für den alternativen Dienst (ALT-SVC) in seine HTTP/1.1-Antwort einschließt. Wenn der Client so konfiguriert ist, dass er das Feld ALT-SVC versteht, beginnen der Client und der Server direkt über HTTP/2 zu kommunizieren, nachdem der Client die Antwort erhalten hat.

Die Citrix ADC-Appliance bietet konfigurierbare Optionen in einem HTTP-Profil für die HTTP/2-Methoden. Diese HTTP/2-Optionen können sowohl auf die Clientseite als auch auf die Serverseite

eines HTTPS- oder HTTP-Lastausgleichs angewendet werden. Weitere Informationen zu HTTP/2-Methoden und Optionen finden Sie im PDF-Format HTTP/2-Optionen .

Bevor Sie beginnen

Beachten Sie die folgenden Punkte, bevor Sie mit der Konfiguration von HTTP/2 auf einer Citrix ADC-Appliance beginnen:

- Die Citrix ADC-Appliance unterstützt HTTP/2 sowohl clientseitig als auch serverseitig.
- Die Citrix ADC-Appliance unterstützt die HTTP/2-Server-Push-Funktionalität nicht.
- Die Citrix ADC-Appliance unterstützt die HTTP/2-Anforderungspriorisierungsfunktion nicht.
- Die Citrix ADC-Appliance unterstützt keine HTTP/2-SSL-Neuverhandlung für HTTPS-Lastausgleichseinrichtun
- Die Citrix ADC-Appliance unterstützt keine HTTP/2-NTLM-Authentifizierung.
- Wenn HTTP/2 aktiviert ist, Verbindungsmultiplexing deaktiviert (wie USIP aktiviert) und Eins-zu-Eins-Zuordnung von Client- und Server-TCP-Verbindungen werden Close-Ereignisse wie FIN, Reset (RST) von der Client- oder Serververbindung zur verknüpften Peer-Verbindung weitergeleitet.

Konfigurieren von HTTP/2

Die Konfiguration von HTTP/2 für ein Lastausgleichs-Setup (HTTPS oder HTTP) umfasst die folgenden Aufgaben:

- **Aktivieren Sie HTTP/2 und setzen Sie optionale HTTP/2-Parameter in einem HTTP-Profil**. Aktivieren Sie HTTP/2 in einem HTTP-Profil. Wenn Sie nur HTTP/2 in einem HTTP-Profil aktivieren, verwendet die Citrix ADC-Appliance nur die Upgrade-Methode (für HTTP) oder die TLS-ALPN-Methode (für HTTPS) für die Kommunikation in HTTP/2.

  Damit die Citrix ADC-Appliance die direkte HTTP/2-Methode verwenden kann, muss die Option **Direct HTTP/2** im HTTP-Profil aktiviert sein. Damit die Citrix ADC-Appliance das direkte HTTP/2 mit der alternativen Dienstmethode verwenden kann, muss die Option **Alternativer Dienst (altsvc)** im HTTP-Profil aktiviert sein.

- **Binden Sie das HTTP-Profil an einen virtuellen Server oder einen Dienst**. Binden Sie das HTTP-Profil an einen virtuellen Server, um HTTP/2 für die Clientseite des Lastausgleichs-Setups zu konfigurieren. Binden Sie das HTTP-Profil an einen Dienst, um HTTP2 für die Serverseite des Lastausgleichs-Setups zu konfigurieren.

> **Hinweis:**
>
> Citrix empfiehlt, separate HTTP-Profile für die Client- und Serverseite zu binden.

- **Aktivieren Sie den globalen Parameter für die serverseitige Unterstützung von HTTP/2**. Aktivieren Sie den globalen **HTTP-Parameter HTTP/2 Service Side(Http2ServerSide**), um die

HTTP/2-Unterstützung auf der Serverseite aller Lastausgleichseinrichtungen zu aktivieren, die HTTP/2 konfiguriert haben.

HTTP/2 funktioniert auf der Serverseite von Lastausgleichseinrichtungen nicht, wenn **HTTP/2 Service Side** deaktiviert ist, selbst wenn **HTTP/2 im HTTP-Profil** aktiviert ist, das an die zugehörigen Lastausgleichsdienste gebunden ist.

Citrix ADC-Befehlszeilenprozeduren:

So aktivieren Sie HTTP/2 und legen HTTP/2-Parameter mithilfe der Citrix ADC-Befehlszeile fest

- Um HTTP/2 zu aktivieren und HTTP/2-Parameter beim Hinzufügen eines HTTP-Profils festzulegen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )] [-altsvc ( ENABLED | DISABLED )]
show ns httpProfile <name>
```

- Um HTTP/2 zu aktivieren und HTTP/2-Parameter festzulegen, während Sie ein HTTP-Profil ändern, geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns httpProfile <name> -http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED)] [-altsvc (ENABLED | DISABLED )]
show ns httpProfile <name>
```

So binden Sie das HTTP-Profil mithilfe der Citrix ADC-Befehlszeile an einen virtuellen Server

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> - httpProfileName <string>
show lb vserver <name>
```

So binden Sie das HTTP-Profil mithilfe der Citrix ADC-Befehlszeile an einen Lastausgleichsdienst

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -httpProfileName <string>
show service <name>
```

So aktivieren Sie die HTTP/2-Unterstützung global auf der Serverseite mithilfe der Citrix ADC-Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns httpParam -HTTP2Serverside( ENABLED | DISABLED )
show ns httpParam
```

So aktivieren Sie HTTP/2 und legen Sie HTTP/2-Parameter über die Citrix ADC GUI fest

1. Navigieren Sie zu **System** > **Profile**und klicken Sie auf die Registerkarte **HTTP-Profile** .

2. Aktivieren Sie **HTTP/2**, während Sie ein HTTP-Profil hinzufügen oder ein vorhandenes HTTP-Profil ändern.

So binden Sie das HTTP-Profil über die Citrix ADC GUI an einen virtuellen Server

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, und öffnen Sie den virtuellen Server.
2. Klicken Sie in den **Erweiterten Einstellungen**auf **+ HTTP-Profil**, um das erstellte HTTP-Profil an den virtuellen Server zu binden.

So binden Sie das HTTP-Profil über die Citrix ADC GUI an einen Lastausgleichsdienst

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Service**, und öffnen Sie den Dienst.
2. Klicken Sie in den **Erweiterten Einstellungen**auf **+ HTTP-Profil**, um das erstellte HTTP-Profil an den Dienst zu binden.

So aktivieren Sie die HTTP/2-Unterstützung global auf der Serverseite über die GUI

Navigieren Sie zu **System** > **Einstellungen**, klicken Sie auf **HTTP-Parameter ändern** und aktivieren Sie **HTTP/2 Serverseite**.

Beispielkonfigurationen

In der folgenden Beispielkonfiguration ist HTTP/2 und direktes HTTP/2 im HTTP-Profil HTTP-PROFILE-HTTP2-CLIENT-SIDE aktiviert. Das Profil ist an den virtuellen Server LB-VS-1 gebunden.

```
set ns httpProfile HTTP-PROFILE-HTTP2-CLIENT-SIDE -http2 enabled -
   http2Direct enabled
Done

set lb vserver LB-VS-1 -httpProfileName HTTP-PROFILE-HTTP2-CLIENT-SIDE

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

In der folgenden Beispielkonfiguration ist HTTP/2 und alternativer Dienst (ALT-SVC) im HTTP-Profil HTTP-PROFILE-HTTP2-SERVER-SIDE aktiviert. Das Profil ist an Service LB-SERVICE-1 gebunden.

```
set ns httpparam -HTTP2Serverside ENABLED
Done

set ns httpProfile HTTP-PROFILE-HTTP2-SERVER-SIDE -http2 ENABLED -
   altsvc ENABLED
```



```
5 Done
6
7 set service LB-SERVICE-1 -httpProfileName HTTP-PROFILE-HTTP2-SERVER-
     SIDE
8 Done
9 <!--NeedCopy-->
```

Konfigurieren Sie die Fenstergröße des HTTP/2-Erstverbindungs

Gemäß RFC 7540 muss das Flusssteuerungsfenster für den HTTP2-Stream und die Verbindung auf 64 K (65535) Oktette eingestellt sein, und jede Änderung an diesem Wert muss dem Peer mitgeteilt werden. Die ADC-Appliance kommuniziert die Änderung der Fenstergröße der Durchflusssteuerung wie folgt:

- Verwenden des `SETTINGS` Frames für den Stream.
- Verwenden des `WINDOW_UPDATE` Rahmens für die Verbindung.

In einem HTTP-Profil müssen Sie den `http2InitialWindowSize` Parameter so konfigurieren, dass die anfängliche Fenstergröße auf Stream-Ebene festgelegt wird. Aufgrund eines internen Systemfehlers initialisiert die ADC-Appliance auch das Flow-Control-Fenster für die Verbindung. Wenn sich das konfigurierte Flow-Steuerungsfenster für den Stream ändert, kommuniziert die ADC-Appliance über den Rahmen SETTINGS mit dem Peer. Die ADC-Appliance kommuniziert jedoch die Änderung des Flow-Steuerungsfensters für die Verbindung über den `WINDOW_UPDATE` Rahmen nicht. Dies führt zu einem Einfrieren der Verbindung.

Um das Problem zu beheben, wird nun der `http2InitialConnWindowSize` Parameter (in Byte) hinzugefügt, um das Flow-Steuerfenster für die Verbindung zu steuern. Mithilfe separater konfigurierbarer Parameter können Sie der Appliance jetzt ermöglichen, Updates für die geänderte Fenstergröße sowohl auf Stream- als auch auf Verbindungsebene zu senden.

Konfigurieren Sie den Größenparameter für das erste Verbindungsfenster HTTP/2 mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set http profile p1 -http2InitialConnWindowSize 8290
2 Initial window size for stream level flow control, in bytes.
3 Default value: 65535
4 Minimum value: 8192
5 Maximum value: 20971520
6 <!--NeedCopy-->
```


HTTP/2 DoS-Abschwächung

October 5, 2021

Die Http/2 Denial-of-Service (DoS) -Angriffe haben keine Auswirkungen mehr auf eine Citrix ADC Appliance. Wenn die Appliance Frames empfängt, die mehr als das Maximallimit überschreiten, schließt die Appliance die Verbindung automatisch.

Um Angriffe zu mildern, können Sie mithilfe des HTTP-Profils die Standardkonfiguration von Frames ändern, die in einer HTTP/2-Verbindung empfangen werden.

Die Tabelle der HTTP/2 DoS-Abschwächung zeigt die Liste der HTTP/2-DoS-Angriffe und deren Abschwächung.

Konfigurieren der Maximalgrenze für HTTP/2-Frames zur Minderung von DoS-Angriffen mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns httpprofile <profile_name> - http2MaxEmptyFramesPerMin <positive_integer
> -http2MaxPingFramesPerMin <positive_integer> -http2MaxSettingsFramesPerMin
 <positive_integer> -http2MaxResetFramesPerMin <positive_integer>
```

Beispiel:

```
set ns httpprofile profile1 -http2MaxEmptyFramesPerMin 20 -http2MaxPingFramesPerMin
 20 -http2MaxSettingsFramesPerMin 20 -http2MaxResetFramesPerMin 20
```

Konfigurieren der Höchstgrenze für Frames, die in einer HTTP/2-Verbindung empfangen werden, mit der Citrix ADC GUI

Führen Sie die folgenden Schritte aus, um das Maximallimit für Frames zu konfigurieren, die in einer HTTP/2-Verbindung empfangen wurden:

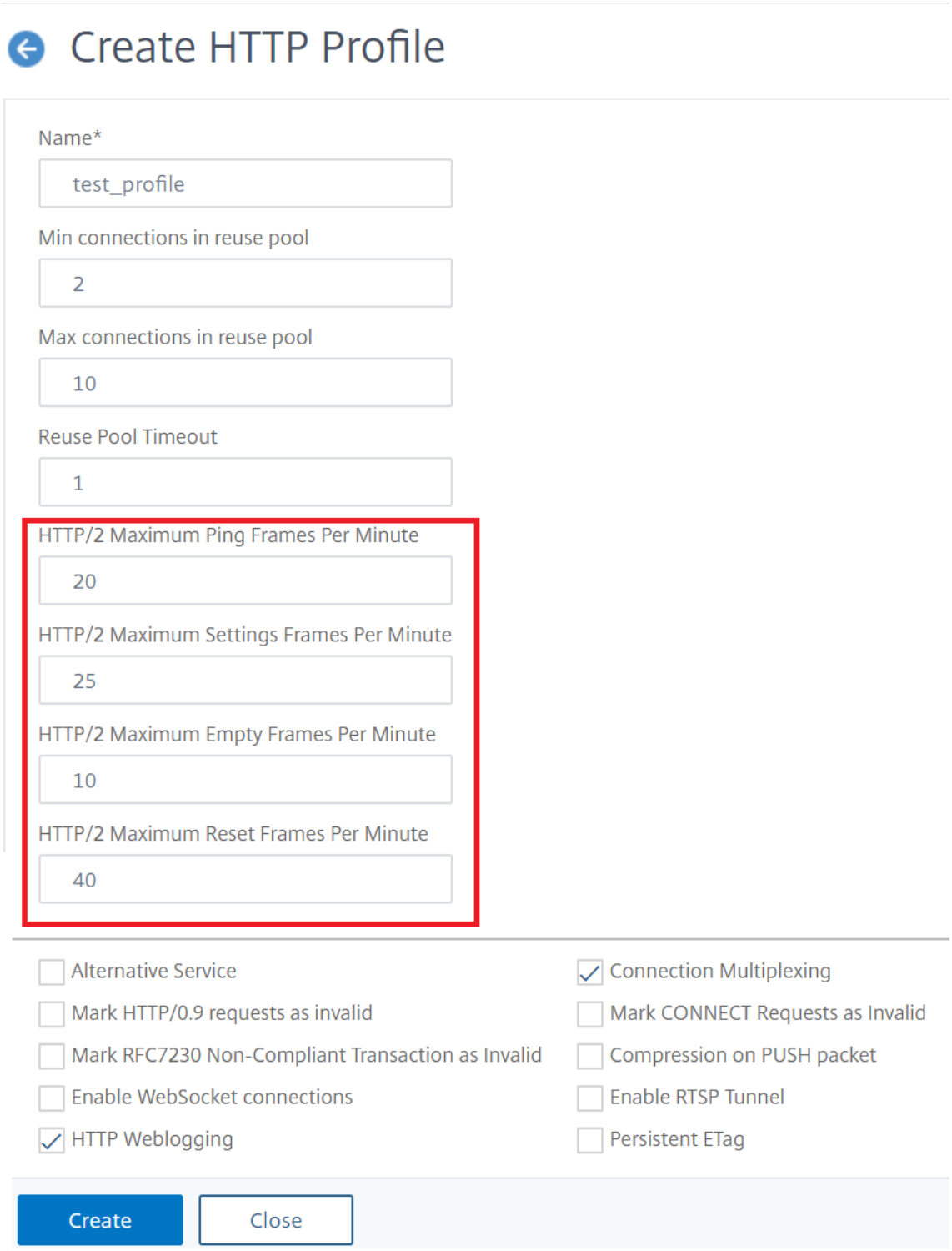
1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Profile** .
2. Wählen Sie auf der Seite **Profil** die Registerkarte **HTTP-Profile** .
3. Klicken Sie auf der Registerkarte **HTTP-Profile** auf **Hinzufügen**.
4. **Legen Sie auf der Seite HTTP-Profil konfigurieren** den folgenden Parameter fest.
    a) http2MaxPingFramesPerMin. Legen Sie die maximal pro Verbindung empfangenen Ping-Frames in einer Minute fest. Wenn die Anzahl der PING-Frames die Konfigurationsgrenze überschreitet, löscht die Appliance automatisch Pakete auf der Verbindung.

b) http2MaxSettingsFramesPerMin. Stellen Sie die maximalen SETTINGS-Frames pro Verbindung in einer Minute ein. Wenn die Anzahl der SETTINGS-Frames die Konfigurationsgrenze überschreitet, löscht ADC automatisch Pakete aus der Verbindung.

c) http2MaxResetFramesPerMin. Stellen Sie die maximalen RESET Frames pro Verbindung in einer Minute ein. Wenn die Anzahl der RESET Frames die Konfigurationsgrenze überschreitet, löscht ADC automatisch Pakete auf der Verbindung.

d) http2MaxEmptyFramesPerMin. Legen Sie die maximalen leeren Frames pro Verbindung in einer Minute fest. Wenn die Anzahl der leeren Frames die Konfigurationsgrenze überschreitet, löscht ADC automatisch Pakete auf der Verbindung.

5. Klicken Sie auf **OK** und **schließen**.



HTTP3 über QUIC-Protokoll

October 5, 2021

HTTP/2 über TCP ist der bevorzugte Standard für das Senden mehrerer Streams von HTTP-Anfragen über eine einzige Verbindung. Im TCP-Transportmechanismus gibt es jedoch gewisse Einschränkungen und Latenzprobleme beim Zugriff auf Websites und Webanwendungen. Wenn Sie mehrere Anfragen über dieselbe Verbindung multiplexieren, unterliegen sie der Zuverlässigkeit derselben Verbindung. Wenn das Paket für eine Anforderung verloren geht, verzögern sich alle anderen multiplexierten Anfragen, bis das verlorene Paket erkannt und erneut übertragen wird. Dies führt zu Verzögerungen beim Blockieren von Head-of-Line-Blockierungen und Latenzproblemen.

Für Verbindungs- und Transportverzögerungen verwendet HTTP/3 QUIC anstelle des TCP-Protokolls. Das QUIC ist ein aufkommendes Protokoll, das UDP anstelle von TCP als Basistransport verwendet. In HTTP-over-Quic können Sie mehrere unabhängige Anfragen multiplexen, ohne von einer einzigen TCP-Verbindung abhängig zu sein. QUIC implementiert eine zuverlässige Verbindung, auf der Sie mehrere HTTP-Anfragen streamen können. QUIC enthält auch TLS als integrierte Komponente und nicht als zusätzliche Layer wie in HTTP/1.1 oder HTTP/2.

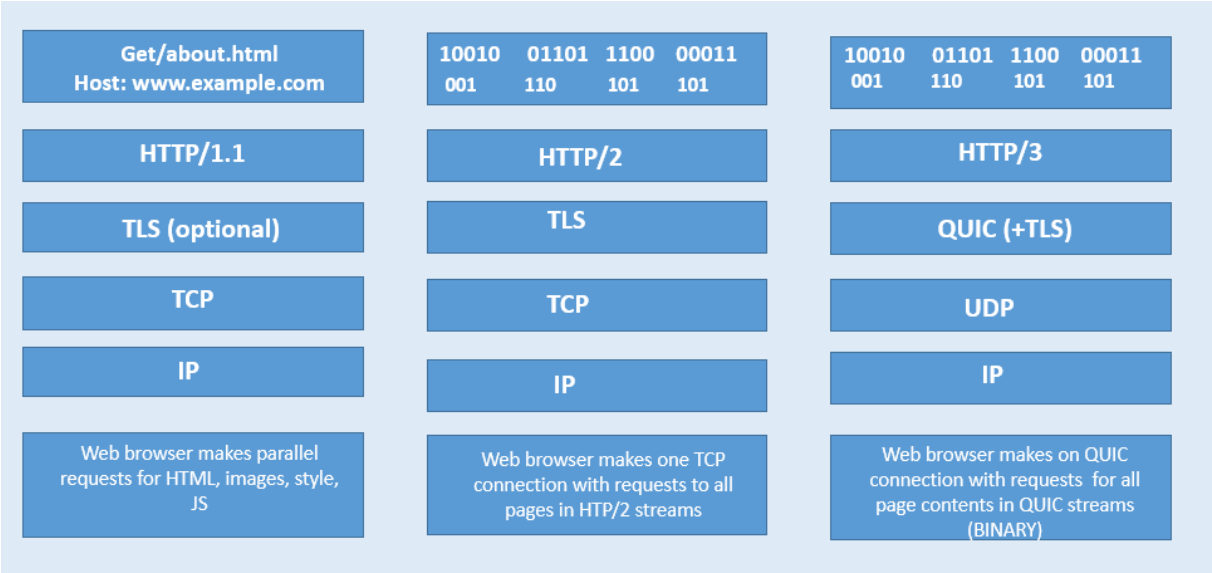
Vorteil der Verwendung des HTTP/3-Protokolls

Einige der wichtigen Vorteile der Verwendung des QUIC-Protokolls für den HTTP/3-Datentransport sind nachstehend aufgeführt:

- Stream-Multiplexen
- Strömungssteuerung auf Stream- und Verbindungsebene
- Verbindungsaufbau mit niedriger Latenz
- Verbindungsmigration und Widerstandsfähigkeit zur NAT-Wiederbindung
- Authentifizierter und verschlüsselter Header und Payload

Transportstapel in HTTP-Protokollen

Die folgende Abbildung zeigt den Transportstapel in den Protokollen HTTP/1.1, HTTP/2 und HTTP/3.



Wie QUIC- und HTTP/3-Verbindungsmanagement in Citrix ADC funktioniert

Die folgende Abbildung zeigt, wie QUIC- und HTTP/3-Verbindungsmanagement in einer Citrix ADC Appliance und wie die Komponenten miteinander interagieren.

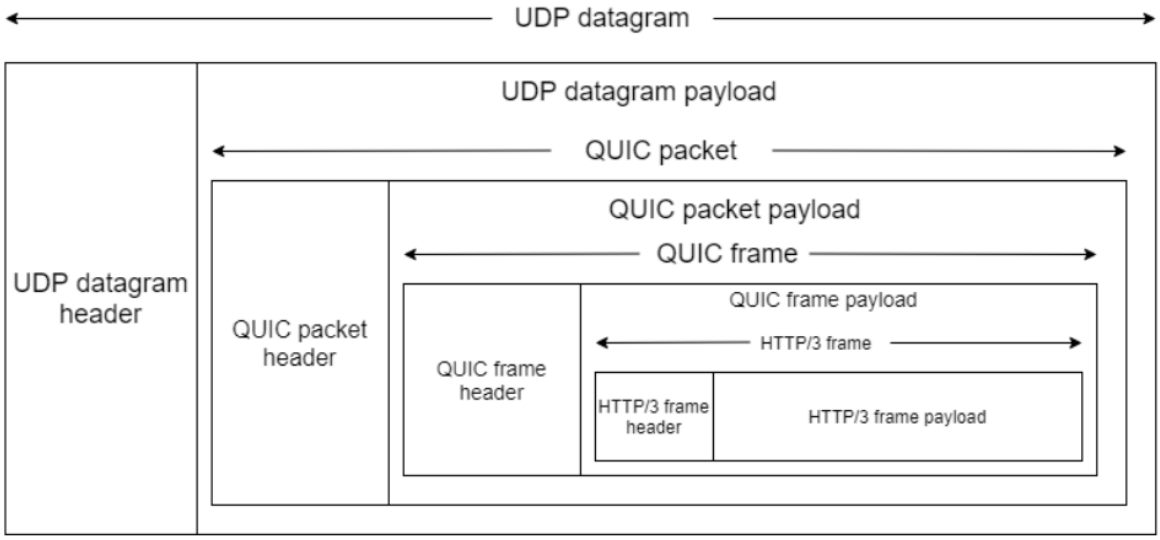
Schritt 1: Clientseitige HTTP/3-Anfrage über das QUIC-Protokoll an die Citrix ADC Appliance.
Schritt 2: Anforderung, die von Citrix ADC AS HTTP/1.1 oder HTTP/2 weitergeleitet wird, abhängig von der Unterstützung des Back-End-Servers.
Schritt 3: Antwort über HTTP/2 oder HTTP/1.1 vom Back-End-Server zu Citrix ADC.
Schritt 4: ADC leitet die Antwort als HTTP/3-Antwort an den Client weiter.

So funktioniert das HTTP/3-Protokoll

Wenn ein Client in HTTP/3 weiß, dass ein HTTP/3-Server an einem bestimmten Endpunkt vorhanden ist, öffnet er eine QUIC-Verbindung. Das QUIC-Protokoll bietet Multiplexing und Flusskontrolle. Innerhalb jedes Streams ist die Basiseinheit der HTTP/3-Kommunikation ein Frame. Jeder Frame-Typ di-

ent einem anderen Zweck. Zum Beispiel bilden HEADER und DATENRAHMEN die Grundlage für HTTP-Anfragen und -Antworten.

Das Multiplexen von Anfragen wird mit der QUIC-Stream-Abstraktion durchgeführt. Jedes Request-Response-Paar verbraucht einen einzelnen QUIC-Stream. Streams sind unabhängig voneinander, daher verhindert ein Stream, der blockiert ist oder einen Paketverlust erleidet, den Fortschritt in anderen Streams nicht. Server-Push ist ein in HTTP/2 eingeführter Interaktionsmodus, der es einem Server ermöglicht, einen Request-Response-Austausch an einen Client zu senden, in Erwartung, dass der Client die angegebene Anfrage stellt. Dies wird von der Netzauslastung gegen einen möglichen Latenzgewinn gehandelt. Zum Verwalten von Server-Push werden mehrere HTTP/3-Frames verwendet, wie PUSH_PROMISE, MAX_PUSH_ID und CANCEL_PUSH. Wie in HTTP/2 werden Anforderungs- und Antwortfelder zur Übertragung komprimiert. Da HPACK auf die orderweise Übertragung komprimierter Feldabschnitte angewiesen ist (eine Garantie, die nicht von QUIC bereitgestellt wird), ersetzt HTTP/3 HPACK durch QPACK. QPACK verwendet separate unidirektionale Streams, um den Status der Feldtabellen zu ändern und zu verfolgen, während codierte Feldabschnitte auf den Status der Tabelle verweisen, ohne ihn zu ändern.



HTTP/3-Konfiguration und Statistikzusammenfassung

July 8, 2022

Um ein HTTP/3-Protokoll für das Senden mehrerer HTTP/3-Datenströme mit QUIC zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Aktivieren Sie SSL- und Load Balancing-Funktionen.

2. Fügen Sie Lastenausgleich und Content Switching (optional) virtuelle Server vom Typ HTTP_QUIC hinzu.
3. Verknüpfen Sie QUIC-Protokollparameter mit dem virtuellen HTTP_QUIC-Server.
4. Aktivieren Sie HTTP/3 auf dem virtuellen HTTP_QUIC-Server.
5. Binden Sie ein SSL-Zertifikatschlüsselpaar mit dem virtuellen HTTP_QUIC-Server.
6. Verknüpfen Sie SSL/TLS-Protokollparameter mit dem virtuellen HTTP_QUIC-Server.

SSL und Load Balancing aktivieren

Bevor Sie beginnen, stellen Sie sicher, dass die SSL- und Load Balancing-Funktionen auf der Appliance aktiviert sind. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 enable ns feature ssl lb
2 <!--NeedCopy-->
```

Fügen Sie Lastenausgleich und Content Switching (optional) virtuelle Server vom Typ HTTP_QUIC für den HTTP/3-Dienst hinzu

Sie fügen einen virtuellen Lastausgleichsserver hinzu, um HTTP/3-Datenverkehr über QUIC zu akzeptieren.
Hinweis: Der virtuelle Lastausgleichsserver vom Typ HTTP_QUIC verfügt über integrierte QUIC-, SSL- und HTTP3-Profile. Wenn Sie es vorziehen, benutzerdefinierte Profile zu erstellen, können Sie neue Profile hinzufügen und an den virtuellen Lastenausgleichsserver binden.

```
1 add lb vserver <vserver-name> HTTP_QUIC <IP-address> <UDP-listening-
     port>
2 add cs vserver <vserver-name> HTTP_QUIC <IP-address> <UDP-listening-
     port>
3 <!--NeedCopy-->
```

Beispiel:

```
add lb vserver lb-http3 HTTP_QUIC 1.1.1.1 443
add cs vserver cs-http3 HTTP_QUIC 10.10.10.10 443
```

Verknüpfen Sie QUIC-Protokollparameter mit dem virtuellen HTTP_QUIC-Server

Sie können ein QUIC-Profil erstellen und QUIC-Parameter für den QUIC-Dienst angeben und es dem virtuellen Lastenausgleichsserver zuordnen. Sie müssen entweder ein benutzerdefiniertes Profil er-

stellen oder das integrierte QUIC-Profil verwenden und das Profil an den virtuellen Load Balancing-Server binden.

Schritt 1: Konfigurieren Sie ein benutzerdefiniertes QUIC-Profil
an der Eingabeaufforderung:

```
set quic profile <profile_name> -transport_param <value>
<!--NeedCopy-->
```

Beispiel:

```
set quic profile quic_http3 -ackDelayExponent 10 -activeConnectionIDlimit 4
```

Die verschiedenen QUIC-Transportparameter lauten wie folgt:

-ackDelayExponent. Ein ganzzahliger Wert, der vom Citrix ADC an den Remote-QUIC-Endpunkt angekündigt wird, der einen Exponenten angibt, den der Remote-QUIC-Endpunkt verwenden sollte, um das Feld ACK Delay in QUIC ACK-Frames zu dekodieren, die vom Citrix ADC gesendet werden.

-activeConnectionIDlimit. Ein ganzzahliger Wert, der vom Citrix ADC für den Remote-QUIC-Endpunkt angekündigt wird. Es gibt die maximale Anzahl von QUIC-Verbindungs-IDs vom Remote-QUIC-Endpunkt an, die der Citrix ADC speichern möchte.

-activeConnectionMigration. Geben Sie an, ob der Citrix ADC dem Remote-QUIC-Endpunkt erlauben muss, eine aktive QUIC-Verbindungsmigration durchzuführen.

-congestionCtrlAlgorithm. Geben Sie den Algorithmus zur Überlastungssteuerung an, der für QUIC-Verbindungen verwendet werden soll.

-initialMaxData. Ein ganzzahliger Wert, der vom Citrix ADC an den Remote-QUIC-Endpunkt angekündigt wird und den Anfangswert in Byte für die maximale Datenmenge angibt, die über eine QUIC-Verbindung gesendet werden kann.

-initialMaxStreamDataBidiLocal. Ein ganzzahliger Wert, der vom Citrix ADC an den Remote-QUIC-Endpunkt angekündigt wird und die anfängliche Flusssteuerungsgrenze in Byte für bidirektionale QUIC-Streams angibt, die vom Citrix ADC initiiert wurden.

-initialMaxStreamDataBidiRemote. Ein ganzzahliger Wert, der vom Citrix ADC für den Remote-QUIC-Endpunkt angekündigt wird und die anfängliche Flusssteuerungsgrenze in Byte für bidirektionale QUIC-Streams angibt, die vom Remote-QUIC-Endpunkt initiiert werden.

-initialMaxStreamDataUni. Ein ganzzahliger Wert, der vom Citrix ADC an den Remote-QUIC-Endpunkt angegeben wird und die anfängliche Flusssteuerungsgrenze in Byte für unidirektionale Streams angibt, die vom Remote-QUIC-Endpunkt initiiert werden.

-initialMaxStreamsBidi. Ein ganzzahliger Wert, der vom Citrix ADC an den Remote-QUIC-Endpunkt angekündigt wird und die anfängliche maximale Anzahl von bidirektionalen Streams angibt, die der

Remote-QUIC-Endpunkt initiieren muss.

-initialMaxStreamsUni. Ein ganzzahliger Wert, der vom Citrix ADC an den Remote-QUIC-Endpunkt angekündigt wird und die anfängliche maximale Anzahl von unidirektionalen Streams angibt, die der Remote-QUIC-Endpunkt initiieren muss.

-maxAckDelay. Ein ganzzahliger Wert, der vom Citrix ADC für den Remote-QUIC-Endpunkt angekündigt wird und die maximale Zeitspanne in Millisekunden angibt, um die der Citrix ADC das Senden von Bestätigungen verzögert.

-maxIdleTimeout. Ein ganzzahliger Wert, der vom Citrix ADC an den Remote-QUIC-Endpunkt ausgegeben wird und das maximale Leerlauf-Timeout für eine QUIC-Verbindung in Sekunden angibt. Eine QUIC-Verbindung, die länger als das Minimum der vom Citrix ADC und dem Remote-QUIC-Endpunkt angekündigten Zeitüberschreitungswerte im Leerlauf bleibt, und das Dreifache des aktuellen Probe Timeout (PTO), wird vom Citrix ADC stillschweigend verworfen.

-maxUDPPayloadSize. Ein ganzzahliger Wert, der vom Citrix ADC für den Remote-QUIC-Endpunkt angekündigt wird und die Größe der größten UDP-Datagramm-Nutzlast in Byte angibt, die der Citrix ADC bereit ist, bei einer QUIC-Verbindung zu empfangen.

-newTokenValidityPeriod. Ein ganzzahliger Wert, der den Gültigkeitszeitraum der vom Citrix ADC gesendeten QUIC NEW_TOKEN-Frames in Sekunden angibt.
-retryTokenValidityPeriod. Ein ganzzahliger Wert, der den Gültigkeitszeitraum der Adressprüfungstoken angibt, die über QUIC Wiederholungspakete ausgegeben werden, die vom Citrix ADC gesendet wurden.
-statelessAddressValidation. Geben Sie an, ob der Citrix ADC eine zustandslose Adressvalidierung für QUIC-Clients durchführen muss, indem er Token in QUIC-Wiederholungspaketen während des Aufbaus der QUIC-Verbindung sendet und Token in QUIC NEW_TOKEN-Frames nach dem Aufbau der QUIC-Verbindung sendet.

Schritt 2: Ordnen Sie das benutzerdefinierte QUIC-Profil einem virtuellen Lastausgleichsserver vom Typ http_quic zu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 set lb vserver <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@]  <
     serviceName>@] [-persistenceType <persistenceType>] [-
     quicProfileName <string>]
2 <!--NeedCopy-->
```

Beispiel:

```
set lb vserver lb-http3 -quicProfileName quic_http3
```


Aktivieren und binden Sie HTTP/3 auf einem virtuellen HTTP_QUIC Server

Um HTTP/3 auf einem virtuellen HTTP_QUIC-Server zu aktivieren, wird der HTTP-Profilkonfiguration eine Reihe von Konfigurationsparametern hinzugefügt. Um die Konfiguration zu erleichtern, ist beim Hinzufügen eines virtuellen HTTP_QUIC-Servers ein neues Standard/integriertes HTTP-Profil auf der Appliance verfügbar. Für das Profil sind die Unterstützungsparameter des HTTP/3-Protokolls auf ENABLED festgelegt und auch an die virtuellen HTTP_QUIC-Server begrenzt (anwendbar, wenn Sie den virtuellen HTTP_QUIC-Server nicht mit einem vom Benutzer hinzugefügten HTTP-Profil verknüpfen möchten). Der Wert der HTTP/3-Parameter im HTTP-Profil entscheidet, ob das HTTP/3-Protokoll ausgewählt und bei der Verarbeitung der Erweiterung TLS ALPN (Application Layer Protocol Negotiation) während des QUIC-Protokoll-Handshake angekündigt werden soll.

Sie können ein HTTP/3-Profil erstellen und HTTP-Parameter für den HTTP/3-Dienst und den virtuellen Lastausgleichsserver angeben. Sie müssen entweder ein benutzerdefiniertes Profil erstellen oder das integrierte HTTP/3-Profil verwenden und das Profil an den virtuellen Lastenausgleichsserver binden.

Schritt 1: Konfigurieren Sie ein benutzerdefiniertes HTTP/3-Profil
an der Eingabeaufforderung:

```
1 Add ns httpProfile <profile_name> -http3 ENABLED
2 <!--NeedCopy-->
```

Beispiel:

```
add ns httpProfile http3_quic -http3 ENABLED
```

Schritt 2: Binden Sie das benutzerdefinierte HTTP/3-Profil an einen virtuellen Lastausgleichsserver vom Typ http_quic Geben Sie
an der Eingabeaufforderung Folgendes ein:

```
1 set lb vserver <name>@ [-IPAddress <ip_addr|ipv6_addr|*>@]  <
     serviceName>@] [-persistenceType <persistenceType>] [-
     httpProfileName <string>]
2 <!--NeedCopy-->
```

Beispiel:

```
set lb vserver lb-http3 -httpProfileName http3_quic
```

Binden Sie SSL-Zertifikatschlüsselpaar mit dem virtuellen HTTP_QUIC Server

Um verschlüsselten Datenverkehr zu verarbeiten, müssen Sie ein SSL-Zertifikatschlüsselpaar hinzufügen und es an den virtuellen HTTP_QUIC-Server binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind ssl vserver <vServerName> -certkeyName <certificate-KeyPairName>

<!--NeedCopy-->
```

Beispiel:

```
bind ssl vserver lb-http3 -certkeyName rsa_certkeypair
```

Weitere Informationen finden Sie unter Thema Bind SSL-Zertifikat .

Binden Sie SSL/TLS-Protokollparameter mit einem virtuellen HTTP_QUIC-Server

Virtuelle Server vom Typ HTTP_QUIC verfügen über eine integrierte TLS 1.3-Serverfunktionalität, da das QUIC-Protokoll TLS 1.3 als obligatorische Sicherheitskomponente verwendet. Um die Konfiguration beim Hinzufügen eines virtuellen HTTP_QUIC-Servers zu erleichtern, wird ein neues Standard- oder integriertes SSL-Profil vom Typ QUIC-FrontEnd hinzugefügt. Das SSL-Profil hat TLS 1.3-Version aktiviert, die mit TLS 1.3-Chiffrier-Suiten (und elliptischen Kurven) konfiguriert ist. Das SSL-Profil muss dann an die neu hinzugefügten virtuellen HTTP_QUIC-Server gebunden sein.
Sie können ein SSL-Profil erstellen und SSL-Verschlüsselungsparameter für den TLP 1.1-Dienst und den virtuellen Lastausgleichsserver angeben. Sie müssen entweder ein benutzerdefiniertes Profil erstellen oder das integrierte SSL-Profil verwenden und das Profil an den virtuellen Lastenausgleichsserver binden.

Schritt 1: Konfigurieren Sie ein benutzerdefiniertes SSL-Profil
an der Eingabeaufforderung:

```
add ssl profile <name> -sslprofileType QUIC-FrontEnd
<!--NeedCopy-->
```

Beispiel:

```
add ssl profile ssl_profile1 -sslprofileType QUIC-FrontEnd -tls13 ENABLED -
tls12 DISABLED -tls11 DISABLED -tls1 DISABLED
```

Schritt 2: Binden Sie das benutzerdefinierte SSL-Profil an einen virtuellen Lastausgleichsserver vom Typ HTTP_QUIC Geben Sie
an der Eingabeaufforderung Folgendes ein:


```
set ssl vserver <name>@ [-sslProfile <string>]
<!--NeedCopy-->
```

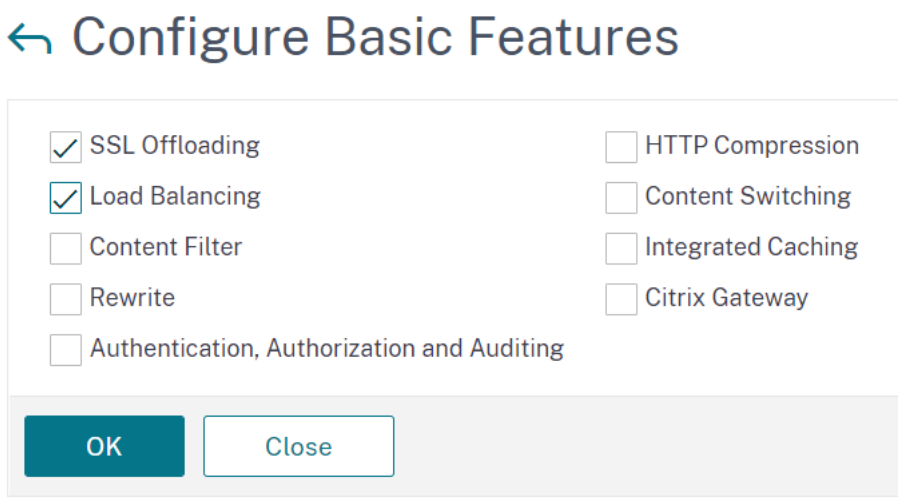
Beispiel:

```
set ssl vserver lb-http3 -sslprofile ssl_profile1
```

Aktivieren Sie SSL- und Load Balancing-Funktionen über die grafische Benutzeroberfläche

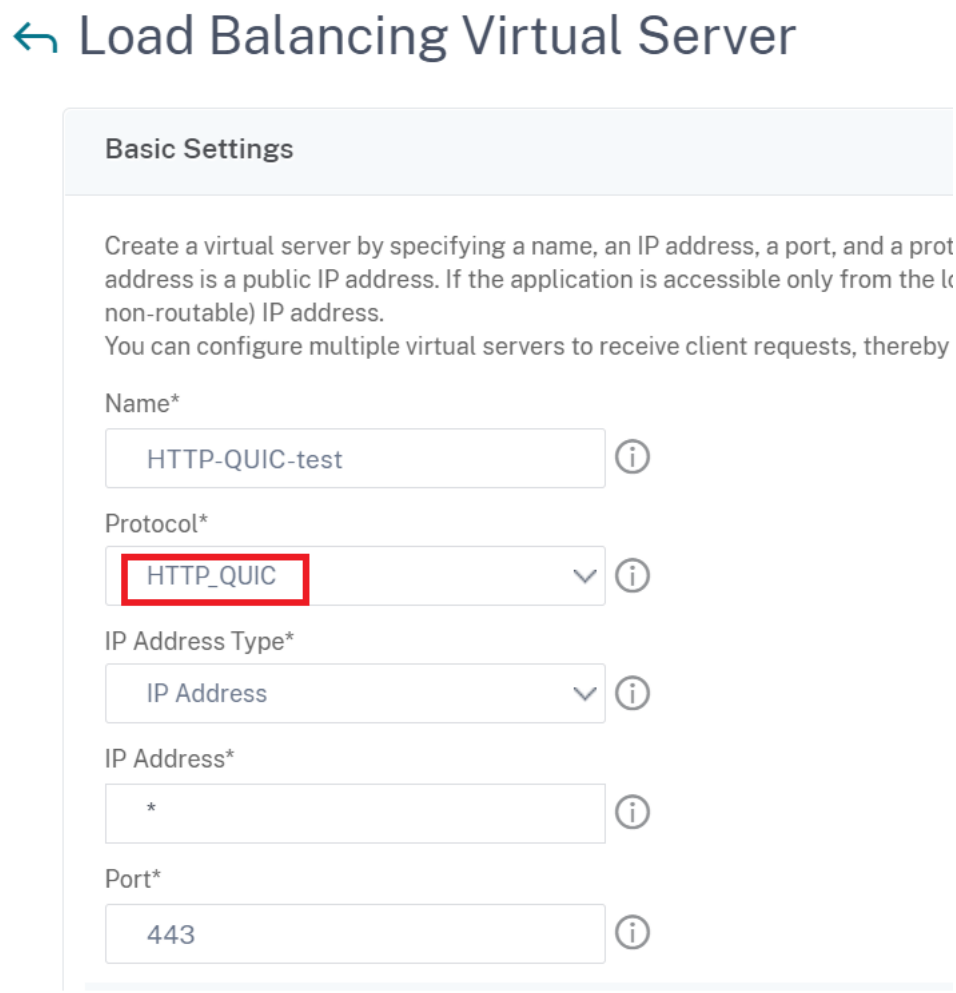
Führen Sie die folgenden Schritte aus, um SSL- und Load Balancing-Funktionen zu aktivieren:

1. Erweitern Sie im Navigationsbereich **System**, und klicken Sie dann auf **Einstellungen**.
2. Wählen Sie auf der Seite **Basisfunktionen konfigurieren** den **SSL** und den **Load Balancing**aus.
3. Klicken Sie auf **OK**, und klicken Sie dann auf **Schließen**.



Fügen Sie Lastenausgleich und Content Switching (optional) virtuelle Server vom Typ HTTP_QUIC mit der GUI hinzu

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie auf **Hinzufügen**, um einen virtuellen Lastenausgleichsserver vom Typ HTTP_QUIC zu erstellen.
3. Klicken Sie auf der Seite **Virtueller Server für Lastenausgleich** auf **Profile**.
4. Wählen Sie im Abschnitt **Profile** den Profiltyp als QUIC aus. Hinweis: QUIC-, HTTP/3- und SSL-Profile sind integrierte Profile.
5. Klicke auf **OK** und dann auf **Fertig**.

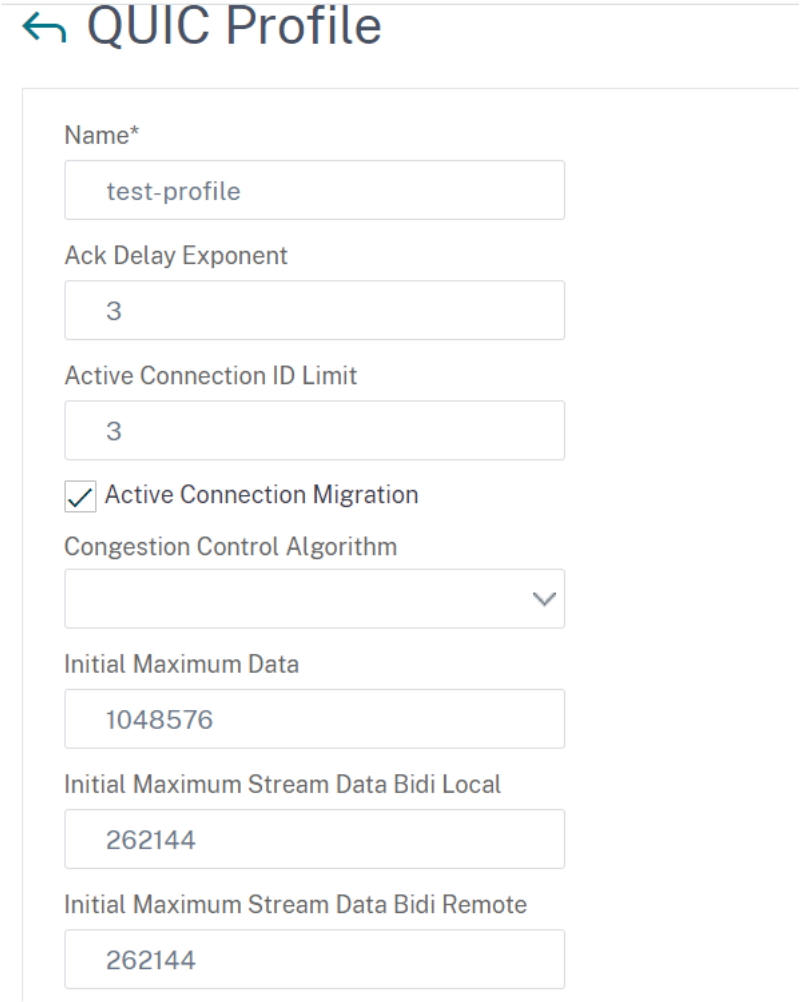


Verknüpfen Sie QUIC-Protokollparameter mit dem virtuellen HTTP_QUIC-Server über die grafische Benutzeroberfläche

Schritt 1: QUIC-Profil hinzufügen

1. Navigieren Sie zu **System > Profile > QUIC-Profil**.
2. Klicken Sie auf **Hinzufügen**.
3. Legen Sie auf der Seite QUIC-Profil die folgenden Parameter fest. Eine ausführliche Beschreibung der einzelnen Parameter finden Sie im Abschnitt “Assoziiertes QUIC-Protokoll CLI”.
   a) `Ack Delay` Exponent
   b) Limit der aktiven Verbindungs-ID
   c) Aktive Verbindungsmigration
   d) Algorithmus zur Überlastungssteuerung
   e) Anfängliche maximale Daten

f) Anfängliche maximale Stream-Daten Bidi Local
g) Anfängliche maximale Stream-Daten Bidi Remote
h) Anfängliche maximale Stream-Dateneinheit
i) Initialer maximaler Stream-Bidi
j) Initialer maximaler Stream-Uni
k) Maximale Verzögerung bei der Bestätigung
l) Maximaler Leerlauf-Timeout
m) Maximale UDP-Daten GramsperBurst
n) Gültigkeitszeitraum des neuen Tokens
o) Gültigkeitszeitraum des Tokens wiederholen
p) Stateless Adressvalidierung

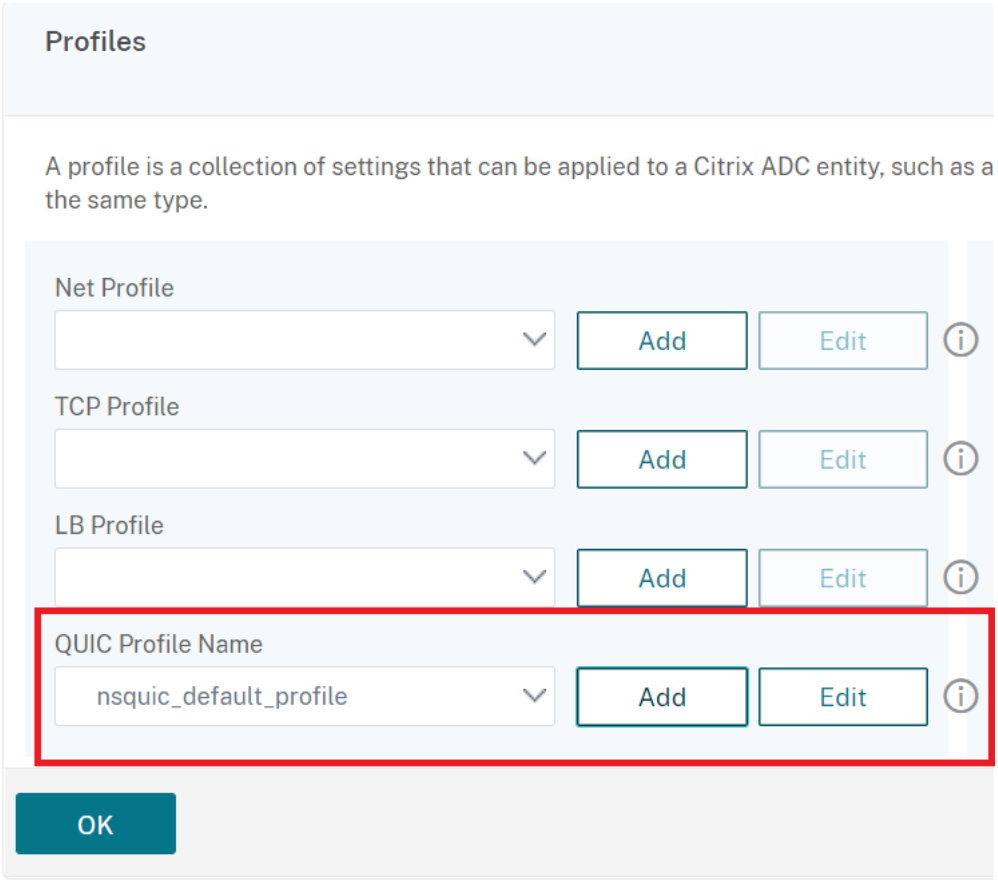


Schritt 2: Verknüpfen Sie QUIC-Profil mit einem virtuellen Lastenausgleichsserver vom Typ HTTP_QUIC

1. Wählen Sie im Abschnitt **Profile** das QUIC-Profil aus. Hinweis: QUIC-, HTTP/3- und SSL-Profile

sind integrierte Profile.

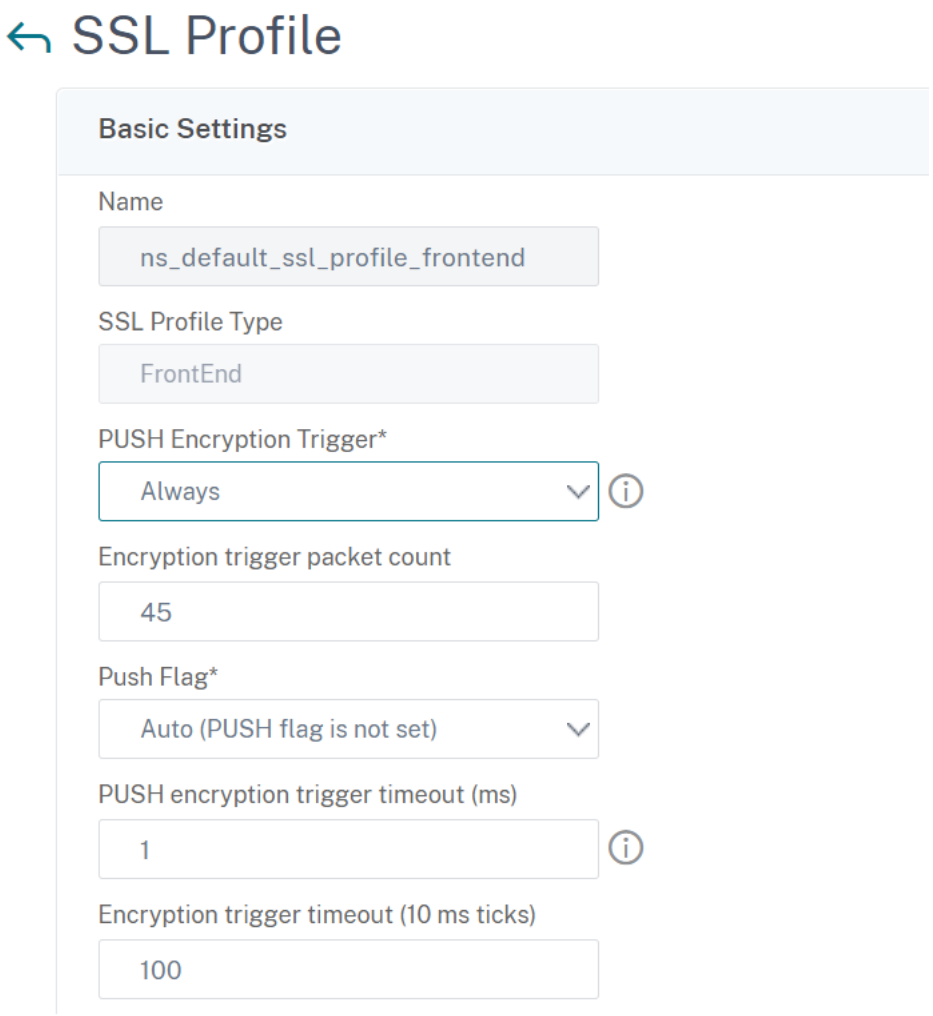
2. Klicke auf **OK** und dann auf **Fertig**.



Verknüpfen Sie SSL/TLS-Protokollparameter mit dem virtuellen Server vom Typ SSL über die grafische Benutzeroberfläche

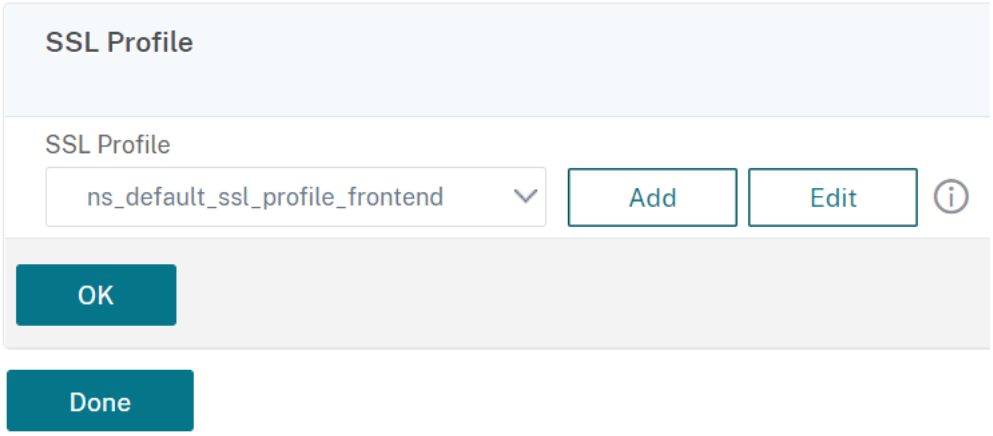
Schritt 1: SSL-Profil hinzufügen

1. Navigieren Sie zu **System > Profile > SSL-Profil**.
2. Klicken Sie auf **Hinzufügen**.
3. Legen Sie auf der Seite **QUIC-Profil** die SSL-Parameter fest. Eine ausführliche Beschreibung finden Sie unter Thema zur SSL-Profilkonfiguration.
4. Klicken Sie auf **OK** und **Schließen**.



Schritt 2: Verknüpfen Sie das SSL-Profil mit einem virtuellen Lastenausgleichsserver vom Typ SSL.

1. Wählen Sie im Abschnitt **Profile** das SSL-Profil aus.
2. Klicke auf **OK** und dann auf **Fertig**.



Quic- und HTTP/3-Statistiken anzeigen

Die folgenden Befehle zeigen eine detaillierte Zusammenfassung der QUIC- und HTTP3-Statistiken. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
> stat quic
> stat quic  - detail
<!--NeedCopy-->
```

Um die Statistikanzeige zu löschen, geben Sie eine der folgenden Optionen ein:

```
> stat quic -clearstats basic
> stat quic -clearstats full

<!--NeedCopy-->
```

So zeigen Sie eine detaillierte Zusammenfassung der HTTP/3-Statistiken an:

```
> stat http3
> stat http3  - detail
<!--NeedCopy-->
```

Um die Statistikanzeige zu löschen, geben Sie eine der folgenden Optionen ein:

```
> stat http3 -clearstats basic
> stat http3 -clearstats full
<!--NeedCopy-->
```

Richtlinienkonfiguration für HTTP/3-Datenverkehr

October 5, 2021

HTTP/3 verwendet den QUIC-Transport, der auf UDP basiert. Wenn Sie einen Richtlinienausdruck für den virtuellen HTTP- oder SSL-Server definiert hatten, der TCP-Richtlinienausdrücke enthält, kann er nicht mehr mit einem virtuellen HTTP_QUIC-Server verwendet werden. Alle anderen Richtlinien, die keinen TCP- oder klassischen Ausdrücke haben, können an einen virtuellen HTTP_QUIC-Server

gebunden werden. Damit die Richtlinien wirksam werden, müssen Sie sicherstellen, dass die Feature-Richtlinien gemäß den folgenden, an die neu hinzugefügten globalen Bindepunkte gebunden sind.

- HTTPQUIC_REQ_DEFAULT
- HTTPQUIC_REQ_OVERRIDE
- HTTPQUIC_RES_DEFAULT
- HTTPQUIC_RES_OVERRIDE

Oder die Richtlinien können an bestimmte Bindepunkte für virtuelle Server gebunden werden:

- REQUEST
- RESPONSE

Weitere Informationen finden Sie unter Thema Binden von Richtlinien mit erweiterter Richtlinieninfrastruktur .

Im Folgenden finden Sie die Richtlinien, die für die HTTP over QUIC-Konfiguration unterstützt werden:

- Responder
- Neuschreiben
- HTTP-Komprimierung
- Integriertes Caching
- Firewall für Webanwendungen
- URL-Transformation
- SSL
- Frontend-Optimierung (FEO)
- AppQoE

Konfiguration der Responder-Richtlinie für HTTP/3-Datenverkehr

Virtuelle Server vom Typ HTTP über QUIC haben Unterstützung für Responder Policy. Da QUIC jedoch UDP als Transportmechanismus verwendet, werden TCP-basierte Ausdrücke ausgeschlossen und UDP-basierte Ausdrücke enthalten.

Neue oder vorhandene Richtlinienkonfigurationen mit TCP-Ausdrücken können nicht an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC globale Bindepunkte gebunden werden. Anstelle von TCP-Ausdrücken können UDP-Ausdrücke in die Richtlinienkonfigurationen einbezogen werden, die an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC-Bindepunkte gebunden sind.

Responder Action zum Umleiten von URLs hinzufügen

Um eine Responder Action hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:


```
1 add responder action <name> <type> (<target> | <htmlpage>) [-comment <
    string>] [-responseStatusCode <positive_integer>] [-reasonPhrase <
    expression>] [-headers <name(value)> ...]
2 <!--NeedCopy-->
```

Beispiel:

```
add responder action redirectURL redirect "\"https://www.citrix.com/\""
```

Responder-Richtlinie hinzufügen

Um eine Responder Policy hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add responder policy <name> <rule> <action> [<undefAction>] [-comment <
    string>] [-logAction <string>] [-appflowAction <string>]
2 <!--NeedCopy-->
```

Beispiel:

```
add responder policy res-pol "CLIENT.IP.SRC.IN_SUBNET(10.10.10.10/32)"
redirectURL
```

Hinzufügen von Responder-Richtlinienbasierten UDP-Ausdruck

Um einen auf der Responder Policy basierten UDP-Ausdruck hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add responder policy <name> <rule> <action> [<undefAction>] [-comment <
    string>] [-logAction <string>] [-appflowAction <string>]
2 <!--NeedCopy-->
```

Beispiel:

```
add responder policy redirectCitrixUdp "CLIENT.UDP.DSTPORT.EQ(443)"redirectURL
```

Binden Responder Policy richtlinienbasierten UDP-Ausdruck mit einem HTTP/3 QUIC-basierten Lastausgleichsserver

Um einen auf Responder Policy basierenden UDP-Ausdruck an einen virtuellen Lastausgleichsserver zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:


```
bind lb vserver <name>@ ((<serviceName>@   [-weight <positive_integer>]
     ) | <serviceGroupName>@ |         (-policyName <string>@  [-
    priority <positive_integer>]  [-gotoPriorityExpression <expression>]
      [-type <type>]  [-invoke  (<labelType>  <labelName>) ]  ) | -
    analyticsProfile <string>@)
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver lb-http3 -policyName redirectCitrixUdp -priority 9 -gotoPriorityExpres
 END -type REQUEST
```

Binden Sie die Responder Policy mit einem HTTP/3 QUIC-basierten Lastenausgleichsserver

Um eine Responder Policy an einen virtuellen Lastausgleichsserver zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name>@ ((<serviceName>@   [-weight <positive_integer>]
     ) | <serviceGroupName>@ |         (-policyName <string>@  [-
    priority <positive_integer>]  [-gotoPriorityExpression <expression>]
      [-type <type>]  [-invoke  (<labelType>  <labelName>) ]  ) | -
    analyticsProfile <string>@)
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver lb-http3 -policyName redirectCitrixUdp -priority 10 -
gotoPriorityExpression END -type REQUEST
```

Binden Sie die Responder Policy an den globalen HTTP/3-Bindepunkt

Um eine Responder Policy an den globalen Bindepunkt HTTP/3 zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind responder global <policyName> <priority>  [<gotoPriorityExpression
    >] [-type <type>] [-invoke (<labelType>  <labelName>) ] bind
    responder global redirectCitrixUdp 3 -type HTTPQUIC_REQ_DEFAULT
<!--NeedCopy-->
```


Beispiel:

```
bind responder global redirectCitrixUdp 3 -type HTTPQUIC_REQ_DEFAULT
```

> **Hinweis:**
>
> Weitere Informationen finden Sie unter Dokumentation zu Responder-Richtlinien.

Richtlinienkonfiguration für HTTP/3-Datenverkehr umschreiben

Virtuelle Server vom Typ HTTP über QUIC verfügen über Rewrite-Richtlinienunterstützung. Da QUIC jedoch UDP als Transportmechanismus verwendet, werden TCP-basierte Ausdrücke ausgeschlossen und UDP-basierte Ausdrücke enthalten.

Neue oder vorhandene Richtlinienkonfigurationen mit TCP-Ausdrücken können nicht an virtuelle HTTP/3-Server oder an die neu hinzugefügten globalen HTTP/3-Bindepunkte gebunden werden. Anstelle von TCP-Ausdrücken können UDP-Ausdrücke in die Richtlinienkonfigurationen einbezogen werden, die an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC-Bindepunkte gebunden sind.

Im Folgenden sind die Konfigurationsschritte zum Konfigurieren der Rewrite-Richtlinie für HTTP3 über QUIC aufgeführt.

Neuschreibaktion für HTTP over QUIC hinzufügen

Um eine Rewrite-Aktion hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-
     pattern <expression> | -search <expression>] [-refineSearch <
     expression>] [-comment <string>]
2 <!--NeedCopy-->
```

Beispiel:

```
add rewrite action http3-altsvc-action insert_http_header Alt-Svc q/"h3
-29=\":443\"; ma=3600; persist=1"/
```

Rewrite-Richtlinie für HTTP over QUIC hinzufügen

Um eine Schreibaktion hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add rewrite policy <name> <rule> <action> [<undefAction>] [-comment  <
     string>] [-logAction <string>]
2 <!--NeedCopy-->
```


Beispiel:

```
add rewrite policy http3-altsvc-policy true http3-altsvc-action
```

Binden Sie die Rewrite-Richtlinie an einen virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC

Um die Rewrite-Richtlinie an den virtuellen Load Balancing-Server zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind lb vserver <name>@ ((<serviceName>@ [-weight <positive_integer>] )
      | <serviceGroupName>@ | (-policyName <string>@ [-priority <
     positive_integer>] [-gotoPriorityExpression <expression>] [-type <
     type>] [-invoke (<labelType> <labelName>) ] ) | -analyticsProfile  <
     string>@)
2 <!--NeedCopy-->
```

Beispiel:

```
bind lb vserver lb-http3 -policyName http3-altsvc-policy -priority 10 -type
 RESPONSE
```

Umschreibrichtlinie an den globalen HTTP/3-Bindepunkt binden

```
1 To bind a responder policy with HTTP/3 global bind point, at the
     command prompt, type:
2 bind rewrite global <policyName> <priority> [<gotoPriorityExpression>]
      [-type <type>] [-invoke (<labelType> <labelName>)]
3 <!--NeedCopy-->
```

Beispiel:

```
bind rewrite global http3-altsvc-policy 3 -type HTTPQUIC_RES_DEFAULT
```

> **Hinweis:**
>
> Weitere Informationen finden Sie unter Umschreiben der Richtliniendokumentation.

Konfiguration der Komprimierungsrichtlinie für HTTP/3-Datenverkehr

Wenn Citrix ADC eine HTTP-Antwort von einem Server empfängt, werden die integrierten Komprimierungsrichtlinien und alle benutzerdefinierten Komprimierungsrichtlinien ausgewertet, um

zu bestimmen, ob die Antwort komprimiert werden soll, und falls ja, der anzuwendende Komprimierungstyp. Die den Richtlinien zugewiesenen Prioritäten bestimmen die Reihenfolge, in der die Richtlinien mit den Anforderungen abgeglichen werden.
Virtuelle Server vom Typ HTTP über QUIC haben Unterstützung für Komprimierungsrichtlinien. Da QUIC jedoch UDP als Transportmechanismus verwendet, werden TCP-basierte Ausdrücke ausgeschlossen und UDP-basierte Ausdrücke enthalten.
Neue oder vorhandene Richtlinienkonfigurationen mit TCP-Ausdrücken können nicht an virtuelle HTTP/3-Server oder an die neu hinzugefügten globalen HTTP/3-Bindepunkte gebunden werden. Anstelle von TCP-Ausdrücken können UDP-Ausdrücke in die Richtlinienkonfigurationen einbezogen werden, die an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC-Bindepunkte gebunden sind.

Komprimierungsrichtlinie hinzufügen

Um eine Komprimierungsrichtlinie hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add cmp policy <name> -rule <expression> -resAction <string>
2 <!--NeedCopy-->
```

Beispiel:

```
add cmp policy udp_port_cmp_policy -rule "CLIENT.UDP.DSTPORT.EQ(443)"-
resAction COMPRESS
```

Binden Sie die Komprimierungsrichtlinie mit einem virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC

Um die URL-Transformationsrichtlinie an einen virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind lb vserver <name>@ ((<serviceName>@  [-weight <positive_integer>]
     ) | <serviceGroupName>@ |  (-policyName <string>@  [-priority <
     positive_integer>]  [-gotoPriorityExpression <expression>]  [-type (
      REQUEST | RESPONSE )] [-invoke  (<labelType>  <labelName>) ]  ) |
     -analyticsProfile <string>@)
2 <!--NeedCopy-->
```

Beispiel:

```
bind lb vserver lb-http3 -policyName udp_port_cmp_policy -priority 10 -type
 RESPONSE
```


Binden Sie die Komprimierung global an den globalen HTTP/3-Bindepunkt

Um eine Komprimierungsrichtlinie an den globalen Bindepunkt HTTP/3 zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind compression global <policyName> <priority>  [<
    gotoPriorityExpression>] [-type <type>] [-invoke (<labelType>  <
    labelName>) ] bind responder global redirectCitrixUdp 3 -type
    HTTPQUIC_REQ_DEFAULT
<!--NeedCopy-->
```

Beispiel:

```
bind cmp global udp_port_cmp_policy -priority 100 -type HTTPQUIC_RES_DEFAULT
 Global built-in compression policies
```

Nachdem Sie Ihre Appliance auf Citrix ADC Release 13.0 Build 82.x aktualisiert haben, werden die folgenden Komprimierungsrichtlinien automatisch an den Standardbindepunkt HTTP/3 gebunden.

```
> sho cmp global -type HTTPQUIC_RES_DEFAULT
        Policy Name: ns_adv_nocmp_xml_ie
        Priority: 8700
        GotoPriorityExpression: END
        Type: HTTPQUIC_RES_DEFAULT

        Policy Name: ns_adv_nocmp_mozilla_47
        Priority: 8800
        GotoPriorityExpression: END
        Type: HTTPQUIC_RES_DEFAULT

        Policy Name: ns_adv_cmp_mscss
        Priority: 8900
        GotoPriorityExpression: END
        Type: HTTPQUIC_RES_DEFAULT

        Policy Name: ns_adv_cmp_msapp
        Priority: 9000
        GotoPriorityExpression: END
        Type: HTTPQUIC_RES_DEFAULT

        Policy Name: ns_adv_cmp_content_type
        Priority: 10000
        GotoPriorityExpression: END
```



```
25          Type: HTTPQUIC_RES_DEFAULT
26  <!--NeedCopy-->
```

Wenn nicht gebunden, können die folgenden Befehle über die Eingabeaufforderung konfiguriert werden und Sie können auf Ihrer Appliance konfigurieren.

```
bind cmp global ns_adv_nocmp_xml_ie -priority 8700 -gotoPriorityExpression
END -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_nocmp_mozilla_47 -priority 8800 -gotoPriorityExpression
 END -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_cmp_mscss -priority 8900 -gotoPriorityExpression END
 -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_cmp_msapp -priority 9000 -gotoPriorityExpression END
 -type HTTPQUIC_RES_DEFAULT

bind cmp global ns_adv_cmp_content_type -priority 10000 -gotoPriorityExpression
 END -type HTTPQUIC_RES_DEFAULT
```

Weitere Informationen finden Sie unter Konfiguration von Komprimierungsrichtlinien.

Caching-Richtlinienkonfiguration für HTTP/3-Datenverkehr

Der integrierte Cache bietet In-Memory-Speicher auf der Citrix ADC Appliance und stellt Webinhalte für Benutzer bereit, ohne dass ein Roundtrip zu einem Ursprungsserver erforderlich ist. Für statische Inhalte benötigt der integrierte Cache nur wenig anfänglich eingerichtet. Nachdem Sie die integrierte Cache-Funktion aktiviert und eine grundlegende Einrichtung durchgeführt haben (z. B. die Bestimmung der Menge des Citrix ADC Appliance-Speichers, den der Cache verwenden darf), verwendet der integrierte Cache integrierte Richtlinien zum Speichern und Bereitstellen bestimmter Arten von statischem Inhalt, einschließlich einfacher Webseiten und Bilddateien. Sie können den integrierten Cache auch so konfigurieren, dass dynamische Inhalte gespeichert und bereitgestellt werden, die von Web- und Anwendungsservern als nicht zwischenspeicherbar gekennzeichnet sind (z. B. Datenbankdatensätze und Aktienkurse).
Virtuelle Server vom Typ HTTP über QUIC haben Cache-Policy-Unterstützung. Da QUIC jedoch UDP als Transportmechanismus verwendet, werden TCP-basierte Ausdrücke ausgeschlossen und UDP-basierte Ausdrücke enthalten.

Neue oder vorhandene Richtlinienkonfigurationen mit TCP-Ausdrücken können nicht an virtuelle HTTP/3-Server oder an die neu hinzugefügten globalen HTTP/3-Bindepunkte gebunden werden. Anstelle von TCP-Ausdrücken können UDP-Ausdrücke in die Richtlinienkonfigurationen einbezogen werden, die an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC-Bindepunkte gebunden sind.

Cache-Inhaltsgruppe hinzufügen

Um die Cache-Inhaltsgruppe hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add cache contentGroup <name> [-weakPosRelExpiry <secs> | -relExpiry <
     secs> | -relExpiryMilliSec <msecs> | -absExpiry <HH:MM> ... | -
     absExpiryGMT <HH:MM> ...] [-heurExpiryParam <positive_integer>] [-
     weakNegRelExpiry <secs>] [-maxResSize <KBytes>] [-memLimit <MBytes>]
     ...
2 <!--NeedCopy-->
```

Beispiel:

```
add cache contentGroup DEFAULT -maxResSize 500
```

Cache-Richtlinie hinzufügen

Um Cache-Richtlinie hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add cache policy <policyName> -rule <expression> -action <action>  [-
     storeInGroup <string>] [-invalGroups <string> ...] [-invalObjects <
     string> ...] [-undefAction ( NOCACHE | RESET )] add cache policy <
     name> <rule> <profileName> [-comment <string>]  [-logAction <string
     >]
2 <!--NeedCopy-->
```

Beispiel:

```
add cache policy ctx_doc_pdf -rule ”HTTP.REQ.URL.ENDSWITH(\”.pdf\”)”-action
 CACHE -storeInGroup DEFAULT
```

Binden Sie die Cache-Richtlinie mit einem virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC

Um die Cache-Richtlinie an einen virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind lb vserver <name>@ ((<serviceName>@  [-weight <positive_integer>]
     ) | <serviceGroupName>@ |  (-policyName <string>@  [-priority <
     positive_integer>]  [-gotoPriorityExpression <expression>]  [-type (
```



```
        REQUEST | RESPONSE )] [-invoke  (<labelType>  <labelName>) ]  ) |
      -analyticsProfile <string>@)
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver lb-http3 -policyName ctx_doc_pdf -priority 100 -type
REQUEST
```

Binden Sie die Cacherichtlinie global an den globalen HTTP/3-Bindepunkt

So binden Sie eine Cache-Richtlinie für den globalen HTTP/3-Bindepunkt:

```
bind cache global <policy> -priority <positive_integer>  [-
    gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
    labelType> <labelName>) ]
<!--NeedCopy-->
```

Beispiel:

```
bind cache global ctx_doc_pdf -priority 3 -type HTTPQUIC_REQ_DEFAULT
```

Weitere Informationen finden Sie unter Integrierte Cache-Richtlinienkonfiguration.

Global integrierte Cache-Richtlinien

Nach dem Upgrade Ihrer Appliance auf Citrix ADC Release 13.0 Build 82.x werden die folgenden Cacherichtlinien automatisch an den HTTP/3-Standardbindepunkt gebunden.

Bei einem Upgrade auf das Release 13.0 82.x werden die folgenden Cacherichtlinien automatisch an den Standardbindepunkt HTTP/3 gebunden.

```
> sho cache global -type HTTPQUIC_REQ_DEFAULT
1)      Policy Name: NOPOLICY
        Priority: 185883
        GotoPriorityExpression: USE_INVOCATION_RESULT
        Invoke type: policylabel        Invoke name:
           _httpquicReqBuiltinDefaults
        Global bindpoint: HTTPQUIC_REQ_DEFAULT

 Done
> sho cache global -type HTTPQUIC_RES_DEFAULT
```



```
1)      Policy Name: NOPOLICY
        Priority: 185883
        GotoPriorityExpression: USE_INVOCATION_RESULT
        Invoke type: policylabel        Invoke name:
            _httpquicResBuiltinDefaults
        Global bindpoint: HTTPQUIC_RES_DEFAULT

<!--NeedCopy-->
```

Wenn die Richtlinien nach einem Upgrade nicht gebunden sind, können Sie die folgenden Befehle verwenden, um die Konfiguration manuell zu binden und zu speichern.

```
add cache policylabel _httpquicReqBuiltinDefaults -evaluates
    HTTPQUIC_REQ

add cache policylabel _httpquicResBuiltinDefaults -evaluates
    HTTPQUIC_RES

bind cache policylabel _httpquicReqBuiltinDefaults -policyName
    _nonGetReq -priority 100

bind cache policylabel _httpquicReqBuiltinDefaults -policyName
    _advancedConditionalReq -priority 200

bind cache policylabel _httpquicReqBuiltinDefaults -policyName
    _personalizedReq -priority 300

bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _uncacheableStatusRes -priority 100

bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _uncacheableVaryRes -priority 200

bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _uncacheableCacheControlRes -priority 300

bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _cacheableCacheControlRes -priority 400

bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _uncacheablePragmaRes -priority 500

bind cache policylabel _httpquicResBuiltinDefaults -policyName
```



```
    _cacheableExpiryRes -priority 600
22
23 bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _imageRes -priority 700
24
25 bind cache policylabel _httpquicResBuiltinDefaults -policyName
    _personalizedRes -priority 800
26
27 bind cache global NOPOLICY -priority 185883 -gotoPriorityExpression
    USE_INVOCATION_RESULT -type HTTPQUIC_REQ_DEFAULT -invoke policylabel
     _httpquicReqBuiltinDefaults
28
29 bind cache global NOPOLICY -priority 185883 -gotoPriorityExpression
    USE_INVOCATION_RESULT -type HTTPQUIC_RES_DEFAULT -invoke policylabel
     _httpquicResBuiltinDefaults
30
31 <!--NeedCopy-->
```

> **Hinweis:**
>
> Die ersten beiden Befehle in der Befehlsliste und die letzten beiden Befehle in derselben Liste sind der Vollständigkeit halber enthalten. Beim Ausführen der vier Befehle tritt möglicherweise ein Fehler auf, da die Befehle bereits zum Zeitpunkt des Neustarts der Appliance ausgeführt werden. Aber Sie können diese Fehler ignorieren.

Konfiguration der URL-Transformationsrichtlinie für HTTP/3-Datenverkehr

Die URL-Transformation ändert alle URLs in bestimmten Anfragen von einer externen Version, die von externen Benutzern gesehen wird, an eine interne URL, die nur von Ihren Webservern und Administratoren angezeigt wird. Sie können Benutzeranforderungen nahtlos umleiten, ohne dass die Netzwerkstruktur Benutzern zugänglich gemacht wird. Sie können auch komplexe interne URLs, die sich Benutzer möglicherweise schwer merken können, in einfachere, leichter zu merkende externe URLs ändern.

Virtuelle Server vom Typ HTTP über QUIC haben Cache-Policy-Unterstützung. Da QUIC jedoch UDP als Transportmechanismus verwendet, werden TCP-basierte Ausdrücke ausgeschlossen und UDP-basierte Ausdrücke enthalten.

Neue oder vorhandene Richtlinienkonfigurationen mit TCP-Ausdrücken können nicht an virtuelle HTTP/3-Server oder an die neu hinzugefügten globalen HTTP/3-Bindepunkte gebunden werden. Anstelle von TCP-Ausdrücken können UDP-Ausdrücke in die Richtlinienkonfigurationen einbezogen werden, die an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC-Bindepunkte gebunden sind.

URL-Transformationsprofil hinzufügen

Um ein URL-Transformationsprofil hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add transform profile <name> [-type URL]
2 <!--NeedCopy-->
```

Beispiel:

```
add transform profile msapps
```

URL-Transformationsaktion hinzufügen

Um eine URL-Transformation hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add transform action <name> <profileName> <priority> [-state ( ENABLED
      | DISABLED )]
2 <!--NeedCopy-->
```

Beispiel:

```
add transform action docx2doc msapps 2
```

URL-Transformationsaktion hinzufügen

Um URL-Transformationsaktion zum Ersetzen der URL hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein

```
1 add transform action <name> <profileName> <priority> [-state ( ENABLED
      | DISABLED )]
2 <!--NeedCopy-->
```

Beispiel:

```
add transform action docx2doc msapps 1
```

URL-Transformationsrichtlinie hinzufügen

Um eine URL-Transformationsrichtlinie hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:


```
add transform policy <name> <rule> <profileName> [-comment <string>]
    [-logAction <string>]
<!--NeedCopy-->
```

Beispiel:

```
add transform policy urltrans_udp ”CLIENT.UDP.DSTPORT.EQ(443)”msapps
```

Binden Sie URL-Transformationsrichtlinie mit einem virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC

Um die URL-Transformationsrichtlinie an einen virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name>@ ((<serviceName>@  [-weight <positive_integer>]
    ) | <serviceGroupName>@ |  (-policyName <string>@  [-priority <
    positive_integer>]  [-gotoPriorityExpression <expression>]  [-type (
     REQUEST | RESPONSE )] [-invoke  (<labelType>  <labelName>) ]  ) |
    -analyticsProfile <string>@)
<!--NeedCopy-->
```

Beispiel:

```
bind lb vs lb-http3 -policyName urltrans_udp -type REQUEST -priority 8
```

Binden Sie URL-Transformationsrichtlinie global mit einem HTTP/3 QUIC-basierten virtuellen Lastenausgleichsserver

Um eine URL-Transformationsrichtlinie zu binden HTTP/3 globaler Bindepunkt, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind transform global <policyName> <priority>  [<gotoPriorityExpression
    >] [-type <type>] [-invoke (<labelType>  <labelName>) ]
<!--NeedCopy-->
```

Beispiel:

```
bind transform global urltrans_udp 100 -type HTTPQUIC_REQ_DEFAULT
```

Weitere Informationen finden Sie unter Konfiguration von URL-Transformationsrichtlinien.

Konfiguration der Frontend-Optimierung (FEO) für HTTP/3-Datenverkehr

Die HTTP-Protokolle, die Webanwendungen zugrunde liegen, wurden ursprünglich entwickelt, um die Übertragung und das Rendern einfacher Webseiten zu unterstützen. Neue Technologien wie JavaScript und Cascading Stylesheets (CSS) sowie neue Medientypen wie Flash-Videos und grafikreiche Bilder stellen hohe Anforderungen an die Front-End-Performance, also an die Leistung auf Browserebene. Die Funktion der Citrix ADC Front-End-Optimierung (FEO) behebt solche Probleme und verkürzt die Ladezeit und die Renderzeit von Webseiten.

> **Hinweis:**
>
> `HTTP_QUIC _Override/Default_Request` Der Typ wird für globale Bindung von FEO-Richtlinien nicht unterstützt.

Aktion zur Frontend-Optimierung (FEO) hinzufügen

Um eine FEO-Aktion hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add feo action <name> [-pageExtendCache] [<cacheMaxage>][-
     imgShrinkToAttrib] [-imgGifToPng] [-imgToWebp] [-imgToJpegXR] [-
     imgInline] [-cssImgInline] [-jpgOptimize] [-imgLazyLoad] [-cssMinify
     ] [-cssInline] [-cssCombine] [-convertImportToLink] [-jsMinify] [-
     jsInline] [-htmlMinify] [-cssMoveToHead] [-jsMoveToEND][-
     domainSharding <string> <dnsShards> ...] [-clientSideMeasurements]
2
3 <!--NeedCopy-->
```

Beispiel:

```
add feo action feoact -imgGifToPng -pageExtendCache
```

Richtlinie zur Frontend-Optimierung (FEO) hinzufügen

Um eine FEO-Richtlinie hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
add feo policy <name> <rule> <action>
```

Beispiel:

```
add feo policy udp_feo_img ”CLIENT.UDP.DSTPORT.EQ(443)”IMG_OPTIMIZE
```


Binden Sie FEO-Richtlinie mit einem virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC

Um die FEO-Richtlinie an einen virtuellen Lastenausgleichsserver vom Typ HTTP/3_QUIC zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name>@ ((<serviceName>@   [-weight <positive_integer>]
     ) | <serviceGroupName>@ |         (-policyName <string>@  [-
    priority <positive_integer>]  [-gotoPriorityExpression <expression>]
      [-type <type>]  [-invoke  (<labelType>  <labelName>) ]  ) | -
    analyticsProfile <string>@)
<!--NeedCopy-->
```

Beispiel:

```
bind lb vserver lb-http3 -policyName udp_feo_img -priority 4 -gotoPriorityExpression
 END -type REQUEST
```

Binden Sie die FEO-Richtlinie an den globalen HTTP/3-Bindepunkt

Um eine Cache-Richtlinie an den globalen Bindepunkt HTTP/3 zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind cache global <policy> -priority <positive_integer>  [-
    gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
    labelType> <labelName>) ]
<!--NeedCopy-->
```

Beispiel:

```
bind cache global ctx_doc_pdf -priority 3 -type HTTPQUIC_REQ_DEFAULT
```

Weitere Informationen finden Sie unter Konfiguration von Front-End-Optimierungsrichtlinien.

SSL-Richtlinienkonfiguration für HTTP/3-Datenverkehr

Virtuelle Server vom Typ HTTP über QUIC verfügen über SSL-Richtlinienunterstützung. Da QUIC jedoch UDP als Transportmechanismus verwendet, werden TCP-basierte Ausdrücke ausgeschlossen und UDP-basierte Ausdrücke enthalten.
Neue oder vorhandene Richtlinienkonfigurationen mit TCP-Ausdrücken können nicht an virtuelle HTTP/3-Server oder an die neu hinzugefügten globalen HTTP/3-Bindepunkte gebunden werden. Anstelle von TCP-Ausdrücken können UDP-Ausdrücke in die Richtlinienkonfigurationen einbezogen

werden, die an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC-Bindepunkte gebunden sind. SSL-Richtlinien mit Aktionen, die für TLSV1.3 unterstützt werden, gelten nur für HTTP/3-Bind-Punkte oder virtuelle Server.

SSL-Richtlinie hinzufügen

Um eine FEO-Richtlinie hinzuzufügen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add ssl policy <name> -rule <expression> [-action <string>] [-
     undefAction <string>] [-comment <string>]
2 <!--NeedCopy-->
```

Beispiel:

```
add ssl policy ssl-pol -rule CLIENT.SSL.IS_SSL -action NOOP
```

Binden Sie SSL-Richtlinie an den virtuellen HTTP/3-Server

So binden Sie eine SSL-Richtlinie an den virtuellen HTTP/3-Server an der Eingabeaufforderung:

```
1 bind ssl policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Beispiel:

```
bind ssl vserver lb-http3 -policyName ssl-pol -priority 4 -type REQUEST
```

Fügen Sie SSL-Richtlinie mit UDP-Ausdruck für SSL-Richtlinie hinzu

So fügen Sie an der Eingabeaufforderung eine SSL-Richtlinie mit UDP-Ausdruck hinzu:

```
1 add ssl policy <name> -rule <expression> [-action <string>] [-
     undefAction <string>] [-comment <string>]
2 <!--NeedCopy-->
```

Beispiel:

```
add ssl policy ssl_udp_clnt -rule "CLIENT.UDP.DSTPORT.EQ(443)"-action NOOP
```


Binden Sie SSL-Richtlinie mit UDP-Ausdruck an den virtuellen HTTP/3-Server

Um eine SSL-Richtlinie mit UDP-Ausdruck an den virtuellen HTTP/3-Server zu binden, geben Sie an der Eingabeaufforderung ein

```
1 bind ssl policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Beispiel:

```
bind ssl vs lb-http3 -policyName ssl_udp_clnt -priority 8 -type REQUEST
```

SSL-Richtlinie für den CLIENTHELLO Bindepunkt für HTTP/3-Datenverkehr hinzufügen

Um die SSL-Richtlinie für den CLIENTHELLO Bindepunkt für HTTP/3-Datenverkehr zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind ssl policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Beispiel:

```
add ssl policy ssl-pol-ch -rule ”CLIENT.SSL.CLIENT_HELLO.CIPHERS.HAS_HEXCODE
(0x1301)”-action RESET
```

Binden Sie SSL-Richtlinie an den CLIENTHELLO Bindepunkt

Um eine SSL-Richtlinie an den CLIENTHELLO Bindepunkt zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind ssl policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Beispiel:

```
bind ssl vs lb-http3 -policyName ssl-pol-ch -type CLIENTHELLO_REQ -priority
 100
```


Binden Sie SSL-Richtlinie an den globalen HTTP/3-Bindepunkt

Um eine SSL-Richtlinie an den globalen Bindepunkt HTTP/3 zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind cache global <policy> -priority <positive_integer> [-gotoPriorityExpression
 <expression>] [-type <type>] [-invoke (<labelType> <labelName>)]
```

Beispiel:

Es folgt ein Beispiel dafür, dass eine DATA-Richtlinie an einen globalen HTTP/3-Bindepunkt gebunden ist:

```
Bind ssl global -policyName ssl-pol-ch -priority 7 -type HTTPQUIC_DATA_DEFAULT
```

> **Hinweis:**
>
> Weiterleitungsaktion, die für den CLIENTHELLO Bindepunkt für virtuelle SSL-Server festgelegt werden kann, wird derzeit für virtuelle Server vom Typ HTTP_QUIC nicht unterstützt.

Konfiguration der Anwendungs-Firewall-Richtlinie für HTTP/3-Datenverkehr

Virtuelle Server vom Typ HTTP über QUIC verfügen über Unterstützung der Firewall-Richtlinien für Webanwendungen. Da QUIC jedoch UDP als Transportmechanismus verwendet, werden TCP-basierte Ausdrücke ausgeschlossen und UDP-basierte Ausdrücke enthalten.
Neue oder vorhandene Richtlinienkonfigurationen mit TCP-Ausdrücken können nicht an virtuelle HTTP/3-Server oder an die neu hinzugefügten globalen HTTP/3-Bindepunkte gebunden werden. Anstelle von TCP-Ausdrücken können UDP-Ausdrücke in die Richtlinienkonfigurationen einbezogen werden, die an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC-Bindepunkte gebunden sind.

Fügen Sie Web Application Firewall-Richtlinie mit UDP-Ausdruck hinzu

So fügen Sie an der Eingabeaufforderung die Web Application Firewall-Richtlinie mit UDP-Ausdruck hinzu:

```
1 add appfw policy <name> <rule> <profileName> [-comment <string>] [-
     logAction <string>]
2 <!--NeedCopy-->
```

Beispiel:

```
add appfw policy appfw_udp ”CLIENT.UDP.DSTPORT.EQ(443)”APPFW_BYPASS
```


Binden von Protokollausdrücken mit UDP-basierten Ausdruck für das Web Application Firewall-Profil

So binden Sie Protokollausdrücke an das UDP for Web Application Firewall-Profil an der Eingabeaufforderung:

Beispiel:

```
bind appfw profile APPFW_BLOCK -logExpression logexp-1 ”CLIENT.UDP.DSTPORT.
EQ(443)”
```

Binden Sie die Richtlinie der Anwendungs-Firewall mit dem virtuellen HTTP/3-Server

So binden Sie die Richtlinie der Web Application Firewall an den virtuellen HTTP/3-Server an der Eingabeaufforderung:

```
1 bind appfw policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Beispiel:

```
bind lb vs lb-http3 -policyName appfw_udp -priority 3 -type REQUEST
```

Binden Sie die Richtlinie der Webanwendungs-Firewall an den globalen HTTP/3-Bindepunkt

Um eine Web Application Firewall-Richtlinie an den globalen Bindepunkt HTTP/3 zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind appfw global <policy> -priority <positive_integer>  [-
     gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
     labelType> <labelName>) ]
2 <!--NeedCopy-->
```

Beispiel:

```
bind appfw global appfw_udp 100 -type HTTPQUIC_REQ_DEFAULT
```

AppQoE-Richtlinienkonfiguration für HTTP/3-Datenverkehr

Virtuelle Server vom Typ HTTP über QUIC verfügen über AppQoE-Richtlinienunterstützung. Da QUIC jedoch UDP als Transportmechanismus verwendet, werden TCP-basierte Ausdrücke ausgeschlossen

und UDP-basierte Ausdrücke enthalten.
Neue oder vorhandene Richtlinienkonfigurationen mit TCP-Ausdrücken können nicht an virtuelle HTTP/3-Server oder an die neu hinzugefügten globalen HTTP/3-Bindepunkte gebunden werden. Anstelle von TCP-Ausdrücken können UDP-Ausdrücke in die Richtlinienkonfigurationen einbezogen werden, die an virtuelle HTTP/3 QUIC-Server oder HTTP over QUIC-Bindepunkte gebunden sind.

AppQoE-Richtlinie mit UDP-basiertem Ausdruck hinzufügen

So fügen Sie an der Eingabeaufforderung eine AppQoE-Richtlinie mit UDP-Ausdruck hinzu:

```
1 add AppQoE policy <name> <rule> <profileName> [-comment <string>] [-
     logAction <string>]
2 <!--NeedCopy-->
```

Beispiel:

```
add appqoe policy appqoe-pol-udp -rule ”CLIENT.UDP.DSTPORT.EQ(443)”-action
appqoe-act-basic-prhigh
```

Binden Sie die AppQoE-Richtlinie mit dem virtuellen HTTP/3-Server

Um die AppQoE-Richtlinie an den virtuellen HTTP/3-Server zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind appqoe policylabel <labelName> <policyName> <priority> [<
     gotoPriorityExpression>] [-invoke (<labelType> <labelName>)
2 <!--NeedCopy-->
```

Beispiel:

```
bind lb vs lb-http3 -policyName appqoe-pol-udp -type REQUEST -priority 3
```

Binden Sie die AppQoE-Richtlinie an den virtuellen HTTP_QUIC Server

Um die AppQoE-Richtlinie an den `HTTP_QUIC` virtuellen Server zu binden, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind appqoe <policy> -priority <positive_integer>  [-
     gotoPriorityExpression <expression>] [-type <type>] [-invoke (<
     labelType> <labelName>) ]
```



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

Beispiel:

```
bind lb vs lb-http3 -policyName appqoe-pol-primd -priority 8 -type REQUEST
```

HTTP/3-Dienstermittlung

October 5, 2021

Das HTTP-Protokoll basiert auf der Verwendung von HTTP-Alternativdiensten für den Ursprungsserver, um die Verfügbarkeit eines gleichwertigen Dienstes bekannt zu geben. Die HTTP/3-Diensterkennung verwendet ebenfalls das gleiche Prinzip. Ein alternativer HTTP/3-Endpunkt kann mit einer der folgenden Methoden beworben werden:

- HTTP Alt-Svc-Antwortheader
- HTTP/2 Alt-Svc Frame in der Antwort
- Application Layer Protocol Negotiation (ALPN)

Der alternative Dienst gibt die Verwendung eines HTTP-Alt-Svc-Antwortheaders und des HTTP/2 Alt-Svc-Frames als HTTP/3-Endpunkt an. Server können HTTP/3 an jedem UDP-Port bereitstellen. Eine alternative Dienstankündigung enthält einen expliziten Port, und URLs enthalten entweder einen expliziten Port oder einen Standardport, der mit dem Schema verknüpft ist.

Clients, die alternative Service-Header oder Frames erhalten, sind nicht verpflichtet, sie zu verwenden. Der Kunde sollte, wenn er auf einen alternativen Dienst aufmerksam gemacht wird und wenn er den alternativen Dienstmechanismus unterstützt, den entsprechenden alternativen Dienst verwenden, der beworben wird. Mit anderen Worten, ein HTTP/1.1-Dienst oder ein HTTP/2-Dienst kann einen äquivalenten Endpunkt ankündigen, der das HTTP/3-Protokoll unterstützt. Der Client, der diese alternativen Dienstinformationen erhält, kann wählen, ob er eine QUIC-Verbindung mit dem angegebenen alternativen Dienst herstellen möchte, und sobald diese Verbindung verfügbar ist, kann diese Verbindung für alle nachfolgenden Anfragen verwendet werden. Wenn der Aufbau der Verbindung mit dem ausgewählten alternativen Dienst fehlschlägt, kann der Client auf den ursprünglichen Endpunkt zurückgreifen. Wenn der Client den beworbenen alternativen Dienst verwendet, wird dies durch Einbeziehung eines Alt-Used-Headers angegeben.

Citrix ADC unterstützt werbeäquivalente HTTP/3-Endpunkte auf virtuellen Servern vom Typ HTTP und SSL.

Konfigurieren der HTTP/3-Diensterkennung

Führen Sie die folgenden Schritte aus, um die HTTP/3-Diensterkennung zu konfigurieren:

1. Konfigurieren des alternativen HTTP/3-Dienstendpunkts mit einem HTTP-Alt-Svc-Header
2. Konfigurieren Sie den alternativen HTTP/3-Dienstendpunkt mithilfe eines HTTP/2 Alt-Svc-Frames
   Konfigurieren Sie den alternativen HTTP/3-Dienstendpunkt mithilfe eines HTTP-Alt-Svc-Headers
   So kündigen Sie einen HTTP/3-Endpunkt mithilfe eines HTTP-Alt-Svc-Headers an, geben Sie den folgenden Befehl ein:

Hinweis: Der Hauptzweck der Werbung für alternative Dienste besteht darin, den Benutzer wissen zu lassen, dass die HTTP/3-Fähigkeit auch über den HTTP/1.1- oder HTTP/2-Dienst unter einem.b.d:443 zugegriffen werden kann.

```
1 add ns httpProfile <name> -custom -altsvc [ ENABLED | DISABLED ]
2 <!--NeedCopy-->
```

Beispiel:

```
1 add ns httpProfile http-profile -altsvc ENABLED -altSvcValue  ”h3-29=”
     :443”; ma=3600; persist=1”
2 <!--NeedCopy-->
```

oder

```
1 set ns httpProfile http-custom -altsvc ENABLED -altSvcValue  ”h3-29=”
     :443”; ma=3600; persist=1”
2 <!--NeedCopy-->
```

Konfigurieren Sie den alternativen HTTP/3-Dienstendpunkt mithilfe eines HTTP/2 Alt-Svc-Frames

Um einen HTTP/3-Endpunkt mithilfe eines HTTP/2 Alt-SVC-Frames anzukündigen, geben Sie den folgenden Befehl ein:

```
1 add ns httpProfile <name> -custom -altsvc [ ENABLED | DISABLED ] -
     http2AltSvcFrame [ ENABLED | DISABLED ]
2 <!--NeedCopy-->
```


Beispiel:

```
add ns httpProfile http-custom -http2 ENABLED -http2Direct ENABLED -http2AltSvcFrame
 ENABLED -altsvc ENABLED -altSvcValue ”h3-29=\”:443\”; ma=3600; persist=1”
```

oder

```
set ns httpProfile http-custom -http2 ENABLED -http2Direct ENABLED -http2AltSvcFrame
 ENABLED -altsvc ENABLED -altSvcValue ”h3-29=\”:443\”; ma=3600; persist=1”
```

Konfigurieren Sie den HTTP/3-Alternativdienst mit HTTP-Alt-Svc-Header-Wert über die grafische Benutzeroberfläche

1. Navigieren Sie zu **System > Profile > HTTP-Profile**.
2. Klicken Sie auf **Hinzufügen**.
3. Wechseln Sie auf der Seite “ **HTTP-Profil erstellen** “ zum Abschnitt HTTP/3 und aktivieren Sie das Kontrollkästchen **Alternativer Dienst** .
4. Das System zeigt das Textfeld **Alternativer Dienstwert** im Abschnitt http2 an.
5. Geben Sie den alternativen Dienstwert als “h3-29=” :443” ein; ma=3600; persist=1”
6. Klicken Sie auf **OK** und **schließen**.

gRPC

October 5, 2021

gRPC in einer Citrix ADC Appliance ist ein leichtgewichtiges, leistungsstarkes und universelles Remote Procedure Call (RPC) -Framework. Das Framework ist optimal, um in mehreren Sprachen zu arbeiten, die auf jedem Betriebssystem laufen. Auch im Vergleich zu anderen Protokollen bietet gRPC eine bessere Leistung und Sicherheit.

gRPC für Citrix ADC wird aus folgenden Gründen bevorzugt:

- Erstellen Sie verteilte Anwendungen für Rechenzentren und öffentliche/private Cloud-Infrastrukturen.
- Stellen Sie Client-Server-Kommunikation für Mobilgeräte, Web oder Cloud bereit.
- Zugriff auf Cloud-Dienste und -Anwendungen
- Microservice-Bereitstellungen

Warum gRPC in Citrix ADC?

gRPC in Citrix ADC ist über HTTP/2 implementiert, um hochleistungsfähige und skalierbare APIs zu unterstützen. Die Verwendung von Binär- als Text hält die Nutzlast kompakt und effizient. In Citrix ADC werden die HTTP/2-Anforderungen über eine einzige Multiplex-TCP-Verbindung gesendet, so dass mehrere gleichzeitige Nachrichten im unterwegs sind, ohne die Netzwerkressourcenauslastung zu beeinträchtigen. Es verwendet auch Header-Komprimierung, um die Größe von Anfragen und Antworten zu reduzieren.

gRPC unterstützt die folgenden Arten von Dienstmethoden für einen Client, um Parameter und Rückgabetypen remote aufzurufen.

1. **Unärer RPC**. Der Client sendet eine einzelne Anfrage an den gRPC-Server und erhält eine einzige Antwort zurück.

   Beispiel:
   ```
   rpc SayHello(HelloRequest)returns (HelloResponse);
   ```

2. **Serverstreaming-RPC** Der Client sendet eine einzelne Anfrage an den gRPC-Server und erhält eine Stream-Antwort.

   Beispiel:
   ```
   rpc StreamingResponse(HelloRequest)returns (HelloResponse);
   ```

3. **Client-Streaming-RPC** Der Client sendet eine Sequenz von Nachrichten und wartet darauf, dass der Server seine Antwort liest und zurückgibt.

   Beispiel:
   ```
   rpc IntroduceYourself(stream HelloRequest)returns (HelloResponse)
   ```

4. **Bidirektionales Streaming-RPC** Sowohl der Client als auch der Server von beiden Seiten senden einen Nachrichtenstrom über den Lese-Schreib-Stream. Die beiden Streams arbeiten unabhängig voneinander.

   Beispiel:
   ```
   rpc ChatSession (stream HelloRequest)returns (stream HelloResponse)
   ```

Citrix ADC unterstützt die folgenden Funktionen für seine Dienste mit gRPC-Endpunkten:

- Lastausgleich
- Content Switching

- Sichere Endpunktdienste wie Web Application Firewall, Authentifizierung.
- Richtlinienkonfiguration
- Statistiken und Logging
- Umschreiben von Inhalten, Filtern von Inhalten
- Layer-4- und Layer-7-Optimierungen, TLS-Angebot
- Gateway-Lösungen für Protokollübersetzungen

gRPC end-to-end configuration

October 5, 2021

Die GrPC-End-to-End-Konfiguration funktioniert, indem eine GrPC-Anfrage von einem Client über das HTTP/2-Protokoll gesendet wird und die vom GrPC-Server beantworteten GrPC-Nachrichten erneut weitergeleitet werden.

Wie funktioniert die End-to-End-gRPC-Konfiguration

Das folgende Diagramm zeigt, dass eine gRPC-Konfiguration in einer Citrix ADC Appliance funktioniert.

1. Um die gRPC-Konfiguration bereitzustellen, müssen Sie zuerst HTTP/2 im HTTP-Profil aktivieren und die HTTP/2-Unterstützung auch serverseitig global aktivieren.
2. Wenn ein Client eine GrPC-Anfrage sendet, wertet der virtuelle Lastausgleichsserver den gRPC-Datenverkehr mithilfe von Richtlinien aus.
3. Basierend auf der Richtlinienbewertung beendet der virtuelle Lastausgleichsserver (an den gRPC-Dienst gebunden ist) die Anforderung und leitet sie als gRPC-Anforderung an den Back-End-gRPC-Server weiter.
4. Wenn der gRPC-Server auf den Client antwortet, beendet die Appliance die Antwort und leitet sie als gRPC-Antwort an den Client weiter.

Beispiel für eine gRPC-Anfrage, die an gRPC-Server gesendet wird

Der Anforderungsheader wird als HTTP/2-Header in HEADERS+CONTINUATION Frames gesendet.

```
```
HEADERS (flags = END_HEADERS)
: method = POST
: scheme = http
: path = /helloworld.citrix-adc/SayHello
: authority = 10.10.10.10.:80
grpc-timeout = 15
content-type = application/grpc+proto
grpc-encoding = gzip
DATA (flags = END_STREAM)
<Length-Prefixed Message>
<!--NeedCopy--> ```
```

### Beispiel für gRPC-Antwortheader vom gRPC-Server zur Citrix ADC Appliance

Nur Response-Header und Trailer werden in einem einzigen HTTP/2 HEADERS-Rahmenblock ausgeliefert. Die meisten Antworten werden voraussichtlich sowohl Header als auch Trailer haben, aber Trailer Only ist für Anrufe zulässig, die einen sofortigen Fehler verursachen. Der Status muss in Trailers gesendet werden, auch wenn der HTTP-Statuscode in Ordnung ist.

```
```
HEADERS (flags = END_HEADERS)
: status = 200
Grpc-encoding= gzip
Content-type = application/grpc+proto
DATA
<Length-Prefixed Message>
HEADERS (flags = END_STREAM, END_HEADERS)
grpc-status = 0 # OK

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

Konfigurieren von GRPC über die CLI

Um eine End-to-End-GrPC-Bereitstellung zu konfigurieren, müssen Sie Folgendes ausführen:

- Fügen Sie ein HTTP-Profil hinzu, wenn HTTP/2 und HTTP/2 direkt aktiviert sind.

- Aktivieren Sie die globale Back-End-HTTP/2-Unterstützung in HTTP-Parametern
- Fügen Sie einen virtuellen Lastausgleichsserver vom Typ SSL/HTTP hinzu und legen Sie das HTTP-Profil fest
- Dienst für GrPC Endpoint hinzufügen und HTTP-Profil festlegen
- Binden Sie den GrPC-Endpunktdienst an den virtuellen Lastausgleichsserver

Fügen Sie ein HTTP-Profil mit aktiviertem HTTP/2 und HTTP/2 hinzu

Sie müssen die direkten HTTP/2- und HTTP/2-Parameter im HTTP-Profil aktivieren. Außerdem müssen Sie den direkten HTTP/2-Parameter aktivieren, wenn gRPC über HTTP/2-Klartext erforderlich ist.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Beispiel:

```
add ns httpProfile http2gRPC -http2Direct ENABLED -http2 ENABLED
```

Aktivieren Sie die globale Back-End-HTTP/2-Unterstützung über HTTP-Parameter

Um die HTTP/2-Unterstützung global auf der Serverseite zu aktivieren, verwenden Sie die Citrix ADC Befehlszeile.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns httpParam -http2ServerSide( ON | OFF )
```

Beispiel:

```
set ns httpParam -http2ServerSide ON
```

Fügen Sie einen virtuellen Lastausgleichsserver vom Typ SSL/HTTP hinzu und legen Sie das HTTP-Profil fest

So fügen Sie einen virtuellen Lastenausgleichsserver mit der **Citrix ADC** Befehlszeilenschnittstelle hinzu:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <service type> [(<IP address>@ <port>)] [-httpProfileName
 <string>]
```

Beispiel:

```
add lb vserver lb-grpc HTTP 10.10.10.11 80 -httpProfileName http2gRPC
```


> **Hinweis:**
>
> Wenn Sie einen virtuellen Lastausgleichsserver vom Typ SSL verwenden, müssen Sie das Serverzertifikat binden. Weitere Informationen finden Sie unter Binden von Serverzertifikaten.

Dienst für GrPC Endpoint hinzufügen und HTTP-Profil festlegen

So fügen Sie mithilfe der **Citrix ADC** Befehlszeilenschnittstelle einen gRPC-Dienst mit HTTP-Profil hinzu: Geben Sie
an der Eingabeaufforderung Folgendes ein:

```
add service <name> (<IP> | <serverName> )<serviceType> <port> [-httpProfileName
 <string>]
```

Beispiel:

```
add service svc-grpc 10.10.10.10 HTTP 80 -httpProfileName http2gRPC
```

Binden Sie den GrPC-Endpunktdienst an den virtuellen Lastausgleichsserver

So binden Sie einen gRPC-Dienst mithilfe der **Citrix ADC** Befehlszeilenschnittstelle an den virtuellen Lastenausgleichsserver:

Geben Sie an der Befehlszeilenschnittstelle Folgendes ein:

```
bind lb vserver <name> <serviceName>
```

Beispiel:

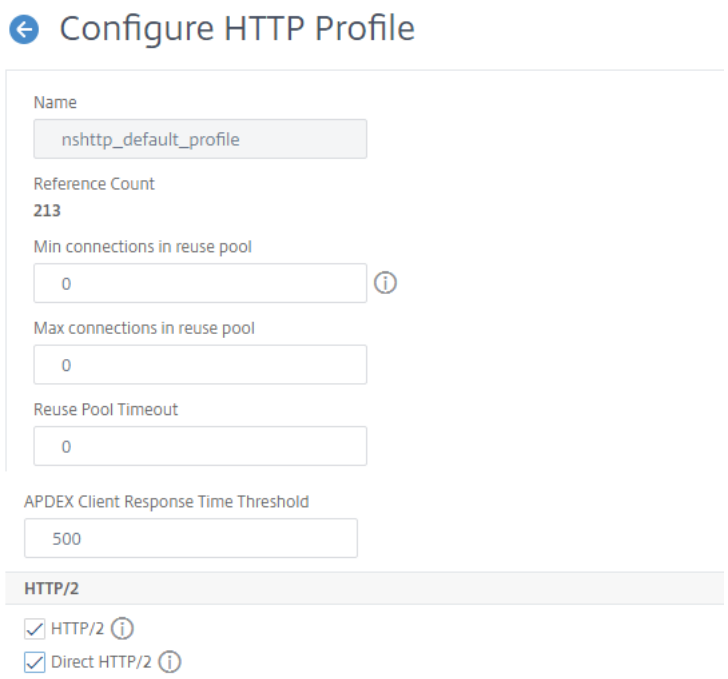
```
bind lb vserver lb-grpc svc-grpc
```

Konfigurieren der End-to-End-GrPC-Bereitstellung über die GUI

Führen Sie die folgenden Schritte durch, um GrPC mit der GUI zu konfigurieren.

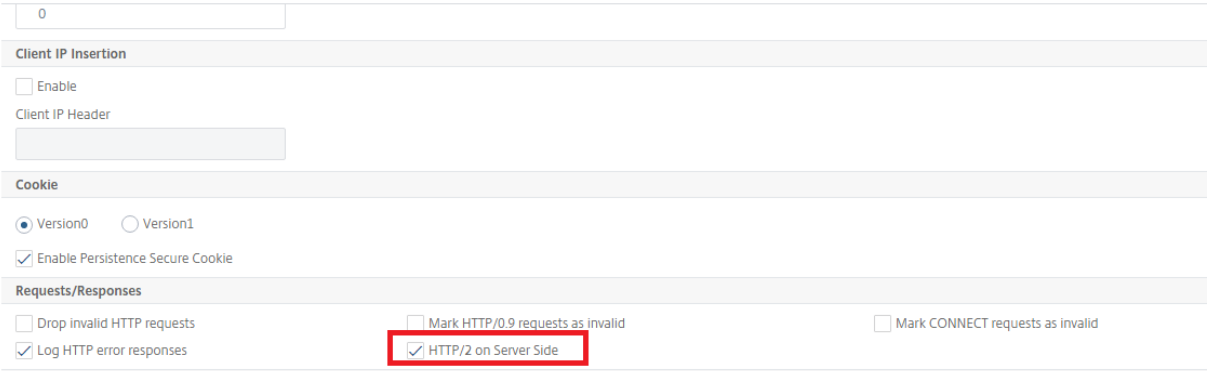
Fügen Sie ein HTTP-Profil mit aktiviertem HTTP/2 und HTTP/2 hinzu

1. Navigieren Sie zu **System > Profile** und klicken Sie auf **HTTP-Profile**.
2. Aktivieren Sie die HTTP/2-Option in einem neuen HTTP-Profil oder einem vorhandenen HTTP-Profil



Aktivieren Sie die globale Back-End-HTTP/2-Unterstützung in HTTP-Parametern

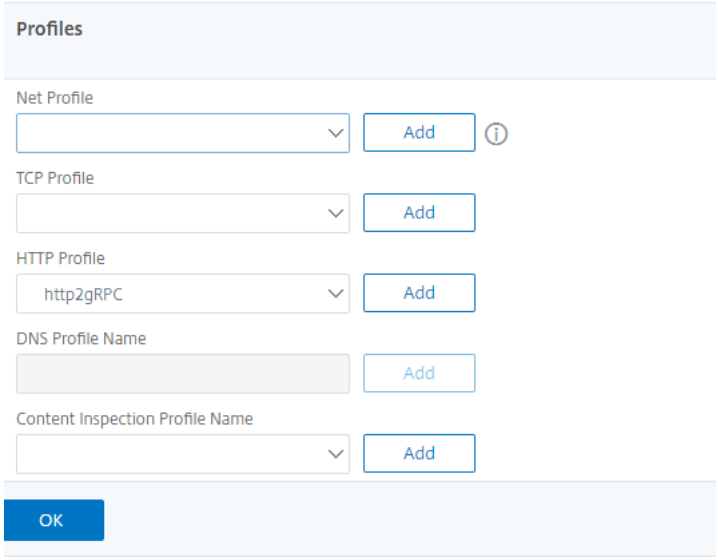
1. Navigieren Sie zu **System > Einstellungen > HTTP-Parameter**.
2. Wählen Sie auf der Seite “HTTP-Parameter konfigurieren” HTTP/2 auf Serverseite aus.
3. Klicken Sie auf **OK**.



Fügen Sie einen virtuellen Lastausgleichsserver vom Typ SSL/HTTP hinzu und legen Sie das HTTP-Profil fest

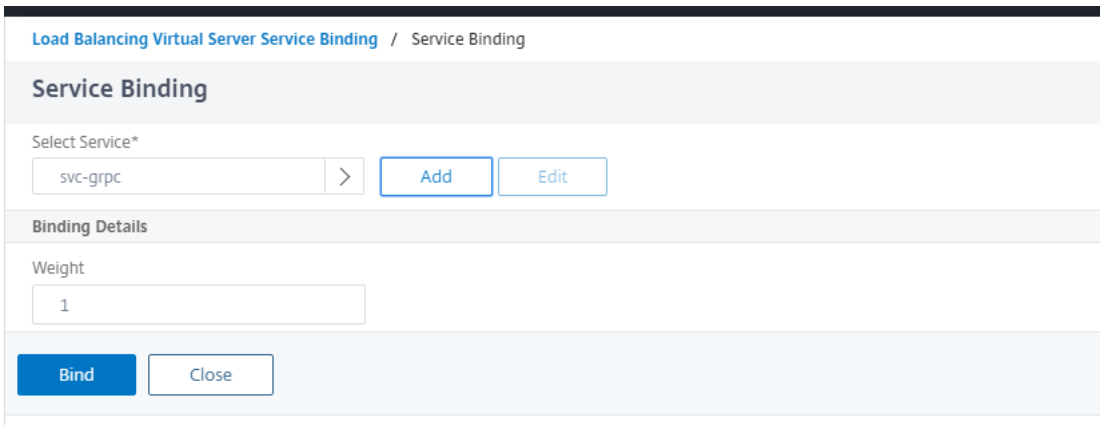
1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie auf Hinzufügen, um einen virtuellen Lastausgleichsserver für gRPC-Datenverkehr zu erstellen.
3. Klicken Sie auf der Seite Virtueller Server für Lastenausgleich auf Profile.

4. Wählen Sie im Abschnitt Profile den Profiltyp als HTTP aus.
5. Klicken Sie auf OK und dann auf Fertig.



Dienst für GrPC Endpoint hinzufügen und HTTP-Profil festlegen

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Klicken Sie auf Hinzufügen, um einen Anwendungsserver für gRPC-Datenverkehr zu erstellen.
3. Wechseln Sie auf der Seite Load Balancing Service zum Abschnitt Profil.
4. Fügen Sie unter Profileein HTTP-Profil für den GrPC-Endpoint hinzu.
5. Klicken Sie auf OK und dann auf Fertig.



Ausführliche GUI-Prozeduren im Zusammenhang mit dem Lastenausgleich finden Sie unter Thema Load Balancing .

gRPC-Bridging

October 5, 2021

Wenn ein Client eine Anfrage über das HTTP/1.1-Protokoll sendet, unterstützt die Citrix ADC Appliance die Überbrückung der gRPC-Anforderungen über das HTTP/1.1-Protokoll, das dem gRPC-Server über das HTTP/2-Protokoll entspricht. In ähnlicher Weise erhält die Appliance beim Reverse Bridging die Client-GrPC-Anforderung über das HTTP/2-Protokoll und führt eine Rückwärtsbrückenüberbrückung für die gRPC-Anforderungen in Übereinstimmung mit dem gRPC-Server des HTTP/1.1-Protokolls durch.

So funktioniert das GrPC-Bridging

In diesem Szenario überbrückt die Citrix ADC Appliance gRPC-Inhalte, die auf einer HTTP/1.1-Verbindung empfangen wurden, nahtlos und leitet sie über HTTP/2 an den Back-End-gRPC-Server weiter.

Das folgende Diagramm zeigt, wie Komponenten in einer gRPC-Bridging-Konfiguration miteinander interagieren.

1. Wenn eine GrPC-Anfrage gesendet wird, prüft die Citrix ADC Appliance, ob die Verbindung HTTP/1.1 ist und der Inhaltstyp application/grpc ist. Die HTTP/1.1-Anfragen werden in die folgenden Pseudo-Header übersetzt.
2. Nach Erhalt einer GrPC-Anfrage für die HTTP/1.1-Verbindung, wie im Content-Type-Header angegeben, wandelt die ADC-Appliance die Anfrage wie folgt in gRPC über HTTP/2 um:

```
    :method: Method-name in HTTP/1.1 request
    :path: Path is HTTP/1.1 request
    content-type: application/grpc
<!--NeedCopy-->
```


1. Basierend auf der Richtlinienbewertung beendet der virtuelle Lastausgleichsserver (an den der gRPC-Dienst gebunden ist) die Anforderung oder leitet sie über HTTP/2-Frames an den Back-End-gRPC-Server weiter.
2. Nach Erhalt der Antwort auf eine HTTP/2-Verbindung vom gRPC-Server puffert die Appliance, bis sie den HTTP/2-Trailer erhält und sucht dann nach dem GRPC-Statuscode. Wenn es sich um einen gRPC-Fehlerstatus ungleich Null handelt, sucht die Appliance nach dem Zuordnungsstatuscode und sendet eine geeignete HTTP/1.1-Fehlerantwort.

Konfigurieren der GRPC-Bridging über die CLI

Um GrPC-Bridging zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Fügen Sie ein HTTP-Profil mit aktiviertem HTTP/2 und HTTP/2 hinzu
2. Aktivieren der globalen Back-End-HTTP/2-Unterstützung im HTTP-Parameter
3. Fügen Sie einen virtuellen Lastausgleichsserver vom Typ SSL/HTTP hinzu und legen Sie das HTTP-Profil fest
4. Fügen Sie den Dienst für den GrPC-Endpunkt hinzu und legen Sie das HTTP-Profil fest
5. Binden Sie den GrPC-Endpunktdienst an den virtuellen Lastausgleichsserver
6. Ordnen Sie der HTTP-Statuscode der HTTP-Antwort zu, um einen gRPC-Status ungleich
7. Konfigurieren Sie die gRPC-Pufferung nach Zeit und/oder Größe

Fügen Sie HTTP-Profil hinzu, wenn HTTP/2 und HTTP/2 direkt aktiviert sind

Um mit der Konfiguration zu beginnen, müssen Sie die HTTP/2-Funktion im HTTP-Profil aktivieren. Wenn der Client die HTTP 1.1-Anfragen sendet, überbrückt die Appliance die Anfrage und leitet sie an den Back-End-Server weiter.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Beispiel:

```
add ns httpProfile http2gRPC -http2Direct ENABLED -http2 ENABLED
```

Aktivieren Sie die globale Back-End-HTTP/2-Unterstützung im HTTP-Parameter

Um die HTTP/2-Unterstützung global auf der Serverseite zu aktivieren, verwenden Sie die Citrix ADC Befehlszeile.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns httpParam -http2ServerSide( ON | OFF )
```


Beispiel:

```
set ns httpParam -http2ServerSide ON
```

Fügen Sie einen virtuellen Lastausgleichsserver vom Typ SSL/HTTP hinzu und legen Sie das HTTP-Profil fest

So fügen Sie einen virtuellen Lastenausgleichsserver mit der **Citrix ADC** Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <service type> [(<IP address>@ <port>)] [-httpProfileName
 <string>]
```

Beispiel:

```
add lb vserver lb-grpc HTTP 10.10.10.10 80 -httpProfileName http2gRPC
```

> **Hinweis:**
>
> Wenn Sie einen virtuellen Lastausgleichsserver vom Typ SSL verwenden, müssen Sie das Serverzertifikat binden. Weitere Informationen finden Sie unter Thema Serverzertifikat binden .

Fügen Sie den Dienst für den GrPC-Endpunkt hinzu und legen Sie das HTTP-Profil fest

So fügen Sie mithilfe der **Citrix ADC** Befehlszeilenschnittstelle einen gRPC-Dienst mit dem HTTP-Profil hinzu.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name> (<IP> | <serverName> )<serviceType> <port> [-httpProfileName
 <string>]
```

Beispiel:

```
add service svc-grpc 10.10.10.10 HTTP 80 -httpProfileName http2gRPC
```

Binden Sie den GrPC-Endpunktdienst an den virtuellen Lastausgleichsserver

So binden Sie einen gRPC-Endpunktdienst mit der CLI an den virtuellen Lastausgleichsserver.

Geben Sie an der Befehlszeilenschnittstelle Folgendes ein:

```
bind lb vserver <name> <serviceName>
```

Beispiel:

```
bind lb vserver lb-grpc svc-grpc
```


Ordnen Sie den gRPC-Statuscode dem HTTP-Statuscode in der HTTP/1.1-Antwort zu

Im gRPC-Bridging-Szenario antwortet der gRPC-Dienst mit einem gRPC-Statuscode auf die Anfrage. Die Appliance ordnet den gRPC-Statuscode einem entsprechenden HTTP-Antwortcode und einer Ursache-Phrase zu. Die Zuordnung erfolgt auf der Grundlage der unten angegebenen Tabelle. Die Citrix ADC Appliance sendet beim Senden der HTTP/1.1-Antwort an den Client den HTTP-Statuscode und die Ursachenphrase.

gRPC Statuscode	HTTP-Antwort-Statuscode	Grundsatz der HTTP-Antwort
OK = 0	200	OK
CANCELLED = 1	499	*
UNKNOWN = 2	500	Interner Serverfehler
INVALID_ARGUMENT = 3	400	Ungültige Anforderung
DEADLINE_EXCEEDED = 4	504	Gatewaytimeout
NOT_FOUND = 5	404	*
ALREADY_EXISTS = 6	409	Konflikt
PERMISSION_DENIED = 7	403	Verboten
UNAUTHENTICATED = 16	401	Nicht autorisiert
RESOURCE_EXHAUSTED = 8	429	*
FAILED_PRECONDITION = 9	400	Ungültige Anforderung
ABORTED = 10	409	Konflikt
OUT_OF_RANGE = 11	400	Ungültige Anforderung
UNIMPLEMENTED = 12	501	Nicht implementiert
INTERNAL = 13	500	Interner Serverfehler
UNAVAILABLE = 14	503	Dienst ist nicht verfügbar
DATA_LOSS = 15	500	Interner Serverfehler

Konfigurieren Sie die gRPC-Pufferung nach Zeit und/oder Größe

Die Citrix ADC Appliance puffert die gRPC-Antwort vom Back-End-Server, bis der Response Trailer empfangen wird. Dies unterbricht bidirektionale GrPC-Anrufe. Wenn die GrPC-Antwort enorm ist, verbraucht sie außerdem eine beträchtliche Menge an Speicher, um die Antwort vollständig zu puffern. Um das Problem zu lösen, wurde die gRPC-Bridging-Konfiguration verbessert, um die Pufferung nach

Zeit und/oder Größe zu begrenzen. Wenn die Puffergröße oder das Zeitlimit den Schwellenwert überschreitet, stoppt die Appliance die Pufferung und leitet die Antwort an den Client weiter, selbst wenn eine der Einschränkungen ausgelöst wird (entweder wird der Trailer nicht innerhalb der konfigurierten Puffergröße empfangen oder wenn das konfigurierte Timeout auftritt). Daher funktionieren die konfigurierten Richtlinien und ihre Ausdrücke (basierend auf dem grpc-statuscode) nicht wie erwartet.

Um die gRPC-Pufferung nach Zeit und/oder Größe durch die CLI zu beschränken, können Sie konfigurieren, wann Sie ein neues HTTP-Profil hinzufügen oder konfigurieren, wann Sie ein vorhandenes Profil ändern.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns httpProfile http2gRPC [-grpcHoldLimit <positive_integer>] [-grpcHoldTimeout
 <positive_integer>]
```

oder

```
set ns httpProfile http2gRPC [-grpcHoldLimit <positive_integer>] [-grpcHoldTimeout
 <positive_integer>]
```

Hierbei gilt:

`grpcholdlimit`. Maximale Größe in Byte, die gRPC-Pakete puffern dürfen, bis der Trailer empfangen wird. Sie können sowohl die Parameter als auch jeden einzelnen konfigurieren.

Standardwert: 131072
Mindestwert: 0
Maximaler Wert: 33554432

`grpcholdtimeout`. Maximale Zeit in Millisekunden, die gRPC-Pakete puffern dürfen, bis der Trailer empfangen wird. Der Wert sollte ein Vielfaches von 100 sein.
Standardwert: 1000
Mindestwert: 0
Maximaler Wert: 180000

Beispiel:

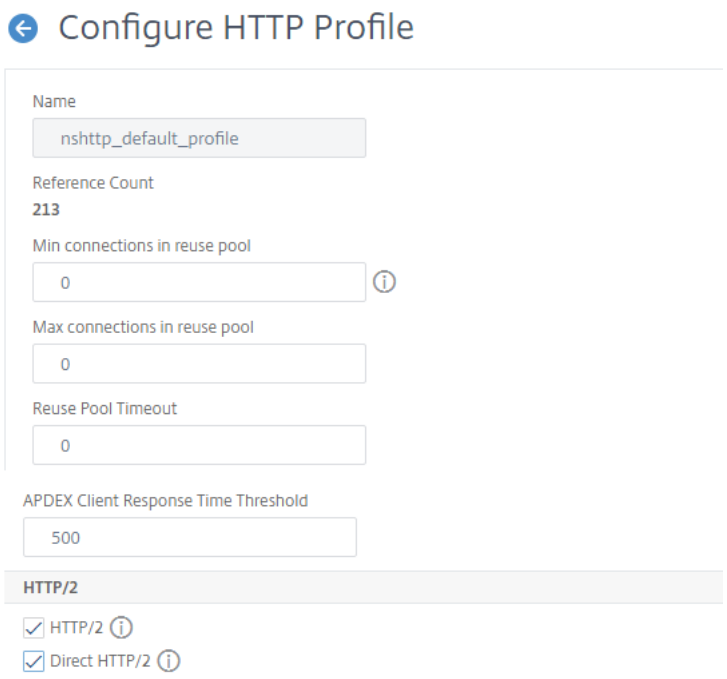
```
add httpprofile http2gRPC -grpcholdlimit 1048576 -grpcholdtimeout 5000
set httpprofile http2gRPC -grpcholdlimit 1048576 -grpcholdtimeout 5000
```

Konfigurieren Sie das GrPC-Bridging mit der GUI

Führen Sie die folgenden Schritte aus, um das GrPC-Bridging mithilfe der Citrix ADC GUI zu konfigurieren.

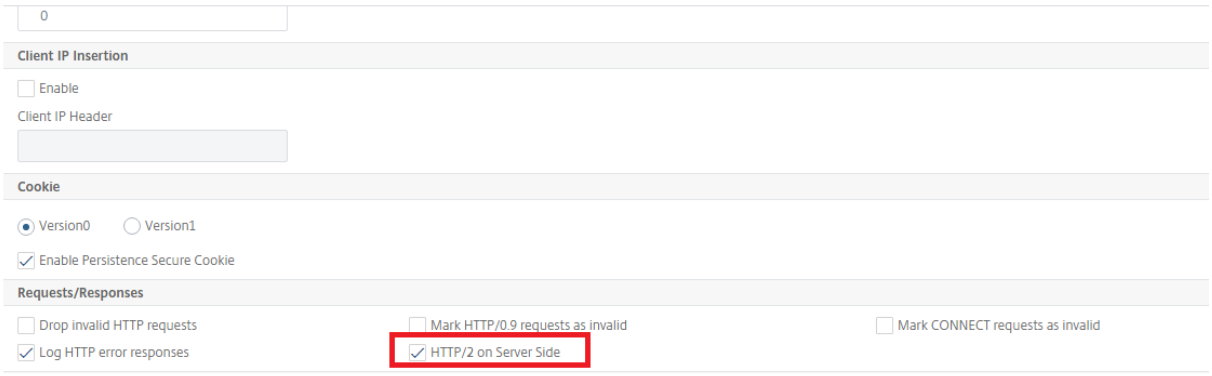
Fügen Sie ein HTTP-Profil mit aktiviertem HTTP/2 und HTTP/2 hinzu

1. Navigieren Sie zu **System > Profile** und klicken Sie auf **HTTP-Profile**.
2. Wählen Sie **HTTP/2** im HTTP-Profil aus.



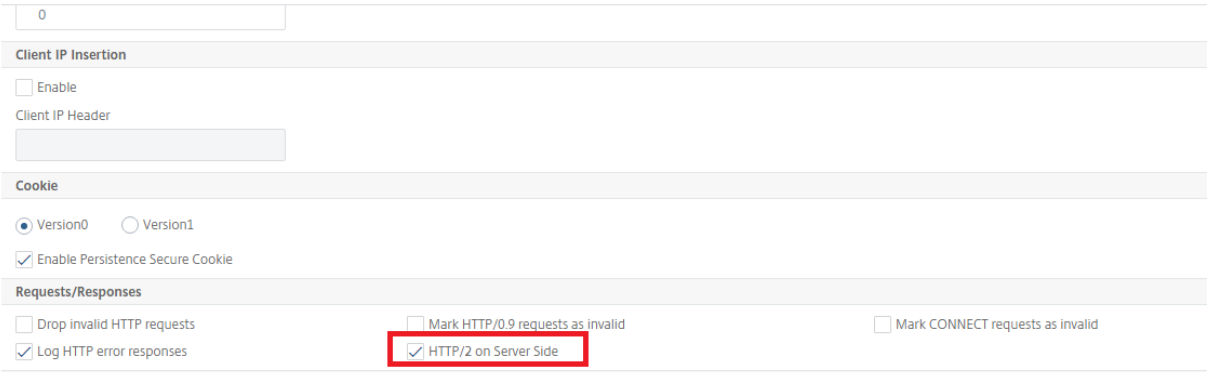
Aktivieren der globalen Back-End-HTTP/2-Unterstützung im HTTP-Parameter

1. Navigieren Sie zu **System > Einstellungen > HTTP-Parameter**.
2. Wählen Sie auf der Seite " **HTTP-Parameter konfigurieren** " die Option **HTTP/2 auf Serverseite** aus.
3. Klicken Sie auf **OK**.



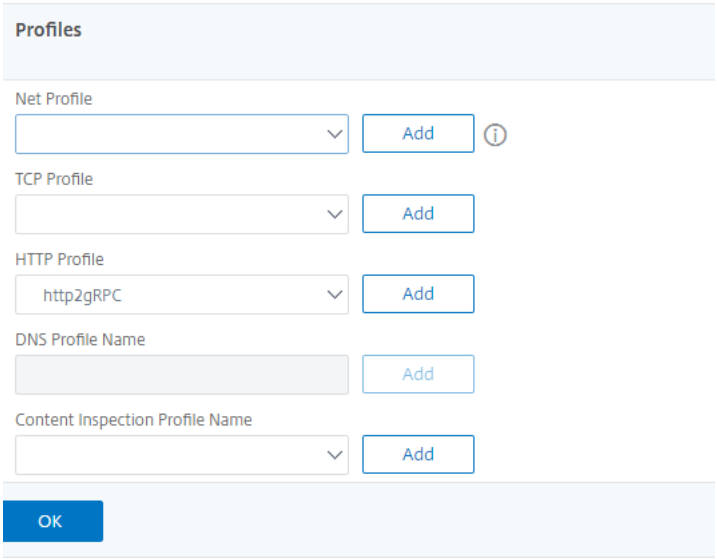
Fügen Sie einen virtuellen Lastausgleichsserver vom Typ SSL/HTTP hinzu und legen Sie das HTTP-Profil fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie auf **Hinzufügen**, um einen virtuellen Lastausgleichsserver für gRPC-Datenverkehr zu erstellen.
3. Klicken Sie auf der Seite **Virtueller Server für Lastenausgleich** auf **Profile**.
4. Wählen Sie im Abschnitt **Profile** den Profiltyp als HTTP aus.
5. Klicken Sie auf **OK** und dann auf **Fertig**.



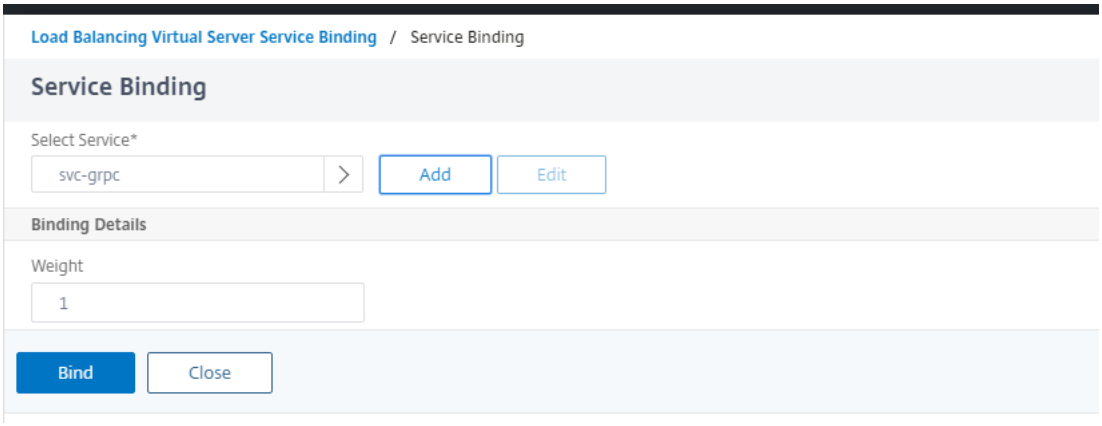
Dienst für GrPC Endpoint hinzufügen und HTTP-Profil festlegen

1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Klicken Sie auf **Hinzufügen**, um einen Anwendungsserver für gRPC-Datenverkehr zu erstellen.
3. Wechseln Sie auf der Seite **Load Balancing Service** zum Abschnitt **Profil**.
4. Fügen Sie unter **Profile**ein **HTTP-Profil** für den GrPC-Endpoint hinzu.
5. Klicken Sie auf **OK** und dann auf **Fertig**.



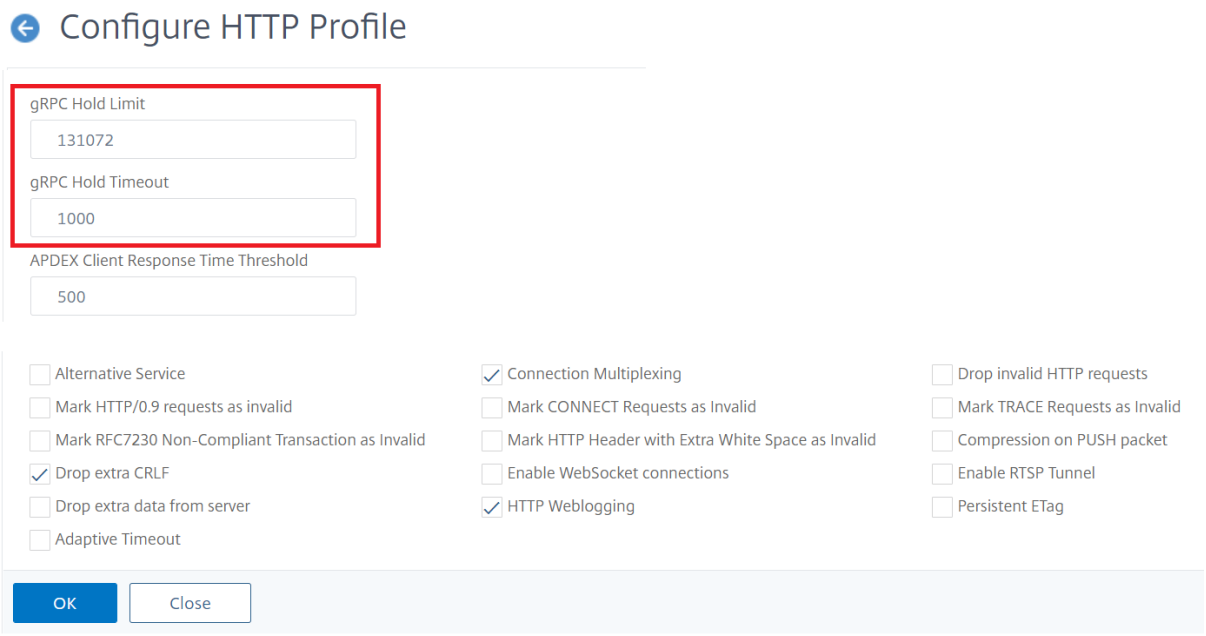
Bind-Dienst für GrPC-Endpunkt zum Lastenausgleich des virtuellen Servers

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie auf **Hinzufügen**, um einen virtuellen Lastausgleichsserver für gRPC-Datenverkehr zu erstellen.
3. Klicken Sie auf der Seite **Load Balancing Virtual Server** auf den Abschnitt **Dienst- und Dienstgruppen** .
4. Wählen Sie auf der Seite **Load Balancing Virtual Server Service Binding** den gRPC-Dienst aus, der gebunden werden soll.
5. Klicken Sie auf **Schließen** und dann auf **Fertig**.



Konfigurieren Sie die gRPC-Pufferung nach Zeit und Größe mit der GUI

1. Navigieren Sie zu **System > Profile** und klicken Sie auf **HTTP-Profile**.
2. Wählen Sie **HTTP/2** im HTTP-Profil aus.
3. Legen Sie auf der Seite **HTTP-Profil konfigurieren** die folgenden Parameter fest:
   a) grpcHoldTimeout. Geben Sie die Zeit in Millisekunden ein, um gRPC-Pakete zu puffern, bis der Trailer empfangen wird.
   b) grpcHoldLimit. Geben Sie die maximale Größe in Bytes ein, um gRPC-Pakete zu puffern, bis der Trailer empfangen wird.
4. Klicken Sie auf **OK** und **schließen**.



Ausführliche GUI-Prozeduren für das Binden von Service und Lastenausgleich virtueller Server finden Sie unter Thema Load Balancing .

GrPC Reverse Bridging

October 5, 2021

In diesem Szenario überbrückt die Citrix ADC Appliance gRPC-Inhalte, die auf einer HTTP/2-Verbindung empfangen wurden, nahtlos und leitet sie über HTTP/1.1 an den Back-End-gRPC-Server weiter.

Wie funktioniert Reverse Bridging

Das folgende Diagramm zeigt, wie Komponenten in einer gRPC-Bridging-Konfiguration miteinander interagieren.

1. Der Client sendet eine gRPC-Anfrage für eine HTTP/2-Verbindung mit gRPC-Headern in HTTP/2-Frames und Proto-buf-Nutzlast.
2. Basierend auf der Richtlinienbewertung übersetzt und leitet der virtuelle Lastausgleichsserver (an den gRPC-Dienst gebunden ist) die Anfrage über die HTTP/1.1-Verbindung an den Backend-Server weiter.
3. Wenn beim Empfang der HTTP/1.1-Antwort kein grpc-statuscode in der Antwort enthalten ist, leitet ADC einen grpc-Statusfall vom HTTP-Antwortcode ab.
4. Die Appliance fügt dann die GrPC-Header in den HTTP/2-Trailer ein, bevor die Antwort an den Client weitergeleitet wird.

Konfigurieren von GRPC Reverse Bridging über die CLI

Um GrPC Reverse Bridging zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

- Fügen Sie HTTP-Profil 1 hinzu, wobei HTTP/2 und HTTP/2 direkt für den virtuellen Lastausgleich aktiviert sind
- Fügen Sie HTTP-Profil 2 hinzu, wobei HTTP/2 für Back-End-Server deaktiviert ist
- Fügen Sie einen virtuellen Lastenausgleichsserver vom Typ SSL/HTTP hinzu und legen Sie ihn auf HTTP-Profil 1 fest
- Dienst für GrPC-Endpoint hinzufügen und auf HTTP-Profil 2 setzen
- Bind-Dienst für GrPC-Endpunkt zum Lastenausgleich des virtuellen Servers
- Ordnen Sie HTTP-Statuscode dem gRPC-Statuscode zu, wenn die Antwort keinen grpc-Statuscode hat

Fügen Sie HTTP-Profil 1 hinzu, wobei HTTP/2 und HTTP/2 direkt für den virtuellen Lastausgleich aktiviert sind

Um mit der Reverse Bridging-Konfiguration zu beginnen, müssen Sie zwei HTTP-Profile hinzufügen. Ein Profil zum Aktivieren von HTTP/2 für GrPC-Clientanfragen und ein weiteres Profil zum Deaktivieren von HTTP/2 für Nicht-GRPC-Serverantwort.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Beispiel:

add ns httpProfile profile1 –http2 ENABLED -http2Direct ENABLED

Fügen Sie HTTP-Profil 2 hinzu, wobei HTTP/2 für Back-End-Server deaktiviert ist

Deaktivieren der HTTP/2-Unterstützung für das HTTP-Profil für Back-End-Serverantwort mithilfe der Citrix ADC Befehlszeile.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ns httpProfile <name> - http2 ( ENABLED | DISABLED )[-http2Direct (
ENABLED | DISABLED )]
```

Beispiel:

add ns httpProfile profile2 –http2 DISABLED http2Direct DISABLED

Fügen Sie einen virtuellen Lastenausgleichsserver vom Typ SSL/HTTP hinzu und legen Sie ihn auf HTTP-Profil 1 fest

So fügen Sie einen virtuellen Lastenausgleichsserver mithilfe der Citrix ADC Befehlszeilenschnittstelle hinzu.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name> <service type> [(<IP address>@ <port>)] [-httpProfileName
 <string>]
```

Beispiel:

add lb vserver lb-grpc HTTP 10.10.10.10 80 -httpProfileName profile1

> **Hinweis:**
>
> Wenn Sie einen virtuellen Lastausgleichsserver vom Typ SSL verwenden, müssen Sie das Serverzertifikat binden. Weitere Informationen finden Sie unter Binden von Serverzertifikaten.

Dienst für GrPC-Endpoint hinzufügen und auf HTTP-Profil 2 setzen

So fügen Sie einen Dienst mit dem GrPC-Endpunkt hinzu und legen das HTTP-Profil 2 mithilfe der Citrix ADC Befehlszeilenschnittstelle fest.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name> (<IP> | <serverName> )<serviceType> <port> [-httpProfileName
 <string>]
```

Beispiel:

```
add service svc-grpc 10.10.10.11 HTTP 80 -httpProfileName profile2
```


Bind-Dienst für GrPC-Endpunkt zum Lastenausgleich des virtuellen Servers

So binden Sie einen gRPC-Dienst mithilfe der Citrix ADC Befehlszeilenschnittstelle an den virtuellen Lastenausgleichsserver.

Geben Sie an der Befehlszeilenschnittstelle Folgendes ein:

```
bind lb vserver <name> <serviceName>
```

Beispiel:

```
bind lb vserver lb-grpc svc-grpc
```

Ordnen Sie HTTP-Antwortcode auf gRPC-Status

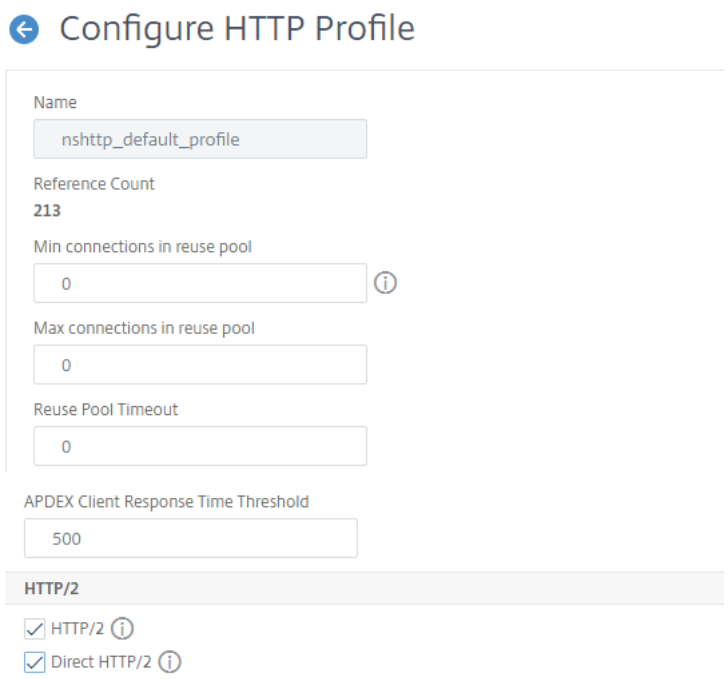
Wenn der Server keinen gRPC-Statuscode generiert, generiert die Citrix ADC Appliance einen geeigneten gRPC-Statuscode basierend auf der empfangenen HTTP-Antwort. Die Statuscodes sind in der folgenden Zuordnungstabelle aufgeführt.

HTTP-Antwort-Statuscode	gRPC Statuscode
200	OK
400	INTERNAL = 13
403	PERMISSION_DENIED = 7
401	UNAUTHENTICATED = 16
429, 502, 503, 504	UNAVAILABLE = 14
404	UNIMPLEMENTED = 12

Konfigurieren Sie das GrPC-Reverse Bridging mit der GUI

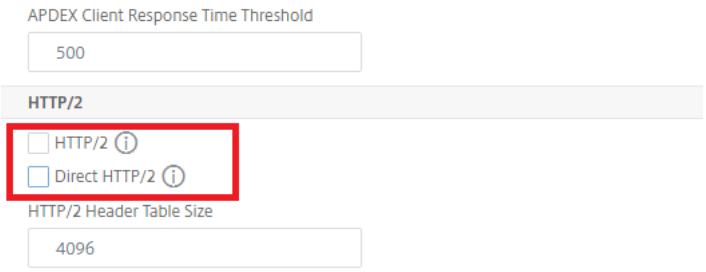
Fügen Sie HTTP-Profil 1 hinzu, wobei HTTP/2 und HTTP/2 direkt für den virtuellen Lastausgleich aktiviert sind

1. Navigieren Sie zu System > Profile und klicken Sie auf HTTP-Profile.
2. Aktivieren Sie die HTTP/2-Option in einem HTTP-Profil 1.



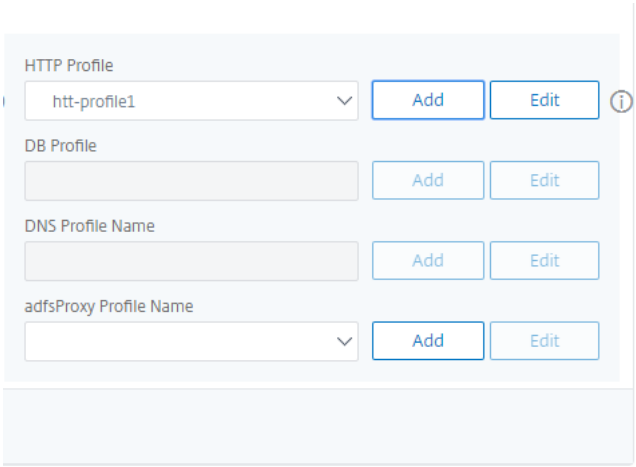
Fügen Sie HTTP-Profil 2 hinzu, wobei HTTP/2 für Back-End-Server deaktiviert ist

1. Navigieren Sie zu **System > Profile** und klicken Sie auf **HTTP-Profile**.
2. Aktivieren Sie die **HTTP/2-Option** in einem HTTP-Profil 2.
3. Klicken Sie auf **OK**.



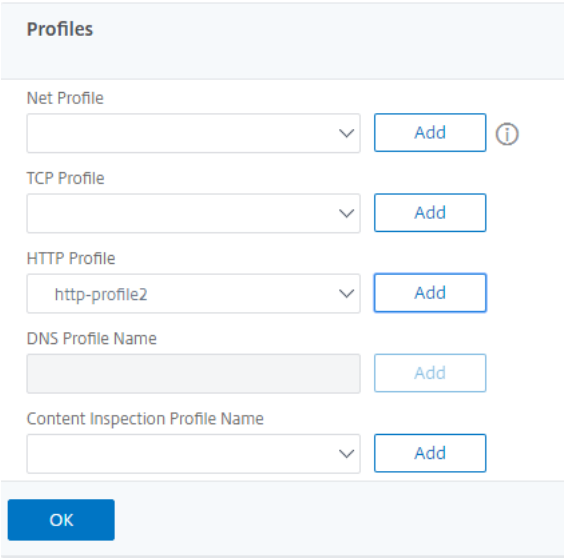
Fügen Sie einen virtuellen Lastenausgleichsserver vom Typ SSL/HTTP hinzu und legen Sie ihn auf HTTP-Profil 1 fest

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie auf **Hinzufügen**, um einen virtuellen Lastausgleichsserver für gRPC-Datenverkehr zu erstellen.
3. Klicken Sie auf der Seite **Virtueller Server für Lastenausgleich** auf **Profile**.
4. Wählen Sie im Abschnitt **Profile** den Profiltyp als HTTP aus.
5. Klicken Sie auf **OK** und dann auf **Fertig**.



Dienst mit GrPC-Endpunkt hinzufügen und auf HTTP-Profil 2 setzen

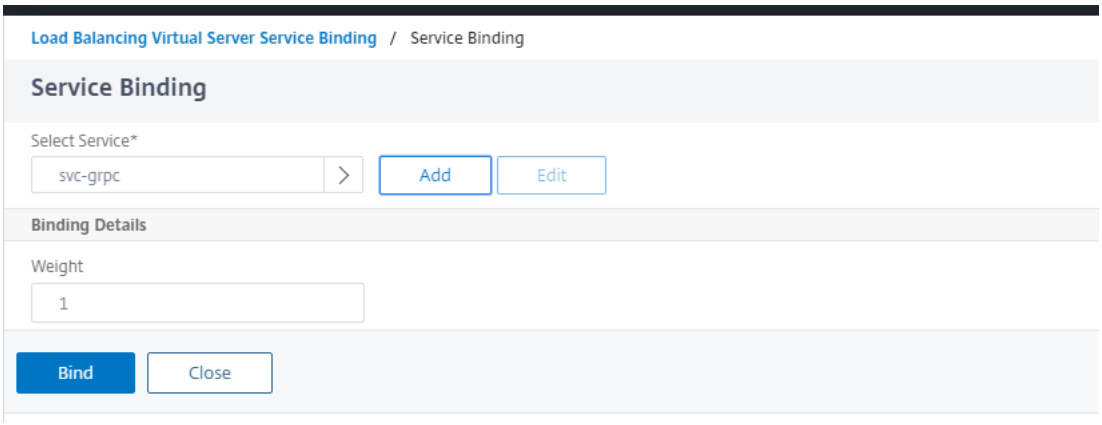
1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**.
2. Klicken Sie auf **Hinzufügen**, um einen Anwendungsserver für gRPC-Datenverkehr zu erstellen.
3. Wechseln Sie auf der Seite **Load Balancing Service** zum Abschnitt **Profil**.
4. Fügen Sie unter **Profile**ein **HTTP-Profil** für den GrPC-Endpoint hinzu.
5. Klicken Sie auf **OK** und dann auf **Fertig**.



Bind-Dienst für GrPC-Endpunkt zum Lastenausgleich des virtuellen Servers

1. Navigieren Sie zu **Traffic Management > Load Balancing > Virtuelle Server**.
2. Klicken Sie auf **Hinzufügen**, um einen virtuellen Lastausgleichsserver für gRPC-Datenverkehr zu erstellen.

3. Klicken Sie auf der Seite **Load Balancing Virtual Server** auf Abschnitt **Service** und **Service Groups**.
4. Wählen Sie auf der Seite **Load Balancing Virtual Server Service Binding** den gRPC-Dienst aus, der gebunden werden soll.
5. Klicken Sie auf **Schließen** und dann auf **Fertig**.



Ausführliche GUI-Prozeduren finden Sie unter Thema Load Balancing .

gRPC call termination

October 5, 2021

Wenn eine Citrix ADC Appliance Richtlinien wie Ratenbegrenzung, Web App Firewall -Sicherheit konfiguriert hat und wenn eine Richtlinie als true bewertet wird, kann die Appliance den Anruf beenden und mit einer computerbaren gRPC-Fehlermeldung an den Client antworten.

gRPC mit Rewrite-Richtlinie

October 5, 2021

Der Anwendungsfall für GrPC mit Umschreibungsrichtlinie erklärt, wie die Citrix ADC Appliance einige Informationen in den GrPC-Anforderungen oder -Antworten umschreibt. Das folgende Diagramm zeigt die Interaktion der Komponenten.

Das folgende Diagramm zeigt, wie Komponenten in einem gRPC mit Rewrite-Richtlinienkonfiguration miteinander interagieren.

1. Aktivieren Sie die Rewrite-Funktion auf der Appliance.
2. Konfigurieren Sie die Aktion zum Umschreiben, um GrPC-Header zu ändern, hinzuzufügen oder zu löschen.
3. Konfigurieren Sie die Rewrite-Richtlinie zur Bestimmung der GrPC-Anforderungen (Traffic), für die eine Aktion durchgeführt werden muss.
4. Binden Sie die Richtlinie zum Umschreiben an den virtuellen Lastausgleichsserver, um zu prüfen, ob der Datenverkehr mit dem Richtlinienausdruck übereinstimmt.
5. Mithilfe einer Rewrite-Richtlinie können Sie basierend auf dem gRPC-Statuscode Folgendes ausführen.
   a) Ändern Sie die Antworten vom gRPC-Webserver.
   b) Ändern, hinzufügen oder löschen Sie GrPC-Header.
   c) Ändern Sie die URL der Anfrage an den GrRC-Server.

Konfigurieren Sie die GrPC-Anrufbeendigung mit Rewrite-Richtlinie

Um die GrPC-Anrufbeendigung mit Rewrite-Richtlinie zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Rewrite-Funktion aktivieren
2. Richtlinie zum Umschreiben hinzufügen
3. Richtlinie zum Umschreiben an den virtuellen Lastenausgleich binden

Rewrite-Funktion aktivieren

Um die Rewrite-Funktion verwenden zu können, müssen Sie sie zuerst aktivieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns rewrite
```


Richtlinie zum Umschreiben hinzufügen

Nachdem Sie eine Umschreibaktion konfiguriert haben, müssen Sie als Nächstes eine Umschreibungsrichtlinie konfigurieren, um die GrPC-Anforderungen auszuwählen, die die Citrix ADC Appliance neu schreiben muss.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add rewrite policy <name> <expression> <action> [<undefaction>]-appFlowaction
 <actionName>
```

Beispiel:

```
add rewrite policy grpc-rewr_pol1 ”http.res.header(\”grpc-status\”).NE
(\”0\”)”RESET
```

Richtlinie zum Umschreiben an den virtuellen Lastenausgleich binden

Um eine Richtlinie in Kraft zu setzen, müssen Sie sie mit dem gRPC-Dienst an den virtuellen Lastausgleichsserver binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind rewrite global <policyName> <priority> [<gotoPriorityExpression> [-
type <type>] [-invoke (<labelType> <labelName>)]
```

Beispiel:

```
bind lb vserver lb-grpc -policyName grpc-rewr_pol1 -priority 100
```

gRPC mit der Responder Policy

October 5, 2021

Die Konfiguration der GrPC mit Responder Policy erklärt, wie eine Citrix ADC Appliance unterschiedliche Antworten auf GrPC-Anfragen über das HTTP/2-Protokoll liefert. Wenn Benutzer eine Website-Homepage anfordern, möchten Sie möglicherweise eine andere Homepage angeben, je nachdem, wo sich jeder Benutzer befindet oder welcher Browser der Benutzer verwendet.

Das folgende Diagramm zeigt die Komponenten, die interagieren.

1. Aktivieren Sie die Responder-Funktion auf der Appliance.
2. Konfigurieren Sie die Responder-Aktion, um eine benutzerdefinierte Antwort zu generieren, eine Anfrage auf eine andere Webseite umzuleiten oder eine Verbindung zurückzusetzen.
3. Konfigurieren Sie die Responder-Richtlinie zur Bestimmung der GrPC-Anforderungen (Traffic), für die eine Aktion durchgeführt werden muss.
4. Binden Sie die Responder-Richtlinie an den virtuellen Lastausgleichsserver, um zu prüfen, ob der Datenverkehr mit dem Richtlinienausdruck übereinstimmt.
5. Mithilfe einer Responder Policy können Sie basierend auf dem gPC-Statuscode Folgendes ausführen.

Konfigurieren Sie die GrPC-Anrufbeendigung mit der Responder Policy über die Befehlszeilenschnittstelle

Um die GrPC-Anrufbeendigung mit der Responder-Richtlinie zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

1. Aktivieren Sie die Responder-Funktion
2. Eine Responder Action hinzufügen
3. Fügen Sie eine Responder Policy hinzu und verknüpfen Sie die Responder Action
4. Binden Sie die Responder Policy an den virtuellen Lastenausgleichsserver

Aktivieren Sie die Responder-Funktion

Um die Responder-Funktion verwenden zu können, müssen Sie sie zuerst aktivieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns responder
```

Fügen Sie die Responder Action hinzu

Nachdem Sie die Funktion aktiviert haben, müssen Sie die Responder-Aktion für die Verarbeitung der gRPC-Antwort basierend auf dem vom Back-End-Server zurückgegebenen Statuscode konfigurieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add responder action <name> <type>
```

Beispiel:

```
add responder action grpc-act respondwith "HTTP/1.1 200 OK\r\nServer: NS
-Responder\r\nContent-Type:application/grpc\r\ngrpc-status: 12\r\ngrpc
-message: Not Implemented\r\n\r\n"+ "Method: "+ HTTP.REQ.URL+ "is not
implemented."
```

Responder-Richtlinie hinzufügen

Nachdem Sie eine Responder-Aktion konfiguriert haben, müssen Sie als Nächstes eine Responder-Richtlinie konfigurieren, um die GrPC-Anforderung auszuwählen, auf die die Citrix ADC Appliance antworten muss.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add responder policy <name> <expression> <action> [<undefaction>]-appFlowaction
 <actionName>
```

Beispiel:

```
add responder policy grpc-resp-pol1 HTTP.REQ.URL.NE( "/helloworld.Greeter/
SayHello" )grpc-act
```

Responder-Richtlinie an virtuellen Lastenausgleichsserver binden

Um eine Richtlinie in Kraft zu setzen, müssen Sie sie mit dem gRPC-Dienst an den virtuellen Lastausgleichsserver binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind responder global <policyName> <priority> [<gotoPriorityExpression> [-
type <type>] [-invoke (<labelType> <labelName>)]
```

Beispiel:

```
bind lb vserver lb-grpc svc-grpc -policyName grpc-resp-pol1 -priority 100
```

Weitere Informationen zur Responder Policy finden Sie unter Thema Responder-Richtlinie .

Richtlinienausdrücke zum Abgleichen von GrPC-Protokollpufferfeldern

Die Citrix ADC Appliance unterstützt die folgenden Richtlinienausdrücke in der grPC-Konfiguration:

- **Zugriff auf den GrPC-Protokollpuffer.** Der willkürliche gRPC-API-Aufruf stimmt mit der Nummer des Nachrichtenfelds mit den neuen Richtlinienausdrücken überein. In einer PI-Konfiguration werden die Übereinstimmungen nur mit den “Feldnummern” und “API-Pfad” durchgeführt.
- **GrPC-Header-Filterung.** Die “HttpProfile” -Parameter für grPC werden verwendet, um das Standardverhalten des GrPC-Parsens (einschließlich GrPC-Richtlinienausdrücken) anzupassen. Die folgenden Parameter gelten für GrPC-Richtlinienausdrücke:
  - **GrpClengthDelimitation.** Es ist standardmäßig aktiviert und erwartet, dass die Protokollpuffer mit einer längengetrennten Nachricht angezeigt werden.
  - **GrpCholdLimit.** Der Standardwert ist 131072. Es ist die maximale Größe der Protokollpuffernachricht in Byte. Es ist auch die maximale Stringlänge und die maximale “Byte” -Feldlänge.

Konfigurieren Sie GrPC Advance Policy Ausdrücke mit der CLI

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns httpProfile <name> -http2 ( ENABLED | DISABLED ) -
    gRPCLengthDelimitation ( ENABLED | DISABLED ) -gRPCHoldLimit <int>
```

Beispiel:

```
set ns httpProfile http2gRPC -http2 ENABLED -gRPCLengthDelimitation
    ENABLED -gRPCHoldLimit 131072
```

Konfigurieren Sie GrPC-Header-Filterparameter mit der GUI

1. Navigieren Sie zu **System > Profile** und klicken Sie auf **HTTP-Profile**.
2. Scrollen Sie auf der Seite “ **HTTP-Profil erstellen** “ nach unten zum Abschnitt **HTTP/3** und wählen Sie **GrPC Length Delimitation**aus.

Das folgende Beispiel für einen Richtlinienausdruck zeigt einen Wert in Nachricht 5, Unternachricht 4 und Feld 3. Es ist ein 32-Bit-Int gleich 2.

```
http.req.body(1000).grpc.message(5).message(4).int32(3).eq(2)
```


Die folgenden Richtlinienausdrücke werden hinzugefügt, um die Nachrichtenfelder des GRPC-Protokollpuffers nach Zahlen abzugleichen:

- message
- double
- float
- int32
- int64
- uint32
- uint64
- sint64
- sint32
- fixed32
- fixed64
- sfixed32
- sfixed64
- bool
- string
- enum
- Bytes

API-Pfadabgleich

Der API-Pfadabgleich wird verwendet, um dem korrekten gRPC-API-Aufruf zu entsprechen, wenn mehr als eine API verwendet wird. Stimmen Sie dem API-Pfad überein, der im Pseudo-Header ': path' in der HTTP-Anfrage zu finden ist.

Beispiel:

```
1 http.req.header(":path").eq("acme.inventory.v1/ListBooks")
```

QUIC

October 5, 2021

Quick UDP Internet Protocol (QUIC) ist eine Kombination aus (TCP+TLS+HTTP/2) Protokollen, die auf UDP implementiert sind. Das QUIC-Transportprotokoll multiplexiert die Verbindungen zwischen zwei Endpunkten unter Verwendung von UDP. Auch im Vergleich zu anderen Protokollen bietet QUIC eine hohe Leistung in Bezug auf Sicherheit, schnelle Bereitstellung von Datenverkehr und geringere Latenz.

Eine QUIC-Brücke ist in einer Citrix ADC Appliance zum Lastenausgleich des QUIC-Datenverkehrs zwischen einem QUIC-Client und einem QUIC-Back-End-Server konfiguriert. Die QUIC-Brücke ermöglicht es Ihnen, dauerhafte QUIC-Verbindungen zwischen Client und Server zu haben, wenn eine NAT-Neubindung oder eine Verbindungsmigration vorliegt. Diese Konfiguration verarbeitet jedoch keine Daten. Es wird nur für den Lastenausgleich des QUIC-Datenverkehrs über die Citrix ADC Appliance verwendet.

QUIC-Pakete enthalten eine Verbindungs-ID, damit Endpoints die Pakete mit einer anderen Adresse oder 4-Tupel derselben Verbindung verknüpfen können. Die Verbindungs-ID enthält die Details der Server-ID, die für die Citrix ADC Appliance und die Back-End-Server freigegeben werden. Die Citrix ADC Appliance extrahiert die Verbindungs-ID-Details der Server-ID und sendet den Datenverkehr zurück an den Back-End-Server. Die Verbindungs-IDs befinden sich in geschützten Paketen, die die Verbindungen im Falle einer Verbindungsmigration robust machen.

> **Wichtig**
>
> Die Back-End-Server müssen Unterstützung haben, um die Server-ID in QUIC-Verbindungs-ID zu codieren.

Vorteile der QUIC-Brücke

Die QUIC-Brücke für die Citrix ADC Appliance wird aus folgenden Gründen bevorzugt:

- Keine teuren Kryptooperationen.
- Zustandsloses Routing ist möglich (kein 4-Tupel-basierter Lastenausgleich).

QUIC-Bridge-Konfiguration

October 5, 2021

Um die QUIC-Brücke zu konfigurieren, müssen Sie Folgendes ausfüllen:

- QUIC-Bridge-Profil hinzufügen
- QUIC-Backend-Server hinzufügen
- QUIC-Dienst auf der Appliance hinzufügen
- Fügen Sie einen virtuellen Lastenausgleichsserver vom Typ QUIC Bridge hinzu
- Binden Sie QUIC-Brücke an einen virtuellen Lastenausgleichsserver vom Typ QUIC Bridge

> **Wichtig**
>
> Bevor Sie die QUIC-Brücke konfigurieren, stellen Sie sicher, dass Sie zuerst die Lastenausgleichs-

> funktion auf der Appliance aktivieren. Weitere Informationen finden Sie unter Einrichten des grundlegenden Lastenausgleichs.

Konfigurieren Sie die QUIC-Brücke mit der CLI

Die folgenden Abschnitte müssen über die Befehlszeilenschnittstelle konfiguriert werden.

Fügen Sie ein QUIC-Bridge-Profil hinzu

Sie müssen ein QUIC-Bridge-Profil hinzufügen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add quicBridge profile <name> -routingAlgorithm <PLAINTEXT> -
    serveridlen <value>
```

Beispiel:

```
add quicBridge profile q1 -routingAlgorithm PLAINTEXT -serveridlen 6
```

> **Hinweis:**
>
> Der im Beispiel konfigurierte `serveridlen` Parameter ist die Länge einer benutzerdefinierten Server-ID, die die Hexadezimalzeichenfolge von IP und PORT ist.

QUIC-Back-End-Anwendungsserver hinzufügen

Sie müssen QUIC-Back-End-Anwendungsserver hinzufügen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
-  add server <name> (<IPAddress>)
-  add server <name> (<IPAddress>)
```

Beispiel:

```
-  add server s1 192.0.2.20
-  add server s2 192.0.2.30
```


QUIC Bridge-Dienst hinzufügen

Sie müssen den Anwendungsservern den QUIC-Bridge-Dienst hinzufügen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 - add service  <name>  (<IP> | <serverName>) <serviceType> <port> [-
    CustomServerID <string>]
2
3 - add service  <name>  (<IP> | <serverName>) <serviceType> <port> [-
    CustomServerID <string>]
```

Beispiel:

```
1 - add service src1 s1 QUIC_BRIDGE 443 -CUSTOMSERVERID C0A8026401BB
2
3 - add service src2 s2 QUIC_BRIDGE 443 -CUSTOMSERVERID C0A802C801BB
```

> **Hinweis:**
>
> Die im vorhergehenden Beispiel konfigurierten `CustomServerID` Parameter sind die Hexadezimalzeichenfolge einer entsprechenden IP und der PORT des Servers (s1 und s2). Für das QUIC-Bridge-Feature empfiehlt Citrix, den `CustomServerID` Parameter nur im Hex-String-Format zu konfigurieren.

Fügen Sie einen virtuellen Load Balancing-Server vom Typ QUIC Bridge hinzu

Sie müssen einen virtuellen Lastenausgleichsserver vom Typ QUIC Bridge hinzufügen.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb vserver <name> [<IPAddress>@ <port> [-persistenceType <
    persistenceType >] [-lbMethod < lbMethod > [-cltTimeout <secs>] [-
    quickBridgeProfilename <name>]
```

Beispiel:

```
1 add lb vserver quic_bridge_vip QUIC_BRIDGE 192.0.2.10 443 -
    persistenceType CUSTOMSERVERID -lbMethod TOKEN -cltTimeout 120 -
    quicBridgeProfilename q1
```


> **Hinweis:**
>
> Während der Konfiguration des virtuellen QUIC-Bridge-Servers müssen Sie den `persistenceType` Parameter als `CUSTOMSERVERID` und den Parameter "LbMethod" als konfigurieren `TOKEN`.

Binden Sie den QUIC Bridge-Dienst an den virtuellen Load Balancing-Server vom Typ QUIC Bridge

Sie müssen den QUIC-Bridge-Dienst an den virtuellen Load Balancing-Server vom Typ QUIC Bridge binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 -  bind lb vserver <name> (<serviceName>)
2
3 -  bind lb vserver <name> (<serviceName>)
```

Beispiel:

```
1 -  bind lb vserver quic_bridge_vip src1
2
3 -  bind lb vserver quic_bridge_vip src2
```

Konfigurieren der QUIC-Brücke für Dienstgruppen

Sie können QUIC-Bridge-Funktionen auch für Dienstgruppen konfigurieren. In den folgenden Schritten können Sie die QUIC-Brücke für Dienstgruppen konfigurieren.

Um QUIC Bridge für Dienstgruppen zu konfigurieren, müssen Sie Folgendes ausführen:

QUIC-Bridge-Profil hinzufügen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add quicBridge profile <name> -routingAlgorithm <PLAINTEXT> -
     serveridlen <value>
```

Beispiel:


```
add quicBridge profile q1 -routingAlgorithm PLAINTEXT -serveridlen 6
```

Server vom Typ QUIC hinzufügen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
- add server <name> (<IPAddress>)
- add server <name> (<IPAddress>)
```

Beispiel:

```
- add server s1 192.0.2.20
- add server s2 192.0.2.30
```

QUIC Bridge-Servicegruppe hinzufügen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add serviceGroup <serviceGroupName> (<IP> | <serverName>) <serviceType>
```

Beispiel:

```
add serviceGroup svg1 QUIC_BRIDGE
```

Binden Sie die QUIC-Server an die Servicegruppe

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
- bind serviceGroup <serviceGroupName> (<IP>@ | (<serverName>) [-
    CustomServerID <string>]
- bind serviceGroup <serviceGroupName> (<IP>@ | (<serverName>) [-
    CustomServerID <string>]
```


Beispiel:

```
1 -  bind serviceGroup svg1 s1 443 -customServerID C0A8026401BB
2 -  bind serviceGroup svg1 s2 443 -customServerID C0A802C801BB
```

Fügen Sie einen virtuellen Lastenausgleichsserver vom Typ QUIC Bridge hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add lb vserver <name> [<IPAddress>@ <port> [-persistenceType <
     persistenceType >] [-lbMethod < lbMethod > [-cltTimeout <secs>] [-
     quickBridgeProfilename <name>]
```

Beispiel:

```
1 add lb vserver quic_bridge_vip QUIC_BRIDGE 192.0.2.10 443 -
     persistenceType CUSTOMSERVERID -lbMethod TOKEN -cltTimeout 120 -
     quicBridgeProfilename q1
```

Binden Sie den virtuellen Load Balancing-Server vom Typ QUIC Bridge an die Dienstgruppe

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 bind lb vserver <name>@ (<serviceName>@ <serviceGroupName>
```

Beispiel:

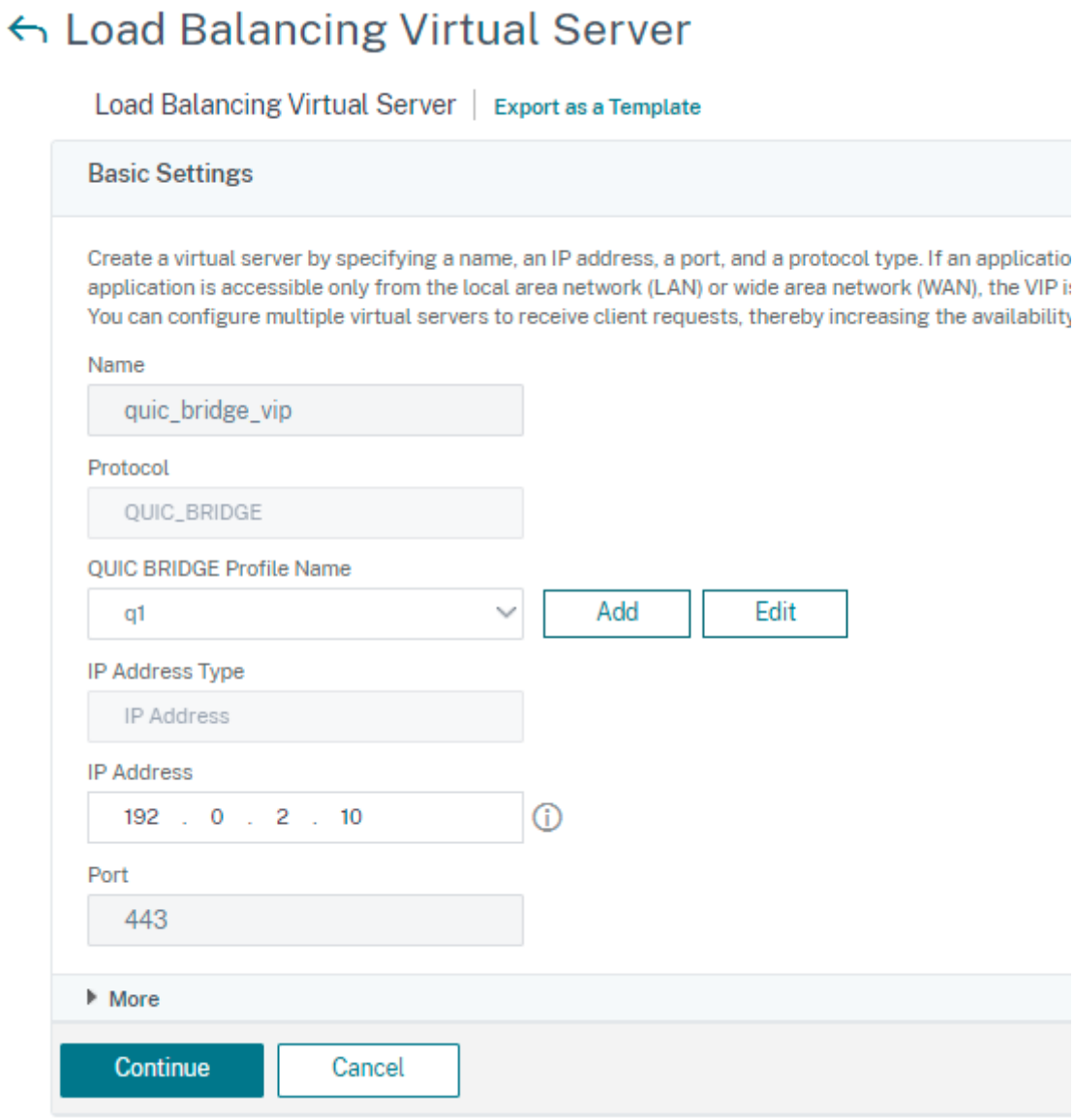
```
1 bind lb vserver quic_bridge_vip svg1
```

Konfigurieren Sie die QUIC-Brücke mit der GUI

Führen Sie die folgenden Schritte aus, um die QUIC-Brücke über die grafische Benutzeroberfläche zu konfigurieren.

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

2. Klicken Sie auf der Seite **Virtuelle Server** auf **Hinzufügen**.
3. Wählen Sie auf der Seite **Load Balancing Virtual Server** das Protokoll als QUIC_BRIDGE aus und geben Sie die Details ein. Klicken Sie auf **OK**.



4. Klicken Sie auf der Seite **Load Balancing Virtual Server** auf **Weiter** und **Fertig**.

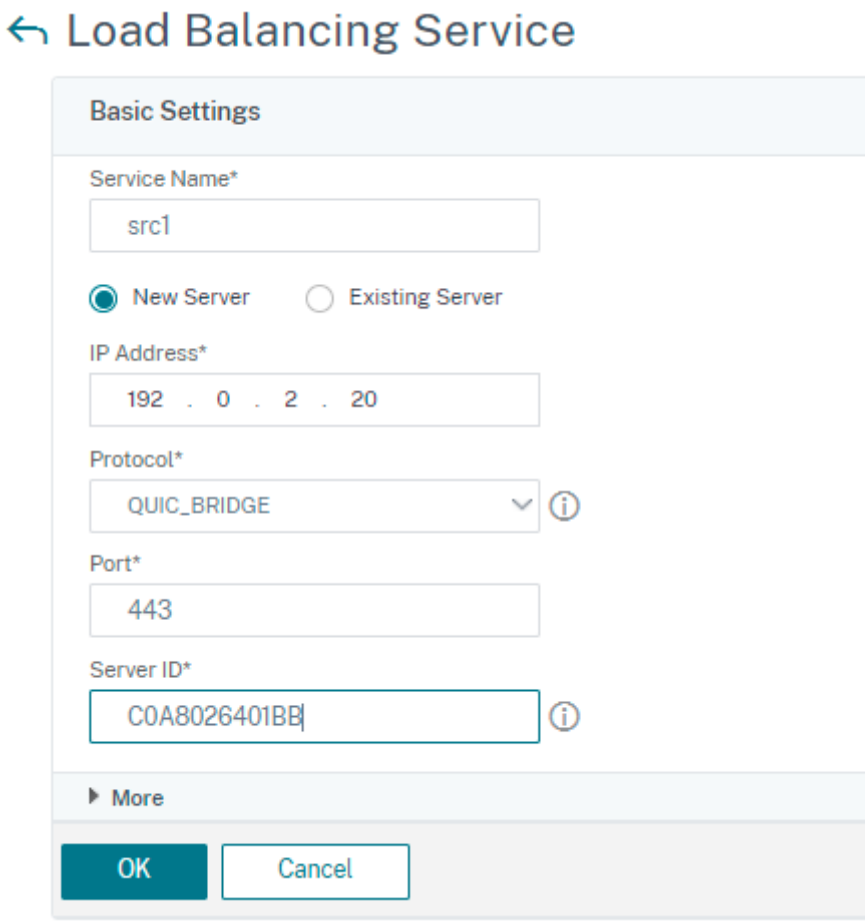
Konfigurieren Sie den Lastenausgleich für die Dienste über die grafische Benutzeroberfläche

Führen Sie die folgenden Schritte aus, um den Lastenausgleich für die Dienste über die grafische Benutzeroberfläche zu konfigurieren.

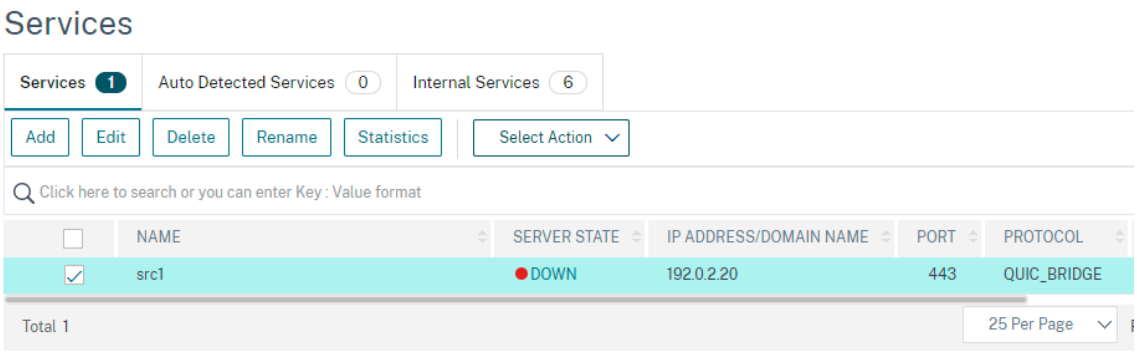
1. Navigieren Sie zu **Traffic Management > Load Balancing > Services**. Klicken Sie auf der Seite

Dienste auf **Hinzufügen**.

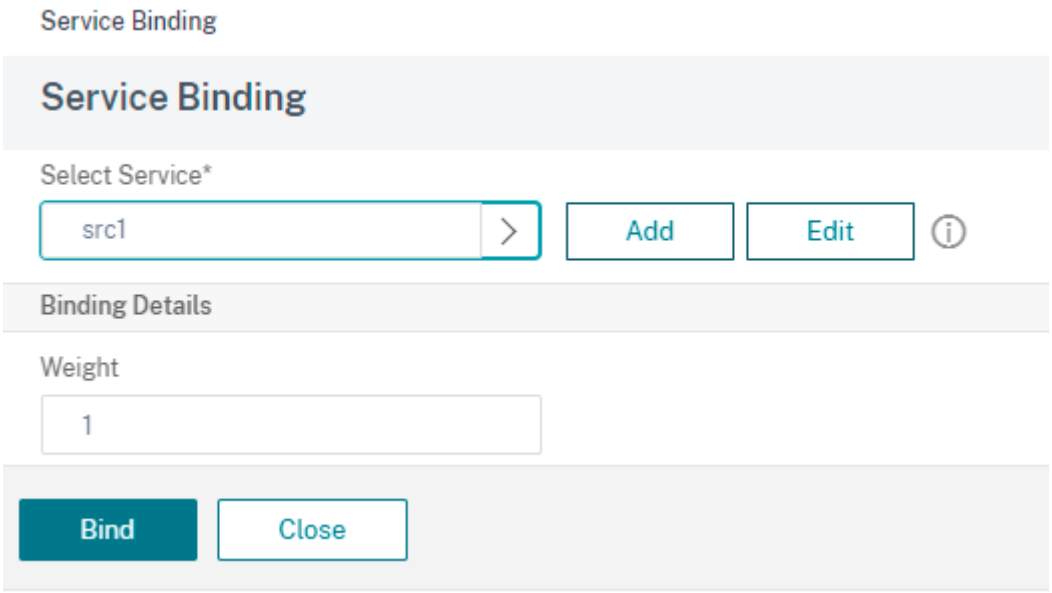
2. Geben Sie auf der Seite **Load Balancing Service** die Details ein und klicken Sie auf **OK**.



3. Wählen Sie auf der Seite **Virtuelle Server** den erstellten virtuellen Server aus, um den Dienst zu binden.
4. Scrollen Sie auf der Seite **Load Balancing Virtual Server** nach unten und wählen Sie die **Dienste und Dienstgruppen**aus.
5. Klicken Sie im Bildschirm **Dienstbindung** auf Feld **Service auswählen** .
6. Wählen Sie im Bildschirm **Dienst den Dienst** aus, der an den virtuellen Lastenausgleichsserver gebunden werden soll, und klicken Sie auf **Auswählen**.



7. Der src1-Dienst ist ausgewählt und klicken Sie im Bildschirm **Dienstbindung** auf **Binden**.



8. Klicken Sie auf der Seite **Load Balancing Virtual Server** auf **Fertig**.

Proxy-Protokoll

June 1, 2022

Das Proxy-Protokoll transportiert Clientdetails sicher von Client zu Server über Citrix ADC-Appliances. Die Appliance fügt einen Proxy-Protokoll-Header mit Clientdetails hinzu und leitet ihn an den Back-End-Server weiter. Im Folgenden sind einige Anwendungsszenarien für das Proxy-Protokoll in einer Citrix ADC-Appliance aufgeführt.

- Erlernen der ursprünglichen Client-IP-Adresse
- Auswählen einer Sprache für eine Website
- Blockieren der Auflistung ausgewählter
- Protokollieren und Sammeln von Statistiken.

Im Folgenden sind die drei Betriebsmodi aufgeführt:

- Einfügen. Die Appliance fügt die Clientdetails ein und sendet sie an den Back-End-Server.
- Vorwärts. Die Appliance leitet die Clientdetails an den Backend-Server weiter.
- Abgestreift. Die Appliance speichert die Clientdetails zu Protokollierungszwecken. Wenn das Proxy-Protokoll auf dem Back-End-Server nicht unterstützt wird, sendet die Clientdetails mithilfe der Konfiguration der Rewriterichtlinie an den Server

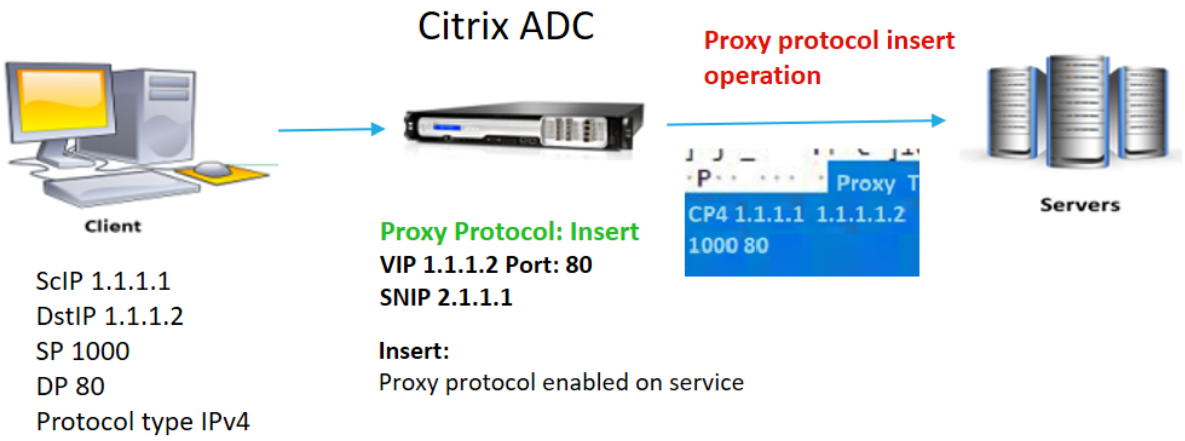
Einschränkungen

Das Proxy-Protokoll wird für die TCP Fast Open (TFO) und MultiPath TCP-Funktionen nicht unterstützt. Die Funktion wird nur für Dienste unterstützt, für die die Citrix ADC Appliance die TCP-Verbindungsbeendigung vornimmt. Es ist keine Unterstützung für andere Dienste, zum Beispiel “ANY”.

So funktioniert das Proxy-Protokoll in einer Citrix ADC-Appliance

Die folgenden Flussdiagramme zeigen, wie Sie das Proxy-Protokoll für Citrix ADC-Appliances für den Insert-, Forwards- und Stripping-Betrieb konfigurieren können:

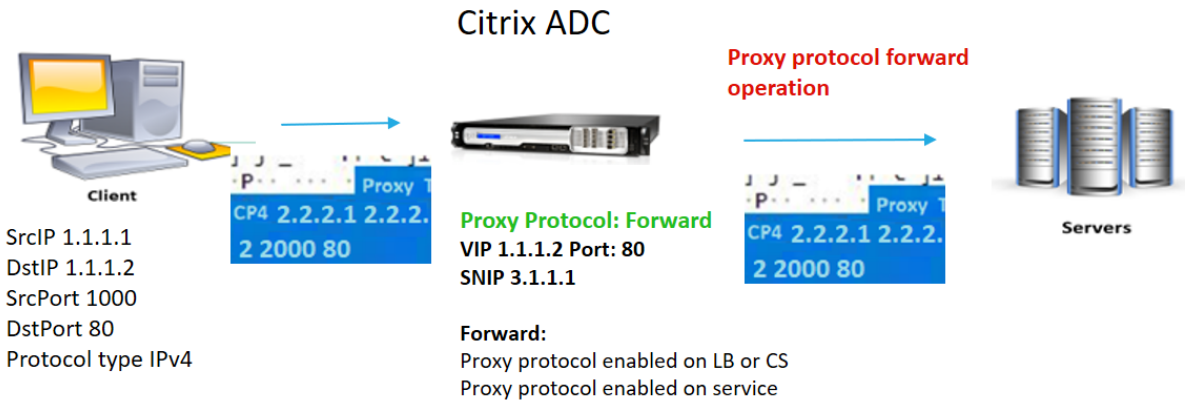
Insert-Betrieb



Die Interaktion der Komponente ist wie folgt:

- Bei der Citrix ADC-Instanz müssen Sie das Proxy-Protokoll im Netzprofil aktivieren und an den Dienst binden.
- Beim Einfügevorgang fügt Citrix ADC einen Proxy-Header mit Clientverbindungsdetails hinzu und leitet ihn an den Backend-Server weiter.
- Auf der sendenden Seite entscheidet die Appliance die Proxy-Protokollversion basierend auf der CLI-Konfiguration.

Vorwärtsbetrieb

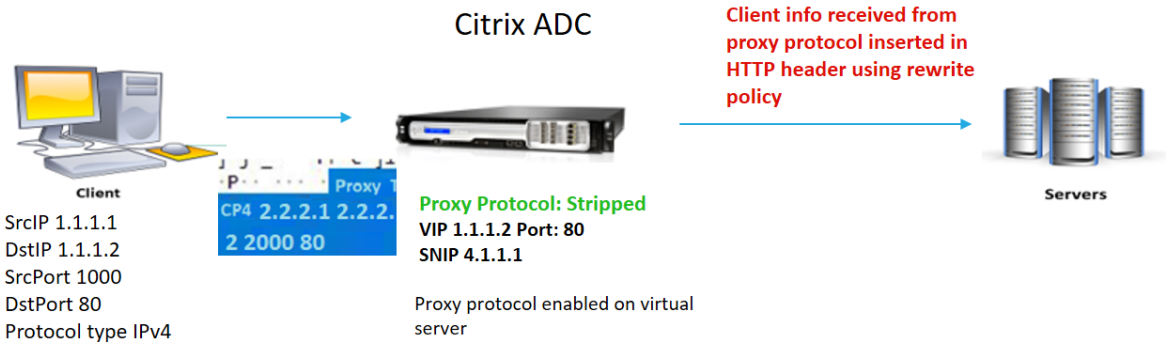


*** The original client details 2.2.2.1, 2.2.2.2, 2000, 80 in the proxy header is forwarded to the back-end server**

Die Interaktion der Komponente ist wie folgt:

- Ein Client sendet eine Anfrage zusammen mit dem Proxy-Header an den Citrix ADC. Die Appliance identifiziert die Version dynamisch.
- In der Citrix ADC-Appliance handelt es sich um einen Forward-Vorgang. Das Proxy-Protokoll ist auf dem virtuellen Lastausgleichsserver oder dem virtuellen Content Switching-Server aktiviert und für den Dienst aktiviert. Die Appliance empfängt den Proxy-Header und leitet die Header-Details an den Backend-Server weiter.
- Wenn die Details des Proxy-Headers ungültig sind, setzt die Appliance die Verbindung zurück.
- Auf der sendenden Seite entscheidet die Appliance die Proxy-Protokollversion basierend auf der CLI-Konfiguration.

Stripped-Vorgang



Die Interaktion der Komponente ist wie folgt:

- Ein Client sendet eine Anfrage zusammen mit einem Proxy-Header an die Citrix ADC-Appliance.
- Wenn es sich in der Citrix ADC-Appliance um einen Stripping-Vorgang handelt, leitet die Appliance die vom Proxy-Protokoll erhaltenen Clientinformationen weiter und fügt sie mithilfe von Rewriterichtlinienausdrücken in den HTTP-Header ein.
- Die Clientdetails wie Quell-IP-Adresse, Ziel-IP-Adresse, Quellport und Zielport werden mithilfe von Rewriterichtlinienausdrücken in einem HTTP-Header hinzugefügt. Die Rewriterichtlinie wertet den Ausdruck aus und wenn "wahr", wird die entsprechende Aktion der Rewriterichtlinie ausgelöst. Und die Clientdetails werden in einem HTTP-Header an den Back-End-Server weitergeleitet.
- Wenn die Details des Proxy-Headers ungültig sind, setzt die Appliance die Verbindung zurück.

Proxy-Protokoll-Versionsformate

Die Proxy-Protokollversion ist in zwei Formaten verfügbar. Die Appliance entscheidet, ein Format basierend auf der Länge der eingehenden Daten zu verwenden. Ausführliche Informationen finden Sie unter Proxy-Protokoll-RFP .

1. Proxyprotokoll-Version-1-Format

   ```
   PROXY TCP4/TCP6/UNKNOWN <SRC IP> <DST IP> <SRC PORT> <DST PORT>
   ```

   - PROXY -> Eindeutiges Zeichenfolgenformat für Proxy-Header-Version -1.
   - Unterstützt Protokolle TCP über IPv4 und TCP über IPv6. Für die verbleibenden Protokolle ist dies UNBEKANNT.
   - SRC-IP — Quell-IP (Ursprüngliche Client-IP) -Adresse eines Pakets.
   - DST IP — Ziel-IP-Adresse eines Pakets.
   - SRC-Port — Quellport eines Pakets.
   - DST-Port — Zielport eines Pakets.

2. Proxyprotokoll-Version-2-Format

   ```
   0D 0A 0D 0A 00 0D 0A 51 55 49 54 0A <13th byte> <14th byte> <15-16th
   byte> <17th byte onwards>
   ```

   - D 0A 0D 0A 00 0D 0A 51 55 49 54 0A -> Eindeutige binäre Zeichenfolge für Proxy-Header-Version -2.
   - Unterstützt Protokolle TCP über IPv4 und TCP über IPv6. Für die verbleibenden Protokolle ist dies UNBEKANNT.
   - Dreizehntes Byte — Protokollversion und Befehl.
   - Vierzehntes Byte — Adresse und Protokollfamilie.
   - 15-16. Byte — Adresslänge in Netzwerkreihenfolge.
   - Siebzehntes Byte ab — Adressiert Informationen, die in der Netzwerkreihenfolge vorhanden sind - src IP, dst IP, src-Port, dst-Port.

Konfigurieren Sie das Proxy-Protokoll in Citrix ADC-Appliance

Führen Sie die folgenden Schritte aus, um das Proxy-Protokoll in Ihrer Citrix ADC Appliance zu konfigurieren.

1. Aktivieren Sie das Proxy-Protokoll als global.
2. Konfigurieren Sie das Proxy-Protokoll für Insert-
3. Konfigurieren Sie das Proxy-Protokoll für Forward-
4. Konfigurieren Sie das Proxy-Protokoll für Strip-Betrieb
5. Konfigurieren Sie das Proxy-Protokoll für keinen Betrieb

Aktivieren Sie das Proxy-Protokoll als global

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ns param -proxyProtocol ENABLED
```

Konfigurieren Sie das Proxy-Protokoll für Insert-

Um das Proxy-Protokoll für den Insert-Vorgang zu konfigurieren, müssen Sie das Protokoll auf dem virtuellen Lastausgleichsserver aktivieren oder deaktivieren und für den Dienst aktivieren.

Hinzufügen eines Netzprofils mit deaktiviertem Proxy-Protokoll für den Lastausgleich des virtuellen Servers

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Beispiel:

```
Add netprofile proxyprofile-1 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

> **Hinweis:**
>
> Wenn Sie das Proxy-Protokoll auf Ihrer Appliance deaktivieren, müssen Sie den Protokollversion-sparameter nicht festlegen.

Fügen Sie ein Netzprofil mit einem für den Dienst aktivierten Proxy-Protokoll hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```


Beispiel:

```
add netprofile proxyprofile-2 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

Fügen Sie einen virtuellen Lastausgleichsserver für Citrix ADC-Appliance in der Proxy-Schicht hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name>@ <serviceType> [(<IPAddress>@ <port>)]
```

Beispiel:

```
add lb vserver lbvserver-1 http 1.1.1.1 80
```

Fügen Sie den HTTP-Dienst für Citrix ADC-Appliance in der Proxy-Schicht hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name>@ (<IP>@ | <serverName>@)<serviceType> <port>
```

Beispiel:

```
Add service http-service-1 2.2.2.1 http 80
```

Festlegen des Netzwerkprofils mit dem virtuellen Lastausgleichsserver in der Citrix ADC-Appliance

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <vserver name> -netprofile <name>
```

Beispiel:

```
set lb vserver lbvserver-1 -netprofile proxyProfile-1
```

Festlegen des Netzwerkprofils mit dem HTTP-Dienst in der Citrix ADC-Appliance

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <service name> -netprofile <name>
```

Beispiel:

```
set service http-service-1 -netprofile proxyProfile-1
```


Konfigurieren des Proxy-Protokolls für Forwar

Konfigurieren des Proxy-Protokolls für den Forward-Betrieb für die nächste Citrix ADC-Instanz in der Proxy-Schicht. Sie müssen das Protokoll aktivieren oder deaktivieren und an den virtuellen Server oder Dienst binden.

Hinzufügen eines Netzprofils mit aktiviertem Proxy-Protokoll für den Lastausgleich des virtuellen Servers

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Beispiel:

```
add netprofile proxyprofile-3 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

Netzprofil mit aktiviertem Proxy-Protokoll für den Dienst hinzufügen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add netprofile <name> -proxyProtocol ENABLED/DISABLED> -proxyprotocoltxversion
 <V1/V2>
```

Beispiel:

```
add netprofile proxyprofile-4 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

Fügen Sie einen virtuellen Lastausgleichsserver für Citrix ADC-Appliance in der Proxy-Schicht hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name>@ <serviceType> [(<IPAddress>@ <port>)]
```

Beispiel:

```
add lb vserver lbvserver-2 http 2.2.2.2 80
```

Fügen Sie den HTTP-Dienst für Citrix ADC-Appliance in der Proxy-Schicht hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name>@ (<IP>@ | <serverName>@)<serviceType> <port>
```


Beispiel:

```
Add service http-service-2 3.3.3.1 http 80
```

Festlegen des Netzwerkprofils mit dem virtuellen Lastausgleichsserver in der Citrix ADC-Appliance

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <vserver name> -netprofile <name>
```

Beispiel:

```
set lb vserver lbvserver-2 -netprofile proxyProfile-3
```

Festlegen des Netzwerkprofils mit dem HTTP-Dienst in der Citrix ADC-Appliance

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <service name> -netprofile <name>
```

Beispiel:

```
set service http-service-2 -netprofile proxyProfile-4
```

Konfigurieren Sie das Proxy-Protokoll für Strip-Betrieb

Um das Proxy-Protokoll für den Strip-Betrieb zu konfigurieren, müssen Sie das Proxy-Protokoll auf dem virtuellen Lastausgleichsserver aktivieren und das Proxy-Protokoll für den Dienst deaktivieren.

Netzprofil mit aktiviertem Proxy-Protokoll für virtuellen Server hinzufügen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add netprofile <name> -proxyProtocol ENABLED> -proxyprotocoltxversion <V1/
V2>
```

Beispiel:

```
add netprofile proxyprofile-5 -proxyProtocol ENABLED -proxyprotocoltxversion
 V1
```

Fügen Sie einen virtuellen Server für Lastenausgleich oder Content Switching für Citrix ADC-Appliance in der Proxy-Schicht hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add lb vserver <name>@ <serviceType> [(<IPAddress>@ <port>)]
```


Beispiel:

```
add lb vserver lbvserver-3 http 2.2.2.2 80
```

Fügen Sie den HTTP-Dienst für Citrix ADC-Appliance in der Proxy-Schicht hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name>@ (<IP>@ | <serverName>@)<serviceType> <port>
```

Beispiel:

```
Add service http-service-3 3.3.3.1 http 80
```

Festlegen des Netzprofils mit Lastausgleich oder virtuellem Content Switching-Server in Citrix ADC-Appliance

Geben Sie an der Eingabeaufforderung Folgendes ein:

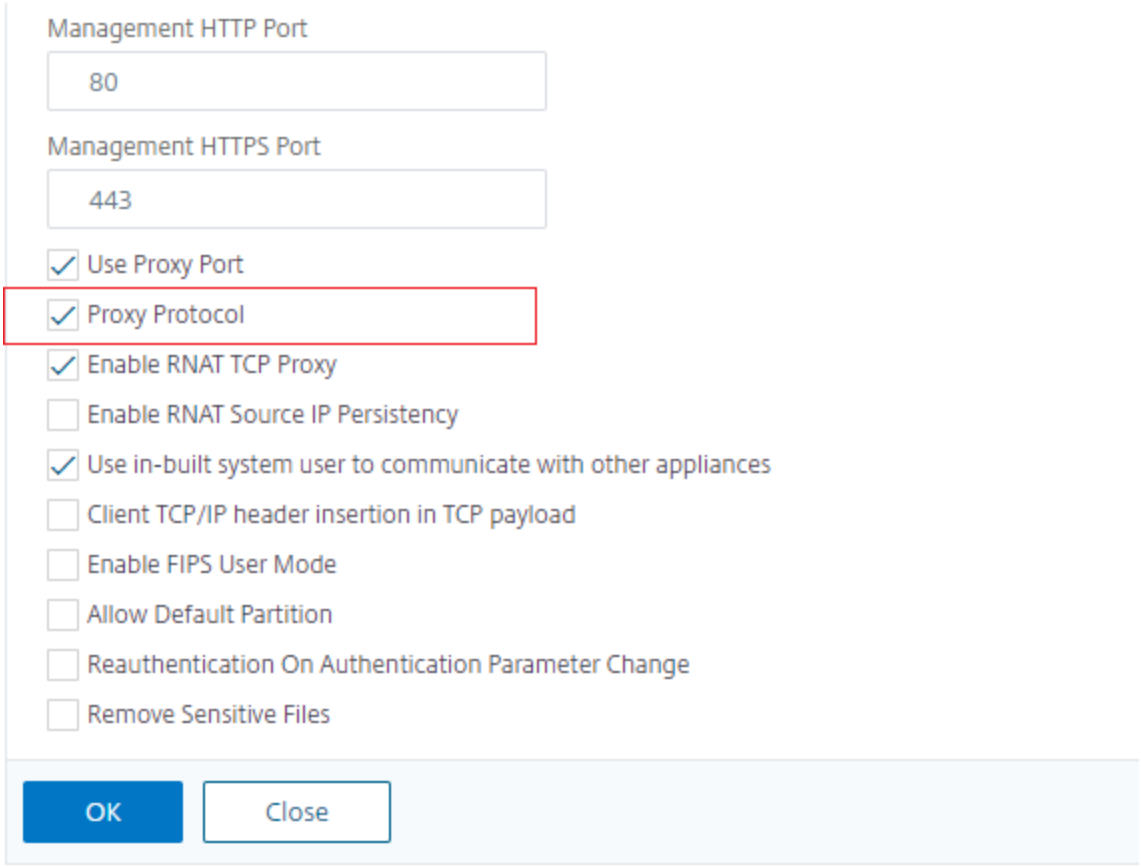
```
set lb vserver <vserver name> -netprofile <name>
```

Beispiel:

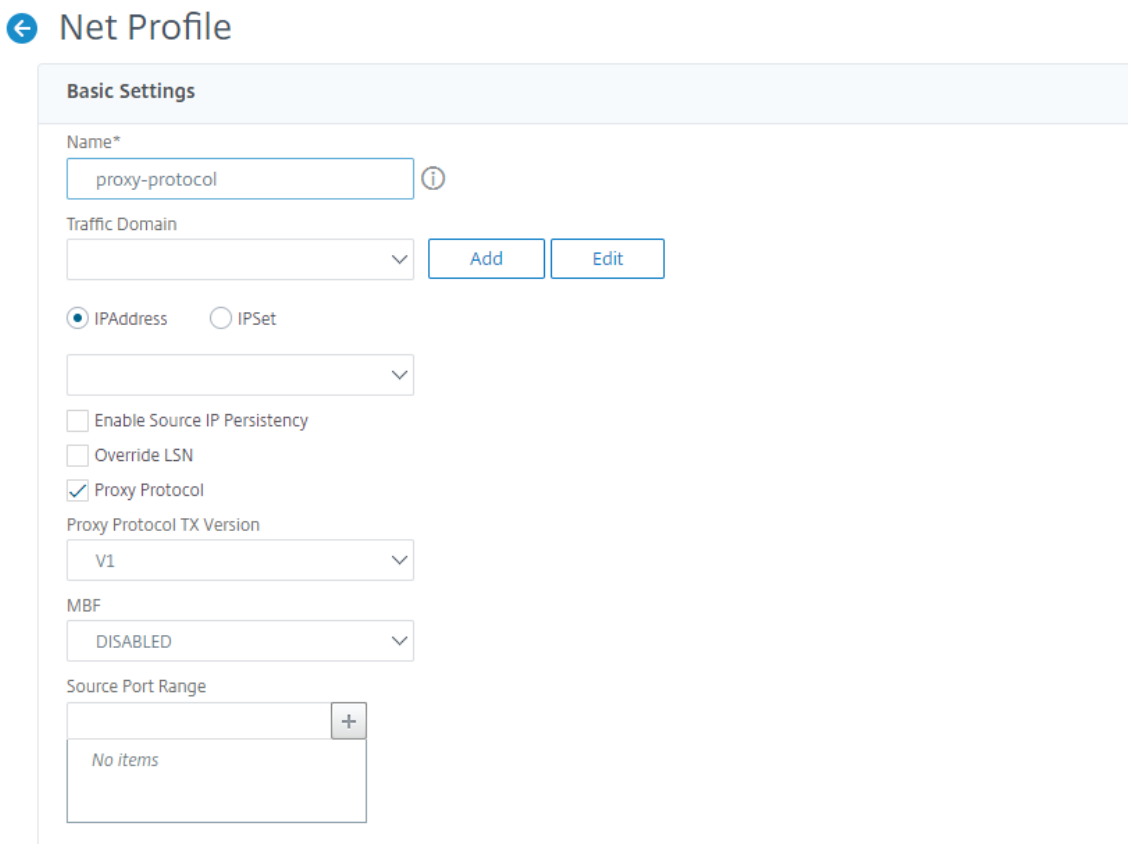
```
set lb vserver lbvserver-3 -netprofile proxyProfile-5
```

Konfigurieren des Proxy-Protokolls über die Citrix ADC GUI

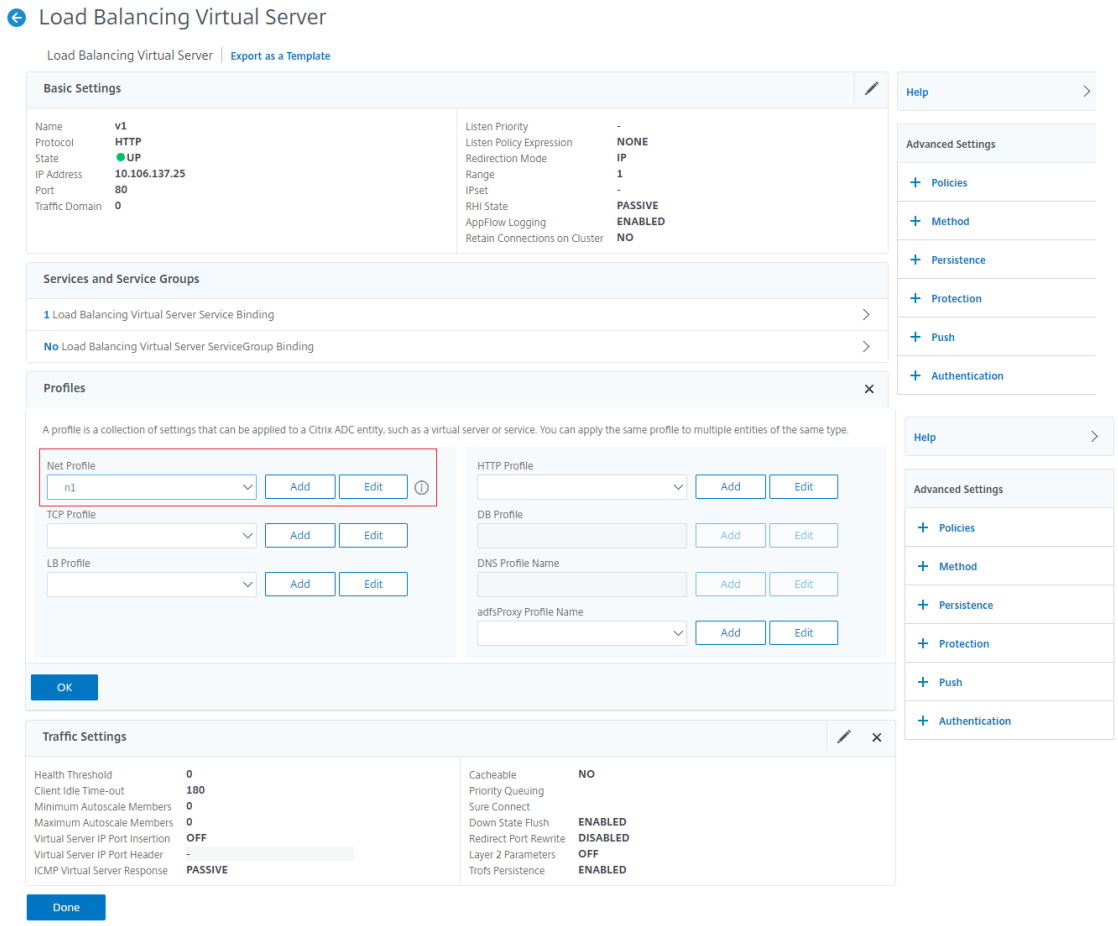
1. Navigieren Sie zu **System** > **Einstellungen** > **Globale Systemeinstellungen ändern**.
2. **Aktivieren Sie auf der Seite "Parameter für globale Systemeinstellungen konfigurieren** " das Kontrollkästchen **Proxy-Protokoll** .
3. Klicken Sie auf **OK** und **Schließen**.



4. Navigieren Sie zu **System** > **Netzwerk** > **Netzprofile**.
5. Klicken Sie im Detailbereich auf **Hinzufügen**, um ein Netzprofil für den virtuellen Lastausgleichsserver zu erstellen.
6. Legen Sie auf der Seite **Net Profile** die folgenden Parameter fest:
   a) Name. Name des Netzprofils.
   b) Proxy-Protokoll. Aktivieren oder deaktivieren Sie das Proxy-Protokoll für den virtuellen Lastausgleichsserver.
   c) Proxy-Protokoll TX-Version. Legen Sie die Proxy-Protokollversion basierend auf dem eingehenden Datenformat als V1 oder V2 fest.
7. Klicken Sie auf **OK**.

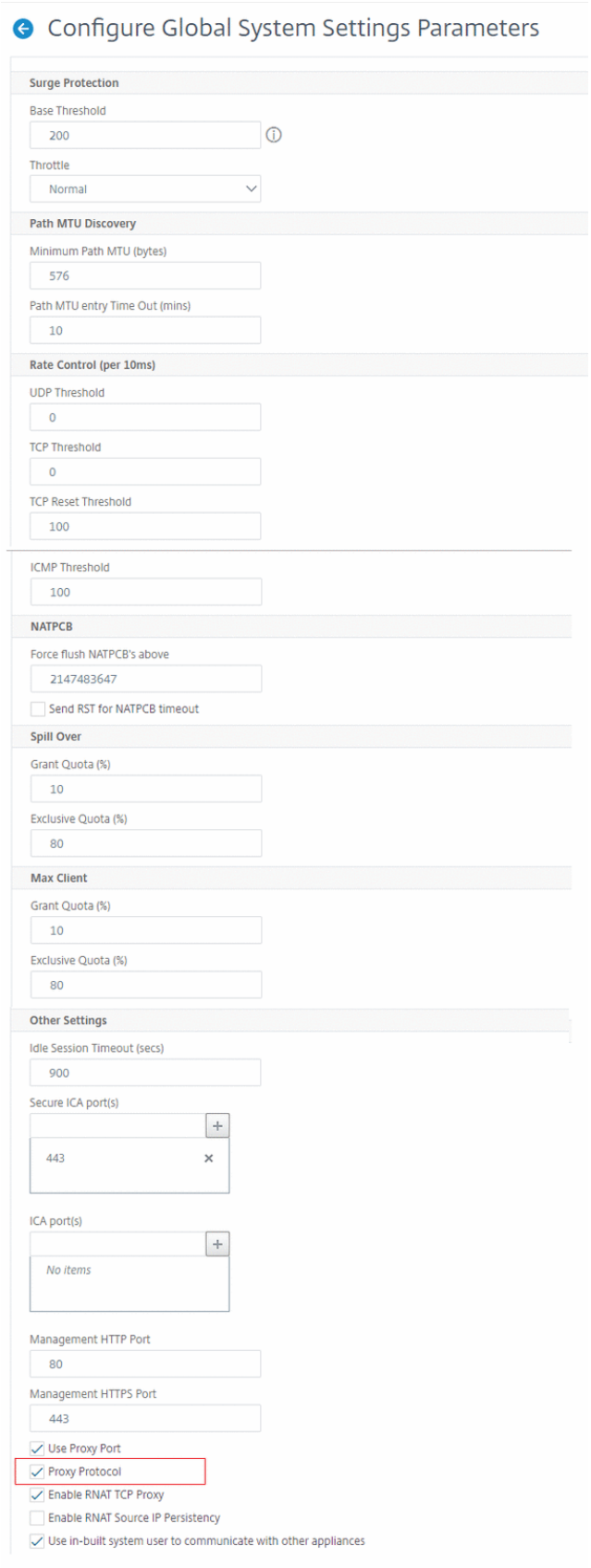


8. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**.
9. Klicken Sie im Detailbereich auf **Hinzufügen**.
10. Legen Sie auf der Seite **Load Balancing Virtual Server** die grundlegenden Parameter fest.
11. Wählen Sie im Abschnitt **Erweiterte Einstellungen** die Option **Profile**aus.
12. Klicken Sie im Abschnitt **Profile** auf das Stiftsymbol.
13. Wählen Sie ein Netzprofil aus und klicken Sie auf **OK**.
14. Klicken Sie auf **Fertig**.



15. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Services**.
16. Klicken Sie im Detailbereich auf **Hinzufügen**.
17. Legen Sie auf der Seite **Load Balancing Service** die grundlegenden Parameter fest.
18. Wählen Sie im Abschnitt **Erweiterte Einstellungen** die Option **Profile**aus.
19. Klicken Sie im Abschnitt **Profile** auf das Stiftsymbol.
20. Wählen Sie ein Netzprofil aus und klicken Sie auf **OK**.
21. Klicken Sie auf **Fertig**.

> **Hinweis:**
>
> Wenn Sie mehr als eine Citrix ADC-Appliance als Teil der Proxy-Schicht haben, müssen Sie die Proxy-Protokollkonfiguration auf jeder Appliance für den Forward-Vorgang festlegen.



Client-IP-Adresse in TCP-Option

October 5, 2021

Die Citrix ADC Appliance verwendet viele Möglichkeiten, um die Clientinformationen an den Back-End-Server zu senden. Eine solche Methode ist das Senden der Client-IP-Adresse in der TCP-Option des ersten Datenpakets. Die Appliance verwendet die TCP-Optionsnummer im TCP-Profil, wenn der Back-End-Server die TCP-Option verwendet, um die Client-IP-Adresse zu lesen. Die IP-Adresse wird in der TCP-Optionsnummer 28 (konfigurierbar auf dem Appliance-Dienst) übertragen.
Die TCP-Optionsmethode umfasst sowohl Einfüge- als auch Weiterleitungsfunktionen beim Tragen der Client-IP-Adresse zum Back-End-Server.
In der TCP-Optionskonfiguration fügt die Appliance eine TCP-Option hinzu, 28, um die Client-IP-Adresse einzufügen und an den Back-End-Server weiterzuleiten. Im Folgenden sind einige der Verwendungsszenarien für die TCP-Optionskonfiguration in einer Citrix ADC Appliance aufgeführt.
Multiplexing ist deaktiviert, wenn diese Funktion für den Datenverkehr aktiviert ist, der zum TCP-Profil kommt. Wenn nsapimgr und clientip tcp-options im TCP-Profil aktiviert sind, hat clientip tcp-option Vorrang.

> **Hinweis:**
>
> Multiplexing ist jedoch auf der Appliance deaktiviert, wenn Client-IP-TCP-Option für den Datenverkehr aktiviert ist, der zum TCP-Profil kommt.

- Erlernen der ursprünglichen Client-IP-Adresse
- Auswählen einer Sprache für eine Website
- Liste ausgewählter IP-Adressen blockieren

Im Folgenden sind die beiden Betriebsarten:

- Einfügen. Die Appliance fügt die Clientdetails im Feld TCP-Option 28 (konfigurierbar, aber bevorzugter Wert 28) hinzu und sendet sie an den Backend-Server.
- Vorwärts. Die Appliance leitet die Clientdetails in der TCP-Option 28 weiter (konfigurierbar am Front-End des Appliance-Dienstes). Die Optionsnummer am Back-End kann jedoch basierend auf dem im Back-End konfigurierten Wert geändert werden.

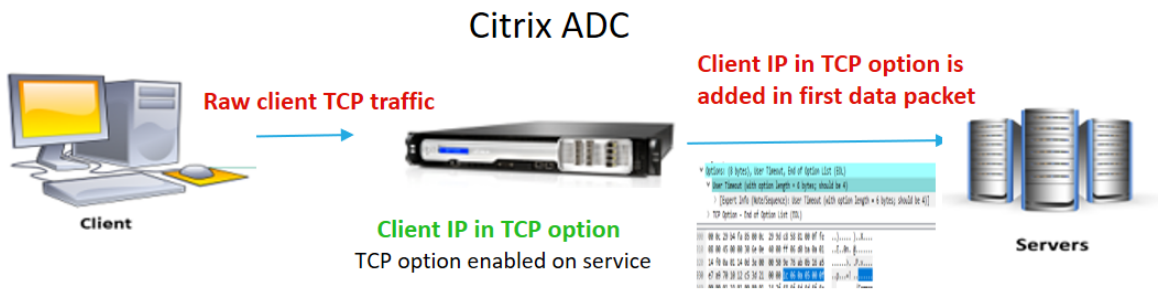
> **Hinweis:**
>
> Bei einem virtuellen TCP oder HTTP-Server wird die TCP-Optionsnummer mit oder ohne diese Funktion im transparenten Modus weitergeleitet.

Einschränkungen

Die TCP-Option Konfigurationsfunktion wird in TFO, MultiPath TCP und HTTP2 Features nicht unterstützt.

Konfiguration der TCP-Optionen in einer Citrix ADC Appliance

Die folgenden Flussdiagramme zeigen, wie Sie die TCP-Option in den Citrix ADC Appliances für Einfüge- und Weiterleitungsvorgänge konfigurieren können.

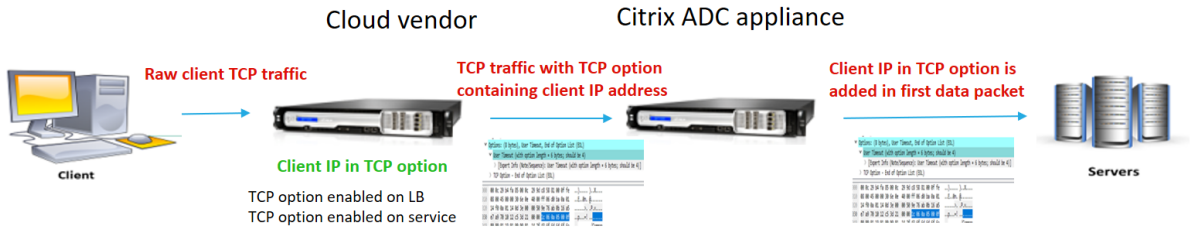


Die Komponente interagieren wie folgt:

- Ein Client sendet eine Anforderung an Citrix ADC.
- In der Citrix ADC Appliance müssen Sie ein TCP-Profil erstellen, die TCP-Optionsfunktion aktivieren und die TCP-Optionsnummer angeben.

  Hinweis: Es ist ratsam, TCP-Optionsnummer als 28 im TCP-Profil zu konfigurieren.
- Im Einfügevorgang fügt Citrix ADC die Clientdetails in die an den Dienst gebundene TCP-Option 28 ein. Die Client-Details werden dann an den Back-End-Server gesendet. Wenn der eingehende Datenverkehr HTTPS ist, wird die Client-IP-Adresse in der TCP-Option in der SSL-Client-Hallo Nachricht gesendet, die das erste Datenpaket auf TCP-Ebene ist

Vorwärtsbetrieb:



Die Komponente interagieren wie folgt:

- Ein Client sendet eine HTTP/HTTPS-Anforderung an Citrix ADC.
- Wenn es sich bei Citrix ADC Appliance um einen Weiterleitungsvorgang handelt, ist die TCP-Option für den Lastenausgleich des virtuellen Servers oder für den virtuellen Content Switching-Server aktiviert und auch für den Dienst aktiviert. Die Appliance empfängt die Clientinformationen in der im virtuellen Server angegebenen TCP-Optionsnummer und leitet sie an den Back-End-Server in der TCP-Optionsnummer (konfigurierbar im Dienst) weiter, die im ersten Datenpaket hinzugefügt wurde.

TCP-Option für den Einfügevorgang konfigurieren

Befolgen Sie die unten angeführte Vorgehensweise zum Konfigurieren der TCP-Option in Ihrer Citrix ADC Appliance.

1. Fügen Sie ein TCP-Profil hinzu.
2. TCP-Option für den Einfügevorgang konfigurieren
3. TCP-Profil an den Dienst binden

Hinzufügen eines TCP-Profils

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add tcpprofile <name> -clientIpTcpOption (enabled | disabled> -clientIpTcpOptionNumber
 <positive_integer>
```

Beispiel:

```
add tcprofile p1
```

TCP-Option für den Einfügevorgang konfigurieren

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add tcpprofile <name> -clientIpTcpOption (enabled | disabled> -clientIpTcpOptionNumber
 <positive_integer>
```

Beispiel:

```
add tcpprofile p1 -clientIpTcpOption ENABLED -clientIpTcpOptionNumber 28
```

Service hinzufügen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add service <name> <server name> <service type> <port>
```

Beispiel:

```
add service service-http1 1.1.1.1 HTTP 80
```

TCP-Profil an den Dienst binden

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set service <name> -tcpprofileName <name>
```

Beispiel:

```
set service s1 -tcpprofileName p1
```


> **Hinweis:**
>
> Die Grundkonfiguration für den Service muss beachtet werden.

TCP-Option für Weiterleitungsvorgang konfigurieren

Nach dem unten angegebenen Verfahren TCP-Option im TCP-Profil für den Weiterleitungsvorgang konfigurieren.

1. TCP-Profil mit TCP-Optionsnummer hinzufügen
2. TCP-Profil an den virtuellen Server binden
3. TCP-Profil an den Dienst binden.

TCP-Profil mit TCP-Optionsnummer hinzufügen

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add tcpprofile <name> -clientIpTcpOption (enabled | disabled> -clientIpTcpOptionNumber
 <positive_integer>
```

Beispiel:

```
add tcpprofile p1 -clientIpTcpOption ENABLED -clientIpTcpOptionNumber 29
```

TCP-Profil an virtuellen Server binden (Lastenausgleich oder Content Switching)

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set lb vserver <name> -tcpprofileName <name>
```

Beispiel:

```
set lb vservice s1 -tcpprofileName p1
```

TCP-Profil an den Dienst binden

Geben Sie an der Eingabeaufforderung Folgendes ein:

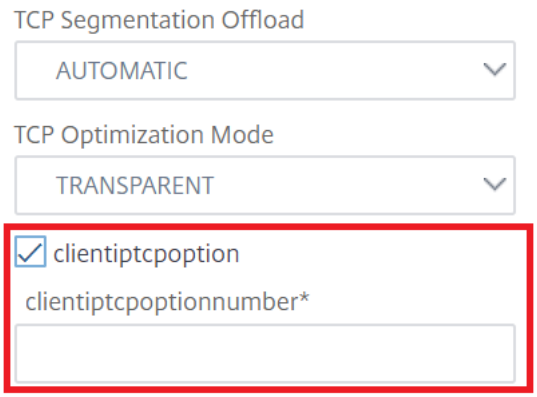
```
set service <name> -tcpprofileName p1
```

Beispiel:

```
set service s1 -tcpprofileName p1
```


Konfigurieren der TCP-Option mit der Citrix ADC GUI

1. Navigieren Sie zu **System** > **Profile**.
2. Klicken Sie auf der Registerkarte **TCP-Profil** auf **Hinzufügen**.
3. **Konfigurieren Sie auf der Seite TCP-Profil** konfigurieren die folgenden Parameter:
   a. clientIptcpoption. TCP-Option zum Senden oder Empfangen von Client-IP-Adresse.
   b. clientiptcpoptionnumber. Konfigurierbare TCP-Optionsnummer, um die Client-IP-Adresse zu empfangen.



4. Klicken Sie auf **OK** und **schließen**.

SNMP

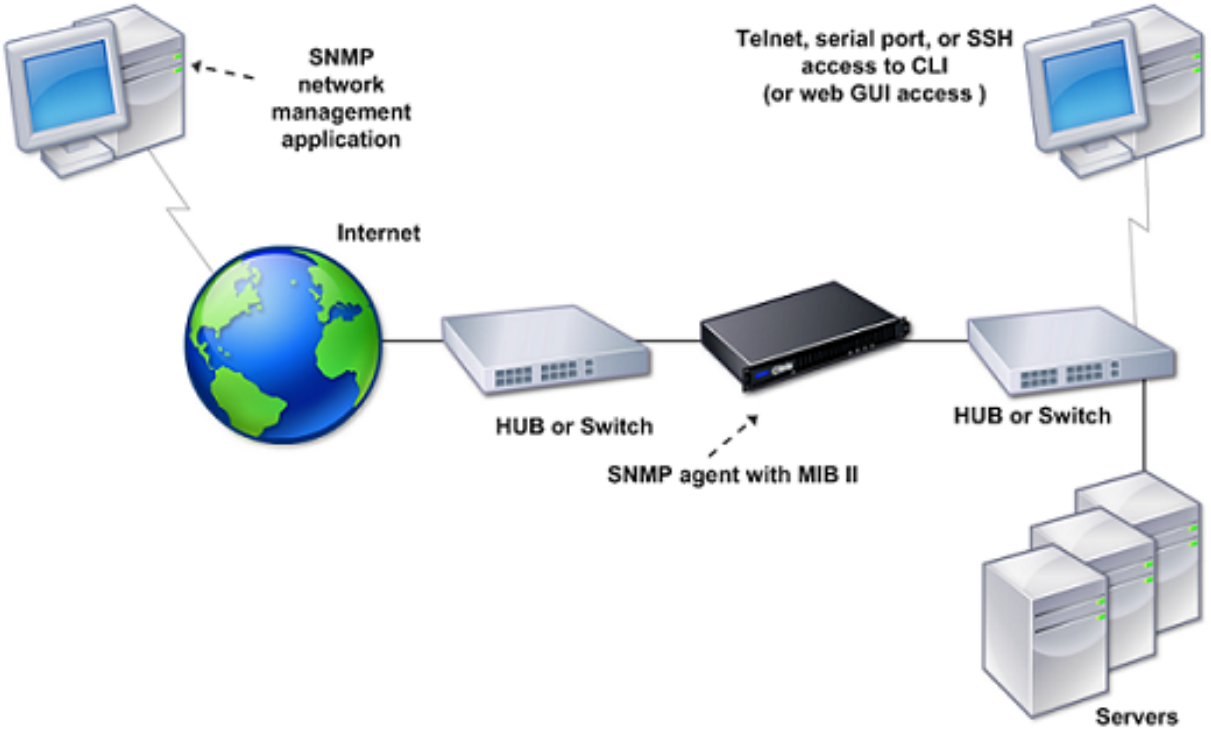
October 5, 2021

Sie können SNMP (Simple Network Management Protocol) verwenden, um den SNMP-Agent auf der Citrix ADC Appliance so zu konfigurieren, dass asynchrone Ereignisse generiert werden, die *Traps*genannt werden. Die Traps werden immer dann generiert, wenn auf dem Citrix ADC abnorme Bedingungen vorliegen. Die Traps werden dann an ein Remote-Gerät gesendet, das als *Trap-Listener* bezeichnet wird, das den anormalen Zustand der Citrix ADC Appliance signalisiert. Oder Sie können den SNMP-Agent systemspezifische Informationen von einem entfernten Gerät namens *SNMP-Manager abfragen*. Der Agent durchsucht dann die Management Information Base (MIB) nach den angeforderten Daten und sendet die Daten an den SNMP-Manager.

Der SNMP-Agent auf dem Citrix ADC kann Traps generieren, die mit SNMPv1, SNMPv2 und SNMPv3 kompatibel sind. Für die Abfrage unterstützt der SNMP-Agent SNMP Version 1 (SNMPv1), SNMP Version 2 (SNMPv2) und SNMP Version 3 (SNMPv3).

Informationen zu SNMP-Parametern, Traps und deren Beschreibungen finden Sie unter Citrix ADC SNMP OID Reference.

Die folgende Abbildung zeigt ein Netzwerk mit einem Citrix ADC, für das SNMP aktiviert und konfiguriert ist. In der Abbildung verwendet jede SNMP-Netzwerkverwaltungsanwendung SNMP, um mit dem SNMP-Agent auf dem Citrix ADC zu kommunizieren. Der SNMP-Agent durchsucht seine Management Information Base (MIB), um die vom SNMP-Manager angeforderten Daten zu sammeln und der Anwendung die Informationen zur Verfügung zu stellen.



Wichtig

Das SNMP-Modul in einer Citrix ADC Appliance unterstützt eine maximale Länge von 128 Byte (gemäß RFC 3416) für eine SNMP-OID. Ein langer Indexvariablenname für ein Objekt kann dazu führen, dass eine SNMP-OID größer als 128 Byte ist.

Um dieses Problem zu beheben, unterstützt das Citrix ADC SNMP-Modul eine maximale Länge von 31 Zeichen für einen Indexvariablennamen. Wenn ein Indexvariablenname 31 Zeichen lang ist, konvertiert das SNMP-Modul, das einen Hash-Algorithmus verwendet, den Namen in einen Hashwert von 31 Zeichen. Dieser Hash-Wert wird in der SNMP-OID für diese Variable verwendet.

Der ursprüngliche Name der Indexvariablen wird in einer anderen Variablen gespeichert, die das folgende Namensformat hat: `<variable type>FullName`. Wenn beispielsweise der Name eines virtuellen Lastausgleichsservers mehr als 31 Zeichen enthält, enthält `vserverName` SNMP OID den Hash-Wert und die `vsvrFullName` SNMP-OID enthält den vollständigen (ursprünglichen) Namen des virtuellen Servers.

In ähnlicher Weise zeigt die Indexvariable für SNMP-Traps einen Hash-Wert an. `<variable`

> `type`>`FullName`, der den vollständigen Namen des ursprünglichen Indexvariablennamens speichert, ist ebenfalls Teil der Fallenmeldungen.

Importieren von MIB-Dateien in den SNMP-Manager und Trap-Listener

Um eine Citrix ADC Appliance zu überwachen, müssen Sie die MIB-Objektdefinitionsdateien herunterladen. Die Citrix ADC Appliance unterstützt die folgenden unternehmensspezifischen MIBs:

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

Sie können die MIB-Objektdefinitionsdateien aus dem Verzeichnis /netscaler/snmp oder über die Registerkarte Downloads der GUI beziehen.

Konfigurieren des Citrix ADC zum Generieren von SNMP-Traps

October 5, 2021

Sie können die Citrix ADC Appliance so konfigurieren, dass asynchrone Ereignisse generiert werden, die *Traps*genannt werden. Die Traps werden immer dann generiert, wenn es abnormale Bedingungen auf der Appliance gibt. Die Traps werden an ein Remote-Gerät gesendet, das als *Trap-Listener*bezeichnet wird. Es hilft Administratoren, die Appliance zu überwachen und umgehend auf Probleme zu reagieren.

Die Citrix ADC Appliance stellt eine Reihe von Zustandsobjekten namens *SNMP-Alarme* bereit. Wenn die Bedingung in einem SNMP-Alarm erfüllt ist, generiert die Appliance SNMP-Trap-Nachrichten, die an die konfigurierten Trap-Listener gesendet werden. Wenn beispielsweise der Alarm LOGIN-FAILURE aktiviert ist, wird eine Trap-Nachricht generiert und an den Trap-Listener gesendet, wenn ein Anmeldefehler auf der Appliance auftritt.

Um die Citrix ADC Appliance zum Generieren von Traps zu konfigurieren, müssen Sie Alarme aktivieren und konfigurieren. Anschließend geben Sie die Trap-Listener an, an die die Appliance die generierten Trap-Nachrichten sendet.

Aktivieren eines SNMP-Alarms

Die Citrix ADC Appliance generiert Traps nur für aktivierte SNMP-Alarme. Einige Alarme sind standardmäßig aktiviert, Sie können sie jedoch deaktivieren.

Wenn Sie einen SNMP-Alarm aktivieren, generiert die Appliance entsprechende Trap-Meldungen, wenn einige Ereignisse auftreten. Einige Alarme sind standardmäßig aktiviert.

So aktivieren Sie einen SNMP-Alarm mit der CLI

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

- `enable snmp alarm <trapName>`
- `show snmp alarm <trapName>`

So aktivieren Sie einen SNMP-Alarm mit der GUI

1. Navigieren Sie zu **System > SNMP > Alarme**und wählen Sie den Alarm aus.
2. Klicken Sie auf **Aktionen** und wählen Sie **Aktivieren** aus.

Konfigurieren von Alarmen

Die Citrix ADC Appliance stellt eine Reihe von Zustandsobjekten namens *SNMP-Alarme* bereit. Wenn die Bedingung für einen SNMP-Alarm erfüllt ist, generiert die Appliance SNMP-Traps-Nachrichten, die an die konfigurierten Trap-Listener gesendet werden. Wenn beispielsweise der Alarm LOGIN-FAILURE aktiviert ist, wird eine Trap-Nachricht generiert und an den Trap-Listener gesendet, wenn ein Anmeldefehler auf der Appliance auftritt.

Sie können einen SNMP-Alarm mit einem Schweregrad zuweisen. Wenn Sie dies tun, wird den entsprechenden Trap-Meldungen dieser Schweregrad zugewiesen.

Im Folgenden werden die auf der Appliance definierten Schweregrade in abnehmender Reihenfolge des Schweregrads aufgeführt.

- Kritisch
- Hauptfach
- Geringfügig
- Warnung
- Zur Information

Wenn Sie beispielsweise einen Schweregrad der Warnung für den SNMP-Alarm mit dem Namen LOGIN-FAILURE festlegen, werden die Trap-Meldungen, die bei einem Anmeldefehler generiert werden, mit dem Schweregrad der Warnung zugewiesen.

> **Hinweis:**
>
> Citrix ADC unterstützt verschiedene SNMP-Alarme. Weitere Informationen finden Sie unter SNMP-Alarme.

Sie können auch einen SNMP-Alarm konfigurieren, um die entsprechenden Trap-Meldungen zu protokollieren, die generiert werden, wenn die Bedingung für diesen Alarm erfüllt ist.

So konfigurieren Sie einen SNMP-Alarm mit der CLI

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

- `set snmp alarm <trapName> [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-time <secs>] [-state ( ENABLED | DISABLED )] [-severity <severity>] [-logging ( ENABLED | DISABLED )]`
- `show snmp alarm <trapName>`

Hierbei gilt:

ThresholdValue: Wert für den hohen Schwellenwert. Die Citrix ADC Appliance generiert eine SNMP-Trap-Meldung, wenn der Wert des Attributs, das dem Alarm zugeordnet ist, größer oder gleich dem angegebenen hohen Schwellenwert ist.

NormalValue: Wert für den Normalschwellenwert. Eine Trap-Meldung wird generiert, wenn der Wert des jeweiligen Attributs nach Überschreitung des hohen Schwellenwerts auf oder unter diesen Wert fällt.

So konfigurieren Sie SNMP-Alarme mit der GUI

Navigieren Sie zu **System > SNMP > Alarme**, wählen Sie einen Alarm aus und konfigurieren Sie die Alarmparameter.

Konfigurieren von SNMPv1- oder SNMPv2-Traps

Nachdem Sie die Alarme konfiguriert haben, müssen Sie den Trap-Listener angeben, an den die Appliance die Trap-Nachrichten sendet. Neben der Angabe von Parametern wie IP- oder IPv6-Adresse und dem Zielport des Trap-Listener können Sie den Trap-Typ (entweder generisch oder spezifisch) und die SNMP-Version angeben.

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

Sie können die Appliance auch so konfigurieren, dass SNMP-Trap-Nachrichten mit einer anderen Quell-IP-Adresse als der Citrix ADC IP-Adresse (NSIP oder NSIP6) an einen bestimmten Trap-Listener gesendet werden. Für einen Trap-Listener mit einer IPv4-Adresse können Sie die Quell-IP entweder auf eine zugeordnete IP-Adresse (MIP) oder eine auf der Appliance konfigurierte Subnetz-IP-Adresse (SNIP) festlegen. Für einen Trap-Listener mit einer IPv6-Adresse können Sie die Quell-IP auf eine auf der Appliance konfigurierte Subnetz-IPv6 (SNIP6) -Adresse setzen.

Sie können die Appliance auch so konfigurieren, dass Trap-Nachrichten basierend auf einem Schweregrad an einen Trap-Listener gesendet werden. Wenn Sie beispielsweise den Schweregrad für einen

Trap-Listener als Minor festlegen, werden alle Trap-Meldungen des Schweregrads kleiner oder größer als Minor (Minor, Major und Critical) an den Trap-Listener gesendet.

Wenn Sie eine Community-Zeichenfolge für den Trap-Listener definiert haben, müssen Sie auch für jede Trap, die an den Listener gesendet werden soll, eine Community-Zeichenfolge angeben. Ein Trap-Listener, für den eine Community-Zeichenfolge definiert wurde, akzeptiert nur Trap-Nachrichten, die eine Community-Zeichenfolge enthalten, die mit der im Trap-Listener definierten Community-Zeichenfolge übereinstimmt. Andere Trap-Nachrichten werden gelöscht.

So fügen Sie eine SNMP-Trap mit der CLI hinzu

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

- `add snmp trap <trapClass> <trapDestination> -version ( V1 | V2 )-destPort <port> -communityName <string> -srcIP <ip_addr> -severity <severity>`
- `show snmp trap`

Beispiel:

```
> `add snmp trap specific 192.0.2.10 -version V2 -destPort 80 -communityName com1 -severity Major`
<!--NeedCopy-->
```

So konfigurieren Sie SNMP-Traps mit der GUI

Navigieren Sie zu **System > SNMP > Traps**und erstellen Sie die SNMP-Trap.

Konfigurieren von SNMPv3-Traps

SNMPv3 bietet Sicherheitsfunktionen wie Authentifizierung und Verschlüsselung mit der Anmeldeinformationen von SNMP-Benutzern. Ein SNMP-Manager kann SNMPv3-Trapmeldungen nur empfangen, wenn seine Konfiguration das dem SNMP-Benutzer zugewiesene Kennwort enthält.

Das Trap-Ziel kann nun SNMPv1-, SNMPv2- und SNMPv3-Trapmeldungen empfangen.

So konfigurieren Sie eine SnmPv3-Trap mit der CLI

Führen Sie an der Eingabeaufforderung die folgenden Schritte aus:

1. Fügen Sie eine SNMPv3-Trap hinzu.

   ```
   add snmp trap <trapClass> <trapDestination> -version ( V1 | V2 | V3)
   -destPort <port> -communityName <string> -srcIP <ip_addr> -severity <
   severity>
   ```

   > **Hinweis:**
   >
   > Nach der Einstellung kann die SNMP-Trap-Version nicht geändert werden.

   Beispiel

   ```
   1 > add snmp trap specific 192.0.2.10 -version V3 -destPort 80 -
       communityName com1 -severity Major
   2 <!--NeedCopy-->
   ```

2. Fügen Sie einen SNMP-Benutzer hinzu.

   ```
   add snmp user <name> -group <string> [ -authType ( MD5 | SHA ){ -
   authPasswd } [-privType ( DES | AES ){ -privPasswd } ]]
   ```

   Beispiel

   ```
   1 > add snmp user edocs_user -group edocs_group
   2 <!--NeedCopy-->
   ```

3. Binden Sie den SNMPv3-Trap an den SNMP-Benutzer.

```
bind snmp trap <trapClass> <trapDestination> [-version <version>] (-userName
 <string> [-securityLevel <securityLevel>])
```

Beispiel

```
1     > bind snmp trap specific 192.0.2.10 -version V3 -userName
        edocs_user -securityLevel authPriv
2 <!--NeedCopy-->
```

So konfigurieren Sie einen SNMPv3-Trap mit der GUI

1. Fügen Sie eine SNMPv3-Trap hinzu.

   Navigieren Sie zu **System > SNMP > Traps**, und erstellen Sie die SNMP-Trap, indem Sie V3 als SNMP-Version auswählen.

2. Fügen Sie einen SNMP-Benutzer hinzu.

   Navigieren Sie zu **System > SNMP > Benutzer** und erstellen Sie den SNMP-Benutzer.

3. Binden Sie den SNMPv3-Trap an den SNMP-Benutzer.

   - Navigieren Sie zu **System > SNMP > Traps**und wählen Sie die Trap der SNMP Version 3 aus.
   - Wählen Sie den Benutzer aus, an den der Trap gebunden werden soll, und definieren Sie die entsprechende Sicherheitsstufe.

SNMP-Trap-Protokollierung

Eine Citrix ADC Appliance kann SNMP-Trap-Nachrichten (für SNMP-Alarme, in denen die Protokollierungsfunktion aktiviert ist) protokollieren, wenn Sie die SNMP-Trap-Protokollierungsoption aktivieren und mindestens ein Trap-Listener auf der Appliance konfiguriert ist. Jetzt können Sie die Überwachungsprotokollstufe von Trap-Nachrichten angeben, die an einen externen Protokollserver gesendet werden. Die Standardprotokollstufe ist Informational. Mögliche Werte sind Emergency, Alert, Kritisch, Fehler, Warnung, Debug und Notice.

Beispielsweise können Sie die Überwachungsprotokollstufe auf Kritisch für eine SNMP-Trapnachricht festlegen, die durch einen Anmeldefehler generiert wird. Diese Informationen stehen dann auf dem NSLOG- oder SYSLOG-Server zur Fehlerbehebung zur Verfügung.

So aktivieren Sie die SNMP-Trap-Protokollierung und konfigurieren Trap Log Level mit der CLI

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um die SNMP-Trap-Protokollierung zu konfigurieren und die Konfiguration zu überprüfen:

- `set snmp option [-snmpTrapLogging (ENABLED | DISABLED)][-snmpTrapLoggingLevel <snmpTrapLoggingLevel>]`
- `show snmp option`

So aktivieren Sie die SNMP-Trapprotokollierung und konfigurieren die SNMP-Trap-Log-Ebene mit der GUI

Navigieren Sie zu **System > SNMP**, klicken Sie auf SNMP-Optionen ändern und legen Sie die folgenden Parameter fest:

1. SNMP-Trapprotokollierung — Aktivieren Sie dieses Kontrollkästchen, um die SNMP-Trapprotokollierung zu aktivieren, wenn mindestens ein Trap-Listener auf der Appliance konfiguriert ist.
2. SNMP-Trap-Protokollierungsebene — Wählen Sie eine Überwachungsprotokollstufe für das SNMP-Trap aus. Standardmäßig ist die Auditstufe für eine SNMP-Trap auf “Informational” festgelegt.

Konfigurieren von Citrix ADC für SNMP-v1- und v2-Abfragen

December 7, 2021

Sie können den Citrix ADC SNMP-Agent systemspezifische Informationen von einem Remotegerät namens *SNMP-Manager abfragen*. Der Agent durchsucht dann die Management Information Base (MIB) nach den angeforderten Daten und sendet die Daten an den SNMP-Manager.

Die folgenden Typen von SNMP v1 und v2 Abfragen werden vom SNMP-Agent unterstützt:

- GET
- GET NEXT
- ALL
- GET BULK

Sie können Zeichenfolgen erstellen, die als Community-Zeichenfolgen bezeichnet werden und jede dieser Abfragetypen zuordnen. Sie können jedem Abfragetyp eine oder mehrere Community-Zeichenfolgen zuordnen. Community-Zeichenfolge sind Kennwörter, die zum Authentifizieren von SNMP-Abfragen von SNMP-Managern verwendet werden.

Wenn Sie z. B. zwei Community-Zeichenfolgen, wie **abc** und **bcd**, dem Abfragetyp GET NEXT zuordnen, berücksichtigt der SNMP-Agent auf der Citrix ADC Appliance nur die GET NEXT SNMP-Abfragepakete, die **abc** oder **bcd** enthalten, als Community -Zeichenkette.

Angeben eines SNMP-Managers

Sie müssen die Citrix ADC Appliance so konfigurieren, dass die entsprechenden SNMP-Manager sie abfragen können. Sie müssen dem SNMP-Manager auch die erforderlichen Citrix ADC-spezifischen Informationen bereitstellen. Sie können bis zu 100 SNMP-Manager oder Netzwerke hinzufügen.

Für einen IPv4-SNMP-Manager können Sie anstelle der IP-Adresse des Managers einen Hostnamen angeben. Wenn Sie dies tun, müssen Sie einen DNS-Namensserver hinzufügen, der den Hostnamen des SNMP-Managers seiner IP-Adresse auflöst. Sie können bis zu fünf Hostnamen basierte SNMP-Manager hinzufügen.

> **Hinweis**:
> Die Appliance unterstützt die Verwendung von Hostnamen für SNMP-Manager mit IPv6-Adressen nicht. Sie müssen die IPv6-Adresse angeben.

Wenn Sie nicht mindestens einen SNMP-Manager konfigurieren, akzeptiert die Appliance SNMP-Abfragen von allen IP-Adressen im Netzwerk und antwortet darauf. Wenn Sie einen oder mehrere SNMP-Manager konfigurieren, akzeptiert die Appliance nur SNMP-Abfragen von diesen spezifischen IP-Adressen und antwortet sie.

Wenn Sie einen SNMP-Manager aus der Konfiguration entfernen, kann dieser Manager die Appliance nicht mehr abfragen.

So fügen Sie SNMP-Manager hinzu, indem Sie IP-Adressen mit der Befehlszeilenschnittstelle angeben

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

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

Beispiel

```
> add snmp manager 10.102.29.10 10.102.29.15 10.102.29.30
```

So fügen Sie einen SNMP-Manager hinzu, indem Sie seinen Hostnamen mit der Befehlszeilenschnittstelle angeben

Wichtig: Wenn Sie anstelle der IP-Adresse den Hostnamen des SNMP-Managers angeben, müssen Sie einen DNS-Nameserver konfigurieren, um den Hostnamen in die IP-Adresse des SNMP-Managers aufzulösen. Weitere Informationen finden Sie unter "Hinzufügen eines Nameservers. "

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

- `add snmp manager <IPAddress> [-domainResolveRetry ** **<integer>]`
- `show snmp manager`

Beispiel

```
add nameserver 10.103.128.15
add snmp manager engwiki.eng.example.net -domainResolveRetry 10
```

So fügen Sie einen SNMP-Manager mit der GUI hinzu

1. Navigieren Sie zu **System** > **SNMP** > **Manager**, und erstellen Sie den SNMP-Manager.

   > **Wichtig**:
   >
   > Wenn Sie anstelle der IPv4-Adresse den Hostnamen des SNMP-Managers angeben, müssen Sie einen DNS-Nameserver konfigurieren, um den Hostnamen in die IP-Adresse des SNMP-Managers aufzulösen.

> **Hinweis**:
> Die Appliance unterstützt keine Hostnamen für SNMP-Manager mit IPv6-Adressen.

Angeben einer SNMP-Community

Sie können Zeichenfolgen erstellen, die als Community-Zeichenfolgen bezeichnet werden und sie den folgenden SNMP-Abfragetypen auf der Appliance zuordnen:

- GET
- GET NEXT
- ALL
- GET BULK

Sie können jedem Abfragetyp eine oder mehrere Community-Zeichenfolgen zuordnen. Wenn Sie z. B. dem Abfragetyp GET NEXT zwei Community-Zeichenfolgen, z. B. **abc** und **bcd**, zuordnen, berücksichtigt der SNMP-Agent auf der Appliance nur die GET NEXT SNMP-Abfragepakete, die **abc** oder **bcd** enthalten, als Community-Zeichenfolge.

Wenn Sie einem Abfragetyp keine Community-Zeichenfolge zuordnen, antwortet der SNMP-Agent auf alle SNMP-Abfragen dieses Typs.

So geben Sie eine SNMP-Community mit der Befehlszeilenschnittstelle an

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

- `add snmp community <communityName> <permissions>`
- `show snmp community`

Beispiel

```
> add snmp community com all
```

So konfigurieren Sie eine SNMP-Community-Zeichenfolge mit der GUI

Navigieren Sie zu **System** > **SNMP** > **Community**, und erstellen Sie die SNMP-Community.

Konfigurieren von Citrix ADC für SNMPv3-Abfragen

October 5, 2021

Simple Network Management Protocol Version 3 (SNMPv3) basiert auf der Grundstruktur und Architektur von SNMPv1 und SNMPv2. SNMPv3 erweitert jedoch die grundlegende Architektur, um Verwaltungs- und Sicherheitsfunktionen wie Authentifizierung, Zugriffskontrolle, Datenintegritätsprüfung, Datenursprungsüberprüfung, Nachrichtenzeitprüfung und Datenvertraulichkeit zu integrieren.

Zur Implementierung von Sicherheit und Zugriffssteuerung auf Nachrichtenebene führt SNMPv3 das benutzerbasierte Sicherheitsmodell (USM) und das ansichtsbasierte Zugriffssteuerungsmodell (VACM) ein.

- **Benutzerbasiertes Sicherheitsmodell.** Das benutzerbasierte Sicherheitsmodell (USM) bietet Sicherheit auf Nachrichtenebene. Sie können Benutzer und Sicherheitsparameter für den SNMP-Agent und den SNMP-Manager konfigurieren. USM bietet folgende Funktionen:
  - **Datenintegrität:** Zum Schutz von Nachrichten während der Übertragung über das Netzwerk vor Änderungen.
  - **Überprüfung der Datenursprung:** Authentifizieren des Benutzers, der die Nachrichtenanforderung gesendet hat.
  - **Aktualität der Nachricht:** Zum Schutz vor Verzögerungen oder Wiederholungen von Nachrichten.
  - **Vertraulichkeit der Daten:** Um den Inhalt von Nachrichten vor der Weitergabe an nicht autorisierte Personen oder Personen zu schützen.
- **Ansichtsbasiertes Zugriffssteuerungsmodell.** Mit dem ansichtsbasierten Zugriffssteuerungsmodell (VACM) können Sie Zugriffsrechte für einen bestimmten Teilbaum der MIB basierend auf verschiedenen Parametern konfigurieren, wie Sicherheitsstufe, Sicherheitsmodell, Benutzername und Ansichtstyp. Es ermöglicht Ihnen, Agenten so zu konfigurieren, dass verschiedenen Managern unterschiedliche Zugriffsebenen auf die MIB zur Verfügung gestellt werden.

Citrix ADC unterstützt die folgenden Entitäten, mit denen Sie die Sicherheitsfunktionen von SNMPv3 implementieren können:

- SNMP-Engines
- SNMP-Ansichten
- SNMP-Gruppen
- SNMP-Benutzer

Diese Entitäten arbeiten zusammen, um die SNMPv3-Sicherheitsfunktionen zu implementieren. Ansichten werden erstellt, um den Zugriff auf Teilbäume der MIB zu ermöglichen. Anschließend werden Gruppen mit der erforderlichen Sicherheitsstufe und Zugriff auf die definierten Ansichten erstellt. Schließlich werden Benutzer erstellt und den Gruppen zugewiesen.

> **Hinweis**:
>
> Die View-, Gruppen- und Benutzerkonfiguration werden synchronisiert und in einem HA-Paar (High Availability) an den sekundären Knoten weitergegeben. Die Engine-ID wird jedoch weder propagiert noch synchronisiert, da sie für jede Citrix ADC Appliance eindeutig ist.

Um die Nachrichtenauthentifizierung und die Zugriffssteuerung zu implementieren, müssen Sie Folgendes tun:

Einstellen der Motorkennung

SNMP-Engines sind Dienstanbieter, die sich im SNMP-Agent befinden. Sie bieten Dienste wie das Senden, Empfangen und Authentifizieren von Nachrichten. SNMP-Engines werden mithilfe von Engine-IDs eindeutig identifiziert.

Die Citrix ADC Appliance verfügt über eine eindeutige EngineID basierend auf der MAC-Adresse einer ihrer Schnittstellen. Es ist nicht notwendig, die EngineID zu überschreiben. Wenn Sie jedoch die Engine-ID ändern möchten, können Sie sie zurücksetzen.

So legen Sie die Engine-ID mit der Befehlszeilenschnittstelle fest

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

- `set snmp engineId <engineID>`
- `show snmp engineId`

Beispiel

```
> set snmp engineId 8000173f0300c095f80c68
```

So legen Sie die Engine-ID mit der GUI fest

Navigieren Sie zu **System** > **SNMP** > **Benutzer**, klicken Sie auf **Engine-ID konfigurieren**, und geben Sie eine Engine-ID ein.

Konfigurieren einer Ansicht

SNMP-Ansichten beschränken den Benutzerzugriff auf bestimmte Teile der MIB. SNMP-Ansichten werden verwendet, um Zugriffskontrolle zu implementieren.

So fügen Sie mit der Befehlszeilenschnittstelle eine SNMP-Ansicht hinzu

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

- `add snmp view <name> <subtree> -type ( included | excluded )`
- `show snmp view <name>`
- `rm snmp view <name> <subtree>`

Hierbei gilt:

Name. Name für die SNMPv3-Ansicht. Es kann aus 1 bis 31 Zeichen bestehen, die Groß- und Kleinbuchstaben, Zahlen und Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), Zeichen (@), Gleich (=), Doppelpunkt (:) und Unterstrich (_) enthalten. Sie sollten einen Namen auswählen, der die SNMPv3-Ansicht identifiziert.

Unterbaum. Ein bestimmter Zweig (Teilbaum) des MIB-Baumes, den Sie dieser SNMPv3-Ansicht zuordnen möchten. Sie müssen den Teilbaum als SNMP-OID angeben. Dies ist ein Argument der maximalen Länge: 99.

type. Fügen Sie den durch den Teilbaum-Parameter angegebenen Teilbaum in oder aus dieser Ansicht ein oder schließen Sie diesen aus. Diese Einstellung kann nützlich sein, wenn Sie einen Teilbaum, z. B. A, in eine SNMPv3-Ansicht aufgenommen haben und einen bestimmten Teilbaum von A, z. B. B, aus der SNMPv3-Ansicht ausschließen möchten. Dies ist ein obligatorisches Argument. Mögliche Werte: eingeschlossen, ausgeschlossen.

Beispiele

add snmp view SNMPv3test 1.1.1.1 -type included
sh snmp view SNMPv3test
rm snmp view SNMPv3test 1.1.1.1

So konfigurieren Sie eine SNMP-Ansicht mit der GUI

Navigieren Sie zu **System** > **SNMP** > **Ansichten**, und erstellen Sie die SNMP-Ansicht.

Konfigurieren einer Gruppe

SNMP-Gruppen sind logische Aggregationen von SNMP-Benutzern. Sie werden verwendet, um die Zugriffssteuerung zu implementieren und die Sicherheitsstufen zu definieren. Sie können eine SNMP-Gruppe so konfigurieren, dass Zugriffsrechte für Benutzer festgelegt werden, die dieser Gruppe zugewiesen sind, wodurch die Benutzer auf bestimmte Ansichten beschränkt werden.

Sie müssen eine SNMP-Gruppe konfigurieren, um Zugriffsrechte für Benutzer festzulegen, die dieser Gruppe zugewiesen sind.

So fügen Sie eine SNMP-Gruppe mit der Befehlszeilenschnittstelle hinzu

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

- `add snmp group <name> <securityLevel> -readViewName <string>`
- `show snmp group <name> <securityLevel>`

Hierbei gilt:

Name. Name für die SNMPv3-Gruppe. Kann aus 1 bis 31 Zeichen bestehen, die Groß- und Kleinbuchstaben, Zahlen und Bindestrich (-), Punkt (.) Pfund (#), Leerzeichen (), Zeichen (@), Gleich (=), Doppelpunkt (:) und Unterstrich (_) enthalten. Sie sollten einen Namen auswählen, der die SNMPv3-Gruppe identifiziert.

securityLevel. Sicherheitsstufe für die Kommunikation zwischen der Citrix ADC Appliance und den SNMPv3-Benutzern, die zur Gruppe gehören, erforderlich. Geben Sie eine der folgenden Optionen an:

noAuthNoPriv. Weder Authentifizierung noch Verschlüsselung erforderlich.

authNoPriv. Authentifizierung erforderlich, aber keine Verschlüsselung.

authPriv. Authentifizierung und Verschlüsselung erforderlich. Hinweis: Wenn Sie die Authentifizierung angeben, müssen Sie einen Verschlüsselungsalgorithmus angeben, wenn Sie der Gruppe einen SNMPv3-Benutzer zuweisen. Wenn Sie auch Verschlüsselung angeben, müssen Sie jedem Gruppenmitglied sowohl eine Authentifizierung als auch einen Verschlüsselungsalgorithmus zuweisen. Dies ist ein obligatorisches Argument. Mögliche Werte: NoAuthNoPriv, AuthNoPriv, AuthPriv.

readViewName. Name der konfigurierten SNMPv3-Ansicht, die Sie an diese SNMPv3-Gruppe binden möchten. Ein an diese Gruppe gebundener SNMPv3-Benutzer kann auf die Teilbäume zugreifen, die an diese SNMPv3-Ansicht als INCLUDED gebunden sind, aber nicht auf die vom Typ EXCLUDED. Wenn die Citrix ADC Appliance über mehrere SNMPv3-View-Einträge mit demselben Namen verfügt, sind alle diese Einträge der SNMPv3-Gruppe zugeordnet. Dies ist ein obligatorisches Argument. Maximale Länge: 31

So konfigurieren Sie eine SNMP-Gruppe mit der GUI

Navigieren Sie zu **System** > **SNMP** > **Gruppen**, und erstellen Sie die SNMP-Gruppe.

Konfigurieren eines Benutzers

SNMP-Benutzer sind die SNMP-Manager, die die Agenten erlauben, auf die MIBs zuzugreifen. Jeder SNMP-Benutzer wird einer SNMP-Gruppe zugewiesen.

Sie müssen Benutzer am Agent konfigurieren und jeden Benutzer einer Gruppe zuweisen.

So konfigurieren Sie einen Benutzer mit der Befehlszeilenschnittstelle

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

- `add snmp user <name> -group <string> [-authType ( MD5 | SHA ){ -authPasswd } [-privType ( DES | AES ){ -privPasswd } ]]`
- `show snmp user <name>`

Hierbei gilt:

AuthType ist die Authentifizierungsoption, die während der Konfiguration eines Benutzers verfügbar ist. Es gibt zwei Authentifizierungstypen wie MD5 und SHA.

PrivType ist die Verschlüsselungsoption, die während der Konfiguration eines Benutzers verfügbar ist. Es gibt zwei Arten von Verschlüsselung wie DES der Schlüsselgröße 128 Bit und AES der Schlüsselgröße 128 Bit.

Beispiel

```
1 > add snmp user edocs_user -group edocs_group
2 <!--NeedCopy-->
```

So konfigurieren Sie einen SNMP-Benutzer mit der GUI

Navigieren Sie zu **System** > **SNMP** > **Benutzer**, und erstellen Sie den SNMP-Benutzer.

Konfigurieren von SNMP-Alarmen für die Ratenbegrenzung

October 5, 2021

Citrix ADC-Appliances wie Citrix ADC MPX 10500, 12500 und 15500 sind begrenzt. Der maximale Durchsatz (Mbit/s) und die Pakete pro Sekunde (PPS) werden durch die für die Appliance erworbene Lizenz bestimmt. Für plattformbeschränkte Plattformen können Sie SNMP-Traps so konfigurieren, dass Benachrichtigungen gesendet werden, wenn Durchsatz und PPS ihren Grenzwerten nähern und wenn sie wieder normal sind.

Durchsatz und PPS werden alle sieben Sekunden überwacht. Sie können Traps mit hohen Schwellenwerten und Normalschwellenwerten konfigurieren, die als Prozentsatz der lizenzierten Grenzwerte

ausgedrückt werden. Die Appliance generiert dann eine Trap, wenn der Durchsatz oder PPS den hohen Schwellenwert überschreitet, und eine zweite Trap, wenn der überwachte Parameter auf den normalen Schwellenwert fällt. Zusätzlich zum Senden der Traps an das konfigurierte Zielgerät protokolliert Citrix ADC die Ereignisse, die den Traps in der Datei /var/log/ns.log zugeordnet sind, als EVENT ALERTSTARTED und EVENT ALERTENDED.

Das Überschreiten der Durchsatzgrenze kann zu Paketverlust führen. Sie können SNMP-Alarme konfigurieren, um Paketverlust zu melden.

Weitere Informationen zu SNMP-Alarmen und Traps finden Sie unter "Konfigurieren des Citrix ADC zum Generieren von SNMP v1- und v2-Traps. "

Dieses Dokument enthält die folgenden Details:

- Konfigurieren eines SNMP-Alarms für Durchsatz oder PPS
- SNMP-Alarm für gelöschte Pakete konfigurieren

Konfigurieren eines SNMP-Alarms für Durchsatz oder PPS

Um sowohl im gesamten als auch in PPS zu überwachen, müssen Sie Seperate Alarme konfigurieren und den Schwellenwert pps-Wert in Mbps festlegen.

So konfigurieren Sie einen SNMP-Alarm für die Durchsatzrate mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den SNMP-Alarm zu konfigurieren, den Schwellenwert in Mbps festzulegen und die Konfiguration zu überprüfen:

- `set snmp alarm PF-RL-RATE-THRESHOLD [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-state ( **ENABLED** | **DISABLED** )] [-severity <severity>] [-logging ( **ENABLED** | **DISABLED** )]`
- `show snmp alarm PF-RL-RATE-THRESHOLD`

Beispiel

```
1 > set snmp alarm PF-RL-RATE-THRESHOLD -thresholdValue 70 -normalValue
     50
2 <!--NeedCopy-->
```

So konfigurieren Sie einen SNMP-Alarm für PPS mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um den SNMP-Alarm für PPS zu konfigurieren und die Konfiguration zu überprüfen:

- `set snmp alarm PF-RL-PPS-THRESHOLD [-thresholdValue <positive_integer> [-normalValue <positive_integer>]] [-state ( **ENABLED** | **DISABLED** )] [-severity <severity>] [-logging ( **ENABLED** | **DISABLED** )]`
- `show snmp alarm PF-RL-PPS-THRESHOLD`

Beispiel

```
> set snmp alarm PF-RL-PPS-THRESHOLD -thresholdValue 70 -normalValue 50
<!--NeedCopy-->
```

So konfigurieren Sie einen SNMP-Alarm für Durchsatz oder PPS mit der GUI

1. Navigieren Sie zu **System** > **SNMP** > **Alarme**, und wählen Sie **PF-RL-RATE-THRESHOLD** (für Durchsatzrate) oder **PF-RL-PPS-THRESHOLD** (für Pakete pro Sekunde).
2. Stellen Sie die Alarmparameter ein und aktivieren Sie den ausgewählten SNMP-Alarm.

SNMP-Alarm für verlorene Pakete konfigurieren

Sie können einen Alarm für Pakete konfigurieren, die infolge der Überschreitung des Durchsatzgrenzwerts und einen Alarm für Pakete, die infolge der Überschreitung des PPS-Grenzwerts fallen.

So konfigurieren Sie einen SNMP-Alarm für Pakete, die aufgrund eines übermäßigen Durchsatzes abgelegt wurden, mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set snmp alarm PF-RL-RATE-PKTS-DROPPED [-state (ENABLED | DISABLED)] [-severity <severity>] [-logging ( ENABLED | DISABLED )]
```

So konfigurieren Sie einen SNMP-Alarm für Pakete, die wegen übermäßiger PPS abgelegt wurden, mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set snmp alarm PF-RL-PPS-PKTS-DROPPED [-state (ENABLED | DISABLED)] [-severity <severity>] [-logging ( ENABLED | DISABLED )]
```


So konfigurieren Sie einen SNMP-Alarm für verlorene Pakete mit der GUI

1. Navigieren Sie zu **System** > **SNMP** > **Alarme**, und wählen Sie **PF-RL-RATE-PKTS-DROPPED** (für Pakete, die aufgrund eines übermäßigen Durchsatzes fallen) oder **PF-RL-PPS-PKTS-DROPPED** (für Pakete, die wegen übermäßiger PPS verworfen wurden).
2. Stellen Sie die Alarmparameter ein und aktivieren Sie den ausgewählten SNMP-Alarm.

Konfigurieren von SNMP im FIPS-Modus

October 5, 2021

Für den FIPS-Modus ist SNMPv3 (Simple Network Management Protocol, Version 3) mit der Authentifizierungs- und Datenschutzoption (authPriv) erforderlich. SNMP Version 1 und Version 2 verwenden einen Community-String-Mechanismus, um einen sicheren Zugriff auf Verwaltungsdaten zu ermöglichen. Die Community-Zeichenfolge wird als Klartext zwischen einem SNMP-Manager und einem SNMP-Agent gesendet. Diese Art der Kommunikation ist unsicher, sodass Eindringlinge auf SNMP-Informationen im Netzwerk zugreifen können.

Das SNMPv3-Protokoll verwendet das benutzerbasierte Sicherheitsmodell (USM) und das View-based Access Control Model (VACM), um den Verwaltungszugriff auf SNMP-Messagingdaten zu authentifizieren und zu steuern. SNMPv3 hat drei Sicherheitsstufen: keine Authentifizierung keine Privatsphäre (NoAuthnoPriv), Authentifizierung und keine Privatsphäre (AuthNoPriv) und Authentifizierung und Datenschutz (AuthNoPriv).

Wenn Sie den FIPS-Modus aktivieren und die Citrix ADC Appliance neu starten, werden die folgenden SNMP-Konfigurationen von der Appliance entfernt:

1. Community-Konfiguration für SNMPv1- und SNMPv2-Protokolle.
2. SNMPv3-Gruppen, die mit der Sicherheitsstufe NoAuthNoPriv oder AuthNoPriv konfiguriert sind.
3. Traps, die für SNMPv1 oder SNMPv2 oder SNMPv3 mit der Sicherheitsstufe NoAuthnoPriv konfiguriert sind.

Nach dem Neustart der Appliance konfigurieren Sie SNMPv3 mit der Option AuthPriv. Weitere Informationen zum Konfigurieren der AuthPriv-Option in SMNP v3 finden Sie im Thema SNMPV3

> **Hinweis**:
>
> Durch Aktivieren des FIPS-Modus und Neustart der Appliance wird die Ausführung der folgenden SNMP-Trap- und Gruppenbefehle blockiert:

```
1      1.  add snmp community <communityName> <permissions>
```



```
2
3     2.  add snmp trap <trapClass> <trapDestination> ... [-version: v1/
          v2]   [-td <positive_integer>] [-destPort <port>] [-
          communityName <string>] [-srcIP <ip_addr|ipv6_addr>] [-severity
          <severity>] [-allPartitions ( ENABLED | DISABLED )]
4
5     3.  add snmp group <name> <securityLevel : noAuthNoPriv/ authNoPriv
           > -readViewName <string>
6
7     4.  bind snmp trap specific <TrapIp>-userName <v3 user name> -
          securityLevel <noAuthNoPriv/ authNoPriv>
8 <!--NeedCopy-->
```

Überwachungsprotokollierung

October 5, 2021

> **Wichtig**
>
> Citrix empfiehlt, dass Sie eine SYSLOG- oder NSLOG-Konfiguration nur während der Wartung oder Ausfallzeit aktualisieren. Wenn Sie eine Konfiguration nach dem Erstellen einer Sitzung aktualisieren, werden die Änderungen nicht auf die vorhandenen Sitzungsprotokolle angewendet.

Auditing ist eine methodische Untersuchung oder Überprüfung eines Zustands oder einer Situation. Mit der Überwachungsprotokollierungsfunktion können Sie die von verschiedenen Modulen gesammelten Citrix ADC Zustände und Statusinformationen protokollieren. Die Protokollinformationen können sich im Kernel und in den Daemons auf Benutzerebene befinden. Für die Überwachungsprotokollierung können Sie das SYSLOG-Protokoll, das native NSLOG-Protokoll oder beides verwenden.

SYSLOG ist ein Standardprotokoll für die Protokollierung. Es besteht aus zwei Komponenten:

- **SYSLOG Auditing-Modul.** Läuft auf der Citrix ADC Appliance.
- **SYSLOG-Server** Läuft auf dem zugrunde liegenden FreeBSD-Betriebssystem (OS) der Citrix ADC Appliance oder auf einem Remote-System.

SYSLOG verwendet ein Benutzerdatenprotokoll (UDP) für die Datenübertragung.

In ähnlicher Weise besteht das native NSLOG-Protokoll aus zwei Komponenten:

- **NSLOG-Auditing-Modul.** Läuft auf der Citrix ADC Appliance.
- **NSLOG-Server** Läuft auf dem zugrunde liegenden FreeBSD-Betriebssystem der Citrix ADC Appliance oder auf einem Remote-System.

NSLOG verwendet TCP für die Datenübertragung.

Wenn Sie einen SYSLOG- oder NSLOG-Server ausführen, stellt er eine Verbindung mit der Citrix ADC Appliance her. Die Citrix ADC Appliance beginnt dann, alle Protokollinformationen an den SYSLOG- oder NSLOG-Server zu senden. Und der Server filtert die Log-Einträge, bevor sie in einer Protokolldatei gespeichert werden. Ein NSLOG- oder SYSLOG-Server erhält Protokollinformationen von mehr als einer Citrix ADC Appliance. Die Citrix ADC Appliance sendet Protokollinformationen an mehr als einen SYSLOG-Server oder NSLOG-Server.

Wenn mehrere SYSLOG-Server konfiguriert sind, sendet die Citrix ADC Appliance ihre SYSLOG-Ereignisse und Nachrichten an alle konfigurierten externen Protokollserver. Dies führt zum Speichern redundanter Nachrichten und erschwert Systemadministratoren die Überwachung. Um dieses Problem zu beheben, bietet die Citrix ADC Appliance Algorithmen für den Lastenausgleich an. Die Appliance kann die SYSLOG-Nachrichten zwischen den externen Protokollservern für eine bessere Wartung und Leistung ausgleichen. Die unterstützten Load Balancing-Algorithmen umfassen RoundRobin, LeastBandWidth, CustomLoad, LeastPackets und AuditLogHash.

> **Hinweis:**
>
> Die Citrix ADC Appliance kann Überwachungsprotokollmeldungen bis zu 16 KB an einen externen SYSLOG-Server senden.

Die Protokollinformationen, die ein SYSLOG- oder NSLOG-Server von einer Citrix ADC Appliance sammelt, werden in einer Protokolldatei in Form von Nachrichten gespeichert. Diese Meldungen enthalten normalerweise die folgenden Informationen:

- Die IP-Adresse einer Citrix ADC Appliance, die die Protokollnachricht generiert hat.
- Zeitstempel
- Meldungstyp
- Die vordefinierten Protokollebenen (Kritisch, Fehler, Hinweis, Warnung, Information, Debug, Alert und Emergency)
- Meldungstext

Zum Konfigurieren der Überwachungsprotokollierung konfigurieren Sie zunächst die Überwachungsmodule auf der Citrix ADC Appliance. Die Appliance umfasst die Erstellung von Überwachungsrichtlinien und die Angabe der NSLOG-Server- oder SYSLOG-Serverinformationen. Anschließend installieren und konfigurieren Sie den SYSLOG- oder NSLOG-Server auf dem zugrunde liegenden FreeBSD-Betriebssystem der Citrix ADC Appliance oder auf einem Remote-System.

> **Hinweis:**
>
> SYSLOG ist ein Industriestandard für die Protokollierung von Programmnachrichten, und verschiedene Anbieter bieten Unterstützung. Die Dokumentation enthält keine Informationen zur SYSLOG-Serverkonfiguration.

Der NSLOG-Server verfügt über eine eigene Konfigurationsdatei (auditlog.conf). Sie können die Protokollierung auf dem NSLOG-Serversystem anpassen, indem Sie zusätzliche Änderungen an der Kon-

figurationsdatei vornehmen (auditlog.conf).

Konfigurieren der Citrix ADC-Appliance für die Überwachungsprotokollierung

January 25, 2022

> **Warnung:**
>
> Klassische Richtlinienausdrücke und ihre Verwendung sind ab Citrix ADC 12.0 Build 56.20 veraltet (von der Verwendung abgeraten, aber immer noch unterstützt). Als Alternative empfiehlt Citrix die Verwendung erweiterter Richtlinien. Weitere Informationen finden Sie unter Erweiterte Richtlinien.

Bei der Audit-Protokollierung werden Statusinformationen aus verschiedenen Modulen angezeigt, sodass ein Administrator den Ereignisverlauf in chronologischer Reihenfolge sehen kann. Hauptbestandteile eines Prüfungsrahmens sind “Prüfungsaktion”, “Audit-Richtlinie”. “Audit-Aktion” beschreibt Konfigurationsinformationen des Überwachungsservers, während “Audit-Richtlinie” eine Bindungseinheit mit einer “Audit-Aktion” verknüpft. Die Prüfungsrichtlinien verwenden das Framework “Classic Policy Engine” (CPE) oder das Progress Integration (PI) -Framework, um “Prüfungsmaßnahmen” mit “globalen Systembindungsgesellschaften” zu verknüpfen.

Die politischen Rahmenbedingungen unterscheiden sich jedoch in der Bindung von Auditprotokoll-Richtlinien an globale Einheiten. Zuvor unterstützte das Audit-Modul nur den klassischen Ausdruck, aber jetzt unterstützt es sowohl klassische als auch erweiterte Richtlinienausdrücke. Derzeit kann der erweiterte Ausdruck Überwachungsprotokollrichtlinien nur an globale Systementitäten binden.

> **Hinweis**
>
> Wenn Sie eine Richtlinie an globale Entitäten binden, müssen Sie sie an eine globale Systementität desselben Ausdrucks binden. Beispielsweise können Sie eine klassische Richtlinie nicht an eine erweiterte globale Entität binden oder eine erweiterte Richtlinie an eine klassische globale Entität binden.
>
> Außerdem können Sie nicht sowohl klassische Überwachungsprotokollrichtlinien als auch erweiterte Überwachungsprotokollrichtlinien an einen virtuellen Lastausgleichsserver binden.

Konfigurieren von Überwachungsprotokollrichtlinien in einem klassischen Richtlinienausdruck

Das Konfigurieren der Audit-Protokollierung in der Classic-Richtlinie umfasst die folgenden Schritte:

1. **Konfigurieren einer Audit-Log-Aktion**. Sie können eine Überwachungsaktion für verschiedene Server und für verschiedene Protokollierungsstufen konfigurieren. “Audit-Aktion” beschreibt Konfigurationsinformationen des Überwachungsservers, während “Audit-Richtlinie” eine Bindungseinheit mit einer “Audit-Aktion” verknüpft. Standardmäßig verwenden SYSLOG und NSLOG nur TCP, um Protokollinformationen an die Protokollserver zu übertragen. TCP ist für die Übertragung vollständiger Daten zuverlässiger als UDP. Wenn Sie TCP für SYSLOG verwenden, können Sie das Pufferlimit auf der Citrix ADC-Appliance festlegen, um die Protokolle zu speichern. Danach werden die Protokolle an den SYSLOG-Server gesendet.
2. **Konfigurieren der Überwachungsprotokoll-Richtlinie**. Sie können entweder SYSLOG-Richtlinien konfigurieren, um Nachrichten auf einem SYSLOG-Server zu protokollieren, oder NSLOG-Richtlinien, um Nachrichten an einen NSLOG-Server zu protokollieren. Jede Richtlinie enthält eine Regel, die die zu protokollierenden Nachrichten identifiziert, und eine SYSLOG- oder NS-LOG-Aktion.
3. **Verbindliche Auditprotokoll-Richtlinien an globale Einheiten**. Sie müssen die Überwachungsprotokollrichtlinien global an globale Entitäten wie SYSTEM, VPN, Citrix ADC AAA usw. binden. Sie können dies tun, um die Protokollierung aller Citrix ADC-Systemereignisse zu aktivieren. Durch Definieren der Prioritätsstufe können Sie die Auswertungsreihenfolge für die Protokollierung des Audit-Servers festlegen. Priorität 0 ist die höchste und wird zuerst ausgewertet. Je höher die Prioritätszahl, desto niedriger ist die Priorität der Bewertung.

Jeder dieser Schritte wird in den folgenden Abschnitten erläutert.

Konfigurieren der Audit-Log-Aktion

Konfigurieren der SYSLOG-Aktion in der erweiterten Richtlinieninfrastruktur über die Befehlszeile.

> **Hinweis**
>
> Mit der Citrix ADC-Appliance können Sie nur eine SYSLOG-Aktion für die IP-Adresse und den Port des SYSLOG-Servers konfigurieren. Die Appliance erlaubt es Ihnen nicht, mehrere SYSLOG-Aktionen für dieselbe Server-IP-Adresse und denselben Port zu konfigurieren.

Eine Syslog-Aktion enthält einen Verweis auf einen Syslog-Server. Es gibt an, welche Informationen protokolliert werden sollen, und erwähnt, wie diese Informationen protokolliert werden sollen.

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

```
1 -  add audit syslogAction <name> <serverIP> [-serverPort <port>] -
     logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )] [-
     transport ( TCP | UDP )]`
```



```
2 -  show audit syslogAction [<name>]
3
4 <!--NeedCopy-->
```

So konfigurieren Sie die NSLOG-Aktion in der erweiterten Richtlinieninfrastruktur über die Befehlszeile

Eine ns-Protokollaktion enthält einen Verweis auf einen NSlog-Server. Es gibt an, welche Informationen protokolliert werden sollen, und erwähnt, wie diese Informationen protokolliert werden sollen.

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

```
1 -  add audit nslogAction <name> <serverIP> [-serverPort <port>] -
     logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )]
2 -  show audit nslogAction [<name>]
3 <!--NeedCopy-->
```

Konfigurieren von Audit-Log-Richtlinien

So konfigurieren Sie Audit-Log-Richtlinien in der klassischen Policy-Infrastruktur über die Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 -  add audit syslogpolicy <name> <-rule> <action>
2 -  add audit nslogpolicy <name> < rule> <action>rm audit nslogpolicy <
     name>show audit nslogpolicy [<name>]set audit nslogpolicy <name>  [-
     rule <expression>] [-action <name>]
3 <!--NeedCopy-->
```

Verbindliche Audit-Syslog-Richtlinien zur Prüfung von syslog global

So binden Sie die Auditlog-Richtlinie im Classic-Richtlinienframework über die Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind audit syslogGlobal <policyName> [-globalBindType <globalBindType
```

```
unbind audit syslogGlobal <policyName>[-globalBindType <globalBindType>]
```


Konfigurieren von Überwachungsprotokollrichtlinien mithilfe eines erweiterten Richtlinien

Das Konfigurieren der Audit-Protokollierung in der Advanced-Richtlinie umfasst die folgenden Schritte:

1. **Konfigurieren einer Audit-Log-Aktion**. Sie können eine Überwachungsaktion für verschiedene Server und für verschiedene Protokollierungsstufen konfigurieren. "Audit-Aktion" beschreibt Konfigurationsinformationen des Überwachungsservers, während "Audit-Richtlinie" eine Bindungseinheit mit einer "Audit-Aktion" verknüpft. Standardmäßig verwenden SYSLOG und NSLOG nur TCP, um Protokollinformationen an die Protokollserver zu übertragen. TCP ist für die Übertragung vollständiger Daten zuverlässiger als UDP. Wenn Sie TCP für SYSLOG verwenden, können Sie das Pufferlimit auf der Citrix ADC-Appliance festlegen, um die Protokolle zu speichern. Danach werden die Protokolle an den SYSLOG-Server gesendet.
2. **Konfigurieren der Überwachungsprotokoll-Richtlinie**. Sie können entweder SYSLOG-Richtlinien konfigurieren, um Nachrichten auf einem SYSLOG-Server zu protokollieren, oder NSLOG-Richtlinien, um Nachrichten an einen NSLOG-Server zu protokollieren. Jede Richtlinie enthält eine Regel, die die zu protokollierenden Nachrichten identifiziert, und eine SYSLOG- oder NS-LOG-Aktion.
3. **Verbindliche Auditprotokoll-Richtlinien an globale Einheiten**. Sie müssen die Überwachungsprotokollrichtlinien global an die globale System-Entität binden, um die Protokollierung aller Citrix ADC-Systemereignisse zu ermöglichen. Durch Definieren der Prioritätsstufe können Sie die Auswertungsreihenfolge für die Protokollierung des Audit-Servers festlegen. Priorität 0 ist die höchste und wird zuerst ausgewertet. Je höher die Prioritätszahl, desto niedriger ist die Priorität der Bewertung.

> **Hinweis**
>
> Die Citrix ADC-Appliance wertet alle Richtlinien aus, die an true gebunden sind.

Konfigurieren der Audit-Log-Aktion

So konfigurieren Sie die Syslog-Aktion in der erweiterten Richtlinieninfrastruktur über die Befehlszeile

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

```
1 - add audit syslogAction <name> <serverIP> [-serverPort <port>] -
    logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )] [-
    transport ( TCP | UDP )]
2 - show audit syslogAction [<name>]
```



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

So konfigurieren Sie die NSLOG-Aktion in der erweiterten Richtlinieninfrastruktur über die Befehlszeile

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

```
- add audit nslogAction <name> <serverIP> [-serverPort <port>] -
   logLevel <logLevel> [-dateFormat ( MMDDYYYY | DDMMYYYY )]
- show audit nslogAction [<name>]
<!--NeedCopy-->
```

Konfigurieren von Audit-Log-Richtlinien

So fügen Sie über die Befehlszeile eine Syslog-Überwachungsaktion hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
    add audit syslogAction <name> (<serverIP> | ((<serverDomainName>[-
       domainResolveRetry <integer>])
    | -lbVserverName <string>))[-serverPort <port>] -logLevel <logLevel
       >[-dateFormat <dateFormat>]
     [-logFacility <logFacility>][-tcp ( NONE | ALL )] [-acl ( ENABLED
        | DISABLED )]
    [-timeZone ( GMT_TIME | LOCAL_TIME )][-userDefinedAuditlog ( YES |
       NO )]
     [-appflowExport ( ENABLED | DISABLED )] [-lsn ( ENABLED | DISABLED
         )][-alg ( ENABLED | DISABLED )]
    [-subscriberLog ( ENABLED | DISABLED )][-transport ( TCP | UDP )]
       [-tcpProfileName <string>][-maxLogDataSizeToHold
<!--NeedCopy-->
```

Beispiel

```
    > add audit syslogaction audit-action1 10.102.1.1 -loglevel
       INFORMATIONAL -dateformat MMDDYYYY
    > add audit nslogAction nslog-action1 10.102.1.3 -serverport 520 -
       loglevel INFORMATIONAL -dateFormat MMDDYYYY
    > add audit syslogpolicy syslog-pol1 TRUE audit-action1
```



```
4       > add audit nslogPolicy nslog-pol1 TRUE nslog-action1
5       > bind system global nslog-pol1 -priority 20
6   <!--NeedCopy-->
```

So fügen Sie über die Befehlszeile eine nslog-Audit-Aktion hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1       add audit nslogAction <name> (<serverIP> | (<serverDomainName>[-
            domainResolveRetry <integer>])) [-serverPort <port>]       -
            logLevel <logLevel> ... [-dateFormat <dateFormat>][-logFacility
            <logFacility>] [-tcp ( NONE | ALL )][-acl ( ENABLED | DISABLED )
            ] [-timeZone ( GMT_TIME | LOCAL_TIME )][-userDefinedAuditlog (
            YES | NO )][-appflowExport ( ENABLED | DISABLED )] [-lsn (
            ENABLED | DISABLED )][-alg ( ENABLED | DISABLED )] [-
            subscriberLog ( ENABLED | DISABLED )]`
2   <!--NeedCopy-->
```

Verbindliche Auditprotokoll-Richtlinien an globale Einheiten

So binden Sie die Syslog-Auditlog-Richtlinie im erweiterten Richtlinienframework über die Befehlszeile

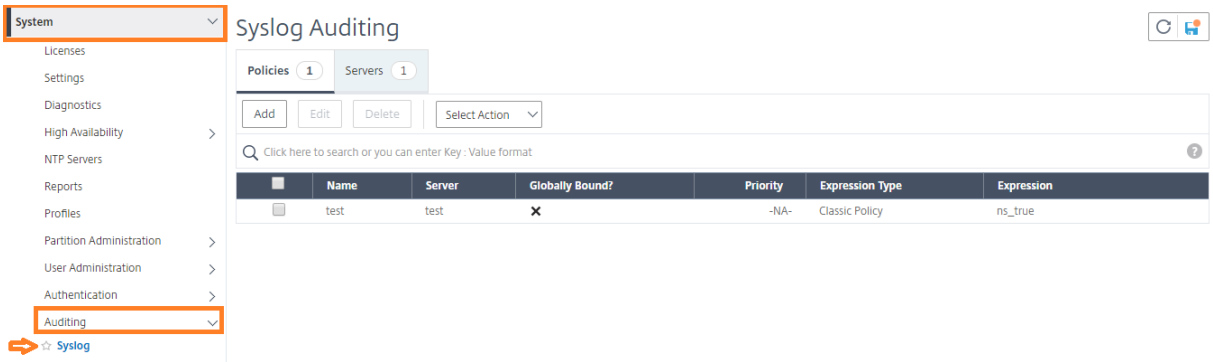
Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind audit syslogGlobal <policyName> [-globalBindType <globalBindType
```

```
unbind audit syslogGlobal <policyName>[-globalBindType <globalBindType>]
```

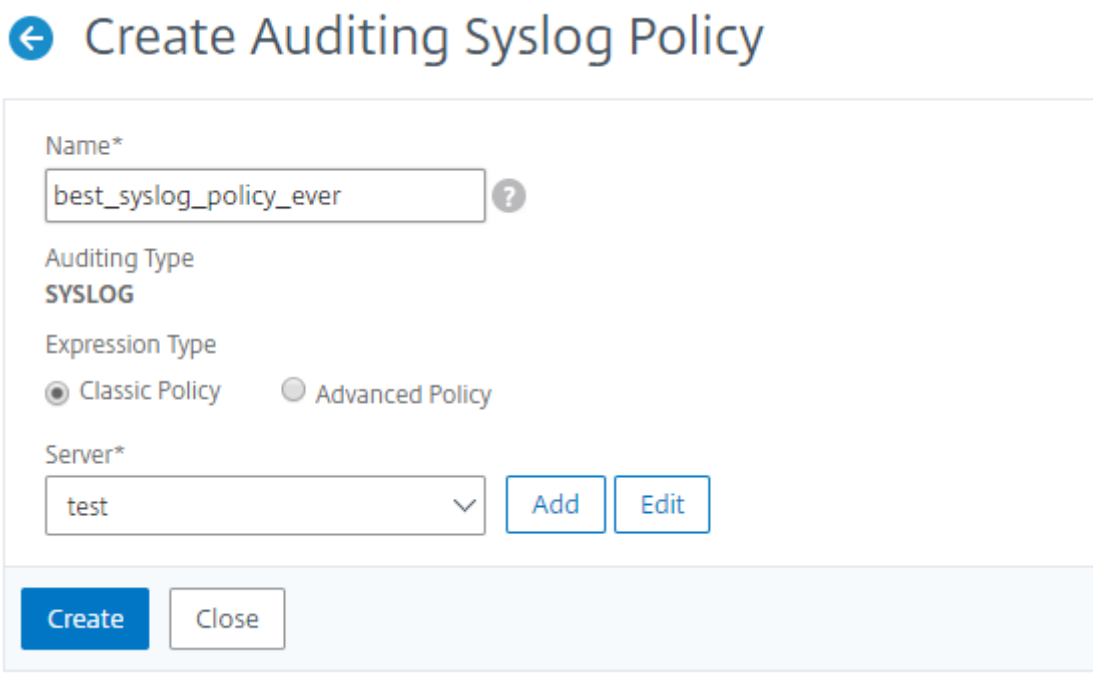
Konfigurieren der Überwachungsprotokollrichtlinie über die GUI

1. Navigieren Sie zu **Konfiguration** > **System** > **Auditing** > **Syslog**.



1. Wählen Sie **die Registerkarte Server** .

2. Klicken Sie auf **Hinzufügen**.
3. Füllen Sie auf der Seite **“Auditing Server erstellen** “ die entsprechenden Felder aus und klicken Sie auf **Erstellen**.
4. Um die Richtlinie hinzuzufügen, wählen Sie die Registerkarte **Richtlinien** aus und klicken Sie auf **Hinzufügen**.
5. Füllen **Sie auf der Seite “Auditing Syslog-Richtlinie** erstellen” die entsprechenden Felder aus und klicken Sie auf **Erstellen**.



6. Um die Richtlinie global zu binden, wählen Sie **Advanced Policy Globale Bindings** aus der Dropdownliste aus. Wählen Sie die Richtlinie **best_syslog_policy_ever** aus. Klicken Sie auf **Select**.
7. Wählen Sie in der Dropdownliste den Bindepunkt als **SYSTEM_GLOBAL** aus, klicken Sie auf **Binden**, und klicken Sie dann auf **Fertig**.

Konfigurieren der richtlinienbasierten Protokollierung

Sie können richtlinienbasierte Protokollierung für Rewrite- und Responder-Richtlinien konfigurieren. Überwachungsmeldungen werden dann in einem definierten Format protokolliert, wenn die Regel in einer Richtlinie auf TRUE ausgewertet wird. Um die richtlinienbasierte Protokollierung zu konfigurieren, konfigurieren Sie eine Überwachungsmeldungsaktion, die Standardsyntaxausdrücke verwendet, um das Format der Überwachungsmeldungen anzugeben. Und verknüpfen Sie die Aktion mit einer Richtlinie. Die Richtlinie kann entweder global oder an einen virtuellen Lastausgleich- oder Content Switching-Server gebunden sein. Sie können Audit-Message-Aktionen verwenden,

um Nachrichten auf verschiedenen Protokollierungsebenen zu protokollieren, entweder nur im Syslog-Format oder sowohl im Syslog- als auch im neuen nslog-Format.

Voraussetzungen

- Die Option Konfigurierbare Protokollmeldungen (UserDefinedAuditLog) ist für die Konfiguration des Überwachungsaktionsservers aktiviert, an den Sie die Protokolle in einem definierten Format senden möchten.
- Die zugehörige Prüfungsrichtlinie ist an das globale System gebunden.

Konfigurieren einer Aktion für Überwachungsnachrichten

Sie können Aktionen für Überwachungsnachrichten konfigurieren, um Nachrichten auf verschiedenen Protokollierungsebenen zu protokollieren, entweder nur im Syslog-Format oder sowohl im Syslog- als auch in neuen ns-Protokollformaten. Auditmeldungsaktionen verwenden Ausdrücke, um das Format der Auditmeldungen anzugeben.

So erstellen Sie eine Aktion für Überwachungsnachrichten über die Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add audit messageaction <name> <logLevel> <stringBuilderExpr> [-
     logtoNewnslog (YES|NO)] [-bypassSafetyCheck (YES|NO)]
2 <!--NeedCopy-->
```

```
1 add audit messageaction log-act1 CRITICAL '"Client:"+CLIENT.IP.SRC+"
     accessed "+HTTP.REQ.URL' -bypassSafetyCheck YES
2 <!--NeedCopy-->
```

So konfigurieren Sie eine Aktion für eine Überwachungsnachricht über die GUI

Navigieren Sie zu **System > Auditing > Nachrichtenaktionen**, und erstellen Sie die Aktion “Überwachungsnachricht”.

Aktion für Audit-Nachrichten an eine Richtlinie binden

Nachdem Sie eine Überwachungsnachrichtenaktion erstellt haben, müssen Sie sie an eine Rewrite- oder Responderrichtlinie binden. Weitere Informationen zum Binden von Protokollnachrichtenaktionen an eine Rewrite- oder Responder Policy finden Sie unter Rewrite oder Responder.

Installieren und Konfigurieren des NSLOG-Servers

October 5, 2021

Während der Installation wird die ausführbare Datei des NSLOG-Servers (auditserver) zusammen mit anderen Dateien installiert. Die ausführbare Datei auditserver enthält Optionen zum Ausführen mehrerer Aktionen auf dem NSLOG-Server, einschließlich Ausführen und Beenden des NSLOG-Servers. Darüber hinaus verwenden Sie die ausführbare Datei auditserver, um den NSLOG-Server mit den IP-Adressen der Citrix ADC Appliances zu konfigurieren, von denen der NSLOG-Server mit dem Sammeln von Protokollen beginnt. Konfigurationseinstellungen werden in der NSLOG-Server-Konfigurationsdatei (auditlog.conf) angewendet.

Anschließend starten Sie den NSLOG-Server, indem Sie die ausführbare Datei auditserver ausführen. Die NSLOG-Serverkonfiguration basiert auf den Einstellungen in der Konfigurationsdatei. Sie können die Protokollierung auf dem NSLOG-Serversystem weiter anpassen, indem Sie zusätzliche Änderungen an der NSLOG-Server-Konfigurationsdatei (auditlog.conf) vornehmen.

> **achtung**:
>
> Die Version des NSLOG-Serverpakets muss mit der des Citrix ADC übereinstimmen. Wenn beispielsweise die Version des Citrix ADC 10.1 Build 125.9 lautet, muss der NSLOG-Server ebenfalls dieselbe Version haben.

In der folgenden Tabelle sind die Betriebssysteme aufgeführt, auf denen der NSLOG-Server unterstützt wird.

Betriebssystem	Softwareanforderungen	Bemerkungen
Windows	Windows XP Professional, Windows Server 2003, Windows 2000/NT, Windows Server 2008, Windows Server 2008 R2	
Linux	RedHat Linux 4 oder höher, SUSE Linux Enterprise 9.3 oder höher	
FreeBSD	FreeBSD 6.3 oder höher	Verwenden Sie für Citrix ADC 10.5 nur FreeBSD 8.4.
Mac OS	Mac OS 8.6 oder höher	Wird in Citrix ADC 10.1 und höheren Versionen nicht unterstützt.

Die Hardwarespezifikationen für die Plattform, auf der der NSLOG-Server ausgeführt wird, lauten wie folgt:

- Prozessor - Intel x86 ~ 501 Megahertz (MHz)
- RAM - 512 Megabyte (MB)
- Steuerung - SCSI

Installieren des NSLOG-Servers auf dem Linux-Betriebssystem

Melden Sie sich als Administrator am Linux-System an. Gehen Sie folgendermaßen vor, um die ausführbaren Dateien des NSLOG-Servers auf dem System zu installieren.

So installieren Sie das NSLOG-Serverpaket unter einem Linux-Betriebssystem

1. Geben Sie an einer Linux-Eingabeaufforderung den folgenden Befehl ein, um die Datei NSauditserver.rpm in ein temporäres Verzeichnis zu kopieren:

   ```
   cp <path_to_cd>/Utilities/auditserver/Linux/NSauditserver.rpm /tmp
   ```

2. Geben Sie den folgenden Befehl ein, um die Datei NsauditServer.rpm zu installieren.

   rpm -i NSauditserver.rpm

   Dieser Befehl extrahiert die Dateien und installiert sie in den folgenden Verzeichnissen:

   - /usr/local/netscaler/etc
   - /usr/local/netscaler/bin
   - /usr/local/netscaler/samples

So deinstallieren Sie das NSLOG-Serverpaket unter einem Linux-Betriebssystem

1. Geben Sie an einer Eingabeaufforderung den folgenden Befehl ein, um das Überwachungsserverprotokollierungsfeature zu deinstallieren:

   ```
   rpm -e NSauditserver
   ```

2. Weitere Informationen über die NSauditServer RPM-Datei finden Sie mit dem folgenden Befehl:

   ```
   rpm -qpi \*.rpm
   ```

3. Verwenden Sie den folgenden Befehl, um die installierten Überwachungsserverdateien anzuzeigen:

   ```
   rpm -qpl *.rpm
   ```

   `*.rpm`: Gibt den Dateinamen an.

Installieren des NSLOG-Servers auf dem FreeBSD-Betriebssystem

Bevor Sie den NSLOG-Server installieren können, müssen Sie das NSLOG-Paket von der Citrix ADC Produkt-CD kopieren oder von www.citrix.comherunterladen. Das NSLOG-Paket hat das folgende Namensformat:

`AuditServer_<release number>-<build number>.zip`

Beispiel: `AuditServer_10.5-58.11.zip`

Dieses Paket enthält Dateien für alle unterstützten Plattformen: Linux, Windows und FreeBSD. Installieren Sie unter einem FreeBSD-Betriebssystem das NSLOG-Paket mit folgendem Namensformat:

`audserver_bsd-<release number>-<build number>.tgz`

Beispiel: `audserver_bsd-10.5-58.11.tgz`

So laden Sie das NSLOG-Paket von www.citrix.com herunter:

1. Gehen Sie in einem Webbrowser zu www.citrix.com.
2. Klicken Sie in der Menüleiste auf **Anmelden**.
3. Geben Sie Ihre Anmeldedaten ein und klicken Sie dann auf **Anmelden**.
4. Klicken Sie in der Menüleiste auf " **Downloads**".
5. **Wählen Sie in der Liste Produkt** auswählen die Option **Citrix ADC** aus.
6. Wählen Sie auf der Seite **Citrix ADC** die Version aus, für die Sie das NSLOG-Paket herunterladen möchten (z. B. Release 10.5), wählen **Firmware**.
7. Wählen Sie unter **Firmware**die Citrix ADC Firmware für die Build-Nummer aus, für die Sie das NSLOG-Paket herunterladen möchten.
8. Führen Sie auf der angezeigten Seite einen Bildlauf nach unten aus, wählen Sie **Überwachungsserver**aus, und klicken Sie neben dem Paket, das Sie herunterladen möchten, auf **Datei**herunterladen.

So installieren Sie das NSLOG-Serverpaket auf einem FreeBSD-Betriebssystem

1. Entpacken Sie auf dem System,`AuditServer_<release number>-<build number>.zip` auf das Sie das NSLOG-Paket`AuditServer_9.3-51.5.zip` heruntergeladen haben`FreeBSD NSLOG server package audserver_bsd-<release number>-<build number>.tgz` (z. B.`audserver_bsd-9.3-51.5.tgz`) aus dem Paket.
2. Kopieren Sie das FreeBSD NSLOG-Serverpaket`audserver_bsd-<release number>-<build number>.tgz` (z. B.`audserver_bsd-9.3-51.5.tgz`) in ein Verzeichnis auf einem System, auf dem FreeBSD OS ausgeführt wird.
3. Führen Sie an einer Eingabeaufforderung für das Verzeichnis aus, in das das FreeBSD NSLOG-Serverpaket kopiert wurde, den folgenden Befehl aus, um das Paket zu installieren:

   `pkg_add audserver_bsd-<release number>-<build number>.tgz`

   Beispiel:


```
pkg_add audserver_bsd-9.3-51.5.tgz
<!--NeedCopy-->
```

Die folgenden Verzeichnisse werden extrahiert:

- <root directory extracted from the FreeBSD NSLOG server **package** tgz file>Citrix ADCbin (zum Beispiel /var/auditserver/netscaler/bin)
- <root directory extracted from the FreeBSD NSLOG server **package** tgz file>netscaler/etc (zum Beispiel /var/auditserver/netscaler/etc)
- <root directory extracted from the FreeBSD NSLOG server **package** tgz file>\netscaler\samples (zum Beispiel /var/auditserver/samples)

4. Geben Sie an einer Eingabeaufforderung den folgenden Befehl ein, um zu überprüfen, ob das Paket installiert ist:

   ```
   pkg_info | grep NSaudserver
   ```

So deinstallieren Sie das NSLOG-Serverpaket unter einem FreeBSD-Betriebssystem

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
pkg_delete NSaudserver
```

Installieren von NSLOG-Serverdateien auf dem Windows-Betriebssystem

Bevor Sie den NSLOG-Server installieren können, müssen Sie das NSLOG-Paket von der Citrix ADC Produkt-CD kopieren oder von www.citrix.comherunterladen. Das NSLOG-Paket hat das folgende Namensformat AuditServer _<release number>-<build number>.zip (z. B. AuditServer_9.3-51.5.zip). Dieses Paket enthält NSLOG-Installationspakete für alle unterstützten Plattformen.

So laden Sie das NSLOG-Paket von www.citrix.com herunter

1. Gehen Sie in einem Webbrowser zu www.citrix.com.
2. Klicken Sie in der Menüleiste auf Anmelden.
3. Geben Sie Ihre Anmeldedaten ein und klicken Sie dann auf Anmelden.
4. Klicken Sie in der Menüleiste auf “ Downloads”.
5. Suchen Sie nach der Seite, die die entsprechende Release-Nummer und den Build enthält.
6. Klicken Sie auf dieser Seite unter Überwachungsserver auf Herunterladen, um das NSLOG-Paket mit dem Format AuditServer_<release number>-<build number>.zip auf Ihr lokales System herunterzuladen (z. B. AuditServer_9.3-51.5.zip).

So installieren Sie den NSLOG-Server unter einem Windows-Betriebssystem

1. Auf dem System, wo Sie das NSLOG-Paket heruntergeladen habenAuditServer_<release number>-<build number>.zip (zum BeispielAuditServer_9.3-51.5.zip), extrahieren Sieaudserver_win-<release number>-<build number>.zip (zum Beispielaudserver_win-9.3-51.5.zip) aus das Paket.
2. Kopieren Sie die extrahierte Datei audserver_<release number>-<build number>.zip (z. B. audserver_win-9.3-51.5.zip) in ein Windows-System, auf dem Sie den NSLOG-Server installieren möchten.
3. Entpacken Sie die audserver_<release number>-<build number>.zip Datei (z. B. audserver_win-9.3-51.5.zip).
4. Die folgenden Verzeichnisse werden extrahiert:
   a) <root directory extracted from the Windows NSLOG server **package** zip file>\bin(zum Beispiel C:\audserver_win-9.3-51.5\bin)
   b) <root directory extracted from the Windows NSLOG server **package** zip file>\etc(zum Beispiel C:\audserver_win-9.3-51.5\etc)
   c) <root directory extracted from the Windows NSLOG server **package** zip file>\samples (zum Beispiel C:\audserver_win-9.3-51.5\samples)
5. Führen Sie an einer Eingabeaufforderung den folgenden Befehl aus der<root directory extracted from the Windows NSLOG server **package** zip file>\bin path

   ```
   audserver -install -f <directorypath>\auditlog.conf
   ```

   <directorypath>: Gibt den Pfad zur Konfigurationsdatei an (auditlog.conf). Standardmäßiglog.conf ist unter\<root directory extracted from Windows NSLOG server **package** zip file\>\samples Verzeichnis. Aber Sie können auditlog.conf in Ihr gewünschtes Verzeichnis kopieren.

So deinstallieren Sie den NSLOG-Server unter einem Windows-Betriebssystem

Führen Sie an einer Eingabeaufforderung den folgenden<root directory extracted from Windows NSLOG server **package** zip file>\bin Pfad aus:

```
audserver -remove
```

NSLOG-Server-Befehlsoptionen

Informationen zu NSLOG-Serverbefehlen finden Sie unter Audit-Server-Optionen.

Führen Sie den Befehl audserver aus dem Verzeichnis aus, in dem die ausführbare Datei des Auditservers vorhanden ist:

- Unter Windows:\ns\bin
- Unter Solaris und Linux:\usr\local\netscaler\bin

Die Überwachungsserver-Konfigurationsdateien befinden sich in den folgenden Verzeichnissen:

- Unter Windows:\ns\etc
- Unter Linux:\usr\local\netscaler\etc

Die ausführbare Datei des Audit-Servers wird wie ./auditserver unter Linux und FreeBSD gestartet.

Hinzufügen der IP-Adressen der Citrix ADC Appliance auf dem NSLOG-Server

Fügen Sie in der Konfigurationsdatei (
auditlog.conf) die IP-Adressen der Citrix ADC Appliances hinzu, deren Ereignisse protokolliert werden müssen.

So fügen Sie die IP-Adressen der Citrix ADC Appliance hinzu

Geben Sie an einer Eingabeaufforderung den folgenden Befehl ein:

```
audserver -addns -f <directorypath\>\auditlog.conf
```

<directorypath>: Gibt den Pfad zur Konfigurationsdatei an (auditlog.conf).

Sie werden aufgefordert, die Informationen für die folgenden Parameter einzugeben:

NSIP: Gibt die IP-Adresse der Citrix ADC Appliance an, z. B. 10.102.29.1.

Benutzer-ID: Gibt den Benutzernamen an, z. B. nsroot.

Kennwort: Gibt das Kennwort an, z. B. nsroot.

Wenn Sie mehrere Citrix ADC IP-Adressen (NSIP) hinzufügen und später nicht alle Ereignisdetails der Citrix ADC-Appliance protokollieren möchten, können Sie die NSIPs manuell löschen, indem Sie die NSIP-Anweisung am Ende der Datei auditlog.conf entfernen. Für ein Hochverfügbarkeit-Setup (HA) müssen Sie mit dem Befehl audserver sowohl primäre als auch sekundäre Citrix ADC IP-Adressen zu auditlog.conf hinzufügen. Bevor Sie die IP-Adresse hinzufügen, stellen Sie sicher, dass der Benutzername und das Kennwort auf dem System vorhanden sind.

Überprüfen der NSLOG-Server-Konfigurationsdatei

Überprüfen Sie die Konfigurationsdatei (audit log.conf) auf Korrektheit der Syntax, um die Protokollierung zu starten und korrekt zu funktionieren.

Um die Konfiguration zu überprüfen, geben Sie an einer Eingabeaufforderung den folgenden Befehl ein:

```
audserver -verify -f <directorypath>\auditlog.conf
```


<directorypath>: Specifies the path to the configuration file (audit log.conf).

Ausführen des NSLOG-Servers

October 5, 2021

So starten Sie die Protokollierung des Überwachungsservers

Geben Sie den folgenden Befehl an einer Eingabeaufforderung ein:

Audserver -start -f<directorypath>\auditlog.conf

<directorypath>: Gibt den Pfad zur Konfigurationsdatei an (audit log.conf).

So beenden Sie die Protokollierung von Überwachungs-Servern, die als Hintergrundprozess in FreeBSD oder Linux gestartet werden

Geben Sie den folgenden Befehl ein:

```
audserver -stop
```

So beenden Sie die Überwachungsserverprotokollierung, die als Dienst in Windows gestartet wird

Geben Sie den folgenden Befehl ein:

```
audserver -stopservice
```

Anpassen der Protokollierung auf dem NSLOG-Server

October 5, 2021

Sie können die Protokollierung auf dem NSLOG-Server anpassen, indem Sie zusätzliche Änderungen an der NSLOG-Server-Konfigurationsdatei (log.conf) vornehmen. Verwenden Sie einen Texteditor, um die Konfigurationsdatei log.conf auf dem Serversystem zu ändern.

Zum Anpassen der Protokollierung verwenden Sie die Konfigurationsdatei, um Filter und Protokolleigenschaften zu definieren.

- **Protokollfilter.** Filtern Sie Protokollinformationen von einer Citrix ADC Appliance oder einer Gruppe von Citrix ADC-Appliances.
- **Protokollierungseigenschaften.** Jeder Filter verfügt über einen Satz von Protokolleigenschaften. Die Protokolleigenschaften legen fest, wie die gefilterten Protokollinformationen gespeichert werden.

Dieses Dokument enthält die folgenden Details:

- Erstellen von Filtern
- Protokolleigenschaften angeben

Erstellen von Filtern

Sie können die Standardfilterdefinition in der Konfigurationsdatei (audit log.conf) verwenden, oder Sie können den Filter ändern oder einen neuen Filter erstellen. Sie können mehrere Protokollfilter erstellen.

> Hinweis: Wenn
> bei der konsolidierten Protokollierung eine Protokolltransaktion auftritt, für die keine Filterdefinition vorhanden ist, wird der Standardfilter verwendet (sofern diese aktiviert ist). Die einzige Möglichkeit, die konsolidierte Protokollierung aller Citrix ADC Appliances zu konfigurieren, besteht darin, den Standardfilter zu definieren.

So erstellen Sie einen Filter

Geben Sie an der Eingabeaufforderung den folgenden Befehl in die Konfigurationsdatei ein (auditlog.conf):

```
filter <filterName> [IP <ip>] [NETMASK <mask>] ON | OFF]
<!--NeedCopy-->
```

FilterName: Geben Sie den Namen des Filters an (maximal 64 alphanumerische Zeichen).

ip: Geben Sie die IP-Adressen an.

mask: Geben Sie die Subnetzmaske an, die in einem Subnetz verwendet werden soll.

Geben Sie ON an, damit der Filter Transaktionen protokollieren kann, oder geben Sie OFF an, um den Filter zu deaktivieren. Wenn kein Argument angegeben wird, ist der Filter ON.

Beispiele:


```
filter F1 IP 192.168.100.151 ON
<!--NeedCopy-->
```

So wenden Sie den Filter F2 auf IP-Adressen 192.250.100.1 bis 192.250.100.254 an:

```
filter F2 IP 192.250.100.0 NETMASK 255.255.255.0 ON
<!--NeedCopy-->
```

FilterName ist ein erforderlicher Parameter, wenn Sie einen Filter mit anderen optionalen Parametern wie IP-Adresse oder der Kombination aus IP-Adresse und Netzmaske definieren.

Festlegen von Protokolleigenschaften

Mit dem Filter verknüpfte Protokolleigenschaften werden auf alle im Filter vorhandenen Protokolleinträge angewendet. Die Definition der Log -Eigenschaft beginnt mit dem Schlüsselwort BEGIN und endet mit END, wie im folgenden Beispiel dargestellt:

```
BEGIN <filtername>
    logFilenameFormat ...
    logDirectory ...
    logInterval ...
    logFileSizeLimit ....
END
<!--NeedCopy-->
```

Einträge in der Definition können Folgendes umfassen:

- **LogFilenameFormat** gibt das Dateinamenformat der Protokolldatei an. Der Name der Datei kann von den folgenden Typen sein:
  - Statisch: Eine konstante Zeichenfolge, die den absoluten Pfad und den Dateinamen angibt.
  - Dynamisch: Ein Ausdruck, der die folgenden Formatbezeichner enthält:
    - Datum (% {format} t)
    - erstellt Dateinamen mit NSIP

  Beispiel:

```
LogFileNameFormat Ex%`{
`%m%d%y }
```



```
t.log
<!--NeedCopy-->
```

Dadurch wird der erste Dateiname als exmmddyy.log erstellt. Neue Dateien werden benannt: exmmddyy.log.0, exmmddyy.log.1 usw. Im folgenden Beispiel werden die neuen Dateien erstellt, wenn die Dateigröße 100 MB erreicht.

Beispiel:

```
LogInterval size
LogFileSize 100
LogFileNameFormat Ex%`{
`%m%d%y }
t
<!--NeedCopy-->
```

> **Achtung**
>
> Das im Parameter LogFileNameFormat angegebene Datumsformat%t überschreibt die Protokollintervall-Eigenschaft für diesen Filter. Verwenden Sie nicht im Parameter LogFileNameFormat, um zu verhindern, dass täglich eine neue Datei erstellt wird, anstatt die angegebene Protokolldateigröße erreicht wird.

- **LogDirectory** gibt das Verzeichnisnamenformat der Protokolldatei an. Der Name der Datei kann eine der folgenden sein:
  - Statisch: Ist eine konstante Zeichenfolge, die den absoluten Pfad und Dateinamen angibt.
  - Dynamisch: Ist ein Ausdruck, der die folgenden Formatbezeichner enthält:
    - Datum (% {format} t)
    - erstellt ein Verzeichnis mit NSIP

  Das Verzeichnistrennzeichen hängt vom Betriebssystem ab. Verwenden Sie unter Windows das Verzeichnistrennzeichen.

  Beispiel:

```
LogDirectory dir1\dir2\dir3
<!--NeedCopy-->
```

  Verwenden Sie in den anderen Betriebssystemen (Linux, FreeBSD usw.) das Verzeichnistrennzeichen.

- **LogInterval** gibt das Intervall an, in dem neue Protokolldateien erstellt werden. Verwenden Sie einen der folgenden Werte:

- Stündlich: Jede Stunde wird eine Datei erstellt. Standardwert.
- Täglich: Eine Datei wird sehr Tag um Mitternacht erstellt.
- Wöchentlich: Jeden Sonntag um Mitternacht wird eine Datei erstellt.
- Monatlich: Eine Datei wird am ersten Tag des Monats um Mitternacht erstellt.
- Keine: Eine Datei wird nur einmal erstellt, wenn die Protokollierung des Überwachungsservers gestartet wird.
- Größe: Eine Datei wird nur erstellt, wenn die Größe der Protokolldatei erreicht ist.

Beispiel:

```
LogInterval Hourly
<!--NeedCopy-->
```

- **LogFileSizeLimit** gibt die maximale Größe (in MB) der Protokolldatei an. Eine neue Datei wird erstellt, wenn das Limit erreicht ist.

> **Hinweis:**
>
> Sie können die logintervall-Eigenschaft überschreiben, indem Sie Größe als Wert zuweisen.

Die Standardeinstellung LogFileSizeLimit ist 10 MB.

Beispiel:

```
LogFileSizeLimit 35
<!--NeedCopy-->
```

SYSLOG über TCP

October 5, 2021

Syslog ist ein Standard für das Senden von Ereignisbenachrichtigungen. Diese Meldungen können lokal oder auf einem externen Protokollserver gespeichert werden. Mit Syslog können Netzwerkadministratoren Protokollmeldungen konsolidieren und Erkenntnisse aus den gesammelten Daten ableiten.

Syslog wurde ursprünglich für die Arbeit über UDP entwickelt, das eine große Menge an Daten innerhalb desselben Netzwerks mit minimalem Paketverlust übertragen kann. Telekommunikationsbetreiber ziehen es jedoch vor, Syslog-Daten über TCP zu übertragen, da sie eine zuverlässige, geord-

nete Datenübertragung zwischen Netzwerken benötigen. Beispielsweise verfolgt Telco Benutzeraktivitäten, und TCP bietet eine erneute Übertragung im Falle eines Netzwerkausfalls.

Funktionsweise von Syslog über TCP

Um zu verstehen, wie Syslog über TCP funktioniert, betrachten Sie zwei hypothetische Fälle:

Sam, ein Netzwerkadministrator, möchte wichtige Ereignisse auf einem externen Syslog-Server protokollieren.

XYZ Telecom, ein ISP, muss eine beträchtliche Menge an Daten auf Syslog-Servern übertragen und speichern, um den staatlichen Vorschriften zu entsprechen.

In beiden Fällen müssen die Protokollmeldungen über einen zuverlässigen Kanal übertragen und sicher auf einem externen Syslog-Server gespeichert werden. Im Gegensatz zu UDP stellt TCP eine Verbindung her, überträgt Nachrichten sicher und überträgt (vom Sender zum Empfänger) alle Daten, die aufgrund eines Netzwerkausfalls beschädigt oder verloren gegangen sind.

Die Citrix ADC Appliance sendet Protokollmeldungen über UDP an den lokalen Syslog-Daemon und sendet Protokollmeldungen über TCP oder UDP an externe Syslog-Server.

SNIP-Unterstützung für Syslog

Wenn das Audit-Log-Modul Syslog-Nachrichten generiert, verwendet es eine Citrix ADC IP (NSIP) -Adresse als Quelladresse für das Senden der Nachrichten an einen externen Syslog-Server. Um ein SNIP als Quelladresse zu konfigurieren, müssen Sie es Teil der NetProfile-Option machen und NetProfile an die syslog-Aktion binden.

> **Hinweis**
>
> TCP verwendet SNIP zum Senden von Überwachungsprüfern, um die Konnektivität zu überprüfen, und sendet dann die Protokolle über NSIP. Daher muss der Syslog-Server über SNIP erreichbar sein. Net-Profile können verwendet werden, um den gesamten TCP-Syslog-Verkehr vollständig über SNIP umzuleiten.

Die Verwendung einer SNIP-Adresse wird in der internen Protokollierung nicht unterstützt.

Vollständig qualifizierter Domainname Unterstützung für Audit-Lo

Zuvor wurde das Überwachungsprotokollmodul mit der Ziel-IP-Adresse des externen Syslog-Servers konfiguriert, an den die Protokollmeldungen gesendet werden. Jetzt verwendet der Audit-Log-Server einen vollqualifizierten Domänennamen (FQDN) anstelle der Ziel-IP-Adresse. Die FQDN-Konfiguration löst den konfigurierten Domänennamen des syslog-Servers in die entsprechende Ziel-IP-Adresse für das Senden der Protokollmeldungen aus dem Audit-Protokollmodul auf. Der Nameserver

muss ordnungsgemäß konfiguriert sein, um den Domänennamen zu lösen und Probleme mit domänenbasierten Diensten zu vermeiden.

> **Hinweis:**
>
> Bei der Konfiguration eines FQDN wird die Konfiguration des Serverdomänennamens derselben Citrix ADC Appliance in Syslog-Aktion oder NSlog-Aktion nicht unterstützt.

Konfigurieren von Syslog über TCP über die Befehlszeile

So konfigurieren Sie eine Citrix ADC Appliance zum Senden von Syslog-Nachrichten über TCP mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1     add audit syslogAction <name> (<serverIP> | ((<serverDomainName>[-
          domainResolveRetry <integer>]) | -lbVserverName<string>))[-
          serverPort <port>] -logLevel <logLevel>[-dateFormat <dateFormat
          >] [-logFacility <logFacility>]   [-tcp ( NONE | ALL )] [-acl (
          ENABLED | DISABLED )][-timeZone ( GMT_TIME | LOCAL_TIME )][-
          userDefinedAuditlog ( YES | NO )][-appflowExport ( ENABLED |
          DISABLED )] [-lsn ( ENABLED | DISABLED )][-alg ( ENABLED |
          DISABLED )] [-subscriberLog ( ENABLED | DISABLED )][-transport (
           TCP | UDP )] [-tcpProfileName <string>][-maxLogDataSizeToHold <
          positive_integer>][-dns ( ENABLED | DISABLED )] [-netProfile <
          string>]
2 <!--NeedCopy-->
```

```
1     add audit syslogaction audit-action1 10.102.1.1 -loglevel
          INFORMATIONAL -dateformat MMDDYYYY -transport TCP
2 <!--NeedCopy-->
```

Hinzufügen der SNIP-IP-Adresse zur Net-Profiloption über die Befehlszeile

So fügen Sie dem Netzprofil über die Befehlszeile eine SNIP-IP-Adresse hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
1     add netProfile <name> [-td <positive_integer>] [-srcIP <string>][-
          srcippersistency ( ENABLED | DISABLED )][-overrideLsn ( ENABLED
          | DISABLED )]add syslogaction <name> <serverIP>  -loglevel all
          -netprofile net1
2 <!--NeedCopy-->
```

```
1     add netprofile net1  -srcip 10.102.147.204`
2 <!--NeedCopy-->
```

Wobei, srcIP die SNIP ist.

Hinzufügen des Netzprofils in einer Syslog-Aktion über die Befehlszeile

So fügen Sie eine NetProfile-Option in einer Syslog-Aktion mit der Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1      add audit syslogaction <name> (<serverIP> | -lbVserverName <string
           >)  -logLevel <logLevel>
2     -netProfile <string> …
3
4 <!--NeedCopy-->
```

```
1     add syslogaction sys_act1 10.102.147.36  -loglevel all  -netprofile
          net1
2 <!--NeedCopy-->
```

Wo, -netprofile gibt den Namen des konfigurierten Netzprofils an. Die SNIP-Adresse wird als Teil des NetProfile konfiguriert, und diese NetProfile-Option ist an die syslog-Aktion gebunden.

> **Hinweis:**
>
> Sie müssen die NetProfile-Option immer an die SYSLOGUDP- oder SYSLOGTCP-Dienste binden, die an den virtuellen Lastausgleichsserver SYSLOGUDP oder SYSLOGTCP gebunden sind, wenn ein virtueller LB-Servername in der Syslog-Aktion konfiguriert ist.

Konfigurieren der FQDN-Unterstützung mit der Befehlszeilenschnittstelle

So fügen Sie einer Syslog-Aktion mit der Befehlszeilenschnittstelle einen Serverdomänennamen hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add audit syslogAction <name> (<serverIP> | ((<serverDomainName>[-
     domainResolveRetry <integer>]) | -lbVserverName <string>)) -logLevel
      <logLevel> ...
2     set audit syslogAction <name> [-serverIP <ip_addr|ipv6_addr|*>]-
        serverDomainName <string>] [-lbVserverName <string>]-
        domainResolveRetry <integer>] [-domainResolveNow]
3 <!--NeedCopy-->
```

So fügen Sie einer Nslog-Aktion mit der Befehlszeilenschnittstelle einen Serverdomänennamen hinzu.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1     add audit nslogAction <name> (<serverIP> | (<serverDomainName>[-
        domainResolveRetry <integer>]))  -logLevel <logLevel> ...
2     set audit nslogAction <name> [-serverIP <ip_addr|ipv6_addr|*>][-
        serverDomainName <string>] [-domainResolveRetry <integer>][-
        domainResolveNow]
3 <!--NeedCopy-->
```

Wo ServerDomainName. Domänenname des Protokollservers. Exklusiv sich gegenseitig mit ServerIP/ lbvServerName.

DomainResolveRetry (Ganzzahl). Zeit (in Sekunden), die die Citrix ADC Appliance nach einem Fehlschlagen einer DNS-Auflösung wartet, bevor die nächste DNS-Abfrage zum Auflösen des Domänennamens gesendet wird.

DomainResolveNow. Eingeschlossen, wenn die DNS-Abfrage sofort gesendet werden muss, um den Domänennamen des Servers aufzulösen.

Konfigurieren von Syslog über TCP mit der GUI

So konfigurieren Sie die Citrix ADC Appliance für das Senden von Syslog-Nachrichten über TCP mit der GUI

1. Navigieren Sie zu **System** > **Auditing** > **Syslog** und wählen Sie die Registerkarte **Servers**.
2. Klicken Sie auf **Hinzufügen** und wählen Sie Transportart als **TCP** aus.

Konfigurieren eines Netzprofils für die SNIP-Unterstützung mit der GUI

So konfigurieren Sie das Netzprofil für die SNIP-Unterstützung über die GUI

1. Navigieren Sie zu **System > Auditing > Syslog** und wählen Sie die Registerkarte **Server** aus.
2. Klicken Sie auf **Hinzufügen**, und wählen Sie ein Netzprofil aus der Liste aus.

Konfigurieren des FQDN mit der GUI

So konfigurieren Sie den FQDN mit der GUI

1. Navigieren Sie zu **System** > **Auditing** > **Syslog** und wählen Sie die Registerkarte **Servers**.
2. Klicken Sie auf **Hinzufügen**, und wählen Sie einen Servertyp und einen Serverdomänennamen aus der Liste aus.

SYSLOG-Server mit Lastenausgleich

September 1, 2022

Die Citrix ADC Appliance sendet ihre SYSLOG-Ereignisse und -Meldungen an alle konfigurierten externen Protokollserver. Dies führt zur Speicherung redundanter Nachrichten und erschwert die Überwachung für Systemadministratoren. Um dieses Problem zu beheben, bietet die Citrix ADC Appliance Lastausgleichsalgorithmen, mit denen die SYSLOG-Meldungen für eine bessere Wartung und Leistung zwischen den externen Protokollservern ausgeglichen werden können. Zu den unterstützten Lastausgleichsalgorithmen gehören RoundRobin, LeastBandwidth, CustomLoad, LeastConnection, LeastPackets und AuditlogHash.

Load-Balancing von SYSLOG-Servern über die Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

1. Fügen Sie einen Dienst hinzu und geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGUDP an.

   ```
   add service <name>(<IP> | <serverName>)<serviceType (SYSLOGTCP |
   SYSLOGUDP)> <port>
   ```

2. Fügen Sie einen virtuellen Lastausgleichsserver hinzu, geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGUDP und die Lastausgleichsmethode als AUDITLOGHASH an.

   ```
   add lb vserver <name> <serviceType (SYSLOGTCP | SYSLOGUDP)> [-lbMethod
   <AUDITLOGHASH>]
   ```

3. Binden Sie den Dienst an den virtuellen Lastausgleichsserver.

   ```
   Bind lb vserver <name> <serviceName>
   ```

4. Fügen Sie eine SYSLOG-Aktion hinzu und geben Sie den Namen des Load Balancing-Servers an, der SYSLOGTCP oder SYSLOGUDP als Diensttyp hat.

   ```
   add syslogaction <name> <serverIP> [-lbVserverName <string>] [-logLevel
    <logLevel>]
   ```


5. Fügen Sie eine SYSLOG-Richtlinie hinzu, indem Sie die Regel und Aktion angeben.

   ```
   add syslogpolicy <name> <rule> <action>
   ```

6. Binden Sie die SYSLOG-Richtlinie an das globale System, damit die Richtlinie wirksam wird.

   ```
   bind system global <policyName>
   ```

Load-Balancing von SYSLOG-Servern über die GUI

1. Fügen Sie einen Dienst hinzu und geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGUDP an.

   Navigieren Sie zu **Traffic Management** > **Services**, klicken Sie auf **Hinzufügen** und wählen Sie **SYLOGTCP** oder **SYSLOGUDP** als Protokoll aus.

2. Fügen Sie einen virtuellen Lastausgleichsserver hinzu, geben Sie den Diensttyp als SYSLOGTCP oder SYSLOGTCP und die Lastausgleichsmethode als AUDITLOGHASH an.

   Navigieren Sie zu **Traffic Management** > **Virtuelle Server**, klicken Sie auf **Hinzufügen** und wählen Sie **SYLOGTCP** oder **SYSLOGUDP** als Protokoll aus.

3. Binden Sie den Dienst an den virtuellen Lastausgleichsserver.

   Navigieren Sie zu **Traffic Management** > **Virtuelle Server**, wählen Sie einen virtuellen Server aus und wählen Sie dann **AUDITLOGHASH in der LoadBalancing-Methode**

4. Fügen Sie eine SYSLOG-Aktion hinzu und geben Sie den Namen des Load Balancing-Servers an, der SYSLOGTCP oder SYSLOGUDP als Diensttyp hat.

   Navigieren Sie zu **System** > **Überwachung**, klicken Sie auf **Server** und fügen Sie einen Server hinzu, indem Sie unter **Server** die Option **LB Vserver** auswählen.

5. Fügen Sie eine SYSLOG-Richtlinie hinzu, indem Sie die Regel und Aktion angeben.

   Navigieren Sie zu **System** > **Syslog**, klicken Sie auf **Richtlinien**, und fügen Sie eine SYSLOG-Richtlinie hinzu.

6. Binden Sie die SYSLOG-Richtlinie an das globale System, damit die Richtlinie wirksam wird.

   Navigieren Sie zu **System** > **Syslog**, wählen Sie eine SYSLOG-Richtlinie aus, und klicken Sie auf **Aktion**. Klicken Sie dann auf **Globale Bindungen**, und binden Sie die Richtlinie an System Global.

Beispiel:

Die folgende Konfiguration legt den Lastausgleich von SYSLOG-Meldungen zwischen den externen Protokollservern fest, wobei AUDITLOGHASH als Load-Balancing-Methode verwendet wird. Die Last der AUDITLOGHASH-Methode gleicht den Datenverkehr basierend auf dem Eingabe-Hashwert der Audit-Agenten aus. Die Agents sind die Module, die Auditlog in einer Citrix ADC Appliance generieren. Wenn beispielsweise ein Agent-LSN Auditlogs basierend auf der Client-IP-Adresse ausbalancieren möchte, generiert das LSN-Modul den Hashwert basierend auf ClientIP und übergibt den Hashwert

an das auditlog-Modul. Das auditlog-Modul sendet die Auditlog-Meldungen, die denselben Hashwert haben, an den externen Syslog-Server.

Die Citrix ADC Appliance generiert SYSLOG-Ereignisse und -Meldungen, die einen Lastausgleich zwischen den Diensten Service1, Service2 und Dienst 3 aufweisen.

```
add service service1 192.0.2.10 SYSLOGUDP 514
add service service2 192.0.2.11 SYSLOGUDP 514
add service service3 192.0.2.11 SYSLOGUDP 514
add lb vserver lbvserver1 SYSLOGUDP -lbMethod AUDITLOGHASH
bind lb vserver lbvserver1 service1
bind lb vserver lbvserver1 service2
bind lb vserver lbvserver1 service3
add syslogaction sysaction1 -lbVserverName lbvserver1 -logLevel All
add syslogpolicy syspol1 ns_true sysaction1
bind system global syspol1
<!--NeedCopy-->
```

Einschränkungen:

- Die Citrix ADC Appliance unterstützt keinen externen Lastenausgleich des virtuellen Servers, der die SYSLOG-Nachrichten zwischen den Protokollservern ausgleicht.

Standardeinstellungen für die Protokolleigenschaften

October 5, 2021

Im Folgenden finden Sie ein Beispiel für den Standardfilter mit Standardeinstellungen für die Protokolleigenschaften:

```
begin default
 logInterval Hourly
 logFileSizeLimit 10
 logFilenameFormat  auditlog%`{
 `%y%m%d }
 t.log
 end default
<!--NeedCopy-->
```

Im Folgenden finden Sie zwei Beispiele für die Definition der Standardfilter:

Beispiel 1:

```
Filter f1 IP 192.168.10.1
<!--NeedCopy-->
```

Dadurch wird eine Protokolldatei für NSI 192.168.10.1 mit den Standardwerten des Protokolls erstellt.

Beispiel 2:

```
Filter f1 IP 192.168.10.1
begin f1
    logFilenameFormat logfiles.log
end f1
<!--NeedCopy-->
```

Dadurch wird eine Protokolldatei für NSIP 192.168.10.1 erstellt. Da das Format des Protokolldateinamens angegeben wird, sind die Standardwerte der anderen Protokolleigenschaften wirksam.

Beispielkonfigurationsdatei (audit.conf)

October 5, 2021

Im Folgenden finden Sie eine Beispielkonfigurationsdatei:

```
##############################
# This is the Auditserver configuration file
# Only the default filter is active
# Remove leading # to activate other filters
##############################
MYIP <NSAuditserverIP>
MYPORT 3023
#   Filter filter_nsip  IP <Specify the Citrix ADC IP address to filter
    on > ON
#   begin filter_nsip
#       logInterval         Hourly
#       logFileSizeLimit    10
#       logDirectory         logdir\%A\
#       logFilenameFormat   nsip%\\{
 \\%d%m%Y }
```



```
 t.log
#   end filter_nsip
Filter default
begin default
    logInterval      Hourly
    logFileSizeLimit    10
    logFilenameFormat   auditlog%\{
 \%y%m%d }
 t.log
end default
<!--NeedCopy-->
```

Webserver-Protokollierung

October 5, 2021

Sie können die Webserverprotokollierungsfunktion verwenden, um Protokolle von HTTP- und HTTPS-Anforderungen zum Speichern und Abrufen an ein Clientsystem zu senden. Diese Funktion besteht aus zwei Komponenten:

- Der Webprotokollserver, der auf dem Citrix ADC ausgeführt wird.
- Der Citrix ADC Web Logging (NSWL) -Client, der auf dem Clientsystem ausgeführt wird.

Wenn Sie den Citrix ADC Web Logging (NSWL) -Client ausführen:

1. Es wird mit dem Citrix ADC verbunden.
2. Citrix ADC puffert die HTTP- und HTTPS-Anforderungsprotokolleinträge, bevor sie an den Client gesendet werden.
3. Der Client kann die Einträge filtern, bevor er sie speichert.

Um die Webserverprotokollierung zu konfigurieren, aktivieren Sie zunächst die Webprotokollierungsfunktion auf dem Citrix ADC und konfigurieren die Größe des Puffers zum vorübergehenden Speichern der Protokolleinträge. Anschließend installieren Sie NSWL auf dem Clientsystem. Anschließend fügen Sie der NSWL-Konfigurationsdatei die Citrix ADC IP-Adresse (NSIP) hinzu. Sie können nun den NSWL-Client starten, um mit der Protokollierung zu beginnen. Sie können die Webserverprotokollierung anpassen, indem Sie zusätzliche Änderungen an der NSWL-Konfigurationsdatei (log.conf) vornehmen.

Konfigurieren des Citrix ADC für die Webserver-Protokollierung

October 5, 2021

Um den Citrix ADC für die Webserverprotokollierung zu konfigurieren, müssen Sie nur die Webserverprotokollierung aktivieren. Optional können Sie die folgenden Konfigurationen durchführen:

- Ändern Sie die Größe des Puffers (Standardgröße ist 16 MB), in dem die protokollierten Informationen gespeichert werden, bevor sie an den Citrix ADC Web Logging (NSWL) -Client gesendet werden.
- Geben Sie die benutzerdefinierten HTTP-Header an, die Sie in den NSWL-Client exportieren möchten. Sie können maximal zwei HTTP-Request- und zwei HTTP-Antwort-Headernamen konfigurieren.

So konfigurieren Sie die Webserverprotokollierung mit der Befehlszeilenschnittstelle

Führen Sie an der Eingabeaufforderung die folgenden Vorgänge aus:

- Aktivieren Sie die Webserver-Protokollierungsfunktion.

  ```
  enable ns feature WL
  ```

- [Optional] Ändern Sie die Puffergröße zum Speichern der protokollierten Informationen.

  ```
  set ns weblogparam -bufferSizeMB <size>
  ```

  > **Hinweis**:
  >
  > Um Ihre Änderung zu aktivieren, müssen Sie die Webserverprotokollierungsfunktion deaktivieren und wieder aktivieren.

- [Optional] Geben Sie die benutzerdefinierten HTTP-Headernamen an, die Sie exportieren möchten.

  ```
  set ns weblogparam [-customReqHdrs <string> ...] [-customRspHdrs <
  string> ...]
  ```

```
1     > enable ns feature WL
2     Done
3     > set ns weblogparam -bufferSizeMB 60
4     Done
5     > show ns weblogparam
6         Web Logging parameters:
7         Log buffer size:  60MB
8         Custom HTTP request headers: (none)
9         Custom HTTP response headers: (none)
10    Done
11    > set ns weblogparam -customReqHdrs req1 req2 -customRspHdrs res1
         res2
12    Done
```



```
    > show ns weblogparam
        Web Logging parameters:
        Log buffer size:  60MB
        Custom HTTP request headers: req1, req2
        Custom HTTP response headers: res1, res2
    Done
<!--NeedCopy-->
```

So konfigurieren Sie die Webserverprotokollierung mit der GUI

1. Navigieren Sie zu **System** > **Einstellungen**, und führen Sie die folgenden Vorgänge aus:
    a) Klicken Sie zum Aktivieren der Webserverprotokollierungsfunktion auf **Erweiterte Funktionen ändern**, und wählen Sie **Webprotokollierung** aus.
    b) Um die Puffergröße zu ändern, klicken Sie auf **Globale Systemeinstellungen ändern** und geben Sie unter **Webprotokollierung** die Puffergröße ein.
    c) Um die benutzerdefinierten HTTP-Header anzugeben, die exportiert werden sollen, klicken Sie auf **Globale Systemeinstellungen ändern** und geben Sie unter **Webprotokollierung** die Header-Werte an.

Installieren des Citrix ADC Webprotokollierungsclients (NSWL)

October 5, 2021

Wenn Sie NSWL installieren, wird die ausführbare Clientdatei (NSWL) zusammen mit anderen Dateien installiert. Die ausführbare NSWL-Datei enthält eine Liste der Optionen, die Sie verwenden können. Weitere Informationen finden Sie unter Konfigurieren des NSWL-Clients.

> **Achtung**
>
> Die Version des NSWL-Clients muss mit Citrix ADC identisch sein. Wenn beispielsweise die Version des Citrix ADC 10.1 Build 125.9 lautet, muss der NSWL-Client ebenfalls dieselbe Version haben. Außerdem funktioniert der Web Logging (NSWL) -Client sowohl auf 32-Bit- als auch auf 64-Bit-Servercomputern. Die Downloadseite hat nur einen 32-Bit-Weblog-Client. Der 64-Bit-Weblog-Client ist auf Anfrage verfügbar und empfiehlt Ihnen, sich an den Citrix Support zu wenden, um weitere Informationen zu erhalten.

In der folgenden Tabelle sind die Betriebssysteme aufgeführt, auf denen der NSWL-Client installiert werden kann.

Betriebssystem	Version	Hardwareanforderungen	Bemerkungen
Windows	Windows Server 2016 or later	Processor - x86/amd64 CPU (1 GHz or higher), RAM - 4 GB (or higher)	
macOS	macOS 8.6 or later	Not supported on Citrix ADC 10.1 and later releases.	
Linux	Ubuntu, SUSE Linux, CentOS, Red Hat Enterprise Linux released in 2016 or later	Processor - x86/amd64 CPU (1 GHz or higher), RAM - 4 GB (or higher)	
Solaris	Solaris Sun OS 5.6 or later	Processor - UltraSPARC-IIi 400 MHz, RAM - 512 MB, Controller - SCSI	Not supported on Citrix ADC 10.5 and later releases.
FreeBSD	FreeBSD 6.3 or later	Processor - x86/amd64 CPU (1 GHz or higher), RAM - 4 GB (or higher)	For Citrix ADC 10.5, use only FreeBSD 8.4.
AIX	AIX 6.1	-	Not supported on Citrix ADC 10.5 and later releases.

Wenn das NSWL-Clientsystem die Protokolltransaktion aufgrund einer CPU-Beschränkung nicht verarbeiten kann, überschreibt der Webprotokollpuffer und der Protokollierungsprozess wird erneut initiiert.

> **Achtung**
>
> Die Wiedereinleitung der Protokollierung kann zum Verlust von Protokolltransaktionen führen.

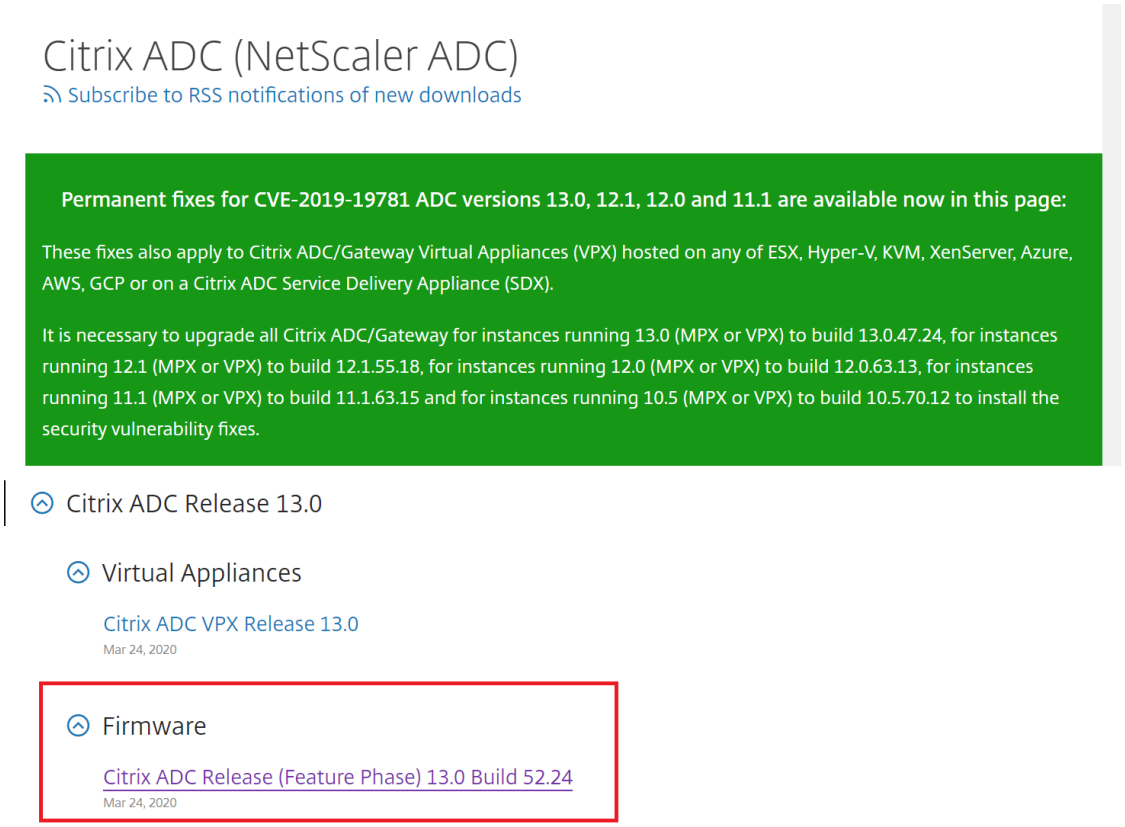
Um einen durch eine CPU-Einschränkung verursachten NSWL-Clientsystem-Engpass vorübergehend zu lösen, können Sie die Puffergröße für die Webserver-Protokollierung auf der Citrix ADC Appliance optimieren. Um das Problem zu lösen, benötigen Sie ein Clientsystem, das den Durchsatz der Site bewältigen kann.

Laden Sie den NSWL-Client herunter

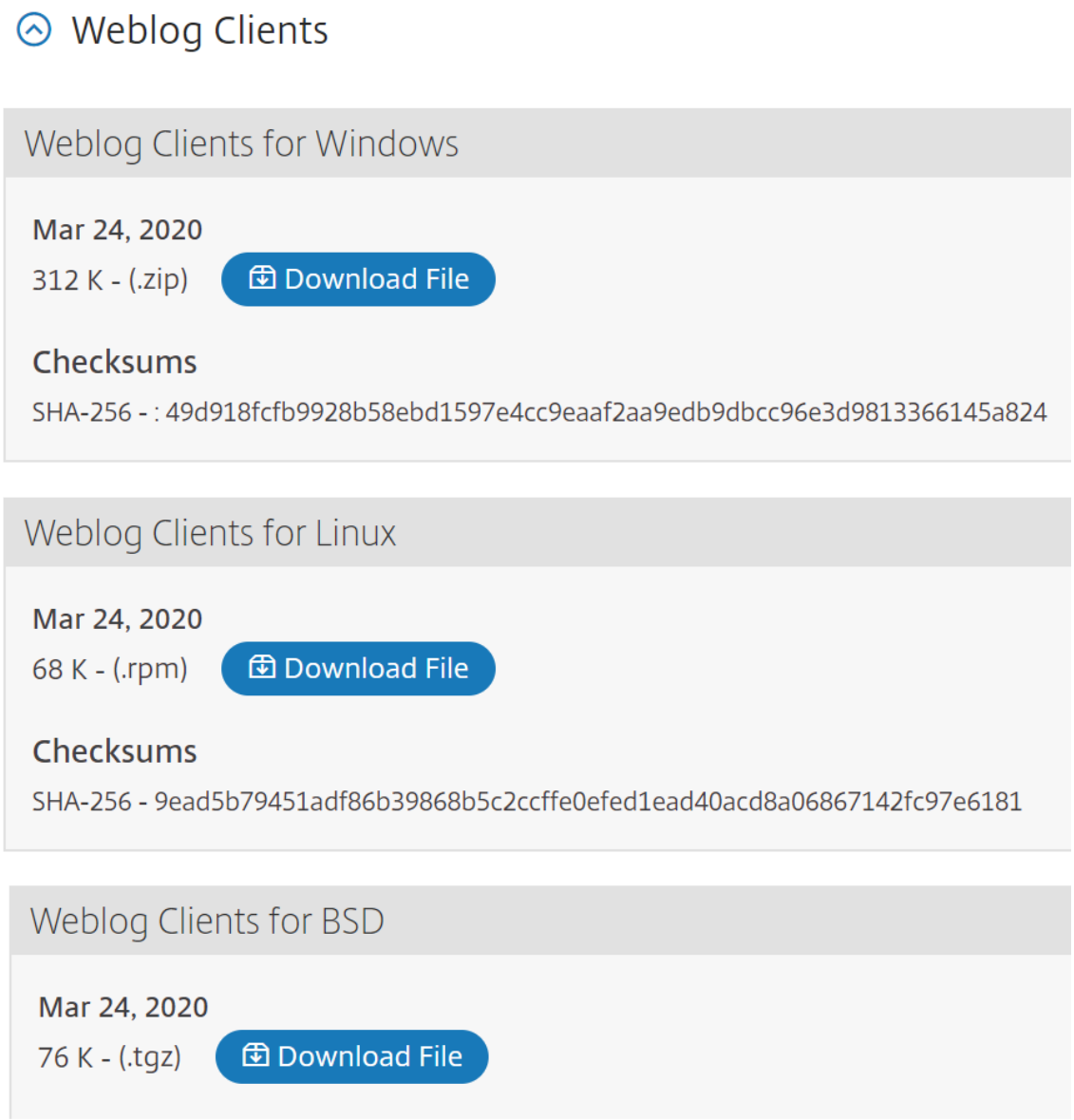
Sie können das NSWL-Clientpaket entweder von der Citrix ADC Produkt-CD oder von der Citrix Download-Site beziehen. Innerhalb des Pakets gibt es separate Installationspakete für jede unterstützte Plattform.

So laden Sie den NSWL-Client von der Citrix Website herunter

1. Melden Sie sich bei Citrix an, indem Sie auf die URL zugreifen `https://www.citrix.com/downloads/citrix-adc/`.
2. Navigieren Sie zu einer bestimmten Citrix ADC Release-Version und suchen Sie nach ihrer Firmware.
3. Klicken Sie auf **Firmware** (z. B. Citrix ADC Release (Feature Phase) 13.0 Build 52.24).



4. Wechseln Sie auf der Seite **Citrix ADC Release (Feature Phase) Build** zum Abschnitt **Weblog-Clients**.
5. In diesem Abschnitt können Sie Weblog-Clients für Windows, Linux und BSD herunterladen.



Installieren Sie den NSWL-Client auf Solaris

Um den NSWL-Client zu installieren, führen Sie die folgenden Vorgänge auf dem System aus, auf dem Sie das Paket heruntergeladen haben.

1. Extrahieren`nswl_solaris-<release number>-<build number>.tar file` Sie die aus dem Paket.
2. Kopieren Sie die extrahierte Datei in ein Solaris-System, auf dem Sie den NSWL-Client installieren möchten.
3. Extrahieren Sie die Dateien aus der tar-Datei mit dem folgenden Befehl:


```
tar xvf nswl_solaris-9.3-51.5.tar
```

Im temporären Verzeichnis wird ein Verzeichnis Weblog erstellt, und die Dateien werden in das Weblog-Verzeichnis extrahiert.

- Installieren Sie das Paket mit dem folgenden Befehl:

  ```
  pkgadd -d
  ```

- Die Liste der verfügbaren Pakete wird angezeigt. Im folgenden Beispiel wird ein Weblog-Paket gezeigt:

  ```
  1 NSweblog Citrix ADC Weblogging (SunOS,sparc)7.0
  ```

Sie werden aufgefordert, die Pakete auszuwählen. Wählen Sie die Paketnummer des zu installierenden Weblogs aus.

Nachdem Sie die Paketnummer ausgewählt und die **Eingabetaste**gedrückt haben, werden die Dateien extrahiert und in den folgenden Verzeichnissen installiert:

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

1. Um zu überprüfen, ob das NSWL-Paket installiert ist, führen Sie den folgenden Befehl aus:

   ```
   pkginfo | grep NSweblog
   ```

2. Um das NSWL-Paket zu deinstallieren, führen Sie den folgenden Befehl aus:

   ```
   pkgrm NSweblog
   ```

Installieren Sie den NSWL-Client unter Linux

> **Wichtig**
>
> Die Installation eines NSWL-Clients unter Linux ersetzt die Konfigurationsdatei. Sie müssen ein Backup erstellen, bevor Sie es installieren.

Um den NSWL-Client zu installieren, führen Sie die folgenden Vorgänge auf dem System aus, auf dem Sie das Paket heruntergeladen haben.

1. Extrahieren nswl_linux-<release number>-<build number>.rpm Sie die Datei aus dem Paket.
2. Kopieren Sie die extrahierte Datei in ein System mit Linux OS, auf dem Sie den NSWL-Client installieren möchten.
3. Um das NSWL-Paket zu installieren, führen Sie den folgenden Befehl aus:

   ```
   rpm -i nswl_linux-9.3-51.5.rpm
   ```


Dieser Befehl extrahiert die Dateien und installiert sie in den folgenden Verzeichnissen.

- /usr/local/netscaler/etc
- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

1. Um das NSWL-Paket zu deinstallieren, führen Sie den folgenden Befehl aus:

   ```
   rpm -e NSweblog
   ```

2. Um weitere Informationen über die Weblog-RPM-Datei zu erhalten, führen Sie den folgenden Befehl aus:

   ```
   rpm -qpi *.rpm
   ```

3. Um die installierten Webserver-Logging-Dateien anzuzeigen, führen Sie den folgenden Befehl aus:

   ```
   rpm -qpl *.rpm
   ```

Installieren Sie den NSWL-Client auf FreeBSD

Um den NSWL-Client zu installieren, führen Sie die folgenden Vorgänge auf dem System aus, auf dem Sie das Paket heruntergeladen haben.

1. Extrahieren `nswl_bsd-<release number>-<build number>.tgz` Sie die Datei aus dem Paket.
2. Kopieren Sie die extrahierte Datei in ein System mit FreeBSD OS, auf dem Sie den NSWL-Client installieren möchten.
3. Um das NSWL-Paket zu installieren, führen Sie den folgenden Befehl aus:

   ```
   pkg_add nswl_bsd-9.3-51.5.tgz
   ```

Dieser Befehl extrahiert die Dateien und installiert sie in den folgenden Verzeichnissen.

```
1 -  /usr/local/netscaler/etc
2 -  /usr/local/netscaler/bin
3 -  /usr/local/netscaler/samples
```

1. Um das NSWL-Paket zu deinstallieren, führen Sie den folgenden Befehl aus:

   ```
   pkg_delete NSweblog
   ```

2. Um zu überprüfen, ob das Paket installiert ist, führen Sie den folgenden Befehl aus:

   ```
   pkg_info | grep NSweblog
   ```


Installieren Sie den NSWL-Client auf dem Mac

Um den NSWL-Client zu installieren, führen Sie die folgenden Vorgänge auf dem System aus, auf dem Sie das Paket heruntergeladen haben.

1. Extrahieren `nswl_macos-<release number>-<build number>.tgz` Sie die Datei aus dem Paket.
2. Kopieren Sie die extrahierte Datei auf ein System mit macOS, auf dem Sie den NSWL-Client installieren möchten.
3. Um das NSWL-Paket zu installieren, führen Sie den folgenden Befehl aus:

   ```
   pkg_add nswl_macos-9.3-51.5.tgz
   ```

Dieser Befehl extrahiert die Dateien und installiert sie in den folgenden Verzeichnissen:

- /usr/local/netscaler/usw
- /usr/local/netscaler/bin
- /usr/local/netscaler/samples

1. Um das NSWL-Paket zu deinstallieren, führen Sie den folgenden Befehl aus:

   ```
   pkg_delete NSweblog
   ```

2. Um zu überprüfen, ob das Paket installiert ist, führen Sie den folgenden Befehl aus:

   ```
   pkg_info | grep NSweblog
   ```

Installieren Sie den NSWL-Client unter Windows

Um den NSWL-Client zu installieren, führen Sie die folgenden Vorgänge auf dem System aus, auf dem Sie das Paket heruntergeladen haben.

1. Extrahieren `nswl_win-<release number>-<build number>.zip` Sie die Datei aus dem Paket.
2. Kopieren Sie die extrahierte Datei in ein Windows-System, auf dem Sie den NSWL-Client installieren möchten.
3. Entpacken Sie die Datei auf dem Windows-System in einem Verzeichnis (bezeichnet als`<NSWL-HOME>`). Die folgenden Verzeichnisse werden extrahiert: `/bin`, und `/etc` und `/samples`.
4. Führen Sie an der Eingabeaufforderung den folgenden Befehl aus der`<NSWL-HOME>\bin directory`:

   ```
   nswl -install -f <directorypath>\log.conf
   ```

Hierbei gilt:

Der Verzeichnispfad bezieht sich auf den Pfad der Konfigurationsdatei (log.conf). Standardmäßig befindet sich die Datei im `/etc` Verzeichnis `<NSWL-HOME>` und. Sie können die Konfigurationsdatei in ein anderes Verzeichnis kopieren.

> **Hinweis:**
>
> Um den NSWL-Client zu deinstallieren, führen Sie an der Eingabeaufforderung den folgenden Befehl aus `<NSWL-HOME>\bin directory:`

```
1 > nswl -remove
```

Installieren Sie den NSWL-Client auf dem AIX-System

Um den NSWL-Client zu installieren, führen Sie die folgenden Vorgänge auf dem System aus, auf dem Sie das Paket heruntergeladen haben.

1. Extrahieren `nswl_aix-<release number>-<build number>.rpm` Sie die Datei aus dem Paket.
2. Kopieren Sie die extrahierte Datei in ein System mit AIX OS, auf dem Sie den NSWL-Client installieren möchten.
3. Um das NSWL-Paket zu installieren, führen Sie den folgenden Befehl aus:

   ```
   rpm -i nswl_aix-9.3-51.5.rpm
   ```

Dieser Befehl extrahiert die Dateien und installiert sie in den folgenden Verzeichnissen.

- `/usr/local/netscaler/etc`
- `/usr/local/netscaler/`
- `usr/local/netscaler/samples`

1. Um das NSWL-Paket zu deinstallieren, führen Sie den folgenden Befehl aus:

   ```
   rpm -e NSweblog
   ```

2. Um weitere Informationen über die Weblog-RPM-Datei zu erhalten, führen Sie den folgenden Befehl aus:

   ```
   rpm -qpi *.rpm
   ```

3. Um die installierten Webserver-Logging-Dateien anzuzeigen, führen Sie den folgenden Befehl aus:

   ```
   rpm -qpl *.rpm
   ```


Konfigurieren des NSWL-Clients

July 8, 2022

Nachdem Sie den NSWL-Client installiert haben, können Sie den NSWL-Client mithilfe der ausführbaren Datei nswl konfigurieren. Diese Konfigurationen werden in der NSWL-Client-Konfigurationsdatei (log.conf) gespeichert.

> **Hinweis:**
>
> Sie können die Protokollierung auf dem NSWL-Client weiter anpassen, indem Sie zusätzliche Änderungen an der NSWL-Konfigurationsdatei (log.conf) vornehmen. Weitere Informationen finden Sie unter Anpassen der Protokollierung auf dem NSWL-Clientsystem.

In der folgenden Tabelle werden die Befehle beschrieben, mit denen Sie den NSWL-Client konfigurieren können.

NSWL-Befehl	Spezifiziert
nswl -help	Die verfügbaren NSWL-Hilfeoptionen.
nswl -addns -f <path-to-configuration-file>	Das System, das die Protokoll-Transaktionsdaten sammelt. Sie werden aufgefordert, die IP-Adresse der Citrix ADC-Appliance einzugeben. Geben Sie einen gültigen Benutzernamen und ein Kennwort ein.
nswl -verify -f <path-to-configuration-file>	Prüfen Sie die Konfigurationsdatei auf Syntax- oder Semantikfehler.
nswl -start -f <path-to-configuration-file>	Starten Sie den NSWL-Client basierend auf den Einstellungen in der Konfigurationsdatei. Hinweis: Für Solaris und Linux: Um die Web-Server-Protokollierung als Hintergrundprozess zu starten, geben Sie am Ende des Befehls das kaufmännische Und-Zeichen (&) ein.
nswl -stop (nur Solaris und Linux)	Stoppen Sie den NSWL-Client, falls er als Hintergrundprozess gestartet wurde. Andernfalls verwenden Sie STRG+C, um die Web-Server-Protokollierung zu beenden.

NSWL-Befehl	Spezifiziert
nswl -install -f <path-to-configuration-file> (nur Windows)	Installieren Sie den NSWL-Client als Dienst in Windows.
nswl -startservice (nur Windows)	Starten Sie den NSWL-Client, indem Sie die Einstellungen in der Konfigurationsdatei verwenden, die in der Installationsoption nswl angegeben ist. Sie können den NSWL-Client auch über Start > Systemsteuerung > Dienste starten. Hinweis: Die NSWL-Protokolldateien werden in C:\Windows\SysWOW64. erstellt
nswl -stopservice (nur Windows)	Beendet den NSWL-Client.
nswl -remove	Entfernen Sie den NSWL-Clientdienst aus der Registrierung.

Führen Sie die folgenden Befehle aus dem Verzeichnis aus, in dem sich die ausführbare NSWL-Datei befindet:

- Windows: \ns\bin
- Solaris and Linux: \usr\local\netscaler\bin

Die Konfigurationsdateien für die Web-Server-Protokollierung befinden sich im folgenden Verzeichnispfad:

- Windows: \ns\etc
- Solaris and Linux: \usr\local\netscaler\etc

Die ausführbare NSWL-Datei wird als gestartet. \ nswl unter Linux und Solaris.

Fügen Sie die IP-Adressen der Citrix ADC-Appliance hinzu

Fügen Sie in der NSWL-Clientkonfigurationsdatei (log.conf) die Citrix ADC-IP-Adresse (NSIP) hinzu, von der der NSWL-Client mit dem Sammeln von Protokollen beginnt.

So fügen Sie die NSIP-Adresse der Citrix ADC-Appliance hinzu

1. Geben Sie an der Eingabeaufforderung des Clientsystems Folgendes ein:

   ```
   nswl -addns -f < directorypath > \log.conf
   < directorypath >: Specifies the path to the configuration file (log.
   conf).
   ```

2. Geben Sie bei der nächsten Eingabeaufforderung die folgenden Informationen ein:

- **NSIP**: Geben Sie die IP-Adresse der Citrix ADC-Appliance an.
- Benutzername und Kennwort: Geben Sie die nsroot-Benutzeranmeldeinformationen der Citrix ADC-Appliance an.

  > **Hinweis:**
  >
  > Jeder Systembenutzer mit aktivierter Protokollierungsberechtigung unterstützt diese Funktionalität.

> **Hinweis**:
>
> Wenn Sie mehrere Citrix ADC-IP-Adressen (NSIP) hinzufügen und später nicht alle Citrix ADC-Systemprotokolldetails protokollieren möchten, können Sie die NSIPs manuell löschen, indem Sie die NSIP-Anweisung am Ende der Datei log.conf entfernen. Während eines Failover-Setups müssen Sie der log.conf sowohl primäre als auch sekundäre Citrix ADC-IP-Adressen hinzufügen, indem Sie den Befehl verwenden. Stellen Sie vor dem Hinzufügen der IP-Adresse sicher, dass der Benutzername und das Kennwort auf den Citrix ADC-Appliances vorhanden sind.

Überprüfen Sie die NSWL-Konfigurationsdatei

Um sicherzustellen, dass die Protokollierung korrekt funktioniert, überprüfen Sie die NSWL-Konfigurationsdatei (log.conf) auf dem Clientsystem auf Syntaxfehler.

So überprüfen Sie die Konfiguration in der NSWL-Konfigurationsdatei

Geben Sie an der Eingabeaufforderung des Clientsystems Folgendes ein:

```
nswl -verify -f <directorypath>\log.conf
```

< directorypath>: Gibt den Pfad zur Konfigurationsdatei (log.conf) an.

NSWL Client ausführen

Starten der Webserver-Protokolle

Geben Sie an der Eingabeaufforderung des Clientsystems Folgendes ein:

```
nswl -start -f <directorypath>\log.conf
```

<directorypath>: Gibt den Pfad zur Konfigurationsdatei (log.conf) an.

Beenden der Web-Server-Protokollierung, die als Hintergrundprozess auf den Betriebssystemen Solaris oder Linux gestartet wurde

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
nswl -stop
```


So beenden Sie die Web-Server-Protokollierung, die als Dienst auf dem Windows-Betriebssystem gestartet wurde

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
nswl -stopservice
```

Anpassen der Protokollierung auf dem NSWL-Clientsystem

May 10, 2022

Sie können die Anmeldung am Citrix ADC Web Logging (NSWL) -Clientsystem anpassen, indem Sie weitere Änderungen an der NSWL-Clientkonfigurationsdatei (log.conf) vornehmen. Verwenden Sie einen Texteditor, um die Konfigurationsdatei log.conf auf dem Clientsystem zu ändern.

Um die Protokollierung anzupassen, verwenden Sie die Konfigurationsdatei, um Filter und Protokolleigenschaften zu definieren.

- **Filter protokollieren.** Filtern Sie Protokollinformationen basierend auf der Host-IP-Adresse, dem Domänennamen und dem Hostnamen der Webserver.
- **Eigenschaften protokollieren.** Jeder Filter hat einen zugehörigen Satz von Protokolleigenschaften. Protokolleigenschaften definieren, wie die gefilterten Protokollinformationen gespeichert werden.

Beispiel für eine Konfigurationsdatei

Es folgt ein Beispiel für eine Konfigurationsdatei:

```
1  ##########
2  # This is the NSWL configuration file
3  # Only the default filter is active
4  # Remove leading # to activate other filters
5  ##########
6  ##########
7  # Default filter (default on)
8  # W3C Format logging, new file is created every hour or on reaching 10
      MB file size,
9  # and the file name is Exyymmdd.log
10 ##########
11 Filter default
12 begin default
13         logFormat               W3C
```



```
        logInterval             Hourly
        logFileSizeLimit        10
        logFilenameFormat       Ex%`{
 `%y%m%d }
 t.log
end default
##########
# Citrix ADC caches example
# CACHE_F filter covers all the transaction with HOST name www.
   netscaler.com and the listed server ip's
##########
#Filter CACHE_F HOST www.netscaler.com IP 192.168.100.89 192.168.100.95
    192.168.100.52 192.168.100.53 ON
##########
# netscaler origin server example
# Not interested in Origin server to Cache traffic transaction logging
##########
#Filter ORIGIN_SERVERS IP 192.168.100.64 192.168.100.65 192.168.100.66
   192.168.100.67 192.168.100.225 192.168.100.226 192.168.
100.227 192.168.100.228 OFF
##########
# netscaler image server example
# all the image server logging.
##########
#Filter IMAGE_SERVER HOST www.netscaler.images.com IP 192.168.100.71
   192.168.100.72 192.168.100.169 192.168.100.170 192.168.10
0.171 ON
##########
# NCSA Format logging, new file is created every day midnight or on
   reaching 20MB file size,
# and the file name is /datadisk5/netscaler/log/NS<hostname>/Nsmmddyy.
   log.
# Exclude objects that ends with .png .jpg .jar.
##########
#begin ORIGIN_SERVERS
#       logFormat               NCSA
#       logInterval             Daily
#       logFileSizeLimit        40
#       logFilenameFormat       /datadisk5/ORGIN/log/%v/NS%`{
 `%m%d%y }
 t.log
#       logExclude              .png .jpg .jar
#end ORIGIN_SERVERS

##########
```



```
# NCSA Format logging, new file is created every day midnight or on reaching 20MB file size,
# and the file name is /datadisk5/netscaler/log/NS<hostname>/Nsmmddyy.log with log record timestamp as GMT.
##########
#begin CACHE_F
#       logFormat               NCSA
#       logInterval             Daily
#       logFileSizeLimit        20
#       logFilenameFormat /datadisk5/netscaler/log/%v/NS%`{ `%m%d%y }  t.log
#       logtime                 GMT
#end CACHE_F

##########
# W3C Format logging, new file on reaching 20MB and the log file path name is
# atadisk6/netscaler/log/server's ip/Exmmyydd.log with log record timestamp as LOCAL.
##########
#begin IMAGE_SERVER
#       logFormat               W3C
#       logInterval             Size
#       logFileSizeLimit        20
#       logFilenameFormat /datadisk6/netscaler/log/%AEx%`{ `%m%d%y }  t
#       logtime                 LOCAL
#end IMAGE_SERVER

##########
# Virtual Host by Name firm, can filter out the logging based on the host name by,
##########

#Filter VHOST_F IP 10.101.2.151 NETMASK 255.255.255.0
#begin VHOST_F
#       logFormat               W3C
#       logInterval             Daily
#       logFileSizeLimit        10
logFilenameFormat /ns/prod/vhost/%v/Ex%`{ `%m%d%y }  t
#end VHOST_F
```



```
93
94 ########## END FILTER CONFIGURATION ##########
95 <!--NeedCopy-->
```

Erstellen von Filtern

Sie können die Standardfilterdefinition in der Konfigurationsdatei (log.conf) verwenden oder den Filter ändern oder einen Filter erstellen. Sie können mehrere Protokollfilter erstellen.

> **Hinweis**
>
> Die konsolidierte Protokollierung, die Transaktionen protokolliert, für die kein Filter definiert ist, verwendet den Standardfilter, wenn er aktiviert ist. Die konsolidierte Protokollierung aller Server kann nur durch Definition des Standardfilters erfolgen.

Wenn der Server mehrere Websites hostet und jede Website einen eigenen Domänennamen hat und jede Domäne einem virtuellen Server zugeordnet ist, können Sie die Webserver-Protokollierung so konfigurieren, dass für jede Website ein separates Protokollverzeichnis erstellt wird. In der folgenden Tabelle werden die Parameter zum Erstellen eines Filters angezeigt.

Parameter	Spezifiziert
Filtername	Name des Filters. Der Filtername kann alphanumerische Zeichen enthalten und darf nicht länger als 59 Zeichen sein. Filternamen, die länger als 59 Zeichen sind, werden auf 59 Zeichen abgeschnitten.
Hostname	Hostname des Servers, für den die Transaktionen protokolliert werden.
IP `ip`	IP-Adresse des Servers, für den Transaktionen protokolliert werden sollen (z. B. wenn der Server mehrere Domänen mit einer IP-Adresse hat).
IP `ip 2...ip` n:	Mehrere IP-Adressen (z. B. wenn die Serverdomäne über mehrere IP-Adressen verfügt).
ip6 IP	IPv6-Adresse des Servers, für den Transaktionen protokolliert werden sollen.
IP-IP-NETMASK-Maske	In einem Subnetz zu verwendende Kombination aus IP-Adressen und Netzwerkmasken.

Parameter	Spezifiziert
ON | OFF	Aktivieren oder Deaktivieren des Filters zur Protokollierung von Transaktionen Wenn kein Argument ausgewählt ist, ist der Filter aktiviert (EIN).

Tabelle 1. Parameter zum Erstellen eines Filters

So erstellen Sie einen Filter

Um einen Filter zu erstellen, geben Sie in der Datei log.conf den folgenden Befehl ein:

- `filter <filterName> <HOST name> | [IP<ip> ] | [IP<ip 2...ip n> ] | <IP ip NETMASK mask> [ON | OFF]`
- `filter <filterName> <HOST name> | [IP6 ip/<prefix length>] [ON | OFF]`

So erstellen Sie einen Filter für einen virtuellen Server

Um einen Filter für einen virtuellen Server zu erstellen, geben Sie in der Datei log.conf den folgenden Befehl ein:

```
filter <filterName> <VirtualServer IP address>
```

Beispiel

Im folgenden Beispiel geben Sie eine IP-Adresse von 192.168.100.0 und eine Netzmaske von 255.255.255.0 an. Der Filter gilt für die IP-Adressen 192.168.100.1 bis 192.168.100.254.

```
1  Filter F1 HOST www.netscaler.com ON
2  Filter F2 HOST www.netscaler.com IP 192.168.100.151 ON
3  Filter F3 HOST www.netscaler.com IP 192.168.100.151 192.165.100.152 ON
4  Filter F4 IP 192.168.100.151
5  Filter F5 IP 192.168.100.151 HOST www.netscaler.com OFF
6  Filter F6 HOST www.netscaler.com HOST www.xyz.com HOST www.abcxyz.com
       IP 192.168.100.200 ON
7  Filter F7 IP 192.250.100.0 NETMASK 255.255.255.0
8  Filter F8 HOST www.xyz.com IP 192.250.100.0 NETMASK 255.255.255.0 OFF
9  For creating filters for servers having IPv6 addresses.
10 Filter F9 2002::8/112 ON
11 Filter F10 HOST www.abcd.com IP6 2002::8 ON
12
```



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

Festlegen von Protokolleigenschaften

Protokolleigenschaften werden auf alle Protokolleinträge angewendet, die mit dem Filter verknüpft sind. Die Definition der Logeigenschaft beginnt mit dem Schlüsselwort BEGIN und endet mit END, wie im folgenden Beispiel dargestellt:

```
1 BEGIN <filtername>
2  logFormat ...
3  logFilenameFormat ...
4  logInterval ...
5  logFileSize ....
6  logExclude ....
7  logTime ….
8  END
9 <!--NeedCopy-->
```

Einträge in der Definition können Folgendes enthalten:

-

LogFormat gibt die Webserver-Protokollierungsfunktion an, die NCSA-, W3C Extended- und benutzerdefinierte Protokolldateiformate unterstützt.

```
1 By default, the `logformat` property is w3c. To override, enter custom
     or NCSA in the configuration file, for example:
```

```
1       LogFormat NCSA
2 <!--NeedCopy-->
```

> **Hinweis**
>
> Für die NCSA- und benutzerdefinierten Protokollformate wird die Ortszeit verwendet, um Transaktionen zu zeitstempeln und für die Dateirotation.

- **LogInterval** gibt die Intervalle an, in denen neue Protokolldateien erstellt werden. Verwenden Sie einen der folgenden Werte:
  - Stündlich: Jede Stunde wird eine Datei erstellt.
  - Täglich: Jeden Tag um Mitternacht wird eine Datei erstellt. Standardwert.

- Wöchentlich: Jeden Sonntag um Mitternacht wird eine Datei erstellt.
- Monatlich: Eine Datei wird am ersten Tag des Monats um Mitternacht erstellt.
- Keine: Eine Datei wird nur einmal erstellt, wenn die Web-Server-Protokollierung gestartet wird.

Beispiel:

```
LogInterval Daily
<!--NeedCopy-->
```

LogFileSizeLimit gibt die maximale Größe der Protokolldatei in MB an. Es kann mit jedem Protokollintervall (wöchentlich, monatlich usw.) verwendet werden. Eine Datei wird erstellt, wenn die maximale Dateigröße erreicht ist oder wenn die definierte Protokollintervall-Zeit verstrichen ist.

Um dieses Verhalten zu überschreiben, geben Sie die Größe als Eigenschaft `loginterval` an, damit eine Datei nur erstellt wird, wenn die Größenbeschränkung der Protokolldatei erreicht ist.

Die Standardeinstellung LogFileSizeLimit ist 10 MB.

Beispiel:

```
LogFileSizeLimit 35
<!--NeedCopy-->
```

- **LogFileNameFormat** gibt das Format des Dateinamens der Protokolldatei an. Der Name der Datei kann aus folgenden Typen bestehen:
  - Statisch: Gibt eine konstante Zeichenfolge an, die den absoluten Pfad und den Dateinamen enthält.

    Dynamisch: Gibt einen Ausdruck an, der das folgende Format enthält:

    * Server-IP-Adresse
    * Datum (% {format} t)
    * URL-Suffix (%x)
    * Hostname (%v)

Beispiel:

```
LogFileNameFormat Ex%`{
 `%m%d%y }
 t.log
<!--NeedCopy-->
```


Dieser Befehl erstellt den ersten Dateinamen als Exmmddyy.log und erstellt dann jede Stunde eine Datei mit einem Dateinamen: ExmmDdyy.log.0, ExmmDdyy.Log.1,…, Exmmddyy.log.n.

Beispiel:

```
1       LogInterval size
2       LogFileSize 100
3       LogFileNameFormat Ex%`{
4    `%m%d%y }
5    t
6  <!--NeedCopy-->
```

> **Achtung**
>
> Das im Befehl LogFileNameFormat angegebene Datumsformat%t überschreibt die Protokollintervall-Eigenschaft für diesen Filter. Um zu verhindern, dass täglich eine neue Datei erstellt wird, anstatt wenn die angegebene Protokolldateigröße erreicht ist, verwenden Sie nicht %t im LogFileName-Format.

- **LogexClude** verhindert das Protokollieren von Transaktionen mit den angegebenen Dateinamenerweiterungen.

Beispiel:

```
1       LogExclude .html
2  <!--NeedCopy-->
```

Mit diesem Befehl wird eine Protokolldatei erstellt, die Protokolltransaktionen für *.html-Dateien ausschließt.

LogTime gibt die Protokollzeit entweder als GMT oder LOCAL an.

Die Standardeinstellungen sind:

- NCSA-Protokolldateiformat: LOCAL
- W3C-Protokolldateiformat: GMT.

NCSA- und W3C-Protokollformate verstehen

Der Citrix ADC unterstützt die folgenden Standardprotokolldateiformate:

- Allgemeines NCSA-Protokollformat
- Erweitertes W3C-Protokollformat

Allgemeines NCSA-Protokollformat

Wenn das Protokolldateiformat NCSA ist, zeigt die Protokolldatei Protokollinformationen im folgenden Format an:

```
1 Client_IP_address -User_Name [Date:Time -TimeZone] ”Method Object
     HTTP_version” HTTP_StatusCode BytesSent
2 <!--NeedCopy-->
```

Um das NCSA Common Protokollformat zu verwenden, geben Sie NCSA in das Argument LogFormat in der Datei log.conf ein.

In der folgenden Tabelle wird das Protokollformat von NCSA Common beschrieben.

Argument	Spezifiziert
Client_IP_Adresse	Die IP-Adresse des Clientcomputers.
Benutzername	Der Benutzername.
Datum	Das Datum der Transaktion.
Zeit	Der Zeitpunkt, zu dem die Transaktion abgeschlossen wurde.
Zeitzone	Die Zeitzone (Greenwich Mean Time oder Ortszeit).
Methode	Die Anforderungsmethode (z. B. GET, POST).
Objekt	Die URL.
HTTP_version	Die vom Client verwendete HTTP-Version.
HTTP_StatusCode	Der Statuscode in der Antwort.
Byte gesendet	Die Anzahl der vom Server gesendeten Byte.

W3C erweitertes Protokollformat

Eine erweiterte Protokolldatei enthält eine Folge von Zeilen mit ASCII-Zeichen, die entweder durch einen Line Feed (LF) oder die Sequenz Carriage Return Line Feed (CRLF) abgeschlossen sind. Protokolldateigeneratoren müssen die Konvention für die Leitungsbeendigung für die Plattform einhalten, auf der sie ausgeführt werden.

Protokollanalysatoren müssen entweder LF- oder CRLF-Formular akzeptieren. Jede Zeile kann entweder eine Direktive oder einen Eintrag enthalten. Wenn Sie das W3C Extended Logformat verwen-

den möchten, geben Sie W3C als Log-Format Argument in der Datei log.conf ein.

Standardmäßig ist das Standard-W3C-Protokollformat intern als benutzerdefiniertes Protokollformat definiert, wie folgt dargestellt:

```
%`{
 `%Y-%m-%d%H:%M:%S }
 t %a %u %S %A %p %m %U %q %s %j %J %T %H %+{
 user-agent }
 i %+{
 cookie }
  i%+{
 referer }
 i
<!--NeedCopy-->
```

Sie können auch die Reihenfolge ändern oder einige Felder in diesem W3C-Protokollformat entfernen. Beispiel:

```
logFormat W3C %`{
 `%Y-%m-%d%H:%M:%S }
 t %m %U
<!--NeedCopy-->
```

W3C-Protokolleinträge werden mit dem folgenden Format erstellt:

```
#Version: 1.0
#Fields: date time cs-method cs-uri
#Date: 12-Jun-2001 12:34
2001-06-12 12:34:23 GET /sports/football.html 2001-06-12 12:34:30
GET /sports/football.html
<!--NeedCopy-->
```

Einträge

Einträge bestehen aus einer Folge von Feldern, die sich auf eine einzelne HTTP-Transaktion beziehen. Felder sind durch Leerzeichen getrennt. Citrix empfiehlt die Verwendung von Tabulatorzeichen. Wenn ein Feld in einem bestimmten Eintrag nicht verwendet wird, markiert ein Bindestrich (-) das ausgelassen Feld.

Richtlinien

Informationen zum Protokollierungsprozess finden Sie in der Tabelle Richtlinien . Zeilen, die mit dem Pfundzeichen (#) beginnen, enthalten Anweisungen.

Beispiel:

Die folgende Beispielprotokolldatei zeigt die Protokolleinträge im W3C-Extended-Protokollformat:

```
#Version: 1.0
#Fields: time cs-method cs-uri
#Date: 12-Jan-1996 00:00:00
00:34:23 GET /sports/football.html
12:21:16 GET /sports/football.html
12:45:52 GET /sports/football.html
12:57:34 GET /sports/football.html
<!--NeedCopy-->
```

Felder

Die Fields Direktive listet eine Sequenz von Feldbezeichnern auf, die die in jedem Eintrag aufgezeichneten Informationen angeben. Feldbezeichner haben möglicherweise eine der folgenden Formen:

- **Bezeichner:** Bezieht sich auf die Transaktion als Ganzes.
- **prefix-identifier: Bezieht** sich auf Informationsübertragung zwischen Parteien, die durch das Wertpräfix definiert sind.
- **Präfix (Header):** Gibt den Wert des HTTP-Header-Feld-Headers für die Übertragung zwischen Parteien an, die durch das Wertpräfix definiert Auf diese Weise angegebene Felder haben immer den Typ.

In der folgenden Tabelle werden definierte Präfixe beschrieben.

Präfix	Spezifiziert
c	Client
s	Server
r	Remote
cs	Client zum Server
Sc	Server zum Client
sr	Server zum Remoteserver (von Proxys verwendetes Präfix)

Präfix	Spezifiziert
rs	Remote-Server zum Server (von Proxys verwendetes Präfix)
x	Anwendungsspezifischer Bezeichner

Beispiele:

Die folgenden Beispiele sind definierte Bezeichner, die Präfixe verwenden:

cs-method: Die Methode in der Anforderung, die vom Client an den Server gesendet wird.

sc(Referer): Das Feld `Referer` in der Antwort.

c-ip: Die IP-Adresse des Clients.

Identifikatoren

In der folgenden Tabelle werden die Bezeichner des erweiterten W3C-Protokollformats beschrieben, die kein Präfix benötigen.

Identifier	Beschreibung
Datum	Das Datum, an dem die Transaktion abgeschlossen wurde.
Zeit	Der Zeitpunkt, zu dem die Transaktion abgeschlossen ist.
Zeit in Anspruch genommen	Die für den Abschluss der Transaktion benötigte Zeit (in Sekunden).
Bytes	Die Anzahl der übertragenen Byte.
zwischengespeichert	Zeichnet auf, ob ein Cache-Treffer aufgetreten ist. Eine Null zeigt einen Cache-Fehler an.

Tabelle 5. Bezeichner für das erweiterte W3C-Protokollformat (kein Präfix erforderlich)

In der folgenden Tabelle werden die Bezeichner des erweiterten W3C-Protokollformats beschrieben, die ein Präfix erfordern.

Identifier	Beschreibung
IP	Die IP-Adresse und die Portnummer.

Identifier	Beschreibung
DNS	Der DNS-Name.
Status	Der Statuscode.
comment	Der Kommentar wurde mit einem Statuscode zurückgegeben.
method	Die Methode.
url	Die URL.
url-Stamm	Der Stammteil der URL.
url-Abfrage	Der Abfrageteil der URL.

Tabelle 6. W3C Extended Log Format Bezeichner (erfordert ein Präfix)

Mit dem Dateiformat W3C Extended Log können Sie Protokollfelder auswählen. Diese Felder sind in der folgenden Tabelle aufgeführt.

Feld	Beschreibung
Datum	Das Datum, an dem die Transaktion abgeschlossen ist.
Zeit	Der Zeitpunkt, zu dem die Transaktion abgeschlossen ist.
Client-IP	Die IP-Adresse des Clients.
Benutzername	Der Benutzername.
Dienstname	Der Dienstname, der immer HTTP ist.
Server-IP	Die Server-IP-Adresse.
Serverport	Die Server-Portnummer
Methode	Die Anforderungsmethode (z. B. GET, POST).
Url-Stamm	Der URL-Stamm.
URL-Abfrage	Der Abfrageteil der URL.
HTTP-Status	Der Statuscode in der Antwort.
Byte gesendet	Die Anzahl der an den Server gesendeten Byte (Anforderungsgröße, einschließlich HTTP-Header).

Feld	Beschreibung
Bytes empfangen	Die Anzahl der vom Server empfangenen Byte (Größe der Antwort, einschließlich HTTP-Header).
Zeitaufwand	Die Zeit, die für den Abschluss einer Transaktion in Sekunden gebraucht wird.
Protokollversion	Die Versionsnummer von HTTP, die vom Client verwendet wird.
Benutzeragent	Das Feld User-Agent im HTTP-Protokoll.
Cookie	Das Cookie-Feld des HTTP-Protokolls.
`Referer`	Das Feld `Referer` des HTTP-Protokolls.

Tabelle 7. W3C Erweitertes Protokolldateiformat (Erlaubt Protokollfelder)

Erstellen eines benutzerdefinierten Protokollformats

Sie können das Anzeigeformat der Protokolldateidaten manuell oder mithilfe der NSWL-Bibliothek anpassen. Mithilfe des benutzerdefinierten Protokollformats können Sie die meisten Protokollformate ableiten, die Apache derzeit unterstützt.

Erstellen eines benutzerdefinierten Protokollformats mithilfe der NSWL-Bibliothek

Verwenden Sie eine der folgenden NSWL-Bibliotheken, je nachdem, ob die ausführbare NSWL-Datei auf einem Windows- oder Solaris-Hostcomputer installiert wurde:

- **Windows:** Die nswl.lib-Bibliothek im Verzeichnis\ ns\ bin auf dem Host-Computer des Systemmanagers.
- **Solaris:** Die libnswl.a-Bibliothek in /usr/local/netscaler/bin.

So erstellen Sie das benutzerdefinierte Protokollformat mit der NSWL-Bibliothek

1. Fügen Sie die folgenden zwei vom System definierten C-Funktionen in einer C-Quelldatei hinzu:

   ns_userdeffieldName (): Diese Funktion gibt die Zeichenfolge zurück, die als benutzerdefinierter Feldname im Protokolldatensatz hinzugefügt werden muss.

   ns_userdeffieldVal (): Diese Funktion implementiert den Wert des benutzerdefinierten Feldes und gibt ihn dann als String zurück, der am Ende des Protokolldatensatzes hinzugefügt werden muss.

2. Kompilieren Sie die Datei in eine Objektdatei.
3. Verknüpfen Sie die Objektdatei mit der NSWL-Bibliothek (und optional mit Bibliotheken von Drittanbietern), um eine neue ausführbare NSWL-Bibliothek zu bilden.
4. Fügen Sie am Ende der LogFormat-Zeichenfolge in der Konfigurationsdatei (log.conf) eine %d Zeichenfolge hinzu.

Beispiel:

```
##########
# A new file is created every midnight or on reaching 20MB file size,
# and the file name is
/datadisk5/netscaler/log/NS<hostname>/Nsmmddyy.log and create
digital
#signature field for each record.
BEGIN CACHE_F
    logFormat custom ”%a - ”%{
 user-agent }
 i” [%d/%B/%Y %T -%g] ”%x”
%s %b%{
 referrer }
 i ”%{
 user-agent }
 i” ”%{
 cookie }
 i” %d ”
    logInterval Daily
    logFileSizeLimit 20
    logFilenameFormat
/datadisk5/netscaler/log/%v/NS%`{
 `%m%d%y }
 t.log
END CACHE_F
<!--NeedCopy-->
```

Manuelles Erstellen eines benutzerdefinierten Protokollformats

Um das Format anzupassen, in dem Protokolldateidaten erscheinen müssen, geben Sie eine Zeichenkette als Argument der LogFormat-Log-Eigenschaftsdefinition an. Im Folgenden finden Sie ein Beispiel, in dem Zeichenfolgen verwendet werden, um ein Protokollformat zu erstellen:


```
LogFormat Custom ""%a - "%{
 user-agent }
 i" %[%d/%m/%Y]t %U %s %b %T"
<!--NeedCopy-->
```

- Die Zeichenfolge kann die Steuerzeichen vom Typ "c"\ n und\ t enthalten, um neue Zeilen und Registerkarten darzustellen.
- Verwenden Sie die Esc-Taste mit literalen Anführungszeichen und umgekehrten Schrägstrichen.

Die Merkmale der Anforderung werden protokolliert, indem %-Direktiven in die Formatzeichenfolge eingefügt werden, die in der Protokolldatei durch die Werte ersetzt werden.

Wenn der Formatbezeichner %v (Hostname) oder %x (URL-Suffix) in einer Protokolldateinamenformatzeichenfolge vorhanden ist, werden die folgenden Zeichen im Dateinamen durch einen Unterstreichungsstrich im Namen der Protokollkonfigurationsdatei ersetzt:

```
" *. /: < > ? \
```

Zeichen, deren ASCII-Werte im Bereich von 0-31 liegen, werden wie folgt ersetzt:

%<ASCII value of character in hexadecimal>.

Beispielsweise wird das Zeichen mit dem ASCII-Wert 22 durch %16 ersetzt.

> **Achtung**
>
> Wenn der Formatbezeichner%v in einer Protokolldateinamen-Formatzeichenfolge vorhanden ist, wird für jeden virtuellen Host eine separate Datei geöffnet. Um eine kontinuierliche Protokollierung sicherzustellen, muss die maximale Anzahl von Dateien, die ein Prozess geöffnet haben kann, ausreichend groß sein. Eine Vorgehensweise zum Ändern der Anzahl der Dateien, die geöffnet werden können, finden Sie in der Dokumentation des Betriebssystems.

Erstellen von Apache-Protokollformaten

Sie können aus den benutzerdefinierten Protokollen die meisten Protokollformate ableiten, die Apache derzeit unterstützt. Die benutzerdefinierten Protokollformate, die den Apache-Protokollformaten entsprechen, sind:

NCSA/Combined: LogFormat custom%h%l%u [%t] "%r" %s%b "% {referer} i" "% {useragent} i"

NCSA/Common: LogFormat custom %h %l %u [%t] "%r" %s %B

Referer Log: LogFormat benutzerdefiniert "% {referer} i" ->%U

Benutzeragent: LogFormat custom% {user-agent} i

Ebenso können Sie die anderen Serverprotokollformate aus den benutzerdefinierten Formaten ableiten.

Argumente zum Definieren eines benutzerdefinierten Protokollformats

Weitere Informationen zum Definieren eines benutzerdefinierten Protokollformats finden Sie in der PDF-Tabelle Benutzerdefiniertes Protokollformat.

> **Hinweis**
>
> Anweisungen zum Exportieren benutzerdefinierter HTTP-Header finden Sie unter Konfigurieren des Citrix ADC für die Webserver-Protokollierung

Wenn Sie beispielsweise das Protokollformat als %+{user-agent}i definieren und der Benutzeragent Wert Citrix ADC System Web Client ist, werden die Informationen als Citrix ADC System+Web+Client protokolliert. Eine Alternative besteht darin, doppelte Anführungszeichen zu verwenden. Zum Beispiel protokolliert “%{user-agent}i” es als “Citrix ADC System Web Client. “ Verwenden Sie die <Esc> Taste nicht für Zeichenfolgen von%.. .r,%.. .i und,%. .o. Es entspricht den Anforderungen des Common Log Formats. Clients können Steuerzeichen in das Protokoll einfügen. Daher müssen Sie vorsichtig sein, wenn Sie mit rohen Logfiles arbeiten.

Zeitformatdefinition

In der Definitionstabelle des Zeitformats erfahren Sie mehr über den Formatteil der Zeichenfolge% {format} t, der in der Tabelle Benutzerdefiniertes Protokollformat beschrieben wird. Werte in Klammern ([]) zeigen den Wertebereich an, der angezeigt wird. Beispielsweise zeigt [1,31] in der %d Beschreibung in der folgenden Tabelle %d Bereiche von 1 bis 31.

> **Hinweis**
>
> Wenn Sie eine Konvertierung angeben, die keiner der in der vorhergehenden Tabelle beschriebenen Konvertierungsspezifikationen entspricht, oder einer der im nächsten Absatz aufgeführten geänderten Konvertierungsspezifikationen entspricht, ist das Verhalten nicht definiert und gibt 0 zurück.

Der Unterschied zwischen %U und %W (und auch zwischen den geänderten Konvertierungen %OU und %OW) ist der Tag, der als erster Tag der Woche betrachtet wird. Woche Nummer 1 ist die erste Januarwoche (beginnend mit einem Sonntag für %U oder einem Montag für %W). Woche 0 enthält die Tage vor dem ersten Sonntag oder Montag im Januar für%U und%W.

Anzeigen von Serverprotokollen

Sie können eine NSWL-Funktion so konfigurieren, dass Serverprotokolle auf der Konsole angezeigt werden oder Serverprotokolle in ein Verzeichnis auf der Citrix ADC-Appliance umleiten.

Es gibt zwei Möglichkeiten, Protokolle auf der Konsole anzuzeigen (Standardausgabe):
Option 1: Alle Protokolle auf der Konsole anzeigen.
Option 2: Zeigt nur ausgewählte Protokolle in der Konsole mit Filtern mit `logfilenameformat` als STDOUT an.

Call Home

October 5, 2021

Appliances können aufgrund von Software- oder Hardwareproblemen manchmal nicht gut funktionieren. In solchen Fällen muss Citrix Daten sammeln und Problemlösung durchführen, bevor am Standort des Kunden potenzielle Auswirkungen auftreten können. Indem Sie Call Home auf der Citrix ADC Appliance aktivieren, können Sie die Fehlerbenachrichtigung automatisieren. Sie vermeiden nicht nur den Anruf von Citrix Support, das Anlasten einer Serviceanfrage und das Hochladen von Systemdaten, bevor das Support-Team das Problem beheben kann, sondern der Support kann ein Problem identifizieren und beheben, bevor es auftritt. Call Home überwacht die Appliance regelmäßig und lädt Daten automatisch auf den Citrix Technical Support Server hoch. Darüber hinaus bieten die eingehenden Call Home Daten Einblicke in die Citrix ADC Nutzung. Mehrere Teams innerhalb von Citrix können diese Daten verwenden, um Citrix ADC besser zu entwerfen, zu unterstützen und zu implementieren.

Standardmäßig ist Call Home auf allen Plattformen und allen Varianten von Citrix ADC (MPX, VPX, SDX) aktiviert. Wenn Sie diese Funktion aktiviert haben, können Sie Citrix das Sammeln von Citrix ADC Bereitstellungs- und Telemetriedaten für eine bessere Implementierung und den Supportdienst ermöglichen.

> **Hinweis:**
>
> Informationen zu Call Home finden Sie auch auf der Seite "Häufig gestellte Fragen zu Call Home".

Vorteile

Call Home bietet die folgenden Vorteile.

- Überwachen Sie Hardware- und Software-Fehlerbedingungen. Weitere Informationen finden Sie im Abschnitt Überwachen kritischer Fehlerbedingungen.
- Benachrichtigen Sie kritische Ereignisse, die sich auf Ihr Netzwerk auswirken.
- Senden Sie Performance-Daten und Systemnutzungsdetails an Citrix an:
  - Analysieren und verbessern Sie die Produktqualität.
  - Bereitstellung von Informationen zur Fehlerbehebung in Echtzeit für proaktive Problemerkennung und schnellere Problemlösung.

Plattformunterstützung

Die Call Home Funktion wird auf allen Citrix ADC Plattformen und allen Appliance-Modellen (MPX, VPX und SDX) unterstützt.

- Citrix ADC MPX: Alle MPX-Modelle.
- Citrix ADC VPX: Alle VPX-Modelle, einschließlich VPX-Appliances, die ihre Lizenz von externen oder zentralen Lizenzierungspools beziehen.
- Citrix ADC SDX: Überwacht das Laufwerk und die zugewiesenen SSL-Chips auf Fehler oder Fehler. Die VPX-Instanzen haben jedoch keinen Zugriff auf das Netzteil (Power Supply Unit) und daher wird ihr Status nicht überwacht. In einer SDX-Plattform können Sie Call Home entweder direkt auf einer einzelnen Instanz oder über die SVM konfigurieren.

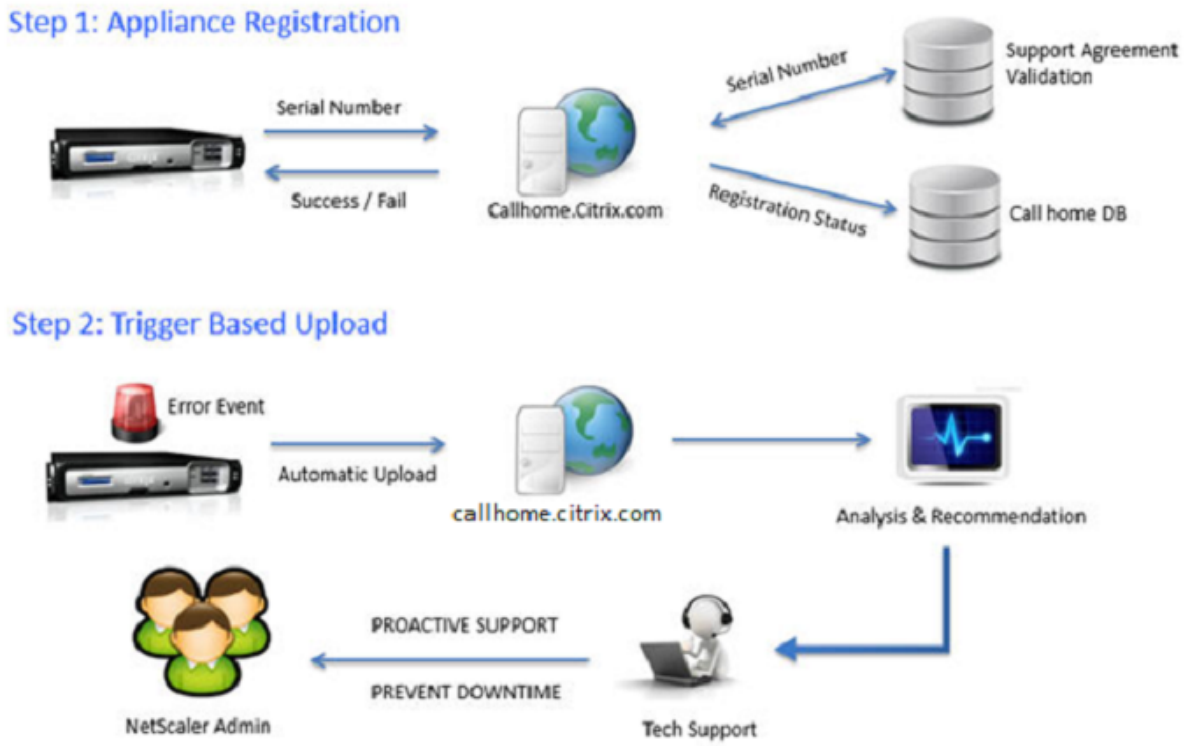
Voraussetzungen

Um Call Home verwenden zu können, muss die Citrix ADC Appliance Folgendes haben:

- **Internetverbindung.** Call Home erfordert eine Internetverbindung für den Citrix ADC, um eine Verbindung zum Citrix Supportserver herzustellen, um ein Datenarchiv hochzuladen.

Funktionsweise von Call Home

Die folgende Abbildung zeigt einen grundlegenden Workflow von Call Home in einer Citrix ADC Appliance, die an einem Kundenstandort bereitgestellt wird.



Im Folgenden ist der Workflow eines Call Home:

1. Richten Sie die Internetverbindung ein. Damit Call Home Systemdaten hochladen kann, muss Ihre Appliance über eine Internetverbindung verfügen. Wenn dies nicht der Fall ist, können Sie eine Proxyserver-Konfiguration so konfigurieren, dass eine Internetverbindung bereitgestellt wird. Weitere Informationen finden Sie im Abschnitt Call Home konfigurieren.

2. Aktivieren Sie Call Home. Wenn Sie Ihre Appliance über die Citrix ADC Befehlszeilenschnittstelle oder GUI auf die neueste Software aktualisieren, ist Call Home standardmäßig aktiviert, und das System verzögert den Registrierungsvorgang um 24 Stunden. Während dieses Zeitraums können Sie die Funktion manuell deaktivieren. Citrix empfiehlt jedoch, sie zu aktivieren.

> **Hinweis:**
>
> Wenn Sie Ihre Appliance von einer älteren Version aktualisieren, bei der Call Home explizit deaktiviert ist, aktiviert das System die Funktion weiterhin standardmäßig und zeigt bei Ihrer ersten Anmeldung eine Benachrichtigung an.

Wenn Sie Konfigurationsänderungen für eine Internetverbindung vornehmen, müssen Sie außerdem Call Home deaktivieren und aktivieren. Es ermöglicht Call Home, sich ohne Fehler beim Citrix Insight Services (CIS) -Server zu registrieren.

3. Registrieren Sie die Citrix ADC Appliance auf dem Citrix Support Server. Wenn Call Home die Appliance beim Citrix Supportserver registriert, überprüft der Server die Datenbank auf die Gültigkeit der Seriennummer der Appliance. Wenn die Seriennummer gültig ist, registriert der Server die

Appliance für den Call Home Dienst und sendet eine erfolgreiche Registrierungsantwort. Andernfalls sendet der Server eine Registrierungsfehlermeldung zurück. Die grundlegenden Systeminformationen werden als separate Nachricht gesendet. Die Daten enthalten Angaben zur Speicher- und CPU-Auslastung sowie die Durchsatzzahlen. Die Daten werden standardmäßig alle 7 Tage als Teil der Heartbeat-Nachricht gesendet. Ein Wert von weniger als 5 Tagen wird jedoch nicht empfohlen, da häufige Uploads nicht sinnvoll sind.

4. Überwachen Sie kritische Fehlerbedingungen. Nach der Registrierung beginnt Call Home mit der Überwachung der Appliance. In der folgenden Tabelle sind die Bedingungen aufgeführt, die Call Home auf der Appliance überwachen kann.

Kritische Fehlerbedingung	Beschreibung	Überwachungsintervall für Call Home	Entsprechender SNMP-Alarmname
Kompakte Flash-Laufwerkfehler	Auf dem kompakten Flash-Laufwerk der Appliance sind Lese- oder Schreibfehler aufgetreten.	24 Stunden	COMPACT-FLASH-ERRORS
Festplattenfehler	Die Festplatten auf der Appliance haben Lese- oder Schreibfehler festgestellt.	24 Stunden	HARD-DISK-DRIVE-ERRORS
Netzteilausfall	Eines der Netzteile der Citrix ADC Appliance ist fehlgeschlagen.	7 Sekunden	POWER-SUPPLY-FAILURE
SSL-Kartenfehler	Eine der SSL-Karten auf der Citrix ADC Appliance ist fehlgeschlagen.	7 Sekunden	SSL-CARD-FAILED
Warmer Neustart	Die Appliance wurde aufgrund eines Ausfalls eines Systemprozesses warm neu gestartet.	Nach jedem Neustart der Citrix ADC Appliance.	WARM-RESTART-EVENT

Kritische Fehlerbedingung	Beschreibung	Überwachungsintervall für Call Home	Entsprechender SNMP-Alarmname
Fehler bei Speicheranomalien	Die Speicherauslastung steigt schrittweise über ihren normalen Grenzwert und überschreitet den Schwellenwert.	1 Tag	Kein SNMP-Alarm
Rate Limit Paketabfall	Die Grenzwerte für den Durchsatz oder die Grenzwerte für Pakete pro Sekunde (pps) sind erreicht.	7 Sekunden	PF-RL-PPS-PKTS-DROPPED, PF-RL-RATE-PKTS-DROPPED

5. Laden Sie Call Home Daten hoch. Wenn eine der vorherigen kritischen Bedingungen auf der Appliance identifiziert wird, benachrichtigt die Call Home Funktion automatisch den Citrix Support. Die Support-Archive werden auf den Citrix Supportserver hochgeladen. Außerdem können Sie den CALLHOME-UPLOAD-EVENT SNMP-Alarm so konfigurieren, dass eine SNMP-Warnung generiert wird, wenn der Upload von Call Home Die SNMP-Warnung benachrichtigt den lokalen Administrator über das kritische Ereignis.

> **Hinweis:**
>
> Call Home erstellt die Tar-Datei Call Home und lädt sie auf den Citrix Technik-Supportserver hoch, um nur das erste Auftreten einer bestimmten Fehlerbedingung seit dem letzten Neustart zu erreichen. Wenn Sie möchten, dass die Appliance jedes Mal Warnungen sendet, wenn eine bestimmte Fehlerbedingung auftritt, konfigurieren Sie den entsprechenden SNMP-Alarm für die Fehlerbedingung.

6. Erstellen Sie eine Serviceanfrage. Call Home erstellt automatisch eine Serviceanfrage für alle kritischen hardwaretätigen Ereignisse. Die Ereignisse werden klassifiziert als Ausfall der Stromversorgung, SSL-Kartenfehler, Festplattenfehler und Compact-Flash-Fehler. Bei anderen Fehlern können Sie sich nach der Überprüfung der Systemprotokolle an das Citrix Support-Team wenden, um eine Serviceanfrage zur Untersuchung zu stellen.

Call Home konfigurieren

Um Call Home zu konfigurieren, überprüfen Sie die Internetverbindung auf der Appliance und stellen Sie sicher, dass ein DNS-Nameserver konfiguriert ist. Wenn keine Internetverbindung besteht, kon-

figurieren Sie einen Proxyserver oder einen Dienst. Aktivieren Sie dann Call Home auf der Appliance und überprüfen Sie den Registrierungsstatus der Appliance beim Citrix Supportserver. Nach der Registrierung kann Call Home Daten überwachen und hochladen. Darüber hinaus können Sie SNMP-Alarme so konfigurieren, dass der Administrator am Kundenstandort benachrichtigt wird.

Um Call Home zu konfigurieren, können Sie entweder die Citrix ADC -Befehlszeilenschnittstelle oder die GUI verwenden, um die folgenden Aufgaben auszuführen:

- Aktivieren Sie “Call Home”
- Konfigurieren Sie Call Home für optionale Proxyserver-Parameter.
- Überprüfen Sie den Status der Call Home-Registrierung.
- Anzeigen von Fehlern und Zeitstempeldetails.
- Konfigurieren Sie SNMP-Alarme.

So konfigurieren Sie Call Home mit der Citrix ADC Befehlszeilenschnittstelle

Mit der Citrix ADC Befehlszeilenschnittstelle können Sie Folgendes tun:

`Enabling Call Home`

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns feature callhome
```

Call Home für optionale Proxyserver-Parameter konfigurieren

Mit Call Home können Sie den optionalen Proxyserver für die Internetverbindung konfigurieren. Sie können entweder einen Proxyserver mit IP-Adresse und Port konfigurieren oder einen Proxyauthentifizierungsdienst mit unidirektioneller oder bidirektioneller Authentifizierung konfigurieren.

`To configure optional proxy server with IP address and port`

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set callhome -proxyMode ( YES | NO )[-IPAddress <ip_addr|ipv6_addr|*>] [-
port <port |*>]
```

```
1 set callhome  - proxyMode YES  - IPAddress 10.102.167.33  - port 80
2 <!--NeedCopy-->
```

> **Hinweis:**
>
> Call Home verwendet den Proxyserver nur, wenn Sie den Proxy-Mode-Parameter auf YES setzen. Wenn Sie es auf NO setzen, funktioniert die Proxyfunktionalität nicht, selbst wenn IP-Adresse und

> Port konfiguriert sind. Die Portnummer muss für einen HTTP-Dienst und nicht für einen HTTPS-Dienst sein.

So konfigurieren Sie den optionalen Proxyauthentifizierungsdienst

Dieser Modus bietet zwei Arten der Sicherheitsauthentifizierung: unidirektionale und bidirektionale. Um beide Typen einzurichten, müssen Sie einen SSL-Dienst konfigurieren. Weitere Informationen finden Sie unter Konfigurieren eines SSL-Dienstes .

Bei der unidirektionalen Authentifizierung authentifiziert nur die Citrix ADC Appliance den Proxyserver. Bei der bidirektionalen Authentifizierung authentifiziert die Citrix ADC Appliance den Proxyserver und der Proxyserver wiederum authentifiziert die Appliance.

So konfigurieren Sie den Proxyauthentifizierungsdienst

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set callhome -proxyMode ( YES | NO )[-proxyAuthService <string>]
```

```
1 set callhome  - proxyMode YES  - proxyAuthService callhome_proxy
2 <!--NeedCopy-->
```

So konfigurieren Sie die unidirektionale Proxyserver-Authentifizierung

Führen Sie die folgenden Aufgaben aus, um die unidirektionale Proxyserverauthentifizierung zu konfigurieren.

1. Erstellen Sie einen SSL-Dienst.
2. Binden Sie ein Zertifizierungsstellenzertifikat an den Dienst.
3. Binden Sie einen HTTPS-Monitor an den Dienst.
4. Konfigurieren Sie Call Home für die Verwendung des SSL-Dienstes.

So konfigurieren Sie die bidirektionale Proxyserver-Authentifizierung

Führen Sie die folgenden Aufgaben aus, um die bidirektionale Proxyserverauthentifizierung zu konfigurieren.

1. Erstellen eines SSL-Dienstes
2. Binden Sie ein Zertifizierungsstellenzertifikat an den Dienst.
3. Binden Sie ein Clientzertifikat.
4. Binden Sie einen HTTPS-Monitor an den Dienst.
5. Konfigurieren Sie Call Home für die Verwendung des SSL-Dienstes.

Überprüfen des Status der Call Home Registrierung

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
show callhome

    show callhome

     Registration with Citrix upload server SUCCESSFUL

     Mode: Default

     Contact email address: exampleadmin@example.com

     Heartbeat Custom Interval (days): 7

     Proxy Mode: Yes

        Proxy IP Address:10.102.29.200

        Proxy Authentication Service:

        Proxy Port: 80

    Trigger event                  State   First occurrence
                      Latest occurrence

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

     1) Warm boot                  Enabled N/A
                                   ..

     2) Compact flash errors       Enabled ..
                                     ..

     3) Hard disk drive errors     Enabled ..
                                     ..

     4) SSL card failure           N/A     N/A
                                   N/A

     5) Power supply unit failure  N/A     N/A
                                   N/A

     6) Rate limit packet drops    Enabled ..
                                     ..

```



```
37       7) Memory anomaly                Enabled ..
                                            ..
38
39       Done
40  <!--NeedCopy-->
```

> **Hinweis:**
>
> Wenn die Call Home nicht bei CIS registriert werden kann, zeigt die Appliance eine Fehlermeldung an.

Aktivieren von SNMP-Alarmen

Die Citrix ADC Appliance stellt eine Reihe von Fehlerzustands-Entitäten bereit, die *SNMP-Alarme*genannt werden. Wenn eine Fehlerbedingung in einem SNMP-Alarm erfüllt ist, generiert die Appliance SNMP-Trap-Nachrichten, die an die konfigurierten Trap-Listener gesendet werden. Wenn beispielsweise der SSL-CARD-FAILED Alarm aktiviert ist, wird eine Trap-Nachricht generiert und an den Trap-Listener gesendet. Die Trap-Nachricht wird bei jedem Ausfall der SSL-Karte auf der Appliance gesendet. Weitere Informationen finden Sie unter SNMP.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable snmp alarm <trapName>
```

```
show snmp alarm <trapName>
```

So konfigurieren Sie Call Home mit der GUI

So überprüfen Sie, ob die Call Home Funktion in der GUI standardmäßig aktiviert ist

1. Navigieren Sie zu **Konfiguration** > **System** > **Einstellungen**.
2. Klicken Sie im **Detailbereich** auf Link **Erweiterte Funktionen konfigurieren**.
3. Auf der Seite **Erweiterte Funktionen konfigurieren** muss die Option **Call Home** als aktiviert angezeigt werden.

So aktivieren Sie Call Home mit der GUI

1. Navigieren Sie zu **Konfiguration** > **System** > **Einstellungen**.
2. Klicken Sie im **Detailbereich** auf **Erweiterte Funktionen konfigurieren** und wählen Sie **Callhome-Option** aus.

So konfigurieren Sie Call Home für die optionale Proxymodusauthentifizierung mit der GUI

1. Sie können eine der beiden Möglichkeiten verwenden, um auf die Call Home-Seite zuzugreifen:
   a) Navigieren Sie zu **System** > **Systeminformationen**.
   b) Navigieren Sie zu **System** > **Diagnose**.

i. Wählen Sie im Detailbereich unter **Technischer Support Tools** die Option **Call Home** aus.

2. Legen Sie auf der Seite **Call Home konfigurieren** die folgenden Parameter fest.
   a) **Modus**. Call Home-Betriebsmodus. Mögliche Typen: Standardbereitstellung, Citrix Service Provider (CSP).

      > **Hinweis:**
      > Diese Option ist nicht vom Benutzer konfigurierbar. Der Modus wird automatisch festgelegt und basierend auf dem Typ der Citrix ADC Bereitstellung festgelegt.

   b) **E-Mail-Adresse**. E-Mail-Adresse des Kontaktadministrators am Kundenstandort.
   c) **CallHome Heartbeats Intervall (Tage).** Überwachungsintervall (in Tagen) zwischen Call Home Heartbeats. Minimalwert=1 und Maximalwert=7.
   d) **Aktivieren Sie "Call Home**" Aktivieren oder deaktivieren Sie die Funktion Call Home, um den Status der Appliance-Registrierung auf dem Citrix Supportserver anzuzeigen.
   e) **Proxy-Modus**. Wenn Sie keine Internetverbindung haben, aktivieren Sie den Proxy-Modus und legen Sie die optionalen Proxy-Parameter fest.
   f) **Proxyserver**. Wenn Sie den Proxymodus mithilfe eines Proxyservers festlegen, geben Sie die Server-IP-Adresse an.
      i. **Proxy-Dienst**. Wenn Sie den Proxy-Modus mithilfe eines Proxy-Dienstes festlegen, geben Sie den Dienstnamen an.
      ii. **IP Adresse**. IP-Adresse des Proxyservers.
      iii. **Port**. Portnummer des Proxyservers.
      iv. **Proxy-Authentifizierungs-SSL-Dienst**. Der Name des Proxy-Dienstes, der Proxy-Modus-Authentifizierung bereitstellt.
3. Klicken Sie auf **OK** und **Fertig**.

So konfigurieren Sie den SSL-Dienst für die Proxyserver-Authentifizierung mit der GUI

Informationen zum Konfigurieren des SSL-Dienstes über die grafische Benutzeroberfläche finden Sie unter Konfigurieren eines SSL-Dienstes .

So überprüfen Sie den Registrierungsstatus von Call Home über die GUI

1. Sie können eine der beiden Möglichkeiten verwenden, um auf die **Call Home**-Seite zuzugreifen:
   a) Navigieren Sie zu **System** > **Systeminformationen**.
   b) Navigieren Sie zu **System** > **Diagnose**.
      i. Wählen Sie im Detailbereich unter **Technischer Support Tools** die Option **Call Home** aus.
2. Auf der Seite **"Call Home konfigurieren** " zeigt das Feld " **Registrierung bei Citrix Upload Server** " den Registrierungsstatus an.

So konfigurieren Sie einen SNMP-Alarm

1. Navigieren Sie zu **System** > **SNMP** > **Alarms**.

2. Wählen Sie im Detailbereich einen Alarm aus, und konfigurieren Sie dessen Parameter.
3. Klicken Sie auf **OK** und **schließen**.

Unterstützung für die Bereitstellung von Citrix Service Provider (CSP)

In einer Citrix Service Provider (CSP) Umgebung, in der Citrix ADC Dienste auf VPX-Instanzen bereitgestellt werden, kann Call Home die lizenzspezifischen Informationen überwachen und verfolgen und die Informationen sicher an Citrix Insight Services (CIS) senden. CIS wiederum sendet die Informationen zu Buchhaltungszwecken an das License Usage Insights (LUI)-Portal und damit CSP-Kunden ihre Lizenzverwendung überprüfen können. Derzeit unterstützen CSP-Umgebungen Citrix ADC Dienste nur auf VPX-Instanzen, nicht auf MPX- oder SDX-Appliances. Die VPX-Instanzen können entweder im Standalone-Modus oder im Hochverfügbarkeitsmodus bereitgestellt werden.

Reporting-Tool

October 5, 2021

Verwenden Sie das Citrix® Citrix ADC® Reporting Tool, um Citrix ADC Performance-Statistiken als Berichte anzuzeigen. Statistikdaten werden vom `nscollect` Dienstprogramm gesammelt und in einer Datenbank gespeichert. Wenn Sie bestimmte Leistungsdaten über einen Zeitraum hinweg anzeigen möchten, zieht das Reporting Tool bestimmte Daten aus der Datenbank heraus und zeigt sie in Diagrammen an.

Berichte sind eine Sammlung von Diagrammen. Das Reporting-Tool bietet integrierte Berichte und die Option zum Erstellen benutzerdefinierter Berichte. In einem Bericht können Sie die Diagramme ändern und neue Diagramme hinzufügen. Sie können auch den Betrieb des Datenerfassungsdienstprogramms ändern und seinen Betrieb beenden oder starten. `nscollect`

Verwenden des Berichtswerkzeugs

Das Reporting Tool ist eine webbasierte Schnittstelle, auf die von der Citrix® Citrix ADC® Appliance aus zugegriffen wird. Verwenden Sie das Tool Berichterstellung, um die Performance-Statistikdaten als Berichte anzuzeigen, die Grafiken enthalten. Zusätzlich zur Verwendung der integrierten Berichte können Sie benutzerdefinierte Berichte erstellen, die Sie jederzeit ändern können. Berichte können zwischen einem und vier Diagrammen haben. Sie können bis zu 256 benutzerdefinierte Berichte erstellen. Sie können einen benutzerdefinierten Bericht für eine beliebige Anzahl von Entitäten erstellen.

So rufen Sie das Berichts-Tool auf

1. Verwenden Sie den Webbrowser Ihrer Wahl, um eine Verbindung mit der IP-Adresse des Citrix ADC herzustellen (z. B. `http://10.102.29.170/`). Das Fenster Webanmeldung wird angezeigt.
2. Geben Sie im Textfeld Benutzername den Benutzernamen ein, der dem Citrix ADC zugewiesen ist.
3. Geben Sie im Textfeld Kennwort das Kennwort ein.
4. Wählen Sie im Dropdownlistenfeld Start in die Option Reporting.Klicken Sie auf Anmelden.

Die folgenden Screenshots zeigen die Berichtssymbolleiste und die Diagrammsymbolleiste, auf die in dieser Dokumentation häufig verwiesen wird.

Abbildung 1. *Bericht-Symbolleiste*

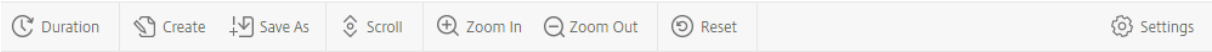
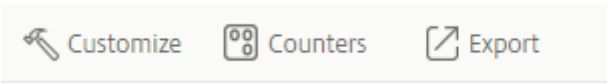


Abbildung 2. *Diagramm-Symbolleiste*



Arbeiten mit Berichten

Sie können Statistiken für die verschiedenen auf dem Citrix ADC konfigurierten Funktionsgruppen über ein bestimmtes Zeitintervall darstellen und überwachen. Berichte ermöglichen es Ihnen, das Verhalten Ihrer Appliance zu beheben oder zu analysieren. Es gibt zwei Arten von Berichten: integrierte Berichte und benutzerdefinierte Berichte. Berichtsinhalte für integrierte oder benutzerdefinierte Berichte können in einem grafischen oder tabellarischen Format angezeigt werden. Die grafische Ansicht besteht aus Linien-, Flächen- und Balkendiagrammen, die bis zu 32 Datensätze (Zähler) anzeigen können. Die tabellarische Ansicht zeigt die Daten in Spalten und Zeilen an. Diese Ansicht ist nützlich, um Fehlerindikatoren zu debuggen.

Der Standardbericht, der im Reporting-Tool angezeigt wird, ist CPU vs. Speicherauslastung und HTTP-Anforderungen Rate. Sie können die Standardberichtansicht ändern, indem Sie den gewünschten Bericht als Standardansicht anzeigen und dann auf Standardbericht klicken.

Berichte können für die letzte Stunde, den letzten Tag, die letzte Woche, den letzten Monat, das letzte Jahr erstellt werden, oder Sie können die Dauer anpassen.

Mit Berichten können Sie Folgendes tun:

- Wechseln Sie zwischen einer tabellarischen Ansicht der Daten und einer grafischen Ansicht der Daten.
- Ändern Sie den grafischen Anzeigetyp, z. B. Balkendiagramm oder Liniendiagramm.

- Anpassen von Diagrammen in einem Bericht.
- Exportieren Sie das Diagramm als CSV-Datei (Comma Separated Value) von Excel.
- Zeigen Sie die Diagramme im Detail an, indem Sie hineinzoomen, verkleinern oder einen Drag-Vorgang verwenden (Scrollen).
- Legen Sie einen Bericht als Standardbericht für die Anzeige bei jeder Anmeldung fest.
- Hinzufügen oder Entfernen von Leistungsindikatoren.
- Berichte drucken.
- Aktualisieren Sie Berichte, um die neuesten Performance-Daten anzuzeigen.

Integrierte Berichte verwenden

Das Reporting-Tool bietet integrierte Berichte für häufig angezeigte Daten. Integrierte Berichte sind für die folgenden Funktionsgruppen verfügbar: System, Netzwerk, SSL, Komprimierung, Integrierter Cache, Citrix ADC Gateway und Citrix ADC Application Firewall. Standardmäßig werden die integrierten Berichte für den letzten Tag angezeigt. Sie können jedoch die Berichte für die letzte Stunde, die letzte Woche, den letzten Monat oder das letzte Jahr anzeigen.

> **Hinweis**:
>
> Sie können keine Änderungen an integrierten Berichten speichern, aber Sie können einen geänderten integrierten Bericht als benutzerdefinierten Bericht speichern.

So zeigen Sie einen integrierten Bericht an

1. Erweitern Sie im linken Bereich des Berichtsprogramms unter Integrierte Berichte eine Gruppe (z. B. SSL).
2. Klicken Sie auf einen Bericht (z. B. **SSL > Alle Backend-Ciphers)**.

Erstellen und Löschen von Berichten

Sie können eigene benutzerdefinierte Berichte erstellen und sie mit benutzerdefinierten Namen zur Wiederverwendung speichern. Sie können verschiedene Zähler für verschiedene Gruppen basierend auf Ihren Anforderungen plotten. Sie können bis zu 256 benutzerdefinierte Berichte erstellen.

Sie können entweder einen neuen Bericht erstellen oder einen integrierten Bericht als benutzerdefinierten Bericht speichern. Standardmäßig enthält ein neu erstellter benutzerdefinierter Bericht ein Diagramm mit dem Namen Systemübersicht, in dem der Zähler CPU-Auslastung angezeigt wird, der für den letzten Tag gezeichnet wurde. Sie können das Intervall anpassen und die Datenquelle und Zeitzone über die Berichtssymbolleiste festlegen.

So erstellen Sie einen benutzerdefinierten Bericht

1. Klicken Sie im **Berichts-Tool** auf der Berichtssymbolleiste auf **Erstellen**, oder wenn Sie einen neuen benutzerdefinierten Bericht basierend auf einem vorhandenen Bericht erstellen möchten, öffnen Sie den vorhandenen Bericht, und klicken Sie dann auf **Speichern unter** .
2. Geben Sie im Feld **Berichtsname** einen Namen für den benutzerdefinierten Bericht ein.
3. Führen Sie einen der folgenden Schritte aus:
   - Um den Bericht einem vorhandenen Ordner hinzuzufügen, klicken Sie unter Erstellen in oder Speichern in auf den Pfeil nach unten, um einen vorhandenen Ordner auszuwählen, und klicken Sie dann auf **OK**.
   - Um einen neuen Ordner zum Speichern des Berichts zu erstellen, klicken Sie auf das Symbol Klicken Sie auf Ordner hinzufügen, geben Sie unter Ordnername den Namen des Ordners ein, und geben Sie unter Erstellen in an, wo der neue Ordner in der Hierarchie gespeichert werden soll, und klicken Sie dann auf **OK**.

> **Hinweis**:
> Sie können bis zu 128 Ordner erstellen.

So löschen Sie einen benutzerdefinierten Bericht

1. Klicken Sie im linken Bereich des Berichtstools neben Benutzerdefinierte Berichte auf das Symbol Klicken, um das Symbol für benutzerdefinierte Berichte zu verwalten.
2. Aktivieren Sie das Kontrollkästchen, das dem Bericht entspricht, den Sie löschen möchten, und klicken Sie dann auf Löschen.

   > **Hinweis**:
   >
   > Wenn Sie einen Ordner löschen, werden alle Inhalte dieses Ordners gelöscht.

Ändern des Zeitintervalls

Standardmäßig werden in integrierten Berichten Daten für den letzten Tag angezeigt. Wenn Sie jedoch das Zeitintervall für einen integrierten Bericht ändern möchten, können Sie den Bericht als benutzerdefinierten Bericht speichern. Das neue Intervall gilt für alle Diagramme im Bericht. In der folgenden Tabelle werden die Optionen für das Zeitintervall beschrieben.

So ändern Sie das Zeitintervall

1. Klicken Sie im linken Bereich des Berichtsprogramms auf einen Bericht.
2. Klicken Sie auf der Berichtssymbolleiste auf **Dauer**, und klicken Sie dann auf ein Zeitintervall.

Festlegen der Datenquelle und Zeitzone

Sie können Daten aus verschiedenen Datenquellen abrufen, um sie in den Berichten anzuzeigen. Sie können auch die Zeitzone für die Berichte definieren und die Zeitauswahl des aktuell angezeigten Berichts auf alle Berichte anwenden, einschließlich der integrierten Berichte.

So legen Sie die Datenquelle und die Zeitzone fest

1. Klicken Sie im **Berichts-Tool**auf der Berichtssymbolleiste auf **Einstellungen**.
2. Wählen Sie im Dialogfeld **Einstellungen unter** Datenquelle die Datenquelle aus, aus der Sie die Leistungsindikatorinformationen abrufen möchten.
3. Führen Sie eine oder beide der folgenden Aktionen aus:
   - Wenn das Werkzeug den Zeitraum merken soll, für den ein Diagramm gezeichnet wird, aktivieren Sie das Kontrollkästchen **Zeitauswahl für Diagramme speichern** .
   - Wenn die Berichte die Zeiteinstellungen Ihrer Citrix ADC Appliance verwenden sollen, aktivieren Sie das Kontrollkästchen **Zeitzone der Appliance verwenden** .

Exportieren und Importieren von benutzerdefinierten Berichten

Sie können Berichte für andere Citrix ADC Administratoren freigeben, indem Sie Berichte exportieren. Sie können auch Berichte importieren.

So exportieren oder importieren Sie benutzerdefinierte Berichte

1. Klicken Sie im linken Bereich des Berichtstools neben Benutzerdefinierte Berichte auf das Symbol **Klicken Sie zum Verwalten benutzerdefinierter Berichte**.
2. Aktivieren Sie das Kontrollkästchen, das dem Bericht entspricht, den Sie exportieren oder importieren möchten, und klicken Sie dann auf **Exportieren** oder **Importieren** .

   > **Hinweis**:
   >
   > Wenn Sie die Datei exportieren, wird sie in ein GZ-Dateiformat exportiert.

Arbeiten mit Diagrammen

Verwenden Sie Diagramme, um Leistungsindikatoren oder Gruppen von Leistungsindikatoren darzustellen und zu überwachen. Sie können bis zu vier Diagramme in einen Bericht aufnehmen. In jedem Diagramm können Sie bis zu 32 Zähler darstellen. Die Diagramme können verschiedene grafische Formate verwenden (z. B. Bereich und Balken) Sie können die Diagramme innerhalb des Berichts nach oben oder unten verschieben, die Farben und die visuelle Anzeige für jeden Leistungsindikator in einem Diagramm anpassen und ein Diagramm löschen, wenn Sie es nicht überwachen möchten.

In allen Berichtsdiagrammen stellt die horizontale Achse die Zeit und die vertikale Achse den Wert des Zählers dar.

Hinzufügen eines Diagramms

Wenn Sie einem Bericht ein Diagramm hinzufügen, wird das Diagramm Systemübersicht mit dem Leistungsindikator CPU-Auslastung für den letzten Tag angezeigt.

> **Hinweis**:
>
> Wenn Sie einem integrierten Bericht Diagramme hinzufügen und den Bericht beibehalten möchten, müssen Sie den Bericht als benutzerdefinierten Bericht speichern.

Gehen Sie wie folgt vor, um einem Bericht ein Diagramm hinzuzufügen.

So fügen Sie einem Bericht ein Diagramm hinzu

1. Klicken Sie im linken Bereich des Berichtsprogramms auf einen Bericht.
2. Klicken Sie unter dem Diagramm, in dem Sie das neue Diagramm hinzufügen möchten, auf das Symbol Hinzufügen.

Ändern eines Diagramms

Sie können ein Diagramm ändern, indem Sie die Funktionsgruppe ändern, für die die Statistiken angezeigt werden, und indem Sie verschiedene Leistungsindikatoren auswählen.

So ändern Sie ein Diagramm

1. Klicken Sie im linken Bereich des Berichtsprogramms auf einen Bericht.
2. Klicken Sie unter dem Diagramm, das Sie ändern möchten, auf Leistungsindikatoren.
3. Geben Sie im angezeigten Dialogfeld im Feld Titel einen Namen für das Diagramm ein.
4. Führen Sie neben dem Plotdiagramm für einen der folgenden Schritte aus:
   - Klicken Sie auf Globale Systemstatistiken, um Leistungsindikatoren für globale Leistungsindikatoren wie Integrierter Cache und Komprimierung zu plotten.
   - Um Entitätsindikatoren für Entitätstypen wie Lastenausgleich und GSLB zu plotten, klicken Sie auf Systementitätsstatistik.
5. Klicken Sie in der Gruppe Auswählen auf die gewünschte Entität.
6. Klicken Sie unter Zähler unter Verfügbar auf einen oder mehrere Zählernamen, die Sie plotten möchten, und klicken Sie dann auf die Schaltfläche >.
7. Wenn Sie in Schritt 4 System-Entitätsstatistiken ausgewählt haben, klicken Sie auf der Registerkarte Entitäten unter Verfügbar auf einen oder mehrere Entitätsinstanznamen, die Sie plotten möchten, und klicken Sie dann auf die Schaltfläche >.

8. Klicken Sie auf OK.

Anzeigen eines Diagramms

Sie können die grafischen Formate der gezeichneten Leistungsindikatoren in einem Diagramm angeben. Diagramme können als Liniendiagramme, Spline-Diagramme, Schrittliniendiagramme, Streudiagramme, Flächendiagramme, Balkendiagramme, gestapelte Flächendiagramme und gestapelte Balkendiagramme angezeigt werden. Sie können auch innerhalb der Zeichnungsfläche eines Diagramms vergrößern, verkleinern oder einen Bildlauf durchführen. Sie können für alle Datenquellen 1 Stunde, 1 Tag, 1 Woche, 1 Monat, 1 Jahr und 3 Jahre verkleinern oder verkleinern.

Weitere Optionen zum Anpassen der Ansicht eines Diagramms umfassen das Anpassen der Achsen der Diagramme, das Ändern der Hintergrundfarbe und der Kantenfarbe der Zeichnungsfläche, das Anpassen der Farbe und Größe der Gitter und das Anpassen der Anzeige jedes Datensatzes (Zählers) in einem Diagramm.

Datensatznummern, z. B. Datensatz 1, entsprechen der Reihenfolge, in der die Zähler im Diagramm am unteren Rand des Diagramms angezeigt werden. Wenn beispielsweise CPU-Auslastung und Speicherauslastung in erster und zweiter Reihenfolge unten im Diagramm angezeigt werden, ist die CPU-Auslastung gleich Datensatz 1 und Speicherauslastung gleich Datensatz 2.

Wenn Sie einen integrierten Bericht ändern, müssen Sie den Bericht als benutzerdefinierten Bericht speichern, um Ihre Änderungen beizubehalten.

So ändern Sie den Diagrammtyp eines Diagramms

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Fensterbereich unter dem Diagramm, das Sie anzeigen möchten, auf der Symbolleiste des Diagramms auf **Anpassen**.
3. Klicken Sie auf der Registerkarte **Diagramm** unter **Kategorie** auf **Plottyp**, und klicken Sie dann auf den Diagrammtyp, den Sie für das Diagramm anzeigen möchten. Wenn Sie das Diagramm 3D anzeigen möchten, aktivieren Sie das Kontrollkästchen 3D verwenden.

So richten Sie ein Diagramm mit detaillierten Daten neu aus

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Fensterbereich auf der Berichtssymbolleiste auf **Vergrößern**, und führen Sie eine oder beide der folgenden Aktionen aus:
    - Um das Diagramm neu zu fokussieren, um Daten für ein bestimmtes Zeitfenster anzuzeigen, ziehen Sie den Cursor von der Startzeit zur Endzeit. Beispielsweise können Sie Daten für einen Zeitraum von einer Stunde an einem bestimmten Tag anzeigen.

- Um das Diagramm neu zu fokussieren, um Daten für einen Datenpunkt anzuzeigen, klicken Sie einfach einmal auf das Diagramm, in dem Sie vergrößern möchten, und erhalten Sie detailliertere Informationen.

3. Wenn Sie über den gewünschten Zeitraum verfügen, für den Sie detaillierte Daten anzeigen möchten, klicken Sie auf der Berichtssymbolleiste auf Tabellarische Ansicht. Tabellarische Ansicht zeigt die Daten in numerischer Form in Zeilen und Spalten an.

So zeigen Sie numerische Daten für ein Diagramm an

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Fensterbereich auf der Berichtssymbolleiste auf Tabellarische Ansicht. Um zur grafischen Ansicht zurückzukehren, klicken Sie auf **Grafische Ansicht**.

> **Hinweis**: Sie können die numerischen Daten auch in der grafischen Ansicht anzeigen, indem Sie den Cursor über die Kerben in den Gitternetzlinien bewegen.

So scrollen Sie durch die Zeit in einem Diagramm

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Fensterbereich auf der Berichtssymbolleiste auf **Bildlauf**, und klicken Sie dann in das Diagramm, und ziehen Sie den Cursor in die Richtung, für die Sie Daten für einen neuen Zeitraum anzeigen möchten. Wenn Sie beispielsweise Daten in der Vergangenheit anzeigen möchten, ziehen Sie nach links.

So ändern Sie die Hintergrundfarbe und die Textfarbe eines Diagramms

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Fensterbereich unter dem Diagramm, für das Sie die Achsen anpassen möchten, auf **Anpassen**.
3. Klicken Sie auf der Registerkarte **Diagramm** unter **Kategorie**auf eine oder mehrere der folgenden Optionen:
   - Um die Hintergrundfarbe zu ändern, klicken Sie auf **Hintergrundfarbe**, und wählen Sie dann die Optionen für Farbe, Transparenz und Effekte aus.
   - Um die Textfarbe zu ändern, klicken Sie auf **Textfarbe**, und wählen Sie dann die Optionen für Farbe, Transparenz und Effekte aus.

So passen Sie die Achsen eines Diagramms an

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Fensterbereich unter dem Diagramm, für das Sie die Achsen anpassen möchten, auf **Anpassen**.

3. Klicken Sie auf der Registerkarte **Diagramm** unter Kategorie auf eine oder mehrere der folgenden Optionen:
   - Um den Maßstab der linken Y-Achse zu ändern, klicken Sie auf **Linke Y-Achse**, und wählen Sie dann den gewünschten Maßstab aus.
   - Um den Maßstab der rechten Y-Achse zu ändern, klicken Sie auf Y-Achse rechts, wählen Sie im zu plotgenden Datensatz den Datumssatz aus, und wählen Sie dann den gewünschten Maßstab aus.

     > Hinweis:
     > Die Datensatznummern, z. B. Datensatz 1, entsprechen der Reihenfolge, in der die Zähler im Diagramm am unteren Rand des Diagramms angezeigt werden. Wenn beispielsweise CPU-Auslastung und Speicherauslastung in erster und zweiter Reihenfolge unten im Diagramm angezeigt werden, ist die CPU-Auslastung gleich Datensatz 1 und Speicherauslastung gleich Datensatz 2.

   - Um jeden Datensatz in einer eigenen ausgeblendeten Y-Achse zu zeichnen, klicken Sie auf Mehrere Achsen, und klicken Sie dann auf Aktivieren.

So ändern Sie die Hintergrundfarbe, die Kantenfarbe und die Gitternetzlinien für eine Zeichnungsfläche eines Diagramms

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Fensterbereich unter dem Diagramm, für das Sie die Zeichnungsfläche anpassen möchten, auf **Anpassen**.
3. Klicken Sie auf der Registerkarte **Plotfläche** unter Kategorie auf eine oder mehrere der folgenden Optionen:
   - Um die Hintergrundfarbe und die Kantenfarbe des Diagramms zu ändern, klicken Sie auf **Hintergrundfarbe und Kantenfarbe**, und wählen Sie dann die Optionen für Farbe, Transparenz und Effekte aus.
   - Um die horizontalen oder vertikalen Raster des Diagramms zu ändern, klicken Sie auf **Horizontale Raster** oder **Vertikale Raster**, und wählen Sie dann die Optionen zum Anzeigen der Raster, der Rasterbreite, der Rasterfarbe, der Transparenz und der Effekte aus.

So ändern Sie die Farbe und den Diagrammtyp eines Datensatzes

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Fensterbereich unter dem Diagramm, für das Sie die Anzeige des Datensatzes (Leistungsindikatoren) anpassen möchten, auf **Anpassen**.
3. Wählen Sie auf der Registerkarte **Datensatz** unter Datensatz auswählen den Datensatz (Leistungsindikator) aus, für den Sie die grafische Anzeige anpassen möchten.
   Hinweis: Die Datensatznummern, z. B. Datensatz 1, entsprechen der Reihenfolge, in der die Zähler im Diagramm am unteren Rand des Diagramms angezeigt werden. Wenn beispielsweise

CPU-Auslastung und
Speicherauslastung in erster und zweiter Reihenfolge unten im Diagramm angezeigt werden, ist die
CPU-Auslastung gleich
Datensatz 1 und
Speicherauslastung gleich
Datensatz 2.

4. Führen Sie unter Kategorie eine der folgenden Aktionen aus:
   - Um die Hintergrundfarbe zu ändern, klicken Sie auf **Farbe**, und wählen Sie dann die Optionen für Farbe, Transparenz und Effekte aus.
   - Um den Diagrammtyp zu ändern, klicken Sie auf **Plottyp**, und wählen Sie dann den Diagrammtyp aus, den Sie für den Datensatz anzeigen möchten. Wenn Sie das Diagramm als 3D anzeigen möchten, aktivieren Sie das Kontrollkästchen 3D verwenden.

Exportieren von Diagrammdaten nach Excel

Zur weiteren Datenanalyse können Sie Diagramme im CSV-Format (kommagetrennte Werte) nach Excel exportieren.

So exportieren Sie Diagrammdaten in Excel

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Fensterbereich unter dem Diagramm mit den Daten, die Sie nach Excel exportieren möchten, auf **Exportieren**.

Löschen eines Diagramms

Wenn Sie kein Diagramm verwenden möchten, können Sie es aus dem Bericht entfernen. Sie können Diagramme nur dauerhaft aus benutzerdefinierten Berichten entfernen. Wenn Sie ein Diagramm aus einem integrierten Bericht löschen und die Änderungen beibehalten möchten, müssen Sie den Bericht als benutzerdefinierten Bericht speichern.

So löschen Sie ein Diagramm

1. Wählen Sie im linken Bereich des Berichtsprogramms einen Bericht aus.
2. Klicken Sie im rechten Fensterbereich unter dem Diagramm, das Sie löschen möchten, auf das Symbol **Löschen** .

Beispiele

So zeigen Sie den Trendbericht zur CPU-Auslastung und Speicherauslastung der letzten Woche an

1. Erweitern Sie im linken Bereich des Berichtsprogramms unter Integrierte Berichte den Eintrag System.
2. Klicken Sie auf den Bericht CPU vs. Speicherauslastung und HTTP-Anforderungen Rate.
3. Klicken Sie im rechten Bereich auf der Berichtssymbolleiste auf **Dauer**, und klicken Sie dann auf **Letzte Woche**.

Um die empfangene Bytes Rate und die übertragene Bytes zwischen den beiden Schnittstellen für die letzte Woche zu vergleichen

1. Klicken Sie im rechten Fensterbereich auf der Berichtssymbolleiste auf Erstellen.
2. Geben Sie im Feld **Berichtsname** einen Namen für den benutzerdefinierten Bericht ein (z. B. Custom_Interfaces), und klicken Sie dann auf **OK** . Der Bericht wird mit dem Standarddiagramm Systemübersicht erstellt, in dem der für die letzte Stunde geplottete CPU-Auslastung angezeigt wird.
3. Klicken Sie unter Systemübersicht auf der Diagrammsymbolleiste auf Leistungsindikatoren.
4. Geben Sie im Bereich der Leistungsindikatorenauswahl unter Titel einen Namen für das Diagramm ein (z. B. Schnittstellenbytedaten)
5. Klicken Sie im Diagramm für auf Systementitätsstatistik, und wählen Sie dann unter Gruppe auswählen die Option Schnittstelle aus.
6. Klicken Sie auf der Registerkarte **Entitäten** auf einen oder mehrere Schnittstellennamen, die Sie plotten möchten (z. B. 1/1 und 1/2), und klicken Sie dann auf die Schaltfläche >.
7. Klicken Sie auf der Registerkarte Leistungsindikatoren auf empfangene Bytes (Rate) und übertragene Bytes (Rate), und klicken Sie dann auf die Schaltfläche >.
8. Klicken Sie auf **OK**.
9. Klicken Sie auf der Berichtssymbolleiste auf **Dauer**, und klicken Sie dann auf **Letzte Woche**.

Stoppen und Starten des Datenerfassungsdienstprogramms

Das Dienstprogramm zur Datenerfassung wird automatisch ausgeführt `nscollect`, wenn Sie den Citrix ADC starten. Dieses Dienstprogramm ruft die Anwendungsleistungsdaten ab und speichert sie in Form von Datenquellen auf dem ADC. Sie können bis zu 32 Datenquellen erstellen. Die Standarddatenquelle ist `/var/log/db/default`.

Das Datenerfassungsdienstprogramm erstellt Datenbanken für globale Leistungsindikatoren und entity-spezifische Leistungsindikatoren und verwendet diese Daten, um Berichte zu generieren. Global-Counter-Datenbanken werden unter erstellt `/var/log/db/<DataSourceName>`. Die

entity-spezifischen Datenbanken werden basierend auf den Entitäten erstellt, die auf dem Citrix ADC konfiguriert sind, und für jeden Entitätstyp in `/var/log/db/<DataSourceName/EntityNameDB>` wird ein separater Ordner erstellt.

Der `nscollect` ruft alle 5 Minuten Daten ab. Es speichert Daten in 5-Minuten-Granularität für einen Tag, stündlich für die letzten 30 Tage und täglich für drei Jahre.

Möglicherweise müssen Sie das Datenerfassungsdienstprogramm anhalten und neu starten, wenn die Daten nicht korrekt aktualisiert werden oder die Berichte beschädigte Daten anzeigen.

Um anzuhalten `nscollect`

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
/netscaler/nscollect stop
```

So starten Sie nscollect in der aktuellen SSH-Sitzung mit dem Citrix ADC:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
/netscaler/nscollect start
```

So starten Sie nscollect auf dem lokalen System:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
/netscaler/nscollect start &
```

CloudBridge-Connector

October 5, 2021

Hinweis: Die aktuelle Version von Citrix ADC 1000V unterstützt diese Funktion nicht.

Die CloudBridge Connector-Funktion der Citrix ADC Appliance verbindet Rechenzentren von Unternehmen mit externen Clouds und Hosting-Umgebungen und macht die Cloud zu einer sicheren Erweiterung Ihres Unternehmensnetzwerks. Cloud-gehostete Anwendungen werden so angezeigt, als ob sie in einem zusammenhängenden Unternehmensnetzwerk ausgeführt würden. Mit Citrix CloudBridge Connector können Sie Ihre Rechenzentren um die Kapazität und Effizienz von Cloud-Anbietern erweitern.

Mit dem CloudBridge Connector können Sie Ihre Anwendungen in die Cloud verschieben, um Kosten zu senken und die Zuverlässigkeit zu erhöhen.

Zusätzlich zur Verwendung von CloudBridge Connector zwischen einem Rechenzentrum und einer Cloud können Sie damit zwei Rechenzentren für eine sichere und beschleunigte Verbindung mit hoher Kapazität verbinden.

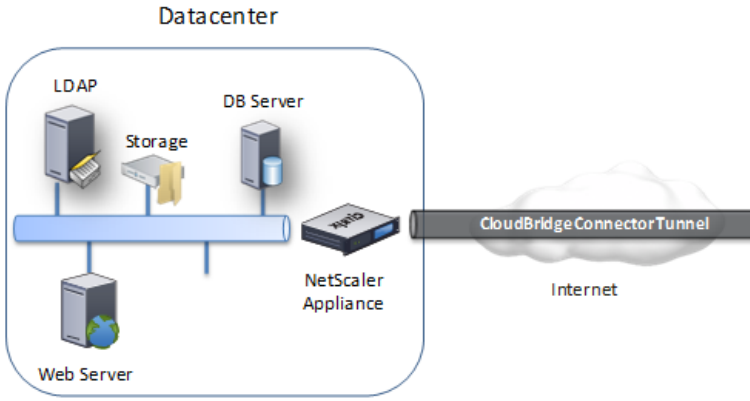
Grundlegendes zu CloudBridge Connector

Um die Citrix CloudBridge Connector-Lösung zu implementieren, verbinden Sie ein Datencenter mit einem anderen Datencenter oder einer externen Cloud, indem Sie einen Tunnel namens CloudBridge Connector-Tunnel einrichten.

Um ein Datencenter mit einem anderen Datencenter zu verbinden, richten Sie einen CloudBridge Connector-Tunnel zwischen zwei Citrix ADC Appliances ein, eine in jedem Rechenzentrum.

Um ein Rechenzentrum mit einer externen Cloud (z. B. Amazon AWS-Cloud) zu verbinden, richten Sie einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance im Rechenzentrum und einer virtuellen Appliance (VPX) ein, die sich in der Cloud befindet. Der Remote-Endpunkt kann ein CloudBridge Connector oder ein Citrix ADC VPX mit Premium-Lizenz sein.

Die folgende Abbildung zeigt einen CloudBridge Connector-Tunnel, der zwischen einem Rechenzentrum und einer externen Cloud eingerichtet wurde.



Die Appliances, zwischen denen ein CloudBridge Connector-Tunnel eingerichtet ist, werden als *Endpunkte* oder *Peers* des CloudBridge Connector-Tunnels bezeichnet.

Ein CloudBridge Connector-Tunnel verwendet die folgenden Protokolle:

- Generisches Routing Encapsulation (GRE) -Protokoll
- Open-Standard-IPsec-Protokoll-Suite, im Transportmodus

Das GRE-Protokoll bietet einen Mechanismus zum Einkapseln von Paketen aus einer Vielzahl von Netzwerkprotokollen, die über ein anderes Protokoll weitergeleitet werden. GRE wird verwendet, um:

- Verbinden Sie Netzwerke mit Nicht-IP- und nicht-routingfähigen Protokollen.
- Brücke über ein WAN (Wide Area Network).
- Erstellen Sie einen Transporttunnel für jede Art von Datenverkehr, der unverändert über ein anderes Netzwerk gesendet werden muss.

Das GRE-Protokoll kapselt Pakete, indem ein GRE-Header und ein GRE-IP-Header zu den Paketen hinzugefügt wird.

Die IPsec-Protokollsuite (Internet Protocol Security) sichert die Kommunikation zwischen Peers im CloudBridge Connector-Tunnel.

In einem CloudBridge Connector-Tunnel stellt IPsec Folgendes sicher:

- Datenintegrität
- Datenursprungauthentifizierung
- Datenvertraulichkeit (Verschlüsselung)
- Schutz vor Replay-Angriffen

IPsec verwendet den Transportmodus, in dem das gekapselte GRE-Paket verschlüsselt ist. Die Verschlüsselung erfolgt durch das ESP-Protokoll (Encapsulating Security Payload). Das ESP-Protokoll stellt die Integrität des Pakets mithilfe einer HMAC-Hash-Funktion sicher und gewährleistet die Vertraulichkeit mithilfe eines Verschlüsselungsalgorithmus. Nachdem das Paket verschlüsselt und der HMAC berechnet wurde, wird ein ESP-Header generiert. Der ESP-Header wird nach dem GRE-IP-Header eingefügt und am Ende der verschlüsselten Nutzlast wird ein ESP-Trailer eingefügt.

Peers im CloudBridge Connector-Tunnel verwenden das IKE-Protokoll (Internet Key Exchange Version) (Teil der IPsec-Protokollsuite), um eine sichere Kommunikation auszuhandeln, wie folgt:

- Die beiden Peers authentifizieren sich gegenseitig mit einer der folgenden Authentifizierungsmethoden:
  - **Authentifizierung mit vorab freigegebenen Schlüsseln**. Eine Textzeichenfolge, die als Pre-Shared Key bezeichnet wird, wird auf jedem Peer manuell konfiguriert. Die vorab geteilten Schlüssel der Peers werden zur Authentifizierung gegeneinander zugeordnet. Damit die Authentifizierung erfolgreich ist, müssen Sie daher den gleichen vorab freigegebenen Schlüssel auf jedem Peers konfigurieren.
  - **Digitale Zertifikatauthentifizierung**. Der Initiator (Absender) Peer signiert Nachrichtenaustauschdaten mithilfe seines privaten Schlüssels, und der andere Empfängerpeer verwendet den öffentlichen Schlüssel des Absenders, um die Signatur zu überprüfen. Normalerweise wird der öffentliche Schlüssel in Nachrichten ausgetauscht, die ein X.509v3-Zertifikat enthalten. Dieses Zertifikat bietet eine Sicherheitsstufe, dass die Identität eines Peers, wie im Zertifikat dargestellt, einem bestimmten öffentlichen Schlüssel zugeordnet ist.
- Die Kollegen verhandeln dann, um eine Einigung zu erzielen über:
  - Ein Verschlüsselungsalgorithmus.
  - Kryptografische Schlüssel zum Verschlüsseln von Daten in einem Peer und zum Entschlüsseln der Daten in der anderen.

Diese Vereinbarung über das Sicherheitsprotokoll, den Verschlüsselungsalgorithmus und die kryptografischen Schlüssel wird als Security Association (SA) bezeichnet. SAs sind einseitig (Simplex).

Wenn beispielsweise zwei Peers, CB1 und CB2, über einen Connector-Tunnel kommunizieren, verfügt CB1 über zwei Sicherheitszuordnungen. Eine SA wird für die Verarbeitung ausgehender Pakete verwendet, und die andere SA wird für die Verarbeitung eingehender Pakete verwendet.

SAs verfallen nach einer bestimmten Zeitspanne, die als *Lebensdauer*bezeichnet wird. Die beiden Peers verwenden das IKE-Protokoll (Internet Key Exchange) (Teil der IPsec-Protokollsuite), um neue kryptografische Schlüssel auszuhandeln und neue SAs einzurichten. Der Zweck der begrenzten Lebensdauer ist es, Angreifer daran zu hindern, einen Schlüssel zu knacken.

In der folgenden Tabelle sind einige IPsec-Vorteile aufgeführt, die von einer Citrix ADC Appliance unterstützt werden:

IPsec-Eigenschaften	Unterstützte Typen
IKE-Versionen	V1, V2
IKE DH-Gruppe	Eine Citrix ADC Appliance unterstützt nur die DH-Gruppe 2 (1024-Bit-MODP-Algorithmus) sowohl für iKEV1 als auch für iKEv2.
IKE-Authentifizierungsmethoden	Authentifizierung mit vordefinierten Schlüsseln, Digitale Zertifikatauthentifizierung
Verschlüsselungsalgorithmus	AES (128 Bit), AES 256 (256 Bit), 3DES
Hash-Algorithmus	HMAC SHA1, HMAC SHA256, HMAC SHA384, HMAC SHA512, HMAC MD5

Überwachung von CloudBridge-Connector-Tunneln

October 5, 2021

Sie können die Statistiken zur Überwachung der Leistung eines CloudBridge Connector-Tunnels anzeigen. Verwenden Sie die GUI oder die Citrix ADC Befehlszeile, um CloudBridge Connector-Tunnelstatistiken auf einer Citrix ADC-Appliance anzuzeigen.

In der folgenden Tabelle sind die statistischen Leistungsindikatoren aufgeführt, die für die Überwachung von CloudBridge Connector-Tunneln auf einer Citrix ADC Appliance verfügbar sind.

Statistischer Zähler	Gibt an
Empfangene Bytes	Gesamtzahl der Bytes, die von der Citrix ADC Appliance über alle konfigurierten CloudBridge Connector-Tunnel seit dem letzten Start der Appliance empfangen wurden.
Gesendete Bytes	Gesamtanzahl der Bytes, die von der Citrix ADC Appliance über alle konfigurierten CloudBridge Connector-Tunnel seit dem letzten Start der Appliance gesendet wurden.
Empfangene Pakete	Gesamtzahl der Pakete, die von der Citrix ADC Appliance über alle konfigurierten CloudBridge Connector-Tunnel seit dem letzten Start der Appliance empfangen wurden.
Gesendete Pakete	Gesamtzahl der Pakete, die von der Citrix ADC Appliance über alle konfigurierten CloudBridge Connector-Tunnel seit dem letzten Start der Appliance gesendet wurden.
Empfangene Bytes Rate	Anzahl der Bytes pro Sekunde, die von der Citrix ADC Appliance über alle konfigurierten CloudBridge Connector-Tunnel empfangen werden.
Übertragungsrate von Bytes	Anzahl der Bytes pro Sekunde, die von der Citrix ADC Appliance über alle konfigurierten CloudBridge Connector-Tunnel gesendet werden
Rate empfangener Pakete	Anzahl der Bytes pro Sekunde, die von der Citrix ADC Appliance über alle konfigurierten CloudBridge Connector-Tunnel empfangen werden
Rate gesendeter Pakete	Anzahl der Bytes pro Sekunde, die von der Citrix ADC Appliance über alle konfigurierten CloudBridge Connector-Tunnel empfangen werden

Alle diese Leistungsindikatoren werden auf 0 zurückgesetzt, wenn die Citrix ADC Appliance neu gestartet wird. Sie erhöhen sich nicht in den folgenden Phasen:

- IKE-Authentifizierung (Pre-Shared Key Exchange) in einem konfigurierten CloudBridge Connector-Tunnel.
- IKE Security Association (SA) -Einrichtungsphase in einem konfigurierten CloudBridge Connector-Tunnel.

So zeigen Sie CloudBridge Connector-Tunnelstatistiken mit der Citrix ADC Befehlszeile an

Geben Sie an der Eingabeaufforderung Folgendes ein:

- **Statt-IPsec-Zähler**

So zeigen Sie CloudBridge Connector-Tunnelstatistiken mit der GUI an

1. Greifen Sie mit einem Webbrowser auf die Benutzeroberfläche zu, um eine Verbindung mit der IP-Adresse der Citrix ADC Appliance herzustellen.
2. Navigieren Sie auf der Registerkarte **Konfiguration** zu **System** > **CloudBridge Connector** .
3. Klicken Sie auf der Seite “CloudBridge Connector” auf **CloudBridge Connector erstellen/überwachen**. Die Diagramme für **IPsec-Bytes** und **IPsec-Pakete** zeigen die empfangene Byte-Rate, gesendete Byte-Rate, empfangene Pakete und gesendete Paketrate aller CloudBridge Connector-Tunnel an, die auf der Citrix ADC Appliance konfiguriert sind.

```
    > stat ipsec counters
    Secure tunnel(s) summary
                        Rate (/s)        Total
    Bytes Received    0    2811248
    Bytes Sent            0    157460630
    Packets Received    0    56787
    Packets Sent        0    200910
    Done
    >
<!--NeedCopy-->
```

Konfigurieren eines CloudBridge Connector-Tunnels zwischen zwei Rechenzentren

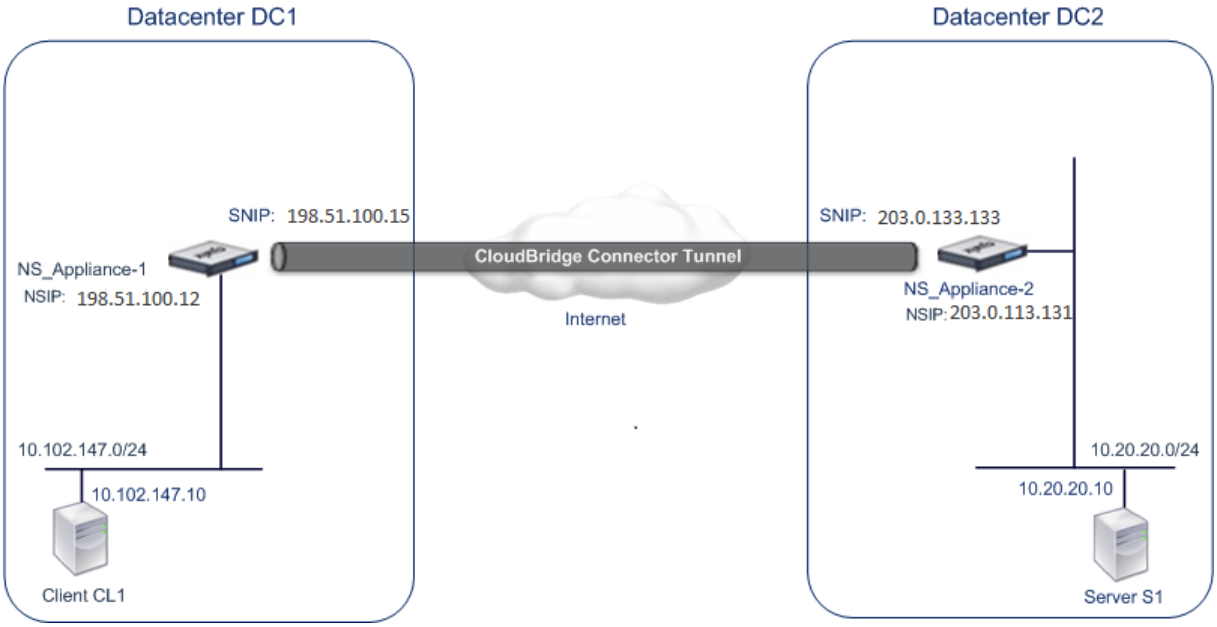
October 5, 2021

Sie können einen CloudBridge Connector-Tunnel zwischen zwei verschiedenen Rechenzentren konfigurieren, um Ihr Netzwerk zu erweitern, ohne es neu zu konfigurieren, und die Funktionen der beiden Rechenzentren nutzen zu müssen. Ein CloudBridge Connector-Tunnel zwischen den beiden geografisch getrennten Rechenzentren ermöglicht es Ihnen, Redundanz zu implementieren und Ihre

Einrichtung vor Fehlern zu schützen. Der CloudBridge Connector-Tunnel ermöglicht eine optimale Nutzung der Infrastruktur und Ressourcen in Rechenzentren. Die Anwendungen, die in den beiden Rechenzentren verfügbar sind, werden für den Benutzer als lokal angezeigt.

Um ein Datencenter mit einem anderen Datencenter zu verbinden, richten Sie einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance in einem Rechenzentrum und einer Citrix ADC-Appliance im anderen Datencenter ein.

Betrachten Sie als Illustration des CloudBridge Connector-Tunnels zwischen Rechenzentren ein Beispiel, in dem ein CloudBridge Connector-Tunnel zwischen der Citrix ADC Appliance NS_Appliance-1 im Rechenzentrum DC1 und der Citrix ADC-Appliance NS_Appliance-2 im Rechenzentrum DC2 eingerichtet wird.



Sowohl NS_Appliance-1 als auch NS_Appliance-2 funktionieren im L2- und L3-Modus. Sie ermöglichen die Kommunikation zwischen privaten Netzwerken in Rechenzentren DC1 und DC2. Im L3-Modus ermöglichen NS_Appliance-1 und NS_Appliance-2 die Kommunikation zwischen Client CL1 im Rechenzentrum DC1 und Server S1 im Rechenzentrum DC2 über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

Da Client CL1 und Server S1 sich in verschiedenen privaten Netzwerken befinden, ist der L3-Modus auf NS_Appliance-1 und NS_Appliance-2 aktiviert und Routen werden wie folgt aktualisiert:

- CL1 hat eine Route zu NS_Appliance-1, um S1 zu erreichen.
- NS_Appliance-1 hat eine Route zu NS_Appliance-2, um S1 zu erreichen.
- S1 hat eine Route zu NS_Appliance-2, um CL1 zu erreichen.
- NS_Appliance-2 hat eine Route zu NS_Appliance-1, um CL1 zu erreichen.

In der folgenden Tabelle sind die Einstellungen der Citrix ADC Appliance NS_Appliance-1 im Rechenzentrum DC1 aufgeführt.

In der folgenden Tabelle sind die Einstellungen der Citrix ADC Appliance NS_Appliance-2 im Rechenzentrum DC2 aufgeführt.

Entität	Name	Details
Die NSIP-Adresse		198.51.100.12
SNIP-Adresse		198.51.100.15
CloudBridge-Connector-Tunnel	Cloud_Connector_DC1-DC2	1. Lokale Endpunkt-IP-Adresse des CloudBridge Connector-Tunnels: 198.51.100.15, 2. Remote-Endpunkt-IP-Adresse des CloudBridge Connector-Tunnels: 203.0.113.133. GRE Tunnel Details Name = Cloud_Connector_DC1-DC2, IPsec-Profildetails Name = Cloud_Connector_DC1-DC2, Verschlüsselungsalgorithmus = AES, Hash-Algorithmus = HMAC SHA1

Punkte, die bei der Konfiguration des CloudBridge Connector-Tunnels berücksichtigt werden müssen

Stellen Sie vor dem Einrichten eines CloudBridge Connector-Tunnels sicher, dass die folgenden Aufgaben ausgeführt wurden:

1. Bereitstellen und Einrichten einer Citrix ADC Appliance in jedem der beiden Rechenzentren.
2. Stellen Sie sicher, dass die Endpunkt-IP-Adressen des CloudBridge Connector-Tunnels für einander zugänglich sind.

Konfigurationsprozedur

Um einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance, die sich in einem Rechenzentrum befindet, und einer anderen Citrix ADC-Appliance, die sich im anderen Rechenzentrum befindet, einzurichten, verwenden Sie die GUI oder die Befehlszeilenschnittstelle einer der Citrix ADC-Appliances.

Wenn Sie die GUI verwenden, wird die CloudBridge Connector-Tunnelkonfiguration, die auf der ersten Citrix ADC Appliance erstellt wurde, automatisch an den anderen Endpunkt (die andere Citrix ADC-Appliance) des CloudBridge Connector-Tunnels übertragen. Daher müssen Sie nicht auf die GUI der anderen Citrix ADC Appliance zugreifen, um die entsprechende CloudBridge Connector-Tunnelkonfiguration zu erstellen.

Die CloudBridge Connector-Tunnelkonfiguration auf jeder der Citrix ADC Appliances besteht aus den folgenden Entitäten:

- **IPsec-Profil**— Eine IPsec-Profilentität gibt die IPsec-Protokollparameter an, z. B. IKE-Version, Verschlüsselungsalgorithmus, Hash-Algorithmus und PSK, die vom IPsec-Protokoll im CloudBridge Connector-Tunnel verwendet werden sollen.
- **GRE-Tunnel**— Ein IP-Tunnel gibt die lokale IP-Adresse (eine öffentliche SNIP-Adresse, die auf der lokalen Citrix ADC Appliance konfiguriert ist), die Remote-IP-Adresse (eine öffentliche SNIP-Adresse, die auf der Remote-Citrix ADC-Appliance konfiguriert ist), das zum Einrichten des CloudBridge Connector-Tunnels verwendet wird, und ein IPsec an -Profil-Entität.
- **Erstellen Sie eine PBR-Regel und verknüpfen Sie den IP-Tunnel damit**—Eine PBR-Entität gibt einen Satz von Bedingungen und eine IP-Tunnelentität an. Der Quell-IP-Adressbereich und der Ziel-IP-Bereich sind die Bedingungen für die PBR-Entität. Sie müssen den Quell-IP-Adressbereich und den Ziel-IP-Adressbereich festlegen, um das Subnetz anzugeben, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll. Betrachten Sie beispielsweise ein Anforderungspaket, das von einem Client im Subnetz im ersten Datencenter stammt und für einen Server im Subnetz im zweiten Datencenter bestimmt ist. Wenn dieses Paket mit dem Quell- und Ziel-IP-Adressbereich der PBR-Entität auf der Citrix ADC Appliance im ersten Datencenter übereinstimmt, wird es über den CloudBridge Connector-Tunnel gesendet, der der PBR-Entität zugeordnet ist.

So erstellen Sie mit der Befehlszeilenschnittstelle ein IPSEC-Profil

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add ipsec profile <name> [-ikeVersion (V1 | V2)] [-encAlgo (AES | 3 DES)...] [-hashAlgo <hashAlgo\> ...] [-lifetime <positive_integer>] (-psk | (-publickey<string> -privatekey <string>-peerPublicKey <string >))[-livenessCheckInterval <positive_intege>][-replayWindowSize \< positive_integer>] [-ikeRetryInterval <positive_integer>] [-retransmissiontime <positive_integer>]`
- `show ipsec profile <name>`

So erstellen Sie einen IP-Tunnel und binden das IPSEC-Profil mit der Befehlszeilenschnittstelle an ihn

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add ipTunnel <name> <remote><remoteSubnetMask> <local> [-protocol < protocol>] [-ipsecProfileName <string>]`

- show ipTunnel <name>

So erstellen Sie eine PBR-Regel und binden den IPSEC-Tunnel mit der Befehlszeilenschnittstelle an ihn

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add ns pbr <pbr_name> ALLOW -srcIP = <local_subnet_range> -destIP = <remote_subnet_range> -ipTunnel <tunnel_name>
- apply ns pbrs
- show ns pbr <pbr_name>

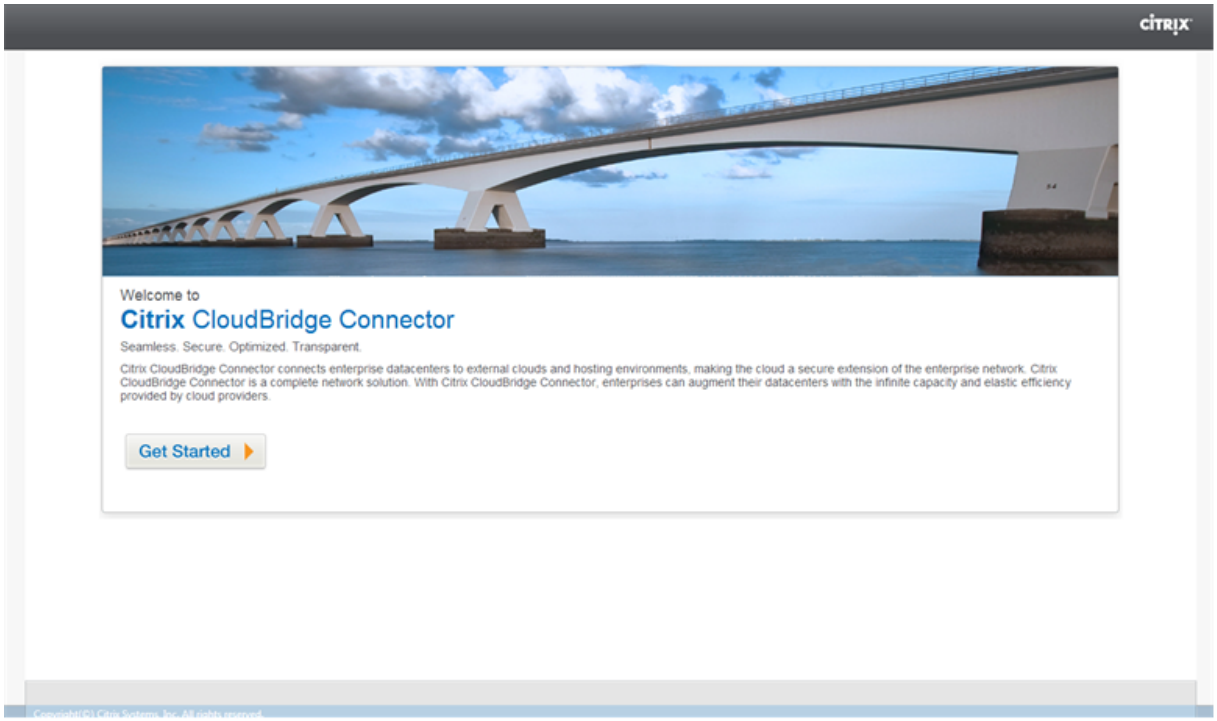
Beispiel

```
1  add ipsec profile Cloud_Connector_DC1-DC2  -encAlgo AES -hashAlgo
       HMAC_SHA1
2      Done
3      > add ipTunnel Cloud_Connector_DC1-DC2 203.0.113.133
           255.255.255.255 198.51.100.15 -protocol GRE -ipsecProfileName
           Cloud_Connector_DC1-DC2
4
5      Done
6      > add ns pbr PBR-DC1-DC2 ALLOW -srcIP 198.51.100.15 -destIP
           203.0.113.133 ipTunnel Cloud_Connector_DC1-DC2
7
8      Done
9      > apply ns pbrs
10
11     Done
12 <!--NeedCopy-->
```

So konfigurieren Sie einen CloudBridge Connector-Tunnel in einer Citrix ADC Appliance mit der GUI

1. Geben Sie die NSIP-Adresse einer Citrix ADC Appliance in die Adresszeile eines Webbrowsers ein.
2. Melden Sie sich mit Ihren Kontoanmeldeinformationen für die Appliance an der Benutzeroberfläche der Citrix ADC Appliance an.
3. Navigieren Sie zu **System** > **CloudBridge Connector** .
4. Klicken Sie im rechten Bereich unter **Erste Schritte**auf **CloudBridge erstellen/überwachen**.

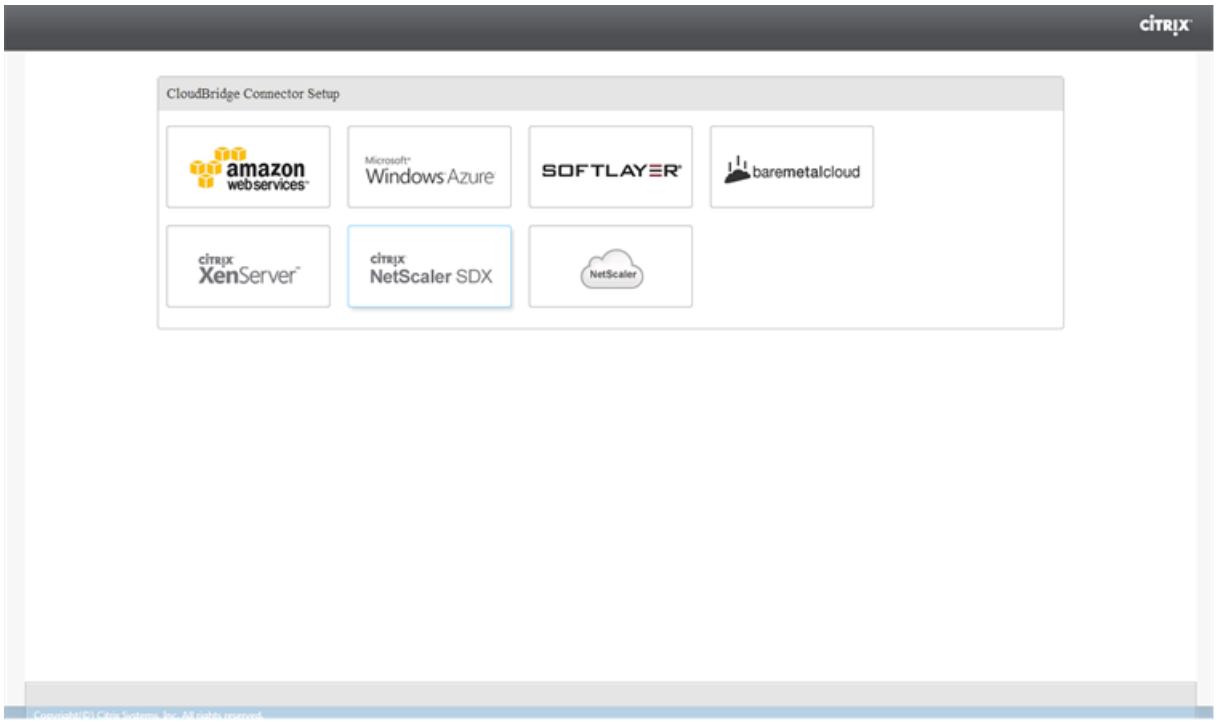
   Wenn Sie zum ersten Mal einen CloudBridge Connector-Tunnel auf der Appliance konfigurieren, wird ein **Begrüßungsbildschirm** angezeigt.
5. Klicken Sie auf der **Willkommensseite** auf **Erste Schritte** .



Hinweis:

Wenn Sie bereits einen CloudBridge Connector-Tunnel auf der Citrix ADC Appliance konfiguriert haben, wird der Begrüßungsbildschirm nicht angezeigt, sodass Sie nicht auf Erste Schritte klicken.

1. Klicken Sie im Bereich **CloudBridge Connector-Setup** auf **Citrix ADC**.



1. Geben Sie im Bereich Citrix ADC Ihre Kontoanmeldeinformationen für die Remote-Citrix ADC Appliance an. Klicken Sie auf **Weiter**.
2. Legen Sie im Bereich **CloudBridge-Connector-Einstellungen** den folgenden Parameter fest:
   - **CloudBridge-Connector-Name**— Name für die CloudBridge Connector-Konfiguration auf der lokalen Appliance. Muss mit einem alphabetischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstrich, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestriche (-) enthalten. Kann nicht geändert werden, nachdem die CloudBridge Connector-Konfiguration erstellt wurde.
3. Legen Sie unter **Lokale Einstellung**den folgenden Parameter fest:
   - **Subnetz-IP**— IP-Adresse des lokalen Endpunkts des CloudBridge Connector-Tunnels.
4. Legen Sie unter **Remote Setting**den folgenden Parameter fest:
   - **Subnetz-IP**— IP-Adresse des Peer-Endpunkts des CloudBridge Connector-Tunnels.
5. Legen Sie unter **PBR** Setting die folgenden Parameter fest:
   - **Operation**—Entweder gleich (=) oder nicht gleich (! =) logischer Operator.
   - **Quell-IP Niedrig** — Die niedrigste Quell-IP-Adresse, die mit der Quell-IP-Adresse eines ausgehenden IPv4-Pakets übereinstimmt.
   - **Source IP High**— Die höchste Quell-IP-Adresse, die mit der Quell-IP-Adresse eines ausgehenden IPv4-Pakets übereinstimmt.
   - **Operation**—Entweder gleich (=) oder nicht gleich (! =) logischer Operator.
   - Ziel-IP Niedrig* — Die niedrigste Ziel-IP-Adresse, die mit der Ziel-IP-Adresse eines ausgehenden IPv4-Pakets übereinstimmt.
   - **Ziel-IP hoch**— Die höchste Ziel-IP-Adresse, die mit der Ziel-IP-Adresse eines ausgehenden IPv4-Pakets übereinstimmt.
6. (Optional) Legen Sie unter **Sicherheitseinstellungen**die folgenden IPsec-Protokollparameter für den CloudBridge Connector-Tunnel fest:
   - **Verschlüsselungsalgorithmus**— Verschlüsselungsalgorithmus, der vom IPsec-Protokoll im CloudBridge-Tunnel verwendet wird.
   - **Hash-Algorithmus**— Hash-Algorithmus, der vom IPsec-Protokoll im CloudBridge-Tunnel verwendet wird.
   - **Schlüssel**— Wählen Sie eine der folgenden IPsec-Authentifizierungsmethoden aus, die von den beiden Peers zur gegenseitigen Authentifizierung verwendet werden soll.
     - **Schlüssel automatisch generieren**— Authentifizierung basierend auf einer Textzeichenfolge, die als Pre-Shared Key (PSK) bezeichnet wird, die automatisch von der lokalen Appliance generiert wird. Die PSKS-Schlüssel der Peers werden zur Authentifizierung gegeneinander abgestimmt.

- **Spezifischer Schlüssel**— Authentifizierung basierend auf einer manuell eingegebenen PSK. Die PSKs der Peers werden zur Authentifizierung gegeneinander abgestimmt.
  - Pre Shared Security Key: Die Textzeichenfolge, die für die Authentifizierung mit vorinstalliertem Schlüssel eingegeben wurde.
- **Zertifikate hochladen**— Authentifizierung basierend auf digitalen Zertifikaten.
  - **Öffentlicher Schlüssel**: Ein lokales digitales Zertifikat, das zur Authentifizierung der lokalen Citrix ADC Appliance beim Peer verwendet wird, bevor IPsec-Sicherheitszuordnungen eingerichtet werden. Das gleiche Zertifikat sollte vorhanden sein und für den Peer-Public Key-Parameter im Peer festgelegt sein.
  - **Privater Schlüssel**— Privater Schlüssel des lokalen digitalen Zertifikats.
  - **Öffentlicher Peer-Schlüssel**— Digitales Zertifikat des Peers. Wird verwendet, um den Peer am lokalen Endpunkt zu authentifizieren, bevor IPsec-Sicherheitszuordnungen eingerichtet werden. Das gleiche Zertifikat sollte vorhanden sein und für den Parameter Öffentlicher Schlüssel im Peer festgelegt sein.

7. Klicken Sie auf **Fertig**.

Die neue CloudBridge Connector-Tunnelkonfiguration auf beiden Citrix ADC Appliances wird auf der Registerkarte Start der jeweiligen GUI angezeigt. Der aktuelle Status des CloudBridge-Connector-Tunnels wird im Bereich Konfigurierte CloudBridge-Connectors angezeigt. Ein grüner Punkt zeigt an, dass der Tunnel oben ist. Ein roter Punkt zeigt an, dass der Tunnel heruntergefahren ist.

Überwachung des CloudBridge-Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer Citrix ADC Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen. Weitere Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer Citrix ADC Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

Konfigurieren von CloudBridge Connector zwischen Rechenzentrum und AWS-Cloud

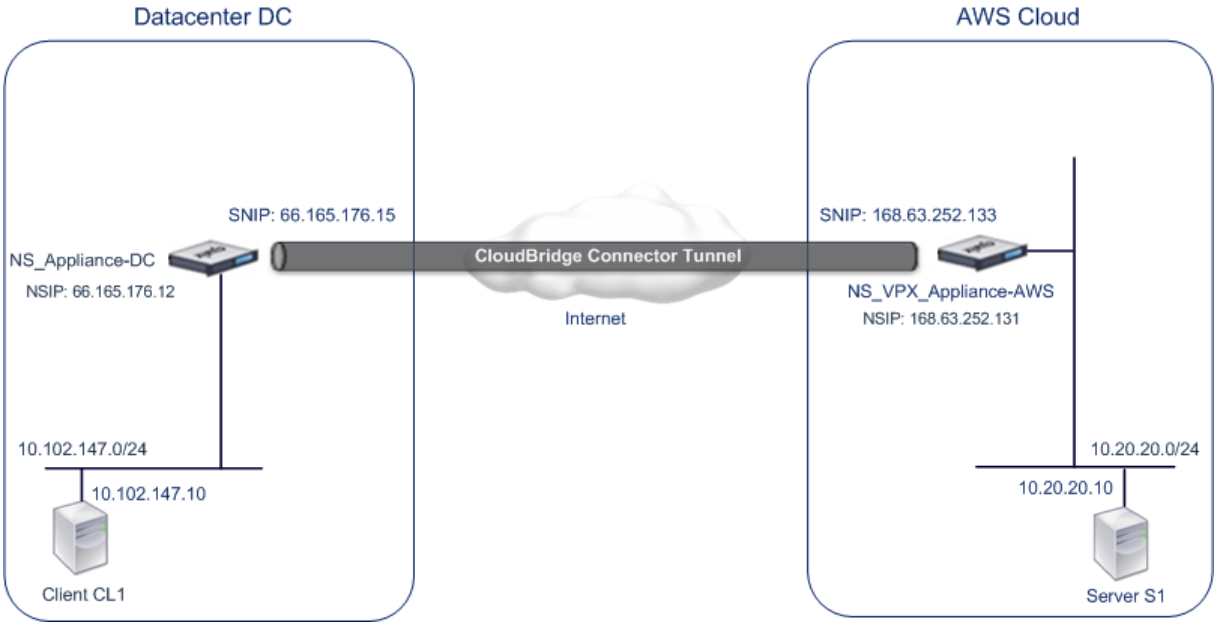
October 5, 2021

Sie können einen CloudBridge Connector-Tunnel zwischen einem Rechenzentrum und einer AWS-Cloud konfigurieren, um die Infrastruktur- und Computing-Funktionen des Rechenzentrums und der AWS-Cloud zu nutzen. Mit AWS können Sie Ihr Netzwerk ohne anfängliche Kapitalinvestitionen oder

die Kosten für die Wartung der erweiterten Netzwerkinfrastruktur erweitern. Sie können Ihre Infrastruktur nach Bedarf nach oben oder unten skalieren. Beispielsweise können Sie mehr Serverfunktionen leasen, wenn der Bedarf steigt.

Um ein Rechenzentrum mit der AWS-Cloud zu verbinden, richten Sie einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance, die sich im Rechenzentrum befindet, und einer virtuellen Citrix ADC-Appliance (VPX), die sich in der AWS-Cloud befindet, ein.

Betrachten Sie ein Beispiel, in dem ein CloudBridge Connector-Tunnel zwischen einem Rechenzentrum und Amazon AWS-Cloud zwischen der Citrix ADC Appliance NS_Appliance-DC, im Rechenzentrums-DC und der virtuellen Citrix ADC-Appliance (VPX) NS_VPX_Appliance-AWS eingerichtet wird.



Sowohl NS_Appliance-DC als auch NS_VPX_Appliance-AWS funktionieren im L3-Modus. Sie ermöglichen die Kommunikation zwischen privaten Netzwerken im Rechenzentrum DC und der AWS-Cloud. NS_Appliance-DC und NS_VPX_Appliance-AWS ermöglichen die Kommunikation zwischen Client CL1 im Rechenzentrum DC und Server S1 in der AWS-Cloud über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

> **Hinweis**:
>
> AWS unterstützt den L2-Modus nicht, daher ist es notwendig, nur den L3-Modus auf beiden Endpunkten aktiviert zu haben.

Für die ordnungsgemäße Kommunikation zwischen CL1 und S1 ist der L3-Modus auf NS_Appliance-DC und NS_VPX_Appliance-AWS aktiviert und Routen werden wie folgt aktualisiert:

- CL1 hat eine Route zu NS_Appliance-DC, um S1 zu erreichen.
- NS_Appliance-DC haben eine Route zu NS_VPX_Appliance-AWS, um S1 zu erreichen.

- S1 sollte eine Route zu NS_VPX_Appliance-AWS haben, um CL1 zu erreichen.
- NS_VPX_Appliance-AWS haben eine Route zu NS_Appliance-DC, um CL1 zu erreichen.

In der folgenden Tabelle sind die Einstellungen der Citrix ADC Appliance NS_Appliance-DC im Rechenzentrums-DC aufgeführt.

Entität	Name	Details
Die NSIP-Adresse		66.165.176.12
SNIP-Adresse		66.165.176.15
CloudBridge-Connector-Tunnel	CC_Tunnel_DC-AWS	Lokale Endpunkt-IP-Adresse des CloudBridge Connector-Tunnels: 66.165.176.15, Remote-Endpunkt-IP-Adresse des CloudBridge Connector-Tunnels: 168.63.252.133, GRE Tunnel Details - Name= CC_Tunnel_DC-AWS

In der folgenden Tabelle sind die Einstellungen für Citrix ADC VPX NS_VPX_Appliance-AWS in der AWS-Cloud aufgeführt.

Entität	Name	Details
NSIP-Adresse		10.102.25.30
Öffentliche EIP-Adresse, die der NSIP-Adresse zugeordnet ist		168.63.252.131
SNIP-Adresse		10.102.29.30
Öffentliche EIP-Adresse, die der SNIP-Adresse zugeordnet ist		168.63.252.133

Entität	Name	Details
CloudBridge-Connector-Tunnel	CC_Tunnel_DC-AWS	Lokale Endpunkt-IP-Adresse des CloudBridge Connector-Tunnels: 168.63.252.133, Remote-Endpunkt-IP-Adresse des CloudBridge Connector-Tunnels: 66.165.176.15; **GRE Tunnel Details** Name = CC_Tunnel_DC-AWS, IPsec-Profildetails, Name= CC_Tunnel_DC-AWS, Verschlüsselungsalgorithmus= AES, Hash-Algorithmus= HMAC SHA1

Voraussetzungen

Stellen Sie vor dem Einrichten eines CloudBridge Connector-Tunnels sicher, dass die folgenden Aufgaben ausgeführt wurden:

1. Installieren, konfigurieren und starten Sie eine Instanz der Citrix ADC Virtual Appliance (VPX) in der AWS-Cloud. Anweisungen zur Installation von Citrix ADC VPX in AWS finden Sie unter Bereitstellen einer Citrix ADC VPX-Instanz auf AWS.
2. Provisioning und Konfigurieren einer physischen Citrix ADC Appliance oder Bereitstellen und Konfigurieren einer virtuellen Citrix ADC Appliance (VPX) auf einer Virtualisierungsplattform im Rechenzentrum.
3. Stellen Sie sicher, dass die Endpunkt-IP-Adressen des CloudBridge Connector-Tunnels für einander zugänglich sind.

Citrix ADC VPX -Lizenz

Nach dem erstmaligen Instanzstart benötigt Citrix ADC VPX for AWS eine Lizenz. Wenn Sie Ihre eigene Lizenz (BYOL) mitbringen, lesen Sie den VPX Licensing Guide unter: http://support.citrix.com/article/CTX122426.

Sie müssen:

1. Verwenden Sie das Lizenzierungsportal auf der Citrix Website, um eine gültige Lizenz zu generieren.

2. Laden Sie die Lizenz auf die Instanz hoch.

Wenn es sich um eine **kostenpflichtige** Marketplace-Instanz handelt, müssen Sie keine Lizenz installieren. Der korrekte Funktionsumfang und die korrekte Leistung werden automatisch aktiviert.

Konfigurationsschritte

Um einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance, die sich in einem Rechenzentrum befindet, und einer virtuellen Citrix ADC-Appliance (VPX), die sich in der AWS-Cloud befindet, einzurichten, verwenden Sie die GUI der Citrix ADC-Appliance.

Wenn Sie die GUI verwenden, wird die auf der Citrix ADC-Appliance erstellte CloudBridge Connector-Tunnelkonfiguration automatisch an den anderen Endpunkt oder Peer (Citrix ADC VPX auf AWS) des CloudBridge Connector-Tunnels übertragen. Daher müssen Sie nicht auf die GUI (GUI) des Citrix ADC VPX in AWS zugreifen, um die entsprechende CloudBridge Connector-Tunnelkonfiguration zu erstellen.

Die CloudBridge Connector-Tunnelkonfiguration auf beiden Peers (die Citrix ADC Appliance, die sich im Rechenzentrum befindet, und die virtuelle Citrix ADC-Appliance (VPX), die sich in der AWS-Cloud befindet) besteht aus den folgenden Entitäten:

- **IPsec-Profil**— Eine IPsec-Profilentität gibt die IPsec-Protokollparameter an, z. B. IKE-Version, Verschlüsselungsalgorithmus, Hash-Algorithmus und PSK, die vom IPsec-Protokoll in beiden Peers des CloudBridge Connector-Tunnels verwendet werden sollen.
- **GRE-Tunnel**— Ein IP-Tunnel gibt eine lokale IP-Adresse (eine öffentliche SNIP-Adresse, die auf dem lokalen Peer konfiguriert ist), eine Remote-IP-Adresse (eine öffentliche SNIP-Adresse, die auf dem Remote-Peer konfiguriert ist), ein Protokoll (GRE) zum Einrichten des CloudBridge Connector-Tunnels und eine IPsec-Profilentität an.
- **Erstellen Sie eine PBR-Regel und verknüpfen Sie den IP-Tunnel damit**—Eine PBR-Entität gibt einen Satz von Bedingungen und eine IP-Tunnelentität an. Der Quell-IP-Adressbereich und der Ziel-IP-Bereich sind die Bedingungen für die PBR-Entität. Sie müssen den Quell-IP-Adressbereich und den Ziel-IP-Adressbereich festlegen, um das Subnetz anzugeben, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll. Betrachten Sie beispielsweise ein Anforderungspaket, das von einem Client im Subnetz im Rechenzentrum stammt und für einen Server im Subnetz in der AWS-Cloud bestimmt ist. Wenn dieses Paket mit dem Quell- und Ziel-IP-Adressbereich der PBR-Entität auf der Citrix ADC Appliance im Rechenzentrum übereinstimmt, wird es über den CloudBridge Connector-Tunnel gesendet, der der PBR-Entität zugeordnet ist.

So erstellen Sie mit der Befehlszeilenschnittstelle ein IPSEC-Profil

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add ipsec profile <name> [-**ikeVersion** (V1 | V2)] [-**encAlgo** (AES | 3DES)...] [-**hashAlgo** <hashAlgo> ...] [-**lifetime** <positive_integer>] (-**psk** | (-**publickey** <string> -**privatekey** <string> -**peerPublicKey** <string>))[-**livenessCheckInterval** <positive_integer>] [-**replayWindowSize** <positive_integer>] [-**ikeRetryInterval** <positive_integer>] [-**retransmissiontime** <positive_integer>]
- **show ipsec profile** <name>

So erstellen Sie einen IP-Tunnel und binden das IPSEC-Profil mit der Befehlszeilenschnittstelle an ihn

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add ipTunnel <name> <remote><remoteSubnetMask> <local> [-protocol <protocol>] [-ipsecProfileName <string>]
- show ipTunnel <name>

So erstellen Sie eine PBR-Regel und binden den IPSEC-Tunnel mit der Befehlszeilenschnittstelle an ihn

Geben Sie an der Eingabeaufforderung Folgendes ein:

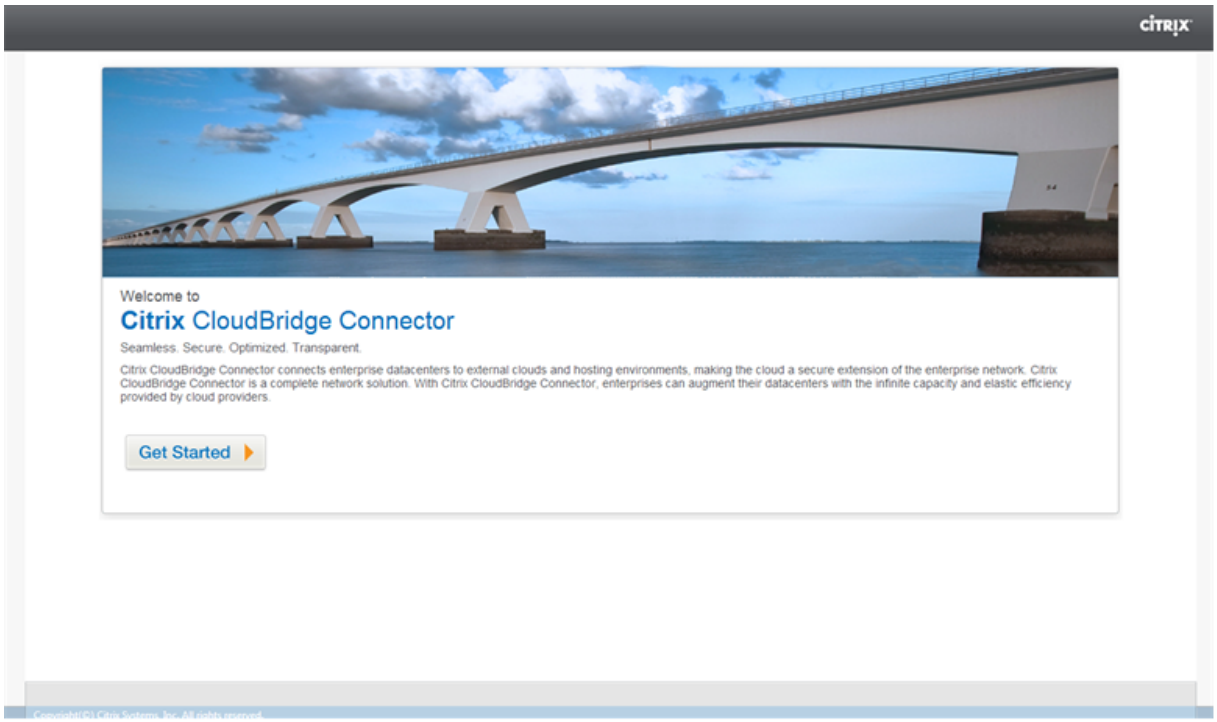
- add ns pbr <pbr_name> ALLOW -srcIP = <local_subnet_range> -destIP = <remote_subnet_range> -ipTunnel <tunnel_name>
- apply ns pbrs
- show ns pbr <pbr_name>

Beispiel

```
1      > add ipsec profile CC_Tunnel_DC-AWS -encAlgo AES -hashAlgo
           HMAC_SHA1
2
3      Done
4      > add ipTunnel CC_Tunnel_DC-AWS 168.63.252.133 255.255.255.0
           66.165.176.15 -protocol GRE -ipsecProfileName CC_Tunnel_DC-AWS
5
6      Done
7      > add ns pbr PBR-DC-AWS ALLOW -srcIP 66.165.176.15 -destIP
           168.63.252.133 ipTunnel CC_Tunnel_DC-AWS
8
9      Done
10     > apply ns pbrs
11
12     Done
13 <!--NeedCopy-->
```

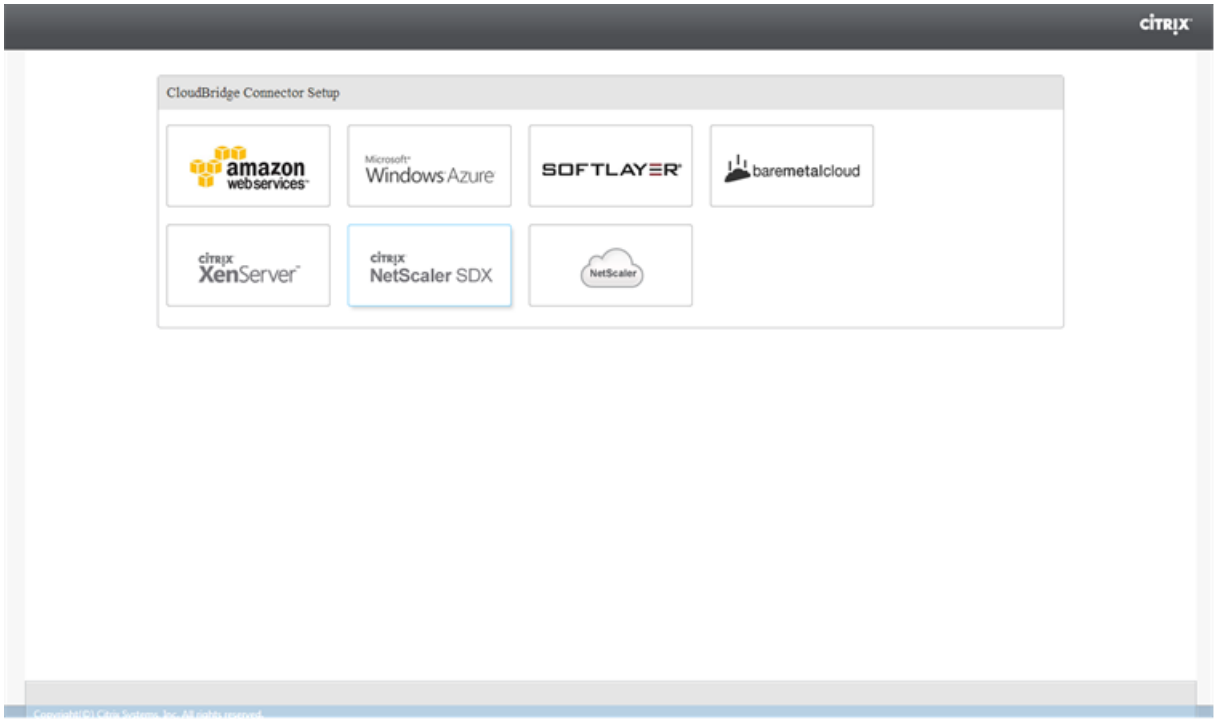

So konfigurieren Sie einen CloudBridge Connector-Tunnel in einer Citrix ADC Appliance mit der GUI

1. Geben Sie die NSIP-Adresse einer Citrix ADC Appliance in die Adresszeile eines Webbrowsers ein.
2. Melden Sie sich mit Ihren Kontoanmeldeinformationen für die Appliance an der Benutzeroberfläche der Citrix ADC Appliance an.
3. Navigieren Sie zu **System** > **CloudBridge Connector** .
4. Klicken Sie im rechten Bereich unter **Erste Schritte**auf **CloudBridge erstellen/überwachen**.
5. Wenn Sie zum ersten Mal einen CloudBridge Connector-Tunnel auf der Appliance konfigurieren, wird ein **Begrüßungsbildschirm** angezeigt.
6. Klicken Sie auf der **Willkommensseite** auf **Erste Schritte** .



> **Hinweis**:
>
> Wenn Sie bereits einen CloudBridge Connector-Tunnel auf der Citrix ADC Appliance konfiguriert haben, wird der Begrüßungsbildschirm nicht angezeigt, sodass Sie nicht auf Erste Schritte klicken.

1. Klicken Sie im **Setup-Bereich von CloudBridge Connector** auf **Amazon Web Services**



1. Geben Sie im Bereich **Amazon** Ihre AWS-Kontoanmeldeinformationen ein: AWS Access Key ID und AWS Secret Access Key. Sie können diese Zugriffsschlüssel über die AWS GUI-Konsole beziehen. Klicken Sie auf **Weiter**.

> **Hinweis:**
>
> Früher stellt der Setup-Assistent immer eine Verbindung zur gleichen AWS-Region her, auch wenn eine andere Region ausgewählt ist. Daher fehlgeschlagen die Konfiguration des Cloud-Bridge Connector-Tunnels für einen Citrix ADC VPX, der in der ausgewählten AWS-Region ausgeführt wird. Dieses Problem wurde jetzt behoben.

1. Wählen Sie im Bereich **Citrix ADC** die NSIP-Adresse der virtuellen Citrix ADC Appliance aus, die in AWS ausgeführt wird. Geben Sie anschließend Ihre Kontoanmeldeinformationen für die virtuelle Citrix ADC Appliance an. Klicken Sie auf **Weiter**.
2. Legen Sie im Bereich **CloudBridge-Connector-Einstellungen** den folgenden Parameter fest:
   - **CloudBridge-Connector-Name**— Name für die CloudBridge Connector-Konfiguration auf der lokalen Appliance. Muss mit einem alphabetischen ASCII-Zeichen oder Unterstrich (_) beginnen und darf nur alphanumerische ASCII-Zeichen, Unterstrich, Hash (#), Punkt (.), Leerzeichen, Doppelpunkt (:), at (@), equals (=) und Bindestriche (-) enthalten. Kann nicht geändert werden, nachdem die CloudBridge Connector-Konfiguration erstellt wurde.
3. Legen Sie unter **Lokale Einstellung**den folgenden Parameter fest:
   - **Subnetz-IP**— IP-Adresse des lokalen Endpunkts des CloudBridge Connector-Tunnels. Muss eine öffentliche IP-Adresse vom Typ SNIP sein.

4. Legen Sie unter **Remote Setting**den folgenden Parameter fest:
    - **Subnetz-IP**— IP-Adresse des CloudBridge Connector-Tunnelendpunkts auf der AWS-Seite. Muss eine IP-Adresse vom Typ SNIP auf der Citrix ADC VPX Instanz in AWS sein.
    - **NAT**— Öffentliche IP-Adresse (EIP) in AWS, die der SNIP zugeordnet ist, die auf der Citrix ADC VPX Instanz in AWS konfiguriert ist.
5. Stellen Sie unter **PBR-Einstellung**die folgenden Parameter ein:
    - **Operation**—Entweder gleich (=) oder nicht gleich (! =) logischer Operator.
    - **Quell-IP Niedrig**— Die niedrigste Quell-IP-Adresse, die mit der Quell-IP-Adresse eines ausgehenden IPv4-Pakets übereinstimmt.
    - **Source IP High**— Die höchste Quell-IP-Adresse, die mit der Quell-IP-Adresse eines ausgehenden IPv4-Pakets übereinstimmt.
    - **Operation**—Entweder gleich (=) oder nicht gleich (! =) logischer Operator.
    - **Ziel-IP Niedrig**— Die niedrigste Ziel-IP-Adresse, die mit der Ziel-IP-Adresse eines ausgehenden IPv4-Pakets übereinstimmt.
    - **Ziel-IP hoch**— Die höchste Ziel-IP-Adresse, die mit der Ziel-IP-Adresse eines ausgehenden IPv4-Pakets übereinstimmt.
6. (Optional) Legen Sie unter **Sicherheitseinstellungen**die folgenden IPsec-Protokollparameter für den CloudBridge Connector-Tunnel fest:
    - **Verschlüsselungsalgorithmus**— Verschlüsselungsalgorithmus, der vom IPsec-Protokoll im CloudBridge-Tunnel verwendet wird.
    - **Hash-Algorithmus**— Hash-Algorithmus, der vom IPsec-Protokoll im CloudBridge-Tunnel verwendet wird.
    - **Schlüssel**— Wählen Sie eine der folgenden IPsec-Authentifizierungsmethoden aus, die von den beiden Peers zur gegenseitigen Authentifizierung verwendet werden sollen.
        - **Schlüssel automatisch generieren**— Authentifizierung basierend auf einer Textzeichenfolge, die als Pre-Shared Key (PSK) bezeichnet wird, die automatisch von der lokalen Appliance generiert wird. Die PSKS-Schlüssel der Peers werden zur Authentifizierung gegeneinander abgestimmt.
        - **Spezifischer Schlüssel**— Authentifizierung basierend auf einer manuell eingegebenen PSK. Die PSKs der Peers werden zur Authentifizierung gegeneinander abgestimmt.
            * **Pre Shared Security Key**: Die Textzeichenfolge, die für die Authentifizierung mit vorinstalliertem Schlüssel eingegeben wurde.
        - **Zertifikate hochladen**— Authentifizierung basierend auf digitalen Zertifikaten.
            * **Öffentlicher Schlüssel**: Ein lokales digitales Zertifikat, das zum Authentifizieren des lokalen Peers beim Remote-Peer verwendet wird, bevor IPsec-Sicherheitszuordnungen eingerichtet werden. Das gleiche Zertifikat sollte vorhanden sein und für den Peer-Public Key-Parameter im Peer festgelegt sein.

* **Privater Schlüssel**— Privater Schlüssel des lokalen digitalen Zertifikats.
* **Öffentlicher Peer-Schlüssel**— Digitales Zertifikat des Peers. Wird verwendet, um den Peer am lokalen Endpunkt zu authentifizieren, bevor IPsec-Sicherheitszuordnungen eingerichtet werden. Das gleiche Zertifikat sollte vorhanden sein und für den Parameter Öffentlicher Schlüssel im Peer festgelegt sein.

7. Klicken Sie auf **Fertig**.

Die neue CloudBridge Connector-Tunnelkonfiguration auf der Citrix ADC Appliance im Rechenzentrum wird auf der Registerkarte Start der GUI angezeigt. Die entsprechende neue CloudBridge Connector-Tunnelkonfiguration auf der Citrix ADC VPX Appliance in der AWS-Cloud wird auf der GUI angezeigt. Der aktuelle Status des CloudBridge-Connector-Tunnels wird im Bereich Konfigurierte CloudBridge angezeigt. Ein grüner Punkt zeigt an, dass der Tunnel oben ist. Ein roter Punkt zeigt an, dass der Tunnel heruntergefahren ist.

Überwachung des CloudBridge Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer Citrix ADC Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen. Weitere Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer Citrix ADC Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

Konfigurieren eines CloudBridge Connector-Tunnels zwischen einer Citrix ADC Appliance und einem virtuellen privaten Gateway in AWS

October 5, 2021

Um ein Rechenzentrum mit Amazon Web Services (AWS) zu verbinden, können Sie einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance im Rechenzentrum und einem virtuellen privaten Gateway in AWS konfigurieren. Die Citrix ADC Appliance und das virtuelle private Gateway bilden die Endpunkte des CloudBridge Connector-Tunnels und werden Peers genannt.

> **Hinweis:**
>
> Sie können auch einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC-Appliance in einem Rechenzentrum und einer Citrix ADC VPX-Instanz (anstelle eines virtuellen privaten Gateway) in AWS einrichten. Weitere Informationen finden Sie unter Konfigurieren von CloudBridge Connector zwischen Datacenter und AWS Cloud.

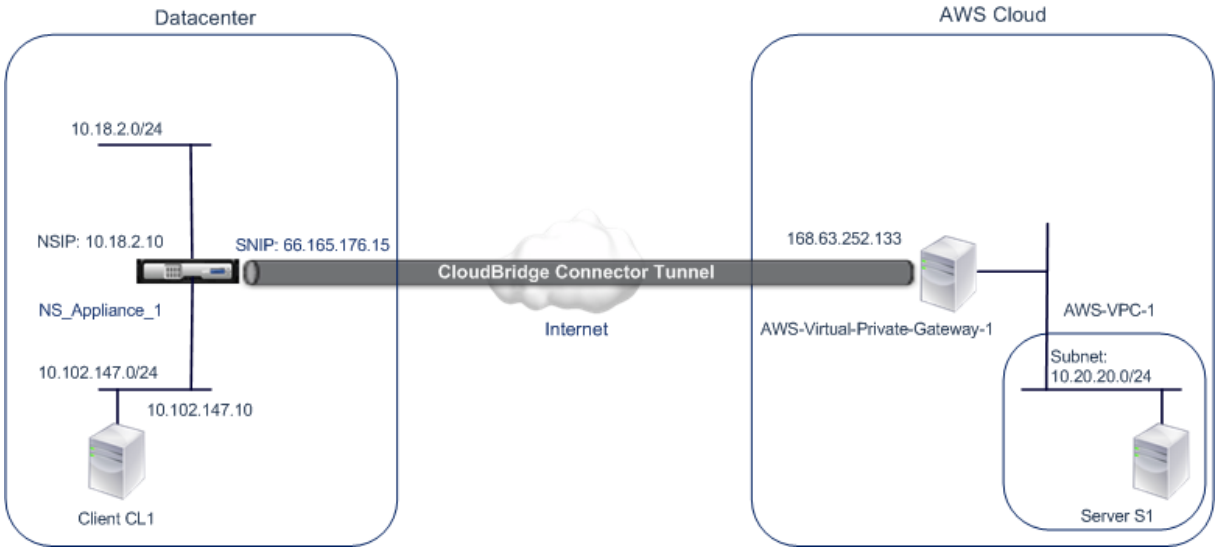
Virtuelle private Gateways in AWS unterstützen die folgenden IPsec-Einstellungen für einen CloudBridge Connector-Tunnel. Daher müssen Sie dieselben IPsec-Einstellungen angeben, wenn Sie die

Citrix ADC Appliance für den CloudBridge Connector-Tunnel konfigurieren.

IPsec-Eigenschaften	Einstellung
IPsec-Modus	Tunnelmodus
IKE-Version	Version 1
IKE-Authentifizierungsmethode	Vorgeteilter Schlüssel
Verschlüsselungsalgorithmus	AES
Hash-Algorithmus	HMAC SHA1

Beispiel für CloudBridge Connector-Tunnelkonfiguration und Datenfluss

Betrachten Sie als Veranschaulichung des Datenverkehrs in einem CloudBridge Connector-Tunnel ein Beispiel, in dem ein CloudBridge Connector-Tunnel zwischen der Citrix ADC Appliance NS_Appliance-1 in einem Rechenzentrum und dem virtuellen privaten Gateway AWS-Virtual-Private-Gateway-1 in der AWS-Cloud eingerichtet wird.



NS_Appliance-1 fungiert auch als L3-Router, der es einem privaten Netzwerk im Rechenzentrum ermöglicht, über den CloudBridge Connector-Tunnel ein privates Netzwerk in der AWS-Cloud zu erreichen. Als Router ermöglicht NS_Appliance-1 die Kommunikation zwischen Client CL1 im Rechenzentrum und Server S1 in der AWS-Cloud über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

Unter NS_Appliance-1 umfasst die CloudBridge Connector-Tunnelkonfiguration eine IPsec-Profilentität namens NS_AWS_IPsec_Profile, eine CloudBridge Connector-Tunnelentität namens NS_AWS_Tunnel und eine richtlinienbasierte Routing-Entität (PBR) mit dem Namen NS_AWS_PBR.

Die IPsec-Profilentität NS_AWS_IPsec_Profile gibt die IPsec-Protokollparameter wie IKE-Version, Verschlüsselungsalgorithmus und Hash-Algorithmus an, die vom IPsec-Protokoll im CloudBridge Connector-Tunnel verwendet werden sollen. NS_AWS_IPsec_Profile ist an die IP-Tunnelentität NS_AWS_Tunnel gebunden.

CloudBridge Connector-Tunnelentität NS_AWS_Tunnel gibt die lokale IP-Adresse (eine öffentliche IP-SNIP-Adresse, die auf der Citrix ADC Appliance konfiguriert ist), die Remote-IP-Adresse (die IP-Adresse des AWS-Virtual-Private-Gateway-1) und das Protokoll (IPsec) zum Einrichten des CloudBridge Connector-Tunnels an. NS_AWS_Tunnel ist an die Policy Based Routing-Entity NS_AWS_PBR (PBR) gebunden.

Die PBR-Entität NS_AWS_PBR gibt einen Satz von Bedingungen und eine CloudBridge Connector-Tunnelentität (NS_AWS_Tunnel) an. Der Quell-IP-Adressbereich und der Ziel-IP-Adressbereich sind die Bedingungen für NS_AWS_PBR. Der Quell-IP-Adressbereich und der Ziel-IP-Adressbereich werden als Subnetz im Rechenzentrum bzw. als Subnetz in der AWS-Cloud angegeben. Jedes Anforderungspaket, das von einem Client im Subnetz im Rechenzentrum stammt und für einen Server im Subnetz in der AWS-Cloud bestimmt ist, entspricht den Bedingungen in NS_AWS_PBR. Dieses Paket wird dann für die Verarbeitung von CloudBridge Connector berücksichtigt und über den CloudBridge Connector-Tunnel (NS_AWS_Tunnel) gesendet, der an die PBR-Entität gebunden ist.

In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt.

IP-Adresse des CloudBridge Connector-Tunnelendpunkts (NS_Appliance-1) auf der Datencenterseite	66.165.176.15
IP-Adresse des CloudBridge Connector-Tunnelendpunkts (AWS-Virtual-Private-Gateway-1) in AWS	168.63.252.133
Datacenter-Subnetz, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll	10.102.147.0/24
AWS-Subnet, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll	10.20.20.0/24

Einstellungen in Amazon AWS

Kunden-Gateway	AWS-Customer-Gateway-1	Routing = Statisch, IP-Adresse = Internet-routbare CloudBridge Connector-Tunnelendpunkt-IP-Adresse auf der Citrix ADC Seite = 66.165.176.15
Virtuelles privates Gateway	AWS-Virtual-Private-Gateway-1	Zugehörige VPC = AWS-VPC-1
VPN-Verbindung	AWS-VPN-Connection-1	Customer Gateway = AWS-Customer-Gateway-1, Virtual Private Gateway= Virtual-Private-Gateway-1, Routing-Optionen: Typ = Statische, Statische IP-Präfixe = Subnetze auf Citrix ADC Seite = 10.102.147.0/24

Einstellungen auf der Citrix ADC Appliance NS_Appliance-1 in Datacenter-1:

Gerät	Einstellungen	
SNIP1 (nur zu Referenzzwecken)	66.165.176.15	
IPsec profile	NS_AWS_IPsec_Profile	IKE version = v1, Encryption algorithm = AES, Hash algorithm = HMAC SHA1
CloudBridge Connector tunnel	NS_AWS_Tunnel	Remote IP = 168.63.252.133, Local IP= 66.165.176.15, Tunnel protocol = IPsec, IPsec profile= NS_AWS_IPsec_Profile
Policy based route	NS_AWS_Pbr	Source IP range = Subnet in the datacenter =10.102.147.0-10.102.147.255, Destination IP range =Subnet in AWS =10.20.20.0-10.20.20.255, IP Tunnel = NS_AWS_Tunnel

Punkte, die für eine CloudBridge Connector-Tunnelkonfiguration zu beachten sind

Bevor Sie einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und AWS-Gateway konfigurieren, beachten Sie die folgenden Punkte:

1. AWS unterstützt die folgenden IPsec-Einstellungen für einen CloudBridge Connector-Tunnel. Daher müssen Sie dieselben IPsec-Einstellungen angeben, wenn Sie die Citrix ADC Appliance für den CloudBridge Connector-Tunnel konfigurieren.
    - IKE Version = v1
    - Verschlüsselungsalgorithmus = AES
    - Hash-Algorithmus = HMAC SHA1
2. Sie müssen die Firewall am Citrix ADC Ende konfigurieren, um Folgendes zuzulassen.
    - Alle UDP-Pakete für Port 500
    - Alle UDP-Pakete für Port 4500
    - Alle ESP-Pakete (IP-Protokollnummer 50)
3. Sie müssen Amazon AWS konfigurieren, bevor Sie die Tunnelkonfiguration im Citrix ADC angeben, da die öffentliche IP-Adresse des AWS-Endes (Gateway) des Tunnels und der PSK automatisch generiert werden, wenn Sie die Tunnelkonfiguration in AWS einrichten. Sie benötigen diese Informationen, um die Tunnelkonfiguration auf der Citrix ADC Appliance anzugeben.
4. AWS-Gateway unterstützt statische Routen und das BGP-Protokoll für Routen-Updates. Die Citrix ADC Appliance unterstützt das BGP-Protokoll in einem CloudBridge Connector-Tunnel zum AWS-Gateway nicht. Daher müssen auf beiden Seiten des CloudBridge Connector-Tunnels geeignete statische Routen verwendet werden, um den Verkehr durch den Tunnel ordnungsgemäß zu leiten.

Konfigurieren von Amazon AWS für den CloudBridge Connector-Tunnel

Um eine CloudBridge Connector-Tunnelkonfiguration in Amazon AWS zu erstellen, verwenden Sie die Amazon AWS Management Console, eine webbasierte grafische Oberfläche zum Erstellen und Verwalten von Ressourcen in Amazon AWS.

Bevor Sie mit der CloudBridge Connector-Tunnelkonfiguration in der AWS-Cloud beginnen, stellen Sie sicher, dass:

- Sie haben ein Benutzerkonto für Amazon AWS Cloud.
- Sie verfügen über eine virtuelle private Cloud, deren Netzwerke Sie über den CloudBridge Connector-Tunnel mit den Netzwerken auf der Citrix ADC Seite verbinden möchten.
- Sie sind mit der Amazon AWS Management Console vertraut.

> **Hinweis**:
>
> Die Verfahren zur Konfiguration von Amazon AWS für einen CloudBridge Connector-Tunnel können sich je nach Amazon AWS-Veröffentlichungszyklus im Laufe der Zeit ändern. Citrix empfiehlt, dass Sie die Amazon AWS-Dokumentation für die neuesten Verfahren nachlesen.

So konfigurieren Sie einen CloudBridge-Connector-Tunnel zwischen einem Citrix ADC und AWS-Gateway, führen Sie die folgenden Aufgaben in der AWS Management Console aus:

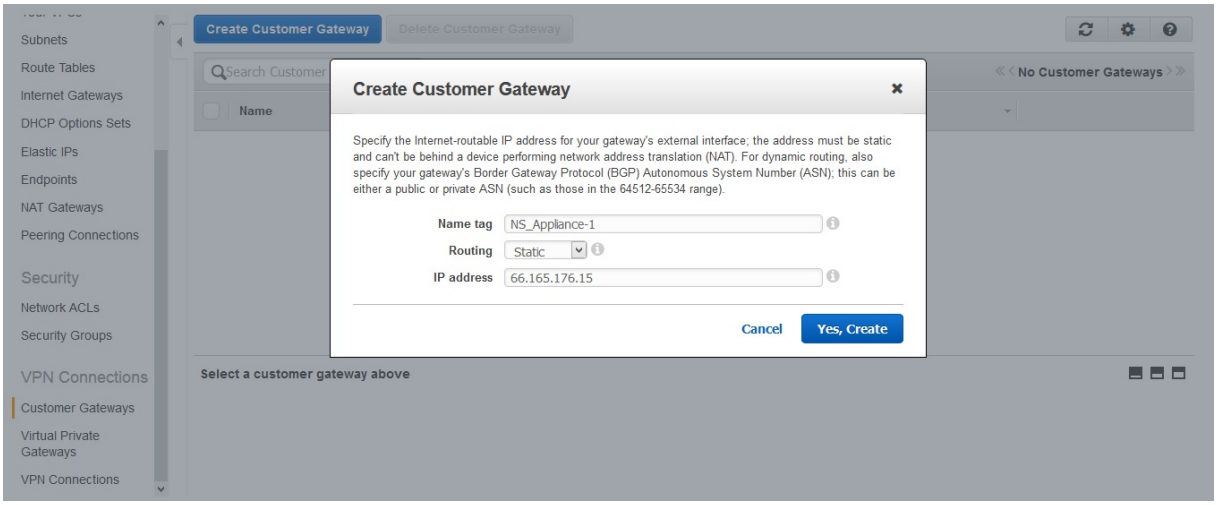
- **Erstellen Sie ein Kundengateway**. Ein Kundengateway ist eine AWS-Entität, die einen CloudBridge Connector-Tunnelendpunkt darstellt. Für einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und AWS-Gateway stellt das Kundengateway die Citrix ADC-Appliance in AWS dar. Das Kundengateway gibt einen Namen, den Typ des Routing (statisch oder BGP) im Tunnel und die IP-Adresse des CloudBridge Connector-Tunnels auf der Citrix ADC Seite an. Bei der IP-Adresse kann es sich um eine mit dem Internet betriebene Citrix ADC besetzte Subnetz-IP (SNIP) -Adresse oder, wenn sich die Citrix ADC-Appliance hinter einem NAT-Gerät befindet, eine internetroutable NAT-IP-Adresse, die die SNIP-Adresse darstellt.
- **Erstellen Sie ein Virtual Private Gateway und fügen Sie es an eine VPC**an. Ein virtuelles privates Gateway ist ein CloudBridge Connector-Tunnelendpunkt auf der AWS-Seite. Wenn Sie ein virtuelles privates Gateway erstellen, haben Sie ihm einen Namen zugewiesen oder AWS gestatten, den Namen zuzuweisen. Anschließend ordnen Sie das virtuelle private Gateway einer VPC zu. Diese Zuordnung ermöglicht es den Subnetzen der VPC, über den CloudBridge Connector-Tunnel eine Verbindung mit den Subnetzen auf der Citrix ADC Seite herzustellen.
- **Erstellen Sie eine VPN-Verbindung**. Eine VPN-Verbindung gibt ein Kundengateway und ein virtuelles privates Gateway an, zwischen dem ein CloudBridge Connector-Tunnel erstellt werden soll. Außerdem wird ein IP-Präfix für die Netzwerke auf der Citrix ADC Seite angegeben. Nur IP-Präfixe, die dem virtuellen privaten Gateway bekannt sind (über statische Routeneingabe), können Datenverkehr von der VPC über den Tunnel empfangen. Außerdem führt das virtuelle private Gateway keinen Datenverkehr, der nicht für die angegebenen IP-Präfixe bestimmt ist, durch den Tunnel. Nachdem Sie eine VPN-Verbindung konfiguriert haben, müssen Sie möglicherweise einige Minuten warten, bis sie erstellt wurde.
- **Routing-Optionen konfigurieren**. Damit das Netzwerk der VPC die Netzwerke auf der Citrix ADC Seite über den CloudBridge Connector-Tunnel erreicht, müssen Sie die Routingtabelle der VPC so konfigurieren, dass Routen für die Netzwerke auf der Citrix ADC-Seite enthalten und diese Routen auf das virtuelle private Gateway verweisen. Sie können Routen in die Routingtabelle einer VPC auf eine der folgenden Arten aufnehmen:
  - **Routenpropagierung aktivieren**. Sie können die Routenpropagierung für die Routingtabelle aktivieren, sodass Routen automatisch an die Tabelle weitergegeben werden. Die statischen IP-Präfixe, die Sie für die VPN-Konfiguration angeben, werden an die Routingtabelle weitergegeben, nachdem Sie die VPN-Verbindung erstellt haben.
  - **Geben Sie Statische Routen manuell**ein. Wenn Sie die Routenpropagierung nicht

aktivieren, müssen Sie die statischen Routen für die Netzwerke auf der Citrix ADC Seite manuell eingeben.

- **Konfiguration herunterladen**. Nachdem die Konfiguration des CloudBridge Connector-Tunnels (VPN-Verbindung) in AWS erstellt wurde, laden Sie die Konfigurationsdatei der VPN-Verbindung auf Ihr lokales System herunter. Möglicherweise benötigen Sie die Informationen in der Konfigurationsdatei zum Konfigurieren des CloudBridge Connector-Tunnels auf der Citrix ADC Appliance.

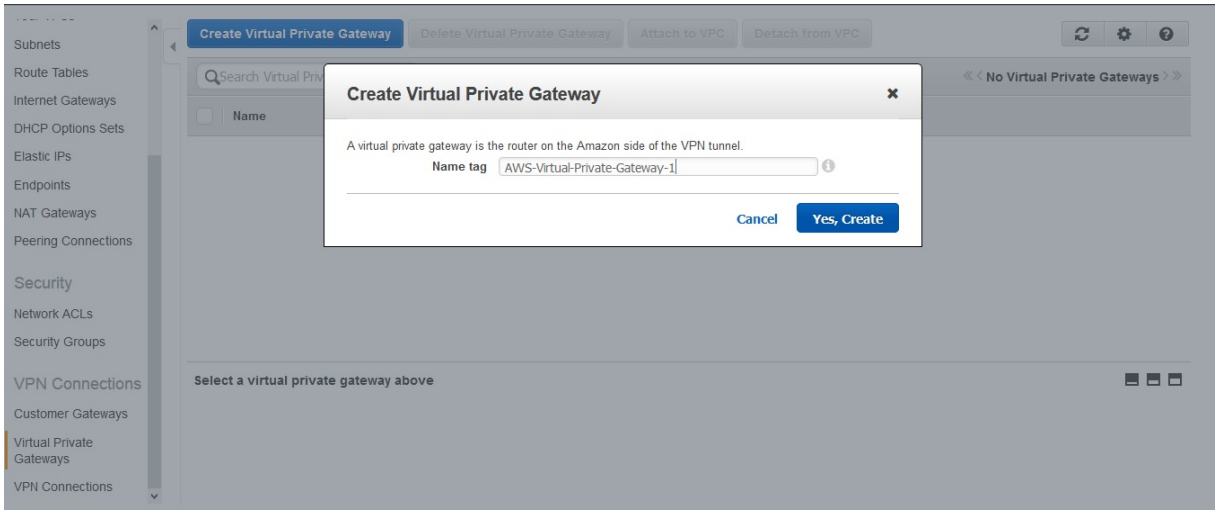
So erstellen Sie ein Kundengateway

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Navigieren Sie zu **VPN-Verbindungen** > **Kundengateways** und klicken Sie auf **Kundengateway erstellen** .
3. **Legen Sie im Dialogfeld Customer Gateway erstellen** die folgenden Parameter fest, und klicken Sie dann auf **Ja, Erstellen** :
   - **Namensschild**. Ein Name für das Kundengateway.
   - **Routingliste**. Art des Routing zwischen der Citrix ADC Appliance und dem virtuellen privaten AWS-Gateway für Werberouten durch den CloudBridge Connector-Tunnel. Wählen Sie **Statisches Routing** aus der Liste **Routing** aus. **Hinweis**: Die Citrix ADC Appliance unterstützt das BGP-Protokoll in einem CloudBridge Connector-Tunnel zum AWS-Gateway nicht. Daher müssen auf beiden Seiten des CloudBridge Connector-Tunnels geeignete statische Routen verwendet werden, um den Verkehr durch den Tunnel ordnungsgemäß zu leiten.
   - **IP Adresse**. Internetroutbare CloudBridge Connector-Tunnelendpunkt-IP-Adresse auf der Citrix ADC Seite. Bei der IP-Adresse kann es sich um eine mit dem Internet betriebene Citrix ADC besetzte Subnetz-IP (SNIP) -Adresse oder, wenn sich die Citrix ADC-Appliance hinter einem NAT-Gerät befindet, eine internetroutable NAT-IP-Adresse, die die SNIP-Adresse darstellt.

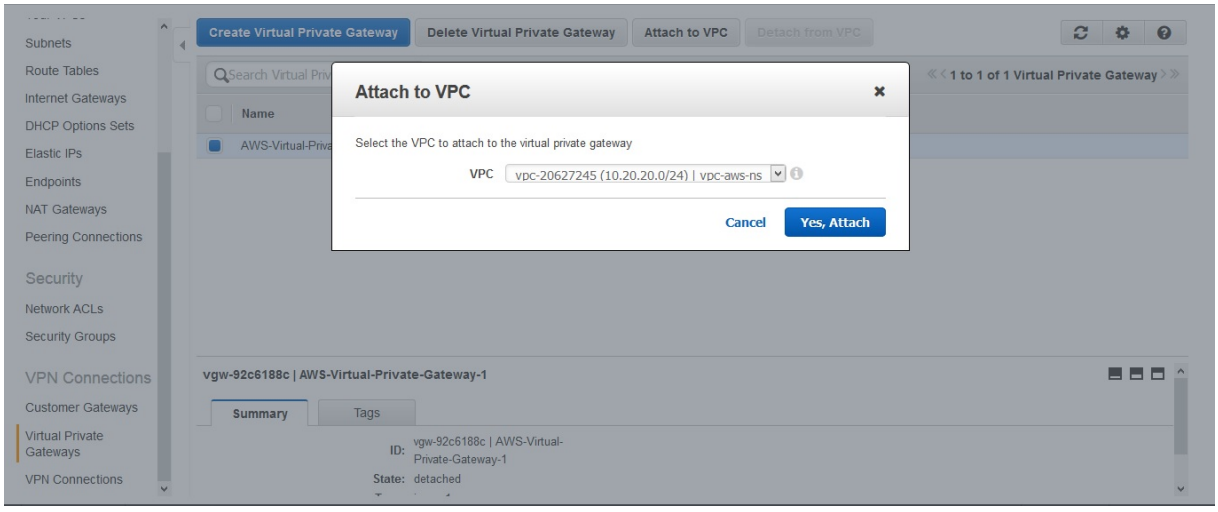


So erstellen Sie ein virtuelles privates Gateway und fügen es an eine VPC an

1. Navigieren Sie zu **VPN-Verbindungen** > **Virtual Private Gateways**, und klicken Sie dann auf Virtual Private Gateway erstellen.
2. Geben Sie einen Namen für das virtuelle private Gateway ein, und klicken Sie dann auf Ja, Erstellen.



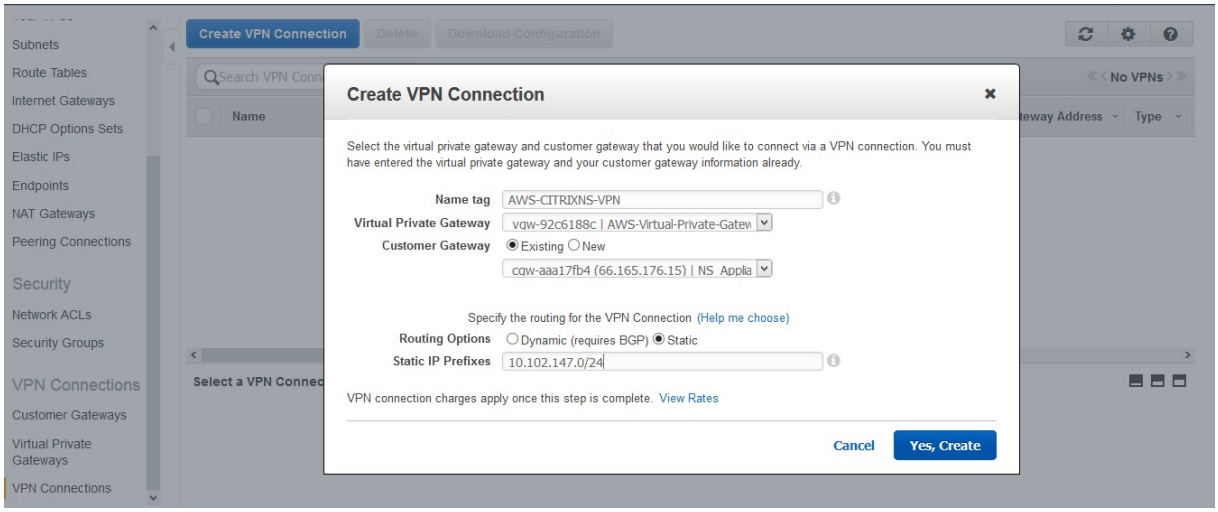
1. Wählen Sie das virtuelle private Gateway aus, das Sie erstellt haben, und klicken Sie dann auf An VPC anhängen.
2. Wählen Sie im Dialogfeld An VPC anhängen die VPC aus der Liste aus, und wählen Sie dann Ja, Anhängen.



So erstellen Sie eine VPN-Verbindung:

1. Navigieren Sie zu VPN-Verbindungen > VPN-Verbindungen, und klicken Sie dann auf VPN-Verbindung erstellen.
2. Legen Sie im Dialogfeld VPN-Verbindung erstellen die folgenden Parameter fest und wählen Sie dann Ja, Erstellen:
   - **Namensschild**. Ein Name für die VPN-Verbindung.

- **Virtuelles privates Gateway**. Wählen Sie das virtuelle private Gateway aus, das Sie zuvor erstellt haben.
- **Kunden-Gateway**. Wählen Sie Bestehend aus. Wählen Sie dann aus der Dropdownliste das Kundengateway aus, das Sie zuvor erstellt haben.
- **Weiterleitungsoptionen**. Art des Routing zwischen dem virtuellen privaten Gateway und dem Kundengateway (Citrix ADC Appliance). Wählen Sie Statisch aus. Geben Sie im Feld Statische IP-Präfixe die IP-Präfixe für das Subnetz auf Citrix ADC Seite an, getrennt durch Kommas.



So aktivieren Sie die Routenpropagierung:

1. Navigieren Sie zu **Routing Tables**, und wählen Sie die Routingtabelle aus, die dem Subnetz zugeordnet ist, dessen Datenverkehr den CloudBridge Connector-Tunnel durchlaufen soll.

> **Hinweis:**
>
> Standardmäßig ist dies die wichtigste Routingtabelle für die VPC.

1. Wählen Sie im Detailbereich auf der Registerkarte **Routenpropagierung** die Option **Bearbeiten**, wählen Sie das virtuelle private Gateway aus, und klicken Sie dann auf **Speichern** .

So geben Sie statische Routen manuell ein:

1. Navigieren Sie zu **Routentabellen**, und wählen Sie die Routingtabelle aus.
2. Klicken Sie auf der Registerkarte **Routen** auf **Bearbeiten** .
3. Geben Sie im Feld **Ziel** die statische Route ein, die von Ihrem CloudBridge Connector-Tunnel (VPN-Verbindung) verwendet wird.
4. Wählen Sie die virtuelle private Gateway -ID aus der Liste **Ziel** aus, und klicken Sie dann auf **Speichern** .

So laden Sie die Konfigurationsdateiherunter:

1. Navigieren Sie zu **VPN-Verbindung**, wählen Sie eine VPN-Verbindung aus, und klicken Sie dann

auf **Konfiguration herunterladen**.

2. Legen **Sie im Dialogfeld Download-Konfiguration** die folgenden Parameter fest, und klicken Sie dann auf **Ja, Download** .
   - **Verkäufer**. Wählen Sie **Generisch**aus.
   - **Plattform**. Wählen Sie **Generisch**aus.
   - **Software**. Wählen Sie **Vendor Agnostic**aus.

Konfigurieren der Citrix ADC Appliance für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und einem virtuellen privaten Gateway in der AWS-Cloud zu konfigurieren, führen Sie die folgenden Aufgaben auf der Citrix ADC-Appliance aus.
Sie können entweder die Citrix ADC Befehlszeile oder die GUI verwenden.

- **Erstellen Sie ein IPsec-Profil**. Eine IPsec-Profilentität gibt die IPsec-Protokollparameter an, z. B. IKE-Version, Verschlüsselungsalgorithmus, Hash-Algorithmus und PSK, die vom IPsec-Protokoll im CloudBridge Connector-Tunnel verwendet werden sollen.
- **Erstellen Sie einen IP-Tunnel, der das IPsec-Protokoll verwendet, und ordnen Sie ihm das IPsec-Profil zu**. Ein IP-Tunnel gibt die lokale IP-Adresse (eine auf der Citrix ADC Appliance konfigurierte SNIP-Adresse), die Remote-IP-Adresse (die öffentliche IP-Adresse des virtuellen privaten Gateway in AWS), das zum Einrichten des CloudBridge Connector-Tunnels verwendete Protokoll (IPsec) und eine IPsec-Profilentität an. Die erstellte IP-Tunnelentität wird auch als CloudBridge Connector-Tunnelentität bezeichnet.
- **Erstellen Sie eine PBR-Regel und verknüpfen Sie sie mit dem IP-Tunnel**. Eine PBR-Entität gibt einen Satz von Regeln und eine IP-Tunnelentität (CloudBridge Connector Tunnel) an. Der Quell-IP-Adressbereich und der Ziel-IP-Adressbereich sind die Bedingungen für die PBR-Entität. Legen Sie den Quell-IP-Adressbereich fest, um das Citrix ADC-seitige Subnetz anzugeben, dessen Datenverkehr den Tunnel durchqueren soll, und legen Sie den IP-Zieladressbereich fest, um das AWS VPC-Subnetz anzugeben, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll. Jedes Anforderungspaket, das von einem Client im Subnetz auf der Citrix ADC Seite stammt und an einen Server im AWS-Cloud-Subnetz bestimmt ist und dem Quell- und Ziel-IP-Bereich der PBR-Entität entspricht, wird über den CloudBridge Connector-Tunnel gesendet, der der PBR-Entität zugeordnet ist.

So erstellen Sie ein IPSEC-Profil über die Citrix ADC Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add ipsec profile <name> -psk <string> -**ikeVersion** v1`
- `show ipsec profile** <name>`

So erstellen Sie einen IPSEC-Tunnel und binden das IPSEC-Profil mit der Citrix ADC Befehlszeile an ihn

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

So erstellen Sie eine PBR-Regel und binden den IPSEC-Tunnel mit der Citrix ADC Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP** <subnet-range> -*ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

Mit den folgenden Befehlen werden alle Einstellungen der Citrix ADC Appliance NS_Appliance-1 erstellt, die in Beispiel für CloudBridge Connector-Konfiguration und Datenfluss verwendet werden.

```
1      > add ipsec profile NS_AWS_IPSec_Profile -psk
           DkiMgMdcbqvYREEuIvxsbKkW0Foyabcd -ikeVersion v1  - lifetime
           31536000
2      Done
3      > add iptunnel NS_AWS_Tunnel 168.63.252.133 255.255.255.255
           66.165.176.15  - protocol IPSEC  - ipsecProfileName
           NS_AWS_IPSec_Profile
4
5      Done
6      > add pbr NS_AWS_Pbr -srcIP 10.102.147.0-10.102.147.255  - destIP
           10.20.0.0-10.20.255.255  - ipTunnel NS_AWS_Tunnel
7      Done
8
9      > apply pbrs
10
11     Done
12 <!--NeedCopy-->
```

So erstellen Sie ein IPSEC-Profil mit der GUI

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IPSec-Profil**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie im Dialogfeld **IPsec-Profil hinzufügen** die folgenden Parameter fest:
    - Name
    - Verschlüsselungsalgorithmus
    - Hash-Algorithmus

- IKE-Protokollversion (wählen Sie V1)

4. Wählen Sie die **Authentifizierungsmethode für den vorinstallierten Schlüssel** aus, und legen Sie den Parameter **Pre-Shared Key Exists** fest.
5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So erstellen Sie einen IP-Tunnel und binden das IPSEC-Profil mit der GUI an ihn

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IP-Tunnel**.
2. Klicken Sie auf der Registerkarte **IPv4-Tunnel** auf Hinzufügen.
3. Legen Sie im Dialogfeld **IP-Tunnel hinzufügen** die folgenden Parameter fest:
   - Name
   - Remote-IP
   - Remote-Maske
   - Lokaler IP-Typ (Wählen Sie in der Dropdownliste Lokaler IP-Typ die Option Subnetz-IP).
   - Lokale IP (Alle konfigurierten IPs des ausgewählten IP-Typs befinden sich in der Dropdownliste Lokale IP. Wählen Sie die gewünschte IP aus der Liste aus.)
   - Protokoll
   - IPsec-Profil
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So erstellen Sie eine PBR-Regel und binden den IPSEC-Tunnel mit der GUI daran

1. Navigieren Sie zu **System** > **Netzwerk** > **PBR**.
2. Klicken Sie auf der Registerkarte **PBR** auf **Hinzufügen**.
3. **Legen Sie im Dialogfeld PBR erstellen** die folgenden Parameter fest:
   - Name
   - Aktion
   - Nächster Hop-Typ (Wählen Sie IP Tunnel)
   - IP-Tunnelname
   - Quell-IP Niedrig
   - Quell-IP hoch
   - Ziel-IP niedrig
   - Ziel-IP hoch
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Die entsprechende neue CloudBridge Connector-Tunnelkonfiguration auf der Citrix ADC Appliance wird in der GUI angezeigt.

Der aktuelle Status des CloudBridge-Connector-Tunnels wird im Bereich Konfigurierter CloudBridge-Connector angezeigt. Ein grüner Punkt zeigt an, dass der Tunnel oben ist. Ein roter Punkt zeigt an, dass der Tunnel heruntergefahren ist.

Überwachung des CloudBridge Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer Citrix ADC Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen.
Weitere Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer Citrix ADC Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

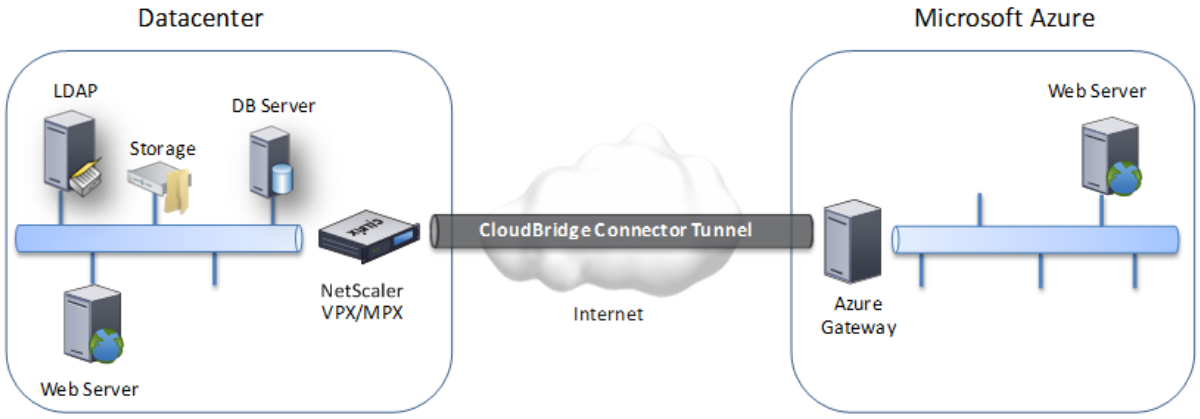
Konfigurieren eines CloudBridge Connector-Tunnels zwischen einem Rechenzentrum und einer Azure-Cloud

May 10, 2022

Die Citrix ADC Appliance bietet Konnektivität zwischen Ihren Unternehmensdatenzentren und dem Microsoft-Cloud-Hosting-Anbieter Azure, wodurch Azure eine nahtlose Erweiterung des Unternehmensnetzwerks darstellt. Citrix ADC verschlüsselt die Verbindung zwischen dem Enterprise-Rechenzentrum und der Azure-Cloud, sodass alle zwischen den beiden übertragenen Daten sicher sind.

Funktionsweise des CloudBridge Connector-Tunnels

Um ein Datencenter mit der Azure-Cloud zu verbinden, richten Sie einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance, die sich im Rechenzentrum befindet, und einem Gateway in der Azure-Cloud ein. Die Citrix ADC Appliance im Rechenzentrum und das Gateway in der Azure-Cloud sind die Endpunkte des CloudBridge Connector-Tunnels und werden als Peers des CloudBridge Connector-Tunnels bezeichnet.



Ein CloudBridge Connector-Tunnel zwischen einem Rechenzentrum und einer Azure-Cloud verwendet die IPsec-Protokollsuite (Internet Protocol Security) im Tunnelmodus, um die Kommunikation

zwischen Peers im CloudBridge Connector-Tunnel zu sichern. In einem CloudBridge Connector-Tunnel stellt IPsec Folgendes sicher:

- Datenintegrität
- Datenursprungauthentifizierung
- Datenvertraulichkeit (Verschlüsselung)
- Schutz vor Replay-Angriffen

IPsec verwendet den Tunnelmodus, in dem das komplette IP-Paket verschlüsselt und dann gekapselt wird. Die Verschlüsselung verwendet das ESP-Protokoll (Encapsulating Security Payload), das die Integrität des Pakets mithilfe einer HMAC-Hash-Funktion gewährleistet und die Vertraulichkeit mithilfe eines Verschlüsselungsalgorithmus gewährleistet. Das ESP-Protokoll generiert nach Verschlüsselung der Nutzlast und Berechnung des HMAC einen ESP-Header und fügt ihn vor dem verschlüsselten IP-Paket ein. Das ESP-Protokoll generiert auch einen ESP-Trailer und fügt ihn am Ende des Pakets ein.

Das IPsec-Protokoll kapselt dann das resultierende Paket, indem ein IP-Header vor dem ESP-Header hinzugefügt wird. Im IP-Header wird die Ziel-IP-Adresse auf die IP-Adresse des CloudBridge Connecter-Peers festgelegt.

Peers im CloudBridge Connector-Tunnel verwenden das IKEv1 (Internet Key Exchange Version 1) -Protokoll (Teil der IPsec-Protokollsuite), um eine sichere Kommunikation auszuhandeln, wie folgt:

1. Die beiden Peers authentifizieren sich gegenseitig, indem sie eine vorab geteilte Schlüsselauthentifizierung verwenden, bei der die Peers eine Textzeichenfolge namens Pre-Shared Key (PSK) austauschen. Die vorab geteilten Schlüssel werden zur Authentifizierung gegeneinander zugeordnet. Damit die Authentifizierung erfolgreich ist, müssen Sie daher den gleichen vorab freigegebenen Schlüssel auf jedem Peers konfigurieren.
2. Die Kollegen verhandeln dann, um eine Einigung zu erzielen über:
   - Ein Verschlüsselungsalgorithmus
   - Kryptografische Schlüssel zum Verschlüsseln von Daten auf einem Peer und zum Entschlüsseln auf dem anderen.

   Diese Vereinbarung über das Sicherheitsprotokoll, den Verschlüsselungsalgorithmus und die kryptografischen Schlüssel wird als Security Association (SA) bezeichnet. SAs sind einseitig (Simplex). Wenn beispielsweise ein CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance in einem Rechenzentrum und einem Gateway in einer Azure-Cloud eingerichtet wird, verfügen sowohl die Datencenter-Appliance als auch das Azure-Gateway über zwei SAs. Eine SA wird für die Verarbeitung ausgehender Pakete verwendet, und die andere SA wird für die Verarbeitung eingehender Pakete verwendet. SAs verfallen nach einem bestimmten Zeitintervall, das als Lebensdauer bezeichnet wird.

Beispiel für CloudBridge Connector-Tunnelkonfiguration und Datenfluss

Betrachten Sie als Illustration des CloudBridge Connector Tunnels ein Beispiel, in dem ein CloudBridge Connector-Tunnel zwischen der Citrix ADC appliance CB_Appliance-1 in einem Rechenzentrum und dem Gateway Azure_Gateway-1 in der Azure-Cloud eingerichtet wird.

CB_Appliance-1 fungiert auch als L3-Router, der es einem privaten Netzwerk im Rechenzentrum ermöglicht, über den CloudBridge Connector-Tunnel ein privates Netzwerk in der Azure-Cloud zu erreichen. Als Router ermöglicht CB_Appliance-1 die Kommunikation zwischen Client CL1 im Rechenzentrum und Server S1 in der Azure-Cloud über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

In CB_Appliance-1 umfasst die CloudBridge Connector-Tunnelkonfiguration eine IPsec-Profilentität mit dem Namen CB_Azure_IPsec_Profile, eine CloudBridge Connector-Tunnelentität namens CB_Azure_Tunnel und eine richtlinienbasierte Routing-Entität mit dem Namen CB_Azure_Pbr.

Die IPsec-Profilentität CB_Azure_IPsec_Profile gibt die IPsec-Protokollparameter an, z. B. IKE-Version, Verschlüsselungsalgorithmus und Hash-Algorithmus, die vom IPsec-Protokoll im CloudBridge Connector-Tunnel verwendet werden sollen. CB_Azure_IPsec_Profile ist an die IP-Tunnelentität CB_Azure_Tunnel gebunden.

CloudBridge Connector-Tunnelentität CB_Azure_Tunnel gibt die lokale IP-Adresse (eine öffentliche IP-Adresse (SNIP), die auf der Citrix ADC Appliance konfiguriert ist), die Remote-IP-Adresse (die IP-Adresse des Azure_Gateway-1) und das Protokoll (IPsec) an, das zum Einrichten des CloudBridge Connector-Tunnels verwendet wird. CB_Azure_Tunnel ist an die PBR-Entität CB_Azure_Pbr gebunden.

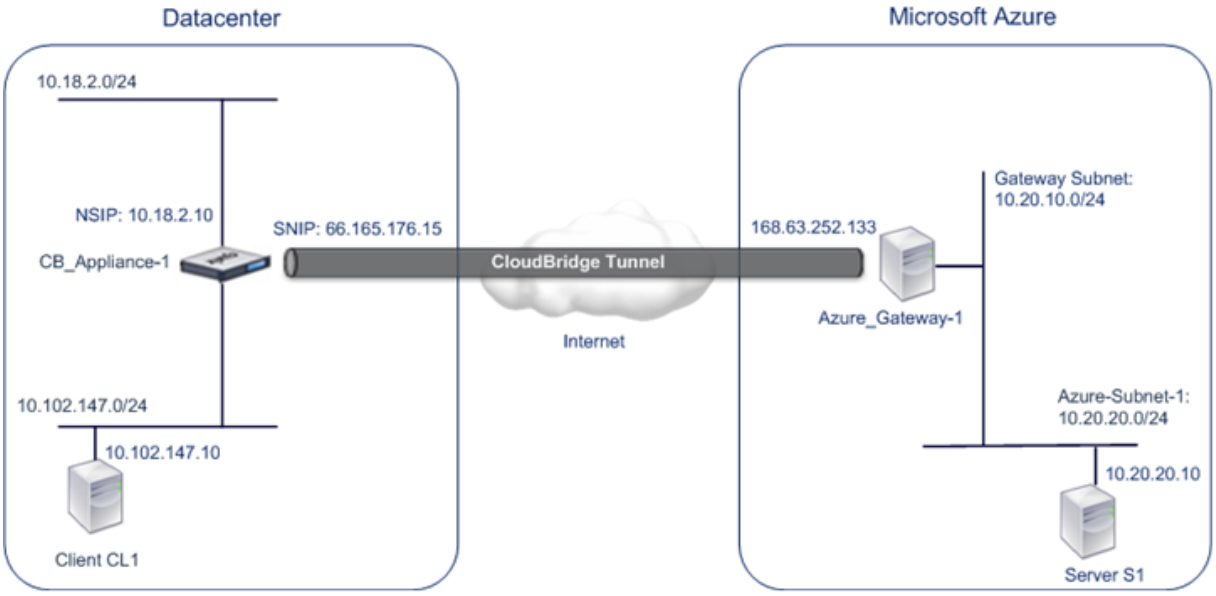
Die PBR-Entität CB_Azure_Pbr gibt einen Satz von Bedingungen und eine CloudBridge Connector-Tunnelentität (CB_Azure_tunnel) an. Der Quell-IP-Adressbereich und der Ziel-IP-Adressbereich sind die Bedingungen für CB_Azure_PBR. Der Quell-IP-Adressbereich und der Ziel-IP-Adressbereich werden als Subnetz im Datencenter bzw. Subnetz in der Azure-Cloud angegeben. Jedes Anforderungspaket, das von einem Client im Subnetz im Rechenzentrum stammt und für einen Server im Subnetz in der Azure-Cloud bestimmt ist, entspricht den Bedingungen in CB_Azure_PBR. Dieses Paket wird dann für die CloudBridge-Verarbeitung berücksichtigt und über den CloudBridge-Connector-Tunnel (CB_Azure_Tunnel) gesendet, der an die PBR-Entität gebunden ist.

Unter Microsoft Azure umfasst die CloudBridge Connector-Tunnelkonfiguration eine lokale Netzwerkentität namens My-Datacenter-Network, eine virtuelle Netzwerkentität mit dem Namen Azure-Network-for-CloudBridge-Tunnel und ein Gateway mit dem Namen Azure_Gateway-1.

Die lokale Netzwerkeinheit (lokal in Azure) My-Datacenter-Network gibt die IP-Adresse der Citrix ADC Appliance auf der Datencenterseite und das Datencenter-Subnetz an, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll. Die virtuelle Netzwerkeinheit Azure-Network-for-CloudBridge-Tunnel definiert in Azure ein privates Subnetz mit dem Namen Azure-Subnet-1. Der

Datenverkehr des Subnetzes durchläuft den CloudBridge Connector-Tunnel. Der Server S1 wird in diesem Subnetz bereitgestellt.

Die lokale Netzwerkeinheit My-Datacenter-Network ist der virtuellen Netzwerkeinheit Azure-Network-for-CloudBridge-Tunnel zugeordnet. Diese Zuordnung definiert die Remote- und lokalen Netzwerkdetails der CloudBridge Connector-Tunnelkonfiguration in Azure. Gateway Azure_Gateway-1 wurde für diese Zuordnung als CloudBridge-Endpunkt am Azure Ende des CloudBridge Connector-Tunnels erstellt.



Weitere Informationen zu den Einstellungen finden Sie im PDF-Dokument CloudBridge Connector Tunnel Settings .

Punkte, die für eine CloudBridge Connector-Tunnelkonfiguration zu beachten sind

Bevor Sie einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance im Rechenzentrum und Microsoft Azure konfigurieren, sollten Sie die folgenden Punkte beachten:

1. Die Citrix ADC Appliance muss über eine öffentliche IPv4-Adresse (Typ SNIP) verfügen, die als Tunnelendpunktadresse für den CloudBridge Connector-Tunnel verwendet werden kann. Außerdem sollte sich die Citrix ADC Appliance nicht hinter einem NAT-Gerät befinden.
2. Azure unterstützt die folgenden IPsec-Einstellungen für einen CloudBridge Connector-Tunnel. Daher müssen Sie bei der Konfiguration des Citrix ADC für den CloudBridge Connector-Tunnel dieselben IPsec-Einstellungen angeben.
   - IKE Version = v1
   - Verschlüsselungsalgorithmus = AES
   - Hash-Algorithmus = HMAC SHA1
3. Sie müssen die Firewall im Rechenzentrumsrand so konfigurieren, dass Folgendes zulässig ist.
   - Alle UDP-Pakete für Port 500

- Alle UDP-Pakete für Port 4500
- Alle ESP-Pakete (IP-Protokollnummer 50)

4. IKE Re-Keying, d. h. Neuverhandlung neuer kryptografischer Schlüssel zwischen den CloudBridge Connector-Tunnelendpunkten, um neue SAs einzurichten, wird nicht unterstützt. Wenn die Sicherheitszuordnungen (SAs) ablaufen, wechselt der Tunnel in den Status DOWN. Daher müssen Sie einen sehr großen Wert für die Lebensdauer von SAs festlegen.
5. Sie müssen Microsoft Azure konfigurieren, bevor Sie die Tunnelkonfiguration auf dem Citrix ADC angeben, da beim Einrichten der Tunnelkonfiguration in Azure die öffentliche IP-Adresse des Azure-Endes (Gateway) des Tunnels und der PSK automatisch generiert werden. Sie benötigen diese Informationen, um die Tunnelkonfiguration auf dem Citrix ADC anzugeben.

Konfigurieren des CloudBridge Connector-Tunnels

Zum Einrichten eines CloudBridge Connector-Tunnels zwischen Ihrem Rechenzentrum und Azure müssen Sie CloudBridge VPX/MPX in Ihrem Rechenzentrum installieren, Microsoft Azure für den CloudBridge Connector-Tunnel konfigurieren und dann die Citrix ADC Appliance im Rechenzentrum für den CloudBridge Connector-Tunnel konfigurieren.

Das Konfigurieren eines CloudBridge Connector-Tunnels zwischen einer Citrix ADC Appliance im Rechenzentrum und Microsoft Azure umfasst die folgenden Aufgaben:

1. **Einrichten der Citrix ADC Appliance im Rechenzentrum**. Diese Aufgabe umfasst die Bereitstellung und Konfiguration einer physischen Citrix ADC Appliance (MPX) oder die Provisioning und Konfiguration einer virtuellen Citrix ADC-Appliance (VPX) auf einer Virtualisierungsplattform im Rechenzentrum.
2. **Konfigurieren von Microsoft Azure für den CloudBridge Connector-Tunnel**. Bei dieser Aufgabe werden lokale Netzwerk-, virtuelle Netzwerk- und Gateway -Entitäten in Azure erstellt. Die lokale Netzwerkentität gibt die IP-Adresse des CloudBridge Connector-Tunnelendpunkts (der Citrix ADC Appliance) auf der Datencenterseite und das Datencenter-Subnetz an, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll. Das virtuelle Netzwerk definiert ein Netzwerk in Azure. Das Erstellen des virtuellen Netzwerks umfasst die Definition eines Subnetzes, dessen Datenverkehr den zu bildenden CloudBridge Connector-Tunnel durchqueren soll. Anschließend verknüpfen Sie das lokale Netzwerk mit dem virtuellen Netzwerk. Schließlich erstellen Sie ein Gateway, das zum Endpunkt am Azure-Ende des CloudBridge Connector-Tunnels wird.
3. **Konfigurieren der Citrix ADC Appliance im Rechenzentrum für den CloudBridge Connector-Tunnel**. Diese Aufgabe umfasst das Erstellen eines IPsec-Profils, einer IP-Tunnelentität und einer PBR-Entität in der Citrix ADC Appliance im Rechenzentrum. Die IPsec-Profilentität gibt die IPsec-Protokollparameter an, z. B. IKE-Version, Verschlüsselungsalgorithmus, Hash-Algorithmus und PSK, die im CloudBridge Connector-Tunnel verwendet werden sollen. Der IP-Tunnel gibt die IP-Adresse sowohl der CloudBridge Connector-Tunnelendpunkte (der Citrix

ADC Appliance im Rechenzentrum und des Gateway in Azure) als auch des Protokolls an, das im CloudBridge Connector-Tunnel verwendet werden soll. Anschließend verknüpfen Sie die IPsec-Profilentität mit der IP-Tunnelentität. Die PBR-Entität gibt die beiden Subnetze im Datencenter und in der Azure-Cloud an, die über den CloudBridge Connector-Tunnel miteinander kommunizieren sollen. Anschließend ordnen Sie die IP-Tunnelentität der PBR-Entität zu.

Konfigurieren von Microsoft Azure für den CloudBridge Connector-Tunnel

Um eine CloudBridge Connector-Tunnelkonfiguration in Microsoft Azure zu erstellen, verwenden Sie das Microsoft Windows Azure-Verwaltungsportal, das eine webbasierte grafische Oberfläche zum Erstellen und Verwalten von Ressourcen in Microsoft Azure ist.

Bevor Sie mit der CloudBridge Connector-Tunnelkonfiguration in der Azure-Cloud beginnen, stellen Sie sicher, dass:

- Sie haben ein Benutzerkonto für Microsoft Azure.
- Sie haben ein konzeptionelles Verständnis von Microsoft Azure.
- Sie sind mit dem Microsoft Windows Azure-Verwaltungsportal vertraut.

Um einen CloudBridge Connector-Tunnel zwischen einem Rechenzentrum und einer Azure-Cloud zu konfigurieren, führen Sie die folgenden Aufgaben unter Microsoft Azure mithilfe des Microsoft Windows Azure-Verwaltungsportal aus:

- **Erstellen Sie eine lokale Netzwerkentität**. Erstellen Sie eine lokale Netzwerkentität in Windows Azure, um die Netzwerkdetails des Rechenzentrums anzugeben. Eine lokale Netzwerkentität gibt die IP-Adresse des CloudBridge Connector-Tunnelendpunkts (Citrix ADC) auf der Datencenterseite und das Datencenter-Subnetz an, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll.
- **Erstellen Sie ein virtuelles Netzwerk**. Erstellen Sie eine virtuelle Netzwerkentität, die ein Netzwerk in Azure definiert. Diese Aufgabe umfasst das Definieren eines privaten Adressraums, in dem Sie einen Bereich von privaten Adressen und Subnetzen angeben, die zu dem im Adressraum angegebenen Bereich gehören. Der Datenverkehr der Subnetze durchquert den CloudBridge Connector-Tunnel. Anschließend verknüpfen Sie eine lokale Netzwerkentität mit der virtuellen Netzwerkentität. Mit dieser Zuordnung kann Azure eine Konfiguration für einen CloudBridge Connector-Tunnel zwischen dem virtuellen Netzwerk und dem Rechenzentrumsnetzwerk erstellen. Ein Gateway (das erstellt werden soll) in Azure für dieses virtuelle Netzwerk ist der CloudBridge-Endpunkt am Azure Ende des CloudBridge-Connector-Tunnels. Anschließend definieren Sie ein privates Subnetz für das zu erstellende Gateway. Dieses Subnetz gehört zu dem Bereich, der im Adressraum in der virtuellen Netzwerkentität angegeben ist.
- **Erstellen Sie ein Gateway in Windows Azure**. Erstellen Sie ein Gateway, das zum Endpunkt am Azure-Ende des CloudBridge Connector-Tunnels wird. Azure weist aus seinem Pool öffentlicher

IP-Adressen dem erstellten Gateway eine IP-Adresse zu.

- **Sammeln Sie die öffentliche IP-Adresse des Gateway und den vorab freigegebenen Schlüssel.** Bei einer CloudBridge Connector-Tunnelkonfiguration in Azure werden die öffentliche IP-Adresse des Gateway und der Pre-Shared Key (PSK) automatisch von Azure generiert. Notieren Sie sich diese Informationen. Sie benötigen es für die Konfiguration des CloudBridge Connector-Tunnels auf dem Citrix ADC im Rechenzentrum.

> **Hinweis:**
>
> Die Verfahren zum Konfigurieren von Microsoft Azure für einen CloudBridge Connector-Tunnel können sich je nach Microsoft Azure-Release-Zyklus im Laufe der Zeit ändern. Die neuesten Verfahren finden Sie in der Microsoft Azure-Dokumentation.

Konfigurieren der Citrix ADC Appliance im Rechenzentrum für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel zwischen einem Rechenzentrum und einer Azure-Cloud zu konfigurieren, führen Sie die folgenden Aufgaben auf dem Citrix ADC im Rechenzentrum aus. Sie können entweder die Citrix ADC Befehlszeile oder die GUI verwenden:

- **Erstellen Sie ein IPsec-Profil**. Eine IPsec-Profilentität gibt die IPsec-Protokollparameter an, z. B. IKE-Version, Verschlüsselungsalgorithmus, Hash-Algorithmus und PSK, die vom IPsec-Protokoll im CloudBridge Connector-Tunnel verwendet werden sollen.
- **Erstellen Sie einen IP-Tunnel mit IPsec-Protokoll und ordnen Sie ihm das IPsec-Profil zu**. Ein IP-Tunnel gibt die lokale IP-Adresse (eine öffentliche SNIP-Adresse, die auf der Citrix ADC Appliance konfiguriert ist), die Remote-IP-Adresse (die öffentliche IP-Adresse des Gateway in Azure), das zum Einrichten des CloudBridge Connector-Tunnels verwendet wird, und eine IPsec-Profilentität an. Die erstellte IP-Tunnelentität wird auch als CloudBridge Connector-Tunnelentität bezeichnet.
- **Erstellen Sie eine PBR-Regel, und ordnen Sie den IP-Tunnel zu**. Eine PBR-Entität gibt einen Satz von Bedingungen und eine IP-Tunnelentität (CloudBridge Connector Tunnel) an. Der Quell-IP-Adressbereich und der Ziel-IP-Bereich sind die Bedingungen für die PBR-Entität. Sie müssen den Quell-IP-Adressbereich festlegen, um das Datencenter-Subnetz anzugeben, dessen Datenverkehr den Tunnel durchqueren soll, und den IP-Zieladressbereich, um das Azure-Subnetz anzugeben, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll. Jedes Anforderungspaket, das von einem Client im Subnetz im Rechenzentrum stammt und für einen Server im Subnetz in der Azure-Cloud bestimmt ist, entspricht dem Quell- und Ziel-IP-Bereich der PBR-Entität. Dieses Paket wird dann für die CloudBridge Connector-Tunnelverarbeitung berücksichtigt und über den CloudBridge Connector-Tunnel gesendet, der der PBR-Entität zugeordnet ist.

Die GUI kombiniert all diese Aufgaben in einem einzigen Assistenten namens CloudBridge Connector

Wizard.
So erstellen Sie ein IPSEC-Profil mit der Citrix ADC Befehlszeile:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ipsec profile <name> -psk <string> -ikeVersion v1
```

So erstellen Sie einen IPSEC-Tunnel und binden das IPSEC-Profil mithilfe der Citrix ADC Befehlszeile an dieses Profil:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -
ipsecProfileName <string>
```

So erstellen Sie eine PBR-Regel und binden den IPSEC-Tunnel mit der Citrix ADC Befehlszeile

```
add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> ipTunnel
 <tunnelName> apply pbrs
```

Beispielkonfiguration

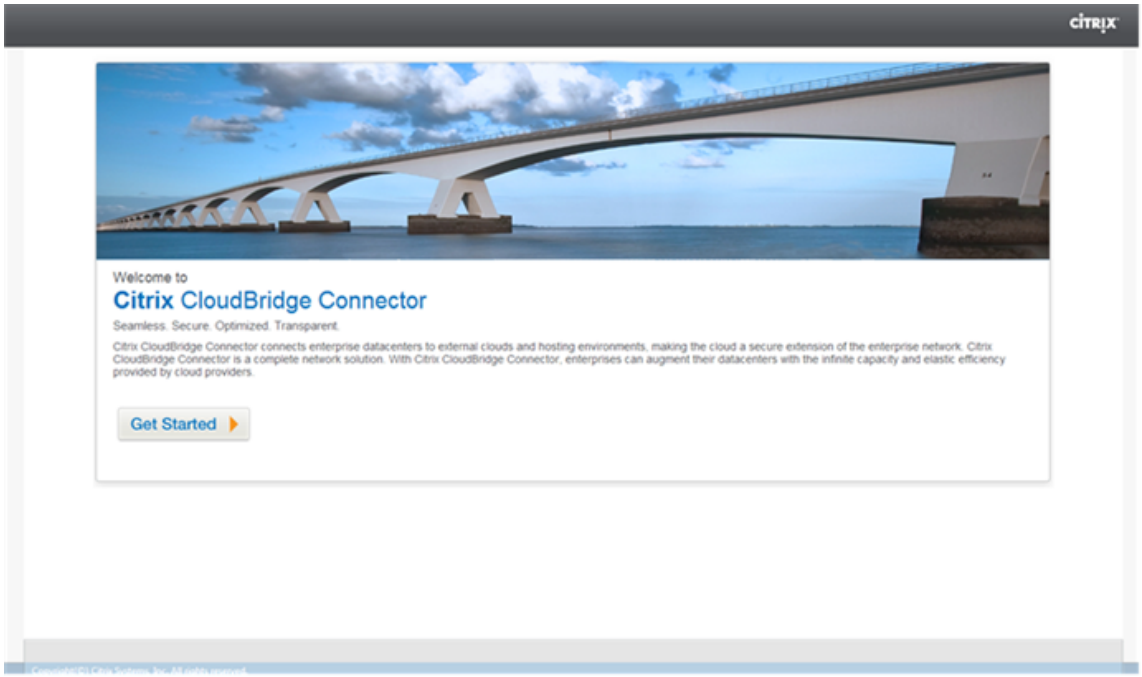
Mit den folgenden Befehlen werden alle Einstellungen der Citrix ADC Appliance CB_Appliance-1 erstellt, die in Beispiel für CloudBridge Connector-Konfiguration und Datenfluss verwendet werden.

```
1  > add ipsec profile CB_Azure_IPSec_Profile -psk
       DkiMgMdcbqvYREEuIvxsbKkW0FOyDiLM  -ikeVersion v1  - lifetime 31536000
2  Done
3
4  >  add iptunnel CB_Azure_Tunnel 168.63.252.133 255.255.255.255
       66.165.176.15  - protocol IPSEC  - ipsecProfileName
       CB_Azure_IPSec_Profile
5  Done
6
7  > add pbr CB_Azure_Pbr -srcIP 10.102.147.0-10.102.147.255  - destIP
       10.20.0.0-10.20.255.255  - ipTunnelCB_Azure_Tunnel
8  Done
9
10 > apply pbrs
11 Done
12 <!--NeedCopy-->
```

So konfigurieren Sie einen CloudBridge Connector-Tunnel in einer Citrix ADC Appliance mit der GUI

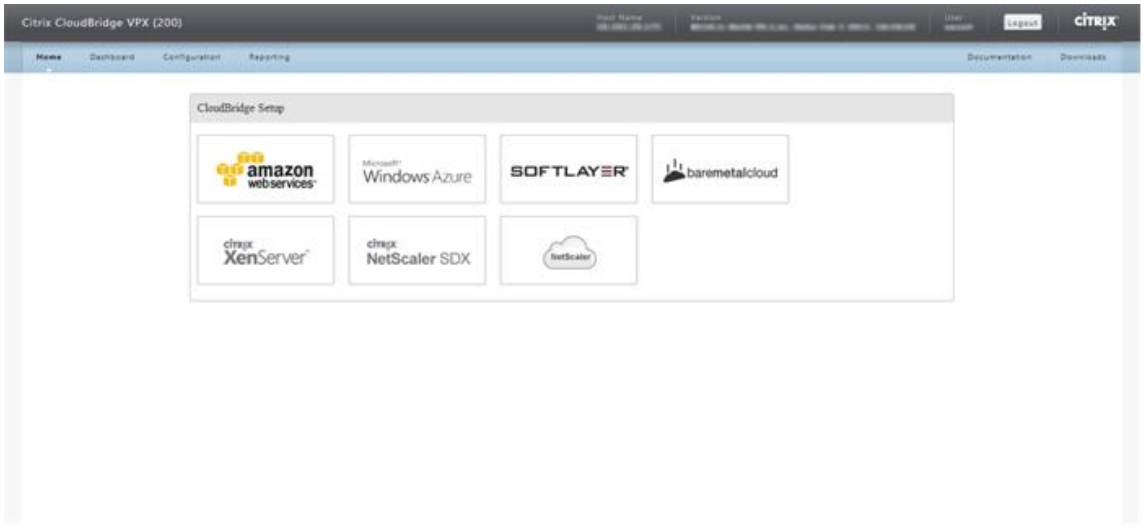
1. Greifen Sie mithilfe eines Webbrowsers auf die Benutzeroberfläche zu, um eine Verbindung mit der IP-Adresse der Citrix ADC Appliance im Rechenzentrum herzustellen.
2. Navigieren Sie zu **System** > **CloudBridge Connector** .

3. Klicken Sie im rechten Bereich unter **Erste Schritte**auf **CloudBridge erstellen/überwachen**.
4. Klicken Sie auf **Erste Schritte**.



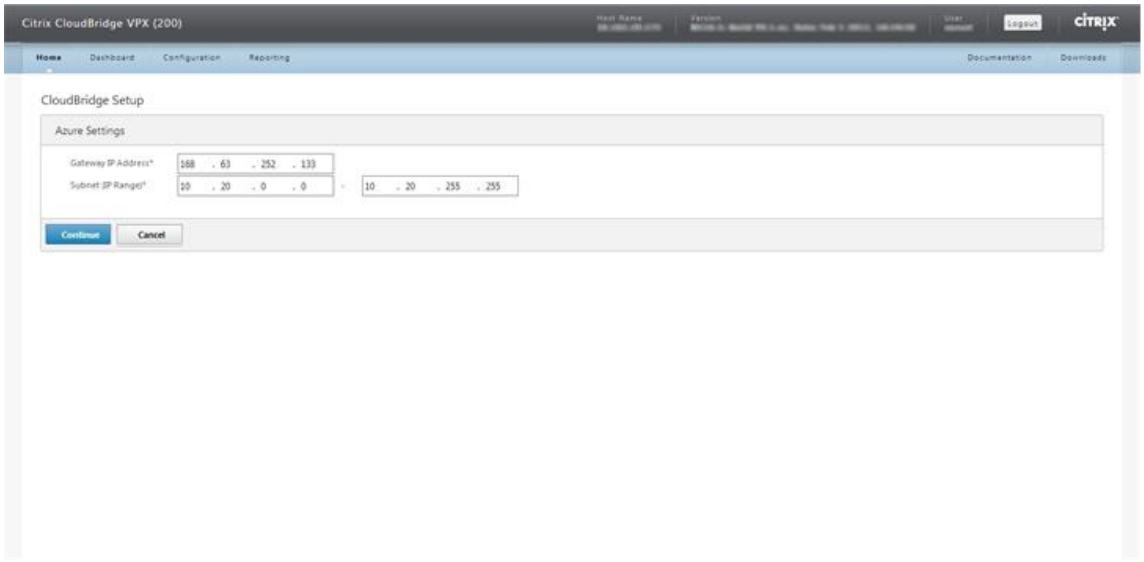
> **Hinweis**: Wenn Sie bereits einen CloudBridge Connector-Tunnel auf der Citrix ADC Appliance konfiguriert haben, wird dieser Bildschirm nicht angezeigt, und Sie gelangen zum Setup-Bereich von CloudBridge Connector.

5. Klicken Sie im Bereich CloudBridge-Setup auf **Microsoft Windows Azure**.

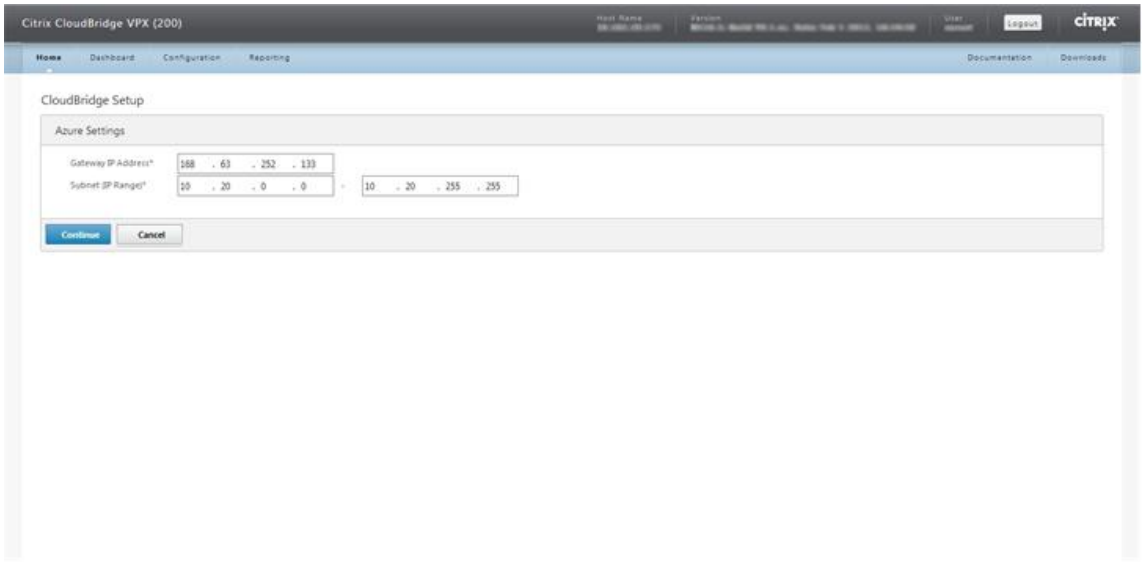


6. Geben Sie im Bereich Azure-Einstellungen im Feld **Gateway-IP-Adresse** die IP-Adresse des Azure-Gateways ein. Der CloudBridge Connector-Tunnel wird dann zwischen der Citrix ADC Appliance und dem Gateway eingerichtet. Geben Sie in den Textfeldern **Subnet (IP-Bereich)** einen Subnetzbereich (in der Azure-Cloud) an, dessen Datenverkehr den CloudBridge

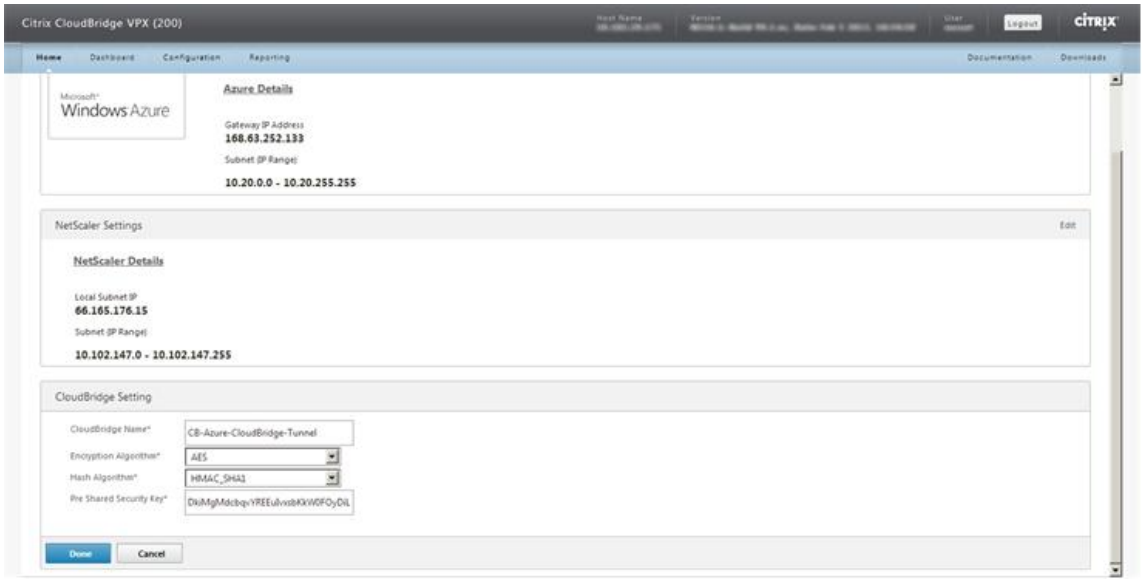
Connector-Tunnel durchqueren soll. Klicken Sie auf **Weiter**.



7. Wählen Sie im Bereich Citrix ADC-Einstellungen aus der Dropdownliste **Lokale Subnetz-IP** eine öffentlich zugängliche SNIP-Adresse aus, die auf der Citrix ADC Appliance konfiguriert ist. Geben Sie in **Subnetz-Textfeldern (IP-Bereich)** einen lokalen Subnetzbereich an, dessen Datenverkehr den CloudBridge Connector-Tunnel durchqueren soll. Klicken Sie auf **Weiter**.



8. Geben Sie im Bereich **CloudBridge-Einstellung** im Textfeld CloudBridge-Name einen Namen für die CloudBridge ein, die Sie erstellen möchten.



9. Wählen Sie in den Dropdownlisten Verschlüsselungsalgorithmus und Hash-Algorithmus die Algorithmen AES bzw. HMAC_SHA1 aus. Geben Sie im Textfeld Pre Shared Security Key den Sicherheitsschlüssel ein.
10. Klicken Sie auf **Fertig**.

Überwachung des CloudBridge Connector-Tunnels

Sie können Statistiken zur Überwachung der Leistung eines CloudBridge Connector-Tunnels zwischen der Citrix ADC Appliance im Rechenzentrum und Microsoft Azure anzeigen. Verwenden Sie GUI- oder Citrix ADC Befehlszeile, um CloudBridge Connector-Tunnelstatistiken auf der Citrix ADC-Appliance anzuzeigen. Verwenden Sie das Microsoft Windows Azure-Verwaltungsportal, um CloudBridge Connector-Tunnelstatistiken in Microsoft Azure anzuzeigen.

Anzeigen von CloudBridge Connector-Tunnelstatistiken in der Citrix ADC Appliance

Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer Citrix ADC Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

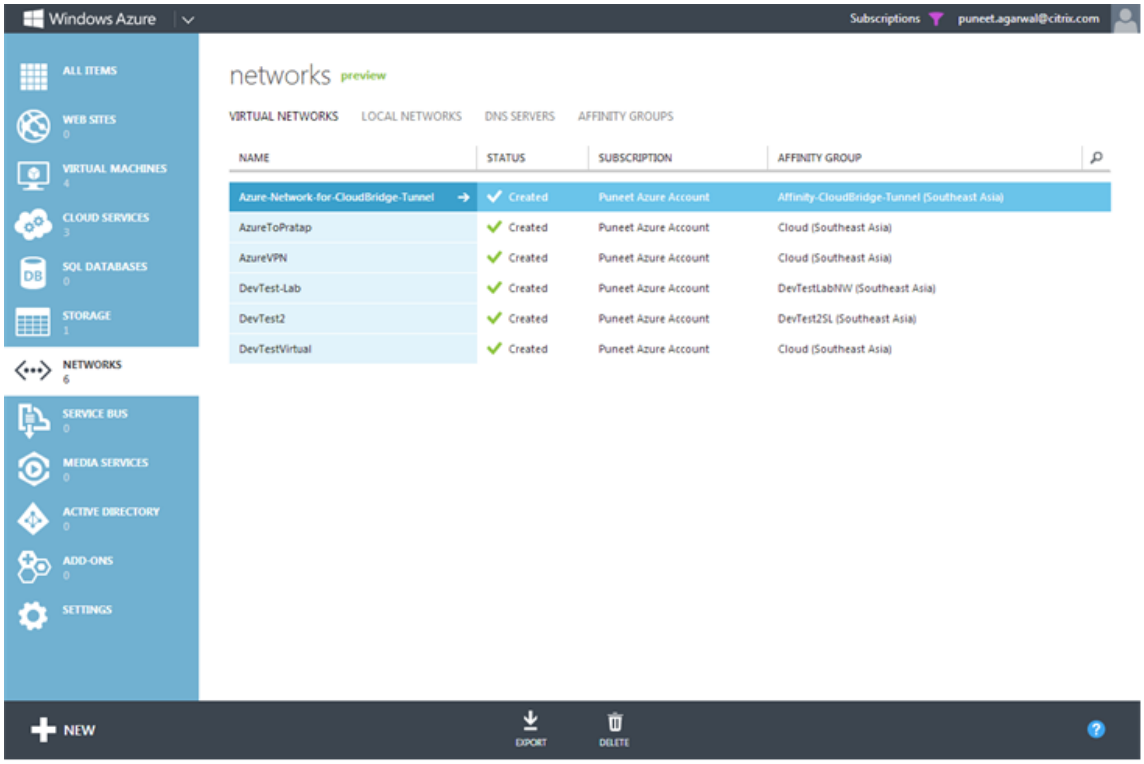
Anzeigen von CloudBridge Connector-Tunnelstatistiken in Microsoft Azure

In der folgenden Tabelle sind die statistischen Leistungsindikatoren aufgeführt, die für die Überwachung von CloudBridge Connector-Tunneln in Microsoft Azure verfügbar sind.

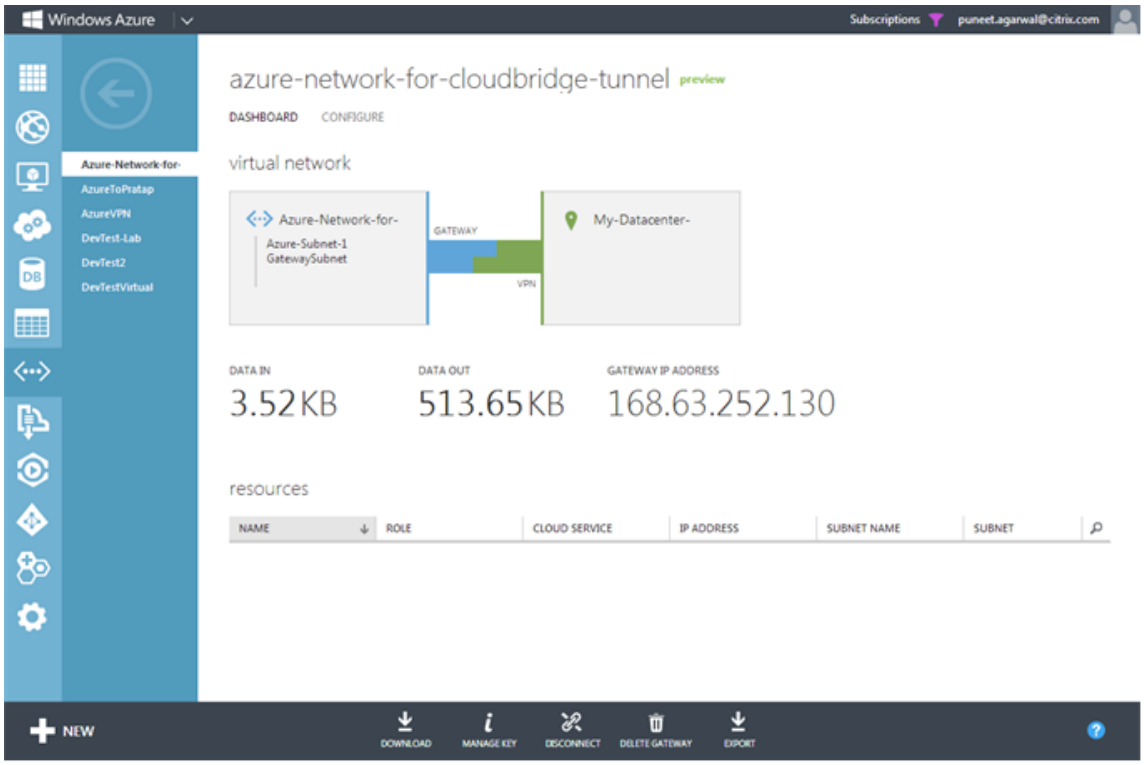
Statistischer Zähler	Gibt an
DATA IN	Gesamtanzahl der Kilobyte, die vom Azure-Gateway über den CloudBridge Connector-Tunnel seit der Erstellung des Gateways empfangen wurden.
DATA OUT	Gesamtanzahl der Kilobyte, die vom Azure-Gateway über den CloudBridge Connector-Tunnel seit der Erstellung des Gateways gesendet wurden.

So zeigen Sie CloudBridge Connector-Tunnelstatistiken mithilfe des Microsoft Windows Azure-Verwaltungsportal an

1. Melden Sie sich mit den Anmeldeinformationen Ihres Microsoft Azure-Kontos am Windows Azure Management Portal an.
2. Klicken Sie im linken Bereich auf **NETWORKS**.
3. Wählen Sie auf der Registerkarte **Virtuelles Netzwerk** in der Spalte Name die virtuelle Netzwerkentität aus, die einem CloudBridge Connector-Tunnel zugeordnet ist, dessen Statistiken Sie anzeigen möchten.



4. Zeigen Sie auf der Seite **Dashboard** des virtuellen Netzwerks die Leistungsindikatoren DATA IN und DATA OUT für den CloudBridge Connector-Tunnel an.



Konfigurieren des CloudBridge Connector-Tunnels zwischen Rechenzentrum und Softlayer Enterprise Cloud

October 5, 2021

Die GUI enthält einen Assistenten, der Ihnen hilft, einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC-Appliance in einem Rechenzentrum und Citrix ADC VPX-Instanzen in der SoftLayer Enterprise Cloud einfach zu konfigurieren.

Wenn Sie den Assistenten der Citrix ADC Appliance im Rechenzentrum verwenden, wird die auf der Citrix ADC-Appliance erstellte CloudBridge Connector-Tunnelkonfiguration automatisch an den anderen Endpunkt oder Peer (Citrix ADC VPX auf SoftLayer) des CloudBridge Connector-Tunnels übertragen.

Mit dem Assistenten der Citrix ADC Appliance im Rechenzentrum führen Sie die folgenden Schritte aus, um einen CloudBridge Connector-Tunnel zu konfigurieren.

1. Stellen Sie eine Verbindung zur Enterprise Cloud von Softlayer her, indem Sie die Anmeldeinformationen des Benutzers angeben.
2. Wählen Sie den Citrix XenServer aus, auf dem die Citrix ADC VPX Appliance ausgeführt wird.

3. Wählen Sie die Citrix ADC VPX Appliance aus.
4. Bereitstellen von CloudBridge Connector-Tunnelparametern für:
    - Konfigurieren Sie einen GRE Tunnel.
    - Konfigurieren Sie IPsec im GRE-Tunnel.
    - Erstellen Sie eine Netbridge, eine logische Darstellung des CloudBridge-Connectors, indem Sie einen Namen angeben.
    - Binden Sie den GRE Tunnel an die Netbridge.

So konfigurieren Sie einen CloudBridge Connector-Tunnel mit der GUI

1. Melden Sie sich an der Benutzeroberfläche der Citrix ADC Appliance im Rechenzentrum an, indem Sie Ihre Kontoanmeldeinformationen für die Appliance verwenden.
2. Navigieren Sie zu **System** > **CloudBridge Connector** .
3. Klicken Sie im rechten Bereich unter **Erste Schritte**auf **CloudBridge Connector erstellen/überwachen**.
4. Klicken Sie auf **Erste Schritte**.

> **Hinweis**:
>
> Wenn Sie bereits einen CloudBridge Connector-Tunnel auf der Citrix ADC Appliance konfiguriert haben, wird dieser Bildschirm nicht angezeigt, und Sie gelangen zum Setup-Bereich von CloudBridge Connector.

1. Klicken Sie im Bereich CloudBridge Connector-Setup auf Softlayer, und folgen Sie dann den Anweisungen im Assistenten.

Überwachung des CloudBridge Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer Citrix ADC Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen. Weitere Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer Citrix ADC Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

Konfigurieren eines CloudBridge Connector-Tunnels zwischen einer Citrix ADC Appliance und einem Cisco IOS-Gerät

October 5, 2021

Sie können einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und einem Cisco-Gerät konfigurieren, um zwei Rechenzentren zu verbinden oder Ihr Netzwerk mit einem

Cloud-Anbieter zu erweitern. Die Citrix ADC Appliance und das Cisco IOS-Gerät bilden die Endpunkte des CloudBridge Connector-Tunnels und werden Peers genannt.

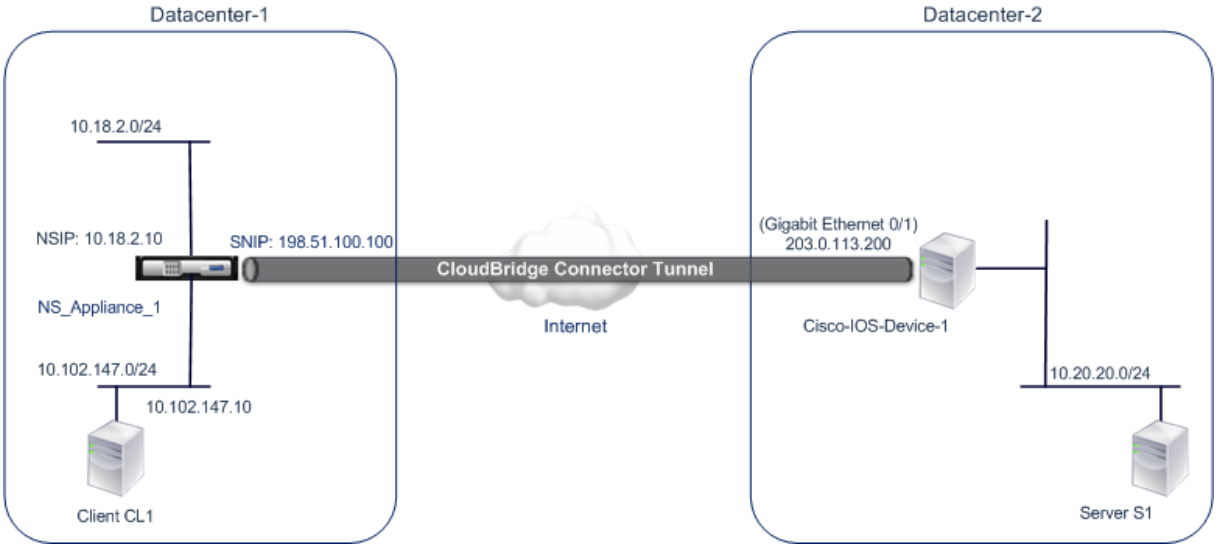
Beispiel für CloudBridge Connector-Tunnelkonfiguration und Datenfluss

Betrachten Sie als Veranschaulichung des Verkehrsflusses in einem CloudBridge Connector-Tunnel ein Beispiel, in dem ein CloudBridge Connector-Tunnel zwischen den folgenden Geräten eingerichtet ist:

- Citrix ADC Appliance NS_Appliance-1 in einem Rechenzentrum, das als Datacenter-1 bezeichnet wird
- Cisco IOS-Gerät Cisco-iOS-Device-1 in einem Rechenzentrum, das als Datacenter-2 bezeichnet wird

NS_Appliance-1 und Cisco-iOS-Device-1 ermöglichen die Kommunikation zwischen privaten Netzwerken in Datacenter-1 und Datacenter-2 über den CloudBridge Connector-Tunnel. Im Beispiel ermöglichen NS_Appliance-1 und Cisco-iOS-Device-1 die Kommunikation zwischen Client CL1 in Datacenter-1 und Server S1 in Datacenter-2 über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

Unter NS_Appliance-1 umfasst die CloudBridge Connector-Tunnelkonfiguration die IPsec-Profilentität NS_CISCO_IPsec_Profile, CloudBridge Connector-Tunnelentität NS_CISCO_Tunnel und die richtlinienbasierte Routing-Entität NS_CISCO_PBR (PBR).



Weitere Informationen finden Sie im CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und den Cisco IOS-Geräteeinstellungen pdf.

Zu berücksichtigende Punkte für eine CloudBridge Connector-Tunnelkonfiguration

Bevor Sie einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und einem Cisco IOS-Gerät konfigurieren, sollten Sie die folgenden Punkte beachten:

- Die folgenden IPsec-Einstellungen werden für einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und einem Cisco IOS-Gerät unterstützt.

IPsec-Eigenschaften	Einstellung
IPsec-Modus	Tunnelmodus
IKE-Version	Version 1
IKE DH-Gruppe	DH-Gruppe 2 (MODP-Algorithmus mit 1024 Bit)
IKE-Authentifizierungsmethode	Vorgeteilter Schlüssel
IKE-Verschlüsselungsalgorithmus	AES, 3DES
IKE-Hash-Algorithmus	HMAC SHA1, HMAC SHA256, HMAC SHA384, HMAC SHA512, HMAC MD5
ESP-Verschlüsselungsalgorithmus	AES, 3DES
ESP-Hash-Algorithmus	HMAC SHA1, HMAC SHA256, HMAC SHA256, HMAC SHA256, HMAC MD5

- Sie müssen dieselben IPsec-Einstellungen auf der Citrix ADC Appliance und dem Cisco IOS-Gerät an den beiden Enden des CloudBridge Connectors angeben.
- Citrix ADC stellt einen gemeinsamen Parameter (in IPsec-Profilen) zur Angabe eines IKE-Hash-Algorithmus und eines ESP-Hash-Algorithmus bereit. Es bietet auch einen weiteren und einen gemeinsamen Parameter für die Angabe eines IKE-Verschlüsselungsalgorithmus und eines ESP-Verschlüsselungsalgorithmus. Daher müssen Sie auf dem Cisco-Gerät den gleichen Hash-Algorithmus und den gleichen Verschlüsselungsalgorithmus für IKE (beim Erstellen von IKE-Richtlinien) und ESP (beim Erstellen von IPsec-Transformationssatz) angeben.
- Sie müssen die Firewall am Citrix ADC Ende und am Cisco-Geräteende konfigurieren, um Folgendes zuzulassen.
  - Alle UDP-Pakete für Port 500
  - Alle UDP-Pakete für Port 4500
  - Alle ESP-Pakete (IP-Protokollnummer 50)

Konfigurieren des Cisco IOS-Geräts für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel auf einem Cisco IOS-Gerät zu konfigurieren, verwenden Sie die Cisco IOS-Befehlszeilenschnittstelle, die die primäre Benutzeroberfläche für die Konfiguration, Überwachung und Wartung von Cisco-Geräten darstellt.

Bevor Sie die CloudBridge Connector-Tunnelkonfiguration auf einem Cisco IOS-Gerät beginnen, stellen Sie sicher, dass:

- Sie haben ein Benutzerkonto mit Administratoranmeldeinformationen auf dem Cisco IOS-Gerät.
- Sie sind mit der Cisco IOS-Befehlszeilenschnittstelle vertraut.
- Das Cisco IOS-Gerät ist betriebsbereit, ist mit dem Internet verbunden und ist auch mit den privaten Subnetzen verbunden, deren Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll.

> **Hinweis**:
>
> Die Verfahren zum Konfigurieren des CloudBridge Connector-Tunnels auf einem Cisco IOS-Gerät können sich je nach Cisco Release-Zyklus im Laufe der Zeit ändern. Citrix empfiehlt, die offizielle Cisco-Produktdokumention zu befolgen, um weitere Informationen zu erhalten, siehe Thema Konfigurieren von IPSec-VPN-Tunneln .

Um einen CloudBridge-Connector-Tunnel zwischen einer Citrix ADC Appliance und einem Cisco IOS-Gerät zu konfigurieren, führen Sie die folgenden Aufgaben in der IOS-Befehlszeile des Cisco-Gerätsaus:

- Erstellen Sie eine IKE-Richtlinie.
- Konfigurieren Sie einen vorab freigegebenen Schlüssel für die IKE-Authentifizierung.
- Definieren Sie einen Transformationssatz und konfigurieren Sie IPsec im Tunnelmodus.
- Erstellen Sie eine Krypto-Zugriffsliste
- Erstellen Sie eine Krypto-Karte
- Wenden Sie die Krypto-Map auf eine Schnittstelle an

Die Beispiele in den folgenden Prozeduren erstellen Einstellungen `Cisco IOS device Cisco-IOS-Device-1` im Abschnitt “Beispiel für CloudBridge Connector-Konfiguration und Datenfluss. “

Informationen**zum Erstellen einer IKE-Richtlinie**finden Sie im PDF-Format der IKE-Richtlinie .

So konfigurieren Sie einen Pre-Shared-Key mithilfe der Cisco IOS-Befehlszeile:

Geben Sie an der Eingabeaufforderung des Cisco IOS-Geräts die folgenden Befehle ein, beginnend im globalen Konfigurationsmodus, in der angegebenen Reihenfolge:

Befehl	Beispiel	Beschreibung des Befehls
crypto isakmp identity address	Cisco-ios-device-1(config)# crypto isakmp identity address	Geben Sie die ISAKMP-Identität (Adresse) an, die das Cisco IOS-Gerät bei der Kommunikation mit dem Peer (Citrix ADC Appliance) während der IKE-Verhandlungen verwendet werden soll. In diesem Beispiel wird das Schlüsselwort address angegeben, das die IP-Adresse 203.0.113.200 (Gigabit Ethernet-Schnittstelle 0/1 von Cisco-iOS-Device-1) als Identität für das Gerät verwendet.
crypto isakmp key keystringaddress peer-address	Cisco-ios-device-1 (config)# crypto isakmp key examplepresharedkey address 198.51.100.100	Geben Sie einen vorab freigegebenen Schlüssel für die IKE-Authentifizierung an. In diesem Beispiel wird der gemeinsam genutzte Schlüssel examplepresharedkey für die Verwendung mit der Citrix ADC Appliance NS_Appliance-1 (198.51.100.100) konfiguriert. Der gleiche vorab freigegebene Schlüssel muss auf der Citrix ADC Appliance konfiguriert werden, damit die IKE-Authentifizierung zwischen dem Cisco IOS-Gerät und der Citrix ADC-Appliance erfolgreich ist.

So erstellen Sie eine Krypto-Zugriffsliste mit der Cisco IOS-Befehlszeile:

Geben Sie an der Eingabeaufforderung des Cisco IOS-Geräts den folgenden Befehl im globalen Konfigurationsmodus in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
access-listaccess-list-number permit IPsource source-wildcard destination destination-wildcard	Cisco-ios-device-1(config)# access-list 111 permit ip 10.20.20.0 0.0.0.255 10.102.147.0 0.0.0.255	Geben Sie Bedingungen an, um die Subnetze zu bestimmen, deren IP-Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll. In diesem Beispiel wird die Zugriffsliste 111 so konfiguriert, dass der Datenverkehr vor Subnetzen 10.20.20.0/24 (auf der Seite Cisco-iOS-Device-1) und 10.102.147.0/24 (auf der Seite NS_Appliance-1) geschützt wird.

So definieren Sie eine Transformation und konfigurieren den IPSec-Tunnelmodus mithilfe der Cisco IOS-Befehlszeile:

Geben Sie an der Eingabeaufforderung des Cisco IOS-Geräts die folgenden Befehle ein, beginnend im globalen Konfigurationsmodus, in der angegebenen Reihenfolge:
Befehl	Beispiel	Beschreibung des Befehls
–	–	–
crypto ipsec transform-Setname ESP_Authentication_Transform ESP_Encryption_Transform Hinweis: ESP_Authentication_Transform kann die folgenden Werte annehmen: esp-sha-hmac, esp-sha256-hmac, esp-sha384-hmac, esp-sha512-hmac, esp-md5-hmac. ESP_Encryption_Transform kann die folgenden Werte annehmen: esp-aes oder esp-3des	Cisco-ios-device-1(config)# crypto ipsec transform-set NS-CISCO-TS esp-sha256-hmac esp-3des	Definieren Sie einen Transformationssatz und geben Sie den ESP-Hash-Algorithmus (für die Authentifizierung) und den ESP-Verschlüsselungsalgorithmus an, der beim Datenaustausch zwischen den CloudBridge Connector-Tunnelpeers verwendet werden soll. In diesem Beispiel wird der Transformationssatz NS-CISCO-TS definiert und der ESP-Authentifizierungsalgorithmus als esp-sha256-hmac und der ESP-Verschlüsselungsalgorithmus als esp-3des angegeben.
Mode-Tunnel	Cisco-IOS-Gerät-1 (config-Crypto-Trans) # Modus-Tunnel	Stellen Sie IPSec im Tun-

nelmodus ein.|
|exit|Cisco-IOS-Device-1 (config-Crypto-Trans) # exit, Cisco-IOS-Device-1 (config) #|Beenden Sie den globalen Konfigurationsmodus.|

So erstellen Sie eine Krypto-Map mit der Cisco IOS-Befehlszeile:

Geben Sie an der Eingabeaufforderung des Cisco IOS-Geräts die folgenden Befehle ab dem globalen Konfigurationsmodus in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
crypto mapmap-name seq-num ipsec-isakmp	Cisco-ios-device-1 (config)# crypto map NS-CISCO-CM 2 ipsec-isakmp	Rufen Sie den Kryptozuordnungskonfigurationsmodus ein, geben Sie eine Sequenznummer für die Kryptozuordnung an und konfigurieren Sie die Kryptozuordnung, um IKE zum Einrichten von Sicherheitszuordnungen (SAs) zu verwenden. In diesem Beispiel werden Sequenznummer 2 und IKE für Kryptozuordnung NS-CISCO-CM konfiguriert.
set peer ip-address	Cisco-ios-device-1 (config-crypto-map)# set peer 172.23.2.7	Geben Sie den Peer (Citrix ADC Appliance) anhand seiner IP-Adresse an. In diesem Beispiel wird 198.51.100.100 angegeben. Dies ist die IP-Adresse des CloudBridge Connectors auf der Citrix ADC Appliance.

Befehl	Beispiel	Beschreibung des Befehls
match addressaccess-list-id	Cisco-ios-device-1 (config-crypto-map)# match address 111	Geben Sie eine erweiterte Zugriffsliste an. Diese Zugriffsliste gibt Bedingungen an, um die Subnetze zu bestimmen, deren IP-Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll. In diesem Beispiel wird die Zugriffsliste 111 angegeben.
set transform-set transform-set-name	Cisco-ios-device-1 (config-crypto-map)# set transform-set NS-CISCO-TS	Geben Sie an, welche Transformationssätze für diesen Kryptozuordnungseintrag zulässig sind. In diesem Beispiel wird der Transformationssatz NS-CISCO-TS angegeben.
Exit	cisco-iOS-Device-1 (config-crypto-map) # exit	
cisco-iOS-Device-1 (config) #	Zurück in den globalen Konfigurationsmodus.	

So wenden Sie eine Krypto-Map über die Cisco IOS-Befehlszeile auf eine Schnittstelle an:

Geben Sie an der Eingabeaufforderung des Cisco IOS-Geräts die folgenden Befehle ab dem globalen Konfigurationsmodus in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
interfaceinterface-ID	Cisco-ios-device-1(config)# interface GigabitEthernet 0/1	Geben Sie eine physikalische Schnittstelle an, auf die die Kryptozuordnung angewendet werden soll, und wechseln Sie in den Schnittstellenkonfigurations-modus. In diesem Beispiel wird die Gigabit-Ethernet-Schnittstelle 0/1 des Cisco-iOS-Device-1 angegeben. Die IP-Adresse 203.0.113.200 ist bereits auf diese Schnittstelle eingestellt.
crypto mapmap-name	Cisco-ios-device-1 (config-if)# crypto map NS-CISCO-CM	Wenden Sie die Kryptozuordnung auf die physische Schnittstelle an. In diesem Beispiel wird die Kryptozuordnung NS-CISCO-CM angewendet.
exit	Cisco-ios-device-1 (config-if)# exit, Cisco-ios-device-1 (config)#	Beenden Sie den globalen Konfigurationsmodus.

Konfigurieren der Citrix ADC Appliance für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und einem Cisco IOS-Gerät zu konfigurieren, führen Sie die folgenden Aufgaben auf der Citrix ADC-Appliance aus. Sie können entweder die Citrix ADC Befehlszeile oder die grafische Benutzeroberfläche (GUI) von Citrix ADC verwenden:

- Erstellen Sie ein IPsec-Profil.
- Erstellen Sie einen IP-Tunnel, der das IPsec-Protokoll verwendet, und verknüpfen Sie das IPsec-Profil damit.
- Erstellen Sie eine PBR-Regel und verknüpfen Sie sie mit dem IP-Tunnel.

So erstellen Sie ein IPSEC-Profil mit der Citrix ADC-Befehlszeile:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add ipsec profile <name> -psk <string> -ikeVersion v1
- show ipsec profile <name>

So erstellen Sie einen IPSEC-Tunnel und binden das IPSEC-Profil mithilfe der Citrix ADC-Befehlszeile daran:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>
- add ipTunnel <name>

So erstellen Sie eine PBR-Regel und binden den IPSEC-Tunnel mithilfe der Citrix ADC-Befehlszeile daran:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>
- apply pbrs
- show pbrs <pbrName>

Die folgenden Befehle erstellen Einstellungen im Citrix ADC appliance NS_Appliance-1 Abschnitt **Beispiel für CloudBridge Connector-Konfiguration und Datenfluss**.

```
1      >  add ipsec profile NS_Cisco_IPSec_Profile -psk
          examplepresharedkey -ikeVersion v1 - lifetime 315360 - encAlgo 3
          DES
2      Done
3      >  add iptunnel NS_Cisco_Tunnel 203.0.113.200 255.255.255.255
          198.51.100.100 - protocol IPSEC - ipsecProfileName
          NS_Cisco_IPSec_Profile
4
5      Done
6      > add pbr NS_Cisco_Pbr -srcIP 10.102.147.0-10.102.147.255 - destIP
          10.20.0.0-10.20.255.255 - ipTunnel NS_Cisco_Tunnel
7
8      Done
9      > apply pbrs
10
11     Done
12 <!--NeedCopy-->
```

So erstellen Sie ein IPSEC-Profil mit der GUI:

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IPSec-Profil**.

2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie im Dialogfeld **IPsec-Profil hinzufügen** die folgenden Parameter fest:
   - Name
   - Verschlüsselungsalgorithmus
   - Hash-Algorithmus
   - IKE-Protokollversion
4. Konfigurieren Sie die **IPSec-Authentifizierungsmethode**, die von den beiden CloudBridge Connector-Tunnel-Peers zur gegenseitigen Authentifizierung verwendet wird: Wählen Sie die **Pre-Shared Key Authentifizierungsmethode** aus, und legen Sie den Parameter **Pre-Shared Key Exists** fest.
5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So erstellen Sie einen IP-Tunnel und binden das IPSEC-Profil über die grafische Benutzeroberfläche daran:

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IP-Tunnel**.
2. Klicken Sie auf der Registerkarte **IPv4-Tunnel** auf **Hinzufügen**.
3. Legen Sie im Dialogfeld **IP-Tunnel hinzufügen** die folgenden Parameter fest:
   - Name
   - Remote-IP
   - Remote-Maske
   - Lokaler IP-Typ (Wählen Sie in der Dropdownliste Lokaler IP-Typ die Option Subnetz-IP).
   - Lokale IP (Alle konfigurierten IPs des ausgewählten IP-Typs befinden sich in der Dropdownliste Lokale IP. Wählen Sie die gewünschte IP aus der Liste aus.)
   - Protokoll
   - IPsec-Profil
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So erstellen Sie eine PBR-Regel und binden den IPSEC-Tunnel mit der GUI daran

1. Navigieren Sie zu **System** > **Netzwerk** > **PBR**.
2. Klicken Sie auf der Registerkarte **PBR** auf **Hinzufügen**.
3. **Legen Sie im Dialogfeld PBR erstellen** die folgenden Parameter fest:
   - Name
   - Aktion
   - Nächster Hop-Typ (Wählen Sie IP Tunnel)
   - IP-Tunnelname
   - Quell-IP Niedrig
   - Quell-IP hoch
   - Ziel-IP niedrig
   - Ziel-IP hoch
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So wenden Sie eine PBR mit der GUIan:

1. Navigieren Sie zu **System** > **Netzwerk** > **PBRs**.
2. Wählen Sie auf der Registerkarte **PBRs** den **PBR**aus, und wählen Sie in der **Liste Aktion**die Option **Übernehmen**aus.

Die entsprechende neue CloudBridge Connector-Tunnelkonfiguration auf der Citrix ADC Appliance wird in der GUI angezeigt. Der aktuelle Status des CloudBridge-Connector-Tunnels wird im Bereich Konfigurierter CloudBridge-Connector angezeigt. Ein grüner Punkt zeigt an, dass der Tunnel oben ist. Ein roter Punkt zeigt an, dass der Tunnel heruntergefahren ist.

Überwachung des CloudBridge-Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer Citrix ADC Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen. Weitere Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer Citrix ADC Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

Konfigurieren eines CloudBridge Connector-Tunnels zwischen einer Citrix ADC Appliance und fortinet FortiGate Appliance

October 5, 2021

Sie können einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und einer Fortinet FortiGate Appliance konfigurieren, um zwei Rechenzentren zu verbinden oder Ihr Netzwerk mit einem Cloud-Anbieter zu erweitern. Die Citrix ADC Appliance und die FortiGate Appliance bilden die Endpunkte des CloudBridge Connector-Tunnels und werden Peers genannt.

Beispiel für eine CloudBridge-Connector-Tunnelkonfiguration

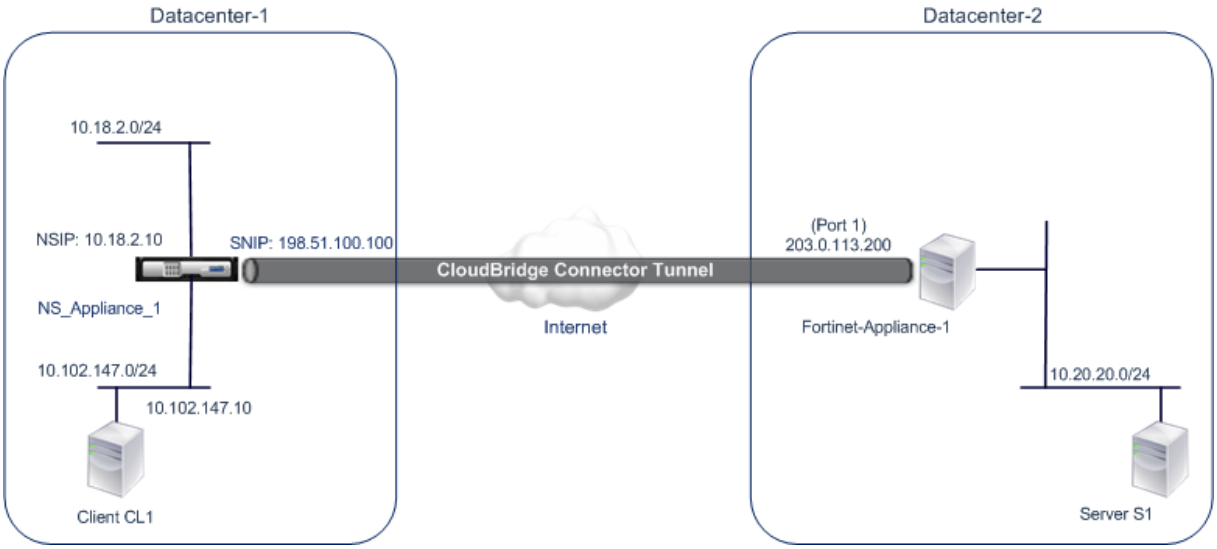
Betrachten Sie als Veranschaulichung des Verkehrsflusses in einem CloudBridge Connector-Tunnel ein Beispiel, in dem ein CloudBridge Connector-Tunnel zwischen den folgenden Geräten eingerichtet ist:

- Citrix ADC Appliance NS_Appliance-1 in einem Rechenzentrum, das als Datacenter-1 bezeichnet wird
- FortiGate Appliance FortiGate-Appliance-1 in einem Rechenzentrum, das als Datacenter-2 bezeichnet wird

NS_Appliance-1 und FortiGate-Appliance-1 ermöglichen die Kommunikation zwischen privaten Netzwerken in Datacenter-1 und Datacenter-2 über den CloudBridge Connector-Tunnel. Im Beispiel

ermöglichen NS_Appliance-1 und FortiGate-Appliance-1 die Kommunikation zwischen Client CL1 in Datacenter-1 und Server S1 in Datacenter-2 über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

Unter NS_Appliance-1 umfasst die CloudBridge Connector-Tunnelkonfiguration die IPsec-Profilentität NS_Fortinet_IPsec_Profile, CloudBridge Connector-Tunnelentität NS_Fortinet_Tunnel und die richtlinienbasierte Routing-Entität NS_Fortinet_PBR (PBR).



Weitere Informationen finden Sie unter CloudBridge Connector-Tunnelkonfigurationstabelle pdf.

Informationen zu Einstellungen für Fortinet Fortigate-Appliance-1 in Rechenzentrum-2 finden Sie in der Tabelle.

Punkte, die für eine CloudBridge Connector-Tunnelkonfiguration zu beachten sind

Bevor Sie einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und einer FortiGate-Appliance konfigurieren, sollten Sie die folgenden Punkte beachten:

- Die folgenden IPsec-Einstellungen werden für einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und einer FortiGate-Appliance unterstützt.

IPsec-Eigenschaften	Einstellungen
IPsec-Modus	Tunnelmodus
IKE-Version	Version 1
IKE DH-Gruppe	DH-Gruppe 2 (MODP-Algorithmus mit 1024 Bit)
IKE-Authentifizierungsmethode	Vorgeteilter Schlüssel
IKE-Verschlüsselungsalgorithmus	AES

IPsec-Eigenschaften	Einstellungen
IKE-Hash-Algorithmus	HMAC SHA1
ESP-Verschlüsselungsalgorithmus	AES
ESP-Hash-Algorithmus	HMAC SHA1

- Sie müssen dieselben IPsec-Einstellungen auf der Citrix ADC Appliance und der FortiGate-Appliance an den beiden Enden des CloudBridge Connectors angeben.
- Citrix ADC stellt einen gemeinsamen Parameter (in IPsec-Profilen) zur Angabe eines IKE-Hash-Algorithmus und eines ESP-Hash-Algorithmus bereit. Es bietet auch einen weiteren gemeinsamen Parameter für die Angabe eines IKE-Verschlüsselungsalgorithmus und eines ESP-Verschlüsselungsalgorithmus. Daher müssen Sie in der FortiGate-Appliance denselben Hash-Algorithmus und denselben Verschlüsselungsalgorithmus in IKE (Phase-1-Konfiguration) und ESP (Phase-2-Konfiguration) angeben.
- Sie müssen die Firewall am Citrix ADC Ende und am FortiGate-Ende konfigurieren, um Folgendes zuzulassen.
  - Alle UDP-Pakete für Port 500
  - Alle UDP-Pakete für Port 4500
  - Alle ESP-Pakete (IP-Protokollnummer 50)
- Die FortiGate Appliance unterstützt zwei Arten von VPN-Tunneln: Policy-based und Route-based. Zwischen einer FortiGate-Appliance und einer Citrix ADC Appliance wird nur richtlinienbasierter VPN-Tunnel unterstützt.

Konfigurieren der FortiGate Appliance für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel auf einer FortiGate Appliance zu konfigurieren, verwenden Sie den Fortinet Web-basierten Manager, der die primäre Benutzeroberfläche für die Konfiguration, Überwachung und Wartung von FortiGate Appliances darstellt.

Bevor Sie mit der CloudBridge Connector-Tunnelkonfiguration auf einer FortiGate Appliance beginnen, stellen Sie sicher, dass:

- Sie verfügen über ein Benutzerkonto mit Administratoranmeldeinformationen auf der FortiGate-Appliance.
- Sie sind mit dem Web-basierten Manager von Fortinet vertraut.
- Die FortiGate Appliance ist UP und läuft, ist mit dem Internet verbunden und ist auch mit den privaten Subnetzen verbunden, deren Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll.

> **Hinweis:**
>
> Die Verfahren zum Konfigurieren des CloudBridge Connector-Tunnels auf einer FortiGate Appliance können sich je nach Fortinet-Release-Zyklus im Laufe der Zeit ändern. Citrix empfiehlt, die offizielle Fortinet-Produktdokumentation zum Konfigurieren von IPSec-VPN-Tunnelnzu befolgen.

Um einen CloudBridge-Connector-Tunnel zwischen einer Citrix ADC Appliance und einer FortiGate-Appliance zu konfigurieren, führen Sie die folgenden Aufgaben auf der FortiGate-Appliance mithilfe des webbasierten Fortinet-Managers aus:

- **Aktivieren Sie die richtlinienbasierte IPsec-VPN-Funktion**. Aktivieren Sie diese Funktion, um richtlinienbasierte VPN-Tunnel auf der FortiGate-Appliance zu erstellen. Zwischen einer FortiGate-Appliance und einer Citrix ADC Appliance wird nur richtlinienbasierte VPN-Tunneltypen unterstützt. Eine richtlinienbasierte VPN-Tunnelkonfiguration auf einer FortiGate-Appliance umfasst Phase-1-Einstellungen, Phase-2-Einstellungen und eine IPsec-Sicherheitsrichtlinie.
- **Definieren Sie Phase-1-Parameter.** Phase 1-Parameter werden von der FortiGate-Appliance für die IKE-Authentifizierung verwendet, bevor ein sicherer Tunnel zur Citrix ADC Appliance gebildet wird.
- **Definieren Sie Phase-2-Parameter**. Phase 2-Parameter werden von der FortiGate-Appliance verwendet, um einen sicheren Tunnel zur Citrix ADC Appliance zu bilden, indem IKE-Sicherheitszuordnungen (SA) eingerichtet werden.
- **Geben Sie private Subnetze**an. Definieren Sie die FortiGate-Seite und die Citrix ADC-seitigen privaten Subnetze, deren IP-Datenverkehr durch den Tunnel transportiert werden soll.
- **Definieren Sie eine IPsec-Sicherheitsrichtlinie für den Tunnel**. Mit einer Sicherheitsrichtlinie kann IP-Datenverkehr zwischen Schnittstellen einer FortiGate-Appliance weitergeleitet werden. Eine IPsec-Sicherheitsrichtlinie gibt die Schnittstelle zum privaten Subnetz und die Schnittstelle an, die die Citrix ADC Appliance über den Tunnel verbindet.

So aktivieren Sie die richtlinienbasierte IPsec-VPN-Funktion mithilfe des Fortinet-Web-basierten Managers

1. Navigieren Sie zu **System** > **Konfiguration** > **Features** .
2. Wählen Sie auf der Seite **Feature-Einstellungen** die Option **Mehr anzeigen** aus und aktivieren Sie **richtlinienbasiertes IPsec-VPN** .

So definieren Sie Phase-1-Parameter mithilfe des Fortinet-Web-basierten Managers

1. Navigieren Sie zu **VPN** > **IPsec** > **Auto Key (IKE)** und klicken Sie auf **Phase1 erstellen** .
2. Legen Sie auf der Seite **Neue Phase 1** die folgenden Parameter fest:
   - Name: Geben Sie einen Namen für diese Phase-1-Konfiguration ein.
   - Remote-Gateway: Wählen Sie *Statische IP-Adresse aus.*
   - Modus: Wählen Sie *Main (ID-Schutz)*.

- Authentifizierungsmethode: Wählen Sie *Preshared Key*aus.
- Pre-Shared Key: Geben Sie einen vorinstallierten Schlüssel ein. Der gleiche vorab freigegebene Schlüssel muss auf der Citrix ADC Appliance konfiguriert werden.
- Peer-Optionen: Legen Sie die folgenden IKE-Parameter für die Authentifizierung einer Citrix ADC Appliance fest.
  - IKE-Version: Wählen Sie *1.*
  - Modus Konfiguration: Deaktivieren Sie diese Option, wenn sie ausgewählt ist.
  - Lokale Gateway-IP: Wählen Sie *Hauptschnittstellen-IP*.
  - P1-Vorschlag: Wählen Sie die Verschlüsselungs- und Authentifizierungsalgorithmen für die IKE-Authentifizierung aus, bevor Sie einen sicheren Tunnel für die Citrix ADC Appliance bilden.
    * 1 - Verschlüsselung: Wählen Sie *AES128*.
    * Authentifizierung: Wählen Sie *SHA1*.
    * Keylife: Geben Sie eine Zeit (in Sekunden) für die Phase-1-Schlüssellebensdauer ein.
    * DH-Gruppe: Wählen Sie 2.
  - X-Auth: Wählen Sie *Deaktivieren*aus.
  - Deed Peer Detection: Wählen Sie diese Option.

3. Klicken Sie auf **OK**.

So geben Sie private Subnetze mit dem Web-basierten Manager von Fortinet an

1. Navigieren Sie zu **Firewall-Objekte** > **Adresse** > **Adressen**, und wählen Sie **Neu erstellen** .
2. Legen Sie auf der Seite **Neue Adresse** die folgenden Parameter fest:
   - Name: Geben Sie einen Namen für das FortiGate-seitige Subnetz ein.
   - Typ: Wählen Sie *Subnetz*aus.
   - Subnetz/IP-Bereich: Geben Sie die Adresse des FortiGate-seitigen Subnetzes ein.
   - Schnittstelle: Wählen Sie die lokale Schnittstelle zu diesem Subnetz aus.
3. Klicken Sie auf **OK**.
4. Wiederholen Sie die Schritte 1-3, um das Citrix ADC-seitige Subnetz anzugeben.

So definieren Sie Phase-2-Parameter mithilfe des Fortinet-Web-basierten Managers

1. Navigieren Sie zu **VPN** > **IPsec** > **Auto Key (IKE)**, und klicken Sie auf **Phase 2 erstellen** .
2. Legen Sie auf der Seite **Neue Phase 2** die folgenden Parameter fest:
   - Name: Geben Sie einen Namen für diese Phase-2-Konfiguration ein.
   - Phase 1: Wählen Sie die Phase-1-Konfiguration aus der Dropdownliste aus.
3. Klicken Sie auf **Erweitert**, und legen Sie die folgenden Parameter fest:
   - P2-Vorschlag: Wählen Sie die Verschlüsselungs- und Authentifizierungsalgorithmen für die Bildung eines sicheren Tunnels zur Citrix ADC Appliance aus.
     - 1 - Verschlüsselung: Wählen Sie *AES128*.
     - Authentifizierung: Wählen Sie *SHA1*.

- Wiedergabeerkennung aktivieren: Wählen Sie diese Option aus.
- Perfect Forward Secrecy (PFS) aktivieren: Wählen Sie diese Option aus.
- DH-Gruppe: Wählen Sie *2.*

- Keylife: Geben Sie eine Zeitspanne (in Sekunden) für die Phase-2-Schlüssellebensdauer ein.
- Autokey Keep Alive: Wählen Sie diese Option aus.
- Automatisch verhandeln: Wählen Sie diese Option aus.
- Schnellmodusauswahl: Geben Sie die FortiGate-Seite und die Citrix ADC-seitigen privaten Subnetze an, deren Datenverkehr durch den Tunnel durchlaufen werden soll.
  - Quelladresse: Wählen Sie das FortiGate-seitige Subnetz aus der Dropdownliste aus.
  - Quellport: Geben Sie *0*ein.
  - Zieladresse: Wählen Sie das Citrix ADC-seitige Subnetz aus der Dropdownliste aus.
  - Zielport: Geben Sie *0*ein.
  - Protokoll: Geben Sie *0*ein.

4. Klicken Sie auf **OK**.

So definieren Sie eine IPsec-Sicherheitsrichtlinie mithilfe des Fortinet Web-basierten Managers

1. Navigieren Sie zu **Richtlinie** > **Richtlinie** > **Richtlinie**, und klicken Sie auf **Neu erstellen** .
2. Legen Sie auf der Seite **Richtlinie bearbeiten** die folgenden Parameter fest:
   - Richtlinientyp: Wählen Sie *VPN*aus.
   - Policy-Untertyp: Wählen Sie *IPsec*aus.
   - Lokale Schnittstelle: Wählen Sie die lokale Schnittstelle zum internen (privaten) Netzwerk aus.
   - Lokales geschütztes Subnetz: Wählen Sie das FortiGate-seitige Subnetz aus der Dropdownliste aus, dessen Datenverkehr durch den Tunnel durchlaufen werden soll.
   - Ausgehende VPN-Schnittstelle: Wählen Sie die lokale Schnittstelle zum externen (öffentlichen) Netzwerk aus.
   - Remotegeschütztes Subnetz: Wählen Sie das Citrix ADC-seitige Subnetz aus der Dropdownliste aus, dessen Datenverkehr durch den Tunnel durchlaufen werden soll.
   - Zeitplan: Behalten Sie die Standardeinstellung (*immer*) bei, es sei denn, Änderungen sind erforderlich, um bestimmte Anforderungen zu erfüllen.
   - Service: Behalten Sie die Standardeinstellung (*ANY*) bei, es sei denn, Änderungen sind erforderlich, um Ihre spezifischen Anforderungen zu erfüllen.
   - VPN-Tunnel: Wählen Sie *Vorhandene verwenden* und wählen Sie den Tunnel aus der Dropdownliste aus.
   - Die Initiierung des Datenverkehrs vom Remotestandort zulassen: Wählen Sie aus, ob der Datenverkehr aus dem Remotenetzwerk den Tunnel initiieren darf.
3. Klicken Sie auf **OK**.

Konfigurieren der Citrix ADC Appliance für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und einer FortiGate-Appliance zu konfigurieren, führen Sie die folgenden Aufgaben auf der Citrix ADC-Appliance aus. Sie können entweder die Citrix ADC Befehlszeile oder die grafische Benutzeroberfläche (GUI) von Citrix ADC verwenden:

- **Erstellen Sie ein IPsec-Profil**. Eine IPsec-Profilentität gibt die IPsec-Protokollparameter an, z. B. IKE-Version, Verschlüsselungsalgorithmus, Hash-Algorithmus und Authentifizierungsmethode, die vom IPsec-Protokoll im CloudBridge Connector-Tunnel verwendet werden sollen.
- **Erstellen Sie einen IP-Tunnel, der das IPsec-Protokoll verwendet, und verknüpfen Sie das IPsec-Profil damit**. Ein IP-Tunnel gibt die lokale IP-Adresse an (CloudBridge Connector-Tunnelendpunkt-IP-Adresse (vom Typ SNIP), die auf der Citrix ADC Appliance konfiguriert ist), die Remote-IP-Adresse (CloudBridge Connector-Tunnelendpunkt-IP-Adresse, die auf der FortiGate-Appliance konfiguriert wurde), das zum Einrichten der CloudBridge verwendete Protokoll (IPsec) an Connector-Tunnel und eine IPsec-Profilentität. Die erstellte IP-Tunnelentität wird auch als CloudBridge Connector-Tunnelentität bezeichnet.
- **Erstellen Sie eine PBR-Regel und verknüpfen Sie sie mit dem IP-Tunnel**. Eine PBR-Entität gibt einen Satz von Regeln und eine IP-Tunnelentität (CloudBridge Connector Tunnel) an. Der Quell-IP-Adressbereich und der Ziel-IP-Adressbereich sind die Bedingungen für die PBR-Entität. Legen Sie den Quell-IP-Adressbereich fest, um das Citrix ADC-seitige Subnetz anzugeben, dessen Datenverkehr über den Tunnel geschützt werden soll, und legen Sie den Ziel-IP-Adressbereich fest, um das Subnetz der FortiGate Appliance anzugeben, dessen Datenverkehr über den Tunnel geschützt werden soll.

So erstellen Sie ein IPSEC-Profil über die Citrix ADC Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1 -perfectForwardSecrecy ENABLE`
- `show ipsec profile <name>`

So erstellen Sie einen IPSEC-Tunnel und binden das IPSEC-Profil mit der Citrix ADC Befehlszeile an ihn

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName** <string>`
- `show ipTunnel <name>`

So erstellen Sie eine PBR-Regel und binden den IPSEC-Tunnel mit der Citrix ADC Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`

- `apply pbrs`
- `show pbr <pbrName>`

So erstellen Sie ein IPSEC-Profil mit der GUI

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IPSec-Profil**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **IPsec-Profil hinzufügen** die folgenden Parameter fest:
   - Name
   - Verschlüsselungsalgorithmus
   - Hash-Algorithmus
   - IKE-Protokollversion
   - Perfect Forward Secrecy (Aktivieren Sie diesen Parameter)
4. Konfigurieren Sie die IPSec-Authentifizierungsmethode, die von den beiden CloudBridge Connector-Tunnel-Peers zur gegenseitigen Authentifizierung verwendet wird: Wählen Sie die Authentifizierungsmethode für Pre-Shared Key Exists aus, und legen Sie den Parameter Pre-Shared Key Exists fest.
5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So erstellen Sie einen IP-Tunnel und binden das IPSEC-Profil mit der GUI an ihn

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IP-Tunnel**.
2. Klicken Sie auf der Registerkarte **IPv4-Tunnel** auf **Hinzufügen**.
3. Legen Sie auf der Seite **IP-Tunnel hinzufügen** die folgenden Parameter fest:
   - Name
   - Remote-IP
   - Remote-Maske
   - Lokaler IP-Typ (Wählen Sie in der Dropdownliste Lokaler IP-Typ die Option *Subnetz-IP*).
   - Lokale IP (Alle konfigurierten IP-Adressen des ausgewählten IP-Typs befinden sich in der Dropdownliste Lokale IP. Wählen Sie die gewünschte IP aus der Liste aus.)
   - Protokoll
   - IPsec-Profil
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So erstellen Sie eine PBR-Regel und binden den IPSEC-Tunnel mit der GUI daran

1. Navigieren Sie zu **System** > **Netzwerk** > **PBR**.
2. Klicken Sie auf der Registerkarte **PBR** auf **Hinzufügen**.
3. Legen Sie auf der Seite **Create PBR** die folgenden Parameter fest:
   - Name
   - Aktion
   - Nächster Hop-Typ (Wählen Sie *IP Tunnel*)
   - IP-Tunnelname
   - Quell-IP Niedrig

- Quell-IP hoch
- Ziel-IP niedrig
- Ziel-IP hoch

4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Die entsprechende neue CloudBridge Connector-Tunnelkonfiguration auf der Citrix ADC Appliance wird in der GUI angezeigt.

Der aktuelle Status des CloudBridge-Connector-Tunnels wird im Bereich Konfigurierter CloudBridge-Connector angezeigt. Ein grüner Punkt zeigt an, dass der Tunnel oben ist. Ein roter Punkt zeigt an, dass der Tunnel heruntergefahren ist.

Die folgenden Befehle erstellen Einstellungen der Citrix ADC Appliance NS_Appliance-1 in Beispiel für eine CloudBridge Connector-Konfiguration.

```
1      >  add ipsec profile NS_Fortinet_IPSec_Profile -psk
          examplepresharedkey -ikeVersion v1  - encAlgo AES  - hashalgo
          HMAC_SHA1  - lifetime 315360 -perfectForwardSecrecy ENABLE
2
3       Done
4      >  add iptunnel NS_Fortinet_Tunnel 203.0.113.200 255.255.255.255
          198.51.100.100  - protocol IPSEC  - ipsecProfileName
          NS_Fortinet_IPSec_Profile
5
6       Done
7      > add pbr NS_Fortinet_Pbr -srcIP 10.102.147.0-10.102.147.255  -
          destIP 10.20.0.0-10.20.255.255  - ipTunnel NS_Fortinet_Tunnel
8
9       Done
10     > apply pbrs
11
12      Done
13 <!--NeedCopy-->
```

Überwachung des CloudBridge Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer Citrix ADC Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen. Weitere Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer Citrix ADC Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

CloudBridge Connector-Tunnel-Diagnose und Fehlerbehebung

October 5, 2021

Wenn Sie Probleme mit einer CloudBridge Connector-Tunnelkonfiguration haben, stellen Sie sicher, dass alle Voraussetzungen eingehalten wurden, bevor der Tunnel eingerichtet wurde. Wenn dies der Fall ist, könnte das Problem mit den IP-Adressen des Tunnelendpunkts, einer NAT-Konfiguration, der Art und Weise des Tunnels oder mit dem Datenverkehr liegen.

Problembehandlung bei einem CloudBridge Connector-Tunnel

Wenn Ihr CloudBridge Connector-Tunnel nicht ordnungsgemäß funktioniert, kann das Problem mit der Einrichtung eines Tunnels oder mit dem Datenverkehr liegen. Wenn Sie nicht sicher sind, welche Art von Problem Sie haben, suchen Sie nach einer Fehlermeldung in der Protokolldatei und prüfen Sie, ob die Fehlermeldung in der Liste der Probleme mit dem Tunnelaufbau aufgeführt ist. Wenn Sie Ihre Fehlermeldung nicht finden, überprüfen Sie die Liste der möglichen Probleme im Zusammenhang mit dem Datenverkehr.

Fragen im Zusammenhang mit der Errichtung von Tunneln

Wenn die Anforderungen für die Konfiguration des IPsec-Tunnels erfüllt sind und der CloudBridge Connector-Tunnel konfiguriert ist, suchen Sie nach Debugging-Informationen in der Datei iked.log auf einer oder beiden Citrix ADC Appliances, die als Tunnelendpunkte konfiguriert sind.

Geben Sie auf beiden Appliances den folgenden Befehl an der Citrix ADC -Shell Eingabeaufforderung ein:

```
cat /tmp/iked.debug | tee /var/iked.log
```

Das PDF zur Fehlerbehebung listet einige häufige Fehler und ihre Lösungen auf.

Probleme im Zusammenhang mit dem Datenverkehr

Wenn die Daten im CloudBridge Connector-Tunnel nicht ordnungsgemäß zwischen den Tunnelendpunkten ausgetauscht werden, gehen Sie wie folgt vor.

- Für einen CloudBridge Connector-Tunnel, der GRE- und IPsec-Protokolle verwendet:
  - Stellen Sie sicher, dass der L2-Modus auf beiden CloudBridge Connector-Tunnelendpunkten aktiviert ist. Geben Sie zum Aktivieren des L2-Modus den folgenden Befehl an der Citrix ADC Befehlszeilenschnittstelle ein:

    ```
    enable mode L2
    ```


    * Wenn einer der CloudBridge Connector-Tunnelendpunkte eine virtuelle CloudBridge-Appliance (VPX) ist und auf einem VMware ESXi Hypervisor bereitgestellt wird, stellen Sie sicher, dass Promiscuous-Modus für den vSwitch festgelegt ist, der der CloudBridge VPX-Appliance zugeordnet ist.
  - Wenn ein VLAN über einen CloudBridge Connector-Tunnel erweitert wird, überprüfen Sie die Eins-zu-Eins-Zuordnung auf der erweiterten VLAN-Entität auf jedem Tunnelendpunkt
  - Stellen Sie sicher, dass die IP-Tunnelentität an die richtige Netbridge-Entität in jedem Tunnelendpunkt gebunden ist.
  - Stellen Sie sicher, dass der ARP-Eintrag für den Peer-CloudBridge Connector-Tunnelendpunkt auf dem lokalen Tunnelendpunkt vorhanden ist, indem Sie den folgenden Befehl an der Citrix ADC Befehlszeilenschnittstelle eingeben:

    ```
    show arp
    ```
  - Wenn die Ausgabe einen unvollständigen ARP-Eintrag anzeigt, fließt der bidirektionale Datenverkehr nicht durch den Tunnel. Wenn der bidirektionale Datenverkehr fließt, zeigt der ARP-Eintrag den Namen der Tunnelschnittstelle für die Geräte auf der anderen Seite des Tunnels an.
  - Entfernen Sie die IP-Tunnelentitäten von beiden Tunnelendpunkten, und fügen Sie sie erneut mit denselben Parametern hinzu, jedoch mit dem IPsec-Profil auf NONE, sodass der Tunnel nur das GRE-Protokoll verwendet.

    Nachdem Sie im IP-Tunnel (der das GRE-Protokoll verwendet) Folgendes überprüft haben, konfigurieren Sie den Tunnel mit IPsec-Parametern, indem Sie für die jeweiligen IP-Tunnelentitäten an jedem Tunnelendpunkt ein gültiges IPsec-Profil angeben.

    Richtiger Ping- oder TCP-Fluss durch den Tunnel.

    Richtiger Datenverkehr durch den Tunnel.

    Nachdem sich der konfigurierte Tunnel (der GRE- und IPsec-Protokolle verwendet) im UP-Zustand befindet, wenn der Datenverkehr nicht ordnungsgemäß durch den Tunnel fließt und ein NAT-Gerät vor einem oder beiden Tunnelendpunkten bereitgestellt wurde, analysieren Sie die Ein- und Ausreißpakete auf den NAT-Geräten.
- Wenn eine Citrix ADC Appliance als Router oder Gateway verwendet wird.
  - Stellen Sie sicher, dass der L3-Modus auf der Citrix ADC Appliance aktiviert ist. Um den L3-Modus zu aktivieren, führen Sie den folgenden Befehl in der CloudBridge-Befehlszeile aus.
  - Aktivierungsmodus L3
  - Wenn Subnetze an eine Netbridge-Entität gebunden sind, stellen Sie sicher, dass die korrekte IP-Tunnelentität auch an die Netbridge gebunden ist.
  - Führen Sie den folgenden Befehl in der Citrix ADC Befehlszeile aus, um zu sehen, wo die Pakete (Input und Output) gelöscht werden:

    ```
    stat ipsec counters
    ```
  - Stellen Sie sicher, dass die richtigen Routen auf beiden Tunnelendpunkten konfiguriert

sind.

- Wenn kein NAT-Gerät vor der Citrix ADC Appliance bereitgestellt wird, stellen Sie sicher, dass die Firewalls so konfiguriert sind, dass alle ESP-Pakete (IP-Protokollnummer 50) und alle UDP-Pakete für Port 4500 zulässig sind.

Wenn keine der oben genannten Maßnahmen zu einem erfolgreichen Austausch des Datenverkehrs zwischen den Tunnelendpunkten führt, wenden Sie sich an den technischen Support von Citrix.

Prüfliste vor der Kontaktaufnahme mit dem technischen Support von Citrix

Um eine schnelle Lösung zu erhalten, stellen Sie sicher, dass die folgenden Elemente bereit sind, bevor Sie sich an den technischen Support von Citrix wenden.

- Details zur Bereitstellung und Netzwerktopologie.
- Protokolldatei, die durch Eingabe des folgenden Befehls an der Citrix ADC -Shell-Eingabeaufforderung erfasst wurde.
  ```
  cat /tmp/iked.debug | tee /var/log/iked.log
  ```
- Technisches Support-Paket, das durch Eingabe des folgenden Befehls in der Citrix ADC Befehlszeile erfasst wird.
  ```
  show techsupport
  ```
- Paketverfolgung, die an beiden CloudBridge Connector-Tunnelendpunkten erfasst wurden. Um eine Paketverfolgung zu starten, geben Sie den folgenden Befehl in der Citrix ADC Befehlszeile ein.
  ```
  start nstrace -size 0
  ```
  Um die Paketverfolgung zu stoppen, geben Sie den folgenden Befehl in der Citrix ADC Befehlszeile ein.
  ```
  stop nstrace
  ```
- Ausgabe des folgenden Befehls, der an der Citrix ADC Eingabeaufforderung eingegeben wurde.
  ```
  show arp
  ```

Interoperabilität des CloudBridge-Connectors — StrongSwan

December 7, 2021

StrongSwan ist eine Open-Source-IPsec-Implementierung für Linux-Plattformen. Sie können einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und einer StrongSwan Appliance konfigurieren, um zwei Rechenzentren zu verbinden oder Ihr Netzwerk mit einem Cloud-Anbieter zu erweitern. Die Citrix ADC Appliance und die StrongSwan-Appliance bilden die Endpunkte des CloudBridge Connector-Tunnels und werden Peers genannt.

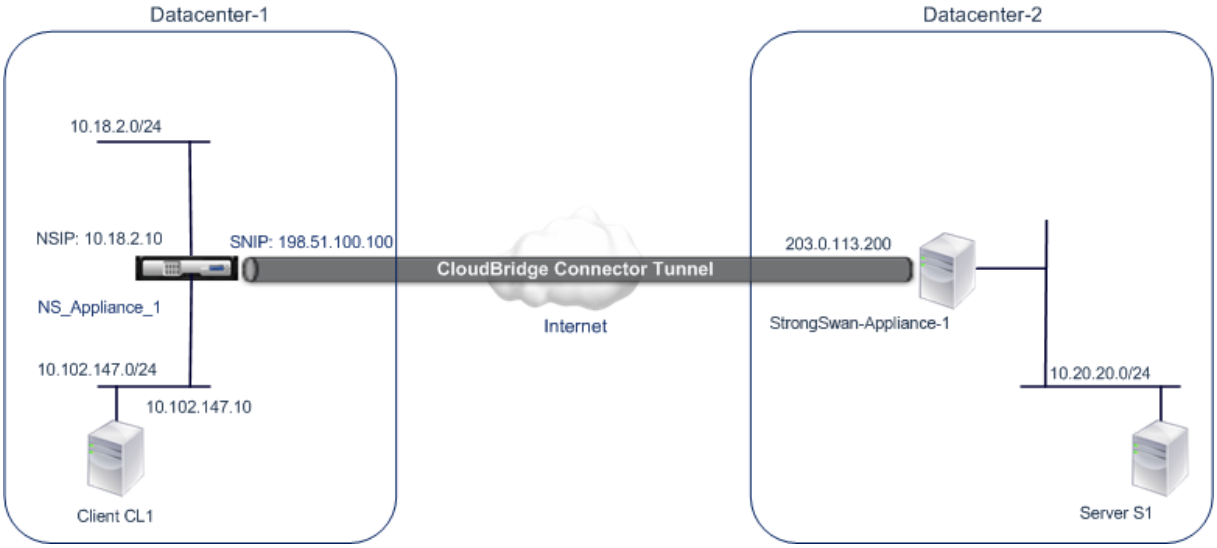
Beispiel für eine CloudBridge Connector-Tunnelkonfiguration

Betrachten Sie als Veranschaulichung des Verkehrsflusses in einem CloudBridge Connector-Tunnel ein Beispiel, in dem ein CloudBridge Connector-Tunnel zwischen den folgenden Geräten eingerichtet ist:

- Citrix ADC Appliance NS_Appliance-1 in einem Rechenzentrum, das als Datacenter-1 bezeichnet wird
- StrongSwan Appliance StrongSwan-Appliance-1 in einem Rechenzentrum, das als Datacenter-2 bezeichnet wird

NS_Appliance-1 und StrongSwan-Appliance-1 ermöglichen die Kommunikation zwischen privaten Netzwerken in Datacenter-1 und Datacenter-2 über den CloudBridge Connector-Tunnel. Im Beispiel ermöglichen NS_Appliance-1 und StrongSwan-Appliance-1 die Kommunikation zwischen Client CL1 in Datacenter-1 und Server S1 in Datacenter-2 über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

Unter NS_Appliance-1 umfasst die CloudBridge Connector-Tunnelkonfiguration die IPsec-Profilentität NS_StrongSwan_IPsec_Profile, CloudBridge Connector-Tunnelentität NS_StrongSwan_Tunnel und Policy Based Routing-Entity NS_StrongSwan_PBR (PBR).



In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt.

Haupteinstellungen des CloudBridge Connector-Tunnels

Entität	Details
IP-Adresse des CloudBridge Connector-Tunnelendpunkts (NS_Appliance-1) in Datacenter-1	198.51.100.100

Entität	Details
IP-Adresse des CloudBridge Connector-Tunnelendpunkts (StrongSwan-Appliance-1) in Datacenter-2	203.0.113.200
Datacenter: Subnetz 1, dessen Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll	10.102.147.0/24
Datacenter — Subnetz von 2, dessen Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll	10.20.20.0/24

Einstellungen auf der Citrix ADC Appliance NS_Appliance-1 in Datacenter-1

SNIP1 (nur zu Referenzzwecken)	198.51.100.100	
IPsec profile	NS_StrongSwan_IPsec_Profile	IKE version: v1, Encryption algorithm: AES, Hash algorithm: HMAC_SHA1
psk = examplepresharedkey (Note: This is an example of a pre-share key, for illustration. Citrix does not recommend to use this string in your CloudBridge Connector configuration)		
CloudBridge Connector tunnel	NS_StrongSwan_Tunnel	Remote IP = 203.0.113.200, Local IP= 198.51.100.100, Tunnel protocol = IPSEC, IPsec profile= NS_StrongSwan_IPsec_Profile

SNIP1 (nur zu Referenzzwecken)	198.51.100.100	
Policy based route	NS_StrongSwan_Pbr	Source IP range = Subnet in the Datacenter-1=10.102.147.0-10.102.147.255, Destination IP range =Subnet in Datacenter-2=10.20.20.0-10.20.20.255, IP Tunnel = NS_StrongSwan_Tunnel

Punkte, die für eine CloudBridge Connector-Tunnelkonfiguration zu beachten sind

Bevor Sie mit der Konfiguration des CloudBridge-Connector-Tunnels beginnen, stellen Sie Folgendes sicher

- Sie haben grundlegende Kenntnisse über Linux-Konfigurationen.
- Sie verfügen über ein grundlegendes Wissen über die IPsec-Protokollsuite.
- Die StrongSwan Appliance ist betriebsbereit, ist mit dem Internet verbunden und ist auch mit den privaten Subnetzen verbunden, deren Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll.
- Die Citrix ADC Appliance ist betriebsbereit, ist mit dem Internet verbunden und ist auch mit den privaten Subnetzen verbunden, deren Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll.
- Die folgenden IPsec-Einstellungen werden für einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und einer StrongSwan-Appliance unterstützt.
  - IPsec-Modus: Tunnelmodus
  - IKE Version: Version 1
  - IKE-Authentifizierungsmethode: Pre-Shared Key
  - IKE-Verschlüsselungsalgorithmus: AES
  - IKE-Hash-Algorithmus: HMAC SHA1
  - ESP-Verschlüsselungsalgorithmus: AES
  - ESP-Hash-Algorithmus: HMAC SHA1
- Sie müssen dieselben IPsec-Einstellungen auf der Citrix ADC Appliance und der StrongSwan-Appliance an den beiden Enden des CloudBridge Connector-Tunnels angeben.
- Citrix ADC stellt einen gemeinsamen Parameter (in IPsec-Profilen) zur Angabe eines IKE-Hash-Algorithmus und eines ESP-Hash-Algorithmus bereit. Es bietet auch einen weiteren gemeinsamen Parameter für die Angabe eines IKE-Verschlüsselungsalgorithmus und eines ESP-Verschlüsselungsalgorithmus. Daher müssen Sie in der StrongSwan-Appliance denselben Hash-Algorithmus und denselben Verschlüsselungsalgorithmus in IKE- und ESP-Parametern in

der Datei IPsec.conf angeben.
- Sie müssen die Firewall am Citrix ADC Ende und am StrongSwan Ende konfigurieren, um Folgendes zuzulassen.
  - Alle UDP-Pakete für Port 500
  - Alle UDP-Pakete für Port 4500
  - Alle ESP-Pakete (IP-Protokollnummer 50)

Konfigurieren von StrongSwan für den CloudBridge Connector-Tunnel

So konfigurieren Sie einen CloudBridge-Connector-Tunnel zwischen einer Citrix ADC Appliance und einer StrongSwan-Appliance:

- **Geben Sie IPsec-Verbindungsinformationen in der Datei ipsec.conf an. Die Datei**ipsec.conf definiert alle Steuerungs- und Konfigurationsinformationen für IPsec-Verbindungen in der StrongSwan Appliance.
- **Geben Sie den vorinstallierten Schlüssel in der Datei ipsec.secrets an. Die Datei**ipsec.secrets definiert Geheimnisse für die IKE/IPsec-Authentifizierung für IPsec-Verbindungen in der StrongSwan Appliance.

Die Verfahren zum Konfigurieren von IPsec VPN (CloudBridge Connector Tunnel) auf einer StrongSwan Appliance können sich je nach StrongSwan Release-Zyklus im Laufe der Zeit ändern. Citrix empfiehlt, die offizielle StrongSwan-Dokumentation zum Konfigurieren von IPSec-VPN-Tunnelnzu befolgen.

Im Anschluss an einen Beispielauszug aus der Datei ipsec.conf werden IPsec-Informationen zum Einrichten des IPsec-VPN-Tunnels angegeben, die unter Beispiel einer CloudBridge-Connector-Konfiguration beschrieben werden. Weitere Informationen finden Sie unter CloudBridge Connector-Konfiguration pdf.

Im Anschluss an einen Beispielauszug aus der Datei ipsec.secrets wird der vorab freigegebene IKE-Authentifizierungsschlüssel zum Einrichten des IPsec-VPN-Tunnels angegeben, der unter Beispiel einer CloudBridge Connector-Konfiguration beschrieben wird.

`/etc/ipsec.secrets` PSK 'beispielpresharedkey' #pre -sharedkey für IPSec IKE-Authentifizierung

Konfigurieren der Citrix ADC Appliance für den CloudBridge Connector-Tunnel

Führen Sie die folgenden Aufgaben auf der Citrix ADC Appliance aus, um einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC-Appliance und einer StrongSwan-Appliance zu konfigurieren. Sie können entweder die Citrix ADC Befehlszeile oder die grafische Benutzeroberfläche (GUI) von Citrix ADC verwenden:

- **Erstellen Sie ein IPsec-Profil**. Eine IPsec-Profilentität gibt die IPsec-Protokollparameter an, z. B. IKE-Version, Verschlüsselungsalgorithmus, Hash-Algorithmus und Authentifizierungsmethode, die vom IPsec-Protokoll im CloudBridge Connector-Tunnel verwendet werden sollen.

- **Erstellen Sie einen IP-Tunnel, der das IPsec-Protokoll verwendet, und verknüpfen Sie das IPsec-Profil damit**. Ein IP-Tunnel gibt die lokale IP-Adresse an (CloudBridge Connector-Tunnelendpunkt-IP-Adresse (vom Typ SNIP), die auf der Citrix ADC Appliance konfiguriert ist), die Remote-IP-Adresse (CloudBridge Connector-Tunnelendpunkt-IP-Adresse, die auf der StrongSwan-Appliance konfiguriert wurde), das zum Einrichten der CloudBridge verwendete Protokoll (IPsec) an Connector-Tunnel und eine IPsec-Profilentität. Die erstellte IP-Tunnelentität wird auch als CloudBridge Connector-Tunnelentität bezeichnet.
- **Erstellen Sie eine PBR-Regel und verknüpfen Sie sie mit dem IP-Tunnel**. Eine PBR-Entität gibt einen Satz von Regeln und eine IP-Tunnelentität (CloudBridge Connector Tunnel) an. Der Quell-IP-Adressbereich und der Ziel-IP-Adressbereich sind die Bedingungen für die PBR-Entität. Legen Sie den Quell-IP-Adressbereich fest, um das Citrix ADC-seitige Subnetz anzugeben, dessen Datenverkehr über den Tunnel geschützt werden soll, und legen Sie den Ziel-IP-Adressbereich fest, um das StrongSwan-Side-Subnetz anzugeben, dessen Datenverkehr über den Tunnel geschützt werden soll.

So erstellen Sie ein IPSEC-Profil über die Citrix ADC Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1`
- `show ipsec profile <name>`

So erstellen Sie einen IPSEC-Tunnel und binden das IPSEC-Profil mit der Citrix ADC Befehlszeile an ihn

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

So erstellen Sie eine PBR-Regel und binden den IPSEC-Tunnel mit der Citrix ADC Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

So erstellen Sie ein IPSEC-Profil mit der GUI

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IPsec-Profil**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **IPsec-Profil hinzufügen** die folgenden Parameter fest:
    - Name
    - Verschlüsselungsalgorithmus

- Hash-Algorithmus
- IKE-Protokollversion

4. Konfigurieren Sie die IPSec-Authentifizierungsmethode, die von den beiden CloudBridge Connector-Tunnel-Peers zur gegenseitigen Authentifizierung verwendet wird: Wählen Sie die **Authentifizierungsmethode für Pre-Shared Key** Exists aus, und legen Sie den Parameter **Pre-Shared Key Exists** fest.
5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So erstellen Sie einen IP-Tunnel und binden das IPSEC-Profil mit der GUI an ihn

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IP-Tunnel**.
2. Klicken Sie auf der Registerkarte **IPv4-Tunnel** auf **Hinzufügen**.
3. Legen Sie auf der Seite IP-Tunnel hinzufügen die folgenden Parameter fest:
   - Name
   - Remote-IP
   - Remote-Maske
   - Lokaler IP-Typ (Wählen Sie in der Dropdownliste Lokaler IP-Typ die Option *Subnetz-IP*).
   - Lokale IP (Alle konfigurierten IP-Adressen des ausgewählten IP-Typs befinden sich in der Dropdownliste Lokale IP. Wählen Sie die gewünschte IP aus der Liste aus.)
   - Protokoll
   - IPsec-Profil
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So erstellen Sie eine PBR-Regel und binden den IPSEC-Tunnel mit der GUI daran

1. Navigieren Sie zu **System** > **Netzwerk** > **PBR**.
2. Klicken Sie auf der Registerkarte **PBR** auf **Hinzufügen**.
3. Legen Sie auf der Seite **Create PBR** die folgenden Parameter fest:
   - Name
   - Aktion
   - Nächster Hop-Typ (Wählen Sie *IP Tunnel*)
   - IP-Tunnelname
   - Quell-IP Niedrig
   - Quell-IP hoch
   - Ziel-IP niedrig
   - Ziel-IP hoch
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Die entsprechende neue CloudBridge Connector-Tunnelkonfiguration auf der Citrix ADC Appliance wird in der GUI angezeigt. Der aktuelle Status des CloudBridge-Connector-Tunnels wird im Bereich Konfigurierter CloudBridge-Connector angezeigt. Ein grüner Punkt zeigt an, dass der Tunnel oben ist. Ein roter Punkt zeigt an, dass der Tunnel heruntergefahren ist.
Die folgenden Befehle erstellen Einstellungen der Citrix ADC Appliance NS_Appliance-1 in Beispiel für

eine CloudBridge Connector-Konfiguration:

```
1      > add ipsec profile NS_StrongSwan_IPSec_Profile -psk
           examplepresharedkey -ikeVersion v1 - encAlgo AES - hashalgo
           HMAC_SHA1
2
3
4      Done
5
6      > add iptunnel NS_StrongSwan_Tunnel 203.0.113.200 255.255.255.255
           198.51.100.100 - protocol IPSEC - ipsecProfileName
           NS_StrongSwan_IPSec_Profile
7
8
9      Done
10
11     > add pbr NS_StrongSwan_Pbr -srcIP 10.102.147.0-10.102.147.255 -
           destIP 10.20.0.0-10.20.255.255 - ipTunnel NS_StrongSwan_Tunnel
12
13
14     Done
15
16     > apply pbrs
17
18
19     Done
20 <!--NeedCopy-->
```

Überwachung des CloudBridge Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer Citrix ADC Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen. Weitere Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer Citrix ADC Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

Interoperabilität des CloudBridge-Connectors — F5 BIG-IP

October 5, 2021

Sie können einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und einer F5

BIG-IP-Appliance konfigurieren, um zwei Rechenzentren zu verbinden oder Ihr Netzwerk mit einem Cloud-Anbieter zu erweitern. Die Citrix ADC Appliance und die F5 BIG-IP-Appliance bilden die Endpunkte des CloudBridge Connector-Tunnels und werden als Peers bezeichnet.

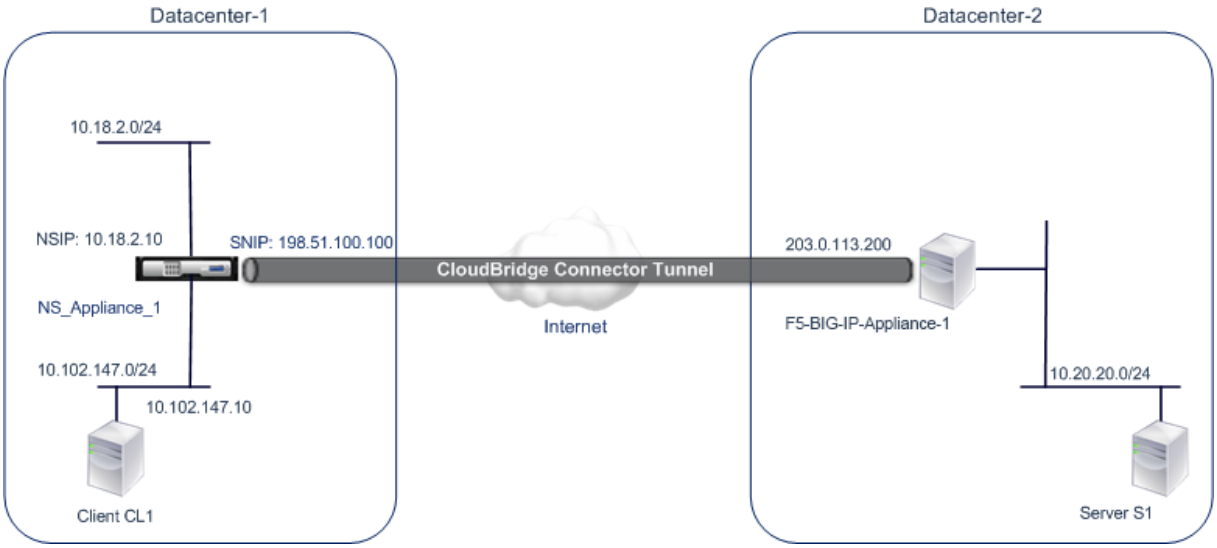
Beispiel für eine CloudBridge Connector-Tunnelkonfiguration

Betrachten Sie als Veranschaulichung des Verkehrsflusses in einem CloudBridge Connector-Tunnel ein Beispiel, in dem ein CloudBridge Connector-Tunnel zwischen den folgenden Geräten eingerichtet ist:

- Citrix ADC Appliance NS_Appliance-1 in einem Rechenzentrum, das als Datacenter-1 bezeichnet wird
- F5 BIG-IP-Appliance F5-BIG-IP-Appliance-1 in einem Rechenzentrum, das als Datacenter-2 bezeichnet wird

NS_Appliance-1 und F5-BIG-IP-Appliance-1 ermöglichen die Kommunikation zwischen privaten Netzwerken in Datacenter-1 und Datacenter-2 über den CloudBridge Connector-Tunnel. Im Beispiel ermöglichen NS_Appliance-1 und F5-BIG-IP-Appliance-1 die Kommunikation zwischen Client CL1 in Datacenter-1 und Server S1 in Datacenter-2 über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

Unter NS_Appliance-1 umfasst die CloudBridge Connector-Tunnelkonfiguration die IPsec-Profilentität NS_F5-BIG-IP_IPsec_Profile, CloudBridge Connector-Tunnelentität NS_F5-BIG-IP_Tunnel und die richtlinienbasierte Routing-Entität NS_F5-BIG-IP_PBR (PBR).



Weitere Informationen finden Sie unter F5 big IP pdf.

Punkte, die für eine CloudBridge Connector-Tunnelkonfiguration zu beachten sind

- Die Citrix ADC Appliance ist betriebsbereit, ist mit dem Internet verbunden und ist auch mit den privaten Subnetzen verbunden, deren Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll.
- Die F5 BIG-IP-Appliance ist UP und läuft, ist mit dem Internet verbunden und ist auch mit den privaten Subnetzen verbunden, deren Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll.
- Die folgenden IPsec-Einstellungen werden für einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und einer F5 BIG-IP-Appliance unterstützt.
  - IPsec-Modus: Tunnelmodus
  - IKE Version: Version 1
  - IKE-Authentifizierungsmethode: Pre-Shared Key
  - IKE-Verschlüsselungsalgorithmus: AES
  - IKE-Hash-Algorithmus: HMAC SHA1
  - ESP-Verschlüsselungsalgorithmus: AES
  - ESP-Hash-Algorithmus: HMAC SHA1
- Sie müssen dieselben IPsec-Einstellungen auf der Citrix ADC Appliance und der F5 BIG-IP-Appliance an den beiden Enden des CloudBridge Connector-Tunnels angeben.
- Citrix ADC stellt einen gemeinsamen Parameter (in IPsec-Profilen) zur Angabe eines IKE-Hash-Algorithmus und eines ESP-Hash-Algorithmus bereit. Es bietet auch einen weiteren gemeinsamen Parameter für die Angabe eines IKE-Verschlüsselungsalgorithmus und eines ESP-Verschlüsselungsalgorithmus. Daher müssen Sie in der F5 BIG-IP-Appliance denselben Hash-Algorithmus und denselben Verschlüsselungsalgorithmus in IKE (Phase-1-Konfiguration) und ESP (Phase-2-Konfiguration) angeben.
- Sie müssen die Firewall am Citrix ADC Ende und am Ende F5 BIG-IP konfigurieren, um Folgendes zuzulassen.
  - Alle UDP-Pakete für Port 500
  - Alle UDP-Pakete für Port 4500
  - Alle ESP-Pakete (IP-Protokollnummer 50)

Konfigurieren von F5 BIG-IP für den CloudBridge Connector-Tunnel

Um einen CloudBridge-Connector-Tunnel zwischen einer Citrix ADC Appliance und einer F5 BIG-IP-Appliance zu konfigurieren, führen Sie die folgenden Aufgaben auf der F5 BIG-IP-Appliance aus:

- **Erstellen Sie einen virtuellen Weiterleitungsserver für IPsec**. Ein virtueller Weiterleitungsserver fängt IP-Datenverkehr für den IPsec-Tunnel ab.
- **Erstellen Sie einen IKE-Peer.** Ein IKE-Peer gibt die lokalen und Remote-IPsec-Tunnelendpunkte an. Es gibt auch Algorithmen und Anmeldeinformationen für IPsec IKE Phase 1 verwendet werden.

- **Erstellen Sie eine benutzerdefinierte IPsec-Richtlinie.** Eine Richtlinie gibt das IPsec-Protokoll (ESP) und den Modus (Tunnel) an, der für die Bildung des IPsec-Tunnels verwendet werden soll. Es gibt auch die Algorithmen und Sicherheitsparameter für IKE IPsec Phase 2 verwendet werden.
- **Erstellen Sie eine bidirektionale IPsec-Verkehrsauswahl**. Eine Verkehrsauswahl gibt die F5 BIG-IP-Seite und die Citrix ADC Seite Subnetze an, deren IP-Datenverkehr durch den IPsec-Tunnel durchlaufen werden soll.

Die Verfahren zum Konfigurieren von IPsec VPN (CloudBridge Connector Tunnel) auf einer F5 BIG-IP-Appliance können sich je nach F5-Release-Zyklus im Laufe der Zeit ändern. Citrix empfiehlt, die offizielle F5 BIG-IP-Dokumentation zum Konfigurieren von IPsec-VPN-Tunneln zu befolgen, unter:

https://f5.com

So erstellen Sie einen virtuellen Weiterleitungsserver für IPsec mit der F5 BIG-IP GUI

1. Klicken Sie auf der Registerkarte **Main** auf **Lokaler Traffic** > **Virtual Servers**und dann auf **Create**.
2. Legen Sie im Fenster **Neue virtuelle Serverliste** die folgenden Parameter fest:
   - **Name**. Geben Sie einen eindeutigen Namen für den virtuellen Server ein.
   - **Geben Sie ein**. Wählen Sie **Weiterleitung (IP)**aus.
   - **Zieladresse**. Geben Sie eine Platzhalternetzwerkadresse im CIDR-Format ein, z. B. 0.0.0.0/0 für IPv4, um Datenverkehr zu akzeptieren.
   - **Dienstport**. Wählen Sie **Alle Ports** aus der Liste aus.
   - **Protokollliste**. Wählen Sie **Alle Protokolle** aus der Liste aus.
   - **VLAN- und Tunnelverkehr**. Behalten Sie die Standardauswahl, **Alle VLANs und Tunnel**.
3. Klicken Sie auf **Fertig**.

So erstellen Sie eine benutzerdefinierte IPsec-Richtlinie mit der F5 BIG-IP-GUI

1. Klicken Sie auf der Registerkarte **Main** auf **Netzwerk** > **IPsec** > **IPsec-Richtlinien**, und klicken Sie dann auf **Erstellen** .
2. Legen Sie im Bildschirm **Neue Richtlinie** die folgenden Parameter fest:
   - **Name**. Geben Sie einen eindeutigen Namen für die Richtlinie ein.
   - **IPsec-Protokoll**. Behalten Sie die Standardauswahl, ESP.
   - **Modus**. Wählen Sie Tunnel aus. Der Bildschirm wird aktualisiert, um weitere verwandte Einstellungen anzuzeigen.
   - **Lokale Adresse des Tunnels**. Geben Sie die IP-Adresse des lokalen IPsec-Tunnelendpunkts ein (Konfiguriert auf der F5 BIG-IP-Appliance).
   - **Tunnel-Remote-Adresse**. Geben Sie die IP-Adresse des Remote-IPsec-Tunnel-Endpunkts ein (konfiguriert auf der Citrix ADC Appliance).
3. Behalten Sie für die IKE Phase 2-Parameter die Standardwerte bei, oder wählen Sie die Optionen aus, die für Ihre Bereitstellung geeignet sind.
4. Klicken Sie auf **Fertig**.

So erstellen Sie einen bidirektionalen IPsec-Datenverkehrs-Selektor mit der F5 BIG-IP GUI

1. Klicken Sie auf der Registerkarte **Main** auf **Netzwerk** > **IPsec** > **Traffic Selectors**und dann auf **Create**.
2. Legen Sie auf dem Bildschirm " **Neuer Traffic Selector** " die folgenden Parameter fest:
   - **Name**. Geben Sie einen eindeutigen Namen für die Verkehrsauswahl ein.
   - **Ordnung**. Behalten Sie den Standardwert **(First)**bei. Diese Einstellung gibt die Reihenfolge an, in der die Verkehrsauswahl auf dem Bildschirm "Traffic Selector List" angezeigt wird.
3. Wählen Sie in der Liste **Konfiguration** die Option **Erweitert** aus, und legen Sie die folgenden Parameter fest:
   - **Quell-IP-Adresse**. Klicken Sie auf **Host** oder **Netzwerk**und geben Sie im Feld **Adresse** die Adresse des F5 BIG-IP-Seiten-Subnetzes ein, dessen Datenverkehr über den IPsec-Tunnel geschützt werden soll.
   - **Quellport**. Wählen Sie *** Alle Ports**aus.
   - **Ziel-IP-Adresse**. Klicken Sie auf **Host**, und geben Sie im Feld **Adresse**die Adresse des Citrix ADC seitigen Subnetzes ein, dessen Datenverkehr über den IPsec-Tunnel geschützt werden soll.
   - **Zielport**. Wählen Sie *** Alle Ports**aus.
   - **Protokoll**. Wählen Sie *** Alle Protokolle**.
   - **Richtung**. Wählen Sie **Beide**aus.
   - **Aktion:** Wählen Sie **Schützen**aus. Die Einstellung **IPsec-Richtlinienname** wird angezeigt.
   - **IPsec-Richtlinienname**. Wählen Sie den Namen der benutzerdefinierten IPsec-Richtlinie aus, die Sie erstellt haben.
4. Klicken Sie auf **Fertig**.

Konfigurieren der Citrix ADC Appliance für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und einer F5 BIG-IP-Appliance zu konfigurieren, führen Sie die folgenden Aufgaben auf der Citrix ADC-Appliance aus. Sie können entweder die Citrix ADC Befehlszeile oder die grafische Benutzeroberfläche (GUI) von Citrix ADC verwenden:

- **Erstellen Sie ein IPsec-Profil**. Eine IPsec-Profilentität gibt die IPsec-Protokollparameter an, z. B. IKE-Version, Verschlüsselungsalgorithmus, Hash-Algorithmus und Authentifizierungsmethode, die vom IPsec-Protokoll im CloudBridge Connector-Tunnel verwendet werden sollen.
- **Erstellen Sie einen IP-Tunnel, der das IPsec-Protokoll verwendet, und verknüpfen Sie das IPsec-Profil damit**. Ein IP-Tunnel gibt die lokale IP-Adresse an (CloudBridge Connector-Tunnelendpunkt-IP-Adresse (vom Typ SNIP), die auf der Citrix ADC Appliance konfiguriert ist), die Remote-IP-Adresse (CloudBridge Connector-Tunnelendpunkt-IP-Adresse, die auf der F5 BIG-IP-Appliance konfiguriert wurde), das zum Einrichten der CloudBridge verwendete Pro-

tokoll (IPsec) an Connector-Tunnel und eine IPsec-Profilentität. Die erstellte IP-Tunnelentität wird auch als CloudBridge Connector-Tunnelentität bezeichnet.

- **Erstellen Sie eine PBR-Regel und verknüpfen Sie sie mit dem IP-Tunnel**. Eine PBR-Entität gibt einen Satz von Regeln und eine IP-Tunnelentität (CloudBridge Connector Tunnel) an. Der Quell-IP-Adressbereich und der Ziel-IP-Adressbereich sind die Bedingungen für die PBR-Entität. Legen Sie den Quell-IP-Adressbereich fest, um das Citrix ADC-seitige Subnetz anzugeben, dessen Datenverkehr über den Tunnel geschützt werden soll, und legen Sie den Ziel-IP-Adressbereich fest, um das F5 BIG-IP-Seite-Subnetz anzugeben, dessen Datenverkehr über den Tunnel geschützt werden soll.

So erstellen Sie ein IPSEC-Profil über die Citrix ADC Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1 -perfectForwardSecrecyENABLE`
- `show ipsec profile** <name>`

So erstellen Sie einen IPSEC-Tunnel und binden das IPSEC-Profil mit der Citrix ADC Befehlszeile an ihn

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

So erstellen Sie eine PBR-Regel und binden den IPSEC-Tunnel mit der Citrix ADC Befehlszeile

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add pbr <pbrName> ALLOW -srcIP <subnet-range> -destIP <subnet-range> -ipTunnel <tunnelName>`
- `apply pbrs`
- `show pbr <pbrName>`

So erstellen Sie ein IPSEC-Profil mit der GUI

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IPsecProfile**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **IPsec-Profil hinzufügen** die folgenden Parameter fest:
   - Name
   - Verschlüsselungsalgorithmus
   - Hash-Algorithmus
   - IKE-Protokollversion
4. Konfigurieren Sie die IPSec-Authentifizierungsmethode, die von den beiden CloudBridge Connector-Tunnel-Peers zur gegenseitigen Authentifizierung verwendet wird: Wählen Sie die

Authentifizierungsmethode für Pre-Shared Key Exists aus, und legen Sie den Parameter **Pre-Shared Key Exists** fest.

5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So erstellen Sie einen IP-Tunnel und binden das IPSEC-Profil mit der GUI an ihn

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IP-Tunnel**.
2. Klicken Sie auf der Registerkarte **IPv4-Tunnel** auf **Hinzufügen**.
3. Legen Sie auf der Seite **IP-Tunnel hinzufügen** die folgenden Parameter fest:
   - Name
   - Remote-IP
   - Remote-Maske
   - Lokaler IP-Typ (Wählen Sie in der Dropdownliste Lokaler IP-Typ die Option *Subnetz-IP*).
   - Lokale IP (Alle konfigurierten IP-Adressen des ausgewählten IP-Typs befinden sich in der Dropdownliste Lokale IP. Wählen Sie die gewünschte IP aus der Liste aus.)
   - Protokoll
   - IPsec-Profil
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So erstellen Sie eine PBR-Regel und binden den IPSEC-Tunnel mit der GUI daran

1. Navigieren Sie zu **System** > **Netzwerk** > **PBR**.
2. Klicken Sie auf der Registerkarte **PBR** auf **Hinzufügen**.
3. Legen Sie auf der Seite **Create PBR** die folgenden Parameter fest:
   - Name
   - Aktion
   - Nächster Hop-Typ (Wählen Sie *IP Tunnel*)
   - IP-Tunnelname
   - Quell-IP Niedrig
   - Quell-IP hoch
   - Ziel-IP niedrig
   - Ziel-IP hoch
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Die entsprechende neue CloudBridge Connector-Tunnelkonfiguration auf der Citrix ADC Appliance wird in der GUI angezeigt. Der aktuelle Status des CloudBridge-Connector-Tunnels wird im Bereich Konfigurierter CloudBridge-Connector angezeigt. Ein grüner Punkt zeigt an, dass der Tunnel oben ist. Ein roter Punkt zeigt an, dass der Tunnel heruntergefahren ist.

Die folgenden Befehle erstellen Einstellungen der Citrix ADC Appliance NS_Appliance-1 in Beispiel für eine CloudBridge Connector-Konfiguration. :


```
    >  add ipsec profile NS_F5-BIG-IP_IPSec_Profile -psk
       examplepresharedkey -ikeVersion v1  - encAlgo AES  - hashalgo
       HMAC_SHA1  - lifetime 315360 -perfectForwardSecrecy ENABLE


    Done

    >  add iptunnel NS_F5-BIG-IP_Tunnel 203.0.113.200 255.255.255.255
       198.51.100.100  - protocol IPSEC  - ipsecProfileName NS_F5-BIG-
       IP_IPSec_Profile


    Done

    > add pbr NS_F5-BIG-IP_Pbr -srcIP 10.102.147.0-10.102.147.255  -
       destIP 10.20.0.0-10.20.255.255  - ipTunnel NS_F5-BIG-IP_Tunnel


    Done

    > apply pbrs


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

Überwachung des CloudBridge Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer Citrix ADC Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen. Weitere Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer Citrix ADC Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

Interoperabilität des CloudBridge-Connectors — Cisco ASA

December 7, 2021

Sie können einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und einer Cisco ASA-Appliance konfigurieren, um zwei Rechenzentren zu verbinden oder Ihr Netzwerk mit einem Cloud-Anbieter zu erweitern. Die Citrix ADC Appliance und die Cisco ASA-Appliance bilden die Endpunkte des CloudBridge Connector-Tunnels und werden als Peers bezeichnet.

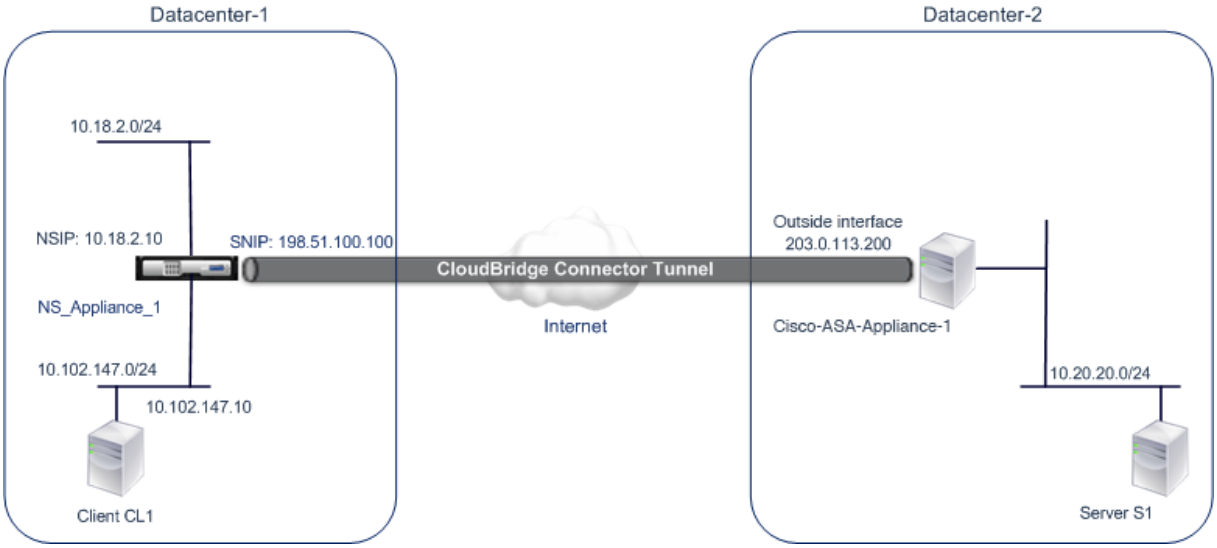
Beispiel für eine CloudBridge Connector-Tunnelkonfiguration

Betrachten Sie als Veranschaulichung des Verkehrsflusses in einem CloudBridge Connector-Tunnel ein Beispiel, in dem ein CloudBridge Connector-Tunnel zwischen den folgenden Appliances eingerichtet ist:

- Citrix ADC Appliance NS_Appliance-1 in einem Rechenzentrum, das als Datacenter-1 bezeichnet wird
- Cisco ASA-Appliance Cisco-ASA-Appliance-1 in einem Rechenzentrum, das als Datacenter-2 bezeichnet wird

NS_Appliance-1 und Cisco-ASA-Appliance-1 ermöglichen die Kommunikation zwischen privaten Netzwerken in Datacenter-1 und Datacenter-2 über den CloudBridge Connector-Tunnel. Im Beispiel ermöglichen NS_Appliance-1 und Cisco-ASA-Appliance-1 die Kommunikation zwischen Client CL1 in Datacenter-1 und Server S1 in Datacenter-2 über den CloudBridge Connector-Tunnel. Client CL1 und Server S1 sind in verschiedenen privaten Netzwerken.

Unter NS_Appliance-1 umfasst die CloudBridge Connector-Tunnelkonfiguration die IPsec-Profilentität NS_cisco-ASA_IPsec_Profile, CloudBridge Connector-Tunnelentität NS_cisco-ASA_Tunnel und die richtlinienbasierte Routing-Entität NS_Cisco-ASA_PBR (PBR).



Punkte, die für eine CloudBridge Connector-Tunnelkonfiguration zu beachten sind

Bevor Sie mit der Konfiguration des CloudBridge-Connector-Tunnels beginnen, stellen Sie Folgendes sicher

- Die folgenden IPsec-Einstellungen werden für einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und einer Cisco ASA-Appliance unterstützt.

IPsec-Eigenschaften	Einstellungen
IPsec-Modus	Tunnelmodus
IKE-Version	Version 1
IKE-Authentifizierungsmethode	Vorgeteilter Schlüssel
IKE-Verschlüsselungsalgorithmus	AES, 3DES
IKE-Hash-Algorithmus	HMAC SHA1, HMAC MD5
ESP-Verschlüsselungsalgorithmus	AES, 3DES
ESP-Hash-Algorithmus	HMAC SHA1, HMAC MD5

- Sie müssen dieselben IPsec-Einstellungen auf der Citrix ADC Appliance und der Cisco ASA-Appliance an den beiden Enden des CloudBridge Connector-Tunnels angeben.
- Citrix ADC stellt einen gemeinsamen Parameter (in IPsec-Profilen) zur Angabe eines IKE-Hash-Algorithmus und eines ESP-Hash-Algorithmus bereit. Es bietet auch einen weiteren gemeinsamen Parameter für die Angabe eines IKE-Verschlüsselungsalgorithmus und eines ESP-Verschlüsselungsalgorithmus. Daher müssen Sie in der Cisco ASA-Appliance denselben Hash-Algorithmus und denselben Verschlüsselungsalgorithmus in IKE (Phase-1-Konfiguration) und ESP (Phase-2-Konfiguration) angeben.
- Sie müssen die Firewall am Citrix ADC Ende und Cisco ASA Ende konfigurieren, um Folgendes zuzulassen.
  - Alle UDP-Pakete für Port 500
  - Alle UDP-Pakete für Port 4500
  - Alle ESP-Pakete (IP-Protokollnummer 50)

Konfigurieren von Cisco ASA für den CloudBridge Connector-Tunnel

Verwenden Sie zum Konfigurieren eines CloudBridge Connector-Tunnels auf einer Cisco ASA-Appliance die Cisco ASA-Befehlszeilenschnittstelle, die die primäre Benutzeroberfläche für die Konfiguration, Überwachung und Wartung von Cisco ASA-Appliances

Bevor Sie mit der CloudBridge Connector-Tunnelkonfiguration auf einer Cisco ASA-Appliance beginnen, stellen Sie sicher, dass:

- Sie verfügen über ein Benutzerkonto mit Administratoranmeldeinformationen auf der Cisco ASA-Appliance.
- Sie sind mit der Cisco ASA-Befehlszeilenschnittstelle vertraut.
- Die Cisco ASA-Appliance ist betriebsbereit, ist mit dem Internet verbunden und ist auch mit den privaten Subnetzen verbunden, deren Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll.

> **Hinweis:**
>
> Die Verfahren zum Konfigurieren des CloudBridge Connector-Tunnels auf einer Cisco ASA-Appliance können sich je nach Cisco Release-Zyklus im Laufe der Zeit ändern. Citrix empfiehlt, die offizielle Cisco ASA-Produktdokumentation zum Konfigurieren von IPsec-VPN-Tunneln zu befolgen, unter:

- http://www.cisco.com

Um einen CloudBridge-Connector-Tunnel zwischen einer Citrix ADC Appliance und einer Cisco ASA-Appliance zu konfigurieren, führen Sie die folgenden Aufgaben über die Befehlszeile der Cisco ASA-Appliance aus:

- **Erstellen Sie eine IKE-Richtlinie**. Eine IKE-Richtlinie definiert eine Kombination von Sicherheitsparametern, die während der IKE-Verhandlung verwendet werden sollen (Phase 1). In dieser Aufgabe werden beispielsweise Parameter wie Hash-Algorithmus, Verschlüsselungsalgorithmus und Authentifizierungsmethode festgelegt, die in der IKE-Verhandlung verwendet werden sollen.
- **Aktivieren Sie IKE auf der externen Schnittstelle**. Aktivieren Sie IKE auf der Außenschnittstelle, über die der Tunnelverkehr zum Tunnelpeer fließt.
- **Erstellen Sie eine Tunnelgruppe**. Eine Tunnelgruppe gibt den Tunneltyp und den vorab freigegebenen Schlüssel an. Der Tunneltyp muss auf ipsec-l2l gesetzt sein, was für IPsec LAN to LAN steht. Ein vorab geteilter Schlüssel ist eine Textzeichenfolge, die die Peers eines CloudBridge Connector-Tunnels verwenden, um sich gegenseitig zu authentifizieren. Die vorinstallierten Schlüssel werden für die IKE-Authentifizierung gegeneinander zugeordnet. Damit die Authentifizierung erfolgreich ist, müssen Sie daher denselben vorinstallierten Schlüssel auf der Cisco ASA-Appliance und der Citrix ADC Appliance konfigurieren.
- **Definieren Sie einen Transformationssatz**. Ein Transformationsset definiert eine Kombination von Sicherheitsparametern (Phase 2), die nach erfolgreicher IKE-Verhandlung beim Austausch von Daten über den CloudBridge Connector-Tunnel verwendet werden sollen.
- **Erstellen Sie eine Zugriffsliste**. Crypto-Zugriffslisten werden verwendet, um die Subnetze zu definieren, deren IP-Datenverkehr über den CloudBridge-Tunnel geschützt wird. Die Quell- und Zielparameter in der Zugriffsliste geben die Cisco-Appliance-Seite und die Citrix ADC Seite Subnetze an, die über den CloudBridge Connector Tunnel geschützt werden sollen. Die Zugriffsliste muss so eingestellt sein, dass sie zulässig ist. Alle Anforderungspakete, die von einer Appliance im Cisco-Appliance-seitigen Subnetz stammen und für eine Appliance im Citrix ADC seitigen Subnetz bestimmt sind und die Quell- und Zielparameter der Zugriffsliste übereinstimmen, werden über den CloudBridge Connector-Tunnel gesendet.
- **Erstellen Sie eine Kryptozuordnung**. Krypto-Karten definieren die IPsec-Parameter für Sicherheitszuordnungen (SAs). Dazu gehören die folgenden: Crypto-Zugriffsliste zur Identifizierung der Subnetze, deren Datenverkehr über den CloudBridge-Tunnel geschützt werden soll, Peer-Identifizierung (Citrix ADC) nach IP-Adresse und Transformationseinstellung entsprechend den

Peer-Sicherheitseinstellungen.

- **Wenden Sie die Kryptozuordnung auf die externe Schnittstelle**an. In dieser Aufgabe wenden Sie die Kryptozuordnung auf die externe Schnittstelle an, über die der Tunnelverkehr zum Tunnelpeer fließt. Durch Anwenden der Kryptozuordnung auf eine Schnittstelle wird die Cisco ASA-Appliance angewiesen, den gesamten Schnittstellenverkehr anhand des Kryptozuordnungssatzes auszuwerten und die angegebene Richtlinie während der Verbindungs- oder Sicherheitszuordnungsverhandlungen zu verwenden.

Die Beispiele in den folgenden Verfahren erstellen Einstellungen der Cisco-ASA-Appliance Cisco-ASA-Appliance-1, die in Beispiel für CloudBridge Connector-Konfiguration und Datenfluss verwendet werden.

So erstellen Sie eine IKE-Richtlinie über die Cisco ASA-Befehlszeile

Geben Sie an der Eingabeaufforderung der Cisco ASA-Appliance die folgenden Befehle ein, beginnend im globalen Konfigurationsmodus, in der angegebenen Reihenfolge:

Befehl	Beispiel	Beschreibung des Befehls
crypto ikev1 policy priority	Cisco-ASA-appliance-1(config)# crypto ikev1 policy 1	Rufen Sie den IKE-Richtlinienkonfigurationsmodus auf, und identifizieren Sie die zu erstellende Richtlinie. (Jede Richtlinie wird durch die von Ihnen zugewiesene Prioritätsnummer eindeutig gekennzeichnet.) In diesem Beispiel wird die Richtlinie 1 konfiguriert.
encryption (3des | aes)	Cisco-ASA-appliance-1 (config-ikev1-policy)# encryption 3des	Gibt den Verschlüsselungsalgorithmus an. In diesem Beispiel wird der 3DES-Algorithmus konfiguriert.
hash (sha | md5)	Cisco-ASA-appliance-1 (config- ikev1-policy)# hash sha	Geben Sie den Hash-Algorithmus an. In diesem Beispiel wird SHA konfiguriert.
authenticationpre-share	Cisco-ASA-appliance-1 (config- ikev1-policy)# authentication pre-share	Gibt die Pre-Share-Authentifizierungsmethode an.

Befehl	Beispiel	Beschreibung des Befehls
group 2	Cisco-ASA-appliance-1 (config- ikev1-policy)# group 2	Geben Sie die 1024-Bit-Diffie-Hellman-Gruppenkennung (2) an.
lifetime seconds	Cisco-ASA-appliance-1 (config- ikev1-policy)# lifetime 28800	Geben Sie die Lebensdauer der Sicherheitsverbindung in Sekunden an. In diesem Beispiel werden 28800 Sekunden konfiguriert, was der Standardwert der Lebensdauer in einer Citrix ADC Appliance ist.

So aktivieren Sie IKE auf der externen Schnittstelle über die Cisco ASA-Befehlszeile

Geben Sie an der Eingabeaufforderung der Cisco ASA-Appliance die folgenden Befehle ein, beginnend im globalen Konfigurationsmodus, in der angegebenen Reihenfolge:

Befehl	Beispiel	Beschreibung des Befehls
crypto ikev1 enable outside	Cisco-ASA-appliance-1(config)# crypto ikev1 enable outside	Aktivieren Sie IKEv1 auf der Schnittstelle, über die der Tunnelverkehr zum Tunnelpeer fließt. In diesem Beispiel wird IKEv1 für die Schnittstelle außerhalb aktiviert.

So erstellen Sie eine Tunnelgruppe über die Cisco ASA-Befehlszeile

Geben Sie an der Eingabeaufforderung der Cisco ASA-Appliance die folgenden Befehle ein, beginnend im globalen Konfigurationsmodus, wie in der angeschlossenen pdf Tunnel Group über die Cisco ASA-Befehlszeilegezeigt:

So erstellen Sie eine Krypto-Zugriffsliste über die Cisco ASA-Befehlszeile

Geben Sie an der Eingabeaufforderung der Cisco ASA-Appliance den folgenden Befehl im globalen Konfigurationsmodus in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
access-list access-list-number permit IP source source-wildcard destination destination-wildcard	Cisco-ASA-appliance-1(config)# access-list 111 permit ip 10.20.20.0 0.0.0.255 10.102.147.0 0.0.0.255	Geben Sie Bedingungen an, um die Subnetze zu bestimmen, deren IP-Datenverkehr über den CloudBridge Connector-Tunnel geschützt werden soll. In diesem Beispiel wird die Zugriffsliste 111 zum Schutz des Datenverkehrs aus Subnetzen 10.20.20.0/24 (auf der Seite Cisco-Asa-Aliance-1) und 10.102.147.0/24 (auf der Seite NS_Appliance-1) konfiguriert.

So definieren Sie einen Transformationssatz über die Cisco ASA-Befehlszeile

Geben Sie an der Eingabeaufforderung der Cisco ASA-Appliance die folgenden Befehle ein, beginnend im globalen Konfigurationsmodus. Siehe Transformieren Set mit ASA-Befehlszeilentabelle pdf.

So erstellen Sie eine Kryptozuordnung über die Cisco ASA-Befehlszeile

Geben Sie an der Eingabeaufforderung der Cisco ASA-Appliance die folgenden Befehle ab dem globalen Konfigurationsmodus in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
crypto map map-name seq-num match address access-list-name	Cisco-ASA-appliance-1 (config)# crypto map NS-CISCO-CM 1 match address 111	Erstellen Sie eine Kryptozuordnung und geben Sie eine Zugriffsliste darauf an. In diesem Beispiel wird die Krypto-Map NS-CISCO-CM mit der Sequenznummer 1 konfiguriert und die Zugriffsliste 111 NS-CISCO-CM zugewiesen.

Befehl	Beispiel	Beschreibung des Befehls
crypto map map-name seq-num set peer ip-address	Cisco-ASA-appliance-1 (config)# crypto map NS-CISCO-CM 1 set peer 198.51.100.100	Geben Sie den Peer (Citrix ADC Appliance) anhand seiner IP-Adresse an. In diesem Beispiel wird 198.51.100.100 angegeben. Dabei handelt es sich um die IP-Adresse des Tunnelendpunkts auf der Citrix ADC Appliance.
crypto map map-name seq-num set ikev1 transform-set transform-set-name	Cisco-ASA-appliance-1 (config)# crypto map NS-CISCO-CM 1 set ikev1 transform-set NS-CISCO-TS	Geben Sie an, welcher Transformationssatz für diesen Kryptozuordnungseintrag zulässig ist. In diesem Beispiel wird der Transformationssatz NS-CISCO-TS angegeben.

So wenden Sie eine Kryptozuordnung auf eine Schnittstelle über die Cisco ASA-Befehlszeile an

Geben Sie an der Eingabeaufforderung der Cisco ASA-Appliance die folgenden Befehle ab dem globalen Konfigurationsmodus in der angegebenen Reihenfolge ein:

Befehl	Beispiel	Beschreibung des Befehls
crypto map map-nameinterface interface-name	Cisco-ASA-appliance-1(config)# crypto map NS-CISCO-CM interface outside	Wenden Sie die Kryptozuordnung auf die Schnittstelle an, über die der CloudBridge Connector-Tunnelverkehr fließt. In diesem Beispiel wird die Kryptozuordnung NS-CISCO-CM auf die Schnittstelle außerhalb angewendet.

Konfigurieren der Citrix ADC Appliance für den CloudBridge Connector-Tunnel

Um einen CloudBridge Connector-Tunnel zwischen einer Citrix ADC Appliance und einer Cisco ASA-Appliance zu konfigurieren, führen Sie die folgenden Aufgaben auf der Citrix ADC-Appliance aus. Sie können entweder die Citrix ADC Befehlszeile oder die grafische Benutzeroberfläche (GUI) von Citrix ADC verwenden:

- Erstellen Sie ein IPsec-Profil.
- Erstellen Sie einen IP-Tunnel, der das IPsec-Protokoll verwendet, und verknüpfen Sie das IPsec-Profil damit.
- Erstellen Sie eine PBR-Regel und verknüpfen Sie sie mit dem IP-Tunnel.

So erstellen Sie ein IPSEC-Profil mit der Citrix ADC Befehlszeile:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add ipsec profile <name> -psk <string> -ikeVersion v1 -encAlgo AES -hashAlgo HMAC_SHA1 -perfectForwardSecrecy ENABLE`
- `show ipsec profile <name>`

So erstellen Sie einen IPSEC-Tunnel und binden das IPSEC-Profil mithilfe der Citrix ADC Befehlszeile an dieses Profil:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add ipTunnel <name> <remote> <remoteSubnetMask> <local> -protocol IPSEC -ipsecProfileName <string>`
- `show ipTunnel <name>`

So erstellen Sie eine PBR-Regel und binden den IPSEC-Tunnel mithilfe der Citrix ADC Befehlszeile an diesen:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `**add pbr** <pbrName> **ALLOW** -**srcIP** <subnet-range> -**destIP** <subnet-range>`
- `**ipTunnel** <tunnelName>`
- `**apply pbrs**`
- `**show pbr** <pbrName>`

So erstellen Sie ein IPSEC-Profil mit der GUI:

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IPSec-Profil**.
2. Klicken Sie im Detailbereich auf **Hinzufügen**.
3. Legen Sie auf der Seite **IPsec-Profil hinzufügen** die folgenden Parameter fest:
    - Name
    - Verschlüsselungsalgorithmus
    - Hash-Algorithmus

- IKE-Protokollversion
- Perfect Forward Secrecy (Diesen Parameter aktivieren)

4. Konfigurieren Sie die IPSec-Authentifizierungsmethode, die von den beiden CloudBridge Connector-Tunnel-Peers zur gegenseitigen Authentifizierung verwendet wird: Wählen Sie die **Authentifizierungsmethode für Pre-Shared Key** Exists aus, und legen Sie den Parameter **Pre-Shared Key Exists** fest.
5. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So erstellen Sie einen IP-Tunnel und binden das IPSEC-Profil über die GUI an dieses Profil:

1. Navigieren Sie zu **System** > **CloudBridge Connector** > **IP-Tunnel**.
2. Klicken Sie auf der **Registerkarte IPv4-Tunnel**auf **Hinzufügen**.
3. Legen Sie auf der Seite **IP-Tunnel hinzufügen** die folgenden Parameter fest:
   - Name
   - Remote-IP
   - Remote-Maske
   - Lokaler IP-Typ (Wählen Sie in der Dropdownliste Lokaler IP-Typ die Option Subnetz-IP).
   - Lokale IP (Alle konfigurierten IP-Adressen des ausgewählten IP-Typs befinden sich in der Dropdownliste Lokale IP. Wählen Sie die gewünschte IP aus der Liste aus.)
   - Protokoll
   - IPsec-Profil
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

So erstellen Sie eine PBR-Regel und binden den IPSEC-Tunnel über die GUI:

1. Navigieren Sie zu **System** > **Netzwerk** > **PBR**.
2. Klicken Sie auf der Registerkarte **PBR** auf **Hinzufügen**.
3. Legen Sie auf der Seite **PBR erstellen** die folgenden Parameter fest:
   - Name
   - Aktion
   - Nächster Hop-Typ (Wählen Sie IP Tunnel)
   - IP-Tunnelname
   - Quell-IP Niedrig
   - Quell-IP hoch
   - Ziel-IP niedrig
   - Ziel-IP hoch
4. Klicken Sie auf **Erstellen**und dann auf **Schließen**.

Die entsprechende neue CloudBridge Connector-Tunnelkonfiguration auf der Citrix ADC Appliance wird in der GUI angezeigt. Der aktuelle Status des CloudBridge-Connector-Tunnels wird im Bereich Konfigurierter CloudBridge-Connector angezeigt. Ein grüner Punkt zeigt an, dass der Tunnel oben ist. Ein roter Punkt zeigt an, dass der Tunnel heruntergefahren ist.

Die folgenden Befehle erstellen Einstellungen der Citrix ADC Appliance NS_Appliance-1 in Beispiel für

eine CloudBridge Connector-Konfiguration. :

```
> add ipsec profile NS_Cisco-ASA_IPSec_Profile -psk
   examplepresharedkey -ikeVersion v1 - encAlgo AES - hashalgo
   HMAC_SHA1 - lifetime 315360 -perfectForwardSecrecy ENABLE

Done

> add iptunnel NS_Cisco-ASA_Tunnel 203.0.113.200 255.255.255.255
   198.51.100.100 - protocol IPSEC - ipsecProfileName NS_Cisco-
   ASA_IPSec_Profile


Done

> add pbr NS_Cisco-ASA_Pbr -srcIP 10.102.147.0-10.102.147.255 - destIP
   10.20.0.0-10.20.255.255 - ipTunnel NS_Cisco-ASA_Tunnel


Done

> apply pbrs

Done

<!--NeedCopy-->
```

Überwachung des CloudBridge-Connector-Tunnels

Sie können die Leistung von CloudBridge Connector-Tunneln auf einer Citrix ADC Appliance mithilfe von CloudBridge Connector-Tunnelstatistikindikatoren überwachen. Weitere Informationen zum Anzeigen von CloudBridge Connector-Tunnelstatistiken auf einer Citrix ADC Appliance finden Sie unter Monitoring von CloudBridge Connector Tunnels.

Hohe Verfügbarkeit

October 5, 2021

Eine Hochverfügbarkeitsbereitstellung von zwei Citrix ADC Appliances kann einen unterbrechungsfreien Betrieb bei jeder Transaktion ermöglichen. Wenn eine Appliance als primärer Knoten und

die andere als sekundärer Knoten konfiguriert ist, akzeptiert der primäre Knoten Verbindungen und verwaltet Server, während der sekundäre Knoten den primären Knoten überwacht. Wenn der primäre Knoten aus irgendeinem Grund keine Verbindungen annehmen kann, übernimmt der sekundäre Knoten die Übernahme.

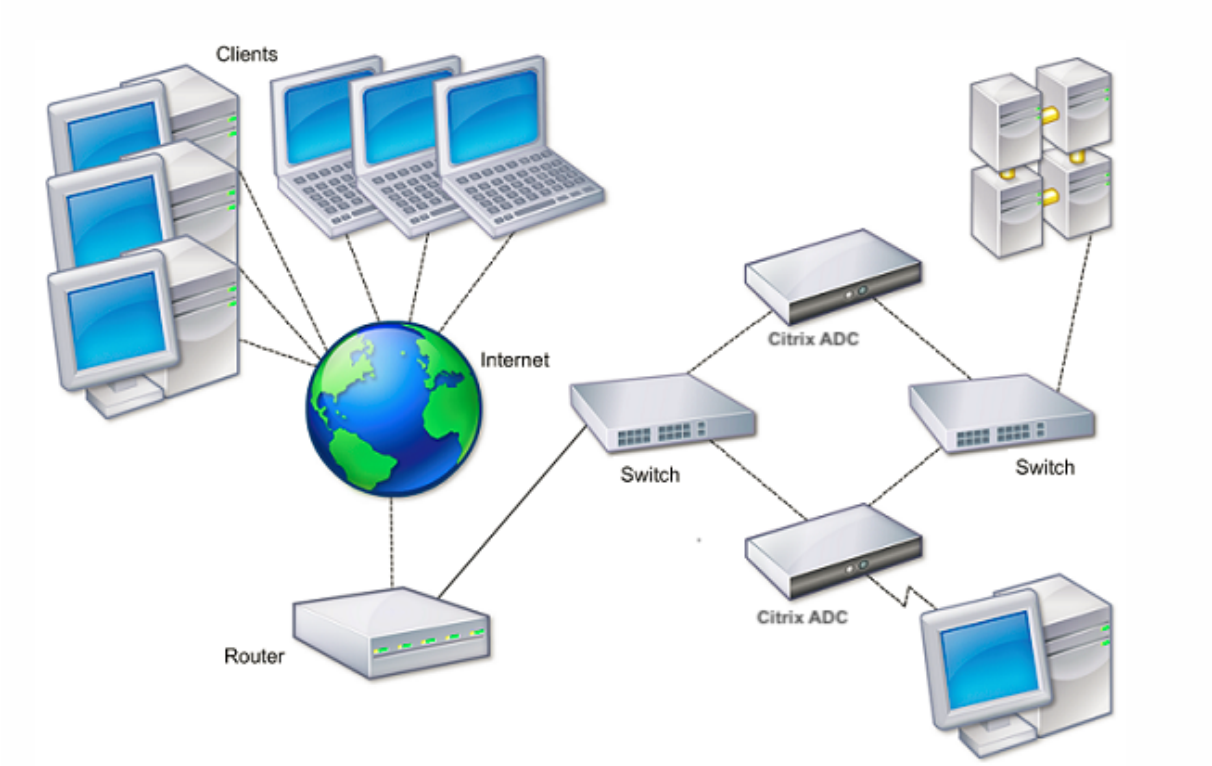
Der sekundäre Knoten überwacht den primären Knoten, indem er periodische Nachrichten sendet (oft Heartbeat-Nachrichten oder Integritätsprüfungen genannt), um festzustellen, ob der primäre Knoten Verbindungen akzeptiert. Wenn eine Integritätsprüfung fehlschlägt, versucht der sekundäre Knoten die Verbindung für einen bestimmten Zeitraum erneut. Danach wird festgestellt, dass der primäre Knoten nicht normal funktioniert. Der sekundäre Knoten übernimmt dann für den primären (ein Prozess namens Failover).

Nach einem Failover müssen alle Clients ihre Verbindungen zu den verwalteten Servern wiederherstellen. Die Sitzungspersistenzregeln werden jedoch wie vor dem Failover beibehalten.

Wenn die Persistenz der Webserverprotokollierung aktiviert ist, gehen aufgrund des Failovers keine Protokolldaten verloren. Damit die Protokollierungsbeständigkeit aktiviert werden kann, muss die Protokollserverkonfiguration Einträge für beide Systeme in der Datei log.conf enthalten.

Die folgende Abbildung zeigt eine Netzwerkkonfiguration mit einem HA-Paar.

Abbildung 1. Citrix ADC Appliances in einer Hochverfügbarkeitskonfiguration



Um HA zu konfigurieren, sollten Sie zunächst ein Basis-Setup erstellen, wobei beide Knoten im selben Subnetz enthalten sind. Anschließend können Sie die Intervalle anpassen, in denen die Knoten Health

Check-Informationen kommunizieren, den Prozess, mit dem Knoten die Synchronisierung aufrechterhalten wird, und die Verteilung von Befehlen vom primären zum sekundären. Sie können den ausfallsicheren Modus konfigurieren, um eine Situation zu verhindern, in der keiner der Knoten primär ist. Wenn Ihre Umgebung Geräte enthält, die keine unentgeltlichen ARP-Nachrichten von Citrix ADC akzeptieren, sollten Sie virtuelle MAC-Adressen konfigurieren. Wenn Sie für eine komplexere Konfiguration bereit sind, können Sie HA-Knoten in verschiedenen Subnetzen konfigurieren.

Um die Zuverlässigkeit Ihrer HA-Setup zu verbessern, können Sie Routenmonitore konfigurieren und redundante Verbindungen erstellen. In einigen Situationen, z. B. bei der Problembehandlung oder beim Ausführen von Wartungsaufgaben, möchten Sie möglicherweise das Failover eines Knotens erzwingen (dem anderen Knoten den primären Status zuweisen), oder Sie möchten den sekundären Knoten dazu zwingen, dass der sekundäre Knoten sekundär bleibt oder der primäre Knoten primär bleibt.

Punkte, die für eine Hochverfügbarkeits-Einrichtung berücksichtigt werden müssen

October 5, 2021

> **Hinweis:**
>
> Die folgenden Anforderungen für die Konfiguration von Systemen in einem HA-Setup:

- In einer HA-Konfiguration sollten die primären und sekundären Citrix ADC Appliances dasselbe Modell aufweisen. Verschiedene Citrix ADC Modelle werden in einem HA-Paar nicht unterstützt.
- In einem HA-Setup müssen beide Knoten dieselbe Version von Citrix ADC ausführen.
- Einträge in der Konfigurationsdatei (ns.conf) auf dem primären und dem sekundären System müssen übereinstimmen, mit den folgenden Ausnahmen:
  - Das primäre und das sekundäre System müssen jeweils mit eigenen eindeutigen IP-Adressen (NSIPs) konfiguriert werden.
  - Bei einem HA-Paar müssen die Knoten-ID und die zugehörige IP-Adresse eines Knotens auf den anderen Knoten zeigen. Wenn Sie beispielsweise die Knoten NS1 und NS2 haben, müssen Sie NS1 mit einer eindeutigen Knoten-ID und der IP-Adresse von NS2 konfigurieren und NS2 mit einer eindeutigen Knoten-ID und der IP-Adresse von NS1 konfigurieren.
- Wenn Sie eine Konfigurationsdatei auf einem beliebigen Knoten mithilfe einer Methode erstellen, die nicht direkt über die GUI oder die CLI geht (z. B. das Importieren von SSL-Zertifikaten oder das Ändern zu Startskripten), müssen Sie die Konfigurationsdatei auf den anderen Knoten kopieren oder eine identische Datei auf diesem Knoten erstellen.

- Zunächst werden alle Citrix ADC Appliances mit demselben RPC-Knotenkennwort konfiguriert. RPC-Knoten sind interne Systementitäten, die für die System-zu-System-Kommunikation von Konfigurations- und Sitzungsinformationen verwendet werden. Aus Sicherheitsgründen sollten Sie die standardmäßigen RPC-Knotenkennwörter ändern.

  Auf jedem Citrix ADC ist ein RPC-Knoten vorhanden. Dieser Knoten speichert das Kennwort, das mit dem vom kontaktierenden System bereitgestellten Kennwort überprüft wird. Für die Kommunikation mit anderen Systemen benötigt jedes Citrix ADC Kenntnisse über diese Systeme, einschließlich der Authentifizierung auf diesen Systemen. RPC-Knoten pflegen diese Informationen, einschließlich der IP-Adressen der anderen Systeme und der Kennwörter, die sie für die Authentifizierung benötigen.

  RPC-Knoten werden implizit erstellt, wenn ein Knoten hinzugefügt oder eine GSLB-Site (Global Server Load Balancing) hinzugefügt wird. Sie können RPC-Knoten nicht manuell erstellen oder löschen.

  > **Hinweis**:
  >
  > Wenn die Citrix ADC Appliances in einem Hochverfügbarkeitssetup im Einarmmodus konfiguriert sind, müssen Sie alle Systemschnittstellen außer derjenigen deaktivieren, die mit dem Switch oder Hub verbunden sind.

  Für eine IPv6-HA-Konfiguration gelten die folgenden Überlegungen:

  - Sie müssen die IPv6pt-Lizenz auf beiden Citrix ADC Appliances installieren.
  - Aktivieren Sie nach der Installation der IPv6pt-Lizenz das IPv6-Feature mit der GUI oder der Befehlszeilenschnittstelle.
  - Beide Citrix ADC Appliances benötigen eine globale NSIP-IPv6-Adresse. Darüber hinaus müssen Netzwerkentitäten (z. B. Switches und Router) zwischen den beiden Knoten IPv6 unterstützen.

Konfiguration der Hochverfügbarkeit

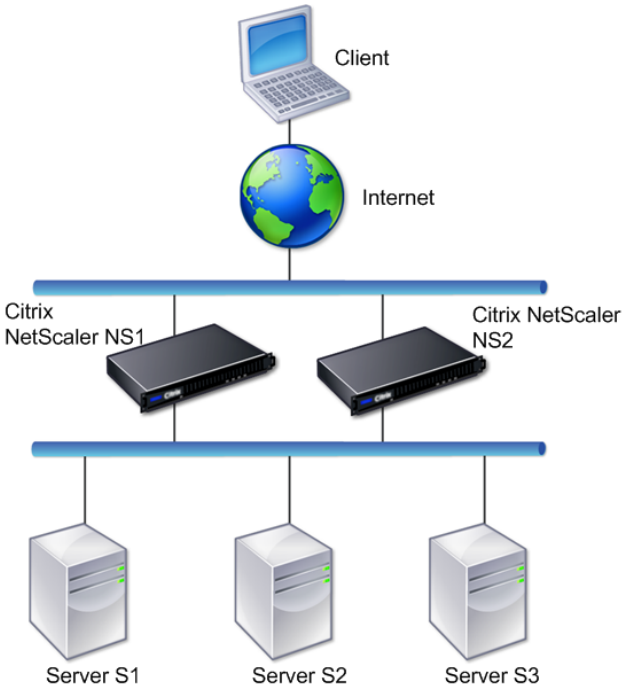
December 3, 2021

Um eine Hochverfügbarkeitskonfiguration einzurichten, erstellen Sie zwei Knoten, von denen jeder die Citrix ADC IP (NSIP) -Adresse des anderen als Remoteknoten definiert. Melden Sie sich zunächst bei einer der beiden Citrix ADC Appliances an, die Sie für Hochverfügbarkeit konfigurieren möchten, und fügen Sie einen Knoten hinzu. Geben Sie die Citrix ADC IP (NSIP) -Adresse der anderen Appliance als Adresse des neuen Knotens an. Melden Sie sich dann bei der anderen Appliance an und fügen Sie einen Knoten hinzu, der die NSIP-Adresse der ersten Appliance enthält. Ein Algorithmus bestimmt, welcher Knoten primär und welcher sekundär wird.

> **Hinweis**:
>
> Die Citrix ADC GUI bietet eine Option, die verhindert, dass Sie sich bei der zweiten Appliance anmelden müssen.

Die folgende Abbildung zeigt ein einfaches HA-Setup, bei dem sich beide Knoten im selben Subnetz befinden.

Abbildung 1. Zwei Citrix ADC Appliances in einer Hochverfügbarkeitskonfiguration angeschlossen



Hinzufügen eines Remote-Knotens

Um eine Citrix ADC Remote-Appliance als Knoten in einem Hochverfügbarkeits-Setup hinzuzufügen, geben Sie eine eindeutige Knoten-ID und die NSIP-Adresse der Appliance an. Wenn Sie einen HA-Knoten hinzufügen, müssen Sie den HA-Monitor für jede Schnittstelle deaktivieren, die nicht angeschlossen ist oder nicht für Datenverkehr verwendet wird. Für CLI-Benutzer ist dies ein separates Verfahren.

> **Hinweis**:
>
> Um sicherzustellen, dass jeder Knoten in der Hochverfügbarkeitskonfiguration dieselben Einstel-

> lungen hat, sollten Sie Ihre SSL-Zertifikate, Startskripte und andere Konfigurationsdateien mit denen auf dem primären Knoten synchronisieren.

So fügen Sie einen Knoten mithilfe der Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add ha node <id> <IPAddress>`
- `show ha node`

Beispiel

```
> add ha node 10 203.0.113.32
<!--NeedCopy-->
```

Deaktivieren eines HA-Monitors mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `set interface <ifNum> [-haMonitor ( ON | OFF )]`
- `show interface <ifNum>`

Beispiel

```
> set interface 1/3 -haMonitor OFF
 Done
<!--NeedCopy-->
```

So fügen Sie einen Remote-Knoten mithilfe der GUI hinzu

Navigieren Sie zu **System** > **Hochverfügbarkeit**, und fügen Sie auf der Registerkarte **Knoten** einen neuen Remote-Knoten hinzu, oder bearbeiten Sie einen vorhandenen Knoten.

Deaktivieren oder Aktivieren eines Nodes

Sie können nur einen sekundären Knoten deaktivieren oder aktivieren. Wenn Sie einen sekundären Knoten deaktivieren, sendet er keine Heartbeat-Nachrichten mehr an den primären Knoten, sodass der primäre Knoten den Status des sekundären Knotens nicht mehr überprüfen kann. Wenn Sie einen Knoten aktivieren, nimmt der Knoten an der Hochverfügbarkeitskonfiguration teil.

So deaktivieren oder aktivieren Sie einen Knoten mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein:

- `set ha node -hastatus DISABLED`
- `set ha node -hastatus ENABLED`

So deaktivieren oder aktivieren Sie einen Knoten mithilfe der GUI

1. Navigieren Sie zu **System** > **Hochverfügbarkeit**, und öffnen Sie auf der Registerkarte **Knoten** den Knoten.
2. Wählen Sie in der Liste **Hochverfügbarkeitsstatus** die **Option AKTIVIERT (aktiv an HA teilnehmen)** oder **DEAKTIVIERT (Nicht an HA teilnehmen)**aus.

Knoten entfernen

Wenn Sie einen Knoten entfernen, befinden sich die Knoten nicht mehr in Hochverfügbarkeitskonfiguration.

So entfernen Sie einen Knoten mithilfe der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm ha node <id>
```

Beispiel

```
1 > rm ha node 10
2   Done
3 <!--NeedCopy-->
```

So entfernen Sie einen Knoten mithilfe der GUI

Navigieren Sie zu **System** > **Hochverfügbarkeit**, und löschen Sie den **Knoten** auf der Registerkarte Knoten.

Konfigurieren der Kommunikationsintervalle

October 5, 2021

Das Hello Intervall ist das Intervall, in dem die Heartbeat-Nachrichten an den Peer-Knoten gesendet werden. Das tote Intervall ist das Zeitintervall, nach dem der Peer-Knoten DOWN markiert wird, wenn Heartbeat-Pakete nicht empfangen werden. Die Heartbeat-Nachrichten sind UDP-Pakete, die an Port 3003 des anderen Knotens in einem HA-Paar gesendet werden. Dead Intervall muss als Vielfaches von Hallo Intervall festgelegt werden.

So legen Sie die hallo und toten Intervalle mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `set HA node [-helloInterval <msecs>] [-deadInterval <secs>]`
- `show HA node <id>`

So legen Sie die Hallo- und Dead-Intervalle mit der GUI fest

1. Navigieren Sie zu **System** > **Hochverfügbarkeit**, und öffnen Sie auf der Registerkarte **Knoten** den Knoten.
2. Legen Sie die folgenden Parameter fest:
   - Hallo Intervall (ms)
   - Dead Intervall (Sekunden)

Synchronisierung konfigurieren

October 5, 2021

Die Synchronisierung ist ein Prozess der Duplizierung der Konfiguration des primären Knotens auf dem sekundären Knoten. Der Zweck der Synchronisierung besteht darin, sicherzustellen, dass keine Konfigurationsinformationen zwischen dem primären und dem sekundären Knoten verloren gehen, unabhängig von der Anzahl der auftretenden Failovers. Die Synchronisierung verwendet Port 3010.

Die Synchronisierung wird durch einen der folgenden Umstände ausgelöst:

- Der sekundäre Knoten in einem HA-Setup wird nach einem Neustart angezeigt.
- Der primäre Knoten wird nach einem Failover sekundär.

Die automatische Synchronisierung ist standardmäßig aktiviert. Sie können die Synchronisierung auch erzwingen.

Deaktivieren oder Aktivieren der Synchronisierung

Die automatische HA-Synchronisierung ist standardmäßig auf jedem Knoten in einem HA-Paar aktiviert. Sie können es auf beiden Knoten aktivieren oder deaktivieren.

So deaktivieren oder aktivieren Sie die automatische Synchronisierung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `set HA node -haSync DISABLED`
- `set HA node -haSync ENABLED`

So deaktivieren oder aktivieren Sie die Synchronisierung mit der GUI

1. Navigieren Sie zu **System** > **Hochverfügbarkeit** .
2. Deaktivieren oder wählen Sie unter HA-Synchronisation den sekundären Knoten, der die Konfiguration von Primär abruft.

Erzwingen der Synchronisierung des sekundären Knotens mit dem primären Knoten

Neben der automatischen Synchronisierung unterstützt Citrix ADC die erzwungene Synchronisierung. Sie können die Synchronisierung entweder vom primären oder vom sekundären Knoten erzwingen. Wenn Sie die Synchronisierung vom sekundären Knoten erzwingen, beginnt die Synchronisierung der Konfiguration mit dem primären Knoten.

Wenn die Synchronisierung jedoch bereits ausgeführt wird, schlägt die erzwungene Synchronisierung fehl, und das System zeigt eine Warnung an. Die erzwungene Synchronisierung schlägt auch unter folgenden Umständen fehl:

- Sie erzwingen die Synchronisierung auf einem eigenständigen System.
- Der sekundäre Knoten ist deaktiviert.
- HA-Synchronisierung ist auf dem sekundären Knoten deaktiviert.

So erzwingen Sie die Synchronisierung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
force HA sync
```

So erzwingen Sie die Synchronisierung mit der GUI

1. Navigieren Sie zu **System** > **Hochverfügbarkeit** .
2. Klicken Sie auf der Registerkarte **Knoten** in der Liste Aktion auf **Synchronisierung erzwingen** .

Synchronisieren von Konfigurationsdateien in einem Hochverfügbarkeitssetup

October 5, 2021

In einem Hochverfügbarkeitssetup werden alle Konfigurationsdateien automatisch vom primären Knoten zum sekundären Knoten in einem Intervall von einer Minute synchronisiert. Die Synchronisierung von Konfigurationsdateien kann manuell über die Befehlszeilenschnittstelle oder die GUI am primären oder sekundären Knoten durchgeführt werden.

Dateien auf der sekundären Seite, die spezifisch für die sekundäre (nicht auf der primären) sind, werden während der Synchronisierung nicht gelöscht.

So synchronisieren Sie Dateien in einem Hochverfügbarkeitssetup mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
sync HA files <mode>
```

Beispiel

```
1 > sync HA files all
2  Done
3 <!--NeedCopy-->
```

```
1 > sync HA files ssl
2  Done
3 <!--NeedCopy-->
```

Parameterbeschreibungen (des in der CLI-Prozedur aufgelisteten Befehls)

```
sync ha files <mode>
```

```
mode
```

Geben Sie einen der folgenden Synchronisierungsmodi an.

- **all** - Synchronisieren Sie Dateien, die sich auf die Systemkonfiguration, Access Gateway-Lesezeichen, SSL-Zertifikate, SSL-CRL-Listen, HTML-Injectionsskripte und XML-Objekte der Application Firewall beziehen.

- **Lesezeichen** - Synchronisieren Sie alle Access Gateway-Lesezeichen.
- **ssl** - Synchronisieren Sie alle Zertifikate, Schlüssel und Zertifikatsperrlisten für die SSL-Funktion.
- **htmlinjection** - Synchronisieren Sie alle Skripts, die für die HTML-Injectionsfunktion konfiguriert sind.
- **imports** - Synchronisieren Sie alle XML-Objekte (z. B. WSDLs, Schemas, Fehlerseiten), die für die Anwendungsfirewall konfiguriert sind.
- **misc** - Synchronisieren Sie alle Lizenzdateien und die rc.conf-Datei.
- **all_plus_misc** - Synchronisieren Sie Dateien im Zusammenhang mit der Systemkonfiguration, Access Gateway-Lesezeichen, SSL-Zertifikaten, SSL-CRL-Listen, HTML-Injectionsskripten, XML-Objekten der Anwendungsfirewall, Lizenzen und der rc.conf-Datei.

So synchronisieren Sie Dateien in einem Hochverfügbarkeitssetup mit der GUI

Navigieren Sie zu **System** > **Diagnose** und klicken Sie in der Gruppe **Dienstprogramme** auf **Synchronisierung von HA-Dateien starten**.

Konfigurieren der Befehlspropagierung

October 5, 2021

In einem HA-Setup werden alle Befehle, die auf dem primären Knoten ausgegeben werden, automatisch an den sekundären Knoten weitergegeben und ausgeführt, bevor er auf dem primären Knoten ausgeführt wird. Wenn die Befehlsausbreitung fehlschlägt oder wenn die Befehlsausführung auf dem sekundären Knoten fehlschlägt, führt der primäre Knoten den Befehl aus und protokolliert einen Fehler. Die Befehlsausbreitung verwendet Port 3010.

In einer HA-Paarkonfiguration ist die Befehlspropagierung sowohl auf dem primären als auch auf dem sekundären Knoten standardmäßig aktiviert. Sie können die Befehlspropagierung auf beiden Knoten in einem HA-Paar aktivieren oder deaktivieren. Wenn Sie die Befehlspropagierung auf dem primären Knoten deaktivieren, werden Befehle nicht an den sekundären Knoten weitergegeben. Wenn Sie die Befehlspropagierung auf dem sekundären Knoten deaktivieren, werden vom primären Knoten propagierte Befehle nicht auf dem sekundären Knoten ausgeführt.

> **Hinweis:**
>
> Denken Sie nach der erneuten Aktivierung der Propagierung daran, die Synchronisierung zu erzwingen.

Wenn die Synchronisierung erfolgt, während Sie die Propagierung deaktivieren, werden alle konfigurationsbezogenen Änderungen, die Sie vornehmen, bevor die Deaktivierung der Propagierung

wirksam wird, mit dem sekundären Knoten synchronisiert. Dies gilt auch für Fälle, in denen die Propagierung während der Synchronisierung deaktiviert ist.

So deaktivieren oder aktivieren Sie die Befehlspropagierung mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

- set HA node -haProp DISABLED
- set HA node -haProp ENABLED

So deaktivieren oder aktivieren Sie die Befehlspropagierung mit der GUI

1. Navigieren Sie zu **System** > **Hochverfügbarkeit**, und öffnen Sie auf der Registerkarte **Knoten** den Knoten.
2. Deaktivieren oder wählen Sie den Primärknoten, der die Konfiguration an die Option Sekundär weitergibt.

Beschränken des Hochverfügbarkeitssynchronisationsverkehrs auf ein VLAN

October 5, 2021

In einer Hochverfügbarkeitsbereitstellung (HA) fließt der Datenverkehr im Zusammenhang mit der Aufrechterhaltung der HA-Konfiguration zwischen den beiden HA-Knoten. Dieser Datenverkehr ist von den folgenden Typen:

- Konfigurations-Synchronisation
- Config-Propagierung
- Verbindungsspiegelung
- Load Balancing Persistency Config-Synchronisation
- Persistente Sitzungssynchronisierung
- Sitzungsstatus-Synchronisierung

Der ordnungsgemäße Ablauf dieses HA-bezogenen Datenverkehrs zwischen den beiden Knoten ist entscheidend für das Funktionieren der HA-Bereitstellung. Typischerweise ist der HA-bezogene Datenverkehr klein, kann aber während eines Failovers sehr hoch werden. Es wird sehr hoch, wenn das statusbehaftete Verbindungs-Failover aktiviert ist und der Knoten, der vor dem Failover primär war, eine große Anzahl von Verbindungen verarbeitet.

Standardmäßig fließt der HA-bezogene Datenverkehr durch die VLANs, an die die NSIP-Adresse gebunden ist. Um einem potenziellen Anstieg dieses Datenverkehrs Rechnung zu tragen, können Sie den HA-bezogenen Datenverkehr vom Verwaltungsdatenverkehr trennen und dessen Fluss auf ein separates VLAN beschränken. Dieses VLAN wird als HA SYNC VLAN bezeichnet.

Punkte, die vor der Konfiguration eines HA SYNC VLAN zu beachten sind

- Die Konfiguration eines HA SYNC VLAN wird weder propagiert noch synchronisiert. Mit anderen Worten, das HA SYNC VLAN ist knotenspezifisch und wird unabhängig auf jedem Knoten konfiguriert.
- HA SYNC VLAN-Konfiguration wird entfernt, wenn Sie die Konfiguration nur im FULL-Modus löschen.
- HA MON muss für Schnittstellen, die Teil des HA SYNC VLAN sind, auf OFF gesetzt werden, um eine Situation zu vermeiden, in der beide Knoten als primärer Knoten fungieren.
- Verwaltungsschnittstellen (z. B. 0/1 und 0/2) dürfen nicht Teil des HA SYNC VLAN sein, sodass der HA-bezogene Datenverkehr nicht über Verwaltungsschnittstellen fließt.
- Citrix empfiehlt, Hochverfügbarkeits-Heartbeat-Meldungen auf Verwaltungsschnittstellen zu deaktivieren und auf HA SYNC VLAN-Schnittstellen zu aktivieren. Nachdem diese Empfehlungen erfüllt wurden, können Hochverfügbarkeits-Heartbeat-Meldungen auch auf Datenschnittstellen aktiviert werden.

  Weitere Informationen zum Deaktivieren von Heartbeat-Nachrichten mit hoher Verfügbarkeit auf Schnittstellen finden Sie unter Verwalten von Heartbeat-Nachrichten mit hoher Verfügbarkeit auf einer Citrix ADC Appliance.

Um ein HA-SYNC-VLAN auf einem Citrix ADC Knoten zu konfigurieren, geben Sie ein konfiguriertes VLAN mit dem HA SYNC-VLAN-Parameter der lokalen Knotenentität an.

So konfigurieren Sie ein HA SYNC-VLAN auf einem lokalen Knoten über die Befehlszeile:

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `set ha node -syncvlan <VLANID>`
- `show node`

Beschreibung des Parameters:

syncvlan (Sync VLAN) - VLAN, auf das HA-bezogener Datenverkehr gesendet wird. Dies umfasst Datenverkehr für Synchronisation, Propagierung, Verbindungsspiegelung, Load Balancing-Persistenz, Konfigurationssynchronisation, persistente Sitzungssynchronisation und Synchronisation des Sitzungsstatus. HA Heartbeats können jedoch jede Schnittstelle verwenden.

So konfigurieren Sie ein HA SYNC-VLAN auf einem Knoten mit der GUI:

1. Navigieren Sie zu **System** > **Hochverfügbarkeit** .
2. Legen Sie den **Sync-VLAN-Parameter** fest, während Sie den lokalen Knoten ändern.

Konfigurieren des ausfallsicheren Modus

October 5, 2021

In einer HA-Konfiguration stellt der ausfallsichere Modus sicher, dass ein Knoten immer primär ist, wenn beide Knoten die Zustandsprüfung fehlschlagen. Damit soll sichergestellt werden, dass, wenn ein Knoten nur teilweise verfügbar ist, Backupmethoden aktiviert sind, um den Datenverkehr so gut wie möglich zu verarbeiten. Der HA-Ausfallsicheremodus wird unabhängig auf jedem Knoten konfiguriert.

Die folgende Tabelle zeigt einige der ausfallsicheren Fälle. Der Status NOT_UP bedeutet, dass der Knoten die Zustandsprüfung fehlgeschlagen ist, aber er ist teilweise verfügbar. Der UP Status bedeutet, dass der Knoten die Integritätsprüfung bestanden hat.

Knoten A (primärer) Integritätsstatus	Knoten B (sekundärer) Integritätsstatus	Standard-HA-Verhalten	Fail-Safe aktiviertes HA-Verhalten	Beschreibung
NOT_UP (zuletzt fehlgeschlagen)	NOT_UP (zuerst fehlgeschlagen)	A (Sekundär), B (Sekundär)	A (Primär), B (Sekundär)	Wenn beide Knoten fehlschlagen, bleibt der Knoten, der der letzte primäre Knoten war, primär.
NOT_UP (zuerst fehlgeschlagen)	NOT_UP (zuletzt fehlgeschlagen)	A (Sekundär), B (Sekundär)	A (Sekundär), B (Primär)	Wenn beide Knoten fehlschlagen, bleibt der Knoten, der der letzte primäre Knoten war, primär.

Knoten A (primärer) Integritätsstatus	Knoten B (sekundärer) Integritätsstatus	Standard-HA-Verhalten	Fail-Safe aktiviertes HA-Verhalten	Beschreibung
BEREIT	BEREIT	A (Primär), B (Sekundär)	A (Primär), B (Sekundär)	Wenn beide Knoten die Integritätsprüfung bestehen, keine Änderung des Verhaltens mit aktivierter Fail-Safe.
BEREIT	NOT_UP	A (Primär), B (Sekundär)	A (Primär), B (Sekundär)	Wenn nur der sekundäre Knoten ausfällt, ändert sich das Verhalten bei aktivierter Fail-Safe nicht.
NOT_UP	BEREIT	A (Sekundär), B (Primär)	A (Sekundär), B (Primär)	Wenn nur der primäre Fehler auftritt, keine Änderung des Verhaltens mit aktivierter Fail-Safe.
NOT_UP	UP (STAYSECONDARY)	A (Sekundär), B (Sekundär)	A (Primär), B (Sekundär)	Wenn der sekundäre als STAYSECONDARY konfiguriert ist, bleibt der primäre Primärserver auch dann primär, wenn er fehlschlägt.

So aktivieren Sie den ausfallsicheren Modus mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set HA node [-failSafe ( **ON** | **OFF** )]
```

Beispiel

```
1 set ha node -failsafe ON
2 <!--NeedCopy-->
```

So aktivieren Sie den ausfallsicheren Modus mit der GUI

1. Navigieren Sie zu **System** > **Hochverfügbarkeit**, und öffnen Sie auf der Registerkarte **Knoten** den Knoten.
2. Wählen Sie unter **Fehlerabgesicherter Modus**die Option **Einen primären Knoten pflegen**, auch wenn beide Knoten fehlerhaft sind.

Konfigurieren von virtuellen MAC-Adressen

October 5, 2021

Eine virtuelle MAC-Adresse ist eine schwebende Entität, die von den primären und den sekundären Knoten in einem HA-Setup gemeinsam genutzt wird.

In einem HA-Setup besitzt der primäre Knoten alle schwebenden IP-Adressen, wie MIPs, SNIPs und VIPs. Der primäre Knoten reagiert auf ARP-Anfragen (Address Resolution Protocol) für diese IP-Adressen mit einer eigenen MAC-Adresse. Daher wird die ARP-Tabelle eines externen Geräts (z. B. eines Upstream-Routers) mit der unverankerten IP-Adresse und der MAC-Adresse des primären Knotens aktualisiert.

Wenn ein Failover auftritt, übernimmt der sekundäre Knoten als neuer primärer Knoten. Es verwendet dann Gratuitous ARP (GARP), um die Floating-IP-Adressen zu werben, die es von der primären erworben hat. Die MAC-Adresse, die die neue primäre Werbung ausgibt, ist jedoch die MAC-Adresse der eigenen Schnittstelle.

Einige Geräte (insbesondere einige Router) akzeptieren die von der Citrix ADC Appliance generierten GARP-Nachrichten nicht. Infolgedessen behalten einige externe Geräte die alte IP-zu-MAC-Zuordnung, die vom alten primären Knoten angekündigt wird. Dies kann zu einem Ausfall der Website führen.

Sie können dieses Problem beheben, indem Sie einen virtuellen MAC auf beiden Knoten eines HA-Paares konfigurieren. Beide Knoten besitzen dann identische MAC-Adressen. Wenn ein Failover

auftritt, bleibt die MAC-Adresse des sekundären Knotens unverändert, und die ARP-Tabellen auf den externen Geräten müssen nicht aktualisiert werden.

Um einen virtuellen MAC zu erstellen, müssen Sie zuerst eine Virtual Router ID (VRID) erstellen und an eine Schnittstelle binden. (In einem HA-Setup müssen Sie die VRID an die Schnittstellen auf beiden Knoten binden.) Sobald die VRID an eine Schnittstelle gebunden ist, generiert das System einen virtuellen MAC mit der VRID als letztes Oktett.

Dieser Abschnitt enthält die folgenden Details:

- Konfigurieren virtueller IPv4-MACs
- Konfigurieren virtueller IPv6-Mac6s

Konfigurieren virtueller IPv4-MACs

Wenn Sie eine virtuelle IPv4-MAC-Adresse erstellen und an eine Schnittstelle binden, verwendet jedes IPv4-Paket, das von der Schnittstelle gesendet wird, die virtuelle MAC-Adresse, die an die Schnittstelle gebunden ist. Wenn kein virtueller IPv4-MAC an eine Schnittstelle gebunden ist, wird die physikalische MAC-Adresse der Schnittstelle verwendet.

Der generische virtuelle MAC hat die Form`00:00:5e:00:01:<VRID>`. Wenn Sie beispielsweise eine VRID mit dem Wert 60 erstellen und an eine Schnittstelle binden, ist der resultierende virtuelle MAC 00:00:5 e: 00:01:3 c, wobei 3c die Hexadezimaldarstellung der VRID ist. Sie können 255 VRIDs mit Werten von 1 bis 255 erstellen.

Erstellen oder Ändern eines virtuellen IPv4-MAC

Sie erstellen einen virtuellen IPv4-MAC, indem Sie ihm eine virtuelle Router-ID zuweisen. Sie können dann den virtuellen MAC an eine Schnittstelle binden. Sie können nicht mehrere VRIDs an dieselbe Schnittstelle binden. Um die virtuelle MAC-Konfiguration zu überprüfen, sollten Sie die virtuellen MACs und die Schnittstellen anzeigen und untersuchen, die an die virtuellen MACs gebunden sind.

So fügen Sie einen virtuellen MAC mit der Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add vrID`
- `bind vrid <id> -ifnum <interface_name>`
- `show vrID`

Beispiel


```
> add vrID 100
 Done
> bind vrid 100 -ifnum 1/1 1/2 1/3
 Done
<!--NeedCopy-->
```

So heben Sie die Bindung von Schnittstellen von einem virtuellen MAC mit der Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `unbind vrid <id> -ifnum <interface_name>`
- `show vrID`

So konfigurieren Sie einen virtuellen MAC mit der GUI

Navigieren Sie zu **System** > **Netzwerk** > **VMAC**, und fügen Sie auf der Registerkarte **VMAC** einen neuen virtuellen MAC hinzu, oder bearbeiten Sie einen vorhandenen virtuellen MAC.

Entfernen eines virtuellen IPv4-MAC

Um einen virtuellen IPv4-MAC zu entfernen, löschen Sie seine virtuelle Router-ID.

So entfernen Sie einen virtuellen IPv4-MAC mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

`rm vrid <id>`

Beispiel

```
rm vrid 100s
<!--NeedCopy-->
```

So entfernen Sie einen virtuellen IPv4-MAC mit der GUI

Navigieren Sie zu **System** > **Netzwerk** > **VMAC**, und löschen Sie auf der Registerkarte **VMAC** den virtuellen IPv4-MAC.

Konfigurieren virtueller IPv6-Mac6s

Citrix ADC unterstützt virtuelles MAC6 für IPv6-Pakete. Sie können jede Schnittstelle an einen virtuellen MAC6 binden, auch wenn ein virtueller IPv4-MAC an die Schnittstelle gebunden ist. Jedes IPv6-Paket, das von der Schnittstelle gesendet wird, verwendet den virtuellen MAC6, der an diese Schnittstelle gebunden ist. Wenn kein virtueller MAC6 an eine Schnittstelle gebunden ist, verwendet ein IPv6-Paket den physischen MAC.

Erstellen oder Ändern eines virtuellen MAC6

Sie erstellen einen virtuellen IPv6-MAC, indem Sie ihm eine virtuelle IPv6-Router-ID zuweisen. Sie können dann den virtuellen MAC an eine Schnittstelle binden. Sie können nicht mehrere IPv6-VRIDs an eine Schnittstelle binden. Um die virtuelle MAC6-Konfiguration zu überprüfen, sollten Sie die virtuellen MAC6s und die an die virtuellen MAC6s gebundenen Schnittstellen anzeigen und untersuchen.

So fügen Sie einen virtuellen MAC6 mit der Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add vrID6 <id>`
- `bind vrID6 <id> -ifnum <interface_name>`
- `show vrID6`

Beispiel

```
1 > add vrID6 100
2 Done
3 > bind vrID6 100 -ifnum 1/1 1/2 1/3
4  Done
5 <!--NeedCopy-->
```

So lösen Sie die Bindung von Schnittstellen von einem virtuellen MAC6 mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `unbind vrID6 <id> -ifnum <interface_name>`
- `show vrID6`

So konfigurieren Sie einen virtuellen MAC6 mit der GUI

Navigieren Sie zu **System** > **Netzwerk** > **VMAC**, und fügen Sie auf der Registerkarte **VMAC6** einen neuen virtuellen MAC6 hinzu, oder bearbeiten Sie einen vorhandenen virtuellen MAC6.

Entfernen eines virtuellen MAC6

Um einen virtuellen IPv4-MAC zu entfernen, löschen Sie seine virtuelle Router-ID.

So entfernen Sie einen virtuellen MAC6 mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm vrid6 <id>
```

Beispiel

```
1 rm vrid6 100s
2 <!--NeedCopy-->
```

So entfernen Sie einen virtuellen MAC6 mit der GUI

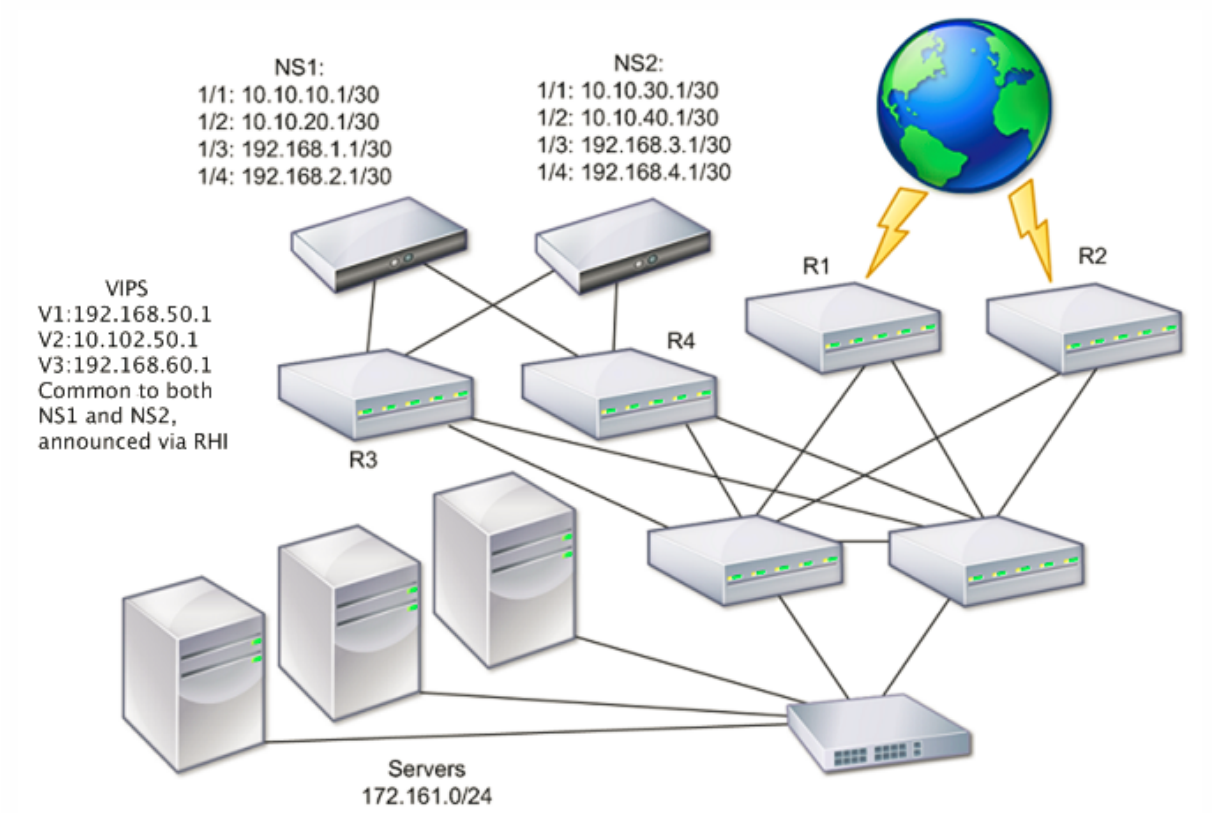
Navigieren Sie zu **System** > **Netzwerk** > **VMAC**, und löschen Sie auf der Registerkarte **VMAC6** die virtuelle Router-ID.

Konfigurieren von Hochverfügbarkeitsknoten in verschiedenen Subnetzen

October 5, 2021

Die folgende Abbildung zeigt eine HA-Bereitstellung mit den beiden Systemen in verschiedenen Subnetzen:

Abbildung 1. Hohe Verfügbarkeit über ein geroutetes Netzwerk



In der Abbildung sind die Systeme NS1 und NS2 mit zwei separaten Routern, R3 und R4, auf zwei verschiedenen Subnetzen verbunden. Die Citrix ADC Appliances tauschen Heartbeat-Pakete über die Router aus. Diese Konfiguration könnte erweitert werden, um Bereitstellungen mit beliebig vielen Schnittstellen zu ermöglichen.

> **Hinweis**:
>
> Wenn Sie statisches Routing in Ihrem Netzwerk verwenden, müssen Sie statische Routen zwischen allen Systemen hinzufügen, um sicherzustellen, dass Heartbeat-Pakete erfolgreich gesendet und empfangen werden. (Wenn Sie dynamisches Routing auf Ihren Systemen verwenden, sind statische Routen nicht erforderlich.)

Wenn sich die Knoten in einem HA-Paar in zwei separaten Netzwerken befinden, müssen der primäre und sekundäre Knoten über unabhängige Netzwerkkonfigurationen verfügen. Dies bedeutet, dass Knoten in verschiedenen Netzwerken keine Entitäten wie SNIP-Adresse, VLANs und Routen gemeinsam nutzen können. Dieser Konfigurationstyp, bei dem die Knoten in einem HA-Paar unterschiedliche konfigurierbare Parameter aufweisen, wird als Independent Network Configuration (INC) oder Symmetric Network Configuration (SNC) bezeichnet.

Die folgende Tabelle fasst die konfigurierbaren Entitäten und Optionen für eine INC zusammen und zeigt, wie sie auf jedem Knoten festgelegt werden müssen.

NetScaler Entitäten	Optionen
IPs (NSIP/Snips)	Knotenspezifisch. Nur auf diesem Knoten aktiv.
VIPs	Schweben.
VLANs	Knotenspezifisch. Nur auf diesem Knoten aktiv.
Routen	Knotenspezifisch. Nur auf diesem Knoten aktiv. Link-Load-Balancing-Routen sind unverankert.
ACLs	Schwebende (üblich). Aktiv auf beiden Knoten.
Dynamisches Routing	Knotenspezifisch. Nur auf diesem Knoten aktiv. Der sekundäre Knoten sollte auch die Routing-Protokolle und Peer mit Upstream-Routern ausführen.
L2-Modus	Schwebende (üblich). Aktiv auf beiden Knoten.
L3-Modus	Schwebende (üblich). Aktiv auf beiden Knoten.
Umgekehrte NAT (RNAT)	RNAT-Konfiguration mit der NAT-IP-Adresse, die auf eine virtuelle Server-IP-Adresse (VIP) eingestellt ist, da die VIP-Adresse floatend (häufig) ist.

Wie bei der Konfiguration von HA-Knoten im selben Subnetz melden Sie sich zum Konfigurieren von HA-Knoten in verschiedenen Subnetzen bei jeder der beiden Citrix ADC Appliances an und fügen einen Remote-Knoten hinzu, der die andere Appliance darstellt.

Hinzufügen eines Remoteknotens

Wenn sich zwei Knoten eines HA-Paares in verschiedenen Subnetzen befinden, muss jeder Knoten über eine andere Netzwerkkonfiguration verfügen. Um zwei unabhängige Systeme so zu konfigurieren, dass sie als HA-Paar funktionieren, müssen Sie den INC-Modus während des Konfigurationsprozesses angeben.

Wenn Sie einen HA-Knoten hinzufügen, müssen Sie den HA-Monitor für jede Schnittstelle deaktivieren, die nicht verbunden ist oder nicht für den Datenverkehr verwendet wird. Für CLI-Benutzer ist dies eine separate Prozedur.

So fügen Sie einen Knoten mit der Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

- add ha node <id> <IPAddress> -inc ENABLED
- show ha node

Beispiel

```
> add ha node 3 10.102.29.170 -inc ENABLED
 Done
> add ha node 3 1000:0000:0000:0000:0005:0600:700a:888b
  Done
<!--NeedCopy-->
```

So deaktivieren Sie einen HA-Monitor mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

- set **interface** <ifNum> [-haMonitor (**ON** | **OFF**)]
- show **interface** <ifNum>

Beispiel

```
> set interface 1/3 -haMonitor OFF
 Done
<!--NeedCopy-->
```

So fügen Sie einen entfernten Knoten mit der GUI hinzu

1. Navigieren Sie zu **System** > **Hochverfügbarkeit**, und fügen Sie auf der Registerkarte **Knoten** einen neuen entfernten Knoten hinzu.
2. Stellen Sie sicher, dass Sie die Option HA-Monitor auf ausgeschalteten Schnittstellen/Kanälen ausschalten und INC (Independent Network Configuration) im Selbstmodus aktivieren auswählen.

Entfernen eines Knotens

Wenn Sie einen Knoten entfernen, befinden sich die Knoten nicht mehr in der Hochverfügbarkeitskonfiguration.

So entfernen Sie einen Knoten mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
rm ha node <id>
```

Beispiel

```
1 > rm ha node 2
2   Done
3 <!--NeedCopy-->
```

So entfernen Sie einen Knoten mit der GUI

Navigieren Sie zu **System** > **Hochverfügbarkeit**, und löschen Sie den **Knoten** auf der Registerkarte Knoten.

> **Hinweis**:
>
> Mit dem Network Visualizer können Sie die Citrix ADC Appliances anzeigen, die als Hochverfügbarkeits-Paar (High Availability, HA-Paar) konfiguriert sind, und Hochverfügbarkeits-Konfigurationsaufgaben ausführen.

Konfigurieren von Routenmonitoren

October 5, 2021

Sie können Routenmonitore verwenden, um den HA-Status von der internen Routingtabelle abhängig zu machen, unabhängig davon, ob die Tabelle dynamisch gelernte oder statische Routen enthält. In einer HA-Konfiguration überwacht ein Routenmonitor auf jedem Knoten die interne Routingtabelle, um sicherzustellen, dass immer ein Routeneintrag zum Erreichen eines bestimmten Netzwerks vorhanden ist. Wenn der Routeneintrag nicht vorhanden ist, ändert sich der Status des Routenmonitors in DOWN.

Wenn eine Citrix ADC Appliance nur statische Routen zum Erreichen eines Netzwerks aufweist und Sie einen Routenmonitor für das Netzwerk erstellen möchten, müssen Sie überwachte statische Routen (MSR) für die statischen Routen aktivieren. MSR entfernt nicht erreichbare statische Routen aus der internen Routingtabelle. Wenn MSR auf statischen Routen deaktiviert ist, kann eine nicht erreichbare statische Route in der internen Routingtabelle verbleiben, was den Zweck des Routenmonitors überwindet.

Routenmonitore werden sowohl im Nicht-INC-Modus als auch im INC-Modus unterstützt.

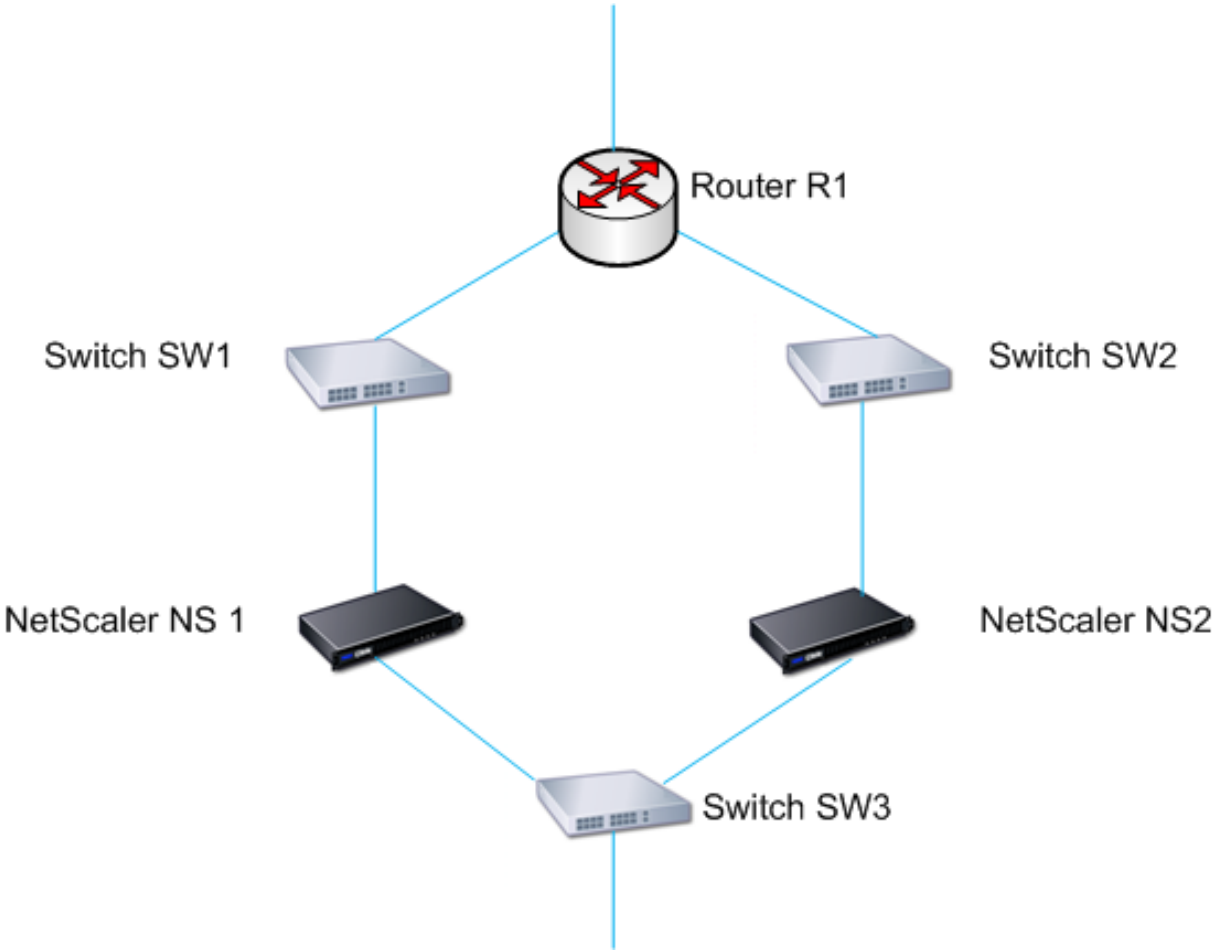
Monitore in HA im Nicht-INC-Modus weiterleiten	Monitore im HA im INC-Modus weiterleiten
Routenmonitore werden von Knoten propagiert und während der Synchronisation ausgetauscht.	Routenmonitore werden weder von Knoten propagiert noch während der Synchronisation ausgetauscht.
Routenmonitore sind nur im aktuellen primären Knoten aktiv.	Routenmonitore sind sowohl auf dem primären als auch auf dem sekundären Knoten aktiv.
Die Citrix ADC Appliance zeigt den Status eines Routenmonitors immer als UP an, unabhängig davon, ob der Routeneintrag in der internen Routingtabelle vorhanden ist oder nicht.	Die Citrix ADC Appliance zeigt den Status des Routenmonitors als DOWN an, wenn der entsprechende Routeneintrag in der internen Routingtabelle nicht vorhanden ist.
Ein Routenmonitor beginnt in den folgenden Fällen nach 180 Sekunden mit der Überwachung seiner Route. [Dies wird durchgeführt, um dynamische Routen zu lernen, was 180 Sekunden dauern kann]: Neustart, Failover, Befehl route6 für v6-Routen setzen, Befehl route msr aktivieren/deaktivieren für v4-Routen festlegen und einen neuen Routenmonitor hinzufügen.	-

Routenmonitore sind in einer HA-Konfiguration ohne INC-Modus nützlich, bei der die Nicht-Erreichbarkeit eines Gateway von einem primären Knoten aus eine der Bedingungen für HA-Failover sein soll.

Betrachten Sie ein Beispiel für ein HA-Setup im Nicht-INC-Modus in einer Zweiarm-Topologie mit Citrix ADC Appliances NS1 und NS2 im selben Subnetz, mit Router R1 und Switches SW1, SW2 und SW3.

Da R1 der einzige Router in diesem Setup ist, soll das HA-Setup Failover erfolgen, wenn R1 vom aktuellen Primärknoten nicht erreichbar ist. Sie können einen Routenmonitor (z. B. RM1 und RM2) auf jedem der Knoten konfigurieren, um die Erreichbarkeit von R1 von diesem Knoten aus zu überwachen.

Abbildung 1.



Bei NS1 als aktueller primärer Knoten lautet der Ausführungsfluss wie folgt:

1. Routenmonitor RM1 auf NS1 überwacht die interne Routingtabelle der NS1 auf das Vorhandensein eines Routeneintrags für Router R1. NS1 und NS2 tauschen Heartbeat-Nachrichten über Switch SW1 oder SW3 in regelmäßigen Abständen aus.
2. Wenn Switch SW1 ausfällt, erkennt das Routingprotokoll auf NS1, dass R1 nicht erreichbar ist, und entfernt daher den Routeneintrag für R1 aus der internen Routingtabelle. NS1 und NS2 tauschen Heartbeat-Nachrichten über Switch SW3 in regelmäßigen Abständen aus.
3. Wenn der Routeneintrag für R1 nicht in der internen Routingtabelle vorhanden ist, initiiert RM1 ein Failover. Wenn die Route zu R1 von NS1 und NS2 ausgefallen ist, findet ein Failover alle 180 Sekunden statt, bis eine der Appliances R1 erreicht und die Konnektivität wiederherstellt.

Hinzufügen eines Routenmonitors zu einem Hochverfügbarkeitsknoten

Eine einzelne Prozedur erstellt einen Routenmonitor und bindet ihn an einen HA-Knoten.

So fügen Sie einen Routenmonitor mit der Befehlszeilenschnittstelle hinzu

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `bind HA node <id> (-routeMonitor <ip_addr|ipv6_addr> [<netmask>])`
- `show HA node`

Beispiel

```
1 > bind HA node 0 -routeMonitor 10.102.71.0 255.255.255.0
2  Done
3 > bind HA node 0 -routeMonitor 1000:0000:0000:0000:0005:0600:700a:888b
4  Done
5 <!--NeedCopy-->
```

So fügen Sie einen Routenmonitor mit der GUI hinzu

Navigieren Sie zu **System** > **Hochverfügbarkeit**, und klicken Sie auf der Registerkarte **Routenmonitore** auf **Konfigurieren** .

Entfernen von Routenmonitoren

So entfernen Sie einen Routenmonitor mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `unbind HA node <id> (-routeMonitor <ip_addr|ipv6_addr> [<netmask>])`
- show ha node

Beispiel

```
1 unbind HA node 3 -routeMonitor 10.102.71.0 255.255.255.0
2 unbind HA node 3 -routeMonitor 1000:0000:0000:0000:0005:0600:700a:888b
3 <!--NeedCopy-->
```

So entfernen Sie einen Routenmonitor mit der GUI

Navigieren Sie zu **System** > **Hochverfügbarkeit**, und löschen Sie auf der Registerkarte **Routenüberwachung** den Routenmonitor.

Beschränken von Failovers, die von Routenmonitoren im Nicht-INC-Modus verursacht werden

October 5, 2021

Wenn in einer HA-Konfiguration im Nicht-INC-Modus Routenmonitore auf beiden Knoten ausfallen, erfolgt ein Failover alle 180 Sekunden, bis einer der Knoten alle Routen erreicht, die von den jeweiligen Routenmonitoren überwacht werden.

Bei einem Knoten können Sie jedoch die Anzahl der Failovers für ein bestimmtes Intervall einschränken, indem Sie die Parameter Maximum Anzahl von Flips und Maximum Flip Time auf den Knoten festlegen. Wenn eine der beiden Grenzwerte erreicht ist, treten keine weiteren Failovers auf, und der Knoten wird als primärer Knoten zugewiesen (aber Knotenstatus als NOT UP), selbst wenn ein Routenmonitor auf diesem Knoten ausfällt. Diese Kombination von HA-Status als Primär und Node Status als NOT UP wird Stick Primär Zustand genannt.

Wenn der Knoten dann alle überwachten Routen erreichen kann, löst der nächste Monitorfehler das Zurücksetzen der Parameter Maximum Anzahl von Flips und Maximum Flip Time auf dem Knoten aus und startet die im Parameter Maximum Flip Time angegebene Zeit.

Diese Parameter werden unabhängig auf jedem Knoten gesetzt und werden daher weder propagiert noch synchronisiert.

Parameter zur Begrenzung der Anzahl von Failovers

- **Maximale Anzahl der Flips (MaxFlips)**

  Maximale Anzahl zulässiger Failovers innerhalb des Maximum Flip Time Intervalls für den Knoten in HA im Nicht-INC-Modus, wenn die Failovers durch einen Route-Monitor-Fehler verursacht werden.

- **Maximale Flipzeit (MaxFlipTime)**

  Zeitraum (in Sekunden), während der Failovers aufgrund eines Route-Monitor-Fehlers für den Knoten in HA im Nicht-INC-Modus zulässig sind.

So beschränken Sie die Anzahl der Failovers mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `set HA node [-maxFlips < positive_integer>] [-maxFlipTime <positive_integer >]`
- `show HA node [< id>]`

So beschränken Sie die Anzahl der Failovers mit der GUI

1. Navigieren Sie zu **System** > **Hochverfügbarkeit**, und öffnen Sie auf der Registerkarte **Knoten** den lokalen Knoten.

2. Legen Sie die folgenden Parameter fest:

- Maximale Anzahl der Flips
- Maximale Flip-Zeit

```
> set ha node -maxFlips 30 -maxFlipTime 60
Done
> sh ha node
1) Node ID: 0
IP: 10.102.169.82 (NS)
Node State: UP
Master State: Primary
Fail-Safe Mode: OFF
INC State: DISABLED
Sync State: ENABLED
Propagation: ENABLED
Enabled Interfaces : 1/1
Disabled Interfaces : None
HA MON ON Interfaces : 1/1
Interfaces on which heartbeats are not seen :None
Interfaces causing Partial Failure:None
SSL Card Status: NOT PRESENT
Hello Interval: 200 msecs
Dead Interval: 3 secs
Node in this Master State for: 0:4:24:1 (days:hrs:min:sec)

2) Node ID: 1
IP: 10.102.169.81
Node State: UP
Master State: Secondary
Fail-Safe Mode: OFF
INC State: DISABLED
Sync State: SUCCESS
Propagation: ENABLED
Enabled Interfaces : 1/1
Disabled Interfaces : None
HA MON ON Interfaces : 1/1
Interfaces on which heartbeats are not seen : None
Interfaces causing Partial Failure: None
SSL Card Status: NOT PRESENT

Local node information:
Configured/Completed Flips: 30/0
Configured Flip Time: 60
```



```
40      Critical Interfaces: 1/1
41
42      Done
43  <!--NeedCopy-->
```

SNMP-Alarm für klebrigen Primärzustand

Aktivieren Sie den HA-Sticky-PRIMARY SNMP-Alarm in einem Knoten mit hochverfügbarer Einrichtung, wenn Sie benachrichtigt werden möchten, dass der Knoten zu klebrigen primären Knoten wird. Wenn der Knoten zu klebrigen primären Knoten wird, warnt er durch Generieren einer Trap-Nachricht (StickyPrimary (1.3.6.1.4.1.5951.1.1.0.138)) und sendet ihn an alle konfigurierten SNMP-Trap-Ziele. Weitere Informationen zum Konfigurieren von SNMP-Alarmen und Trap-Zielen finden Sie unter Onfiguring des Citrix ADC zum Generieren von SNMPv1- und SNMPv2-Traps.

Häufig gestellte Fragen

Betrachten Sie ein Beispiel für ein Hochverfügbarkeitssetup von zwei Citrix ADC Appliances NS-1 und NS-2 im Nicht-INC-Modus. Die maximale Anzahl von Flips und die maximale Flip-Zeit in beiden Knoten wurden mit den gleichen Werten festgelegt.

In der folgenden Tabelle sind die in diesem Beispiel verwendeten Einstellungen aufgeführt:

Entität	Detail
IP-Adresse von NS-1	10.102.173.211
IP-Adresse von NS-2	10.102.173.212
Maximale Anzahl von Flips	2
Maximale Flip-Zeit	200

Informationen über die maximale Anzahl von Flips und die maximale Drehzeiteinstellungenfinden Sie in der PDF-Datei.

Konfigurieren des Failover-Schnittstellensatzes

October 5, 2021

Ein Failover Interface Set (FIS) ist eine logische Gruppe von Schnittstellen. In einer HA-Konfiguration ist die Verwendung einer FIS eine Möglichkeit, Failover zu verhindern, indem Schnittstellen gruppiert

werden, sodass bei einem Ausfall einer Schnittstelle noch andere funktionierende Schnittstellen verfügbar sind. Eine FIS kann auch für die Knoten eines Citrix ADC Clusters konfiguriert werden.

HA-MON-Schnittstellen, die nicht an eine FIS gebunden sind, werden als Critical Interfaces (CI) bezeichnet, da ein Failover ausgelöst wird.

> **Hinweis**:
>
> Eine FIS erstellt keine aktive und Standby-Konfiguration. Es verhindert auch nicht, dass Schleifen überbrückt werden, wenn Verbindungen mit demselben VLAN verbunden werden.

FIS erstellen oder ändern

So fügen Sie eine FIS hinzu und binden Schnittstellen dazu über die Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `add fis <name>`
- `bind fis \<name\> \<ifnum\> ...`
- `show fis \<name\>`

Beispiel

```
1 > add fis fis1
2  Done
3 > bind fis fis1 1/3 1/5
4  Done
5 <!--NeedCopy-->
```

Eine ungebundene Schnittstelle wird zu einer kritischen Schnittstelle (CI), wenn sie aktiviert ist und HA MON eingeschaltet ist.

So heben Sie die Bindung einer Schnittstelle von einer FIS mit der Befehlszeilenschnittstelle auf

Geben Sie an der Eingabeaufforderung Folgendes ein:

- `unbind fis \<name\> \<ifnum\> ...`
- `show fis \<name\>`

Beispiel

```
1 > unbind fis fis1 1/3
2  Done
3 <!--NeedCopy-->
```


So konfigurieren Sie eine FIS mit der GUI

Navigieren Sie zu System > Hochverfügbarkeit, und fügen Sie auf der Registerkarte Failover-Schnittstellensatz eine neue FIS hinzu, oder bearbeiten Sie eine vorhandene FIS.

Entfernen einer FIS

Wenn die FIS entfernt wird, werden ihre Schnittstellen als kritische Schnittstellen markiert.

So entfernen Sie eine FIS mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
rm fis <name>
```

Beispiel

```
1 > rm fis fis1
2   Done
3 <!--NeedCopy-->
```

So entfernen Sie eine FIS mit der GUI

Navigieren Sie zu **System** > **Hochverfügbarkeit**, und löschen Sie auf der Registerkarte **Failover-Schnittstellensatz** die FIS.

Die Ursachen von Failover verstehen

October 5, 2021

Die folgenden Ereignisse können zu Failover in einer Hochverfügbarkeitskonfiguration führen:

1. Wenn der sekundäre Knoten für einen Zeitraum kein Heartbeat-Paket vom Primär erhält, der das tote Intervall überschreitet, das auf der Sekundarstufe festgelegt ist. (Siehe Anmerkung 1.)
2. Der primäre Knoten erlebt einen Hardwarefehler seiner SSL-Karte.
3. Der primäre Knoten erhält drei Sekunden lang keine Heartbeat-Pakete auf seinen Netzwerkschnittstellen.
4. Auf dem primären Knoten schlägt eine Netzwerkschnittstelle fehl, die nicht Teil eines Failover Interface Sets (FIS) oder eines Link Aggregation (LA) -Kanals ist und der HA-Monitor (HAMON) aktiviert ist. (Siehe Anmerkung 2.)

5. Auf dem primären Knoten schlagen alle Schnittstellen in einem FIS fehl. (Siehe Anmerkung 2.)
6. Auf dem primären Knoten schlägt ein LA-Kanal mit aktiviertem HAMON fehl. (Siehe Anmerkung 2.)
7. Auf dem primären Knoten schlagen alle Schnittstellen fehl (siehe Anmerkung 2). In diesem Fall tritt ein Failover unabhängig von der HAMON-Konfiguration auf.
8. Auf dem primären Knoten sind alle Schnittstellen manuell deaktiviert. In diesem Fall tritt ein Failover unabhängig von der HAMON-Konfiguration auf.
9. Sie erzwingen ein Failover, indem Sie den Befehl Force Failover auf beiden Knoten ausgeben.
10. Ein Routenmonitor, der an den primären Knoten gebunden ist, geht DOWN.

> **Hinweis 1:**
>
> Weitere Informationen zum Einstellen des Totintervalls finden Sie unter Konfigurieren der Kommunikationsintervalle. Mögliche Ursachen für einen Knoten, der keine Heartbeat-Pakete von einem Peer-Knoten empfängt, sind:
>
> - Ein Netzwerkkonfigurationsproblem verhindert, dass Heartbeats das Netzwerk zwischen den HA-Knoten durchqueren.
> - Der Peer-Knoten kommt es zu einem Hardware- oder Softwarefehler, der dazu führt, dass er einfriert (hängt), neu startet oder anderweitig die Verarbeitung und Weiterleitung von Heartbeat-Paketen stoppt.
>
> **Hinweis 2:**
>
> In diesem Fall bedeutet Fail, dass die Schnittstelle aktiviert wurde, aber in den DOWN-Status wechselt, wie aus dem Befehl show interface oder aus der GUI hervorgeht. Mögliche Ursachen für eine aktivierte Schnittstelle im Zustand DOWN sind LINK DOWN und TXSTALL.

Failover für Knoten erzwingen

October 5, 2021

Sie können ein Failover erzwingen, wenn Sie beispielsweise den primären Knoten ersetzen oder aktualisieren müssen. Sie können das Failover entweder vom primären oder vom sekundären Knoten erzwingen. Ein erzwungenes Failover wird nicht propagiert oder synchronisiert. Um den Synchronisierungsstatus nach einem erzwungenen Failover anzuzeigen, können Sie den Status des Knotens anzeigen.

Ein erzwungenes Failover schlägt unter folgenden Umständen fehl:

- Sie erzwingen ein Failover auf einem eigenständigen System.
- Der sekundäre Knoten ist deaktiviert.
- Der sekundäre Knoten ist so konfiguriert, dass er sekundär bleibt.

Die Citrix ADC Appliance zeigt eine Warnmeldung an, wenn beim Ausführen des Befehls Failover erzwingen ein potenzielles Problem festgestellt wird. Die Nachricht enthält die Informationen, die die Warnung ausgelöst haben, und fordert eine Bestätigung an, bevor Sie fortfahren.

Sie können ein Failover auf einem primären Knoten, einem sekundären Knoten und bei Knoten im Listenmodus erzwingen.

- **Erzwingen eines Failovers auf dem primären Knoten**.

  Wenn Sie das Failover auf dem primären Knoten erzwingen, wird der primäre und der sekundäre zum primären Knoten. Ein erzwungenes Failover ist nur möglich, wenn der primäre Knoten feststellen kann, dass der sekundäre Knoten UP ist.

  Wenn der sekundäre Knoten DOWN ist, gibt der Befehl Failover erzwingen die folgende Fehlermeldung zurück: “Operation aufgrund ungültiger Peer-Status nicht möglich. Behebung und Wiederholen.”

  Wenn sich das sekundäre System im Anspruchs-Status befindet oder inaktiv ist, wird die folgende Fehlermeldung zurückgegeben:

  ```
  Operation not possible now. Please wait for the system to stabilize
  before retrying.
  ```

- **Erzwingen eines Failovers auf dem sekundären Knoten**.

  Wenn Sie den Befehl Failover erzwingen vom sekundären Knoten ausführen, wird der sekundäre Knoten primär und der primäre Knoten wird sekundär. Ein Force-Failover kann nur auftreten, wenn der Zustand des sekundären Knotens gut ist und nicht so konfiguriert ist, dass er sekundär bleibt.

  Wenn der sekundäre Knoten nicht zum primären Knoten werden kann oder wenn der sekundäre Knoten so konfiguriert wurde, dass er sekundär bleibt (mit der Option STAYSECONDARY), zeigt der Knoten die folgende Fehlermeldung an:

  ```
  Operation not possible as my state is invalid. View the node for more
  information.
  ```

- **Failover erzwingen, wenn sich Knoten im Listenmodus befinden**.

  Wenn auf den beiden Knoten eines HA-Paares verschiedene Versionen der Systemsoftware ausgeführt werden, wechselt der Knoten, auf dem die höhere Version ausgeführt wird, in den Abhörmodus. In diesem Modus funktioniert weder die Befehlsausbreitung noch die Synchronisierung.

  Bevor Sie die Systemsoftware auf beiden Knoten aktualisieren, testen Sie die neue Version auf einem der Knoten. Um dies zu tun, müssen Sie ein Failover auf dem System erzwingen, das bereits aktualisiert wurde. Das aktualisierte System übernimmt dann als primärer Knoten,

aber weder die Befehlsausbreitung noch die Synchronisierung erfolgt. Außerdem müssen alle Verbindungen wiederhergestellt werden.

> **Wichtig!**
>
> Wenn Sie ein Failover erzwingen, wenn ein HA-Synchronisationsvorgang ausgeführt wird, gehen möglicherweise einige aktive Datensitzungen im HA-Setup verloren. Warten Sie also, bis der HA-Synchronisationsvorgang abgeschlossen ist, bevor Sie den Force-Failover-Vorgang ausführen.

So erzwingen Sie Failover auf einem Knoten mithilfe der Befehlszeilenschnittstelle:

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
force HA failover
```

So erzwingen Sie Failover auf einem Knoten über die grafische Benutzeroberfläche:

Navigieren Sie zu **System** > **Hochverfügbarkeit**, und wählen Sie auf der Registerkarte **Knoten** den Knoten aus, wählen Sie in der Liste Aktion die Option **Failover erzwingen** aus.

Erzwingen des sekundären Knotens, sekundär zu bleiben

October 5, 2021

In einem HA-Setup kann der sekundäre Knoten gezwungen werden, unabhängig vom Status des primären Knotens sekundär zu bleiben.

Angenommen, der primäre Knoten muss aktualisiert werden und der Prozess dauert einige Sekunden. Während des Upgrades wird der primäre Knoten möglicherweise einige Sekunden lang heruntergefahren, aber Sie möchten nicht, dass der sekundäre Knoten übernommen wird. Sie möchten, dass er der sekundäre Knoten bleibt, selbst wenn er einen Fehler im primären Knoten erkennt.

Wenn Sie den sekundären Knoten zwingen, sekundär zu bleiben, bleibt er auch dann sekundär, wenn der primäre Knoten ausfällt. Wenn Sie erzwingen, dass der Status eines Knotens in einem HA-Paar sekundär bleibt, nimmt er nicht an Übergängen des HA-Zustands der Maschine teil. Der Status des Knotens wird als STAYSECONDARY angezeigt.

Das Erzwingen des Knotens, sekundär zu bleiben, funktioniert sowohl auf eigenständigen als auch auf sekundären Knoten. Auf einem eigenständigen Knoten müssen Sie diese Option verwenden, bevor Sie einen Knoten zum Erstellen eines HA-Paares hinzufügen können. Wenn Sie den neuen Knoten hinzufügen, stoppt der vorhandene Knoten die Verarbeitung von Datenverkehr und wird zum sekundären Knoten. Der neue Knoten wird zum primären Knoten.

> **Hinweis**:
>
> Wenn Sie ein System zwingen, sekundär zu bleiben, wird der erzwungene Prozess weder

> propagiert noch synchronisiert. Es betrifft nur den Knoten, auf dem Sie den Befehl ausführen.

So zwingen Sie, dass der sekundäre Knoten mit der Befehlszeilenschnittstelle sekundär bleibt

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ha node -hastatus STAYSECONDARY
```

So zwingen Sie, dass der sekundäre Knoten mit der GUI sekundär bleibt

Navigieren Sie zu **System** > **Hochverfügbarkeit**, öffnen Sie auf der Registerkarte **Knoten** den lokalen Knoten, und wählen Sie **STAY SECONDARY**.

Erzwingen des primären Knotens, primär zu bleiben

October 5, 2021

In einem HA-Setup können Sie erzwingen, dass ein gesunder Primärknoten auch nach einem Failover primär bleibt. Sie können diese Option entweder auf einem primären Knoten in einem HA-Paar aktivieren. Mit dieser Option kann sich der primäre Knoten im Primärzustand befinden, solange er gesund ist.

Auf einem eigenständigen Knoten müssen Sie diese Option verwenden, bevor Sie einen Knoten zum Erstellen eines HA-Paares hinzufügen können. Wenn Sie den neuen Knoten hinzufügen, funktioniert der vorhandene Knoten weiterhin als primärer Knoten, und der neue Knoten wird zum sekundären Knoten.

So zwingen Sie, dass der primäre Knoten mit der Befehlszeilenschnittstelle primär bleibt

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
set ha node -hastatus STAYPRIMARY
```

So zwingen Sie, dass der primäre Knoten mit der GUI primär bleibt

Navigieren Sie zu **System** > **Hochverfügbarkeit**, öffnen Sie auf der Registerkarte **Knoten** den lokalen Knoten, und wählen Sie **STAY PRIMARY** .

Grundlegendes zur Berechnung der Hochverfügbarkeitsprüfung

October 5, 2021

In der folgenden Tabelle werden die in einer Zustandskontrolle untersuchten Faktoren zusammengefasst:

- Status der Failover-Schnittstellensätze
- Zustand der kritischen Schnittstellen
- Status der Routenüberwachung

In der folgenden Tabelle wird die Berechnung der Zustandsprüfung zusammengefasst.

Failover-Schnittstellensätze	Kritische Schnittstellen	Routenüberwachung	Bedingung
N	J	N	Wenn das System über kritische Schnittstellen verfügt, müssen alle diese kritischen Schnittstellen UP sein.
J	J	N	Wenn das System über Failover-Schnittstellensätze verfügt, müssen alle diese Failover-Schnittstellensätze UP sein.
J	J	J	Wenn auf dem System Routenmonitore konfiguriert sind, müssen alle überwachten Routen im Failover-Schnittstellensatz vorhanden sein.

Häufig gestellte Fragen zur Hochverfügbarkeit

October 5, 2021

1. Welche Ports werden verwendet, um die HA-bezogenen Informationen zwischen den Knoten in einer HA-Konfiguration auszutauschen?

   In einer HA-Konfiguration verwenden beide Knoten die folgenden Ports, um Informationen für HA auszutauschen:

   - UDP-Port 3003, um Heartbeat-Pakete auszutauschen.
   - Port 3010, für Synchronisation und Befehlsausbreitung.

2. Was sind die Bedingungen, die die Synchronisation auslösen?

   Die Synchronisierung wird durch eine der folgenden Bedingungen ausgelöst:

   - Die Inkarnationsnummer des primären Knotens, der vom sekundären empfangen wird, stimmt nicht mit der des sekundären Knotens überein.
     Hinweis: Beide Knoten in einer HA-Konfiguration behalten einen Leistungsindikator namens
     Inkarnationsnummer, der die Anzahl der Konfigurationen in der Konfigurationsdatei des Knotens zählt. Jeder Knoten sendet seine Inkarnationsnummer an jeden anderen Knoten in den Heartbeat-Nachrichten. Die Inkarnationsnummer wird für die folgenden Befehle nicht erhöht:
     a) Alle HA-Konfigurationsbefehle. Fügen Sie beispielsweise ha-Knoten hinzu, setzen Sie ha-Knoten und binden Sie ha-Knoten.
     b) Alle Interface-bezogenen Befehle. Zum Beispiel, setzen Sie Schnittstelle und unset interface.
     c) Alle kanalbezogenen Befehle. Fügen Sie beispielsweise Kanal hinzu, setzen Sie den Kanal ein und binden Sie den Kanal ein.
   - Der sekundäre Knoten wird nach einem Neustart angezeigt.
   - Der primäre Knoten wird nach einem Failover sekundär.

3. Welche Konfigurationen werden in einer HA-Konfiguration im INC- oder Nicht-INC-Modus nicht synchronisiert oder weitergegeben?

   Die folgenden Befehle werden weder propagiert noch mit dem sekundären Knoten synchronisiert:

   - Alle knotenspezifischen HA-Konfigurationsbefehle. Fügen Sie beispielsweise ha-Knoten hinzu, setzen Sie ha-Knoten und binden Sie ha-Knoten.
   - Alle Interface-bezogenen Konfigurationsbefehle. Zum Beispiel, setzen Sie Schnittstelle und unset interface.

- Alle kanalbezogenen Konfigurationsbefehle. Fügen Sie beispielsweise Kanal hinzu, setzen Sie den Kanal ein und binden Sie den Kanal ein.

> **Hinweis:**
>
> Die folgenden Konfigurationen werden weder im HA im INC-Modus synchronisiert noch weitergegeben. Jeder Knoten hat seinen eigenen:
>
> ```
> 1 - SNIPs
> ```
>
> - VLANs
> - Routen (außer LLB-Routen)
> - Routenüberwachung
> - RNAT Regeln (außer RNAT Regel mit VIP als NAT IP)
> - Dynamische Routing-Konfigurationen
> - Netzprofile

4. Wird eine dem sekundären Knoten hinzugefügte Konfiguration auf dem primären Knoten synchronisiert?

   Nein, eine dem sekundären Knoten hinzugefügte Konfiguration wird nicht mit dem primären Knoten synchronisiert.

5. Was könnte der Grund dafür sein, dass beide Knoten die primäre in einer HA-Konfiguration sein?

   Der wahrscheinlichste Grund ist, dass der primäre und sekundäre Knoten beide fehlerfrei sind, aber der sekundäre nicht die Heartbeat-Pakete vom primären erhalten. Das Problem könnte mit dem Netzwerk zwischen den Knoten liegen.

6. Steht bei einer HA-Konfiguration Probleme auf, wenn Sie die beiden Knoten mit unterschiedlichen Systemtakteinstellungen bereitstellen?

   Unterschiedliche Systemtakteinstellungen auf den beiden Knoten können folgende Probleme verursachen:

   - Die Zeitstempel in den Protokolldateieinträgen stimmen nicht überein. Diese Situation macht es schwierig, die Protokolleinträge auf Probleme zu analysieren.
   - Nach einem Failover können Probleme mit jeder Art von Cookie-basierte Persistenz für den Lastenausgleich auftreten. Ein signifikanter Unterschied zwischen den Zeiten kann dazu führen, dass ein Cookie früher als erwartet abläuft, was zur Beendigung der Persistenzsitzung führt.
   - Ähnliche Überlegungen gelten für zeitbezogene Entscheidungen auf den Knoten.

7. Wie lauten die Bedingungen für den Ausfall des *force HA sync-Befehls* ?

   Die erzwungene Synchronisierung schlägt unter folgenden Umständen fehl:

- Sie erzwingen die Synchronisierung, wenn die Synchronisation bereits ausgeführt wird.
- Sie erzwingen die Synchronisierung auf einer eigenständigen Citrix ADC Appliance.
- Der sekundäre Knoten ist deaktiviert.
- HA-Synchronisierung ist auf dem aktuellen sekundären Knoten deaktiviert.
- Die HA-Propagierung ist auf dem aktuellen primären Knoten deaktiviert, und Sie erzwingen die Synchronisierung vom primären Knoten.

8. Wie lauten die Bedingungen für den Ausfall des Befehls " *HA files sync* "?

   Das Synchronisieren von Konfigurationsdateien schlägt in einem der folgenden Situationen fehl:

   - Auf einem eigenständigen System.
   - Der sekundäre Knoten ist deaktiviert.

9. Wenn der sekundäre Knoten in einer HA-Konfiguration als primärer Knoten übernimmt, wechselt er in den sekundären Status zurück, wenn der ursprüngliche primäre Knoten wieder online ist?

   Nein. Nachdem der sekundäre Knoten als primärer Knoten übernommen hat, bleibt er auch dann als primär, wenn der ursprüngliche primäre Knoten wieder online ist. Führen Sie zum Austausch des primären und sekundären Status der Knoten den Befehl *force failover* aus.

10. Was sind die Bedingungen für den Ausfall des Force-Failover-Befehls?

    Ein erzwungenes Failover schlägt unter folgenden Umständen fehl:

    - Sie erzwingen ein Failover auf einem eigenständigen System.
    - Der sekundäre Knoten ist deaktiviert.
    - Der sekundäre Knoten ist so konfiguriert, dass er sekundär bleibt.
    - Der primäre Knoten ist so konfiguriert, dass er primär bleibt.
    - Der Status des Peer-Knotens ist unbekannt.

Beheben von Problemen mit hoher Verfügbarkeit

October 5, 2021

Die häufigsten Probleme mit der Hochverfügbarkeit beinhalten, dass die Hochverfügbarkeitsfunktion überhaupt nicht funktioniert oder nur zeitweise funktioniert. Im Folgenden finden Sie häufige Probleme mit hoher Verfügbarkeit sowie wahrscheinliche Ursachen und Lösungen.

- **Problem**
  Die Unfähigkeit der Citrix ADC-Appliances, die Citrix ADC-Appliances in einem Hochverfügbarkeitssetup zu koppeln.

- **Ursache**
  Netzwerkkonnektivität
  Lösung
  Stellen Sie sicher, dass beide Appliances mit dem Switch verbunden sind und die Schnittstellen aktiviert sind.
- **Ursache**
  Nichtübereinstimmung im Kennwort für das standardmäßige Administratorkonto
  Lösung
  Stellen Sie sicher, dass das Kennwort auf beiden Appliances identisch ist.
- **Ursache**
  IP-Konflikt
  Lösung
  Stellen Sie sicher, dass beide Appliances über eine eindeutige Citrix ADC IP-Adresse (NSIP) verfügen. Die Appliances sollten nicht dieselbe NSIP-Adresse haben.
- **Ursache**
  Knoten-ID stimmt nicht überein
  Lösung
  Stellen Sie sicher, dass die Knoten-ID-Konfiguration auf beiden Appliances eindeutig ist. Die Appliances sollten nicht über dieselbe Node-ID-Konfiguration verfügen. Darüber hinaus müssen Sie Wert für eine Node-ID zwischen 1 und 64 zuweisen.
- **Ursache**
  Nichtübereinstimmung im Kennwort des RPC-Knotens
  Lösung
  Stellen Sie sicher, dass beide Knoten das gleiche RPC-Knotenkennwort haben.
- **Ursache**
  Ein Administrator hat den entfernten Knoten deaktiviert.
  Lösung
  Aktivieren Sie den entfernten Knoten.
- **Ursache**
  Die Firewall-Anwendung hat die Heartbeat-Pakete blockiert
  Lösung

Stellen Sie sicher, dass der UDP-Port 3003 zulässig ist.

- **Problem**
  Beide Appliances behaupten, die primäre Appliance zu sein.
  - **Ursache**
    Fehlende Heartbeat-Pakete zwischen den Appliances
    Lösung
    Stellen Sie sicher, dass der UDP-Port 3003 für die Kommunikation zwischen den Appliances nicht blockiert ist.

- **Problem**
  Die Citrix ADC Appliance kann die Konfiguration nicht synchronisieren.
  - **Ursache**
    Eine Firewall-Anwendung blockiert den erforderlichen Port.
    Lösung
    Stellen Sie sicher, dass der UDP-Port 3010 (oder UDP-Port 3008 mit sicherer Synchronisation) für die Kommunikation zwischen den Appliances nicht blockiert ist.
  - **Ursache**
    Ein Administrator hat die Synchronisierung deaktiviert.
    Lösung
    Aktivieren Sie die Synchronisierung auf der Appliance, die das Problem hat.
  - **Ursache**
    Verschiedene Citrix ADC Versionen oder Builds werden auf Appliances installiert.
    Lösung
    Aktualisieren Sie die Appliances auf dieselbe Citrix ADC Version oder denselben Build.
- Die Propagierung von**Issue**
  Command schlägt zwischen den Appliances fehl.
  - **Ursache**
    Eine Firewall-Anwendung blockiert den Port.
    Lösung
    Stellen Sie sicher, dass der UDP-Port 3011 (oder UDP-Port 3009 mit sicherer Propagierung) für die Kommunikation zwischen den Appliances nicht blockiert ist.
  - **Ursache**
    Ein Administrator hat die Befehlspropagierung deaktiviert.
    Lösung
    Aktivieren Sie die Befehlspropagierung auf der Appliance, die das Problem hat.
  - **Ursache**
    Verschiedene Citrix ADC Versionen oder Builds werden auf Appliances installiert.
    Lösung
    Aktualisieren Sie die Appliances auf dieselbe Citrix ADC Version oder denselben Build.
- **Problem**
  Die Citrix ADC Appliances im Hochverfügbarkeitspaar können den Erzwungen-Failover-Prozess nicht ausführen.
  - **Ursache**
    Der sekundäre Knoten ist deaktiviert.
    Lösung
    Aktivieren Sie den sekundären Knoten.
  - **Ursache**
    Der sekundäre Knoten ist so konfiguriert, dass er sekundär bleibt.

Lösung

Legen Sie den sekundären Hochverfügbarkeitsstatus des sekundären Knotens auf Aktivieren von Sekundär bleiben fest.

- **Problem**

  Die sekundäre Appliance empfängt nach dem Failover-Prozess keinen Datenverkehr.

  - **Ursache**

    Der Upstream-Router versteht GARP-Nachrichten der Citrix ADC Appliance nicht.

    Lösung

    Konfigurieren Sie die virtuelle MAC-Adresse auf der sekundären Appliance.

Verwalten von Heartbeat-Meldungen mit hoher Verfügbarkeit auf einer Citrix ADC Appliance

September 1, 2022

Die beiden Knoten in einer Hochverfügbarkeitskonfiguration senden und empfangen auf allen aktivierten Schnittstellen Heartbeat-Meldungen zueinander und voneinander. Die Heartbeat-Meldungen fließen unabhängig von der HA MON-Einstellung auf diesen Schnittstellen. Wenn NSVLAN oder beide (NSVLAN und SYNC) auf einer Appliance konfiguriert sind, fließen die Heartbeat-Nachrichten nur über die aktivierten Schnittstellen, die Teil von NSVLAN und SYNCVLAN sind.

Wenn ein Knoten die Heartbeat-Meldungen auf einer aktivierten Schnittstelle nicht empfängt, sendet er kritische Warnungen an die angegebenen SNMP-Manager. Diese kritischen Warnungen geben Fehlalarme aus und ziehen unnötige Aufmerksamkeit der Administratoren auf Schnittstellen, die nicht als Teil der Verbindungen zum Peer-Knoten konfiguriert sind.

Um dieses Problem zu beheben, wird die HAHeartbeat-Option für Schnittstellen und Kanäle verwendet, um den HA-Heartbeat-Nachrichtenfluss auf diesen zu aktivieren oder zu deaktivieren.

So verwalten Sie die Hochverfügbarkeits-Heartbeat-Meldungen auf einer Schnittstelle mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

- `set interface <ID> [-HAHeartBeat ( ON | OFF )]`
- `show interface <ID>`

So verwalten Sie die Hochverfügbarkeits-Heartbeat-Meldungen auf einem Kanal mithilfe der Befehlszeilenschnittstelle

Geben Sie in der Befehlszeile Folgendes ein:

- `set channel <ID> [-HAHeartBeat ( ON | OFF )]`
- `show channel <ID>`

So verwalten Sie die Hochverfügbarkeits-Heartbeat-Meldungen für eine Schnittstelle über die GUI

1. Navigieren Sie zu **System** > **Netzwerk** > **Schnittstellen**.
2. Aktivieren oder deaktivieren Sie den **HA-Heart-Beat-Parameter** .

So verwalten Sie die Hochverfügbarkeits-Heartbeat-Meldungen auf einem Kanal über die GUI

1. Navigieren Sie zu **System** > **Netzwerk** > **Kanäle**.
2. Aktivieren oder deaktivieren Sie den **HA-Heart-Beat-Parameter** .

Entfernen und Ersetzen eines Citrix ADC in einem Hochverfügbarkeit-Setup

October 5, 2021

Dieser Artikel hilft Ihnen mit RMA-Ersetzungen. Außerdem enthält dieser Artikel Anweisungen zum Sichern von Konfigurationen, zum Upgrade oder Downgrade der gelieferten Softwareversion und zum Einrichten des RPC-Kennworts auf ADC.

Zu berücksichtigende Punkte

Die folgenden Konfigurationen werden nicht in einer Hochverfügbarkeitskonfiguration im INC-Modus (Independent Network Configuration) oder Nicht-INC-Modus synchronisiert oder weitergegeben:

- Alle knotenspezifischen HA-Konfigurationsbefehle. Fügen Sie beispielsweise ha-Knoten hinzu, setzen Sie ha-Knoten und binden Sie ha-Knoten.
- Alle Interface-bezogenen Konfigurationsbefehle. Zum Beispiel, setzen Sie Schnittstelle und unset interface.
- Alle kanalbezogenen Konfigurationsbefehle. Fügen Sie beispielsweise Kanal hinzu, setzen Sie den Kanal ein und binden Sie den Kanal ein.
- Alle Konfigurationsbefehle für die Schnittstelle HA-Überwachung.

Die folgenden Konfigurationen werden in einer HA-Konfiguration im INC-Modus (Unabhängige Netzwerkkonfiguration) weder synchronisiert noch weitergegeben:

- SNIPs
- VLANs
- Routen (außer LLB-Routen)
- Routenüberwachung
- RNAT Regeln (außer RNAT Regel mit VIP als NAT IP)
- Dynamische Routing-Konfigurationen

Anweisungen

Führen Sie die folgenden Schritte aus, um einen Citrix ADC in Hochverfügbarkeit-Setup zu ersetzen:

- Entfernen eines sekundären Active Citrix ADC Knotens
- Konfigurieren des sekundären Ersatzknotens
- Überprüfen und Aktualisieren der Software auf Ersatz-ADC
- Kennwort für neu sekundär auf primäre Übereinstimmung festlegen
- Hinzufügen von Lizenzen zum Ersatz-ADC
- HA-Paar zwischen primären und neuem sekundären Knoten erstellen

Entfernen eines aktiven sekundären Knotens

1. Melden Sie sich bei beiden ADCs an und führen Sie den folgenden Befehl aus, um zu bestätigen, welcher Knoten primär ist und welcher Knoten sekundär ist:

```
show ha node
<!--NeedCopy-->
```

2. Melden Sie sich am primären ADC an, sichern Sie die Konfigurationen auf dem primären Knoten, und kopieren Sie die Dateien vor den Änderungen aus dem ADC. Diese Dateien befinden sich im Verzeichnis /var /ns_sys_backup/.

   Führen Sie die folgenden Schritte aus:

   a) Speichern Sie die ADC-Ausführungskonfigurationen im Arbeitsspeicher:

```
save ns config
<!--NeedCopy-->
```

   b) Erstellen Sie das vollständige Backupdateipaket:

```
create system backup -level full
<!--NeedCopy-->
```

   c) Erstellen Sie das grundlegende Backupdateipaket:

```
create system backup -level basic
<!--NeedCopy-->
```


3. Nachdem alle Backupdateien generiert wurden, müssen Sie sie vom Gerät kopieren, bevor Sie fortfahren.

   Öffnen Sie von einem Windows-Terminal eine Eingabeaufforderung und kopieren Sie die Backupdateien vom ADC auf die lokale Festplatte. Dies kann mit dem folgenden Befehl erfolgen:

```
pscp <username>@<NSIP>:<Target file source>  <Target file
   destination>
<!--NeedCopy-->
```

   Beispiel:

```
pscp nsroot@10.125.245.78:/var/ns_sys_backup/backup_basic_10
   .125.245.78_2016_09_14_15_08.tgz c:\nsbackup\backup_basic_10
   .125.245.78_2016_09_14_15_08.tgz
<!--NeedCopy-->
```

   Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort für das angegebene Administratorkonto ein und drücken Sie dann die Eingabetaste. Wiederholen Sie diese Schritte, bis alle Backuppakete auf den lokalen PC kopiert werden, bevor Sie fortfahren.

4. SSH in den sekundären ADC, und stellen Sie das Gerät auf den Status STAYSECONDARY. Dadurch wird die Einheit gezwungen, die primäre Rolle im Falle eines erkannten Fehlers während des Austauschs nicht zu übernehmen. Stellen Sie sicher, dass Sie mit dem sekundären ADC verbunden sind, bevor Sie diesen Schritt ausführen

```
set ha node  -haStatus <state>
set ha node  -haStatus STAYSECONDARY
<!--NeedCopy-->
```

5. Sobald der **Knotenstatus** des sekundären ADC erfolgreich STAYSECONDARY angezeigt wird, wechseln Sie zum primären ADC, löschen Sie den sekundären Knoten, und führen Sie den folgenden Befehl aus:

```
save ns config
<!--NeedCopy-->
```

   Führen Sie die folgenden Befehle aus, während Sie am primären ADC angemeldet sind

a) Führen Sie den folgenden Befehl aus, um zu ermitteln, welcher numerische Wert den sekundären HA-Knoten darstellt:

```
1 show ha node
2 <!--NeedCopy-->
```

b) Führen Sie den folgenden Befehl aus, um den sekundären ADC aus dem primären HA-Paar zu entfernen.

```
1 rm ha node <node ID>
2 <!--NeedCopy-->
```

c) Führen Sie den folgenden Befehl aus, um die Konfiguration zu speichern:

```
1 save ns config
2 <!--NeedCopy-->
```

d) Wenn der sekundäre ADC nun entfernt ist, wird der sekundäre ADC aus dem Netzwerk heruntergefahren, getrennt und entfernt.

Hinweis. Achten Sie darauf, alle Verbindungen zu beschriften, bevor Sie die Verbindung trennen.

Konfigurieren des sekundären Ersatzknotens

1. Schalten Sie das neue Gerät mit dem Ersatz-ADC ein. Schließen Sie die Netzwerkverbindungen an diesem Punkt NICHT an.
2. Wenn der Start abgeschlossen ist, verwenden Sie den Konsolenport, um eine Verbindung mit dem ADC herzustellen, und konfigurieren Sie den NSIP, den Sie für die Verbindung mit dem Gerät verwenden.
3. Wenn Sie dazu aufgefordert werden, wählen Sie **4.**

   Hinweis. In diesem Beispiel verwenden wir einen anderen NSIP für den Ersatz ADC. Wenn Sie die IP der ursprünglichen sekundären Einheit verwenden möchten, können Sie sie auf dem Ersatz ändern, bevor Sie den neuen ADC an die primäre HA-Einheit binden.
4. Der ADC sollte nun gestartet werden. Verbinden Sie nun die Netzwerkschnittstelle, die für den Verwaltungsdatenverkehr verwendet wird, und bestätigen Sie, dass die IP-Adresse von Ihrem Netzwerk aus erreichbar ist.

Überprüfen und Aktualisieren der Software auf Ersatz-ADC

Bevor Sie die neue Einheit mit dem primären ADC synchronisieren, müssen wir sicherstellen, dass beide ADCs denselben Build ausführen.

1. Führen Sie den folgenden Befehl aus, um die Version auf ADC zu überprüfen:

```
show version
<!--NeedCopy-->
```

2. Erstellen Sie während des neuen sekundären ADC einen Unterordner in **/var**, der für das Upgrade verwendet werden soll.
3. Gehen Sie zu Citrix Downloads und laden Sie das entsprechende Paket herunter, das der Build-Version entspricht, die auf dem primären ADC ausgeführt wird.
4. Laden Sie die TGZ-Datei herunter und extrahieren Sie sie:

```
tar -xvzf ”file.tgz”
<!--NeedCopy-->
```

5. Kopieren Sie die extrahierten Dateien in den sekundären ADC. Öffnen Sie auf Ihrem Windows-Terminal eine Eingabeaufforderung und navigieren Sie zu dem Verzeichnis, das das extrahierte .tgz-Build-Paket enthält, und führen Sie den folgenden pscp-Befehl aus:

```
pscp <Target file source>  <username>@<NSIP>:<Target file
   destination>
<!--NeedCopy-->
```

   Beispiel:

```
C:\inetpub>pscp c:\inetpub\build-12.1-47.14_nc.tgz nsroot@10
   .20.245.80:/var/NS_upg_12.1_47.14/build-12.1-47.14_nc.tgz
<!--NeedCopy-->
```

6. Nachdem die Datei übertragen wurde, kehren Sie zum sekundären ADC zurück und aktualisieren Sie das Upgrade. Ausführliche Anweisungen finden Sie unter Upgrade einer Citrix ADX Standalone Appliance.
7. Sobald der neue sekundäre neu gestartet wurde, wird SSH wieder in das Gerät aufgenommen und bestätigt, dass das Upgrade erfolgreich ist und der Build dem des primären entspricht.

Kennwort für den sekundären Ersatzknoten so festlegen, dass er primär entspricht

Hinweis: Wenn Sie an dieser Stelle die Verwaltungs-IP-Adresse (NSIP) des neuen sekundären ADC ändern möchten, können Sie dies tun, bevor Sie fortfahren.

Ändern Sie das Kennwort auf dem neuen sekundären ADC so, dass es mit dem Kennwort übereinstimmt, das sich derzeit auf dem primären ADC befindet.

1. Stellen Sie sicher, dass das standardmäßige Administratorkontokennwort (nsroot) dem primären ADC entspricht. Dies geschieht mit dem folgenden Befehl, während Sie über SSH in der neuen sekundären Einheit angemeldet sind:

   ```
   set system user <user> <password>
   <!--NeedCopy-->
   ```

   Dieser Befehl set/setzt das Kennwort für den angegebenen Benutzer zurück.

2. SSH in den primären und neuen sekundären ADC und bestätigen, dass Kennwörter übereinstimmen.

Hinzufügen von Lizenzen zum sekundären Ersatzknoten

Wenn der neue ADC aktualisiert und bereit für die Kopplung ist, laden Sie die entsprechende Lizenzierung für den Ersatzknoten herunter und installieren Sie sie.

1. Navigieren Siehttps://www.citrix.com zu, um Lizenzen für das neue Ersatzgerät anzufordern und herunterzuladen.
2. Nachdem Sie alle entsprechenden Lizenzen heruntergeladen haben, geben Sie SSH in den neuen sekundären ADC ein, und geben Sie den folgenden Befehl ein, um den aktuellen Lizenzierungsstatus anzuzeigen:

   ```
   show license
   <!--NeedCopy-->
   ```

3. Von der Windows Terminal-Eingabeaufforderung müssen Sie nun die Lizenzdateien mit dem folgenden Befehl in den neuen sekundären ADC hochladen:

   Hinweis. Wenn Sie mehrere Lizenzen haben, wiederholen Sie diesen Schritt, bis alle Lizenzen hochgeladen sind.


```
pscp <Target file source>  <username>@<NSIP>:<Target file
   destination>
<!--NeedCopy-->
```

Beispiel:

```
C:\inetpub>pscp c:\inetpub\NS-VPX-3K-LIC-020030ad0024.lic
   nsroot@10.125.245.80:/nsconfig/license/NS-VPX-3K-LIC-020030
   ad0024.lic
<!--NeedCopy-->
```

4. SSH in den neuen sekundären ADC und führen einen Warm-Neustart mit dem folgenden Befehl durch:

```
reboot  -w
<!--NeedCopy-->
```

Nachdem das Gerät neu gestartet wurde, SSH in das Gerät und führen Sie den Befehl show license erneut aus. An dieser Stelle sollten die Lizenzen angewendet werden.

Hochverfügbarkeit zwischen primären und neuem sekundären Knoten einrichten

Zu diesem Zeitpunkt sind wir bereit, die Citrix ADC Einheiten zu einem Hochverfügbarkeitspaar zu verbinden. Weitere Informationen finden Sie unter Konfigurieren von Hochverfügbarkeit.

Wiederholungsversuche anfordern

December 3, 2021

Wenn eine Citrix ADC Appliance eine HTTP-Anforderung erhält, aber einen Verbindungsfehler mit einem Back-End-Server aufweist, verwendet die Appliance eine Wiederholungsanweisung. Die erneute Anfrage behebt Szenarien mit Verbindungsfehlern und ermöglicht es der Appliance, den nächsten verfügbaren Dienst auszuwählen und die Anforderung weiterzuleiten. Durch eine Neu-Anfrage kann der Client Roundtrip-Zeit (RTT) sparen.

Die Funktion “Wiederholung anfordern” ist für die folgenden Szenarien mit Verbindungsfehlern anwendbar:

- Wenn ein Backend-Server eine TCP-Verbindung zurücksetzt, wenn eine HTTP-Anfrage empfangen wird. Weitere Informationen finden Sie unter Wiederholungsversuche beantragen.
- Wenn ein Backend-Server während des Verbindungsaufbaus eine TCP-Verbindung zurücksetzt. Weitere Informationen finden Sie unter Wiederholungsversuche beantragen.
- Wenn eine Antwort von einem Back-End eine Zeitüberschreitung (basierend auf dem konfigurierten Timeoutwert), wenn eine Appliance eine HTTP-Anfrage sendet. Weitere Informationen finden Sie unter Wiederholungsversuche beantragen.

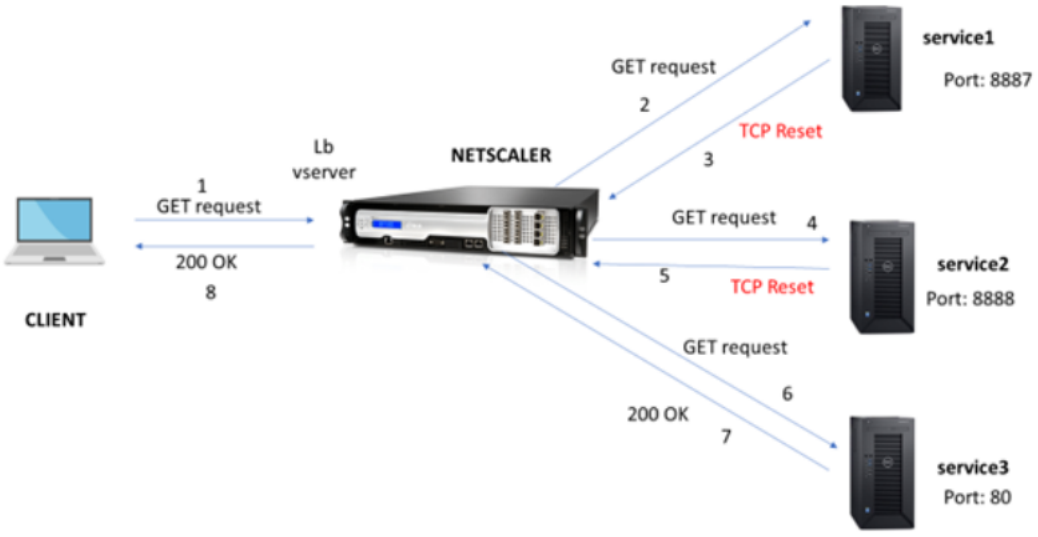
Wiederholungsversuche anfordern, wenn der Backend-Server die TCP-Verbindung zurücksetzt

October 5, 2021

Wenn ein Back-End-Server eine TCP-Verbindung zurücksetzt, leitet die Funktion zur Wiederholung der Anforderung die Anfrage an den nächsten verfügbaren Server weiter, anstatt den Reset an den Client zu senden. Durch den Reload-Balancing speichert der Client RTT, wenn die Appliance dieselbe Anfrage an den nächsten verfügbaren Dienst initiiert.

So funktioniert die Wiederholung der Anfrage, wenn der Backend-Server eine TCP-Verbindung zurücksetzt

Das folgende Diagramm zeigt, wie Komponenten miteinander interagieren.



1. Der Prozess beginnt mit der Aktivierung der Appqoe-Funktion auf Ihrer Appliance.

2. Wenn der Client eine HTTP- oder HTTPS-Anfrage sendet, sendet der virtuelle Lastausgleichsserver die Anfrage an den Back-End-Server.
3. Wenn der angeforderte Dienst nicht verfügbar ist, setzt der Back-End-Server die TCP-Verbindung zurück.
4. Wenn in der Appqoe-Konfiguration “Wiederholung” mit der gewünschten Anzahl von Wiederholungsversuchen aktiviert ist, verwendet der virtuelle Lastausgleichsserver den konfigurierten Load Balancing-Algorithmus, um die Anforderung an den nächsten verfügbaren Anwendungsserver weiterzuleiten.
5. Nachdem der virtuelle Lastausgleichsserver die Antwort erhalten hat, leitet die Appliance die Antwort an den Client weiter.
6. Wenn die verfügbaren Back-End-Server gleich oder kleiner als die Wiederholungsanzahl sind und wenn alle Server einen Reset senden, würde die Appliance einen internen 500-Serverfehler beantworten. Betrachten Sie ein Szenario mit fünf verfügbaren Servern und der Wiederholungsanzahl, die auf sechs festgelegt ist. Wenn alle fünf Server die Verbindung zurücksetzen, gibt die Appliance einen internen 500-Serverfehler an den Client zurück.
7. Wenn die Anzahl der Back-End-Server höher ist als die Wiederholungsanzahl und wenn die Back-End-Server die Verbindung zurücksetzen, leitet die Appliance den Reset an den Client weiter. Stellen Sie sich ein Szenario mit drei Back-End-Servern und der Wiederholungsanzahl vor, die auf zwei festgelegt ist. Wenn die drei Server die Verbindung zurücksetzen, sendet die Appliance eine Reset-Antwort an den Client.

Konfigurieren der Wiederholung der Anfrage für die GET-Methode

Um die Wiederholungsfunktion für die GET-Methode zu konfigurieren, müssen Sie die folgenden Schritte ausführen.

1. Aktivieren Sie AppQoE
2. Add AppQoE action
3. Add AppQoE policy
4. Binden Sie die AppQoE -Richtlinie an den virtuellen Server mit Lastenausgleich

Aktivieren Sie AppQoE

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns feature appqoe
```

Add AppQoE action

Sie müssen eine AppQoE-Aktion konfigurieren, um anzugeben, ob die Appliance nach einem TCP-Reset und die Anzahl der Wiederholungsversuche erneut versucht werden soll.


```
add appqoe action reset_action -retryOnReset ( YES | NO )-numretries <
positive_integer>]
```

Beispiel:

```
add appqoe action reset_action -retryOnReset YES -numretries 5
```

Wo,
RetryonReset. Aktivieren Sie “Wiederholen”, wenn der Back-End-Server eine TCP-Verbindung zurücksetzt.
numretries. Wiederholte Anzahl.

Add AppQoE policy

Um AppQoE zu implementieren, müssen Sie die AppQoE-Richtlinie konfigurieren, um eingehende HTTP- oder SSL-Anfragen in einer bestimmten Warteschlange zu priorisieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add appqoe policy <name> -rule <expression> -action <string>
```

Beispiel:

```
add appqoe policy reset_policy -rule http.req.method.eq(get)-action reset_action
```

Binden Sie die Appqoe-Richtlinie an den virtuellen Server mit Lastenausgleich

Wenn ein Backend-Server eine TCP-Paketanforderung zurücksetzt und der virtuelle Lastausgleichsserver die Anforderung an den nächsten verfügbaren Dienst weiterleiten soll, müssen Sie den virtuellen Lastausgleichsserver an die AppQoE-Richtlinie binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name> ((<serviceName> (-policyName <string> [-priority <
positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST
| RESPONSE )]
```

Beispiel:

```
bind lb vserver v1 -policyName reset_policy -type REQUEST -priority 1
```

Konfigurieren der Wiederholung der Anfrage für POST-Anfragen

Sie müssen immer Vorsicht walten lassen, wenn Sie Kontostandsanforderungen neu laden, die Daten in den Backend-Server schreiben. Stellen Sie bei solchen Anfragen sicher, dass die Inhaltslänge kurz ist. Wenn die Inhaltslänge lang ist, kann dies zum Ressourcenverbrauch führen. Befolgen Sie die unten angegebenen Schritte, um den Reload-Balancing für POST-Anfragen zu konfigurieren.

1. Aktivieren Sie AppQoE
2. Add AppQoE action
3. Add AppQoE policy
4. Binden Sie die AppQoE -Richtlinie an den virtuellen Server mit Lastenausgleich

Aktivieren Sie AppQoE

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns feature appqoe
```

Appqoe Aktion hinzufügen

Sie müssen eine AppQoE-Aktion hinzufügen, die Sie nach einem TCP-Reset und der Anzahl der Wiederholungsversuche erneut versuchen können.

```
add appqoe action reset_action -retryOnReset ( YES | NO )-numretries <
positive_integer>]
```

Beispiel:

```
add appqoe action reset_action -retryOnReset YES -numretries 5
```

Appqoe Richtlinie hinzufügen

Um AppQoE zu implementieren, müssen Sie die AppQoE-Richtlinie konfigurieren, um zu definieren, wie die Verbindungen in einer bestimmten Warteschlange in die Warteschlange gestellt werden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add appqoe policy <name> -rule <expression> -action <string>
```

Beispiel:

```
add appqoe policy reset_policy -rule HTTP.REQ.CONTENT_LENGTH.le(2000)-
action reset_action
```

> **Hinweis:**
>
> Sie können diese Konfiguration verwenden, wenn Sie es vorziehen, die Funktion zur Wiederholung der Anforderung für eine Inhaltslänge von weniger als 2000 einzuschränken.

Binden von virtuellen Lastenausgleichsserver an AppQoE-Richtlinie

Wenn ein Backend-Server eine TCP-Paketanforderung zurücksetzt und der virtuelle Lastausgleichsserver die Anforderung über eine bestimmte Warteschlange an den nächsten verfügbaren Dienst weiterleitet, müssen Sie den virtuellen Lastausgleichsserver an die AppQoE-Richtlinie binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

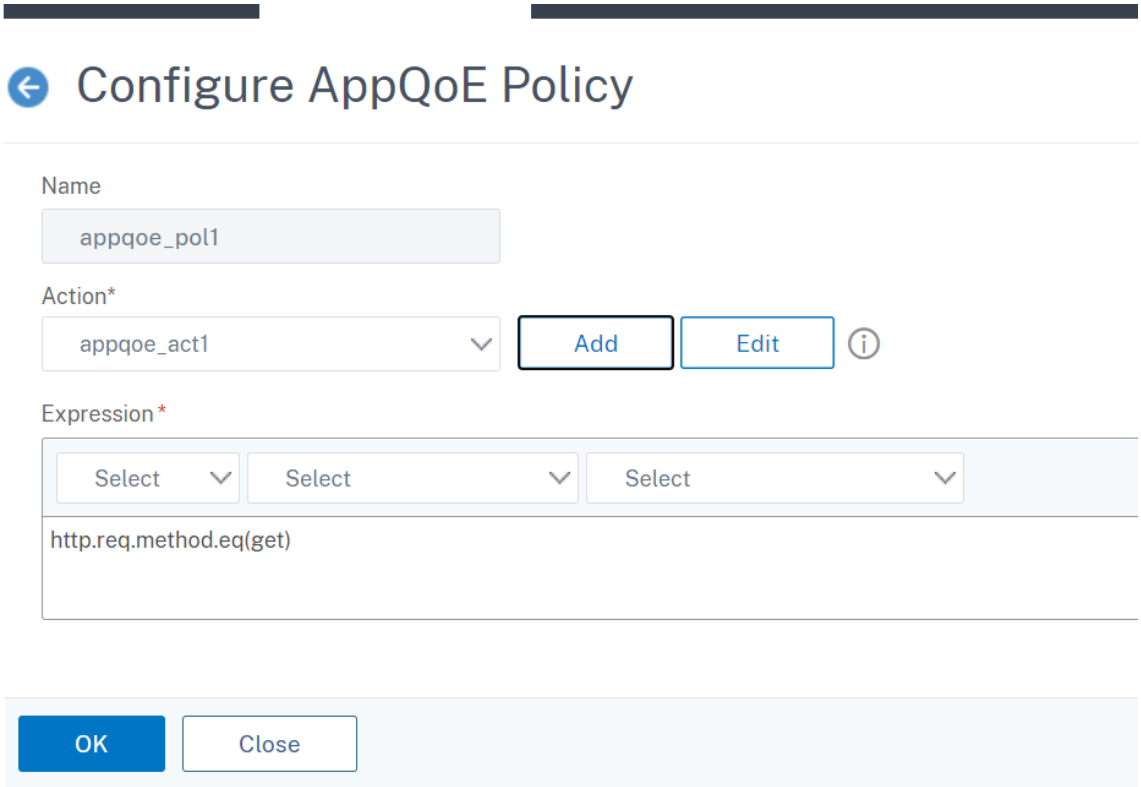
```
bind lb vserver <name> ((<serviceName> (-policyName <string> [-priority <
positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST
| RESPONSE )]
```

Beispiel:

```
bind lb vserver v1 -policyName reset_policy -type REQUEST -priority 1
```

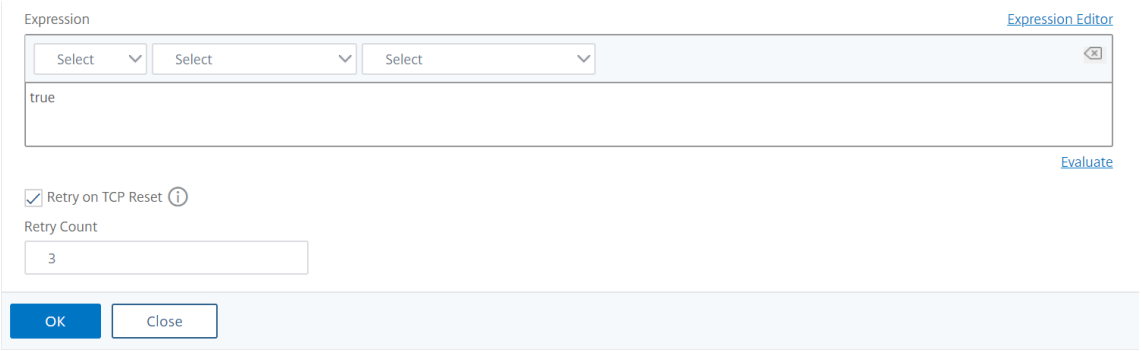
Konfigurieren der AppQoE-Richtlinie für die Wiederholung von Anfragen mithilfe der Citrix ADC GUI

1. Navigieren Sie zu **AppExpert** > **AppQoe** > **Richtlinien**.
2. Klicken Sie auf der **AppQoe-Richtlinienseite** auf **Hinzufügen**.
3. Legen Sie auf der Seite **Create an AppQoE Policy** die folgenden Parameter fest:
   a. Name. AppQoE -Richtlinienname
   b. Aktion. Fügen Sie eine Aktion hinzu oder bearbeiten Sie sie. Informationen zum Erstellen einer Aktion finden Sie im Abschnitt .
   c. Ausdruck. Wählen Sie einen `HTTP.REQ.CONTENT_LENGTH.le (2000)` Richtlinienausdruck aus oder
4. Klicken Sie auf **Erstellen** und **Schließen**.



Konfigurieren der AppQoE-Aktion für den Wiederholungsausgleich von Anfragen mithilfe der Citrix ADC GUI

1. Navigieren Sie zu **AppExpert** > **AppQoe** > **Action**.
2. Klicken Sie auf der **AppQoE -Aktionsseite** auf **Hinzufügen**.
3. Legen Sie auf der Seite **AppQoE Action erstellen** die folgenden Parameter für die Wiederholung beim TCP-Reset fest:
   a. Wiederholen Sie es bei TCP-Reset. Aktivieren Sie das Kontrollkästchen, um die Wiederholungsaktion für TCP-Reset zu aktivieren.
   b. Wiederholen Sie die Anzahl. Geben Sie die Anzahl der Wiederholungen ein.
4. Klicken Sie auf **Erstellen** und **Schließen**.



Konfigurieren der Wiederholung der Anfrage für die GET-Methode beim Zurücksetzen des Backend-Servers bei TCP-SYN-Einrichtung

Die CLI- und GUI-Konfiguration ähnelt den Schritten, die für die GET-Methode verfolgt werden. Weitere Informationen finden Sie unter Abschnitt Konfigurieren von Anforderungstversuchen für GET-Methode. wenn der Back-End-Server einen Verbindungsabschnitt zurücksetzt.

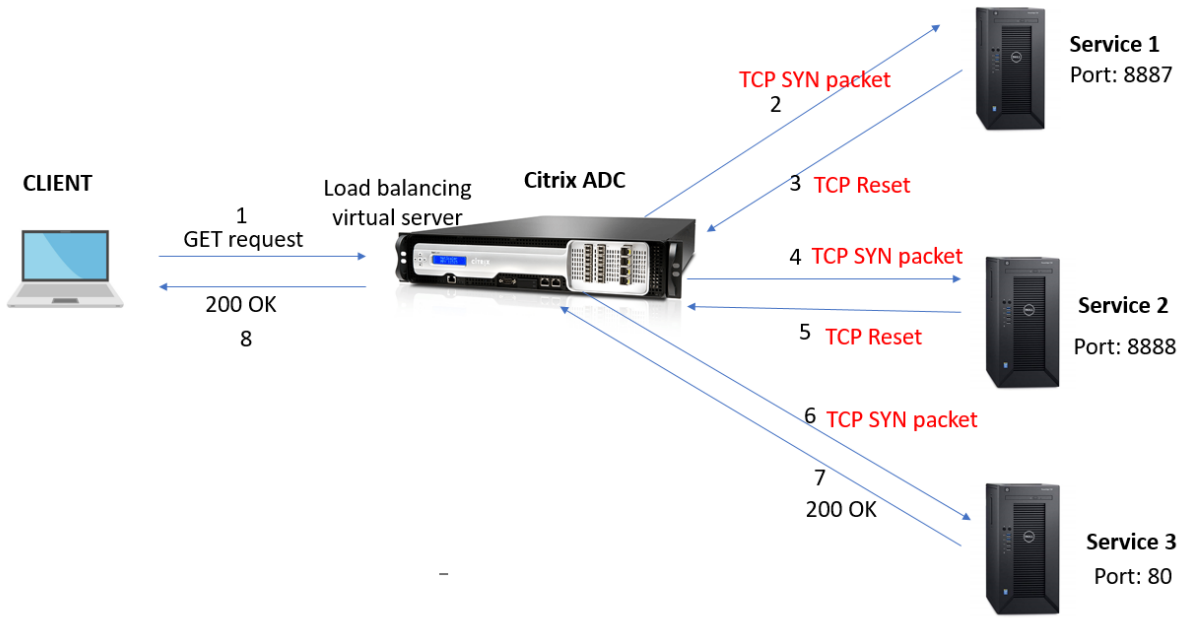
Wiederholungsversuche anfordern, wenn der Backend-Server während der Verbindungseinrichtung die TCP-Verbindung zurücksetzt

October 5, 2021

Wenn ein Back-End-Server eine TCP-Verbindung während des Verbindungsaufbaus zurücksetzt, leitet die Funktion zur Wiederholung der Anforderung die Anfrage an den nächsten verfügbaren Server weiter, anstatt den Reset an den Client zu senden. Durch den Reload-Balancing speichert der Client RTT, wenn die Appliance dieselbe Anfrage an den nächsten verfügbaren Dienst initiiert.

So funktioniert die Wiederholung der Anfrage, wenn der Back-End-Server eine TCP-Verbindung bei der SYN-Einrichtung zurücksetzt

Das folgende Diagramm zeigt, dass die Komponenten miteinander interagieren:



1. Der Prozess beginnt mit der Aktivierung der Appqoe-Funktion auf Ihrer Appliance.
2. Wenn der Client eine HTTP- oder HTTPS-Anfrage sendet, initiiert der virtuelle Lastausgleichsserver eine Verbindung zum Backend-Server.
3. Wenn der angeforderte Dienst bei TCP-SYN-Einrichtung nicht verfügbar ist, setzt der Backend-Server die TCP-Verbindung zurück.
4. Wenn in der Appqoe-Konfiguration “Wiederholung” mit der gewünschten Anzahl von Wiederholungsversuchen aktiviert ist, verwendet der virtuelle Lastausgleichsserver den konfigurierten Load Balancing-Algorithmus, um die Anforderung an den nächsten verfügbaren Anwendungsserver weiterzuleiten.
5. Nachdem der virtuelle Lastausgleichsserver die Antwort erhalten hat, leitet die Appliance die Antwort an den Client weiter.
6. Wenn die verfügbaren Back-End-Server gleich oder kleiner als die Wiederholungsanzahl sind und wenn alle Server einen Reset senden, würde die Appliance einen internen 500-Serverfehler beantworten. Betrachten Sie ein Szenario mit fünf verfügbaren Servern und der Wiederholungsanzahl, die auf sechs festgelegt ist. Wenn alle fünf Server die Verbindung zurücksetzen, gibt die Appliance einen internen 500-Serverfehler an den Client zurück.
7. Wenn die Anzahl der Back-End-Server höher ist als die Wiederholungsanzahl und wenn die Back-End-Server die Verbindung bei TCP-SYN-Einrichtung zurücksetzen, leitet die Appliance den Reset an den Client weiter. Stellen Sie sich ein Szenario mit drei Back-End-Servern und der Wieder-

holungsanzahl vor, die auf zwei festgelegt ist. Wenn die drei Server die Verbindung zurücksetzen, sendet die Appliance ein Reset-Paket an den Client.

Konfigurieren der Wiederholung der Anforderung (GET und POST-Methode), wenn der Back-End-Server bei TCP-SYN-Einrichtung zurückgesetzt wird

Die CLI- und GUI-Konfiguration ähnelt den Schritten, die für die GET- und POST-Methode befolgt werden. Weitere Informationen finden Sie unter Konfigurieren der Wiederholung der Anforderung für die GET-Methode, Konfigurieren der Wiederholung der Anforderung für die POST-Methode, wenn der Back-End-Server einen Verbindungsabschnitt zurücksetzt.

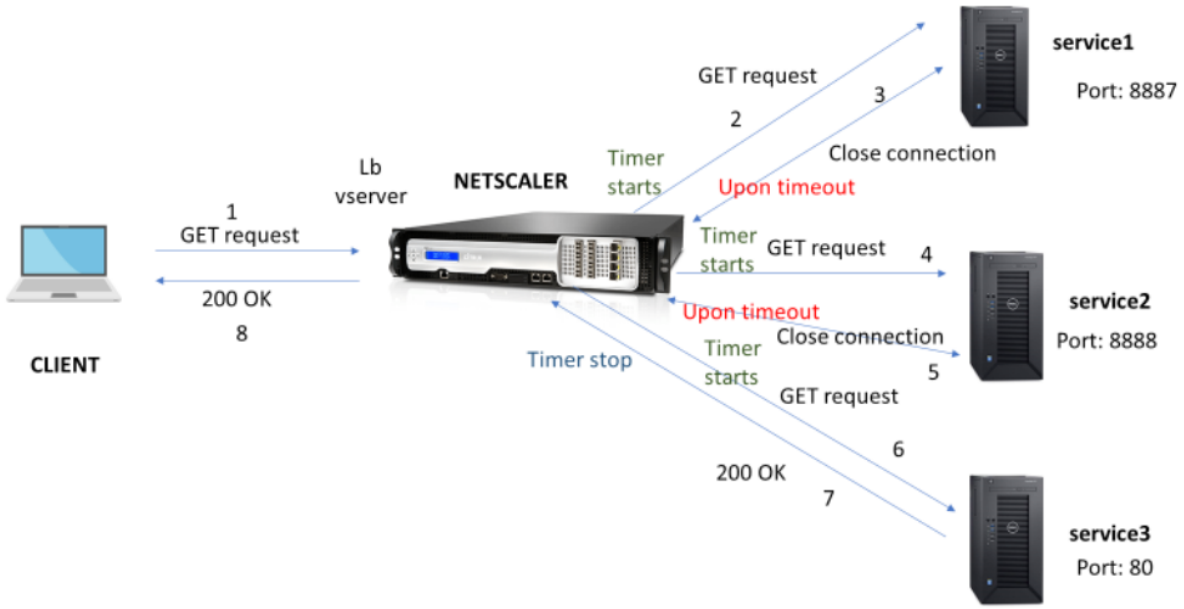
Wiederholungsversuche anfordern, wenn die Antwort auf den Backend-Server abgeht

October 5, 2021

Die Wiederholung von Anfragen ist für ein weiteres Szenario verfügbar, in dem die Appliance, wenn ein Back-End-Server mehr Zeit benötigt, um auf Anfragen zu antworten, nach dem Timeout einen erneuten Lastausgleich durchführt und die Anfrage an den nächsten verfügbaren Server weiterleitet.

So funktioniert die Wiederholung der Anforderung, wenn eine Zeitendigung der Backend-Server-Antwort

Das folgende Diagramm zeigt, dass die Komponenten miteinander interagieren:



1. Der Prozess beginnt mit der Aktivierung der Appqoe-Funktion auf Ihrer Appliance.
2. Die appqoe Konfiguration hat den Parameter “retryOnTimeout” in Millisekunden.
3. Wenn die Appliance eine Anfrage sendet und der Server mehr Zeit benötigt, um zu antworten, führt die Appliance einen erneuten Lastausgleich basierend auf dem konfigurierten Time-outwert durch. Die Appliance setzt die Verbindung zurück, wählt einen anderen Dienst und leitet die Anfrage weiter, anstatt auf die Serverantwort zu warten.
4. Nachdem der virtuelle Lastausgleichsserver die Antwort erhalten hat, leitet die Appliance die Antwort an den Client weiter. Die Verwendung eines Timeout-Parameters verhindert, dass die Appliance weiterhin auf eine Serverantwort wartet, die zu einem erhöhten RTT führt.
5. Wenn die verfügbaren Back-End-Server gleich oder kleiner als die Anzahl der Wiederholungen sind und wenn alle Server ein Timeout für die Anforderung haben, würde die Appliance einen internen 500-Serverfehler beantworten. Betrachten Sie ein Szenario mit fünf verfügbaren Servern und der Wiederholungsanzahl, die auf sechs festgelegt ist. Wenn alle fünf Server ein Timeout für die Anforderung haben, gibt die Appliance einen internen 500-Serverfehler an den Client zurück.
6. Wenn die Anzahl der Backend-Server höher ist als die Anzahl der Wiederholungsversuche und wenn der Back-End-Server bei einer Anfrage ein Timeout hat, wartet die Appliance weiterhin auf den letzten Dienst, bis der Server eine Antwort oder ein Timeout für die Verbindung mit dem Client sendet. Stellen Sie sich ein Szenario mit drei Back-End-Servern und der Wiederholungsanzahl vor, die auf zwei festgelegt ist. Wenn bei allen drei Servern ein Timeout aufwies, wartet die Appliance weiterhin auf den dritten Dienst, bis der Server eine Antwort sendet oder die Verbindungszeit des Clients im Leerlauf hat.

Konfigurieren Sie die Wiederholung der Anfrage (GET und POST-Methode), wenn eine Zeitendigung der Rücksende-Serverant

Um die Anforderungswiederholung für die GET-Methode im Timeout zu konfigurieren, müssen Sie die folgenden Schritte ausführen.

1. aktiviere appqoe
2. Konfigurieren der appqoe Aktion
3. Appqoe Richtlinie hinzufügen
4. Binden Sie die Appqoe-Richtlinie an den virtuellen Lastenausgleich

> **Hinweis:**
>
> Das Szenario “Wiederholung der Anforderung bei Zeitüberschreitung gilt auch für die POST-Methode.

aktiviere appqoe

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
enable ns feature appqoe
```

Fügen Sie eine appqoe Aktion für Timeout hinzu

Sie müssen die appqoe-Aktion konfigurieren, um es bei einem Timeout erneut zu versuchen und die Anzahl der Wiederholungsversuche zu definieren.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add appqoe action <name> -retryOnTimeout <msecs> -numRetries <positive_integer
>
```

Beispiel:

```
add appqoe action appact1 -retryOnTimeout 35 -numRetries 5
```

Appqoe Richtlinie hinzufügen

Um appqoe zu implementieren, müssen Sie die Appqoe-Richtlinie konfigurieren, um festzulegen, wie die Verbindungen in die Warteschlange gestellt werden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add appqoe policy <name> -rule <rule> -action <name>
```

Beispiel:

```
add appqoe policy timeout_policy -rule http.req.method.eq(get)-action
appact1
```


Binden Sie die Appqoe-Richtlinie an den virtuellen Server mit Lastenausgleich

Wenn ein Back-End-Server lange braucht, um zu antworten, und wenn Sie möchten, dass der virtuelle Lastausgleichsserver die Anforderung an den nächsten verfügbaren Dienst weiterleitet, müssen Sie die appqoe-Richtlinie an den Ausgleich des virtuellen Servers binden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
bind lb vserver <name> ((<serviceName> (-policyName <string> [-priority <
positive_integer>] [-gotoPriorityExpression <expression>] [-type ( REQUEST
| RESPONSE )]
```

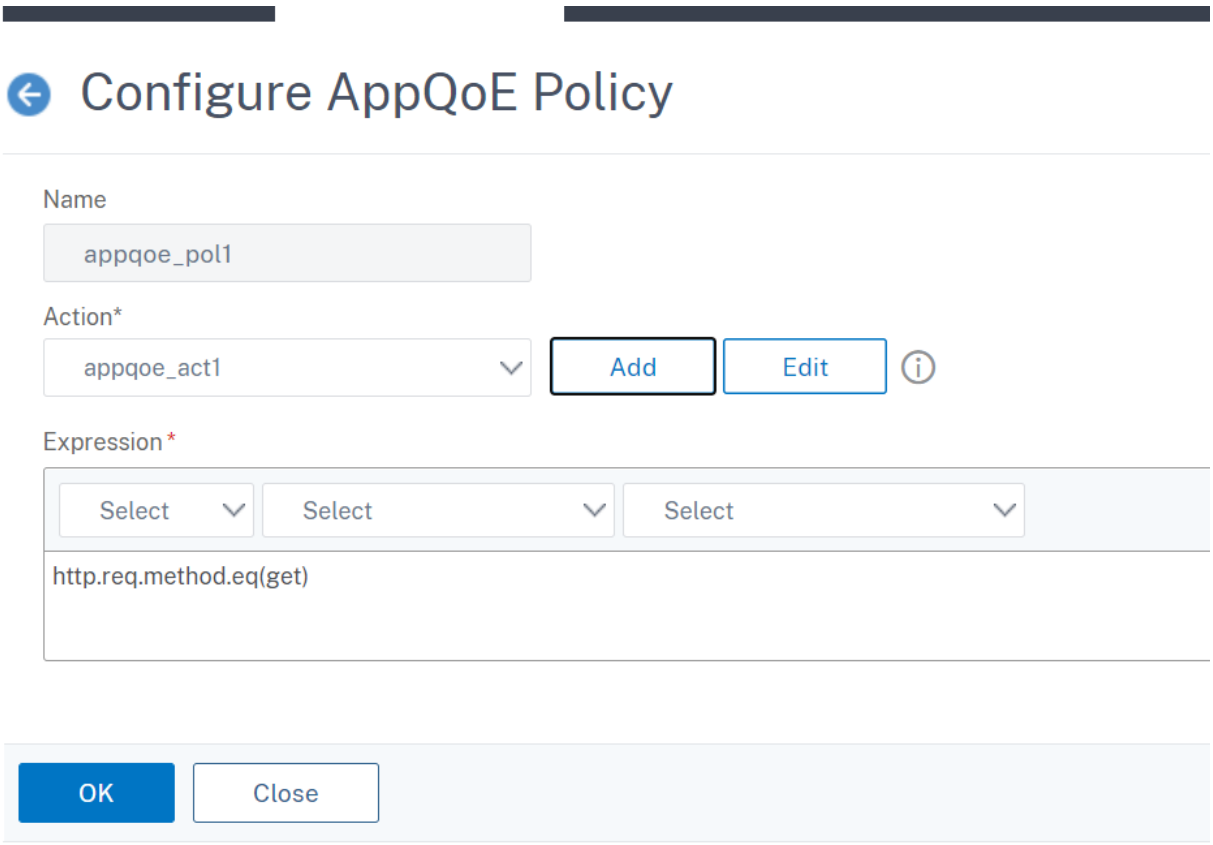
Beispiel:

```
bind lb vserver v1 -policyName timeout_policy -type REQUEST -priority 1
```

Konfigurieren der AppQoE-Richtlinie für das erneute Loadbalancing bei Timeout mithilfe der Citrix ADC GUI

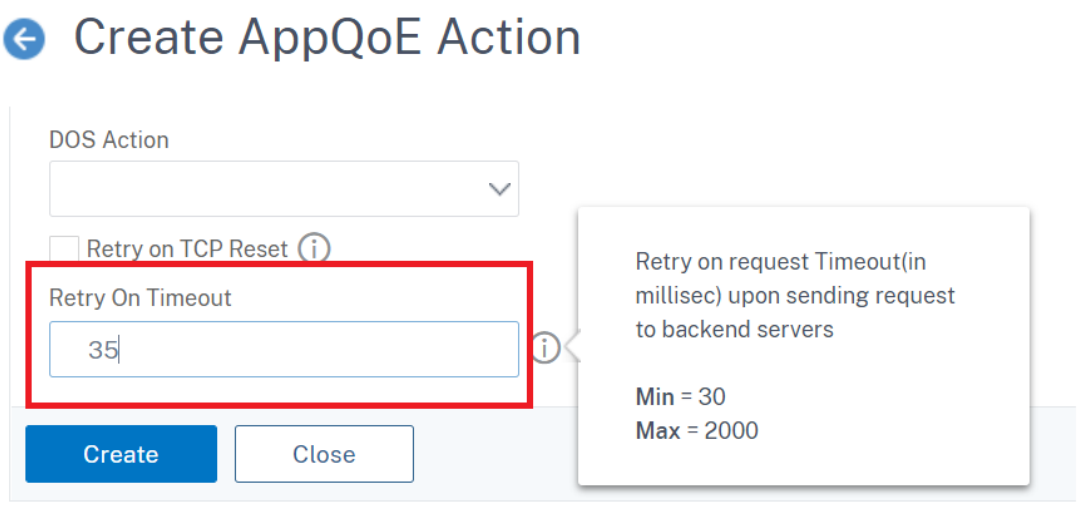
1. Navigieren Sie zu **AppExpert > AppQoe > Richtlinien**.
2. Klicken Sie auf der **AppQoe-Richtlinienseite** auf **Hinzufügen**.
3. Legen Sie auf der Seite **Create an AppQoE Policy** die folgenden Parameter fest:

   a. Name. AppQoE -Richtlinienname
   b. Aktion. Fügen Sie eine Aktion hinzu oder bearbeiten Sie sie. Informationen zum Erstellen einer neuen Aktion finden Sie im Abschnitt AppQoE -Aktion erstellen.
   c. Ausdruck. Wählen Sie den Richtlinienausdruck “http.req.method.eq (get)” aus oder geben Sie ein.
4. Klicken Sie auf **Erstellen** und **Schließen**.



Konfigurieren der AppQoE-Aktion für die Wiederholung von Anfragen mithilfe der Citrix ADC GUI

1. Navigieren Sie zu **AppExpert > AppQoe > Aktion**.
2. Klicken Sie auf der **AppQoE -Aktionsseite** auf **Hinzufügen**.
3. Legen Sie auf der Seite **AppQoE Action erstellen** den folgenden Parameter für die Wiederholung auf Back-End-Server-Antwortzeiten fest:
   a. Wiederholen Sie es bei Timeout. Wiederholen Sie das Timeout bei Anforderung (in Millisec), wenn Sie eine Anfrage an Backend-Server senden.
4. Klicken Sie auf **Erstellen** und **Schließen**.



TCP-Optimierung

October 5, 2021

TCP verwendet die folgenden Optimierungstechniken und Engpasskontrollstrategien (oder Algorithmen), um Netzwerküberlastung bei der Datenübertragung zu vermeiden.

Engpasskontrollstrategien

Der TCP wird seit langem verwendet, um Internetverbindungen herzustellen und zu verwalten, Übertragungsfehler zu behandeln und Webanwendungen reibungslos mit Clientgeräten zu verbinden. Der Netzwerkverkehr ist jedoch schwieriger zu kontrollieren, da der Paketverlust nicht nur von der Staus im Netzwerk abhängt und Staus nicht notwendigerweise zu Paketverlust führt. Daher sollte sich ein TCP-Algorithmus auf Paketverlust und Bandbreite konzentrieren, um Engpässe zu messen.

Proportional Rate Recovery (PRR) -Algorithmus

TCP Fast Recovery-Mechanismen reduzieren die Weblatenz, die durch Paketverluste verursacht wird. Der neue PRR-Algorithmus (Proportional Rate Recovery) ist ein schneller Recovery-Algorithmus, der TCP-Daten während einer Verlustwiederherstellung auswertet. Es wird nach der Rate-Halving gemustert, indem der Bruch verwendet wird, der für das Zielfenster geeignet ist, das vom Algorithmus zur Staus gewählt wird. Es minimiert die Fensteranpassung, und die tatsächliche Fenstergröße am Ende der Wiederherstellung liegt nahe am Slow-Start-Schwellenwert (ssthresh).

TCP Fast Open (TFO)

TCP Fast Open (TFO) ist ein TCP-Mechanismus, der einen schnellen und sicheren Datenaustausch zwischen einem Client und einem Server während des ersten Handshakes von TCP ermöglicht. Diese Funktion ist als TCP-Option im TCP-Profil verfügbar, das an einen virtuellen Server einer Citrix ADC Appliance gebunden ist. TFO verwendet ein TCP Fast Open Cookie (ein Sicherheits-Cookie), das die Citrix ADC Appliance generiert, um den Client zu validieren und zu authentifizieren, der eine TFO Verbindung zum virtuellen Server initiiert. Mit diesem TFO Mechanismus können Sie die Netzwerklatenz einer Anwendung um die Zeit reduzieren, die für eine vollständige Hin- und Rückfahrt erforderlich ist, was die Verzögerung bei kurzen TCP-Übertragungen erheblich reduziert.

Funktionsweise von TFO

Wenn ein Client versucht, eine TFO Verbindung herzustellen, enthält er ein TCP Fast Open Cookie mit dem anfänglichen SYN-Segment, um sich selbst zu authentifizieren. Wenn die Authentifizierung erfolgreich ist, kann der virtuelle Server auf der Citrix ADC Appliance Daten in das SYN-ACK-Segment aufnehmen, obwohl er nicht das endgültige ACK-Segment des Dreiwege-Handshakes erhalten hat. Dies spart bis zu einer vollständigen Hin- und Rückfahrt im Vergleich zu einer normalen TCP-Verbindung, die einen Dreiwege-Handshake erfordert, bevor Daten ausgetauscht werden können.

Ein Client und ein Back-End-Server führen die folgenden Schritte aus, um während des ersten TCP-Handshakes eine TFO-Verbindung herzustellen und Daten sicher auszutauschen.

1. Wenn der Client über kein TCP Fast Open Cookie verfügt, um sich selbst zu authentifizieren, sendet er eine Fast Open Cookie-Anforderung im SYN-Paket an den virtuellen Server auf der Citrix ADC Appliance.
2. Wenn die TFO-Option in dem TCP-Profil aktiviert ist, das an den virtuellen Server gebunden ist, generiert die Appliance ein Cookie (indem sie die IP-Adresse des Clients unter einem geheimen Schlüssel verschlüsselt) und antwortet dem Client mit einem SYN-ACK, das das generierte Fast Open Cookie in einem TCP-Optionsfeld enthält.
3. Der Client speichert das Cookie für zukünftige TFO-Verbindungen mit demselben virtuellen Server auf der Appliance.
4. Wenn der Client versucht, eine TFO Verbindung mit demselben virtuellen Server herzustellen, sendet er SYN, die das zwischengespeicherte Fast Open Cookie (als TCP-Option) zusammen mit HTTP-Daten enthält.
5. Die Citrix ADC Appliance validiert das Cookie, und wenn die Authentifizierung erfolgreich ist, akzeptiert der Server die Daten im SYN-Paket und erkennt das Ereignis mit einem SYN-ACK, TFO-Cookie und einer HTTP-Antwort an.

> **Hinweis:**
>
> Wenn die Clientauthentifizierung fehlschlägt, löscht der Server die Daten und bestätigt das Ereignis nur mit einem SYN, der ein Sitzungszeitlimit angibt.

1. Wenn auf Serverseite die TFO Option in einem an einen Dienst gebundenen TCP-Profil aktiviert ist, bestimmt die Citrix ADC Appliance, ob das TCP Fast Open Cookie in dem Dienst vorhanden ist, zu dem es versucht, eine Verbindung herzustellen.
2. Wenn das TCP Fast Open Cookie nicht vorhanden ist, sendet die Appliance eine Cookie-Anfrage im SYN-Paket.
3. Wenn der Back-End-Server das Cookie sendet, speichert die Appliance das Cookie im Server-Informationscache.
4. Wenn die Appliance bereits ein Cookie für das angegebene Ziel-IP-Paar hat, wird das alte Cookie durch das neue ersetzt.
5. Wenn das Cookie im Serverinformations-Cache verfügbar ist, wenn der virtuelle Server versucht, sich mit derselben SNIP-Adresse wieder mit demselben Back-End-Server zu verbinden, kombiniert die Appliance die Daten im SYN-Paket mit dem Cookie und sendet sie an den Back-End-Server.
6. Der Back-End-Server bestätigt das Ereignis sowohl mit Daten als auch mit einem SYN.

Hinweis: Wenn der Server das Ereignis nur mit einem SYN-Segment bestätigt, sendet die Citrix ADC Appliance das Datenpaket sofort erneut, nachdem das SYN-Segment und die TCP-Optionen aus dem ursprünglichen Paket entfernt wurden.

TCP schnelles Öffnen konfigurieren

Um die TCP-Funktion Fast Open (TFO) zu verwenden, aktivieren Sie die Option TCP Fast Open im entsprechenden TCP-Profil und setzen Sie den Parameter TFO Cookie Timeout auf einen Wert, der der Sicherheitsanforderung für dieses Profil entspricht.

Aktivieren oder Deaktivieren von TFO mit der CLI

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um TFO in einem neuen oder vorhandenen Profil zu aktivieren oder zu deaktivieren.

Hinweis: Der Standardwert ist DEAKTIVIERT.

```
1    add tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
2    set tcpprofile <TCP Profile Name> - tcpFastOpen ENABLED | DISABLED
3    unset tcpprofile <TCP Profile Name> - tcpFastOpen
4    Examples
5    add tcpprofile Profile1 - tcpFastOpen
```



```
6     Set tcpprofile Profile1 - tcpFastOpen Enabled
7     unset tcpprofile Profile1 - tcpFastOpen
8  <!--NeedCopy-->
```

So legen Sie den Timeout-Wert für TCP Fast Open Cookie mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
1     set tcpparam - tcpfastOpenCookieTimeout <Timeout Value>
2     Example
3     set tcpprofile - tcpfastOpenCookieTimeout 30secs
4  <!--NeedCopy-->
```

So konfigurieren Sie TCP Fast Open mit der GUI

1. Navigieren Sie zu **Konfiguration** > **System** > **Profile** >, und klicken Sie dann auf **Bearbeiten**, um ein TCP-Profil zu ändern.
2. Aktivieren Sie auf der Seite **TCP-Profil konfigurieren** das Kontrollkästchen **TCP Fast Open**.
3. Klicken Sie auf **OK** und dann auf **Fertig**.

So konfigurieren Sie den TCP Fast Cookie Timeout-Wert mit der GUI

Navigieren Sie zu **Konfiguration** > **System** > **Einstellungen** > **TCP-Parameter ändern** und dann Seite **TCP-Parameter konfigurieren**, um den TCP-Zeitüberschreitungswert für TCP Fast Open Cookie festzulegen.

TCP HyStart

Ein neuer TCP-Profilparameter, HyStart, ermöglicht den HyStart-Algorithmus, ein Langsamlauf-Algorithmus, der dynamisch einen sicheren Punkt zum Beenden bestimmt (ssthresh). Es ermöglicht einen Übergang zur Stauvermeidung ohne hohe Paketverluste. Dieser neue Parameter ist standardmäßig deaktiviert.

Wenn eine Überlastung festgestellt wird, tritt HyStart in eine Phase zur Vermeidung von Staus ein. Durch die Aktivierung erhalten Sie einen besseren Durchsatz in Hochgeschwindigkeitsnetzen mit hohem Paketverlust. Dieser Algorithmus hilft, bei der Verarbeitung von Transaktionen nahezu die maximale Bandbreite beizubehalten. Dadurch kann der Durchsatz verbessert werden.

Konfigurieren von TCP HyStart

Um die HyStart-Funktion zu verwenden, aktivieren Sie die Option Cubic HyStart im entsprechenden TCP-Profil.

So konfigurieren Sie HyStart mit der Befehlszeilenschnittstelle (CLI)

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um HyStart in einem neuen oder vorhandenen TCP-Profil zu aktivieren oder zu deaktivieren.

```
add tcpprofile <profileName> -hystart ENABLED
set tcpprofile <profileName> -hystart ENABLED
unset tcprofile <profileName> -hystart
<!--NeedCopy-->
```

Beispiele:

```
    add tcpprofile profile1 -hystart ENABLED
    set tcpprofile profile1 -hystart ENABLED
    unset tcprofile profile1 -hystart
<!--NeedCopy-->
```

So konfigurieren Sie die Unterstützung von HyStart mit der GUI

1. Navigieren Sie zu **Konfiguration** > **System** > **Profile** > und klicken Sie auf **Bearbeiten**, um ein TCP-Profil zu ändern.
2. Aktivieren Sie auf der Seite **TCP-Profil konfigurieren** das Kontrollkästchen **Cubic Hystart**.
3. Klicken Sie auf **OK** und dann auf **Fertig**.

TCP-Burstratensteuerung

Es wird beobachtet, dass TCP-Steuerungsmechanismen zu einem explosiven Verkehrsfluss in Hochgeschwindigkeitsnetzwerken führen können, was sich negativ auf die Gesamteffizienz des Netzwerks auswirkt. Aufgrund von Mobilfunkbedingungen wie Überlastung oder Layer-2-Weiterübertragung von Daten treten TCP-Bestätigungen beim Absender ein, der einen Übertragungsbruch auslöst. Diese Gruppen von aufeinanderfolgenden Paketen werden mit einer kurzen Interpaketlücke gesendet, es wird TCP-Paket-Burst genannt. Zur Überwindung des Datenverkehrs verwendet die Citrix ADC Appliance eine TCP-Burstratensteuerung. Diese Technik räumt Daten gleichmäßig in das Netzwerk über eine ganze Round-Trip-Zeit ein, so dass die Daten nicht in einen Burst gesendet werden. Mit dieser Methode zur Burstratensteuerung können Sie einen besseren Durchsatz und niedrigere Paketabfallraten erzielen.

Funktionsweise der TCP-Burstratensteuerung

In einer Citrix ADC Appliance verteilt diese Technik die Übertragung eines Pakets gleichmäßig über die gesamte Dauer der Round-Trip-Zeit (RTT). Dies wird durch die Verwendung eines TCP-Stacks und eines Netzwerkpaketplaners erreicht, der die verschiedenen Netzwerkbedingungen für die Ausgabe von Paketen für laufende TCP-Sitzungen identifiziert, um die Bursts zu reduzieren.

Statt Pakete sofort nach Erhalt einer Bestätigung zu übertragen, kann der Absender die Übertragung von Paketen verzögern, um sie mit der vom Scheduler (Dynamische Konfiguration) oder vom TCP-Profil (Feste Konfiguration) definierten Rate zu verteilen.

TCP-Burstratensteuerung konfigurieren

Verwenden Sie die Option TCP-Aufteilungsratensteuerung im entsprechenden TCP-Profil und legen Sie die Parameter für die Aufteilungsratensteuerung fest.

So legen Sie die TCP-Aufteilungsratensteuerung mit der Befehlszeile fest

Legen Sie an der Eingabeaufforderung einen der folgenden TCP-Burstratensteuerungsbefehle fest, der in einem neuen oder vorhandenen Profil konfiguriert ist.

Hinweis: Der Standardwert ist DISABLED.

```
1 add tcpprofile <TCP Profile Name> -burstRateControl Disabled | Dynamic
     | Fixed
2
3 set tcpprofile <TCP Profile Name> -burstRateControl Disabled | Dynamic
     | Fixed
4
5 unset tcpprofile <TCP Profile Name> -burstRateControl Disabled |
     Dynamic | Fixed
6 <!--NeedCopy-->
```

Hierbei gilt:

Disabled — Wenn die Burstratensteuerung deaktiviert ist, führt eine Citrix ADC Appliance nur die MaxBurst-Einstellung durch.

Fixed — Wenn die TCP-Aufteilungsratensteuerung Fixed lautet, verwendet die Appliance den im TCP-Profil erwähnten Sendewert für TCP-Verbindungsnutzlast.

Dynamic— Wenn die Burstratensteuerung Dynamisch ist, wird die Verbindung basierend auf verschiedenen Netzwerkbedingungen reguliert, um TCP-Bursts zu reduzieren. Dieser Modus funk-

tioniert nur, wenn sich die TCP-Verbindung im ENDPOINT-Modus befindet. Wenn die dynamische Burstratensteuerung aktiviert ist, ist der MaxBurst-Parameter des TCP-Profils nicht wirksam.

```
add tcpProfile  profile1 -burstRateControl Disabled

set tcpProfile profile1 -burstRateControl Dynamic

unset tcpProfile profile1 -burstRateControl Fixed
<!--NeedCopy-->
```

So legen Sie Parameter für die TCP-Burstratensteuerung mit der Befehlszeilenschnittstelle fest

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
    set ns tcpprofile nstcp_default_profile  - burstRateControl <type of
        burst rate control>  - tcprate <TCP rate> -rateqmax <maximum
       bytes in queue>

    T1300-10-2> show ns tcpprofile nstcp_default_profile
            Name: nstcp_default_profile
            Window Scaling status:  ENABLED
            Window Scaling factor: 8
            SACK status: ENABLED
            MSS: 1460
            MaxBurst setting: 30 MSS
            Initial cwnd setting: 16 MSS
            TCP Delayed-ACK Timer: 100 millisec
            Nagle's Algorithm: DISABLED
            Maximum out-of-order packets to queue: 15000
            Immediate ACK on PUSH packet: ENABLED
            Maximum packets per MSS: 0
            Maximum packets per retransmission: 1
            TCP minimum RTO in millisec: 1000
            TCP Slow start increment: 1
            TCP Buffer Size: 8000000 bytes
            TCP Send Buffer Size: 8000000 bytes
            TCP Syncookie: ENABLED
            Update Last activity on KA Probes: ENABLED
            TCP flavor: BIC
            TCP Dynamic Receive Buffering: DISABLED
```



```
25              Keep-alive probes: ENABLED
26              Connection idle time before starting keep-alive probes: 900
                    seconds
27              Keep-alive probe interval: 75 seconds
28              Maximum keep-alive probes to be missed before dropping
                   connection: 3
29              Establishing Client Connection: AUTOMATIC
30              TCP Segmentation Offload: AUTOMATIC
31              TCP Timestamp Option: DISABLED
32              RST window attenuation (spoof protection): ENABLED
33              Accept RST with last acknowledged sequence number: ENABLED
34              SYN spoof protection: ENABLED
35              TCP Explicit Congestion Notification: DISABLED
36              Multipath TCP: DISABLED
37              Multipath TCP drop data on pre-established subflow:
                   DISABLED
38              Multipath TCP fastopen: DISABLED
39              Multipath TCP session timeout: 0 seconds
40              DSACK: ENABLED
41              ACK Aggregation: DISABLED
42              FRTO: ENABLED
43              TCP Max CWND : 4000000 bytes
44              FACK: ENABLED
45              TCP Optimization mode: ENDPOINT
46              TCP Fastopen: DISABLED
47              HYSTART: DISABLED
48              TCP dupack threshold: 3
49              Burst Rate Control: Dynamic
50              TCP Rate: 0
51              TCP Rate Maximum Queue: 0
52  <!--NeedCopy-->
```

So konfigurieren Sie die TCP-Burstratensteuerung mit der GUI

1. Navigieren Sie zu **Konfiguration** > **System** > **Profile** >, und klicken Sie dann auf **Bearbeiten**, um ein TCP-Profil zu ändern.
2. Wählen Sie auf der Seite **TCP-Profil konfigurieren** aus der Dropdownliste die Option **TCP-Burst Control** aus:
   a) BurstRateCntrl
   b) CreditBytePrms
   c) RateBytePerms
   d) RateSchedulerQ
3. Klicken Sie auf **OK** und dann auf **Fertig**.

Schutz gegen Wrapped Sequence (PAWS) -Algorithmus

Wenn Sie die TCP-Zeitstempeloption im Standard-TCP-Profil aktivieren, verwendet die Citrix ADC Appliance den PAWS-Algorithmus (Protection Against Wrapped Sequence), um alte Pakete zu identifizieren und abzulehnen, deren Sequenznummern sich innerhalb des Empfangsfensters der aktuellen TCP-Verbindung befinden, da die Sequenz umgebrochen (seinen Maximalwert erreicht und von 0 neu gestartet).

Wenn Netzwerküberlastung ein Nicht-SYN-Datenpaket verzögert und Sie eine neue Verbindung öffnen, bevor das Paket eintrifft, kann das Umbrechen von Sequenznummern dazu führen, dass die neue Verbindung das Paket als gültig akzeptiert, was zu Datenbeschädigung führt. Wenn jedoch die TCP-Zeitstempeloption aktiviert ist, wird das Paket verworfen.

Standardmäßig ist die TCP-Zeitstempeloption deaktiviert. Wenn Sie es aktivieren, vergleicht die Appliance den TCP-Zeitstempel (Seg.tsval) im Header eines Pakets mit dem Wert für den letzten Zeitstempel (ts.Recent). Wenn Seg.tsval gleich oder größer als ts.Recent ist, wird das Paket verarbeitet. Andernfalls lässt die Appliance das Paket fallen und sendet eine Korrekturbestätigung.

Wie funktioniert PAWS?

Der PAWS-Algorithmus verarbeitet alle eingehenden TCP-Pakete einer synchronisierten Verbindung wie folgt:

1. Wenn `SEG.TSval` < `Ts.recent`: Das eingehende Paket ist nicht akzeptabel. PAWS sendet eine Bestätigung (wie in RFC-793 angegeben) und lässt das Paket fallen. Hinweis: Das Senden eines ACK-Segments ist erforderlich, um die Mechanismen von TCP zum Erkennen und Wiederherstellen von halboffenen Verbindungen beizubehalten.
2. Wenn das Paket außerhalb des Fensters liegt: PAWS lehnt das Paket ab, wie bei der normalen TCP-Verarbeitung.
3. Wenn `SEG.TSval` > das Paket `Ts.recent`: `PAWS` akzeptiert und verarbeitet.
4. Wenn `SEG.TSval` <= `Last.ACK.sent`(ankommendes Segment erfüllt): PAWS muss den `SEG.TSval` Wert nach kopieren `Ts.recent` (wird es nach Ts kopiert. Das jüngste Feld in der Datenbank?.
5. Wenn das Paket nacheinander ist: PAWS akzeptiert das Paket.
6. Wenn das Paket nicht in der Reihenfolge ist: Das Paket wird als normales TCP-Segment im Fenster behandelt. Beispielsweise kann es für eine spätere Zustellung in die Warteschlange gestellt werden.
7. Wenn der `Ts.recent` Wert länger als 24 Tage inaktiv ist: Die Gültigkeit von `Ts.recent` wird überprüft, wenn die Prüfung des PAWS-Zeitstempels fehlschlägt. Wenn sich herausstellt, dass der T.-Neult-Wert ungültig ist, wird das Segment akzeptiert und das `Ts.recent` mit dem TSval-Wert des neuen Segments `PAWS rule` aktualisiert.

So aktivieren oder deaktivieren Sie TCP-Zeitstempel mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
`set nstcpprofile nstcp_default_profile -TimeStamp (ENABLED | DISABLED)
    `
```

So aktivieren oder deaktivieren Sie TCP-Zeitstempel mit der GUI

Navigieren Sie zu **System** > **Profil** > **TCP-Profil**, wählen Sie das Standard-TCP-Profil aus, klicken Sie auf **Bearbeiten**, und aktivieren oder deaktivieren Sie das Kontrollkästchen **TCP-Zeitstempel**.

Optimierungstechniken

TCP verwendet die folgenden Optimierungstechniken und -methoden für optimierte Flusssteuerungen.

Richtlinienbasierte TCP-Profilauswahl

Der Netzwerkverkehr ist heute vielfältiger und bandbreitenintensiver als je zuvor. Mit dem erhöhten Datenverkehr ist die Wirkung, die Quality of Service (QoS) auf die TCP-Leistung hat, signifikant. Um QoS zu verbessern, können Sie jetzt AppQoE-Richtlinien mit unterschiedlichen TCP-Profilen für verschiedene Klassen von Netzwerkverkehr konfigurieren. Die AppQoE-Richtlinie klassifiziert den Datenverkehr eines virtuellen Servers, um ein TCP-Profil zu verknüpfen, das für einen bestimmten Typ von Datenverkehr optimiert ist, z. B. 3G, 4G, LAN oder WAN.

Um dieses Feature zu verwenden, erstellen Sie für jedes TCP-Profil eine Richtlinienaktion, ordnen Sie eine Aktion AppQoE-Richtlinien zu und binden Sie die Richtlinien an die virtuellen Server mit Lastenausgleich.

Informationen zur Verwendung von Abonnentenattributen zur TCP-Optimierung finden Sie unter Richtlinienbasiertes TCP-Profil.

Konfigurieren der Richtlinienbasierten TCP-Profilauswahl

Die Konfiguration der richtlinienbasierten TCP-Profilauswahl umfasst die folgenden Aufgaben:

- AppQoE wird aktiviert. Bevor Sie das TCP-Profilfeature konfigurieren, müssen Sie die AppQoE -Funktion aktivieren.
- AppQoE-Aktion hinzufügen. Nachdem Sie die AppQoE-Funktion aktiviert haben, konfigurieren Sie eine AppQoE-Aktion mit einem TCP-Profil.

- Konfigurieren der AppQoE-basierten TCP-Profilauswahl. Um die TCP-Profilauswahl für verschiedene Verkehrsklassen zu implementieren, müssen Sie AppQoE-Richtlinien konfigurieren, mit denen Ihr Citrix ADC die Verbindungen unterscheiden und die richtige AppQoe-Aktion an jede Richtlinie binden kann.
- Binden der AppQoE -Richtlinie an den virtuellen Server. Nachdem Sie die AppQoE-Richtlinien konfiguriert haben, müssen Sie sie an einen oder mehrere virtuelle Load Balancing-, Content Switching- oder Cache-Umleitungsserver binden.

Konfiguration über die Befehlszeilenschnittstelle

So aktivieren Sie AppQoE mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung die folgenden Befehle ein, um das Feature zu aktivieren, und überprüfen Sie, ob es aktiviert ist:

- `enable ns feature appqoe`
- `show ns feature`

So binden Sie ein TCP-Profil beim Erstellen einer AppQoE-Aktion mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung den folgenden appQoE-Aktionsbefehl mit der `tcpprofiletobind` Option ein.

```
add appqoe action <name> [-priority <priority>] [-respondWith ( ACS | NS )
[<CustomFile>] [-altContentSvcName <string>] [-altContentPath <string>] [-
maxConn <positive_integer>] [-delay <usecs>]] [-polqDepth <positive_integer
>] [-priqDepth <positive_integer>] [-dosTrigExpression <expression>] [-
dosAction ( SimpleResponse |HICResponse )] [-tcpprofiletobind <string>]
show appqoe action
```

So konfigurieren Sie eine AppQoE-Richtlinie mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
add appqoe policy <name> -rule <expression> -action <string>
```

So binden Sie eine AppQoE-Richtlinie an virtuelle Lastausgleichs-, Cache-Umleitungs- oder Content Switching-Server mit der Befehlszeilenschnittstelle

Geben Sie an der Eingabeaufforderung Folgendes ein:


```
bind cs vserver cs1 -policyName <appqoe_policy_name> -priority <priority>
bind lb vserver <name> - policyName <appqoe_policy_name> -priority <priority
>
bind cr vserver <name> -policyName <appqoe_policy_name> -priority <priority
>
```

Beispiel

```
1     add ns tcpProfile tcp1 -WS ENABLED -SACK ENABLED -WSVal 8 -nagle
         ENABLED -maxBurst 30 -initialCwnd 16 -oooQSize 15000 -minRTO 500
          -slowStartIncr 1 -bufferSize 4194304 -flavor BIC -KA ENABLED -
         sendBuffsize 4194304 -rstWindowAttenuate ENABLED -spoofSynDrop
         ENABLED -dsack enabled -frto ENABLED -maxcwnd 4000000 -fack
         ENABLED -tcpmode ENDPOINT
2     add appqoe action appact1 -priority HIGH -tcpprofile tcp1
3     add appqoe policy apppol1 -rule "client.ip.src.eq(10.102.71.31)" -
         action appact1
4     bind lb vserver lb2 -policyName apppol1 -priority 1 -
         gotoPriorityExpression END -type REQUEST
5     bind cs vserver cs1 -policyName apppol1 -priority 1 -
         gotoPriorityExpression END -type REQUEST
6  <!--NeedCopy-->
```

Konfigurieren der richtlinienbasierten TCP-Profilerstellung mit der GUI

So aktivieren Sie AppQoE mit der GUI

1. Navigieren Sie zu **System** > **Einstellungen**.
2. Klicken Sie im Detailbereich auf **Erweiterte Funktionen konfigurieren**.
3. Aktivieren Sie im Dialogfeld **Erweiterte Funktionen konfigurieren** das Kontrollkästchen **AppQoE**.
4. Klicken Sie auf **OK**.

So konfigurieren Sie die AppQoE -Richtlinie mit der GUI

1. Navigieren Sie zu **App-Expert** > **AppQoe** > **Aktionen** .
2. Führen Sie im Detailbereich eine der folgenden Aktionen aus:
3. Um eine neue Aktion zu erstellen, klicken Sie auf **Hinzufügen**.
4. Um eine vorhandene Aktion zu ändern, wählen Sie die Aktion aus, und klicken Sie dann auf **Bearbeiten**.

5. Geben **Sie im Bildschirm AppQoE-Aktion erstellen** oder im Fenster **AppQoE-Aktion konfigurieren** Werte für die Parameter ein oder wählen Sie sie aus. Der Inhalt des Dialogfensters entspricht den unter Parameter für die Konfiguration der AppQoE-Aktion beschriebenen Parametern wie folgt (Sternchen gibt einen erforderlichen Parameter an):
   a) Name — Name
   b) Aktionstyp: RespondWith
   c) Priorität — Priorität
   d) Richtlinienwarteschlangentiefe — polqDepth
   e) Warteschlangentiefe — priqDepth
   f) DOS-Aktion — dosAction
6. Klicken Sie auf **Erstellen**.

So binden Sie AppQoE-Richtlinie mit der GUI

1. Navigieren Sie zu **Traffic Management** > **Load Balancing** > **Virtuelle Server**, wählen Sie einen Server aus, und klicken Sie dann auf **Bearbeiten** .
2. Klicken Sie im Abschnitt **Richtlinien** auf (+), um eine AppQoE-Richtlinie zu binden.
3. Führen Sie im Schieberegler **Richtlinien** die folgenden Schritte aus:
   a) Wählen Sie einen Richtlinientyp als AppQoe aus der Dropdownliste aus.
   b) Wählen Sie einen Datenverkehrstyp aus der Dropdownliste aus.
4. Gehen Sie im Abschnitt **Richtlinienbindung** folgendermaßen vor:
   a) Klicken Sie auf **Neu**, um eine neue AppQoE-Richtlinie zu erstellen.
   b) Klicken Sie auf **Vorhandene Richtlinie**, um eine AppQoE-Richtlinie aus der Dropdownliste auszuwählen.
5. Legen Sie die **Bindungspriorität fest, und klicken Sie auf An die Richtlinie an den virtuellen Server binden** .
6. Klicken Sie auf **Fertig**.

SACK-Blockgenerierung

Die TCP-Leistung verlangsamt sich, wenn mehrere Pakete in einem Datenfenster verloren gehen. In einem solchen Szenario überwindet ein Selective Acknowledgment (SACK) -Mechanismus in Kombination mit einer selektiven Richtlinie zur wiederholten Weiterverbreitung dieser Einschränkung. Für jedes eingehende Out-of-Order-Paket müssen Sie einen SACK-Block generieren.

Wenn das Paket nicht in den Warteschlangenblock passt, fügen Sie Paketinformationen in den Block ein, und legen Sie die vollständigen Blockinformationen als SACK-0 fest. Wenn ein Paket außerhalb der Bestellung nicht in den Wiederzusammenbaublock passt, senden Sie das Paket als SACK-0 und wiederholen Sie die früheren SACK-Blöcke. Wenn ein nicht bestelltes Paket ein Duplikat ist und Paketinfo als SACK-0 gesetzt ist, dann ist D-SACK der Block.

Hinweis: Ein Paket gilt als D-SACK, wenn es sich um ein quittiertes Paket handelt, oder um ein veraltetes Paket, das bereits empfangen wurde.

Client-Abtrennung

Eine Citrix ADC Appliance kann das Reneging von Clients während der SACK-basierten Wiederherstellung verarbeiten.

Speicherprüfungen zur Kennzeichnung von end_point auf der Leiterplatte berücksichtigen nicht den gesamten verfügbaren Speicher

Wenn in einer Citrix ADC Appliance der Schwellenwert für die Speichernutzung auf 75 Prozent festgelegt ist, anstatt den gesamten verfügbaren Speicher zu verwenden, bewirkt dies, dass neue TCP-Verbindungen TCP-Optimierung umgehen.

Unnötige Weiterübertragungen durch fehlende SACK-Blocks

Wenn Sie in einem Nicht-Endpunkt-Modus DUPACKS senden, wenn SACK-Blöcke für wenige nicht in Ordnung bekommene Pakete fehlen, werden mehr erneute Übertragungen vom Server ausgelöst.

SNMP für Verbindungen hat Optimierung wegen Überlast umgangen

Die folgenden SNMP-IDs wurden einer Citrix ADC Appliance hinzugefügt, um die Anzahl der Verbindungen zu verfolgen, die TCP-Optimierungen aufgrund von Überlastung umgangen haben.

1. 1.3.6.1.4.1.5951.4.1.1.46.131 (tcpOptimizationEnabled). Um die Gesamtzahl der Verbindungen zu verfolgen, die mit TCP-Optimierung aktiviert sind.
2. 1.3.6.1.4.1.5951.4.1.1.46.132 (tcpOptimizationBypassed). Um die Gesamtzahl der Verbindungen zu verfolgen, wurde TCP-Optimierung umgangen.

Dynamischer Empfangspuffer

Um die TCP-Leistung zu maximieren, kann eine Citrix ADC Appliance nun die Größe des TCP-Empfangspuffers dynamisch anpassen.

Tail-Loss Sonde Algorithmus

Ein Retransmission Timeout (RTO) ist ein Verlust von Segmenten am Ende einer Transaktion. Ein RTO tritt auf, wenn Probleme mit der Anwendungslatenz auftreten, insbesondere bei kurzen Webtransaktionen. Um den Verlust von Segmenten am Ende einer Transaktion wiederherzustellen, verwendet TCP den Tail Loss Probe (TLP) -Algorithmus.

TLP ist ein Algorithmus für den Absender. Wenn eine TCP-Verbindung für einen bestimmten Zeitraum keine Bestätigung erhält, überträgt TLP das letzte nicht bestätigte Paket (Loss Probe). Bei einem Endverlust im Originalgetriebe löst Quittieren von Verlustsonde eine SACK- oder FACK-Wiederherstellung aus.

Konfigurieren der Tail Loss Probe

Um den TLP-Algorithmus (Tail Loss Probe) zu verwenden, müssen Sie die Option TLP im TCP-Profil aktivieren und den Parameter auf einen Wert festlegen, der der Sicherheitsanforderung für dieses Profil entspricht.

Aktivieren Sie TLP mit der Befehlszeile

Geben Sie an der Eingabeaufforderung einen der folgenden Befehle ein, um TLP in einem neuen oder vorhandenen Profil zu aktivieren oder zu deaktivieren.

> **Hinweis**:
>
> Der Standardwert ist DISABLED.

```
add tcpprofile <TCP Profile Name> - taillossprobe ENABLED | DISABLED

set tcpprofile <TCP Profile Name> - taillossprobe ENABLED | DISABLED

unset tcpprofile <TCP Profile Name> - taillossprobe
```

Beispiele:

```
add tcpprofile nstcp_default_profile - taillossprobe

set tcpprofile nstcp_default_profile -taillossprobe Enabled

unset tcpprofile nstcp_default_profile -taillossprobe
```

Konfigurieren des Tail Loss Probe-Algorithmus mit der Citrix ADC GUI

1. Navigieren Sie zu **Konfiguration** > **System** > **Profile** >, und klicken Sie dann auf **Bearbeiten**, um ein TCP-Profil zu ändern.
2. Aktivieren Sie auf der Seite **TCP-Profil konfigurieren** das Kontrollkästchen **Tail Loss Probe**.
3. Klicken Sie auf **OK** und dann auf **Fertig**.

Lösungen zur Problembehandlung für Citrix ADC

October 5, 2021

In diesem Artikel finden Sie einige grundlegende Lösungen zur Problembehandlung, die zur Behebung von Problemen in Ihrer Appliance erforderlich sind. Sie erhalten einen Überblick über die NetScaler Appliance, die Integration in das Netzwerk und die Probleme, die Sie bei grundlegenden Systemfunktionen erwarten können.

Aufzeichnen eines Pakettracings in Citrix ADC

June 21, 2022

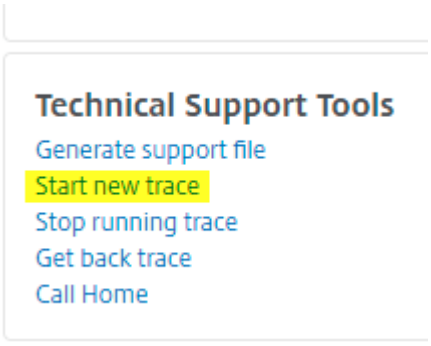
In diesem Artikel zur Fehlerbehebung wird erläutert, wie ein Administrator mithilfe der Citrix ADC GUI eine Netzwerkpaketverfolgung aufzeichnen kann.

Wichtige Punkte

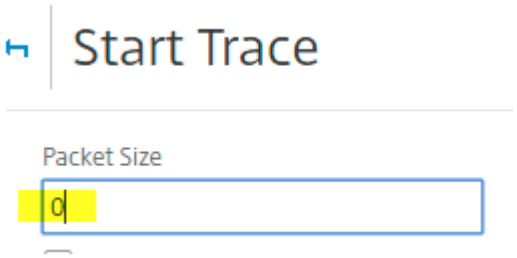
- Citrix empfiehlt die Verwendung der aktuellen Wireshark-Version aus dem “Abschnitt zum automatisierten Erstellen”, der auf der folgenden Webseite verfügbar ist: http://www.wireshark.org/download/automated.
- In Citrix ADC Version 11.1 oder höher, um die Erfassung zu entschlüsseln und sicherzustellen, dass ECC (Elliptic Curve Cryptography), Sitzungswiederverwendung und DH-Parameter auf dem virtuellen Server deaktiviert sind. Sie müssen dies tun, bevor Sie eine Spur aufnehmen.

Packet-Trace auf NetScaler Version 11.1 aufzeichnen

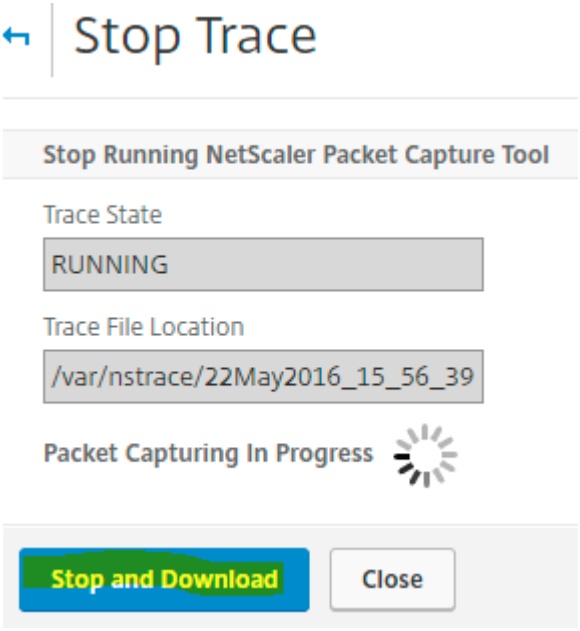
1. Navigieren Sie zur Seite **System** > **Diagnose** .
2. klicken Sie auf der **Diagnoseseite** auf den Link **Neue Ablaufverfolgung starten**, wie im folgenden Screenshot gezeigt.



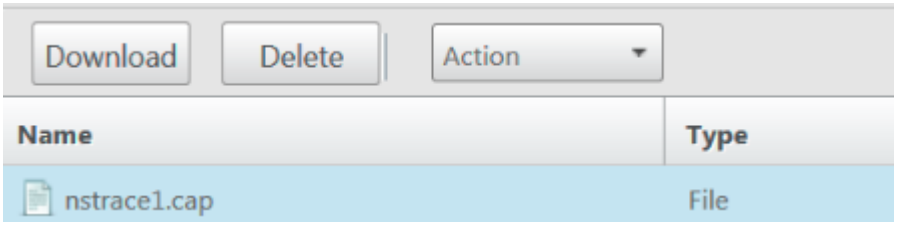
3. Aktualisieren Sie die Paketgröße im Feld **Paketgröße** auf 0.



4. Klicken Sie auf **Start**, um die Aufzeichnung des Netzwerk-Paket-Trace
5. Klicken Sie auf **Beenden und herunterladen**, um die Aufzeichnung des Netzwerk-Paket-Trace nach Abschluss des Tests zu beenden.

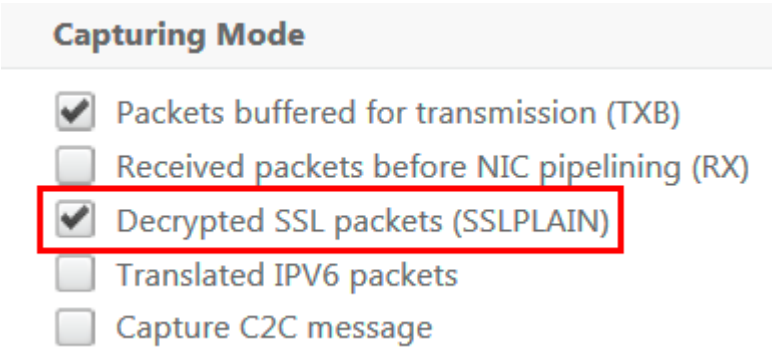


6. Wählen Sie die gewünschte Datei aus, klicken Sie auf **Auswählen** und dann auf **Herunterladen**.



7. Öffnen Sie die Netzwerk-Paket-Trace-Datei mit dem Wireshark-Dienstprogramm, um den Inhalt der Datei anzuzeigen.

> **Hinweis**: Wählen Sie Entschlüsselte SSL-Pakete (SSLPLAIN) aus, um die Paketverfolgung ohne den privaten Schlüssel zu entschlüsseln.



SSL-Masterschlüssel erfassen

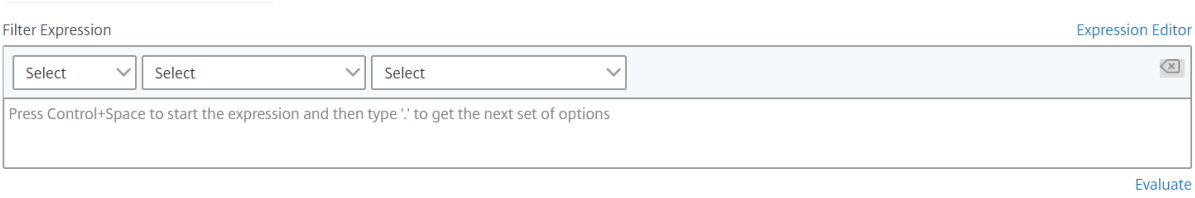
In der Version 11.0, 11.1 und höher gibt es eine Option zum Erfassen der Sitzungsschlüssel, die nur für diese bestimmte Sitzung/nstrace gültig ist. Diese Option kann verwendet werden, wenn Sie den privaten Schlüssel nicht teilen oder den SSLPLAIN-Modus verwenden möchten. Weitere Informationen finden Sie unter https://support.citrix.com/article/CTX135889.

Exportieren von Sitzungsschlüsseln ohne privaten Schlüssel zu teilen

In den meisten Szenarien ist der private Schlüssel nicht verfügbar oder wird nicht freigegeben. In solchen Szenarien können wir vorschlagen, die **SSL-Sitzungsschlüssel** anstelle des privaten Schlüssels zu exportieren. Lesen Sie,
[Exportieren und Verwenden von SSL-Sitzungsschlüsseln zum Entschlüsseln von SSL-Traces ohne gemeinsame Nutzung des privaten SSL-Keys, siehe https://support.citrix.com/article/CTX135889.

Filter

Außerdem wird immer empfohlen, IP-basierte Filter hinzuzufügen, während Spuren aufgezeichnet werden. Der Prozess stellt sicher, dass Sie nur interessierten Datenverkehr erfassen, was Ihre Fehlerbehebung erleichtert. Das Hinzufügen von Filtern verringert auch die Belastung des Geräts beim Aufnehmen von Spuren.



Einfache IP-basierte Filter reichen aus, um die richtigen Aufnahmen zu erhalten. Weitere Informationen zu `nstrace`-Filtern und -Beispielen finden Sie in der Citrix-Dokumentation .

Anwendungsfall zur Erfassung einer Paketverfolgung mit IP-Filter des virtuellen Servers (sowohl Front-End als auch Back-End)

Wenn Sie einen Filter der IP-Adresse des virtuellen Servers verwenden und die Option “—link” in der CLI aktivieren oder die Option “Gefilterten Verbindungs-Peer-Verkehr verfolgen” in der GUI (verfügbar ab Version 10.1) auswählen, können Sie sowohl den Front-End- als auch den Back-End-Verkehr für die IP-Adresse erfassen.

```
start nstrace -size 0 -filter "CONNECTION.IP.EQ(1.1.1.1)" -link ENABLED

show nstrace
        State:  RUNNING          Scope:  LOCAL            TraceLocation
           :  "/var/nstrace/24Mar2017_16_00_19/..." Nf:  24
                           Time:  3600             Size:  0
                          Mode:  TXB NEW_RX
        Traceformat:  NSCAP      PerNIC:  DISABLED        FileName:  24
           Mar2017_16_00_19 Filter:  "CONNECTION.IP.EQ(1.1.1.1)" Link:
            ENABLED          Merge:  ONSTOP           Doruntimecleanup
           :  ENABLED
        TraceBuffers:  5000      SkipRPC:  DISABLED       Capsslkeys:
           DISABLED    InMemoryTrace:  DISABLED
<!--NeedCopy-->
```

Erfassung zyklischer Spuren

Es ist immer schwierig, ein zeitweiliges Problem zu beheben. Die zyklische Ablaufverfolgung eignet sich am besten für intermittierende Probleme. Die Traces können über einen Zeitraum von wenigen Stunden oder Tagen ausgeführt werden, bevor das Problem auftritt. Sie können auch einen bestimmten Filter verwenden und die Größe der generierten Ablaufverfolgungsdateien auswerten, bevor Sie sie für eine längere Zeit ausführen.

Führen Sie den folgenden Befehl in der CLI aus:

```
start nstrace -nf 60 -time 30 -size 0
```



```
This particular trace will create 60 files each of them for 30 sec.
   This means the files will start getting overwritten after 60 trace
   files or 30 mins
Show nstrace à To check the status of the nstrace
Stop nstrace à To stop the nstrace.

<!--NeedCopy-->
```

Bewährte Methoden

Auf einer Einheit, die GB Verkehr pro Sekunde verarbeitet, ist das Erfassen von Datenverkehr ein sehr ressourcenintensiver Prozess. Die Auswirkungen auf Ressourcen beziehen sich hauptsächlich auf die CPU und den Speicherplatz. Die Auswirkungen auf den Speicherplatz können durch die Verwendung von Filterausdrücken reduziert werden. Die Auswirkungen auf die CPU bleiben jedoch bestehen und führen manchmal zu einem leichten Anstieg, da die Appliance nun Pakete gemäß dem Filter verarbeiten muss, bevor sie erfasst werden.

Die beste Vorgehensweise in Bezug auf die Rückverfolgung ist:

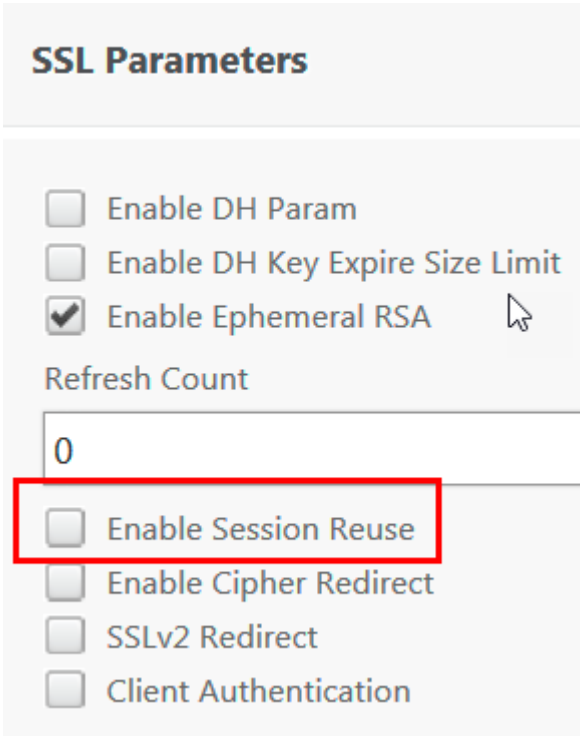
1. Die Dauer, für die die Ablaufverfolgung ausgeführt wird, muss so begrenzt wie möglich sein, wenn Sie dennoch sicherstellen, dass die Pakete von Interesse erfasst werden.
2. Planen Sie die Verfolgungsaktivität so ein, dass sie zu einem Zeitpunkt stattfindet, an dem die Anzahl der Benutzer (und damit der Verkehr) stark reduziert wird, z. B. außerhalb der Geschäftszeiten.

Weitere Ressourcen

Deaktivieren Sie die Wiederverwendung von Sitzungen auf einem virtuellen Server über die

Die Wiederverwendung von Sitzungen ist deaktiviert, wenn Sie einen Trace erfassen, um einen SSL-Handshake im Trace abzuschließen. Wenn es aktiviert ist, können Sie einen teilweisen Handshake in der Ablaufverfolgung erfassen. Stellen Sie sicher, dass Sie die Option nach der Trace-Erfassung aktivieren.
Deaktivieren Sie die Wiederverwendung einer SSL-Sitzung nicht, wenn die Persistenzmethode sslsession ist, da dies die Persistenz für bestehende Verbindungen beeinträchtigt. Weitere Informationen finden Sie unter https://support.citrix.com/article/CTX121925.

1. Öffnen Sie den virtuellen Server und navigieren Sie zu SSL-Parameter.
2. Deaktivieren Sie “Sitzungswiederverwendung aktivieren”, falls aktiviert



Deaktivieren Sie die Wiederverwendung von Sitzungen auf einem virtuellen Server über die CLI

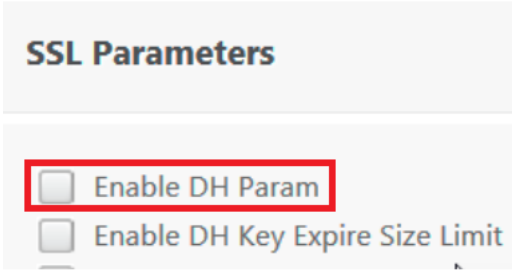
1. SSH an die Appliance-Konsole.
2. Führen Sie den folgenden Befehl aus, um DH Param vom virtuellen Server aus zu deaktivieren:

```
set ssl vserver "vServer_Name"-sessReuse DISABLED
```

DH-Parameter auf virtuellem Server über die GUI deaktivieren

Weitere Informationen zu DH-Parametern finden Sie unter https://support.citrix.com/article/CTX213335.

1. Öffnen Sie den virtuellen Server und navigieren Sie zu SSL-Parameter.
2. Deaktivieren Sie DH Param, falls aktiviert.



Deaktivieren Sie den DH-Parameter auf dem virtuellen Server über die CLI

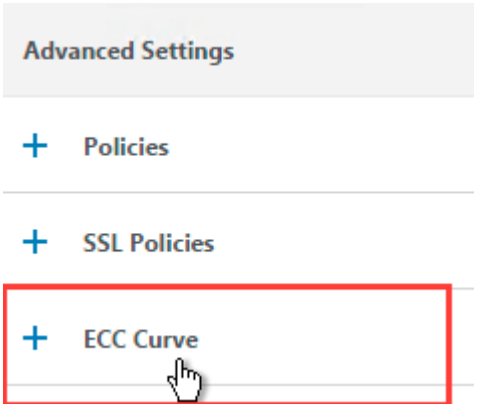
1. SSH an die Appliance-Konsole.
2. Führen Sie den folgenden Befehl aus, um DH Param vom virtuellen Server aus zu deaktivieren:

```
set ssl vserver "vServer_Name"-dh DISABLED
```

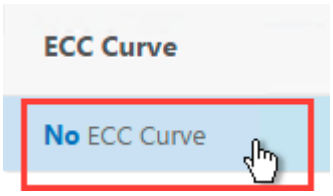
Deaktivieren Sie die ECC-Kurve auf dem virtuellen Server über die GUI

Die ECC-Kurve ist deaktiviert, um den erfassten SSL-Trace mit einem privaten Schlüssel zu entschlüssel Sie dürfen die Schlüssel nicht deaktivieren, wenn die zugehörigen SSL-Chiffren verwendet werden. Weitere Hinweise zur ECC-Kurve finden Sie unter https://support.citrix.com/article/CTX205289

1. Öffnen Sie den virtuellen Server und navigieren Sie zu ECC Curve.



2. Wenn keine ECC-Kurve an den virtuellen Server gebunden ist, ist keine weitere Aktion erforderlich.



3. Wenn eine ECC-Kurve an den virtuellen Server gebunden ist, klicken Sie auf die ECC-Kurve und lösen Sie sie vom virtuellen Server.

Deaktivieren Sie die ECC-Kurve auf dem virtuellen Server über die CLI

1. SSH an die Appliance-Konsole.
2. Führen Sie den folgenden Befehl für jede an den virtuellen Server gebundene ECC-Kurve aus:

```
unbind ssl vserver "vServer_Name"-eccCurveName "ECC_Curve_Name"
```


So geben Sie Speicherplatz im VAR-Verzeichnis frei, um Probleme mit einer Citrix ADC-Appliance zu protokollieren

October 5, 2021

Im folgenden Artikel wird erläutert, wie ein Administrator den Speicherplatz aus dem `/var` Verzeichnis einer Citrix ADC-Appliance freigeben kann. Sie können die Schritte ausführen, wenn auf die Citrix GUI nicht zugegriffen werden kann.

Wenn der Speicherplatz im Verzeichnis /var der Appliance gering ist, können Sie sich möglicherweise nicht bei der Citrix GUI anmelden. In diesem Szenario können Sie die alten Protokolldateien entfernen, um freien Speicherplatz im Verzeichnis /var zu erstellen.

Wichtige Punkte

- Stellen Sie sicher, dass Sie die Dateien sichern, bevor Sie die Dateien von der Appliance entfernen.

Führen Sie das folgende Verfahren aus, um Speicherplatz im `/var` Verzeichnis einer Citrix ADC-Appliance freizugeben:

1. Melden Sie sich mit SSH an der CLI von Citrix ADC an. Weitere Informationen zum Abschließen dieser Aufgabe finden Sie in der Citrix ADC Dokumentation.
2. Nachdem Sie sich bei der Citrix ADC CLI angemeldet haben, wechseln Sie mit dem folgenden Befehl zur Shell-Eingabeaufforderung. `shell`
3. Führen Sie den folgenden Befehl aus, um die Verfügbarkeit von Speicherplatz auf der Citrix ADC-Appliance anzuzeigen. `df -h`
4. Wenn die Speicherkapazität des `/var` Verzeichnisses bis zu 90 Prozent gefüllt ist, müssen Sie einige Dateien aus diesem Verzeichnis löschen.
   - Führen Sie die folgenden Befehle aus, um den Inhalt des Verzeichnisses /var anzuzeigen:
     ```
     cd /var
     ls -l
     ```

   Die Verzeichnisse, die normalerweise von Interesse sind, sind wie folgt:

```
/var/nstrace - This directory contains trace files.This is the
    most common reason for HDD being filled on the Citrix ADC
    appliance. This is due to an nstrace being left running for
    indefinite amount of time. All traces that are not of interest
    can and should be deleted. To stop an nstrace, go back to the
    CLI and issue stop nstrace command.
```



```
2
3 /var/log - This directory contains system specific log files.
4
5 /var/nslog - This directory contains Citrix ADC log files.
6
7 /var/tmp/support - This directory contains technical support files
    , also known as, support bundles. All files not of interest
    should be deleted.
8
9 /var/core - Core dumps are stored in this directory. There will be
     directories within this directory and they will be labeled
    with numbers starting with 1. These files can be quite large in
     size. Clear all files unless the core dumps are recent and
    investigation is required.
10
11 /var/crash - Crash files, such as process crashes are stored in
    this directory. Clear all files unless the crashes are recent
    and investigation is required.
12
13 /var/nsinstall -  Firmware is placed in this directory when
    upgrading. Clear all files, except the firmware that is
    currently being used.
```

- Überprüfen Sie, ob eines der Verzeichnisse mehr Speicherplatz belegt:

```
1 du -hs *
2 44k    cache
3 2.0k    clusterd
4 2.0k    configdb
5 6.0k    core
6 989M    crash
7 4.0k    cron
8 2.0k    dev
9 6.0k    download
10 2.0k    gui
11 2.0k    install
12 2.0k    krb
13 2.0k    learnt_data
14 122M    log
15 366M    NetScaler
16 14k    ns_gui
17 86k    ns_sys_backup
18 631M    nsinstall
```



```
883M    nslog
32k    nsproflog
2.0k    nssynclog
16k    nstemplates
36k    nstmp
4.5G    nstrace
8.1M    opt
6.0k    pubkey
52k    run
28M    safenet
72M    tmp
2.0k    vmtools
14k    vpn
```

- Löschen Sie die Dateien, die nicht benötigt werden:

```
rm -r nstrace/*
```

For more help on deleting files see FreeBSD Man Pages.

- Delete the files which are not required.
  `rm -r nstrace/*`
  For more help on deleting files see FreeBSD Man Pages.
- If the log or `nslog` directory is using more space, then run the following commands to open the log directory and view its contents:

```
cd /var/log
ls -l
cd /var/nslog
ls -l
```

1. Stellen Sie sicher, dass alle Dateien komprimiert sind. Dies wird durch die Dateinamenerweiterung .tar.gz angezeigt.
2. Wenn Sie Citrix ADM oder Command Center verwenden, überprüfen Sie das Verzeichnis /var/ns_system_backup. Stellen Sie sicher, dass Citrix ADM oder Command Center die erstellten Sicherungsdateien löscht.

Weitere Ressourcen

Informationen zu einem der im vorherigen Verfahren genannten Befehle finden Sie unter - http://ss64.com/bash/

Herunterladen von Kerndateien oder abgestürzten Dateien von der Citrix ADC Appliance

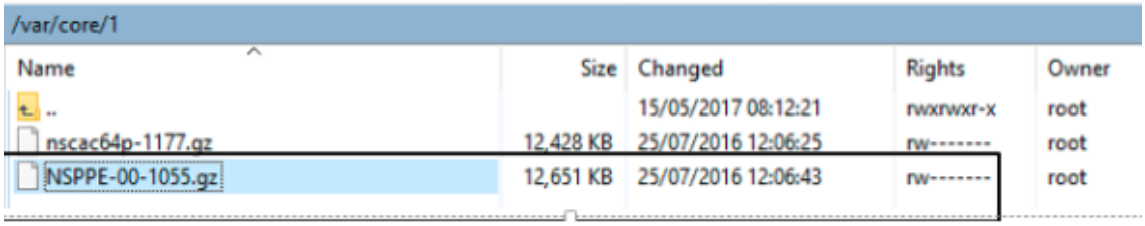
October 5, 2021

In diesem Artikel zur Fehlerbehebung wird erläutert, wie ein Administrator Kern- oder Absturzdateien von der Citrix ADC Appliance herunterladen kann.

Laden Sie Kern- oder Absturzdateien von der Citrix ADC Appliance mit dem SFTP-Client herunter

Gehen Sie folgendermaßen vor, um die Kern- oder Absturzdateien von einer NetScaler Appliance herunterzuladen:

1. Öffnen Sie WinSCP und melden Sie sich bei der NetScaler Management-IP-Adresse an.
2. Navigieren Sie/`var`/`core`/`1` zu dem, um die Dateien herunterzuladen.



> **Hinweis:**
>
> Um die neueste Crash- oder Core-Datei herunterzuladen, können Sie das WinSCP-Tool auch über die Befehlszeilenschnittstelle verwenden. Die Dateien können sich entweder im Kern- oder Absturzverzeichnis befinden.

So sammeln Sie Leistungsstatistiken und Ereignisprotokolle

October 5, 2021

Sie können Leistungsstatistiken virtueller Server und zugehöriger Dienste aus einer archivierten Datei `newnslog` im Verzeichnis `/var/nslog` erfassen. Die Dateien `newnslog` werden durch Ausführen von `/netscaler/nsconmsg` interpretiert.

Erfassen von Leistungsstatistiken und Ereignisprotokollen über die CLI

Sie können den Befehl `nsconmsg` an der Citrix ADC -Shell-Eingabeaufforderung ausführen, um Ereignisse zu melden.

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
/netscaler/nsconmsg -K /var/nslog/newnslog -d event
```

```
1 Displaying event information
2 NetScaler V20 Performance Data
3 NetScaler NS10.5: Build 57.7.nc, Date: May 14 2015, 07:35:21
4 rtime: Relative time between two records in milliseconds
5 seqno rtime event-message                          event-time
6 11648 16310 PPE-0 MonServiceBinding_10.104.20.110:443_(tcp-default)
7 <!--NeedCopy-->
```

Anzeigen der Zeitspanne, die von einer bestimmten “newnslog” -Datei abgedeckt wird

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
/netscaler/nsconmsg -K /var/nslog/newnslog -d setime
```

Die aktuellen Daten werden an die Datei `/var/nslog/newnslog` angehängt. NetScaler archiviert die Datei `newnslog` standardmäßig alle zwei Tage automatisch. Um die archivierten Daten zu lesen, müssen Sie das Archiv wie im folgenden Beispiel gezeigt extrahieren:

`cd /var/nslog` - Befehl, um von NetScaler Shell Prompt zu einem bestimmten Verzeichnis zu wechseln.

`tar xvfz newnslog.100.tar.gz` - Befehl zum Extrahieren der Tar-Datei.

`/netscaler/nsconmsg -K newnslog.100 -d setime` - Befehl, um die Zeitspanne zu überprüfen, die von der bestimmten Datei abgedeckt wird, in diesem Beispiel `newnslog.100`.

`ls -l` - Befehl überprüft alle Protokolldatei und Zeitstempel, die diesen Dateien zugeordnet sind.

```
root@NETSCALER## cd /var/nslog
root@NETSCALER## ls -l
```

```
1  wheel    461544 Aug  7  2014 newnslog.1.tar.gz
2 -rw-r--r--   1 root       wheel    191067 Aug  7  2014 newnslog.10.tar.
     gz
3 -rw-r--r--   1 root       wheel  11144873 Apr 26 22:04 newnslog.100.tar
     .gz
4 -rw-r--r--   1 root       wheel  11095053 Apr 28 22:04 newnslog.101.tar
     .gz
5 -rw-r--r--   1 root       wheel  11114284 Apr 30 22:04 newnslog.102.tar
     .gz
```



```
-rw-r--r--   1 root       wheel  11146418 May  2 22:04 newnslog.103.tar
    .gz
-rw-r--r--   1 root       wheel  11104227 May  4 22:04 newnslog.104.tar
    .gz
-rw-r--r--   1 root       wheel  11297419 May  6 22:04 newnslog.105.tar
    .gz
-rw-r--r--   1 root       wheel  11081212 May  8 22:04 newnslog.106.tar
    .gz
-rw-r--r--   1 root       wheel  11048542 May 10 22:04 newnslog.107.tar
    .gz
-rw-r--r--   1 root       wheel  11101869 May 12 22:04 newnslog.108.tar
    .gz
-rw-r--r--   1 root       wheel  11378787 May 14 22:04 newnslog.109.tar
    .gz
-rw-r--r--   1 root       wheel  44989298 Apr 11  2014 newnslog.11.gz
<!--NeedCopy-->
```

Anzeige der Zeitspanne innerhalb einer Datei

Verwenden Sie den Befehl `nsconmsg`, um nur eine Zeitspanne innerhalb der angegebenen Datei anzuzeigen, wie im folgenden Beispiel gezeigt:

```
/netscaler/nsconmsg -K /var/nslog/newnslog -s time=22Mar2007:20:00 -T 7 -s
ConLb=2 -d oldconmsg
```

Hierbei gilt:

`s` - time=22Mar2007:20:00:00 bedeutet am 22. März 2007 exakt um 20:00 Uhr starten.

`T 7` - Zeigt sieben Sekunden Daten an

`s` - Zeigt den Detailgrad der Lastausgleichsstatistiken an.

`d` - Zeigt statistische Informationen an.

> **Hinweis:**
>
> Ab ADC Release 12.1 müssen Sie auch zur "Zeit" Sekunden hinzufügen, das heißt: 22Mar2007:20:00:00

Die vom Parameter `-d oldconmsg` bereitgestellten statistischen Informationen werden alle sieben Sekunden aufgezeichnet. Das Folgende ist eine Beispielausgabe.

```
VIP(10.128.58.149:80:UP:WEIGHTEDRR): Hits(38200495, 18/sec) Mbps(1.02)
    Pers(OFF) Err(0)
Pkt(186/sec, 610 bytes) actSvc(4) DefPol(NONE) override(0)
Conn: Clt(253, 1/sec, OE[252]) Svr(3)
```



```
4  S(10.128.49.40:80:UP) Hits(9443063, 4/sec, P[2602342, 0/sec]) ATr(5)
       Mbps(0.23) BWlmt(0 kbits) RspTime(112.58 ms)
5  Other: Pkt(36/sec, 712 bytes) Wt(10000) RHits(31555)
6  Conn: CSvr(42, 0/sec) MCSvr(20) OE(16) RP(11) SQ(0)
7  S(10.128.49.39:80:UP) Hits(9731048, 4/sec, P[2929279, 0/sec]) ATr(9)
       Mbps(0.27) BWlmt(0 kbits) RspTime(161.69 ms)
8  Other: Pkt(41/sec, 756 bytes) Wt(10000) RHits(31555)
9  Conn: CSvr(32, 0/sec) MCSvr(19) OE(13) RP(4) SQ(0)
10 S(10.128.49.38:80:UP) Hits(9341366, 5/sec, P[2700778, 0/sec]) ATr(4)
       Mbps(0.27) BWlmt(0 kbits) RspTime(120.50 ms)
11 Other: Pkt(42/sec, 720 bytes) Wt(10000) RHits(31556)
12 Conn: CSvr(37, 0/sec) MCSvr(19) OE(13) RP(9) SQ(0)
13 S(10.128.49.37:80:UP) Hits(9685018, 4/sec, P[2844418, 0/sec]) ATr(3)
       Mbps(0.23) BWlmt(0 kbits) RspTime(125.38 ms)
14 Other: Pkt(38/sec, 670 bytes) Wt(10000) RHits(31556)
15 Conn: CSvr(32, 0/sec) MCSvr(20) OE(10) RP(7) SQ(0)
16 <!--NeedCopy-->
```

> **Hinweis:**
>
> Die Anzahl der Clientverbindungen der einzelnen Dienste summiert sich nicht zur Anzahl der Clientverbindungen des virtuellen Servers. Der Grund liegt in der Wiederverwendung von Sitzungen zwischen der Citrix ADC Appliance und dem Back-End-Service.

Ausgabe virtueller Server

```
VIP(10.128.58.149:80:UP:WEIGHTEDRR): Hits(38200495, 18/sec)Mbps(1.02)Pers(
OFF)Err(0)Pkt(186/sec, 610 bytes)actSvc(4)DefPol(NONE)override(0)Conn: Clt
(253, 1/sec, OE[252])Svr(3)
```

In der folgenden Liste werden die Statistiken des virtuellen Servers beschrieben:

1. `IP (IP address:port:state:Load balancing method)`. Die IP-Adresse und der Port der virtuellen IP-Adresse wie konfiguriert. Der Status des virtuellen Servers oder die virtuelle IP-Adresse lautet UP, DOWN oder OUT OF SERVICE; Lastausgleichsmethode für die virtuelle IP-Adresse konfiguriert.
2. `Hits (##)`. Anzahl der Anfragen, die den virtuellen Server erreicht haben
3. `Mbps (##)`. Gesamter Traffic Volume auf dem virtuellen Server (Rx + Tx) in Mbit/s umgewandelt
4. `Pers`: Art der konfigurierten Persistenz.
5. `Err (##)`. Häufigkeit, mit der eine Fehlerseite vom virtuellen Server generiert wurde.
6. `Pkt (##/sec, ## bytes)`: Volumen des Netzwerkverkehrs (als Pakete), der durch den virtuellen Server fließt, und durchschnittliche Paketgröße, die durch den virtuellen Server fließt.

7. actSvc(##). Anzahl der aktiven Dienste, die an den virtuellen Server gebunden sind
8. DefPol (RR). Gibt an, ob die standardmäßige Load Balancing-Methode aktiv ist. Die standardmäßige Load Balancing-Methode wird für eine Reihe von anfänglichen Anforderungen verwendet, um das Verhalten der anderen Methoden zu glätten.
9. Clt (##, ##/sec). Anzahl der aktuellen Clientverbindungen mit der Rate des virtuellen Servers.
10. OE [##]. Anzahl der Serververbindungen vom virtuellen Server im offenen Status.
11. Svr (##). Anzahl der aktuellen Serververbindungen vom virtuellen Server.

In der vorherigen Ausgabe Svr(3) gibt an, dass der Befehl die statistische Stichprobe sammelt. Es gibt drei aktive Verbindungen für den virtuellen Server mit dem Back-End-Server, obwohl es insgesamt vier Dienste gibt. Wenn ein Client eine Verbindung mit dem virtuellen Server herstellt, ist es nicht erforderlich, dass der Client Datenverkehr sendet oder empfängt, wenn der Befehl die Informationen sammelt. Daher ist es üblich, dass der Svr Zähler niedriger als die OE[] Zahl ist. Der Svr Zähler gibt die Anzahl der aktiven Verbindungen an, die aktiv Daten senden oder empfangen. Die zugeordnete IP-Adresse (MIP) oder Subnetz-IP-Adresse (SNIP) ist mit dem zugehörigen Back-End-Server verbunden. Und der Citrix ADC verfolgt den virtuellen Server, der mit dem Back-End-Server verbunden ist, und berechnet den Zähler.

Ausgabe virtueller Dienste

```
1 S(10.128.49.40:80:UP) Hits(9443063, 4/sec, P[2602342, 0/sec]) ATr(5)
     Mbps(0.23) BWlmt(0 kbits) RspTime(112.58 ms)
2 Other: Pkt(36/sec, 712 bytes) Wt(10000) RHits(31555)
3 Conn: CSvr(42, 0/sec) MCSvr(20) OE(16) RP(11) SQ(0)
4 <!--NeedCopy-->
```

In der folgenden Liste werden die Service-Statistiken beschrieben:

1. S (IP address:port:state). IP-Adresse, Port und Status des Dienstes wie DOWN, UP oder OUT OF SERVICE
2. Hits (##, P[##]). Anzahl der Anfragen, die an den Dienst gerichtet sind, Anzahl der Anforderungen, die aufgrund der konfigurierten Serverpersistenz an den Dienst gerichtet sind.
3. ATr (##). Anzahl der aktiven Verbindungen mit dem Dienst.

> **Hinweis:**
>
> Aktive Verbindungen sind Verbindungen, die die ausstehende Anfrage an den Dienst haben oder derzeit Traffic-Aktivitäten haben.

1. Mbps (##.####). Gesamtverkehrsaufkommen Volumen auf dem Service (Rx + Tx) in Mbit/s umgewandelt
2. BWlmt (## kbits): Definiertes Bandbreitenlimit.

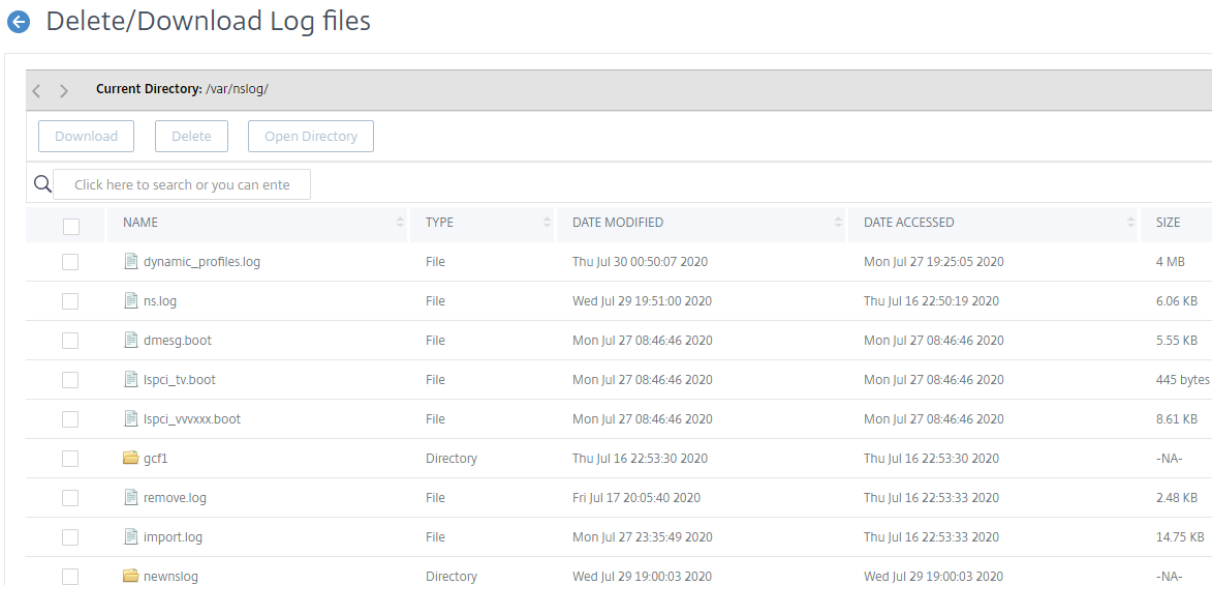
3. `RspTime (## ms)`. Durchschnittliche Reaktionszeit des Dienstes in Millisekunden.
4. `Pkt(##/sec, ##bytes)`. Verkehrsvolumen in Bezug auf Pakete pro Sekunde, die an den Dienst gehen; Durchschnittsgröße der Pakete.
5. `Wt (##)`. Gewichtindex, der im Load Balancing-Algorithmus verwendet wird.

> **Hinweis:**
>
> Wenn Sie diesen Wert durch 10.000 teilen, erhalten Sie das tatsächlich konfigurierte Gewicht des Dienstes.

1. `RHits (##)`. Laufender Anforderungszähler, der im Load Balancing-Algorithmus von Round
2. `CSvr (##, ##/sec)`. Anzahl der Verbindungen mit der Servicerate.
3. `MCSvr (##)`. Maximale Anzahl von Verbindungen mit dem Dienst.
4. `OE (##)`. Anzahl der Verbindungen mit dem Dienst im Status “Etabliert”.
5. `RP (##)`. Anzahl der Verbindungen mit dem Dienst, die sich im Wiederverwendungspool befinden.
6. `SQ (##)`. Anzahl der Verbindungen zum Dienst, die in der Überspannungswarteschlange warten.

Erfassen Sie Performance-Statistiken und Ereignisprotokolle mit der Citrix ADC GUI

1. Navigieren Sie zu **System > Diagnostics > Wartung > Log-Dateien löschen/herunterladen**.
2. Wählen Sie eine Datei aus und klicken Sie auf **Herunterladen**, um die Datei herunterzuladen.



So konfigurieren Sie die Drehung der Protokolldatei

October 5, 2021

Die Citrix ADC Appliance generiert Protokolle in mehreren Verzeichnissen und in verschiedenen Formaten. Einige dieser Protokolle werden nicht standardmäßig gedreht und können an Größe zunehmen und zu viel Speicherplatz belegen. Durch die Verwendung der mitgelieferten Dienstprogramme für die Protokollrotation (`newsyslog`) können Sie diese Protokolle konsistent verwalten, indem Sie nur relevante Informationen für eine einfachere Verwaltung und Verwaltung aufbewahren.

Das in der Citrix ADC -Firmware enthaltene `newsyslog` Dienstprogramm archiviert Protokolldateien und rotiert die Systemprotokolle, sodass das aktuelle Protokoll während der Rotation leer ist. Die Systemcrontab führt dieses Dienstprogramm stündlich aus und liest die Konfigurationsdatei, die die zu rotierenden Dateien und die Bedingungen angibt. Die archivierten Dateien werden möglicherweise bei Bedarf komprimiert.

Die bestehende Konfiguration befindet sich in `/etc/newsyslog.conf`. Da sich diese Datei jedoch im Speicherdateisystem befindet, muss der Administrator die Änderungen speichern, `/nsconfig/newsyslog.conf` damit die Konfiguration den Neustart des NetScaler überlebt.

Die in dieser Datei enthaltenen Einträge haben das folgende Format:
`logfilename [owner:group] mode count size when flags [/pid_file] [sig_num]`

> **Hinweis:**
>
> Felder in eckigen Klammern sind optional und können weggelassen werden.

Jede Zeile in der Datei steht für eine Protokolldatei und die Bedingungen, unter denen eine Rotation erfolgen muss.

Im Beispiel zeigt das `size` Feld an, dass die Größe von `ns.log` 100 Kilobyte beträgt. Das `count` Feld zeigt an, dass die Anzahl der archivierten `ns.log` Dateien 25 ist. Eine Größe von 100 K und eine Anzahl von 25 sind die Standardwerte für Größe und Anzahl.

> **Hinweis:**
>
> Wenn das Feld mit einem Sternchen (*) konfiguriert ist, bedeutet dies, dass die Datei ns.log nicht basierend auf der Zeit gedreht wird. Jede Stunde führt ein crontab-Job das `newsyslog` Dienstprogramm aus, das überprüft, ob die Größe von ns.log größer oder gleich der in dieser Datei konfigurierten Größe ist. Wenn es in diesem Beispiel größer oder gleich 100 K ist, rotiert es diese Datei.

```
root@ns# cat /etc/newsyslog.conf
# Netscaler newsyslog.conf

```



```
# This file is present in the memory filesystem by default, and any
    changes
# to this file will be lost following a reboot. If changes to this file
# require persistence between reboots, copy this file to the /nsconfig
# directory and make the required changes to that file.
#
# logfilename [owner:group] mode count size when flags [/pid_file] [
    sig_num]
/var/log/cron 600 3 100 * Z
/var/log/amd.log 644 7 100 * Z
/var/log/auth.log 600 7 100 * Z
/var/log/ns.log 600 25 100 * Z
<!--NeedCopy-->
```

Das `size` Feld kann geändert werden, um die Mindestgröße der `ns.log` Datei zu ändern, oder das Feld kann geändert werden, um die `ns.log` Datei basierend auf einer bestimmten Zeit zu drehen.

Die tägliche, wöchentliche und/oder monatliche Spezifikation wird wie folgt angegeben: `[Dhh]`und `[Dhh [Mdd]]`. Die Freilichtfelder für die Tageszeit, die optional sind, sind standardmäßig auf Mitternacht festgelegt. Die Bereiche und Bedeutungen für diese Spezifikationen sind:

```
Hh hours, range 0 ... 23
w day of week, range 0 ... 6, 0 = Sunday
dd day of month, range 1 ... 31, or the letter L or l to specify the
    last day of the month.
<!--NeedCopy-->
```

Beispiele:

Hier sind einige Beispiele mit Erläuterungen für die Logs, die standardmäßig gedreht werden:

`/var/log/auth.log 600 7 100 * Z`

Das Authentifizierungsprotokoll wird gedreht, wenn die Datei 100 K erreicht, die letzten 7 Kopien der Datei archiviert und mit gzip (Z-Flag) komprimiert, und den resultierenden Archiven werden die folgenden Berechtigungen zugewiesen - rw-. auth.log

`/var/log/all.log 600 7 * @T00 Z`

Das Catch-All-Protokoll wird jede Nacht um Mitternacht um 7 Mal gedreht (@T00) und mit gzip komprimiert. Die resultierenden Archive erhalten die folgenden Berechtigungen —rw-r—.

`/var/log/weekly.log 640 5 * $W6D0 Z`

Das wöchentliche Protokoll wird jeden Montag um Mitternacht um 5 Mal gedreht. Die resultierenden Archive werden mit Berechtigungen zugewiesen.

Allgemeine Rotationsmuster:

- `D0`. drehen jede Nacht um Mitternacht
- `D23`. jeden Tag um 23:00 Uhr drehen
- `W0D23`. wechseln jede Woche am Sonntag um 23:00 Uhr
- `W5`. wechseln jede Woche am Freitag um Mitternacht
- `MLD6`. am letzten Tag eines jeden Monats um 6:00 Uhr drehen
- `M5`. an jedem fünften Tag des Monats um Mitternacht drehen

Wenn beide ein Intervall und eine Zeitangabe angegeben sind, müssen beide Bedingungen erfüllt sein. Das heißt, die Datei muss so alt oder älter als das angegebene Intervall sein, und die aktuelle Zeit muss mit der Zeitangabe übereinstimmen.

Sie können die minimale Dateigröße steuern, aber es gibt keine Begrenzung für die Dateigröße, bevor das `newsyslog` Dienstprogramm in der nächsten Stunde an die Reihe kommt.

Debuggen Sie newsyslog:

Um das Verhalten des `newsyslog` Dienstprogramms zu debuggen, fügen Sie das ausführliche Flag hinzu.

```
root@dj_ns# newsyslog -v
/var/log/cron <3Z>: size (Kb): 31 [100] --> skipping
/var/log/amd.log <7Z>: does not exist, skipped.
/var/log/auth.log <7Z>: size (Kb): 2 [100] --> skipping
/var/log/kerberos.log <7Z>: does not exist, skipped.
/var/log/lpd-errs <7Z>: size (Kb): 0 [100] --> skipping
/var/log/maillog <7Z>: --> will trim at Tue Mar 24 00:00:00 2009
/var/log/sendmail.st <10>: age (hr): 0 [168] --> skipping
/var/log/messages <5Z>: size (Kb): 7 [100] --> skipping
/var/log/all.log <7Z>: --> will trim at Tue Mar 24 00:00:00 2009
/var/log/slip.log <3Z>: size (Kb): 0 [100] --> skipping
/var/log/ppp.log <3Z>: does not exist, skipped.
/var/log/security <10Z>: size (Kb): 0 [100] --> skipping
/var/log/wtmp <3>: --> will trim at Wed Apr 1 04:00:00 2009
/var/log/daily.log <7Z>: does not exist, skipped.
/var/log/weekly.log <5Z>: does not exist, skipped.
/var/log/monthly.log <12Z>: does not exist, skipped.
/var/log/console.log <5Z>: does not exist, skipped.
/var/log/ns.log <5Z>: size (Kb): 18 [100] --> skipping
/var/log/nsvpn.log <5Z>: size (Kb): 0 [100] --> skipping
/var/log/httperror.log <5Z>: size (Kb): 1 [100] --> skipping
/var/log/httpaccess.log <5Z>: size (Kb): 1 [100] --> skipping
root@dj_ns#
<!--NeedCopy-->
```


So geben Sie Speicherplatz in einem /Flash-Verzeichnis in einer Citrix ADC Appliance frei

October 5, 2021

In diesem Artikel zur Fehlerbehebung wird erläutert, wie ein Administrator Speicherplatz aus dem /flash Verzeichnis einer Citrix ADC Appliance freigeben kann.

Vorgehensweise zum Freigeben von Speicherplatz im /flash Verzeichnis einer Citrix ADC Appliance

1. Melden Sie sich mit SSH an der CLI von Citrix ADC an.
2. Nachdem Sie sich bei der Citrix ADC CLI angemeldet haben, wechseln Sie mit dem folgenden Befehl zur Shell-Eingabeaufforderung.`shell`.
3. Führen Sie den `df -h` Befehl aus, um die Verfügbarkeit von Speicherplatz auf der Citrix ADC Appliance anzuzeigen.
4. Wenn die Kapazität des Verzeichnisses /flash mehr als 90 Prozent oder niedrig ist, müssen Sie einige Dateien aus diesem Verzeichnis löschen.
5. Führen Sie die folgenden Befehle aus, um den Inhalt des /flash -Verzeichnisses anzuzeigen:

```
cd /flash
ls -l
```

6. Möglicherweise finden Sie mehrere Dateien verschiedener Versionen des NetScaler Software-Releases. Stellen Sie sicher, dass die an diesem Speicherort vorhandenen Dateien für die aktuelle Version der NetScaler-Software auf Ihrer Appliance gelten. Führen Sie den folgenden Befehl aus, um alle anderen Dateien von der Appliance zu entfernen.

```
rm <filename>
```

> **Hinweis:**
>
> Entferne nur die älteren Versionen des Kernels. Das /flash Verzeichnis muss die Dateien enthalten, die die aktuelle Version oder der aktuelle Build der NetScaler-Softwareversion verwendet,

> und die Datei kernel.gz. Citrix empfiehlt, diese Dateien nicht aus dem /flash Verzeichnis zu entfernen.

Referenzmaterial

December 3, 2021

Verwenden Sie diese Referenzinformationen, um ein vertieftes Verständnis der folgenden Citrix ADC Komponenten zu erhalten:

Citrix ADC SNMP OIDs - Details der SNMP-OIDs, mit denen Informationen von einer Citrix ADC Appliance abgerufen werden können.

Citrix ADC Syslog Messages - Details zu den Syslog-Nachrichten, die von der Citrix ADC Appliance bereitgestellt werden.

Citrix ADC CLI-Befehle - Details zu den Befehlen, mit denen die Citrix ADC Appliance über die CLI konfiguriert werden kann. Sie können auch die Details jedes Befehls in der CLI anzeigen, indem Sie den `man <ns-command-name>` Befehl eingeben.

Citrix NITRO API-Referenz - Details zu allen Vorgängen, die mithilfe der REST-API auf der Citrix ADC Appliance ausgeführt werden können.

Citrix ADC Advanced Policy Expressions - Details zu den Ausdrücken, mit denen erweiterte Richtlinien definiert werden können.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States